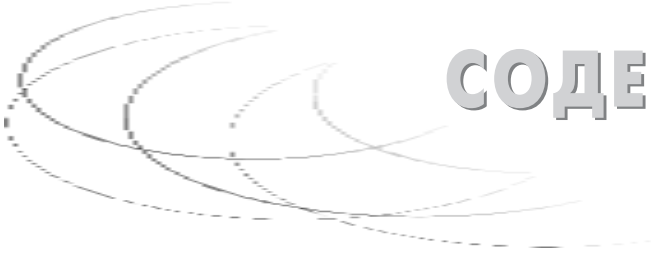

# СОДЕРЖАНИЕ

## Глава 2
## Краткий обзор сети: все, что нужно знать о TCP/IP ..... 38

# Глава 4
# Краткий обзор Windows NT/2000: все, что нужно знать о Windows

# Глава 6
# Этап 2: сканирование ... 180

## Глава 7
## Этап 3: получение доступа с помощью атак на приложения и операционные системы ..... 242

## Глава 8
## Этап 3: получение доступа посредством сетевых атак ... 300

## Глава 9
## Этап 3: DoS-атаки ... 349



## Глава 10
## Этап 4: поддержание доступа: троянцы, черные ходы и RootKit ... 371

# Предисловие

Сложно представить себе мир без сети Internet. Сейчас через Internet мы можем узнать о состоянии своего счета в банке, посмотреть медицинскую карту, выяснить маршрут, купить что-нибудь и даже поговорить с друзьями. Многим компаниям не удалось бы выжить без Всемирной паутины – ведь только с ее помощью они общаются со своими клиентами.

Однако посредством Internet не только компании связываются с клиентами, врачи просматривают медицинские карты, а друзья общаются. Через Глобальную сеть вы получаете доступ к нужным ресурсам, а злоумышленники – к вашей системе.

Операционные системы разрабатывались в такое время, когда даже мысли не возникало об их взломе: они использовались честными исследователями для обмена информацией либо устанавливались на персональных компьютерах, где пользователи работали с текстом или запускали игры. Развитие Internet – а также мысли об атаке систем с политической целью или ради интереса – происходило настолько стремительно, что операционные и сетевые системы не успевали за ним и не смогли стать действительно надежными – такими, какими они должны быть. И теперь трудно не оказаться очередной жертвой атак.

Гораздо проще сдаться, признать всю безвыходность ситуации, переехать в Вермонт и разводить там кроликов. Но в то время как выращивание тысяч кроликов кажется самым легким и простым выходом из сложившейся ситуации, на помощь приходит Эд Скудис (Ed Skoudis) со своей безграничной энергией, энтузиазмом и оптимизмом. Книга «Противостояние хакерам» соответствует характеру ее автора. Он заставляет нас поверить в то, что мы можем выиграть битву со злоумышленниками. Мы *должны* выиграть, и Эд Скудис нам поможет.

*Радиа Перлмен (Radia Perlman),*
*главный инженер компании Sun Microsystems, Inc.*

# Вступление

Зазвонил мой сотовый телефон. С трудом открыв глаза, я посмотрел на часы. Тьфу! 1 января, 4 часа утра. Излишне говорить, что этой ночью я спал совсем немного.

Я снял трубку и услышал голос Фреда, моего приятеля. Фред – администратор по безопасности в одной небольшой компании-провайдере Internet. Он часто звонит мне и задает разные вопросы по безопасности.

«Нашу систему взломали!» – прокричал Фред слишком громко для такого времени суток. Я протер глаза, пытаясь собраться с мыслями. «С чего ты взял, что они проникли в систему? Что они сделали?» – спросил я. Фред ответил: «Они испортили множество Web-страниц. Это ужасно, Эд. Мой босс убьет меня, когда узнает». Я осведомился: «Как они проникли в систему? Ты смотрел системные журналы?»

Запинаясь, Фред пояснил: «Н-ну, мы записываем не так много информации, так как при этом падает скорость работы. На некоторых компьютерах я вообще отменил запись системного журнала. А там, где мы записываем, взломщики стерли все сохраненные данные».

«А вы применяли последние патчи безопасности, о которых сообщил продавец операционных систем?» – задал я следующий вопрос, пытаясь узнать подробнее о состоянии системы безопасности в компании Фреда.

Колеблясь, Фред ответил: «Мы применяем патчи каждые три месяца. Последний раз это было... м-м-м... два с половиной месяца назад».

Голова гудела, почесав ее, я сказал: «На прошлой неделе были обнаружены две крупные атаки, связанные с переполнением буферов. Удар мог быть нанесен и по вашей компании. Они (злоумышленники) устанавливали какие-нибудь RootKit? Ты проверял уязвимые файлы своей системы, не противоречат ли они друг другу?»

«Знаешь, я хотел установить программу, подобную Tripwire, но руки до этого так и не дошли», – признал Фред.

Я тихо вздохнул и сказал: «Ладно. Не волнуйся. Я сейчас приеду, и мы разберемся, в чем дело».

Конечно, вы не желаете попасть в положение Фреда, а я предпочел бы, чтобы 1 января в 4 часа утра как можно меньше людей звонило мне по телефону. Хотя, рассказывая эту историю, я изменил имя моего приятеля, такая ситуация действительно имела место. Компания, в которой работал Фред, не смогла обеспечить минимальный уровень безопасности, и, когда злоумышленник атаковал систему, фирме пришлось за это поплатиться. По своему опыту я знаю: многие организации обнаруживали, что не готовы обеспечить надлежащую защиту информации.

Но положение дел на данный момент выходит за пределы основных постулатов безопасности. Даже если вы применяли все то, о чем я говорил с Фредом, существует множество других способов защиты, которые вы используете для своих систем. Конечно, можно задействовать патчи безопасности, включить инструмент проверки файлов и правильно вести системный журнал, но скажите, когда последний раз вы проверяли незащищенные модемы? А как насчет активизации безопасности на уровне портов в коммутаторах (switches) на уязвимых участках сети, позволяющей предотвратить новые мощные атаки снифферов? Думали ли вы о неисполняемых стеках, отражающих наиболее распространенный на сегодняшний день вид атак – переполнение стековых буферов? Готовы ли вы к RootKit? Если вы хотите подробнее узнать об этом и о многом другом, моя книга для вас.

Читая ее, вы поймете, что компьютерные атаки происходят каждый день и становятся все более и более серьезными. Для создания хорошей системы безопасности необходимо знать, какими методами пользуется ваш противник при взломе. Когда я работал архитектором систем защиты информации, испытывая их на проникновение извне, я видел множество атак, начиная от простого непрофессионального сканирования и заканчивая мощными атаками, которые финансировались криминальными группировками. В этой книге подробно рассказывается о наиболее часто встречающихся стратегиях реальных атак, а также даются советы, как избежать возможных нападений. Вы узнаете, как злоумышленники атакуют, рассмотрите каждую стадию данного процесса, чтобы затем применить всестороннюю защиту.

Книга написана для системных и сетевых администраторов, профессионалов в области безопасности, а также для всех, кто хочет узнать о компьютерных атаках и способах их предотвращения. Стратегии атак и методы защиты, о которых здесь рассказывается, используются многими предприятиями и организациями, имеющими компьютерные сети.

Удивительно, насколько охотно компьютерные взломщики делятся друг с другом информацией о том, как атаковать конкретную систему. Скорость, с которой распространяется информация о жертвах, поразительна, жалости не ждите! Я надеюсь, что эта книга действительно поможет вам, так как в ней даются практические советы по защите компьютерной системы от проникновения извне. Применив

способы защиты, изложенные ниже, вы значительно повысите уровень безопасности ваших данных, и, возможно, на следующий Новый год мы будем спать спокойно.

## Благодарности

Мои друзья предупреждали меня о том, сколько сил потребуется для написания книги. Как правило, я не обращал на их разговоры никакого внимания, думая, что сделать это будет так же просто, как и напечатать 500 страниц. Как я ошибался! Исправления, внесенные рецензентами, заставили меня пересмотреть написанное. Технически грамотные критики хотели видеть больше технических подробностей, в то время как менее знающие мечтали получить наглядное учебное пособие. Я благодарю рецензентов, которые помогли мне найти баланс между наглядностью материала и необходимостью пояснения технических деталей.

Идея о написании подобного руководства возникла у Радии Перлмен еще четыре года назад, и именно она побудила меня к его созданию. Радиа руководила моей работой на протяжении всего времени, пока я писал книгу, не только поддерживая меня, но и предоставляя ценные технические данные. Огромное спасибо, Радиа!

Мэри Френз (Mary Franz) из издательства Prentice Hall помогала мне в течение всего времени написания книги. Она была спокойной, невозмутимой и действительно поддерживала меня.

Я благодарен всем работникам издательства Prentice Hall за их содействие в создании книги, особенно Скотту Саклингу (Scott Suckling), который в процессе редактирования присматривал за моим детищем, а также предложил включить в текст весьма полезную информацию.

Спасибо Маркусу Личу (Marcus Leech), Пэту Кэйну (Pat Cain) и Ричарду Энкни (Richard Ankney), которые рецензировали написанное и помогли своими ценными замечаниями. Спасибо также Норин Реджине (Noreen Regina), оказавшей огромную помощь в организации процесса рецензирования.

Хотелось бы также поблагодарить Джина Шульца (Gene Schultz), моего друга, который написал главу 4 и дал много полезных советов по другим разделам книги. Отличный парень!

Майк Ресслер (Mike Ressler) тщательно просмотрел текст, делая весьма проницательные замечания. Его комментарии стали ценным вкладом в создание книги. Именно Майк открыл для меня мир информационной безопасности, за что я всегда буду ему благодарен.

Эниш Бимани (Anish Bhimani) изначально дал «зеленый свет» для моего проекта и помог уладить политические вопросы, мешавшие закончить работу. Спасибо ему за одобрение книги, а также за то, что помог мне одним из первых войти в мир информационной безопасности.

Рич Уитмен (Rich Whitman) был отличным руководителем, когда готовились основные разделы книги. Его умелое управление помогло мне справиться с делом,

на которое вообще-то нужно было тратить весь день, в то время как я работал только вечерами и по выходным.

Несколько лет назад Стив Брэниган (Steve Branigan), сидя в ресторане Перкинса (Perkins), познакомил меня с удивительным миром противостояния компьютерным атакам. Именно от Стива я узнал многое о защите и понял, что описывать ее можно захватывающе интересно, как она этого заслуживает.

Алан Паллер (Alan Paller) и Стефен Норткатт (Stephen Northcutt) из института SANS провели потрясающую работу, заставив меня создать соответствующие современным технологиям материалы для презентации. Я всегда ценил то, насколько непринужденно, но профессионально и информативно они помогли мне провести презентацию.

Джефф Посланс (Jeff Posluns) дал отличный совет, как организовать обсуждение книги, и помог ускорить написание главы об искусных методах атак. Билл Стиарнс (Bill Stearns) внес огромный вклад в создание раздела по применению инструмента Netcat, и вообще он отличный парень. Просто дух захватывает!

Огромное спасибо создателям всех инструментов, о которых идет речь в этой книге. В то время как некоторые программисты создавали их с умыслом, большинство все-таки хотело помочь людям найти уязвимые места в системе безопасности, прежде чем до них доберутся взломщики. Хотя вы можете не согласиться с такой оценкой их мотивов, нельзя не заметить, сколько знаний было вложено в разработку подобных инструментов и насколько тщательно продумывались стратегии атак, поэтому не стоит недооценивать такой труд.

Студенты, посещавшие мой курс на протяжении последних четырех с половиной лет, помогли сделать книгу более понятной, а также предоставили полезную информацию. Часто небольшое замечание с их стороны приводило к значительному изменению материала, а это в свою очередь способствовало тому, что примеры становились более жизненными, и соответственно увеличивало ценность книги. Спасибо всем, кто в течение нескольких лет помогал мне!

Особая благодарность моей замечательной жене Жозефине (Josephine) и нашей дочери Джессике (Jessica) за их помощь и понимание. Когда днем и ночью я писал эту книгу, они оказывали мне великолепную поддержку, предоставляя гораздо больше свободы, чем я того заслуживаю. Это было нелегко, но весело... И теперь книга перед вами!

*Эд Скудис*

# ГЛАВА 1

# Введение

Компьютерные атаки происходят каждый день. Просто подключите компьютер к Internet, и три, пять или десять раз в день кто-то будет пытаться проникнуть в вашу систему. Даже если ни реклама, ни ссылки не привлекают внимания к компьютеру, его все равно будут постоянно сканировать. Если компьютер используется для бизнеса, например для поддержки коммерческого, некоммерческого, образовательного сайта или сайта вооруженных сил, ему будет уделяться еще больше внимания со стороны злоумышленников.

Многие атаки представляют собой простое сканирование компьютера, их цель – найти уязвимые места в системе безопасности. Но существуют действительно сложные сценарии атак, которые реализуются все чаще и чаще, о чем нам сообщают заголовки газет. В течение одного года многие крупные банки США стали жертвами хакеров, которые получили возможность просматривать информацию о состоянии счетов клиентов. Взломщики украли большое количество номеров кредитных карточек с сайтов Internet-магазинов. С компаний, занимающихся электронной торговлей, злоумышленники часто требовали денег в обмен на обещание не разглашать информацию о кредитных карточках клиентов. Многочисленные фирмы, реализующие продукцию в режиме реального времени, информационные компании и сайты Internet-магазинов были вынуждены временно приостанавливать свою работу, а их покупатели обращались в другие фирмы. В результате организации, подвергшиеся атаке, теряли миллиарды долларов. Американская компания, один из лидеров в области разработки программного обеспечения, обнаружила, что взломщики обошли их систему защиты и украли исходный программный код будущих версий популярных программ. Подобные истории случаются все чаще и чаще.

Цель этой книги заключается в том, чтобы наглядно показать, сколько атак происходит сегодня, и помочь защитить компьютер от кибервзломщиков. Изучая стратегии атак, можно наилучшим образом продумать защиту своей системы, чтобы дать достойный отпор атакующим.

# Мир компьютеров и золотой век хакеров

Только за последние несколько десятилетий компьютерные технологии стали существенной частью жизни общества. Мы получили возможность контролировать многие сферы человеческой деятельности, создав при помощи электронных машин виртуальный мир, неотделимый от реального. Современные компьютерные системы хранят точные данные о болезнях каждого человека, осуществляют навигацию по всему миру, контролируют практически все финансовые операции, планируют распределение продовольственных товаров и даже пересылают любовные письма. Когда я был ребенком, считалось, что компьютеры предназначены для зануд, и многие люди избегали этих машин. Десять лет назад сеть Internet использовалась в основном учеными, а сейчас, когда компьютерные технологии стали частью повседневной жизни, будь это работа за компьютером или разговор по сотовому телефону, они постепенно занимают одну из главенствующих позиций в экономике, и о них все чаще пишут в газетах.

Вы наверняка заметили, что компьютерные и сетевые технологии имеют множество уязвимых мест. Конечно, пользовательский интерфейс не всегда бывает интуитивно понятен, да и сами компьютеры частенько ломаются, но это только верхушка айсберга. Есть и незаметные на первый взгляд, однако немаловажные проблемы, такие как недостатки дизайна операционных систем, приложений и протоколов. Используя слабые места, злоумышленник может украсть ценную информацию, захватить управление системой или навредить еще каким-либо способом.

Конечно, мы создали мир, который, по существу, подвержен хакерским атакам. Поскольку мы практически полностью полагаемся на компьютеры, а большинство систем несовершенны, можно констатировать факт, что мы, к сожалению, живем в золотой век хакеров[1]. Каждый день они находят все больше и больше уязвимых мест, о чем быстро становится известно в компьютерном андеграунде. Имея в своих домах лаборатории, атакующие и исследователи систем безопасности могут создавать модели компьютерных платформ, которые используются крупными корпорациями, правительственными и военными организациями. При этом применяются те же операционные системы, маршрутизаторы и другие устройства. Тщательно изучая системы в поисках слабых мест, злоумышленники оттачивают свое мастерство, а также находят новые пути проникновения в чужую систему.

---

[1] Изначально хакерами называли высококлассных компьютерных специалистов, а взломщиков именовали кракерами (cracker). Путаницей в терминологии мы обязаны масс-медиа, которые присвоили звание хакеров обычным преступникам. Подробнее об этом написано ниже. – *Прим. ред.*

Компьютерные технологии входят во все сферы жизнедеятельности человека. Сегодня некоторые компании продают электрические одеяла с подключением к Сети, так что можно нагреть кровать из другой комнаты или даже другого уголка планеты. Энди Гроув (Andy Grove), председатель компании Intel, часто говорит о том, что скоро у холодильника будет выход в Internet, чтобы он мог заказать молоко в магазине, если оно заканчивается. Скотт Макнили (Scott McNealy), CEO фирмы Sun Microsystems, предрекает появление электрических лампочек с подключением к Сети: это позволит послать сигнал в компанию по производству лампочек в том случае, если лампочка вскоре перегорит, и новую лампочку доставят туда, откуда был сделан вызов. Вскоре в любом автомобиле появится подключение к Internet по радиосвязи; водитель сможет посмотреть маршрут следования, обратиться за помощью по устранению возникших неполадок и даже отправить и получить электронную почту во время пути. Что же лежит в основе этих быстро развивающихся технологий будущего? Компьютеры и связывающие их сети.

Со всеми описанными нововведениями золотой век хакеров может стать веком их абсолютной власти. Подумайте: сегодня злоумышленник пытается взломать вашу систему, сканируя ее через Internet. В ближайшем будущем кто-то может попытаться «влезть» в систему вашего автомобиля, подключенного к Сети, в то время как вы едете по улице. Вы слышали об ограблении машин? Приготовьтесь к эпохе автомобильного хакерства.

# Для чего нужна эта книга

> Если вы знаете себя и знаете врага, не нужно беспокоиться об исходе сотен битв. Если вы знаете себя, но не знаете врага, после победы ждите поражения. Если вы не знаете ни себя, ни врага, вы будете повержены.
>
> *Сан Цу «Искусство войны». Перевод и комментарий Лайнала Гайлса (отрывок из книги «Проект Гутенберг»)*

«Черт возьми! – может подумать кто-нибудь из читателей. – Зачем писать книгу о хакерах? Это лишь побуждает их к нападению!» Я уважаю ваше мнение, но, к сожалению, в такой логической цепочке имеется слабое звено: у злоумышленников есть все сведения, необходимые для атаки и разрушения системы. Если же у них нет такой информации, они легко получат ее на многих Web-сайтах, посвященных хакерам (о чем говорится в конце книги). Опытные взломщики зачастую делятся опытом с непосвященными. На самом деле каналы связи между представителями компьютерного андеграунда работают гораздо лучше, нежели между профессионалами-программистами. Эта книга – один из способов исправить ситуацию.

Я не стремлюсь организовать армию хакеров, безжалостно взламывающих системы и постепенно занимающих господствующее положение в мире; напротив, я хочу рассказать, как защищаться от них. Для создания эффективной защиты необходимо знать о тех инструментах, которыми пользуются наши противники. Изучая, каким образом действуют эти инструменты, мы не только осознаем потребность в безопасности, но и лучше представляем, как применять соответствующие способы защиты.

Настоящая книга написана для системных и сетевых администраторов, а также других людей, работа которых заключается в обеспечении надлежащей защиты информации. Те, кто хочет узнать о методах работы взломщиков и способах защиты систем, тоже извлекут некоторую пользу из этой книги. Здесь даются практические советы для администраторов, которые хотят обезопасить свою систему от взлома. Зная о методах защиты, мы можем создать такой мир, в котором эффективная защита будет скорее правилом, нежели исключением. Как сказал Сан Цу, мы должны знать не только собственные возможности, но и возможности наших врагов, поэтому рассказ о стратегиях компьютерного нападения сопровождается описанием реальных методов защиты. Вы можете сравнить вашу защиту информации с теми принципами, которые описаны далее, чтобы оценить, насколько действенна данная система безопасности. Там, где есть уязвимые места в системе, процедуре или самой политике ведения дел, можно применить соответствующую защиту от злоумышленников. В этой книге рассказывается только о том, что делают атакующие и как от них защититься.

## Зачем рассказывать о специальных инструментах и стратегиях атак

На сегодняшний день можно свободно получить тысячи различных инструментов компьютерных и сетевых атак и узнать о десятках тысяч стратегий взломщиков. Для охвата всего множества вероятных атак в этой книге внимание акцентируется на определенных группах хакерских инструментов и стратегий, рассказывается о наиболее опасных и широко распространенных инструментах из каждой группы. Если досконально знать, как защититься от самых опасных инструментов и стратегий атак каждой категории, нетрудно обезопасить себя от всех инструментов из этой же группы. Например, существуют тысячи инструментов, которые позволяют хакеру захватить и проанализировать сетевой трафик, – такой процесс называется *сниффингом* (sniffing). Вместо того чтобы разбирать каждый известный на сегодняшний день инструмент сниффинга, мы более подробно рассмотрим самый мощный и широко использующийся инструмент – Dug Song's Dsniff. Обезопасив себя от Dug Song's Dsniff, вы проведете огромную работу по защите своей системы от всех видов снифферских атак. Аналогично, узнавая о самых мощных инструментах из других категорий, можно создать и применить самую эффективную защиту против всех атак из этих групп.

### Чем эта книга отличается от других

В последние годы появилось несколько книг об атаках и их стратегиях. Некоторые из них хорошо написаны и весьма полезны для понимания того, как осуществляются атаки и как от них защититься. Зачем добавлять еще одну книгу к уже изданным? Дело в том, что между этой книгой и всеми остальными есть различия:

- перед вами не словарь, а, скорее, энциклопедия. В других книгах о хакерах рассказывается о тысячах инструментов, при этом каждому из них отводится абзац или в лучшем случае страница. Здесь каждая категория инструментов рассматривается более подробно. Тщательно изучая каждую группу инструментов атак, можно лучше понять, как действуют соответствующие средства защиты;
- поэтапное рассмотрение атаки. В других книгах говорится о том, как злоумышленники получают доступ к системе, акцентируя внимание именно на проникновении в нее. Это, несомненно, важный элемент большинства атак, но наши противники не только взламывают систему: многие атакующие стараются сохранить доступ к ней, а также скрыть следы своего пребывания. Здесь же рассказывается об атаке с начала и до конца, чтобы для каждого этапа нападения можно было поставить соответствующую защиту. Большинство атак состоит из следующих этапов: исследование системы, сканирование, получение доступа, сохранение доступа и сокрытие следов. В данной книге вы найдете подробную информацию о каждом этапе;
- анализ совместного использования инструментов. Инструменты атакующих похожи на кирпичики, каждый из которых служит определенной, но ограниченной цели. Только зная, как из этих кирпичиков строится атака, можно понять, как лучше защитить себя. Опытные хакеры берут определенные инструменты и комбинируют их таким образом, что получается весьма изящная атака. Ниже рассказывается, что на каждой стадии атаки часто задействуется сразу несколько программ. В главе 12 описано несколько сценариев совместного применения инструментов;
- проведение параллелей с реальным миром для лучшего понимания концепций, на которых основаны компьютерные технологии. В этой книге я привожу аналогии, чтобы лучше объяснить, как работают те или иные технологии. Хотя некоторые аналогии слишком просты, я надеюсь, что с ними книга стала более интересной и понятной читателю.

## Не следует недооценивать противника

Итак, кто такие атакующие, от которых мы должны защищаться? Часто, говоря о компьютерных атаках, люди представляют себе прыщавого подростка, который сидит перед компьютером в своей комнате и попивает «Маунтин Дью». Этот образ

успокаивает некоторых пользователей, и они снижают уровень безопасности, думая: «Какой вред может причинить ребенок?» Такой подход неправилен, по крайней мере, по трем причинам.

Во-первых, у многих юных взломщиков удивительно чистая кожа, без единого прыщика. Во-вторых, что более важно, многие подростки поразительно быстро и легко проникают в чужую систему, у них превосходные навыки и огромная доля решимости. Конечно, у большинства подростков знаний немного. Однако, если ваша организация попадет под удар молодого, но опытного хакера, компьютерной системе может быть причинен значительный ущерб. Не ослабляйте систему защиты только потому, что, на ваш взгляд, атакующий всего лишь подросток.

Третья причина, вероятно, самая важная. Как правило, организациям грозит бульшая опасность, нежели проделки озорных мальчишек. Никогда не следует недооценивать противника. На самом деле атаковать систему способны откуда угодно и причины нападения могут быть самыми разнообразными. Назовем лишь несколько:

- *конкуренция*. Зачастую конкуренция вашей фирмы с другими компаниями может привести к компьютерной атаке со стороны соперников, которые хотят одержать победу в борьбе за потребителя. Во время таких атак злоумышленник в одном случае просто собирает интересующую его информацию о ваших планах на будущее, в другом – проникает в систему, чтобы подробнее узнать о ваших стратегиях, а в третьем – может даже провести DoS-атаку[1], чтобы помешать покупателям связаться с вами;
- *взломщики-активисты* (hacktivist). Если ваша организация участвует в политической жизни страны, то вы можете стать жертвой взломщиков-активистов. Эта группа атакующих пытается взломать систему, чтобы добавить в вашу политическую программу пункты, направленные на ее дискредитацию. Активисты стремятся изменить ваш Web-сайт, оставить на нем сообщения, дезинформирующие сотрудников и членов вашей организации, или сделать невозможной обработку информации, таким образом тормозя вашу деятельность;
- *организованная преступность*. Если ваша фирма работает с деньгами (а на определенном этапе работать с деньгами приходится), ваша компьютерная система способна стать мишенью для преступников. Злоумышленники могут искать удобный способ отмывания денег, полезную в их бизнесе информацию или доступ к системе для других незаконных целей;
- *террористы*. Если ваша организация считается важной частью инфраструктуры страны или мира, вам грозят атаки террористов. Они в силах внедрить по всему предприятию специальные программы, которые в чрезвычайной ситуации закроют важные системы или вызовут проблемы, угрожающие жизни и здоровью людей;

[1] DoS (Denial of Service) – атака типа «отказ в обслуживании».

- *государство*. Многие государства интересуются деятельностью различных предприятий, функционирующих на их территории. Некоторые прибегают к помощи компьютерных атак, чтобы узнать о деятельности отечественных компаний и оказать юридическое давление на них, получить сведения, которые помогут компаниям-резидентам конкурировать с иностранными организациями, или даже подавить фирмы, не согласные с государственной политикой;
- *наемники*. Наемники пытаются заработать деньги, воруя информацию или получая доступ к компьютерным системам от лица клиента. Такой тип атак также можно включить в список внешних угроз.

Кроме внешних атак существуют и внутренние нападения, которые совершаются людьми, по долгу службы имеющими непосредственный доступ к компьютерной системе. К внутренним угрозам относятся:

- *недовольные работники*. Сотрудники обучаются на предприятии, получают доступ к компьютерной системе и могут вносить в нее изменения. Собственные работники организации – наиболее часто встречающиеся и опасные атакующие;
- *покупатели*. К сожалению, покупатели иногда атакуют компьютерные системы поставщиков, пытаясь получить информацию о других покупателях, снизить цены или другим образом изменить данные организации;
- *поставщики*. Поставщики тоже атакуют компьютерные системы покупателей. Работник в сети поставщика может разнообразными способами атаковать вашу систему;
- *продавцы*. Продавцам часто предоставляется неограниченный доступ к компьютерной системе для ее диагностики, усовершенствования и администрирования. Таким образом, они в состоянии атаковать только ту систему, к которой у них есть доступ, но потенциально могут проникнуть и во всю сеть;
- *деловые партнеры*. Возникновение предприятий со смешанным капиталом, ведение совместных проектов и другие деловые связи предполагают создание сети между участниками этих взаимоотношений, чтобы они могли обмениваться важной информацией. Посредством сети взломщик способен атаковать делового партнера. Организация системы защиты соответствует поговорке про цепь, у которой есть слабое звено. Если внешний атакующий пробьет слабую защиту вашего партнера, он получит доступ и к вашей системе, поскольку они соединены;
- *подрядчики*, *временные сотрудники* и *консультанты*. Проработав консультантом почти десять лет, я могу с уверенностью сказать, что такие сотрудники – самые опасные. Многие организации не проводят тщательной проверки временных работников, которую они осуществляют для постоянного штата. Часто временные работники имеют почти неограниченный доступ к компьютерной системе и информации. Осознав проблему, организация не в состоянии

закрыть доступ для временных сотрудников так же быстро, как для уволенного персонала. Я наблюдал ситуации, когда учетные записи закрывались на следующее утро после увольнения работника, в то время как учетная запись временного сотрудника могла существовать еще месяцы.

Конечно, опасности, перечисленные выше, не исключают друг друга. Например, террористическая группировка способна внедрить своих людей в вашу организацию под видом временных работников, чтобы получить доступ к компьютерной системе и установить в ней нужное программное обеспечение. Аналогично конкурент может нанять высококвалифицированного молодого взломщика, чтобы украсть необходимую информацию из вашей системы. Таких ситуаций бесконечное множество.

Однако так же, как не нужно недооценивать грозящие вам опасности, не следует их и переоценивать. Вы же не хотите озолотить службу безопасности, пытаясь защититься от взломщиков, которые никогда не заинтересуются вашей компьютерной системой и информацией. Никто не устанавливает дорогостоящую сигнализацию на автомобиль-универсал Chevy 1985 года выпуска. Однако в определенных местах вы, конечно же, запираете такую машину, чтобы люди не устраивали себе увеселительных поездок за ваш счет. Вы должны продумать, что может угрожать вашей организации, подсчитать материальную и нематериальную ценность активов, которые хотите защитить, а затем применить такие средства защиты, стоимость которых сопоставима с потенциальными опасностями и ценностью системы и информации.

## Навыки атакующего: от «сценаристов» до элиты

Некоторые хакеры обладают лишь элементарными знаниями в области взлома систем: они не понимают, как работают их программы, и полагаются на инструменты атак, созданные другими. Таких атакующих часто иронически называют *«сценаристами»* (script kiddies), поскольку они в основном используют чужие сценарии атак и программное обеспечение, созданное более опытными хакерами. «Сценаристы» сканируют множество систем в Internet, часто не разбирая, что это за система, а просто пытаясь найти наиболее легкую для взлома. Проникая в подобную систему, «сценаристы» начинают хвалиться своими достижениями и продолжают атаковать. Так как большинство хостов в Internet плохо защищены, даже немного знающие атакующие способны взломать сотни и тысячи систем по всему миру. На сегодняшний день в Internet работает множество «сценаристов», и число их растет с каждым днем.

Вслед за простыми «сценаристами» можно выделить атакующих, знания которых находятся на среднем уровне; они взламывают только определенные операционные системы. С некоторой степенью вероятности можно сказать, что такой тип взломщиков в силах нанести значительный ущерб атакуемой компании. Более того, хакеры со средним или высоким уровнем знаний, а также исследователи

систем безопасности работают в следующем направлении компьютерного андеграунда: они обнаруживают уязвимые места систем и создают легкие в использовании инструменты, которые и выявляют эти слабые места. Иногда они выставляют свои творения на всеобщее обозрение, например на Web-сайте. Некоторые разработки сложны, но удобны. На самом деле во многих программах применяется графический интерфейс или простая командная строка. «Сценаристы» берут такие инструменты, написанные более опытными людьми, и задействуют их при атаках, не понимая, какие именно уязвимые места они обнаруживают.

На самой вершине мастерства находятся взломщики, которых можно назвать *элитой*. Они стремятся досконально изучить многие компьютерные платформы. В отличие от «сценаристов» атакующие из элиты редко хотят получить известность. Когда они взламывают систему, то стараются остаться незамеченными, тщательно скрывают следы своего пребывания и собирают важную информацию для дальнейшего использования. Элита также занимается детальным исследованием, в процессе которого в приложениях, операционных системах и других программах находят «дыры», помогающие проникнуть в систему. На основе проведенного исследования хакеры разрабатывают специальные инструменты для взлома. Большинство атакующих из элиты хранят созданные инструменты и сведения о найденных уязвимых местах при себе, а не делятся ими с широкой общественностью. Держа инструменты и стратегии атак в тайне, эти атакующие стараются предотвратить разработку и использование эффективных способов защиты против подобных нападений.

У другой группы людей, знающих очень многое об атаках, противоположное мнение. У них более благородные мотивы, они стараются найти уязвимые места в системе прежде, чем это сделают недоброжелатели, чтобы получить эффективные методы защиты. Такие честные люди порой становятся профессионалами в области компьютерной безопасности, могут работать в качестве консультантов на предприятиях или предлагают организациям усовершенствовать их систему защиты информации.

# Кратко о терминологии и иконографии

По традиции договоримся о терминологии, применяемой в книге, и основных элементах рисунков.

## Хакеры, взломщики и злоумышленники

Эскимосы используют множество слов для обозначения обычного снега, однако они не путаются в терминологии, как мы, когда хотим назвать людей, взламывающих компьютерные системы. В средствах массовой информации (и соответственно в обществе) людей, атакующих компьютерные системы, называют хакерами. Однако многие представители компьютерного андеграунда говорят, что,

если обратиться к истории, слово «хакер» (hacker) относится к человеку, который увеличивал функциональные возможности компьютеров. Следовательно, хакеры – это «хорошие» люди, действующие с благородной целью: они обучают компьютер выполнению новых функций. Применение слова «хакер» по отношению к компьютерным вандалам или ворам искажает не только смысл самого термина, но и историческую концепцию хакерства.

Для тех, кто использует термин «хакер» с положительной точки зрения, люди, атакующие компьютерные системы, – просто взломщики. Итак, на профессиональном жаргоне хакеры «хорошие», а взломщики «плохие». Однако, поскольку средства массовой информации называют и тех, и других хакерами, термин «взломщик» встречается крайне редко.

Иногда можно увидеть сочетания типа *black hat* или *white hat* по отношению к разного рода атакующим. Как в фильмах о ковбоях, где «плохие ребята» носили черные шляпы, а «хорошие ребята» – белые, термин «black hat» (черная шляпа) служит для обозначения атакующего-злоумышленника, а «white hat» (белая шляпа) – эксперта в области компьютерной безопасности, который старается защитить системы от взлома. Black hat пытается проникнуть в систему, а white hat находит уязвимые места и исправляет недостатки. Очевидно, что людей, которые работают на два фронта (иногда атакуют системы, а иногда защищают их), именуют *gray hats* – серые шляпы.

Неразбериха в терминологии вынудила меня назвать всех, кто атакует компьютеры, *атакующими* (attacker). Атакующий может быть хакером, взломщиком, white hat, black hat, gray hat, исследователем системы безопасности, испытателем системы на проникновение извне и даже принадлежать к элите компьютерного андеграунда: независимо от уровня их знаний, мотивов и привычных для вас имен, все они атакуют компьютеры.

## Рисунки и сценарии

В то время как термин «атакующий» относится ко всем лицам, пытающимся взломать систему, необходимо и на рисунках показывать, какая машина относится к атакующему. Для того чтобы ее легко было узнать, я позаимствовал образ черной шляпы. В этой книге на всех рисунках компьютер атакующего изображен в черной шляпе (рис. 1.1).

Кроме того, в книге описаны многообразные сценарии, которые лучше иллюстрируют различные методы атак. В большинстве сценариев будет использоваться один и тот же набор персонажей: Элис, Боб и Ева. Элис и Боб – безобидные компьютеры, которые выполняют свою работу. Ева – атакующий, который пытается взломать систему Элис и Боба, украсть информацию, изменить данные или другим

***Рис. 1.1.*** *Машина атакующего в черной шляпе*

образом нарушить их спокойное существование. Пожалуйста, обратите внимание, что имена Элис, Боб и Ева часто применяются в криптографии и среди людей, работающих с системами безопасности, причем никакого разделения по половому признаку не подразумевается. Конечно, есть определенный теологический смысл в том, что атакующий именуется Евой. Однако для наших целей Ева не имеет пола. Неважно, как обращаться к системе: он, она или оно. В криптографии атакующему было дано имя Ева, поскольку оно созвучно со словом «подслушивающий»[1].

### Имена разработчиков

В книге приводятся имена людей, создавших инструменты, о которых будет идти речь. Кто-то может посчитать, что предавать гласности эти имена не стоит. Я не согласен. Некоторые инструменты способны служить как благой, так и дурной цели. Например, качественно разработанный инструмент перехвата трафика (сниффер) применяется и для усовершенствования сети, и для кражи паролей других пользователей. Аналогично сканер уязвимых мест помогает найти слабые места в системе, чтобы ее владелец устранил их, либо чтобы атакующий обнаружил «дыры» в системе, а затем атаковал ее. Другие инструменты, служащие исключительно неблаговидной цели, показывают важность определенных методов защиты, и потому тоже имеют ценность.

Хотя мы вправе не одобрять некоторые мотивы создателей подобных программ, следует уважать знания, время и усилия, потраченные на их разработку. Отдавая должное людям, придумавшим описанные здесь инструменты атак и соответствующие методы защиты, я привожу имена авторов инструментов и адреса в Internet, откуда можно загрузить сами инструменты.

## Инструменты атак могут быть направлены и против вас

Да, в этой книге даются Web-адреса, откуда можно загрузить каждый описанный инструмент. Но необходимо понимать, что вы применяете подобные инструменты на свой страх и риск! Хотя некоторые программы, о которых пойдет речь ниже, разработаны продавцами программного обеспечения, консультантами в сфере безопасности и иными приверженцами защищенных сетей, другие рассмотренные инструменты создавались людьми, у которых были более корыстные мотивы. Как с любым программным обеспечением, при загрузке и запуске таких программ в своей системе нужно быть осторожным.

---

[1] Подслушивающий – eavesdropper, а Ева – Eve. – *Прим. перев.*

Многие инструменты, которые будут здесь рассмотрены, могут навредить вашей системе. Атакующий без труда напишет программу, которая заключает в себе не только общеизвестные функции: в ней может быть заложена возможность использования той системы, в которой программа будет запущена. Вы полагаете, что инструмент, который вы загрузили, просто просканирует сеть на наличие уязвимых мест. К сожалению, он способен также отослать атакующему копию отчета о найденных слабых местах или запустить вирус на вашем компьютере.

Что же делать? Может, вообще не стоит запускать инструменты, о которых пойдет речь в этой книге? Конечно, вы должны решать сами, но я рекомендую поэкспериментировать с ними в регулируемой среде, чтобы понять, как происходят атаки, и защитить себя.

## Создание лаборатории для исследования

Советую экспериментировать с инструментами атакующих в регулируемой среде, на тех системах, которые полностью изолированы от основной сети. Программы, которые будут описаны ниже, не требуют слишком много ресурсов, достаточно использовать компьютер Pentium 90 МГц с 64 Мб оперативной памяти и жестким диском емкостью 3 Гб. Установите две или три машины на изолированном участке локальной сети с последними версиями операционных систем. Убедитесь, что на жестких дисках не хранится какой-либо важной информации. Соедините системы между собой с помощью недорогого концентратора или коммутатора, который можно купить в компьютерном магазине.

Для максимальной гибкости такой лаборатории я рекомендую создать системы с многовариантной загрузкой, например Linux, Windows NT, OpenBSD или Solaris x86. Большинство инструментов атакующих работают под Linux и Windows NT: эти платформы – самые распространенные в компьютерном андеграунде. Не забудьте включить их в свою систему. На рис. 1.2 показана одна из возможных конфигураций сети, та, которую я использовал для собственной лаборатории.

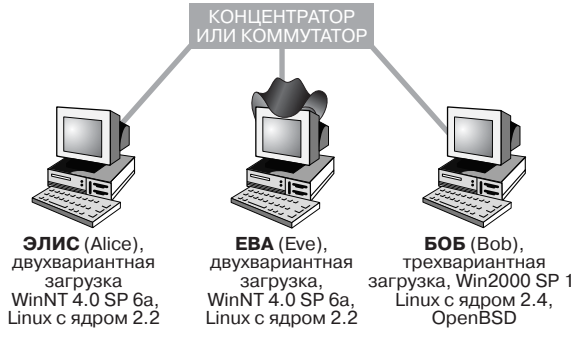


*Рис. 1.2. Экспериментальная лаборатория для анализа инструментов атакующих*

### Дополнительная информация

Хотя многие Web-сайты программного обеспечения, которые упоминаются в книге, управляются фирмами-консультантами или профессионалами в области компьютеров, некоторые Web-сайты, на которые я ссылаюсь, были созданы весьма сомнительными личностями. Когда вы будете заходить на такие сайты, адрес вашей компьютерной сети останется в их системных журналах, что может привести к атаке. Многие операторы подобных сайтов слишком заняты, чтобы атаковать вашу систему только потому, что вы посетили их Web-страницу, однако я советую быть осторожными. Когда бы вы ни искали инструменты и методы атак в Internet, я настоятельно рекомендую задействовать компьютер, на котором не содержатся сколько-нибудь важные данные. Также постарайтесь воспользоваться услугами не того Internet-провайдера, с которым работает ваша организация. Легкомысленно оставлять сетевой адрес организации или другую информацию в системных журналах Web-сайтов, где вы ищете инструменты атакующих.

При загрузке инструментов вам может понадобиться просмотреть исходный программный код. Иногда в этом коде имеются полезные комментарии. Хотя для того, чтобы увидеть этот код, придется приложить усилия, из него можно извлечь весьма ценную информацию, в частности о дополнительных функциях программы, о которых создатель инструмента не стал упоминать, поскольку они могут нанести вред системе.

Пожалуйста, обратите внимание, что географическое положение ограничивает применение определенных инструментов. В некоторых странах использование опасных программ в общей сети запрещено, даже если они установлены в собственной системе. Поэтому сначала проконсультируйтесь у юриста и убедитесь, что у вас есть полномочия и/или разрешение запускать подобные инструменты в компьютерной системе собственной организации. Я не хочу подвергать вашу работу опасности, советуя поэкспериментировать с этими инструментами! И напоследок я хотел бы сказать, что не несу никакой ответственности, если вы нарочно или случайно навредите своей или чужой системе при помощи указанных программ. Данный вопрос будет решаться между вами, владельцем атакованной системы и уполномоченными лицами местных органов власти.

## Структура книги

Оставшаяся часть книги разбита на три основных раздела: обзор технологий, подробное описание атак и советы на будущее. В последнем разделе также резюмируется изложенная информация и приводятся ссылки на Web-сайты. Рассмотрим каждый раздел подробнее.

### Современные технологии

Для того чтобы понять, как противники атакуют системы, необходимо хорошо представлять себе базовые технологии, на которых построена бульшая часть систем

и которыми атакующие пользуются для проникновения. В трех первых главах книги дается обзор нескольких ключевых технологий:

- глава 2: работа в сети с TCP/IP;
- глава 3: UNIX;
- глава 4: Windows NT и Windows 2000.

На сегодняшний день эти три технологии получили широкое распространение среди компаний и являются основными компонентами Глобальной сети. Во многих организациях большое число компьютеров с системами UNIX и Windows NT/2000 используются как внутри предприятия, так и для доступа в Internet. Даже в тех фирмах, которые больше полагаются на Novell NetWare, мэйнфреймы, системы на основе VMS и другие, платформы соединены между собой с помощью протокола TCP/IP и/или для доступа к Глобальной сети применяются системы UNIX либо Windows NT/2000.

Атакующие пользуются теми же самыми технологиями для своих атак. Бульшая часть их программ работает на платформах UNIX или Windows NT/2000 – в зависимости от выбора атакующего. Хотя инструменты функционируют на этих платформах, многие из них нацелены на компьютерные системы любого типа. Например, атакующий может применять инструмент нападения на компьютере с системой UNIX, чтобы перехватить соединение между системой VAX и вашим мэйнфреймом. Или еще: атакующий способен начать DoS-атаку против сети Novell или карманного компьютера с выходом в Internet посредством Windows NT. Помните, что, хотя каждый инструмент, о котором будет рассказываться в данной книге, работает на определенной платформе, с его помощью легко атаковать любую систему. Аналогично одни и те же способы защиты против атак допустимо установить на различных компьютерных системах.

## Этапы атаки

После того как будут рассмотрены основные на сегодняшний день технологии, мы проведем анализ стандартных этапов большинства атак. Многие атаки состоят из пяти основных этапов: первоначальное исследование системы, сканирование, проникновение в систему, сохранение доступа и сокрытие следов пребывания. Прочитав несколько глав, вы узнаете о каждом этапе атаки, инструментах и стратегиях, применяемых на данном этапе, а также о проверенных способах защиты от каждого типа атаки:

- глава 5: этап 1, исследование;
- глава 6: этап 2, сканирование;
- глава 7: этап 3, получение доступа на уровне операционных систем и приложений;
- глава 8: этап 3, получение доступа на уровне сети;
- глава 9: этап 3, проникновение в систему и DoS-атаки;

- глава 10: этап 4, сохранение доступа;
- глава 11: этап 5, сокрытие следов пребывания.

Затем в главе 12 вы узнаете о том, как комбинируются разные инструменты и стратегии на примере нескольких сценариев, взятых из реальных атак.

### Советы на будущее, выводы и справочная информация

В конце книги вашему вниманию представлен прогноз, какими могут стать инструменты и стратегии атак, а также приводится справочная информация, которая поможет лучше понять новые атаки и способы защиты от них.

## Принятые обозначения

Чтобы упростить восприятие материала, в книге используются следующие обозначения:

- *курсивом* в тексте выделены базовые термины и определения.
- моноширинным шрифтом набраны все листинги (фрагменты программного кода), команды, вводимые из командной строки, а также названия файлов и каталогов.
- **полужирным начертанием** при описании работы программ отмечены названия элементов интерфейса (окон, пунктов меню, опций и кнопок).

## Резюме

Так как существенная часть нашей жизни связана с компьютерными технологиями, с каждым днем все большее количество систем подвергаются атакам. Мы живем в золотой век хакеров. Чтобы быть осведомленным об атакующих и защищать свою систему, необходимо понимать стратегии их атак. Данная книга была написана как раз по этой причине: помочь системным и сетевым администраторам и другим людям, работа которых связана с защитой информации, обеспечением безопасности компьютерных систем.

Никогда не следует недооценивать противника. Атакующим способен оказаться кто угодно, у него могут быть какие угодно мотивы. Уровень его знаний, а следовательно, и уровень ущерба, который он способен нанести, предугадать невозможно. Необходимо четко представлять, какая потенциальная опасность угрожает вашей организации, и применять такие средства защиты, стоимость которых сопоставима со стоимостью активов, которые вы защищаете.

Людей, атакующих системы, называют по-разному: хакерами, взломщиками, black hat и т.д. В этой книге будет использоваться лишь термин «атакующий», а компьютер атакующего на рисунках будет изображаться с черной шляпой. Во

многих сценариях для примера взяты системы с именами Элис, Боб и Ева. Элис и Боб – безобидные системы, а Ева – атакующий.

Если вы хотите поэкспериментировать с инструментами, о которых рассказывается ниже, будьте осторожны! Запускайте их только на таких системах, на которых отсутствует сколько-нибудь ценная информация и которые физически изолированы от основной сети. Создайте небольшую лабораторию из двух или трех компьютеров. Убедитесь, что законодательные акты страны и руководство компании позволяют вам использовать подобные инструменты против собственных компьютеров или в общей сети.