РОДЖЕР ГРАЙМС

# КАК ПРОТИВОСТОЯТЬ ХАКЕРСКИМ АТАКАМ

## УРОКИ ЭКСПЕРТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДЫ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ ▶ СЕКРЕТЫ ПРОФЕССИОНАЛЬНЫХ ХАКЕРОВ ▶ ЗАЩИТА ОТ СЕТЕВЫХ АТАК

БОМБОРА
ИЗДАТЕЛЬСТВО

КиберБез. Лучшие книги о безопасности в сети

Роджер Граймс

# Как противостоять хакерским атакам. Уроки экспертов по информационной безопасности

«Эксмо»

2017

УДК 004.056
ББК 32.973.2

**Граймс Р.**

Как противостоять хакерским атакам. Уроки экспертов по информационной безопасности / Р. Граймс — «Эксмо», 2017 — (КиберБез. Лучшие книги о безопасности в сети)

ISBN 978-5-04-189137-4

Кибербезопасностью сегодня озабочены все, от рядовых пользователей сети до владельцев крупных корпораций и государственных служащих. Но мало кто из них на самом деле знает, как функционирует мир хакерских атак и сетевых взломов изнутри. Эта книга — ваш проводник в мир информационной безопасности. Благодаря ей вы узнаете, какими методами пользуются самые продвинутые хакеры, как защититься от них и почему на самом деле это не так просто, как кажется. В формате PDF A4 сохранен издательский макет книги.

УДК 004.056
ББК 32.973.2

ISBN 978-5-04-189137-4

# Содержание

# Роджер Граймс
# Как противостоять хакерским атакам? Уроки экспертов по информационной безопасности

*Я посвящаю эту книгу своей супруге Трише.*
*Во всех смыслах это женщина, стоящая за мужчиной*



БОМБОРА
ИЗДАТЕЛЬСТВО
Москва 2023

# Об авторе

Роджер Граймс борется со злонамеренными компьютерными хакерами уже свыше трех десятилетий (с 1987 года). Он получил десятки сертификатов информационной безопасности (включая CISSP, CISA, MCSE, CEH и Security+), а также успешно сдал очень трудный экзамен дипломированных бухгалтеров (CPA), хотя это не имеет ничего общего с ИБ. Роджер создал и обновил курсы информационной безопасности, был инструктором и научил тысячи студентов, как взламывать и защищать. Он часто выступает на национальных конференциях по информационной безопасности. Граймсу платят как профессиональному пентестеру, чтобы он взламывал сети и веб-сайты компаний, и практически всегда он укладывается в пару-тройку часов. Ранее он написал (в том числе в соавторстве) восемь книг по информационной безопасности и около тысячи статей. С августа 2005 года Роджер пишет статьи про ИБ на сайте CSO Online (**https://www.csoonline.com/author/Roger-A.-Grimes/**), а также работает штатным консультантом более 20 лет. Роджер консультирует крупный и малый бизнес по всему миру по вопросам предотвращения хакерских и вредоносных атак. Опыт показал ему, что большинство злонамеренных хакеров не так умны, как многие считают, и они определенно проигрывают специалистам в области ИБ.

# Благодарности

Я хотел бы поблагодарить Джима Минателa, давшего зеленый свет книге, которую я обдумывал на протяжении 10 лет, и Келли Тэлбот, лучшего редактора, с которой я сотрудничал на протяжении 15 лет. Келли отлично справляется с проблемами, не повышая голоса. Я хочу поблагодарить компанию Microsoft, моего лучшего работодателя за последние 10 лет. Спасибо Брюсу Шнайеру за его негласное покровительство надо мной и всеми в этой отрасли. Мое почтение Брайану Кребсу за его большое расследование и за то, что он приоткрыл завесу тайны крупного бизнеса, каковым уже стала киберпреступность. Спасибо Россу Гринбергу, Биллу Чесвику и другим авторам, которые настолько интересно писали об информационной безопасности, что я решил построить на этом карьеру. Наконец, я не был бы тем, кто есть сегодня, без моего брата-близнеца Ричарда Граймса, лучшего писателя, подтолкнувшего меня к написанию книги более 20 лет назад. Всем специалистам по ИБ респект за помощь от имени всех нас.

# Предисловие

Роджер Граймс работает в сфере информационной безопасности почти три десятилетия, и я, к моему удовольствию, знаком с ним 15 лет. Это один из немногих избранных профессионалов среди моих знакомых, у кого безопасность в крови – интуитивное понимание предмета, которое в сочетании с колоссальным опытом поимки плохих парней и устранения уязвимостей в системах безопасности превращает его в идеального автора этой книги. Роджер впервые начал писать в журнал InfoWorld в 2005 году, когда по электронной почте раскритиковал автора статей по безопасности, причем настолько убедительно, что мы сразу же попросили его внести свой вклад в публикацию. С тех пор он написал сотни статей в InfoWorld, каждая из которых демонстрирует любовь к теме, а также понимание с точки зрения психологии как злонамеренных хакеров, так и людей, которые противостоят им. В своей еженедельной журнальной колонке «советника по безопасности» Роджер демонстрирует уникальный талант сосредоточиваться на значимых вопросах, а не преследовать эфемерные угрозы или новые технологии. У него было стойкое стремление к убеждению специалистов по информационной безопасности и их руководителей уделять ей больше внимания, несмотря на склонность многих организаций пренебрегать основами и переключаться на последние технологичные решения. В этой книге Роджер описывает этичных хакеров в сфере ИБ, которые повлияли на ситуацию. Их неустанные усилия помогают удерживать линию обороны против растущей армии злоумышленников, чьи цели с годами сместились от деструктивных воздействий в сторону кражи ценной интеллектуальной собственности и миллионов долларов у финансовых учреждений и их клиентов. Мы в неоплатном долгу перед ними. Упоминая о таких людях, как Брайан Кребс, Дороти Деннинг и Брюс Шнайер, Роджер отдает должное потраченным ими усилиям, формируя увлекательный сборник, который и развлекает, и информирует одновременно. Эту книгу важно прочесть всем, кто интересуется информационной безопасностью, и людям, которые стремятся нас обезопасить.

*Эрик Кнорр, главный редактор журнала InfoWorld*

# Введение

Цель этой книги – раскрыть мир специалистов по информационной безопасности (ИБ), некоторых из лучших хакеров, защитников конфиденциальных данных, преподавателей и писателей. Я надеюсь, что вы прочитаете ее с большим удовольствием от осознания усилий, которые потребовались, чтобы реализовать фантастический мир компьютеров, в котором мы живем сегодня. Без добрых людей на светлой стороне, воюющих против злоумышленников, компьютеры, Интернет и все, что с ними связано, были бы невозможны. Эта книга – ода специалистам по ИБ.

Я хочу призвать всех, кто собирается сделать карьеру в области информационных технологий, подумать о карьере в сфере информационной безопасности. Я также хочу призвать всех начинающих хакеров, особенно тех, кто переживает насчет этичности применения своих знаний, сделать карьеру в этой области. Я противостоял вредоносным хакерам и их творениям. Я смог исследовать каждый интерес в области хакинга, который у меня был, этичным и законопослушным способом. И десятки тысяч других. Информационная безопасность – одна из самых востребованных и высокооплачиваемых отраслей в любой стране. Это стало моим призванием и может стать вашим.

Книга разделена на главы, в которых кратко описывается реализация определенного способа атаки, а затем приводится один или два профиля специалистов по ИБ, преуспевших в этой области. Я попытался выбрать лучших из множества легенд, светил и даже некоторых относительно скромных специалистов, которые достигли блестящих успехов, даже если они не очень известны обывателям. Я попытался сформировать сочетание опыта ученых, разработчиков, преподавателей, лидеров, писателей и частных практиков, живущих в Соединенных Штатах и во всем мире. Я надеюсь, что читатели, заинтересованные в карьере специалиста ИБ, смогут так же мотивировать себя, как и я, чтобы сделать сферу ИТ значительно безопаснее для всех нас.

Да пребудет с вами сила!

# 1. Что ты за хакер?

Много лет назад я переехал в дом с прекрасным гаражом. В нем было очень удобно парковаться и даже хранить лодку и небольшой фургон. Сооружение было построено из отличных прочных досок. Электрику провели профессионалы, а качественные окна выдерживали порывы ветра скоростью 70 метров в секунду. Большую часть интерьера создал профессиональный плотник из ароматного красного кедра. Я неспособен и гвоздь забить, не то что собрать мебель, но даже мне было понятно, что он знает свое дело, думает о качестве и уделяет внимание деталям.

Через несколько недель после новоселья пришел чиновник и сказал, что гараж, построенный много лет назад, не имеет нужных документов, и придется снести незаконную постройку, иначе мне грозят крупные штрафы за каждый день просрочки исполнения постановления. Я позвонил в ведомство, чтобы утрясти вопрос, ведь гараж возвели задолго до моего переезда, и продавался он как часть недвижимости. Безрезультатно. Его нужно было немедленно снести. Штрафные санкции за один день превышали сумму, которую я мог выручить за отделку, если бы аккуратно ее снял. Проще говоря, в целях экономии, чем быстрее я демонтирую гараж, тем лучше.

Я достал кувалду и за несколько часов превратил сооружение в груду деревянных обломков и прочего мусора. В процессе я думал о том, что строителю, вероятно, потребовались недели, если не месяцы, чтобы возвести гараж, а я уничтожил его творение своими варварскими руками гораздо быстрее.

Вопреки распространенному мнению, злонамеренный взлом – это скорее кувалда стропальщика, чем тонкий инструмент ремесленника.

Если вы уверены, что сможете стать хакером, вам придется решить, будете вы стремиться к защите общего блага или довольствоваться низменными целями. Вы хотите быть скрывающимся, преступным хакером или праведным, опытным специалистом по ИБ? Эта книга – доказательство, что лучшие хакеры работают во благо. Они практикуются, развиваются интеллектуально, и им не нужно скрываться от правоохранительных органов. Они могут работать в центре сферы информационной безопасности, приводить в восхищение коллег и получать хорошие деньги. Эта книга о порой невоспетых героях, которые делают нашу невероятную цифровую жизнь возможной.

**Примечание.** Хотя термины «хакер» или «взлом» могут означать человека или деятельность как с хорошими, так и с плохими намерениями, в основном их используют в негативном ключе. Я понимаю, что хакеры могут быть разными, но во имя экономии бумаги впредь буду использовать эти слова без оговорок, подразумевая либо отрицательный, либо положительный их оттенок. Вникайте в смысл текста, чтобы понимать намерения, в связи с которыми упоминаются термины.

## Большинство хакеров отнюдь не гении

К сожалению, почти каждый, кто пишет о «злых» хакерах, не имея реального опыта, романтизирует их как умные, богоподобные, мифические фигуры. Они могут подобрать любой пароль менее чем за минуту (особенно под прицелом пистолета, если верить Голливуду), взломать любую систему и секретный шифр. Они работают в основном по ночам и пьют много энергетических напитков, а их рабочее место завалено упаковками от чипсов и фастфуда. Школьник крадет пароль учителя, чтобы изменить свои оценки, и СМИ подлизываются к нему, как к потенциальному Биллу Гейтсу или Марку Цукербергу.

Хакеры необязательно гениальны. Я – живое тому доказательство. Несмотря на то, что я вламывался в системы всех компаний, в которых меня когда-либо нанимали для проверки систем защиты, я никогда полностью не понимал квантовую физику или теорию относительности Эйнштейна. Я дважды провалил экзамен по родному языку в средней школе, никогда не получал оценки выше тройки с плюсом по математике, а мой средний балл в первом семестре колледжа составил 0,62. Я получил пять двоек и одну пятерку. Одинокая пятерка была по курсу безопасности на водах, потому что я на тот момент пять лет работал пляжным спасателем. Плохие оценки были не только следствием того, что я не учился. Я просто не был достаточно умен и не пытался с этим справиться. Позже я узнал, что учеба и усердная работа часто более ценны, чем врожденный высокий уровень интеллекта. Я окончил университет и преуспел в мире информационной безопасности.

Тем не менее, даже когда писатели не называют «злых» хакеров сверхумными, читатели частенько предполагают, что они именно таковы, потому что, похоже, практикуют какую-то передовую черную магию, о которой остальной мир не подозревает. Коллективный всемирный разум считает, что «злой хакер» и «суперинтеллект» должны идти рука об руку. Это неправда. Некоторые из них умные, большинство средние, а остальные вообще бестолковы, как и многие другие люди. Просто хакерам известно о сведениях и процессах, которые незнакомы людям других профессий, например плотникам, сантехникам и электрикам.

## Специалисты по ИБ – продвинутые хакеры

Если проводить интеллектуальное сравнение, то специалист по ИБ в среднем умнее хакера. Он должен знать все, на что способен злоумышленник, а также уметь остановить атаку. Защита не сработает, если нет участия конечного пользователя, работает скрытно и справляется идеально (или почти идеально) все время. Покажите мне «злого» хакера с определенной техникой, и я покажу вам много специалистов по ИБ, которые умнее и лучше его. Однако атакующим обычно уделяется больше внимания. И моя книга призвана исправить ситуацию.

# Хакеры особенны

Несмотря на то, что я не разделяю хакеров на гениальных, хороших и плохих, все они имеют несколько общих черт. Одна из них – широкое интеллектуальное любопытство и готовность пробовать новое за пределами данных интерфейсов или границ. Они не боятся идти своим путем. Компьютерные хакеры, как правило, таковы и по жизни, взломщики всевозможного за пределами компьютеров. Они относятся к тому типу людей, которые, столкнувшись с системой безопасности в аэропорту, размышляют о том, как пронести оружие, которого у них нет, мимо детекторов. Они выясняют, можно ли подделать дорогие билеты на концерт, даже если не собираются посещать его. А покупая телевизор, задаются вопросом, можно ли получить доступ к его операционной системе, чтобы что-нибудь там изменить. Покажите мне хакера, и я покажу вам того, кто постоянно ставит под сомнение статус-кво и все исследует.

**Примечание.** В какой-то момент моя собственная гипотетическая схема пронесения оружия через охрану аэропорта строилась на использовании инвалидных колясок с оружием или взрывчаткой, спрятанными внутри металлического каркаса. Инвалидные кресла часто провозят мимо охраны аэропорта, не подвергая тщательному досмотру.

## Хакеры настойчивы

Следующее после любопытства важное качество хакера – настойчивость. Каждый хакер – и хороший, и плохой – проходил через пытку, когда ты долгими часами пытаешься снова и снова заставить что-то работать. Злоумышленники ищут бреши в защите. Одна ошибка специалиста по ИБ, по сути, сводит на нет всю защиту. Специалист по ИБ должен быть идеальным. Все компьютеры и программное обеспечение должны быть пропатчены, каждая конфигурация проверена на отсутствие уязвимостей, и каждый конечный пользователь отлично обучен. По крайней мере, в идеальном мире. Специалисты по ИБ знают, что применяемые средства защиты не всегда работают или применяются в соответствии с инструкциями, поэтому выстраивают уровни «глубокоэшелонированной обороны». И злоумышленники, и специалисты по ИБ ищут слабые места, только с противоположных сторон баррикад. Обе стороны участвуют в непрерывной войне со многими столкновениями, победами и поражениями. Самые стойкие выходят победителями.

# Шляпных дел мастера

Я всю свою жизнь был хакером. Мне платили за то, чтобы я вламывался куда-либо (на что у меня были юридические полномочия). Я взламывал пароли, сети, писал вредоносные программы и при этом ни разу не нарушил закон и не преступил границ этики. Это не значит, что никто из знакомых не пытался меня на это соблазнить. На протяжении многих лет друзья просили меня взломать мобильный телефон супруга, уличенного в измене; заместители хотели получить доступ к электронной почте начальства; а также люди без ордера требовали «вскрыть» компьютер одного злого хакера, чтобы предотвратить его дальнейшие взломы. На ранней стадии вы должны решить, кто вы и какова ваша этика. Я решил, что буду хорошим хакером («в белой шляпе»), а «белые шляпы» не совершают незаконных или неэтичных действий.

Хакеры, которые участвуют в незаконной и неэтичной деятельности, называются «черными шляпами». Хакеры, которые зарабатывают на жизнь законным образом в сфере ИБ, но в духе «Бойцовского клуба» тайно промышляют взломами, известны как «серые шляпы». Мое представление о кодексе чести предусматривает лишь два варианта. Для меня «серых шляп» не существует. Ты либо делаешь незаконные вещи, либо нет. Ограбь банк, и я назову тебя грабителем, каковой бы ни была твоя цель.

Однако «черные шляпы» могут стать «белыми». Это происходит сплошь и рядом. Вопрос в том, станет ли хакер «белым», прежде чем ему придется сесть за решетку. Кевин Митник – один из самых известных арестованных хакеров в истории (см. главу 5), который после выхода из тюрьмы начал карьеру в сфере ИБ на всеобщее благо. Роберт Т. Моррис, написавший и выпустивший первого компьютерного червя, чуть не уничтожившего Интернет (**https://ru.wikipedia.org/wiki/Червь_Морриса**), в итоге стал членом Ассоциации вычислительной техники (**https://awards.acm.org/award_winners/morris_4169967.cfm**) за «вклад в компьютерные сети, распределенные и операционные системы».

Раньше грань между легальным и нелегальным взломом была не столь четкой. Более того, многие ранние «злые» хакеры получили статус супергероев. Даже я не мог открещиваться от некоторых из них. Джон Дрейпер (ник Capitan Crunch) свистел в игрушечный свисток, обнаруженный им в коробке кукурузных хлопьев Cap'n Crunch, чтобы сымитировать тон частотой 2600 Гц. Таким образом он мог бесплатно звонить по межгороду. Многие хакеры, которые публиковали приватную информацию «во имя общественного блага», часто становились известными. Но, за некоторыми исключениями, я никогда не придерживался чрезмерно идеализированного взгляда на хакеров-злоумышленников. У меня была довольно четкая позиция, что люди, которые делают несанкционированные вещи с чужими компьютерами и данными, совершают преступление.

Много лет назад, впервые заинтересовавшись компьютерами, я прочитал книгу Стивена Леви «Хакеры: герои компьютерной революции»[1]. На заре эры персональных компьютеров Леви написал занимательную историю о хакерах, хороших и плохих, воплощающих хакерский идеал. Бóльшая часть книги посвящена людям, которые улучшили мир с помощью компьютеров, но в ней также упоминаются и те, кто сегодня был бы арестован за свою деятельность. Некоторые из этих хакеров полагали, что цель оправдывает средства, и следовали свободе морали, воплощенной, по словам Леви, «хакерской этикой». Главным среди этих верований была философия о том, что каждый компьютер может быть доступен по любой законной причине, что вся информация должна быть свободной, и не следует доверять властям. Это был

[1] http://rus-linux.net/MyLDP/BOOKS/zip/hackers-heroes.pdf.

романтический взгляд на хакерство, хотя он не скрывал сомнительных этических и юридических вопросов. На самом деле все вокруг вновь расширили границы.

Ради автографа я отправил Стивену Леви экземпляр его книги (мне тоже стали присылать мои книги на подпись после того, как я выпустил восемь предыдущих). Леви публиковал свои статьи и редактировал чужие в нескольких крупных журналах, включая Newsweek, Wired и Rolling Stone. Кроме того, он написал еще шесть книг по вопросам информационной безопасности. Леви пишет и по сей день. Его книга «Хакеры: герои компьютерной революции» открыла для меня поразительный мир хакерства.

Позже другие книги, такие как *Flu-Shot* Росса Гринберга (давно не издается) и *Computer Viruses, Worms, Data Diddlers, Killer Programs, and Other Threats to Your System* Джона Макафи **(https://www.amazon.com/Computer-virusesdiddlers-programs-threats/dp/031202889X)** познакомили меня со стратегиями борьбы со злонамеренными хакерами. Я настолько ими впечатлился, что всерьез задумался о карьере борца с этими угрозами.

Позже я узнал, что специалисты по ИБ – самые умные хакеры. Я не хочу сводить всех злонамеренных хакеров под одну гребенку посредственности. Каждый год редкие гениальные хакеры обнаруживают что-то новое. Но подавляющее большинство «черных шляп» довольно посредственны и просто повторяют то, что работает уже на протяжении двадцати лет. Среднестатистический хакер-злоумышленник не имеет достаточного таланта в программировании, чтобы написать простое приложение типа «Блокнот», а тем более самостоятельно проникнуть куда-то, взломать ключи шифрования или самолично успешно подобрать пароли – без помощи других хакеров, которые реально талантливы и успешны на протяжении многих лет.

Ирония в том, что умные люди в компьютерном мире, о которых я знаю, – это не злые хакеры, а специалисты по ИБ. Они должны знать все, что делает хакер, предугадывать то, что он может совершить, и выстроить качественную оборону. Мир специалистов по ИБ полон кандидатов наук, магистрантов и успешных предпринимателей. Теперь хакеры редко меня впечатляют. А вот специалисты по ИБ – всегда.

Обычно специалисты по ИБ открывают для себя новый способ взлома, чтобы предотвратить атаки такого рода, и умалчивают о своем достижении. Это сродни министерству обороны, и предоставление злоумышленникам новых способов взлома до того, как оборона будет возведена, никому не облегчит жизнь. Это их образ жизни: выяснить новый способ взлома и помочь с латанием бреши, прежде чем она будет обнаружена кем-то еще. Такое случается гораздо чаще, чем обратное (например, злонамеренный хакер обнаруживает новую уязвимость).

Я был свидетелем тому, как специалисты по ИБ находят новый способ взлома, но из-за высоких затрат или недостатка времени уязвимость не закрывается немедленно, и какой-нибудь хакер получает звание «первооткрывателя». К сожалению, специалисты по ИБ не всегда получают славу и признание, когда выполняют свою повседневную работу.

Я тридцать лет изучал приемы работы как вредоносных хакеров, так и специалистов по ИБ, и мне стало ясно, что специалисты впечатляют сильнее. Вредоносные хакеры даже рядом не стояли. Если вы хотите показать всем, насколько хорошо разбираетесь в компьютерах, не раскрывайте новый способ взлома – лучше покажите новую стратегию обороны. Не требуется особого ума, чтобы что-то по-новому сломать. Это в основном требует лишь настойчивости. Но человек должен быть особенным и одаренным, чтобы построить то, что может выдержать непрерывные атаки в течение длительного времени.

Если вы хотите произвести впечатление на мир, не сносите гараж. Вместо этого создайте код, который сможет выдержать кувалду хакера-взломщика.

# 2. Как хакеры взламывают

Самый приятный аспект моей работы – это тестирование на проникновение (также известное как пентестирование). Пентестирование – это взлом в прямом смысле этого слова. Это битва интеллектов человека и машины. Человек – «атакующий» – может использовать собственную изобретательность и новые или существующие инструменты, когда исследует слабые стороны машин или людей. За все годы, что я занимался тестированием, хотя мне на это обычно дают недели, я успешно взламывал цель примерно за час. Самый долгий взлом, помню, продолжался три часа. Это касается любого банка, медицинского, правительственного или корпоративного учреждения, который когда-либо нанимал меня для тестирования на проникновение.

При этом я не могу назвать себя отличным пентестером. По шкале от 1 до 10, где 10 – высший балл, мои способности составляют примерно 6 или 7. С точки зрения специалиста по ИБ я чувствую себя лучшим в мире, но я весьма посредственный взломщик. Я был окружен потрясающими пентестерами, как мужчинами, так и женщинами, которые не помышляли о написании собственных инструментов пентестирования или не считали свои действия успешными, если не они привели к созданию хотя бы одного события с предупреждением в логах. Но даже люди, которых я оцениваю на 10 баллов, обычно считают себя середнячком и восхищаются другими пентестерами, которых, по их мнению, десятки. Насколько же хороши должны быть эти хакеры?

Вам не нужно быть исключительным, чтобы стать очень успешным хакером. Для начала карьеры даже не нужно успешно взламывать клиента, который вас нанял (я предполагаю, что вам платят за законные пентесты). На самом деле клиенты будут в абсолютном восторге, если вы *не* взломаете систему. Они смогут похвастаться, что наняли хакеров, а их сеть выдержала атаку. Это беспроигрышный вариант для всех участников. Вы получаете свои деньги, а они радуются, что атака отражена. На моей памяти это единственная работа, где не может быть плохого результата. К сожалению, я не знаком ни с одним пентестером, который когда-либо успешно взламывал *все* свои цели. Я уверен, что есть хакеры, которые терпят неудачу, но подавляющее большинство «сорвут свой куш».

**Примечание.** Если ваши тесты не обнаружили слабых мест, а клиент вскоре был скомпрометирован реальными злоумышленниками, это выставит вас не в лучшем свете. Если это произойдет несколько раз, дурная слава не обойдет вас стороной, и вы, вероятно, будет искать новую работу. Слабые места есть. Ищите их.

Обычно пентестеры делают что-то еще, чтобы произвести впечатление на своих клиентов. Например, удаленно снимают генерального директора за рабочим столом на веб-камеру или взламывают пароль к серверу и размещают «Веселого Роджера» на рабочем столе компьютера сетевого администратора. Это стоит тысячи слов. Не стоит недооценивать, насколько одна глупая картинка может повысить удовлетворенность клиентов вашей работой. Они будут вспоминать о ней (и хвастаться вами) спустя годы после того, как вы закончите работу. Если можете, всегда заканчивайте красивым жестом. Это мой «золотой совет».

## Секрет взлома

Если у хакеров и есть секрет взлома, то он точно не в том, как ломать. Это процесс изучения правильных методов и использования верных инструментов, точно как у электриков, сантехников или строителей. Нет определенного способа взлома. Однако существует вполне конкретный набор шагов, которые объединяются в более крупные этапы; это процесс, который включает в себя все, что необходимо хакеру для выполнения задачи. Не каждый хакер проходит все шаги. Некоторые вообще делают только один. Но в целом, если вы будете следовать этапам, то, скорее всего, придете к успеху. Вы можете пропустить один или несколько шагов и все равно быть успешным хакером. Вредоносные программы и другие инструменты взлома часто позволяют пропускать шаги, но по крайней мере один из них – первоначальное проникновение – требуется всегда. Независимо от желания сделать официальную карьеру хакера, если вы собираетесь бороться со злоумышленниками, нужно понимать методологию взлома. Модели могут различаться, включая количество шагов, их названия и конкретные детали, но все они содержат одни и те же основные компоненты.

## Методология взлома

Методология взлома содержит следующие прогрессивные шаги.

1. Сбор информации.
2. Проникновение.
3. Упрощение доступа в будущем (необязательный).
4. Разведка системы.
5. Перемещение (необязательный).
6. Выполнение намеченного действия.
7. Заметание следов (необязательный).

## Сбор информации

Как правило, если хакер не рассчитывает взламывать все потенциально уязвимые сайты, он придерживается конкретной цели. Проникая в конкретную компанию, первое, что он делает, это собирает о ней всю информацию, которая поможет проникнуть в систему. Это IP-адреса, адреса электронной почты и доменные имена. Хакер узнает, сколько потенциальных сайтов и сервисов, к которым он может получить доступ, подключены к компании. Используя средства массовой информации и публичные документы, он находит сведения о руководителях высшего звена и прочих сотрудниках для проведения атак средствами социальной инженерии. Хакер просматривает новости, чтобы узнать, какое крупное программное обеспечение недавно купил объект, какие происходили слияния или разделения (такие мероприятия часто сопровождаются ослаблением уровня безопасности), и даже с какими партнерами взаимодействует «жертва». Многие компании были скомпрометированы гораздо более слабым партнером.

В большинстве хакерских атак важнее всего выяснить, с какими цифровыми активами связана компания. Обычно идентифицируются не только основные (публичные) сайты и службы; чаще злоумышленнику полезнее обратить внимание на менее популярные, такие как ресурсы сотрудников и партнеров. Такие сайты и серверы, скорее всего, имеют более слабую систему безопасности, нежели крупные порталы компаний.

Затем толковый хакер начинает собирать сведения обо всем ПО и сервисах, доступных на каждом из этих сайтов. Это процесс, известный как сбор цифровых отпечатков. Очень важно узнать, какие операционные системы (ОС) и их версии используются. Версии ОС могут сказать

хакеру об уровнях защиты системы и ошибках, которые могут или не могут присутствовать. Представим, что он встречает операционную систему Windows Server 2012 R2 или Linux Centos 7.3-1611. По той же причине он ищет программы и вариации версий программного обеспечения, работающие на каждой из этих ОС. Если это веб-сервер, он может встретить Internet Information Server 8.5 на Windows или Apache 2.4.25 на Linux. Он проводит инвентаризацию каждого устройства, операционной системы, приложений и версий, запущенных на каждом из целевых объектов. Всегда лучше провести тщательную инвентаризацию, чтобы получить полную картину, но в других случаях хакер может найти крупную уязвимость на ранней стадии и перейти к следующему шагу. Если отбросить этот быстрый способ, как правило, чем больше информации хакер соберет о том, что работает, тем лучше. Каждое дополнительное ПО и версия предоставляет дополнительные возможные векторы атаки.

**Примечание.** Некоторые хакеры называют общий нетехнический сбор информации поиском следов, а поиск информации об операционной системе и программном обеспечении – сбором цифровых отпечатков.

Порой, когда хакер подключается к сайту, тот услужливо отвечает очень подробной информацией о версиях программного обеспечения, поэтому не нужны никакие дополнительные инструменты. На случай, если этого не происходит, существует много инструментов, упрощающих сбор цифровых отпечатков. На сегодня первый инструмент, который использует хакер для сбора цифровых отпечатков, – это Nmap **(https://nmap.org/)**. Программа разработана в 1997 году. Она представлена в нескольких версиях, поддерживающих операционные системы Windows и Linux, и, по сути, представляет собой швейцарский армейский нож, только для хакера. Nmap может выполнять все виды сканирования и тестирования хоста, и это очень хороший способ сбора цифровых отпечатков. Для этого существуют и более мощные приложения, в частности сосредоточенные на сборе определенных данных, таких как информация о веб-серверах, базах данных или серверах электронной почты. Например, программа Nikto2 **(https://cirt.net/Nikto2)** не только эффективнее Nmap собирает цифровые отпечатки с веб-серверов, но и выполняет тысячи пентестов и позволяет выявить уязвимые места.

## Проникновение

Это шаг, который позволяет хакеру получить первоначальный доступ. От его успешности зависит весь дальнейший процесс. Если хакер хорошо поработал на этапе снятия цифровых отпечатков, то проникновение будет действительно не таким уж сложным. Честно говоря, я всегда его проходил. В сфере ИБ есть недостатки: используется старое программное обеспечение, остаются незакрытые уязвимости из-за игнорирования патчей и почти всегда что-то неправильно настроено в системе аутентификации.

**Примечание.** Один из моих любимых трюков – атаковать ПО и устройства, которые специалисты по ИБ используют для защиты своих сетей. Часто такое обеспечение и устройства проблематично пропатчить, и в них на многие годы остаются незалатанные уязвимости.

Если вдруг все ПО и устройства полностью защищены (а такого не бывает), то можно атаковать через человеческий фактор, который всегда оказывается самым слабым элементом системы уравнения. Но без первоначального проникновения для хакера все потеряно. К счастью для него, есть много способов проникнуть к жертве. Вот различные методы, которые хакер может для этого использовать:

- уязвимости нулевого дня (0day);

- непропатченное программное обеспечение;
- вредоносные программы;
- социальная инженерия;
- подбор паролей;
- перехват или атака посредника;
- утечка данных;
- неправильная конфигурация оборудования;
- отказ в обслуживании;
- участие инсайдеров, партнеров, консультантов, производителей и других третьих лиц;
- пользовательский фактор;
- физический доступ;
- повышение привилегий.

## Уязвимости нулевого дня

Уязвимости нулевого дня (0day[2]) – это эксплойты (внедрения), которые встречаются реже, чем другие известные уязвимости, большинство которых производители давно закрыли патчами. Для его исправления еще не выпущен патч, и общественность (как, впрочем, и разработчик) не знает об этом. Любые компьютерные системы, на которых присутствует программное обеспечение с уязвимостями нулевого дня, подвержены взлому, если потенциальная жертва не удалит его или не использует инструмент для смягчения последствий (например, брандмауэр, список контроля доступа, сегментация посредством виртуальных ЛВС, средства защиты от переполнения буфера и т. д.).

Уязвимости нулевого дня не так распространены, как другие эксплойты, поэтому не могут постоянно эксплуатироваться злоумышленником. Если хакер ими злоупотребляет, они будут обнаружены и исправлены специалистами по ИБ и добавлены в сигнатуры антивирусных программ. В большинстве таких ситуаций специалисты по ИБ могут исправлять новые эксплойты через нескольких часов, максимум дней после обнаружения. Когда в ход идут уязвимости нулевого дня, они либо используются очень широко против нескольких целей сразу для максимально возможного эффекта, либо применяются только в крайнем случае. Лучшие в мире профессиональные хакеры обычно имеют подборки уязвимостей нулевого дня, которые используют только тогда, когда все остальные подходы не удались. И даже в таких ситуациях они атакуют так, чтобы сохранять максимальную скрытность. Уязвимость нулевого дня может быть использована для получения первичного доступа к особенно устойчивой системе, а затем все ее следы удаляются и далее реализуются более традиционные методы взлома.

## Непропатченное программное обеспечение

Вовремя непропатченное ПО – одна из главных причин, почему компьютером или устройством завладевает злоумышленник. Каждый год публикуются сведения о тысячах (обычно 5–6 тысяч, т. е. около 15 в день) новых обнаруженных уязвимостях в популярном программном обеспечении. (Познакомиться со списком можно на сайте службы безопасности Microsoft: **https://www.microsoft.com/ru-ru/security/business/security-intelligence-report**.) Разработчики, как правило, стараются писать более защищенный код и исправлять собственные ошибки, но число программ и миллиардов строк кода растет, поэтому общее количество ошибок остается относительно неизменным в течение последних двадцати лет. Большинство разработчиков своевременно выпускают патчи для своего ПО, и чаще всего происходит это после того, как уязвимость становится общеизвестной. К сожалению, пользо-

[2] Читается как «зеро-дэй». – *Прим. перев.*

ватели их продукции, как известно, нерасторопно применяют эти патчи, нередко даже отключая процедуру автоматического обновления. Определенный процент пользователей и вовсе не патчит системы. Они либо игнорируют предупреждения и оповещения об обновлениях, либо раздражаются при их появлении, либо вообще не знают, зачем их применять (например, многие торговые системы не уведомляют кассиров о необходимости обновления). Большинство эксплойтов касаются программного обеспечения, которое не патчилось (т. е. не обновлялось) в течение многих лет. Даже если конкретная компания или пользователь исправляет критические уязвимости так же быстро, как они появляются, терпеливый хакер может ждать «дыру», которая будет обнаружена со временем, и запустит соответствующую атаку, прежде чем специалисты по ИБ успеют выявить ее и инициировать выпуск патча. (Хакеру относительно легко удается обратная разработка таких «брешей», и он узнает, как эксплуатировать ту или иную уязвимость.) Как уязвимость нулевого дня, так и обычные уязвимости ПО сводятся к небезопасным методам, применяемым при разработке программного обеспечения. Мы рассмотрим их в главе 6.

## Вредоносные программы

Вредоносные программы бывают разных видов. Наиболее известные из них – это вирусы, троянские программы и черви. При этом современные вредоносные программы часто представляют собой гибридную смесь нескольких типов. Вредоносное ПО позволяет хакеру реализовать метод эксплойта, чтобы было проще атаковать или чтобы быстрее охватить большее количество жертв. Когда обнаруживается новый эксплойт, специалисты по ИБ знают, что авторы вредоносных программ будут использовать автоматизированное вредоносное ПО для более быстрого распространения. Этот процесс известен как «вооружение». В то время как эксплойтов следует избегать, зачастую именно их эксплуатация создает наибольший риск для конечных пользователей и общественности. Без вредоносных программ злоумышленник был бы вынужден атаковать каждую жертву поочередно. С их помощью миллионы компьютеров могут подвергнуться взлому в течение нескольких минут. Мы познакомимся с вредоносными программами поближе в главе 9.

## Социальная инженерия

Одна из самых успешных стратегий взлома – социальная инженерия. Независимо от того, осуществляется она вручную или автоматически, это хакерский трюк, обманывающий конечного пользователя, который наносит вред собственному компьютеру или безопасности. Это может быть электронное письмо, которое обманом принуждает перейти по вредоносной ссылке или открыть зараженное вложение. Хакер может заставить пользователя раскрыть свои персональные данные для авторизации (так называемый фишинг). Социальная инженерия уже давно находится на лидирующих позициях среди атак, реализуемых хакерами. Опытный хакер в «белой шляпе», Кевин Митник, – один из лучших примеров социальных инженеров-злоумышленников. Речь о нем пойдет в главе 5, а социальная инженерия более подробно рассматривается в главе 4.

## Подбор паролей

Пароли или их деривации могут быть подобраны или украдены. Долгое время простой подбор паролей (или социальная инженерия) был одним из самых популярных способов получения начального доступа к компьютерной системе или сети и до сих пор таковым остается. Но кража учетных данных и так называемые атаки повторного воспроизведения (pass-the-hash), по существу, затмили атаки со взломом паролей в течение последних нескольких лет. При атаках с кражей учетных данных злоумышленник обычно получает административный доступ

к компьютеру или устройству и перехватывает одну или несколько записей учетных данных, хранящихся в системе (в памяти или на жестком диске). Украденные данные затем используются для доступа к другим системам. Почти каждая крупная корпоративная атака включала кражи учетных данных в качестве общего компонента эксплойта, так что традиционный подбор паролей уже не так популярен. Взломы паролей описаны в главе 21.

## Перехват или атака посредника

Перехват и атака посредника (MITM-атака) ставят под угрозу легитимное сетевое подключение, позволяя получить доступ к нему или злонамеренно участвовать в коммуникациях. Большинство таких атак успешны из-за недостатков в сетевых или прикладных протоколах, но также могут быть результативны вследствие человеческого фактора. В наши дни самые большие атаки происходят в беспроводных сетях. Сетевые атаки будут рассмотрены в главе 33, а беспроводные – в главе 23.

## Утечка данных

Утечка персональной информации может быть результатом одной из форм взлома, а также непреднамеренного или преднамеренного действия самого владельца данных. Большинство утечек происходят из-за непреднамеренной (и незащищенной) их публикации или потому, что некий хакер выяснил способ доступа к определенным персональным данным. Но инсайдерские атаки, когда сотрудник или контрагент намеренно крадет или использует персональную информацию, – не менее распространенная форма взлома. Некоторые главы этой книги посвящены предотвращению утечек данных.

## Неправильная конфигурация оборудования

Неправильная настройка компьютеров также часто реализует очень слабые варианты защиты, иногда непреднамеренно. Я не смогу сосчитать, сколько раз заходил на общедоступный веб-сайт и видел, что его самые важные файлы непонятным образом доступны всем пользователям или даже всему миру. Когда вы сообщаете миру, что любой желающий может получить доступ к любому файлу, который им нравится, ваш сайт или файлы, хранящиеся на нем, недолго будут оставаться приватными. Безопасные операционные системы и конфигурации описаны в главе 30.

## Отказ в обслуживании

Даже если владелец не совершил ни одной ошибки или строго ставил все патчи на программное обеспечение, с помощью Интернета все равно можно взломать почти любой сайт или компьютер. Даже если вы совершенны, компьютеры, которые вы используете, полагаются на одну или несколько неподконтрольных вам служб, которые потенциально уязвимы. Сегодня масштабные атаки отказа в обслуживании могут положить или значительно повлиять на работу почти любого сайта или компьютера, подключенного к Интернету. В процессе таких атак часто передаются миллиарды вредоносных пакетов в секунду, из-за которых падает (становится недоступен) целевой сайт (или его вышестоящие/нижестоящие соседи). Существуют десятки коммерческих, в том числе незаконных служб, которые можно использовать как для создания, так и для защиты от мощных атак отказа в обслуживании. Рассмотрим их в главе 28.

## Участие инсайдеров, партнеров, консультантов, производителей и других третьих лиц

Даже если ваша сеть и ее компьютеры совершенны (что едва ли возможно), вы можете быть скомпрометированы дефектом в системе подключенного партнера или инсайдером. Эта категория довольно широка и пересекается с рядом других хакерских методов.

## Пользовательский фактор

Эта категория проникновения также пересекается с другими методами. Например, пользователь может случайно отправить персональные данные неавторизованному пользователю, указав в адресе электронной почты один неверно введенный символ. Пользователь может случайно пропустить критический патч для серверного ПО или установить неверное разрешение. Частая ошибка пользователя – отвечая на электронное письмо определенному человеку или группе людей, случайно разослать письмо всем или даже, по ошибке, отреагировать в негативном ключе. Я отдельно выделил пользовательские ошибки только потому, что человеческий фактор иногда срабатывает, и хакеры готовы этим воспользоваться.

## Физический доступ

Общепринятое мнение гласит, что, если злоумышленник имеет физический доступ к устройству, он может просто украсть его (секунда – и ваш мобильный телефон благополучно уведен) и уничтожить или в итоге обойти все средства защиты для доступа к персональным данным. Этот метод остается довольно успешным до сих пор, даже против средств, явно предназначенных для защиты от физических атак. Например, многие программы шифрования диска могут быть взломаны с помощью электронного микроскопа для выявления защищенного секретного ключа путем идентификации отдельных электронов, составляющих ключ. Или оперативная память может быть заморожена баллончиком со сжатым воздухом, чтобы прочитать секретный ключ шифрования в открытом виде из-за ошибки в том, как она хранит данные.

## Повышение привилегий

Каждый хакер использует один из методов проникновения, описанных в предыдущих разделах, чтобы получить доступ к целевой системе. Единственный вопрос – это тип доступа, который он получает. Если хакер использует программное обеспечение или службы, запущенные в собственном контексте безопасности пользователя, он изначально имеет только те же права доступа и разрешения, что и авторизованный пользователь. Или он может открыть святой Грааль и получить полный доступ к административной системе. Если злоумышленник получает только обычные, непривилегированные разрешения доступа, то он обычно выполняет вторую атаку для эскалации привилегий, чтобы попытаться получить более высокий доступ. Атаки эскалации привилегий охватывают весь спектр, по существу, дублируя те же подходы, что и для проникновения, но они начинаются с более высокой начальной точки, уже имеющей некоторый доступ. Атаки с повышением привилегий обычно проще выполнить, чем первоначальные эксплойты. И поскольку начальные эксплойты почти всегда гарантированно будут успешными, эскалация привилегий намного проще.

## Упрощение доступа в будущем

Затем, хотя это необязательно, после получения первоначального доступа, злоумышленник работает над реализацией дополнительного метода, чтобы убедиться, что сможет легко

получить доступ к тому же ресурсу или ПО в следующий раз. Многие хакеры размещают «прослушивающий» бэкдор, с помощью которого можно подключиться вновь. В других случаях это означает взлом паролей или создание новых учетных записей. Злоумышленник всегда может использовать те же эксплойты, которые успешно отработали в прошлый раз, чтобы снова взломать систему, но обычно применяет другой метод, который будет работать, даже если жертва исправляет уязвимость.

## Разведка системы

Чаще всего, как только хакер проник в систему, он начинает выполнять команды или программы, чтобы узнать больше о цели, к которой получен доступ, и о том, что с ней связано. Обычно это означает поиск в оперативной памяти, файлов на жестком диске, сетевых подключений, общих ресурсов, служб и программ. Эта информация используется для лучшего понимания цели, а также для планирования следующей атаки.

## Перемещение

Это редкая разновидность атаки или вредоносного воздействия, применяемого для взлома определенной цели. Почти все хакеры и вредоносные программы хотят подчинить себе как можно больше. Как только они получают доступ к первоначальной цели, распространение их влияния в пределах одной сети или объекта упрощается. Методы проникновения хакеров, перечисленные в этой главе, суммируют различные способы, которыми они могут это сделать, но, сравнивая их с первоначальными усилиями, последующее перемещение облегчается. Если атакующий движется к другим подобным целям, это называется боковым перемещением. Если злоумышленник переходит с устройств с одной привилегией на более высокую или более низкую, это называется вертикальным перемещением.

Большинство атакующих переходят от низких уровней к высоким, используя методы вертикального перемещения (опять же, реализуя методы хакерского проникновения, с которыми мы познакомились). После проникновения они ищут пароли от учетной записи локального администратора. Затем, если эти учетные данные совместно используются несколькими компьютерами (что часто бывает), они перемещаются горизонтально и повторяют процесс, пока не смогут получить доступ к самым привилегированным учетным записям. Иногда это делается во время первого взлома, так как авторизованный пользователь или система уже имеет очень высокие привилегии. Затем они перемещаются на сервер аутентификации и считывают учетные данные каждого пользователя. Это стандартный алгоритм для большинства современных хакерских атак, и переход от первоначального взлома к полному овладению сетью может занять менее часа.

Как хакеру средней руки, мне обычно требуется около часа, чтобы проникнуть, и еще час, чтобы захватить централизованную базу данных аутентификации. Так что на захват сети компании в среднем уходит около двух часов. Самое долгое проникновение заняло у меня три часа.

## Выполнение запланированного действия

После формирования лазеек и установки прав собственности на файлы хакеры выполняют то, что намеревались сделать (если только действие взлома не выявило новые задачи). У каждого хакера есть цель. Официальный пентестер заключает договор на выполнение одной или нескольких процедур. Злоумышленник может распространять вредоносное ПО, читать или красть конфиденциальную информацию, вносить вредоносные изменения и причинять иной вред. Цель хакера, желающего скомпрометировать одну или несколько систем, – что-то с

ней сделать. Давным-давно (два или три десятилетия назад) целью хакеров было просто продемонстрировать, что они взломали систему. Сегодня 99 % взломов криминально мотивированы, и хакер собирается сделать что-то вредоносное для цели (даже если единственный ущерб, который он наносит, это скрытное проникновение для потенциальных действий). Несанкционированный доступ без прямого ущерба – это все равно ущерб.

## Заметание следов

Некоторые хакеры пытаются замести следы. Раньше это делали почти все, но в наши дни компьютерные системы настолько сложны и присутствуют в таком количестве, что большинство владельцев данных не проверяют хакерские следы. Они не проверяют логи, не ищут НИКАКИХ признаков незаконного проникновения, если те не бросаются в глаза. Каждый год отчет компании Verizon о расследованиях случаев несанкционированного доступа к данным **(https://www.verizon.com/business/resources/reports/dbir/)** сообщает, что большинство атакующих остаются незамеченными в течение нескольких месяцев или даже лет, а более 80 % атак были бы замечены, если бы специалисты по ИБ потрудились над анализом. Из-за такой статистики большинство хакеров уже не утруждают себя заметанием следов.

Хакеры сегодня еще меньше стремятся к этому, потому что используют методы, которые невозможно обнаружить традиционными способами. Или действия хакера настолько распространены в среде жертвы, что практически нельзя отличить легитимную деятельность от незаконной. Например, после взлома хакер обычно выполняет действия в контексте безопасности законного пользователя, часто получая доступ к тем же серверам и службам, что и последний. И они используют те же инструменты (например, программное обеспечение удаленного доступа и сценарии), что и администраторы. Кто может определить, что злонамеренно, а что нет? Области обнаружения вторжений рассматриваются в главе 14.

## Взлом скучно успешен

Если вы хотите знать, как хакеры взламывают, то обратились по адресу. Единственное, что осталось сделать, это добавить инструменты, любопытство и настойчивость. Процесс взлома настолько успешен, что многие пентестеры после первоначального восторга от профессионального хакинга через несколько лет впадают в уныние и меняют сферу деятельности. Понимаете, насколько хорошо отработан процесс? Вот почему специалистам по ИБ нужно бороться с хакерами.

# Автоматизированная вредоносная программа как инструмент взлома

Вредоносная программа может выполнять один или несколько шагов в автоматическом режиме или передать хакеру управление, как только цель достигнута. Большинство хакерских групп сочетают социальную инженерию, автоматизированное вредоносное ПО и действия самих хакеров для достижения целей. В больших группах отдельным хакерам могут назначаться роли и должности. Вредоносная программа может выполнить один шаг проникновения и достигнуть успеха, не пытаясь осуществить любой из других шагов. Например, самая быстрая вредоносная программа в истории, SQL Slammer, имела размер всего 376 байт. Она выполняла задачу по переполнению буфера на UDP-порте SQL 1434 независимо от того, был ли на целевом устройстве запущен SQL. Поскольку на большинстве компьютеров он не выполняется, можно подумать, что атака будет весьма неэффективна. Но нет, за 10 минут этот червь изменил мир. Ни одна вредоносная программа никогда даже не приближалась к заражению такого количества устройств за столь короткое время.

**Примечание.** Если я пропустил какой-то шаг в хакерской методологии или способ проникновения, прошу прощения. С другой стороны, я же предупреждал, что я ничем не примечательный хакер.

# Этика взлома

Я хотел бы думать, что мои читатели – этичные хакеры, которые проводят взлом своих целей законным образом. Взлом сайта, на который у вас нет предопределенных и выраженных полномочий, неэтичен и часто незаконен. Также неэтично (и даже незаконно) взломать сайт и сообщить владельцам о найденной уязвимости бесплатно. Неэтично и часто незаконно найти уязвимость, а затем попросить владельцев сайта нанять вас в качестве пентестера. Последнее происходит сплошь и рядом. Если вы сообщите кому-то, что нашли способ взломать его сайты или серверы, и попросите работу, это будет рассматриваться как вымогательство. Могу вас уверить, что почти все владельцы сайтов, получающие такой непрошеный совет, не задумаются о вашей пользе и не захотят вас нанимать. Они увидят в вас врага и передадут дело адвокатам.

Остальная часть книги посвящена описанию конкретных типов взлома, методов проникновения и способов противостояния им со стороны специалистов по ИБ. Если вы хотите зарабатывать на жизнь хакерством или бороться с хакерами, следует понять их методологию. Люди, упомянутые здесь, – гиганты в своей области, и вы можете многому у них научиться. Думаю, лучше всего начать с Брюса Шнайера, речь о котором пойдет в следующей главе. Многие считают его отцом современной компьютерной криптографии.

# 3. Профиль: Брюс Шнайер

Брюс Шнайер обладает столь большим опытом и знаниями, что при его упоминании многие люди используют словосочетание «светило индустрии» или называют его «отцом современной компьютерной криптографии». Однако интерес Шнайера не ограничивается шифрами, он уже давно задается более глобальными вопросами о том, почему в сфере информационной безопасности за все эти десятилетия произошло так мало улучшений. Поскольку он имеет авторитетное мнение по широкому кругу вопросов, связанных с ИБ, его часто приглашают в качестве эксперта на национальные телевизионные шоу. Несколько раз он даже выступал перед Конгрессом Соединенных Штатов. Шнайер пишет книги и ведет блоги, и я всегда считал ознакомление с его работами получением неофициальной степени магистра в области информационной безопасности. Я и наполовину не был бы тем специалистом по ИБ, которым стал, без знаний, которые почерпнул у него. Он мой неофициальный наставник.

# Конец ознакомительного фрагмента.