Содержание

Предисловие

Меня зовут Ройс Дэвис, и я профессиональный хакер, член «красной команды», пентестер, атакующий специалист по безопасности – в этой отрасли нас называют разными именами. В течение последнего десятилетия я предоставлял профессиональные услуги по имитации состязательной защиты широкому кругу клиентов практически во всех сферах бизнеса, которые вы только можете себе представить. Все это время у меня не возникало никаких сомнений в том, какие сервисные компании больше всего заинтересованы в том, чтобы платить профессиональным хакерам за их работу. Я, конечно, говорю о *тесте на проникновение во внутреннюю сеть* (internal network penetration test, INPT).

INPT – это сложное корпоративное задание, которое можно изложить в нескольких предложениях. Злоумышленник (которого играете вы) сумел физически проникнуть в корпоративный офис, используя любой из многочисленных и весьма правдоподобных методов, которые намеренно не рассматриваются в этой книге. Что теперь? Имея только портативный компьютер с хакерскими инструментами и не зная заранее о сетевой инфраструктуре компании, злоумышленник как можно глубже проникает в корпоративную среду компании. Индивидуальные цели и задачи варьируются от проникновения к проникновению, от компании к компании. Тем не менее сценарий, при котором вы (злоумышленник) получаете полный контроль над сетью, является наиболее распространенной целью проведения INPT.

За свою карьеру я провел сотни таких мероприятий для сотен компаний, от малых предприятий с одним «ИТ-специалистом» до конгломератов из списка Fortune-10 с офисами на всех континентах.

Что меня больше всего удивило во время моей деятельности, так это то, насколько прост процесс управления сетью компании изнутри, независимо от специфики и размера компании или отраслевой вертикали. Не имеет значения, является ли целью банк в Южной Дакоте, компания по производству видеоигр в Калифорнии, химический завод в Сингапуре или кол-центр в Лондоне. Все сети настроены более или менее одинаково. Конечно, отдельные технологии, оборудование и приложения

сильно различаются от организации к организации, но сценарии проникновения в целом одинаковы.

В компаниях есть сотрудники, использующие компьютерные устройства для доступа к централизованным серверам, на которых размещены документы и внутренние приложения. Каждый сотрудник имеет учетные данные, определяющие его права доступа к обработке запросов, транзакций и информации, которые в конечном итоге помогают компании функционировать и зарабатывать деньги. Независимо от того, какова моя цель в роли злоумышленника, мой метод обнаружения сетевых хостов, перечисления их прослушивающих служб (их *поверхность атаки*) и обнаружения слабых мест безопасности в механизмах аутентификации, конфигурации и обновлениях этих систем не меняется от клиента к клиенту.

Опираясь на опыт многолетней работы и успешных взломов сетей, я решил задокументировать свою методологию выполнения INPT и предоставить исчерпывающий набор практических инструкций, которым новичок в этой отрасли может пошагово следовать, чтобы провести надлежащий тест на проникновение. Лично я считаю, что аналогичные по наполнению ресурсы не существуют или, по крайней мере, не существовали в то время, когда я писал эту книгу.

Существует множество программ профессионального обучения и сертификации, которые предлагают студентам широкий спектр ценных навыков и методов. Я нанял и обучил много стажеров, но даже после окончания самых сложных и уважаемых учебных курсов многие студенты на самом деле не знают, как выполнить тест на проникновение. Если я скажу им: «Ребята, у вас проникновение в сеть XYZ, которое начнется в следующий понедельник; вот техническое задание», – они уставятся на меня широко распахнутыми испуганными глазами, как олень в свете фар.

Мои обязательства перед вами относительно этой книги просты. Если кто-то поручит вам выполнить настоящий пентест, нацеленный на реальную сеть с сотнями или даже тысячами компьютерных систем, и если это проникновение будет более или менее похоже на то, что я позже назову «типичным» INPT, то вы можете выполнить поручение, пошагово следуя инструкциям, изложенным в этой книге, даже если вы раньше не делали ничего подобного.

Если вы хакер или компьютерный гик, читающий книгу просто из любви к предмету, вы обязательно зададите вопросы наподобие «А что насчет взлома беспроводных сетей?», «Почему вы не рассказываете про обход антивирусов?» и «Где глава о переполнении буфера?». Так вот, я хочу сказать вам, что в *профессиональном* мире услуг по имитации проникновения компании нанимают людей для выполнения *конкретных* задач. Заказы без ограничений, когда разрешено делать все, что угодно, как бы захватывающе это ни звучало, случаются редко (если вообще когда-либо случаются).

Эта книга, вместо того чтобы вкратце касаться каждой темы, связанной с этическим взломом, представляет собой руководство для проведения полного цикла INPT. В ней есть все необходимое для успешного про-

ведения наиболее распространенного типа вторжения в сеть, которое вас попросят выполнить, если вы начнете карьеру в сфере профессионального пентестинга.

Когда вы закончите читать эту книгу и выполните лабораторные упражнения, вы овладеете навыком, за выполнение которого компании платят сотрудникам начального уровня шестизначную зарплату. По моему личному мнению, другие публикации в этой области стремятся охватить слишком широкий спектр, и в результате они могут посвятить только одну главу каждой теме. В этой книге вы сосредоточитесь на одной задаче: захвате контроля над корпоративной сетью. Я надеюсь, что вы готовы начать, потому что вы многому научитесь, и я думаю, вы будете удивлены тем, на что вы способны, когда дойдете до конца последней главы. Удачи!

О чем эта книга

Перед вами полное поэтапное руководство по проведению типичного теста на проникновение во внутреннюю сеть (INPT). В книге описана пошаговая методология, которую автор использовал для проведения сотен INPT для компаний любого размера. Она служит не столько концептуальным введением в теории и идеи, сколько практическим пособием, которое читатели с небольшим опытом или совсем без опыта могут использовать на протяжении всего процесса.

Кому следует прочитать эту книгу

Эта книга написана в первую очередь для потенциальных пентестеров и этичных хакеров. Тем не менее эту книгу должен прочитать любой, кто занимается проектированием, разработкой или реализацией систем, приложений и инфраструктуры.

Как организована эта книга: краткое содержание

Эта книга разделена на четыре части, каждая из которых посвящена одному из четырех этапов проведения типичного INPT. Книгу следует читать по порядку от начала до конца, поскольку каждый этап рабочего процесса INPT опирается на результаты предыдущего.

Этап 1 представляет собой сбор общей информации INPT, которая дает вам подробное представление о поверхности атаки вашей цели:

- *глава 2* знакомит вас с процессом обнаружения сетевых хостов в пределах заданного диапазона IP-адресов;
- *глава 3* объясняет, как составить перечень сетевых служб, прослушивающих хосты, обнаруженные в предыдущей главе;
- *глава 4* описывает несколько методов выявления уязвимостей аутентификации, настроек и обновлений в сетевых службах.

Этап 2 представляет собой переход к целенаправленному проникновению, где ваша задача – получить несанкционированный доступ

к скомпрометированным целям с помощью слабых мест безопасности или *уязвимостей*, выявленных на предыдущем этапе:

- *глава 5* демонстрирует, как взломать несколько уязвимых веб-приложений, в частности Jenkins и Apache Tomcat;
- *глава 6* описывает, как атаковать и взломать уязвимый сервер базы данных, а также получить конфиденциальные файлы из неинтерактивных командных оболочек;
- *глава 7* исследует долгожданную тему использования отсутствующего обновления безопасности Microsoft и использования полезной нагрузки Metasploit meterpreter с открытым исходным кодом.

Этап 3 описывает *постэксплуатацию* – действия злоумышленника после того, как он скомпрометировал уязвимую цель. В нем представлены три основные концепции – обеспечение надежного повторного входа, сбор учетных данных и горизонтальный переход к новым доступным системам (уровень 2):

- *глава 8* посвящена постэксплуатации в системах на базе Windows;
- в *главе 9* рассказывается о различных методах постэксплуатации для целей на базе Linux/UNIX;
- в *главе 10* описан процесс повышения прав администратора домена и безопасного извлечения «бриллиантов короны» из контроллера домена Windows.

Этап 4 завершает проникновение фазами очистки оставленных следов и написания отчета:

- в *главе 11* показано, как вернуться к началу и удалить ненужные, потенциально опасные артефакты, возникшие в результате ваших действий по тестированию на проникновение;
- в *главе 12* рассказано о восьми компонентах качественного результата тестирования на проникновение.

Опытные пентестеры могут предпочесть перейти к конкретным интересующим их разделам, таким как постэксплуатация Linux/UNIX или атака на уязвимые серверы баз данных. Однако если вы новичок в тестировании на проникновение в сеть, вам обязательно следует прочитать главы последовательно от начала до конца.

Содержимое листингов

Эта книга содержит большой объем вывода терминала командной строки, как в виде пронумерованных листингов, так и в виде обычного текста. В обоих случаях исходный код отформатирован `шрифтом фиксированной ширины`, чтобы отделить его от обычного текста.

Дискуссионный форум liveBook

Приобретение оригинала этой книги включает в себя бесплатный доступ к частному веб-форуму Manning Publications, где вы можете комменти-

ровать книгу, задавать технические вопросы и получать помощь от автора и других пользователей. Чтобы получить доступ к форуму, перейдите по ссылке https://livebook.manning.com/#!/book/the-art-of-network-penetration-testing/. Вы также можете узнать больше о форумах Manning и правилах поведения на https://livebook.manning.com/#!/discussion.

Обязательство издательства Manning перед читателями состоит в том, чтобы обеспечить место, где может состояться содержательный диалог между отдельными читателями, а также между читателями и автором. Это не является обязательством какого-либо гарантированного сервиса со стороны автора, чей вклад в форум остается добровольным (и неоплачиваемым). Мы предлагаем вам попробовать задать автору несколько сложных вопросов, чтобы мотивировать его! Форум и архивы предыдущих обсуждений будут доступны на веб-сайте Manning до тех пор, пока книга не снята с публикации.

Отзывы и пожелания

Мы всегда рады отзывам наших читателей. Расскажите нам, что вы думаете об этой книге, – что понравилось или, может быть, не понравилось. Отзывы важны для нас, чтобы выпускать книги, которые будут для вас максимально полезны.

Вы можете написать отзыв на нашем сайте www.dmkpress.com, зайдя на страницу книги и оставив комментарий в разделе «Отзывы и рецензии». Также можно послать письмо главному редактору по адресу dmkpress@gmail.com; при этом укажите название книги в теме письма.

Если вы являетесь экспертом в какой-либо области и заинтересованы в написании новой книги, заполните форму на нашем сайте по адресу http://dmkpress.com/authors/publish_book/ или напишите в издательство по адресу dmkpress@gmail.com.

Скачивание исходного кода примеров

Скачать файлы с дополнительной информацией для книг издательства «ДМК Пресс» можно на сайте www.dmkpress.com или www.дмк.рф на странице с описанием соответствующей книги.

Список опечаток

Хотя мы приняли все возможные меры для того, чтобы обеспечить высокое качество наших текстов, ошибки все равно случаются. Если вы найдете ошибку в одной из наших книг, мы будем очень благодарны, если вы сообщите о ней главному редактору по адресу dmkpress@gmail.com. Сделав это, вы избавите других читателей от недопонимания и поможете нам улучшить последующие издания этой книги.

Нарушение авторских прав

Пиратство в интернете по-прежнему остается насущной проблемой. Издательства «ДМК Пресс» и Manning Publications очень серьезно относятся к вопросам защиты авторских прав и лицензирования. Если вы столкнетесь в интернете с незаконной публикацией какой-либо из наших книг, пожалуйста, пришлите нам ссылку на интернет-ресурс, чтобы мы могли применить санкции.

Ссылку на подозрительные материалы можно прислать по адресу электронной почты dmkpress@gmail.com.

Мы высоко ценим любую помощь по защите наших авторов, благодаря которой мы можем предоставлять вам качественные материалы.

Об авторе

Ройс Дэвис – профессиональный этичный хакер и пентестер, специализирующийся на тестировании проникновения в сеть и имитации корпоративных атак. Он более десяти лет помогает клиентам защитить свои сетевые среды и представляет свои исследования, методы и инструменты на конференциях по кибербезопасности на всей территории Соединенных Штатов. Он внес свой вклад в создание инструментов и фреймворков для тестирования безопасности с открытым исходным кодом и является соучредителем образовательного онлайн-ресурса PentestGeek.com, предназначенного для обучения методикам этичного взлома.

Изображение на обложке

Рисунок на обложке этой книги называется *Habit d'un Morlaque d'Uglin en Croatie* – «Одежда человека из племени морлак с острова Углян в Хорватии». Иллюстрация взята из коллекции костюмов разных стран Жака Грассе де Сен-Совера (1757–1810) под названием *Costumes de Différents Pays* («Костюмы разных стран»), изданной во Франции в 1797 году. Каждая иллюстрация тщательно нарисована и раскрашена вручную. Богатое разнообразие коллекции Грассе де Сен-Совера ярко напоминает нам о том, насколько обособленными в культурном отношении города и регионы мира были всего 200 лет назад. Изолированные друг от друга люди говорили на разных диалектах и языках. При встрече можно было легко определить место проживания и род занятий человека по его одежде.

С тех пор наша манера одеваться изменилась, а культурное разнообразие регионов, столь богатое в те времена, исчезло. Сейчас трудно отличить жителей разных континентов, не говоря уже о разных городах, регионах или странах. Возможно, мы обменяли культурное разнообразие на более разнообразную личную жизнь – конечно, по большей части в техническом плане.

В то время когда трудно отличить одну компьютерную книгу от другой, издательство Manning и его авторы стараются украсить обложки книг картинами Грассе де Сен-Совера, основанными на богатом разнообразии региональной жизни два столетия назад.

1 Тестирование сетей на проникновение

Краткое содержание главы:

- утечки корпоративных данных;
- моделирование состязательных атак;
- когда организациям не нужен тест на проникновение;
- четыре этапа теста на проникновение во внутреннюю сеть.

Сегодня мы все так или иначе обитаем в цифровом виде в сетевых компьютерных облаках. Ваши налоговые декларации, фотографии ваших детей, которые вы делаете на мобильный телефон, местоположения, даты и время всех мест, куда вы направлялись с помощью GPS, – все они хранятся там и готовы для похищения любым злоумышленником, которому хватит опыта и упорства.

Обычное предприятие среднего размера имеет в 10 раз (как минимум) больше подключенных устройств, работающих в его сети, чем сотрудников, которые используют эти устройства для выполнения повседневных бизнес-операций. Возможно, сначала данный факт не вызовет у вас тревогу, учитывая, насколько глубоко интегрированы компьютерные системы в наше общество, наше существование и как от них зависит наше выживание.

Если предположить, что вы живете на планете Земля – а у нас есть достоверные сведения, что это так, – с вероятностью выше среднего вы имеете:

- учетную запись электронной почты (или четыре);
- аккаунт в социальной сети (или семь);

- как минимум два десятка комбинаций имени пользователя и пароля, которые вам приходится бережно хранить, чтобы иметь возможность входить на различные веб-сайты, мобильные приложения и облачные сервисы, необходимые для вашей ежедневной продуктивной работы.

Независимо от того, оплачиваете ли вы счета, покупаете продукты, бронируете номер в отеле или ищете что-нибудь в интернете, вам необходимо создать профиль учетной записи, содержащий как минимум имя пользователя, юридическое имя и адрес электронной почты. Часто вас просят предоставить дополнительную личную информацию, например такую:

- почтовый адрес;
- номер телефона;
- девичья фамилия матери;
- номер банковского счета;
- данные кредитной карты.

Мы все устали от этой рутины. Мы даже не утруждаем себя чтением всплывающих юридических соглашений, в которых говорится, что компании планируют делать с информацией, которую мы им предоставляем. Мы просто нажимаем «Я согласен» и поскорее переходим на страницу, которая нас заинтересовала, – чтобы посмотреть вирусное видео про кошек или заказать очаровательную кофейную кружку с саркастической шуткой о том, как вы устали.

Ни у кого нет времени читать всю эту юридическую чушь, особенно когда срок действия бесплатной доставки истекает всего через 10 минут. (Постойте, что это? Они предлагают программу вознаграждений! Мне нужно срочно создать новую учетную запись!) Возможно, даже более тревожным, чем частота, с которой мы раскрываем случайным интернет-компаниям нашу личную информацию, является тот факт, что большинство из нас наивно полагают, будто корпорации, с которыми мы взаимодействуем, принимают надлежащие меры предосторожности для безопасного и надежного хранения нашей конфиденциальной информации. Вы не представляете, насколько это далеко от реальности.

1.1 Утечки корпоративных данных

Если вы не жили в горной пещере последние двадцать лет, то, полагаю, вы много слышали об утечках корпоративных данных. Только в первой половине 2018 года было выявлено 943 нарушения согласно отчету корпорации Gemalto, которая специализируется на средствах контроля доступа и защиты данных (http://mng.bz/YxRz). С точки зрения публикаций в СМИ, большинство нарушений, как правило, выглядят примерно так: «Транснациональная корпорация XYZ только что сообщила, что неизвестное количество конфиденциальных учетных записей клиентов было украдено неизвестной группой злоумышленников, которым удалось

проникнуть в сеть компании, используя неизвестную уязвимость или способ атаки». Полный масштаб взлома, включая все, что похитили хакеры, – как вы уже догадались – неизвестен. Затем мы наблюдаем падение стоимости акций, поток гневных твитов, громкие заголовки в газетах и заявление об отставке генерального директора, а также нескольких членов наблюдательного совета. Генеральный директор уверяет нас, что отставка не имеет ничего общего с утечкой персональных данных; он уже давно собирался уйти на заслуженный отдых. Конечно, кто-то должен взять на себя официальную вину, но мы ведь понимаем, что главный директор по информационной безопасности (CISO), который много лет безупречно служил компании, не может уйти в отставку; вместо этого увольняют и публично забивают камнями в социальных сетях подвернувшихся под руку менеджеров, гарантируя, что, как принято говорить в Голливуде, они больше никогда не войдут в этот город.

1.2 Как работают хакеры

Почему взломы происходят так часто? Неужели компании настолько плохо умеют действовать по правилам, когда дело касается информационной безопасности и защиты наших данных? И да, и нет.

Неудобная правда заключается в том, что колода карт в этой игре оказывается подтасованной в пользу киберзлоумышленников. Помните мое предыдущее замечание о количестве сетевых устройств, которые предприятия постоянно подключают к своей инфраструктуре? Это значительно увеличивает возможность атаки, или *ландшафт угроз* компании.

1.2.1 Что делает защитник

Позвольте мне пояснить. Предположим, ваша работа – защищать организацию от киберугроз. Вам необходимо уделить внимание каждому ноутбуку, настольному компьютеру, смартфону, физическому серверу, виртуальному серверу, маршрутизатору, коммутатору и модной кофеварке, подключенной к вашей сети.

Затем вы должны убедиться, что каждое приложение, работающее на этих устройствах, правильно защищено с помощью надежных паролей (предпочтительно с двухфакторной аутентификацией) и настроено в соответствии с текущими стандартами и передовыми методами для каждого соответствующего устройства. Кроме того, вы должны своевременно применять все исправления безопасности и обновления, выпущенные отдельными поставщиками программного обеспечения, как только они становятся доступными. Однако, прежде чем сделать хоть малейшее движение в этом направлении, вы должны трижды проверить, не мешают ли обновления повседневной деятельности вашего бизнеса, иначе люди будут злиться на вас за попытку защитить компанию от хакеров.

Все перечисленное нужно делать постоянно для каждого устройства, имеющего IP-адрес в вашей сети. Так просто, правда?

1.2.2 Что делает злоумышленник

А теперь перейдем на темную сторону. Предположим, ваша задача – проникнуть в компанию, т. е. каким-то образом взломать сеть и получить несанкционированный доступ к системам или информации с ограниченным доступом. Вам достаточно найти только одну систему, которая осталась без внимания защитника; только одно устройство, которое пропустило исправление или содержит пароль по умолчанию или легкоугадываемый пароль; единственное неправильно настроенное приложение, развернутое в спешке, чтобы уложиться в невыполнимые сроки для бизнеса, обусловленные целевыми показателями прибыли, поэтому небезопасная настройка конфигурации (которая по умолчанию задана поставщиком) осталась без внимания. Это все, что нужно для проникновения, даже если цель проделала безупречную работу по контролю за каждым узлом в сети. В компаниях постоянно работают команды, которым нужно срочно внести какие-то изменения.

Если вы сейчас подумали, что это несправедливо или что это слишком сложно для защитников и слишком легко для атакующих, значит, вы поняли истинное положение дел. Итак, что должны делать организации, чтобы избежать взлома? Вот тут-то и пригодится *тестирование на проникновение*, или *пентестинг* (сокращение от penetration testing).

1.3 Моделирование состязательной атаки: тестирование на проникновение

Один из наиболее эффективных способов выявления слабых мест в системе безопасности до того, как они приведут к взлому, – это нанять профессионального «злоумышленника», или *пентестера*, чтобы смоделировать атаку на инфраструктуру компании. Пентестер должен предпринять все доступные действия, чтобы имитировать настоящего злоумышленника, в некоторых случаях действуя в обстановке полной секретности, незаметно для ИТ-отдела и службы внутренней безопасности организации, пока не придет время опубликовать свой окончательный отчет. В этой книге я буду называть данный тип наступательных действий по обеспечению безопасности просто *тестом на проникновение*.

Конкретный объем и способы выполнения теста могут отличаться в зависимости от потребностей организации, заказывающей оценку (клиента), а также от возможностей и предложений услуг консалтинговой фирмы, проводящей тест. Воздействие пентестера может быть сосредоточено на веб-приложениях и мобильных приложениях, сетевой инфраструктуре, беспроводных устройствах, физических офисах и всем остальном, что вы можете придумать для атаки. Упор можно сделать на скрытность, пытаясь остаться незамеченным, или на сбор информации об уязвимостях как можно большего количества хостов за короткое время. Пентестеры могут использовать человеческий фактор (социальная

инженерия), специально разработанный код эксплойта или даже копаться в мусорных баках клиента в поисках паролей для доступа. Все зависит от масштаба планируемого вторжения. Однако наиболее распространенный тип вторжения – тот, который я выполнял для сотен компаний за последнее десятилетие. Я называю его *тестом на проникновение во внутреннюю сеть* (internal network penetration test, INPT). Этот тип проникновения имитирует наиболее опасный тип злоумышленника для любой организации: злонамеренного или иным образом скомпрометированного инсайдера – человека, имеющего доступ к внутренней сети организации.

ОПРЕДЕЛЕНИЕ *Злоумышленник* – это обобщенное название лица, осуществляющего ту или иную атаку. Это определение относится к любому, кто пытается нанести вред информационной инфраструктуре организации.

Планируя INPT, вы предполагаете, что злоумышленник смог успешно получить физический доступ в корпоративный офис или, возможно, получил удаленный доступ к рабочей станции сотрудника с помощью фишинга. Также возможно, что злоумышленник посетил офис в нерабочее время, представившись охранником, или в течение дня, представившись торговцем либо доставщиком цветов. Возможно, злоумышленник – действующий сотрудник компании, который прошел со своим пропуском через парадную дверь.

Существует бесчисленное множество способов получить физический доступ в офис, которые не вызовут особых затруднений. Во многих случаях злоумышленнику просто нужно пройти через главный вход и бродить по коридорам, вежливо улыбаясь любому, кто проходит мимо, и делая вид, что он разговаривает по мобильному телефону, пока он не обнаружит укромный уголок, где можно подключиться к розетке локальной сети. Профессиональные компании, предлагающие услуги высококлассного тестирования на проникновение (пентест), обычно выставляют счета от 150 до 500 долларов в час. В результате для клиента, заказавшего тест на проникновение, зачастую дешевле пропустить эту творческую часть вторжения и с самого начала предоставить злоумышленнику физический доступ к внутренней подсети.

Так или иначе, злоумышленнику удалось получить доступ к корпоративной сети. Что он может сделать? Что он видит? Обычный сценарий вторжения предполагает, что злоумышленник ничего не знает о внутренней сети и не имеет специального доступа или учетных данных. Все, что у него есть, – это доступ к сети, и обычно этого ему достаточно.

1.3.1 Типичные этапы вторжения

Типичное тестовое вторжение состоит из четырех этапов, выполняемых по порядку, как показано на рис. 1.1. Отдельные названия каждого этапа – это не догма, их можно выбирать. Одна компания-пентестер может использовать термин «разведка» вместо сбора информации. Другая ком-

пания может использовать термин «доклад» вместо документации. Независимо от того, как называется каждый этап, большинство экспертов в нашей отрасли соглашаются с перечнем задач пентестера на каждом этапе.

Рис. 1.1 Четыре этапа теста на проникновение в сеть

- *Этап 1* – сбор информации:
  a) составьте карту сети;
  b) определите возможные цели;
  c) перечислите слабые места в службах, работающих на этих целях.
- *Этап 2* – целенаправленное проникновение:
  a) взломайте уязвимые сервисы (получите к ним несанкционированный доступ).
- *Этап 3* – постэксплуатация и повышение привилегий:
  a) определите информацию о скомпрометированных системах, которая может быть использована для дальнейшего доступа (закрепления в системе);
  b) поднимите привилегии до самого высокого уровня доступа в сети, фактически став системным администратором компании;
- *Этап 4* – документирование:
  a) соберите доказательства проникновения;
  b) составьте окончательный отчет.

После того как тестовая часть вторжения завершена, пентестер мысленно покидает позиции злоумышленника и превращается в консультанта. Остальную часть вторжения он посвящает составлению максимально подробного отчета. Этот отчет содержит детальное описание

всех способов, которыми удалось взломать сеть и обойти меры безопасности, а также предложение мер, которые компания может предпринять, чтобы закрыть эти выявленные бреши и гарантировать, что они больше не будут использованы кем-либо еще. В 9 из 10 случаев этот процесс занимает в среднем около 40 часов, но необходимое время может меняться в зависимости от размера организации.

1.4 Когда тест на проникновение наименее эффективен

Наверняка вы слышали известную поговорку: «Если у вас в руках молоток, все вокруг кажется гвоздями». Оказывается, это высказывание можно применить практически к любой профессии. Хирург хочет разрезать пациента, фармацевт хочет выписать ему таблетки, а пентестер хочет взломать вашу сеть. Но действительно ли всем организациям нужен тест на проникновение?

На самом деле ответ на этот вопрос зависит от уровня информационной безопасности компании. Я не могу сказать вам точно, сколько раз мне удавалось перехватить управление внутренней сетью компании в первый же день теста на проникновение, но количество таких компаний исчисляется сотнями. Конечно, мне хотелось бы сказать, что это получилось благодаря моим суперхакерским навыкам или потому, что я такой крутой, но это было бы грубым преувеличением.

Мои успехи гораздо больше связаны с чрезвычайно распространенной ситуацией: незрелая организация, которая не озаботилась даже базовыми требованиями безопасности, заказывает продвинутый тест на проникновение, хотя ей следовало бы начать с простой оценки уязвимости или моделирования угроз высокого уровня и анализа инфраструктуры. Нет смысла проводить тщательный тест на проникновение через защитные барьеры, если в безопасности вашей инфраструктуры зияют дыры, которые может обнаружить даже новичок.

1.4.1 Доступные мишени

Злоумышленники часто ищут путь наименьшего сопротивления и пытаются найти легкие пути в сеть, прежде чем выкатить на позицию большие пушки и взломать проприетарное программное обеспечение или разработать собственный код эксплойта нулевого дня. По правде говоря, средний пентестер обычно не умеет делать подобные вещи, потому что у него никогда не возникало потребности в этих навыках. Нет необходимости усложнять простые задачи, когда в большинстве корпораций можно найти гораздо более легкие пути. Мы называем эти простые способы *низко висящими фруктами* (low-hanging fruit, LHF), или *доступными мишенями*. В качестве примеров подобных мишеней можно назвать следующие уязвимости:

- пароли/конфигурации по умолчанию;
- одинаковые учетные данные в нескольких системах;
- наличие прав локального администратора у всех пользователей;
- отсутствующие патчи общедоступных эксплойтов.

Доступных мишеней гораздо больше, но эти четыре чрезвычайно распространены и чрезвычайно опасны. Однако следует отметить, что большинство векторов LHF-атак легко устранимы своими силами. Вы должны научиться соблюдать базовые принципы безопасности, прежде чем нанимать профессионального хакера для атаки на вашу сетевую инфраструктуру.

Организации со значительным количеством LHF-систем в своей сети не должны расходовать средства на оплату комплексного теста на проникновение. Было бы лучше потратить это время и деньги на то, чтобы сосредоточиться на базовых концепциях безопасности, таких как надежные учетные данные во всех подсистемах, регулярное обновление программного обеспечения, укрепление и развертывание системы, а также каталогизация активов.

1.4.2 Когда компании действительно нужен тест на проникновение?

Если компания задается вопросом, следует ли проводить тест на проникновение, я советую честно ответить на следующие вопросы. Начните с простых ответов «да/нет». Затем каждый ответ «да» компания должна подкрепить утверждением «Да, это обеспечено за счет процесса/процедуры/приложения XYZ, за которое отвечает сотрудник ABC». Итак, попробуйте ответить на следующие вопросы:

1. Ведем ли мы актуальные записи о каждом IP-адресе и DNS-имени в сети?
2. Есть ли у нас регламент установки исправлений для всех операционных систем и сторонних приложений, работающих в сети?
3. Используем ли мы коммерческие инструменты поиска уязвимостей для выполнения планового сканирования сети?
4. Удалили ли мы права локального администратора на всех ноутбуках сотрудников?
5. Требуем ли мы и обеспечиваем ли использование надежных паролей для всех учетных записей во всех системах?
6. Используем ли мы везде многофакторную аутентификацию?

Если ваша компания не может однозначно ответить «да» на все эти вопросы, то у квалифицированного пентестера, вероятно, не возникнет проблем со взломом раковины и извлечением жемчужины вашей организации. Я не говорю, что в таком случае вам совершенно незачем покупать тест на проникновение, просто вы должны ожидать болезненных результатов.

Ваш заказ может показаться пентестерам забавным; они могут даже хвастаться своим друзьям или коллегам тем, как легко они проникли

в вашу сеть. Но настоящая проблема в том, что такое тестирование будет бесполезным для вашей организации. Это подобно тому, как если бы человек никогда не занимался спортом или не придерживался здоровой диеты, а затем нанял тренера по фитнесу, чтобы тот посмотрел на его тело оценивающим взглядом и сказал: «Вы в плохой физической форме. С вас 10 000 долларов».

1.5 Проведение теста на проникновение в сеть

Итак, вы ответили на все вопросы и определили, что вашей организации действительно нужны услуги пентестера. Хорошо! Что дальше? До сих пор я обсуждал тестирование на проникновение как услугу, за которую вы обычно платите стороннему консультанту. Однако все больше и больше организаций создают собственные «красные команды» для регулярного проведения таких тестовых вторжений.

> **ОПРЕДЕЛЕНИЕ** *Красная команда* – специализированное подразделение отдела собственной безопасности организации, полностью сосредоточенное на учениях по обеспечению безопасности и имитации состязательных атак. Кроме того, термин «красная команда» часто используется для описания конкретного типа вторжения, которое считается максимально реалистичным, имитирует продвинутых злоумышленников и использует целенаправленный подход, а не методы, основанные на широте охвата.

Я могу предположить, что вы получили или надеетесь получить должность, которая потребует от вас проведения теста на проникновение для компании, в которой вы работаете. Возможно, вы уже провели несколько тестов, но чувствуете, что вам не помешают дополнительные знания и опыт.

Мое намерение при написании этой книги – предоставить вам руководство «от первого до последнего шага», которое вы можете использовать для проведения тщательного теста на проникновение, нацеленного на вашу компанию или любую другую организацию, от которой вы получили письменное разрешение на это.

Вы изучите именно ту методику, которую я выработал за десятилетия своей карьеры и использовал для успешного и безопасного выполнения сотен тестов на проникновение в сеть, нацеленных на многие крупнейшие компании мира. Этот процесс выполнения контролируемых, смоделированных кибератак, имитирующих реальные сценарии внутреннего взлома, хорошо зарекомендовал себя при выявлении критических слабых мест в современных корпоративных сетях любого уровня сложности. Прочитав эту книгу и выполнив предложенные упражнения, вы можете быть уверены, что сумеете выполнить контролируемое вторжение в сеть независимо от размера или рода деятельности бизнеса, который вы атакуете. Вы освоите четыре этапа моей методики INPT, используя вирту-

альную сеть воображаемой корпорации Capsulecorp, которую я создал в качестве дополнения к этой книге. Каждый из четырех этапов разбит на несколько глав, демонстрирующих различные инструменты, методы и векторы атак, которые пентестеры часто используют во время реальных вторжений.

1.5.1 Этап 1: сбор информации

Представьте, что инженеры, разработавшие корпоративную сеть, сидят с вами за одним столом и демонстрируют вам огромную схему, из которой становится понятно строение зон и подсетей, расположение компонентов и почему сеть устроена именно так. Ваша задача на этапе сбора информации в ходе теста на проникновение заключается в том, чтобы максимально приблизиться к этому уровню понимания без помощи сетевых инженеров (рис. 1.2). Чем больше информации вы получите, тем выше ваши шансы обнаружить слабое место.

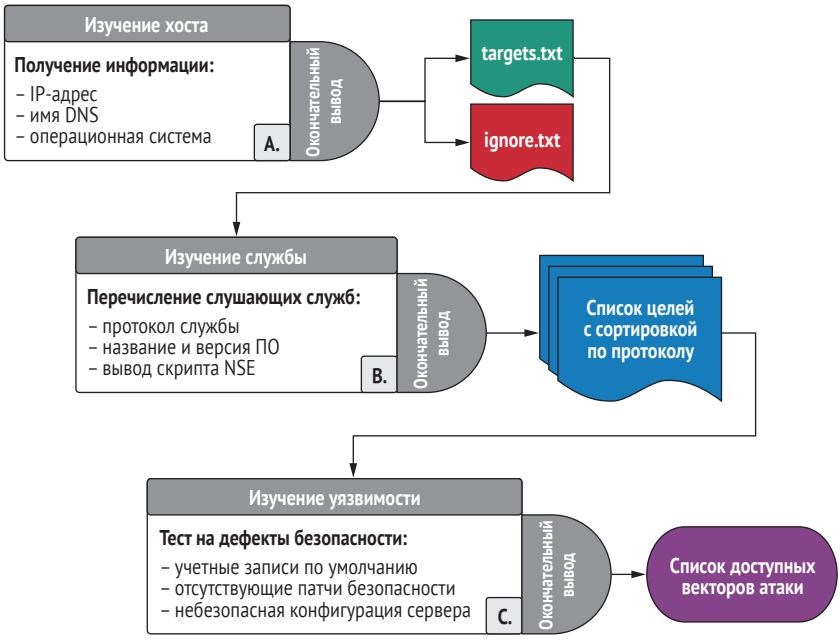

Рис. 1.2 Этап сбора информации

На протяжении первых нескольких глав этой книги я научу вас собирать всю информацию о целевой сети, необходимую вам для взлома. Вы узнаете, как определять топологию сети с помощью Nmap и обнаруживать работающие хосты внутри заданного диапазона IP-адресов. Вы также изучите службы прослушивания, которые работают на сетевых портах, привязанных к этим хостам. Затем вы научитесь опрашивать эти службы для получения конкретной информации, включая, помимо прочего, следующее:

- название и номер версии программного обеспечения;
- текущий патч и настройки конфигурации;
- баннеры работающих служб и HTTP-заголовки;
- механизмы аутентификации.

Вы также узнаете, как использовать, кроме Nmap, и другие мощные инструменты пентестинга с открытым исходным кодом, такие как фреймворк Metasploit CrackMapExec (CME), Impacket и многие другие, для дальнейшего сбора информации о сетевых целях, службах и уязвимостях, которой вы можете воспользоваться, чтобы получить несанкционированный доступ к защищенным областям целевой сети.

1.5.2 Этап 2: целенаправленное проникновение

Теперь начинается самое интересное! На втором этапе проникновения все семена, посеянные на предыдущем этапе, начинают приносить плоды (рис. 1.3). Теперь, когда вы определили векторы атак на уязвимости во всей сетевой среде, пришло время скомпрометировать эти хосты и начать контролировать сеть изнутри.

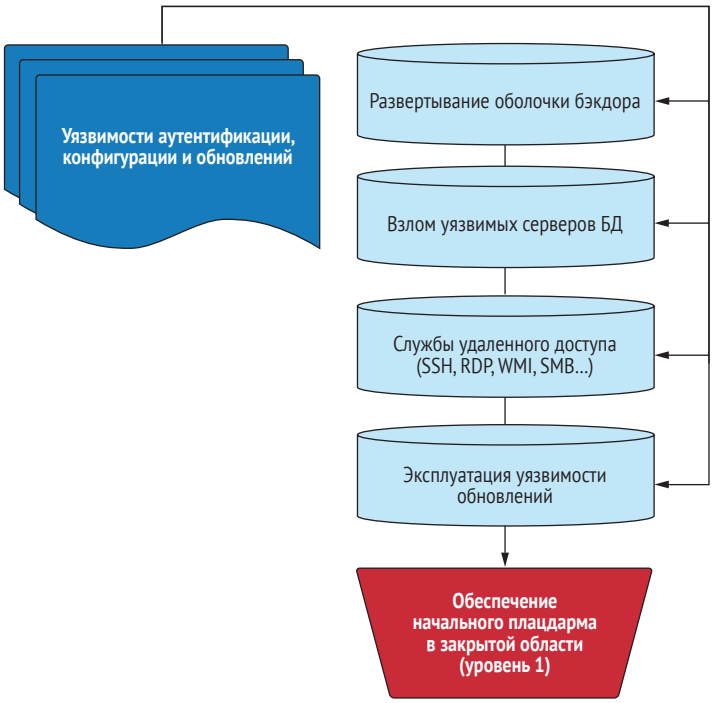

Рис. 1.3 Этап целенаправленного проникновения

В этом разделе книги вы познакомитесь с несколькими типами атак, которые приведут к возможности *удаленного выполнения кода* (remote code execution, RCE) на уязвимых целях. RCE означает, что вы можете

подключиться к терминалу командной строки и вводить своей скомпрометированной жертве команды, которые будут выполнены и отправят вам нужные данные по вашему запросу.

Я также научу вас развертывать пользовательские веб-оболочки с помощью уязвимых веб-приложений. К тому времени, когда вы закончите читать эту часть книги, вы успешно взломаете и получите контроль над серверами баз данных, веб-серверами, общими файловыми ресурсами, рабочими станциями и серверами, работающими в операционных системах Windows и Linux.

1.5.3 Этап 3: постэксплуатация и повышение привилегий

Один из моих любимых блогов по безопасности написан и поддерживается авторитетным пентестером по имени Карлос Перес (@Carlos_Perez). Заголовок вверху его страницы (https://www.darkoperator.com) идеально подходит для этого раздела книги: «Shell – это только начало».

После того как вы узнали, как взломать несколько уязвимых хостов в целевой среде, пора перейти на следующий уровень (рис. 1.4). Я предпочитаю называть эти начальные хосты, доступные через уязвимость прямого доступа, хостами уровня 1. Следующий этап вторжения – это достижение уровня 2.

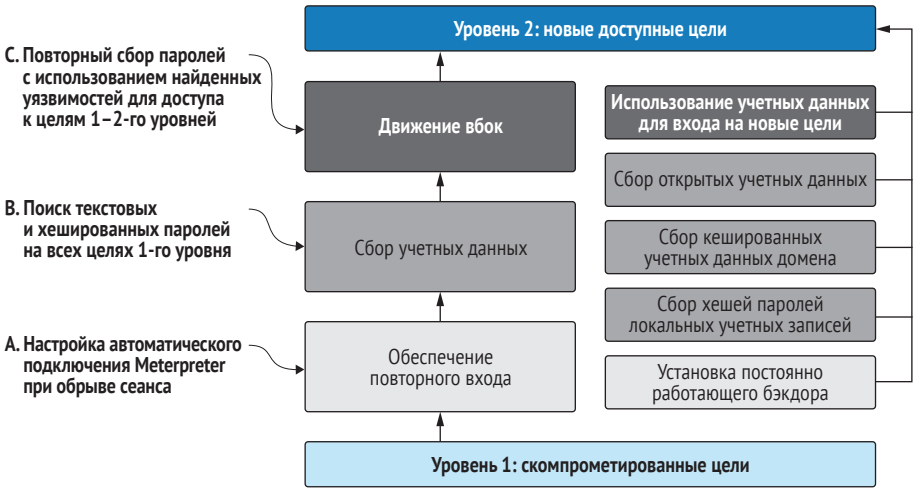

Рис. 1.4 Этап повышения привилегий

Хосты уровня 2 – это цели, которые изначально были недоступны на этапе сосредоточенного проникновения, потому что вы не могли определить какие-либо прямые уязвимости в их службах прослушивания. Но после того как вы получили доступ к целям уровня 1, вы обнаружили информацию или векторы, ранее недоступные для вас, что позволило вам скомпрометировать ранее недоступную систему уровня 2. Это называется *закреплением* (pivoting).

В этом разделе вы познакомитесь с методами постэксплуатации как для операционных систем на базе Windows, так и для Linux. Эти методы включают сбор открытого текста и хешированные учетные данные для перехода к соседним целям. Вы попрактикуетесь в повышении прав пользователей, не являющихся администраторами, до прав администратора на скомпрометированных хостах. Я также научу вас некоторым полезным приемам, которые освоил за долгие годы поиска паролей внутри скрытых файлов и папок, которые известны тем, что хранят конфиденциальную информацию. Кроме того, вы узнаете несколько различных методов получения учетной записи администратора домена (суперпользователя в сети Windows Active Directory).

К тому времени, когда вы закончите с этим разделом книги, вы поймете, почему мы говорим в этой индустрии, что вам нужен только один скомпрометированный хост, чтобы вы могли распространяться по сети, как лесной пожар, и в конечном итоге захватывать ключи от королевства.

1.5.4 Этап 4: документирование

В начале своей карьеры я понял, что нанять профессиональную консалтинговую фирму для проведения теста на проникновение в сеть – все равно что купить PDF-документ за 20 000 долларов. Без отчета тест на проникновение ничего не значит. Вы вторглись в сеть, обнаружили кучу дыр в их безопасности и максимально повысили свои права доступа. Какую пользу это приносит целевой организации? По правде говоря, никакую, если вы не предоставите подробную документацию, показывающую, как именно вам это удалось и что организация должна сделать, чтобы гарантировать, что вы (или кто-то другой) не сможете сделать это снова (рис. 1.5).

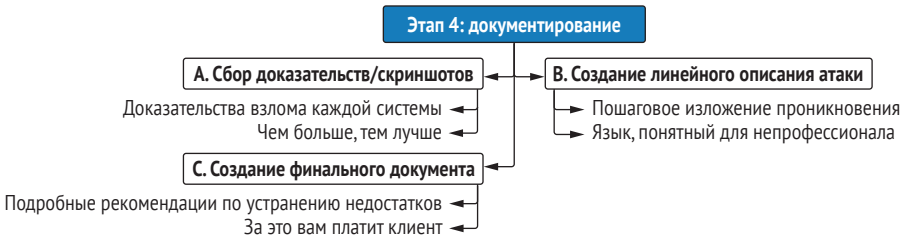

Рис. 1.5 Этап документирования

Я написал сотни отчетов по результатам пентеста, и мне пришлось усвоить – иногда на собственном горьком опыте, – что клиенты хотят видеть в отчете. Я также пришел к выводу, что поскольку они платят тысячи долларов за чтение отчета, неплохо было бы убедиться, что они достаточно впечатлены.

Помимо рассказа о том, что именно нужно включить в результат пентеста, я также поделюсь некоторыми выработанными за многие годы приемами повышения эффективности, которые сохранили мне тысячи рабо-

чих часов моего времени и дали возможность наслаждаться успешными взломами, вместо того чтобы смотреть в редактор документов Word.

Что отличает эту книгу от других изданий про пентестинг?

Глядя на оглавление этой книги, вы можете спросить, почему в ней отсутствуют темы, которые вы видели в других книгах подобного рода: социальная инженерия, обход антивирусного программного обеспечения, взлом беспроводной сети, тестирование мобильных и веб-приложений, взлом замков – я мог бы продолжить, но вы и так поняли. На самом деле все эти темы заслуживают отдельной книги, и рассмотрение их в одной главе не дает читателю должный объем информации, доступной по каждой из них.

Цель этой книги – вооружить вас инструментами, необходимыми для проведения типичного теста на проникновение во внутреннюю сеть (INTP). Такой тест продается каждой фирмой, предлагающей услугу пентестинга, и является наиболее распространенным типом проникновения, которое вы будете выполнять, если в конечном итоге сделаете карьеру профессионального пентестера.

Во время типичных INTP (где вы будете проводить не менее 80 % своего времени) вам не предложат (или даже запретят) воздействовать на беспроводную инфраструктуру вашего клиента, отправлять фишинговые сообщения электронной почты сотрудникам компании или пытаться проникнуть в ее физические центры обработки данных. У вас не будет времени или ресурсов для правильного создания пользовательских учетных данных, предназначенных для обхода конкретного решения EDR организации.

Вместо того чтобы поверхностно скользить по темам, которые являются интересными и определенно имеют ценность для других способов вторжения, в этой книге я предпочитаю сосредоточиться исключительно на рассматриваемой теме.

1.6 Настройка лабораторной среды

Тема тестирования на проникновение в сеть должна быть изучена на практике. Я написал эту книгу в формате, предполагающем, что у вас, читателя, есть доступ к корпоративной сети и разрешение на выполнение основных действий по тестированию на проникновение. Я понимаю, что у некоторых из вас может не быть такого доступа. Поэтому я создал проект с открытым исходным кодом под названием Capsulecorp Pentest, который будет служить лабораторной средой для проработки всего процесса INPT на протяжении оставшихся глав.

1.6.1 Проект Capsulecorp Pentest

Среда Capsulecorp Pentest – это виртуальная сеть, созданная с использованием VirtualBox, Vagrant и Ansible. Помимо уязвимых корпоративных

систем, она также поставляется с предварительно настроенной системой Ubuntu Linux, которую вы можете использовать в качестве атакующей машины. Скачайте репозиторий с веб-сайта книги (https://www.manning.com/books/the-art-of-network-Pentestration-testing) или GitHub (https://github.com/r3dy/caplecorp-pentest) и следуйте инструкциям по установке, прежде чем переходить к следующей главе.

1.7 Создание собственной виртуальной платформы для пентеста

Некоторые из вас предпочтут развернуть свою собственную систему с нуля. Я вас полностью понимаю и поддерживаю. Но если вы хотите создать свою собственную систему пентестинга, сначала обдумайте несколько вещей, прежде чем выбирать платформу операционной системы.

1.7.1 Начните с Linux

Как и большинство профессиональных пентестеров, для выполнения технических этапов проникновения я предпочитаю использовать операционную систему Linux. Это в первую очередь связано с парадоксом курицы и яйца, который я попытаюсь объяснить.

Большинство пентестеров используют Linux. Когда человек разрабатывает инструмент для облегчения своей работы, он делится им со всем миром, обычно через GitHub. Скорее всего, этот инструмент был разработан для Linux и – какое совпадение – лучше всего работает при запуске из системы Linux. По крайней мере, чтобы заставить его работать в Linux, требуется меньше головной боли и борьбы с зависимостями. Поэтому все больше и больше людей разрабатывают и выполняют свои тесты на проникновение на платформе Linux, чтобы иметь возможность использовать новейшие и лучшие из доступных инструментов. Как видите, можно сказать, что Linux – самый популярный выбор среди пентестеров, потому что это самый популярный выбор среди пентестеров, – и, следовательно, это рассуждение о приоритете курицы или яйца.

Однако есть веская причина, почему это произошло. До появления языка сценариев PowerShell от Microsoft только операционные системы на базе Linux/UNIX поставлялись с встроенной поддержкой программирования и выполнения сценариев для автоматизированных рабочих процессов. Вам не нужно было загружать и устанавливать большую громоздкую среду IDE, если вы хотели написать программу. Все, что вам нужно было сделать, – это открыть пустой файл в Vim или Vi (самых мощных текстовых редакторах на планете), написать код, а затем запустить его со своего терминала. Если вам интересно, какая связь между тестированием на проникновение и написанием кода, ответ прост: лень. Как и разработчики, пентестеры бывают ленивыми и не желают выпол-

нять повторяющиеся задачи; поэтому мы пишем код для автоматизации всего, что можем.

Есть и определенные политические причины для использования Linux, о которых я не буду подробно рассказывать, потому что я не политик. Я скажу, однако, что большинство пентестеров воображают себя хакерами. Хакеры – по крайней мере, традиционно – предпочитают программное обеспечение с открытым исходным кодом, которое можно бесплатно получить и настроить, в отличие от коммерческих приложений с закрытым исходным кодом, разработанных алчными корпорациями. Кто знает, что эти большие плохие компании спрятали в своих продуктах? Информация должна быть бесплатной, сражайтесь и побеждайте, взломайте систему … ну, вы поняли суть.

> **СОВЕТ** Linux – это операционная система, которую предпочитают большинство пентестеров. Некоторые из них написали по-настоящему мощные инструменты, которые лучше всего работают на платформе Linux. Если вы хотите провести тестирование на проникновение, вам также следует использовать Linux.

1.7.2 Проект Ubuntu

Здесь ключевую роль играют мои личные предпочтения: мне удобнее всего работать в Ubuntu Linux, производной от гораздо более старого Debian Linux. И это не эстетское мнение самоуверенного профессионала. Просто Ubuntu – это самая эффективная платформа из десятка или около того дистрибутивов, с которыми я экспериментировал на протяжении многих лет. Я не буду отговаривать вас от выбора другого дистрибутива, особенно если вы уже привыкли к чему-то другому. Но я рекомендую вам выбрать проект, который очень хорошо документирован и поддерживается обширным сообществом образованных пользователей. Ubuntu определенно соответствует этим критериям и превосходит их.

Выбор дистрибутива Linux очень похож на выбор языка программирования. Вы не найдете недостатка в стойких сторонниках, стоящих по горло в трясине и кричащих изо всех сил о причинах, по которым их лагерь лучше других. Но эти дебаты бессмысленны, потому что лучший язык программирования – это тот, который вы знаете лучше всего, и поэтому он может быть наиболее продуктивным. То же самое и с дистрибутивами Linux.

Что такое дистрибутив Linux?

В отличие от коммерческих операционных систем, таких как Microsoft Windows, Linux имеет открытый исходный код и свободно настраивается по вашему желанию. Как следствие, существуют сотни различных версий Linux, созданные отдельными лицами, группами или даже компаниями, у которых есть собственное видение того, как Linux должен выглядеть и работать. Эти версии называют дистрибутивами, сборками или иногда разновидностями (flavors), в зависимости от того, с кем вы разговариваете.

Главный компонент операционной системы Linux называется *ядром* (kernel), которое в большинстве версий остается нетронутым. Остальная часть операционной системы, однако, активно подвергается изменениям: диспетчер окон, диспетчер пакетов, среда оболочки и т. д.

1.7.3 Почему бы не использовать пентест-дистрибутив?

Возможно, вы слышали о Kali Linux, Black Arch или каком-либо другом специальном дистрибутиве Linux, предназначенном для тестирования на проникновение и этичного взлома. Не было бы проще просто загрузить один из них, вместо того чтобы создавать платформу с нуля? Как вам сказать… и да, и нет.

Несмотря на то что простота подготовки, несомненно, выглядит привлекательно, приобретя опыт работы в пентестинге, вы обнаружите, что эти предварительно сконфигурированные платформы склонны к раздуванию ненужными инструментами, которые никогда не используются. Это похоже на подготовку к ремонту квартиры своими руками. В большом хозяйственном магазине, таком как Home Depot, есть абсолютно все, что вам может когда-либо понадобиться, но конкретный ремонт, который вы планируете, каким бы сложным он ни был, требует всего дюжины или около того инструментов. Я хочу официально выразить свое уважение и восхищение тяжелой работой, проделанной различными разработчиками и волонтерами поддержки этих дистрибутивов.

Однако в какой-то момент вы неизбежно погуглите «Как делать XYZ в Linux», находясь прямо в процессе проникновения, и найдете действительно отличную статью или учебное пособие всего с четырьмя простыми командами, которые работают на Ubuntu, но не на Kali, хотя Kali основана на Ubuntu! Разумеется, вы можете углубиться в проблему, которая, конечно же, имеет простое решение, как только вы в ней разберетесь; но мне приходилось делать это так много раз, что я просто запускаю Ubuntu и устанавливаю то, что мне нужно, – и только то, что мне нужно, и это лучше всего подходит для меня. Правильно это или неправильно, но это *моя* философия.

Напоследок скажу вот что. Я придаю большое значение созданию вашей собственной среды не только для повышения вашей компетентности и навыков, но и для того, чтобы вы могли с уверенностью посмотреть в глаза своим клиентам и рассказать им обо всем, что работает в вашей системе, если они попросят вас. Клиенты часто опасаются тестирования на проникновение, потому что у них нет большого опыта на этот счет, поэтому они нередко проявляют осторожность, прежде чем позволить посторонним людям подключить подозрительное устройство к своей сети. Меня много раз просили описать все инструменты, которые я использую, и дать ссылки на документацию.

ПРИМЕЧАНИЕ Может быть, вы думаете: «Я все еще хочу использовать Kali». Это нормально. Большинство инструментов, описан-

ных в этой книге, изначально доступны в Kali Linux. В зависимости от вашего уровня подготовки может быть проще пойти по этому пути. Имейте в виду, что все упражнения и демонстрации в книге выполняются с использованием специально созданной машины Ubuntu, описанной в приложении А. Я полагаю, что вы можете следовать этой книге, используя Kali Linux, если вам так больше нравится.

При этом если вы предпочитаете создать свою собственную систему с нуля, вы можете воспользоваться приложением А, где я описал полную установку и конфигурацию. В противном случае, если вы просто хотите начать изучение того, как проводить INPT, вы можете загрузить и настроить среду Capsulecorp Pentest по ссылке GitHub в разделе 1.6.1. В любом случае сделайте свой выбор, настройте лабораторную среду, а затем начните проводить свой первый тест на проникновение, как сказано в главе 2.

1.8 Заключение

- Мир, каким мы его знаем, управляется сетевыми компьютерными системами.
- Компаниям становится все труднее управлять безопасностью своих компьютерных систем.
- Злоумышленникам достаточно найти только одну дыру в сети, чтобы открыть двери настежь.
- Учения по моделированию состязательных атак или тесты на проникновение – это активный подход к выявлению слабых мест в системе безопасности организации до того, как хакеры смогут их найти и использовать.
- Наиболее распространенный тип моделирования атаки – это тест на проникновение во внутреннюю сеть, который имитирует угрозы от злонамеренного или скомпрометированного инсайдера.
- Типичный тест на проникновение может выполняться в течение 40-часовой рабочей недели и состоит из четырех этапов:
  1. сбор информации;
  2. сосредоточенное проникновение;
  3. эксплуатация доступа и повышение привилегий;
  4. документирование.