1

Введение в этичный хакинг

Кибербезопасность — одна из самых интересных и быстро развивающихся областей знаний. Каждый день специалисты по безопасности и исследователи находят новые и новые угрозы и множество организаций обнаруживают, что их системы и сети были скомпрометированы злоумышленниками, в то время как другие, не имеющие надлежащей киберзащиты, вообще не подозревают, что их активы подвергаются риску. В связи с ростом количества кибератак и угроз во всем мире все больше организаций создают рабочие места для сотрудников, отвечающих за кибербезопасность, и стремятся привлечь лучших отраслевых экспертов и квалифицированных специалистов для усиления защиты активов от киберпреступников. Миссия этой книги — поделиться знаниями и навыками, необходимыми этичному хакеру и тестировщику на проникновение (пентестеру) для успешного старта в индустрии кибербезопасности.

С помощью этой книги вы разовьете новые умения и изучите методы моделирования реальных кибератак на системы и сети, необходимые специалисту по кибербезопасности. Вы научитесь обнаруживать скрытые уязвимости в организациях с помощью *тактик, техник и процедур* (ТТП, Tactics, Techniques, and Procedures, TTPs), которые используются реальными злоумышленниками для компрометации своих целей. Вы узнаете, как применять один из самых популярных в индустрии кибербезопасности дистрибутивов Linux — *Kali Linux* — для проведения этичного взлома и тестирования на проникновение в целевых системах и сетевой инфраструктуре. Дистрибутив Kali Linux имеет множество предустановленных пакетов Linux и инструментов безопасности, которые обычно используются отраслевыми экспертами, — это целый арсенал со всеми необходимыми этичному хакеру и тестировщику на проникновение инструментами. На протяжении всей книги я буду стремиться сделать ваше обучение максимально удобным и эффективным: она наполнена практическими упражнениями, которые помогут вам постепенно перейти от простых тем к темам среднего и продвинутого уровня.

В этой главе вы узнаете о различных типах субъектов угроз и намерениях/мотивах их атак на цели. Вы увидите, на какие ключевые факторы ориентируются злоумышленники при планировании кибератаки и как такие факторы определя-

ют уровень сложности компрометации целевой системы, сети или организации. Мы рассмотрим их с точки зрения профессионалов в области кибербезопасности — этичных хакеров и пентестеров, ответственных за обнаружение скрытых уязвимостей внутри компании. Кроме того, вы узнаете о различных этапах этичного взлома и подходах к тестированию на проникновение, которые обычно используются профессионалами отрасли.

Наконец, вы получите четкое представление о том, как методология *Cyber-Kill Chain* помогает специалистам по кибербезопасности лучше понять механики кибератак и методы и техники тестирования на проникновение, применяемые на каждом этапе атаки.

В этой главе мы рассмотрим следующие темы:

- Необходимость кибербезопасности.
- Важность тестирования на проникновение.
- Типы субъектов угроз и их намерений.
- Интересы и цели субъектов угроз.
- Методологии тестирования на проникновение.
- Подходы к пентесту.
- Виды тестирования на проникновение.
- Этапы тестирования на проникновение.
- Структура Cyber Kill Chain.

Надеюсь, вы так же, как и я, взволнованы этим удивительным путешествием, которое нам предстоит. Давайте начнем!

Необходимость кибербезопасности

Кибербезопасность защищает системы, сети и организации от специализированных атак и угроз, разработанных киберпреступниками с намерением причинить им вред или ущерб. Таких киберпреступников обычно называют *субъектами угроз*. С течением времени все больше пользователей и организаций подключают свои системы и сети к крупнейшей сети в мире — интернету, а киберпреступники разрабатывают новые стратегии кражи денег у потенциальных жертв. Например, создают достаточно сложные угрозы, такие как программы-вымогатели.

Давайте воспользуемся этим примером, чтобы подчеркнуть важность кибербезопасности. *Программы-вымогатели* — это тип криптовредоносного ПО, предназначенный для шифрования всех обнаруженных в системе жертвы данных, за исключением операционной системы хоста. Цель состоит в том, чтобы зашифровать данные, хранящиеся на локальном носителе, — самый ценный актив жертвы

в скомпрометированной системе — и запросить выкуп в виде криптовалюты в обмен на ключи расшифровки для восстановления данных. Чем дольше программа-вымогатель находится в скомпрометированной системе, тем вероятнее, что агент программы-вымогателя сможет установить *канал управления и контроля* (Command and Control, C2) с одним или несколькими серверами C2, которые управляются киберпреступниками, для получения обновлений и дополнительных инструкций. Злоумышленник может отправлять апдейты агенту программы-вымогателя, чтобы тот чаще обновлял используемые для шифрования данных жертвы криптографические ключи, что снижает шансы жертвы безопасно восстановить свои данные. В это время злоумышленник извлечет найденные в системе жертвы данные и продаст их на различных торговых площадках и аукционах даркнета. Киберпреступники умны, они прекрасно понимают, что организации знают ценность данных, хранящихся на их компьютерах и серверах, и сделают практически все, чтобы восстановить свои данные как можно скорее.

ПРИМЕЧАНИЕ Программы-вымогатели также могут поставить под угрозу данные, находящиеся в облачных хранилищах, к которым подключена зараженная система. Например, представьте, что в пользовательской системе работает агент облачного хранилища, обеспечивающий постоянную синхронизацию данных пользователя. Если система заражена программой-вымогателем, та зашифрует все данные на компьютере, в том числе синхронизируемые с облачным хранилищем. Однако различные поставщики облачных хранилищ имеют встроенную защиту от этого типа угроз.

Специалисты в области кибербезопасности не рекомендуют платить выкуп, поскольку у вас не будет ни гарантий, ни уверенности в том, что злоумышленники вернут вам зашифрованные данные или предоставят ключ для восстановления. Важно отметить, что одновременно с требованием выкупа за зашифрованные данные злоумышленники, как правило, угрожают раскрытием конфиденциальных данных организации и клиентов, публикацией их на специализированных сайтах утечек данных, таких как pastebin.com, и в средствах массовой информации. Очевидно, что из-за такого «повышения ставок» и оказываемого давления жертвам труднее не поддаться требованиям банд-вымогателей.

Множество организаций в мире придерживаются реактивного подхода к кибербезопасности. Вместо того чтобы принимать меры по предотвращению будущих угроз, они начинают реагировать только тогда, когда их системы и сети уже скомпрометированы кибератакой. Однако если организация не реализует надлежащую киберзащиту, не имеет эффективного плана реагирования на инциденты, заразившая одну систему программа-вымогатель может автоматически распространяться на другие уязвимые системы внутри организации, увеличивая очаг заражения. Таким образом, чем больше времени уйдет на сдерживание/изоляцию угрозы в сети, тем больший ущерб она может нанести.

ПРИМЕЧАНИЕ Во время работы над предыдущим изданием этой книги технический рецензент г-н Ришалин Пиллэй (Mr. Rishalin Pillay) упомянул, что, будучи сотрудником Microsoft, он наблюдал, как злоумышленники якобы передают ключ дешифрования жертве, однако на самом деле под этим предлогом внедряют дополнительное вредоносное ПО, чтобы позже вернуться и получить дополнительную прибыль. По сути, целевая организация становится дойной коровой для субъектов угрозы (атакующей группы).

Таким образом, организации, не нанявшие специалистов или исследователей[1] по кибербезопасности и не внедрившие решения безопасности, остаются незащищенными от различных типов угроз. Например, многие банки предоставляют систему онлайн-банкинга, которая позволяет их клиентам выполнять различные типы транзакций, таких как осуществление платежей, перевод средств и т. д. Представьте себе, что будет, если киберпреступники обнаружат слабые протоколы безопасности на веб-портале банка и найдут способ воспользоваться уязвимостью безопасности, — они смогут получить несанкционированный доступ к учетным записям множества клиентов, чтобы украсть их *персональные данные* (ПДН, на английском — PII, Personally Identifiable Information) и вывести деньги с их счетов. Поэтому конфиденциальность данных клиентов имеет решающее значение не только для защиты людей от немедленных финансовых потерь, но и для предотвращения будущих кибератак.

Терминология кибербезопасности

Во время погружения в тему кибербезопасности вы познакомитесь с терминологией, которая обычно используется в различных исследовательских работах, статьях, литературе, дискуссиях и учебных материалах. Становясь профессионалом в области кибербезопасности, вы должны иметь четкое понимание общей терминологии и ее связи с этичным хакингом и пентестом.

Ниже приведены наиболее распространенные термины индустрии кибербезопасности.

- *Актив* — в области кибербезопасности так мы обычно определяем все, что имеет ценность для организации или человека. Например, активы — это системы внутри сети, с которыми можно взаимодействовать и которые потенциально подвержены уязвимостям и могут быть скомпрометированы, что

[1] Некоторые компании запускают программы Bug Bounty, чтобы повысить безопасность своих продуктов без найма «безопасников». Суть таких программ в том, что независимые исследователи и этичные хакеры ищут уязвимости, сообщают о них напрямую компании, а она выплачивает вознаграждение или благодарят иным способом. Такое решение помогает вовремя закрывать проблемы и снижает риск их использования злоумышленниками. — *Примеч. науч. ред.*

обеспечит киберпреступнику несанкционированный доступ и предоставит возможность повысить права в скомпрометированной системе и получить привилегии не обычного пользователя, а администратора/суперпользователя (root-уровня). Однако важно отметить, что активы не ограничиваются техническими системами. Другие формы активов включают персонал (людей), средства физической безопасности, находящиеся в сети и защищаемые системой данные. Активы обычно классифицируют следующим образом:

- *Материальные активы* — физические объекты, имеющие стоимость, например компьютеры, серверы, сетевые устройства (маршрутизаторы, коммутаторы и т. д.) и устройства безопасности (брандмауэры). Они помогают обычным пользователям и сотрудникам получать доступ к ресурсам в сети и выполнять свои повседневные обязанности внутри организации. Серверы обычно используются для хранения данных и размещения приложений, а также предоставления услуг, необходимых в типичной сетевой инфраструктуре. Сетевые устройства содержат конфигурационные параметры, которые нужны для пересылки сетевого трафика между системами и устройствами безопасности, а сетевые устройства безопасности применяются для фильтрации нежелательного трафика между сетями и системами и предотвращения угроз. Если эти системы и устройства будут скомпрометированы, киберпреступники смогут перенаправить сетевой трафик на принадлежащие злоумышленникам вредоносные веб-сайты и расширить свое влияние.
- *Нематериальные активы* — ресурсы, которые не имеют физической формы, но представляют ценность: это могут быть приложения, лицензионные ключи программного обеспечения, интеллектуальная собственность, бизнес-планы и модели, данные.
- *Люди* — клиенты и сотрудники организации. Защита данных клиентов от кражи и утечек в даркнет, защита сотрудников от различных типов угроз имеют первостепенное значение. Важно понимать, какими активами располагает организация, и осознавать потенциальные риски для них.

- *Угроза* — это все, что потенциально может причинить вред или ущерб системе, сети или человеку. На каком бы аспекте кибербезопасности — наступательном или оборонительном — вы ни были сосредоточены, важно хорошо разбираться в различных видах угроз. Множество организаций по всему миру каждый день сталкивается с самыми разнообразными угрозами, а команды кибербезопасности круглосуточно работают над защитой активов компаний от киберпреступников.

  Особенность кибербезопасности, захватывающая и в то же время пугающая, заключается в том, что профессионалам отрасли всегда необходимо быть на шаг впереди злоумышленников, чтобы быстрее них находить слабые места в защите систем, сетей и приложений, а также реализовывать контрмеры для смягчения последствий любых потенциальных угроз активам организации.
- *Уязвимость* — это недостаток системы безопасности, воспользовавшись которым хакер может получить несанкционированный доступ к сети и контроль

над системами внутри нее. Одними из самых распространенных уязвимостей в организациях можно назвать человеческий фактор (главная уязвимость глобального масштаба), некорректную конфигурацию устройств, ненадежность учетных данных, небрежную программную реализацию, необновленные версии операционных систем, устаревшие приложения на хостах, использование настроек по умолчанию и т. д.

- Злоумышленник обычно ищет легкую мишень — уязвимости целевой системы, которые требуют минимальных усилий для их эксплуатации. Та же концепция применима и к тестированию на проникновение. Во время оценки безопасности пентестер будет применять различные методы и инструменты для обнаружения уязвимостей и попытается сначала проверить простые уязвимости, прежде чем перейти к более сложным недостаткам безопасности в целевой системе.
- *Эксплойт* — это инструменты, которые могут применяться для атаки на уязвимость системы. Например, целые программы или фрагменты кода. Представьте молоток, кусок дерева и гвоздь. Уязвимость — это мягкая, проницаемая структура древесины, эксплойт — это акт забивания гвоздя в дерево, а угроза — это молоток. При обнаружении уязвимости целевой системы злоумышленник или пентестер может воспользоваться ею, получив эксплойт из различных онлайн-источников либо разработав его самостоятельно.
- Приобретенный таким образом эксплойт важно протестировать в целевой системе, чтобы убедиться, что он работает должным образом и способен эту систему скомпрометировать. Иногда хорошо показавший себя в одной определенной системе эксплойт может не работать в другой. Поэтому опытные пентестеры всегда проверяют, работают ли их эксплойты должным образом, и оценивают степень их успешности для определенной уязвимости.
- *Атака* — это метод или прием, применяемый злоумышленником для выполнения эксплойта. Существуют различные виды атак, которые обычно используются киберпреступниками для нарушения конфиденциальности, целостности и/или доступности целевой системы. Например, программа-вымогатель LockBit 3.0 фокусируется на эксплуатации уязвимостей безопасности, обнаруженных в системах с выходом в интернет. При этом она не заражает компьютеры с определенными языковыми настройками. В список исключенных языков входят, например, румынский, арабский и татарский. Если язык системы совпадает с одним из этих языков, LockBit 3.0 прекращает работы и не заражает компьютер. Атака запускает в интернете программу-вымогатель, которая автоматически ищет и компрометирует уязвимые системы.

ПРИМЕЧАНИЕ Чтобы узнать больше о программе-вымогателе LockBit 3.0, посетите официальный отчет *Агентства по кибербезопасности и безопасности инфраструктуры* (Cybersecurity and Infrastructure Security Agency, CISA) по адресу https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a.

- *Вектор атаки* — это подсистема или направление атаки, с помощью которых злоумышленник может скомпрометировать целевую систему, сеть или организацию.

  Ниже приведены распространенные векторы атак:

  - *прямой доступ* — физический доступ к целевому компьютеру или сети;
  - *беспроводная связь* — использование уязвимостей безопасности, обнаруженных в инфраструктуре беспроводной сети цели;
  - *электронная почта* — отправка по электронной почте вредоносных сообщений, содержащих ссылки на зараженные вредоносным ПО службы, поддельные веб-сайты и вредоносные вложения[1];
  - *цепочка поставок* — нарушение безопасности продавца или поставщика для получения доступа к цели;
  - *социальные сети* — отправка вводящих в заблуждение сообщений или вредоносной рекламы (malvertising), чтобы обманом заставить получателя раскрыть конфиденциальную информацию или загрузить вредоносный файл;
  - *съемные носители* — подключение носителя, зараженного вредоносным ПО, к целевой системе;
  - *облако* — использование уязвимостей безопасности в облачных сервисах и их инфраструктуре.

  Все перечисленное — это инфраструктура доставки вредоносного кода к своей цели злоумышленником.

- *Риск* — потенциальное воздействие, которое уязвимость, угроза или атака оказывает на активы организации, а также шансы на то, что атака или угроза могут действительно причинить вред системам. Оценка риска помогает определить, насколько вероятна утечка данных, которая, в свою очередь, нанесет ущерб финансам, репутации или соблюдению нормативных требований в организации. Уменьшение риска имеет решающее значение для многих организаций. Существует множество сертификаций, нормативных стандартов и структур, призванных помочь компаниям понять, идентифицировать и снизить риски.

  Может показаться, что этичных хакеров и пентестеров нанимают для имитации реальных кибератак на целевую организацию, но на самом деле цель их действий серьезнее. В конце теста на проникновение специалист по кибербезопасности представит все уязвимости и возможные решения, которые помогут организации смягчить последствия и снизить риск потенциальной кибератаки, одновременно уменьшая поверхность атаки на компанию.

---

[1] Это также называется фишингом (phishing — англ. «рыбалка»). Мошенники руководствуются схожей логикой: закидывают «наживку» (поддельные сообщения и ссылки) и ждут, когда кто-нибудь «клюнет» и поделится своими конфиденциальными данными. — *Примеч. науч. ред.*

- *Поверхность атаки* (attack surface) — это все уязвимые точки входа в систему, сеть или организацию, через которые злоумышленник может получить несанкционированный доступ и расширить свое присутствие в сети. Этичные хакеры и пентестеры идентифицируют уязвимости точек входа, оценивая поверхность атаки организации и потенциальные способы, которыми злоумышленники могут воспользоваться для нарушения линии защиты.
- *Нулевой день* (zero-day, 0-day) — это период времени, когда злоумышленник уже обнаружил уязвимость в продукте или приложении и может ее эксплуатировать, а поставщик ПО о ней не знает или не успел выпустить обновление для решения проблемы. Такого рода уязвимости часто используются группами, представляющими *постоянную серьезную угрозу* (Advanced Persistent Threat, APT), и крупными преступными организациями для широкомасштабных атак. Обнаружение «уязвимости нулевого дня» очень ценится у этичных хакеров и пентестеров и может принести им bug bounty[1]. Это денежные вознаграждения, которые компании[2] платят исследователям за нахождение неизвестных дыр в их ПО.

  Существует множество программ вознаграждения за обнаружение ошибок. Исследователям безопасности, специалистам и всем обладающим необходимыми навыками для обнаружения уязвимостей предлагают сообщать о своих находках за вознаграждение, особенно если это «уязвимость нулевого дня». При этом реальные субъекты угроз будут пытаться использовать уязвимость целевой системы для личной выгоды, которую обычно называют ценностью взлома цели.

Итак, вы узнали о важности кибербезопасности. Далее давайте разберемся с различными типами субъектов угроз и мотивами, стоящими за их кибератаками.

Выявление субъектов угроз и их намерений

Начинающему этичному хакеру и пентестеру важно обладать хорошим моральным компасом и понимать различия между типами киберпреступников и мотивами их действий. Давайте подробнее познакомимся с встречающимися в индустрии кибербезопасности субъектами угроз.

- *Скрипт-кидди* (Script kiddie) — распространенный тип злоумышленника, и это не обязательно ребенок или молодой человек. Скорее это дилетант — тот, кто не до конца разбирается в технических деталях кибербезопасности и не может спланировать кибератаку или создать угрозу самостоятельно.

---

[1] Для этого стоит заранее ознакомиться с этой программой конкретной компании, прежде чем писать об уязвимостях (в некоторых случаях надо заранее зарегистрироваться в программе).

[2] И провайдеры облачных сервисов. — *Примеч. пер.*

Скрипт-кидди обычно следует инструкциям и руководствам настоящих хакеров, чтобы проводить собственные атаки против целевой системы или сети.

Вам может показаться, что скрипт-кидди относительно безвреден, потому что у него нет необходимых знаний и навыков, однако в реальности ущерб от его действий сравним с последствиями атаки настоящего хакера или даже превышает их. Злоумышленники этого типа используют инструменты, не зная, как они работают, тем самым нанося еще больший вред.

- *Кибертеррорист* — совершает кибератаки для достижения некой идеологической цели. Как правило, своими действиями, направленными на компрометацию сетей, каналов и систем связи, он хочет посеять страх и запугать целевую аудиторию.
- *Хактивист* — еще один тип «идейного» злоумышленника. Во многих странах мира существуют социальные и политические группы и партии, у которых есть как сторонники, так и противники. Вы наверняка встречали таких протестующих, организующих митинги и марши или даже прибегающих к незаконной деятельности, например порче общественной собственности.

  Хактивист использует свои хакерские навыки для поддержки политической или социальной повестки дня, для выполнения вредоносных действий, таких как повреждение веб-сайтов или запуск *DoS-атак* (Denial of Service, Отказ в обслуживании). Хотя некоторые хактивисты имеют благие намерения, не забывайте, что взлом по-прежнему является незаконным действием и субъект атаки может столкнуться с судебным иском со стороны правоохранительных органов. Напоминаю, что этичные хакеры и пентестеры должны получить юридическое разрешение, прежде чем приступать к совершению любых атак на цель.
- *Инсайдер* — хакер-шпион. Многие взломщики знают, как сложно внедриться в организацию через интернет и что гораздо легче это сделать, уже находясь в сети организации. Злоумышленник может создать резюме поддельной личности, подать заявку на работу в целевой организации и стать ее сотрудником. Такой субъект угрозы обычно называется *злонамеренным инсайдером*. Как только субъект угрозы приступает к работе, он получает доступ к внутренней сети и шанс детально изучить ее архитектуру и уязвимости систем безопасности компании. Затем он может создать сетевые импланты и несанкционированные точки входа (бэкдоры, backdoors) для удаленного доступа к критически важным системам.

ПРИМЕЧАНИЕ Сетевые импланты бывают программными или аппаратными. Программные импланты — это вредоносный код, который устанавливается и работает в скомпрометированной системе. Он позволяет злоумышленнику удаленно получать доступ к цели и контролировать ее. Аппаратные сетевые импланты — это физические устройства, подключенные напрямую к внутренней сети цели. С их помощью злоумышленник может выполнять атаки удаленно. Сетевые импланты обычно используются для мониторинга, управления и кражи данных.

Кроме того, существуют *непреднамеренные инсайдеры* — это законные сотрудники организации, которые неумышленно причиняют вред системам и сети организации из-за халатности, например, при подключении персонального USB-накопителя к компьютеру организации.

- *Спонсируемый государством* — также называемый *субъектом на службе у государства*. Во время войны страны отправляют армии солдат на фронт, а в мирное время происходят сражения в киберпространстве (такие, как шпионаж, подрывная деятельность, операции по оказанию влияния и подготовке к потенциальным горячим конфликтам). Это противостояние известно как *кибервойна*. Многие государства уже осознали необходимость развития кибербезопасности для защиты своих граждан, национальных активов и критически важной инфраструктуры от киберпреступников и враждебных государств.

  Правительство может нанять спонсируемых государством хакеров, которым будут поручены разведка и сбор разведданных о других странах, а также защита своей страны от кибератак и возникающих угроз. Некоторые страны используют этот тип субъектов угроз для получения секретной информации о других странах или даже атак на системы, контролирующие коммунальную инфраструктуру или другие критически важные ресурсы. Имейте в виду, что спонсируемые государством субъекты угроз — это не обязательно государственные служащие, ими могут быть группы либо отдельные лица, финансируемые, управляемые или поддерживаемые национальными правительствами.

ПРИМЕЧАНИЕ Кибершпионаж предполагает скрытное извлечение секретной, конфиденциальной или служебной информации: технологических чертежей, правительственных планов или даже личных данных ключевых лиц.

- *Организованная преступность*. В новостях мы часто слышим об организованных преступных группировках и синдикатах во всем мире. В сфере кибербезопасности также существуют преступные организации — группы людей, объединенные общими целями. Каждый человек внутри группы является экспертом в определенной области или обладает специальным набором навыков. Например, один может отвечать за проведение обширной разведки цели, другие — быть профессионалами в области социальной инженерии или проникновения в сеть, аналитиками вредоносного ПО, финансовыми специалистами по отмыванию денег и юрисконсультами. Успешность преступной группировки складывается из экспертных знаний и навыков всех участников.

  Достигнув определенного уровня влияния и контролируемых ресурсов, группа становится *постоянной серьезной угрозой* (уже упоминавшейся Advanced Persistent Threat, APT). В ее составе обычно есть человек, отвечающий за финансирование и предоставляющий лучшие из ресурсов, которые

можно купить за деньги, — это гарантирует успех атаки. Взломщики такого уровня обычно не мелочатся: например, стараются украсть критически важные данные, чтобы продать их и получить солидный куш.

- *Black Hat-хакер*[1] — это злоумышленник, который использует свои хакерские навыки в преступных целях. Это широкая категория; хакер может оказаться кем угодно, и причины для взлома целевой системы или сети могут быть самыми разными. Иногда «черные шляпы» идут на взлом, чтобы разрушить репутацию своей жертвы, для кражи данных или воспринимают это как личный вызов, чтобы доказать свою точку зрения, а бывает — и просто ради развлечения.
- *White Hat-хакер* — еще одна широкая категория, охватывающая людей без преступных намерений. «Белые шляпы» стремятся помочь организациям и людям защитить свои сети и свои активы от злоумышленников. Этичные хакеры и пентестеры относятся к этой категории, поскольку они используют свои навыки с добрыми намерениями, позитивным и этичным образом.
- *Gray Hat-хакер* — находятся между White Hat и Black Hat. Это означает, что квалифицированный хакер в «серой шляпе», будучи специалистом по кибербезопасности, при свете дня защищает людей и организации, а в ночное время использует свою квалификацию со злым умыслом. Как упоминалось ранее, этичные хакеры и пентестеры имеют верно настроенный моральный компас, а «серые шляпы», в отличие от них, нарушают законы морали и превращаются во взломщиков, преследующих злонамеренные цели.

Непрерывное развитие новых технологий всегда будет побуждать пытливые умы вникать в основы функционирования систем. Это часто приводит к обнаружению недостатков безопасности в конструкции систем и, в конечном счете, к открытию возможности использовать уязвимость. Изучив этот раздел, вы узнали о характеристиках различных субъектов угроз и причинах, побуждающих их к совершению кибератаки. В следующих разделах вы получите более глубокое понимание того, на что они обращают внимание при планировании кибератаки на цель.

Что важно для субъектов угроз

Взлом системы или устройства всегда был интересен для многих людей во всем мире как способ защиты от киберопасности. Еще одна сфера, которая привлекает любознательных, — реверс-инжиниринг системы (обратная разработка). Это процесс, помогающий понять, как работает система или код. Хакерство также направлено на лучшее понимание принципов функционирования системы и поиск

[1] Дословно — хакер в черной шляпе. Аналогично: White Hat-хакер — хакер в белой шляпе; Gray Hat хакер — хакер в серой шляпе. — *Примеч. пер.*

недостатков в ее дизайне и программировании, с помощью которых можно изменить работу системы или получить контроль над ней.

Но прежде чем начинать атаку на целевую организацию, киберпреступнику важно ее спланировать и оценить необходимые для этого ресурсы, сопоставить уровень сложности атаки и ценность взлома цели и определить, имеет смысл продолжать реализацию плана или нет.

Время

В первую очередь оценивается количество времени, которое будет затрачено на весь цикл: от начала сбора информации о цели до достижения задач атаки. На тщательное планирование кибератаки может уйти от нескольких дней до нескольких месяцев — пока не будет уверенности в том, что каждый этап цепочки *Cyber Kill Chain*®, выполненный в правильном порядке, будет успешным. Мы обсудим это в разделе «Структура Cyber Kill Chain» далее в этой главе.

Злоумышленникам также приходится учитывать опасность того, что атака или эксплойт не сработают в целевой системе и это приведет к неожиданной задержке и увеличит время, необходимое для достижения целей взлома. Ведь время требуется не только на получение доступа, но и на дальнейшие этапы, например поддержание присутствия, латеральное перемещение[1] и организацию утечки данных.

Концепцию времени следует взять на вооружение и этичным хакерам и пентестерам: им тоже необходимо определять, сколько времени потребуется для завершения теста на проникновение и представления отчета с выводами и рекомендациями по улучшению уровня безопасности для клиента.

Ресурсы

Любую задачу сложно выполнить без надлежащих ресурсов. Субъектам угроз нужны программные и аппаратные инструменты. Да, опытные хакеры могут вручную обнаруживать и использовать недостатки безопасности в целевых системах, но это занимает много времени. Наличие ресурсов позволяет автоматизировать эти задачи и сократить время, затрачиваемое на поиск брешей в безопасности и проникновение в систему. Кроме того, не имея необходимых навыков, злоумышленник может столкнуться с трудностями при осуществлении кибератаки, и ему потребуется поддержка тех, кто этими навыками обладает. То же верно и для профессионалов в области безопасности. Не у всех есть должная квалификация, и при тестировании на проникновение для оценки безопасности клиента может потребоваться команда.

---

[1] Это перемещение злоумышленника внутри уже скомпрометированной сети от одной системы к другой для расширения контроля и доступа к ценным ресурсам. — *Примеч. науч. ред.*