УДК 004.382
ББК 32.973.018
Ф73

Флоу С.
Ф73 Занимайся хакингом как невидимка / пер. с англ. В. С. Яценкова. – М.: ДМК Пресс, 2022. – 272 с.: ил.

ISBN 978-5-97060-977-4

Эта книга позволит вам примерить на себя роль хакера и атаковать вымышленную консалтинговую фирму Gretsch Politico, чтобы на ее примере изучить стратегии и методы опытных взломщиков. Вы узнаете о том, как построить надежную хакерскую инфраструктуру, гарантирующую анонимность в интернете, рассмотрите эффективные приемы разведки, разработаете инструменты взлома с нуля и освоите низкоуровневые функции обычных систем.

Независимо от того, являетесь ли вы профессионалом в области безопасности или просто энтузиастом, это практическое руководство поможет вам научиться проводить реальные хакерские атаки и распознавать скрытые уязвимости облачных технологий.

УДК 004.382
ББК 32.973.018

ISBN 978-1-7185-0126-3 (англ.)
ISBN 978-5-97060-977-4 (рус.)

СОДЕРЖАНИЕ

Об авторе

Спарк Флоу (Sparc Flow) – эксперт по компьютерной безопасности, специализирующийся на этичном хакинге. Он представлял свои исследования на международных конференциях по безопасности, таких как Black Hat, DEF CON, Hack In The Box и многих других. В то время как его основная работа состоит в том, чтобы взламывать компании и показывать им, как исправить уязвимости в системе безопасности, его страстью остается разработка инструментов и методов обеспечения безопасности.

Ранее он написал серию из четырех книг[1], получивших широкую известность во всем мире:

- *How to Hack Like a Pornstar*;
- *How to Hack Like a GOD*;
- *How to Investigate Like a Rockstar*;
- *How to Hack Like a Legend*.

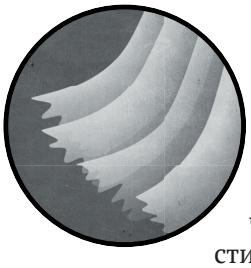
О техническом обозревателе

Мэтт Берроу – старший специалист по тестированию на проникновение в корпоративной красной команде, где он оценивает безопасность служб облачных вычислений и внутренних систем. Он также является автором книги *Pentesting Azure Applications* (No Starch Press, 2018). Мэтт получил степень бакалавра в области сетей, безопасности и системного администрирования в Рочестерском технологическом институте и степень магистра в области информатики в Университете Иллинойса в Урбана-Шампейн.

---

[1] На русском языке эти книги официально не издавались и распространяются в самодеятельных переводах под разными названиями. – *Прим. перев.*

ВВЕДЕНИЕ



Индустрия безопасности сложна. Я поддерживаю отношения любви/ненависти с этой неоднозначной отраслью в немалой степени из-за ее непостоянной и мимолетной природы. Вы можете потратить месяцы или годы, оттачивая свои навыки в определенной области безопасности – скажем, в повышении привилегий и расширении охвата с помощью PowerShell – только для того, чтобы почувствовать себя совершенно бесполезным, оказавшись в среде Linux или macOS.

К тому времени, когда вы научитесь подбирать ключи к дверям macOS и побеждать привратника Linux, новая сборка Windows 10 выйдет с новыми мерами обнаружения, что сделает любую привычную атаку через PowerShell абсолютно бесполезной. Вы возвращаетесь к тому, с чего начинали: охотитесь за блогами, посещаете конференции и погружаетесь в исследование документации и кода, чтобы обновить свои инструменты и разработать новые методы взлома.

Если подумать трезво, эти тараканьи бега могут показаться полным безумием. Вы, конечно, всегда можете утешить свое эго, вторгаясь в сети компаний из списка Fortune 500, которые считают Windows XP/2003 драгоценным вымирающим видом, который нужно сохранить любой ценой, но волна забвения настигает вас. В глубине души вы знаете, что вам придется постоянно догонять уходящий поезд.

В конце концов, это и есть хакерство. Разочарование от потери любимого трюка может сравниться только с восторгом от освоения новой блестящей технологии.

Я в общих чертах определяю хакерство (или взлом) как совокупность приемов и инструкций, предназначенных для достижения нестандартных результатов в системе или процессе. Тем не менее срок годности этих уловок истекает все быстрее. Ваша цель как специалиста по безопасности или энтузиаста – найти и употребить как можно больше полезных трюков, пока они не протухли.

Никогда не знаешь, какое копье остановит бегущего на тебя быка.

В других своих книгах я много внимания уделял атакам, связанным с Windows, потому что большинство компаний из списка Fortune 500

построили большую часть своей среды на основе Active Directory. Это было идеальное решение для управления тысячами пользователей, серверов и приложений.

Однако времена меняются. Компания, создающая свою инфраструктуру с нуля, больше не будет запускать контроллер домена Windows на «голом железе» в общем центре обработки данных на окраине города. В самом деле, покажите мне системного администратора, который все еще хочет управлять устаревшим оборудованием и кластером ESXi из трех десятков машин с различными брандмауэрами, коммутаторами, маршрутизаторами и балансировщиками нагрузки. Не мешайте ему засунуть голову в петлю и закройте дверь!

Зачем так напрягаться, если вы можете настроить все необходимое в облачной среде за считанные секунды? Базы данных, контейнеры Docker и Active Directory находятся на расстоянии одного клика мыши, а бесплатная пробная версия порадует вашего бухгалтера. Конечно, первоначальная низкая плата быстро увеличивается по мере роста масштаба ваших серверов, но большинство стартапов будут только рады таким проблемам. Это означает, что бизнес растет.

В этой книге я решил не рассматривать традиционную архитектуру, применяемую в старых жирных компаниях. Давайте посмотрим, как злоумышленник может победить современного и достойного противника: компанию, которая пустила свои корни в динамичной и отказоустойчивой облачной среде и поддерживает свой рост с помощью методов DevOps.

Это не просто модные словечки, которые обожают употреблять невежественные боссы компаний и хищные рекрутеры из кадровых агентств. Это потрясающие новые парадигмы, и когда им следуют успешно, они настолько глубоко меняют архитектуру и принципы работы сетей и приложений, что приходится напрягать все свое чутье и собирать знания по крупицам, чтобы искать и находить лазейки. Уязвимости, на которые можно было не обращать внимания в классической среде, внезапно приобретают смертельный потенциал в облачной инфраструктуре. Забудьте о SQL-инъекциях. Как только вы узнаете, что машина размещена в Amazon Web Services (AWS), вам следует полностью сосредоточиться на другом классе уязвимостей.

Злоумышленники перескакивали с одной машины на другую, обходя правила брандмауэра и прокладывая себе путь к внутренней базе данных, Active Directory и тому подобному. Это путешествие часто включало сканирование сети, туннелирование трафика и так далее. В облачной среде вы можете управлять основными элементами инфраструктуры с любого IP-адреса в мире. Вы обнаружили, что брандмауэр блокирует доступ к определенной машине? Раздобыв подходящие учетные данные, вы можете отменить это конкретное правило одним вызовом API из Китая и получить доступ к этому «внутреннему» компьютеру с Филиппин.

Конечно, это не значит, что больше не нужно взламывать пароли и перескакивать с машины на машину. Нам по-прежнему не обойтись без сетевой магии, чтобы получить доступ к драгоценной конечной

точке, содержащей бизнес-данные, но цель сместилась от контроля над отдельными машинами к контролю над самой инфраструктурой.

Рассмотрим DevOps – еще один ключевой набор принципов, отстаиваемых технологическими компаниями. В общих чертах он определяется как комплекс технических или организационных мер, направленных на автоматизацию разработки программного обеспечения и повышение производительности и надежности кода. DevOps охватывает все: от определения инфраструктуры как кода до контейнеризации и автоматизированного мониторинга. Одним из основных следствий внедрения культуры DevOps является то, что компании все меньше и меньше боятся изменять свою инфраструктуру и приложения. Забудьте типичную ИТ-мантру: «Работает – не трогай». Когда вы развертываете приложение в рабочей среде пять раз в неделю, вам удобнее изменять его так, как вы считаете нужным.

Когда вы перестаете жестко привязывать приложение к системе, в которой оно работает, у вас появляется больше возможностей для обновления инфраструктуры. Когда у вас есть сквозные интеграционные тесты, вы можете легко позволить себе исправлять критические части кода с минимальными побочными эффектами. Когда у вас есть инфраструктура, определяемая как код, вы можете исключить «серые зоны» и строго контролировать каждую машину в инфраструктуре – роскошь, за которую многие крупные компании готовы пойти на преступление.

Эта новая волна методик DevOps исключает многие допущения, на которые мы исторически полагались при поиске дыр в корпоративной сети. Хакеры привыкли проникать в сознание человека, проектирующего систему, чтобы воспользоваться его ложными предпосылками и поспешными решениями. Но как это сделает хакер, застрявший в старых способах проектирования и эксплуатации систем?

Конечно, новая эра облачных вычислений – это отнюдь не волшебный мир единорогов, писающих радугой.

Грандиозные ошибки, совершенные в 1970-х годах, до сих пор добросовестно – если не сказать фанатично – повторяются в этом десятилетии. Разве не возмутительно, что в сегодняшнем неспокойном мире безопасность по-прежнему считается «предпочтительной», а не основной функцией первоначального *минимально жизнеспособного продукта* (minimum viable product, MVP)? Я говорю не про IoT-стартапы, которым остался один раунд финансирования до банкротства, а о крупных инфраструктурных продуктах, таких как Kubernetes, Chef, Spark и так далее. Людей, позволяющих себе подобные высказывания, нужно медленно и больно бить по лбу стальной ложкой до потери сознания:

> «Безопасность в Spark по умолчанию отключена. Это может означать, что с настройками по умолчанию вы уязвимы для атак».

Но я отвлекся. Я хочу сказать, что DevOps и переход в облака принесли с собой потрясающие изменения, но вдумчивому хакеру доста-

точно небольших намеков и корректировок, чтобы успешно двигаться по новому пути. Это было волнующее прозрение, которое вдохновило меня написать эту книгу.

О чем расскажет эта книга

Это не типичная техническая книга и не учебник в его традиционном понимании. Мы с вами примеряем на себя роль хакера, и наша цель – вымышленная политическая консалтинговая фирма Gretsch Politico. Я проведу вас через день (или несколько) из жизни хакера, по всему пути от начала до конца – от создания качественной анонимной инфраструктуры до проведения предварительной разведки и, наконец, проникновения в систему и захвата контроля над целью. Компании и названия, используемые здесь, в основном вымышлены, за исключением очевидных брендов типа Kubernetes или AWS. Вы должны понимать, что хотя вы можете адаптировать и опробовать многое (и я призываю вас это сделать), вы не сможете буквально следовать каждому шагу, как показано в книге. Например, в конечном итоге мы взломаем электронную почту генерального директора компании Gretsch Politico Александры Стикс. Разумеется, в реальной жизни ни компания, ни директор не существуют.

Продвигаясь на ощупь в инфраструктуре компании, мы столкнемся со многими тупиками и препятствиями, но я покажу вам, как можно использовать самые скромные зацепки, чтобы скорректировать свой путь. Так происходит взлом в реальном мире. Не каждый маршрут приведет к успеху, но при достаточной настойчивости, капельке творчества и чистой удаче можно наткнуться на интересные находки. Для большей достоверности примеров дальше я буду говорить о наших вымышленных целях так, будто они столь же реальны, как вы или я.

Несколько слов о цели нашего взлома. Gretsch Politico Consulting – это фирма, которая помогает политикам проводить свои предвыборные кампании. Gretsch Politico (которую я также буду называть GP) утверждает, что имеет миллионы точек данных и сложные профили моделирования для эффективного взаимодействия с ключевой аудиторией. Как они красиво написали на своем веб-сайте: «Результат выборов часто зависит от последних критически настроенных избирателей. Наши услуги по управлению данными и микротаргетингу помогут вам обратиться к нужным людям в нужное время».

Истинный смысл этой фразы такой: «У нас есть огромная база данных симпатий и антипатий миллионов людей, и мы можем целенаправленно загрузить им в голову любой контент, полезный для вашей политической программы».

Так гораздо понятнее, но гораздо страшнее, верно?

Хотел бы я, чтобы и это было вымыслом, но, к сожалению, именно так в наши дни проходят почти все «демократические выборы», так что описанный в этой книге вымышленный пример очень близок к реальной жизни.

Краткое содержание книги

Я не хочу заранее раскрывать интригу, поэтому скажу лишь, что книга разбита на четыре части. Часть I, «Поймай меня, если сможешь», рассказывает о построении надежной хакерской инфраструктуры, гарантирующей анонимность в интернете. Мы создадим арсенал пользовательских скриптов, контейнеров и серверов управления и контроля (C2) и настроим внутреннюю атакующую инфраструктуру на максимально эффективную работу в автоматическом режиме.

С оружием наперевес мы переходим к части II, «За работу», где речь идет о базовой разведке, которую вам нужно выполнить, чтобы лучше узнать свою цель и отыскать начальные уязвимости.

В части III, «Полное погружение», мы получаем доступ к сетевой среде, которая поначалу кажется бесплодной. Мы переходим в ней от одного приложения к другому и от одной учетной записи к другой, пока не достигнем полного контроля над целевой инфраструктурой.

Наконец, в части IV «Враг внутри» мы собираем все достижения в один атакующий кулак и пожинаем плоды, кропотливо прочесывая терабайты данных и используя скрытые связи между нашими целями.

Я не стал подробно разбирать каждый возможный вектор атаки или потенциально полезный инструмент, иначе книга никогда бы не закончилась. Вместо этого в конце каждой главы я даю вам список дополнительных материалов, с которыми вы можете ознакомиться на досуге.

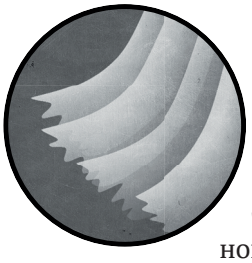
ЧАСТЬ I

ПОЙМАЙ МЕНЯ, ЕСЛИ СМОЖЕШЬ

…Конечно, у нас есть свобода воли,
потому что у нас нет другого выбора, кроме как иметь ее.
Кристофер Хитченс

1

СТАНЬТЕ АНОНИМНЫМ В СЕТИ



Пентестеры и члены красных команд любят устанавливать и настраивать свою инфраструктуру так же сильно, как и писать отчеты о вторжении, – то есть совсем никак. Они испытывают эстетическое удовольствие от развертывания эксплойтов на компьютере жертвы, горизонтального перемещения по сети и повышения привилегий. Создание безопасной инфраструктуры – скучная работа. Если пентестер случайно «засветит» свой IP-адрес в логах доступа к серверу своей жертвы, что с того? Он вечером угостит команду пивом за то, что напортачил, синюю команду начальство похлопает по плечу за то, что она обнаружила и разоблачила нападение, а на следующий день каждый сможет начать все заново.

ПРИМЕЧАНИЕ *Краткий словарь терминов на случай, если вы новичок в мире информационной безопасности: пентестеры исчерпывающе оценивают безопасность приложения, сети или системы, имитируя определенные действия злоумышленника. Красная команда оценивает уровень системы безопасности компании, имитируя реальные атаки хакеров (желательно без предварительных знаний о системе). Синяя команда защищает компанию и противостоит красным командам.*

В реальном мире все по-другому. Например, для хакеров нет никаких послаблений. У них нет такой роскоши, как юридически обязывающий договор о тестировании на проникновение. Их свобода, а иногда и жизнь зависит от безопасности инструментов и анонимности инфраструктуры. Вот почему в каждой из своих книг я стараюсь написать об основных процедурах *операционной безопасности* (OpSec) и о том, как построить анонимную и эффективную хакерскую инфраструктуру: краткое руководство, как оставаться в безопасности в этом все более жестком и авторитарном мире, в котором мы живем. Я начну эту книгу с рассказа о том, как стать максимально анонимным в сети, используя виртуальную частную сеть (virtual private network, VPN), Tor, опорные серверы и заменяемую и переносимую инфраструктуру атаки.

Если вы уже знакомы с текущим *фреймворком управления и контроля* (command and control, C2), контейнерами и инструментами автоматизации, такими как Terraform, вы можете сразу перейти к главе 4, где начинается разговор о настоящем взломе.

VPN и его недостатки

Я надеюсь, что сегодня почти все знают, что раскрывать свой домашний или рабочий IP-адрес целевому веб-сайту, который вы атакуете, – это большая глупость. Тем не менее большинство людей всерьез полагают, что вполне достаточно посещать веб-сайты через VPN-сервис, который обещает полную анонимность, – сервис, на котором они зарегистрировались со своего домашнего IP-адреса, возможно, даже с оплатой собственной кредитной карты, вместе со своим именем и адресом. Что еще хуже, они установили это VPN-соединение со своего домашнего ноутбука во время потоковой передачи своего любимого шоу Netflix и общения с друзьями на Facebook.

Давайте внесем ясность прямо сейчас. Независимо от того, что они говорят, VPN-сервисы всегда, *всегда* будут вести логи в той или иной форме: IP-адрес, DNS-запросы, активные сеансы и так далее. Давайте на секунду прикинемся наивным лузером и представим, что нет законов, обязывающих каждого провайдера виртуального доступа вести логи метаданных исходящих соединений, – такие законы действуют в большинстве стран, и ни один VPN-провайдер не станет их нарушать ради вашей жалкой ежемесячной подписки, – но давайте на минутку представим, что этих законов нет. Поставщик VPN имеет сотни, если не тысячи серверов в нескольких центрах обработки данных по всему миру. У них также есть тысячи пользователей – одни на машинах с Linux, другие на Windows и даже несколько испорченных пользователей на Mac. Вы действительно можете поверить, что можно управлять столь огромной и разнородной инфраструктурой без таких элементарных вещей, как логи?

ПРИМЕЧАНИЕ *Метаданные относятся к описанию сеанса связи – какой IP-адрес связывался с каким IP-адресом, с использованием какого протокола, в какое время и т. д., – но не к ее содержанию.*

Без логов техподдержка была бы такой же бесполезной и невежественной, как и растерянный клиент, звонящий им для решения проблемы. Никто в компании не знал бы, как начать решать простую проблему поиска DNS, не говоря уже о загадочных проблемах маршрутизации, связанных с потерей пакетов, предпочтительными маршрутами и прочим сетевым шаманством. Многие провайдеры VPN считают необходимым громогласно защищать свой «сервис без логов», чтобы не отставать от конкурентов, делающих аналогичные заявления, но это бессмысленная гонка, основанная на вопиющей лжи или «маркетинге», как это нынче принято называть.

Лучшее, на что вы можете надеяться в отношении провайдера VPN, – это то, что он не продает данные клиентов любому, кто предложит достаточно высокую цену. И даже не связывайтесь с бесплатными провайдерами. Инвестируйте в свою конфиденциальность как время, так и деньги. Я рекомендую начать с AirVPN и ProtonVPN, которые являются серьезными игроками в бизнесе.

Такое же представление об анонимности применимо к Tor (The Onion Router, *https://www.torproject.org*), который обещает анонимную работу в интернете через сеть узлов и ретрансляторов, скрывающих ваш IP-адрес. Назовите мне хоть одну причину, по которой вы должны слепо доверять первому узлу, с которым вы связываетесь, для входа в сеть Tor. Почему вы должны доверять ему больше, чем нигерийскому принцу, который обещает поделиться наследством в обмен на номер вашей кредитной карты? Конечно, первый узел знает только ваш IP-адрес, но, как правило, даже этого предостаточно.

Физическое местоположение

Один из способов повысить свою анонимность – следить за своим физическим местоположением при взломе. Не поймите меня неправильно: Tor по-своему великолепен. VPN – отличная альтернатива. Но когда вы полагаетесь на эти службы, всегда предполагайте, что ваш IP-адрес – и, следовательно, ваше географическое положение и/или отпечаток браузера – известен этим посредникам и может быть обнаружен вашей конечной целью или любым лицом, проводящим расследование от их имени. Как только вы принимаете эту предпосылку, естественным образом напрашивается вывод: чтобы быть по-настоящему анонимным в интернете, вам нужно уделять своему физическому следу ничуть не меньше внимания, чем вы уделяете цифровым следам в интернете.

Если вам посчастливилось жить в большом городе, используйте оживленные вокзалы, торговые центры или подобные обществен-

ные места, где есть общедоступный Wi-Fi, чтобы спокойно проводить свои операции. Станьте еще одной молекулой в ежедневном потоке пассажиров. Однако будьте осторожны, чтобы не стать жертвой нашей коварной человеческой природы, склонной к шаблонному поведению. Старайтесь не сидеть на одном и том же месте изо дня в день. Возьмите за правило посещать новые места и даже время от времени менять города.

В некоторых странах, таких как Китай, Япония, Великобритания, Сингапур и США, установлено большое количество камер, наблюдающих за улицами и общественными местами. В этом случае альтернативой было бы использование одного из старейших приемов: блуждающий доступ в сеть. Используйте автомобиль, чтобы покататься по городу в поисках открытых точек доступа Wi-Fi. Типичный приемник Wi-Fi может ловить сигнал на расстоянии до 40 метров, которое вы можете увеличить до пары сотен метров с помощью направленной антенны.

Как только вы найдете открытую или плохо защищенную точку доступа, которую вы можете взломать – шифрование WEP и слабые пароли WPA2 не редкость и могут быть взломаны с помощью таких инструментов, как Aircrack-ng и Hashcat, – припаркуйте поблизости свой автомобиль и приступайте к работе. Если вы не любите бесцельно колесить по городу, посмотрите онлайн-проекты, такие как WiFi Map на *https://www.wifimap.io*, в которых перечислены открытые точки доступа Wi-Fi, иногда с их паролями. Быть хакером – это на самом деле образ жизни. Если вы действительно привержены своему делу, вы должны полностью принять его и избегать небрежности любой ценой.

Рабочий ноутбук

Теперь, когда мы позаботились о местоположении, давайте разберемся с ноутбуком. Люди очень дорожат своими ноутбуками с логотипами брендов, сумасшедшими техническими характеристиками и, черт возьми, со списком закладок, которые все клянутся, что когда-нибудь просмотрят. Такой компьютер хорош на местной конференции компьютерных гиков, а не для взлома. Любой компьютер, который вы используете для болтовни в соцсетях и проверки почтового ящика Gmail, практически наверняка известен большинству государственных учреждений. Никакой навороченный VPN не спасет ваше милое лицо, если цифровой отпечаток вашего браузера каким-то образом станет известен службе безопасности крутой конторы, которую вы атакуете.

Для целей взлома нам нужна *эфемерная операционная система* (ОС), которая сбрасывает все логи при каждой перезагрузке. Мы храним эту ОС на USB-накопителе, и всякий раз, оказавшись в удобном месте, подключаем накопитель к компьютеру, чтобы загрузить нашу рабочую среду.

Tails (*https://tails.boum.org/*) – это специальный дистрибутив Linux для такого типа деятельности. Он автоматически меняет MAC-адрес, заставляет все соединения проходить через Tor и избегает хранения данных на жестком диске ноутбука. (Наоборот, традиционные операционные системы, как правило, хранят часть памяти на диске для оптимизации параллельного выполнения – операции, известной как подкачка.) Если дистрибутив Tails был достаточно хорош для Сноудена, то, держу пари, он устроит почти всех. Я рекомендую настроить ОС Tails и сохранить ее на внешнем диске, прежде чем делать что-либо еще.

Некоторые люди испытывают необъяснимую любовь к Chromebook. Это недорогое оборудование, на котором установлена минимальная операционная система, поддерживающая только браузер и терминал. Выглядит идеально, правда? Ничего подобного. Это даже хуже, чем лизать железный столб зимой. Мы говорим об ОС, разработанной Google, которая требует, чтобы вы вошли в свою учетную запись Google, синхронизировали свои данные и сохранили их на Google Диске. Нужно ли мне продолжать? Да, существуют расширения Chromium OS, которые отключают часть синхронизации Google, например NayuOS, но правда заключается в том, что ни устройства Google, ни расширения не были разработаны специально для сохранения конфиденциальности, и ни при каких обстоятельствах они не должны использоваться для анонимных хакерских действий. Должно быть, в Google изрядно повеселились по этому поводу.

Ваш рабочий ноутбук должен содержать только временные рабочие данные, такие как вкладки браузера, набор команд для быстрого копирования/вставки и т. д. Если вам абсолютно необходимо экспортировать огромные объемы данных, обязательно храните эти данные в зашифрованном виде на портативном накопителе.

Опорные серверы

Единственное назначение нашего ноутбука – подключить нас к набору *опорных* или *прыгающих* серверов (bouncing server), которые содержат необходимые инструменты и сценарии для подготовки к нашему приключению. Это виртуальные хосты, которые мы настраиваем анонимно, подключаемся к ним только через Tor или VPN, доверяем взаимодействие с нашими более вредоносными виртуальными машинами (virtual machine, VM) и храним нашу добычу.

Эти серверы предоставляют нам надежный и стабильный шлюз для нашей будущей атакующей инфраструктуры. Мы будем подключаться к опорному серверу по SSH непосредственно после того, как удостоверимся, что установили соединение через VPN или Tor. Мы можем инициировать соединение Secure Shell (SSH) через случайную точку доступа на холодном и оживленном вокзале и оказаться в теплой и уютной обстановке, где нас ждут все наши инструменты и любимые псевдонимы Zsh.

Опорные серверы могут быть размещены у одного или нескольких облачных провайдеров, разбросанных по разным географическим точкам. Очевидным ограничением является платежное решение, поддерживаемое этими провайдерами. Вот несколько примеров облачных провайдеров с достойными ценами, которые принимают криптовалюты:

- RamNode (*https://www.ramnode.com/*) стоит около 5 долларов США в месяц за сервер с 1 ГБ памяти и двумя ядрами виртуального ЦП (vCPU). Принимает только биткойн;
- NiceVPS (*https://nicevps.net/*) стоит около 14,99 евро в месяц за сервер с 1 ГБ памяти и одним ядром виртуального ЦП. Принимает Monero и Zcash;
- Cinfu (*https://www.cinfu.com/*) стоит около 4,79 доллара в месяц за сервер с 2 ГБ памяти и одним ядром виртуального ЦП. Принимает Monero и Zcash;
- PiVPS (*https://pivps.com/*) обойдется около 14,97 доллара в месяц за сервер с 1 ГБ памяти и одним ядром виртуального ЦП. Принимает Monero и Zcash;
- SecureDragon (*https://securedragon.net/*) стоит около 4,99 доллара в месяц за сервер с 1 ГБ памяти и двумя ядрами виртуальных ЦП. Принимает только биткойн.

Некоторые сервисы, такие как BitLaunch (*https://bitlaunch.io/*), могут выступать в роли простого посредника. BitLaunch принимает платежи в биткойнах, но затем создает серверы в DigitalOcean и Linode, используя свою собственную учетную запись (конечно, в три раза дороже, что просто возмутительно). Еще один посреднический сервис с чуть более выгодной стоимостью – это bithost (*https://bithost.io/*), который по-прежнему берет комиссию 50 %. Их недостаток, помимо откровенно мошеннических расценок, заключается в том, что ни один из этих провайдеров не предоставляет вам доступ к API DigitalOcean, который помогает автоматизировать большую часть настройки.

Выбор облачного провайдера может приводит нас к горькому компромиссу: поддержка криптовалют и псевдоанонимность против простоты использования и автоматизации.

Все основные облачные провайдеры – AWS, Google Cloud, Microsoft Azure, Alibaba и т. д. – требуют пройти проверку валидности вашей кредитной карты перед подтверждением учетной записи. В зависимости от того, где вы живете, это может не доставить никаких проблем, так как существует множество сервисов, которые предоставляют предоплаченные кредитные карты в обмен на наличные. Некоторые онлайн-сервисы даже принимают кредитные карты для пополнения с помощью биткойнов, но для большинства из них потребуется удостоверение личности государственного образца. Это риск, который вы должны тщательно изучить.

В идеале опорные серверы должны использоваться для размещения инструментов, таких как Terraform, Docker и Ansible, которые поз-

же помогут нам создать несколько инфраструктур для атак. Общий обзор хакерской архитектуры представлен на рис. 1.1.

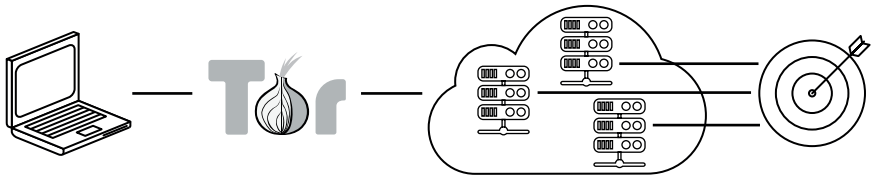


Рис. 1.1. Наиболее общий обзор хакерской инфраструктуры

Наши опорные серверы никогда не будут взаимодействовать с целью. Ни единого звука. Поэтому мы можем позволить себе пользоваться ими немного дольше перед сменой – несколько недель или месяцев – без значительных рисков. Тем не менее опытные службы безопасности могут найти способ связать эти серверы с теми, которые используются для прямого взаимодействия с целью, поэтому я рекомендую регулярно удалять и повторно создавать такие серверы.

Инфраструктура атаки

Наша инфраструктура атаки имеет гораздо более высокий уровень волатильности, чем наши отказоустойчивые серверы, и ее следует хранить всего несколько дней. Если возможно, она должна быть уникальной для каждой операции или цели. Последнее, что нам нужно, – это чтобы безопасники собрали воедино различные улики от разных целей, пораженных с одного и того же IP.

Инфраструктура атаки обычно состоит из интерфейсной и серверной систем. Интерфейсная система может инициировать соединения с целью, сканировать машины и т. д. Ее также можно использовать – в случае оболочки с обратным подключением – для маршрутизации входящих пакетов через веб-прокси и доставки их, при необходимости, в серверную систему (обычно это среда C2, такая как Metasploit или Empire). Только некоторые запросы перенаправляются на серверную часть C2; большинство страниц возвращают заурядное содержимое, как показано на рис. 1.2.

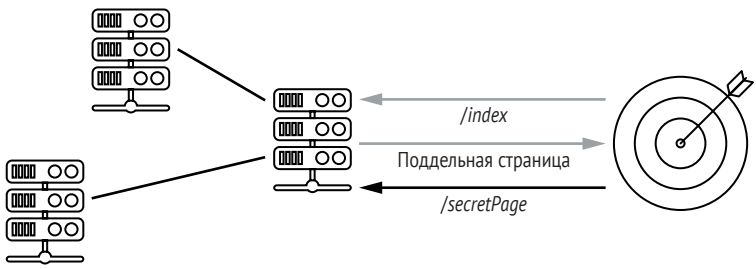


Рис. 1.2. Маршрутизация пакетов к серверной части

Эта маршрутизация пакетов может быть выполнена с помощью обычного веб-прокси, такого как Nginx или Apache, который действует как фильтр: запросы обратной оболочки от зараженных компьютеров направляются непосредственно на соответствующий серверный экземпляр C2, в то время как в ответ на остальные запросы – например, от аналитиков безопасности – отображается невинная веб-страница. Базовая среда C2 на самом деле является позвоночником инфраструктуры атаки, выполняя команды на зараженных машинах, извлекая файлы, доставляя эксплойты и делая многое другое.

Вам нужно, чтобы ваша инфраструктура была модульной и заменяемой по желанию. Обход запрета доступа с некоторых IP-адресов должен быть таким же простым, как отправка одной команды для создания нового прокси. Проблемы с серверной частью C2? Введите одну команду, и у вас будет новый сервер C2, работающий с точно такой же конфигурацией.

Достижение такого уровня автоматизации не является причудливым способом опробовать самые модные инструменты и методы программирования. Чем проще запустить полностью настроенные атакующие серверы, тем меньше ошибок мы совершаем, особенно в стрессовых ситуациях. Это хороший повод примерить на себя шкуру DevOps-специалиста, изучить его ремесло и подстроить его под свои нужды. Надеюсь, это подскажет нам некоторые недостатки атакуемых систем, которыми мы позже воспользуемся в нашем хакерском приключении. Следующая глава будет посвящена построению серверной инфраструктуры.

Дополнительные ресурсы

- Удивительный рассказ о жизни и приключениях Эдварда Сноудена в разведывательном сообществе можно найти в книге «Личное дело» Эдварда Сноудена (Эксмо, 2019).
- Учебник darkAudax по взлому зашифрованных WEP-сообщений можно найти здесь: *https://aircrack-ng.org/*.
- Руководство Брэннона Дорси по взлому Wi-Fi-маршрутизаторов WPA/WPA2 с помощью Aircrack-ng и Hashcat по адресу *https://hakin9.org/*.
- Руководство Мухаммада Арула по настройке Zsh на компьютере с Linux на странице *https://www.howtoforge.com/*.