СОДЕРЖАНИЕ

ОБ АВТОРЕ

Джо Грей, ветеран ВМС США, является основателем и главным инструктором OSINTion, основателем и главным исследователем Transparent Intelligence Services, а также первым победителем DerbyCon Social Engineering CTF. Будучи сотрудником Агентства по проверке паролей, Грей выиграл конкурс TraceLabs OSINT Search Party на DEFCON 28. Недавно он разработал профессиональные инструменты для проведения OSINT и операций по обеспечению кибербезопасности DECEPTICON Bot и WikiLeaker.

О ТЕХНИЧЕСКОМ РЕЦЕНЗЕНТЕ

Кен Пайл – партнер CYBIR, специализирующийся на информационной безопасности, разработке эксплойтов, тестировании на проникновение и управлении корпоративными рисками, а также дипломированный профессор кибербезопасности в Колледже Честнат-Хилл. Как авторитетный и популярный лектор по информационной безопасности, он выступал на отраслевых мероприятиях, таких как DEFCON, ShmooCon, Secureworld и HTCIA International.

ПРЕДИСЛОВИЕ

Социальная инженерия – чрезвычайно опасный вектор атаки! Он часто используется как средство доставки вредоносного ПО или проникновения в сеть, но иногда это конечная цель, например в атаках, направленных на то, чтобы обманным путем заставить жертву предоставить доступ к своему банковскому счету. Причина катастрофических последствий, которые влечет за собой социальная инженерия, заключается в том, что, если не считать фишинга, ее очень трудно обнаружить. Независимо от того, начинаете ли вы свой путь в индустрии информационной безопасности, являетесь опытным пентестером или занимаетесь защитой, вы, скорее всего, рано или поздно столкнетесь с социальной инженерией.

Изучение «почему?» и «как?» социальной инженерии расширит ваше понимание отрасли информационной безопасности, поможет вам построить более эффективные рабочие процессы, а также позволит определить бреши в защите жертв и выполнить успешную атаку. Ответ на вопрос «как?» со временем меняется, но вопрос «почему?» уходит своими корнями в сотни, если не тысячи лет истории человечества.

Для кого эта книга

Эта книга предназначена для всех, кто хочет лучше понять, что такое социальная инженерия и как проводятся успешные атаки. Эта книга для вас, если вы:

- новичок в индустрии информационной безопасности;
- опытный специалист по тестированию на проникновение или сотрудник красной команды;

- сотрудник службы кибербезопасности или член синей команды;
- руководитель или менеджер, которому поручено разработать программы обнаружения нарушений безопасности или повышения квалификации персонала для вашей организации.

Что вы найдете в этой книге

Эта книга состоит из трех ключевых разделов.

Основы

Здесь мы обсуждаем различные виды деятельности, составляющие социальную инженерию, и психологические концепции, лежащие в основе дисциплины. Отдельная глава посвящена этическим соображениям социальной инженерии.

В отличие от традиционного тестирования на проникновение, которое нацелено на данные и системы, тесты на проникновение с помощью социальной инженерии нацелены на людей и поэтому требуют исключительной осторожности.

Наступательная социальная инженерия

Здесь говорится о том, как проводить атаку с применением социальной инженерии. Мы начнем со сбора информации OSINT, анализа ее полезности в атаках социальной инженерии и того, как ее собрать с помощью ряда профессиональных инструментов. Затем рассмотрим изощренную фишинговую атаку, предназначенную для кражи учетных данных пользователей, обращая внимание на множество уловок, используемых для обмана как пользователей, так и защитников. Мы также расскажем, как измерить последствия вашей атаки и сообщить о ее серьезности вашему заказчику.

Защита от социальной инженерии

В этом разделе мы рассуждаем с точки зрения защитника. Мы обсудим многочисленные методы опережающей защиты вашей команды от атак социальной инженерии, а также стратегии быстрого восстановления после успешной атаки. Мы также изучим технические элементы управления электронной почтой и инструменты для анализа потенциально подозрительных электронных писем.

Один из этих разделов может быть более актуальным для вас (и вашей текущей должности или намерений), чем другие, но я рекомендую прочитать всю книгу, чтобы лучше понять, чего ожидать от противоположной стороны.

Вывод

Эта книга не является универсальным ресурсом для изучения социальной инженерии. После прочтения вы можете продолжать пользо-

ваться ей в качестве справочника или дополнения к другому материалу. Вы должны продолжать изучать психологию, социологию и взаимодействие человека с компьютером, чтобы не отстать от злоумышленников, которые тоже непрерывно совершенствуют свои навыки в социальной инженерии. Эта область безопасности и связанные с ней исследования постоянно развиваются.

Теперь давайте, наконец, перейдем к делу!

ЧАСТЬ I

ОСНОВЫ

1

ЧТО ТАКОЕ СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ?

Социальная инженерия (social engineering) – это любая атака, которая использует человеческую психологию для воздействия на цель, заставляя ее либо выполнить нужное действие, либо предоставить секретную информацию. Эти атаки играют важную роль в индустрии информационной безопасности и хакерском сообществе, но мы регулярно встречаем примеры подобного поведения в своей повседневной жизни.

Например, отделы продаж и маркетинга часто используют тактику социальной инженерии. Продавец, который обзванивает потенциальных клиентов, может попытаться повлиять на людей на другом конце линии, предложив решения их проблем. Дети часто ссылаются на «крутых ребят», чтобы добиться желаемого у своих родителей, в то время как родители могут преувеличивать негативный эффект от неправильного поведения ребенка (вспомните, какими последствиями вас пугали взрослые, если вы будете есть много сладкого).

Многие из тех, кто читает эту книгу, вероятно, отвечали на звонок «службы безопасности банка» или получали электронное письмо от «нигерийского принца». Многие люди, в том числе и я, получали фишинговые письма с угрозами взлома почтового ящика и предложения обновить пароли от соцсети на поддельном сайте.

Эта книга научит основам социальной инженерии с точки зрения *пентестера*[1]. Представленные здесь концепции помогут вам лучше понять, как использовать социальную инженерию с *этической* точки зрения, копируя тактику злоумышленника, чтобы обнаружить слабые места в системе безопасности, которые вы сможете исправить позже. В отличие от настоящих злоумышленников у вас будет разрешение на проведение атак социальной инженерии, и вы не будете намеренно причинять вред объектам атаки.

Важные понятия социальной инженерии

В следующих разделах описаны компоненты социальной инженерии, включая наиболее распространенные виды атак. Как пентестер, вы можете применить любую из них, но я обычно придерживаюсь строгих этических ограничений, избегая использования личных ресурсов сотрудников, включая их мобильные устройства, учетные записи в социальных сетях и домашние компьютеры. Плохие парни редко ограничивают себя моралью, но это не означает, что вы должны подражать им во всем, когда проводите тестирование! Мы обсудим этот момент в главе 2.

Предлог

Согласно концепции социальной инженерии *предлог* (pretexting) – это акт выдачи себя за кого-то. Вы можете надеть чужую униформу, рассказать выдуманную предысторию или создать фиктивный повод для контакта. Я использую этот термин для обозначения любого вашего предлога для разговора с жертвой. Если, например, вы заявили охраннику на проходной, что работаете в компании по обслуживанию мусорных баков, держите в руках блокнот и одеты в униформу компании – это и есть предлог.

Разведка по открытым источникам

Разведка по открытым источникам (open source intelligence, OSINT) – это сбор информации о вашей цели из общедоступных ресурсов. Источники OSINT включают газеты, поисковые системы, документы из различных регулирующих органов, социальные сети, рекламу и обзорные сайты, и это неполный перечень. OSINT поможет вам придумать повод для контакта.

[1] Пентест (pentest) – это сокращение от *penetration test*, т. е. тест на вторжение в закрытую область (например, в корпоративную сеть). Пентестер – это специалист по информационной безопасности, которого нанимают для проверки надежности защиты от вторжений. – *Прим. перев.*

OSINT может поддержать или разрушить ваши усилия по социальной инженерии, потому что для достижения успеха вам часто нужно знать важные подробности о компании-жертве и ее сотрудниках. Какую виртуальную частную сеть (VPN) они используют? Какие еще технологии они применяют в своей работе? Какова физическая планировка здания организации? Зная эту информацию, вы сможете значительно упростить взаимодействие. Несколько ведущих специалистов по тестированию на проникновение сказали мне, что оптимальное отношение времени, затрачиваемого на сбор данных OSINT, к времени, затраченному на фактическое проникновение, колеблется от 30/70 до 70/30.

Фишинг

Вероятно, это наиболее распространенная форма социальной инженерии. *Фишинг* (ловля рыбы) – это отправка мошеннических электронных писем с целью повлиять на жертву или заставить ее предоставить информацию, открыть файлы или перейти по ссылкам. Позже в этой книге я расскажу о различных методах, которые вы можете использовать для этого.

Обычные фишинговые электронные письма, как правило, не адресованы какому-либо конкретному получателю. Вместо этого их рассылают по обширным спискам адресов электронной почты, купленным мошенниками и преступниками. Это означает, что вы можете отправить электронное письмо большому количеству людей, не собирая о них OSINT. Например, почти не владея контекстом жертвы, вы можете разослать одинаковое для всех электронное письмо, которое попытается заставить пользователя либо войти на мошеннический веб-сайт, либо загрузить файл. Когда жертвы открывают файл, на их компьютере может открыться удаленный доступ к оболочке командной строки или произойдет установка вредоносной программы. После того как злоумышленники запустили удаленную оболочку или установили вредоносное ПО, они могут в интерактивном режиме взаимодействовать с системой и выполнять атаки на запуск эксплойтов и повышение привилегий, чтобы продолжить компрометацию системы и сети.

Иногда *наборы эксплойтов* (программное обеспечение, используемое для совершения других атак и загрузки вредоносных программ) используют фишинг для распространения вредоносного ПО. Согласно отчету Symantec Internet Security Threat Report (ISTR) за 2018 год, 0,5 % всего URL-трафика являются фишинговыми, а 5,8 % этого трафика – вредоносными. Это 1 из 224 всех URL-адресов!

Тем не менее простые фишинговые атаки, подобные описанной выше, не распространены в этическом взломе и тестировании на проникновение. Если клиент нанимает вас для проведения теста на проникновение, можно с уверенностью предположить, что он достаточно компетентен в области безопасности, чтобы избежать простой фишинговой атаки.

Целевой фишинг

Целевой фишинг – это разновидность обычного фишинга, при котором специалист по социальной инженерии фокусируется на конкретной цели. Если бы вы были рыбаком, использующим копье, а не сеть, вам, вероятно, нужно было бы знать, как ведет себя каждый вид рыб и как к ним подходить. Точно так же вам, как пентестеру, нужно будет собирать, объединять и использовать OSINT о вашей целевой компании или человеке, чтобы должным образом заманить их в ловушку.

ISTR заявляет, что целевой фишинг является вектором номер один в целевых атаках. По оценкам отчета за 2018 год, 71 % организованных групп, включая национальные разведки, киберпреступников и хактивистов, используют целевой фишинг для достижения своих целей. В 2019 году этот показатель упал до 65 %.

Если бы вы были пентестером с уклоном в социальную инженерию (или консультантом в фирме, где другие компании платят вам за то, чтобы вы выступали в роли злоумышленников), то, вероятно, тратили бы большую часть своего рабочего времени на разработку целевого фишинга. Это наиболее распространенные атаки, с которыми сталкиваются компании, и они требуют наименьшего количества прямого взаимодействия, что делает их более доступными для потенциальных клиентов.

Вы бы начали с OSINT-расследования в направлении компании-жертвы или конкретного человека. Например, можете раздобыть информацию о поставщиках услуг, которыми они пользуются. Затем – создать фишинговое электронное письмо, в котором сказано, что вы являетесь представителем страховой компании и хотите уточнить некоторые данные. Вы бы вставили логотип страховой компании в электронное письмо вместе с формулировками, характерными для таких компаний, а затем отправили жертву на клон реального веб-сайта компании, чтобы попытаться получить их учетные данные или заставить их загрузить файл.

Вейлинг

Вейлинг (*whaling*, китобойный промысел) – это фишинг, направленный на «большую рыбу» – как правило, топ-менеджеров компании. Во время проведения тестов на проникновение с помощью социальной инженерии я обнаружил, что эти люди вызывают больше доверия, чем многие другие. Они также обычно имеют больше прав доступа, чем средний пользователь. Например, они могут быть локальными администраторами в системе компании. Вам нужно подходить к атакам на этих людей иначе, чем к фишингу или целевому фишингу, потому что у этих людей другие мотивы и интересы, чем, скажем, у рядовых сотрудников службы поддержки или отдела продаж.

Представьте, что ваша цель – финансовый директор компании. Можете попытаться изготовить вейлинговое письмо от имени отдела кадров, чтобы установить дополнительные отношения с потенциаль-

ной жертвой. Вы можете персонализировать письмо, упомянув имя и должность, или затронуть другие ключевые особенности компании-жертвы, которые должен знать только получатель или отдел кадров. Или вам, возможно, придется задействовать совершенно другой сценарий, включающий торговую организацию или профессиональную группу, к которой принадлежит ваша цель. OSINT может послужить источником профессионального жаргона, чтобы сойти за своего.

Вишинг

При *вишинге* (*vishing*) злоумышленник звонит жертве и разговаривает с ней по телефону. Вишинг часто сложнее, чем фишинг, потому что требует навыков импровизации. В то время как фишинг дает вам время подумать о том, что вы хотели бы сказать, прежде чем отправить электронное письмо, при вишинге вам нужно составлять разговор на ходу и постоянно держать его в голове вплоть до малейших деталей. У вас также может возникнуть куча проблем: жертва не отвечает на звонок; вы неправильно поняли, кто кому подчиняется в компании; вы случайно позвонили от имени человека, который сидит в одном кабинете с жертвой, или использовали неправильный акцент или пол.

Преимущество вишинга в том, что вы сразу видите результат своей атаки. Отправляя электронное письмо, вам нужно дождаться, пока получатель откроет сообщение, перейдет по ссылке и введет данные. Хотя для этого требуется больше времени, чем при фишинге (особенно, когда потенциальных жертв много), вы можете нанести гораздо больший ущерб за более короткий период с помощью успешной вишинговой кампании.

Во время этих встреч вы, вероятно, будете подменять номер телефона с помощью специального приложения или другого программного обеспечения и звонить кому-то под определенным предлогом. Во время звонка вы устанавливаете взаимопонимание со своей жертвой, а затем пытаетесь заставить ее выполнить действие или предоставить информацию.

Можете сказать, что занимаетесь проведением опроса, или заявить, что вы являетесь клиентом, поставщиком или покупателем. Вы спросите у них информацию, относящуюся к вашему предлогу, а затем задокументируете ее в своем отчете.

Будьте осторожны при записи этих звонков. Постарайтесь получать и фиксировать только минимально необходимую служебную информацию, которая не подпадает под законы о разглашении персональных данных медицинской или банковской тайны. Прежде чем проводить какое-либо тестирование таким образом, предусмотрительный тестировщик или фирма должны проконсультироваться с юристом, чтобы убедиться, что все действия законны.

Приманка

Иногда, чтобы заставить жертву выполнить нужное действие, можно воспользоваться *приманкой*. Традиционно в этом качестве применя-

ли USB-накопители, но теперь можно воспользоваться и более современным вариантом в виде QR-кода, чтобы заставить жертву скачать вредоносный код.

Вы можете загрузить поддельные документы на USB-накопитель или в специальное устройство, которое хакеры называют Rubber Ducky[1] («резиновая уточка»), а затем положить это устройство в пакет с привлекательной надписью типа «список на увольнение/повышение», «выплата бонусов», «доклад генеральному директору» и т. п. Затем подбросьте приманку на парковку, у входа в офис или в коридоре компании-жертвы.

Использование «резиновой уточки» имеет свои преимущества. С помощью этого устройства вы можете загружать вредоносные скрипты на устройство вместе с законными файлами. Когда кто-то подключает «уточку» к компьютеру, она обходит любые инструменты предотвращения потери данных (программные или аппаратные решения, которые предотвращают перемещение файлов с компьютера через USB-накопитель, электронную почту или протокол, такой как FTP или SCP), поскольку выдает себя за USB-клавиатуру. Если вы используете обычный USB-накопитель, вас может остановить программное обеспечение для предотвращения потери данных, установленное на компьютере жертвы. В отличие от него «уточка» откроет файл и развернет *полезную нагрузку* (скрипт или инструмент, помогающий получить желаемый результат).

Можно использовать приманку, чтобы получить удаленный доступ к оболочке командной строки в системе, что впоследствии позволит вам напрямую взаимодействовать с хост-компьютером. Но с приманкой непросто достичь успеха, потому что трудно гарантировать, что она достанется жертве и что оболочка, подключения или информация с рабочего компьютера окажутся в пределах вашего доступа. Люди могут взять диск домой и подключить его к домашнему компьютеру, на атаку которого у вас не будет разрешения.

Мусорные баки

Вероятно, наименее привлекательный прием социальной инженерии – это копание в содержимом мусорных баков или в мешках с мусором, собранным в офисе компании-жертвы, а затем вывоз их за пределы офиса для анализа и сбора информации. Вы можете многое узнать об организации и найти именно то, что искали. Вспомните о вещах, которые сами выбрасываете. Некоторые из них чрезвычайно личные. Впрочем, мешки с мусором могут быть наполнены объедками из офисного кафетерия, не имеющими отношения к секретам компании.

Для этого типа разведки вам, скорее всего, придется притвориться сотрудником мусорной компании и придумать какую-то историю, чтобы добраться до местной помойки. Оказавшись там, первым де-

[1] Rubber Ducky Hak5 – это устройство с микрокомпьютером внутри, заключенное в корпус, идентичный обычному USB-накопителю, которое действует как клавиатура и может вводить данные в систему так, как если бы пользователь печатал их сам.

лом соберите несколько мешков с мусором, вынесите их за пределы офиса и спокойно изучите содержимое.

Ковыряясь в мусорных контейнерах, вероятно, захочется использовать перчатки и респиратор. Вы даже можете стимулировать местную экономику и нанять старшеклассников или студентов для выполнения грязной работы. Делайте заметки о том, что нашли, читайте любые письменные материалы и склеивайте обратно все разорванные документы. Найденное вами может оказаться как окончательной целью проникновения, так и ступенькой к чему-то большему.

Психологические концепции в социальной инженерии

В отличие от традиционной информационной безопасности, которая заимствует концепции из информатики, системного администрирования, программирования и администрирования баз данных, социальная инженерия заимствует большинство своих концепций из психологии. По этой причине специалисты в области социальной инженерии должны хорошо разбираться в психологии и человеческом поведении.

Работая над докторской диссертацией (которую так и не закончил), я тратил больше времени на чтение психологических и социологических журналов, чем журналов по компьютерным технологиям. Я до сих пор время от времени просматриваю толстую папку, полную научных статей, и использую доступ к академическим журналам для получения новой информации. В этом разделе я рассматриваю некоторые основные психологические концепции, полезные для социальной инженерии.

Влияние

Влияние – это нейтральный термин, обозначающий деятельность человека, которая побуждает других к определенному результату. Влияние может быть положительным или отрицательным. Примером влияния может служить врач, беседующий с пациентом о его состоянии здоровья, изменениях в образе жизни, которые он должен предпринять, и рисках, с которыми он сталкивается, чтобы вдохновить пациента вести более здоровый образ жизни.

Манипуляции

За пределами мира психологии люди обычно не видят разницы между *манипуляцией* и влиянием. Но среди специалистов эти термины имеют совершенно разные значения. Манипуляция – это пагубное влияние, обычно направленное на причинение вреда. В социальной инженерии как злоумышленники, так и благонамеренные пентестеры часто используют манипуляции вместо влияния из-за недостаточной подготовки или по недомыслию.

Взаимопонимание (раппорт)

Если коротко, *взаимопонимание* – это взаимное доверие. Большинство словарей определяют взаимопонимание как «дружеские, гармоничные отношения» и добавляют, что такие отношения обычно «характеризуются соглашением, взаимным доверием или сопереживанием, которые делают общение возможным или легким». Американская психологическая ассоциация (АПА) основывается на этом определении, говоря, что «установление взаимопонимания с клиентом в психотерапии часто является важной промежуточной целью для терапевта, чтобы облегчить и углубить терапевтический опыт и способствовать оптимальному прогрессу и улучшению».

Как и психотерапевты, специалисты по социальной инженерии пытаются установить контакт со своими объектами для завоевания их доверия. Чтобы построить взаимопонимание, они часто полагаются на общий опыт (реальный или выдуманный), играют на интересах жертвы и подчеркивают свои собственные черты характера. Вы можете использовать OSINT, чтобы узнать о симпатиях и антипатиях жертвы.

Шесть принципов влияния доктора Чалдини

В своей книге «Психология влияния» психолог Роберт Чалдини подробно описывает взаимосвязь между влиянием и манипуляцией. Доктор Чалдини выделяет шесть основных принципов влияния: *авторитет*, *привлекательность*, *срочность и дефицит*, *постоянство и последовательность*, *социальное доказательство*, *взаимность*.

Рассмотрим подробнее эти принципы и их применение.

Авторитет

Люди склонны совершать определенные действия, когда кто-то, наделенный властью, просит их об этом или когда их заставляют поверить (правдиво или под ложным предлогом), что такое же действие совершает авторитетная фигура. Мне нравится использовать в вишинге ссылки на авторитеты. Например, я могу позвонить и сказать, что действую по распоряжению генерального директора, директора по информационной безопасности или в соответствии с определенным законом.

Использование авторитета может быть очень эффективным. Имейте в виду, однако, что вы никогда не должны прикидываться сотрудником правоохранительных органов, налоговой службы, таможни и других государственных организаций, обладающих особыми полномочиями на сбор конфиденциальной и иной информации. Это незаконно!

Привлекательность

Люди, как правило, стремятся помочь тем, кого считают милым и привлекательным. Вы когда-нибудь встречали продавца, который хотя бы не пытался выглядеть приятным человеком? Скорее всего,

он будет делать вам комплименты по поводу одежды, внешности и интеллекта, чтобы завоевать ваше расположение.

Срочность и дефицит

Если есть риск, что человек чего-то не получит, он начинает хотеть этого намного сильнее. Недавно я воспользовался рекламной акцией местного спортзала. В процессе регистрации на странице сайта появился таймер, предупреждающий меня о том, что осталась одна минута, чтобы завершить процедуру, иначе я буду исключен из списка льготных клиентов. В качестве эксперимента я прошел процедуру регистрации трижды. Первые два раза я проделал регистрацию с одного и того же IP-адреса в течение минуты. В третий раз потратил около пяти минут, и таймер просто сбрасывался без последствий каждый раз, когда минута заканчивалась.

Мораль этой истории: спортзал пытался использовать *срочность*, чтобы заставить меня подписаться на что-то, что могло принести мне пользу, а могло и не принести. Таймер дает потенциальным клиентам искусственное ограничение по времени и ощущение, что они потеряют что-то важное, если не будут действовать быстро.

Занимаясь фишингом, многие мошенники заявляют, что продают или раздают что-то такое, чего существует лишь небольшое количество. Чтобы соблазнить жертву действовать, будь то переход по ссылке или ввод информации, они предлагают нечто ценное в сделке, которая слишком хороша, чтобы быть правдой, но с оговоркой, что жертва должна действовать в кратчайший срок.

В других случаях преступник может попытаться заставить заплатить выкуп за свою программу-вымогатель, выделяя жертве всего несколько часов на оплату, прежде чем безвозвратно удалить, украсть или обнародовать данные, – независимо от того, собирается ли он исполнить угрозу. В любом случае преступник надеется напугать жертву и заставить ее действовать до того, как она успеет все обдумать.

Постоянство и последовательность

Люди ценят постоянство и в большинстве своем не любят перемены. Специалисты по социальной инженерии иногда остаются последовательными, а иногда нарушают постоянство и последовательность, чтобы влиять на жертву. Продавец может утверждать, что больше заинтересован в успехе своего клиента, чем в комиссионных, говоря что-то вроде: «Я всегда заботился о своих клиентах. Я понимаю ваши потребности с первого дня сотрудничества. Я всегда работаю с вами по принципу “что обещано, то и сделано”». Этот прием распространен среди продавцов, успех которых зависит от прочных долгосрочных отношений.

Социальное доказательство

Общество требует от нас «не отставать от соседа». Другими словами, мы часто делаем что-то исключительно потому, что остальные счи-

тают это нормальным, уместным или статусным. Вы можете попытаться убедить свою жертву в том, что определенное поведение или действие повышает социальный статус или что все другие эффективные сотрудники выполняют некое нужное вам действие. Убеждение собеседника в желательности чего-либо называется *социальным доказательством*. Продавец автомобилей может попытаться уговорить вас купить роскошную машину, сказав, например, что на ней ездят успешные люди вашего возраста.

Злоумышленник может придумать социальное доказательство, используя информацию, полученную из OSINT. Например, он может определить, кто в компании является влиятельным лицом. Затем отправит вам электронное письмо, утверждая, что разговаривал с авторитетным человеком, который восторженно отзывался о вас и предоставил вашу контактную информацию, чтобы вы помогли «решить проблему». Я встречал двух или трех не очень умных рекрутеров, которые писали мне по электронной почте, утверждая, что мой друг дал им мою контактную информацию, но просил не называть его имя. Вакансии, что они предлагали, были связаны с Java-разработкой, о которой я не упоминаю ни в своем резюме, ни в LinkedIn. Разумеется, я сразу внес их в черный список.

Взаимность

Мы более охотно помогаем людям, которые помогли нам. Часто социальные пентестеры помогают кому-то, а затем просят сделать что-то взамен (и не всегда это в интересах того, кто помогает). Один из таких случаев произошел со мной, когда я посетил *Layer 8 Conference*, конференцию по социальной инженерии в Ньюпорте, Род-Айленд. Рядом с пирсом я увидел пару, которая пыталась сфотографироваться на фоне парусника. Я предложил их сфотографировать.

«А вас это точно не затруднит?» – спросили они.

«Нисколько. И кстати, подержите мой телефон, чтобы знать, что я не убегу с вашим», – ответил я, чтобы наладить с ними более тесный контакт.

Я сделал снимок. В этот момент прямо за этой парой проплыла еще одна красивая яхта, и я попросил их не сходить с места. «Давайте я сфотографирую вас еще раз на фоне этой яхты», – сказал я.

Они согласились: «Это было бы круто».

Я сделал еще несколько снимков. Закончив, я передал им телефон, чтобы они могли просмотреть снимки, а мои новые знакомые поблагодарили меня.

«Пустяки, не за что. Не найдется ли у вас минутка, чтобы помочь мне с антропологическим исследованием, которое я провожу этим летом?» – поинтересовался я.

«Конечно, а что это за исследование?» – спросили они в ответ.

Поскольку я помог им сфотографироваться, они чувствовали себя обязанными отплатить взаимностью, даже несмотря на то, что ответы на мои вопросы не сулили им никакой выгоды.

«Я провожу исследование о характере миграции людей и о том, как смешиваются разные этнические группы. Собираю информацию об именах, о том, где путешествуют эти люди, о моделях поведения и так далее. Увы, у меня очень мало информации о родителях членов тех семей, с которыми я беседовал. Например, как звали вашу маму до того, как она вышла замуж?»

Заметьте, я не спросил «Какой была девичья фамилия вашей матери?», потому что этот вопрос моментально вызывает тревогу. Это распространенный вопрос для восстановления пароля, и люди защищают эту информацию.

Они оба ответили на мой вопрос, а потом рассказали, откуда они. Я сказал, что у меня в этом городе есть друзья. Это была ложь – на самом деле я просто был смутно знаком с этой местностью. Я сообщил, что мои друзья ходили в одну среднюю школу в том городе. Они ответили, что эта школа конкурировала с той, в которой учились они.

«А что было изображено на гербе вашей школы?» – спросил я.

Мои собеседники охотно ответили и на этот вопрос. Я мог бы продолжать расспросы еще очень долго…

Симпатия или эмпатия?

Отличным способом установить взаимопонимание является проявление *симпатии* – это забота о человеке, который чувствует себя плохо или испытывает стресс, например после потери любимого человека или домашнего животного. В отличие от симпатии *эмпатия* – это способность испытывать те же чувства, что и другие люди, как будто вы оказались на их месте. Эмпатия означает *общие* эмоции или точки зрения, тогда как симпатия выражает сочувствие и заботу с вашей стороны.

То и другое важно для установления взаимопонимания при определенных обстоятельствах. Вы должны уметь выражать свои чувства и понимать чувства жертвы, иметь возможность оказывать влияние и знать, когда вы заходите слишком далеко. Взаимодействуя с жертвой, можете поделиться историей (будь то реальность, вымысел или какая-то приукрашенная комбинация) о похожей ситуации, в которой вы оказались, и о том, как вы себя чувствовали при этом. Это позволит им проявить встречное сочувствие к вашей ситуации и улучшит ваше взаимопонимание. В качестве альтернативы, если кто-то рассказывает о ситуации, к которой вы не имеете никакого отношения, просто задавайте уточняющие вопросы, а потом скажите, что вы сожалеете о том, что это произошло, выражая таким образом сочувствие. Однако будьте осторожны: если у вас есть наготове ответ или история абсолютно на все, что вам рассказывает человек, у него могут возникнуть подозрения, поэтому используйте этот подход с осторожностью.

Вывод

Социальная инженерия может быть невероятно мощным инструментом для получения доступа к чужим секретам. В этой главе вы по-

знакомились с целым рядом приемов, многие из которых мы рассмотрим более подробно на протяжении всей книги.

Имейте в виду, что взаимопонимание – это особая игра. После того как вы установили взаимопонимание, остальная часть взаимодействия будет проще. Понимание психологических концепций и принципов человеческого поведения является одним из полезных способов установить связь с кем-то. Кроме того, чем больше OSINT вы соберете, тем умнее сможете говорить о компании-жертве. Можно найти идеальные поводы для установления контакта с сотрудниками, а также узнать о культуре, процессах и технологиях, которые облегчат последующий пентестинг или взаимодействие с красной командой. Иметь взаимопонимание полезно независимо от того, занимаетесь ли вы фишингом, целевым фишингом, вейлингом, вишингом, разбрасываете приманки или роетесь в мусорных баках.