

*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 .....	10
Об авторах .....	11
О техническом рецензенте .....	11
Благодарности .....	12
Предисловие .....	14
<b>Часть I. Основы .....</b>	<b>17</b>
<b>Глава 1. Что такое социальная инженерия? .....</b>	<b>18</b>
Важные понятия социальной инженерии .....	19
Предлог .....	19
Разведка по открытым источникам .....	19
Фишинг .....	20
Целевой фишинг .....	21
Вейлинг .....	21
Вишинг .....	22
Приманка .....	22
Мусорные баки .....	23
Психологические концепции в социальной инженерии .....	24
Влияние .....	24
Манипуляции .....	24
Взаимопонимание (раппорт) .....	25
Шесть принципов влияния доктора Чалдини .....	25
Симпатия или эмпатия? .....	28
Вывод .....	29
<b>Глава 2. Этические соображения в социальной инженерии .....</b>	<b>30</b>
Этическая социальная инженерия .....	31
Соблюдение границ .....	31
Понимание юридических аспектов .....	32
Особенности предоставления услуг третьей стороны .....	32
Подведение итогов после вторжения .....	33
Практический пример: социальная инженерия зашла слишком далеко .....	34
Этические рамки OSINT .....	34
Защита данных .....	35
Соблюдение законов и правил .....	36
Практический пример: этические ограничения социальной инженерии .....	38
Вывод .....	40
<b>Часть II. Наступательная социальная инженерия .....</b>	<b>41</b>
<b>Глава 3. Подготовка к атаке .....</b>	<b>42</b>
Согласование с клиентом .....	43
Ознакомление с задачей .....	43
Определение целей .....	44
Определение методов .....	44

Разработка удачных предлогов .....	45
Использование специализированных ОС для социальной инженерии .....	46
Последовательные фазы атаки .....	47
Практический пример: почему изучение задачи имеет значение .....	51
Вывод .....	52
<b>Глава 4. Бизнес-разведка по открытым источникам .....</b>	<b>53</b>
Практический пример: почему OSINT имеет значение .....	54
Разберемся с типами OSINT .....	54
Сбор данных OSINT об организации .....	55
Получение базовой бизнес-информации из Crunchbase .....	55
Идентификация владельцев веб-сайтов с помощью WHOIS .....	59
Сбор OSINT из командной строки с помощью Recon-ng .....	60
Вывод .....	71
<b>Глава 5. Социальные медиа и публичные документы .....</b>	<b>72</b>
Анализ социальных сетей для сбора OSINT .....	72
LinkedIn .....	73
Доски объявлений и карьерные сайты .....	76
Facebook (Meta) .....	77
Instagram .....	80
Использование Shodan для OSINT .....	83
Использование параметров поиска Shodan .....	84
Поиск IP-адресов .....	84
Поиск доменных имен .....	84
Поиск имен хостов и субдоменов .....	85
Делаем автоматические скриншоты с помощью Hunchly .....	86
Вывод .....	87
<b>Глава 6. Сбор OSINT о людях .....</b>	<b>89</b>
Использование инструментов OSINT для анализа адресов электронной почты .....	89
Выяснение того, был ли пользователь взломан .....	90
Составление списка учетных записей социальных сетей с помощью Sherlock .....	91
Составление списка учетных записей веб-сайтов с помощью WhatsMyName .....	91
Анализ паролей с помощью Pwdlogy .....	92
Анализ изображений цели .....	93
Ручной анализ данных EXIF .....	94
Анализ изображений с помощью ExifTool .....	95
Анализ социальных сетей без инструментов .....	98
LinkedIn .....	98
Instagram .....	98
Facebook .....	98
Twitter .....	98
Пример из практики: неожиданно информативный ужин .....	99
Вывод .....	100
<b>Глава 7. Фишинг .....</b>	<b>102</b>
Настройка фишинговой атаки .....	102
Настройка защищенного экземпляра VPS для фишинговых целевых страниц .....	104
Выбор платформы электронной почты .....	112

Покупка доменов для рассылки и целевых страниц .....	114
Настройка инфраструктуры фишинга и веб-сервера.....	115
Дополнительные действия для успешного фишинга.....	116
Использование пикселей отслеживания .....	116
Автоматизация фишинга с помощью Gophish .....	117
Добавление поддержки HTTPS для фишинговых целевых страниц .....	122
Использование сокращенных URL-адресов в фишинге .....	123
Использование SpoofCard для спуфинга вызовов .....	123
Соглашение о сроках проведения атаки.....	123
Практический пример: серьезный фишинг за 25 долларов .....	124
Вывод.....	127
<b>Глава 8. Клонирование целевой страницы.....</b>	<b>128</b>
Пример клонированного сайта.....	129
Страница входа .....	129
Страница критичных вопросов.....	132
Клонирование веб-сайта .....	135
Поиск страниц входа и профиля пользователя .....	135
Клонирование страниц с помощью HTTrack .....	135
Изменение кода поля входа .....	137
Добавление веб-страниц на сервер Apache.....	139
Вывод.....	140
<b>Глава 9. Обнаружение, измерение и отчетность .....</b>	<b>141</b>
Обнаружение .....	142
Измерение.....	142
Выбор показателей .....	143
Отношения, медианы, средние значения и стандартные отклонения .....	143
Количество открытий писем электронной почты .....	144
Количество переходов .....	146
Ввод информации в формы.....	147
Действия жертвы.....	149
Время обнаружения .....	149
Своевременность корректирующих действий.....	150
Эффективность ответных действий .....	150
Количественная оценка риска.....	151
Составление отчетов .....	152
Знайте, когда звонить по телефону .....	152
Написание отчета.....	153
Вывод.....	155
<b>Часть III. Защита от социальной инженерии .....</b>	<b>157</b>
<b>Глава 10. Опережающие способы защиты .....</b>	<b>158</b>
Программы повышения осведомленности.....	159
Как и когда проводить обучение.....	159
Некарательная политика .....	160
Поощрение за хорошее поведение .....	161
Проведение фишинговых кампаний.....	161
Репутация и OSINT-мониторинг .....	162
Реализация программы мониторинга.....	162
Аутсорсинг .....	163

Реагирование на инциденты.....	163
Процесс реагирования на инциденты по версии SANS .....	164
Реагирование на фишинг .....	166
Реагирование на вишинг .....	166
Реагирование на сбор OSINT.....	167
Управление вниманием СМИ.....	168
Как пользователи должны сообщать об инцидентах .....	168
Технический контроль и изоляция .....	169
Вывод.....	169
<b>Глава 11. Инструменты управления электронной почтой .....</b>	<b>171</b>
Стандарты .....	171
Поля «От кого».....	172
Стандарт DKIM .....	172
Инфраструктура политики отправителя .....	178
Аутентификация сообщений на основе домена, отчетность и соответствие.....	181
Уровень шифрования TLS .....	184
MTA-STLS .....	186
TLS-RPT.....	186
Технологии фильтрации электронной почты .....	186
Другие средства защиты.....	187
Вывод.....	188
<b>Глава 12. Методы выявления угроз.....</b>	<b>189</b>
Использование Alien Labs OTX.....	190
Анализ фишингового письма в OTX.....	191
Создание импульса .....	191
Анализ источника электронной почты .....	192
Ввод индикаторов .....	193
Тестирование потенциально вредоносного домена в Вугр .....	197
Анализ загружаемых файлов .....	200
Проведение OSINT для анализа угроз.....	201
Поиск в базе VirusTotal .....	201
Выявление вредоносных сайтов в WHOIS.....	202
Обнаружение фишинга с помощью PhishTank .....	203
Просмотр ThreatCrowd.....	205
Консолидация информации в ThreatMiner .....	206
Вывод.....	207
<b>Приложение 1. Обзорные таблицы для подготовки контракта .....</b>	<b>209</b>
<b>Приложение 2. Шаблон отчета.....</b>	<b>212</b>
<b>Приложение 3. Сбор рабочей информации .....</b>	<b>218</b>
<b>Приложение 4. Примеры предложений для контакта .....</b>	<b>221</b>
<b>Приложение 5. Упражнения для развития навыков социальной инженерии.....</b>	<b>223</b>
<b>Предметный указатель .....</b>	<b>225</b>

# 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](http://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](mailto: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/](http://dmkpress.com/authors/publish_book/) или напишите в издательство по адресу [dmkpress@gmail.com](mailto: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](mailto: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](mailto: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 WikiLeaks.

## 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 любят 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 Кириш, 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*<sup>1</sup>. 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.

---

<sup>1</sup> 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 копьё, 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 тестирующий 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<sup>1</sup> («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-

---

<sup>1</sup> 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.

Конец ознакомительного фрагмента.

Приобрести книгу можно

в интернет-магазине

«Электронный универс»

[e-Univers.ru](http://e-Univers.ru)