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 ... 10
Об авторах ... 11
О техническом рецензенте ... 11
Благодарности ... 12
Предисловие ... 14

Часть I. Основы ... 17

Глава 1. Что такое социальная инженерия? ... 18
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

Глава 2. Этические соображения в социальной инженерии ... 30
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

Часть II. Наступательная социальная инженерия ... 41

Глава 3. Подготовка к атаке ... 42
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

Глава 4. Бизнес-разведка по открытым источникам ... 53

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

Глава 5. Социальные медиа и публичные документы ... 72

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

Глава 6. Сбор OSINT о людях ... 89

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

Глава 7. Фишинг ... 102

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

Глава 8. Клонирование целевой страницы....128

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

Глава 9. Обнаружение, измерение и отчетность 141

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

Часть III. Защита от социальной инженерии 157

Глава 10. Опережающие способы защиты 158

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

Глава 11. Инструменты управления электронной почтой 171

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-STS 186
TLS-RPT 186
Технологии фильтрации электронной почты 186
Другие средства защиты 187
Вывод 188

Глава 12. Методы выявления угроз 189

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 Burp 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

Приложение 1. Обзорные таблицы для подготовки контракта 209

Приложение 2. Шаблон отчета 212

Приложение 3. Сбор рабочей информации 218

Приложение 4. Примеры предлогов для контакта 221

Приложение 5. Упражнения для развития навыков социальной инженерии 223

Предметный указатель 225