Оглавление

Благодарности 8

Список использованных сокращений 9

От издательства 10

ЧАСТЬ I. НАПАДЕНИЕ. 11

Введение 12

Глава 1. Начало 13

Как провести аудит законно? 13

Методология взлома 14

Этап первый: пассивный и активный сбор информации. 14

Этап второй: сканирование системы 15

Этап третий: получение доступа 15

Этап четвертый: закрепление в системе 15

Этап пятый: скрытие следов пребывания 16

Резюме 16

Глава 2. Получение информации из открытых источников 17

Введение 17

Что искать? 18

Использование Google для сбора информации 18

Ограничение поиска одним сайтом 19

Поиск файлов определенного типа 20

Поиск определенных частей сайта 22

Google Hacking 23

Поиск информации о людях 24

Архивные данные 25

Netcraft 26

Получение информации о домене 26

Автоматизация процесса 30
FOCA 30
Сбор базы данных адресов e-mail 32
recon-ng 34
Упорядочить информацию 38
Резюме 39

Глава 3. Получение информации от сетевых сервисов 40
Введение 40
Сканирование портов 40
Определение активных хостов 41
UDP-сканирование 42
NMAP 43
Получение информации от DNS-сервера 46
Типы записей 46
Взаимодействие с DNS-сервером. 47
MX-записи 47
NS-запросы. 48
Перебор имен. 48
Перебор обратных записей 49
Передача зоны DNS 50
Получение информации с использованием SNMP 52
Получение информации с использованием NetBIOS 54
Null session 56
Работа с электронной почтой 60
Анализ баннеров 61
Получение информации от NTP-сервера 62
Поиск уязвимостей 63
Резюме 65

Глава 4. Атаки на веб-приложения 67
Знакомство с cookie 67
Межсайтовый скриптинг (XSS) 68
Включение локальных или удаленных файлов 72
SQL-инъекции 74
Резюме 87

Глава 5. Социальная инженерия 88
На кого обратить внимание? 88
Фазы атаки 89
Манипулирование людьми 90

Типы атак 91
Social-Engineer Toolkit 94
Резюме 97

Глава 6. Получаем пароли 98
Основные методы 98
Работа со списками паролей 99
Онлайн-атаки 101
Офлайн-атаки 103
Радужные таблицы 106
Резюме 107

Глава 7. Беспроводные сети 108
Краткий обзор Wi-Fi 108
WEP 110
WPA 113
Bluetooth 115
Резюме 117

Глава 8. Перехват информации 119
Пассивный перехват трафика 121
Активный перехват 129
Резюме 132

Глава 9. Обход систем безопасности 134
Системы обнаружения атак 134
Брандмауэры 137
Приманки 140
Резюме 140

Глава 10. Вредоносные программы 142
Вирусы 142
Черви 144
Шпионы 145
Рекламное ПО 145
Троянские кони 145
Практическая часть 146
Резюме 150

Глава 11. Metasploit Framework 151
Интерфейс 151
Вспомогательные модули 154
Эксплойты 158

Полезная нагрузка 160
Практические навыки 165
Резюме 168

Глава 12. Передача файлов 170
TFTP 170
FTP 171
Загрузка файлов с использованием скриптов 172
Резюме 173

Глава 13. Превышение привилегий 174
Локальное повышение прав в Linux 174
Локальное повышение прав в Windows 175
Повышение привилегий в случае некорректной конфигурации прав доступа 177
Резюме 178

Глава 14. Перенаправление портов и туннелирование 179
Перенаправление портов 179
SSH-туннелирование 180
proxychains 182
Резюме 183

Глава 15. Переполнение буфера 184
Атаки, направленные на переполнение буфера 184
Введение 184
Что такое переполнение буфера? 185
Программы, библиотеки и бинарные файлы 187
Угрозы 187
Основы компьютерной архитектуры 188
Организация памяти 188
Разбиение стека (Smashing the stack) 190
Перезапись указателя фрейма 198
Атака возврата в библиотеку 200
Переполнение динамической области памяти 201
Пример нахождения уязвимости переполнения буфера 202
Резюме 211

Глава 16. Собирая все воедино 212
Стандарт выполнения тестов на проникновение 213
Подготовительная фаза 214
Договор о проведении работ 216

Получение разрешения 216
Сбор данных 217
Анализ уязвимостей 218
Моделирование 218
Эксплуатация уязвимостей 219
Постэксплуатационный этап 219
Отчет 220
Зачистка 220

ЧАСТЬ II. ЗАЩИТА 221

Введение 222

Глава 17. Личный пример 223

Глава 18. Бумажная работа 229
Политика безопасности 230
Стандарты 231
Процедуры 232
Инструкции 233
Техническая документация 233

Глава 19. Обучение и тренировки 235
Тренировки 236

Глава 20. Защита от утечки информации 238

Глава 21. Брандмауэры 245

Глава 22. Системы обнаружения вторжения (IDS) 252

Глава 23. Виртуальные защищенные сети (VPN) 257
Компоненты виртуальной частной сети 258
Безопасность VPN 261
Создание VPN из компонентов с открытым исходным кодом 263

Заключение 267