

# Оглавление

<b>Об авторах</b> .....	9
<b>О научном редакторе</b> .....	10
<b>Предисловие</b> .....	11
<b>Введение</b> .....	13
От издательства .....	14
<b>Благодарности</b> .....	15
<b>Глава 1. Подготовка среды для Python</b> .....	16
Установка Kali Linux.....	16
Подготовка Python 3 .....	18
Установка IDE.....	20
Правила оформления кода.....	21
<b>Глава 2. Основные сетевые инструменты</b> .....	24
Работа с сетью в Python в одном абзаце.....	25
TCP-клиент.....	25
UDP-клиент.....	26
TCP-сервер.....	27
Замена netcat.....	28
Написание TCP-прокси.....	36
SSH с применением Paramiko .....	44
Туннелирование по SSH.....	49
<b>Глава 3. Написание анализатора трафика</b> .....	55
Разработка средства обнаружения сетевых узлов по UDP.....	56
Анализ пакетов в Windows и Linux .....	57

---

Декодирование пакетов сетевого уровня.....	59
Декодирование ICMP.....	67
<b>Глава 4. Захват сети с помощью Scapy.....</b>	<b>74</b>
Похищение учетных данных электронной почты.....	75
ARP-спуфинг с использованием Scapy.....	79
Анализ данных в формате pcap.....	86
<b>Глава 5. Веб-хакерство.....</b>	<b>95</b>
Использование веб-библиотек.....	96
Получение структуры каталогов веб-приложений с открытым исходным кодом.....	101
Определение структуры папок методом перебора.....	108
Взлом HTML-формы аутентификации методом перебора.....	113
<b>Глава 6. Расширение прокси Burp Proxy.....</b>	<b>120</b>
Подготовка.....	121
Фаззинг с использованием Burp.....	122
Использование Bing в сочетании с Burp.....	133
Подбор паролей на основе содержимого веб-сайта.....	139
<b>Глава 7. Удаленное управление с помощью GitHub.....</b>	<b>147</b>
Подготовка учетной записи GitHub.....	148
Создание модулей.....	149
Настройка трояна.....	150
Разработка трояна, который умеет работать с GitHub.....	152
<b>Глава 8. Распространенные троянские задачи в Windows.....</b>	<b>158</b>
Кейлоггер для перехвата нажатий клавиш.....	159
Создание снимков экрана.....	162
Выполнение шелл-кода на Python.....	164
Обнаружение виртуальных окружений.....	167
<b>Глава 9. Похищение данных.....</b>	<b>173</b>
Шифрование и расшифровка файлов.....	174
Вывод похищенных данных по электронной почте.....	177
Вывод похищенных данных путем передачи файлов.....	179

Вывод похищенных данных с помощью веб-сервера.....	180
Собираем все вместе.....	184
<b>Глава 10. Повышение привилегий в Windows.....</b>	<b>188</b>
Установка необходимого ПО.....	189
Создание уязвимой хакерской службы.....	190
Создание средства мониторинга процессов.....	192
Привилегии маркеров в Windows.....	195
Наперегонки с чужим кодом.....	198
Внедрение кода.....	202
<b>Глава 11. Методы компьютерно-технической экспертизы</b>	
<b>в арсенале хакера.....</b>	<b>206</b>
Установка.....	207
Сбор общих сведений.....	209
Сбор сведений о пользователе.....	211
Поиск уязвимостей.....	214
Интерфейс volshell.....	215
Пользовательские подключаемые модули для Volatility.....	216
Что дальше.....	224