



Бухарев Р. С.

# ХАКИНГ на Python



+ виртуальный диск с кодом

НИТ  
nit.com.ru

# Содержание

<b>ВВЕДЕНИЕ В МИР ХАКИНГА.....</b>	<b>11</b>
<b>МИФЫ ХАКИНГА .....</b>	<b>16</b>
Миф: взлом секретных баз данных за несколько секунд .....	16
Миф: хакеры всегда действуют в одиночку .....	16
Миф: хакеры всегда используют высокотехнологичное оборудование.....	17
Миф: хакеры всегда действуют в зловредных целях .....	17
Миф: хакеры всегда оставляют ярлыки своих действий.....	17
<b>ОПРЕДЕЛЕНИЯ ТЕРМИНОВ .....</b>	<b>19</b>
Этика хакинга .....	27
<b>КЛЮЧЕВЫЕ ПОНЯТИЯ.....</b>	<b>29</b>
Сетевые технологии .....	29
Языки программирования .....	31
Базы данных .....	33
<hr/>	
<b>ГЛАВА 1. Основы Python для хакинга.....</b>	<b>37</b>
<b>1.1. ПЛАТФОРМЫ ДЛЯ ОБУЧЕНИЯ PYTHON .....</b>	<b>38</b>
Codecademy .....	39
Coursera.....	39
edX.....	39
Udemy.....	40
Khan Academy .....	40
SoloLearn .....	40
DataCamp .....	41
Google's Python Class .....	41
<b>1.2. УСТАНОВКА И НАСТРОЙКА PYTHON .....</b>	<b>42</b>
1.2.1. Загрузка и установка Python.....	43
1.2.2. Основы работы с pip.....	45
1.2.3. Использование виртуальных сред .....	48
<b>1.3. ОСНОВЫ ЯЗЫКА PYTHON .....</b>	<b>51</b>
Переменные и типы данных .....	52
Целочисленные числа (int) .....	53

Задания для практики по разделу .....	56
Числа с плавающей точкой (float) .....	58
Проблемы точности.....	60
Задания для практики по разделу.....	62
Строки (str) .....	63
Операции со строками .....	64
Методы строк .....	65
Задания для практики по разделу.....	67
Списки (list).....	68
Операции со списками.....	68
Методы списков .....	70
Примеры использования списков .....	71
Задания для практики по разделу.....	72
Кортежи (tuple).....	74
Примеры создания кортежей.....	75
Преимущества кортежей.....	77
Использование кортежей в Python .....	77
Примеры использования кортежей .....	77
Задания для практики по разделу.....	78
Словари (dict).....	80
Примеры словарей в Python.....	80
Основные операции со словарями .....	81
Преимущества словарей .....	83
Примеры использования словарей.....	84
Задания для практики по разделу.....	85
<b>1.4. УСЛОВНЫЕ ОПЕРАТОРЫ .....</b>	<b>87</b>
1.4.1. Оператор <i>if</i> .....	88
Задания для практики по разделу.....	89
1.4.2. Оператор <i>elif</i> .....	91
Задания для практики по разделу.....	93
1.4.3. Оператор <i>else</i> .....	95
Задания для практики по разделу.....	97
<b>1.5. ЦИКЛЫ И ИТЕРАЦИИ .....</b>	<b>99</b>
1.5.1. Подробнее о цикле <i>for</i> .....	101
Перебор числовых диапазонов с помощью <i>range()</i> .....	102
Перебор строк.....	102
Использование <i>enumerate()</i> .....	103

Перебор словарей.....	103
Примеры использования цикла <b>for</b> .....	104
Задания для практики по разделу.....	105
1.5.2. Подробнее о цикле <b>while</b> .....	108
Примеры использования цикла <b>while</b> .....	110
Задания для практики по разделу.....	111
<b>1.6. ФУНКЦИИ</b> .....	<b>114</b>
Возврат значений из функции.....	115
Аргументы по умолчанию.....	115
Переменное число аргументов.....	116
Примеры использования функций.....	117
Задания для практики по разделу.....	118
<b>1.7. КЛАССЫ</b> .....	<b>118</b>
Практические примеры.....	120
Задания для практики по разделу.....	121
<b>1.8. SWITCH-CASE В PYTHON</b> .....	<b>122</b>
Практические примеры использования конструкции <b>switch-case</b> в Python.....	123
Задания для практики по разделу.....	125
<b>1.9. РАБОТА С ФАЙЛАМИ</b> .....	<b>126</b>
Примеры работы с файлами в Python.....	127
Задания для практики по разделу.....	128
<b>1.10. РАБОТА С CSV</b> .....	<b>129</b>
Примеры работы с CSV в Python и аналоги уже выше описанных функций.....	132
Задания для практики по разделу.....	134

## ГЛАВА 2. Сетевое программирование на Python.....135

<b>2.1. ОСНОВЫ ДЛЯ СЕТЕВОГО ПРОГРАММИРОВАНИЯ</b> .....	<b>136</b>
Принципы работы сокетов.....	141
Типы сокетов.....	141
Применение сокетов.....	142
Преимущества использования сокетов.....	143
Создание и управление сокетами.....	143
Продвинутые темы в сетевом программировании.....	145

Протоколы и инструменты для анализа и манипулирования сетевым трафиком .....	146
<b>2.2. РАБОТА С СОКЕТАМИ .....</b>	<b>147</b>
2.2.1. Основные шаги для работы с сокетами .....	147
Примеры простого серверного и клиентского приложений..	149
Дополнительные возможности и особенности работы с сокетами.....	150
Задания для практики по разделу.....	152
2.2.2. Создание сокетов .....	153
Семейство адресов (Address Family).....	153
Тип сокета (Socket Type) .....	153
Примеры создания сокетов .....	154
Задания для практики по разделу.....	156
2.2.3. Прослушивание и подключение .....	157
Примеры приложений на прослушивание и подключение..	158
Задания для практики по разделу.....	159
2.2.4. Обмен данными.....	160
Примеры клиента для обмена и отправки сообщений.....	161
Задания для практики по разделу.....	163
<b>2.3. ПРОТОКОЛЫ И АТАКИ НА СЕТЕВОМ УРОВНЕ.....</b>	<b>164</b>
Примеры защиты от атак на сетевом уровне.....	165
2.3.1. ARP-отравление .....	166
Задания для практики по разделу.....	170
2.3.2. Сниффинг трафика .....	171
Основные шаги сниффинга трафика.....	171
Примеры использования снифферов.....	172
Примеры использования снифферов в качестве инструментов.	172
Примеры на Python .....	173
Задания для практики по разделу.....	176
<b>ГЛАВА 3. Веб-хакинг с использованием Python.....177</b>	
<b>3.1. ОСНОВЫ HTTP И HTTPS.....</b>	<b>180</b>
3.1.1. Основные принципы работы HTTP .....	181
3.1.2. Основные принципы работы HTTPS .....	182
3.1.3. Примеры использования HTTP и HTTPS .....	183
3.1.4. Методы запросов.....	184
Задания для практики по разделу.....	189

3.1.5. Анализ заголовков .....	190
Заголовки запроса .....	190
Заголовки ответа .....	191
Общие заголовки .....	191
Значение анализа заголовков .....	192
Инструменты для анализа заголовков.....	192
Задания для практики по разделу.....	193
<b>3.2. ИНСТРУМЕНТЫ ДЛЯ ВЕБ-ХАКИНГА .....</b>	<b>194</b>
Сканеры уязвимостей .....	194
Прокси-инструменты .....	195
Инструменты для взлома паролей.....	195
Инструменты для анализа и извлечения информации .....	196
Практические примеры использования инструментов .....	196
Задания для практики по разделу.....	198
3.2.1. BeautifulSoup и парсинг HTML .....	200
HTML и структура веб-страниц.....	200
CSS и селекторы .....	200
HTTP и веб-запросы.....	200
Работа с API .....	201
Python и его библиотеки.....	201
Этические и правовые аспекты парсинга .....	201
Практические советы и передовые практики .....	202
Установка BeautifulSoup .....	202
Парсинг HTML.....	202
Извлечение данных.....	203
Навигация по дереву элементов .....	203
Полный пример парсинга.....	204
Задания для практики по разделу.....	209
User-Agent .....	212
CAPTCHA .....	214
Пример рабочего процесса с 2Captcha .....	218
Основные аспекты эмуляции человеческого поведения .....	219
Инструменты для эмуляции человеческого поведения.....	220
Пример эмуляции человеческого поведения с помощью Selenium .....	221
3.2.2. Requests для отправки HTTP-запросов .....	225
Задания для практики по разделу.....	227
3.2.3. Selenium для автоматизации веб-браузера .....	227
Задания для практики по разделу.....	232

## ГЛАВА 4. Атаки на приложения.....233

<b>4.1. ОСНОВЫ ПО БАЗАМ ДАННЫХ.....</b>	<b>237</b>
Типы баз данных.....	237
Основные понятия и термины SQL.....	238
Основные элементы SQL.....	239
Нормализация и денормализация данных.....	240
Транзакции и целостность данных.....	241
Запросы SQL.....	241
Управление доступом и безопасностью.....	242
Внедрение SQL-инъекций.....	242
Атаки на сессии пользователей и куки (нет, не атака на печеньки, хотя автору этого бы хотелось).....	243
<b>4.2. SQL-ИНЪЕКЦИИ.....</b>	<b>243</b>
Задания для практики по разделу.....	247
4.2.1. Определение уязвимостей.....	248
Задания для практики по разделу.....	255
4.2.2. Использование SQL-инъекций для атак.....	256
Принципы SQL-инъекций.....	256
Примеры SQL-инъекций.....	256
Пример реализации на Python.....	257
Защита от SQL-инъекций.....	258
Примеры использования SQL-инъекций для атак.....	265
Задания для практики по разделу.....	266
<b>4.3. АТАКИ НА СЕССИИ И КУКИ.....</b>	<b>267</b>
4.3.1. Основы и определения.....	267
4.3.2. Перехват и изменение данных сессий.....	271
4.3.3. Методы обхода механизмов аутентификации.....	276

## ГЛАВА 5. Безопасность, взлом и защита Wi-Fi-сетей.....281

<b>5.1. ОСНОВЫ БЕСПРОВОДНЫХ СЕТЕЙ.....</b>	<b>285</b>
5.1.1. Основные принципы.....	285
5.1.2. Стандарты Wi-Fi.....	286
Пример сканирования доступных сетей с использованием библиотеки <i>pywifi</i> .....	291

Задания для практики по разделу .....	292
5.1.3. Режимы работы беспроводных устройств .....	294
Режим инфраструктуры (Infrastructure Mode) .....	294
Режим ад-хок (Ad-hoc Mode) .....	295
Режим моста (Wireless Bridge Mode) .....	295
Режим повторителя (Repeater Mode) .....	296
<b>5.2. ВЗЛОМ WI-FI-ПАРОЛЕЙ .....</b>	<b>299</b>
5.2.1. Использование инструментов для аудита Wi-Fi .....	301
Aircrack-ng .....	301
Kismet .....	302
Wireshark .....	302
Reaver .....	303
Fern WiFi Cracker .....	303
Scapy .....	304
pywifi .....	305
Wireless .....	305
Scapy-HTTP .....	306
Pyshark .....	306
Задания для практики по разделу .....	311
<b>ГЛАВА 6. Защита от хакинга на Python.....313</b>	
<b>6.1. БИБЛИОТЕКИ ДЛЯ ШИФРОВАНИЯ ДАННЫХ.....</b>	<b>314</b>
<b>6.2. ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ .....</b>	<b>316</b>
6.2.1. Общая концепция .....	316
6.2.2. Методы обнаружения атак.....	319
Системы обнаружения вторжений (IDS).....	319
Системы обнаружения вторжений в реальном времени (RTIDS) .....	320
Системы противодействия атакам (IPS).....	320
Мониторинг журналов событий .....	321
Анализ трафика сети.....	321
Использование сетевых сенсоров .....	321
Машинное обучение и анализ больших данных.....	322
Практики защиты от взлома .....	325
6.2.3. Особенности практик защиты от взлома .....	328

<b>6.3. РАЗВИТИЕ НАВЫКОВ: СОЗДАНИЕ СОБСТВЕННЫХ ИНСТРУМЕНТОВ БЕЗОПАСНОСТИ</b> .....	<b>336</b>
6.3.1. Практическое задание: разработка сканера уязвимостей.....	338
Шаги выполнения .....	338
6.3.2. Практическое задание: создание инструмента для обнаружения ARP-отравления .....	340
Шаги выполнения .....	340
6.3.3. Практическое задание: реализация инструмента для обнаружения сетевого sniffинга.....	342
Шаги выполнения .....	342
6.3.4. Практическое задание: разработка простого файрвола .....	346
Шаги выполнения .....	346

## ГЛАВА 7. Современные вызовы и тренды в сфере хакинга..351

<b>7.1. ОСНОВНЫЕ ВЫЗОВЫ И ТРЕНДЫ ПО КИБЕРБЕЗОПАСНОСТИ</b> .....	<b>352</b>
Распространение IoT (Интернета вещей).....	352
Угрозы и атаки на облачные сервисы .....	353
Социальная инженерия и фишинг .....	353
Мобильные угрозы .....	353
Распространение искусственного интеллекта и машинного обучения..	354
Угрозы кибершпионажа и кибервойны.....	354
Блокчейн и криптовалюты .....	355
<b>7.2. ПЕРСПЕКТИВЫ РАЗВИТИЯ НАВЫКОВ ХАКЕРА НА PYTHON</b> .....	<b>355</b>
Глубокое понимание языка Python .....	356
Изучение библиотек и фреймворков .....	356
Развитие навыков в области сетевой безопасности.....	357
Изучение машинного обучения и искусственного интеллекта.....	357
Развитие навыков в области веб-хакинга.....	357
<b>7.3. РЕСУРСЫ ДЛЯ ДОПОЛНИТЕЛЬНОГО ИЗУЧЕНИЯ</b> .....	<b>358</b>
Онлайн-курсы и платформы для обучения .....	358
Книги .....	359
Веб-сайты и блоги .....	360
Инструменты и библиотеки.....	360
Форумы и сообщества.....	361
<b>ЗАКЛЮЧЕНИЕ</b> .....	<b>362</b>
<b>СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ ИНФОРМАЦИИ</b> .....	<b>364</b>