

PYTHON

ГЛАЗАМИ ХАКЕРА



Создание reverse shell

Служба за людьми
и разгадывание капчи

Обработка сложных форм

Программирование
микроконтроллеров

Устройство вредоносных
программ на Python

Инструментарий для
динамического анализа
вредоносного кода

Использование
API VirusTotal
в своих проектах

Автоматизированный сбор
информации о системе

Создание навыка
для «Алисы»

Применение Python
для автоматизации iOS

Библиотека журнала

ХАКЕР

bhv®

PYTHON

ГЛАЗАМИ ХАКЕРА

Санкт-Петербург
«БХВ-Петербург»

2022

УДК 004.43
ББК 32.973-018.1
П12

П12 Python глазами хакера. — СПб.: БХВ-Петербург, 2022. — 176 с.: ил. —
(Библиотека журнала «Хакер»)

ISBN 978-5-9775-6870-8

Рассмотрены современные интерпретаторы языка Python. Описано устройство reverse shell, файлового вируса, трояна, локера и шифровальщика. Представлены примеры инструментов для автоматизированного сбора информации о компьютере, динамического анализа вредоносного кода, в том числе с использованием API VirusTotal. Приведены примеры программ для разгадывания капчи, поиска людей на видео, обработки сложных веб-форм, автоматизации iOS. Показано, как написать на Python новый навык для голосового помощника «Алиса» и различные программы для одноплатных компьютеров.

Для программистов и специалистов по информационной безопасности.

УДК 004.43
ББК 32.973-018.1

Группа подготовки издания:

Руководитель проекта	<i>Павел Шалин</i>
Зав. редакцией	<i>Людмила Гауль</i>
Редактор	<i>Марк Бруцкий-Стемпковский</i>
Компьютерная верстка	<i>Ольги Сергиенко</i>
Дизайн обложки	<i>Зои Канторович</i>

Подписано в печать 02.06.22.

Формат 70×100^{1/16}. Печать офсетная. Усл. печ. л. 14,19.

Доп. тираж 2000 экз. Заказ № 4221.

"БХВ-Петербург", 191036, Санкт-Петербург, Гончарная ул., 20.

Отпечатано с готового оригинал-макета

ООО "Принт-М", 142300, М.О., г. Чехов, ул. Полиграфистов, д. 1

ISBN 978-5-9775-6870-8

© ИП Югай А.О., 2022
© Оформление. ООО "БХВ-Петербург", ООО "БХВ", 2022

Оглавление

Предисловие	7
1. Разборки в террариуме. Изучаем виды интерпретаторов Python <i>(Николай Марков)</i>	9
Чтобы понять Python, надо понять Python	9
Нижний уровень	10
Змея в коробке	11
Виртуальная реальность	12
Jython	12
IronPython	13
Заключение	14
2. Reverse shell на Python. Осваиваем навыки работы с сетью на Python на примере обратного шелла <i>(Илья Афанасьев)</i>	15
Переходим к практике	15
Используем UDP	16
Сторона сервера	16
Сторона клиента	17
Тестируем	17
Используем TCP	18
Сторона сервера	18
Сторона клиента	19
Тестируем	20
Применяем знания на практике	21
Делаем полноценный reverse shell	21
Сторона клиента (атакованная машина)	22
Сторона сервера (атакующего)	23
Шелл одной строчкой	25
В завершение	26
3. YOLO! Используем нейросеть, чтобы следить за людьми и разгадывать капчу <i>(Татьяна Бабичева)</i>	27
Какие бывают алгоритмы	28
R-CNN, Region-Based Convolutional Neural Network	28
Fast R-CNN, Fast Region-Based Convolutional Neural Network	28
Faster R-CNN, Faster Region-Based Convolutional Neural Network	28
YOLO, You Only Look Once	28
Пишем код	29

Модифицируем приложение.....	33
Итоги.....	35
4. Идеальная форма. Обрабатываем сложные формы на Python с помощью WTFORMS (Илья Русанен)..... 37	
Зачем это нужно?.....	37
Установка.....	39
Создание формы.....	39
Работа с формой.....	40
Генерация формы (GET /users/new).....	41
Парсинг пейлоада (POST /users).....	42
Опции для частичного парсинга пейлоада.....	43
Валидаторы.....	44
Динамическое изменение свойств полей формы.....	45
Сборные и наследуемые формы.....	46
Заполнение реляционных полей (one-to-many, many-to-many).....	47
Кастомные виджеты и расширения.....	49
Вместо заключения.....	50
5. Python для микроконтроллеров. Учимся программировать одноплатные компьютеры на языке высокого уровня (Виктор Паперно)..... 51	
С чего все началось?.....	51
А чем эта плата лучше?.....	51
И что, только официальная плата?.....	52
Подготовка к работе.....	53
Прошивка контроллера.....	53
Взаимодействие с платой.....	53
Начинаем разработку.....	56
Hello world.....	56
Радужный мир.....	57
Монитор. Рисование, письмо и каллиграфия.....	59
Настраиваем Wi-Fi и управляем через сайт.....	60
Управление моторами.....	62
Интернет вещей.....	64
Заключение.....	65
Полезные ссылки.....	65
6. Создаем простейший троян на Python (Валерий Линьков)..... 67	
Теория.....	67
Определяем IP.....	68
Бэконнект по почте.....	69
Троян.....	71
Wi-Fi-стилер.....	74
Доработки.....	78
Заключение.....	79
7. Используем Python для динамического анализа вредоносного кода (Евгений Дроботун)..... 81	
Отслеживаем процессы.....	83

Следим за файловыми операциями.....	87
Используем API Windows	88
Используем WMI	92
Мониторим действия с реестром	93
Используем API	94
Используем WMI	95
Мониторим вызовы API-функций.....	96
Заключение.....	99
8. Разведка змеем. Собираем информацию о системе с помощью Python	
<i>(Марк Клинтон)</i>	101
Инструменты.....	101
Задачи	102
Создаем основу программы	102
Сбор данных.....	103
Скорость интернет-соединения	104
Часовой пояс и время	104
Частота процессора	104
Скриншот рабочего стола	105
Запись в файл	105
Отправка данных	106
Собираем программу.....	107
Пишем сборщик с графическим интерфейсом.....	108
Вывод.....	109
9. Как сделать новый навык для «Алисы» на Python (Виктор Паперно)	111
Первый навык — эхо-бот.....	111
Тестирование навыков	113
Поиграем в слова	118
А теперь картинки	122
Размещение в сети	123
10. Тотальная проверка. Используем API VirusTotal в своих проектах	
<i>(Евгений Дроботун)</i>	125
Получаем API Key	126
Версии API	126
API VirusTotal. Версия 2	127
Ошибки	127
Отправка файла на сервер для сканирования.....	128
Получение отчета о последнем сканировании файла	128
Отправка URL на сервер для сканирования	131
Получение отчета о результатах сканирования URL-адреса	131
Получение информации об IP-адресах и доменах	132
API VirusTotal. Версия 3	133
Ошибки	133
Функции работы с файлами.....	134
Функции для работы с URL	139
Функции работы с доменами и IP-адресами	140
GET-запрос типа /analyses.....	140
Заключение.....	141

Модифицируем приложение.....	33
Итоги.....	35
4. Идеальная форма. Обрабатываем сложные формы на Python с помощью WTForms (Илья Русанен)	37
Зачем это нужно?	37
Установка	39
Создание формы	39
Работа с формой	40
Генерация формы (GET /users/new).....	41
Парсинг пейлоада (POST /users).....	42
Опции для частичного парсинга пейлоада	43
Валидаторы	44
Динамическое изменение свойств полей формы	45
Сборные и наследуемые формы	46
Заполнение реляционных полей (one-to-many, many-to-many)	47
Кастомные виджеты и расширения.....	49
Вместо заключения.....	50
5. Python для микроконтроллеров. Учимся программировать одноплатные компьютеры на языке высокого уровня (Виктор Паперно)	51
С чего все началось?.....	51
А чем эта плата лучше?.....	51
И что, только официальная плата?.....	52
Подготовка к работе	53
Прошивка контроллера	53
Взаимодействие с платой.....	53
Начинаем разработку	56
Hello world.....	56
Радужный мир.....	57
Монитор. Рисование, письмо и каллиграфия	59
Настраиваем Wi-Fi и управляем через сайт.....	60
Управление моторами	62
Интернет вещей.....	64
Заключение.....	65
Полезные ссылки	65
6. Создаем простейший троян на Python (Валерий Линьков).....	67
Теория.....	67
Определяем IP	68
Бэкконнект по почте	69
Троян.....	71
Wi-Fi-стилер.....	74
Доработки.....	78
Заключение.....	79
7. Используем Python для динамического анализа вредоносного кода (Евгений Дроботун).....	81
Отслеживаем процессы	83

Следим за файловыми операциями.....	87
Используем API Windows	88
Используем WMI	92
Мониторим действия с реестром	93
Используем API	94
Используем WMI	95
Мониторим вызовы API-функций.....	96
Заключение.....	99

8. Разведка змеем. Собираем информацию о системе с помощью Python

<i>(Марк Клинтон)</i>	101
Инструменты.....	101
Задачи	102
Создаем основу программы.....	102
Сбор данных.....	103
Скорость интернет-соединения	104
Часовой пояс и время	104
Частота процессора	104
Скриншот рабочего стола	105
Запись в файл	105
Отправка данных	106
Собираем программу.....	107
Пишем сборщик с графическим интерфейсом.....	108
Вывод.....	109

9. Как сделать новый навык для «Алисы» на Python (Виктор Паперно)

Первый навык — эхо-бот.....	111
Тестирование навыков	113
Поиграем в слова	118
А теперь картинки	122
Размещение в сети.....	123

10. Тотальная проверка. Используем API VirusTotal в своих проектах

<i>(Евгений Дроботун)</i>	125
Получаем API Key	126
Версии API	126
API VirusTotal. Версия 2	127
Ошибки	127
Отправка файла на сервер для сканирования.....	128
Получение отчета о последнем сканировании файла	128
Отправка URL на сервер для сканирования	131
Получение отчета о результатах сканирования URL-адреса	131
Получение информации об IP-адресах и доменах	132
API VirusTotal. Версия 3	133
Ошибки.....	133
Функции работы с файлами.....	134
Функции для работы с URL	139
Функции работы с доменами и IP-адресами	140
GET-запрос типа /analyses.....	140
Заключение.....	141

11. Как использовать Python для автоматизации iOS (Виктор Паперно).....	143
Введение.....	143
Скрипты.....	146
Быстрая отправка твита.....	147
Быстрое сохранение в Instararer.....	147
Генератор паролей.....	148
Отправка текущего местоположения на email.....	148
Отправка фотографии на сервер по FTP.....	149
Работа с удаленным сервером по SSH.....	150
Сокращаем ссылки при помощи goo.gl.....	151
Очистка записной книжки.....	152
Импорт друзей из ВК в записную книжку.....	152
Заключение.....	154
12. Пишем на Python простейшую малварь: локер, шифровальщик и вирус (Валерий Линьков)	155
Настройка среды.....	156
Локаль.....	156
Шифровальщик.....	158
Вирус.....	161
Делаем исполняемый файл.....	163
Заключение.....	164
«Хакер»: безопасность, разработка, DevOps.....	165
Предметный указатель	169