

Bash

и кибербезопасность

Атака, защита и анализ
из командной строки Linux

Пол Тронкон
Карл Олбинг



НАВУКОВАЯ БІБЛІЯТЭКА

Беларускага нацыянальнага
тэхнічнага ўніверсітэта

Інв. № **1883841**



Санкт-Петербург • Москва • Екатеринбург • Воронеж

Нижний Новгород • Ростов-на-Дону

Самара • Минск

2021

Оглавление

Введение.....	12
Для кого эта книга.....	13
Bash или bash.....	13
Надежность скриптов	13
Рабочая среда.....	14
Условные обозначения.....	14
Использование примеров кода	15
Благодарности	15
От издательства	16

Часть I. Основы

Глава 1. Работа с командной строкой.....	18
Определение командной строки	18
Почему именно bash	19
Примеры использования командной строки.....	19
Запуск Linux и bash в Windows	20
Основы работы с командной строкой	22
Выводы.....	28
Упражнения	28
Глава 2. Основы работы с bash.....	30
Вывод.....	30
Переменные.....	31

Ввод.....	33
Условия.....	33
Циклы.....	37
Функции.....	39
Шаблон соответствия в bash.....	41
Написание первого сценария: определение типа операционной системы.....	43
Выводы.....	44
Упражнения.....	45
Глава 3. Регулярные выражения.....	46
Используемые команды.....	47
Метасимволы регулярного выражения.....	48
Группирование.....	50
Квадратные скобки и классы символов.....	50
Обратные ссылки.....	53
Квантификаторы.....	54
Якоря и границы слов.....	55
Выводы.....	55
Упражнения.....	55
Глава 4. Принципы защиты и нападения.....	57
Кибербезопасность.....	57
Жизненный цикл атаки.....	59
Выводы.....	63

Часть II. Защитные операции с использованием bash

Глава 5. Сбор информации.....	66
Используемые команды.....	67
Сбор информации о системе.....	71
Поиск в файловой системе.....	81
Передача данных.....	93
Выводы.....	94
Упражнения.....	94

Глава 6. Обработка данных	96
Используемые команды	96
Обработка файлов с разделителями	101
Обработка XML	103
Обработка JSON	105
Агрегирование данных	107
Выводы	109
Упражнения	109
Глава 7. Анализ данных	110
Используемые команды	110
Ознакомление с журналом доступа к веб-серверу	111
Сортировка и упорядочение данных	113
Подсчет количества обращений к данным	114
Суммирование чисел в данных	118
Отображение данных в виде гистограммы	120
Поиск уникальности в данных	126
Выявление аномалий в данных	128
Выводы	131
Упражнения	131
Глава 8. Мониторинг журналов в режиме реального времени	133
Мониторинг текстовых журналов	133
Мониторинг журналов Windows	136
Создание гистограммы, актуальной в реальном времени	137
Выводы	143
Упражнения	143
Глава 9. Инструмент: мониторинг сети	145
Используемые команды	146
Шаг 1. Создание сканера портов	146
Шаг 2. Сравнение с предыдущим выводом	149
Шаг 3. Автоматизация и уведомление	152
Выводы	155
Упражнения	156

Глава 10. Инструмент: контроль файловой системы	157
Используемые команды	157
Шаг 1. Определение исходного состояния файловой системы	158
Шаг 2. Обнаружение изменений в исходном состоянии системы.....	159
Шаг 3. Автоматизация и уведомление	162
Выводы.....	166
Упражнения	166
Глава 11. Анализ вредоносных программ	168
Используемые команды	168
Реверс-инжиниринг.....	171
Извлечение строк	174
Взаимодействие с VirusTotal.....	176
Выводы.....	183
Упражнения	183
Глава 12. Форматирование и отчетность	184
Используемые команды	184
Форматирование для отображения в виде HTML-документа.....	185
Создание панели мониторинга	191
Выводы.....	195
Упражнения	196

Часть III. Тестирование на проникновение

Глава 13. Разведка	198
Используемые команды	198
Просмотр веб-сайтов.....	199
Автоматический захват баннера.....	200
Выводы.....	205
Упражнения	205
Глава 14. Обфускация сценария	207
Используемые команды	207
Обфускация синтаксиса.....	208
Обфускация логики.....	210
Шифрование	213

Выводы.....	224
Упражнения	224
Глава 15. Инструмент: Fuzzer.....	226
Реализация.....	227
Выводы.....	231
Упражнения	232
Глава 16. Создание точки опоры.....	233
Используемые команды	233
Бэкдор одной строкой.....	234
Пользовательский инструмент удаленного доступа.....	237
Выводы.....	242
Упражнения	242
 Часть IV. Администрирование систем обеспечения безопасности	
Глава 17. Пользователи, группы и права доступа.....	244
Используемые команды	244
Пользователи и группы.....	247
Права доступа к файлам и списки управления доступом	250
Внесение массовых изменений.....	253
Выводы.....	254
Упражнения	254
Глава 18. Добавление записей в журнал	255
Используемые команды	255
Запись событий в журнал Windows.....	256
Создание журналов Linux	257
Выводы.....	258
Упражнения	258
Глава 19. Инструмент: мониторинг доступности системы.....	259
Используемые команды	259
Реализация.....	260
Выводы.....	262
Упражнения	262

Глава 20. Инструмент: проверка установленного программного обеспечения	263
Используемые команды	264
Реализация.....	266
Определение остального программного обеспечения.....	267
Выводы.....	269
Упражнения	269
Глава 21. Инструмент: проверка конфигурации	270
Реализация.....	270
Выводы.....	275
Упражнения	276
Глава 22. Инструмент: аудит учетных записей	277
Меня взломали?.....	277
Проверяем, не взломан ли пароль	278
Проверяем, не взломан ли адрес электронной почты.....	280
Выводы.....	285
Упражнения	285
Глава 23. Заключение	286