

УДК 004.056
ББК 32.971.3
Б64

Б64 **Бирюков А. А.**

Собираем устройства для тестов на проникновение. – М. : ДМК Пресс, 2018. – 378 с.

ISBN 978-5-97060-637-7

Многообразие и доступность различных недорогих аппаратных платформ, таких как Arduino, Raspberry Pi и др., простота их программирования, и при этом практически полное отсутствие средств защиты от них делают хакерские устройства мощным и опасным средством реализации компьютерных атак. В книге рассматриваются как теоретические основы информационной безопасности, так и практические аспекты создания собственных устройств с исходными кодами, схемами и примерами реализации. Также рассматриваются механизмы защиты от данного вида атак.

Издание предназначено для читателей, знакомых с основами информационной безопасности и владеющих навыками программирования на языках высокого уровня.

УДК 004.056
ББК 32.971.3

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

Материал, изложенный в данной книге, многократно проверен. Но, поскольку вероятность технических ошибок все равно существует, издательство не может гарантировать абсолютную точность и правильность приводимых сведений. В связи с этим издательство не несет ответственности за возможные ошибки, связанные с использованием книги.

ISBN 978-5-97060-637-7

© Бирюков А. А., 2018
© Оформление, издание, ДМК Пресс, 2018

ОГЛАВЛЕНИЕ

Вступление	8
Приступая к работе	10
Для кого эта книга	10
Структура книги	11
Какие детали нам потребуются	11
Немного о программном обеспечении	14
Заключение	15
Чего в книге не будет	15
Кодекс надо читать	15
Ничего не прячем	18
Никакой «физики»	19
Простота – залог успеха	19
Заключение	19
Итоги главы	20
Глава 1. Теория и практика информационной безопасности	21
1.1. Кратко о теории информационной безопасности (ИБ)	21
1.1.1. Угрозы	22
1.1.2. Нарушители	24
1.1.3. Риски	26
1.1.4. Модель нарушителя	28
1.1.5. Модель угроз	30
1.1.6. Заключение	36
1.2. Практика	36
1.2.1. Строим систему информационной безопасности	36
1.2.2. Защищаем периметр	37
1.2.3. Защищаем серверы и рабочие места	40
1.2.4. Защищаем каналы связи	47
1.2.5. Предотвращение хищения конфиденциальной информации	51
1.2.6. Средства двухфакторной аутентификации	58
1.2.7. Мониторинг событий ИБ	59
1.2.8. Заключение	62
1.3. Итоги главы	62
Глава 2. Наш инструментарий	64
2.1. Arduino	64
2.1.1. Описание макетной платы	64
2.1.2. Устанавливаем среду разработки	66
2.1.3. Проверяем корректность работы	70
2.1.4. Заключение	74

2.2. Teensy.....	74
2.2.1. Описание макетной платы	74
2.2.2. Настройка среды разработки	75
2.2.3. Проверяем корректность работы	79
2.2.4. Заключение	80
2.3. Digispark	80
2.3.1. Описание макетной платы	80
2.3.2. Настройка среды разработки	81
2.3.3. Проверяем корректность работы	83
2.3.4. Заключение	84
2.4. ESP 8266/NodeMCU	84
2.4.1. Описание макетной платы	85
2.4.2. Настройка среды разработки	86
2.4.3. Проверяем корректность работы	89
2.4.4. Заключение	90
2.5. Raspberry Pi 3	90
2.5.1. Описание микрокомпьютера	90
2.5.2. Устанавливаем ОС.....	91
2.5.3. Проверка базовой конфигурации.....	92
2.5.4. Собираем хакерский планшет.....	92
2.5.5. Пишем удобный Shell	97
2.5.6. Заключение	106
2.6. Raspberry Pi Zero	106
2.6.1. Описание и основные отличия.....	106
2.6.2. Устанавливаем ОС.....	107
2.6.3. Дополнительные настройки.....	112
2.6.4. Проверка базовой конфигурации.....	113
2.6.5. Заключение	113
2.7. Onion Omega	114
2.7.1. Описание микрокомпьютера.....	114
2.7.2. Особенности подключения	115
2.7.3. Подключение к устройству.....	118
2.7.4. Проверка базовой конфигурации	118
2.7.5. Заключение.....	119
2.8. WRT-прошивки и устройства	119
2.8.1. Восстановление в случае неудачной перепрошивки	123
2.8.2. Установка новой прошивки и проверка корректной работы	127
2.8.3. Заключение	130
2.9. Итоги главы	130

Глава 3. Внешний пентест 132

3.1. Сканер беспроводных сетей на основе NodeMCU	132
3.1.1. Необходимая информация о беспроводных сетях.....	133
3.1.2. Исходный код	134

3.1.3. Проверка работы	138
3.1.4. Заключение	138
3.2. Подключаем SD-карту и сохраняем найденные Wi-Fi-сети	139
3.2.1. Суть атаки	139
3.2.2. Схема устройства	139
3.2.3. Исходный код	140
3.2.4. Проверка работы	144
3.2.5. Заключение	144
3.3. Заглушаем сигнал Wi-Fi с помощью NodeMCU	144
3.3.1. Суть атаки	144
3.3.2. Схема устройства	146
3.3.3. Исходный код	146
3.3.4. Проверка работы	146
3.3.5. Заключение	148
3.4. Атаки на беспроводные сети с помощью Raspberry Pi 3	148
3.4.1. Что мы можем сделать	148
3.4.2. Поиск беспроводных сетей	149
3.4.3. Подключение к Wi-Fi	150
3.4.4. Перехват трафика	155
3.4.5. Сканирование сети	156
3.4.6. Подбор паролей	161
3.4.7. Поиск уязвимостей	162
3.4.8. Эксплуатация найденных уязвимостей	166
3.4.9. Поддельная точка доступа	173
3.4.10. Ищем уязвимость KRACK	178
3.4.11. Заключение	188
3.5. Атаки на беспроводные сети с помощью Onion Omega	188
3.5.1. Сканер беспроводных сетей Wi-Fi	188
3.5.2. Заключение	193
3.6. Итоги главы	194

Глава 4. Моделируем внутренние угрозы..... 195

4.1. HID-атаки с помощью Teensy	195
4.1.1. Странная флешка	195
4.1.2. Базовый код для атак	196
4.1.3. Добавление пользователя	205
4.1.4. Замена DNS	212
4.1.5. Модификация файла Hosts	217
4.1.6. Включаем RDP	223
4.1.7. Включаем сервер Telnet	228
4.1.8. Загрузка через Powershell	233
4.1.9. Выполнение эксплоита	241
4.1.10. Собираем профили WLAN	248
4.1.11. Создаем свою беспроводную сеть	254
4.1.12. Автоматическое копирование собранной информации на флешку	260

4.1.13. Извлекаем учетные данные без прав администратора	270
4.1.14. Автоматическая настройка приложений на пользовательской машине	279
4.1.15. Автоматизируй это	283
4.1.16. Немного робототехники	289
4.1.17. Простейший робот.....	290
4.1.18. Linux не исключение.....	296
4.1.19. Реверсивный Shell.....	297
4.1.20. И MacOS тоже.....	299
4.1.21. Заключение.....	301
4.2. HID-атаки с помощью Digispark	301
4.2.1. Суть атак.....	301
4.2.2. Безумная мышь	301
4.2.3. Крохотная клавиатура	304
4.2.4. Заключение	306
4.3. HID-атаки с помощью Raspberry Pi Zero	306
4.3.1. Суть атак.....	306
4.3.2. Перехват трафика	307
4.3.3. Перехват cookies	308
4.3.4. Удаленный доступ по Wi-Fi	310
4.3.5. Заключение	311
4.4. Атаки с помощью Arduino.....	312
4.4.1. Перехват сигналов с беспроводной клавиатуры	312
4.4.2. Перехватываем сигналы на ИК-порт.....	313
4.4.3. Общая концепция организации взаимодействия с атакуемой машиной	318
4.4.4. Заключение	327
4.5. Проводные атаки с помощью Raspberry Pi.....	327
4.5.1. ARP Spoofing.....	327
4.5.2. DHCP Starvation или DoS для DHCP	328
4.5.3. Поддельный DHCP	330
4.5.4. Аппаратный TAP.....	332
4.5.5. «Раздеваем» SSL.....	333
4.5.6. Заключение	334
4.6. Сетевые атаки с помощью OpenWRT.....	335
4.6.1. MiniPwner	335
4.6.2. Заключение	338
4.7. Итоги главы.....	339

Глава 5. Рекомендуемые методы и средства защиты 340

5.1. Защищаемся от внешних угроз.....	340
5.1.1. Защита беспроводных сетей.....	340
5.1.2. Заключение	343
5.2. Защищаемся от внутренних угроз	343
5.2.1. Находим чужие сети	343
5.2.2. Оргмеры.....	346

5.2.3. Защита от проводных сетей	346
5.2.4. Защита проводных сетей	347
5.2.5. Защита от HID-атак.....	348
5.2.6. И снова оргмеры.....	353
5.2.7. Заключение.....	353
5.3. Общие рекомендации.....	353
5.3.1. Умный мониторинг событий ИБ	354
5.3.2. Регулярный анализ защищенности	360
5.3.3. Оргмеры... как всегда	363
5.3.4. Заключение	365
5.4. Итоги главы	365

Глава 6. Заключительные выводы 366

Приложение 367

П.1. Использованные источники, или Что еще можно почитать.....	367
П.2. Модельный ряд Arduino	368
П.3. Модельный ряд Teensy.....	375
П.4. Модельный ряд Digispark	375
П.5. Модельный ряд ESP 8266	376
П.6. Модельный ряд Raspberry Pi	377