

УДК 004.065
ББК 32.973.26-018.2
Б64

Бирюков А. А.

Б64 Информационная безопасность: защита и нападение. – 2-е изд., перераб. и доп. – М.: ДМК Пресс, 2017. – 434 с.: ил.

ISBN 978-5-97060-435-9

В книге приводится как техническая информация, описывающая атаки и защиту от них, так и рекомендации по организации процесса обеспечения информационной безопасности. Рассмотрены практические примеры для организации защиты персональных данных в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и другими нормативными актами.

Во втором издании проведена актуализация технической информации, а также описано более глубокое погружение в практические аспекты, связанные с проведением аудитов по безопасности и тестов на проникновение для различных систем. Подробно рассматриваются современные решения по маршрутизации, беспроводной связи и другим направлениям развития информационных технологий.

Книга предназначена для системных администраторов и пользователей малых и средних сетей, осуществляющих защиту корпоративных ресурсов.

УДК 004.065
ББК 32.973.26-018.2

Все права защищены. Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения владельца права.

Все торговые марки и названия программ являются собственностью их владельцев.

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. По этой причине издательство не несет ответственности за возможные ошибки, связанные с использованием книги.

ISBN 978-5-97060-435-9

© Бирюков А. А., 2017

© Оформление, издание, ДМК Пресс, 2017



ОГЛАВЛЕНИЕ

Вступление.....	10
------------------------	-----------

Глава 1. Теоретические основы	25
--	-----------

1.1. Модель OSI.....	26
1.1.1. Прикладной (7) уровень (Application Layer)	27
1.1.2. Представительский (6) уровень (Presentation Layer)	28
1.1.3. Сеансовый (5) уровень (Session Layer).....	28
1.1.4. Транспортный (4) уровень (Transport Layer).....	28
1.1.5. Сетевой (3) уровень (Network Layer)	28
1.1.6. Канальный (2) уровень (Data Link Layer)	29
1.1.7. Физический (1) уровень (Physical Layer).....	29
1.2. Модель DOD.....	31
1.3. Заключение	31

Глава 2. Классификация атак по уровням иерархической модели OSI	32
--	-----------

2.1. Атаки на физическом уровне	32
2.1.1. Концентраторы	32
2.2. Атаки на канальном уровне.....	36
2.2.1. Атаки на коммутаторы	36
2.2.2. Переполнение CAM-таблицы	36
2.2.3. VLAN Hopping.....	40
2.2.4. Атака на STP	41
2.2.5. MAC Spoofing	46
2.2.6. Атака на PVLAN (Private VLAN)	47
2.2.7. Атака на DHCP	48
2.2.8. ARP-spoofing	49
2.2.9. Заключение.....	53
2.3. Атаки на сетевом уровне.....	54

2.3.1. Атаки на маршрутизаторы	54
2.3.2. Среда со статической маршрутизацией	57
2.3.3. Безопасность статической маршрутизации.....	58
2.3.4. Среда с динамической маршрутизацией.....	58
2.3.5. Scapy – универсальное средство для реализации сетевых атак	59
2.3.6. Среда с протоколом RIP	63
2.3.7. Безопасность протокола RIP.....	64
2.3.8. Ложные маршруты RIP	66
2.3.9. Понижение версии протокола RIP	71
2.3.10. Взлом хэша MD5.....	72
2.3.11. Обеспечение безопасности протокола RIP	74
2.3.12. Среда с протоколом OSPF	75
2.3.13. Безопасность протокола OSPF.....	82
2.3.14. Среда с протоколом BGP	83
2.3.15. Атака BGP Router Masquerading.....	84
2.3.16. Атаки на MD5 для BGP.....	84
2.3.17. «Слепые» DoS-атаки на BGP-маршрутизаторы	85
2.3.18. Безопасность протокола BGP.....	86
2.3.19. Атаки на BGP.....	89
2.3.20. Вопросы безопасности	90
2.3.21. Среда с протоколом IS-IS.....	91
2.3.22. Атаки на протокол IS-IS.....	92
2.3.23. Среда с протоколом MPLS	94
2.3.24. Безопасность протокола MPLS.....	96
2.3.25. IPSec как средство защиты на сетевом уровне.....	97
2.3.26. Целостность данных	97
2.3.27. Защита соединения.....	98
2.3.28. Заключение	108
2.4. Атаки на транспортном уровне	108
2.4.1. Транспортный протокол TCP.....	108
2.4.2. Известные проблемы.....	111
2.4.3. Атаки на TCP	112
2.4.4. IP-spoofing	112
2.4.5. TCP hijacking.....	114
2.4.6. Десинхронизация нулевыми данными	114
2.4.7. Сканирование сети.....	115
2.4.8. SYN-флуд	116
2.4.9. Атака Teardrop	118
2.4.10. Безопасность TCP	118

2.4.11. Атаки на UDP	119
2.4.12. UDP Storm	120
2.4.13. Безопасность UDP	121
2.4.14. Протокол ICMP	121
2.4.15. Методология атак на ICMP	121
2.4.16. Обработка сообщений ICMP	122
2.4.17. Сброс соединений (reset)	124
2.4.18. Снижение скорости	124
2.4.19. Безопасность ICMP	124
2.5. Атаки на уровне приложений	125
2.5.1. Безопасность прикладного уровня	125
2.5.2. Протокол SNMP	125
2.5.3. Протокол Syslog	129
2.5.4. Протокол DNS	132
2.5.5. Безопасность DNS	134
2.5.6. Веб-приложения	134
2.5.7. Атаки на веб через управление сессиями	135
2.5.8. Защита DNS	141
2.5.9. SQL-инъекции	142
2.6. Угрозы IP-телефонии	144
2.6.1. Возможные угрозы VoIP	146
2.6.2. Поиск устройств VoIP	147
2.6.3. Перехват данных	148
2.6.4. Отказ в обслуживании	149
2.6.5. Подмена номера	150
2.6.6. Атаки на диспетчеров	151
2.6.7. Хищение сервисов и телефонный спам	152
2.7. Анализ удаленных сетевых служб	153
2.7.1. ICMP как инструмент исследования сети	154
2.7.2. Утилита fping	156
2.7.3. Утилита Nmap	157
2.7.4. Использование «Broadcast ICMP»	157
2.7.5. ICMP-пакеты, сообщающие об ошибках	158
2.7.6. UDP Discovery	159
2.7.7. Исследование с помощью TCP	160
2.7.8. Использование флага SYN	161
2.7.9. Использование протокола IP	162
2.7.10. Посылки фрагмента IP-датаграммы	162

2.7.11. Идентификация узла с помощью протокола ARP	163
2.7.12. Меры защиты	164
2.7.13. Идентификация ОС и приложений.....	165
2.7.14. Отслеживание маршрутов	165
2.7.15. Сканирование портов.....	166
2.7.16. Идентификация сервисов и приложений	169
2.7.17. Особенности работы протоколов	172
2.7.18. Идентификация операционных систем	174
2.8. Заключение	174

Глава 3. Атаки на беспроводные устройства 175

3.1. Атаки на Wi-Fi	175
3.1.1. Протоколы защиты	175
3.1.2. Протокол WEP	176
3.1.3. Протокол WPA.....	176
3.1.4. Физическая защита.....	178
3.1.5. Соккрытие ESSID	178
3.1.6. Возможные угрозы	178
3.1.7. Отказ в обслуживании.....	179
3.1.8. Поддельные сети.....	181
3.1.9. Ошибки при настройке.....	182
3.1.10. Взлом ключей шифрования	182
3.1.11. Уязвимость 196.....	183
3.1.12. В обход защиты.....	183
3.1.13. Защита через Web	184
3.1.13. Проводим пентест Wi-Fi	184
3.1.14. Заключение	191
3.2. Безопасность Bluetooth	191
3.2.1. Угрозы Bluetooth	191
3.2.2. Другие беспроводные угрозы	194
3.3. Заключение	195

Глава 4. Уязвимости 196

4.1. Основные типы уязвимостей	196
4.1.1. Уязвимости проектирования	196
4.1.2. Уязвимости реализации	197
4.1.3. Уязвимости эксплуатации	197

4.2. Примеры уязвимостей.....	200
4.2.1. Права доступа к файлам	200
4.2.2. Оперативная память.....	202
4.2.3. Объявление памяти	202
4.2.4. Завершение нулевым байтом.....	203
4.2.5. Сегментация памяти программы	203
4.2.6. Переполнение буфера.....	207
4.2.7. Переполнения в стеке	208
4.2.8. Эксплоит без кода эксплоита	212
4.2.9. Переполнения в куче и bss	214
4.2.10. Перезапись указателей функций.....	215
4.2.11. Форматные строки	215
4.2.12. Сканирование приложений на наличие уязвимостей.....	220
4.2.12. Эксплуатация найденных уязвимостей.....	222
4.3. Защита от уязвимостей.....	228
4.3.1. WSUS.....	228
4.4. Заключение	229

Глава 5. Атаки в виртуальной среде 230

5.1. Технологии виртуализации.....	230
5.2. Сетевые угрозы в виртуальной среде.....	233
5.3. Защита виртуальной среды.....	234
5.3.1. Trend Micro Deep Security	234
5.3.2. Схема защиты Deep Security	236
5.3.3. Защита веб-приложений	238
5.3.4. Подводя итоги	241
5.4. Security Code vGate.....	241
5.4.1. Что защищает vGate?	242
5.4.2. Разграничение прав	243
5.4.3. Ограничение управления и политики.....	243
5.5. Виртуальные угрозы будущего	245
5.6. Заключение	248

Глава 6. Облачные технологии..... 249

6.1. Принцип облака.....	249
6.1.1. Структура ЦОД	250
6.1.2. Виды ЦОД	251

6.1.3. Требования к надежности	252
6.2. Безопасность облачных систем.....	252
6.2.1. Контроль над ситуацией	256
6.2.2. Ситуационный центр	256
6.2.3. Основные элементы построения системы ИБ облака.....	257
6.3. Заключение	258

Глава 7. Средства защиты 259

7.1. Организация защиты от вирусов.....	260
7.1.1. Способы обнаружения вирусов	261
7.1.2. Проблемы антивирусов.....	265
7.1.3. Архитектура антивирусной защиты.....	269
7.1.4. Борьба с нежелательной почтой	272
7.2. Межсетевые экраны	276
7.2.1. Принципы работы межсетевых экранов	277
7.2.2. Аппаратные и программные МЭ.....	279
7.2.2. Специальные МЭ	279
7.3. Средства обнаружения и предотвращения вторжений	281
7.3.1. Системы IDS/IPS.....	281
7.3.2. Мониторинг событий ИБ в Windows 2008.....	287
7.3.3. Промышленные решения мониторинга событий.....	296
7.4. Средства предотвращения утечек	309
7.4.1. Каналы утечек.....	312
7.4.2. Принципы работы DLP.....	315
7.4.3. Сравнение систем DLP	320
7.4.4. Заключение.....	326
7.5. Средства шифрования	326
7.5.1. Симметричное шифрование	326
7.5.2. Инфраструктура открытого ключа.....	327
7.6. Системы двухфакторной аутентификации.....	368
7.6.1. Принципы работы двухфакторной аутентификации	369
7.6.2. Сравнение систем.....	372
7.6.3. Заключение.....	379
7.7. Однократная аутентификация	379
7.7.1. Принципы работы однократной аутентификации	381
7.7.2. Сравнение систем.....	383
7.8. Honeyrot – ловушка для хакера.....	389

7.8.1. Принципы работы.....	390
7.9. Заключение	393

Глава 8. Нормативная документация 395

8.1. Политики ИБ.....	395
8.2. Регламент управления инцидентами.....	409
8.3. Заключение	423

Приложение. Kali Linux – наш инструментарий 424

9.1. Немного о LiveCD	424
9.2. Инструментарий Kali Linux	427
9.2.1. Сбор сведений Information Gathering	429
9.2.2. Анализ уязвимостей Vulnerability Analysis	429
9.2.3. Анализ веб-приложений Web Application Analysis.....	429
9.2.4. Работа с базами данных Database Assessment	430
9.2.5. Взлом паролей Password Attacks.....	430
9.2.6. Работа с беспроводными сетями Wireless Attacks	430
9.2.7. Инструменты кракера Reverse Engineering	430
9.2.8. Средства Exploitation Tools	430
9.2.9. Средства перехвата Sniffing & Spoofing.....	430
9.2.10. Инструменты для закрепления Post Exploitation	431
9.2.11. Средства расследования Forensics.....	431
9.2.12. Построение отчетов Reporting Tools	431
9.2.13. Работа с людьми Social Engineering Tools.....	431
9.2.14. Системные сервисы System Services.....	431
9.4. Заключение	432
9.5. События BGP	432
9.6. Использованные источники.....	433