

Бирюков А.А.

# Информационная безопасность: защита и нападение

Третье издание,  
переработанное и дополненное





# ОГЛАВЛЕНИЕ

<b>Вступление .....</b>	<b>10</b>
0.1. Комментарии ко второму изданию .....	12
0.2. Комментарии к третьему изданию .....	13
0.3. Почему «защита и нападение» .....	14
0.4. Социальная инженерия вместо пролога.....	15
0.4.1. Чем грозит наличие у злоумышленника знаний о вашей сети? .....	16
0.4.2. «Разбираем» сканеры уязвимостей.....	16
0.4.3. Социальная инженерия.....	16
0.4.4. Исходные данные .....	20
0.4.5. Анализируем вакансии .....	20
0.4.6. Беседа как источник информации .....	21
0.4.7. Анализируем результат .....	22
0.4.8. Немного о средствах связи .....	22
0.4.9. Электронная почта как источник информации о сети .....	23
0.4.10. Доменное имя как источник информации .....	23
0.4.11. Атака на клиента.....	24
0.4.12. Срочный звонок.....	25
0.4.13. Кто потерял флешку?.....	26
0.4.14. Промежуточные итоги .....	27
0.4.15. Защита от СИ.....	27
0.4.16. Заключение .....	28
<b>Глава 1. Теоретические основы.....</b>	<b>29</b>
1.1. Модель OSI .....	30
1.1.1. Прикладной (7-й) уровень (Application Layer).....	31
1.1.2. Представительский (6-й) уровень (Presentation Layer).....	32
1.1.3. Сеансовый (5-й) уровень (Session Layer).....	32
1.1.4. Транспортный (4-й) уровень (Transport Layer) .....	32
1.1.5. Сетевой (3-й) уровень (Network Layer).....	32
1.1.6. Канальный (2-й) уровень (Data Link Layer) .....	32

1.1.7. Физический (1-й) уровень (Physical Layer) .....	33
1.2. Модель DOD.....	34
1.3. Заключение .....	35

## **Глава 2. Классификация атак по уровням иерархической модели OSI..... 36**

2.1. Атаки на физическом уровне .....	36
2.1.1. Концентраторы .....	36
2.1.2. Установка в разрыв.....	39
2.2. Атаки на канальном уровне.....	41
2.2.1. Атаки на коммутаторы.....	41
2.2.2. Переполнение CAM-таблицы.....	41
2.2.3. VLAN Hopping.....	45
2.2.4. Атаки на STP.....	46
2.2.5. DoS на STP .....	51
2.2.6. MAC Spoofing .....	52
2.2.7. Атака на PVLAN (Private VLAN) .....	52
2.2.8. Атака на DHCP .....	54
2.2.9. ARP-spoofing.....	55
2.2.10. Заключение .....	59
2.3. Атаки на сетевом уровне.....	59
2.3.1. Атаки на маршрутизаторы.....	59
2.3.2. Среды со статической маршрутизацией .....	62
2.3.3. Безопасность статической маршрутизации .....	63
2.3.4. Среды с динамической маршрутизацией.....	64
2.3.5. Scary – универсальное средство для реализации сетевых атак .....	64
2.3.6. Среды с протоколом RIP .....	68
2.3.7. Безопасность протокола RIP .....	69
2.3.8. Ложные маршруты RIP.....	71
2.3.9. Понижение версии протокола RIP .....	76
2.3.10. Взлом хеша MD5 .....	76
2.3.11. Обеспечение безопасности протокола RIP.....	78
2.3.12. Среды с протоколом OSPF .....	80
2.3.13. Безопасность протокола OSPF .....	86
2.3.14. Среды с протоколом BGP .....	87
2.3.15. Атака BGP Router Masquerading.....	87
2.3.16. Атаки на MD5 для BGP.....	88
2.3.17. «Слепые» DoS-атаки на BGP-маршрутизаторы .....	89
2.3.18. Безопасность протокола BGP .....	90
2.3.19. Атаки на BGP .....	92
2.3.20. Вопросы безопасности .....	97
2.3.21. Среды с протоколом IS-IS .....	98
2.3.22. Атаки на протокол IS-IS .....	99
2.3.23. Среды с протоколом MPLS.....	101
2.3.24. Безопасность протокола MPLS.....	103

2.3.25. IPSec как средство защиты на сетевом уровне .....	104
2.3.26. Целостность данных .....	104
2.3.27. Защита соединения .....	105
2.3.28. Заключение .....	114
2.4. Атаки на транспортном уровне .....	115
2.4.1. Транспортный протокол TCP .....	115
2.4.2. Известные проблемы .....	117
2.4.3. Атаки на TCP .....	118
2.4.4. IP-spoofing .....	118
2.4.5. TCP hijacking .....	120
2.4.6. Десинхронизация нулевыми данными .....	121
2.4.7. Сканирование сети .....	122
2.4.8. SYN-флуд .....	123
2.4.9. Атака Teardrop .....	124
2.4.10. Безопасность TCP .....	125
2.4.11. Атаки на UDP .....	126
2.4.12. UDP Storm .....	127
2.4.13. Безопасность UDP .....	128
2.4.14. Протокол ICMP .....	129
2.4.15. Методология атак на ICMP .....	130
2.4.16. Обработка сообщений ICMP .....	130
2.4.17. Сброс соединений (reset) .....	132
2.4.18. Снижение скорости .....	133
2.4.19. Безопасность ICMP .....	133
2.5. Атаки на уровне приложений .....	133
2.5.1. Безопасность прикладного уровня .....	133
2.5.2. Протокол SNMP .....	134
2.5.3. Протокол Syslog .....	138
2.5.4. Протокол DNS .....	140
2.5.5. Атаки на DNS .....	140
2.5.6. DNS для злоумышленника .....	142
2.5.7. Безопасность DNS .....	143
2.5.8. Веб-приложения .....	143
2.5.9. Атаки на веб через управление сессиями .....	144
2.5.10. Защита DNS .....	151
2.5.11. SQL-инъекции .....	152
2.6. Угрозы IP-телефонии .....	154
2.6.1. Возможные угрозы VoIP .....	156
2.6.2. Поиск устройств VoIP .....	157
2.6.3. Перехват данных .....	158
2.6.4. Отказ в обслуживании .....	159
2.6.5. Подмена номера .....	160
2.6.6. Атаки на диспетчеров .....	161
2.6.7. Хищение сервисов и телефонный спам .....	162
2.7 Анализ удаленных сетевых служб .....	163
2.7.1. ICMP как инструмент исследования сети .....	163

2.7.2. Утилита <code>fping</code> .....	165
2.7.3. Утилита <code>Nmap</code> .....	166
2.7.4. Использование «Broadcast ICMP» .....	167
2.7.5. ICMP-пакеты, сообщающие об ошибках.....	167
2.7.6. UDP Discovery.....	168
2.7.7. Исследование с помощью TCP .....	169
2.7.8. Использование флага SYN.....	170
2.7.9. Использование протокола IP.....	171
2.7.10. Посылки фрагмента IP-датаграммы .....	171
2.7.11. Идентификация узла с помощью протокола ARP .....	172
2.7.12. Меры защиты .....	173
2.7.13. Идентификация ОС и приложений .....	173
2.7.14. Отслеживание маршрутов .....	174
2.7.15. Сканирование портов .....	175
2.7.16. Идентификация сервисов и приложений .....	178
2.7.17. Особенности работы протоколов .....	180
2.7.18. Идентификация операционных систем.....	182
2.8. Заключение .....	183
<b>Глава 3. Атаки на беспроводные устройства.....</b>	<b>184</b>
3.1. Атаки на Wi-Fi.....	184
3.1.1. Протоколы защиты .....	184
3.1.2. Протокол WEP .....	185
3.1.3. Протокол WPA .....	185
3.1.4. Физическая защита .....	186
3.1.5. Соккрытие ESSID .....	187
3.1.6. Возможные угрозы .....	188
3.1.7. Отказ в обслуживании .....	188
3.1.8. Поддельные сети.....	189
3.1.9. Ошибки при настройке .....	190
3.1.10. Взлом ключей шифрования .....	191
3.1.11. Уязвимость 196.....	192
3.1.12. В обход защиты.....	192
3.1.13. Защита через веб .....	193
3.1.14. Проводим пентест Wi-Fi.....	193
3.1.15. Заключение .....	199
3.2. Безопасность Bluetooth .....	199
3.2.1. Угрозы Bluetooth.....	199
3.2.2. Другие беспроводные угрозы .....	202
3.3. Заключение .....	203
<b>Глава 4. Уязвимости.....</b>	<b>204</b>
4.1. Основные типы уязвимостей .....	204
4.1.1. Уязвимости проектирования .....	204

4.1.2. Уязвимости реализации .....	205
4.1.3. Уязвимости эксплуатации.....	205
4.2. Примеры уязвимостей .....	208
4.2.1. Права доступа к файлам .....	208
4.2.2. Оперативная память .....	210
4.2.3. Объявление памяти .....	210
4.2.4. Завершение нулевым байтом .....	211
4.2.5. Сегментация памяти программы.....	211
4.2.6. Переполнение буфера .....	214
4.2.7. Переполнения в стеке.....	216
4.2.8. Эксплойт без кода эксплойта.....	220
4.2.9. Переполнения в куче и bss .....	222
4.2.10. Перезапись указателей функций.....	222
4.2.11. Форматные строки.....	223
4.2.12. Сканирование приложений на наличие уязвимостей.....	227
4.2.13. Эксплуатация найденных уязвимостей.....	229
4.3. Защита от уязвимостей .....	235
4.3.1. WSUS .....	235
4.4. Заключение .....	236
<b>Глава 5. Атаки в виртуальной среде.....</b>	<b>237</b>
5.1. Технологии виртуализации.....	237
5.2. Сетевые угрозы в виртуальной среде .....	239
5.3. Защита виртуальной среды .....	240
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. Контейнеризация. Контейнеры Docker.....	244
5.6. Kubernetes.....	253
5.7. Заключение.....	268
<b>Глава 6. Облачные технологии.....</b>	<b>269</b>
6.1. Принцип облака .....	269
6.1.1. Структура ЦОД.....	270
6.1.2. Виды ЦОД.....	271
6.1.3. Требования к надежности.....	271
6.2. Безопасность облачных систем .....	282
6.2.1. Контроль над ситуацией .....	285
6.2.2. Ситуационный центр .....	286
6.2.3. Основные элементы построения системы ИБ облака.....	286
6.3. Заключение .....	287

<b>Глава 7. Средства защиты.....</b>	<b>288</b>
7.1. Организация защиты от вирусов.....	289
7.1.1. Способы обнаружения вирусов .....	290
7.1.2. Проблемы антивирусов .....	294
7.1.3. Архитектура антивирусной защиты.....	298
7.1.4. Борьба с нежелательной почтой.....	300
7.2. Межсетевые экраны.....	303
7.2.1. Принципы работы межсетевых экранов.....	305
7.2.2. Аппаратные и программные МЭ .....	307
7.2.3. Программный МЭ Iptables.....	307
7.2.4. Специальные МЭ.....	311
7.2.5. Next Generation Firewall.....	312
7.3. Средства обнаружения и предотвращения вторжений .....	314
7.3.1. Системы IDS/IPS.....	314
7.3.2. Web Application Firewall.....	320
7.3.2. Мониторинг событий ИБ в Windows 2019 .....	324
7.3.3. Промышленные решения мониторинга событий.....	331
7.4. Средства предотвращения утечек .....	334
7.4.1. Каналы утечек .....	337
7.4.2. Принципы работы DLP .....	340
7.4.3. Сравнение систем DLP.....	344
7.4.4. Заключение.....	345
7.5. Средства шифрования .....	346
7.5.1. Симметричное шифрование .....	346
7.5.2. Инфраструктура открытого ключа .....	346
7.6. Системы двухфакторной аутентификации.....	384
7.6.1. Принципы работы двухфакторной аутентификации .....	385
7.6.2. Сравнение систем .....	387
7.6.3. Заключение.....	391
7.7. Однократная аутентификация .....	391
7.7.1. Принципы работы однократной аутентификации .....	393
7.7.2. Решение Avanpost.....	394
7.8. Honeypot – ловушка для хакера .....	398
7.8.1. Принципы работы.....	399
7.9. Заключение.....	402
<b>Глава 8. Нормативная документация.....</b>	<b>403</b>
8.1. Политики ИБ .....	403
8.2. Регламент управления инцидентами .....	416
8.4. Заключение .....	429
<b>Приложение. Kali Linux – наш инструментарий.....</b>	<b>430</b>
П.1. Немного о LiveCD.....	430

П.2. Инструментарий Kali Linux .....	433
П.2.1. Сбор сведений Information Gathering.....	434
П.2.2. Анализ уязвимостей Vulnerability Analysis .....	435
П.2.3. Анализ веб-приложений Web Application Analysis.....	435
П.2.4. Работа с базами данных Database Assessment.....	435
П.2.5. Взлом паролей Password Attacks .....	435
П.2.6. Работа с беспроводными сетями Wireless Attacks.....	436
П.2.7. Инструменты кракера Reverse Engineering .....	436
П.2.8. Средства Exploitation Tools .....	436
П.2.9. Средства перехвата Sniffing & Spoofing .....	436
П.2.10. Инструменты для закрепления Post Exploitation.....	436
П.2.11. Средства расследования Forensics .....	437
П.2.12. Построение отчетов Reporting Tools.....	437
П.2.13. Работа с людьми Social Engineering Tools .....	437
П.2.14. Системные сервисы System Services.....	437
П.4. Заключение .....	437
П.5. События BGP.....	438
<b>Библиография .....</b>	<b>439</b>