УДК 004.065
ББК 32.973.26-018.2
Б64

Бирюков А. А.
Б64 Информационная безопасность: защита и нападение. – 3-е изд., перераб. и доп. – М.: ДМК Пресс, 2023. – 440 с.: ил.

ISBN 978-5-93700-219-8

Книги по информационной безопасности (ИБ) преимущественно делятся на две группы: в одних большей частью присутствует нормативная информация и мало сведений о технической реализации угроз и защите от них, в других описываются только технические аспекты (серии «…глазами хакера»).

Данная книга выдерживает уже третье издание, предлагая читателю глубокое погружение в практические аспекты реализации конкретных атак и средств защиты. Представлены как актуальная техническая информация, так и советы по организации процесса обеспечения информационной безопасности с соответствующими примерами.

В числе рассматриваемых тем: атаки на беспроводные устройства, безопасность облачных систем, выявление уязвимостей, средства обнаружения и предотвращения вторжений, борьба с утечками, обзор методов шифрования и многое другое.

Издание предназначено системным администраторам и пользователям малых и средних сетей, осуществляющим защиту корпоративных ресурсов.

УДК 004.065
ББК 32.973.26-018.2

ISBN 978-5-93700-219-8

ОГЛАВЛЕНИЕ

Вступление 10

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

Глава 1. Теоретические основы 29

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
2.2.5. MAC Spoofing 52
2.2.6. Атака на PVLAN (Private VLAN) 52
2.2.7. Атака на DHCP 54
2.2.8. ARP-spoofing 55
2.2.9. 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. Scapy – 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
2.5.4. Атаки на DNS 140
2.5.4. DNS для злоумышленника 142
2.5.5. Безопасность DNS 143
2.5.6. Веб-приложения 143
2.5.7. Атаки на веб через управление сессиями 144
2.5.8. Защита DNS 151
2.5.9. 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 fping 165
2.7.3. Утилита Nmap 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

Глава 3. Атаки на беспроводные устройства 184

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. Сокрытие 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
3.1.13. Проводим пентест Wi-Fi 193
3.1.14. Заключение 199
3.2. Безопасность Bluetooth 199
3.2.1. Угрозы Bluetooth 199
3.2.2. Другие беспроводные угрозы 202
3.3. Заключение 203

Глава 4. Уязвимости 204

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
4.2.12. Эксплуатация найденных уязвимостей 229
4.3. Защита от уязвимостей 235
4.3.1. WSUS 235
4.4. Заключение 236

Глава 5. Атаки в виртуальной среде 237

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

Глава 6. Облачные технологии 269

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

Глава 7. Средства защиты 288

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
7.2.2. Программный МЭ Iptables 307
7.2.2. Специальные МЭ 311
7.2.2. 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

Глава 8. Нормативная документация 403

8.1. Политики ИБ 403
8.2. Регламент управления инцидентами 416
8.4. Заключение 429

Приложение. Kali Linux – наш инструментарий 430

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

Библиография 439

ВСТУПЛЕНИЕ

В последние три десятилетия информационные технологии совершили настоящий прорыв. Появление гипертекста, IP-телефонии, увеличение тактовых частот процессоров и пропускной способности каналов связи, развитие «облачных технологий» и мобильных устройств и многое другое. Все это существенно усложнило процесс не только разработки, но и обслуживания ИТ-инфраструктуры. Появилась новая профессия – системный администратор.

Системный администратор является специалистом, обеспечивающим бесперебойную работу всей ИТ-инфраструктуры компании. Далеко не последнее место в работе сисадмина занимает обеспечение информационной безопасности корпоративных ресурсов.

Для обеспечения информационной безопасности администратору нужно как самому корректно устанавливать программное обеспечение, так и устанавливать обновления и исправления на уже использующееся ПО. Решение данных задач, особенно в крупных компаниях, требует зачастую много времени и большого числа специалистов, так как обычно в крупных компаниях обслуживанием системы телефонии, серверов электронной почты, веб-ресурсов и других систем занимаются разные специалисты. Но при этом каждая из этих систем должна быть построена с учетом требований по обеспечению информационной безопасности. Однако информационные системы, как правило, взаимосвязаны, например серверы электронной почты под управлением Microsoft Exchange должны входить в домен Active Directory, система IP-телефонии связана с почтовой системой, а веб-серверы связаны с серверами баз данных. Кроме того, благодаря развитию концепции BYOD (Bring Your Own Device, Принеси свое устройство с собой) многие сотрудники теперь используют для работы свои мобильные устройства: планшеты и телефоны. Эффективное обеспечение информационной безопасности для таких интегрированных систем требует от соответствующего специалиста обширных технических знаний в смежных областях, так как иначе плохая защищенность одного элемента интегрированной системы может свести на нет все усилия по защите других ее элементов. Как говорится, прочность всей цепи определяется прочностью ее самого слабого звена.

Лучше всего непосредственно при построении корпоративной сети использовать наиболее жесткие настройки для всех ресурсов. Как правило, произво-

дители приложений и оборудования сами рекомендуют использовать наиболее защищенные режимы работы и подробно описывают их настройку (например, применение сложных паролей для входа пользователей в систему, защита электронной почты от нежелательных рассылок, отключение учетных записей пользователей по умолчанию, запрет удаленного доступа к корпоративным ресурсам и т. д.).

Однако типичной ситуацией является наличие какой-либо корпоративной инфраструктуры, которая строилась на протяжении нескольких лет различными специалистами, на разных моделях оборудования и приложений. При этом в данную инфраструктуру встраиваются «облачные» сервисы, такие как «облачное» хранилище файлов, офисные приложения и другое. Также здесь актуальна проблема, уже упоминавшаяся ранее с использованием мобильных устройств. В таких случаях корпоративные ресурсы по различным причинам содержат уязвимости и недостатки, связанные с информационной безопасностью.

У системного администратора, как правило, много работы. Особенно в небольших компаниях, где порядка 100 рабочих мест, полтора-два десятка серверов и один, максимум два человека должны все это обслуживать. В результате эти специалисты ежедневно заняты текущей работой, такой как решение проблем пользователей, замена картриджей в принтерах и бумаги в факсах, подготовка рабочих мест для новых пользователей и т. п. При этом зачастую задачи по обеспечению безопасной настройки программного обеспечения и оборудования, написания инструкций и политик по информационной безопасности для пользователей ставятся на задний план и, как правило, не выполняются. Причиной этого является как занятость системных администраторов, так и отсутствие у них соответствующих знаний и навыков для обеспечения информационной безопасности.

Для крупных компаний эта проблема не так актуальна, потому что, например, в больших банках имеется отдел или даже департамент по обеспечению информационной безопасности. Соответственно, решением задач ИБ занимаются уже не системные администраторы, а администраторы по безопасности. При этом системные администраторы и администраторы по ИБ выполняют различные задачи, одни обслуживают ИТ-ресурсы и обеспечивают их функциональность, а другие обеспечивают безопасность ИТ-инфраструктуры. Администраторы по ИБ готовят политики и инструкции для системных администраторов.

Но в любом случае, независимо от того, кто отвечает за обеспечение информационной безопасности, системный администратор или администратор по ИБ, этому специалисту необходимо регулярно производить оценку защищенности корпоративных ИТ-ресурсов, то есть аудит информационной безопасности системы.

Конечно, многие крупные организации предпочитают привлекать для осуществления проверки защищенности корпоративной информационной системы профессиональных аудиторов. Однако это имеет смысл только для крупных организаций, к которым предъявляются требования различных стандартов (ГОСТ, ISO и др.). Небольшим компаниям подобный аудит просто не по карману, и поэтому задача осуществления практического аудита ложится на системного администратора как главного специалиста по корпоративной

сети. К тому же такие проверки необходимо делать регулярно, что также накладывает дополнительные расходы.

0.1. Комментарии ко второму изданию

Эта книга является вторым изданием. В отличие от предыдущей версии, здесь я несколько сократил описание устаревших технологий и протоколов, оставив лишь необходимые основы. При этом больше внимания было уделено современным решениям. Также со времени первого издания вышли новые версии операционных систем и приложений, которые представлены в этой книге, поэтому во втором издании данная информация также актуализирована. Кроме того, в книгу добавлены описания новых технологий и соответствующих угроз безопасности.

Отдельно в книге рассматриваются изменения в российском законодательстве, связанные с информационной безопасностью.

Более подробно основные отличия второго издания от первого представлены в следующей таблице:

Таблица 0.1. *Изменения во втором издании*

Глава	Что изменилось во втором издании
0. Вступление	Добавлен материал по хакерским USB-устройствам на базе макетной платы Teensy, предназначенным для хищения информации с пользовательских машин
1. Теоретические основы	Добавлен небольшой материал по модели DOD. В остальном данная глава оставлена без изменений
2. Классификация атак по уровням иерархической модели OSI	Разделы этой главы подверглись наибольшим изменениям: 1. Добавлены описания протоколов IS-IS и MPLS и возможные варианты реализации атак на них. 2. Сокращено описание большинства протоколов, описанных в главе. 3. Добавлено описание работы с утилитой Scapy. 4. Более подробно рассмотрены вопросы безопасности протокола BGP. 5. Примеры работы с IPSec рассмотрены для Windows Server 2008
3. Атаки на беспроводные устройства	В эту главу добавлен раздел, посвященный проведению аудита безопасности беспроводных соединений, в котором описываются практические действия, выполняемые хакером для проникновения. Также приводится концепция устройства для перехвата информации с беспроводных периферийных устройств типа клавиатура и мышь
4. Уязвимости	Эта глава существенно переработана. Помимо теоретического описания того, что такое уязвимости, в главе также приводится описание работы со сканерами уязвимостей Nessus и Open VAS, от установки до проведения непосредственного сканирования. Также в главе приводится подробное описание работы с пакетом Metasploit Framework, от начальной настройки до эксплуатации найденных при сканировании уязвимостей
5. Атаки в виртуальной среде	Обновлена информация об используемых для защиты технологиях и продуктах

Таблица 0.1 *(окончание)*

Глава	Что изменилось во втором издании
6. Облачные технологии	Глава дополнена новыми требованиями регуляторов в части размещения облачных систем
7. Средства защиты	В данной главе добавлены российские аналоги наиболее распространенных средств защиты информации. В частности, дается подробное описание таких средств, как SIEM, двухфакторная аутентификация и т. д.
8. Нормативная документация	Оставлено без изменений
9. Приложения	Добавлено актуальное описание Kali-Linux и библиография. Сокращен раздел, посвященный событиям BGP

0.2. Комментарии к третьему изданию

С момента выхода предыдущего издания книги прошло уже более пяти лет. Ландшафт российского рынка ИБ, да и ИТ в целом за это время изменился до неузнаваемости. Геополитические события последних полутора лет привели к тому, что российский рынок покинули практически все иностранные компании. В результате освободившиеся ниши на рынке активно заполняют российские разработчики.

Соответственно, разделы книги, посвященные технологиям и средствам защиты, были существенно переработаны. В частности, из книги полностью удалены описания иностранных решений. Единственное, что осталось из иностранного, – это описания настроек в ОС Windows. Например, настройка PKI. Описание настроек для Windows оставлено преднамеренно, так как пока еще данная ОС достаточно широко распространена у российских заказчиков. Однако, как известно, с 2025 года на объектах критической инфраструктуры, и не только, будет запрещено использование решений иностранного производства. Поэтому в книге добавлен материал по российским ОС.

Таблица 0.2. *Изменения в третьем издании*

Глава	Что изменилось в третьем издании
0. Вступление	Добавлен материал по OSINT и социальной инженерии
1. Теоретические основы	Данная глава оставлена без изменений
2. Классификация атак по уровням иерархической модели OSI	Разделы этой главы подверглись наибольшим изменениям: 1. Добавлено описание технологии TAP. 2. Добавлены описания DoS атак на сети и BGP Hijacking. 3. Добавлены описания TCP Handshake, технологии UDP инкапсуляция udp2raw. 4. Представлено описание использования DNS для злоумышленника. 5. Внесены дополнения по NMAP. 6. Добавлены описания атак на веб CSRF, аутентификация форм
3. Атаки на беспроводные устройства	В эту главу внесены небольшие изменения в части описания атак

Таблица 0.2 *(окончание)*

Глава	Что изменилось в третьем издании
4. Уязвимости	Добавлено дополнение по BufferOverflow
5. Атаки в виртуальной среде	Эта глава претерпела наибольшие изменения. Добавлена российская виртуализация, контейнеры, создание, настройка. Kubernetes-настройка и администрирование, вопросы безопасности. Удалены описания иностранных решений по обеспечению ИБ
6. Облачные технологии	Глава дополнена материалом про надежность ЦОД
7. Средства защиты	Эта глава также была серьезно изменена. Удалены иностранные антивирусы. Добавлено описание Iptables, NGFW, TAP vs. SPAN, WAF. Удалены иностранные SIEM, добавлены российские. Добавлены российские DLP и российские средства 2ФА, SSO
8. Нормативная документация	Оставлено без изменений
9. Приложения	Добавлено актуальное описание Kali-Linux и библиография

Также не осталось без внимания и развитие технологий. Так, добавлены разделы, посвященные контейнеризации и проблемам, связанным с ее безопасностью. Добавлены описания атак и инструментов для их реализации и защиты. Много внимания уделено решениям с открытым исходным кодом.

0.3. Почему «защита и нападение»

Моя книга называется «Информационная безопасность: защита и нападение». С понятием «защита», я думаю, ни у кого вопросов не возникнет. Администратор ИБ должен осуществлять защиту корпоративных ИТ-ресурсов. А вот причем здесь нападение? Для того чтобы эффективно защищать что-либо, необходимо хорошо знать способы нападения, дабы уметь предугадывать действия нападающих и предотвращать их.

А теперь поговорим о том, как все это связано с тематикой данной книги. Для кого она предназначена? Эта книга предназначена прежде всего для системных администраторов и специалистов по информационной безопасности, которые хотели бы разобраться в практических аспектах защиты корпоративных ресурсов от различных угроз. Основной упор при написании книги я делал именно на практические аспекты, то есть здесь не будет «размышлений на тему». Вместо пространных размышлений я постарался сделать основной упор на практические способы решения проблем ИБ, то есть здесь будут описываться различные сценарии и настройки приложений и сетевого оборудования, работа со средствами по поиску уязвимостей и многое другое. Также мы поговорим о том, как нужно писать инструкции и политики по обеспечению ИБ, коснемся законодательных основ обеспечения ИБ в контексте нормативных правовых актов Российской Федерации.

Итак, мы определились с тем, что эта книга является в определенной степени практическим руководством. Но у многих может возникнуть вопрос: а как насчет хакеров? Является ли эта книга руководством для компьютерных взломщиков? Отвечу так: в общем случае для начинающего хакера данная

книга может оказаться полезной в плане изучения основ ИБ, средств проникновения и защиты сетей и приложений. Однако использовать на практике для взломов конкретных систем приведенные в книге эксплойты и утилиты вряд ли получится, так как за то время, пока писалась и издавалась данная книга, были выпущены заплатки и обновления, закрывающие эти уязвимости. Кроме того, многие приведенные примеры уязвимостей и некорректных настроек сознательно упрощены автором, для того чтобы дать читателю представление об общем типе подобных уязвимостей и средствах борьбы с ними, а не для того чтобы научить проникать в чужие сети. Так что, юные исследователи компьютерных систем, если вы хотите узнать, как что работает в компьютерных системах, то эта книга для вас, но если вы хотите узнать, как взломать Пентагон, то тут она вряд ли сможет вам помочь.

Вот мы и подошли к основному вопросу, который рассматривается в моей книге, – поиску и устранению угроз безопасности информационной системы. Задача обнаружения и тем более устранения угроз безопасности информационной системы не является тривиальной. Как уже упоминалось выше, современные корпоративные сети состоят из множества различных устройств и приложений, и для обнаружения угроз необходимо иметь четкое представление о принципах работы данных систем, используемых протоколах, средствах защиты и многом другом.

В своей книге я постараюсь уделить как можно больше внимания практическим аспектам информационной безопасности применительно к техническим аспектам функционирования различных систем. То есть при рассмотрении вопросов, связанных с защитой локальной сети, я также расскажу об общих принципах функционирования различных сетевых протоколов и устройств. Возможно, для кого-то из читателей это покажется лишним напоминанием прописных истин и он пропустит данные разделы, но мне все же хотелось бы, чтобы практический материал, приведенный в этой книге, был понятен даже начинающим специалистам.

Да, говоря о практике, замечу, что для выполнения многих примеров, описанных в этой книге, вам потребуется дистрибутив Kali Linux. Более подробно узнать об этом дистрибутиве вы можете в приложениях.

Надеюсь, я сумел привлечь внимание читателя. Теперь перейдем к обсуждению ряда теоретических основ информационной безопасности, без которых вам будет сложно понять дальнейший материал.

0.4. Социальная инженерия вместо пролога

Прежде чем начать обсуждение технических аспектов обеспечения информационной безопасности, нелишним будет рассмотреть некоторые вопросы, связанные с социальной инженерией. В частности, рассмотрим, какую информацию о сети своей потенциальной жертвы злоумышленник может почерпнуть из открытых источников, не прибегая к каким-либо специальным средствам и вредоносному программному обеспечению.

В любой корпоративной сети, как правило, используется множество разнообразных устройств и приложений. Активное сетевое оборудование (Cisco, DLink, Huawei), операционные системы (Windows, разнообразные Linux и Unix),

веб-серверы (Apache, IIS, WebSphere), системы управления базами данных (MSSQL, MySQL, Oracle) и другие программные продукты – все это можно встретить в корпоративной сети даже средних размеров. Отдельной строкой идут средства информационной безопасности: антивирусы, межсетевые экраны, системы обнаружения вторжений. Конечно, системный администратор всегда должен хорошо знать свою сеть (хотя на практике часто бывает не совсем так). А вот потенциальным злоумышленникам знать о том, что используется в сети, совсем необязательно и даже крайне нежелательно.

0.4.1. Чем грозит наличие у злоумышленника знаний о вашей сети?

Идентификация сетевых ресурсов является важным подготовительным этапом перед осуществлением взлома. Если хакер знает, что ваш корпоративный портал работает под управлением IIS 10 под управлением Windows Server 2019, то ему необходимо найти уязвимости, которым подвержены данные программные продукты. Для этого проще всего поискать в базах уязвимостей. В случае если найти ничего не удалось, то особо продвинутый взломщик может попытаться самостоятельно найти «лазейку», собрав у себя точную копию взламываемой системы и попытавшись самостоятельно проанализировать код. Для этого есть специальные инструменты, которых мы коснемся в этом разделе. Проведя анализ уязвимостей «офлайн», затем хакер сможет быстро провести атаку и внедрить в атакуемую систему вредоносный код.

Далее в этой книге мы еще будем подробно рассматривать вопросы, посвященные удаленному анализу сетевых служб. В этом разделе мы рассмотрим такой малоизученный, но тем не менее важный аспект, как социальная инженерия.

0.4.2. «Разбираем» сканеры уязвимостей

Ознакомившись с предыдущими абзацами, многие могут задаться вопросом: зачем мне все это нужно, у меня же есть специализированный сканер уязвимостей, например Nessus или OpenVAS? Однако здесь стоит заметить, что коммерческие сканеры стоят недешево, и их, как правило, используют только для сканирования наиболее важных узлов в сети. Например, тех, что участвуют в обработке персональных данных в соответствии с ФЗ № 152 или защите критической инфраструктуры в соответствии с ФЗ № 187. Кроме этого, не стоит полагаться только на автоматизированные средства, которые при желании можно обмануть. При использовании социальной инженерии можно получить достоверную информацию, причем зачастую ее сообщает сам администратор целевой сети.

0.4.3. Социальная инженерия

Выше я попытался обосновать саму необходимость удаленного анализа сети для системных администраторов. Зная методы злоумышленников, легче от них защититься. Однако, говоря об информационной безопасности, все почему-то сразу вспоминают про антивирусы, межсетевые экраны и прочие технические

средства. А вот про людей, работающих в компании, при этом часто забывают. А ведь массу полезной информации хакер может почерпнуть из общения с сотрудниками компании и из открытых источников, не прибегая при этом к помощи вредоносных программ и других технических средств. Кстати, уязвимости, связанные с человеческим фактором, не получится обнаружить с помощью сканеров уязвимостей.

Конечно, работа с персоналом – это прежде всего задача HR-департамента (отдела кадров). Служба персонала осуществляет прием сотрудника на работу, подписание соответствующих документов, ознакомление с различными правилами, политиками и регламентами. Однако сотрудники отделов ИТ и ИБ должны также участвовать в этом процессе. В компании должна быть разработана политика информационной безопасности.

Рис. 0.1. *Типичный подход к пентесту*

Понятие OSINT

OSINT (open-source intelligence, разведка на основе открытых данных) – сбор информации о человеке или организации из открытых источников и ее последующий анализ.

Разведка на основе открытых данных активно применялась еще во время Второй мировой войны в Британии и США: специальные подразделения мониторили трансляции противника. В настоящее время методы OSINT используются не только во внешней политике, но и в сфере информационной безопасности.

В результате такого сбора информации можно выйти на нужных людей, отвечающих за выполнение тех или иных задач для последующей реализации атак с помощью социальной инженерии.

Конечно, OSINT – это отдельная большая тема, о которой можно было бы написать не одну книгу. Но, помимо прочего, сбор информации о других людях является не совсем законным занятием, так как нарушает ФЗ о персональных данных. Поэтому мы не будем углубляться в эту тему, но рассмотрим основные моменты, связанные с «пробивом», именно так на жаргоне называют сбор информации методами OSINT.

Итак, основной идентификатор, по которому можно искать данные о человеке, – это, конечно же, номер его мобильного телефона. Можно использовать для поиска и городской номер телефона, но, по-моему, большинство сейчас использует для связи именно мобильные номера, и по ним искать гораздо интереснее. Самым мощным и интересным инструментом для пробива является мессенджер Telegram. В отличие от традиционного веба, в Tg все очень быстро меняется, и в случае блокировки одного канала владельцы моментально создают его клоны.

Для поиска по номеру телефона в Telegram есть специальные боты. Обычно работа с этими ботами строится на платной основе по подписке, но в некоторых случаях довольно много информации можно получить бесплатно. В этой книге я не буду приводить названия каналов, в которых можно делать запросы данных по нескольким причинам. Прежде всего это не совсем законно. Кроме того, с момента написания этих строк до издания книги пройдет немало времени, и каналы за это время, скорее всего, изменятся. Ну и те, кому эти инструменты действительно нужны, найдут нужные каналы без труда сами.

Резонный вопрос: откуда эти боты берут информацию? Источниками информации, как правило, выступают базы данных, которые в свое время утекли в сеть. Так, на рисунке ниже представлен скриншот поискового запроса по номеру телефона, в результате которого была найдена информация из базы клиентов одного популярного сервиса по доставке еды.

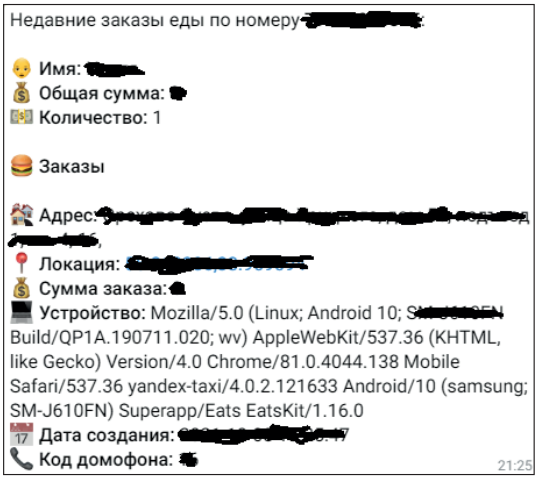

Рис. 0.2. *Результат запроса по номеру телефона*

Обычно боты агрегируют информацию из нескольких источников, таких как базы ГИБДД, сервисы такси, доставка товаров и еды, социальные сети и т. д. Ниже приведен небольшой фрагмент такого списка.

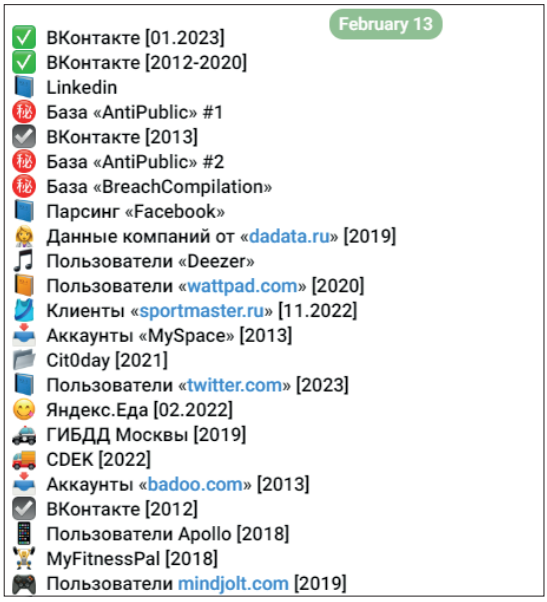

Рис. 0.3. *Список баз данных*

Как вы можете видеть, почти у каждого источника указан год. Это означает, что данные в этой базе актуальны на данный период, проще говоря, они были украдены именно в этот год. То есть информация, предоставляемая этими ботами, не является полностью актуальной, и это надо учитывать при ее использовании.

Однако поиск возможен не только по номеру телефона, например по ФИО, номеру машины, адресу и т. д.

Бот из примера ниже (рис. 0.4) предлагает поискать информацию о человеке по его изображению.

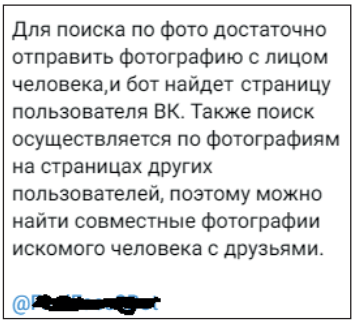

Рис. 0.4. *Описание поискового сервиса*

Конечно, телеграм-боты – это не единственное средство поиска информации о человеке. Иногда с помощью запроса в поисковике можно узнать много интересного. Также нелишним будет поиск в соцсетях.

Ну и для тех, кто серьезно заинтересовался этой темой, немного не совсем стандартных методов. Так, некоторые приложения для онлайн-банкинга при попытке перевода по номеру телефона показывают имя, отчество и первую букву фамилии получателя, а также банки, которые он использует. Иногда такая информация тоже может оказаться полезной.

0.4.4. Исходные данные

Прежде всего условимся о том, что известно злоумышленнику. Будем считать, что в самой компании у него нет никаких знакомых-инсайдеров, которые могут сообщить интересующую информацию. Также условимся, что хакер не нарушает закон. Он не использует всевозможные средства прослушивания, «жучки», скрытые камеры и прочее. В этом разделе мы не будем использовать никакие специализированные утилиты. Вся информация будет добываться исключительно из открытых источников.

Пусть он знает только название компании, сеть которой ему необходимо взломать. Кто-то посчитает, что этого недостаточно для того, чтобы начать взлом, и будет неправ.

Введя в поисковой системе название компании, злоумышленник быстро найдет ее официальный сайт. Вряд ли сейчас найдется хоть одна уважающая себя организация, у которой отсутствует свой сайт. А реклама, как известно, – двигатель торговли, и для связи могут использоваться не только стандартные телефон и e-mail, но и более современные средства коммуникации, такие как мессенджеры. В контексте удаленного анализа сети нам наиболее интересны электронная почта и Telegram. Очень часто в качестве контактов многие специалисты используют номера мобильных телефонов. В таком случае мы можем использовать методы из предыдущего раздела.

Также на корпоративном портале, помимо контактной информации, как правило, есть раздел Вакансии. Начнем сбор информации с этого пункта.

0.4.5. Анализируем вакансии

В разделе Вакансии могут оказаться описания требований к соискателям, в том числе и для ИТ-специалистов. В случае если такого раздела нет, можно попробовать поискать вакансии данной компании на сайтах по поиску работы. В описании вакансии системного администратора очень часто указывается наименование оборудования, операционных систем и приложений, с которыми придется работать. Вот пример описания реальной вакансии в одной компании:

Сетевой администратор в большую компанию ~ 1000 человек.
Филиалы компании в регионах по всей стране и СНГ.
Обязанности и требования:

- поддержка сетевых устройств: коммутаторов, маршрутизаторов и межсетевых экранов Checkpoint, Cisco, 3COM;

- мониторинг работы сетевых устройств и каналов связи на базе решений HPOpenView;
- обеспечение сетевого взаимодействия с филиалами;
- взаимодействие с провайдером услуг связи в процессе всего жизненного цикла предоставляемой услуги связи;
- обеспечение максимально быстрого восстановления работоспособности сетевой инфраструктуры.

Из этого на вид безобидного описания злоумышленник может сделать следующие выводы: в сети компании порядка 1000 машин, сеть географически распределенная, значит, используется VPN или арендованы каналы. В качестве средств защиты, скорее всего, применяется Checkpoint, маршрутизация и коммутация на Cisco и 3Com. Для подключения к интернету, вероятно, используются каналы связи только одного провайдера. Пока все достаточно размыто, осталось много вопросов.

Для их уточнения взломщику необходимо перейти к личному общению со специалистами. Для этого злоумышленнику проще всего воспользоваться той контактной информацией, которая предоставлена на сайте. Например, позвонить и поинтересоваться опубликованными на сайте вакансиями. Многие компании в целях экономии времени начальное собеседование проводят по телефону. Таким образом, специалисты по персоналу отсеивают явно не подходящих кандидатов. Злоумышленнику из общения с HR-менеджером вряд ли удастся получить много полезной технической информации, разве что уточнить количество пользователей и филиалов, да и то не всегда. Зато в процессе телефонного интервью злоумышленник может показать себя квалифицированным специалистом в требуемой области и быть приглашенным на собеседование.

На собеседования к квалифицированным кандидатам зачастую приглашают большое число специалистов (сетевых администраторов, инженеров по серверам, безопасников). Тут для злоумышленника большой простор для деятельности. В процессе дискуссии можно ненавязчиво узнать число филиалов. Кроме того, потенциального работника будут «гонять» прежде всего по тем технологиям, которые используются в корпоративной сети. Например, системные администраторы компании интересуются знаниями соискателя в области серверных операционных систем Windows и ActiveDirectory. Соискатель рассказывает про Windows 2016, затем про Windows 2019. На что собеседующие отвечают, что пока не все контроллеры используют Windows 2019. Далее обсуждается тема миграции доменов, вследствие чего выясняется, что все филиалы находятся в одном домене. Поддомены не используются.

0.4.6. Беседа как источник информации

Далее в процессе собеседования «берут слово» сетевики и безопасники. Они спрашивают, с чем и как приходилось работать. Какие модели оборудования использовались для межсетевого экранирования? Какие протоколы использовались для динамической маршрутизации? Какие корпоративные антивирусы знакомы соискателю? Внедрял ли он систему управления событиями безопасности? По степени их внимания к определенным темам можно сделать вывод об используемом в организации оборудовании.

0.4.7. Анализируем результат

В результате беседы выясняется, что в сети используется «зоопарк» решений. В некоторых филиалах применяются программные межсетевые экраны на базе Linux и iptables. В качестве коммутаторов в филиалах используются неуправляемые. Домен один для всех филиалов. Уровень домена Windows 2003. В филиалах установлены DC. Следовательно, все контроллеры домена равноправные, и взламывать можно сеть филиала, которая защищена хуже. Также было выявлено, что на данный момент централизованный мониторинг событий сейчас не ведется и они только готовятся к внедрению ArcSight. Количество рабочих мест в филиалах было также уточнено.

В довершение всего начальник ИТ-отдела посетовал, что во многих филиалах отсутствуют системные администраторы и обслуживанием имеющихся систем занимается кто-то из бухгалтеров или менеджеров. Из этого можно сделать вывод, что уровень технической грамотности в филиалах намного ниже и атаку будет провести значительно легче.

Кстати, многие руководители ИТ-отделов любят проводить экскурсии в серверную для своих потенциальных работников. А еще зачастую собеседования проводятся непосредственно в тех же комнатах, где и сидят ИТ-специалисты. Очень часто в таких помещениях на стенах висят планы сети с IP-адресацией. За полчаса, которые обычно длится собеседование, профессионал запомнит данную схему.

Кроме всего прочего, у злоумышленника после беседы останутся контакты тех, с кем он беседовал. Это могут быть визитки или письмо с приглашением на собеседование. Чем больше имен, тем больше дополнительной информации сможет собрать злоумышленник.

Информацию о данных специалистах можно поискать в интернете, а точнее в социальных сетях. Например, в сети LinkedIn многие специалисты размещают свои резюме, где описывается их профессиональная деятельность. Ознакомившись с такими резюме, злоумышленник сможет получить более точное представление о том, в каких технологиях наиболее силен данный специалист. Например, если в сети используется ОС Linux в качестве межсетевых экранов, а все администраторы компании являются специалистами по Windows, то можно предположить, что iptables настроен не лучшим образом.

Вообще, социальные сети – это большое зло. Люди своими руками пишут досье на самих себя и выкладывают это всем на обозрение.

0.4.8. Немного о средствах связи

В случае если попасть на собеседование не удалось. Допустим, компания не нуждается в технических специалистах. Злоумышленник может воспользоваться телефоном или мессенджером. Например, можно позвонить в компанию и попросить соединить с системным администратором. В случае если секретарь сплоховала и соединила, дальше под видом предложения о продаже расходных материалов и оргтехники попытаться выяснить используемое в сети оборудование и ПО. Способ, конечно, не самый эффективный, но лучше, чем ничего.

Дальше вспоминаем про мессенджеры. Посредством Skype злоумышленник может попытаться узнать IP-адрес корпоративного шлюза. Для этого хакер может попробовать отправить файл по Skype или Telegram. Далее с помощью пакетного анализатора можно отследить, на какой IP-адрес уходят пакеты. Правда, этот способ срабатывает не всегда, иногда в адресе получателя оказывается другой сервер Skype.

0.4.9. Электронная почта как источник информации о сети

Несмотря на то что данный материал посвящен социальной инженерии, мы постепенно переходим к техническим аспектам как к результату сбора информации. Ранее мы говорили о корпоративном портале, где обязательно должен быть контактный адрес электронной почты. Задача злоумышленника – отправив на этот адрес письмо, обязательно получить ответ. Затем необходимо открыть полученное письмо в исходном виде, включая заголовки.

```
Received: from mxfront29.mail.yandex.net ([127.0.0.1])
          by mxfront29.mail.yandex.net with LMTP id 6Axma6HQ
          for<xxxx@yandex.ru>; Wed, 1 Feb 2012 12:06:10 +0400
Received: from mx1.xxxx.ch (mx1.xxxx.ch [194.209.xx.xx])
          by mxfront29.mail.yandex.net (nwsmtp/Yandex) with ESMTP id 696C4lPv-696Wxxxx;
          Wed,  1 Feb 2012 12:06:10 +0400
X-Yandex-Front: mxfront29.mail.yandex.net
X-Yandex-TimeMark: 1328083570
X-Yandex-Spam: 1
```

Из приведенного заголовка можно узнать IP-адрес почтового сервера отправителя. Хотя этот адрес также можно выяснить и другим способом, о котором мы поговорим далее. Также последние три строки сообщают о том, какая система использовалась в качестве антиспама. В данном случае это антиспам Яндекса.

Кстати, получить свойства письма можно в веб-интерфейсе бесплатной почтовой службы.

Иногда в свойствах почтовых сообщений может присутствовать более интересная информация, например внутренний IP-адрес отправителя. Вообще, NAT должен скрывать внутреннюю адресацию, так как эта информация тоже интересна злоумышленнику.

0.4.10. Доменное имя как источник информации

Еще одно техническое отступление от темы СИ, тем не менее связанное с ней. Располагая название корпоративного сайта, злоумышленник может собрать ряд интересующих его сведений с помощью общедоступного сетевого ресурса. Зайдем на страницу http://www.ripn.net/whois. В строке запроса необходимо указать доменное имя интересующей компании. Вот пример результата поиска информации по доменному имени:

```
Domain: mydomain.com
Type: CORPORATE
Nserver: a.ns.mydomain.com. 82.198.xx.xx
Nserver: ns4.nic.ru.
```

```
Nserver: b.ns.mydomain.com. 212.33.xx.xx
State: REGISTERED, DELEGATED
Org: Joint Stock Company …
```

Мы получили информацию о DNS-записях, зарегистрированных для данного домена. Можно воспользоваться еще одним, русскоязычным сервисом – leader.ru. На этом сайте в поле Whois необходимо доменное имя (рис. 0.5).

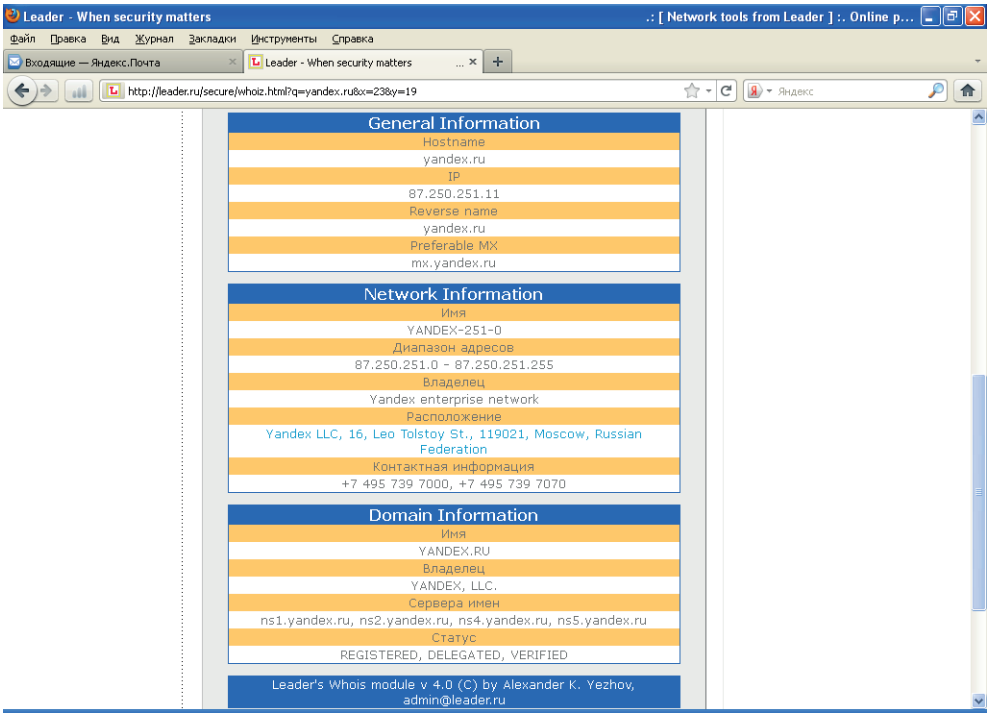

Рис. 0.5. *Результат работы*

Здесь результат более интересный. Помимо тех сведений, которые нам выдал предыдущий портал, здесь мы также получили сведения о диапазоне адресов, владельце и контактной информации, включающие в себя имя и фамилию ответственного, адрес электронной почты и телефон организации.

Полученные сведения можно также использовать для сбора информации теми методами, которые описывались ранее в этом разделе. Например, поискать информацию об ответственном специалисте в социальных сетях.

0.4.11. Атака на клиента

До этого момента мы рассматривали ситуацию, когда злоумышленник приходил на собеседование для сбора необходимой информации. Однако возможна и обратная ситуация, когда компания-конкурент приглашает на собеседование сотрудника и различными способами пытается получить необходимую информацию.

Например, можно заманить на собеседование системного администратора и попросить для подтверждения его профессиональных навыков рассказать о топологии той сети, которую он обслуживает. Еще можно попросить его показать те документы, которые приходилось разрабатывать. Таким образом можно также собирать информацию о сети для последующей атаки.

0.4.12. Срочный звонок

Вообще, социальная инженерия – это очень мощный инструмент, при правильном умении вести разговор (вспомните разведчика Штирлица) собеседник сам расскажет вам обо всем, что нужно.

Для начала приведу небольшую историю про известного взломщика Кевина Митника. Он умудрялся похищать информацию даже из тех сегментов сети, которые не были подключены к интернету. Делалось это следующим образом. Допустим, отдел А имеет подключение к интернету, а отдел Б той же компании не имеет. Митник, располагая адресной книгой компании, звонил сотруднику отдела Б, представляясь работником из А, и вежливо просил прислать ему факс с интересующей информацией, объясняя это тем, что он находится вне офиса и ему срочно нужны эти данные. Кто-то отказывал, но рано или поздно обязательно находился сотрудник (как правило, женщина), который выполнял просьбу хакера.

Несмотря на то что этой истории уже не один десяток лет, подобный способ получения информации до сих пор практикуется. Например, вам на мобильный телефон звонит некто, кого не очень хорошо слышно, представляется реально существующим сотрудником и просит сообщить, например, контактную информацию вашего руководителя или кого-либо из других сотрудников. Объясняется это тем, что звонящий находится вне офиса и ему срочно нужна данная информация. Многие в такой ситуации выполняют просьбу позвонившего. А ведь это может оказаться злоумышленник.

Правильным действием в такой ситуации является вежливый отказ в предоставлении информации. Например, можно сказать, что вам плохо слышно, и попросить перезвонить попозже. Однако этого не достаточно. В идеале об этом звонке необходимо сообщить в службу безопасности компании. Если же таковая отсутствует, или по каким-либо личным причинам вы не хотите к ним обращаться, то сообщите хотя бы своему непосредственному руководителю.

Кстати, та же служба безопасности часто проводит подобные «учения», звоня своим сотрудникам от имени неизвестных. Если требуемая информация была получена – сотрудника ждет наказание, в случае если ничего узнать не удалось, но при этом сообщили в службу безопасности, то сотрудника поощряют. Многие сочтут подобные провокации аморальными, однако этому методу обучают не только в учебных заведениях соответствующих силовых структур, но и на различных курсах по информационной безопасности.

Но вообще, действия пользователей в подобных ситуациях должны быть четко прописаны в корпоративной политике безопасности, которую подписывает каждый сотрудник при принятии на работу.

0.4.13. Кто потерял флешку?

Наверняка многим читателям приходилось находить флеш-накопители. Это может быть как собственная флешка, купленная очень давно и вновь найденная где-то под кипой документов, так и чей-то чужой накопитель, который вы обнаружили, например, по дороге в офис. В любом случае, обнаружив чужой USB-диск, вы обязательно захотите узнать, какая информация на нем находится, то есть попытаетесь подключить его к своему компьютеру. Конечно, многие задумаются, перед тем как подключать незнакомый носитель: а нет ли там вируса? Но, понадеявшись на свой антивирус и другое защитное ПО, все-таки подключат флешку к носителю. Однако даже если на USB-диске не было никаких вредоносных файлов, радоваться еще рано. Существуют устройства, по виду похожие на флешки, способные маскироваться в системе под легитимную периферию (HID, Human Interface Device) типа клавиатуры или мыши и выполнять практически любые действия под правами текущего пользователя. Однако обо всем по порядку.

В последние годы в мире ИТ набирает все больше оборотов концепция DIY (Do It Yourself – собери сам). Производители из Юго-Восточной Азии снабжают весь мир недорогими электронными компонентами, и прежде всего микросхемами. В интернете можно без труда найти не только спецификации на конкретные устройства, но и примеры рабочих проектов любого уровня сложности – от мигающих светодиодов до шагающих роботов. А появление беспаечных плат позволяет собрать проект буквально за несколько минут. Благодаря этому на рынке стали появляться недорогие (порядка $30) макетные платы, представляющие собой микроконтроллер с необходимыми деталями и контактами и USB-интерфейсом, с помощью которого она может получать питание и взаимодействовать с компьютером.

Тут стоит обратить внимание на еще один важный момент: раньше для прошивки микроконтроллеров необходимо было использовать дорогостоящие профессиональные устройства – программаторы, стоимость которых составляла от $1000. Однако функционал большинства таких устройств позволяет перепрошивать контроллер с помощью USB-порта, минуя дополнительные устройства.

Самой известной макетной платой является Arduino [10]. Для нее разработано множество готовых примеров конфигураций различных устройств. Доступна бесплатная среда разработки, в которой можно с помощью C-подобного языка запрограммировать микроконтроллер на выполнение определенных задач.

Для создания «протрояненных флешек» обычно используется один из клонов Arduino – макетная плата Teensy. По форм-фактору она представляет собой небольшую плату размером не больше флешки с разъемом типа Mini-USB. Будучи вмонтирована в какое-либо легальное устройство типа той же флешки или, как в моем случае, в USB-концентратор, она при подключении определяется в системе как клавиатура и начинает фактически имитировать нажатия пользователем различных клавиш, то есть выполнение команд, сценариев и т. д.

Разберем пример. Допустим, злоумышленник хочет похитить с машины жертвы некоторые файлы. С помощью социальной инженерии жертве каким-

либо образом подсовывается «заряженное» USB-устройство на базе платы Teensy. Например, он оставил на охране взламываемой компании несколько флешек, которые якобы выпали у входившего в здание сотрудника. Естественно, охранники, а затем и сотрудники не смогли побороть свое любопытство, и к вечеру у злоумышленника уже был доступ к нескольким машинам. Так что не стоит пренебрегать таким инструментом взлома. А вот дальше вступает в бой встроенный в это же устройство GSM-модуль.

Когда жертва включает флешку и необходимое ПО прописывается в системе, злоумышленник незаметно отправляет команды и получает результаты. Для специалиста изготовление GSM-модуля и его интеграция с USB-платой не являются очень сложной задачей, материалов в сети достаточно. Так что не стоит считать приведенный пример излишне надуманным.

Вообще, тема создания «хакерских» устройств – это материал для отдельной книги. Здесь я лишь упомянул о существовании таких устройств. Так что не стоит забывать, что в связке с социальной инженерией «протрояненные флешки» могут нести в себе большую опасность.

0.4.14. Промежуточные итоги

На этом я завершаю тему анализа сети посредством социальной инженерии и, прежде чем перейти к рассмотрению вопросов, связанных с защитой от данного типа атак, предлагаю подвести промежуточные итоги. Замечу, что собранная информация будет активно использоваться для дальнейшего исследования сети в других разделах книги.

В результате анализа сети было выявлено следующее: используется домен ActiveDirectoryWindows 2019, известно точное число филиалов, количество пользователей в каждой из подсетей, IP-адресация и модели используемого оборудования.

Теперь поговорим о том, как можно попытаться защититься от описанных ранее угроз.

0.4.15. Защита от СИ

Защититься от атак, осуществляемых с помощью социальной инженерии, не так просто, как от технических. Дело в том, что здесь основная угроза исходит не от плохо защищенного оборудования или неправильно настроенного приложения, а от людей, работающих с этими системами. Необходимо в разумных пределах ограничить ту информацию, которую может получить злоумышленник посредством социальной инженерии.

Например, в случае телефонных звонков секретарь должна обязательно спрашивать, кто звонит и по какому вопросу. Это позволит отсечь часть попыток сбора информации. Хотя, конечно, более продвинутые злоумышленники без труда обойдут такой «фейс-контроль».

Что касается объявлений о вакансиях, публикуемых на корпоративном сайте, то лучше указать несколько различных технологий и моделей оборудования в качестве требований, для того чтобы усложнить взломщику задачу сбора информации.

Пример с собеседованием, конечно, является не самым распространенным вариантом сбора информации, так как большинство хакеров работают удаленно и они скорее будут использовать сканеры портов и генераторы пакетов, чем общаться с представителями взламываемой организации напрямую. Однако не стоит забывать о таком способе сбора информации.

Кроме того, не все обладают соответствующими актерскими способностями и навыками, для того чтобы грамотно пройти собеседование и получить необходимую информацию.

Собеседования с соискателями лучше проводить в переговорных комнатах. А для проверки профессиональных навыков лучше не полениться и придумать несколько «задач», которые не связаны с текущей сетевой архитектурой компании.

Вообще, наилучшим решением описанных ранее проблем является внимательное рассмотрение той информации, которую может злоумышленник получить, что он с ней потом сможет сделать. Например, в процессе технического собеседования задавать вопросы соискателю, но при этом стараться избегать ответов на его вопросы относительно имеющейся инфраструктуры сети. Например, говорить, что у вас несколько сотен рабочих мест, не уточняя более точного значения.

Просто не стоит забывать, что диалог – это общение нескольких человек и что вы можете не только получать информацию, но и отдавать ее, иногда сами не замечая этого.

0.4.16. Заключение

В этой главе я привел примеры того, как, не используя никаких хакерских утилит и прочих не совсем законных методов, потенциальный злоумышленник может собрать информацию, необходимую для осуществления взлома сети. Данный материал я преднамеренно разместил в самом начале своей книги, для того чтобы обратить внимание технических специалистов на проблему «социальной инженерии».

Пожелания и предложения можно направить автору в телеграм @Andrey_A2512.

ГЛАВА 1
Теоретические основы

В любой организации, независимо от ее размеров, всегда есть корпоративная сеть. Даже если у вас маленькая контора, в которой всего два или три компьютера, они все равно должны быть объединены в сеть и иметь доступ в интернет. Таковы реалии современного бизнеса, всем нужен доступ к электронной почте, всем нужен доступ к информации во Всемирной информационной паутине. Однако локальные сети бывают не только в организациях. Зачастую во многих квартирах имеется по нескольку компьютеров и каждому из них тоже необходим доступ к ресурсам интернета. Например, у многих пользователей дома есть основной компьютер, ноутбук, карманный компьютер или коммуникатор. Всем этим устройствам в той или иной степени необходимо обмениваться файлами между собой, иметь доступ в интернет. Для организации такого доступа используют активное сетевое оборудование: маршрутизаторы, межсетевые экраны, коммутаторы, беспроводные точки доступа и концентраторы. Хотя последние встречаются все реже. Вообще, сейчас, как правило, для доступа домашних пользователей в интернет используют устройства, сделанные по принципу «все в одном». То есть одно устройство объединяет в себе функции межсетевого экрана, простейшего маршрутизатора, коммутатора и точки беспроводного доступа. Для домашних пользователей такое устройство является наилучшим решением, так как одна «коробка» занимает меньше места, к ней нужно вести меньше проводов, кроме того, ее легче настраивать. В корпоративных сетях, где присутствует более 20 рабочих станций, такие решения стараются не использовать, так как при одновременном подключении большого количества рабочих станций у многофункциональных сетевых устройств резко снижается производительность. Кроме того, в случае выхода из строя такого устройства вы лишитесь как доступа в интернет, так и доступа во внутреннюю локальную сеть. Так что, господа системные администраторы, если ваш дешевый Dlink прекрасно работает в домашней сети, то не торопитесь советовать руководству покупать такой же дешевый Dlink для корпоративной сети. Решать проблемы, которые потом возникнут, придется прежде всего вам.

Но вернемся к вопросам сетевой безопасности. Любая локальная сеть не мыслима без сетевого оборудования. А против сетевых устройств существует масса различных атак, направленных на перехват информации, проходящей по сети, захват управления устройством или временный вывод его из строя.

У читателя может возникнуть вопрос: почему, говоря о сети, я говорю только о сетевом оборудовании, ведь в сети также работает множество приложений, например серверы баз данных или электронная почта? Отвечу так: несомненно, в сети работает множество различных приложений, но в рамках обсуждения сетевой безопасности мы обсудим работу именно сетевого оборудования,

так как работу приложений мы будем рассматривать в главе «Атаки на уровне приложений».

Однако, прежде чем начать обсуждение способов осуществления этих атак и средств защиты, необходимо вспомнить (я надеюсь) основы сетевых технологий, иначе материал последующих разделов может превратиться для читателя в набор непонятных терминов. Конечно, если вы можете слету вспомнить модель OSI, знаете, что такое Spanning Tree Protocol или PVLAN, то вы можете смело переходить к чтению следующих разделов.

1.1. Модель OSI

При осуществлении передачи данных от компьютера к компьютеру в сети производится множество операций. При этом пользователя совершенно не интересует, как именно это происходит, ему необходим доступ к приложению или компьютерному ресурсу, расположенному в другом компьютере сети. На самом деле вся передаваемая информация проходит много этапов обработки. Прежде всего она разбивается на блоки, каждый из которых снабжается управляющей информацией. Получившиеся в результате блоки оформляются в виде сетевых пакетов, затем эти пакеты кодируются, передаются с помощью электрических или световых сигналов по сети в соответствии с выбранным методом доступа, далее из принятых пакетов вновь восстанавливаются заключенные в них блоки данных, блоки соединяются в данные, которые и становятся доступны другому приложению. Приведенное здесь описание является упрощенным пояснением происходящих процессов. Часть из указанных процедур реализуется только программно, другая часть – аппаратно, а какие-то операции могут выполняться как программами, так и аппаратурой. Упорядочить все выполняемые процедуры, разделить их на уровни и подуровни, взаимодействующие между собой, как раз и призваны модели сетей. Модели сетей позволяют правильно организовать взаимодействие как абонентам внутри одной сети, так и самым разным сетям на различных уровнях. В настоящее время наибольшее распространение получила так называемая эталонная модель обмена информацией открытой системы OSI (Open System Interchange). Под термином «открытая система» понимается не замкнутая в себе система, имеющая возможность взаимодействия с какими-то другими системами (в отличие от закрытой системы).

Обращаясь к истории создания иерархической модели, скажу, что модель OSI была предложена Международной организацией стандартов ISO (International Standards Organization) в 1984 году. С тех пор ее используют (более или менее строго ей соответствуют) все производители сетевых продуктов. Модель OSI не лишена ряда недостатков, присущих универсальным моделям, а именно она громоздка, избыточна и не слишком гибка. В результате реальные сетевые средства, предлагаемые различными фирмами, не обязательно придерживаются принятого разделения функций, то есть возможны устройства, сочетающие в себе функционал различных уровней. Однако знакомство с моделью OSI позволяет лучше понять, что же происходит в сети и соответственно как лучше ее защищать. Все сетевые функции в модели разделены на 7 уровней. При этом вышестоящие уровни выполняют более сложные, глобальные задачи,

для чего используют в своих целях нижестоящие уровни, а также управляют ими. Цель нижестоящего уровня – предоставление услуг вышестоящему уровню, причем вышестоящему уровню не важны детали выполнения этих услуг. Нижестоящие уровни выполняют более простые и конкретные функции. В идеале каждый уровень взаимодействует только с теми, которые находятся рядом с ним (выше и ниже него). Верхний уровень соответствует прикладной задаче, работающему в данный момент приложению, например веб-браузеру, нижний – непосредственной передаче сигналов по каналу связи.

Данные, которые необходимо передать по сети, на пути от верхнего (седьмого) уровня приложений до нижнего (первого) физического, проходят процесс инкапсуляции, то есть каждый нижеследующий уровень не только производит обработку данных, приходящих с более высокого уровня, но и снабжает их своим заголовком, а также добавляет к нему служебную информацию. Такой процесс обрастания служебной информацией продолжается до последнего (физического) уровня. На физическом уровне вся эта многооболочечная конструкция передается по кабелю приемнику. Там происходит обратный процесс – декапсуляция, то есть при передаче на вышестоящий уровень убирается одна из оболочек. Верхнего, седьмого, уровня достигают уже данные, освобожденные от всех оболочек, то есть от всей служебной информации нижестоящих уровней. При этом каждый уровень принимающего абонента производит обработку данных, полученных с нижеследующего уровня в соответствии с убираемой им служебной информацией.

В тех случаях, когда на пути между абонентами в сети включаются некие промежуточные устройства (например, концентраторы, коммутаторы, маршрутизаторы), то и они тоже могут выполнять функции, входящие в нижние уровни модели OSI. Чем больше сложность промежуточного устройства, тем больше уровней оно захватывает. В случае если между получателем и отправителем присутствует межсетевой экран, будут обработаны все семь уровней иерархической модели. Но любое промежуточное устройство должно принимать и возвращать информацию на нижнем, физическом уровне. Все внутренние преобразования данных должны производиться дважды и в противоположных направлениях. Промежуточные сетевые устройства, в отличие от полноценных абонентов (например, компьютеров), работают только на нижних уровнях и к тому же выполняют двустороннее преобразование.

Теперь поговорим подробнее о функциях разных уровней.

1.1.1. Прикладной (7-й) уровень (Application Layer)

Это уровень приложений, который обеспечивает услуги, непосредственно поддерживающие приложения пользователя. Примером таких приложений являются: программные средства работы с гипертекстом (HTTP), передачи файлов (FTP), доступа к базам данных (клиенты баз данных), средства электронной почты (Microsoft Outlook), службы регистрации на сервере (RADIUS). Этот уровень фактически управляет всеми остальными шестью уровнями. Примером может являться работа с таблицами Excel, когда пользователь сохраняет файл на сетевой ресурс. В этом случае прикладной уровень обеспечивает перемещение файла с рабочего компьютера на сетевой диск прозрачно для пользователя.

1.1.2. Представительский (6-й) уровень (Presentation Layer)

Это уровень представления данных, который определяет и преобразует форматы данных и их синтаксис в форму, удобную для сети, то есть выполняет функцию переводчика. Здесь же производится шифрование и дешифрирование данных, а при необходимости – и их сжатие. Стандартные форматы существуют для текстовых файлов (ASCII, HTML), звуковых файлов (MPEG, WAV), рисунков (JPEG, GIF, TIFF), видео (AVI). Все преобразования форматов делаются на представительском уровне. Если данные передаются в виде двоичного кода, то преобразования формата не требуется.

1.1.3. Сеансовый (5-й) уровень (Session Layer)

На этом уровне производится управление проведением сеансов связи (то есть осуществляются установка, поддержка и прекращение связи). Этот уровень предусматривает три режима установки сеансов: симплексный (передача данных в одном направлении), полудуплексный (передача данных поочередно в двух направлениях) и полнодуплексный (передача данных одновременно в двух направлениях). Сеансовый уровень может также вставлять в поток данных специальные контрольные точки, которые позволяют контролировать процесс передачи при разрыве связи. Этот же уровень распознает логические имена абонентов, контролирует предоставленные им права доступа.

1.1.4. Транспортный (4-й) уровень (Transport Layer)

Этот уровень обеспечивает доставку пакетов без ошибок и потерь, а также в нужной последовательности. На нем же производится разбивка передаваемых данных на блоки, помещаемые в пакеты, и восстановление принимаемых данных из пакетов. Доставка пакетов возможна как с установлением соединения (виртуального канала), так и без. Транспортный уровень является пограничным и связующим между верхними тремя, сильно зависящими от приложений, и тремя нижними уровнями, сильно привязанными к конкретной сети.

1.1.5. Сетевой (3-й) уровень (Network Layer)

Производит адресацию пакетов и перевод логических имен (логических адресов, например IP-адресов) в физические сетевые MAC-адреса (и обратно). На этом же уровне решается задача выбора маршрута (пути), по которому пакет доставляется по назначению (если в сети имеется несколько маршрутов). На сетевом уровне действуют такие сложные промежуточные сетевые устройства, как маршрутизаторы.

1.1.6. Канальный (2-й) уровень (Data Link Layer)

Другое название – уровень управления каналом передачи – отвечает за формирование пакетов (кадров) стандартного для данной сети (например, Ethernet) вида, включающих начальное и конечное управляющие поля. Здесь же произ-

водится управление доступом к сети, обнаруживаются ошибки передачи путем подсчета контрольных сумм и производится повторная пересылка приемнику ошибочных пакетов. Канальный уровень делится на два подуровня: верхний LLC и нижний MAC. Верхний подуровень (LLC – Logical Link Control) осуществляет управление логической связью, то есть устанавливает виртуальный канал связи. Строго говоря, эти функции не связаны с конкретным типом сети, но часть из них все же возлагается на аппаратуру сети (сетевой адаптер). Другая часть функций подуровня LLC выполняется программой драйвера сетевого адаптера. Подуровень LLC отвечает за взаимодействие с уровнем 3 (сетевым). Нижний подуровень (MAC – Media Access Control) обеспечивает непосредственный доступ к среде передачи информации (каналу связи). Он напрямую связан с аппаратурой сети. Именно на подуровне MAC осуществляется взаимодействие с физическим уровнем. Здесь производятся контроль состояния сети, повторная передача пакетов заданное число раз при коллизиях, прием пакетов и проверка правильности передачи. На канальном уровне работают такие промежуточные сетевые устройства, как, например, коммутаторы.

1.1.7. Физический (1-й) уровень (Physical Layer)

Это самый нижний уровень модели, который отвечает за кодирование передаваемой информации в уровни сигналов, принятые в используемой среде передачи, и обратное декодирование. Здесь же определяются требования к соединителям, разъемам, электрическому согласованию, заземлению, защите от помех и т. д. На физическом уровне работают такие сетевые устройства, как концентраторы (рис. 1.1).

Для того чтобы читателю стал более понятен приведенный выше материал, приведу несколько простых примеров. Что происходит, когда вы запрашиваете какие-либо данные по сети, например HTML-страницу? Ваш веб-браузер (уровень приложений) формирует запрос по протоколу HTTP (уровень представлений и сеансовый уровень), формируются пакеты, передаваемые на порт 80 (транспортный уровень), на IP-адрес веб-сервера (сетевой уровень). Эти пакеты передаются сетевой карте вашего компьютера, которая передает их в сеть (канальный и физический уровни). По пути следования пакеты проходят через различные промежуточные устройства: коммутаторы, маршрутизаторы, межсетевые экраны. Каждое из этих устройств может осуществлять проверку пакета в соответствии со своими настройками. Например, в зависимости от IP-адреса назначения маршрутизатор перешлет пакеты в определенную сеть. А межсетевой экран разрешит или запретит передачу данных пакетов. Когда пакеты достигнут узла назначения, будет произведено обратное преобразование. Из пакетов будет извлечена информация, соответствующая каждому из уровней иерархической модели.

Говоря о том, на каком уровне данной модели работают различные устройства, хотелось бы отдельно сказать о таких устройствах безопасности, как межсетевые экраны. В общем случае межсетевой экран работает на уровне приложений. То есть он разбирает проходящий через него пакет, выделяя из него атрибуты каждого из уровней модели и проверяя их на соответствие корпоративной политике безопасности. Выполняемые при этом действия будут выглядеть так:

- проверка IP-адреса отправителя и получателя (сетевой уровень);
- проверка порта, на который передается пакет (транспортный уровень);
- проверка соответствия сеансовым уровням и уровням представления;
- проверка, соответствует ли содержимое пакета структуре данных того протокола, который разрешен на данном порту (уровень приложений).

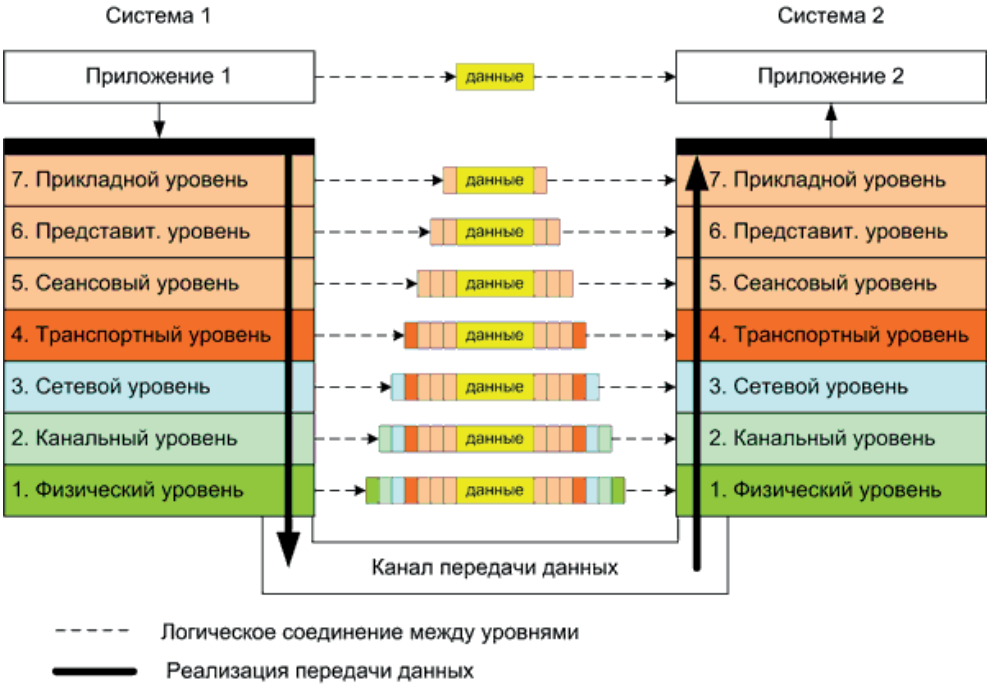

Рис. 1.1. *Схема пакета для различных уровней OSI*

Например, если вы попытаетесь под видом DNS-пакета передать, скажем, HTTP-пакет (осуществить туннелирование, спрятать HTTP в DNS), то межсетевой экран выполнит алгоритм, приведенный выше. Очевидно, что IP-адрес, порт и проверка сеансового уровня будут пройдены успешно. А вот дальше в зависимости от конкретной политики межсетевого экрана на уровне представлений или на уровне приложений будет обнаружено, что в нашем DNS-пакете на самом деле находятся данные, не соответствующие структуре пакетов для данного протокола. И такой пакет должен быть заблокирован.

Но не все межсетевые экраны разбирают пакет до уровня приложений, многие дешевые модели ограничиваются проверкой данных сетевого и транспортного уровней, что не всегда безопасно.

1.2. Модель DOD

Многие разработчики считают модель OSI излишне сложной в плане классификации протоколов, так как современные устройства зачастую работают сразу

на нескольких уровнях иерархической модели. В противовес модели OSI была разработана модель DOD, состоящая из следующих четырех уровней:

- уровень приложений, или прикладной уровень (англ. *process/application*; соответствует трем верхним уровням модели OSI (прикладному уровню, уровню представления и сеансовому уровню));
- транспортный уровень (англ. *transport*; соответствует транспортному уровню модели OSI);
- межсетевой уровень (англ. *internet*; соответствует сетевому уровню модели OSI);
- уровень сетевого доступа (англ. *network access*; соответствует двум нижним уровням модели OSI (физическому уровню и канальному уровню)).

Хотя четырехуровневая модель DOD больше подходит для классификации некоторых устройств, на практике иерархическая модель OSI получила более широкое распространение, поэтому в дальнейшем мы будем классифицировать протоколы и атаки именно по уровням модели OSI.

1.3. Заключение

Итак, мы разобрались с устройствами, выяснили, как организовано взаимодействие между ними. Теперь поговорим о том, какие атаки возможны на сетевые устройства, работающие на определенном уровне модели OSI.