

# СОДЕРЖАНИЕ

|   |           |
|---|-----------|
| <b>Отзывы о книге</b>                                     | <b>13</b> |
| <b>Благодарности</b>                                      | <b>15</b> |
| <b>Введение</b>   | <b>17</b> |
| Зачем нужна эта книга                                     | 17        |
| Основные понятия и принятый подход                        | 18        |
| Как пользоваться этой книгой                              | 20        |
| О примерах файлов перехвата                               | 20        |
| Фонд поддержки технологий в сельской местности            | 21        |
| Как связаться с автором книги                             | 21        |
| От издательства   | 21        |
| <b>Глава 1. Анализ пакетов и основы организации сетей</b> | <b>23</b> |
| Анализ пакетов и их анализаторы                           | 24        |
| Оценка анализатора пакетов                                | 24        |
| Принцип действия анализаторов пакетов                     | 26        |
| Установление связи между компьютерами                     | 26        |
| Сетевые протоколы   | 27        |
| Семиуровневая модель OSI                                  | 28        |
| Сетевое оборудование                                      | 35        |
| Классификация сетевого трафика                            | 41        |
| Широковещательный трафик                                  | 41        |
| Многоадресатный трафик                                    | 43        |
| Одноадресатный трафик                                     | 43        |
| Заключительные соображения                                | 43        |
| <b>Глава 2. Подключение к сети</b>                        | <b>45</b> |
| Прослушивание сети в смешанном режиме                     | 46        |
| Анализ пакетов через концентраторы                        | 47        |
| Анализ пакетов в коммутируемой среде                      | 49        |
| Зеркальное отображение портов                             | 50        |
| Перехват пакетов через концентратор                       | 52        |
| Применение сетевого ответвителя                           | 54        |
| Заражение ARP-кеша  | 58        |

|   |            |
|---|------------|
| Анализ пакетов в маршрутизируемой среде                                       | 64         |
| Размещение анализатора пакетов на практике                                    | 66         |
| <b>Глава 3. Введение в Wireshark</b>  | <b>69</b>  |
| Краткая история создания Wireshark  | 69         |
| Преимущества Wireshark  | 70         |
| Установка Wireshark   | 71         |
| Установка в системах Windows  | 72         |
| Установка в системах Linux  | 74         |
| Основы работы в Wireshark   | 77         |
| Первый перехват пакетов   | 77         |
| Главное окно Wireshark  | 79         |
| Глобальные параметры настройки Wireshark                                      | 80         |
| Цветовая кодировка пакетов  | 82         |
| Файлы конфигурации  | 85         |
| Профили конфигурации  | 85         |
| <b>Глава 4. Обработка перехваченных пакетов</b>                               | <b>89</b>  |
| Обработка файлов перехвата  | 89         |
| Сохранение и экспорт файлов перехвата   | 89         |
| Объединение файлов перехвата  | 90         |
| Обработка пакетов   | 91         |
| Поиск пакетов   | 92         |
| Отметка пакетов   | 93         |
| Вывод пакетов на печать   | 94         |
| Задание форматов отображения времени и привязок к нему                        | 95         |
| Форматы отображения времени   | 95         |
| Временная привязка к пакетам  | 96         |
| Временной сдвиг   | 97         |
| Настройка параметров перехвата  | 98         |
| Вкладка Input   | 98         |
| Вкладка Output  | 99         |
| Вкладка Options   | 101        |
| Применение фильтров   | 102        |
| Фильтры перехвата   | 103        |
| Фильтры отображения   | 110        |
| Сохранение фильтров   | 114        |
| Помещение фильтров отображения на панель инструментов                         | 115        |
| <b>Глава 5. Дополнительные возможности Wireshark</b>                          | <b>117</b> |
| Конечные точки и сетевые диалоги  | 117        |
| Просмотр статистики в конечных точках   | 118        |
| Просмотр сетевых диалогов   | 120        |
| Выявление наиболее активных сетевых узлов с помощью конечных точек и диалогов | 121        |

|   |            |
|---|------------|
| Статистические данные по иерархии сетевых протоколов  | 124        |
| Преобразование имен                                   | 126        |
| Активизация процесса преобразования имен              | 126        |
| Потенциальные недостатки преобразования имен          | 128        |
| Применение специального файла hosts                   | 129        |
| Иницилируемое вручную преобразование имен             | 130        |
| Дешифрирование сетевых протоколов                     | 131        |
| Смена дешифратора                                     | 131        |
| Просмотр исходного кода дешифраторов                  | 134        |
| Отслеживание потоков                                  | 134        |
| Отслеживание потоков SSL                              | 136        |
| Длина пакетов   | 138        |
| Составление графиков                                  | 139        |
| Просмотр графиков ввода-вывода                        | 139        |
| Составление графика времени круговой передачи пакетов | 143        |
| Составление графиков потоков                          | 145        |
| Экспертная информация                                 | 146        |
| <b>Глава 6. Анализ пакетов из командной строки</b>    | <b>149</b> |
| Установка утилиты TShark                              | 150        |
| Установка утилиты tcpdump                             | 151        |
| Перехват и сохранение пакетов                         | 152        |
| Манипулирование выводимыми результатами               | 156        |
| Преобразование имен                                   | 160        |
| Применение фильтров                                   | 161        |
| Форматы отображения времени в TShark                  | 163        |
| Сводная статистика в TShark                           | 164        |
| Сравнение утилит TShark и tcpdump                     | 168        |
| <b>Глава 7. Протоколы сетевого уровня</b>             | <b>169</b> |
| Протокол преобразования адресов (ARP)                 | 170        |
| Структура ARP-пакета                                  | 172        |
| Пакет 1: ARP-запрос                                   | 173        |
| Пакет 2: ARP-ответ                                    | 174        |
| Непрошенные, или самообращенные ARP-пакеты            | 174        |
| Межсетевой протокол (IP)                              | 176        |
| Межсетевой протокол версии 4 (IPv4)                   | 176        |
| Межсетевой протокол версии 6 (IPv6)                   | 185        |
| Протокол межсетевых управляющих сообщений (ICMP)      | 199        |
| Структура заголовка в пакете ICMP                     | 200        |
| Типы и коды сообщений протокола ICMP                  | 200        |
| Эхо-запросы и ответы                                  | 201        |
| Протокол ICMP версии 6 (ICMPv6)                       | 207        |

|  |            |
|--|------------|
| <b>Глава 8. Протоколы транспортного уровня</b>             | <b>209</b> |
| Протокол управления передачей (TCP)                        | 209        |
| Структура заголовка в пакете TCP                           | 210        |
| Порты TCP  | 211        |
| Трехэтапный процесс установки связи по протоколу TCP       | 214        |
| Разрыв связи по протоколу TCP                              | 217        |
| Сбросы соединений по протоколу TCP                         | 219        |
| Протокол пользовательских дейтаграмм (UDP)                 | 220        |
| Структура заголовка в пакете UDP                           | 221        |
| <b>Глава 9. Распространенные протоколы верхнего уровня</b> | <b>223</b> |
| Протокол динамической настройки узла сети (DHCP)           | 223        |
| Структура заголовка в пакете DHCP                          | 224        |
| Процесс инициализации по протоколу DHCP                    | 225        |
| Возобновление аренды IP-адреса по протоколу DHCP           | 231        |
| Параметры и типы сообщений в протоколе DHCP                | 232        |
| Версия 6 протокола DHCP (DHCPv6)                           | 233        |
| Система доменных имен (DNS)                                | 235        |
| Структура заголовка в пакете DNS                           | 235        |
| Простой DNS-запрос   | 237        |
| Типы запросов по протоколу DNS                             | 238        |
| Рекурсия в DNS   | 240        |
| Перенос DNS-зон  | 244        |
| Протокол передачи гипертекста (HTTP)                       | 247        |
| Просмотр веб-страниц с помощью протокола HTTP              | 247        |
| Публикация данных по протоколу HTTP                        | 250        |
| Простой протокол передачи электронной почты (SMTP)         | 252        |
| Отправка и получение электронной почты                     | 252        |
| Отслеживание сообщений электронной почты                   | 254        |
| Отправка вложений по протоколу SMTP                        | 262        |
| Заключительные соображения                                 | 266        |
| <b>Глава 10. Основные реальные сценарии</b>                | <b>267</b> |
| Отсутствие веб-содержимого                                 | 268        |
| Подключение к сети   | 269        |
| Анализ   | 269        |
| Усвоенные уроки  | 274        |
| Не реагирующая метеорологическая служба                    | 274        |
| Подключение к сети   | 275        |
| Анализ   | 276        |
| Усвоенные уроки  | 280        |
| Отсутствие доступа к Интернету                             | 281        |
| Трудности конфигурирования шлюза                           | 281        |
| Нежелательная переадресация                                | 284        |
| Проблемы с обратным потоком данных                         | 289        |

|  |            |
|--|------------|
| Испорченный принтер  | 292        |
| Подключение к сети   | 293        |
| Анализ   | 293        |
| Усвоенные уроки  | 296        |
| Отсутствие связи с филиалом  | 297        |
| Подключение к сети   | 298        |
| Анализ   | 298        |
| Усвоенные уроки  | 301        |
| Повреждение данных программы   | 302        |
| Подключение к сети   | 302        |
| Анализ   | 303        |
| Усвоенные уроки  | 306        |
| Заключительные соображения   | 307        |
| <b>Глава 11. Меры борьбы с медленной сетью</b>   | <b>309</b> |
| Функциональные средства устранения ошибок в протоколе TCP                                      | 310        |
| Повторная передача данных в протоколе TCP  | 310        |
| Дублирующие подтверждения и быстрые повторные передачи по протоколу TCP                        | 314        |
| Управление потоками данных в протоколе TCP   | 320        |
| Изменение размера окна приема  | 321        |
| Прекращение потока данных с помощью установки нулевого окна приема                             | 323        |
| Применение механизма скользящего окна на практике  | 324        |
| Выводы из анализа пакетов для исправления ошибок и управления потоками данных по протоколу TCP | 328        |
| Выявление источника большой сетевой задержки   | 329        |
| Обычный обмен данными  | 330        |
| Медленный обмен данными из-за сетевой задержки   | 330        |
| Медленный обмен данными из-за задержки на стороне клиента                                      | 332        |
| Медленный обмен данными из-за задержки на стороне сервера                                      | 333        |
| Порядок обнаружения задержек в сети  | 334        |
| Сравнение с исходными характеристиками сети  | 335        |
| Исходные характеристики сети для сайта   | 335        |
| Исходные характеристики сети для хоста   | 337        |
| Исходные характеристики сети для приложений  | 338        |
| Дополнительные рекомендации относительно исходных характеристик сети                           | 339        |
| Заключительные соображения   | 340        |
| <b>Глава 12. Анализ пакетов на безопасность</b>  | <b>341</b> |
| Обследование сети  | 342        |
| Сканирование пакетами SYN  | 343        |
| Получение отпечатка операционной системы   | 348        |

|   |            |
|---|------------|
| Манипулирование сетевым трафиком  | 353        |
| Заражение ARP-кеша  | 353        |
| Перехват сеансов связи  | 359        |
| Вредоносное программное обеспечение   | 363        |
| Операция “Аврора”   | 364        |
| Троянская программа удаленного доступа  | 372        |
| Набор эксплойтов и программы-вымогатели                                       | 381        |
| Заключительные соображения  | 389        |
| <b>Глава 13. Анализ пакетов в беспроводных сетях</b>                          | <b>391</b> |
| Физические особенности беспроводных сетей                                     | 392        |
| Анализ пакетов по отдельным каналам   | 392        |
| Перекрестные помехи в беспроводных сетях                                      | 393        |
| Обнаружение и анализ наложения сигналов                                       | 394        |
| Режимы работы адаптера беспроводной связи                                     | 395        |
| Анализ пакетов в беспроводной сети в системе Windows                          | 396        |
| Настройка устройства AirPcap  | 398        |
| Перехват сетевого трафика с помощью устройства AirPcap                        | 400        |
| Анализ пакетов в беспроводной сети в системе Linux                            | 401        |
| Структура пакета по стандарту 802.11  | 403        |
| Добавление столбцов, характерных для беспроводной сети, на панель Packet List | 405        |
| Специальные фильтры для беспроводных сетей                                    | 407        |
| Фильтрация сетевого трафика по конкретному идентификатору BSSID               | 407        |
| Фильтрация пакетов по конкретным типам  | 407        |
| Фильтрация пакетов по отдельным каналам                                       | 408        |
| Сохранение профиля беспроводной сети  | 409        |
| Безопасность в беспроводной сети  | 409        |
| Успешная аутентификация по алгоритму WEP                                      | 410        |
| Неудачная аутентификация по алгоритму WEP                                     | 412        |
| Удачная аутентификация по алгоритму WPA                                       | 413        |
| Неудачная аутентификация по алгоритму WPA                                     | 416        |
| Заключительные соображения  | 417        |
| <b>Приложение А. Дополнительная информация</b>                                | <b>419</b> |
| Инструментальные средства для анализа пакетов                                 | 419        |
| CloudShark  | 419        |
| WireEdit  | 420        |
| Cain & Abel   | 421        |
| Scapy   | 421        |
| TraceWrangler   | 421        |
| Tcpreplay   | 421        |
| NetworkMiner  | 422        |

|  |            |
|--|------------|
| CapTiffer  | 423        |
| ngrep  | 423        |
| libpcap  | 423        |
| Npcap  | 424        |
| hping  | 424        |
| Python   | 424        |
| <b>Ресурсы по анализу пакетов</b>                                | <b>425</b> |
| Начальная страница веб-сайта, посвященного Wireshark             | 425        |
| Онлайновые практические курсы по анализу пакетов                 | 425        |
| Углубленные курсы в институте SANS по обнаружению вторжений      | 425        |
| Блог Криса Сандерса  | 426        |
| Веб-сайт Бреда Дункана, посвященный анализу вредоносного трафика | 426        |
| Веб-сайт IANA  | 426        |
| Иллюстрированная серия по протоколам TCP/IP                      |            |
| Ричарда У. Стивенса  | 426        |
| Руководство по стеку протоколов TCP/IP                           | 427        |
| <b>Приложение Б. Интерпретация пакетов</b>                       | <b>429</b> |
| Представление пакетов  | 429        |
| Применение схем пакетов  | 432        |
| Интерпретация неизвестного пакета                                | 435        |
| Заключительные соображения                                       | 438        |
| <b>Предметный указатель</b>                                      | <b>439</b> |