

УДК 004.382
ББК 32.973.018
Ф79

Форшоу Дж.

Ф79 Атака сетей на уровне протоколов / пер. с англ. Д. А. Беликова. – М.: ДМК Пресс, 2022. – 340 с.: ил.

ISBN 978-5-97060-972-9

Это руководство фокусируется на анализе пользовательских протоколов для поиска уязвимостей в системе безопасности. В ходе чтения вы ознакомитесь с методами обучения перехвату сетевого трафика, выполнением анализа протоколов, обнаружением и эксплуатацией уязвимостей. Также в книге приводятся справочная информация о сетях и сетевой защите и практические примеры протоколов для анализа. Сетевая библиотека Canare Core, разработанная автором, поможет вам создать собственные инструменты для тестирования угроз.

Издание будет полезно тем, кто интересуется анализом и атаками сети на уровне протоколов. Хотите ли вы атаковать сеть, чтобы сообщить о возможных рисках поставщику приложения, или просто узнать, как ваше IoT-устройство обменивается данными, вы найдете здесь интересующие вас темы.

УДК 004.382
ББК 32.973.018

Title of English-language original: Attacking Network Protocols: A Hacker's Guide to Capture, Analysis, and Exploitation, ISBN 9781593277505, published by No Starch Press Inc. 245 8th Street, San Francisco, California United States 94103. The Russian-Language 1st edition Copyright © 2021 by ДМК Пресс Publishing under license by No Starch Press Inc. All rights reserved.

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

ISBN 978-1-59327-750-5 (англ.)
ISBN 978-5-97060-972-9 (рус.)

© James Forshaw, 2018
© Перевод, оформление,
издание, ДМК Пресс, 2022

СОДЕРЖАНИЕ

| | |
|---|----|
| От издательства | 11 |
| Об авторе | 12 |
| О рецензенте | 12 |
| Предисловие | 13 |
| Благодарности | 16 |
| Введение | 18 |
| Глава 1. Основы сетей | 23 |
| Сетевая архитектура и протоколы | 23 |
| Набор интернет-протоколов | 24 |
| Инкапсуляция данных | 27 |
| Заголовки, концевики и адреса..... | 27 |
| Передача данных | 28 |
| Сетевая маршрутизация..... | 29 |
| Моя модель для анализа сетевых протоколов..... | 31 |
| Заключительное слово | 33 |
| Глава 2. Перехват трафика | 34 |
| Пассивный перехват сетевого трафика | 34 |
| Краткое руководство по Wireshark..... | 35 |
| Альтернативные методы пассивного перехвата..... | 37 |
| Отслеживание системных вызовов..... | 37 |
| Утилита strace для Linux | 39 |

| | |
|---|----|
| Мониторинг сетевых подключений с помощью DTrace | 40 |
| Process Monitor в Windows | 41 |
| Преимущества и недостатки пассивного перехвата | 43 |
| Активный перехват сетевого трафика | 43 |
| Сетевые прокси..... | 44 |
| Прокси-сервер с переадресацией портов..... | 44 |
| Прокси-сервер SOCKS..... | 48 |
| Прокси-серверы HTTP | 53 |
| Перенаправление HTTP-прокси | 54 |
| Обратный прокси-сервер HTTP | 57 |
| Заключительное слово | 61 |

Глава 3. Структура сетевых протоколов

| | |
|--|----|
| Структура двоичных протоколов | 63 |
| Числовые данные..... | 63 |
| Логические значения..... | 66 |
| Битовые флаги..... | 66 |
| Двоичный порядок байтов..... | 67 |
| Текстовые и удобочитаемые данные | 68 |
| Данные переменной длины в двоичном формате | 72 |
| Даты и время | 75 |
| POSIX/Unix-время..... | 75 |
| Windows FILETIME | 76 |
| Шаблон TLV | 76 |
| Мультиплексирование и фрагментация..... | 77 |
| Информация о сетевом адресе | 78 |
| Структурированные двоичные форматы | 78 |
| Структуры текстового протокола | 80 |
| Числовые данные..... | 80 |
| Текстовые логические значения..... | 81 |
| Даты и время | 81 |
| Данные переменной длины | 82 |
| Структурированные текстовые форматы | 82 |
| Кодирование двоичных данных | 85 |
| Шестнадцатеричное кодирование | 86 |
| Base64 | 86 |
| Заключительное слово | 88 |

Глава 4. Расширенный перехват трафика приложений

| | |
|---|----|
| Перенаправление трафика..... | 89 |
| Использование traceroute..... | 90 |
| Таблицы маршрутизации | 91 |
| Настройка маршрутизатора | 92 |
| Активируем маршрутизацию в Windows..... | 93 |
| Активируем маршрутизацию в Unix-подобных системах | 93 |
| Преобразование сетевых адресов | 94 |
| Активируем SNAT | 94 |
| Настройка SNAT в Linux | 95 |

| | |
|--------------------------------------|-----|
| Активируем DNAT | 96 |
| Перенаправление трафика на шлюз..... | 98 |
| DHCP-спуфинг..... | 98 |
| ARP-спуфинг..... | 101 |
| Заключительное слово | 105 |

Глава 5. Анализ на практике

| | |
|--|-----|
| Приложение для генерирования трафика: SuperFunkyChat..... | 106 |
| Запуск сервера..... | 107 |
| Запуск клиентов..... | 107 |
| Обмен данными между клиентами..... | 108 |
| Экспресс-курс анализа с помощью Wireshark..... | 109 |
| Генерация сетевого трафика и перехват пакетов..... | 110 |
| Базовый анализ..... | 111 |
| Чтение содержимого TCP-сеанса..... | 112 |
| Определение структуры пакета с помощью шестнадцатеричного дампа..... | 113 |
| Просмотр отдельных пакетов..... | 114 |
| Определение структуры протокола | 115 |
| Проверим свои предположения..... | 117 |
| Анализ протокола с помощью Python | 118 |
| Разработка диссекторов Wireshark на Lua..... | 124 |
| Создание диссектора | 126 |
| Разбор при помощи Lua | 128 |
| Парсинг пакета сообщения | 128 |
| Использование прокси-сервера для активного анализа трафика | 131 |
| Настройка прокси-сервера..... | 132 |
| Анализ протокола с использованием прокси-сервера..... | 134 |
| Добавляем базовый парсинг протокола | 136 |
| Изменение поведения протокола..... | 137 |
| Заключительное слово | 139 |

Глава 6. Обратная разработка приложения.....

| | |
|--|-----|
| Компиляторы, интерпретаторы и ассемблеры | 141 |
| Интерпретируемые языки..... | 141 |
| Компилируемые языки | 142 |
| Статическая и динамическая компоновки | 142 |
| Архитектура x86 | 143 |
| Архитектура набора команд | 143 |
| Регистры ЦП..... | 145 |
| Порядок выполнения..... | 147 |
| Основы операционной системы..... | 148 |
| Форматы исполняемых файлов | 148 |
| Сегменты | 149 |
| Процессы и потоки..... | 150 |
| Сетевой интерфейс операционной системы | 150 |
| Двоичный интерфейс приложений..... | 153 |
| Статический обратный инжиниринг | 154 |
| Краткое руководство по использованию IDA Pro Free Edition..... | 155 |

| | |
|---|-----|
| Анализ переменных и аргументов стека | 158 |
| Определение ключевой функциональности | 159 |
| Динамический обратный инжиниринг | 164 |
| Установка точек останова | 165 |
| Отладчик Windows | 166 |
| Где установить точки останова? | 168 |
| Обратное проектирование управляемого кода | 168 |
| Приложения .NET | 168 |
| Использование ILSpy | 169 |
| Приложения Java | 172 |
| Работа с обфускацией | 174 |
| Ресурсы | 175 |
| Заключительное слово | 176 |

Глава 7. Безопасность сетевого протокола

| | |
|--|-----|
| Алгоритмы шифрования | 178 |
| Подстановочные шифры | 179 |
| XOR-шифрование | 180 |
| Генераторы случайных чисел | 181 |
| Симметричное шифрование | 182 |
| Блочные шифры | 182 |
| Режимы блочного шифрования | 185 |
| Дополнение (padding) | 188 |
| Атака padding oracle | 189 |
| Потоковые шифры | 192 |
| Асимметричное шифрование | 193 |
| Алгоритм RSA | 193 |
| RSA с дополнением | 195 |
| Протокол Диффи–Хеллмана | 196 |
| Алгоритмы подписи | 197 |
| Алгоритмы криптографического хеширования | 198 |
| Асимметричные алгоритмы подписи | 199 |
| Имитовставки (коды аутентификации сообщения) | 200 |
| Инфраструктура открытых ключей | 203 |
| Сертификаты X.509 | 203 |
| Проверка цепочки сертификатов | 205 |
| Пример использования: протокол защиты транспортного уровня | 206 |
| TLS-рукопожатие | 207 |
| Начальное согласование | 207 |
| Аутентификация конечной точки | 208 |
| Установка зашифрованного соединения | 210 |
| Соответствие требованиям безопасности | 211 |
| Заключительное слово | 212 |

Глава 8. Реализация сетевого протокола

| | |
|---|-----|
| Воспроизведение существующего перехваченного сетевого трафика | 214 |
| Перехват трафика с помощью Netcat | 215 |

| | |
|---|-----|
| Использование Python для повторной отправки перехваченного UDP-трафика..... | 217 |
| Изменяем назначение нашего прокси..... | 219 |
| Повторное использование существующего исполняемого кода..... | 224 |
| Повторное использование кода в приложениях .NET | 225 |
| Повторное использование кода в приложениях Java | 230 |
| Неуправляемые исполняемые файлы | 232 |
| Шифрование и работа с TLS..... | 236 |
| Изучение используемого шифрования | 237 |
| Расшифровка TLS-трафика | 238 |
| Заключительное слово | 243 |

Глава 9. Основные причины уязвимостей.....244

| | |
|--|-----|
| Классы уязвимостей | 245 |
| Удаленное выполнение кода..... | 245 |
| Отказ в обслуживании..... | 245 |
| Утечка информации..... | 246 |
| Обход аутентификации..... | 246 |
| Обход авторизации | 246 |
| Уязвимости пореждения памяти..... | 247 |
| Безопасные и небезопасные языки программирования с точки зрения доступа к памяти | 247 |
| Переполнение буфера..... | 248 |
| Индексирование буфера за пределами границ..... | 253 |
| Атака расширения данных | 255 |
| Сбой при динамическом выделении памяти | 255 |
| Учетные данные, используемые по умолчанию или вшитые в код | 256 |
| Перечисление пользователей..... | 257 |
| Неправильный доступ к ресурсам..... | 258 |
| Канонизация..... | 258 |
| Подробные сообщения об ошибках | 259 |
| Исчерпание памяти | 261 |
| Исчерпание хранилища..... | 262 |
| Исчерпание ресурсов ЦП..... | 263 |
| Алгоритмическая сложность | 263 |
| Конфигурируемая криптография | 265 |
| Уязвимости строки форматирования | 266 |
| Внедрение команд | 267 |
| Внедрение SQL-кода..... | 268 |
| Замена символов в текстовой кодировке..... | 269 |
| Заклучительное слово | 271 |

Глава 10. Поиск и эксплуатация уязвимостей.....272

| | |
|----------------------------|-----|
| Фаззинг | 273 |
| Простейший тест..... | 273 |
| Мутационный фаззер | 274 |
| Создание тест-кейсов | 275 |

| | |
|---|------------|
| Сортировка уязвимостей..... | 275 |
| Отладка приложений..... | 275 |
| Повышаем наши шансы найти первопричину сбоя..... | 282 |
| Эксплуатация распространенных уязвимостей..... | 285 |
| Эксплуатация уязвимостей пореждений памяти..... | 285 |
| Произвольная запись в память..... | 293 |
| Написание шелл-кода..... | 296 |
| Приступим..... | 296 |
| Простая техника отладки..... | 299 |
| Вызов системных вызовов..... | 300 |
| Выполнение других программ..... | 305 |
| Генерация шелл-кода с помощью Metasploit..... | 306 |
| Устранение уязвимостей повреждения памяти..... | 308 |
| Предотвращение выполнения данных..... | 309 |
| Использование метода возврата-ориентированного программирования..... | 310 |
| Рандомизация размещения адресного пространства..... | 312 |
| Обнаружение переполнения стека с помощью предохранителей..... | 316 |
| Заключительное слово..... | 319 |
| Набор инструментов для анализа сетевых протоколов..... | 320 |
| Предметный указатель..... | 335 |