

Анализ пакетов с помощью Wireshark Analyzer (продвинутый уровень) (АРАW)

ID FL-APAW Цена 119 000,- руб. Длительность 3 дня

Кому следует посетить

Сетевые администраторы, технический персонал, отвечающий за планирование, внедрение и разработку отказоустойчивых сетей передачи данных.

Предварительные требования

- Базовое понимание основ работы сетей передачи данных и стека TCP/IP
- Опыт работы с ПО Wireshark или
- Основы сетевых технологий и протоколов TCP/IP (NWF)
- [Анализ пакетов с помощью Wireshark Analyzer \(PAW\)](#)

Цели курса

По окончании обучения слушатели будут иметь возможность:

- Обнаруживать аномальное поведение сетевых протоколов
- Обнаруживать источники проблем: сеть, рабочие станции, серверы и приложения
- По возможности повышать сетевую производительность
- Исправлять некорректную сетевую конфигурацию

Содержание курса

Advanced Packet Analysis with Wireshark Analyzer (APAW) v1.3 – это курс компании Фаст Лейн, разработанный для расширения знаний по поиску и устранению неполадок в работе сетевых протоколов и обнаружению узких мест по производительности с использованием ПО Wireshark. Курс АРАW включает в себя теоретическую часть и практические занятия с детальным разбором сетевых проблем.

Программа курса

1. Введение

2. перехват данных в сети

- 2.1. Топологии: проводные и беспроводные
- 2.2. Полудуплекс/полный дуплекс
- 2.3. Hub, SPAN, RSPAN, TAP/Splitter
- 2.4. перехват данных в беспроводной среде

3. Ethernet

- 3.1. Стандарт Ethernet
- 3.2. Протокол Spanning Tree Protocol сравнение с версией RSTP)
- 3.3. VLAN
- 3.4. Лабораторная работа 1: Анализ протокола STP

4. Протокол Internet Protocol (IP)

- 4.1. Негарантированная доставка
- 4.2. Фрагментация
- 4.3. Основы маршрутизации

5. Протокол ICMP

- 5.1. ICMP коды и типы
- 5.2. Сообщения типа Echo Request/Echo Reply
- 5.3. Сообщение Destination Unreachable
- 5.4. TTL exceeded, Redirect
- 5.5. Лабораторная работа 3: Поиск и устранение неполадок в работе ICMP

6. Протокол ARP

- 6.1. Определение MAC адресов по IP
- 6.2. ARP в разных широковещательных доменах
- 6.3. Сообщение типа Gratuitous ARP
- 6.4. Поиск и устранение неполадок в работе протокола ARP
- 6.5. Технология Proxu ARP
- 6.6. Лабораторная работа 4: Работа с протоколом ARP

7. DHCP

Анализ пакетов с помощью Wireshark Analyzer (продвинутый уровень) (АРАW)

- 7.1. Функции DHCP
- 7.2. Опции DHCP
- 7.3. Статическое назначение адреса оконечному устройству, пулы адресов
- 7.4. Сообщение типа DHCP Inform
- 7.5. Технология DHCP Relay Agent (настройка IP Helper)
- 7.6. Лабораторная работа 5: Проблемы в работе протокола DHCP
- 11.4. Лабораторная работа 11: Анализ работы протокола HTTP

8. Протоколы TCP и UDP

- 8.1. Характеристики TCP (флаги, порты, сокет)
- 8.2. Процесс установления/закрытия TCP-соединения (включая Reset Packets и сброшенные сессии)
- 8.3. Разбор заголовков TCP-сегментов
- 8.4. TCP Keep Alive
- 8.5. Процесс повторной отправки пакетов при потерях
- 8.6. Обзор UDP
- 8.7. Лабораторная работа 6: Анализ установления TCP-соединения
- 8.8. Лабораторная работа 7: Плавающий размер окна в TCP
- 8.9. Лабораторная работа 8: Процесс повторной отправки пакетов в TCP
- 8.10. Лабораторная работа 9: Алгоритм Nagle

9. DNS

- 9.1. Алгоритмы DNS и WINS
- 9.2. Доменное дерево и корневые серверы
- 9.3. Основы работы протокола DNS
- 9.4. Тип запросов в DNS
- 9.5. События об ошибках в работе DNS
- 9.6. Фильтрация запросов DNS в Wireshark

10. FTP

- 10.1. Каналы управления и передачи в рамках работы протокола FTP
- 10.2. Активный и пассивный режим работы протокола FTP
- 10.3. Режимы команд и передачи
- 10.4. Аутентификация и коды ошибок
- 10.5. Потенциальные проблемы в работе протокола FTP
- 10.6. Лабораторная работа 10: Устранение неполадок в работе FTP

11. Протокол HTTP

- 11.1. Методы HTTP
- 11.2. Коды ответов HTTP
- 11.3. Параметры передачи: Query string, StdIO, Cookies