Анализ пакетов с помощью Wireshark Analyzer (PAW+APAW)

ID FL-PAPW **Цена** 170 000,– руб. **Длительность** 5 дней

Кому следует посетить

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

Предварительные требования

!Основы сетевых технологий и протоколов TCP/IP (NWF)

Цели курса

По окончании обучения слушатели будут иметь возможность:

- Работать с пользовательским интерфейсом и осуществлять настройку Wireshark
- Вбирать методы и средства измерений
- Собирать и анализировать сетевые статистики
- Идентифицировать возможные причины неполадок
- 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

Packet Analysis Power Workshop (PAPW) v1.2 это курс компании Фаст Лейн, который обеспечит слушателей базовыми навыками использования Wireshark Analyzer со всеми инструментами и функциями. Слушатели также получат навыки поиска и устранения неполадок в работе сетевых протоколов и обнаружения узких мест по производительности с использованием ПО Wireshark. Курс PAPW включает в себя теоретическую часть и практические занятия с детальным разбором сетевых проблем.

Программа курса

Характеристики, функции и базвые принципы работы Wireshark Analyzer

- Обзор и функционирование Wireshark
- Live Capture и настройки
- Опции отображения и базовые интерпретации
- Работа с фильтрами отображения и захвата
- File Input and Output

Расширенные функции Wireshark Analyzer

- Пользовательские профили
- Разрешение имен
- Восстановление пользовательских данных – сборка протоколов
- Покраска пакетов

Методология и принципы сетевого анализа

- Что такое анализ пакетов?
- Шаги и иетоды анализа трафика
- Анализ коммутируемых сетей Ethernet
- Перехват трафика беспроводных сетей
- Измерение сетевой задержки и времени отклика
- Измерение сетевой пропускной способности и накладных расходов

Статистика и контрольные измерения

- Контрольные измерения в сетях
- Статистика Wireshark

Анализ сетей и приложений

- Типовые сетевые пролемы
- Типы приложений и проблемы приложений
- "Это сеть или приложение?" – изоляция проблем
- Анализ и восстановление голосового трафика

Анализ коммутируемых сетей Ethernet

- Принципы работы и анализ Spanning Tree
- Анализ VLANs, VLAN-Tagging

Анализ стека TCP/IP, сетевой уровень

- IP адресация
- Типовые IP сценарии

- Опции IP
- ICMP, ARP и DHCP

Анализ стека TCP/IP, транспортный уровень

- Функции TCP
- Session Setup, Data Transfer и Session Teardown
- Размер окна TCP
- Опции TCP (SACK, Window Scaling) и таймеры TCP
- Функции UDP

Анализ TCP/IP с использованием Wireshark

- Настройки Wireshark для расширенного анализа стека TCP/IP
- Типовые проблемы стека TCP/IP
- Информационные сообщения Wireshark Expert и их значение

Прикладные протоколы стека TCP/IP

- HTTP
- FTP
- DNS
- SSL

Лабораторные работы

- Поиск в трейс-файлах
- Фильтры отображения
- Сборка пакетов TCP/IP
- Графики TCP
- Пропускная способность и накладные расходы
- Типовые проблемы
- Анализ Spanning Tree
- Поиск и устранение неполадок ICMP
- Работа ARP
- Проблемы DHCP
- TCP Handshake & Options
- Скользящий размер окнаTCP
- Переотправка пакетов
- Алгоритм Nagle
- Поиск и устранение неполадок
- FTP
- HTTP