Advanced Packet Analysis with Wireshark Analyzer (APAW)

Duration: 24 Hours (3 Days)

Overview

The Advanced Packet analysis with Wireshark Analyzer (APAW) course is an intensive training program designed to equip learners with expert-level skills in Packet analysis using the Wireshark network protocol analyzer. This course delves deep into the complexities of Network troubleshooting, Security analysis, and Optimization of network traffic.By participating in Wireshark Packet analysis training, students will gain a comprehensive understanding of the intricacies of Network protocols and how they operate within a Switched Ethernet environment in Module 1. The course then progresses to Module 2, where learners will dissect the Network layer of TCP/IP, covering IP addressing, Typical IP scenarios, and essential Protocols like ICMP, ARP, and DHCP.In Module 3, the focus shifts to Packet analysis with Wireshark at the transport layer, explaining TCP functions, Session management, and optimization techniques. Module 4 enhances the learner's ability to use Wireshark for advanced TCP/IP analysis, including troubleshooting and interpreting Expert Info messages. Finally, Module 5 covers TCP/IP applications such as HTTP, FTP, DNS, and SSL.Overall, the APAW course is beneficial for network professionals looking to hone their Packet analysis skills and improve network performance and security.

Audience Profile

The Advanced Packet Analysis with Wireshark Analyzer course equips professionals with in-depth network troubleshooting skills using Wireshark.

- Target audience for the APAW course includes:
- Network Administrators
- Network Analysts
- Security Engineers
- IT Professionals involved in network maintenance and management
- System Administrators
- Network Architects
- Cybersecurity Analysts
- Incident Response / Forensics Analysts
- Infrastructure Engineers
- Technical Support Staff
- Network Consultants
- Data Center Engineers
- Students studying network engineering or cybersecurity

Course Syllabus

Switched Ethernet analysis

- Spanning Tree operation and Spanning Tree analysis
- Analyzing VLANs, VLAN-Tagging

TCP/IP analysis of the network layer

- IP addressing
- Typical IP scenarios
- IP options
- ICMP, ARP and DHCP

TCP/IP analysis of the transport layer

- TCP functions
- Session Setup, Data Transfer and Session Teardown
- Window Mechanism and Window optimization
- TCP options (SACK, Window Scaling) and TCP timers
- UDP functions

Analyzing TCP/IP with Wireshark

- Wireshark preferences for advanced TCP/IP analysis
- Typical TCP/IP related problems
- Wireshark Expert Info messages and their meanings

TCP/IP applications

- HTTP
- FTP
- DNS
- SSL