NETWORK PACKET ANALYSIS PROGRAM

Duration: 3 days (21 hours)
Mode:

1. Instructor Led Class room Training and Labs
2. Online

In this hands-on course, you will receive in-depth training on Protocol analysis using Wireshark. You will learn to identify the most common causes of performance problems in TCP/IP communications.

What will you Learn?

What will you learn?

- Place the analyzer properly for traffic capture on a variety of network types
- Capture packets on wired and wireless networks
- Navigate through, split, and work with large traffic files
- Use time values to identify network performance problems
- Filter out traffic for more efficient troubleshooting and analysis
- Customize Wireshark coloring to focus on network problems faster
- Analyze normal/abnormal Domain Name System (DNS) traffic
- Analyze normal/abnormal Address Resolution Protocol (ARP) traffic
- Analyze normal/abnormal Internet Protocol v4 (IPv4) traffic
- Analyze normal/abnormal Internet Control Messaging Protocol (ICMP) traffic
- Analyze normal/abnormal User Datagram Protocol (UDP) traffic
- Analyze normal/abnormal Transmission Control Protocol (TCP) traffic
- Analyze normal/abnormal Hypertext Transport Protocol (HTTP/HTTPS) traffic

Who Needs to Attend?

- Anyone interested in learning to troubleshoot and optimize TCP/IP networks and analyze network traffic with Wireshark, especially network engineers, information technology specialists, security analysts.

Prerequisites

- Hands on Knowledge in Computer Networks.

Course Content

- Installing Wireshark Protocol Analyser
- What are dissectors
- Resolution Process – Dissectors
- Understanding Dissectors
- Dissector Tables, Use of Dissectors

- List of Dissectors
- The Core engine of the Analyser
- Protocol identifying parameters & Protocol Structure

Traffic Capturing methods

- Capture to Ring Buffer
- Capture Filters
- Display Filters
- Capture formats & conversions
- Time Display Formats

Analyse ARP Traffic

- Analysing ARP Traffic
- ARP Overview
- ARP Packet Structure
- Filter on ARP Traffic

Analyse ICMP traffic

- Analysing ICMP Traffic
- ICMP Overview
- ICMP Packet Structure
- Filter on ICMP Traffic
- ICMP Type numbers, Code numbers
- TTL Value, TTL Expired in Transit.

Saving / Retrieving Traces

- Capturing Traffic on the cabling system
- Opening Trace Files
- Processing Packets based on powerful filtering system
- The Changing Status Bar

Coloring Techniques

- Coloring Techniques
- The Navigation Techniques
- Tracing packets based on various Characteristics
- Build Permanent Coloring Rules
- Identify a Coloring Source
- Mark Packets of Interest

Filtering traffic using Display Filters

- How to configure Display Filters
- Filtering traffic using Display Filters
- Build Filters Based on Packets
- Display Filter Syntax

Analysing DHCP Traffic

- Analysing DHCP Traffic
- DHCP packet structure
- Discover, Offer, Request and Acknowledgement packets
- Flooded Broadcast packet identification
- DHCP packet analysis
- The significance of bootp packet

Analyse DNS Traffic

- Analysing DNS Traffic
- DNS Overview
- DNS Packet Structure
- DNS Queries
- Filter on DNS Traffic
- The Opcode values and its meaning
- Analyze Normal/Problem DNS Traffic
- UDP 53 and TCP 53 packet parameter analysis

Analysing IPV4 Traffic

- Analysing IPv4 Traffic
- IPv4 Overview
- IPv4 Packet Structure
- Analyze Broadcast/Multicast Traffic
- Filter on IPv4 Traffic
- IP Protocol Preferences

Analysing UDP Traffic

- Analysing UDP Traffic
- UDP Overview
- Watch for Service Refusals
- UDP Packet Structurev
- Filter on UDP Traffic

- Follow UDP Streams to Reassemble Data

Analysing TCP Protocol

- TCP Overview
- The TCP Connection Process
- TCP Handshake Problem
- TCP Packet Structure
- Analysis of TCP Flags
- The TCP Sequencing/Acknowledgment Process
- Packet Loss Detection
- Retransmission Detection
- Out-of-Order Segment Detection
- Filter on TCP Traffic and TCP Problems
- Follow TCP Streams to Reassemble Data
- Determining the Next Sequence Numbers
- Understanding Packet size

Analysing HTTP

- Analysing HTTP Traffic
- HTTP Overview
- HTTP Packet Structure
- Filter on HTTP Traffic
- HTTP Statistics

Analysing SSL Encrypted Traffic

- Analysing SSL-Encrypted Traffic (HTTPS)
- Examining SSL/HTTPS Traffic
- Filter on SSL

Analysing File Transfer Protocol (FTP)

- FTP Overview
- FTP Packet Structure
- Analyze FTP Control Connections
- Analyze FTP Data Connections
- Filter on FTP Traffic

Hands on Labs

1. Installation of Wireshark Protocol Analyser and setting it up with NIC for capture.
2. Generating ICMP error messages and TCP reset packets for analysis
3. Find the various parameters of Protocols/Applications on a Network, RFC
4. Capture Traffic to/from the Hardware Address using the Ring Buffer method and Capture filter method.
5. Set Time Display format and trace delays in the packet transfer process.
6. Capture and Analysis of ARP packets,
7. ARP Padding, Layer 2 Broadcast identification, Need for L2 broadcasting, Encapsulation process, Analysing ARP Payload
8. Capture ICMP traffic and analyse the packets for Type number and Code number of the ICMP packet captured.
9. Capture traffic on Cabling system and save it to the Disk.
10. Open Existing Capture files into Packet Analyser
11. Filter the traffic with specific Parameters.
12. Understand the Status bar while capturing the packets.
13. Capture / Open Trace files and Find, Mark, Save, and Colorize Packets
14. Capture live packets. Filter the traffic using display filters. Use various display filter parameters and analyse.
15. Capture and analyse DHCP DORA process packets, Analyse the DHCP Error Message packet, Leasing Parameters.
16. Installation of DNS Server, Creating zone and resource records, Capturing the DNS Traffic, Analyse DNS Query & Response, Unusual DNS packets Secondary DNS and Zone Transfer packet analysis.
17. Capture and Analyse the Network Layer Header, Source IP, Destination IP, Time difference between the request and response, IPV4 parameters.
18. Capture UDP Traffic. Analyse source port and destination port.
19. Capture the packets of TCP 3 way handshake and analyse the Sequence numbers, Port numbers and Acknowledgement numbers
20. Explain each parameter in the TCP Flags.
21. Capture and Analyse HTTP packets, the Source IP, Destination IP, Source and Destination Port numbers, packet fragmentation details, size of the fragment.