Network Troubleshooting Using Wireshark - the Complete Course

Hands-on 40 hours training

Description

The purpose of the course is to provide the participant with practical knowledge of Wireshark protocol analyser and how to use it for network analysis. The course provides understanding of the software and how to use it for in TCP/IP based networks. The course starts with in-depth review of the software, including filters, statistical tools and the expert system, continue with the TCP/IP protocol stack analysis and then goes through application protocol analysis including HTTP/HTTPs, FTP and Mail protocols, DNS, database applications, MS-TS, Voice and Video over IP and network forensics. All topics covered in the course include theory, real-world case studies and hand-on exercises, and is based on the new Wireshark version 3.

Objectives

By the end of the course, the participant will be able to:

- Run Wireshark and perform efficient data capture
- Set up various display and capture filters
- Use statistical tools to detect network failures
- Use I/O graphs and stream graphs
- Use the Expert system
- Analyse TCP/IP traffic and locate connectivity and performance problems
- Identify and locate faults in common Internet-based applications – HTTP/FTP/Mail and DNS, database and various enterprise applications
- Identify and locate faults in various Voice/Video over IP and streaming applications, including SIP and RTP/RTCP
- Identify security risks and isolate problems that can cause network down-time and performance degradation

Target Audience

R&D, engineering and technical Support, IT and communications managers

Prerequisites

Basic knowledge in networking and the TCP/IP protocol stack. The participants should come with Laptops with Wireshark software (free download from the site - www.wireshark.org)

Duration

5 Days

Outline

1. **Introduction to Wireshark**
   - How Wireshark Works
   - Capturing Packets
   - Wireshark toolbars and menus
   - Navigation and colorization techniques
   - Using Time Values and Summaries
   - Examining Basic Trace File Statistics
   - Save, Export and Print
   - Lab exercises and case studies
2. **Where to locate Wireshark**
   - How to decide where to capture data from
   - Taps and port-mirror
   - Local and remote monitoring
   - Capture data from multiple interfaces
   - Capture data on virtual machines
   - Capture data to single and multiple files
   - Capture data from local and remote interfaces

- Wireshark folders, configuration files and plugins
- Configure user interface, global and protocols preferences
- MAC/IP/TCP-UDP protocol resolution
- Import and export files
- Working with profiles
- Lab exercises and case studies

3. **Capture filters**
   - Capture filters syntax and Tcpdump
   - Compound capture filters
   - Offset filters
   - The cfilters file
   - Lab exercises and case studies
4. **Display filters**
   - Ways to configure display filters
   - Simple and structured filters
   - Focusing on protocol and text strings
   - The dfilters file
   - Lab exercises and case studies
5. **Using basic statistics tools**
   - Capture file properties
   - Resolved addresses properties
   - Protocol hierarchies
   - Endpoint and conversation statistics
   - Protocols statistics
   - Lab exercises and case studies
6. **Using smart statistics tools**
   - Create basic and advanced I/O graphs
   - Create TCP Time-Sequence graphs
   - Analyze flow graphs
   - Evaluate service response times

- Create Round-Trip-Time graphs
- Analyze TCP/IP flows
- Analyse applications flows
- Lab exercises and case studies

7. The Expert System Basics

- The Expert-Infos window and how to use it for network troubleshooting
- Error events and understanding them
- Warnings events and understanding them
- Notes events and understanding them
- Lab exercises and case studies

8. Ethernet and LAN switching analysis

- The Ethernet protocols
- What to look for
- Basic Ethernet issues

9. ARP and IPv4 analysis

- IPv4 principles of operation and packet structure: duplicate addresses, routing issues, fragmentation
- ICMPv4 - protocol operation, analysis and troubleshooting
- IPv4 ARP - operation and troubleshooting
- Lab exercises and case studies

10. TCP/UDP analysis

- Principles of operation (brief)
    - L4 operation
    - UDP principles and packet structure
- TCP principles and packet structure
    - TCP principles and packet structure
    - The Sliding-window mechanism and window size changes
    - Ack frequency, delayed Ack and the Nagel algorithm
    - Slow start, flow and congestion control

- TCP enhancements: Selective Ack, Time stamps, scale factor and more
- The TCP chimney offload mechanism
- Bandwidth/throughput and delay issues

- Lab exercises and case studies (TCP flow understanding)

11. Packet Loss, Delay, Jitter and Retransmissions

- Packet loss and recovery - UDP and TCP
- Previous segment lost and Out-of-Order Segments events
- Duplicate ACKs and Fast Retransmissions
- TCP Retransmissions and their impact on network performance
- Delay/jitter influence on TCP behaviour
- Zero window, Window changes and other window problems
- TCP Resets and their causes
- Lab exercises and case studies

12. Internet Applications Analysis and Troubleshooting

- Application behaviour and requirements
- TRANSUM and applications response times
- Lab exercises and case studies

13. HTTP/HTTPs analysis and troubleshooting

- HTTP/HTTPs network behaviour, methods and response codes
- HTTP troubleshooting
- HTTPs troubleshooting
- Lab exercises and case studies

14. FTP analysis and troubleshooting

- FTP behaviour, active and passive FTP
- FTP protocols analysis
- Lab exercises and case studies

15. Mail protocols - SMTP, POP and Web-based protocols

- Mail protocols brief
- Performance issues

- Events and error messages
- Lab exercises and case studies

16. **DNS operation and troubleshooting**
    - DNS brief - modes of operation, protocol types and message structure
    - DNS performance issues
    - DNS error messages and their causes
    - Lab exercises and case studies

17. **Enterprise applications analysis**
    - MS-Terminal and Citrix operation and troubleshooting
    - SMB/CIFS operation and analysis
    - DCS/RPC operation and analysis
    - Database applications, network behaviour and analysis
    - Lab exercises and case studies

18. **SIP/RTP and video applications**
    - SIP protocol basics
    - RTP protocol basics and Wireshark analysis tools
    - SIP/RTP troubleshooting
    - Video surveillance troubleshooting
    - Lab exercises and case studies

19. **Network Security and Forensics**
    - Gather information – what to look for
    - Unusual traffic patterns
    - Complementary tools
    - MAC and IP address spoofing
    - Attacks signatures and signature locations
    - ARP poisoning
    - Header and sequencing signatures
    - Attacks and exploits
    - TCP splicing and unusual traffic
    - DoS and DDoS Attacks
    - Protocol scans

- DNS-based attacks
- Find maliciously malformed packets
- Lab exercises and case studies

Labs

- LAB 1: Configuring packet capture on single and multiple interfaces
- LAB 2: Using navigation and colouring techniques
- LAB 3: Using time values
- LAB 4: Configuring L2/L3/L4 name resolution
- LAB 5: Saving, importing and exporting files
- LAB 6: Configuring user interface and global preferences
- LAB 7: Configuring basic capture filters and the cfilters file
- LAB 8: Configuring structured and offset capture filters
- LAB 9: Configuring basic L2/3/4 display filters and the dfilters file
- LAB 10: Locate text-strings in a capture file
- LAB 11: Using basic statistics tools for IP and UDP/TCP traffic analysis
- LAB 12: Find the top talkers and protocols on a Network
- LAB 13: Working with IO graphs for traffic analysis
- LAB 14: Using IO graphs for bandwidth and throughput analysis
- LAB 15: Using IO graphs with display filters
- LAB 16: Using the Expert Infos to find network issue
- LAB 17: discovering broadcast storms and broadcast loads
- LAB 18: Analysing TCP streams
- LAB 19: Analysing ARP traffic and ARP problems
- LAB 20: Understanding normal UDP and TCP behaviour
- LAB 21: Resolving TCP retransmission problems
- LAB 22: TCP Duplicate ACKs and Fast retransmissions problems
- LAB 23: TCP resets and why they happen
- LAB 24: TCP zero-window and window changes and why they happen
- LAB 25: Determine the cause for slow applications
- LAB 26: Delays and how they influence applications

- LAB 27: Use TCP stream graphs to analyse TCP behaviour
- LAB 28: Analysing packet losses, where they come from and why
- LAB 29: Using the Expert Infos to find application events
- LAB 30: TCP performance issues
- LAB 31: TCP delay/jitter calculations
- LAB 32: TCP timestamps, scale factor and selective ACKs
- LAB 33: Analysing SIP connectivity problems
- LAB 34: Analyse SSL/TLS connectivity
- LAB 35: Analysing DNS problems
- LAB 36: SIP connectivity problems
- LAB 37: Degradation in voice quality
- LAB 38: Video freezes analysis
- LAB 39: Unusual traffic patterns
- LAB 40: DDoS attack patterns
- LAB 41: DNS Attacks
- LAB 42: Case studies and challenges

Thank You!