Network Troubleshooting Using Wireshark

Hands-on

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 network analysis of TCP/IP based networks, with emphasis on TCP connectivity and performance issues. In the course we learn how to analyse DNS, HTTP and HTTPs protocols, along with enterprise protocols like Database applications, with special attention provided to VoIP and streaming protocols. All topics covered in the course include theory, 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:

- Understand Wireshark and use it for network analysis
- Understand the TCP/IP protocol suite and its behaviour over the network
- Understand common applications behaviour over the network
- Locate abnormal behaviour of network protocols and applications
- Troubleshoot network problems in small to mid-range enterprise networks
- Analyse performance degradation issues and locate their causes
- Locate the root cause for most common network problems

Target Audience

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

Prerequisites

Basic knowledge in networking and the TCP/IP protocol stack (Introduction to Networking course level).

Duration

3 Days

Outline

1. Introduction to network troubleshooting
   - Troubleshooting methodology
   - Troubleshooting tools
2. 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
3. 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
4. Capture filters
   - Capture filters syntax
   - Tshark and Tcpdump (brief)
   - Compound capture filters
   - Offset filters

- The cfilters file
- Lab exercises and case studies

5. 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
6. Using basic statistics tools
    - Capture file properties
    - Resolved addresses properties
    - Protocol hierarchies
    - Endpoint and conversation statistics
    - Protocols statistics
    - Lab exercises and case studies
7. 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 (Transum)
    - Lab exercises and case studies
8. 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
9. Ethernet and LAN switching analysis
    - The Ethernet protocols

- What to look for
- Basic Ethernet issues

10. 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
11. 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)
12. 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
13. Internet Applications Analysis and Troubleshooting
    - SSL/TLS analysis and troubleshooting
    - HTTP1/2 and HTTPs analysis and troubleshooting

- FTP analysis and troubleshooting
- Mail protocols – SMTP, POP and IMAP analysis
- DNS operation and troubleshooting
- SIP/RTP and video applications
- Lab exercises and case studies

14. Enterprise applications analysis
    - MS-Terminal and Citrix operation and troubleshooting
    - SMB/CIFS operation and analysis
    - DCS/RPC operation and analysis
    - Database applications analysis (from the network point of view)
    - Lab exercises and case studies

Labs:

1. Configuring packet capture on single and multiple interfaces
2. Using navigation and colouring techniques
3. Using time values
4. Configuring L2/L3/L4 name resolution
5. Saving, importing and exporting files
6. Configuring user interface and global preferences
7. Configuring basic capture filters and the cfilters file
8. Configuring structured and offset capture filters
9. Configuring basic L2/3/4 display filters and the dfilters file
10. Locate text-strings in a capture file
11. Using basic statistics tools for IP and UDP/TCP traffic analysis
12. Find the top talkers and protocols on a Network
13. Working with IO graphs for traffic analysis
14. Using IO graphs with display filters
15. Using IO graphs non-traffic related Y-Axis measures
16. Using TCP stream graphs
17. Using the Expert Infos to find network issue
18. Discovering broadcast storms and broadcast loads

19. Analysing ARP traffic and ARP problems
20. Understanding normal UDP and TCP behaviour
21. Resolving TCP retransmission problems
22. TCP Duplicate ACKs and Fast retransmissions problems
23. TCP resets and why they happen
24. TCP zero-window and window changes and why they happen
25. Determine the cause for slow applications
26. Delays and how they influence applications
27. Analysing packet losses, where they come from and why
28. Analysing TCP performance issues
29. Analysing databases problems
30. Analysing NetBIOS/SMB problems
31. Analysing HTTP and DNS slowness
32. Analysing SIP connectivity problems
33. Analysing Degradation in voice quality
34. Resolve Video freezes analysis

Thank You!