Wireshark Assisted Troubleshooting for Windows Servers Administrators

- 3 Days
- Lecture and Hands-on Labs

Course Overview

Learn to use Wireshark to identify and fix your TCP/IP network performance problems. Optimize TCP/IP networks with Wireshark®. This hands-on, in-depth course provides the skills to isolate and fix network performance issues. Learn how Wireshark can solve your TCP/IP network problems by improving your ability to analyze network traffic.

Who Should 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, and those preparing for the Wireshark Certified Network Analyst exam.

What You'll Learn

- Top 10 reasons for network performance complaints
- Place the analyzer properly for traffic capture on a variety of network types
- Capture packets on wired and wireless networks
- Configure Wireshark for best performance and non-intrusive analysis
- Navigate through, split, and work with large traffic files
- Use time values to identify network performance problems
- Create statistical charts and graphs to pinpoint performance issues
- Filter out traffic for more efficient troubleshooting and analysis
- Customize Wireshark coloring to focus on network problems faster
- Use Wireshark's Expert System to understand various traffic problems
- Use the TCP/IP Resolution Flowchart to identify possible communication faults
- 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
-

Outline

Day 1 - Capture Cleanly

- 💻 Lecture + Lab: Installing Wireshark
- 💬 Lecture: Overview of Network Analysis
- 💬 Lecture: Introduction to TCP IP Terms
- 💻 Lecture + Lab: Introduction to Using Wireshark

Capturing Packets

- 💬 Lecture: Starting and Stopping Captures with Wireshark
- 💻 Lecture + Lab: Capture Filters
- 💻 Lecture + Lab: Using TCPdump to make pcap Files for Wireshark
- 💻 Lecture + Lab: Introduction to Termshark
- 💻 Lecture + Lab: Ring Buffer and Zero Downtime Capturing
- 💬 Lecture: SPAN Mirror Port vs TAPs
- 💬 Lecture: Display Filters in Wireshark
- 💻 Lecture + Lab: Working with Display Filters
- 💬 Lecture: Wireshark Colorization Rules
- 💻 Lecture + Lab: Find packet
- 💻 Lecture + Lab: Flow and IO Graphs
- 💻 Lecture + Lab: Is It Even the Network - PowerShell Checklist
- 💻 Lecture + Lab: Windows NIC Offloads

Day 2 - Find the Real Culprit

- 💻 Lecture + Lab: Nmap Fundamentals
- 💻 Lecture + Lab: TCP Zero-Window, Socket Buffer Exhaustion, Port Exhaustion
- 💻 Lecture + Lab: MTU & PMTUD Black-Hole Detection
- 💬 Lecture: Decoding SSL Traffic with Wireshark
- 💻 Lecture + Lab: Service Response Time Statistics
- 💻 Lecture + Lab: Filter on Text Strings
- 💻 Lecture + Lab: Find packet
- 💻 Lecture + Lab: PCAPs to Text, CSV, JSON, XML, and PDF
- 💻 Lecture + Lab: Resolve Network Addresses with Wireshark
- 💻 Lecture + Lab: Display Macros
- 💻 Lecture + Lab: TShark on Windows for Evidence Based Workflows
- 💻 Lecture + Lab: Wireshark Profile for Windows Network Administrators
- 💻 Lecture + Lab: Capstone

Appendix

- 💬 Lecture: Wireshark Cheatsheet