Wireshark Network Analysis

Duration: 5 Days

Prerequisites:

To ensure that you can fully benefit from the Wireshark Network Analysis course, the following prerequisites are recommended:

- Basic understanding of networking concepts, including the OSI model, IP addressing, and common networking protocols (TCP/IP, DNS, HTTP, etc.).
- Familiarity with network infrastructure components such as switches, routers, and firewalls.
- Experience with operating systems, primarily Windows or Linux, as Wireshark can be used on various platforms.
- Ability to operate a PC or laptop, including installing and running software applications.
- Some previous experience in network administration or IT support can be helpful but is not mandatory.
- Eagerness to learn and a problem-solving mindset.
- No prior experience with Wireshark is required, as this course is designed to introduce you to the tool and guide you through its various features and applications.

Course Description:

The Wireshark Network Analysis course is a comprehensive program designed to educate learners on the powerful features of Wireshark, the world's foremost network protocol analyzer. Through the course, participants will gain a deep understanding of network analysis and how to use Wireshark effectively to monitor network traffic, troubleshoot network problems, and improve network security. Starting with an introduction to network analysis in Chapter 1, the course progresses through a series of detailed lessons, each focusing on key aspects of Wireshark and network traffic analysis. From capturing and filtering traffic in Chapters 3 and 4, to advanced topics such as analyzing specific protocols and network forensics covered from Chapters 14 to 32, learners build a strong foundation in network diagnostics. By the end of the course, participants will be well-prepared to pursue the WCNA certification, validating their expertise in Wireshark and network analysis. This credential is highly regarded in the field of network administration and security, making it a valuable asset for professionals looking to enhance their skill set and career opportunities.

Target Audience:

The Wireshark Network Analysis course equips participants with skills to monitor and troubleshoot network traffic for enhanced security and performance.

- Network Administrators
- Security Analysts
- Systems Engineers
- Network Engineers
- IT Professionals involved in network maintenance and management
- Cybersecurity Students
- Incident Response and Forensic Analysts
- Security Operations Center (SOC) Staff
- Performance Analysts
- Network Architects
- Technical Support Personnel
- IT Managers overseeing network operations
- Ethical Hackers and Penetration Testers looking to understand network traffic patterns
- Compliance Officers auditing network traffic logs
- Researchers and Educators in Networking and Cybersecurity disciplines

Course Outlines:

- Chapter 1: The World of Network Analysis
- Chapter 2: Introduction to Wireshark
- Chapter 3: Capture Traffic
- Chapter 4: Create and Apply Capture Filters
- Chapter 5: Define Global and Personal Preferences
- Chapter 6: Colorize Traffic
- Chapter 7: Define Time Values and Interpret Summaries
- Chapter 8: Interpret Basic Trace File Statistics
- Chapter 9: Create and Apply Display Filters
- Chapter 10: Follow Streams and Reassemble Data
- Chapter 11: Customize Wireshark Profiles
- Chapter 12: Annotate, Save, Export and Print Packets
- Chapter 13: Use Wireshark's Expert System
- Chapter 14: TCP/IP Analysis Overview
- Chapter 15: Analyze Domain Name System (DNS) Traffic
- Chapter 16: Analyze Address Resolution Protocol (ARP) Traffic
- Chapter 17: Analyze Internet Protocol (IPv4/IPv6) Traffic
- Chapter 18: Analyze Internet Control Message Protocol (ICMPv4/ICMPV6) Traffic
- Chapter 19: Analyze User Datagram Protocol (UDP) Traffic
- Chapter 20: Analyze Transmission Control Protocol (TCP) Traffic
- Chapter 21: Graph IO Rates and TCP Trends
- Chapter 22: Analyze Dynamic Host Configuration Protocol (DHCPv4/DHCPv6)
- Traffic
- Chapter 23: Analyze Hypertext Transfer Protocol (HTTP) Traffic
- Chapter 24: Analyze File Transfer Protocol (FTP) Traffic
- Chapter 25: Analyze Email Traffic
- Chapter 26: Introduction to 802.11 (WLAN) Analysis
- Chapter 27: Introduction to Voice over IP (VoIP) Analysis
- Chapter 28: Baseline "Normal" Traffic Patterns
- Chapter 29: Find the Top Causes of Performance Problems
- Chapter 30: Network Forensics Overview
- Chapter 31: Detect Scanning and Discovery Processes
- Chapter 32: Analyze Suspect Traffic
- Chapter 33: Effective Use of Command-Line Tools