Using Wireshark to Analyze and Troubleshoot TCP/IP Networks

Duration: 5 Days **Course Code: GK840150** **Version: 1.0**

Overview:

Master the art of packet analysis and network troubleshooting with Wireshark in this immersive, hands-on course built for real-world challenges.
Using Wireshark to Analyze and Troubleshoot TCP/IP Networks is a hands-on course designed for IT professionals who want to sharpen their skills in network traffic analysis. The course blends theory with practical labs, guiding learners through capturing, filtering, and interpreting network packets using Wireshark. Participants will explore real-world scenarios involving performance bottlenecks, security threats, and protocol-specific behaviors, gaining the confidence to troubleshoot complex network issues.
Throughout the course, learners will build custom Wireshark profiles, apply advanced filtering techniques, and analyze traffic across wired and wireless networks. From identifying scanning activity and suspicious payloads to visualizing TCP trends and using command-line tools, the curriculum is structured to provide both foundational knowledge and advanced troubleshooting strategies. While not marketed as official certification prep, the course aligns well with the Wireshark Certified Analyst (WCA) exam objectives, making it a valuable resource for those pursuing certification or simply looking to deepen their expertise.

Target Audience:

- Network engineers, IT professionals, and cybersecurity practitioners aiming to learn network analysis and troubleshooting using Wireshark.
- Developers and administrators responsible for monitoring and managing network infrastructure effectively.
- Professionals seeking to implement best practices in network security and performance analysis with Wireshark

Objectives:

- Explain the purpose of network analysis and the role of Wireshark in troubleshooting, optimization, and security.
- Describe Wireshark's functionality, including installation, configuration, and navigation.
- Capture network traffic on wired and wireless networks, and apply capture filters to isolate specific traffic.
- Analyze TCP/IP communications, including DNS, ARP, IPv4/IPv6, ICMP, UDP, and TCP traffic.
- Create and apply display filters to focus on specific packets and interpret trace file statistics.
- Follow streams and reassemble data for deeper analysis of conversations.
- Customize Wireshark profiles for different analysis scenarios.
- Annotate, save, export, and print packets for documentation and further analysis.
- Use Wireshark’s expert system to identify and troubleshoot network issues.
- Graph IO rates and TCP trends to visualize network performance.
- Detect scanning and discovery processes, and analyze suspect traffic for security purposes.
- Effectively use command-line tools for advanced network analysis.

Prerequisites:

- Basic understanding of networking concepts and TCP/IP protocols.
- Familiarity with network analysis tools and techniques.
- Knowledge of foundational network security principles and practices.
- Experience with packet analysis and troubleshooting (recommended).
- GK3150 - Understanding Networking Fundamentals (Network+)
- GK9025 - TCP/IP Networking

Content:

Introduction to Network Analysis and Wireshark

- Overview of TCP/IP Analysis
- Identifying Common Performance Issues
- Installing and Updating Wireshark
- Capturing Network Traffic
- Network Forensics Overview
- Network Forensics Techniques

Capture Methods and Filters

- Analyzing Switched Networks
- Using Network TAPs for Full-Duplex Links
- Wireless Network Analysis
- Configuring Capture Filters
- Detect Scanning and Discovery Processes
- Detecting Scanning and Discovery Processes

Customization and Advanced Navigation

- Creating a Troubleshooting Profile
- Setting Up a Custom Troubleshooting Profile
- Customizing the User Interface
- Adding Custom Columns and Configuring Preferences
- Advanced Navigation Techniques
- Building Permanent Coloring Rules
- Creating and Applying Coloring Rules
- Analyze Suspect Traffic
- Analyzing Suspect Traffic

Time Values, Summaries, and Basic Statistics

- Examining Delta Time
- Setting Time References
- Comparing Timestamp Values
- Using TCP Conversation Timestamps
- Enabling and Analyzing TCP Conversation Timestamps
- Effective Use of Command-Line Tools
- Using Command-Line Tools for Network Analysis

Protocol-Specific Traffic Analysis and Troubleshooting

- Using Display Filters
- Filtering Conversations and Endpoints
- Building Filters Based on Packets
- Building and Applying Packet-Based Filters
- TCP/IP Communications and Resolutions

Further Information:

For More information, or to book your course, please call us on 00 966 92000 9278

training@globalknowledge.com.sa

www.globalknowledge.com/en-sa/

Global Knowledge - KSA, 393 Al-Uroubah Road, Al Worood, Riyadh 3140, Saudi Arabia