interface
We teach. You do.

Wireless Training

SHARK400: Analyzing Network Security Using Wireshark Training

$3,695.00

- 4 Days
- Wireshark Training from Dr. Avril Salter
- Use Wireshark - capture traffic & identify security protocols
- "Deep-dive" analysis of network security protocols
- Replay recordings not included due to content licensing

Upcoming Dates

Course Description

Industry expert Dr. Avril Salter teaches this 4-day instructor-led Wireshark Training course. You'll learn how to use Wireshark to understand common network security protocols that are deployed in IP networks today, including:

- Telnet & SSH
- TLS both the legacy versions & the new version 1.3
- Key IPsec protocols, which includes IKE, ISAKMP, AH, & ESP
- 802.1X port-based access control, which encompasses RADIUS, EAP & EAPoL

Network security protocols are designed to ensure the privacy and integrity of data that is transitioning our networks and prevent unauthorized access. They define the processes and message exchanges to protect networks from illegitimate attempts to capture and extract meaningful information about the network or the data carried over the network.

In this Wireshark training course, you'll capture traffic and identify the security protocols implemented in today's enterprise networks. This is a deep dive analysis of network security protocols. You will also understand key capabilities in Wireshark that can be used to analyze and troubleshoot network traffic to identify security issues, including:

- Defining Wireshark security profiles
- Using Wireshark capture and display filters to identify protected and unprotected traffic
- Coloring rules
- Using relevant Wireshark statistical tools
- Leveraging Wireshark decryption capabilities

Instructor and author Dr. Avril Salter, CCNP-W, CCNA-S, has extensive experience in packet-level network security analysis and frequently lectures on this topic. She is a guest instructor at numerous telecommunications and network companies, teaching their internal staff to perform network security analysis on the equipment that they design and manufacture. This experience gives Dr. Salter the unique, industry-wide perspective that she brings to the classroom.

Course Outline

Module 1: Getting started with Wireshark

- The ethics of capturing wireless traffic
- Understanding why Wireshark does and doesn't do

- Installing Wireshark and doing a live capture
- Exporting and saving packet captures
- Cryptography
- A close look at Telnet

Labs: Telnet
Part 1: Live packet capture and timestamps
Part 2: Export package and Telnet port numbers
Part 3: Changing columns and Telnet authentication

Module 2: Deep dive analysis of Secure Shell (SSH)

- Leveraging Wireshark’s packet search capabilities
- Using capture filters
- Analyzing traffic with display filters
- Public and private cryptography
- Hashing algorithms
- A close look at SSH

Labs: SSH
Part 1: Display filters and SSH service requests
Part 2: Expressions and SSH performance
Part 3: Filtering TCP conversations

Module 3: Deep dive analysis of Transport Layer Security (TLS)

- Creating coloring rules to identify key security issues
- Diffie-Hellman key agreement protocol
- Shared secret
- Digital certificates
- A close look at SLS/TLS

Labs: TLS
Part 1: Coloring rules and TLS versions
Part 2: Colorizing packets and TLS 1.2 security attributes
Part 3: Compare and contrast TLS 1.2 and TLS 1.3
Part 4: TLS 1.3 0-RTT

Module 4: Deep dive analysis of Internet Key Exchange

- Defining your preferences
- Creating configuration profiles
- Random nonces
- Security Association (SA)
- A close look at IKE

Labs: IKE
Part 1: Configuration profiles and ISAKMP
Part 2: Establishing and IKE security association

Module 5: Deep dive analysis of IPsec

- Leveraging Wireshark statistics in analyzing network traffic
- Authentication, encryption and message integrity
- Decryption traffic in Wireshark
- A close look at AH
- A close look at ESP

Labs: IPsec
Part 1: Statistics and IPSEC AH
Part 2: Decryption and IPSEC ESP

Module 6: Deep dive analysis of network access security

- Merging packet captures
- Authentication protocols
- A close look at IEEE 802.1X
- Analyzing RADIUS messages
- A close look at EAP and EAP Authentication methods
- Analyzing EAPoL messages
- Wi-Fi Protected Access (WPA)

Labs: 802.1X
Part 1: 802.1X USING PEAP AND RADIUS
Part 2: EAPOL and the 4-Way Handshake
WPA2-Enterprise authentication

Module 7: Supplemental material

- A look at Layer 2 Tunneling Protocol (L2TP)
- A look at the new QUIC protocol

Labs: Supplemental labs
Layer 2 Tunneling Protocol (L2TP)
Quick UDP Internet Connections (QUIC)

Audience

This course is designed for individuals that require a deeper understanding of network security protocols, including designers, product developers, analysts, and technical support personnel. Specific use cases include:

- Security professionals that need to understand how to leverage Wireshark in their job
- Network administrator that need to understand the security mechanisms implemented in the networks they support
- Network security engineers that need to examine and investigate network security issues
- Developers that need to debug protocol implementations
- IT professionals that need to understand and explore network security protocol

Prerequisites

This course is designed to appeal to anyone needing to further their understanding of network security protocols, and looking to use Wireshark for packet analysis and troubleshooting. This course provides an in-depth look at security protocols and the message exchange between network nodes. The ideal student should be familiar with network security principles, such as authentication, cryptography and message integrity, and have attended the CompTIA Security+ course. It is strongly recommended that students have fundamental network knowledge covered in CCNA or CompTIA Network+.

What You Will Learn

- Capture and analyze network traffic.
- Understand how to identify network security protocols and mechanisms being deployed to protect network traffic.
- Develop Wireshark profiles, filters, and coloring rules to facilitate analyzing and troubleshoot network security protocols and mechanisms.
- Use the Wireshark statistical and decryption tools available to analyze network security traffic
- Distinguish between common security protocols being applied at the application, transport, network, and data link layers.
- Define the different security mechanisms being used to protect enterprise-level networks, including SSH, TLS, IPsec, 802.1X, RADIUS, and L2TP.

- Explore in detail the most common security protocols used in protecting network traffic, including SSL/TLS, HTTPS, Telnet, SSH, IPsec including IKE, ISAKMP, AH and ESP, and 802.1X, including RADIUS, EAP, and EAPoL.