



WSU02: Wireshark TCP/IP Network Analysis

This course focuses on both the normal and abnormal communications patterns of the TCP/IP suite and most common applications including ARP, ICMP, UDP, TCP, IPv4, DHCP, DNS, FTP, telnet, HTTP, POP and SMTP. Follow along as Laura explains the options for creating capture filters and display filters to view packets based on commands.

Course Contents

Course Overview

Section 1: TCP/IP Functionality Overview

- Module A. Resources and References for Analysts
- Module B. Capture on Hubbed, Switched and Routed Networks
- Module C. The TCP/IP Resolution Process
- Module D. Faults in the Resolution Process

Section 2: Analyze Domain Name System (DNS) Traffic

- Module A. Understand DNS Packet Structure
- Module B. Filter on DNS Traffic
- Module C. Analyze Normal DNS Traffic
- Module D. Analyze Unusual DNS Traffic

Section 3: Analyze Address Resolution Protocol (ARP) Traffic

- Module A. Understand ARP Packet Structure
- Module B. Filter on ARP Traffic
- Module C. Analyze Normal ARP Traffic
- Module D. Analyze Unusual ARP Traffic

Section 4: Analyze Internet Protocol Version 4 (IPv4) Traffic

- Module A. Understand IPv4 Packet Structure
- Module B. Filter on IPv4 Traffic
- Module C. Analyze Normal IPv4 Traffic
- Module D. Analyze Unusual IPv4 Traffic

Section 5: Analyze Internet Control Message Protocol (ICMP) Traffic

- Module A. Understand ICMP Packet Structure
- Module B. Filter on ICMP Traffic
- Module C. Analyze Normal ICMP Traffic
- Module D. Analyze Unusual ICMP Traffic

Section 6: Analyze User Datagram Protocol (UDP) Traffic

- Module A. Understand UDP Packet Structure
- Module B. Filter on UDP Traffic
- Module C. Analyze Normal UDP Traffic
- Module D. Analyze Unusual UDP Traffic

Section 7: Analyze Transmission Control Protocol (TCP) Traffic

- Module A. Understand TCP Packet Structure
- Module B. Filter on TCP Traffic
- Module C. Analyze Normal TCP Traffic
- Module D. Analyze Unusual TCP Traffic
- Module E. Analyze Handshake Problems
- Module F. Analyze the TCP Recovery Process
- Module G. Analyze TCP Congestion Traffic

Section 8: Analyze Dynamic Host Configuration Protocol (DHCP) Traffic

- Module A. Understand DHCP Packet Structure
- Module B. Filter on DHCP Traffic
- Module C. Analyze Normal DHCP Traffic
- Module D. Analyze Unusual DHCP Traffic

Section 9: Analyze Hypertext Transfer Protocol (HTTP) Traffic

- Module A. Understand HTTP Packet Structure
- Module B. Filter on HTTP Traffic
- Module C. Analyze Normal HTTP Traffic
- Module D. Analyze Unusual HTTP Traffic

Section 10: Analyze Telnet Traffic

- Module A. Understand Telnet Packet Structure
- Module B. Filter on Telnet Traffic
- Module C. Analyze Normal Telnet Traffic
- Module D. Analyze Unusual Telnet Traffic

Section 11: Analyze File Transfer Protocol (FTP) Traffic

- Module A. Understand FTP Packet Structure
- Module B. Filter on FTP Traffic
- Module C. Analyze Normal FTP Traffic
- Module D. Analyze Unusual FTP Traffic

Section 12: Analyze Post Office Protocol (POP) Traffic

- Module A. Understand POP Packet Structure
- Module B. Filter on POP Traffic
- Module C. Analyze Normal POP Traffic
- Module D. Analyze Unusual POP Traffic

Section 13: Analyze Simple Mail Transfer Protocol (SMTP) Traffic

- Module A. Understand SMTP Packet Structure
- Module B. Filter on SMTP Traffic
- Module C. Analyze Normal SMTP Traffic
- Module D. Analyze Unusual SMTP Traffic

Appendix A: Trace File Catalog

Appendix B: Requests for Comments Sets

Appendix C: Command-Line Tools Reference

Appendix D: Wireshark University Course List