Wireshark Troubleshooting and Security

Course 5443 – 24 Hours

Overview

Network forensics including capture locations, stealth-mode capture, optimal capture and display filters, validating encrypted logins, identifying reconnaissance processes, locating header and payload signatures, catching penetration tests, malware behavior, backdoor communications and virus traffic

Who Should Attend

- Channel Partner / Reseller
- Customer
- Employee

Prerequisites

- IP network address structure
- Display filtering on protocol or field
- Basic Wireshark graphs and tables (IO, conversations, endpoints)
- Save packets based on filters, markers or range value
- Basic security knowledge
  - Resources, viruses, worms, denial of service
- Network components
  - Hubs, switches, routers, firewalls, IDS, etc.

Course Contents

Part 1: Analysis Overview

Tapping into the network

- Wired v. wireless
- Tapping into hubbed networks
- Tapping into switched networks
  - Hubbing out
  - Port monitoring and spanning
  - Redirecting traffic
- Tapping into routed networks
  - Capture options
  - Windows wireless (WinPcap) issues
  - Capturing to a file
  - Using the ring buffer
  - Optimizing the capture process

- Command-line capture

Part 2: TCP/IP Analysis

Tapping into the network (wired, wireless, hubbed, switched, routed) TCP/IP traffic analysis

- Port usage and resolution
- Name resolution (network and hardware addresses)
- Route resolution and redirection
- ICMP functionality (packet structure, functionality)
- TCP functionality (handshake, fault tolerance, recovery)
- DNS functionality (address lookup, errors)
- IP functionality (addressing, fragmentation)

Part 3: Troubleshooting Network Performance

Causes of Performance Problems

- Where Network Faults Occur
- Time is of the Essence
- Wireshark Functions for Troubleshooting
- Using Pre-Defined Coloring Rules
- Basic and Advanced IO Graphs
- Use the Delta Time Value
- Analyze Expert Information
- Look Who's Talking
- Graph Bandwidth Use, Round Trip Time and TCP Performance
- Flow Graphing
- Statistics (Various)
- Latency Issues
- The Five Primary Points in Calculating Latency
- Plotting High Latency Times
- Free Latency Calculators
- Using the frame.time_delta Filter
- Packet Loss and Retransmissions
- Packet Loss and Recovery – UDP v. TCP
- Previous Segment Lost Events
- Duplicate ACKs
- TCP Retransmissions and Fast Retransmissions
- Out-of-Order Segments
- Misconfigurations and Redirections
- Visible Misconfigurations
- Don't Forget the Time
- Dealing with Congestion
- Shattered Windows
- Flooded Out
- Baseline Network Communications

- Baselining methods
- Trace file cataloging
- Trace file log book usage

Part 4:Network Forensics and Security

Overview of Network Forensics

- Tapping in
- Evidence recovery issues

Reconnaissance Process

- Port Scans
- Mutant Scans
- IP Scans
- Application Mapping
- OS Fingerprinting

Analyzing ICMP Traffic

- ICMP Types and Codes
- ICMP Discovery
- Router Redirection
- Dynamic Router Discovery
- Service Refusal
- OS Fingerprinting

TCP Security

- TCP Segment Splicing
- TCP Fake Resets

Address Spoofing

- MAC Address Spoofing
- IP Address Spoofing

Building Firewall ACL Rules

- Overview of ACL Rule Types

Signatures of Attacks

- Signature Locations
- Header Signatures
- Sequencing Signatures
- Payload Signatures
- Obtaining Signatures

Attacks and Exploits

- Password Cracks
- Denial of Service Attacks
- Redirections