



WSU04: Wireshark Network Forensics and Security

This course focuses on network forensics including capture locations, stealth-mode capture, optimal capture and display filters, validating encrypted communications, reconnaissance processes, header and payload signatures, penetration tests, malware behavior and backdoor/virus communications.

Course Contents

Course Overview – Introduction

Section 1: Analyzer Placement

- Module A. Tap in to Hubbed, Switched and Routed Networks
- Module B. Tap in to Full-Duplex Links
- Module C. Capture in Stealth Mode
- Module D. Your Analysis Lab

Section 2: Unusual Network Communications

- Module A. Understanding Normal TCP/IP Resolution Processes
- Module B. TCP/IP Resolution Process Vulnerabilities
- Module C. Spotting Unusual Traffic

Section 3: Reconnaissance Processes

- Module A. Port Scans
- Module B. Mutant Scans
- Module C. IP Scans
- Module D. Application Mapping
- Module E. OS Fingerprinting

Section 4: Analyzing ICMP Traffic

- Module A. ICMP Types and Codes
- Module B. ICMP Discovery
- Module C. Router Redirection
- Module D. Dynamic Router Discovery
- Module E. Service Refusal
- Module F. OS Fingerprinting

Section 5: TCP Security

- Module A. TCP Segment Splicing
- Module B. Malformed TCP Packets
- Module C. Reset Injections (aka Reset Attacks)
- Module D. Fake TCP Resets

Section 6: Address Spoofing

Module A. MAC Address Spoofing
Module B. IP Address Spoofing

Section 7: Building Firewall ACL Rules

Module A. Overview of ACL Rule Types and Options
Module B. Automatically Generating ACL Rules

Section 8: Signatures of Attacks

Module A. Signature Locations
Module B. Obtaining Signatures
Module C. Sample Botnet Attacks
Module D. Password Cracks
Module E. Denial of Service Attacks
Module F. Redirections

Appendix A: Wireshark Lab Exercises
Lab Exercise Information
Covert FTP Communications
Dueling Honeypots
Worm-Infected System
Hidden Data
Checking for a Poisoner
Clear Text Passwords
Decrypt SSL Traffic with an RSA Key

Appendix B: Trace File Catalog

Appendix C: Wireshark Code Sample

Appendix D: ICMP Type and Code List

Appendix E: IANA Port List

Appendix F: Snort Rules

Appendix G: Command-Line Tools Reference

Appendix H: Wireshark University Course List