



WSU04 [Self-Paced Course]

Network Forensics and Security



Course Format

This course is available only in self-paced format (voice-over-video) taught by **Laura Chappell**. The course DVD includes videos, supplemental files (in PDF format) and reference/resource materials for the network analyst.

Course Content

This course focuses on 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.

- Section 1: Analyzer Placement
 - a) Analyzing Hubbed Networks
 - b) Analyzing Switched Networks
 - c) Analyzing Routed Networks
 - d) Analyzing WAN Links
 - e) Tapping into Full-Duplex Links
 - f) Capturing in Stealth Mode
 - g) Obtaining Evidence Using a Honeypot

- Section 2: Unusual Network Communications
 - a) Vulnerabilities in the TCP/IP Resolution Process
 - b) Route Resolution
 - c) Spotting Unacceptable Traffic

- Section 3: Reconnaissance Processes
 - a) Port Scans
 - b) Mutant Scans
 - c) IP Scans
 - d) Application Mapping
 - e) OS Fingerprinting

[continued]



- Section 4: Analyzing ICMP Traffic
 - a) ICMP Types and Codes
 - b) ICMP Discovery
 - c) Router Redirection
 - d) Dynamic Router Discovery
 - e) Service Refusal
 - f) OS Fingerprinting

- Section 5: TCP Security
 - a) TCP Segment Splicing
 - b) TCP Fake Resets

- Section 6: Address Spoofing
 - a) MAC Address Spoofing
 - b) IP Address Spoofing

- Section 7: Building Firewall ACL Rules
 - a) Overview of ACL Rule Types

- Section 8: Signatures of Attacks
 - a) Signature Locations
 - b) Header Signatures
 - c) Sequencing Signatures
 - d) Payload Signatures
 - e) Obtaining Signatures
 - f) Attacks and Exploits
 - g) Password Cracks
 - h) Denial of Service Attacks
 - i) Redirections

[continued]



Recommended Course Prerequisites

This course focuses on 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.

Recommended prerequisite knowledge:

- Basic security knowledge (resources, viruses, worms, denial of service)
- Basic and advanced network components (hubs, switches, routers, firewalls, IDS)
- Very strong knowledge of Wireshark functionality and features
 - Navigation
 - Capture filters and methods
 - Packet details (TCP/IP protocols and applications)
 - Display filtering on protocol or field or bit value
 - Search by display filter, hex value or string
 - Basic Wireshark graphs and tables (IO, conversations, endpoints)
 - Advanced Wireshark graphs (CALC, SEQ/ACK, RTT)
 - Save packets based on filters, markers or range value
- Very strong knowledge of TCP/IP protocol and application functionality
 - Port usage and resolution
 - Name resolution (network and hardware address) and route resolution
 - ICMP functionality (packet structure, functionality)
 - TCP functionality (handshake, fault tolerance, recovery)
 - DNS functionality (address lookup, errors)
 - IP functionality (addressing, fragmentation)
 - ARP functionality (structure, functionality)
 - Follow TCP Streams
 - Expert Info/Expert Info Composite interpretation



Note:

If you cannot check off at 70% of the items listed in the prerequisite checklist, we recommend you take Wireshark University Courses WSU01 (Wireshark Functionality and Fundamentals) and WSU02 (TCP/IP Network Analysis).