CNFE - Certified Network Forensics Examiner

Course Overview

This course will introduce students to examining network forensics. Topics covered include investigative methodology, physical interception, wireless traffic capture and analysis, malware forensics, and more.

Module 1 - Digital Evidence Concepts 21m

Digital Evidence Concepts
Concepts in Digital Evidence
Overview
Background
Real Evidence
Best Evidence
Direct Evidence
Circumstantial Evidence
Hearsay
Business Records
Digital Evidence
Network-Based Digital Evidence
Section Summary

Module 2 - Network Evidence Challenges 24m

Network Evidence Challenges
Challenges Relating to Network Evidence
Overview
Acquisition
Content
Storage
Privacy
Seizure
Admissibility
Section Summary

Module 3 - Network Forensics Investigative Methodology 43m

Network Forensics Investigative Methodology
Oscar Methodology
Overview
Obtain Information
Obtain Information
Strategize
Strategize
Collect Evidence
Collect Evidence
Collect Evidence

Collect Evidence
Analyze
Analyze
Analyze
Analyze
Analyze
Analyze
Report
Section Summary

Module 4 - Network-Based Evidence 1h 3m
Network-Based Evidence
Sources of Network-Based Evidence
Overview
Background
Background
On the Wire
In the Air
Switches
Routers
DHCP Servers
Name Servers
Authentication Servers
Network Intrusion Detection/Prevention Systems
Firewalls
Web Proxies
Application Servers
Central Log Servers
A Quick Protocol Review
A Quick Protocol Review
Internet Protocol Suite Review
IPv4 vs IPv6
IPv4 vs IPv6
TCP vs UDP
TCP vs UDP
Section Summary

Module 5 - Network Principles 27m
Network Principles
Principles of Internetworking
Overview
Background
History
Functionality
Figure 5-1 The OSI Model
Functionality
Functionality
Encapsulation/De-encapsulation
Encapsulation/De-encapsulation
Figure 5-2 OSI Model Encapsulation

Encapsulation/De-encapsulation
Encapsulation/De-encapsulation
Encapsulation/De-encapsulation
Figure 5-3 OSI Model Peer Layer Logical Channels
Encapsulation/De-encapsulation
Figure 5-4 OSI Model Data Names
Section Summary

Module 6 - Internet Protocol Suite 1h 19m

Internet Protocol Suite
Overview
Background
History of Internet Protocol Suite
Application Layer
Application Layer Examples
Transport Layer
Layer 4 Protocols
Internet Layer
Network Access Layer
Comparing the OSI Model and TCP/IP Model
Similarities of the OSI and TCP/IP Models
Differences of the OSI and TCP/IP Models
Internet Architecture
IPv4
IP Address as a 32-Bit Binary Number
Binary and Decimal Conversion
IP Address Classes
IP Address Classes
IP Addresses as Decimal Numbers
Hosts for Classes of IP Addresses
IP Addresses as Decimal Numbers
Network IDs and Broadcast Addresses
Private Addresses
Reserved Address Space
Basics of Subnetting
Subnetworks
Subnetworks
Subnet Mask
Subnet Mask
IPv6
IPv4 versus IPv6
Transmission Control Protocol
User Datagram Protocol
ARP
ARP Operation Within a Subnet
ARP Process
Advanced ARP Concepts
Default Gateway
How ARP Sends Data to Remote Networks
Proxy ARP
Section Summary

Module 7 - Physical Interception 47m

Physical Interception
Overview
Goal
Background
Pigeon Sniffing
Cables
Copper
Optical
Radio Frequency
Information that Can Be Gained from Wi-Fi Traffic
Inline Network Tap
Vampire Tap
Radio Frequency
Radio Frequency
Hubs
Switches
Obtaining Traffic from Switches
Sniffing on Switches
Section Summary

Module 8 - Traffic Acquisition Software 50m

Traffic Acquisition Software
Agenda
Libpcap and WinPcap
Background
Libpcap - Introduction
Installing Libpcap using the RPMs
Installing Libpcap using the RPMs
Installing Libpcap from the Source Files
Installing Libpcap from the Source Files (Configure)
Installing Libpcap from the Source Files (Make/Make Install))
WinPcap - Introduction
Installing WinPcap
Section Summary
The Berkeley Packet Filter (BPF) Language
Overview
Background
BPF Primitives
Filtering Packets by Byte Value
Examples
Filtering Packets by Bit Value
Filtering Packets by Bit Value
Section Summary
Tcpdump
Overview
Background
Basics
Basics
Installing tcpdump (Windows Installation)

Installing tcpdump (Windows Installation)
Installing tcpdump (Linux Installation)
Installing tcpdump (Linux Installation)
Installing tcpdump (Linux Installation)
Filtering Packets with tcpdump
Filtering Packets with tcpdump
Section Summary
Wireshark
Overview
Background
Installing Wireshark
Installing Wireshark (Microsoft Windows Systems)
Installing Wireshark (Linux Systems)
Wireshark Protocol Analyzer
Section Summary
Tshark
Overview
Background
Examples of tshark
Statistics
Examples
Section Summary

Module 9 - Live Acquisition 1h 10m

Live Acquisition
Agenda
Common Interfaces
Overview
Background
Console
Secure Shell (SSH)
Secure Copy (SCP) and SFTP
Telnet
Simple Network Management Protocol (SNMP)
SNMP
Web and Proprietary Interfaces
Section Summary
Inspection without Access
Overview
Background
Port Scanning
Vulnerability Scanning
Section Summary
Strategy
Overview
Refrain
Connect
Record the Time
Collect Evidence
Record Investigative Activities
Section Summary

Module 10 - Layer 2 Protocol 31m

Layer 2 Protocol
The IEEE Layer 2 Protocol Series
Overview
Background
Layer 2 Protocols
CSMA/CD
CSMA/CD
802.11 Protocol Suite: Frame Types
802.11 Protocol Suite: Frame Types (Management Frames)
802.11 Protocol Suite: Frame Types (Management Frames)
802.11 Protocol Suite: Frame Types (Control Frames)
802.11 Protocol Suite: Frame Types (Data Frames)
802.11 Protocol Suite: Frame Analysis
802.11 Protocol Suite: Network-Byte Order
802.11 Protocol Suite: Endianness
802.11 Protocol Suite: Network-Byte Order
802.11 Protocol Suite: Wired Equivalent Privacy
802.11 Protocol Suite: Wired Equivalent Privacy
An 802.11 Packet Capture Displayed in Wireshark
802.1X
Section Summary

Module 11 - Protocol Analysis 1h 28m

Protocol Analysis
Agenda
Protocol Analysis
Overview
Background
Tools
Tools
Tools
Techniques
Section Summary
Packet Analysis
Agenda
Fundamentals and Challenges
Protocol Analysis
Documentation
Protocol Analysis Tools
Packet Details Markup Language and Packet Summary Markup Language
Packet Details Markup Language and Packet Summary Markup Language
Packet Details Markup Language and Packet Summary Markup Language
Wireshark
Wireshark Display
Tshark
Tshark Display
Protocol Analysis Techniques
Protocol Identification
Protocol Decoding

Exporting Fields
Defined
Packet Analysis Tools
Wireshark and Tshark Display Filters
ngrep
Hex Editors
Packet Analysis Techniques
Pattern Matching
Parsing Protocol Fields
Packet Filtering
Section Summary
Flow Analysis
Agenda
Overview
Background
Defined
Tools
Follow TCP Stream
Tools
Flow Analysis Techniques
Lists Conversations and Flows
List TCP Flows
Export Flow
Manual File and Data Carving
Automatic File Carving
Higher-Layer Traffic Analysis
HTTP
DHCP
SMTP
DNS
Higher-Layer Analysis Tools
Higher-Layer Analysis Tools
Section Summary

Module 12 - Wireless Access Points 20m

Wireless Access Points
Overview
Background
Background
Background
Background
Background
Why Investigate WAPs?
Types of WAPs
Types of WAPs
Types of WAPs
Volatile Data and Persistent Data
Section Summary

Module 13 - Wireless Traffic Capture and Analysis 25m

Wireless Traffic Capture and Analysis
Overview
Spectrum Analysis
Spectrum Analysis
Spectrum Analysis
Wireless Passive Evidence Acquisition
Wireless Passive Evidence Acquisition
Wireless Passive Evidence Acquisition
Analyzing 802.11 Efficiently
Section Summary

Module 14 - NIDS/Snort 57m

NIDS/Snort
Agenda
Investigating NIDS/NIPS and NIDS/NIPS Functionality
Overview
Background
Sniffing
Higher-Layer Protocols Awareness
Alerting on Suspicious Bits
Section Summary
NIDS/NIPS Evidence Acquisition
Overview
Background
Types of Evidence: Configuration
Types of Evidence: Alert Data
Types of Evidence: Packet Header/Content Data
Types of Evidence: Activities Correlated Across Multiple Sensors
NIDS/NIPS Interfaces
Section Summary
Comprehensive Packet Logging
Overview
Background
Background
Evidence
Section Summary
Snort
Overview
Background
Basic Architecture
Snort File Locations
Snort Rule Language
Snort Rules
Section Summary

Module 15 - Centralized Logging and Syslog 52m

Centralized Logging and Syslog
Agenda
Sources of Logs

Overview
Operating System Logs
Operating System Logs
Operating System Logs
Operating System Logs
Operating System Logs
Application Logs
Application Logs
Physical Device Logs
Network Devices
Section Summary
Network Log Architecture
Overview
Three Types of Logging Architectures
Three Types of Logging Architectures
Three Types of Logging Architectures
Remote Logging: Common Pitfalls and Strategies
Remote Logging: Common Pitfalls and Strategies
Remote Logging: Common Pitfalls and Strategies
Remote Logging: Common Pitfalls and Strategies
Log Aggregation and Analysis Tools
Log Aggregation and Analysis Tools
Section Summary
Collecting and Analyzing Evidence
Overview
Obtain Information
Obtain Information
Obtain Information
Strategize
Strategize
Strategize
Strategize
Collect Evidence
Collect Evidence
Collect Evidence
Collect Evidence
Analyze
Report
Section Summary

Module 16 - Investigating Network Devices 54m

Investigating Network Devices
Agenda
Storage Media
Overview
Background
DRAM (Dynamic Random-Access Memory)
CAM (Content-Addressable Memory)
NVRAM (Non-Volatile Random-Access Memory)
Hard Drive

ROM
Section Summary
Switches
Overview
Background
CAM Tables (Content-Addressable Memory)
ARP
Types of Switches
Types of Switches
Switch Evidence
Section Summary
Routers
Overview
Background
Types of Routers
Router Evidence
Section Summary
Firewalls
Overview
Background
Types of Firewalls
Types of Firewalls
Firewall Evidence
Section Summary

Module 17 - Web Proxies and Encryption 45m

Web Proxies and Encryption
Agenda
Web Proxy Functionality
Overview
WAP Attacks
Caching
URI Filtering
Content Filtering
Section Summary
Web Proxy Evidence
Overview
Background
Types of Evidence
Obtaining Evidence
Section Summary
Web Proxy Analysis
Overview
Background
Log Analysis Tools
Log Analysis Tools
Log Analysis Tools
Log Analysis Tools
Section Summary
Encrypted Web Traffic

Overview
Background
Transport Layer Security (TLS)
Gaining Access to Encrypted Content

Module 18 - Network Tunneling 36m

Network Tunneling
Tunneling for Functionality
Overview
VLAN Trunking
Inter-Switch Link (ISL)
Generic Routing Encapsulation (GRE)
IPv4 over IPv6 with Teredo
Implications for the Investigator
Section Summary
Tunneling for Confidentiality
Overview
Background
Internet Protocol Security (IPsec)
TLS/SSL
Implications for the Investigator
Section Summary
Covert Tunneling
Overview
Covert Tunneling Strategies
TCP Sequence Numbers
DNS Tunnels
Implications for the Investigator

Module 19 - Malware Forensics 33m

Malware Forensics
Trends in Malware Evolution
Overview
Background
Botnets
Encryption and Obfuscation
Distributed Command-and-Control Systems
Automatic Self-Updates
Metamorphic Network Behavior
Section Summary

Module 20 - Network Forensics and Investigating Logs 51m

Network Forensics and Investigating Logs
Agenda
Key Term
Network Forensics
Analyzing Network Data
The Intrusion Process
Looking for Evidence
Looking for Evidence

Looking for Evidence
Looking for Evidence
End-to-End Forensic Investigation
End-to-End Forensic Investigation
End-to-End Forensic Investigation
Log File as Evidence
Legality of Using Logs
Legality of Using Logs
Legality of Using Logs
Legality of Using Logs
Examining Intrusion and Security Events
Examining Intrusion and Security Events
Intrusion Detection
Using Multiple Logs as Evidence
Maintaining Credible IIS Log Files
Log File Accuracy
Logging Everything
Extended Logging in IIS Server
Extended Logging in IIS Server
Extended Logging in IIS Server
Keeping Time
UTC (Coordinated Universal Time)

Total Duration: 15h 18m