C)NFE: Certified Network Forensics Examiner

Course ID #: 7000-783-ZZ-Z

Hours: 35

Course Content

Course Description:

In this course you will cover 20+ modules of network forensic topics. The C)NFE provides practical experience through our lab exercises that simulate real-world scenarios covering investigation and recovery of data in network. The C)NFE focuses on centralizing and investigating logging systems as well as network devices.

Course Objectives:

Upon successful completion of this course, students will:

- Have knowledge to perform network forensic examinations
- Be able to accurately report on their findings, and
- Be ready to sit for the C)NFE exam

Prerequisites:

2 years networking experience
2 years in IT Security
Working knowledge of TCPIP

Target Audience:

- Digital and Network Forensics Examiners
- IS Managers
- Network Auditors
- IT Managers

Topics:

Module 1 -Digital Evidence Concepts

- Overview
- Concepts in Digital Evidence
- Section Summary
- Module Summary

Module 2 -Network Evidence Challenges

- Overview
- Challenges Relating to Network Evidence
- Section Summary
- Module Summary

Module 3 - Network Forensics Investigative Methodology

- Overview
- OSCAR Methodology
- Section Summary
- Module Summary

C)NFE: Certified Network Forensics Examiner

Course ID #: 7000-783-ZZ-Z

Hours: 35

Module 4 - Network-Based Evidence
- Overview
- Sources of Network-Based Evidence
- Section Summary
- Module Summary

Module 5 - Network Principles
- Background
- History
- Functionality
- FIGURE 5-1 The OSI Model
- Functionality
- Encapsulation/De-encapsulation
- FIGURE 5-2 OSI Model 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 Summary

Module 6 - Internet Protocol Suite
- Overview
- Internet Protocol Suite
- Section Summary
- Module Summary

Module 7 - Physical Interception
- Physical Interception
- Section Summary
- Module Summary

Module 8 - Traffic Acquisition Software
- Agenda
- Libpcap and WinPcap
- LIBPCAP
- WINPCAP
- Section Summary
- BPF Language
- Section Summary
- TCPDUMP
- Section Summary
- WIRESHARK
- Section Summary
- TSHARK
- Section Summary
- Module Summary

Module 9 - Live Acquisition
- Agenda
- Common Interfaces
- Section Summary
- Inspection Without Access
- Section Summary
- Strategy
- Section Summary
- Module Summary

Module 10 - Analysis
- Agenda
- Protocol Analysis
- Section Summary
- Section 02
- Packet Analysis
- Section Summary
- Section 03
- Flow Analysis
- Protocol Analysis
- Section Summary
- Section 04
- Higher-Layer Traffic Analysis
- Section Summary
- Module Summary

C)NFE: Certified Network Forensics Examiner

Course ID #: 7000-783-ZZ-Z

Hours: 35

Module 11 - Layer 2 Protocol
- Agenda
- The IEEE Layer 2 Protocol Series
- Section Summary
- Module Summary

Module 12- Wireless Access Points
- Agenda
- Wireless Access Points (WAPs)
- Section Summary
- Module Summary

Module 13 - Wireless Capture Traffic and Analysis
- Agenda
- Wireless Traffic Capture and Analysis
- Section Summary
- Module Summary

Module 14 - Wireless Attacks
- Agenda
- Common Attacks
- Section Summary
- Module Summary

Module 15 - NIDS_Snort
- Agenda
- Investigating NIDS/NIPS
- and Functionality
- Section Summary
- NIDS/NIPS Evidence Acquisition
- Section Summary
- Comprehensive Packet Logging
- Section Summary
- Snort
- Section Summary
- Module Summary

Module 16 - Centralized Logging and Syslog
- Agenda
- Sources of Logs
- Section Summary
- Network Log Architecture
- Section Summary
- Collecting and Analyzing Evidence
- Section Summary
- Module Summary

Module 17 - Investigating Network Devices
- Agenda
- Storage Media
- Section Summary
- Switches
- Section Summary
- Routers
- Section Summary
- Firewalls
- Section Summary
- Module Summary

Module 18 - Web Proxies and Encryption
- Agenda
- Web Proxy Functionality
- Section Summary
- Web Proxy Evidence
- Section Summary
- Web Proxy Analysis
- Section Summary
- Encrypted Web Traffic
- Section Summary
- Module Summary

C)NFE: Certified Network Forensics Examiner

Course ID #: 7000-783-ZZ-Z

Hours: 35

Module 19 - Network Tunneling

- Agenda
- Tunneling for Functionality
- Section Summary
- Tunneling for Confidentiality
- Section Summary
- Covert Tunneling
- Section Summary
- Module Summary

Module 20 - Malware Forensics

- Trends in Malware Evolution
- Section Summary
- Module Summary

Labs:

Lab 1: Sniffing with Wireshark
Lab 2: HTTP Protocol Analysis
Lab 3: SMB Protocol Analysis
Lab 4: SIP/RTP Protocol Analysis
Lab 5: Protocol Layers
Lab 6: Analyzing the capture of MacOf
Lab 7: Manipulating STP algorithm
Lab 8: Active Evidence Acquisition
Lab 9: IEEE 802.11
Lab 10: Use Snort as Packet Sniffer
Lab 11: Use Snort as Packet Logger
Lab 12: Check Snort's IDS abilities with pre-captured attack pattern files
Lab 13: Syslog lab
Lab 14: Network Device Log
Lab 15: Log Mysteries
Lab 16:

- Step 1: Open a Trace
- Step 2: Inspect the Trace
- Step 3: The SSL Handshake
- Hello Messages
- Certificate Messages
- Client Key Exchange and Change Cipher Messages
- Alert Message

Lab 17: SSL and Friendly Man-in-the-middle
Lab 18: Analyzing Malicious Portable Destructive Files
Lab 19: Mobile Malware

Accreditations:

Register for this class by visiting us at:
www.tcworkshop.com or calling us at 800-639-3535