

Certified Network Forensics Examiner

KEY DATA

Course Title: Certified Network Forensics Examiner

Duration: 5 days

Language: English

Format: Instructor-led
(Lecture and Lab)

Prerequisite:

- 2 years of networking experience
- 2 years of IT Security
- Working Knowledge of TCP/IP

Student Materials:

- Student workbook
- Student lab guide
- Student Exam Prep guide

Certification Exam:

- Mile2 C)NFE

CPEs: 40

WHO SHOULD ATTEND?

- Digital & Network Forensic Engineers
- IS & IT managers
- Network Auditors

COURSE OVERVIEW

The Certified Network Forensics Examiner vendor neutral certification was developed for a U.S. classified government agency. The C)NFE takes a digital and network forensic skill set to the next level by navigating through over twenty modules of network forensic topics.

The CNFE provides practical experience through our lab exercises that simulate real-world scenarios that cover investigation and recovery of data in network, Physical Interception, Traffic Acquisition, Analysis, Wireless Attacks and SNORT. The course focuses on the centralizing and investigating of logging systems as well as network devices.

Forensics Career



All Combos Include:

- Online Video
- Electronic Book (Workbook/Lab guide)
- Exam Prep Questions
- Exam
- Cyber Range Lab



ACCREDITATION



NICCS™

NATIONAL INITIATIVE FOR
CYBERSECURITY CAREERS AND STUDIES



UPON COMPLETION

Students will:

- Have knowledge to perform network forensic examinations.
- Have knowledge to accurately report on their findings from examinations
- Be ready to sit for the C)NFE Exam

Exam Information

The Certified Network Forensics Examiner certification exam is taken online through Mile2's Assessment and Certification System (MACS), which is accessible on your mile2.com account. The exam will take 2 hours and consist of 100 multiple choice questions. The cost is \$400 USD and must be purchased from the store on Mile2.com.



OUTLINE

Module 1: Digital Evidence Concepts
 Module 2: Network Evidence Challenges
 Module 3: Network Forensics Investigative Methodology
 Module 4: Network-Based Evidence
 Module 5: Network Principles
 Module 6: Internet Protocol Suite
 Module 7: Physical Interception
 Module 8: Traffic Acquisition Software
 Module 9: Live Acquisition
 Module 10: Analysis
 Module 11: Layer 2 Protocol
 Module 12: Wireless Access Points
 Module 13: Wireless Capture Traffic and Analysis
 Module 14: Wireless Attacks

Module 15: NIDS_Snort
 Module 16: Centralized Logging and Syslog
 Module 17: Investigating Network Devices
 Module 18: Web Proxies and Encryption
 Module 19: Network Tunneling
 Module 20: Malware Forensics

DETAILED COURSE OUTLINE

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

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

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

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

HANDS-ON LABORATORY EXERCISES



Module 4, 5 and 6 - Working with captured files

- 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

Module 7, 8, 9, 10, 11 – Evidence Acquisition

- Lab 1: Analyzing the capture of MacOf
- Lab 2: Manipulating STP algorithm
- Lab 3: Active Evidence Acquisition

Module 12, 13, 14 – Wireless Traffic Evidence Acquisition

- Lab 1: IEEE 802.11

Module 15: IDS/IPS Forensics

- Lab 1: Use Snort as Packet Sniffer
- Lab 2: Use Snort as Packet Logger
- Lab 3: Check Snort's IDS abilities with pre-captured attack pattern files

Module 16 and 21 - Network forensics and investigating logs

- Lab 1: Syslog lab
- Lab 2: Network Device Log
- Lab 3: Log Mysteries

Modules 17, 18 – SSL and Encryption

Objective

- Step 1: Open a Trace
- Step 2: Inspect the Trace

Answers

Step 3: The SSL Handshake

Hello Messages

Questions

Answers

Certificate Messages

Answer

Client Key Exchange and Change Cipher Messages

Answers

Alert Message

Answers to Alert Message

Lab 2: SSL and Friendly Man-in-the-middle

Module 20 - Malware Forensics

- Lab 1: Analyzing Malicious Portable Destructive Files
 - Lab 2: Mobile Malware
- Appendix: Forensic Challenge