Certified Network Forensics Examiner

Description:

The Certified Network Forensics Examiner, C)NFE, certification was developed for a U.S. classified government agency. It's purpose is to push students with a digital and network forensic skill set to the next level. In this course you will navigate through 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. Take your forensics career to the next level with Mile2's Network Forensics Engineer course.

Annual Salary Potential $99,000 AVG/year

Key Course Information

Live Class Duration: 5 Days
CEUs: 40
Language: English
Class Formats Available:

Instructor Led

Self-Study

Live Virtual Training

Suggested Prerequisites:

- 2 years networking experience

- 2 years in IT Secuirty

- Working knowledge of TCPIP

Modules/Lessons

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 13-20: See Detailed Outline Below

Hands-On 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
Labs 13-19: See Detailed Outline Below

Upon Completion

Upon completion, Certified Network Forensics Examiner 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.

Who Should Attend

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

Accreditations

Exam Information

The Certified Network Forensics Examiner exam is taken online through Mile2's Learning Management System and is accessible on you Mile2.com account. The exam will take approximately 2 hours and consist of 100 multiple choice questions.

A minimum grade of 70% is required for certification.

Re-Certification Requirements

All Mile2 certifications will be awarded a 3-year expiration date.

There are two requirements to maintain Mile2 certification:

1) Pass the most current version of the exam for your respective existing certification
2) Earn and submit 20 CEUs per year in your Mile2 account.

Course FAQ's

Question: Do I have to purchase a course to buy a certification exam?

Answer: No

Question: Do all Mile2 courses map to a role-based career path?

Answer: Yes. You can find the career path and other courses associated with it at www.mile2.com.

Question: Are all courses available as self-study courses?

Answer: Yes. There is however 1 exception. The Red Team vs Blue Team course is only available as a live class.

Question: Are Mile2 courses transferable/shareable?

Answer: No. The course materials, videos, and exams are not meant to be shared or transferred.

Course and Certification Learning Options

Detailed Outline:

Course Introduction

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

Detailed Labs Outline:

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 6: Analyzing the capture of MacOf
Lab 7: Manipulating STP algorithm
Lab 8: Active Evidence Acquisition
Module 12, 13, 14 – Wireless Traffic Evidence Acquisition
Lab 9: IEEE 802.11
Module 15: IDS/IPS Forensics
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
Module 16 and 21 - Network forensics and investigating logs
Lab 13: Syslog lab
Lab 14: Network Device Log
Lab 15: Log Mysteries
Modules 17, 18 – SSL and Encryption
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
Module 20 - Malware Forensics
Lab 18: Analyzing Malicious Portable Destructive Files
Lab 19: Mobile Malware