CNFE
Certified Network Forensics Examiner

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.

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

Course Length

5 days

Format

- Instructor-led classroom
- Instructor-led Online Training

Prerequisites

- Must have a Digital or Computer Forensics Certification or equivalent knowledge
- 2 years of IT Security

- Working Knowledge of TCPIP

Student Materials

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

Certification Exam

- Mile2 C)NFE

Who Should Attend?

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

Exam Information

The Certified Network Forensics Examiner 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.

Course Contents

- 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 SoftwareScanning
- 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 Scanning
- Module 20: Malware Forensics

Lab Outline

- Module 4, 5 & 6: - Working with Captured Files
- Module 7, 8, 9 10, 11: Evidence Acquisition
- Module 12, 13, 14: Wireless Traffic Evidence Acquisition
- Module 15: IDS/IPS Forensics
- Module 16 & 21: Network forensics and investigating logs
- Module 17 & 18: SSL & Encryption
- Module 20: Malware Forensics