C)NFE™

mile2®
Cyber Security Training & Consulting

Certified Network Forensics Examiner

COURSE OVERVIEW

5 Days | 40 CPE Credits | $3,500

The Certified Network Forensics Examiner was created when a U.S. Government Agency contracted us to train their team on advanced forensics in computer networks. The C)NFE will take your digital forensic skill set to the next level by navigating through over twenty modules of network forensic topics and providing you with hands-on, practical experience through our lab exercises that walk you through real-world situations that are solved with investigation and recovery of data in networks.

With the skill set of a C)NFE, students can understand exactly what is going on in a network to ensure its proper use by those entrusted with access. Every organization can benefit by employing a C)NFE to audit their network; everyone deserves to know how their resources are being used.

C)NFE TRACK

Professional Roles:
Forensic Auditor
IT Auditor
Law Enforcement
Internal Auditor
IT Professional

Prerequisites:
C)DFE: Digital Forensics Examiner
Or Equivalent Experience

C)NFE Exam:
2 Hours
100 Questions
$300 USD
Purchase on mile2.com

Advanced Course:
C)IHE: Incident Handling Engineer

UPON COMPLETION

Students will:

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

COURSE CONTENT

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

Lab 1: Working with captured files
Lab 2: Layer 2 Attacks & Active Evidence Acquisition
Lab 3: Preparing for Packet Inspection
Lab 4: Analyzing Packet Captures
Lab 5: Case Study: ABC Real Estate
Lab 6: NIDS/NIPS
Lab 7: Syslog Exercise
Lab 8: Network Device Log
Lab 9: SSL

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. The cost is $300 USD and must be purchased from Mile2.com.

DETAILED MODULE DESCRIPTION

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 LAB DESCRIPTION

Lab 1 - Working with captured files
Exercise 1 - HTTP.pcap
Exercise 2 - SMB.pcap
Exercise 3 - SIP_RTP.pcap
Lab 2 – Layer 2 Attacks & Active Evidence Acquisition
Exercise 1 – Analyze the capture of macof.
Exercise 2 – Manipulating the STP root bridge election process
Lab 3 - Preparing for Packet Inspection
Lab 4 - Analyzing Packet Captures
Exercise 1: Analyze TKIP and CCMP Frames starting from 4-Way Handshake process.
Lab 5 - Case Study: ABC Real Estate
Lab 6 - NIDS/NIPS
Exercise 1 - Use Snort as Packet Sniffer
Exercise 2 - Use Snort as a packet logger
Exercise 3 - Check Snort's IDS abilities with pre-captured attack pattern files
Lab 7 - Syslog Exercise
Lab 8 - Network Device Log
LAB 9 - SSL
Exercise 1 – Decrypting SSL Traffic by using a given Certificate Private Key
Exercise 2 – SSL and Friendly Man-in-the-middle