C)NFE™
CERTIFIED NETWORK
FORENSICS ENGINEER

Certified Network Forensics Examiner™

DATOS CLAVE

Nombre del curso
CNFE™

Duración: 40 horas

Materiales digitales:

- Manual de Referencia
- Lab Guide

Examen de Certificación:

- CNFE - Certified Network Forensics Examiner™

DESCRIPCIÓN DEL CURSO

Este curso fue diseñado originalmente para la Agencia de Inteligencia de EEUU. El programa CNFE prepara a los estudiantes para ejercer técnicas verdaderamente avanzadas de análisis forense de redes a través del uso de laboratorios exclusivos desarrollados por Mile2. Este curso es recomendado para los miembros de TI que desean avanzar en su red de investigación y respuesta a incidentes, manejo de políticas, procedimientos y técnicas.

MÓDULOS DEL CURSO

Módulo 1: Digital Evidence Concepts
Overview
Concepts in Digital Evidence
Section Summary
Module Summary

Módulo 2: Network Evidence Challenges
Overview
Challenges Relating to Network Evidence
Section Summary
Module Summary

Módulo 3: Network Forensics Investigative Methodology
Overview
OSCAR Methodology
Section Summary
Module Summary

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

Módulo 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

Módulo 6: Internet Protocol Suite
Overview
Internet Protocol Suite
Section Summary
Module Summary

Módulo 7: Physical Interception
Physical Interception
Section Summary
Module Summary

Módulo 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

Módulo 9: Live Acquisition
Agenda
Common Interfaces
Section Summary
Inspection Without Access
Section Summary
Strategy
Section Summary
Módulo Summary

CNSS

COMPUTER FORENSICS

Módulo 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

Módulo 11: Layer 2 Protocol
Agenda
The IEEE Layer 2 Protocol Series
Section Summary
Module Summary

Módulo 12: Wireless Access Points
Agenda
Wireless Access Points (WAPs)
Section Summary
Module Summary

Módulo 13: Wireless Capture Traffic and Analysis
Agenda
Wireless Traffic Capture and Analysis
Section Summary
Module Summary

Módulo 14: Wireless Attacks
Agenda
Common Attacks
Section Summary
Module Summary

Módulo 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

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

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

Módulo 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

Módulo 19: Network Tunneling
Agenda
Tunneling for Functionality
Section Summary
Tunneling for Confidentiality
Section Summary
Covert Tunneling
Section Summary
Module Summary

Módulo 20: Malware Forensics
Trends in Malware Evolution
Section Summary
Module Summary

LABORATORIOS HANDS-ON

Lab 1: Working with captured files
Exercise 1: HTTP.pcap
Exercise 2: SMB.pcap
Exercise 3: SIP_RTP.pcap

Lab 2: Layer 2 Attacks
Exercise 1 – Analyze the capture of macof.
Exercise 2 – Manipulating the STP root bridge election process

Lab 2: Active Evidence Acquisition

Lab 3: Preparing for Packet Inspection

Lab 4: Analyzing Packet Captures
Exercise 2: 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