Network Forensics

Course 71586 – 40 Hours

Overview

Network forensics training is about the analysis of network traffic to identify intrusions or anomalous activity. Compared to computer forensics, where evidence is usually preserved on disk, network data is more volatile and unpredictable and therefore requires a different approach. This course sets the groundwork of understanding networks and the investigation process on them. Students will master the fundamentals of conducting forensic analysis in a network environment. This course will incorporate demonstrations and lab exercises to reinforce hands-on capabilities.

The course helps prepare for the certification exam CNFE (Mile2).

On completion, Delegates will be able to

- Detect various types of computer and network incidents
- Analyze network artifacts left on a compromised system
- Understand alerts and advisories
- Respond to incidents
- Perform network traffic monitoring and analyzing logs
- Learn to work with different tools

Who should attend

- Law enforcement officers & intelligence corps
- Incident responders
- Computer investigators
- IT/network administrators
- IT security personnel
- Junior cyber forensics analysts

Prerequisites

This course addresses those with basic knowledge of:

- Linux
- Network Research or Network Security
- Windows Forensics

Course Contents:

Module Title	Description
Module 1: Network Forensics During this module, participants will learn how to read packets of data, perform file carving, and identify suspicious activity on the network. Students will get an insight into how an attack on the network is carried out and how it can be identified. Students will be tasked with constructing essential defensive tools that will raise alerts when the system is attacked.	▪ **Understanding Network-Based Firewalls** o Packet Filter o Common IDS ▪ **Traffic Analysis** ▪ **Understanding Packet Structure** o Packet Analysis ▪ **HAProxy** ▪ **EtherApe** ▪ **Wireshark** o Acquaintance with Wireshark o Statistics o TCP Stream o Understanding Coloring Rules o View Options on Packets o Dive Into Common Protocols
Module 2: Case Investigation During this module, students will understand the challenges of investigating network-based cases. Students will practice using various tools and investigation methodologies to correlate data and collect evidence.	▪ **Network Forensics Investigation Process** o Automation skills o MiTM Attack o Find Network Anomalies o Flow Analysis o Network File Carving o Discovering Network Tunnels
Module 3: Advanced Network Analysis During this module, students will master techniques for collecting evidence, accessing, and retrieving volatile and non-volatile information. Students will learn techniques for collecting evidence, accessing, and retrieving volatile and non-volatile information.	▪ **Advanced Network Analysis** o Advanced Wireshark o Advanced Tshark ▪ **Zeek** o Output Logs o Automating Process o Monitoring Data into Logs o Zeek-Cut Parsing
Module 4: Intrusion Detection and Mitigation In this module, students will learn how to deploy automatic data analyzers, using preset rules or craft custom rule-sets to alert and block on detection of suspicious traffic.	▪ **IPS vs IDS** o Essential Intrusion Detection Tools and Methods o IDS/IPS Analysis