Syllabus

Network Forensics

CYBERIUM ARENA
-SIMULATOR-

Description

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 requires a different approach. This course sets the groundwork for 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).

Target Audience

This course addresses those with basic knowledge in networks and Linux.

Pre-requisites

Linux

Networking

Objectives

- Detecting various types of computer and network incidents
- Analyzing network artifacts left on a compromised system
- Performing network traffic monitoring and analyzing logs
- Learning to work with different network analysis tools

Module 1: Intrusion Detection

During this module, participants will further explore data packets' and study on a deeper level, learn to identify network anomalies, and understand system alerts. Students will master the use of well-known command-line-interface (CLI) and graphic-user-interface (GUI) tools to further specialize in the field. Students will learn methodologies to approach investigations of incidents.

Networking
- Network Protocols
- The OSI Model
- Analyzing Packets

Basic Intrusion Detection Tools and Methods
- Wireshark
- TShark
- GeoIP Integration

Using the Scapy Module
- Crafting and Analysing Packets
- Working with PCAP Files
- Replaying Packets for Investigating

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.

Investigation Process
- MiTM Attack
- Find Network Anomalies
- Flow Analysis
- Network File Carving
- NetworkMiner
- File Carvers

Module 3: Advanced Network Analysis

During this module, participants will further explore data packets' study on a deeper level, learn to identify network anomalies, and understand system alerts. Students will master the use of well-known command-line-interface(CLI) and graphic-user-interface(GUI) tools to further specialize in the field.

Zeek

- Output Logs
- Automating Process
- Monitoring Data into Logs
- Zeek-Cut Parsing

Module 4: Intrusion Detection and Mitigation

Students will learn how to deploy automatic data analyzers in this module, using preset rules or craft custom rulesets to alert and block suspicious traffic detection.

IPS and IDS

- Essential Intrusion Detection Tools and
- Methods Installing and Configuration Sysmon
- Network Events
- IDS/IPS Operation
- Process
- IDS/IPSconfiguration
- Snort