CYBERIUM ARENA

Description

Network Forensics offers a deep dive into network analysis and intrusion detection. Participants will master packet analysis with tools like Wireshark, explore the network analysis framework Zeek, and tackle real-world case investigations, from detecting network anomalies to MiTM attacks. The course concludes with a focus on mitigation strategies, emphasizing the configuration and operation of IPS and IDS systems like Sysmon and Snort.

NETWORK FORENSICS

Module 1: Intrusion Detection

Delve into the core of networking with an in-depth exploration of network protocols and packet structures. Master advanced tools and techniques, from Wireshark and TShark analysis to GeoIP integration and Scapy module applications. Enhance your skills in intrusion detection, packet crafting, and working with IPv6.

Networking
Network Protocols
Packet Structure
Netstat and ProcMon
SysInternal
Intrusion Detection Methods
Wireshark Advanced: Network Attacks
TShark Analysis
GeoIP Integration
Using the Scapy Module
Crafting and Analyzing Packets
Working with IPv6

Module 2: Network Analysis

Dive into the world of Zeek, a dynamic network analysis framework. Master the art of automating processes, monitoring data into logs, and utilizing Zeek-Cut parsing. Enhance investigative skills by replaying packets and crafting detailed timelines.

Zeek
Output Logs
Automating Process
Monitoring Data into Logs
Zeek-Cut Parsing
Replaying Packets for Investigating
Creating a Timeline

Module 3: Case Investigation

Embark on a comprehensive journey through network investigations, from understanding the MiTM attack and identifying network anomalies to mastering flow analysis. Delve into tools like NetworkMiner and file carvers, and navigate the intricacies of Wi-Fi, from capturing wireless traffic to managing network access modes.

Investigation Process
MiTM Attack
Find Network Anomalies
Flow Analysis
Network File Carving
NetworkMiner
File Carvers
Capturing Wireless Traffic
Gaining Access Through Wi-Fi
HTTPS Traffic

Module 4: Mitigation

Deepen your understanding of network security with IPS and IDS systems, focusing on their operation and configuration. Dive into the world of Sysmon, from installation to capturing network events. Enhance your expertise with tools like Snort, a cornerstone in intrusion detection.

IPS and IDS
Sysmon
Installing and Configuration Sysmon
Network Events
IDS/IPS Operation Process
IDS/IPS Configuration
Snort

NX Defense | LEVEL: 4 | DURATION: 40h