CYBERIUM ARENA

— SIMULATOR —

SYLLABUS

NETWORK FORENSICS

MAIN FEATURES

Labs

The labs hold questions and tasks to support the training.

Book

The coursebooks accompany the lecturers and students alike in cybersecurity studies.

Scenarios

Provide participants possible situations from cybersecurity or cyberterrorism to solve.

Project

Trainees must complete a practical built-in project, produce defense and assault tools.

CYBERIUM ARENA

— SIMULATOR —

Description

The Network forensics training is about the analysis of network traffic, identifying intrusions and 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.

MODULES

Module 1: Intrusion Detection

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

Module 2: Network Analysis

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

Module 3: Case Investigation

Investigation Process
MiTM Attack
Find Network Anomalies
Flow Analysis
Network File Carving
NetworkMiner
File Carvers
Gaining Access Through Wi-Fi
HTTPS Traffic
Wi-Fi
Capturing Wireless Traffic
Management and Monitor Modes
Gaining Access to the Network

Module 4: Mitigation

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