CYBERIUM ARENA

— SIMULATOR —

SYLLABUS

LINUX 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

Forensics is the art of extracting evidence and important artifacts from a digital crime scene to help the investigator reconstruct the chain of events. This program dives into the technical details of analyzing logs, images, and memory files. Trainees learn to collect and analyze forensic evidence.

MODULES

Module 1: Computer Hardware

Drives and Disks
The Anatomy of a Drive
Data Sizes
Volumes & Partitions
Disk Partitioning
Disk Management
Solid State Drive (SSD)
Understanding Linux OS
Linux Directory Structure
Services and systemd
Users and Groups
Understanding Shells

Module 2: Forensic Fundamentals

Hashes and Encodings
The Use of Hash for Forensics
Base Encodings
Linux OS Artifacts
User Activity Files
Service Logging
Log Analysis
Files in /dev
Data and Files Structure
Hexadecimal Editing Tools
File Structure
Embedded Metadata
Working with Clusters

Module 3: Collecting Evidence

Forensic Data Carving
File Carving Tools
Suspicious User-Info
Collecting Information
Program Execution Evidence
Detecting Hidden Files and Directories
Collecting Network Information
Mounted Filesystems
Loaded Kernel Modules
Drive Data Acquisition
Exploring System Files
Creating an Image
Introduction to Memory Acquisition
Dumping a Memory-File
Understanding the /proc/kcore

Module 4: Analyzing Findings

Analyzing captured images
Extracting Protected Files
Mounting an Image as a drive
Volatile Memory Capturing
Analyzing Inode Numbering
Advanced Linux Analysis
Working with Binaries
Introduction to GDB