CYBERIUM ARENA

— SIMULATOR —

SYLLABUS

WINDOWS 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

Windows Forensics is an essential skill in the cybersecurity world. Participants will learn how different computer components work and how to investigate during and after a cyber incident. The training will focus on developing hands-on capabilities of forensics teams or individual practitioners.

MODULES

Module 1: Computer Hardware

Drives and Disks
Data Representation
Volumes & Partitions
Disk Partitioning and the Disk Management Tool
Solid State Drive (SSD) Features
Understanding Windows OS structure
NTFS Structure
Master File Table
Windows System Files
Data and Files structure
Hex Editors
File Structure

Module 2: Forensics Fundamentals

Understanding Hashes and Encodings
The Use of Hash for Forensics
Base Encodings
Windows Artifacts
Startup Files
Jump List
Thumbnail Cache
Shadow Copy
Prefetch and Temp Directories
RecentApps
Registry Hives
Embedded Metadata

Module 3: Collecting Evidence

Forensic Data Carving
Manual Carving
Automatic Tools
Collecting Information
Event Viewer
Detecting Hidden Files
Collecting Network Information
Sysinternals
Extracting Credentials

Module 4: Analyzing Forensic Findings

Drive Data Acquisition
Creating an Image
Analyzing Prefetch Files
Working with Volatile-Memory
Extracting Data from RAM
Identifying Network Connections
Dumping Processes from Memory
Registry analysis
Viewing Registry Dumps
Using Dat Files
Forensics Findings in the Registry
Anti-Forensics Techniques
Wiping Drives
Artifact Removing