CYBERIUM ARENA

SIMULATOR

SYLLABUS

MALWARE ANALYSIS

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

Malware Analysis is the study and close examination of malware to understand its origins, purpose, and potential impact on the system. Malware analysts accomplish their tasks using various tools and expert-level knowledge to understand what a piece of malware can do and how it does it. This program provides participants with the practical skills and knowledge to analyze malware required for their tasks.

MODULES

Module 1: Intro to Malware Analysis

Malware Analysis
Types of Malwares
Understanding the PE Format
Windows Libraries and Processes
Windows APIs
Setting a Sandbox
Building and Configuring Virtual Machine
Malware Analysis Tools
Extracting Malware from Data Segments
Network PCAP File
Volatile Memory

Module 2: Windows API

Windows API Overview
Windows Internals
Drivers
Memory
Threads
Process Listing
Syscall
System Activity in Windows Kernel
Dumping DLL
Detect Remote Thread Injection
Enumerating the Structure
Tokens and Privileges
Reading Process Memory

Module 2: Basic Analysis

Basic Static Analysis
PE File Sections
Analyzing Program Dependency Libraries
Resources Section Anomaly
Basic Dynamic Analysis
Identifying Virtual Machines
Searching for Ports
Testing Network Traffic
Analyzing Processes
Registry Analysis
Simulating Internet Services

Module 4: Advanced Analysis

Advanced Dynamic Analysis
Understanding Debuggers
Running Malware in OllyDbg
Running Malware in Windbg
Assembly Language Basics
x86 Processor Architecture
Understanding Buses and Data Traffic
Syscalls Table
Number and Character Representation
Basic Assembly x86 Programming
Disassembler
IDA Features
Analyzing Malware with IDA Pro