CYBERIUM ARENA

SIMULATOR

SYLLABUS

EXPLOIT DEVELOPMENT

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 ability to trace and exploit based on the deep understanding of program structure, execution patterns, finding vulnerabilities, and exploiting them to gain control over remote systems and applications. The trainees learn programming languages, write shellcodes, and the essential skills for advanced penetration testers and security professionals.

MODULES

Module 1: C Programming

C Programming Fundamentals

Variables and I/O
Expressions and Statements
Control Flow
The C Preprocessor
Functions
Code Structures
Memory Allocation

Module 2: Assembly x86

x86 Processor Architecture

Understanding Buses and Data Traffic
Syscalls Table
Number and Character Representation
Basic Assembly x86 Programming
Standard Output
Registers
Jumps and Flags

Module 3: Exploitation

Writing Shellcodes

Processor Registers Structure
Syscalls with Arguments
Windows Calling Convention
DLL and Functions
Spawning a Shell

Module 4: Overflow Attacks

Stack Overflow

Environment Variables
Overwriting Function Pointers
Segmentation Fault Error
System instructions and OP Codes
Finding Executable Crash-Address
Crashing Executables with Programming
Allocating Sizes
Stack Common Defense Mechanisms
Format strings vulnerability
Modify Arbitrary Memory Locations

Heap Overflow

Heap Structure and Functionality
Influence the Code Flow
Hijacking in Data Overwrite
Advance Overflow Techniques
Converting Strings to Little Endian Integers
Convert Binary Integers into ASCII Representation
Remote Blind Format String
Remote Heap Overflow Attack