CYBERIUM ARENA

— SIMULATOR —

SYLLABUS

REVERSE ENGINEERING

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

Reverse Engineering is a technique used to analyze software to identify and understand its components and its flows. It is a process of understanding code infringement processes and analyzing software weaknesses. Reverse Engineers analyze systems to create system representations in another form of abstraction.

MODULES

Module 1: Counting & Representing

Calculation of Bases
Hexadecimal Base
Binary Base
Transition Between Bases
Numerical Actions

Module 2: Assembly Language

Assembly
Registries
Processor Architecture
Portable Executable
Installing a Workspace
Linux syscall Table
File Descriptor
Debugging Process
IDA
Professionalization in GDB
Jumps & Conditions
Manipulation on a Processor
Activating Number-Detonation on the Processor
Ordering Bytes
Maintaining Flags Mode using a Stack
Stack
Calling Conventions
Build printf Functions using Assembly
Call to Functions

Module 3: Exploitation

Buffer
Protostar
Buffer Overflow
Writing Exploits to Bypass Protections
Processes in Computer Science
Race Condition
Anti-Reversing
Return Oriented Programming (ROP)
Memory Management Policy
W^X
NX bit
DEP
Ret2libc
Format String
Overcoming the ASLR M
Memory Management
How a Process Gets Memory from the System
Heap Overflow
Exploitation Over the Internet
Buffer Overflow Over the Internet
Tracer Browser Detection
Fuzzing
SPIKE
Debug Using OllyDbg to Restore Crash
Shellcode
Manually Create Shellcode
Create Shellcode Using Metasploit
Bad Characters