CYBERIUM ARENA

— SIMULATOR —

SYLLABUS

CYBER WARFARE

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

This program provides an advanced understanding of cyberspace operations, the complexities of the cyberspace environment, and planning, organizing, and integrating cyberspace operations. The trainees practice the different attack methodologies during the training, learning advanced penetration techniques inside and outside the organization.

MODULES

Module 1: Domain Attacks

Analyzing the Network
Automations Using NMAP
Using NSE
Capturing Spoofed Data
Data Enumeration
Password Authentication
Setting Up Your Lab
Passive Scanning
Host Enumeration
Domain Enumeration
Attacking the Local Network

Module 2: Post Exploitation

Post Exploitation
Configuring Payloads
Analyzing Local Exploits
Privilege Escalation
Meterpreter Modules
Post Frameworks

Module 3: Red-Team Techniques

Domain Techniques
Port Forwarding and Exfiltration
Privilege Escalation
Lateral Movement
Persistence Techniques
Detection and Defenses
Red Team Frameworks
C2 Framework
Password Extractors
Persistence
Process Injection

Module 4: Social Engineering

Social Engineering Techniques
Setting Phishing Servers
Creating Malicious Files
Delivering Malicious USB
Spear Phishing and Social Media
Phishing Tools