



CYBERIUM ARENA

— SIMULATOR —



SYLLABUS

OFFENSIVE PYTHON

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 world of information security consists of many complex issues and techniques for dealing with the many environments that can be vulnerable to global cyber-attacks. The program offers participants an advanced level of attack and evades many defense mechanisms available with the help of independent tools and Python programming capabilities.

MODULES

Module 1: Python Networking

Introduction to Sockets

- Connecting with TCP and UDP
- Banner Grabbing
- Port Scanner

Useful Libraries for Security

- Cymruwhois
- Faker

Password Cracking

- Brute Force Attacks
- Brute Force Zip Attacks
- FTP Cracker

Scanners

- Nmap
- Shodan

Module 2: Packet Crafting

Scapy

- Sniffing with Scapy
- Researching Pcap Files
- Crafting Packets
- Sending Packets
- Automation with Scapy
- Port Scanners
- MiTM Attack
- Creating Security Tools

Module 3: WebApp Security

HTTP Programming

- Simple Web Server
- Urllib
- BeautifulSoup
- Requests

Web Application Security

- Setting the User Agent
- Setting Cookies
- Using Web Proxy
- Spidering

Module 4: Metasploit Features

Working with Payloads

- MSFVenom
- The Python Payload
- TCP Reverse Shell Explained
- HTTP Reverse Shell Explained
- Persistence Explained
- Upgrading your Shell
- DDNS Reverse Shell

Local Attacks

- DNS Poison
- Extracting Passwords from Chrome
- Keylogger