ZX-310

Syllabus

Cyber Warfare

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.The course helps prepare for the certification exam OSCP (Offensive Security).

Target audience

This course targets penetration testers that would like to embrace Red-Team's capabilities.

Pre-requisites

Networking
Penetration Testing

Web Application Hacking

Objectives

- Acquiring the knowledge and tools to become a Red-Team member
- Working with tools for security-related tasks
- Becoming familiar with a variety of attack scenarios
- Understanding different attack possibilities
- Using automation as a Red-Team member

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

Configuring Payloads
Analyzing Local Exploits
Privilege Escalation
Meterpreter Modules
Post Frameworks

Module 3: Red-Team Domain Techniques

Domain Techniques
Port Forwarding and Exfiltration
Privilege Escalation
Lateral Movement
Persistence Techniques
Detection and Defenses
Red Team Framework
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