SDA.ACADEMY
Cybersecurity training

THINKCYBER

Syllabus

Cyber Warfare

CYBERIUM **ARENA**

-SIMULATOR-

Description

This training is an advanced course that covers topics in the Red-Team cyber warfare methodologies. Participants will get an in-depth look into the mind of a Black-Hat hacker and take a deep dive into its practical world using both IT and IoT devices. Students will learn the different information-gathering tools and security bypassing products that can be leveraged to attack against every defense layer.

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
- Becoming familiar with IoT
- Acquiring the necessary techniques and tools for IoT exploitation
- Firmware exploitation and analysis

Module 1: Introduction to IoT Security

Students will learn about IoT and smart devices, IoT device architecture analysis, and breaking it down to individual components, techniques, and tools during this module. Students will learn to find vulnerabilities all around the internet using smart queries.

Fundamental Concepts

- Understanding Firmwares
- Retrieving Firmwares

Mapping the Internet

- Mapping Attack Surface of a IoT Device
- Setting up Debian-OS for IoT Penetration Testing
- Nmap Basics
- Banner Grabbing Techniques
- IoT Mapping with Shodan

Module 2: Embedded IoT Operating Systems

In this module, students will get familiar with Linux and network-based exploitation and use their IoT environments skills.

Introduction to Embedded OS

- Working with SquashFS
- Using Binwalk
- Detecting Default Password
- Analyzing System Files
- Firmware Analysis - Identifying Hardcoded Secrets

Emulating Firmware Binary

- Working with QEMU
- Deploying Firmadyne
- Automating the Deployments
- Weaponising Firmwares

Web application Security for IoT

- Installing BurpSuite and Setting Proxy Interruption
- BurpSuite Components
- Exploitation with Command Injection
- Online Brute-Force Basics

Module 3: Red-Team Domain Techniques

In this module, students will learn to act as Red-Team while attempting to gain information about the target using different techniques.

Mastering Domain Techniques

- Setting Up Your Lab
- Passive Scanning
- Host Enumeration
- Domain Enumeration
- Port Forwarding and Exfiltration
- Privilege Escalation
- Lateral Movement
- Persistence Techniques - Domain and Local
- Detection and Defenses

Red Team Tools

- C2 Framework
- Password Extractors
- Persistence
- Configuring Your Metasploit Payloads
- Post Exploitation
- Process Injection

Module 4: Social Engineering

In this module, students will learn to perform attacks on targets using various sites and tools, and develop payloads that effectively compromise the system.

Social Engineering

- Social Engineering Techniques
- Making a Phishing Email
- Creating a Malicious File
- Delivering Malicious USB
- Spear Phishing and Social Media
- Phishing Tools