CYBERIUM ARENA

Description

Dive into advanced cybersecurity modules, starting with domain attacks and mastering tools like Mimikatz and post-exploitation techniques. Explore red-team operations, emphasizing domain techniques, persistence, and social engineering. Delve into IoT security, understanding vulnerabilities, and data extraction. Finally, immerse in embedded OS, learning about firmware emulation, deployment automation, and various IoT exploitation methods.

CYBER WARFARE

Module 1: Domain Attacks

Delve into comprehensive network security, starting with advanced reconnaissance and passive scanning techniques. Master tools like Mimikatz, understand the nuances of fileless attacks, and buffer overflows. Dive deeper into post-exploitation strategies, from configuring payloads to automating processes, ensuring a thorough grasp of privilege escalation and process injection.

Analyzing the Network
Advanced Recon and Scanning
Working with CVE
Mimikatz
Manual Exploitation
Fileless Attacks
Buffer Overflow
Configuring Payloads
Analyzing Local Exploits
Privilege Escalation
Process Injection
Automating Post Attacks

Module 2: Red-Team Techniques

Master port forwarding and data exfiltration to understanding lateral movements. Dive into red-team strategies, leveraging frameworks like C2, and fortify defenses against threats. Enhance skills in social engineering, setting up phishing servers, and crafting malicious files for comprehensive cybersecurity preparedness.

Lateral Movement
Port Forwarding and Exfiltration
Persistence Techniques
Detection and Defenses
Red Team Frameworks
C2 Framework
Persistence
Social Engineering Techniques
Setting Phishing Servers
Creating Malicious Files

Module 3: Intro to IoT Security

Learn to collect and extract crucial data, pinpoint IoT vulnerabilities, and grasp fundamental concepts. Delve into the intricacies of embedded OS, firmware understanding, and attack surface mapping. Enhance your expertise by setting up virtual machines, mounting file systems, and detecting hardcoded secrets.

Finding IoT Device
Advanced Shodan Use
Collecting and Extracting Data
Identifying IoT Vulnerabilities
Fundamental Concepts
Setting your VM
Introduction to Embedded OS
Understanding Firmware
Attack Surface
Mapping IoT Attack Surface
Mounting File Systems
Identifying Hardcoded Secrets

Module 4: Embedded OS

Delve into IoT system file analysis, firmware emulation, and the deployment of Firmadyne. Enhance your skills in weaponizing and backdooring firmware. Dive deeper into IoT exploitation techniques, from utilizing Burp to mastering command injections and brute-force attacks.

Introduction to Embedded OS
Working with SquashFS
Analyzing IoT System Files
Emulating Firmware Binary
Working with QEMU
Deploying Firmadyne
Automating the Deployments
Weaponizing Firmware
Backdooring a Firmware
Exploitation IoT with Burp

ZX Offense | LEVEL: 6 | DURATION: 40h