CYBERIUM ARENA

Description

The Penetration Testing training equips learners with crucial skills to identify and exploit system vulnerabilities. Covering data gathering, system infiltration, post-breach techniques, and emphasizing WebApp Security, this program prepares participants to effectively safeguard digital assets against cyber threats.

PENETRATION TESTING

Module 1: Collecting Information

This module empowers learners with fundamental penetration testing skills. It commences with Information Gathering, enabling understanding of targeted systems. Scanning follows, teaching detection of open ports and services. Lastly, Enumeration provides detailed system information, critical for crafting effective cyberattack strategies.

Information Gathering
Whois and Dmitry
Google and GHDB
Shodan CLI
DNS Reconnaissance
Online Databases
Scanning
Nmap Scanning
NSE Scripting
Enumeration
Services
Msfconsole
Enumeration Tools
Vulnerabilities Detection Methods
Nessus

Module 2: Exploitation

This module is focused on the practical aspects of penetration testing, with a keen focus on Exploitation. It starts by teaching the methodologies to leverage vulnerabilities for unauthorized system access. Further, it explores payloads, which are pieces of code executed post successful exploitation, providing crucial insights into cyberattack mechanics.

Exploitation
Brute Force Tools
Exploits Database
Msfconsole
Exploiting Manually
Payloads
Msfvenom Payloads
Payloads Automation
Meterpreter

Module 3: Post Exploitation

Post exploitation tactics, used after gaining unauthorized access, are explored, giving insights into maintaining access, data extraction, and covering tracks. Furthermore, it examines social engineering, a human manipulation tactic for information or access, underscoring the human element in cybersecurity.

Local vs. Remote Exploits
Privilege Escalation
Persistence
Disabling Security
Social Engineering
Online Services
BeEF
Phishing Frameworks
Advanced Techniques

Module 3: WebApp Security

This module sheds light on the crucial aspect of safeguarding web applications. It navigates through various aspects of web application security, highlighting common vulnerabilities, and providing effective strategies to counteract them. A key focus is on securing data transactions, user authentication processes, and ensuring overall application integrity.

HTML Basics
About OWASP
XSS
LFI/RFI
Brute Force
SQL Injection
Web Payloads
Reverse Shell
Burp Suite
Proxy
Repeater
Intruder
Encoder

ZX Offense | LEVEL: 3 | DURATION: 10-12 weeks (self-paced) / 40h (trainer-led)