Syllabus

Penetration Testing

CVBERIUM **ARENA**

-SIMULATOR-

Description

Penetration testers face a combination of intrusion detection systems, host-based protection, hardened systems, and analysts that pour over data collected by their security information management systems.

Penetration tests help find flaws in the system to take appropriate security measures to protect the data and maintain functionality. This training will provide the student with a steppingstone on running penetration testing in practice and taking on the complex task of effectively targeting and planning a penetration attack on a traditionally secured environment.

The course helps prepare for the certification exams CEH (ECICouncil), PenTest+ (CompTIA), and GPEN (SANS).

Target Audience

This course targets people from the IT world that want to upgrade their careers and master the art of penetration testing.

Pre-requisites

Linux
Networking

Objectives

- Bypass security and attack the network
- Becoming familiar with penetration
- Testing existing security weaknesses

Module 1: Planning and Collecting Information

Before the penetration testing team can analyze and conduct a series of tests and attacks, the team needs to gather data to construct a better action plan. In this module, the student will go through the basics of information gathering and reconnaissance.

Passive Information Gathering

The OSINT Framework
Monitoring Personal and Corporate Blogs
Collecting Employees Personal Information
Harvesting Organization Emails

Active Information Gathering

NMAP Scanning
Services Versions
DNS Enumeration

Identifying Vulnerability and Exploits

NSE Scripting
Vulnerabilities Detection Methods
Shodan Search Engine
Finding Exploits
Automating the Scanning

Module 2: Gaining Access and Post-Exploitation

In this module, the students will learn to use their knowledge in the first two phases to gain access, either using an existing exploit or brute-forcing them into the network. After gaining control of the target, the students will learn to abuse existing services to elevate their permissions.

Finding a Way In

Social Engineering
Brute-Forcing Services
Metasploit

Gaining Access Through Wi-Fi

Wi-Fi Basics
Management and Monitor Modes
Gaining Access to the Network

Post Exploitation and Evidence Gathering

Basic Privilege Escalation Using the Meterpreter Modules
Windows and Linux Privesc Basics
Network Pivoting

Module 3: Inside Threats

Finding vulnerabilities on the network using different sniffing methods is very important and can reveal the organization's vulnerabilities and weaknesses. In this module, students will use.

Sniffing and Attacks

- MAC Attacks
- DHCP Attacks
- ARP Poisoning
- Spoofing Attacks
- DNS Poisoning
- Sniffing Tools
- Sniffing Detection Techniques
- Kerberos Attacks
- Silver Tickets for Persistence
- Domain Mapping and Exploitation
- Effective Domain Privilege Escalation
- SMB Exploits
- SNMP Exploits SMTP Exploits
- FTP Exploits
- Pass-The-Hash

Module 4: Intro to WebApplication Security

In this module, students will learn the importance of web application security analysis. Many organizations were hacked using vulnerabilities in the application layer.

Hacking Web Servers

- SQL Injection
- File Upload Vulnerability
- Local File Inclusion
- Remote File Inclusion
- xss
- BeEF
- Password Attacks