SDA-ACADEMY
Cybersecurity training

THINKCYBER

NX-222

Syllabus

Penetration Testing

CYBERIUM **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.

Prerequisites

- Linux
- Networking

Objectives

- Bypass security and attack the network
- Becoming familiar with penetrations
- 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

Monitoring Personal and Corporate Blogs
Collecting Employees Personal Info
Harvesting Organization Emails
Shodan Search Engine

Active Information Gathering

NMAP Scanning
Services Versions
NSE Scripting

Module 2: Enumeration

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.

Service Enumeration

DNS Enumeration
DHCP Enumeration
SMB Enumeration
Network Traffic

Identifying Vulnerability and Exploits

NSE Enumeration
Vulnerabilities Detection Methods
Automating the Scanning

Module 3: Exploitation

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.

Attack Vectors

Brute-Forcing Services
Metasploit
Working with Exploits
Meterpreter
Social Engineering

Module 4: Post Exploitation

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

Post Exploitation

Configuring Payloads
Analyzing Local Exploits
Privilege Escalation
Using the Meterpreter Modules
Social Engineering