Penetration Testing certification

Day 1 Introduction, Basics of Linux & Networking, Shell Scripting

Introduction

- Introduction to Ethical Hacking
- Types of Hackers and their motives
- Some Basic Terminologies
- CIA Triad
- About threats and threat actors
- The Security Principles, Controls, and Associated Strategies
- Cybersecurity Laws, Regulations, Standards, and Frameworks

Networking Basics

- OSI Model
- TCP/IP Protocol Stack
- Protocol and their related Services
- IP Address, MAC Address, Port Address
- Subnetting and Routing
- Wireshark – Packet Sniffing and Analysis

Software Installation and Experimental Setup

- About Linux/Unix Operating System
- Setting-up your Hacking environment
- Honeypots

Linux Basics

- Linux File Structure
- Basic Linux Commands
- TCPDump, Tshark, Netcat etc. (Network Analysis)
- Basics of Vulnerability Scanning using Nmap & related Scripts
- MAC Changer

Linux Booting Process

- Linux Run Levels
- Linux Permissions
- Basics of Bash Scripting

Linux Internals Basics

- Introduction to Linux Internals
- Linux Kernel Architecture
- Process Management
- Memory Management
- File Systems
- Device Drivers
- System Calls
- Troubleshooting and Performance Tuning
- Analysing System Logs

Day 2 – Linux Privilege Escalation

Linux Privilege Escalation.

- Module 1: Introduction to Linux Privilege Escalation

1.1 Overview of Privilege Escalation

1.2 Linux Security Model

1.3 Common Vulnerabilities Leading to Privilege Escalation

- Module 2: Information Gathering

2.1 System Enumeration

2.2 Service Enumeration

2.3 User Enumeration

- Module 3: Exploitation Techniques

3.1 Exploiting Weak File/Folder Permissions

3.2 Exploiting sudo Misconfigurations.

3.3 Exploiting SUID and SGID Binaries

- Module 4: Post-Exploitation

4.1 Maintaining Access

4.2 Privilege Escalation Tools

- Module 5: Defensive Strategies

5.1 Linux Hardening Techniques

5.2 Monitoring and Detection

5.3 Incident Response

• Module 6: Case Studies and Real-world Scenarios

6.1 Analysing Historical Exploits

6.2 Hands-on Labs

Day 3 – Windows Internals , Privilege escalation

Windows Internal Basics

• Introduction to Windows Internals

• System Architecture

• Processes and Threads

• Memory Management

• I/O Subsystem

• Security and Access Control

• Networking Internals

• Windows registry.

Windows Privilege Escalation

• Module 1: Introduction to Windows Privilege Escalation

1.1 Overview of Privilege Escalation

1.2 Windows Security Model

1.3 Common Vulnerabilities Leading to Privilege Escalation

• Module 2: Information Gathering

2.1 System Enumeration

2.2 Service Enumeration

2.3 User Enumeration

• Module 3: Exploitation Techniques

3.1 Exploiting Weak File/Folder Permissions

3.2 DLL Hijacking

3.3 Registry-based Exploitation

• Module 4: Post-Exploitation

4.1 Maintaining Access

4.2 Privilege Escalation Tools

• Module 5: Defensive Strategies

5.1 Windows Hardening Techniques

5.2 Monitoring and Detection

5.3 Incident Response

• Module 6: Case Studies and Real-world Scenarios

6.1 Analysing Historical Exploits

6.2 Hands-on Labs

Day 4 - Web App PT, Information Gathering and OSINT

Passive Reconnaissance

• Netcraft

• nslookup

• Google Dorking

• Shodan

• Censys

• The Harvester

• Whois Enumeration and Reverse Whois

• DNS Enumeration

Active Reconnaissance and Connection Establishment

• Traceroute

• Netcat

• Nmap

• Proxy tools

• Metasploit (overview)

• FTP Connection and Remote File Uploading/download

• SSH Connection

• Telnet Connection

• Subdomain Enumeration

Vulnerability Scanning and exploitation tools.

Advanced Vulnerability Scanning using NMAP.

OpenVAS/Nessus

BurpSuite

Gobuster

Wfuzz

Hakrawler

Shells

Metasploit

- Introduction to Metasploit
- Creating payloads using Metasploit
- Reverse Listeners
- Exploiting Windows System
- HTTP Request and Methods
- Status Codes
- CVSS

Day 5 - Introduction to Web Pen-testing & OWASP Top 10

Introduction to Web Pen-testing

- Threat modelling of web application
- Cross site scripting discovery and exploitation
- JavaScript Validation
- Injection attacks
- XML External entities attack
- OWASP Top 10
- 2013 v/s 2017 v/s 2021
- Directory traversal attacks
- Content Security Policy
- Server-side template attacks
- Cross-origin attacks
- Security Headers

Web to shell attacks

- Introduction to web-shells
- Web to shell vulnerabilities
- Exploitation methods

Day 6 - Password Cracking, Malwares and Deepweb, Cryptography and Steganography

Password Cracking

- Wordlists
- Creating Custom Wordlists using Crunch
- Hydra for Password Cracking
- John the Ripper
- Metasploit for SSH password cracking
- Cyber Chef
- Rainbow Tables
- Basic Authentication Attacks

Malwares, Trojans, Virus and Worm

- Different Types of Malwares and Viruses
- Different Types of Bombs
- Dos and DDoS Attacks

Darkweb

- TOR
- Onion Websites

Cryptography and Steganography

- Symmetric Encryption / Private Key Cryptography
- Asymmetric Encryption / Public Key Cryptography
- Cryptographic Hash Functions and Values
- Encoding Decoding
- Steganography and different types.
- Steghide, stegseek etc.

Day 7 – Reciting Extremity Topics

- Waybackurls
- Tips & Tricks for technical interviews
- CTF Solving Approach
- Study and practise plans
- Pentest Reports Writing