15 Days - Introduction to Penetration Testing

Module 1: Introduction to Penetration Testing (1 Day)

- What is Penetration Testing?
- Types of Penetration Testing: Black Box, White Box, and Grey Box
- Overview of the Penetration Testing Lifecycle
- Legal and Ethical Considerations

Module 2: Setting up the Lab Environment (2 Days)

- Installing and configuring Virtual Machines (Kali Linux, Metasploitable)
- Overview of Penetration Testing Tools: Kali Linux, Burp Suite, Nmap, Netcat

Module 3: Reconnaissance and Information Gathering (4 Days)

- Active vs Passive Reconnaissance
- Tools: Nmap, Netcat, Whois, DNS Recon
- Gathering Information through Google Dorks and Social Media

Module 4: Vulnerability Scanning and Analysis (4 Days)

- Using Tools: Nessus, OpenVAS, Nikto
- Identifying and Exploiting Vulnerabilities
- Understanding CVE and Exploit Databases

Module 5: Basic Exploitation Techniques (4 Days)

- Introduction to Metasploit
- Exploiting a Vulnerability using Metasploit
- Understanding Buffer Overflow and Remote Code Execution

30 Days - Intermediate Penetration Testing

Includes All 15-Day Modules

Module 6: Network Penetration Testing (6 Days)

- Network Scanning and Mapping (Nmap, Netcat)
- Vulnerability Assessment on Network Services

- Exploiting Common Network Vulnerabilities (SMB, FTP, Telnet)

Module 7: Web Application Penetration Testing (8 Days)

- Introduction to OWASP Top 10
- Tools: Burp Suite, ZAP Proxy
- Exploiting Web Application Vulnerabilities: SQL Injection, XSS, CSRF, Command Injection

Module 8: Wireless Network Penetration Testing (4 Days)

- Cracking WEP, WPA, and WPA2
- Using Aircrack-ng, Kismet, and Wireshark
- Attacking Wireless Networks and MitM Techniques

Module 9: Penetration Testing Reporting (2 Days)

- Writing Detailed Penetration Test Reports
- Documenting Findings, Exploits, and Recommendations