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

45 Days - Advanced Penetration Testing

Includes All 30-Day Modules

Module 10: Social Engineering and Phishing Attacks (5 Days)

- Introduction to Social Engineering Techniques
- Phishing: Email and Website Spoofing
- Creating and Delivering a Phishing Attack

Module 11: Post-Exploitation Techniques (5 Days)

- Privilege Escalation: Windows and Linux
- Maintaining Access: Backdoors, Web Shells
- Data Exfiltration and Covering Tracks

Module 12: Exploit Development (5 Days)

- Introduction to Buffer Overflow and Stack Smashing
- Writing Custom Exploits
- Using Debuggers (Immunity Debugger, OllyDbg)

Module 13: Exploiting Common Platforms (5 Days)

- Penetration Testing Windows, Linux, and MacOS
- Exploiting Common Vulnerabilities on Different Platforms

Module 14: Advanced Reporting and Documentation (5 Days)

- Creating Comprehensive Penetration Test Reports
- Legal Considerations in Report Writing
- Presenting the Findings to Non-Technical Audiences

60 Days - Comprehensive Penetration Testing

Includes All 45-Day Modules

Module 15: Penetration Testing of Cloud Environments (6 Days)

- Overview of Cloud Security Models: IaaS, PaaS, SaaS
- Cloud Penetration Testing: AWS, Azure, GCP
- Identifying Misconfigurations in Cloud Environments

Module 16: Mobile Application Penetration Testing (6 Days)

- Mobile OS Penetration Testing: Android vs iOS
- Tools for Mobile Testing: Drozer, MobSF
- Exploiting Common Mobile Vulnerabilities: Insecure Data Storage, Intent Injection

Module 17: Advanced Web Application Attacks (5 Days)

- Advanced SQL Injection Techniques
- Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF)
- XML External Entity (XXE) Attacks

Module 18: Bypassing Firewalls and IDS/IPS (5 Days)

- Techniques for Bypassing Web Application Firewalls (WAF)
- Evasion Methods for IDS/IPS Systems