Penetration Testing Course Outline

Duration: 6 months.

Training Overview

Module 1. Introduction to Penetration Testing (Theory) (10 Days)

1. Definition and Objectives
2. Types of Penetration Testing
    - Network, Web, Cloud, and Mobile (Android)

3. Legal and Ethical Considerations
4. Penetration Testing Life Cycle

Module 2. Penetration Testing Methodology and Tools (Setup & theory)

1. Overview of Penetration Testing Process
    - Planning, Scanning, Exploitation, Reporting
2. Essential Tools and Software
    - Kali Linux, Burp Suite, Metasploit, etc.
3. Setting Up a Testing Environment
    - Virtual Machines, Labs, and Test Networks

Module 3. Network Penetration Testing (15 Days)

1. **Reconnaissance and Information Gathering (Practical)**
    - Network Mapping, DNS Interrogation
    - Tools: Nmap, Netcat
2. **Scanning and Enumeration**
    - Port Scanning, Service Identification
    - Vulnerability Scanning
    - Tools: Nessus, OpenVAS
3. **Exploitation**
    - Common Network Vulnerabilities
    - Wi-fi Attacks
    - Privilege Escalation Techniques
4. **Post-Exploitation**
    - Maintaining Access, Data Exfiltration

5. **Reporting and Documentation**

Module 4: Web Application Penetration Testing (30 days)

1. **Understanding Web Application Architecture (Theoretical)**
    - Client-Server Model, Common Technologies
2. **Reconnaissance and Information Gathering (Theoretical)**
    - Identifying Application Components
    - Tools: OWASP ZAP, Burp Suite
3. **Vulnerability Scanning**
    - Automated vs. Manual Testing
4. **Exploitation**
    - OWASP Top Ten Vulnerabilities
    - Common Attacks: SQL Injection, XSS, CSRF
5. **Server-side web attack**
    - SQL Injection
    - Authentication vulnerabilities
    - Path-traversal
    - OS command injection
    - SSRF

- **Client-side topics**
    - XSS
    - CSRF
    - CORS
    - Clickjacking
- Advanced topics
    - JWT Attack
    - Insecure deserialization

- SSTI
- HTTP Host Header Attacks
- HTTP request smuggling

6. **Reporting and Documentation**

Module 5: Cloud Security and Penetration Testing

1. **Overview of Cloud Environments**
   - IaaS, PaaS, SaaS Models
2. **Cloud Services and Components**
   - AWS, Azure, Google Cloud
3. **Reconnaissance and Information Gathering**
   - Identifying Cloud Resources and Configurations
4. **Scanning and Enumeration**
   - Cloud-Specific Scanning Tools
5. **Exploitation**
   - Cloud-Specific Vulnerabilities
   - Privilege Escalation in Cloud Environments
6. **Security Best Practices and Remediation**
7. **Reporting and Documentation**

Module 6 : Android Penetration Testing (20 Days)

- **Introduction to Android Architecture (Theoretical)**
  - Android Components and Lifecycle

- **Setting Up the Android Testing Environment (Practical)**
  - Emulators, Rooted Devices
- **Reconnaissance and Static Analysis**
  - Decompiling APK Files, Analyzing Manifest and Resources
  - Tools: APKTool, jadx, dex2jar
- **Dynamic Analysis**
  - Instrumentation and Runtime Analysis
  - Tools: Frida, Burp Suite
- **Common Vulnerabilities and Exploits**
  - Insecure Data Storage, Insecure Communication
- **Advanced Techniques**
  - Exploiting Intents, Custom Payloads
- **Reporting and Documentation**

Module 7: Hands-On Labs and Practical Exercises (15 Days) Including Doubt Session

- **Network Penetration Testing Labs**
  - Simulated Network Environments, Capture the Flag (CTF) Challenges
- **Web Application Labs**
  - Testing Real-World Web Apps, Vulnerability Exploitation Scenarios
- **Cloud Security Labs**
  - Configuring and Securing Cloud Resources, Vulnerability Assessment
- **Android Penetration Testing Labs**
  - Analyzing and Exploiting Android Apps, Real-World App Testing

THANK YOU FOR CHOOSING US!