



**Course Overview:**

**Penetration Testing Course**

Step into the world of Penetration Testing and build a strong foundation in identifying and exploiting security vulnerabilities in systems and applications. This course is designed for beginners, developers, and tech enthusiasts who want to understand how real-world cyber attacks are performed and prevented.

You will learn penetration testing fundamentals, reconnaissance techniques, vulnerability assessment, exploitation basics, and real-time security testing using industry-standard tools. Through practical examples and hands-on learning, you will gain the skills needed to discover and report security weaknesses.

By the end of the course, you will be equipped with practical knowledge and job-ready skills to start a career in Penetration Testing.

**1. Advanced Penetration Testing Overview :**

- Penetration Testing Methodologies (PTES, OSSTMM, NIST)
- Legal & Ethical Considerations
- Rules of Engagement (RoE)
- Scoping & Reporting
- Advanced Attack Lifecycle

## **2. Advanced Reconnaissance & Enumeration :**

- Passive vs Active Reconnaissance
- Advanced OSINT Techniques
- Subdomain Enumeration
- DNS & Network Enumeration
- Service & Version Fingerprinting
- Automated Recon Tools

## **3. Advanced Network Penetration Testing:**

- Advanced Nmap Techniques
- Firewall & IDS/IPS Evasion
- SMB Enumeration & Exploitation
- SNMP & LDAP Attacks
- Man-in-the-Middle Attacks
- Network Pivoting & Tunneling

## **4. Advanced Web Application Penetration Testing :**

- Deep Dive into OWASP Top 10
- Advanced SQL Injection (Union, Blind, Time-Based)
- Advanced XSS & Filter Bypass
- Authentication & Authorization Attacks
- Business Logic Flaws
- File Upload & Deserialization Attacks

## **5. API & Modern Application Testing :**

- REST & GraphQL API Security
- OWASP API Top 10
- Broken Object Level Authorization (BOLA)
- API Token Attacks
- Rate Limit Bypass
- API Fuzzing Techniques

## **6. Exploitation & Post-Exploitation :**

- Exploit Development Basics
- Metasploit Advanced Usage
- Privilege Escalation (Linux & Windows)
- Credential Dumping
- Persistence Techniques
- Lateral Movement

## **7. Active Directory Penetration Testing :**

- AD Architecture & Protocols
- Enumeration (LDAP, SMB, Kerberos)
- Kerberoasting & AS-REP Roasting
- Pass-the-Hash & Pass-the-Ticket
- BloodHound Analysis
- Domain Privilege Escalation

## **8. Cloud Penetration Testing :**

- Cloud Pentesting Rules & Scope
- AWS / Azure Attack Surface
- IAM Misconfigurations
- Cloud Storage Attacks
- Container & Kubernetes Attacks
- Cloud Post-Exploitation

## **9. Wireless & Mobile Penetration Testing :**

- Wi-Fi Security (WPA2/WPA3)
- Evil Twin Attacks
- Bluetooth Attacks
- Android & iOS Pentesting Basics
- Mobile App Reverse Engineering

## **10. Red Team Techniques :**

- Red Team vs Blue Team
- Command & Control (C2) Basics
- Phishing & Social Engineering
- Payload Obfuscation
- Evasion Techniques
- Purple Teaming Concepts

## **11: Advanced Tools & Automation :**

- Burp Suite Professional
- Metasploit Framework
- BloodHound
- Cobalt Strike (Conceptual)
- Custom Scripts (Python, Bash)
- Automation in Pentesting

## **12: Reporting, Certification & Capstone :**

- Advanced Pentest Reporting
- Risk Rating & Mitigation Advice
- Client Presentation Skills
- Certification Overview (CEH, OSCP, CRTP)
- Full-Scale Penetration Testing Project
- Capture The Flag (CTF) Challenge



SPYPRO SECURITY SOLUTIONS PVT. LTD.

**Contact Details :**

**+91 8182881234**

**+91 8182891234**

**Address:**

**Spypro Security Solutions Pvt.Ltd.,  
100 Ft Road , Backside Madhapur,  
Hyderabad, Telangana, 500081.**

