Cyber Security

Professional Penetration Tester (PENT)

Course Code: CS1PT

Duration: 45 hours

Course Overview

The Professional Penetration Tester(PENT) training is an intermediate to advanced cyber security course to equip students to learn professional penetration testing & vulnerability assessment skills by building lab networks to practice network and application enumeration, vulnerability scanning, exploitation, privilege escalation, and lateral movement skills.

This penetration testing and vulnerability assessment course helps you identify, detect and exploit any vulnerability in the target applications, networks, infrastructure and cloud security.

WHO SHOULD ATTEND ?

- Penetration Testers
- Security Engineers
- Security Researchers
- Bug Hunters
- Information Security Engineers
- Engineering Managers
- Web Developers

- QA Engineers
- Software Developers
- IT Professionals
- Students (Freshers)

Course Modules and Syllabus

Introduction

- Introduction to Cybersecurity
- Network Fundamentals
- Introduction to Penetration Testing
- Penetration Testing Methodology
- Lab Setup
- Introduction to Kali Linux & Tools
- Bash for Pentesters
- Python for Pentesters
- Note-taking: Chery Tree

Information Gathering

- Passive Reconnaissance
- Active Reconnaissance

Enumeration

- SMTP
- SNMP
- DNS

- NFS
- SMB
- FTP
- HTTP

Vulnerability Scanning

- Nessus
- CVSS Scoring

Web Application Scanning (DAST)

- Introduction to ZAP & Burp Suite
- OWASP ZAP
- Burp Suite Pro

Attacking Web Applications

- OWASP Top Ten
- CWE/SANS Top 25
- OWASP ASVS
- OWASP Testing Guide & Checklist
- Web Application Enumeration
- Injection Attacks
- File Inclusions
- Client-Side Attacks
- Server-Side Attacks
- File Upload Bypass

Web API Attacks

- Injection Attacks
- IDOR

- Mass Assignment
- Open Redirection

Exploit DB

- Choosing Exploits
- Fixing Exploits
- Updating Payload
- Compile & Deliver Exploit
- Execute Exploit

Metasploit Framework

- Introduction
- Modules
- Payloads
- MSFvenom
- Meterpreter
- Case Study: EternalBlue

Privilege Escalation

- Windows Privilege Escalation
- Linux Privilege Escalation

Password Attacks

- Brute force with Wordlists
- Password Cracking
- Capturing Password Hashes
- Pass the Hash Attack

Tunnelling & Port Forwarding

- Local Port Forwarding
- Remote Port Forwarding
- Dynamic Port Forwarding

Post Exploitation

- Autoroute
- Pivoting
- Lateral Movement

Cloud Security

- Introduction to Cloud Penetration Testing
- AWS Infrastructure & Components
- Cloud Reconnaissance & Tools
- Cloud Environment Security Audit
- AWS Web Application Penetration Testing
- AWS Web API Penetration Testing
- AWS Container Penetration Testing
- Penetration Testing Practice Scenarios
- AWS Security Services: IAM, KMS, Security Hub, Inspector, Guard Duty
- AWS Security Best Practices

Penetration Testing Labs

- Setting up Vulnerable Machines
- Building containerized Vulnerable Machines

Report Generation

- Penetration Testing Report Template
- Writing Professional Reports

Conclusion

- Next Steps
- Certification Exam
- Building a better Resume
- Career Guidance

Contact Us

ipsr solutions limited

Merchant's Association Building

M.L. Road, Kottayam - 686001

Kerala, India

Phone: +91 481-2301085

Mobile: +91 9447294635 | +91 94471 69776

Email: training@ipsrsolutions.com

Website: https://www.ipsr.org/

We have branches at Kochi, Thiruvananthapuram, Calicut and Bengaluru and Subsidiaries in UK, USA and Canada