

# Penetration Testing

## 90 Days Training Program



**"Penetration Testing: Uncover Vulnerabilities  
Before They Do."**

IIHT Jaipur believe that upskilling is mightier than massive layoffs. And not just us, but countless companies attest to it and have adopted this approach in their businesses as well. The domain expertise these upskilled individuals bring in is what sets them apart. We focus on nurturing these aspects. So, whether you are a student in college or a fresh graduate entering corporate, we have something for you to offer. We are an online and offline training institution that provides students and professionals with courses in high demand. We provide training in a vast array of technologies, including Cloud Computing, DevOps, Cyber Security, Full stack development, Data Science, Digital Marketing, and Web Development, among others.

**Penetration testing is an extremely important part of cybersecurity. In the current information age, data has grown to become the most valuable commodity, with many experts even suggesting it to be more valuable than oil. So, it should come as no surprise that cybersecurity has become paramount, and with it, so has penetration testing. Penetration testing (pen testing) is a deliberately planned attack on computer systems to assess the existing cybersecurity measures and discover vulnerabilities. Cybercrime is a continuously evolving threat and innovations in security measures always seem to be a step behind those for hacking. Thus, a prudent way of ensuring adequate levels of cybersecurity is to commission regular penetration testing and continuously find ways to improve.**



## S1. INTRODUCTION

- Difference and Approach between VA and PT
- Domains of VAPT
- Types of VAPT
- Red Team and Blue Team
- Black Box Testing
- White Box Testing

## 2. WEB SCANNERS

- Acunetix
- ZAP
- Nikto
- Pretty Recon
- Nuclei

## 3. BURP SUITE

- Proxy
- Spider
- Scanner
- Intruder
- Repeater
- Sequencer
- Decoder
- Comparer
- Extender · Alerts
- App Store

## 4. WEB Recon ( Advance Level )

- Whois lookup
- Reverse lookup
- IP history
- Detecting Backend Technology
- Subdomain Enumeration
- Eyewitness
- Google Dorking
- Shodan

## 5. CMS TESTING

- INTRODUCTION
- WPScan
- JoomScan
- DPScan

## 6. Python Based tools

- Parameter Finding
- Content Discovery
- Fuzzing
- Wayback
- Js Files



## 7. OWASP TOP 10

- Injection
- Broken Authentication and Session Management
- Cross-site scripting
- IDOR
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function level Access Control
- CSRF
- Using Components with known vulnerabilities
- Un-validated redirects and forwards

## 8. WEB EXTREME BUGS

- S3 Bucket
- HTTP Parameter Pollution
- Bypassing 2FA
- SSRF
- LFI
- RFI
- RCE
- Clickjacking
- Account Lockout
- Knoxss

## 9. WEB VAPT REPORTING

- Ways to report
- Formatting and Guidelines of report
- Case Study

## 10. BUG BOUNTY HUNTING

- Bug hunting
- Finding Bugs
- Common vulnerabilities neglected by Testers
- Making valid POC

## 11. ANDROID VAPT

- Introduction Android architecture
- Understanding of APK
- DEX to Jar
- Drozer
- Android network analysis
- OWASP Mobile Top 10

## 12. NETWORK VAPT

- Network Infrastructure
- Information Gathering
- Nessus, Searchsploit
- Backdoors, Compromising DCs
- Pass the Hash
- Role of AD
- Post Exploitation

## 13. NMAP ANALYSIS

- Introduction
- Installing nmap and cloud labs
- Nmap Discovery and Ping Scanning
- Nmap Scripting Engine
- Nmap Analysis

## 14. METASPLOIT

- Introduction Information Gathering
- Exploits modules
- Payloads
- Auxiliary
- Meterpeter
- Armitage

## 15. PORT REDIRECTION AND TUNNELING

- Port Forwarding/Redirection
- SSH Tunneling
- Proxychains
- HTTP Tunneling
- Traffic Encapsulation

## 16. FIREWALL

- Introduction
- Understanding of WEP, WPA, WPA2
- WEP, WPA Cracking

## 17. NETWORK VAPT REPORTING

- Ways to report .
- Formatting and Guidelines of report
- Case Study

## 18. BASICS OF IOT

- Introduction
- Benefits & Applications of IoT
- Issues with IoT
- IoT Attack Surface
- OWASP Top 10

## 19. Some Ways to Find Logical Vulnerability

- Misusing Features of Application
- Exploring Functionality & their Weakness
- Chaining of Different Vulnerability
- Out of the box thinking & Experimentation

## 20. Tryhackme & HacktheBox

- . Introduction
- . How to connect
- . Walkthrough
- . How to solve

## 21. Global Certificates

## 22. Resources




 9462081318 | 7877536377

 0141-2721218

 [www.iiht.org.in](http://www.iiht.org.in)

 [info@iiht.org.in](mailto:info@iiht.org.in)

 47, Jai Ambey Nagar, Opp. Jaipur Hospital, Main Tonk Road, Flyover, Near Gopalpura, Jaipur, Rajasthan - 302018