Wissenhive

CompTIA Pentest+ Training Certification

Table of Contents

About the Program

CompTIA PenTest+ certification is designed to measure pupils' practical skills for distinguishing weak policies, prone areas of cyber-attacks & threats, and competence for creating methods and policies for the implementation of exceptional protection to the organizational support.

CompTIA pentest + Certification is an intermediate-skills level course designed for IT cybersecurity professionals that concentrate and covers offensive skills through penetration testing, information gathering, and vulnerability identification. This certification also includes exploitation of networks, applications, wireless, and RF-based vulnerabilities, performing post-exploitation methods, understanding penetration testing through numerous coding scripts, and summarizing physical security attacks.

Key Training Features

- Ask Questions Real-Time and Interact with the Trainer Live
- Learner assistance and support - 24x7x365
- Flexible classes
- High-quality content created by industry experts
- Professionally designed Student Training Material
- High-Quality Audio-Video Lectures
- Lifetime Training Access
- Assessments

Training Options

- Self-paced Training
- Live Virtual Classes
- One on One Training

Why CompTIA Pentest+?

- Higher Paying Opportunities
- Gain Knowledge and Credibility
- Stand Out Among the Ordinary
- Knowledge of CompTIA Pentest+ Best Practices
- Better Career Growth & Job Opportunities
- Better ROI with Flexibility
- Sharpen your IT Skillset

What will you learn?

- Planning & scoping
- Information gathering & vulnerability identification,
- Attacks & exploits
- Penetration testing tools (in Bash, Ruby, Python, PowerShell)
- Reporting & communication

Career Option with Salary Compensation

Penetration Tester

- Minimum - $58,000
- Avg Salary - $86,000
- Maximum - $139,000

Security Analyst

- Minimum - $49,000
- Avg Salary - $69,000
- Maximum - $100,000

Systems Administrator

- Minimum - $45,000
- Avg Salary - $63,000
- Maximum - $89,000

Network Administrator

- Minimum - $43,000
- Avg Salary - $60,000
- Maximum - $84,000

Information Security Officer

- Minimum - $59,000
- Avg Salary - $93,000
- Maximum - $136,000

CompTIA PenTest+

Target Audience

- Penetration Tester
- Network Security Operations
- Vulnerability Tester
- Vulnerability Assessment Analyst
- Security Analyst (II)
- Application Security Vulnerability
- System Administrator
- Network Administrator

Prerequisites

There are no particular prerequisites for the CompTIA PenTest+ certification course, but Wissenhive recommends at least having one of the following:

- 2-3 years experience in information security, IT management, or IT operations role

  OR
- Basic familiarity with systems and networks.
- Degree in network and security

Course Details

This PenTest+ certification is an advanced course designed for intermediate-level cybersecurity specialists or who wants to strengthen their skills in penetration testing, vulnerability assessment management, and the ability to gain hands-on experience in environments such as desktop, servers, and cloud.

In this course, apprentices learn about the detailed concept of Pentest, which includes

- Implementing penetration testing and vulnerability scanning
- Analyzing results and data through effective reporting.
- Understanding pen-testing to gather information
- Analyzing the planning weightage and key aspects of compliance
- Understanding network flexibility and pliability

Course Curriculum:

1. In-depth Understanding Course

- CompTIA Pentest+ Certification Information
- How to Get the Most Out of This Course?
- Advantages of CompTIA Pentest+
- Virtual Machine Installation
- Installation of Windows and Kali Linux
- Download Windows and Kali Linux

2. Penetration Testing

- Planning and Scoping
- Penetration Testing Methodology
- Planning a Penetration Test
- Impacts and Constraints
- Resources and Budgets
- Penetration Testing Strategies
- Rules of Engagement
- Threat Actors
- Types of Assessments
- Penetration Testing Terminologies
- Legal Information

Course Curriculum:

3. Information Gathering

- Basics Information Gathering
- Discover Active Machines in the Network
- Various Nmap Commands
- Discover Open Ports in the Network Using Nmap
- Discover Website Frontend and Backend Information
- Download Website Folders Offline
- Discover Subdomains of a Website
- Discover Social Networking Accounts Associated with a Person
- Discover Relations between Organizations
- Discover Emails of the Target's Friends

4. Vulnerability Identification

- Vulnerability Assessment Basics
- Network Scanning and Report Generation
- Nessus – Network Vulnerability Scanner Installation
- Website Scanning and Report Generation
- Acunetix – Web Vulnerability Scanner Installation
- OWASP ZAP Web Vulnerability Scanner
- WPScan WordPress Analyzer
- Burp Suite Web Analyzer

Course Curriculum:

5. Penetration Testing Tools
- Password Attack Tools
- Database Attack Tools
- Social Engineering Tools
- Wireless Attack Tools
- Exploitation Tools
- Sniffing Tools
- Post Exploitation Tools

6. Attacks and Exploits
- Database Attack Using sqlmap Tool
- Password Attack Using Hydra Tool
- Database Attack Using jSQL Tool
- Exploitation Attack Using Metasploit Framework
- Password Attack Using Medusa Tool
- Exploitation Attack Using BeEF Framework
- Wireless Attack Using Fern Wi-Fi Cracker
- Wireless Exploitation Setup
- AV Bypass Using Shell and Python Scripts
- Shell and Python Scripts

7. Reporting and Communication
- Report Writing Steps
- MagicTree – Reporting Tool
- Metagoofil – Reporting Tool
- Recordmydesktop – Reporting Tool
- Report Summary

Contact us

WISSENHIVE E-LEARNING PRIVATE LIMITED

Noida

B-115, B Block, Sector 2,
Noida, Uttar Pradesh-201301

If you have any further questions or would like to chat with us, give us a call

Contact - sales@wissenhive.com

https://www.facebook.com/Wissenhive

https://www.linkedin.com/company/wissenhive/

https://www.instagram.com/wissenhive/

https://twitter.com/HiveWissen

https://in.pinterest.com/wissenhive/

https://www.youtube.com/channel/UCEaIUuf4czgsl9F0PTs0lDg