New Horizons®

# CompTIA Penetration Testing Certification (PenTest+) - (Exam PT0-002)

## Summary

Length: 40 hours Level: Experienced

As organizations scramble to protect themselves and their customers against privacy or security breaches, the ability to conduct penetration testing is an emerging skill set that is becoming ever more valuable to the organizations seeking protection, and ever more lucrative for those who possess these skills. In this course, you will be introduced to general concepts and methodologies related to pen testing, and you will work your way through a simulated pen test for a fictitious company. This course will assist you if you are pursuing the CompTIA PenTest+ certification, as tested in exam PT0-002. PenTest+ is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements. This course may earn a Credly Badge.

## Learning Objectives

This course will prepare students for the CompTIA PenTest+ (PT0-002) exam and verify the successful candidate has the knowledge and skills required to:

Plan and scope a penetration testing engagement
Understand legal and compliance requirements
Perform vulnerability scanning and penetration testing using appropriate tools and techniques, and then analyze the results
Produce a written report containing proposed remediation techniques, effectively communicate results to the management team, and provide practical recommendations

## Course Outline

1. ### Scoping Organizational/Customer Requirements

   Topic 1A- Define Organizational PenTesting
   Topic 1B- Acknowledge Compliance Requirements
   Topic 1C- Compare Standards and Methodologies
   Topic 1D- Describe Ways to Maintain Professionalism

2. ### Defining the Rules of Engagement

   Topic 2A- Assess Environmental Considerations
   Topic 2B- Outline the Rules of Engagement
   Topic 2C- Prepare Legal Documents

3. ### Footprinting and Gathering Intelligence

   Topic 3A- Discover the Target
   Topic 3B- Gather Essential Data
   Topic 3C- Compile Website Information
   Topic 3D- Discover Open-Source Intelligence Tools

4. ### Evaluating Human and Physical Vulnerabilities

   Topic 4A- Exploit the Human Psyche
   Topic 4B- Summarize Physical Attacks
   Topic 4C- Use Tools to Launch a Social Engineering Attack

5. ### Preparing the Vulnerability Scan

Topic 5A- Plan the Vulnerability Scan
Topic 5B- Detect Defenses
Topic 5C- Utilize Scanning Tools

6. Lesson 6- Scanning Logical Vulnerabilities

Topic 6A- Scan Identified Targets
Topic 6B- Evaluate Network Traffic
Topic 6C- Uncover Wireless Assets

7. Analyzing Scanning Results

Topic 7A- Discover Nmap and NSE
Topic 7B- Enumerate Network Hosts
Topic 7C- Analyze Output from Scans

8. Avoiding Detection and Covering Tracks

Topic 8A- Evade Detection
Topic 8B- Use Steganography to Hide and Conceal
Topic 8C- Establish a Covert Channel

9. Exploiting the LAN and Cloud

Topic 9A- Enumerating Hosts
Topic 9B- Attack LAN Protocols
Topic 9C- Compare Exploit Tools
Topic 9D- Discover Cloud Vulnerabilities
Topic 9E- Explore Cloud-Based Attacks

10. Testing Wireless Networks

Topic 10A- Discover Wireless Attacks
Topic 10B- Explore Wireless Tools

11. Targeting Mobile Devices

Topic 11A- Recognize Mobile Device Vulnerabilities
Topic 11B- Launch Attacks on Mobile Devices
Topic 11C- Outline Assessment Tools for Mobile Devices

12. Attacking Specialized Systems

Topic 12A- Identify Attacks on the IoT
Topic 12B- Recognize Other Vulnerable Systems
Topic 12C- Explain Virtual Machine Vulnerabilities

13. Web Application-Based Attacks

Topic 13A- Recognize Web Vulnerabilities
Topic 13B- Launch Session Attacks
Topic 13C- Plan Injection Attacks
Topic 13D- Identify Tools

14. Performing System Hacking

Topic 14A- System Hacking
Topic 14B- Use Remote Access Tools
Topic 14C- Analyze Exploit Code

15. **Scripting and Software Development**

    Topic 15A- Analyzing Scripts and Code Samples
    Topic 15B- Create Logic Constructs
    Topic 15C- Automate Penetration Testing

16. **Leveraging the Attack- Pivot and Penetrate**

    Topic 16A- Test Credentials
    Topic 16B- Move Throughout the System
    Topic 16C- Maintain Persistence

17. **Communicating During the PenTesting Process**

    Topic 17A- Define the Communication Path
    Topic 17B- Communication Triggers
    Topic 17C- Use Built-In Tools for Reporting

18. **Summarizing Report Components**

    Topic 18A- Identify Report Audience
    Topic 18B- List Report Contents
    Topic 18C- Define Best Practices for Reports

19. **Recommending Remediation**

    Topic 19A- Employ Technical Controls
    Topic 19B- Administrative and Operational Controls
    Topic 19C- Physical Controls

20. **Performing Post-Report Delivery Activities**

    Topic 20A- Post-Engagement Cleanup
    Topic 20B- Follow-Up Actions

## Audience

This course is designed for those whose job role could be Penetration Tester, Security Consultant, Cloud Penetration Tester, Cloud Security Specialist, Network & Security Specialist, Web App Penetration Tester, Information Security Engineer, and Security Analyst.

## Prerequisites

3–4 years of hands-on experience performing penetration tests, vulnerability assessments, and code analysis Network+, Security, or equivalent certifications/knowledge