Over 35 Years Of Technology Training

Document Generated: 12/18/2025

Learning Style: On Demand

Technology: CompTIA

Difficulty: Intermediate

Course Duration: 9 Hours

CompTIA Pentest+ Certification Exam Bundle

This course is for professionals preparing for the PT0-002 certification exam. The course also includes the official exam voucher.

About this Course:

PenTest+ is unique because our certification requires a candidate to demonstrate the hands-on ability and knowledge to test devices in new environments such as the cloud and mobile, in addition to traditional desktops and servers.

Course objectives:

- The CompTIA PenTest+ certification verifies that successful candidates have the knowledge and skills required to plan and scope an assessment
- Understand legal and compliance requirements, perform vulnerability scanning and penetration testing.
- Analyze data, and effectively report and communicate results.

Audience:

- Security Analysts
- Penetration Testers
- Vulnerability Testers
- Network Security Operations
- Application Security Vulnerability Testers

Prerequisites:

- While there is no required prerequisite, PenTest+ is intended to follow CompTIA Security+ or equivalent experience and has a technical, hands-on focus. Recommended experience in Network+, Security+ or equivalent knowledge. Minimum of 3-4 years of hands-on information security or related experience.

Course Outline:

- Course Introduction
- Lesson 1: Scoping Organizational/Customer Requirements
- Lesson 2: Defining the Rules of Engagement
- Lesson 3: Footprinting and Gathering Intelligence
- Lesson 4: Evaluating Human and Physical Vulnerabilities
- Lesson 5: Preparing the Vulnerability Scan
- Lesson 6: Scanning Logical Vulnerabilities
- Lesson 7: Analyzing Scanning Results
- Lesson 8: Avoiding Detection and Covering Tracks
- Lesson 9: Exploiting the LAN and Cloud
- Lesson 10: Testing Wireless Networks
- Lesson 11: Targeting Mobile Devices
- Lesson 12: Attacking Specialized Systems
- Lesson 13: Web Application-Based Attacks
- Lesson 14: Performing System Hacking
- Lesson 15: Scripting and Software Development
- Lesson 16: Leveraging the Attack: Pivot and Penetrate
- Lesson 17: Communicating During the PenTesting Process
- Lesson 18: Summarizing Report Components
- Lesson 19: Recommending Remediation

- Lesson 20: Performing Post-Report Delivery Activities