CompTIA

PENTEST+
EXAM PT0-002

The CompTIA PenTest+ certification is an IT workforce certification and an intermediate credential for security professionals. Candidates receive training on penetration testing, and vulnerability assessment and management skills necessary to determine the resiliency of the network against attacks. In addition, the course provides hands-on training for planning and scoping a penetration testing engagement including vulnerability scanning, understanding legal and compliance requirements, analyzing results, and producing a written report with remediation techniques.

Course Modules

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

Scope

- Duration: 5 days
- Format: Lecture, demo and hands-on labs
- Certification Exam (Not Included):
  - CompTIA PenTest: Exam PT0-002

Objectives

This course can benefit you in two ways. If you intend to pass the CompTIA PenTest+ (Exam PT0-002) certification examination, this course can be a significant part of your preparation. But certification is not the only key to professional success in the field of server management. Today's job market demands individuals have demonstrable skills, and the information and activities in this course can help you build your penetration testing skill set so that you can confidently perform your duties in a security consultant or penetration tester job role.

On course completion, you will be able to:

- Scope organizational/customer requirements.
- Define the rules of engagement.
- Footprint and gather intelligence.
- Evaluate human and physical vulnerabilities.
- Prepare the vulnerability scan.
- Scan logical vulnerabilities.
- Analyze scan results.
- Avoid detection and cover tracks.
- Exploit the LAN and cloud.
- Test wireless networks.
- Target mobile devices.
- Attack specialized systems.
- Perform web application-based attacks.
- Perform system hacking.
- Script and software development.
- Leverage the attack: pivot and penetrate.
- Communicate during the PenTesting process.
- Summarize report components.
- Recommend remediation.
- Perform post-report delivery activities.

Target Audience

The Official CompTIA PenTest+ Guide (Exam PT0-002) is the primary course you will need to take if your job responsibilities include planning and scoping, information gathering and vulnerability scanning, attacks and exploits, reporting and communication, and tools and codeanalysis.

Prerequisites

- Network+, Security+ or equivalent knowledge.
- Minimum of 3-4 years of hands-on information security or related experience.