CompTIA PenTest+

Course Description

CompTIA is a not-for-profit trade association with the purpose of advancing the interests of IT professionals and IT channel organizations; its industry-leading IT certifications are an important part of that mission. CompTIA's PenTest+ Certification is an intermediate-level certification designed for professionals with three to four years of hands-on experience working in a security consultant or penetration tester job role.

This exam will certify 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 and produce written reports containing proposed remediation techniques, effectively communicate results to the management team, and provide practical recommendations.

Course Duration:

5 days

Prerequisites:

To ensure your success in this course, you should have basic IT skills comprising three to four years of hands-on experience working in a performing penetration test, vulnerability assessments, and code analysis. CompTIA Network+ certification, Security+ certification, or the equivalent knowledge is strongly recommended

Objectives:

After you successfully complete this course, expect to 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

Course Outline:

- Scoping Organizational/Customer Requirements
- Defining the Rules of Engagement
- Footprinting and Gathering Intelligence
- Evaluating Human and Physical Vulnerabilities
- Preparing the Vulnerability Scan
- Scanning Logical Vulnerabilities
- Analyzing Scanning Results
- Avoiding Detection and Covering Tracks
- Exploiting the LAN and Cloud
- Testing Wireless Networks
- Targeting Mobile Devices
- Attacking Specialized Systems
- Web Application-Based Attacks
- Performing System Hacking
- Scripting and Software Development
- Leveraging the Attack: Pivot and Penetrate
- Communicating During the PenTesting Process
- Summarizing Report Components
- Recommending Remediation
- Performing Post-Report Delivery Activities

Who Should Attend

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 code analysis. You can take this course to prepare for the CompTIA PenTest+ (Exam PT0- 002) certification examination.