CompTIA PenTest+

Course Duration: 5 Days
Exam Reference: PTO-003

Course Overview

CompTIA PenTest+ is for cybersecurity professionals tasked with penetration testing and security consulting. It is the only product on the market covering artificial intelligence (AI), hands-on inventory, scanning and analysis, attacks, lateral movement, as well as planning, scoping, and vulnerability management. Unlike other penetration testing exams that only cover a portion of stages, CompTIA PenTest+ uses both performance-based and knowledge-based questions to ensure all stages are mastered.

CompTIA PenTest+ requires a candidate to demonstrate key pen testing skills for all attack surfaces, including the cloud, web apps, APIs, IoT, on-premises and hybrid network environments.

Prerequisites

It is highly recommended to have Network+, Security+ or equivalent knowledge, as well as 3–4 years in a penetration tester job role.

APPLIED TECHNOLOGY ACADEMY

Contact Us

800.674.3550

2151 W. Hillsboro Blvd., Ste 210
Deerfield Beach, FL 33442

Connect With Us

CompTIA PenTest+

Course Objectives

The CompTIA PenTest+ will certify the successful candidate has the knowledge and skills required to plan and scope a penetration testing engagement within compliance requirements, conduct enumeration and reconnaissance activities, analyze vulnerabilities, launch attacks, exfiltrate data and produce a written report with remediation techniques.

After taking this course, you will have learned:

Engagement Management
Includes updated techniques emphasizing scoping and organizational/customer requirements, governance, risk and compliance concepts, reporting, communication, remediation recommendations and demonstrating an ethical hacking mindset.

Attacks and Exploits
Includes new techniques to analyze targets, select the best approach, and perform network attacks, wireless attacks, application-based attacks, and cloud attacks. Learn about artificial intelligence (AI) attacks and scripting automation.

Reconnaissance and Enumeration
Expanded coverage of information gathering, enumeration, and passive/active reconnaissance, with the goal of conducting inventory. Includes identifying scripts and explaining use cases of various scripting languages (scripting or coding is not required).

Post-exploitation and Lateral Movement
Additional focus on maintaining persistence, lateral movement, staging, exfiltration and post-exploitation, including clean up and restoration activities.

Vulnerability Discovery and Analysis
Updated skills that cover vulnerability scanning tools, analysis, management, and physical security weaknesses.

CompTIA PenTest+

Course Outline

- Module 1: Penetration Testing: Before You Begin
- Module 2: Applying Pre-Engagement Activities
- Module 3: Reconnaissance and Enumeration
- Module 4: Scanning and Identifying Vulnerabilities
- Module 5: Conducting Pentest Attacks
- Module 6: Web-Based Attacks
- Module 7: Enterprise Attacks
- Module 8: Specialized Attacks
- Module 9: Performing Penetration Testing Tasks
- Module 10: Reporting and Recommendations
- Module 11: Practice Exams, Interactive Activities, and Labs