THE LEARNING CENTER
A TECHNICAL TRAINING INSTITUTION

CompTIA PenTest+ assesses the most up-to-date penetration testing, and vulnerability assessment and management skills necessary to determine the resiliency of the network against attacks. The CompTIA PenTest+ certification exam will verify successful candidates have 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

CompTIA PenTest+ is compliant with ISO 17024 standards and approved by the US DoD to meet directive 8140/8570.01-M requirements.

The new CompTIA PenTest+ PT0-002 exam is available as of October 28, 2021

Our unique model follows a streamlined approach to workforce development and skills attainment

Assess: Assess each student to determine existing skill sets

Educate: Deliver goal-specific training utilizing all delivery modalities

Mentor: Expose students to instructors and mentors with front-line IT and cybersecurity experience

Certify: Certify students with the requisite hands-on skills to perform the tasks related to their functional roles

Validate: Validate student abilities through performance analytics and real-world exercises hosted on a cyber range

Exam Objectives: PT0-002

Planning and Scoping	14%
Information Gathering and Vulnerability Scanning	22%
Attacks and Exploits	30%
Reporting and Communication	18%
Tools and Code Analysis	16%

Course Outline:

Chapter 1: Introduction to Ethical Hacking and Penetration Testing
Chapter 2: Planning and Scoping a Penetration Testing Assessment
Chapter 3: Information Gathering and Vulnerability Scanning
Chapter 4: Social Engineering Attacks
Chapter 5: Exploiting Wired and Wireless Networks
Chapter 6: Exploiting Application-Based Vulnerabilities
Chapter 7: Cloud, Mobile, and IoT Security
Chapter 8: Performing Post-Exploitation Techniques
Chapter 9: Reporting and Communication
Chapter 10: Tools and Code Analysis

Included

40 hours of instructor-led training sessions
CompTIA authorized textbook and class materials
Practice questions and exam study tips