APPLIED TECHNOLOGY ACADEMY

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

CompTIA PenTest+ Training

CompTIA Authorized Training · Applied Technology Academy

Global cybercrime costs are expected to grow 15% over the next five years. Now more than ever, it is imperative that organizations prevent sensitive data from falling into the wrong hands. Updates to PenTest+ reflect newer pen testing techniques for the latest attack surfaces, including the cloud, hybrid environments, and web applications, as well as more ethical hacking concepts, vulnerability scanning, and code analysis.

LEVEL	DURATION	EXAM	EXPERIENCE	AVERAGE SALARY
Intermediate	**5 Days**	**PT0-003**	**3-4 years: Penetration testing**	**$112,000**

Course Overview

The CompTIA PenTest+ Certification Study Guide will prepare you to take the CompTIA PenTest+ exam by providing 100% coverage of the objectives and content examples listed on the syllabus, including how to:

- Plan and scope penetration tests
- Conduct passive reconnaissance
- Perform non-technical tests to gather information
- Conduct active reconnaissance
- Analyze vulnerabilities
- Penetrate networks
- Exploit host-based vulnerabilities
- Test applications
- Complete post-exploit tasks
- Analyze and report penetration test results

Course Outline

- **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**

800.674.3550
Info@AppliedTechAc.com
AppliedTechnologyAcademy.com

- **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**

Intended Audience

To ensure your success in this course, you should have:

Intermediate knowledge of information security concepts, including but not limited to identity and access management (IAM), cryptographic concepts and implementations, computer networking concepts and implementations, and common security technologies.

Practical experience in securing various computing environments, including small to medium businesses, as well as enterprise environments.

- Who should attend?
- Penetration Tester
- Vulnerability Tester
- Security Analyst (II)
- Vulnerability Assessment Analyst
- Network Security Operations
- Application Security Vulnerability

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.

Follow-On Courses

- EC-Council Certified Security Analyst
- EC-Council Certified Ethical Hacker (CEH)
- PEN-200 Penetration Testing with Kali Linux PWK/OSCP

Ready to enroll? Call 800.674.3550 or email Info@AppliedTechAc.com — private team cohorts, GSA MAS purchasing, military credentialing funding, VA GI Bill and VR&E and student financing available.