CO-PEN+

COMPTIA PENTEST+

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
5 Days	Intermediate	Cybersecurity	Instructor Led	NA

INTRODUCTION

As organisations scramble to protect themselves and their customers against privacy or security breaches, the ability to conduct penetration testing is an emerging skill set that is becoming ever more valuable to the organisations seeking protection, and ever more lucrative for those who possess these skills. In this course, you will be introduced to general concepts and methodologies related to pen testing, and you will work your way through a simulated pen test for a fictitious company.

The CompTIA PenTest+ certification requires a candidate to demonstrate the hands-on ability and knowledge to test devices in new environments such as the cloud and mobile, in addition to traditional desktops and servers. CompTIA PenTest+ joins CompTIA Cybersecurity Analyst (CySA+) at the intermediate-skills level of the cybersecurity career pathway as shown below. Depending on your course of study, PenTest+ and CySA+ can be taken in any order but typically follows the skills learned in Security+. While CySA+ focuses on defense through incident detection and response, PenTest+ focuses on offense through penetration testing and vulnerability assessment.

Although the two exams teach opposing skills, they are dependent on one another. The most qualified cybersecurity professionals have both offensive and defensive skills. Earn the PenTest+ certification to grow your career within the CompTIA recommended cybersecurity career pathway.

AUDIENCE PROFILE

Cybersecurity professionals involved in hands-on penetration testing to identify, exploit, report, and manage vulnerabilities on a network.

PREREQUISITES

Before attending this course, delegates must have achieved the following requirements:

- 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.

You can obtain this level of skills and knowledge by attending the CompTIA Security+ Certification Training. Individuals seeking the CompTIA PenTest+ certification should also have three to four years of hands-on experience performing penetration tests, vulnerability assessments, and vulnerability management.

COURSE OBJECTIVES

After completing the CompTIA PenTest+ course, delegates will have the skills and knowledge 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

COURSE OUTLINE

COURSE CONTENT

Lesson 1: Planning and Scoping Penetration Tests
- Introduction to Penetration Testing Concepts
- Plan a Pen Test Engagement
- Scope and Negotiate a Pen Test Engagement
- Prepare for a Pen Test Engagement

Lesson 2: Conducting Passive Reconnaissance
- Gather Background Information
- Prepare Background Findings for Next Steps

Lesson 3: Performing NonTechnical Tests
- Perform Social Engineering Tests
- Perform Physical Security Tests on Facilities

Lesson 4: Conducting Active Reconnaissance
- Scan Networks
- Enumerate Targets
- Scan for Vulnerabilities
- Analyze Basic Scripts

Lesson 5: Analyzing Vulnerabilities
- Analyze Vulnerability Scan Results
- Leverage Information to Prepare for Exploitation

Lesson 6: Penetrating Networks
- Exploit Network-Based Vulnerabilities
- Exploit Wireless and RFBased Vulnerabilities
- Exploit Specialized Systems

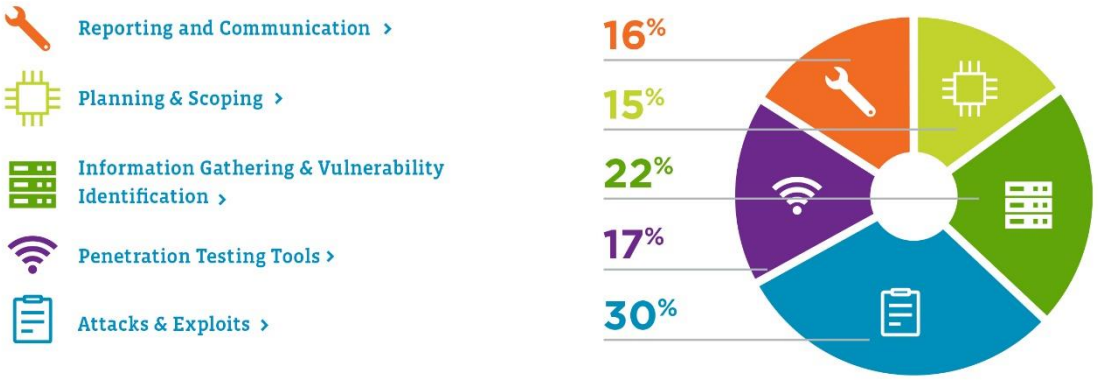
Lesson 7: Exploiting Host-Based Vulnerabilities
- Exploit Windows-Based Vulnerabilities
- Exploit *nix-Based Vulnerabilities

Lesson 8: Testing Applications
- Exploit Web Application Vulnerabilities
- Test Source Code and Compiled Apps

Lesson 9: Completing PostExploit Tasks
- Use Lateral Movement Techniques
- Use Persistence Techniques
- Use Anti-Forensics Techniques

Lesson 10: Analyzing and Reporting Pen Test Results
- Analyze Pen Test Data
- Develop Recommendations for Mitigation Strategies
- Write and Handle Reports
- Conduct Post-ReportDelivery Activities

SKILLS AND COMPETENCIES COVERED



ASSOCIATED CERTIFICATIONS & EXAM

This course is designed to prepare students to take the CompTIA PenTest+ PT0-001 Exam. Successfully passing this exam will result in the achievement of the CompTIA PenTest+ Certification.