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

COURSE CONTENT

Lesson 1: Scoping Organizational/Customer Requirements
- Define Organizational PenTesting
- Acknowledge Compliance Requirements
- Compare Standards and Methodologies
- Describe Ways to Maintain Professionalism

Lesson 2: Defining the Rules of Engagement
- Assess Environmental Considerations
- Outline the Rules of Engagement
- Prepare Legal Documents

Lesson 3: Foot printing and Gathering Intelligence
- Discover the Target
- Gather Essential Data
- Compile Website Information
- Discover Open-Source Intelligence Tools

Lesson 4: Evaluating Human and Physical Vulnerabilities
- Exploit the Human Psyche
- Summarize Physical Attacks
- Use Tools to Launch a Social Engineering Attack

Lesson 5: Preparing the Vulnerability Scan
- Plan the Vulnerability Scan
- Detect Defences
- Utilize Scanning Tools

Lesson 6: Scanning Logical Vulnerabilities
- Scan Identified Targets
- Evaluate Network Traffic
- Uncover Wireless Assets

Lesson 7: Analysing Scanning Results
- Discover Nmap and NSE
- Enumerate Network Hosts

Lesson 8: Avoiding Detection and Covering Tracks
- Evade Detection
- Use Steganography to Hide and Conceal
- Establish a Covert Channel

Lesson 9: Exploiting the LAN and Cloud
- Enumerating Hosts
- Attack LAN Protocols
- Compare Exploit Tools
- Explore Cloud-Based Attacks

Lesson 10: Testing Wireless Networks
- Discover Wireless Attacks
- Explore Wireless Tools
- Write and Handle Reports

Lesson 11: Testing Wireless Networks
- Recognize Mobile Device Vulnerabilities
- Launch Attacks on Mobile Devices
- Outline Assessment Tools for Mobile Devices

Lesson 12: Attacking Specialized Systems
- Identify Attacks on the IoT
- Recognize Other Vulnerable Systems
- Explain Virtual Machine Vulnerabilities

Lesson 13: Web Application-Based Attacks
- Recognize Web Vulnerabilities
- Launch Session Attacks
- Plan Injection Attacks
- Identify Tools

Lesson 14: Performing System Hacking
- System Hacking
- Use Remote Access Tools
- Analyze Exploit Code

Lesson 15: Scripting and Software Development
- Analyzing Scripts and Code Samples
- Create Logic Constructs
- Automate Penetration Testing

Lesson 16: Leveraging the Attack: Pivot and Penetrate
- Test Credentials
- Move Throughout the System
- Maintain Persistence

Lesson 17: Communicating During the PenTesting Process
- Define the Communication Path
- Communication Triggers
- Use Built-In Tools for Reporting

Lesson 18: Summarizing Report Components
- Identify Report Audience
- List Report Contents
- Define Best Practices for Reports

Lesson 19: Recommending Remediation
- Employ Technical Controls
- Administrative and Operational Controls
- Physical Controls

Lesson 20: Performing Post-Report Delivery Activities
- Post-Engagement Cleanup
- Follow-Up Actions

SKILLS AND COMPETENCIES COVERED

1. Planning and Scoping - 14%

2. Information Gathering and Vulnerability Scanning - 22%

3. Attacks and Exploits - 30%

4. Reporting and Communication - 18%

5. Tools and Code Analysis - 16%

ASSOCIATED CERTIFICATIONS & EXAM

This course is designed to prepare students to take the CompTIA PenTest+ PT0-002 Exam. Successfully passing this exam will result in the achievement of the CompTIA PenTest+ Certification.