



## COURSE OUTLINE

Course Name: CompTia PenTest+

DURATION	SKILLS LEVEL	DILIVERY METHOD	TRAINING CREDITS	TECHNOLOGY
5 Days	Intermediate	Instructor-Led	60	Cybersecurity

### Course Description:

The CompTIA PenTest+ will certify the successful candidate has the knowledge and skills required to plan and scope a penetration testing engagement including vulnerability scanning, understand legal and compliance requirements, analyze results, and produce a written report with remediation technique.

- 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.
- Successful candidates will have the intermediate skills required to customize assessment frameworks to effectively collaborate on and report findings.
- Candidates will also have the best practices to communicate recommended strategies to improve the overall state of IT security.

### Prerequisites:

- Network+, Security+ or equivalent knowledge.
- Minimum of 3-4 years of hands-on information security or related experience.
- While there is no required prerequisite, PenTest+ is intended to follow CompTIA Security+ or equivalent experience and has a technical, hands-on focus.

### Target Audience:

- CompTIA PenTest+ is for cybersecurity professionals tasked with penetration testing and vulnerability management.

## Learning Objectives:

What skills will you learn?

- **Planning and Scoping:** Explain the importance of planning and key aspects of compliance-based assessments.
- **Information Gathering & Vulnerability Identification:** Gather information to prepare for exploitation then perform a vulnerability scan and analyse results.
- **Attacks & Exploits:** Exploit network, wireless, application, and RF based vulnerabilities, summarize physical security attacks and perform post exploitation techniques.
- **Penetration Testing Tools:** Conduct information gathering exercises with various tools and analyse output and basic scripts (Limited to: Bash, Python, Ruby, PowerShell).
- **Reporting & Communication:** Utilize report writing and handling best practices explaining recommended mitigation strategies for discovered vulnerabilities.

## Course Outline

### Lesson 1: Planning and Scoping

- Explain the importance of planning for an engagement.
- Explain key legal concepts.
- Explain the importance of scoping an engagement properly.
- Explain the key aspects of compliance-based assessments.

### Lesson 2: Information Gathering and Vulnerability Identification

- Given a scenario, conduct information gathering using appropriate techniques.
- Given a scenario, perform a vulnerability scan.
- Given a scenario, analyse vulnerability scan results.
- Explain the process of leveraging information to prepare for exploitation.
- Explain weaknesses related to specialized systems.

### Lesson 3: Attacks and Exploits

- Compare and contrast social engineering attacks.
- Given a scenario, exploit network-based vulnerabilities.
- Given a scenario, exploit wireless and RF-based vulnerabilities.
- Given a scenario, exploit application-based vulnerabilities.
- Given a scenario, exploit local host vulnerabilities.
- Summarize physical security attacks related to facilities.
- Given a scenario, perform post exploitation techniques.

### Lesson 4: Penetration Testing Tools

- Given a scenario, perform post exploitation techniques.
  - Compare and contrast various use cases of tools.
  - Given a scenario, analyse tool output or data related to a penetration test.
  - Given a scenario, analyse a basic script (limited to Bash, Python, Ruby, and PowerShell).
-

## Lesson 5: Reporting and Communication

- Given a scenario, use report writing and handling best practices.
- Explain post-report delivery activities.
- Given a scenario, recommend mitigation strategies for discovered vulnerabilities.
- Explain the importance of communication during the penetration testing process.

## Associated Exam and Certification

This course will prepare students to take the CompTIA PenTest+ PTO-001 exam.

Successfully passing this exam will result in the attainment of the CompTIA PenTest+ certification.

## Exams and Certifications

## Notes and Annotations

## What is Next

---