COMPTIA PENTEST +

DURATION: 5 DAYS

COURSE OVERVIEW

As organizations 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 organizations 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 Pen Test+ 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 Pen Test+ joins CompTIA Cybersecurity Analyst (CySA+) at the intermediate-skills level of the cybersecurity career pathway as shown below. Depending on your course of study, Pen Test+ 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, Pen Test+ 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 Pen Test+ certification to grow your career within the CompTIA recommended cybersecurity career pathway.

TARGET AUDIENCE

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

COURSE OBJECTIVES

After completing this course you should be able to:

1. Explain the importance of planning and key aspects of compliance-based assessments.
2. Conduct information gathering exercises with various tools and analyses output and basic scripts (limited to: Bash, Python, Ruby, PowerShell).

3. Gather information to prepare for exploitation then perform a vulnerability scan and analyze results.
4. Utilize report writing and handling best practices explaining recommended mitigation strategies for discovered vulnerabilities.
5. Exploit network, wireless, application, and RF-based vulnerabilities, summarize physical security attacks, and perform post-exploitation techniques.

COURSE CONTENT

Planning and Scoping Penetration Tests

1. Introduction to Penetration Testing Concepts
2. Plan a Pen Test Engagement
3. Scope and Negotiate a Pen Test Engagement
4. Prepare for a Pen Test Engagement

Conducting Passive Reconnaissance

1. Gather Background Information
2. Prepare Background Findings for Next Steps

Performing Non-Technical Tests

1. Perform Social Engineering Tests
2. Perform Physical Security Tests on Facilities

Conducting Active Reconnaissance

1. Scan Networks
2. Enumerate Targets
3. Scan for Vulnerabilities
4. Analyze Basic Scripts

Analyzing Vulnerabilities

1. Analyze Vulnerability Scan Results
2. Leverage Information to Prepare for Exploitation

Penetrating Networks

1. Exploit Network-Based Vulnerabilities
2. Exploit Wireless and RF-Based Vulnerabilities
3. Exploit Specialized Systems

Exploiting Host-Based Vulnerabilities

1. Exploit Windows-Based Vulnerabilities
2. Exploit *Nix-Based Vulnerabilities

Testing Applications

1. Exploit Web Application Vulnerabilities
2. Test Source Code and Compiled Apps

Completing Post-Exploit Tasks

1. Use Lateral Movement Techniques
2. Use Persistence Techniques
3. Use Anti-Forensics Techniques

Analyzing and Reporting Pen Test Results

1. Analyze Pen Test Data
2. Develop Recommendations for Mitigation Strategies
3. Write and Handle Reports
4. Conduct Post-Report-Delivery Activities

Appendix A: Mapping Course Content to CompTIA Pen Test+ (Exam PT0-001) Solutions Glossary Index

COURSE PREREQUISITES

Attendees should meet the following prerequisites:

1. 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.
2. Practical experience in securing various computing environments, including small to medium businesses, as well as enterprise environments.
3. CompTIA Network + or CompTIA Security + or equivalent knowledge
4. Hands-on information security experience

TEST CERTIFICATION

Recommended as preparation for the following exams:

PT0-001 - CompTIA Pentest+ Certification

FOLLOW ON COURSES

The following courses are recommended for further study.

GK5867 - CompTIA CySA+ Cybersecurity Analyst