CompTIA PenTest+ Bootcamp

Length: 5 days
Format: Bootcamp
Time: Day

About This Course

CompTIA PenTest+ is the primary course you will need to take if your job responsibilities include penetration testing, vulnerability assessments and management within your organization. You can also take this course to prepare for the CompTIA PenTest+ certification examination. In this course, you will build on your knowledge of vulnerability identification, penetration testing tools, reporting and communication of mitigation strategies.

This primary goal of this course is to help each student pass the exam required to earn the PenTest+ certification. To do this, your knowledgeable instructor will blend hands-on labs with lecture and practice exams to prepare you to pass the certification exam. The practice exams identify knowledge gaps that the instructor will fill with customized, hands-on labs and tailored lectures. Our on-site testing center allows you to take the exam when you are ready.

To learn more about the course objectives and opportunities in the industry for PenTest+ certified professionals, view our PenTest+ Certification Info Session.

Click here to find your place on the CompTIA pathway.

Required Exams

Audience Profile

This course is designed for IT professionals who want to develop penetration testing skills to enable them to identify information-system vulnerabilities and effective remediation techniques for those vulnerabilities. Target students who also need to offer practical recommendations for action to properly protect information systems and their contents will derive those skills from this course.

This course is also designed for individuals who are preparing to take the CompTIA PenTest+ certification, or who plan to use PenTest+ as the foundation for more advanced security certifications or career roles. Individuals seeking this certification should have three to four years of hands-on experience performing penetration tests, vulnerability assessments, and vulnerability management.

Course Objectives

After completing this course, students will be able 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 pen test results.

Outline

Lesson 1: Planning and Scoping Penetration Tests * Topic A: Introduction to Penetration Testing Concepts
* Topic B: Plan a Pen Test Engagement
* Topic C: Scope and Negotiate a Pen Test Engagement
* Topic D: Prepare for a Pen Test Engagement

Lesson 2: Conducting Passive Reconnaissance * Topic A: Gather Background Information
* Topic B: Prepare Background Findings for Next Steps

Lesson 3: Performing Non-Technical Tests * Topic A: Perform Social Engineering Tests
* Topic B: Perform Physical Security Tests on Facilities

Lesson 4: Conducting Active Reconnaissance * Topic A: Scan Networks
* Topic B: Enumerate Targets
* Topic C: Scan for Vulnerabilities
* Topic D: Analyze Basic Scripts

Lesson 5: Analyzing Vulnerabilities * Topic A: Analyze Vulnerability Scan Results
* Topic B: Leverage Information to Prepare for Exploitation

Lesson 6: Penetrating Networks * Topic A: Exploit Network-Based Vulnerabilities
* Topic B: Exploit Wireless and RF-Based Vulnerabilities
* Topic C: Exploit Specialized Systems

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

Lesson 8: Testing Applications * Topic A: Exploit Web Application Vulnerabilities
* Topic B: Test Source Code and Compiled Apps

Lesson 9: Completing Post-Exploit Tasks * Topic A: Use Lateral Movement Techniques
* Topic B: Use Persistence Techniques
* Topic C: Use Anti-Forensics Techniques

Lesson 10: Analyzing and Reporting Pen Test Results * Topic A: Analyze Pen Test Data
* Topic B: Develop Recommendations for Mitigation Strategies
* Topic C: Write and Handle Reports
* Topic D: Conduct Post-Report-Delivery Activities