CompTIA PenTest+ Training Course

CompTIA PenTest+ is a certification that assesses intermediate penetration testing skills to identify, exploit, report, and manage vulnerabilities on a network.

SEC-202

Course Outcomes

Professional, practical, & hands-on live instructor-led training

Further your skills and graduate as a certified professional, with the skills, experience, and job-search know how to get your career started.

Start Today

Potential Career Tracks

Penetration Tester · Vulnerability Assessment Analyst · Security Consultant · Information Security Engineer · Cybersecurity Analyst · Network Security Specialist

Taught by Industry Veterans &
World Class Instructors

Introduction to CompTIA PenTest+

Course Overview

Intellectual Point's CompTIA PenTest+ training program is meticulously curated to equip you with the essential knowledge and practical competencies needed to excel as a penetration tester. This course prepares you for the CompTIA PenTest+ certification exam, aiming to validate your proficiency in identifying, exploiting, reporting, and managing vulnerabilities on a network. Uniting theory with extensive hands-on training, this course ensures that you not only understand penetration testing methodologies but also can execute them effectively in real-world scenarios.

Throughout, you will explore advanced concepts such as vulnerability identification, exploitation techniques, legal documentation, and ethical hacking practices. The course integrates practical labs and simulations to help you assert your skills in live environments, simulating real-world scenarios. By the end of the program, you'll be competent to perform comprehensive penetration testing and confidently apply your technical skills in a professional context.

Obtainable Skills

Ethical Hacking Techniques · Vulnerability Assessment · Network Pentesting · Security Report Writing · Exploit Development · Risk Analysis · Threat Analysis · Security Controls Assessment · Incident response

Course Insights

Audience Profile

This CompTIA PenTest+ course is tailored for IT and cybersecurity professionals interested in specializing in network penetration testing and vulnerability assessment. The ideal candidates include security analysts, systems administrators, network engineers, and anyone striving to strengthen their cybersecurity defenses and validate their skills with a respected industry credential. Emerging professionals with a background in IT or computer science and a keen interest in ethical hacking and cybersecurity will also find great value in this course. It's particularly advantageous for individuals seeking to advance into more specialized cybersecurity roles or augment their existing security expertise.

Course Outcomes

By the end of this course, participants will:

1. Conduct effective penetration testing using specified methodologies and standard practices.
2. Accurately identify, prioritize, and report vulnerabilities following industry standards.
3. Develop and perform exploits, ensuring a practical understanding of threat impacts.
4. Generate comprehensive documentation reports that reflect penetration testing results.
5. Pass the CompTIA PenTest+ certification exam, reinforcing your professional value in cybersecurity.

Module by Module Learning *Outline*

6 Modules

Module 1: Introduction to Penetration Testing

Learning Objectives:

- Understand the role and objectives of penetration testing in cybersecurity.
- Get familiarized with the CompTIA PenTest+ certification exam structure and objectives.

Topics Covered

Fundamentals of Penetration Testing:

- Definition and purpose of penetration testing.
- Overview of penetration testing methodologies.

CompTIA PenTest+ Certification Overview:

- Exam objectives and key competencies.
- Preparing effectively for the PenTest+ exam.

Module 2: Pre-Engagement and Planning

Learning Objectives:

- Learn how to plan and scope a penetration test.
- Understand legal and compliance considerations in penetration testing.

Topics Covered

Penetration Test Scope and Objectives Setting:

- Determining goals and required resources.
- Defining scope: Networks, applications, and systems.

Legal and Compliance Frameworks:

- Legal implications of penetration testing.
- Compliance standards and ethical guidelines.

Module 3: Information Gathering and Vulnerability Identification

Learning Objectives:

- Master techniques for effective information gathering and vulnerability assessment.
- Utilize tools to identify and prioritize vulnerabilities.

Topics Covered

Open Source Intelligence (OSINT) Techniques:

- Gathering data from publicly available sources.
- Analyzing OSINT data for vulnerabilities.

Vulnerability Scanning Tools and Techniques:

- Utilizing automated scanning tools.
- Manual verification of identified vulnerabilities.

Module 4: Exploitation Techniques

Learning Objectives:

- Explore various exploitation techniques to identify potential threats.
- Develop skills in exploit development and payload creation.

Topics Covered

Exploitation Frameworks and Tools:

- Using Metasploit and other tools.
- Developing custom exploits.

Creating and Deploying Payloads:

- Understanding payload types and delivery mechanisms.
- Testing payload effectiveness in controlled environments.

Module 5: Post-Exploitation and Reporting

Learning Objectives:

- Understand post-exploitation techniques and their importance.
- Develop skills in generating comprehensive penetration testing reports.

Topics Covered

Post-Exploitation Tactics and Techniques:

- Persistence, escalation, and data exfiltration.
- Maintaining access and covering tracks.

Security Report Writing:

- Structuring and writing comprehensive reports.
- Presenting findings to non-technical stakeholders.

Module 6: Hands-On Labs and Real-World Simulations

Learning Objectives:

- Apply penetration testing methodologies in practical, hands-on labs.
- Simulate real-world scenarios to test skills and knowledge.

Topics Covered

Interactive Lab Scenarios:

- Setting up and executing penetration tests in virtual environments.
- Analyzing and acting on lab results.

Real-World Simulation Exercises:

- Comprehensive simulation of a penetration test.
- Reporting and reflection on simulated penetration testing exercises.