CyberGate ACADEMY

CPT

COMPTIA PENTEST+ COURSE

Course Overview

CompTIA PenTest+ is the most comprehensive cybersecurity exam covering all red team activities and is designed for cybersecurity professionals tasked with penetration testing and vulnerability management. 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. The CompTIA PenTest+ certification exam will verify successful candidates have the knowledge and skills required to:

- Plan and scope a penetration testing engagement.
- Understand legal and compliance requirements.
- Perform vulnerability scanning and penetration testing using appropriate tools and
- Techniques, and then analyze the results.
- Produce a written report containing proposed remediation techniques, effectively.
- Communicate results to the management team, and provide practical recommendations.

Course Duration

5 Days (40 Hours).

Target Audience

- Individuals seeking a career in cybersecurity.
- IT professionals wanting to enhance their skills.
- Security specialists aiming for an advanced certification.
- Network administrators seeking knowledge in penetration testing.
- Cybersecurity students desiring an industry-recognised certification.
- Professionals aiming to handle system vulnerabilities and threats effectively.
- Security Consultant.
- Cloud Penetration Tester.
- Web App Penetration Tester.
- Cloud Security Specialist.
- Network & Security Specialist.

During this course you should learn

After completing CompTIA Pentest+ (PT0-002) certification training, an individual can acquire skills in multiple areas like planning and scoping a penetration testing assessment, conducting passive and active reconnaissance, analyzing vulnerabilities, understanding legal and compliance requirements, and effectively reporting and communicating results. They will also learn how to utilize various penetration testing tools and techniques, understand and exploit network-based, wireless, application-based, and cryptographic vulnerabilities, and apply appropriate mitigation strategies.

The learning objectives of the CompTIA Pentest+ (PT0-002) course are to equip students with the essential skills and knowledge to carry out penetration testing and vulnerability management. Students will understand how to plan and scope an assessment, understand legal and compliance requirements, perform vulnerability scanning and penetration testing using appropriate tools and techniques, and effectively analyze results. The course aims to prepare students to manage vulnerabilities in a professional context, thus enabling them to protect an organization's IT infrastructure from cyber threats, thereby helping maintain data integrity, confidentiality, and availability.

Course Content

Module 1: Scoping Organizational/Customer Requirements.

Module 2: Defining the Rules of Engagement.

Module 3: Footprinting and Gathering Intelligence.

Module 4: Evaluating Human and Physical Vulnerabilities.

Module 5: Preparing the Vulnerability Scan.

Module 6: Scanning Logical Vulnerabilities.

Module 7: Analyzing Scanning Results.

Module 8: Avoiding Detection and Covering Tracks.

Module 9: Exploiting the LAN and Cloud.

Module 10: Testing Wireless Networks.

Module 11: Targeting Mobile Devices.

Module 12: Attacking Specialized Systems.

Module 13: Web Application-Based Attacks.

Module 14: Performing System Hacking.

Module 15: Scripting and Software Development.

Module 16: Leveraging the Attack: Pivot and Penetrate.

Module 17: Communicating During the PenTesting Process.

Module 18: Summarizing Report Components.

Module 19: Recommending Remediation.

Module 20: Performing Post-Report Delivery Activities.

Prerequisites

Attendees should meet the following prerequisites:

- 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.
- CompTIA Network + or CompTIA Security + or equivalent knowledge
- Hands-on information security experience

Recommended prerequisites:

- G005 - CompTIA Network+
- G013 - CompTIA Security+

Course Agenda

Day 1	Module 1: Scoping Organizational/Customer Requirements Module 2: Defining the Rules of Engagement Module 3: Footprinting and Gathering Intelligence Module 4: Evaluating Human and Physical Vulnerabilities
Day 2	Module 5: Preparing the Vulnerability Scan Module 6: Scanning Logical Vulnerabilities Module 7: Analyzing Scanning Results Module 8: Avoiding Detection and Covering Tracks
Day 3	Module 9: Exploiting the LAN and Cloud Module 10: Testing Wireless Networks Module 11: Targeting Mobile Devices Module 12: Attacking Specialized Systems
Day 4	Module 13: Web Application-Based Attacks Module 14: Performing System Hacking Module 15: Scripting and Software Development Module 16: Leveraging the Attack: Pivot and Penetrate
Day 5	Module 17: Communicating During the PenTesting Process Module 18: Summarizing Report Components Module 19: Recommending Remediation Module 20: Performing Post-Report Delivery Activities

Technical Requirement

1. Laptop with minimum 8GB Ram.
2. Connected Monitor for iLabs.
3. Hi speed Internet Connection as All the labs it will be accessed through EC-Council Cloud.

Exam Voucher Validity

It will be valid for 12month starting from the last day of the course.

Certification Expiry

It will be valid for 3 years.

CyberGate ACADEMY

YOUR TRUSTED DEFENDERS

ADDRESS

CyberGate Academy
ADPOLY, MBZ City

WEB

academy@cybergate.tech
training@cybergate.tech