# CompTIA PenTest+ Certification Prep Training

Duration: **5 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

## Overview

**Master penetration testing, vulnerability assessment, and ethical hacking techniques while preparing for the CompTIA PenTest+ (PT0-003) certification exam.**

The **CompTIA PenTest+ Certification Prep Course** is a comprehensive hands-on cybersecurity training program designed to help professionals successfully prepare for the **CompTIA PenTest+ (PT0-003)** certification exam.

This intensive course develops the mindset and technical skills required of modern**penetration testers**, enabling participants to perform real-world offensive security assessments across multiple IT environments.

Throughout the training, learners gain practical experience in:

- **Penetration testing**
- **Vulnerability assessment**
- **Ethical hacking**
- **Reconnaissance**
- **Exploit techniques**
- **Security reporting**

The course focuses on the five core domains covered in the PT0-003 certification exam:

- **Planning and Scoping**
- **Information Gathering and Vulnerability Identification**
- **Attacks and Exploits**
- **Reporting and Communication**
- **Tools and Code Analysis**

Participants will explore network, host-based, cloud, wireless, mobile, and web application attacks while learning to identify vulnerabilities, exploit weaknesses, maintain persistence, and communicate findings professionally.

The training also emphasizes **ethical hacking principles**, **legal compliance**, and responsible security testing practices aligned with industry standards.

This program is ideal for professionals pursuing careers in**penetration testing**, **red teaming**, **security consulting**, or advanced **cybersecurity operations**.

## Prerequisites

Participants should have intermediate knowledge of:

- **Identity and Access Management (IAM)**
- Cryptography fundamentals
- Computer networking
- Security technologies
- Enterprise security environments

BILGINÇ IT Academy

info@bilginc.com

bilginc.com


- System and network security practices

## Who Should Attend

This course is ideal for:

- **Penetration Testers**
- **Vulnerability Analysts**
- **Security Consultants**
- **Red Team Members**
- **SOC Analysts**
- **Cybersecurity Specialists**
- **Network Security Engineers**
- **Ethical Hackers**

This training is especially valuable for cybersecurity professionals seeking to advance into**offensive security** and **ethical hacking** roles.

## What You Will Learn

Participants will learn how to:

- Plan and scope penetration tests
- Apply legal and ethical security requirements
- Perform active and passive reconnaissance
- Identify and validate vulnerabilities
- Conduct network, host, web, and cloud attacks
- Use professional **vulnerability scanning tools**
- Perform persistence and lateral movement activities
- Create professional penetration testing reports
- Recommend remediation strategies

## Outline

### 1. Scoping Organizational / Customer Requirements

- Penetration testing scope definition
- Engagement planning
- Requirement analysis

### 2. Rules of Engagement

- Legal and ethical considerations
- Authorization processes

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com


- Engagement guidelines

## 3. Footprinting and Gathering Intelligence

- OSINT techniques
- Reconnaissance methodologies
- Intelligence gathering strategies

## 4. Evaluating Human and Physical Vulnerabilities

- Human-based attack vectors
- Physical security assessments
- Social engineering risks

## 5. Preparing the Vulnerability Scan

- Vulnerability assessment preparation
- Scanner configuration

## 6. Scanning Logical Vulnerabilities

- Network and host scanning
- Vulnerability identification techniques

## 7. Analyzing Scanning Results

- Scan analysis
- False positive validation
- Risk assessment

## 8. Avoiding Detection and Covering Tracks

- Detection evasion techniques
- Operational security
- Log manipulation

## 9. Exploiting the LAN and Cloud

- Network exploitation
- Cloud penetration testing
- Internal attack techniques

## 10. Testing Wireless Networks

- Wireless security testing
- Wi-Fi attack methodologies
- Wireless vulnerability analysis

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com


## 11. Targeting Mobile Devices

- Mobile device security
- Mobile penetration testing
- Mobile exploit techniques

## 12. Attacking Specialized Systems

- IoT security testing
- Embedded system attacks
- Specialized system vulnerabilities

## 13. Web Application-Based Attacks

- Web application security
- **OWASP Top 10**
- Web exploitation techniques

## 14. Performing System Hacking

- Host exploitation
- Privilege escalation
- System compromise methods

## 15. Scripting and Software Development

- Security scripting
- Automation tools
- Exploit development fundamentals

## 16. Leveraging the Attack: Pivot and Penetrate

- Pivoting techniques
- Lateral movement
- Advanced exploitation

## 17. Communicating During the PenTesting Process

- Technical communication
- Stakeholder management
- Security reporting communication

## 18. Summarizing Report Components

- PenTest reporting standards
- Executive summaries
- Technical documentation

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com


## 19. Recommending Remediation

- Security improvement recommendations
- Risk mitigation strategies

## 20. Performing Post-Report Delivery Activities

- Post-engagement activities
- Follow-up validation
- Security reassessment