CompTIA PenTest+ Certification Prep Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

Penetration testing, vulnerability assessment ve ethical hacking alanlarında uzmanlaşarak CompTIA PenTest+ (PT0-003) sertifikasına hazırlanın.

CompTIA PenTest+ Certification Prep Course, katılımcıları **CompTIA PenTest+ (PT0-003)** sınavına hazırlamak için tasarlanmış kapsamlı ve uygulamalı bir siber güvenlik eğitim programıdır.

Bu eğitim, profesyonel bir **penetration tester** bakış açısı kazandırarak katılımcıların gerçek dünya saldırı senaryoları üzerinde çalışmasını sağlar. Eğitim boyunca öğrenciler; **penetration testing**, **vulnerability management**, **ethical hacking**, **reconnaissance**, **exploit development** ve **security reporting** süreçlerini uygulamalı laboratuvarlarla deneyimler.

Program, CompTIA PenTest+ sınavının kapsadığı beş temel alanı detaylı şekilde ele almaktadır:

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

Katılımcılar; ağ sistemleri, web uygulamaları, cloud ortamları ve mobil cihazlar üzerinde güvenlik açıklarını analiz etmeyi, exploit tekniklerini uygulamayı ve bulguları profesyonel raporlarla sunmayı öğrenir.

Eğitim aynı zamanda **etik hacking prensipleri**, **hukuki gereklilikler** ve modern siber güvenlik standartları konusunda da güçlü bir temel sağlar.

Bu program; **penetration tester**, **red team specialist**, **vulnerability analyst** veya **security consultant** olmak isteyen profesyoneller için ideal bir kariyer geliştirme fırsatı sunmaktadır.

Prerequisites

Katılımcıların aşağıdaki konularda orta seviyede bilgi sahibi olması önerilir:

- **Identity and Access Management (IAM)**
- Kriptografi temelleri
- Bilgisayar ağları
- Güvenlik teknolojileri
- Enterprise güvenlik ortamları
- Sistem ve ağ güvenliği deneyimi

CompTIA PenTest+ Certification Prep Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Who Should Attend

Bu eğitim aşağıdaki profesyoneller için idealdir:

- **Penetration Tester**
- **Vulnerability Analyst**
- **Security Consultant**
- **Red Team Member**
- **SOC Analyst**
- **Cybersecurity Specialist**
- **Network Security Engineer**
- **Ethical Hacker**

Bu program özellikle **offensive security**, **ethical hacking** ve **penetration testing** alanlarında uzmanlaşmak isteyen siber güvenlik profesyonelleri için uygundur.

What You Will Learn

Eğitim sonunda katılımcılar şunları öğrenir:

- **Penetration test planlama ve scoping süreçleri**
- Hukuki ve etik güvenlik gerekliliklerini uygulamak
- Active ve passive reconnaissance teknikleri
- Güvenlik açıklarını analiz etmek ve doğrulamak
- Ağ, sistem, web uygulaması ve cloud saldırıları gerçekleştirmek
- **Vulnerability scanning** araçlarını kullanmak
- Persistence ve lateral movement teknikleri
- Profesyonel penetration test raporları hazırlamak
- Remediation önerileri geliştirmek

Outline

1. Scoping Organizational / Customer Requirements

- Penetration test gereksinimlerini belirleme
- Scope yönetimi
- Engagement planning

2. Rules of Engagement

- PenTest kuralları
- Hukuki ve etik gereklilikler
- Yetkilendirme süreçleri

3. Footprinting and Gathering Intelligence

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Information gathering teknikleri
- OSINT süreçleri
- Reconnaissance yöntemleri

4. Evaluating Human and Physical Vulnerabilities

- İnsan kaynaklı güvenlik açıkları
- Fiziksel güvenlik analizleri
- Social engineering riskleri

5. Preparing the Vulnerability Scan

- Vulnerability assessment hazırlığı
- Tarama araçları yapılandırması

6. Scanning Logical Vulnerabilities

- Ağ ve sistem taramaları
- Güvenlik açığı tespit yöntemleri

7. Analyzing Scanning Results

- Scan sonuçlarını yorumlama
- False positive analizi
- Risk değerlendirmesi

8. Avoiding Detection and Covering Tracks

- Detection avoidance teknikleri
- Log manipulation
- Operational security

9. Exploiting the LAN and Cloud

- Network exploitation
- Cloud penetration testing
- Internal network attacks

10. Testing Wireless Networks

- Wireless security testing
- Wi-Fi saldırı teknikleri
- Wireless vulnerability analysis

11. Targeting Mobile Devices

- Mobil cihaz güvenliği
- Mobile penetration testing
- Mobile exploit teknikleri

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

12. Attacking Specialized Systems

- IoT ve specialized system saldırıları
- Embedded systems security

13. Web Application-Based Attacks

- Web application security
- OWASP Top 10
- Web exploit teknikleri

14. Performing System Hacking

- Host exploitation
- Privilege escalation
- System compromise teknikleri

15. Scripting and Software Development

- Security scripting
- Automation tools
- Exploit development basics

16. Leveraging the Attack: Pivot and Penetrate

- Pivoting teknikleri
- Lateral movement
- Advanced exploitation

17. Communicating During the PenTesting Process

- Teknik iletişim
- Stakeholder management
- Incident communication

18. Summarizing Report Components

- PenTest raporlama standartları
- Executive summary hazırlama
- Teknik rapor yazımı

19. Recommending Remediation

- Güvenlik iyileştirme önerileri
- Risk azaltma stratejileri

20. Performing Post-Report Delivery Activities

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Post-engagement süreçleri
- Follow-up değerlendirmeleri
- Security validation