# CEH - Certified Ethical Hacker v13 Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

## Overview

**Certified Ethical Hacker (CEH)**, dünya çapında en çok tanınan **etik hackleme** sertifikasıdır ve siber güvenlik profesyonelleri için endüstri standardını belirler.
Bu yeni sürüm — **CEH v13** — yapay zekâ entegrasyonları, bulut tabanlı laboratuvarlar ve güncel tehdit senaryolarıyla **tamamen yeniden tasarlanmıştır.**

CEH v13, katılımcılara **saldırgan bakış açısıyla düşünmeyi**, güvenlik açıklarını tespit etmeyi, ve bu açıkları **etik kurallar çerçevesinde test ederek** organizasyonların savunma kapasitesini güçlendirmeyi öğretir.

Bu eğitim, **gerçek siber saldırı ortamlarını simüle eden Cyber Range** altyapısıyla desteklenir ve katılımcılara hem teorik hem pratik olarak **profesyonel sızma testi (penetration testing)** becerisi kazandırır.

### Neden CEH v13?

CEH v13, klasik etik hackleme eğitimlerinin ötesine geçer:

- **AI Destekli Saldırı Simülasyonları:** Yapay zekâ ile güçlendirilmiş analiz ve saldırı senaryoları
- **Cloud Range Laboratuvarları:** AWS, Azure, GCP ortamlarında pratik güvenlik testleri
- **Gerçek Zamanlı Zafiyet Analizi:** Canlı sistemlerde savunma ve istismar uygulamaları
- **Güncel Siber Tehdit Kapsamı:** Ransomware, APT, Zero-Day, Fileless Malware
- **İleri Seviye Sınav Sistemi:** CEH Knowledge + Practical sınavları (toplam 10 saat)

**Certified Ethical Hacker (CEH) v13**, etik hacker'ların, sızma testi uzmanlarının ve siber güvenlik mühendislerinin
global standartta profesyonel becerilerini kanıtladığı **endüstri lideri sertifikasyon programıdır.**

Bu eğitimi tamamlayanlar, yalnızca **bilgiyi değil uygulamayı** da ustalaşır:

- Modern saldırı tekniklerini anlar,
- Sistemleri analiz eder,
- Savunma stratejileri geliştirir,
- Ve global geçerliliğe sahip CEH unvanını taşır.

**Bilginç IT Academy**, **EC-Council'in Resmî Yetkili Eğitim Ortağı (Accredited Training Partner)** olarak, dünya genelinde EC-Council onaylı siber güvenlik eğitimlerini ve sertifikasyon programlarını sunmaktadır.

# CEH - Certified Ethical Hacker v13 Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

## Prerequisites

Bu eğitime katılmadan önce önerilen bilgi birikimi:

- Temel ağ bilgisi (TCP/IP, portlar, servisler, router, switch)
- Windows ve Linux işletim sistemlerinde temel seviyede deneyim
- Temel bilgi güvenliği ve siber tehdit farkındalığı

CEH v13, hem **siber güvenlik kariyerine başlayanlar** hem de **deneyimli güvenlik profesyonelleri** için uygundur.

## Who Should Attend

- Siber Güvenlik Uzmanları
- Ağ Güvenliği Mühendisleri
- Sistem Yöneticileri ve Mühendisleri
- Penetrasyon Test Uzmanları
- Bilgi Güvenliği Analistleri
- Risk, Tehdit ve Zafiyet Değerlendirme Uzmanları
- Siber Güvenlik Yöneticileri
- CEH sertifikasyonunu hedefleyen profesyoneller

## What You Will Learn

Bu eğitimi tamamlayan katılımcılar:

- Etik hackleme metodolojisini (Reconnaissance → Scanning → Gaining Access → Maintaining Access → Covering Tracks) etkin şekilde uygular.
- Güvenlik açıklarını yasal çerçevede test edebilmek için gerekli araçları (Nmap, Metasploit, Burp Suite, Wireshark vb.) kullanır.
- Zararlı yazılım türlerini (Trojan, Worm, Ransomware, APT) analiz eder.
- Web uygulamaları, veritabanları ve bulut altyapılarındaki zafiyetleri tespit eder.
- DDoS, SQL Injection, XSS, Phishing ve Social Engineering saldırılarını simüle eder.
- IDS/IPS, antivirüs ve güvenlik duvarlarını atlatma tekniklerini uygular.
- Şifreleme, PKI, VPN ve güvenli iletişim protokollerini uygular.
- Yapay zekâ destekli saldırı tespiti ve otomatik istismar sistemleri ile çalışır.
- CEH Knowledge ve CEH Practical sınavlarına eksiksiz hazırlanır.

# CEH - Certified Ethical Hacker v13 Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

## Outline

### Etik Hackleme Temelleri

- Etik hacklemenin tanımı, kapsamı ve yasal sınırlar
- Siber güvenlik çerçeveleri (ISO 27001, NIST, GDPR)
- Hacker türleri ve saldırı motivasyonları

### Keşif ve Bilgi Toplama (Reconnaissance)

- Açık kaynak istihbaratı (OSINT)
- DNS sorgulama, Whois, e-posta izleme
- Ağ tarama araçları (Nmap, Angry IP Scanner)

### Tarama ve Sayım (Scanning & Enumeration)

- Port tarama teknikleri
- Banner grabbing
- NetBIOS, SNMP, LDAP sayımı

### Sistem Hackleme (System Hacking)

- Parola saldırıları ve parola kırma teknikleri
- Yetki yükseltme (Privilege Escalation)
- Geri kapı (Backdoor) oluşturma
- Dosya gizleme (Steganography)

### Zararlı Yazılım Tehditleri (Malware Threats)

- Trojan, virüs, worm ve rootkit analizi
- Fileless malware tespiti
- Anti-forensics teknikleri

### Sosyal Mühendislik ve Kimlik Avı (Phishing)

- Manipülasyon teknikleri
- Kurumsal phishing senaryoları
- Savunma stratejileri

# CEH - Certified Ethical Hacker v13 Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

### Hizmet Engelleme (DoS/DDoS) Saldırıları

- SYN flood, UDP flood, Smurf, HTTP Flood
- DDoS karşı önlemleri

### Oturum Ele Geçirme ve IDS Kaçışı

- Session hijacking
- Man-in-the-Middle (MITM) saldırıları
- IDS/IPS atlatma teknikleri

### Web Uygulama ve Veritabanı Güvenliği

- OWASP Top 10 zafiyetleri
- SQL Injection, Command Injection, CSRF
- Web sunucusu güvenliği

### Kablosuz, Mobil ve IoT Güvenliği

- Wi-Fi saldırıları (Evil Twin, WPA2 crack)
- Android/iOS istismarı
- IoT cihaz güvenliği ve analizi

### Bulut Güvenliği (Cloud Security)

- AWS, Azure, GCP tehdit senaryoları
- Bulut kimlik yönetimi (IAM)
- Sanallaştırma güvenliği

### Kriptografi ve Güvenli İletişim

- Şifreleme algoritmaları (AES, RSA, ECC)
- Dijital imzalar, PKI, SSL/TLS
- VPN güvenliği

### Yapay Zekâ Destekli Etik Hackleme (AI-Augmented Hacking)

- AI tabanlı saldırı otomasyonu
- Zafiyet tespiti için makine öğrenmesi
- AI ile sızma testi simülasyonları

# CEH - Certified Ethical Hacker v13 Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

## Sınavlar ve Değerlendirmeler

Eğitim sonrasında iki EC-Council sertifikasyon değerlendirmesi bulunmaktadır:

- **CEH Knowledge Exam:** 125 çoktan seçmeli soru ve 4 saatlik sınav süresi
- **CEH Practical Exam:** 20 senaryo tabanlı uygulama ve 6 saatlik sınav süresi

## Uygulamalı Laboratuvarlar (Hands-On)

- 100+ **Cyber Range** tabanlı uygulama
- Gerçek güvenlik açıkları içeren sanal hedef sistemler
- OWASP Top 10 exploit senaryoları
- **AI destekli otomatik saldırı simülasyonları**
- Gerçek ağ trafiği analizi (Wireshark, Snort, Splunk)