

# Certified Ethical Hacker v10 (Bundle)

Learn via: **Classroom / Virtual Classroom / Online**

Duration: **5 Gün**

## **Overview**

Sertifikalı Etik Bilgisayar Korsanı (CEH), hedef sistemlerdeki zayıflıkları ve savunmasız noktaları nasıl arayacağını bilen ve anlayan ve kötü niyetli bir bilgisayar korsanı ile aynı bilgileri ve araçları, hedef sistem(ler)in güvenlik özelliklerini değerlendirmek amacıyla yasal ve meşru bir şekilde kullanan becerikli bir profesyoneldir. CEH sertifikası ile kişilerin tedarikçi bağımsız bir bakış açısıyla Etik Bilgisayar Korsanlığında belirli bir ağ güvenliği alanındaki yetkinliği onaylanmaktadır.

CEH sertifikasının amacı:

- Profesyonel bilgi güvenliği uzmanlarının etik bilgisayar korsanlığı alanında onaylanmasına yönelik asgari standartları belirlemek ve yönetmek,
- Sertifikalı kişilerin asgari standartları yerine getirdiği veya aştığı konusunda kamuyu bilgilendirmek,
- Etik bilgisayar korsanlığını benzersiz ve kendi kendini düzenleyen bir meslek olarak desteklemektir.

CEHv10 eğitimi artık GCHQ Sertifikalı Eğitim (GCT) Programı kapsamındadır.

## **Neler dahil?**

CEHv10 eğitimimize dahil olanlar:

- CEHv10 (ANSI) & CEHv10 (ANSI) Sınav Makbuzu
- CEHv10 iLabs (Eğitim Sonrası CEHv10 Laboratuvar Erişimi - 6 ay)

*'Sertifikalı Etik Bilgisayar Korsanı (CEH) eğitiminde olağanüstü bir eğitim deneyimi yaşadım. Programın her bir noktası birçok bilgiye doluydu ve bana birçok farklı test teknikleri konusunda bilgi vermesinin yanı sıra muazzam bir bilgi Güvenliği kariyeri için gereken becerileri geliştirmeme de yardımcı oldu. Programın kaliteli içeriğini ve programa dahil olan sanal laboratuvarları çok sevdim. Bana göre programın teori ve pratik bölümleri birbirini mükemmel bir şekilde destekledi.'*

## **Jeffery Osuya, NHS'de Ağ Güvenliği Analisti**

### **Prerequisites**

Bu hızlandırılmış etik bilgisayar korsanı eğitimine katılmadan önce BT alanında en az iki yıllık iş deneyimine ve Linux ve/veya Unix konusunda temel bilgiye sahip olmalısınız. Ayrıca aşağıdaki konularda güçlü bir çalışma bilgisine sahip olmanızı da öneririz:

- TCP/IP
- Windows Server

Katılımcılar, kendilerine eğitmen birinci gününde verilecek olan oturum açma bilgilerini alana dek AT Konseyi CEHv10 eğitim malzemelerine erişim imkanına sahip olmayacaktır.

## **Who Should Attend**

Bu eğitime güvenlik görevlileri, denetçiler, güvenlik uzmanları, web sitesi yöneticileri, penetrasyon test edenler ve ağ altyapısının bütünlüğü konusunda endişe duyan bireyler katılabilir.

## **What You Will Learn**

- Footprinting
- Ağ Tarama
- Sayım
- Packet Sniffing

- Sosyal Mühendislik
- DoS / DDoS Saldırıları
- Oturum Çalma
- Web Sunucusu ve Web Uygulama Saldırıları ve Karşı Önlemler
- SQL Injection Attacks
- Kablosuz Şifreleme
- Bulut Bilgi İşlem Tehditleri
- Kripto Şifreleri
- Penetrasyon Testi

## **Outline**

- Module 01: Introduction to Ethical Hacking
- Module 02: Footprinting and Reconnaissance
- Module 03: Scanning Networks
- Module 04: Enumeration
- Module 05: Vulnerability Analysis
- Module 06: System Hacking
- Module 07: Malware Threats
- Module 08: Sniffing
- Module 09: Social Engineering
- Module 10: Denial-of-Service
- Module 11: Session Hijacking
- Module 12: Evading IDS, Firewalls, and Honeypots
- Module 13: Hacking Web Servers
- Module 14: Hacking Web Applications
- Module 15: SQL Injection
- Module 16: Hacking Wireless Networks
- Module 17: Hacking Mobile Platforms
- Module 18: IoT Hacking
- Module 19: Cloud Computing
- Module 20: Cryptography