CEH - Certified Ethical Hacker v12 Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

EC-Council'in Sertifikalı Etik Hacker (CEH v12) Eğitim programı, temel güvenlik temelleri hakkındaki bilginizi geliştirecektir. Sertifikalı Etik Hacker (CEH V12) sertifikasyon eğitimi, dünyada en çok aranan güvenlik yeterliliklerinden biridir. Uluslararası kabul görmüş bu güvenlik eğitimi, kuruluşların ağ altyapısındaki zayıflıkları keşfetme yeteneğinizi doğrular ve siber saldırılarla etkin mücadeleye yardımcı olur.

C|EH v12 programı, uygulamalı eğitim, laboratuvarlar, değerlendirme, deneme katılımı (alıştırma) ve küresel bilgisayar korsanlığı yarışmasıyla etik bilgisayar korsanlığı hakkında her şeyi öğreten uzmanlaşmış, türünün tek örneği bir eğitim programıdır.

Bu sertifika, Savunma Bakanlığı Onaylı bir 8570 Temel Sertifikasyonudur ve Savunma Bakanlığı 8140/8570 eğitim gereksinimlerini karşılar.

Siber dünyadaki tehditler sürekli arttığı için sektörün dünya çapındaki kuruluşlarda tehdit ve saldırıları önleyecek siber güvenlik profesyonellerine ihtiyacı var. Sertifikalı Etik Hacker (C|EH v12) programı, siber güvenlik alanında en saygın sertifikalardan biridir.

EC Council, C|EH v12 programında MITRE ATT&CK Çerçevesi, Elmas Saldırı Analizi Modeli, Kalıcılık Oluşturma Teknikleri, NAC'den Kaçınma ve Uç Nokta Güvenliği, Sis Hesaplama, Kenar Bilgi İşlem ve Izgara Hesaplama dahil olmak üzere yeni güncellenmiş teknolojileri tanıtıyor. Bu güncellenmiş teknolojiler sizi bir bilgisayar korsanı gibi düşünmeye hazırlayacak, böylece altyapınızı koruyacak becerilere sahip olacaksınız.

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.

Prerequisites

- Katılımcıların işletim sistemi, TCP/IP ve Ağ konusunda iyi bilgi ve anlayışa sahip olmaları gerekmektedir.
- Ağ temellerinin temel anlayışı, sunucu ve ağ bileşenleri dahil temel kavramlara hakim olunması önerilir.

CEH - Certified Ethical Hacker v12 Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Who Should Attend

- Orta Düzey Bilgi Güvenliği Denetçisi
- Siber Güvenlik Denetçisi
- Güvenlik Yöneticisi
- BT Güvenlik Yöneticisi
- Siber Savunma Analisti
- Güvenlik Açığı Değerlendirme Analisti
- Uyarı Analisti
- Bilgi Güvenliği Analisti 1
- Güvenlik Analisti L1
- Infosec Güvenlik Yöneticisi
- Siber Güvenlik Analisti seviye 1, seviye 2 ve seviye 3
- Ağ Güvenliği Mühendisi
- SOC Güvenlik Analisti
- Güvenlik Analisti
- Ağ Mühendisi
- Kıdemli Güvenlik Danışmanı
- Bilgi Güvenliği Yöneticisi
- Kıdemli SOC Analisti
- Çözüm Mimarı
- Siber Güvenlik Danışmanı

CEH - Certified Ethical Hacker v12 Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

- Etik bilgisayar korsanlığının temelleri, bilgi güvenliği kontrolleri, ilgili yasalar ve standart prosedürler dahil olmak üzere bilgi güvenliği dünyasındaki önemli konuların temellerini kapsar.
- Etik hackleme sürecinin kritik bir saldırı öncesi aşaması olan ayak izi ve keşif gerçekleştirmek için en son teknikleri ve araçları nasıl kullanacağınızı öğrenin.
- Etik bilgisayar korsanlığının temelleri, bilgi güvenliği kontrolleri, ilgili yasalar ve standart prosedürler dahil olmak üzere bilgi güvenliği dünyasındaki önemli konuların temellerini kapsar.
- Sınır Ağ Geçidi Protokolü (BGP) ve Ağ Dosya Paylaşımı (NFS) açıklarından yararlanmalar ve bunlara ilişkin karşı önlemler gibi çeşitli numaralandırma tekniklerini öğrenin.
- Hedef kuruluşun ağındaki, iletişim altyapısındaki ve uç sistemlerindeki güvenlik açıklarını nasıl belirleyeceğinizi öğrenin.
- Sistem ve ağdaki güvenlik açıklarını keşfetmek için kullanılan steganografi, steganaliz saldırıları ve izleri gizleme dahil olmak üzere çeşitli sistem korsanlığı metodolojileri hakkında bilgi edinin.
- Truva atları, virüsler ve solucanlar gibi farklı kötü amaçlı yazılım türlerinin yanı sıra kötü amaçlı yazılım saldırılarına yönelik sistem denetimi, kötü amaçlı yazılım analizi ve karşı önlemler hakkında bilgi edinin.
- Paket koklama teknikleri ve bunların ağdaki güvenlik açıklarını keşfetmek için nasıl kullanılacağının yanı sıra koklama saldırılarına karşı savunma önlemleri hakkında bilgi edinin.
- Hırsızlık girişimlerinin nasıl tespit edileceği, insan düzeyindeki güvenlik açıklarının nasıl denetleneceği ve sosyal mühendislik karşı önlemlerinin nasıl önerileceği dahil olmak üzere sosyal mühendislik kavramlarını ve tekniklerini öğrenin.
- Farklı Hizmet Reddi (DoS) ve Dağıtılmış DoS (DDoS) saldırı tekniklerinin yanı sıra bir hedefi denetlemek ve DoS ve DDoS karşı önlemlerini ve korumalarını tasarlamak için kullanılan araçlar hakkında bilgi edinin.
- Ağ düzeyinde oturum yönetimi, kimlik doğrulama, yetkilendirme ve kriptografik zayıflıkları ve ilgili karşı önlemleri keşfetmek için kullanılan çeşitli oturum ele geçirme tekniklerini anlayın.
- Güvenlik duvarı, izinsiz giriş tespit sistemi ve bal küpü kaçırma teknikleriyle tanışın; bir ağ çevresini zayıf noktalara karşı denetlemek için kullanılan araçlar; ve karşı önlemler.
- Web sunucusu altyapılarındaki güvenlik açıklarını ve karşı önlemleri denetlemek için kullanılan kapsamlı bir saldırı metodolojisi de dahil olmak üzere web sunucusu saldırıları hakkında bilgi edinin.
- Web uygulamalarındaki güvenlik açıklarını ve karşı önlemleri denetlemek için kullanılan kapsamlı bir web uygulaması korsanlığı metodolojisi de dahil olmak üzere web uygulaması saldırıları hakkında bilgi edinin.
- SQL enjeksiyon saldırı teknikleri, enjeksiyon tespit araçları ve SQL enjeksiyon girişimlerini tespit etmek ve bunlara karşı savunma yapmak için karşı önlemler hakkında bilgi edinin.
- Kablosuz şifreleme, kablosuz bilgisayar korsanlığı metodolojileri ve araçları ile Wi-Fi güvenlik araçları hakkında bilgi edinin.
- Mobil platform saldırı vektörleri, Android'deki güvenlik açığı istismarları ve mobil güvenlik yönergeleri ve araçları hakkında bilgi edinin.
- Paket koklama teknikleri ve bunların ağdaki güvenlik açıklarını keşfetmek için nasıl kullanılacağının yanı sıra koklama saldırılarına karşı savunma önlemleri hakkında bilgi edinin.
- Konteyner teknolojileri ve sunucusuz bilgi işlem, çeşitli bulut tabanlı tehditler ve saldırılar ile bulut güvenliği teknikleri ve araçları gibi farklı bulut bilişim kavramlarını öğrenin.
- Kriptografi ve şifreler, genel anahtar altyapısı, kriptografi saldırıları ve kriptanaliz araçları hakkında bilgi edinin.

Outline

CEH - Certified Ethical Hacker v12 Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

1. **Etik Hacking'e Giriş**

- Bilgi Güvenliğine Genel Bakış
- Hacking Metodolojileri ve Çerçeveleri
- Hacking Kavramları
- Etik Hacking Kavramları
- Bilgi Güvenliği Kontrolleri
- Bilgi Güvenliği Kanunları ve Standartları

2. Ayak İzi ve Keşif

- Ayak İzi Konseptleri
- Arama Motorları Aracılığıyla Ayak İzi
- Web Hizmetleri aracılığıyla Ayak İzi
- Sosyal Ağ Siteleri Aracılığıyla Ayak İzi
- Web Sitesi Ayak İzi
- E-posta Ayak İzi
- Whois Ayak İzi
- DNS Ayak İzi
- Ağ Ayak İzi
- Sosyal Mühendislik Yoluyla Ayak İzi
- Ayak İzi Araçları
- Ayak İzi Önlemleri

3. Ağları Tarama

- Ağ Tarama Kavramları
- Tarama Araçları
- Ana Bilgisayar Keşfi
- Liman ve Hizmet Keşfi
- İşletim Sistemi Keşfi (Banner Yakalama/İşletim Sistemi Parmak İzi Alma)
- IDS ve Güvenlik Duvarının Ötesinde Tarama
- Ağ Taramasına Karşı Önlemler

4. Numaralandırma

- Numaralandırma Kavramları
- NetBIOS Numaralandırması
- SNMP Sayımı
- LDAP Numaralandırması
- NTP ve NFS Sayımı
- SMTP ve DNS Numaralandırması
- Diğer Numaralandırma Teknikleri
- Sayım Karşı Önlemleri

5. Güvenlik Açığı Analizi

- Güvenlik Açığı Değerlendirme Kavramları
- Güvenlik Açığı Sınıflandırması ve Değerlendirme Türleri
- Güvenlik Açığı Değerlendirme Araçları
- Güvenlik Açığı Değerlendirme Raporları

6. Sistem Hackleme

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Erişim Kazanmak
- Ayrıcalıkların Yükseltilmesi
- Erişimi Sürdürmek
- Günlükleri Temizleme

7. Kötü Amaçlı Yazılım Tehditleri

- Kötü Amaçlı Yazılım Kavramları
- APT Konseptleri
- Truva Atı Kavramları
- o Solucan Yapıcılar
- Dosyasız Kötü Amaçlı Yazılım Kavramları
- Kötü Amaçlı Yazılım Analizi
- Kötü Amaçlı Yazılımlara Karşı Önlemler
- Kötü Amaçlı Yazılımdan Koruma Yazılımı

8. Sniffing

- Sniffing Kavramları
- Sniffing Tekniği: MAC Saldırıları
- Sniffing Tekniği: DHCP Saldırıları
- Koklama Tekniği: ARP Zehirlenmesi
- Sniffing Tekniği: Sahtekarlık Saldırıları
- Sniffing Tekniği: DNS Zehirlenmesi
- Koklama Araçları

9. Sosyal Mühendislik

- Sosyal Mühendislik Kavramları
- Sosyal Mühendislik Teknikleri
- İçeriden Tehditler
- Sosyal Ağ Sitelerinde Kimliğe Bürünme
- Kimlik Hırsızı
- Sosyal Mühendislik Önlemleri

10. Denial-of-Service

- DoS/DDoS Kavramları
- Bot ağları
- DoS/DDoS Saldırı Teknikleri
- DDoS Örnek Olay İncelemesi
- DoS/DDoS Saldırısına Karşı Önlemler

11. Session Hijacking

- Oturum Ele Geçirme Kavramları
- Uygulama Düzeyinde Oturum Ele Geçirme
- Ağ Düzeyinde Oturum Ele Geçirme
- Oturum Ele Geçirme Araçları
- Oturum Ele Geçirmeye Karşı Önlemler

12. IDS, Güvenlik Duvarları ve Honeypot'lardan Kaçınmak

- IDS, IPS, Güvenlik Duvarı ve Honeypot Kavramları

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- IDS, IPS, Güvenlik Duvarı ve Honeypot Çözümleri
- Kimliklerden Kaçınmak
- Güvenlik Duvarlarından Kaçınmak
- NAC ve Uç Nokta Güvenliğinden Kaçınmak
- IDS/Güvenlik Duvarından Kaçınma Araçları
- Honeypot'ları Tespit Etme
- IDS/Güvenlik Duvarından Kaçınmaya Karşı Önlemler

13. Web Sunucularını Hacklemek

- Web Sunucusu Kavramları
- Web Sunucusu Saldırıları
- Web Sunucusu Saldırı Metodolojisi
- Web Sunucusu Saldırısına Karşı Önlemler

14. Web Uygulamalarını Hacklemek

- Web Uygulama Kavramları
- Web Uygulaması Tehditleri
- Web Uygulaması Hacking Metodolojisi
- Web API'si, Web Kancaları ve Web Kabuğu
- Web Uygulama Güvenliği

15. SQL Enjeksiyonu

- SQL Enjeksiyon Kavramları
- SQL Enjeksiyon Türleri
- SQL Enjeksiyon Metodolojisi
- SQL Enjeksiyon Araçları
- SQL Enjeksiyonuna Karşı Önlemler

16. Kablosuz Ağları Hacklemek

- Kablosuz Kavramlar
- Kablosuz şifreleme
- Kablosuz Tehditler
- Kablosuz Hackleme Metodolojisi
- Kablosuz Hackleme Araçları
- Bluetooth Hackleme
- Kablosuz Saldırıya Karşı Önlemler
- Kablosuz Güvenlik Araçları

17. Mobil Platformları Hacklemek

- Mobil Platform Saldırı Vektörleri
- Android işletim sistemini hacklemek
- iOS'u hacklemek
- mobil cihaz Yönetimi
- Mobil Güvenlik Yönergeleri ve Araçları

18. IoT and OT Hackleme

- Nesnelerin İnterneti Hackleme
- Nesnelerin İnterneti Kavramları

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Nesnelerin İnterneti Saldırıları
- IoT Hacking Metodolojisi
- OT Hacking
- Fazla Mesai Konseptleri
- Uzatma Saldırıları
- OT Hacking Metodolojisi

19. Bulut Bilişim

- Bulut Bilişim Kavramları
- Konteyner Teknolojisi
- CloudTrial Hizmetini Yönetme
- Bulut Güvenliği

20. Kriptografi

- Kriptografi Kavramları
- Şifreleme Algoritmaları
- Kriptografi Araçları
- E-posta Şifreleme
- Disk Şifreleme
- Kriptanaliz
- Kriptografi Saldırısına Karşı Önlemler