OffSec PEN-200 (OSCP) Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

OffSec PEN-200, etik hackerlık ve penetrasyon testi alanında kariyer yapmak isteyen profesyoneller için hazırlanmış uygulamalı bir eğitim programıdır. Program, katılımcıların gerçek dünyadaki sistemleri analiz edebilmesini, güvenlik açıklarını tespit edebilmesini ve kontrollü ortamlarda bu zafiyetleri değerlendirebilmesini amaçlar.

Kali Linux tabanlı laboratuvar ortamlarında gerçekleştirilen çalışmalar sayesinde katılımcılar profesyonel penetrasyon testi metodolojilerini öğrenir ve güvenlik değerlendirme süreçlerini uçtan uca uygulama fırsatı bulurlar.

Eğitim süresince bilgi toplama, zafiyet analizi, web uygulama güvenliği, istemci tarafı saldırıları ve exploit geliştirme gibi konular detaylı olarak ele alınır. Program aynı zamanda OffSec Certified Professional (OSCP / OSCP+) sertifikasyonlarına hazırlık için gerekli teknik altyapıyı sağlar.

Katılımcılar eğitim içeriğine ve laboratuvar ortamlarına 12 ay boyunca erişim hakkına sahip olur.

Prerequisites

Bu eğitim için resmi bir ön koşul bulunmamakla birlikte aşağıdaki bilgi ve deneyimlere sahip olunması önerilir:

- TCP/IP ağ yapıları hakkında bilgi sahibi olmak
- Linux ve Windows işletim sistemleriyle çalışma deneyimi
- Bash, Python veya benzeri betik dillerinde temel seviyede programlama bilgisi
- Temel bilgi güvenliği ve sistem yönetimi bilgisi

Etik hackerlık alanına yeni başlayan katılımcılar için temel güvenlik eğitimlerinin tamamlanmış olması fayda sağlayacaktır.

Who Should Attend

Bu eğitim aşağıdaki profesyoneller için uygundur:

- Penetrasyon Test Uzmanları
- Siber Güvenlik Analistleri
- Threat Hunter ve Güvenlik Araştırmacıları
- Sistem ve Ağ Yöneticileri
- Red Team üyeleri
- Offensive Security alanında kariyer hedefleyen profesyoneller
- OSCP sertifikasına hazırlanmak isteyen katılımcılar

OffSec PEN-200 (OSCP) Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

Eğitim sonunda katılımcılar:

- Penetrasyon testi metodolojilerini uygulayabilecek,
- Hedef sistemlerde bilgi toplama ve keşif çalışmaları gerçekleştirebilecek,
- Güvenlik açıklarını analiz edip doğrulayabilecek,
- Yaygın web uygulaması zafiyetlerini değerlendirebilecek,
- İstemci tarafı saldırı tekniklerini kullanabilecek,
- Açık kaynak exploitleri analiz edip özelleştirebilecek,
- Profesyonel penetrasyon testi raporları hazırlayabilecek,
- OSCP ve OSCP+ sınavlarına yönelik pratik deneyim kazanabileceklerdir.

Outline

Siber Güvenliğe Giriş

- Güncel tehdit ortamı
- Güvenlik kavramları ve terminolojisi
- Etik hackerlığın rolü
- Penetrasyon testi süreçleri

Penetrasyon Testi Raporlama

- Teknik bulguların dokümante edilmesi
- Risk değerlendirmesi
- Düzeltici aksiyon önerileri
- Yönetici seviyesinde raporlama teknikleri

Bilgi Toplama ve Keşif

- Aktif ve pasif keşif yöntemleri
- Ağ haritalama
- Hedef belirleme süreçleri
- Nmap ve benzeri araçlarla keşif çalışmaları

Zafiyet Analizi

- Güvenlik açığı tarama yöntemleri
- Sonuçların yorumlanması
- Risk önceliklendirmesi
- Güvenlik açığı doğrulama süreçleri

Web Uygulama Güvenliği

- Modern web uygulama mimarileri
- Saldırı yüzeylerinin belirlenmesi
- Yaygın güvenlik zafiyetleri

Web Saldırı Teknikleri

OffSec PEN-200 (OSCP) Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

- Cross-Site Scripting (XSS)
- SQL Injection
- Session Management zafiyetleri
- Kimlik doğrulama ve yetkilendirme problemleri

SQL Injection Uygulamaları

- Enjekte edilebilir parametrelerin tespiti
- Veri çıkarımı
- Yetki yükseltme senaryoları

İstemci Tarafı Saldırıları

- Tarayıcı güvenliği
- JavaScript tabanlı zafiyetler
- Kullanıcı odaklı saldırı senaryoları

Exploit Araştırma ve Kullanımı

- Güvenilir exploit kaynaklarının kullanımı
- Exploit doğrulama süreçleri
- Penetrasyon test süreçlerine entegrasyon

Exploit Özelleştirme

- Payload uyarlama teknikleri
- Savunma mekanizmalarının aşılması
- Proof-of-Concept geliştirme