Etik Hacking

Açıklama

5 günlük eğitim boyunca katılımcılar siber saldırganların bakış açısını, kullandıkları araçları ve teknikleri uygulamalı olarak ele almaktadırlar. Bu süre sonunda sistemlerin, ağların ve uygulamaların zafiyetlerini tespit edebilecek ve bunları istismar edecek bilgi ve beceriyi kazanmaları hedeflenir.

Bu eğitimde neler öğreneceksiniz?

- Etik Hacking'e Giriş
- Bilgi Toplamak
- Zafiyet Tespiti
- Sistem Güvenliği
- Ağ Güvenliği
- Tehdit Analizi ve Risk Yönetimi
- Uygulama Güvenliği
- Sosyal Mühendislik Saldırıları

Eğitim İçeriği

Etik Hacking'e Giriş

- Bilgi güvenliğine giriş
- Bilgi güvenliğinin temelleri
- Gizlilik, bütünlük ve erişilebilirlik üçgeni
- Güvenliğin zorlukları
- Siber saldırgan türleri
- Bütüncül güvenlik yaklaşımı
- Kademeli güvenlik yaklaşımı
- Sızma testi metodolojileri
- Hacking döngüsü

Etik Hacking

Bilgi Toplamak

- Sistem tespiti
- Whois sorguları
- DNS sorguları
- Hedef bulmak
- Tarama türleri
- Port taraması
- Google hacking
- Açık kaynak istihbarat teknikleri
- Bilgi toplama araçları

Zafiyet Tespiti

- Ağ seviyesinde zafiyet tespiti
- Sistem seviyesinde zafiyet tespiti
- Uygulama zafiyetlerinin tespiti

Sistem Güvenliği

- Parola kırma saldırıları
- Zafiyet tarama araçları
- Metasploit kullanımı
- Diğer zafiyet/istismar bulma yöntemleri
- Önbellek taşırma saldırıları
- Zararlı yazılımlar
- DNS tünelleme
- Sistem güvenliğinin sağlanması
- İstemci güvenlik duvarı (host firewall/Host IPS)
- Antivirüsler
- Yama yönetimi

Ağ Güvenliği

- Ağ temelleri
- Ağların taranması
- Açık portlar
- Çalışan protokoller
- Ağ trafiğinin izlenmesi
- Wireshark kullanımı

- Zafiyet tespiti
- Yerel ağda yapılan saldırılar
- Güvenlik duvarları (Firewall)
- IPS/IDS
- Güvenli ağ tasarımı

Tehdit Analizi ve Risk Yönetimi

- Tehdit tespit yöntemleri
- Risk yönetimi yaklaşımı
- Teknik etkinin değerlendirilmesi
- İşe etkilerin değerlendirilmesi
- Zafiyet yönetimi süreçlerinin belirlenmesi

Uygulama Güvenliği

- Uygulama yapıları
- Saldırı noktalarının tespiti
- Testlerde kullanılacak araçlar
- OWASP Top 10
- OWASP test metodolojisi
- Uygulama test metodolojisi
- Hizmet dışı bırakma saldırıları
- Uygulama mimarisinin anlaşılması
- Kaynak kod analiz teknikleri

Sosyal Mühendislik Saldırıları

- Sosyal mühendisliğin temelleri
- Sosyal mühendislik saldırı belirtileri
- Social Engineering Toolkit kullanımı
- Oltalama (Phishing) saldırıları
- Sosyal mühendislik için bilgi toplama teknikleri

Ön Koşullar

Herhangi bir ön koşul bulunmamaktadır.