

Etik Hacking Eğitimi

Süre: 5 Gün

Etik Hacking Eğitimi Hakkında

Etik Hacking Eğitimi, siber saldırganların bakış açısını, kullandıkları araçları ve teknikleri uygulamalı olarak ele alan 5 günlük sanal sınıf / online programdır. Katılımcıların sistem, ağ ve uygulama zafiyetlerini tespit etme ve değerlendirme bilgi ve becerilerini geliştirmesi hedeflenir.

Program; etik hacking'e giriş, bilgi toplama, zafiyet tespiti, sistem güvenliği, ağ güvenliği, tehdit analizi ve risk yönetimi, uygulama güvenliği ile sosyal mühendislik saldırıları olmak üzere sekiz ana modülden oluşur. Bilgi güvenliğinin temelleri, sızma testi metodolojileri ve hacking döngüsüyle başlayan içerik, farklı güvenlik katmanlarını birlikte ele alır.

Müfredatta Metasploit, Wireshark, OWASP Top 10, OWASP test metodolojisi ve Social Engineering Toolkit gibi başlıklar yer alır. Teknik ve iş etkilerinin değerlendirilmesi, zafiyet yönetimi süreçleri ve güvenli ağ tasarımı da eğitim kapsamındadır.

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

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 taşıma 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.