Sızma Testi Uzmanlığı Eğitimi

Süre: **4 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

Siber güvenliğin en kritik alanlarından biri olan **Sızma Testi (Pentest)**, kurumların bilgi sistemlerindeki zafiyetleri **etik hacker gözüyle tespit etmek** ve bu açıkları sömürülmeden önce gidermeyi amaçlar. Bu eğitim, katılımcılara **planlamadan raporlamaya kadar uçtan uca bir sızma testi sürecini** hem teorik hem de uygulamalı olarak öğretir.

Katılımcılar, eğitim sonunda bir sızma testi uzmanının sahip olması gereken tüm bilgi ve becerilere hâkim olur — **yasal çerçevede, profesyonel araçlar ve yöntemlerle.**

Prerequisites

Temel seviyelerde Linux & Windows sistem, ağ, programlama, web teknolojisi, veritabanı.

Who Should Attend

Bu eğitim aşağıdaki profesyoneller için özel olarak tasarlanmıştır:

- Siber güvenlik uzmanları
- Ağ ve sistem yöneticileri
- Red Team üyeleri
- Güvenlik denetçileri ve danışmanları
- Etik hacker olmak isteyen IT profesyonelleri

Temel ağ ve sistem bilgisine sahip herkes eğitime katılabilir.

What You Will Learn

Eğitimi tamamlayan katılımcılar:

- Profesyonel sızma testi sürecini baştan sona yönetebilir.
- Kurumsal sistemlerde güvenlik açıklarını tespit edebilir.
- Etik hacker metodolojilerini yasal çerçevede uygulayabilir.
- Raporlama ve risk analizi konularında yetkinlik kazanır.
- Siber güvenlik denetimlerinde aktif rol alabilir.

Sızma Testi Uzmanlığı Eğitimi

Süre: **4 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Outline

Eğitim içeriği, **güncel pentest metodolojileri (OSSTMM, OWASP, NIST)** ve **global güvenlik standartları** dikkate alınarak hazırlanmıştır.

Genel Kavramlar ve Hazırlık Aşaması

- Sızma testi nedir, nasıl yapılır?
- Yasal süreçler ve gerekli izinler (NDA, Etik sınırlar)
- Sızma testine neden ihtiyaç duyulur?
- Güncel metodolojiler ve planlama yaklaşımları

Bilgi Toplama ve Keşif (Reconnaissance)

- Pasif / aktif bilgi toplama yöntemleri
- Özelleştirilmiş arama motorları ile bilgi toplama
- hping ve benzeri network analiz araçlarının kullanımı
- Paket analizi ve sniffing uygulamaları

Güvenlik Zafiyeti Analizi

- Güvenlik zafiyeti tarama araçları (Nessus, OpenVAS, Nmap)
- Güvenlik testlerinin yasal durumu ve sorumluluklar
- Tarama sonuçlarının yorumlanması ve risk önceliklendirmesi

Sistem Bazlı Sızma Testleri

- **Windows sistemleri:** Kullanıcı hakları, servis zafiyetleri, exploit testleri
- **Linux / Unix sistemleri:** Yetki yükseltme ve servis istismarı teknikleri
- **Cisco ağ cihazları:** IOS zafiyetleri, SNMP testleri ve yapılandırma hataları
- **Veritabanı sistemleri:** SQL injection, erişim denetimi, veri sızıntısı testleri

Ağ Güvenliği Testleri

- Yerel ağ zafiyetlerinin keşfi
- Firewall, IPS, WAF testleri
- IPS / WAF atlatma teknikleri
- Güvenlik sistemlerini aşma stratejileri

Sızma Testi Uzmanlığı Eğitimi

Süre: **4 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Kablosuz Ağ ve DDoS Testleri

- Kablosuz ağ zafiyetleri (WPA2/WPA3 testleri)
- DoS/DDoS saldırı simülasyonları ve önleme yöntemleri

Exploitation ve Saldırı Teknikleri

- Exploitation nedir ve nasıl yapılır?
- İleri düzey exploit geliştirme yöntemleri
- Malware, trojan, backdoor analizleri
- Parola saldırıları (Brute-force, Dictionary, Hybrid)

Sosyal Mühendislik ve Kullanıcı Güvenliği

- Sosyal mühendislik saldırı türleri
- E-posta, telefon ve fiziksel güvenlik senaryoları
- Gerçek dünyadan vaka analizleri

Raporlama ve Sonuçlandırma

- Sızma testi raporunun hazırlanması
- Bulguların sınıflandırılması (CVSS, CWE)
- Yönetim özet raporu yazma
- Rapor optimizasyonu ve profesyonel sunum teknikleri