01 Tanıtıma Başlarken
CyberLab Bilgi Güvenliği Merkezi

PENETRASYON(SIZMA TESTİ)
GENEL TANITIM BROŞÜRÜ

2019

02 Penetrasyon (Sızma Testi)
CyberLab Bilgi Güvenliği Merkezi

Sızma testlerinde siber suçluların gerçek dünyada kullandığı yöntemler kullanılarak bir kurumun bilişim altyapısına sızılmaya ve ele geçirilmeye çalışılır.

Böylelikle penetrasyon testi-Pentest yapan güvenlikçiler, hacker gibi düşünüp sisteme sızma ve ele geçirme senaryolarını uygulayarak ve saldırganların deneyebileceği tüm yöntemleri deneyerek gerçek bir saldırı ile karşılaşıldığında sistemin açıklık barındıran noktalarının onarılmış ve güvenliği sıkılaştırılmış olmasını sağlamaktadırlar.

Penetrasyon testlerinde lisanslı veya açık-kaynak kodlu araçlar kullanılmakta, mümkün olduğunca tüm zafiyetler tespit edilip düzeltilmeye çalışılmaktadır.

03 Kurumsal Riskler
CyberLab Bilgi Güvenliği Merkezi

Günümüzde bireysel ya da kurumsal ekonomik her türlü gelişme, İnternet ve bilgi teknolojileri sistemlerine daha da fazla bağlı hale gelmektedir. Bunun sonucu olarak sistemler üzerindeki riskler, daha fazla fark edilmekte ve önemli olarak görülmektedir. Bilgi sistemleri üzerindeki güvenlik açıkları ya da hatalar, ciddi iş krizlerine ve itibar kayıplarına yol açabilmektedir.

Bu sebeple, pek çok düzenleyici kuruluş yeni uyum zorunlulukları getirmektedir. Bu uyum zorunluluklarının kurumunuza uyarlanması sürecinde, şirketimiz CyberLab Bilgi Güvenliği Merkezi olarak yanınızdayız.

04 Sızma Testi Amaçlar
CyberLab Bilgi Güvenliği Merkezi

- Kurumun güvenlik politikalarının ve kontrollerinin verimliliğini test etmek ve denetlemek
- Zafiyet ve açıklık taramasını içten ve dıştan derinlemesine uygulamak
- Standartlara uyumluluk için veri toplayan denetleme ekiplerine kullanılabilir data sağlamak
- Kurumun güvenlik kapasitesi hakkında kapsamlı ve ayrıntılı analiz sunarak güvenlik denetlemelerinin maliyetini düşürmek
- Bilinen zafiyetlere uygun yamaların uygulanmasını sistematik bir hale getirmek
- Kurumun ağ ve sistemlerinde mevcut olan risk ve tehditleri ortaya çıkarmak
- Gelecek saldırı, sızma ve istismar girişimlerini önlemek için alınabilecek aksiyonları belirleyen kapsamlı bir plan sunmak

05 Test İşlemleri
CyberLab Bilgi Güvenliği Merkezi

Sızma testlerinin uygulama yöntemleri ihtiyaçlar doğrultusunda değişebilir. Bazı kurumlar için internet üzerinden; sunucu, uygulama ve cihazlara yönelik gerçekleştirilebileceği gibi, bazı kurumlarda doğrudan iç ağdaki BT varlıklarına ve iç ağda kullanılan özel uygulamalara yönelik olarak da gerçekleştirilebilir.

İhtiyaç duyulursa, hem iç tehditleri hem de dış tehditleri kapsayan senaryolar oluşturulabilir.

Belirli aralıklarla uygulanan sızma testi, bilgi güvenliği sisteminin sağlığının sürekli en iyi kondisyonda kalabilmesini sağlar.

06 Test İşlemleri (White Box)
CyberLab Bilgi Güvenliği Merkezi

White Box Sızma Testi'nde, siber güvenlik uzmanı, firma içinde yetkili kişilerce bilgilendirilir ve firma hakkındaki tüm sistemler hakkında bilgi sahibi olur.

Bu yöntemde daha önce firmada yer almış, hala çalışmakta olan veya misafir olarak ağa sonradan dahil olan kişilerin sistemlere verebilecekleri zararlar gözetilir ve raporlanır.

07 Test İşlemleri (Black Box)
CyberLab Bilgi Güvenliği Merkezi

Black Box Sızma Testi yapılırken sızma testini gerçekleştiren firmayla herhangi bir bilgi paylaşımında bulunulmaz sadece hedef verilir. Bilgi sızdırmak ya da zarar vermek amacıyla sızmaya çalışan bir hacker gibi davranılarak verilebilecek zararlar gözetilir ve raporlanır.

08 Test İşlemleri (Gray Box)
CyberLab Bilgi Güvenliği Merkezi

White Box ile Black Box testlerini kapsayan yani hem içeriden hem dışarıdan olarak yapılan test diye tanımlayabiliriz. Gray Box'ta ek olarak Sosyal Mühendislik Saldırıları ve Kablosuz Ağ Saldırıları da eklenmektedir.

09 Test İşlemleri - İşlemler
CyberLab Bilgi Güvenliği Merkezi

- Pasif Bilgi Toplama
- Aktif Bilgi Toplama
- Ağ Analizi
- Port Analizi
- Sistem Analizi
- Yetki Yükseltme
- Sistem Durdurma
- Kaynakların Doldurulması
- Yetkisiz Erişim Sağlama
- Risk Değerlendirmesi
- Web Tabanlı Uygulamalara Yönelik Saldırılar
- Sosyal Mühendislik Saldırıları

- Tespit edilen güvenlik açıkları raporlanırken teknik olarak zafiyet bazlı veya IP bazlı olabilir.
- Raporda teknik detay olarak ; zaafiyet ismi, etkilenen makineler (kullanıcılar, sunucular, switch vb.), açıklama, çözüm önerisi, ilgili port/servis, referanslar (MS08-067 –> CVE-2008-250) , elde edilen detaylar ve ekran görüntüleri yer almalıdır.
- Güvenlik açıklarının neden olabileceği sonuçlar ile risk değerlendirilmesi yapılmalıdır.
- Açıklıklarının kapatılmasının takibi yapılmalıdır.
- Raporda yer alan açıklar belirlenerek hangi açığın kimin sorumluluğunda olduğu belirlenmelidir.

11 İletişim Kanallarımız
CyberLab Bilgi Güvenliği Merkezi

Telefon : +90 216 740 00 56
Gsm : +90 533 737 17 71
Fax : +90 242 255 55 97

E-posta : hello@cyberlab.center
Web : www.cyberlab.center