Sızma Testi (Penetrasyon Testi)

BİLGİ GÜVENLİĞİ VE KRİPTOLOJİ

Sızma (Penetrasyon) Testi Nedir?

Sızma - Penetrasyon Testi kötü niyetli bir saldırgan perspektifinde, hedeflenen sistemlere ve verilere yetkisiz erişim sağlamayı amaçlayan bir saldırı simülasyonudur. Dışarıdan gelebilecek saldırıları önceden görüp önlem almak için sızma - penetrasyon testi yapılmalıdır.

Sızma (Penetrasyon) testi PCI-DSS, ISO 27001, CoBIT gibi uluslararası standartların yanı sıra Türkiye'de BDDK, EPDK ve SPK gibi regülatörler tarafından da yapılması zorunlu tutulan çalışmalardan biridir.

Sızma (Penetrasyon) Testi Nasıl Yapılır?

Kurumların bilişim altyapısını içerisinde barındırdığı tüm sistemler, alanında uzman kişiler tarafından saldırganın kullanabileceği araç ve yöntemleri kullanarak sızılması ve elde edilen zafiyet sonuçlarının raporlanmasıdır.

Sızma Testi Süreçleri Nasıl Yürütülür?

Testin yapılacağı hedef sistemler sistem tarafından belirlenir ve test edilecek sistemler hakkında testi yapan kuruma bilgi verilir. Gerekli anlaşmalar sonucu testin yapılacağı IP adresi müşteri ile paylaşılır, böylelikle kuruma farklı IP adresinden gelen saldırıların test olup olmadığı anlaşılması sağlanır. Teste başlanılır, kritik bulgular test esnasında müşteri ile paylaşılırken, düşük seviyeli bulgular/zafiyetler test sonunda kritik bulgularla beraber raporlanır ve test sonlanır.

Sızma Testi Aşamaları Nelerdir?

1. Kapsam Belirlenmesi

Müşteri, testin yapılmasını istediği hedefi/kapsamı belirler. Testin yaklaşım türüne göre (Black Box, White Box, Gray Box) testi yapacak olan firma ile bilgiler paylaşılır.

2. Bilgi Toplama

Kapsam/Hedef hakkında pasif (sistem ile doğrudan etkileşime geçmeden) ve aktif (sistem ile doğrudan etkileşime geçerek) bilgi toplama işlemi gerçekleştirilir. Bunlara; kullanılan teknoloji, uygulama ve versiyon bilgisi, fonksiyonlar gibi bilgiler örnek gösterilebilir.

3. Güvenlik Açığı Tespiti

Toplanan bilgiler ışığında var olan güvenlik açıklıklarının belirlendiği aşamadır. Otomatize araçlar kullanılarak taranan sistemler, tarama sonrasında/esnasında uzmanlar tarafından manuel olarak test edilir. Bilgi toplama aşamasında tespit edilen servis ve versiyon bilgisi araştırılarak var olan bir güvenlik açığı olup olmadığı kontrol edilir.

Sızma Testi Aşamaları Nelerdir?

4. Bilgilerin Analizi ve Planlama

Tespit edilen güvenlik açıklıklarının sömürülmesi için gerekli araştırmalar yapılarak sömürü kodları, zararlı yazılımlar gibi ofansif araçlar hazırlanır.

5. Sömürü Aşaması

Tespit edilen zafiyetler saldırgan bakış açısı ile sömürülmeye çalışılır ve zafiyetin sistem üzerindeki etkileri incelenir. Saldırgan, sisteme yetkisiz giriş yapabiliyor mu? Servisi durdurabiliyor mu? Gibi sorulara cevap aranır.

6. Yetki Yükseltme/Sömürü Sonrası Aşama

Saldırgan sisteme erişim elde ettikten sonraki aşamada halihazırdaki yetkilerini yükseltebilecek mi? Yetkisi olmayan dosyaları görebilecek mi? Veya sızılan sistem/ler kullanılarak nasıl ilerlenebilir? Ne gibi kritik dosyalara erişim sağlanabilir? Gibi sorulara yanıt aranır. Saldırganın sömürü sonrası yapacağı teknik/taktik/prosedürler simüle edilmeye çalışılır.

Sızma Testi Aşamaları Nelerdir?

7. Temizlik

Test edilen sistemlerde yapılan değişiklikler geri alınır. Test için oluşturulan/yüklenen dosyalar sistemden temizlenir.

8. Raporlama

Yukarıdaki adımların özeti çıkarılır. Var olan veya ileride oluşabilecek potansiyel riskler, alınması gereken önlemler gibi bilgiler raporlanır.

Sızma Testi, Etik Hackleme

Sızma testi hedefi, beyaz kutu (arka plan ve sistem bilgisi sağlayan) veya kara kutu (şirket adı dışında yalnızca temel bilgi sağlayan veya hiç bilgi sağlamayan) olabilir. **Sızma testi**, bir sistemin saldırılara açık olup olmadığını, savunmaların yeterli olup olmadığını ve testin sonucunda hangi önlemlerin alınacağını belirlemeye yardımcı olabilir.

Sızma Testi, Etik Hackleme

Etik hackleme ise tüm hackleme yöntemlerini ve diğer ilgili siber saldırı yöntemlerini içeren kapsamlı bir terimdir. Etik bir hacker'ın rolü bir penetrasyon test uzmanınkine benzer, ancak daha geniş görevleri içerir. Etik saldırı tanımı "genellikle bir kuruluşla birlikte çalışan ve kötü niyetli bir bilgisayar korsanıyla aynı yöntem ve teknikleri kullanarak ağlara ve / veya bilgisayar sistemlerine nüfuz etme girişiminde bulunabilecek bir kişidir. "

Genel olarak farklar şu şekildedir:

Sızma / Penetrasyon testi	Etik hackleme
Temel amaç, hedef ortamdaki güvenlik açıklarını bulmaktır.	Güvenlik kusurlarını bulmak için farklı saldırı teknikleriyle çeşitli saldırıları kullanmayı amaçlamaktadır.
Sızma testi, test için tanımlanan belirli alanın güvenliğine odaklanır.	Etik hacking kapsamlı bir terimdir ve penetrasyon testi etik hacker'ın işlevlerinden biridir.
Penetrasyon testinde farklı metodolojiler uyguladığından ve her metodolojinin amacını, nasıl ve ne zaman uygulanacağını bilmesi beklenir.	Etik hackerlar, hackleme metodolojileri hakkında kapsamlı bilgiye sahip olmalıdır.

Sızma / Penetrasyon testi	Etik hackleme
İyi bir penetrasyon test uzmanı olmak için etik hacklemede önceden deneyimli olmak gereklidir.	Etik hack, penetrasyon testine doğru bir adımdır. Metodolojileri bilmedikleri sürece, pentest yapamazlar.
Bir penetrasyon test uzmanı belirli bir alan ve ağ üzerinde çalışabilir. Beklenen bilgi uzman düzeyinde daha belirgindir.	Etik bilgisayar korsanları dizüstü bilgisayar hırsızlığı ve çalışan sahtekarlığıyla ilgili sorunları da ele alabilir.

En İyi Penetrasyon Testi Araçları

Bu araçlar, geniş bir test kapsamı sunan ve güvenlik açıklarını tespit etmek ve düzeltmek için uzmanlara yardımcı olan güçlü ve etkili araçlardır.

Metasploit: Metasploit, en popüler ve etkili penetrasyon testi araçlarından biridir. Kapsamlı bir saldırı ve penetrasyon testi çerçevesi sunar. Modüler yapısı sayesinde farklı saldırı vektörlerini hedefleyebilir ve siber saldırı senaryolarını simüle edebilir. Metasploit, zengin veritabanıyla birlikte gelir ve saldırganların hedef sistemlere yönelik açıkları tespit etmelerine yardımcı olur. Ayrıca, raporlama ve analiz yetenekleri ile test sonuçlarını anlamlı bir şekilde sunar.

Nmap: Nmap (Network Mapper), ağ analizi ve keşif için kullanılan güçlü bir araçtır. Ağdaki cihazları ve hizmetleri tespit etmek, açık portları tarayarak güvenlik açıklarını bulmak gibi işlevlere sahiptir. Nmap, çeşitli tarama tekniklerini destekler ve hedef ağın güvenlik durumu hakkında kapsamlı bilgiler sağlar. Kullanıcı dostu bir arayüze sahip olması ve farklı işletim sistemlerinde kullanılabilmesi, Nmap'i popüler bir seçenek haline getirir.

En İyi Penetrasyon Testi Araçları

Burp Suite: Burp Suite, web uygulamalarının güvenlik testlerinde yaygın olarak kullanılan bir araçtır. HTTP/HTTPS trafiğini analiz etmek, otomatik saldırılar gerçekleştirmek, zayıf oturum yönetimi ve güvenlik açıklarını tespit etmek gibi işlevlere sahiptir. Burp Suite, kullanıcı dostu arayüzü ve kapsamlı özellikleriyle web uygulamalarının güvenlik açıklarını tespit etmek ve gidermek için etkili bir seçenektir. Ayrıca, proxy özelliği sayesinde web trafiğini yönlendirme imkanı sunar.

Wireshark: Wireshark, ağ trafiğini analiz etmek ve paketleri yakalamak için kullanılan popüler bir araçtır. Ağ üzerinden iletilen verileri izleyebilir, protokol analizi yapabilir ve güvenlik açıklarını tespit etmek için kullanılabilir. Wireshark, ağ üzerinde gerçekleşen saldırıları tespit etmek ve ağ trafiğini daha iyi anlamak için güçlü bir araçtır. Hem başlangıç düzeyindeki kullanıcılar hem de deneyimli uzmanlar tarafından tercih edilmektedir.

En İyi Penetrasyon Testi Araçları

OpenVAS: OpenVAS (Open Vulnerability Assessment System), güvenlik açıkları taraması ve zafiyet değerlendirmesi için kullanılan bir açık kaynaklı araçtır. Bir sunucu istemcisine dayanan OpenVAS, ağ ve sistem düzeyinde güvenlik açıklarını tespit etmek için geniş bir tarama veritabanı ve kapsamlı tarama özellikleri sunar. Geniş bir raporlama ve analiz yetenekleri sayesinde kullanıcıların tespit edilen güvenlik açıklarını etkin bir şekilde yönetmelerine olanak sağlar