SecroMix

"A New Freedom of Security"

Sızma Testi / Penetrasyon Araçları

www.secromix.com ® 2020

Sızma Testi Nedir ?

Sızma Testi / Penetrasyon Testi, şirketinizin bilişim sisteminin hacker saldırılarına karşı ne kadar korunduğunu kontrol etmeyi sağlayan testlerdir. Sızma testi şirketinizin bilişim faaliyetlerini sabote etmek amacıyla kötü niyetli kişiler tarafından yapılabilecek olası saldırıları önlemeye yarayan bir ön testtir. Bu test ile iç ve dış ağ sistemleri, veri tabanları, web ve mobil uygulamaları dahil tüm sistemin güçlü ve zayıf noktaları belirlenerek olası saldırılar gerçekleşmeden önüne geçilmeye çalışılır.

Sızma testi, yetkili ve profesyonel personellerimiz tarafından yasal izinler çerçevesinde sisteminizin bir ön taraması gerçekleştirilerek yapılır ve özellikle sisteminizin zayıf noktalarını açığa çıkarmayı hedefler. Zayıf noktalar açığa çıkarıldıktan sonra bu noktaların ne gibi saldırılara maruz kalabileceği ve sisteminizin güvenlik protokollerini nasıl aşabileceği öngörülerek gerekli güvenlik önlemleri alınır. Kuruluşunuzun daha güvenilir hale getirilmesi için yasal ve yetkili kişilerce yapılan Sızma testi sisteme yönelik potansiyel tehditlerin bir bütün olarak etkisiz hale getirilmesine yardımcı olabilir.

Kuruluşunuzun olası ihlallerini önlemek ve mevcut güvenlik kontrollerini kalifiye bir saldırgana karşı güçlendirmek için **SecroMix** ekibi, özel ağ altyapısını ve uygulamalarını hedefleyen çok aşamalı bir saldırı planına dayanan Sızma testi / Penetrasyon testi hizmetleri sunmaktadır.

SecroMix
"A New Freedom of IT Security"

www.secromix.com

Sızma Testi için kullanılan

İşletim Sistemi Dağıtımları

Popüler sızma testi / penetrasyon testi araçlarının ve uygulamalarının çoğunu içeren birkaç popüler güvenlik dağıtımı vardır. Genellikle mevcut Linux dağıtımlarını temel alırlar ve revize edilmiş sürümleridir.

Kali Linux

BlackArch

Parrot Security

BackBox Linux

Gentoo Linux

NST Linux

DeftLinux

Samurai Web Testing Framework

Pentest Box

Santoku Linux

Wifi Slax

CommandoWM

Windows Tabanlı

SecroMix

"A New Freedom of IT Security"

www.secromix.com

Sızma Testi için kullanılan

Web Uygulama Araçları

Sızma ve saldırı testi araçları, güvenlik endüstrilerinde ağ ve uygulamalardaki güvenlik açıklarını kontrol etmek için sık kullanılan araçlardır. Dünya genelinde penetrasyon testi operasyonlarının yürütülmesini kapsayan araçlarının tam bir listesini bulabilirsiniz.

- Hedef sistemde hangi portların açık olduğunu **NMAP** En iyi tarama aracıdır,
- **Metasploit**, açıkları kullanarak sistemlere sızmak ve BT altyapısı güvenlik ihlallerinin diğer sonuçlarını önlemek için riskleri ve bunların eliminasyon önlemlerini değerlendirmenizi sağlayan bir tehdit aynı zamanda sızma testi çözümüdür.
- **Wireshark** ağdan geçen trafiği yakalayıp incelemek için kullanılan analizatörüdür,
- **Cuckoo** açık kaynak kodlu bir kötü amaçlı yazılım analiz sistemidir.
- Şifre kırma araçlarında en çok tercih edilen **JOHN THE Ripper ve Hydra**,
- Web trafiği kontrolü için **ZED ATTACK PROXY**
- SQL enjeksiyon için **sqlmap**,
- Kablosuz ağ güvenliği için **AIRCRACK-NG**
- Klavyeden girilen karakterlerin görüntüsünü alan **keylogger** yazılımları
- **Nikto** Web vulnerability scanner. Web sayfalarındaki güvenlik açıklarını listeler.
- Bunların yanı sıra Güvenlik açığı tarayıcıları, Web Tarayıcıları, Ağ kontrol araçları, DDoS Araçları ve komutları, Anonim olma araçları (Tor, i2p), Ters mühendislik araçları (WDK, OllyDbg), Hash Hack Araçları, fuzzdb,burpsuite gibi listeyi uzatabiliriz.

SecroMix
"A New Freedom of IT Security"

www.secromix.com

Sızma Testi için kullanılan

Bilgi Toplama Araçları

Veri toplama **sızma testi** için önemli bir rol oynar. El ile veri toplanabilindiği gibi çevrimiçi olarak ücretsiz olarak kullanılabilen araç hizmetleri de vardır. Bu araçlar ile ip tabloları, veritabanı sürümleri, veritabanları içeriği, yazılım, donanım ve hatta çeşitli üçüncü taraf eklentiler gibi bilgilerin toplanmasına yardımcı olur.

- **Arama Motorları, Sosyal Medya ve Arşiv Siteleri**
  Sızma testi / Penetrasyon testi uygulanacak hedef hakkında bilgi toplamak için kullanılacak ilk pasif araç grubu arama motorlarıdır.

- **Whois Servisleri ve Ping**
  Internet servislerinde bir alan adı ve hosting kavramı vardır. Internet üzerinde bulunan birçok Whois sitesi ile hedef sitenin alan adına, sunucusuna dair bilgilere ulaşılır.

- **Shodan.io**
  Shodan, küresel ağa bağlı cihazları endeksleyen bilgisayar güvenliği uzmanları için bir arama motorudur.

- **YouGetSignal.com**
  İçerisinde mail adresi ve telefon numarası aratma, port tarama ve ters IP adresi araması gibi birçok bilgi toplama aracını barındıran bir sistemdir.

- **Osint Teknolojisi**
  OSINT framework içerisinde kategorilenmiş halde yüzlerce bilgi toplama servislerine kaynak olan yapıdır.

Sızma Tesi için kullanılan

Adli Bilişim

Araçları

Veri toplama **sızma testi** için önemli bir rol oynar. El ile veri toplanabilindiği gibi çevrimiçi olarak ücretsiz olarak kullanılabilen araç hizmetleri de vardır. Bu araçlar ile ip tabloları, veritabanı sürümleri, veritabanları içeriği, yazılım, donanım ve hatta çeşitli üçüncü taraf eklentiler gibi bilgilerin toplanmasına yardımcı olur.

- **SOFTWARE IMAGE PROGRAMLARI:**
  Safeback v3 *Encase v 4.20 Forensic Replicatorv 3.1 PDA Seizure v 3.0.1.35 Pdd (Palm dd, Windows, Free) Forensic Toolkit (FTK) v 1.50 WinHex v 12.0NTI Image (DOS) SMART (Linux Redhat) ByteBack (DOS) v 3 Anadisk v 2.10 ILook v 8.0.8AIR-(Linux-Free) Automated Image & Restore Forensic Explorer Sans
- **UNALLOCATED ALANDA YER ALAN DOSYALARIN ÇIKARILMASI**:
  ENCASE, FTK Restorer R-Studio Autopsy Smart
- **GİZLİ BİLGİLERİN BULUNMASI:**
  Encase FTK FILTER_I V.4.1 GETSLACK, GETFREE TextSearch Plus
- **ENCRYPT(ŞIFRELI) DOSYALAR BULMAK İÇİN:**
  FTK Accent P.R. John The Ripper Rixler Office P.R. Elcomsoft Ophcrack
- **STEGONAGRAFI(VERİ GİZLEME) UYGULANMIŞ VERİLERİN TESBİTİ:**
  BlackYard DriveCrypt EzStego S-Tools Image Hide Hide and Seek
- **ZARARLI KODLARI İNCELEMEK İÇİN:**
  Encase, FTK QuickView Plus PSTools ChkRootKit Fport ve Netstat Pedestal Software Camuflage

SecroMix
"A New Freedom of IT Security"

www.secromix.com

Sızma Testi için kullanılan

Kablosuz Ağ

Araçları

Şifrelenmemiş WLAN (Açık Kimlik Doğrulama) kullanırken, kablosuz ağınız hiçbir şekilde korunmaz. AP'nin çevresinde bulunan ve bir sinyal duyabilen herkes ağa katılabilir ve ağı kullanabilir. Tüm kimlik doğrulama süreci çok basitleştirilmiştir ve kimlik doğrulama / ilişkilendirme değişimlerinden oluşur

- **Aircrack-ng**
  Veri paketlerini yakalar ve aynısını 802.11 WEP ve WPA-PSK anahtarlarının kurtarılması için kullanır.
- **Wireshark**
  Bu temelde bir ağ protokolü analizcisidir - ağ protokolleriniz, paket bilgileriniz, şifre çözme vb. Hakkında en küçük ayrıntıları sağlamak için çok kullanılır.
- **Canvas**
  Immunity's CANVAS, 400'den fazla istismar ve çoklu yük seçeneği içeren, yaygın olarak kullanılan bir araçtır. Web uygulamaları, kablosuz sistemler, ağlar vb. İçin kullanışlı hale getirir.
- **H4Rpy**
  Otomatik WPA / WPA2 PSK Saldırı Aracı
- **WiFi Passview**
  WiFi Parolanı saniyeler içinde kolayca kurtarabilen açık kaynaklı, toplu komut tabanlı bir programdır.

Sızma Testi için kullanılan

Aktif Bilgi Toplama Yöntemleri

Sızma/pentest testi yapmak için öncelikle hedefe ulaşmak gerekmektedir. Bu durum sadece sızma/pentest testleri için değil, genel olarak hackerlar tarafından da kullanılan yöntemlerdir. Çünkü sistemler karmaşık yapılardır ve hakkında ne kadar çok şey bilinirse, sızma işlemi o kadar kolay olmaktadır.

- **dirb**
  Kali Linux'a kurulu olarak gelen dirb, çok sık tercih edilen bir araçtır. Web sitelerinin görüntülenebilecek uzantılarını tespit eder ve bu uzantılar hakkında bilgiler sağlar.

- **Sandmap**
  Ağ ve sistemler bulmaya yarayan bir araçtır. Nmap Scripting Engine ve TOR desteği bulunmaktadır.

- **DMitry**
  Açık portların, e-posta adreslerinin ve subdomain (alt alan adı) gibi tarayarak, bilgiler sağlayan araçtır.

Sızma Tesi için kullanılan

Pasif Bilgi Toplama Yöntemleri

Pasif bilgi toplama yönteminde hedef ile doğrudan iletişime geçilmezken, herkese açık bilgilerin taranması yapılarak bilgiler toplanmaktadır. Bu sebeple hedef kendisi hakkında bilgi toplandığını bilmemektedir.

- **Arama Motorları**
  Arama motorları interneti tarayan devasa sistemlerdir. İnsanlar, şirketler ve toplulukların internet ortamında bırakmış oldukları dijital ayak izleri arama motorları tarafından indexlenir ve uzun bir süre boyunca arama motorlarında erişilebilir halde bulunur.
- **Online Arşiv Siteleri ve Wayback Machine**
  Online arşiv siteleri arama motorlarına benzer bir şekilde interneti tararlar ve internet üzerinde bulunan bileşenleri arşivler.
- **Netcraft**
  Web sitesinin sunucusunu, sunucunun işletim sistemini ve arka planda çalışan yazılımlarını tespit eden bir web sitesidir.
- **Whois**
  Web sitesinin yayınlandığı alan adının kime ait olduğunu sorgulayan sitedir. Adres, e-posta adresi ve telefon numarası gibi kritik bilgileri sağlayabilmektedir.
- **TinfoLeak**
  Twitter hesaplarını kullanarak hedefteki kişinin bilgilerini toplamaya yarayan bir araçtır.

SecroMix
"A New Freedom of Security"

Neden SecroMix?

Ekibimiz, en prestijli CTF hack yarışmalarına ("Capture the Flag") katılan penetrasyon testi deneyimine ve gerekli sertifikalara sahip (CEH, LPT,…), standartlara uygun (KVKK, GDPR, BDDK, TSE, PCI DSS, ISO 27001) araştırmacı ve hata ödül programlarında başarılı katılımcıları içerir.

Firma olarak riskleri azaltmak, tüm güvenlik açıklarını düzeltmeye yardımcı olmak ve bilgi güvenliği sürecinize destek sağlamak için ayrıntılı öneriler ve özel planlar sunuyoruz.

Unutmayın sistem sızma testleri/pentest/penetrasyon testleri, herhangi bir kuruluş için bilgi güvenliğinin gerekli bir unsuru olmazsa olmazlarındandır.

SecroMix
"A New Freedom of IT Security"

www.secromix.com