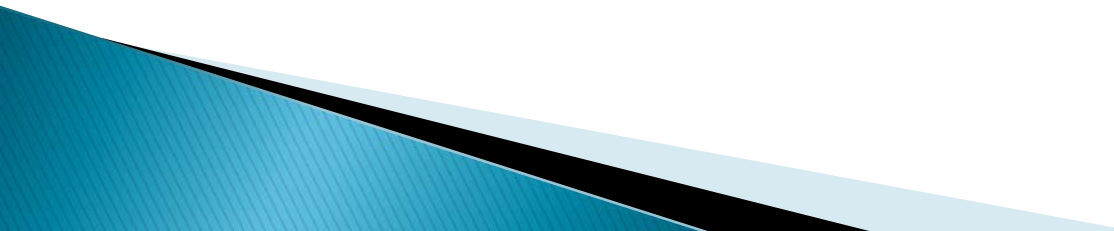


Penetration Test and Tools

Penetration Test nedir?

- ▶ Herhangi bir bilgisayar sistemini ya da bilgisayar ağını sistem sahibinin bilgisi dahilinde olası saldırı senaryolarıyla test etmek ve sistemin bu tür saldırılar karşısındaki dayanıklılık seviyesini ölçmek ve değerlendirmektir. Bu testlerin amacı sistemlerin güvenlik seviyesini değerlendirmek ve olası kötü niyetli saldırılar öncesinde sistemlerin açıklarını kapatarak, kurum/kuruluş ya da şirketlerin veri/itibar ve çoğu zaman da para kayıplarını önlemektir.

Test Aşamaları

- ▶ Sistemlerin türüne göre özelleşebilecek sızma testleri genel manada 3 aşamadan oluşur;
 - ▶ **Bilgi toplama**
 - ▶ **Saldırı senaryolarının uygulanması**
 - ▶ **Raporlama**
- 

Test Aşamaları

- ▶ **Bilgi Toplama**
- ▶ Bilgi toplama aşamasında sistemle ilgili erişilebilecek bütün bilgilere ulaşılarak sistemin saldırı yüzeyi belirlenir. Pasif veya aktif olarak gerçekleştirilebilecek bu aşamada sistemin dışarıyla olan bütün iletişim noktaları belirlenerek bu noktalarda çalışan servislerin veya politikaların doğruluğu ve güvenliği kontrol edilir. Bu kontroller sistemin web ara yüzünde kanal güvenliği için kullanılan algoritmanın anahtar uzunluğu detayında bir teknik bilgi olabileceği gibi, giriş kapısında kimlik kontrolü yapan güvenlik görevlisinin sosyal mühendislik (social engineering) uygulanarak aldatılabilme riskine kadar bütün noktaların tespit edilmesini içerir. Bu kısımda toplanan veriler saldırı senaryolarının hazırlanması sırasında kullanılır.

Test Aşamaları

- ▶ **Saldırı Senaryolarının Uygulanması**
- ▶ Bu aşamada 1. kısımda toplanan bilgiler çerçevesinde belirlenen saldırı senaryoları sistem üzerinde test edilir. Bu testlerin amacı sistem içerisindeki servis, veri veya alt sistemlerin ele geçirilmesi ve/veya kötüye kullanılmasıdır. Bu testler sistem sahibinin bilgisi dahilinde olup servis kesintisi gibi kalıcı zararlara sebep olabilecek testler yine ortak alınan kararlar çerçevesinde uygulanır. Bu testlerden başarılı olanlar raporlama aşamasında çözüm yöntemleri ile birlikte sistem sahibine raporlanır.

Test Aşamaları

- ▶ **Raporlama**
- ▶ Sızma testlerinin son aşaması olan raporlamada, önceki aşamada bulunan bilgi ve belgeler derlenerek sistem sahibine iletilir. Bu bilgiler özetle; bulunan sistem zafiyetleri ve çözüm yöntemleri, zafiyetlerin önem/öncelik sıralaması, sistemin genel görünümü, sistemin açık olduğu tehditler ve sahip olduğu riskler ve test kapsamına özel çıktılarıdır.

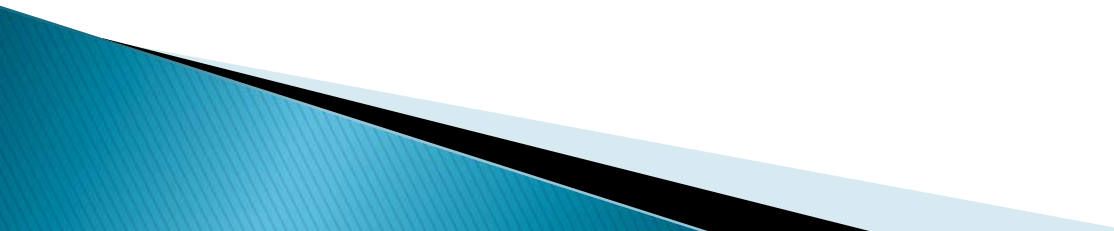
Test Çeşitleri

- ▶ Whitebox
 - ▶ Blackbox
 - ▶ Graybox
- 

Test Çeşitleri

- ▶ **Whitebox**
- ▶ Kurum ve kuruluşların bilgi sistemleri uzmanları tarafından, kullandığı sistemler hakkında detaylı bilgiler öğrenildikten sonra oluşturulan sızma senaryolarının yürütülmesidir.

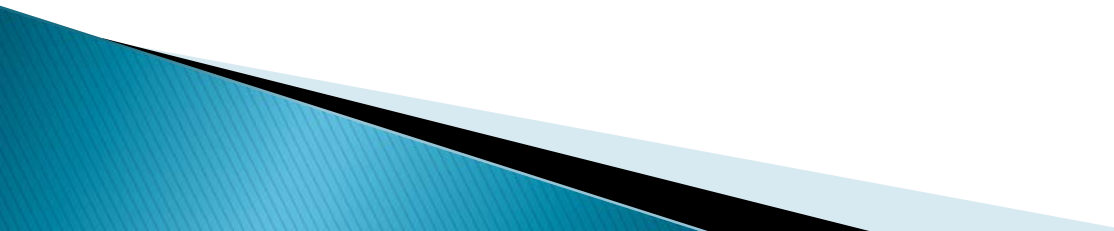
Test Çeşitleri

- ▶ **Blackbox**
 - ▶ Kurum ve kuruluşlardan, kullanılan bilgi sistemleri hakkında bilgi alınmadan; önceden belirlenen sızma senaryolarını uygulanmasıdır.
- 

Test Çeşitleri

- ▶ **Graybox**
- ▶ Whitebox ile Blackbox karışımı olan bir kategoridir. Sızma testi sadece belirli sistemlere yapılır ve bu sistemler hakkında detaylı bilgilendirme yapılmadan sistemlerin sınanmasıdır.

Penetration Tools

1. Ağ dinleme araçları
 2. Port tarayıcılar
 3. Açıklık tarayıcılar
 4. Açıklık gerçekleştirme araçları
 5. Paket üreticileri
 6. Topoloji çıkarım araçları
 7. İşletim sistemi tespit araçları
 8. Şifre kırma araçları
 9. Kablosuz ağ araçları
 10. VPN test araçları
 11. Web güvenliği test araçları
 12. Veritabanı test araçları
- 

Penetration Tools

- ▶ Ağ Dinleme Araçları
- ▶ Ağ ve sunucu trafiğini izlemek için ve ağ dinlemek için kullanılan araçlardır.

Penetration Tools

Ağ Dinleme Araçları

Wireshark

- ▶ Ağ dinleme araçları arasında en çok kullanılan ve en yaygın olanı eski adıyla Ethereal, yeni adıyla Wireshark programıdır.
- ▶ Wireshark açık kaynak kodlu bir yazılımdır ve internetten ücretsiz olarak indirilebilir. Hem Windows hem de Linux işletim sistemleri üzerinde çalışmaktadır. Wireshark trafiği kaynak adres, hedef adres, kaynak port, hedef port gibi belirli kriterlere göre yakalayabilmektedir. Ayrıca izlenen trafik sonradan incelenmek üzere kaydedilebilir. Bu program aynı zamanda kablosuz ağları da dinleyebilmektedir.

Penetration Tools

Ağ Dinleme Araçları

Ettercap

- ▶ Ettercap programı da açık kaynak kodlu bir yazılımdır.

Hem Windows hem de Linux üzerinde çalışabilmektedir. Bu program şifreleri ve kullanıcı isimlerini yakalayabilmektedir (Örneğin: Telnet, FTP, http, SNMP vb...). Ettercap programı ile araya girme saldırısı yapılabilmektedir. Bunun sonucunda kurulu olan bağlantılar izlenebilmektedir ve bu bağlantılar kesilebilmektedir.

Penetration Tools

- ▶ Port Tarayıcılar
- ▶ Hedef makine de ne kadar çok açık port varsa, açıklık potansiyeli de o kadar fazla olmaktadır. Bu yüzden kullanılmayan portların kapatılmış olması gerekir. Hedef bilgisayar üzerinde açık olan portlar, port tarayıcı yazılımlar ile tespit edilmektedir.

Penetration Tools

Port Tarayıcılar

NMAP

- ▶ En yaygın olarak kullanılan port tarayıcı programıdır. Nmap, açık kaynak kodlu bir yazılım olup ücretsizdir. Hem Windows hem de Linux üzerinde çalışabilmektedir. Nmap programının en önemli özellikleri şunlardır:
 - TCP ve UDP port taraması yapabilmektedir.
 - İşletim sistemi tespiti yapabilmektedir.
 - Çalışan servisleri tespit edebilmektedir.
 - Yazılımların sürümünü tahmin edebilmektedir.
 - Bir ağdaki canlı bilgisayarları tespit edebilmektedir.
 - Raporlama yeteneği bulunmaktadır.
- ▶ Test sonucunda HTML formatında raporlar çıkarmaktadır. Nmap, komut satırıyla çalışan bir programdır. Ancak, Zenmap isminde kullanıcı arayüzüne sahip olan sürümü de çıkmıştır.

Penetration Tools

- ▶ Açıklık Tarayıcılar
- ▶ Açıklık tarayıcı programlar, herhangi bir bilgisayarda veya bilgisayar sisteminde bulunan açıklıkları veya servisleri tespit eden programlardır. Bunlardan en yaygın olanları Nessus, GFI Languard, Microsoft Baseline Security Analyser, Internet Security Scanner, NetIQ, Foundstone vb... programlardır.
- ▶ Bazıları tüm sistemler üzerindeki açıklıkları taramayı hedeflemesine rağmen bazıları sadece iç ağ da konumlandırılarak belirli işletim sistemleri için açıklıkları yakından takip edip raporlamaktadır.

Penetration Tools

Açıklık Tarayıcılar

Nessus

- ▶ Açıklık tarayıcı olarak kullanılabilecek en önemli programdır.
- ▶ Nessus, hem Linux hem de Windows işletim sistemleri üzerinde çalışmaktadır. Tenable firması tarafından ticari sürümleri de satılmaktadır. Bilinen açıklıkları, işletim sistemleri ve servis tespiti yapabilmektedir. Domainle entegre olarak çalışabilmekte olup html, xml, latex gibi değişik formatta raporlar üretebilmektedir.

Penetration Tools

- ▶ Açıklık Gerçekleme Araçları
- ▶ Güvenlik açıklığı gerçekleştirme programları sistemde bulunan bazı açıklıkları hedef cihaza uygulayabilmektedir. Bu programlar kendileri açıklık taraması yapabilmesinin yanında diğer açıklık tarayıcı programlarla entegre edilerek, onların bulduğu açıklıkları gerçekleyebilmektedir.

Penetration Tools

Açıklık Gerçekleme Araçları

Metasploit

- ▶ Açık kaynak kodlu bir program olup hem Windows hem de Linux işletim sistemleri üzerinde çalışabilmektedir.
- ▶ 261 tane açıklık tanımı, 76 tane payload içermektedir. İstendiğinde yeni açıklıklar eklenebilir.

Penetration Tools

- ▶ Paket Üreteçleri
 - ▶ Paket üreteçleri karşıdaki sisteme özel bir paket göndermek için kullanılan programlardır. Bu programlar aşağıdaki amaçlar için yaygın olarak kullanılır:
 - TCP/IP yığını test etmek
 - Güvenlik duvarı kural tablosunu test etmek
 - Parçalı paketler göndermek
 - Pakete ait bayrakları (flag) değiştirerek sistemin işletim sistemini tanımak
 - Sistemi devre dışı bırakmak ya da ele geçirmek
 - Yakalanmış paketleri göndererek bağlantı kurmaya çalışmak
 - İleri düzey port tarama
- Hping (<http://www.hping.org>), Nemesis, Engage Packet Builder ve TCPreplay programları paket üreteç programlarına örnek olarak verilebilir..

Penetration Tools

- ▶ Topoloji Çıkarım Araçları
- ▶ Hedef sistemde yer alan cihazların konumlarını tespit etmek ve topolojisini elde etmek için topoloji çıkarım araçları kullanılır. Bu alanda en önemli araçlardan biri sıklıkla kullanılan ping komutudur. Ping komutu çoğu işletim sisteminde bulunmaktadır. Bu komut kullanılarak hedef cihazın ayakta olup olmadığı tespit edilir.

Penetration Tools

- ▶ Topoloji Çıkarım Araçları
- ▶ Ping komutuna benzer bir yapıda çalışan diğer bir komut tracert komutudur. Bu komut hedef cihaza giden yol üzerindeki cihazları (yönlendirici, güvenlik duvarı, anahtar vb...) tespit etmek için kullanılır. Tracert komutuna benzer çalışan ama ICMP protokolü ile değil, TCP protokolü vasıtasıyla cihaz tespiti yapan Tcptraceroute komutu da oldukça kullanışlıdır. Örneğin hedef ağda bulunan bir web sunucu ve 80 numaralı tcp portu kullanılarak, Web sunucuya giden yol üzerindeki cihazlar kolaylıkla tespit edilebilir.

Penetration Tools

- ▶ İşletim Sistemi Tespit Araçları
- ▶ Hedef cihazda çalışan işletim sistemini tespit etmek, bir saldırgan için en önemli aşamalardan biridir. Bu işlemi yapmak için işletim sistemi tespit araçları kullanılır. Bu araçlardan en önemlileri Hping, Xprobe2, P0F, Nmap programlarıdır.

Penetration Tools

İşletim Sistemi Tespit Araçları

- ▶ **Hping** değişik ICMP paketleri göndererek karşı cihazın işletim sistemini tespit etmeye çalışır.
- ▶ **Xprobe2** hedef cihazda çalışan işletim sistemine ait tahminler ve bu tahminlerin doğruluğuna ilişkin yüzdeler vermektedir. Linux işletim sisteminde ve komut satırında çalışmaktadır.

Penetration Tools

- ▶ Şifre Kırma Araçları
- ▶ Hedef cihazda çalışan bir servise ait kullanıcı adını ve parolayı kırmak için şifre kırma araçları kullanılmaktadır. Örneğin bir yönlendiricinin yönetimini ele geçirmek için şifre kırma araçları kullanılabilir. Bu araçlar vasıtasıyla yönlendiriciyi yönetmek için kullanılan kullanıcı adı ve parola elde edilebilir. Bu araçlara örnek olarak Cain and Abel, Brutus, Hydra ve L0phtCrack programları verilebilir.

Penetration Tools

Şifre Kırma Araçları

- ▶ Bu araçlardan Cain and Abel, ücretsiz bir yazılımdır. Kullanım alanları şu şekilde verilebilir:
 - Ağı dinleyerek şifreleri yakalama
 - Sözlük (dictionary) veya kaba kuvvet (bruteforce) saldırısıyla şifre kırma
 - Saklanmış şifreleri kırma
 - Çevrimdışı şifre kırma

Cain and Abel pek çok protokolde şifre kırma işlemi gerçekleştirebilmektedir. FTP, HTTP, SMTP, POP3, TELNET ve VNC bu protokollerden sadece bir kaçıdır. Cain and Abel şifre kırma yeteneği dışında, ağdaki saldırı tespit sistemlerini tespit etme, araya girme saldırısı yapma, SSH-1, HTTPS protokollerine ait trafiği kaydedip çözme yeteneklerine de sahiptir.

Penetration Tools

- ▶ Veritabanı Test Araçları
- ▶ **ISS Database Scanner** güvenlik açıklıklarını ve yanlış konfigürasyonları tespit etmek için kullanılan ticari bir yazılımdır (<http://www.iss.net>). Bu açıklıklar veritabanında bulunan yama eksiklikleri, varsayılan kullanıcı şifrelerinin değiştirilmemesi ya da basit şifreler verilmesi gibi açıklıkları test eder.

Penetration Tools

Veritabanı Test Araçları

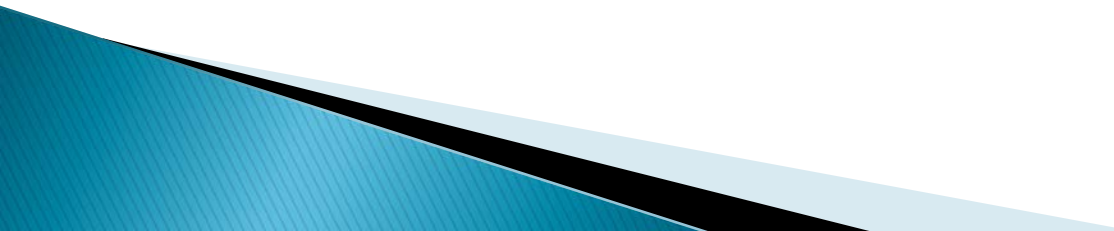
- ▶ Oracle, MSSQL ve Sybase veritabanları üzerinde tarama yapılabilir. Seçilen bir sözlük üzerinden veritabanı kullanıcı şifreleri için sözlük atağı yapılabilir. Veritabanının üzerinde koştuğu işletim sisteminin veritabanı ile ilgili özelliklerini de tarayabilmektedir (Veri tabanı kurulduktan sonra ona ait dosyalar üzerindeki hakları kontrol eder). ISS veritabanı tarayıcısının etkin bir raporlama aracı vardır.

Penetration Tools

Veritabanı Test Araçları

- ▶ **Bruteforce Script**, varsayılan kullanıcı isimleri ve şifreleri ile veritabanlarına bağlantı yapmaya çalışan bir perl betiğidir. Bağlanılmak için istenilen veritabanının IP adresi port numarası ve kullanıcı isim/şifrelerinin olduğu bir dosya girilir. Bu script üzerinde yapılan değişikliklerle Oracle veritabanının değişik sürümlerinin parola bilgilerinin kontrolü yapılabilmektedir.

Penetration Tools

- ▶ Web Güvenliği Test Araçları
 - ▶ Günümüzde uygulama güvenliği diğer güvenlik araçlarının da önüne geçmiştir. Çünkü uygulamalar genellikle sınırlı bir ekip tarafından geliştirilmekte ve test edilmektedir. Bu da bilinen genel güvenlik yazılım ya da donanımlarına göre daha çok açıklık barındırmalarına sebep olmaktadır.
- 

Penetration Tools

Web Güvenliği Test Araçları

- ▶ **Paros**
- ▶ Genellikle internet tarayıcı ara yüzünden girilmesine izin verilmeyen karakterlerin uygulama yazılımına gönderilmesi için kullanılır. Aynı şekilde uygulama yazılımına paketler gönderilirken yakalanarak içerikleri değiştirilip gönderilebilir. Ya da daha önceden yakalanmış olan paketler gönderilir. Bunların sonucunda uygulama devre dışı bırakılmaya zorlanabilir ya da uygulamanın yapısı hakkında bilgi toplanabilir. Paros kullanılarak ağın haritası çıkarılabilir. Buradan ağın haritasına bakılarak hangi sayfaların olduğu kolayca görülebilir. Web testi kısmında ise injection, oturum numarası tahmin etme gibi birçok açıklığı uygulama üzerinde deneyebilir

Penetration Tools

Web Güvenliği Test Araçları

- ▶ **FireBug**
- ▶ Mozilla Firefox'un bir uzantısı olarak çalışır.
- ▶ Platformdan bağımsız olarak çalışır. Web abilir. sayfasının istenilen herhangi bir yerine gelindiğinde o kısımla ilgili kodu gösterebilir ve o kısımda inceleme yapılabilir. O kısmın kodu kolayca değiştirilebilir. Bu araç hem geliştiriciler hem de testçiler tarafından etkin olarak kullanılır

Kaynaklar

- ▶ <http://oktay-sahin.blogspot.com/2009/01/gvenlii-test-aralar-penetration-tools.html>
- ▶ <http://omerbulenthayirli.blogspot.com/2012/05/penetration-test-tools.html?zx=ca07f2992ddad0af>
- ▶ <http://www.cyber-security.org.tr/Madde/787/Penetration%20Testing>
- ▶ <http://www.btyon.com.tr/sizma-testi.php>
- ▶ <http://www.bga.com.tr/danismanlik/bga-sizma-test-penetration-test-hizmetleri/>