F.Ü. Mühendislik Fakültesi

Bilgisayar Mühendisliği Bölümü

Bilgisayar Sistemleri Laboratuvarı

DENEY NO: 4
PENETRASYON TESTİ

Deneyin Amacı:

Etik saldırının ve ağ güvenliğinin yapısının ve adımlarının anlaşılması ve bu saldırıda kullanılan yöntemlerin ve araçların incelenmesi ve kullanımıdır.

Penetrasyon Testi nedir?

Penetrasyon Testi; pen test, etik hack, beyaz şapkalı hack olarak da adlandırılabilir. Bu test; bilgisayar ağının ya da sisteminin içeriden ya da dışarıdan gelebilecek saldırılara karşı ne kadar güvende olduğu konusunda fikir edinilmesini sağlar. Bu test sistemin güvenli olmasını sağlamak amacıyla, yasal ve izinli olarak açıklarının aranmasıdır. Bu sayede sistemin zayıf noktalarının tespiti ve saldırı düzenlenerek sistemin gerçek bir hacker'ın saldırısına karşı savunmasız olup olmadığı belirlenir. Sonuç olarak sistemin ve verilerin ne kadar güvende olduğu sorusu spesifik bir sorudur ve cevabı görecelidir. Penetrasyon testi bu sorulara objektifcevaplar bulmaya yardımcı olur.

Penetrasyon testi; dos, application (uygulama), internet, intranet, process gibi farklı bölümler içerebilir. Bu test bu bölümlerin birini veya bir kaçını kaplayacak şekilde yapılabilir.

- Dos testinde şirketin herhangi bir saldırıda hizmetlerinin çöküp çökmeyeceği ve bu saldırıya karşı dayanıklılığı test edilir.
- Application (uygulama), kısmında kullanılan uygulamalar ve kodlarında açık taraması yapılır. Kullanılan uygulamaların güncelliğinin korunması, iç ağın durumunun test edilmesinde bu testler kapsamındadır.
- Dış ağın penetrasyon testinde(intranet) yapılanmanın dış dünyadan gelebilecek herhangi bir tehdide karşı durumu tespit edilir. Örnek olarak web siteye gelebilecek herhangi bir saldırı bu kapsamdadır.

Şirketler pentest ile her türlü saldırıya karşı kendilerini hazırlayabilir ve saldırıya gerekli tedbiri alabilirler. Böylelikle bir saldırı durumunda ya hiç etkilenmezler ya da en az zararla saldırıyı atlatabilirler. Dışarıdan saldırgan bakış açısıyla güvenlik açıklarının kontrolü ve raporlanması güvenlik açısından önemlidir. Şirketlerin kendi içlerindeki güvenlik tedbirleri çoğunlukla yeterli olmamakta ve önlemler güncelliğini koruyamamaktadır. Ayrıca kötü niyetli hackerların sayısının artması ve bilgi düzeylerinin genellikle birçok şirket çalışanından önde olması pentestin önemini ortaya koymaktadır. Pentest bir şirketin bilişim sistemleri için iç ve dış tehditlere karşı güncel önlemler alınmasını ve zafiyetlerin giderilmesini sağlar. Bununla birlikte bu testlerin faydaları aşağıdaki gibi sıralanabilir.

- Saldırılara karşı daha dirençli bir bilişim altyapısı
- Kullanıcı bazlı olarak bilgi güvenliği farkındalığının artması
- Sistemlerin durdurulma veya kaynak doldurmaların engellenmesi
- Yasal olarak uyum sağlama
- Kurum prestijinin ve marka değerinin korunması sağlanır.
- BT kaynaklı risklerinin azalması

Pen testinde Hack sanatında üç terimin sıklıkla kullanılır. Bunlar Beyaz şapkalı (White hats), siyah şapkalı (black hats) ve gri şapkalı (gray hats). Beyaz şapkalılar art niyetli olmayan ve sistemlerin savunmalarını güçlendirmek amacıyla pen test yapan hacker'lardır. Siyah şapkalılar aynı zamanda crackers olarak da adlandırılırlar ve art niyetli amaçlar için hack'i kullanırlar. (Kredi kartı bilgilerinizi çalarak satmak ya da firma sırlarını çalmak gibi…) Bu amaçla beyaz şapkalıların siyah şapkalıların kullandıkları araç ve yöntemleri bilmeleri önemlidir böylece siyah şapkalıların bir adım önünde kalarak art niyetli eylemlerini engelleyebilirler. Gri şapkalılara ise beyaz ve siyah şapkalıların kombinasyonudur ve genellikle yapabildikleri için ya da meydan okumayı sevdikleri için hack'lerler.

Penetrasyon Testinin Adımları

- **Bilgi toplama:** Sistem hakkında ön bilgi edinmek. internet, rakip bilgileri, WHOIS, DNS, ağ, web sitesi, e-posta, Google yoluyla olabilir. Whois, bize aradığımız hedefin alan adı bilgilerini ve dns sunucularını verir. Alan adları ve yapıları bize hedef hakkındaönemli bilgiler verir.
- **Tarama:** Sistemi tarayarak bilgi edinmek. (Sistemdeki bilgisayarlar ve network

cihazlarını tespit etmek, sistemdeki cihazlarda bulunan açık portların tespiti, sistemdeki açıklarının taranması vs.)

- **Erişim Sağlama:** Sistemde bulunan açıklar kullanılarak sisteme izinsiz erişim sağlanması. (yetki yükseltme, sistem durdurma, kaynakların doldurulması, yetkisiz erişim sağlama)
- **Erişim Koruma:** Elde edilen erişimin korunması. (sistem üzerinde elde edilen erişim haklarını kalıcı kılma, sistem üzerinde yetkili bir kullanıcı oluşturma, arka kapı açma).
- **İzleri yok etme:** Hedef sistem üzerinde ilk dört adımda yapılan işlemlerin bıraktığı izler (log kaydı gibi) temizlenir veya kirletilir. (APT-Advanced Persistent Threat).

Penetrasyon Test Araçları

Bilgi güvenliği, özellikle e-ticaret ve e-devlet uygulamalarının yaygınlaşmasıyla birlikte oldukça önemli bir hâle gelmiştir. Bilginin güvenli bir şekilde iletilmesi, işlenmesi ve saklanması bilişim uzmanlarının başlıca görevlerinden birisi olmuştur. İletilen bilginin veya bilgiyi ileten sistemin gerekli güvenlik özelliklerini sağlayıp sağlamadığını test etmek ve denetlemek için ağ güvenliği test ve denetim araçları kullanılmaktadır. Bu araçlardan bazıları ücretsizdir, bazıları ise belirli bir ücretlendirmeye tabidir. Ağ güvenliği test ve denetim araçlarının birçoğu Backtrack altında toplanmıştır. Backtrack, Linux işletim sistemi üzerine kuruludur ve CD'den boot edilerek kullanılmaktadır.

Ağ güvenliği test ve denetim araçları aşağıdaki başlıklar altında gruplandırılabilir:

1. Ağ dinleme araçları
2. Port tarayıcılar
3. Şifre kırma araçları
4. Web güvenliği test araçları
5. Genel Amaçlı Güvenlik Açığı Tarayıcılar

1. Ağ Dinleme Araçları

Ağ ve sunucu trafiğini izlemek için ve ağ dinlemek için kullanılan araçlardır. Ağ dinleme araçları arasında en çok kullanılan ve en yaygın olanı 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. Wireshark'ın kurulumu kullanımı ile ilgili geniş anlatıma sahip bir kayağa*http://www.enderunix.org/docs/wireshark.pdf*

Ping ve Ping Sweeps

Ping özel bir network paketi olup ICMP packet olarak adlandırılır. Ping sweep(pingtaraması) yapmanın en kolay yolu FPing adlı aracı kullanmaktır. FPing'i kullanmak için terminali açarak;

fping –a –g 172.16.45.1 172.16.45.254>hosts.txt

2. 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.

En yaygın olarak kullanılan port tarayıcı program Nmap yazılımıdır 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.

Kullanımı için;

Nmap –p 192.168.56.101

-p hedef makinedeki tüm portların taranması anlamını taşır.

HTTrack

Pen testimize hedef siteyi gözden geçirerek başlamak isteriz. Bu amaçla HTTrack adlı araç kullanılarak web sitesinin sayfa sayfa kopyası çıkarılabilir. HTTrack web sayfasının sayfa sayfa ofline kopyasını çıkaran ücretsiz bir programdır. Kopyalanan web sitesi tüm sayfaları, linkleri, resimleri ve orijinal web sitesinin kodlarını içerir ancak tüm bunlar sizin lokal bilgisayarınızda bulunur. HTTrack gibi bir araç kullanarak siteye offline erişim sağlanması şirketin web sunucusunda uzun zaman geçirerek dikkat çekmenin önün geçer. Ve sitenin içeriklerine geniş ulaşım imkânı sağlar. HTTrack işini bitirince hedef sitenin tam bir offline kopyası inceleme için bilgisayarınızda hazır bulunacaktır.

3. 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 ve Hydra programları verilebilir.

Bu araçlardan Cain and Abel, ücretsiz bir yazılımdır (Linkleri Görebilmek İçin Üye Olun veya Giriş Yapın.). Sadece Windows işletim sistemleri üzerinde çalışabilmektedir.

Medusa

Medusa, brute force (kaba kuvvet) yöntemini kullanarak şifreyi tahmin etmeye çalışan ve uzak servislere erişim sağlayan bir araçtır. Medusa FTP, http, MySQL, Telnet, VNC, Web Form ve daha pek çok servise saldırı yapma yeteneğine sahiptir. Medusanın kullanılabilmesi için bellibilgilere ihtiyaç duyulur bu bilgiler;

- Hedef IP adresi
- Girişi yapmak için kullanılacak kullanıcı adı veya kullanıcı adı listesi
- Şifre ya da şifre olarak kullanılacak bir sözlük
- Giriş yapmak istediğini servisin adı

Medusa, Backtrack 5'de yüklü olarak gelmektedir. Ancak başka bir sürüm ya da dağıtım kullanıyorsanız yüklemek için konsolda;

```
apt-get update apt-get install medusa
```

Daha önceki bölümlerde yapılan araştırmalardan elde edilen e- mail adresleri ya da hesap isimleri ve şifreler bu bölümde Medusaya girilir. Medusa gibi programlar bu kullanıcı isimlerini ve şifreleri kullanarak başarılı olana kadar denerler. Burada dikkat edilmesi gereken önemli bir nokta günümüz sistemlerinin belirli sayıdaki denemenin ardından saldırınızı fark edip IP'nizi kilitleyebileceğidir. Elbette ki dijital izleriniz kayıt altına alınacak ve sistem yöneticisi uyarılacaktır. Şifresini denediğiniz kullanıcı adının kilitlenmesi de ihtimal dâhilindedir.

Çeşitli şifre listeleri(sözlükler-dictionary) internette bulanabileceği gibi sıklıkla kullanılan şifreleri içeren bir liste Backtrak'da mevcuttur;

/pentest/passwords/wordlists/

Brute-force saldırıyı gerçekleştirmek için konsolda;

medusa –h target_ip –u username –P path_to_password_dictionary –M service_to_attack

-h Hedef hostun IP adresi

-u Medusanın kullanacağı tek kullanıcı adı

-P şifre listesi-Kelime sözlüğü-dictinary file- yolu

-M saldırılacak servis

4. 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. Bu yüzden piyasada bu tür araçlar hızla artmaktadır. Web uygulama güvenliği alanında en önemli araçlardan bazıları şunlardır. Paros, açık kaynak kodlu bir yazılımolup platform bağımsız çalışmaktadır

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. FireBug, Mozilla Firefox'un bir uzantısı olarak çalışır Platformdan bağımsız olarak çalışır. Web 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 kullanılabilir.

Ticari bir yazılım olan Acunetix, Windows işletim sistemi üzerinde çalışmakta olup version check, CGI kontrol, parametre değişimi, dosya kontrolü, dizin kontrolü gibi testleri yapmaktadır Bu testleri yaparken istenilen testler için profiller oluşturularak sadece seçilen testlerin yapılması sağlanmaktadır. Uygulama açıklığı taraması yapmaktadır. İstenilen açıklıkları ekleyebilme yeteneği mevcuttur. Yapılan açıklıklarla ilgili detaylı raporlar üretmesinin yanında tek tuşla internetten güncellenebilmektedir.

Netsparker

Netsparker, bir web uygulaması güvenlik tarayıcısıdır. Otomatik olarak bir web sitesini uygulama seviyesindeki güvenlik açıklarına karşı analiz edip güvenlik açıklarını raporlar. Ek olarak raporlamanın bir adım da ötesine geçip güvenlik açıklarını kullanarak aynı bir saldırgangibi sistemden veri çıkartabilir ya da sisteme tam erişim sağlayabiliyor. Bu sayede SQL Injection, Cross-site Scripting gibi açıkları bulmayı sağlar.

Acunetix Web Vulnerability Scanner

Sadece web uygulamalarını denetlemekle kalmamakta, aynı zamanda web uygulamasının bulunduğu sunucu da tüm saldırı yöntemlerine göre denetlemektedir. Serverda bulunan güvenlik açıklarını bize belirtmektedir. Kendi Crawler'ı ile bize web sunucu tipini ve dilinigöstermektedir. Tüm kodlama dillerinin güvenlik açıklarını tarar.

Webinspect

WebInspect, web uygulamalarındaki güvenlik açıklarını, kodlama hatalarını bulup çözüm önerileri getirerek güvenlik duvarı ve saldırı tespit sistemleri için tamamlayıcı bir rol oynar. WebInspect çözümünün kolay yönetilen arayüzü, genişletilebilen fonksiyonları ile ister test ortamında, ister gerçek ortamında, web uygulamalarınızı ve web servislerinizi güvenlik değerlendirmesinden en doğru sonuçları elde ederek geçirebilir. WebInspect kullanıcılara, herhangi bir web uygulamasının ve/veya web servisin in teknolojilerinin uygulama günveliği

açısından denetleme ve olası riskleri bulma olanağı sunar.

5. Genel Amaçlı Güvenlik Açığı Tarayıcılar

Metasploit

Bu penetrasyon testi için en gelişmiş ve en popüler olanıdır. Güvenlik önlemlerini aşmak ve belli bir sisteme girebilecek "Exploit" kavramına dayalıdır. Eğer hedef bir makinede başarılı olduysa, penetrasyon testi için mükemmel bir kod çalıştırır. Web uygulamaları, ağlar, sunucularve benzerleri üzerinde kullanılabilir.

Qualys

Açık tespiti için kullanacağınız programların yanında doğrudan bu iş için tasarlanmış web sitelerine bağlanarak çevrimiçi açık tespiti yapabilirsiniz. Qualysguard Enterprise Intranet Scanner hizmeti böylesi bir açık hat web sitesidir

Nessus

Linux'ta sıkça kullanılan, kapsamlı bir güvenlik açığı tarama yazılımıdır. Kişisel ve hertür kurumsal olmayan kullanım için ücretsizdir. Genel amacı, bilgisayar sistemlerinde ve bilgisayar ağlarında potansiyel güvenlik açıklarını tespit etmektir. Nessus bir port tarama yazılımından çok daha üstün özelliklere sahiptir. Nessus, servislerdeki açıkları eklentilerinin güncelliğine bağlı olarak test edebilir. Çalışma prensibi istemci/sunucu biçimini kullanır ve test edilecek sistemde nessus sunucu yazılımının açık olması daha derinlemesine test ve analiz imkânı sunar.

Örnek Uygulamalar:

1) Ping sweep işlemini gerçekleştiriniz.
2) TCP ve UDP Port tarama işlemini gerçekleştiriniz.
3) Ağda görünen kullanıcı adı ve şifreleri bir log dosyasına yazan bir uygulama gerçekleştiriniz.
4) Ağ trafiğinin istatistiğini çıkaran bir uygulama gerçekleştiriniz.
5) Ağdaki DHCP trafiğini yakalayarak ağ bilgisi çıkaran bir uygulama gerçekleştiriniz.
6) SMTP protokolü için kaba kuvvet saldırısı (brute force attack) yapan bir uygulama gerçekleştiriniz.

7) FTP protokolü için kaba kuvvet saldırısı (brute force attack) yapan bir uygulama gerçekleştiriniz.

Kaynaklar:

1. http://backtracktutorials.com/backtrack-basics
2. "METASPLOIT The Penetration Tester's Guide" by David Kennedy, Jim O'Gorman,Devon Kearns, and Mati Aharoni
3. "The Basics of hacking and penetration Testing Ethical hacking and penetration TestingMade Easy" by Patrick Engebretson