

Ağ Güvenliği Test ve Denetim 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. Bu yazıda ağ güvenliği test ve denetim araçlarından en çok kullanılan ve en etkili olanlar anlatılacaktır.

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. 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

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 eski adıyla **Ethereal**, yeni adıyla **Wireshark** programıdır (<http://www.wireshark.org>). Wireshark açık kaynak kodlu bir yazılımdır ve internette 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 ağı da dinleyebilmektedir.

Diğer bir ağ dinleme programı da **tcpdump** açık kaynak kodlu yazılımıdır (<http://www.tcpdump.org>). Tcpdump, Linux işletim sisteminde çalışabilmektedir. Windows işletim sisteminde çalışan sürümü ise **windump**'tır.

Ettercap programı da açık kaynak kodlu bir yazılımdır (<http://ettercap.sourceforge.net>). 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.

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 (<http://nmap.org>). 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.

Nmap kadar yaygın olmayan diğer bir port tarama yazılımı **Superscan** programıdır. Bu programda ücretsiz olarak elde edilebilmektedir. Windows işletim sistemi üzerinde çalışabilmektedir. Basit bir kullanıcı arayüzüne sahiptir. TCP ve UDP portlarını tarayabilmektedir. Nmap programına göre daha sınırlı özelliklere sahiptir.

3. 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.

Açıklık tarayıcı olarak kullanılabilir en önemli program olan **Nessus**, Tenable şirketi tarafından ticari bir ürün olarak satılmaktadır (<http://www.nessus.org/nessus>). Bunun yanında açık kaynak kodlu olarak da kullanılabilir. Nessus, hem Linux hem de Windows işletim sistemleri üzerinde çalışmaktadır. Tenable firması tarafından ticari sürümleri de satılmaktadır. Bilinen açıklıkları, işletim sistemleri ve servis tespitini yapabilmektedir. Domainle entegre olarak çalışabilmekte olup html, xml, latex gibi değişik formatta raporlar üretebilmektedir.

GFI Languard yazılımı nessus gibi genel amaçlı ticari bir açıklık tarama yazılımıdır (<http://www.gfi.com>). Açıklıkları, portları ve servisleri belirlemesinin yanında, tarama sonuçlarını eski tarama sonuçları ile karşılaştırabilmektedir. Ticari bir yazılım olduğu için çok çeşitli yapıda ve formatta raporlar sunmaktadır.

Microsoft Baseline Security Analyser yazılımı ücretsiz bir yazılım olup Microsoft işletim sistemleri ve programları için bilinen açıklıkları ve eksik yamaları raporlamaktadır (<http://www.microsoft.com/technet/security/tools/mbsahome.msp>). Aşağıdaki kontrolleri yapmaktadır:

Ofis güvenlik güncellemeleri

Windows güvenlik güncellemeleri

Yerel parola politikaları

Yönetici hesapları

Parola bitim tarihleri

Otomatik güncellemeler

Güvenlik duvarları

Auto logon

Anonymous hesabı

İzleme

Servisler

Paylaşımlar

Windows sürümü

IIS hakkında bilgiler

Sql hakkında bilgiler

Macro güvenliği

IE güvenlik ayarları

4. 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 bulunduğu açıklıkları gerçekleyebilmektedir.

Açıklık gerçekleştirme araçlarının en önemlilerinden biri olan **Metasploit**, açık kaynak kodlu bir program olup hem Windows hem de Linux işletim sistemleri üzerinde çalışabilmektedir (<http://www.metasploit.com>). Halihazırda 3.1 sürümü bulunmaktadır. 261 tane açıklık tanımı, 76 tane payload içermektedir. İstendiğinde yeni açıklıklar eklenebilir.

Diğer bir açıklık gerçekleştirme aracı olan **CoreImpact**, grafik arayüzü olan ticari bir üründür (<http://www.coresecurity.com>). Açıklıkları tespit etme ve uygulama yeteneğine sahiptir. Sonuçları değişik formatlarda raporlayabilmektedir.

5. 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.

6. 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.

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 sunucusu ve 80 numaralı tcp portu kullanılarak, Web sunucusuya giden yol üzerindeki cihazlar kolaylıkla tespit edilebilir.

7. 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.

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 (<http://xprobe.sourceforge.net>). Linux işletim sisteminde ve komut satırında çalışmaktadır.

Diğer bir işletim sistemi tespit aracı da **P0F** (Passive OS Fingerprinting) programıdır. Windows ve Linux işletim sistemlerinde çalışabilmektedir.

8. 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.

Bu araçlardan **Cain and Abel**, ücretsiz bir yazılımdır (<http://www.oxid.it/cain.html>). Sadece Windows işletim sistemleri üzerinde çalışabilmektedir. 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.

Brutus yazılımı, Cain and Abel kadar geniş özelliklere sahip olmasa da şifre kırma konusunda temel işlemleri yapabilmektedir. Brutus, sözlük ve kaba kuvvet saldırıları yapabilmekte ve kullanıcılara özel uygulamalarda (TELNET, HTTP vb...) şifre kırabilmektedir.

Bir başka şifre kırma aracı olan **Hydra**, windows, unix ve macos işletim sistemleri üzerinde çalışabilmektedir (<http://freeworld.thc.org/thc-hydra>). Hydra, sadece sözlük saldırısı yapabilmektedir. Ayrıca pek çok uygulamanın şifresini kırabilmektedir. Bu yazılım, diğer araçlar a göre nispeten daha hızlı çalışmaktadır.

9. Kablosuz Ağ Araçları

Kablosuz ağların yaygınlaşmasıyla birlikte, bu ağlara yapılan saldırılarda artmıştır. Artan saldırılar, kablosuz ağ güvenliğini çok önemli kılmaktadır. Kablosuz ağ güvenliğini denetlemek ve test etmek için de pek çok araç bulunmaktadır. Kablosuz ağ araçlarını üç grup altında toplamak mümkündür:

Tespit ve Analiz Araçları: Kablosuz cihazların tespit edilmesi, kanallardaki cihazların tespit edilmesi, sinyal analizi, kablosuz ağ trafiğinin dinlenmesi ve kaydedilmesi için geliştirilmiş araçlardır. En önemlileri **Kismet** (<http://www.kismetwireless.net>) ve **Netstumbler** (<http://www.netstumbler.com>) olarak gösterilebilir.

Denetleme araçları: Kablosuz haberleşmede kullanılan şifreleme ve kimlik doğrulama yöntemleri, paket dinleme, analiz etme ve önemli olayların kaydını tutma gibi işlemlerde denetleme araçları kullanılır. Denetleme araçlarına örnek olarak **Airmagnet**, **Airdefense** ve **Airopeek** (<http://www.wildpackets.com>) verilebilir.

Saldırı araçları: WEP/WPA anahtarlarının ele geçirilmesi, hedef bilgisayara erişim, hedef bilgisayarın veya erişim noktasının (EN) ağa erişiminin engellenmesi, yetkilendirme ve doğrulama mekanizmasının aşılması veya etkisiz hale getirilmesi gibi işlemler için saldırı araçları kullanılır. Kablosuz ağ saldırı araçlarına örnek olarak **Aircrack** (<http://aircrack-ng.org>), **HostAP**, **SoftAP**, **Airjack**, **Airsnarf**, **Airsnot** ve **LEAPcracker** yazılımları verilebilir.

10. VPN Cihazı Test Araçları

VPN cihazlarının güvenliğini test etmek için özel yazılımlar üretilmiştir. Bu yazılımların en önemlilerinden biri **ipseccan** yazılımıdır (<http://www.ntsecurity.nu/toolbox/ipseccan>). Sunucu üzerinde ipsec servisinin çalışıp çalışmadığını kontrol etmek için kullanılır. Ücretsiz bir yazılım olan ipsecscan, Windows işletim sistemi üzerinde çalışmaktadır. Bir veya daha çok IP adresini aynı anda tarayabilmektedir.

Açık kaynak kodlu bir yazılım olan **ike-scan** ise Windows, Linux ve MacOS işletim sistemleri üzerinde çalışabilmektedir (<http://www.nta-monitor.com/tools/ike-scan>). VPN cihazlarını tespit etme ve test amaçlı kullanılmaktadır.

ikeprobe yazılımı da ücretsiz bir olup VPN cihazının PSK gerçekleştirilmesinde açıklık olup olmadığını test etmek için kullanılır (<http://secure2s.net/tools/2007/04/01/ikeprobe>). VPN cihazını agresif moda çalışmaya zorlar.

11. 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 yazılım olup platform bağımsız çalışmaktadır (<http://www.parosproxy.org/index.shtml>). 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 (<http://www.getfirebug.com>). Platformdan bağımsız olarak çalışır. Web sayfasının istenilen herhangi bir yerine gelindiğinde o kısım ile 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, izin kontrolü gibi testleri yapmaktadır (<http://www.acunetix.com>). 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.

12. 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. Oracle, MSSQL ve Sybase veritabanları üzerinde tarama yapabilir. Seçilen bir sözlük üzerinden veritabanı kullanıcı şifreler için sözlük atağı yapabilir. Veritabanının üzerinde koştugu 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.

Appdedective ticari bir ürün olup açıklık tespiti ve yapılandırma hatalarını tespit edebilmektedir (<http://www.appsecinc.com/products/appdetective>). Çok geniş bir veritabanı tarama seçeneğine sahiptir. Sözlük atağı yapabilme yeteneğinden dolayı sızma aracı olarak da kullanılabilir. Tarama sonuçlarını rapor halinde sunabilmektedir. Web sunucuya ait kontroller yapmaktadır.

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. Excel dosyası ile kullanıcı ismi ve şifreleri parametre olarak girilir.

Oktay ŞAHİN

REFERANSLAR

<http://insecure.org>

<http://www.nessus.org/nessus>

<http://nmap.org>

<http://www.metasploit.com>

<http://www.wireshark.org>

<http://www.tcpdump.org>

<http://ettercap.sourceforge.net>

<http://www.gfi.com>

<http://www.microsoft.com/technet/security/tools/mbsahome.mspx>

<http://www.coresecurity.com>

<http://www.hping.org>

<http://xprobe.sourceforge.net>

<http://www.oxid.it/cain.html>

<http://freeworld.thc.org/thc-hydra>

<http://www.kismetwireless.net>

<http://www.netstumbler.com>

<http://www.wildpackets.com>

<http://aircrack-ng.org>

<http://www.ntsecurity.nu/toolbox/ipsecscan>

<http://www.nta-monitor.com/tools/ike-scan>

<http://secure2s.net/tools/2007/04/01/ikeprobe>

<http://www.parosproxy.org/index.shtml>

<http://www.getfirebug.com>

<http://www.acunetix.com>

<http://www.iss.net>

<http://www.appsecinc.com/products/appdetective>