Açık Kaynak Kodlu Güvenlik Projeleri

Açık kod dünyasında uzun zamandır kullanılan, belli bir kararlılığa ulaşmış ve kendini ispatlamış birçok güvenlik yazılımı vardır. Bunlar aşağıdaki alt başlıklar altında incelenebilir.

- **Güvenlik Duvarı(Firewall) Ürünleri**
  - OpenBSD PF(Packet Filter)
  - IPF(IP filter)
  - Iptables
    - Ebtables(http://ebtables.sourceforge.net/)
    - L7-filter (http://l7-filter.sourceforge.net/)

- **Ağ tabanlı Atak tespit ve engelleme yazılımları**
  - Snort***
  - Snortsam

- **Bütünlük doğrulayıcı yazılımları**
  - Samhain

- **Trafik dinleme, analiz ve manipulation Yazılımları**
  - Ethereal
  - Ettercap
  - Dsniff
  - Snoop / solaris

- **Şifreleme/ VPN Araçları**
  - OpenSSL
  - SSH(OpenSSH)
  - Stunnel
  - OpenVPN
  - PopTop

- **Ağ tarama sistemleri**
  - Nmap
  - Hping

- **Güvenlik Test araçları**
  - John The ripper
  - Nessus

- **Antivirüs ve Rootkit Araçları**
    - Clam Antivirüs
    - Rootkit hunter
- **İçerik Filtreleme Araçları**
    - Squid***
    - Dansguardian
- **Sunucu izleme araçları**
    - Nagios

Firewall Araçları

Günümüz internet kullanımının getirdiği riskler sonucunda basit ya da karmaşık ne şekilde bir ağ olursa olsun bir firewall aracılığı ile korunması gerekir. Açık kod dünyası da bu problemi en iyi şekilde kapatacak çözümler geliştirmiştir. Bu projelerden en çok bilineni, kullanılanı ve gelişime açık olanları aşağıdaki gibidir.

Iptables

Iptables linux 2.4.X ve 2.6.X kerneli ile birlikte dağıtılan Netfilter API'sinin kullanımı için yazılmış bir arabirimdir. Rusty russel tarafından başlatılmış ve şuanki proje yöneticisi Harald Welte'dir. Iptables'in bazı önemli özellikleri aşağıdaki gibi listelenebilir;

- Durum Korumasız (stateless) packet filtreleme (IPv4 ve IPv6)
- Durum Korumalı (stateful packet) filtering (IPv4)
- Tüm ağ adres çevirim(Network Address Translation) çeşitlerini destekler(NAT/NAPT)
- Esnek ve geliştirtirilebilir yapı
- Sonradan eklenebilen modül desteği
    - Patch-o-matic

Iptables ile neler yapılabilir?

- Durum korumalı ateş duvarı kuralları yazarak ağınızı hedefleyen tehlikelerden korunabilirsiniz.
- İç ağa tek bir Ip adresi üzerinden veya bir grup IP adresi üzerinden internet erişimini paylaştırılabilir.

- Tc ve iproute2 ile birlikte kullanılarak çeşitli QOS ve policy routing tanımları yapılabilir.
- Çeşitli paket mangle işlemleri yapılabilir.

- Iptables komut satırından yönetilebilen bir araç olmasının yanında sourceforge.net ve Freshmeat.Net'den bulunabilecek onlarca Web arabirimi ile de yönetilebilir.

Patch-o-matic(`p-o-m`) nedir?

Patch-o-matic bir sonraki çıkacak olan netfilter sürümüne eklenebilecek özelliklerin geliştirildiği ve test edildiği bir ortamdır. Netfilter'a eklenmesi istenen özellikler öncelikle patch-o-matic ortamına aktarılır burada çeşitli geliştiriciler tarafından eklemeler yapılır, varsa eksiklikleri giderilir.

Bu kodlar gerekli kararlılığa ulaşınca netfilter koduna eklenir. Patch-o-matic kullanmak isteyen kullanıcıların istediği eklenti için çıkrılmış yamayı indirerek çekirdeğini bu yama ile yamadıktan sonra tekrar derlemelidir. Derleme sonrasında iptables aracılığı ile bu ek özellikler kullanılabilecektir .

Ebtables

Ebtables Nedir?

2.6 Serisi çekirdekler için 2. katmanda ileri düzey filtreleme işlemleri yapabilen bir yazılımdır. 2.4 çekirdek sürümleri ile de ek bir yama ile kullanılabilir.

Özellikleri

- Ethernet protokolü filtreleme(Ethernet Frame filtering)
- Mac adresine göre filtreleme(iptables ile de yapilabiliyor.)
- MAC adresine göre NAT tanımlama özelliği
- Detaylı Loglama

L7-Filter

Linux 2.4 ve 2.6.X çekirdeklerinde bulunan netfilter altsistemi için uygulama seviyesinde trafik sınıflandırma aracıdır. Diger trafik sınıflandırma araçlarından farklı olarak uygulama bazında trafigi anlayarak işlem yapar.

L7-Filter uygulama katmanı verisini inceleyerek kendisine belirli olan bir dosya ile karşılaştırarak hangi protokol olduğuna karar verir.

/etc/l7-protocols dosyasında protokollere ait söz dizimleri yer alır. L7-Filter bu dosyayı kullanarak sınıflandırma yapar. L7-filter gelen ilk 8 pakete(~2kb) bakarak işlem yapar, fakat bu değer değiştirilebilir.

Kaynaklar:

[1] http://www.netfilter.org
[2] http://www.linuxguruz.com/iptables/
[3] http://www.netfilter.org/documentation/HOWTO//netfilter-extensions-HOWTO.html
[4] http://l7-filter.sourceforge.net

IPF(Ip Filter)

FreeBSD üzerinde kullanılan kaliteli bir Firewall projesidir. OpenBSD PF'in çıkması ile populerliğini yitirmiştir. OpenBSD PF'in ilham aldığı Firewall projesi denilebilir.

PF(Packet Filter)

OpenBSD PF

OpenBSD projesi bünyesinde başlatılmış ve diğer BSD'lere port edilmiş UNIX dünyasının gelmiş geçmiş en iyi, en kolay ve en esnek özelliklere sahip olduğu söylenebilecek açık kodlu güvenlik duvarı(Firewall) yazılımıdır.

PF'e ait bazı önemli özellikler;

- Detaylı , anlaşılır dökümantasyon. PF'e ait her özelliğin anlatıldığı FAQ ve man sayfaları.
- BSD Lisansı ile özgürce kullanım ve dağıtım hakkı.
- Her türlü NAT işlemi(Nat, port redirection, binat) gerçekleştirelbilme.
- Bant genişliği(Banwidth) yönetimi.
- Üstün performans.
- İleri düzey paket filtreleme yeteneği.
- Kural yazımı için basit söz dizimi.
- Layer 2 düzeyinde çalışarak kolayca ağ yapısına uyum sağlar

- İleri düzey Yük paylaşımı ve yüksek bulunurluk(HA) desteği

PF Kullanımı

PF kullanımı ile ilgili belgeler için aşağıdaki linkler kullanılabilir;

http://www.enderunix.org/docs/pf.pdf
http://www.enderunix.org/docs/pf_tr.pdf

Ağ tabanlı Atak tespit ve engelleme yazılımları

Snort

Eklenecek***

SnortSam

Snortsam Snort IDS sistemine IPS özelliği katan bir plugindir. Snortsam iki ana parçadan oluşur. Bu parçalardan biri Snort için output sistemidir, diğeri de Güvenlik duvarı üzerinde ajan vazifesi görecek parçadır. Snortsam kurulduktan sonra snort kurallarına "fwsam" anahtar kelimesi eklenir. Snortsam'in kullanımı bu anahtar kelimeyle yapılır. Snort üzerine yazılan kurallar snortsam ajanı aracılığı ile Firewall'a aktarılır ve engellenmesi gereken trafik Firewall tarafından yasaklanır.

Snortsam ile birlikte kullanılabilecek Güvenlik duvarı yazılımları:

Checkpoint Firewall-1 , Cisco PIX firewalls , Cisco Routers, Juniper firewalls, IP Filter (ipf), FreeBSD ipfw2, OpenBSD Packet Filter (pf), Linux IPchains , IPtables , Ebtables, WatchGuard Firebox, 8signs firewalls for Windows
MS ISA Server firewall/proxy for Windows, CHX packet filter, Ali Basel's Tracker SNMP

Bütünlük doğrulayıcı yazılımları

Samhain

Unix sistemlerin temel felsefelerinden biri olan `herşey dosyadır` yaklaşımı dikkate alınırsa UNIX sistemlerdeki dosya bütünlüğünün önemi anlaşılır. İşletim sisteminin temelini oluşturan dosyalarda yapılan bir değişikliğin zamanında farkedilmesi ilerde oluşabilecek birçok güvenlik problemini gidermiş olur. Mesela /etc/passwd dosyasında yapılacak basit bir değişiklik ile sistem üzerindeki normal bir kullanıcı root yetkilerine sahip olabilir. Eğer /etc/passwd dosyasını belirli aralıklarla bütünlük kontrolünden geçiren bir sisteminiz varsa bu dosyadaki değişikliklerden kısa sürede haberdar olabilirsiniz ve gerekeni yaparsınız.

Samhain, açık kaynak kodlu , multiplatform , merkezi bir yapıda çalışan bütünlük doğrulayıcı yazılımıdır. Istemci sunucu mimarisine uygun bir yapıda çalışır. Dosya bütünlüğü izlenmek istenen sistemlere ajan bir program kurularak o sistemin kontrolu ajan programa bırakılır. Ajan program merkezi loglama sunucusuna belirli zamanlarda şifreli TCP bağlantısı kurarak gerekli güncellemeleri, kuralları alabilir.

Samhain , Beltane programı ile web arabiriminden kolayca yönetilebilir.

Samhain'e ait bazı önemli özellikler:

- İstenilen zaman aralığında sistem taraması gerçekleştirebilir.
- Linux ve FreeBSD sistemlerinde çekirdek için rootkit taraması yapabilir.
- Sisteme yeni eklenen SUID/SGID bitli dosyaları kontrol edebilir. Istenildiği takdirde yeni eklenen dosyaları karantineye alabilir ya da silebilir
- Sisteme giriş çıkışları loglayabilir
-

Samhain aşağıdaki işletim sistemlerini desteklemektedir.

- POSIX (e.g. Linux, *BSD, Solaris 2.x, AIX 5.x, AIX 4.x, HP-UX 10.20, HP-UX 11, Unixware 7.1.0, Alpha/True64, and Mac OS X)
- Windows 2000 / WindowsXP POSIX emulasyonu ile (e.g. Cygwin)

Samhain ile ilgili detay bilgi http://la-samhna.de/samhain/ adresinden edinilebilir.

Trafik dinleme, analiz ve değiştirme yazılımları

Ethereal

Ethereal, açık kaynak kodlu bir Trafik analiz programıdır. Gelişmiş grafik arabirimi sayesinde kullanımı oldukça kolaydır. Bunun yanında istenirse komut satırından da kullanılabilir. Komut satırından kullanım için **tethereal** komutu ve ek parametreleri kullanılabilir.

Windows, UNIX(BSD, Solaris, vb) ve Linux işletim sistemleri üzerinde GPL lisansı ile özgürce kullanılabilmektedir.

Ethereal, açık kod dünyasının desteğini arkasına alarak kısa sürede piyasadaki ticari Trafik analiz programlarının işlevlerinin çoğunu yerine getirebilecek seviyeye ulaşmıştır.

Ethereal'in bazı önemli özellikleri:

- Yakalanan paketleri kaydedebilme , kaydedilen paketleri analiz edebilme
- tcpdump , NAI's Sniffer™ , Sniffer™ Pro , NetXray™, Sun snop ve atmsnoop, Shomiti/Finisar Surveyor vb gibi birçok paket analiz programları ile yakalanmış ve kaydedilmiş paketleri analiz edebilme
- Paketleri tethereal yada bir gui aracılığı ile izleyebilme
- 3COMXNS, 3GPP2 A11, 802.11 MGT, 802.11 Radiotap, 802.3 Slow protocols, 9P, AAL1, AAL3/4, AARP, ACAP, ACN, ACSE, ACtrace, ADP, AFP, AFS (RX), AH, AIM, AIM Administration, AIM Advertisements, AIM BOS, AIM Buddylist, AIM Chat, AIM ChatNav, AIM Directory, AIM Email, AIM Generic, AIM ICQ, AIM Invitation, AIM Location, AIM Messaging, AIM OFT, AIM Popup, AIM SSI, AIM SST, AIM Signon, AIM Stats, AIM Translate vs .. 706 protokol desteği
- Yakalanan paketler düz yazı yada PostScript olarak kaydedebilme
- Filtreleme esnasında istenilen protokollerin istenilen renkde gösterilebilmesi

Ettercap

Ettercap çok özellikli bir trafik analiz ve trafik injection programıdır. Ettercap ile basit trafik dinleme işlemlerinden öte switch'li ağlarda birçok geçerli yöntem(apr spoofing, arp poisoning, mac address cloning) kullanarak trafik izleme , trafiğe yön verme işlemleri gerçeklenebilir. SSL bağlantılarında araya girerek sadece trafiği izlemekle

yetinmeyip izlenilen trafiğin değiştirilmesini de sağlar(MITM).

Ettecap kullanarak özellikle Layer2 üzerinde çalışan protokoller ve işleyiş yapıları iyice öğrenilebilir.

Desteklenen Platformlar:
Linux 2.4.x, Linux 2.6.x FreeBSD 4.x 5.x, OpenBSD 2.X 3.x, NetBSD 1.5 , Mac OS X (darwin 6.x 7.x), Windows 2000/XP/2003, Solaris 2.x

Lisansı: GPL

Dsniff

Dsniff Dug Song tarafından ağ güvenliği denetimi ve trafik dinleme amaçlı yazılmış bir programdır.

Dsniff'in oluşturan bazı programlar ve işlevleri ;

Mailsnarf, urlsnarf, filesnarf, msgsnarf, webspy araçları ağ ortamında gezen zayıf parolaları ve çeşitli bilgileri okunabilir formatta sunmak için kullanılabilir. Mesela urlsnarf aracı kullanılarak akan trafik içerisinden 80, 3128 ve 8080 portlarını dinleyerek web trafiğine ait URL'leri Microsoft IIS ve Apache tarafından da kullanılan Common Log Format (CLF) formatında kaydeder.

 # urlsnarf -i xl0
urlsnarf: listening on x10 [tcp port 80 or port 8080 or port 3128]

Bunların dışında kotu amaçlı ellerde oldukça tehlikeli ***olabilecek arpspoof, macof, dnsspoof*** gibi ileri düzey araçlara da sahiptir. Bu araçlarla sağlam korunmamış bir LAN içerisinde SSL, SSH, SSH ve DNS trafikleri yanıltılabilir. Dsniff kullanılarak Switched ağlardaki güvenlik sorununu anlatan bir yazıya http://www.mutasyon.net/makaleoku.asp?id=756 adresinden erisilebilir. Kısacası güvenlik üzerine uğraşan yöneticilerin elinin altında bulunması gereken bir yazılımdır.

Dsniff Windows işletim sistemi üzerinde de çalışır. http://www.datanerds.net/~mike/dsniff.html adresinden Dsniff'in Win32 sürümü edinilebilir.

Cain Abel: Dsniff araçlar bütününü yaptığı herşeyi Windows ortamında GUI aracılığı ile yapabilme olanağı sağlar.

http://naughty.monkey.org/~dugsong/dsniff/ adresinden Dsniff ile ilgili detay bilgi edinilebilir.

http://www-128.ibm.com/developerworks/library/s-sniff.html

Snoop

Snoop solaris işletim sisteminde çalışan bir snifferdir. Snoop ile realtime trafik izleme yapılabileceği gibi trafiği snoop formatında kaydedip sonra inceleme amaçlı da kullanılabilir.

#Snoop –o dosya_ismi

Kaydedilen dosya

#Snoop –i dosya_ismi ile incelenebilir.

Snoop ile mac adresine gore de trafik analizi yapılabilir.

#Snoop from 00:04:5b:f2:83:33 or to 02:06:5b:f2:87:41

Şeklinde bir komut ile belirli mac adresleri arasındaki trafigin yakalanması sağlanır.

Snoop üç modda çalışır, özet mod detay özet ve detay mod. Varsayılan mod özet moddur(summary) ve bu modda trafik 5,67 gibi üst katmanlar için yakalanır.
-V ile çalıştırıldığında layer2Den layer 7'ye kadar özet bir şekilde sunar.
-v ile çalıştırıldığında yakalanan pakete ait tüm detaylar görülebilir.

!!Snoop herhangi bir özgür lisansa sahip değildir ve kaynak kodları açık değildir. Snoop'un Linux için çalışan versionları bulunmaktadır.

Şifreleme/ VPN Araçları

OpenSSL

OpenSSL güvenli ağ iletişimi için düşünülmüş SSL/TLS protokollerinin tamamen özgür olarak kullanılabilen versiyonudur.

Eric A. Young ve Tim J. Hudson tarafından 1995 yılında başlatıltılan SSLeay projesinin 1998 yılında son bulması ile

hayat bulmuştur. OpenSSL şifreleme kütüphanesi ve SSL araçlarından oluşmaktadır.
C ve C++ programlama dilleri kullanılarak yazılmıştır. Windows, Unix ve Linux sistemlerde sorunsuz çalıştırılabilir.

OpenSSL sağladığı API sayesinde bir çok 3. parti yazılımı için güvenli versiyonlar sunar. Mesela OpenSSH OpenSSL kullanır. Diğer bir örnekte Mysql., mysql'i –with-openssl --with-vio seçenekleri ile derlenirse MySQL sunucusu ve istemcisi arasındaki trafik şifrelenmiş bir şekilde gerçekleştirilir.

Apache mod_ssl aracılığı ile HTTPS hizmeti sunabilir, mosssl ise OpenSSL tabanlı bir modüldür.

OpenSSL Kullanılarak özel de sertifikalar oluşturulabilir ve bu sertifikalar imzalanabilir. CA kurulabilir. Ve sertifika dağtımı yapılabilir.

Temel OpenSSL Kullanımı

Bir dosyaya ait hash çıkarımı

$ openssl dgst -md5 /etc/pf.conf
MD5(/etc/pf.conf)= be11833967a109ad3dd3411bbe32f578

/etc/pf.conf dosyasına ait MD5 imzasını alır.
Bu imzayı standart çıktıya değilde bir dosyay yazdırmak istersek

$openssl dgst -sha1 -out imza /etc/pf.conf

$cat imza
SHA1(/etc/pf.conf)= b968003786b48d10299176b795a6f5e7d954536d

Stunnel

Şifrelenmemiş protokolleri şifreli tünel aracılığı ile kullanmak

Internet üzerinde sık kullanılan çoğu protokol şifreli iletişimi desteklememektedir. Bu durumda bu protokolleri şifreli bir tünel aracılığı ile kullanarak son kullanıcı ile sunucu arasındaki iletişimi kullanıcıya ek bir müdahele gerektirmeden şifreli hale getirebiliriz. Bunun için kullanılabilecek birçok program vardır. Açık kaynak kod dünyasında bu programlardan en bilineni stunnel'dir (http://www.stunnel.org). Stunnel yapısında şifreleme özellikleri bulunmayan protokoller için bir aracı vazifesi

görür. Örnek verecek olursak, bir mail sunucu kurduk fakat kurduğumuz mail sunucunun doğal yapısında şifreleme özelliği yok. Kullandığımız mail istemci programı (Mozilla Thunderbird, Outlook, the Bat!)şifreli mail kullanımı desteklediği halde sunucuda böyle bir özellik olmadığı için kullanılamaz haldedir.

Kullanıcıda şifreli mail ayarları yapılarak mail sunucu tarafında bir şifreli tünel yapısı oluşturuyoruz. Burada devreye STUNNEL giriyor, kullanıcı yapılandırdığı mail istemci programı ile sunucuya bağlanmak istiyor. Sunucuda smtp ve pop3 portlarını mail sunucu değilde STUNNEL programı dinliyor, stunnel programı kendisine gelen istekleri deşifre ettikten sonra aynı sistemde çalışian mail sunucuya aktarıyor ve mail sunucudan gelen cevapları da şifreleyerek kullanıcıya aktarıyor. Böylece mail sunucu yazılımında herhangi bir değişiklik yapmadan mail trafiğini güvenli hale getirmiş oluyoruz.

OpenSSH

SSH Nedir?

Ssh (Secure Shell/Güvenli Kabuk) ağ üzerinden başka bilgisayarlara erişim sağlayan, uzak bir bilgisayarda komutlar çalıştıran ve bir bilgisayardan diğerine dosya taşımamzızı sağlayan bir programdır. Güvensiz kanallar üzerinden güvenli haberleşme sağlar.

Özgür bir SSH versiyonu olan OpenSSH *BSD Unixlerin asi çocuğu olarak nitelenen OpenBSD projesi çerçevesinde yürütülen SSH1 ve SSH2 protokollerini içeren yazılım takımıdır. OpenBSD sürümü hariç diğer tüm versiyonları OpenBSD için geliştirilen sürümün gerekli sisteme uyarlanmış versiyonlarıdır.

OpenSSH birçok platforma uyarlanmış sürümlerini bulabilirsiniz ve platformlar arası kullanımı çok az farklılıklar gösterir. Aşağıda OpenSSH ın kullanılabileceği bazı platformları listelenmiştir , detaylı bilgi ve liste için http://www.openssh.org/portable.html adresini ziyaret edebilirsiniz. Bu liste haricinde Windows ortamında da çalışmaktadır. Arama motorlarından yapılacak kısa bir araştırma sonucunda projenin hangi kurum ve kuruluştar tarafından desteklendiği ve kullanıldığı öğrenilebilir

OpenSSH aşağıdaki işletim sistemlerinde çalışır;

- AIX, HP-UX , Irix L, Linux , NeXT , SCO , SNI/Reliant Unix , Solaris , Digital Unix/Tru64/OSF , Mac OS X , Cygwin ile Windows

Kullanım Alanları

SSH'ı güvenliğin gerektiği her ortamda kullanılabilir. Sadece karşı sisteme bağlanıp komut çalıştırmak ya da dosya aktarımı yapmak için değil güvensiz olarak gördüğümüz protokolleri SSH üzerinden güvenli bir şekilde iletişimi de sağlanabilir . Mesela POP3 servisi ağ üzerinden tüm iletişimini şifrelenmemiş şekilde(plain text) gerçekleştirir, biz pop3 servisini SSH üzerinden aktarım yaparak şifrelenmiş ve güvenli hale getirebiliriz, buna port forwarding denir. Portforwarding basitce aşağıdaki gibi yapılır;

ssh -f -L 1234:server.bizimhost.net:6667 server.se7enhost.com sleep 10

OpenSSH takımı aşağıdaki programlardan oluşmaktadır;

Ssh, Scp, Sftp, Sshd, ssh-add, ssh-agent, ssh-keysign, ssh-keyscan, ssh-keygen, sftp-server

OpenVPN

OpenVPN multi platform bir SSL VPN çözümüdür. SSL VPN denilince akla gelen bir browser aracılığı ile VPN yapmaktır fakat buradaki SSL VPN tanımı bu tanımdan farklıdı. Yani OpenVPN bir browser ve TCP/443 portu kullanarak **kullanılamaz.** OpenVPN ile yapılabilecekler;

Linux, Windows 2000/XP ve üzeri, OpenBSD, FreeBSD, NetBSD, Mac OS X ve Solaris işletim sistemlerinde çalıştırılabilir.

- OpenSSL kütüphanesinin sunduğu encryption, authentication, ve certification
- Özelliklerini kullanabilir.
- Nat üzerinden sorunsuz tünetl oluşturma
- İsteğe bağlı olarak GUI ile yönetim.
- Bridge ve route mode olmak üzere 2 farklı katmanda VPN çözümü olarak kullanılabilir.

PopTop

PopTop (The PPTP server for Linux) Linux/Solaris ve BSD sistemler için başlatılmış bir PPTP(point to point tunneling protokol) projesidir. PPTP, uçtan uca tünelleme/şifreleme sunar. Microsoft'unda aralarında bulunduğu bir konsorsiyum tarafından internet üzerinden güvenli VPN erişimleri için geliştirilmiştir. PPTP istemci-sunucu mantığı ile çalışır, özellikle Windows istemci makinelerin hazır PPTP istemci yazılımları ile dağıtıldığı düşünülürse oldukça kolay yapılandırılabilir bir VPN çözümü ortaya çıkmış olur. Linux ve diğer işletim sistemleri içinde pptp istemci yazılımları bulunabilir bunlardan Linux için olannına http://pptpclient.sourceforge.net/ adresinden erisim saglanabilir.

GPL Lisansı ile özgürce kullanılabilir.

PopTop'a ait bazı özellikler;

- Microsoft uyumlu kimlik denetimi ve şifreleme(MSCHAPv2, MPPE 40 - 128 bit RC4)
- Eşzamanlı birden fazla kullanıcı desteği
- Windows 95/98/Me/NT/2000/XP PPTP istemcileri ile birlikte çalışabilir.
- Radius eklentisi ile samba ve ldap üzerinden onaylama yapabilir.

PPTP'nin de kendine has çeşitli güvenlik sorunları vardır. Dökümantasyon için: http://poptop.sourceforge.net/dox/

Proje ana sayfası http://www.poptop.org

Ağ tarama araçları

Nmap

Nmap(Network Mapper) çok amaçlı ağ araştırma ve port tarama aracıdır. Kolay kullanımı ve sunduğu esnek özellikler yıllardır NMAP'i güvenlik dünyasında haklı bir yere oturtmuştur. Uzun süredir Fyodor Arkin tarafından geliştirilmektedir ve birçok Linux dağıtımı ile birlikt gelmektedir. BSD sistemler için port ağacından kolaylıkla kurulabilir. Oldukça detaylı ve anlaşılır bir man sayfası vardır.

Sistemini komut satırından kullanmaya alışmış unix uzmanlarına hitap ettiği gibi komut satırına hiç bulaşmadan kullanmak

isteyen kullanıcılar içinde oldukça basit anlaşılır bir grafik arabirim sunar. Bunun yanında çeşitli ağ ve güvenlik araştırmacıları tarafından NMAP'i temel almış çeşitli yazılar yayınlanmıştır, bu yazılara google arama motorunda yapılacak basit aramalar sonucu ulaşmak mümkündür. Aslında NMAP bu şekilde birkaç cümleye sığdırılamayacak kadar özelliği bünyesinde bulundurur. Nmap ile yapılabilecek bazı işlemler

- Çeşitli Port tarama tekniklerini destekler
  - UDP,
  - TCP connect(),
  - TCP SYN (half open),
  - ftp proxy(bounce attack),
  - ICMP (ping sweep),
  - FIN, ACK sweep,
  - Xmas Tree,
  - SYN sweep,
  - IP Protocol,
  - Null scan
- TCP/IP fingerprint ile işletim sistemi saptama
- Paralel port tarama
- Çalışan servis tipi ve versiyonu belirleme
- Uptime süresi belirleme
-

Lisansı :

GNU GPL Lisansı altında özgürce dağıtılmaktadır

Desteklediği platformlar

NMAP'in desteklediği bazı populer işletim sistemleri;

Linux, Microsoft Windows, FreeBSD, OpenBSD, NetBSD, Solaris, Sun OS, IRIX, Mac OS X, HP-UX, Amiga,

Hping

Hping komut satırı tabanlı bir TCP/IP analiz programıdır. İsmi ping programından esinlenilmesine rağmen ping programı gibi sadece icmp echo paketleri ile değil icmp, tcp, udp raw-ip protokolleri ile çalışabilir. Hping'in kullanım amaçlarından bazıları aşağıdaki gibidir,

- Ateş duvarı testleri
- Gelişmiş port tarama

- Gelişmiş traceroute
- İşletim sistemi saptama
- Uzak sistemlerin uptime surelerini belirleme
- TCP/IP yığın testi

Güncel sürümü 2.03 olmakla beraber yeni ve daha gelişmiş bir sürümünün testlerine de hping'in sitesinden ulaşılabilir.

Hping 3 versiyonu ile birlikte artık bir betik dili(TCL) aracılığı ile ileri düzey güvenlik testleri yapılabilir hale gelecek. Betik dili sayesinde yüzlerce satır C kodu ile yapılabilecek eklentiler, işlemler çok kısa bir sürede yapılabilecek. Mesela bu betik dili sayesinde hping'e tarama yapılan hostları bir mySQL veritabanına yazması sağlanabilir benzer şekilde güvenlik tarama sonuçların dan çeşitli istatistikler çıkarması sağlanabilir.

Desteklenen platformlar

- Linux, FreeBSD, NetBSD, OpenBSD, Solaris, MacOs X

Lisansı

Hping GNU GPL lisansı altında özgürce dağıtılmaktadır.

Kurulum:

Birçok Linux dağıtımı için hazır paketler internette bulunabilir. FreeBSD, OpenBSD kullanıcıları port ağacında /usr/ports/security/hping dizini altında bulunur. Kurulum için

#cd /usr/ports/security/hping
#make install

komutlarının verilmesi yeterlidir.

Kaynaklar:

[1]http://www.hping.org
[2]http://www.sans.org/rr/audit/hping2.php
[3]http://infosecuritymag.techtarget.com/2003/jul/logoff.shtml

Nessus

Güvenlik zaafiyeti inceleme programı

1998 yılında Renaud Deraison tarafından açık kaynak kodlu, kolay kullanımlı ve güncel bir zayıflık inceleme projesi

olarak başlatılmıştır. Projenin geldiği nokta incelendiğinde üzerinden geçen 6 yılda internet dünyasında hatırı sayılır bir yer edindiği görülebiblir. Internet üzerine free/commercial güvenlik tarama işlemi yapan birçok şirket altyapı olarak Nessus'u kullanmaktadır.
Son raporlara göre dünya üzerinde 75.000 profesyonel güvenlik uzmanı tarafından aktif olarak kullanıldığı saptanmıştır.

Projeye ait bazı önemli özellikler
- GPL lisansı ile özgür dağıtım ve kullanım
- Güncel zayıflık veritabanı (Günlük)
- Uzak ve yerel sistem güvenlik tarama özelliği
  - Nessus yerel güvenlik taraması yapabilen ik ürün
  - Windows, UNIX ve Mac makinelere login olarak gerekli taramaları, eksik yamaları belirleyebilir
- Gelişmiş Plugin() desteği
  - Yaklaşık 8000 farklı plugin
- Plugin geliştirmek için ayrı bir programlama dili(NASL) Nessus Attack Scripting Language)
- SSL tabanlı servisleri tarama özelliği (https, smtps, imaps etc)
- Komut satırından kullanım olanağı
- Kullanıcı desteği
  - Günlük ~2000 indirim sayısı
  - Ortalama 50000 kullanıcı

Yerel ve Uzak sistemler güvenlik testi

Normal bir güvenlik tarayıcısı ağ üzerinde hedef olarak belirtilen sistemlere tcp/ip protokolü kullanarak tarama yapar. Bu işlemlerde hedef sisteme ait servislerdeki güvenlik zaafiyetlerini belirleyebilir. Hedef sistemde bulunan fakat dışarıya bir servis olarak sunulmayan güvenlik açıklarını belirleyemez. Mesela normal güvenlik tarayıcıları bir sistemde hangi güvenlik yamalarının eksik olduğunu belirleyemez .
Nessus burda bir adım öne çıkarak belirtilen hedef sisteme SSH(Linux, UNIX) ve ya smb(MS Windows©) üzerinden bağlanarak(doğru erişim bilgileri verilmek sureti ile) işletim sistemine ait güvenlik yamalarını belirleyebilir.

Güncel olarak Nessus aşağıda belirtilen işletim sistemlerine ait gerekli yamaları inceleyebilir.

- AIX 5.x
- Debian
- Fedora Core 1 and 2
- FreeBSD 4.x, 5.x (including the port collection)
- Gentoo Linux (all advisories from 2004)
- HP-UX (10 and 11)
- Mac OS X (and Mac OS X Server)

- Mandrake Linux (8.0 to 10.0)
- RedHat Enterprise Linux (2.1 and 3.0)
- Solaris (2.5.1, 2.6, 7, 8 and 9)
- SuSE Linux (7.0 to 9.1)
- Microsoft Windows NT, 2000, XP, 2003

http://nessuswx.nessus.org/ adresinden Windows için istemci

edinilebilir.

Nessus Web Arabirimleri

Bilbo http://www.doc-s.co.uk/
NessusWC http://www.frank4dd.com/sw.htm

John The ripper

John the Ripper, Linux/UNIX/Windows sistemlerinde çalışan hızlı bir parola kırma programıdır. Temel amacı zayıf UNIX parolalarını kırmak olsa da birçok sistem için parolar kırma işlemini başarılı bir şekilde yerine getirir. JTR in başarılı bir şekilde kırabileceği bazı parola tipleri;

- Parola ile korunmus Microsoft Office dosyaları
- Internet Explorer da saklanan parolalar
- Adobe Acrobat parolaları
- Outlook/Outlook Express parolaları
- Parola ile korunmuş birçok zip formatı(zip, rar, arj, ace).
- Yahoo!, MSN, ICQ gibi populer programların parolaları.
- Windows9x/me/2000/XP ve Unix isletim sistemi parolaları.

http://www.openwall.com/john/ adresinden programile ilgili detay bilgiye erişilebilir

Antivirüs ve Rootkit Araçları

ClamAV

Açık kod antivirüs yazılımıdır.

Özellikleri;

- Komut satırından yönetim.
- 34000 den fazla viru, worm ve trojans imzasını tanır
- Sıkıştırılmış dosyalarını tarayabilme

    - RAR (2.0), Zip, Gzip, Bzip2, Tar, MS OLE2, MS Cabinet files, MS CHM (Compressed HTML), MS SZDD
- Hızlı güncellenen virüs veritabanı
- Haftada birkaç kere güncelleniyor, virüs belirtisinin ardından saatler içerisinde.
- Otomatik güncelleme imkanı(freshclam)
- Kendi virüs imzalarınızı ekleme imkanı

Desteklediği Platformlar
Linux, Solaris, FreeBSD, OpenBSD, NetBSD, AIX, Mac OS X

Lisansı : GPL

Online Virüs Tarama Hizmeti

http://test-clamav.power-netz.de/ adresinde altyapısı ClamAv kullanılarak hazırlanmış online virüs tarama hizmeti bulunmaktadır. Bilgisayarınızdaki herhangi bir dosyayı en güncewl virüs veritabanının bulunduğu bu sayfadan kontrol ettirilebilir.

3. parti yazılımlar

ClamAV ile birlkte çalışan bazı 3.parti yazılımlar:**qSheff**

qSheff, qmail e-posta sunucusu ile çalışan virüs ve spam taraması yapabilen gelişmiş özelliklere sahip bir içerik filitreleyicidir. qmail-queue 'nun yerine geçerek qmail-smtpd veya qmail-inject ile gelen e-postaları önce kendisi alır. İçerik taramasından sonra eğer e-postanın geçişine izin veriyorsa kuyruğa bırakıyor ve yoluna devam etmesini sağlıyor. qSheff, e-postaları kuyruğa girmeden keserek e-posta sunucunun yükünü büyük oranda azaltmaktadır.

DansGuardian Anti-Virus Patch

mod_clamav

ClamAV module for ProFTPD
ClamWin
Webmin ClamAV
snort-inline

Refransları;

- SourceForge:
- The MacOSX server features page
- OnLamp
- DynDNS:
- FastMail
- Tüm referanslara ulaşmak için http://www.clamav.net/whos.html#pagestart adresi ziyaret edilebilir.

RootKIT

Rootkit Hunter Unix, Linux benzeri işletim sistemleri için rootkit tarama aracıdır. Rootkithunter ,bash, perl scriptleri ve rootkitler'in imzalarını tuttuğu bir veritabından oluşmaktadır. Kullanım oldukça basit olmasına rağme kullanım sonrası verdiği çıktıları anlamak için bazı detaylarının bilinmesinde fayda vardır.

Rootkitler değiştirilmiş sistem binarylerini kontrol ederken üzerinde tuttukları veritabanı ile karşılaştırırlar. Eğer bu veritabanına uymayan bir rootkit yüklenmişse sisteme rootkit tarayıcı programlar bunu tanıyamaz. Budurumda rootkit tarama programlarının sunduğu ileri düzey seçenekler kullanılarak anormallikler belirlenebilir.

Kaynaklar:

www.Rootkit.com
www.Rootkit.org
www.Rootkit.nl

Squid

Eklenecek***

DansGuardian

Squid ya da Oops ile kullan
Labilen tam donanımlı içerik filtreleyicidir. Squid ile yapılamauacak birçok filtreleme özelliği Dansguardian ile kolaylıkla yapılabilir.

Dansguardian'in temel özellikleri;

- Siteleri PICS(http://www.w3.org/PICS/) etiketleme sistemine göre bloklayabilir

- MIME tipine ve dosya uzantısına göre filtreleme yapabilir.
- Düzenli ifadeler ile URL filtreleme yapabilir.
- IP tabanlı URL filtreleme
- Veritabanına uygun CSV formatında log üretir.
- Belirli IP ve kullanıcı adına göre filtreleme

Sunucu izleme araçları

Nagios

Nagios açık kodlu host, ağ ve servis gözlem sistemidir. Sistem yöneticisi tarafından belirlenen gözlem parametrelerine göre belirli sistemleri, servisleri gözlemleyerek servislerde meydana gelebilecek problemleri sistem yöneticisine çeşitli şekillerde(E-posta, SMS, SNMP, Anlık mesajlaşma (IM)) bildirebilir.

Nagios'a ait bazı önemli özellikler;

- Çeşitli ağ servislerini gözlemleyebilir(SMTP, POP3, HTTP, NNTP, PING,vb)
- İşletim sistemine ait çeşitli yerel kaynaklarıgözlemleyebilir(işlemci yükü, bellek kullanımı , disk kullanımı, çalışan prosesler)
- Uygun eklentilerle ortam sicakligi gibi fizikesel verileri izleyebilir
- Modüler yapısı sayesinde 3. şahıslar tarafından yazılan çeşitli eklentiler kullanılabilir ya da kendi istediğiniz eklentiyi yazıp kullanma imkanı sunar
- GPL Lisansı ile özgür dağıtım ve kullanım hakkı
- CGI tabanlı web arabiriminden kolay yönetim ve izleme imkanı
- Zamanlanabilir ayarlama imkanı
- Kolay kurulum ve yönetim
  - Debian, Suse, Mandrake gibi Linux dağıtımları ile birlikte gelmektedir. BSD sistemler için port ağacından kurularak kullanılabilir.
- Açık, detaylı dökümantasyon
- E-posta listeleri aracılığı ile geniş destek.

Kaynaklar:

http://www.enderunix.org/docs/nagios.pdf
http://www.nagios.org/docs/
http://www.linuxjournal.com/article/6767

http://www.onlamp.com/pub/a/onlamp/2002/09/05/nagios.html
http://seminer.linux.org.tr/seminer-notlari/nagios-140504.sxi

Huzeyfe ÖNAL <**huzeyfe@EnderUNIX.org**>