GÜVENLİK DUVARI VE TEKNOLOJİLERİ

Yasin ALTUNBAŞAK

GİRİŞ

İnternet ve teknolojilerinin hızla gelişmekte olan bulunduğumuz dönemde, şirketlerin ve bireylerin kullandığı bilgisayar tabanlı tüm cihazların güvenliği giderek daha önemli bir hal almaktadır. Bu güvenliği sağlamak için IT ekiplerinin bu alanda önemli çalışmalar yapmış olduğu ve yapmaya devam ettikleri **güvenlik duvarı (Firewall)**, firma ve kişilerin tüm verilerini, elektronik cihazlarını güven altına almaları için çok ciddi önem arz etmektedir.

Güvenlik Duvarı (Firewall) Nedir?

Firewall bilgisayar sistemleri için üretilen güvenlik duvarı sistemleridir. Firewall cihazları ise bu yazılımların uygun donanımlarla birleştirilerek üretilmesinden meydana gelmiş olan fiziksel ürünlerdir. Firewall kelimesi Türkçede "güvenlik duvarı" olarak ifade edilir.

Güvenlik duvarları yani firewall sistemleri, gelen ve giden tüm ağ trafiğini kontrol ederek belirli filtrelerden geçirip, ağ trafiği içerisindeki zararlı eylemleri durdurmayı amaçlar. Bu sayede ağ güvenliği sağlanır. Şirket içi ağ veya ağlar üzerindeki cihaz ve bilgisayarlarınızı diğer ağlar (internet) üzerinden gelecek saldırılara karşı koruyan, iç ve dış ağlar arası ağ trafiğini (network) belirli kurallara göre denetleyen bir güvenlik mekanizmasıdır.

Temel olarak firewall, network üzerinde kendisine gelen paketlerin ulaşması gereken yerlere (önceden tanımlanmış kurallarla) gidip gidemeyeceğine karar verir. Güvenlik duvarı üzerinde belirtilmiş kuralla uymayan trafiği engelleyerek koruma sağlanır. Ayrıca birçok firewall, kullanıcıların istek paketlerini ağa gitmeden önce karşılayacağı bir Proxy sunucusuna sahip olabilir veya bir Proxy ile çalışabilirler.

Firewall Nasıl Çalışır?

Özel kurallar ve belirli protokoller üzerinden ağı denetleyen ve gelebilecek dış tehlikelere karşı kullanıcının cihazlarını ve sistemlerini güvenli konuma getiren Firewall; mevcut ağı denetleyerek dışarıdan gelen ve ağı tehdit eden davranışlara karşı bir kalkan görevi görür. Firewall çalışma prensipleri, IT ekiplerinin ya da kullanıcıların belirlemiş olduğu kurallara dayanır. Önceden belirlenmiş kurallar çerçevesinde hareket eden güvenlik sistemleri, belirlenmiş olan protokollere uygun olmayan bir trafik tespit ettiğinde ağa erişimi engeller ve güvenli bir katman oluşturarak bu trafiğin akışını keser. Bu sayede sadece izin verilen ve kurallara uyan ağ trafiğinin akışına izin erir. Evdeki veya şirketteki internet ile ağ arasındaki iletişimin güvenli bir seviyede olmasına ve öyle kalmasına ortam sağlar.

Küçük bir ağı korumak veya konumlandırmak kolaydır. Ancak günümüz teknoloji dünyasında ev içi ağlarda dahi birçok cihaz ve uygulama kullanmaktayız. Bu noktada her geçen gün yeni bir siber saldırıya maruz kalmaktayız. Özellikle de saldırganlar iç ağımıza sızmak için yepyeni saldırı türleri ve mekanizmaları kullanmaya başlamışken. Bu saldırılardan korunmak için yazılımsal veya donanımsal firewall cihazları kullanmak zorunlu hale gelmiştir.

Gelişen ve yenilenen teknoloji karşısında neredeyse her yerde Firewall kullanımına tanık olabilirsiniz. Küçük ve büyük ölçekteki herhangi bir şirket veya işletme, internet ağını ve cihazlarını korumak için Firewall hizmetlerinden faydalanır. Siber saldırılar karşısında cihazlarınızı ve bilgilerinizi korumak için hazırlanmış olan bu sistemler, White List yani beyaz liste mantığı ile çalışır. Bu liste içerisine dahil edilen servisler, portlar, işlemler ve ağ trafiklerini, güvenli bir şekilde kullanılmasına izin verir. Bu liste dışarısında kalan aktiviteleri ise zararlı görerek bloke eder.

FİREWALL TEKNOLOJİLERİ VE TÜRLERİ

Güvenlik duvarları geleneksel olarak bir ağ bağlantısı üzerinden satır içi olarak yerleştirilir ve bu noktadan geçen tüm trafiğe bakar. Bunu yaparken, hangi ağ protokolü trafiğinin iyi huylu olduğunu ve hangi paketlerin bir saldırının parçası olduğunu söylemekle görevlendirilirler. Güvenlik duvarları, trafiği zararlı içeriği elemek için tasarlanmış önceden belirlenmiş bir dizi kurala göre izler. Hiçbir güvenlik ürünü tüm içeriğin amacını tam olarak tahmin edemese de güvenlik teknolojisindeki gelişmeler, diğer kuruluşlara daha önce yapılan saldırıların sinyalini vermiş olan ağ verilerinde bilinen kalıpları uygulamayı mümkün kılıyor.

Tüm güvenlik duvarları, belirli bir paketin -veya bir işlemdeki paket kümesinin- amaçlanan alıcıya güvenli bir şekilde yönlendirilebileceği kriterleri tanımlayan kurallar uygular. Bugün kurumsal ortamlarda önemli roller oynamaya devam eden beş güvenlik duvarı türü şunlardır;

Birinci Nesil Firewall (Paket Filtre Güvenlik Duvarları)

Son derece basit ve pratik bir şekilde hazırlanmış olan 1.nesil internet güvenlik sistemi, 1988 yılında Digital Equipment Corporation'dan Jeff Mogul tarafından hazırlanmıştır. Birkaç küçük kural ve protokol ile hazırlanmış olan bu sistem, hızla yayılıp şirketler ve kuruluşlar tarafından kullanılmıştır. Paket filtre olarak hazırlanan bu basit sistem yıllar içerisinde gelişmiş ve daha karmaşık bir hâl almıştır. AT&T'den Bill Cheswick ve Steve Bellovin, ilk nesil güvenlik duvarı üzerinde çalışmalar yaparak kendi firmaları için geliştirmiştir. İlk geliştirilen bu filtre sayesinde istenmeyen ve zararlı paketler engellenerek veri akışının ve cihazların güvenliği sağlanır.

İkinci Nesil Firewall (Devre Seviyesi Güvenlik Duvarları)

Devre düzeyindeki ağ geçitleri, kötü amaçlı içeriği tanımlamanın nispeten hızlı bir başka yolunu kullanarak, başlatılan oturumun meşru olup olmadığını belirlemek için yerel ve uzak ana bilgisayarlar arasında oluşturulurken, ağ üzerindeki TCP el sıkışmalarını ve diğer ağ protokolü oturum başlatma mesajlarını izler. Uzak sistem güvenilir olarak kabul edilir. Ancak paketleri kendileri incelemezler.

Devre düzeyindeki ağ geçitleri, paket filtreleyen güvenlik duvarlarından daha yüksek düzeyde güvenlik sağlarken, diğer sistemlerle birlikte kullanılmaları gerekir. Örneğin, devre seviyesindeki ağ geçitleri tipik olarak uygulama seviyesindeki ağ geçitlerinin yanında kullanılır. Bu strateji, paket ve devre düzeyinde ağ geçidi güvenlik duvarlarının özniteliklerini içerik filtreleme ile birleştirir.

Üçüncü Nesil Firewall (Uygulama Seviyesi Güvenlik Duvarları)

Gene Spafford, Bill Cheswick ve Marcus Ranum'un yayınları ile tanımlanmış olan üçüncü nesil güvenlik duvarları, uygulama seviyesi güvenlik duvarları ya da Proxy tabanlı güvenlik duvarları olarak bilinir. OSI katmanlarında çalışma sergileyen bu sistemler, internet üzerindeki Proxy ayarlarına izin vererek hangi sitelerin güvenli olduğunu ve hangi ağ trafiklerine izin verilmesi gerektiğini belirler. SEAL Product olarak piyasaya sürülen üçüncü nesil ilk Firewall, daha iyi filtreleme hizmeti vererek güvenlik seviyesini bir üst noktaya taşır. Bu sayede ağ sistemlerinin ve cihazların, yeni nesil saldırılara karşı güvenliği sağlanır.

Uygulama katmanı güvenlik duvarları, kurumsal kaynakları web uygulaması tehditlerinden korumak için en iyi şekilde kullanılır. Hem zararlı sitelere erişimi engelleyebilir hem de güvenlik duvarından hassas bilgilerin sızdırılmasını önleyebilirler. Bununla birlikte, iletişimde bir gecikmeye neden olabilirler.

Durum Bilgisi Olan Güvenlik Duvarı

Duruma duyarlı cihazlar yalnızca her paketi incelemekle kalmaz, aynı zamanda bu paketin kurulu bir TCP veya başka bir ağ oturumunun parçası olup olmadığını da takip eder. Bu, tek başına paket filtreleme veya devre izlemeden daha fazla güvenlik sunar, ancak ağ performansı üzerinde daha büyük bir etki yaratır.

Durum bilgisi olan denetimin başka bir çeşidi, yedi katmanlı Açık Sistemler Ara Bağlantısı (OSI) modelinin birden çok protokol katmanında işlemdeki işlemlerin akışını dikkate alan çok katmanlı denetim güvenlik duvarıdır.

Çoğu kuruluş, durum bilgisi olan bir inceleme güvenlik duvarının kullanımından yararlanır. Bu cihazlar, güvenlik duvarı içindeki bilgisayarlar ve diğer varlıklar ile kuruluşun ötesindeki kaynaklar arasında daha kapsamlı bir ağ geçidi görevi görür. Ayrıca, ağ cihazlarını DoS gibi belirli saldırılara karşı savunmada oldukça etkili olabilirler.

Sonraki Nesil Güvenlik Duvarları

Renkli ve görsel bir arayüze sahip olan ilk sistemler, 1992 yılında Bob Braden ve Annette DeSchon tarafından dördüncü nesil paket filtreleme hizmeti olarak geliştirilir. 1994 yılında CPST ismiyle bilinen bir İsrail firması, bu servisi bir seviye öteye taşıyarak piyasaya sürer. Firewall-1 adıyla anılan bu servis, ağ üzerindeki tüm izinleri denetleyerek kişisel verilerin ve cihazların korunmasını sağlar. Bu tariften sonra geliştirilen güvenlik duvarları dördüncü, beşinci ve yeni nesil güvenlik duvarı adını alır. Derin Paket Kontrol adı verilen güvenlik moturundan gücünü alan ve IPS olarak bilinen teknolojileri birleştiren yeni nesil güvenlik duvarları, artık daha güçlü ve güvenli bir hâle gelir. Tam bu noktada da UTM yani Unified Threat Management adıyla bilinen güvenlik duvarı cihazları ortaya çıkar**.**

Sonraki nesil güvenlik duvarları, sağlık veya finans gibi ağır şekilde düzenlenmiş sektörlerdeki kuruluşlar için önemli bir korumadır. Bu güvenlik duvarları, tehdit ortamının ne kadar tehlikeli olduğu konusunda güçlü bir kavrayışa sahip olanlara hitap eden çok işlevli yetenek sunar. Sonraki nesil güvenlik duvarları, çoğu durumda yüksek derecede uzmanlık gerektiren diğer güvenlik sistemleriyle entegre edildiğinde en iyi şekilde çalışır.

Yapılarına Göre Güvenlik Duvarı Sistemleri

Şirketlerin ve kurumların güvenliğini sağlamak ve siber saldırılara karşı korumak amacı ile hazırlanmış olan güvenlik duvarı sistemlerini iki sınıfa ayırmak mümkündür. Bunlar yapılarına göre ve mimarisine göre olarak sınıflandırılır. Yapılarına göre hazırlanmış olan firewall sistemleri yazılımsal ve donanımsal olarak karşımıza çıkar. Mimarisine göre hazırlanmış sistemler ise; Statik Paket Filtre Firewall'lar, Devre Seviyesi Firewall'lar, Dinamik Paket (Durum Denetimli) Filtre Firewall'lar, Proxy Destekli Firewall'lar ve Melez (Hibrit) Firewall'lardır.

Yazılımsal Güvenlik Duvarı Sistemleri

Herhangi bir bilgisayar üzerinde rahatlıkla çalışabilen yazılımsal güvenlik duvarı sistemleri, bilgisayara gelen veri akışını kontrol eder ve bu akışın güvenli olmasını sağlar. Oldukça düşük maliyete sahip olan bu sistemler, kurulum ve kullanım açısından da son derece basittir. Az sayıda bilgisayar ağına sahip olan yerlerde kullanıma uygun olan bu sistemler, işletim sistemi üzerinde çalışır. Bu yüzden sunucuya daha falza yük bindirirler. Ayrıca, devre dışı bırakılmaları kolay olduğu için kullanıcılar tarafından kontrol edildiği zaman güvenlik riskleri oluşturabilir.

Donanımsal Güvenlik Duvarı Sistemleri

Yeni nesil Firewall cihazları ve UTM cihazları olarak bilinen donanımsal güvenlik sistemler, router ve benzeri bir donanıma entegre edilmiş cihazlardır. Paket filtreleme yöntemi kullanarak ağa giriş ve çıkışları kontrol edebilmenizi sağlar. Network ile internet arasında bir köprü oluşturarak gelen ve giden trafiği analiz edip yönetirler. İşletim sistemi ya da sunucuya kurulmadığı için performans ve sunucu hızını etkilemezler. Geniş ölçekli ağ kullanan işletmeler için idealdir. Kolayca devre dışı bırakılamadığı için yazılımsal firewall'lara kıyasla daha güvenlidir**.**

Mimarisine Göre Sistemler

Statik Paket Filtre Firewall'lar

Ağ içerisindeki trafikte akan verilerin başlık kısmını okuyup analiz ederek çalışan bu sistemler, ağ üzerinde oluşturduğunuz izinlere göre paketlerin geçişine izin veren bir yapıya sahiptir. Trafikteki verilerin kaynak adresi, hedef adresi, erişmek istediği port ve kullanacağı protokol gibi analizler sonucunda gelen verilerin girişine izin verir ya da engel olurlar. OSI modelinde network katmanında çalışan bu sistemler, eskimiş olmasına rağmen hala tercih edilen sistemler arasındadır. En büyük dezavantajı ise ilk gönderen sistemin bazen tespit edilemiyor olmasıdır.

Devre Seviyesi Firewall'lar

Network Address Translation adı verilen bir ağ adresinin farklı bir adrese dönüştürüldüğü bir tekniği kullanan bu sistemler, güvenli bir katman oluşturmakla görevlidir. Ağ geçidi sistemin yerel ağdaki IP adresini dışarıdan gelen kaynaklardan gizleyerek erişimi kısıtlarlar. Bu sayede esnek bir yapıya sahiplerdir. Paketleri son derece küçük bir ölçekte incelediği için yüksek performans seviyesi gösterirler. Ancak, kaynak ile hedef arasında direkt bağlatı kurmayan bu sistemler, kaynak ile hedef arasında yer alan paketleri analiz edemez.

Dinamik Paket (Durum Denetimli) Filtre Firewall'lar

Verilerin kaynaktan hedefe kadar takibini sağlayan bu sistemler, statik paket filtre güvenlik duvarlarının yetersiz kaldığı durumlar için geliştirilmiştir. Paketin başlığından başlayarak içeriğine kadar pek çok farklı katmanı kontrol eden bu güvenlik duvarları, gelen ve giden paketler hakkında daha fazla bilgi elde edilmesine yardım eder. Bütün portları kapalı devre olarak tutan bu sistemler, yalnızca yetki verildiğinde o portu kullanıma açar. Yüksek seviyede denetim ve kontrol mekanizmasına sahip olduğu için son derece gelişmiş bir sistemdir.

Proxy Destekli Firewall'lar

Application Layer yani uygulama katmanları üzerinde çalışma prensiplerine göre tasarlanmış olan bu sistemlerin en önemli özelliği oturumu kendisinin başlatabiliyor olmasıdır. Kaynak sistem oturum açma isteği gönderdiğinde bu sistem o isteği güvenlik duvarına gönderir ve güvenli duvarı da bunu kaynağa yönlendirir. Oturum açıldıktan sonra da bu işleyiş böyle devam eder ve bu sayede gelişmiş bir güvenlik duvarı önlemi oluşturur. Hedef ile kaynak arasında bir izolasyon görevi sağlayan bu sistemler network güvenliği üst seviyede tutar. Paket içeriklerini doğrudan kontrol edebilirler.

Melez (Hibrit) Firewall'lar

Yukarıda yer alan mimarilerin iki ya da daha fazlasını aynı anda barındıran güvenlik duvarı sistemleridir. Bilgisayar, sunucu, tablet ya da telefon gibi cihazlara ve network'ünüze internet üzerinden gelebilecek siber saldırıları ve zararlı yazılımları engelleyen bir kalkan görevi görür. Farklı protokol ve kurallar ile çalıştığı için son derece güvenli bir mimariye sahiptir. Kaynak ve hedef arasında köprü görevini üstlenen bu sistemler, veri akışını kontrol ederek zararlı olabilecek her türlü girdiyi engeller.

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.

OpenBSD (Packet Filter=PF)

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.

OpenBSD (PF)'ye ait bazı önemli özellikleri:

- Detaylı, anlaşılır dökümantasyon. PF'e ait her özelliğinanlatıldığı 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

OpenBSD'nin kullanım alanları ve detayları aşağıdaki linktedir;

http://csirt.ulakbim.gov.tr/dokumanlar/openbsd_pf_guvenlik_duvari.pdf

Iptables

Iptables linux 2.4.X ve 2.6.X kerneli ile 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:

- 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 Modül Desteği Patch-o-matic(p-o-m)

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.

Iptables'ın Kullanım alanı

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

L7-Filter

Linux 2.4 ve 2.6.X çekirdeklerinde bulunan netfilter altsistemi için uygulama seviyesinde trafik sınıflandırm aaracıdır. Diger trafik sınıflandırma araçlarından farklı olarak uygulama bazında trafigi anlayarak işlem yapar. L7-Filter uygulama katmanı verisini inceleyerek kendisinebelirli olan bir dosya ile karşılaştırarak hangi protokol olduğuna karar verir. /etc/l7-protocols dosyasında protokollere ait söz dizimler yer alır. L7-Filter bu dosyayı kullanarak sınıflandırma yapar. L7-filter gelen ilk 8 pakete(~2kb) bakarak işlem yapar, fakat bu değer değiştirilebilir.

http://www.netfilter.org

Dsniff

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

Dsniff'i 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 xl0 [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.

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

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.

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:

$ openssl dgst -md5 /etc/pf.conf Bir dosyaya ait hash çıkarımı

MD5(/etc/pf.conf)= be11833967a109ad3dd3411bbe32f578/etc/pf.conf dosyasına ait MD5 imzasını alır.

Bu imzayı standart çıktıya değil de bir dosyay yazdırmak istersek

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

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

OpenSSH

Ssh (Secure Shell/Güvenli Kabuk) ağ üzerinden başka bilgisayarlara erişim sağlayan, uzak bir bilgisayarda komutlar çalıştıran ve bir bilgisayardan diğerine dosya taşımamızı 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 kuruluşlar tarafından desteklendiği ve kullanıldığı öğrenilebilir.

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, sshkeyscan, ssh-keygen, sftp-server

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 birlikte

gelmektedir. BSD sistemler için port ağacından kolaylıkla kurulabilir. Oldukça detaylı ve anlaşılır bir man(el kitabı) 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.

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 rawip 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.

Linux, FreeBSD, NetBSD, OpenBSD, Solaris, MacOs X platformlarında desteklenmektedir.

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

]http://www.hping.org

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. Bu durumda rootkit tarama programlarının sunduğu ileri düzey seçenekler kullanılarak anormallikler belirlenebilir.

Kaynakça;

https://www.malwarebytes.com/antirootkit

https://www.mcafee.com

https://www.alastyr.com

https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

https://www.kaspersky.com

https://github.com/antonioribeiro/firewall

https://github.com/vincentcox/bypass-firewalls-by-DNS-history

https://github.com/antirez/hping

https://www.techtarget.com/searchsecurity/definition/firewall

https://github.com/nurupo/rootkit

https://www.siberkavram.com

https://berqnet.com

https://tr.wikipedia.org/wiki/G%C3%BCvenlik_duvar%C4%B1

https://it.bilgi.edu.tr/tr/guvenlik/firewall

https://www.ticimax.com/blog

https://www.forcepoint.com/cyber-edu/firewall