Firewall Nedir?

Bir sistemin özel bölümlerini halka açık bölümlerinden ayıran, insanların kendilerine tanınan haklardan daha fazlasını almalarını engelleyen yapılardır.

Ilk kullanılan bilgisayar güvenlik duvarı; routing yapamayan bir UNIX makinasıydı. Bilgisayarın üzerindeki bir ethernet kartı internete bağlı, diğer ethernet kartı ise yerel ağa bağlı bulunmaktaydı. Yerel kullanıcılar internete erişmek için Unix(firewall) makinaya giriş yapmaları gerekiyordu, daha sonra sunucu makinanın kaynaklarını kullanrak internet imkanlarına erişiyorlardı.

IpTables ve IpChains Ile Firewall

Mert ALTA
mertalta@yahoo.com

Firewall Nedir?

- Firewall olarak kullanılacak bilgisayarın;
  - Yerel ağ ile internet arasındaki tek geçiş noktası olması gerekir.
  - Akan trafiği anlamlı kurallar doğrultusunda incelemesi gerekir.
  - Kurallara uygun verilerin diğer tarafa geçişini sağlaması gerekir.

Firewall Çeşitleri

- Paket filtreleyen
- Proxy
- Network Address Translation (NAT)
- Saldırı Tespit
- Kayıt tutma

Packet filtreleyen

- Nasıl Çalışırlar
  - Paketin başlığını okur ve, geçerli bölümlere göre filtreleme yapar.
  - SYN bayrakları router'a bağlantının yeni veya dışarı giden paketlere sahip olduğunu açıklar.
  - Paket filtreleri, dump, standart, özelleştirilmiş, stateful(duruma bağlı) şekillerinde olurlar.

Standard packet filtreleme

- Portlar açık olduğu sürece bağlantıya izin verir.
- Yeni geridönmüş bağlantıları SYN bayrağı sayesinde reddeder.
- Örnekler: Cisco ve diğer router'lar, Karlbridge, Unix sunucuları, steelhead.

Packet filtreleyen güvenlik duvarlarının zayıflıkları

- Kuralları aşmak kolaydır.
- Iyi kayıt tutmak zordur.
- Gizli taramalar iyi çalışır.
- Paket fragmentleri, IP opsiyonları, ve kaynak dolaştırma kolaydır.
- Routerlar genelde son noktalarda şifre sorgulama yapamazlar.

Stateful packet filtreleri

- SPFleri ağ üzerindeki son zamanlarda olan hareketliliği takip eder, uygunsuz bir paket bulunursa direk olarak düşürülür.
- Güçlü araştırma motorları paketin içindeki verileri tarayabilir.
- Örnekler: Firewall One, ON Technologies, SeattleLabs, ipfilter

SPF Zayıflıkları

- Standart filtrelemedeki tüm zayıflıklar mevcuttur.
- Öntanımlı ayarlar genelde güvensiz olur.
- Uzaktaki siteden ayrılan paket istemciye gelen paket ile aynıdır.
- İzin verilmiş bağlantıdaki veri zararlı olabilir.
- Genellikle iyi kayıt tutma mekanizmaları yoktur.

Proxy güvenlik duvarları

- Proxy’ler iki ayrı bağlantı arasındaki verinin taşınmasını sağlar.
- Proxy’ler arayüzler arasındaki paketleri taşımamalıdırlar.
- Çeşitleri: circuit level proxy, application proxy, store and forward proxy.

Genel proxy zayıflıkları

- Sunucu makine işlemlerle ilgilendiği için saldırılara açık haldedir.
  - Sunucu daha güvenli hale getirilmelidir.
- Durum IP bloğunda tutulur.
- Spoofing IP & DNS, giriş kontrolu yapılmadığı sürece tehlikelidir.
- Yüksek gecikme ve düşük etkinlik

Network Address Translation (NAT)

- NAT bir paketin içindeki ip adreslerini değiştirerek, yerel istemci ile ilgili bilgilerin dışarı çıkmasını engeller.
- Örnekler: Cisco PIX, Linux Masquerading, Firewall One, ipfilter

IpChains Kurulumu

IpChains'i kullanmaya başlamadan önce çekirdeğimizin bu işlemleri yapabilecek yeteneğe sahip olması gerekir.

Bu sebeple;

/usr/src/linux dizinine geçip

make menuconfig komutu ile çekirdek opsiyonlarını düzenlemeye başlayalım.

Gerekli Olan Seçenekler:

Network firewalls (CONFIG_FIREFALL) [N] Y

IP:Firewalling (CONFIG_IP_FIREWALL) [N] Y

IP:TCP syncookie support (CONFIG_SYN_COOKIES) [N] Y

IP:Masquerading (CONFIG_IP_MASQUERADE) [N] Y

IP:ICMP Masquerading (CONFIG_IP_MASQUERADE_ICMP) [N] Y

bu işlemlerden sonra

make dep ; make bzlilo ; reboot komutları ile yeni çekirdeği etkin hale gelirebiliriz.

IpChains Kullanımı

Ipchains te paketler için ön tanımlı olarak 3 grup vardır.
input: (Giriş) Makinanızanın arayüzüne gelen paketller.
output: (Çıkış) Makinanızın ara yüzünden çıkan paketler.
forward: (Yönlendirme) Makinanızın bir arayüzünden gelip , diğer arayüzüne geçen paketler
(MASQUARING gibi)
bunların dışında kullanıcıların kendilerine grup tanımlayabilirler. Kendi grubunuzu tanımlamak için
 # ipchains -N grubadı komutu ile belirtilen grub adında bir grub oluşur.

IpChains Parametreleri

-A: (Append) Yeni bir kural ekleme
-D: (Delete) Tanımlanmış bir kuralı silme
-R: (Replace) Bır kuralı değiştirmek için kullanılır.
-I :(Insert) Araya kural eklemk için kullanılır
-F:(Flush) Bir kurallar tablosunun tamamen silinmesini sağlar(tablonun içeriği sıfırlanır).
-X: içeriği sıfır olan kural grublarını (input , output, forward, kullanıcının tanımladıkları)siler.
-N: (New) Yeni bir kural grubu oluşturur.
-L: (List) Tanımlı kural grublarındaki kuralları listeler
-P:(Policy) ipchains in ön tanımlı kural grublarının kurallarını ayarlar.
-i interface(arayüz):Hangi arayüzün kullanılacağını belirtir.
-s kaynak (source):Paketin geldiği kaynağın IP adresi veya ağ grubunu belirtilir.
-d hedef (destination):Paketin gideceği adres veya adres grubu
-p protokol(protocol):Paketin kullandığı protokol adını belirtir.
-j (jump) :Paket ile ilgili hangi kararın verileceğini belirtir.
-l log(kayıt) :Paket ile ilgili bilgilerin log dosyasına yazılmasını sağlar
-v (verbose):Paket ile ilgili detaylı bilgi verir.
! :Bu parametre kuralın değilinıi (tersini) belirtilir.

Karar Mekanizmaları(Policy)

ACCEPT:Paketin kabul edildiğini belirtir.
DENY:Paketin kabul edilmediğini belirtir. Paket blok edilir ve paketi gönderen tarafa hiç bir şey gönderilmez.
REJECT:Paket reddedilir ve paketi gönderen tarafa paketin reddedildiğine dair bilgi gönderilir.
MASQ :Paketin maskelendigini belirtir. (MASQUARING de kullanılır)
REDIRECT:Bir porta (gelen , giden, yönlendirilen) paketin başka bir yerel porta yönlendirilmesi işini yapar.(Genelde Web isteklerini yerel makinadaki proxy portuna yönlendirmek için kullanılır.),
Portlarla ilğili olarakta.
1:1000 ifadesi 1 ile 1000 arasındaki portları tanımlayabilirsiniz.
1500: ifadesi ise 1500 ile 65535 (En sonuncu port) demektir.

IpChains Kullanım Örnekleri

 # ipchains -A input -i eth0 -p tcp -s 193.12.3.100 -d 212.65.128.100 80 -j ACCEPT Bu komut eth0 arayüzüne(-i eth0), 193.12.3.100 IP adresinden (-s 193.12.3.100) gelen (-A input) , tcp (-p tcp) protokolunu kullanan ve 212.65.128.100 IP li (-d 212.65.128.100)bilgisayarın 80 portuna gelen paketleri kabul et(-jACCEPT) manasına gelmektedir.

 # ipchains -A output -s 212.65.128.100 25 -d 0/0 -p tcp -i eth0 -j ACCEPT

Bu komut ise eth0 arayüzünü kullanan 212.65.128.100 IP li makinanın 25 portundan gelen ve herhangi bir yere (0/0) giden tcp protokolu kullananan paketlerin çıkışına (-A output) izin ver (-j ACCEPT) demektir.

#ipchains -A forward -s 0/0 -i eth1 -d 200.1.2.3 -p icmp -j ACCEPT

Bu ifade ise herhangi bir yerden eth1 arayüzüne gelen ve 200.1.2.3 IP li makinaya giden tüm icmp protokolu paketlerini kabul et demektir.

#ipchains -D forward -s 0/0 -i eth1 -d 200.1.2.3 -p icmp -j ACCEPT

İfadesi ile bir üstte oluşturduğumuz kuralı kurallar tablosundan sil demektir.

 # ipchains -P input DENY

 # ipchains -P output DENY

 # ipchains -P forward DENY

Bu komutlar ile ön tanımlı üç kural grubu için gelen paketleri yasakla (DENY) demektir. Bu durumda hiç bir paket giriş
çıkışı olmaz

 # ipchains -A forward -i eth0 -p tcp -s 192.168.1.0/24 -d 0/0 -j MASQ

Bu komut ile yerel ağdan gelen ve dışarı giden (nereye olursa olsun internet veya diğer ağa) tüm paketlere MASQUARING uygula demektir.

IpTables

IpTables Çekirdekte bulunan Ip paket filtreleme kurallar tablolarının yönetimini sağlayan uygulamadır. Pekçok farklı tablolar belirlenebilir, Her tabloda bazı öntanımlı chain'ler bulunmaktadır ayrıca kullanıcıda chain'ler ekleyebilir. Her bir chain paketler kümesine uygulanacak kurallar listesidir. Target'lar ise chain'lara uygun düşen paketlere ne yapılacağını belirler.
Öntanımlı Target'lar;
Accept Paketin hedefine değiştirilmeden ulaşmasını sağlar.
Drop Paketin hiçbir işlem görmemesini sağlar.
Queue Paketi kullanıcı alanına yönlendirir.
Return Kullanımda olan chain'in işleyişini sonlandırıp bir önceki chain'in işleme başlamasını sağlar.

Stateful Firewall

State’ler:

New state; Bir bağlantı gerçekleştirmek için karşı tarafa yollanan ilk paketin durumu NEW olacaktır.

Established state; Bağlantı gerçekleştikten sonra veri transferi amaçlı taşınan tüm paketlerin durumu ESTABLISHED olur.

Related state; Bağlantı gerçekleştirmek amacı ile yollanmış ancak başka bir bağlantı ile ilgili paketlerin durumu.

Invalid state;Yukarıdaki sınıflardan hiç birine uymayan paketlerin durumu.

IpTables - IpChains Arasındaki Farklar

Firstly, the names of the built-in chains have changed from lower case to UPPER case, because the INPUT and OUTPUT chains now only get locally-destined and locally-generated packets. They used to see all incoming and all outgoing packets respectively.
The `-i' flag now means the incoming interface, and only works in the INPUT and FORWARD chains. Rules in the FORWARD or OUTPUT chains that used `-i' should be changed to `-o'.
TCP and UDP ports now need to be spelled out with the --source-port or --sport (or --destination-port/--dport) options, and must be placed after the `-p tcp' or `-p udp' options, as this loads the TCP or UDP extensions respectively.
The TCP -y flag is now --syn, and must be after `-p tcp'.
The DENY target is now DROP, finally.
Zeroing single chains while listing them works.
Zeroing built-in chains also clears policy counters.
Listing chains gives you the counters as an atomic snapshot.
REJECT and LOG are now extended targets, meaning they are separate kernel modules.
Chain names can be up to 31 characters.
MASQ is now MASQUERADE and uses a different syntax. REDIRECT, while keeping the same name, has also undergone a syntax change. See the NAT-HOWTO for more information on how to configure both of these.
The -o option is no longer used to direct packets to the userspace device (see -i above).
Packets are now sent to userspace via the QUEUE target.
Probably heaps of other things I forgot.
Bunlar Dışında parametreler ipchains ile aynı şekilde çalışmaktadır.

IpTables Kullanımı

```
#!/bin/bash
UPLINK="eth1"
ROUTER="yes"
NAT="1.2.3.4"
INTERFACES="lo eth0 eth1"
if [ "$1" = "start" ]
then
echo "Starting firewall..."
iptables -P INPUT DROP
iptables -A INPUT -i ! ${UPLINK} -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -p tcp -i ${UPLINK} -j REJECT --reject-with tcp-reset
iptables -A INPUT -p udp -i ${UPLINK} -j REJECT --reject-with icmp-port-unreachable
#explicitly disable ECN
if [ -e /proc/sys/net/ipv4/tcp_ecn ]
then
  echo 0 > /proc/sys/net/ipv4/tcp_ecn
 fi
for x in ${INTERFACES}
      do
          echo 1 > /proc/sys/net/ipv4/conf/${x}/rp_filter
     done
```

```
if [ "$ROUTER" = "yes" ]
     then
echo 1 > /proc/sys/net/ipv4/ip_forward
               if [ "$NAT" = "dynamic" ]
               then
echo "Enabling masquerading (dynamic ip)..."
 iptables -t nat -A POSTROUTING -o ${UPLINK} -j MASQUERADE
               elif [ "$NAT" != "" ]
               then
echo "Enabling SNAT (static ip)..."
iptables -t nat -A POSTROUTING -o ${UPLINK} -j SNAT --to ${UPIP}
               fi
        fi
elif [ "$1" = "stop" ]
then
 echo "Stopping firewall..."
        iptables -F INPUT
        iptables -P INPUT ACCEPT
iptables -t nat -F POSTROUTING
fi
```