Puesta en marcha de un cortafuegos con Iptables

Administración de Sistemas y Aplicaciones Distribuidas

Gabriel Fernández Díaz y David Morales Sáez

01/12/2011

Índice

1.- Denegación por defectos a todos los servicios

Para cortar la conexión a todos y cada uno de los servicios, hemos de bloquear tanto el tráfico entrante, saliente y de paso, además de limpiar la configuración del iptables y sus parámetros para evitar que algo obstruya su funcionamiento:

```
iptables -F
iptables -X
iptables -Z
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
```

2.- Activar los siguientes servicios con las siguientes especificaciones

IP-SPOOFING: Evitar SPOOFING en nuestras direcciones de red

Los ataques de SPOOFING tienen a llegar desde una IP privada, por lo que rechazamos aquellas IP's privadas más comunes en ataques:

```
iptables –A INPUT –i ppp+ -s 0.0.0.0/8 -j DROP
iptables –A INPUT –i ppp+ -s 127.0.0.0/8 -j DROP
iptables –A INPUT –i ppp+ -s 10.0.0.0/8 -j DROP
iptables –A INPUT –i ppp+ -s 172.16.0.0/12 -j DROP
iptables –A INPUT –i ppp+ -s 198.168.0.0/16 -j DROP
iptables –A INPUT –i ppp+ -s 224.0.0.0/3 -j DROP
```

ICMP: Permitir "pings" a máquinas internas, sólo desde la máquina 172.16.1.20

Para permitir recibir pings a las máquinas internas de la red pero sólo desde la máquina con la IP 172.16.1.20 hemos de incluir estos comandos:

```
iptables -A INPUT -p icmp --icmp-type echo-request -s 172.16.1.20 -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type echo-reply -d 172.16.1.20 -j ACCEPT
```

SSH: Redirigirlo al Puerto 333

Dado que por defecto el Puerto de ssh es el 443, para redirigirlo al Puerto 333 hemos de utilizar el siguiente comando:

iptables -t nat -A PREROUTING -p tcp --dport 443 -j REDIRECT --to-ports 333

FTP: Solo hacia fuera

Para permitir que sólo se pueda acceder a un servidor FTP externo (no uno interno desde fuera) hay que utilizar el siguiente comando:

iptables -A OUTPUT -p tcp --dport 23 -j ACCEPT

SMTP: Solo hacia fuera con la máquina 172.16.1.24

Para permitir utilizar el protocolo SMTP solo hacia fuera, para ser exactos, a la máquina 172.16.1.24, la cual lleva a cabo el relay del correo, primero hay que permitir salir hacia el servidor de relay:

iptables -A FORWARD -i 172.16.9.1 -d 172.16.1.24 -p tcp --dport 24 -j ACCEPT
iptables -A OUTPUT -d 172.16.1.24 -p tcp --dport -j ACCEPT

Ahora, debemos permitir que los paquetes de las conexiones entre la máquina que lleva a cabo el relay y la máquina que inicia la conexión entren:

iptables -A FORWARD -s 172.16.1.24 -p tcp .m tcp --sport 25 -m state --state 'ESTABLISHED' --state 'RELATED' -j ACCEPT

DNS: Ambos sentidos

Dado que el DNS está en la máquina 172.16.1.1, hemos de habilitar el protocolo DNS en ambos sentidos con esa máquina:

iptables -A INPUT -s 172.16.1.1 -p udp -m udp --sport 53 -j ACCEPT
iptables -A OUTPUT -d 172.16.1.1 -p udp -m udp --dport 53 -j ACCEPT

HTTP: Redirigir todas la peticiones salientes al servidor proxy hecho en la práctica anterior

Dado que el servidor proxy está montado en la máquina 172.16.9.1, hemos de redirigir todas las peticiones salientes HTTP a esa IP:

iptables -t nat - I PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination 172.16.9.1:8080
iptables -t nat -I PREROUTING -i eth0 -p tcp --dport 80 -d 172.16.9.1 -RETURN