UT04: Instalación y configuración de cortafuegos - 3) – IPTables.

Nombre: Francisco Jesús García – Uceda Díaz - Albo

Curso: 2º ASIR.

Índice

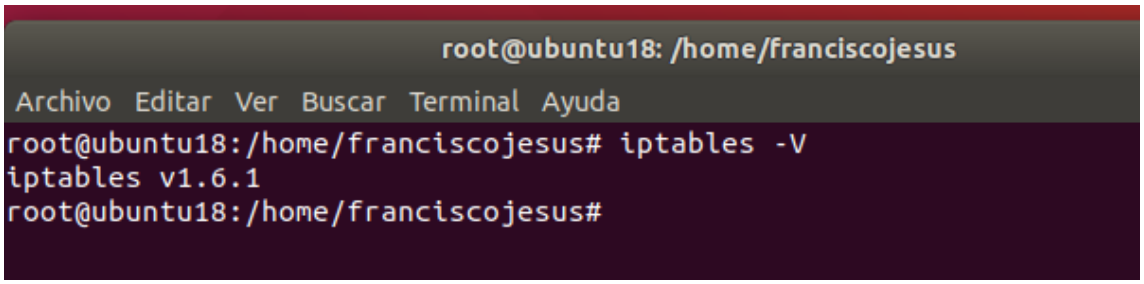
UT04: Instalación y configuración de cortafuegos - 3) – IPTables. 1
Introducción 2
IPTables 2

Introducción

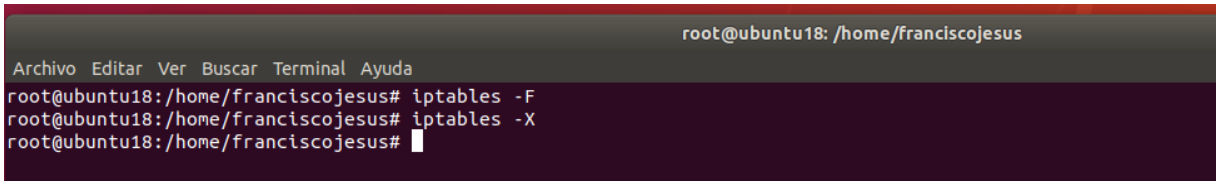
En esta práctica realizaremos distintos ejercicios sobre IPTables en Linux. Los ejercicios realizados serán llevados a cabo según las preguntas que hay en el PDF subidos en la plataforma. Veremos distintos casos en los que usar IPTables según lo pedido en los ejercicios. La verificación se hará en algunos casos con un cliente Windows 7.

IPTables

1º) Ver la versión de IPTables:



2º) Borrado de todas las reglas



3º) Añadir una regla a la cadena INPUT para aceptar todos los paquetes que se originan desde la dirección 192.168.0.155.

```
root@ubuntu18: /home/franciscojesus
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@ubuntu18:/home/franciscojesus# iptables -A INPUT -s 192.168.0.155 -j ACCEPT
root@ubuntu18:/home/franciscojesus#
```

Podemos ver como funciona en un cliente Windows 7:

```
C:\Windows\system32\cmd.exe

C:\Users\FranciscoJesus>ping 192.168.0.154

Haciendo ping a 192.168.0.154 con 32 bytes de datos:
Respuesta desde 192.168.0.154: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.0.154: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.0.154: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.0.154: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.0.154:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\FranciscoJesus>
```

4º) Eliminar todos los paquetes que entren.

```
root@ubuntu18:/home/franciscojesus# iptables -A INPUT  -j DROP
root@ubuntu18:/home/franciscojesus#
```

*Lo realizo desde el mismo cliente de Windows 7 con otra IP para que surja efecto ya que la de arriba tiene priorización:

```
C:\Windows\system32\cmd.exe

C:\Users\FranciscoJesus>ping 192.168.0.154

Haciendo ping a 192.168.0.154 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.0.154:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),

C:\Users\FranciscoJesus>
```

5º) Permitir la salida de paquetes.

```
root@ubuntu18:/home/franciscojesus# iptables -A OUTPUT  -j ACCEPT
root@ubuntu18:/home/franciscojesus#
```

```
root@ubuntu18:/home/franciscojesus# ping 192.168.0.155
PING 192.168.0.155 (192.168.0.155) 56(84) bytes of data.
64 bytes from 192.168.0.155: icmp_seq=1 ttl=128 time=0.895 ms
64 bytes from 192.168.0.155: icmp_seq=2 ttl=128 time=0.842 ms
64 bytes from 192.168.0.155: icmp_seq=3 ttl=128 time=0.731 ms
```

6º) Añadir una regla a la cadena INPUT para rechazar todos los paquetes que se originan desde la dirección 192.168.0.155.

```
root@ubuntu18:/home/franciscojesus# iptables -A INPUT -s 192.168.0.155 -j DROP
root@ubuntu18:/home/franciscojesus#
```

```
C:\Users\FranciscoJesus>ping 192.168.0.154

Haciendo ping a 192.168.0.154 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.0.154:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),

C:\Users\FranciscoJesus>
```

7º) Añadir una regla a la cadena INPUT para rechazar todos los paquetes que se originan desde la dirección de red 192.168.0.0.

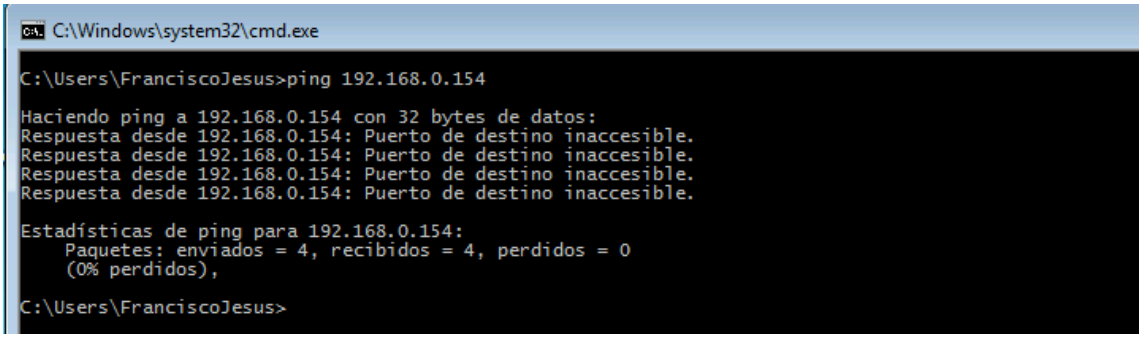
```
root@ubuntu18:/home/franciscojesus# iptables -A INPUT -s 192.168.0.0/24 -j DROP
root@ubuntu18:/home/franciscojesus#
```

```
^C
C:\Users\FranciscoJesus>ping 192.168.0.154

Haciendo ping a 192.168.0.154 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.0.154:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),
```

8º) Añadir una regla a la cadena INPUT para rechazar todos los paquetes que se originan desde la dirección 192.168.0.155 y enviar un mensaje de error icmp.

```
root@ubuntu18:/home/franciscojesus# iptables -A INPUT -s 192.168.0.155 -j REJECT
root@ubuntu18:/home/franciscojesus#
```

Que chulo, esto no lo sabía.



9º) Permitir conexiones locales (al localhost), por ejemplo, a MySQL.

```
root@ubuntu18:/home/franciscojesus# iptables -A INPUT -i lo -p tcp --dport 3306 -j ACCEPT
root@ubuntu18:/home/franciscojesus#
```

10º) Permitir el acceso a nuestro servidor web (puerto TCP 80).

```
root@ubuntu18:/home/franciscojesus# iptables -A INPUT -p tcp --dport 80 -j ACCEPT
root@ubuntu18:/home/franciscojesus#
```

11º) Permitir el acceso a nuestro servidor ftp (puerto TCP 20 y 21).

```
root@ubuntu18:/home/franciscojesus# iptables -A INPUT -p tcp --dport 20 -j ACCEPT
root@ubuntu18:/home/franciscojesus# iptables -A INPUT -p tcp --dport 21 -j ACCEPT
root@ubuntu18:/home/franciscojesus#
```

12ª) Permitimos a la máquina con IP 192.168.0.155 conectarse a nuestro equipo a través de SSH.

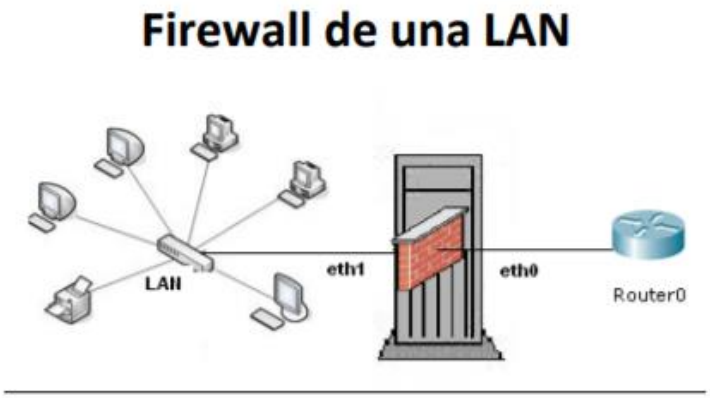
```
root@ubuntu18:/home/franciscojesus# iptables -A INPUT -p tcp --dport 22 -j ACCEPT
root@ubuntu18:/home/franciscojesus#
```

13º) Rechazamos a la máquina con IP 192.168.0.155 conectarse a nuestro equipo a través de Telnet.

```
root@ubuntu18:/home/franciscojesus# iptables -A INPUT -p tcp --dport 23 -j DROP
root@ubuntu18:/home/franciscojesus#
```

14º) Rechazamos las conexiones que se originen de la máquina con la dirección física 00:db:f0:34:ab:78.

```
root@ubuntu18:/home/franciscojesus# iptables -A INPUT -M 00:db:f0:34:ab:78
root@ubuntu18:/home/franciscojesus#
```



15º) Rechazamos todo el tráfico que ingrese a nuestra red LAN 192.168.0.0 /24 desde una red remota, como Internet, a través de la interfaz eth0.

```
root@ubuntu18:/home/franciscojesus# iptables -A FORWARD -s 0.0.0.0 -i eth0 -d 192.168.0.0/24  -j DROP
root@ubuntu18:/home/franciscojesus#
```

Si estamos en la misma red tendremos ping:

```
C:\Users\FranciscoJesus>ping 192.168.0.154

Haciendo ping a 192.168.0.154 con 32 bytes de datos:
Respuesta desde 192.168.0.154: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.0.154: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.0.154: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.0.154: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.0.154:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

En caso de estar en otra red no tendremos ping:

```
C:\Users\FranciscoJesus>ping 192.168.0.154

Haciendo ping a 192.168.0.154 con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.0.154:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),

C:\Users\FranciscoJesus>
```

16º) Cerramos el rango de puerto bien conocido desde cualquier origen:

```
root@ubuntu18:/home/franciscojesus# iptables -A INPUT -s 0.0.0.0/0 -p tcp --dport 1:1024 -j DROP
root@ubuntu18:/home/franciscojesus#
```

17º) Aceptamos que vayan de nuestra red 192.168.0.0/24 a un servidor web (puerto 80):

```
root@ubuntu18:/home/franciscojesus# iptables -A FORWARD -s 192.168.0.0/24 -i eth0 -p tcp --dport 80 -j ACCEPT
root@ubuntu18:/home/franciscojesus#
```

18º) Aceptamos que nuestra LAN 192.168.0.0/24 vayan a puertos https:

```
root@ubuntu18:/home/franciscojesus# iptables -A FORWARD -s 192.168.0.0/24 -p tcp --dport 443 -j ACCEPT
root@ubuntu18:/home/franciscojesus#
```

19º) Aceptamos que los equipos de nuestra red LAN 192.168.0.0/24 consulten los DNS, y denegamos todo el resto a nuestra red:

```
root@ubuntu18:/home/franciscojesus# iptables -A FORWARD -s 192.168.0.0/24 -p tcp --dport 54 -j ACCEPT
root@ubuntu18:/home/franciscojesus#
```

20º) Permitimos enviar y recibir e-mail a todos:

```
root@ubuntu18:/home/franciscojesus# iptables -A FORWARD -s 192.168.0.0/24 -p tcp --dport 25 -j ACCEPT
root@ubuntu18:/home/franciscojesus# iptables -A FORWARD -s 192.168.0.0/24 -p tcp --dport 110 -j ACCEPT
root@ubuntu18:/home/franciscojesus#
```

21º) Cerramos el acceso de una red definida 192.168.3.0/24 a nuestra red LAN 192.168.2.0/24:

```
root@ubuntu18:/home/franciscojesus# iptables -A INPUT -s 192.168.3.0/24 -d 192.168.2.0 -j DROP
root@ubuntu18:/home/franciscojesus#
```

22º) Permitimos el paso de un equipo específico 192.168.3.5 a un servicio (puerto 5432) que ofrece un equipo específico (192.168.0.5) y su respuesta:

```
root@ubuntu18:/home/franciscojesus# iptables -A FORWARD -s 192.168.3.5 -d 192.168.0.5 -p tcp --dport 5432 -j ACCEPT
root@ubuntu18:/home/franciscojesus#
```

23º) Permitimos el paso de paquetes cuya conexión ya se ha establecido o es nueva, pero está relacionada a una conexión ya establecida.

```
root@ubuntu18:/home/franciscojesus# iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
root@ubuntu18:/home/franciscojesus#
```