**IPTABLES**

Es un cortafuegos que decide que se hace con el tráfico de tu máquina.

**Tabla Filter**: INPUT (paquetes de entrada), OUTPUT (paquetes de salida), FORWARD (paquetes de paso a través de mi máquina).

Hay que estar en modo Bridge para realizar las pruebas.

**Iptables –L** Lista las reglas de la tabla por defecto.

**Iptables –P** Cambia las políticas por defecto.

Iptables –P INPUT DROP elimina la política por defecto los paquetes de entradas.

**Iptables –A** Añade una regla.

Iptables –A INPUT –i lo –j DROP Añade una regla que interrumpe el tráfico local que llega a mi máquina.

**Iptables –D** Elimina una regla

Iptables –D INPUT –i lo –j DROP Elimina la regla que interrumpe el tráfico local que llega a mi máquina.

**DROP** (descarta paquetes), **ACCEPT** (acepta paquetes) y **REJECT** (descarta paquetes pero manda un mensaje cuando se intenta realizar una conexión).

Para **cambiar de puerto** en los ping: ping [www.google.es](http://www.google.es) 80 El último número es el del puerto.

-p protocolo

-j acción

-dport puerto de destino

-sport puerto de origen

-d dirección ([www.ugr.es](http://www.ugr.es), etc)

-s origen

-t tabla que utiliza (nat, etc)

Iptables –A OUTPUT –p tcp –dport 80 –j DROP

**telnet** para conectarte y hacer las pruebas. Se puede usar ping pero si no contesta, no tenemos la certeza de que haya o no conexión, ya que algunos sitios no contestan a un ping.

**PRÁCTICA 4 (DUDAS)**

**EJERCICIO 3:**

iptables ­-A INPUT -­i lo -­j DROP

puedes hacer ping a otra máquina de la red o a google pero no a ti mismo (localhost).

**PRÁCTICA 5**

**1 - Hemos visto el funcionamiento del firewall más extendido de Linux, iptables. Después de ver como configurarlo añadiéndole reglas, añádele las reglas necesarias para que nuestro firewall deje pasar las peticiones que se hagan de nuestra red local al usar correo electrónico, sabiendo que estas peticiones usan los puertos 25 SMTP y 110 POP3.**

iptables -A FORWARD -s 190.168.100.2/24 -i ens38 -p tcp --dport 110 -j ACCEPT  
iptables -A FORWARD -s 190.184.100.2/24 -i ens38 -p tcp --dport 25 -j ACCEPT

**2 -**  **Si sólo quisiéramos que el cliente de la red local con la IP 192.168.2.30 pudiera acceder por SSH al servidor, ¿Qué regla deberíamos definir en iptables?**

iptables -A INPUT -s 192.168.2.30 -p tcp --dport 22 -j ACCEPT

**3 - Se dispone de una red local con dirección 192.168.1.0 y máscara 255.255.255.0. Crear un archivo de configuración squid.conf que permita el acceso a Squid a todos los ordenadores de la red y no lo permita a los restantes.**

acl all src 0.0.0.0/0.0.0.0

acl localhome src 192.168.1.0/255.255.255.0

http\_access allow localhome

http\_access deny all

**4 - Crear un archivo de configuración squid.conf para denegar el acceso a todos los equipos a la dirección www.google.es**

http\_port 80 acl all src 0.0.0.0/0.0.0.0

acl nopermitir dstdomain [www.google.es](http://www.google.es)

http\_access deny nopermitir

**5 - Se dispone de una red de área local con dirección 192.168.1.0 y máscara 255.255.255.0. Se desea permitir el acceso a Squid a los ordenadores con las IP que están comprendidas en el rango 192.168.1.1 y 192.168.1.10 (ambas incluidas). Crea en tu  
directorio personal un fichero llamado ip\_permitidas que tenga estas direcciones (cada  
dirección en una línea diferente). A continuación indica que fichero de configuración para Squid crearías para permitir el acceso a Squid a todas estas direcciones y denegar el acceso a las restantes.**

acl localhome src “home/nombre\_usuario/ip\_permitidas”

http\_access allow local\_home

http\_access deny all

**6 - Deniega las conexiones a todos los equipos en horario de 18:00 a 21:00 horas.**

acl horario time 18:00-21:00

http\_access deny horario

**7 - Deniega el acceso a Squid al equipo con IP 192.168.1.5. Permite el resto de accesos a  
Squid.**