Práctica iptables

Comandos útiles:

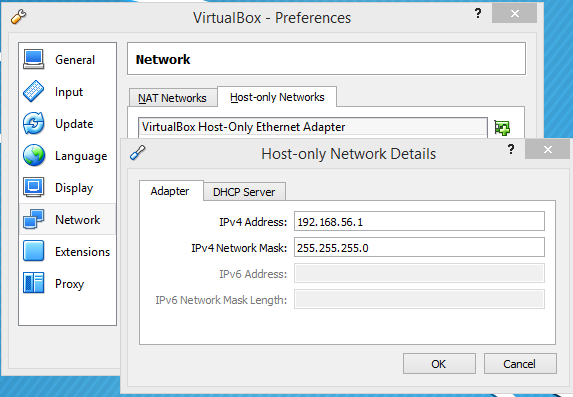
* *Mostrar reglas actuales:*

# iptables --line-numbers –n –L

* *Almacenar reglas actuales:*
* # iptables-save > /root/my.active.firewall.rules
* *Eliminar reglas especificas:*
* # iptables -D TARGET NUMERO
* *Donde TARGET se refiera a INPUT, OUTPUT, FORWARD, y NUMERO al numero de regla en la lista*
* *E.g # iptables -D INPUT 1*

Para los ejercicios en donde se bloquea tráfico, se puede hacer de dos formas: entre compañeros en la misma red, o a través de una red interna en una máquina virtual, de la siguiente forma. En VirtualBox, configurar como adaptador host-only en preferencias de la máquina virtual:

Después, entrar a preferencias generales > red y seleccionar el adaptador host-only, y al editarlo se mostrará la dirección de red con la que la máquina virtual se comunica con el host.



Ejercicio 1: Bloqueo de todo el tráfico

1. Bloquear todo el tráfico de entrada

# iptables –P INPUT DROP

1. Hacer ping desde el host a la máquina virtual.
2. Bloquear todo el tráfico de salida:

# iptables –P OUTPUT DROP

1. Intentar entrar a cualquier página web.
2. Devolver el tráfico a su estado original

# iptables –P INPUT ACCEPT

# iptables –P OUTPUT ACCEPT

Ejercicio 2: Bloqueo de direcciones específicas y de ping

1. Verificar que se pueda hacer ping de otra dirección a la suya exitosamente.
2. Bloquear los paquetes de ping.

# iptables -A INPUT -p icmp --icmp-type echo-request -j DROP  
# iptables -A INPUT -i eth1 -p icmp --icmp-type echo-request -j DROP

1. Volver a hacer ping a su dirección desde otro equipo.
2. Borrar las reglas:

*# iptables -D INPUT 1 (dos veces)*

1. Repetir lo anterior, pero con target REJECT en vez de DROP.
2. Obtener la dirección IP de otro equipo, o usar la del host como se explicó anteriormente.
3. Bloquear tráfico de entrada de la dirección específica

# iptables -A INPUT -s 1.2.3.4 -j DROP

1. Volver a intentar hacer ping a su equipo
2. Borrar la regla:

# iptables -D INPUT 1

Ejercicio 3: Bloqueo de un dominio

1. Verificar que se pueda acceder a la dirección deseada.
2. Obtener dirección IP del dominio (Facebook en este caso, puede hacerse con cualquera)

# host -t a [www.facebook.com](http://www.facebook.com/)

1. Bloquear tráfico de salida a la dirección obtenida:

# iptables -A OUTPUT -p tcp -d 31.13.66.36 -j DROP

1. Abrir el navegador web e intentar acceder a esa dirección.
2. Borrar la regla

# iptables -D OUTPUT 1

1. Bloquear el tráfico, pero ahora dando dominio en vez de dirección

# iptables -A OUTPUT -p tcp -d facebook.com -j DROP

1. Volver a intentar acceder al sitio
2. Borrar la regla

# iptables -D OUTPUT 1