

Practica con iptables.

1. Implementa el cortafuegos propuesto en punto 6.3.4 del libro. Comprueba el funcionamiento de todas sus reglas y haz capturas de pantalla donde se observe.

La maquina al ser el cliente la realizare con Ubuntu 18.04 LTS, la visualización serán en Virtualbox que te adjuntare la maquina como “Cliente Firewall.ova”

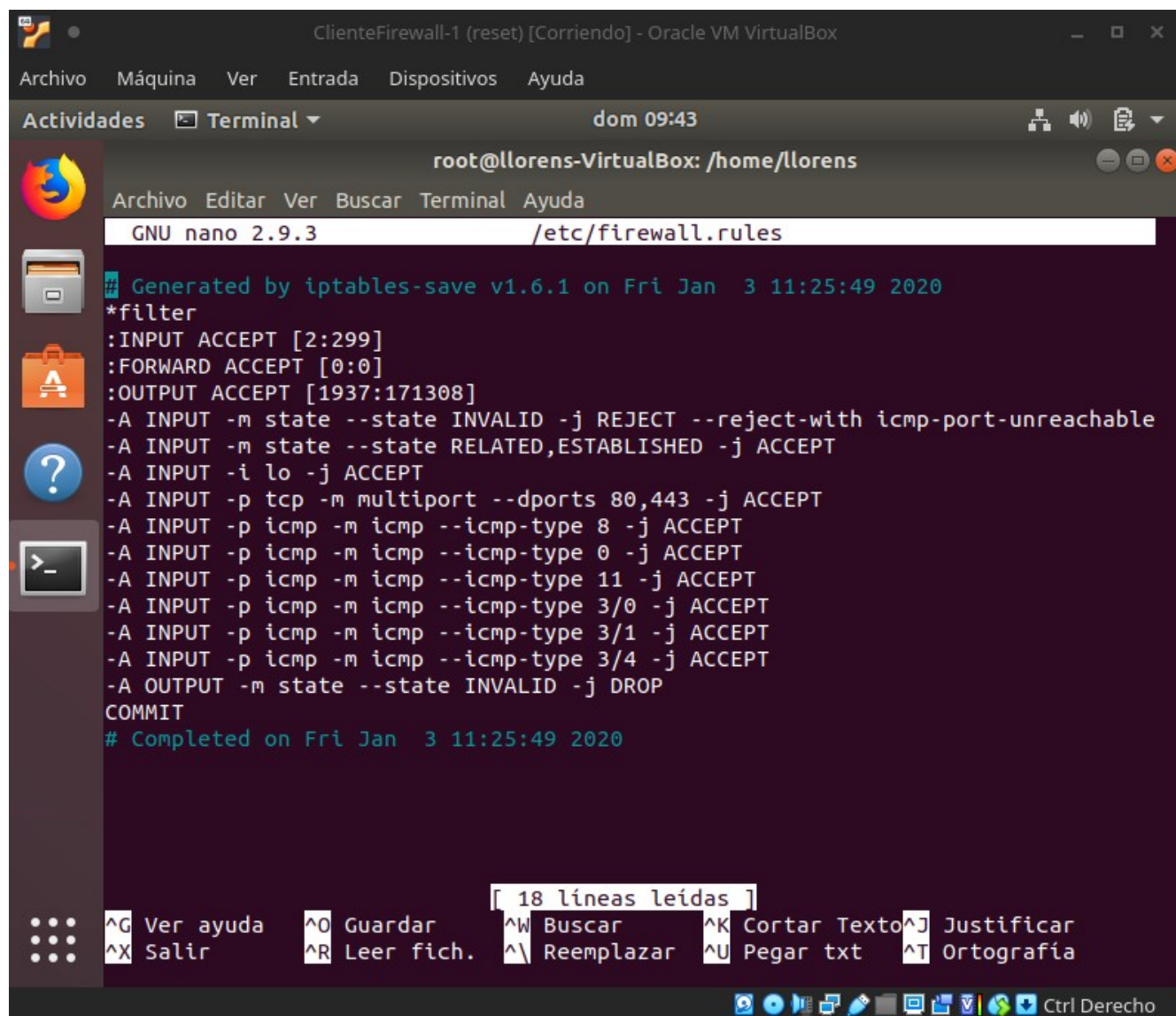
El usuario y la contraseña es

llorens

Primeramente creamos un archivo con las reglas del firewall en /etc/firewall.rules con

`iptables-restore < /etc/firewall.rules`

Seguidamente con nano, editamos el archivo para implementar las reglas del firewall



```
ClienteFirewall-1 (reset) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal  dom 09:43
root@llorens-VirtualBox: /home/llorens
GNU nano 2.9.3 /etc/firewall.rules
# Generated by iptables-save v1.6.1 on Fri Jan  3 11:25:49 2020
*filter
:INPUT ACCEPT [2:299]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [1937:171308]
-A INPUT -m state --state INVALID -j REJECT --reject-with icmp-port-unreachable
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m multiport --dports 80,443 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 0 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 11 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 3/0 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 3/1 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 3/4 -j ACCEPT
-A OUTPUT -m state --state INVALID -j DROP
COMMIT
# Completed on Fri Jan  3 11:25:49 2020
[ 18 líneas leídas ]
^G Ver ayuda  ^O Guardar  ^W Buscar  ^K Cortar Texto  ^J Justificar
^X Salir      ^R Leer fich. ^\ Reemplazar ^U Pegar txt  ^T Ortografía
Ctrl Derecho
```

Practica con iptables.

Realmente se a realizado anteriormente pero estoy realizando la memoria con la practica ya terminada, solo estoy documentado.

Una vez guardado vamos a crear los scripts que describe el libro en la pagina para que en cada reinicio del sistema no haga falta escribir

`iptables-restore < /etc/firewall.rules`

1. Creamos el fichero `/etc/firewall.rules` con las reglas actuales de nuestro sistema:

```
iptables-save > /etc/firewall.rules
```

2. Creamos un *script* de inicio `/etc/network/if-pre-up.d/firewall` con el siguiente contenido:

```
#!/bin/sh
/sbin/iptables-restore < /etc/firewall.rules
```

3. Creamos el *script* de cierre `/etc/network/if.down.d/firewall` con el siguiente contenido:

```
#!/bin/sh
/sbin/iptables-save > /etc/firewall.rules
```

EL CORTAFUEGOS

4. Cada vez que queramos hacer un cambio en nuestro cortafuegos, podemos editar el fichero de reglas y aplicarlas a continuación con `iptables-apply`:

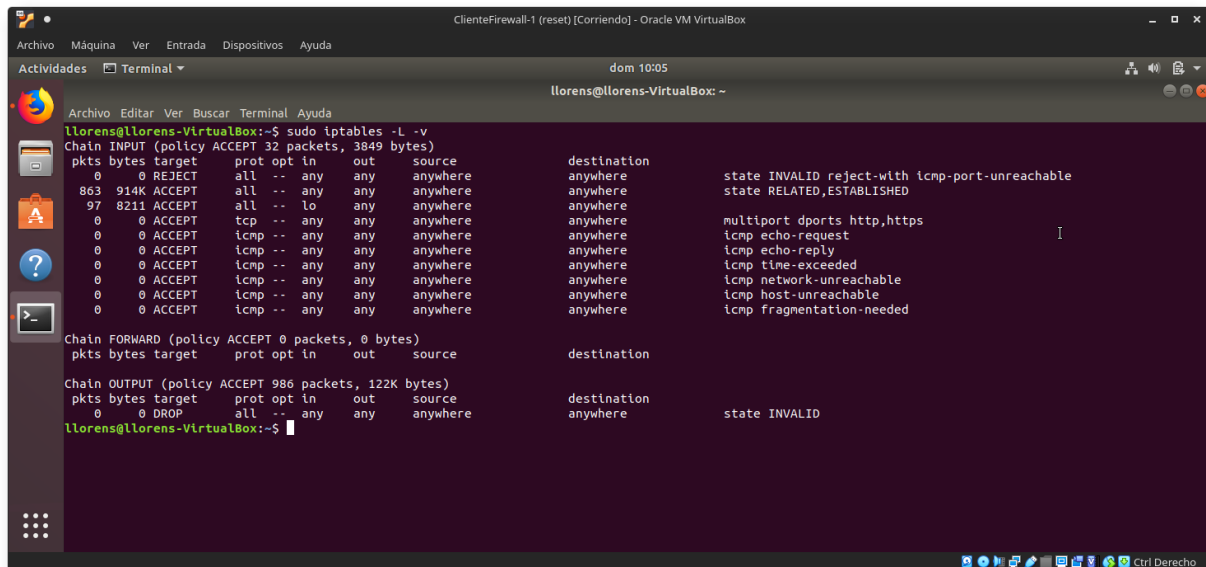
```
nano /etc/firewall.rules
iptables-apply /etc/firewall.rules
```

5. No olvidemos hacer ejecutables ambos scripts (`chmod +x <fichero>`).

Practica con iptables.

Se realiza tal cual describe el libro y después comprobamos si las reglas están aplicadas con:

```
sudo iptables -L -v
```



```
llorens@llorens-VirtualBox:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 32 packets, 3849 bytes)
pkts bytes target prot opt in out source destination state
0 0 REJECT all -- any any anywhere anywhere state INVALID reject-with icmp-port-unreachable
863 914K ACCEPT all -- any any anywhere anywhere state RELATED,ESTABLISHED
97 8211 ACCEPT all -- lo any anywhere anywhere multiport dports http,https
0 0 ACCEPT tcp -- any any anywhere anywhere icmp echo-request
0 0 ACCEPT icmp -- any any anywhere anywhere icmp echo-reply
0 0 ACCEPT icmp -- any any anywhere anywhere icmp time-exceeded
0 0 ACCEPT icmp -- any any anywhere anywhere icmp network-unreachable
0 0 ACCEPT icmp -- any any anywhere anywhere icmp host-unreachable
0 0 ACCEPT icmp -- any any anywhere anywhere icmp fragmentation-needed

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination

Chain OUTPUT (policy ACCEPT 986 packets, 122K bytes)
pkts bytes target prot opt in out source destination
0 0 DROP all -- any any anywhere anywhere state INVALID
llorens@llorens-VirtualBox:~$
```

Se aprecia en chain e input el trafico de paquetes y bytes que han aplicado las reglas del firewall

2.Implementa el cortafuegos propuesto en punto 6.3.6 del libro. Comprueba el funcionamiento de todas sus reglas y haz capturas de pantalla donde se observe. Para realizar la configuración de red necesaria puedes usar máquinas virtuales conectadas mediante red interna o bien montar un proyecto en GNS3. Si optáis por este último caso, por favor, subidlo como proyecto GNS3 exportado a la tarea.

Este ejercicio lo hice con GNS3 pero he tenido problemas al instalarlo ya que aunque activo el enrutamiento descomentando

```
net.ipv4.ip_forward=1
```

en /etc/sysctl.conf

seguidamente aplicando las normas del firewall del libro del ejercicio.

No hay forma de que las otras redes tengan internet, solo tiene internet la que hace de router.

Lo he intentado todo usar la nube NAT o la CLOUD seleccionando previamente las interfaz correspondiente.

Practica con iptables.

Te paso el proyecto por si lo puedes verlo, solo tiene un “pero” que tampoco consigo que inicie automáticamente las normas del firewall, pero estas están guardadas en

`/etc/firewall.rules`

Por lo tanto no puedo realizar los ejercicios.