**Dibujo de una persona

Descripción generada automáticamente con confianza baja**

Enrutamiento NAT

**Carlos González Martín**

Contenido

[1. Primeros pasos 3](#_Toc179130720)

[2. Cambiar el nombre al server 3](#_Toc179130721)

[3. Configurar interfaces 4](#_Toc179130722)

[4. Instalar iptables 6](#_Toc179130723)

[5. Habilitar enrutamiento 6](#_Toc179130724)

[6. IPTABLES 8](#_Toc179130725)

[7. Script 9](#_Toc179130726)

[8. Conclusión 12](#_Toc179130727)

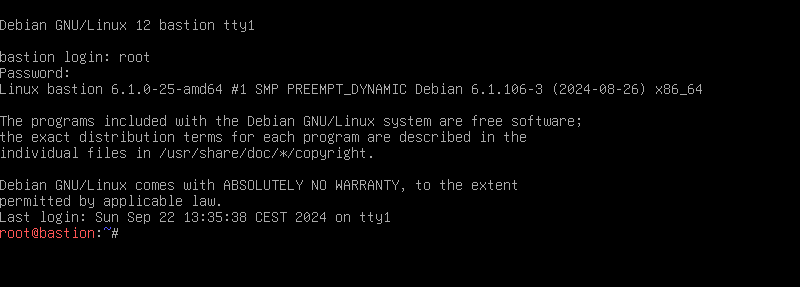
# Primeros pasos

Deberemos tener 2 máquinas en la cual tendremos un bastión y un cliente, el cliente podemos tener tanto Windows como Linux, en el bastión sí que necesitamos un equipo Linux ya que vamos a usar las “maravillosas” iptables, también debe tener 2 interfaces de red en la cual una de ellas estará en red interna conectada al cliente y otra conectada a nuestra red local.

# Cambiar el nombre al server

Una vez arrancado el server procederemos a cambiar el nombre al servidor y poder diferenciarlo, en este caso como solo tenemos un cliente y un server no hace mucha falta, pero cuando tengamos varias máquinas sin interfaz gráfica como es mi caso nos podremos liar si tenemos el mismo hostname

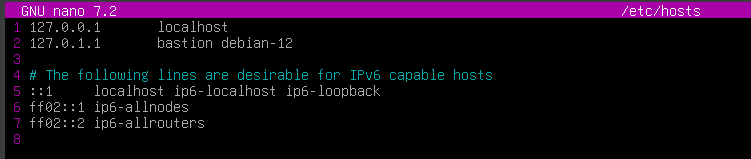
Hostnamectl set-hostname bastion



En mi caso siempre suelo iniciar sesión con superusuario o Root, no es una práctica muy común, pero para estos pequeños casos es mucho mejor ya que así no tenemos que poner todo el rato delante del comando “sudo”.

Ahora cambiamos en el /etc/hosts el nombre que tiene la máquina, ya que a veces nos puede dar fallos la máquina, ya que el DNS interno no encuentra el nombre de la maquina que le hemos indicado anteriormente.

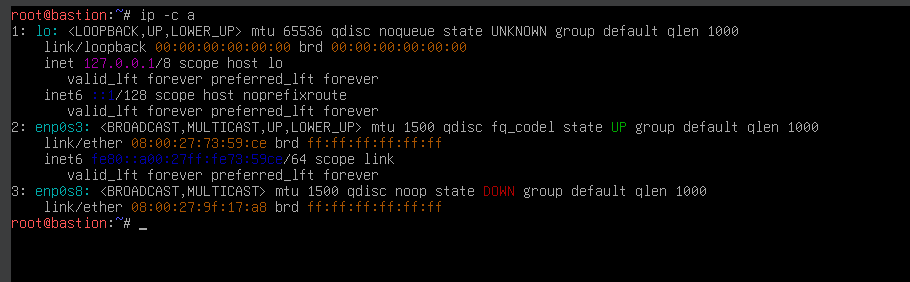
Nano /etc/hosts



# Configurar interfaces

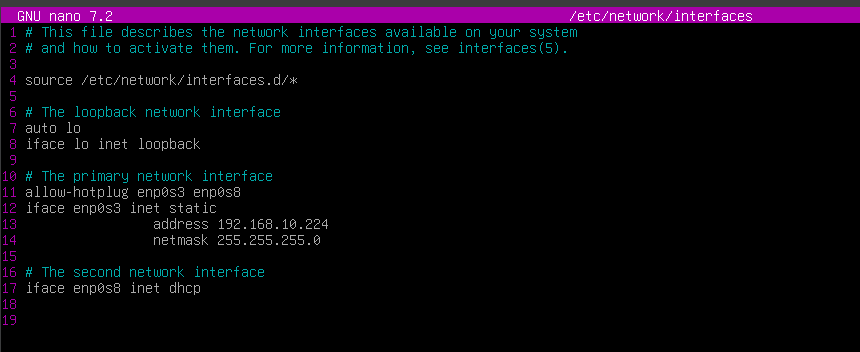
Como vemos haciendo un “ip -c a”, vemos que la primera interfaz esta levantada, pero sin IP, ya que es red interna y la segunda interfaz está en modo puente y no está configurada.

Ip -c a



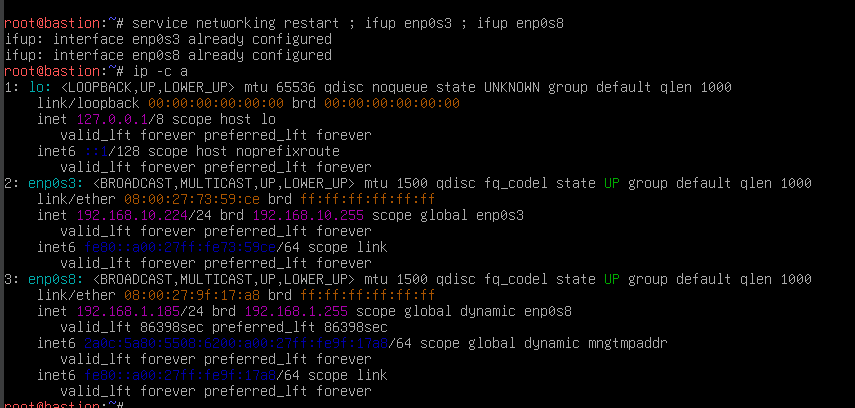
Una vez que hemos visto que no tenemos IPs ni conexión modificaremos el archivo de configuración de la red que está en el directorio /etc/

Nano /etc/network/interfaces



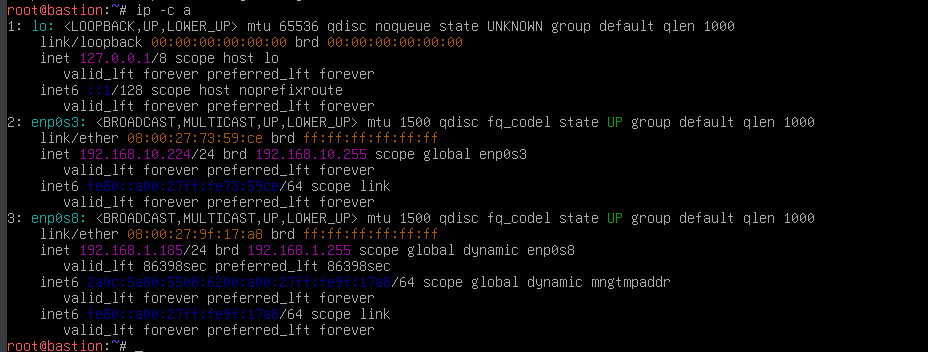
Ahora reiniciamos el servicio, podemos reiniciar la maquina o reiniciar el servicio y levantar los interfaces.

Service networking restart ; ifup enp0s3 ; ifup enp0s8

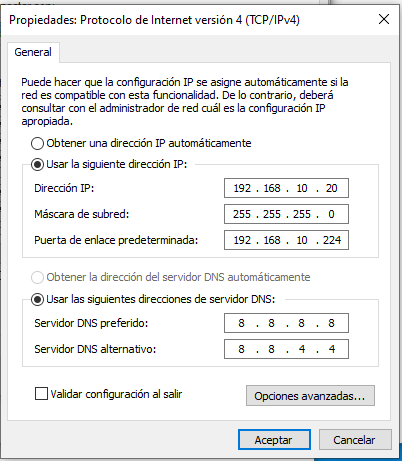


Ahora con un “ip -c a” revisamos si se han levantado los servicios y tienen las direcciones IP correctas.

Ip -c a



Una vez que hemos cambiado las IP al server vamos a cambiárselo al cliente.

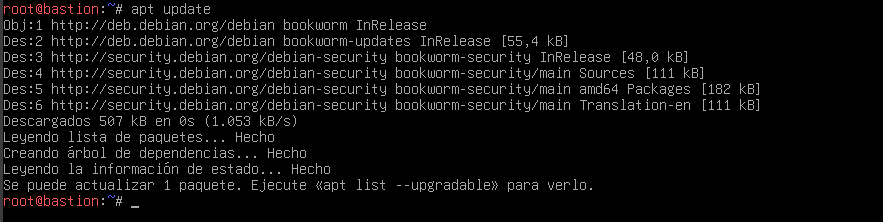


Importante cambiar los DNS preferido para poder comunicarnos con el exterior.

# Instalar iptables

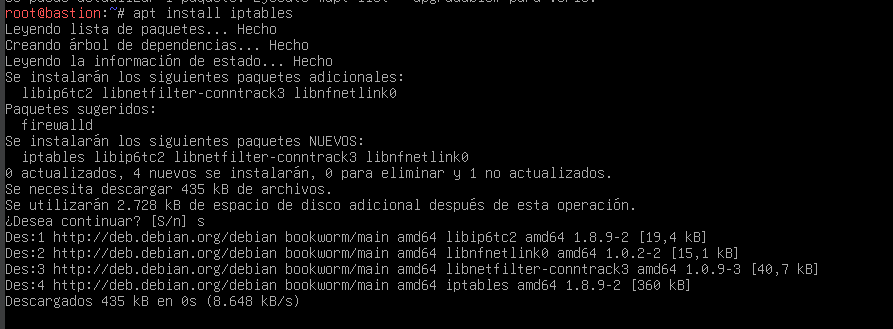
Ahora lo que haremos será comprobar si podemos descargar el paquete iptables, para ello usaremos el comando “APT update”.

Apt update



Una vez que vemos que tenemos conexión a internet procederemos a instalar iptables.

Apt install iptables



# Habilitar enrutamiento

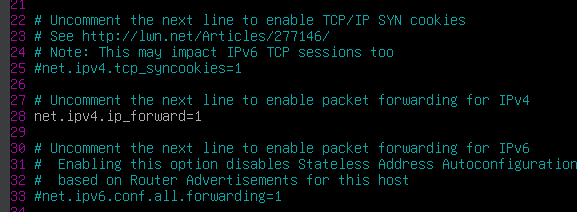
Una vez que hemos instalado el paquete iptables podremos ya configurar todas las reglas iptables.

Echo “1” > /proc/sys/ipv4/ip\_forward



Ahora modificamos la línea 28 del siguiente archivo de configuración.

Nano /etc/sysctl.conf

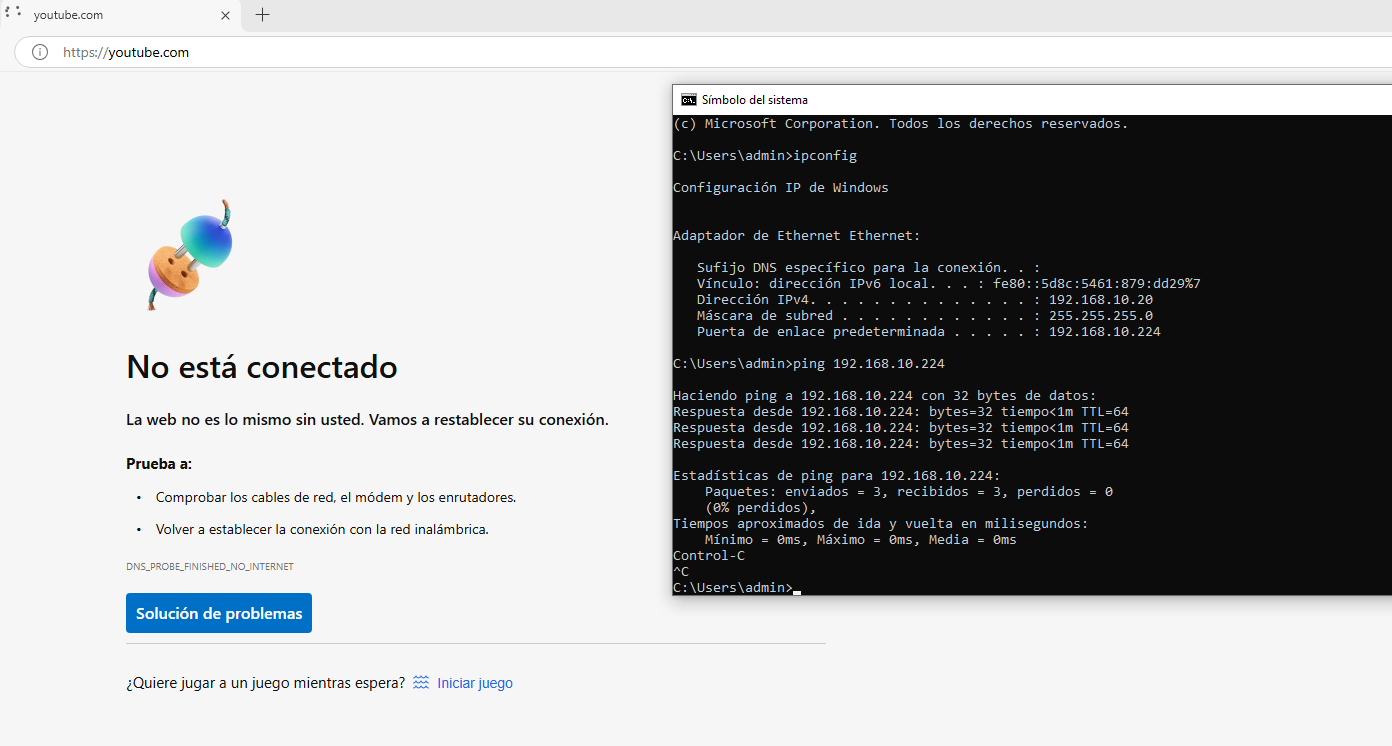


Y aplicamos el cambio.

Sysctl -p



Si probamos por como lo tenemos ahora no podremos conectarnos, pero si podremos hacer ping entre las dos máquinas.



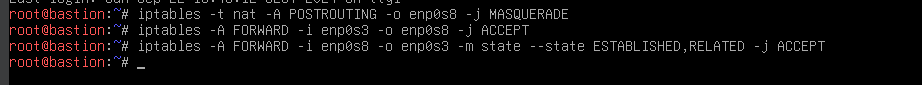
# IPTABLES

Ahora configuraremos las iptables.

Iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE

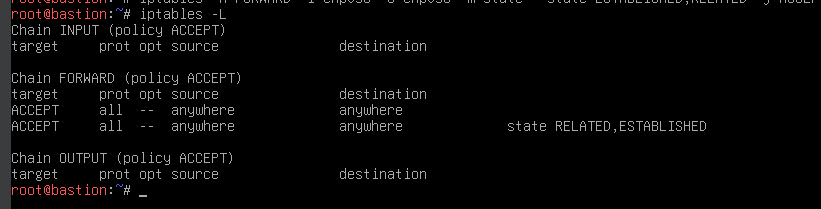
Iptables -A FORWARD -i enp0s3 -o enp0s8 -j ACCEPT

Iptables -A FORWARD -i enp0s8 -o enp0s3 -m state –state ESTABLISHED,RELATED -j ACCEPT

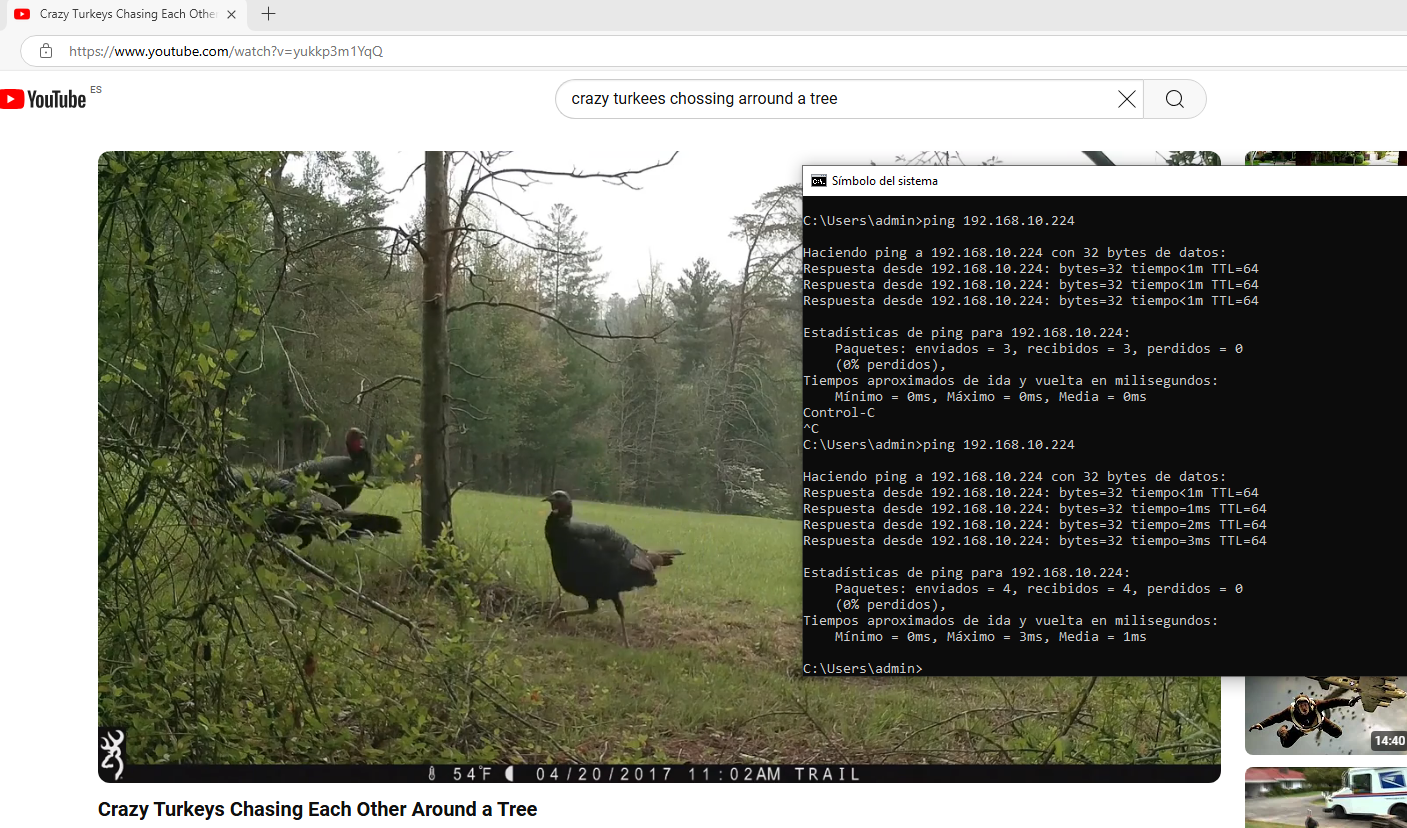


Ahora veremos si se ha configurado las iptables correctamente.

Iptables -L



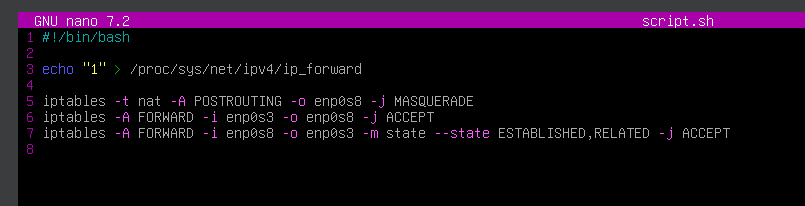
Una vez puesta las reglas podremos cargar la página web de YouTube sin problema alguno.



# Script

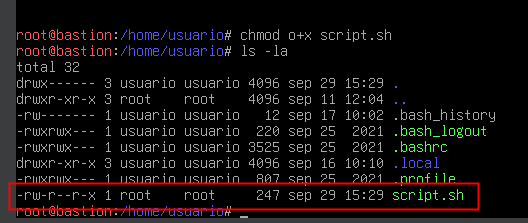
Ahora lo que haremos será poner las reglas de iptables en un script para que cuando arranquemos la maquina solo tengamos que ejecutar una instrucción.

Nano script.sh

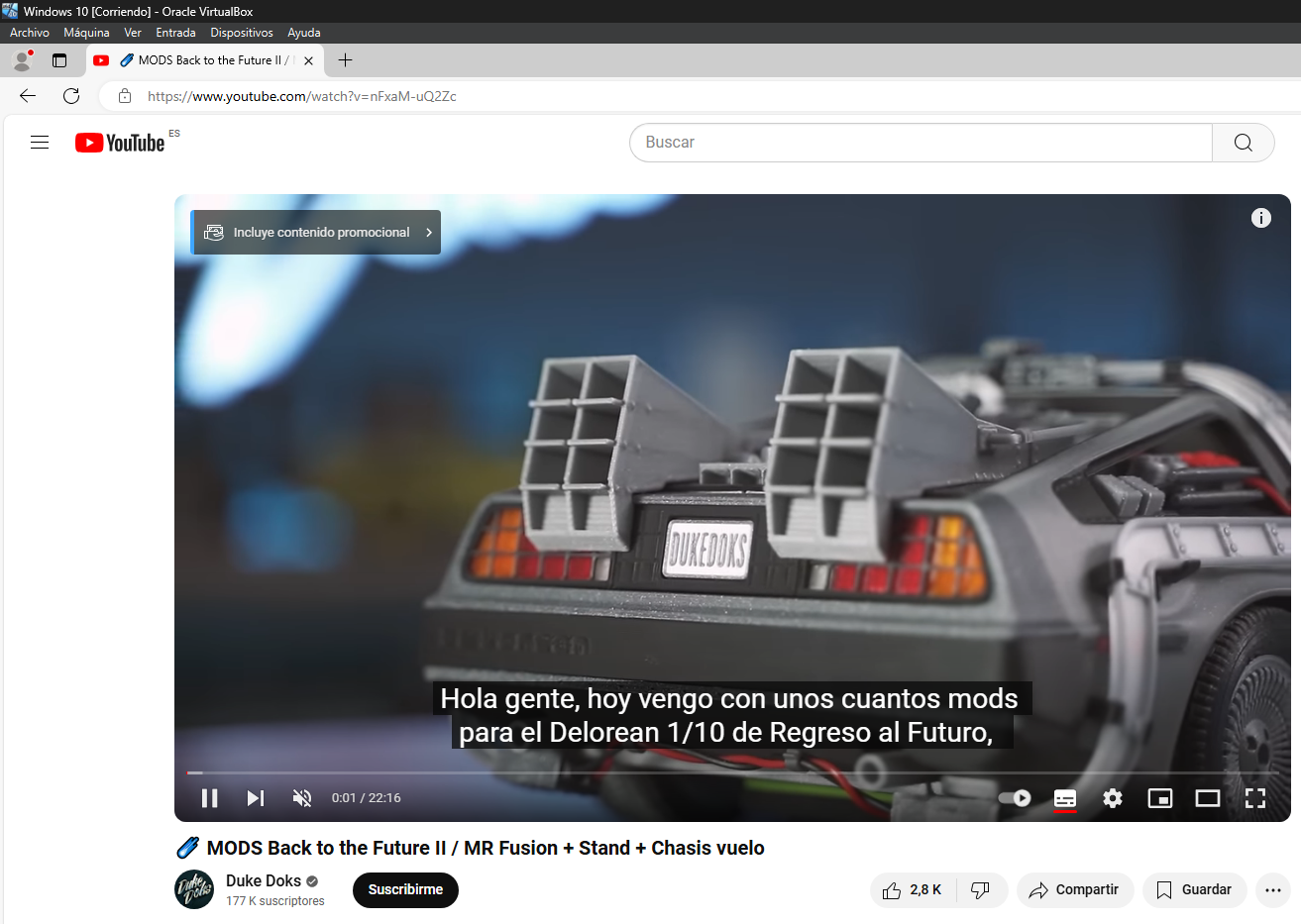


Ahora lo que haremos será dar permisos de ejecución al grupo otros, ya que ese grupo pertenece en una parte al sistema, ya que vamos a tocar parámetros del sistema.

Chmod o+x script.sh

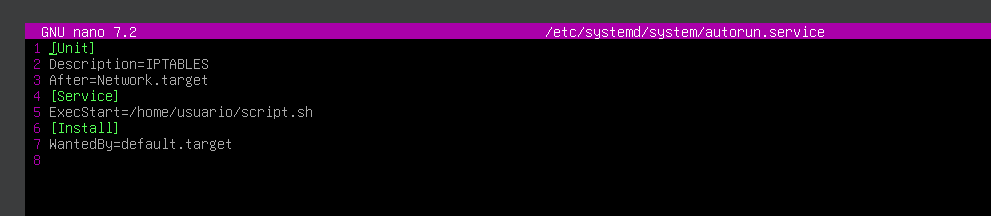


Y ahora ejecutaremos el script y probaremos si las reglas de iptables se configuran correctamente.



Ahora haremos que se inicie el script nada más arranque la máquina.

Nano /etc/systemd/system/autorun.service

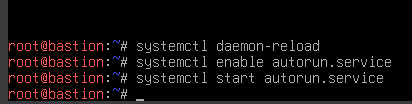


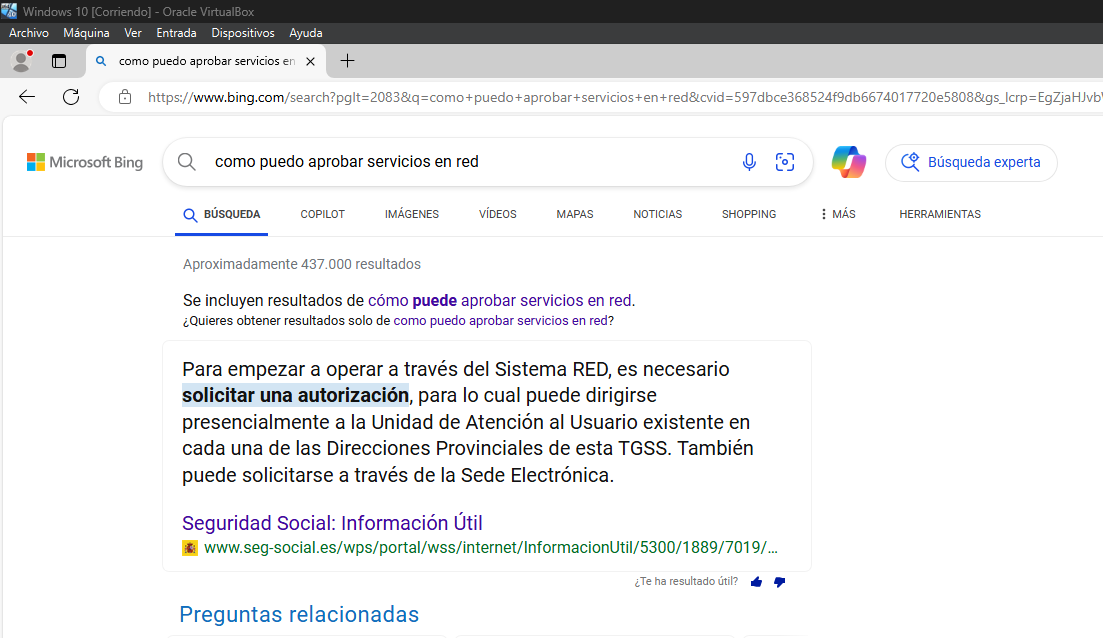
Escribiremos lo siguientes comandos para indicar que tiene que arrancar el archivo.

Systemctl Daemon-reload

Systemctl enable autorun.service

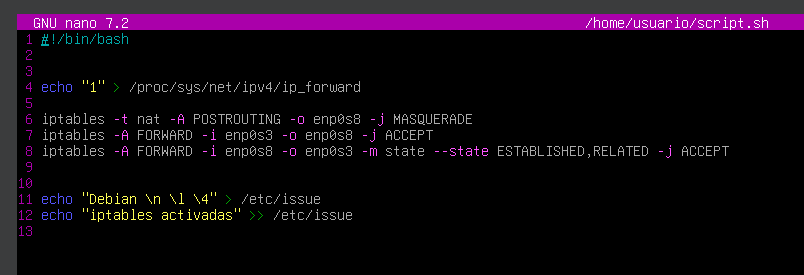
Systemctl start autorun.service



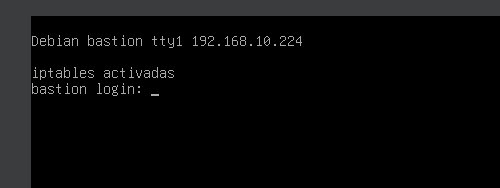
Reiniciamos la maquina y sin iniciar sesión vamos a comprobar si funciona.

Como cosa extra hemos puesto los siguientes comandos, para que cuando inicie la maquina modifique el archivo /etc/issue, que es el encargado de que podamos ver el nombre de la máquina, el tty…, modificar y también poner el “iptables activadas”, si hacíamos solo el ultimo comando al final de varios días de apagar y encender la maquina nos saldrían muchos más y al final no sabríamos si esta activado o no.

Nano /home/usuario/script.sh



Reiniciamos la maquina para ver si se ha configurado correctamente el archivo /etc/issue.



# Conclusión

Para esta práctica hemos aprendido como hacer un enrutamiento entre 2 interfaces, esto viene bien para cuando tenemos otras reglas de iptables y hacer una “DMZ” salvando las distancias y poder separar los equipos más vulnerables y no tener hackeos