

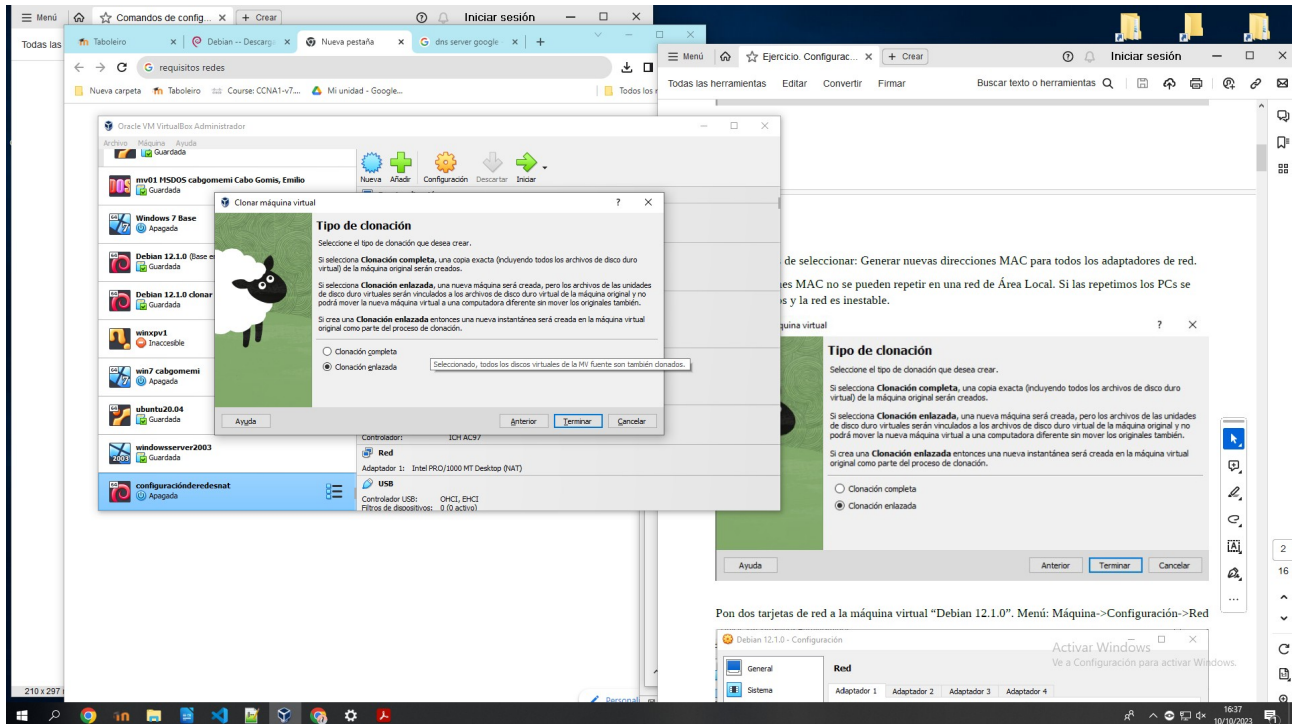
Ejercicio Guiado

Configuración de dispositivos Linux

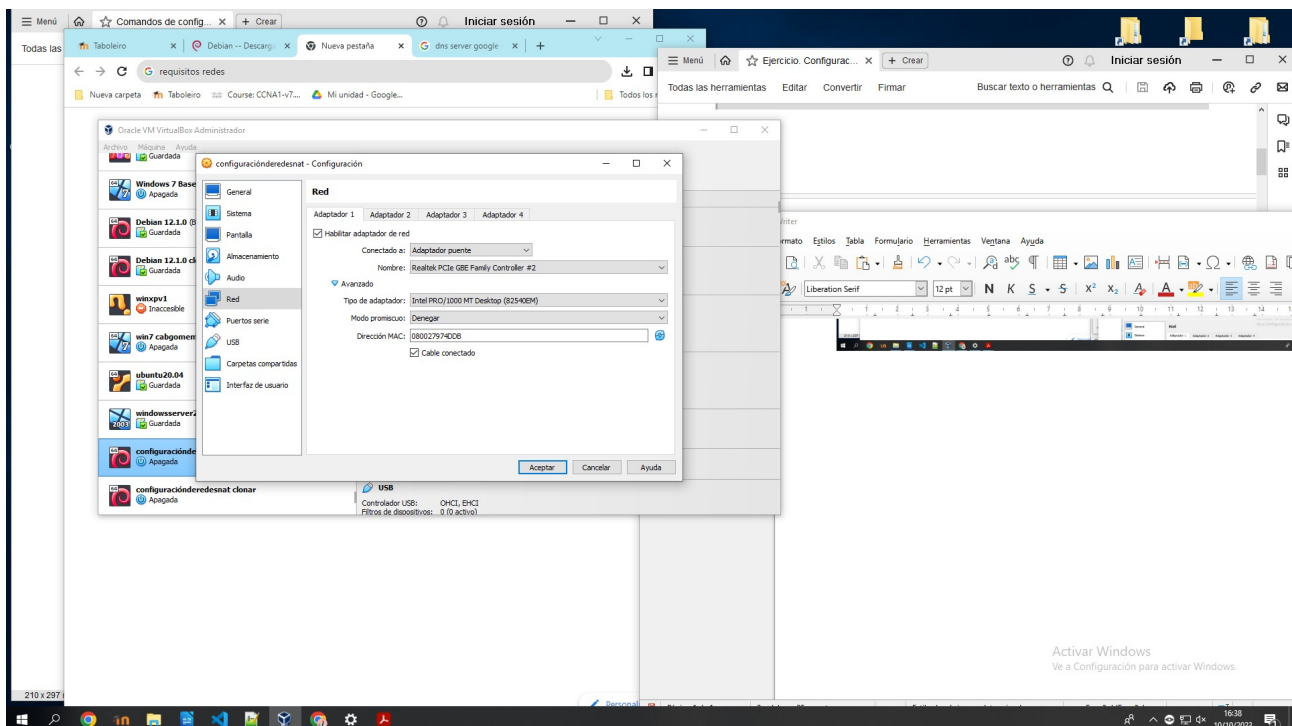
Índice alfabético

Clonación Máquina virtual.....	2
Comprobado la conectividad de “Debian base”	6
Comprobamos mediante la cmd de windows que podemos conectarnos mediante ssh a la máquina “Debian clonar”.....	12
Comprobamos que podemos acceder mediante la herramienta gráfica WinSCP.....	12
Comprobamos que podemos iniciar sesión mediante ssh en “Debian clonar”.....	10
Comprobamos que sshd.service está activo y escuchando en el puerto 22.....	9
Configuración adaptador de red máquina “Debian clonar”.....	3
Configuración de adaptador de red puente Máquina “Debian base”.....	2
Configuración de máquina “Debian” sin ayuda del NetworkManager.....	4
Configuración de red “Debian clonar.”.....	4
Configuración de red manual en la máquina “Debian”	5
Configuración de servidores dns en “Debian base”	6
Configuramos el prerouting en la máquina “Debian”.....	11
Editamos el archivo de configuración /etc/ssh/sshd_config.....	9
Instalamos SSH en la máquina “Debian Clonar”	8
Redireccionamiento de puertos en postrouting:.....	7

Clonación Máquina virtual



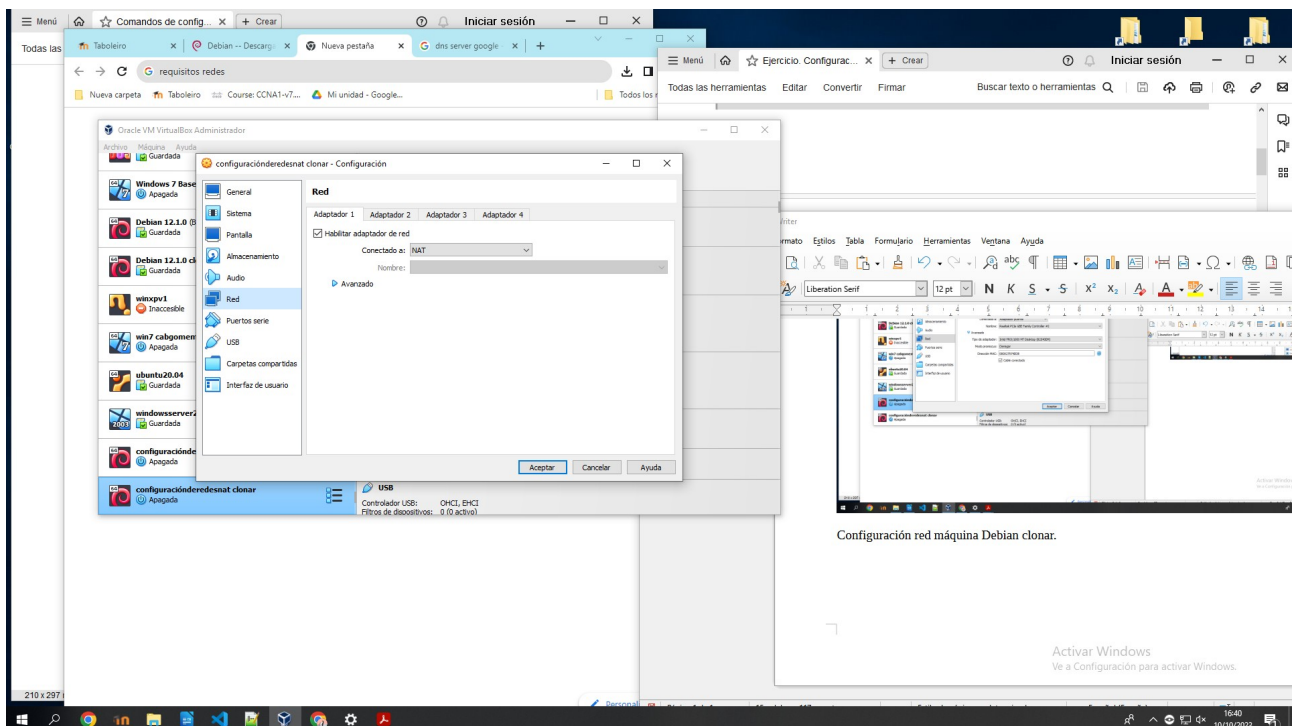
Configuración de adaptador de red puente Máquina “Debian base”



Debemos configurar el adaptador de red de la máquina Debian base en la configuración de red de vbox. Debemos refrescar la MAC

Configuramos el segundo adaptador de red en la máquina Debian base
Este será el adaptador de red al que se conectará el adaptador de la red Debian Clonar, Deberemos configurarlo en red interna.

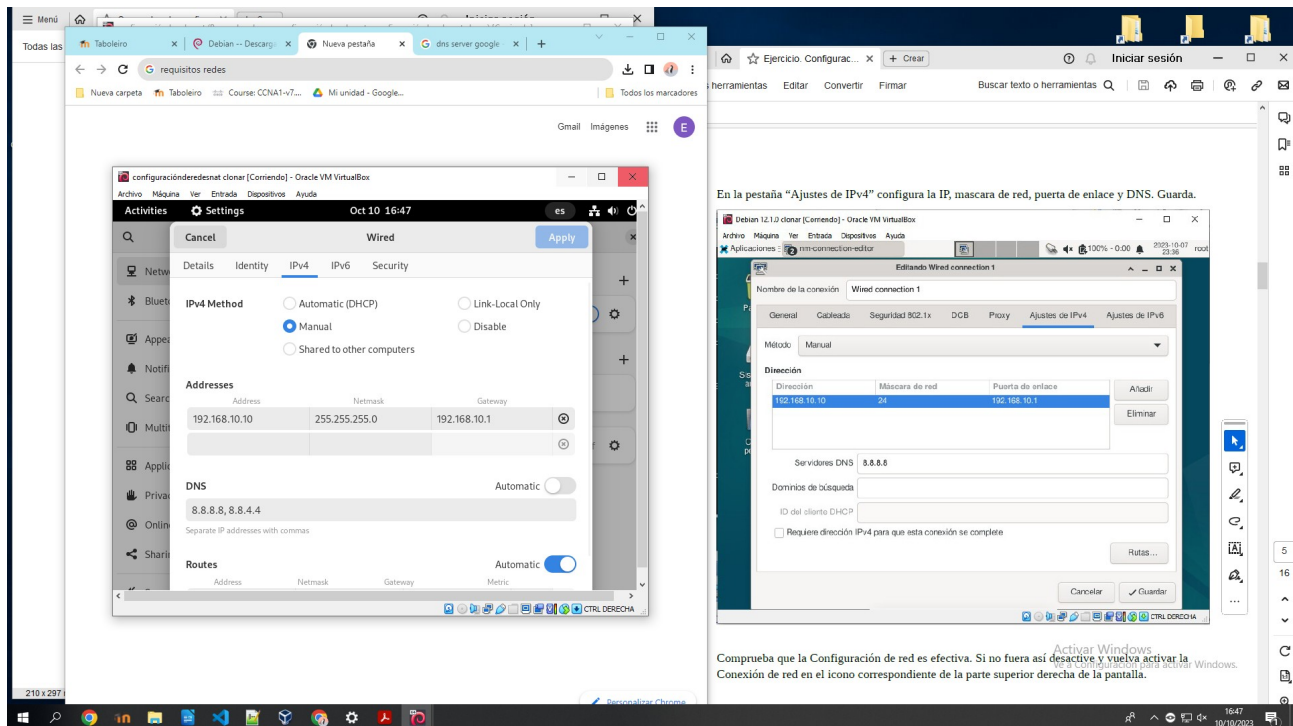
Configuración adaptador de red máquina “Debian clonar”.



Configuración red máquina Debian clonar.

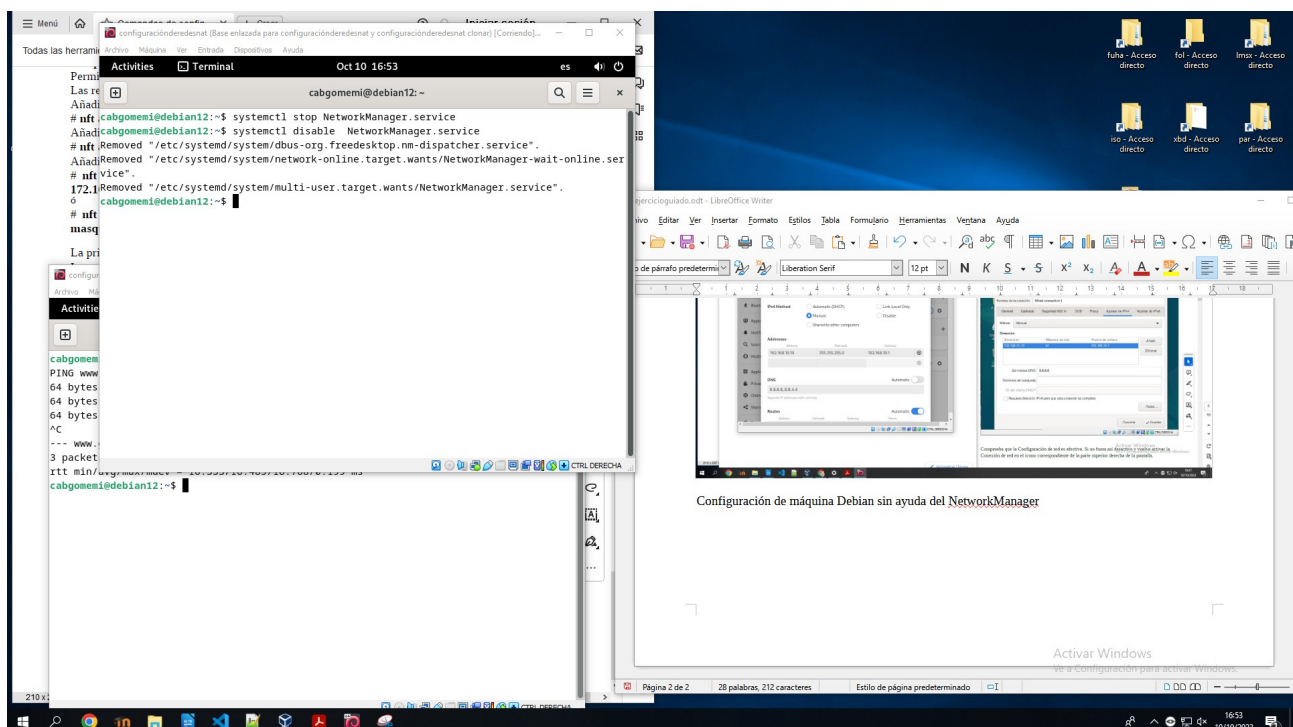
Configuramos el adaptador de red de la máquina Debian clonar en los ajustes de red de vbox para trabajar en nat.

Configuración de red “Debian clonar.”



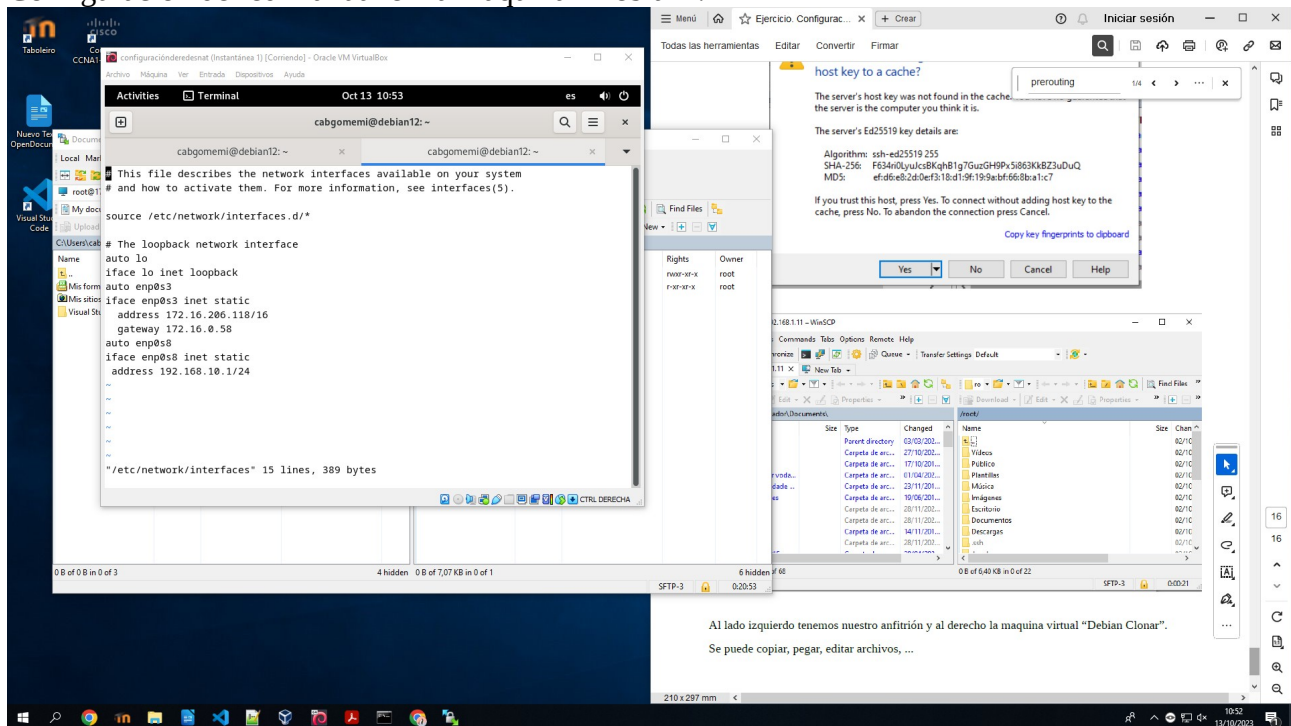
Ahora deberemos configurar aspectos como la ip, servidores dns, máscara y gateway de la red.
192.168.10.10 es la ip (No importa que entre en conflicto, dado que esta máquina está en NAT)
255.255.255.0 es la máscara
Gateway es 192.168.10.1 (Esta es la dirección ip del adaptador de red interna)

Configuración de máquina “Debian” sin ayuda del NetworkManager



Hemos desactivado el Networkmanager, ahora haremos la configuración de red de manera manual.

Configuración de red manual en la máquina “Debian”.



Editamos el archivo de configuración /etc/network/interfaces. Configurando los dos adaptadores de red.

enp0s3 es el adaptador puente.

enp0s8 es el adaptador de red interna al que se conectará el adaptador de red de la máquina “Debian Clonar”

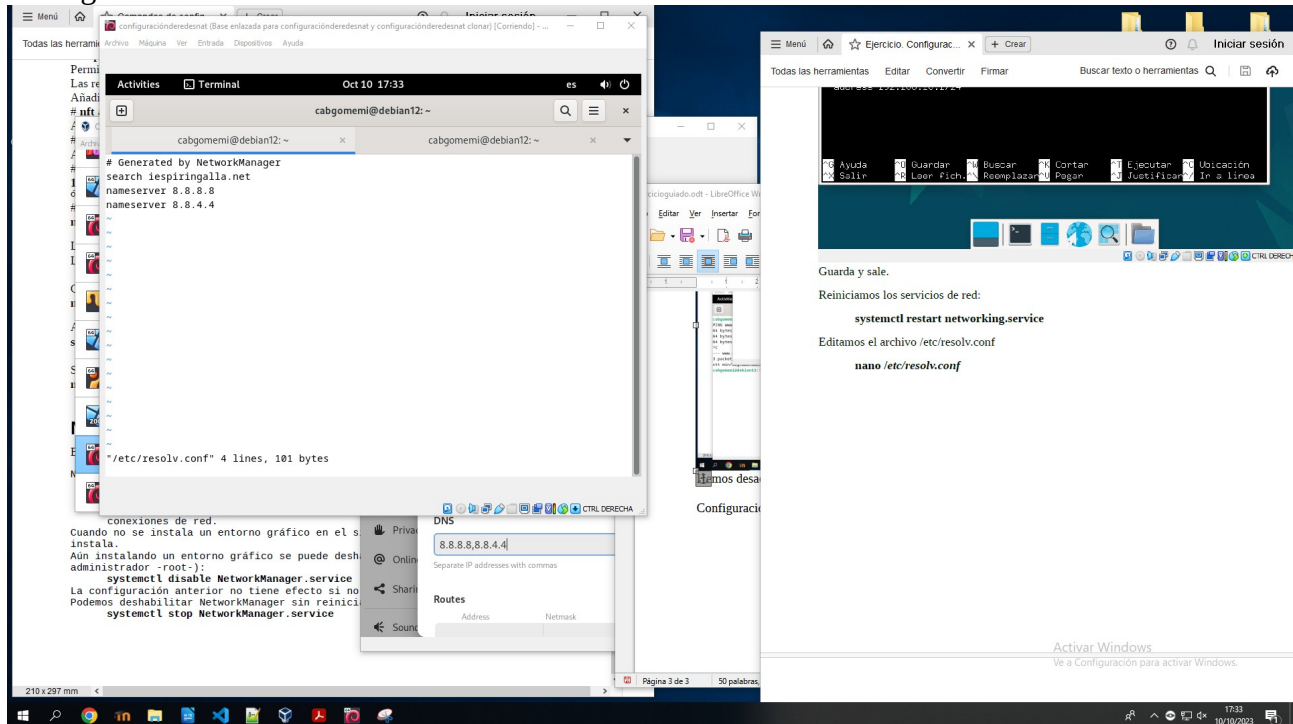
****IMPORTANTE****

Deberemos en la ip del adaptador puente poner un 100 a la dirección.

Ej 172.16.206.10 es la ip del equipo real.

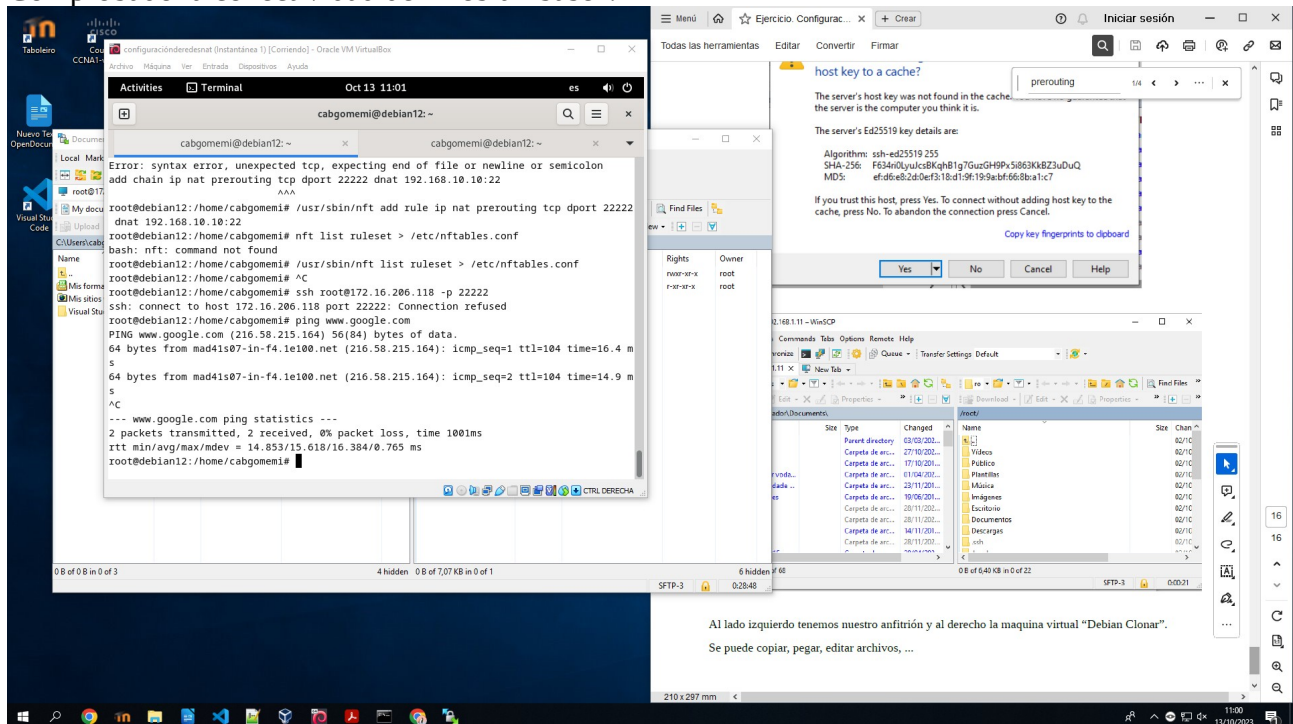
172.16.206.110 es la ip que debemos configurar en el adaptador puente.

Configuración de servidores dns en “Debian base”



Los servidores dns (8.8.8.8, 8.8.4.4) son de Google.

Comprobado la conectividad de “Debian base”.



Ping desde Debian base

Redireccionamiento de puertos en postrouting:

Debido a que los equipos dentro de la red NAT (192.168.10.0) nos son accesibles por los equipos de la red 172.16.00.00 conectada al adaptador de red (enp0s3). Debemos redireccionar los puertos para que los paquetes que lleguen por el adaptador de red (enp0s3) lleguen a la máquina “Debian clonar” sin necesariamente conocer la ip.

Para ello debemos configurar el redireccionamiento de puertos. SSH es un servicio que utiliza el puerto 22.

Para ello introducimos los siguientes comandos:

****Atención****

Es posible que la ruta al comando nft no esté establecida por defecto, para ello indicamos para ejecutar el comando la ruta directa “/etc/sbin/sft”

Activa el firewall de “Debian”:

systemctl start nftables.service

Hacer que nftables inicie al arrancar el sistema

systemctl enable nftables.service

Activar el paso de los paquetes a través del equipo (si el equipo se reinicia se pierde el cambio):

echo 1 > /proc/sys/net/ipv4/ip_forward

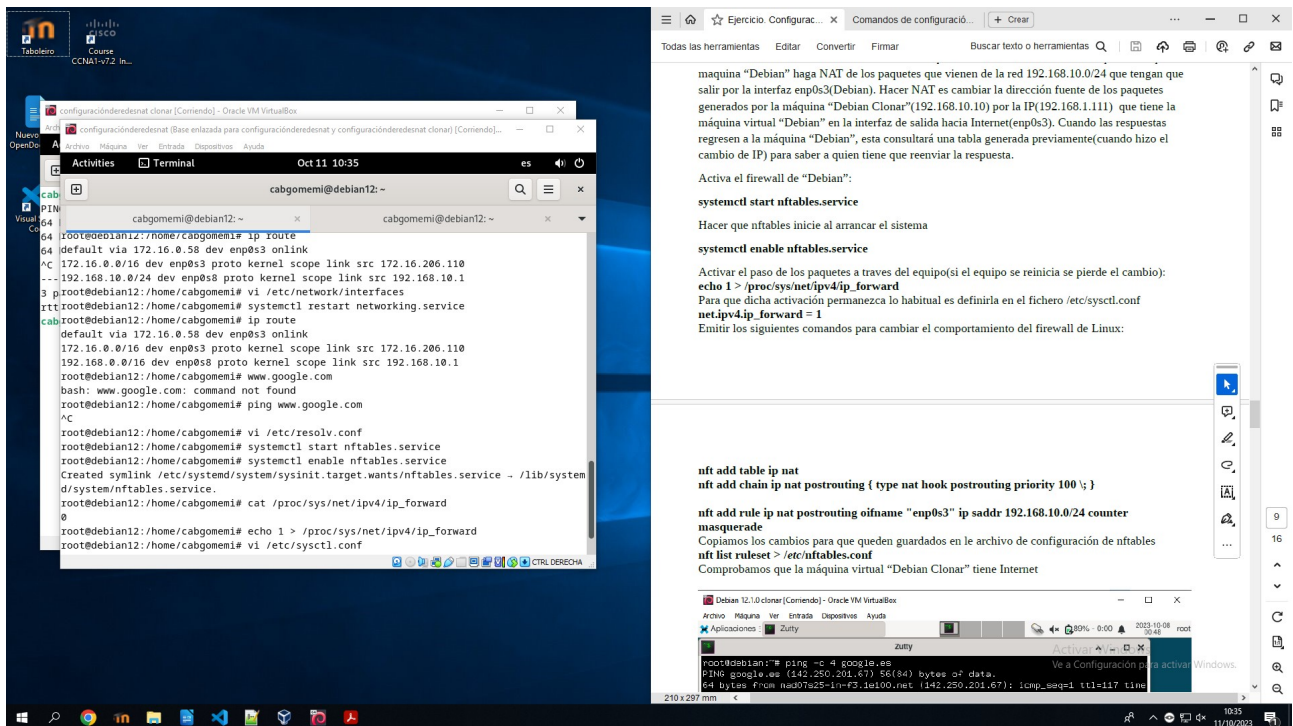
Para que dicha activación permanezca lo habitual es definirla en el fichero /etc/sysctl.conf

net.ipv4.ip_forward = 1

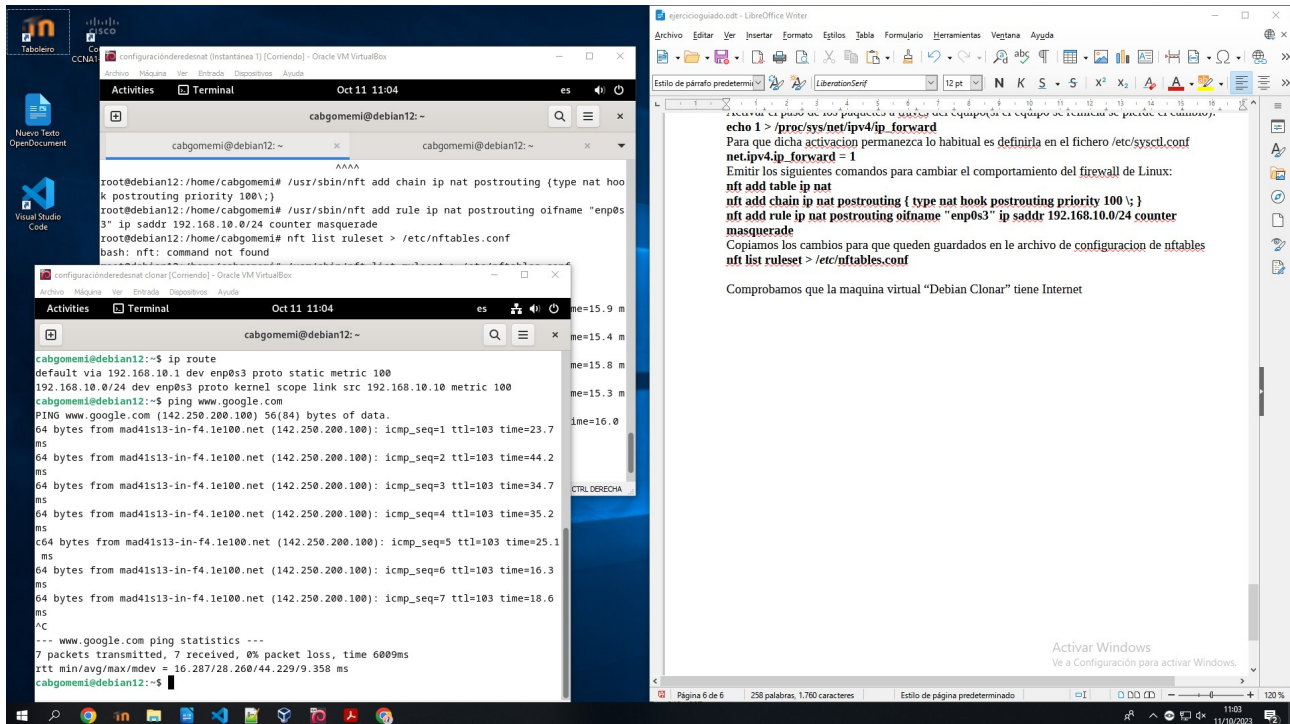
Emitir los siguientes comandos para cambiar el comportamiento del firewall de Linux:

nft add table ip nat

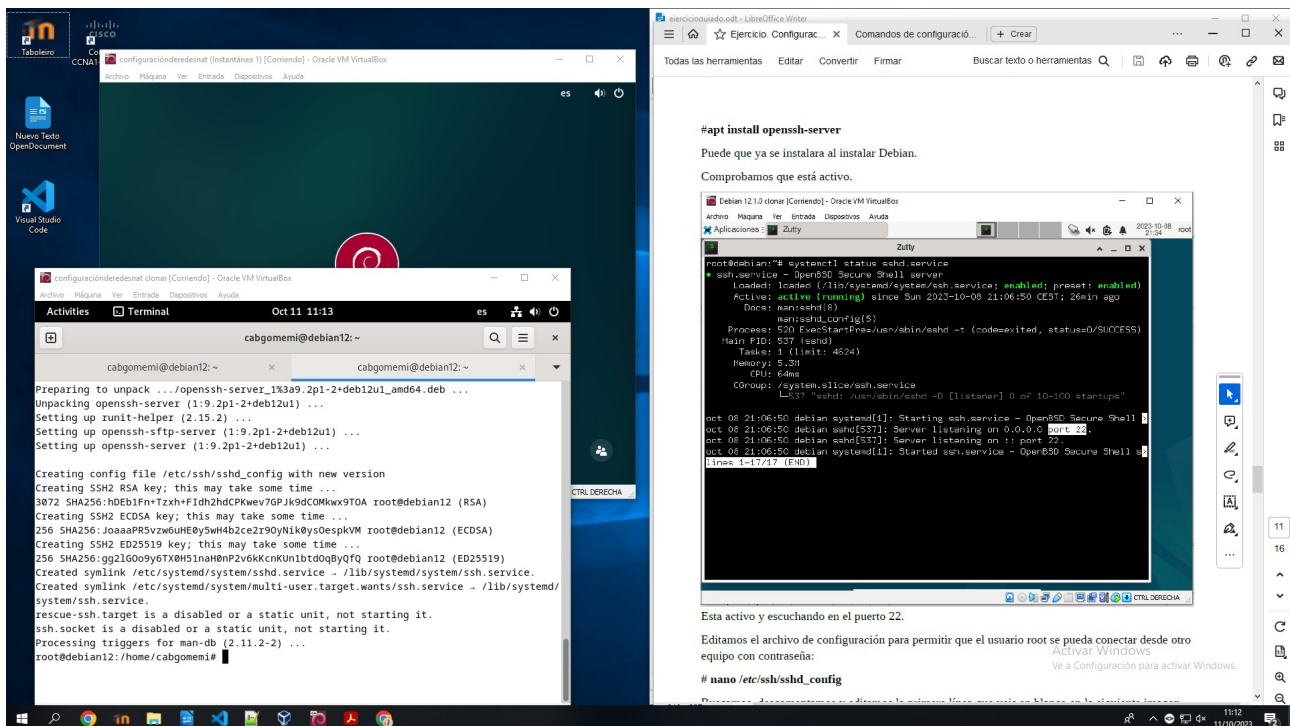
nft add chain ip nat postrouting { type nat hook postrouting priority 100 ; }



Comprobamos que la maquina virtual “Debian Clonar” tiene Internet

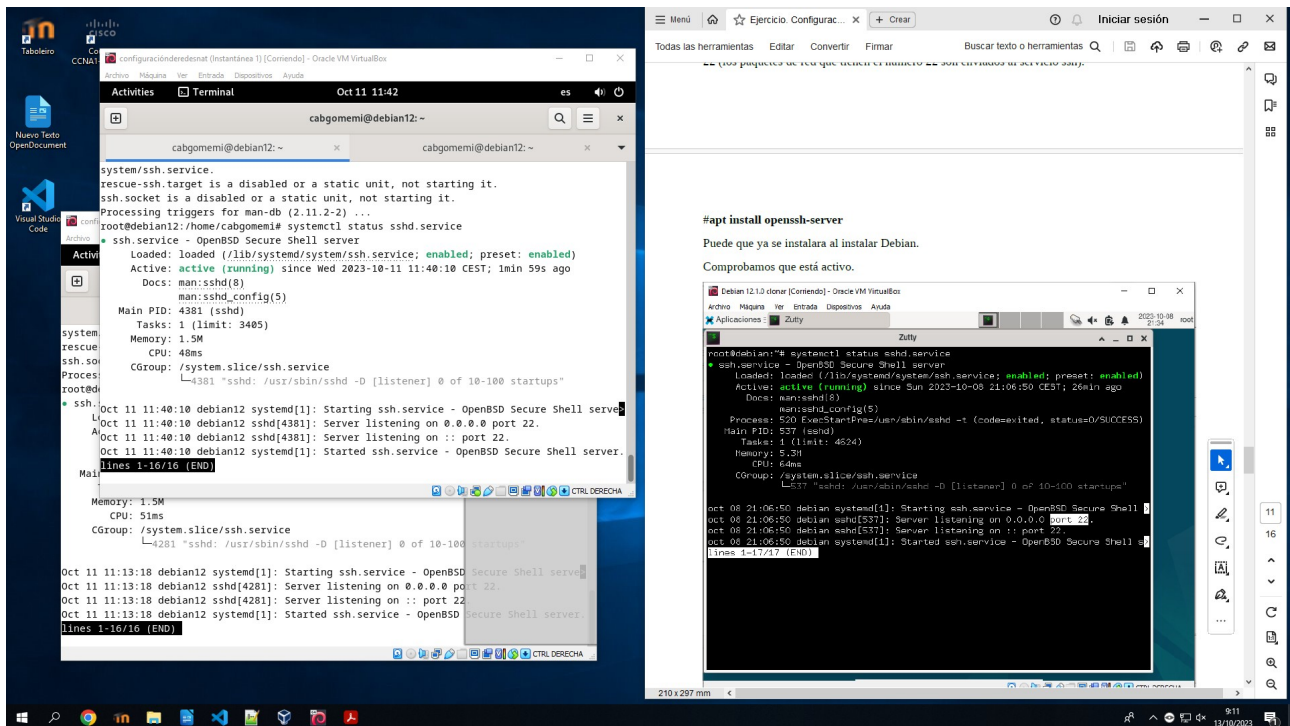


Instalamos SSH en la máquina “Debian Clonar”



#Apt-get install openssh-server

Comprobamos que sshd.service está activo y escuchando en el puerto 22

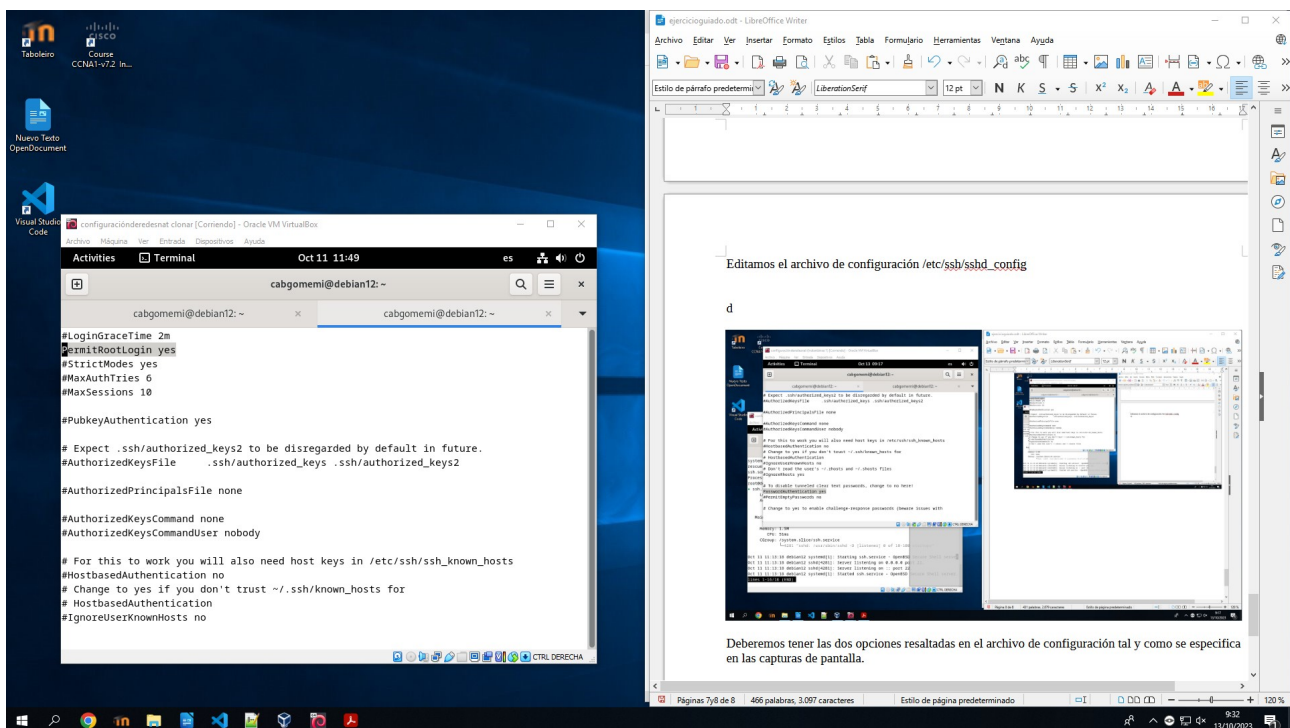


The left screenshot shows a terminal window with the command `systemctl status sshd.service` executed. The output indicates that the service is active and running, listening on port 22. The right screenshot shows a terminal window with the command `systemctl status sshd.service` executed, displaying the service's status and logs.

```
systemctl status sshd.service
ssh.service - OpenBSD Secure Shell server
Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
Active: active (running) since Wed 2023-10-11 11:40:10 CEST; 1min 59s ago
Docs: man:ssh(8)
      man:ssh_config(5)
Main PID: 4381 (sshd)
Tasks: 1 (limit: 3405)
Memory: 1.5M
CPU: 48ms
CGroup: /system.slice/ssh.service
        └─4381 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
```

```
Oct 11 11:40:10 debian12 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server.
Oct 11 11:40:10 debian12 sshd[4381]: Server listening on 0.0.0.0 port 22.
Oct 11 11:40:10 debian12 sshd[4381]: Server listening on :: port 22.
Oct 11 11:40:10 debian12 systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
lines 1-16/16 (END)
```

Editamos el archivo de configuración /etc/ssh/sshd_config



The left screenshot shows a terminal window with the command `cat /etc/ssh/sshd_config` executed, displaying the configuration file's contents. The right screenshot shows a terminal window with the command `cat /etc/ssh/sshd_config` executed, displaying the configuration file's contents.

```
#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

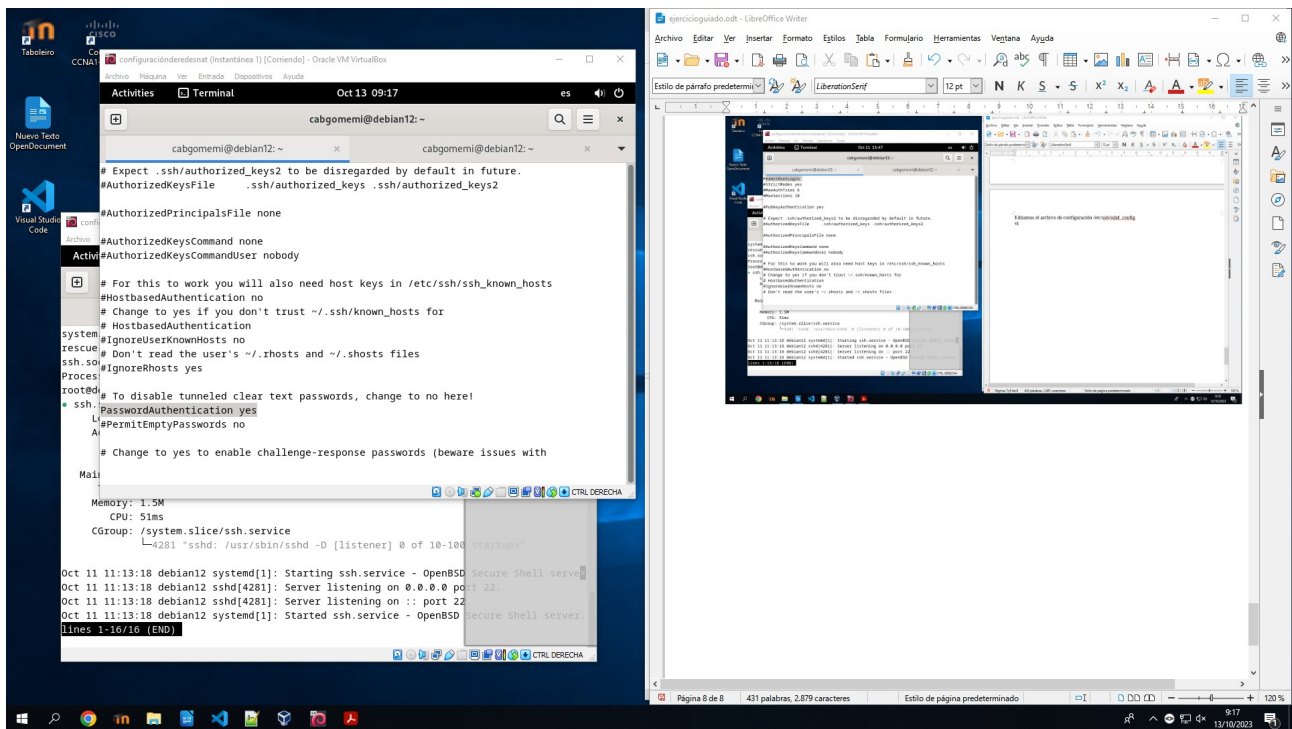
#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
#HostbasedAuthentication
#IgnoreUserKnownHosts no
```



Deberemos tener las dos opciones resaltadas en el archivo de configuración tal y como se especifica en las capturas de pantalla.

Opciones

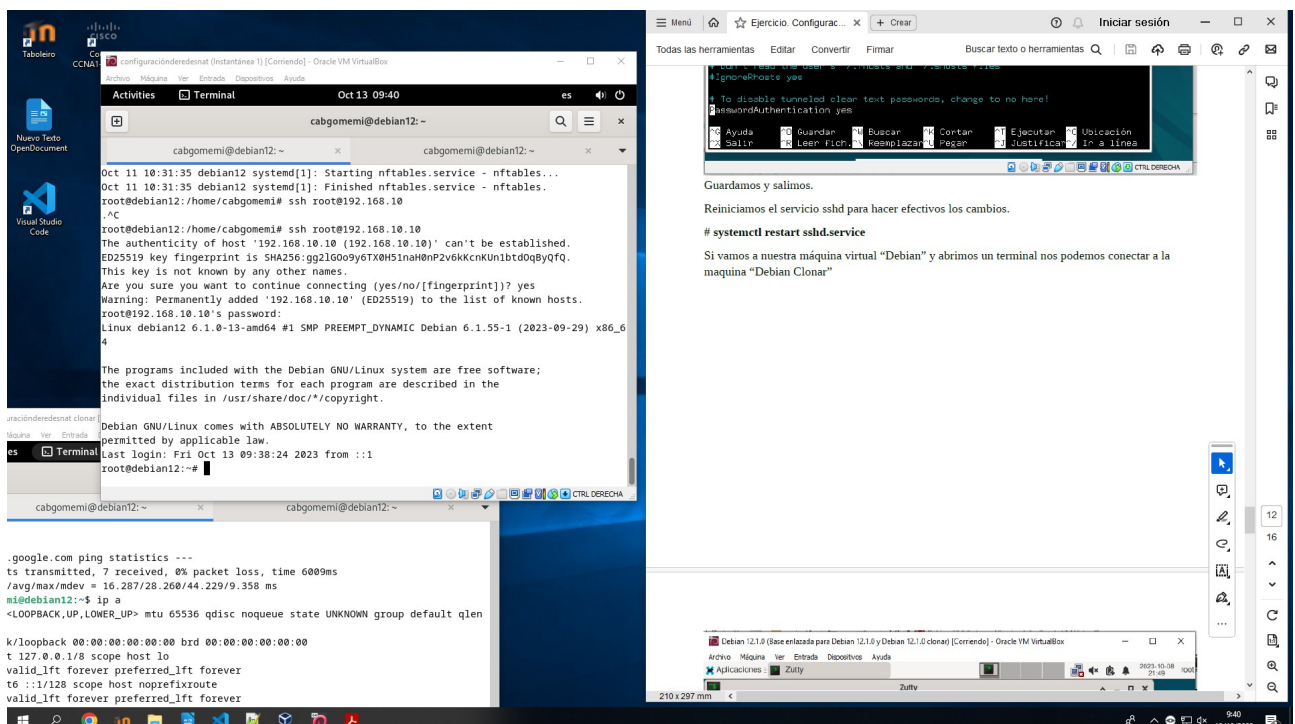
Permitrootlogin yes

PasswordAuthentication yes

Reiniciamos el servicio de sshd

#systemctl restart sshd.service

Comprobamos que podemos iniciar sesión mediante ssh en “Debian clonar”



Configuramos el *prerouting* en la máquina “Debian”.

Vamos a hacer que cuándo lleguen paquetes mediante el puerto 22222 al 172.16.206.110 , el tráfico sea redirigido al puerto 22 en la IP (192.168.10.10). Que es el puerto para el que el servicio de ssh está configurado para escuchar.

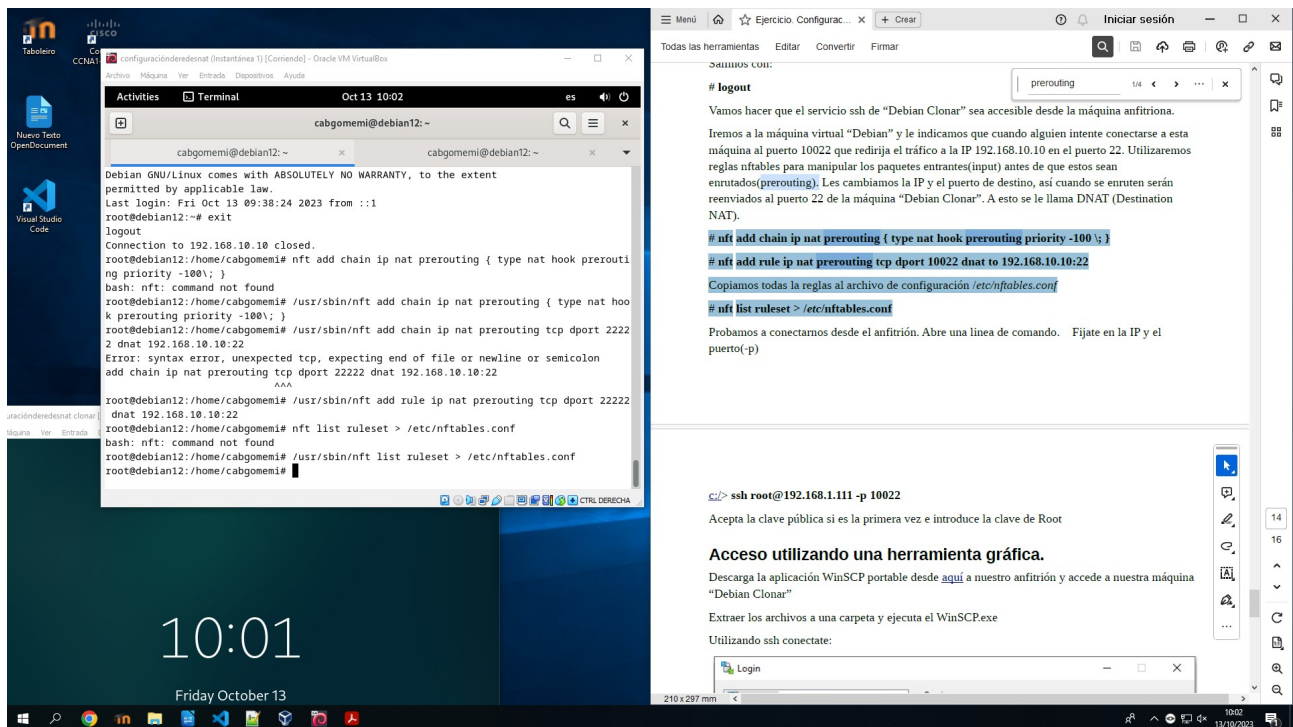
Para ello aplicamos los siguientes comandos:

```
# nft add chain ip nat prerouting { type nat hook prerouting priority -100 ; }
```

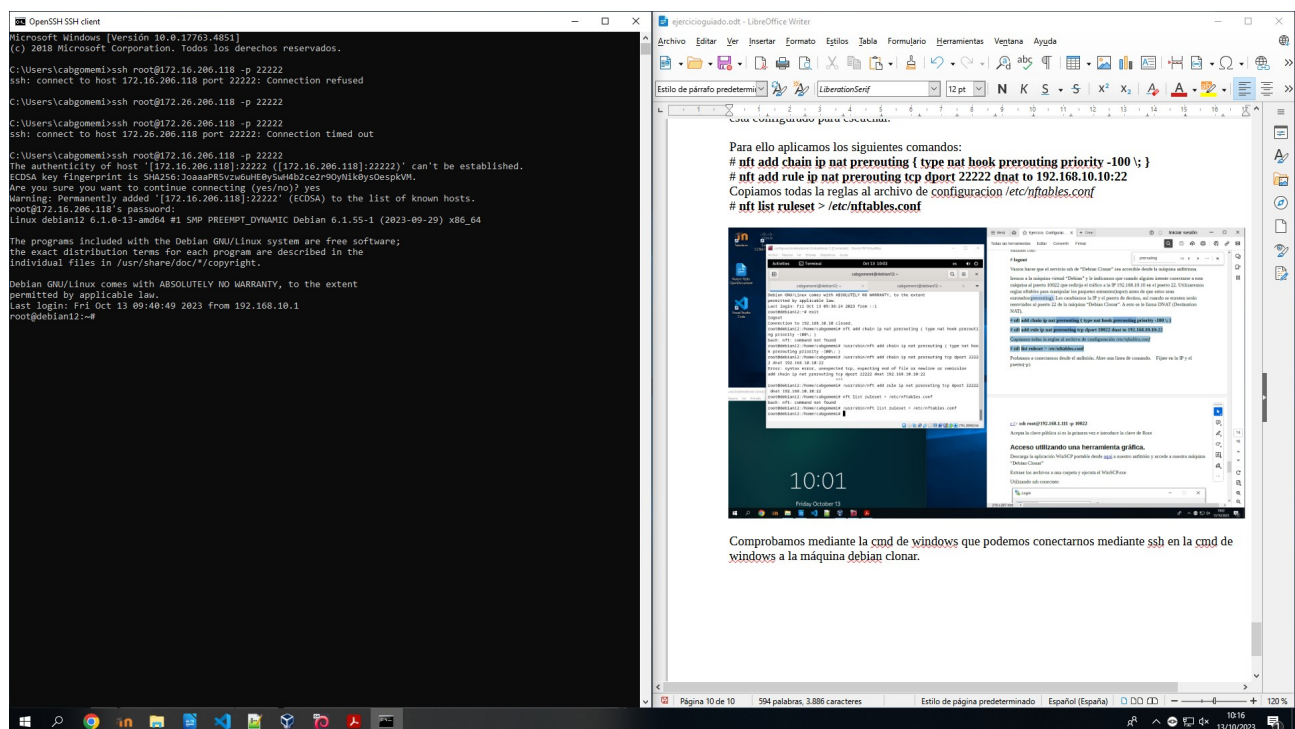
```
# nft add rule ip nat prerouting tcp dport 22222 dnat to 192.168.10.10:22
```

Copiamos todas la reglas al archivo de configuracion */etc/nftables.conf*

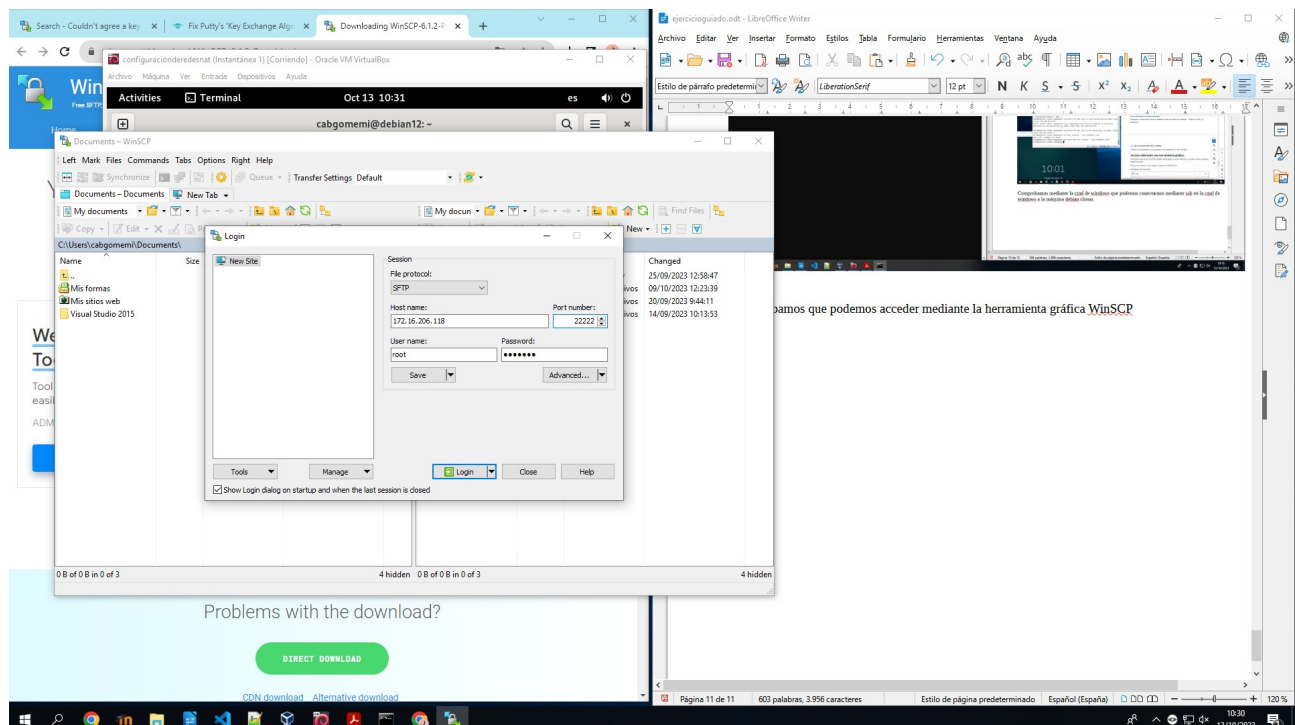
```
# nft list ruleset > /etc/nftables.conf
```



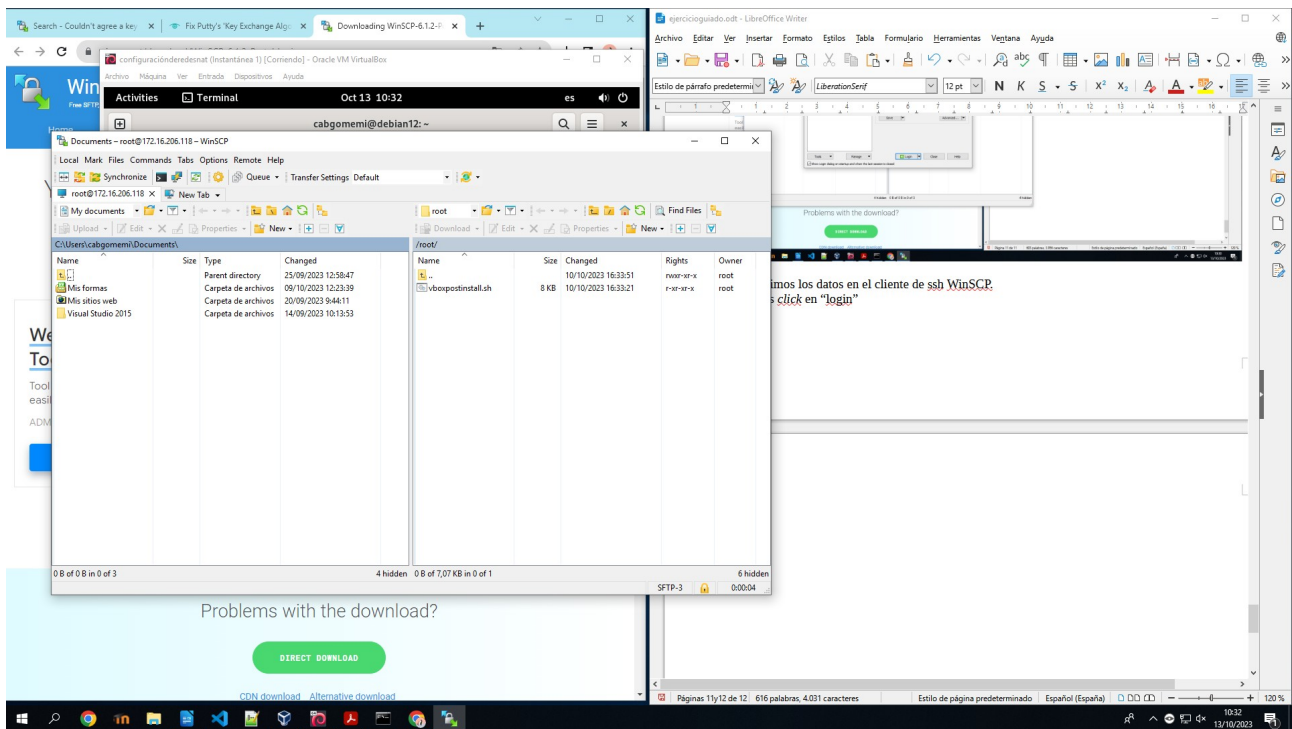
Comprobamos mediante la cmd de windows que podemos conectarnos mediante ssh a la máquina “Debian clonar”.



Comprobamos que podemos acceder mediante la herramienta gráfica WinSCP



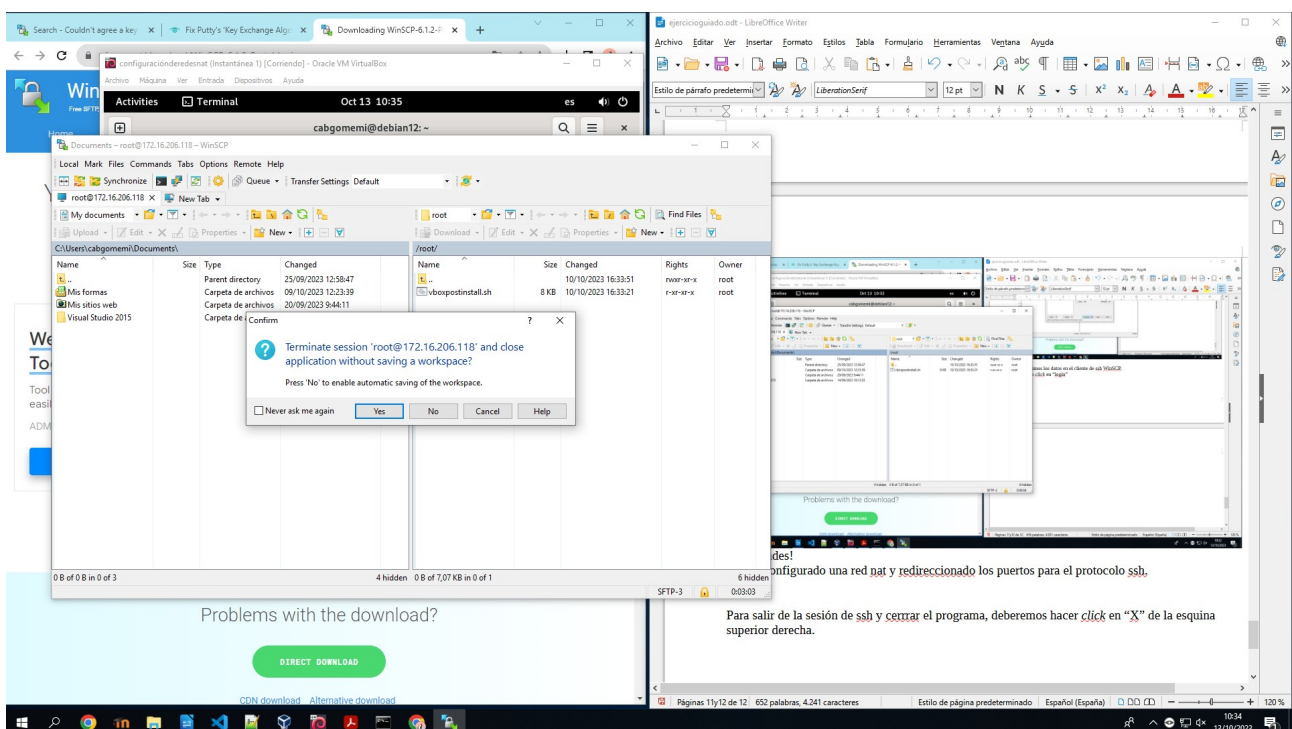
Introducimos los datos en el cliente de ssh WinSCP.
Hacemos click en “login”



¡Felicidades!

Ya has configurado una red nat y redireccionado los puertos para el protocolo ssh.

Para salir de la sesión de ssh y cerrar el programa, deberemos hacer *click* en “X” de la esquina superior derecha.



Haremos *click* en “yes”.