

NAT EN WINDOWS Y LINUX.

Paulino Esteban Bermúdez Rodríguez.
IES ALONSO DE AVELLANEDA. 2017-2018.

Tabla de contenido

Activa el NAT en la máquina A.	3
Listar reglas	3
Borrar todas las reglas de una cadena.	3
Conectar a B por medio de escritorio remoto, desde tu PC físico	5

ENTORNO.

A: Máquina virtual Linux (recomendado Debian)

- No necesita mucha memoria (256 MBytes)
- Tendrá una tarjeta de red bridged con la dirección 192.168.255.N/24 (siendo N tu número de ordenador)
- Tendrá una tarjeta de red bridged con una IP en la red del aula, para la comunicación con Internet.
- Tendrá una tarjeta de red interna, con una dirección privada clase B.

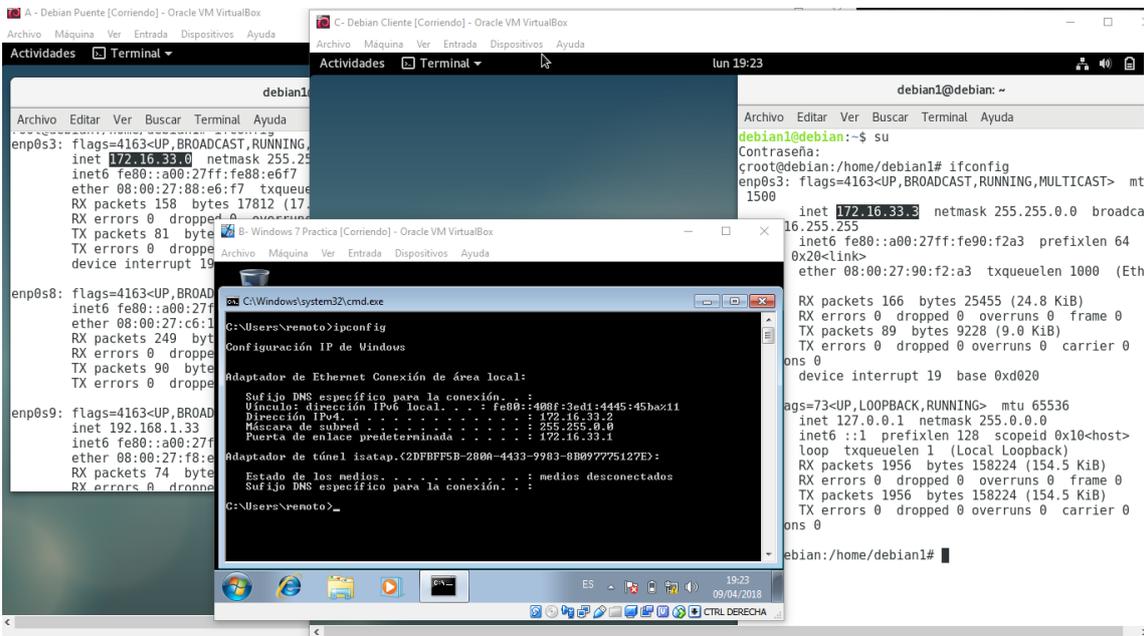
B: Máquina virtual Windows, versión profesional, ultimate o equivalente.

- No necesita mucha memoria (256 MBytes)
- Tendrá una tarjeta de red interna, con una dirección privada clase B

C: Máquina virtual Linux

- No necesita mucha memoria (256 MBytes)
- Tendrá una tarjeta de red interna, con una dirección privada clase B

La máquina A, B y C deben poder conectarse a nivel IP por sus tarjetas interna. A es el router por defecto de B y C.



Activa el NAT en la máquina A.

Iptables permite filtración de paquetes, traducción de direcciones de red y modificación del encabezado de los paquetes.

- Instalación de iptables

Instalamos el paquete iptables:

```
# aptitude install iptables
```

Listar reglas

Utilizamos el parámetro -L (normalmente se acompaña de -n para que los resultados se muestren de forma numérica y evitar consultas DNS)

```
# iptables -t nat -L -n
```

Borrar todas las reglas de una cadena.

Antes de empezar a utilizar iptables, una norma elemental es escribir:

```
# iptables -t nat -F
```

```
# iptables -t nat -Z
```

Todos estos pasos para no estar realizando la configuración continua, hacemos la creación de un Script que guarde estas órdenes y configure el sistema, de antemano se configurará el acceso al escritorio remoto.

El ejecutable es el siguiente (Ilustración 1).

```
GNU nano 2.7.4          Fichero: route.sh          Modificado
echo 0 > /proc/sys/net/ipv4/ip_forward
iptables -t nat -F
iptables -t nat -Z
echo 1 > /proc/sys/net/ipv4/ip_forward
iptables -A FORWARD -j ACCEPT
iptables -t nat -A POSTROUTING -o enp0s8 -j MASQUERADE
iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
iptables -t nat -A PREROUTING -p udp --dport 400 -j DNAT --to 192.168.33.2
iptables -t nat -A PREROUTING -p tcp --dport 400 -j DNAT --to 192.168.33.2
iptables -t nat -A PREROUTING -p udp --match multiport --dport 135:139 -i enp0s$
iptables -t nat -A PREROUTING -p tcp --match multiport --dport 135:139 -i enp0s$
iptables -t nat -A PREROUTING -p tcp --dport 3389 -j DNAT --to 172.16.33.2:3389
iptables -t nat -A PREROUTING -p tcp --dport 2222 -j DNAT --to 172.16.33.3:22
echo Terminado.
```

Ilustración 1 Script con iptables.

Con esta configuración, configuramos las iptables.

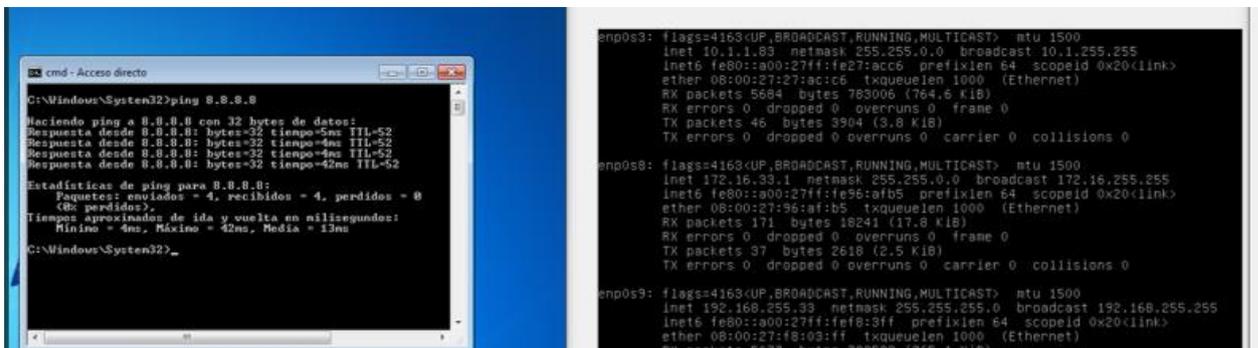
```
root@debian:/home/debian1# bash route.sh
Terminado.
root@debian:/home/debian1#
```

Ilustración 2 Ejecución del Script.

Comprobamos que hay comunicación entre las máquinas clientes, y, además, con el ordenador real.

```
root@debian:/home/debian1# bash route.sh
Terminado.
root@debian:/home/debian1# ping 172.16.33.2
PING 172.16.33.2 (172.16.33.2) 56(84) bytes of data.
64 bytes from 172.16.33.2: icmp_seq=1 ttl=128 time=0.943 ms
64 bytes from 172.16.33.2: icmp_seq=2 ttl=128 time=0.347 ms
64 bytes from 172.16.33.2: icmp_seq=3 ttl=128 time=0.317 ms
^C
--- 172.16.33.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2025ms
rtt min/avg/max/mdev = 0.317/0.535/0.943/0.289 ms
root@debian:/home/debian1# ping 172.16.33.3
PING 172.16.33.3 (172.16.33.3) 56(84) bytes of data.
64 bytes from 172.16.33.3: icmp_seq=1 ttl=64 time=0.446 ms
64 bytes from 172.16.33.3: icmp_seq=2 ttl=64 time=0.243 ms
64 bytes from 172.16.33.3: icmp_seq=3 ttl=64 time=0.294 ms
^C
--- 172.16.33.3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2055ms
rtt min/avg/max/mdev = 0.243/0.327/0.446/0.088 ms
root@debian:/home/debian1# ping 192.168.1.137
PING 192.168.1.137 (192.168.1.137) 56(84) bytes of data.
64 bytes from 192.168.1.137: icmp_seq=1 ttl=128 time=0.612 ms
64 bytes from 192.168.1.137: icmp_seq=2 ttl=128 time=0.332 ms
^C
--- 192.168.1.137 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1016ms
rtt min/avg/max/mdev = 0.332/0.472/0.612/0.140 ms
root@debian:/home/debian1# █
```

Ilustración 3 Comunicación entre máquinas.



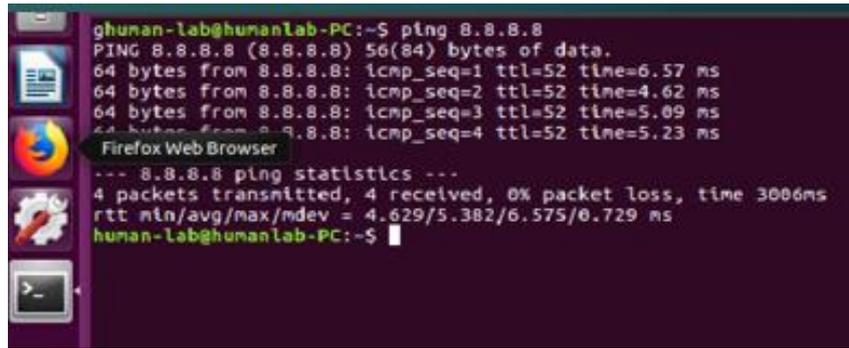


Ilustración 4 Comunicación entre máquinas.

Conectar a B por medio de escritorio remoto, desde tu PC físico

Activa el escritorio remoto en B (Propiedades del sistema → Remoto → Permitir escritorio remoto).

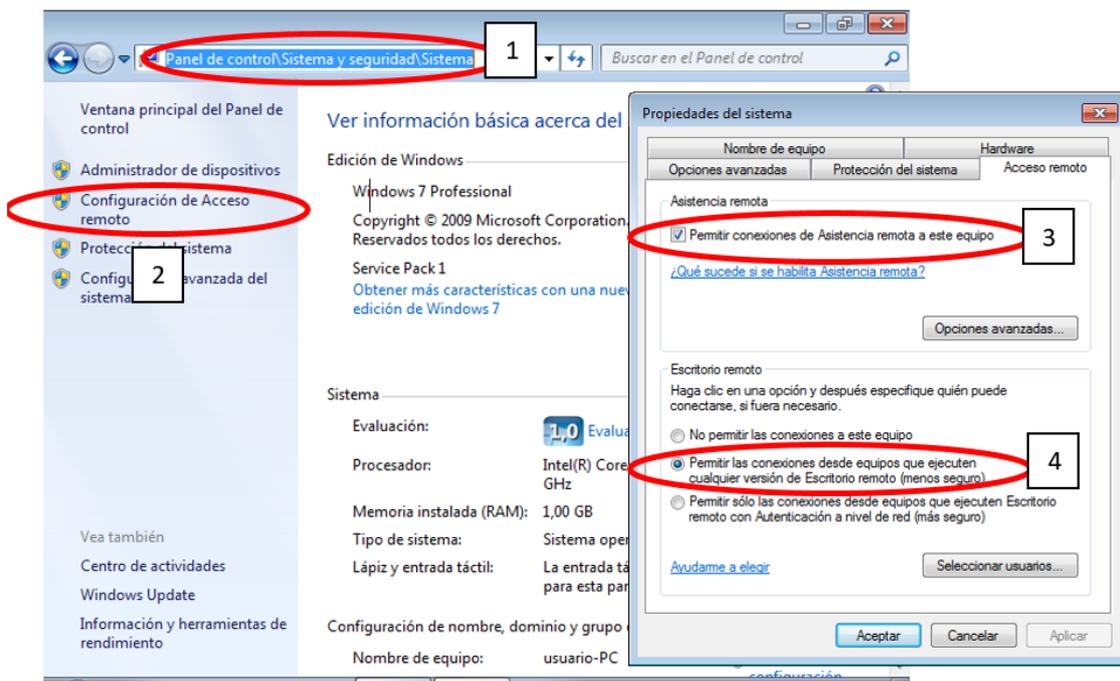


Ilustración 5 Configuración de Acceso remoto en Windows 7.

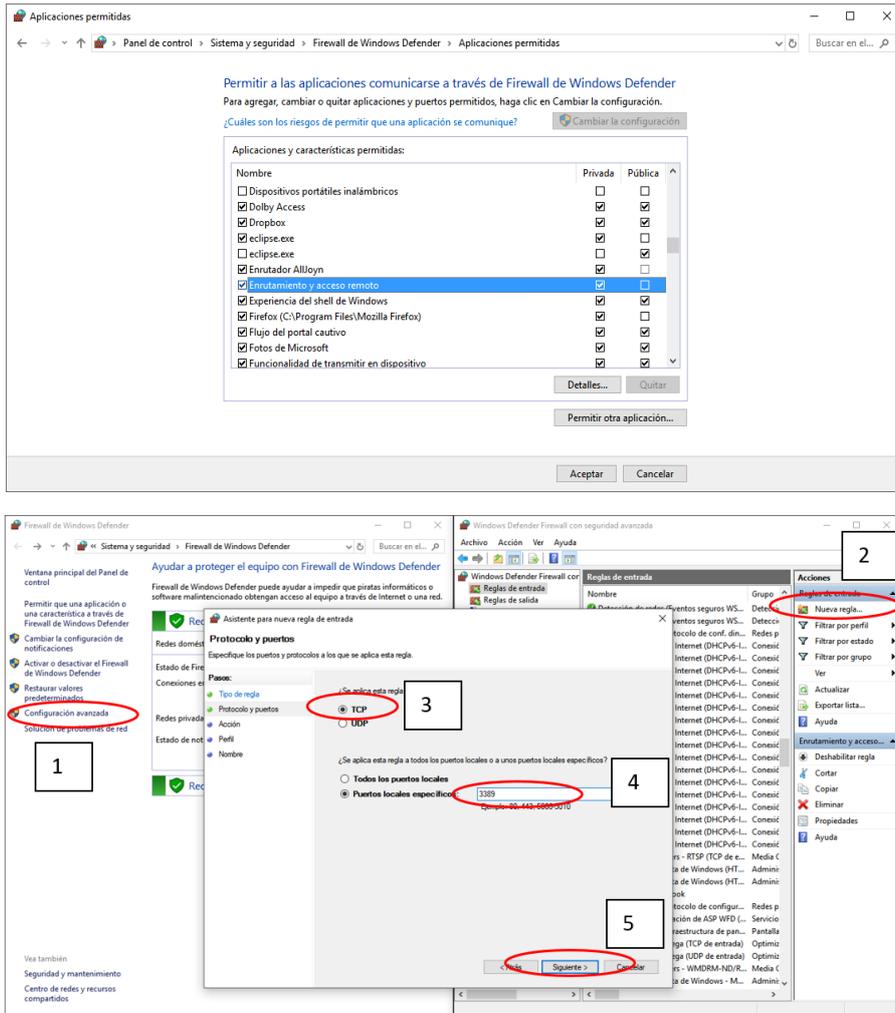


Ilustración 6 Excepción de firewall para puerto 3389

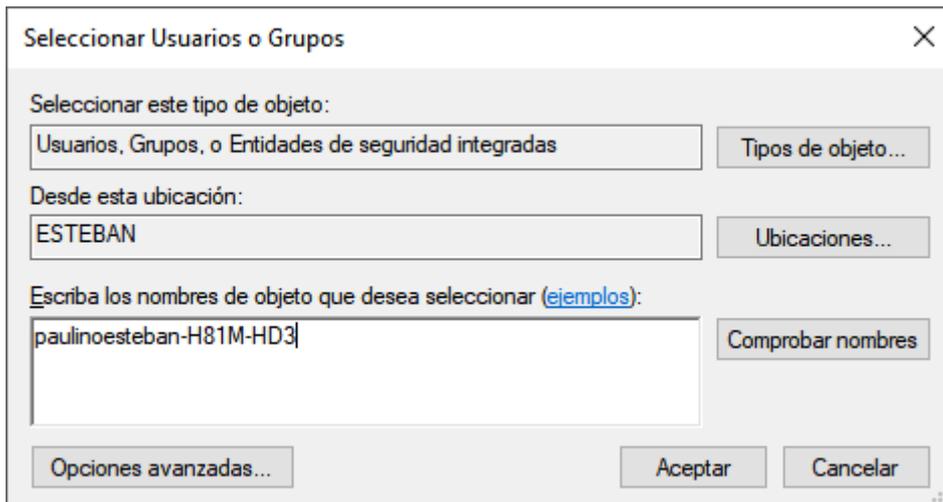


Ilustración 7 Permitir acceso al PC el usuario del PC2.

Conectar desde tu PC físico con la orden mstsc en Windows.

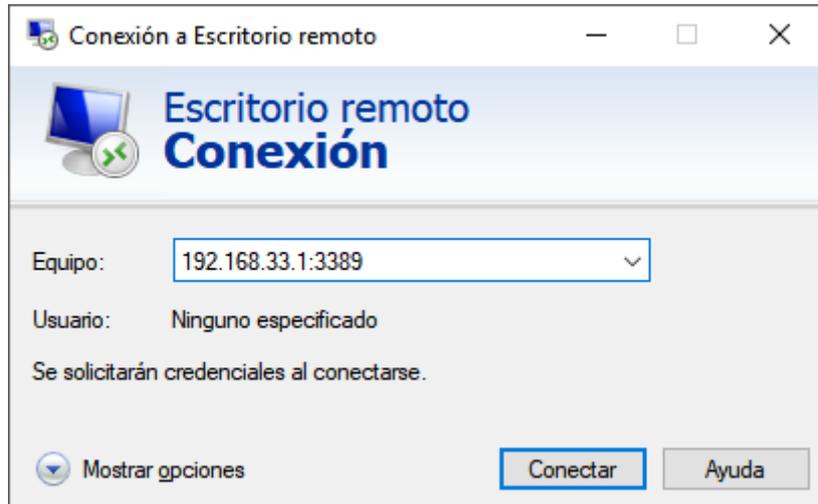


Ilustración 8 Conexión a Escritorio remoto usando la interfaz.

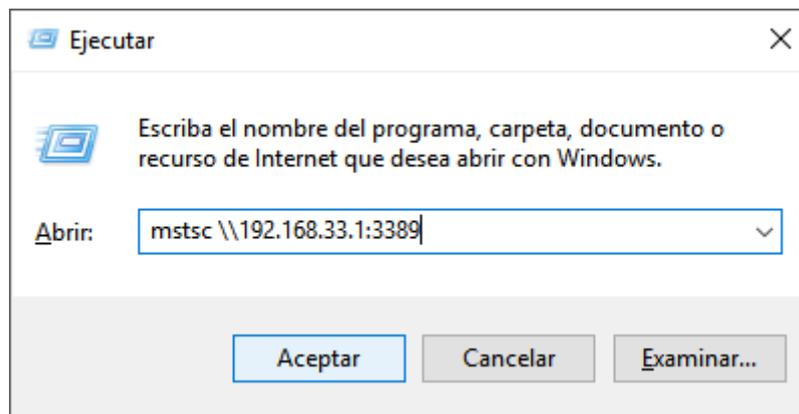


Ilustración 9 Conexión a Escritorio remoto.

Conectarse a B desde el equipo B de otro compañero.

```

echo 0 > /proc/sys/net/ipv4/ip_forward
iptables -t nat -F
iptables -t nat -Z
echo 1 > /proc/sys/net/ipv4/ip_forward
iptables -A FORWARD -j ACCEPT
iptables -t nat -A POSTROUTING -o enp0s8 -j MASQUERADE
iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
iptables -t nat -A PREROUTING -p udp --dport 400 -j DNAT --to 192.168.33.2
iptables -t nat -A PREROUTING -p tcp --dport 400 -j DNAT --to 192.168.33.2
iptables -t nat -A PREROUTING -p udp --match multiport --dport 135:139 -i enp0s8
iptables -t nat -A PREROUTING -p tcp --match multiport --dport 135:139 -i enp0s8
iptables -t nat -A PREROUTING -p udp --dport 135 -j DNAT --to 192.168.33.2
iptables -t nat -A PREROUTING -p udp --dport 136 -j DNAT --to 192.168.33.2
iptables -t nat -A PREROUTING -p udp --dport 137 -j DNAT --to 192.168.33.2
iptables -t nat -A PREROUTING -p udp --dport 138 -j DNAT --to 192.168.33.2
iptables -t nat -A PREROUTING -p udp --dport 139 -j DNAT --to 192.168.33.2
iptables -t nat -A PREROUTING -p tcp --dport 135 -j DNAT --to 192.168.33.2
iptables -t nat -A PREROUTING -p tcp --dport 136 -j DNAT --to 192.168.33.2
iptables -t nat -A PREROUTING -p tcp --dport 137 -j DNAT --to 192.168.33.2
iptables -t nat -A PREROUTING -p tcp --dport 138 -j DNAT --to 192.168.33.2
iptables -t nat -A PREROUTING -p tcp --dport 139 -j DNAT --to 192.168.33.2
iptables -t nat -A PREROUTING -p tcp --dport 3389 -j DNAT --to 172.16.33.2:3389
iptables -t nat -A PREROUTING -p tcp --dport 2222 -j DNAT --to 172.16.33.3:22
echo Terminado.

```

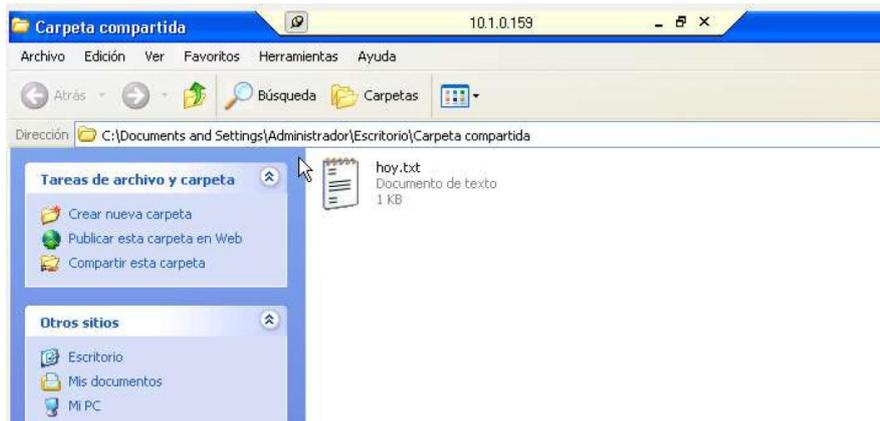


Ilustración 10 Conexión a PC compañero.

Carpetas compartidas entre usuarios.

Accediendo a las ubicaciones de la red, realizamos la conexión con el servidor, introduciendo la dirección IP.

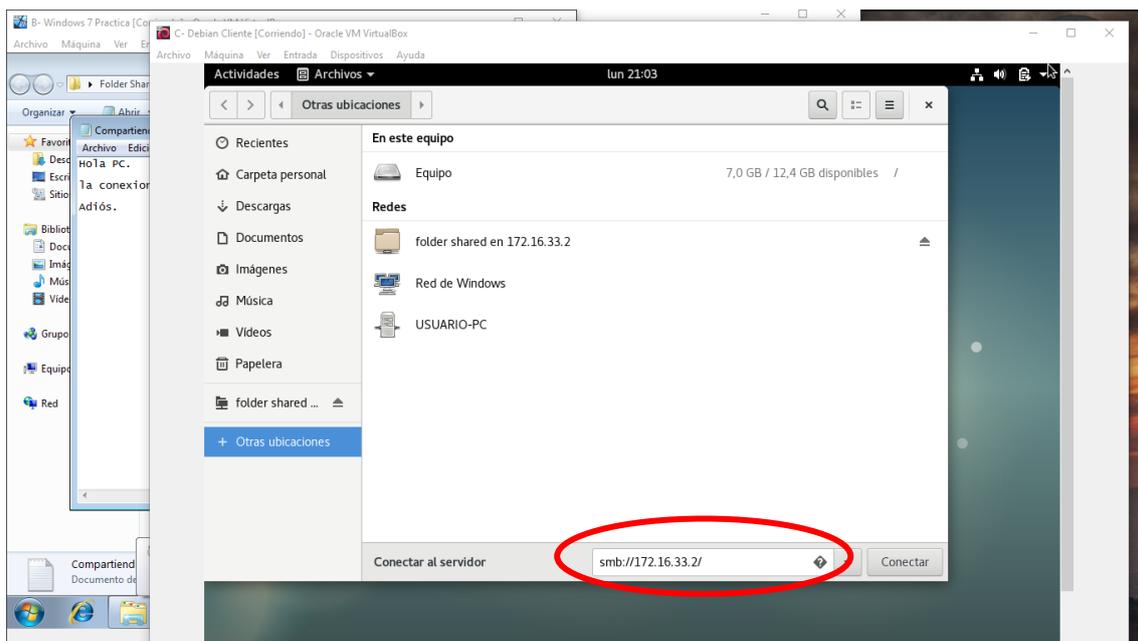


Ilustración 11 Conexión a la IP 172.16.33.2

Realizamos la conexión a nuestro servidor.

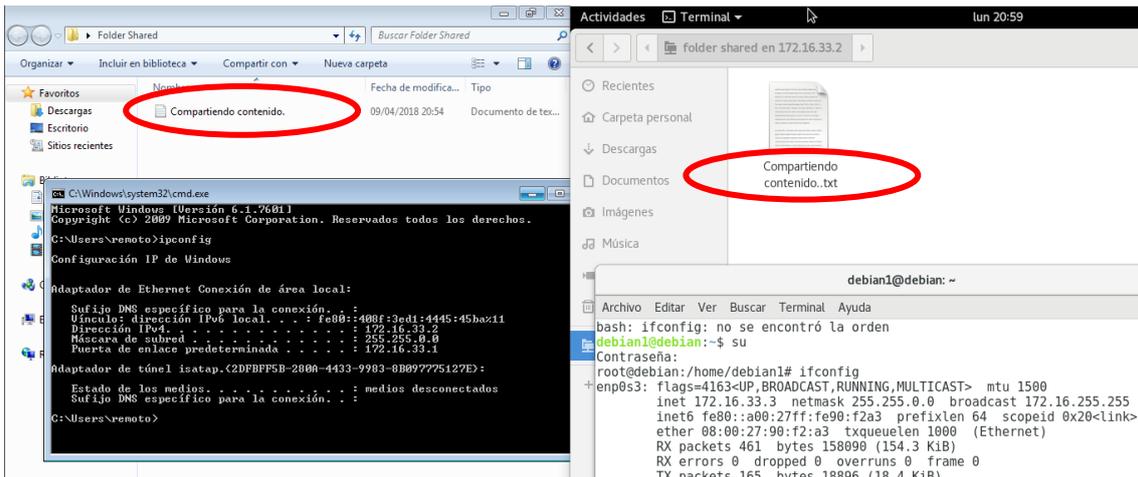


Ilustración 12 Carpetas compartidas entre usuarios de la red

Vemos el contenido del archivo compartido entre los equipos de la red.

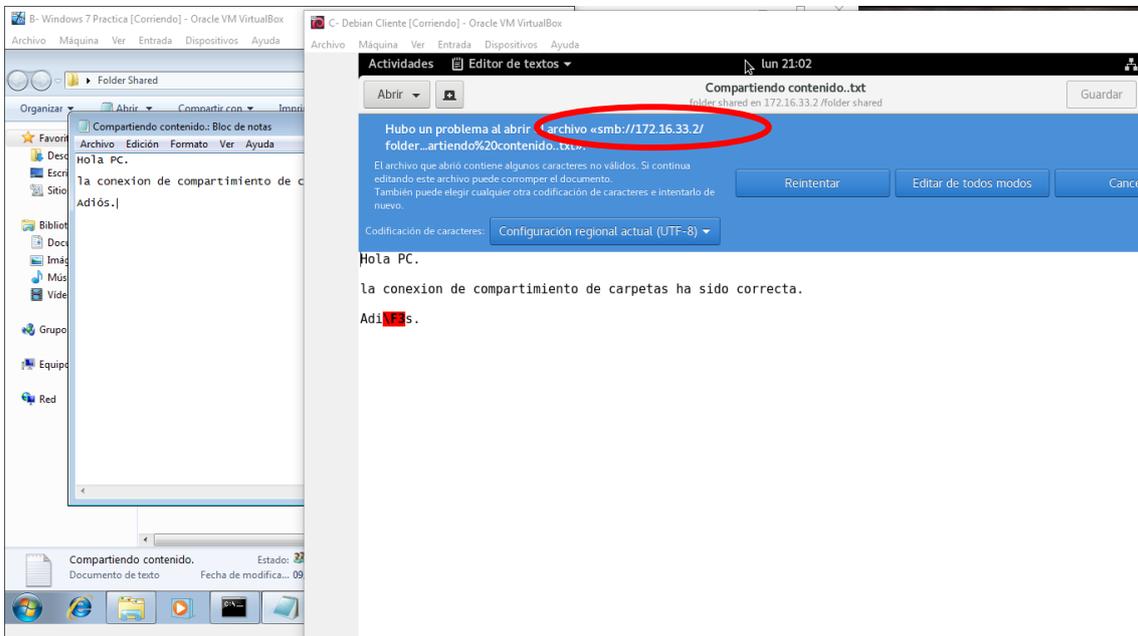


Ilustración 13 Edición del archivo compartido.