

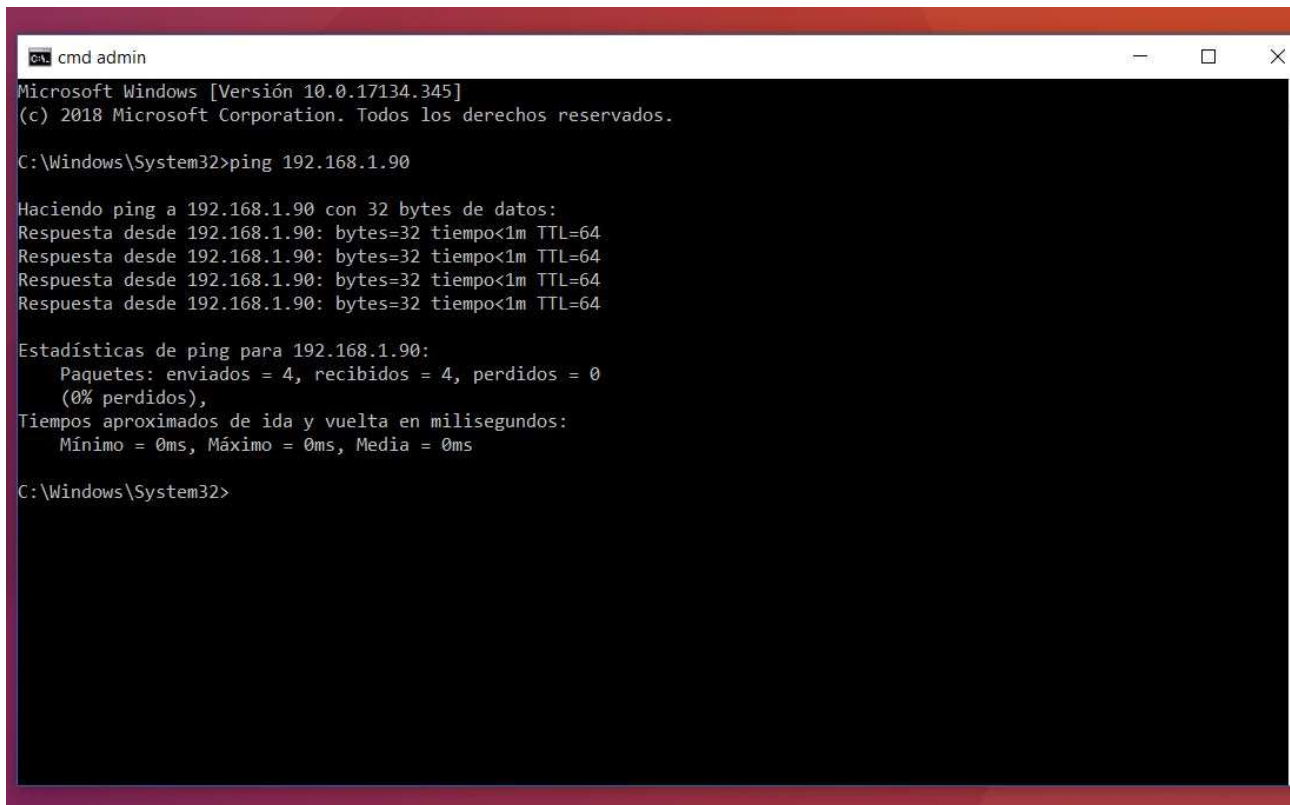
IP TABLETS

Partimos de 2 máquinas:

Ubuntu16 con ip 192.168.1.90

Windows con ip 192.168.1.101

Comenzamos probando ping 192.168.1.101



```
C:\cmd admin
Microsoft Windows [Versión 10.0.17134.345]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Windows\System32>ping 192.168.1.90

Haciendo ping a 192.168.1.90 con 32 bytes de datos:
Respuesta desde 192.168.1.90: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.90: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.90: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.90: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 192.168.1.90:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Windows\System32>
```

Modifico el fichero “iptables” adaptado a nuestras ip

```
#!/bin/sh
## SCRIPT de IPTABLES - ejemplo del manual de iptables
## Ejemplo de script para proteger la propia máquina

echo -n Aplicando Reglas de Firewall...

## FLUSH de reglas
iptables -F
iptables -X
iptables -Z
iptables -t nat -F

## Establecemos politica por defecto
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT

## Empezamos a filtrar

# El localhost se deja (por ejemplo conexiones locales a mysql)
/sbin/iptables -A INPUT -i lo -j ACCEPT

# A nuestra IP le dejamos todo
iptables -A INPUT -s 192.168.1.90 -j ACCEPT

# A un colega le dejamos entrar al ssh
iptables -A INPUT -s 192.168.1.101 -p tcp --dport 22 -j ACCEPT

# A un diseñador le dejamos usar el FTP
iptables -A INPUT -s 192.168.1.101 -p tcp --dport 21 -j ACCEPT

# El puerto 22 de ssh debe estar abierto.
iptables -A INPUT -p tcp --dport 22 -j ACCEPT

# Y el resto, lo cerramos
iptables -A INPUT -p tcp --dport 20:21 -j DROP
iptables -A INPUT -p tcp --dport 3306 -j DROP
iptables -A INPUT -p tcp --dport 80 -j DROP
iptables -A INPUT -p tcp --dport 10000 -j DROP

echo " OK . Verifique que lo que se aplica con: iptables -L -n"

# Fin del script
```

Ahora damos permisos de ejecución y ejecutamos el iptables:

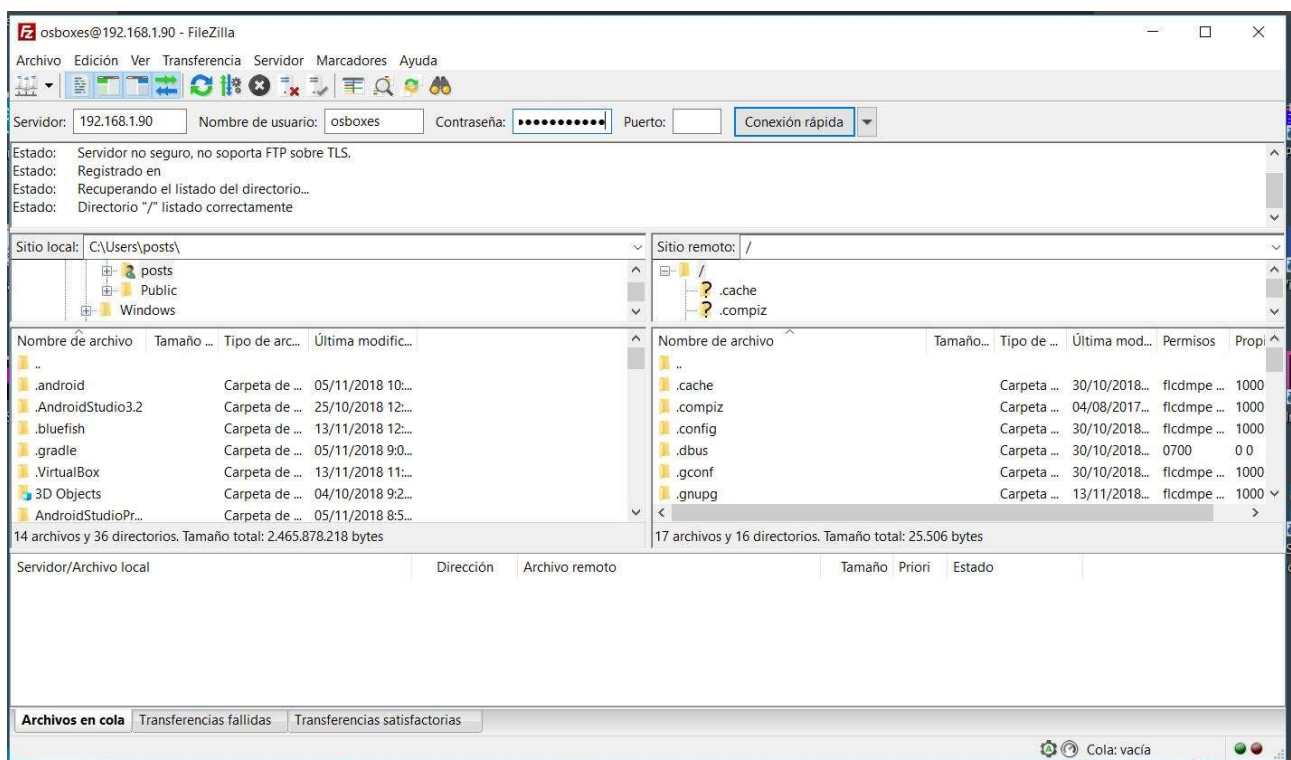
*** Siendo Root ***

- chmod 777 iptablesinputs.sh

./iptables.sh

```
root@osboxes: ~
drwx----- 3 osboxes osboxes 4096 Aug  4 2017 .local
drwx----- 4 osboxes osboxes 4096 Oct  9 05:53 .mozilla
drwxr-xr-x  2 osboxes osboxes 4096 Aug  4 2017 Music
drwxr-xr-x  2 osboxes osboxes 4096 Oct  5 04:04 Pictures
-rw-r--r--  1 osboxes osboxes  655 Aug  4 2017 .profile
drwxr-xr-x  2 osboxes osboxes 4096 Aug  4 2017 Public
-rwxrwxrwx  1 root    root    115 Oct 10 08:04 rutado
-rw-r--r--  1 osboxes osboxes   0 Oct  5 03:48 .sudo_as_admin_successful
drwxr-xr-x  2 osboxes osboxes 4096 Aug  4 2017 Templates
-rw-r----- 1 osboxes osboxes   5 Nov 13 05:55 .vboxclient-clipboard.pid
-rw-r----- 1 osboxes osboxes   5 Nov 13 05:55 .vboxclient-display.pid
-rw-r----- 1 osboxes osboxes   5 Nov 13 05:55 .vboxclient-draganddrop.pid
-rw-r----- 1 osboxes osboxes   5 Nov 13 05:55 .vboxclient-seamless.pid
drwxr-xr-x  2 osboxes osboxes 4096 Aug  4 2017 Videos
-rw-----  1 osboxes osboxes  52 Nov 13 05:55 .Xauthority
-rw-----  1 osboxes osboxes  82 Nov 13 05:55 .xsession-errors
-rw-----  1 osboxes osboxes 1160 Nov  6 06:41 .xsession-errors.old
root@osboxes:~# chmod 777 +x iptablesinputs.sh
chmod: cannot access '+x': No such file or directory
root@osboxes:~# chmod +x iptablesinputs.sh
root@osboxes:~# ./iptablesinputs.sh
Aplicando Reglas de Firewall... OK . Verifique que lo que se aplica con: iptables -L -n
root@osboxes:~#
```

Probamos que si conecta con las reglas de iptables:



Cambiamos el iptables para no permitir conexiones y lo probamos

