

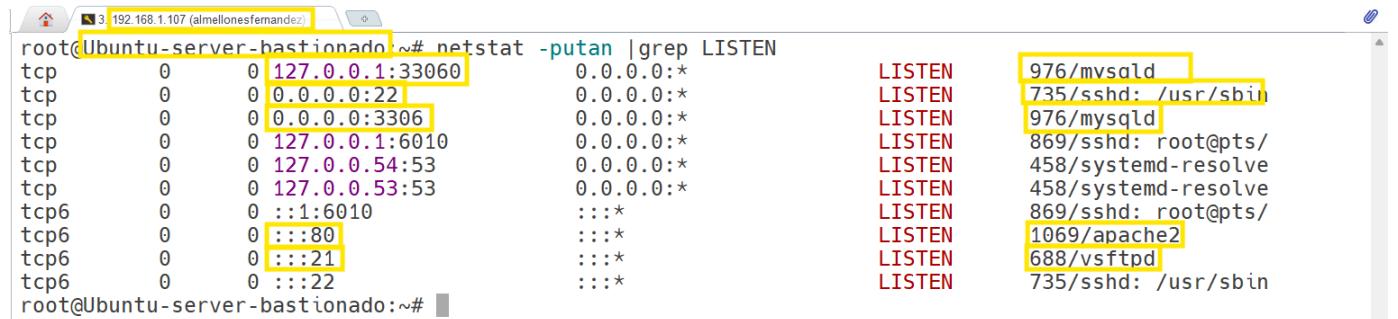
PRÁCTICA 3

U.D.2. REDES DE COMPUTADORAS SEGURAS

(I). SEGURIDAD A NIVEL DE HOST. FIREWALL DE SERVIDOR

SCRIPTS. HOST SIN CORTAFUEGOS. CONOCIENDO LA TARJETA LOOPBACK.

1. (**SERVICIOS INNECESARIOS, MONITORIZACIÓN**) Partiendo de un servidor Ubuntu Server recién instalado, actualizado, con la hora correctamente (y huso horario), realice las siguientes operaciones: a) Instalación de SSHD (configurado para entrar con llave privada por su comodidad), apache, vsftpd, mysql-server (se permitirá conexiones desde el exterior, no sólo localhost). Se deberá mostrar evidencias de que están escuchando (**netstat -putan | grep LISTEN**) dichos servicios instalados. ¿Podrías decir con tus palabras si hay algún otro servicio/demonio más instalado en este servidor, y a qué se dedica? (**0,5 puntos**)



```
root@Ubuntu-server-bastionado:~# netstat -putan | grep LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*                  LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*                  LISTEN
tcp        0      0 0.0.0.0:3306          0.0.0.0:*                  LISTEN
tcp        0      0 127.0.0.1:6010          0.0.0.0:*                  LISTEN
tcp        0      0 127.0.0.54:53          0.0.0.0:*                  LISTEN
tcp        0      0 127.0.0.53:53          0.0.0.0:*                  LISTEN
tcp6       0      0 ::1:6010             ::*:*                      LISTEN
tcp6       0      0 ::::80              ::*:*                      LISTEN
tcp6       0      0 ::::21              ::*:*                      LISTEN
tcp6       0      0 ::::22              ::*:*                      LISTEN
root@Ubuntu-server-bastionado:~#
```

Si hay un servicio más instalado , se llama **systemd-resolve** que usa el puerto 53 y este servicio es el encargado de las gestiones DNS

- b) Evidencie de que desde cliente Ubuntu Desktop se produce conexiones remotas (**netstat -putan | grep ESTABLISHED, ss, tcpdump, iptraf-ng**) a cada uno de estos servicios instalados en apartado anterior, además de poder hacerle ping. Intentar realizar un script que haga todas las comprobaciones desde el cliente o use &&. (**0,5 puntos**)

Álvaro Almellones Fernández

The screenshot shows a terminal window with two tabs. The left tab has the title 'almellonesfernandez@almellonesfernandez...' and contains the command 'wget 192.168.1.107'. The output shows a successful connection to port 80, receiving a 200 OK response for index.html. The right tab has the title 'almellonesfernandez@almellonesfernandez-VirtualBox:' and contains the command 'ping 192.168.1.107'. The output shows multiple ICMP echo requests being sent to the target host at 192.168.1.107.

```
almellonesfernandez@almellonesfernandez-VirtualBox:~$ wget 192.168.1.107
--2024-11-17 17:16:03-- http://192.168.1.107/
Conectando con 192.168.1.107:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 10671 (10K) [text/html]
Guardando como: 'index.html'

index.html          100%[=====] 10,42K  ---KB/s   en 0s

2024-11-17 17:16:03 (694 MB/s) - 'index.html' guardado [10671/10671]

almellonesfernandez@almellonesfernandez-VirtualBox:~$ ping 192.168.1.107
PING 192.168.1.107 (192.168.1.107) 56(84) bytes of data.
64 bytes from 192.168.1.107: icmp_seq=1 ttl=64 time=1.73 ms
64 bytes from 192.168.1.107: icmp_seq=2 ttl=64 time=0.810 ms
64 bytes from 192.168.1.107: icmp_seq=3 ttl=64 time=0.885 ms
64 bytes from 192.168.1.107: icmp_seq=4 ttl=64 time=1.16 ms
64 bytes from 192.168.1.107: icmp_seq=5 ttl=64 time=1.03 ms
64 bytes from 192.168.1.107: icmp_seq=6 ttl=64 time=1.27 ms
64 bytes from 192.168.1.107: icmp_seq=7 ttl=64 time=0.929 ms
64 bytes from 192.168.1.107: icmp_seq=8 ttl=64 time=0.895 ms
64 bytes from 192.168.1.107: icmp_seq=9 ttl=64 time=1.15 ms
64 bytes from 192.168.1.107: icmp_seq=10 ttl=64 time=1.05 ms
64 bytes from 192.168.1.107: icmp_seq=11 ttl=64 time=2.98 ms
64 bytes from 192.168.1.107: icmp_seq=12 ttl=64 time=0.921 ms
```

Las pestanas señaladas de la terminal tienen el resto de comandos ejecutados que realiza las conexiones del resto de servicios que se piden y se muestra la conexión a continuación

The screenshot shows a terminal window with the title '192.168.1.107 (almellonesfernandez)'. It displays the output of the 'netstat -putan | grep ESTABLISHED' command, which lists established network connections. A 'grep 192.168.1.108' filter is applied to the results, highlighting several connections to the IP address 192.168.1.108, likely representing a remote server.

```
root@Ubuntu-server-bastionado:~# netstat -putan | grep ESTABLISHED | grep 192.168.1.108
tcp        0      0 192.168.1.107:22          192.168.1.108:44804      ESTABLISHED
tcp        0      0 192.168.1.107:3306        192.168.1.108:58950      ESTABLISHED
tcp6       0      0 192.168.1.107:21          192.168.1.108:37894      ESTABLISHED
root@Ubuntu-server-bastionado:~#
```

c) Evidencie qué desde Ubuntu Server, actuando como **cliente**, puede: (0,5 puntos)

i. Resolver dns con servidores remotos (\$ping www.diariosur.es)

The screenshot shows a terminal window with the title '192.168.1.107 (almellonesfernandez)'. It displays the output of the 'ping www.diariosur.es' command. The command uses the IP address 2.16.88.183 as a remote DNS resolver. The output shows the ping statistics for 8 packets transmitted, with 8 received and 0% packet loss. The round-trip time (rtt) is listed as 15.402/19.426/43.721/9.189 ms.

```
root@Ubuntu-server-bastionado:~# ping www.diariosur.es
PING e15414.a.akamaiedge.net (2.16.88.183) 56(84) bytes of data.
64 bytes from a2-16-88-183.deploy.static.akamaitechnologies.com (2.16.88.183): icmp_seq=1 ttl=55 time=16.7 ms
64 bytes from a2-16-88-183.deploy.static.akamaitechnologies.com (2.16.88.183): icmp_seq=2 ttl=55 time=16.0 ms
64 bytes from a2-16-88-183.deploy.static.akamaitechnologies.com (2.16.88.183): icmp_seq=3 ttl=55 time=43.7 ms
64 bytes from a2-16-88-183.deploy.static.akamaitechnologies.com (2.16.88.183): icmp_seq=4 ttl=55 time=15.6 ms
64 bytes from a2-16-88-183.deploy.static.akamaitechnologies.com (2.16.88.183): icmp_seq=5 ttl=55 time=15.9 ms
64 bytes from a2-16-88-183.deploy.static.akamaitechnologies.com (2.16.88.183): icmp_seq=6 ttl=55 time=16.2 ms
64 bytes from a2-16-88-183.deploy.static.akamaitechnologies.com (2.16.88.183): icmp_seq=7 ttl=55 time=15.4 ms
64 bytes from a2-16-88-183.deploy.static.akamaitechnologies.com (2.16.88.183): icmp_seq=8 ttl=55 time=15.9 ms
^C
--- e15414.a.akamaiedge.net ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7010ms
rtt min/avg/max/mdev = 15.402/19.426/43.721/9.189 ms
root@Ubuntu-server-bastionado:~#
```

Álvaro Almellones Fernández

ii. Actualizar la hora del S.O. (#ntpdate hora.rediris.es && sleep 10 && hwclock -h)

```
root@Ubuntu-server-bastionado:~# ntpdate pool.ntp.org && sleep 10 && hwclock --systohc
2024-11-17 17:57:16.355426 (+0100) -0.001038 +/- 0.008574 pool.ntp.org 193.149.0.221 s1 no-leap
root@Ubuntu-server-bastionado:~# date
Sun Nov 17 17:57:48 CET 2024
root@Ubuntu-server-bastionado:~#
```

No pude usar los servidores hora.rediris.es porque me ponía que no eran servidores elegibles

iii. Hacer ping algún equipo exterior (\$ping 8.8.8.8).

```
root@Ubuntu-server-bastionado:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=16.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=16.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=15.2 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=15.6 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 15.227/15.816/16.246/0.410 ms
root@Ubuntu-server-bastionado:~#
```

iv. Descargarse una web remota (#wget ..)

```
root@Ubuntu-server-bastionado:~# wget marca.com
--2024-11-17 18:10:25-- http://marca.com/
Resolving marca.com (marca.com)... 34.147.120.111, 2001:67c:2294:1000::f199
Connecting to marca.com (marca.com)|34.147.120.111|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://marca.com/ [following]
--2024-11-17 18:10:25-- https://marca.com/
Connecting to marca.com (marca.com)|34.147.120.111|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.marca.com/ [following]
--2024-11-17 18:10:25-- https://www.marca.com/
Resolving www.marca.com (www.marca.com)... 151.101.133.50
Connecting to www.marca.com (www.marca.com)|151.101.133.50|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 826035 (807K) [text/html]
Saving to: 'index.html'

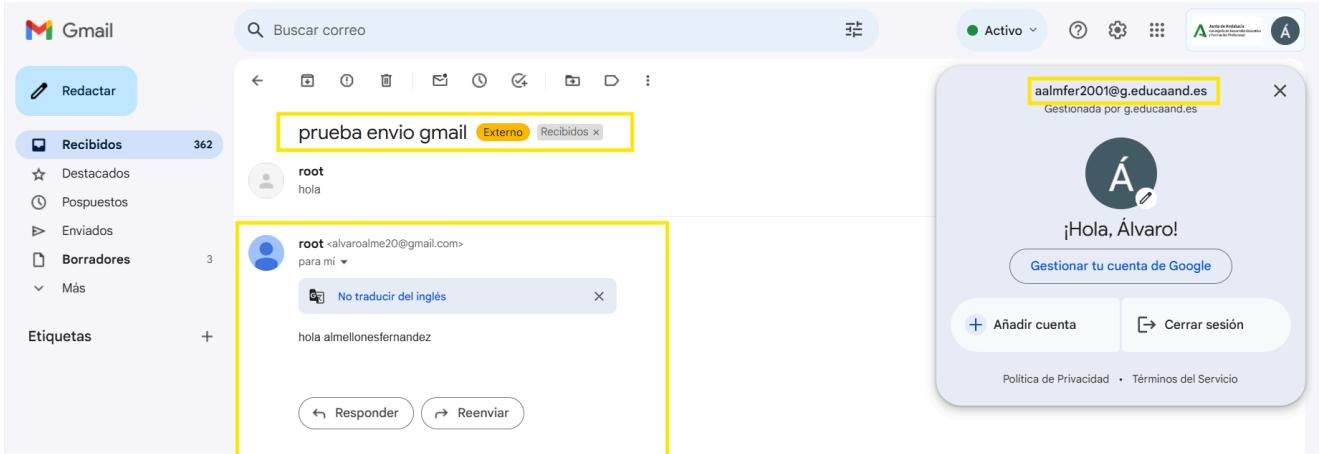
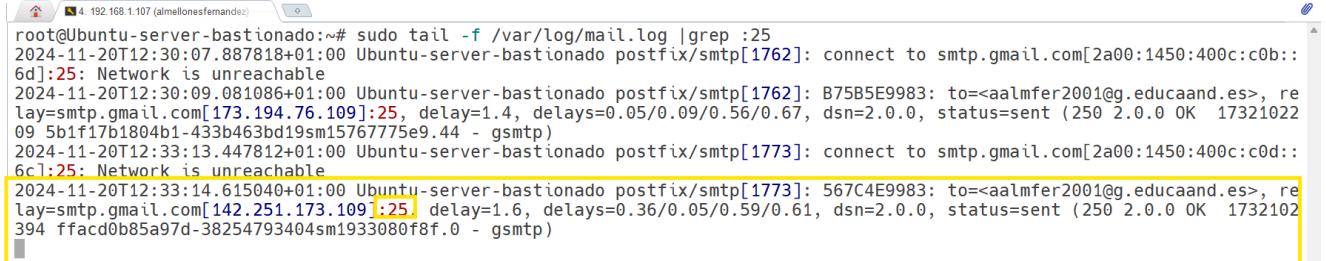
index.html          100%[=====] 806.67K  --.-KB/s   in 0.06s

2024-11-17 18:10:25 (12.6 MB/s) - 'index.html' saved [826035/826035]
root@Ubuntu-server-bastionado:~#
```

v. Enviar un correo (#echo hola | mailx -s "Asunto" XXX@gmail.com) (puerto 25).

```
root@Ubuntu-server-bastionado:~# echo "hola almellonesfernandez" | mail -s "prueba envio gmail" aalmfer2001@g.educaand.es
root@Ubuntu-server-bastionado:~#
```

Álvaro Almellones Fernández



vi. Conectarse por ssh algún equipo remoto



El mantenimiento de seguridad expandido para Applications está desactivado

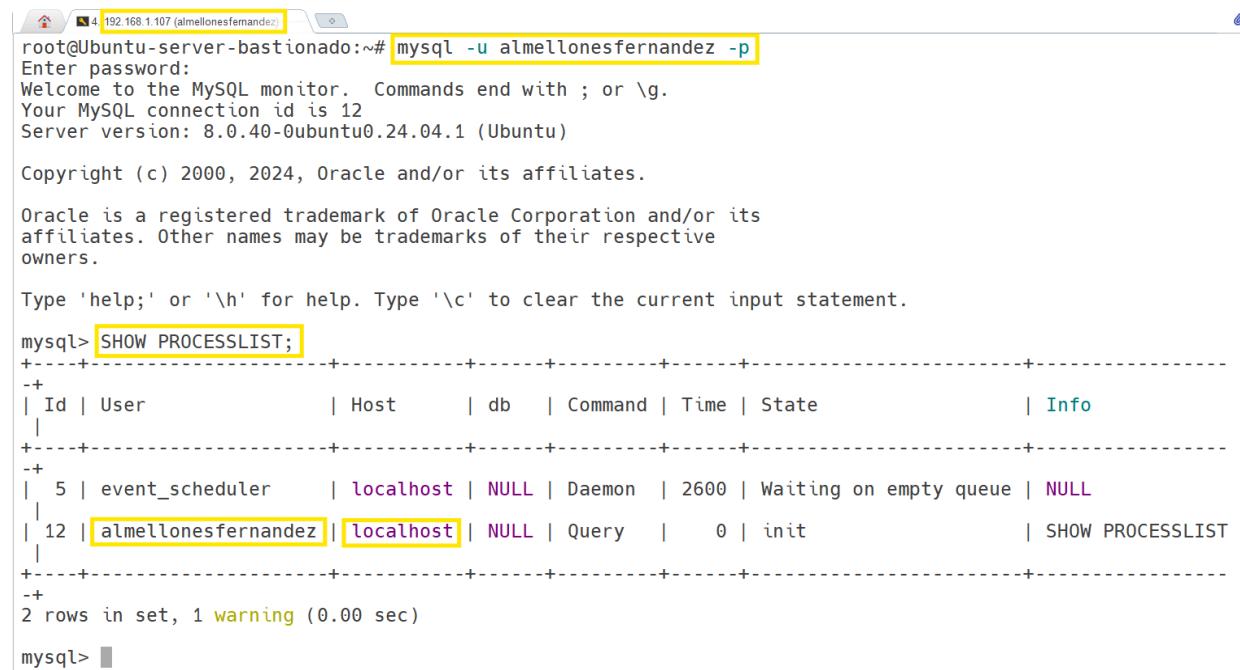
Se pueden aplicar 85 actualizaciones de forma inmediata.
6 de estas son actualizaciones de seguridad estándares.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea <https://ubuntu.com/esm> o ejecute «sudo pro status»

Last login: Sun Nov 17 18:40:46 2024 from 192.168.1.107
almellonesfernandez@almellonesfernandez-VirtualBox:~\$

vii. Entrar en el servidor mysqld vía localhost. (`netstat -putan | grep ESTABLISHED, ss, tcpdump, iptraf-ng`)

Álvaro Almellones Fernández



```
root@Ubuntu-server-bastionado:~# mysql -u almellonesfernandez -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 8.0.40-Ubuntu0.24.04.1 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> SHOW PROCESSLIST;
+----+-----+-----+-----+-----+-----+
| Id | User          | Host     | db      | Command | Time   | State           |
+----+-----+-----+-----+-----+-----+
| 5  | event_scheduler | localhost | NULL    | Daemon  | 2600   | Waiting on empty queue | NULL
| 12 | almellonesfernandez | localhost | NULL    | Query   | 0      | init             | SHOW PROCESSLIST
+----+-----+-----+-----+-----+-----+
2 rows in set, 1 warning (0.00 sec)

mysql>
```

*** Haga un snapshot a la máquina virtual, con el nombre XXXx-Dia y escriba lo que contiene ese S.O. Muestre dicho snapshot aunque no se valorará.

INICIANDONOS EN IPTABLES y SCRIPTS. CORTAFUEGOS DE SERVIDOR.

CONOCIENDO LA TARJETA LOOPBACK. Consideraciones a tener en cuenta:

- En este ejercicio además de los “sensores” usados en prácticas anteriores, tendréis que tener en cuenta #iptables -L -n -v, #iptables -L -n -v | grep , tail -f /var/log/kern....
- Realice un script (XXxx-iptables.sh) para la ejecución de iptables.
- **Este es típico ejercicio que hay que probar que se puede y que no se puede.**
Ajustar a cada ejercicio.
 - Es importante que en las capturas aparezca parte izquierda equipo/s cliente/s con las conexiones que se prueban, y en la parte derecha el servidor (para visualizar conexiónado, fichero de logs, iptables -L -n -v, etc.)
 - En alguno de los apartados (a elección del alumno) quiere que use los contadores para evidenciar lo que ocurre.

Álvaro Almellones Fernández

2. (INICIANDO SCRIPTS) Realice un script de Linux (cortafuegos.sh) que se arranque en el inicio del S.O del servidor Ubuntu Server con las siguientes consideraciones (**0,5 puntos cada uno**)

- a) Se borren los contadores (-Z) y todas las reglas (-F) que estuvieran cargadas en el kernel del S.O.

```
Ubuntu_desktop_bastionado (Recien instalado SO) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
23 de nov 11:08
almellonesfernandez@almellonesfernandez-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.108 netmask 255.255.255.0 broadcast 192.168.1.255
        inet6 fe80::a00:27ff:fea7:5133 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:a7:51:33 txqueuelen 1000 (Ethernet)
    RX packets 4266 bytes 5589487 (5.5 MB)
    RX errors 0 dropped 14 overruns 0 frame 0
    TX packets 931 bytes 102696 (102.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Bucle local)
    RX packets 173 bytes 16420 (16.4 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 173 bytes 16420 (16.4 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

almellonesfernandez@almellonesfernandez-VirtualBox:~$ 

192.168.1.107 (almellonesfernandez)
Terminal Sessions View Xserver Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Q 192.168.1.107 (almellonesfernandez)
GNU nano 7.2
#!/bin/bash
# Variables
tarjeta="enp0s3"
IP_Confianza="192.168.1.108"
MAC_Confianza=""

echo "Iniciandose cortafuegos de Host: Alvaro Almellones"
iptables -F #Borra reglas de filtrado.
iptables -X #Borra cadenas personalizadas.
iptables -Z #Reinicia contadores.

Activar Windows
Help Write Out Where Is Configuration Cut Execut
Exit Read File Replace Paste Justif
UNREGISTERED VERSION - Please support Mobaxterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

7. 192.168.1.107 (almellonesfernandez)
Chain INPUT (policy DROP 33 packets, 2092 bytes)
pkts bytes target prot opt in out source destination
0 0 ACCEPT 6 -- enp0s3 * 192.168.1.108 0.0.0.0/0
:22
225 15048 ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
:22 MAC 38:fc:98:0f:99:7f

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

Chain OUTPUT (policy DROP 1 packets, 76 bytes)
pkts bytes target prot opt in out source destination
149 14248 ACCEPT 0 -- * enp0s3 0.0.0.0/0 0.0.0.0/0

RELATED,ESTABLISHED
root@Ubuntu-server-bastionado:~/scripts# ./almellonesfernandez-iptables.sh
Iniciandose cortafuegos de Host: Alvaro Almellones
root@Ubuntu-server-bastionado:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 1 packets, 40 bytes)
pkts bytes target prot opt in out source destination
0 0 ACCEPT 6 -- enp0s3 * 192.168.1.108 0.0.0.0/0
:22
10 640 ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
:22 MAC 38:fc:98:0f:99:7f

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

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
7 648 ACCEPT 0 -- * enp0s3 0.0.0.0/0 0.0.0.0/0

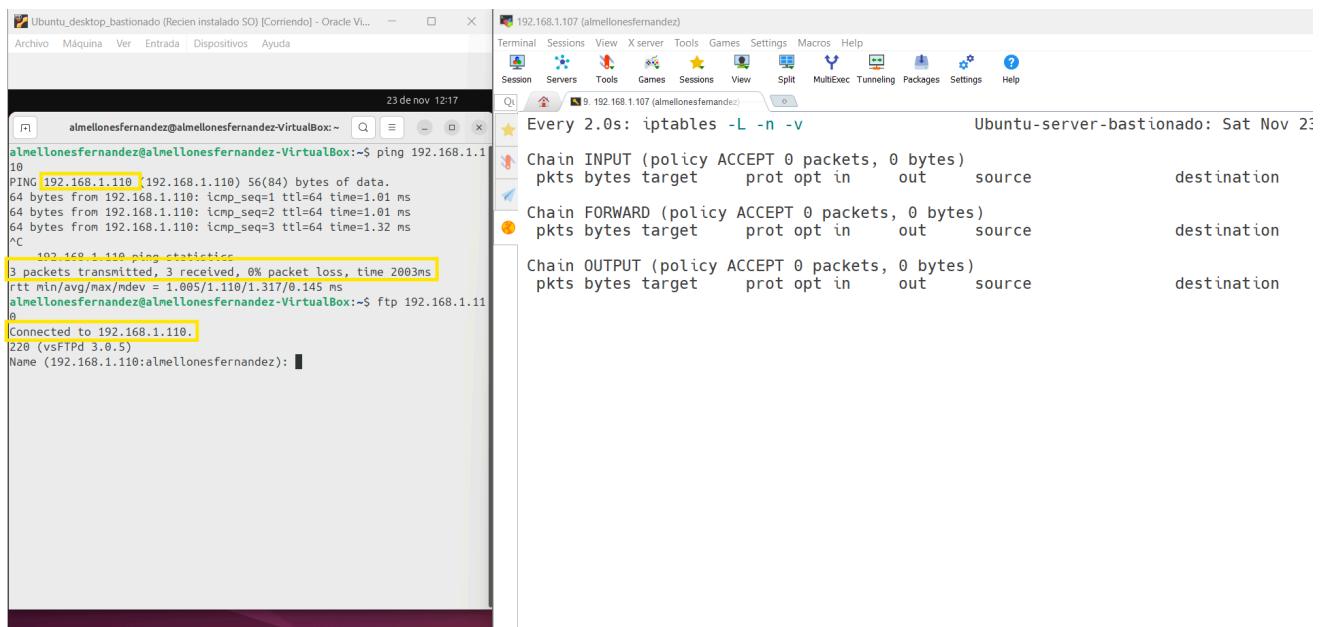
RELATED,ESTABLISHED
root@Ubuntu-server-bastionado:~/scripts# 
```

Álvaro Almellones Fernández

Se ve como al volver a iniciar el script se borrar las reglas que ya estuvieran cargadas

b) Las políticas por defecto sean DROP tanto en INPUT, OUTPUT y FORWARD en todo momento. En este momento de la práctica todo lo evidenciado en ejercicio número 1 debe fallar. Demuestre esto con los contadores de DROP.

Antes de aplicar las reglas : (voy a probar con un par de servicios de ejemplo del ejercicio anterior)



He ajustado las reglas iptable de input para que pueda acceder por ssh desde una ip de confianza (Ubuntu Desktop) y una mac de confianza (la red de mi casa para que las capturas se vean en el fondo blanco)

The screenshot shows a terminal window titled '7. 192.168.1.107 (almellonesfernandez)' running a script named 'iptables.sh'. The script starts by defining variables: 'tarjeta="enp0s3"', 'IP_Confianza="192.168.1.108"', and 'MAC_Confianza="38:FC:98:0F:99:7F"'. It then prints a welcome message and uses 'iptables' commands to clear existing rules and set default policies to DROP for INPUT, OUTPUT, and FORWARD. Finally, it adds rules to accept established/related connections and allow traffic from the trusted IP and MAC address.

```
#!/bin/bash

# Variables
tarjeta="enp0s3"
IP_Confianza="192.168.1.108"
MAC_Confianza="38:FC:98:0F:99:7F"

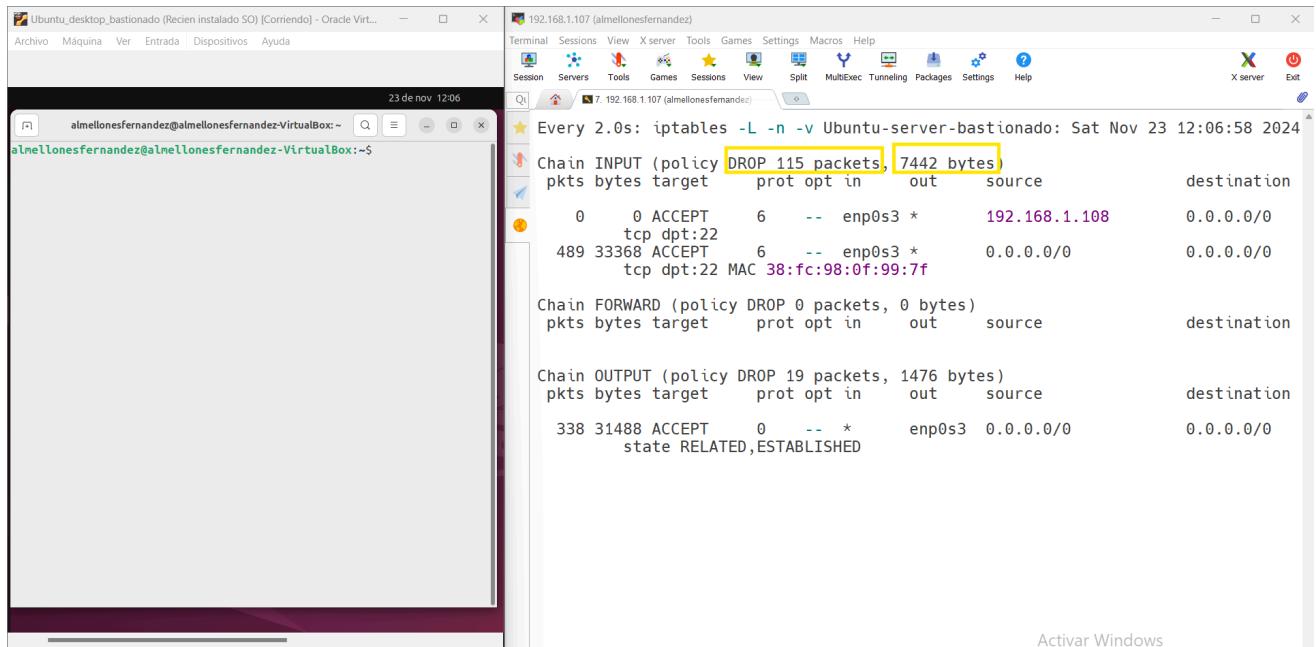
echo "Iniciandose cortafuegos de Host: Alvaro Almellones"

iptables -F #Borra reglas de filtrado.
iptables -X #Borra cadenas personalizadas.
iptables -Z #Reinicia contadores.

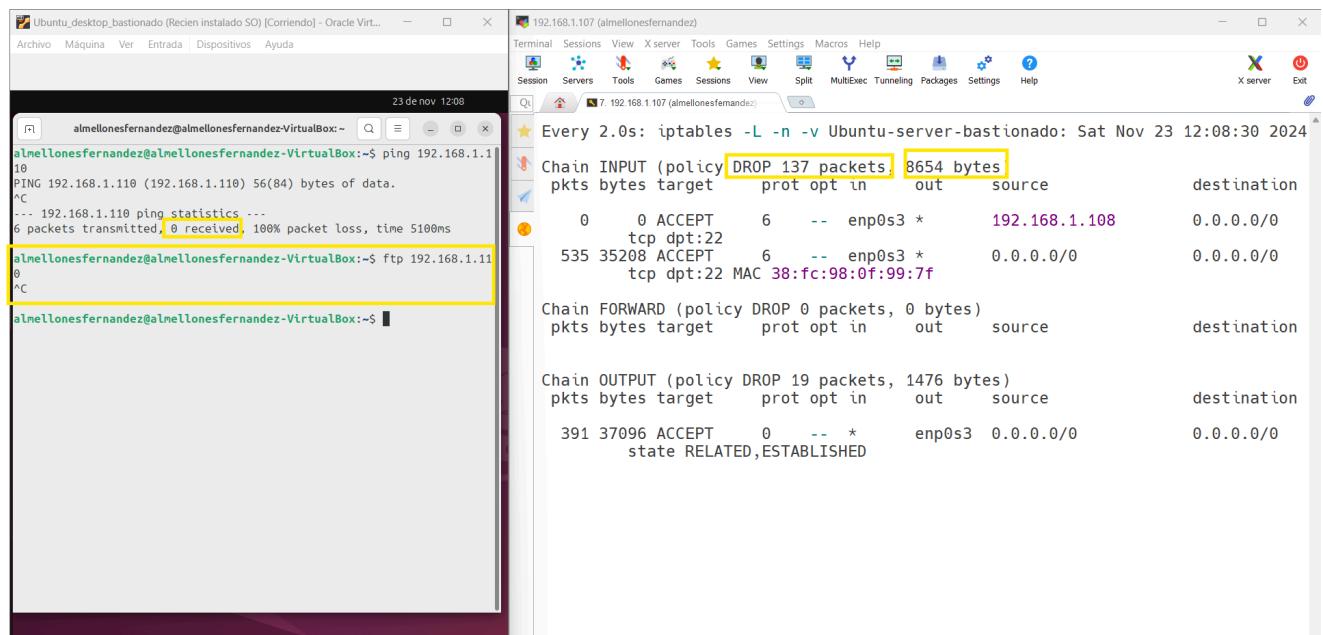
iptables -P INPUT DROP #Politica por defecto DROP
iptables -P OUTPUT DROP #Politica por defecto DROP
iptables -P FORWARD DROP #Politica por defecto DROP

# Reglas de INPUT
iptables -A OUTPUT -o $tarjeta -m state --state ESTABLISHED,RELATED -j ACCEPT # Re
iptables -A INPUT -i $tarjeta -p tcp --dport 22 -s $IP_Confianza -j ACCEPT
iptables -A INPUT -i $tarjeta -p tcp --dport 22 -m mac --mac-source $MAC_Confianza
```

Álvaro Almellones Fernández



Después de aplicar las reglas:



(Nota Importante: Por alguna razón que desconozco la ip de mi ubuntu server cambiado de .107 a .110)

Los packets y bytes aumentan en drop y como podemos ver por ejemplo en el ping del Ubuntu Desktop nos revela que el server no ha recibido packets

- c) Se permite al interfaz loopback conexiones entrantes y salientes al servicio mysqld, pero no a ningún otro servicio (ssh, web, vsftpd, ping). Dejar posteriormente que se permita todo.

Álvaro Almellones Fernández

```
GNU nano 7.2                                         almellonesfernandez@ubuntu-server-bastionado:~/scripts$ iptables.sh *
```

```
# Variables
tarjeta="enp0s3"
IP_Confianza="192.168.1.108"
MAC_Confianza="38:FC:98:0F:99:7F"

echo "Iniciandose cortafuegos de Host: Alvaro Almellones"

iptables -F #Borra reglas de filtrado.
iptables -X #Borra cadenas personalizadas.
iptables -Z #Reinicia contadores.

iptables -P INPUT DROP #Politica por defecto DROP
iptables -P OUTPUT DROP #Politica por defecto DROP
iptables -P FORWARD DROP #Politica por defecto DROP

#Reglas de loopback permitiendo solo mysql
iptables -A INPUT -i lo -p tcp --dport 3306 -j ACCEPT
iptables -A OUTPUT -o lo -p tcp --dport 3306 -j ACCEPT

# Reglas de INPUT
iptables -A INPUT -o $tarjeta -m state --state ESTABLISHED,RELATED -j ACCEPT # Respuesta de los input que recibe el servidor
iptables -A INPUT -i $tarjeta -p tcp --dport 22 -s $IP_Confianza -j ACCEPT
iptables -A INPUT -i $tarjeta -p tcp --dport 22 -m mac --mac-source $MAC_Confianza -j ACCEPT
```

```
root@Ubuntu-server-bastionado:~/scripts$ ./almellonesfernandez-iptables.sh
Iniciandose cortafuegos de Host: Alvaro Almellones
root@Ubuntu-server-bastionado:~/scripts$ sudo iptables -L -n -v
Chain INPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in     out    source               destination
  0   0 ACCEPT  6  --  lo      *       0.0.0.0/0            0.0.0.0/0          [REDACTED]
  0   0 ACCEPT  6  --  enp0s3   *       192.168.1.108      0.0.0.0/0          [REDACTED]
 10  640 ACCEPT  6  --  enp0s3   *       0.0.0.0/0            0.0.0.0/0          [REDACTED]
Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in     out    source               destination

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in     out    source               destination
  0   0 ACCEPT  6  --  *       lo      0.0.0.0/0            0.0.0.0/0          [REDACTED]
  7  616 ACCEPT  0  --  *       enp0s3  0.0.0.0/0           0.0.0.0/0          state RELATED,ESTABLISHED
root@Ubuntu-server-bastionado:~/scripts$ mysql -u root -p -h localhost
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 18
Server version: 8.0.40-Ubuntu0.24.04.1 (Ubuntu)

Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> exit
Bye
root@Ubuntu-server-bastionado:~/scripts#
```

```
Activar Windows
Ve a Configuración para activar Windows.
```

```
root@Ubuntu-server-bastionado:~/scripts$ ping localhost
PING localhost (127.0.0.1) 56(84) bytes of data.
^C
--- localhost ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2027ms
root@Ubuntu-server-bastionado:~/scripts$ ftp localhost
^C

root@Ubuntu-server-bastionado:~/scripts$ wget localhost
--2024-11-23 15:21:45-- http://localhost/
Resolving localhost (localhost)... 127.0.0.1
Connecting to localhost (localhost)|127.0.0.1:80... ^C
root@Ubuntu-server-bastionado:~/scripts$ ssh localhost
^C

root@Ubuntu-server-bastionado:~/scripts$ sudo iptables -L -n -v
Chain INPUT (policy DROP 58 packets, 2933 bytes)
pkts bytes target prot opt in     out    source               destination
  0   0 ACCEPT  6  --  lo      *       0.0.0.0/0            0.0.0.0/0          [REDACTED]
  0   0 ACCEPT  6  --  enp0s3   *       192.168.1.108      0.0.0.0/0          [REDACTED]
 362 23552 ACCEPT  6  --  enp0s3   *       0.0.0.0/0            0.0.0.0/0          [REDACTED]

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

Chain OUTPUT (policy DROP 11 packets, 732 bytes)
pkts bytes target prot opt in     out    source               destination
  0   0 ACCEPT  6  --  *       lo      0.0.0.0/0            0.0.0.0/0          [REDACTED]
 214 19648 ACCEPT  0  --  *       enp0s3  0.0.0.0/0           0.0.0.0/0          state RELATED,ESTABLISHED
root@Ubuntu-server-bastionado:~/scripts#
```

- d) No se permitirá **conexiones entrantes**, pero se logeará (-j LOG) con el prefijo (“Intentos-ataque-SSH Server-XXXX”, “Intentos-ataque-Web-Server-XXXX”,

Álvaro Almellones Fernández

"Intentos-ataque-mysql-XXxx") en el fichero /var/log/iptablesXXXX.log. Provocar dichas conexiones "fallidas" mediante hping3, nmap -S, ssh, ftp, wget, etc., desde cliente Ubuntu Desktop. Realizar conexiones para que se llene el fichero log.

The screenshot shows a terminal session on an Ubuntu desktop machine (IP 192.168.1.107) with the title bar "almellonesfernandez". The user runs "nano 50-default.conf" to edit the rsyslog configuration. A specific line is highlighted: ":msg,contains,"Intentos-ataque" /var/log/iptablesalmellonesfernandez.log". The user then runs "sudo systemctl restart rsyslog". Below this, the command "iptables -L -n -v" is run, showing several log entries from the kernel. One entry is highlighted: "root@Ubuntu-server-bastionado:/etc/rsyslog.d# iptables -L -n -v". The log entries show various connection attempts, including SSH, MySQL, and Web Server connections, all containing the string "Intentos-ataque". The final part of the screenshot shows the terminal again with the command "cat /var/log/iptablesalmellonesfernandez.log" running, displaying the captured log messages.

En el iptable -L -n -v se ve que he puesto la ip del Ubuntu desktop, pero ha sido por error al copiar y pegar, si se elimina la ip de la regla iptable se vería todas las ip que han intentado hacer una conexión ssh

***** Haga un backup de este script final (Xxxx-iptables-v1.0.sh). Muestre, aunque no se valorará. ***** Haga un nuevo snapshot para tener guardo este nuevo estado. Muestre, aunque no se valorará.

Álvaro Almellones Fernández

3. (REGLAS DE FILTRADO OUTPUT) Continuando con el script anterior y con las **respuestas (INPUT)** a las conexiones salientes(respuestas a esos OUTPUT),tienen que ser **exclusivamente** para conexiones establecidas o relacionadas, demostrar paso a paso que: **(0,5 puntos cada uno)**

- a) Únicamente puede hacer ping (ICMP) al exterior, pero no permite descargar web, resolver DNS, ni poder actualizar la hora (`# ntpdate`).

```
10.192.168.1.107 almellonesfernandez
GNU nano 7.2 almellonesfernandez-iptables.sh *

# Variables
tarjeta="enp0s3"
IP_Confianza="192.168.1.108"
MAC_Confianza="38:FC:98:0F:99:7F"

echo "Iniciandose cortafuegos de Host: Alvaro Almellones"

iptables -F #Borra reglas de filtrado.
iptables -X #Borra cadenas personalizadas.
iptables -Z #Reinicia contadores.

iptables -P INPUT DROP #Politica por defecto DROP
iptables -P OUTPUT DROP #Politica por defecto DROP
iptables -P FORWARD DROP #Politica por defecto DROP

#Reglas de loopback
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# Reglas de INPUT
iptables -A INPUT -o $tarjeta -m state --state ESTABLISHED,RELATED -j ACCEPT # Respuesta de los input que recibe el servidor
iptables -A INPUT -i $tarjeta -p tcp --dport 22 -s $IP_Confianza -j ACCEPT
iptables -A INPUT -i $tarjeta -p tcp --dport 22 -m mac --mac-source $MAC_Confianza -j ACCEPT

#Reglas de OUTPUT
iptables -A OUTPUT -i enp0s3 -m state --state ESTABLISHED,RELATED -j ACCEPT #Permite escuchar la respuesta de cuando hablo
iptables -A OUTPUT -o enp0s3 -p icmp -j ACCEPT

root@Ubuntu-server-bastionado:~/scripts# ./almellonesfernandez-iptables.sh
Iniciando cortafuegos de Host: Alvaro Almellones
root@Ubuntu-server-bastionado:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 1 packets, 63 bytes)
pkts bytes target     prot opt in     out    source        destination
   0    0 ACCEPT      0   --  lo      *       0.0.0.0/0      0.0.0.0/0
   0    0 ACCEPT      6   --  enp0s3  *       192.168.1.108  0.0.0.0/0
  12  768 ACCEPT      6   --  enp0s3  *       0.0.0.0/0      0.0.0.0/0
   0    0 ACCEPT      0   --  enp0s3  *       0.0.0.0/0      0.0.0.0/0
   0    0 LOG         6   --  *       *       0.0.0.0/0      0.0.0.0/0
e-SSH Server-al"
   0    0 LOG         6   --  *       *       0.0.0.0/0      0.0.0.0/0
que-mysql-almello"
   0    0 LOG         6   --  *       *       0.0.0.0/0      0.0.0.0/0
e-Web-Server-al"
Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target     prot opt in     out    source        destination

Chain OUTPUT (policy DROP 4 packets, 260 bytes)
pkts bytes target     prot opt in     out    source        destination
   0    0 ACCEPT      0   --  *       lo      0.0.0.0/0      0.0.0.0/0
   7  648 ACCEPT      0   --  *       enp0s3  0.0.0.0/0      0.0.0.0/0
   0    0 ACCEPT      1   --  *       enp0s3  0.0.0.0/0      0.0.0.0/0
root@Ubuntu-server-bastionado:~/scripts#
```

Álvaro Almellones Fernández

root@Ubuntu-server-bastionado:~/scripts# ping 192.168.1.108
PING 192.168.1.108 (192.168.1.108) 56(84) bytes of data.
64 bytes from 192.168.1.108: icmp_seq=1 ttl=64 time=0.784 ms
64 bytes from 192.168.1.108: icmp_seq=2 ttl=64 time=1.09 ms
^C
--- 192.168.1.108 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1030ms
rtt min/avg/max/mdev = 0.784/0.938/1.092/0.154 ms
root@Ubuntu-server-bastionado:~/scripts# ping marca.com
^C
root@Ubuntu-server-bastionado:~/scripts# wget 8.8.8.8
--2024-11-23 16:51:19-- http://8.8.8.8/
Connecting to 8.8.8.8:80... ^C
root@Ubuntu-server-bastionado:~/scripts# ntpdate time.inm.es
^C^C^C
root@Ubuntu-server-bastionado:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 32 packets, 1609 bytes)
pkts bytes target prot opt in out source destination
10 676 ACCEPT 0 -- lo * 0.0.0.0/0 0.0.0.0/0
0 0 ACCEPT 6 -- enp0s3 * 192.168.1.108 0.0.0.0/0
187 11800 ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
2 168 ACCEPT 0 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
e-SH Server-al"
0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
que-mysql-almello"
0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
e-Web-Server-al"
Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
destination
Chain OUTPUT (policy DROP 110 packets, 6876 bytes)
pkts bytes target prot opt in out source destination
10 676 ACCEPT 0 -- * lo 0.0.0.0/0 0.0.0.0/0
109 10148 ACCEPT 0 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
1 84 ACCEPT 1 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
root@Ubuntu-server-bastionado:~/scripts#

Activar Windows
Ve a Configuración para activar Windows.

root@Ubuntu-server-bastionado:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 32 packets, 1609 bytes)
pkts bytes target prot opt in out source destination
10 676 ACCEPT 0 -- lo * 0.0.0.0/0 0.0.0.0/0
0 0 ACCEPT 6 -- enp0s3 * 192.168.1.108 0.0.0.0/0
187 11800 ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
2 168 ACCEPT 0 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
e-SH Server-al"
0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
que-mysql-almello"
0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
e-Web-Server-al"
Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
destination
Chain OUTPUT (policy DROP 110 packets, 6876 bytes)
pkts bytes target prot opt in out source destination
10 676 ACCEPT 0 -- * lo 0.0.0.0/0 0.0.0.0/0
109 10148 ACCEPT 0 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
1 84 ACCEPT 1 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
root@Ubuntu-server-bastionado:~/scripts#

state RELATED,ESTABLISHED
Activar Windows
Ve a Configuración para activar Windows.

b) Resuelve DNS y ping, pero que no deja actualizar el S.O ni puede actualizar la hora del S.O.

```
GNU nano 7.2                                         almellonesfernandez-iptables.sh
# Variables
tarjeta="enp0s3"
IP_Confianza="192.168.1.108"
MAC_Confianza="38:FC:98:0F:99:7F"

echo "Iniciándose cortafuegos de Host: Alvaro Almellones"

iptables -F #Borra reglas de filtrado.
iptables -X #Borra cadenas personalizadas.
iptables -Z #Reinicia contadores.

iptables -P INPUT DROP #Politica por defecto DROP
iptables -P OUTPUT DROP #Politica por defecto DROP
iptables -P FORWARD DROP #Politica por defecto DROP

#Reglas de loopback
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# Reglas de INPUT
iptables -A OUTPUT -o $tarjeta -m state --state ESTABLISHED,RELATED -j ACCEPT # Respuesta de los input que recibe el servidor
iptables -A INPUT -i $tarjeta -p tcp --dport 22 -s $IP_Confianza -j ACCEPT
iptables -A INPUT -i $tarjeta -p tcp --dport 22 -m mac --mac-source $MAC_Confianza -j ACCEPT

#Reglas de OUTPUT
iptables -A INPUT -i $tarjeta -m state --state ESTABLISHED,RELATED -j ACCEPT #Permite escuchar la respuesta de cuando hable
iptables -A OUTPUT -o $tarjeta -p icmp -j ACCEPT
iptables -A OUTPUT -o $tarjeta -p udp --dport 53 -j ACCEPT
```

Álvaro Almellones Fernández

```
root@Ubuntu-server-bastionado:/~scripts# nano almellonesfernandez-iptables.sh
root@Ubuntu-server-bastionado:/~scripts# ./almellonesfernandez-iptables.sh
Iniciandose cortafuegos de Host: Álvaro Almellones
root@Ubuntu-server-bastionado:/~scripts# iptables -L -n -v
Chain INPUT (policy DROP 1 packets, 40 bytes)
pkts bytes target prot opt in out source destination
  0   0 ACCEPT  0 -- lo * 0.0.0.0/0 0.0.0.0/0
  0   0 ACCEPT  6 -- enp0s3 * 192.168.1.108 0.0.0.0/0
 10  640 ACCEPT  6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
  0   0 ACCEPT  0 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
  0   0 LOG    6 -- * * 0.0.0.0/0 0.0.0.0/0
e-SSH Server-al"
  0   0 LOG    6 -- * * 0.0.0.0/0 0.0.0.0/0
que-mysql-almello"
  0   0 LOG    6 -- * * 0.0.0.0/0 0.0.0.0/0
e-Web-Server-al"
Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
  0   0 ACCEPT  0 -- * lo 0.0.0.0/0 0.0.0.0/0
  6  560 ACCEPT  0 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
  0   0 ACCEPT  1 -- * enp0s3 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
  0   0 ACCEPT  17 -- * enp0s3 0.0.0.0/0 0.0.0.0/0 udp dpt:53
root@Ubuntu-server-bastionado:/~scripts#
```

```
root@Ubuntu-server-bastionado:/~scripts# ping google.com
PING google.com (216.58.215.142) 56(84) bytes of data.
64 bytes from mad41s04-in-f14.1e100.net (216.58.215.142): icmp_seq=1 ttl=116 time=17.1 ms
64 bytes from mad41s04-in-f14.1e100.net (216.58.215.142): icmp_seq=2 ttl=116 time=17.1 ms
64 bytes from mad41s04-in-f14.1e100.net (216.58.215.142): icmp_seq=3 ttl=116 time=16.2 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 16.236/16.802/17.113/0.401 ms
root@Ubuntu-server-bastionado:/~scripts# nslookup google.com
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
Name: google.com
Address: 216.58.215.142
Name: google.com
Address: 2a00:1450:4003:80f::200e

root@Ubuntu-server-bastionado:/~scripts# sudo apt update
sudo ntpdate pool.ntp.org
[0%] [Connecting to archive.ubuntu.com (2620:2d:4002:1::103)] [Connecting to security.ubuntu.com (2620:2d:4002:1::102)]^C
ntpdiq: no eligible servers
root@Ubuntu-server-bastionado:/~scripts#
```

```
root@Ubuntu-server-bastionado:/~scripts# iptables -L -n -v
Chain INPUT (policy DROP 44 packets, 1392 bytes)
pkts bytes target prot opt in out source destination
 38 4250 ACCEPT  0 -- lo * 0.0.0.0/0 0.0.0.0/0
  0   0 ACCEPT  6 -- enp0s3 * 192.168.1.108 0.0.0.0/0
 160 10256 ACCEPT  6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
  20 2950 ACCEPT  0 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
  0   0 LOG    6 -- * * 0.0.0.0/0 0.0.0.0/0
e-SSH Server-al"
  0   0 LOG    6 -- * * 0.0.0.0/0 0.0.0.0/0
que-mysql-almello"
  0   0 LOG    6 -- * * 0.0.0.0/0 0.0.0.0/0
e-Web-Server-al"
Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
Chain OUTPUT (policy DROP 178 packets, 10744 bytes)
pkts bytes target prot opt in out source destination
 38 4250 ACCEPT  0 -- * lo 0.0.0.0/0 0.0.0.0/0
140 14232 ACCEPT  0 -- * enp0s3 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
  1  84 ACCEPT   1 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 17 1284 ACCEPT  17 -- * enp0s3 0.0.0.0/0 0.0.0.0/0 udp dpt:53
root@Ubuntu-server-bastionado:/~scripts#
```

c) Resuelve DNS y ping y permite actualizar el S.O. **exclusivamente** (IP servidores de Ubuntu), pero no permite descargar ninguna web, ni puede actualizar la hora del S.O.

Álvaro Almellones Fernández

```
GNU nano 7.2                                         almellonesfernandez-iptables.sh *
```

```
iptables -F #Borra reglas de filtrado.
iptables -X #Borra cadenas personalizadas.
iptables -Z #Reinicia contadores.

iptables -P INPUT DROP #Politica por defecto DROP
iptables -P OUTPUT DROP #Politica por defecto DROP
iptables -P FORWARD DROP #Politica por defecto DROP

#Reglas de loopback
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# Reglas de $tarjeta
iptables -A OUTPUT -o $tarjeta -m state --state ESTABLISHED,RELATED -j ACCEPT # Respuesta de los input que recibe el servidor
iptables -A INPUT -i $tarjeta -p tcp --dport 22 -s $IP_Confianza -j ACCEPT
iptables -A INPUT -i $tarjeta -p tcp --dport 22 -m mac --mac-source $MAC_Confianza -j ACCEPT

#Reglas de OUTPUT
iptables -A INPUT -i $tarjeta -m state --state ESTABLISHED,RELATED -j ACCEPT #Permite escuchar la respuesta de cuando hablo
iptables -A OUTPUT -o $tarjeta -p icmp -j ACCEPT
iptables -A OUTPUT -o $tarjeta -p udp --dport 53 -j ACCEPT
iptables -A OUTPUT -o $tarjeta -p tcp -d 91.189.91.83 --dport 80 -j ACCEPT # Permitir trafico HTTP (puerto 80) hacia archive.ubuntu.com
iptables -A OUTPUT -o $tarjeta -p tcp -d 91.189.91.83 --dport 443 -j ACCEPT # Permitir trafico HTTPS (puerto 443) hacia archive.ubuntu.com
iptables -A OUTPUT -o $tarjeta -p tcp -d 185.125.190.83 --dport 80 -j ACCEPT # Permitir trafico HTTP (puerto 80) hacia security.ubuntu.com
iptables -A OUTPUT -o $tarjeta -p tcp -d 185.125.190.83 --dport 443 -j ACCEPT # Permitir trafico HTTPS (puerto 443) hacia security.ubuntu.com
```

```
root@Ubuntu-server-bastionado:~/scripts# nano almellonesfernandez-iptables.sh
root@Ubuntu-server-bastionado:~/scripts# ./almellonesfernandez-iptables.sh
Iniciandose cortafuegos de Host: Álvaro Almellones
root@Ubuntu-server-bastionado:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 2 packets, 72 bytes)
pkts bytes target     prot opt in     out    source         destination
  0   0 ACCEPT      0   --  lo      *       0.0.0.0/0      0.0.0.0/0
  0   0 ACCEPT      6   --  enp0s3  *       192.168.1.108  0.0.0.0/0
 60 3840 ACCEPT      6   --  enp0s3  *       0.0.0.0/0      0.0.0.0/0
  0   0 ACCEPT      0   --  enp0s3  *       0.0.0.0/0      0.0.0.0/0
  0   0 LOG        6   --  *      *       0.0.0.0/0      0.0.0.0/0
e-SSH Server-al"
  0   0 LOG        6   --  *      *       0.0.0.0/0      0.0.0.0/0
que-mysql-almello"
  0   0 LOG        6   --  *      *       0.0.0.0/0      0.0.0.0/0
e-Web-Server-al"
Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target     prot opt in     out    source         destination

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target     prot opt in     out    source         destination
  0   0 ACCEPT      0   --  *      lo      0.0.0.0/0      0.0.0.0/0
 31 2984 ACCEPT      0   --  *      enp0s3  0.0.0.0/0      0.0.0.0/0
  0   0 ACCEPT      1   --  *      enp0s3  0.0.0.0/0      0.0.0.0/0
  0   0 ACCEPT      17  --  *      enp0s3  0.0.0.0/0      0.0.0.0/0
  0   0 ACCEPT      6   --  *      enp0s3  0.0.0.0/0      91.189.91.83
  0   0 ACCEPT      6   --  *      enp0s3  0.0.0.0/0      91.189.91.83
  0   0 ACCEPT      6   --  *      enp0s3  0.0.0.0/0      185.125.190.83
  0   0 ACCEPT      6   --  *      enp0s3  0.0.0.0/0      185.125.190.83
```

Activar Windows

```
root@Ubuntu-server-bastionado:~/scripts# ping google.com
PING google.com (142.250.184.14) 56(84) bytes of data.
64 bytes from mad41s10-in-f14.1e100.net (142.250.184.14): icmp_seq=1 ttl=116 time=64.2 ms
64 bytes from mad41s10-in-f14.1e100.net (142.250.184.14): icmp_seq=2 ttl=116 time=16.1 ms
^C
--- google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 16.056/40.120/64.185/24.064 ms
root@Ubuntu-server-bastionado:~/scripts# nslookup google.com
Server:     127.0.0.53
Address:   127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.184.14
Name:   google.com
Address: 2a00:1450:4003:80f::200e
```

```
root@Ubuntu-server-bastionado:~/scripts# sudo apt update
Hit:1 http://archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
44 packages can be upgraded. Run 'apt list --upgradable' to see them.
root@Ubuntu-server-bastionado:~/scripts#
```

Álvaro Almellones Fernández

```
10.192.168.1.107 (almellonesfernandez)
root@Ubuntu-server-bastionado:~/scripts# wget marca.com
--2024-11-23 18:05:22-- http://marca.com/
Resolving marca.com (marca.com)... 34.147.120.111, 2001:67c:2294:1000::f199
Connecting to marca.com (marca.com)|34.147.120.111:80... ^C
root@Ubuntu-server-bastionado:~/scripts# ntpdate time.inm.es
^C^C

root@Ubuntu-server-bastionado:~/scripts# 

10.192.168.1.107 (almellonesfernandez)
root@Ubuntu-server-bastionado:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 106 packets, 3642 bytes)
pkts bytes target prot opt in     out    source          destination
  64  6407 ACCEPT  --   lo      *       0.0.0.0/0      0.0.0.0/0
  0   0 ACCEPT   6   --  enp0s3  *       192.168.1.108  0.0.0.0/0
 546 33744 ACCEPT  6   --  enp0s3  *       0.0.0.0/0      0.0.0.0/0
 51  6292 ACCEPT  0   --  enp0s3  *       0.0.0.0/0      0.0.0.0/0
  0   0 LOG      6   --   *      *       0.0.0.0/0      0.0.0.0/0
e-SSH Server-al"
  0   0 LOG      6   --   *      *       0.0.0.0/0      0.0.0.0/0
que-mysql-almello"
  0   0 LOG      6   --   *      *       0.0.0.0/0      0.0.0.0/0
e-Web-Server-al"
Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in     out    source          destination

Chain OUTPUT (policy DROP 73 packets, 4652 bytes)
pkts bytes target prot opt in     out    source          destination
  64  6407 ACCEPT  0   --   *      lo       0.0.0.0/0      0.0.0.0/0
374 35889 ACCEPT  0   --   *      enp0s3  0.0.0.0/0      0.0.0.0/0
  1   84 ACCEPT   1   --   *      enp0s3  0.0.0.0/0      0.0.0.0/0
 35  2536 ACCEPT  17  --   *      enp0s3  0.0.0.0/0      0.0.0.0/0
  0   0 ACCEPT   6   --   *      enp0s3  0.0.0.0/0      91.189.91.83
  0   0 ACCEPT   6   --   *      enp0s3  0.0.0.0/0      91.189.91.83
  2   120 ACCEPT  6   --   *      enp0s3  0.0.0.0/0      185.125.190.83
  0   0 ACCEPT   6   --   *      enp0s3  0.0.0.0/0      185.125.190.83
root@Ubuntu-server-bastionado:~/scripts#
```

d) Resuelve DNS y ping, y que se puede actualizar el S.O. y descargar web (http/https) pero no se permite actualizar la hora del S.O.

```
10.192.168.1.107 (almellonesfernandez)
GNU nano 7.2                                     al mellonesfernandez-iptables.sh
IP_Confianza="192.168.1.108"
MAC_Confianza="38:FC:98:0F:99:7F"

echo "Iniciando cortafuegos de Host: Alvaro Almellones"

iptables -F #Borra reglas de filtrado.
iptables -X #Borra cadenas personalizadas.
iptables -Z #Reinicia contadores.

iptables -P INPUT DROP #Politica por defecto DROP
iptables -P OUTPUT DROP #Politica por defecto DROP
iptables -P FORWARD DROP #Politica por defecto DROP

#Reglas de loopback
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# Reglas de INPUT
iptables -A OUTPUT -o $tarjeta -m state --state ESTABLISHED,RELATED -j ACCEPT # Respuesta de los input que recibe el servidor
iptables -A INPUT -i $tarjeta -p tcp --dport 22 -s $IP_Confianza -j ACCEPT
iptables -A INPUT -i $tarjeta -p tcp --dport 22 -m mac --mac-source $MAC_Confianza -j ACCEPT

#Reglas de OUTPUT
iptables -A INPUT -i $tarjeta -m state --state ESTABLISHED,RELATED -j ACCEPT #Permite escuchar la respuesta de cuando hable
iptables -A OUTPUT -o $tarjeta -p icmp -j ACCEPT
iptables -A OUTPUT -o $tarjeta -p udp --dport 53 -j ACCEPT
iptables -A OUTPUT -o $tarjeta -p tcp --dport 80 -j ACCEPT
iptables -A OUTPUT -o $tarjeta -p tcp --dport 443 -j ACCEPT
```

Álvaro Almellones Fernández

```
root@Ubuntu-server-bastionado:~/scripts# nano almellonesfernandez-iptables.sh
root@Ubuntu-server-bastionado:~/scripts# ./almellonesfernandez-iptables.sh
Iniciandose cortafuegos de Host: Álvaro Almellones
root@Ubuntu-server-bastionado:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 3 packets, 390 bytes)
 pkts bytes target  prot opt in   out    source          destination
   0   0 ACCEPT  0   --  lo   *      0.0.0.0/0      0.0.0.0/0
   0   0 ACCEPT  6   --  enp0s3 *      192.168.1.108  0.0.0.0/0
  14  896 ACCEPT  6   --  enp0s3 *      0.0.0.0/0      0.0.0.0/0
   0   0 ACCEPT  0   --  enp0s3 *      0.0.0.0/0      0.0.0.0/0
   0   0 LOG    6   --  *      *      0.0.0.0/0      0.0.0.0/0
e-SSH Server-al"
   0   0 LOG    6   --  *      *      0.0.0.0/0      0.0.0.0/0
que-mysql-almello"
   0   0 LOG    6   --  *      *      0.0.0.0/0      0.0.0.0/0
e-Web-Server-al"
Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target  prot opt in   out    source          destination
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target  prot opt in   out    source          destination
  9   840 ACCEPT  0   --  *      lo   0.0.0.0/0      0.0.0.0/0
  0   0 ACCEPT  1   --  *      enp0s3 0.0.0.0/0      0.0.0.0/0
  0   0 ACCEPT  17  --  *      enp0s3 0.0.0.0/0      0.0.0.0/0
  0   0 ACCEPT  6   --  *      enp0s3 0.0.0.0/0      0.0.0.0/0
  0   0 ACCEPT  6   --  *      enp0s3 0.0.0.0/0      0.0.0.0/0
root@Ubuntu-server-bastionado:~/scripts#
```

```
root@Ubuntu-server-bastionado:~/scripts# ping google.com
PING google.com (142.250.184.174) 56(84) bytes of data.
64 bytes from mad07s23-in-f14.1e100.net (142.250.184.174): icmp_seq=1 ttl=116 time=16.1 ms
64 bytes from mad07s23-in-f14.1e100.net (142.250.184.174): icmp_seq=2 ttl=116 time=16.1 ms
64 bytes from mad07s23-in-f14.1e100.net (142.250.184.174): icmp_seq=3 ttl=116 time=23.7 ms
^C
-- google.com ping statistics --
3 packets transmitted. 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 16.088/18.631/23.687/3.574 ms
root@Ubuntu-server-bastionado:~/scripts# wget marca.com
--2024-11-23 18:24:52-- http://marca.com/
Resolving marca.com (marca.com)... 34.147.120.111, 2001:67c:2294:1000::f199
Connecting to marca.com (marca.com)|34.147.120.111|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://marca.com/ [following]
--2024-11-23 18:24:52-- https://marca.com/
Connecting to marca.com (marca.com)|34.147.120.111|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.marca.com/ [following]
--2024-11-23 18:24:53-- https://www.marca.com/
Resolving www.marca.com (www.marca.com)... 151.101.133.50
Connecting to www.marca.com (www.marca.com)|151.101.133.50|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 817368 (798K) [text/html]
Saving to: 'index.html'

index.html                                              100%[=====] 798.21K  --.KB/s  in 0.07s

2024-11-23 18:24:53 (12.0 MB/s) - 'index.html' saved [817368/817368]

root@Ubuntu-server-bastionado:~/scripts# ntpdate time.inm.es
^C^C^C
```

Activar Windows
Ve a Configuración para activar Windows.

```
root@Ubuntu-server-bastionado:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 48 packets, 2720 bytes)
 pkts bytes target  prot opt in   out    source          destination
  30 2471 ACCEPT  0   --  lo   *      0.0.0.0/0      0.0.0.0/0
   0   0 ACCEPT  6   --  enp0s3 *      192.168.1.108  0.0.0.0/0
 179 11048 ACCEPT  6   --  enp0s3 *      0.0.0.0/0      0.0.0.0/0
 114  836K ACCEPT  0   --  enp0s3 *      0.0.0.0/0      0.0.0.0/0
   0   0 LOG    6   --  *      *      0.0.0.0/0      0.0.0.0/0
e-SSH Server-al"
   0   0 LOG    6   --  *      *      0.0.0.0/0      0.0.0.0/0
que-mysql-almello"
   0   0 LOG    6   --  *      *      0.0.0.0/0      0.0.0.0/0
e-Web-Server-al"
Chain FORWARD (policy DROP 0 packets, 0 bytes)
 pkts bytes target  prot opt in   out    source          destination
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target  prot opt in   out    source          destination
  30 2471 ACCEPT  0   --  *      lo   0.0.0.0/0      0.0.0.0/0
 208 18082 ACCEPT  0   --  *      enp0s3 0.0.0.0/0      0.0.0.0/0
  1   84 ACCEPT   1  --  *      enp0s3 0.0.0.0/0      0.0.0.0/0
 22 1497 ACCEPT   17 --  *      enp0s3 0.0.0.0/0      0.0.0.0/0
  1   60 ACCEPT   6  --  *      enp0s3 0.0.0.0/0      0.0.0.0/0
  2   120 ACCEPT  6  --  *      enp0s3 0.0.0.0/0      0.0.0.0/0
root@Ubuntu-server-bastionado:~/scripts#
```

Me debería aparecer paquetes DROP por el cambio de hora porque no me deja actualizarla , pero nose porque no aumenta el contador

Álvaro Almellones Fernández

e) Además, permite actualizar la hora del S.O., pero **exclusivamente** con un servidor por su IP (elija usted dos servidores horarios, uno de España y otro de fuera de España).

```
10.192.168.1.107 almellonesfernandez
GNU nano 7.2
IP_Confianza="192.168.1.108"
MAC_Confianza="38:FC:98:0F:99:7F"

echo "Iniciando cortafuegos de Host: Álvaro Almellones"

iptables -F #Borra reglas de filtrado.
iptables -X #Borra cadenas personalizadas.
iptables -Z #Reinicia contadores.

iptables -P INPUT DROP #Política por defecto DROP
iptables -P OUTPUT DROP #Política por defecto DROP
iptables -P FORWARD DROP #Política por defecto DROP

#Reglas de loopback

iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# Reglas de INPUT
iptables -A OUTPUT -o $tarjeta -m state --state ESTABLISHED,RELATED -j ACCEPT # Respuesta de los input que recibe el servidor
iptables -A INPUT -i $tarjeta -p tcp --dport 22 -s $IP_Confianza -j ACCEPT
iptables -A INPUT -i $tarjeta -p tcp --dport 22 -m mac --mac-source $MAC_Confianza -j ACCEPT

#Reglas de OUTPUT
iptables -A INPUT -i $tarjeta -m state --state ESTABLISHED,RELATED -j ACCEPT #Permite escuchar la respuesta de cuando hablo
iptables -A OUTPUT -o $tarjeta -p icmp -j ACCEPT
iptables -A OUTPUT -o $tarjeta -p udp --dport 53 -j ACCEPT
iptables -A OUTPUT -o $tarjeta -p tcp --dport 80 -j ACCEPT
iptables -A OUTPUT -o $tarjeta -p tcp --dport 443 -j ACCEPT
iptables -A OUTPUT -o $tarjeta -p udp -d 193.204.114.231 --dport 123 -j ACCEPT # Permitir la actualización de hora desde el servidor NTP de España
iptables -A OUTPUT -o $tarjeta -p udp -d 216.239.35.0 --dport 123 -j ACCEPT # Permitir la actualización de hora desde el servidor NTP internacional
```

```
10.192.168.1.107 (almellonesfernandez)
root@Ubuntu-server-bastionado:~/scripts$ nano almellonesfernandez-iptables.sh
root@Ubuntu-server-bastionado:~/scripts$ ./almellonesfernandez-iptables.sh
Iniciando cortafuegos de Host: Álvaro Almellones
root@Ubuntu-server-bastionado:~/scripts$ iptables -L -n -v
Chain INPUT (policy DROP 4 packets, 124 bytes)
pkts bytes target     prot opt in     out    source               destination
  0   0 ACCEPT      --   lo      *      0.0.0.0/0          0.0.0.0/0
  0   0 ACCEPT      6    enp0s3  *      192.168.1.108        0.0.0.0/0
121 7960 ACCEPT      6    enp0s3  *      0.0.0.0/0          0.0.0.0/0
  0   0 ACCEPT      6    enp0s3  *      0.0.0.0/0          0.0.0.0/0
  0   0 LOG         6    *      *      0.0.0.0/0          0.0.0.0/0
e-SSH Server-al"
  0   0 LOG         6    *      *      0.0.0.0/0          0.0.0.0/0
que-mysql-almello"
  0   0 LOG         6    *      *      0.0.0.0/0          0.0.0.0/0
e-Web-Server-al"
Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target     prot opt in     out    source               destination
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target     prot opt in     out    source               destination
  0   0 ACCEPT      0    --   *      lo      0.0.0.0/0          0.0.0.0/0
  0   0 ACCEPT      67  enp0s3  *      0.0.0.0/0          0.0.0.0/0
  0   0 ACCEPT      1    enp0s3  *      0.0.0.0/0          0.0.0.0/0
  0   0 ACCEPT      17   enp0s3  *      0.0.0.0/0          0.0.0.0/0
  0   0 ACCEPT      6    enp0s3  *      0.0.0.0/0          0.0.0.0/0
  0   0 ACCEPT      6    enp0s3  *      0.0.0.0/0          0.0.0.0/0
  0   0 ACCEPT      17   enp0s3  *      0.0.0.0/0          193.204.114.231
  0   0 ACCEPT      17   enp0s3  *      0.0.0.0/0          216.239.35.0
```

```
10.192.168.1.107 (almellonesfernandez)
root@Ubuntu-server-bastionado:~/scripts$ ping google.com
PING google.com (142.250.200.142) 56(84) bytes of data.
64 bytes from mad41s14-in-f14.1e100.net (142.250.200.142): icmp_seq=1 ttl=116 time=16.6 ms
64 bytes from mad41s14-in-f14.1e100.net (142.250.200.142): icmp_seq=2 ttl=116 time=16.9 ms
64 bytes from mad41s14-in-f14.1e100.net (142.250.200.142): icmp_seq=3 ttl=116 time=17.2 ms
^C
--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 16.634/16.895/17.155/0.212 ms
root@Ubuntu-server-bastionado:~/scripts$ wget marca.com
--2024-11-23 19:01:36-- http://marca.com/
Resolving marca.com (marca.com)... 34.147.120.111, 2001:67c:2294:1000::f199
Connecting to marca.com (marca.com)|34.147.120.111|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://marca.com/ [following]
--2024-11-23 19:01:36-- https://marca.com/
Connecting to marca.com (marca.com)|34.147.120.111|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.marca.com/ [following]
--2024-11-23 19:01:37-- https://www.marca.com/
Resolving www.marca.com (www.marca.com)... 151.101.133.50
Connecting to www.marca.com (www.marca.com)|151.101.133.50|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 826595 (807K) [text/html]
Saving to: 'index.html.1'

index.html.1          100%[=====] 807.22K --.-KB/s   in 0.07s

2024-11-23 19:01:37 (12.1 MB/s) - 'index.html.1' saved [826595/826595]

root@Ubuntu-server-bastionado:~/scripts$ ntpdate 193.204.114.231
2024-11-23 19:02:25.919440 (+0100) +0.005116 +/- 0.027739 193.204.114.231 s1 no-leap
root@Ubuntu-server-bastionado:~/scripts$ ntpdate 216.239.35.0
2024-11-23 19:02:49.305548 (+0100) -0.001008 +/- 0.017764 216.239.35.0 s1 no-leap
root@Ubuntu-server-bastionado:~/scripts#
```

Activar Windows
Ve a Configuración para activar Windows.

Álvaro Almellones Fernández

```
root@Ubuntu-server-bastionado:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 53 packets, 1970 bytes)
pkts bytes target     prot opt in     out    source          destination
  30  3052 ACCEPT      0 --   lo      *       0.0.0.0/0      0.0.0.0/0
    0     0 ACCEPT      6 --   enp0s3  *       192.168.1.108  0.0.0.0/0
  634 41440 ACCEPT     6 --   enp0s3  *       0.0.0.0/0      0.0.0.0/0
 111  846K ACCEPT     0 --   enp0s3  *       0.0.0.0/0      0.0.0.0/0
    0     0 LOG        6 --   *      *       0.0.0.0/0      0.0.0.0/0
-al"
    0     0 LOG        6 --   *      *       0.0.0.0/0      0.0.0.0/0
mello"
    0     0 LOG        6 --   *      *       0.0.0.0/0      0.0.0.0/0
-al"
Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target     prot opt in     out    source          destination

Chain OUTPUT (policy DROP 17 packets, 1292 bytes)
pkts bytes target     prot opt in     out    source          destination
  30  3052 ACCEPT      0 --   *      lo      0.0.0.0/0      0.0.0.0/0
 450 40394 ACCEPT     0 --   *      enp0s3  0.0.0.0/0      0.0.0.0/0
  1     84 ACCEPT      1 --   *      enp0s3  0.0.0.0/0      0.0.0.0/0
 16  1202 ACCEPT     17 --   *      enp0s3  0.0.0.0/0      0.0.0.0/0
  1     60 ACCEPT      6 --   *      enp0s3  0.0.0.0/0      0.0.0.0/0
  2     120 ACCEPT     6 --   *      enp0s3  0.0.0.0/0      0.0.0.0/0
  1     76 ACCEPT     17 --   *      enp0s3  0.0.0.0/0      193.204.114.231
  1     76 ACCEPT     17 --   *      enp0s3  0.0.0.0/0      216.239.35.0
root@Ubuntu-server-bastionado:~/scripts#
```

f) Además, permita enviar correos salientes con el comando mailx o el que desee.

```
root@Ubuntu-server-bastionado:~/scripts# nano almellonesfernandez-iptables.sh
root@Ubuntu-server-bastionado:~/scripts# ./almellonesfernandez-iptables.sh
Iniciando cortafuegos de Host: Álvaro Almellones
root@Ubuntu-server-bastionado:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 1 packets, 40 bytes)
pkts bytes target     prot opt in     out    source          destination
    0     0 ACCEPT      0 --   lo      *       0.0.0.0/0      0.0.0.0/0
    0     0 ACCEPT      6 --   enp0s3  *       192.168.1.108  0.0.0.0/0
  36 2304 ACCEPT     6 --   enp0s3  *       0.0.0.0/0      0.0.0.0/0
    0     0 ACCEPT      0 --   enp0s3  *       0.0.0.0/0      0.0.0.0/0
    0     0 LOG        6 --   *      *       0.0.0.0/0      0.0.0.0/0
-al"
    0     0 LOG        6 --   *      *       0.0.0.0/0      0.0.0.0/0
mello"
    0     0 LOG        6 --   *      *       0.0.0.0/0      0.0.0.0/0
-al"
Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target     prot opt in     out    source          destination

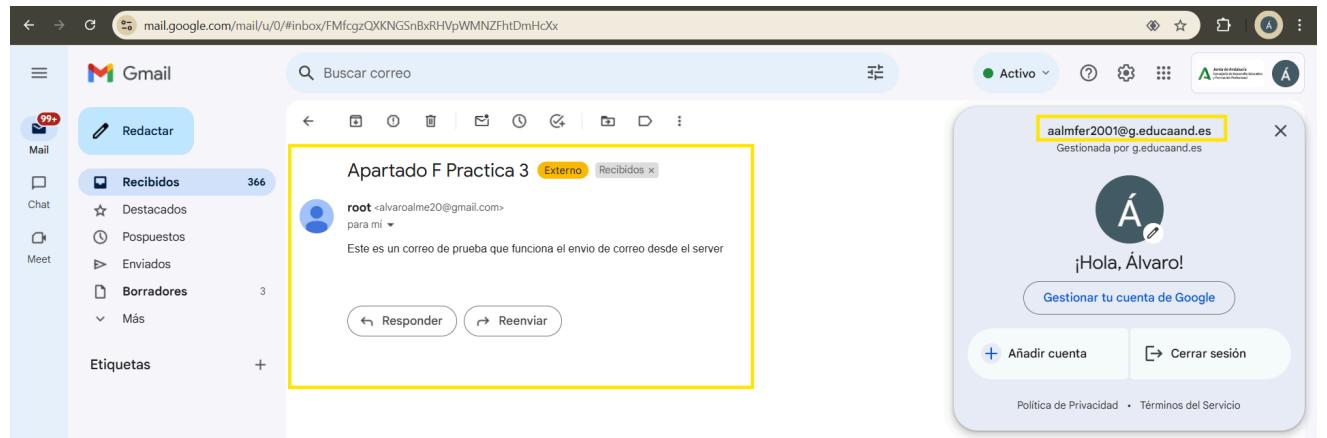
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target     prot opt in     out    source          destination
    0     0 ACCEPT      0 --   *      lo      0.0.0.0/0      0.0.0.0/0
  20 1888 ACCEPT     0 --   *      enp0s3  0.0.0.0/0      0.0.0.0/0
  0     0 ACCEPT      1 --   *      enp0s3  0.0.0.0/0      0.0.0.0/0
  0     0 ACCEPT     17 --   *      enp0s3  0.0.0.0/0      0.0.0.0/0
  0     0 ACCEPT      6 --   *      enp0s3  0.0.0.0/0      0.0.0.0/0
  0     0 ACCEPT     17 --   *      enp0s3  0.0.0.0/0      193.204.114.231
  0     0 ACCEPT     17 --   *      enp0s3  0.0.0.0/0      216.239.35.0
  0     0 ACCEPT      6 --   *      enp0s3  0.0.0.0/0      0.0.0.0/0
root@Ubuntu-server-bastionado:~/scripts#
```

```
root@Ubuntu-server-bastionado:~/scripts# ping google.com
PING google.com (142.250.201.78) 56(84) bytes of data.
64 bytes from mad07s25-in-f14.1e100.net (142.250.201.78): icmp_seq=1 ttl=116 time=45.7 ms
```
-- google.com ping statistics --
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 45.718/45.718/45.718/0.000 ms
root@Ubuntu-server-bastionado:~/scripts# wget marca.com
--2024-11-23 19:23:11-- http://marca.com/
Resolving marca.com (marca.com)... 34.147.120.111, 2001:67c:2294:1000::f199
Connecting to marca.com (marca.com)|34.147.120.111|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://marca.com/ [following]
--2024-11-23 19:23:11-- https://marca.com/
Connecting to marca.com (marca.com)|34.147.120.111|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.marca.com/ [following]
--2024-11-23 19:23:11-- https://www.marca.com/
Resolving www.marca.com (www.marca.com)... 151.101.133.50
Connecting to www.marca.com (www.marca.com)|151.101.133.50|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 822425 (803K) [text/html]
Saving to: 'index.html.3'

index.html.3 100%[=====] 803.15K --.-KB/s in 0.07s
2024-11-23 19:23:12 (11.9 MB/s) - 'index.html.3' saved [822425/822425]

root@Ubuntu-server-bastionado:~/scripts# ntpdate 193.204.114.231
2024-11-23 19:23:15.375855 (+0100) +0.012609 +/- 0.022798 193.204.114.231 s1 no-leap
root@Ubuntu-server-bastionado:~/scripts# ntpdate 216.239.35.0
2024-11-23 19:23:18.107281 (+0100) +0.02528 +/- 0.020516 216.239.35.0 s1 no-leap
root@Ubuntu-server-bastionado:~/scripts# echo "Este es un correo de prueba que funciona el envío de correo desde el server Álvaro Almellones Fernández" | mailx -s "Práctica 3" aalmfer2001@g.eduand.es
root@Ubuntu-server-bastionado:~/scripts#
```

# Álvaro Almellones Fernández



Este es un correo de prueba que funciona el envío de correo desde el server

[Responder](#) [Reenviar](#)

aalmfer2001@g.educaand.es  
Gestionada por g.educaand.es

¡Hola, Álvaro!

[Gestionar tu cuenta de Google](#)

[Añadir cuenta](#) [Cerrar sesión](#)

Política de Privacidad • Términos del Servicio

```
root@Ubuntu-server-bastionado:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 42 packets, 1324 bytes)
pkts bytes target prot opt in out source destination
 32 2822 ACCEPT 0 -- lo * 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 6 -- enp0s3 * 192.168.1.108 0.0.0.0/0
 701 45720 ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
 226 1688K ACCEPT 0 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
-al"
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
mello"
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
-al"
root@Ubuntu-server-bastionado:~/scripts#
```

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

```
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
 32 2822 ACCEPT 0 -- * lo 0.0.0.0/0 0.0.0.0/0
624 55050 ACCEPT 0 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 2 168 ACCEPT 1 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
13 946 ACCEPT 17 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 2 120 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 4 240 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 2 152 ACCEPT 17 -- * enp0s3 0.0.0.0/0 193.204.114.231
 2 152 ACCEPT 17 -- * enp0s3 0.0.0.0/0 216.239.35.0
 1 60 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
root@Ubuntu-server-bastionado:~/scripts#
```

\*\*\*\* Haga un backup de este script final (Xxxx-iptables-v2.0.sh). Muestre, aunque no se valorará. \*\*\*\* Haga un nuevo snapshot para tener guardo este nuevo estado. Muestre, aunque no se valorará.

## Álvaro Almellones Fernández

4. (REGLAS DE FILTRADO INPUT) Continuando con el script anterior y que las **respuestas (OUTPUT)** a las conexiones entrantes tienan que ser **exclusivamente** para conexiones establecidas o relacionadas. Se **recomienda** que se prepare un script para Linux (XXxx-cliente.sh) para ejecutar la prueba completa de servicios para conexiones OUTPUT. Demostrar paso a paso.

a) Que se puede realizar ping a este servidor. (0,5 puntos).

```
192.168.1.107 (almellonesfernandez)
Terminal Sessions View Xserver Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
10. 192.168.1.107 (almellonesfernandez)

GNU nano 7.2 almellonesfernandez-iptables.sh
#!/bin/bash

Variables
tarjeta="enp0s3"
IP_Confianza="192.168.1.108"
MAC_Confianza="38:FC:98:0F:99:7F"

echo "Iniciandose cortafuegos de Host: Alvaro Almellones"

iptables -F #Borra reglas de filtrado.
iptables -X #Borra cadenas personalizadas.
iptables -Z #Reinicia contadores.

iptables -P INPUT DROP #Politica por defecto DROP
iptables -P OUTPUT DROP #Politica por defecto DROP
iptables -P FORWARD DROP #Politica por defecto DROP

#Reglas de loopback

iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

Reglas de INPUT
iptables -A OUTPUT -o $tarjeta -m state --state ESTABLISHED,RELATED -j ACCEPT # Respuesta de los inp
iptables -A INPUT -i $tarjeta -p tcp --dport 22 -s $IP_Confianza -j ACCEPT
iptables -A INPUT -i $tarjeta -p tcp --dport 22 -m mac --mac-source $MAC_Confianza -j ACCEPT
iptables -A INPUT -i $tarjeta -p icmp -j ACCEPT
```

```
Ubuntu_desktop_bastionado (Recién instalado SO) [Corriendo] - Or... Archivo Máquina Ver Entrada Dispositivos Ayuda
23 de Nov 192.168.1.107 (almellonesfernandez)
Terminal Sessions View Xserver Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
10. 192.168.1.107 (almellonesfernandez)

Every 2.0s: iptables -L -n -v Ubuntu-server-bastionado: Sat Nov 23 20:45:11 UTC 2019

Chain INPUT (policy DROP 4 packets, 128 bytes)
pkts bytes target prot opt in out source destination
 0 0 ACCEPT 0 -- lo * 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 0 -- enp0s3 * 192.168.1.108 0.0.0.0/0
 106 7280 ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
 9:7f 0 0 ACCEPT 1 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 0 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
 4 prefix "Intentos-ataque-SSH Server-al"
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
 el 4 prefix "Intentos-ataque-mysql-almello"
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
 4 prefix "Intentos-ataque-Web-Server-al"
Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
 0 0 ACCEPT 0 -- * lo 0.0.0.0/0 0.0.0.0/0
 75 7384 ACCEPT 0 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 1 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 17 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 17 -- * enp0s3 0.0.0.0/0 193.204.114.231
 0 0 ACCEPT 17 -- * enp0s3 0.0.0.0/0 216.239.35.0
 0 0 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
```

Álvaro Almellones Fernández

The screenshot shows two terminal windows side-by-side. The left window is on a 'Ubuntu\_desktop\_bastionado' host (IP 192.168.1.109) and displays a ping command to 192.168.1.110, showing various ICMP sequence numbers and times. The right window is on a 'Ubuntu-server-bastionado' host (IP 192.168.1.107) and shows the output of the command 'Every 2.0s: iptables -L -n -v'. It lists several chains: INPUT, FORWARD, and OUTPUT. The INPUT chain includes rules for ICMP (accepting seq 1-10, dropping seq 11-18), TCP (accepting seq 1-10, dropping seq 11-18), and state RELAT (accepting seq 1-10). The FORWARD chain has one rule for state RELATED (accepting seq 1-10). The OUTPUT chain has one rule for state RELATED (accepting seq 1-10).

```
almelonesfernandez@almelonesfernandez-VirtualBox:~$ ping 192.168.1.110
PING 192.168.1.110 (192.168.1.110) 56(84) bytes of data.
64 bytes from 192.168.1.110: icmp_seq=1 ttl=64 time=0.766 ms
64 bytes from 192.168.1.110: icmp_seq=2 ttl=64 time=0.04 ms
64 bytes from 192.168.1.110: icmp_seq=3 ttl=64 time=0.945 ms
64 bytes from 192.168.1.110: icmp_seq=4 ttl=64 time=1.02 ms
64 bytes from 192.168.1.110: icmp_seq=5 ttl=64 time=1.33 ms
64 bytes from 192.168.1.110: icmp_seq=6 ttl=64 time=1.12 ms
64 bytes from 192.168.1.110: icmp_seq=7 ttl=64 time=0.852 ms
64 bytes from 192.168.1.110: icmp_seq=8 ttl=64 time=1.02 ms
64 bytes from 192.168.1.110: icmp_seq=9 ttl=64 time=1.18 ms
64 bytes from 192.168.1.110: icmp_seq=10 ttl=64 time=0.807 ms
64 bytes from 192.168.1.110: icmp_seq=11 ttl=64 time=1.33 ms
64 bytes from 192.168.1.110: icmp_seq=12 ttl=64 time=1.19 ms
64 bytes from 192.168.1.110: icmp_seq=13 ttl=64 time=2.66 ms
64 bytes from 192.168.1.110: icmp_seq=14 ttl=64 time=3.96 ms
^C
... 192.168.1.110 ping statistics ...
14 packets transmitted, 14 received 0% packet loss, time 1387ms
rtt min/avg/max/mdev = 0.766/1.371/3.955/0.843 ms
almelonesfernandez@almelonesfernandez-VirtualBox:~$
```

192.168.1.107 (almelonesfernandez)

Terminal Sessions View Xserver Tools Games Settings Macros Help

Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help

Every 2.0s: iptables -L -n -v

| Chain                                           | policy | pkts | bytes                                  | target | prot | opt | in     | out    | source        | destination     |
|-------------------------------------------------|--------|------|----------------------------------------|--------|------|-----|--------|--------|---------------|-----------------|
| Chain INPUT (policy DROP 11 packets, 352 bytes) | DROP   | 11   | 352                                    |        |      |     |        |        |               |                 |
|                                                 |        | pkts | bytes                                  | target | prot | opt | in     | out    | source        | destination     |
|                                                 |        | 0    | 0                                      | ACCEPT | 0    | --  | lo     | *      | 0.0.0.0/0     | 0.0.0.0/0       |
|                                                 |        | 0    | 0                                      | ACCEPT | 6    | --  | enp0s3 | *      | 192.168.1.108 | 0.0.0.0/0       |
|                                                 |        | 140  | 8640                                   | ACCEPT | 6    | --  | enp0s3 | *      | 0.0.0.0/0     | 0.0.0.0/0       |
| 9:7:f                                           |        | 15   | 1204                                   | ACCEPT | 1    | --  | enp0s3 | *      | 0.0.0.0/0     | 0.0.0.0/0       |
|                                                 |        | 0    | 0                                      | ACCEPT | 0    | --  | enp0s3 | *      | 0.0.0.0/0     | 0.0.0.0/0       |
|                                                 |        | 0    | 0                                      | LOG    | 6    | --  | *      | *      | 0.0.0.0/0     | 0.0.0.0/0       |
|                                                 |        | 4    | prefix "Intentos-ataque-SSH Server-al" |        |      |     |        |        |               |                 |
|                                                 |        | 0    | 0                                      | LOG    | 6    | --  | *      | *      | 0.0.0.0/0     | 0.0.0.0/0       |
|                                                 |        | el 4 | prefix "Intentos-ataque-mysql-almello" |        |      |     |        |        |               |                 |
|                                                 |        | 0    | 0                                      | LOG    | 6    | --  | *      | *      | 0.0.0.0/0     | 0.0.0.0/0       |
|                                                 |        | 4    | prefix "Intentos-ataque-Web-Server-al" |        |      |     |        |        |               |                 |
| Chain FORWARD (policy DROP 0 packets, 0 bytes)  | DROP   | 0    | 0                                      |        |      |     |        |        |               |                 |
|                                                 |        | pkts | bytes                                  | target | prot | opt | in     | out    | source        | destination     |
| Chain OUTPUT (policy DROP 0 packets, 0 bytes)   | DROP   | 0    | 0                                      |        |      |     |        |        |               |                 |
|                                                 |        | pkts | bytes                                  | target | prot | opt | in     | out    | source        | destination     |
|                                                 |        | 0    | 0                                      | ACCEPT | 0    | --  | *      | lo     | 0.0.0.0/0     | 0.0.0.0/0       |
|                                                 |        | 130  | 12892                                  | ACCEPT | 0    | --  | *      | enp0s3 | 0.0.0.0/0     | 0.0.0.0/0       |
|                                                 |        | 0    | 0                                      | ACCEPT | 1    | --  | *      | enp0s3 | 0.0.0.0/0     | 0.0.0.0/0       |
|                                                 |        | 0    | 0                                      | ACCEPT | 17   | --  | *      | enp0s3 | 0.0.0.0/0     | 0.0.0.0/0       |
|                                                 |        | 0    | 0                                      | ACCEPT | 6    | --  | *      | enp0s3 | 0.0.0.0/0     | 0.0.0.0/0       |
|                                                 |        | 0    | 0                                      | ACCEPT | 6    | --  | *      | enp0s3 | 0.0.0.0/0     | 0.0.0.0/0       |
|                                                 |        | 0    | 0                                      | ACCEPT | 17   | --  | *      | enp0s3 | 0.0.0.0/0     | 193.204.114.231 |
|                                                 |        | 0    | 0                                      | ACCEPT | 17   | --  | *      | enp0s3 | 0.0.0.0/0     | 216.239.35.0    |
|                                                 |        | 0    | 0                                      | ACCEPT | 6    | --  | *      | enp0s3 | 0.0.0.0/0     | 0.0.0.0/0       |

- b) Demostrar que se permite la conexión al servidor SSHD (no web ni vsftpd, ni mysql, ni apache), pero de la siguiente manera (cada apartado se demuestra por separado)

i. Desde la IP concreta de un determinado cliente.

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal title is '192.168.1.107 (almellonesfernandez)'. The window contains a script named 'almellonesfernandez.sh' which configures iptables rules. Several lines of the script are highlighted with yellow boxes, specifically: 'IP\_Confianza="192.168.1.108"', 'MAC\_Confianza="38:FC:98:0F:99:7F"', and the entire section under '# Reglas de INPUT'.

```
192.168.1.107 (almellonesfernandez)
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Qt 10. 192.168.1.107 (almellonesfernandez)
GNU nano 7.2 almellonesfernandez-iptables.sh
#!/bin/bash

Variables
tarjeta="enp0s3"
IP_Confianza="192.168.1.108"
MAC_Confianza="38:FC:98:0F:99:7F"

echo "Iniciandose cortafuegos de Host: Alvaro Almellones"

iptables -F #Borra reglas de filtrado.
iptables -X #Borra cadenas personalizadas.
iptables -Z #Reinicia contadores.

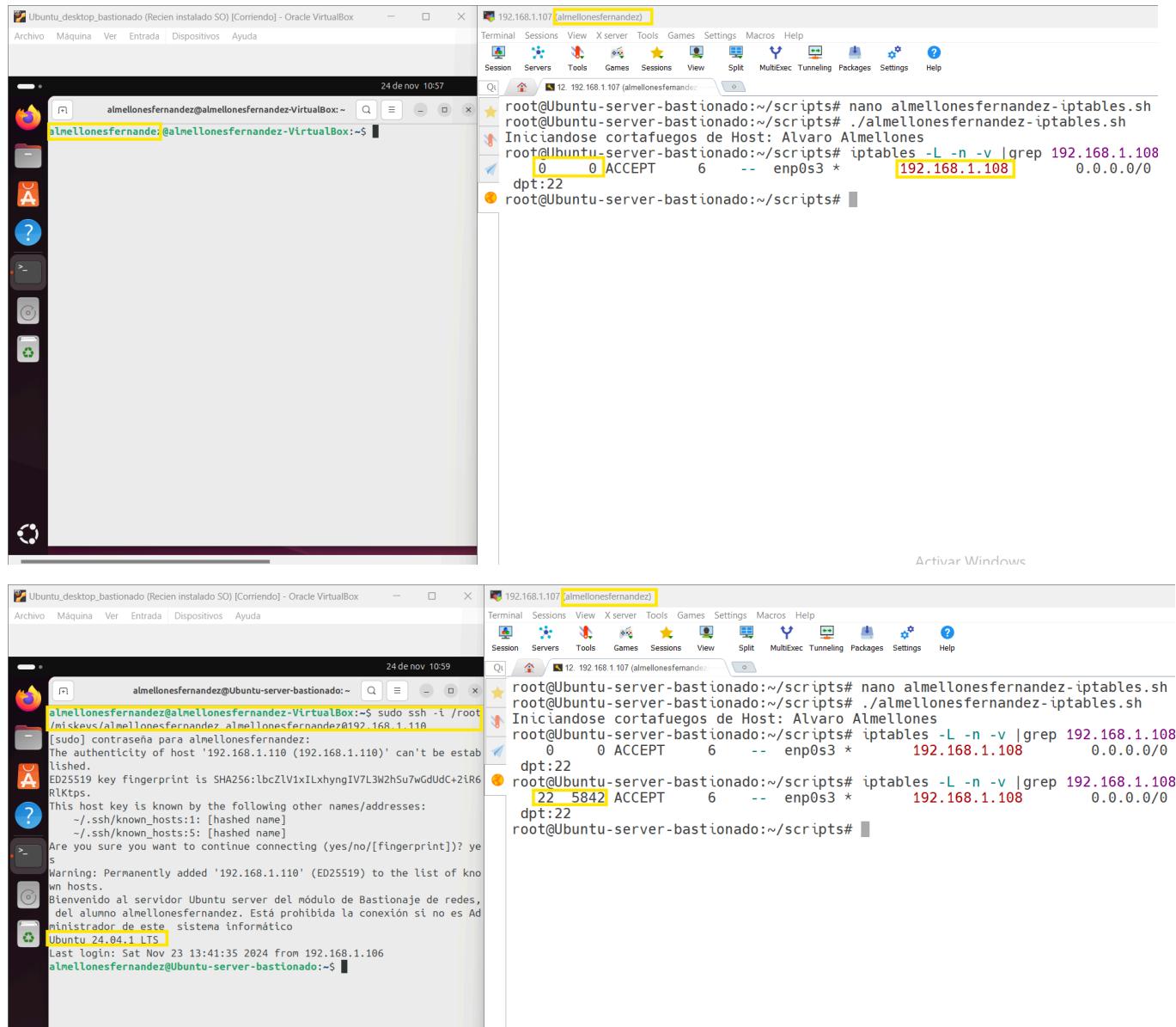
iptables -P INPUT DROP #Politica por defecto DROP
iptables -P OUTPUT DROP #Politica por defecto DROP
iptables -P FORWARD DROP #Politica por defecto DROP

#Reglas de loopback

iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

Reglas de INPUT
iptables -A OUTPUT -o $tarjeta -m state --state ESTABLISHED,RELATED -j ACCEPT # Respuesta de
iptables -A INPUT -i $tarjeta -p tcp --dport 22 -s $IP_Confianza -j ACCEPT
iptables -A INPUT -i $tarjeta -p tcp --dport 22 -m mac --mac-source $MAC_Confianza -j ACCEPT
iptables -A INPUT -i $tarjeta -p icmp -j ACCEPT
```

## Álvaro Almellones Fernández



ii. Lo mismo que el anterior, pero que además se permita sólo 3 conexiones de esa IP. (0,5 puntos)

```
GNU nano 7.2 almellonesfernandez-iptables.sh
#!/bin/bash

Variables
tarjeta="enp0s3"
IP_Confianza="192.168.1.108"
MAC_Confianza="38:FC:98:0F:99:7F"

echo "Iniciandose cortafuegos de Host: Alvaro Almellones"

iptables -F #Borra reglas de filtrado.
iptables -X #Borra cadenas personalizadas.
iptables -Z #Reinicia contadores.

iptables -P INPUT DROP #Politica por defecto DROP
iptables -P OUTPUT DROP #Politica por defecto DROP
iptables -P FORWARD DROP #Politica por defecto DROP

#Reglas de loopback
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

Reglas de INPUT
iptables -A INPUT -o $tarjeta -m state --state ESTABLISHED,RELATED -j ACCEPT # Respuesta de los input que recibe el servidor
iptables -A INPUT -i $tarjeta -p tcp --dport 22 -s $IP_Confianza -m connlimit --connlimit-above 3 -j DROP
iptables -A INPUT -i $tarjeta -p tcp --dport 22 -s $IP_Confianza -j ACCEPT
iptables -A INPUT -i $tarjeta -p tcp --dport 22 -m mac --mac-source $MAC_Confianza -j ACCEPT
iptables -A INPUT -i $tarjeta -p icmp -j ACCEPT
```

## Álvaro Almellones Fernández

```
Iniciando cortafuegos de Host: Álvaro Almellones
root@Ubuntu-server-bastionado:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 1 packets, 32 bytes)
pkts bytes target prot opt in out source destination
 0 0 ACCEPT 0 -- lo * 0.0.0.0/0 0.0.0.0/0
 0 0 DROP 6 -- enp0s3 * 192.168.1.108 0.0.0.0/0
 0 0 ACCEPT 6 -- enp0s3 * 192.168.1.108 0.0.0.0/0
113 7688 ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 1 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 0 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
ntos-ataque-SSH Server-al"
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
tentos-ataque-mysql-almello"
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
ntos-ataque-Web-Server-al"
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
 0 0 ACCEPT 0 -- * lo 0.0.0.0/0 0.0.0.0/0
 68 6208 ACCEPT 0 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 1 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 17 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 17 -- * enp0s3 0.0.0.0/0 193.204.114.231
 0 0 ACCEPT 17 -- * enp0s3 0.0.0.0/0 216.239.35.0
 0 0 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
Activar Windows
Ve a Configuración para activar Windows.
root@Ubuntu-server-bastionado:~/scripts#
```

```
24 de nov 11:18
almellonesfernandez@Ubuntu-server-bastionado:~
```

```
almellonesfernandez@albellonesfernandez-VirtualBox:~/Escritorio$ sudo ssh -i /root/miskeys/almellonesfernandez almellone
sfernandez@192.168.1.110
[sudo] contrasena para almellonesfernandez:
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almellonesfernandez. Está prohibida l
a conexión si no es Administrador de este sistema informático
Ubuntu 24.04.1 LTS
Last login: Sun Nov 24 11:09:05 2024 from 192.168.1.108
almellonesfernandez@Ubuntu-server-bastionado:~$
```

```
almellonesfernandez@albellonesfernandez-VirtualBox:~/Escritorio$ sudo ssh -i /root/miskeys/almellonesfernandez almellone
sfernandez@192.168.1.110
[sudo] contrasena para almellonesfernandez:
```

En las tres terminales señaladas la conexión se realiza , pero en la de abajo que se muestra en pantalla no accede ya que supera el límite de 3

Álvaro Almellones Fernández

```

root@Ubuntu-server-bastionado:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 32 packets, 1024 bytes)
pkts bytes target prot opt in out source destination
 0 0 ACCEPT 0 -- lo * 0.0.0.0/0 0.0.0.0/0
 11 660 DROP 6 -- enp0s3 * 192.168.1.108 0.0.0.0/0 tcp dpt:22 #conn src/32 > 3
 60 17302 ACCEPT 6 -- enp0s3 * 192.168.1.108 0.0.0.0/0 tcp dpt:22
135 9000 ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22 MAC 38:fc:98:0f:99:7f
 2 56 ACCEPT 1 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 0 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:22 LOG flags 0 level 4 prefix "Inte
ntos-ataque-SSH Server-al"
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:3306 LOG flags 0 level 4 prefix "In
tentos-ataque-mysql-almello"
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:80 LOG flags 0 level 4 prefix "Inte
ntos-ataque-Web-Server-al"

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

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
 0 0 ACCEPT 0 -- * lo 0.0.0.0/0 0.0.0.0/0
 146 26346 ACCEPT 0 -- * enp0s3 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
 0 0 ACCEPT 1 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 17 -- * enp0s3 0.0.0.0/0 0.0.0.0/0 udp dpt:53
 0 0 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0 tcp dpt:80
 0 0 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0 tcp dpt:443
 0 0 ACCEPT 17 -- * enp0s3 0.0.0.0/0 193.204.114.231 udp dpt:123
 0 0 ACCEPT 17 -- * enp0s3 0.0.0.0/0 216.239.35.0 udp dpt:123
 0 0 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0 tcp dpt:25

```

Podemos observar que ha aumentado los contadores de la regla accept ya que nos hemos conectado con las tres terminales desde la ip de confianza y a su vez la regla drop también ha aumentado ya que la cuarta conexión se ha intentado pero se rechaza

iii. Desde la MAC concreta de un determinado cliente. **(0,5 puntos)**

```
12.192.168.1.10 (almellonesfernande...)
GNU nano 7.2 almellonesfernandez-iptables.sh

Variables
tarjeta="enp0s3"
IP_Confianza="192.168.1.108"
MAC_Confianza="38:FC:98:0F:99:7F"

echo "Iniciandose cortafuegos de Host: Alvaro Almellones"

iptables -F #Borra reglas de filtrado.
iptables -X #Borra cadenas personalizadas.
iptables -Z #Reinicia contadores.

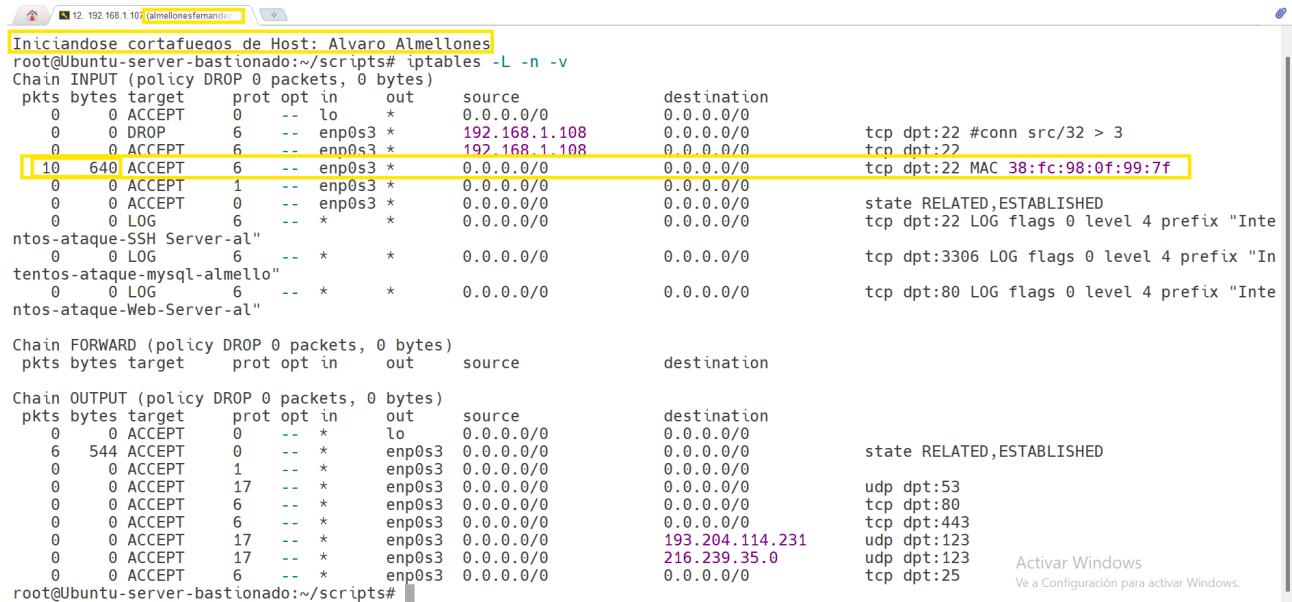
iptables -P INPUT DROP #Politica por defecto DROP
iptables -P OUTPUT DROP #Politica por defecto DROP
iptables -P FORWARD DROP #Politica por defecto DROP

#Reglas de loopback
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

Reglas de INPUT
iptables -A INPUT -o $tarjeta -m state --state ESTABLISHED,RELATED -j ACCEPT # Respuesta de los input que recibe el servidor
iptables -A INPUT -i $tarjeta -p tcp --dport 22 -s $IP_Confianza -m connlimit --connlimit-above 3 -j DROP
iptables -A INPUT -i $tarjeta -p tcp --dport 22 -s $IP_Confianza -i ACCEPT
iptables -A INPUT -i $tarjeta -p tcp --dport 22 -m mac --mac-source $MAC_Confianza -j ACCEPT
iptables -A INPUT -i $tarjeta -p icmp -j ACCEPT
```

**He estado usando esta regla durante toda la practica para poder realizar las capturas desde el Moba**

## Álvaro Almellones Fernández



```
Iniciandose cortafuegos de Host: Alvaro Almellones
root@Ubuntu-server-bastionado:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
 0 0 ACCEPT 0 -- lo * 0.0.0.0/0 0.0.0.0/0
 0 0 DROP 6 -- enp0s3 * 192.168.1.108 0.0.0.0/0
 0 0 ACCEPT 6 -- enp0s3 * 192.168.1.108 0.0.0.0/0
[10 640 ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 1 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 0 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
ntos-ataque-SSH Server-al"
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
tentos-ataque-mysql-almello"
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
ntos-ataque-Web-Server-al"
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
 0 0 ACCEPT 0 -- * lo 0.0.0.0/0 0.0.0.0/0
 6 544 ACCEPT 0 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 1 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 17 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 17 -- * enp0s3 0.0.0.0/0 193.204.114.231
 0 0 ACCEPT 17 -- * enp0s3 0.0.0.0/0 216.239.35.0
 0 0 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
Activar Windows
Ve a Configuración para activar Windows.
root@Ubuntu-server-bastionado:~/scripts#
```

## Al estar usando Moba estar aumentando los contadores

iv. Desde la red concreta en la que se encuentra Ubuntu Server. (0,5 puntos)

Para comprobar este apartado voy a comentar la regla de MAC anterior y asegurar que me deja acceder íntegramente solo por la red concreta



```
GNU nano 7.2 almellonesfernandez-iptables.sh
Variables
tarjeta="enp0s3"
IP_Confianza="192.168.1.108"
MAC_Confianza="38:FC:98:0F:99:7F"

echo "Iniciandose cortafuegos de Host: Alvaro Almellones"

iptables -F #Borra reglas de filtrado.
iptables -X #Borra cadenas personalizadas.
iptables -Z #Reinicia contadores.

iptables -P INPUT DROP #Politica por defecto DROP
iptables -P OUTPUT DROP #Politica por defecto DROP
iptables -P FORWARD DROP #Politica por defecto DROP

#Reglas de loopback
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

Reglas de INPUT
iptables -A OUTPUT -o $tarjeta -m state --state ESTABLISHED,RELATED -j ACCEPT # Respuesta de los input que recibe el servidor
iptables -A INPUT -i $tarjeta -p tcp --dport 22 -s $IP_Confianza -m connlimit --connlimit-above 3 -j DROP
iptables -A INPUT -i $tarjeta -p tcp --dport 22 -s $IP_Confianza -j ACCEPT
iptables -A INPUT -i $tarjeta -p tcp --dport 22 -s 192.168.1.0/24 -j ACCEPT
#iptables -A INPUT -i $tarjeta -p tcp --dport 22 -m mac --mac-source $MAC_Confianza -j ACCEPT
iptables -A INPUT -i $tarjeta -p icmp -j ACCEPT
```

## Álvaro Almellones Fernández

```
root@Ubuntu-server-bastionado:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 1 packets, 40 bytes)
pkts bytes target prot opt in out source destination
 0 0 ACCEPT 0 -- lo * 0.0.0.0/0 0.0.0.0/0
 0 0 DROP 6 -- enp0s3 * 192.168.1.108 0.0.0.0/0
 0 0 ACCEPT 6 -- enp0s3 * 192.168.1.108 0.0.0.0/0
16 1024 ACCEPT 6 -- enp0s3 * 192.168.1.0/24 0.0.0.0/0
 0 0 ACCEPT 1 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 0 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
ntos-ataque-SSH Server-al"
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
tentos-ataque-mysql-almello"
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
ntos-ataque-Web-Server-al"
Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
 0 0 ACCEPT 0 -- * lo 0.0.0.0/0 0.0.0.0/0
 9 808 ACCEPT 0 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 1 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 17 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 17 -- * enp0s3 0.0.0.0/0 193.204.114.231
 0 0 ACCEPT 17 -- * enp0s3 0.0.0.0/0 216.239.35.0
 0 0 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
root@Ubuntu-server-bastionado:~/scripts#
```

Igual que en el apartado anterior , al estar conectado desde moba el contador aumenta, pero al comentar la regla de MAC sabemos que se accede por la red concreta

v. A unas determinada fecha y hora del día (inventarse dicho horario). (0,5 puntos)

Voy a realizar este apartado con la ip de ubuntu Desktop para poder sacar las capturas con fondo blanco

```
root@Ubuntu-server-bastionado:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 2 packets, 72 bytes)
pkts bytes target prot opt in out source destination
 0 0 ACCEPT 0 -- lo * 0.0.0.0/0 0.0.0.0/0
 0 0 DROP 6 -- enp0s3 * 192.168.1.108 0.0.0.0/0
 0 0 ACCEPT 6 -- enp0s3 * 192.168.1.108 0.0.0.0/0
 starting from 2024-11-25 00:00:00 until date 2024-11-25 23:59:00 UTC
62 3968 ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 0 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
ntos-ataque-SSH Server-al"
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
tentos-ataque-mysql-almello"
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
ntos-ataque-Web-Server-al"
Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
 0 0 ACCEPT 0 -- * lo 0.0.0.0/0 0.0.0.0/0
 34 3184 ACCEPT 0 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 1 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 17 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 17 -- * enp0s3 0.0.0.0/0 193.204.114.231
 0 0 ACCEPT 17 -- * enp0s3 0.0.0.0/0 216.239.35.0
 0 0 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
root@Ubuntu-server-bastionado:~/scripts#
```

```
24 nov 12:31
[+]
al mellonesfernandez@almellonesfernandez-VirtualBox:~/Escritorio
al mellonesfernandez@almellonesfernandez-VirtualBox:~/Escritorio$ sudo ssh -i /root/miskeys/almellonesfernandez almellone
sfernandez@192.168.1.110
ssh: connect to host 192.168.1.110 port 22: Connection timed out
al mellonesfernandez@almellonesfernandez-VirtualBox:~/Escritorio$
```

# Álvaro Almellones Fernández

```
root@Ubuntu-server-bastionado:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 45 packets, 2034 bytes)
pkts bytes target prot opt in out source destination
 0 0 ACCEPT 0 -- lo * 0.0.0.0/0 0.0.0.0/0
 0 0 DROP 6 -- enp0s3 * 192.168.1.108 0.0.0.0/0
 0 0 ACCEPT 6 -- enp0s3 * 192.168.1.108 0.0.0.0/0
tarting from 2024-11-25 00:00:00 until date 2024-11-25 23:59:00 UTC
 136 8672 ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 0 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
 11 660 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
ntos-ataque-SSH Server-al"
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
tentos-ataque-mysql-almelito"
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
ntos-ataque-Web-Server-al"
Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
 0 0 ACCEPT 0 -- * lo 0.0.0.0/0 0.0.0.0/0
 85 8456 ACCEPT 0 -- enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 1 -- enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 17 -- enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 6 -- enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 6 -- enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 17 -- enp0s3 0.0.0.0/0 193.204.114.231
 0 0 ACCEPT 17 -- enp0s3 0.0.0.0/0 216.239.35.0
 0 0 ACCEPT 6 -- enp0s3 0.0.0.0/0 0.0.0.0/0
root@Ubuntu-server-bastionado:~/scripts#
```

```
Iniciandose cortafuegos de Host: Álvaro Almellones
root@Ubuntu-server-bastionado:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
 0 0 ACCEPT 0 -- lo * 0.0.0.0/0 0.0.0.0/0
 0 0 DROP 6 -- enp0s3 * 192.168.1.108 0.0.0.0/0
 0 0 ACCEPT 6 -- enp0s3 * 192.168.1.108 0.0.0.0/0
tarting from 2024-11-24 00:00:00 until date 2024-11-24 23:59:00 UTC
 14 896 ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 0 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
ntos-ataque-SSH Server-al"
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
tentos-ataque-mysql-almelito"
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
ntos-ataque-Web-Server-al"

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

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
 0 0 ACCEPT 0 -- * lo 0.0.0.0/0 0.0.0.0/0
 8 736 ACCEPT 0 -- enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 1 -- enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 17 -- enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 6 -- enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 6 -- enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 17 -- enp0s3 0.0.0.0/0 193.204.114.231
 0 0 ACCEPT 17 -- enp0s3 0.0.0.0/0 216.239.35.0
 0 0 ACCEPT 6 -- enp0s3 0.0.0.0/0 0.0.0.0/0
root@Ubuntu-server-bastionado:~/scripts#
```

```
24 de nov 12:34
al mellonesfernandez@Ubuntu-server-bastionado:~ al mellonesfernandez@Ubuntu-server-bastionado:~
al mellonesfernandez@Ubuntu-server-bastionado:~$ sudo ssh -i /root/miskeys/almellonesfernandez almellone
sfernandez@192.168.1.110
Bienvenido al servidor Ubuntu server del módulo de Bastionaje de redes, del alumno almellonesfernandez. Está prohibida l
a conexión si no es Administrador de este sistema informático
Ubuntu 24.04.1 LTS
Last login: Sun Nov 24 12:21:30 2024 from 192.168.1.108
al mellonesfernandez@Ubuntu-server-bastionado:~$
```

## Álvaro Almellones Fernández

```
root@Ubuntu-server-bastionado:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 9 packets, 284 bytes)
pkts bytes target prot opt in out source destination
 12 1350 ACCEPT 0 -- lo * 0.0.0.0/0 0.0.0.0/0
 0 0 DROP 6 -- enp0s3 * 192.168.1.108 0.0.0.0/0
 19 5686 ACCEPT 6 -- enp0s3 * 192.168.1.108 0.0.0.0/0
tarting from 2024-11-24 00:00:00 until date 2024-11-24 23:59:00 UTC
 43 276 ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
 6 882 ACCEPT 0 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
ntos-ataque-SSH Server-al"
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
tentos-ataque-mysql-almello"
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
ntos-ataque-Web-Server-al"
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0

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

Chain OUTPUT (policy DROP 10 packets, 760 bytes)
pkts bytes target prot opt in out source destination
 12 1350 ACCEPT 0 -- * lo 0.0.0.0/0 0.0.0.0/0
 46 8622 ACCEPT 0 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 1 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 6 468 ACCEPT 17 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 17 -- * enp0s3 0.0.0.0/0 193.204.114.231
 0 0 ACCEPT 17 -- * enp0s3 0.0.0.0/0 216.239.35.0
 0 0 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0

root@Ubuntu-server-bastionado:~/scripts#
```

Por último, deje que permita la conexión desde cualquier cliente y a cualquiera hora del día (0,5 puntos)

```
root@Ubuntu-server-bastionado:~/scripts# nano almellonesfernandez-iptables.sh
root@Ubuntu-server-bastionado:~/scripts# ./almellonesfernandez-iptables.sh
Iniciando cortafuegos de Host: Álvaro Almellones
root@Ubuntu-server-bastionado:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 2 packets, 64 bytes)
pkts bytes target prot opt in out source destination
 0 0 ACCEPT 0 -- lo * 0.0.0.0/0 0.0.0.0/0
 10 640 ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 1 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 0 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
ntos-ataque-SSH Server-al"
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
tentos-ataque-mysql-almello"
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
ntos-ataque-Web-Server-al"
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0

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

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
 0 0 ACCEPT 0 -- * lo 0.0.0.0/0 0.0.0.0/0
 7 680 ACCEPT 0 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 1 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 17 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0
 0 0 ACCEPT 17 -- * enp0s3 0.0.0.0/0 193.204.114.231
 0 0 ACCEPT 17 -- * enp0s3 0.0.0.0/0 216.239.35.0
 0 0 ACCEPT 6 -- * enp0s3 0.0.0.0/0 0.0.0.0/0

root@Ubuntu-server-bastionado:~/scripts#
```

El contador está aumentando ya que estoy usando moba

c) Que se permita también conexiones al servidor web (http), vsftpd y mysql. (0,5 puntos)

# Álvaro Almellones Fernández

```
al mellonesfernandez@almellonesfernandez-VirtualBox:~/Escritorio$ ftp 192.168.1.110
al mellonesfernandez@almellonesfernandez-VirtualBox:~/Escritorio$ wget 192.168.1.110
Conectando con 192.168.1.110:80... ^C
al mellonesfernandez@almellonesfernandez-VirtualBox:~/Escritorio$ mysql -u almellonesfernandez -p -h 192.168.1.110
Enter password:
^C
al mellonesfernandez@almellonesfernandez-VirtualBox:~/Escritorio$

root@Ubuntu-server-bastionado:~/scripts# nano almellonesfernandez-iptables.sh
root@Ubuntu-server-bastionado:~/scripts# iptables -L -n -v
Chain INPUT (policy DROP 117 packets, 4342 bytes)
pkts bytes target prot opt in out source destination
 4 426 ACCEPT 0 -- lo * 0.0.0.0/0 0.0.0.0/0
 303 23885 ACCEPT 6 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
 10 300 ACCEPT 1 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
 19 8507 ACCEPT 0 -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
 state RELATED,ESTABLISHED
 0 0 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
 tcp dpt:22 LOG flags 0 level 4 prefix "Intentos-ataque-SSH Server-al"
 4 240 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
 tcp dpt:3306 LOG flags 0 level 4 prefix "Intentos-ataque-mysql-almello"
 5 300 LOG 6 -- * * 0.0.0.0/0 0.0.0.0/0
 tcp dpt:80 LOG flags 0 level 4 prefix "Intentos-ataque-Web-Server-al"

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

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
```

```
GNU nano 7.2 almellonesfernandez-iptables.sh
iptables -X #Borra cadenas personalizadas.
iptables -Z #Reinicia contadores.

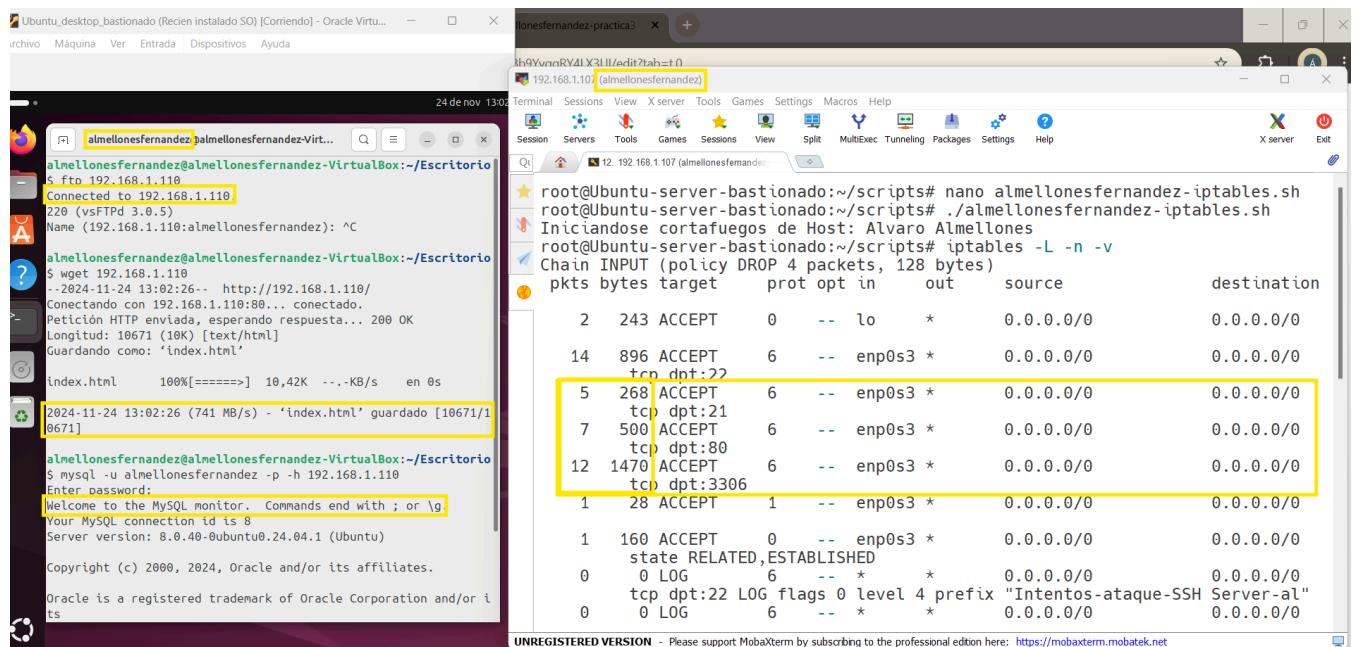
iptables -P INPUT DROP #Politica por defecto DROP
iptables -P OUTPUT DROP #Politica por defecto DROP
iptables -P FORWARD DROP #Politica por defecto DROP

#Reglas de loopback

iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

Reglas de INPUT
iptables -A OUTPUT -o $tarjeta -m state --state ESTABLISHED,RELATED -j ACCEPT #>
iptables -A INPUT -i $tarjeta -p tcp --dport 22 -j ACCEPT
iptables -A INPUT -i $tarjeta -p tcp --dport 21 -j ACCEPT
iptables -A INPUT -i $tarjeta -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -i $tarjeta -p tcp --dport 3306 -j ACCEPT
```

# Álvaro Almellones Fernández



\*\*\* Haga un backup de este script final (Xxxx-iptables-v3.0.sh).

\*\* Sería bueno realizar un snapshot final de este servidor Ubuntu Server. Muestre, aunque no se valorará.

## AMPLIACIÓN/INVESTIGACIÓN

- Realizar el mismo script (.bat), pero ejecutando desde un cliente Microsoft Windows, “atacando” los dos equipos (o más Linux).
- Realizar el mismo ejercicio, pero sobre S.O. Windows 10/11 o Windows Server. Puede implementar otros protocolos interesantes (RDP, VNC, SAMBA, etc.).
- Configuración y uso de HoneySSH.
- Uso de Snoopy.
- Cualquier cosa relacionada con lo visto en esta práctica, que no haya sido explicado por el profesor. Otros tipos de ataques, etc.
- Eliminación de protocolos innecesarios en S.O. Microsoft Windows.

## CRITERIOS DE EVALUACIÓN

|      |                                                                                                                             |
|------|-----------------------------------------------------------------------------------------------------------------------------|
| 5.a  | Se han configurado dispositivos de seguridad perimetral acorde a una serie de requisitos de seguridad.                      |
| 5.b  | Se han detectado errores de configuración de dispositivos de red mediante el análisis de tráfico.                           |
| 5.c. | Se han identificado comportamientos no deseados en una red a través del análisis de los registros (Logs), de un cortafuego. |

## Álvaro Almellones Fernández

|     |                                                                                                                                      |
|-----|--------------------------------------------------------------------------------------------------------------------------------------|
| 5.e | Se han caracterizado, instalado y configurado diferentes herramientas de monitorización.                                             |
| 6.c | Se ha incrementado la seguridad del sistema de administración remoto SSH y otros.                                                    |
| 7.a | Se han enumerado y eliminado los programas, servicios y protocolos innecesarios que hayan sido instalados por defecto en el sistema. |