

## PRÁCTICA 10

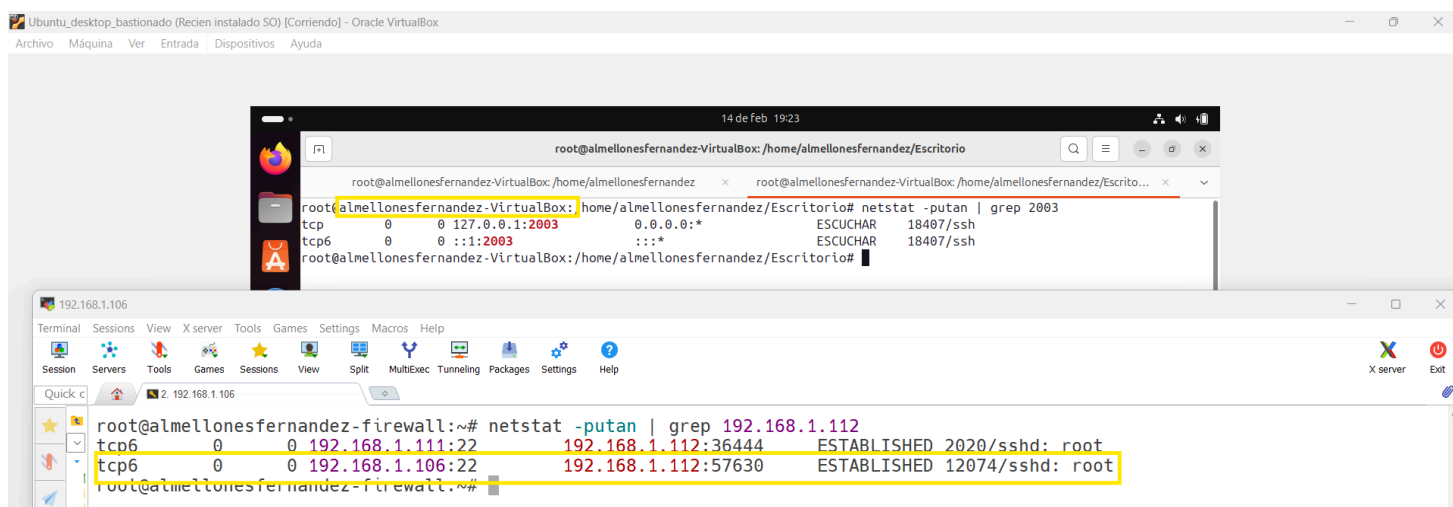
### TÚNELES SEGUROS CON SSH. REENVIO DE PUERTOS LOCALES

1. (5 puntos) Desde la zona wan usando un cliente Linux en modo terminal y autenticándonos con **llave privada al servidor firewall**, realice la conexión mediante un túnel SSH con el servidor SSHD de la zona (172.16.?.2). Se deja a elección del alumno el puerto usado para realizar el túnel. Se deberá mostrar las siguientes evidencias:

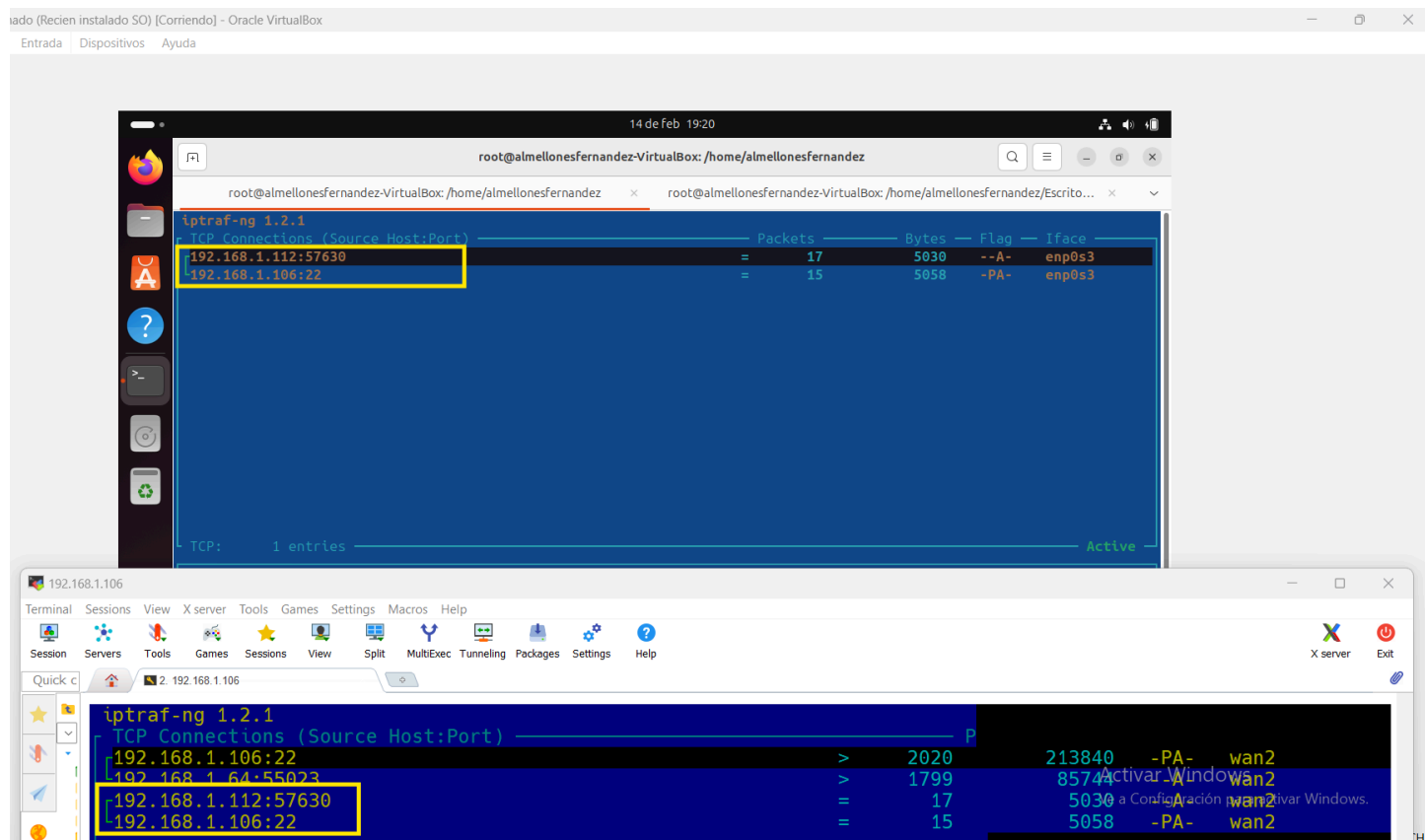
```
root@almellonesfernandez-VirtualBox:/home/almellonesfernandez/Escritorio# ssh -N -f -i /home/almellonesfernandez/Descargas/almellonesfernandez -L 2003:172.16.102.2:22 root@192.168.1.106
The authenticity of host '192.168.1.106 (192.168.1.106)' can't be established.
ED25519 key fingerprint is SHA256:BjipMtMZmAj4tR6Wxt0/9tJ9TR/uWQhE+knS8vD73G8.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.106' (ED25519) to the list of known hosts.
root@almellonesfernandez-VirtualBox:/home/almellonesfernandez/Escritorio#
```

a) Conexiones establecidas (netstat e iptraf-ng) una vez realizado el túnel y antes de acceder al servicio final (172.16.?.2). Se mostrará una única captura con los dos terminales abiertos en el siguiente orden de izquierda a derecha (cliente en zona wan desde donde se lanza el túnel, firewall al cual le hacemos la conexión ssh). Se valorará que se muestre mediante líneas o comentarios en las capturas que muestre el orden cronológico en la que ocurre la conexión.

He puesto el netstat del cliente de la zona wan (En mi caso un ubuntu desktop) arriba y abajo el netstat del firewall para que se vea mejor



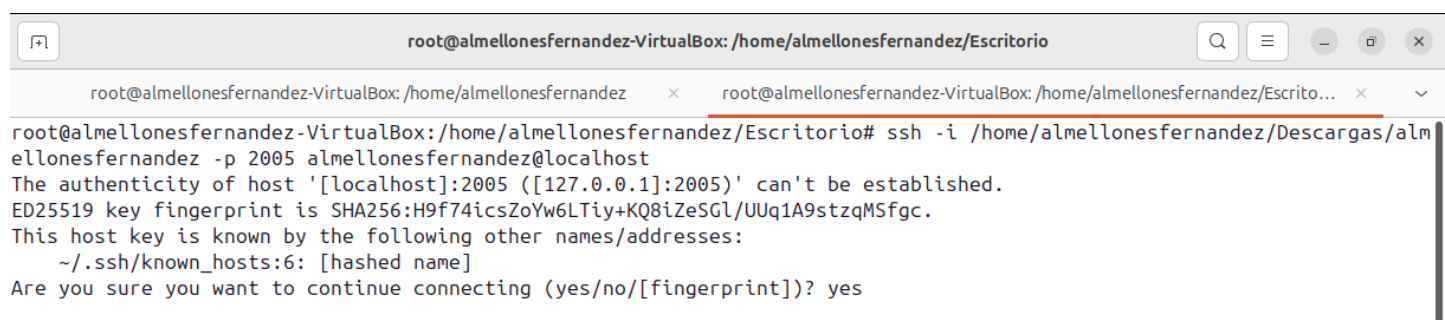
## Álvaro Almellones Fernández



En el cliente se habilita el puerto 2000 de localhost para el túnel seguro , pero en el firewall si filtramos por las conexiones a la ip del ubuntu Desktop no aparece nada del puerto 2000 ya que los túneles funcionan por ssh , por tanto como se observa usamos el puerto predeterminado de ssh (22)

b) Conexiones establecidas (netstat, iptraf-ng y tcpdump) mostrando **una única captura** con los tres terminales abiertos en el siguiente orden de izquierda a derecha (cliente en zona wan desde donde se lanza el túnel, firewall al cual le hacemos conexión ssh, servidor final en la zona LAN 172.16.?.2). Se valorará que se muestre mediante líneas o comentarios en las capturas que muestre el orden cronológico en la que ocurre la conexión.

He cambiado el puerto porque se me ha cambiado la ip de la wan y he tenido que rehacer el túnel



# Álvaro Almellones Fernández

The screenshot shows a virtual machine environment with two terminal windows. The left window is titled 'Ubuntu\_desktop\_bastionado (Recien instalado SO) [Corriendo] - Oracle VirtualBox' and shows a terminal session with the command 'netstat -putan | grep ESTABLISHED'. The output shows several established connections, including one from 192.168.1.112:35174 to 192.168.1.108:22. The right window is titled '6. 192.168.1.108' and shows a terminal session with the command 'netstat -putan | grep ESTABLISHED'. The output shows several established connections, including one from 192.168.1.108:22 to 192.168.1.112:35174. Yellow boxes highlight the relevant connection information in both windows, and yellow arrows point from the left window to the right window.

```
root@almellonesfernandez-VirtualBox:/home/almellonesfernandez# netstat -putan | grep ESTABLISHED
tcp        0      0  192.168.1.112:35174  192.168.1.108:22    ESTABLISHED 18650/s
tcp6       0      0  ::::2005             ::::*                ESTABLISHED 18650/s
```

```
root@almellonesfernandez-us-intranet:/home/almellonesfernandez# netstat -putan | grep ESTABLISHED
tcp6       0      0  172.16.102.2:22      172.16.102.1:48528  ESTABLISHED 2508/sshd: almellon
tcp6       0      0  172.16.102.2:22      172.16.102.1:35620  ESTABLISHED 1348/sshd: almellon
```

```
root@almellonesfernandez-firewall:/# netstat -putan | grep ESTABLISHED
tcp        0      0  192.168.1.108:22     192.168.1.64:55628  ESTABLISHED 1981/ssh
tcp        0      0  192.168.1.108:22     192.168.1.64:55674  ESTABLISHED 2529/sshd: root
tcp6       0      0  192.168.1.108:22     192.168.1.64:55675  ESTABLISHED 1538/sshd: root@pts
tcp6       0      0  192.168.1.108:22     192.168.1.112:53828 ESTABLISHED 1857/sshd: root@pts
tcp6       0      0  192.168.1.108:22     192.168.1.112:35174 ESTABLISHED 1540/sshd: root@not
tcp6       0      0  192.168.1.108:22     192.168.1.112:35174 ESTABLISHED 1859/sshd: root@not
tcp6       0      0  192.168.1.108:22     192.168.1.112:35174 ESTABLISHED 2323/sshd: root
```

The screenshot shows a virtual machine environment with two terminal windows. The left window is titled 'Ubuntu\_desktop\_bastionado (Recien instalado SO) [Corriendo] - Oracle VirtualBox' and shows a terminal session with the command 'iptraf-ng 1.2.1'. The output shows several network connections, including one from 192.168.1.112:35174 to 192.168.1.108:22. The right window is titled '6. 192.168.1.108' and shows a terminal session with the command 'iptraf-ng 1.2.1'. The output shows several network connections, including one from 192.168.1.108:22 to 192.168.1.112:35174. Yellow boxes highlight the relevant connection information in both windows, and yellow arrows point from the left window to the right window.

```
root@almellonesfernandez-VirtualBox:/home/almellonesfernandez# iptraf-ng 1.2.1
TCP: 2 entries
UDP (244 bytes) from 192.168.1.64:138 to 192.168.1.255:138 on enp0s3
IGMP (46 bytes) from 192.168.1.1 to 224.0.0.1 on enp0s3
IP (76 bytes) from fe80::ceed:dcff:fe5c:142 to ff02::1 on enp0s3
IP (96 bytes) from fe80::a00:27ff:fea7:5133 to ff02::16 on enp0s3
IGMP (46 bytes) from 192.168.1.64 to 224.0.0.251 on enp0s3
UDP (63 bytes) from 192.168.1.33:49470 to 192.168.1.255:15600 on enp0s3
ICMPv6 router adv (64 bytes) from fe80::ceed:dcff:fe5c:142 to ff02::1 on enp0s3
Packets captured: 619 TCP flow rate:
Up/Dn/PgUp/PgDn-scroll M-more TCP info M-chg actv win S-sort TCP X-exit
```

```
iptraf-ng 1.2.1
TCP Connections (Source Host:Port)
192.168.1.108:22 > 28 562108-PA-ens33
192.168.1.108:22 > 26 142144-A-ens33
192.168.1.108:22 = 1 14414-A-ens33
192.168.1.108:22 = 1 16014-PA-ens33
```

```
iptraf-ng 1.2.1
TCP Connections (Source Host:Port)
192.168.1.108:22 > 24 283632-PA-wan2
192.168.1.108:22 > 24 116248-A-wan2
192.168.1.108:22 > 23 112032-A-wan2
192.168.1.108:22 > 24 254288-PA-wan2
192.168.1.108:22 > 1 18852-A-wan2
192.168.1.108:22 > 1 20400-PA-wan2
```

# Álvaro Almellones Fernández

Ubuntu\_desktop\_bastionado (Recien instalado SO) [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

14 de feb. 20:34

root@almellonesfernandez-VirtualBox: /home/almellonesfernandez

20:50:59.954840 IP almellonesfernandez-VirtualBox.35174 > 192.168.1.108.ssh: Flags [P.], seq 42596:42816, win 1092, options [nop,nop,TS val 1673680118 ecr 1946444652], length 76

20:50:59.955451 IP 192.168.1.108.ssh > almellonesfernandez-VirtualBox.35174: Flags [P.], seq 42816:43020, ack 2233, win 1092, options [nop,nop,TS val 1946444672 ecr 1673680118], length 76

20:50:59.983236 IP almellonesfernandez-VirtualBox.59491 > 254.red-80-58-61.staticip.rima-tde.net.domain: Flags [P.], seq 43592:43980, ack 2233, win 1092, options [nop,nop,TS val 1946444724 ecr 1673680170], length 76

20:50:59.984492 IP almellonesfernandez-VirtualBox.35174 > 192.168.1.108.ssh: Flags [P.], seq 43592:43980, ack 2233, win 1092, options [nop,nop,TS val 1946444724 ecr 1673680170], length 76

20:50:59.985127 IP 192.168.1.108.ssh > almellonesfernandez-VirtualBox.35174: Flags [P.], seq 43980:44192, ack 42816, win 1092, options [nop,nop,TS val 1946444754 ecr 1673680200], length 76

20:51:00.006572 IP almellonesfernandez-VirtualBox.35174 > 192.168.1.108.ssh: Flags [P.], seq 44192:44404, ack 43980, win 1092, options [nop,nop,TS val 1946444777 ecr 1673680223], length 76

20:51:00.007091 IP 192.168.1.108.ssh > almellonesfernandez-VirtualBox.35174: Flags [P.], seq 44404:44616, ack 44192, win 1092, options [nop,nop,TS val 1946444777 ecr 1673680223], length 76

20:51:00.025243 IP 254.red-80-58-61.staticip.rima-tde.net.domain > almellonesfernandez-VirtualBox.59491: Flags [P.], seq 43592:43980, ack 2233, win 1092, options [nop,nop,TS val 1946444777 ecr 1673680223], length 76

20:51:00.025703 IP almellonesfernandez-VirtualBox.54360 > 254.red-80-58-61.staticip.rima-tde.net.domain: Flags [P.], seq 43592:43980, ack 2233, win 1092, options [nop,nop,TS val 1946444777 ecr 1673680223], length 76

20:51:00.036296 IP almellonesfernandez-VirtualBox.35174 > 192.168.1.108.ssh: Flags [P.], seq 44616:44828, ack 44404, win 1092, options [nop,nop,TS val 1946444777 ecr 1673680223], length 76

20:51:00.037109 IP 192.168.1.108.ssh > almellonesfernandez-VirtualBox.35174: Flags [P.], seq 44828:45040, ack 44616, win 1092, options [nop,nop,TS val 1946444777 ecr 1673680223], length 76

20:51:00.037887 IP 254.red-80-58-61.staticip.rima-tde.net.domain > almellonesfernandez-VirtualBox.59491: Flags [P.], seq 43592:43980, ack 2233, win 1092, options [nop,nop,TS val 1946444777 ecr 1673680223], length 76

20:51:00.059210 IP almellonesfernandez-VirtualBox.35174 > 192.168.1.108.ssh: Flags [P.], seq 45040:45252, ack 44828, win 1092, options [nop,nop,TS val 1946444777 ecr 1673680223], length 76

20:51:00.059940 IP 192.168.1.108.ssh > almellonesfernandez-VirtualBox.35174: Flags [P.], seq 45252:45464, ack 45040, win 1092, options [nop,nop,TS val 1946444777 ecr 1673680223], length 76

340 packets captured  
342 packets received by filter

6. 192.168.1.108

Re-attach Fullscreen Stay on top Duplicate Hide toolbar Close

35620: Flags [P.], seq 42596:42816, ack 2233, win 1092, options [nop,nop,TS val 3982419280 ecr 1275155419], length 220

19:49:50.175095 IP almellonesfernandez-us-intranet.ssh > \_gateway.35620: Flags [P.], seq 42816:43020, ack 2233, win 1092, options [nop,nop,TS val 3982419280 ecr 1275155419], length 204

19:49:50.175425 IP \_gateway.35620 > almellonesfernandez-us-intranet.ssh: Flags [P.], seq 43020:43592, ack 2233, win 1092, options [nop,nop,TS val 3982419280 ecr 1275155419], length 204

19:49:50.279043 IP almellonesfernandez-us-intranet.ssh > \_gateway.35620: Flags [P.], seq 43592:43980, ack 2233, win 1092, options [nop,nop,TS val 3982419280 ecr 1275155419], length 204

19:49:50.279661 IP \_gateway.35620 > almellonesfernandez-us-intranet.ssh: Flags [P.], seq 43980:44192, ack 43592, win 1092, options [nop,nop,TS val 3982419280 ecr 1275155419], length 204

19:49:50.382991 IP almellonesfernandez-us-intranet.ssh > \_gateway.35620: Flags [P.], seq 44192:44404, ack 43980, win 1092, options [nop,nop,TS val 3982419280 ecr 1275155419], length 204

3. 192.168.1.108

Re-attach Fullscreen Stay on top Duplicate Hide toolbar Close

11.ssh: Flags [P.], seq 240 336, ack 3889, win 4097, length 96

20:49:48.537478 IP almellonesfernandez-firewall.ssh > 192.168.1.64.55674: Flags [P.], seq 3889:3937, ack 336, win 1333, length 48

20:49:48.578630 IP 192.168.1.64.55674 > almellonesfernandez-firewall.ssh: Flags [P.], seq 3937:4097, ack 3889, length 0

20:49:48.630863 IP almellonesfernandez-firewall.ssh > 192.168.1.64.55674: Flags [P.], seq 7312 7392, ack 241, win 1629, length 80

20:49:48.631203 IP almellonesfernandez-firewall.ssh > 192.168.1.64.55674: Flags [P.], seq 7392:7552, ack 241, win 1629, length 160

20:49:48.631425 IP 192.168.1.64.55674 > almellonesfernandez-firewall.ssh: Flags [P.], seq 4097:4273, ack 336, win 1333, length 336

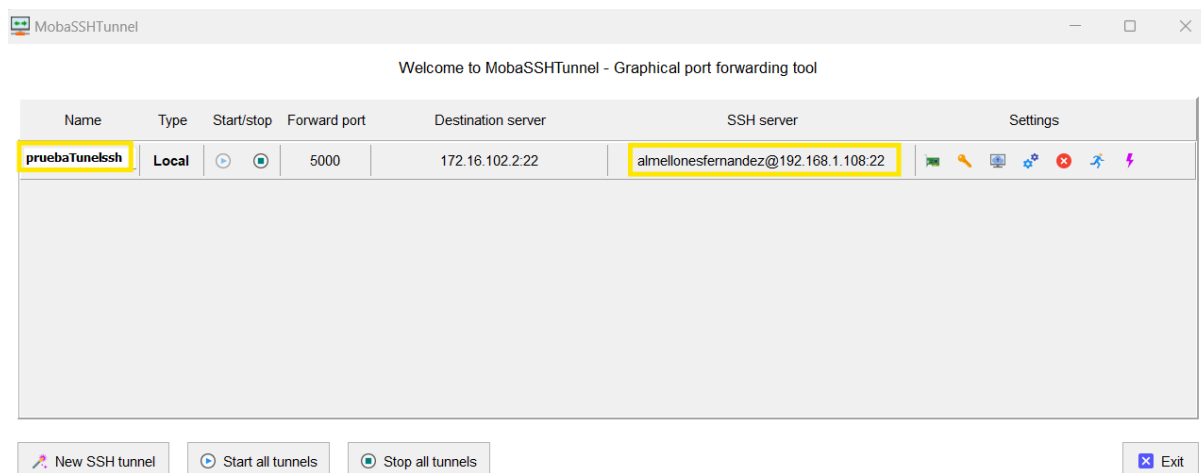
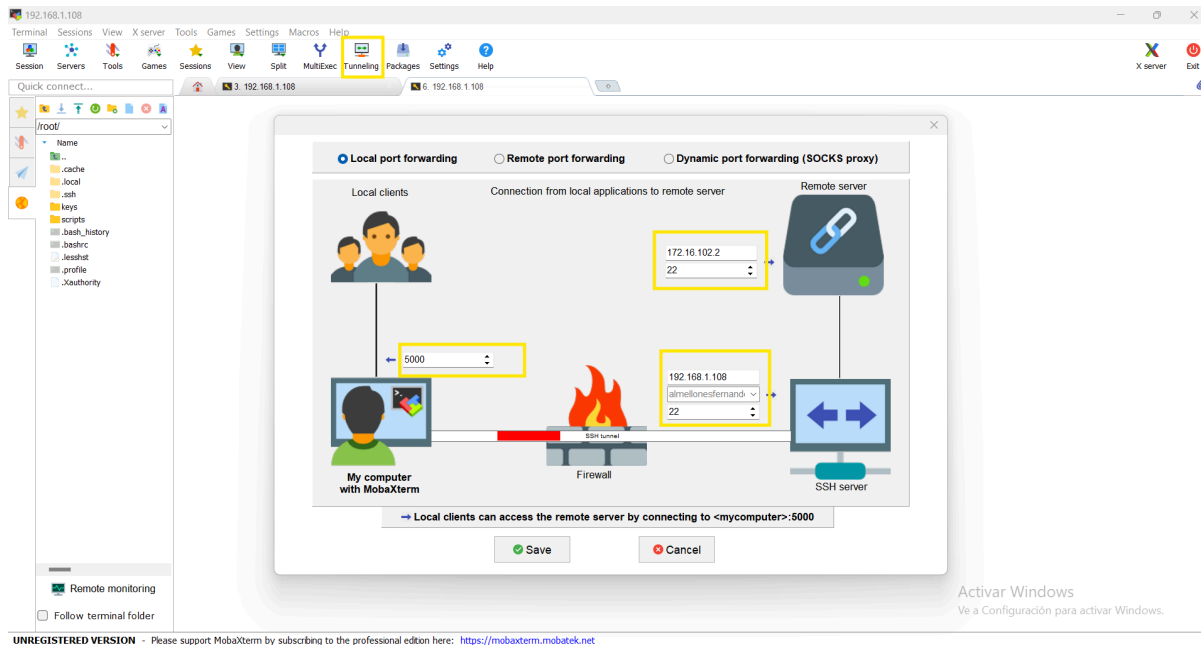
20:49:48.634181 IP almellonesfernandez-firewall.ssh > 192.168.1.64.55674: Flags [P.], seq 4273:4409, ack 4097, length 0

20:49:48.634860 IP almellonesfernandez-firewall.ssh > 192.168.1.64.55674: Flags [P.], seq 4409:4541, ack 4273, win 1333, length 336

20:49:48.634860 IP 192.168.1.64.55674 > almellonesfernandez-firewall.ssh: Flags [P.], seq 4541:4673, ack 4409, length 0

## Álvaro Almellones Fernández

2. (2,5 puntos, investigación) Realice el mismo ejercicio número 1, pero usando en este caso un cliente SSH GUI (putty, bitTunnelier, etc). Además, de las evidencias descritas en el apartado anterior, se tiene que mostrar la configuración realizada en el cliente GUI.



# Álvaro Almellones Fernández

```
almellonesfernandez@almell... x + -
```

```
C:\Users\alvar>ssh -i Desktop\MisKeys\almellonesfernandez -p 5000 almellonesfernandez@localhost
The authenticity of host '[localhost]:5000 ([::1]:5000)' can't be established.
ED25519 key fingerprint is SHA256:H9F74icsZoYw6LTiy+KQ8iZeSGL/UUq1A9stzqMSfGc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[localhost]:5000' (ED25519) to the list of known hosts.
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-51-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of vie 14 feb 2025 20:10:21 UTC

System load:  0.07          Processes:      237
Usage of /:   57.0% of 9.75GB Users logged in:    1
Memory usage: 60%          IPv4 address for ens33: 172.16.102.2
Swap usage:   20%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.
   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 196 actualizaciones de forma inmediata.
40 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 esudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Fri Feb 14 10:22:56 2025 from 172.16.102.1
almellonesfernandez@almellonesfernandez-us-intranet:~$ clear
```

C:\Users\alvar>netstat -ano | findstr "4512"

| Protocol | Local Address      | Foreign Address  | State       | PID  |
|----------|--------------------|------------------|-------------|------|
| TCP      | 0.0.0.0:5000       | 0.0.0.0:0        | LISTENING   | 4512 |
| TCP      | 192.168.1.64:56461 | 192.168.1.108:22 | ESTABLISHED | 4512 |
| TCP      | :::1:5000          | :::1:0           | LISTENING   | 4512 |
| TCP      | :::1:5000          | :::1:56547       | ESTABLISHED | 4512 |

C:\Users\alvar>

3. 192.168.1.108

```
root@almellonesfernandez-firewall:~# netstat -putan | grep ESTABLISHED | grep 22
```

| Protocol    | Local Address       | Foreign Address      | State               | PID |
|-------------|---------------------|----------------------|---------------------|-----|
| tcp         | 0                   | 0 172.16.102.1:35620 | 172.16.102.2:22     |     |
| ESTABLISHED | 1981/ssh            |                      |                     |     |
| tcp         | 0                   | 0 172.16.102.1:48528 | 172.16.102.2:22     |     |
| ESTABLISHED | 2529/sshd: root     |                      |                     |     |
| tcp         | 0                   | 0 172.16.102.1:42658 | 172.16.102.2:22     |     |
| ESTABLISHED | 2824/sshd: almellon |                      |                     |     |
| tcp6        | 0                   | 48 192.168.1.108:22  | 192.168.1.64:55628  |     |
| ESTABLISHED | 1538/sshd: root@pts |                      |                     |     |
| tcp6        | 0                   | 0 192.168.1.108:22   | 192.168.1.64:56461  |     |
| ESTABLISHED | 2777/sshd: almellon |                      |                     |     |
| tcp6        | 0                   | 0 192.168.1.108:22   | 192.168.1.64:55674  |     |
| ESTABLISHED | 1857/sshd: root@pts |                      |                     |     |
| tcp6        | 0                   | 0 192.168.1.108:22   | 192.168.1.64:55632  |     |
| ESTABLISHED | 1540/sshd: root@not |                      |                     |     |
| tcp6        | 0                   | 0 192.168.1.108:22   | 192.168.1.64:55675  |     |
| ESTABLISHED | 1859/sshd: root@not |                      |                     |     |
| tcp6        | 0                   | 0 192.168.1.108:22   | 192.168.1.112:53828 |     |
| ESTABLISHED | 2323/sshd: root     |                      |                     |     |
| tcp6        | 0                   | 0 192.168.1.108:22   | 192.168.1.112:35174 |     |
| ESTABLISHED | 2529/sshd: root     |                      |                     |     |

root@almellonesfernandez-firewall:~#

6. 192.168.1.108

```
root@almellonesfernandez-us-intranet:/home/almellonesfernandez# netstat -putan | grep ESTABLISHED | grep 22
```

| Protocol    | Local Address       | Foreign Address    | State              | PID |
|-------------|---------------------|--------------------|--------------------|-----|
| tcp6        | 0                   | 0 172.16.102.2:22  | 172.16.102.1:48528 |     |
| ESTABLISHED | 2508/sshd: almellon |                    |                    |     |
| tcp6        | 0                   | 0 172.16.102.2:22  | 172.16.102.1:42658 |     |
| ESTABLISHED | 2794/sshd: almellon |                    |                    |     |
| tcp6        | 0                   | 52 172.16.102.2:22 | 172.16.102.1:35620 |     |
| ESTABLISHED | 1348/sshd: almellon |                    |                    |     |

root@almellonesfernandez-us-intranet:/home/almellonesfernandez#

En windows he filtrado las conexiones por el id del proceso concreto del túnel. Pero es el mismo funcionamiento, localhost se pregunta a sí mismo por el puerto elegido y al responderse se conecta por ssh al firewall y del firewall al ubuntu server de lan.

## Álvaro Almellones Fernández

3. (2,5 puntos) Desde la zona wan usando un cliente Linux en modo terminal y autenticándonos con **llave privada al servidor firewall**, realice la conexión mediante un túnel SSH con el servidor apache (puerto 80 o puerto 443) de la zona (10.0.?.2). Se deja a elección del alumno el puerto usado para realizar el túnel. Se deberá mostrar las siguientes evidencias:

a) (1,25 puntos) Conexiones establecidas (netstat e iptraf-ng) una vez realizado el túnel y antes de acceder al servicio final (10.0.?.2). Se mostrará una única captura con los dos terminales abiertos en el siguiente orden de izquierda a derecha (cliente en zona wan desde donde se lanza el túnel, firewall al cual le hacemos la conexión ssh). Se valorará que se muestre mediante líneas o comentarios en las capturas que muestre el orden cronológico en la que ocurre la conexión.

```
root@almellonesfernandez-VirtualBox: /home/almellonesfernandez/Escritorio# ssh -N -f -i /home/almellonesfernandez/Descargas/almellonesfernandez -L 8003:10.0.102.2:80 -p 22 almellonesfernandez@192.168.1.108
root@almellonesfernandez-VirtualBox: /home/almellonesfernandez/Escritorio#
```

The screenshot displays two terminal windows side-by-side. The left window, titled 'almellonesfernandez@almellonesfernandez-VirtualBox: ~/Escritorio', shows the execution of the command `sudo netstat -putan | grep 22`. The output lists several listening and established connections on port 22, including one from 192.168.1.112:38102 to 192.168.1.108:22. The right window, titled '4. 192.168.1.108', shows the output of `netstat -putan | grep 22` from the firewall perspective. It shows an established connection from 10.0.102.1:58838 to 10.0.102.2:22, and another established connection from 192.168.1.108:22 to 192.168.1.112:38102. Yellow boxes highlight the relevant parts of both outputs, and a yellow arrow points from the left window's output to the right window's output, indicating the flow of the connection.

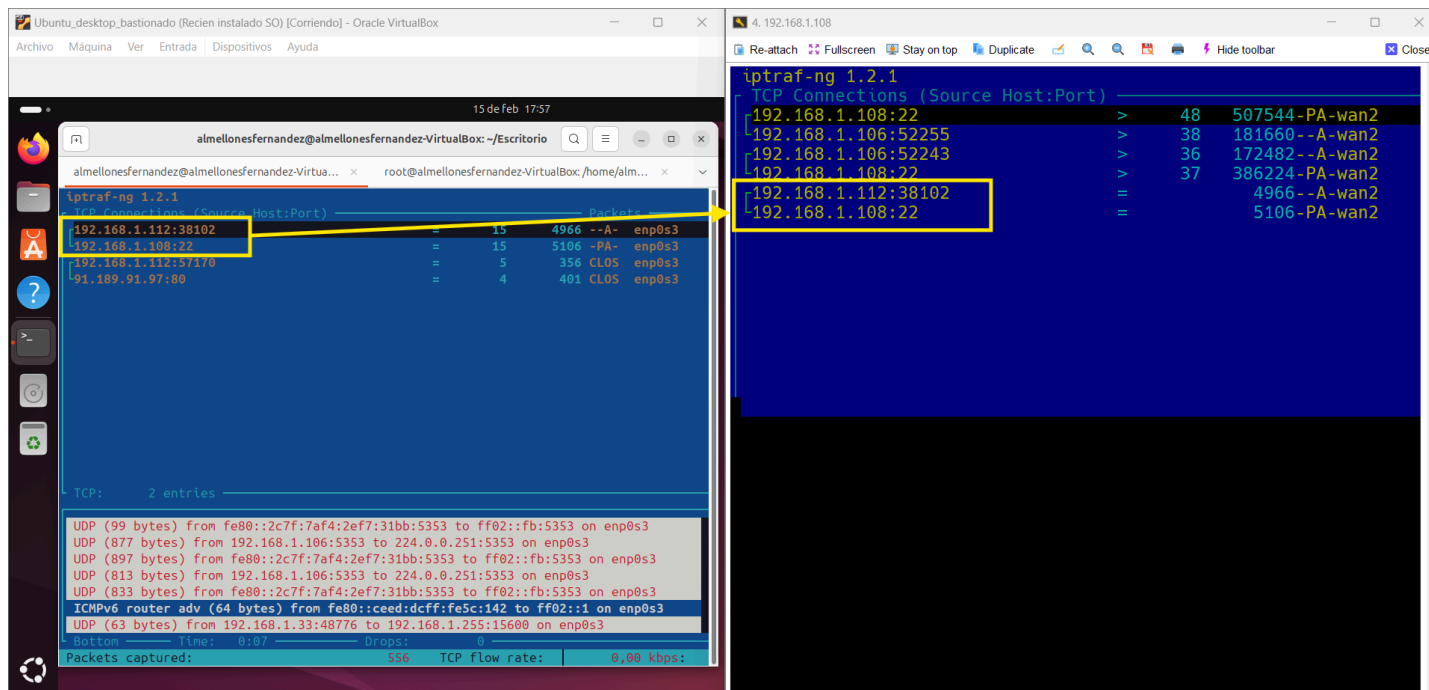
```
almellonesfernandez@almellonesfernandez-VirtualBox: ~/Escritorio$ sudo netstat -putan | grep 22
tcp        0      0 127.0.0.1:8003        0.0.0.0:*           ESCUCHAR    2702/ss
tcp        0      0 192.168.1.112:38102  192.168.1.108:22    ESTABLECIDO  2702/ss
tcp6       0      0 :::8003              :::*                 ESCUCHAR    2702/ss

almellonesfernandez@almellonesfernandez-VirtualBox: ~/Escritorio$

root@almellonesfernandez-firewall: ~# netstat -putan | grep 22
tcp        0      0 10.0.102.1:58838     10.0.102.2:22       ESTABLISHED  1909/ssh
tcp6       0      0 :::22                :::*                 LISTEN      1/init
tcp6       0      0 192.168.1.108:22     192.168.1.106:52257 ESTABLISHED  1912/sshd: root@not
tcp6       0      0 192.168.1.108:22     192.168.1.106:52243 ESTABLISHED  1801/sshd: root@pts
tcp6       0      0 192.168.1.108:22     192.168.1.106:52244 ESTABLISHED  1803/sshd: root@not
tcp6       0      0 192.168.1.108:22     192.168.1.106:52255 ESTABLISHED  1910/sshd: root@pts
tcp6       0      0 192.168.1.108:22     192.168.1.112:38102 ESTABLISHED  2043/sshd: almellon
root@almellonesfernandez-firewall: ~#
```



## Álvaro Almellones Fernández



b) (1,25 puntos) Conexiones establecidas (netstat, iptraf-ng y tcpdump) mostrando **una única captura** con los tres terminales abiertos en el siguiente orden de izquierda a derecha (cliente en zona wan desde donde se lanza el túnel, firewall al cual le hacemos conexión ssh, servidor final en la zona LAN 10.0.?.2). Se valorará que se muestre mediante líneas o comentarios en las capturas que muestre el orden cronológico en la que ocurre la conexión.

```
almellonesfernandez@almellonesfernandez-Virtua... x root@almellonesfernandez-VirtualBox: /home/alm... x
root@almellonesfernandez-VirtualBox /home/almellonesfernandez/Escritorio# wget localhost:8003
--2025-02-15 18:35:03-- http://localhost:8003/
Resolviendo localhost (localhost)... 127.0.0.1
Conectando con localhost (localhost)[127.0.0.1]:8003... conectado.
Petición HTTP enviada, esperando respuesta... 301 Moved Permanently
Ubicación: https://192.168.1.108/ [siguiente]
--2025-02-15 18:35:03-- https://192.168.1.108/
Conectando con 192.168.1.108:443... conectado.
ERROR: no se puede verificar el certificado de 192.168.1.108, emitido por 'CN=CA-almellonesfernandez':
Se encontró un certificado autofirmado.
ERROR: el nombre común 'almellonesfernandez-https' del certificado no encaja con el nombre de equipo '192.168.1.108' solicitado.
Para conectar inseguramente a 192.168.1.108, use '--no-check-certificate'.
root@almellonesfernandez-VirtualBox: /home/almellonesfernandez/Escritorio#
```

No me devuelve el index ya que en este ubuntu desktop no tengo la key de cliente, y en la práctica anterior configuramos para que se redirigiera de http a https, por lo cual no me lo devuelve



# Álvaro Almellones Fernández

The screenshot displays a VirtualBox window titled 'Ubuntu\_desktop\_bastionado (Recien instalado SO) [Corriendo] - Oracle VirtualBox'. Inside, there are two terminal windows. The left terminal shows the output of the 'netstat -tlnp' command, listing listening ports and processes. The right terminal shows the output of the 'ss -tlnp' command, listing established connections and processes. Yellow boxes highlight specific entries in both terminals, and yellow arrows point from the left terminal to the right terminal, indicating a correlation between the two outputs.

**Left Terminal (netstat -tlnp):**

| Protocol | Local Address | Local Port | State       | Process |
|----------|---------------|------------|-------------|---------|
| tcp      | 0.0.0.0       | 1167       | LISTEN      | cu      |
| tcp      | 0.0.0.0       | 1180       | LISTEN      | co      |
| tcp      | 0.0.0.0       | 2702       | LISTEN      | ss      |
| tcp      | 0.0.0.0       | 374        | LISTEN      | sys     |
| tcp      | 0.0.0.0       | 374        | LISTEN      | sys     |
| tcp      | 127.0.0.1     | 53868      | ESTABLISHED | 2702/ss |
| tcp      | 192.168.1.112 | 38102      | ESTABLISHED | 2702/ss |
| tcp      | 127.0.0.1     | 39696      | TIME_WAIT   | -       |
| tcp      | 127.0.0.1     | 57576      | TIME_WAIT   | -       |
| tcp      | 127.0.0.1     | 34438      | TIME_WAIT   | -       |
| tcp      | 127.0.0.1     | 53200      | TIME_WAIT   | -       |
| tcp      | 127.0.0.1     | 37632      | TIME_WAIT   | -       |
| tcp      | 127.0.0.1     | 59288      | TIME_WAIT   | -       |
| tcp      | 127.0.0.1     | 39686      | TIME_WAIT   | -       |
| tcp      | 127.0.0.1     | 57564      | TIME_WAIT   | -       |

**Right Terminal (ss -tlnp):**

| Protocol | Local Address | Local Port | State       | Process          |
|----------|---------------|------------|-------------|------------------|
| tcp6     | 0.0.0.0       | 1167       | LISTEN      | systemd-resolve  |
| tcp6     | 0.0.0.0       | 2107       | LISTEN      | apache2          |
| tcp6     | 0.0.0.0       | 1          | LISTEN      | init             |
| tcp6     | 0.0.0.0       | 962        | LISTEN      | vsftpd           |
| tcp6     | 0.0.0.0       | 2107       | LISTEN      | apache2          |
| tcp6     | 10.0.102.2    | 80         | ESTABLISHED | 10.0.102.1:50784 |
| tcp6     | 10.0.102.2    | 22         | ESTABLISHED | 10.0.102.1:58838 |
| udp      | 127.0.0.54    | 53         | ESTABLISHED | 0.0.0.0:*        |
| udp      | 127.0.0.53    | 53         | ESTABLISHED | 0.0.0.0:*        |
| tcp6     | 0.0.0.0       | 1167       | LISTEN      | systemd-resolve  |
| tcp6     | 0.0.0.0       | 2107       | LISTEN      | apache2          |
| tcp6     | 0.0.0.0       | 1          | LISTEN      | init             |
| tcp6     | 0.0.0.0       | 962        | LISTEN      | vsftpd           |
| tcp6     | 0.0.0.0       | 2107       | LISTEN      | apache2          |
| tcp6     | 10.0.102.2    | 80         | ESTABLISHED | 10.0.102.1:50784 |
| tcp6     | 10.0.102.2    | 22         | ESTABLISHED | 10.0.102.1:58838 |
| udp      | 127.0.0.54    | 53         | ESTABLISHED | 0.0.0.0:*        |
| udp      | 127.0.0.53    | 53         | ESTABLISHED | 0.0.0.0:*        |

The screenshot displays a VirtualBox window titled 'Ubuntu\_desktop\_bastionado (Recien instalado SO) [Corriendo] - Oracle VirtualBox'. Inside, there are two terminal windows. The left terminal shows the output of the 'tcpdump -i enp0s3' command, displaying captured network packets. The right terminal shows the output of the 'nmap -sS' command, displaying the results of a SYN scan. Yellow boxes highlight specific entries in both terminals, and yellow arrows point from the left terminal to the right terminal, indicating a correlation between the two outputs.

**Left Terminal (tcpdump -i enp0s3):**

| Protocol | Source Host:Port    | Destination Host:Port | Length | Flags | Interface   |
|----------|---------------------|-----------------------|--------|-------|-------------|
| TCP      | 192.168.1.112:38102 | 192.168.1.108:22      | 7      | 692   | -PA- enp0s3 |
| TCP      | 192.168.1.108:22    | 192.168.1.112:38102   | 5      | 980   | --A- enp0s3 |
| TCP      | 192.168.1.112:54202 | 192.168.1.108:22      | 5      | 356   | CLOS enp0s3 |
| TCP      | 185.125.190.18:80   | 192.168.1.108:22      | 4      | 405   | CLOS enp0s3 |

**Right Terminal (nmap -sS):**

| Host       | Port  | State | Service |
|------------|-------|-------|---------|
| 10.0.102.2 | 22    | OPEN  | ssh     |
| 10.0.102.1 | 58838 | OPEN  | ssh     |
| 10.0.102.1 | 38466 | OPEN  | ssh     |
| 10.0.102.2 | 80    | OPEN  | http    |