

Práctica repaso - Diccionarios, Hashes e IPTables

A.D.G.

1. Hash en zip, de la contraseña del zip sabes que es un día de la semana, empezando con mayúsculas o no, y al final la hora. También puede tener cambidas las e por \$.

a. ENTREGA, foto de las reglas de John The Ripper

```
john.conf: Bloc de notas
Archivo Edición Formato
[!List:reglas]
:
$[0-2]$[0-9]
c:$[0-2]$[0-9]
see:$[0-2]$[0-9]
se$:$[0-2]$[0-9]
see:see:$[0-2]$[0-9]
se$:see:$[0-2]$[0-9]
se$:see:$[0-2]$[0-9]
se$:see:$[0-2]$[0-9]
c:see:$[0-2]$[0-9]
c:se$:$[0-2]$[0-9]
c:see:see:$[0-2]$[0-9]
c:see:se$:$[0-2]$[0-9]
c:se$:see:$[0-2]$[0-9]
c:se$:se$:$[0-2]$[0-9]
```

diccionarioexamen.

Archivo Edición Forn

lunes

martes

miercoles

jueves

viernes

sabado

domingo

b. ENTREGA, foto de la linea de comandos de la contraseña

```
C:\john\run>john --wordlist=diccionarioexamen.txt --rules=reglas --format=ZIP hashguardada.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Mi$rcol$03 (hashExamen.zip/hashExamen.txt)
1g 0:00:00:00 DONE (2022-12-07 20:43) 12.19g/s 35939p/s 35939c/s 35939C/s lunes..Domingo29
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

2. Deshashear contraseñas de dentro del zip, las hashes son unalarga + dos numeros + muylarga + dos numeros ejemplo unalarga22muylarga88

a. ENTREGA, las fotos de la linea de comandos de crear el diccionario

```
(kali@kali)-[~]
$ crunch 20 20 -t unalarga%%muylarga%% -o /home/kali/Desktop/cruncheado.txt

Crunch will now generate the following amount of data: 210000 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 10000

crunch: 100% completed generating output
```

b. ENTREGA, la foto de la linea de comando del john the ripper actuando

```
(kali@kali)-[~]
$ john --wordlist=/home/kali/Desktop/cruncheado.txt /home/kali/Desktop/hashExamen.txt
Created directory: /home/kali/.john
Warning: only loading hashes of type "bcrypt", but also saw type "Raw-SHA1"
Use the "--format=Raw-SHA1" option to force loading hashes of that type instead
Warning: only loading hashes of type "bcrypt", but also saw type "Raw-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading hashes of that type instead
Warning: only loading hashes of type "bcrypt", but also saw type "LM"
Use the "--format=LM" option to force loading hashes of that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:15 6.66% (ETA: 16:14:36) 0g/s 42.99p/s 87.19c/s 87.19C/s unalarga06muylarga65
unalarga10muylarga90 (?)
unalarga40muylarga11 (?)
2g 0:00:00:59 DONE (2022-12-07 16:11) 0.03382g/s 67.88p/s 86.45c/s 86.45C/s unalarga39muylarga96..unalarga40muylarga13
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

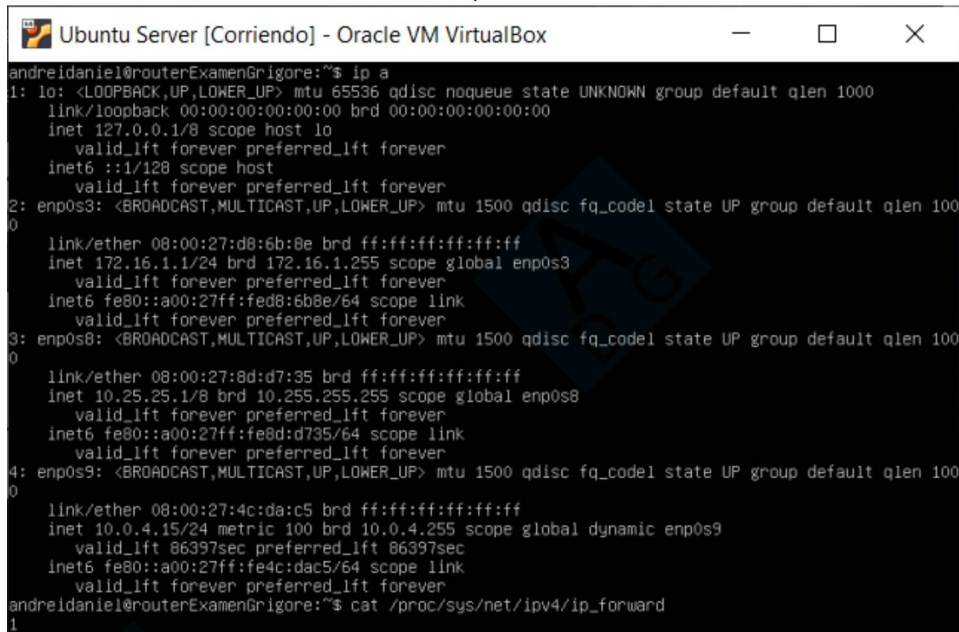
```
(kali@kali)-[~]
$ john --wordlist=/home/kali/Desktop/cruncheado.txt /home/kali/Desktop/hashExamen.txt --format=Raw-SHA1-AxCrypt
Using default input encoding: UTF-8
Loaded 3 password hashes with no different salts (Raw-SHA1-AxCrypt [SHA1 128/128 SSE2 4x])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
unalarga24muylarga55 (?)
unalarga76muylarga43 (?)
2g 0:00:00:00 DONE (2022-12-07 16:14) 50.00g/s 250000p/s 250000c/s 502500C/s unalarga99muylarga96..unalarga99muylarga99
Use the "--show --format=Raw-SHA1-AxCrypt" options to display all of the cracked passwords reliably
Session completed.
```

3. IPTABLES

a. (Preparacion de las tres maquinas)

b. Prepara maquina un ubuntu server que haga de router,

- i. con dos interfaces en red local y un NAT o bridge por si acaso se necesita instalar algo.
- ii. Pon de nombre maquina routerExamenTuApellido, y de usuario tu nombre.
- iii. Pon las ips de red para las redes locales, 10.25.25.1/8 en la red interna y 172.16.1.1/24 en la red local que hace de externa
- iv. ENTREGA una foto con el comando ip a

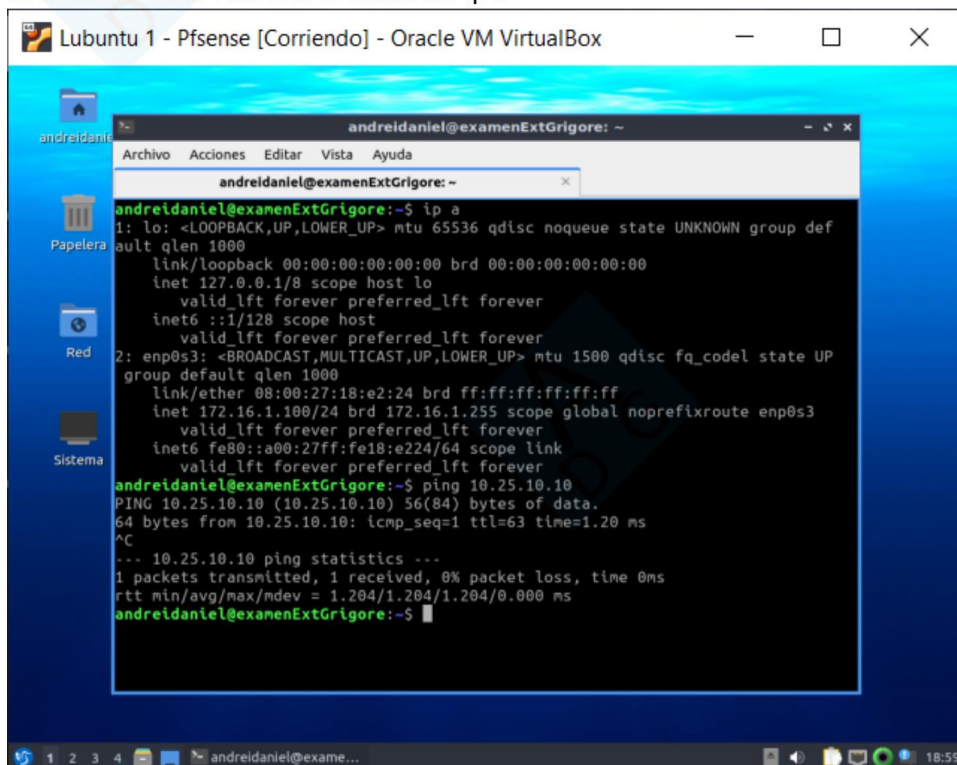


```

andreidaniel@routerExamenGrigore:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d8:6b:8e brd ff:ff:ff:ff:ff:ff
    inet 172.16.1.1/24 brd 172.16.1.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe8b:6b8e/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:8d:d7:35 brd ff:ff:ff:ff:ff:ff
    inet 10.25.25.1/8 brd 10.255.255.255 scope global enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe8d:d735/64 scope link
        valid_lft forever preferred_lft forever
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:4c:dac:5 brd ff:ff:ff:ff:ff:ff
    inet 10.0.4.15/24 metric 100 brd 10.0.4.255 scope global dynamic enp0s9
        valid_lft 86397sec preferred_lft 86397sec
    inet6 fe80::a00:27ff:fe4c:dac5/64 scope link
        valid_lft forever preferred_lft forever
andreidaniel@routerExamenGrigore:~$ cat /proc/sys/net/ipv4/ip_forward
1

```

- c. Prepara una maquina con un ubuntu cliente para la red externa
- i. Pon de nombre de maquina examenExtTuApellido, y de usuario tu nombre
- ii. Pon la ip de la red externa, 172.16.1.100 y la puerta de enlace del router
- iii. ENTREGA una foto con el comando ip a



```

andreidaniel@examenExtGrigore:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:18:e2:24 brd ff:ff:ff:ff:ff:ff
    inet 172.16.1.100/24 brd 172.16.1.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe18:e224/64 scope link
        valid_lft forever preferred_lft forever
andreidaniel@examenExtGrigore:~$ ping 10.25.10.10
PING 10.25.10.10 (10.25.10.10) 56(84) bytes of data:
64 bytes from 10.25.10.10: icmp_seq=1 ttl=63 time=1.20 ms
^C
--- 10.25.10.10 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.204/1.204/1.204/0.000 ms
andreidaniel@examenExtGrigore:~$

```


- d. Prepara una maquina con un ubuntu cliente para la red interna
- i. Pon de nombre internaExamenTuApellido y de usuario tu nombre
- ii. Pon la ip 10.25.10.10 y la puerta de enlace del router
- iii. ENTREGA una foto con el comando ip a

```

andredaniel@internaExamenGrigore: ~
Archivo Acciones Editar Vista Ayuda
andredaniel@internaExamenGrigore: ~
andredaniel@internaExamenGrigore:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
    qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
    group default qlen 1000
    link/ether 08:00:27:d5:35:85 brd ff:ff:ff:ff:ff:ff
    inet 10.25.10.10/8 brd 10.255.255.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fed5:3585/64 scope link
        valid_lft forever preferred_lft forever
andredaniel@internaExamenGrigore:~$ sudo nano /etc/netplan/01-network-manage
r-all.yaml
andredaniel@internaExamenGrigore:~$ ping 172.16.1.100
PING 172.16.1.100 (172.16.1.100) 56(84) bytes of data:
64 bytes from 172.16.1.100: icmp_seq=1 ttl=63 time=1.77 ms
^C
--- 172.16.1.100 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.774/1.774/1.774/0.000 ms
andredaniel@internaExamenGrigore:~$
  
```

- e. Probar el ping desde el cliente interno al externo con iptables en ACCEPT en el router. i.
- ENTREGA una foto con el ping
- ii. ENTREGA una foto con el comando iptables -L -nv en el router

```

root@routerExamenGrigore:~# iptables -F INPUT ACCEPT
root@routerExamenGrigore:~# iptables -F OUTPUT ACCEPT
root@routerExamenGrigore:~# iptables -F FORWARD ACCEPT
root@routerExamenGrigore:~# iptables -L -nv
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
root@routerExamenGrigore:~#
  
```

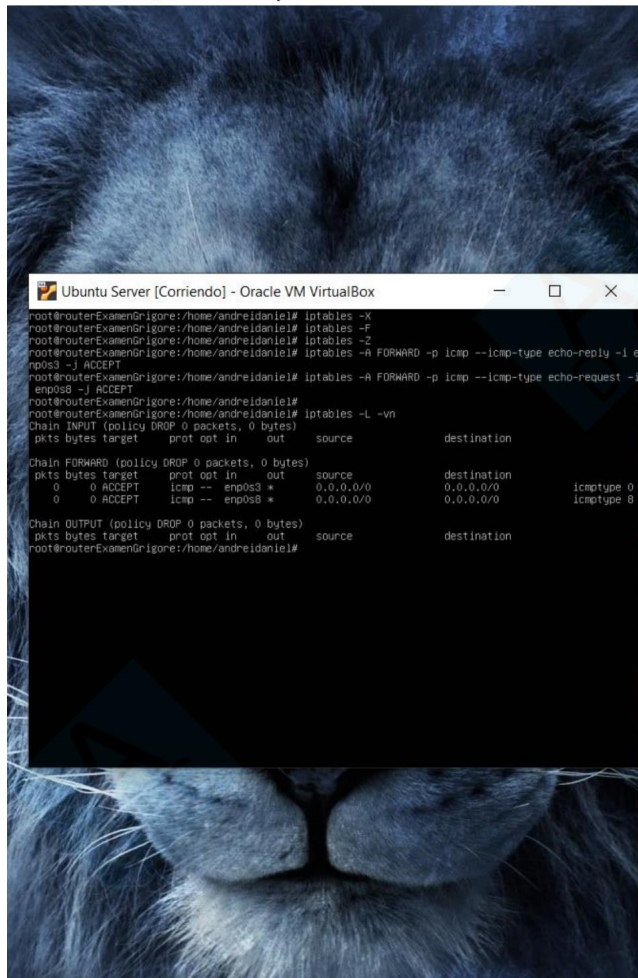
Pon todas las tablas INPUT, OUTPUT, FORWARD a DROP

f. Consigue un ping desde el ubuntu interno al externo pero al revés no

i. ENTREGA, foto del ping del ubuntu interno al externo

ii. ENTREGA, foto del ping fallido del ubuntu externo al interno

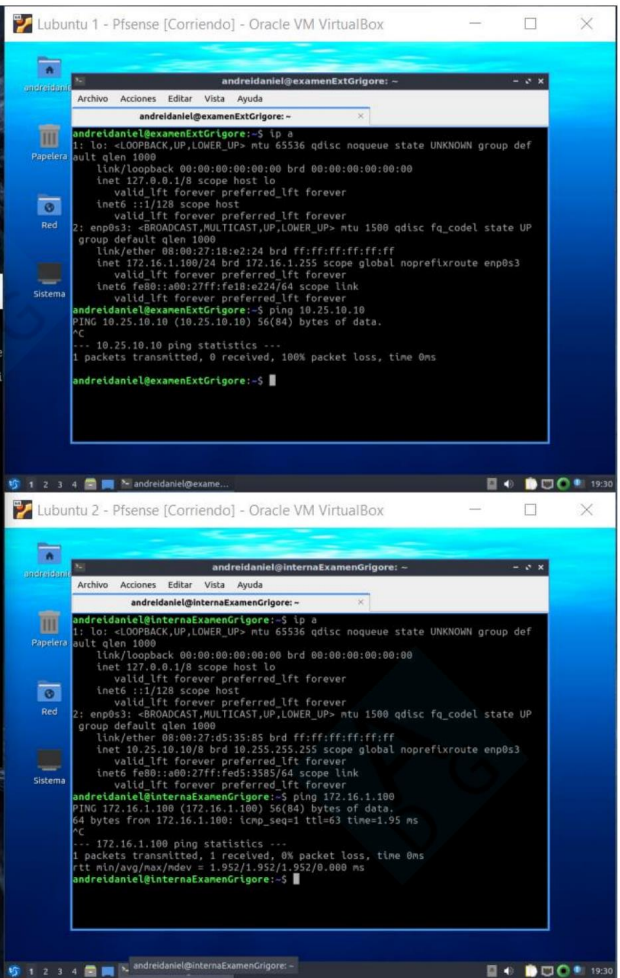
iii. ENTREGA, foto del iptables -L -nv desde el router



```
root@routerExamenGrigore:/home/andreidaniel# iptables -X
root@routerExamenGrigore:/home/andreidaniel# iptables -F
root@routerExamenGrigore:/home/andreidaniel# iptables -Z
root@routerExamenGrigore:/home/andreidaniel# iptables -A FORWARD -p icmp --icmp-type echo-reply -i enp0s3 -j ACCEPT
root@routerExamenGrigore:/home/andreidaniel# iptables -A FORWARD -p icmp --icmp-type echo-request -i enp0s3 -j ACCEPT
root@routerExamenGrigore:/home/andreidaniel# iptables -L -vn
Chain INPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
0 0 ACCEPT icmp -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
0 0 ACCEPT icmp -- enp0s3 * 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
0 0 ACCEPT icmp -- enp0s3 * 0.0.0.0/0 0.0.0.0/0
0 0 ACCEPT icmp -- enp0s3 * 0.0.0.0/0 0.0.0.0/0

Chain OUTPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
root@routerExamenGrigore:/home/andreidaniel#
```



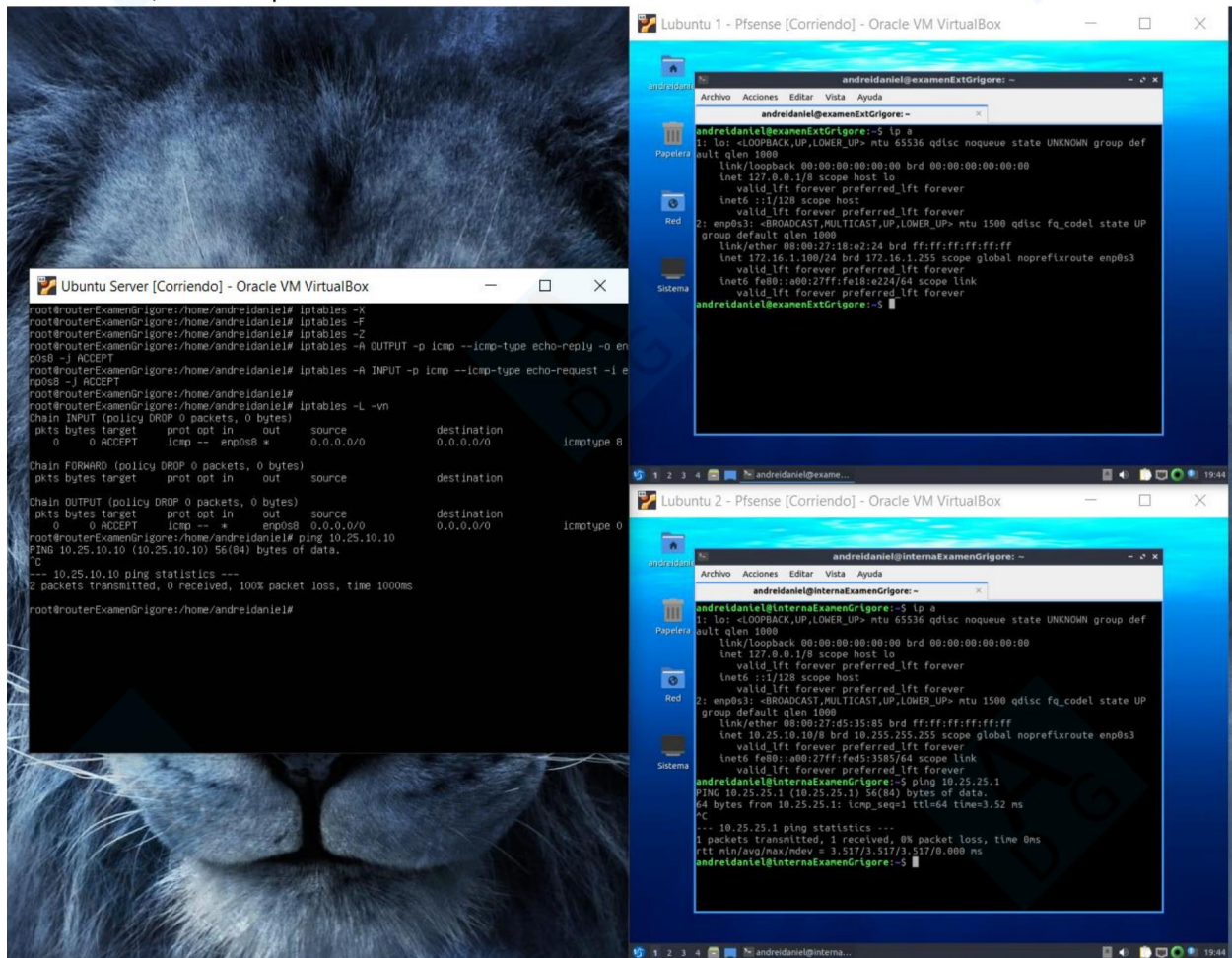
```
andreidaniel@examenExtGrigore:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:18:c2:24 brd ff:ff:ff:ff:ff:ff
    inet 172.16.1.100/24 brd 172.16.1.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe18:c224/64 scope link
        valid_lft forever preferred_lft forever
andreidaniel@examenExtGrigore:~$ ping 10.25.10.10
PING 10.25.10.10 (10.25.10.10) 56(84) bytes of data:
-- 10.25.10.10 ping statistics --
1 packets transmitted, 0 received, 100% packet loss, time 0ms

andreidaniel@examenExtGrigore:~$
```

```
andreidaniel@internaExamenGrigore:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d5:35:85 brd ff:ff:ff:ff:ff:ff
    inet 10.25.10.10/8 brd 10.255.255.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fed5:3585/64 scope link
        valid_lft forever preferred_lft forever
andreidaniel@internaExamenGrigore:~$ ping 172.16.1.100
PING 172.16.1.100 (172.16.1.100) 56(84) bytes of data:
64 bytes from 172.16.1.100: icmp_seq=1 ttl=63 time=1.95 ms
-- 172.16.1.100 ping statistics --
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/ndev = 1.952/1.952/1.952/0.000 ms

andreidaniel@internaExamenGrigore:~$
```


- g. Consigue que se haga un ping del servidor interno al router pero no del router al servidor interno.
- i. ENTREGA, foto del ping del ubuntu interno al router
- ii. ENTREGA, foto del ping fallido del router al ubuntu interno
- iii. ENTREGA, foto del iptables -L -nv desde el router



- h. Consigue que al ssh del router puede acceder el externo pero el interno no.
- i. ENTREGA, foto del ssh del ubuntu interno al router
- ii. ENTREGA, foto del ssh del ubuntu externo al router
- iii. ENTREGA, foto del iptables -L -nv desde el router

