

## Seguridad en Sistemas de Información: Tarea 3

Jorge E. Chávez Saab

CINVESTAV-IPN

12 de Junio 2020

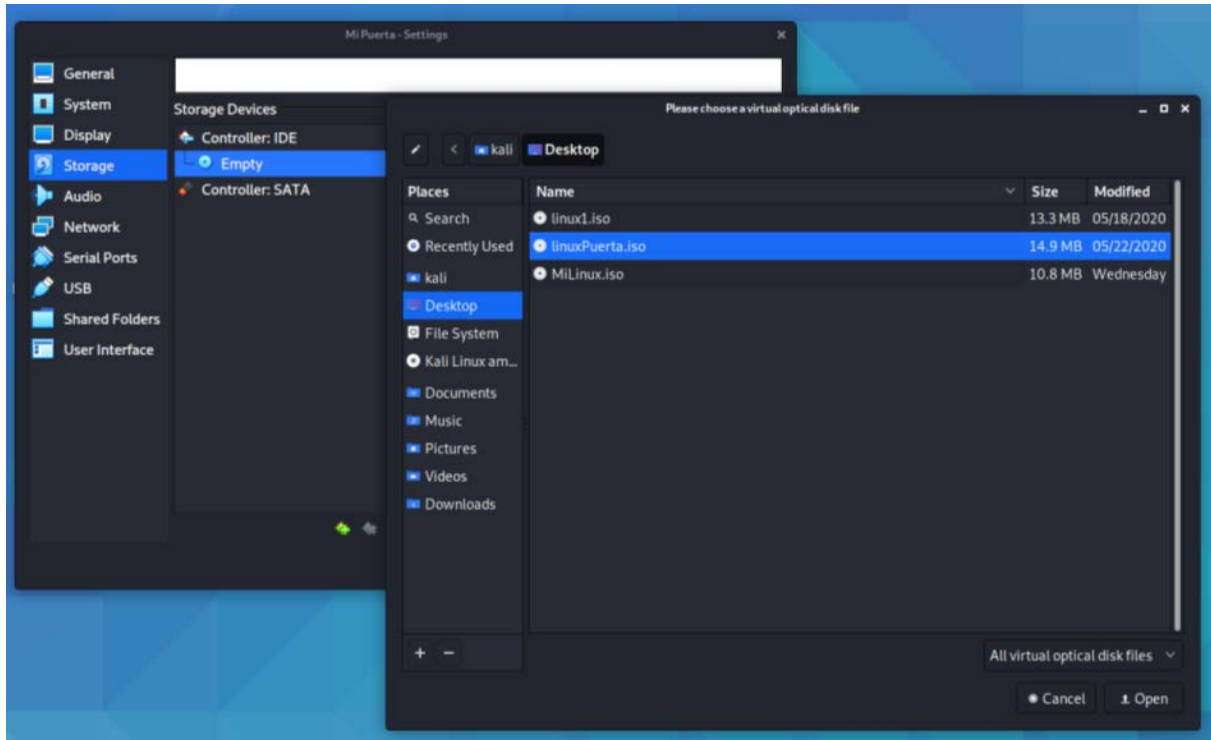
En esta práctica realizamos los pasos para configurar una red virtual que consiste en una máquina cliente y otra que actúa como puerta y cortafuegos, conectada a internet a través de la conexión NAT de VirtualBox.

### 1. Crear la máquina virtual para la puerta

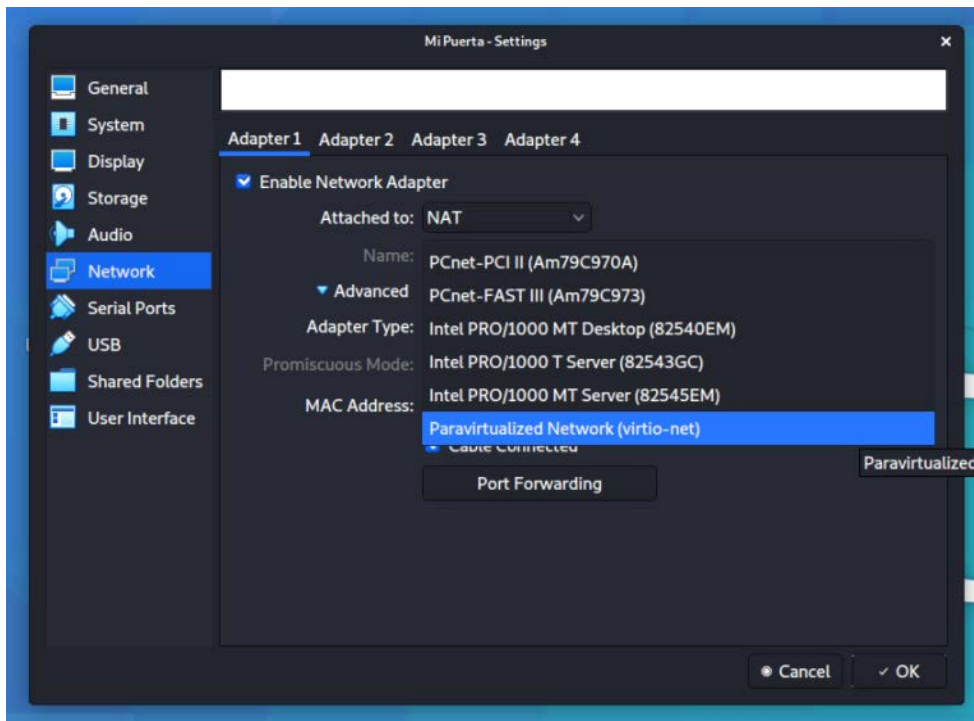
Descargamos el archivo .iso disponible para la puerta y creamos una nueva máquina virtual llamada “Mi Puerta” con la misma configuración que en la primera práctica.



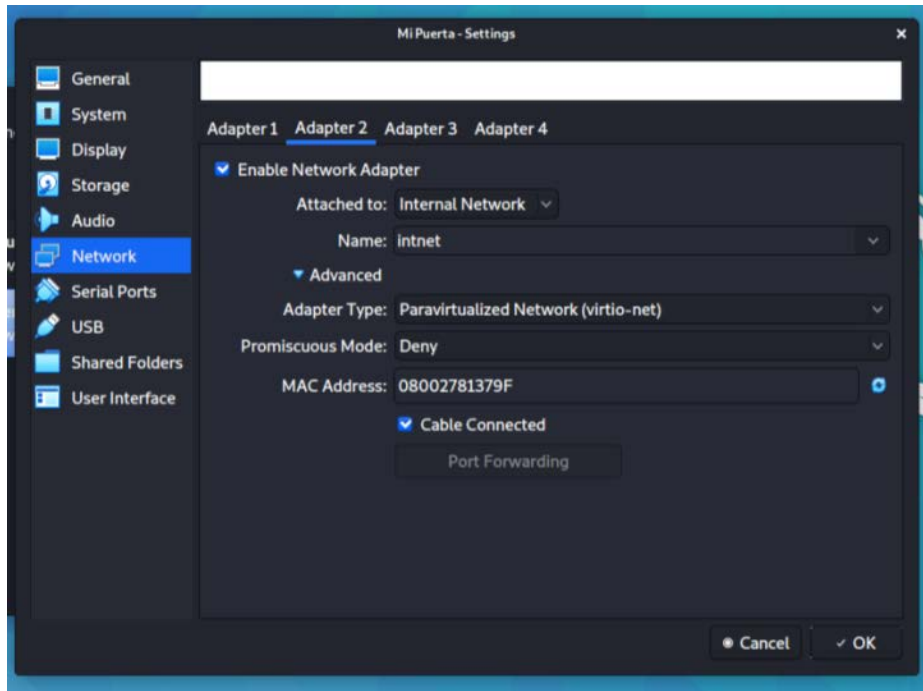
En la configuración de la nueva máquina, vamos a la pestaña Storage>Controller:IDE y elegimos el .iso que descargamos para arrancar la máquina.



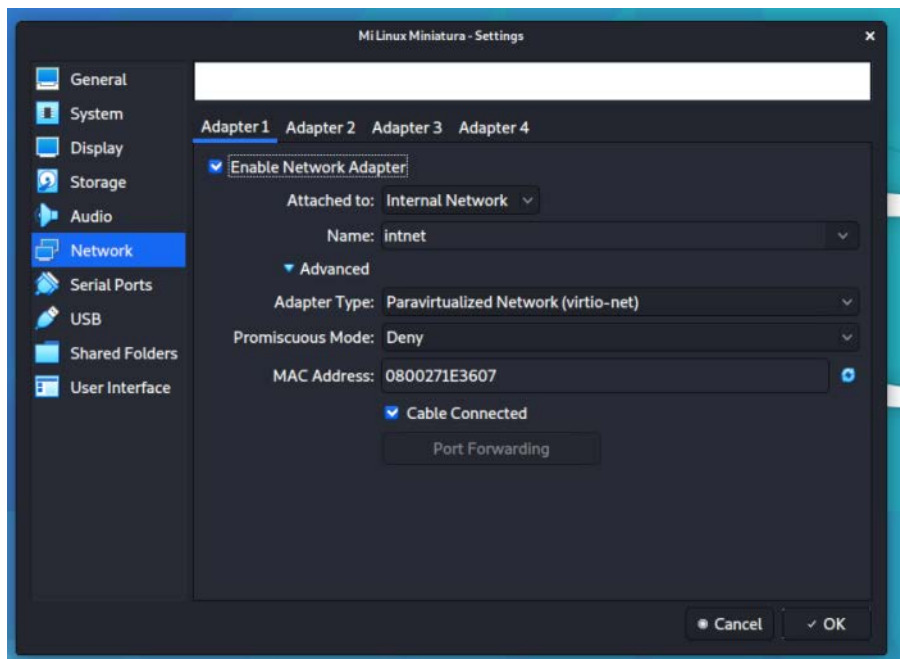
Después vamos a Network>Advanced y elegimos el adaptador virtio. Este adaptador está conectado con NAT, ya que será el que se conecte a internet a través de la interfaz de VirtualBox.



Necesitaremos un segundo adaptador para que se conecte con la máquina cliente, así es que vamos a la pestaña de “Adapter 2” y lo habilitamos. Ya que el cliente también es una máquina en VirtualBox, para este adaptador elegimos la opción “internal network” en vez de NAT.



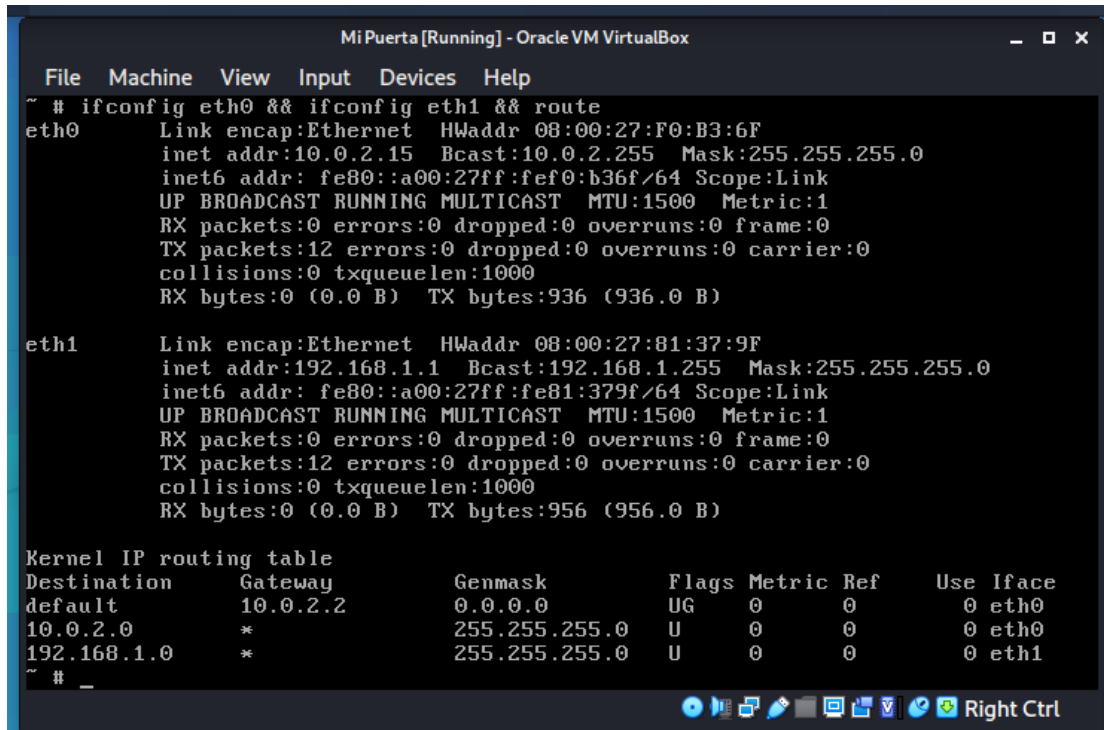
La máquina virtual que creamos en la práctica anterior, llamada “Mi Linux Miniatura”, es la que nos servirá de cliente. Como sólo se conectará a la puerta, necesitamos un solo adaptador y este debe estar en “internal network” también. Debemos asegurarnos que el nombre de la red sea el mismo para que las máquinas estén conectadas a la misma red virtual:



## 2. Configurar la red

Iniciamos ambas máquinas virtuales (cliente y puerta), y modificamos sus archivos `/etc/resolv.conf` para incluir la dirección de nuestro DNS como en la práctica anterior.

Usando el comando `ifconfig eth0 && ifconfig eth1 && route` en la máquina puerta, podemos verificar que `eth0` está conectado a la interfaz de VirtualBox, que como vimos en la práctica anterior, tiene el Default Gateway `10.0.2.2`, mientras que `eth1` está conectado a la red virtual con dirección `192.168.1.1`, que es la misma red que al red física en mi hogar.



```
Mi Puerta [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
~ # ifconfig eth0 && ifconfig eth1 && route
eth0      Link encap:Ethernet  HWaddr 08:00:27:F0:B3:6F
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feF0:b36f/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:936 (936.0 B)

eth1      Link encap:Ethernet  HWaddr 08:00:27:81:37:9F
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feB1:379f/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:956 (956.0 B)

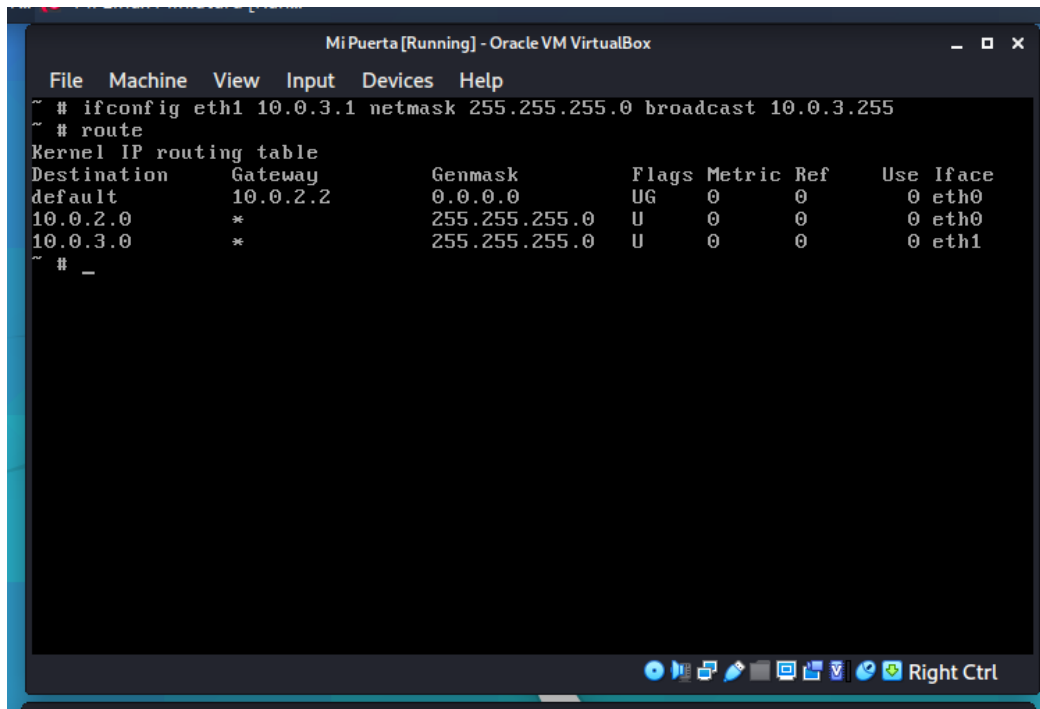
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default    10.0.2.2  0.0.0.0 UG 0 0 0 eth0
10.0.2.0   *         255.255.255.0 U 0 0 0 eth0
192.168.1.0 *         255.255.255.0 U 0 0 0 eth1
~ # _
```

Para evitar confusiones asignamos otro número a la red virtual. Para esto hemos elegido la red `10.0.3.0/24`. En donde la puerta tendrá la dirección `10.0.3.1` y el cliente la dirección `10.0.3.2`.

Para implementar esto usamos el comando

```
ifconfig eth1 10.0.3.1 netmask 255.255.255.0 broadcast 10.0.3.255
```

en la puerta para asignarle dicha dirección:



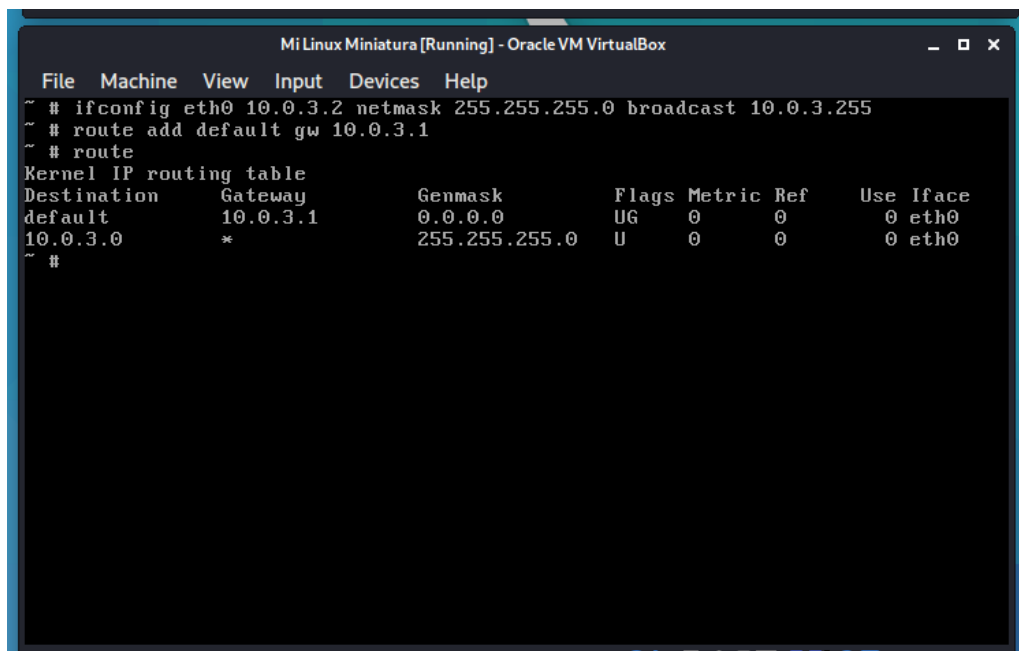
```
File Machine View Input Devices Help
~ # ifconfig eth1 10.0.3.1 netmask 255.255.255.0 broadcast 10.0.3.255
~ # route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default 10.0.2.2 0.0.0.0 UG 0 0 0 eth0
10.0.2.0 * 255.255.255.0 U 0 0 0 eth0
10.0.3.0 * 255.255.255.0 U 0 0 0 eth1
~ # _
```

Ahora debemos ir a la máquina cliente y conectar su única interfaz a la misma red. Para esto, usamos

```
ifconfig eth0 10.0.3.2 netmask 255.255.255.0 broadcast 10.0.3.255
```

y además registramos la dirección de la puerta como default gateway con el comando

```
route add default gw 10.0.3.1:
```



```
File Machine View Input Devices Help
~ # ifconfig eth0 10.0.3.2 netmask 255.255.255.0 broadcast 10.0.3.255
~ # route add default gw 10.0.3.1
~ # route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default 10.0.3.1 0.0.0.0 UG 0 0 0 eth0
10.0.3.0 * 255.255.255.0 U 0 0 0 eth0
~ #
```

Para asegurarnos de que la conexión es correcta, podemos hacer un ping desde la máquina cliente a la máquina puerta usando `ping 10.0.3.1`:

```
Mi Linux Miniatura [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
~ # ifconfig eth0 10.0.3.2 netmask 255.255.255.0 broadcast 10.0.3.255
~ # route add default gw 10.0.3.1
~ # route
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
default          10.0.3.1       0.0.0.0        UG    0     0     0 eth0
10.0.3.0         *              255.255.255.0  U    0     0     0 eth0
~ # ping 10.0.3.1 -c 10
PING 10.0.3.1 (10.0.3.1): 56 data bytes
64 bytes from 10.0.3.1: seq=0 ttl=64 time=1.256 ms
64 bytes from 10.0.3.1: seq=1 ttl=64 time=1.065 ms
64 bytes from 10.0.3.1: seq=2 ttl=64 time=0.559 ms
64 bytes from 10.0.3.1: seq=3 ttl=64 time=1.080 ms
64 bytes from 10.0.3.1: seq=4 ttl=64 time=0.595 ms
64 bytes from 10.0.3.1: seq=5 ttl=64 time=0.707 ms
64 bytes from 10.0.3.1: seq=6 ttl=64 time=0.532 ms
64 bytes from 10.0.3.1: seq=7 ttl=64 time=1.067 ms
64 bytes from 10.0.3.1: seq=8 ttl=64 time=0.657 ms
64 bytes from 10.0.3.1: seq=9 ttl=64 time=0.996 ms

--- 10.0.3.1 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 0.532/0.851/1.256 ms
~ #
```

### 3. Configuración de la puerta y cortafuegos

Ahora configuramos la puerta. Debemos editar el script `/etc/fw_nat2.sh` que hace la configuración del firewall usando `iptables` para habilitar los servicios de `ssh` (22), `http` (80), `dns` (53) y `https` (443) solamente. En el encabezado del archivo, modificamos el valor de `IPADDR` para que sea la dirección que se conecta a la interfaz de VirtualBox (es decir `10.0.2.15`) así como el valor de `REDLOCAL`, `DNS` (donde insertamos la dirección del DNS que da nuestro ISP) y `REDINTERNA` (donde introducimos la red `10.0.3.0/24` que creamos).

```
MI Linux Miniatura [Run...
Mi Puerta [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
# habilita la traducci..n de paquetes y
# filtra los servicios de
# SSH (22),
# http (80),
# https (443),
# DNS (53),
# para la red interna
#
PATH=/usr/sbin
LOOPBACK_INTERFAZ=lo

#
INTERFAZ_EXT=eth0
IPADDR=10.0.2.15/32
REDLOCAL=10.0.2.0/24
DNS=192.168.1.1/32

#
INTERFAZ_INT=eth1
REDINTERNA=10.0.3.0/24
UNIVERSO=0.0.0.0/0

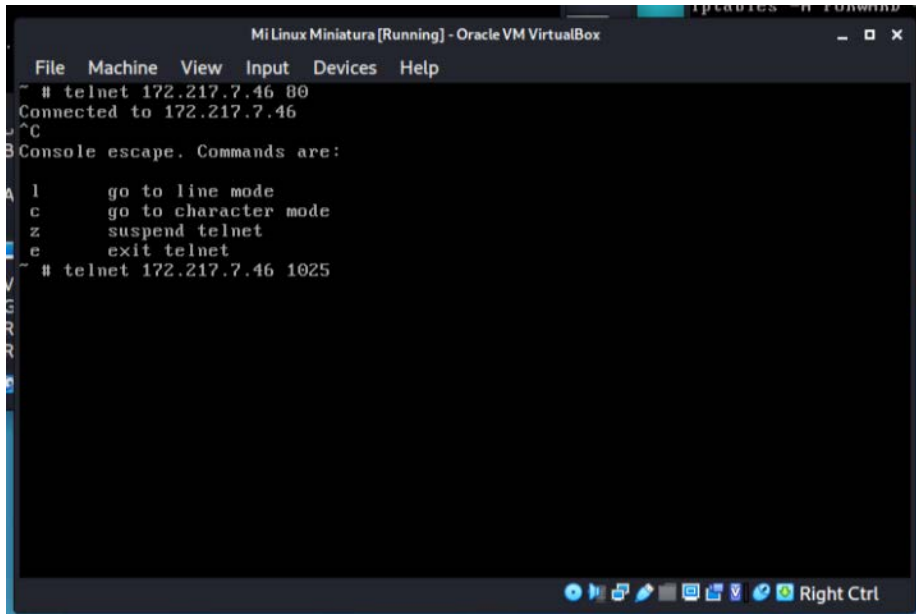
# Limpiamos las reglas actuales
iptables -F
I /etc/fw_nat2.sh [Modified] 27/99 27%
```

Finalmente, usamos el comando `echo 1 > /proc/sys/net/ipv4/ip_forward` para habilitar el traspaso de paquetes y ejecutamos nuestro script:

```
MI Puerta [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
~ # echo 1 > /proc/sys/net/ipv4/ip_forward
~ # sh /etc/fw_nat2.sh
~ # _
```

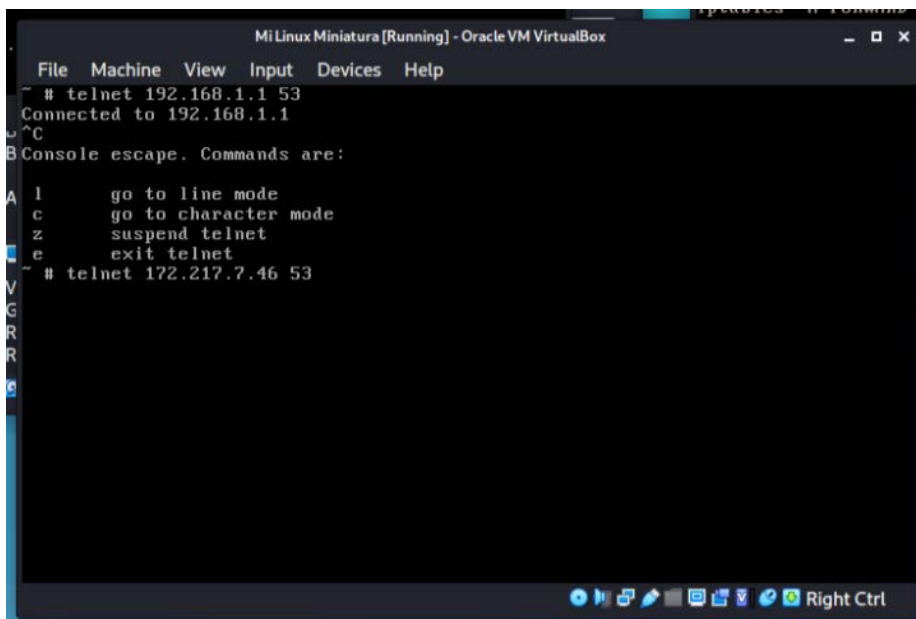
## 4. Prueba de conexión y del cortafuegos

Ahora nuestra red virtual está completamente configurada. Para verificar que la máquina cliente tiene acceso a internet, podemos usar un `telnet 172.217.7.46 80` (que es la dirección de google.com) lo cual es válido porque el cortafuegos admite conexiones a direcciones externas por el puerto 80 (http), pero si usamos `telnet 172.217.7.46 1025` entonces no hay respuesta ya que el cortafuegos no permite conectarse a ningún puerto de usuario de una dirección externa.



```
Mi Linux Miniatura [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
~ # telnet 172.217.7.46 80
Connected to 172.217.7.46
^C
B Console escape. Commands are:
A l      go to line mode
  c      go to character mode
  z      suspend telnet
  e      exit telnet
~ # telnet 172.217.7.46 1025
```

Por otro lado, si usamos `telnet 192.168.1.1 53` entonces logramos conectarnos a nuestro DNS por el puerto 53, pero con `telnet 172.217.7.48 53` no hay respuesta ya que el cortafuegos solo permite tráfico por el puerto 53 si va hacia la dirección del DNS que introdujimos.



```
Mi Linux Miniatura [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
~ # telnet 192.168.1.1 53
Connected to 192.168.1.1
^C
B Console escape. Commands are:
A l      go to line mode
  c      go to character mode
  z      suspend telnet
  e      exit telnet
~ # telnet 172.217.7.46 53
```