

Montaje y Configuración de un Pequeño Laboratorio de Pruebas

Seguridad y Alta Disponibilidad

Gonzalo Tudela Chavero

2º ASIR

ÍNDICE DE CONTENIDOS

Descripción de la práctica.	1
Creación y configuración de las VM	1
Creación de la maquina Kali Linux.	1
Configuración de la red NAT en VMware.....	4
Configuración de la VM Metasploitable 2.	6
Configuración de la VM Kali en la red NAT.....	7
Comprobación e interpretación de la comunicación entre las VM.	9

ÍNDICE DE FIGURAS

Figura 1 - Configuración VMware de la versión Linux de la máquina virtual.	1
Figura 2 - Configuración del nombre y la ruta de la VM.	2
Figura 3 - Configuración de la CPU para la VM Kali.	2
Figura 4 - Memoria RAM recomendada para Kali Linux.	3
Figura 5 - Configuración de la red en modo NAT para la máquina Kali.....	3
Figura 6 - Finalización de la configuración de la VM Kali.....	4
Figura 7 - Instalación de la ISO Kali en la máquina virtual.	4
Figura 8 - Configuración de la red NAT en VMware.....	5
Figura 9 - Configuración de la puerta de enlace.....	5
Figura 10 - Configuración del servicio DHCP.	6
Figura 11 - Login y password msfadmin.	6
Figura 12 - Configuración de la interfaz de red eth0 en metasploitable 2.	7
Figura 13 - Comprobación de la configuración de interfaces de red en metasploitable 2.	7
Figura 14 - La máquina no cuenta con una configuración para eth0.	7
Figura 15 - eth0 funcionando a pesar de que interfaces no sabe nada de esto.....	8
Figura 16 - Configuración interfaces en kali linux.....	8
Figura 17 - Levantamos eth0 con ifup.....	8
Figura 18 - PING desde VM Kali.	9
Figura 19 - PING desde Metasploitable2.....	9

Descripción de la práctica.

Se quiere disponer de un pequeño laboratorio para realizar pruebas de penetración, con la condición de que el entorno tiene que ser controlado.

Para ello, de momento, se utilizarán las siguientes dos máquinas que deberán tener comunicación entre ellas:

- Kali Linux (<https://www.kali.org/downloads/>): será, en la mayoría de los casos, la máquina utilizada para realizar las pruebas de seguridad ofensiva.
- Metasploitable (<https://information.rapid7.com/download-metasploitable-2017.html>): será la máquina objetivo de las pruebas. Para que éstas se puedan realizar.

Crea y configura las máquinas virtuales necesarias para la creación del entorno de pruebas controlado.

Comprueba que las máquinas tienen comunicación entre sí e interpreta los resultados.

Indica los pasos necesarios que has realizado para que las máquinas puedan comunicarse entre sí.

Realiza una memoria con los resultados obtenidos en formato PDF. Deberá de tener una portada con el nombre de alumno/s que realizan las prácticas, así como de los resultados obtenidos con un índice para cada uno de los ejercicios.

Creación y configuración de las VM

Para la creación de las máquinas virtuales se han descargado las correspondientes imágenes ISO de las URL suministradas en la descripción de la práctica y se han creado las correspondientes máquinas virtuales mediante el software VMware Workstation como se puede ver en las siguientes figuras.

Creación de la máquina Kali Linux.

Las máquinas virtuales ya creadas que proporciona Offensive Security para VMware están configuradas con Debian 8.x, por lo que para esta creación manual elegiremos también Debian 8.x en la versión 64bits, lo que afecta a las opciones avanzadas de virtualización disponibles más adelante en el apartado CPU como Intel VT-x/EPT, CPU performance counters e IOMMU (IO memory management unit).

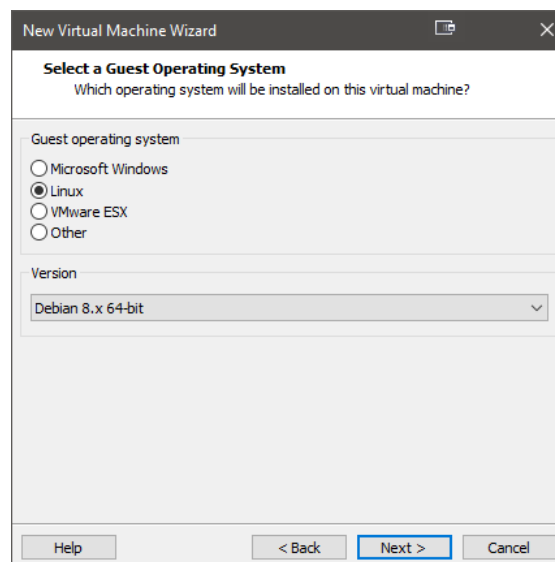


Figura 1 - Configuración VMware de la versión Linux de la máquina virtual.

Configuramos el nombre y la ruta.

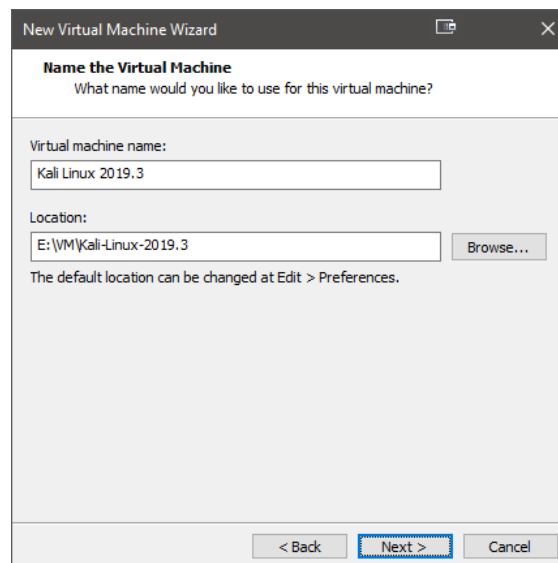


Figura 2 - Configuración del nombre y la ruta de la VM.

Como el host es capaz de 8 hilos de proceso configuraremos la VM con un procesador de 4 hilos.

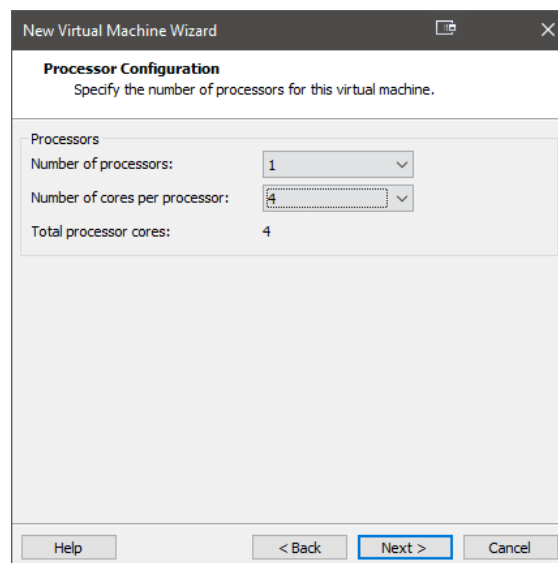


Figura 3 - Configuración de la CPU para la VM Kali.

Configuración de la memoria RAM, 2Gbytes de memoria son recomendados en la documentación de Kali.

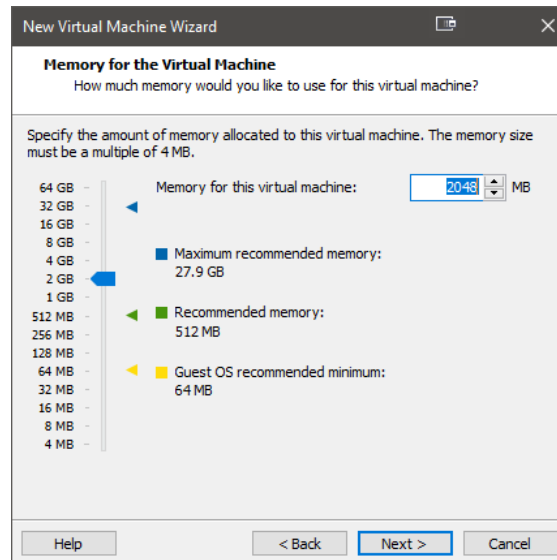


Figura 4 - Memoria RAM recomendada para Kali Linux.

Configuración de la red virtual en VMware que utilizara nuestra máquina virtual.

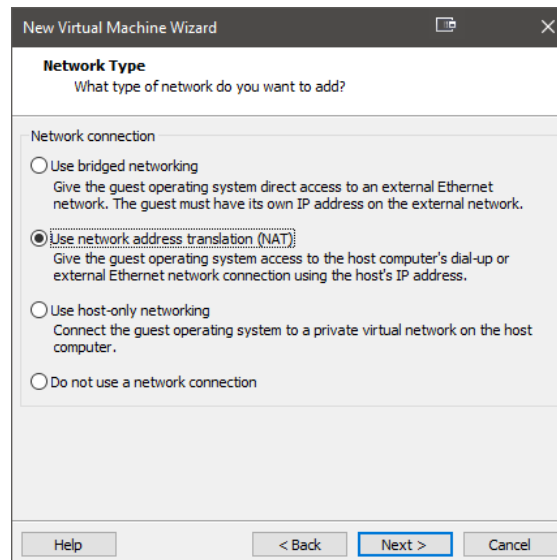


Figura 5 - Configuración de la red en modo NAT para la máquina Kali.

Finalizamos la creación de la maquina virtual dejando por defecto el resto de las opciones que no se han visto en las figuras y eliminando dispositivos virtuales en la maquina como la tarjeta de sonido y la impresora.

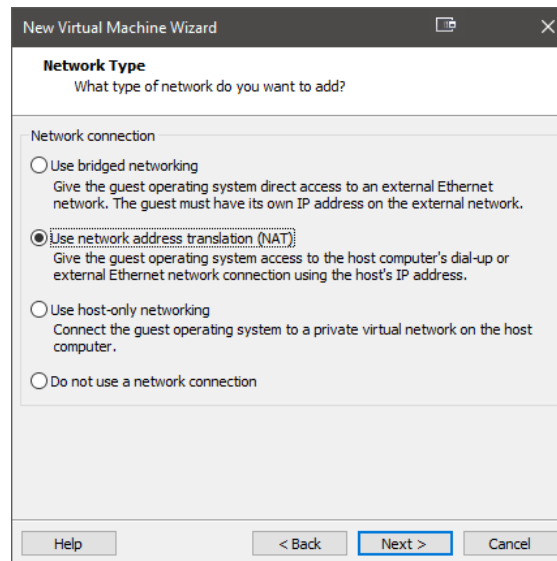


Figura 6 - Finalización de la configuración de la VM Kali.

Iniciamos la maquina y realizamos una instalación con la interfaz grafica en la que configuramos el hostname como Gon-Kali, así como todos los archivos en la misma partición (home, var y tmp).

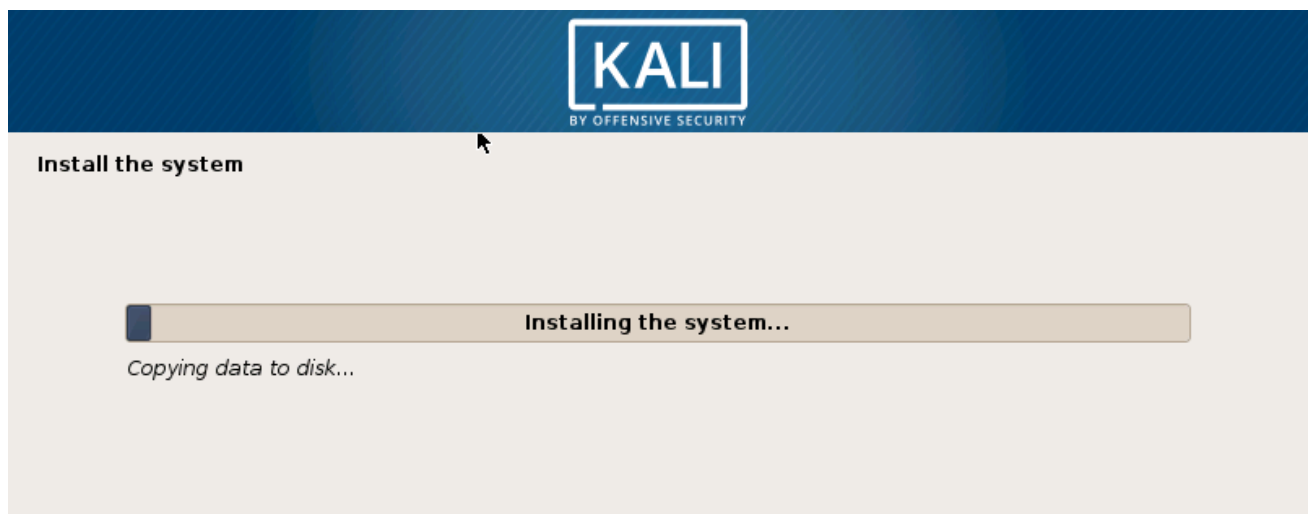


Figura 7 - Instalación de la ISO Kali en la máquina virtual.

Tras el reinicio del sistema y comprobación de que todo funciona correctamente procedemos a apagar la maquina y realizar un Snapshot para poder volver a un estado de recién instalado siempre que lo necesitemos.

Configuración de la red NAT en VMware.

Para aislar el laboratorio de pruebas en su propia red utilizaremos una configuraciónshut NAT, que consiste en una red de VMware conectada a un router virtual que hace de puente con la red del host.

La red será la siguiente: 192.168.100.0/24

La interfaz del router virtual que enlaza con la red del host tendrá la IP 192.168.100.254

Este router tendrá un servicio DHCP que otorgará direcciones IP en el rango 192.168.100.1 a 192.168.100.200

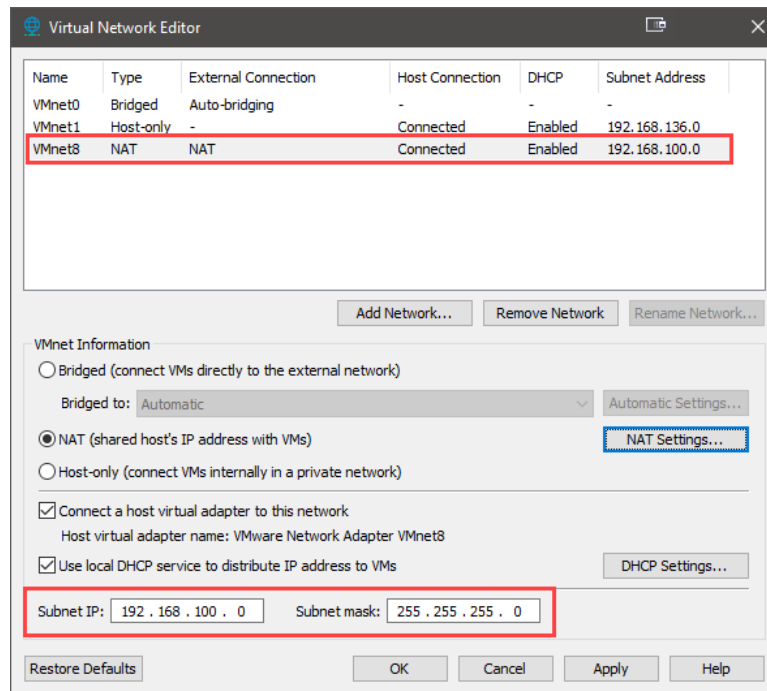


Figura 8 - Configuración de la red NAT en VMware.

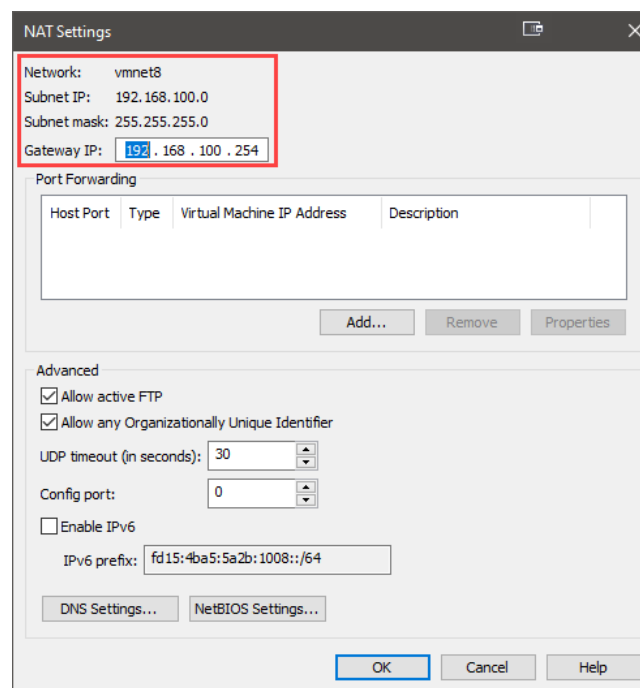


Figura 9 - Configuración de la puerta de enlace.

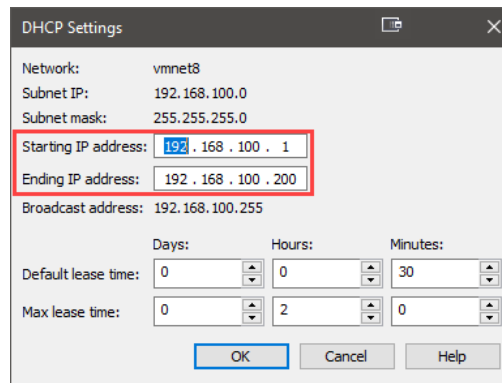


Figura 10 - Configuración del servicio DHCP.

Configuración de la VM Metasploitable 2.

La VM metasploitable viene creada en formato VMware por lo que la extraemos y añadimos VMware Workstation.

Tras agregar la maquina a VMware podemos observar que posee 2 interfaces de red virtuales instaladas en VMware una en modo NAT y otra en modo Host-Only.

Iniciamos la maquina y accedemos con el login y contraseña `msfadmin`.

```
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Sun Sep 15 11:10:25 EDT 2019 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ _
```

Figura 11 - Login y contraseña msfadmin.

Con el comando `ifconfig` comprobamos la configuración de las interfaces de red y podemos ver que `eth0` esta configurada para solicitar una IP mediante el servicio DHCP ya que ya tiene una dirección en la red como se puede ver en la siguiente figura.

```
Try 'uname --help' for more information.
msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:b0:e0:f0
          inet addr:192.168.100.1  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feb0:e0f0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:46 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5220 (5.0 KB)  TX bytes:7728 (7.5 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:121 errors:0 dropped:0 overruns:0 frame:0
          TX packets:121 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:33793 (33.0 KB)  TX bytes:33793 (33.0 KB)

msfadmin@metasploitable:~$
```

Figura 12 - Configuración de la interfaz de red `eth0` en metasploitable 2.

Comprobamos el resto de la configuración si la hubiese con `cat /etc/network/interfaces`

```
msfadmin@metasploitable:~$ cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet dhcp

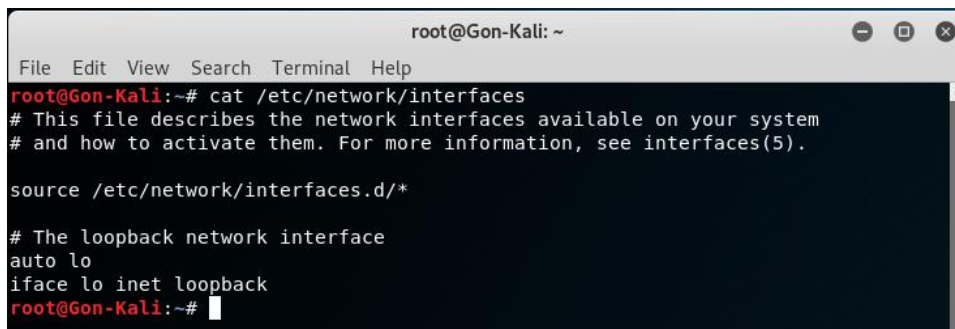
msfadmin@metasploitable:~$
```

Figura 13 - Comprobación de la configuración de interfaces de red en metasploitable 2.

La maquina esta en la red que queremos, ahora procedemos a configurar la VM Kali.

Configuración de la VM Kali en la red NAT.

Comprobamos la configuración del archivo `interfaces`.



```
root@Gon-Kali: ~
File Edit View Search Terminal Help
root@Gon-Kali:~# cat /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback
root@Gon-Kali:~#
```

Figura 14 - La máquina no cuenta con una configuración para `eth0`.

Este archivo no tiene configurada la interfaz `eth0`, pero a pesar de esto Kali en su interfaz grafica si dispone de una configuración y esta ha solicitado una IP al servicio DHCP de la red NAT de VMware, pero para centralizar la configuración y poder utilizar `ifdown` e `ifup` (lanzan un error diciendo que `eth0` no existe) procederemos a configurar el archivo `interfaces`, relanzar `eth0` mediante `ifup eth0` y finalmente comprobar la configuración, esto hará que la IP en alquiler otorgada por el servidor DHCP se encuentre ocupada (192.168.100.2) y se nos otorgue la siguiente (192.168.100.3).

```

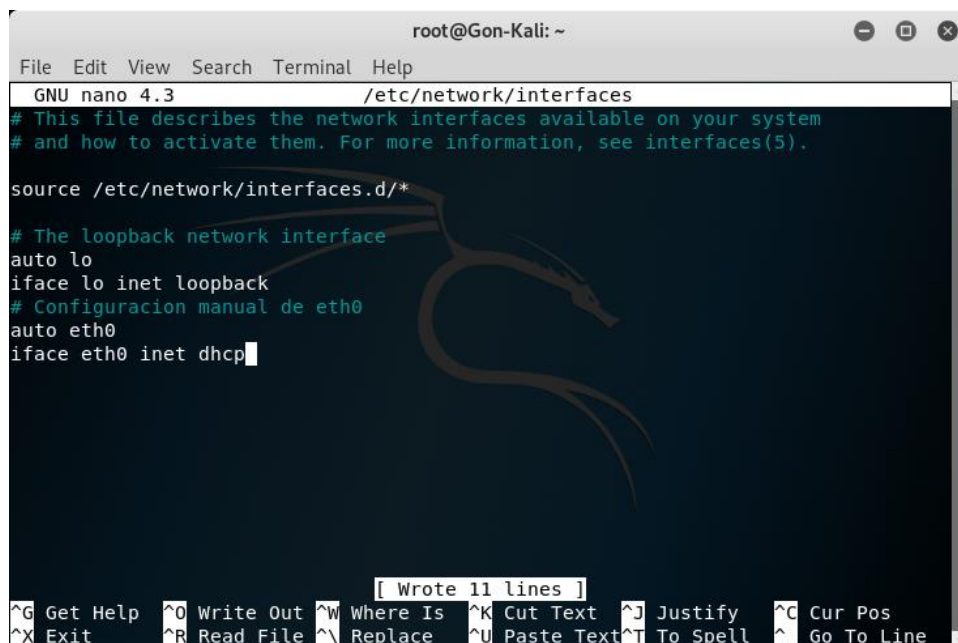
root@Gon-Kali:~# ifdown eth0
ifdown: unknown interface eth0
root@Gon-Kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.100.2 netmask 255.255.255.0 broadcast 192.168.100.255
    inet6 fe80::20c:29ff:fef1:137 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:f1:01:37 txqueuelen 1000 (Ethernet)
    RX packets 70 bytes 10780 (10.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 118 bytes 13502 (13.1 KiB)
    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 (Local Loopback)
    RX packets 20 bytes 1116 (1.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 20 bytes 1116 (1.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Figura 15 - eth0 funcionando a pesar de que interfaces no sabe nada de esto.

Configuramos eth0 para solicitar una dirección IP mediante DHCP.



```

root@Gon-Kali: ~
File Edit View Search Terminal Help
GNU nano 4.3 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback
# Configuración manual de eth0
auto eth0
iface eth0 inet dhcp

```

Figura 16 - Configuración interfaces en Kali Linux.

Levantamos eth0 con `ifup` y obtenemos una dirección nueva del servicio DHCP, 192.168.100.3 que

```

root@Gon-Kali:~# ifup eth0
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/00:0c:29:f1:01:37
Sending on LPF/eth0/00:0c:29:f1:01:37
Sending on Socket/fallback
Created duid "\000\001\000\001%\021\0258\000\014)\361\0017".
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 6
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 11
DHCPOFFER of 192.168.100.3 from 192.168.100.200
DHCPREQUEST for 192.168.100.3 on eth0 to 255.255.255.255 port 67
DHCPACK of 192.168.100.3 from 192.168.100.200
bound to 192.168.100.3 -- renewal in 710 seconds.

```

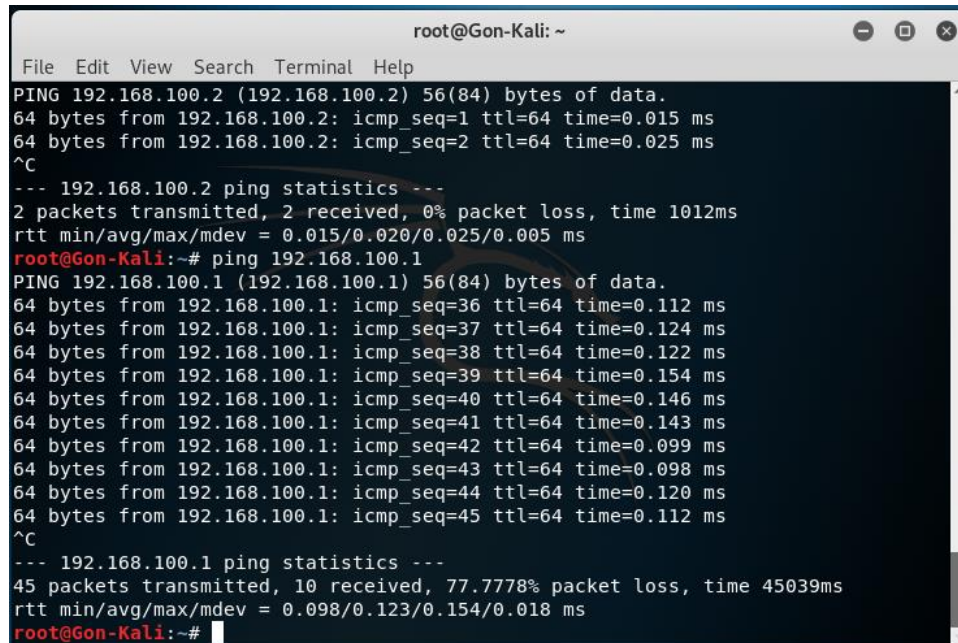
Figura 17 - Levantamos eth0 con `ifup`.

Comprobación e interpretación de la comunicación entre las VM.

Tras reiniciar la máquina Kali para evitar conflictos con la configuración por defecto de la interfaz gráfica procedemos a comprobar si las máquinas pueden comunicarse mediante un sencillo ping.

Podemos observar que el TTL (time to live) de los paquetes es de 64 saltos, indicativo de que la respuesta probablemente procede de una máquina Linux.

También se observa que en la primera comunicación existe packet loss, esto es debido a que la primera vez que la solicitud es enviada el router virtual tiene que enviar una solicitud ARP para conocer la MAC del destino y posteriormente establecer la comunicación, mientras esta tarea no se complete las peticiones no obtienen respuesta.

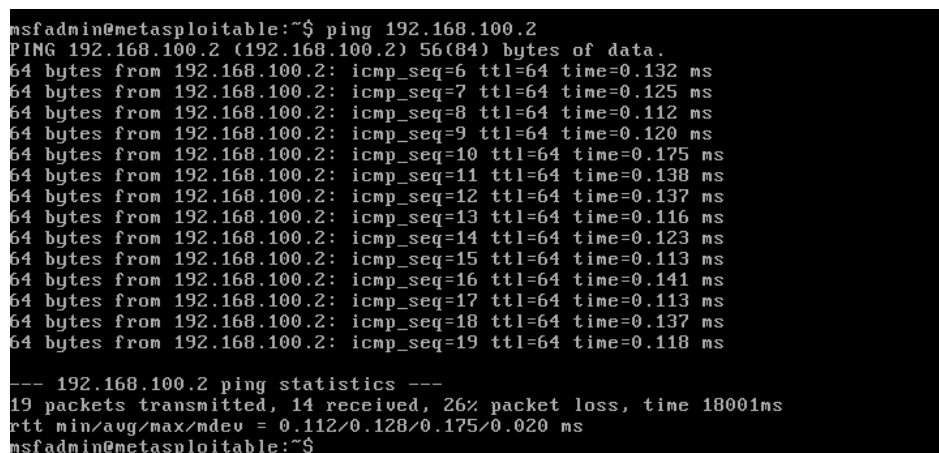


```

root@Gon-Kali: ~
File Edit View Search Terminal Help
PING 192.168.100.2 (192.168.100.2) 56(84) bytes of data.
64 bytes from 192.168.100.2: icmp_seq=1 ttl=64 time=0.015 ms
64 bytes from 192.168.100.2: icmp_seq=2 ttl=64 time=0.025 ms
^C
--- 192.168.100.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1012ms
rtt min/avg/max/mdev = 0.015/0.020/0.025/0.005 ms
root@Gon-Kali:~# ping 192.168.100.1
PING 192.168.100.1 (192.168.100.1) 56(84) bytes of data.
64 bytes from 192.168.100.1: icmp_seq=36 ttl=64 time=0.112 ms
64 bytes from 192.168.100.1: icmp_seq=37 ttl=64 time=0.124 ms
64 bytes from 192.168.100.1: icmp_seq=38 ttl=64 time=0.122 ms
64 bytes from 192.168.100.1: icmp_seq=39 ttl=64 time=0.154 ms
64 bytes from 192.168.100.1: icmp_seq=40 ttl=64 time=0.146 ms
64 bytes from 192.168.100.1: icmp_seq=41 ttl=64 time=0.143 ms
64 bytes from 192.168.100.1: icmp_seq=42 ttl=64 time=0.099 ms
64 bytes from 192.168.100.1: icmp_seq=43 ttl=64 time=0.098 ms
64 bytes from 192.168.100.1: icmp_seq=44 ttl=64 time=0.120 ms
64 bytes from 192.168.100.1: icmp_seq=45 ttl=64 time=0.112 ms
^C
--- 192.168.100.1 ping statistics ---
45 packets transmitted, 10 received, 77.7778% packet loss, time 45039ms
rtt min/avg/max/mdev = 0.098/0.123/0.154/0.018 ms
root@Gon-Kali:~#

```

Figura 18 - PING desde VM Kali.



```

msfadmin@metasploitable:~$ ping 192.168.100.2
PING 192.168.100.2 (192.168.100.2) 56(84) bytes of data.
64 bytes from 192.168.100.2: icmp_seq=6 ttl=64 time=0.132 ms
64 bytes from 192.168.100.2: icmp_seq=7 ttl=64 time=0.125 ms
64 bytes from 192.168.100.2: icmp_seq=8 ttl=64 time=0.112 ms
64 bytes from 192.168.100.2: icmp_seq=9 ttl=64 time=0.120 ms
64 bytes from 192.168.100.2: icmp_seq=10 ttl=64 time=0.175 ms
64 bytes from 192.168.100.2: icmp_seq=11 ttl=64 time=0.138 ms
64 bytes from 192.168.100.2: icmp_seq=12 ttl=64 time=0.137 ms
64 bytes from 192.168.100.2: icmp_seq=13 ttl=64 time=0.116 ms
64 bytes from 192.168.100.2: icmp_seq=14 ttl=64 time=0.123 ms
64 bytes from 192.168.100.2: icmp_seq=15 ttl=64 time=0.113 ms
64 bytes from 192.168.100.2: icmp_seq=16 ttl=64 time=0.141 ms
64 bytes from 192.168.100.2: icmp_seq=17 ttl=64 time=0.113 ms
64 bytes from 192.168.100.2: icmp_seq=18 ttl=64 time=0.137 ms
64 bytes from 192.168.100.2: icmp_seq=19 ttl=64 time=0.118 ms
--- 192.168.100.2 ping statistics ---
19 packets transmitted, 14 received, 26% packet loss, time 18001ms
rtt min/avg/max/mdev = 0.112/0.128/0.175/0.020 ms
msfadmin@metasploitable:~$

```

Figura 19 - PING desde Metasploitable2.