



Carátula para entrega de prácticas

Facultad de Ingeniería

Laboratorios de docencia

Laboratorio de Redes y Seguridad

Profesor: MTRO. CÉSAR SANABRIA PINEDA

Asignatura: LABORATORIO DE SEGURIDAD INFORMÁTICA AVANZADA

Grupo: 02

No de Práctica: Práctica 1: Preparación de los escenarios de uso

Integrante(s): Rodrigo Macías Eljure

*No. de Equipo de
cómputo empleado:* No aplica

Semestre: 2021-2

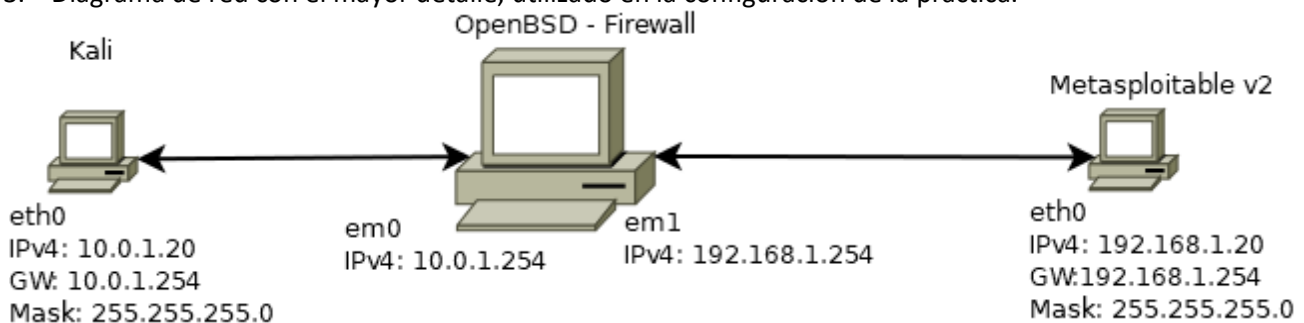
Fecha de entrega: 1 de septiembre 2023

Observaciones:

CALIFICACIÓN: _____

Sección 1: Introducción

1. ¿Cuáles son las características generales y posibles escenarios de uso de los siguientes sistemas operativos?
 - A) Kali Linux: Es una distribución de Linux basada en Debian enfocada en ciberseguridad y seguridad de la información. Cuenta con varias herramientas precargadas. Principalmente se utiliza para Pentesting y auditorías de seguridad, aunque también podría llegar a ser utilizada para hardening de redes caseras e incluso delitos cibernéticos.
 - B) Metasploitable v2: Se trata de una máquina virtual de Linux que cuenta con vulnerabilidades a propósito, con el fin de crear un ambiente seguro para practicar y aprender sobre ciberseguridad y pentesting. Cuenta con una documentación detallada sobre las vulnerabilidades existentes y está pensada para ser utilizada con el framework Metasploit.
 - C) Metasploitable is an intentionally vulnerable Linux virtual machine. This VM can be used to conduct security training, test security tools, and practice common penetration testing techniques.
 - D) OpenBSD: OpenBSD es un sistema operativo de código abierto basado en la rama "Berkeley Unix" desarrollada por primera vez en la década de 1970. Es bastante similar a Linux, pero existen algunas diferencias importantes. Mientras que las distribuciones de Linux incluyen el núcleo y varias utilidades adicionales, OpenBSD se desarrolla como un sistema completo.
2. URL's de descarga de software y sistemas operativos utilizados.
 - A) Kali Linux <https://www.kali.org/>
 - B) Metasploitable v2 <https://sourceforge.net/projects/metasploitable/>
 - C) OpenBSD <https://cdn.openbsd.org/pub/OpenBSD/7.2/>
 - D) VirtualBox: <https://www.virtualbox.org/wiki/Downloads>
3. Diagrama de red con el mayor detalle, utilizado en la configuración de la práctica.



Sección 2: Informe de la práctica

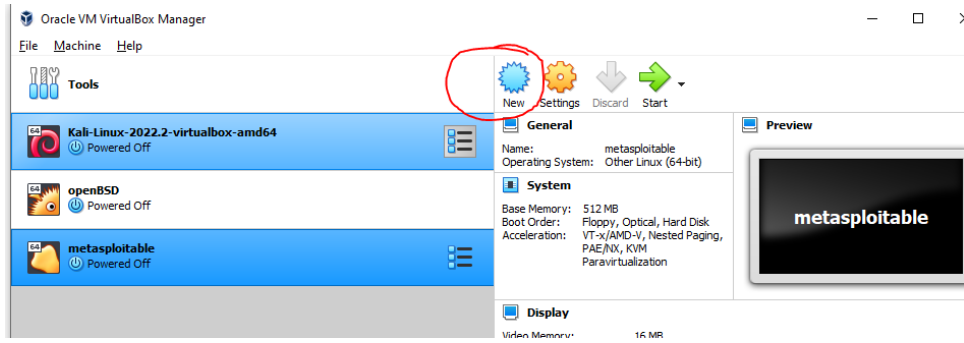
Instalación de máquinas virtuales:

El primer paso fue instalar el software VirtualBox desde el enlace <https://www.virtualbox.org/wiki/Downloads>, siguiendo el instalador descargado.

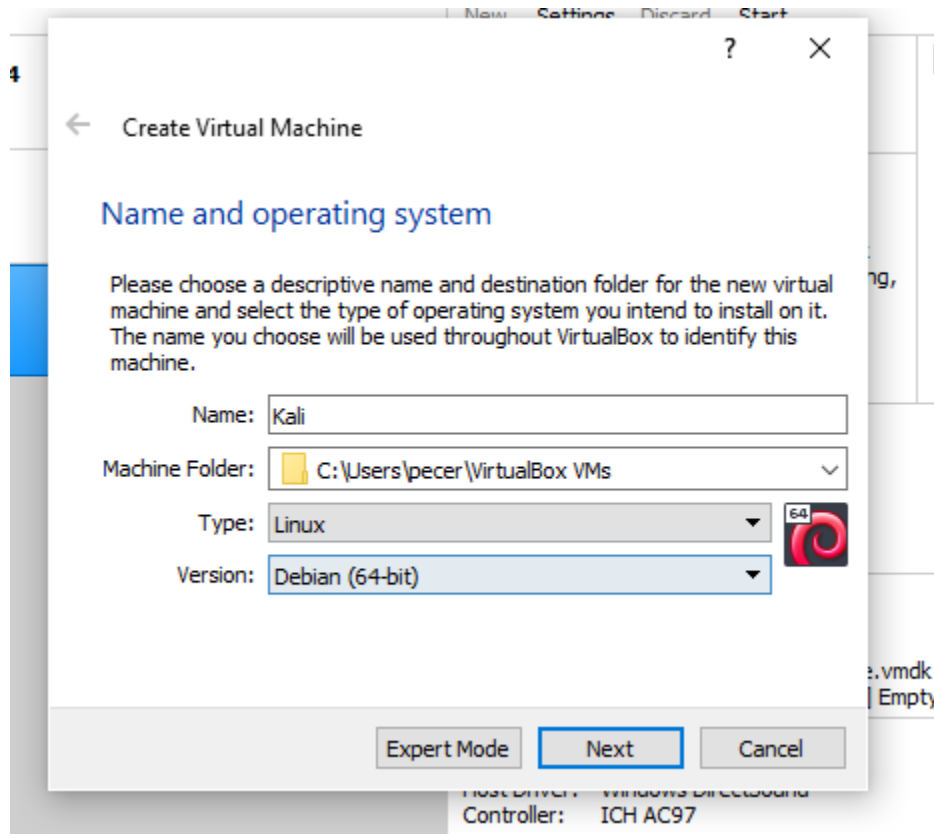
Después, verificamos que la virtualización se encuentra activada, entrando al BIOS de la computadora usada y habilitando la opción "Enable Virtualization technologies". Éste proceso depende de cada fabricante de tarjetas.

Posteriormente se tuvo que obtener imágenes .iso de los instaladores de las distribuciones de Linux Kali, OpenBSD y Metasploitable desde sus respectivos enlaces.

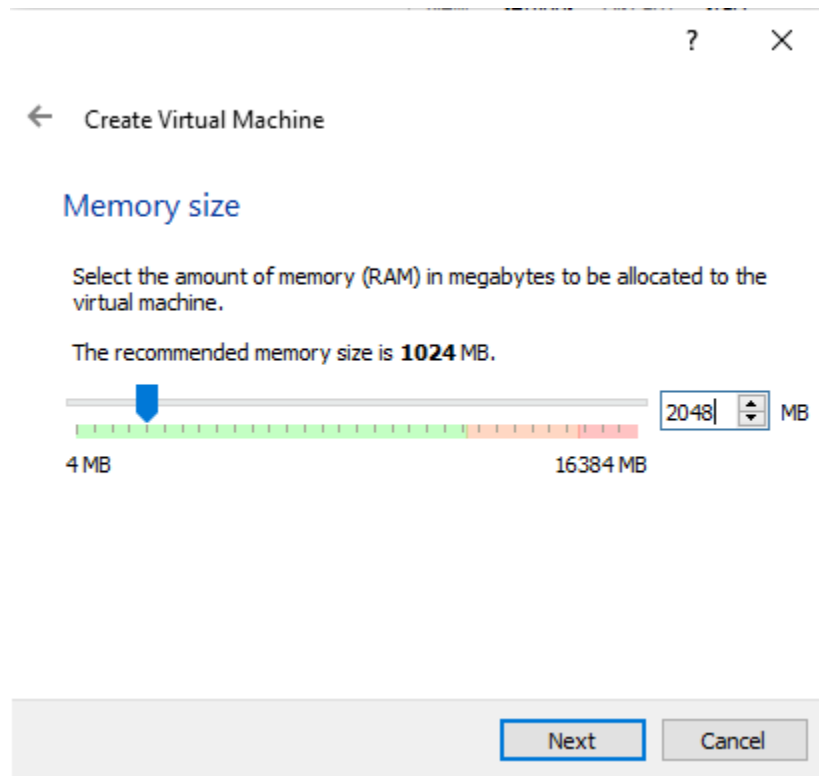
Una vez que se obtuvieron las imágenes de disco procedí a crear las máquinas virtuales ejecutando el programa VirtualBox y haciendo click en el botón NEW:



En este ejemplo muestro cómo instalé Kali, por lo que utilicé la siguiente configuración:

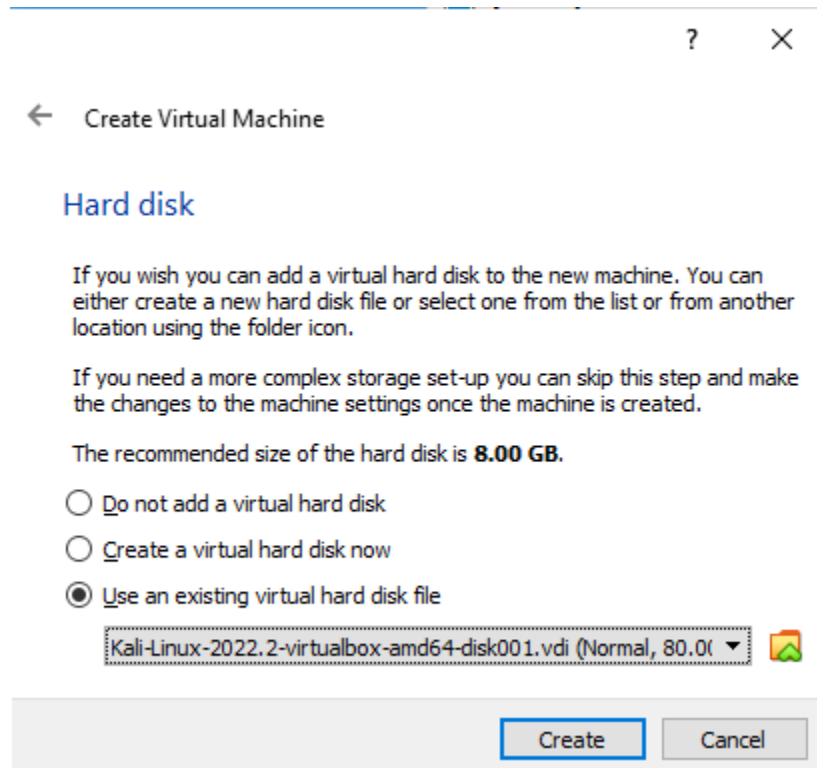


Luego pidió asignar la cantidad de RAM para la máquina virtual. En el caso de Kali le asigné 2048 MB, en el caso de OpenBSD y Metasploitable le asigné 1024 MB.

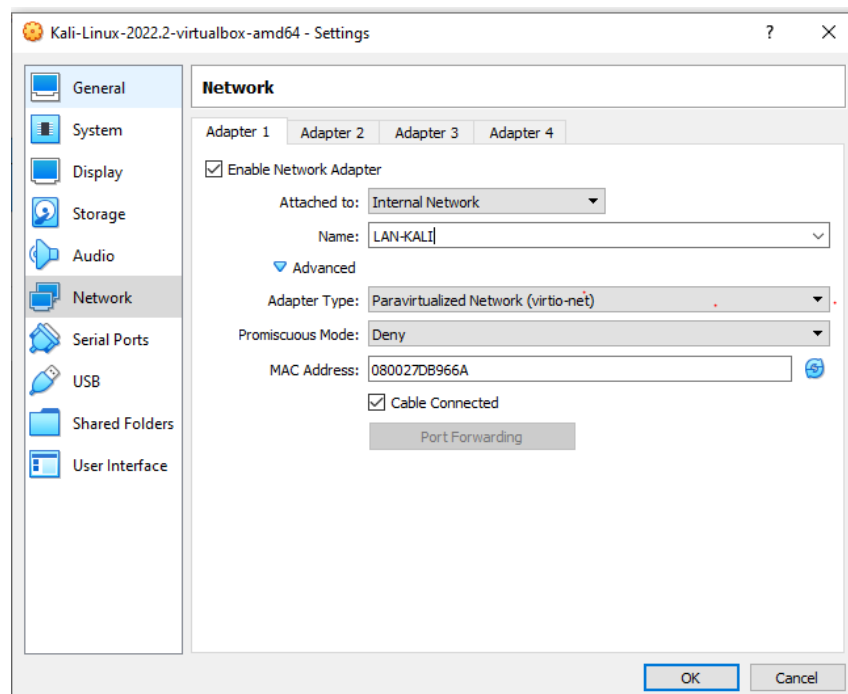


Como seleccioné la opción de máquinas virtuales de Kali, descargué un archivo comprimido en formato .7z, que dentro tenía una carpeta con dos archivos: **kali-linux-2023.3-virtualbox-amd64.vbox** y **kali-linux-2023.3-virtualbox-amd64.vdi**.

Seleccioné la opción .vdi:



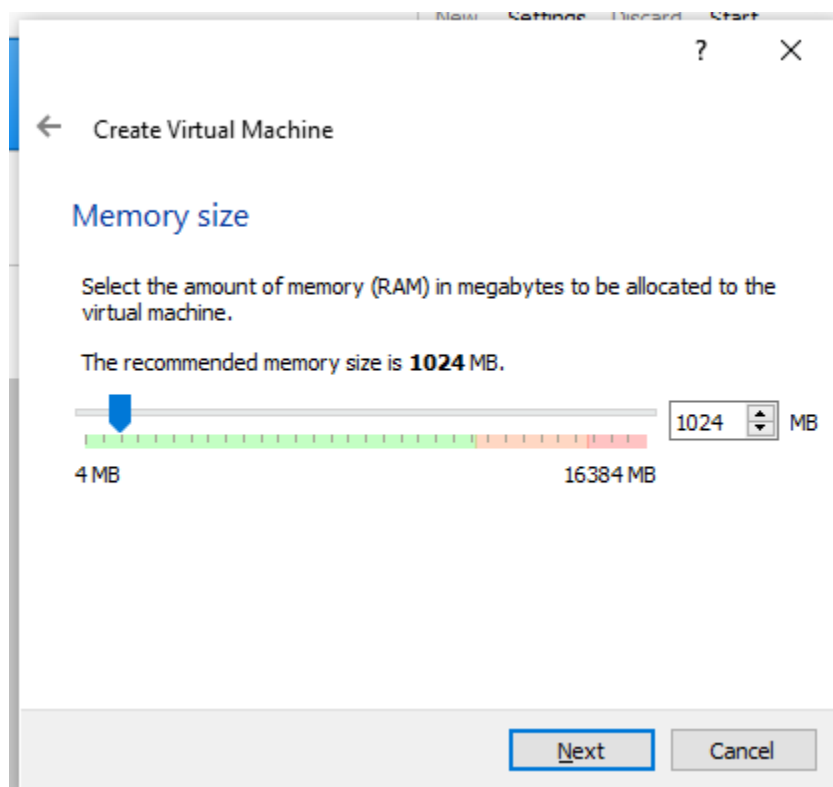
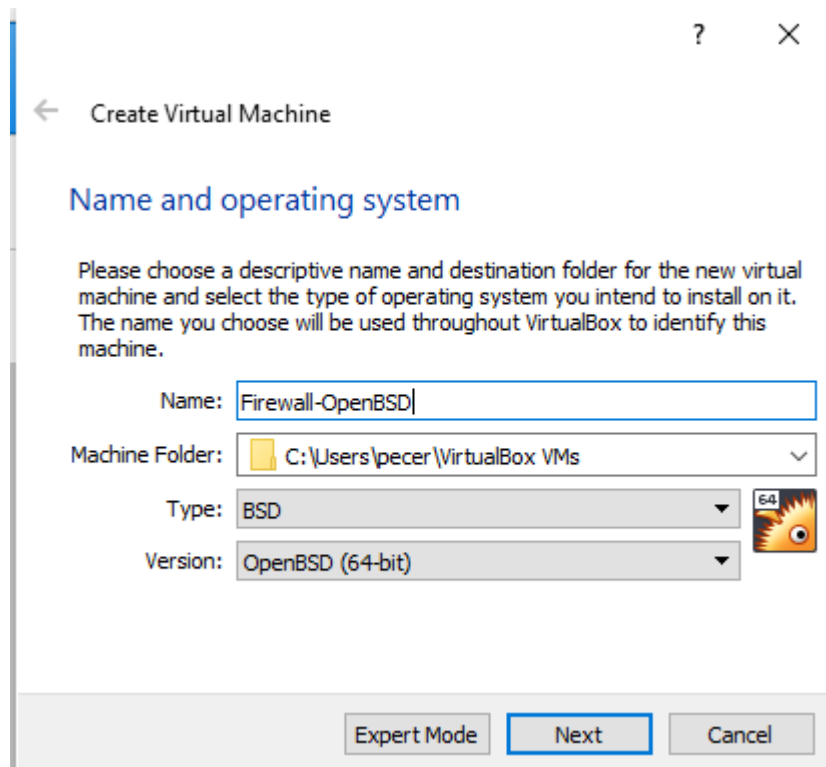
Una vez creado se tiene que configurar los adaptadores de red:

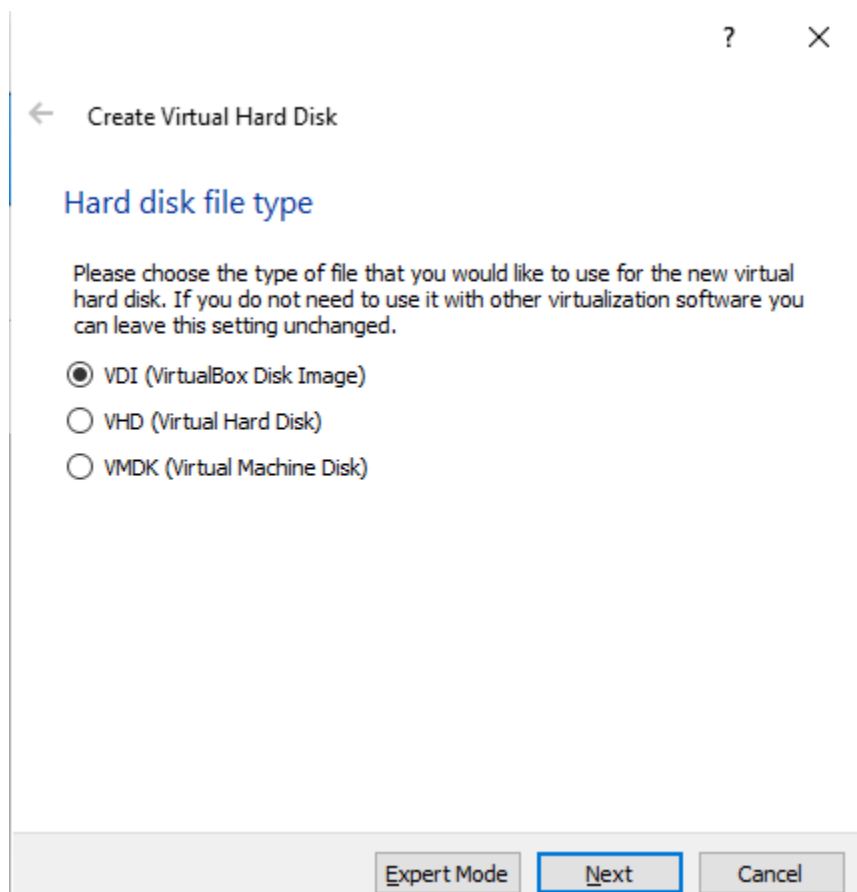
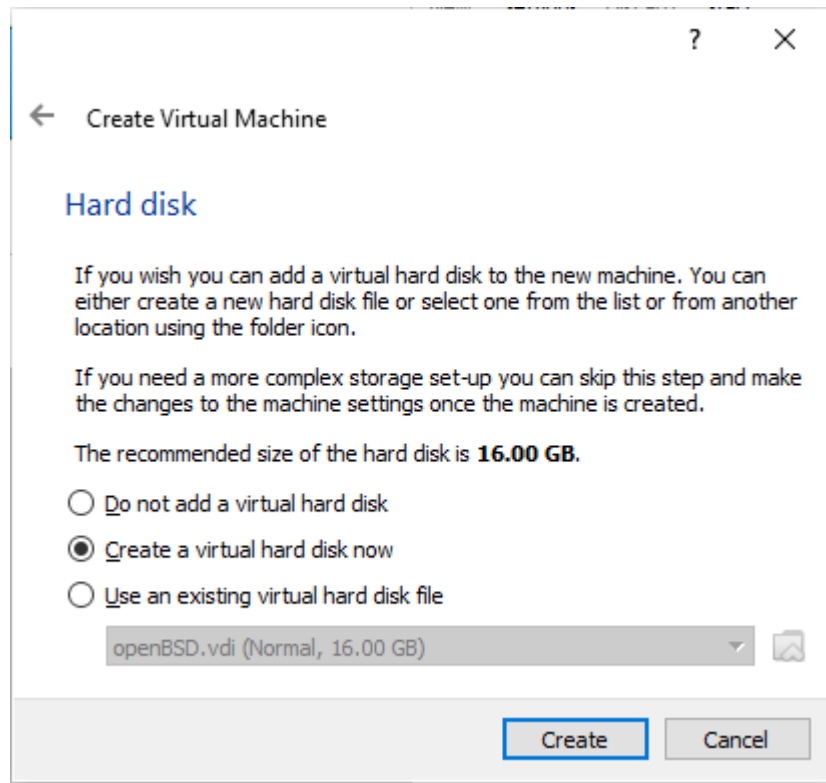


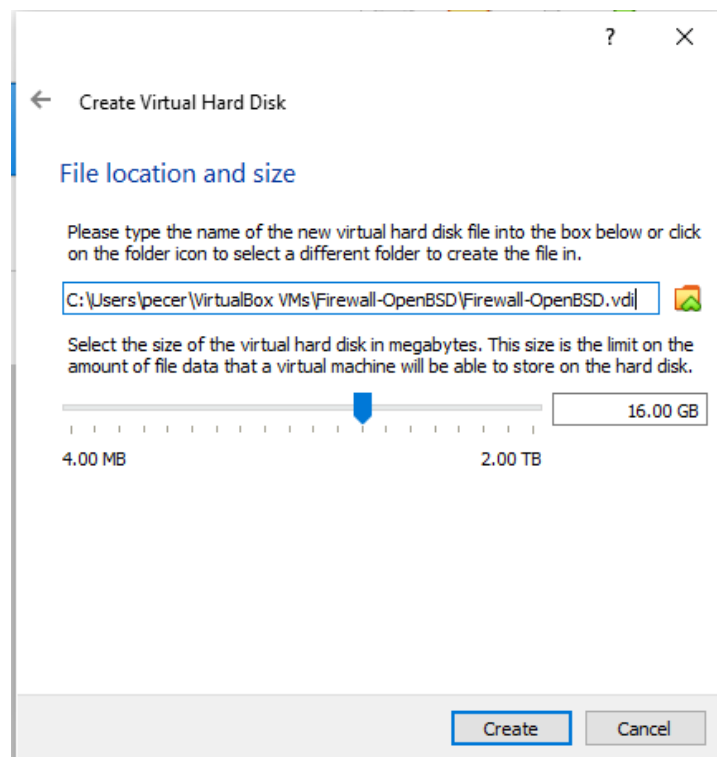
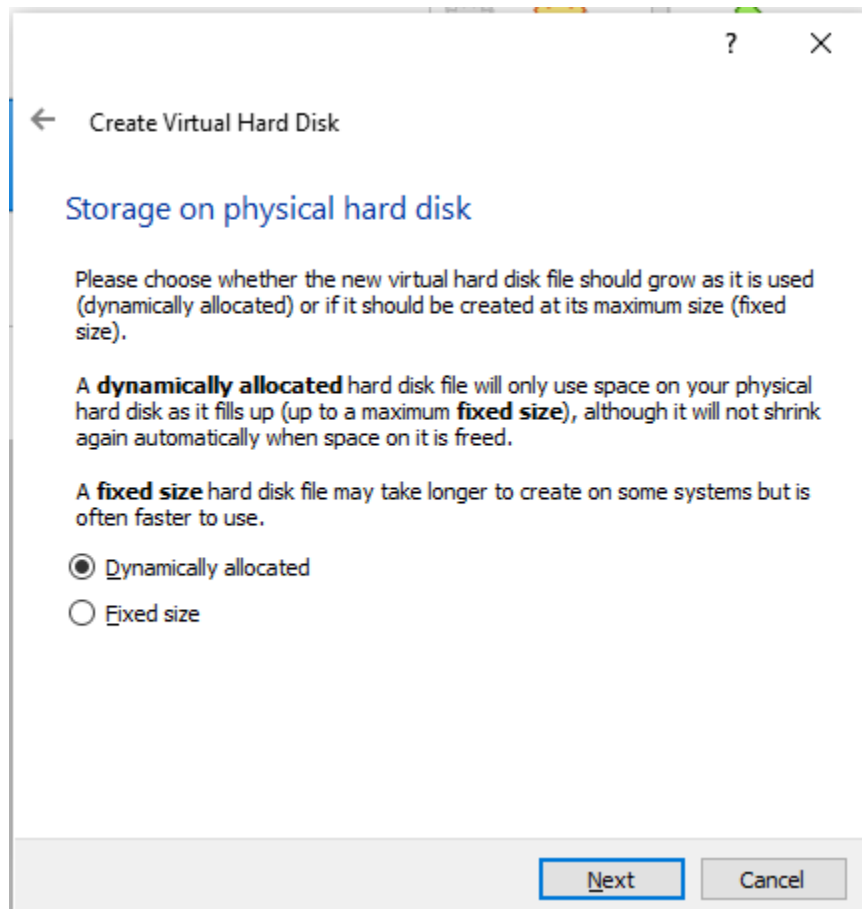
Para la máquina de Metasploitable el proceso es idéntico al de kali-linux, pero usando su respectivo archivo descomprimido.

Para OpenBSD el proceso es un poco diferente, la configuración es la siguiente:

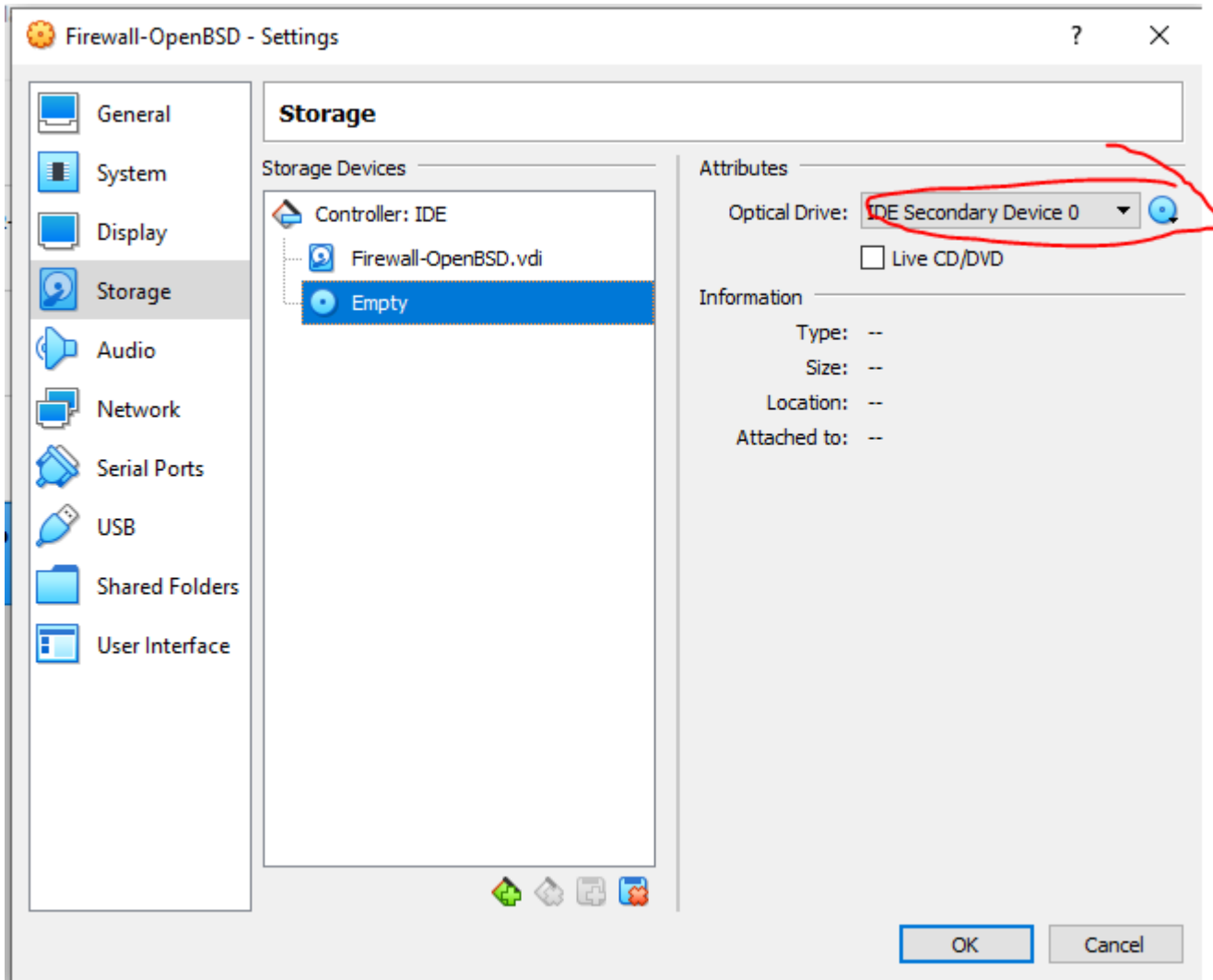
La versión utilizada de OpenBSD es la 72, puesto que la 73 presentó muchos problemas en la instalación.





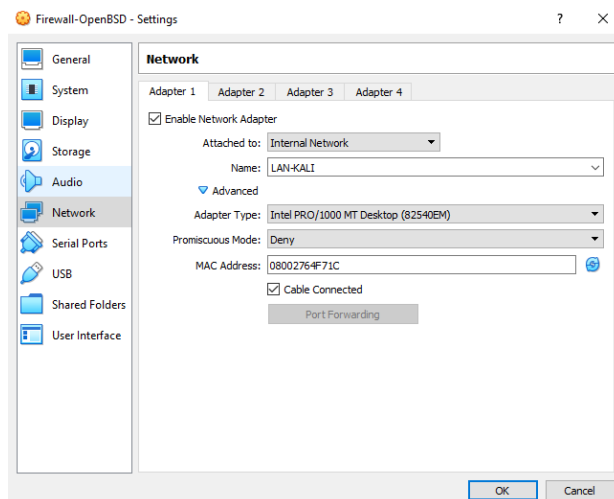


Una vez terminados los pasos anteriores seleccioné Settings > Storage > Empty para cargar la imagen de disco:

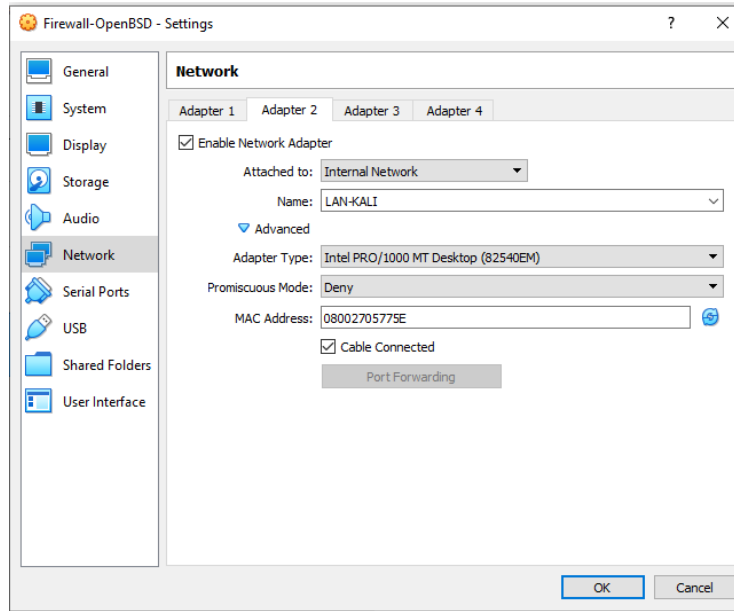


Luego seleccioné la imagen de disco.

Posteriormente configuré los dos adaptadores de red, en Network> Adapter #:



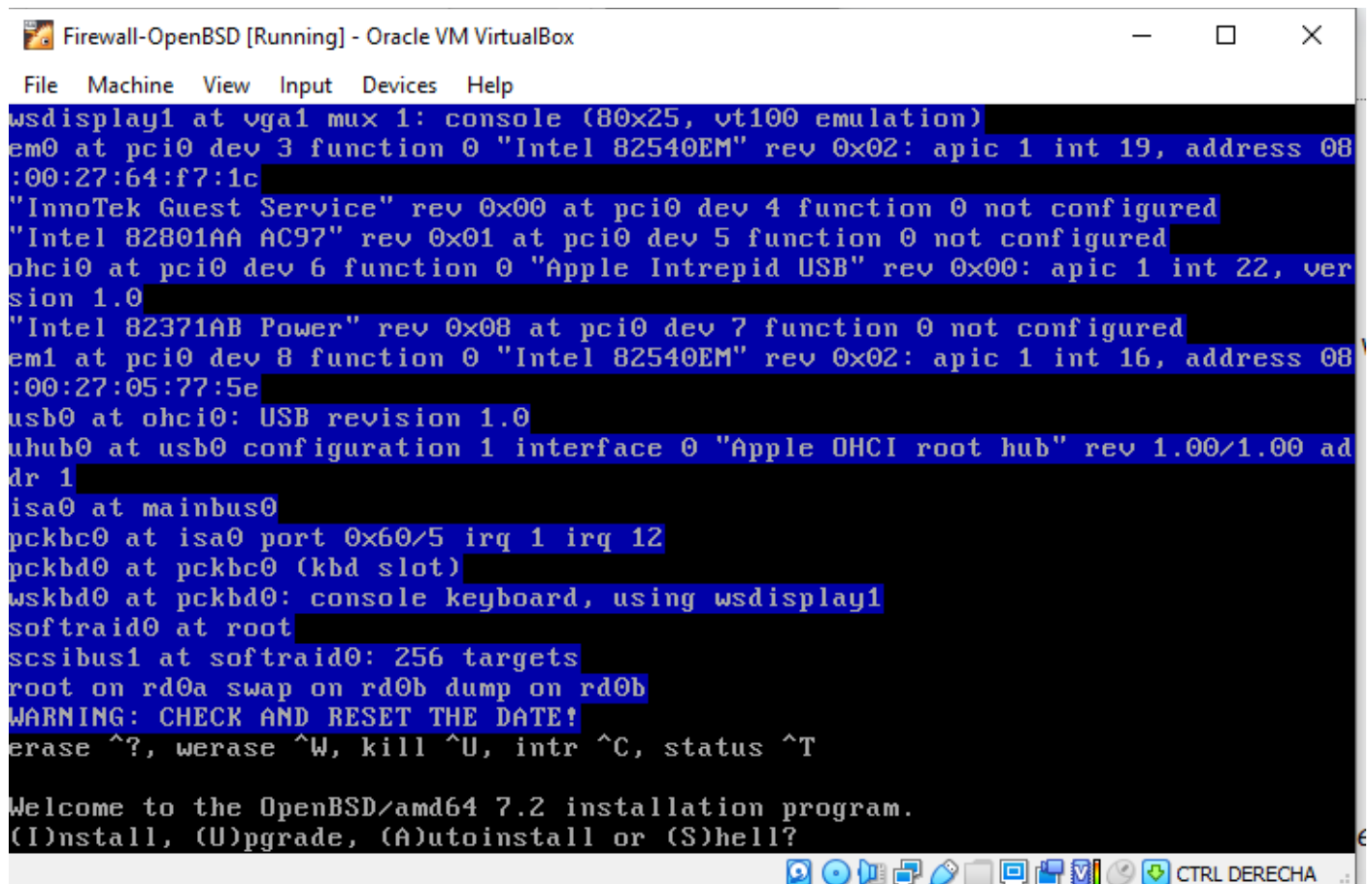
El segundo adaptador tiene la siguiente configuración:



Todas las máquinas virtuales deben de tener el mismo nombre de Internal Network.

Pulsé OK y luego fui a iniciar la instalación de OpenBSD, ejecutando la máquina virtual recién creada.

Esperé a que terminara de cargar el instalador hasta que apareció el siguiente mensaje:



Las instrucciones usadas son las siguientes:

```
Firewall-OpenBSD [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Welcome to the OpenBSD/amd64 7.2 installation program.
(I)nstall, (U)pgrade, (A)utoinstall or (S)hell? i
At any prompt except password prompts you can escape to a shell by
typing '!'. Default answers are shown in []'s and are selected by
pressing RETURN. You can exit this program at any time by pressing
Control-C, but this can leave your system in an inconsistent state.

Choose your keyboard layout ('?' or 'L' for list) [default] es
System hostname? (short form, e.g. 'foo') area51

Available network interfaces are: em0 em1 vlan0.
Which network interface do you wish to configure? (or 'done') [em0] em0
IPv4 address for em0? (or 'autoconf' or 'none') [autoconf] 10.0.1.254
Netmask for em0? [255.255.255.0]
IPv6 address for em0? (or 'autoconf' or 'none') [none]
Available network interfaces are: em0 em1 vlan0.
Which network interface do you wish to configure? (or 'done') [done] em1
Symbolic (host) name for em1? [area51]
IPv4 address for em1? (or 'autoconf' or 'none') [autoconf] 192.168.1.254
Netmask for em1? [255.255.255.0]
IPv6 address for em1? (or 'autoconf' or 'none') [none]
Available network interfaces are: em0 em1 vlan0.
Which network interface do you wish to configure? (or 'done') [done]
Default IPv4 route? (IPv4 address or none)
```

```
Firewall-OpenBSD [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Which network interface do you wish to configure? (or 'done') [done] em1
Symbolic (host) name for em1? [area51]
IPv4 address for em1? (or 'autoconf' or 'none') [autoconf] 192.168.1.254
Netmask for em1? [255.255.255.0]
IPv6 address for em1? (or 'autoconf' or 'none') [none]
Available network interfaces are: em0 em1 vlan0.
Which network interface do you wish to configure? (or 'done') [done]
Default IPv4 route? (IPv4 address or none) 192.168.1.254
add net default: gateway 192.168.1.254
DNS domain name? (e.g. 'example.com') [my.domain]
DNS nameservers? (IP address list or 'none') [none]

Password for root account? (will not echo)
Password for root account? (again)
Start sshd(8) by default? [yes]
Do you expect to run the X Window System? [yes] no
Setup a user? (enter a lower-case loginname, or 'no') [no] roy
Full name for user roy? [roy] roy
Password for user roy? (will not echo)
Password for user roy? (again)
WARNING: root is targeted by password guessing attacks, pubkeys are safer.
Allow root ssh login? (yes, no, prohibit-password) [no]

Available disks are: wd0.
Which disk is the root disk? ('?' for details) [wd0]
```

```
Firewall-OpenBSD [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Full name for user roy? [roy] roy
Password for user roy? (will not echo)
Password for user roy? (again)
WARNING: root is targeted by password guessing attacks, pubkeys are safer.
Allow root ssh login? (yes, no, prohibit-password) [no]

Available disks are: wd0.
Which disk is the root disk? ('?' for details) [wd0]
No valid MBR or GPT.
Use (W)hole disk MBR, whole disk (G)PT or (E)dit? [whole]
Setting OpenBSD MBR partition to whole wd0...done.
The auto-allocated layout for wd0 is:
#          size      offset  fstype  [fsize bsize  cpgh]
a:         420.1M         64  4.2BSD   2048 16384    1 # /
b:         620.2M      860416    swap
c:        16384.0M         0  unused
d:         552.1M     2130592  4.2BSD   2048 16384    1 # /tmp
e:         782.2M     3261376  4.2BSD   2048 16384    1 # /var
f:        2040.2M     4863424  4.2BSD   2048 16384    1 # /usr
g:         546.0M     9041728  4.2BSD   2048 16384    1 # /usr/X11R6
h:        1834.3M    10160032  4.2BSD   2048 16384    1 # /usr/local
i:        1608.0M    13916640  4.2BSD   2048 16384    1 # /usr/src
j:         5336.1M    17209888  4.2BSD   2048 16384    1 # /usr/obj
k:         2644.7M    28138176  4.2BSD   2048 16384    1 # /home
Use (A)uto layout, (E)dit auto layout, or create (C)ustom layout? [a] _
```

```
Firewall-OpenBSD [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/dev/wd0j (4d57aa14f6668a1b.j) on /mnt/usr/obj type ffs (rw, asynchronous, local,
, nodev, nosuid)
/dev/wd0i (4d57aa14f6668a1b.i) on /mnt/usr/src type ffs (rw, asynchronous, local
, nodev, nosuid)
/dev/wd0e (4d57aa14f6668a1b.e) on /mnt/var type ffs (rw, asynchronous, local, no
dev, nosuid)

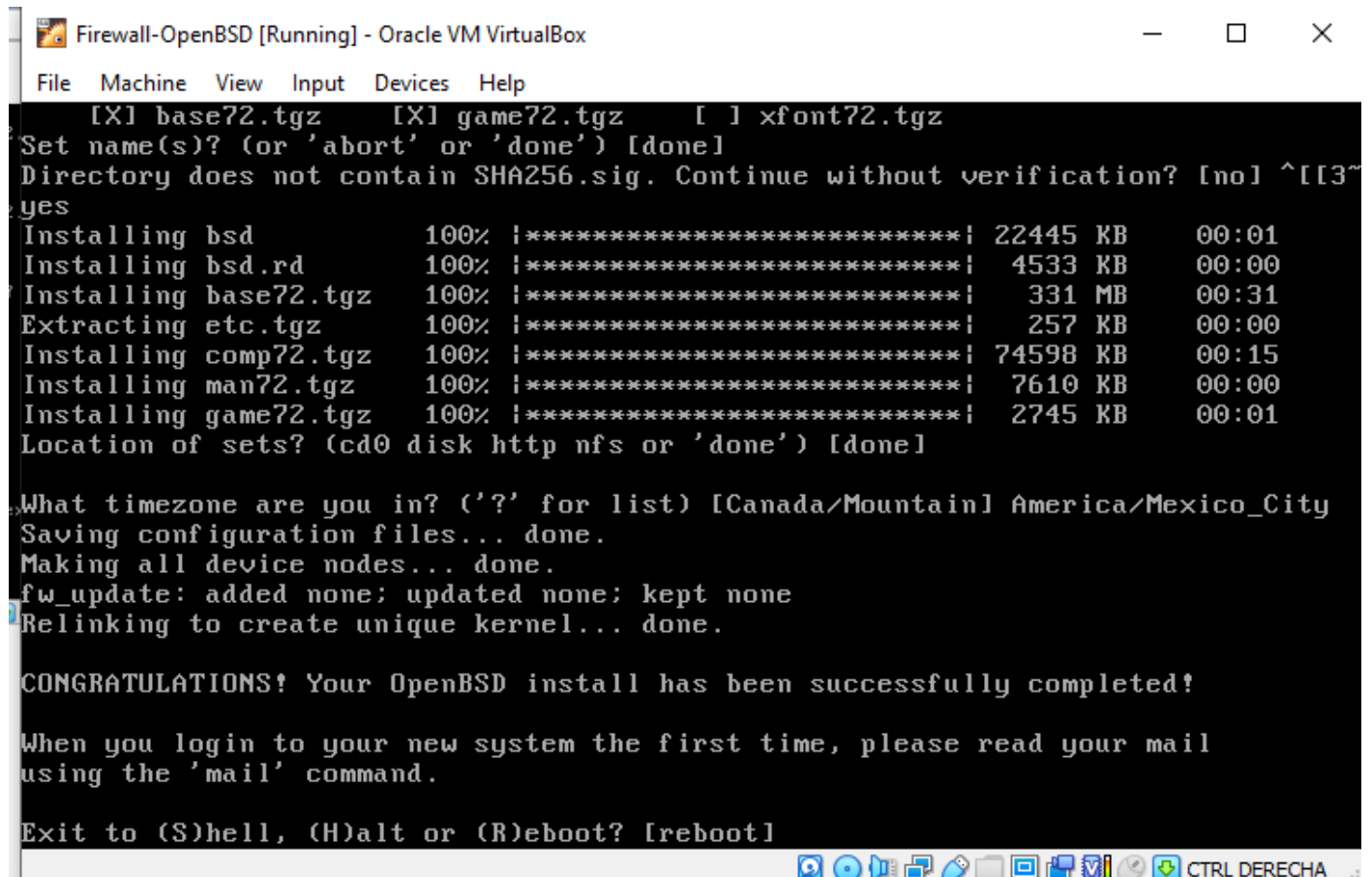
Let's install the sets!
Location of sets? (cd0 disk http nfs or 'done') [cd0]
Pathname to the sets? (or 'done') [/7.2/amd64]

Select sets by entering a set name, a file name pattern or 'all'. De-select
sets by prepending a '-', e.g.: '-game*'. Selected sets are labelled '[X]'.
[X] bsd [X] comp72.tgz [X] xbase72.tgz [X] xserv72.tgz
[X] bsd.rd [X] man72.tgz [X] xshare72.tgz
[X] base72.tgz [X] game72.tgz [X] xfont72.tgz
Set name(s)? (or 'abort' or 'done') [done] -x*
[X] bsd [X] comp72.tgz [ ] xbase72.tgz [ ] xserv72.tgz
[X] bsd.rd [X] man72.tgz [ ] xshare72.tgz
[X] base72.tgz [X] game72.tgz [ ] xfont72.tgz
Set name(s)? (or 'abort' or 'done') [done] -g
[X] bsd [X] comp72.tgz [ ] xbase72.tgz [ ] xserv72.tgz
[X] bsd.rd [X] man72.tgz [ ] xshare72.tgz
[X] base72.tgz [X] game72.tgz [ ] xfont72.tgz
Set name(s)? (or 'abort' or 'done') [done] ^[
```

```
Firewall-OpenBSD [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Set name(s)? (or 'abort' or 'done') [done] -x*
[X] bsd [X] comp72.tgz [ ] xbase72.tgz [ ] xserv72.tgz
[X] bsd.rd [X] man72.tgz [ ] xshare72.tgz
[X] base72.tgz [X] game72.tgz [ ] xfont72.tgz
Set name(s)? (or 'abort' or 'done') [done] -g
[X] bsd [X] comp72.tgz [ ] xbase72.tgz [ ] xserv72.tgz
[X] bsd.rd [X] man72.tgz [ ] xshare72.tgz
[X] base72.tgz [X] game72.tgz [ ] xfont72.tgz
Set name(s)? (or 'abort' or 'done') [done]
Directory does not contain SHA256.sig. Continue without verification? [no] ^[[3~
yes
Installing bsd 100% |*****| 22445 KB 00:01
Installing bsd.rd 100% |*****| 4533 KB 00:00
Installing base72.tgz 100% |*****| 331 MB 00:31
Extracting etc.tgz 100% |*****| 257 KB 00:00
Installing comp72.tgz 100% |*****| 74598 KB 00:15
Installing man72.tgz 100% |*****| 7610 KB 00:00
Installing game72.tgz 100% |*****| 2745 KB 00:01
Location of sets? (cd0 disk http nfs or 'done') [done]

What timezone are you in? ('?' for list) [Canada/Mountain] America/Mexico_City
Saving configuration files... done.
Making all device nodes... done.
fw_update: added none; updated none; kept none
Relinking to create unique kernel..._
CTRL DERECHA
```

Cuando salió el siguiente mensaje configuré la unidad de disco de la máquina virtual para quitar la imagen de disco y apagué la máquina virtual.



```
[X] base72.tgz      [X] game72.tgz      [ ] xfont72.tgz
Set name(s)? (or 'abort' or 'done') [done]
Directory does not contain SHA256.sig. Continue without verification? [no] ^[[3~
yes
Installing bsd             100% |*****| 22445 KB    00:01
Installing bsd.rd          100% |*****|  4533 KB    00:00
Installing base72.tgz      100% |*****|   331 MB    00:31
Extracting etc.tgz         100% |*****|   257 KB    00:00
Installing comp72.tgz      100% |*****| 74598 KB    00:15
Installing man72.tgz       100% |*****|   7610 KB   00:00
Installing game72.tgz      100% |*****|   2745 KB   00:01
Location of sets? (cd0 disk http nfs or 'done') [done]

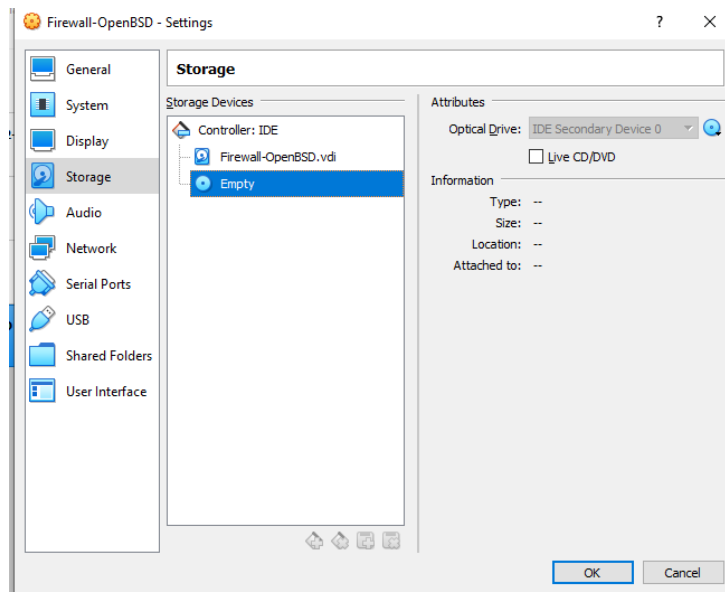
What timezone are you in? ('?' for list) [Canada/Mountain] America/Mexico_City
Saving configuration files... done.
Making all device nodes... done.
fw_update: added none; updated none; kept none
Relinking to create unique kernel... done.

CONGRATULATIONS! Your OpenBSD install has been successfully completed!

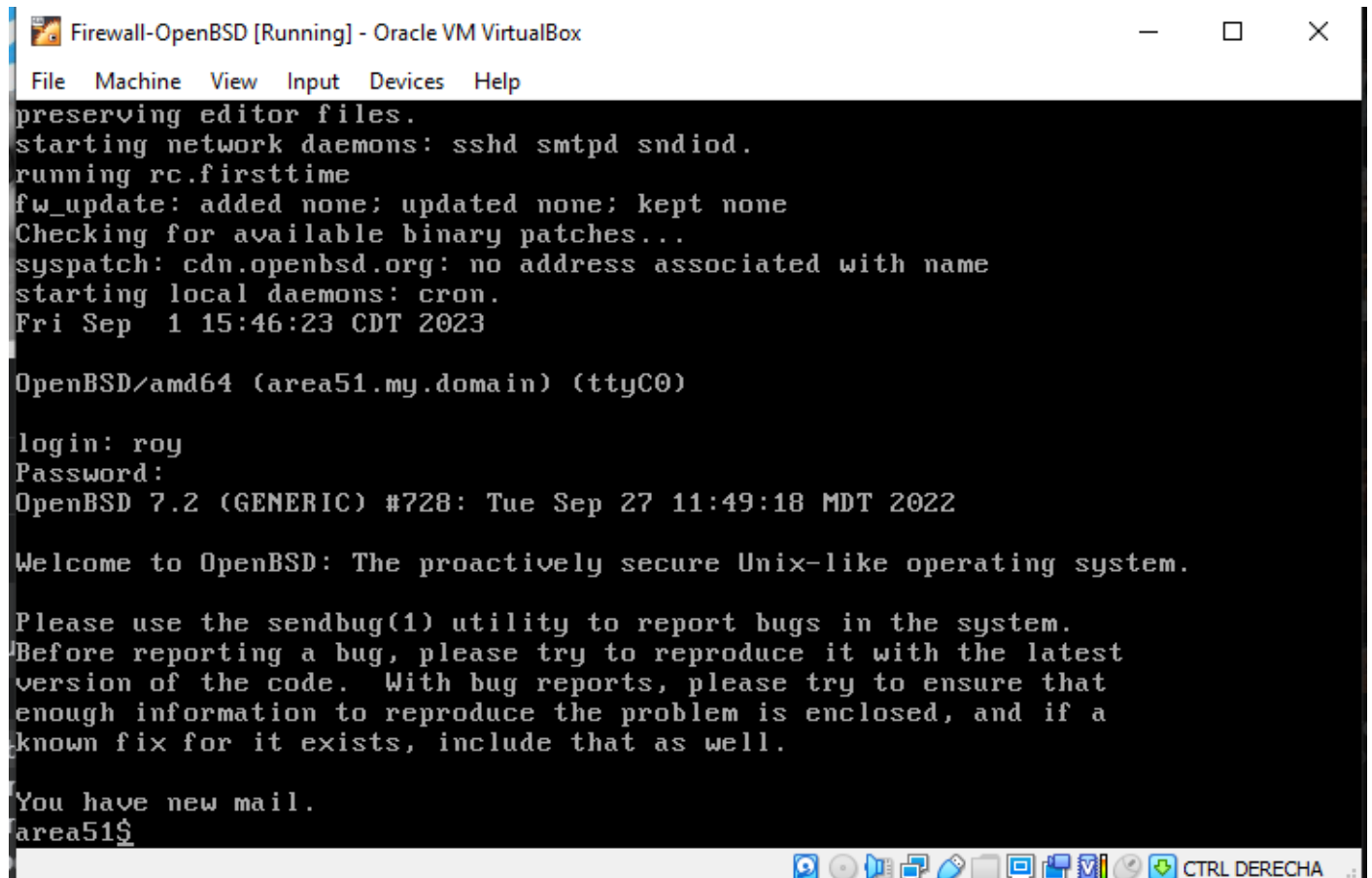
When you login to your new system the first time, please read your mail
using the 'mail' command.

Exit to (S)hell, (H)alt or (R)eboot? [reboot]
```

La configuración de Storage tiene que quedar así:



Volví a ejecutar la máquina virtual de OpenBSD, esperé a que terminara de cargar el SO e ingresé las credenciales que definí en pasos anteriores: usuario Roy y contraseña Roy



```
File Machine View Input Devices Help
preserving editor files.
starting network daemons: sshd smtpd sndiod.
running rc.firsttime
fw_update: added none; updated none; kept none
Checking for available binary patches...
syspatch: cdn.openbsd.org: no address associated with name
starting local daemons: cron.
Fri Sep 1 15:46:23 CDT 2023

OpenBSD/amd64 (area51.my.domain) (ttyC0)

login: roy
Password:
OpenBSD 7.2 (GENERIC) #728: Tue Sep 27 11:49:18 MDT 2022

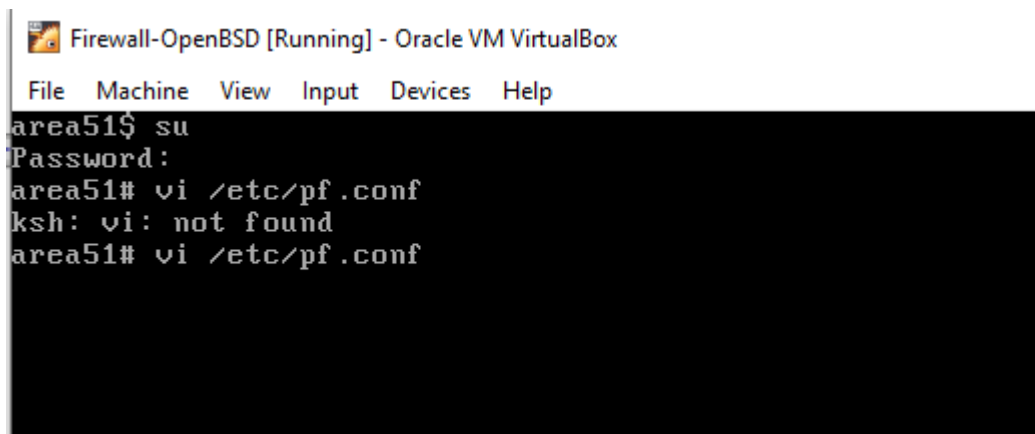
Welcome to OpenBSD: The proactively secure Unix-like operating system.

Please use the sendbug(1) utility to report bugs in the system.
Before reporting a bug, please try to reproduce it with the latest
version of the code. With bug reports, please try to ensure that
enough information to reproduce the problem is enclosed, and if a
known fix for it exists, include that as well.

You have new mail.
area51$
```

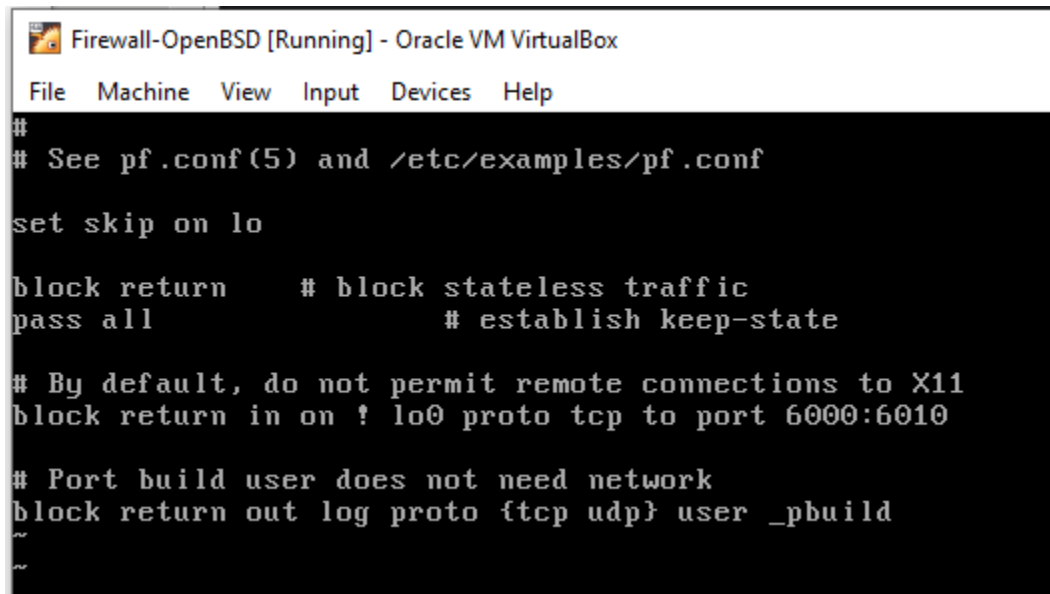
Con los comandos `vi /etc/hostname.em0` y `vi /etc/hostname.em1` se puede cambiar la configuración de los adaptadores de red, específicamente las direcciones ip de cada una.

Luego accedí como superusuario con el comando `su` e ingresé la contraseña establecida en pasos anteriores para el root y edité el archivo `/etc/pf.conf` con `vi`:



```
File Machine View Input Devices Help
area51$ su
Password:
area51# vi /etc/pf.conf
ksh: vi: not found
area51# vi /etc/pf.conf
```

Se tiene que agregar la línea **pass all**



```
#
# See pf.conf(5) and /etc/examples/pf.conf

set skip on lo

block return      # block stateless traffic
pass all          # establish keep-state

# By default, do not permit remote connections to X11
block return in on ! lo0 proto tcp to port 6000:6010

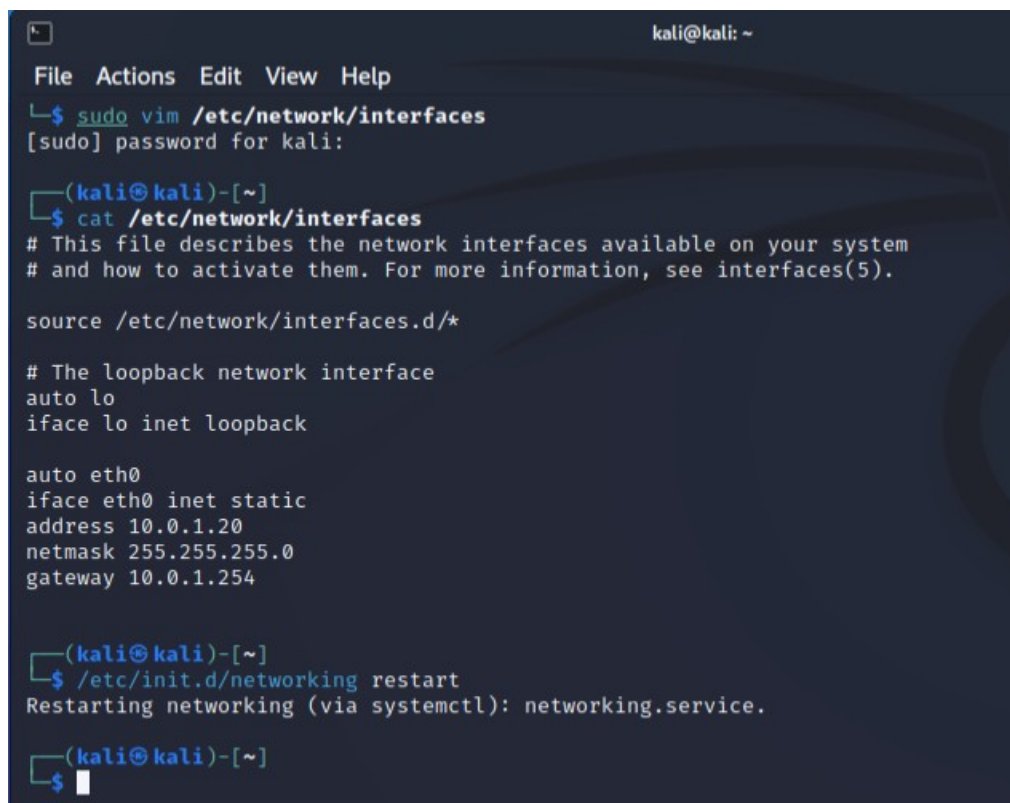
# Port build user does not need network
block return out log proto {tcp udp} user _pbuild
```

Por último se tiene que crear un archivo llamado **/etc/sysctl.conf** con el contenido **net.inet.ip.forwarding=1**

Se puede utilizar el comando **echo 'net.inet.ip.forwarding=1' >> /etc/sysctl.conf** para más practicidad

Terminado el proceso se tiene que reiniciar la máquina virtual con **reboot** y configurar el resto de máquinas virtuales.

Configuración de kali: Abrí una terminal, edité **/etc/network/interfaces.d** y reinicié **/etc/init.d/networking**



```
kali@kali: ~
File Actions Edit View Help
└─$ sudo vim /etc/network/interfaces
[sudo] password for kali:

(kali@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

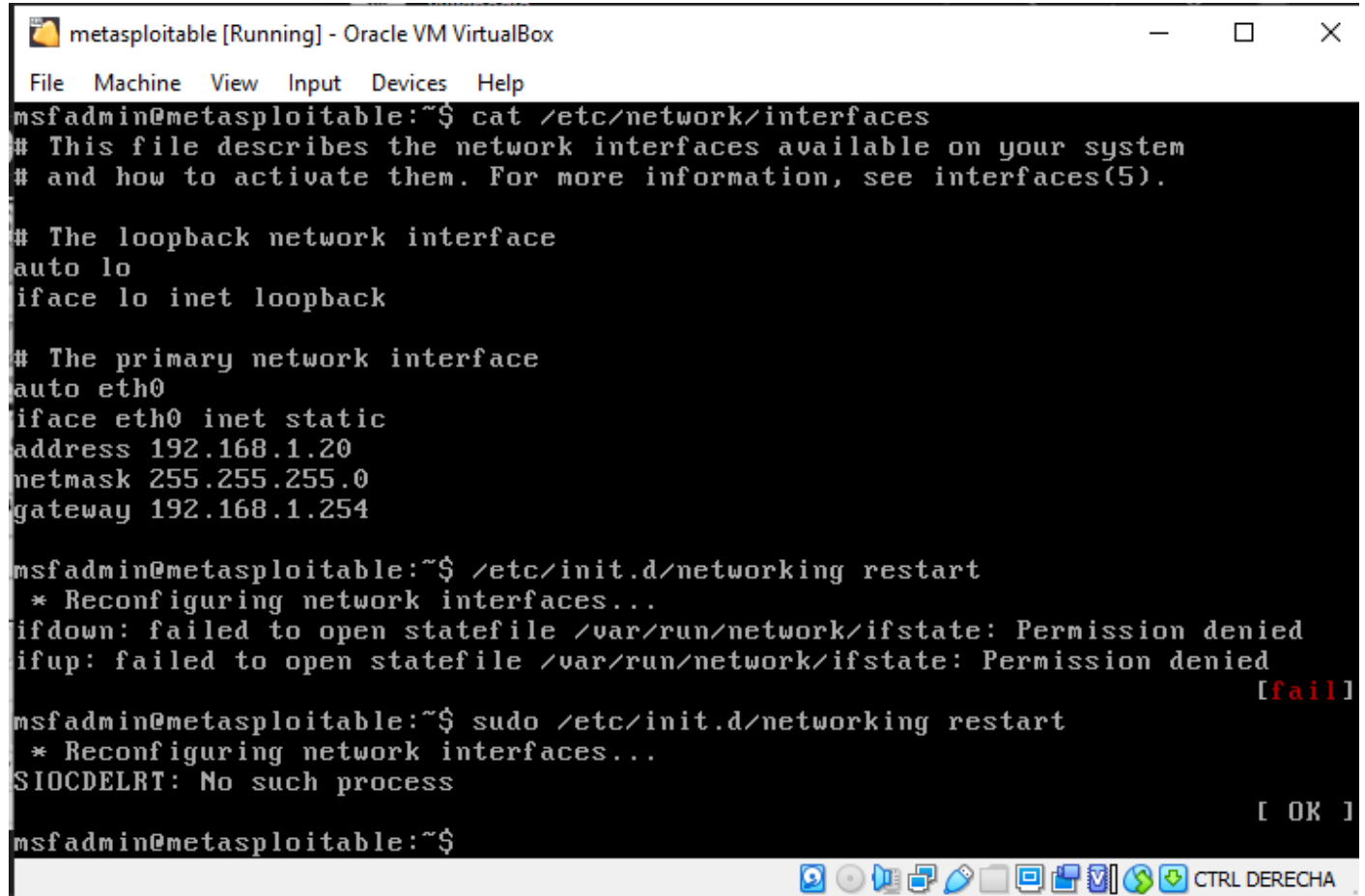
auto eth0
iface eth0 inet static
address 10.0.1.20
netmask 255.255.255.0
gateway 10.0.1.254

(kali@kali)-[~]
└─$ /etc/init.d/networking restart
Restarting networking (via systemctl): networking.service.

(kali@kali)-[~]
└─$
```


Configuración de Metasploitable:

Ingresé con el usuario **msfadmin** con contraseña **msfadmin**, y al igual que en kali, edité **/etc/network/interfaces.d**



```
metasploitable [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
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 static
address 192.168.1.20
netmask 255.255.255.0
gateway 192.168.1.254

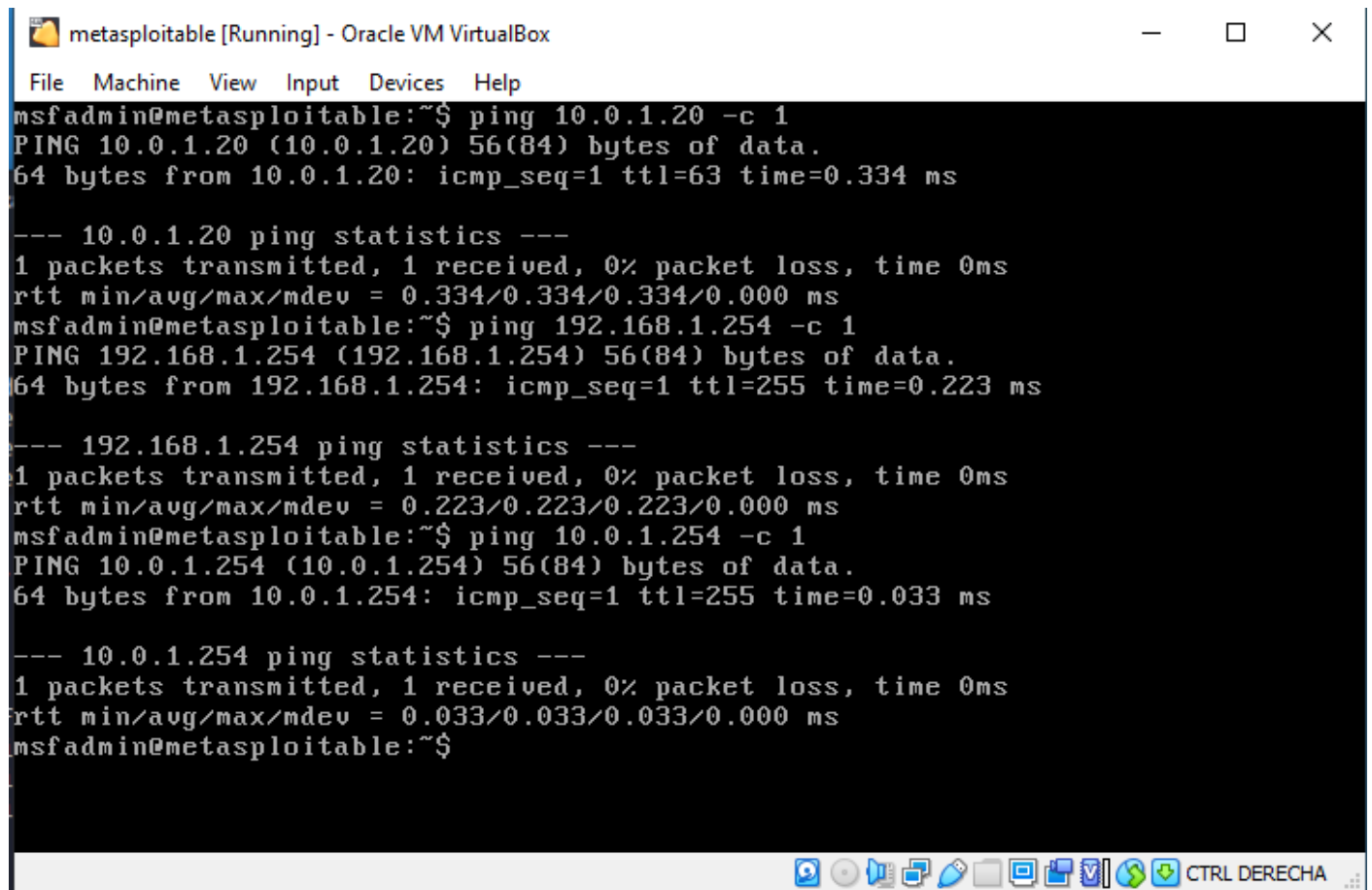
msfadmin@metasploitable:~$ /etc/init.d/networking restart
* Reconfiguring network interfaces...
ifdown: failed to open statefile /var/run/network/ifstate: Permission denied
ifup: failed to open statefile /var/run/network/ifstate: Permission denied
[fail]
msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart
* Reconfiguring network interfaces...
SIOCDELRT: No such process
[ OK ]
msfadmin@metasploitable:~$
```

Probamos haciendo ping a todas las direcciones de la red desde kali y desde metasploitable:

Kali:

```
kali@kali: ~  
File Actions Edit View Help  
  
└─(kali@kali)-[~]  
└─$ ping 192.168.1.20 -c 3  
PING 192.168.1.20 (192.168.1.20) 56(84) bytes of data.  
64 bytes from 192.168.1.20: icmp_seq=1 ttl=63 time=0.333 ms  
64 bytes from 192.168.1.20: icmp_seq=2 ttl=63 time=0.348 ms  
64 bytes from 192.168.1.20: icmp_seq=3 ttl=63 time=0.401 ms  
  
— 192.168.1.20 ping statistics —  
3 packets transmitted, 3 received, 0% packet loss, time 2039ms  
rtt min/avg/max/mdev = 0.333/0.360/0.401/0.029 ms  
  
└─(kali@kali)-[~]  
└─$ ping 192.168.1.254 -c 3  
PING 192.168.1.254 (192.168.1.254) 56(84) bytes of data.  
64 bytes from 192.168.1.254: icmp_seq=1 ttl=255 time=0.196 ms  
64 bytes from 192.168.1.254: icmp_seq=2 ttl=255 time=0.222 ms  
64 bytes from 192.168.1.254: icmp_seq=3 ttl=255 time=0.217 ms  
  
— 192.168.1.254 ping statistics —  
3 packets transmitted, 3 received, 0% packet loss, time 2047ms  
rtt min/avg/max/mdev = 0.196/0.211/0.222/0.011 ms  
  
└─(kali@kali)-[~]  
└─$ ping 10.0.1.254 -c 3  
PING 10.0.1.254 (10.0.1.254) 56(84) bytes of data.  
64 bytes from 10.0.1.254: icmp_seq=1 ttl=255 time=0.249 ms  
64 bytes from 10.0.1.254: icmp_seq=2 ttl=255 time=0.227 ms  
64 bytes from 10.0.1.254: icmp_seq=3 ttl=255 time=0.190 ms  
  
— 10.0.1.254 ping statistics —  
3 packets transmitted, 3 received, 0% packet loss, time 2045ms  
rtt min/avg/max/mdev = 0.190/0.222/0.249/0.024 ms  
  
└─(kali@kali)-[~]  
└─$ █
```

Metasploitable:



The screenshot shows a terminal window titled "metasploitable [Running] - Oracle VM VirtualBox". The terminal displays the following commands and output:

```
msfadmin@metasploitable:~$ ping 10.0.1.20 -c 1
PING 10.0.1.20 (10.0.1.20) 56(84) bytes of data.
64 bytes from 10.0.1.20: icmp_seq=1 ttl=63 time=0.334 ms

--- 10.0.1.20 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.334/0.334/0.334/0.000 ms
msfadmin@metasploitable:~$ ping 192.168.1.254 -c 1
PING 192.168.1.254 (192.168.1.254) 56(84) bytes of data.
64 bytes from 192.168.1.254: icmp_seq=1 ttl=255 time=0.223 ms

--- 192.168.1.254 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.223/0.223/0.223/0.000 ms
msfadmin@metasploitable:~$ ping 10.0.1.254 -c 1
PING 10.0.1.254 (10.0.1.254) 56(84) bytes of data.
64 bytes from 10.0.1.254: icmp_seq=1 ttl=255 time=0.033 ms

--- 10.0.1.254 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.033/0.033/0.033/0.000 ms
msfadmin@metasploitable:~$
```

The terminal window has a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help". The bottom of the window shows a taskbar with various icons and the text "CTRL DERECHA".

Sección 3: Escenario de uso reales, de las tecnologías y/o procesos usados en la práctica.

El uso de máquinas virtuales como metasploitable permite el entrenamiento en la ciberseguridad y el pentesting, y el utilizar redes de máquinas virtuales, como lo hicimos en esta práctica, permite hacer pruebas antes de desplegar en entornos reales.

El funcionamiento de la máquina virtual de OpenBSD sirve como un firewall, por lo que en la vida real también se podría configurar una máquina física con OpenBSD como sistema operativo para ser utilizada como firewall. En cuanto a la distribución Kali, por lo que leí e investigué, es utilizada muy a menudo para realizar auditorías y pentesting.

Bibliografía

Kali Linux. (s.f.). Kali Linux Penetration Testing and Ethical Hacking Linux Distribution. Recuperado de <https://www.kali.org/> el 31 de agosto de 2023

Tanveer, S. (2023) What is Kali Linux? Everything to know about the popular Linux distro. Recuperado de <https://www.xda-developers.com/kali-linux/> el 31 de agosto de 2023

Delony, D. (2021) What Is OpenBSD? Everything You Need to Know. Recuperado de :<https://www.makeuseof.com/what-is-openbsd/> el 31 de agosto de 2023

Kumar, B. (2022) A Look At 'What Is Metasploitable', A Hacker's Playground Based On Ubuntu Virtual Machines. Recuperado de: <https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-metasploit> el 31 de agosto de 2023

Rapid7. (s.f.). Metasploitable 2 - Rapid7. Recuperado de <https://docs.rapid7.com/metasploit/metasploitable-2/> el 31 de agosto de 2023

OpenBSD. (s.f.). OpenBSD. Recuperado de <https://www.openbsd.org/> el 31 de agosto de 2023