# Tecnológico Nacional de México
# Instituto Tecnológico de Tlaxiaco

Carrera: Ingeniería en Sistemas Computacionales

Materia: Seguridad Y Virtualización

Actividad: Reporte de Practica 6


| | | |
|---|---|---|
| Alumnos: | Feria Ortiz Eduardo Tomas | 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

# 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

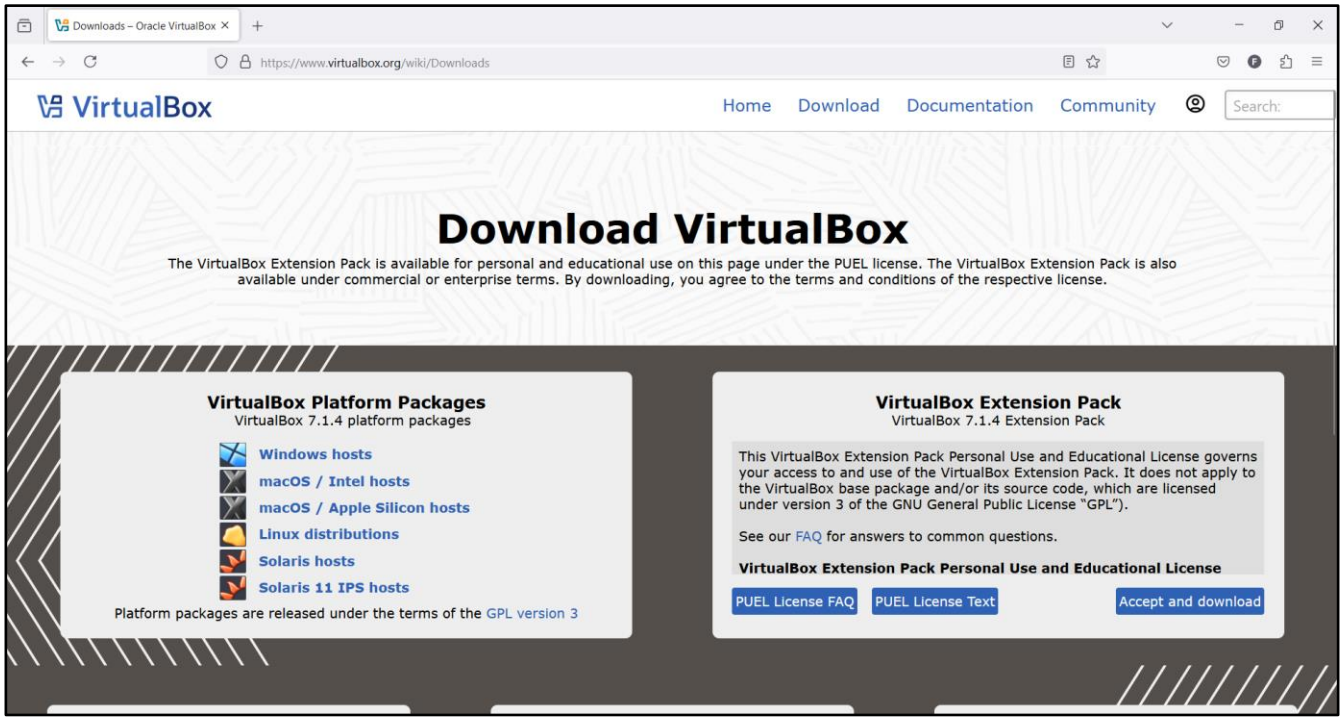


*Ilustración 1. VirtualBox.org*

**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.

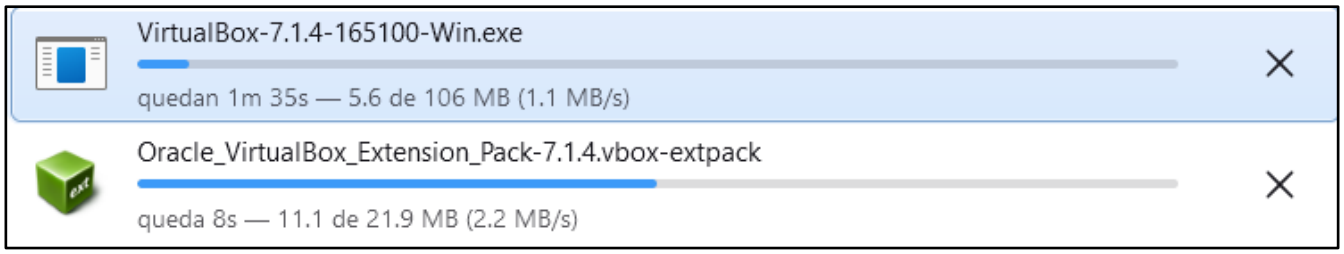


*Ilustración 2. Descarga de VirtualBox*

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

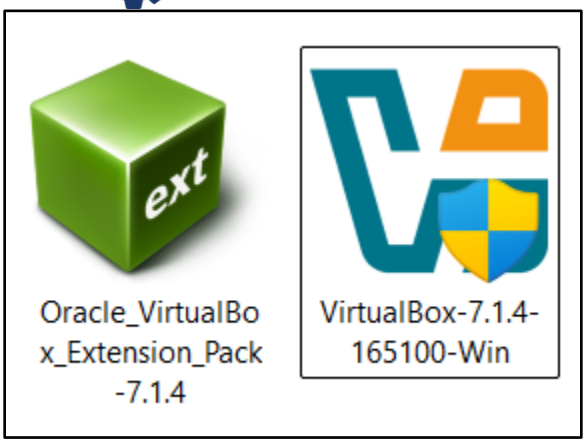


*Ilustración 3. Instalación de VirtualBox*

## 2. Instalación y configuración de OpnSense

### Instalación:

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

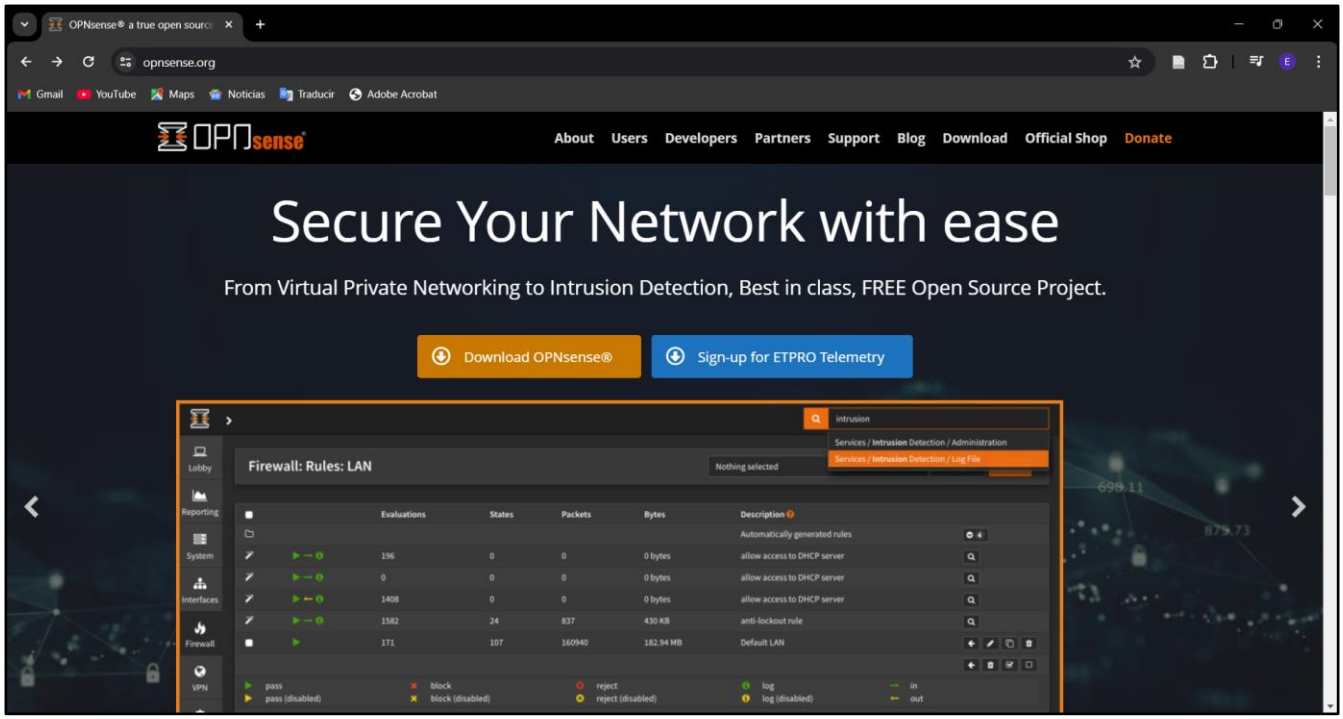


*Ilustración 4. OPNsense*

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

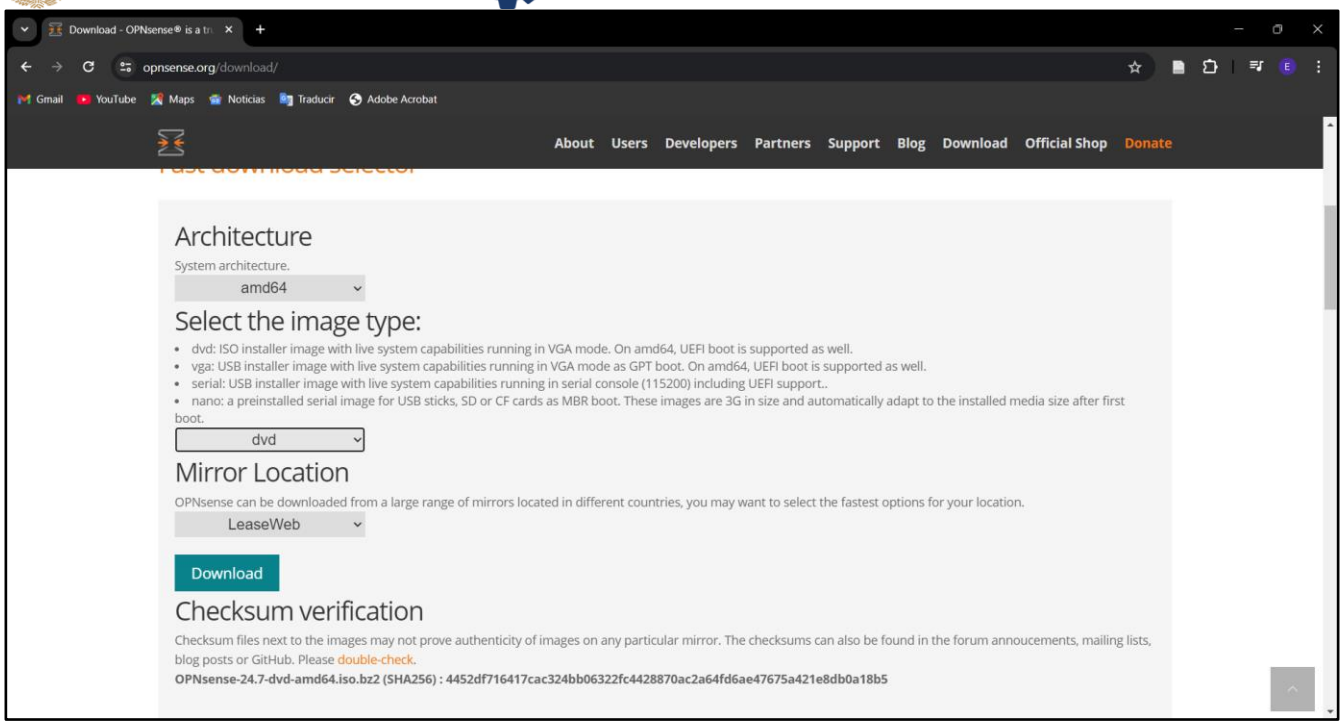


*Ilustración 5. Configuración de descarga OPNsense*

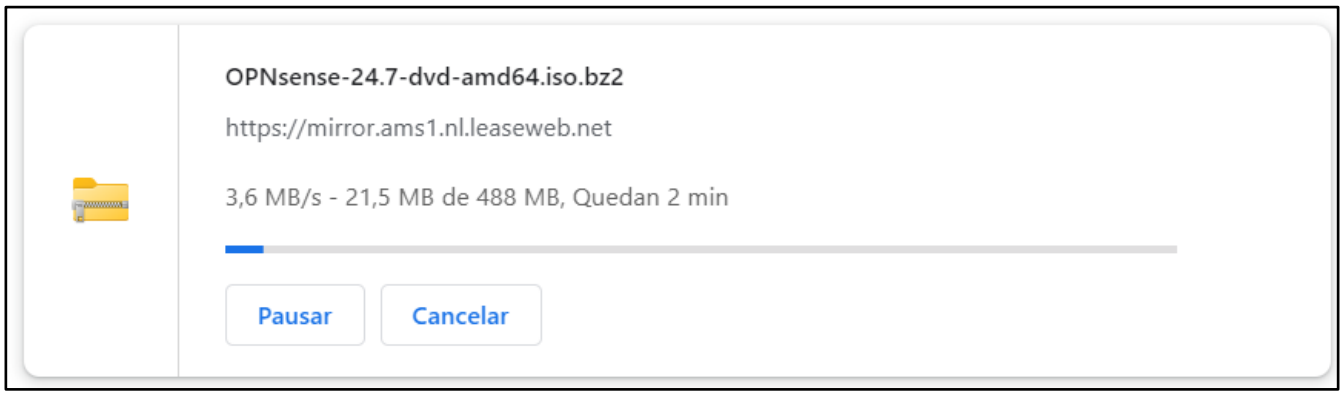


*Ilustración 6. Descarga OPNsense*

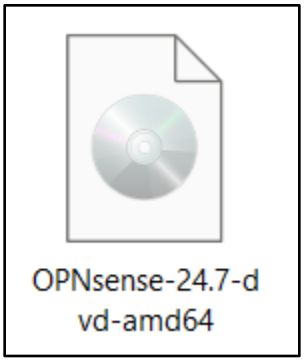


*Ilustración 7, Instalación OPNsense*

**c)** Creamos una máquina virtual:

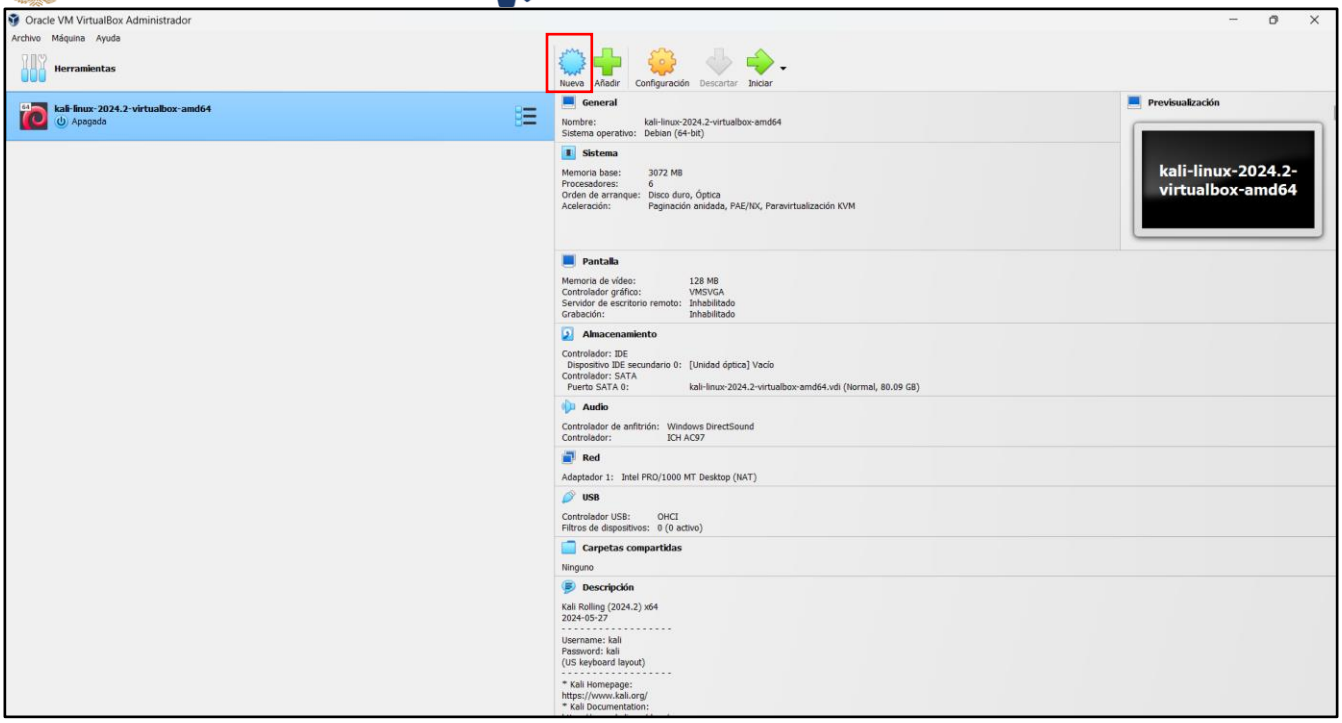


*Ilustración 8. OPNsense MV*

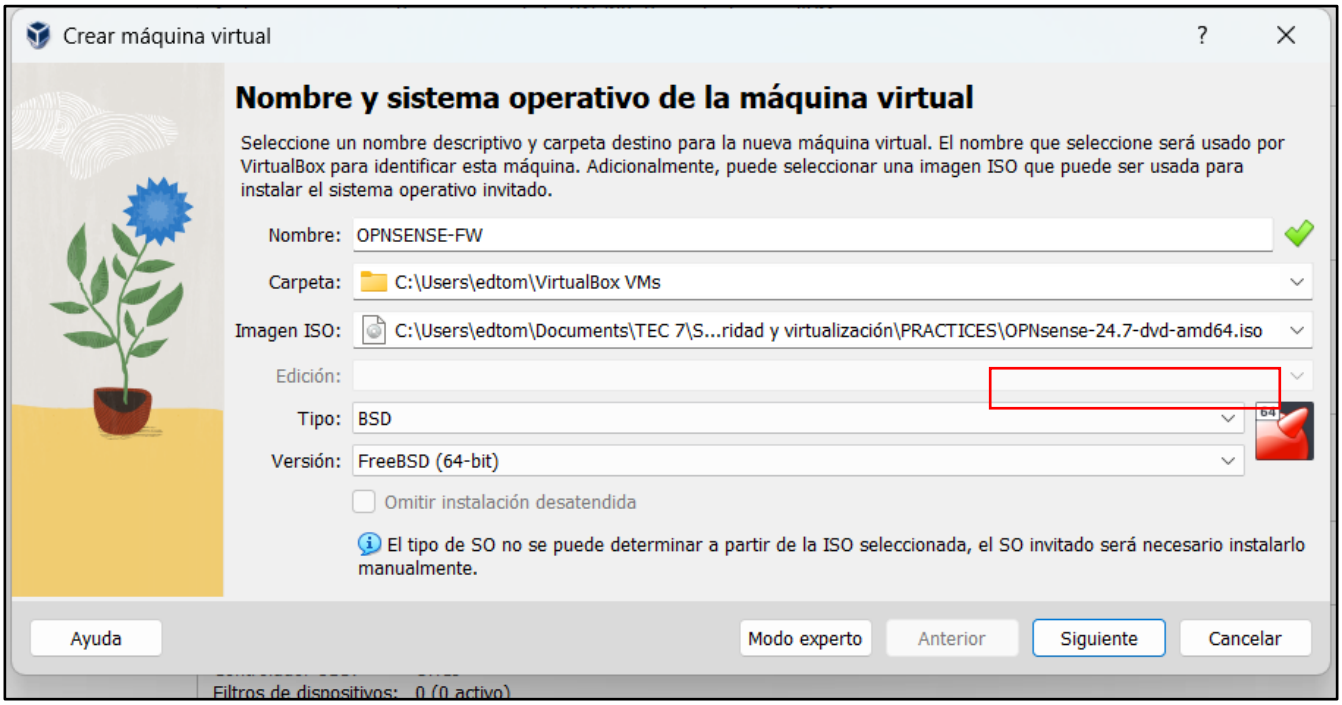


*Ilustración 9. Configuración MV OPNsense*

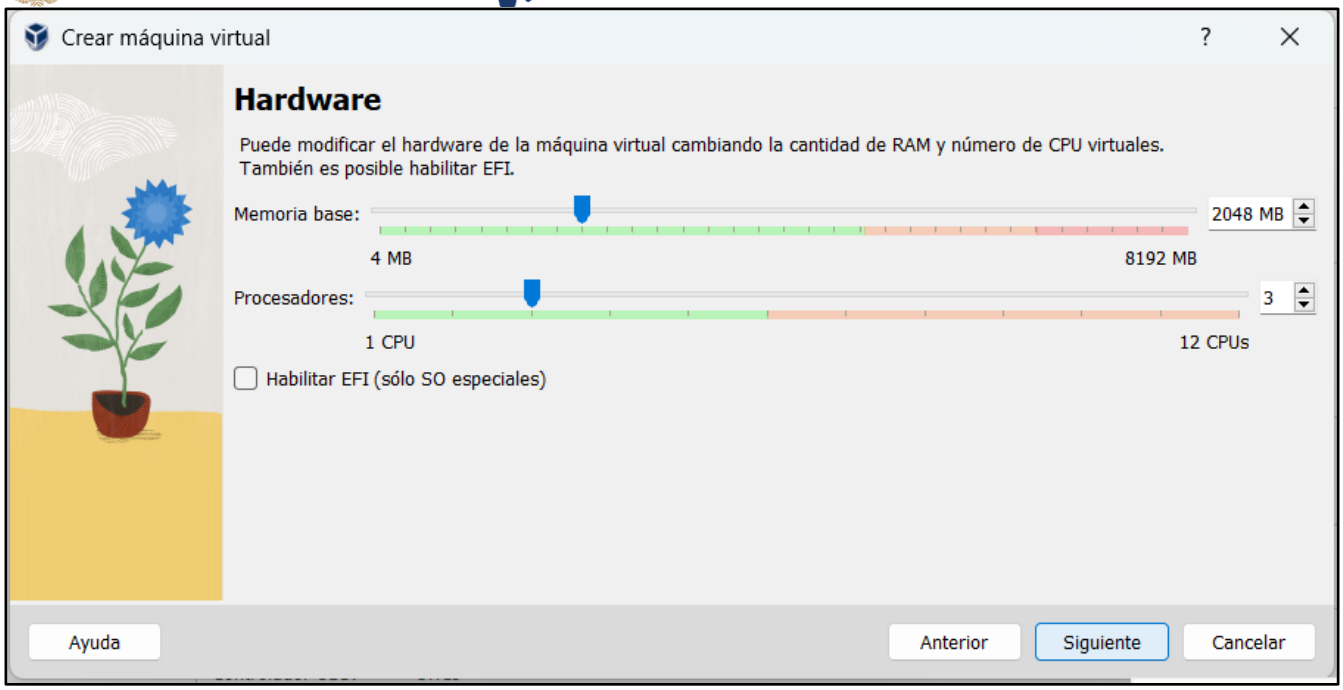


*Ilustración 10. Configuración pt 2 MV OPNsense*

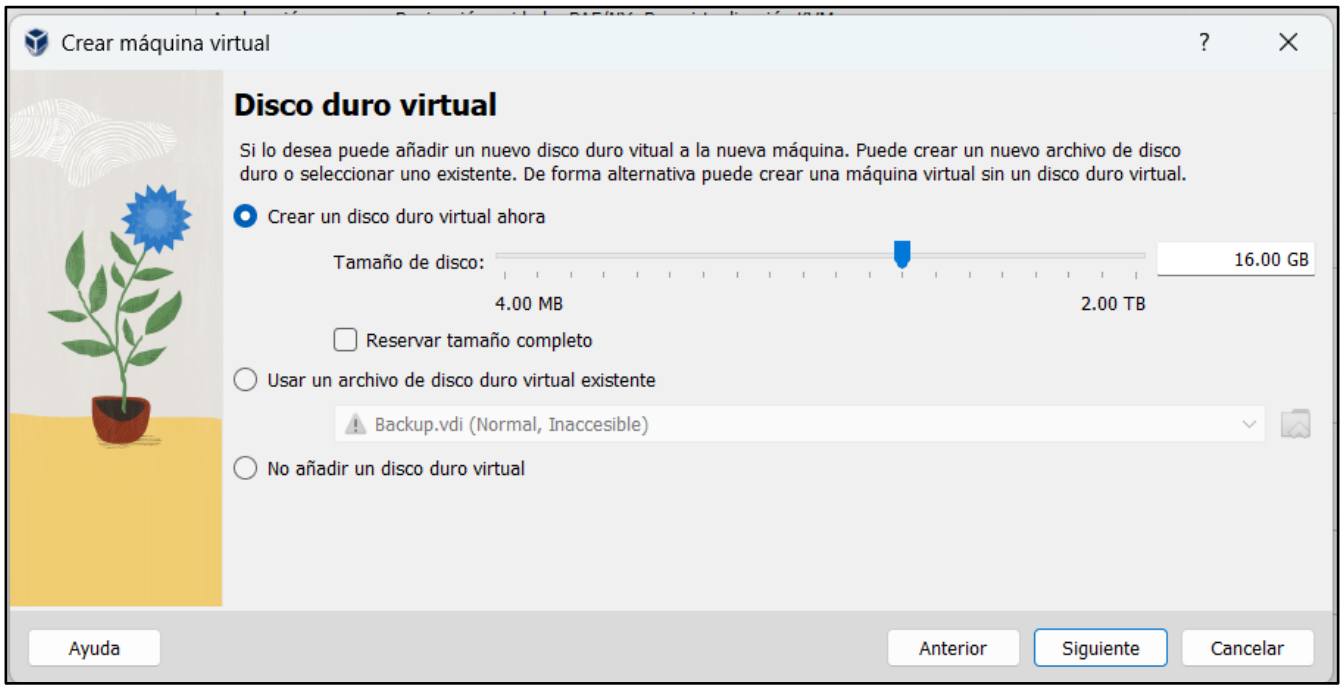


*Ilustración 11. Configuración pt 3 MV OPNsense*

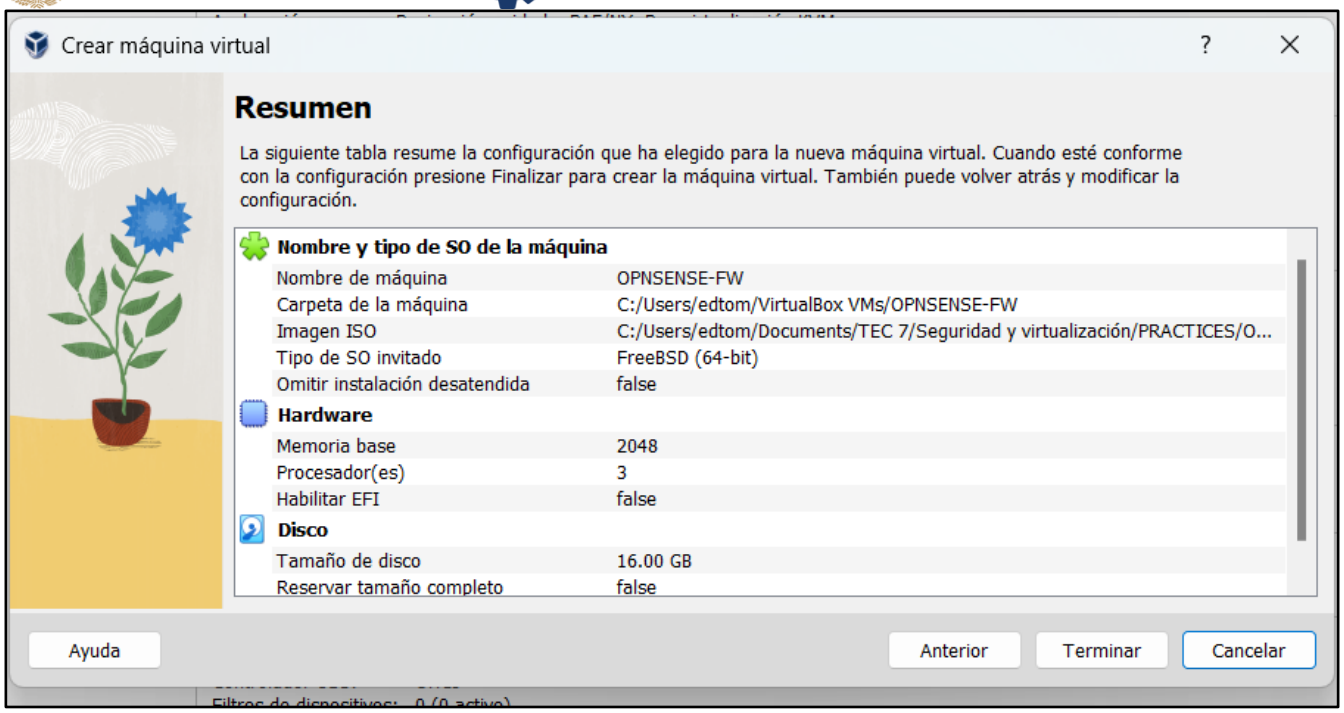


*Ilustración 12. Configuración pt 4 MV OPNsense*

## Configuración:

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

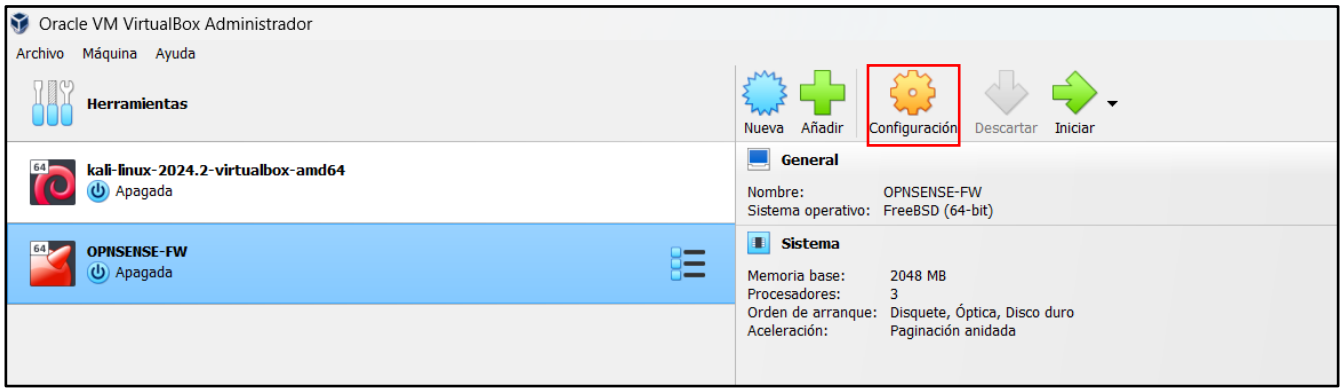


*Ilustración 13. Configuración pt 5 MV OPNsense*

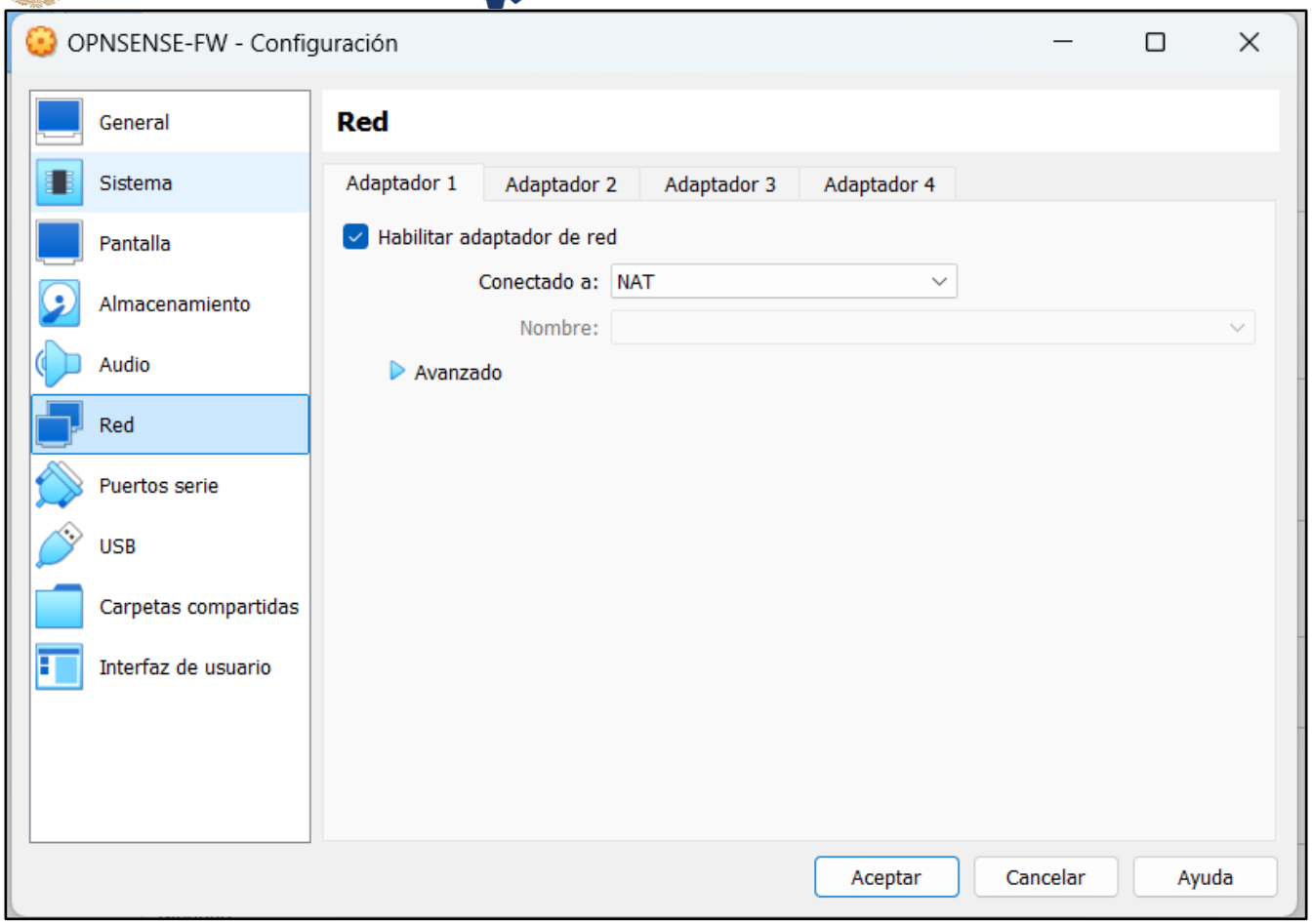


*Ilustración 14. Configuración pt 6 MV OPNsense*

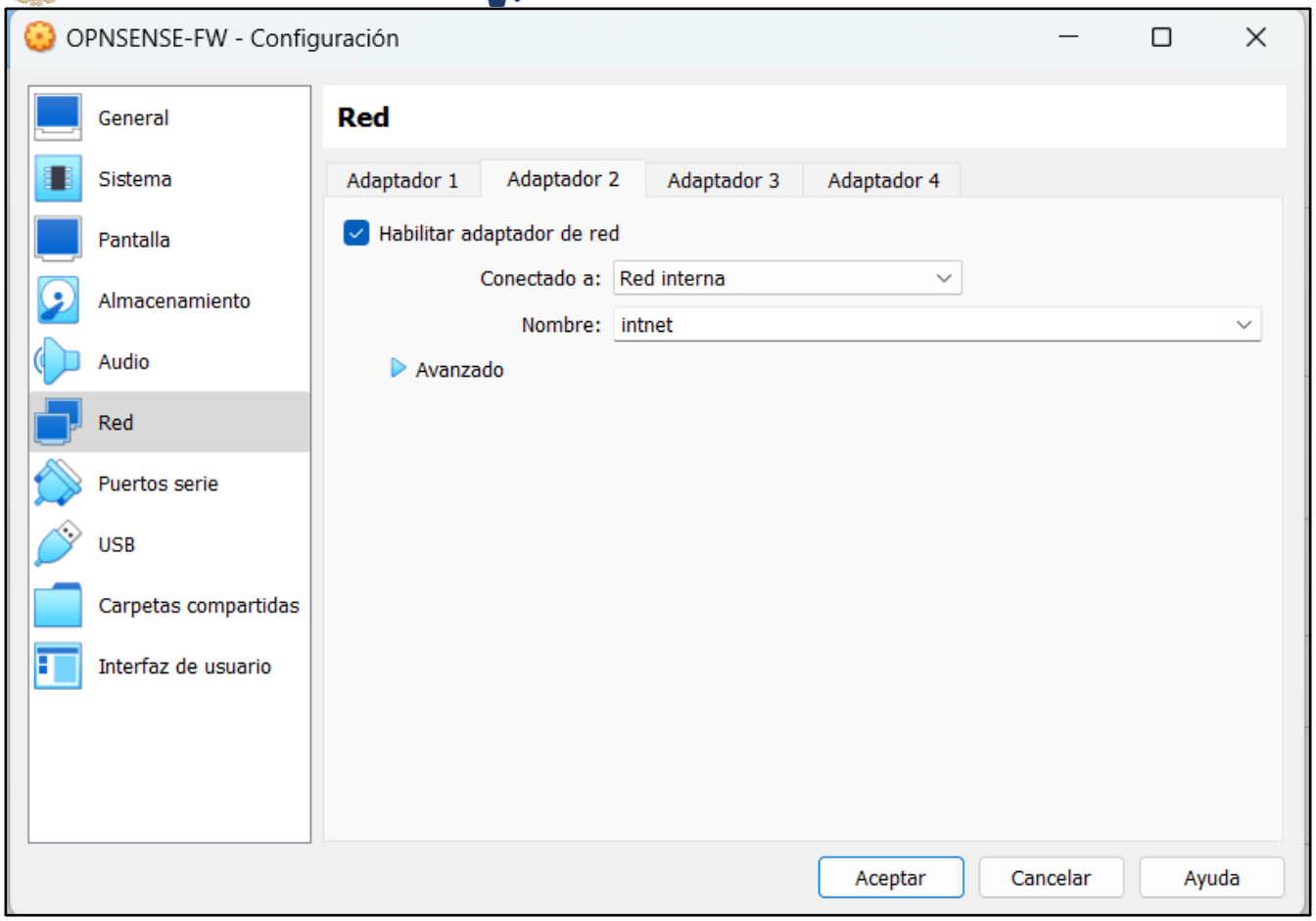


*Ilustración 15. Configuración pt 7 MV OPNsense*

**b)** Iniciamos la máquina virtual

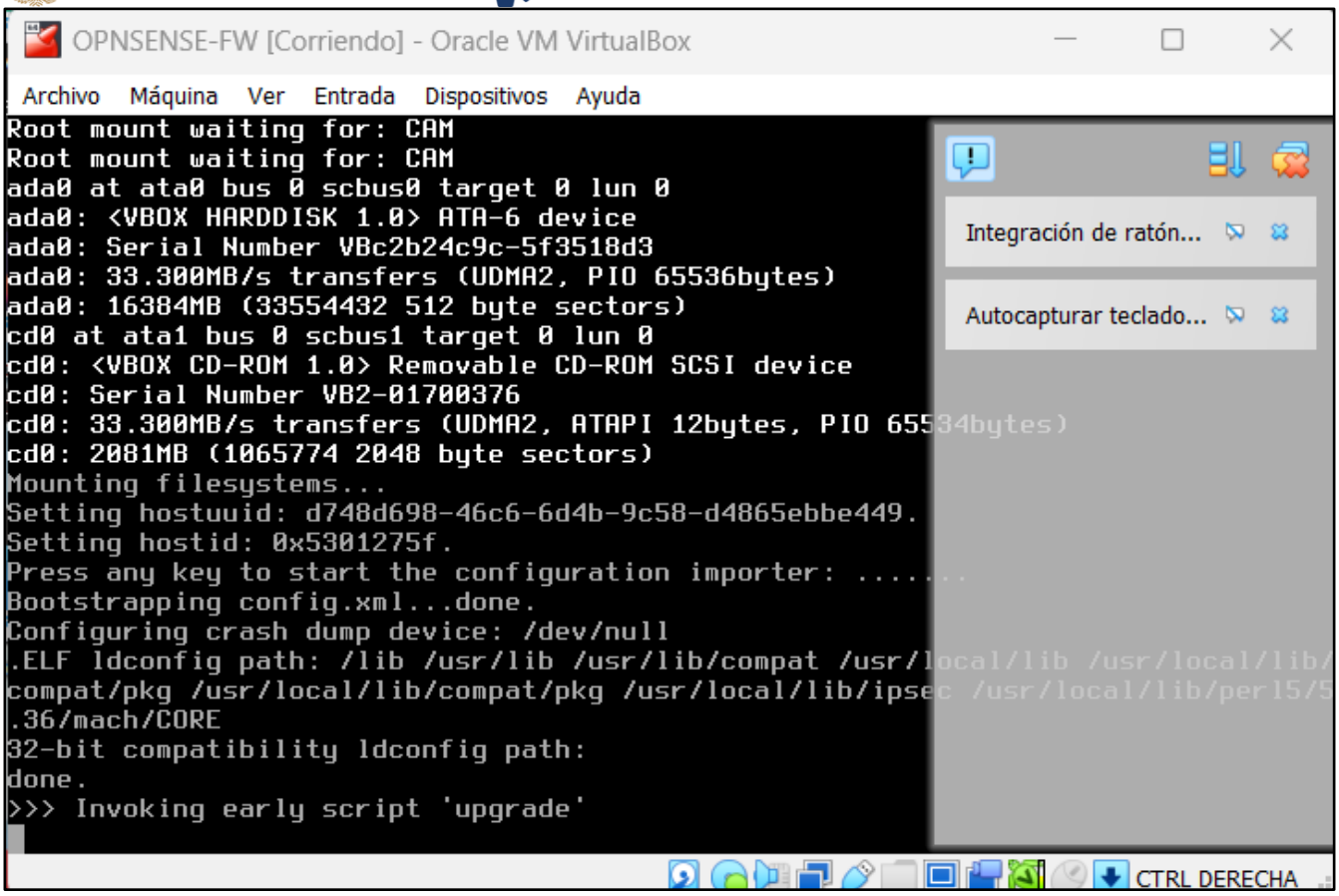


*Ilustración 16. Virtualización OPNsense*

**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.

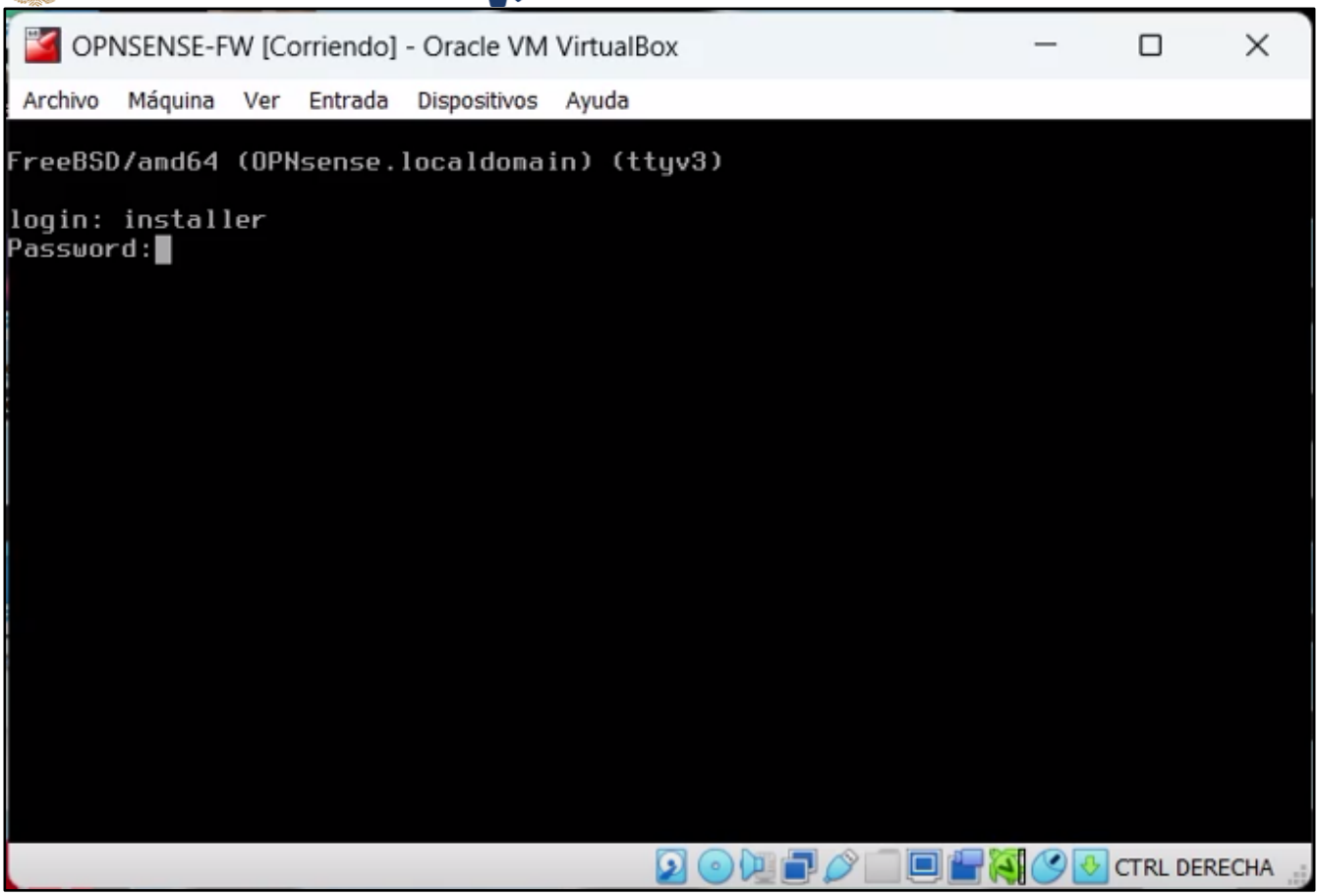


*Ilustración 17. Configuración OPNsense*

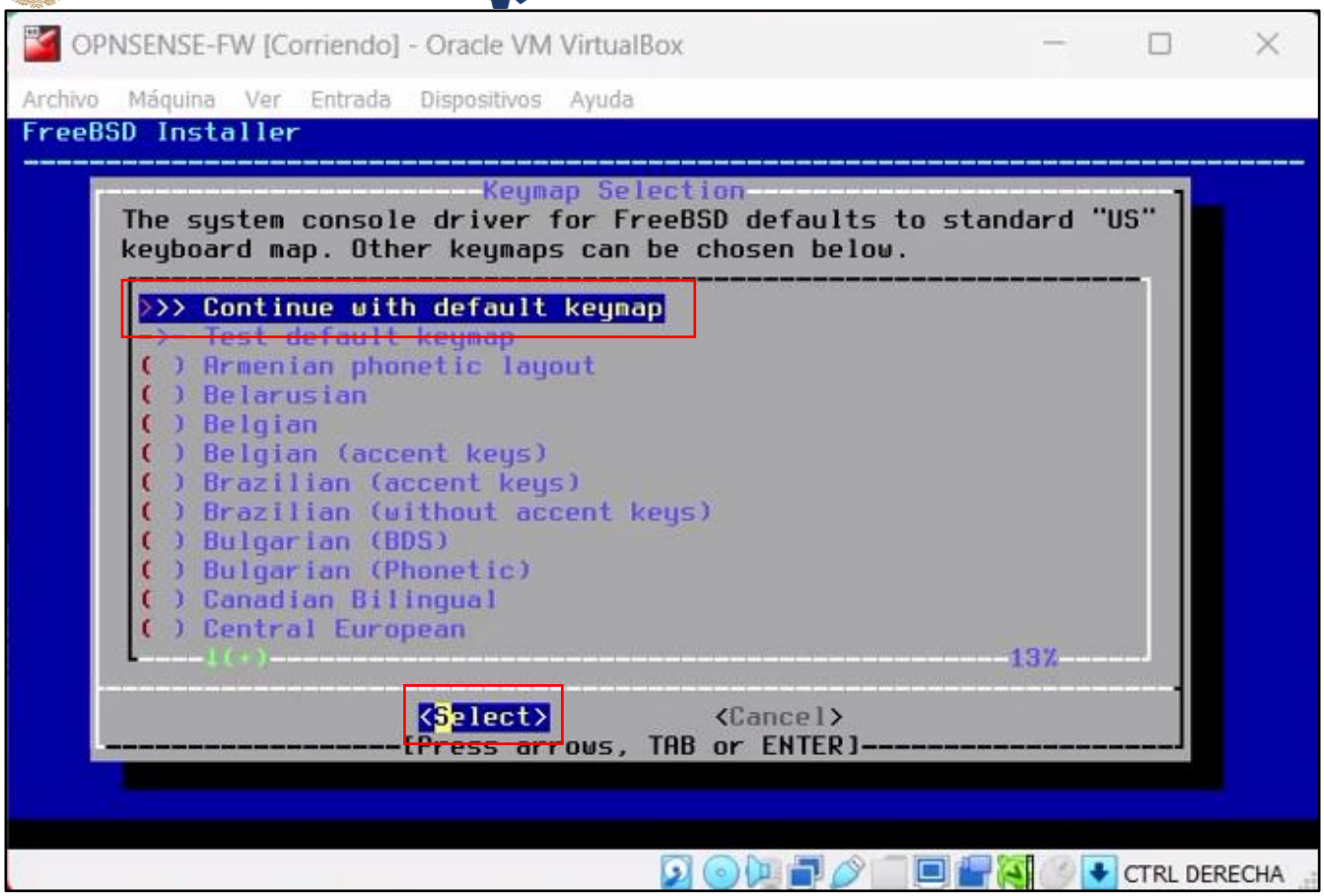


*Ilustración 18. Configuración OPNsense pt 2*

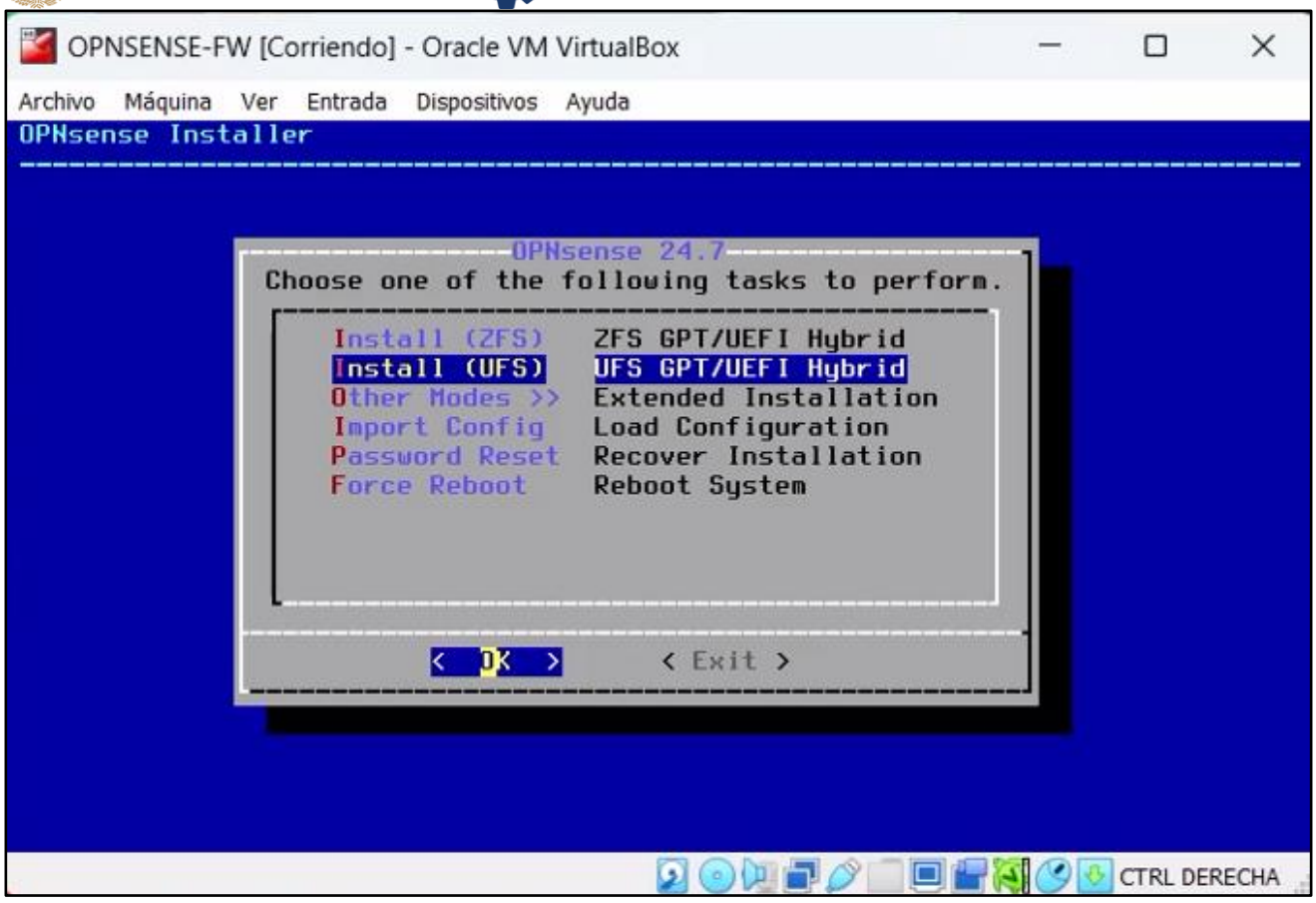


*Ilustración 19. Configuración OPNsense pt 3*

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.

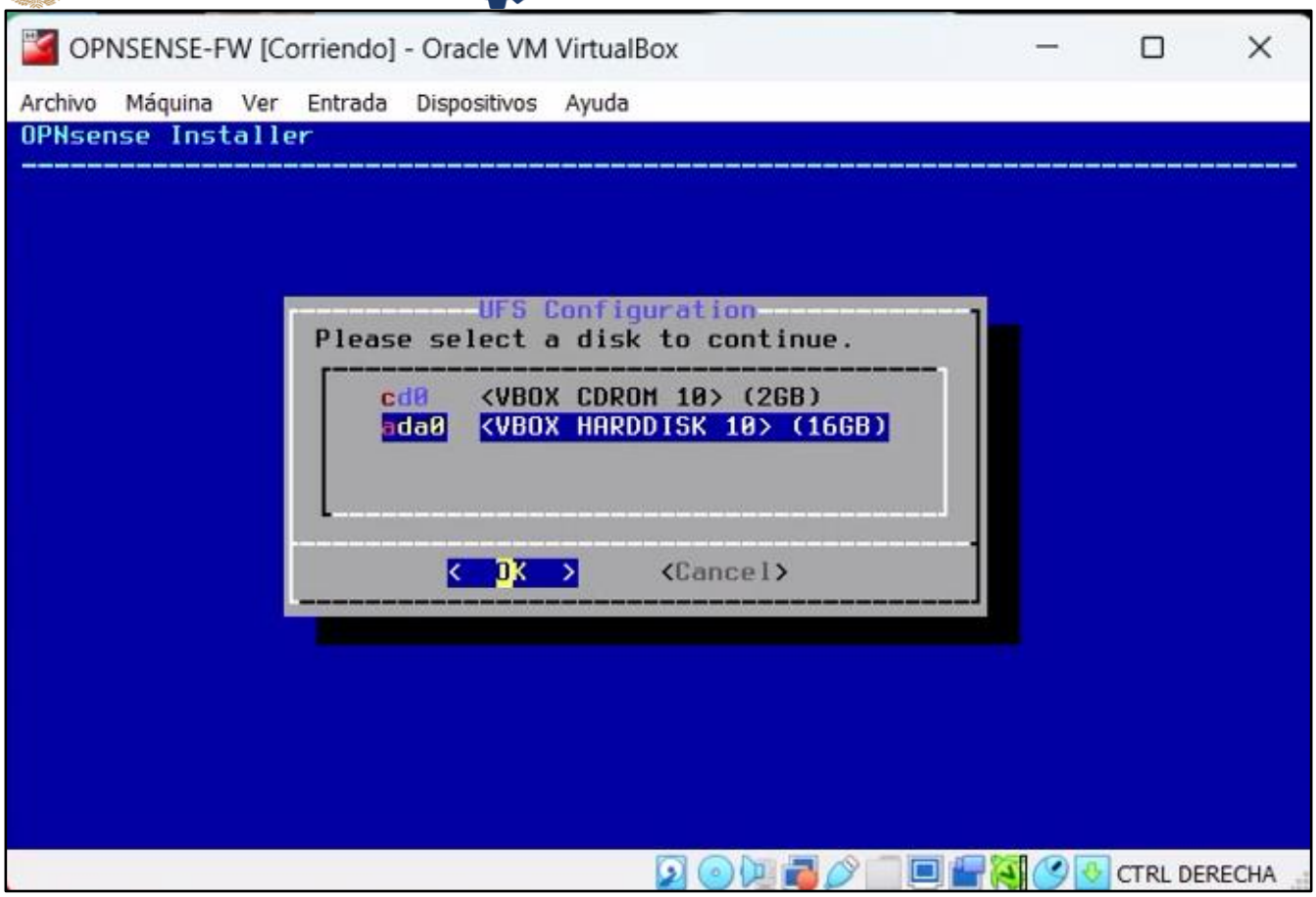


*Ilustración 20. Configuración OPNsense pt 4*

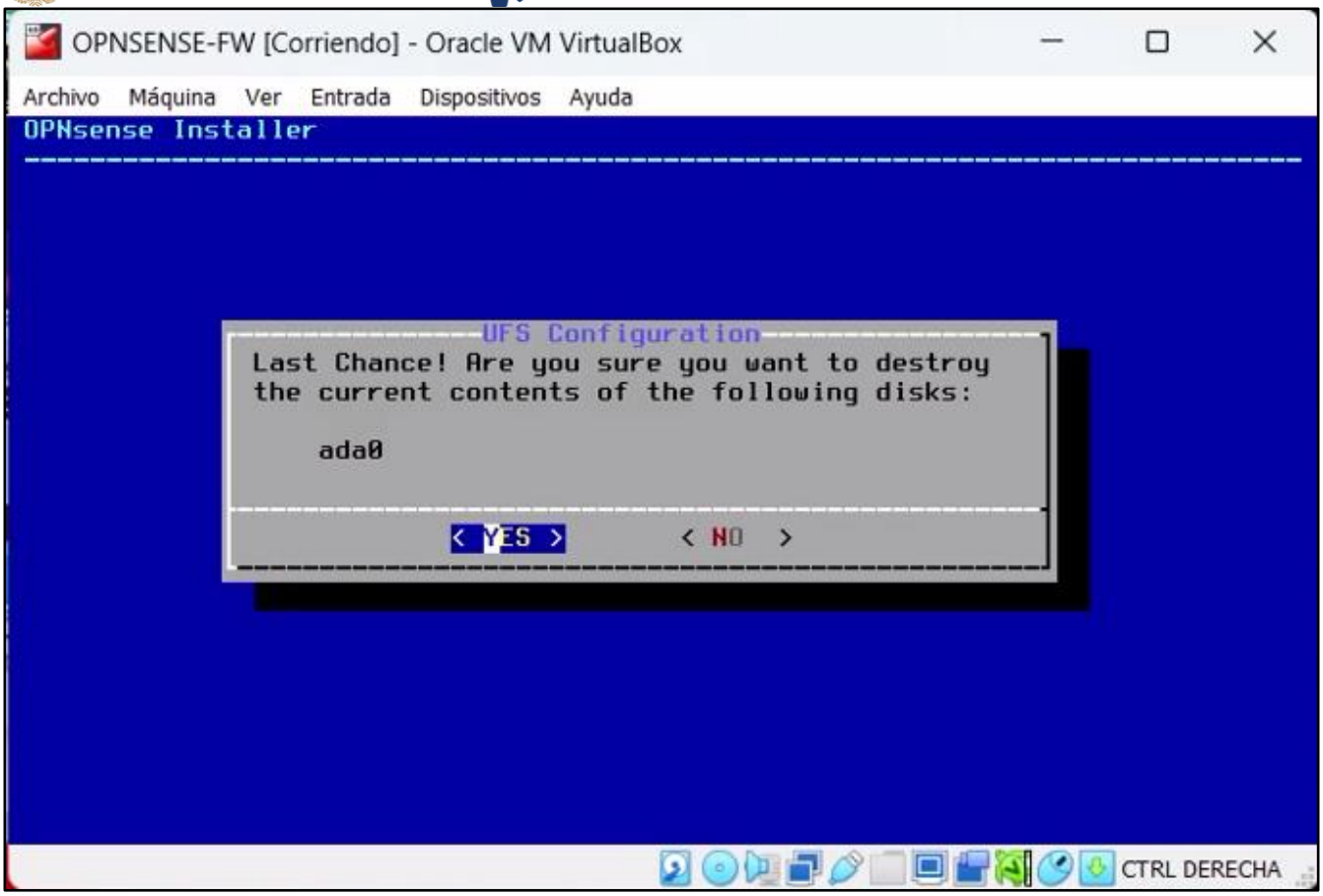


*Ilustración 21. Configuración OPNsense pt 5*

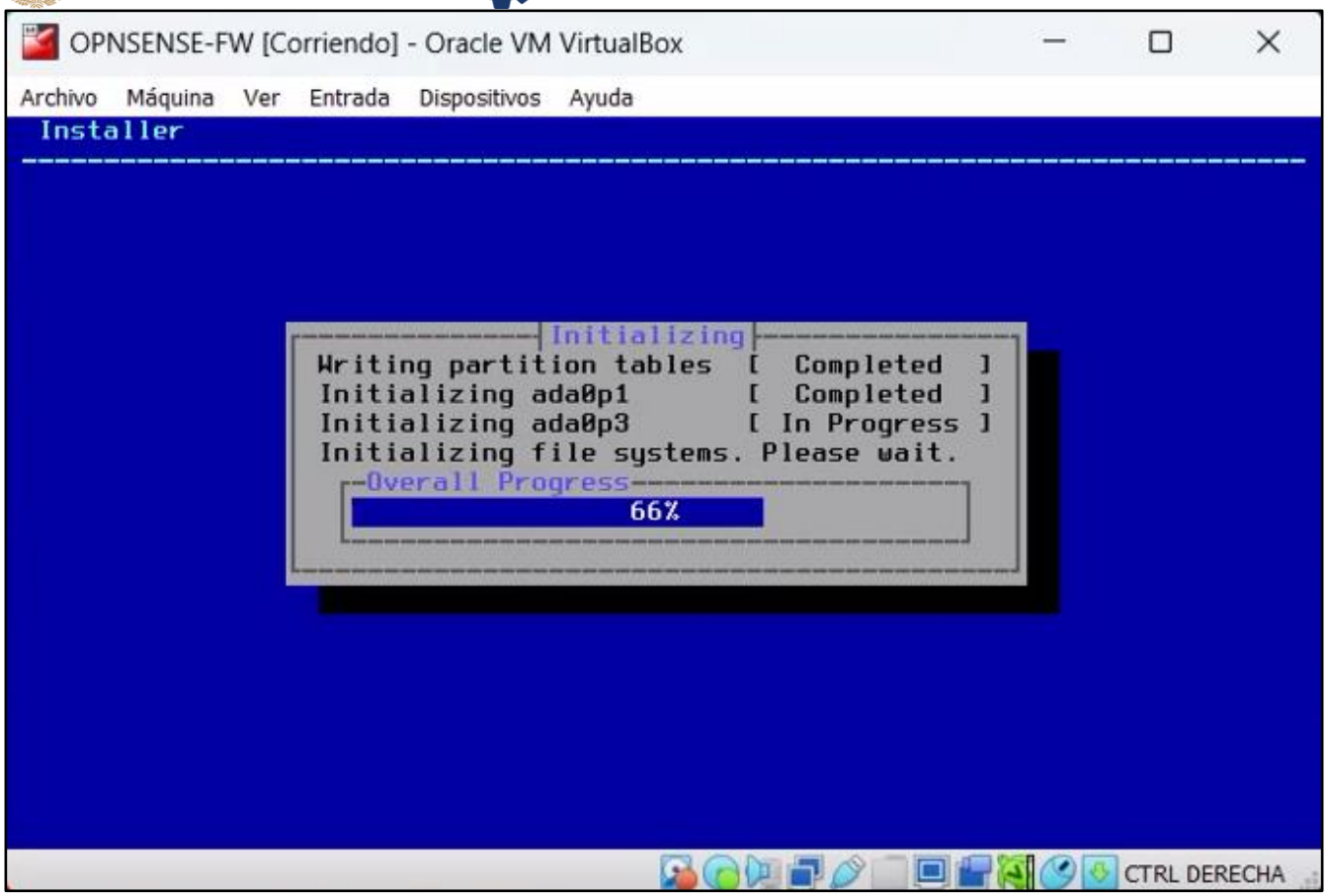


*Ilustración 22. Configuración OPNsense pt 6*

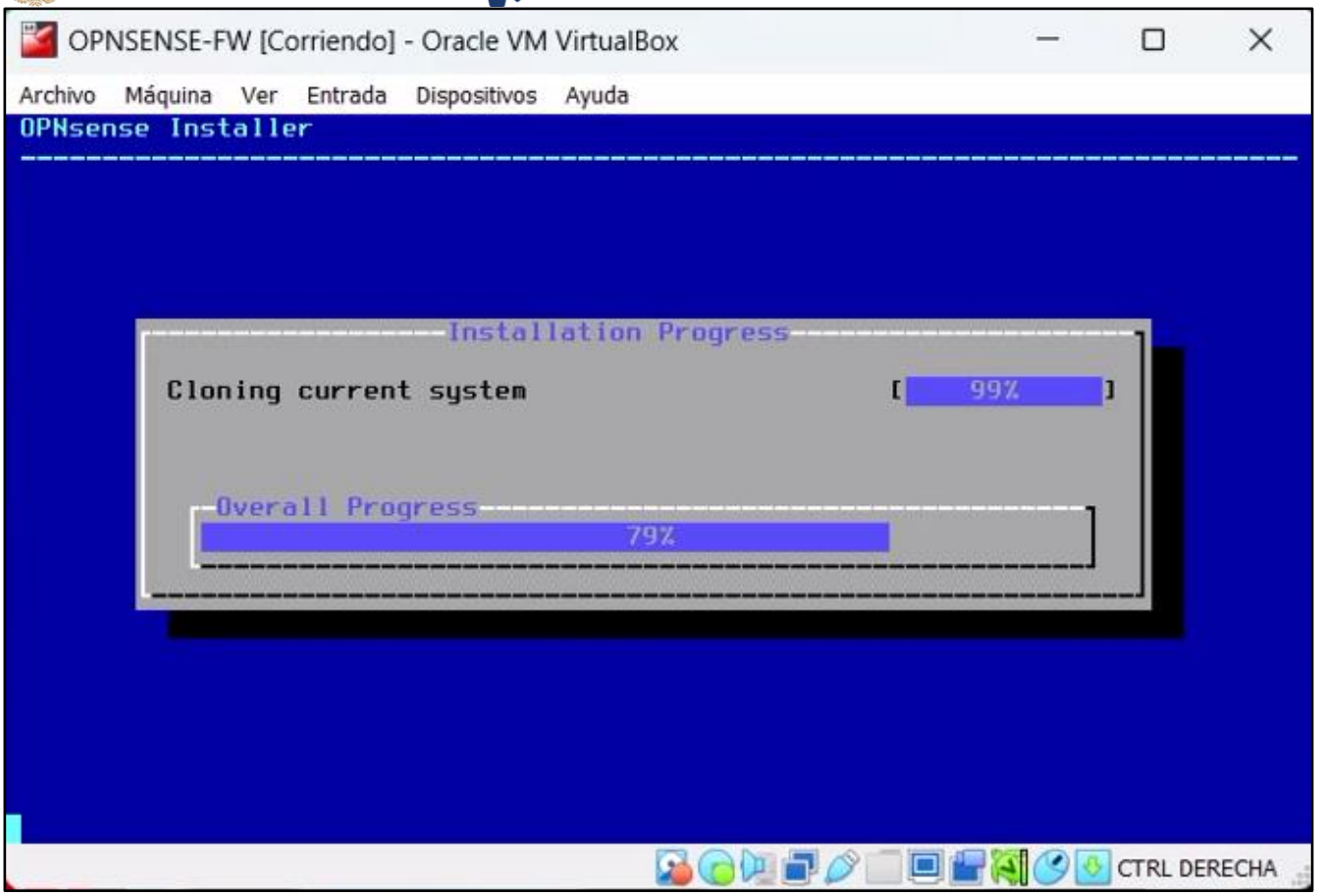


*Ilustración 23. Configuración OPNsense pt 7*

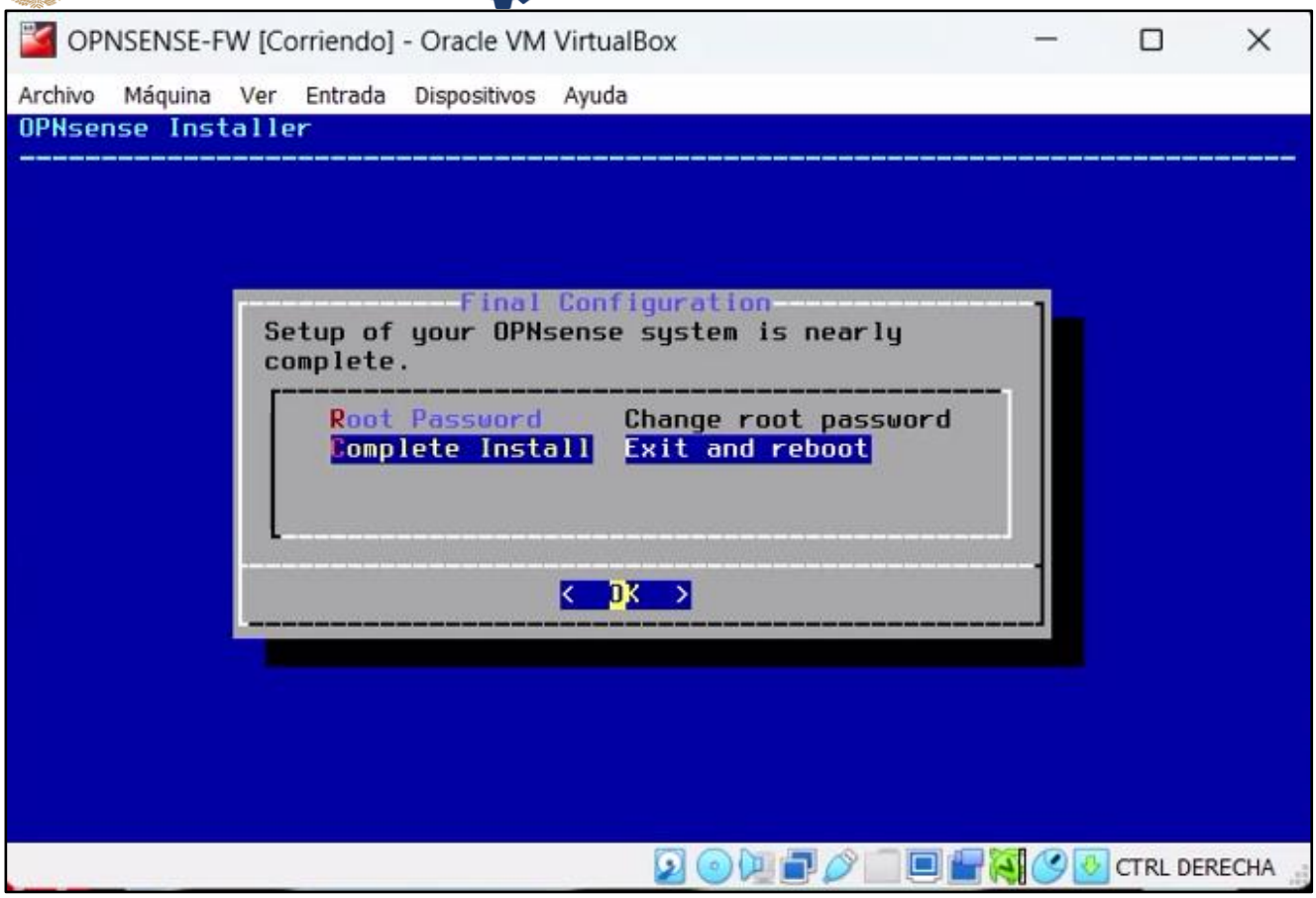


*Ilustración 24. Configuración OPNsense pt 8*

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

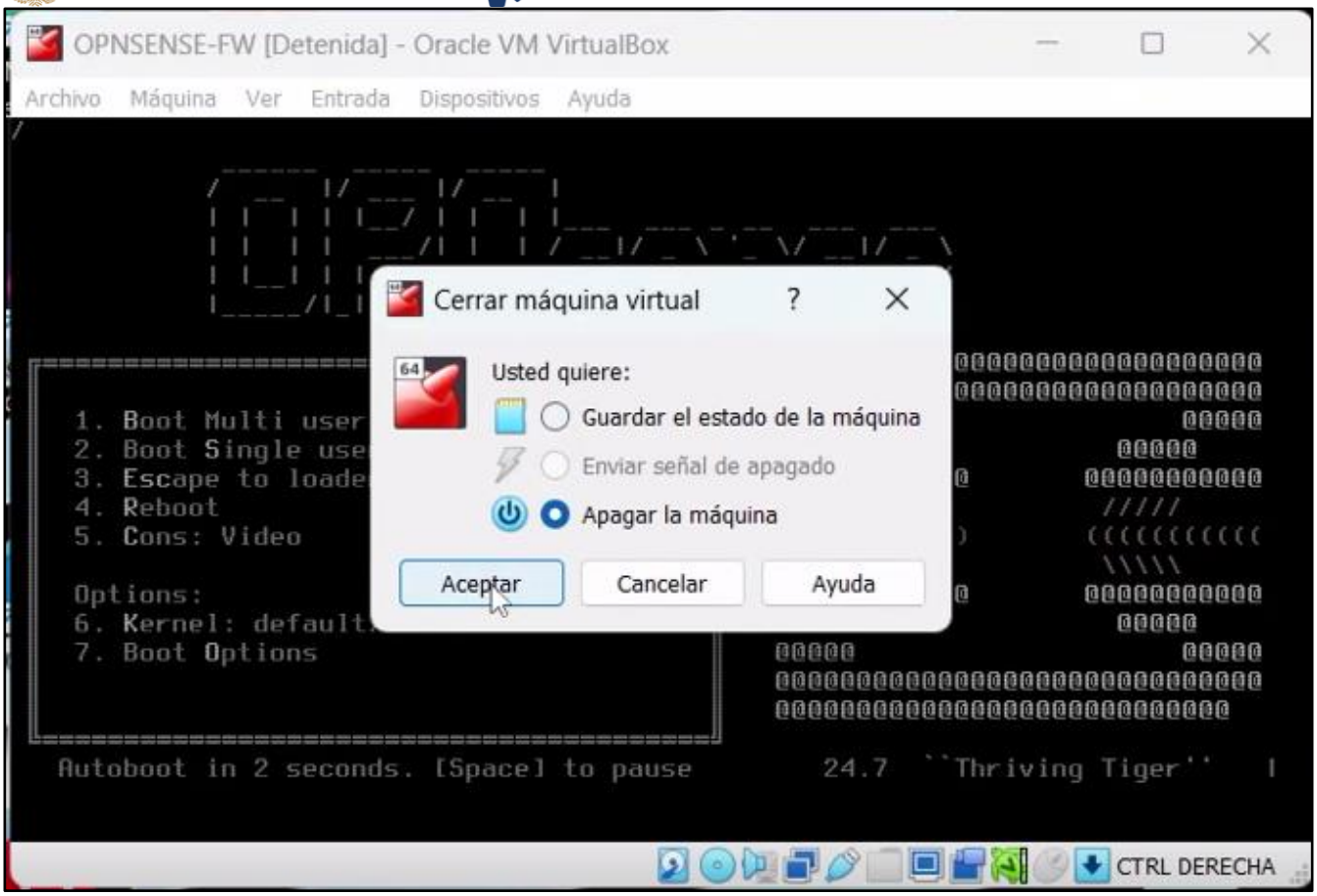


*Ilustración 25. Configuración OPNsense pt 9*

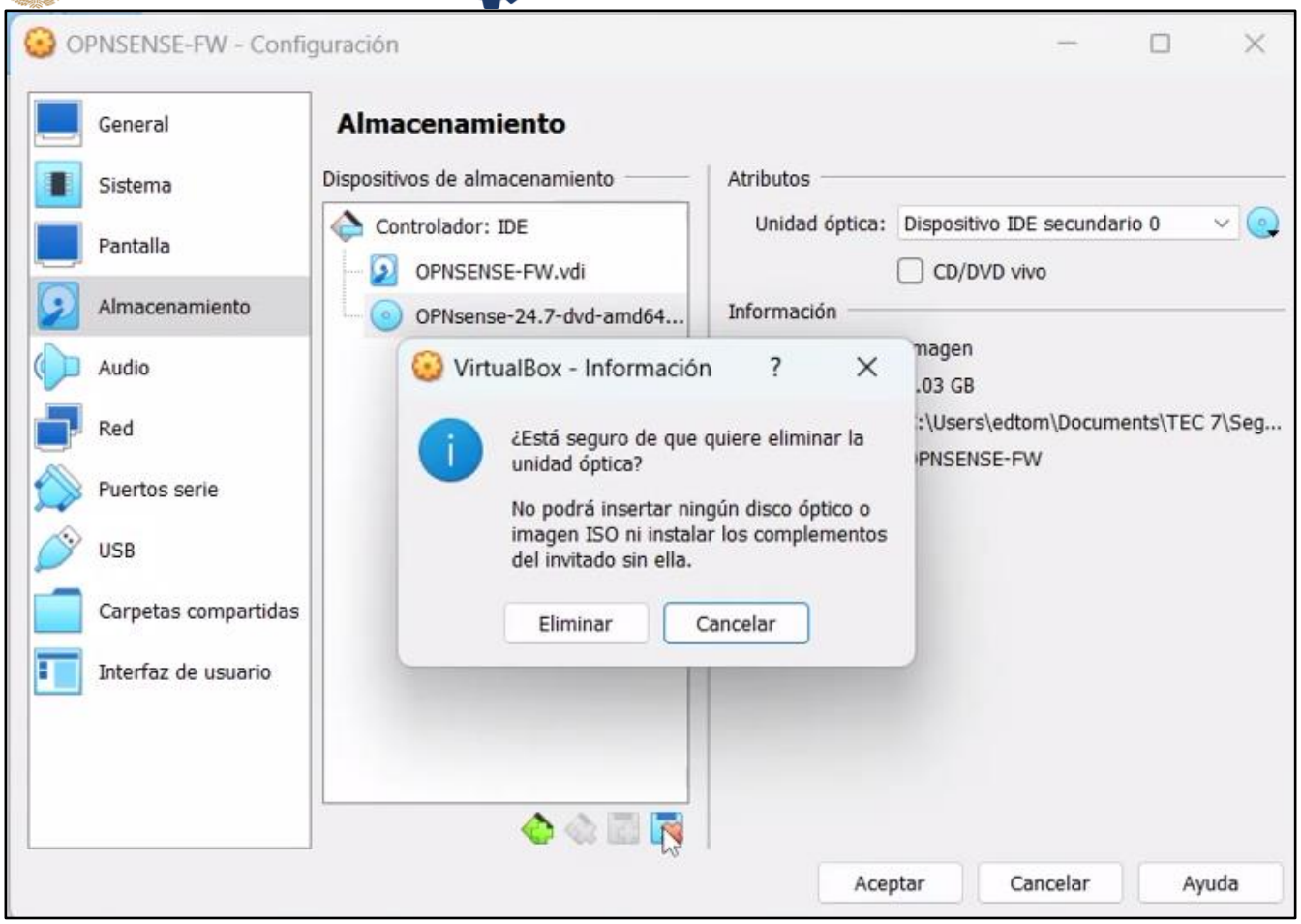


*Ilustración 26. Configuración OPNsense pt 10*

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

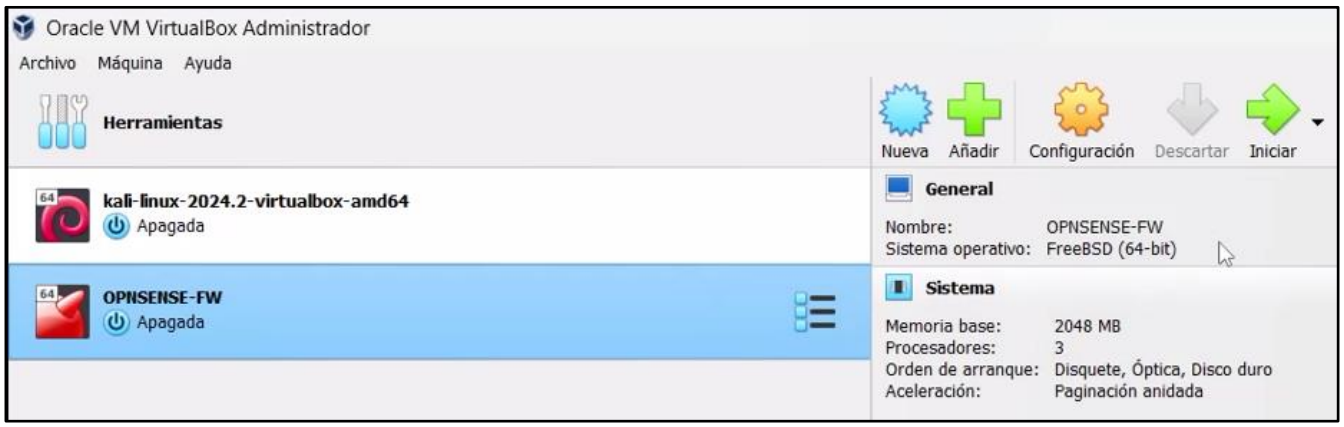


*Ilustración 27. Configuración OPNsense pt 11*

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

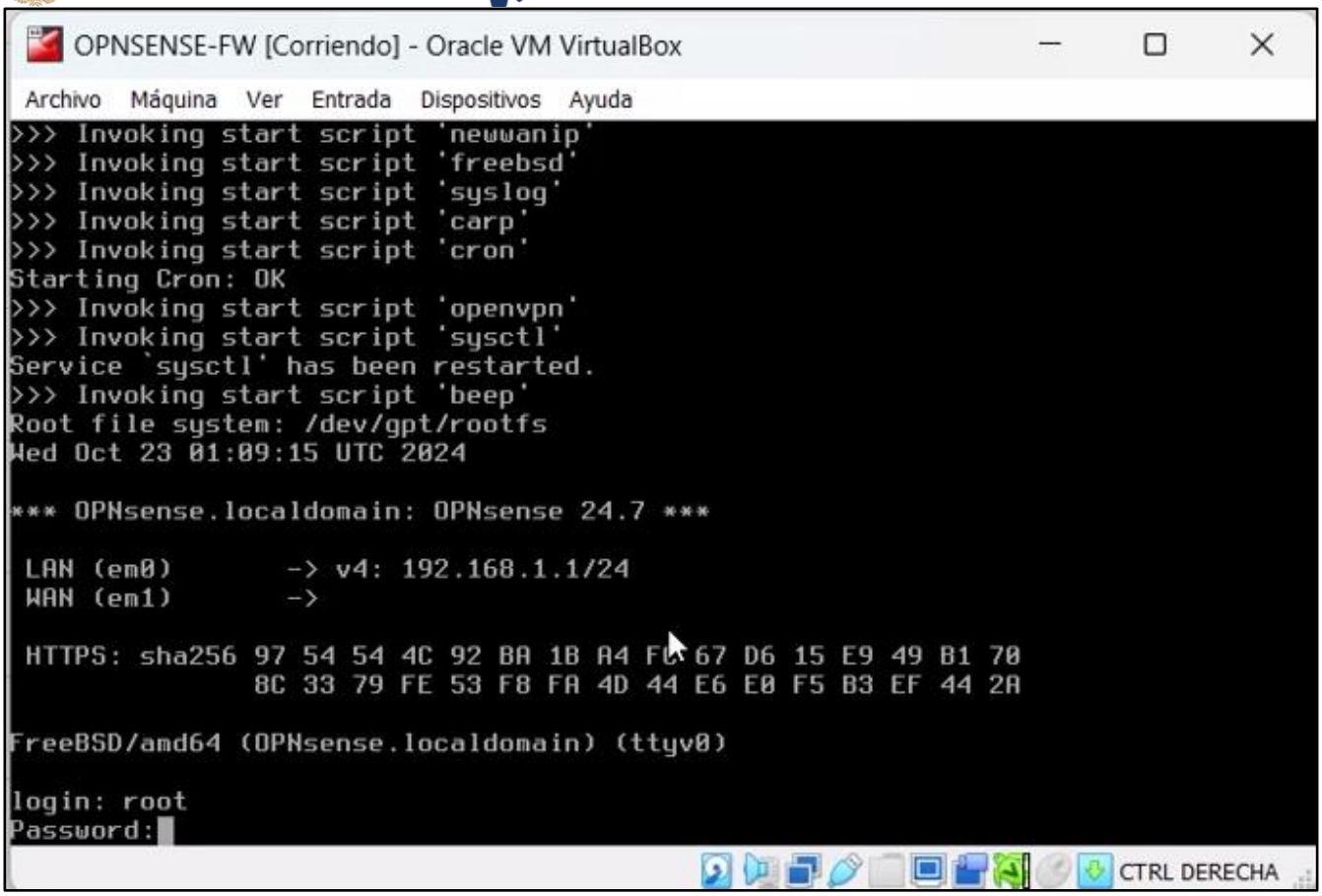


*Ilustración 28. Inicio de OPNsense*

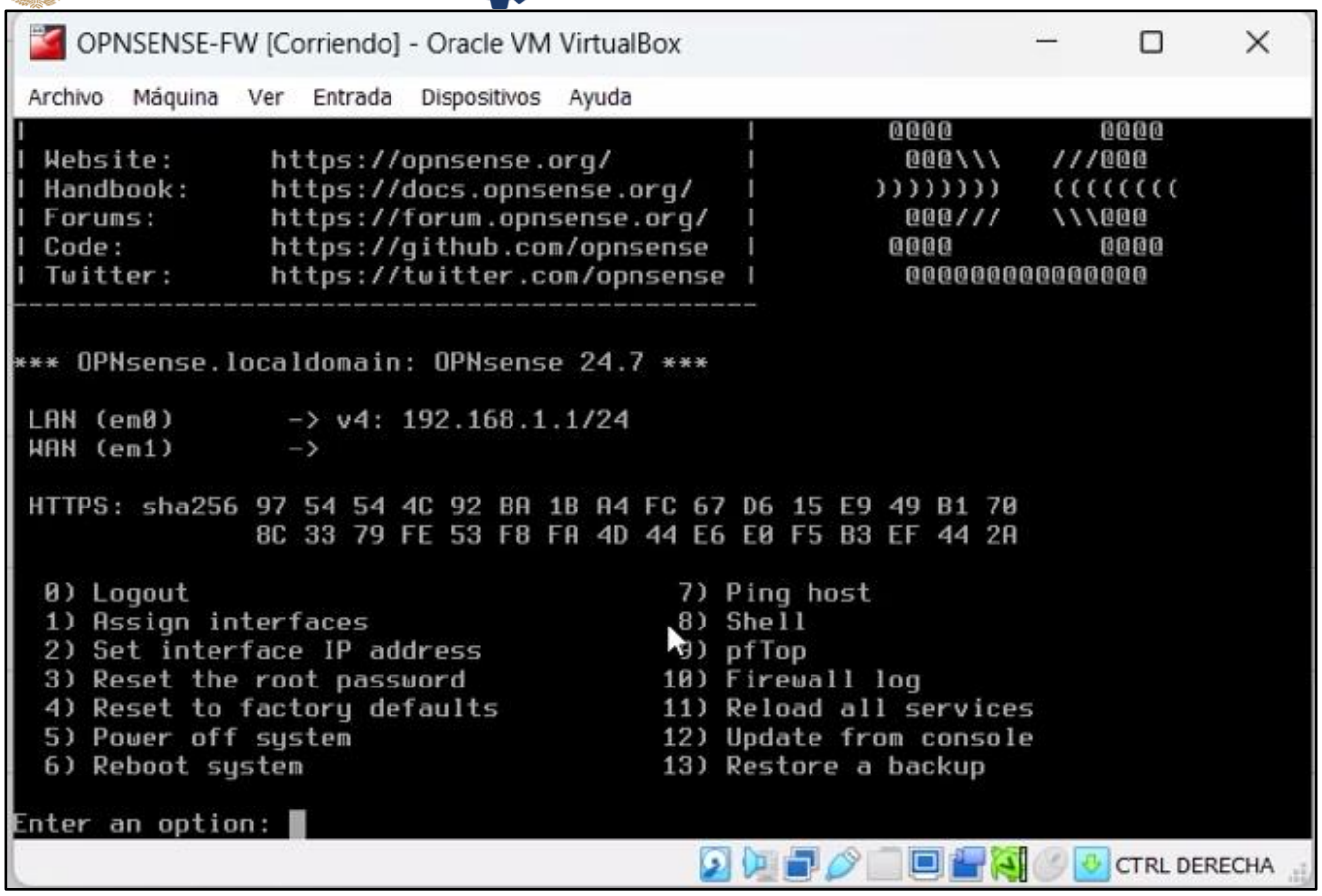


*Ilustración 29. Inicio de OPNsense pt 2*

**e)** Asignamos las interfaces

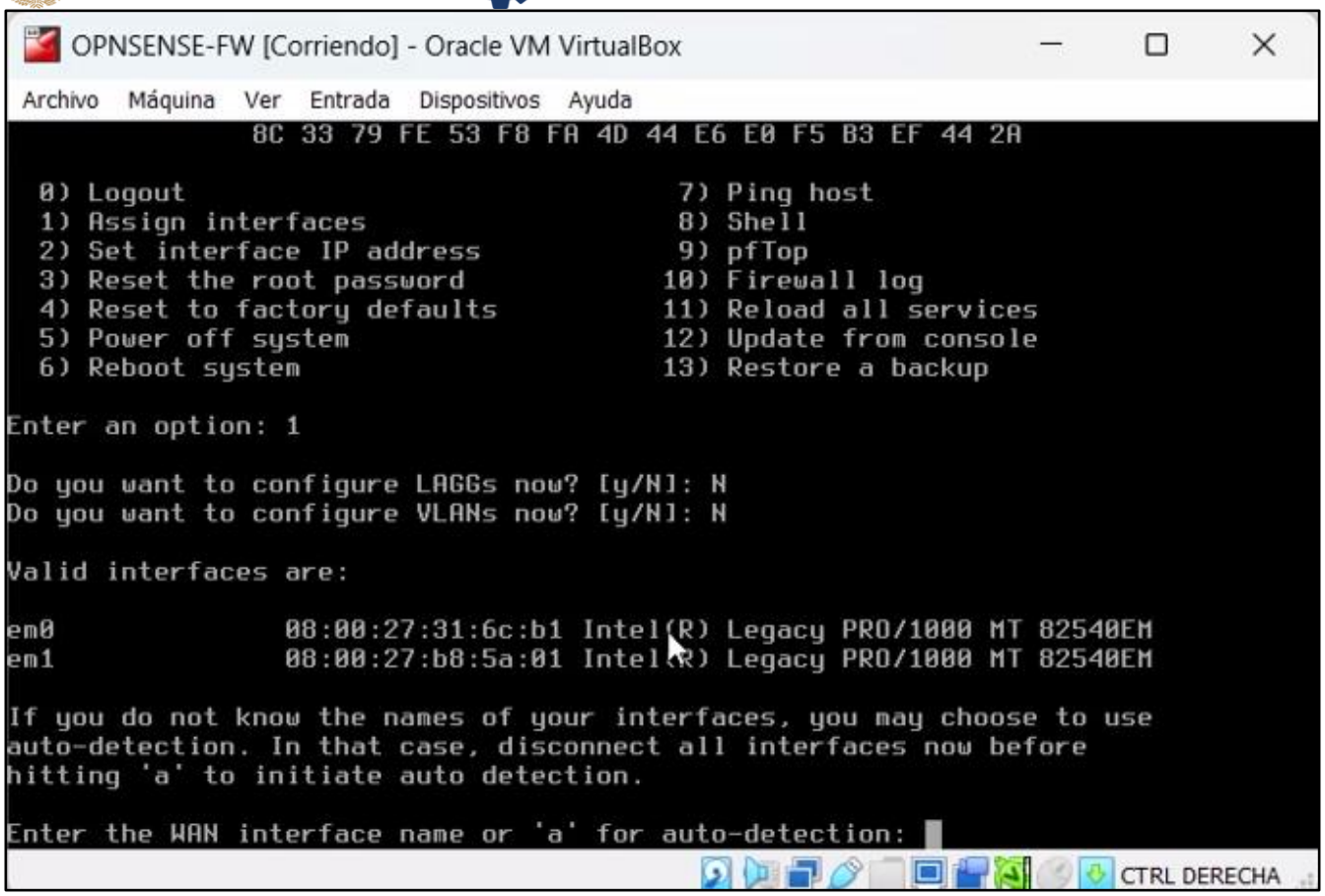


*Ilustración 30. Inicio de OPNsense pt 3*

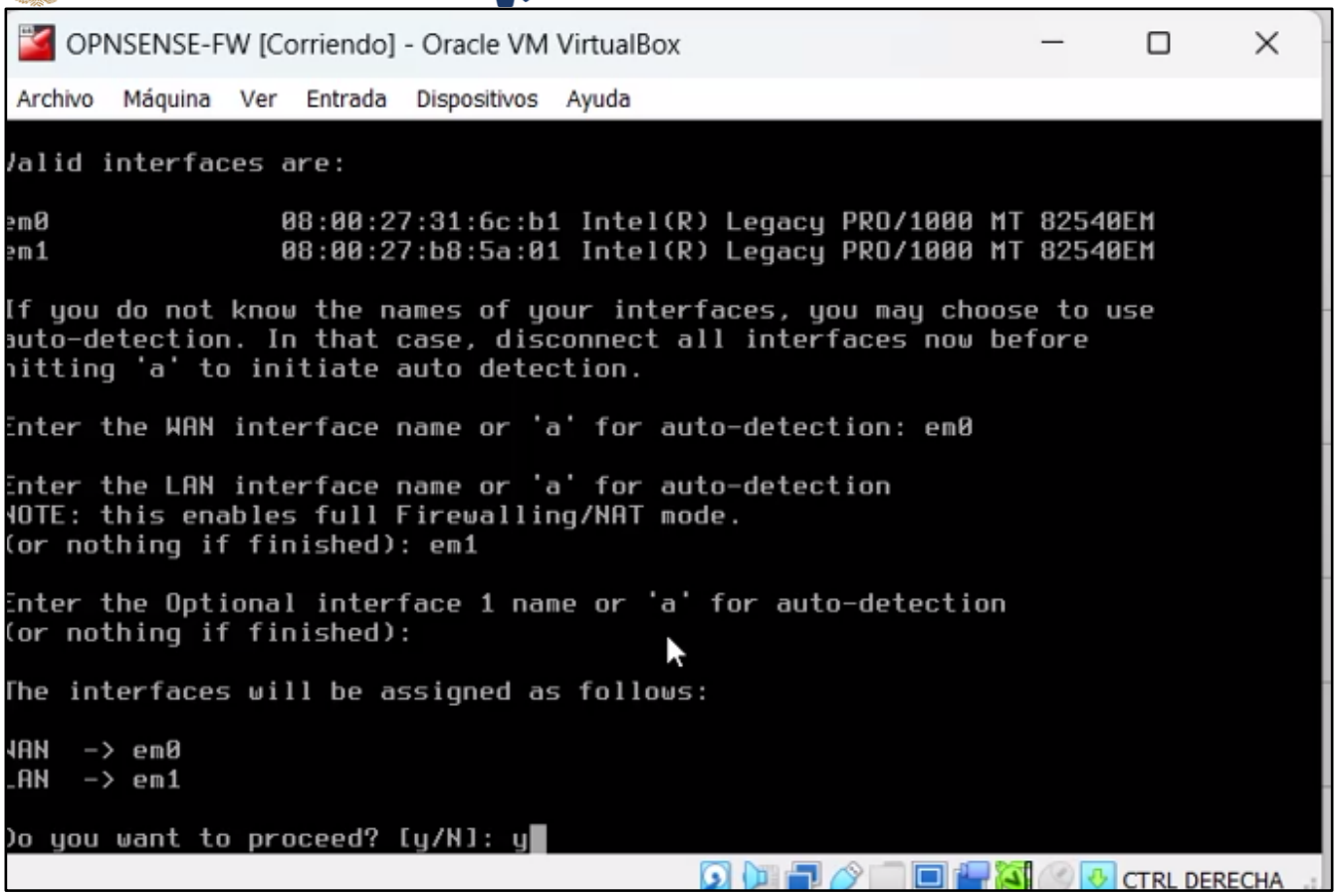


*Ilustración 31. Inicio de OPNsense pt 4*

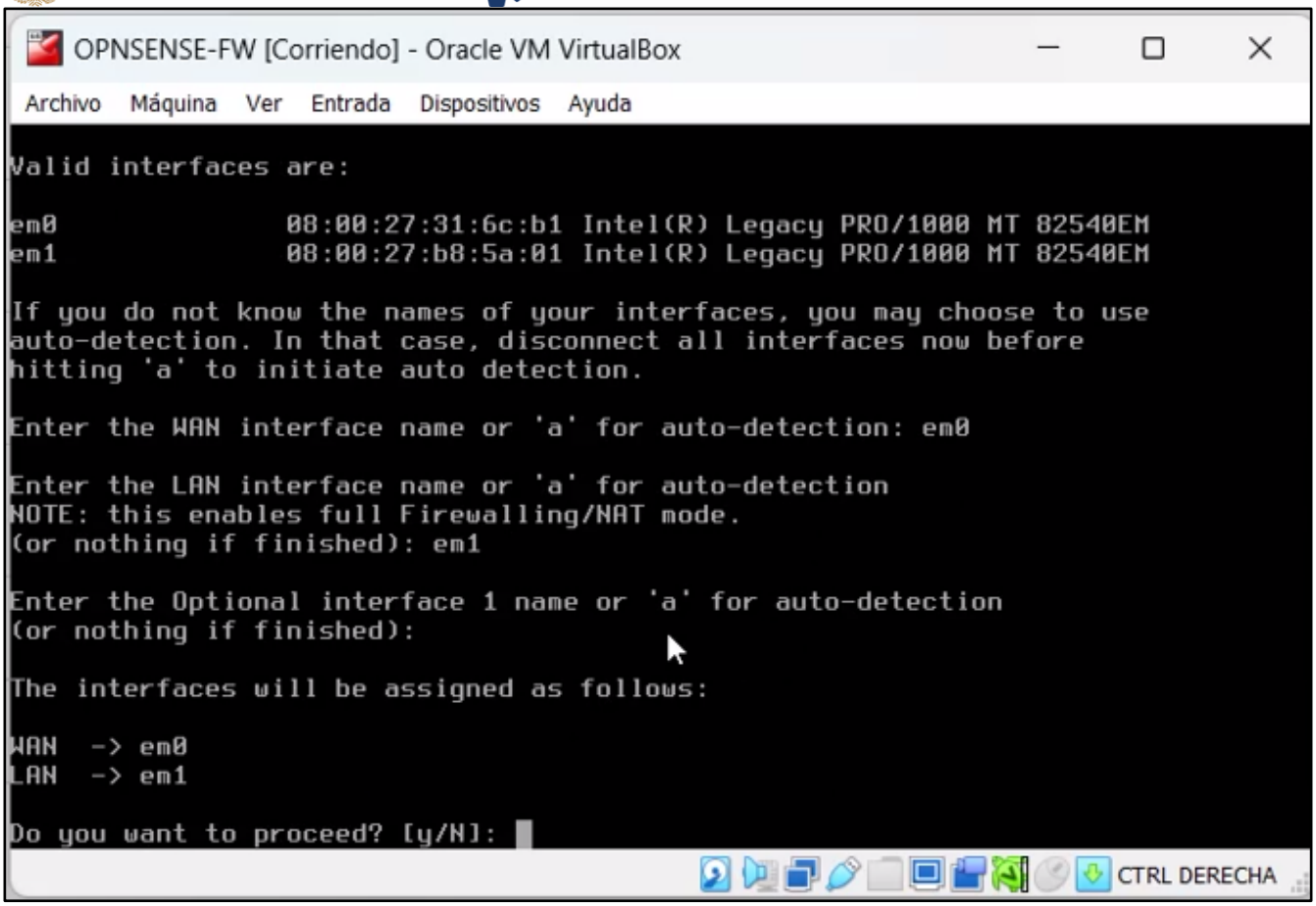


*Ilustración 32. Inicio de OPNsense pt 5*

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

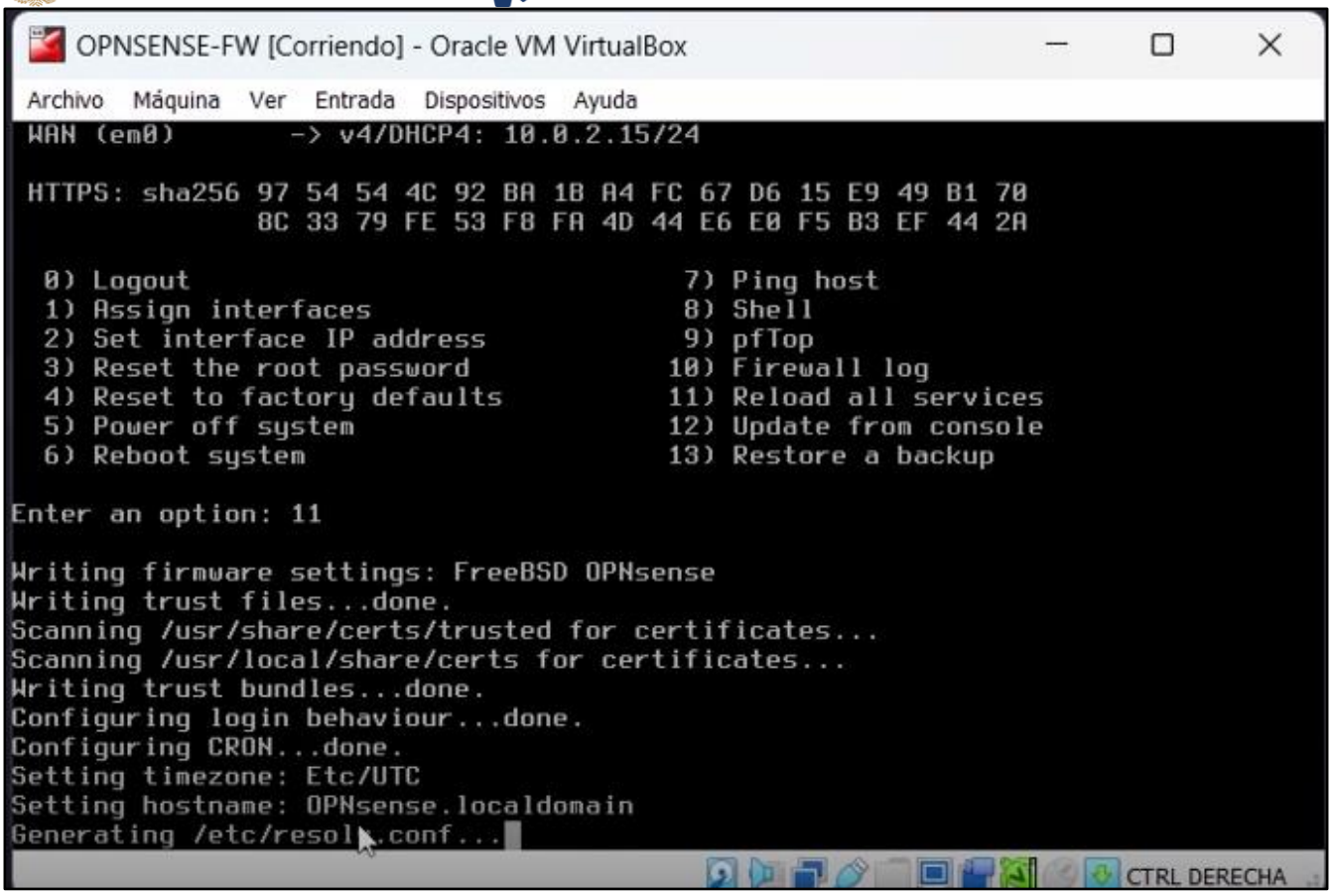


*Ilustración 33. Actualización de OPNsense*

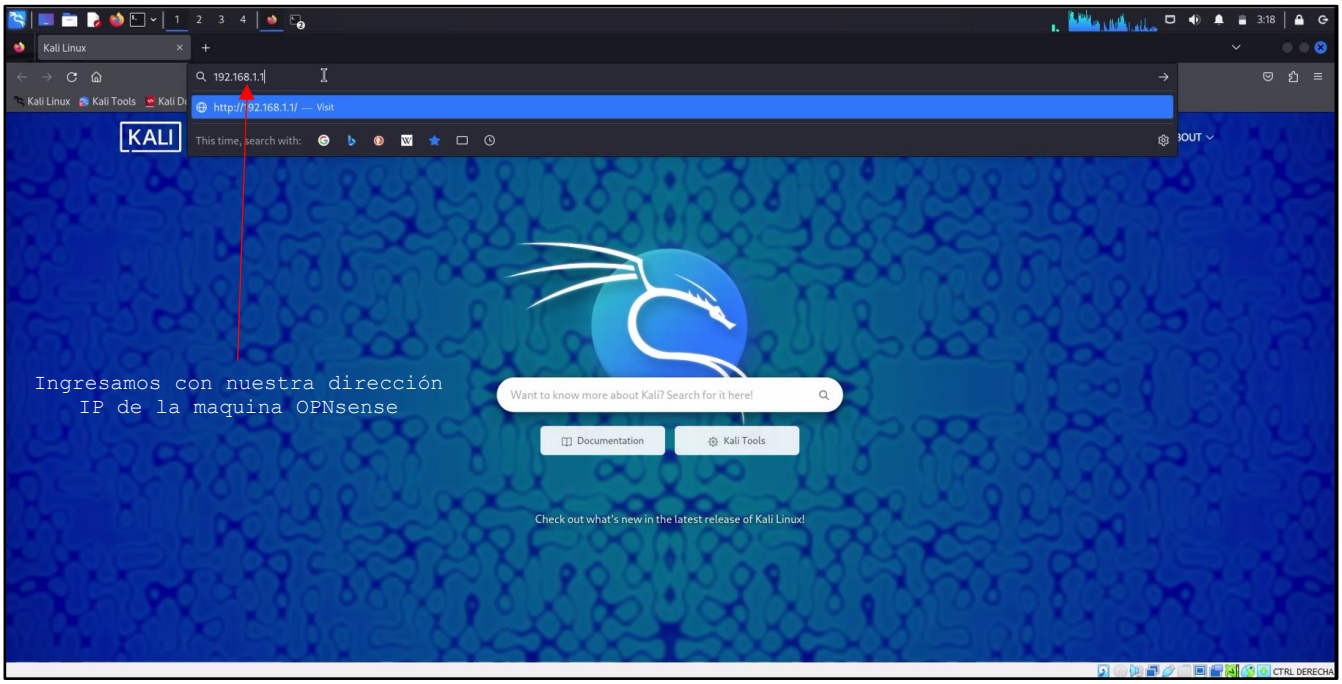


*Ilustración 34. Ingreso a la interfaz de OPNsense*

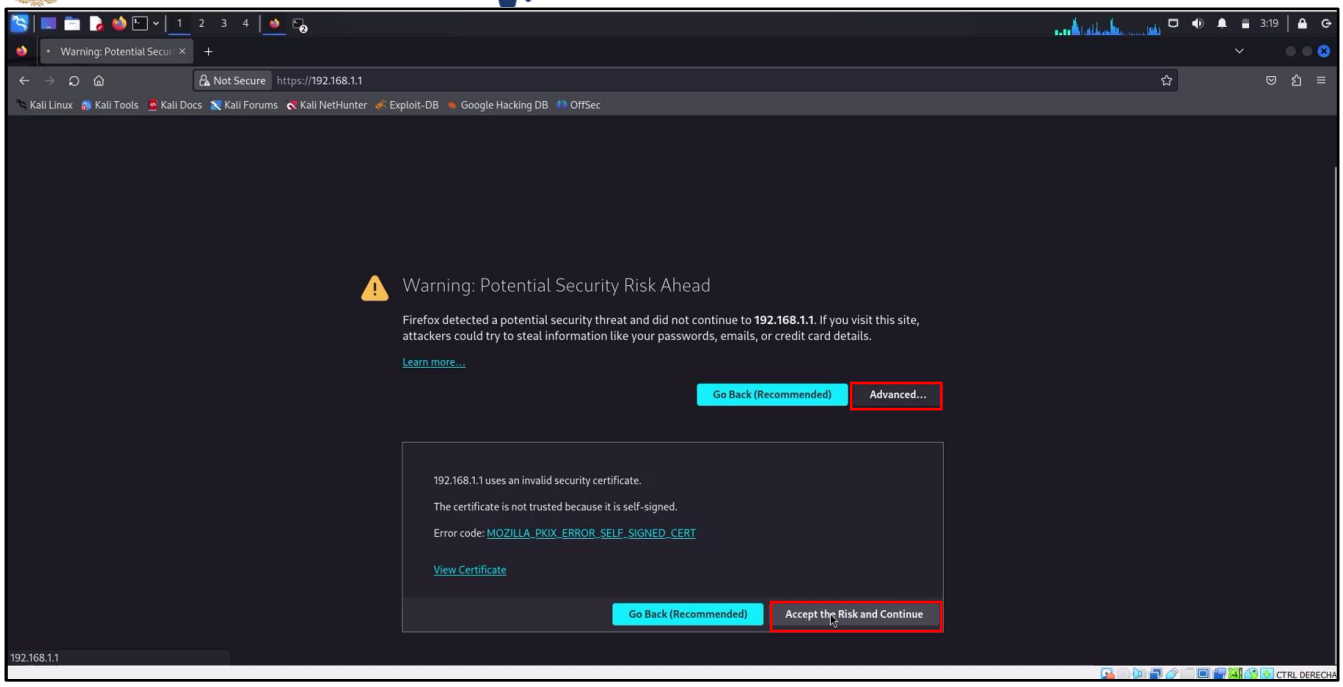


*Ilustración 35. Ingreso a la interfaz de OPNsense pt 2*

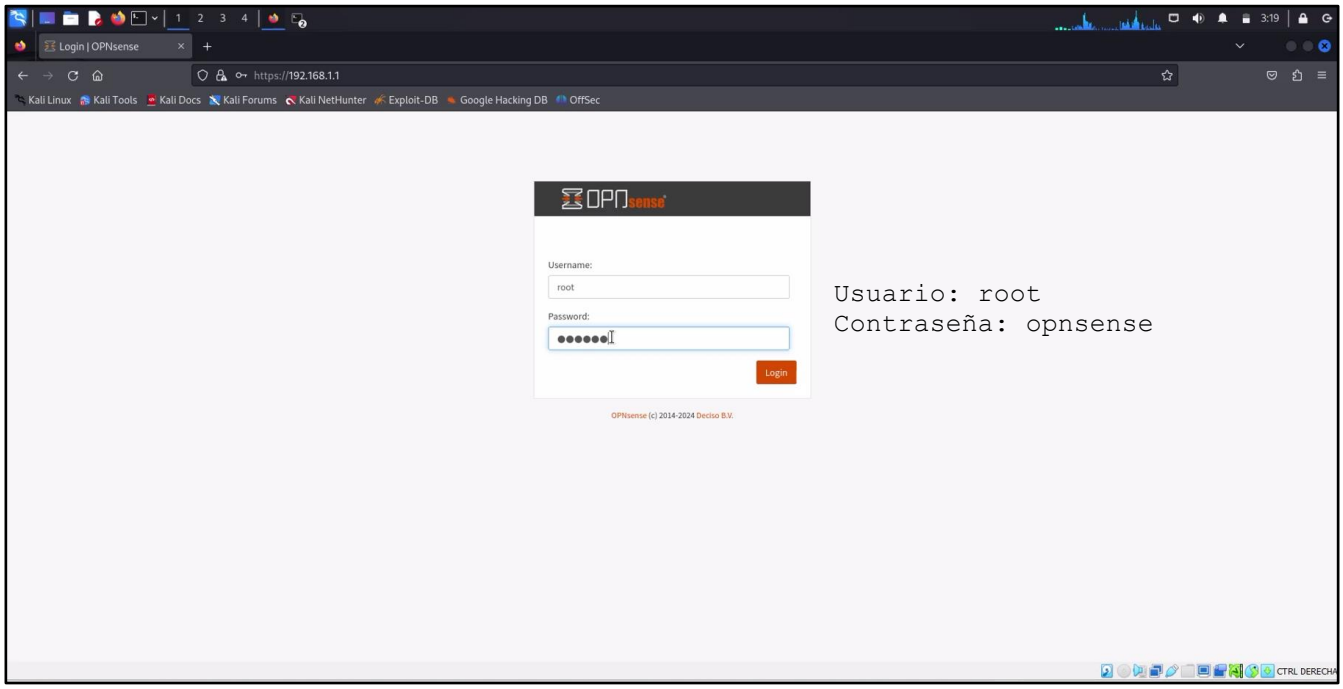


*Ilustración 36. Ingreso a la interfaz de OPNsense pt 3*

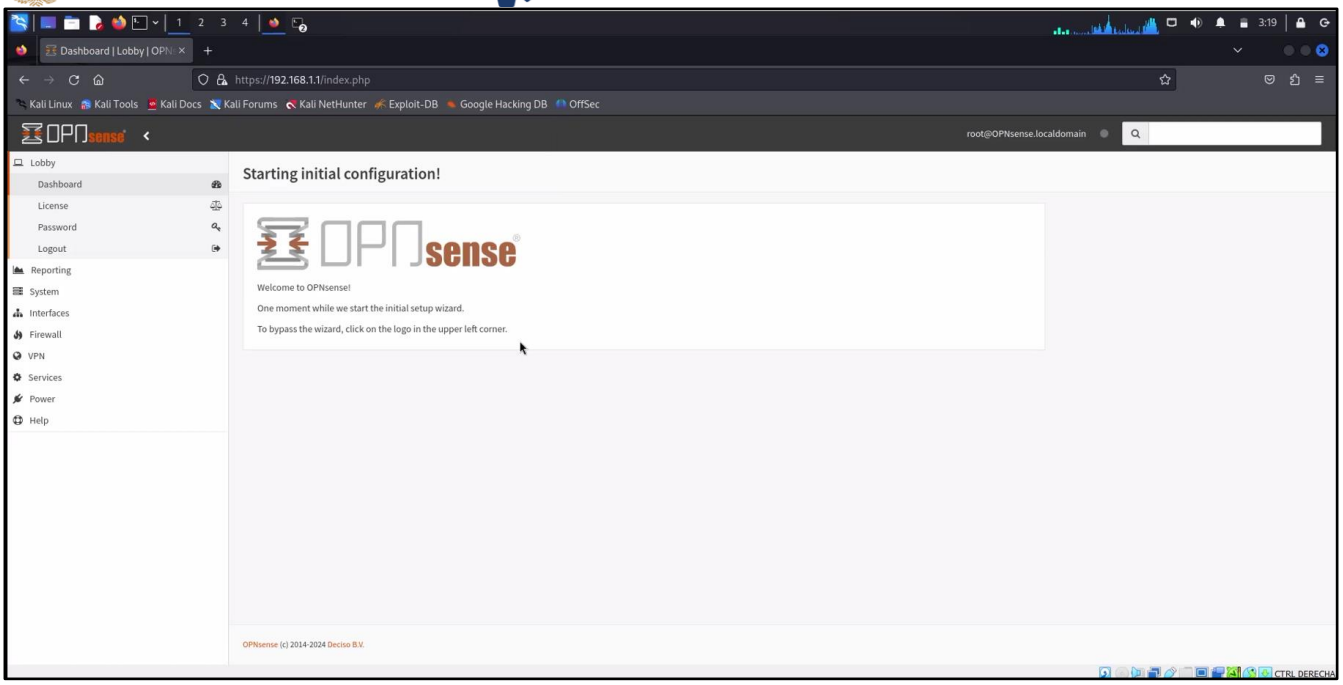


*Ilustración 37. Ingreso a la interfaz de OPNsense pt 4*

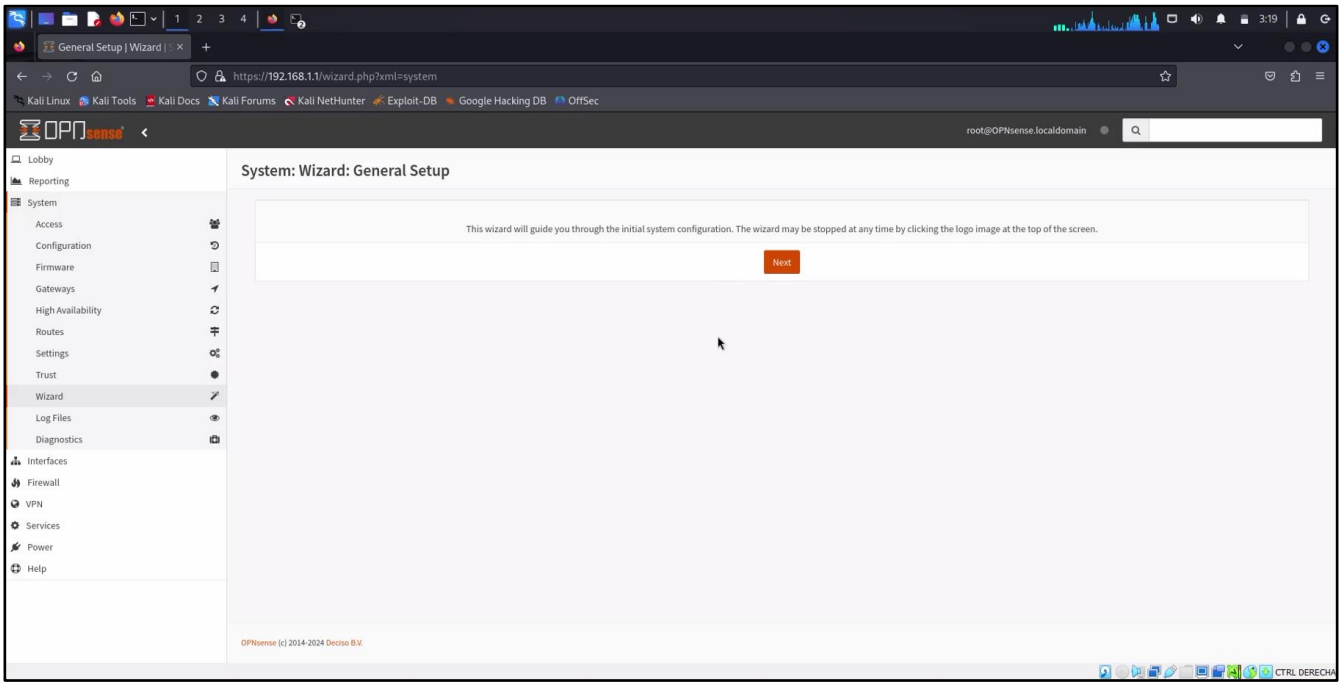


*Ilustración 38. Ingreso a la interfaz de OPNsense pt 5*

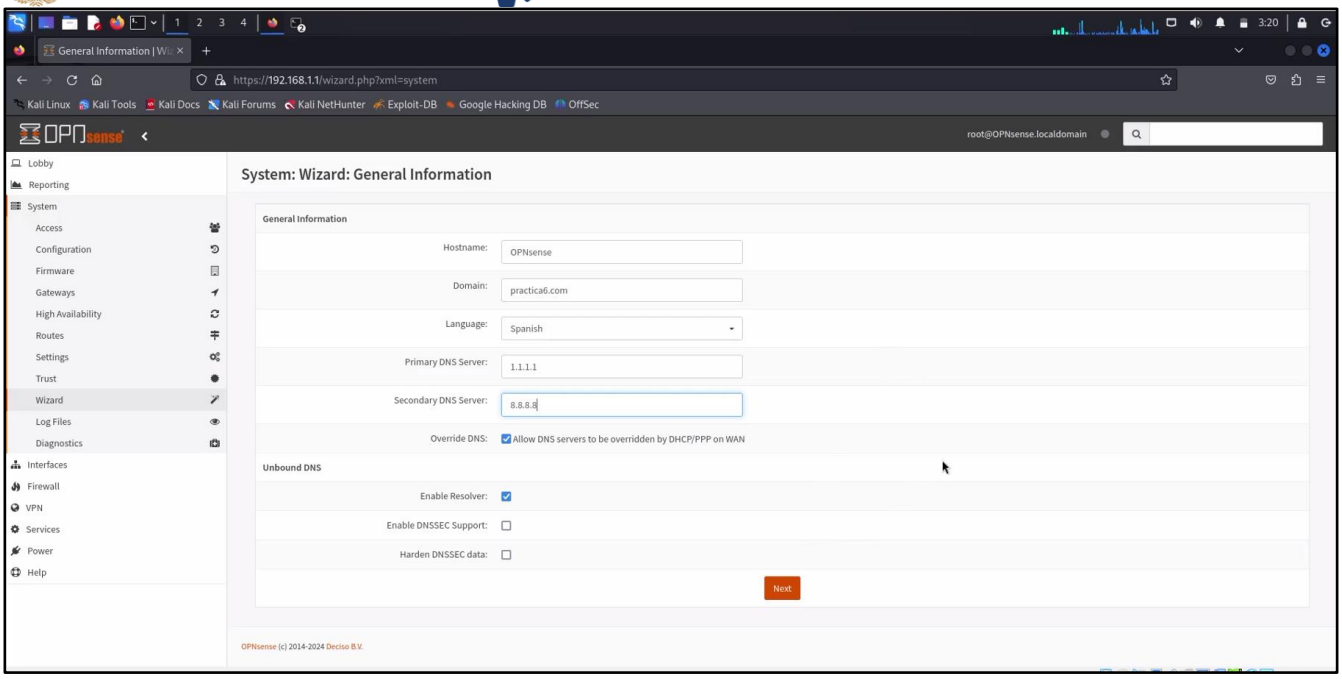


*Ilustración 39. Ingreso a la interfaz de OPNsense pt 6*

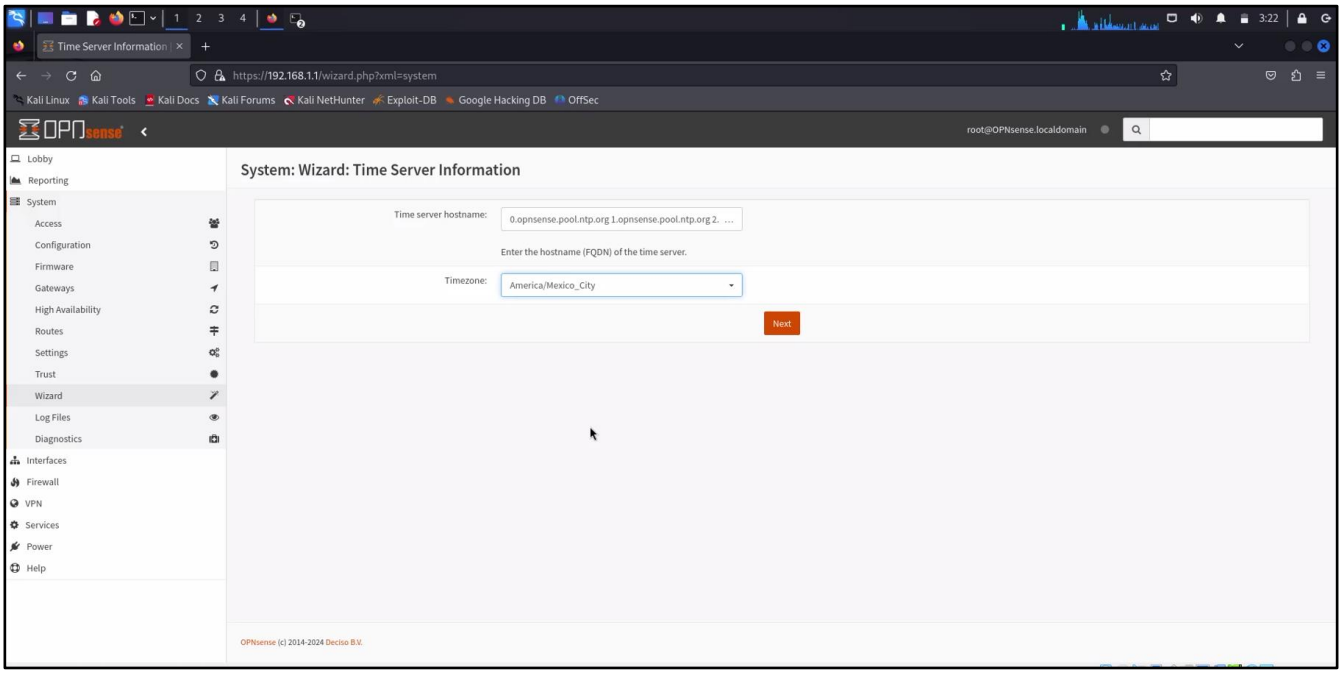


*Ilustración 40. Ingreso a la interfaz de OPNsense pt 7*

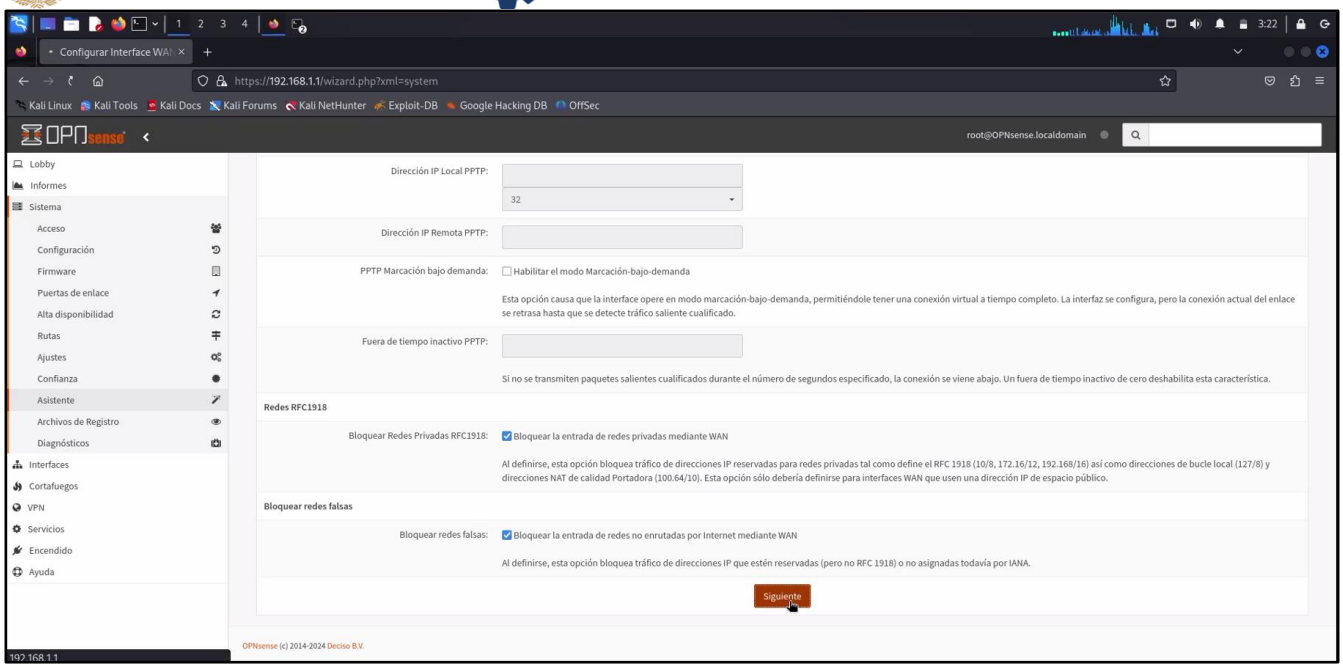


*Ilustración 41. Ingreso a la interfaz de OPNsense pt 8*

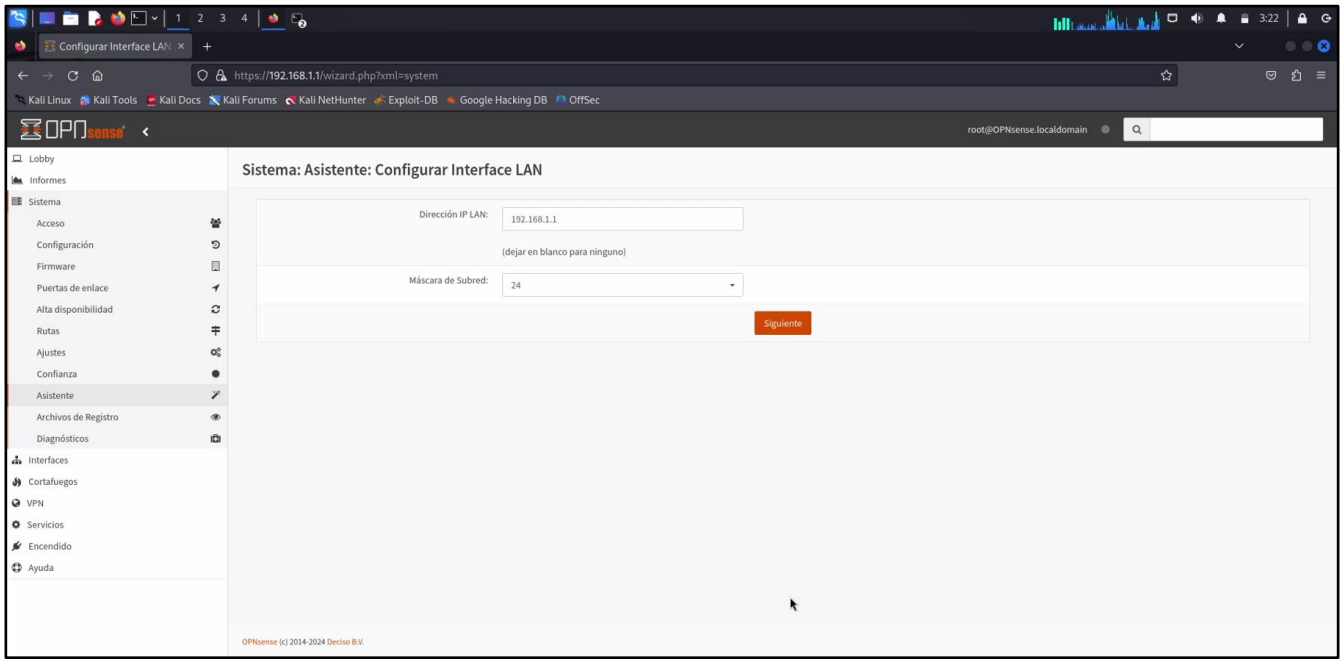


*Ilustración 42. Ingreso a la interfaz de OPNsense pt 9*

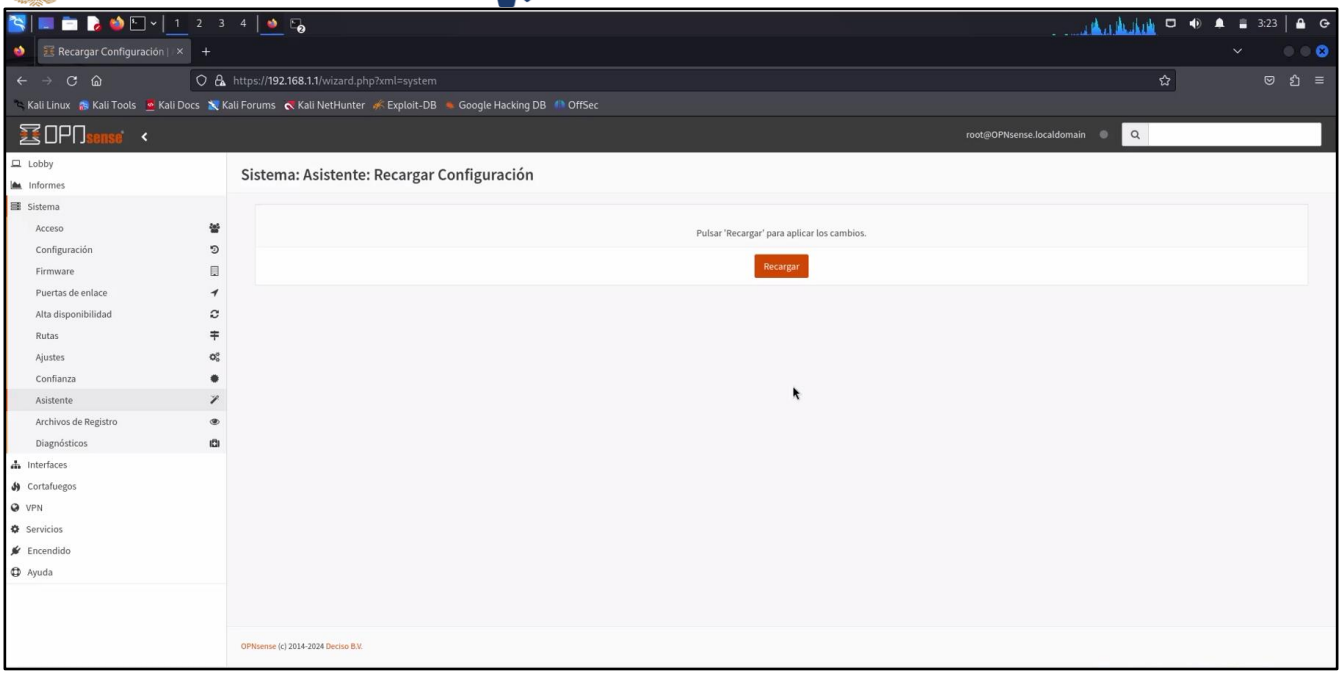


*Ilustración 43. Ingreso a la interfaz de OPNsense pt 10*

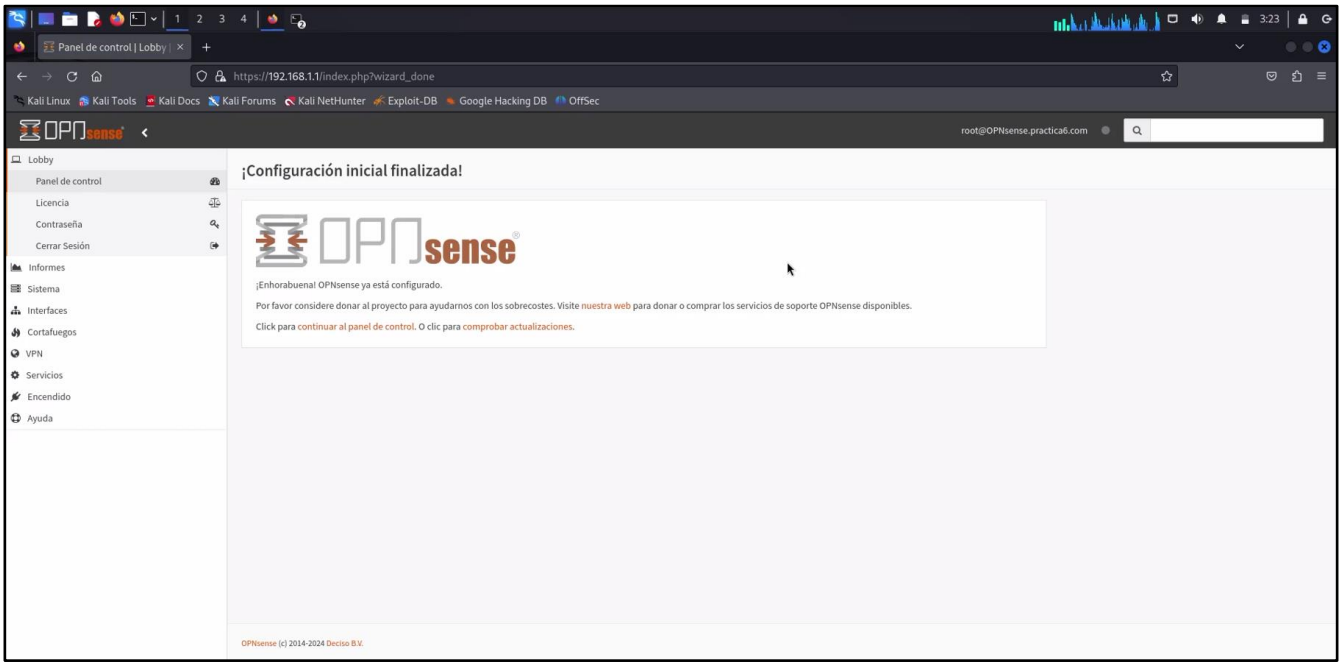


*Ilustración 44. Ingreso a la interfaz de OPNsense pt 11*

# 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

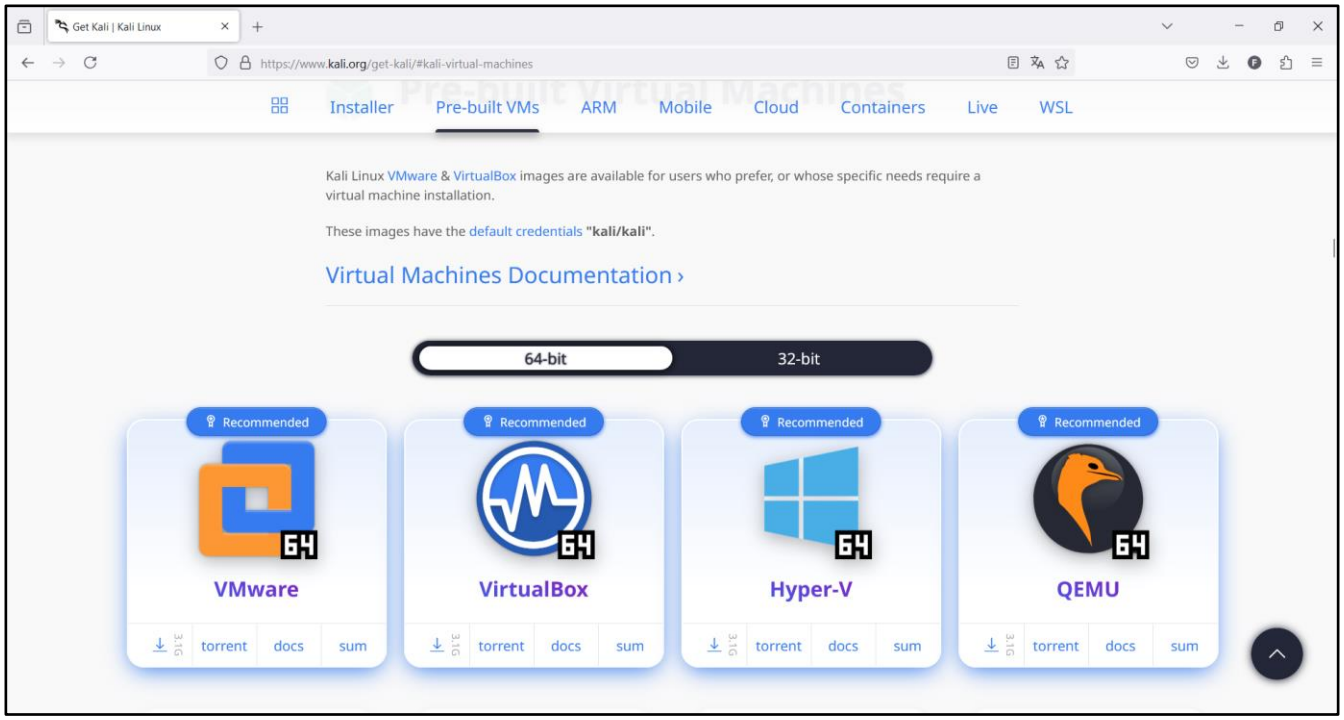


*Ilustración 45. Descarga de Kali Linux*

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

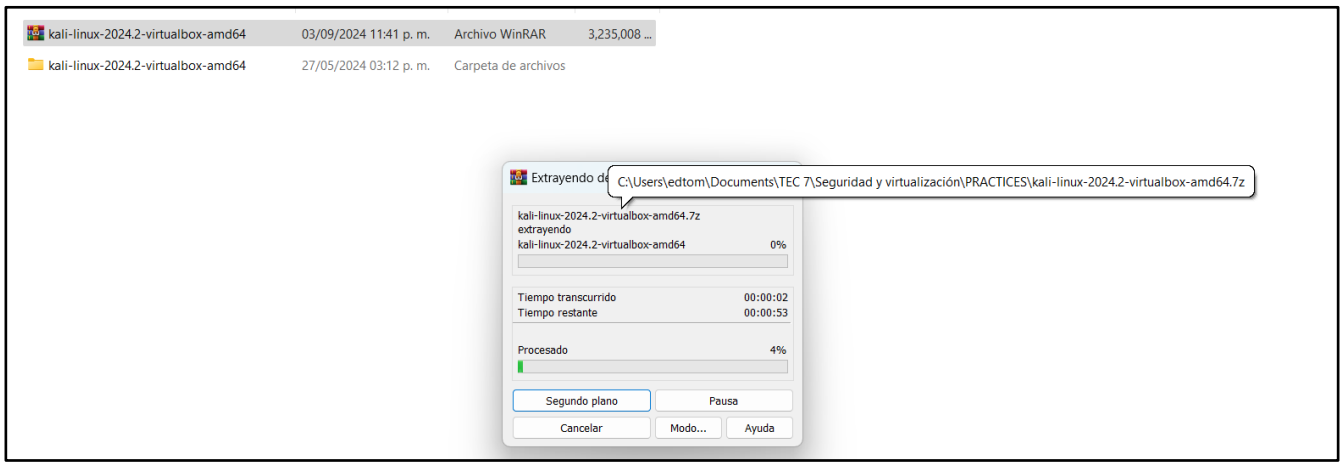


*Ilustración 46. Pre-Instalación Kali Linux*

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

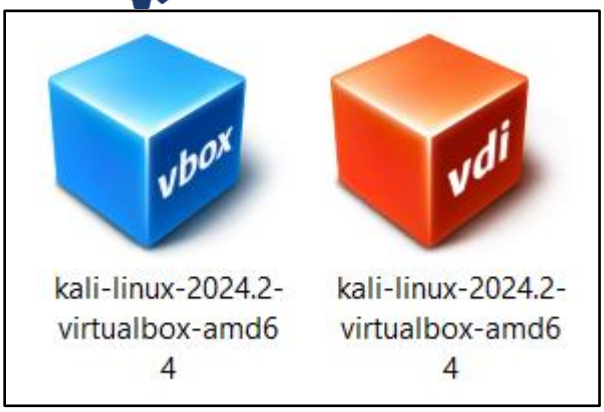


*Ilustración 47. Pre-Instalación Kali Linux pt 2*

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

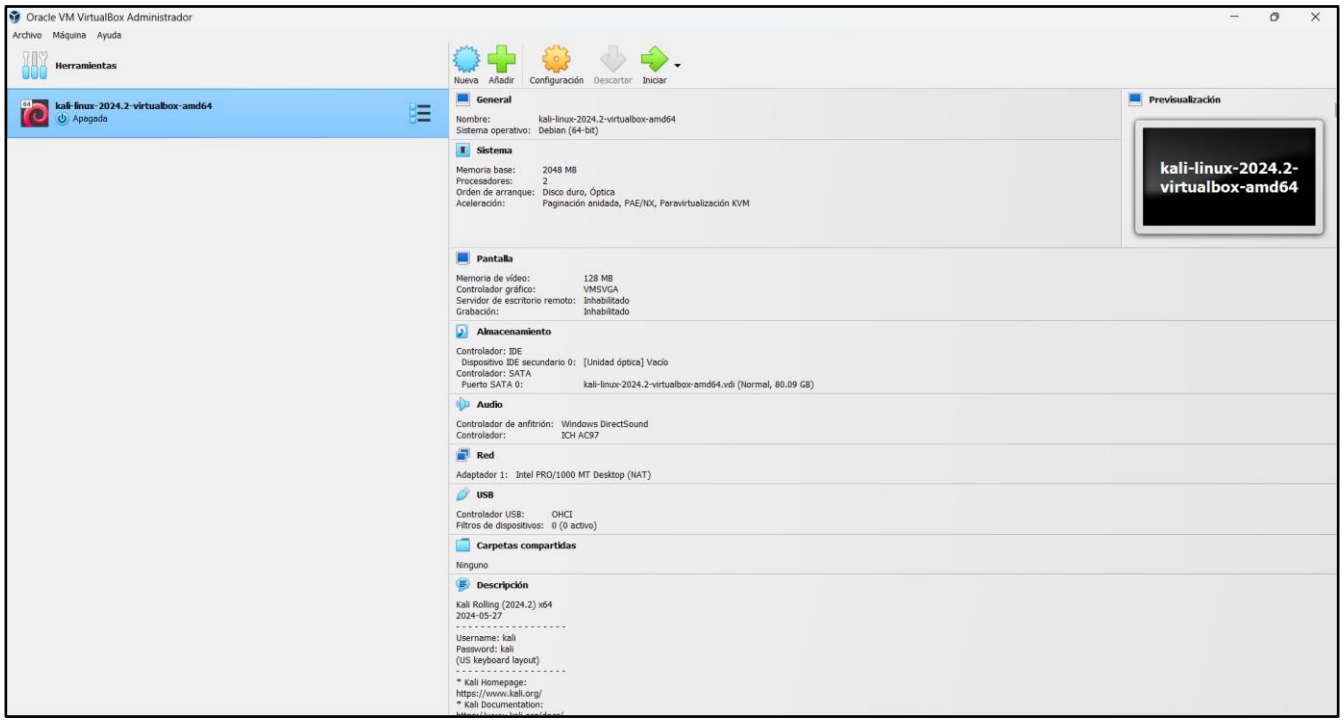


*Ilustración 48. Configuración MV Kali Linux*

**Configuración:**

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

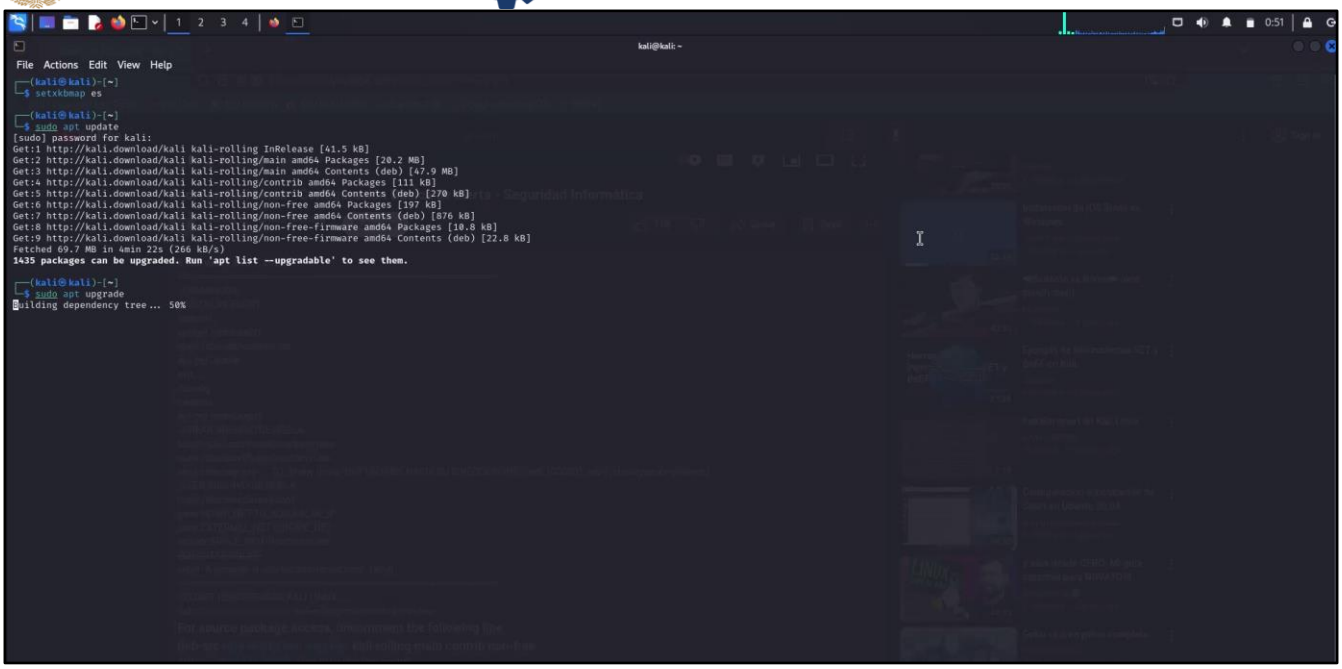


*Ilustración 49. Actualización Kali Linux*

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

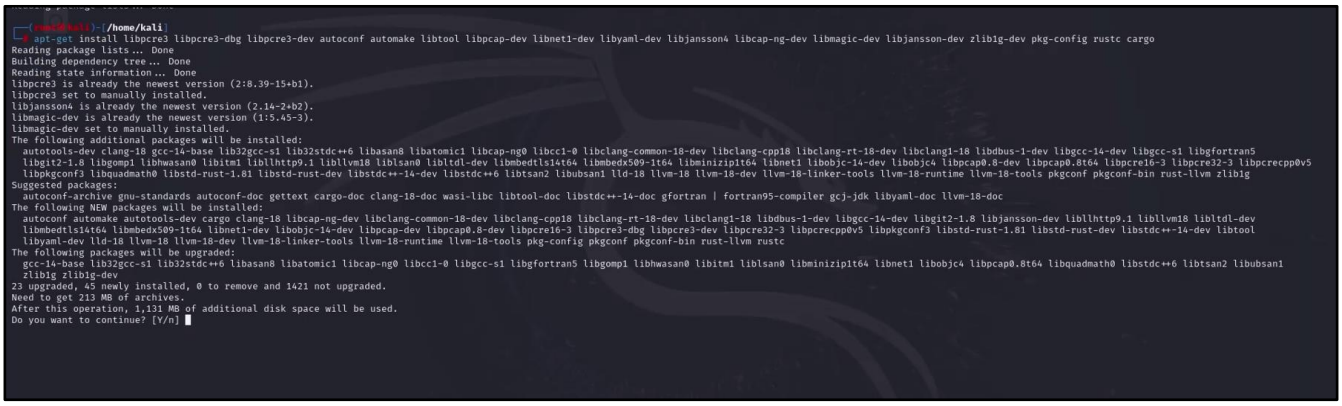


*Ilustración 50. Paquetes necesarios*

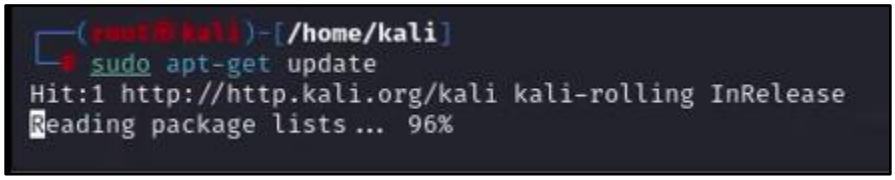


*Ilustración 51. Actualización Kali Linux pt 2*

**c)** Instalamos suricata y más dependencias

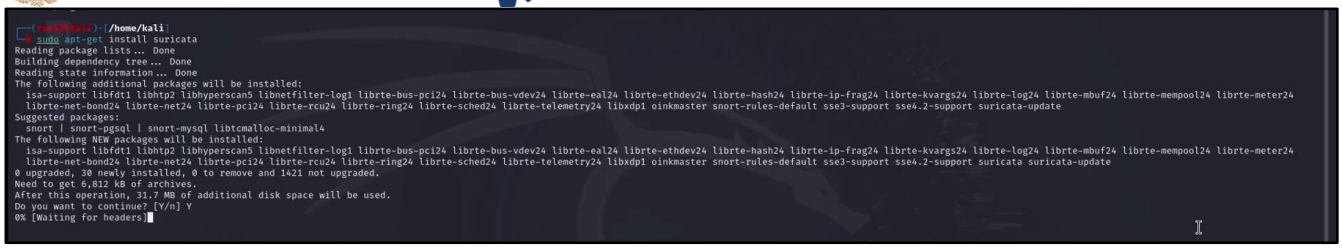


*Ilustración 52. Suricata*


*Ilustración 53. Dependencias Suricata*

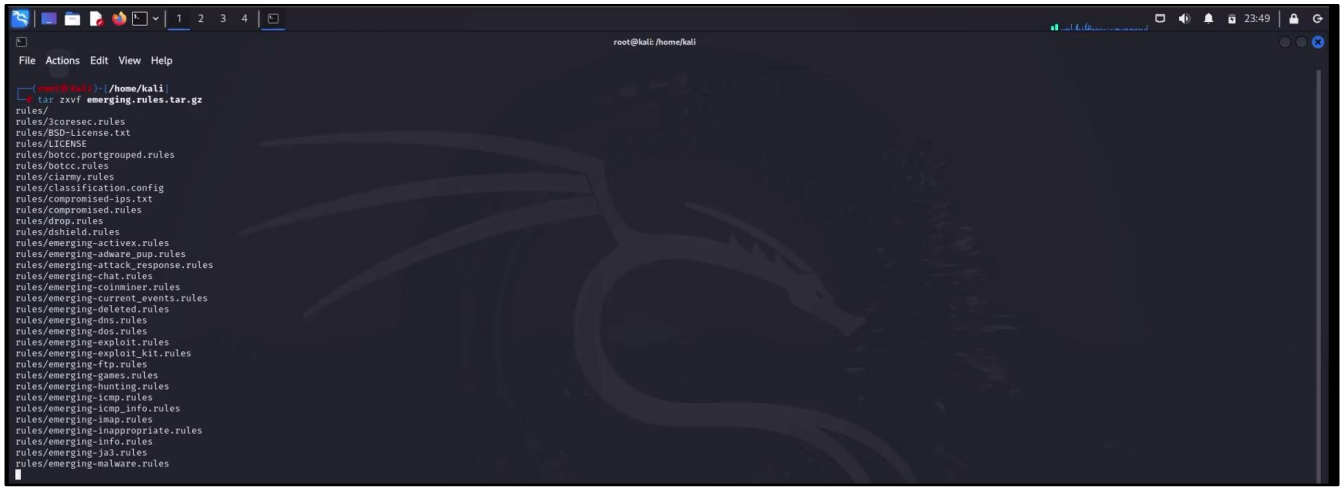


*Ilustración 54. Dependencias Suricata pt 2*

**c)** Movemos “rules”, creamos “my-rules” y modificamos “my-rules”


*Ilustración 55. Cambio de direcciones*

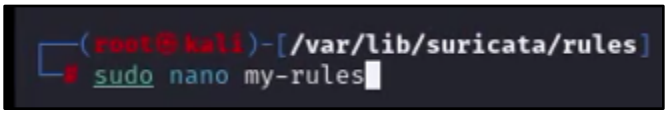


*Ilustración 56. Creación de archivos*

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 maquina virtual


*Ilustración 57. Rules*

**d)** Modificamos otros archivos

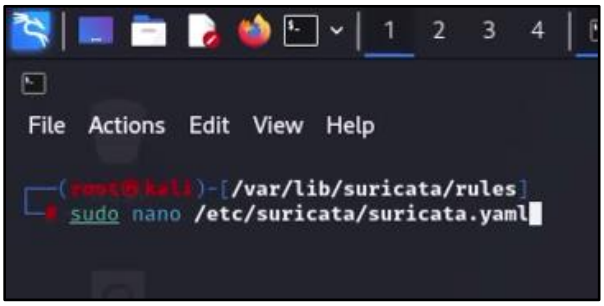


*Ilustración 58. Implementación de las reglas*

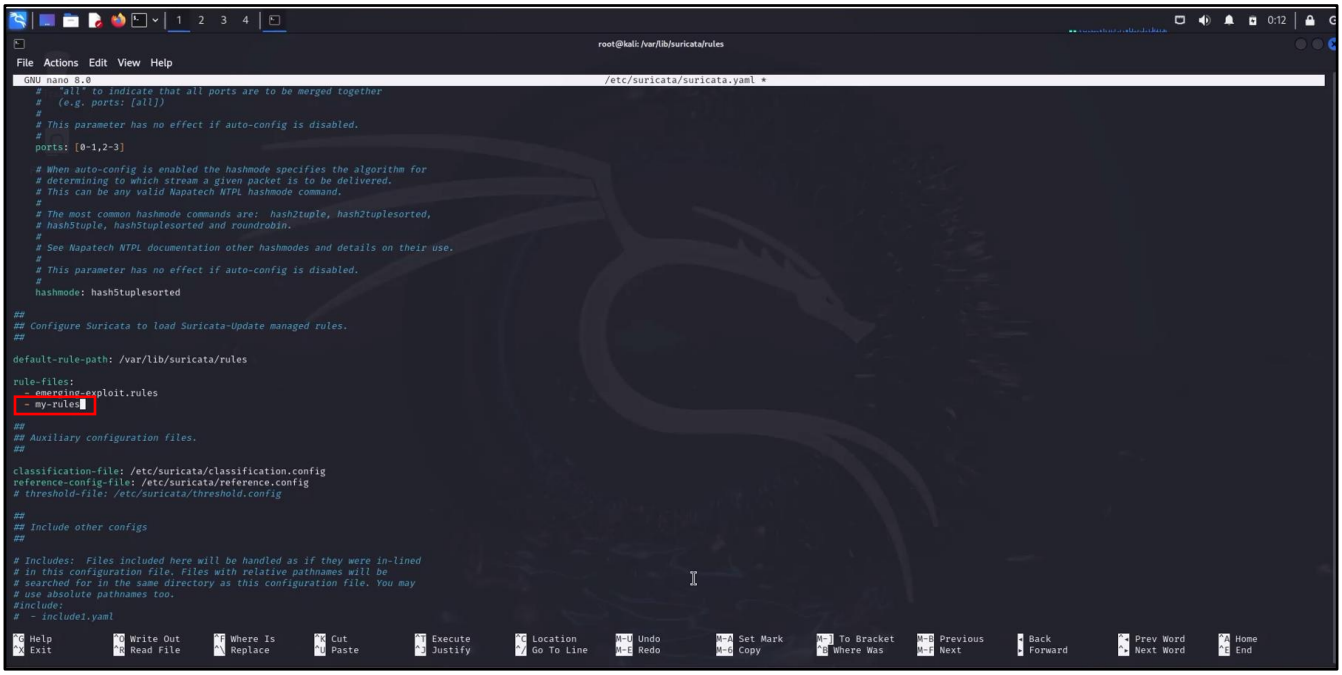


*Ilustración 59. Declaración de reglas*

**e)** Ejecutamos

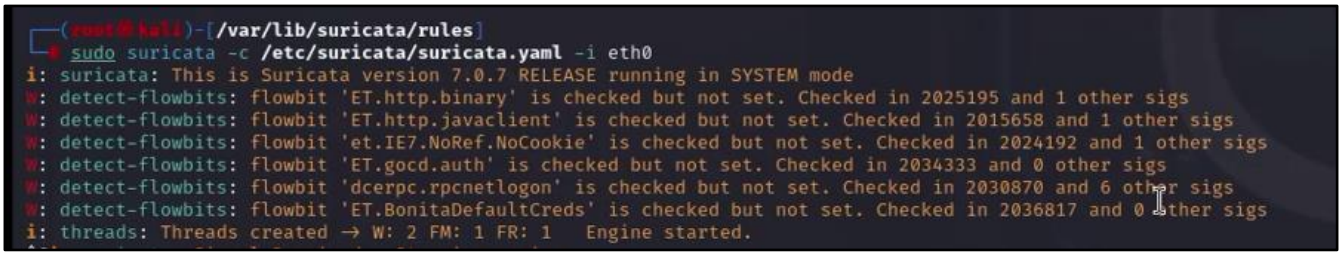


*Ilustración 60. Primeras dos reglas*

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

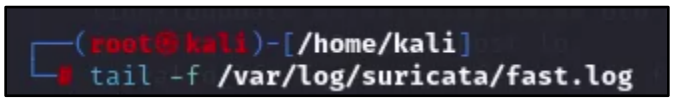


*Ilustración 61. Comando para la tercera regla*

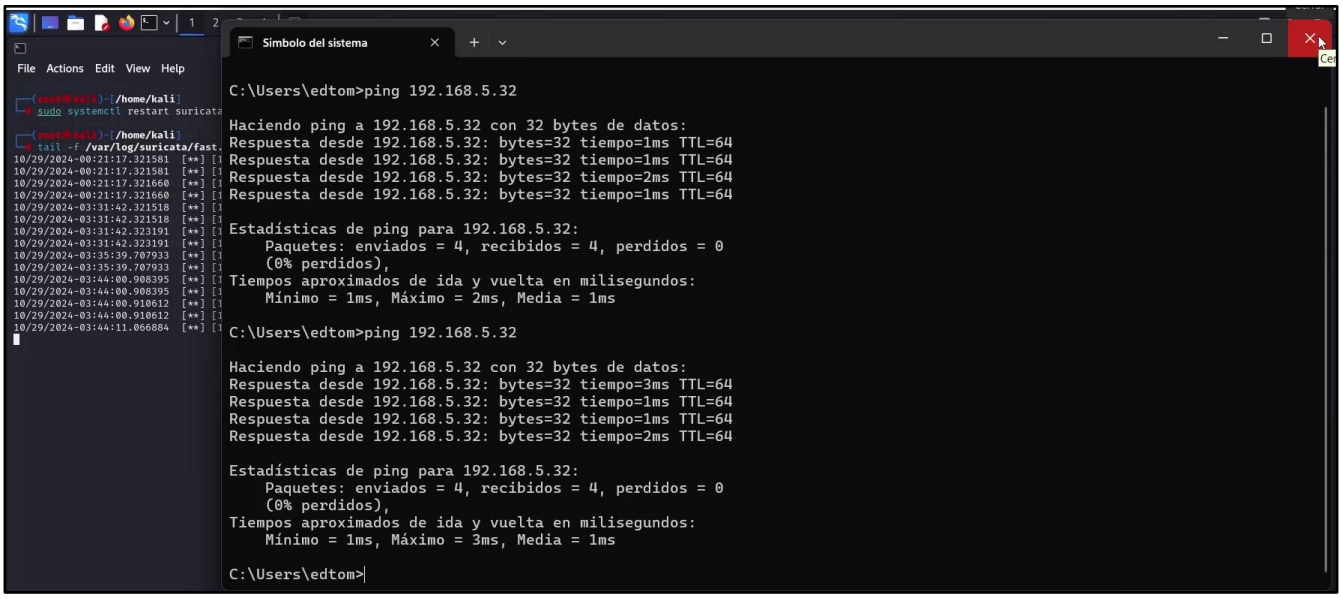


*Ilustración 62. Tercera regla*

## 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/

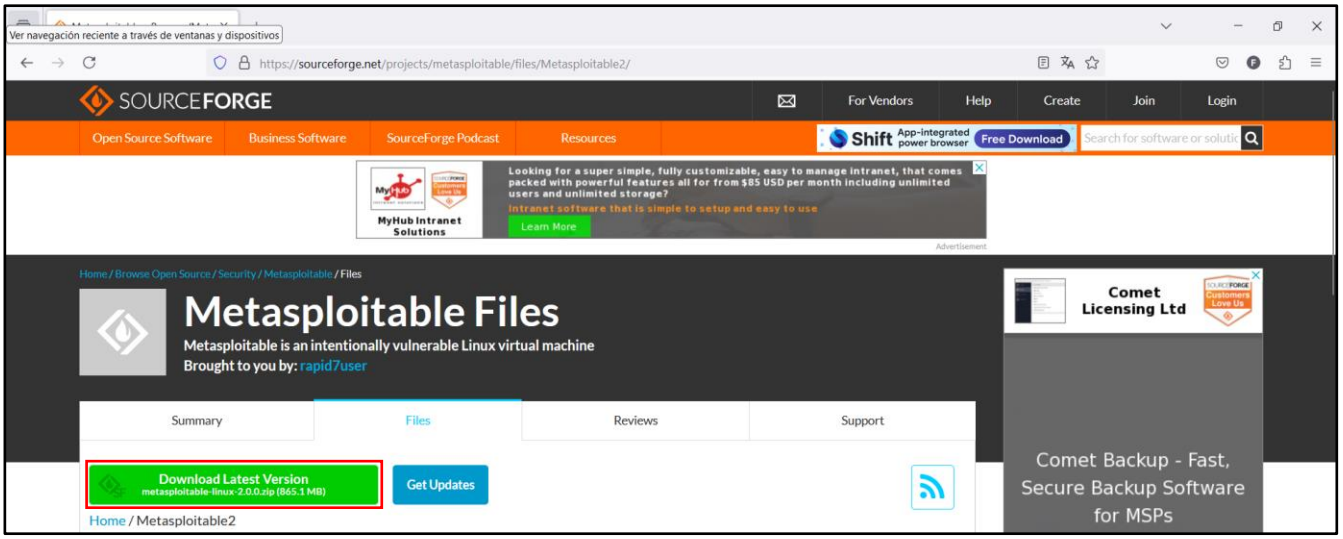


*Ilustración 63. Descarga metasploit2*

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

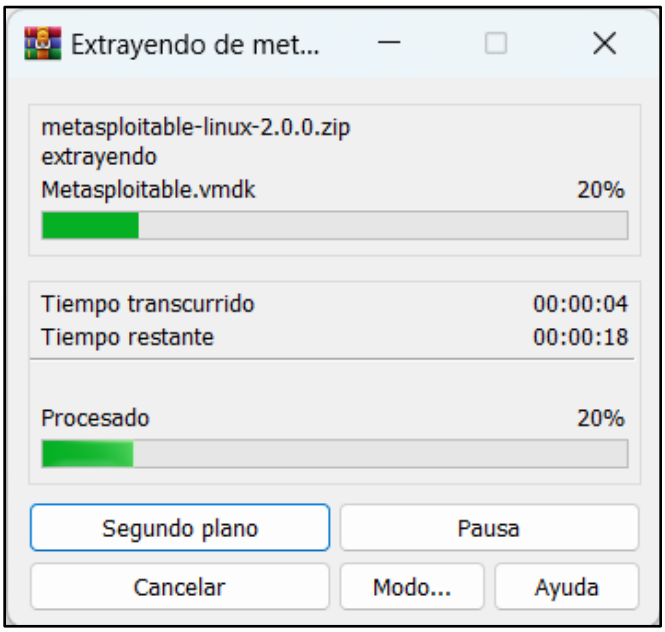


*Ilustración 64. Extracción de paquetes MS2*

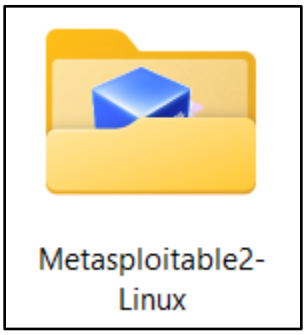


*Ilustración 65. Metasploit2*

**Configuración:**

**a)** Creamos la máquina virtual.


*Ilustración 66. Configuración MV metasploit2*

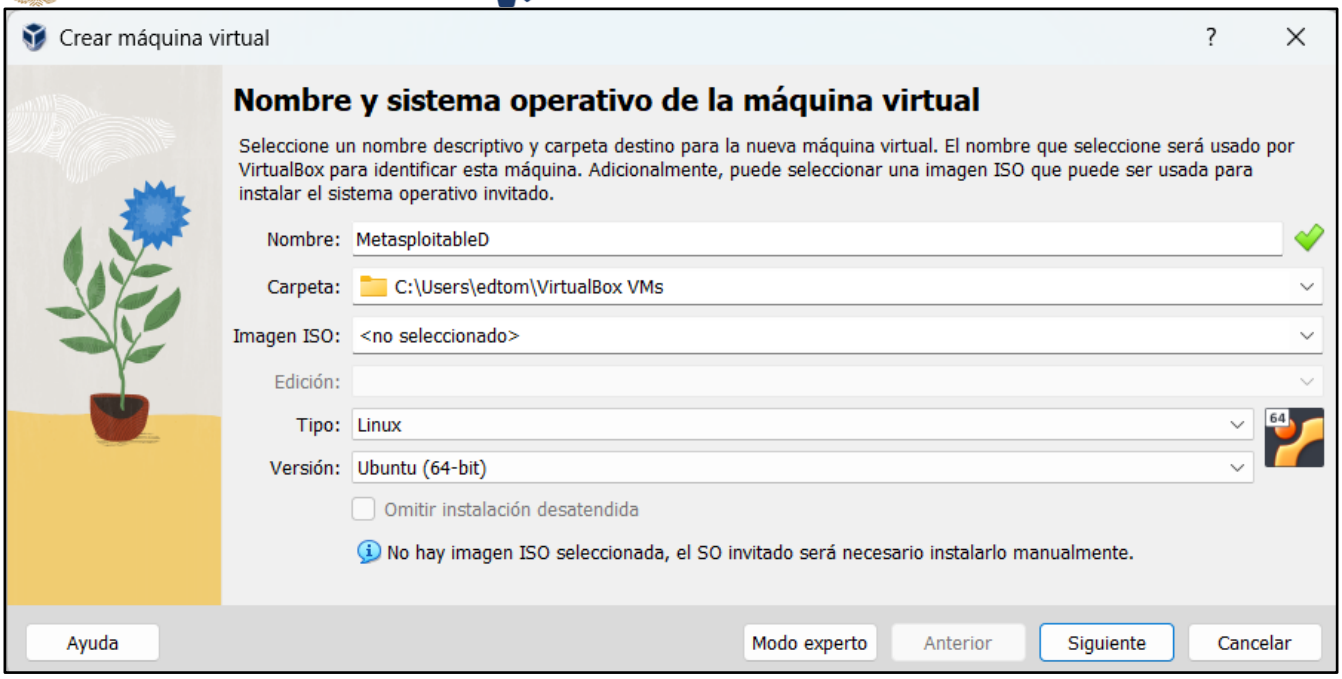


*Ilustración 67. Configuración MV metasploit2 pt 2*

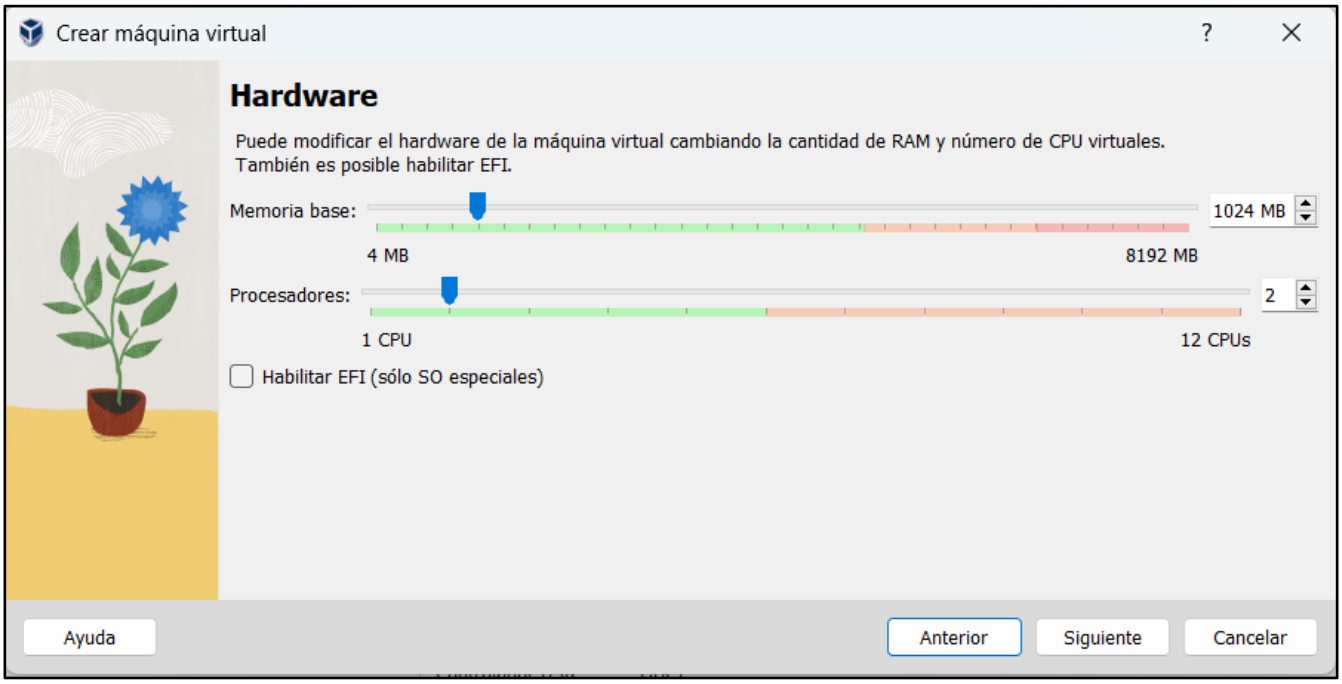


*Ilustración 68. Configuración MV metasploit2 pt 3*

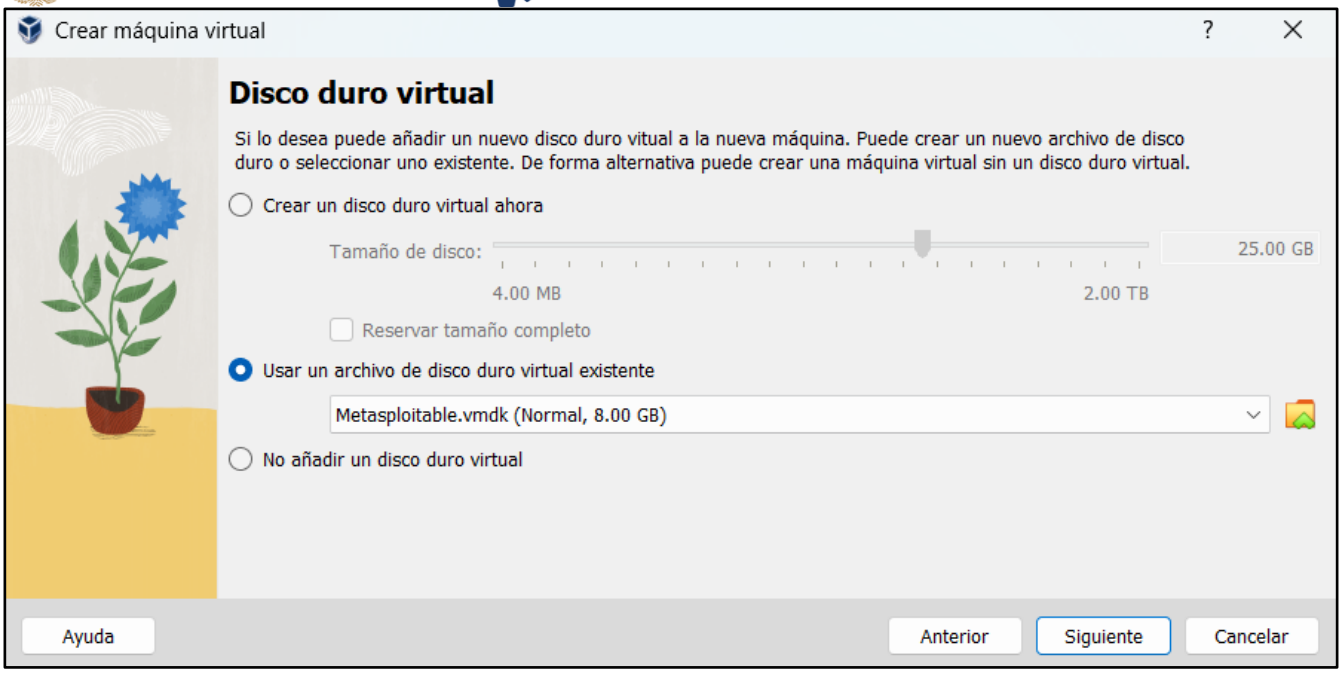


*Ilustración 69. Configuración MV metasploit2 pt 3*

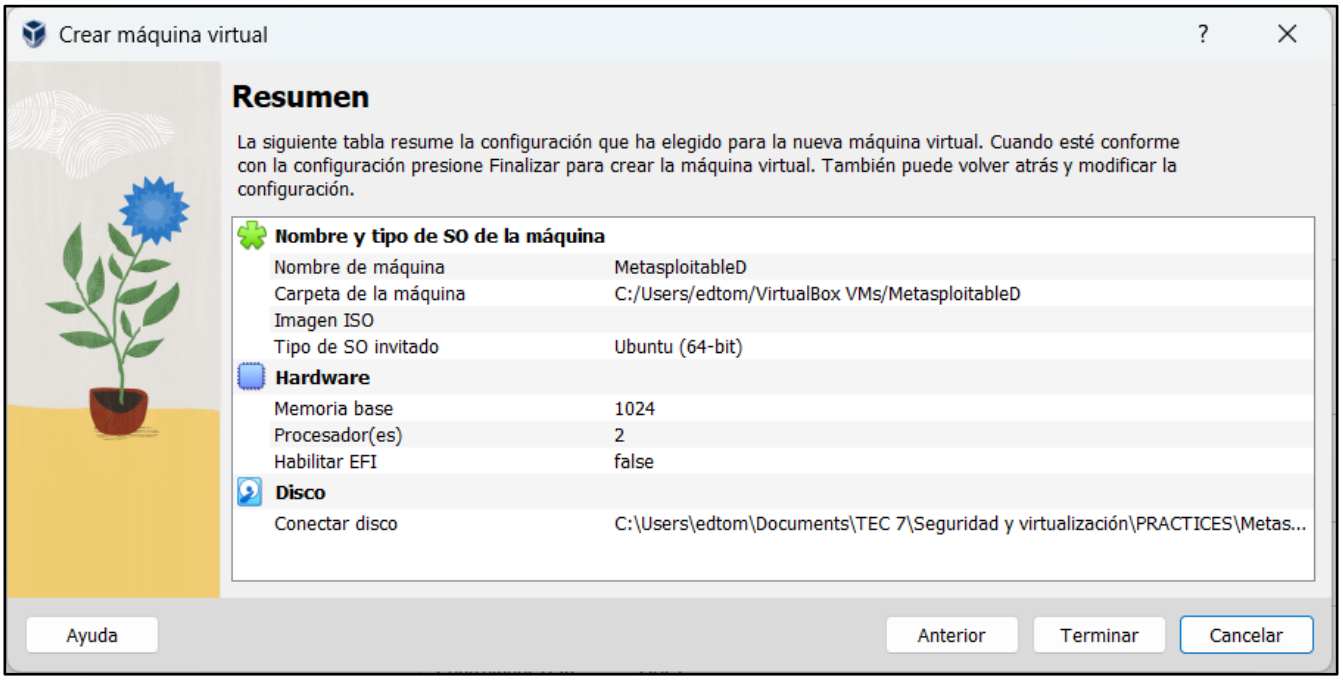


*Ilustración 70. Configuración MV metasploit2 pt 5*

**b)** Iniciamos la máquina virtual metasploit2

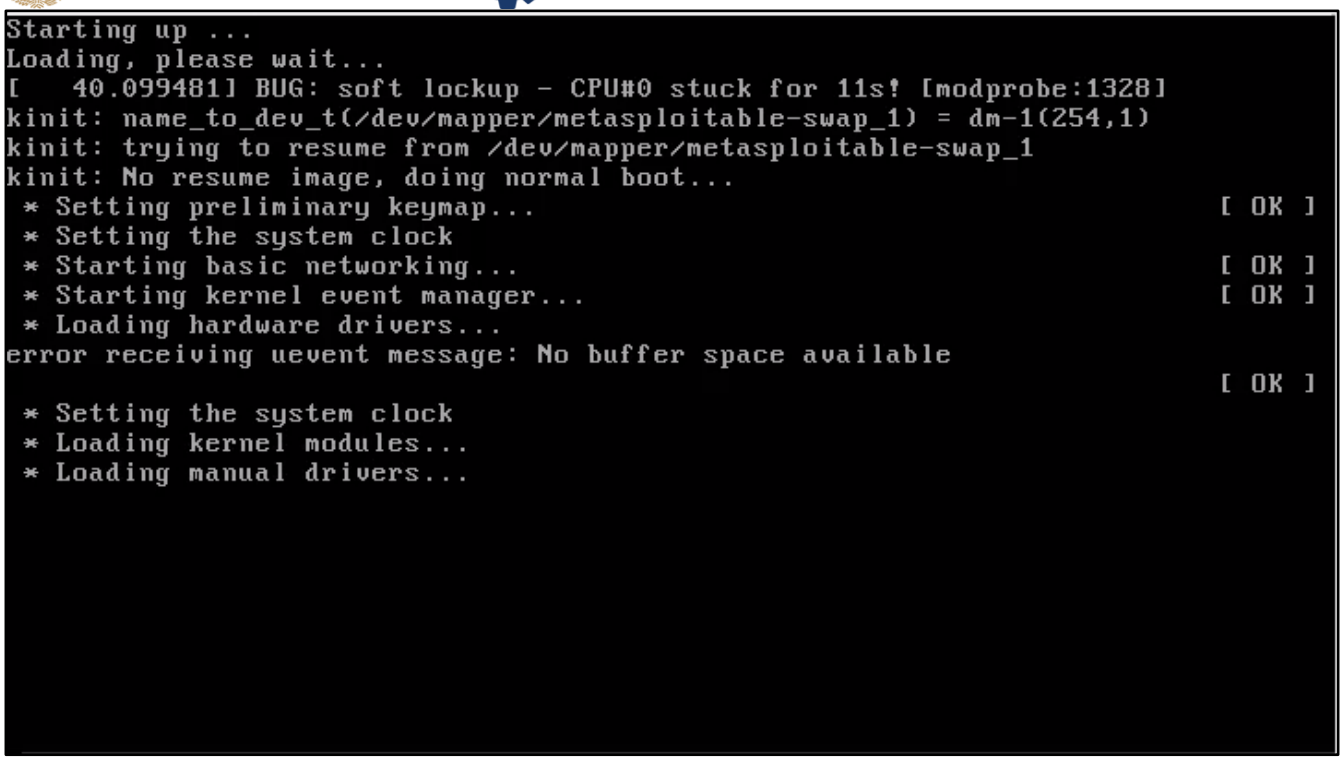


*Ilustración 71. MV metasploit2*

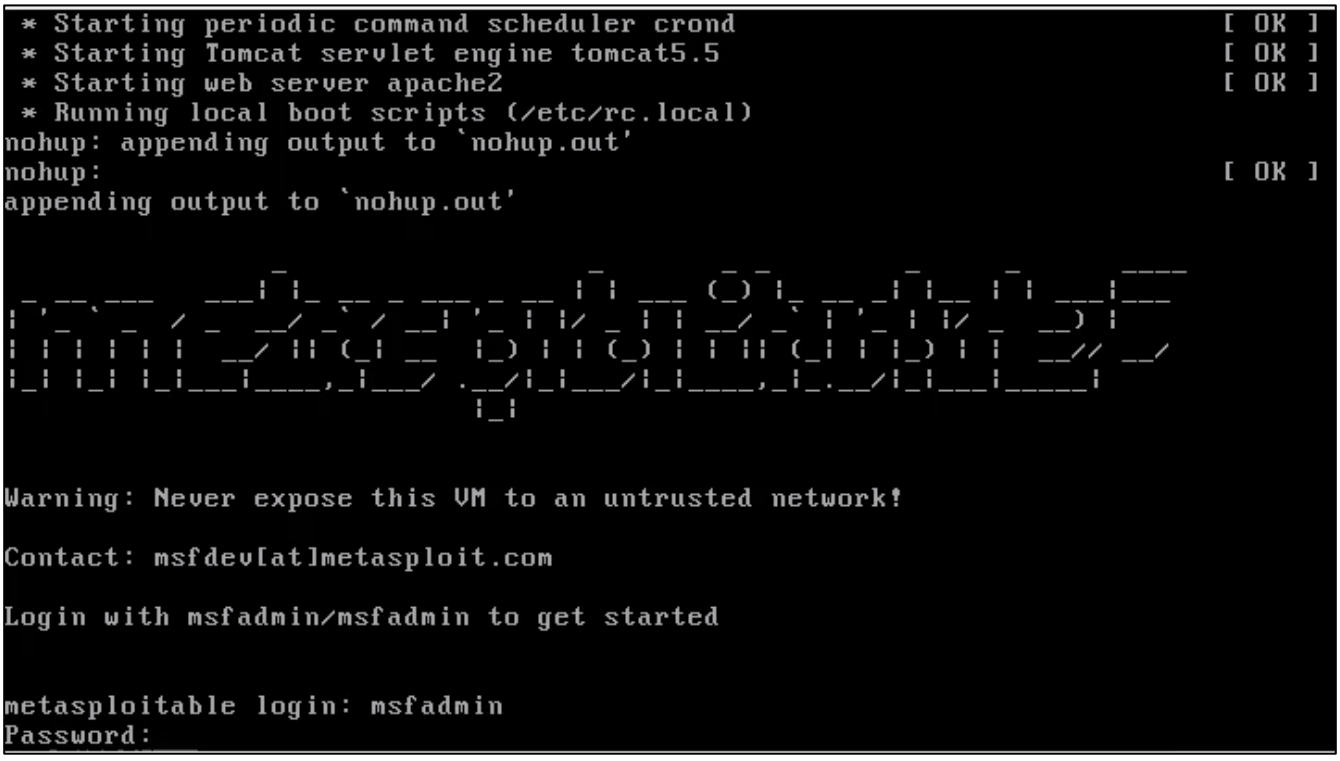


*Ilustración 72. Inicio de sesión*

```
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
[sudo] 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)-[/home/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%O2=M5B4ST11NW6%O3
OS:=M5B4NNT11NW6%O4=M5B4ST11NW6%O5=M5B4ST11NW6%O6=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=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40
OS:%W=16A0%S=O%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%O=%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*

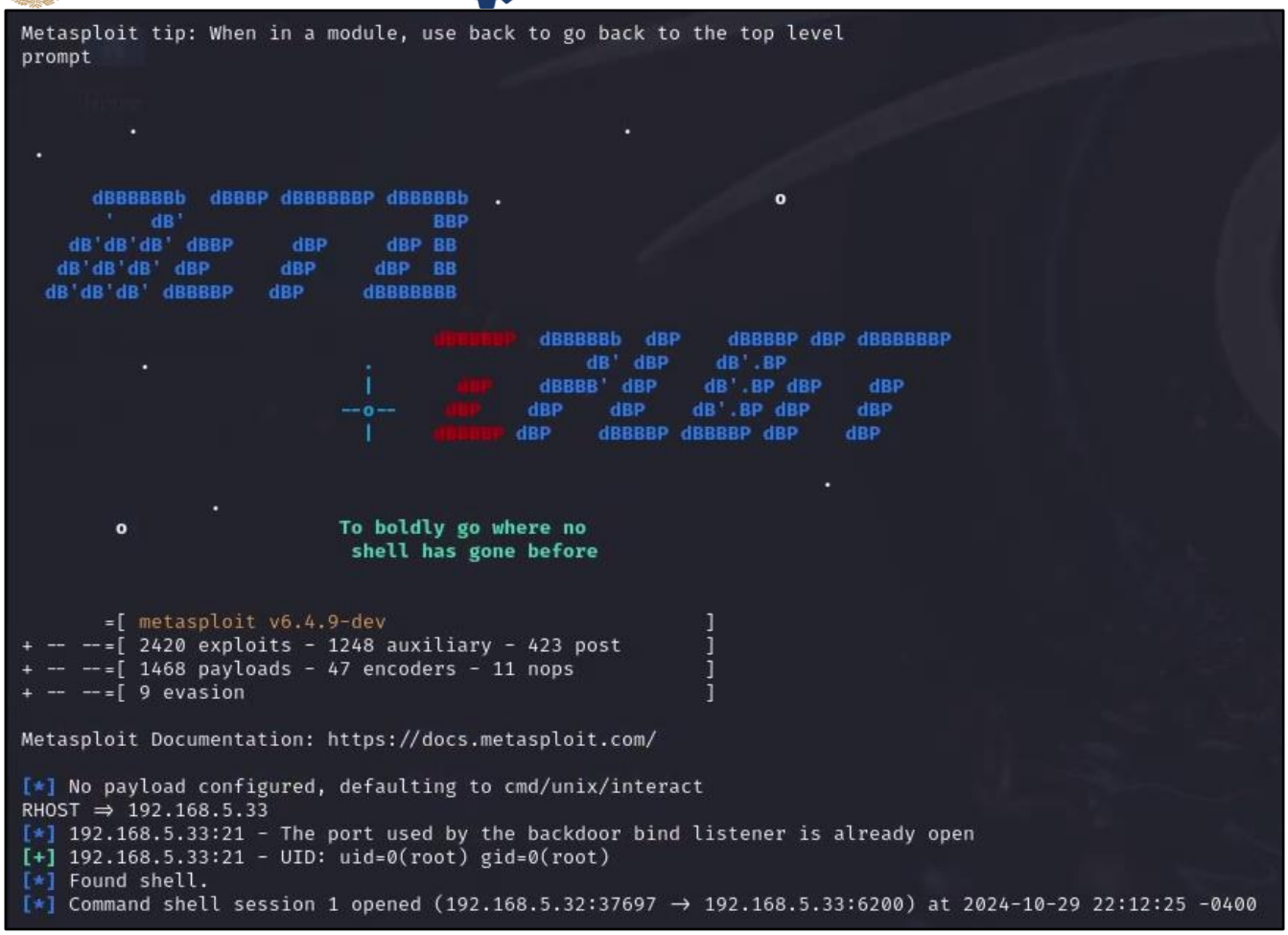


*Ilustración 80. Prueba Final*

**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.