



# TECNOLÓGICO NACIONAL DE MÉXICO

## INSTITUTO TECNOLÓGICO DE TLAXIACO

---

### SEGURIDAD Y VIRTUALIZACIÓN

---

**Nombre de los Integrantes de equipo:**

**No. Control**

Edwin López Santiago

21620123

Yanet González García

21620273

**Tema:**

Práctica 6.- Creación de un laboratorio de seguridad P1

**Docente:**

Ing. Osorio Salinas Edward

**Carrera:**

Ingeniería en Sistemas Computacionales

**Grupo: 7US**

**Tlaxiaco, Oaxaca. A 23 de Octubre de 2024.**



## Índice

<b>Introducción.....</b>	<b>3</b>
<b>1. INSTALAR VIRTUALBOX.....</b>	<b>4</b>
<b>2. INSTALAR OPNSENSE O PFSENSE EN UNA MÁQUINA VIRTUAL Y CONFIGURAR UN FIREWALL. ....</b>	<b>9</b>
2.1 INSTALACIÓN DE OPNSENSE EN UNA MÁQUINA VIRTUAL.....	9
2.2 CONFIGURACIÓN DE INTERFACES.....	12
2.3 CONFIGURACIÓN DE REGLAS DE FIREWALL.....	17
2.4 CONFIGURAR EL NAT.....	19
2.5 CONFIGURACIÓN DE DHCP.....	21
2.6 CONFIGURACIÓN DE DNS.....	22
2.7 ASIGNACIÓN DE DIRECCIÓN IP ESTÁTICA AL FIREWALL.....	22
<b>3. INSTALAR KALI LINUX EN UNA MÁQUINA VIRTUAL Y CONFIGURAR UN SISTEMA DE DETECCIÓN DE INTRUSOS.....</b>	<b>23</b>
3.1 INSTALAR UN SISTEMA DE DETECCIÓN DE INTRUSOS COMO SNORT O SURICATA.....	34
3.2 CONFIGURAR LAS REGLAS DE DETECCIÓN DE INTRUSOS.....	37
3.3 CONFIGURAR LAS ALERTAS DE DETECCIÓN DE INTRUSOS.....	38
3.4 ASIGNAR UNA DIRECCIÓN IP ESTÁTICA A KALI LINUX.....	39
<b>4. CREAR UNA MÁQUINA VIRTUAL VULNERABLE POR DISEÑO COMO METASPLOITABLE2. ....</b>	<b>40</b>
4.1 ASIGNAR UNA DIRECCIÓN IP ESTÁTICA A METASPLOITABLE2. ....	43
<b>5. PING SATISFACTORIO ENTRE LAS MÁQUINAS VIRTUALES. ....</b>	<b>45</b>
5.1 CONFIGURAR LAS INTERFACES DE RED DE LAS MÁQUINAS VIRTUALES.....	45
5.2 CONFIGURAR LAS REGLAS DE FIREWALL PARA PERMITIR EL TRÁFICO DE PING.....	46
5.3 REALIZAR UN PING ENTRE LAS MÁQUINAS VIRTUALES.....	47
<b>Conclusión.....</b>	<b>48</b>
<b>Bibliografías.....</b>	<b>49</b>



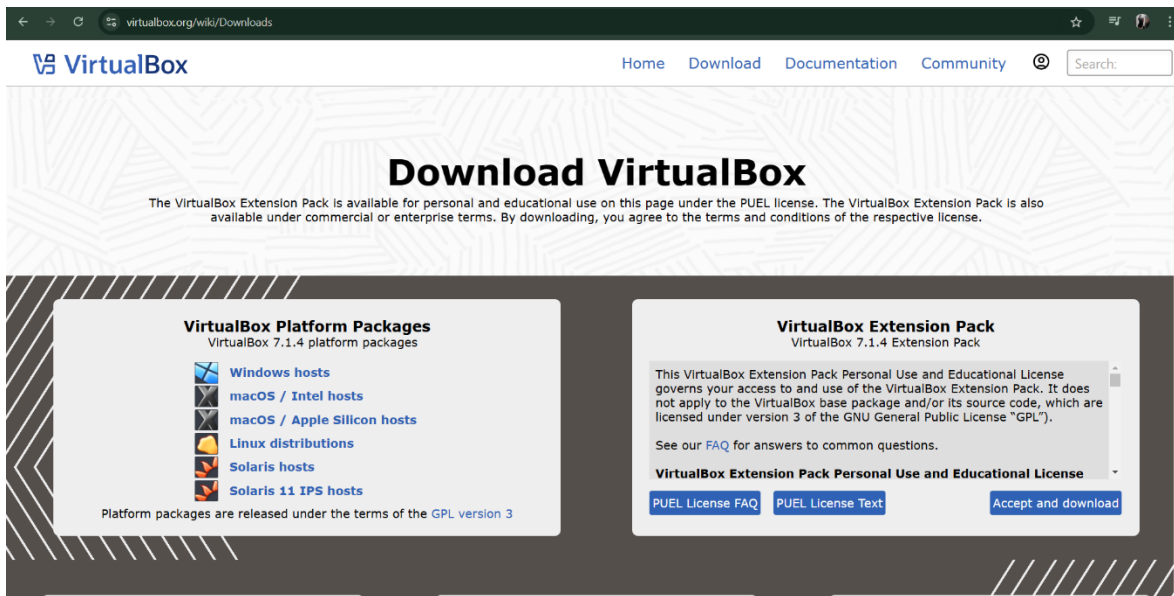
## Introducción

En esta práctica, el objetivo es crear un laboratorio de seguridad usando máquinas virtuales en VirtualBox. Lo que se busca es configurar tres máquinas: una que actúe como firewall con OpnSense o pfSense, otra con Kali Linux que funcione como un sistema para detectar intrusos, y una tercera que sea vulnerable, usando MetaSploitable2. Al final, todas las máquinas deben estar conectadas entre sí y poder comunicarse, lo que se puede verificar con un ping entre ellas. Durante el proceso se presentará paso a paso cómo se configuraron las máquinas y se incluirán capturas de pantalla de cada paso importante.

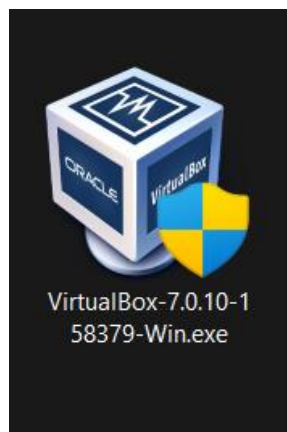
Realizar esto, es importante porque nos permite practicar y entender mejor cómo funcionan los sistemas de seguridad y las redes en un entorno controlado. Nos da la oportunidad de configurar un firewall y un sistema de detección de intrusos, y luego probar su efectividad. Esta práctica es esencial para aprender a proteger redes reales, detectar posibles amenazas y mejorar nuestras habilidades en ciberseguridad sin poner en riesgo un sistema real. Además, ayuda a comprender mejor cómo se comunican las máquinas entre sí y cómo se pueden bloquear o permitir ciertos tipos de tráfico en una red.

## 1. INSTALAR VIRTUALBOX.

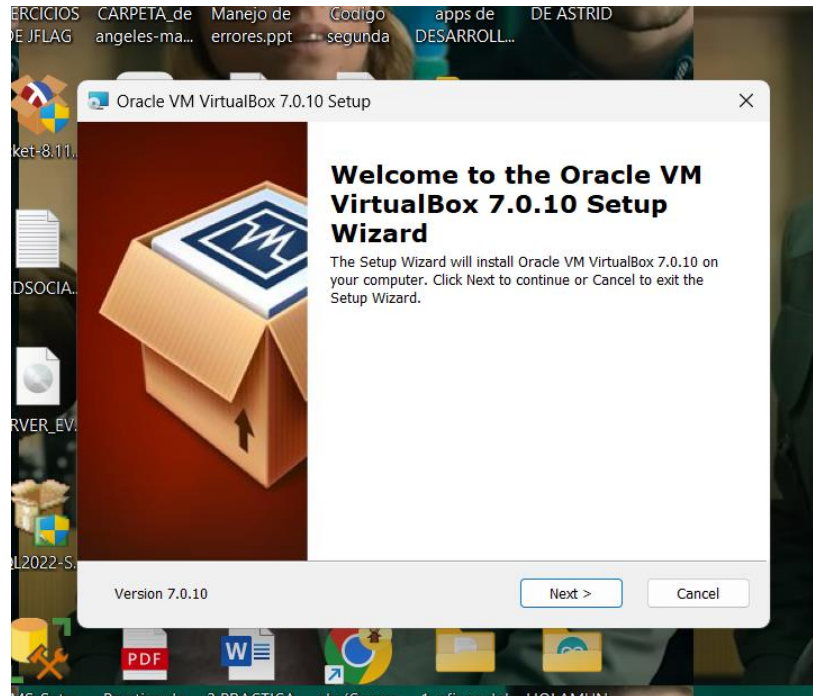
**Paso 1.** Nos dirigimos al sitio oficial de VirtualBox en <https://www.virtualbox.org>. Una vez ahí, busca el apartado llamado "Downloads" y hacemos clic en ello para comenzar la descarga. En este caso elegir en la cual vamos a trabajar, para esto damos clic en "Windows host".



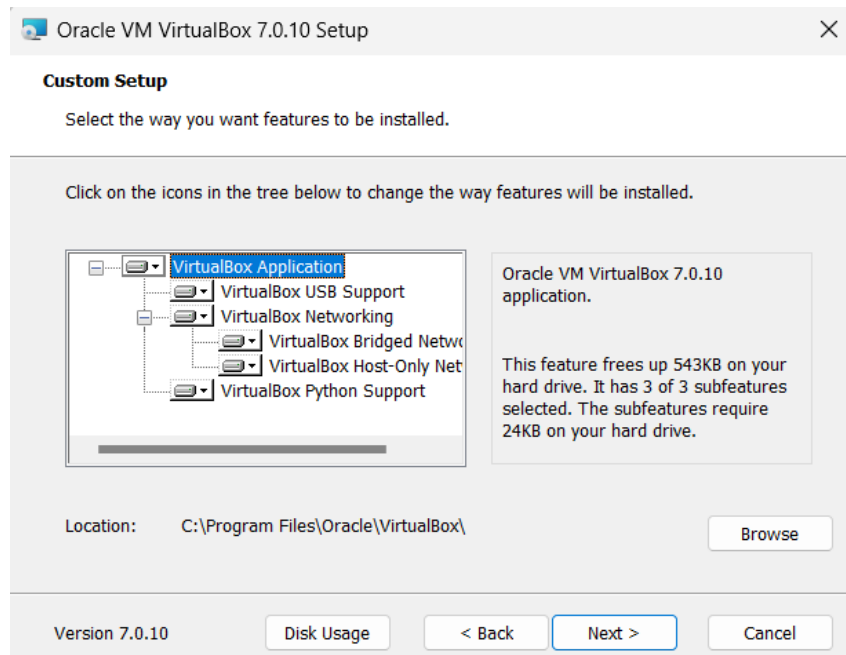
**Paso 2.** Una vez que se halla terminado la descarga nos debe aparecer de la siguiente manera. Para después poder ejecutarlo y empezar con la instalación.



**Paso 3.** Al dar clic derecho y ejecutarlo como administrador, nos aparecerá la ventana de Bienvenida. Clic en "Next".



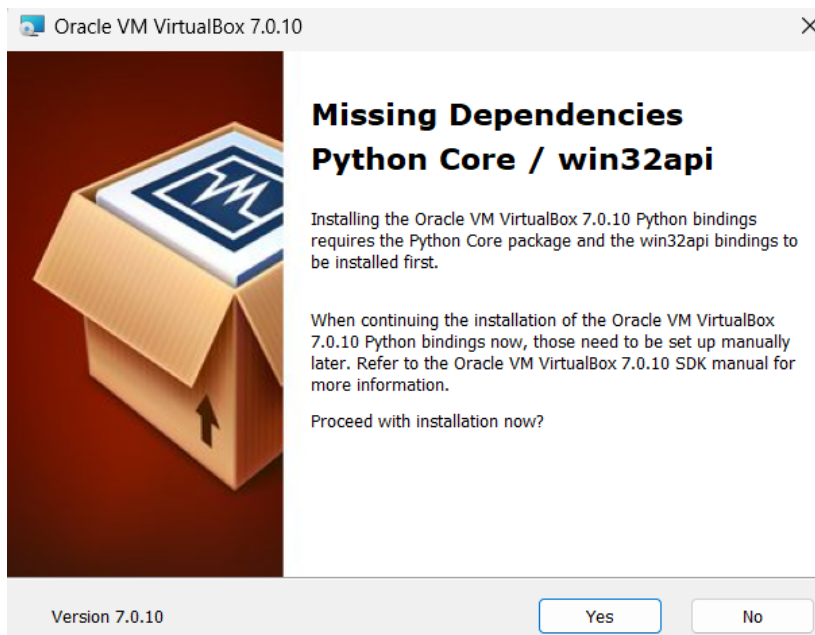
**Paso 4.** En la pantalla de selección de características, se muestran los componentes disponibles para instalar. Para nuestro propósito, mantendremos la configuración por defecto y simplemente seleccionamos "Next" para avanzar.



**Paso 5.** Luego se abrirá una ventana con una advertencia relacionada con la interfaz de red. Para seguir con la instalación, seleccionamos “YES”.

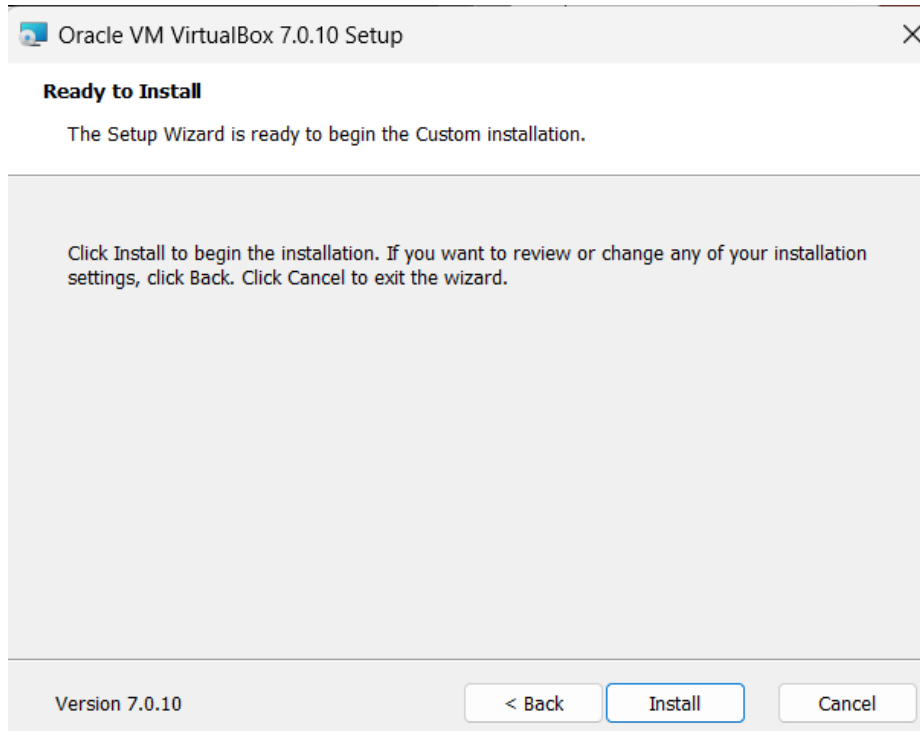


**Paso 6.** Posteriormente aparecerá la ventana de dependencias, en este caso de igual forma se le da “Yes” para que sigamos con la instalación.

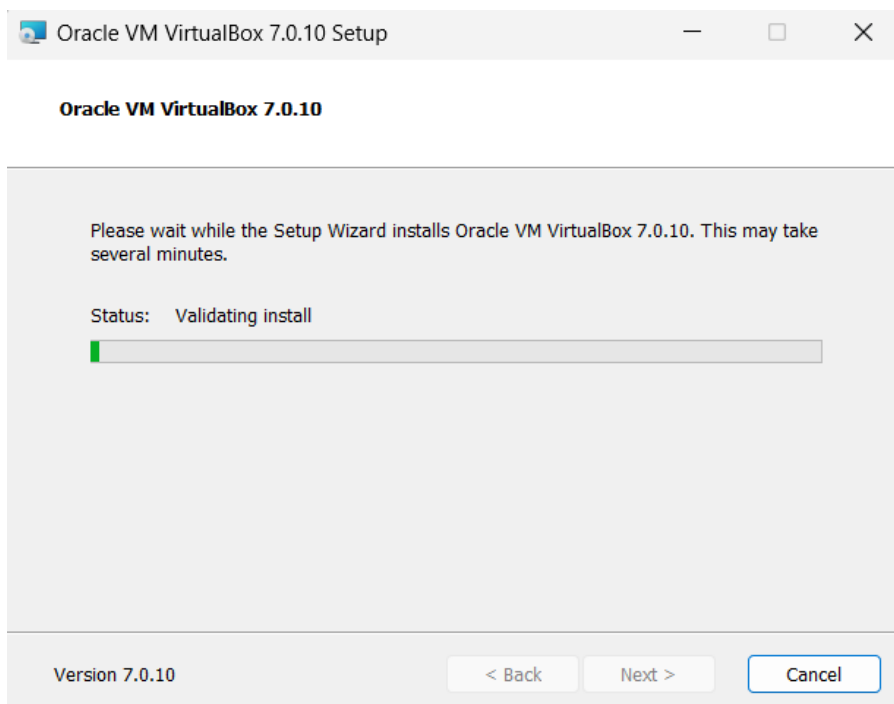




**Paso 7.** En esta ventana se nos pedirá revisar los pasos anteriores por si queremos cambiar alguna opción. En este caso, simplemente seleccionamos "Install" para iniciar la instalación.



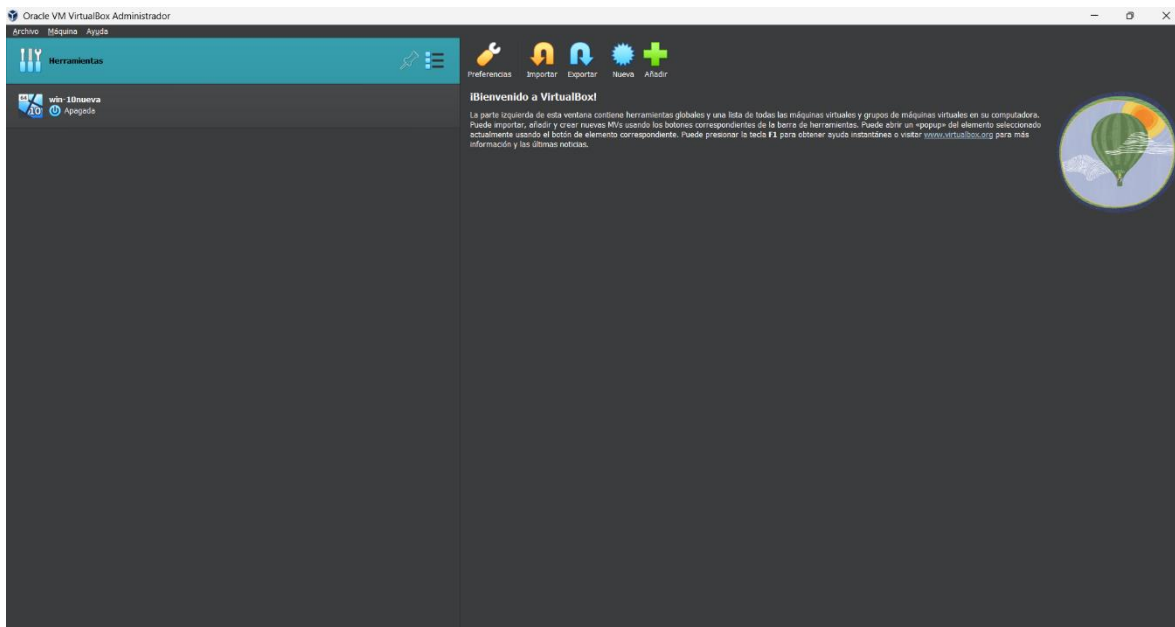
**Paso 8.** Esperar a que se complete la instalación y enseguida dar "Next", con este paso finalizaremos el proceso.



**Paso 9.** Una vez que se haya completado la instalación, nos aparecerá esta ventana, la cual quiere decir que el proceso fue un éxito, para esto, clic en “Finish”.



**Paso 10.** Al finalizar la instalación, procedemos a abrir “VirtualBox” y se verá de la siguiente manera.

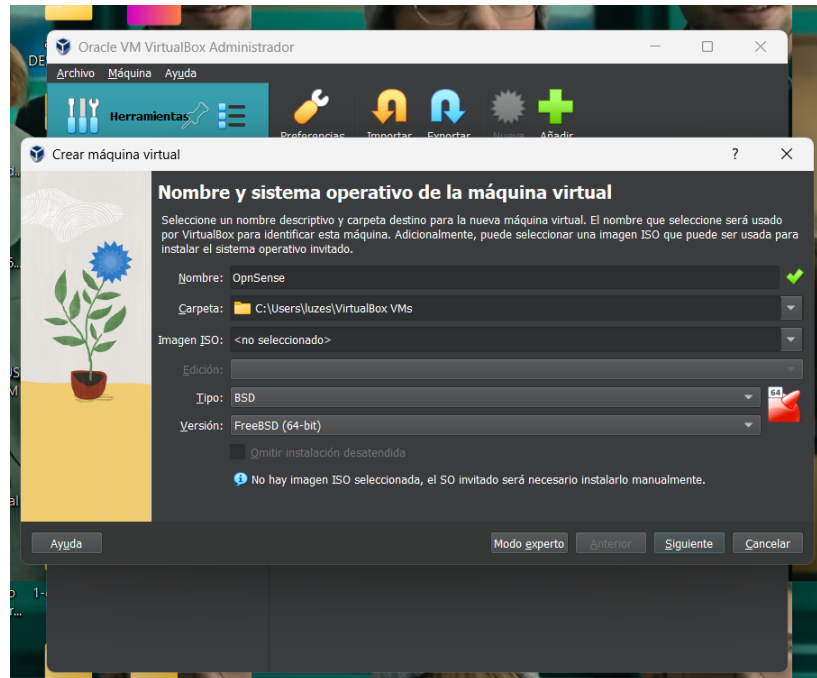




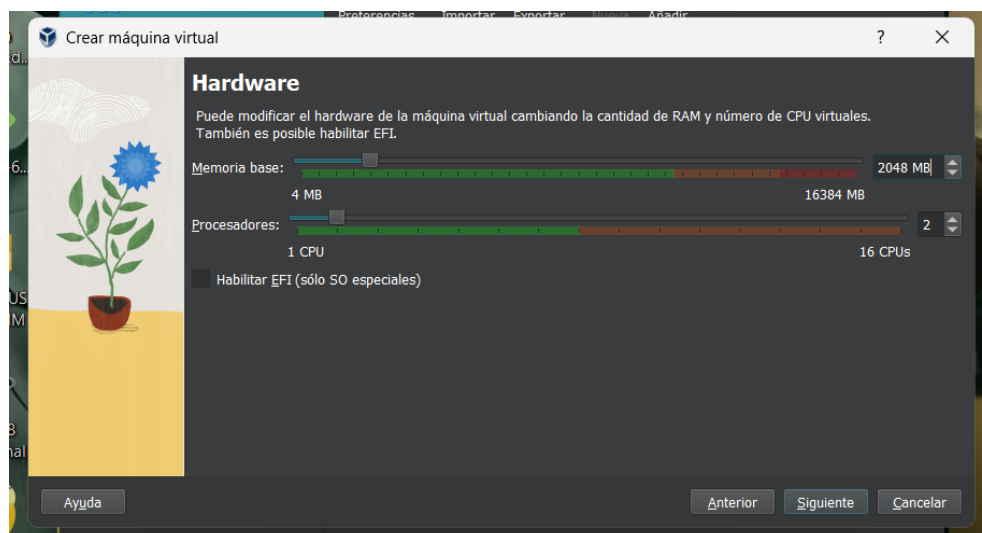
## 2. INSTALAR OPNSENSE O PFSENSE EN UNA MÁQUINA VIRTUAL Y CONFIGURAR UN FIREWALL.

### 2.1 INSTALACIÓN DE OPNSENSE EN UNA MÁQUINA VIRTUAL.

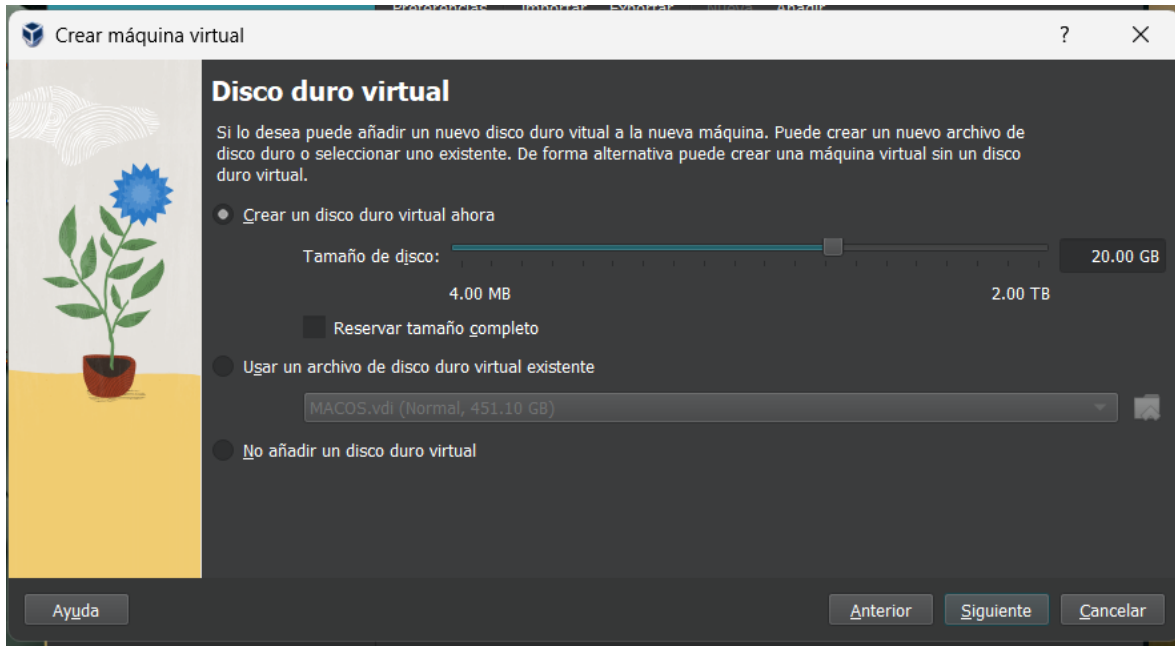
**Paso 1.** Damos clic en “Nueva” para crear una máquina virtual de nombre “OpnSense” y seleccionamos en tipo BSD y la versión FreeBSD(64-bit), esto para que sea exitosa nuestra configuración.



**Paso 2.** Se abrirá una nueva ventana en la que seleccionaremos la cantidad de memoria que utilizaremos en nuestra máquina virtual. Es importante recordar que no debemos asignar toda la barra verde, ya que nuestra computadora física también tiene un sistema operativo en ejecución. Asignaremos 2048 MB de memoria y configuraremos el procesador con 2 núcleos. Luego, haremos clic en "Siguiente" para continuar.



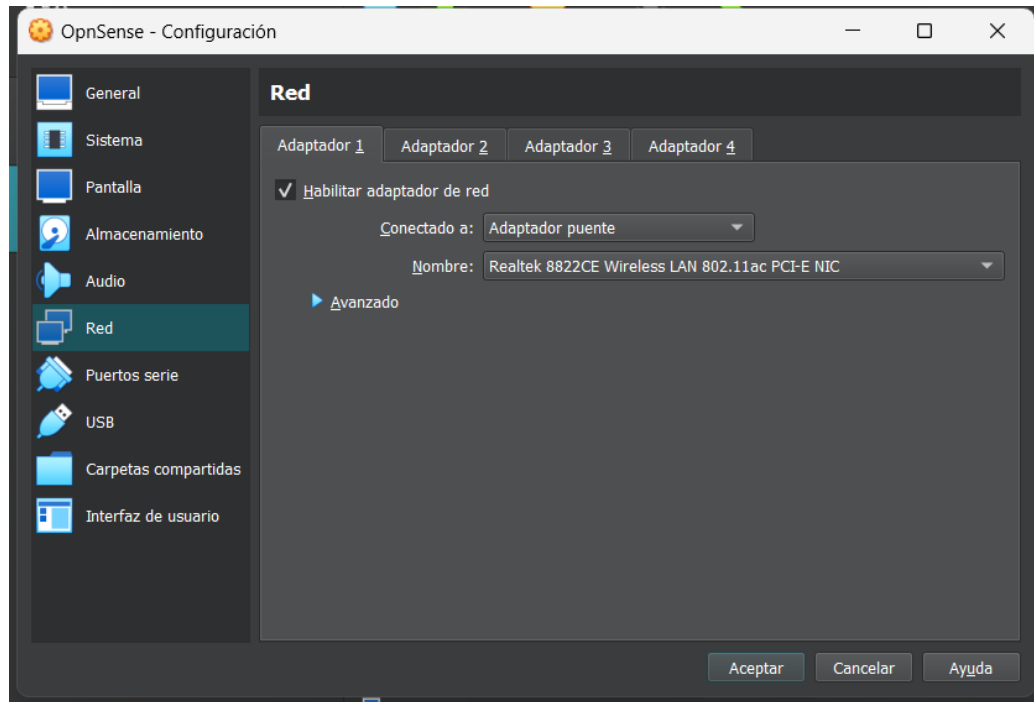
**Paso 3.** Luego, se mostrará una ventana en la que nos pedirá especificar el espacio de almacenamiento para el sistema operativo que vamos a instalar. En este caso, asignamos 20 GB de espacio y, después, seleccionamos "Siguiente" para continuar.



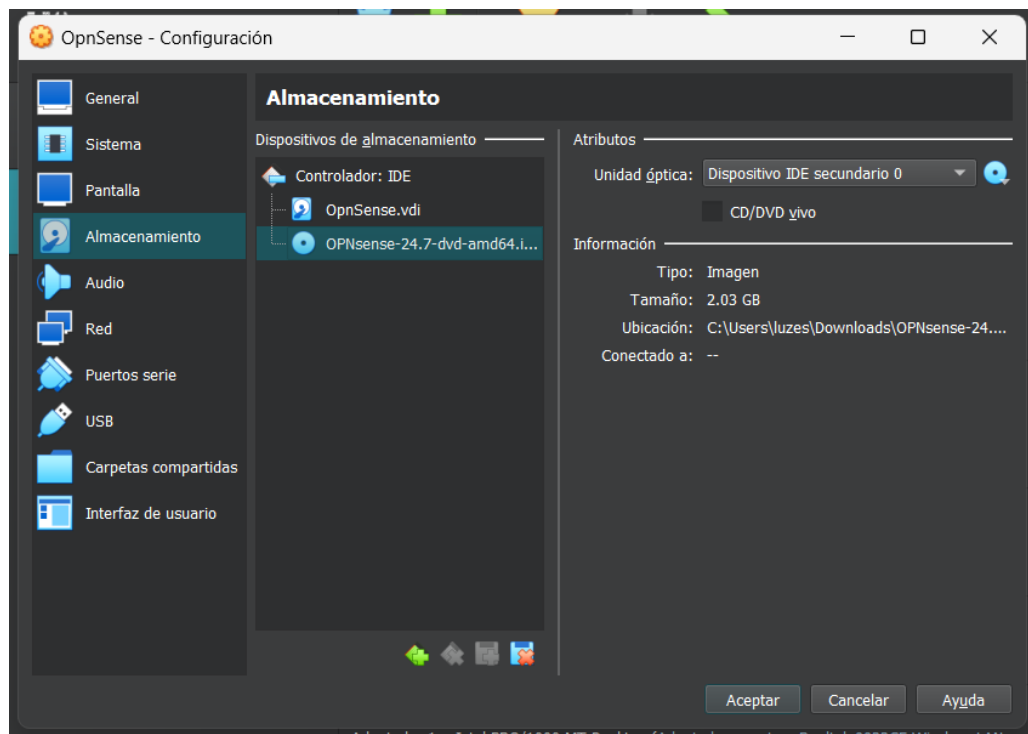
**Paso 4.** Enseguida nos mostrará un resumen de lo que hemos seleccionado como queremos que sea nuestra máquina virtual. Una vez revisado bien, clic en "Terminar".



**Paso 5.** Al completar la creación de nuestra máquina virtual, procederemos a configurar el adaptador de red y el archivo ISO. Para hacerlo, hacemos clic en el icono de engranaje ubicado en la parte superior. Luego, vamos al apartado de "Red" y, en "Adaptador 1", seleccionamos la opción "Adaptador puente".

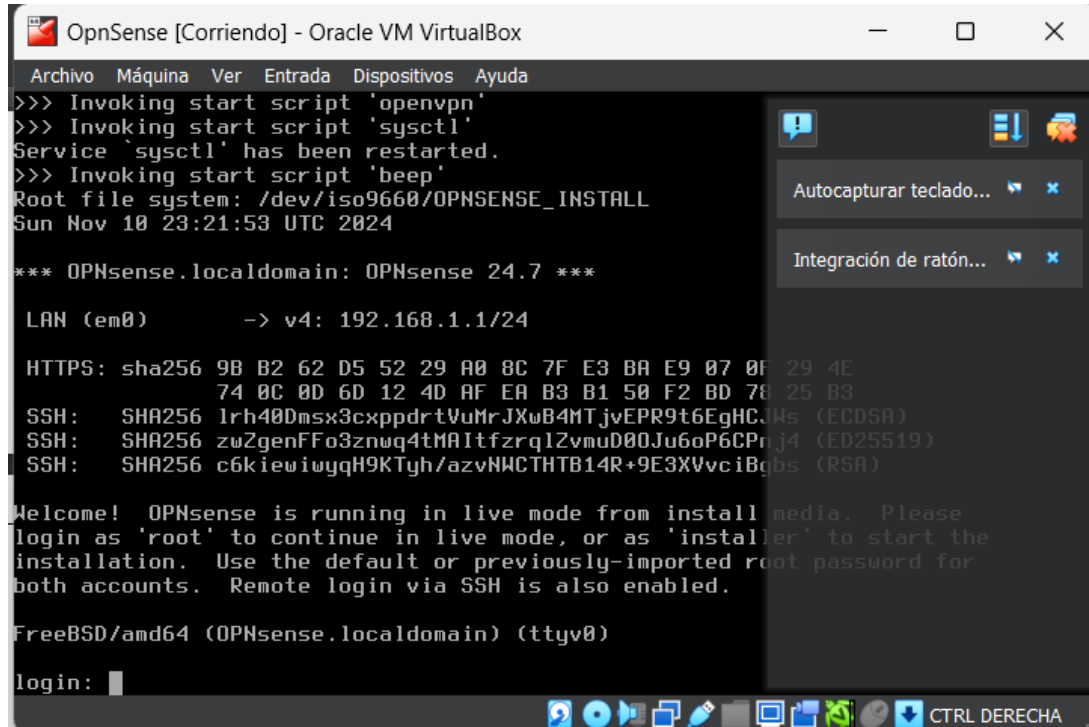


**Paso 6.** Al terminar de ajustar la configuración del adaptador de red, pasamos al apartado de "Almacenamiento". En esta sección, seleccionamos el archivo ISO que utilizaremos para la instalación del sistema operativo. Después de cargar el ISO, confirmamos los cambios haciendo clic en el botón "Aceptar".

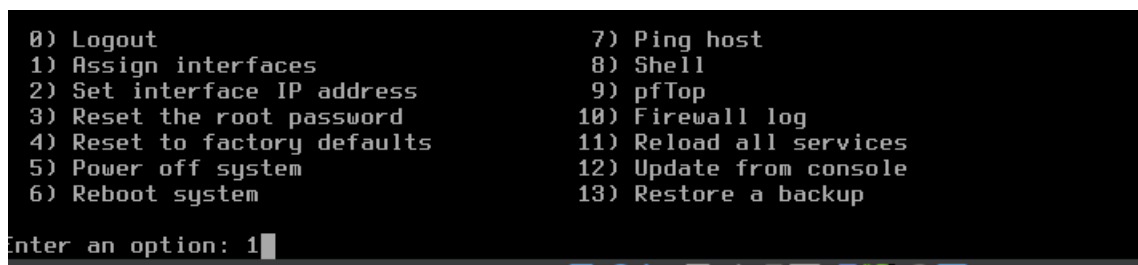


## 2.2 CONFIGURACIÓN DE INTERFACES

**Paso 7.** Al iniciar la máquina virtual nos aparecerá de la siguiente manera en la cual nos pedirá que ingresemos un usuario (root) y una contraseña (opnsense).



**Paso 8.** En este punto, veremos una lista de opciones para personalizar varios aspectos. Para nuestro caso, elegiremos la opción correspondiente a la configuración de la interfaz de red.



**Paso 9.** A continuación, se nos preguntará si deseamos configurar los LAGGs en este momento. En nuestro caso, seleccionaremos la opción de "no" y continuaremos presionando enter.

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



**Paso 10.** Luego, aparecerá una opción que solicitará ingresar la interfaz para la WAN. Asignaremos "em0" en este campo y presionaremos enter para continuar.

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

**Paso 11.** A continuación, se mostrarán las configuraciones que se aplicaron a las interfaces.

```
WAN -> em0  
LAN -> em1
```

**Paso 12.** Para proceder con los demás pasos, ingresamos y.

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

**Paso 13.** Ingresamos la opción 2 para realizar la configuración y enseguida damos enter.

```
Enter an option: 2
```

**Paso 14.** En este paso, se nos solicitará elegir una de las opciones disponibles para configurar.

```
1 - LAN (em1 - static, track6)  
2 - WAN (em0 - dhcp, dhcp6)  
Enter the number of the interface to configure: 1
```

**Paso 15.** Una vez que se haya escrito el número 1 y presionamos enter. Luego, se nos preguntará si deseamos configurar la dirección de la interfaz LAN para DHCP; elegimos "no" y continuamos con enter.

```
Configure IPv4 address LAN interface via DHCP? [y/N] n  
Enter the new LAN IPv4 address. Press <ENTER> for none:  
>
```

**Paso 16.** Después, se nos solicitará ingresar la dirección IP para la interfaz LAN. Escribimos la IP que queremos y presionamos enter para continuar.

```
Enter the new LAN IPv4 address. Press <ENTER> for none:  
> 172.16.4.2
```

**Paso 17.** A continuación, ingresamos la máscara de subred en formato numérico, por ejemplo, 24 para una máscara 255.255.255.0, y presionamos enter para seguir.

```
Subnet masks are entered as bit counts (like CIDR notation).  
e.g. 255.255.255.0 = 24  
255.255.0.0 = 16  
255.0.0.0 = 8  
Enter the new LAN IPv4 subnet bit count (1 to 32):  
> 24
```



**Paso 18.** Se nos preguntará si deseamos configurar IPv6 para la interfaz LAN; seleccionamos "no" y continuamos presionando enter.

```
Configure IPv6 address LAN interface via WAN tracking? [Y/n] n
```

**Paso 19.** También en esta configuración escribiremos que no, enseguida dar enter.

```
Configure IPv6 address LAN interface via DHCP6? [y/N] n
Enter the new LAN IPv6 address. Press <ENTER> for none:
>
```

**Paso 20.** A continuación, se nos preguntará si queremos activar el servidor DHCP en la interfaz LAN. Escribimos "sí" y presionamos enter para continuar.

```
Do you want to enable the DHCP server on LAN? [y/N] y
```

**Paso 21.** Luego, se nos solicitará ingresar el rango de direcciones IP para iniciar. Introducimos "172.16.4.5" y presionamos enter para continuar.

```
Enter the start address of the IPv4 client address range: 172.16.4.5
```

**Paso 22.** A continuación, se nos pedirá definir hasta qué dirección IP queremos que llegue el rango. Ingresamos "172.16.4.200" como la última dirección y presionamos enter. El sistema comenzará a reiniciarse.

```
Enter the end address of the IPv4 client address range: 172.16.4.200
```

**Paso 23.** En este apartado ingresamos un no primeramente y enseguida con un sí, posteriormente con un enter para que nos muestre una dirección.

```
Do you want to change the web GUI protocol from HTTPS to HTTP? [y/N] n
Do you want to generate a new self-signed web GUI certificate? [y/N] y
Restore web GUI access defaults? [y/N]
```

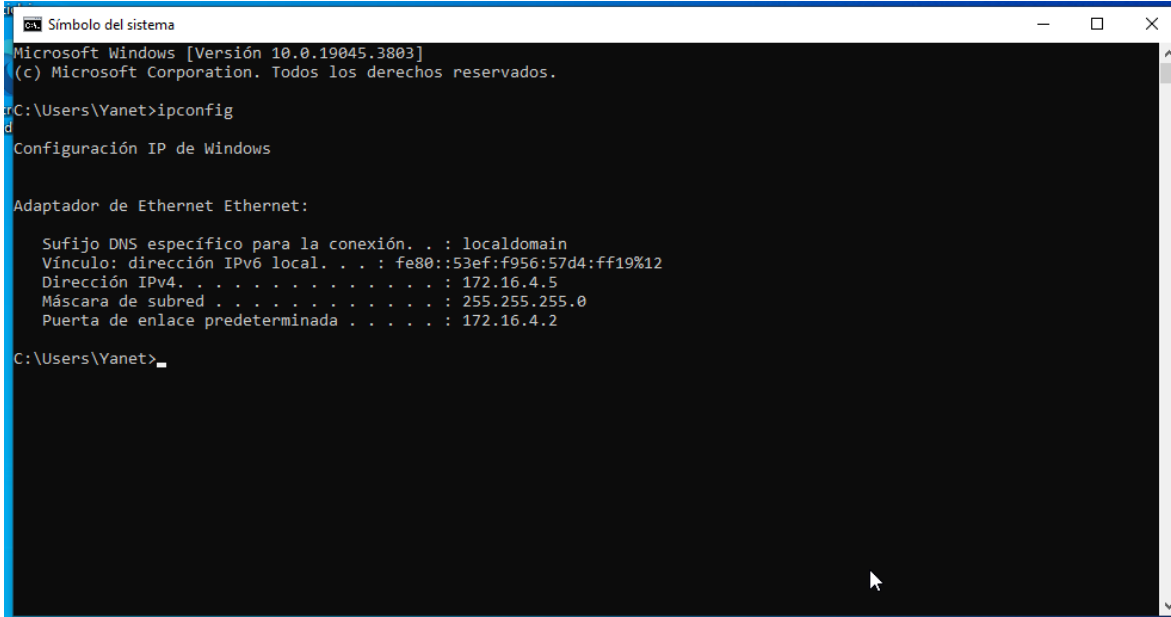
**Paso 24.** Una vez finalizado el reinicio, se mostrará una dirección en la que podremos acceder a la interfaz de OPNsense.

```
https://172.16.4.2
```

**Paso 25.** Debemos de tener guardado estos datos que se muestran a continuación ya que al terminar las configuraciones se realizarán pines con las direcciones generadas.

```
https://172.16.4.2
*** OPNsense.localdomain: OPNsense 24.7 ***
LAN (em1)      -> v4: 172.16.4.2/24
WAN (em0)      -> v4/DHCP4: 192.168.20.105/24
```

**Paso 26.** Accedemos a nuestra máquina virtual con el sistema operativo 10 “Windows 10”, lo iniciamos y abrimos la terminal. Allí, ejecutamos el comando ipconfig para comprobar que nuestra máquina esté configurada con la puerta de enlace de OPNsense. Si la dirección IP es correcta, podremos acceder a la interfaz de OPNsense a través del navegador sin inconvenientes.



```
Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.3803]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Yanet>ipconfig

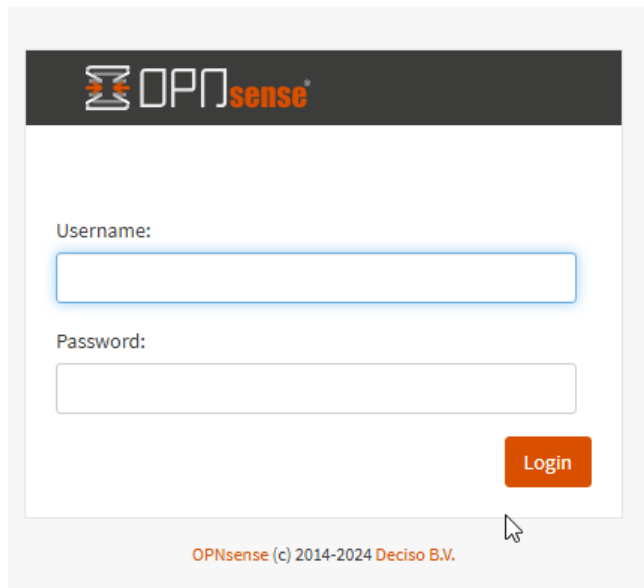
Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufixo DNS específico para la conexión. . . : localdomain
    Vínculo: dirección IPv6 local. . . . : fe80::53ef:f956:57d4:ff19%12
    Dirección IPv4. . . . . : 172.16.4.5
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 172.16.4.2

C:\Users\Yanet>
```

**Paso 27.** Abrimos el navegador que tengamos instalado, en este caso “Microsoft Edge” y escribimos la dirección IP de nuestro OPNsense en la barra de direcciones. Así como “**172.16.4.2**”



OPNsense

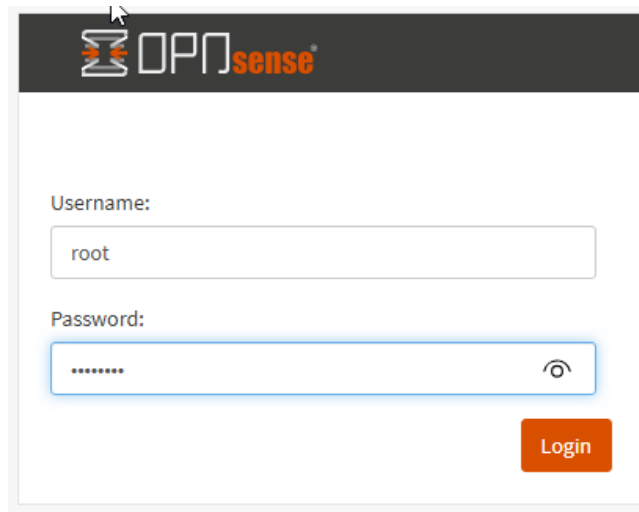
Username:

Password:

Login

OPNsense (c) 2014-2024 Deciso B.V.

**Paso 28.** Escribimos "root" en el campo de usuario y "opnsense" en el de contraseña. Estos son los mismos datos de acceso que usamos para acceder a OPNsense.



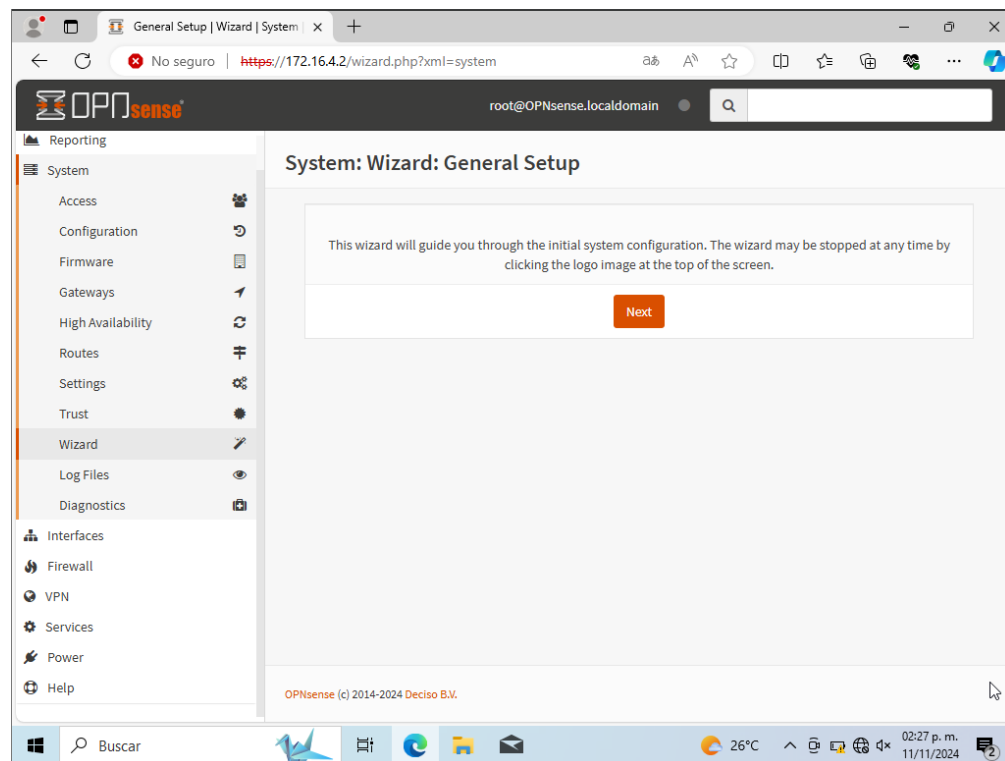
OPNsense

Username:

Password:

Login

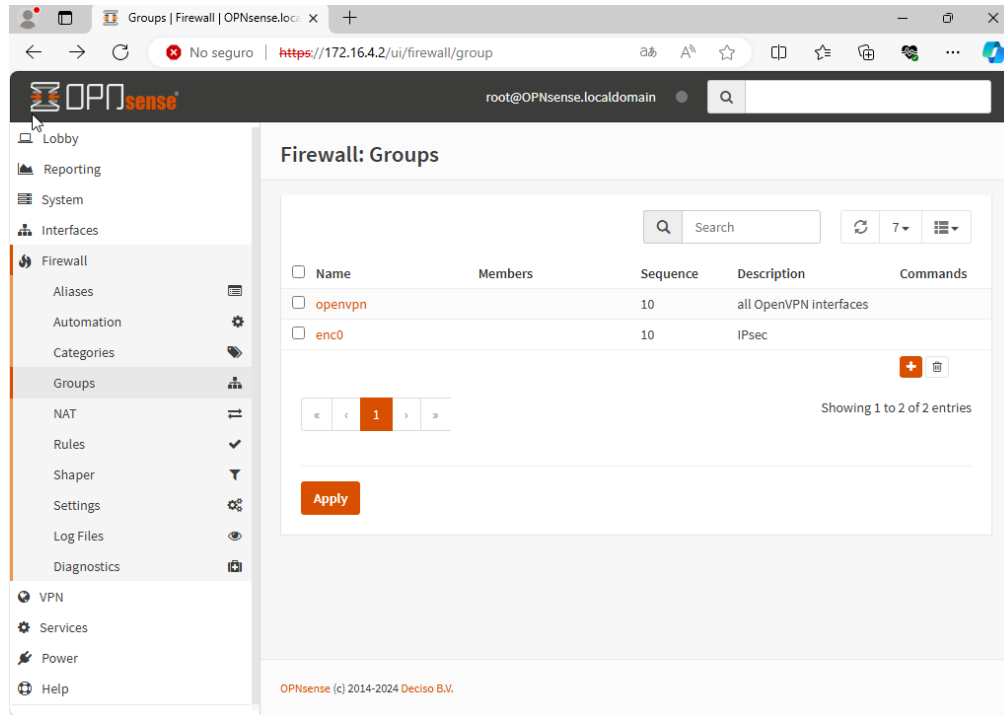
**Paso 29.** Una vez dentro, veremos la interfaz de OPNsense, desde donde podremos realizar diferentes configuraciones.



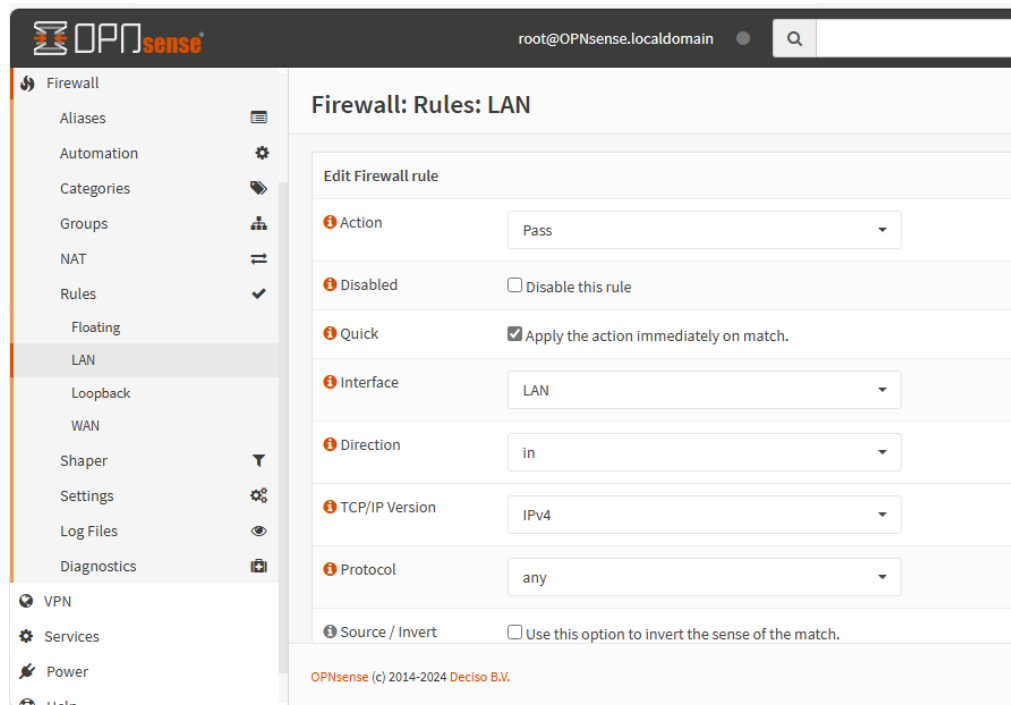


## 2.3 CONFIGURACIÓN DE REGLAS DE FIREWALL

**Paso 29.** Para configurar las reglas del firewall, navegamos a la sección llamada "Firewall". Ahí, se abrirá una nueva ventana, donde haremos clic en el botón naranja con el símbolo de más para añadir una nueva regla al firewall.



**Paso 30.** A continuación, se abrirá una ventana donde podremos establecer una regla para nuestra red LAN. Aquí se muestra cómo quedó la configuración realizada.





**Paso 31.** Una vez que hayamos configurado todas las opciones, haremos clic en el botón "save" para guardar los cambios.

Firewall

- Aliases
- Automation
- Categories
- Groups
- NAT
- Rules
- Floating
- LAN
- Loopback
- WAN
- Shaper
- Settings
- Log Files
- Diagnostics

VPN

Services

Power

Help

range

any

any

Log ☒ Log packets that are handled by this rule

Category

Description permitir todo el tráfico desde LAN

No XMLRPC Sync ☐

Schedule none

Gateway default

Advanced features Show/Hide

Save Cancel

OPNsense (c) 2014-2024 Deciso B.V.

**Paso 32.** Podremos observar que ahora tenemos tres reglas configuradas en la sección LAN de nuestro firewall.

	Protocol	Source	Description ?	
				<span>+</span> <span>←</span> <span>🗑️</span> <span>✅</span> <span>📄</span>
			Automatically generated rules	<span>👇</span> 19
<input type="checkbox"/>	IPv4 *	LAN net	Default allow LAN to any rule	<span>←</span> <span>🔧</span> <span>📄</span> <span>🗑️</span>
<input type="checkbox"/>	IPv6 *	LAN net	Default allow LAN IPv6 to any rule	<span>←</span> <span>🔧</span> <span>📄</span> <span>🗑️</span>
<input type="checkbox"/>	IPv4 *	LAN net	permitir todo el tráfico desde LAN	<span>←</span> <span>🔧</span> <span>📄</span> <span>🗑️</span>

## 2.4 CONFIGURAR EL NAT

**Paso 33.** Para configurar el NAT, en la sección de modo seleccionaremos la opción "Hybrid outbound rule generation - automatically generated rules".

Mode

☐ Automatic outbound NAT rule generation  
(no manual rules can be used)

☒ Hybrid outbound NAT rule generation  
(automatically generated rules are applied after manual rules)

☐ Manual outbound NAT rule generation  
(no automatic rules are being generated)

☐ Disable outbound NAT rule generation  
(outbound NAT is disabled)

Save

**Paso 34.** Vamos a la opción llamada "Outbound" y configuramos cada uno de los apartados que aparecen ahí.

## Firewall: NAT: Outbound

Edit Advanced Outbound NAT entry

Disabled

☐ Disable this rule

Do not NAT

☐

Interface

WAN ▾

TCP/IP Version

IPv4 ▾

Protocol

any ▾

Source invert

☐

Source address

any ▾

Source port

any ▲

OPNsense (c) 2014-2024 Desire B.V.



**Paso 35.** Continuamos ajustando las configuraciones necesarias y, al terminar, hacemos clic en el botón "Save" para guardar los cambios.

Destination address	LAN net
Destination port	any
Translation / target	Interface address
Log	<input type="checkbox"/> Log packets that are handled by this rule
Translation / port:	
Static-port:	<input type="checkbox"/>
Pool Options:	Default
Set local tag	
Match local tag	

**Paso 36.** Podemos ver que hemos añadido correctamente la configuración de nuestro NAT.

Manual rules					
<input type="checkbox"/>	Interface	Static Port	Description	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	WAN	YES		<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Enabled rule				
<input type="checkbox"/>	Disabled rule				



## 2.5 CONFIGURACIÓN DE DHCP

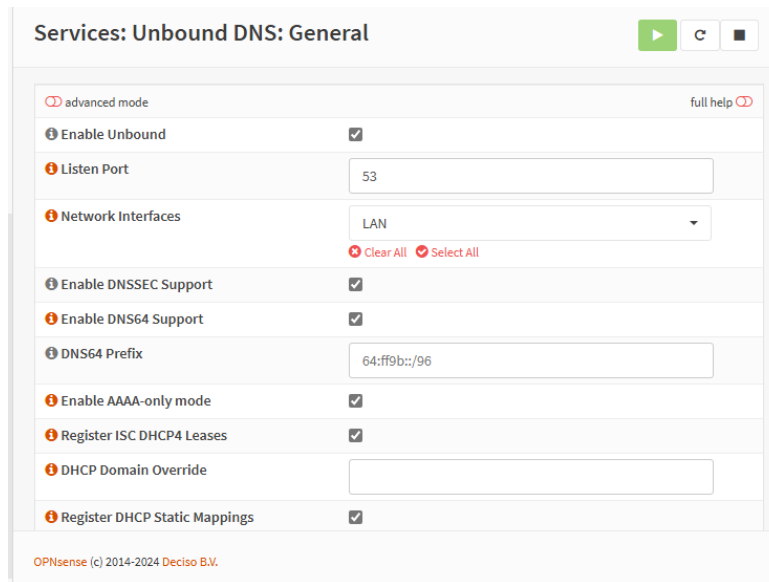
**Paso 37.** A continuación, configuraremos el DHCP para nuestra red LAN. Se mostrará un conjunto de opciones que debemos ajustar, como la dirección IP, la máscara de subred y el rango de direcciones IP permitidas.

La imagen muestra la interfaz de configuración de DHCPv4 en Mikrotik WinBox. En el menú de la izquierda, se encuentran las opciones: VPN, Services, Captive Portal, DHCP Relay, Dnsmasq DNS, Intrusion Detection, ISC DHCPv4 (seleccionado), [LAN], Leases, Log File, ISC DHCPv6, Kea DHCP [new], Monit, Network Time, OpenDNS y Unbound DNS. El panel principal muestra la configuración para 'Services: ISC DHCPv4: [LAN]'. Las opciones de configuración son:

- Enable:** ☒ Enable DHCP server on the LAN interface
- Deny unknown clients:** ☐
- Ignore Client UIDs:** ☐
- Subnet:** 172.16.4.0
- Subnet mask:** 255.255.255.0
- Available range:** 172.16.4.1 - 172.16.4.254
- Range:** from 172.16.4.5 to 172.16.4.200

## 2.6 CONFIGURACIÓN DE DNS.

**Paso 38.** En este paso, procederemos a configurar nuestro DNS. En la ventana que aparece, veremos varias opciones de configuración; seleccionamos las opciones principales para evitar problemas más adelante.



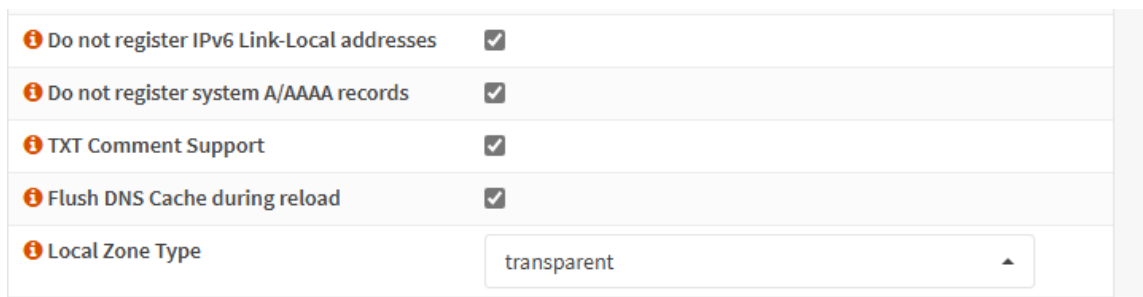
Services: Unbound DNS: General

advanced mode full help

Enable Unbound	<input checked="" type="checkbox"/>
Listen Port	53
Network Interfaces	LAN <small>Clear All Select All</small>
Enable DNSSEC Support	<input checked="" type="checkbox"/>
Enable DNS64 Support	<input checked="" type="checkbox"/>
DNS64 Prefix	64:ff9b::/96
Enable AAAA-only mode	<input checked="" type="checkbox"/>
Register ISC DHCP4 Leases	<input checked="" type="checkbox"/>
DHCP Domain Override	
Register DHCP Static Mappings	<input checked="" type="checkbox"/>

OPNsense (c) 2014-2024 Deciso B.V.

**Paso 39.** De la misma manera, marcamos las casillas correspondientes y, al finalizar, hacemos clic en el botón "Apply" para que los cambios se apliquen.



Do not register IPv6 Link-Local addresses	<input checked="" type="checkbox"/>
Do not register system A/AAAA records	<input checked="" type="checkbox"/>
TXT Comment Support	<input checked="" type="checkbox"/>
Flush DNS Cache during reload	<input checked="" type="checkbox"/>
Local Zone Type	transparent

## 2.7 ASINACIÓN DE DIRECCION IP STATIC AL FIREWALL

**Paso 40.** En este paso, configuraremos la interfaz del firewall. Como podemos ver, ya tenemos una dirección inicial de 172.16.4.1 con una máscara de subred 24.

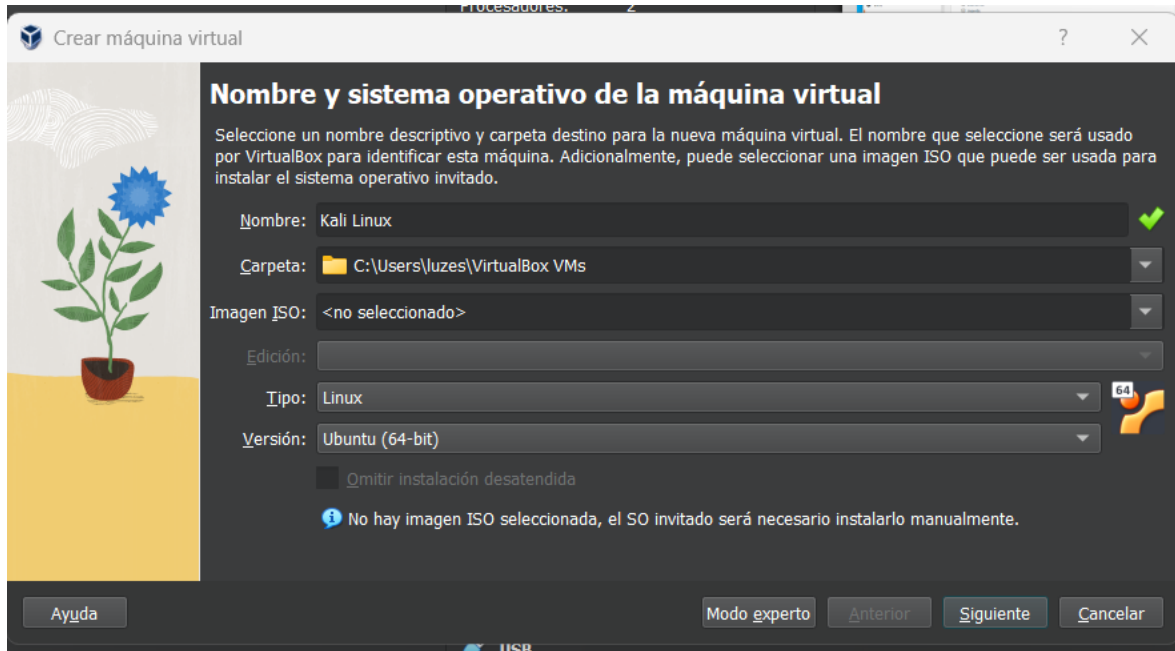


Static IPv4 configuration

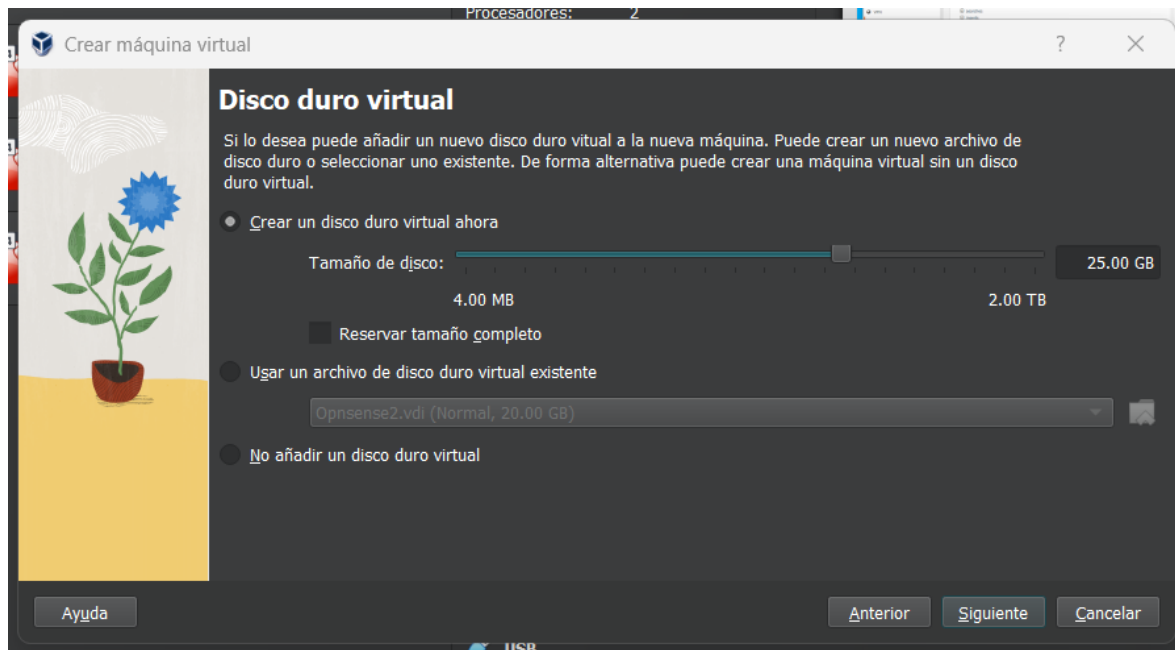
IPv4 address	172.16.4.1	24
IPv4 gateway rules	Disabled	

### 3. INSTALAR KALI LINUX EN UNA MÁQUINA VIRTUAL Y CONFIGURAR UN SISTEMA DE DETECCIÓN DE INTRUSOS

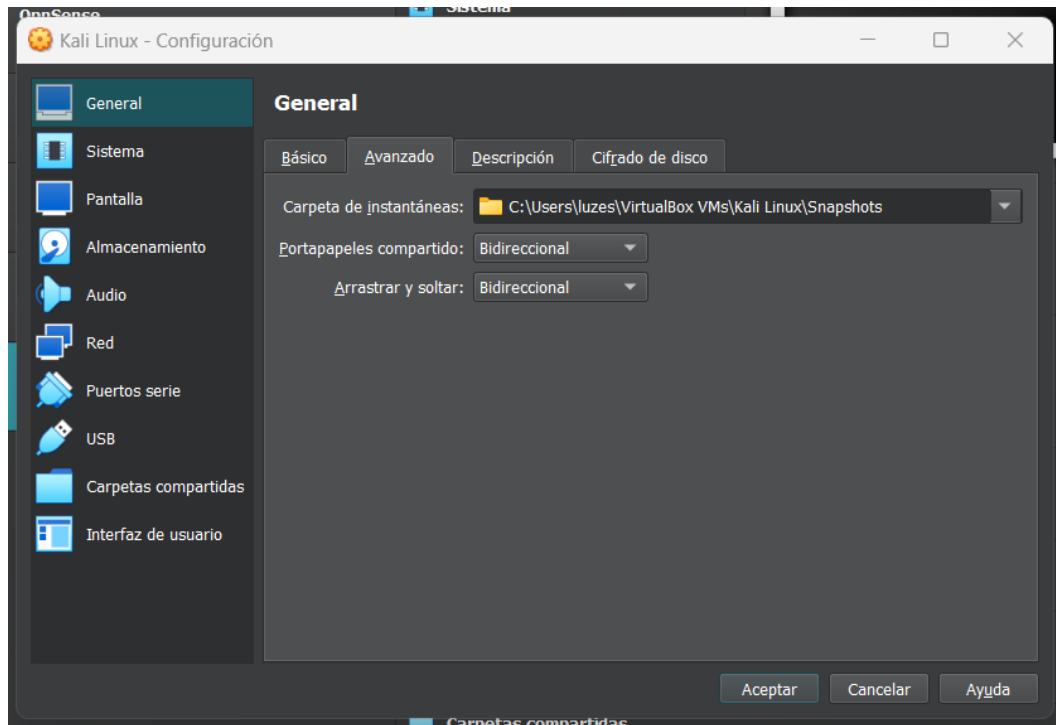
**Paso 1.** Comenzamos creando una nueva máquina virtual, asignándole el nombre "Kali Linux". Después, elegimos el archivo ISO, configuramos el tipo como "Linux" y seleccionamos "Ubuntu (64-bit)" para la versión. Por último, hacemos clic en **"Siguiente"**.



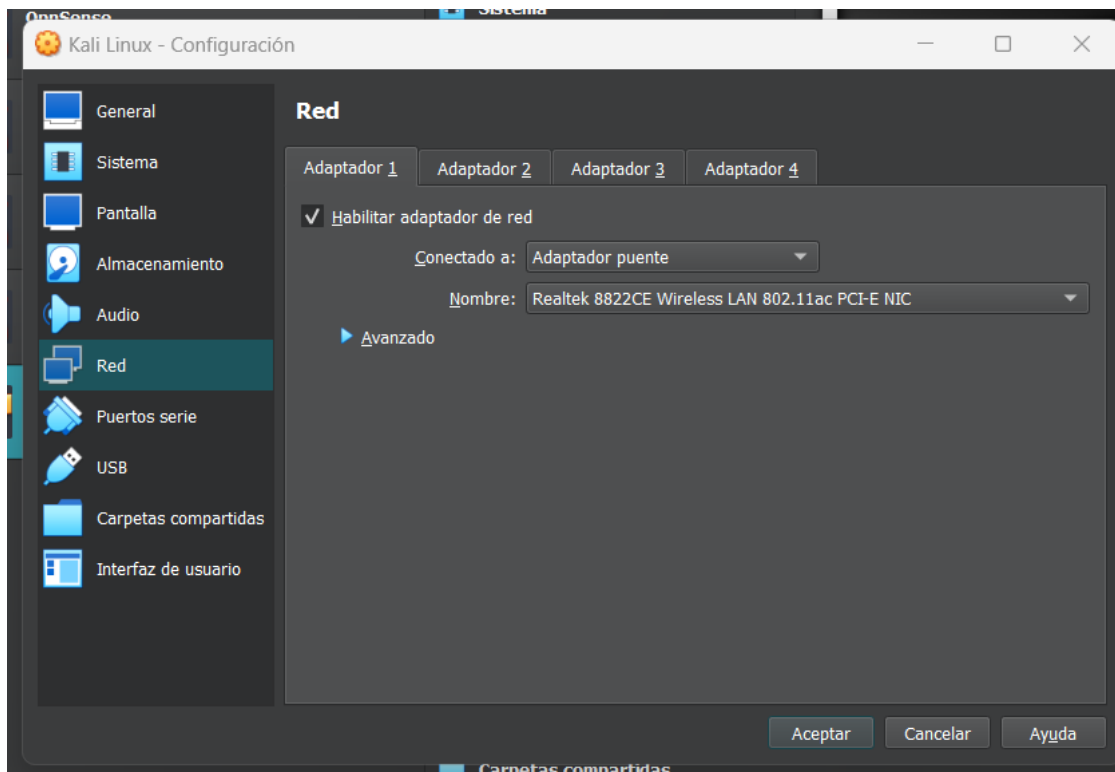
**Paso 2.** En este paso, establecemos el tamaño del disco duro virtual que necesitaremos para la máquina. Luego, hacemos clic en **"Siguiente"**.



**Paso 3.** En este paso, vamos a la sección de configuración, en el apartado "General". En las opciones de "Portapapeles compartido" y "Arrastrar y soltar", seleccionamos la opción "Bidireccional" para ambos.

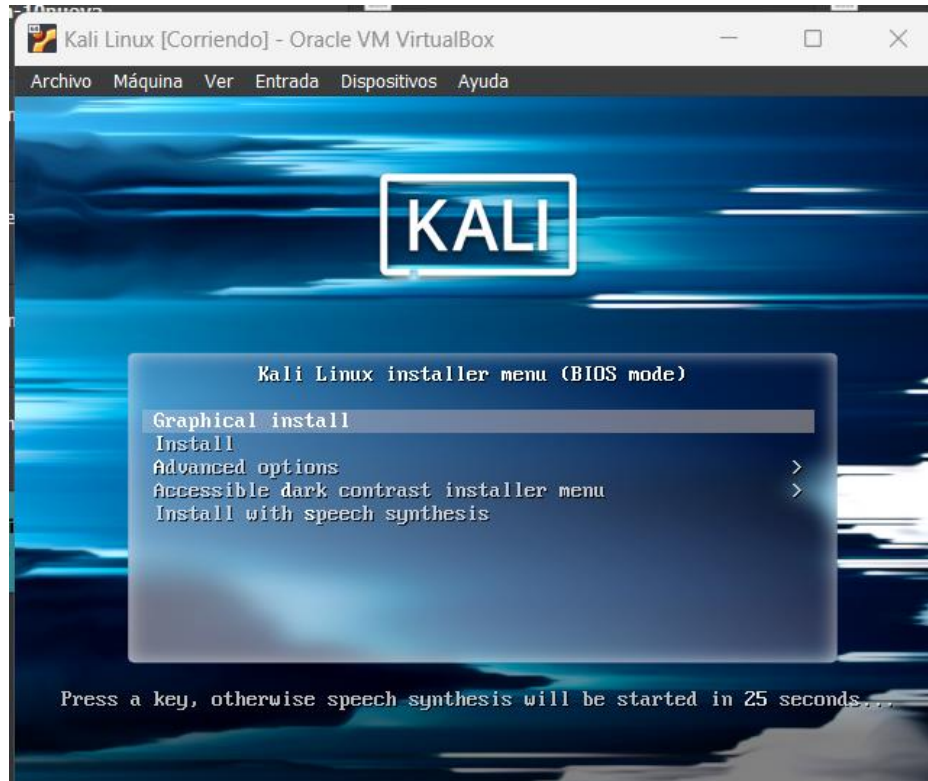


**Paso 4.** Una vez completados los pasos anteriores, nos dirigimos a la sección "Red". En el adaptador 1, elegimos la opción "Adaptador puente" en el campo "Conectado a" para asignar una dirección IP a la máquina virtual. Luego, hacemos clic en "**Aceptar**" y arrancamos la máquina virtual.

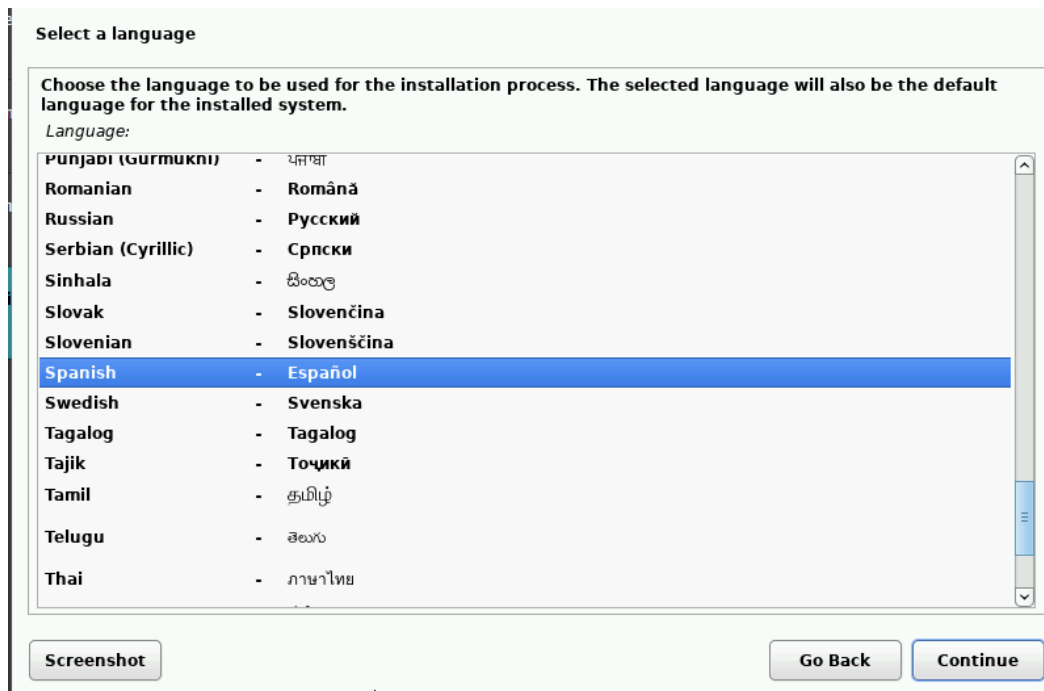




**Paso 5.** Al iniciar, se mostrará la interfaz de Kali Linux. Allí, seleccionamos la primera opción que dice "Graphical Install".



**Paso 6.** En este paso, elegimos el idioma que deseamos utilizar y luego hacemos clic en el botón "Continue".





**Paso 7.** A continuación, seleccionamos nuestro país de origen, en este caso "México", y luego hacemos clic en el botón "Continuar".

**Seleccione su ubicación**

La ubicación seleccionada aquí se utilizará para fijar su zona horaria y también como ejemplo para ayudarle a seleccionar la localización de su sistema. Esta localización será habitualmente el país donde vd. vive.

Esta es una lista reducida de ubicaciones basada en el idioma que ha seleccionado. Escoja «otro» si su ubicación no está en la lista.

*País, territorio o área:*

- Chile
- Colombia
- Costa Rica
- Cuba
- Ecuador
- El Salvador
- España
- Estados Unidos
- Guatemala
- Honduras
- México**
- Nicaragua
- Panamá

**Capturar la pantalla** **Retroceder** **Continuar**

**Paso 8.** En este paso, configuramos el teclado seleccionando la opción "Latinoamericano" y luego hacemos clic en el botón "Continuar".

**Configure el teclado**

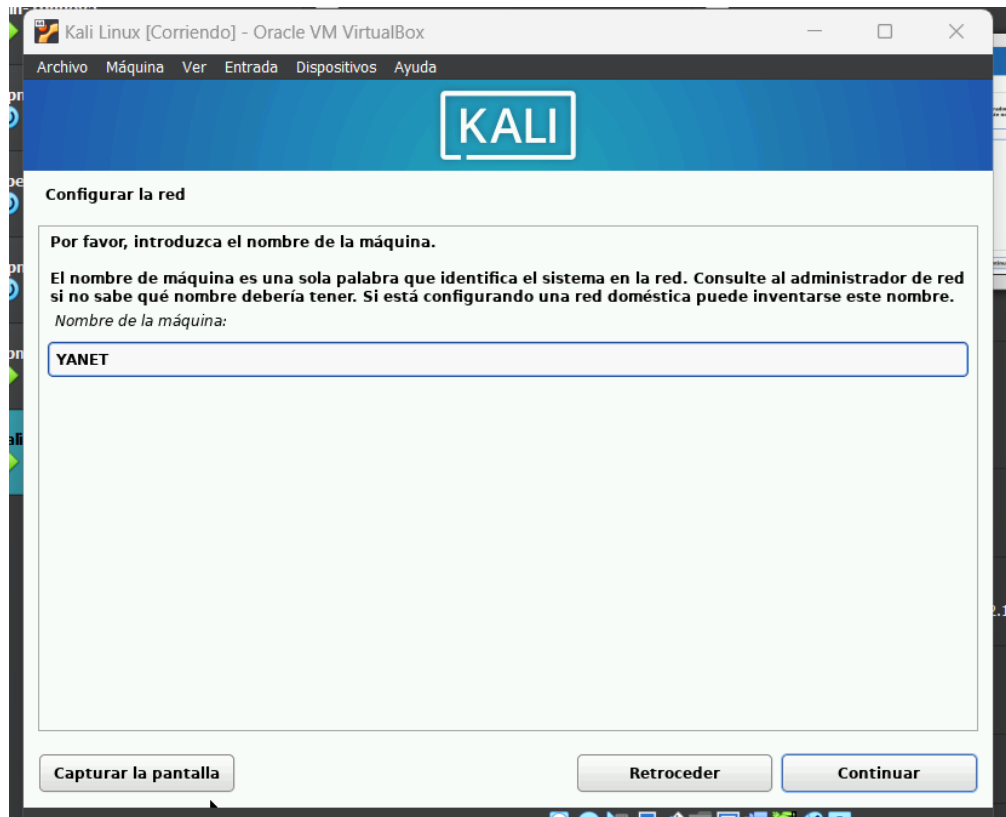
*Mapa de teclado a usar:*

- Canarés
- Kazajo
- Jemer
- Kirghizo
- Coreano
- Kurdo (variante F)
- Kurdo (variante Q)
- Laosiano
- Latinoamericano**
- Letón
- Lituano
- Macedonio
- Malayalamo
- Nepalés
- Sami septentrional
- Noruego
- Persa

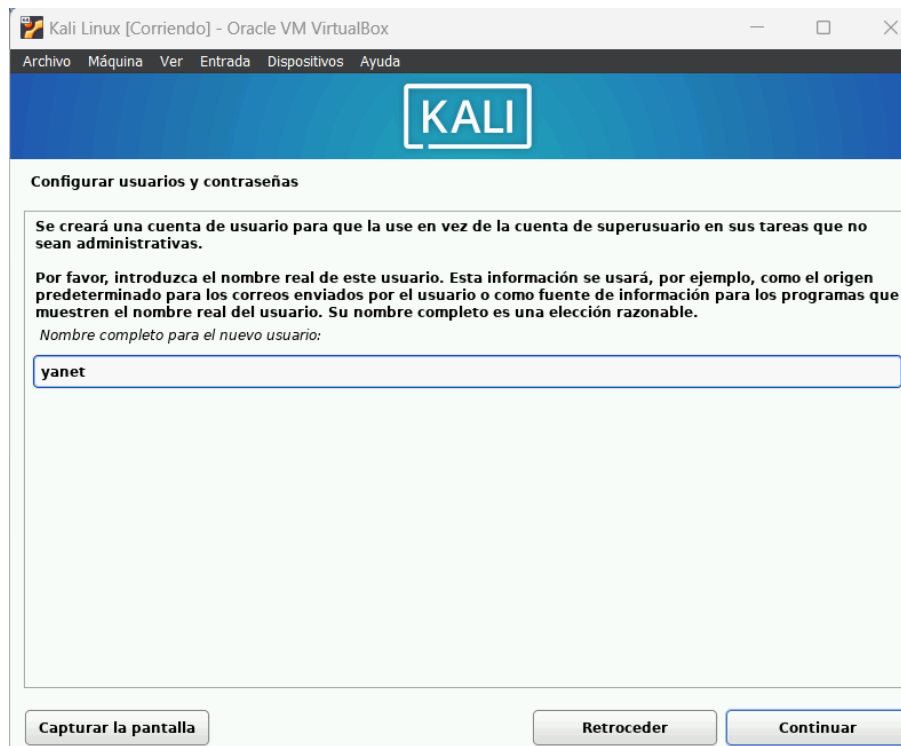
**Capturar la pantalla** **Retroceder** **Continuar**



**Paso 9.** En este paso, asignamos el nombre "YANET" a nuestra máquina y luego hacemos clic en el botón **"Continuar"**.



**Paso 10.** En este paso, asignamos el nombre de usuario "yanet" a nuestra máquina y luego hacemos clic en el botón **"Continuar"**.





**Paso 11.** Luego, nos solicitará que establezcamos una contraseña. Ingresamos la contraseña en el primer campo y la volvemos a escribir en el segundo para confirmarla.

**Configurar usuarios y contraseñas**

**Asegúrese de seleccionar una contraseña segura que no pueda ser adivinada.**  
*Elija una contraseña para el nuevo usuario:*

●●●●●

☐ Mostrar la contraseña en claro

**Por favor, introduzca la misma contraseña de usuario de nuevo para verificar que la introdujo correctamente.**  
*Vuelva a introducir la contraseña para su verificación:*

●●●●●

☐ Mostrar la contraseña en claro

Capturar la pantalla

Retroceder

Continuar

**Paso 12.** En este paso, configuramos la zona horaria de la máquina según nuestra ubicación. En nuestro caso, seleccionamos la opción "Central" y luego hacemos clic en el botón "**Continuar**".

**Configurar el reloj**

**Si la zona horaria deseada no está en la lista entonces vuelva atrás al paso «Escoja el idioma» y seleccione un país que utilice la zona horaria deseada (el país donde vive o está ubicado).**  
*Seleccione su zona horaria:*

Noroeste

Pacífico

Sonora

**Central**

Sureste

Capturar la pantalla

Retroceder

Continuar



**Paso 13.** En este paso, se nos pedirá que elijamos una opción para particionar el disco. Seleccionamos la primera opción, "Guiado - usar todo el disco", y luego hacemos clic en el botón **"Continuar"**.

Particionado de discos

Este instalador puede guiarle en el particionado del disco (utilizando distintos esquemas estándar) o, si lo desea, puede hacerlo de forma manual. Si escoge el sistema de particionado guiado tendrá la oportunidad más adelante de revisar y adaptar los resultados.

Si elige la partición guiada en un disco completo, se le preguntará qué disco desea utilizar.

Método de particionado:

- Guiado - utilizar todo el disco**
- Guiado - utilizar el disco completo y configurar LVM
- Guiado - utilizar todo el disco y configurar LVM cifrado
- Manual

Capturar la pantalla

Retroceder Continuar

**Paso 14.** En este paso, mantenemos la primera opción predeterminada y luego hacemos clic en **"Continuar"**.

Particionado de discos

Seleccionado para particionar:

SCSI3 (0,0,0) (sda) - ATA VBOX HARDDISK: 26.8 GB

Este disco puede particionarse siguiendo uno o varios de los diferentes esquemas disponibles. Si no está seguro, escoja el primero de ellos.

Esquema del particionado:

- Todos los ficheros en una partición (recomendado para novatos)**
- Separar la partición /home
- Separar particiones /home, /var y /tmp

Capturar la pantalla

Retroceder Continuar



**Paso 15.** A continuación, aparecerá una ventana en la que se confirmarán todos los cambios realizados en el disco. Seleccionamos la opción "Sí" y luego hacemos clic en el botón "**Continuar**".

Particionado de discos

Se escribirán en los discos todos los cambios indicados a continuación si continúa. Si no lo hace podrá hacer cambios manualmente.

Se han modificado las tablas de particiones de los siguientes dispositivos:  
SCSI3 (0,0,0) (sda)

Se formatearán las siguientes particiones:  
partición #1 de SCSI3 (0,0,0) (sda) como ext4  
partición #5 de SCSI3 (0,0,0) (sda) como intercambio

¿Desea escribir los cambios en los discos?

☐ No

☒ **Sí**

Capturar la pantalla

Continuar

**Paso 16.** A continuación, se mostrará una ventana donde se nos pedirá elegir el tipo de programa que queremos instalar. Dejamos las opciones predeterminadas seleccionadas y luego hacemos clic en el botón "**Continuar**".

Selección de programas

At the moment, only the core of the system is installed. The default selections below will install Kali Linux with its standard desktop environment and the default tools.

You can customize it by choosing a different desktop environment or a different collection of tools.

Choose software to install:

☒ Desktop environment [selecting this item has no effect]

☒ ... Xfce (Kali's default desktop environment)

☐ ... GNOME

☐ ... KDE Plasma

☒ Collection of tools [selecting this item has no effect]

☒ ... top10 -- the 10 most popular tools

☒ ... default -- recommended tools (available in the live system)

Capturar la pantalla

Continuar

**Paso 17.** A continuación, aparecerá un mensaje de advertencia sobre la instalación del cargador de arranque GRUB. Elegimos la opción "Sí" y hacemos clic en "Continuar".

Instalando el cargador de arranque GRUB

Parece que esta instalación es el único sistema operativo en el ordenador. Si esto es así, puede instalar sin riesgos el cargador de arranque GRUB en su unidad principal (partición UEFI o registro de arranque).

Advertencia: si su ordenador tiene otro sistema operativo que el instalador no pudo detectar, esto hará que ese sistema operativo no se pueda iniciar temporalmente, aunque GRUB se puede configurar manualmente más tarde para iniciarlo.

¿Desea instalar el cargador de arranque GRUB en su unidad principal?

☐ No

☒ **Sí**

Capturar la pantalla Retroceder Continuar

**Paso 18.** En este paso, seleccionamos la primera opción para configurar el dispositivo manualmente y luego hacemos clic en "Continuar". El proceso tomará algunos minutos.

Instalando el cargador de arranque GRUB

Ahora debe configurar el sistema recién instalado para que sea arrancable, instalando para ello el cargador GRUB en un dispositivo del que se pueda arrancar. La forma habitual de hacerlo es instalar GRUB en su unidad principal (partición UEFI o registro principal de arranque). Si lo prefiere, puede instalar GRUB en cualquier otra unidad (o partición), o incluso en un medio removible.

Dispositivo donde instalar el cargador de arranque:

**Introducir el dispositivo manualmente**

/dev/sda (ata-VBOX\_HARDDISK\_VBee23691b-67461c27)

Capturar la pantalla Retroceder Continuar



**Paso 19.** Seleccionamos este apartado predeterminado ya que con esto instalamos el cargador de arranque de GRUB. Clic en continuar.

Instalando el cargador de arranque GRUB

Ahora debe configurar el sistema recién instalado para que sea arrancable, instalando para ello el cargador GRUB en un dispositivo del que se pueda arrancar. La forma habitual de hacerlo es instalar GRUB en su unidad principal (partición EFI o registro principal de arranque). Si lo prefiere, puede instalar GRUB en cualquier otra unidad (o partición), o incluso en un medio removable.

Dispositivo donde instalar el cargador de arranque:

Introducir el dispositivo manualmente

/dev/sda (ata-VBOX\_HARDDISK\_VBee23691b-67461c27)

Capturar la pantalla

Retroceder

Continuar

**Paso 20.** Una vez finalizada la instalación, aparecerá un mensaje indicando que el proceso se completó y que es necesario reiniciar. Hacemos clic en el botón "Continuar".

Terminar la instalación



Instalación completada

La instalación se ha completado. Ahora podrá arrancar el nuevo sistema. Asegúrese de extraer el medio de instalación para que el sistema arranque del disco en lugar de reiniciar la instalación.

Por favor, elija <Continuar> para reiniciar.

Capturar la pantalla

Retroceder

Continuar



**Paso 21.** Al ingresar, la parte que pusimos como usuario y contraseña nos pedirá que ingresemos en esta parte para poder continuar y ver la interfaz de Kali Linux.

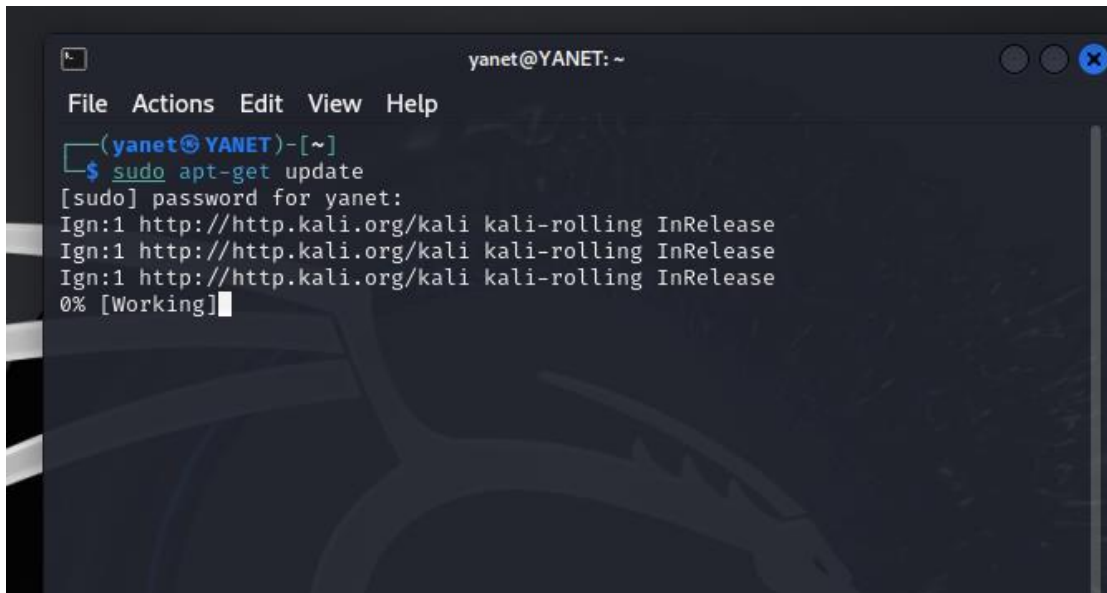


**Paso 22.** Después del reinicio, se nos pedirá que ingresemos el nombre de usuario y la contraseña configurados durante la instalación del sistema operativo. Al ingresar los datos correctamente, accederemos a la interfaz de Kali Linux.



## 3.1 INSTALAR UN SISTEMA DE DETECCIÓN DE INTRUSOS COMO SNORT O SURICATA

**Paso 23.** Abrimos la terminal y escribimos el comando `sudo apt-get update` para actualizar la información sobre los paquetes disponibles y sus versiones en los repositorios. Este comando solo descarga la información más reciente y no realiza ninguna instalación ni actualización. Esperamos a que termine el proceso.

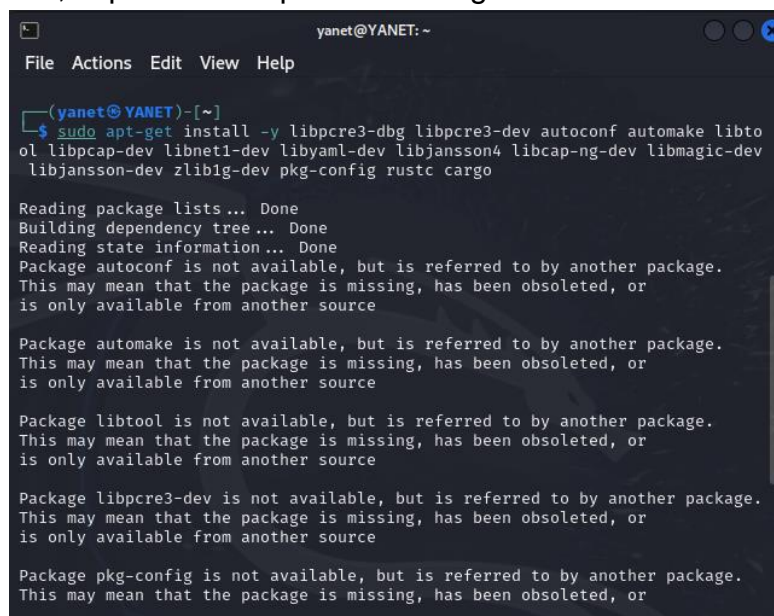


```
yanet@YANET: ~  
File Actions Edit View Help  
(yanet@YANET)-[~]  
$ sudo apt-get update  
[sudo] password for yanet:  
Ign:1 http://http.kali.org/kali kali-rolling InRelease  
Ign:1 http://http.kali.org/kali kali-rolling InRelease  
Ign:1 http://http.kali.org/kali kali-rolling InRelease  
0% [Working]
```

**Paso 24.** Una vez completado el paso anterior, ingresamos el siguiente comando:

```
sudo apt-get install libpcrc3-dbg libpcrc3-dev autoconf automake libtool libpcap-dev libnet1-dev  
libyaml-dev libjansson4 libcap-ng-dev libmagic-dev libjansson-dev zlib1g-dev pkg-config rustc cargo.
```

Este comando instalará varios paquetes y dependencias necesarias en Kali Linux. Al igual que antes, esperamos a que se descarguen e instalen.



```
yanet@YANET: ~  
File Actions Edit View Help  
(yanet@YANET)-[~]  
$ sudo apt-get install -y libpcrc3-dbg libpcrc3-dev autoconf automake libtool libpcap-dev libnet1-dev libyaml-dev libjansson4 libcap-ng-dev libmagic-dev libjansson-dev zlib1g-dev pkg-config rustc cargo  
  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
Package autoconf is not available, but is referred to by another package.  
This may mean that the package is missing, has been obsoleted, or  
is only available from another source  
  
Package automake is not available, but is referred to by another package.  
This may mean that the package is missing, has been obsoleted, or  
is only available from another source  
  
Package libtool is not available, but is referred to by another package.  
This may mean that the package is missing, has been obsoleted, or  
is only available from another source  
  
Package libpcrc3-dev is not available, but is referred to by another package.  
This may mean that the package is missing, has been obsoleted, or  
is only available from another source  
  
Package pkg-config is not available, but is referred to by another package.  
This may mean that the package is missing, has been obsoleted, or
```

**Paso 25.** A continuación, procedemos a instalar Suricata, el motor de detección y prevención de intrusiones (IDS/IPS) en la red, utilizando el siguiente comando:

```
sudo apt install suricata -y.
```

Esperamos a que la instalación se complete.

```
└─$ sudo apt install suricata -y
Installing:
suricata

Installing dependencies:
isa-support      librtt-bus-vdev24  librtt-log24      librtt-pci24      oinkmaster
libfdt1          librtt-eal24      librtt-mbuf24     librtt-rcu24      snort-rules-default
libhttp2         librtt-ethdev24   librtt-mempool24  librtt-ring24     sse3-support
libhyperscan5    librtt-hash24     librtt-meter24    librtt-sched24    sse4.2-support
libnetfilter-log1 librtt-ip-frag24  librtt-net-bond24  librtt-telemetry24 suricata-update
librtt-bus-pci24 librtt-kvargs24   librtt-net24      libxdp1

Paquetes sugeridos:
snort | snort-pgsql | snort-mysql | libtcmalloc-minimal4

Summary:
Upgrading: 0, Installing: 30, Removing: 0, Not Upgrading: 1145
Download size: 6.812 kB
Space needed: 31,7 MB / 9.427 MB available
```

**Paso 26.** Después de completar la instalación, aparecerá una ventana que indica que algunos de los servicios instalados requieren un reinicio para aplicar las actualizaciones. Seleccionamos la opción "Sí" para proceder con el reinicio.

```
Configuración de libc6:amd64

Hay algunos servicios instalados en el sistema que requieren reiniciarse al actualizar paquetes como libpam, libc, y libssl. Ya que reiniciar estos servicios puede provocar una interrupción de servicio del sistema, habitualmente se le solicitará en cada actualización una lista de los servicios que desea reiniciar. Puede seleccionar esta opción para impedir que se le solicite esta información; en su lugar, cada reinicio de servicio se hará de forma automática de forma que evitará que se le planteen preguntas cada vez que se actualice una biblioteca.

¿Quiere que los servicios se actualicen durante una actualización de paquete sin solicitar confirmación?

<S> <No>
```

**Paso 27.** El sistema comenzará a actualizar todos los servicios que se mencionaron previamente en el mensaje.

```
Setting up libobjc-14-dev:amd64 (14.2.0-6) ...
Setting up zlib1g-dev:amd64 (1:1.3.dfsg+really1.3.1-1+b1) ...
Setting up rustc (1.81.0+dfsg1-2) ...
Setting up llvm-18 (1:18.1.8-12) ...
Setting up llvm-18-dev (1:18.1.8-12) ...
Setting up clang-18 (1:18.1.8-12) ...
Setting up cargo (1.81.0+dfsg1-2) ...
Setting up rust-llvm (1.81.0+dfsg1-2) ...
```

**Paso 28.** Una vez completada la actualización, continuamos ingresando el siguiente comando:

```
wget http://rules.emergingthreats.net/open/suricata/emerging.rules.tar.gz
```

Este comando descargará un archivo llamado `emerging.rules.tar.gz`, el cual contiene un conjunto de reglas de Emerging Threats que utilizaremos con Suricata.

```
(yanet@YANET)-[~]  
$ wget http://rules.emergingthreats.net/open/suricata/emerging.rules.tar.gz
```

**Paso 29.** Ejecutamos el siguiente comando para descomprimir y extraer el archivo descargado previamente.

```
$ tar zxvf emerging.rules.tar.gz  
rules/  
rules/3coresec.rules  
rules/BSD-License.txt
```

**Paso 30.** Ejecutamos el siguiente comando para mover la carpeta `rules` al directorio `/var/lib/suricata/`:

```
sudo mv rules /var/lib/suricata/
```

De esta manera, la carpeta `rules`, que contiene las reglas extraídas, será trasladada a la ubicación donde Suricata las utilizará para su configuración.

```
(yanet@YANET)-[~]  
$ sudo mv rules /var/lib/suricata/
```

**Paso 31.** Ingresamos al directorio con el siguiente comando.

```
(yanet@YANET)-[~]  
$ cd /var/lib/suricata/rules
```

**Paso 32.** Ejecutamos el siguiente comando:

```
sudo nano /etc/suricata/suricata.yaml
```

Esto abrirá el archivo de configuración de Suricata (suricata.yaml) en el editor de texto nano, donde podremos realizar las modificaciones necesarias para configurar el motor de detección y prevención de intrusiones.

```
$ sudo nano /etc/suricata/suricata.yaml
```

### 3.2 CONFIGURAR LAS REGLAS DE DETECCIÓN DE INTRUSOS.

**Paso 33.** En este paso, configuramos reglas personalizadas en Suricata, un motor de detección y prevención de intrusiones, para identificar patrones de tráfico específicos en la red. Estas reglas se enfocan en detectar eventos como:

Intentos de conexión ICMP, Intentos de conexión SSH, Posibles ataques DDoS en el puerto 80.

Estas reglas permiten generar alertas basadas en estos patrones de tráfico, lo que ayuda a identificar actividades sospechosas y potencialmente maliciosas en la red. Para guardar los cambios realizados en la configuración, se utiliza el comando Ctrl + O seguido de Enter, y para salir del editor se usa Ctrl + X.

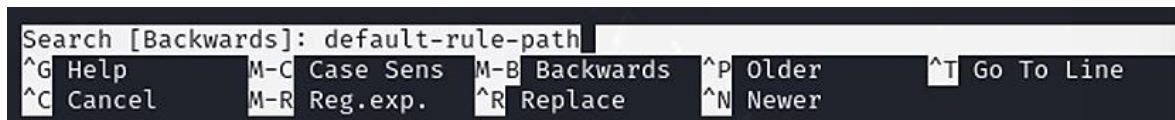
```
GNU nano 8.1 my-rules *
alert icmp any any -> $HOME_NET any (msg:"ICMP connection attempt"; sid:1000002; rev:1;)
alert tcp any any -> $HOME_NET 22 (msg:"SSH connection attempt"; sid:1000003; rev:1;)
alert tcp any any -> $HOME_NET 80 (msg:"DDoS Unusually fast port 80 SYN packets outbound, Potential DDoS"; flags: S,12; threshold: type both, track by_dst, count 500, seconds 5; classtype:misc-activity; sid:6;)
```



### 3.3 CONFIGURAR LAS ALERTAS DE DETECCIÓN DE INTRUSOS.

**Paso 34.** En este paso, se utiliza el comando Ctrl + B para activar la función de búsqueda dentro del archivo de configuración de Suricata. Luego, se ingresa el parámetro `default-rule-path`, que se usa para especificar la ubicación de los archivos de reglas que Suricata debe cargar. Este parámetro asegura que Suricata sepa dónde buscar las reglas que se utilizarán para el análisis del tráfico de red.

Una vez encontrado el parámetro, es posible editar su valor para que apunte al directorio correcto donde se encuentran las reglas personalizadas (por ejemplo, `/var/lib/suricata/rules`), lo que permitirá que Suricata utilice esas reglas al realizar su análisis.



**Paso 35.** En este paso, se abre una nueva ventana de configuración en Suricata donde se debe agregar información sobre los archivos de reglas específicos que Suricata debe cargar. Se ingresan los siguientes nombres de archivos:

- **emerging-exploit.rules:** Este archivo contiene reglas que están diseñadas para detectar posibles intentos de explotación (exploits) en la red.
- **my-rules:** Este archivo hace referencia a un conjunto de reglas personalizadas que han sido creadas o modificadas por el administrador o usuario para adaptarlas a necesidades específicas de detección de intrusos.

```
default-rule-path: /var/lib/suricata/rules
rule-files:
- emerging-exploit.rules
```

**Paso 36.** Este comando inicia Suricata en modo de monitoreo, utilizando el archivo de configuración `suricata.yaml` y especificando la interfaz de red `eth0` para que Suricata comience a analizar el tráfico de red en esa interfaz.

Al ejecutar este comando, el sistema pedirá la contraseña del usuario para proceder con la ejecución de Suricata. Una vez ingresada correctamente, Suricata comenzará a cargar y se pondrá en funcionamiento, monitorizando el tráfico de red y detectando posibles amenazas o intrusiones según las reglas configuradas.

```
$ sudo suricata -c /etc/suricata/suricata.yaml -i eth0
```

**Paso 37.** Este comando permite monitorear en tiempo real el archivo de registro fast.log de Suricata. El archivo fast.log contiene información detallada sobre los eventos y alertas generadas por el sistema de detección de intrusiones (IDS/IPS) de Suricata. Al usar tail -f, se visualizan las últimas líneas del archivo y cualquier nuevo evento que ocurra se añadirá en tiempo real, lo que permite monitorear las alertas y actividades de red detectadas por Suricata de manera continua.

```
$ tail -f /var/log/suricata/fast.log
10/31/2024-14:56:23.558268  [**] [1:1000002:1] ICMP connection attempt [**] [
Classification: (null)] [Priority: 3] {ICMP} 192.168.0.1:3 → 192.168.0.125:1
10/31/2024-14:56:39.007268  [**] [1:1000002:1] ICMP connection attempt [**] [
Classification: (null)] [Priority: 3] {ICMP} 192.168.0.1:3 → 192.168.0.125:1
10/31/2024-14:58:18.566396  [**] [1:1000002:1] ICMP connection attempt [**] [
Classification: (null)] [Priority: 3] {ICMP} 192.168.0.1:3 → 192.168.0.125:1
10/31/2024-14:58:36.814247  [**] [1:1000002:1] ICMP connection attempt [**] [
Classification: (null)] [Priority: 3] {ICMP} 192.168.0.108:8 → 192.168.0.125
```

**Paso 38.** Ingresamos el siguiente comando sudo nano /etc/network/interfaces para la configuración de la interfaz de red.

```
$ sudo nano /etc/network/interfaces
```

### 3.4 ASIGNAR UNA DIRECCIÓN IP ESTÁTICA A KALI LINUX.

**Paso 39.** En este apartado se ingresa lo que se muestra a continuación, guardamos cambios y salimos de la configuración.

```
source /etc/network/interfaces.d/*

# The loopback network interface
auto eth0
iface eth0 inet static
address 192.168.1.125
netmask 255.255.255.0
gateway 192.168.1.1
dns-nameservers 8.8.8.8
```

**Paso 40.** Este comando reinicia el servicio de red en el sistema. Al ejecutar este comando, se aplican los cambios realizados en la configuración de las interfaces de red, asegurando que las nuevas configuraciones de red entren en vigor sin necesidad de reiniciar el sistema completo. Es una manera rápida de restablecer la conectividad de red después de modificar los archivos de configuración de red.

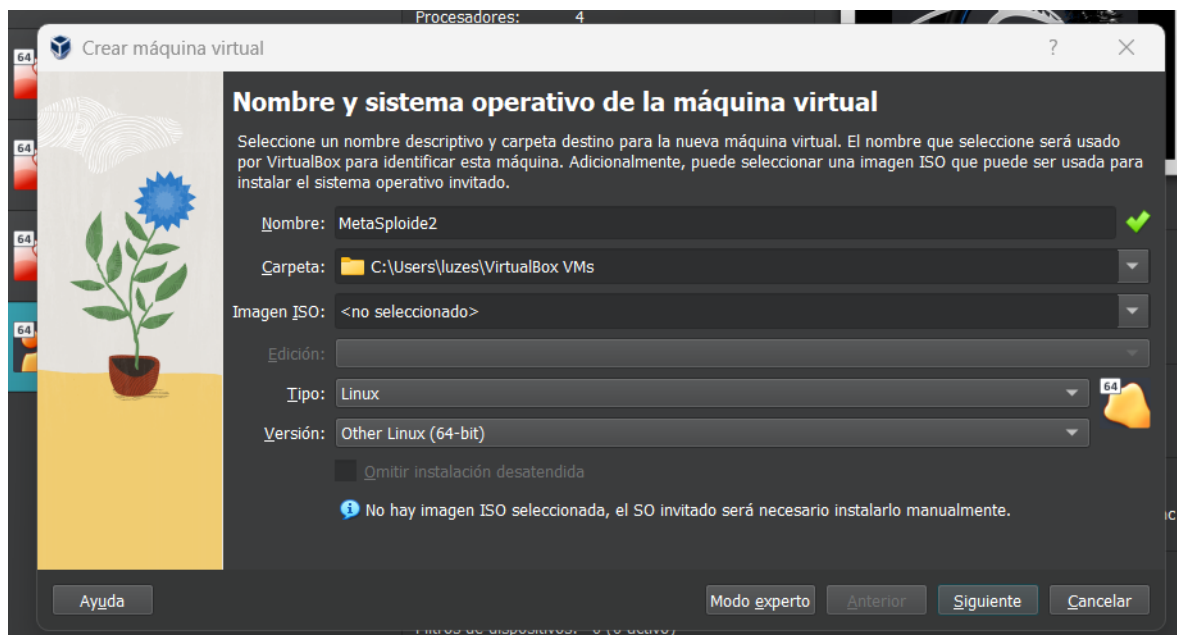
```
(yanet@YANET)-[~]
$ sudo systemctl restart networking
```

**Paso 41.** Este comando muestra la información detallada sobre la interfaz de red eth0. Al ejecutarlo, se verifica si la configuración de red se aplicó correctamente. Es útil para confirmar que la dirección IP y otros parámetros de la interfaz se han actualizado según las configuraciones previas, como el nombre de la interfaz y los ajustes de IP.

```
$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel s
tate UP group default qlen 1000
    link/ether 08:00:27:47:77:54 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.110/24 brd 192.168.1.255 scope global dynamic nop
refixroute eth0
        valid_lft 5292sec preferred_lft 5292sec
    inet 192.168.1.125/24 brd 192.168.1.255 scope global secondary e
th0
```

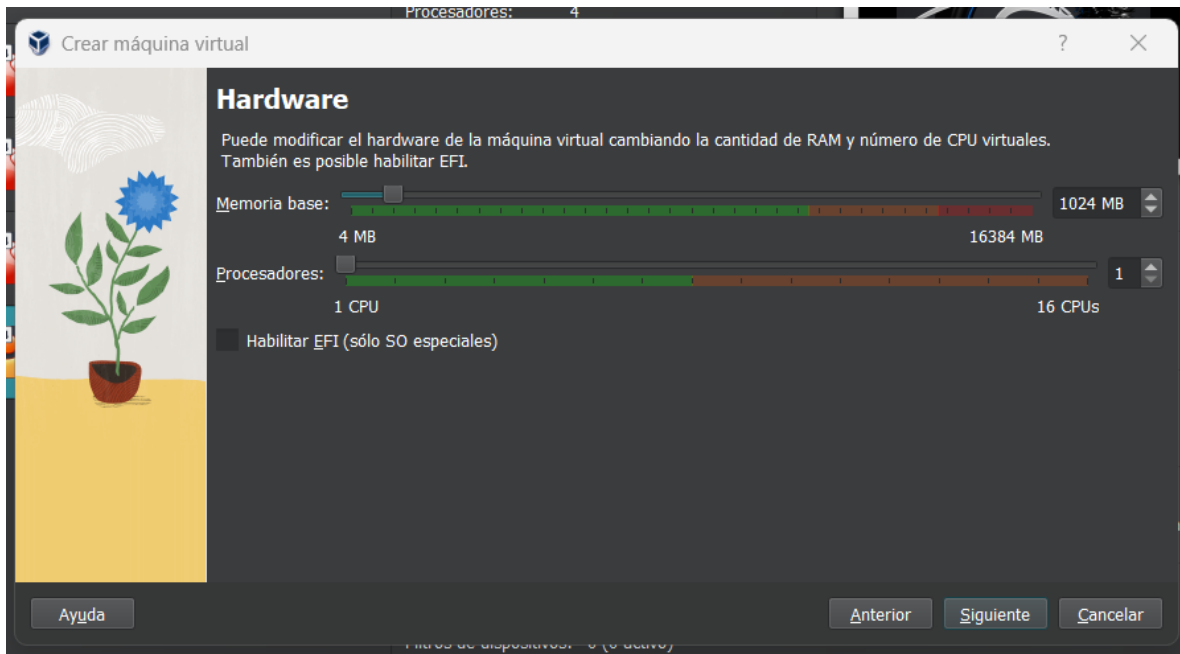
## 4. CREAR UNA MÁQUINA VIRTUAL VULNERABLE POR DISEÑO COMO METASPLOITABLE2.

**Paso 1.** Configuramos una nueva máquina virtual llamada MetaSploitable2, seleccionamos "Linux" como tipo y, en la opción de versión, elegimos "Other Linux (64-bit)", luego hacemos clic en el botón "**Siguiente**".

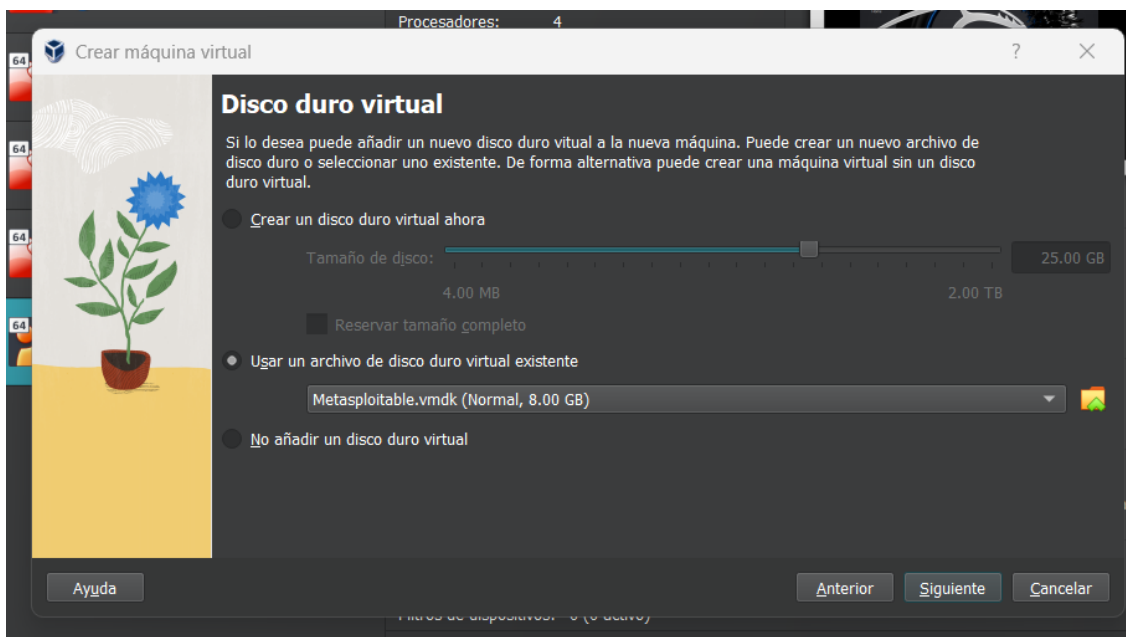




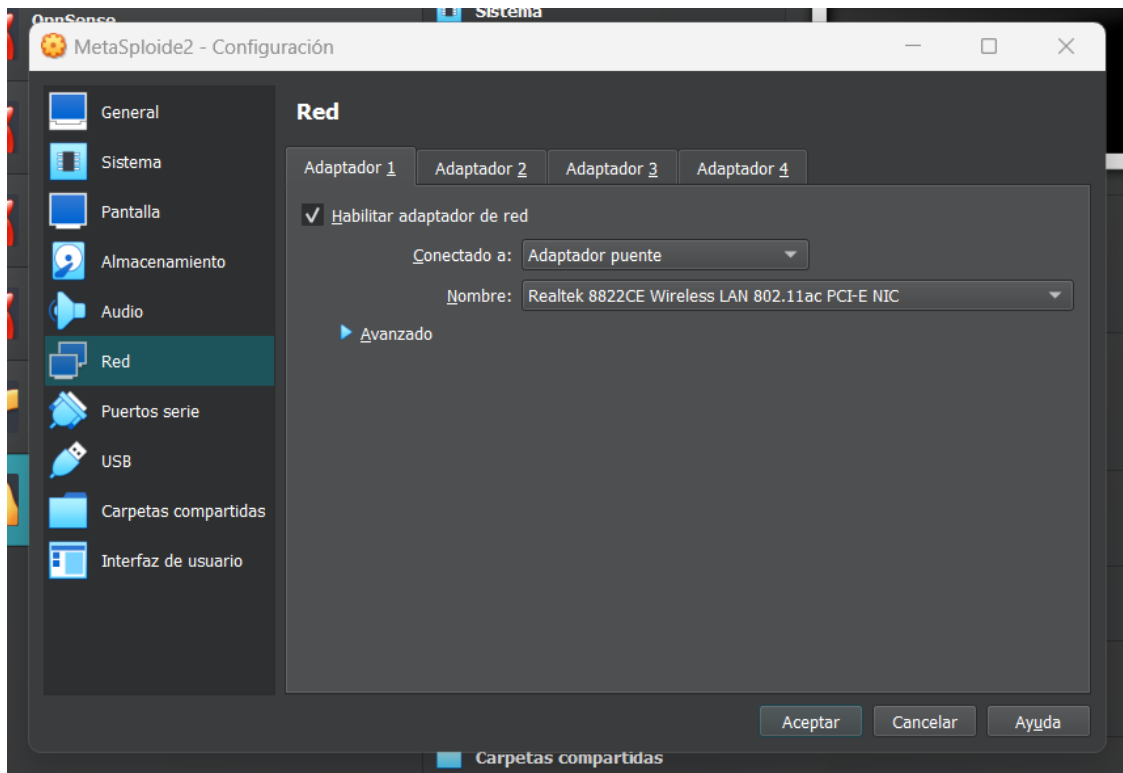
**Paso 2.** En la configuración de hardware, asignamos 1 GB de memoria RAM y dejamos los procesadores con la configuración predeterminada. Luego, hacemos clic en "**Siguiente**".



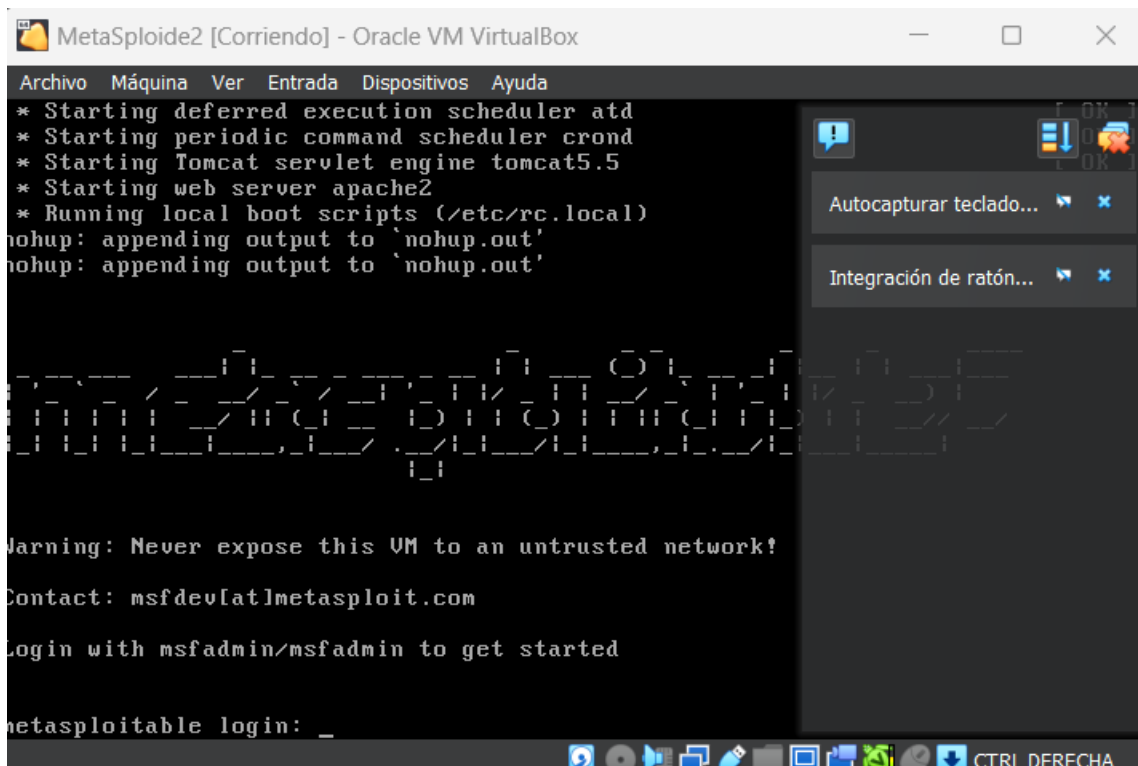
**Paso 3.** Asignamos 25 GB de espacio de almacenamiento y activamos la opción para utilizar un archivo de disco duro virtual existente. Seleccionamos el archivo ISO y luego hacemos clic en el botón "**Siguiente**" para continuar.



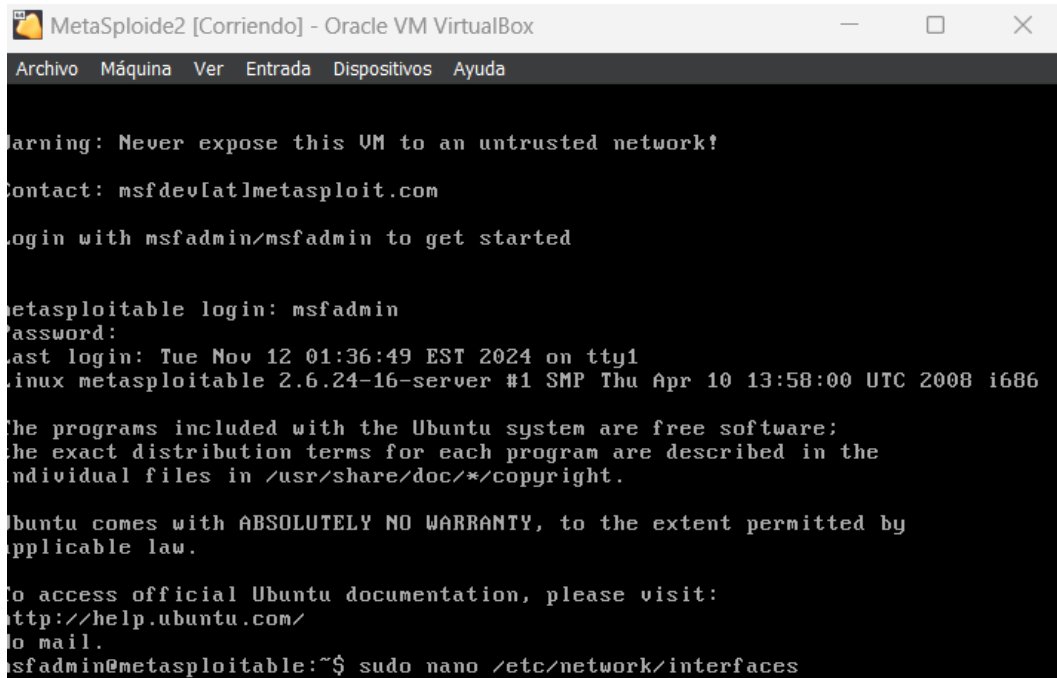
**Paso 4.** Después de crear la máquina virtual, configuramos la tarjeta de red. En este caso, seleccionamos "Adaptador puente" para asignar una dirección IP a la máquina virtual. Luego, hacemos clic en "**Aceptar**" y procedemos a iniciar la máquina.



**Paso 5.** Al iniciar la máquina virtual, comenzará a cargar y nos solicitará que ingresemos el nombre de usuario y la contraseña.



**Paso 6.** Después de ingresar el usuario y la contraseña, estaremos dentro del sistema y podremos realizar las acciones necesarias. Ingresamos el siguiente comando: `sudo nano /etc/network/interfaces` para acceder a la configuración de la interfaz de red.



```
MetaSploide2 [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

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

metasploitable login: msfadmin
Password:
Last login: Tue Nov 12 01:36:49 EST 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

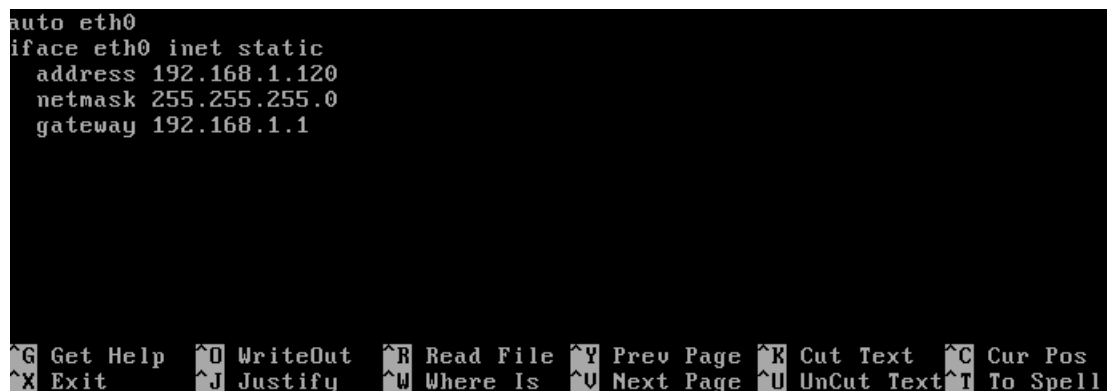
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

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

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
or mail.
msfadmin@metasploitable:~$ sudo nano /etc/network/interfaces
```

## 4.1 ASIGNAR UNA DIRECCIÓN IP ESTÁTICA A METASPLOITABLE2.

**Paso 7.** En la interfaz de red, añadimos lo siguiente para asignar una dirección IP estática.



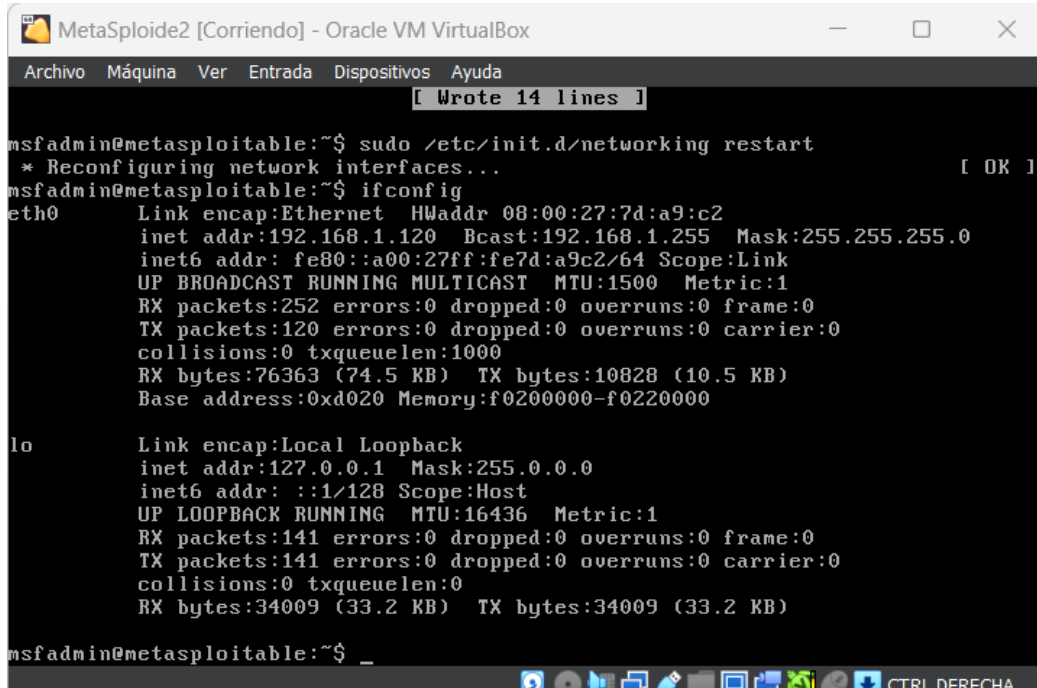
```
auto eth0
iface eth0 inet static
    address 192.168.1.120
    netmask 255.255.255.0
    gateway 192.168.1.1

^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text   ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page  ^U UnCut Text ^T To Spell
```

**Paso 8.** Ingresamos el siguiente comando para reiniciar los servicios de red.

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

**Paso 9.** Verificamos que los cambios se hayan aplicado correctamente.



```
MetaSploide2 [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
[ Wrote 14 lines ]
msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart
* Reconfiguring network interfaces... [ OK ]
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:7d:a9:c2
          inet addr:192.168.1.120  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe7d:a9c2/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:252 errors:0 dropped:0 overruns:0 frame:0
          TX packets:120 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:76363 (74.5 KB)  TX bytes:10828 (10.5 KB)
          Base address:0xd020  Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:141 errors:0 dropped:0 overruns:0 frame:0
          TX packets:141 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:34009 (33.2 KB)  TX bytes:34009 (33.2 KB)

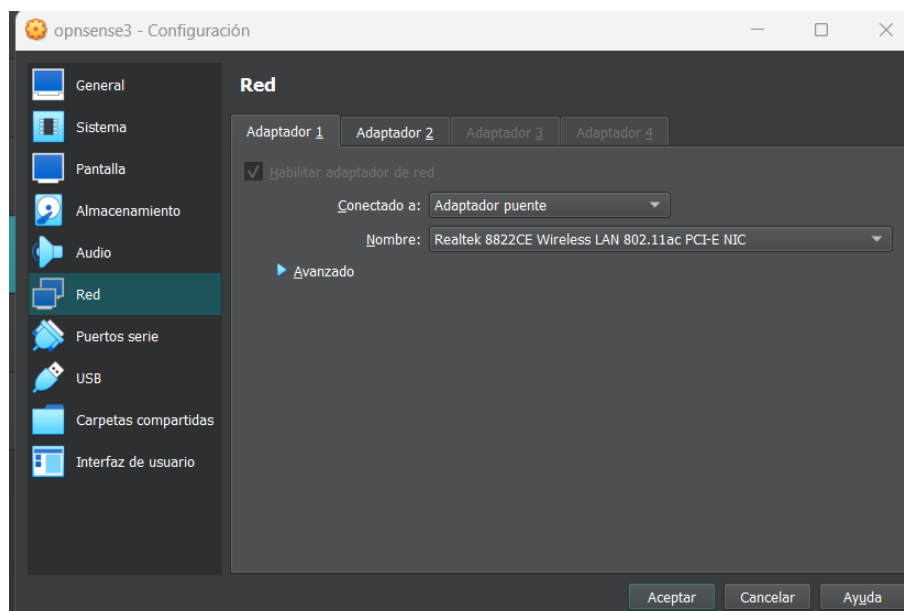
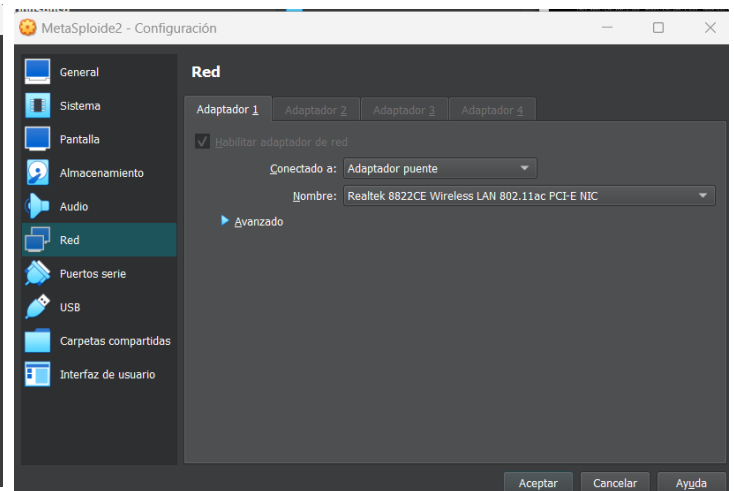
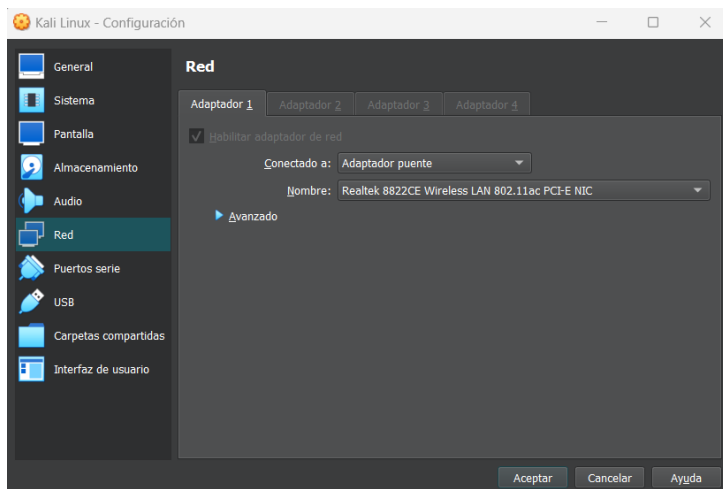
msfadmin@metasploitable:~$ _
```

## 5. PING SATISFACTORIO ENTRE LAS MÁQUINAS VIRTUALES.

Para realizar un ping exitoso entre las máquinas virtuales, necesitamos seguir los siguientes pasos:

### 5.1 CONFIGURAR LAS INTERFACES DE RED DE LAS MÁQUINAS VIRTUALES.

La configuración de las interfaces de red en máquinas virtuales es esencial para garantizar que puedan comunicarse correctamente entre ellas.





## 5.2 CONFIGURAR LAS REGLAS DE FIREWALL PARA PERMITIR EL TRÁFICO DE PING.

Configurar correctamente las reglas del firewall para permitir el tráfico de ping es esencial para probar la conectividad entre máquinas virtuales.

### Firewall: Rules: LAN

#### Edit Firewall rule

full help

Action	Pass
Disabled	<input type="checkbox"/> Disable this rule
Quick	<input checked="" type="checkbox"/> Apply the action immediately on match.
Interface	LAN
Direction	in
TCP/IP Version	IPv4
Protocol	ICMP
ICMP type	any

OPNsense (c) 2014-2024 Deciso B.V.

#### Source

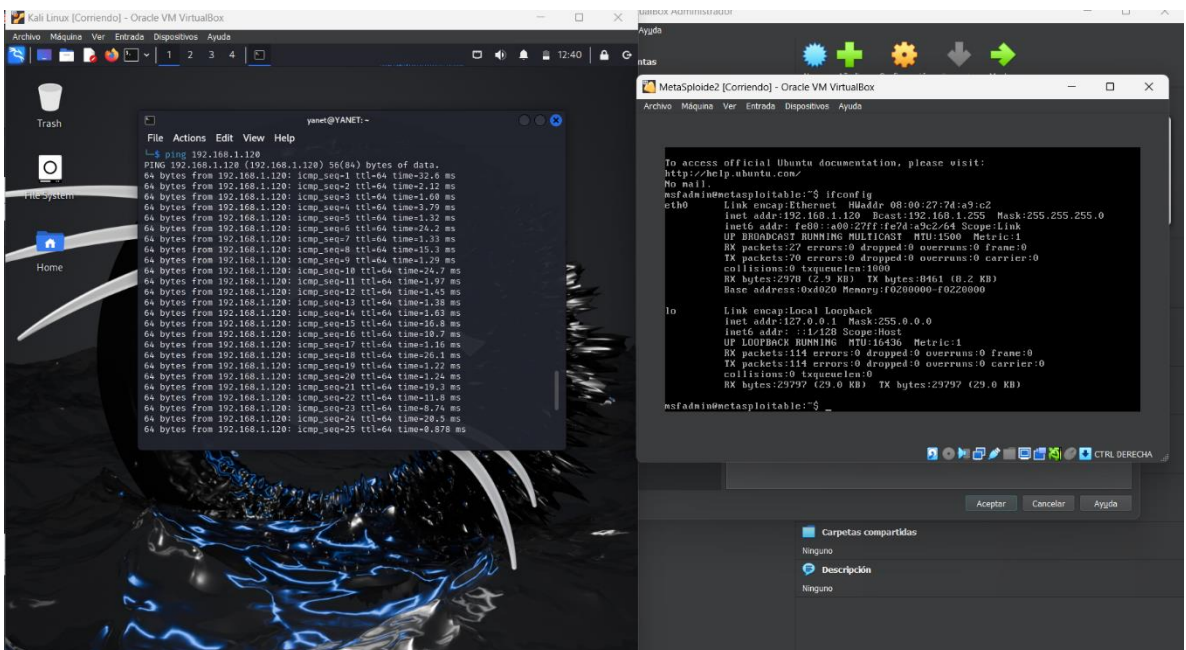
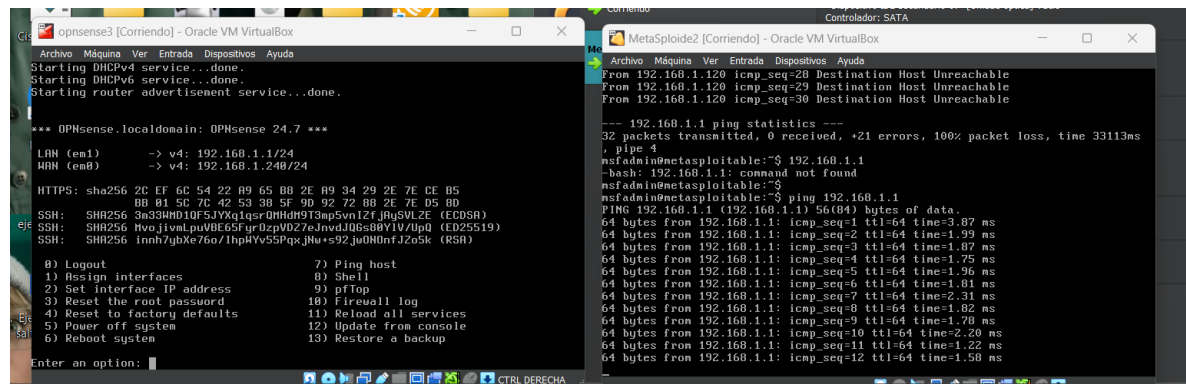
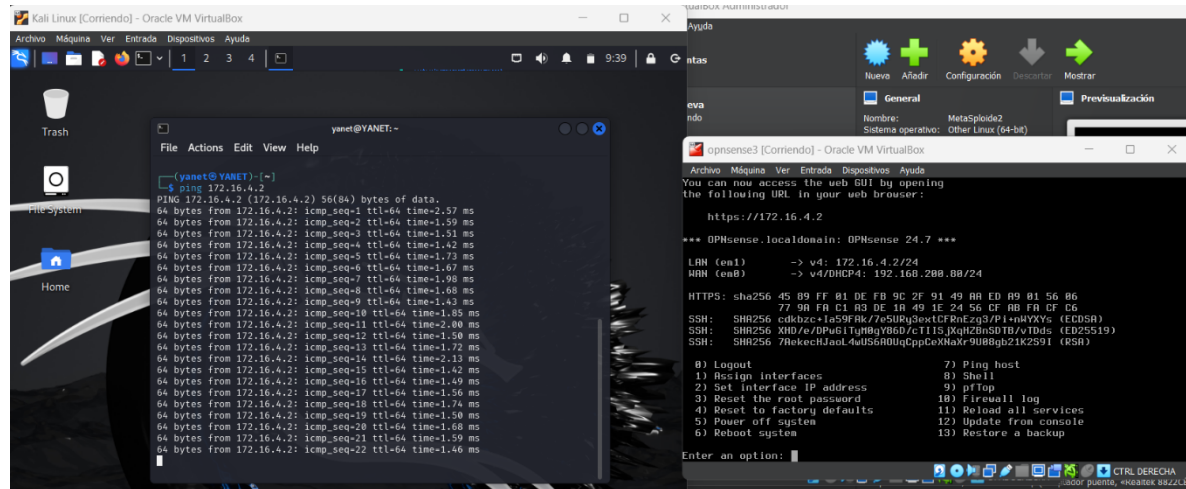
Advanced

Destination / Invert	<input type="checkbox"/> Use this option to invert the sense of the match.
Destination	any
Destination port range	from: any to: any
Log	<input checked="" type="checkbox"/> Log packets that are handled by this rule
Category	
Description	
No XMLRPC Sync	<input type="checkbox"/>
Schedule	none

OPNsense (c) 2014-2024 Deciso B.V.



## 5.3 REALIZAR UN PING ENTRE LAS MÁQUINAS VIRTUALES.





## Conclusión

Esta práctica fue un éxito porque logramos configurar las tres máquinas virtuales que se necesitaban: un firewall con OpnSense, un sistema para detectar intrusos con Kali Linux, y una máquina vulnerable con MetaSploitable2. Seguimos todos los pasos como estaban planeados, y pudimos verificar que las máquinas se comunicaban bien entre sí, usando el comando de ping para comprobarlo.

Es muy importante realizar este tipo de práctica porque nos ayudan a entender mejor cómo funcionan las redes y los sistemas de seguridad. Al trabajar en un entorno controlado, podemos aprender sin correr el riesgo de dañar un sistema real. Además, nos permitió practicar cómo detectar amenazas y proteger una red de posibles ataques, algo esencial si queremos mejorar nuestras habilidades en ciberseguridad. Es fundamental seguir haciendo estos ejercicios para seguir aprendiendo y estar mejor preparados para enfrentar los desafíos en la protección de redes y sistemas. Cada práctica nos da más confianza y nos acerca a ser más competentes en el manejo de la seguridad. Es así como se ha concluido esta práctica.





## Bibliografías

1. <https://support.academicsoftware.eu/hc/es/articles/360006725277-C%C3%B3mo-instalar-Oracle-VM-VirtualBox>
2. <https://www.virtualbox.org/wiki/Downloads>
3. <https://www.redeszone.net/2017/02/04/opnsense-conoce-este-completo-firewall-gratuito-instalar-red-domestica-empresa/>
4. <https://keepcoding.io/blog/que-es-pfsense/>
5. <https://openwebinars.net/blog/kali-linux-que-es-y-caracteristicas-principales/>
6. <https://rinku.tech/curso-kali-linux/instalar-metasploitable2/>