



**TECNOLÓGICO  
NACIONAL DE MÉXICO**



**TECNOLÓGICO NACIONAL DE  
MÉXICO**  
**INSTITUTO TECNOLÓGICO DE TLAXIACO**

**REPORTE DE  
PRACTICA 6**

**CATEDRATICO:** ING. EDWARD OSORIO SALINAS

**ASIGNATURA:** SEGURIDAD Y VIRTUALIZACIÓN

**INTEGRANTES DE EQUIPO:** SAÚL LÓPEZ BAUTISTA, LUZ ARLETH  
LOPEZ BAUTISTA

**GRADO:** SEPTIMO SEMESTRE

**GRUPO:** 7 US

Heroica ciudad de Tlaxiaco. A 25 de octubre del 2024

## INDICE

1. INSTALAR VIRTUALBOX.....	3
2. INSTALAR OPNSENSE O PFSENSE EN UNA MÁQUINA VIRTUAL Y CONFIGURAR UN FIREWALL.....	9
2.1 INSTALACIÓN DE OPNSENSE EN UNA MAQUINA VIRTUAL. ....	9
2.2 CONFIGURACIÓN DE INTERFACES.....	13
2.3 CONFIGURACIÓN DE REGLAS DE FIREWALL.....	19
2.4 CONFIGURAR EL NAT .....	21
2.5 CONFIGURACIÓN DE DHCP .....	23
2.6 CONFIGURACIÓN DE DNS.....	24
2.7 ASINACIÓN DE DIRECCION IP STATIC AL FIREWALL .....	25
3. INSTALAR KALI LINUX EN UNA MAQUINA VIRTUAL Y CONFIGURAR UN SISTEMA DE DETECCIÓN DE INTRUSOS .....	26
3.1 INSTALAR UN SISTEMA DE DETECCIÓN DE INTRUSOS COMO SNORT O SURICATA.....	38
3.2 CONFIGURAR LAS REGLAS DE DETECCIÓN DE INTRUSOS.....	42
3.3 CONFIGURAR LAS ALERTAS DE DETECCIÓN DE INTRUSOS.....	43
3.4 ASIGNAR UNA DIRECCIÓN IP ESTÁTICA A KALI LINUX.....	45
4. CREAR UNA MÁQUINA VIRTUAL VULNERABLE POR DISEÑO COMO METASPLOITABLE2.....	46
4.1 ASIGNAR UNA DIRECCIÓN IP ESTÁTICA A METASPLOITABLE2.....	49
5. PING SATISFACTORIO ENTRE LAS MÁQUINAS VIRTUALES.....	50
5.1 CONFIGURAR LAS INTERFACES DE RED DE LAS MÁQUINAS VIRTUALES. ....	50
5.2 CONFIGURAR LAS REGLAS DE FIREWALL PARA PERMITIR EL TRÁFICO DE PING.....	50
5.3 REALIZAR UN PING ENTRE LAS MÁQUINAS VIRTUALES.....	51
CONCLUSIONES .....	52
BIBLIOGRAFIA.....	53

## 1. INSTALAR VIRTUALBOX.

**Paso 1.** Descargamos Virtual Box en el sitio oficial <https://www.virtualbox.org/>. Donde buscamos la sección "Downloads", una vez que nos encontremos en la sección le damos clic.

### Welcome to VirtualBox.org!

VirtualBox is a powerful x86 and AMD64/Intel64 virtualization product enterprise as well as home use. Not only is VirtualBox an extremely feature rich, high performance product for enterprise customers, it is also the only professional solution that is freely available as Open Source Software under the terms of the GNU General Public License (GPL) version 3. See "About VirtualBox" for an introduction.

Presently, VirtualBox runs on Windows, Linux, macOS, and Solaris hosts and supports a large number of guest operating systems including but not limited to Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, Windows 8, Windows 10), DOS/Windows 3.x, Linux (2.4, 2.6, 3.x and 4.x), Solaris and OpenSolaris, OS/2, and OpenBSD.

VirtualBox is being actively developed with frequent releases and has a ever growing list of features, supported guest operating systems and platforms it runs on. VirtualBox is a community effort backed by a dedicated company: everyone is encouraged to contribute while Oracle ensures the product always meets professional quality criteria.



**Paso 2.** Una vez estando dentro de sección de aparecerán una cantidad de versiones tanto actualizados con versiones anteriores en mi caso descargamos la versión de VirtualBox 6.1.32 para Windows. Donde debemos encontrar un enlace con el nombre de "Windows hosts", ya que lo hayamos encontrado le damos clic en el enlace para descargar el instalador.

- **VirtualBox 6.1.32** (released January 18 2022)
  - [Windows hosts](#)
  - [Solaris hosts](#)
  - [Solaris 11 IPS hosts](#)
  - Linux Hosts:
    - [Oracle Linux 8 / Red Hat Enterprise Linux 8](#)
    - [Oracle Linux 7 / Red Hat Enterprise Linux 7 / CentOS 7](#)
    - [Oracle Linux 6 / Red Hat Enterprise Linux 6 / CentOS 6](#)
    - [Ubuntu 19.10 / 20.10 / 21.04](#)
    - [Ubuntu 18.04 / 18.10 / 19.04](#)
    - [Ubuntu 16.04](#)
    - [Debian 11](#)
    - [Debian 10](#)
    - [Debian 9](#)
    - [openSUSE 15.0](#)
    - [openSUSE 13.2 / Leap 42](#)
    - [Fedora 33 / 34](#)
    - [Fedora 32](#)
    - [All distributions](#)
  - [Extension Pack](#)

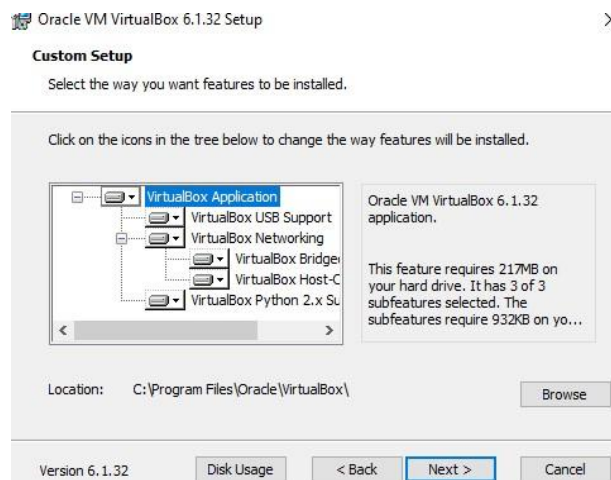
**Paso 3.** Después de que termine la descarga, nos dirigimos para nuestro centro de descargas que está en archivos buscamos el instalador, ya que lo hayamos encontrado le damos doble clic sobre el.



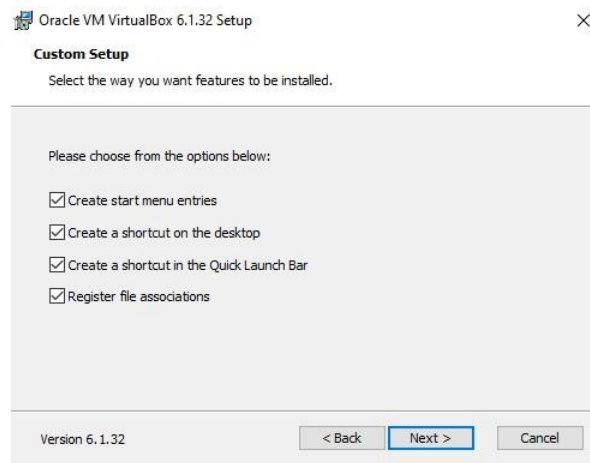
**Paso 4.** El instalador de VirtualBox se abrirá una nueva ventana de bienvenida. Le damos clic en la opción "Next".



**Paso 5.** En esta pantalla de selección de características, podemos elegir los componentes que deseamos instalar. Pero en nuestro caso dejamos las opciones predeterminadas y le damos clic en "Next".



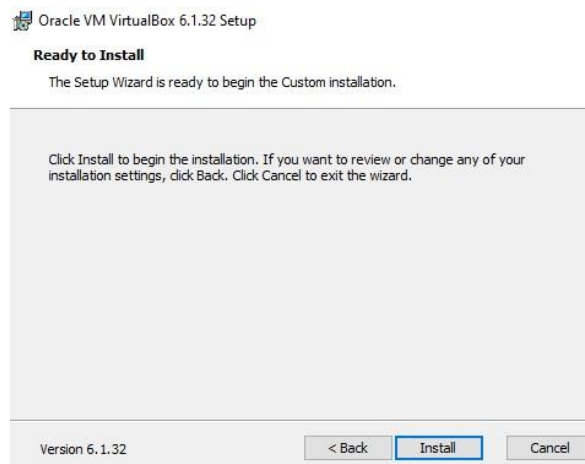
**Paso 6.** Nos aparecerá la siguiente ventana en este caso lo vamos a dejar como predeterminado y le damos clic en la opción “Next”.



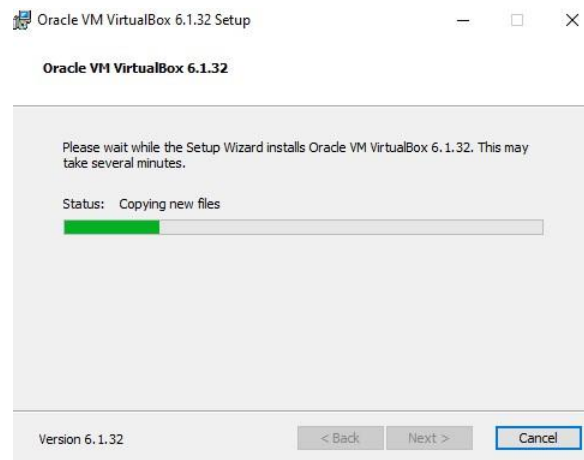
**Paso 7.** Después aparecerá una nueva ventana donde nos estará mostrando una advertencia sobre la red de interfaz le damos clic en la opción “YES” para poder continuar con la instalación.



**Paso 8.** En esta ventana nos dira que verifiquemos el procedimiento anterior si deseamos descartar algunas opciones en este caso le damos clic en “INSTALL” para comenzar con la instalación.



**Paso 9.** Nos aparecerá la ventana de instalación esperaremos el proceso hasta que termine.



**Paso 10.** Cuando se complete la instalación, veremos una pantalla de finalización. Nos aseguramos de que la casilla "Iniciar Oracle VM VirtualBox después de la instalación" esté marcada si deseamos abrir VirtualBox inmediatamente. Luego, le damos clic en "Finalizar" para salir del instalador.



**Paso 11.** Una vez finalizado la instalación nos aparecerá otra ventana donde nos pedirá que de nuevo si deseamos instalar el software en el dispositivo le damos clic en instalar



**Paso 12.** Después de la instalación, abrimos VirtualBox desde el menú Inicio o desde el acceso directo en el escritorio.



**Paso 13.** Podemos observar que la aplicación se agregó a nuestro escritorio.

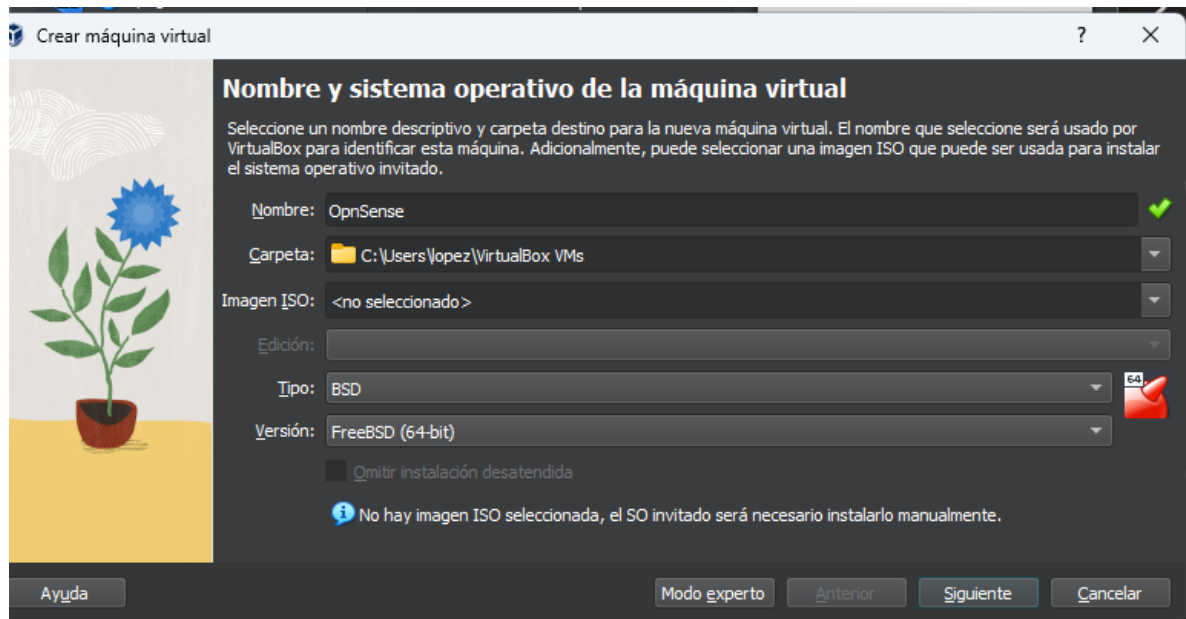




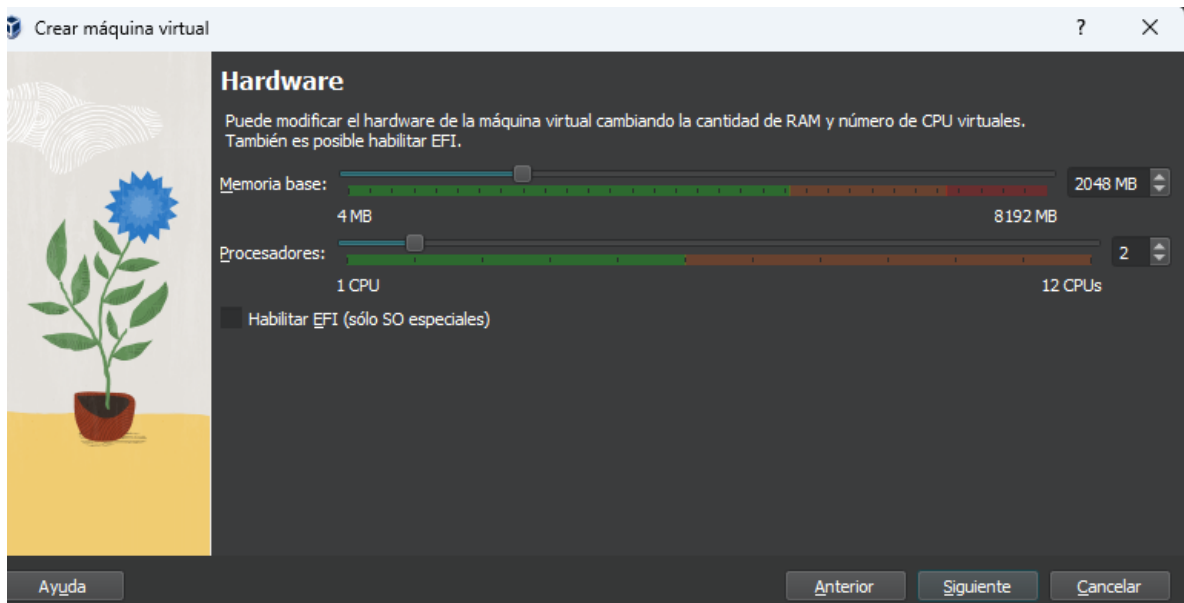
## 2. INSTALAR OPNSENSE O PFSENSE EN UNA MÁQUINA VIRTUAL Y CONFIGURAR UN FIREWALL.

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

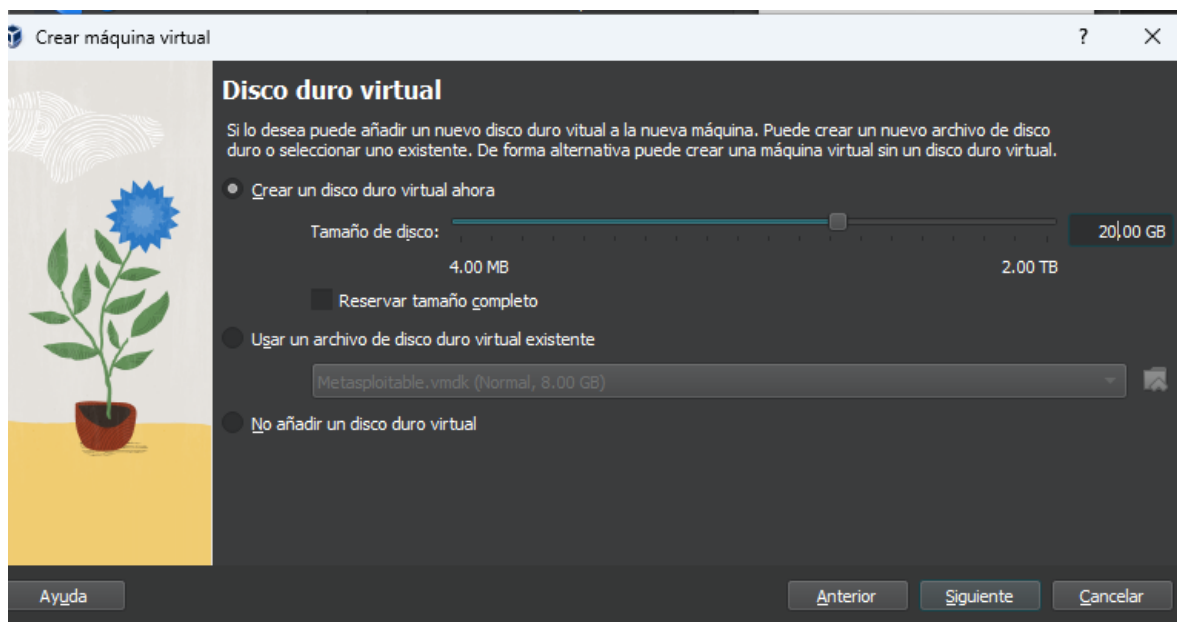
**Paso 1.** Creamos una nueva máquina virtual con el nombre de OPNSENSE en tipo seleccionamos BSD y en versión seleccionamos FreeBSD(64-bit) una vez seleccionado todo proseguimos a dar clic en siguiente.



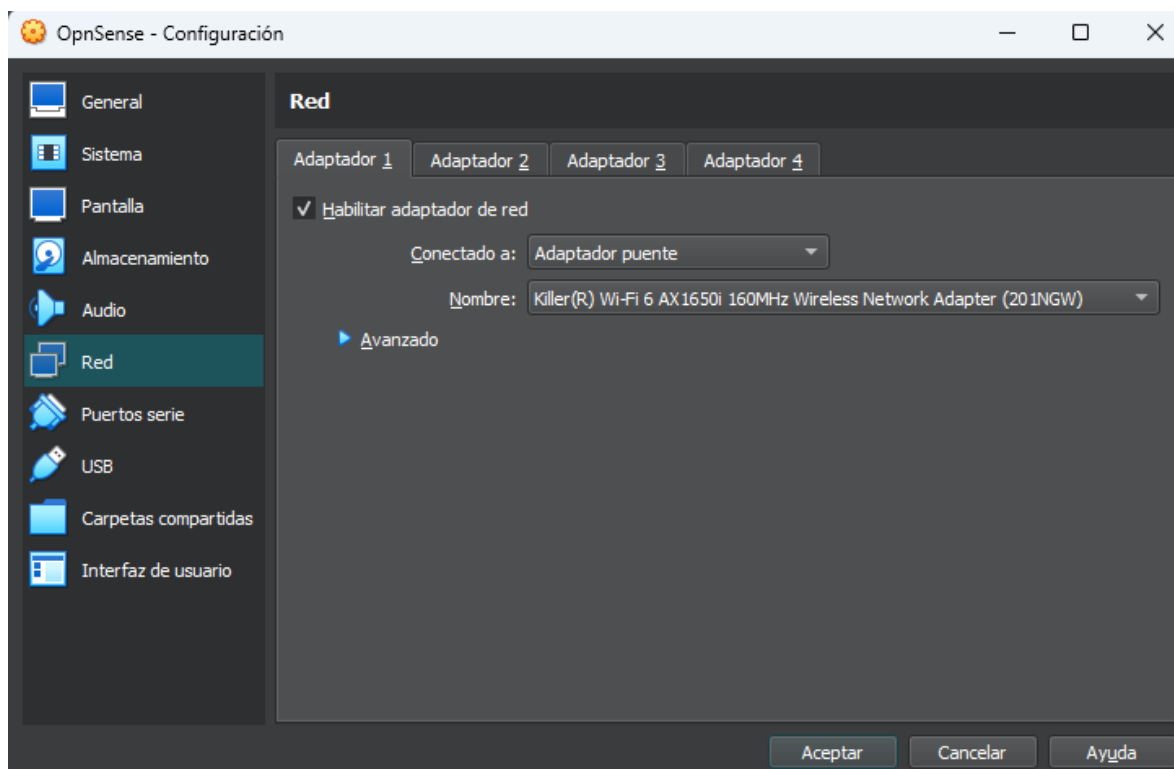
**Paso 2.** Nos aparecerá una nueva ventana donde le asignaremos la cantidad de memoria que vayamos a ocupar en nuestra máquina, hay que tomar en cuenta que no podemos asignarle toda la franja color verde ya que nuestro computadora física también está cargando un sistema operativo, le asignamos 2048 mb de memoria y en procesador le asignamos 2, proseguimos a darle clic en siguiente.



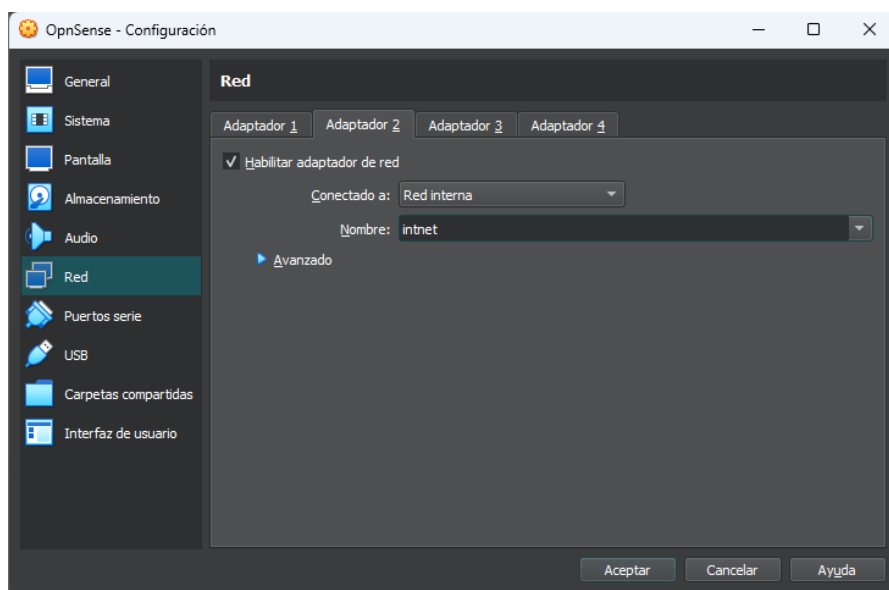
**Paso 3.** Después nos aparecerá una nueva ventana donde nos pide que agreguemos el tamaño de almacenamiento para el sistema operativo a ejecutar en nuestro caso le asignamos 20 gb de almacenamiento, le damos clic en siguiente.



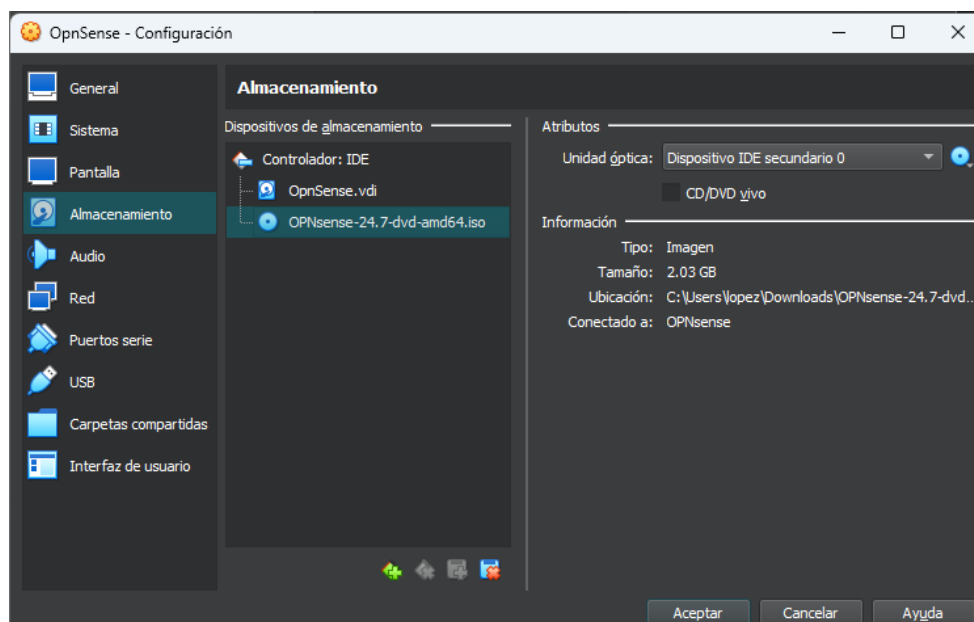
**Paso 4.** Una vez terminado de crear nuestra máquina virtual nos vamos a configurar lo que sería el adaptador de red a ocupar al igual que el ISO, para ello nos dirigimos en el engranaje que aparece en la parte superior, nos dirigimos en el apartado que dice red, en adaptador 1 seleccionamos adaptador puente.



**Paso 5.** En adaptador 2 seleccionamos red interna.



**Paso 6.** Una vez terminado de configurar nuestro adaptador de red nos dirigimos en el apartado que dice almacenamiento, cargamos nuestro ISO y le damos clic en aceptar.



## 2.2 CONFIGURACIÓN DE INTERFACES

**Paso 7.** Corremos nuestra máquina virtual nos aparecerá la interfaz de OPNSENSE esperamos a que termine de ejecutarse, cuando finalice la carga del sistema de OPNSENSE nos pedirá que ingresemos un usuario(login) y una contraseña(password), nos aparecerá

```
*** OPNsense.localdomain: OPNsense 24.7 ***  
LAN (em0)      -> v4: 192.168.1.1/24  
WAN (em1)      ->
```

**Paso 8.** Nos aparecerá un enlistado de opciones para configurar en nuestro caso seleccionamos el numero para configurar la interfaz de red.

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

**Paso 9.** Nos aparecerá una pregunta si queremos configurar los LAGGs ahora en nuestro caso pondremos que no y proseguimos a darle enter.

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

**Paso 10.** Después nos aparecerá un opción donde nos pedirá que ingresemos la interfaz de la WAN nosotros le asignaremos em0 le damos enter.

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

**Paso 11.** Ahora nos pedirá que ingresemos la interfaz de red para nuestra red LAN, ingresamos em1 y proseguimos a darle enter.

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

**Paso 12.** Nos mostrará las configuraciones que se realizaron a las interfaces.

```
The interfaces will be assigned as follows:  
WAN  -> em0  
LAN   -> em1
```

**Paso 13.** Aquí vemos que ya tenemos unas direcciones ips para la LAN Y WAN, pero proseguiremos a configurarlos.

```
LAN (em1)      -> v4: 192.168.1.1/24  
WAN (em0)      -> v4/DHCP4: 192.168.0.126/24
```

**Paso 14.** Para realizar la configuración ingresaremos el número 2 y daremos enter

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

**Paso 15.** En este apartado nos pedirá que seleccionemos una de las opciones a configurar.

```
Available interfaces:  
  
1 - LAN (em1 - static, track6)  
2 - WAN (em0 - dhcp, dhcp6)
```

**Paso 16.** Ingresamos el número 1y le daremos enter, nos pedirá si queremos configurar la dirección de la interfaz LAN para el DHCP, ingresaremos que no, proseguimos a dar enter.

```
Enter the number of the interface to configure: 1  
Configure IPv4 address LAN interface via DHCP? [y/N] N
```

**Paso 17.** A continuación, se nos pedirá que ingresemos la dirección IP para la interfaz LAN. Ingresamos la IP deseada y procedemos con Enter.

```
Enter the new LAN IPv4 address. Press <ENTER> for none:  
> 172.16.4.1
```

**Paso 18.** Luego, ingresamos la máscara de subred en formato, 24 para una máscara 255.255.255.0 y presionamos Enter.

```
Enter the new LAN IPv4 subnet bit count (1 to 32):  
> 24
```

**Paso 19.** Nos pedirá si queremos configurar el IPv6 de la interfaz LAN, le pondremos que no y proseguiremos a dar enter.

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

**Paso 20.** De igual en esta configuración escribiremos que no.

```
Configure IPv6 address LAN interface via DHCP6? [y/N] n
```

**Paso 21.** Nos pedirá que si queremos habilitar el servidor DHCP en LAN, escribiremos que sí y proseguiremos a dar enter.

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

**Paso 22.** Después nos pedirá que ingresemos el rango de donde va a empezar nuestra dirección ip, Ingresaremos que queremos del 172.16.4.5 y daremos enter.

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

**Paso 23.** Ahora nos pedirá que ingresemos hasta donde queremos la dirección ip ingresaremos que la última dirección ip sea 172.16.4.200 y daremos enter se empezara a reiniciar.

```
Enter the start address of the IPv4 client address range: 172.16.4.5  
Enter the end address of the IPv4 client address range: 172.16.4.200
```

**Paso 24.** Una vez terminado el reinicio nos aparecerá la siguiente dirección donde podremos ingresar a la interfaz del OPNsense

`https://172.16.4.1`

**Paso 25.** Nos dirigimos a nuestra máquina virtual donde tenemos el sistema operativo 10, lo ejecutamos y en la terminal y escribiremos ipconfig para ver que nuestra maquina tenga la puerta de enlace de OPNsense y efectivamente tiene su dirección IP por lo cual podremos ingresar sin problemas al la interfaz de opnsense desde el navegador.

```
Microsoft Windows [Versión 10.0.19042.631]
(c) 2020 Microsoft Corporation. Todos los derechos reservados.

C:\Users\saul>ipconfig

Configuración IP de Windows

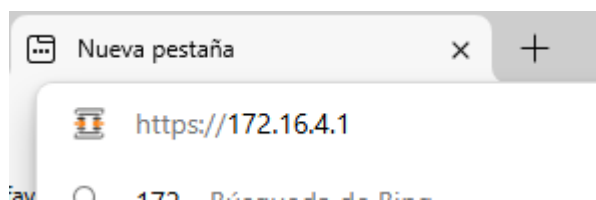
Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . : localdomain
    Vínculo: dirección IPv6 local. . . : fe80::9985:2819:eb56:ca6b%6
    Dirección IPv4. . . . . : 172.16.4.5
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 172.16.4.1

C:\Users\saul>
```



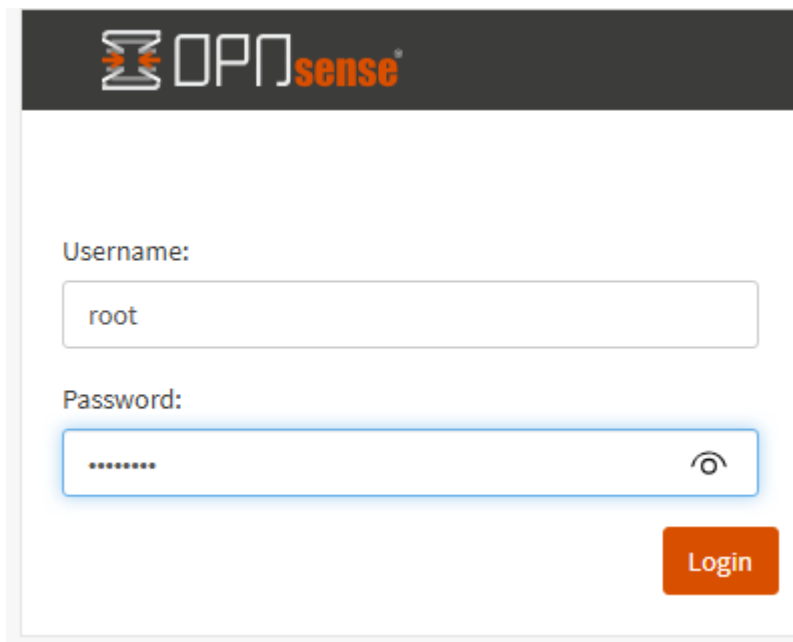
**Paso 26.** En el navegador que tengamos instalados escribimos la siguiente url de la dirección Ip de nuestro opnsense.



**Paso 27.** Nos aparecerá la siguiente interfaz donde nos pedirá que ingresemos el nombre de usuario al igual que el password.

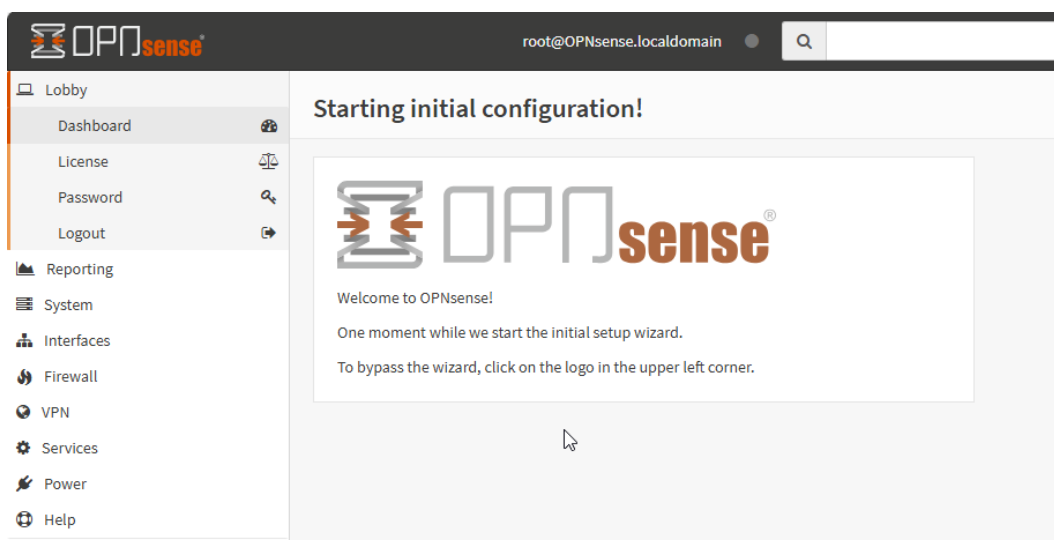
A screenshot of the OPNsense login interface. At the top, there is a dark header with the OPNsense logo. Below the header, the text 'Username:' is followed by a text input field. Below that, the text 'Password:' is followed by another text input field. To the right of the password field is an orange 'Login' button. At the bottom of the page, there is a footer that reads 'OPNsense (c) 2014-2024 Deciso B.V.'.

**Paso 28.** Ingresamos en usuario root y en password Ingresamos opnsense como podemos notar el usuario y la contraseña ingresados son los mismos que ingresábamos a nuestro opnsense.



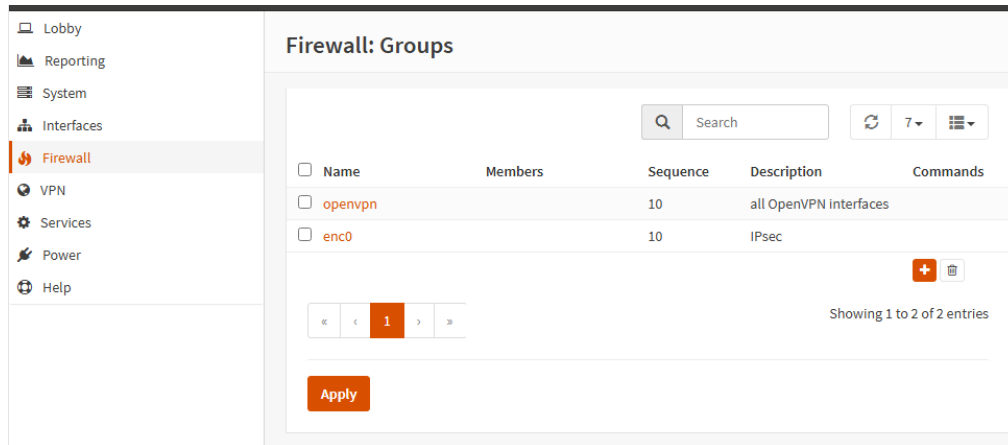
The image shows the OPNsense login interface. At the top is the OPNsense logo. Below it, there are two input fields: 'Username:' with 'root' entered, and 'Password:' with a masked password '.....'. To the right of the password field is an eye icon for toggling visibility. A blue 'Login' button is positioned to the right of the password field.

**Paso 29.** Una vez estando a dentro podremos ver una interfaz de nuestro opnsense donde podemos hacer diversas configuraciones.



## 2.3 CONFIGURACIÓN DE REGLAS DE FIREWALL

**Paso 30.** Para aplicar lo que serían las reglas de firewall nos vamos en el apartado donde dice Firewall y nos aparecerá la siguiente ventana daremos clic en el botón anaranjado con el signo de más, para agregar una regla al firewall.

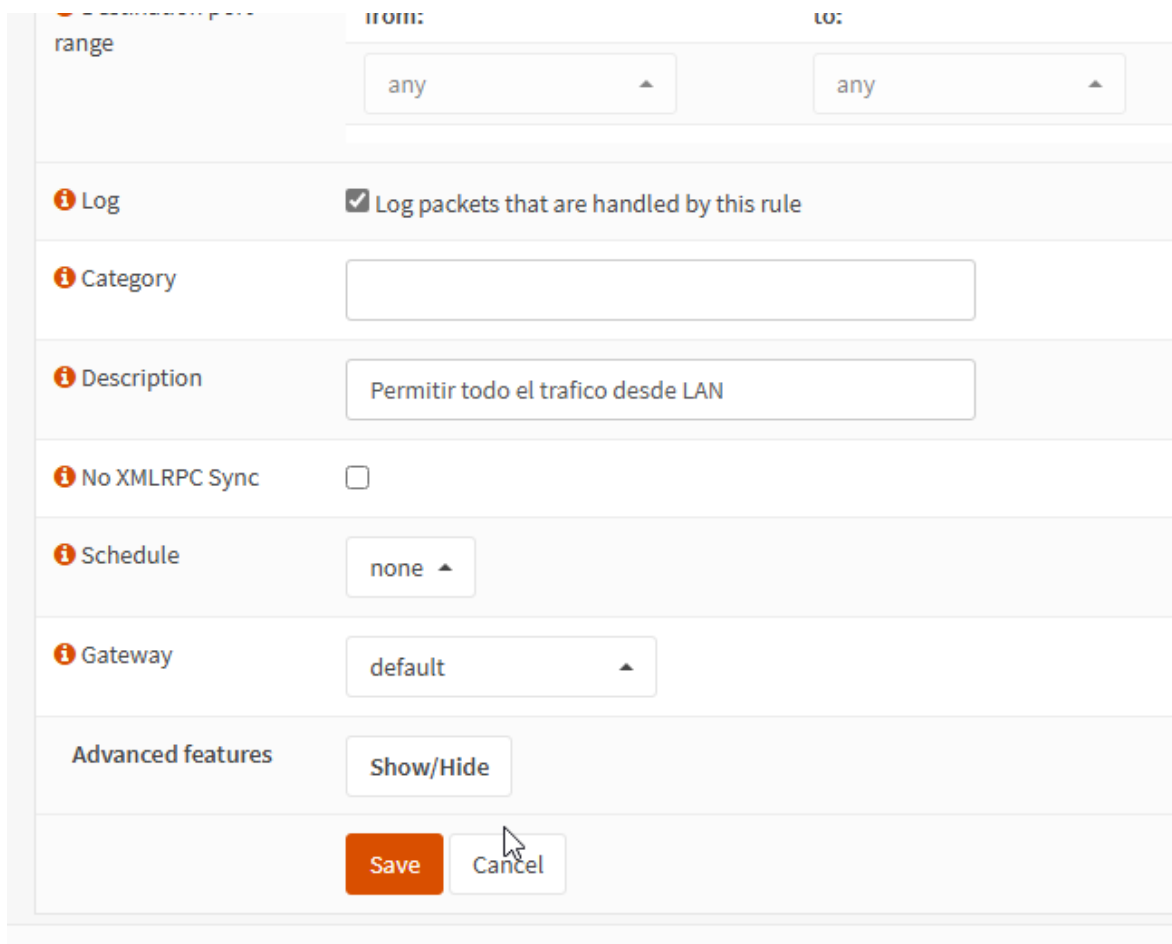


**Paso 31.** Después nos aparecerá la siguiente ventana donde podremos crear una regla para nuestra red LAN, A continuación se muestra la configuración que se llevó a cabo.

The screenshot shows the 'Firewall: Rules: LAN' configuration window. The title is 'Firewall: Rules: LAN'. Below the title is a section 'Edit Firewall rule'. The configuration fields are as follows:

- Action:** Pass (dropdown)
- Disabled:** ☐ Disable this rule
- Quick:** ☒ Apply the action immediately on match.
- Interface:** LAN (dropdown)
- Direction:** in (dropdown)
- TCP/IP Version:** IPv4 (dropdown)
- Protocol:** any (dropdown)
- Source / Invert:** ☐ Use this option to invert the sense of the match

**Paso 32.** Terminando de configurar cada una de las opciones daremos clic en el botón que dice save.



range

from: any to: any

**Log** ☒ Log packets that are handled by this rule

**Category**

**Description** Permitir todo el trafico desde LAN

**No XMLRPC Sync** ☐

**Schedule** none

**Gateway** default

**Advanced features** Show/Hide

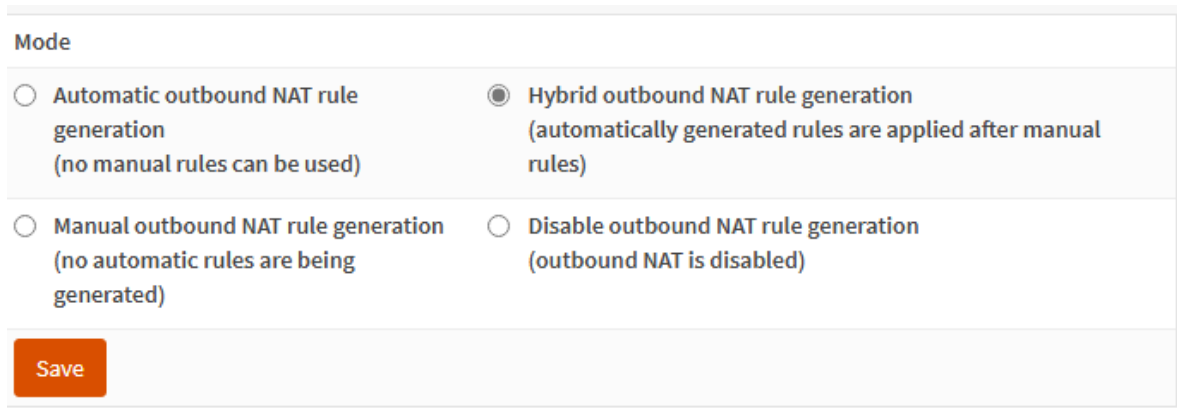
**Save** **Cancel**

**Paso 33.** Podemos ver que tenemos 3 reglas LAN configuradas para nuestro firewall.

<input type="checkbox"/>		IPv4 *	LAN net	Default allow LAN to any rule				
<input type="checkbox"/>		IPv6 *	LAN net	Default allow LAN IPv6 to any rule				
<input type="checkbox"/>		IPv4 *	LAN net	Permitir todo el trafico desde LAN				

## 2.4 CONFIGURAR EL NAT

**Paso 34.** Para la configuración de nuestro NAT en el apartado de modo seleccionaremos el que dice Hybrid outbound rule generation automatically generated rules.

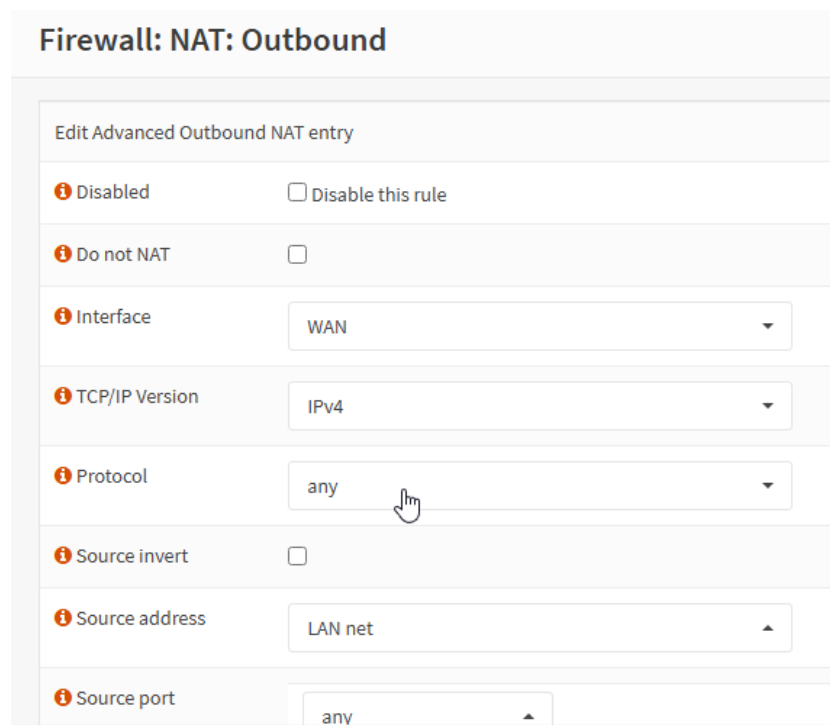


The screenshot shows a configuration window titled "Mode" with four radio button options. The "Hybrid outbound NAT rule generation" option is selected. Below the options is an orange "Save" button.

Mode	
<input type="radio"/> Automatic outbound NAT rule generation (no manual rules can be used)	<input checked="" type="radio"/> Hybrid outbound NAT rule generation (automatically generated rules are applied after manual rules)
<input type="radio"/> Manual outbound NAT rule generation (no automatic rules are being generated)	<input type="radio"/> Disable outbound NAT rule generation (outbound NAT is disabled)

Save

**Paso 35.** Nos dirigimos en la opción que dice Outbound de igual forma configuraremos cada una de los apartados que nos aparecen.



The screenshot shows the "Firewall: NAT: Outbound" configuration window. It contains several settings for an "Advanced Outbound NAT entry".

Firewall: NAT: Outbound	
Edit Advanced Outbound NAT entry	
<b>Disabled</b>	<input type="checkbox"/> Disable this rule
<b>Do not NAT</b>	<input type="checkbox"/>
<b>Interface</b>	WAN
<b>TCP/IP Version</b>	IPv4
<b>Protocol</b>	any
<b>Source invert</b>	<input type="checkbox"/>
<b>Source address</b>	LAN net
<b>Source port</b>	any

**Paso 36.** Igualmente seguimos configurando y al finalizar la configuración daremos clic en el botón de Save.

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

**Paso 37.** Como podemos observar hemos agregado nuestro Nat de una forma correcta.




#### Manual rules

<input type="checkbox"/>	Interface	Static Port	Description	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	WAN	YES	NAT saliente para LAN a internet	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## 2.5 CONFIGURACIÓN DE DHCP

**Paso 39.** Ahora proseguiremos a configurar nuestro DHCP para este caso la configuración aplicaría para nuestra red LAN. Nos aparecerá una serie de opciones a configurar donde va incluido la dirección IP, mascara de subred al igual que el rango de dirección ip.

**Services: ISC DHCPv4: [LAN]**



[full help](#)

<b>Enable</b>	<input checked="" type="checkbox"/> Enable DHCP server on the LAN interface				
<b>Deny unknown clients</b>	<input type="checkbox"/>				
<b>Ignore Client UIDs</b>	<input type="checkbox"/>				
<b>Subnet</b>	172.16.4.0				
<b>Subnet mask</b>	255.255.255.0				
<b>Available range</b>	172.16.4.1 - 172.16.4.254				
<b>Range</b>	<table><thead><tr><th>from</th><th>to</th></tr></thead><tbody><tr><td><input type="text" value="172.16.4.10"/></td><td><input type="text" value="172.16.4.245"/></td></tr></tbody></table>	from	to	<input type="text" value="172.16.4.10"/>	<input type="text" value="172.16.4.245"/>
from	to				
<input type="text" value="172.16.4.10"/>	<input type="text" value="172.16.4.245"/>				

## 2.6 CONFIGURACIÓN DE DNS.

**Paso 40.** Ahora configuraremos nuestro DNS en esta ventana que se muestra una serie de configuraciones, nosotros seleccionamos la mayoría para no tener problemas después

Services: Unbound DNS: General

[advanced mode](#) [full help](#)

Enable Unbound	<input checked="" type="checkbox"/>
Listen Port	53
Network Interfaces	LAN
<a href="#">Clear All</a> <a href="#">Select All</a>	
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"/>

**Paso 41.** De igual forma seleccionamos las casillas y al finalizar damos clic en el botón que dice 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

Apply



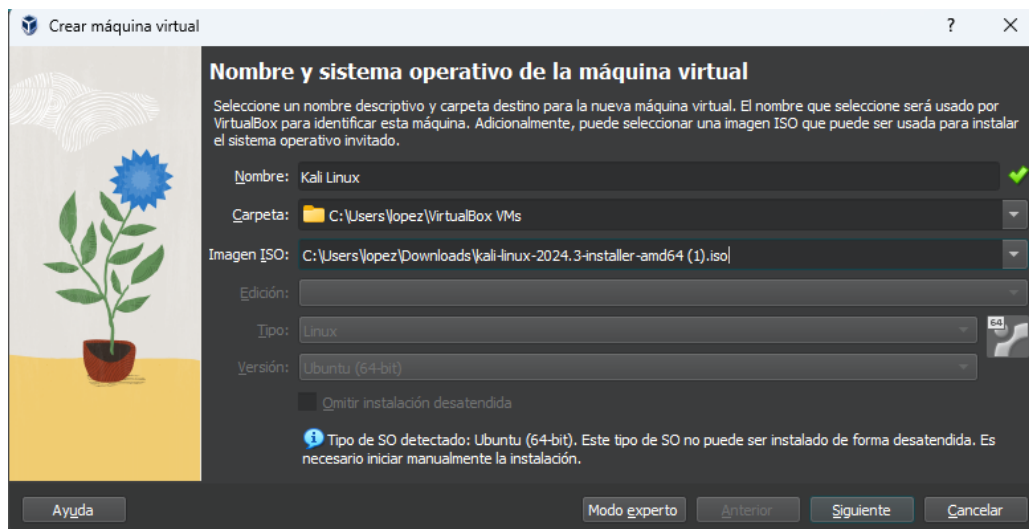
## 2.7 ASINACIÓN DE DIRECCION IP STATIC AL FIREWALL

**Paso 42.** En este apartado configuraremos lo que sería la interfaz del firewall como vemos tenemos una dirección inicial que es 172.16.4.1 con una máscara de subred 24.

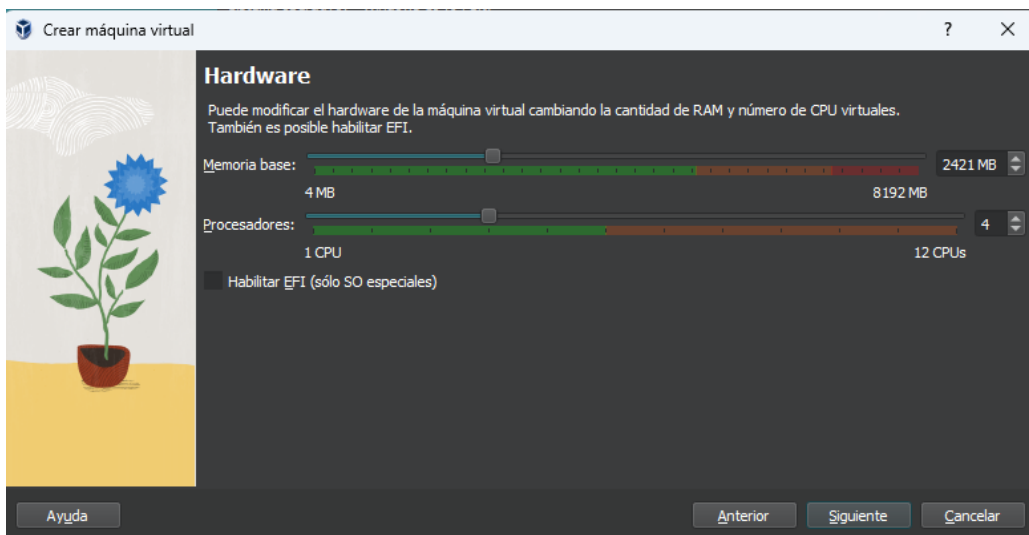
Static IPv4 configuration	
 IPv4 address	<div>172.16.4.1</div> <div>24 ▲</div>
 IPv4 gateway rules	<div>Disabled ▼</div>

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

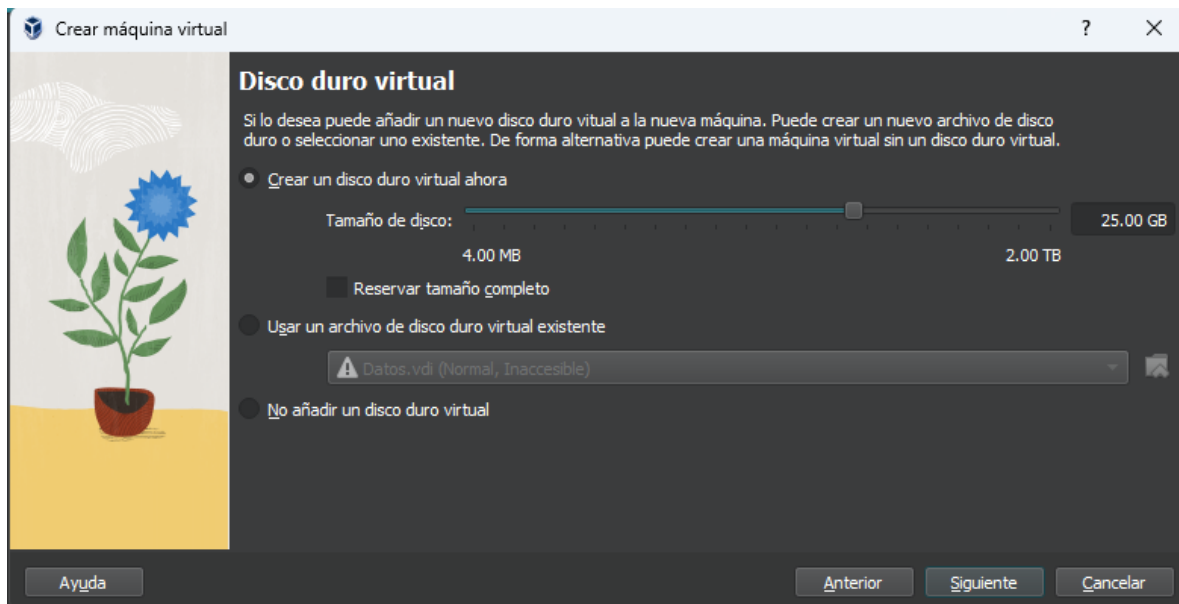
**Paso 1.** Creamos nuestra máquina virtual, donde ponemos el nombre de nuestra máquina, el cual es kali Linux, después seleccionamos el ISO, en tipo seleccionamos Linux y en versión seleccionamos Ubuntu (64-bit), le damos clic en el botón de siguiente.



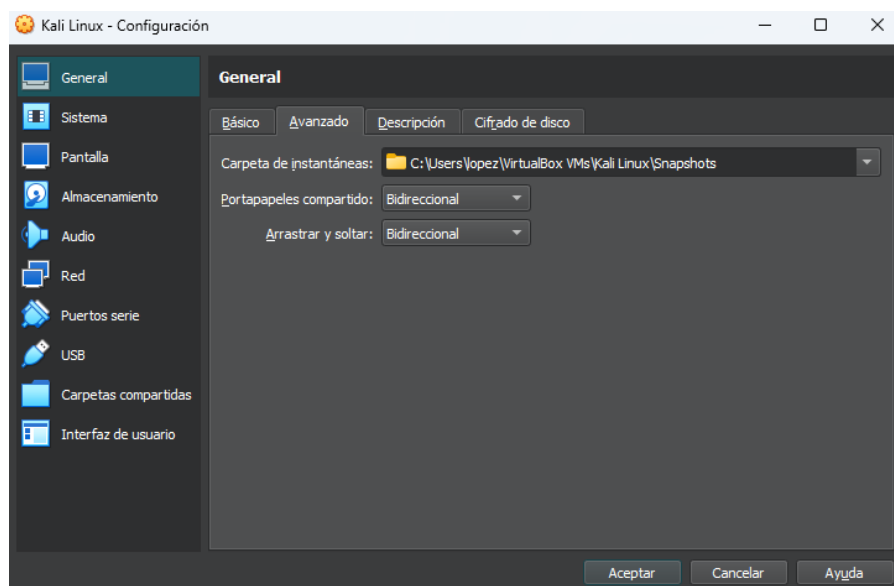
**Paso 2.** Agregamos la capacidad de nuestra memoria a nuestra máquina virtual al igual que la capacidad del procesador que ocuparemos, le damos clic en el botón de siguiente.



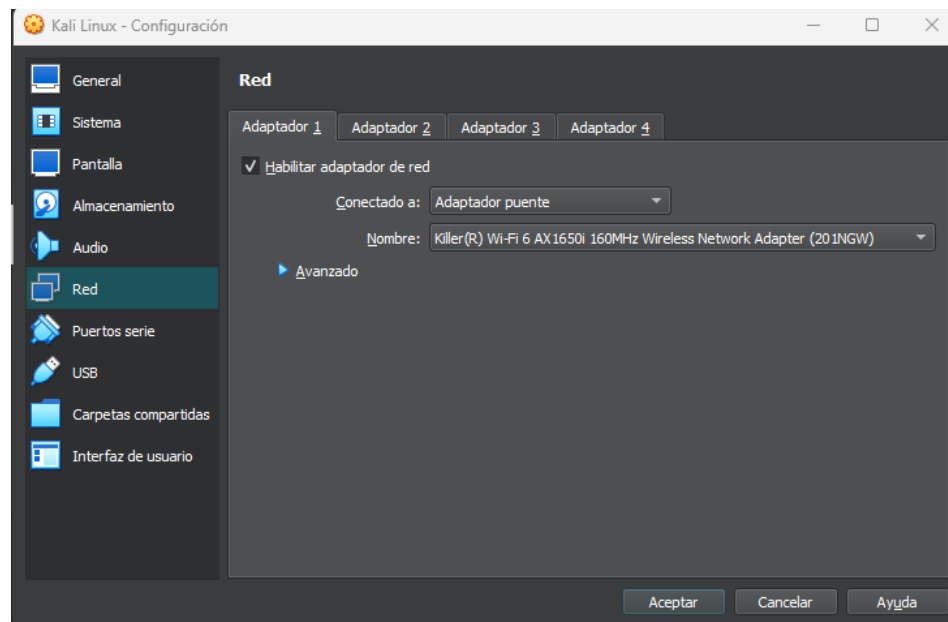
**Paso 3.** Asignamos el tamaño de nuestra máquina virtual que ocuparemos, le damos clic en el botón de siguiente.



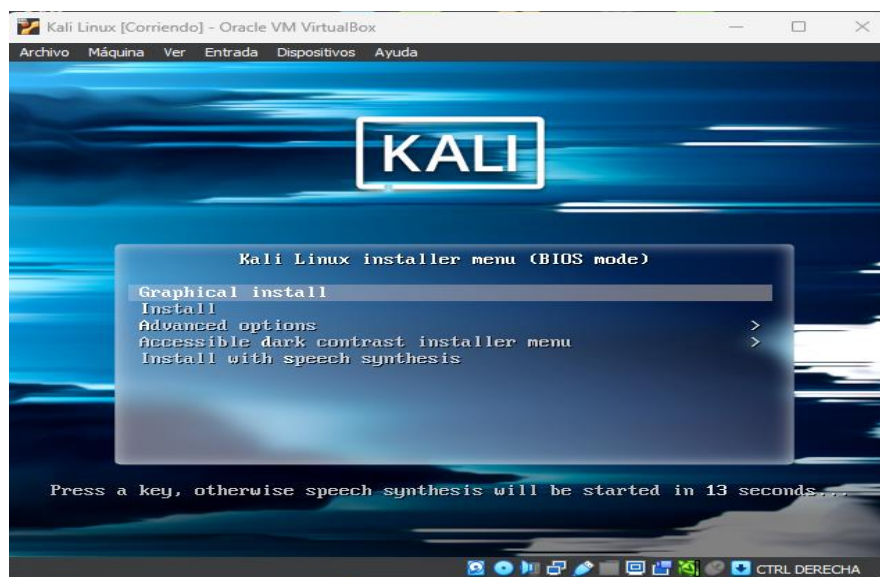
**Paso 4.** Nos vamos a la parte de configuración en el apartado de general en las opciones de portapapeles compartidos y arrastrar y soltar seleccionamos la opción de Bidireccional en ambos.



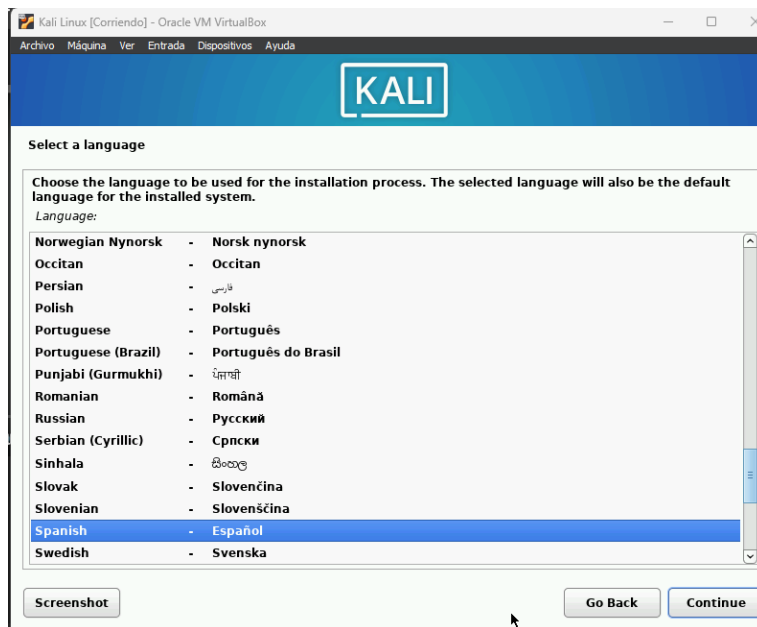
**Paso 5.** Después de haber realizado lo anterior nos redirigimos en el apartado de red donde en el adaptador uno en la opción de conectado a seleccionamos adaptador puente para que nuestra máquina virtual se le asigne una dirección ip, después le damos clic en el botón de aceptar y proseguimos a iniciar nuestra máquina virtual.



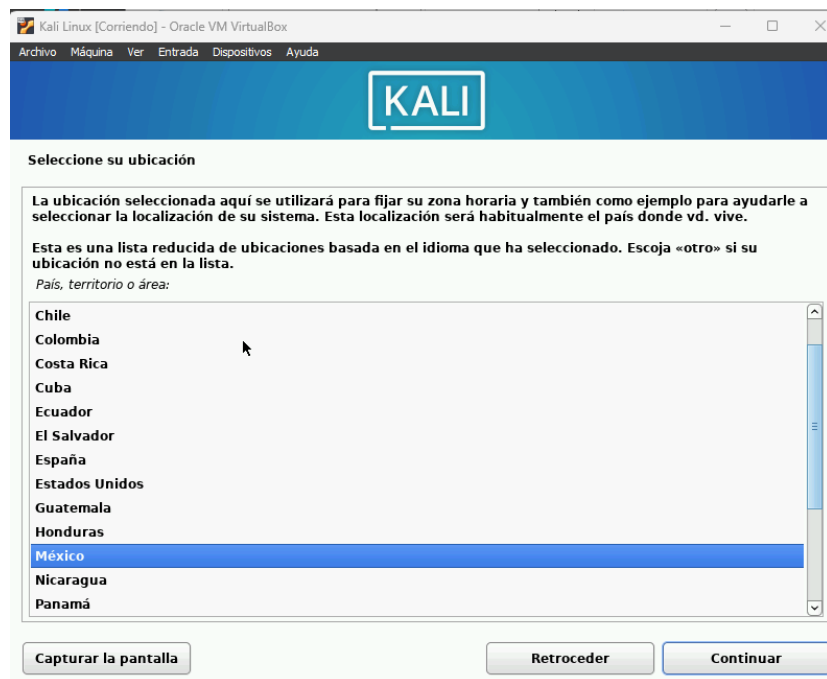
**Paso 6.** Nos aparecerá la interfaz de Kali linux donde seleccionamos la primera opción Graphical Install.



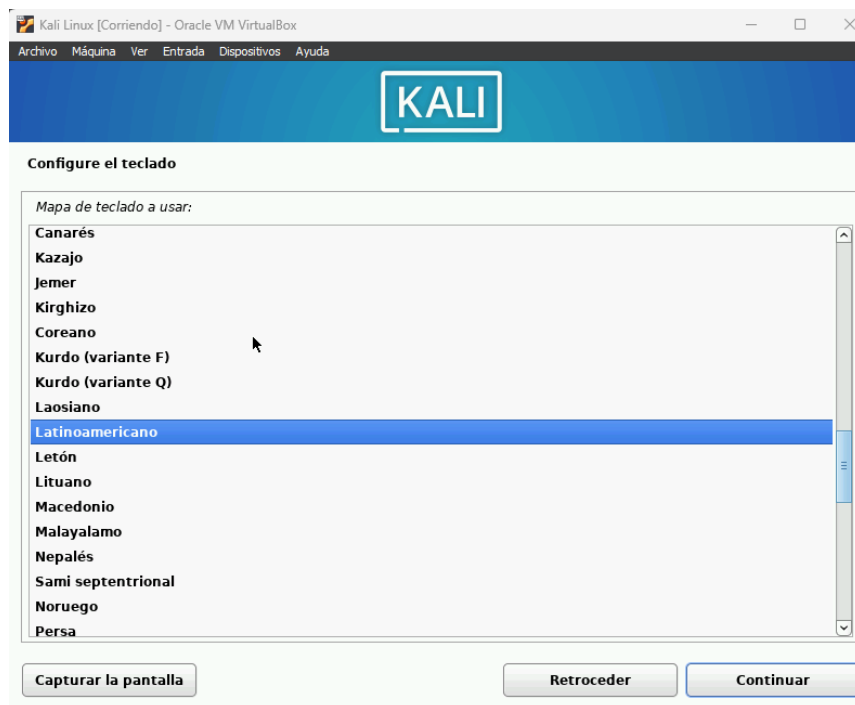
**Paso 7.** En este apartado seleccionamos nuestro idioma, después le damos clic en el botón de continue.



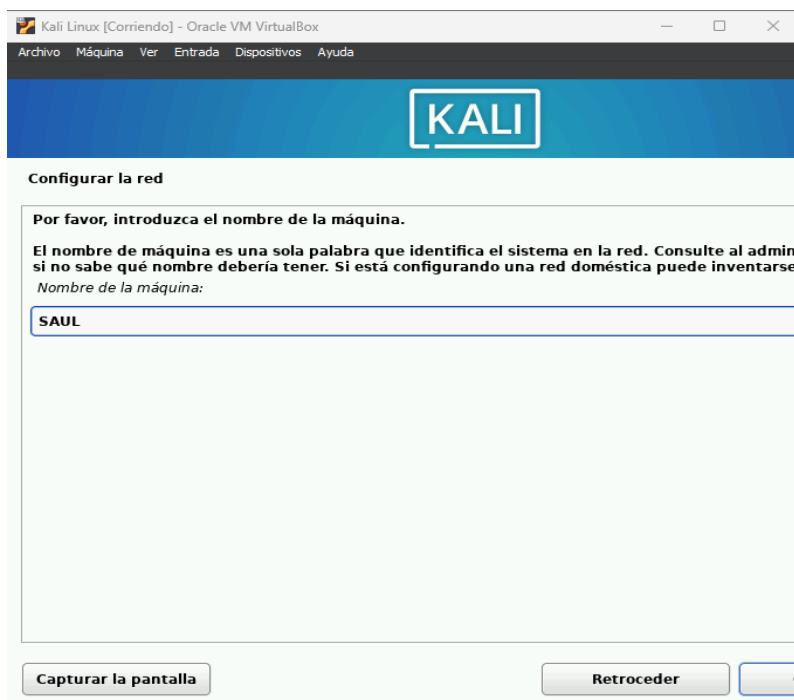
**Paso 8.** Después proseguimos seleccionar nuestro país de origen en este caso seleccionamos México y le damos clic en el botón de continuar.



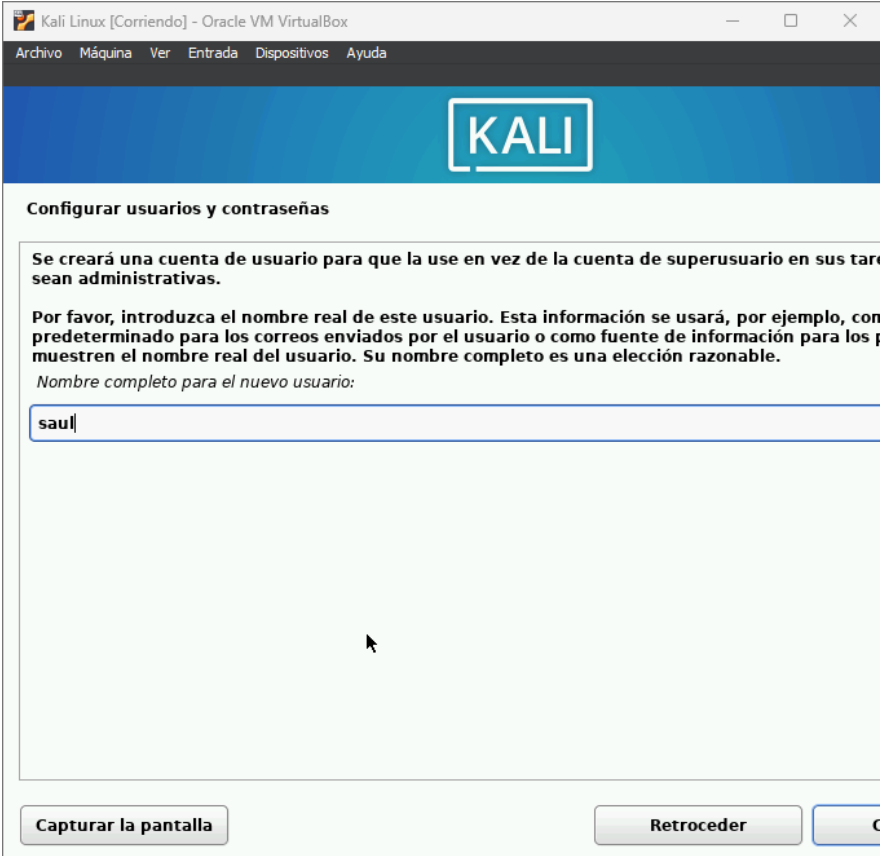
**Paso 9.** Configuramos nuestro teclado seleccionando la opción de latinoamericano y le damos clic en el botón de continuar.



**Paso 10.** En esta ventana le pusimos un nombre a nuestra maquina el cual le fue SAUL y le damos clic en el botón de continuar.



**Paso 11.** En este apartado ponemos un nombre de usuario a nuestra máquina, como nombre le pusimos saul y proseguimos a darle clic al botón de continuar.



The screenshot shows a window titled "Kali Linux [Corriendo] - Oracle VM VirtualBox". The window contains a menu bar with "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". Below the menu is a blue header with the "KALI" logo. The main content area is titled "Configurar usuarios y contraseñas". It contains the following text: "Se creará una cuenta de usuario para que la use en vez de la cuenta de superusuario en sus tareas administrativas." followed by "Por favor, introduzca el nombre real de este usuario. Esta información se usará, por ejemplo, como predeterminado para los correos enviados por el usuario o como fuente de información para los paquetes. Muestren el nombre real del usuario. Su nombre completo es una elección razonable." and "Nombre completo para el nuevo usuario:". Below this is a text input field containing "saul". At the bottom of the window are three buttons: "Capturar la pantalla", "Retroceder", and a partially visible "Continuar" button.

Kali Linux [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

**KALI**

**Configurar usuarios y contraseñas**

Se creará una cuenta de usuario para que la use en vez de la cuenta de superusuario en sus tareas administrativas.

Por favor, introduzca el nombre real de este usuario. Esta información se usará, por ejemplo, como predeterminado para los correos enviados por el usuario o como fuente de información para los paquetes. Muestren el nombre real del usuario. Su nombre completo es una elección razonable.

Nombre completo para el nuevo usuario:

saul

Capturar la pantalla Retroceder Continuar

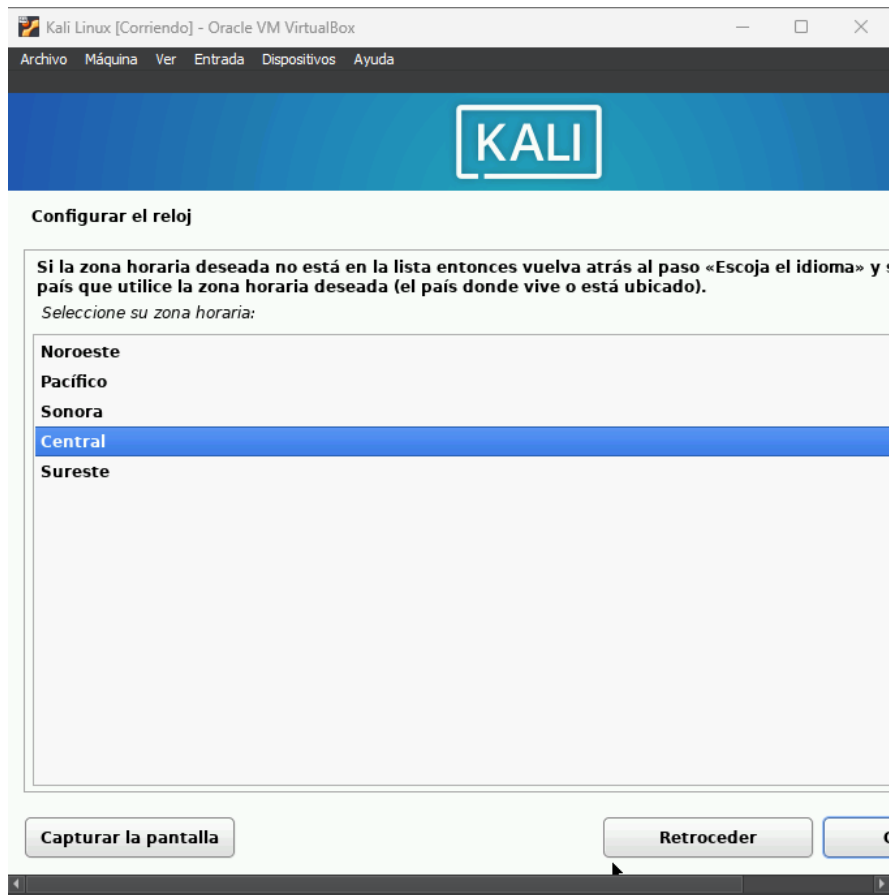
**Paso 12.** A continuación nos pedirá que agreguemos una contraseña el cual nosotros ingresaremos en la primera sección introducimos la contraseña y ya en la segunda la volvemos a ingresar para que sea valida.



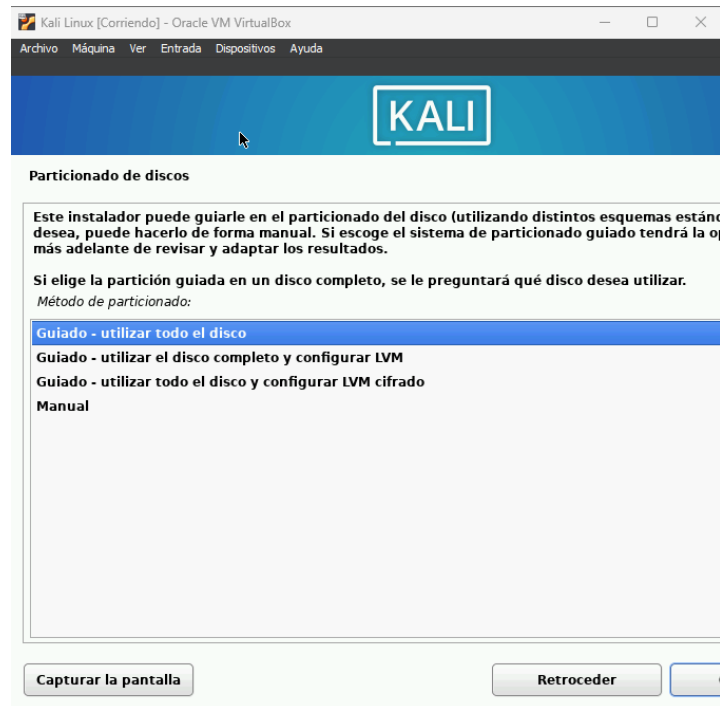
The screenshot shows a window titled "Kali Linux [Corriendo] - Oracle VM VirtualBox". Inside the window, there is a menu bar with "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". Below the menu bar is a blue header with the "KALI" logo. The main content area is titled "Configurar usuarios y contraseñas". It contains the following text: "Asegúrese de seleccionar una contraseña segura que no pueda ser adivinada." followed by "Elija una contraseña para el nuevo usuario:". Below this is a password input field filled with dots. There is a checkbox labeled "Mostrar la contraseña en claro" with a mouse cursor hovering over it. Below the checkbox, it says "Por favor, introduzca la misma contraseña de usuario de nuevo para verificar que la introdujo co" and "Vuelva a introducir la contraseña para su verificación:". This is followed by another password input field filled with dots. There is another checkbox labeled "Mostrar la contraseña en claro". At the bottom of the window, there are three buttons: "Capturar la pantalla", "Retroceder", and a partially visible "Continuar" button.



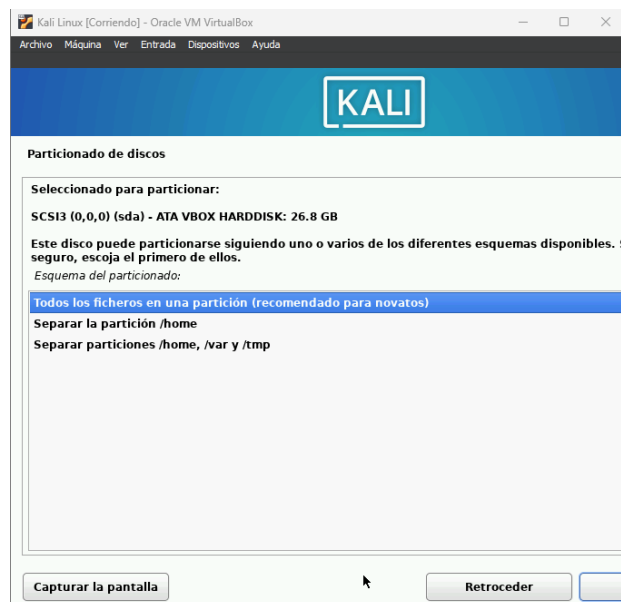
**Paso 13.** Configuramos la zona horaria de nuestra máquina de acuerdo al lugar donde nos encontramos en nuestro caso nosotros seleccionamos la opción de central y le damos clic en el botón continuar.



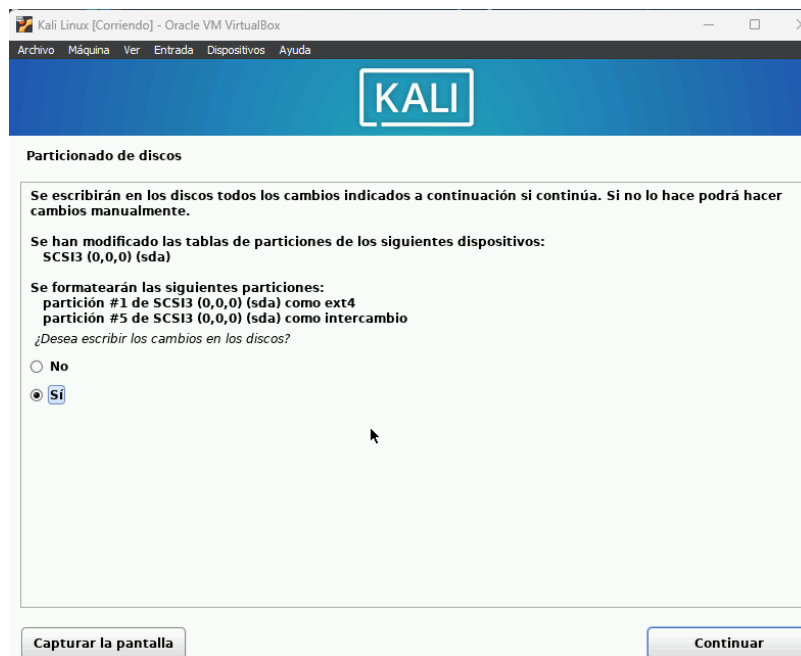
**Paso 14.** En este apartado nos pedirá que seleccionemos una opción sobre el particionamiento del disco en este caso dejamos la primera opción Guiado-utilizar todo el disco duro, le damos clic en el botón de continuar.



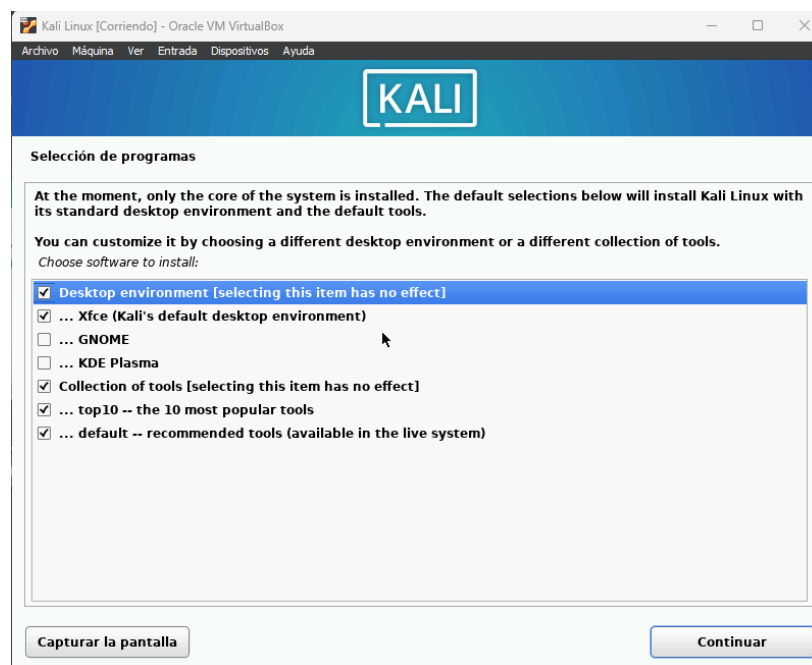
**Paso 15.** De igual forma dejamos la primera opción por default y le damos clic en el botón de continuar.



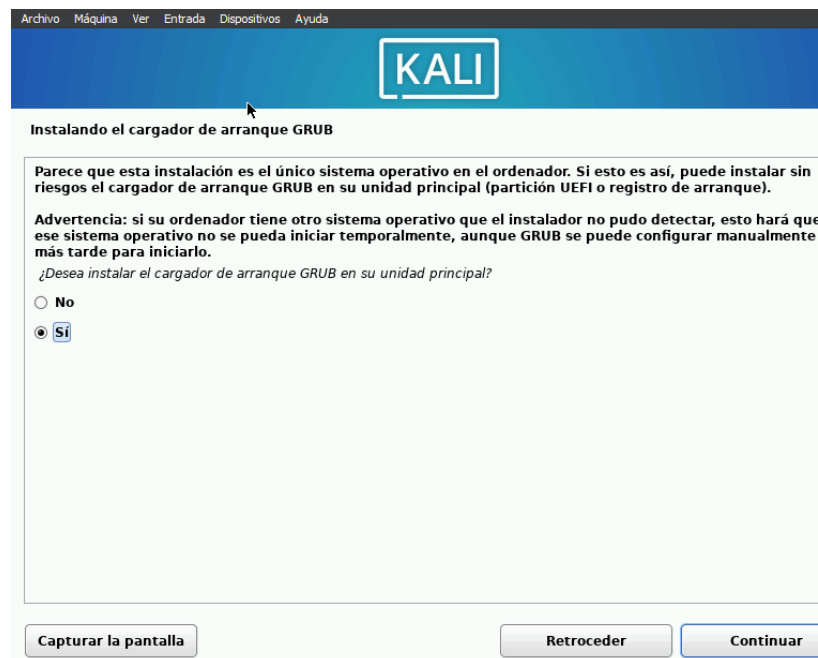
**Paso 16.** Después nos aparecerá esta ventana, donde todos los cambios realizados anteriormente serán escritos en el disco seleccionamos la opción de si y le damos clic en el botón de continuar.



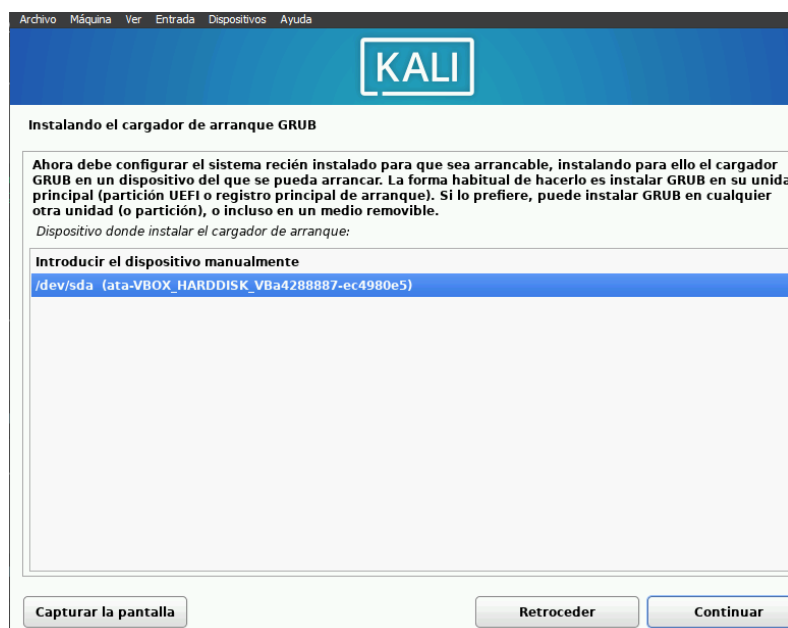
**Paso 17.** Nos aparecerá la siguiente ventana donde nos pedirá la selección del tipo de programa que queremos en este caso lo dejamos con las opciones seleccionadas y le damos clic en el botón de continuar.



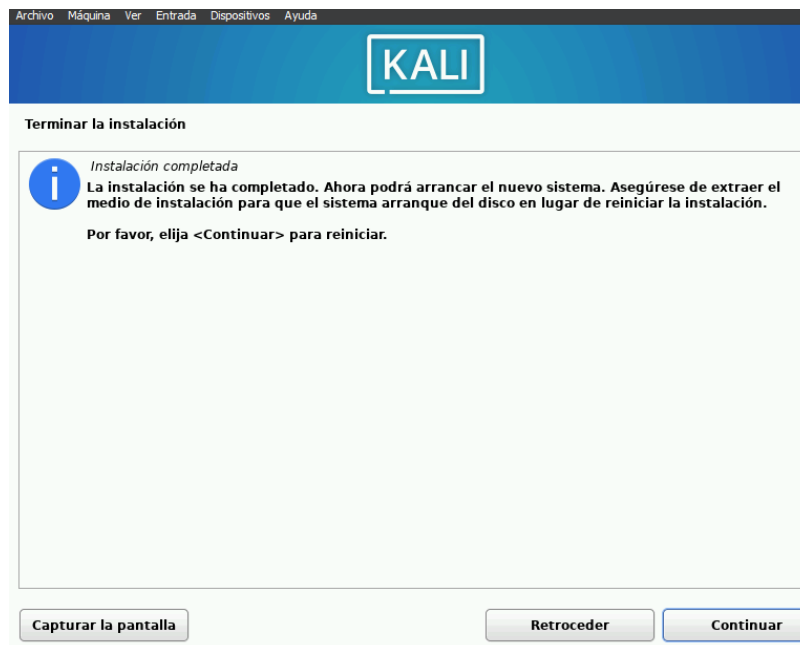
**Paso 18.** Después nos aparecerá un tipo de advertencia para el instalador del cargador de arranque de GRUB seleccionamos la opción de si, y le damos clic en el botón de continuar.



**Paso 19.** En este apartado seleccionamos la primera opción de dispositivo manualmente y le damos clic en el botón de continuar, el proceso tardará unos minutos.



**Paso 20.** Una vez terminado la espera de instalación nos mostrará el siguiente mensaje que la instalación se ha completado y que hay que reiniciar le damos clic en el botón de continuar.



**Paso 21.** Cuando termine el reinicio nos pedirá que ingresemos el nombre del usuario y la contraseña que se agregó cuando se instaló el sistema operativo, una vez ingresado el usuario y su contraseña nos mostrara la interfaz de kali linux.



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

**Paso 22.** Abrimos la terminal ingresamos el comando `sudo apt-get update`, para actualizar la lista de paquetes disponibles y sus versiones en los repositorios configurados. Esto no instala ni actualiza los paquetes, solo descarga la información más reciente sobre ellos, esperamos a que se realicen las pequeñas descargas.

```
(saul@SAUL)-[~]
$ sudo apt-get update
[sudo] contraseña para saul:
Des:1 http://kali.download/kali kali-rolling InRelease [41,5 kB]
Des:2 http://kali.download/kali kali-rolling/main amd64 Packages [20,2 MB]
Ign:2 http://kali.download/kali kali-rolling/main amd64 Packages
Des:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [48,4
MB]
Ign:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb)
Des:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [111 kB]
Des:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [27
2 kB]
Des:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [197 kB]
Des:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [8
76 kB]
Des:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages
[10,8 kB]
Des:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents
(deb) [22,8 kB]
Des:2 http://kali.download/kali kali-rolling/main amd64 Packages [20,2 MB]
Ign:2 http://kali.download/kali kali-rolling/main amd64 Packages
Des:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [48,4
MB]
Ign:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb)
Des:2 http://kali.download/kali kali-rolling/main amd64 Packages [20,2 MB]
26% [2 Packages 4.812 kB/20,2 MB 24%] 2.144 B/s 8h 16min 2s^
```

**Paso 23.** Una vez terminado lo 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`, el cual nos ayudara para instalar una serie de paquetes y dependencias de kali Linux, de igual forma esperamos a que se descarguen.

```
(saul@SAUL)-[~]
$ sudo apt-get install libpcrc3-dbg libpcrc3-dev autoconf automake libtool libpcap-dev libnet1-dev li
byaml-dev libjansson4 libcap-ng-dev libmagic-dev libjansson-dev zlib1g-dev pkg-config rustc cargo
No se ha encontrado la orden «udo», pero se puede instalar con:
sudo apt install udo
¿Quiere instalarlo? (N/y)y
sudo apt install udo
Installing:
udo
Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1145
Download size: 202 kB
Space needed: 597 kB / 9.215 MB available
Des:1 http://kali.download/kali kali-rolling/main amd64 udo amd64 6.4.1-8 [202 kB]
Descargados 202 kB en 7s (27,2 kB/s)
Seleccionando el paquete udo previamente no seleccionado.
[Leyendo la base de datos ... 85%
```

**Paso 24.** Proseguimos a instalar suricata para el motor de detección y prevención de intrusiones en la red (IDS/IPS) con el siguiente comando `sudo apt install suricata -y`, esperamos a que se descargue.

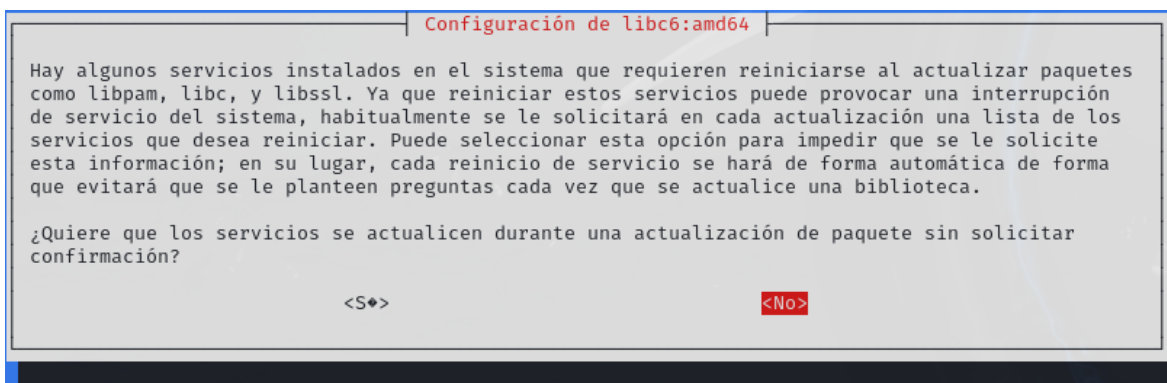
```
(saul@SAUL)-[~]
$ sudo apt install suricata -y
Installing:
suricata

Installing dependencies:
isa-support          librt-eal24          librt-log24          librt-pci24          oinkmaster
libfdt1             librt-ealdev24       librt-mbuf24         librt-rcu24          snort-rules-default
libhtp2             librt-ethdev24       librt-mempool24      librt-ring24         sse3-support
libhyperscan5       librt-hash24         librt-meter24        librt-sched24        sse4.2-support
libnetfilter-log1   librt-ip-frag24      librt-net-bond24     librt-telemetry24    suricata-update
librt-bus-pci24     librt-kvargs24       librt-net24          libxdpi

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
Des:1 http://kali.download/kali kali-rolling/main amd64 isa-support amd64 24 [14,4 kB]
Des:2 http://kali.download/kali kali-rolling/main amd64 sse3-support amd64 24 [3.536 B]
Des:4 http://kali.download/kali kali-rolling/main amd64 libhtp2 amd64 1:0.5.49-1 [72,8 kB]
Des:5 http://kali.download/kali kali-rolling/main amd64 libhyperscan5 amd64 5.4.2-2 [2.600 kB]
Des:3 http://kali.mirror.rafael.ca/kali kali-rolling/main amd64 sse4.2-support amd64 24 [3.496 B]
Des:15 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main amd64 librt-meter24 amd64 23.11.2-2 [15,9 kB]
Des:21 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main amd64 librt-rcu24 amd64 23.11.2-2 [20,3 kB]
Des:23 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main amd64 librt-ip-frag24 amd64 23.11.2-2 [31,6 kB]
Des:6 http://http.kali.org/kali kali-rolling/main amd64 libnetfilter-log1 amd64 1.0.2-4+b1 [13,3 kB]
Des:7 http://http.kali.org/kali kali-rolling/main amd64 libfdt1 amd64 1.7.0-2+b1 [19,2 kB]
Des:8 http://kali.download/kali kali-rolling/main amd64 librt-log24 amd64 23.11.2-2 [18,8 kB]
Des:9 http://kali.download/kali kali-rolling/main amd64 librt-kvargs24 amd64 23.11.2-2 [16,0 kB]
Des:10 http://kali.download/kali kali-rolling/main amd64 librt-telemetry24 amd64 23.11.2-2 [24,7 kB]
Des:11 http://kali.download/kali kali-rolling/main amd64 librt-eal24 amd64 23.11.2-2 [153 kB]
```

**Paso 25.** Una vez terminado la instalación anterior nos aparecerá una ventana que nos muestra alguno de los servicios instalados en el sistema que requiere ser reiniciado para que se actualicen, le damos clic en el botón de sí.



**Paso 26.** Se empezara a actualizar todos los servicios anteriormente mostrados 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) ...
Processing triggers for libc-bin (2.40-3) ...
Processing triggers for systemd (256.2-1) ...
Processing triggers for man-db (2.12.1-2) ...
Processing triggers for sgml-base (1.31) ...
Processing triggers for base-files (1:2024.3.0) ...
Processing triggers for kali-menu (2024.3.1) ...
Processing triggers for doc-base (0.11.2) ...
Processing 1 added doc-base file...
Setting up libpcap0.8-dev:amd64 (1.10.5-1) ...
Setting up libpcap-dev:amd64 (1.10.5-1) ...
```



**Paso 27.** Una vez terminado la actualización anterior proseguimos a ingresar el siguiente comando `wget` <http://rules.emergingthreats.net/open/suricata/emerging.rules.tar.gz> cual va a descargar un archivo desde internet llamado `emerging.rules.tar.gz`, el cual contiene un conjunto de reglas de Emerging Threats que se van a usar con suricata.

```
(saul@SAUL)-[~]
$ wget http://rules.emergingthreats.net/open/suricata/emerging.rules.tar.gz
--2024-10-31 14:23:10-- http://rules.emergingthreats.net/open/suricata/emerging.rules.tar.gz
Resolving rules.emergingthreats.net (rules.emergingthreats.net) ... 52.72.132.76, 34.192.96.151, 18.210.119.231, ...
Connecting to rules.emergingthreats.net (rules.emergingthreats.net)|52.72.132.76|:80 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4569742 (4.4M) [application/octet-stream]
Saving to: 'emerging.rules.tar.gz'

emerging.rules.tar. 19%[=>] 884.69K 84.6KB/s eta 27s
```

**Paso 28.** Ingresamos el siguiente comando `tar zxvf emerging.rules.tar.gz` para descomprimir y extraer el archivo que se descargó anteriormente.

```
(saul@SAUL)-[~]
$ tar zxvf emerging.rules.tar.gz
rules/
rules/3coresec.rules
rules/BSD-License.txt
rules/LICENSE
rules/botcc.portgrouped.rules
rules/botcc.rules
rules/ciarmy.rules
```

**Paso 29.** Utilizamos el siguiente comando `sudo mv rules /var/lib/suricata/` para mover la carpeta `rules` al directorio `/var/lib/suricata/`, la carpeta `rules` contiene las reglas extraídas que se utilizarán para configurar suricata.

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

**Paso 30.** Accedemos al directorio con el siguiente comando `cd /var/lib/suricata/rules`.

```
(saul@SAUL)-[~]  
$ cd /var/lib/suricata/rules
```

**Paso 31.** Ingresamos el siguiente comando `sudo nano /etc/suricata/suricata.yaml` donde realizaremos las configuraciones de Suricata

```
(saul@SAUL)-[/var/lib/suricata/rules]  
$ sudo nano /etc/suricata/suricata.yaml
```

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

**Paso 32.** Nos aparecerá una interfaz donde agregaremos los siguientes:

- `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;)`

Esto nos permitirá generar las alertas basadas en los patrones específicos, para guardar cambios pulsamos la tecla `ctrl + o` después `enter` y para salir `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 32.** Pulsamos la tecla ctrl + b para búsqueda e ingresamos el siguiente parámetro default-rule-path en el archivo de configuración de suricata el cual buscará los archivos de reglas.

```
#HOME_NET: "any"
Search [Backwards]: default-rule-path
^G Help      M-C Case Sens  M-B Backwards  ^P Older      ^T Go To Line
^C Cancel    M-R Reg.exp.   ^R Replace     ^N Newer
```

**Paso 33.** Nos abrirá una nueva ventana donde ingresaremos lo siguiente:

- emerging-exploit.rules
- my-rules

Esto indicará los nombres específicos de los archivos de reglas específicas de suricata debe de cargar y utilizar, el primer archivo contiene reglas relacionadas con la detección de posibles exploits y el segundo archivo de reglas personaliza que un administrador o usuario ha creado para adaptar la detección, guardamos cambios y salimos.

```
##
default-rule-path: /var/lib/suricata/rules

rule-files:
- emerging-exploit.rules
- my-rules

##
## Auxiliary configuration files.
##
```

**Paso 34.** Ingresamos el siguiente comando `sudo suricata -c /etc/suricata/suricata.yaml -i eth0` para iniciar suricata en modo de monitoreo, nos pedirá que ingresemos la contraseña del usuario, empezará a cargar.

```
└─$ sudo suricata -c /etc/suricata/suricata.yaml -i eth0
[sudo] password for saul:
i: suricata: This is Suricata version 7.0.7 RELEASE running in SYSTEM mode
W: detect-flowbits: flowbit 'ET.http.binary' is checked but not set. Checked
in 2025195 and 1 other sigs
W: detect-flowbits: flowbit 'ET.http.javaclient' is checked but not set. Chec
ked in 2015658 and 1 other sigs
W: detect-flowbits: flowbit 'et.IE7.NoRef.NoCookie' is checked but not set. C
hecked in 2024192 and 1 other sigs
W: detect-flowbits: flowbit 'ET.gocd.auth' is checked but not set. Checked in
2034333 and 0 other sigs
W: detect-flowbits: flowbit 'dcerpc.rpcnetlogon' is checked but not set. Chec
ked in 2030870 and 6 other sigs
W: detect-flowbits: flowbit 'ET.BonitaDefaultCreds' is checked but not set. C
hecked in 2036817 and 0 other sigs
W: detect: rule 6: SYN-only to port(s) 80:80 w/o direction specified, disabli
ng for toclient direction
i: threads: Threads created → W: 1 FM: 1 FR: 1 Engine started.
```

**Paso 35.** Ingresamos el siguiente comando `tail -f /var/log/suricata/fast.log` que nos ayudara para monitorear en tiempo real el archivo de registro

```
└─(saul@SAUL)-[~/Desktop]
└─$ 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
:0
10/31/2024-14:58:36.815781  [**] [1:1000002:1] ICMP connection attempt [**] [
Classification: (null)] [Priority: 3] {ICMP} 192.168.0.125:0 → 192.168.0.108
:0
10/31/2024-14:59:03.414932  [**] [1:1000002:1] ICMP connection attempt [**] [
Classification: (null)] [Priority: 3] {ICMP} 192.168.0.1:3 → 192.168.0.125:1
█
```

**Paso 36.** Ingresamos el siguiente comando `sudo nano /etc/network/interfaces` para la configuración de la interfaz de red.



```
(saul@SAUL)-[~]  
$ sudo nano /etc/network/interfaces
```

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

**Paso 37.** Se abrirá una interfaz donde ingresaremos lo siguiente:

`auto eth0`

`iface eth0 inet static`

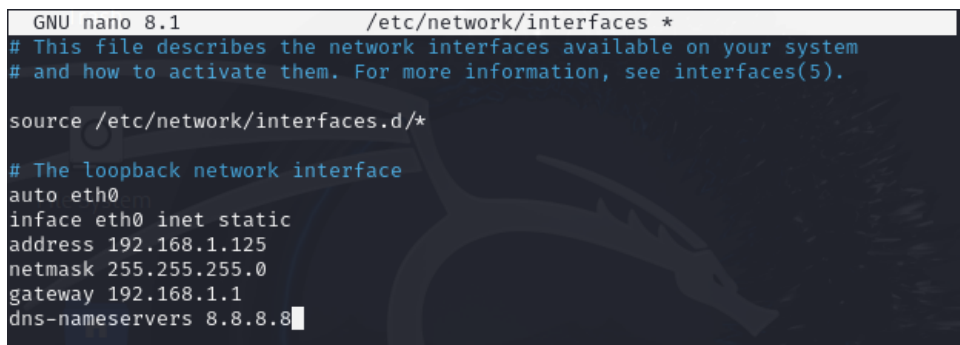
`address 192.168.1.125`

`netmask 255.255.255.0`

`gateway 192.168.1.1`

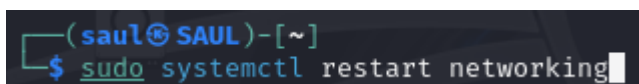
`dns-nameservers 8.8.8.8`

guardamos cambios y salimos de la configuración.



```
GNU nano 8.1 /etc/network/interfaces *  
# This file describes the network interfaces available on your system  
# and how to activate them. For more information, see interfaces(5).  
  
source /etc/network/interfaces.d/*  
  
# The loopback network interface  
auto 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 38.** Ingresamos el siguiente comando `sudo systemctl restart networking` para reiniciar los servicios.



```
(saul@SAUL)-[~]  
$ sudo systemctl restart networking
```

**Paso 39.** Ingresamos el siguiente comando `ip addr show eth0` para verificar que se haya aplicado correctamente.

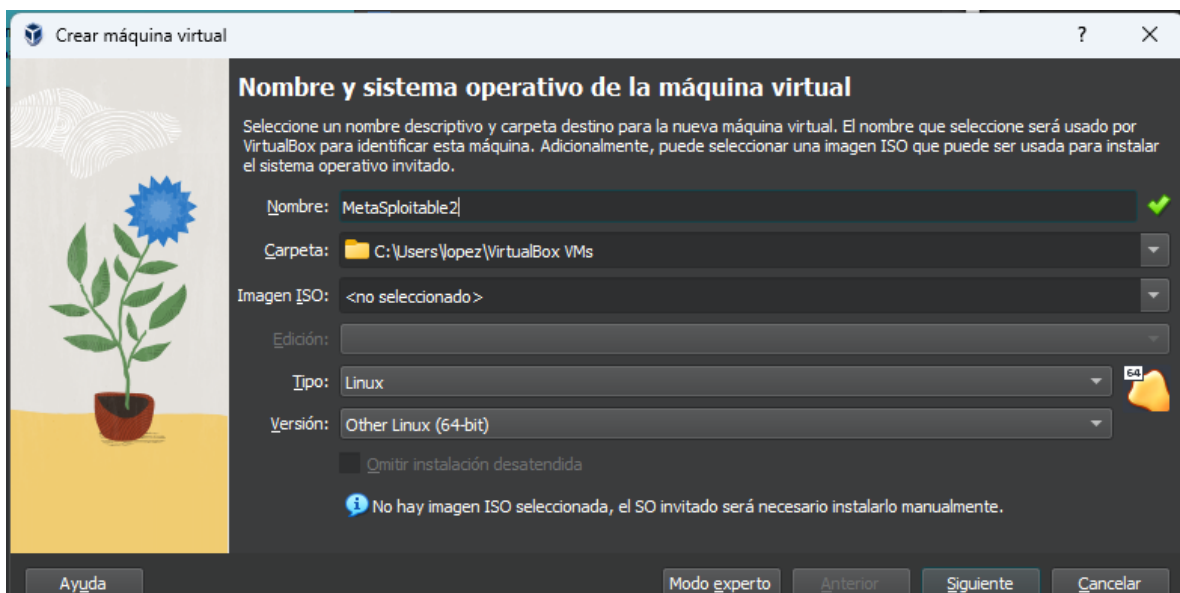
```

$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state 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 noprefixroute eth0
        valid_lft 5292sec preferred_lft 5292sec
    inet 192.168.1.125/24 brd 192.168.1.255 scope global secondary eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe47:7754/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

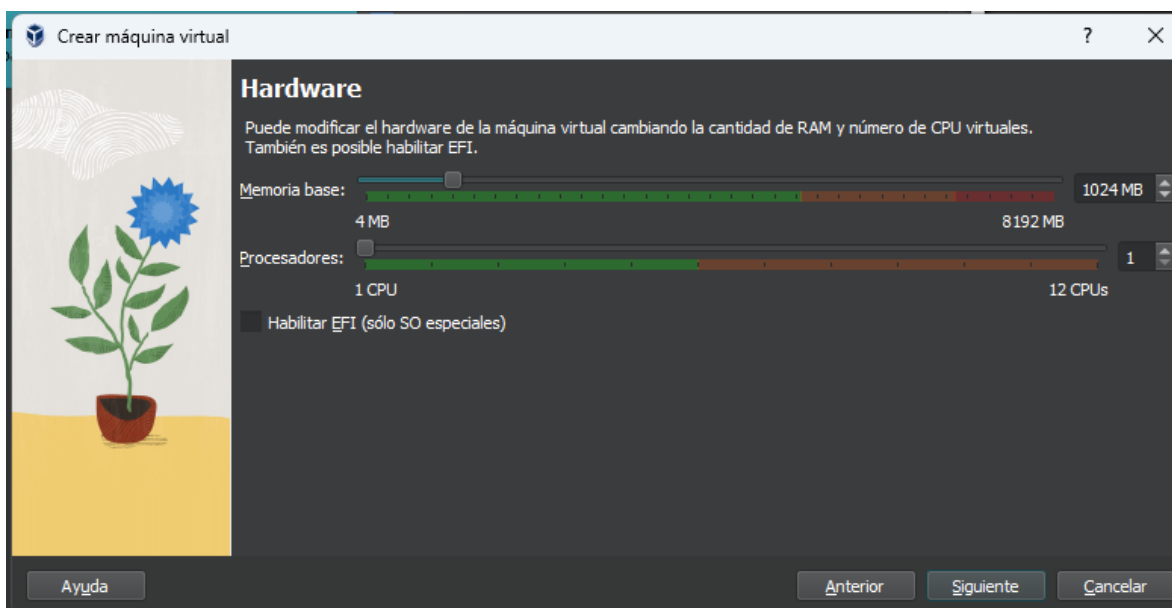
```

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

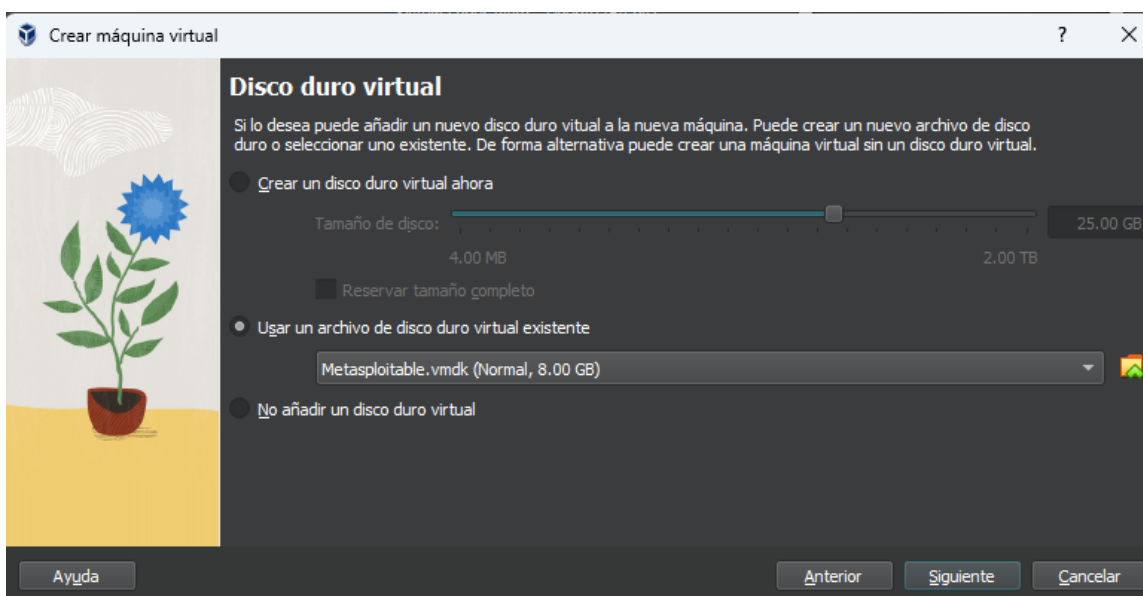
**Paso 1.** Creamos una máquina virtual con el nombre de MetaSploitable2, en tipo seleccionamos Linux y en versión seleccionamos other linux(64-bit), le damos clic en el botón de siguiente.



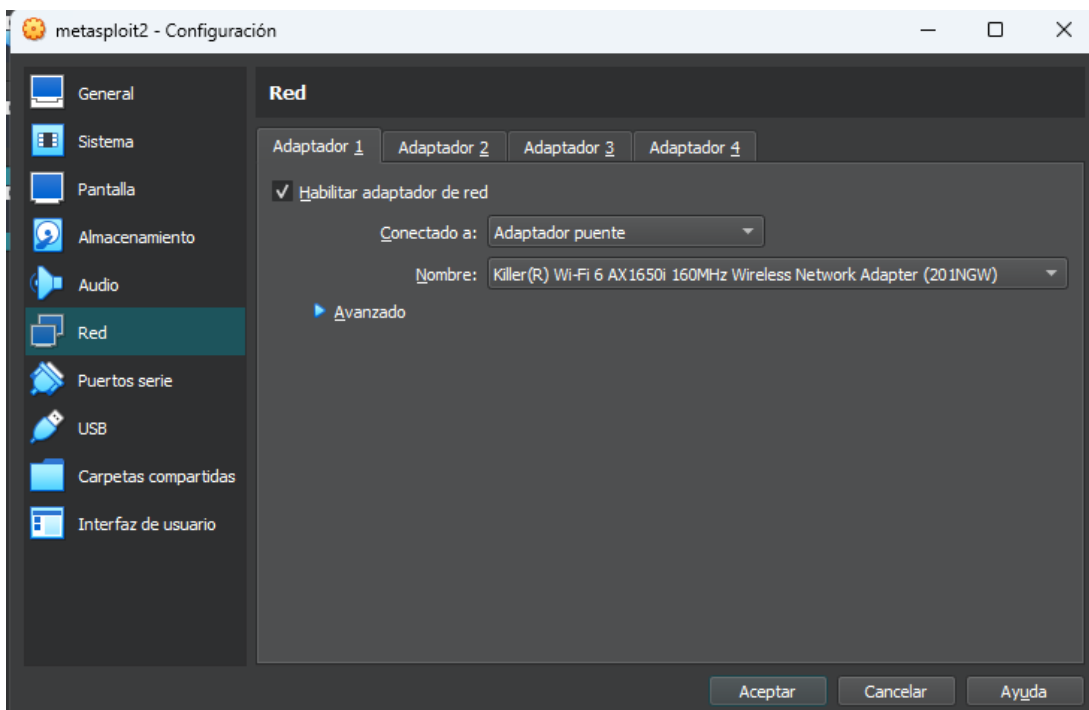
**Paso 2.** En el hardware seleccionamos un 1 de memoria ram y en procesadores lo dejamos por default y le damos clic en siguiente.



**Paso 3.** En almacenamiento le asignamos 25 gb y habilitamos la opción de usar un archivo de disco duro virtual existente y seleccionamos el Iso y proseguimos a darle clic en el botón de siguiente.



**Paso 4.** Una vez creado configuramos la tarjeta de res en nuestro caso seleccionamos adaptador puente para que se le asigne una dirección ip a la máquina virtual, le damos clic en el botón de aceptar e iniciamos la máquina.



**Paso 5.** Una vez iniciada la máquina virtual empezará a cargar y nos pedirá que ingresemos el usuario y su contraseña.

```
metasploit2 [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out' [ OK ]

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

metasploitable login:
```



**Paso 6.** Una vez ingresado lo que es el usuario y contraseña ya estaremos dentro para realizar lo que se pide, ingresamos el siguiente comando `sudo nano /etc/network/interfaces` para acceder a la interfaz de red.

```
msfadmin@metasploitable:~$ sudo nano /etc/network/interfaces
```

#### 4.1 ASIGNAR UNA DIRECCIÓN IP ESTÁTICA A METASPLOITABLE2.

**Paso 7.** En dicha interfaz agregamos lo siguiente para asignarle un dirección ip statica.

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

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

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

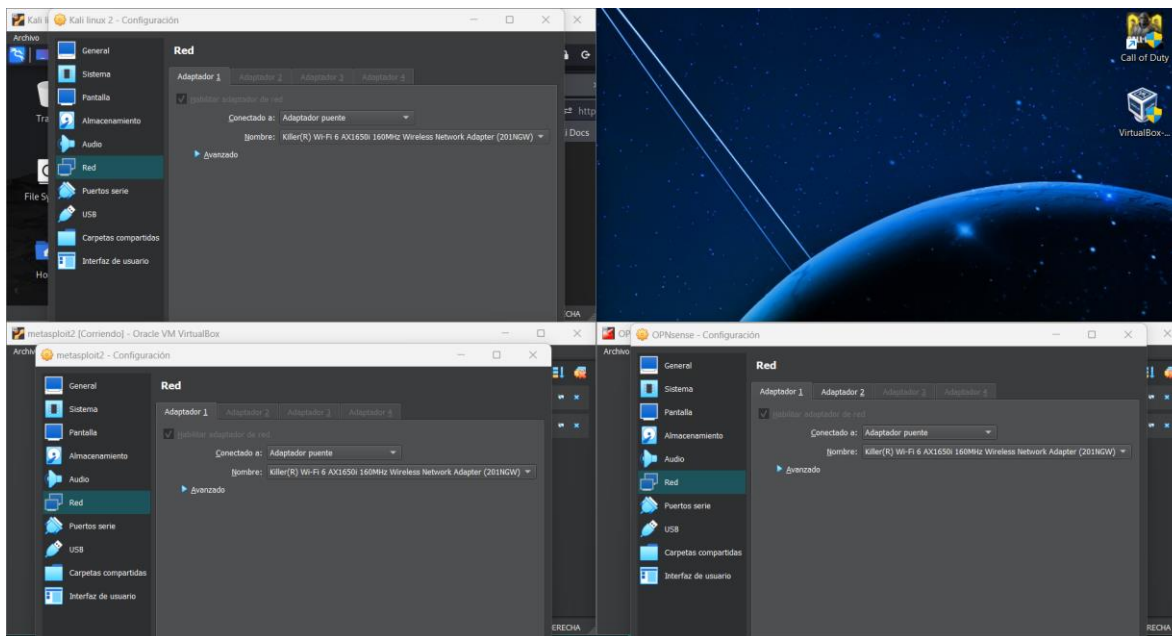
**Paso 9.** Podemos observar que los cambios se realizaron correctamente.

```
eth0      Link encap:Ethernet  HWaddr 08:00:27:39:0c:69
          inet addr:192.168.1.120  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe39:c69/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:60 errors:0 dropped:0 overruns:0 frame:0
          TX packets:143 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5835 (5.6 KB)  TX bytes:15903 (15.5 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

## 5. PING SATISFACTORIO ENTRE LAS MÁQUINAS VIRTUALES.

Para realizar un ping satisfactorio entre las máquinas virtuales, se recomienda seguir los siguientes pasos:

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

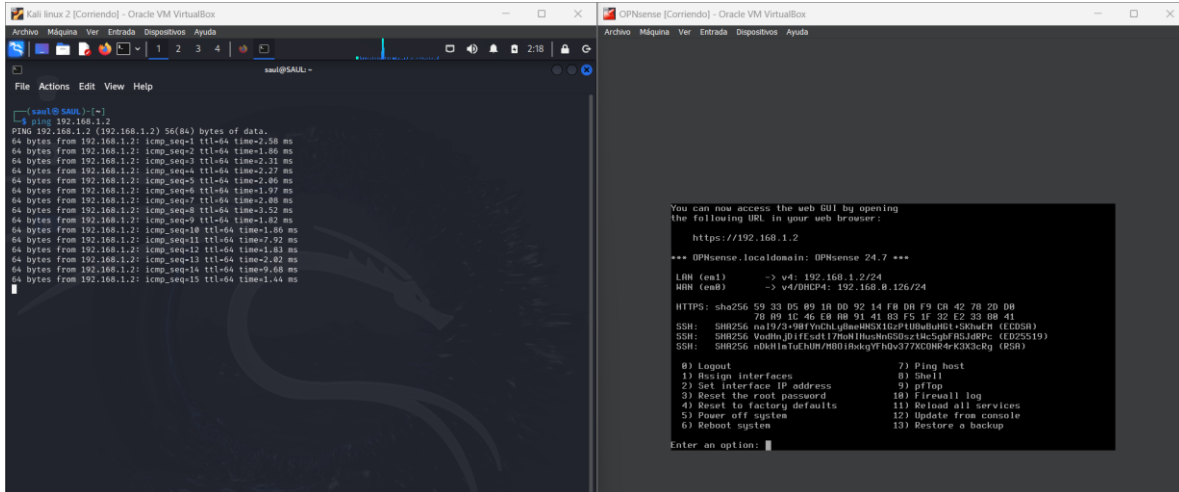


### 5.2 CONFIGURAR LAS REGLAS DE FIREWALL PARA PERMITIR EL TRÁFICO DE PING.

Firewall: Rules: LAN	
full help	
Edit Firewall rule	
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
Source / Invert	<input type="checkbox"/> Use this option to invert the sense of the match.
Source	any
Source	Advanced
OPNsense [c] 2014-2024 Deciso B.V.	

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
Gateway	default
Advanced features	Show/Hide
Save Cancel	

## 5.3 REALIZAR UN PING ENTRE LAS MÁQUINAS VIRTUALES.

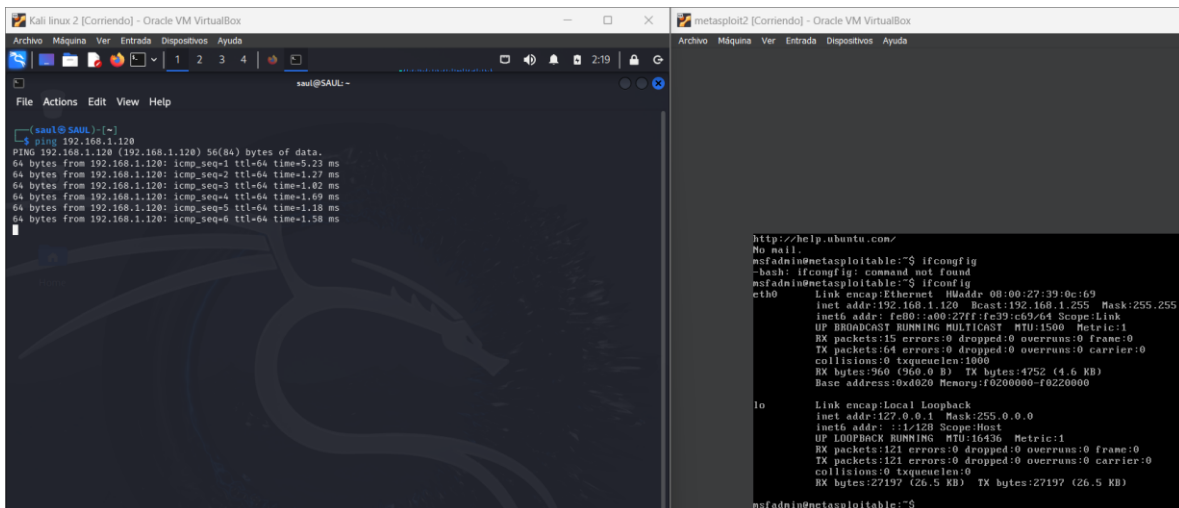


```
kali linux 2 [Corriendo] - Oracle VM VirtualBox
File Actions Edit View Help
[saul@SAUL: ~]$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data:
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=2.58 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=1.86 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=2.23 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=64 time=2.27 ms
64 bytes from 192.168.1.2: icmp_seq=5 ttl=64 time=2.86 ms
64 bytes from 192.168.1.2: icmp_seq=6 ttl=64 time=2.52 ms
64 bytes from 192.168.1.2: icmp_seq=7 ttl=64 time=2.88 ms
64 bytes from 192.168.1.2: icmp_seq=8 ttl=64 time=1.97 ms
64 bytes from 192.168.1.2: icmp_seq=9 ttl=64 time=1.82 ms
64 bytes from 192.168.1.2: icmp_seq=10 ttl=64 time=1.86 ms
64 bytes from 192.168.1.2: icmp_seq=11 ttl=64 time=7.93 ms
64 bytes from 192.168.1.2: icmp_seq=12 ttl=64 time=1.83 ms
64 bytes from 192.168.1.2: icmp_seq=13 ttl=64 time=2.82 ms
64 bytes from 192.168.1.2: icmp_seq=14 ttl=64 time=9.18 ms
64 bytes from 192.168.1.2: icmp_seq=15 ttl=64 time=1.44 ms
^C

```

```
OPNsense [Corriendo] - Oracle VM VirtualBox
File Actions Edit View Help
You can now access the web GUI by opening
the following URL in your web browser:
https://192.168.1.2
*** OPNsense.localdomain: OPNsense 24.7 ***
LAN (en1) -> v4: 192.168.1.2/24
WAN (em0) -> v4/00C4: 192.168.0.126/24
HTTPS: sha256 59 33 05 89 18 D0 92 14 F8 08 F9 C8 42 78 2D D0
78 89 1C 46 E8 A8 91 41 83 F5 1F 32 E2 33 08 41
SSH: Ssh256 na19/3*9MTYvChLghe4M6X1GzP4U8uWuHGT+SKuHn (ECDSA)
SSH: Ssh256 VodianJO1Fcst17h0tHusW6S0z3LmSgRfR5JdRPe (ED25519)
SSH: Ssh256 n8H1aTuChNM/800 (RsaGvYHdv377XG0N8+K3X3C8g (RSA))
0) Logout 7) Ping host
1) Assign interfaces 8) Shell
2) Set interface IP address 9) pflog
3) Reset the root password 10) Firewall log
4) Reset to factory defaults 11) Reload all services
5) Power off system 12) Update from console
6) Reboot system 13) Restore a backup
Enter an option:

```



```
kali linux 2 [Corriendo] - Oracle VM VirtualBox
File Actions Edit View Help
[saul@SAUL: ~]$ ping 192.168.1.120
PING 192.168.1.120 (192.168.1.120) 56(84) bytes of data:
64 bytes from 192.168.1.120: icmp_seq=1 ttl=64 time=5.23 ms
64 bytes from 192.168.1.120: icmp_seq=2 ttl=64 time=5.27 ms
64 bytes from 192.168.1.120: icmp_seq=3 ttl=64 time=1.02 ms
64 bytes from 192.168.1.120: icmp_seq=4 ttl=64 time=1.69 ms
64 bytes from 192.168.1.120: icmp_seq=5 ttl=64 time=1.18 ms
64 bytes from 192.168.1.120: icmp_seq=6 ttl=64 time=1.58 ms
^C

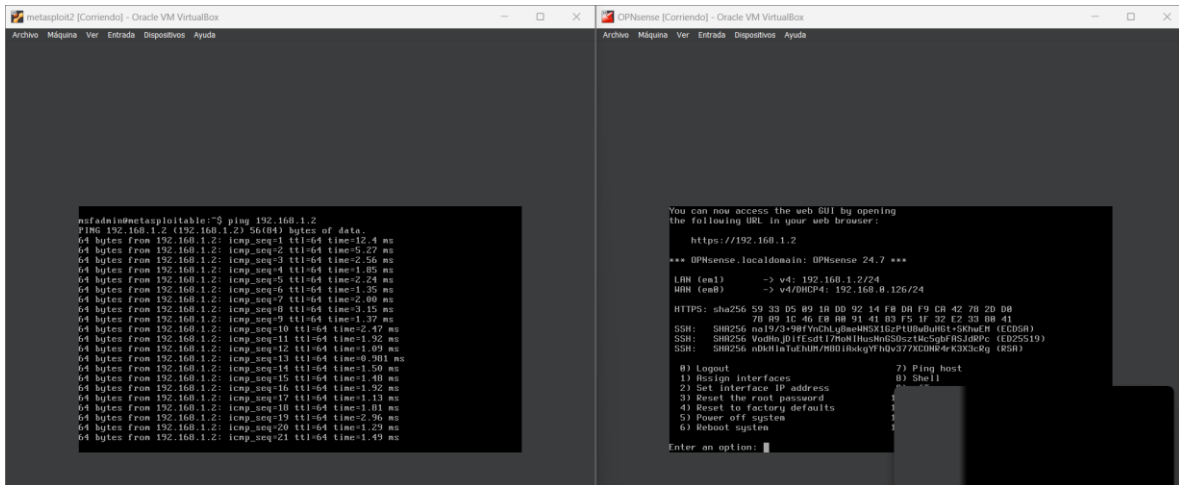
```

```
metasploit2 [Corriendo] - Oracle VM VirtualBox
File Actions Edit View Help
msfadmin@metasploitable:~$ ifconfig
bash: ifconfig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:39:0c:69
          inet addr: 192.168.1.120  Bcast: 192.168.1.255  Mask: 255.255.255
          inet6 addr: fe80::a00:27ff:fe39:c69:64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:15 errors:0 dropped:0 overruns:0 frame:0
          TX packets:64 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:960 (960.0 B)  TX bytes:4752 (4.6 KB)
          Base address: 0xb020 Memory: f0200000-f0208000

lo        Link encap:Local Loopback
          inet addr: 127.0.0.1  Mask: 255.0.0.0
          inet6 addr: ::1:1 Scope:Host
          UP LOOPBACK RUNNING  MTU:1636  Metric:1
          RX packets:121 errors:0 dropped:0 overruns:0 frame:0
          TX packets:121 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:27197 (26.5 KB)  TX bytes:27197 (26.5 KB)

msfadmin@metasploitable:~$ _

```



```
metasploit2 [Corriendo] - Oracle VM VirtualBox
File Actions Edit View Help
msfadmin@metasploitable:~$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data:
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=12.4 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=5.27 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=2.56 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=64 time=1.86 ms
64 bytes from 192.168.1.2: icmp_seq=5 ttl=64 time=2.24 ms
64 bytes from 192.168.1.2: icmp_seq=6 ttl=64 time=1.35 ms
64 bytes from 192.168.1.2: icmp_seq=7 ttl=64 time=2.80 ms
64 bytes from 192.168.1.2: icmp_seq=8 ttl=64 time=3.15 ms
64 bytes from 192.168.1.2: icmp_seq=9 ttl=64 time=1.32 ms
64 bytes from 192.168.1.2: icmp_seq=10 ttl=64 time=2.47 ms
64 bytes from 192.168.1.2: icmp_seq=11 ttl=64 time=1.92 ms
64 bytes from 192.168.1.2: icmp_seq=12 ttl=64 time=1.09 ms
64 bytes from 192.168.1.2: icmp_seq=13 ttl=64 time=0.901 ms
64 bytes from 192.168.1.2: icmp_seq=14 ttl=64 time=1.50 ms
64 bytes from 192.168.1.2: icmp_seq=15 ttl=64 time=1.40 ms
64 bytes from 192.168.1.2: icmp_seq=16 ttl=64 time=1.92 ms
64 bytes from 192.168.1.2: icmp_seq=17 ttl=64 time=1.13 ms
64 bytes from 192.168.1.2: icmp_seq=18 ttl=64 time=1.01 ms
64 bytes from 192.168.1.2: icmp_seq=19 ttl=64 time=2.96 ms
64 bytes from 192.168.1.2: icmp_seq=20 ttl=64 time=1.29 ms
64 bytes from 192.168.1.2: icmp_seq=21 ttl=64 time=1.49 ms
^C

```

```
OPNsense [Corriendo] - Oracle VM VirtualBox
File Actions Edit View Help
You can now access the web GUI by opening
the following URL in your web browser:
https://192.168.1.2
*** OPNsense.localdomain: OPNsense 24.7 ***
LAN (en1) -> v4: 192.168.1.2/24
WAN (em0) -> v4/00C4: 192.168.0.126/24
HTTPS: sha256 59 33 05 89 18 D0 92 14 F8 08 F9 C8 42 78 2D D0
78 89 1C 46 E8 A8 91 41 83 F5 1F 32 E2 33 08 41
SSH: Ssh256 na19/3*9MTYvChLghe4M6X1GzP4U8uWuHGT+SKuHn (ECDSA)
SSH: Ssh256 VodianJO1Fcst17h0tHusW6S0z3LmSgRfR5JdRPe (ED25519)
SSH: Ssh256 n8H1aTuChNM/800 (RsaGvYHdv377XG0N8+K3X3C8g (RSA))
0) Logout 7) Ping host
1) Assign interfaces 8) Shell
2) Set interface IP address 9) pflog
3) Reset the root password 10) Firewall log
4) Reset to factory defaults 11) Reload all services
5) Power off system 12) Update from console
6) Reboot system 13) Restore a backup
Enter an option:

```

## CONCLUSIONES

SAÚL: Para concluir, la instalación y configuración de VirtualBox, OPNsense (o pfSense), y Kali Linux en un entorno virtual proporciona una base sólida para experimentar con la virtualización y la seguridad en redes. VirtualBox facilita la gestión de múltiples sistemas operativos en un solo equipo, permitiendo al usuario probar distintas configuraciones de red y seguridad de forma segura y controlada. La instalación de OPNsense como firewall virtual proporciona una experiencia práctica en la configuración de reglas de firewall, NAT, DHCP, y DNS, aspectos clave en la seguridad de red. Esta herramienta, al estar en una red interna y contar con direcciones IP estáticas, permite la administración centralizada del tráfico y protege el entorno de posibles amenazas.

LUZ: La integración de Kali Linux, configurado como un sistema de detección de intrusos, añade una capa adicional de seguridad y monitorización en el entorno virtual. Esto permite analizar y prevenir intentos de intrusión, siendo una práctica valiosa para el desarrollo de habilidades en ciberseguridad. En conjunto, estos pasos brindan una infraestructura virtual completa para realizar pruebas y experimentos de red y seguridad, sin comprometer los recursos del sistema anfitrión ni afectar la red principal. Este enfoque fomenta un ambiente de aprendizaje seguro para mejorar las habilidades en administración de redes y seguridad informática.

## **BIBLIOGRAFIA.**

[Visión de Máquina Industrial Presentado por Mouser Electronics | Mouser Electronics](#)

[2 - OPNSENSE Firewall - Asignar Interfaces WAN y LAN en OPNSENSE Curso Gratuito](#)

[https://mundowin.com/guia-completa-instalar-y-configurar-pfsense-en-virtualbox/#google\\_vignette](https://mundowin.com/guia-completa-instalar-y-configurar-pfsense-en-virtualbox/#google_vignette)

[Installation | Kali Linux Documentation](#)

[Cómo Descargar e Instalar METASPLOITABLE 2 en VirtualBox](#)