



TECNOLÓGICO NACIONAL DE MÉXICO
INSTITUTO TECNOLÓGICO DE TLAXIACO

SEGURIDAD Y VIRTUALIZACIÓN

Practica 6

CREACIÓN DE UN LABORATORIO DE SEGURIDAD P1

CARRERA:

INGENIERIA EN SISTEMAS COMPUTACIONALES

INTEGRANTES:

REYES LÓPEZ LUZ KARINA

ROQUE CABALLERO JERONIMA

REYES GARCÍA SANDRA YOLOTZIN

DOCENTE

OSORIO SALINAS EDWARD

Tlaxiaco, Oax., Octubre de 2024.



“Educación, ciencia y tecnología, progreso día con día”®

INDICE

INTRODUCCIÓN	3
INSTALACIÓN DE VIRTUAL BOX.	4
INSTALACIÓN DE OPNSENSE EN UNA MÁQUINA VIRTUAL	8
CONFIGURACIÓN DE INTERFACES	11
CONFIGURACIÓN DE REGLAS DE FIREWALL:	15
CONFIGURAR EL NAT	17
CONFIGURACIÓN DE DHCP	18
CONFIGURACIÓN DE DNS.....	19
ASIGNACIÓN DE DIRECCIÓN IP ESTÁTICA AL FIREWALL	19
INSTALAR KALI LINUX EN UNA MÁQUINA VIRTUAL Y CONFIGURAR UN SISTEMA DE DETECCIÓN DE INTRUSOS	20
INSTALAR UN SISTEMA DE DETECCIÓN DE INTRUSOS COMO SNORT O SURICATA:	28
CONFIGURAR LAS REGLAS DE DETECCIÓN DE INTRUSOS.	31
CONFIGURAR LAS ALERTAS DE DETECCIÓN DE INTRUSOS.	31
ASIGNAR UNA DIRECCIÓN IP ESTÁTICA A KALI LINUX.	32
CREAR UNA MÁQUINA VIRTUAL VULNERABLE POR DISEÑO COMO METASPLOITABLE2:	33
ASIGNAR UNA DIRECCIÓN IP ESTÁTICA A METASPLOITABLES2:	36
PING SATISFACTORIO ENTRE LAS MÁQUINAS VIRTUALES:.....	37
CONFIGURAR LAS REGLAS DE FIREWALL PARA PERMITIR EL TRÁFICO DE PING:	37
REALIZAR UN PING ENTRE LAS MÁQUINAS VIRTUALES:	38
CONCLUSIÓN	39
BIBLIOGRAFÍAS:	40

INTRODUCCIÓN

La Práctica 6 tiene como objetivo principal implementar un laboratorio de seguridad en un entorno virtualizado utilizando plataformas como Virtual Box o VMware. Este practica nos permite recrear un ambiente controlado y seguro para simular configuraciones y prácticas esenciales en ciberseguridad.

En esta pratica, se establece un firewall utilizando OpnSense o pfSense, se configuró un sistema de detección de intrusos con Kali Linux, y se despliega una máquina virtual vulnerable por diseño, MetaSploitable2. Estas herramientas trabajan en conjunto para comprender la dinámica de defensa, detección y análisis de amenazas en un entorno realista.

El laboratorio fomenta la conexión entre las máquinas virtuales, incluyendo pruebas como el ping satisfactorio entre ellas, permitiendo experimentar y aprender sobre configuraciones de red, reglas de firewall, NAT, DHCP, DNS y sistemas de detección de intrusos. Esta práctica no solo refuerza los conocimientos teóricos, sino que desarrolla habilidades prácticas fundamentales para la protección de infraestructuras digitales.

INSTALACIÓN DE VIRTUAL BOX.

Para descargar Virtual Box, el primer paso es acceder a su sitio web oficial a través del enlace <https://www.virtualbox.org>. Una vez en la página principal, dirígete a la sección "Downloads" haciendo clic en la opción correspondiente.

A continuación, selecciona el archivo adecuado según el sistema operativo en el que trabajarás. Por ejemplo, si utilizas Windows, elige la opción "Windows host". Esto iniciará la descarga del instalador, como se ilustra en la siguiente imagen.



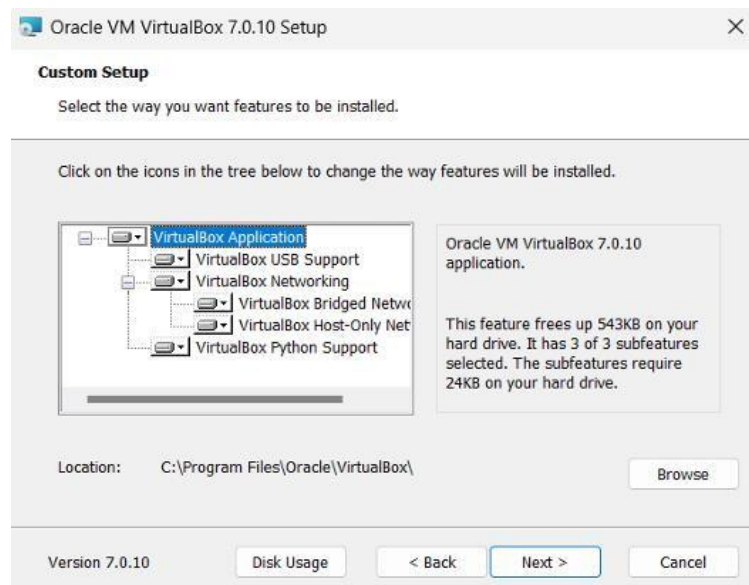
Una vez completada la descarga, el instalador aparecerá en la ubicación predeterminada de descargas de tu equipo. Para iniciar el proceso de instalación, haz clic derecho sobre el archivo descargado y selecciona la opción "Ejecutar como administrador". Esto abrirá el asistente de instalación, como se muestra en la siguiente imagen, permitiéndote continuar con los pasos para instalar Virtual Box.



Después de hacer clic derecho en el archivo descargado y seleccionar **“Ejecutar como administrador”**, se abrirá el asistente de instalación de Virtual Box. La primera ventana que aparece es la de **“Bienvenida”**, donde se inicia el proceso de configuración del software. Haz clic en el botón **“Next”** para continuar, como se muestra en la siguiente imagen.



En la siguiente pantalla, aparecerá la sección de **“Selección de características”**, donde se muestran los componentes que se instalarán junto con Virtual Box. Por defecto, el asistente selecciona las opciones recomendadas para una instalación completa. En este caso, no es necesario realizar cambios, así que simplemente haz clic en **“Next”** para continuar con el proceso, como se muestra en la siguiente imagen.



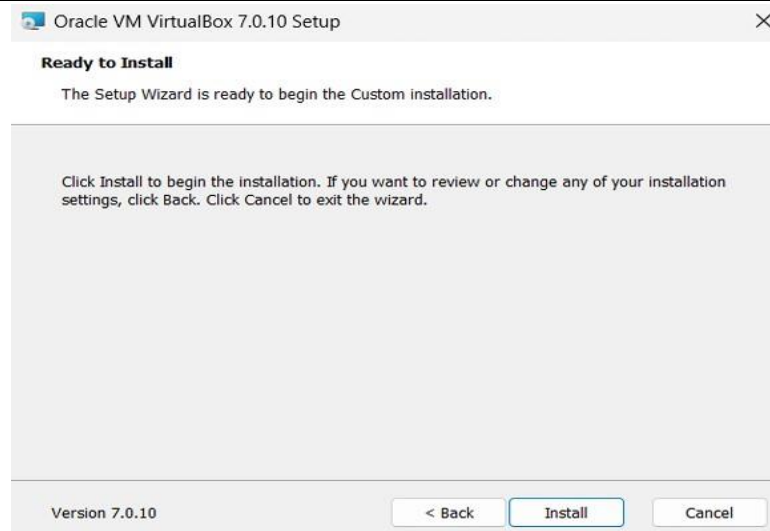
A continuación, se mostrará una ventana con una advertencia relacionada con la configuración de la interfaz de red. Esta advertencia informa que el proceso de instalación puede interrumpir temporalmente la conectividad de red. Para continuar con la instalación sin problemas, selecciona la opción **“YES”**, como se ilustra en la siguiente imagen.



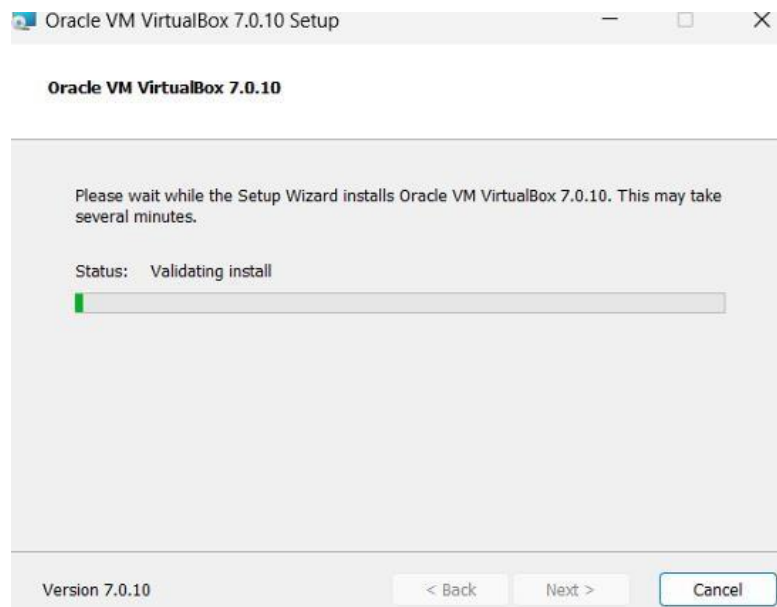
Luego, aparecerá una ventana informando sobre la instalación de dependencias adicionales necesarias para el correcto funcionamiento de Virtual Box. Al igual que en el paso anterior, selecciona la opción “Yes” para proceder con la instalación, como se muestra en la siguiente imagen.



En esta ventana, se te presentará un resumen de las opciones seleccionadas durante el proceso de instalación. Es importante revisar que todo esté correcto. Si no deseas hacer cambios, simplemente haz clic en `***Install***` para comenzar con la instalación de Virtual Box, como se muestra en la siguiente imagen.



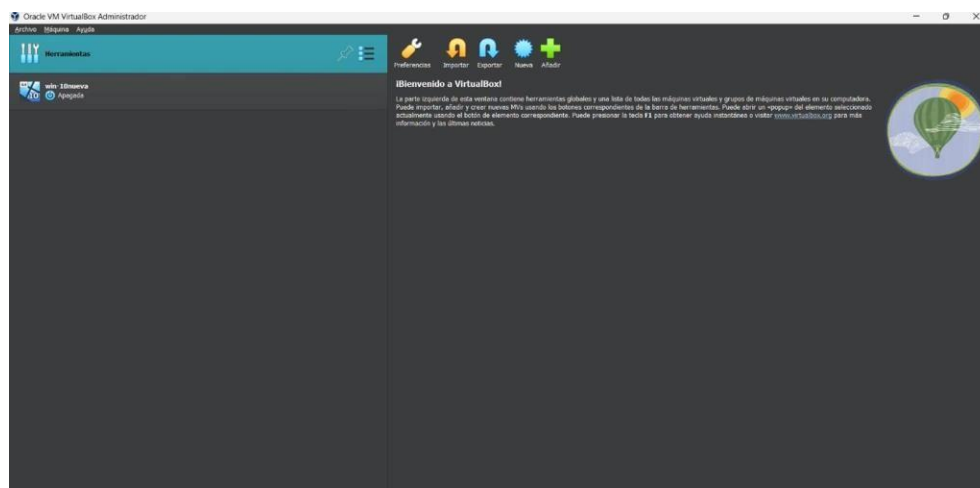
Una vez que la instalación se haya completado, deberás esperar a que el proceso termine. Cuando aparezca la opción, haz clic en **Next** para continuar y finalizar la instalación de Virtual Box, como se muestra en la siguiente imagen.



Una vez que la instalación haya finalizado correctamente, aparecerá una ventana de confirmación indicando que el proceso fue exitoso. Para cerrar el asistente de instalación y completar el proceso, haz clic en "Finish", como se muestra en la siguiente imagen.

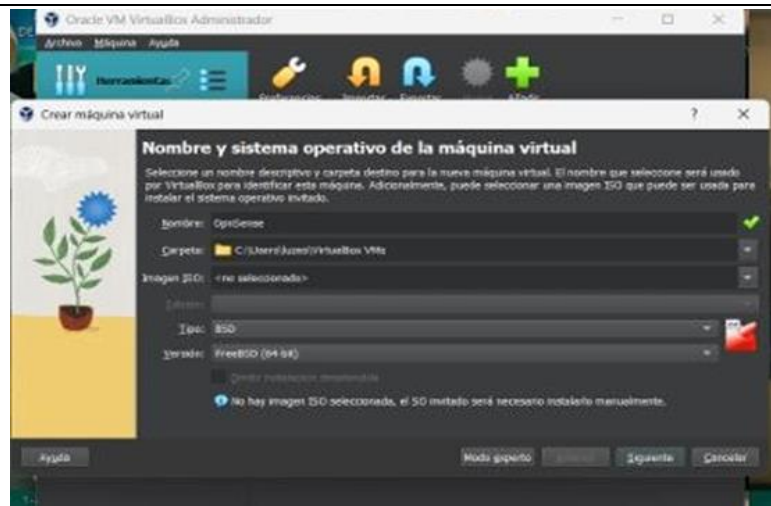


Una vez que la instalación haya finalizado, puedes proceder a abrir Virtual Box. Al hacerlo, la interfaz principal de Virtual Box se abrirá y se mostrará de la siguiente manera, como se puede observar en la siguiente imagen.



INSTALACIÓN DE OPNSENSE EN UNA MÁQUINA VIRTUAL

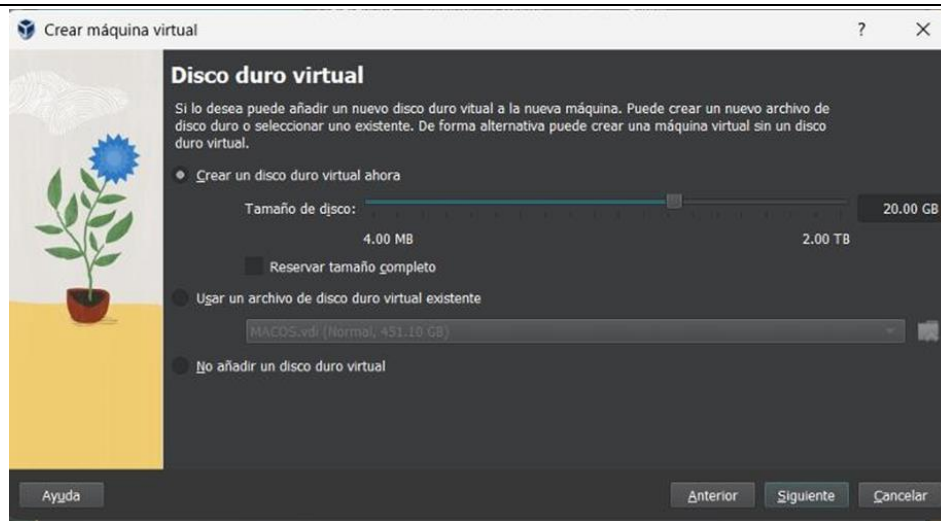
Para crear una nueva máquina virtual, haz clic en el botón "Nueva". En la ventana que aparece, asigna un nombre a la máquina virtual, por ejemplo, "OpnSense". Luego, selecciona "BSD" como el tipo de sistema operativo y "FreeBSD (64-bit)" como la versión. Esto asegurará que la configuración sea compatible y exitosa, como se muestra en la siguiente imagen.



Así mismo una vez 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". Como se puede observar a continuación en la siguiente imagen:



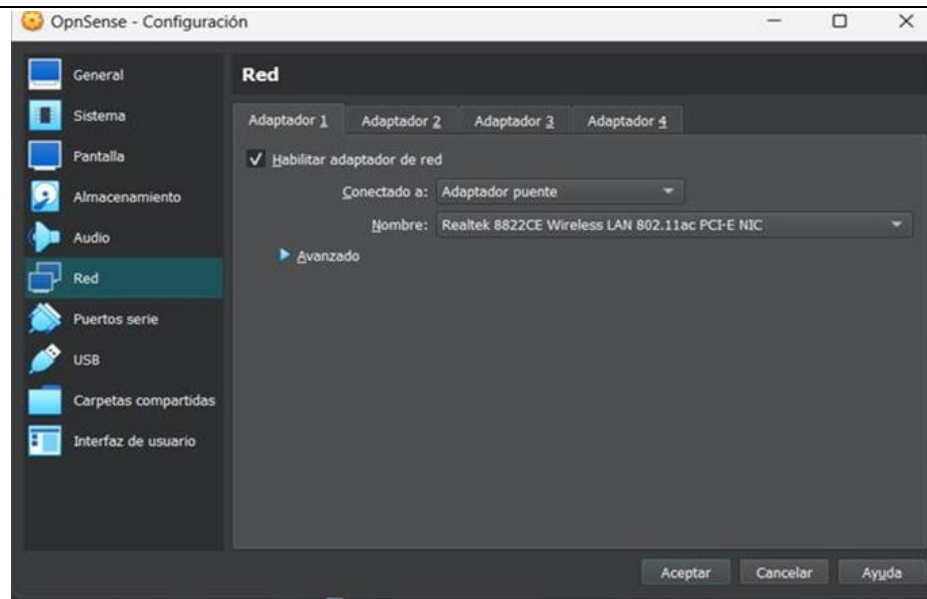
Una vez que hayas seleccionado el tipo y la versión del sistema operativo, se abrirá una ventana en la que se te pedirá especificar el espacio de almacenamiento para la máquina virtual. En este caso, asigna 20 GB de espacio en disco para el sistema operativo. Después de ingresar el tamaño, haz clic en "Siguiente" para continuar con el proceso, como se puede observar en la siguiente imagen.



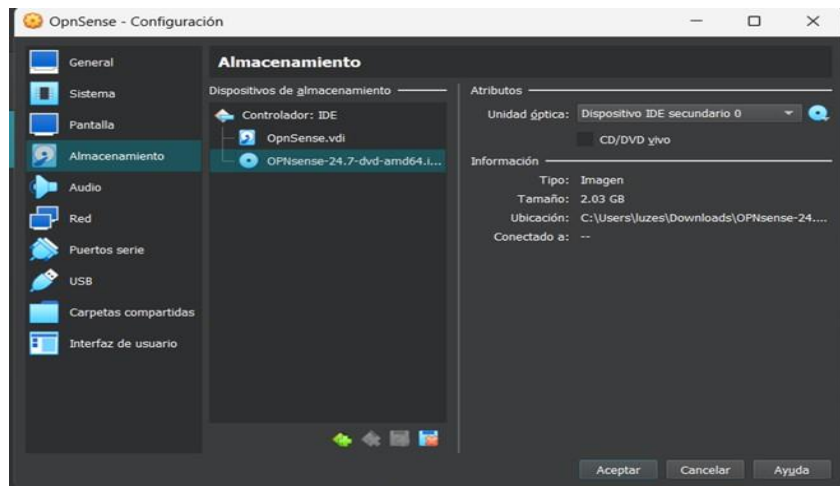
A continuación, se mostrará un resumen con todas las opciones seleccionadas para la máquina virtual. Revisa cuidadosamente los detalles para asegurarte de que todo esté configurado correctamente. Si todo está en orden, haz clic en "Terminar" para completar la creación de la máquina virtual, como se puede ver en la siguiente imagen.



Una vez que la máquina virtual haya sido creada, el siguiente paso es configurar el adaptador de red y el archivo ISO para la instalación del sistema operativo. Para esto, haz clic en el ícono de engranaje ubicado en la parte superior de la ventana de Virtual Box. Luego, ve a la sección "Red" y, en "Adaptador 1", selecciona la opción "Adaptador puente". Esto permitirá que la máquina virtual se conecte a la red como si fuera un dispositivo físico, como se muestra en la siguiente imagen.

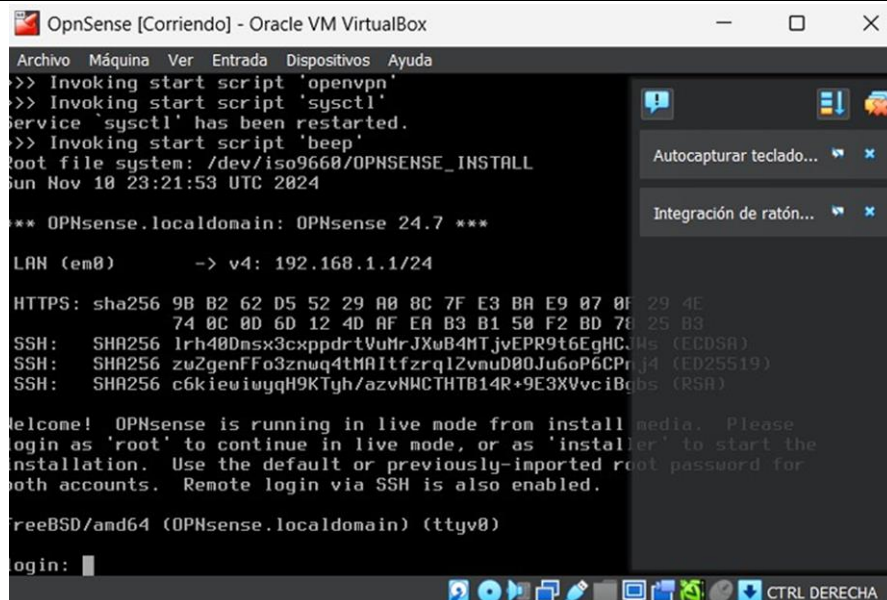


Una vez que hayas terminado de ajustar la configuración del adaptador de red, dirígete a la sección "Almacenamiento". Aquí, selecciona el archivo ISO que utilizarás para la instalación del sistema operativo. Después de cargar el archivo ISO, confirma los cambios haciendo clic en el botón "Aceptar" para guardar la configuración, como se muestra en la siguiente imagen.



CONFIGURACIÓN DE INTERFACES

Una vez que inicies la máquina virtual, aparecerá una pantalla de inicio donde se te pedirá ingresar un usuario y una contraseña. En este caso, el nombre de usuario es root y la contraseña es opnsense. Ingresa los datos correctamente para continuar con la configuración, como se puede ver en la siguiente imagen.



```
OpnSense [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
>> Invoking start script 'openvpn'
>> Invoking start script 'sysctl'
service 'sysctl' has been restarted.
>> Invoking start script 'beep'
root file system: /dev/iso9660/OPNSENSE_INSTALL
Sun Nov 10 23:21:53 UTC 2024

** OPNsense.localdomain: OPNsense 24.7 ***

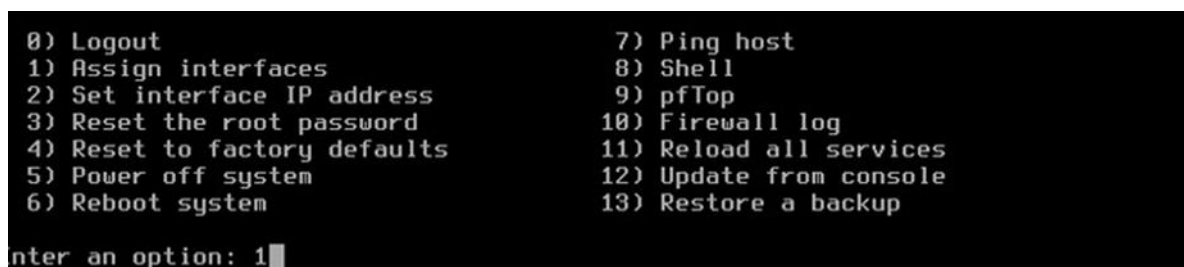
LAN (em0)      -> v4: 192.168.1.1/24

HTTPS: sha256 9B B2 62 D5 52 29 A0 8C 7F E3 BA E9 07 0F 29 4E
       74 0C 0D 6D 12 4D AF EA B3 B1 50 F2 BD 78 25 B3
SSH:   SHA256 1rh40Dasx3cxppdrTvuMrJXuB4MTjvEPR9t6EgHCJMs (ECDSA)
SSH:   SHA256 zu2genFFo3znuq4tMAItfzrq1ZvnuD00Ju6oP6CPnJ4 (ED25519)
SSH:   SHA256 c6kieuiuyqH9KTyh/azvNMCtHTB14R+9E3XVvciBqbs (RSA)

Welcome! OPNsense is running in live mode from install media. Please
login as 'root' to continue in live mode, or as 'installer' to start the
installation. Use the default or previously-imported root password for
both accounts. Remote login via SSH is also enabled.

FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)
login: 
```

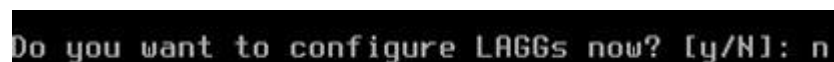
Después de ingresar el usuario y la contraseña, aparecerá una lista de opciones para personalizar varios aspectos de la configuración. En este caso, seleccionaremos la opción relacionada con la configuración de la **interfaz de red**, ya que necesitamos ajustar la red para que funcione correctamente en el entorno de la máquina virtual. Esto se muestra en la siguiente imagen.



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

Enter an option: 1
```

A continuación, se nos preguntará si deseamos configurar los LAGGs (Link Aggregation Groups) en este momento. Dado que no es necesario configurar esta opción para este laboratorio, seleccionaremos "no" y luego presionamos "Enter" para continuar con el proceso.



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

A continuación, aparecerá una opción en la que se te pedirá ingresar la interfaz para la **WAN** (Wide Área Network). En este caso, asigna **"em0"** en el campo correspondiente y presiona **Enter** para continuar con la configuración, como se muestra en la siguiente imagen.



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

A continuación, se mostrarán las configuraciones aplicadas a las interfaces, como se puede observar en la siguiente imagen



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

Posteriormente, continuamos con los pasos siguientes e ingresamos la línea de código correspondiente, como se muestra en la siguiente imagen

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

Después ingresamos la opción número 2 para así posteriormente realizar la

```
Enter an option: 2
```

Una vez completado este paso, se nos pedirá elegir las opciones disponibles para configurar, tal como se muestra en la siguiente imagen

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

Enter the number of the interface to configure: 1
```

Después de escribir el número 1, presionamos Enter. A continuación, configuramos la dirección de la interfaz LAN para DHCP. Aparecerá una opción, en la cual elegiremos 'NO' y presionamos Enter, tal como se muestra en la siguiente imagen

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

Posteriormente, se nos pedirá ingresar la dirección IP para la interfaz LAN. Escribimos la IP deseada y presionamos Enter para continuar, como se puede observar en la siguiente imagen

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

A continuación, ingresamos la máscara de subred en formato numérico (por ejemplo, 24 para una máscara 255.255.255.0) y presionamos Enter para continuar, como se muestra en la siguiente imagen

```
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
```

Se nos preguntará si deseamos configurar IPv6 para la interfaz LAN. Seleccionamos 'no' y presionamos Enter para continuar, como se muestra en la siguiente imagen

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

Posteriormente, en esta configuración, escribimos 'no' y presionamos Enter, como se puede apreciar en la siguiente imagen

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

También se nos preguntará si queremos activar el servidor DHCP en la interfaz LAN. Escribimos 'sí' y presionamos Enter para continuar, como se muestra en la siguiente imagen

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

Posteriormente, se nos solicitará ingresar el rango de direcciones IP de inicio. Introducimos '172.16.4.5' y presionamos Enter para continuar, como se muestra en la siguiente imagen

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

A continuación, se nos pedirá definir la dirección IP y establecer el rango, donde ingresamos '172.16.4.2000'. Después, presionamos Enter. El sistema comenzará a reiniciarse, como se muestra en la siguiente imagen

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

En este apartado, primero ingresamos 'no' y luego 'sí'. Después, presionamos Enter para que se muestre una dirección, como se muestra en la siguiente imagen:

```
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]
```

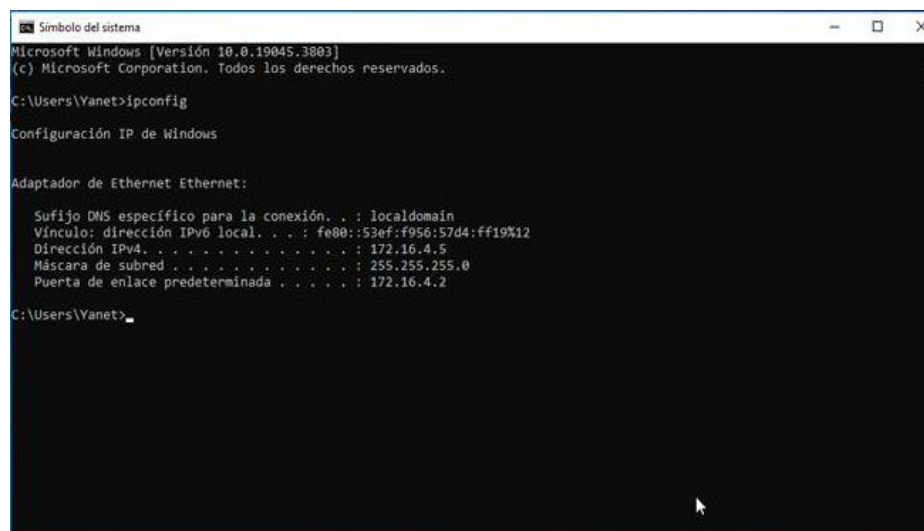
Una vez que el reinicio del sistema haya finalizado, se mostrará una dirección a la que podremos acceder a la interfaz de OPNSense, como se muestra en la siguiente imagen:

```
https://172.16.4.2
```

Finalmente, guardamos los datos que se muestran. Una vez terminadas las configuraciones, se generarán pines con las direcciones correspondientes, como se muestra en la siguiente imagen:

```
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
```

Luego, accedemos a la máquina virtual con el sistema operativo Windows 10. Una vez dentro, la iniciamos, abrimos la terminal y ejecutamos el comando ipconfig para verificar que la máquina virtual está funcionando correctamente. De esta manera, podremos acceder a la interfaz de OPNSense a través del navegador sin inconvenientes, como se muestra en la siguiente imagen



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

C:\Users\Yanet>ipconfig

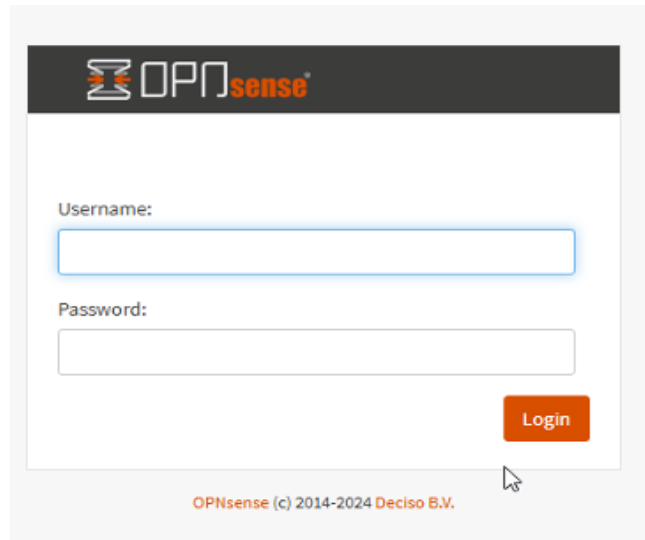
Configuración IP de Windows

Adaptador de Ethernet Ethernet:

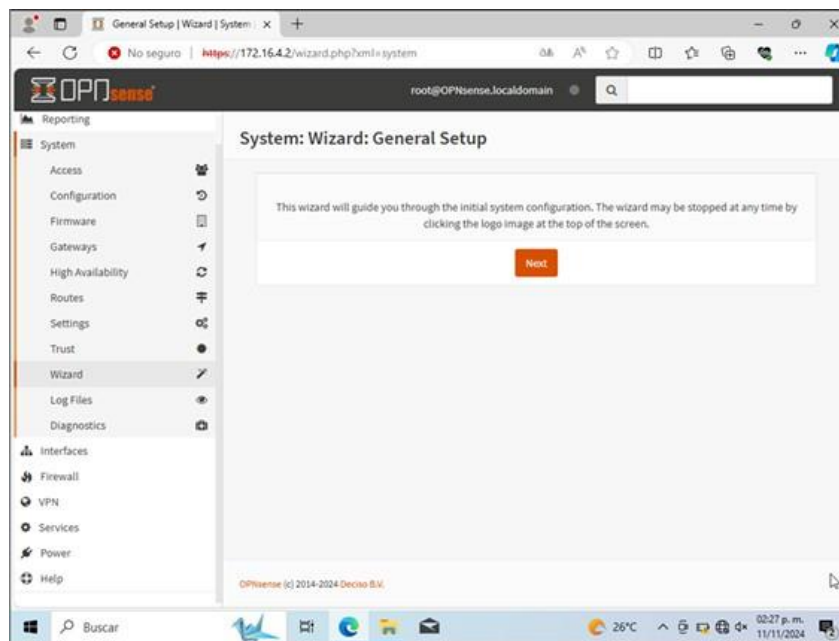
    Sufixo DNS específico para la conexión. . . : localdomain
    Vínculo: dirección IPv6 local. . . : fe80::53ef:f956:57d4:ff19%12
    Dirección IPv4. . . . . : 172.16.4.5
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada. . . . . : 172.16.4.2

C:\Users\Yanet>
```


A continuación, abrimos el navegador instalado, en este caso 'Microsoft Edge', y escribimos la dirección IP de nuestro OPNsense en la barra de direcciones, que es '172.16.4.2', como se muestra en la siguiente imagen

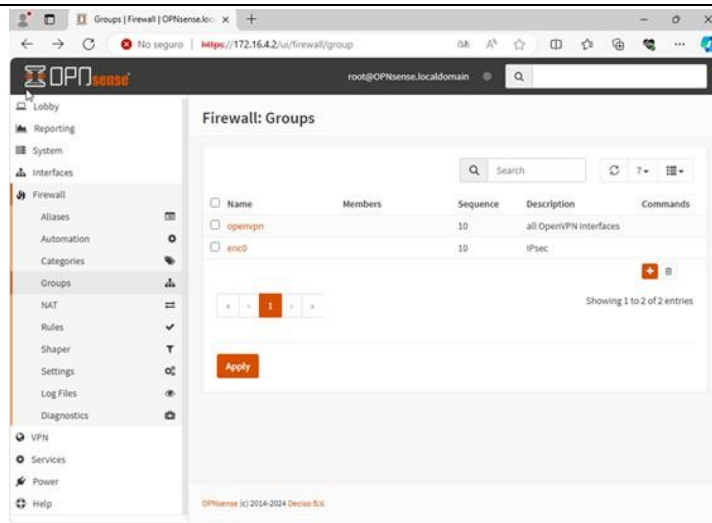


Posteriormente, escribimos 'root' en el campo de usuario y 'opnsense' en el de contraseña. A partir de ahí, podremos realizar diversas configuraciones, como se muestra en la siguiente imagen

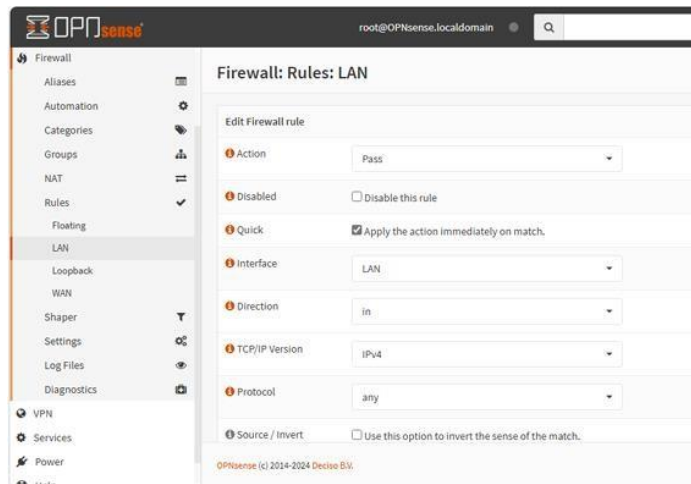


CONFIGURACIÓN DE REGLAS DE FIREWALL:

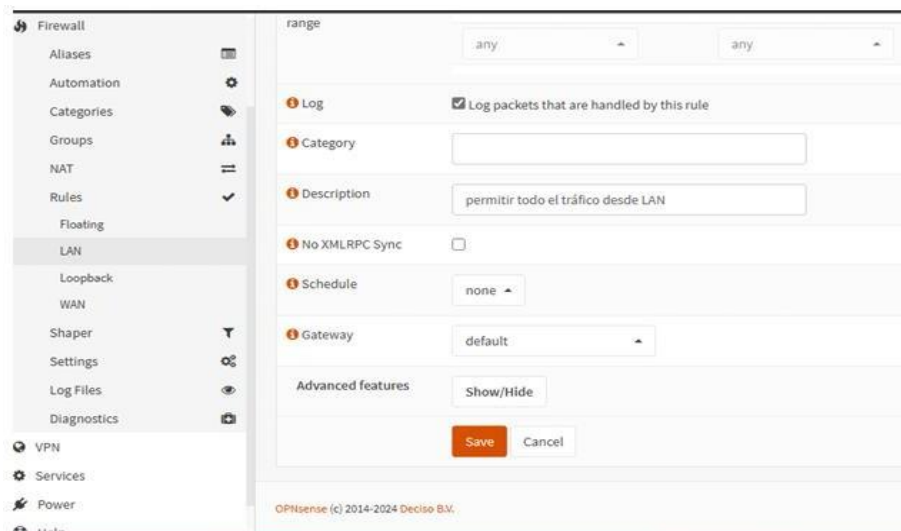
Para configurar las reglas del firewall, dirígete a la sección llamada **"Firewall"**. Al hacerlo, se abrirá una nueva ventana. En esta ventana, haz clic en el botón naranja con el símbolo de **"+"** para añadir una nueva regla al firewall. Esto te permitirá configurar las reglas necesarias para el control del tráfico de red, como se muestra en la siguiente imagen.



Después de hacer clic en el botón **+**, se abrirá una ventana donde podrás establecer una regla para la red **LAN**. En esta ventana, podrás configurar los parámetros específicos para controlar el tráfico de red según tus necesidades. Una vez configurada la regla, podrás guardarla y aplicarla, como se muestra en la siguiente imagen.



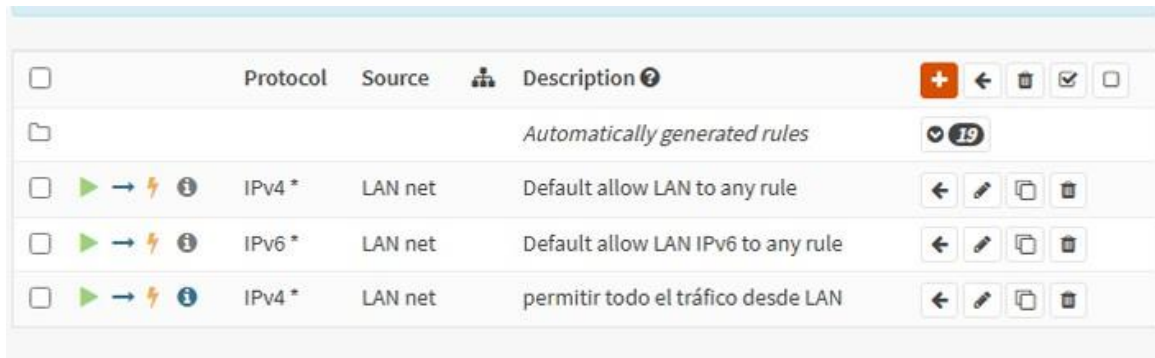
Una vez que hayas configurado todas las opciones de la regla para la red LAN, haz clic en el botón **Save** para guardar los cambios realizados. Esto aplicará la nueva regla al firewall,



asegurando que se mantengan las configuraciones que acabas de establecer, como se muestra en la siguiente imagen.

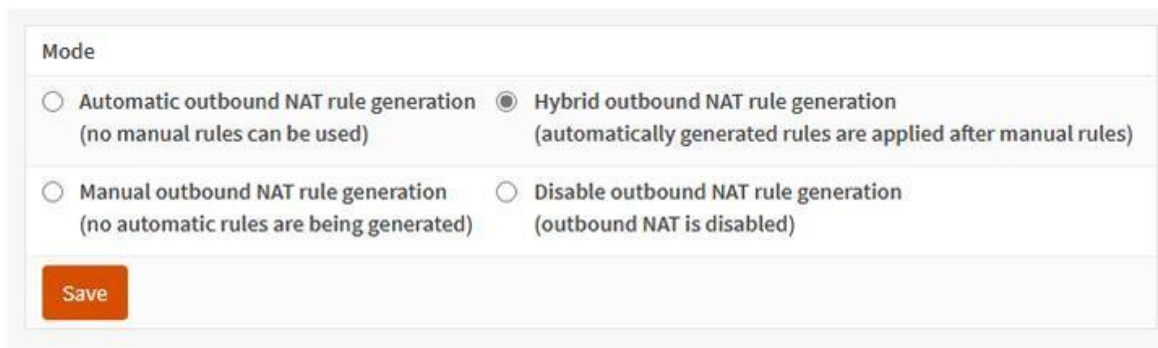
CONFIGURAR EL NAT

Luego de guardar los cambios, podrás observar que ahora hay tres reglas configuradas en la sección ****LAN**** del firewall. Estas reglas permiten gestionar y controlar el tráfico de red según los parámetros establecidos, asegurando una configuración adecuada, como se puede ver en la siguiente imagen.



<input type="checkbox"/>	Protocol	Source	Description	
Automatically generated rules 19				
<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 tráfico desde LAN	

Para configurar el ****NAT**** (Network Address Translation), dirígete a la sección correspondiente y selecciona el ****modo**** de operación. Escoge la opción *****Hybrid outbound rule generation - automatically generated rules*****. Esta configuración combina reglas automáticas con la posibilidad de añadir reglas personalizadas, ofreciendo mayor flexibilidad, como se muestra en la siguiente imagen.



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)

A continuación, navega a la opción llamada *****Outbound***** dentro de la configuración del NAT. En esta sección, ajusta cada uno de los apartados según los requisitos específicos de la red. Esto incluye seleccionar interfaces, protocolos y rangos de direcciones, asegurando que las reglas de NAT se implementen correctamente, como se muestra en la siguiente imagen.

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

© 2014-2024 Pfsense, Inc.

Una vez configurados todos los apartados en la sección **"Outbound"**, podrás verificar que la configuración del **"NAT"** se ha añadido correctamente. Esto asegura que las reglas estén activas y funcionando según lo previsto, como se muestra en la siguiente imagen.

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

CONFIGURACIÓN DE DHCP

A continuación, configuraremos el **"DHCP"** para la red **"LAN"**. En esta sección, se mostrará un conjunto de opciones que necesitan ser ajustadas, incluyendo la **"dirección IP"**, la **"máscara de subred"** y el **"rango de direcciones IP permitidas"** para los dispositivos conectados a la red. Realiza las configuraciones necesarias según tus requerimientos, como se muestra en la siguiente imagen.

Services: ISC DHCPv4: [LAN]

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

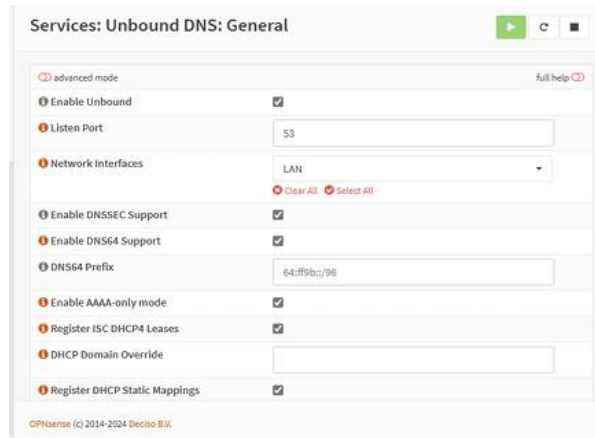
Available range 172.16.4.1 - 172.16.4.254

Range from 172.16.4.5 to 172.16.4.200

full help

CONFIGURACIÓN DE DNS

A continuación, configuraremos el ****DNS****. En la ventana correspondiente, se mostrarán varias opciones de configuración. Selecciona las opciones principales necesarias para tu red, asegurándote de establecer correctamente los servidores DNS y otros parámetros relevantes, como se puede observar en la siguiente imagen.



Una vez que hayas seleccionado las casillas correspondientes en la configuración del ****DNS****, haz clic en el botón ****"Apply"**** para aplicar y guardar los cambios realizados, asegurando que el sistema adopte las configuraciones establecidas, como se muestra en la siguiente imagen.



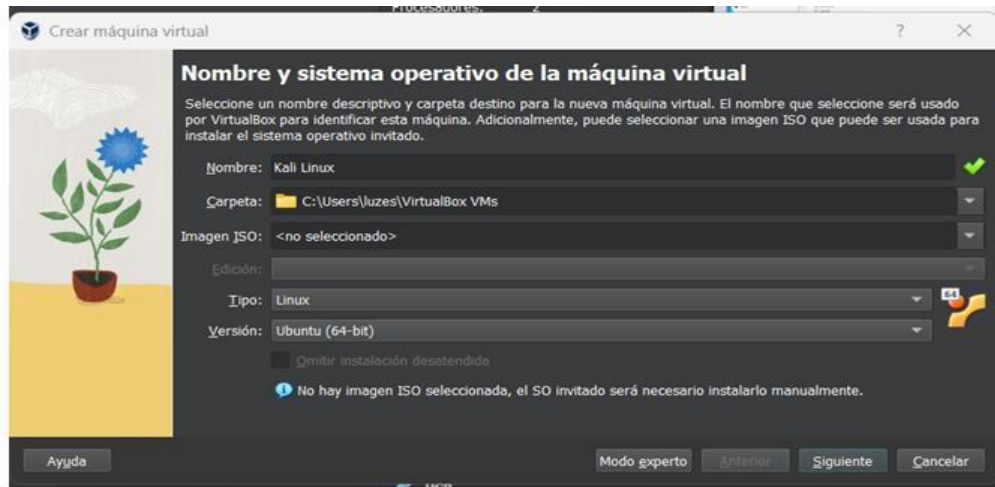
ASIGNACIÓN DE DIRECCIÓN IP ESTÁTICA AL FIREWALL

A continuación, configura la interfaz del firewall asignándole una ****dirección IP estática****, por ejemplo, ****172.16.4.1****, con una máscara de subred ****24****. Esto permitirá una comunicación eficiente y estable dentro de la red configurada, como se puede observar en la siguiente imagen.

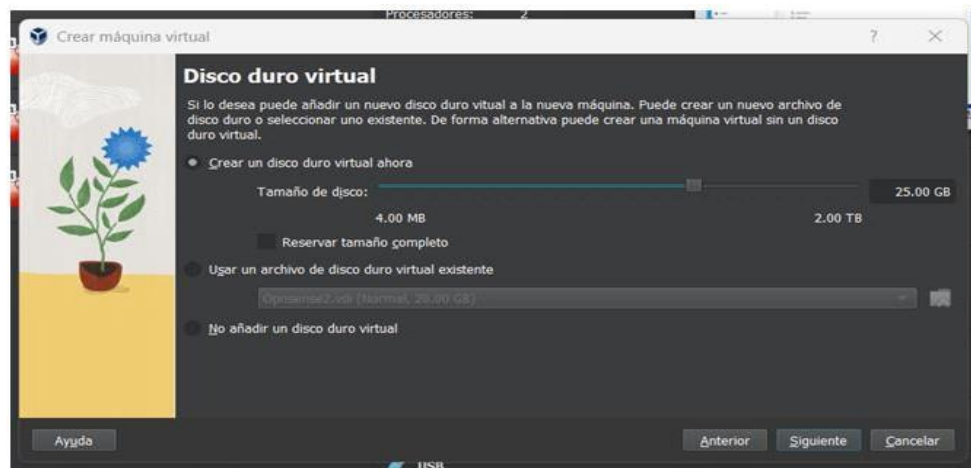


INSTALAR KALI LINUX EN UNA MÁQUINA VIRTUAL Y CONFIGURAR UN SISTEMA DE DETECCIÓN DE INTRUSOS

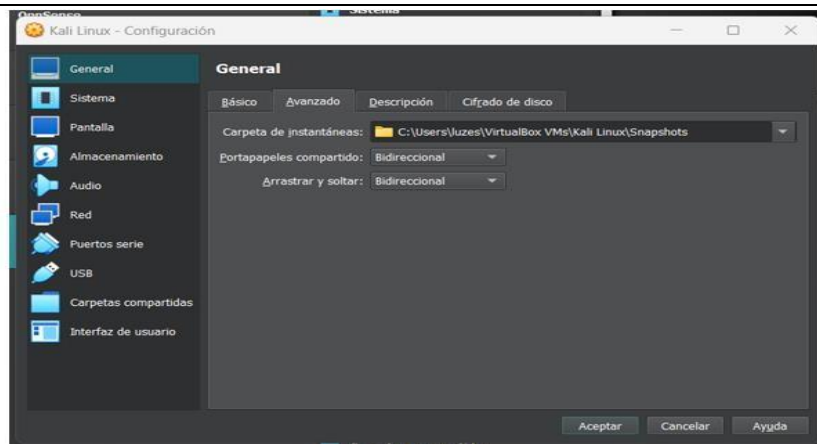
Para comenzar, crea una nueva máquina virtual en VirtualBox o VMware. Asigna el nombre **"Kali Linux"** a la máquina. Luego, selecciona el archivo **"ISO"** correspondiente a Kali Linux y configura el tipo de sistema operativo como **"Linux"**, eligiendo la versión **"Ubuntu (64-bit)"**. Una vez configurado, haz clic en **"Siguiente"** para continuar, como se puede observar en la siguiente imagen.



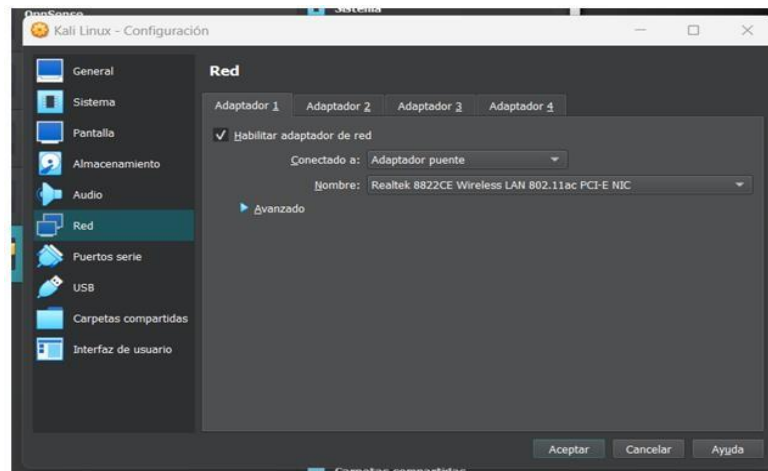
A continuación, configura el tamaño del **"disco duro virtual"** necesario para la máquina. Especifica el tamaño adecuado según los requisitos de Kali Linux, asegurándote de que sea suficiente para su instalación y funcionamiento. Una vez establecido, haz clic en **"Siguiente"** para proceder, como se muestra en la siguiente imagen.



Luego, accede a la sección de **"Configuración"** de la máquina virtual y selecciona el apartado **"General"**. Aquí, ajusta las opciones de **"Portapapeles compartido"** y **"Arrastrar y soltar"**, configurándolas en **"Bidireccional"**. Esto permitirá compartir archivos y texto entre la máquina virtual y el sistema anfitrión de manera eficiente. Una vez configurado, continúa con el siguiente paso, como se observa en la siguiente imagen.



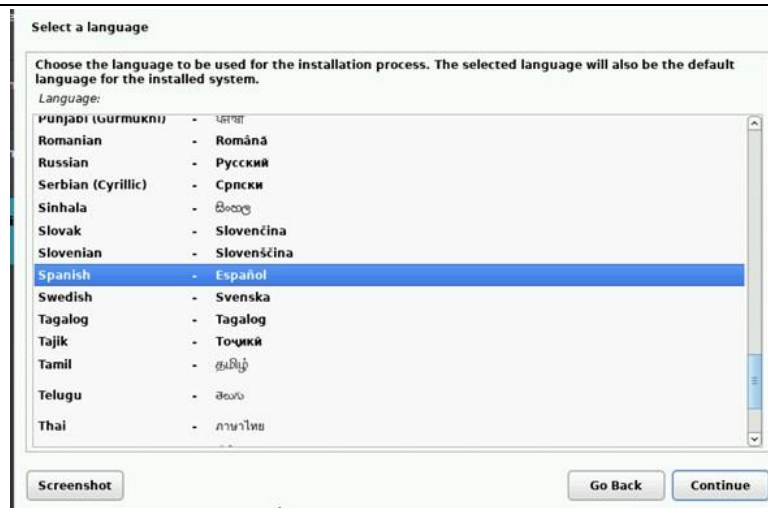
Una vez completada la configuración de **General**, dirígete a la sección **Red**. En **Adaptador 1**, selecciona la opción **Adaptador puente** en el campo **Conectado a**. Esto permitirá que la máquina virtual se conecte a la red local, similar a un dispositivo físico. A continuación, asigna una **dirección IP** adecuada a la máquina virtual para que pueda comunicarse correctamente dentro de la red, como se muestra en la siguiente imagen.



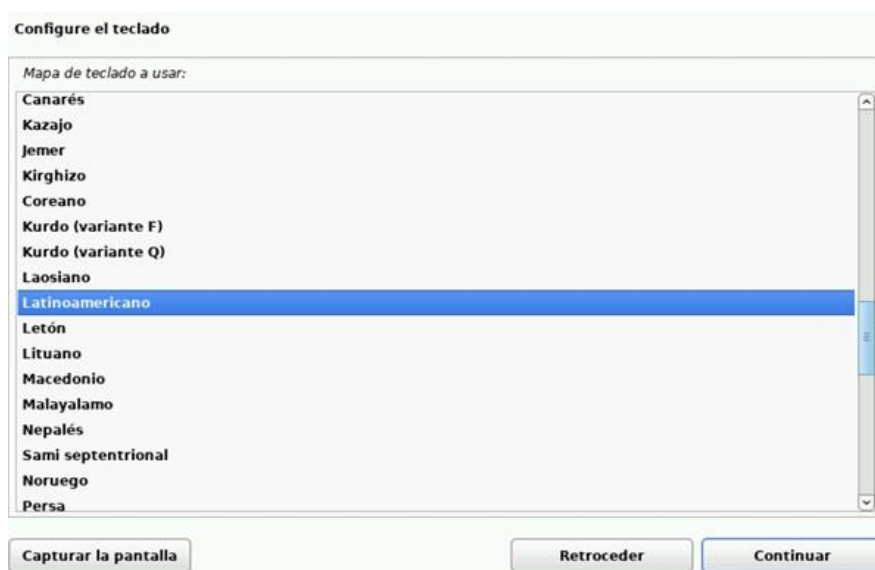
Al iniciar la máquina virtual, se mostrará la interfaz de Kali Linux. En esta pantalla, selecciona la primera opción que dice **Graphical Install** para comenzar con la instalación gráfica, como se muestra en la siguiente imagen.



A continuación, se te pedirá elegir el idioma que deseas utilizar durante la instalación. Selecciona el idioma deseado y luego haz clic en el botón **Continue** para continuar con el proceso, como se puede observar en la siguiente imagen.



Después, seleccionamos el país de origen, y después damos continuar:



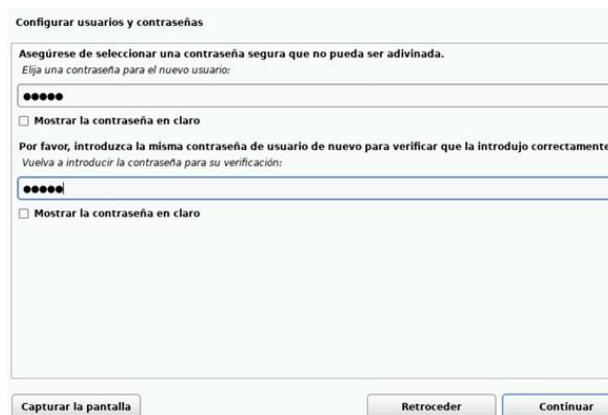
Después de seleccionar el idioma, el siguiente paso es asignar un ****nombre**** a tu máquina virtual. Ingresa un nombre identificativo para la máquina y, una vez completado, haz clic en el botón ****"Continuar"**** para seguir con el proceso de instalación, como se muestra en la siguiente imagen.



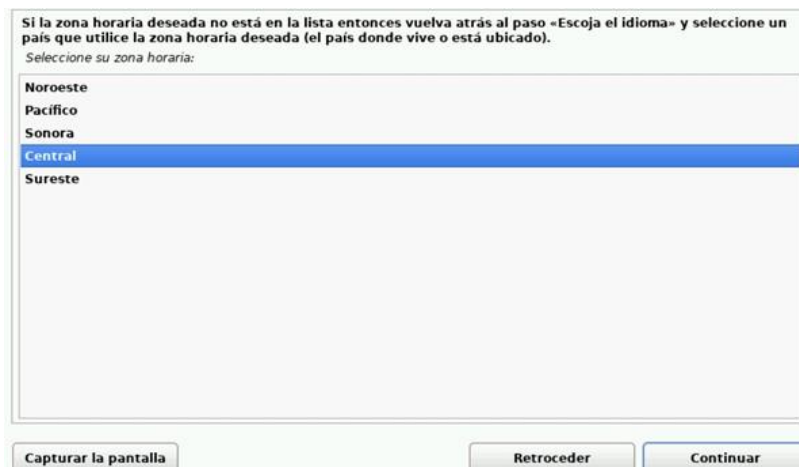
Después de asignar el nombre de la máquina virtual, el siguiente paso es asignar un **nombre de usuario** para la máquina virtual. Ingresas el nombre de usuario deseado y, después, haz clic en **Continuar**.



A continuación, se te pedirá establecer una **contraseña**. Ingresas la contraseña en el primer campo y luego confírmala escribiéndola nuevamente en el segundo campo. Una vez completado, haz clic en **Continuar** para continuar con el proceso, como se muestra en la siguiente imagen.

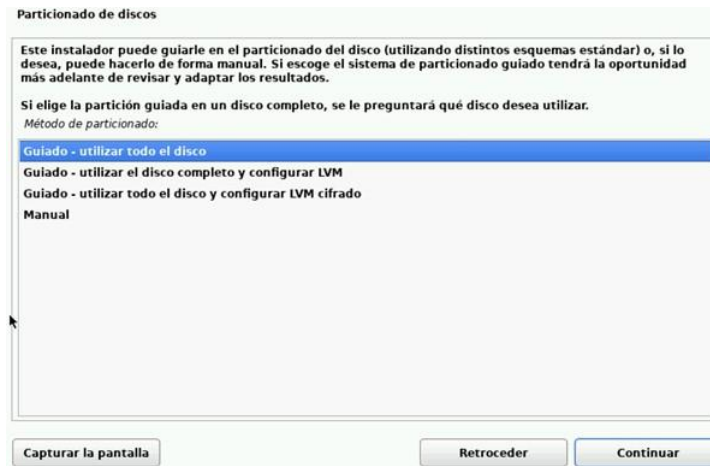


En este paso, deberás configurar la **zona horaria** de la máquina según tu ubicación. Para ello, selecciona la opción **Central** (o la zona horaria que corresponda) y luego haz clic en **Continuar**, como se muestra en la siguiente imagen.

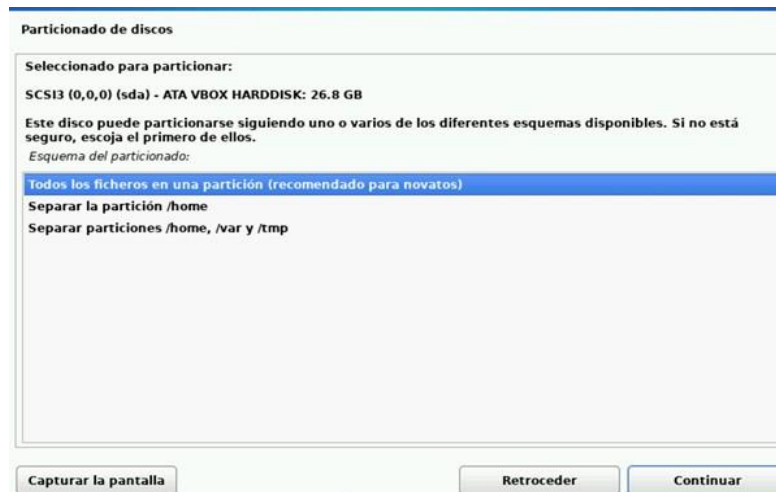


A continuación, se te pedirá elegir una opción para **particionar el disco**. Selecciona la primera opción, **Guiado – usar todo el disco**, que permite utilizar todo el espacio

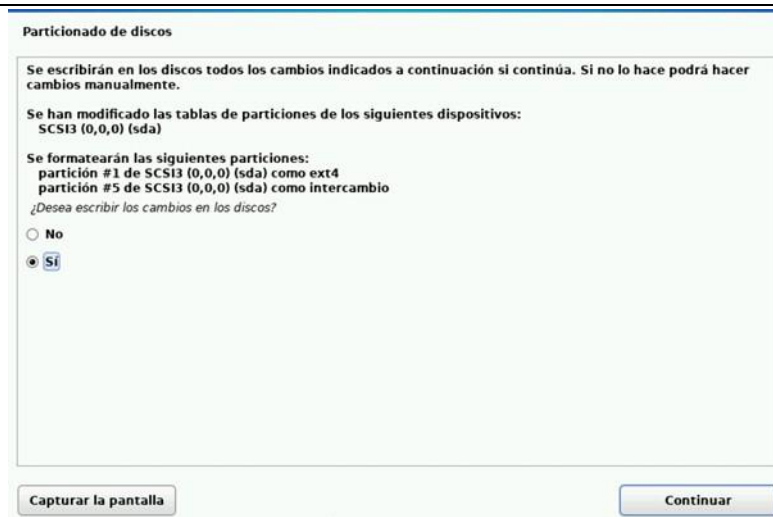
disponible en el disco para la instalación del sistema operativo. Después, haz clic en **"Continuar"** para proceder, como se muestra en la siguiente imagen.



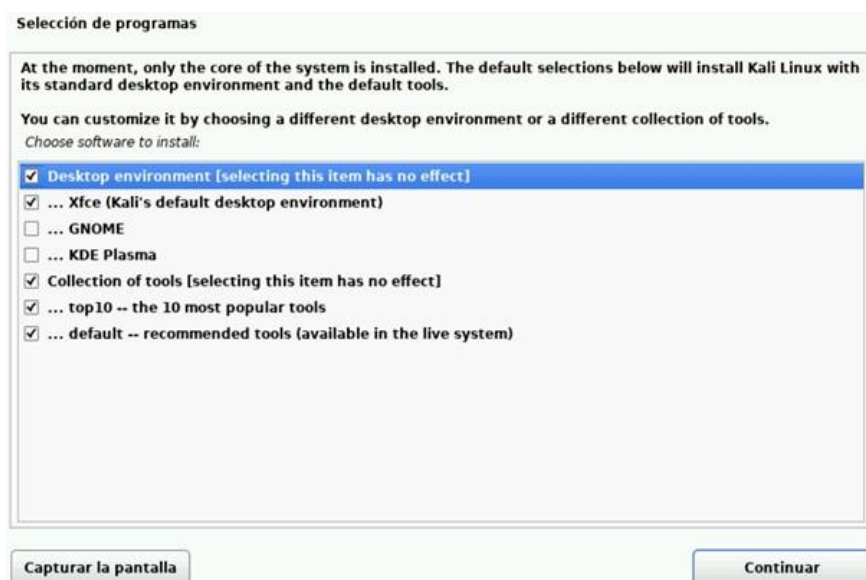
Después de seleccionar **"Guiado – usar todo el disco"**, mantén la primera opción predeterminada y haz clic en **"Continuar"** para seguir con el proceso de particionado, como se muestra en la siguiente imagen.



A continuación, aparecerá una ventana de confirmación que te mostrará todos los cambios realizados en el disco. Para confirmar que deseas continuar con estos cambios, selecciona la opción **"Sí"** y luego haz clic en **"Continuar"** para proceder, como se muestra en la siguiente imagen.



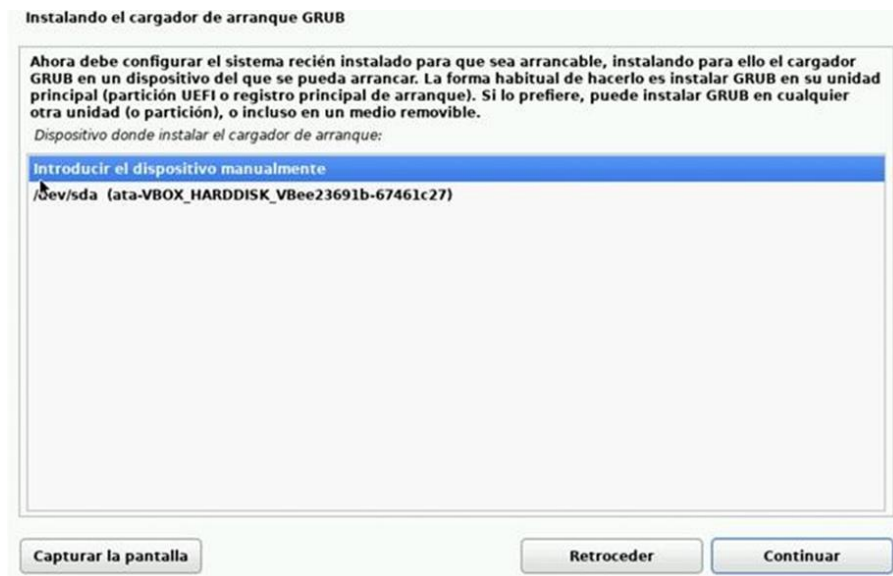
A continuación, aparecerá una ventana donde se te pedirá elegir el tipo de **programa** que deseas instalar. Deja las opciones predeterminadas seleccionadas, ya que son las más adecuadas para la instalación estándar, y luego haz clic en el botón **"Continuar"**, como se muestra en la siguiente imagen.



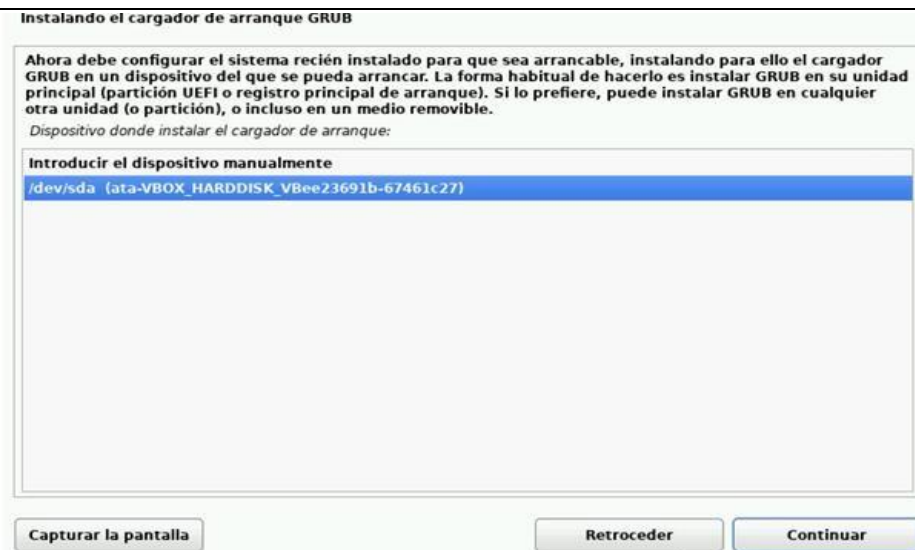
Posteriormente, aparecerá un mensaje de advertencia relacionado con la instalación del **cargador de arranque GRUB**. Este cargador es necesario para que el sistema operativo arranque correctamente. Selecciona la opción **"Sí"** para proceder con la instalación de GRUB, y luego haz clic en **"Continuar"**, como se puede observar en la siguiente imagen.



En este paso, selecciona la primera opción para configurar el dispositivo ****manual****. Luego, haz clic en ****"Continuar"**. Este proceso puede tardar algunos minutos mientras se configura el sistema.**



Después, asegúrate de que el apartado predeterminado para la instalación del ****cargador de arranque GRUB**** esté seleccionado, ya que es esencial para que el sistema operativo arranque correctamente. Haz clic en ****"Continuar"**. para proceder con la instalación, como se muestra en la siguiente imagen.**



Una vez que la instalación haya finalizado, aparecerá un mensaje indicando que el proceso se completó y que es necesario reiniciar la máquina. Haz clic en el botón **"Continuar"** para reiniciar el sistema.



Después de reiniciar, se te pedirá que ingreses el ****nombre de usuario**** y la ****contraseña**** que configuraste durante la instalación. Ingresa tus credenciales y presiona ****Enter**** para acceder a la interfaz de ****Kali Linux**** y continuar con el uso del sistema.

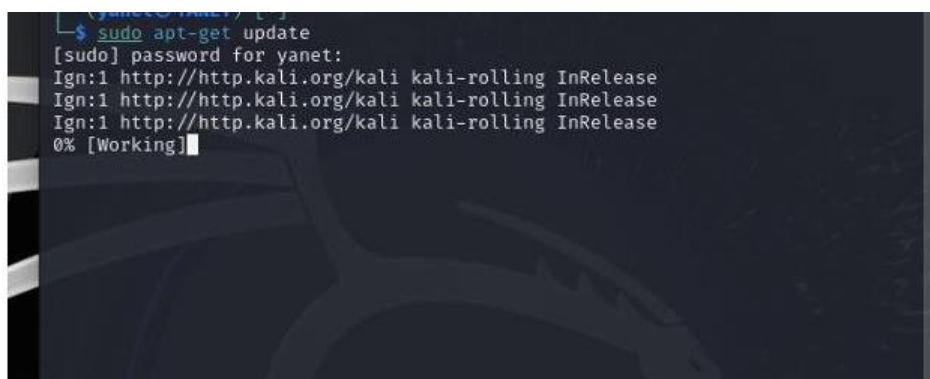


Después del reinicio, se te pedirá ingresar el **nombre de usuario** y la **contraseña** que configuraste durante la instalación de Kali Linux. Al introducir los datos correctamente, accederás a la interfaz de **Kali Linux**, donde podrás comenzar a trabajar con el sistema.



INSTALAR UN SISTEMA DE DETECCIÓN DE INTRUSOS COMO SNORT O SURICATA:

Abre la **terminal** en Kali Linux y escribe el siguiente comando para actualizar la información sobre los paquetes disponibles y sus versiones en los repositorios: **“bash sudo apt-get update”** Este comando **solo descarga la información más reciente** de los paquetes y sus versiones disponibles, pero no realiza ninguna instalación ni actualización de los paquetes en sí. Espera a que termine el proceso antes de continuar.



Una vez completado el paso anterior, ingresa el siguiente comando para instalar los paquetes y dependencias necesarias en Kali Linux:

```
sudo apt-get install libpcap3-dbg libpcap3-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 una serie de bibliotecas y herramientas requeridas para configurar **Suricata**, el motor de detección y prevención de intrusiones (IDS/IPS). Espera a que todos los paquetes se descarguen e instalen correctamente.

```

$ 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

```

A continuación, para instalar **Suricata**, ejecuta el siguiente comando:

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

Este comando instalará Suricata en Kali Linux. Al igual que con el paso anterior, espera 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

```

Después de completar la instalación de Suricata, aparecerá un mensaje indicando que algunos de los servicios instalados requieren un reinicio para aplicar las actualizaciones. Selecciona "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>

```

El sistema comenzará a actualizar todos los servicios mencionados previamente en el mensaje. Espera a que el proceso termine.


```
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) ...
```

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.

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

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
```

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.

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

Ingresamos al directorio con el siguiente comando.

```
$ cd /var/lib/suricata/rules
```

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
```

CONFIGURAR LAS REGLAS DE DETECCIÓN DE INTRUSOS.

En este paso, vamos a configurar **reglas personalizadas** en **Suricata**, un motor de detección y prevención de intrusiones (IDS/IPS), para identificar patrones de tráfico específicos en la red. Estas reglas están diseñadas para 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.

Una vez configuradas las reglas, para guardar los cambios realizados, utiliza el comando **Ctrl + O** seguido de **Enter**. Para salir del editor de texto, usa **Ctrl + X**. Esto asegurará que las reglas personalizadas queden guardadas y activas en Suricata.

```
GNU nano 2.1 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;)
```

CONFIGURAR LAS ALERTAS DE DETECCIÓN DE INTRUSOS

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.

```
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
```

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
```

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 específica. Al ejecutar el comando, el sistema solicitará la **contraseña** del usuario para proceder con la ejecución de Suricata. Una vez que se ingrese la contraseña correctamente, Suricata comenzará a cargar y a activarse, monitoreando el tráfico de red en tiempo real. Durante este proceso, Suricata detectará y generará alertas sobre posibles amenazas o intrusiones, siguiendo las reglas que se hayan configurado previamente en el sistema.

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

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 intrusos (IDS/IPS) de Suricata. Al utilizar el comando **tail -f**, se visualizan las últimas líneas del archivo y cualquier nuevo evento que ocurra se añadirá automáticamente en tiempo real. Esto permite monitorear continuamente las alertas y actividades de red detectadas por Suricata, proporcionando una visión actualizada de las posibles amenazas e intrusiones, como se muestra en la siguiente imagen.

```
$ 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
```

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

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

ASIGNAR UNA DIRECCIÓN IP ESTÁTICA A KALI LINUX.

```
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
```

Posteriormente en este apartado se ingresa lo que se muestra a continuación, guardamos cambios y salimos de la configuración, como se muestra a continuación en la siguiente imagen:

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.

```
$ sudo systemctl restart networking
```

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.

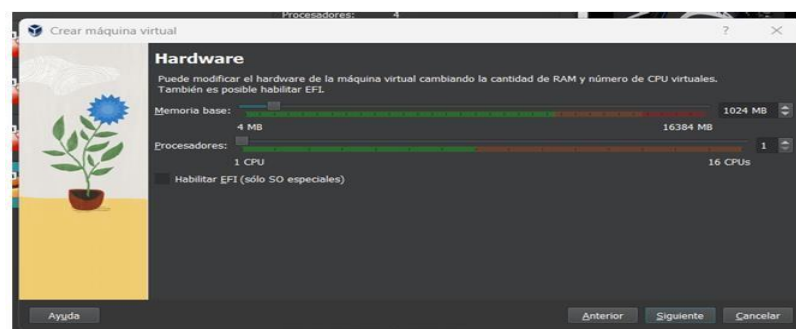
```
$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:47:77:54 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.110/24 brd 192.168.1.255 scope global dynamic noprefroute eth0
        valid_lft 5292sec preferred_lft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

CREAR UNA MÁQUINA VIRTUAL VULNERABLE POR DISEÑO COMO METASPLOITABLE2:

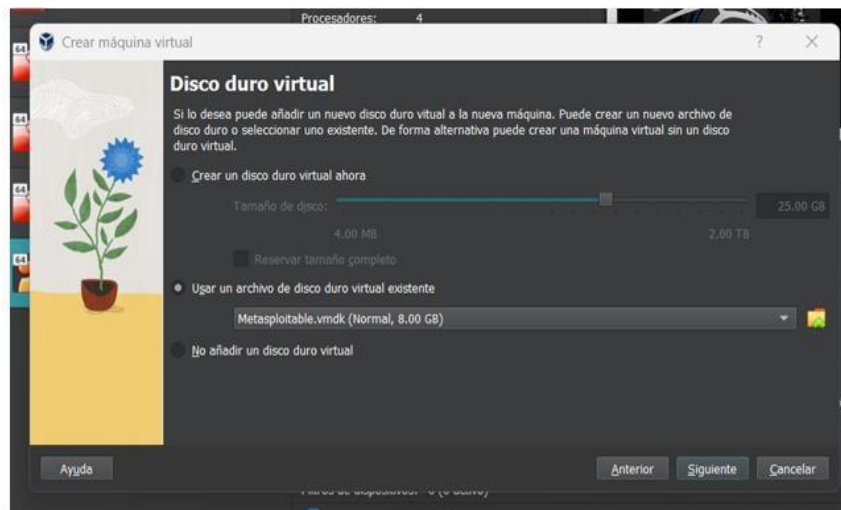
Configuramos una nueva máquina virtual llamada MetaSploitable2, seleccionamos "Linux" como tipo y, en la opción de versión, elegimos "Other Linux (64-bit)", luego hacemos clic en el botón "Siguiente".



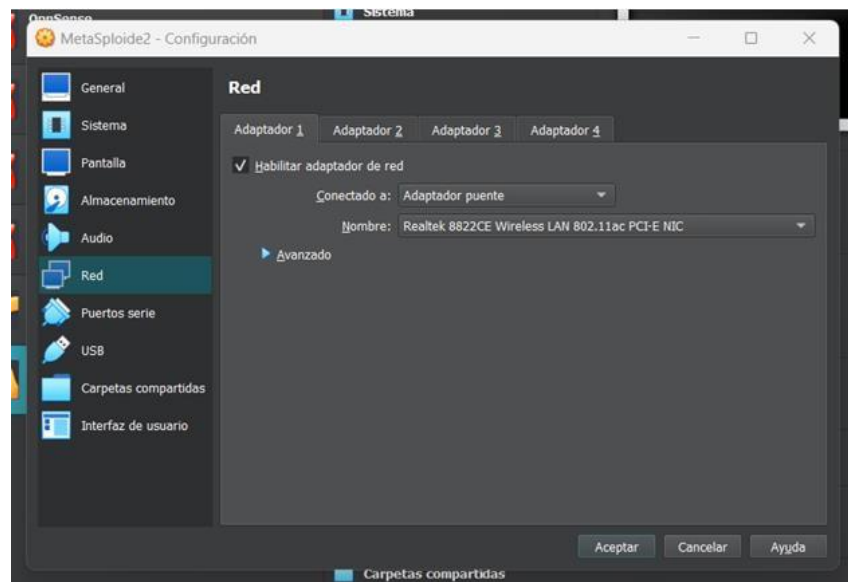
En la configuración de hardware, asignamos 1 GB de memoria RAM y dejamos los procesadores con la configuración predeterminada. Luego, hacemos clic en "Siguiente".

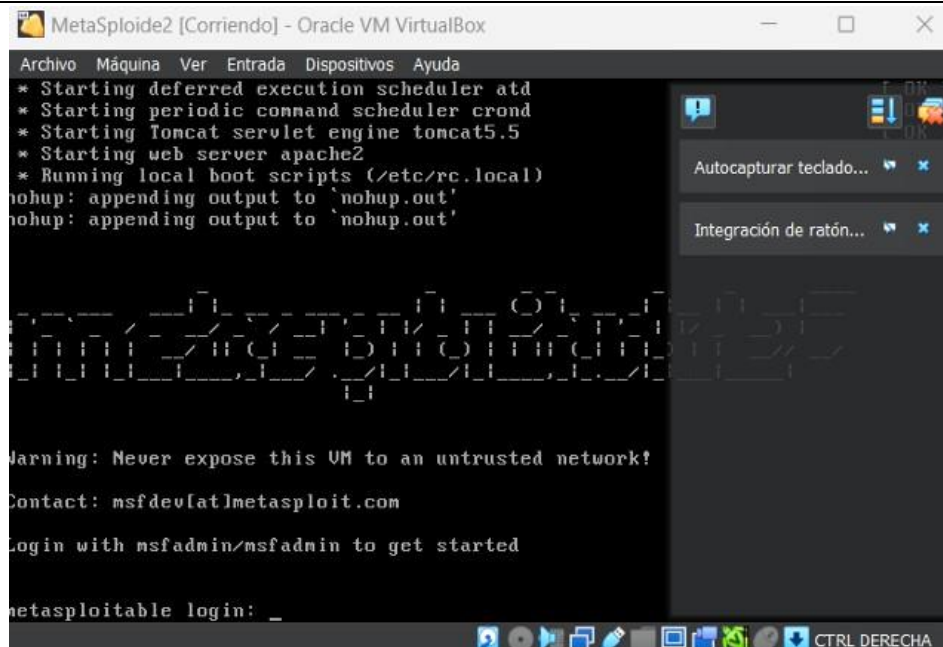


Asignamos 25 GB de espacio de almacenamiento y activamos la opción para utilizar un archivo de disco duro virtual existente. Seleccionamos el archivo ISO y luego hacemos clic en el botón "Siguiente" para continuar, como se muestra a continuación en la siguiente imagen:



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, como se muestra a continuación en la siguiente imagen:





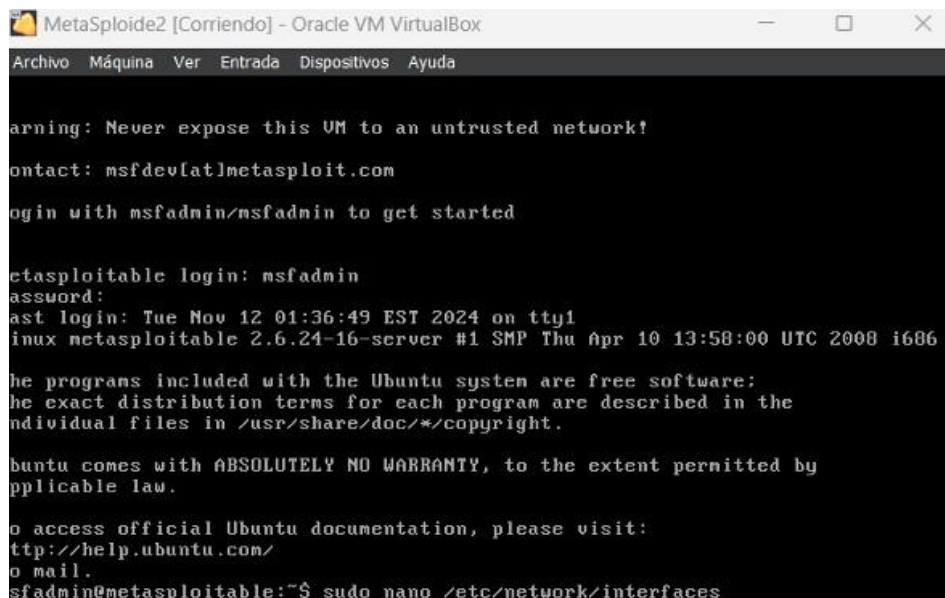
```
MetaSploide2 [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
* Starting deferred execution scheduler atd
* Starting periodic command scheduler crond
* Starting Tomcat servlet engine tomcat5.5
* Starting web server apache2
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out'

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

metasploitable login: _
```

Al iniciar la máquina virtual, comenzará a cargar y nos solicitará que ingresamos el nombre de usuario y la contraseña.

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
```

ASIGNAR UNA DIRECCIÓN IP ESTÁTICA A METASPLOITABLES2:

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 ^U Next Page ^U UnCut Text ^T To Spell

Ingresamos el siguiente comando para reiniciar los servicios de red.

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

Verificamos que los cambios se hayan aplicado correctamente.

MetaSploide2 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

[Wrote 14 lines]

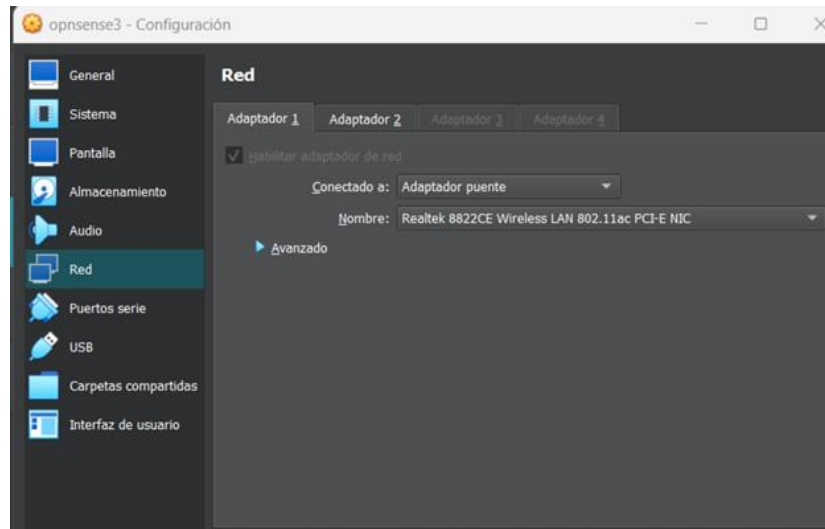
```
msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart
* Reconfiguring network interfaces... [ OK ]
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:7d:a9:c2
          inet addr:192.168.1.120  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 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:~$ _
```

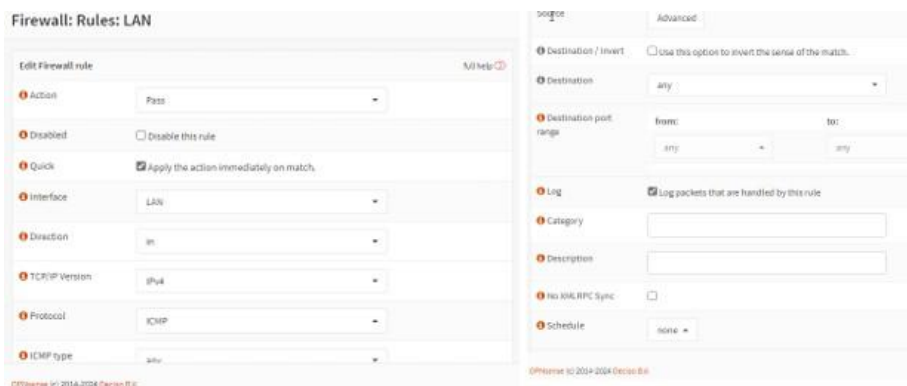
PING SATISFACTORIO ENTRE LAS MÁQUINAS VIRTUALES:

Para realizar un ping exitoso entre las máquinas virtuales, necesitamos seguir los siguientes pasos, como se muestra a continuación en la siguiente imagen:

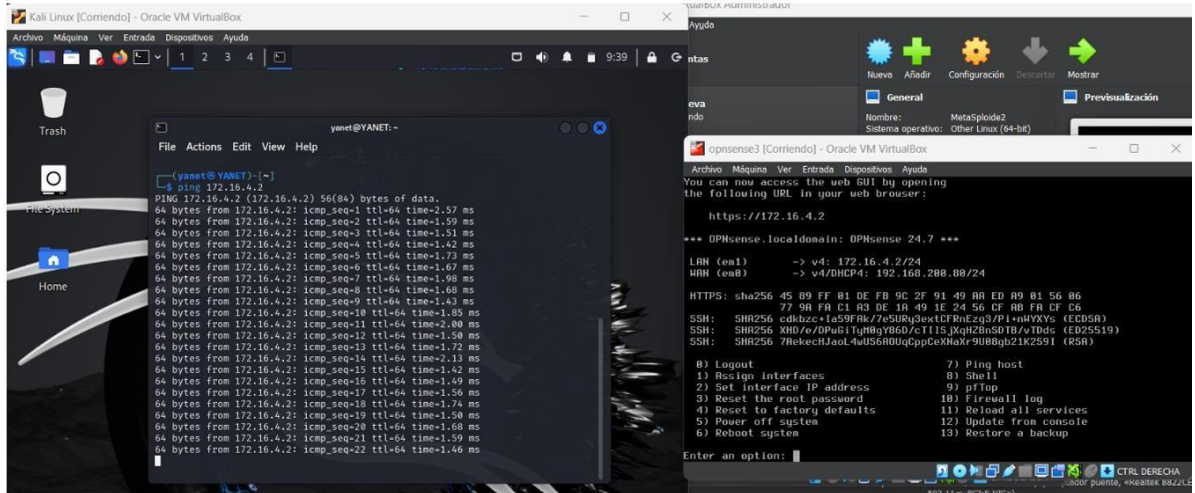


CONFIGURAR LAS REGLAS DE FIREWALL PARA PERMITIR EL TRÁFICO DE PING:

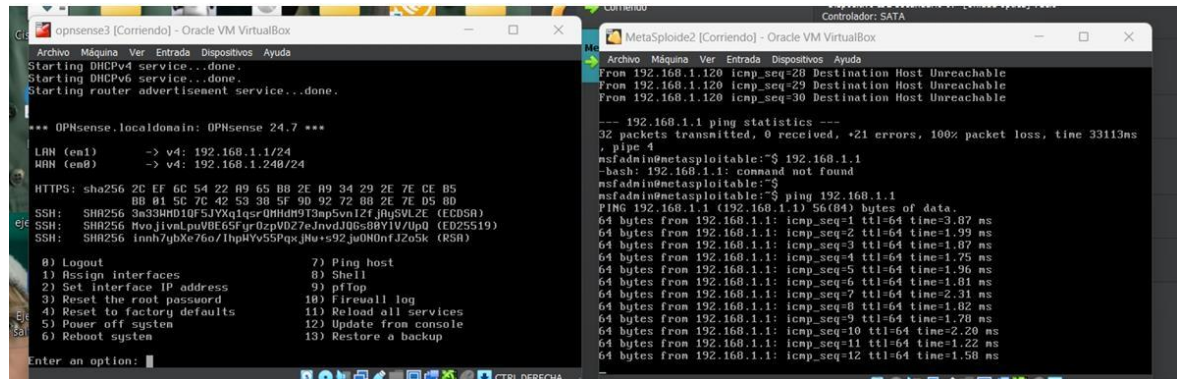
Configurar correctamente las reglas del firewall para permitir el tráfico de ping es esencial para probar la conectividad entre máquinas virtuales, como se muestra a continuación en la siguiente imagen:



REALIZAR UN PING ENTRE LAS MÁQUINAS VIRTUALES:



```
yamet@YANET:~$ ping 172.16.4.2
PING 172.16.4.2 (172.16.4.2) 56(84) bytes of data:
64 bytes from 172.16.4.2: icmp_seq=1 ttl=64 time=2.57 ms
64 bytes from 172.16.4.2: icmp_seq=2 ttl=64 time=1.59 ms
64 bytes from 172.16.4.2: icmp_seq=3 ttl=64 time=1.51 ms
64 bytes from 172.16.4.2: icmp_seq=4 ttl=64 time=1.42 ms
64 bytes from 172.16.4.2: icmp_seq=5 ttl=64 time=1.73 ms
64 bytes from 172.16.4.2: icmp_seq=6 ttl=64 time=1.67 ms
64 bytes from 172.16.4.2: icmp_seq=7 ttl=64 time=1.98 ms
64 bytes from 172.16.4.2: icmp_seq=8 ttl=64 time=1.68 ms
64 bytes from 172.16.4.2: icmp_seq=9 ttl=64 time=1.43 ms
64 bytes from 172.16.4.2: icmp_seq=10 ttl=64 time=1.85 ms
64 bytes from 172.16.4.2: icmp_seq=11 ttl=64 time=2.00 ms
64 bytes from 172.16.4.2: icmp_seq=12 ttl=64 time=1.50 ms
64 bytes from 172.16.4.2: icmp_seq=13 ttl=64 time=1.72 ms
64 bytes from 172.16.4.2: icmp_seq=14 ttl=64 time=2.13 ms
64 bytes from 172.16.4.2: icmp_seq=15 ttl=64 time=1.42 ms
64 bytes from 172.16.4.2: icmp_seq=16 ttl=64 time=1.49 ms
64 bytes from 172.16.4.2: icmp_seq=17 ttl=64 time=1.56 ms
64 bytes from 172.16.4.2: icmp_seq=18 ttl=64 time=1.74 ms
64 bytes from 172.16.4.2: icmp_seq=19 ttl=64 time=1.50 ms
64 bytes from 172.16.4.2: icmp_seq=20 ttl=64 time=1.68 ms
64 bytes from 172.16.4.2: icmp_seq=21 ttl=64 time=1.59 ms
64 bytes from 172.16.4.2: icmp_seq=22 ttl=64 time=1.46 ms
```



```
*** OPNsense.localdomain: OPNsense 24.7 ***
LRN (en1) -> v4: 192.168.1.1/24
WRN (en0) -> v4: 192.168.1.248/24

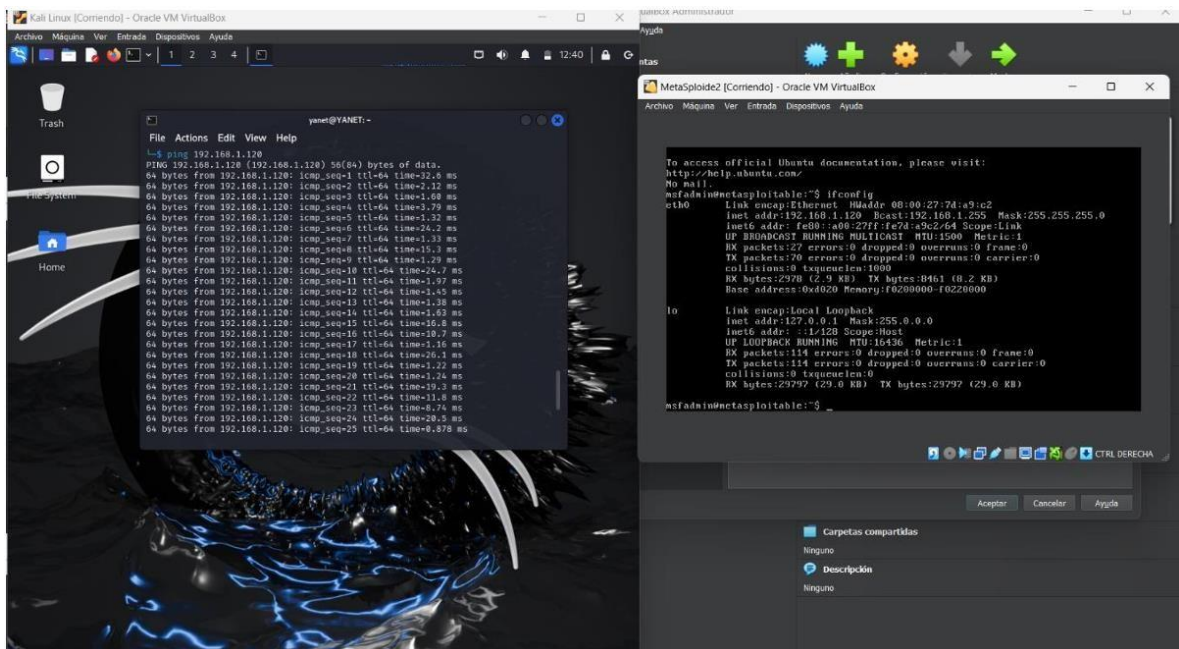
HTTPS: sha256 2C 7F 6C 54 22 A9 65 80 2E A9 34 29 2E 7E CE 85
      BB 81 5C 7C 42 53 30 5F 9D 92 72 88 2E 7E D5 8D
SSH:   SHA256 3a33MHD1QF5JYXqIqsrQHdmd9I3ap5vn12fJhJ5VLZE (ECDSA)
SSH:   SHA256 RvoJjvalpuVBE65fyrQzpV027eJndJQ6s8BY1VUpQ (ED25519)
SSH:   SHA256 inn7gbKx76o71hpHfV55PqKJhu+s92jUd0Nt1J3oSk (RSA)

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

Enter an option: 7
```

```
From 192.168.1.120 icmp_seq=28 Destination Host Unreachable
From 192.168.1.120 icmp_seq=29 Destination Host Unreachable
From 192.168.1.120 icmp_seq=30 Destination Host Unreachable

--- 192.168.1.1 ping statistics ---
32 packets transmitted, 0 received, +21 errors, 100% packet loss, time 33113ms
, pipe 4
msfadmin@metasploitable:~$ ping 192.168.1.1
-bash: ping: command not found
msfadmin@metasploitable:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data:
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=3.87 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=1.99 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=1.07 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=1.75 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=1.90 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=1.81 ms
64 bytes from 192.168.1.1: icmp_seq=7 ttl=64 time=2.31 ms
64 bytes from 192.168.1.1: icmp_seq=8 ttl=64 time=1.82 ms
64 bytes from 192.168.1.1: icmp_seq=9 ttl=64 time=1.70 ms
64 bytes from 192.168.1.1: icmp_seq=10 ttl=64 time=2.20 ms
64 bytes from 192.168.1.1: icmp_seq=11 ttl=64 time=1.22 ms
64 bytes from 192.168.1.1: icmp_seq=12 ttl=64 time=1.50 ms
```



```
yamet@YANET:~$ 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=32.6 ms
64 bytes from 192.168.1.120: icmp_seq=2 ttl=64 time=1.22 ms
64 bytes from 192.168.1.120: icmp_seq=3 ttl=64 time=1.68 ms
64 bytes from 192.168.1.120: icmp_seq=4 ttl=64 time=3.79 ms
64 bytes from 192.168.1.120: icmp_seq=5 ttl=64 time=1.32 ms
64 bytes from 192.168.1.120: icmp_seq=6 ttl=64 time=26.2 ms
64 bytes from 192.168.1.120: icmp_seq=7 ttl=64 time=1.33 ms
64 bytes from 192.168.1.120: icmp_seq=8 ttl=64 time=1.51 ms
64 bytes from 192.168.1.120: icmp_seq=9 ttl=64 time=1.79 ms
64 bytes from 192.168.1.120: icmp_seq=10 ttl=64 time=24.7 ms
64 bytes from 192.168.1.120: icmp_seq=11 ttl=64 time=1.97 ms
64 bytes from 192.168.1.120: icmp_seq=12 ttl=64 time=2.15 ms
64 bytes from 192.168.1.120: icmp_seq=13 ttl=64 time=1.38 ms
64 bytes from 192.168.1.120: icmp_seq=14 ttl=64 time=1.63 ms
64 bytes from 192.168.1.120: icmp_seq=15 ttl=64 time=10.8 ms
64 bytes from 192.168.1.120: icmp_seq=16 ttl=64 time=10.7 ms
64 bytes from 192.168.1.120: icmp_seq=17 ttl=64 time=1.16 ms
64 bytes from 192.168.1.120: icmp_seq=18 ttl=64 time=26.1 ms
64 bytes from 192.168.1.120: icmp_seq=19 ttl=64 time=1.22 ms
64 bytes from 192.168.1.120: icmp_seq=20 ttl=64 time=1.24 ms
64 bytes from 192.168.1.120: icmp_seq=21 ttl=64 time=19.3 ms
64 bytes from 192.168.1.120: icmp_seq=22 ttl=64 time=11.8 ms
64 bytes from 192.168.1.120: icmp_seq=23 ttl=64 time=8.74 ms
64 bytes from 192.168.1.120: icmp_seq=24 ttl=64 time=29.5 ms
64 bytes from 192.168.1.120: icmp_seq=25 ttl=64 time=8.87 ms
```

```
msfadmin@metasploitable:~$ ifconfig
eth0: Link encap:Ethernet HWaddr 08:00:27:74:a9:c2
      inet addr:192.168.1.120 Bcast:192.168.1.255 Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fe74:a9c2:64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:27 errors:0 dropped:0 overruns:0 frame:0
      TX packets:114 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:2970 (2.9 KB) TX bytes:8461 (8.2 KB)
      Base address: 0x4020 Memory: f6200000-f6200000

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:65536 Metric:1
      RX packets:114 errors:0 dropped:0 overruns:0 frame:0
      TX packets:114 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:29797 (29.8 KB) TX bytes:29797 (29.8 KB)

msfadmin@metasploitable:~$
```

CONCLUSIÓN

La implementación de este laboratorio de seguridad en Kali Linux ha proporcionado una comprensión profunda de cómo configurar un sistema de detección y prevención de intrusos (IDS/IPS) en una red. A través de la instalación de herramientas como **Suricata**, y la configuración de reglas personalizadas para detectar patrones de tráfico específicos, como intentos de conexión ICMP, SSH y posibles ataques DDoS, se ha mejorado la capacidad para identificar y mitigar amenazas. Además, al asignar una **dirección IP estática** a Kali Linux y reiniciar los servicios de red, se garantizó una conectividad estable, permitiendo que el sistema esté siempre accesible y configurado correctamente para monitorear el tráfico de red.

El uso del comando **tail -f** para monitorear el archivo **fast.log** de Suricata en tiempo real permitió seguir de cerca las alertas y actividades de red, ofreciendo visibilidad continua sobre posibles intrusiones. Todo este proceso fortaleció las habilidades prácticas en ciberseguridad, destacando la importancia de una correcta configuración de las herramientas de monitoreo y la integración de reglas personalizadas para la protección efectiva de una infraestructura de red.

BIBLIOGRAFIAS:

<https://www.universitatcarlemany.com/actualidad/blog/seguridad-informatica-que-es/>

<https://aws.amazon.com/es/what-is/cybersecurity/#:~:text=La%20ciberseguridad%20es%20la%20pr%C3%A1ctica,cliente%20y%20cumplir%20la%20normativa>

<https://www.cesuma.mx/blog/que-tipos-de-ciberseguridad-existen.html>

<https://insights.encora.com/es/blog/que-es-ciberseguridad-un-enfoque-practico#:~:text=En%20conclusi%C3%B3n%2C%20la%20ciberseguridad%20en,caos%20dentro%20de%20una%20compa%C3%B1%C3%ADa>