



TECNOLOGICO NACIONAL DE MEXICO
INSTITUTO TECNOLÓGICO DE TLAXIACO

INTEGRANTES:

JULISSA MIGDALIA JOSE CRUZ

LUZ MARIA MENDOZA CORTES

MAYTE ELISAHAD LEON DE JESUS

ANGELES GONZÁLEZ MARTÍNEZ

DOCENTE:

ING. EDWARD OSORIO SALINAS

MATERIA:

SEGURIDAD Y VIRTUALIZACION

GRUPO: 7US

SEMESTRE: SEPTIMO

FECHA:10 DE NOVIEMBRE DEL 2024



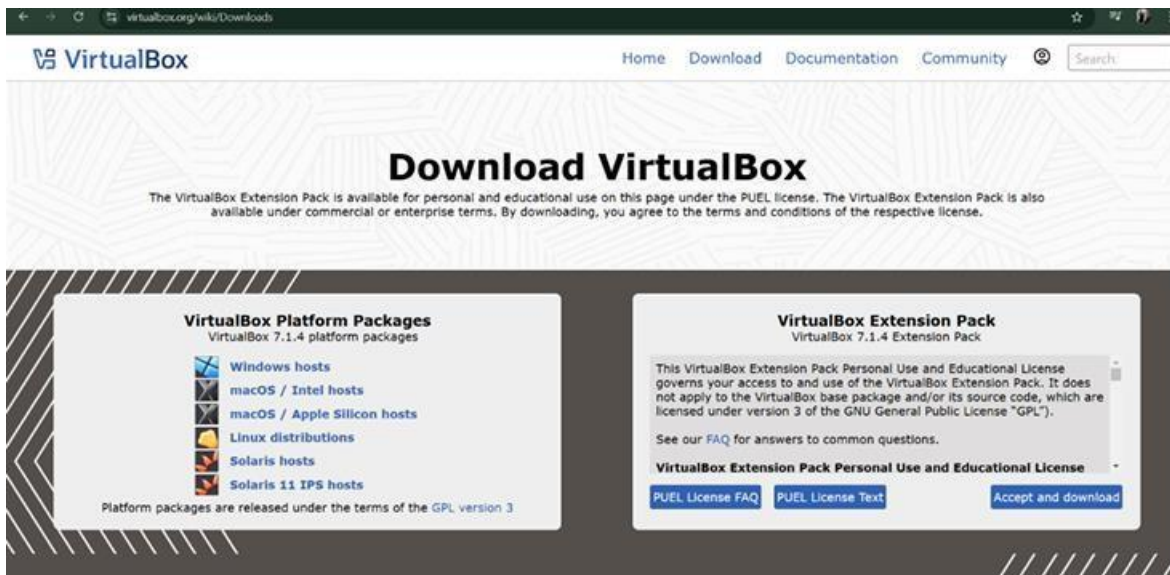
INTRODUCCION:

En la Práctica 6 de la Unidad 2 sobre virtualización, realicé un laboratorio de seguridad utilizando plataformas como VirtualBox y VMware. En este laboratorio, instalé y configuré un firewall con OpnSense o pfSense, un sistema de detección de intrusos usando Kali Linux, y una máquina vulnerable, MetaSploitable2. Este entorno me permitió experimentar con herramientas de seguridad y comprender cómo interactúan entre sí para defender una red. A lo largo de la práctica, el objetivo fue simular situaciones reales de ciberseguridad para mejorar mis habilidades en la detección y respuesta ante amenazas.



1. INSTALAR VIRTUALBOX.

Principalmente nos dirigimos al sitio de VirtualBox donde lo encontramos en el siguiente enlace <https://www.virtualbox.org> . Una vez ahí, buscamos el apartado llamado "**DOWNLOADS**" y hacemos clic en ello para comenzar la descarga. Posteriormente en este caso elegimos en la cual vamos a trabajar, para esto damos clic en "Windows host", como se puede mostrar a continuación en la siguiente imagen:



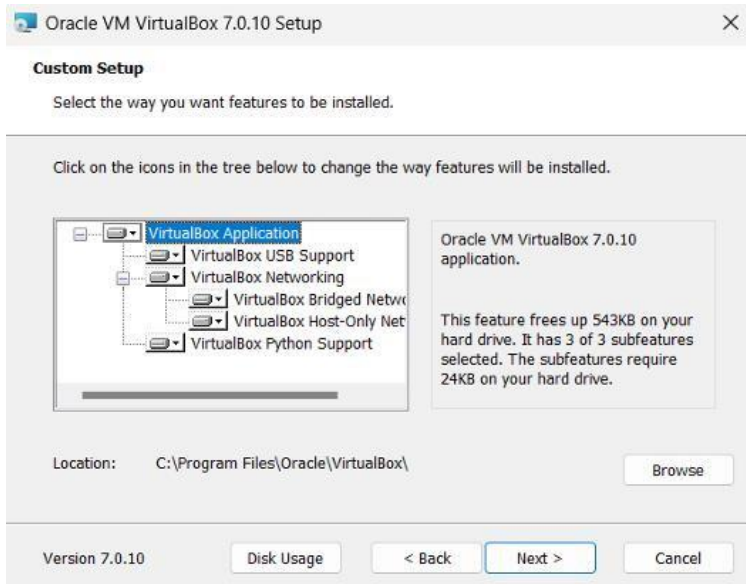
Después una vez descargado el archivo nos debe aparecer de la siguiente manera. Para después poder ejecutarlo y empezar con la instalación, como se puede mostrar a continuación en la siguiente imagen:



Después una vez hacemos al dar clic derecho y ejecutarlo como administrador, nos aparecerá la ventana de Bienvenida. Clic en "Next", como se puede mostrar a continuación en la siguiente imagen:



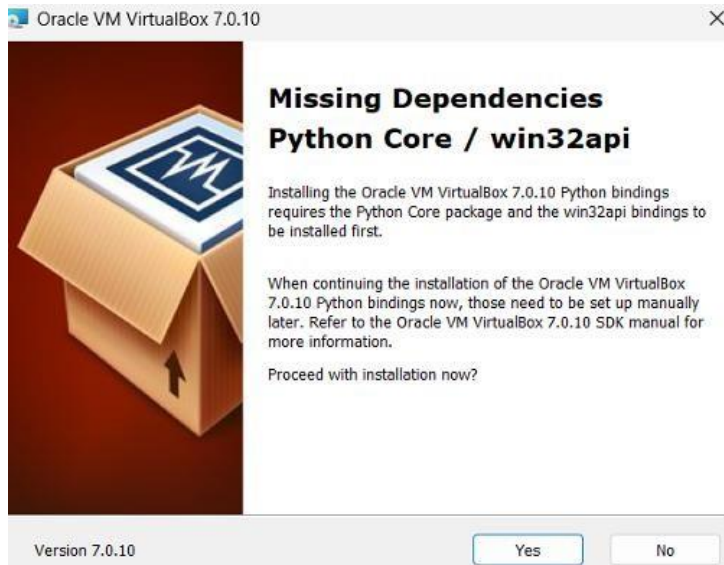
Después posteriormente en la pantalla de selección de características, nos muestra los componentes disponibles para instalar. Para este caso, mantendremos la configuración por defecto y simplemente seleccionamos "Next" para avanzar, como se puede ver a continuación en la siguiente imagen:



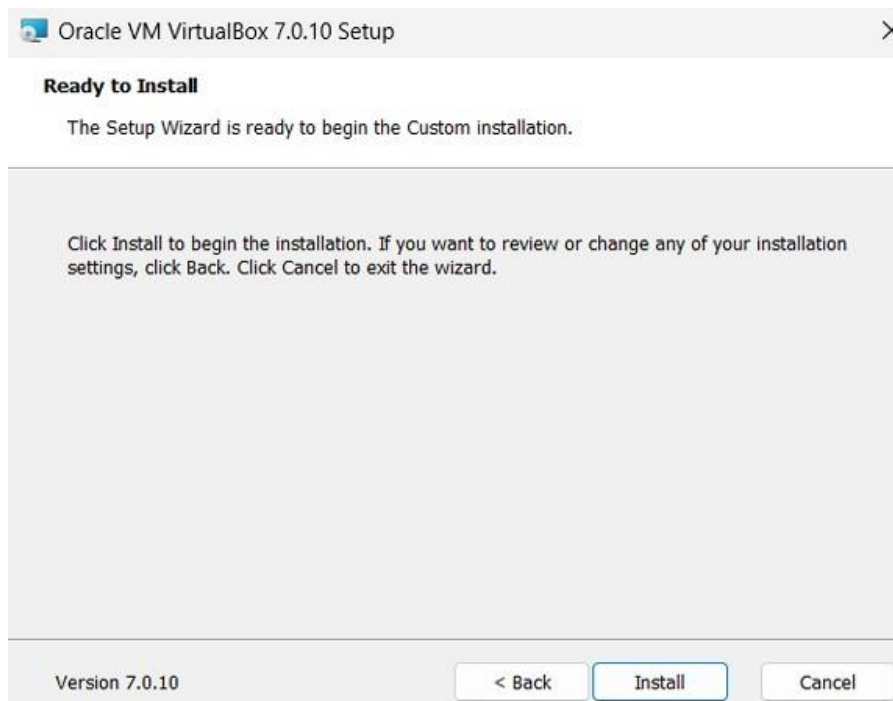
Después así mismo una vez dando click luego se abrirá una ventana con una advertencia relacionada con la interfaz de red. Para seguir con la instalación, seleccionamos “YES”, como se puede apreciar a continuación en la siguiente imagen:



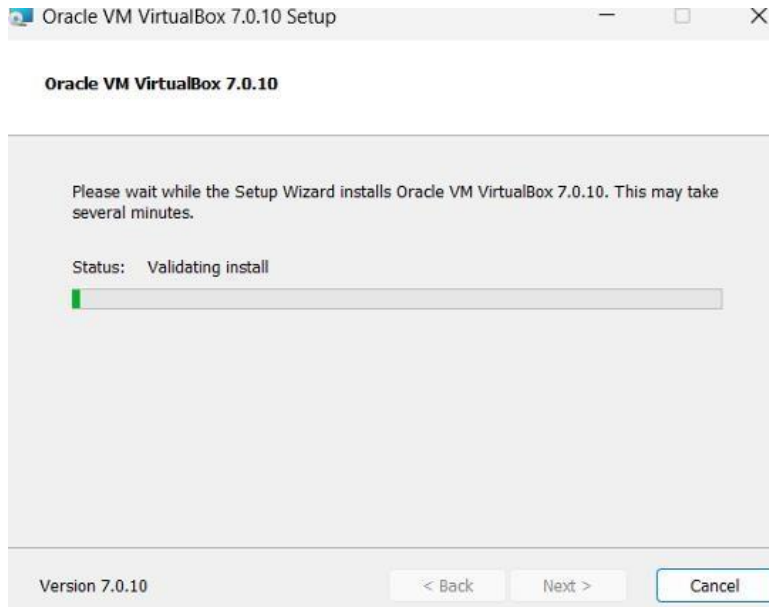
Posteriormente aparecerá la ventana de dependencias, en este caso de igual forma se le da “Yes” para que sigamos con la instalación, como se muestra a continuación en la siguiente imagen:



Despues en esta ventana se nos pedirá revisar los pasos anteriores por si queremos cambiar alguna opción. En este caso, simplemente seleccionamos "Install" para iniciar la instalación, como se muestra a continuación:



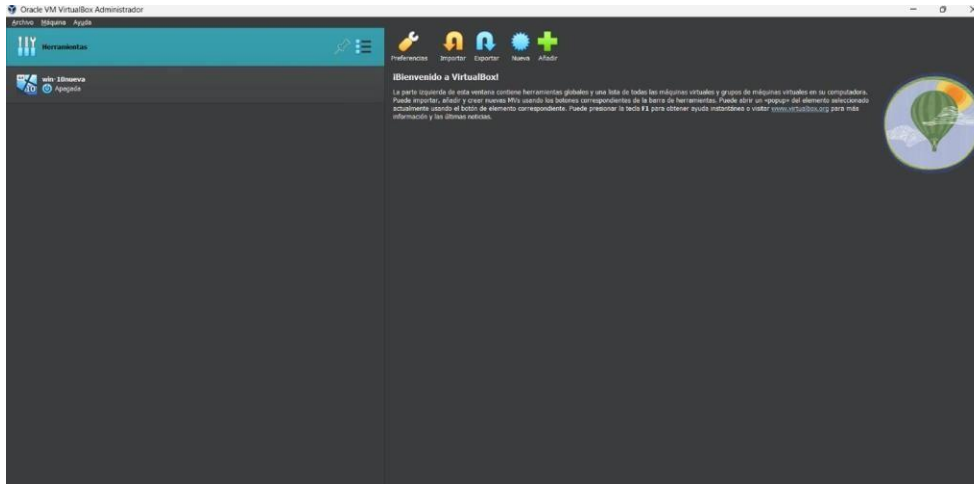
Posteriormente asi mismo esperar a que se complete la instalación y enseguida dar "Next", con este paso finalizaremos el proceso, como se muestra a continuación en la siguiente imagen:



Después una vez que se haya completado la instalación, nos aparecerá esta ventana, la cual quiere decir que el proceso fue un éxito, para esto, clic en “Finish”, como se puede apreciar a continuación en la siguiente imagen:



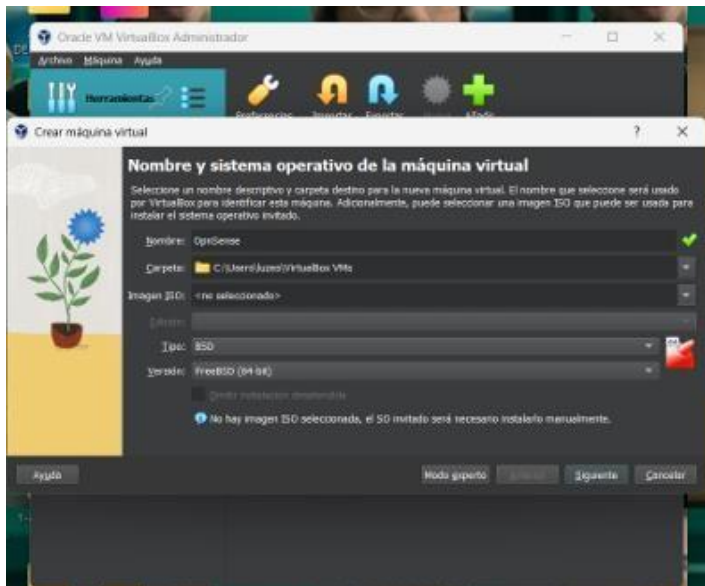
Después una vez al finalizar la instalación, procedemos a abrir “VirtualBox” y se verá de la siguiente forma, como se puede observar a continuación en la siguiente imagen:



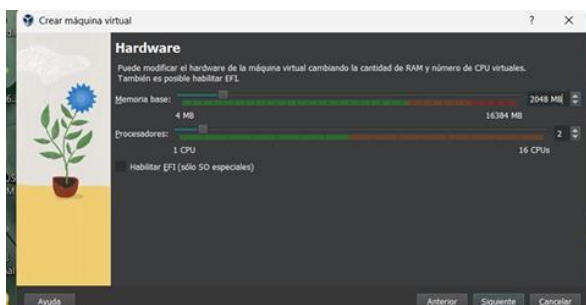
INSTALAR OPNSENSE O PFSENSE EN UNA MÁQUINA VIRTUAL Y CONFIGURAR UN FIREWALL.

INSTALACIÓN DE OPNSENSE EN UNA MÁQUINA VIRTUAL:

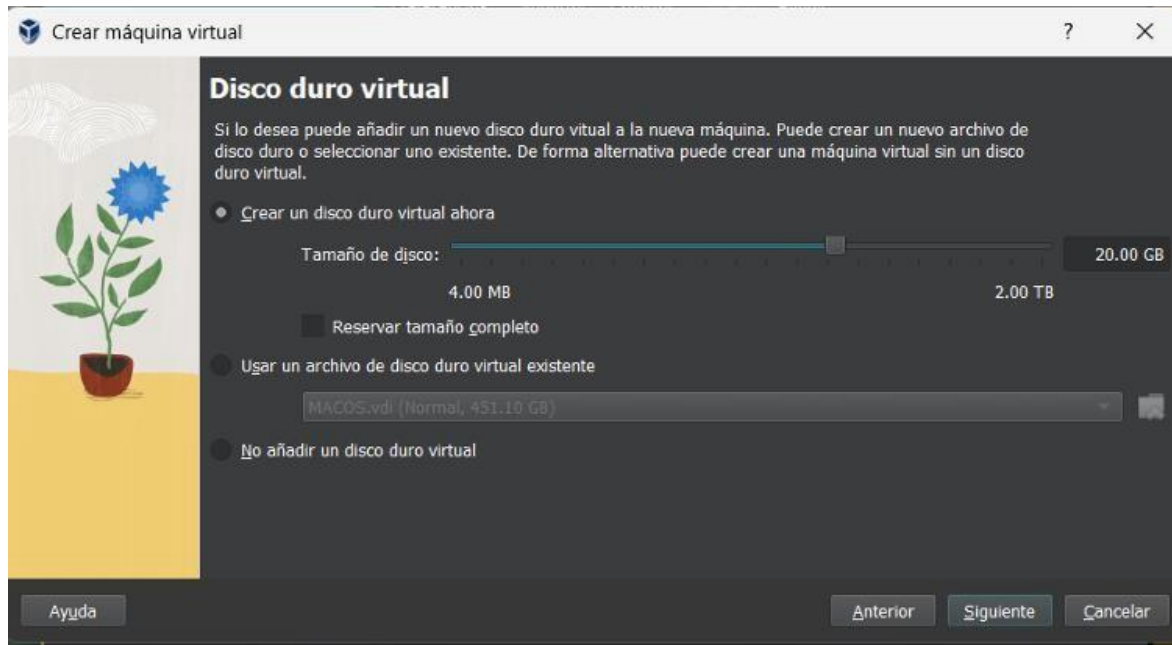
Principalmente le damos clic en “**Nueva**” para crear una máquina virtual de nombre “**OpnSense**” y seleccionamos en tipo BSD y la versión FreeBSD(64-bit), esto para que sea exitosa nuestra configuración, como se muestra a continuación en la siguiente imagen:



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 "Siguiendo". Como se puede observar a continuación en la siguiente imagen:



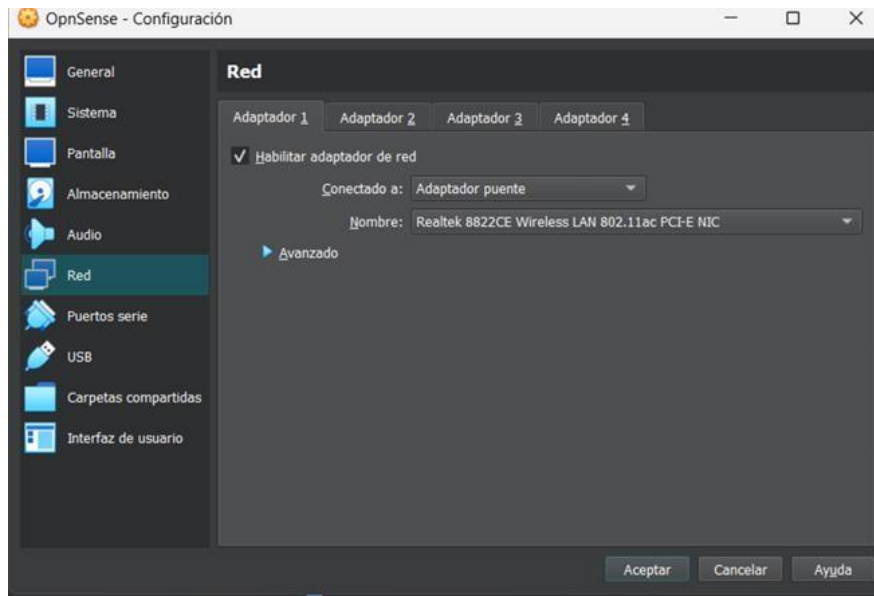
Después una vez instalado nos mostrará una ventana en la que nos pedirá especificar el espacio de almacenamiento para el sistema operativo que vamos a instalar. En este caso, asignamos 20 GB de espacio y, después, seleccionamos "Siguiendo" para continuar, como se puede observar a continuación en la siguiente imagen:



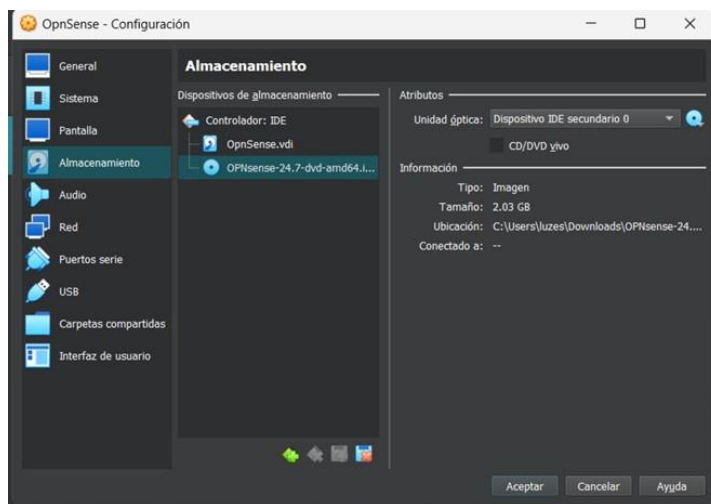
Después así mismo nos mostrará un resumen de lo que hemos seleccionado como queremos que sea nuestra máquina virtual. Una vez revisado bien, clic en "Terminar", como nos puede mostrar a continuación en la siguiente imagen:



Después al completar la creación de nuestra máquina virtual, procederemos a configurar el adaptador de red y el archivo ISO. Para hacerlo, hacemos clic en el icono de engranaje ubicado en la parte superior. Luego, vamos al apartado de "Red" y, en "Adaptador 1", seleccionamos la opción "Adaptador puente", como se puede mostrar a continuación en la siguiente imagen:



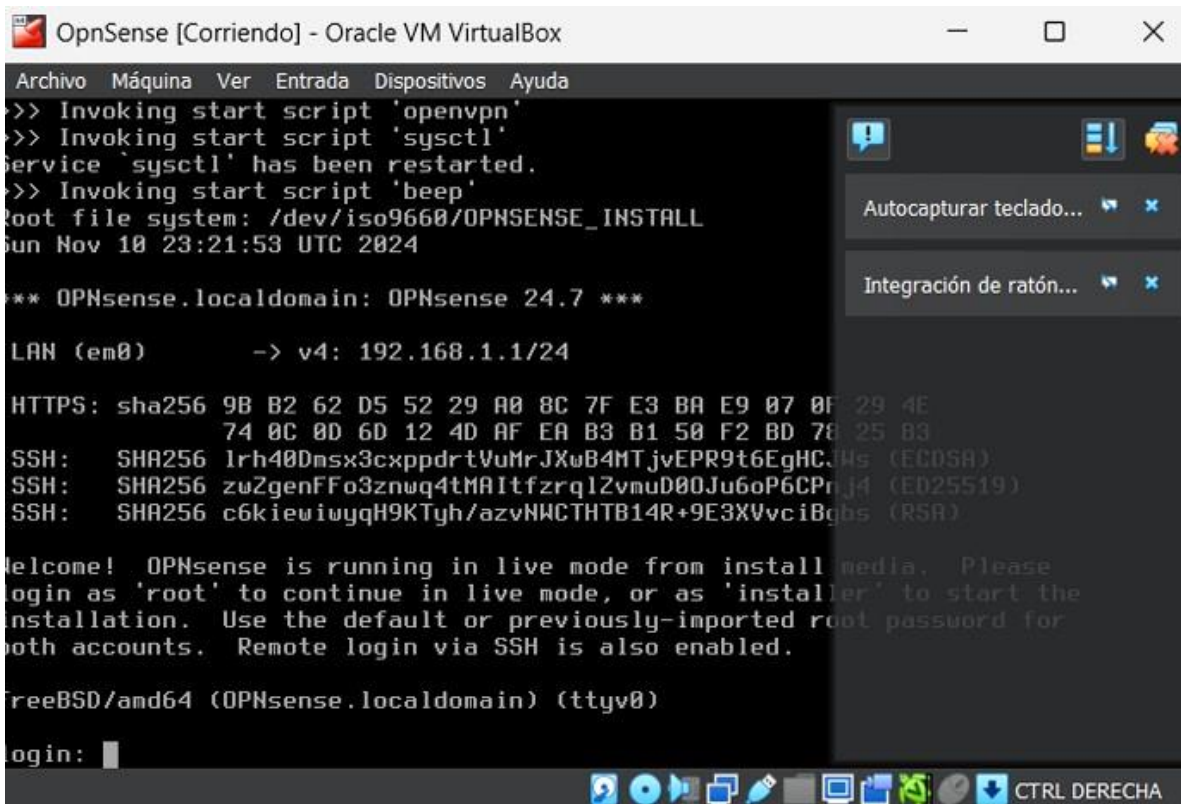
Después una vez al terminar de ajustar la configuración del adaptador de red, pasamos al apartado de "Almacenamiento". En esta sección, seleccionamos el archivo ISO que utilizaremos para la instalación del sistema operativo. Después de cargar el ISO, confirmamos los cambios haciendo clic en el botón "Aceptar", como se muestra a continuación en la siguiente imagen:



CONFIGURACIÓN DE INTERFACES:

Después una vez al iniciar la máquina virtual nos aparecerá de la siguiente manera en la cual nos pedirá que ingresemos un usuario (root) y una

contraseña (opnsense), como se puede mostrar a continuación 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 ***

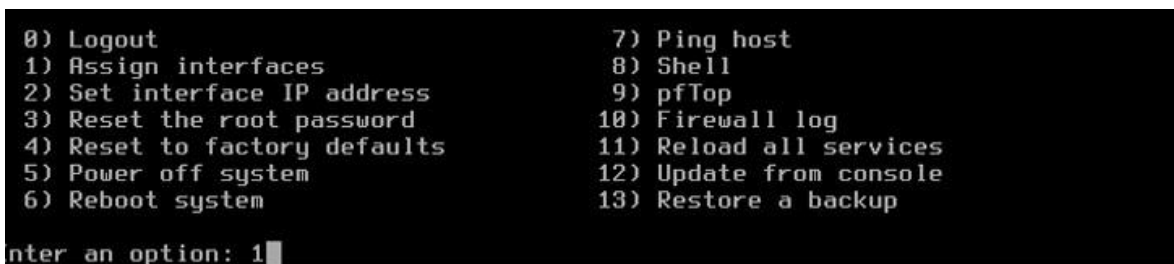
LAN (em0)      -> v4: 192.168.1.1/24

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 lrh40Dmsx3cxppdrTVuMrJXwB4MTjvEPR9t6EgHCJHs (ECDSA)
SSH:   SHA256 zu2genFFo3znwq4tMAItfzrq12vmuD00Ju6oP6CPnjd (ED25519)
SSH:   SHA256 c6kieuiwyqH9KTyh/azvNwCTHTB14R+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: █
```

Posteriormente en este punto, veremos una lista de opciones para personalizar varios aspectos. Para nuestro caso, elegiremos la opción correspondiente a la configuración de la interfaz de red, como se puede mostrar a continuación 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█
```

Después posteriormente a continuación, se nos preguntará si deseamos configurar los LAGGs en este momento. En nuestro caso, seleccionaremos la opción de "no" y continuaremos presionando enter.



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

Después así posteriormente luego, aparecerá una opción que solicitará ingresar la interfaz para la WAN. Asignaremos "em0" en este campo y presionaremos enter para continuar, como se muestra a continuación en la siguiente imagen:

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

Después así mismo se mostrarán las configuraciones que se aplicaron a las interfaces, como se puede observar a continuación en la siguiente imagen:

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

Después así posteriormente seguimos con los demás pasos y ingresamos las siguiente línea de código, como se muestra a continuación en la siguiente imagen:

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

Después ingresamos la opción numero 2 para así posteriormente realizar la

```
Enter an option: 2
```

Una vez hecho, nos solicitara elegir opciones disponibles para configurar como nos muestra a continuación en la siguiente imagen:

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

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

Después ya que se haya escrito el numero 1 presionamos enter, y así mismo configuraremos la dirección de la interfaz LAN para DHCP, y nos mostrara una opción y elegiremos "NO" y así mismo le damos enter, como se puede mostrar a continuación en la siguiente imagen:



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

Después, se nos solicitará ingresar la dirección IP para la interfaz LAN. Escribimos la IP que queremos y presionamos enter para continuar, como se puede observar a continuación en la siguiente imagen:

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

Posteriormente a continuación, ingresamos la máscara de subred en formato numérico, por ejemplo, 24 para una máscara 255.255.255.0, y presionamos enter para seguir, como se muestra a continuación 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 continuamos presionando enter, como se muestra a continuación en la siguiente imagen:

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

Posteriormente también en esta configuración escribiremos que no, enseguida dar enter, como se puede apreciar a continuación en una imagen:

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




Así mismo, se nos preguntará si queremos activar el servidor DHCP en la interfaz LAN. Escribimos "sí" y presionamos enter para continuar, como nos muestra a continuación en la siguiente imagen:

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

Posteriormente luego, se nos solicitará ingresar el rango de direcciones IP para iniciar. Introducimos "127.16.4.5" y presionamos enter para continuar, como nos muestra a continuación en la siguiente imagen:

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

Posteriormente a continuación igual se nos pedirá definir lo que es la dirección IP y llega al rango donde se ingreso "172.16.4.2000" como se muestra en esta dirección y presionamos enter, y así posteriormente el sistema empezara a reiniciarse, como se muestra a continuación en la siguiente imagen:

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

Despues en este apartado ingresamos un no primeramente y enseguida con un sí, posteriormente con un enter para que nos muestre una dirección, como se muestra a continuación 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]
```

Posteriormente así mismo ya que tenemos finalizado el renicio del sistema, se mostrará una direccionen la que podremos acceder a la interfaz de OPPSENSE, como se muestra a continuación en la siguiente imagen:

```
https://172.16.4.2
```

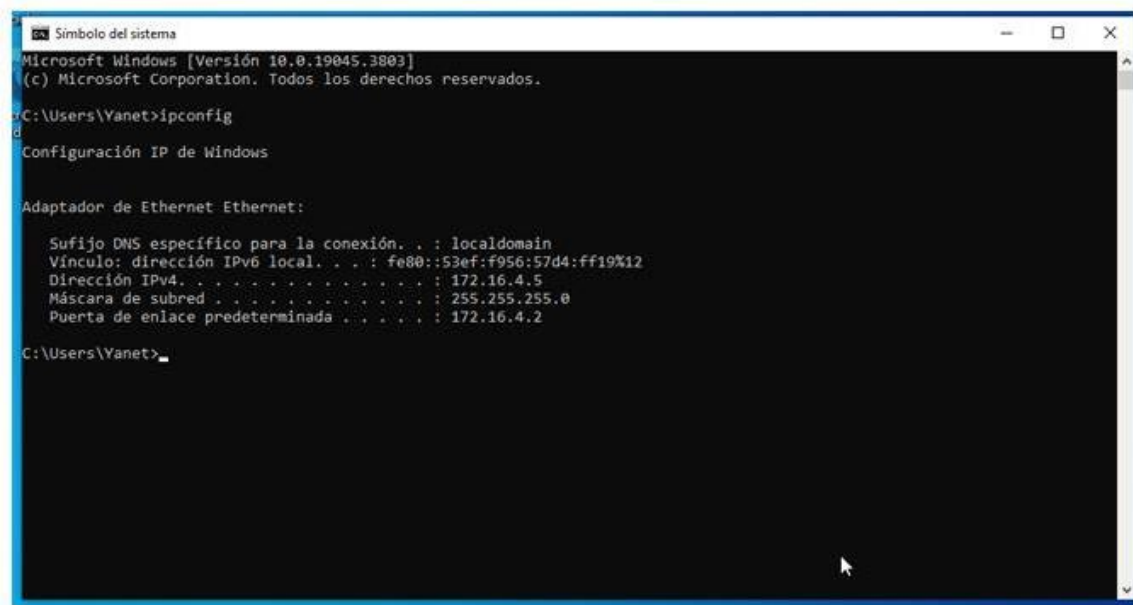
Posteriormente después guardamos los datos que se muestran, donde posteriormente al terminar las configuraciones se realizaran pines con las direcciones generadas, como se muestra a continuación en la siguiente imagen:

```
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
```

Después accedemos a la maquina virtual con el sistema operativo 10, una vez ya estando hay lo iniciamos y abrimos la terminal, y después ejecutamos el comando ipconfig para verificar que la maquina virtual esta funcionando correctamente, y asi mismo podremos acceder a la interfaz de OPNsense a través del navegador sin inconvenientes , como se puede observar a continuación 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>
```

Posteriormente se abre el navegador que se tiene instalado, en este caso es el de “Microsoft Edgde” y escribimos la dirección IP de nuestro OPNsense en la barra de direcciones , como la IP que se escribió que es la de “172.16.4.2”, como se muestra a continuación en la siguiente imagen:



OPNsense

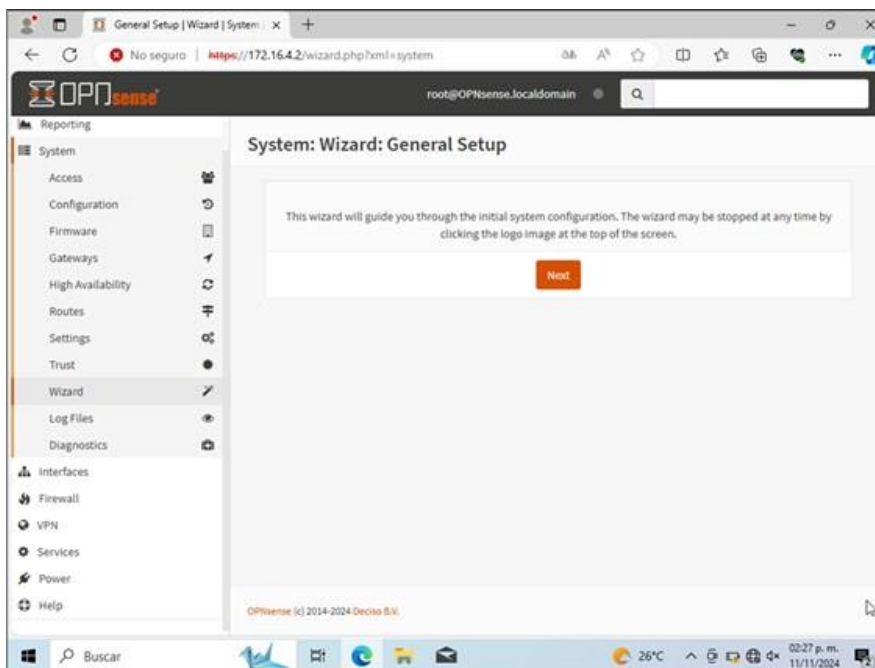
Username:

Password:

Login

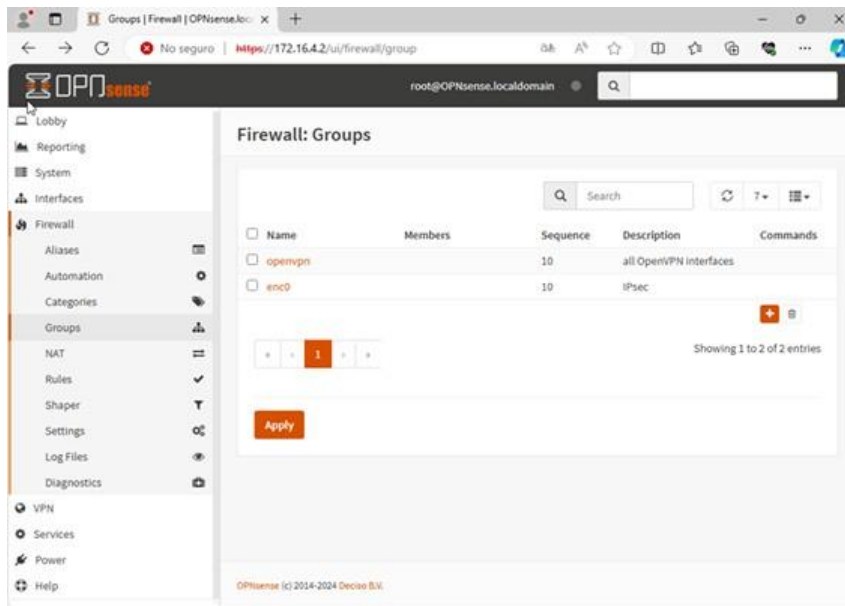
OPNsense (c) 2014-2024 Deciso B.V.

Posteriormente escribimos “root” en el campo de usuario y “opnsense”, donde posteriormente se puede realizar diferentes configuraciones, como se puede observar a continuación en la siguiente imagen:

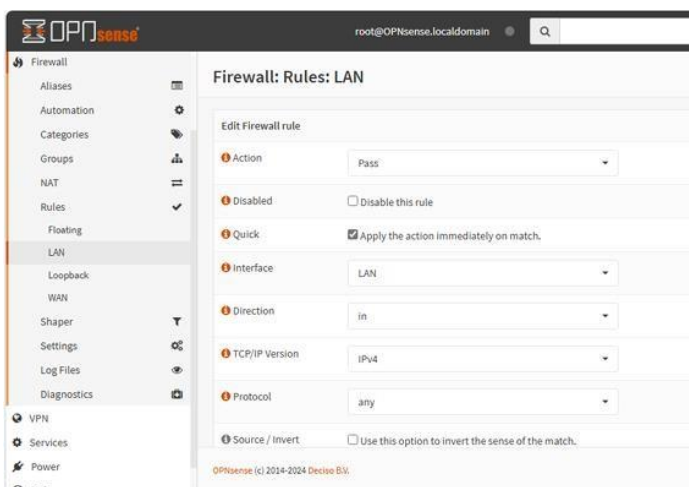


CONFIGURACIÓN DE REGLAS DE FIREWALL:

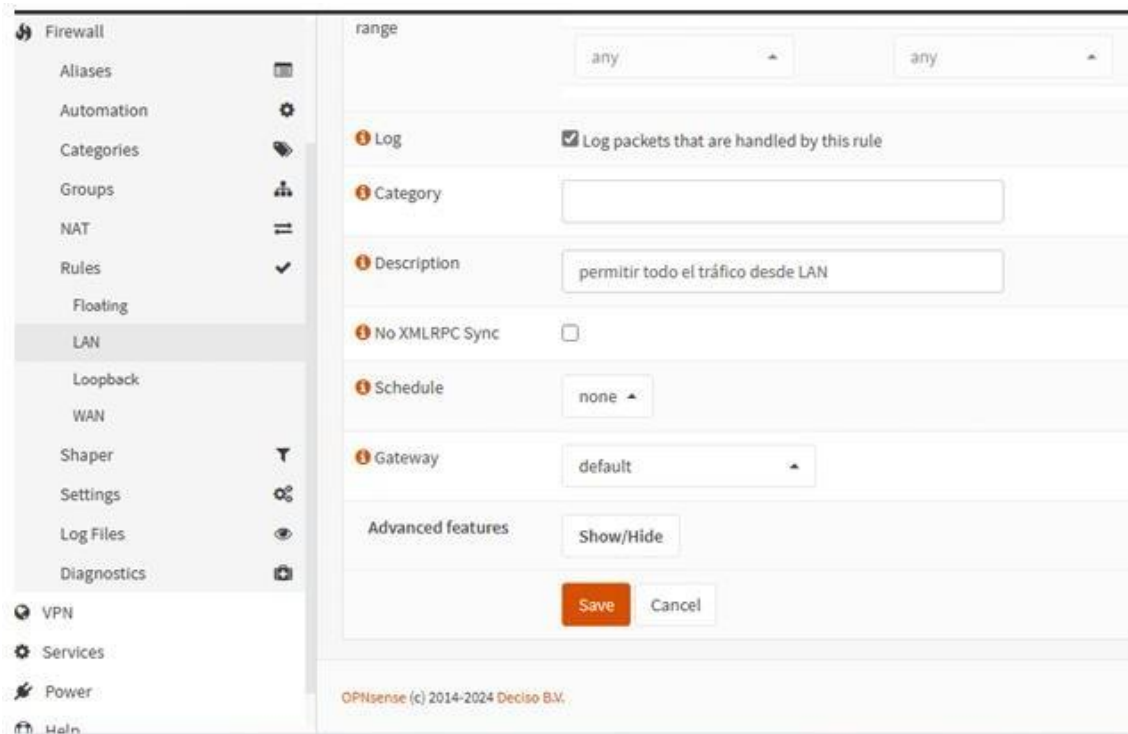
Posteriormente después para configurar las reglas del firewall, navegamos a la sección llamada "Firewall". Ahí, se abrirá una nueva ventana, donde haremos clic en el botón naranja con el símbolo de más para añadir una nueva regla al firewall, como se muestra a continuación en la siguiente imagen:



Posteriormente una vez dando click se abrirá una ventana donde se podrá establecer una regla para nuestra red LAN, como se muestra a continuación la configuración en la siguiente imagen:



Posteriormente una vez que hayamos configurado todas las opciones, haremos clic en el botón "save" para guardar los cambios, como se muestra a continuación en la siguiente imagen:



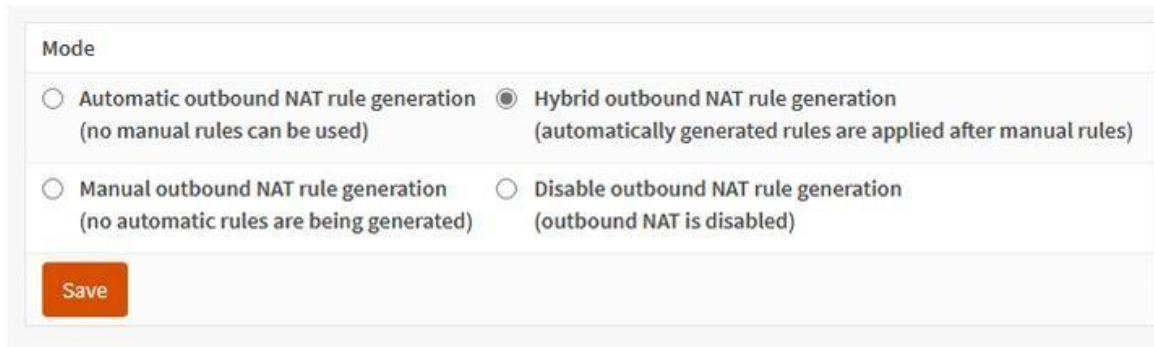
La imagen muestra la interfaz de configuración de reglas de firewall en OPNsense. En el menú lateral izquierdo, se encuentran las opciones: Firewall, Aliases, Automation, Categories, Groups, NAT, Rules, Floating, LAN (seleccionada), Loopback, WAN, Shaper, Settings, Log Files, Diagnostics, VPN, Services, Power y Help. La sección principal muestra la configuración de una regla en la interfaz LAN. Los campos configurados son: range (any), Log (marcado), Category (vacío), Description (permitir todo el tráfico desde LAN), No XMLRPC Sync (desmarcado), Schedule (none) y Gateway (default). En la parte inferior, hay un botón "Save" en naranja y un botón "Cancel".

Después así mismo podemos observar que ahora tenemos tres reglas configuradas en la sección LAN del firewall, como se puede mostrar a continuación en la siguiente imagen:

<input type="checkbox"/>	Protocol	Source	Description	<input type="checkbox"/>
<input type="checkbox"/>	Automatically generated rules			
<input type="checkbox"/>	IPv4 *	LAN net	Default allow LAN to any rule	<input type="checkbox"/>
<input type="checkbox"/>	IPv6 *	LAN net	Default allow LAN IPv6 to any rule	<input type="checkbox"/>
<input type="checkbox"/>	IPv4 *	LAN net	permitir todo el tráfico desde LAN	<input type="checkbox"/>

CONFIGURAR EL NAT:

Posteriormente después para configurar el NAT, en la sección de modo seleccionaremos la opción "Hybrid outbound rule generation - automatically generated rules", como se muestra a continuación en la siguiente imagen:



Mode

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

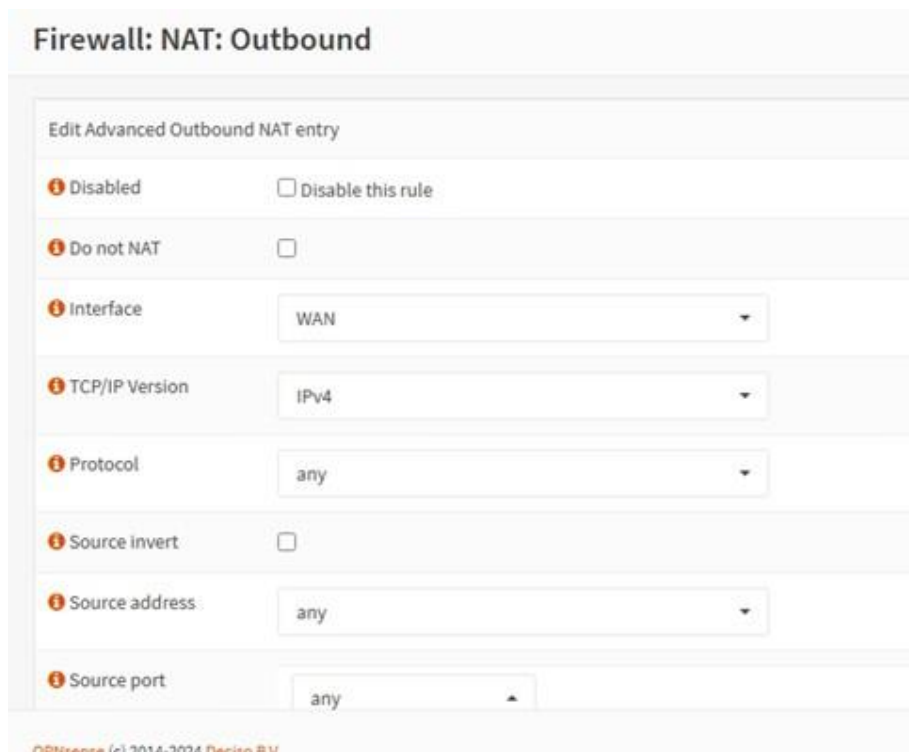
☒ Hybrid outbound NAT rule generation
(automatically generated rules are applied after manual rules)

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

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

Save

Posteriormente nos vamos a la opción llamada "Outbound" y así mismo configuramos cada uno de los apartados que aparecen ahí como se muestra a continuación 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

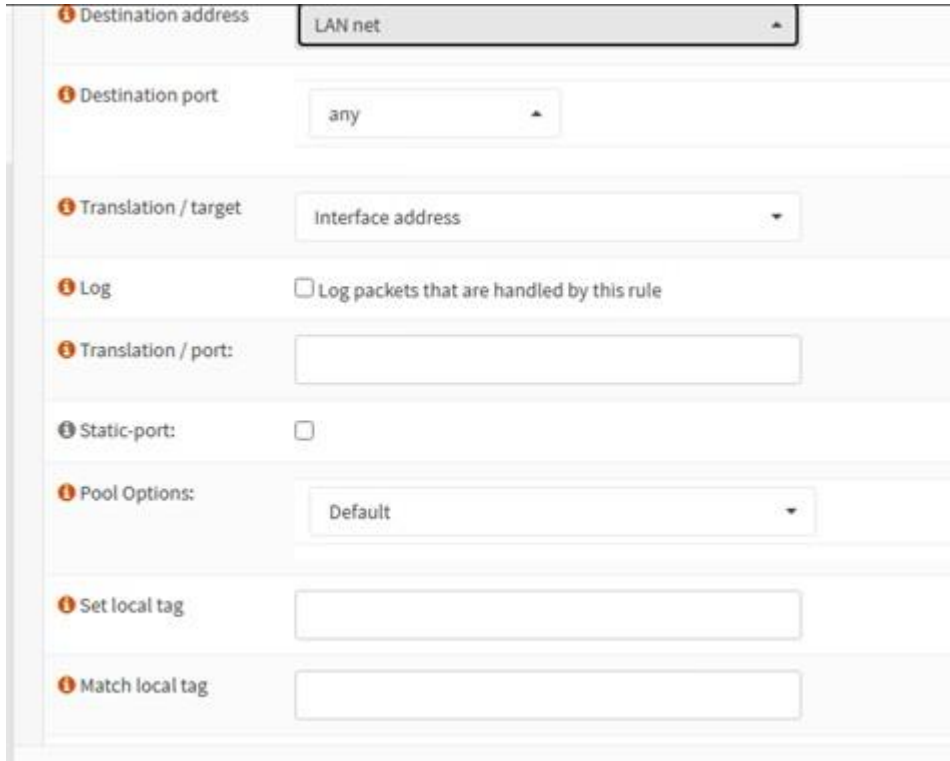
Source invert ☐

Source address any

Source port any

© 2014-2024 Pfsense R.U

Después posteriormente continuamos ajustando las configuraciones necesarias y, al terminar, hacemos clic en el botón "Save" para guardar los cambios, como se puede ver a continuación en la siguiente imagen:

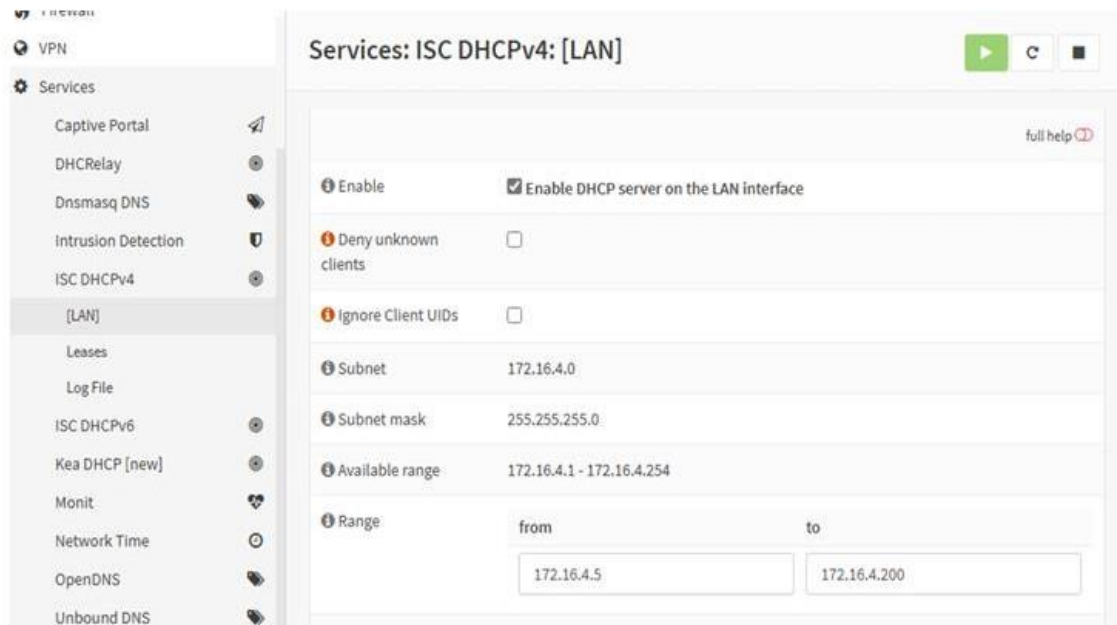


Posteriormente después de puede ver que hemos añadido correctamente la configuración de nuestro NAT, como se muestra a continuación en la siguiente imagen:

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			

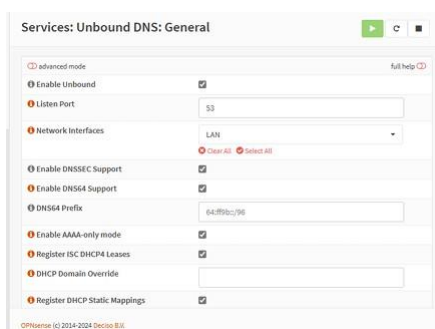
CONFIGURACIÓN DE DHCP:

Después así mismo, configuraremos el DHCP para nuestra red LAN. Se mostrará un conjunto de opciones que debemos ajustar, como la dirección IP, la máscara de subred y el rango de direcciones IP permitidas, como se muestra a continuación en la siguiente imagen:



2.6 CONFIGURACIÓN DE DNS:

Después vamos a configurar el DNS . donde en la ventana que aparece, se vera varias opciones de configuración, donde se selecciona las opciones principales, como se puede observar en la siguiente imagen:



Después así mismo, seleccionamos las casillas correspondientes, y al finalizar , hacemos click en el botón “Apply” para que los cambios se apliquen , como se puede ver a continuación en la siguiente imagen:



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

2.7 ASINACIÓN DE DIRECCION IP STATIC AL FIREWALL:

Posteriormente se configura la interfaz de firewall, con una dirección inicial de 172.16.4.1 con una mascara de subred 24, como se puede ver a continuación en la siguiente imagen:

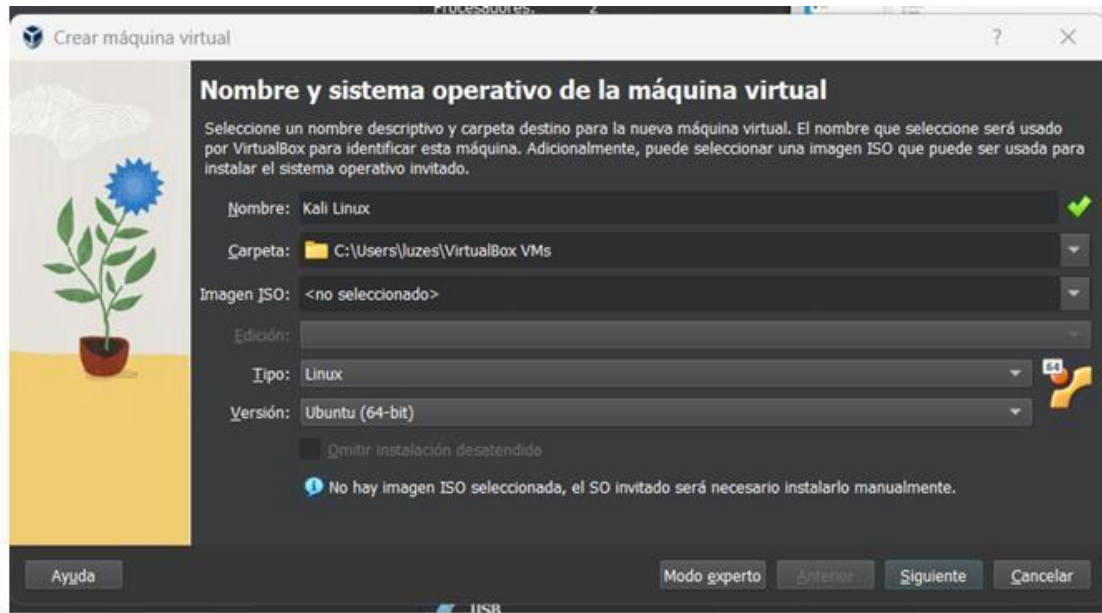


Static IPv4 configuration

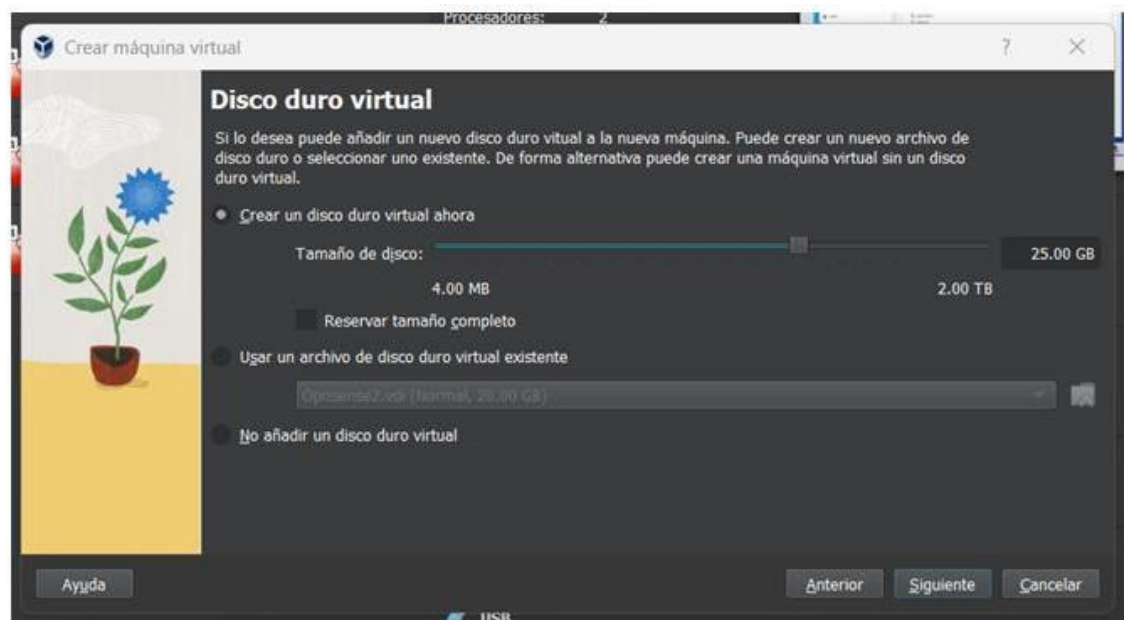
IPv4 address	172.16.4.1	24
IPv4 gateway rules	Disabled	

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

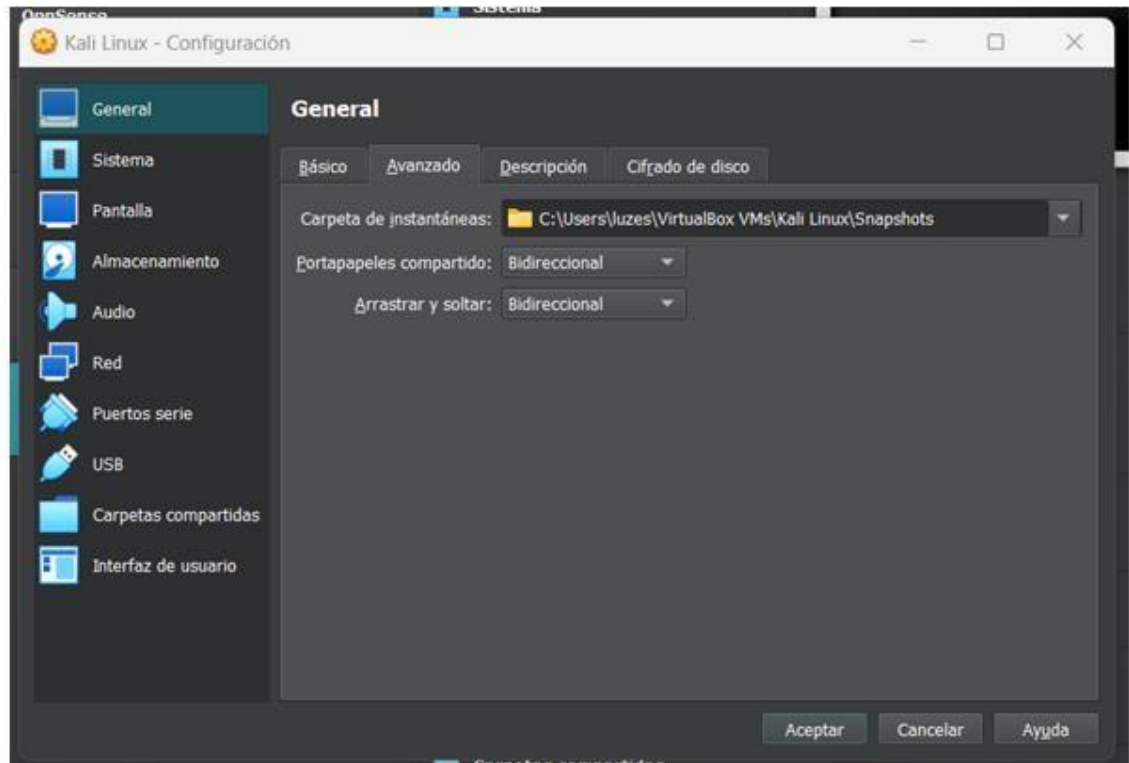
Después Comenzamos creando una nueva máquina virtual, asignándole el nombre "Kali Linux". Después, elegimos el archivo ISO, configuramos el tipo como "Linux" y seleccionamos "Ubuntu (64-bit)" para la versión. Por último, hacemos clic en "Siguiente", como se puede observar a continuación en la siguiente imagen:



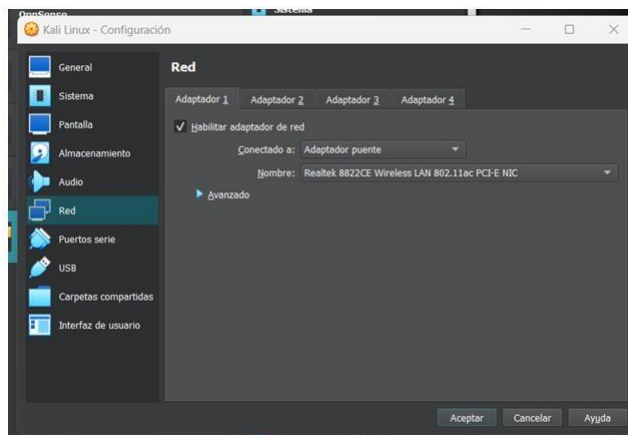
Después establecemos lo que es el tamaño del disco duro virtual que se necesita para la máquina, y después hacemos click en “siguiente”, como se muestra a continuación en la siguiente imagen:



Después así nos vamos a la sección de configuración, en el apartado “General”. En las opciones de “Portapapeles compartido” y “Arrastrar y soltar”, y así mismo seleccionamos la opción de “Bidireccional”, como se puede observar a continuación en la siguiente imagen:



Después una vez completado, nos dirigimos a la sección “Red”. En el adaptador 1, elegimos la opción “Adaptador puente” en el campo “Conectado” después asignamos una dirección IP a la maquina virtual , como se puede ver a continuación en la siguiente imagen:



Posteriormente al iniciar se mostrara la interfaz de Kali Linux , y despues seleccionamos la primera opción que dice “Graphical Install”, como se muestra a continuación en la siguiente imagen:

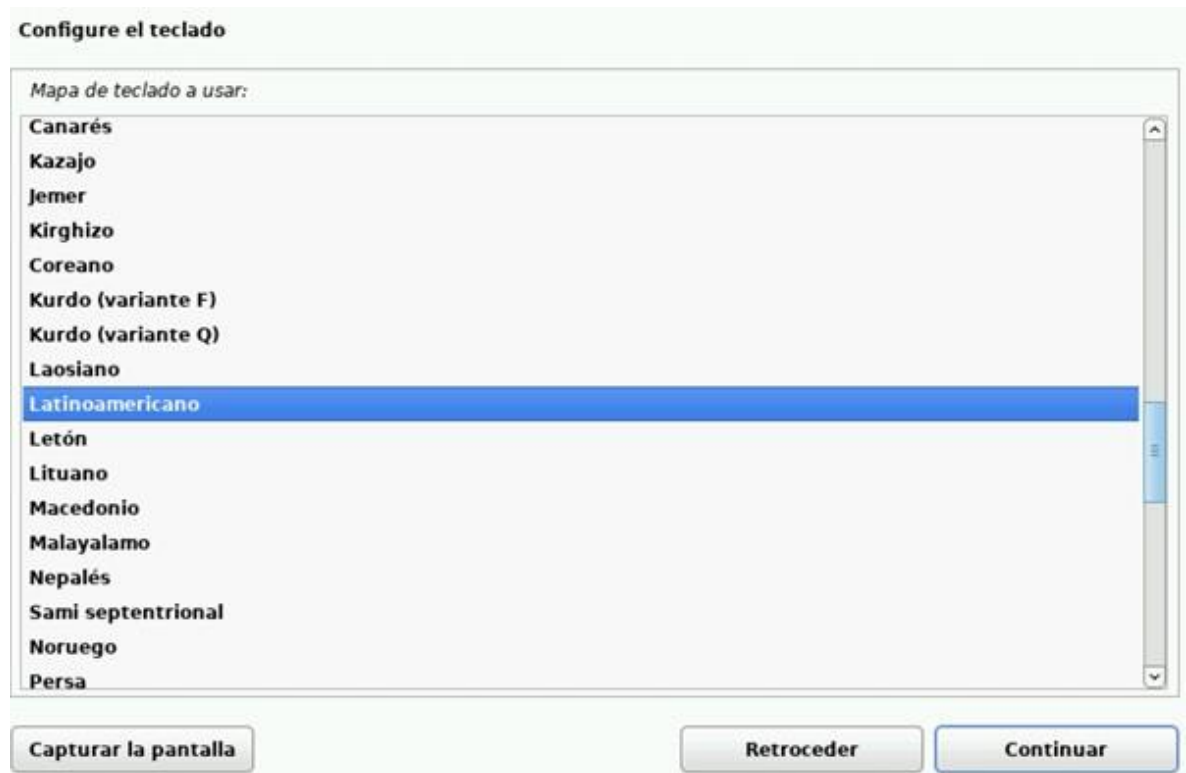


Después posteriormente elegimos lo que viene siendo el idioma que deseamos utilizar y luego hacemos click en el botón “continúe”, como se puede ver a continuación en la siguiente imagen:





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



Después asignamos el nombre a nuestra maquina y luego hacemos click en el botón “continuar”, como se puede ver a continuación en la siguiente imagen:





Después posteriormente, asignamos el nombre de usuario a la maquina virtual como se puede ver a continuación en la siguiente imagen:

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 que no sean administrativas.

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

Nombre completo para el nuevo usuario:

yanet

Capturar la pantalla Retroceder Continuar

Luego, nos solicitará que establezcamos una contraseña. Ingresamos la contraseña en el primer campo y la volvemos a escribir en el segundo para confirmarla, como se muestra a continuación en la siguiente imagen:

Configurar usuarios y contraseñas

Asegúrese de seleccionar una contraseña segura que no pueda ser adivinada.

Elija una contraseña para el nuevo usuario:

•••••

☐ Mostrar la contraseña en claro

Por favor, introduzca la misma contraseña de usuario de nuevo para verificar que la introdujo correctamente.

Vuelva a introducir la contraseña para su verificación:

•••••

☐ Mostrar la contraseña en claro

Capturar la pantalla Retroceder Continuar



En este paso, configuramos la zona horaria de la máquina según nuestra ubicación. En nuestro caso, seleccionamos la opción "Central" y luego hacemos clic en el botón "Continuar", como se muestra a continuación en la siguiente imagen:

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

Seleccione su zona horaria:

Noroeste
Pacífico
Sonora
Central
Sureste

Capturar la pantalla Retroceder Continuar

Después se nos pedirá que elijamos una opción para particionar el disco. Seleccionamos la primera opción, "Guiado – usar todo el disco", y luego hacemos click en el botón "continuar", como se muestra a continuación en la siguiente imagen:

Particionado de discos

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

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

Método de particionado:

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

Capturar la pantalla Retroceder Continuar



Después mantenemos la primera opción predeterminada y luego hacemos click en “continua”, como se muestra a continuación en la siguiente imagen:

Particionado de discos

Seleccionado para particionar:

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

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

Esquema del particionado:

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

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

A continuación, aparecerá una ventana en la que se confirmarán todos los cambios realizados en el disco. Seleccionamos la opción "Sí" y luego hacemos clic en el botón "Continuar", como se muestra a continuación en la siguiente imagen:

Particionado de discos

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

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

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

¿Desea escribir los cambios en los discos?

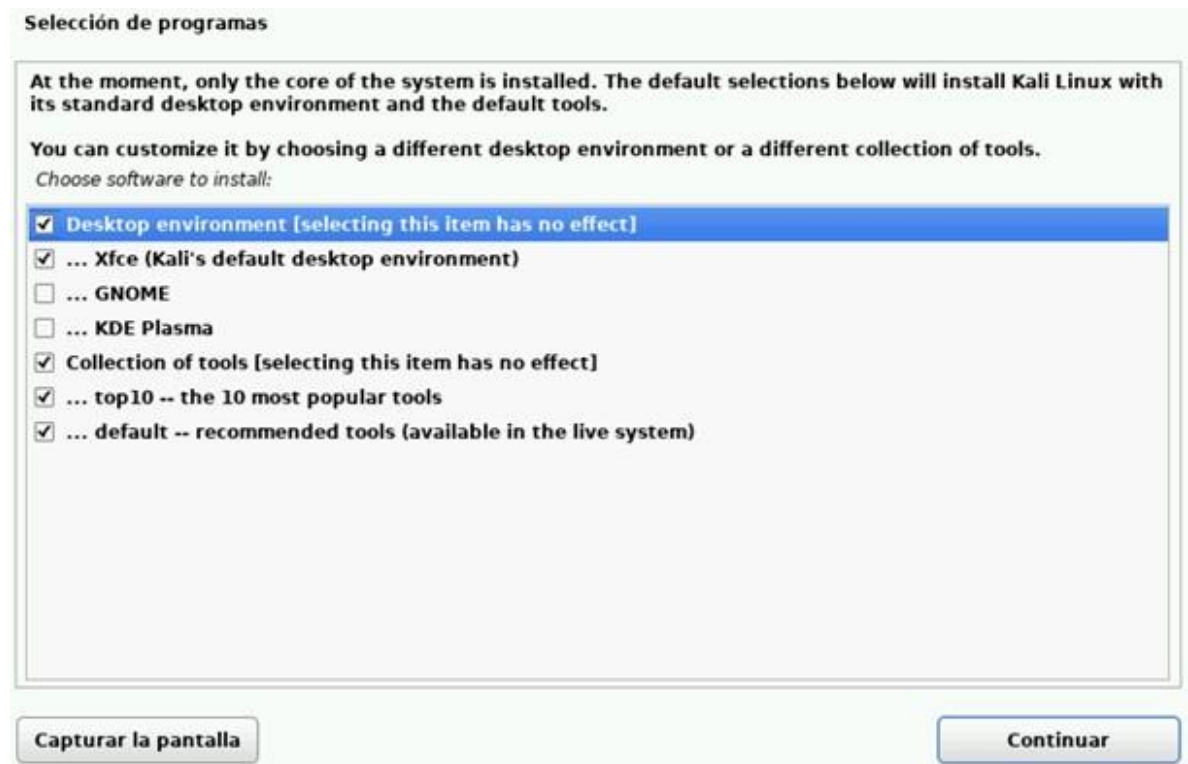
☐ No

☒ **Sí**

Capturar la pantalla **Continuar**



Después así mismo se mostrara una ventana donde nos pedirá elegir el tipo de programa que queremos instalar , y asi mismo dejamos las opciones predeterminadas seleccionadas y leugo hacemos click en el botón “continua”, como se observa a continuación en la siguiente imagen:



Después a continuación, aparecerá un mensaje de advertencia sobre la instalación de cargador de arranque GRUB. Después elegimos la opción “SI” y hacemos clic en “continuar”, como se puede observar a continuación en la siguiente imagen:





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

Instalando el cargador de arranque GRUB

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

Dispositivo donde instalar el cargador de arranque:

Introducir el dispositivo manualmente

`/dev/sda (ata-VBOX_HARDDISK_VBee23691b-67461c27)`

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

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

Instalando el cargador de arranque GRUB

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

Dispositivo donde instalar el cargador de arranque:

Introducir el dispositivo manualmente

`/dev/sda (ata-VBOX_HARDDISK_VBee23691b-67461c27)`

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



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



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



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



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

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

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

Una vez completado el paso anterior, ingresamos el siguiente comando:

```
sudo apt-get install libpcr3-dbg libpcr3-dev autoconf automake libtool  
libpcap-dev libnet1-dev libyaml-dev libjansson4 libcap-ng-dev libmagic-dev  
libjansson-dev zlib1g-dev pkg-config rustc cargo.
```

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

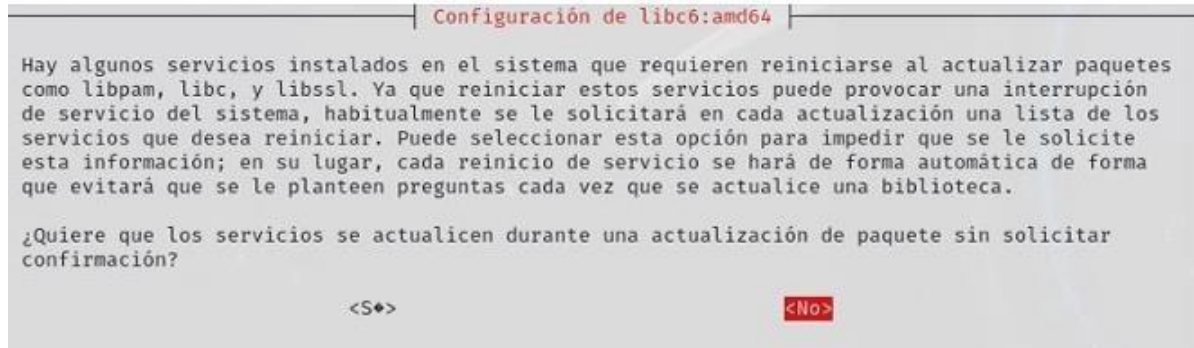
```
yanet@YANET: ~  
File Actions Edit View Help  
  
(yanet@YANET)-[~]  
$ sudo apt-get install -y libpcr3-dbg libpcr3-dev autoconf automake libtool  
libpcap-dev libnet1-dev libyaml-dev libjansson4 libcap-ng-dev libmagic-dev  
libjansson-dev zlib1g-dev pkg-config rustc cargo  
  
Reading package lists... 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 libpcr3-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, procedemos a instalar Suricata, el motor de detección y prevención de intrusiones (IDS/IPS) en la red, utilizando el siguiente comando: `sudo apt install suricata -y`. Esperamos a que la instalación se complete.

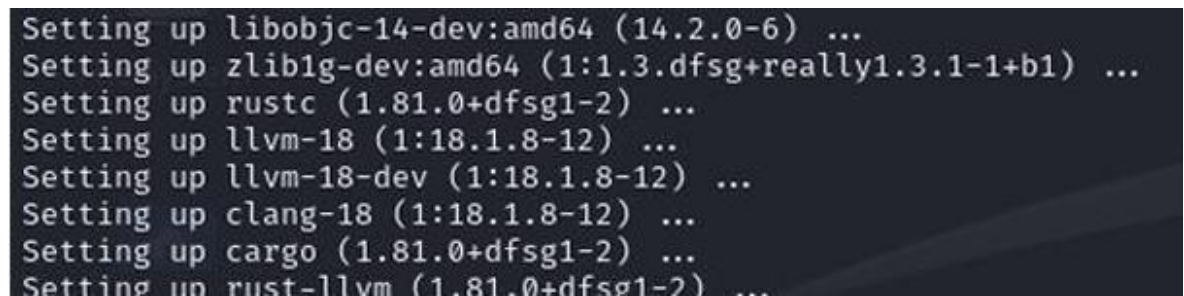
```
$ sudo apt install suricata -y  
Installing:  
suricata  
  
Installing dependencies:  
isa-support      librtt-bus-vdev24  librtt-log24      librtt-pci24      oinkmaster  
libfdt1          librtt-eal24       librtt-mbuf24      librtt-rcu24      snort-rules-default  
libhttp2         librtt-ethdev24    librtt-mempool24   librtt-ring24     sse3-support  
libhyperscan5    librtt-hash24      librtt-meter24     librtt-sched24    sse4.2-support  
libnetfilter-log1 librtt-ip-frag24   librtt-net-bond24  librtt-telemetry24 suricata-update  
librtt-bus-pci24 librtt-kvargs24    librtt-net24       libxdp1  
  
Paquetes sugeridos:  
snort | snort-pgsql | snort-mysql | libtcmalloc-minimal4  
  
Summary:  
Upgrading: 0, Installing: 30, Removing: 0, Not Upgrading: 1145  
Download size: 6.812 kB  
Space needed: 31,7 MB / 9.427 MB available
```



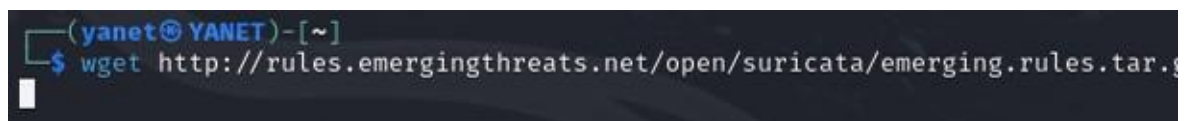
Después de completar la instalación, aparecerá una ventana que indica que algunos de los servicios instalados requieren un reinicio para aplicar las actualizaciones. Seleccionamos la opción "Sí" para proceder con el reinicio.



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



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.



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.

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

Ingresamos al directorio con el siguiente comando.

```
(yanet@YANET)-[~]
$ 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, configuramos reglas personalizadas en Suricata, un motor de detección y prevención de intrusiones, para identificar patrones de tráfico específicos en la red. Estas reglas se enfocan en detectar eventos como: Intentos de conexión ICMP, Intentos de conexión SSH, Posibles ataques DDoS en el puerto 80. Estas reglas permiten generar alertas basadas en estos patrones de tráfico, lo

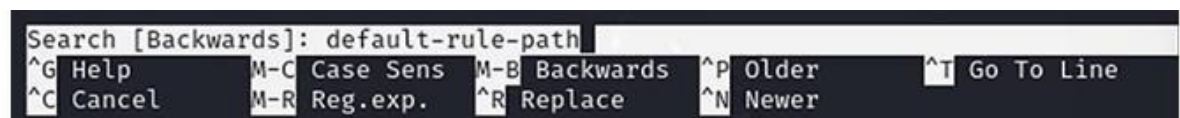
que ayuda a identificar actividades sospechosas y potencialmente maliciosas en la red. Para guardar los cambios realizados en la configuración, se utiliza el comando Ctrl + O seguido de Enter, y para salir del editor se usa Ctrl + X.

```
GNU nano 2.8.1 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:"DOS: Unusually fast port 80 SYN packets outbound, Potential DOS"; 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:

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.



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.

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

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

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

3.4 ASIGNAR UNA DIRECCIÓN IP ESTÁTICA A KALI LINUX.

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:

```
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
```

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

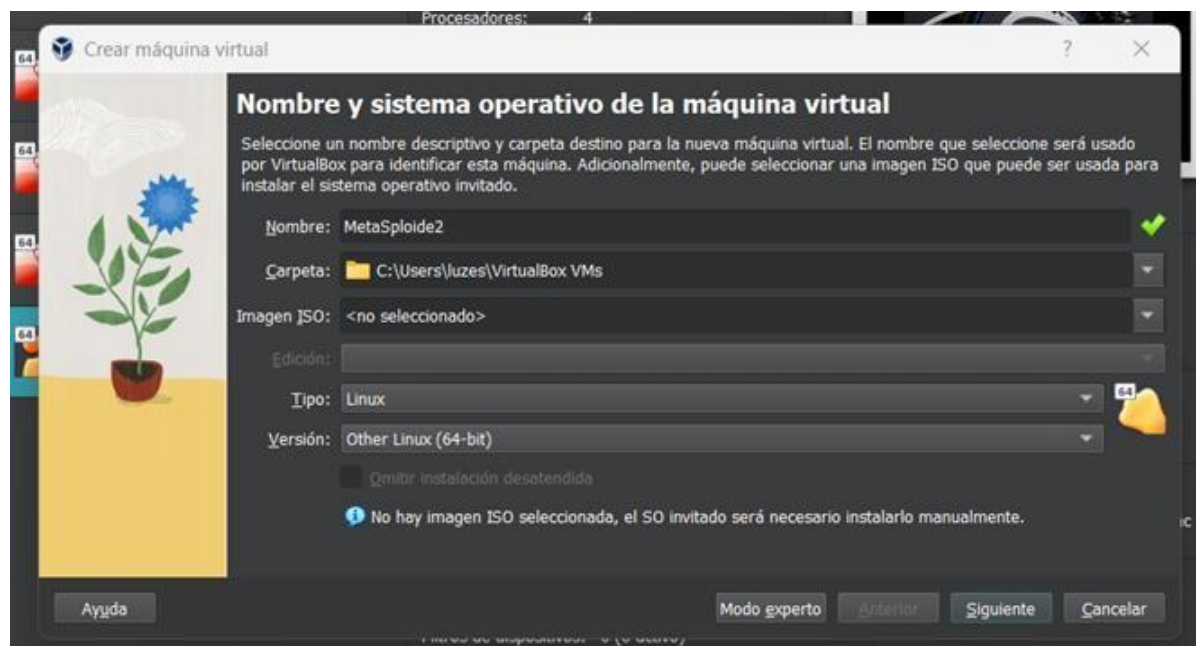
```
(yanet@YANET)-[~]  
$ sudo systemctl restart networking
```

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

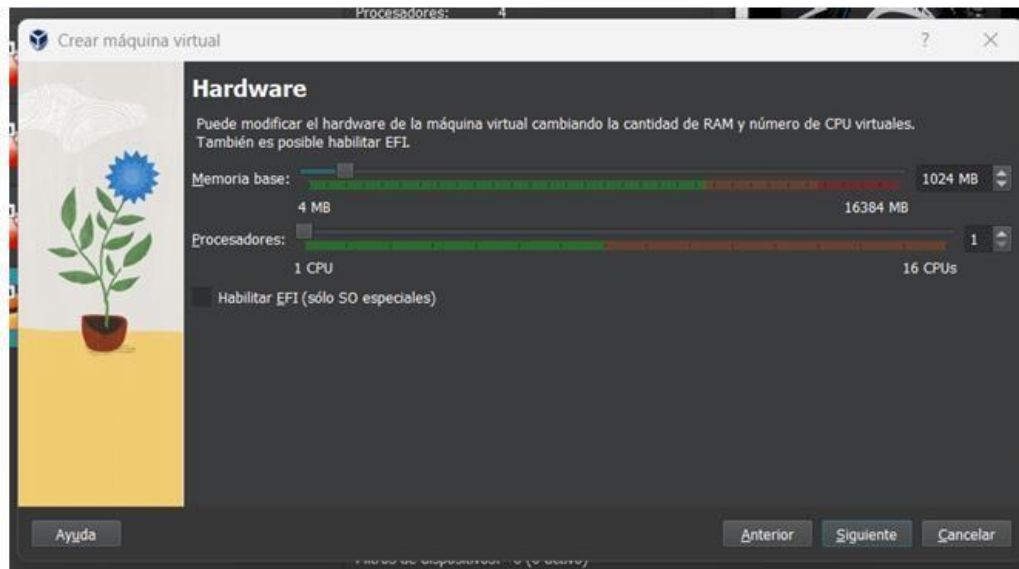

```
$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel s
tate UP group default qlen 1000
    link/ether 08:00:27:47:77:54 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.110/24 brd 192.168.1.255 scope global dynamic nop
refixroute eth0
        valid_lft 5292sec preferred_lft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

CREAR UNA MÁQUINA VIRTUAL VULNERABLE POR DISEÑO COMO METASPLOITABLE2:

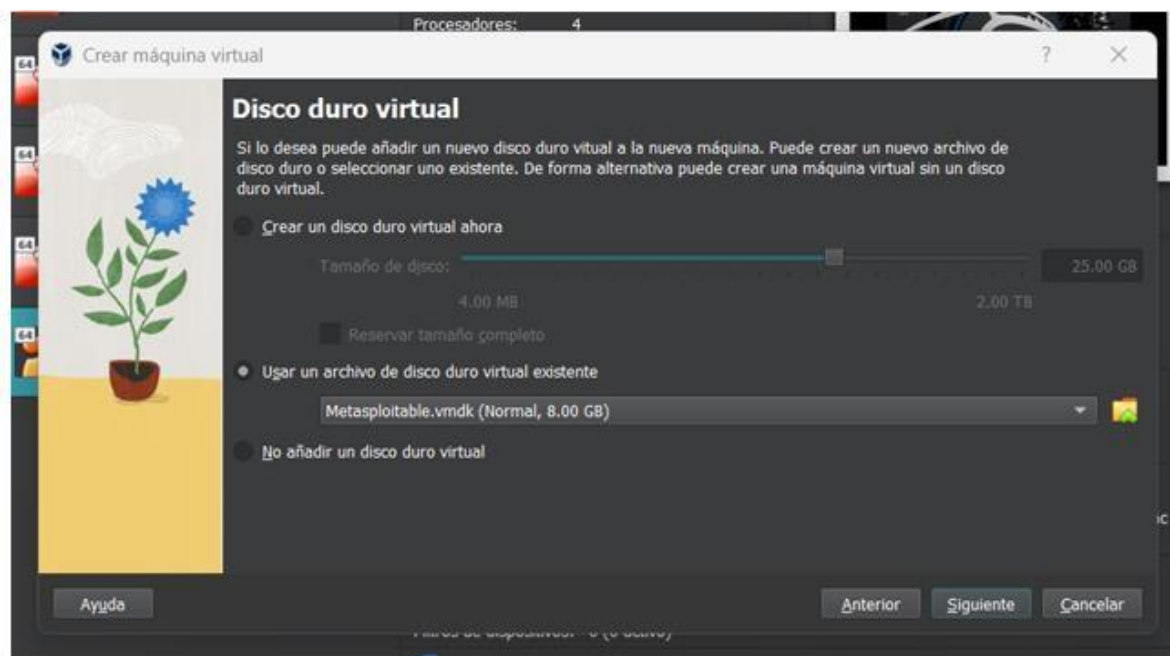
Configuramos una nueva máquina virtual llamada MetaSploitable2, seleccionamos "Linux" como tipo y, en la opción de versión, elegimos "Other Linux (64-bit)", luego hacemos clic en el botón "Siguiente".



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

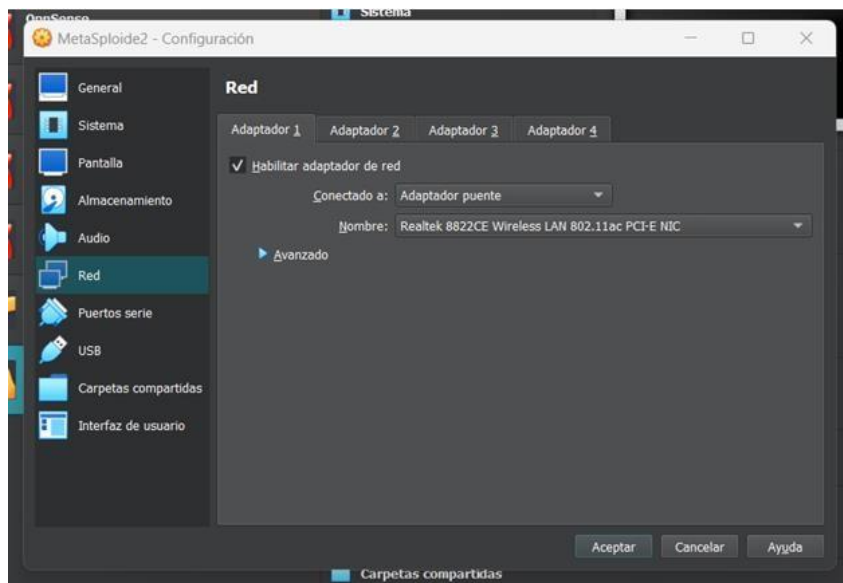


Asignamos 25 GB de espacio de almacenamiento y activamos la opción para utilizar un archivo de disco duro virtual existente. Seleccionamos el archivo ISO y luego hacemos clic en el botón "Siguiete" para continuar, como se muestra a continuación en la siguiente imagen:

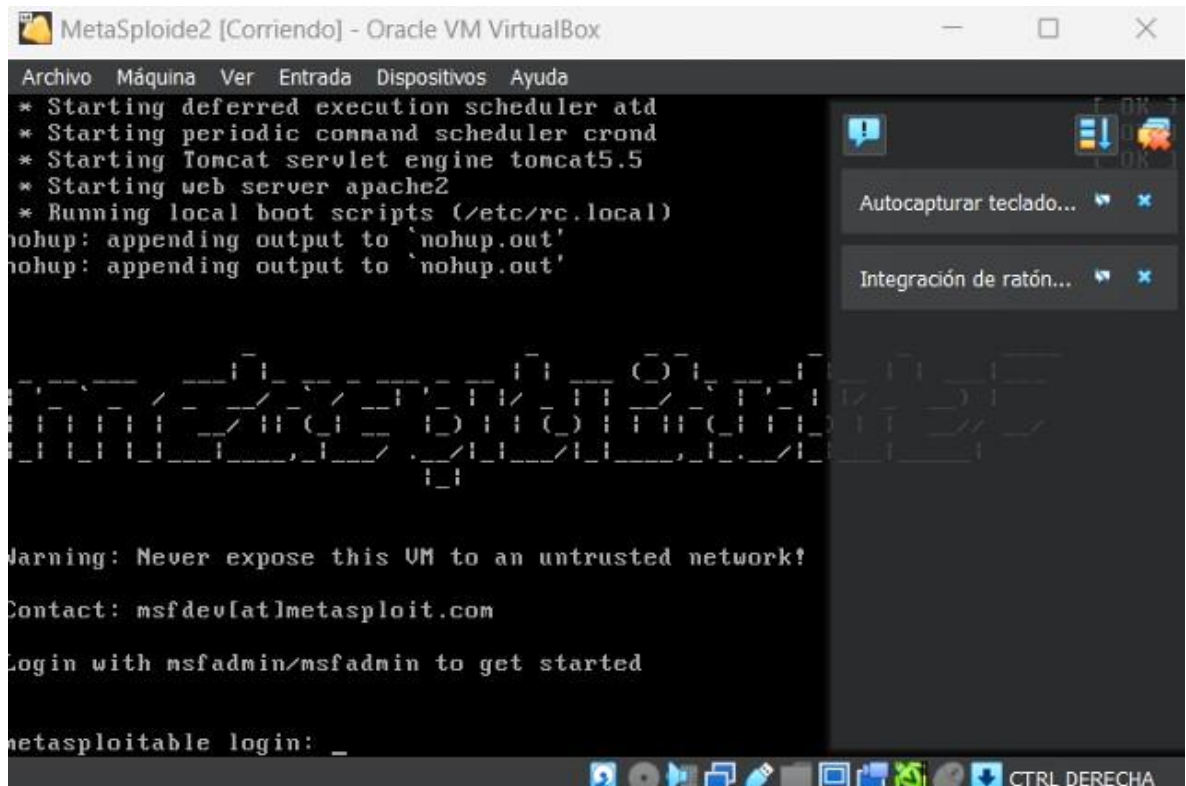


Después de crear la máquina virtual, configuramos la tarjeta de red. En este caso, seleccionamos "Adaptador puente" para asignar una dirección IP a la máquina

virtual. Luego, hacemos clic en "Aceptar" y procedemos a iniciar la máquina, como se muestra a continuación en la siguiente imagen:



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

arning: Never expose this VM to an untrusted network!
ontact: msfdev[at]metasploit.com
ogin with msfadmin/msfadmin to get started

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

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

buntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
pplicable law.

o access official Ubuntu documentation, please visit:
tp://help.ubuntu.com/
o mail.
sfadmin@metasploitable:~$ sudo nano /etc/network/interfaces
```

ASIGNAR UNA DIRECCIÓN IP ESTÁTICA A METASPLOITABLES:

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

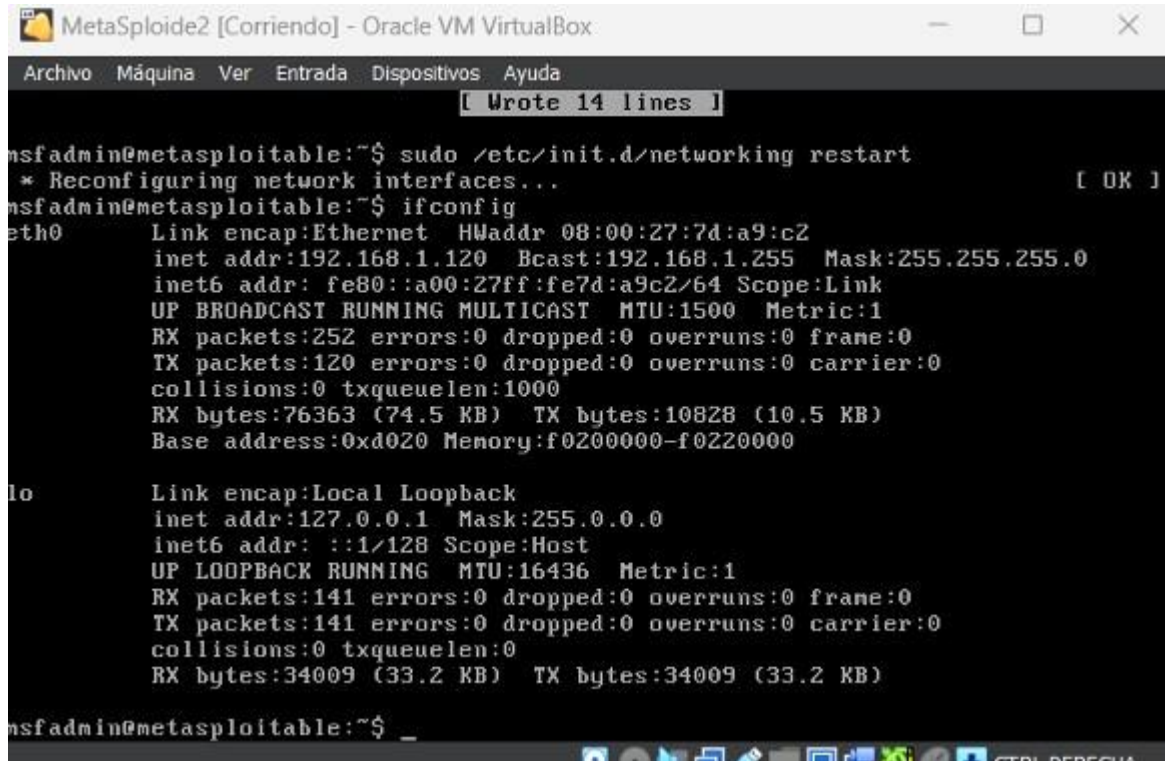
```
auto eth0
iface eth0 inet static
    address 192.168.1.120
    netmask 255.255.255.0
    gateway 192.168.1.1

^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 ]

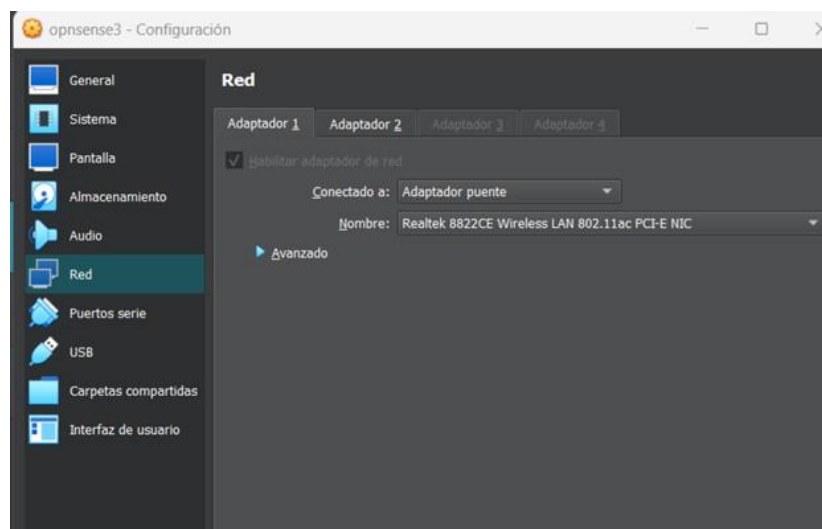
msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart
* Reconfiguring network interfaces... [ OK ]
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:7d:a9:c2
          inet addr:192.168.1.120  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe7d:a9c2/64 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:~$ _
```

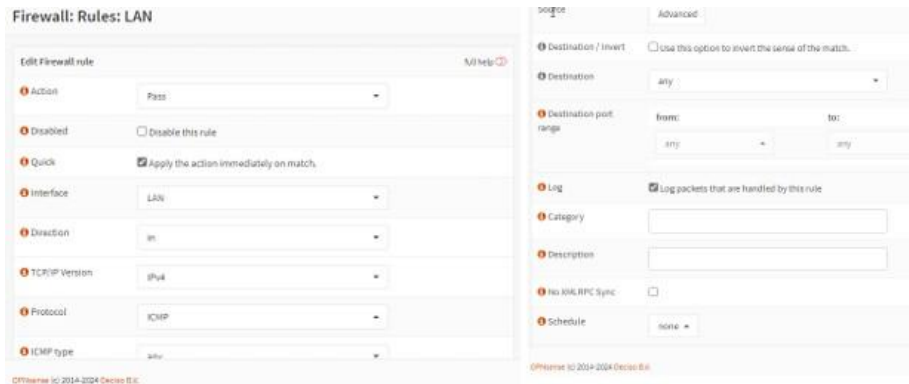
PING SATISFACTORIO ENTRE LAS MÁQUINAS VIRTUALES:

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

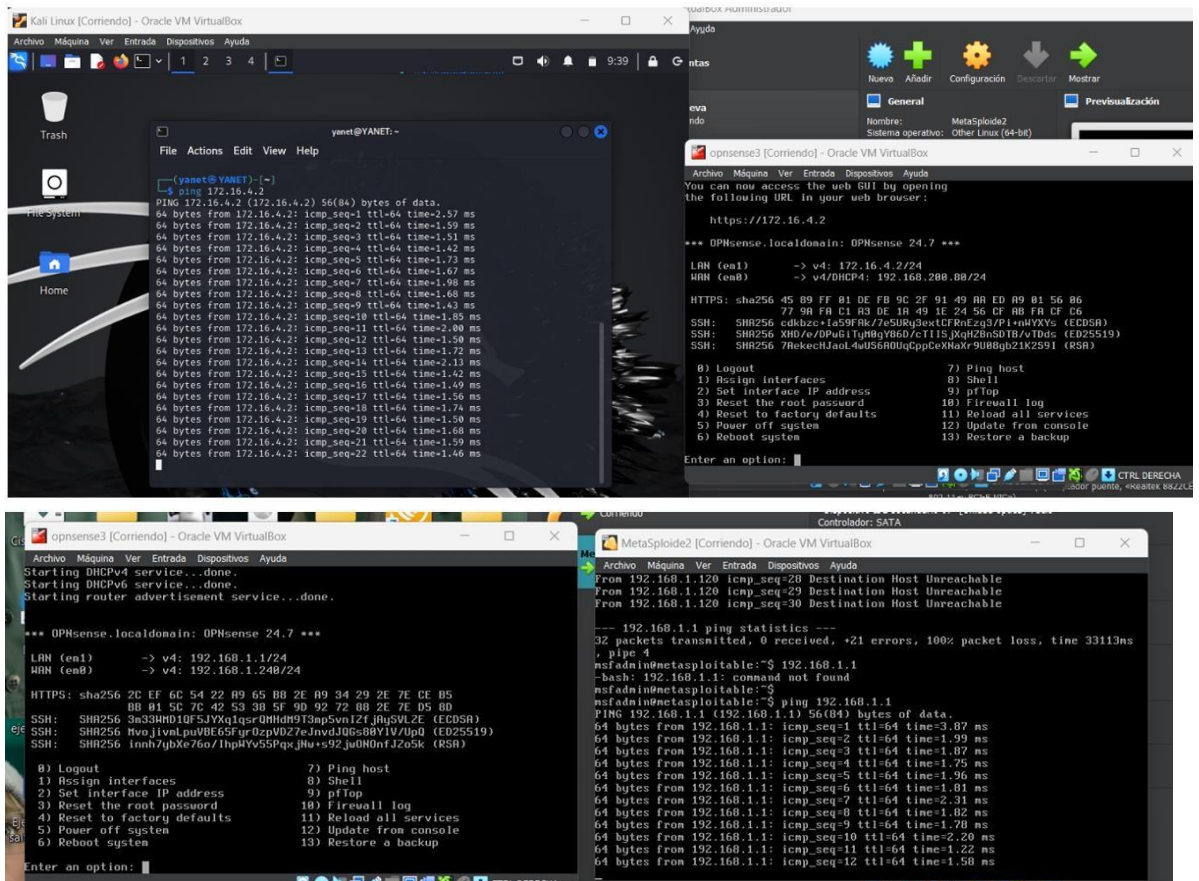


CONFIGURAR LAS REGLAS DE FIREWALL PARA PERMITIR EL TRÁFICO DE PING:

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:





La imagen muestra una interfaz de usuario de una máquina virtual Oracle VM VirtualBox. En el centro, hay una ventana de terminal de Kali Linux con el prompt de usuario 'yanet@YANET: ~'. Se ha ejecutado el comando 'ping 192.168.1.120', lo que ha generado una salida de 25 pings exitosos, cada uno de 64 bytes, con tiempos de ida y vuelta que oscilan entre 0.874 ms y 32.6 ms.

A la derecha, se encuentra una ventana de Metasploit (Metasploit2) con el prompt 'msfadmin@metasploitable: ~'. El usuario ha ingresado el comando 'ifconfig', lo que ha devuelto la configuración de red de la interfaz 'eth0'. Los detalles incluyen la dirección MAC '08:00:27:7d:e9:c2', la dirección IP '192.168.1.120', la máscara de subred '255.255.255.0' y la puerta de enlace '192.168.1.255'. También se muestran estadísticas de paquetes RX/TX y la configuración de la interfaz de enlace.

Debajo de la ventana de Metasploit, se ve una ventana de diálogo de 'Carpetas compartidas' (Shared Folders) con los campos 'Ninguno' y 'Descripción' vacíos, y botones para 'Aceptar', 'Cancelar' y 'Ayuda'.



CONCLUSION:

Al finalizar la Práctica 6, pude reconocer la importancia de contar con un firewall como primera línea de defensa, así como la relevancia de un sistema de detección de intrusos para monitorear actividades sospechosas. La integración de MetaSploitable2 me dio la oportunidad de realizar pruebas de penetración y aprender sobre las vulnerabilidades que los atacantes pueden aprovechar. Esta práctica no solo fortaleció mis conocimientos teóricos sobre la protección de redes, sino que también me permitió desarrollar habilidades prácticas esenciales para gestionar incidentes y proteger infraestructuras digitales. La experiencia destacó la necesidad de seguir trabajando en laboratorios seguros para seguir perfeccionando mis capacidades en ciberseguridad.



BIBLIOGRAFÍAS:

<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>