



EDUCACIÓN



TECNOLÓGICO
NACIONAL DE MÉXICO

**TECNOLÓGICO NACIONAL DE MÉXICO
INSTITUTO TECNOLÓGICO DETLAXIACO**

VIRTUALIZACION

Nombre de los Integrantes de equipo:

Fernanda Ruiz Heras	21620151
Ana Michel león león	21620112
Rosa Salazar Doroteo	18620216
Rufino Mendoza Vásquez	21620198

Actividad:

Práctica 6

Docente:

Ing. Edwuar Osorio Salinas

Carrera:

Ingeniería en Sistemas Computacionales

Grupo: 7US

Semestre: Séptimo.



Imagen 1 instalación de virtual Box	5
Imagen 2 aceptación de términos.....	5
Imagen 3 advertencia durante la instalación.....	6
Imagen 4 custom setup.....	6
Imagen 5 proceso de instalación.....	7
Imagen 6 virtualBox administrador.....	7
imagen 7 Pfsense en virtualBox	8
imagen 8 conectividad de una máquina virtual a una red.....	8
imagen 9 redes "host-only".....	9
imagen 10 creación de máquina virtual.....	9
imagen 11 Pfsense configuracion	10
imagen 12 configuración de red	10
imagen 13 ejecucion de Pfsense	11
imagen 14 instalacion de Pfsense	12
imagen 15 seleccion del proceso de instalacion	12
imagen 16 configuración del instalador de pfSense	13
imagen 17 instalacion crucial	13
imagen 18 formateo y sobrescribir el contenido del disco.....	14
imagen 19 extracción los archivos	14
imagen 20 reinicio del sistema automáticamente.....	15
imagen 21 finalizacion del Pfsense	15
Imagen 22 Pfsense	16
Imagen 23 aspectos básicos de Pfsense	16
Imagen 24 configuración del firewall pfSense	17
Imagen 25 asignación de interfaces.....	17
Imagen 26 configuración de las IP.....	18
Imagen 27 seguimiento de las configuraciones.....	18
Imagen 28 IPs asignados	19
Imagen 29 Inicio de instalación de Kali Linux en máquina virtual	20
Imagen 30 Cambio a cuenta de root en Kali Linux usando comando <code>sudo su</code>	20
Imagen 31 instalación de Snort en Kali Linux mediante <code>apt-get install snort</code>	21
Imagen 32 Modificación del archivo <code>sources.list</code> en Kali Linux para gestión de repositorios.....	21
Imagen 33 Visualización de interfaces de red en Kali Linux usando <code>ifconfig</code>	22
Imagen 34 creación de archivo <code>custom.rules</code> en Kali Linux para reglas personalizadas en Snort	22
Imagen 35 Configuración de regla en Snort para alertar sobre ping hacia la dirección IP 192.168.0.101	23
Imagen 36 Definición de red interna (<code>HOME_NET</code>) y externa (<code>EXTERNAL_NET</code>) en archivo de configuración de Snort.....	23
Imagen 37 Ejecución de Snort en la interfaz de red <code>eth0</code> para monitoreo de tráfico en Kali Linux	24
Imagen 38 Configuración de prueba de ping desde Kali Linux hacia dispositivo en rojo para detección.....	24



Imagen 39 Detalle de alerta en Snort por actividad ICMP (ping) detectada hacia la dirección 192.168.0.105	25
Imagen 40 Personalización de reglas de Snort para monitoreo específico de red.....	25
Imagen 41 Configuración final de Snort para iniciar monitoreo de red y detección de intrusiones en Kali Linux.....	26
Imagen 42 instalación dell archivo comprimido metasploitable-linux-2.0.0.zipen sistema anfitrión	27
Imagen 43 Configuración inicial	27
Imagen 44 Configuración inicial de nueva máquina virtual con nombre "Meta" en VirtualBox	28
Imagen 45 Asignación de recursos de hardware (RAM y CPU) a la máquina virtual "Meta" en VirtualBox	28
Imagen 46 Selección de archivo de configuración "Metasploitable" en explorador de archivos	29
Imagen 47 Inicio de la máquina virtual "Metasploitable" en VirtualBox.....	29
Imagen 48 Confirmación de conectividad de red en máquina virtual Metasploitable.....	30
Imagen 49 Proceso de instalación de Windows 10.....	31
Imagen 50 Proceso de arranque inicial de Windows 10	31
Imagen 51 Asignación de recursos de hardware	31
Imagen 52 proceso de instalacion de windows 10	31
Imagen 53 terminación de la instalación	31
Imagen 54 Proceso de arranque inicial de Windows 10	31
Imagen 55 Confirmación de finalización de instalación de Windows 10.....	31
Imagen 56 proceso del ping de windows	31
Imagen 57 sistema en una máquina virtual con Windows 10	31
Imagen 58 ping realizado exitosa mente	31



INTRODUCCIÓN

El presente reporte documenta el proceso de configuración de un entorno virtual de ciberseguridad mediante el uso de software de virtualización como VMware y Oracle VirtualBox. La virtualización permite emular múltiples sistemas operativos y aplicaciones en una sola máquina física, lo cual es especialmente útil para simular y probar configuraciones de red y herramientas de seguridad informática. A lo largo del informe se explican los pasos necesarios para instalar y configurar entornos virtuales en Oracle VirtualBox, incluyendo la selección de opciones iniciales, la aceptación de acuerdos de licencia y la configuración de redes virtuales. Se realiza también la instalación de un firewall en pfSense y de un sistema de detección de intrusos (IDS) en Kali Linux, detallando cada etapa de configuración de red y gestión de interfaces, esenciales para implementar y mantener un entorno seguro.

Además de las instalaciones individuales, se revisa la creación de redes host-only y adaptadores puente, aspectos que permiten configurar redes internas y personalizadas, aisladas de la red anfitriona para proteger el entorno virtual. Con este tipo de configuración, es posible simular ataques y evaluar las respuestas de sistemas de defensa como los firewalls y los IDS. Finalmente, el informe incluye la instalación de una máquina virtual con Metasploitable2, diseñada intencionalmente con vulnerabilidades, para realizar pruebas de penetración controladas. Este laboratorio virtual no solo facilita el aprendizaje y la práctica de conceptos clave en ciberseguridad, sino que también permite experimentar en un entorno aislado, minimizando los riesgos para el sistema anfitrión y para la red externa.

DESARROLLO

1. INSTALAR VMWARE O VIRTUAL BOX.

- 📌 Aquí se muestra la pantalla de instalación de VMware/VirtualBox, donde se están seleccionando las opciones de configuración inicial y el directorio de instalación en el sistema operativo anfitrión.

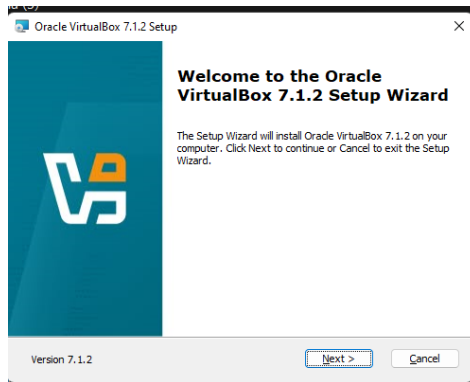


Imagen 1 instalación de virtual Box

- 📌 Se muestra una pantalla de instalación de **Oracle VirtualBox 7.1.2** en Windows, donde el usuario debe aceptar el **Acuerdo de Licencia de Usuario Final** para continuar.

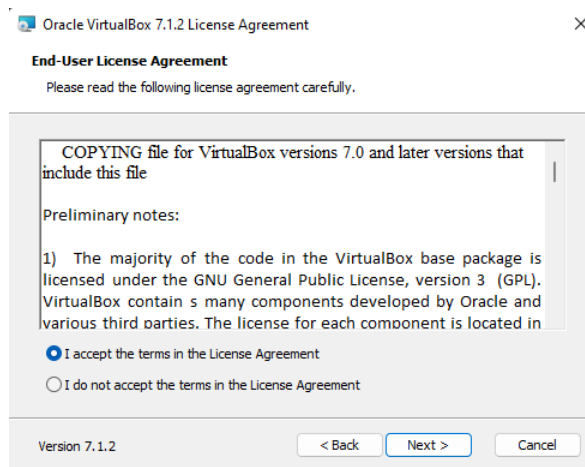


Imagen 2 aceptación de términos

- Se muestra una pantalla de advertencia durante la instalación de **Oracle VirtualBox 7.1.2** en Windows. El mensaje advierte al usuario que la función de red del software restablecerá temporalmente la conexión de red y lo desconectará brevemente. Se pregunta si desea proceder con la instalación en estas condiciones.

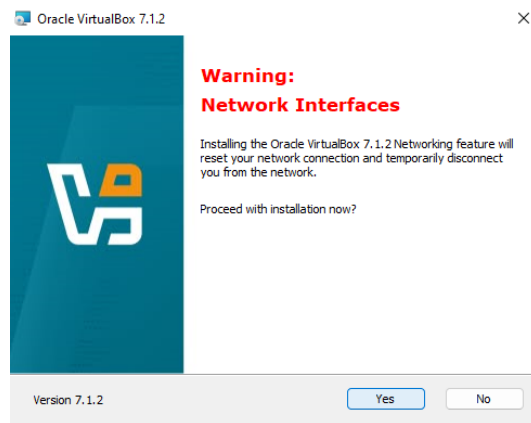


Imagen 3 advertencia durante la instalación

- Esta ventana de configuración permite al usuario personalizar la instalación de Oracle VirtualBox seleccionando las opciones que desea. Las opciones disponibles incluyen crear accesos directos en diferentes ubicaciones y registrar asociaciones de archivos.

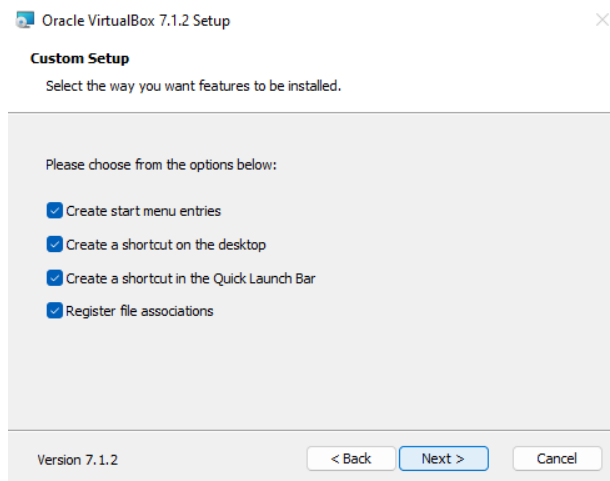


Imagen 4 custom setup

- Esta pantalla te informa de que la instalación de Oracle VirtualBox está en curso y te pide que esperes hasta que finalice. No es necesario que hagas nada más en este momento, a menos que quieras cancelar la instalación.

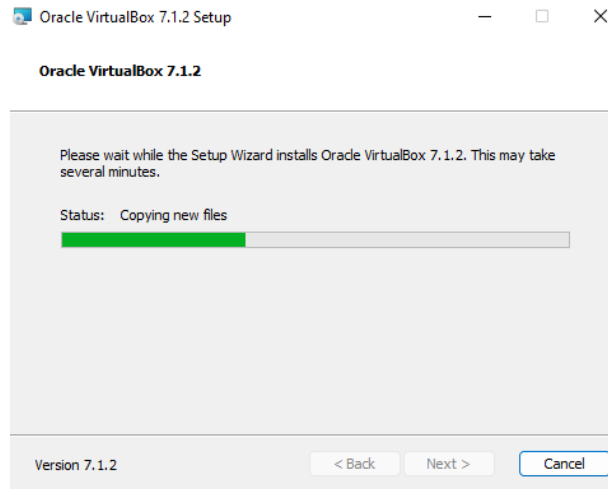


Imagen 5 proceso de instalación

- La ventana principal de VirtualBox ofrece un punto de partida para crear y gestionar las máquinas virtuales. La elección entre el Modo Básico y el Modo Experto dependerá de nuestros conocimientos y necesidades.



Imagen 6 virtualBox administrador

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

La ventana principal de VirtualBox es el centro de control para gestionar todas las máquinas virtuales. Desde aquí podemos crear nuevas máquinas, configurarlas, iniciarlas, apagarlas y realizar muchas otras acciones. Dándole herramientas no manda otras opciones donde se selecciona la opción administradora de medios virtuales

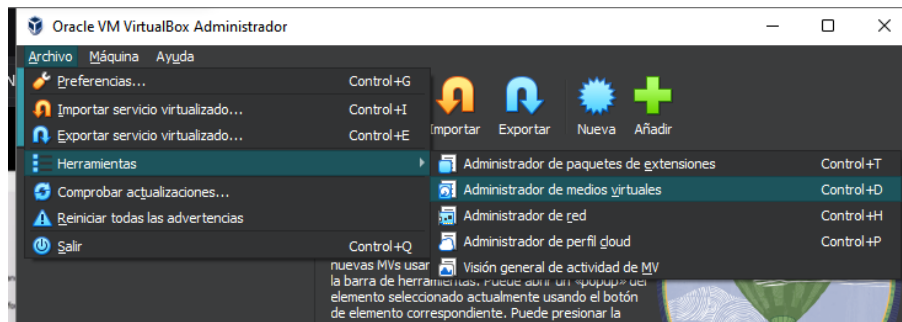


imagen 7 Pfsense en virtualBox

La ventana del Administrador de redes en VirtualBox nos brinda un control preciso sobre cómo se conectan nuestras máquinas virtuales a la red. Configurar correctamente las redes es esencial para garantizar un funcionamiento adecuado a las máquinas virtuales y para crear entornos de red personalizados. Donde se configuro un adaptador manualmente ipv4 "192.168.111.1" con una máscara de red "255.255.255.0"

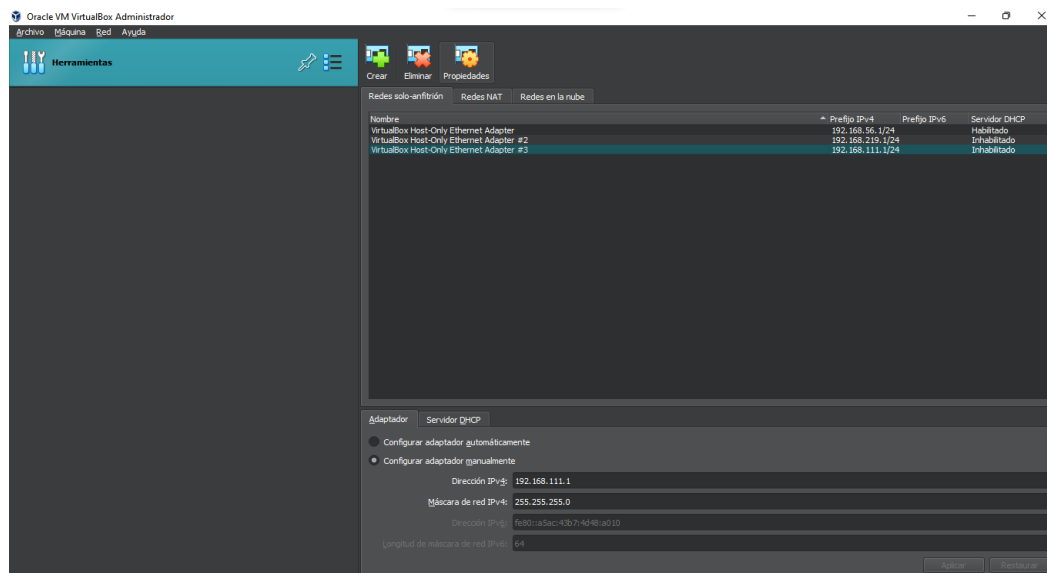


imagen 8 conectividad de una máquina virtual a una red

- Se muestra la sección de gestión de redes "host-only" en Oracle VirtualBox, donde se pueden crear, eliminar y configurar redes virtuales aisladas para las máquinas virtuales, separándolas de la red física del equipo.

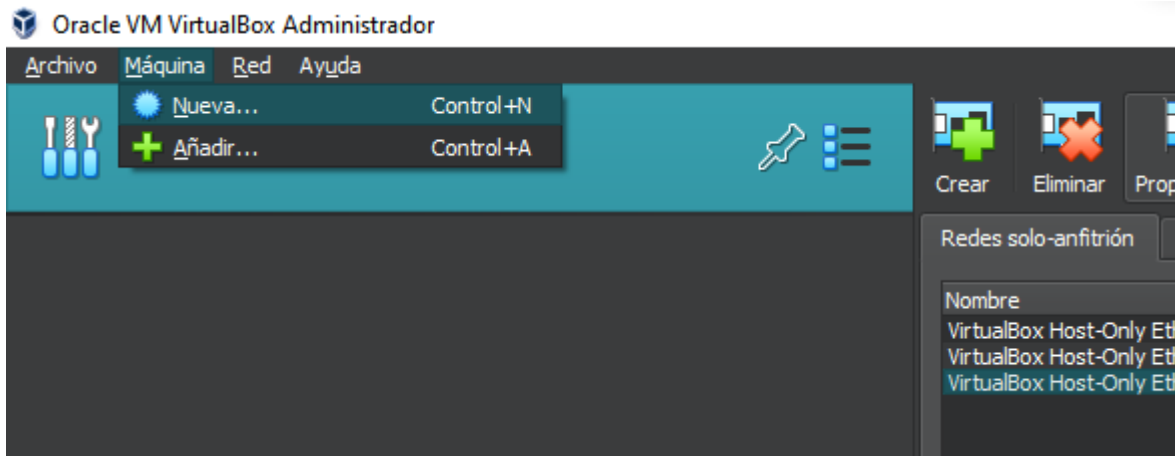


imagen 9 redes "host-only"

- Se muestra la ventana de configuración de una nueva máquina virtual en Oracle VirtualBox. En esta sección, se pueden definir el nombre en este caso es **"Pfsense"** de la máquina virtual, la carpeta de destino, y seleccionar una imagen ISO para instalar el sistema operativo. Además, se especifica el tipo y la versión del sistema operativo invitado.

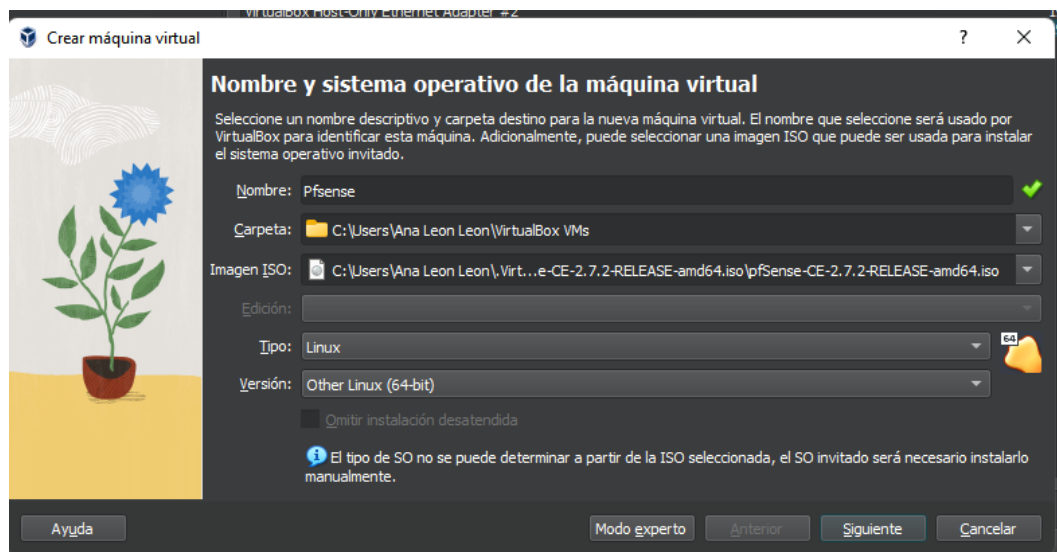


imagen 10 creación de máquina virtual

- Se muestra la configuración de red de una máquina virtual en Oracle VirtualBox. En esta sección, se puede habilitar el adaptador de red y seleccionar el tipo de conexión, en este caso configurado como "Adaptador puente" con un adaptador de red físico específico.

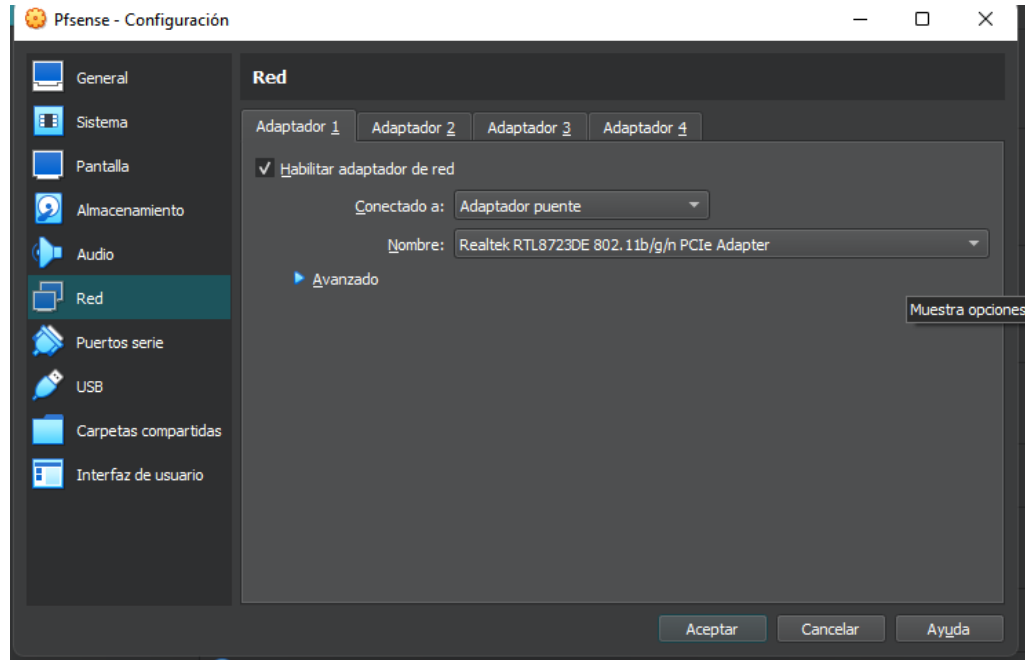


imagen 11 Pfsense configuracion

- Se muestra la configuración de red de una máquina virtual en Oracle VirtualBox, con el adaptador configurado como "Adaptador solo anfitrión". Esta opción permite conectar la máquina virtual a una red virtual aislada, usando el adaptador "VirtualBox Host-Only Ethernet Adapter #2".

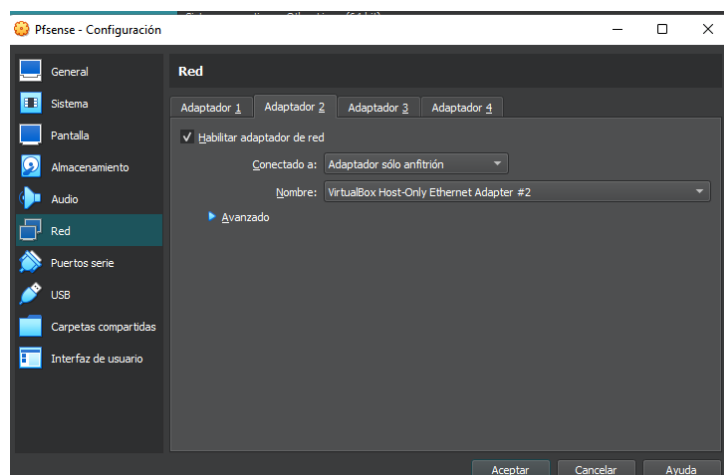
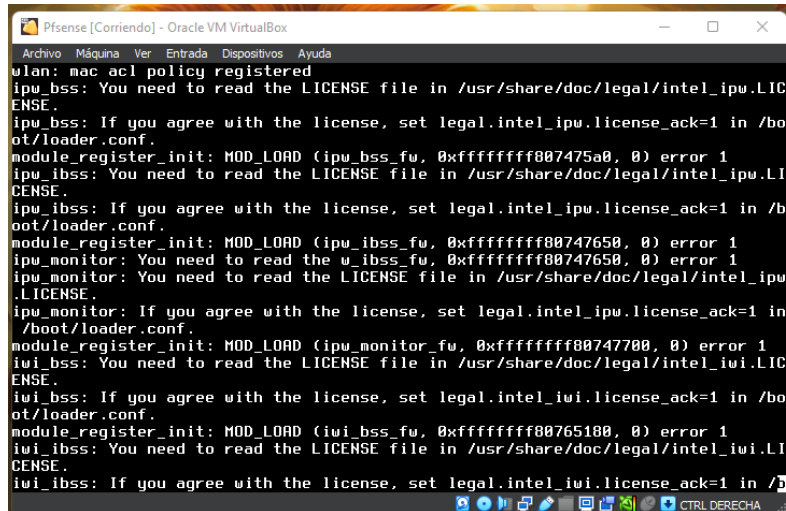


imagen 12 configuración de red

- En la imagen, se está ejecutando **pfSense**, un sistema de firewall basado en **FreeBSD**, dentro de una máquina virtual en **Oracle VM VirtualBox**. Durante el arranque, aparecen mensajes de advertencia relacionados con ciertos módulos de hardware de Intel, como **ipu_bss** y **iwi_bss**, indicando que se necesita aceptar las licencias de estos módulos.



```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
wlan: mac acl policy registered
ipu_bss: You need to read the LICENSE file in /usr/share/doc/legal/intel_ipu.LI
ENSE.
ipu_bss: If you agree with the license, set legal.intel_ipu.license_ack=1 in /bo
ot/loader.conf.
module_register_init: MOD_LOAD (ipu_bss_fw, 0xffffffff807475a0, 0) error 1
ipu_ibss: You need to read the LICENSE file in /usr/share/doc/legal/intel_ipu.LI
CENSE.
ipu_ibss: If you agree with the license, set legal.intel_ipu.license_ack=1 in /b
oot/loader.conf.
module_register_init: MOD_LOAD (ipu_ibss_fw, 0xffffffff80747650, 0) error 1
ipu_monitor: You need to read the LICENSE file in /usr/share/doc/legal/intel_ipu
.LICENSE.
ipu_monitor: If you agree with the license, set legal.intel_ipu.license_ack=1 in /b
oot/loader.conf.
module_register_init: MOD_LOAD (ipu_monitor_fw, 0xffffffff80747700, 0) error 1
iwi_bss: You need to read the LICENSE file in /usr/share/doc/legal/intel_iwi.LI
CENSE.
iwi_bss: If you agree with the license, set legal.intel_iwi.license_ack=1 in /bo
ot/loader.conf.
module_register_init: MOD_LOAD (iwi_bss_fw, 0xffffffff80765180, 0) error 1
iwi_ibss: You need to read the LICENSE file in /usr/share/doc/legal/intel_iwi.LI
CENSE.
iwi_ibss: If you agree with the license, set legal.intel_iwi.license_ack=1 in /b
```

imagen 13 ejecución de Pfsense

Instalación del Pfsense

- Se muestra en pantalla la instalación de **pfSense**, en la que se presentan los avisos de derechos de autor y marcas registradas de la distribución. seleccionar la opción **[Aceptar]**.

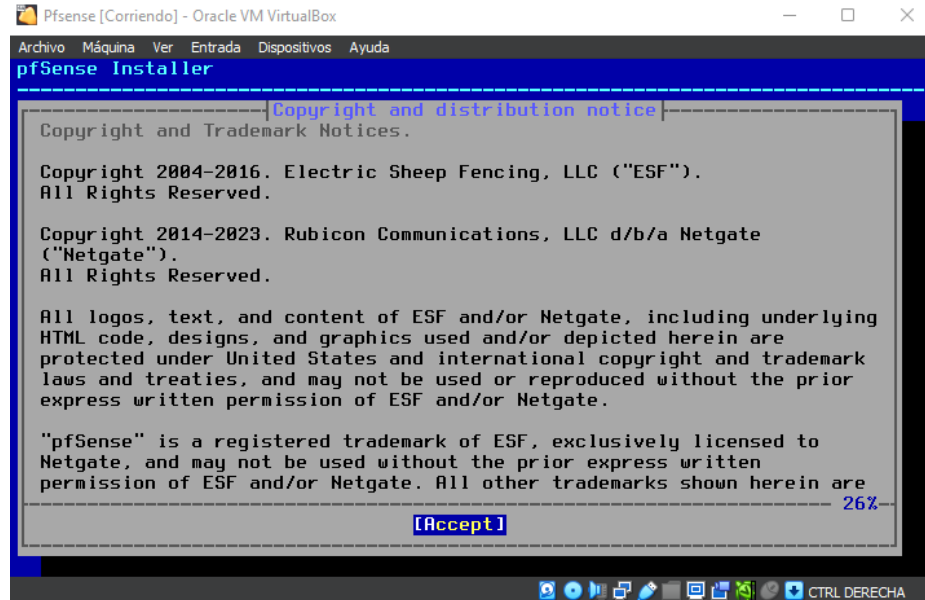


imagen 14 instalacion de Pfsense

- En la pantalla de partición de disco de **pfSense** se seleccione la opción **Auto (ZFS)** para configurar el sistema de archivos automáticamente con ZFS, recomendado por su confiabilidad y rendimiento. Esta opción es ideal para sistemas con 8 GB de RAM o más, aunque se puede ajustar para menor memoria siguiendo la guía de **FreeBSD**. Al seleccionar **Auto (ZFS)**, el instalador creará automáticamente las particiones necesarias, facilitando la instalación y optimizando el rendimiento de **pfSense**.

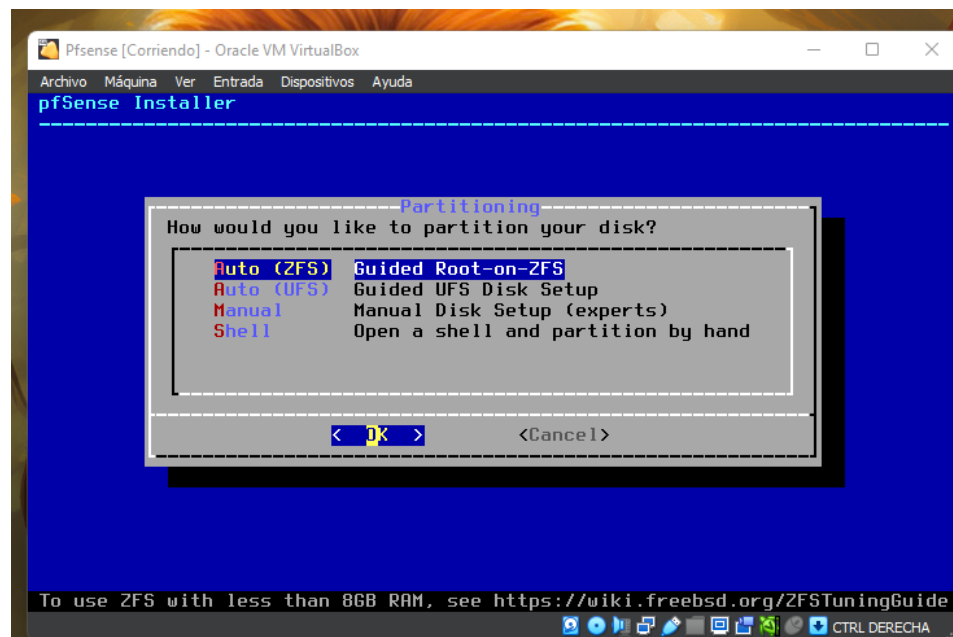


imagen 15 seleccion del proceso de instalacion

- Se muestra una pantalla de configuración del instalador de pfSense donde se están definiendo las opciones para crear el sistema de archivos ZFS. Esta configuración es fundamental para el correcto funcionamiento del firewall. Donde seleccionamos la opción S "Swap Size" donde se está definiendo la cantidad de espacio en disco que se asignará al espacio de intercambio.

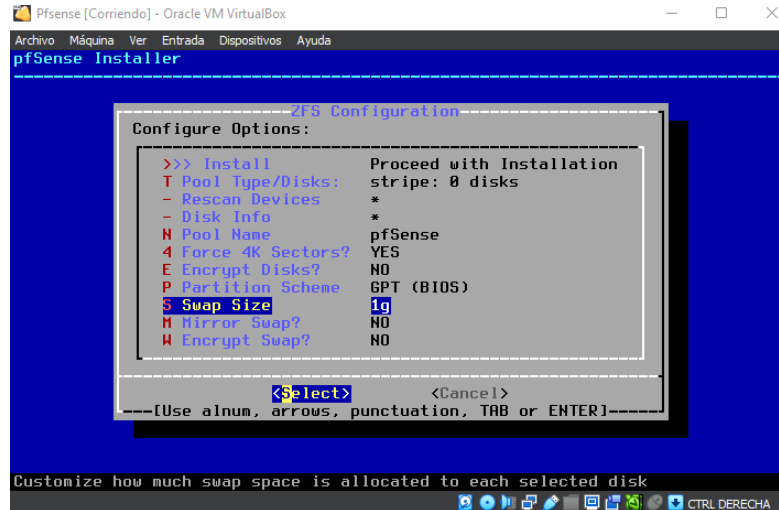


imagen 16 configuración del instalador de pfSense

- Se muestra que ha llegado a una etapa crucial de la instalación de pfSense, donde estás confirmando el dispositivo de almacenamiento que se utilizará para el sistema.
- [*]: El asterisco indica que este dispositivo está seleccionado.
- ada0: Es el nombre del dispositivo.
- VBOX HARDDISK: Indica que es un disco duro virtual creado dentro de VirtualBox.

Al seleccionar la opción "OK", estaremos indicando al instalador que utilice este disco para crear el pool de almacenamiento ZFS.

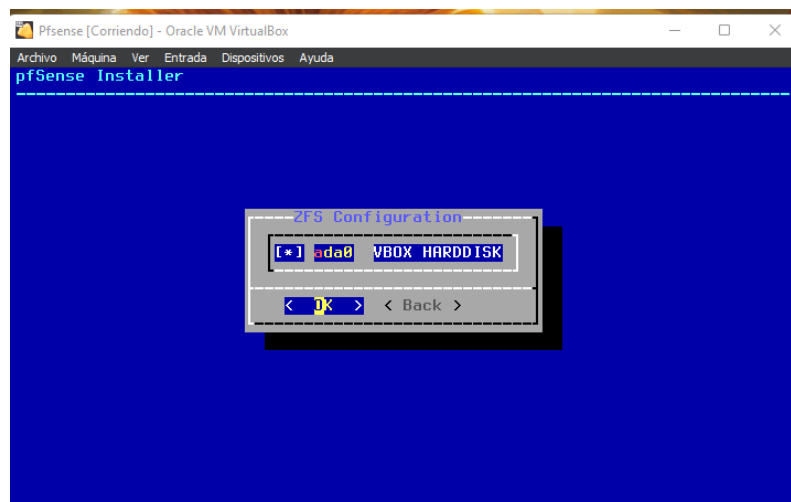


imagen 17 instalacion crucial

- Se muestra la siguiente pantalla es un punto crítico en el proceso de instalación. seleccionar la opción correcta para evitar perder datos importantes. El instalador se está preguntando si estás **seguro de querer formatear y sobrescribir todo el contenido del disco** seleccionado (en este caso, "ada0"). Seleccionamos "YES".

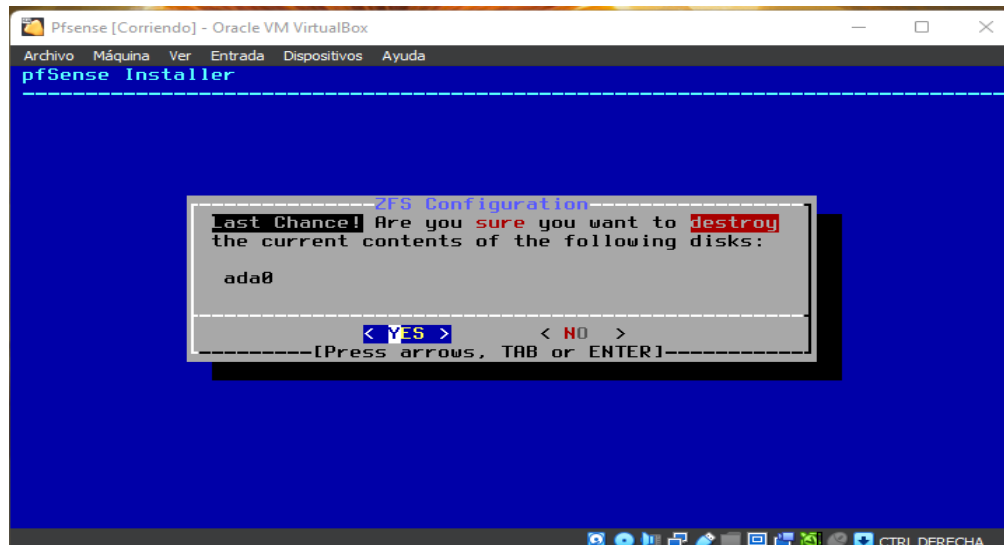


imagen 18 formateo y sobrescribir el contenido del disco

- El sistema está preparando los archivos necesarios para instalar pfSense en el sistema. El instalador de pfSense está extrayendo los archivos necesarios para la instalación desde un archivo comprimido llamado "base.txz".

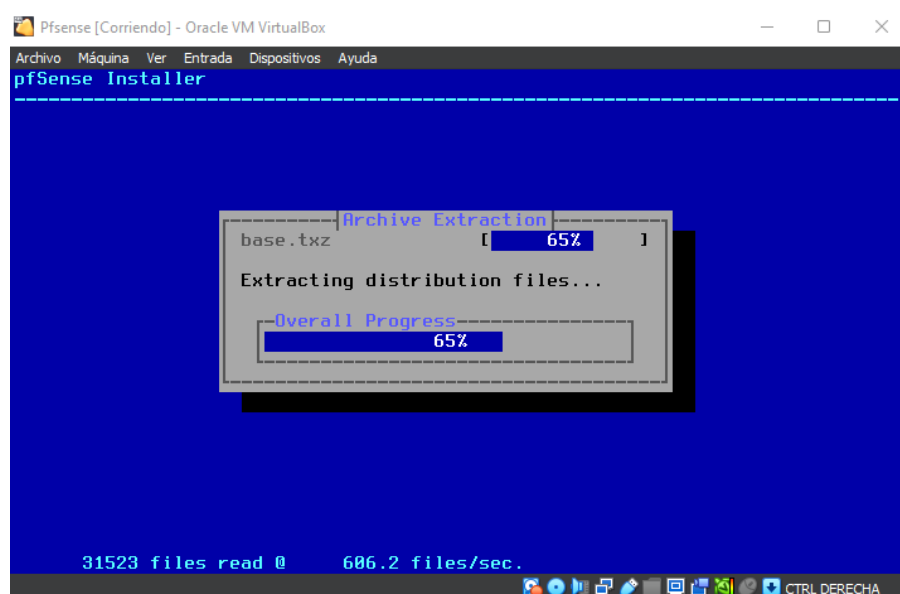


imagen 19 extracción los archivos

- Una vez terminado el proceso de instalación seleccionamos la opción “REBOOT”, donde el sistema se reiniciará automáticamente y arrancará directamente en el nuevo sistema operativo pfSense.

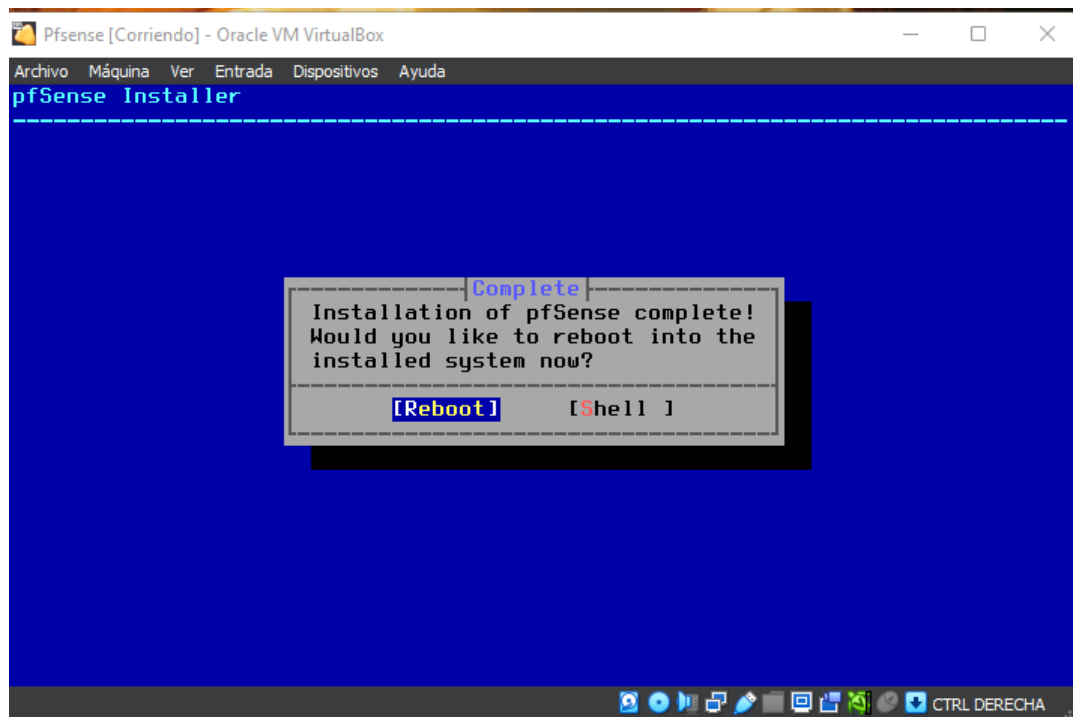


imagen 20 reinicio del sistema automáticamente

- El instalador ha finalizado de copiar e instalar todos los archivos necesarios de pfSense en tu sistema. Donde seleccionamos Boot **Multi user** [Enter]: Esta es la opción recomendada para la mayoría de los usuarios. Al seleccionarla, se iniciará pfSense en modo multiusuario, lo que nos permitirá acceder a la interfaz web para configurar el firewall.

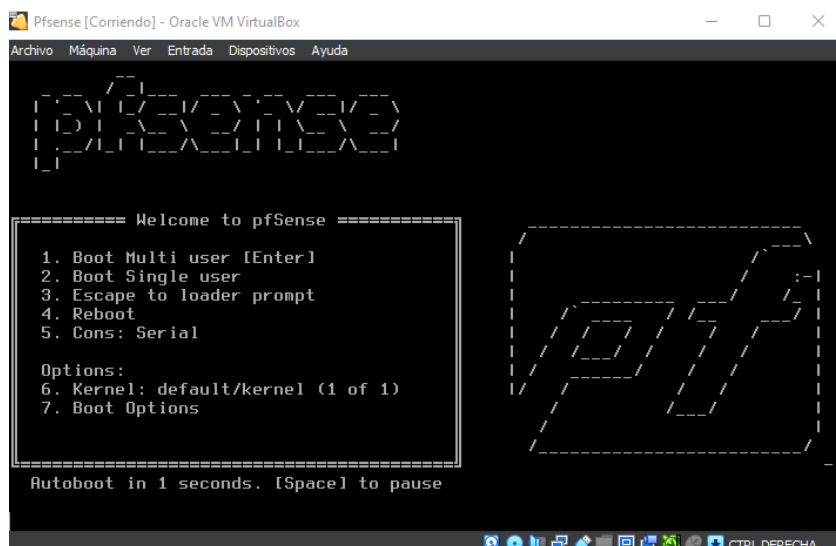


imagen 21 finalizacion del Pfsense

- Esta pantalla brinda la oportunidad de personalizar algunos aspectos básicos de la instalación de pfSense.

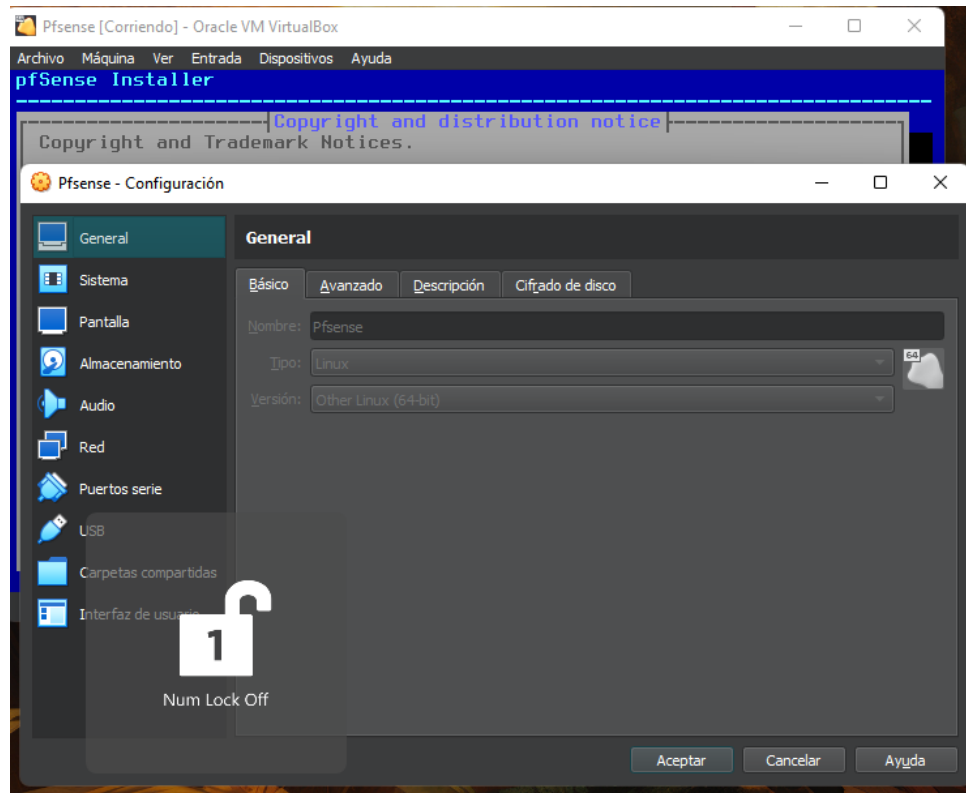


Imagen 22 PfSense

- Esta ventana permite personalizar algunos aspectos básicos de la instalación de pfSense. Una vez que se haga clic en "Aceptar", el instalador continuará con los pasos finales y estará listo para reiniciar y comenzar a usar el nuevo firewall.

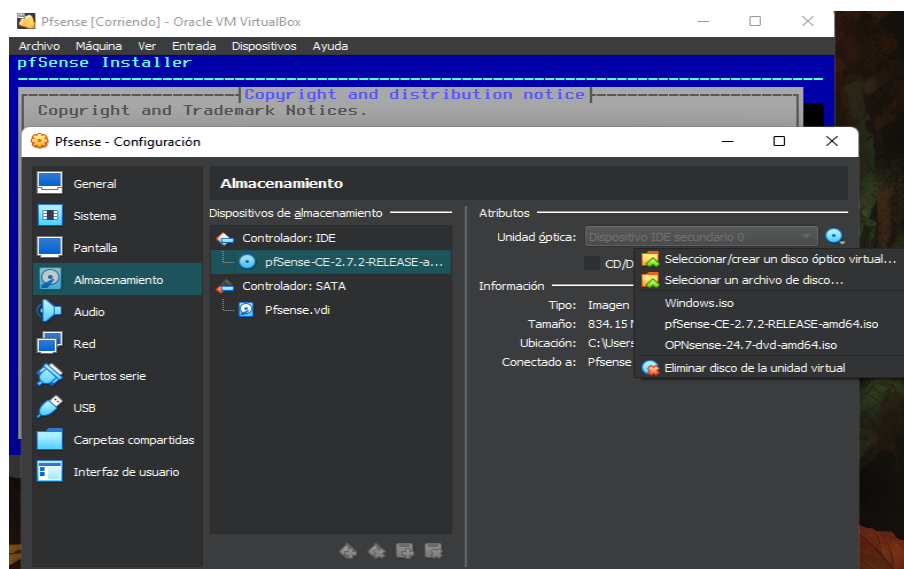
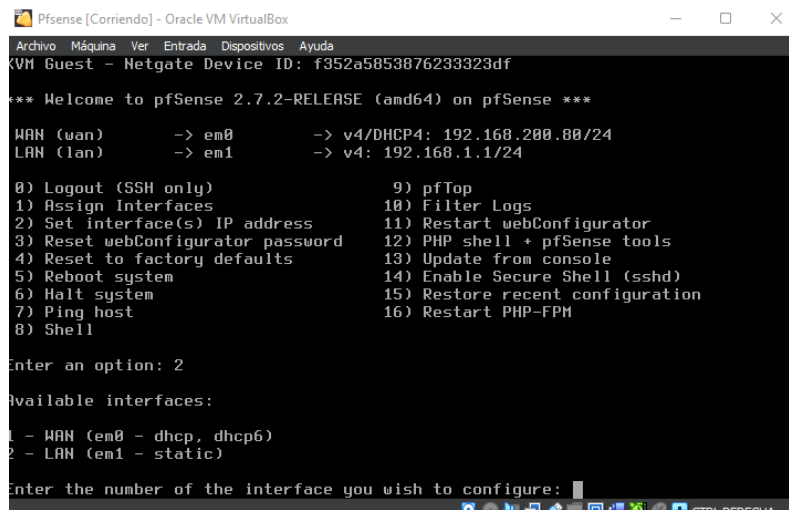


Imagen 23 aspectos básicos de PfSense

- Esta pantalla ofrece las herramientas básicas para configurar el firewall pfSense desde consola. Donde posterior se selecciona la opción 2 indicado que deseas configurar las interfaces de red.



```
Pfsense [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
VM Guest - Netgate Device ID: f352a5853876233323df

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.200.80/24
LAN (lan)       -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: 2

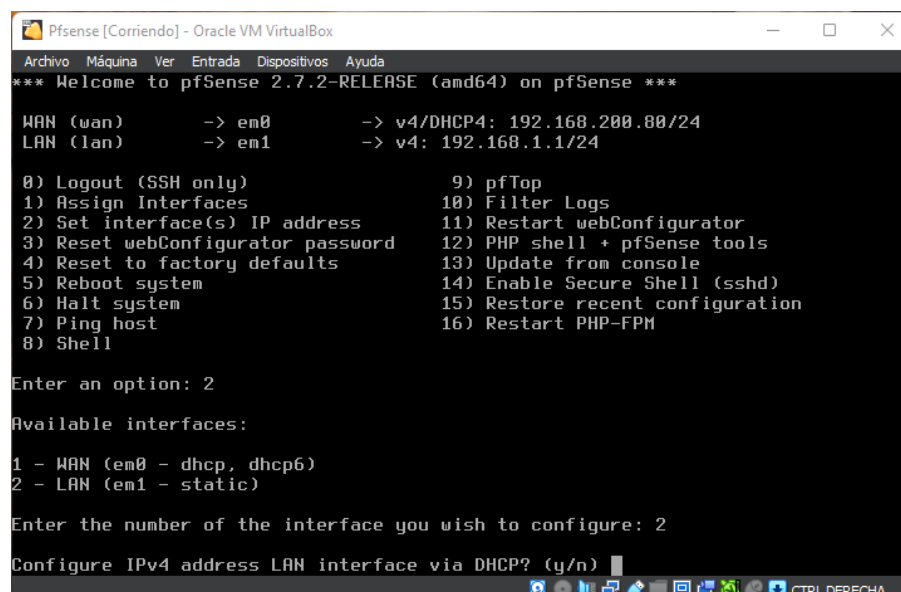
Available interfaces:

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

Enter the number of the interface you wish to configure: 
```

Imagen 24 configuración del firewall pfSense

- Después de elegir la opción 2 para asignar interfaces, el sistema ha presentado las opciones disponibles y se ha seleccionado la interfaz LAN (número 2). Ahora, pfSense pregunta si deseas configurar la dirección IP de la interfaz LAN de forma automática a través de DHCP (Dynamic Host Configuration Protocol) o si prefieres asignarle una dirección IP estática manualmente. Posteriormente se selecciona n: Si seleccionas "y", pfSense buscará automáticamente una dirección IP disponible en la red local a través del servidor DHCP.



```
Pfsense [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.200.80/24
LAN (lan)       -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:

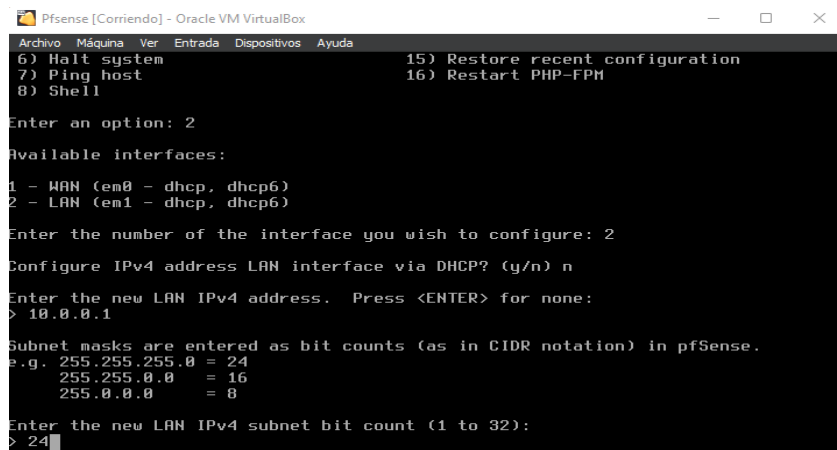
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) 
```

Imagen 25 asignación de interfaces

- Después de elegir la interfaz LAN, se ha decidido **no** utilizar DHCP para obtener una dirección IP automáticamente. En lugar de eso, se está ingresando manualmente la dirección IP que se desea asignar a la interfaz LAN. En esta pantalla, se te pide que ingreses la máscara de subred en notación CIDR (Classless Inter-Domain Routing). En lugar de escribir la máscara de subred completa (por ejemplo, 255.255.255.0), solo ingresamos el número de bits que representan la parte de red de la dirección IP. En este caso asignamos el número 24. Esto significa que los primeros 24 bits de la dirección IP (10.0.0.1) corresponden a la red y los últimos 8 bits corresponden al host. En otras palabras, la red local puede tener hasta 254 dispositivos con direcciones IP que comiencen por 10.0.0.1.



```
Pfsense [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
6) Halt system
7) Ping host
8) Shell
15) Restore recent configuration
16) Restart PHP-FPM

Enter an option: 2

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

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

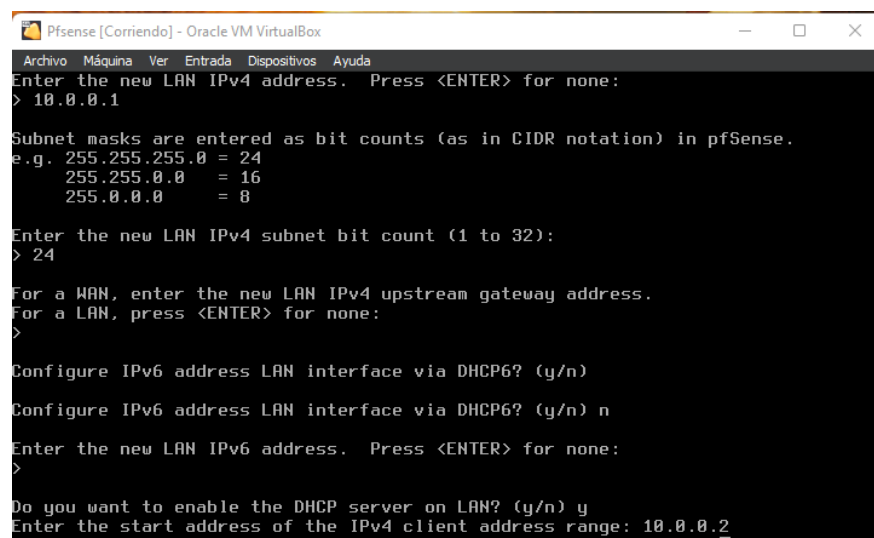
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.0.0.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
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
```

Imagen 26 configuración de las IP

- En las etapas anteriores, ya hemos ingresado la dirección IP que tendrá tu interfaz LAN (10.0.0.1) y la máscara de subred en notación CIDR (24 bits). Esto define el rango de direcciones IP disponibles en tu red local. Donde posteriormente como rango inicial **10.0.0.2**. y como rango final **10.0.0.20**. damos enter para seguir con las configuraciones.



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

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.0.0.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
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

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

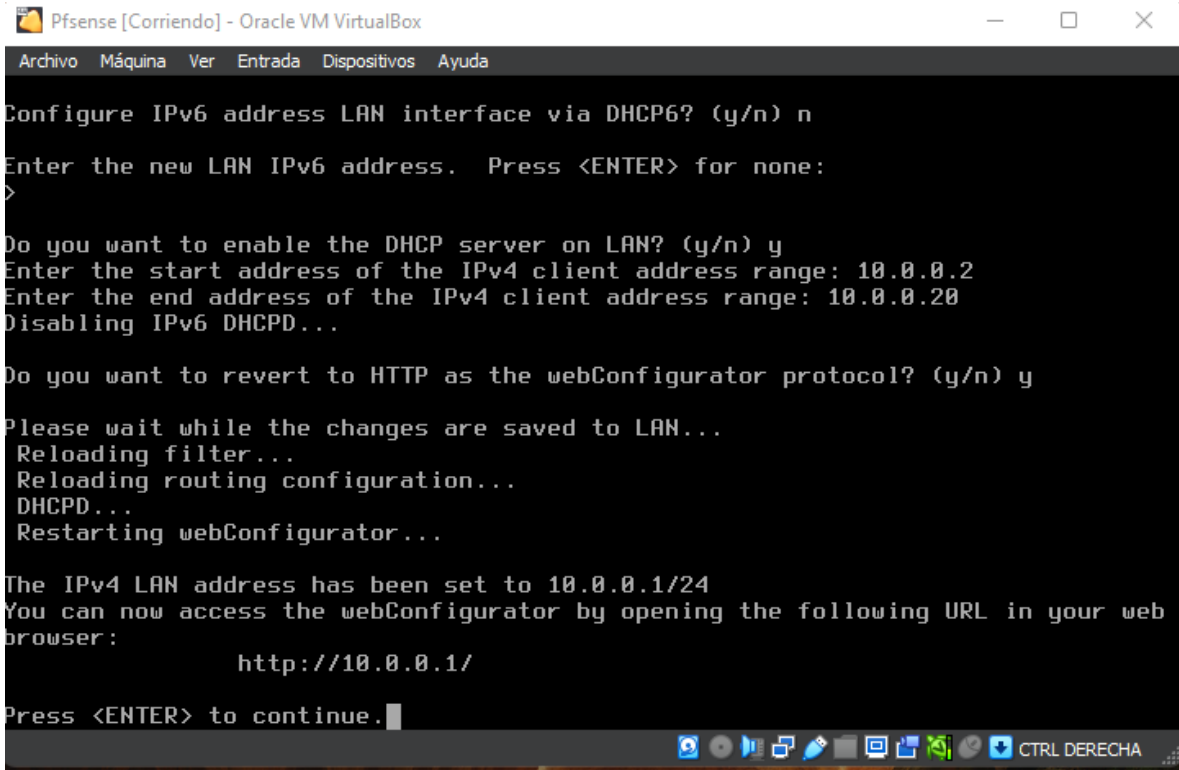
Configure IPv6 address LAN interface via DHCP6? (y/n)
Configure IPv6 address LAN interface via DHCP6? (y/n) n

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 10.0.0.2
Enter the end address of the IPv4 client address range: 10.0.0.20
```

Imagen 27 seguimiento de las configuraciones

- En esta parte una vez darle enter a la ventana anterior se muestra una indicación si queremos reiniciar le damos Y, ENTER , se muestra la ip con la que está asignado, nos muestra un código donde se está reiniciando



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

Configure IPv6 address LAN interface via DHCP6? (y/n) n
Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 10.0.0.2
Enter the end address of the IPv4 client address range: 10.0.0.20
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...
Restarting webConfigurator...

The IPv4 LAN address has been set to 10.0.0.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
    http://10.0.0.1/

Press <ENTER> to continue.
```

Imagen 28 IPs asignados

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

- Instalamos principalmente Kali Linux

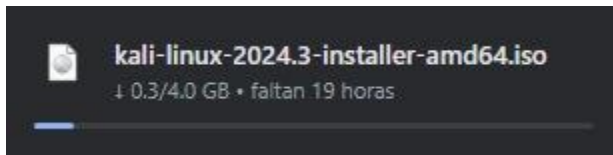


Imagen 29 Inicio de instalación de Kali Linux en máquina virtual

- Se muestra el momento justo antes de que el usuario obtenga los privilegios de administrador en el sistema Kali Linux.

Al ejecutar `sudo su`, el usuario está solicitando cambiar a la cuenta de root. Esto le otorgará todos los permisos para realizar cualquier acción en el sistema, desde instalar software hasta modificar la configuración del sistema.

(kali@kali:~/home/kali) indica el usuario actual (kali), el nombre del equipo (kali) y el directorio actual (/home/kali).

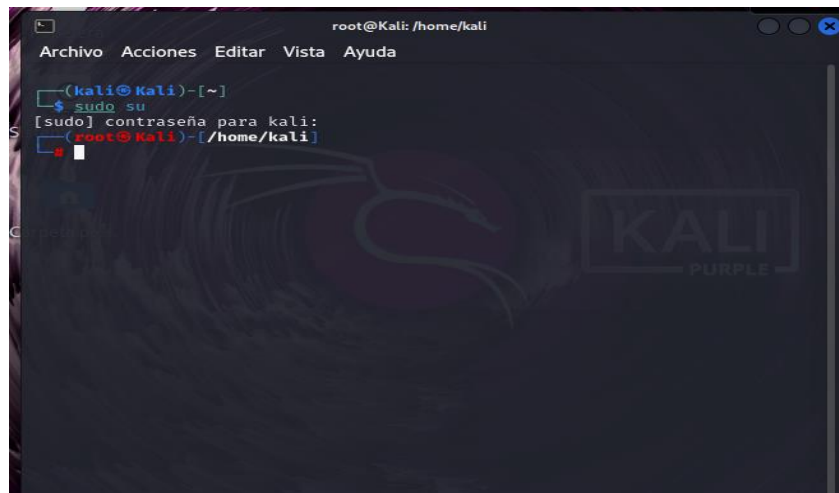
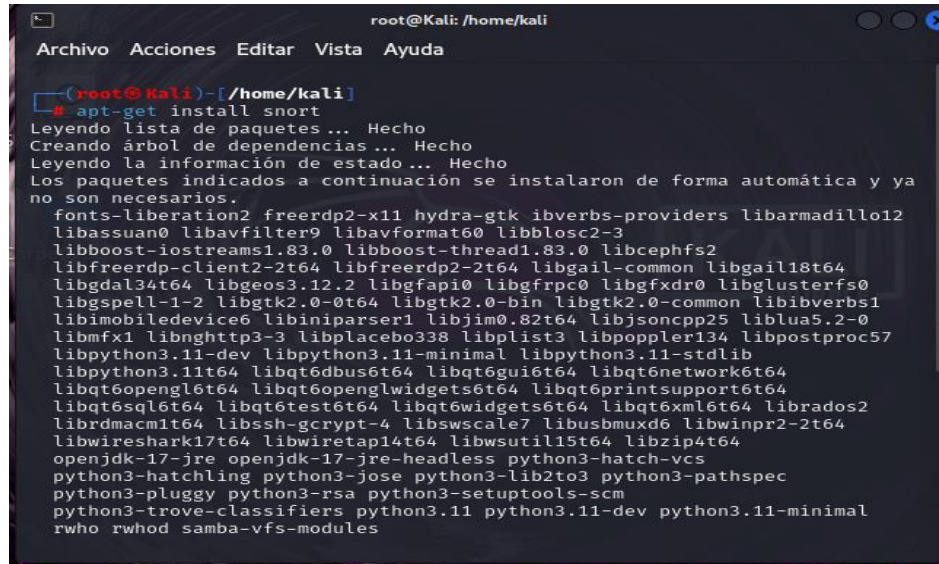


Imagen 30 Cambio a cuenta de root en Kali Linux usando comando `sudo su`

- Se muestra el momento en el que se está instalando Snort en el sistema Kali Linux. Este proceso implica descargar e instalar no solo Snort, sino también una serie de paquetes adicionales que son necesarios para su funcionamiento.

EL comando `apt-get install snort`: Este comando le indica al sistema que instale un nuevo programa llamado "snort". Snort es una herramienta de detección de

intrusiones (IDS), muy utilizada en seguridad informática para monitorizar redes y detectar posibles ataques.



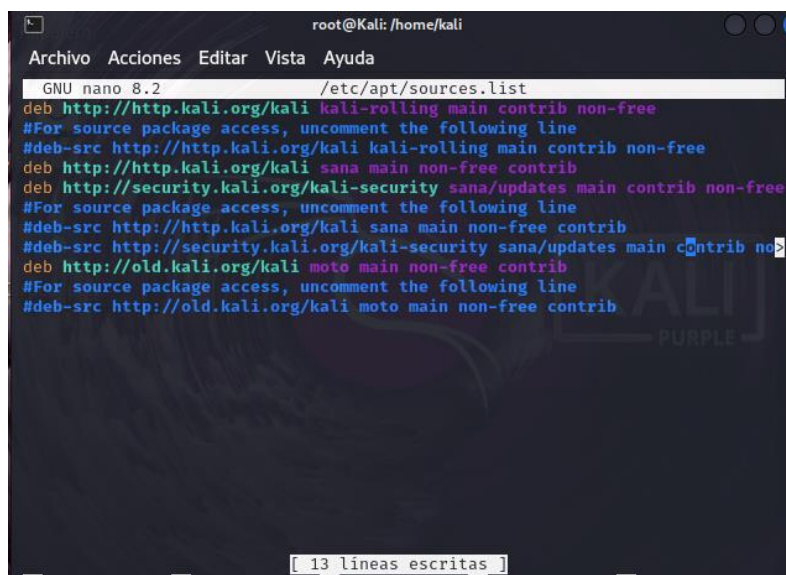
```
root@kali: /home/kali
Archivo Acciones Editar Vista Ayuda

(root@kali)-[/home/kali]
# apt-get install snort
Leyendo lista de paquetes ... Hecho
Creando árbol de dependencias ... Hecho
Leyendo la información de estado ... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya
no son necesarios.
fonts-liberation2 freerdp2-x11 hydra-gtk ibverbs-providers libarmadillo12
libassuan0 libavfilter9 libavformat60 libblosc2-3
libboost-iostreams1.83.0 libboost-thread1.83.0 libcephfs2
libfreerdp-client2-2t64 libfreerdp2-2t64 libgail-common libgail18t64
libgdal34t64 libgeos3.12.2 libgfapi0 libgfrpc0 libgfxdr0 libglusterfs0
libgspell1-1-2 libgtk2.0-0t64 libgtk2.0-bin libgtk2.0-common libibverbs1
libimobiledevice6 libiniparser1 libjim0.82t64 libjsoncpp25 liblua5.2-0
libmfx1 libnghttp3-3 libplacebo338 libplist3 libpoppler134 libpostproc57
libpython3.11-dev libpython3.11-minimal libpython3.11-stdlib
libpython3.11t64 libqt6dbus6t64 libqt6gui6t64 libqt6network6t64
libqt6opengl6t64 libqt6openglwidgets6t64 libqt6printsupport6t64
libqt6sql6t64 libqt6test6t64 libqt6widgets6t64 libqt6xml6t64 librados2
librdmacm1t64 libssh-gcrypt-4 libswscale7 libusbmuxd6 libwinpr2-2t64
libwirehark17t64 libwiretap14t64 libwsutil15t64 libzip4t64
openjdk-17-jre openjdk-17-jre-headless python3-hatch-vcs
python3-hatchling python3-jose python3-lib2to3 python3-pathspect
python3-pluggy python3-rsa python3-setuptools-scm
python3-trove-classifiers python3.11 python3.11-dev python3.11-minimal
rwho rwhod samba-vfs-modules
```

Imagen 31 instalación de Snort en Kali Linux mediante `apt-get install snort`

El archivo `sources.list` determina qué software está disponible para su instalación en el sistema. Al modificar este archivo, se puede personalizar el conjunto de paquetes disponibles y controlar desde dónde se obtienen. Se muestra al usuario interactuando con el archivo `sources.list` de Kali Linux, que es fundamental para gestionar las fuentes de software del sistema.

main, contrib, non-free: Estos son secciones dentro de los repositorios que contienen diferentes tipos de paquetes (software libre, contribuciones de terceros, software no libre, etc.).



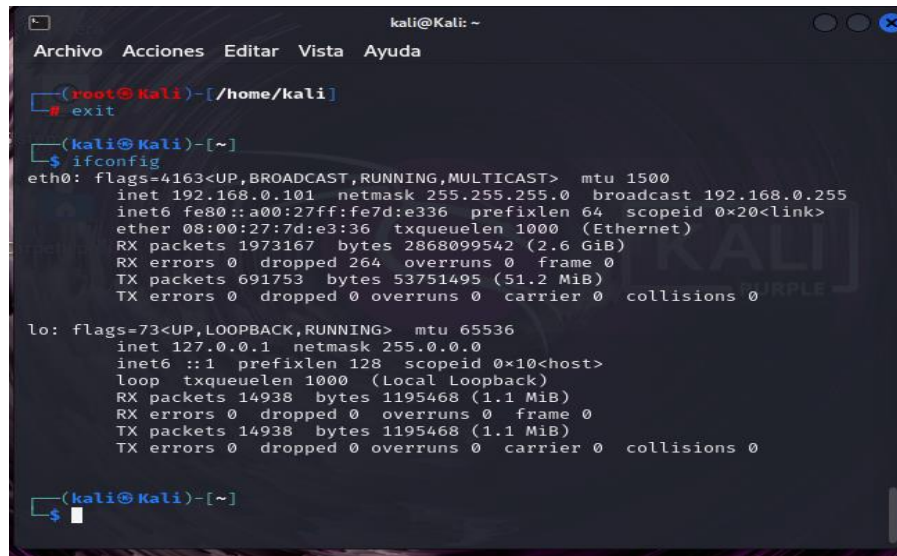
```
root@kali: /home/kali
Archivo Acciones Editar Vista Ayuda

GNU nano 8.2 /etc/apt/sources.list
deb http://http.kali.org/kali kali-rolling main contrib non-free
#For source package access, uncomment the following line
#deb-src http://http.kali.org/kali kali-rolling main contrib non-free
deb http://http.kali.org/kali sana main non-free contrib
deb http://security.kali.org/kali-security sana/updates main contrib non-free
#For source package access, uncomment the following line
#deb-src http://http.kali.org/kali sana main non-free contrib
#deb-src http://security.kali.org/kali-security sana/updates main contrib no
deb http://old.kali.org/kali moto main non-free contrib
#For source package access, uncomment the following line
#deb-src http://old.kali.org/kali moto main non-free contrib

[ 13 líneas escritas ]
```

Imagen 32 Modificación del archivo `sources.list` en Kali Linux para gestión de repositorios

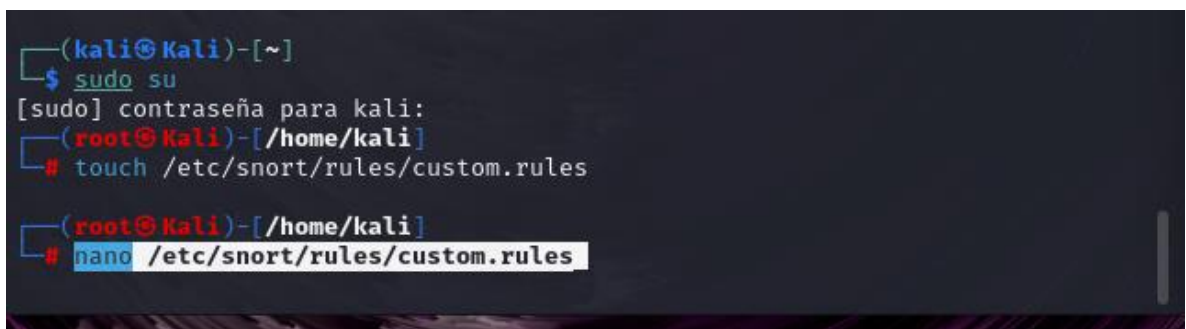
- En este apartado el sistema Kali Linux tiene al menos dos interfaces de red activas: una conexión Ethernet (eth0) y una interfaz de bucle (lo). La conexión Ethernet está configurada con una dirección IP y está lista para comunicarse en la red. Donde se ha ejecutado el comando `ifconfig` en la terminal de Kali Linux para obtener información detallada sobre las interfaces de red de su sistema. La salida del comando muestra información sobre la dirección IP, máscara de subred, dirección MAC y estadísticas de tráfico de cada interfaz.



```
kali@Kali: ~  
Archivo Acciones Editar Vista Ayuda  
(root@Kali)~[/home/kali]  
# exit  
(kali@Kali)~[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.0.101 netmask 255.255.255.0 broadcast 192.168.0.255  
    inet6 fe80::a00:27ff:fe7d:e336 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:7d:e3:36 txqueuelen 1000 (Ethernet)  
    RX packets 1973167 bytes 2868099542 (2.6 GiB)  
    RX errors 0 dropped 264 overruns 0 frame 0  
    TX packets 691753 bytes 53751495 (51.2 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 14938 bytes 1195468 (1.1 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 14938 bytes 1195468 (1.1 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@Kali)~[~]  
$
```

Imagen 33 Visualización de interfaces de red en Kali Linux usando `ifconfig`

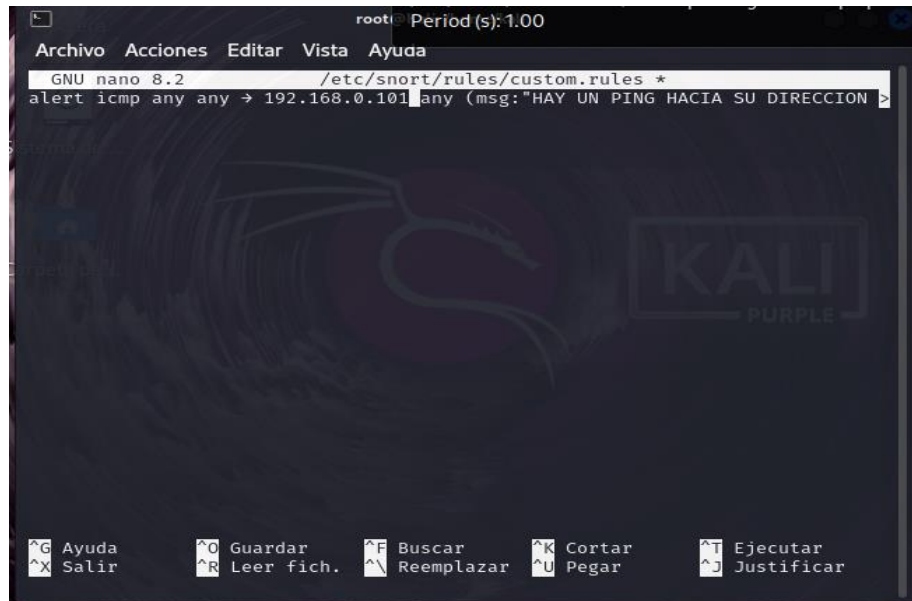
- El usuario está personalizando su sistema de detección de intrusiones para mejorar la seguridad de su red. Se cambia al usuario root (`sudo su`) para obtener permisos administrativos en Kali Linux, lo que permite realizar cambios en el sistema. Luego, se crea un archivo vacío llamado `custom.rules` en `/etc/snort/rules/` (`touch /etc/snort/rules/custom.rules`), destinado a almacenar reglas personalizadas para el sistema de detección de intrusiones Snort. Finalmente, se abre este archivo con `nano` para agregar o modificar las reglas que Snort utilizará para monitorear el tráfico de red.



```
(kali@Kali)~[~]  
$ sudo su  
[sudo] contraseña para kali:  
(root@Kali)~[/home/kali]  
# touch /etc/snort/rules/custom.rules  
  
(root@Kali)~[/home/kali]  
# nano /etc/snort/rules/custom.rules
```

Imagen 34 creación de archivo `custom.rules` en Kali Linux para reglas personalizadas en Snort

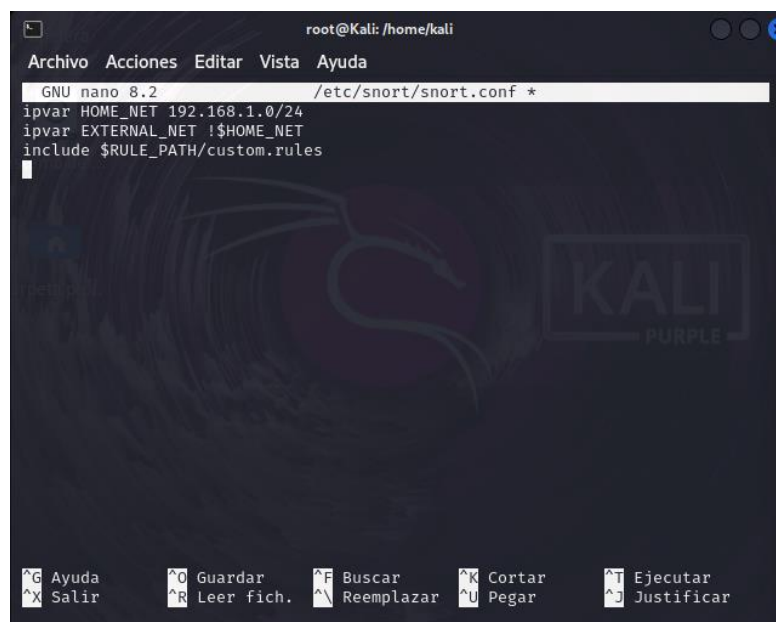
- Se está editando el archivo `custom.rules` en el editor `nanopara` para agregar una regla personalizada para Snort. Donde se está configurando una regla en Snort para que envíe una alerta cuando haya un ping hacia la dirección IP `192.168.0.101`, mostrando el mensaje "HAY UN PING HACIA SU DIRECCION".



```
root@kali: /etc/snort/rules/custom.rules *
GNU nano 8.2
alert icmp any any -> 192.168.0.101 any (msg:'HAY UN PING HACIA SU DIRECCION')
```

Imagen 35 Configuración de regla en Snort para alertar sobre ping hacia la dirección IP `192.168.0.101`

- Se configura Snort para definir la red interna (`HOME_NET`) como `192.168.1.0/24`, el tráfico externo (`EXTERNAL_NET`) como todo lo que no pertenece a `HOME_NET`, y se incluye el archivo `custom.rules` para agregar reglas personalizadas a la configuración de Snort.



```
root@kali: /home/kali
GNU nano 8.2
/etc/snort/snort.conf *
ipvar HOME_NET 192.168.1.0/24
ipvar EXTERNAL_NET !$HOME_NET
include $RULE_PATH/custom.rules
```

Imagen 36 Definición de red interna (`HOME_NET`) y externa (`EXTERNAL_NET`) en archivo de configuración de Snort

- Estas dos líneas de código muestran que se está personalizando la configuración de Snort para adaptarla a sus necesidades específicas. Al editar las reglas y la configuración general, el usuario puede mejorar la capacidad de Snort para detectar y responder a amenazas de seguridad en su red.

nano /etc/snort/rules/custom.rules

nano /etc/snort/snort.conf

```
(root@Kali)-[/home/kali]
# nano /etc/snort/rules/custom.rules

(root@Kali)-[/home/kali]
# nano /etc/snort/snort.conf
```

Imagen 37 Ejecución de Snort en la interfaz de red `eth0` para monitoreo de tráfico en Kali Linux

- La primera línea abre el archivo de configuración de Snort (`/etc/snort/snort.conf`) en el editor **nano**, permitiendo personalizar opciones como las redes a monitorear y los tipos de alertas. La segunda línea ejecuta Snort con esta configuración en la interfaz de red `eth0`, mostrando las alertas en la consola. Esto permite iniciar el monitoreo de red para detectar posibles amenazas según las reglas definidas.

```
(root@Kali)-[/home/kali]
# nano /etc/snort/snort.conf

(root@Kali)-[/home/kali]
# snort -A console -q -c /etc/snort/snort.conf -i eth0
```

Imagen 38 Configuración de prueba de ping desde Kali Linux hacia dispositivo en rojo para detección

3.1. Ping de Kali a Windows

- Principalmente se muestra un entorno de pruebas de seguridad en red. En Kali Linux, se ha configurado Snort para monitorear la interfaz de red **eth0** y detectar actividades sospechosas utilizando reglas definidas en su archivo de configuración. Al mismo tiempo, en Windows, se están ejecutando comandos ping hacia dispositivos específicos en la red (192.168.0.105 y 192.168.1.13) para verificar la conectividad. En conjunto, estas acciones indican que se está evaluando la seguridad de la red, probando la capacidad de Snort para detectar intrusiones y verificando la respuesta de los dispositivos en la red.

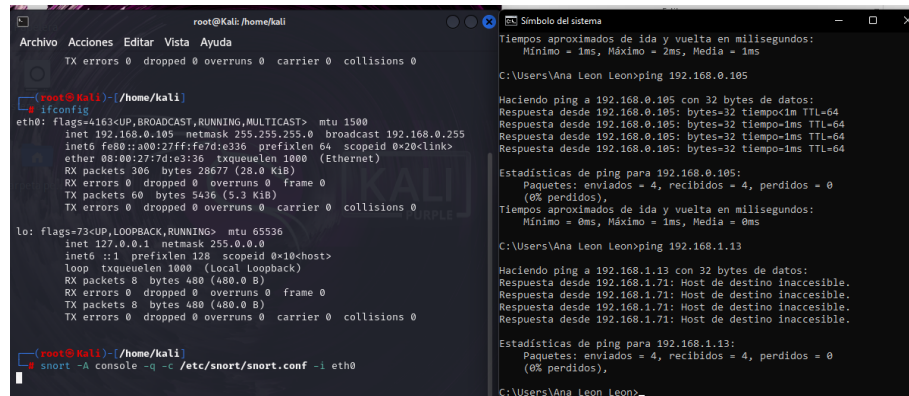


Imagen 39 Detalle de alerta en Snort por actividad ICMP (ping) detectada hacia la dirección 192.168.0.105

- La imagen muestra una ejecución de **Snort**, un sistema de detección de intrusiones (IDS), en una terminal de Linux. Snort está detectando actividad de tipo **ICMP** (Protocolo de mensajes de control de Internet), específicamente **pings** dirigidos hacia la dirección IP del sistema monitorizado. Los mensajes indican que la dirección IP 192.168.1.10 está enviando pings a la IP 192.168.0.105, lo cual Snort clasifica como un "evento ICMP genérico" con prioridad baja.

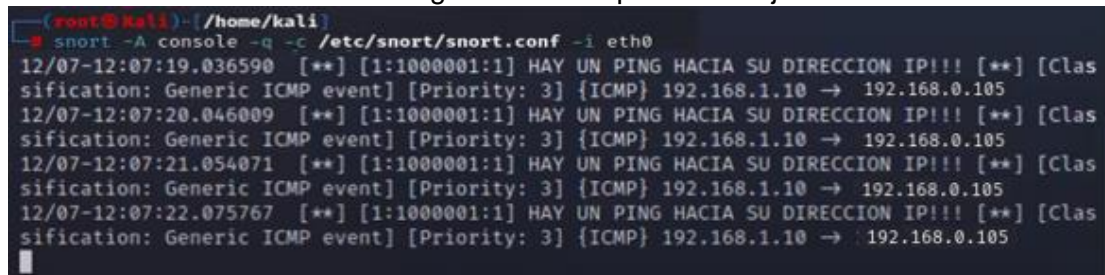


Imagen 40 Personalización de reglas de Snort para monitoreo específico de red

- En este proceso de **evaluación de seguridad de red**. Por un lado, se verifica la conectividad mediante comandos **ping** hacia una IP específica, y, por otro, se utiliza **Snort** en Kali Linux para analizar el tráfico de red en busca de posibles amenazas. Esta combinación de herramientas permite comprobar la comunicación entre dispositivos y monitorear la red para identificar actividades sospechosas, siendo común en pruebas de penetración y configuraciones de sistemas de detección de intrusos.

```
Simbolo del sistema
adaptador de LAN inalámbrica Conexión de área local* 2:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :
adaptador de LAN inalámbrica Wi-Fi:
Sufijo DNS específico para la conexión. . :
Vínculo: dirección IPv6 local. . . : fe80::2c32:d923:e862:b47324
Dirección IPv4. . . . . : 192.168.0.108
Máscara de subred. . . . . : 255.255.255.0
Puerta de enlace predeterminada. . . . : 192.168.0.1

adaptador de Ethernet Conexión de red Bluetooth:
Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . :

.\Users\Ana Leon Leon>ping 192.168.0.105

Estando ping a 192.168.0.105 con 32 bytes de datos:
respuesta desde 192.168.0.105: bytes=32 tiempo=1ms TTL=64
respuesta desde 192.168.0.105: bytes=32 tiempo=1ms TTL=64
respuesta desde 192.168.0.105: bytes=32 tiempo=1ms TTL=64
estadísticas de ping para 192.168.0.105:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 1ms, Máximo = 1ms, Media = 1ms

.\Users\Ana Leon Leon>

kali@kali:~$ ifconfig
TX packets 156 bytes 14446 (14.1 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (local loopback)
RX packets 8 bytes 408 (408.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 408 (408.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

kali@kali:~$ ping 192.168.0.108
PING 192.168.0.108 (192.168.0.108) 56(84) bytes of data:
64 bytes from 192.168.0.108: icmp_seq=1 ttl=128 time=0.749 ms
64 bytes from 192.168.0.108: icmp_seq=2 ttl=128 time=0.507 ms
64 bytes from 192.168.0.108: icmp_seq=3 ttl=128 time=0.770 ms
64 bytes from 192.168.0.108: icmp_seq=4 ttl=128 time=1.47 ms
64 bytes from 192.168.0.108: icmp_seq=5 ttl=128 time=1.11 ms
64 bytes from 192.168.0.108: icmp_seq=6 ttl=128 time=0.603 ms
64 bytes from 192.168.0.108: icmp_seq=7 ttl=128 time=0.747 ms
64 bytes from 192.168.0.108: icmp_seq=8 ttl=128 time=0.797 ms
```

Imagen 41 Configuración final de Snort para iniciar monitoreo de red y detección de intrusiones en Kali Linux

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

🔗 Instalamos principalmente **METASPLOITABLE** para empezar a configurar

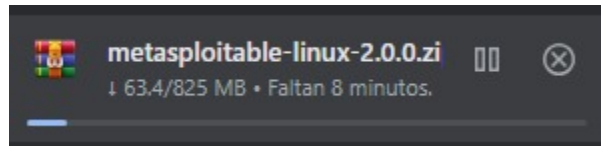


Imagen 42 instalación dell archivo comprimido metasploitable-linux-2.0.0.zipen sistema anfitrión

🔗 Se esta guardando un archivo comprimido (.zip) llamado "metasploitable-linux-2.0.0" en una ubicación específica de la computadora con Windows. Este archivo probablemente contenga recursos o programas relacionados con **Metasploit** , una herramienta utilizada en pruebas de seguridad informática.

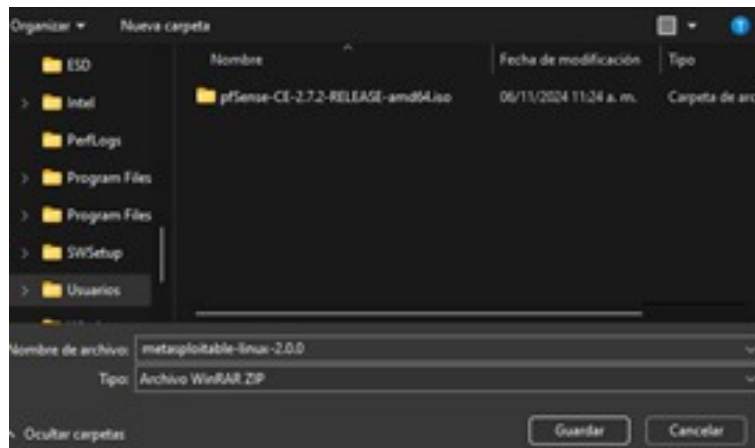


Imagen 43 Configuración inicial

- Se está configurando una máquina virtual para instalar y ejecutar un sistema operativo (como Ubuntu) dentro de la computadora. Se está asignando un nombre a la máquina virtual “**meta**”, seleccionando la ubicación donde se guardarán sus archivos y eligiendo el sistema operativo a instalar. Esta configuración inicial nos permitirá probar sistemas operativos y aplicaciones en un entorno aislado, sin afectar nuestro sistema principal.

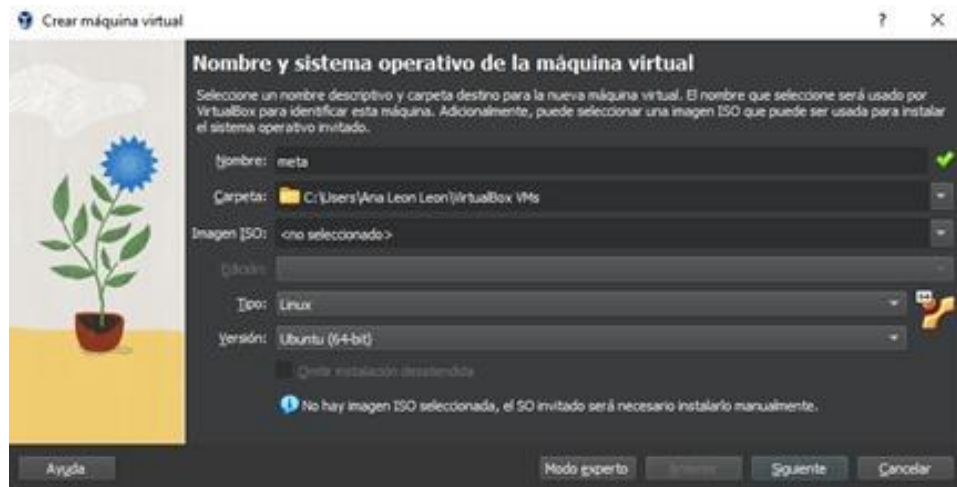


Imagen 44 Configuración inicial de nueva máquina virtual con nombre "Meta" en VirtualBox

- Se estás asignando recursos de hardware a nuestra máquina virtual, como la cantidad de **RAM** y **procesadores**. Esta configuración nos permitirá optimizar el desempeño de la máquina virtual y ajustarla al tipo de tareas que se planea ejecutar en ella.

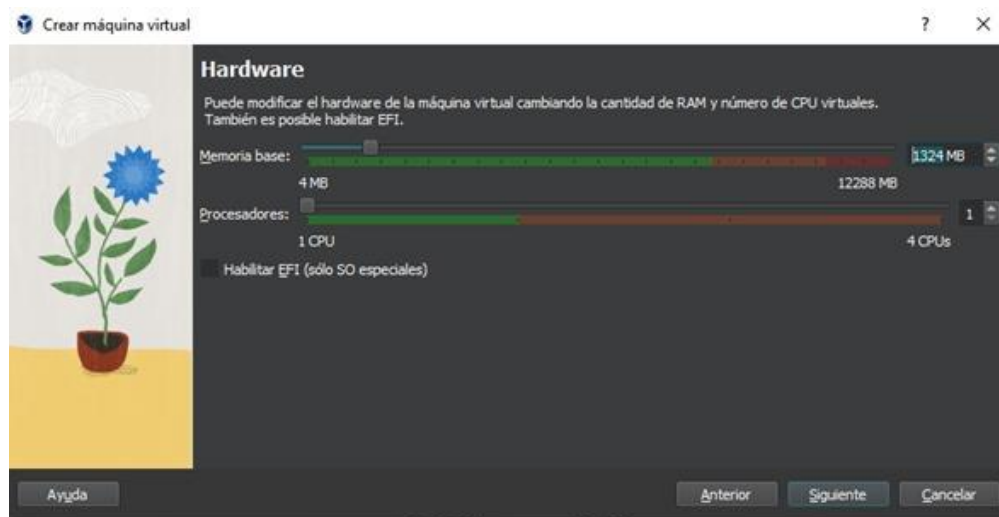


Imagen 45 Asignación de recursos de hardware (RAM y CPU) a la máquina virtual "Meta" en VirtualBox

- Buscando un archivo de configuración de máquina virtual (llamado "**Metasploitable**") en el explorador de archivos de Windows, con el objetivo de cargarlo en un software de virtualización y ejecutarlo como una máquina virtual dentro de nuestra computadora.

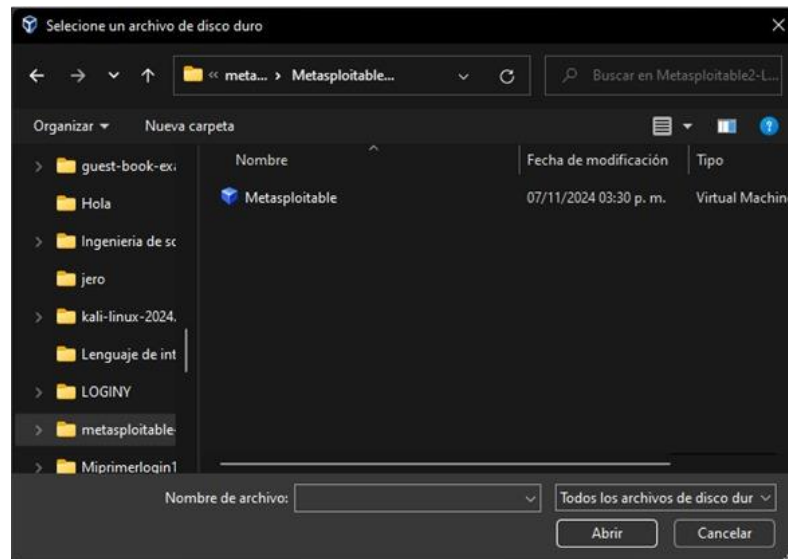


Imagen 46 Selección de archivo de configuración "Metasploitable" en explorador de archivos

- estamos usando **Oracle VM VirtualBox** para ejecutar una máquina virtual llamada **Metasploitable**, diseñada para practicar ciberseguridad y pruebas de penetración en un entorno controlado. Hemos iniciado sesión en el sistema Linux de Metasploitable, que está configurado intencionalmente con vulnerabilidades conocidas. La advertencia nos recuerda no exponer esta máquina virtual a redes no seguras, ya que su propósito es exclusivamente para entrenamiento y pruebas en seguridad informática.

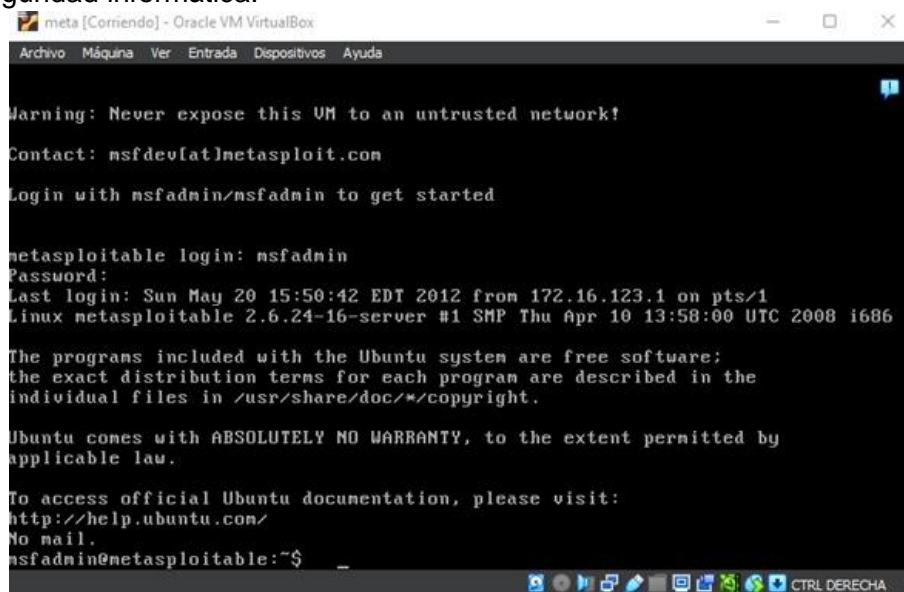
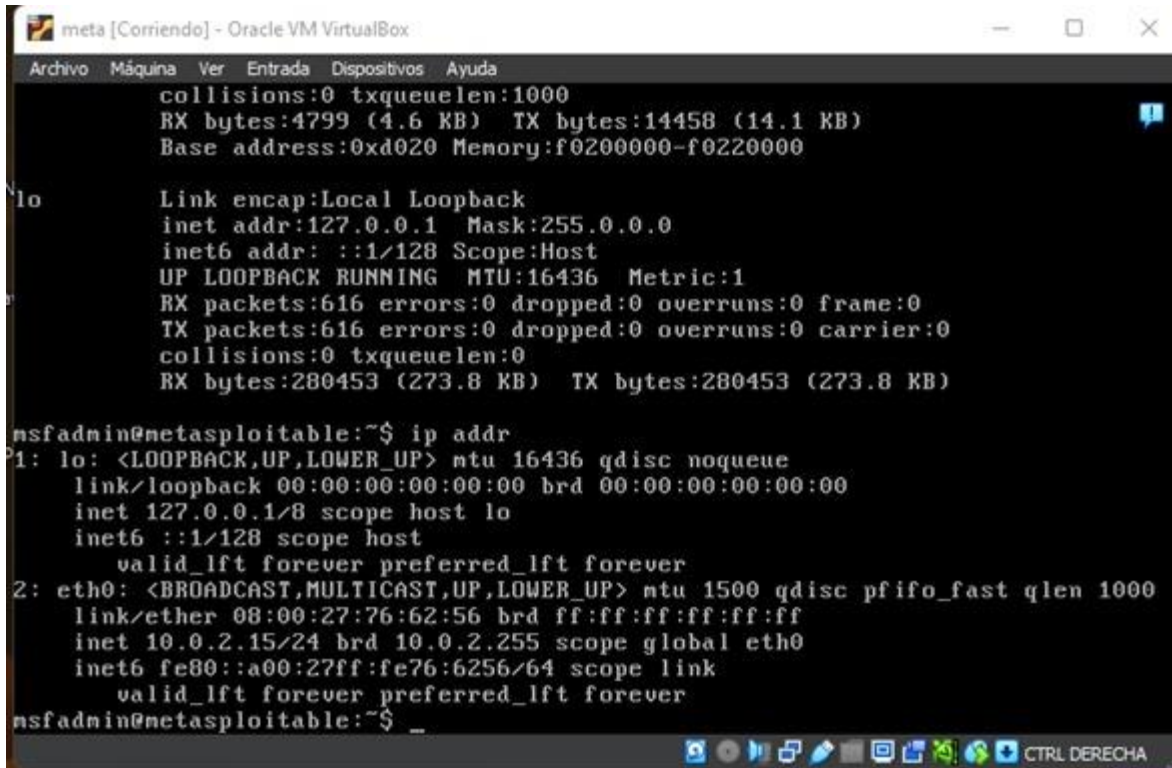


Imagen 47 Inicio de la máquina virtual "Metasploitable" en VirtualBox

Estamos utilizando comandos dentro de la máquina virtual **Metasploitable** en **Oracle VM VirtualBox** para verificar la configuración de red. Hemos ejecutado el comando `ip addr`, que muestra la información de las interfaces de red de la máquina. comprobando que las interfaces de red están activadas y que la máquina tiene una dirección IP en la red local. Esto asegura que la máquina virtual esté lista para pruebas de seguridad y comunicación en la red.



```
meta [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
collisions:0 txqueuelen:1000
RX bytes:4799 (4.6 KB) TX bytes:14458 (14.1 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:616 errors:0 dropped:0 overruns:0 frame:0
TX packets:616 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:280453 (273.8 KB) TX bytes:280453 (273.8 KB)

nsfadmin@metasploitable:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:76:62:56 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global eth0
    inet6 fe80::a00:27ff:fe76:6256/64 scope link
        valid_lft forever preferred_lft forever
nsfadmin@metasploitable:~$ _
```

Imagen 48 Confirmación de conectividad de red en máquina virtual Metasploitable

5. PING SATISFACTORIO ENTRE LAS MÁQUINAS VIRTUALES PFSENSE EN WINDOWS

INSTALACION DE WINDOWS 10 PARA HACER PING

- Esta ventana permite configurar e instalar los parámetros iniciales de una nueva máquina virtual, que será como una computadora dentro de la computadora. Donde le damos el nombre a la máquina virtual para identificarla fácilmente. En este caso, el nombre es "Windows 10". De igual manera el directorio donde será instalado y el archivo ISO que contiene los datos de instalación del sistema operativo Windows 10.

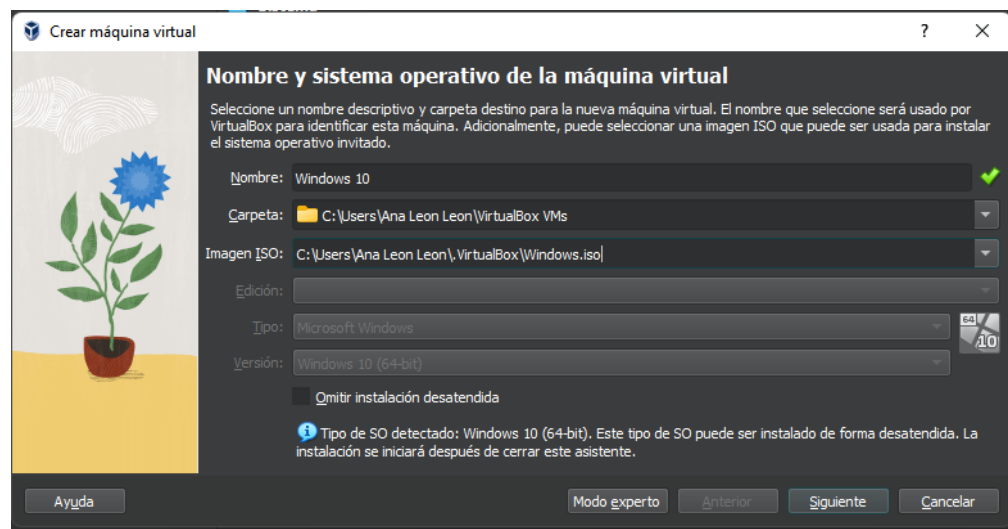


Imagen 49 Proceso de instalación de Windows 10

- En esta ventana, se está personalizando la instalación de Windows 10 dentro de la máquina virtual. Al proporcionar esta información, se está automatizando gran parte del proceso de instalación y configurando el sistema operativo según tus preferencias. Se configura el SO invitado

Nombre: Leon

Contraseña Analeon

La clave del producto , el nombre de la maquina “Windws 10” y el nombre de dominio

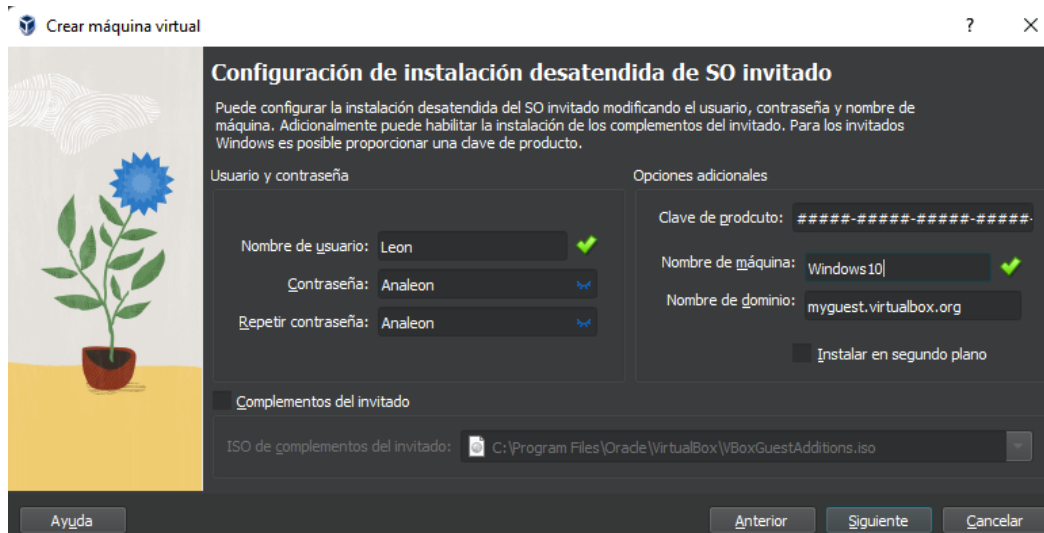


Imagen 50 Proceso de arranque inicial de Windows 10

- En esta etapa, se está definiendo la potencia de la máquina virtual asignando una cantidad específica de RAM y procesadores. Una vez que se complete la configuración, podremos continuar con los pasos finales de la creación de la máquina virtual.

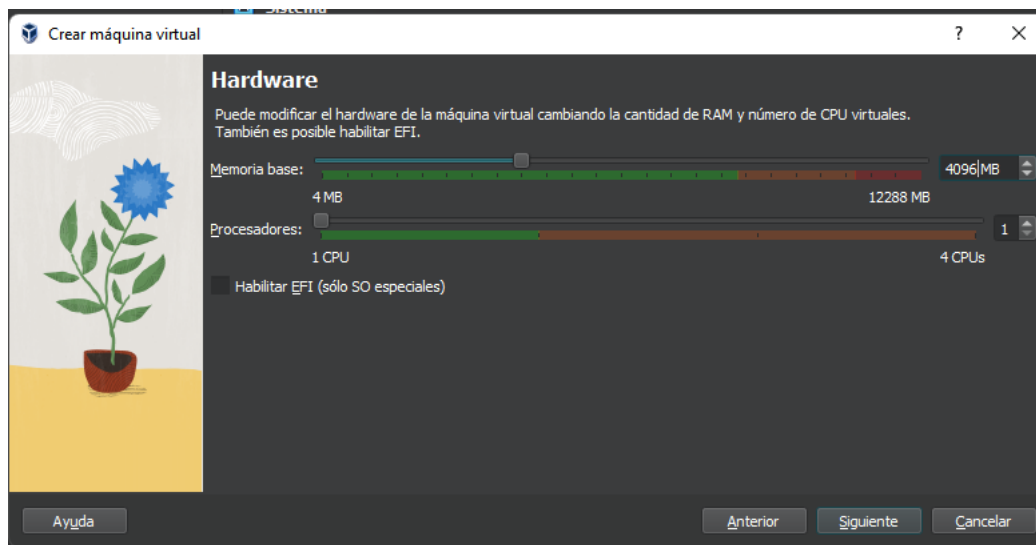


Imagen 51 Asignación de recursos de hardware

- La máquina virtual está en pleno proceso de instalación de Windows 10.

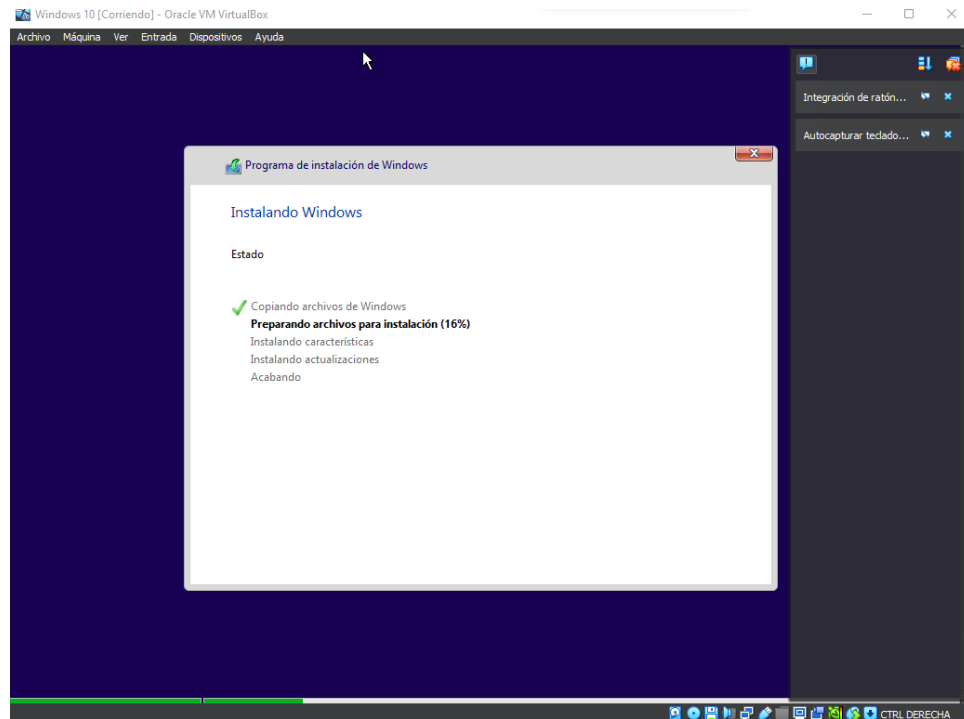


Imagen 52 proceso de instalacion de windows 10

- En este momento, la instalación se encuentra en la etapa final, "**Acabando**". Se están instalando las actualizaciones más recientes para asegurar que el sistema esté actualizado.

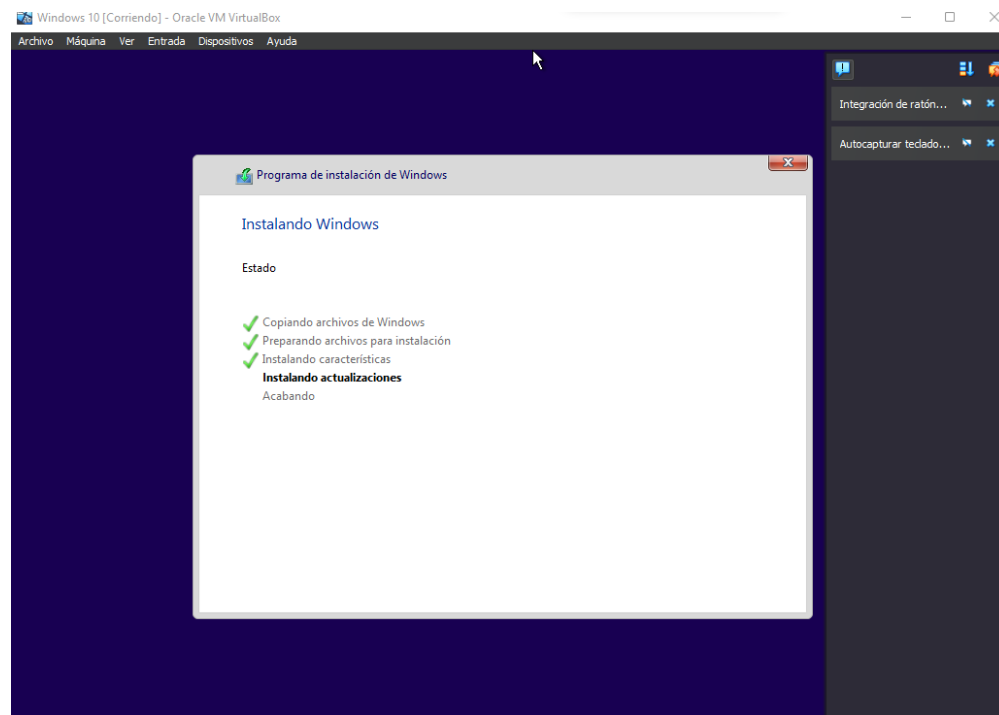


Imagen 53 terminación de la instalación

- La máquina virtual se encuentra en el proceso de arranque inicial. Una vez que se complete esta etapa, podremos acceder al escritorio de Windows 10 y comenzar a utilizar la máquina virtual.

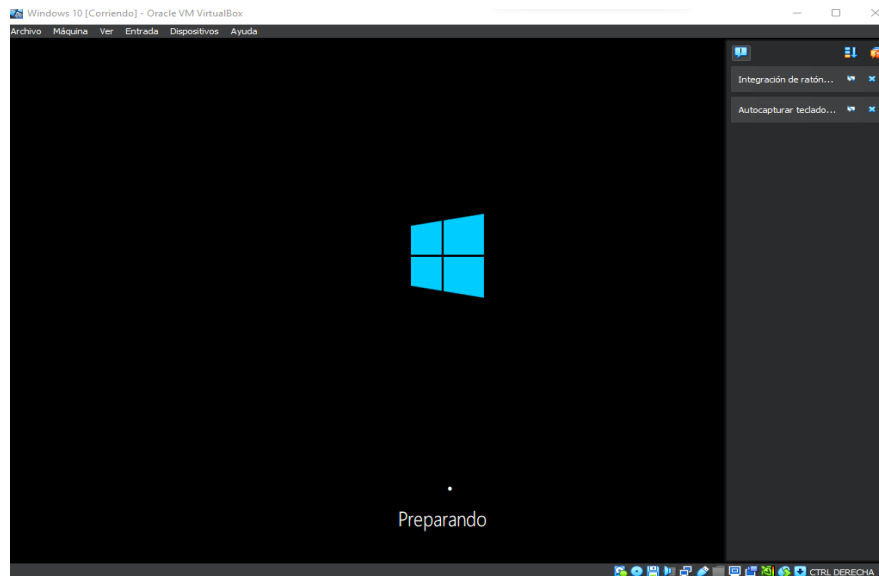


Imagen 54 Proceso de arranque inicial de Windows 10

🌈 la máquina virtual está completamente funcional

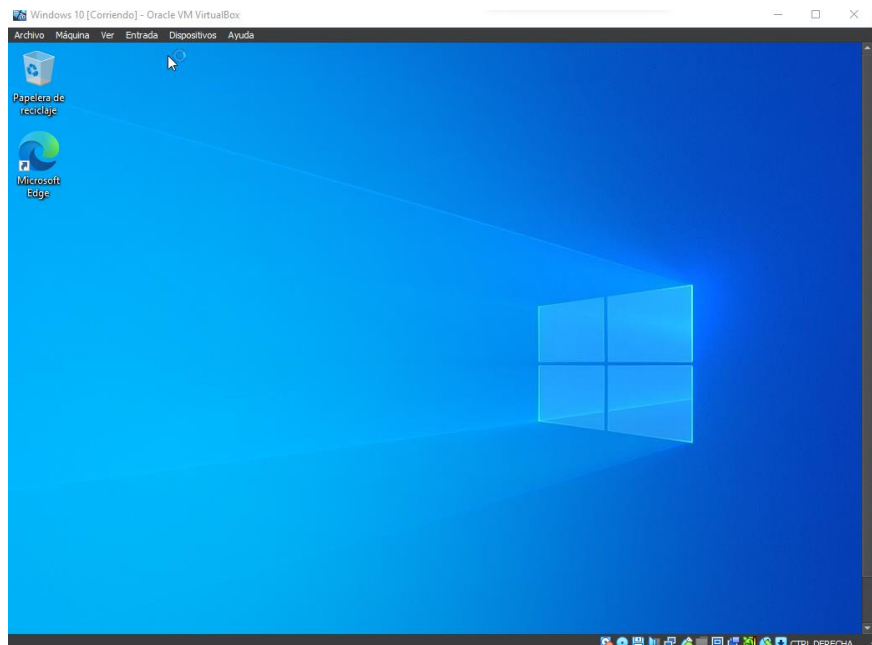


Imagen 55 Confirmación de finalización de instalación de Windows 10

- **DESARROLLO DEL PING**
- Se muestra la configuración de la red de una máquina virtual en VirtualBox. En la pestaña **Roja** de la ventana de configuración, se ha seleccionado el **Adaptador 1** y se ha configurado para estar "Conectado a: Adaptador solo anfitrión". Esto permite que la máquina virtual se comuniqué únicamente con el sistema anfitrión (es decir, la computadora física donde está instalada VirtualBox), sin acceso directo a Internet u otras redes externas.

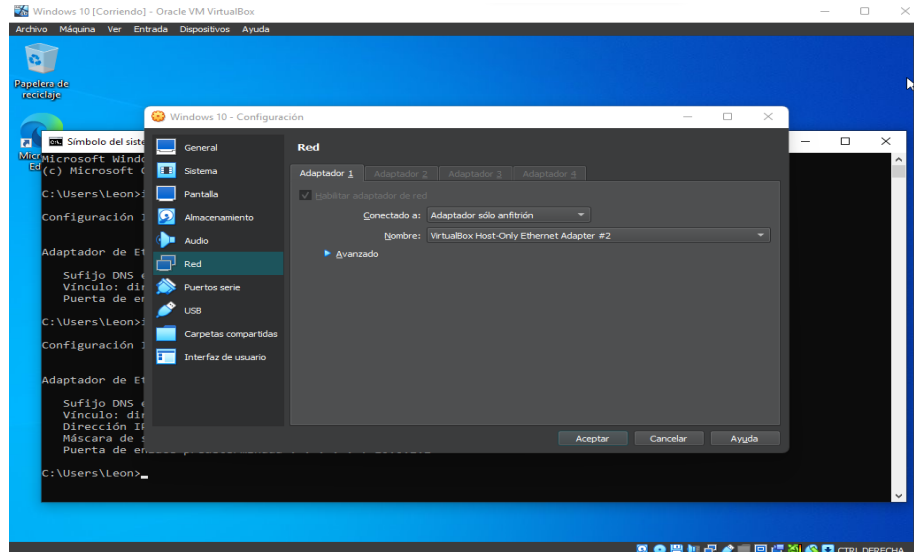


Imagen 56 proceso del ping de windows

- Se está utilizando el símbolo del sistema en una máquina virtual con Windows 10 para liberar y renovar la configuración de la dirección IP.
 1. Se ejecuta el comando `ipconfig /release` para liberar la dirección IP actual.
 2. Luego, se utiliza `ipconfig /renew` para solicitar una nueva dirección IP al servidor DHCP.

Esto es útil para obtener una nueva configuración de red sin necesidad de reiniciar la máquina virtual.

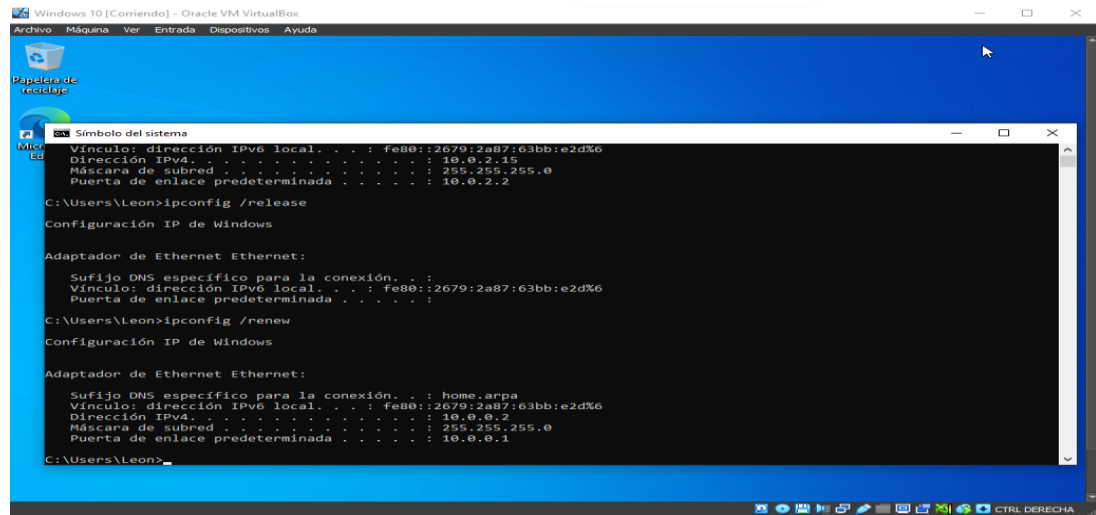
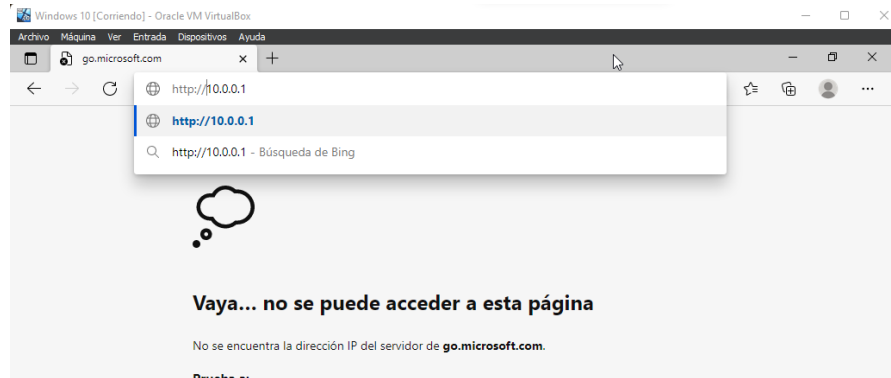


Imagen 57 sistema en una máquina virtual con Windows 10

- Se observa que en una máquina virtual con Windows 10 se está intentando acceder a la dirección IP 10.0.0.1 a través de un navegador web. Sin embargo, el navegador muestra un mensaje de error indicando que no se puede acceder a la página, lo que sugiere que no hay respuesta desde esa dirección IP en la red actual de la máquina virtual.



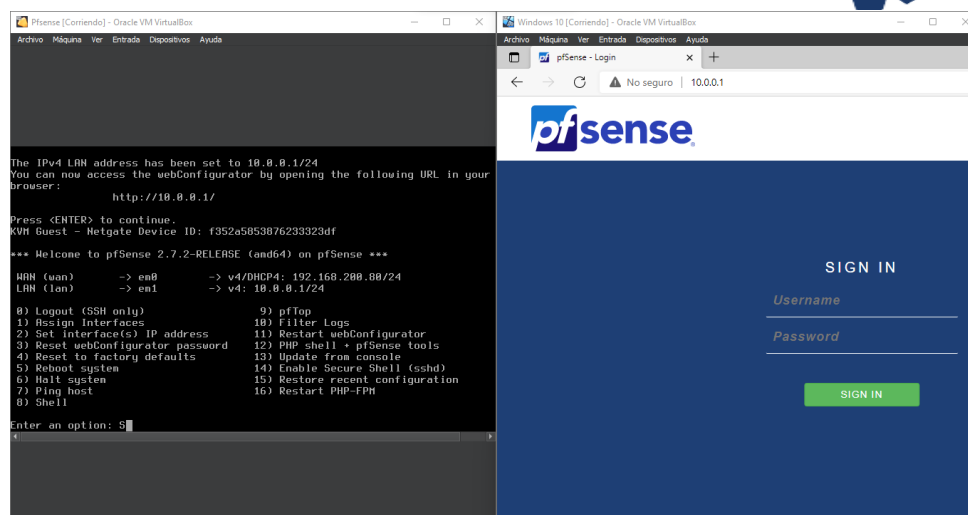


Imagen 58 ping realizado exitosa mente

CONCLUSIÓN

El desarrollo de este entorno de virtualización ha permitido crear un laboratorio de ciberseguridad seguro y funcional, donde se pueden implementar y probar diversos ajustes de red y herramientas de detección de intrusos. La instalación de máquinas virtuales como pfSense y Kali Linux, junto con la configuración detallada de adaptadores y redes virtuales en VirtualBox, permite analizar el tráfico y verificar la respuesta de sistemas de firewall e IDS. Estas prácticas son fundamentales para reforzar las habilidades en ciberseguridad y comprender las configuraciones necesarias para crear entornos seguros y bien administrados. La metodología documentada en este informe proporciona un enfoque integral para el aprendizaje y la aplicación de técnicas de seguridad en redes virtuales.