



TECNOLÓGICO NACIONAL DE MÉXICO
INSTITUTO TECNOLÓGICO DE TLAXIACO

INGENIERÍA EN SISTEMAS COMPUTACIONALES.
SEGURIDAD Y VIRTUALIZACIÓN.

PRACTICA 6: CREACIÓN DE UN LABORATORIO DE SEGURIDAD P1.

INTEGRANTES DEL EQUIPO:

JEANETTE ARLET SALAZAR NICOLÁS	21620202
NELSY ORTIZ LÓPEZ	21620165
MARIBEL LUCERO ZUÑIGA	21620139

SEMESTRE: SÉPTIMO. GRUPO: 7 US

ASESOR: ING. EDWARD OSORIO SALINAS.

TLAXIACO, OAXACA A 28 DE OCTUBRE DEL 2024.

CONTENIDO

INTRODUCCIÓN:	5
1. INSTALACIÓN DE VIRTUAL BOX.....	5
2. INSTALAR OPNSENSE O PFSENSE EN UNA MÁQUINA VIRTUAL Y CONFIGURAR UN FIREWALL.	8
3. INSTALAR KALI LINUX EN UNA MÁQUINA VIRTUAL Y CONFIGURAR UN SISTEMA DE DETECCIÓN DE INTRUSOS.....	18
CONFIGURACIÓN DE UN SISTEMA DE DETECCIÓN DE INTRUSOS EN KALI LINUX.....	22
CREACION Y VERIFICACIÓN DE ARCHIVO DE REGLAS	25
4. CREAR UNA MÁQUINA VIRTUAL VULNERABLE POR DISEÑO COMO METASPLOITABLE2.	27
5. PING SATISFACTORIO ENTRE LAS MÁQUINAS VIRTUALES.....	30
PING ENTRE WINDOWS Y PFSENSE	30
PING ENTRE WINDOWS Y KALI LINUX.....	31
6. CONCLUSIÓN	31
7. BIBLIOGRAFÍA	32

TABLA DE ILUSTRACIONES.

Ilustración 1: Página oficial para descargar Visual Box	5
Ilustración 2: Pantalla de bienvenida de Oracle VM Virtual Box	6
Ilustración 3: Configuración personalizada.....	6
Ilustración 4: Seleccionar las funciones de instalación.....	7
Ilustración 5: Finalizar con la instalación de Oracle Virtual Box.....	7
Ilustración 6 Página oficial para descargar Opnsense.....	8
Ilustración 7 Descarga de Opnsense	8
Ilustración 8 Administrador de red.....	9
Ilustración 9 Creación de redes.	9
Ilustración 10 Creación de una máquina virtual.....	9
Ilustración 11 Asignación de atributos para nuestra máquina virtual.....	10
Ilustración 12 Incorporación de tarjetas de red WAN	11
Ilustración 13 Interfaz de Red para el adaptador 2.....	11
Ilustración 14 Aceptar los derechos de autor	12
Ilustración 15 Bienvenida de pfsense.....	12
Ilustración 16 Configuración de pfsense en proceso.....	13
Ilustración 17 Selección de Interfaz WAN	13
Ilustración 18 Configuración del modo de red de pfsense	14
Ilustración 19 Confirmación de instalación	14
Ilustración 20 Pfsense instalado correctamente	15
Ilustración 21 Establecer las direcciones Ip de las interfaces.....	15
Ilustración 22 Configuración de nuestra LAN	16
Ilustración 23 Activación del servidor DHCP	16
Ilustración 24 Pfsense configurado correctamente.....	17
Ilustración 25 Página oficial para descargar Kali Linux	18
Ilustración 26 Elección de Máquina a utilizar	18
Ilustración 27 Descarga de Kali Linux en Proceso	19
Ilustración 28 Kali Linux montado directamente	19
Ilustración 29 Revisión de usuario y contraseña de Kali Linux	20
Ilustración 30 Asignación de atributos para nuestra máquina virtual de Kali Linux.....	20
Ilustración 31 Inicio de Sesión en Kali Linux	21
Ilustración 32 Interfaz de Kali Linux	21
Ilustración 33 Actualización y preparación de Kali Linux	22

Ilustración 34 Herramientas adicionales en Kali Linux	22
Ilustración 35 Instalación del sistema de detección de intrusos Snort	23
Ilustración 36 Configuración de Snort	23
Ilustración 37 Verificación de red en Snort.....	24
Ilustración 38 Edición del archivo de configuración	24
Ilustración 39 Creación y verificación de las reglas del archivo	25
Ilustración 40 Asignación de la regla de detección de intrusos	25
Ilustración 41 Definición de la subred que deseamos proteger	26
Ilustración 42 Ejecución de Snort en modo IDS	26
Ilustración 43 Página oficial para descargar Metasploitable2	27
Ilustración 44 Descarga en proceso.....	27
Ilustración 45 Asignación de atributos para nuestra máquina virtual.....	28
Ilustración 46 Instalación de Metasploitable2 instalado correctamente	28
Ilustración 47 Inicio de sesión	29
Ilustración 48 Configuración y asignación de la IP statica.....	29
Ilustración 49 Ping entre Pfsense y Windows	30

INTRODUCCIÓN:

En esta presente práctica realizaremos la instalación de distintas máquinas virtuales como firewalls ya que esto puede ser útil para una variedad de propósitos, como probar la detección de intrusos permitiendo la identificación y análisis de posibles amenazas, así como también aprender a poner en práctica habilidades un entorno seguro y controlado gestionando el tráfico de redes y finalmente se incluirá una máquina virtual vulnerable con la ayuda de MetaSploitable2.

Este laboratorio permitirá la interacción y la comunicación entre las máquinas virtuales con un ping satisfactorio, estableciendo un entorno perfecto para pruebas de seguridad, monitoreo y análisis de tráfico de red.

1. INSTALACIÓN DE VIRTUAL BOX.

Descarga el instalador: https://www.virtualbox.org/wiki/Download_Old_Builds_6_1 (ORACLE, 2024)

Ir al sitio web oficial de VirtualBox y navegar a la sección de descargas. En la página buscar "VirtualBox 6.1" y descargar el instalador adecuado para tu sistema operativo Windows.

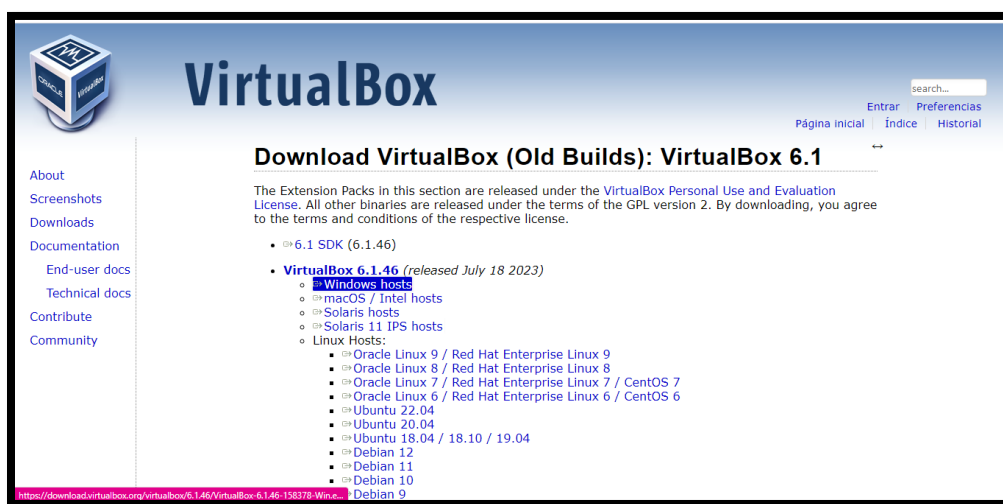


Ilustración 1: Página oficial para descargar Visual Box.

Ejecuta el instalador: Una vez que se complete la descarga, ejecuta el archivo de instalación que acabas de descargar. El nombre del archivo podría ser algo como "VirtualBox-6.1.x-Installer.exe".

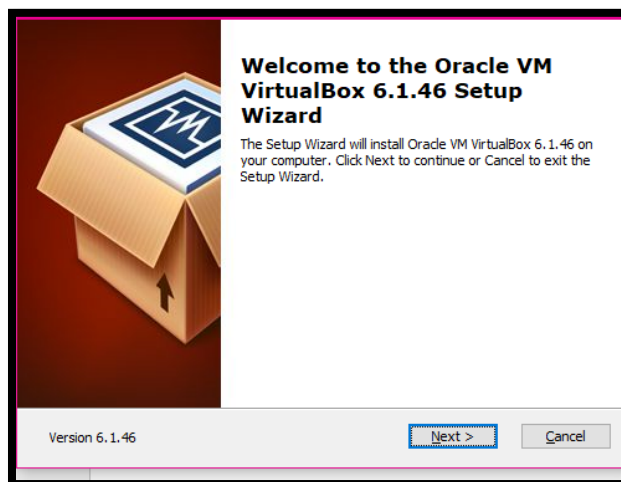


Ilustración 2: Pantalla de bienvenida de Oracle VM Virtual Box

Seguir las instrucciones del asistente de instalación. Aceptar los términos de licencia y elegir las opciones de instalación. En este caso se dejaron las opciones predeterminadas.

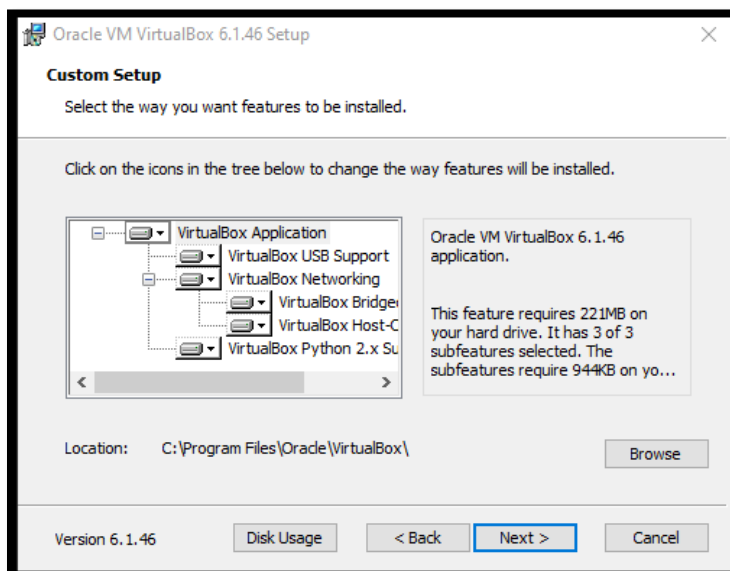


Ilustración 3: Configuración personalizada.

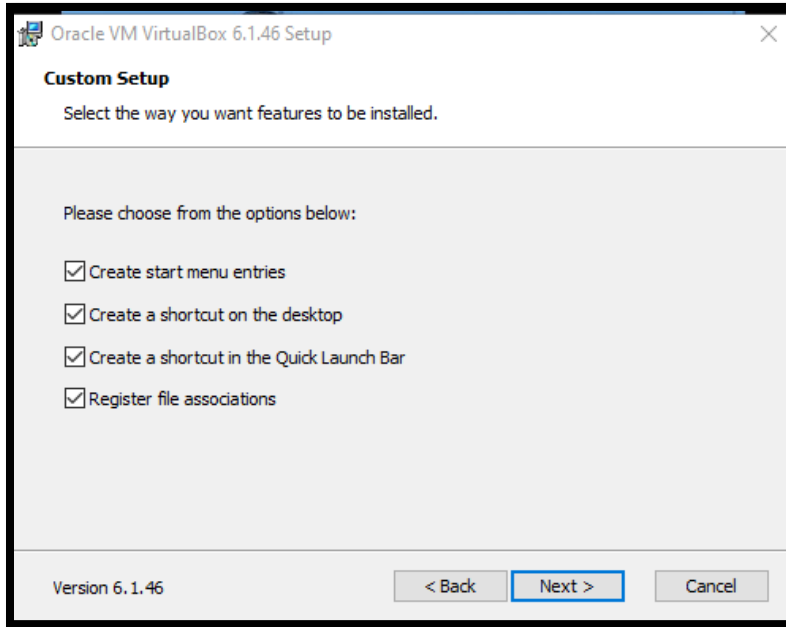


Ilustración 4: Seleccionar las funciones de instalación.

Finalizar la instalación: Después de completar la instalación, VirtualBox estará listo para usar.

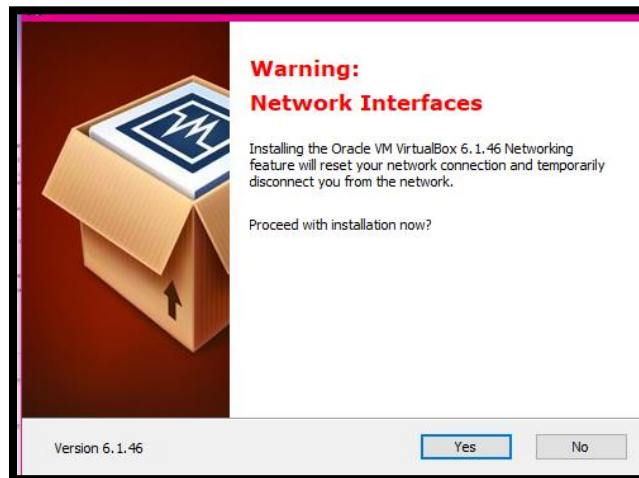


Ilustración 5: Finalizar con la instalación de Oracle Virtual Box.

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

Descarga el instalador: <https://opnsense.org/download/> (OPNsense, s.f.)

Ir al sitio web oficial de opnsense y seleccionar la arquitectura para su posterior descarga.

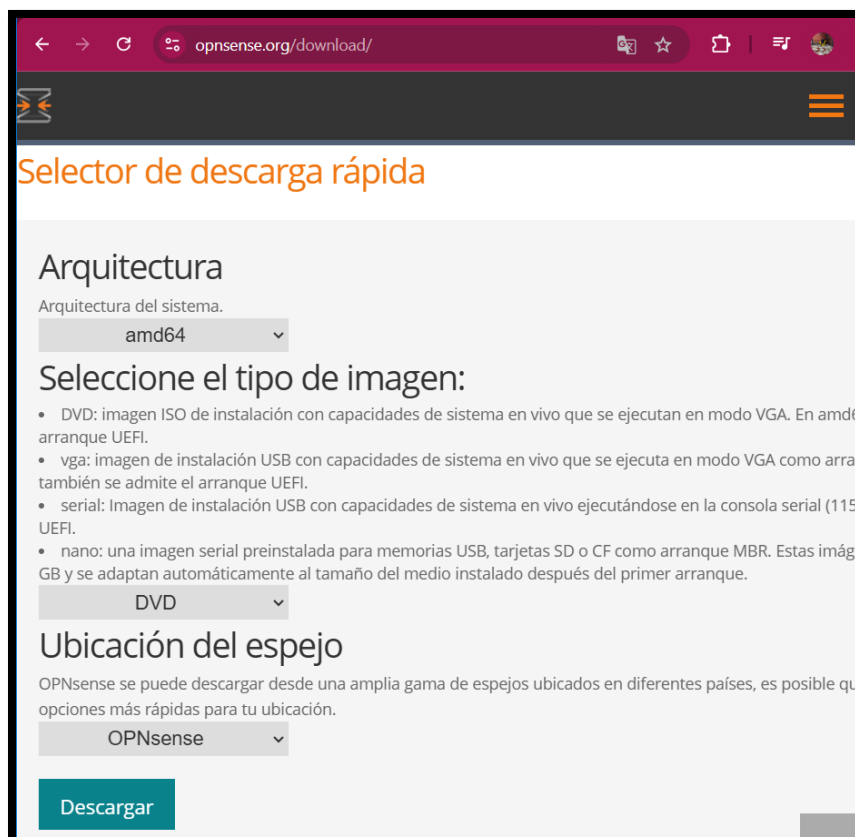


Ilustración 6 Página oficial para descargar Opnsense

En seguida comenzara a descargarse y solo quedaría esperar a que finalice.

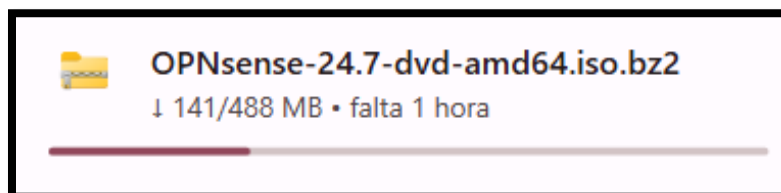


Ilustración 7 Descarga de Opnsense

Posteriormente creamos nuestras redes para ello primeramente nos dirigimos al apartado de “Archivo”, “Herramientas” y “Administrador de red”.

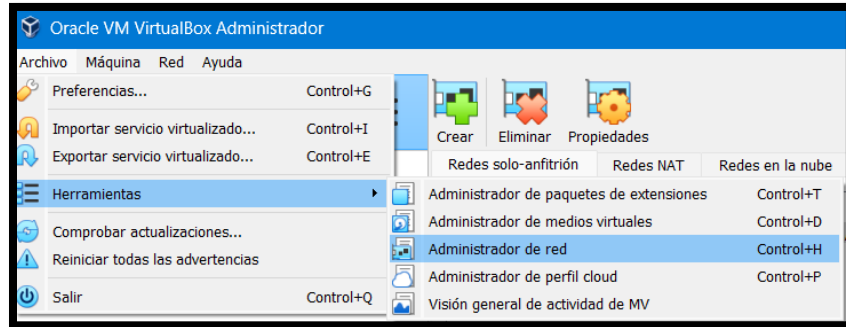


Ilustración 8 Administrador de red

Para crear nuestras redes nos redirigimos en el apartado de “Redes solo-anfitrión”, una vez estando ahí le damos clic en crear en total creamos dos redes.

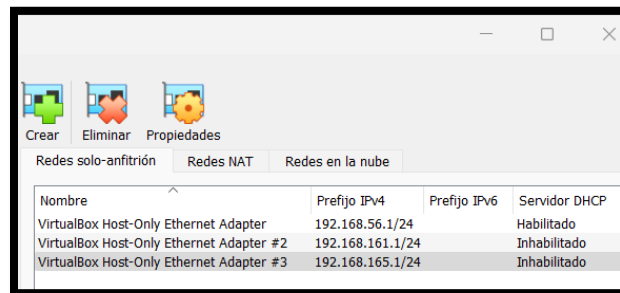


Ilustración 9 Creación de redes.

Creo una nueva máquina virtual: Abre VirtualBox y haz clic en "Nueva" para crear una nueva máquina virtual, ingresa un nombre para tu máquina virtual en este caso le asignamos ("Pfsense"). Selecciona el tipo de sistema operativo como "Other" y la versión como "Other/Unknown (64-bit)".

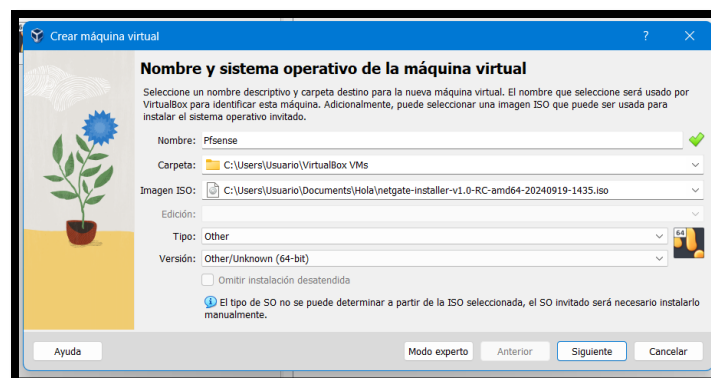


Ilustración 10 Creación de una máquina virtual

Asignar la cantidad de memoria RAM que deseas dedicar a tu máquina virtual. En nuestro caso le asignamos 512 MB, de procesadores 1 y en tanto al tamaño de disco duro 8GB.

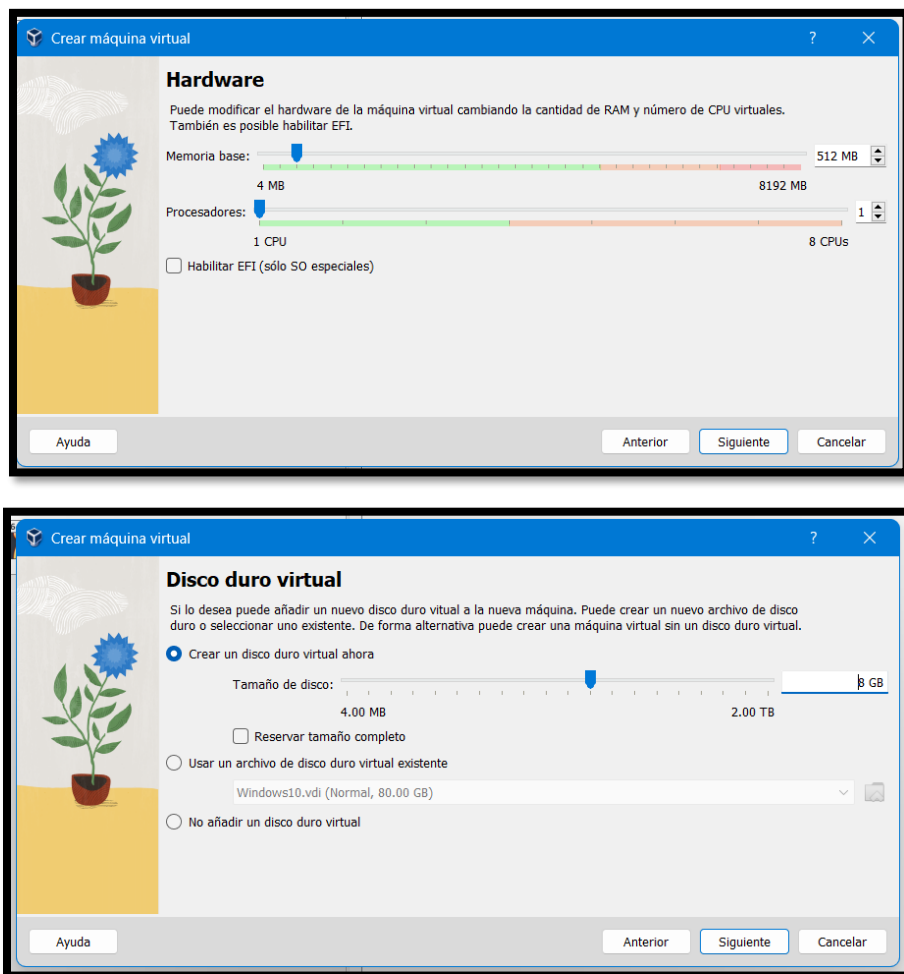


Ilustración 11 Asignación de atributos para nuestra máquina virtual

Incorporación de tarjetas de red: para ello en el primer adaptador lo configuramos que sea “Adaptador Puente” y en nombre que sea la tarjeta integrada, esto para que sea nuestra red WAN.

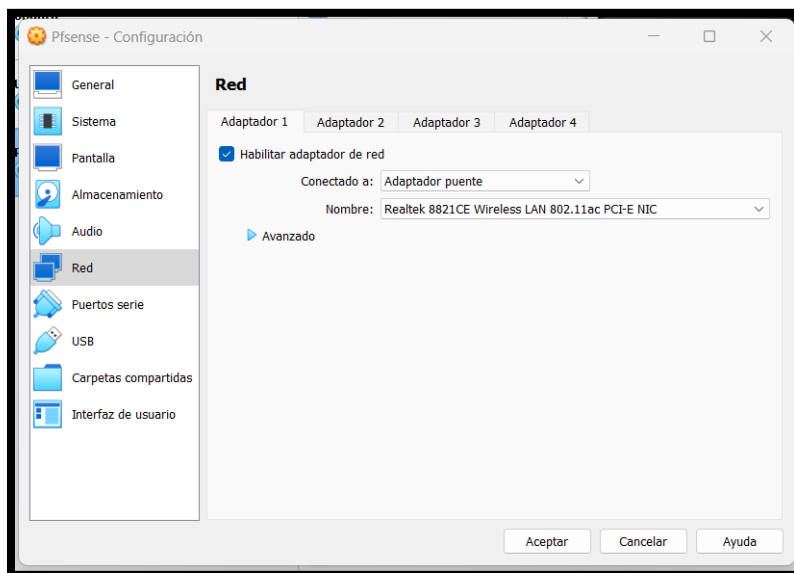


Ilustración 12 Incorporación de tarjetas de red WAN

Para el adaptador 2 primeramente lo habilitamos y en seguida en el apartado de conectado seleccionamos “Host-only Adapter” y en nombre ahora utilizaremos el dos.

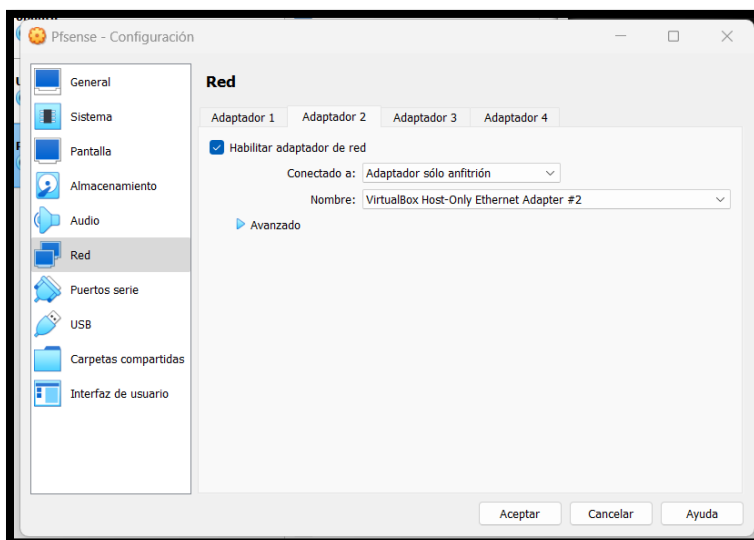


Ilustración 13 Interfaz de Red para el adaptador 2

Arranque del sistema: una vez que se haya configurado correctamente procedemos a iniciar la máquina y la primera ventana emergente que nos parece es solo para aceptar los derechos de autor.

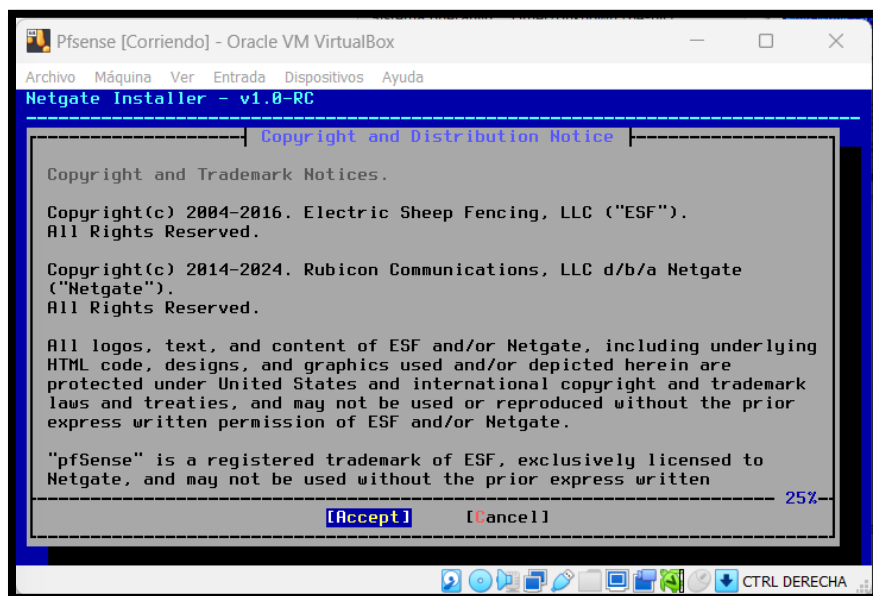


Ilustración 14 Aceptar los derechos de autor

En seguida le damos clic en ok ya que solo te da la bienvenida para la instalación respectiva

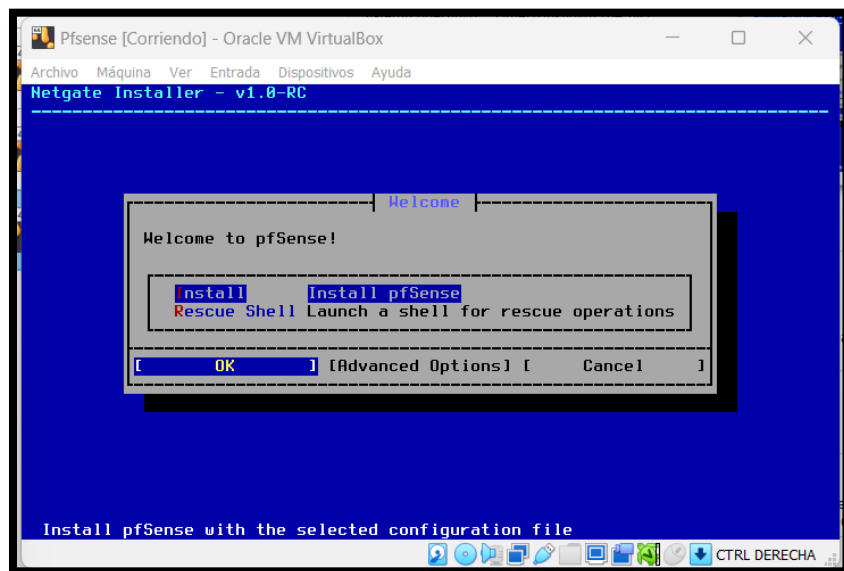


Ilustración 15 Bienvenida de pfsense

Le damos clic en aceptar para su posterior configuración

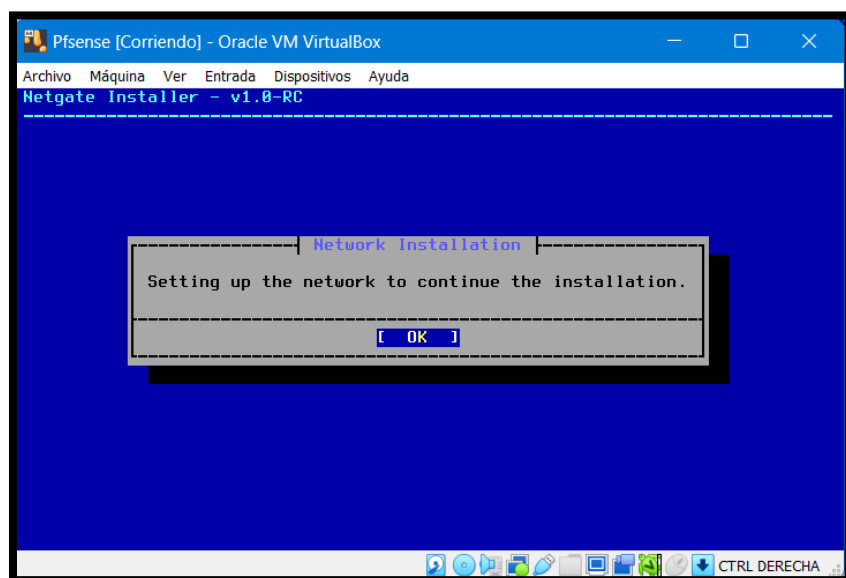


Ilustración 16 Configuración de pfsense en proceso

Para la selección de la interfaz WAN lo dejamos por default y le damos clic en “OK”.

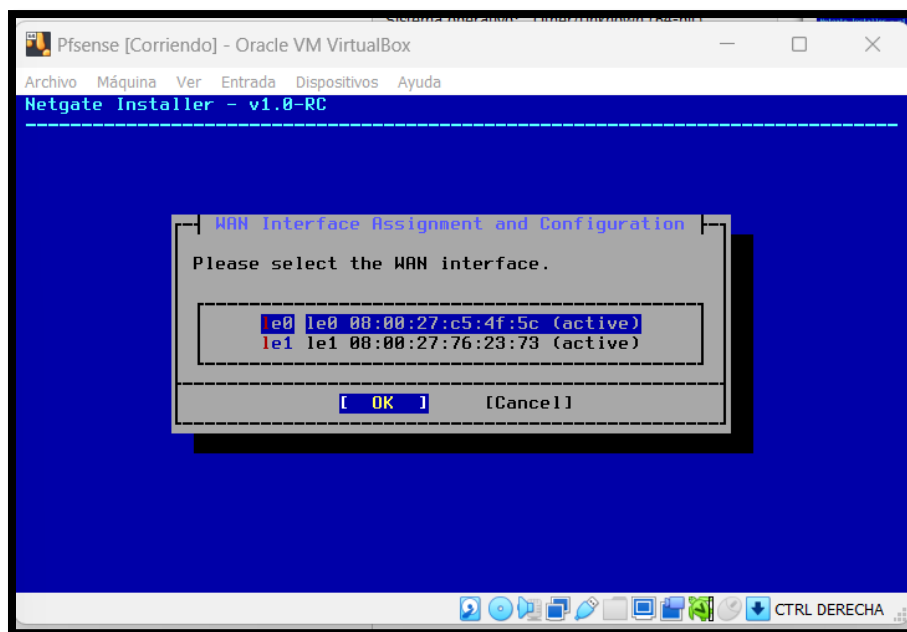


Ilustración 17 Selección de Interfaz WAN

En seguida le damos clic en “OK” dejando la configuración recomendada.

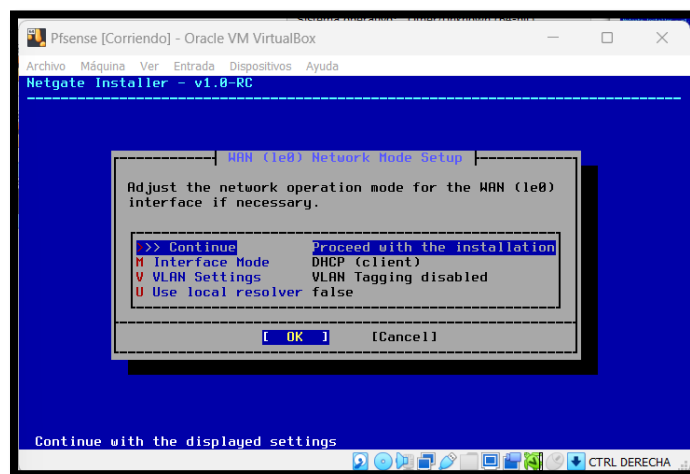


Ilustración 18 Configuración del modo de red de pfsense

Finalmente, solo queda aceptar la confirmación para su posterior instalación dando clic en “YES”.

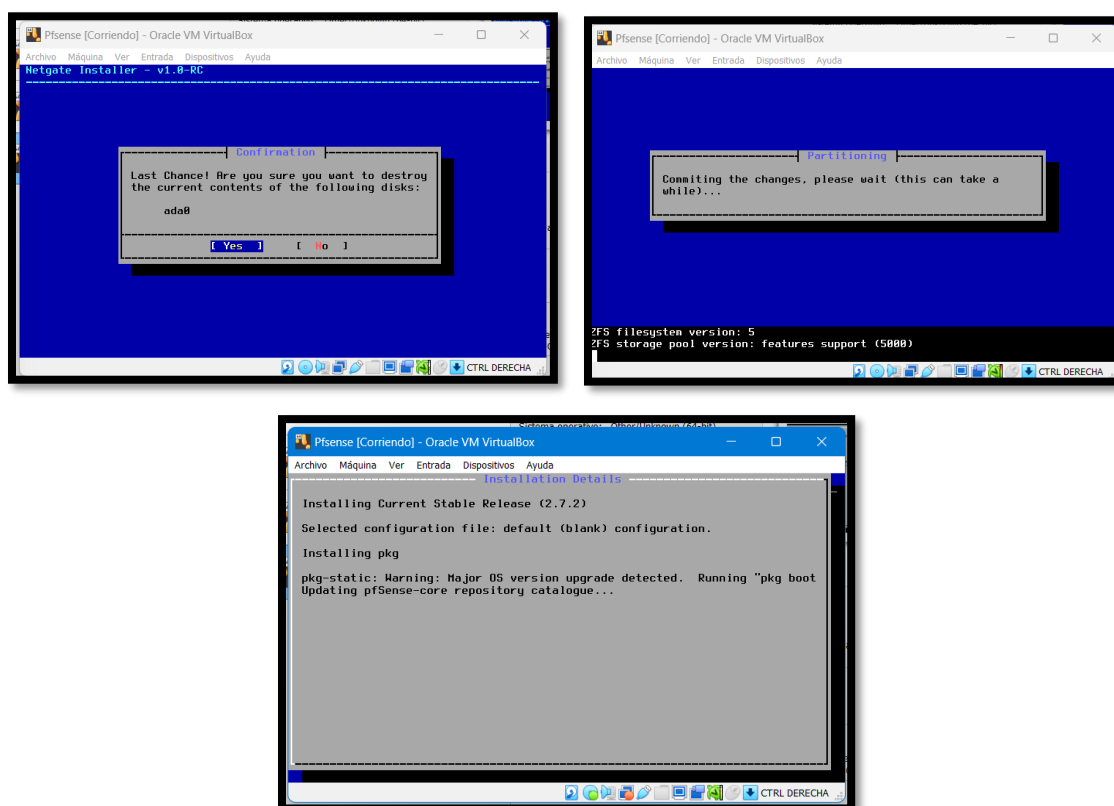


Ilustración 19 Confirmación de instalación

Finalmente pfsense quedara instalado, en seguida solo queda reiniciar la máquina, para ello le damos clic en “Reboot”.

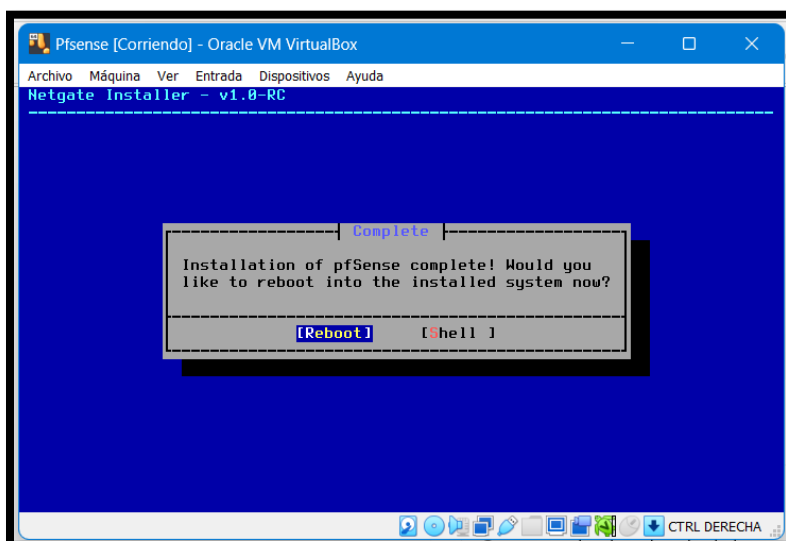


Ilustración 20 Pfsense instalado correctamente

Configuración de pfsense: para ello tecleamos el numero dos donde podremos establecer nuestras direcciones IP en nuestras interfaces

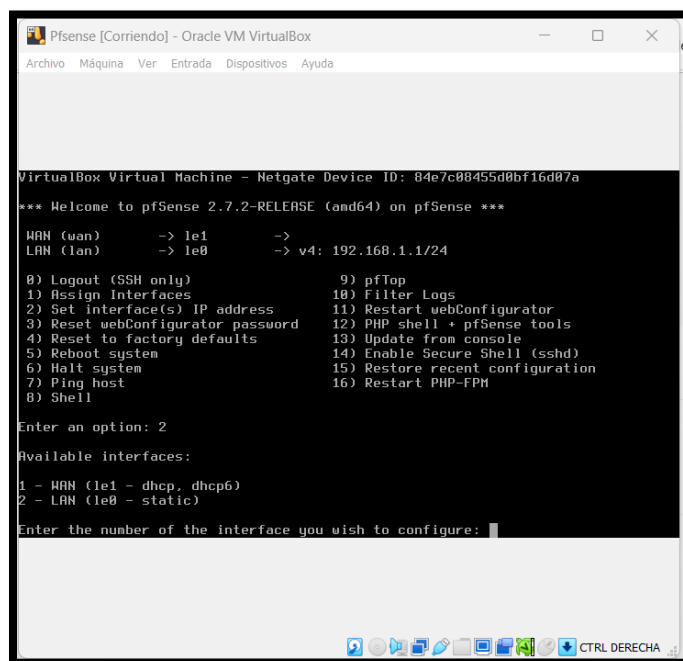
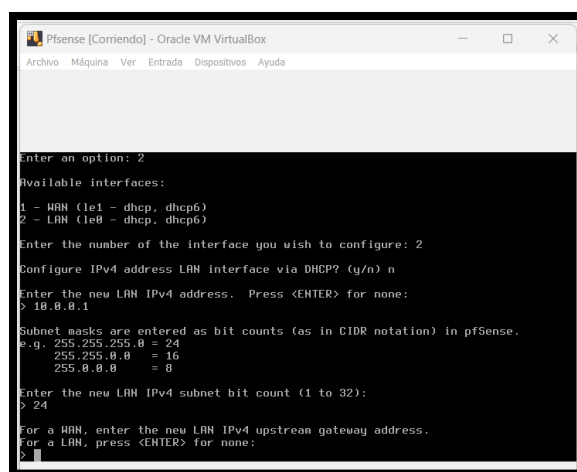


Ilustración 21 Establecer las direcciones Ip de las interfaces

En seguida procedemos a configurar la LAN en este caso es la opción 2, nos pregunta si deseamos configurarla por medio del DHCP le pones “n” ya que no queremos configurarla por ese medio, después nosotros le asignamos el rango de ip “10.0.0.1” y nuestra mascara de red es “24”.

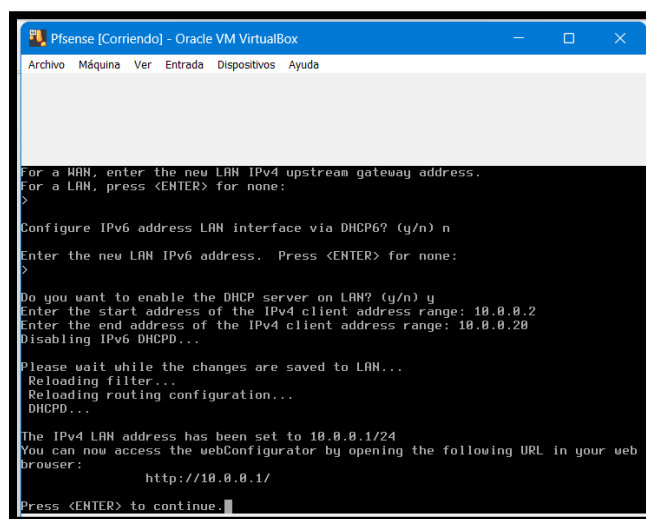


```
PfSense [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

Enter an option: 2
Available interfaces:
1 - WAN (le1 - dhcp, dhcp6)
2 - LAN (le0 - 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
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

Ilustración 22 Configuración de nuestra LAN

Luego nos pide nuestro Gateway, pero en nuestro caso no lo asignamos ya que nuestro Gateway seria nuestra WAN así como tampoco trabajaremos con IPv6, nos pregunta se deseamos habilitar el servidor DHCP hasta entonces tecleamos la letra “y”.



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

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

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.
```

Ilustración 23 Activación del servidor DHCP

Finalmente, nuestro firewall estará configurado para poder utilizarlo.

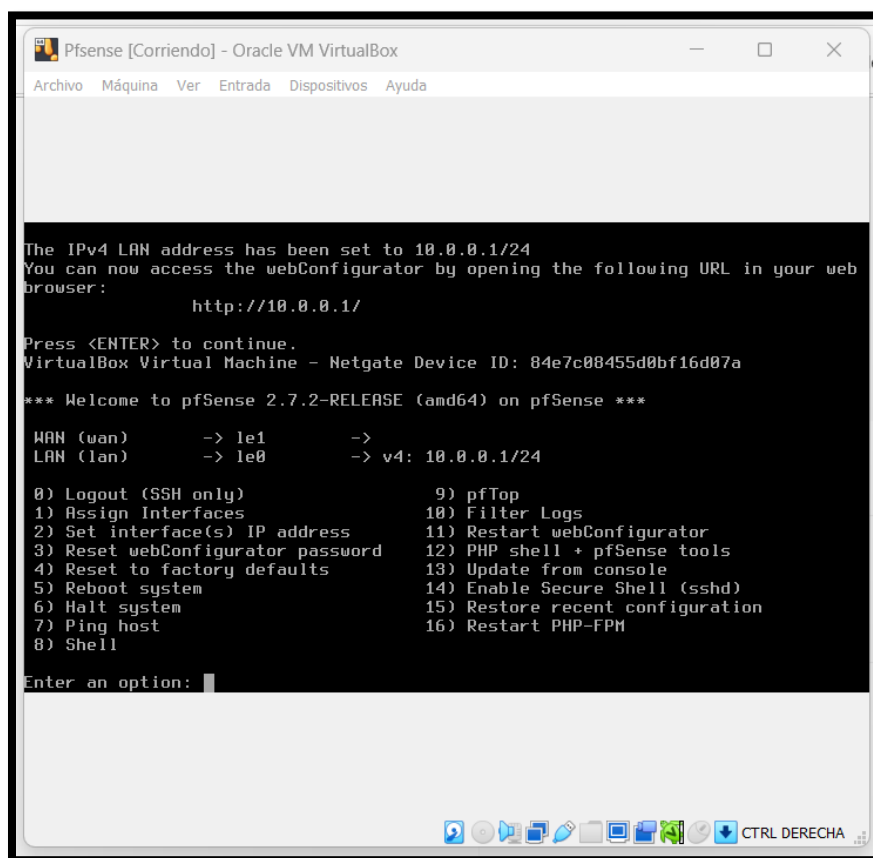


Ilustración 24 Pfsense configurado correctamente

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

Descarga el instalador: <https://www.kali.org/get-kali/#kali-platforms> (Kali, s.f.)

Ir al sitio web oficial de Kali Linux y seleccionar la imagen para máquinas virtuales para su posterior descarga.

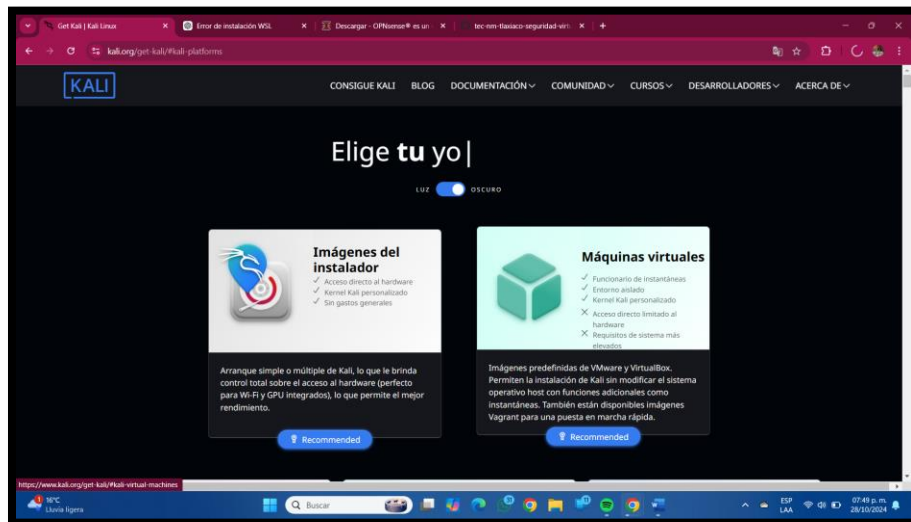


Ilustración 25 Página oficial para descargar Kali Linux

En seguida seleccionamos en qué tipo de máquina lo deseamos instalar y los bits dependiendo a nuestro equipo de cómputo en nuestro caso sería “VirtualBox” de “64 Bits”.

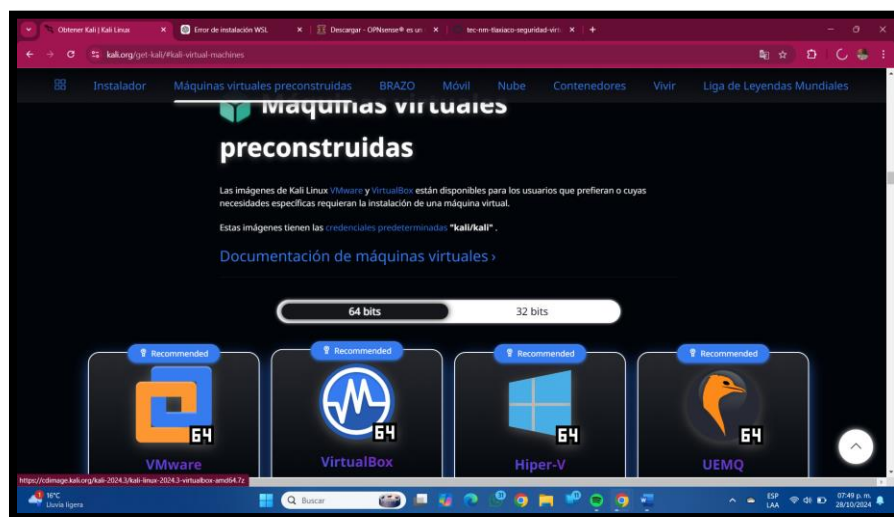


Ilustración 26 Elección de Máquina a utilizar

Iniciar la descarga

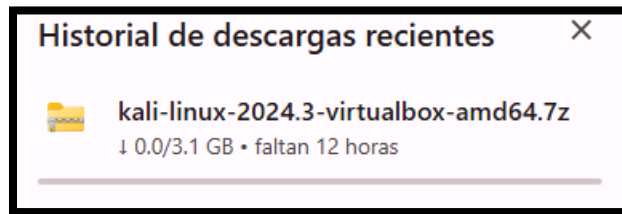


Ilustración 27 Descarga de Kali Linux en Proceso

Una vez que se haya culminado de descargar Kali Linux procedemos a montarlo en el archivo donde se encuentran nuestras máquinas virtuales para su fácil uso posteriormente y se podrá visualizar en Virtual Box cuando se abra.

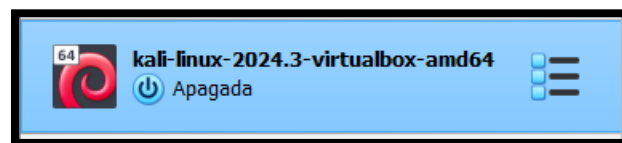
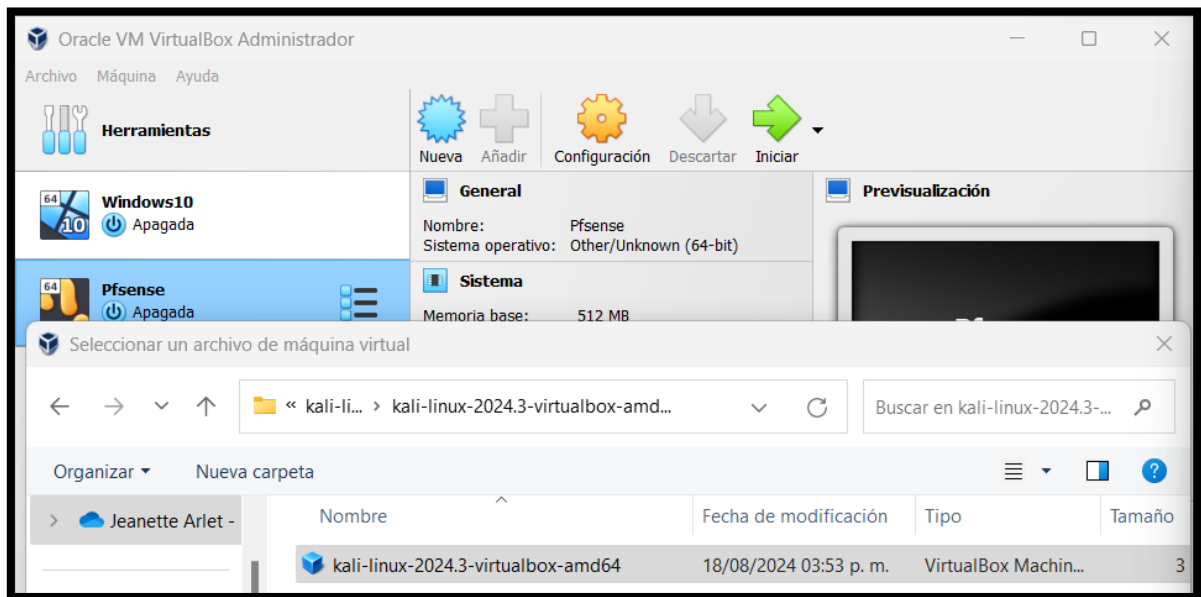


Ilustración 28 Kali Linux montado directamente

Configuración de Kali Linux: en seguida procedemos a la configuración para ellos sobre la máquina damos clic derecho y nos redirigimos a la parte de configuración, es importante que en el aparatado de “General”, “Descripción” revisemos el usuario y contraseña ya que después la utilizaremos para iniciar sesión.

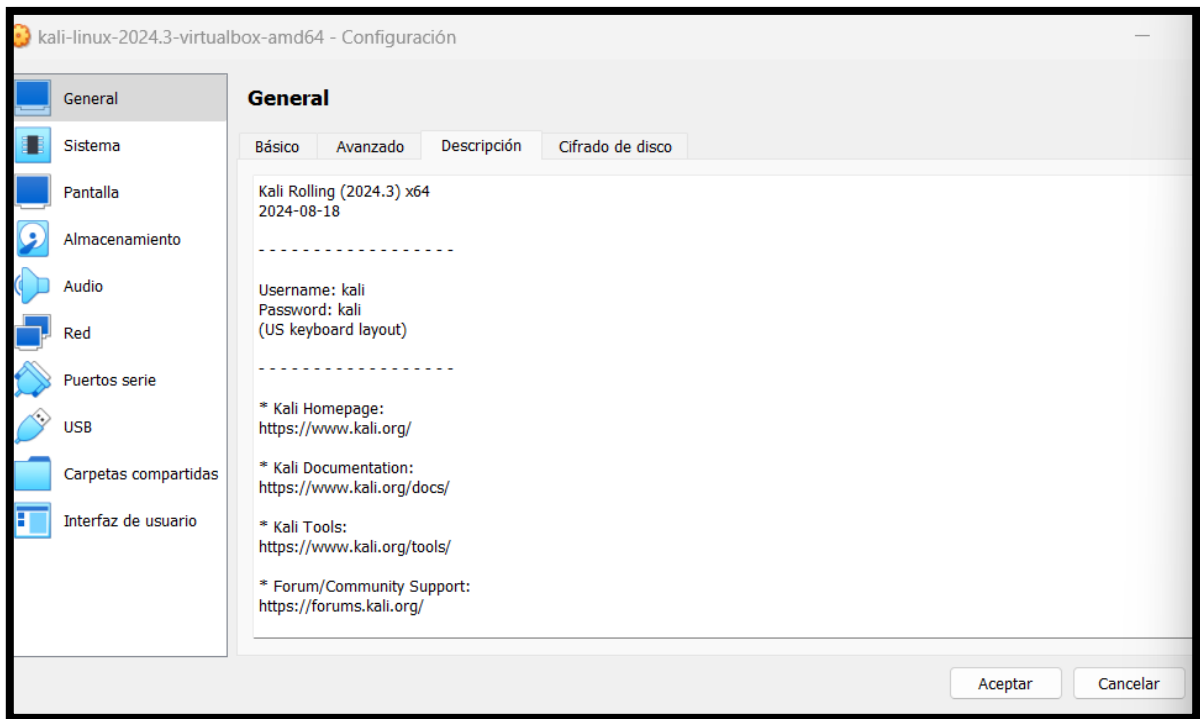


Ilustración 29 Revisión de usuario y contraseña de Kali Linux

Asignar la cantidad de memoria RAM que deseas dedicar a tu máquina virtual. En nuestro caso le asignamos 4096 MB, de procesadores 1 y en tanto al tamaño de disco duro 8GB, una vez hecho eso iniciamos la máquina dando clic derecho e “Iniciar”.

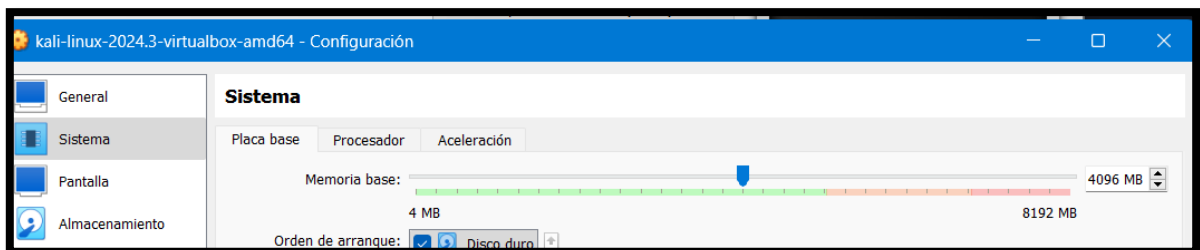


Ilustración 30 Asignación de atributos para nuestra máquina virtual de Kali Linux

Inicio de sesión: Finalmente ingresamos el usuario y contraseña que anteriormente revisamos para poder ingresar a la interfaz de Kali Linux.

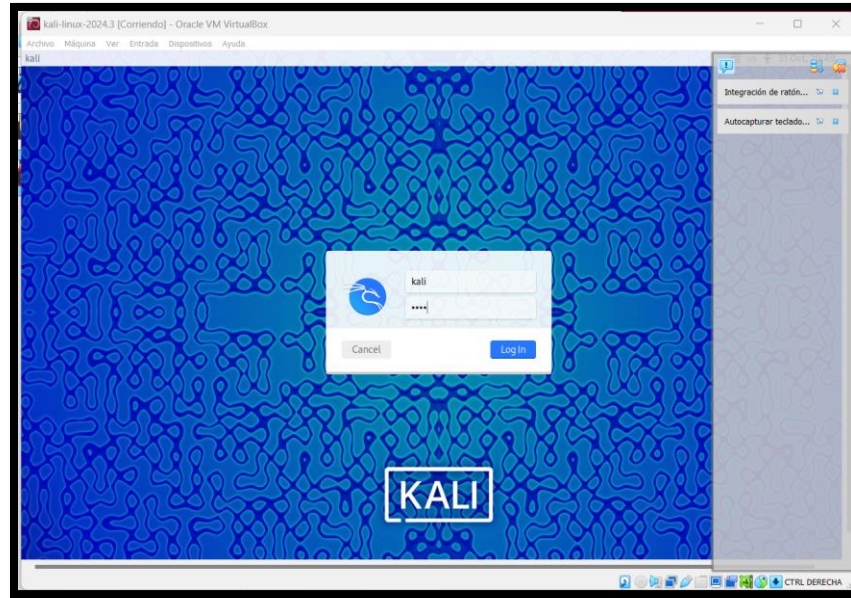


Ilustración 31 Inicio de Sesión en Kali Linux

Interfaz de Kali Linux

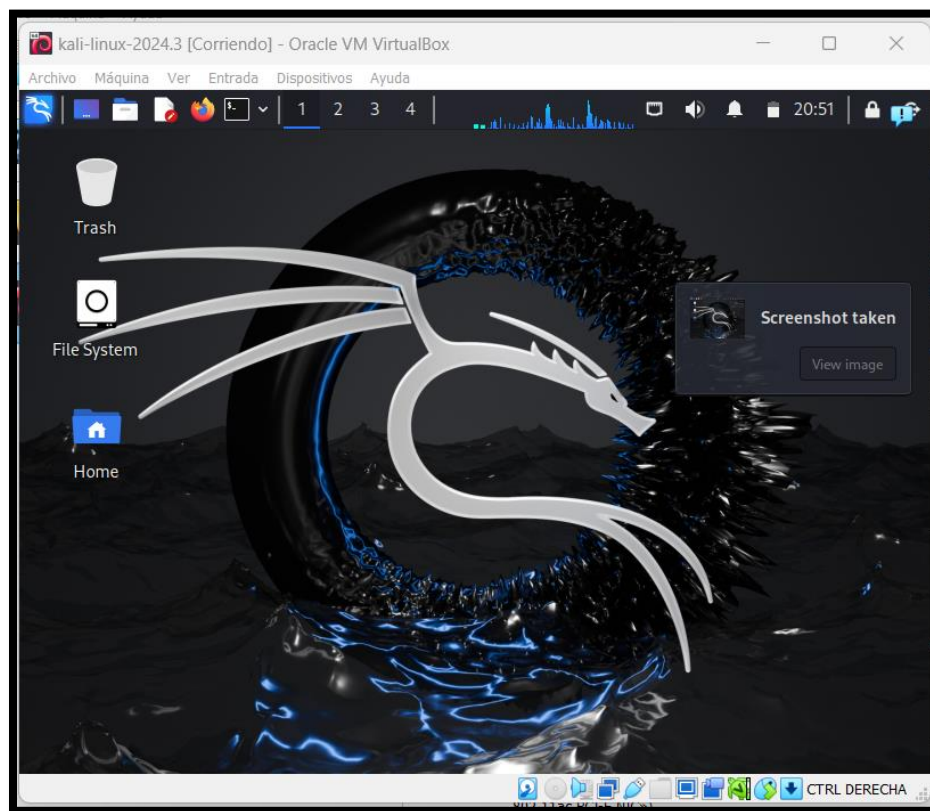


Ilustración 32 Interfaz de Kali Linux

CONFIGURACIÓN DE UN SISTEMA DE DETECCIÓN DE INTRUSOS EN KALI LINUX.

Actualización y preparación de Kali Linux mediante los siguientes comandos:

- `sudo apt update`
- `sudo apt upgrade`

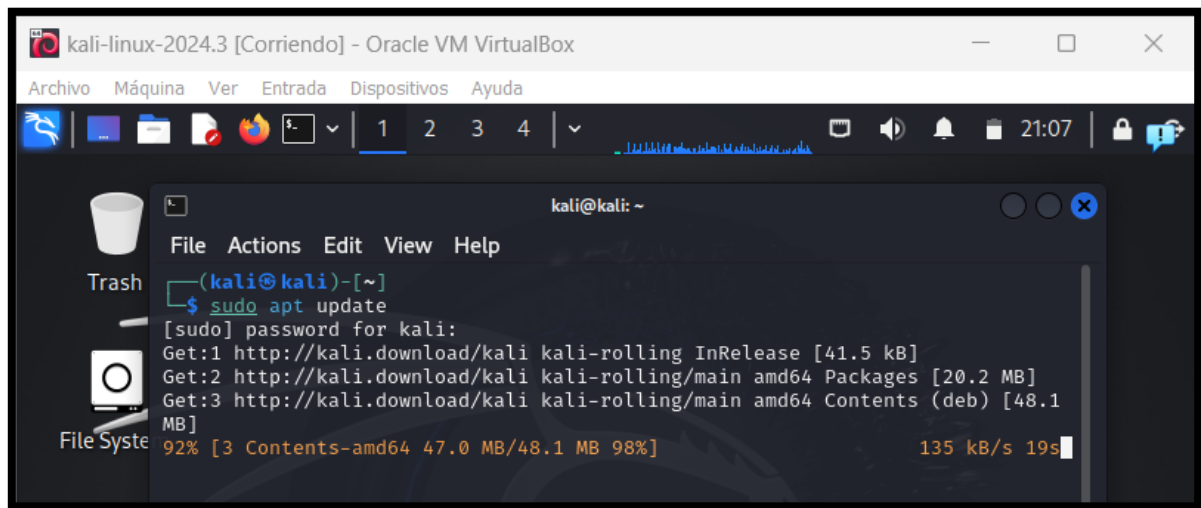


Ilustración 33 Actualización y preparación de Kali Linux

Instalar herramientas adicionales para que en lo posterior no marque errores “Opcional”.

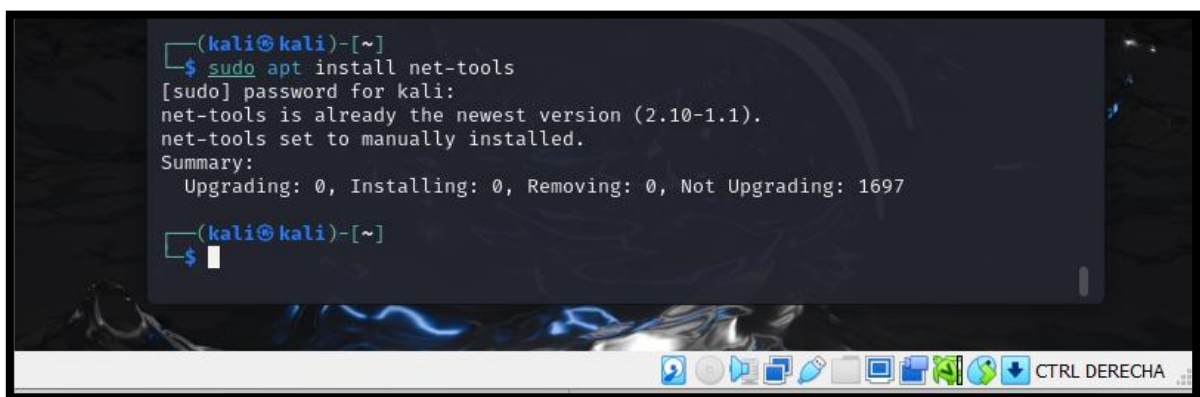
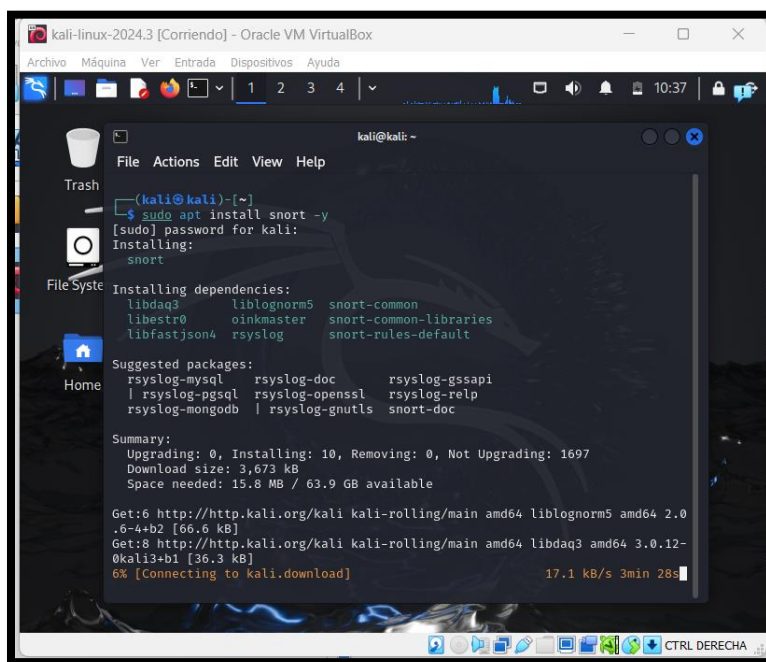


Ilustración 34 Herramientas adicionales en Kali Linux

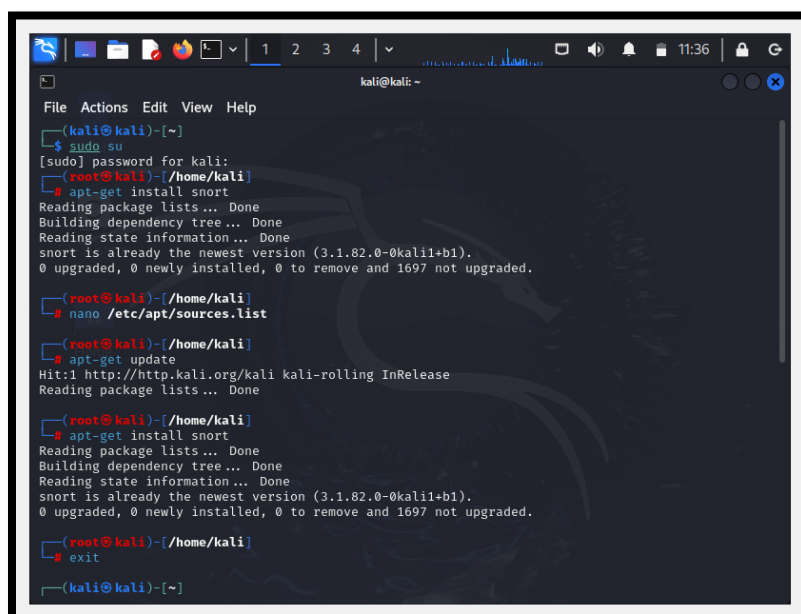
Instalar un sistema de detección de intrusos Snort mediante el comando de sudo
apt install Snort -y



```
kali@kali: ~  
$ sudo apt install snort -y  
[sudo] password for kali:  
Installing:  
snort  
  
Installing dependencies:  
libdaq3 liblognorm5 snort-common  
libestr0 oinkmaster snort-common-libraries  
libfastjson4 rsyslog snort-rules-default  
  
Suggested packages:  
rsyslog-mysql rsyslog-doc rsyslog-gssapi  
rsyslog-pgsql rsyslog-openssl rsyslog-relp  
rsyslog-mongodb rsyslog-gnutls snort-doc  
  
Summary:  
Upgrading: 0, Installing: 10, Removing: 0, Not Upgrading: 1697  
Download size: 3,673 kB  
Space needed: 15.8 MB / 63.9 GB available  
  
Get:6 http://http.kali.org/kali kali-rolling/main amd64 liblognorm5 amd64 2.0  
.6-4+b2 [66.6 kB]  
Get:8 http://http.kali.org/kali kali-rolling/main amd64 libdaq3 amd64 3.0.12-  
0kali3+b1 [36.3 kB]  
6% [Connecting to kali.download] 17.1 kB/s 3min 28s
```

Ilustración 35 Instalación del sistema de detección de intrusos Snort

Ingresar al administrador de Kali Linux donde procedemos a r5evisar que se haya
instalado correctamente Snort.



```
kali@kali: ~  
$ sudo su  
[sudo] password for kali:  
(root@kali)~ /home/kali  
# apt-get install snort  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
snort is already the newest version (3.1.82.0-0kali1+b1).  
0 upgraded, 0 newly installed, 0 to remove and 1697 not upgraded.  
(root@kali)~ /home/kali  
# nano /etc/apt/sources.list  
(root@kali)~ /home/kali  
# apt-get update  
Hit:1 http://http.kali.org/kali kali-rolling InRelease  
Reading package lists... Done  
(root@kali)~ /home/kali  
# apt-get install snort  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
snort is already the newest version (3.1.82.0-0kali1+b1).  
0 upgraded, 0 newly installed, 0 to remove and 1697 not upgraded.  
(root@kali)~ /home/kali  
# exit  
(kali@kali)~
```

Ilustración 36 Configuración de Snort

En seguida procedemos a verificar la interfaz de red que Snort debe monitorear.

```
(kali@kali)~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.13 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 2803:4600:1110:2d6f:a00:27ff:feb3:56cb prefixlen 64 scopeid 0<global>
    inet6 2803:4600:1110:2d6f:3b80:6449:f1d0:2e10 prefixlen 64 scopeid 0<global>
    inet6 fe80::a00:27ff:feb3:56cb prefixlen 64 scopeid 0<link>
    ether 08:00:27:b3:56:cb txqueuelen 1000 (Ethernet)
    RX packets 3859 bytes 530585 (518.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1683 bytes 195943 (191.3 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 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Ilustración 37 Verificación de red en Snort

A continuación, editamos el archivo de configuración ingresando con el comando `sudo nano /etc/snort/snort.conf` y una vez realizado los cambios le tecleamos “ctrl + o”, finalmente “ctrl + x” para salir.

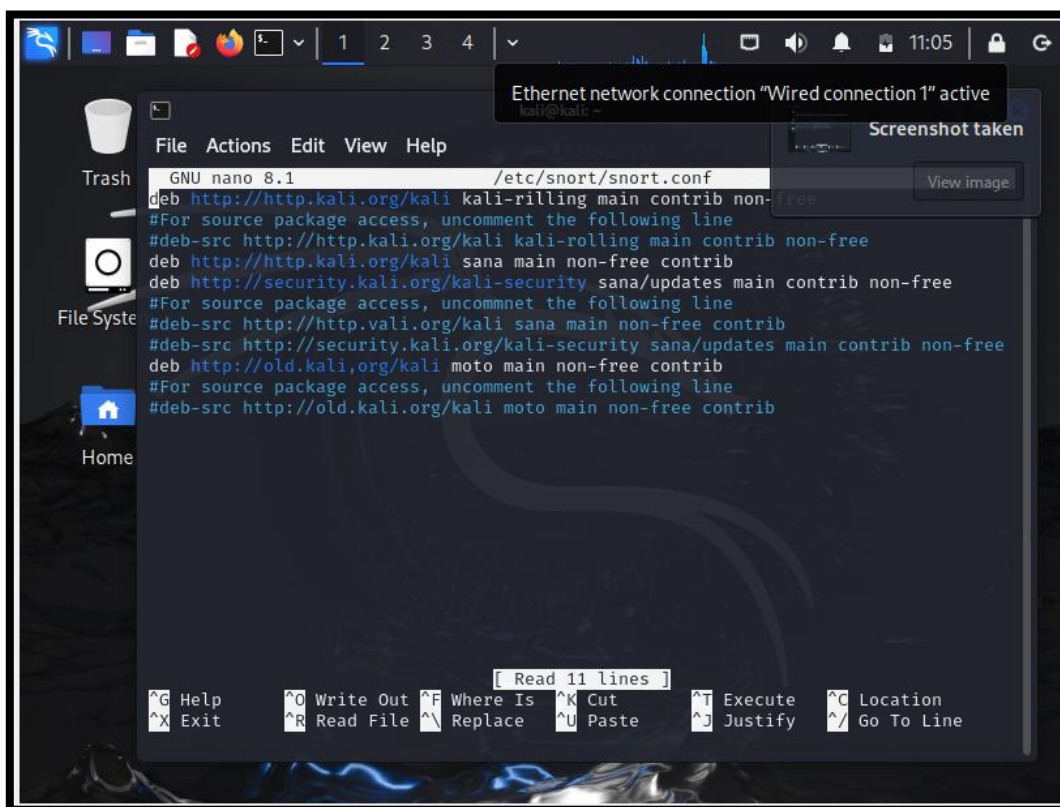


Ilustración 38 Edición del archivo de configuración

CREACION Y VERIFICACIÓN DE ARCHIVO DE REGLAS

Las reglas de Snort determinan qué patrones y comportamientos se consideran sospechosos, para ello ingresamos mediante el comando `touch /etc/snort/rules/custom.rules` y `nano /etc/snort/rules/custom.rules`

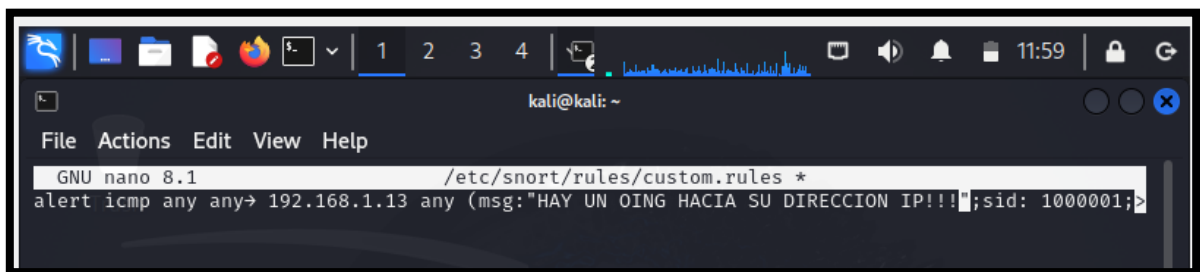
```
(kali@kali)-[~]
$ sudo su
(root@kali)-[/home/kali]
# touch /etc/snort/rules/custom.rules

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

(root@kali)-[/home/kali]
#
```

Ilustración 39 Creación y verificación de las reglas del archivo

En nuestro caso para la asignación de la regla de detección de intrusos fue mediante nuestra ip y mostrando un mensaje cuando se quiera o intente hacer ping.



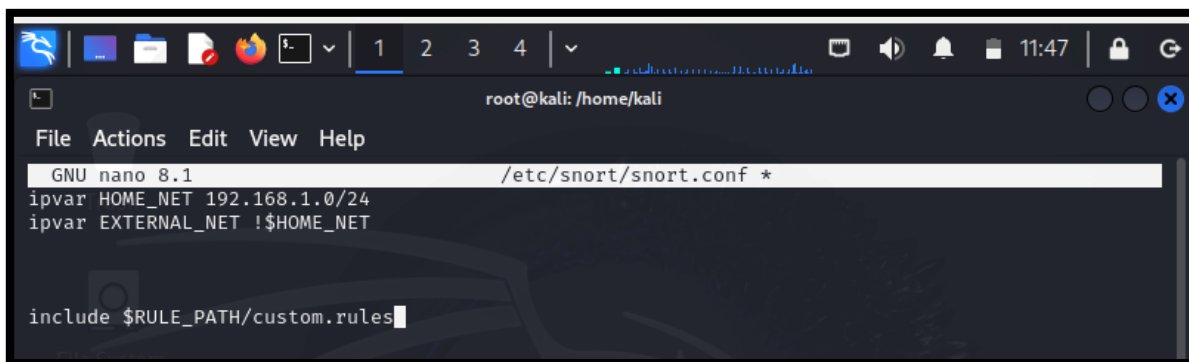
```
kali@kali: ~
File Actions Edit View Help
GNU nano 8.1 /etc/snort/rules/custom.rules *
alert icmp any any-> 192.168.1.13 any (msg:'HAY UN OING HACIA SU DIRECCION IP!!!';sid: 1000001; >
```

Ilustración 40 Asignación de la regla de detección de intrusos

Después continuamos configurando el archivo de snort mediante `nano /etc/snort/snort.conf`

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

En seguida buscamos la línea que define la variable HOME_NET y la ajustamos a la subred que deseamos proteger “192.168.1.0/24” así mismo definimos la regla para detectar un intento de acceso HTTP



```
GNU nano 8.1 /etc/snort/snort.conf *
ipvar HOME_NET 192.168.1.0/24
ipvar EXTERNAL_NET !$HOME_NET

include $RULE_PATH/custom.rules
```

Ilustración 41 Definición de la subred que deseamos proteger

Ejecutar el snort en modo IDS mediante el comando `snort -A console -q -c /etc/snort/snort.conf -i eth0`



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

Ilustración 42 Ejecución de Snort en modo IDS

- -A console: Muestra las alertas en la consola.
- -q: Modo silencioso (reduce la información de diagnóstico).
- -c: Especifica el archivo de configuración.
- -i: Especifica la interfaz de red a monitorear.

4. CREAR UNA MÁQUINA VIRTUAL VULNERABLE POR DISEÑO COMO METASPLOITABLE2

Descarga el instalador:

<https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>

(SOURCEFORGE, 2024). Ir al sitio web oficial de Metasploitable2 y seleccionar "Descargar la Última versión".

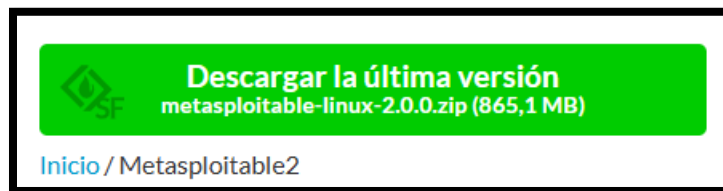


Ilustración 43 Página oficial para descargar Metasploitable2

Inicia la descarga

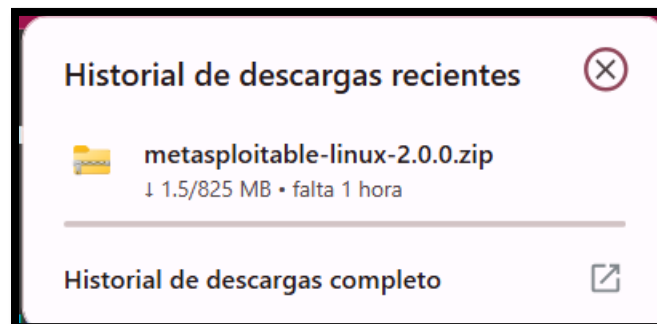


Ilustración 44 Descarga en proceso

Crea una nueva máquina virtual: Abre VirtualBox y haz clic en "Nueva" para crear una nueva máquina virtual, ingresa un nombre para tu máquina virtual en este caso le asignamos ("MetaSploitable"). Selecciona el tipo de sistema operativo como "Linux" y la versión como "Ubuntu (64-bit)".

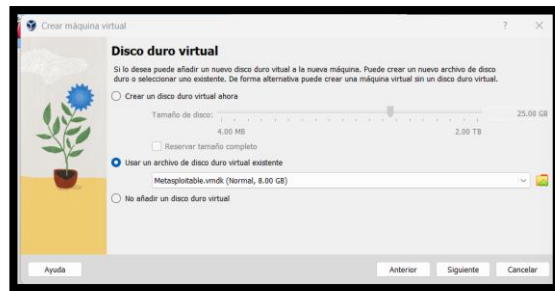
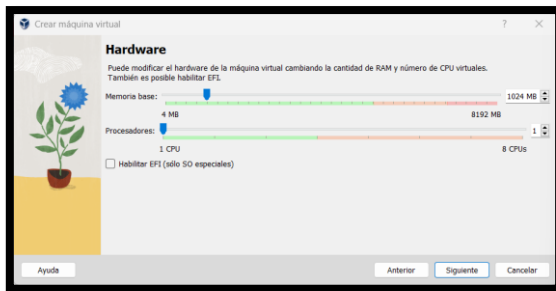
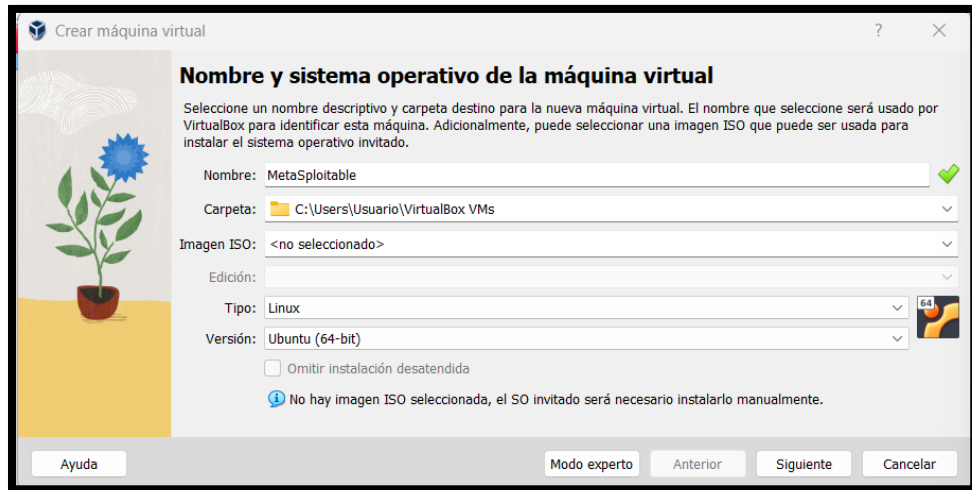


Ilustración 45 Asignación de atributos para nuestra máquina virtual

En seguida procedemos a iniciar nuestra máquina virtual e ingresamos con el usuario y contraseña que nos da por default “msfadmin” para ambos.

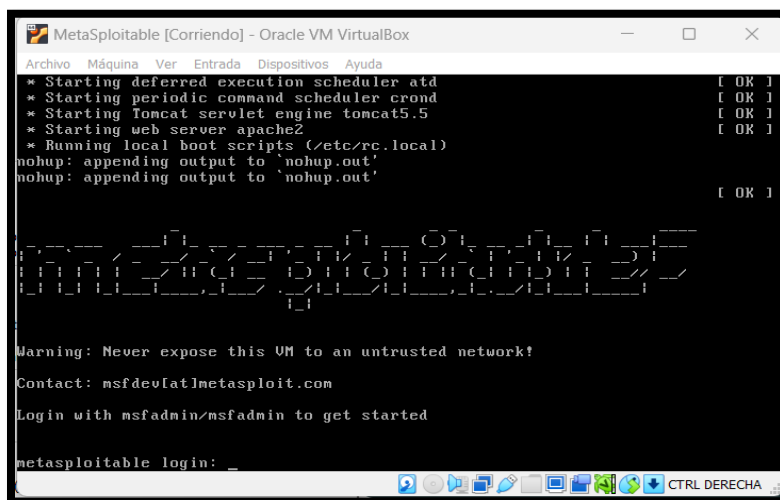
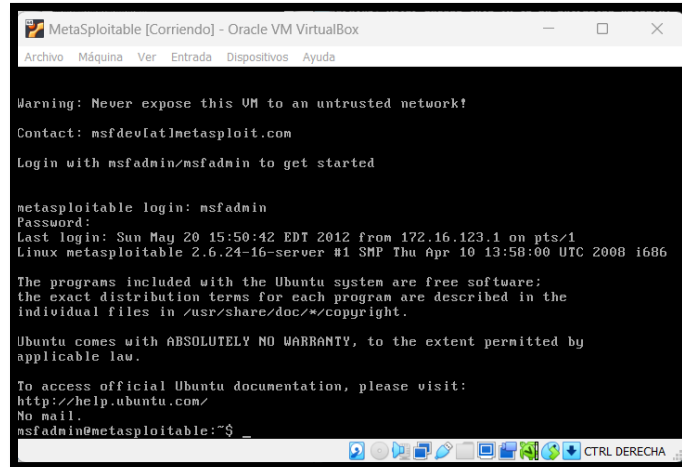


Ilustración 46 Instalación de Metasploitable2 instalado correctamente



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

metasploitable login: msfadmin
Password:
Last login: Sun May 20 15:50:42 EDT 2012 from 172.16.123.1 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

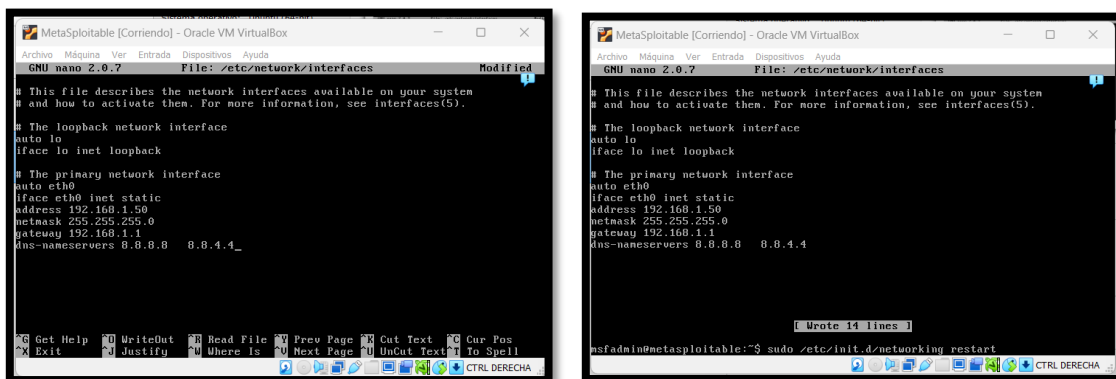
The programs included with the Ubuntu system are free software:
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

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

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

Ilustración 47 Inicio de sesión

Configuración y asignación de la IP statica



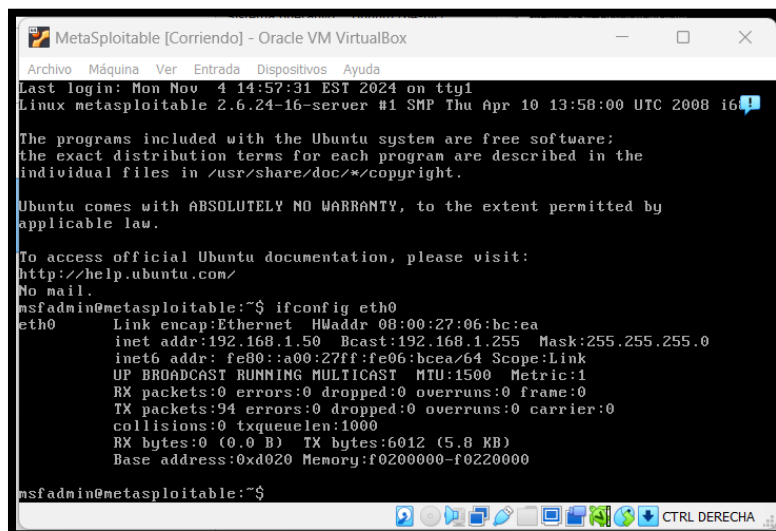
```
GNU nano 2.0.7 File: /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.50
netmask 255.255.255.0
gateway 192.168.1.1
dns-nameservers 8.8.8.8 8.8.4.4

[ Wrote 14 lines ]
msfadmin@metasploitable:~$ sudo /etc/init.d/networking restart
```

Ilustración 48 Configuración y asignación de la IP statica



```
Last login: Mon Nov 4 14:57:31 EST 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

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

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 08:00:27:06:bc:ea
          inet addr:192.168.1.50  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe06:bca/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:94 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:6012 (5.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

msfadmin@metasploitable:~$
```

5. PING SATISFACTORIO ENTRE LAS MÁQUINAS VIRTUALES.

PING ENTRE WINDOWS Y PFSENSE

Para poder hacer el ping entre las maquinas nos redirigimos al cmd en Windows y ponemos “ipconfig /release”, en seguida enter y tecleamos “ipconfig /renew” para que tome la dirección ip nueva y nos da la dirección ip que habíamos puesto en el Pfsense.

La otra manera de revisar es ingresar a nuestro Pfsense desde Windows mediante la dirección ip que habíamos asignado “10.0.0.1” en el mismo teniendo acceso sin problema.

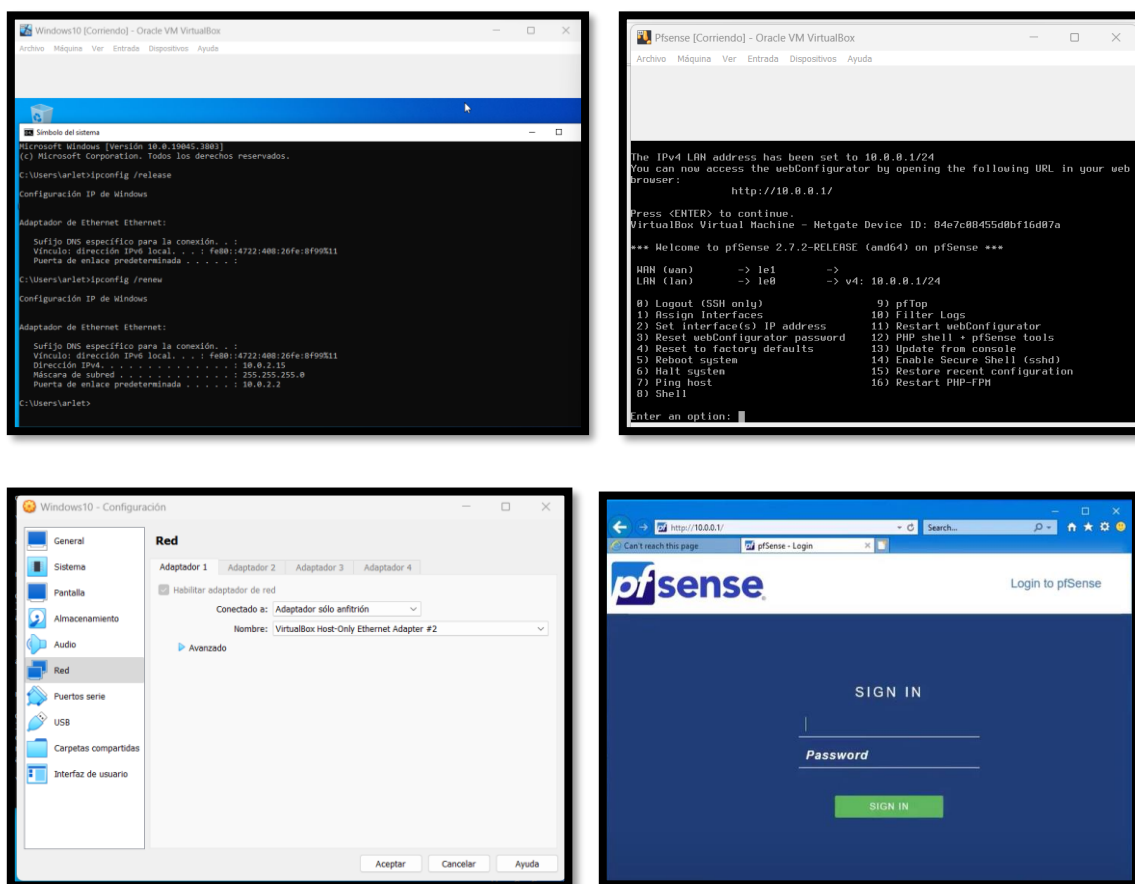


Ilustración 49 Ping entre Pfsense y Windows

PING ENTRE WINDOWS Y KALI LINUX

Haciendo ping desde nuestra máquina de Windows utilizando nuestra dirección ip de Kali que era 192.168.1.13

Máquina Kali Linux

```
(root@kali)~/home/derm
# snort -A console -q -c /etc/snort/snort.conf -i eth0
12/07-12:07:19.036590  [**] [1:1000001:1] HAY UN PING HACIA SU DIRECCION IP!!! [**] [Clas
sification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.1.10 → 192.168.1.13
12/07-12:07:20.046009  [**] [1:1000001:1] HAY UN PING HACIA SU DIRECCION IP!!! [**] [Clas
sification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.1.10 → 192.168.1.13
12/07-12:07:21.054071  [**] [1:1000001:1] HAY UN PING HACIA SU DIRECCION IP!!! [**] [Clas
sification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.1.10 → 192.168.1.13
12/07-12:07:22.075767  [**] [1:1000001:1] HAY UN PING HACIA SU DIRECCION IP!!! [**] [Clas
sification: Generic ICMP event] [Priority: 3] {ICMP} 192.168.1.10 → 192.168.1.13
```

Máquina de Windows

```
Haciendo ping a 192.168.1.13 con 32 bytes de datos:
Respuesta desde 192.168.1.13: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.13: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.13: bytes=32 tiempo<1m TTL=64
Respuesta desde 192.168.1.13: bytes=32 tiempo=1ms TTL=64

Estadísticas de ping para 192.168.1.13:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 1ms, Media = 0ms
```

6. CONCLUSIÓN

Al final de dicha práctica y la implementación del laboratorio podemos agregar que son herramientas poderosas para tener conocimientos previos sobre ciberseguridad sabiendo que pfSense actúa como firewall, Kali Linux como sistema de detección de intrusos y MetaSploitable2 como máquina vulnerable.

7. BIBLIOGRAFÍA

Kali. (s.f.). Kali: <https://www.kali.org/get-kali/#kali-platforms>

OPNsense. (s.f.). OPNsense: <https://opnsense.org/download/>

ORACLE. (2024). *ORACLE*. ORACLE: https://www.virtualbox.org/wiki/Download_Old_Builds_6_1

SOURCEFORGE. (2024). SOURCEFORGE:
<https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>