

## Table of Contents

|  |          |
|--|----------|
| <b>Laboratorio No. 5: Construcción de un laboratorio para pruebas de penetración .....</b> | <b>2</b> |
| Introducción .....   | 2        |
| Requerimientos técnicos.....   | 2        |
| Comprensión de la descripción general del laboratorio y sus tecnologías.....               | 3        |
| Configuración de un hipervisor y redes virtualmente aisladas .....                         | 5        |
| Paso 1: Implementación del hipervisor .....  | 6        |
| Paso 2: Crear redes virtualmente aisladas .....  | 7        |
| Configurar y trabajar con Kali Linux.....  | 8        |
| Parte 1: Configurar Kali Linux como una máquina virtual .....                              | 9        |
| Paso 2: Personalización de la máquina virtual Kali Linux y los adaptadores de red.....     | 11       |
| Paso 3: Comenzar con Kali Linux .....  | 17       |
| Paso 4: Actualización de fuentes y paquetes .....  | 20       |
| Implementación de Metasploitable 2 como sistema de destino .....                           | 21       |
| Parte 1: Implementación de Metasploitable 2.....   | 22       |
| Parte 2: Configurar los ajustes de red .....   | 26       |

## Laboratorio No. 5: Construcción de un laboratorio para pruebas de penetración

### Introducción

Como futuro hacker ético o probador de penetración, es muy importante cuando pruebe exploits, cargas útiles o practique sus habilidades de piratería que no interrumpa ni cause ningún tipo de daño o daño a los sistemas o la infraestructura de red de otra persona, como la de su organización. Trabajar en el campo de las pruebas de penetración significa enfocarse en mejorar continuamente sus habilidades. Mucha gente puede hablar sobre piratería y explicar la metodología con bastante claridad, pero no saben cómo realizar un ataque. Al aprender sobre las pruebas de penetración, es muy importante comprender la teoría y cómo usar sus habilidades para aplicarlas a un ciberataque en el mundo real.

En esta guía, aprenderá a diseñar y crear su entorno de laboratorio de pruebas de penetración en su computadora existente utilizando tecnologías de virtualización. Aprenderá a crear una red virtual aislada para asegurarse de no atacar accidentalmente sistemas que no son de su propiedad. Luego, aprenderá cómo configurar Kali Linux como un sistema atacante y clientes y servidores vulnerables como sus objetivos. Practicar sus habilidades de piratería en sistemas y redes que no son de su propiedad es intrusivo e ilegal porque puede causar daños y perjuicios a esos sistemas.

### Requerimientos técnicos

Para seguir los ejercicios de este laboratorio, asegúrese de cumplir con los siguientes requisitos de hardware y software:

- Oracle VM VirtualBox: <https://www.virtualbox.org/wiki/Downloads>
- Oracle VM VirtualBox Extension Pack: <https://www.virtualbox.org/wiki/Downloads>
- Kali Linux 2021.2: <https://www.kali.org/get-kali/>
- OWASP Juice Shop: <https://owasp.org/www-project-juice-shop/>

- Metasploitable 2:  
<https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>
- OWASP Broken Web Applications:  
<https://sourceforge.net/projects/owaspbwa/files/>

## Comprensión de la descripción general del laboratorio y sus tecnologías

La creación de un laboratorio de pruebas de penetración virtual le permite crear un entorno seguro para perfeccionar sus habilidades, escalar el entorno para agregar nuevos sistemas vulnerables e incluso eliminar sistemas heredados más antiguos que quizás ya no necesite, e incluso crear redes virtuales para pivotar sus ataques de una red a otra. El concepto de crear su propio laboratorio de pruebas de penetración virtualizado le permite maximizar los recursos en su computadora existente, sin la necesidad de comprar tiempo de laboratorio en línea de varios proveedores de servicios o incluso comprar computadoras y servicios adicionales. En general, ahorrará mucho dinero en lugar de comprar computadoras físicas y equipos de red, como conmutadores y enrutadores.

Las siguientes son algunas de las desventajas de un laboratorio físico:

- Se requiere espacio físico para almacenar los numerosos servidores y dispositivos de red que se necesitan.
- El consumo de energía por dispositivo dará como resultado una alta tasa general de gastos financieros.
- El costo de construir/comprar cada dispositivo físico es alto, ya sea un dispositivo de red o un servidor.

Poder utilizar las tecnologías de virtualización que han surgido como respuesta a estos inconvenientes ha abierto multitud de puertas en el campo de las TI. Esto ha permitido a muchas personas y organizaciones optimizar y administrar sus recursos de hardware de manera más eficiente.

En el mundo de la virtualización, un hipervisor es una aplicación especial que permite a un usuario virtualizar los recursos de hardware en su sistema para que puedan compartirse con otro sistema operativo o una aplicación. Esto le permite instalar más de un sistema

operativo sobre el sistema operativo existente de su computadora. Imagine que está ejecutando Microsoft Windows 10 como su sistema operativo principal, pero desea ejecutar Linux al mismo tiempo en la misma computadora. Puede lograr esto usando un hipervisor. Por lo tanto, vamos a utilizar la virtualización para garantizar que podamos construir un entorno de laboratorio de pruebas de penetración rentable.

Necesitaremos los siguientes componentes para construir nuestro laboratorio de pruebas de penetración:

- **Hipervisor:** Necesario para crear máquinas virtuales. Usaremos Oracle VM VirtualBox como nuestra aplicación de hipervisor preferida.
- **Acceso a Internet:** Requerido para descargar aplicaciones adicionales. Se proporcionará acceso a Internet a nuestro sistema atacante mientras se asegura que todos nuestros sistemas permanezcan virtualmente aislados.
- **Una máquina de pruebas de penetración:** Este sistema será el sistema atacante. Usaremos Kali Linux.
- **Sistemas de clientes vulnerables:** estos serán nuestros sistemas objetivo/víctima para las pruebas de seguridad. Los sistemas vulnerables incluirán Metasploitable 2 y Metasploitable 3 (ambas versiones de Windows y Linux), aunque se pueden agregar sistemas adicionales a medida que avanza en este libro.
- **Aplicaciones web vulnerables:** estos son sistemas que contienen aplicaciones web vulnerables para ayudarlo a comprender las debilidades de seguridad en las aplicaciones web. Estos serán el proyecto de seguridad de aplicaciones web abiertas (OWASP) Juice Shop y los sistemas de aplicaciones web rotas (BWA) de OWASP.

Además, el siguiente diagrama es nuestra topología de laboratorio de pruebas de penetración de red:

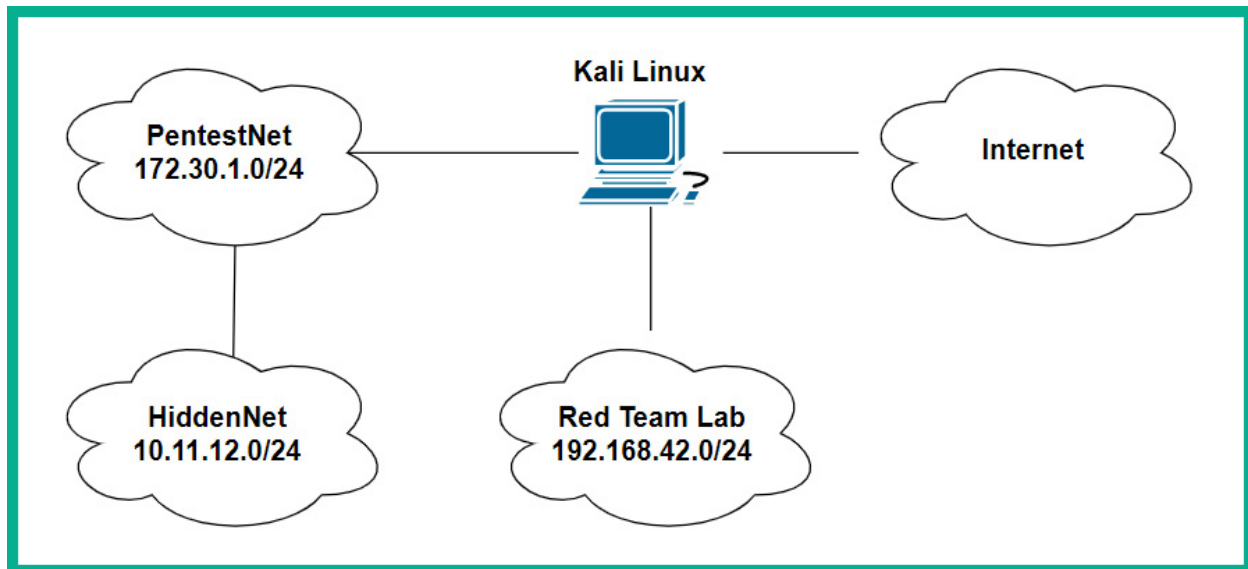


Figura 1: Topología del laboratorio

Como se muestra en el diagrama anterior, hay tres redes privadas.

1. La red PentestNet está en la red 172.30.1.0/24, que contiene sistemas vulnerables como Metasploitable 2/3 y máquinas virtuales OWASP BWA.
2. La red HiddenNet está en la red 10.11.12.0/24, a la que solo se puede acceder a través de la red 172.30.1.0/24. Esta es una configuración perfecta para aprender sobre el movimiento lateral y pivotar.
3. Además, Kali Linux está conectado directamente al laboratorio Red Team, que contiene una red de Active Directory (AD).

Ahora que se tiene una idea de la topología del laboratorio, así como de los sistemas y tecnologías con los que trabajaremos a lo largo de este curso, comencemos por configurar un hipervisor y redes virtuales.

### Configuración de un hipervisor y redes virtualmente aisladas

Si bien hay muchos otros hipervisores disponibles dentro de la industria, Oracle VM VirtualBox es un hipervisor gratuito y fácil de usar que contiene casi todas las características de los productos comerciales.

En esta sección, aprenderá cómo configurar el hipervisor VirtualBox y cómo crear redes virtuales.

Antes de comenzar, los siguientes son algunos factores y requisitos importantes:

- Asegúrese de que su procesador sea compatible con las funciones de virtualización VT-x/AMD-V.
- Asegúrese de que la función de virtualización esté habilitada en su BIOS/UEFI.

### Paso 1: Implementación del hipervisor

Si bien existen muchas aplicaciones de hipervisor de varios proveedores dentro de la industria, usaremos Oracle VirtualBox a lo largo de este curso. Sin embargo, si desea utilizar otro hipervisor, simplemente asegúrese de configurarlo con los mismos sistemas y diseño de red.

Para comenzar a implementar Oracle VirtualBox, realice los siguientes pasos:

Para descargar VirtualBox, vaya a <https://www.virtualbox.org/wiki/Downloads> y elija un paquete de plataforma según su sistema operativo:

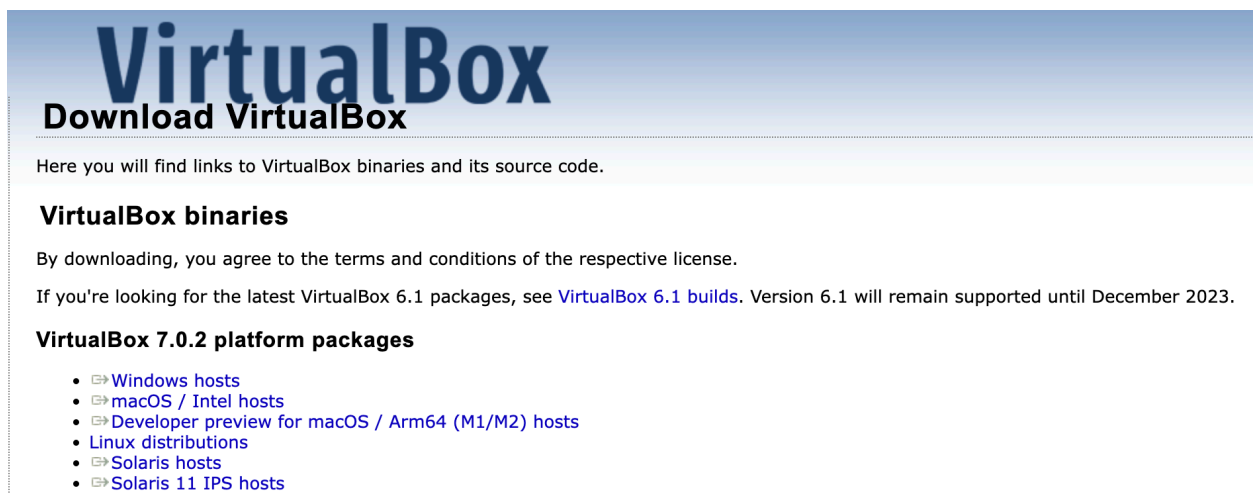


Figura 2: Sitio de descarga de VirtualBox

---

Prof. Ing. Adrián Argüello Quesada, M.A.E.

Fuente: Glen D. Sight (2022). The Ultimate Kali Linux Book - Second Edition. Packt Publishing <https://learning.oreilly.com/library/view/the-ultimate-kali/9781801818933/>

A continuación, necesitaremos Oracle VM VirtualBox Extension Pack, que nos permite realizar funciones adicionales mediante VirtualBox, como la creación de redes virtuales aisladas. En la misma página de descarga, desplácese un poco hacia abajo para encontrar el enlace de descarga:



Figura 3: Paquete de extensión de VirtualBox

A continuación, instale el paquete de la plataforma VirtualBox que descargó en el paso 1. Asegúrese de utilizar las configuraciones predeterminadas. Una vez instalada la aplicación, aparecerá la interfaz de VirtualBox Manager.

Para instalar VirtualBox Extension Pack, simplemente haga clic derecho y seleccione Abrir con > VirtualBox Manager. Asegúrese de aceptar el acuerdo de usuario y continúe con la instalación.

## Paso 2: Crear redes virtualmente aisladas

Al crear un entorno de laboratorio de pruebas de intrusión, no debe escanear ni liberar accidentalmente una carga útil maliciosa en los sistemas y redes de su propiedad, como los de Internet. Los siguientes pasos le enseñarán cómo crear redes virtuales aisladas dentro de Oracle VirtualBox para admitir nuestra topología de laboratorio de pruebas de penetración de red:

1. Para crear una red virtual con un servidor DHCP para la red 172.30.1.0/24, abra el símbolo del sistema de Windows y ejecute los siguientes comandos:

```
C:\> cd C:\Program Files\Oracle\VirtualBox
C:\Program Files\Oracle\VirtualBox> vboxmanage dhcpserver add --
network=PentestNet --server-ip=172.30.1.1 --lower-ip=172.30.1.20 --
upper-ip=172.30.1.50 --netmask=255.255.255.0 --enable
```

Estos comandos permiten a VirtualBox crear un servidor DHCP con una dirección IP de 172.30.1.1 para distribuir un rango de direcciones IP de 172.30.1.20 a 172.30.1.50 para cualquier máquina virtual conectada a la red PentestNet.

2. A continuación, en el mismo símbolo del sistema de Windows, use los siguientes comandos para crear una red virtual con un servidor DHCP para la red oculta. Lo llamaremos HiddenNet:

```
C:\> cd C:\Program Files\Oracle\VirtualBox
C:\Program Files\Oracle\VirtualBox> vboxmanage dhcpserver add --
network=HiddenNet --server-ip=10.11.12.1 --lower-ip=10.11.12.20 -
-upper-ip=10.11.12.50 --netmask=255.255.255.0 --enable
```

3. A continuación, creemos una red virtual aislada para nuestro laboratorio Red Team:

```
C:\> cd C:\Program Files\Oracle\VirtualBox
C:\Program Files\Oracle\VirtualBox> vboxmanage dhcpserver add --
network=RedTeamLab --server-ip=192.168.42.1 --lower-
ip=192.168.42.20 --upper-ip=192.168.42.50 --netmask=255.255.255.0
--enable
```

4. Asegúrese de utilizar la convención de nomenclatura adecuada para cada laboratorio a lo largo de este libro (PentestNet, HiddenNet y RedTeamLab) para garantizar que su red virtual funcione como se espera.

## Configurar y trabajar con Kali Linux

El sistema operativo Kali Linux se basa en Debian de Linux y consta de más de 300 herramientas preinstaladas, con funciones que van desde el reconocimiento hasta la explotación e incluso análisis forense. El sistema operativo Kali Linux ha sido diseñado no solo para profesionales de seguridad, sino también para administradores de TI e incluso profesionales de seguridad de redes dentro de la industria. Al ser un sistema operativo de seguridad gratuito, contiene las herramientas necesarias para realizar pruebas de seguridad.



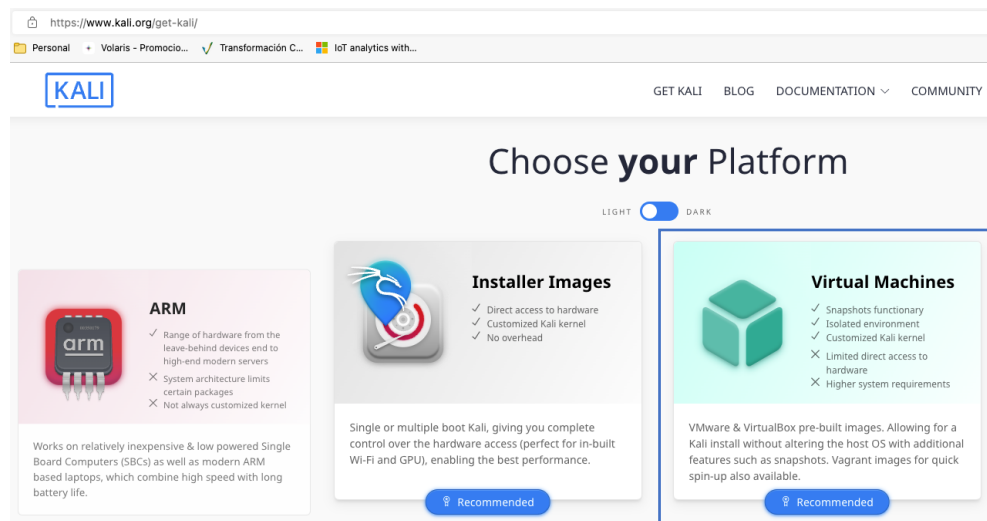
Kali Linux tiene muchas características y herramientas que hacen que el trabajo de un Pentester o un ingeniero de seguridad sea un poco más fácil cuando están trabajando. Existen muchas herramientas, scripts y marcos para realizar diversas tareas, como recopilar información sobre un objetivo, realizar análisis de red, descubrir vulnerabilidades e incluso explotar, por nombrar solo algunas.

En esta sección, aprenderá cómo configurar Kali Linux como una máquina virtual, establecer conexiones de red a Internet y redes aisladas, y conocer los conceptos básicos de Kali Linux.

## Parte 1: Configurar Kali Linux como una máquina virtual

Hay muchos tipos de implementación para Kali Linux, desde realizar una instalación completa directamente en el hardware hasta instalarlo en dispositivos Android. Para simplificar el proceso de configuración, aprenderemos cómo configurar la imagen de la máquina virtual Kali Linux dentro de Oracle VirtualBox. Este método garantiza que pueda estar en funcionamiento muy rápidamente. Para comenzar, realice los siguientes pasos:

1. Para descargar la imagen virtual oficial de Kali Linux 2021.2, vaya a <https://www.kali.org/get-kali/> y haga clic en el archivo Virtual Machines.

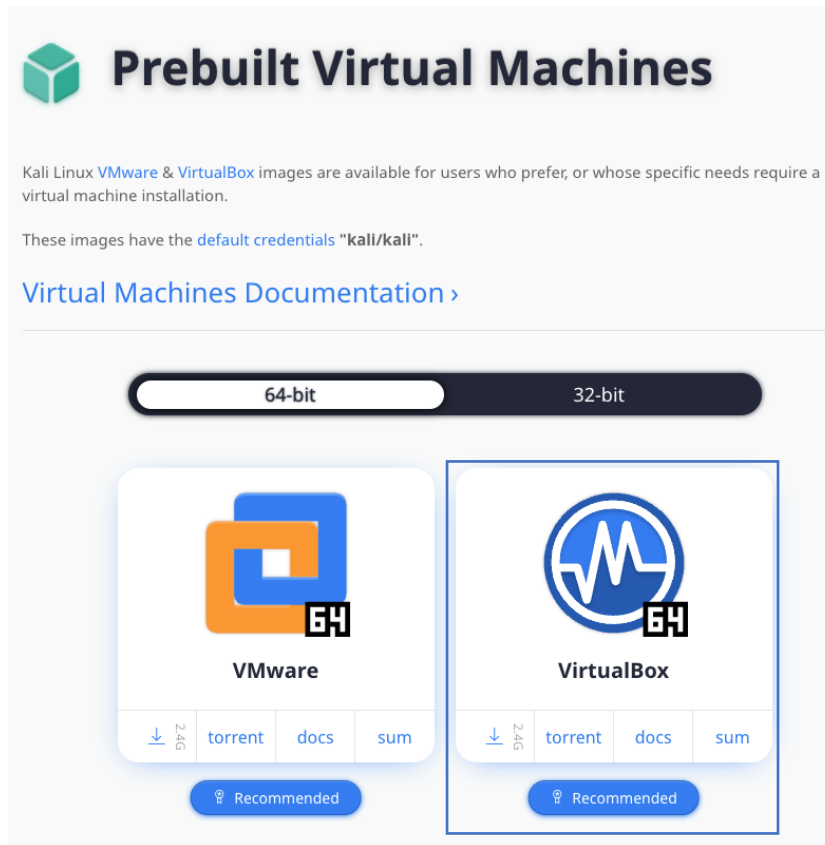


Prof. Ing. Adrián Argüello Quesada, M.A.E.

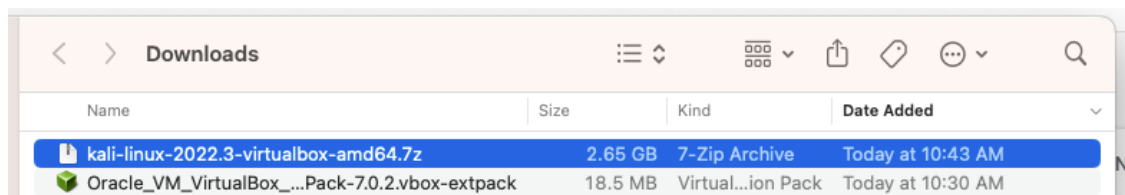
Fuente: Glen D. Sight (2022). The Ultimate Kali Linux Book - Second Edition. Packt

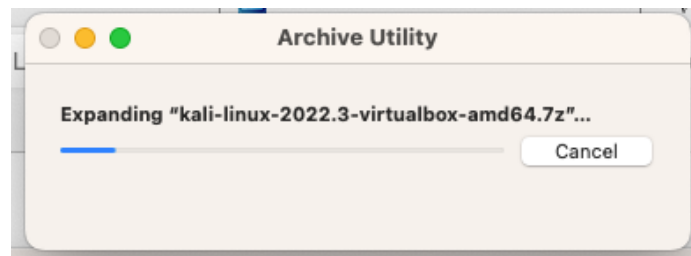
Publishing <https://learning.oreilly.com/library/view/the-ultimate-kali/9781801818933/>

- Haga clic en la imagen de VirtualBox 64 para descargar el archivo OVA de Kali Linux. Alternativamente, puede usar el enlace oficial de torrent, como se muestra aquí:

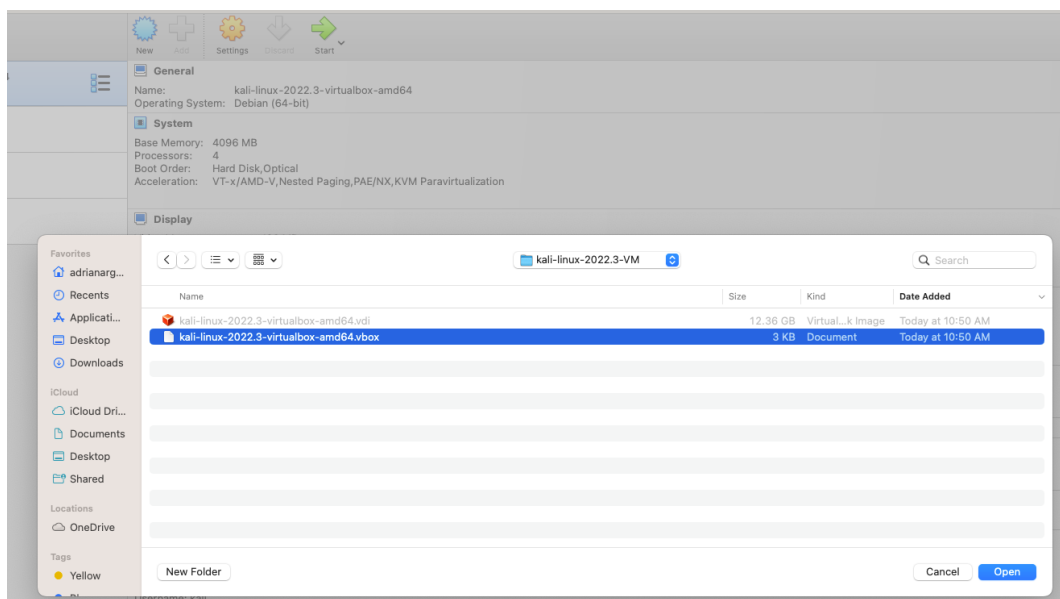


- A continuación, una vez que el archivo se haya descargado en su sistema, en caso de estar comprimido, debe descomprimirlo con alguna herramienta adecuada.





4. Una vez hecho esto, ejecute Oracle VirtualBox para importarlo a VirtualBox como una máquina virtual.
5. A continuación, haga clic en la opción Add y seleccione el archivo .vbox



6. Una vez que se complete el proceso de importación, verá que su máquina virtual Kali Linux ahora está disponible en Oracle VirtualBox Manager.

## Paso 2: Personalización de la máquina virtual Kali Linux y los adaptadores de red

Los siguientes pasos le enseñarán cómo personalizar el entorno virtual de Kali Linux y alinearlos con nuestra topología de laboratorio de pruebas de penetración. Realice los

---

Prof. Ing. Adrián Argüello Quesada, M.A.E.

Fuente: Glen D. Sight (2022). The Ultimate Kali Linux Book - Second Edition. Packt Publishing <https://learning.oreilly.com/library/view/the-ultimate-kali/9781801818933/>

siguientes pasos para asegurarse de que sus máquinas virtuales Kali Linux se hayan configurado correctamente para la red de laboratorio:

Para garantizar que se pueda acceder a la función Nested VT-x/AMD-V entre la máquina virtual y el procesador, necesitaremos ejecutar los siguientes comandos dentro del símbolo del sistema de Windows:

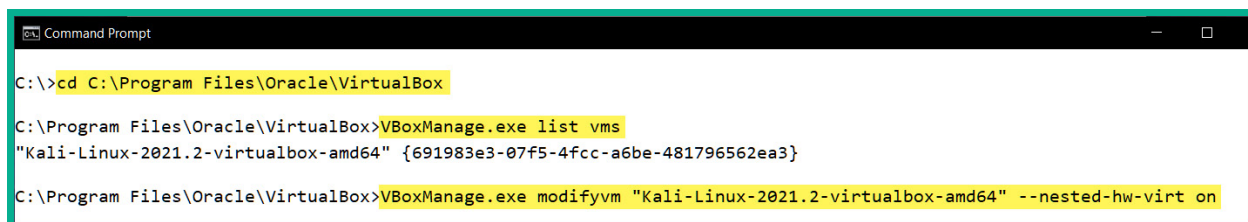
```
C:\> cd C:\Archivos de programa\Oracle\VirtualBox  
C:\Archivos de programa\Oracle\VirtualBox> VBoxManage.exe list vms
```

Este comando le permite ver una lista de todas las máquinas virtuales y sus nombres dentro de VirtualBox.

Luego, usando el nombre de su máquina virtual Kali Linux, use el siguiente comando para habilitar la función Nested VT-x/AMD-V en la máquina virtual:

```
C:\Program Files\Oracle\VirtualBox> VBoxManage.exe modifyvm "VM Name"  
--nested-hw-virt on
```

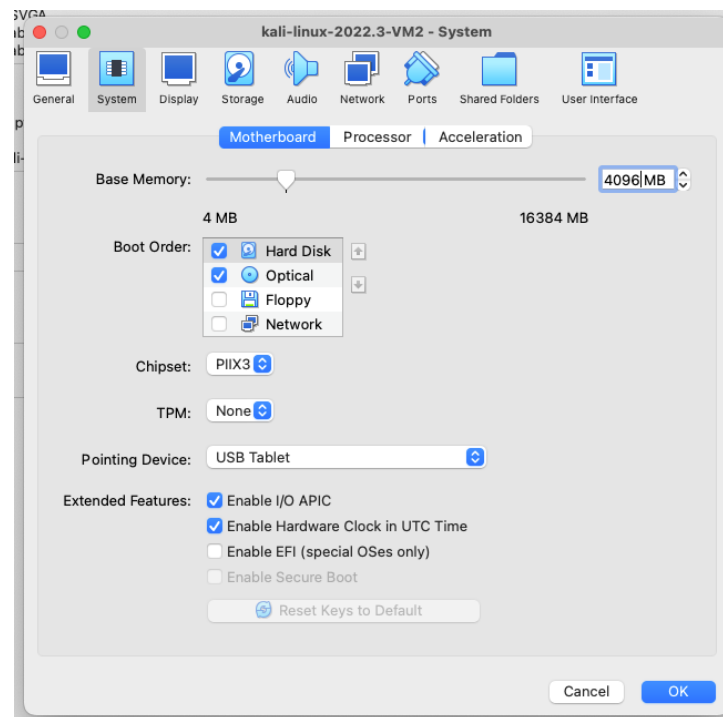
Asegúrese de sustituir el nombre de su máquina virtual Kali Linux con el nombre que se muestra entre comillas, como se muestra aquí:



```
Command Prompt  
C:\>cd C:\Program Files\Oracle\VirtualBox  
C:\Program Files\Oracle\VirtualBox>VBoxManage.exe list vms  
"Kali-Linux-2021.2-virtualbox-amd64" {691983e3-07f5-4fcc-a6be-481796562ea3}  
C:\Program Files\Oracle\VirtualBox>VBoxManage.exe modifyvm "Kali-Linux-2021.2-virtualbox-amd64" --nested-hw-virt on
```

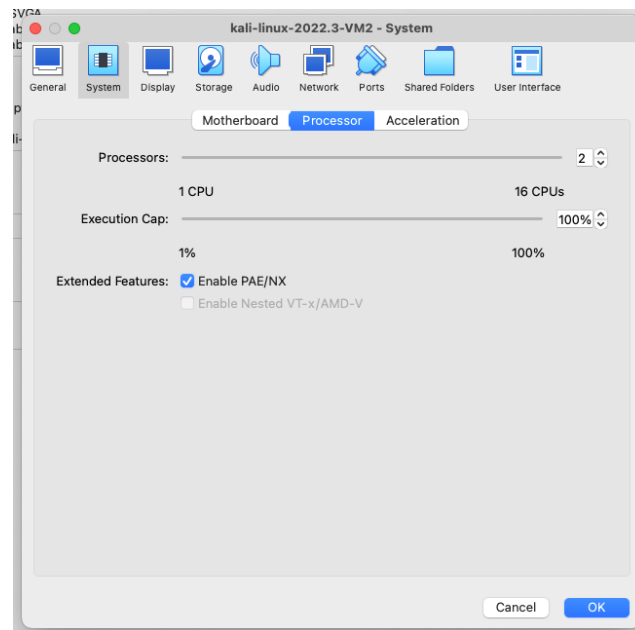
A continuación, para asignar Kali Linux a cada red virtual, seleccione la máquina virtual Kali Linux y haga clic en Configuración, como se muestra aquí:

Puede ajustar la cantidad de memoria (RAM) que se puede asignar a la máquina virtual yendo a Sistema > Placa base > Memoria base:



Se recomienda que se asegure de no asignar memoria dentro de las zonas amarilla y roja, como se muestra en la captura de pantalla anterior. Kali Linux puede ejecutarse eficientemente con 2 GB de RAM; sin embargo, si su sistema tiene más de 8 GB disponibles, considere asignar 4 GB de RAM.

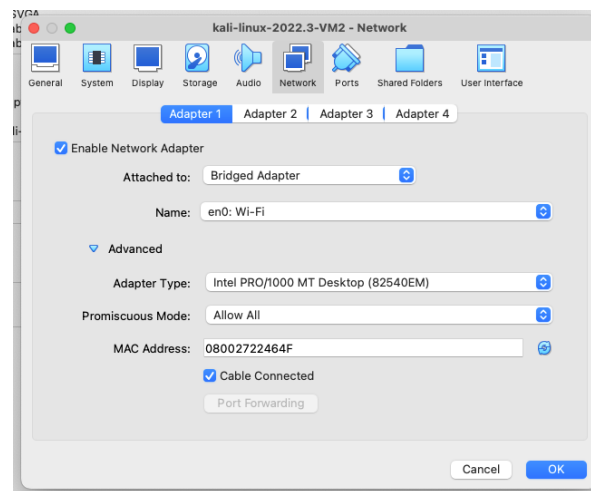
En la pestaña Sistema > Procesador, también puede ajustar la cantidad de núcleos de CPU que se asignarán a la máquina virtual. Usar entre 1 y 2 núcleos es suficiente; sin embargo, puede asignar más según los recursos disponibles en la computadora.



A continuación, permitamos que Kali Linux acceda directamente a Internet. En el menú Configuración de Kali Linux, seleccione la categoría Red > Adaptador 1 y use las siguientes configuraciones:

- Habilite el adaptador de red.
- Adjunto a: Adaptador en puente.
- Nombre: establezca esto en la tarjeta de interfaz de red de su dispositivo, que debe tener conectividad a Internet.
- Modo promiscuo: permitir todo.

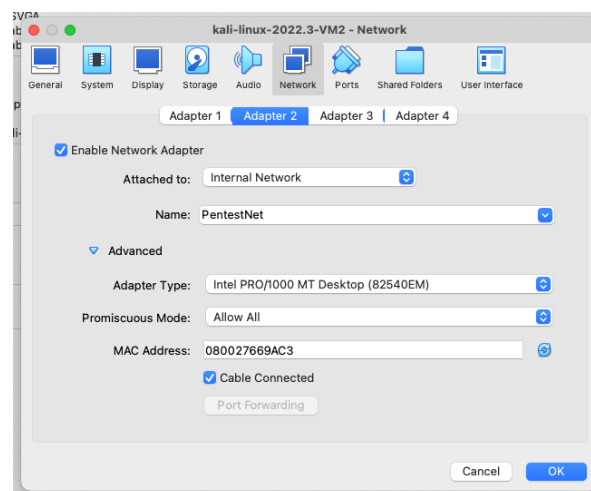
La siguiente captura de pantalla muestra estas configuraciones aplicadas al adaptador:



A continuación, asignemos la red PentestNet a Kali Linux. Simplemente seleccione el Adaptador 2 y use las siguientes configuraciones:

- Marque Habilitar adaptador de red
- Adjunto a: Red Interna
- Nombre: PentestNet
- Modo promiscuo: permitir todo

La siguiente captura de pantalla muestra estas configuraciones aplicadas al adaptador:



---

Prof. Ing. Adrián Argüello Quesada, M.A.E.

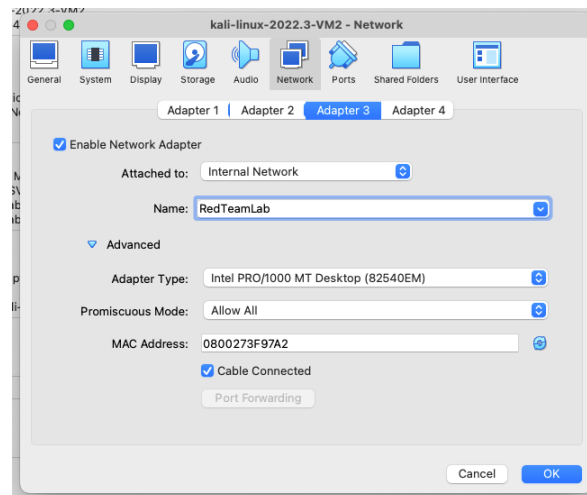
Fuente: Glen D. Sight (2022). The Ultimate Kali Linux Book - Second Edition. Packt Publishing <https://learning.oreilly.com/library/view/the-ultimate-kali/9781801818933/>

Después de configurar los ajustes en el Adaptador 2, desmarque la casilla *Habilitar adaptador de red* para deshabilitar el adaptador. Dado que estamos utilizando el servidor DHCP virtual dentro de VirtualBox, a veces crea un conflicto al conectar una sola máquina virtual a más de una red virtual con varios servidores DHCP virtuales.

Por último, asignemos la red RedTeamLab a Kali Linux. Simplemente seleccione el Adaptador 3 y use las siguientes configuraciones:

- Marque *Habilitar adaptador de red*
- Adjunto a: Red Interna
- Nombre: RedTeamLab
- Modo promiscuo: permitir todo

La siguiente captura de pantalla muestra estas configuraciones aplicadas al adaptador:



Después de configurar los ajustes en el Adaptador 3, desmarque la casilla *Habilitar adaptador de red* para deshabilitar el adaptador. Asegúrese de hacer clic en *Aceptar* para guardar la configuración de la máquina virtual.

En este punto, hemos configurado los tres adaptadores de red. Sin embargo, solo el adaptador con conectividad a Internet está conectado virtualmente a la máquina virtual

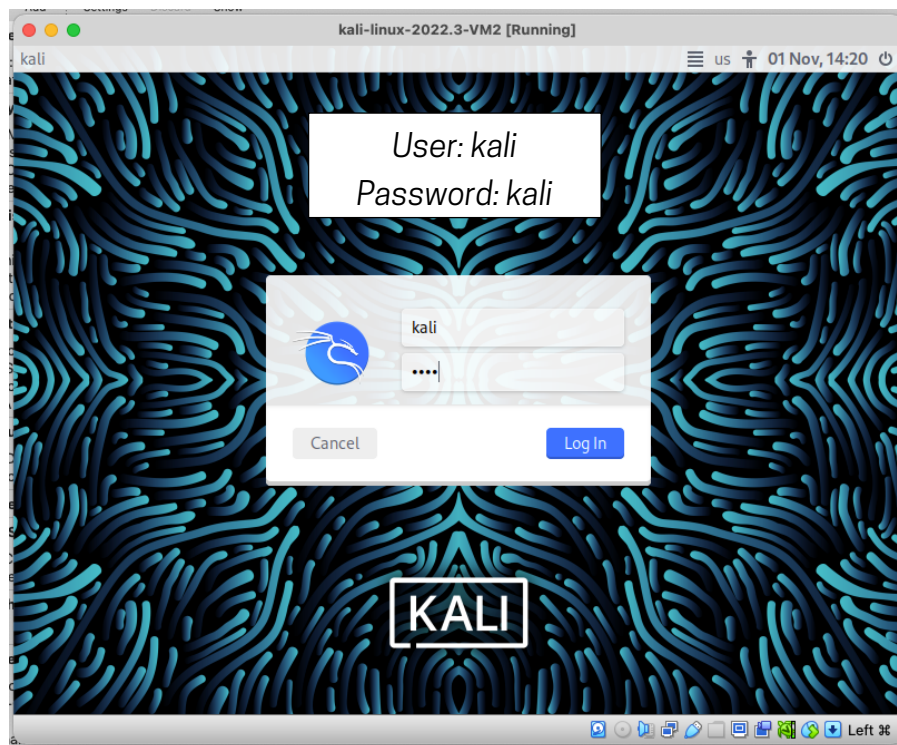


Kali Linux; los otros dos están virtualmente desconectados para prevenir futuros conflictos.

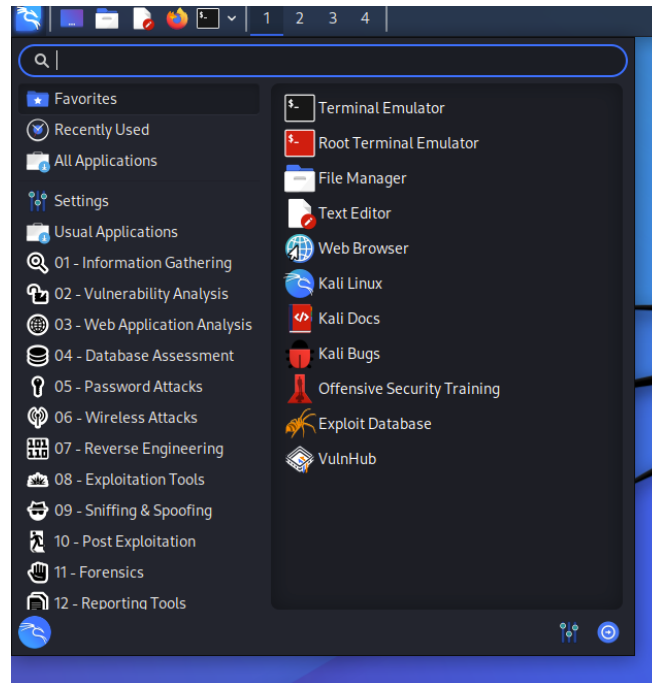
### Paso 3: Comenzar con Kali Linux

Iniciar sesión en Kali Linux puede ser muy emocionante si es la primera vez que usa un sistema basado en Linux, o incluso si simplemente sabe que Kali Linux es una de las distribuciones de pruebas de penetración más populares dentro de la industria. Los siguientes pasos lo ayudarán a comenzar con Kali Linux:

1. En la interfaz de VirtualBox Manager, seleccione su máquina virtual Kali Linux y haga clic en Iniciar para iniciar el sistema.
2. Se le presentará una solicitud de inicio de sesión. Use las credenciales predeterminadas de kali para el nombre de usuario y kali para la contraseña, como se muestra aquí:

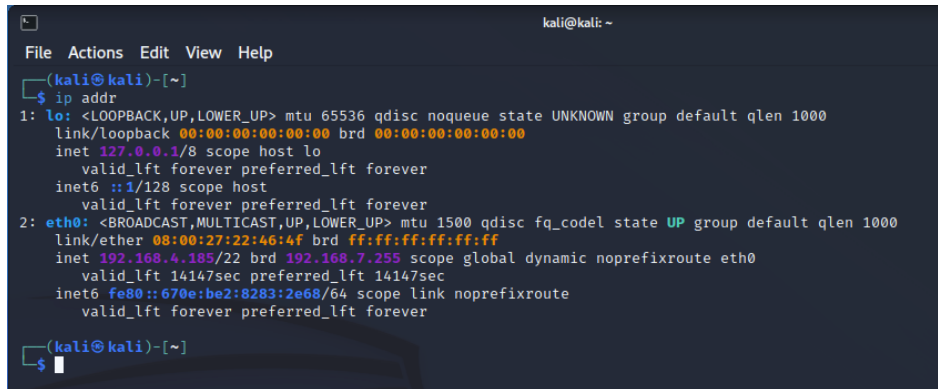


3. Una vez que haya iniciado sesión, para ver la lista de herramientas disponibles, haga clic en el ícono de Kali Linux en la esquina superior derecha, como se muestra aquí:



4. Como se muestra en la captura de pantalla anterior, todas las herramientas se clasifican según las fases secuenciales de las pruebas de penetración. Por ejemplo, todas las herramientas que se utilizan para el reconocimiento se pueden encontrar en la categoría 01 – Recopilación de información, mientras que las herramientas para descifrar contraseñas se pueden encontrar en la categoría 05 – Ataques de contraseña.
5. A lo largo de esta guía, trabajará principalmente con la terminal de Linux.

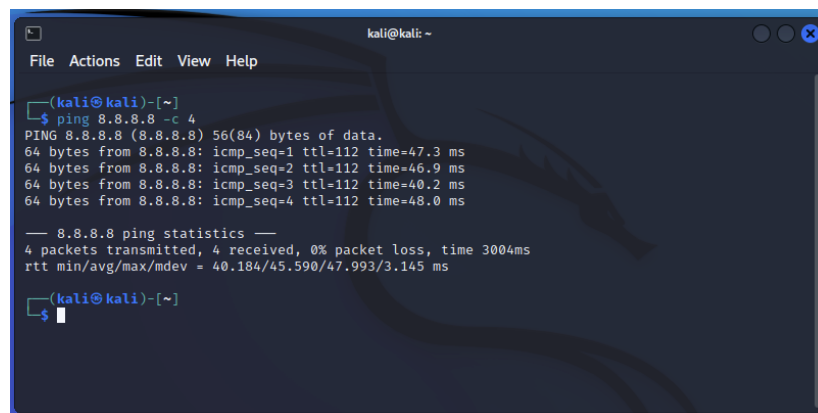
6. A continuación, determinemos si nuestra máquina virtual Kali Linux recibe una dirección IP automáticamente desde nuestra red a través del Adaptador 1 (Puente). Abra la Terminal y ejecute el comando `ip addr`, como se muestra aquí:



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ip addr  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:22:46:4f brd ff:ff:ff:ff:ff:ff  
    inet 192.168.4.185/22 brd 192.168.7.255 scope global dynamic noprefixroute eth0  
        valid_lft 14147sec preferred_lft 14147sec  
    inet6 fe80::670e:be2:8283:2e68/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
(kali@kali)-[~]  
$
```

Como se muestra en la captura de pantalla anterior, el adaptador de red se identificó como `eth0` y tiene una dirección IP de `192.168.4.185`. Tenga en cuenta que esta dirección IP se obtuvo de mi red, por lo que su dirección IP será diferente. Por lo tanto, asegúrese de conocer las direcciones IP de sus máquinas virtuales para futuras referencias.

7. Probemos la conectividad a Internet usando el comando `ping 8.8.8.8 -c 4` para enviar cuatro mensajes de ping (solicitud de eco ICMP) al servidor DNS público de Google, como se muestra aquí:



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ping 8.8.8.8 -c 4  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=112 time=47.3 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=112 time=46.9 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=112 time=40.2 ms  
64 bytes from 8.8.8.8: icmp_seq=4 ttl=112 time=48.0 ms  
— 8.8.8.8 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3004ms  
rtt min/avg/max/mdev = 40.184/45.590/47.993/3.145 ms  
(kali@kali)-[~]  
$
```

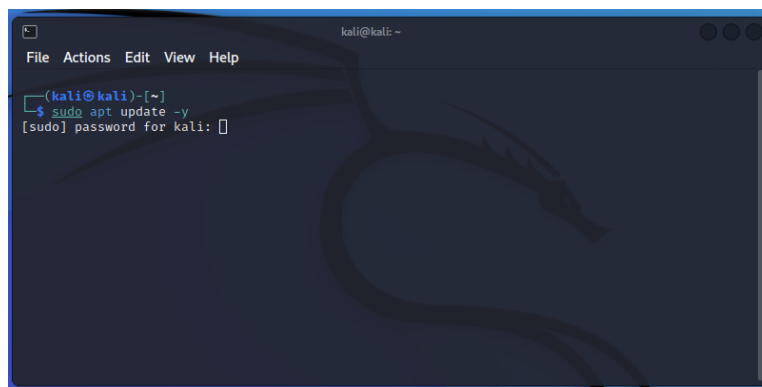
Como se muestra en el fragmento anterior, la máquina Kali Linux recibió respuestas de 8.8.8.8. Por lo tanto, el acceso a Internet está disponible en el sistema del atacante.

8. Dado que Kali Linux usa el nombre de usuario y la contraseña predeterminados de kali:kali, puede cambiar la contraseña predeterminada a algo más seguro y preferible para usted. Esto se puede hacer usando el comando `passwd kali`. Al ingresar la contraseña en Linux, es invisible por razones de seguridad.

#### Paso 4: Actualización de fuentes y paquetes

A veces, es posible que una herramienta no funcione como se esperaba, o incluso que se bloquee inesperadamente durante una prueba de penetración o una auditoría de seguridad. Los desarrolladores suelen publicar actualizaciones para sus aplicaciones. Estas actualizaciones están destinadas a corregir errores y agregar nuevas funciones a la experiencia del usuario. Aprendamos cómo actualizar fuentes y paquetes siguiendo estos pasos:

1. Para actualizar los paquetes de software en Kali Linux, necesitamos volver a sincronizar los archivos de índice del paquete con sus fuentes usando el comando `sudo apt update -y`, como se muestra aquí:



```
kali@kali ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo apt update -y  
[sudo] password for kali: 
```

2. A continuación, para actualizar los paquetes existentes (aplicaciones) en Kali Linux a sus últimas versiones, use el comando `sudo apt-get upgrade -y` o `sudo apt upgrade -y`, si es la primera vez que ejecuta este comando puede tardar varios minutos dependiendo de la velocidad de conexión a internet de su computador.
3. Si, durante el proceso de actualización, recibe un error acerca de que Kali Linux no puede realizar la actualización, use el comando `sudo apt-get update --fix-missing` seguido de `sudo apt upgrade -y` una vez más.

Una vez completada esta sección, ha aprendido cómo configurar Kali Linux como una máquina virtual, habilitar Internet y otras conexiones de red para la máquina virtual y actualizar la lista de fuentes del repositorio de paquetes. A continuación, aprenderá cómo agregar clientes vulnerables a su laboratorio de pruebas de penetración.

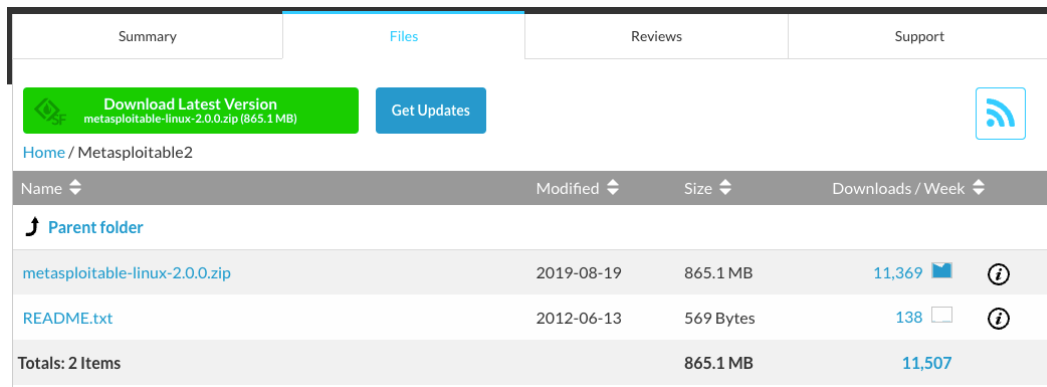
### Implementación de Metasploitable 2 como sistema de destino

Al construir un laboratorio de pruebas de penetración, es importante incluir sistemas vulnerables que actuarán como nuestros objetivos. Estos sistemas contienen servicios y aplicaciones vulnerables intencionales para que podamos practicar y desarrollar nuestras habilidades para comprender cómo descubrir y explotar vulnerabilidades. Una máquina vulnerable muy popular se conoce como Metasploitable 2. Esta máquina vulnerable contiene muchas vulnerabilidades que pueden explotarse y es buena para aprender sobre las pruebas de penetración.

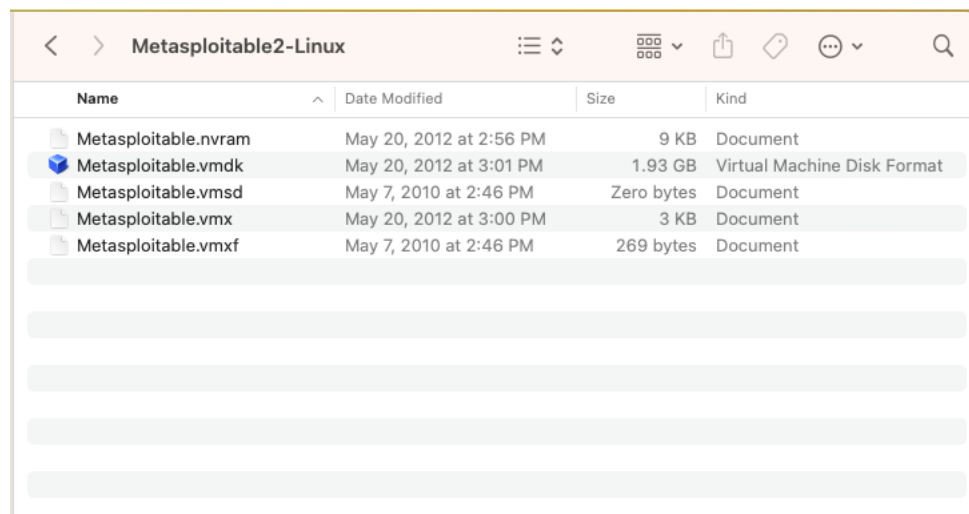
## Parte 1: Implementación de Metasploitable 2

Los siguientes pasos lo ayudarán a adquirir máquinas virtuales vulnerables Metasploitable 2 para que pueda implementarlas dentro del hipervisor:

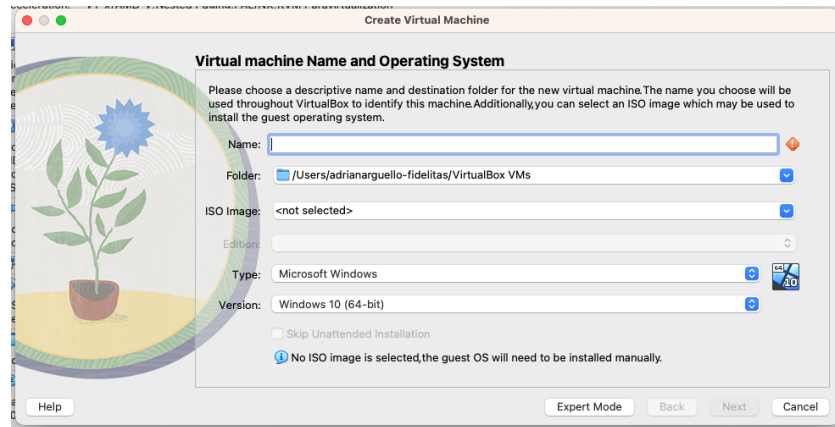
1. Vaya a <https://sourceforge.net/projects/metasploitable/files/Metasploitable2/> y descargue el archivo metasploitable-linux-2.0.0.zip en su sistema host.



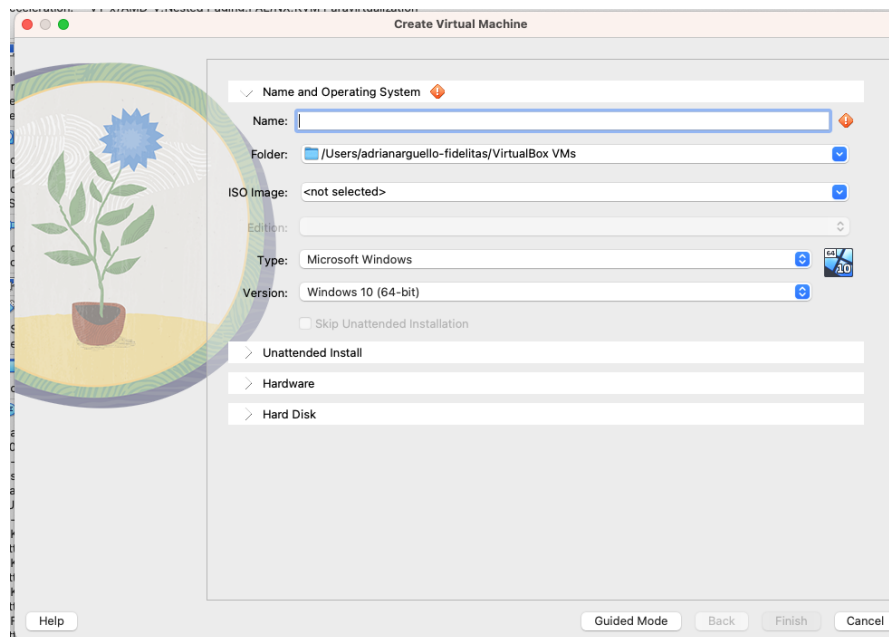
2. Una vez que se haya descargado el archivo ZIP, extraiga (descomprima) su contenido en la ubicación donde residen sus otras máquinas virtuales. Los archivos extraídos son los archivos del disco duro virtual para Metasploitable 2.



3. A continuación, creemos un entorno virtual para implementar la máquina virtual Metasploitable 2. Abra *VirtualBox Manager* y haga clic en *Nuevo*.



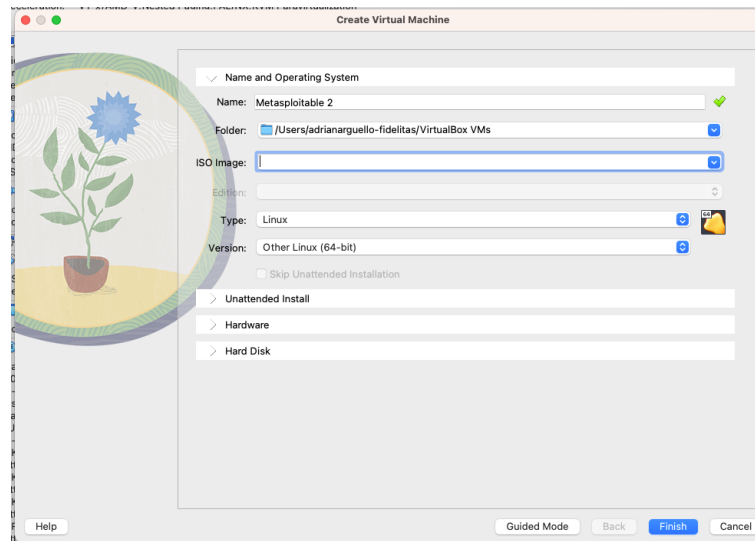
4. Cuando se abra la ventana *Crear máquina virtual*, haga clic en *Modo experto* para cambiar la vista de configuración.



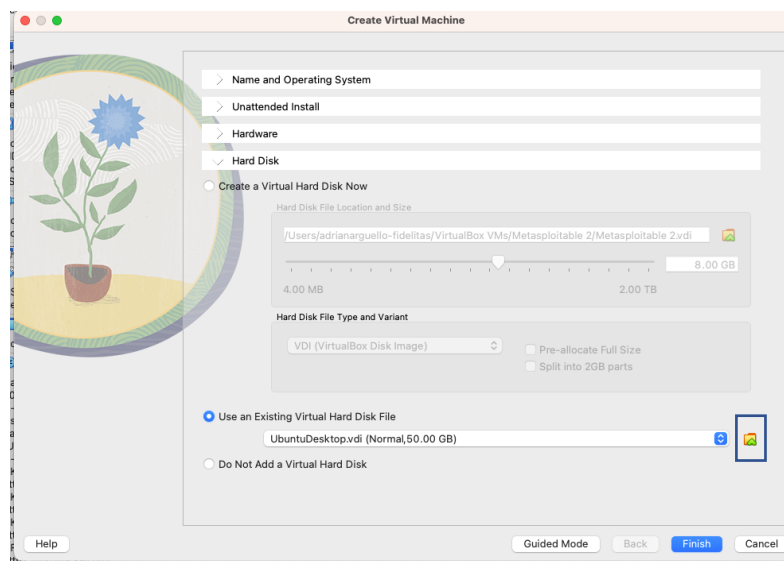
5. A continuación, utilice los siguientes parámetros para crear el entorno virtual:
- a. Nombre: Metasploitable 2



- b. Tipo: Linux
- c. Versión: Otro Linux (64 bits)
- d. Tamaño de la memoria: 512 MB

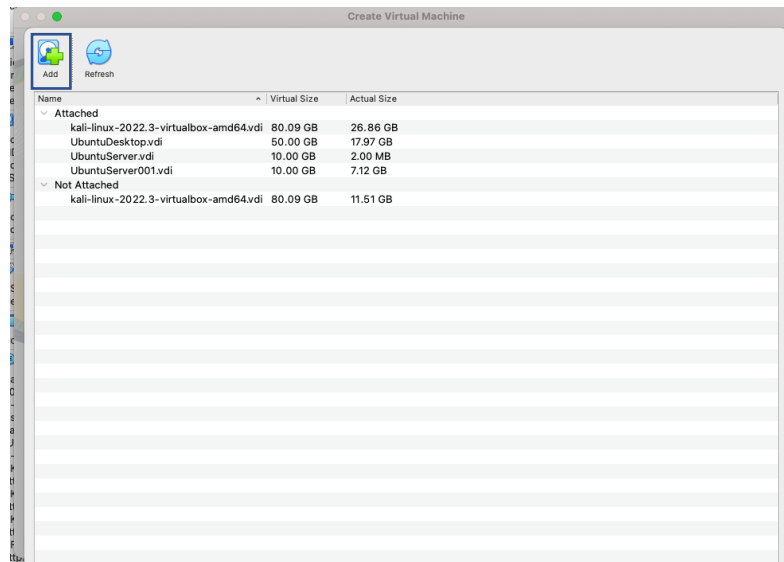


6. En la misma ventana Crear máquina virtual, cambie la opción Disco Duro a Usar un archivo de disco duro virtual existente y haga clic en el ícono de la carpeta en el lado derecho para abrir el Selector de disco duro, como se muestra aquí:

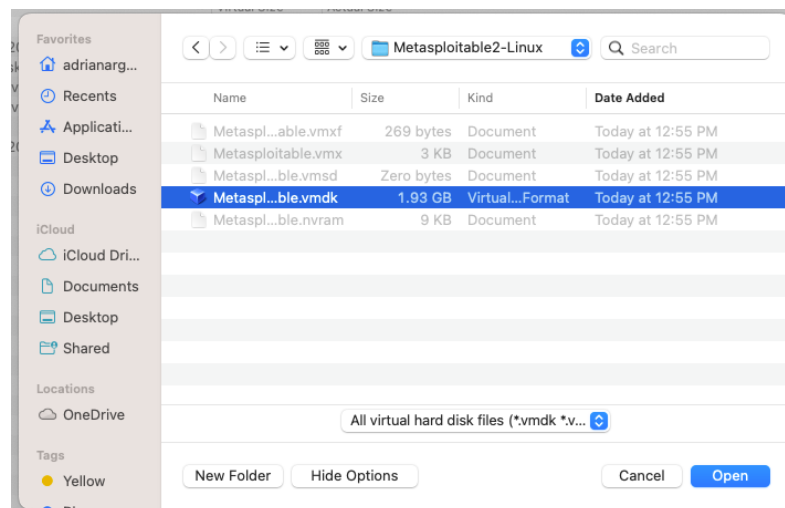




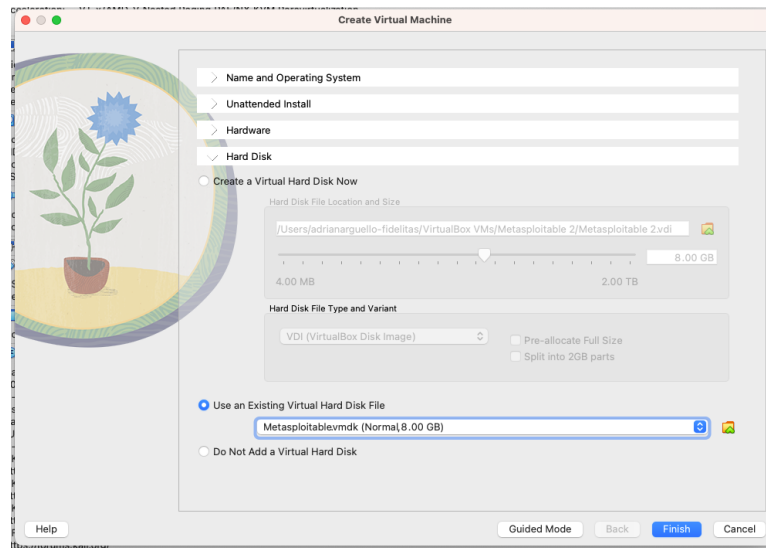
7. A continuación, haga clic en **Agregar** y navegue hasta la ubicación de los archivos extraídos del Paso 2. Seleccione el archivo del disco duro virtual llamado **Metasploitable** y haga clic en **Abrir**.



8. A continuación, seleccione el archivo **Metasploitable.vmdk** y haga clic en **Elegir**, como se muestra aquí:



9. Ahora, volverá a la ventana Crear máquina virtual con el disco duro virtual conectado; simplemente haga clic en Finalizar.

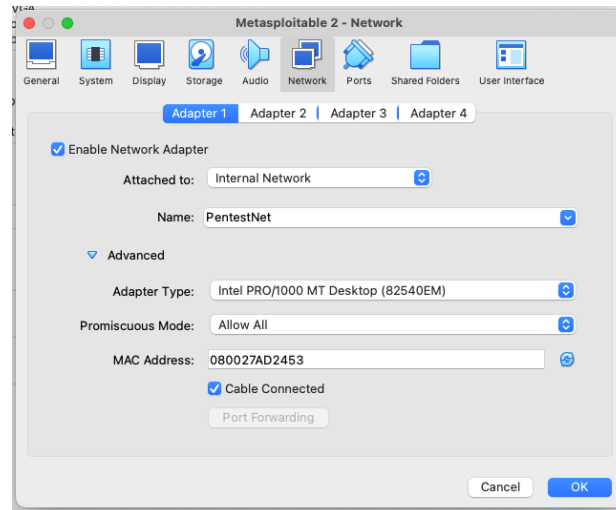


## Parte 2: Configurar los ajustes de red

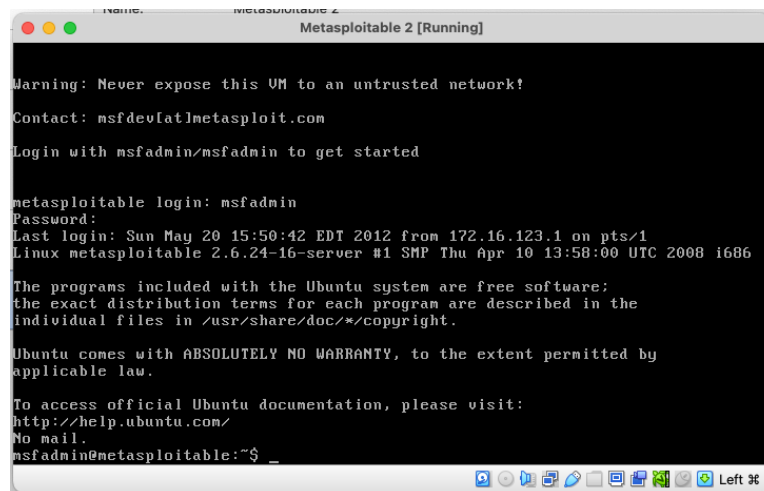
Dado que nuestra topología de laboratorio de pruebas de penetración contiene más de una red virtual, los siguientes pasos ayudarán a garantizar que la máquina virtual Kali Linux tenga conectividad de red de extremo a extremo con Metasploitable 2:

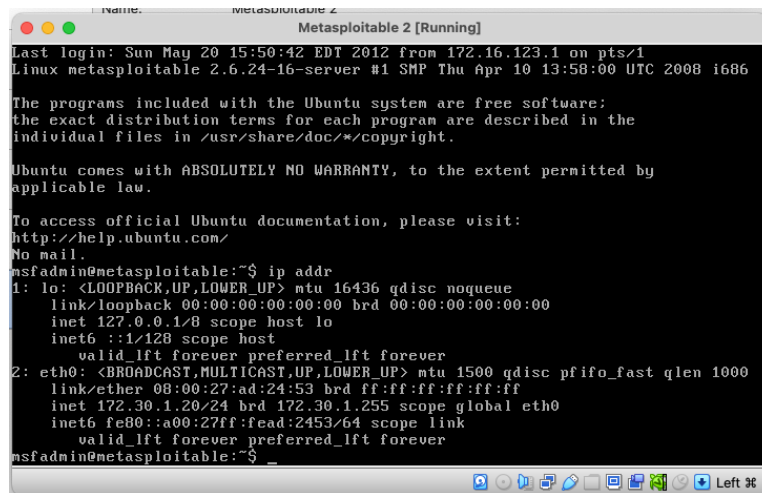
1. Para configurar los ajustes de red, seleccione la nueva máquina virtual Metasploitable 2 dentro de VirtualBox Manager y haga clic en Configuración.
2. Vaya a la sección Red, habilite el Adaptador 1 y use los siguientes parámetros para configurar el Adaptador 1 para que forme parte de la red PentestNet de nuestro laboratorio:
  - a. Adjunto a: Red Interna
  - b. Nombre: PentestNet
  - c. Modo promiscuo: permitir todo

La siguiente captura de pantalla muestra los ajustes de configuración en el adaptador de red virtual:



3. A continuación, encienda la máquina virtual Metasploitable 2 e inicie sesión en Metasploitable 2 proporcionando `msfadmin` como nombre de usuario y contraseña. Use el comando `ip addr` para verificar que la máquina virtual esté recibiendo una dirección IP en la red 172.30.1.0/24, como se muestra aquí:





```
Metasploitable 2 [Running]
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:~$ 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:ad:24:53 brd ff:ff:ff:ff:ff:ff
    inet 172.30.1.20/24 brd 172.30.1.255 scope global eth0
    inet6 fe80:a00:27ff:fead:2453/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

4. Por último, cuando haya terminado de usar Metasploitable 2, use el comando `sudo halt` para apagar la máquina virtual.