

Taller de Seguridad Informática

TA051

Setting Up ambiente de trabajo

Gallino, Pedro	107587
Pol, Manuel	108448
Velazquez, Joaquín	105980
Martinez, Francisco	108460
Lazcano, Luca	107044

Docente:

Profesor: Mariano Mendez

16 de Abril de 2025

Setting Up

En esta guía se detalla la creación de un laboratorio virtual orientado al hacking ético, utilizando máquinas virtuales y redes simuladas que replican entornos reales de forma segura. Este entorno controlado te permitirá experimentar y poner en práctica técnicas de ataque y defensa sin comprometer sistemas reales ni vulnerar ningún marco legal.

Máquinas virtuales a utilizar

- **pfSense:** Actuará como firewall y router del laboratorio, asegurando que las máquinas vulnerables queden protegidas de accesos no autorizados desde el exterior.
- **Kali Linux:** Será la máquina de ataque principal, equipada con herramientas especializadas para realizar pruebas de penetración y técnicas de hacking ético.
- **Metasploitable:** Un servidor Linux intencionadamente vulnerable, ideal para practicar exploits, escaneos y ataques a nivel de servidor.
- **Ubuntu Desktop (x2):** Dos estaciones de trabajo que simulan entornos de escritorio reales, pensadas para ensayar técnicas contra equipos de usuarios finales (phishing, acceso remoto, etc.).

Networks

- **Red interna principal (Main Internal Network):**

Es la red donde están conectadas las máquinas virtuales: **Kali**, **pfSense**, **Metasploitable**, **Ubuntu**.

Está aislada de internet gracias a pfSense, que actúa como un firewall/router.

- **Red privada (Private Network):**

Es una red interna dentro de la red interna. Está aislada incluso del resto del laboratorio y protegida detrás de la máquina **Metasploitable**.

Simula escenarios reales donde un hacker tiene que comprometer una máquina (**pivoting**) para llegar a otra.

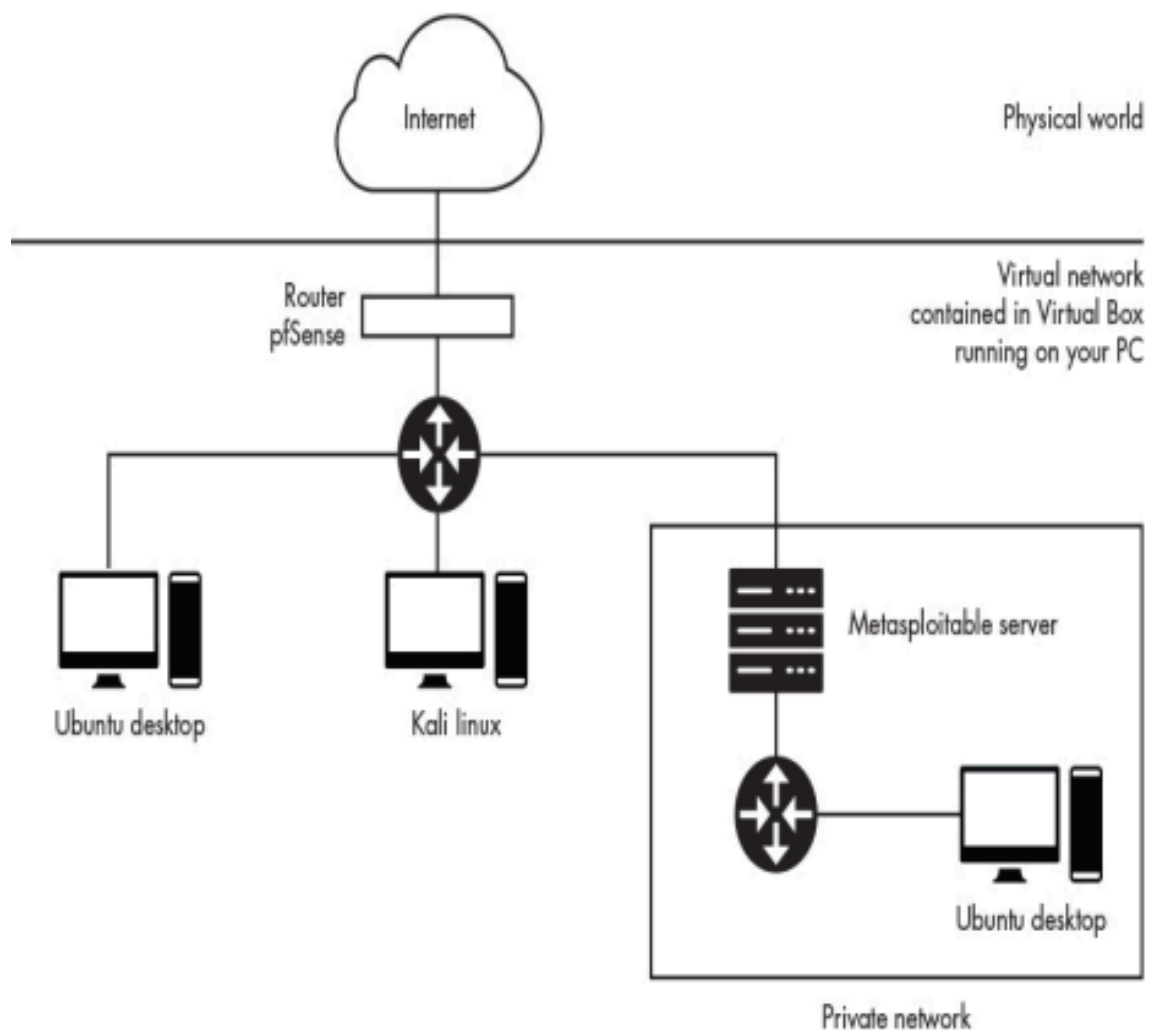


Figura 1: Overview el ambiente del laboratorio

Requisitos mínimos

- PC con **4 GB RAM** mínimo (recomendable 8 GB o más).
- Al menos **30 GB** de espacio libre (Hard drive).
- Sistema operativo: Windows / **Linux** / macOS.

Van a estar corriendo múltiples máquinas virtuales en simultáneo, por lo que será necesario tener una máquina potente.

De todas maneras, en este primer acercamiento aún no setearemos las máquinas ubuntu.

Setting Up VirtualBox

Para configurar el entorno de red y crear las máquinas virtuales, es necesario instalar **VirtualBox**, un software de virtualización que permite construir y administrar computadoras virtuales.

Permite crear máquinas virtuales personalizadas, definiendo recursos como:

- Capacidad del disco duro
- Memoria RAM
- Número de procesadores

Se puede descargar desde: <https://www.virtualbox.org/wiki/Downloads>

Una vez descargado, basta con ejecutarlo y seguir los pasos del asistente. El proceso de instalación puede variar levemente según el sistema operativo (Windows, macOS o Linux), pero en la mayoría de los casos es suficiente con aceptar las opciones predeterminadas.

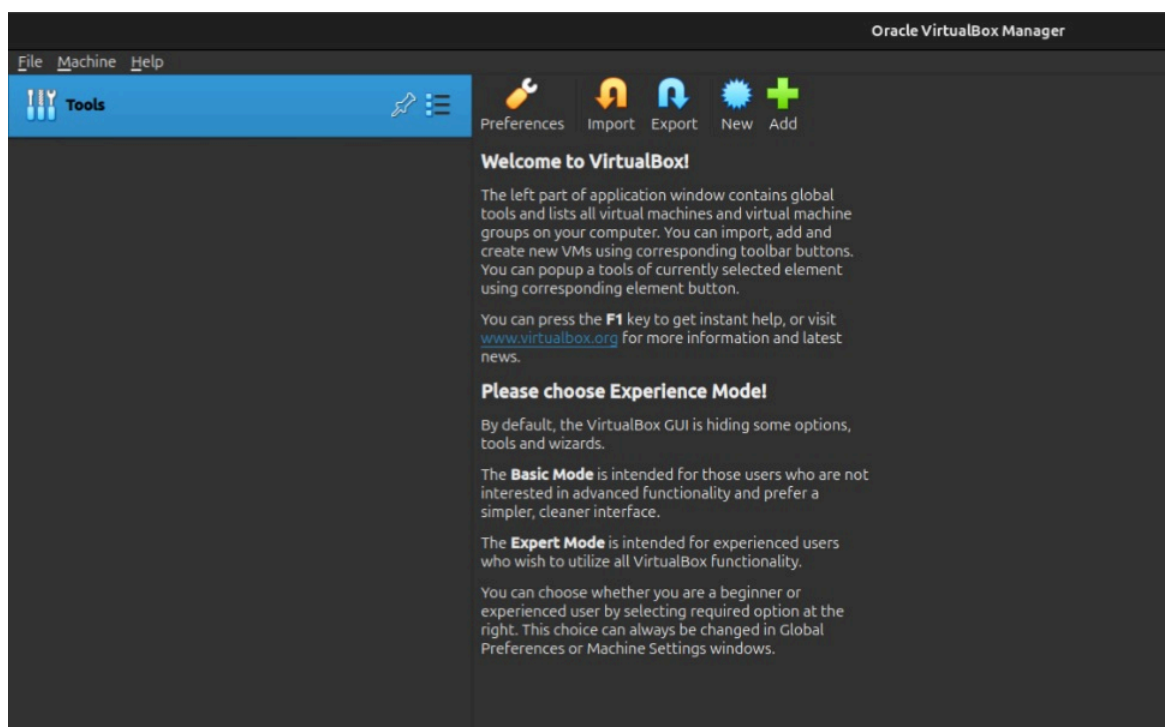


Figura 2: Pantalla inicial VirtualBox

Setting Up pfSense

El siguiente paso es configurar **pfSense**, un router/firewall de código abierto que va a funcionar como la primera línea de defensa dentro del laboratorio virtual. Su función será proteger a las máquinas virtuales del entorno ante posibles accesos o ataques externos no autorizados.

Para comenzar, es necesario descargar los archivos de instalación desde el sitio oficial: <https://www.pfsense.org/download/>

En la sección de descargas, hay que elegir el método de instalación **Netgate Installer**. Para poder acceder, se requiere crear una cuenta gratuita en el sitio.

Una vez dentro, seleccionar la opción: **AMD64 ISO - IPMI / Virtual Machines**, que es la versión recomendada para usar en entornos virtualizados como VirtualBox.



NETGATE INSTALLER

\$0⁰⁰

Shipping calculated at checkout.

Pay over time for orders over \$ 35,00 with [shop Pay](#) [Learn more](#)

Customers using Shop Pay Installments might experience a 1-2 day delay in order processing.

Installation Image

SELECT IMAGE TYPE


SELECT IMAGE TYPE

AMD64 Memstick USB (Netgate 1537, 1541, 4100, 4200, 5100, 6100, 7100, 8200, All Other Intel/AMD 64-bit)

AMD64 ISO IPMI/Virtual Machines

AARCH64 Memstick ARM (Netgate 1100 and 2100)

Select an Image Type

 ADD TO CART


 FIND A PARTNER

Figura 3: Opción de instalación de pfSense en Netgate installer.

Una vez completada la compra (gratuita), se podrá instalar el archivo de instalación.

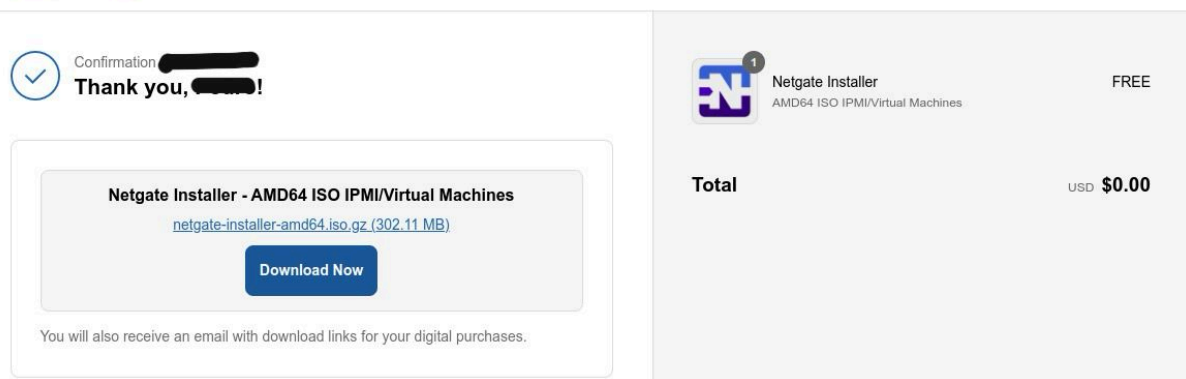


Figura 4: Pantalla de descarga post compra del instalador de pfSense.

Para descomprimir el archivo **iso.gz** en una máquina basada en Unix, se puede utilizar el siguiente comando en la terminal: `gunzip <nombre del archivo>`

```
gunzip netgate-installer-amd64.iso.gz
```

Una vez descomprimido el archivo, abrí **VirtualBox** y hacé click en el botón **New** para crear una nueva máquina virtual.

Allí, completar los siguientes campos:

- **Name:** PFSense.
- **Type:** BSD.
- **SubType:** FreeBSD.
- **Version:** FreeBSD (64-bit).

Además, en **ISO Image**, debes seleccionar el archivo .iso previamente descargado

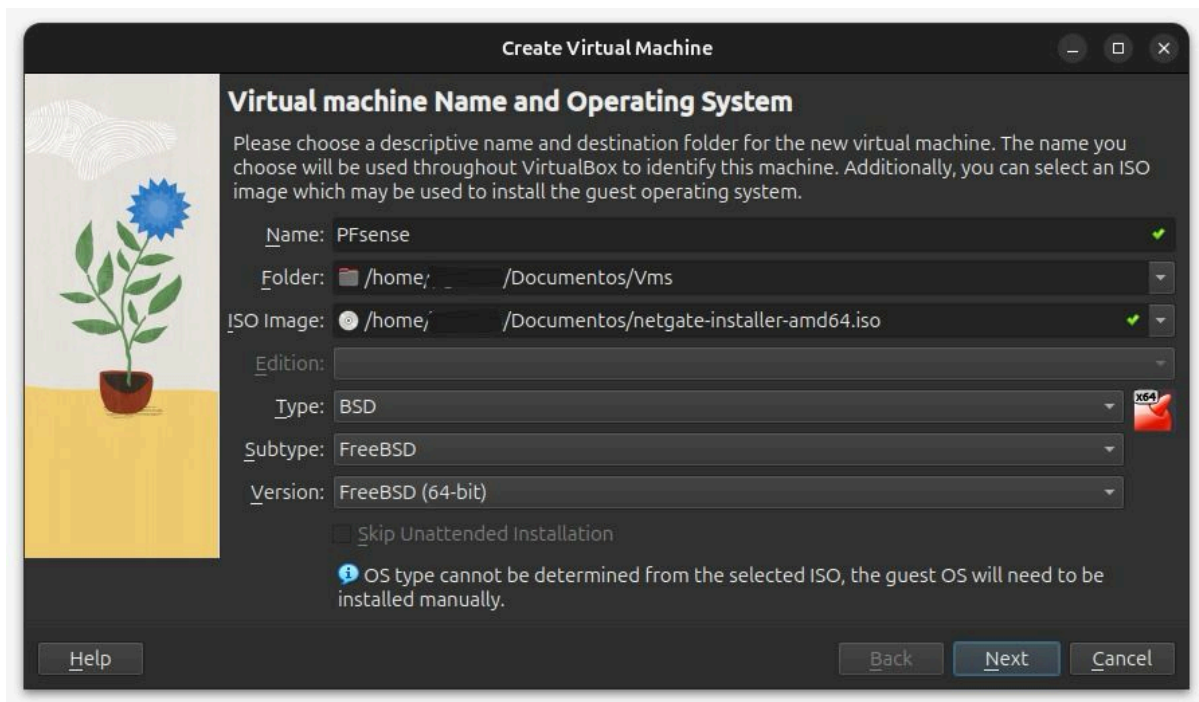


Figura 5: Creación de PFSense Virtual Machine.

Luego, cuando se te solicite configurar la memoria, asigna **1024MB** de RAM, ya que **pfSense** no requiere mucha memoria.

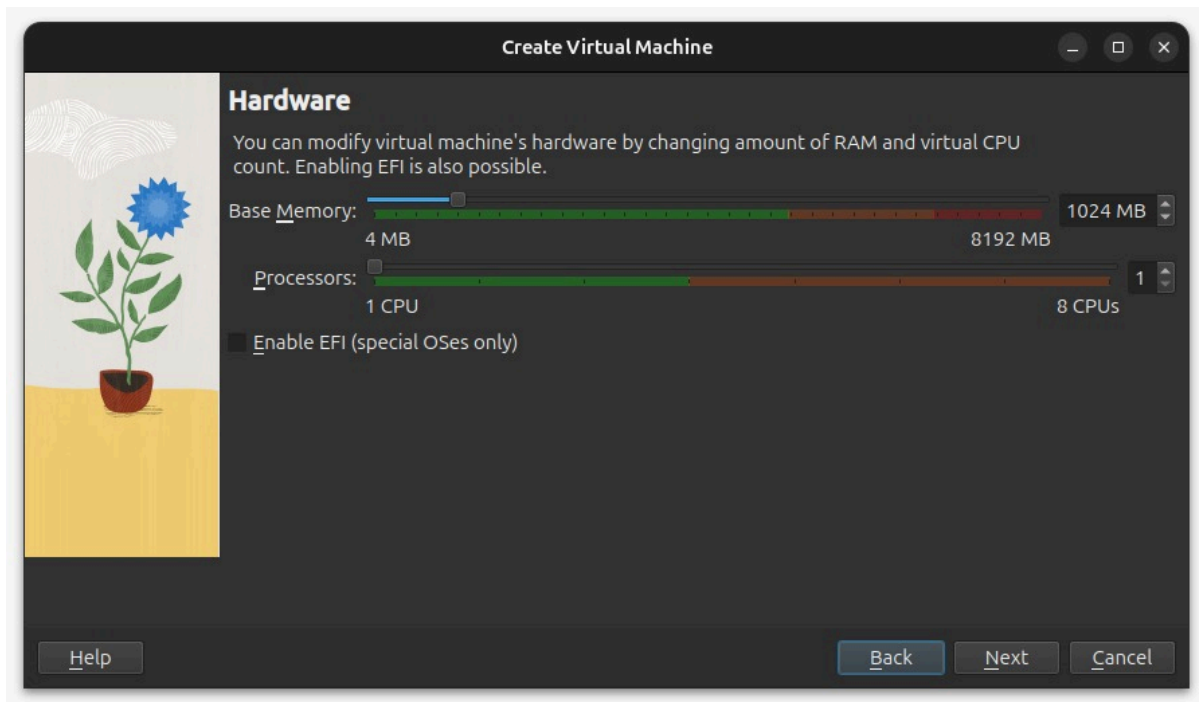


Figura 6: Selección de Base Memory y Processors para PFSense.

Cuando llegues a las opciones del disco duro virtual, selecciona **Create a virtual hard disk now**.

Para el tipo de archivo de disco, elige **VDI (VirtualBox Disk Image)** y establece su tamaño en **5GB**.

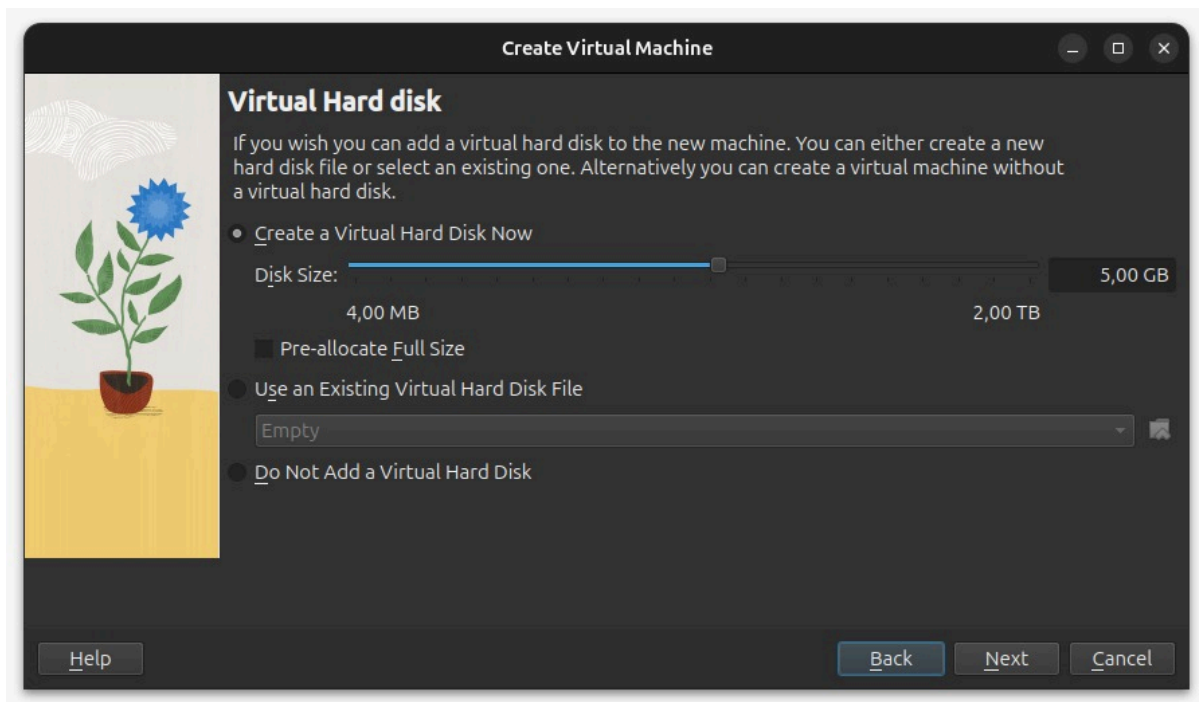


Figura 7: Creación de Virtual Hard Disk para pfSense.

Configuración de Red

pfSense puede considerarse como un "portero digital" o "gatekeeper" entre la red interna de tu laboratorio y el resto del mundo. Su función principal es:

- **Inspeccionar** todo el tráfico que entra y sale de la red virtual.
- **Bloquear** accesos no deseados desde el exterior, funcionando como una barrera de seguridad.
- **Permitir practicar ataques** sin poner en riesgo la computadora real ni conectarse a internet de manera insegura.

Una vez configurada la máquina virtual en **VirtualBox**, seguí estos pasos:

1. En el panel de inicio de **VirtualBox**, haz clic derecho sobre la máquina virtual de **pfSense** y selecciona **Settings**.
2. Dentro de la configuración, ve a la sección de **Network**. Asegúrate de activar el **modo Expert** para tener acceso a configuraciones avanzadas.
3. Verifica que el **Adaptador 1 (Adapter 1)** esté habilitado y configurado como **Adaptador en Puente (Bridged Adapter)**. Asegurate de que se esté usando el mismo nombre que tu placa de red inalámbrica o por cable.

Habilitar un **Bridged Adapter** crea una conexión directa entre la máquina virtual de **pfSense** y la red de internet, permitiéndole actuar como un firewall entre la red interna y el mundo exterior.

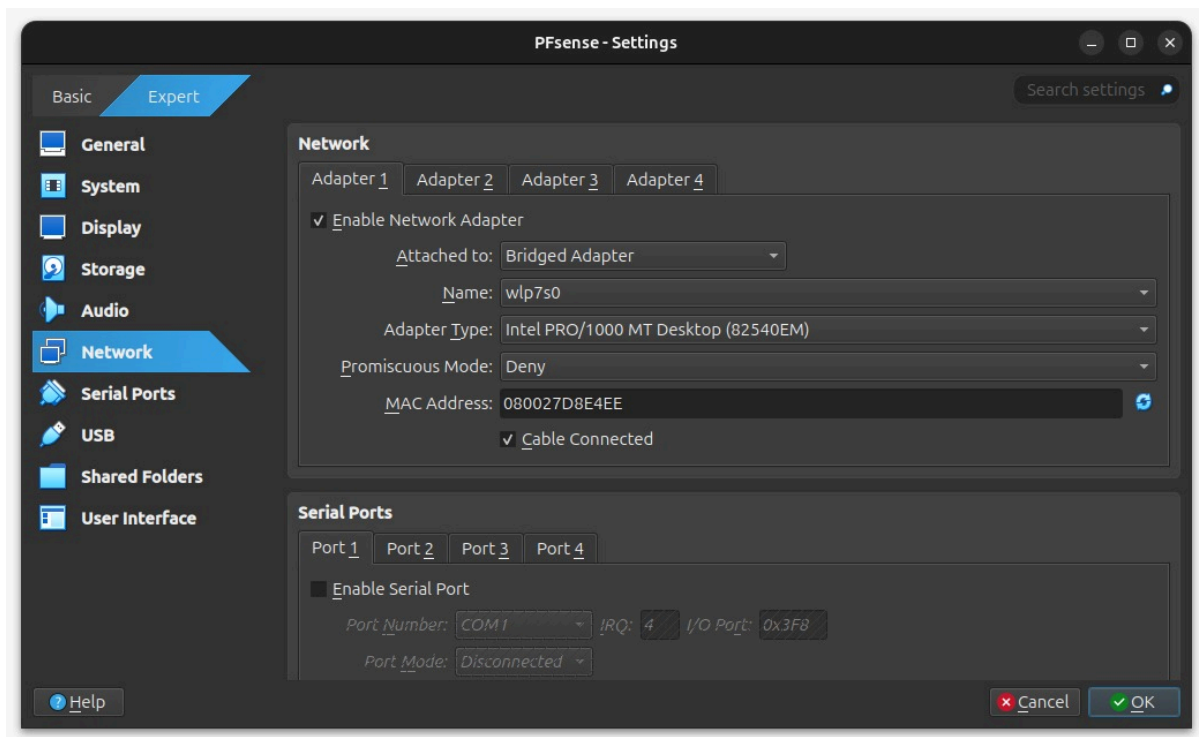


Figura 8: Network settings – adapter 1 (PFsense)

Luego, hacé click en la pestaña **Adaptador 2 (Adapter 2)** y activá la opción **Enable Network Adapter**.

Configurá este adaptador como **Red Interna (Internal Network)** y poné el nombre **Internal LAN**. Esta red interna conectará **pfSense** con las demás máquinas virtuales del laboratorio, permitiendo la comunicación entre ellas de forma aislada del exterior.

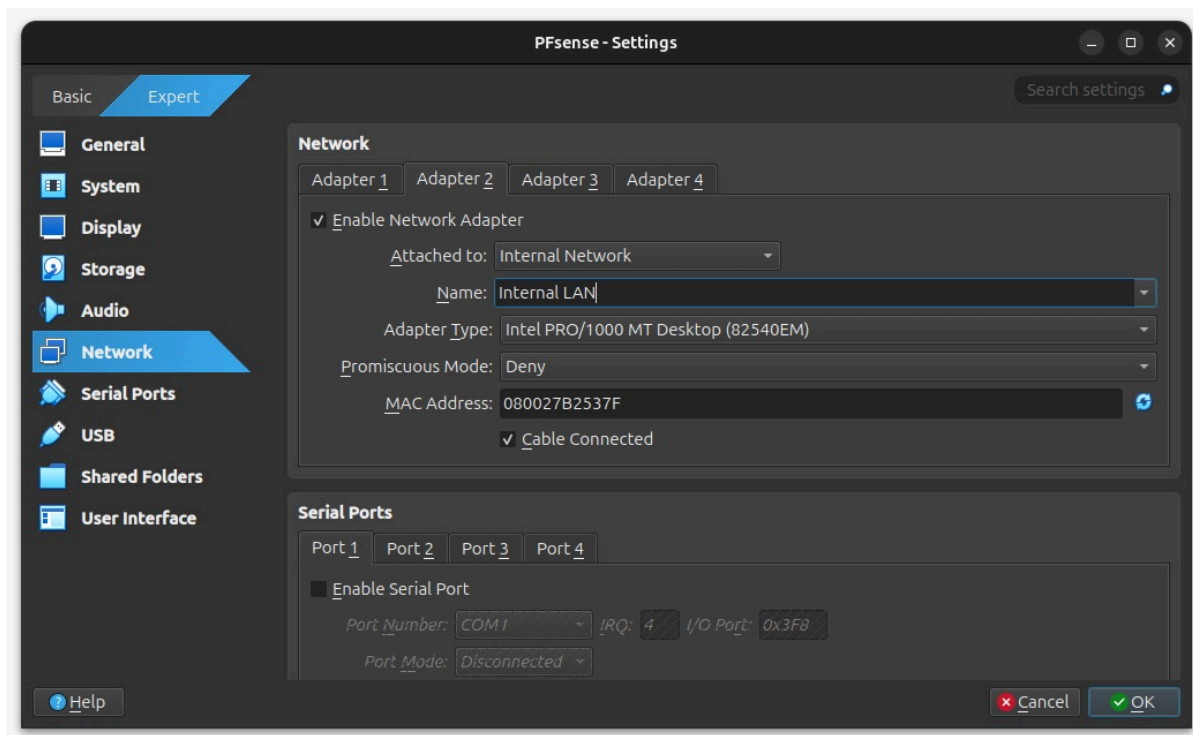


Figura 9: Network settings – adapter 2 (PFsense)

Configuración de Router pfSense

En este punto, podés iniciar la máquina virtual de **pfSense** para comenzar con la configuración del router virtual.

Es importante tener en cuenta que una configuración incorrecta podría hacer que las demás máquinas virtuales pierdan el acceso a internet.

Para continuar, hacé doble click sobre **pfSense** en la lista de máquinas virtuales. Esto iniciará tanto la máquina virtual como el proceso de instalación de **pfSense**.

Seleccionar interfaces:

- Para **WAN**, seleccioná **em0** (interfaz de red externa).
- Para **LAN**, seleccioná **em1** (interfaz de red interna).

Seleccioná las opciones por defecto en este paso.

Instalar pfSense CE:

- Elegí la opción **Install CE** para instalar la versión gratuita de **pfSense**.

Seleccionar el sistema de archivos:

- Dejá las opciones por defecto seleccionadas.

Seleccionar la versión de pfSense:

- Seleccioná la opción **Current Stable Release** para instalar la versión más reciente y estable.

Realizar la instalación:

- Seguí con el proceso de instalación y, al finalizar, seleccioná **Reboot** para reiniciar pfSense.

Apagar la máquina virtual:

- Una vez que **pfSense** haya reiniciado, hacé clic en **File (Archivo)** en la parte superior izquierda y seleccioná **Close (Cerrar)**.
- Luego, elegí **Power off the machine (Apagar la máquina)**.

Quitar la ISO:

- Hacé clic derecho sobre la máquina virtual de **pfSense** en la lista de **VirtualBox** y seleccioná **Settings (Configuración)**.
- En la pestaña **Storage (Almacenamiento)**, hacé clic derecho sobre la ISO y seleccioná **Remove Attachment (Eliminar adjunto)**.
- Finalmente, doble click sobre la máquina virtual de **pfSense** para iniciarla.

Setting Up Metasploitable

La máquina virtual **Metasploitable** es un servidor Linux diseñado intencionalmente con vulnerabilidades, ideal para realizar pruebas de hacking ético dentro del laboratorio. Sin embargo, es importante asegurarse de que **Metasploitable** esté protegida y no sea accesible desde fuera del laboratorio. Para esto, se debe conectar a la red interna, que está protegida por el firewall **pfSense**.

Descargar Metasploitable:

- Descargar **Metasploitable** desde SourceForge: [SourceForge](#).

(Puede tardar mucho horas, podés obtenerlo rápido desde el repositorio del tutorial)

Descomprimir el archivo ZIP:

- Descomprimir el archivo ZIP descargado de Metasploitable.

Crear máquina virtual:

- Deberás crear la máquina virtual siguiendo el mismo proceso que usaste con **pfSense**.
 - **Name:** Metasploitable.
 - **Type:** Linux.
 - **Version:** Ubuntu (64-bit).
- Al seleccionar un disco duro, elegir **Usar un archivo de disco duro virtual existente**.

cliqueá en el ícono de la carpeta, navegá hasta donde descomprimiste **Metasploitable** y seleccioná el archivo con extensión **.vmdk**.

Configuración de la Red:

- Hacé clic derecho sobre la máquina **Metasploitable** en la lista de máquinas virtuales y seleccioná Configuración.
- En la sección **network**:

En **Adaptador 1 (Adapter 1)**, seleccioná la casilla habilitar **adaptador de red (network adapter)**

En el menú desplegable **Conectado a (attached to)**, elegí la red interna que creaste previamente (**Internal LAN**)

Finalmente abrí la máquina virtual de Metasploitable en VirtualBox y esperé a que termine de cargar la terminal. Deberías ver el logo de Metasploitable en pantalla, lo que indica que el sistema arrancó correctamente.

Una vez cargado el sistema, inicié sesión con usuario y contraseña : **msfadmin**.

Setting Up Kali Linux

Kali Linux es una distribución de **Linux** especialmente diseñada para pruebas de penetración, ya que viene equipada con un amplio conjunto de herramientas para hacking ético. En este laboratorio, vamos a usar la **máquina virtual** de **Kali** para realizar ataques controlados sobre el resto de las máquinas del entorno virtual.

Descargar Kali Linux:

- Descargá la imagen para VirtualBox desde el sitio oficial de Offensive Security:
<https://www.kali.org/get-kali/#kali-virtual-machines>
- Asegurate de elegir los archivos correspondientes a **VirtualBox** y **no los de VMware**. También verificá que coincida con la arquitectura de tu sistema (64-bit o 32-bit).

Descompresión:

- Extraé el archivo **.7z** descargado. Vas a encontrar dos archivos: uno **.vbox** y otro **.vdi**.

Importación en VirtualBox:

- En **VirtualBox**, click en **Agregar (Add)** y seleccioná el archivo **.vbox**.

Verificación de almacenamiento:

- Entrá a **Configuración (Settings)** → pestaña **Almacenamiento (Storage)**. Verificá que el archivo **.vdi** esté correctamente enlazado al controlador **SATA**. Si no, hacé clic derecho → **Eliminar adjunto (Remove Attachment)** y volvé a agregarlo con **Elegir disco existente (Choose Existing Disk)**.

Configuración de la Red:

- Hacé clic derecho sobre la máquina **Kali** en la lista de máquinas virtuales y seleccioná **Configuración (settings)**.
- En la sección **network**:

En **Adaptador 1 (Adapter 1)**, seleccioná la casilla habilitar **adaptador de red (network adapter)**

En el menú desplegable **Conectado a (attached to)**, elegí la red interna que creaste previamente (**Internal LAN**)

Procesador:

- En **Configuración (Settings)** → **Sistema (System)** → **Procesador (Processor)**:
Activá la opción **PAE/NX** si no está activada.

Inicio y login:

- Inicia la máquina haciendo doble click sobre la VM en la lista. Cuando aparezca la pantalla de login, usá usuario y contraseña: **kali**

Primer Hack

Ahora que ya tenés todo configurado, vamos a probar la infraestructura de la red virtual ejecutando un ataque. El objetivo es acceder a la máquina Metasploitable explotando una vulnerabilidad llamada **backdoor**. Un **backdoor** es una falla intencional que le da acceso no autorizado a un atacante.

En julio de 2011, la comunidad de seguridad descubrió que un atacante había insertado un backdoor en el código de la versión 2.3.4 de vsftpd, un servidor FTP de código abierto para UNIX. Este backdoor permite que el atacante acceda al terminal de la máquina vulnerable.

Lo único que tiene que hacer el atacante es iniciar sesión en el servidor FTP con un nombre de usuario que termine en :) y una contraseña inválida. Una vez activado el ataque, se abre un shell en el puerto 6200. El shell es un programa que conecta la máquina del atacante con la máquina comprometida, permitiéndole ejecutar comandos en el terminal.

Poné a correr **pfSense**, **Metasploitable** y **Kali** en **VirtualBox**.

Paso 1: Obtener la dirección IP de Metasploitable

El primer paso en la mayoría de los ataques es identificar la máquina a la que nos queremos conectar. Cada máquina tiene una **dirección IP única**. Para obtener la IP de **Metasploitable**, usaremos la herramienta **netdiscover**.

- Abrió el terminal en Kali Linux y ejecuta el comando: netdiscover (Si el terminal te dice que el comando no se encuentra o necesitas ser root, ejecuta: sudo netdiscover)
- **Netdiscover** buscará las direcciones IP en tu red y te mostrará las máquinas conectadas. En unos minutos, deberías ver la dirección IP de **Metasploitable**.

Ejemplo de salida:

```
IP At MAC Address      Count Len  MAC Vendor / Hostname
-----
192.168.1.1 08:00:27:3b:8f:ed  1 60 PCS Systemtechnik GmbH
192.168.1.101 08:00:27:fe:31:e6  1 60 PCS Systemtechnik GmbH
```

La **primera IP** es **pfSense** (tu firewall) y la **segunda IP** es **Metasploitable**.

Paso 2: Conectar al servidor FTP y activar el backdoor

Una vez que tengas la IP de **Metasploitable**, vamos a explotar el **backdoor** usando **Netcat (nc)**, una herramienta de línea de comandos que permite abrir un **socket TCP** en el puerto del servidor.

- En el terminal de **Kali Linux**, conectate al servidor FTP en **Metasploitable** usando este comando:

```
nc <IP_de_Metasploitable> 21
```

Usuario: Hacker:)

Contraseña: invalid

El valor al final del primer comando es el **número de puerto**. Los servidores **FTP** normalmente funcionan en el **puerto 21**.

- Ahora que activaste el **shell** asociado con el **backdoor**, abrí una **nueva ventana de terminal** e ingresá el siguiente comando para conectarte al shell que debería estar corriendo en el **puerto 6200** de la máquina **Metasploitable**:

```
nc -v <IP_de_Metasploitable> 6200
```

Una vez que te conectes, parecerá que la terminal no responde. Pero no es así, solo está esperando que escribas algo. Ingresá el comando **ls** para listar todos los archivos en el directorio actual.

Ahora deberías poder ingresar comandos en tu terminal de **Kali Linux** y hacer que se ejecuten como si los hubieras escrito en la terminal de la máquina **Metasploitable**. Por ejemplo, usa el shell para reiniciar la máquina ejecutando los siguientes comandos en la terminal de Kali y luego observa lo que sucede en la máquina **Metasploitable**:

```
whoami
```

```
reboot
```

Si el ataque se ejecuta correctamente, la máquina **Metasploitable** se reiniciará. Aunque reiniciar la máquina no parezca tan peligroso, un atacante con privilegios de **root** podría hacer muchas más cosas; por ejemplo, eliminar todos los datos del servidor.

Video ejemplo: [Ejemplo Backdoor introductorio](#)

Archivos Utilizados

En el siguiente link se adjuntan los zips utilizados durante el setting up.

Durante el proceso, descargar metasploitable desde el link original tardó cuatro horas, por lo que puede descargarse de forma más rápida desde este link.

[Archivos utilizados durante el setting up](#)

Bibliografía

Graham, D. G. (2021). *Ethical hacking*. No Starch Press.

(Capítulo: *Setting Up*)