ENTRE SOMBRAS Y ESCUDOS: TALLER DE SIMULACIÓN DE ATAQUES Y ANÁLISIS FORENSE

Este taller tiene por objetivo enseñar al alumno una breve introducción al hacking ético y el análisis forense informático, realizando para ello un ejercicio de explotación de una máquina virtual vulnerable que se entrega previamente al ejercicio y, posteriormente, realizando el análisis forense de la misma para tratar de evidenciar las acciones de ataque realizadas anteriormente.

Para poder aprovechar al máximo la sesión, se recomienda al alumno realizar los pasos que se indican a continuación para la preparación del entorno de laboratorio que se utilizará durante el taller.

Requisitos técnicos necesarios

- Almacenamiento: 20 GB libres aproximadamente (puede emplearse el almacenamiento de un disco duro o una memoria USB externa)
- Memoria RAM: 8 GB (se emplearán 4GB de memoria RAM para el taller, 2 por máquina virtual)
- Permisos del usuario: administrador

Instalación de VirtualBox

En caso de ya disponer de un entorno de virtualización como VirtualBox o VMware Pro instalado en el equipo, puede omitirse el presente apartado. Cabe destacar que la versión gratuita de VMware Player no permite la configuración de redes virtuales, por lo que se recomienda la instalación de VirtualBox para la realización del presente ejercicio.

1. Ir a la página web oficial de VirtualBox y descargar el instalador para nuestra versión de arquitectura y sistema operativo.
2. Instalar el programa VirtualBox recién descargado (es necesario disponer de privilegios de **administrador**).

Descargar e importar máquina virtual del taller

1. Ir al enlace compartido para la descarga de la máquina del taller desde Google Drive y descargar el fichero ZIP de la carpeta de la máquina virtual para nuestra versión de arquitectura (32/64 bits) y tecnología de virtualización (VirtualBox/VMware Pro).
2. Descomprimir el fichero **.zip** recién descargado, proporcionando como **contraseña** de descompresión "**uah**" (sin comillas), en una ruta de nuestra elección (se recomienda que sea en un disco con suficiente almacenamiento disponible – aprox. 20 GB – para poder descomprimir tanto la presente máquina como la Kali Linux en la misma ruta).

VirtualBox

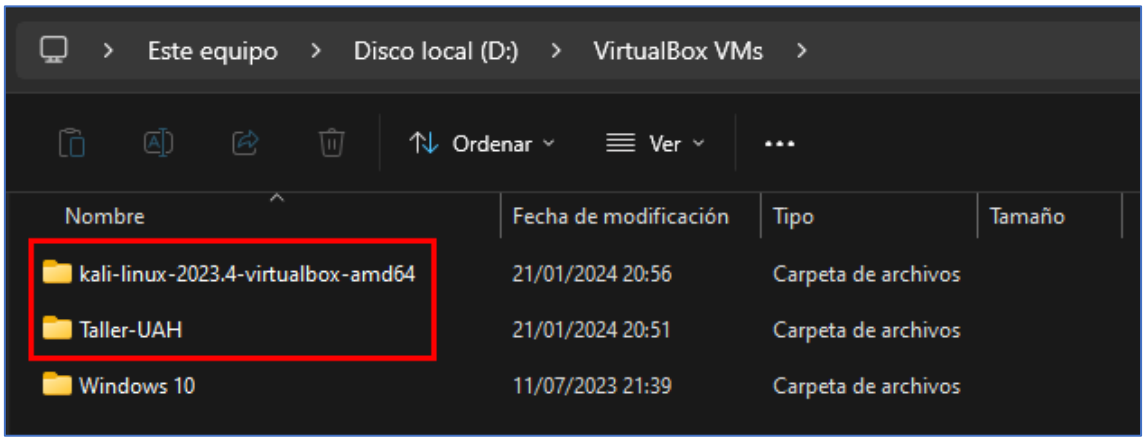
1. Hacer **doble click** sobre el archivo con extensión **.vbox** para abrir directamente la máquina virtual en VirtualBox.

VMware Pro

1. Hacer **doble click** sobre el archivo con extensión .**vmx** para abrir directamente la máquina virtual en VMware Pro.

Descargar e importar máquina virtual Kali

1. Ir a la [página web oficial de Kali Linux] y descargar la carpeta de la máquina virtual para nuestra versión de arquitectura y tecnología de virtualización.
2. Descomprimir el fichero **.7z** recién descargado en la misma ruta donde hemos creado la máquina virtual para el taller.
    - En caso de no disponer de un programa para la descompresión de ficheros con extensión 7Z, se recomienda la descarga e instalación de **7-zip**.



VirtualBox

1. Hacer **doble click** sobre el archivo con extensión .**vbox** para abrir directamente la máquina virtual en VirtualBox.

VMware Pro

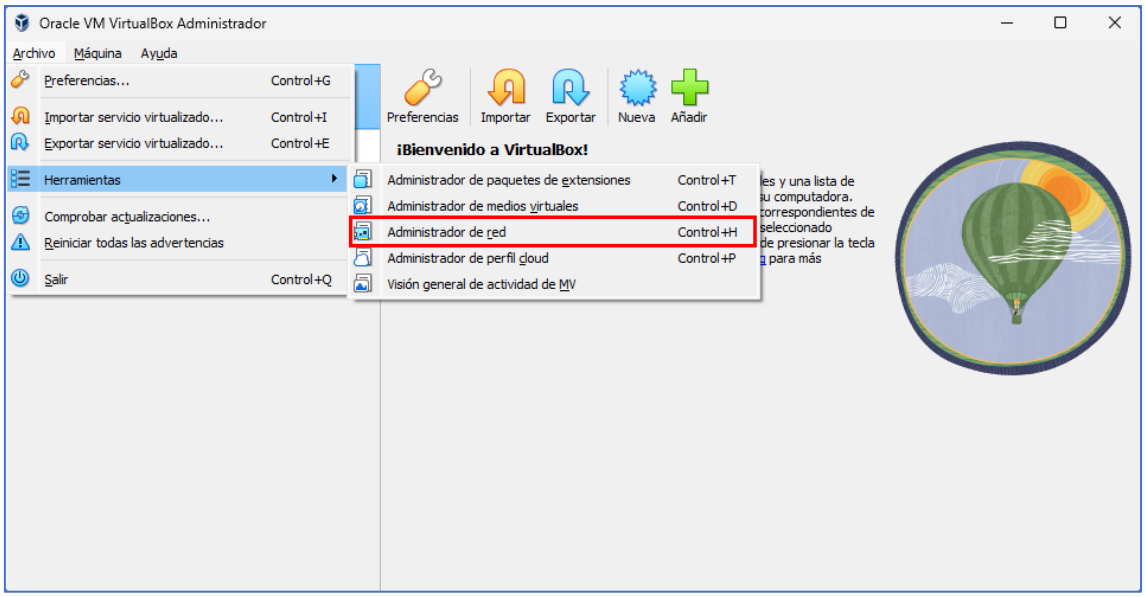
2. Hacer **doble click** sobre el archivo con extensión .**vmx** para abrir directamente la máquina virtual en VMware Pro.

Configurar red interna virtual

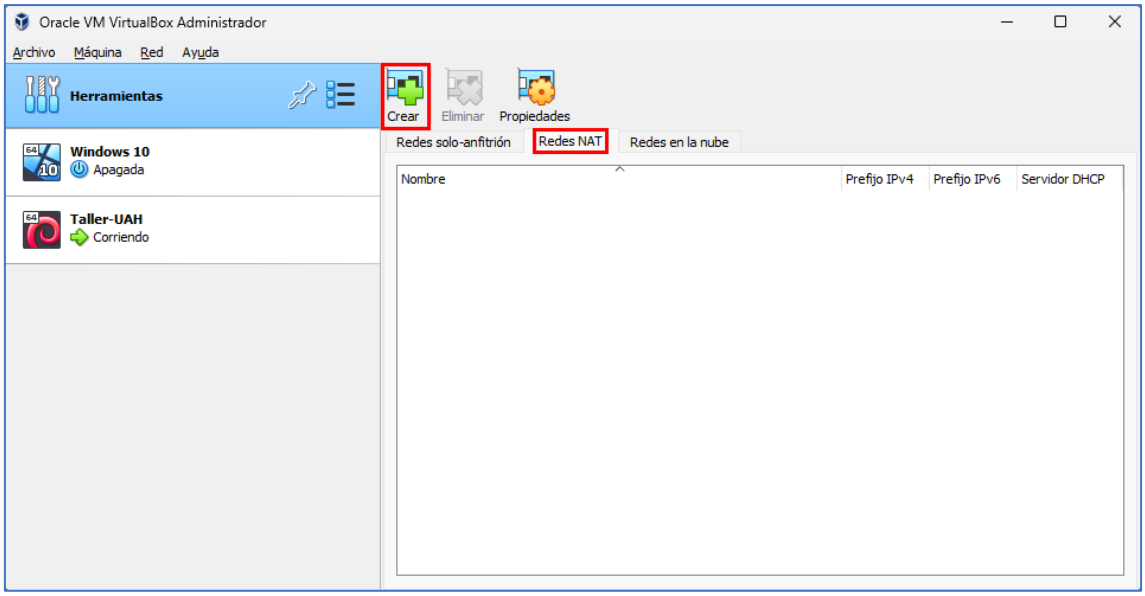
Para que nuestra máquina de ataque Kali Linux y la máquina del taller tengan visión entre sí, deberemos primeramente configurar una red interna virtual en nuestra tecnología de virtualización.

VirtualBox

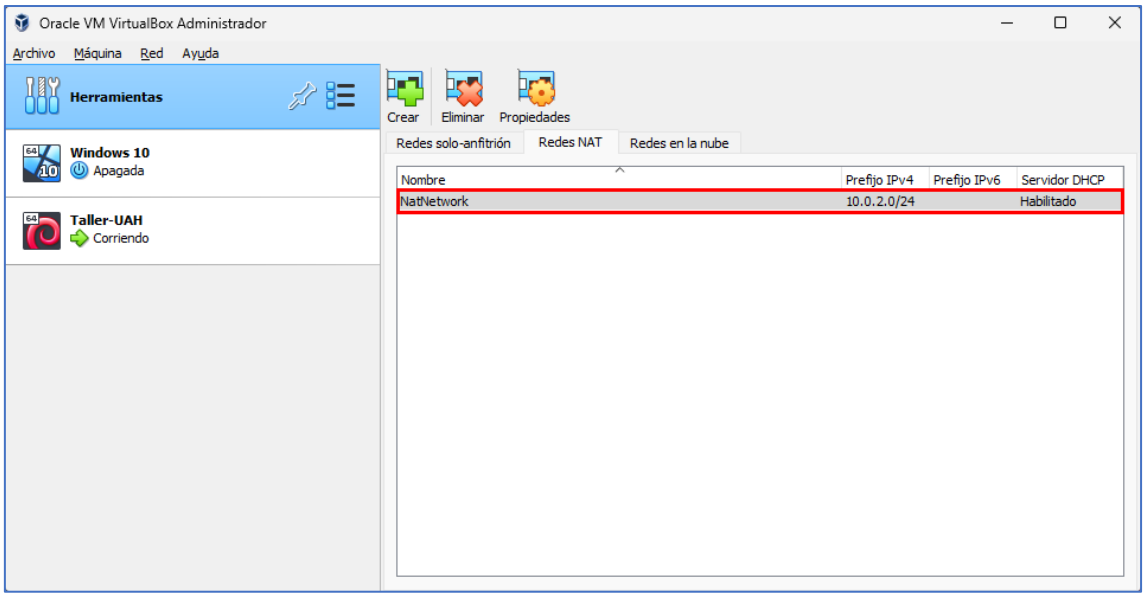
Crear la red interna para que las máquinas tengan visión entre sí: navegaremos para ello en el menú de administración principal de VirtualBox, en el barra de menú superior, a **Archivo > Herramientas > Administrador de red**.



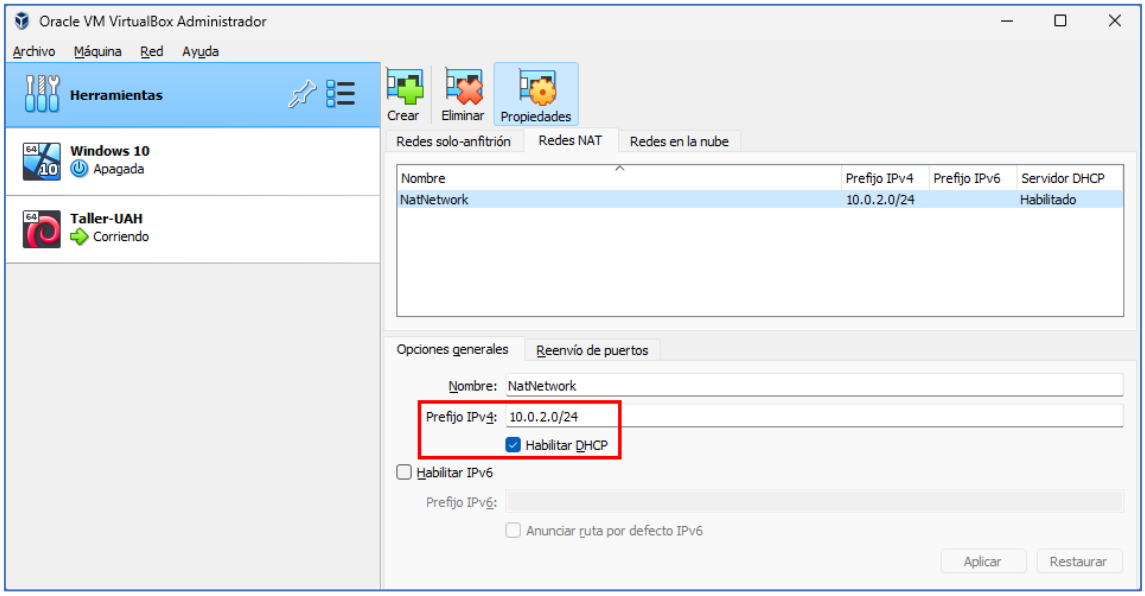
Posteriormente, seleccionaremos la pestaña "**Redes NAT**" y crearemos una nueva con el botón "**Crear**".



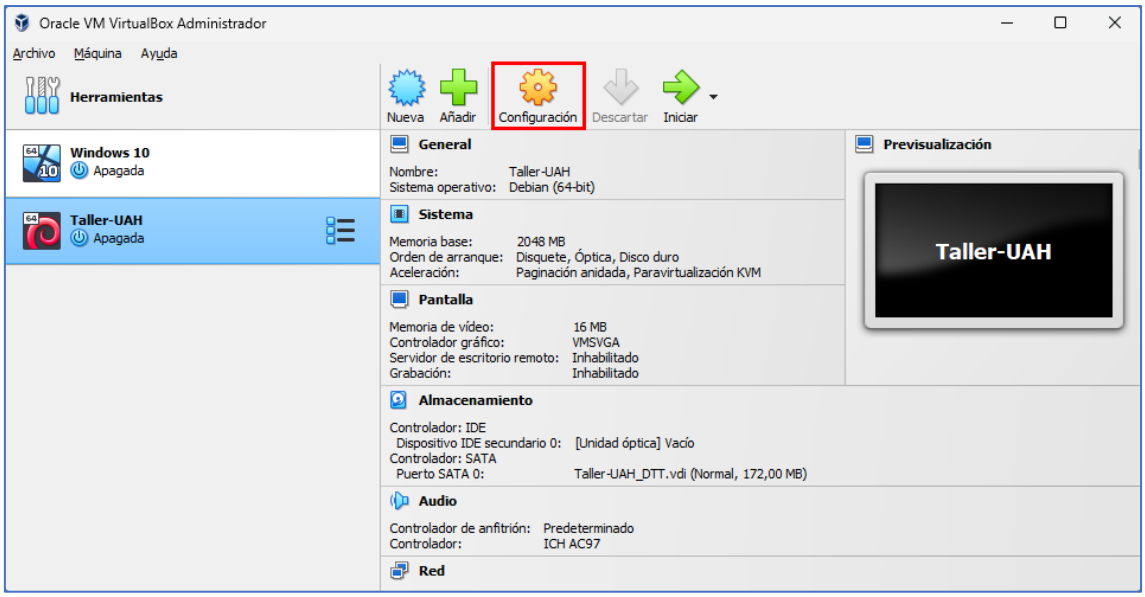
Por defecto, se creará una red con el nombre "**NatNetwork**" y un direccionamiento de subred IP automático.



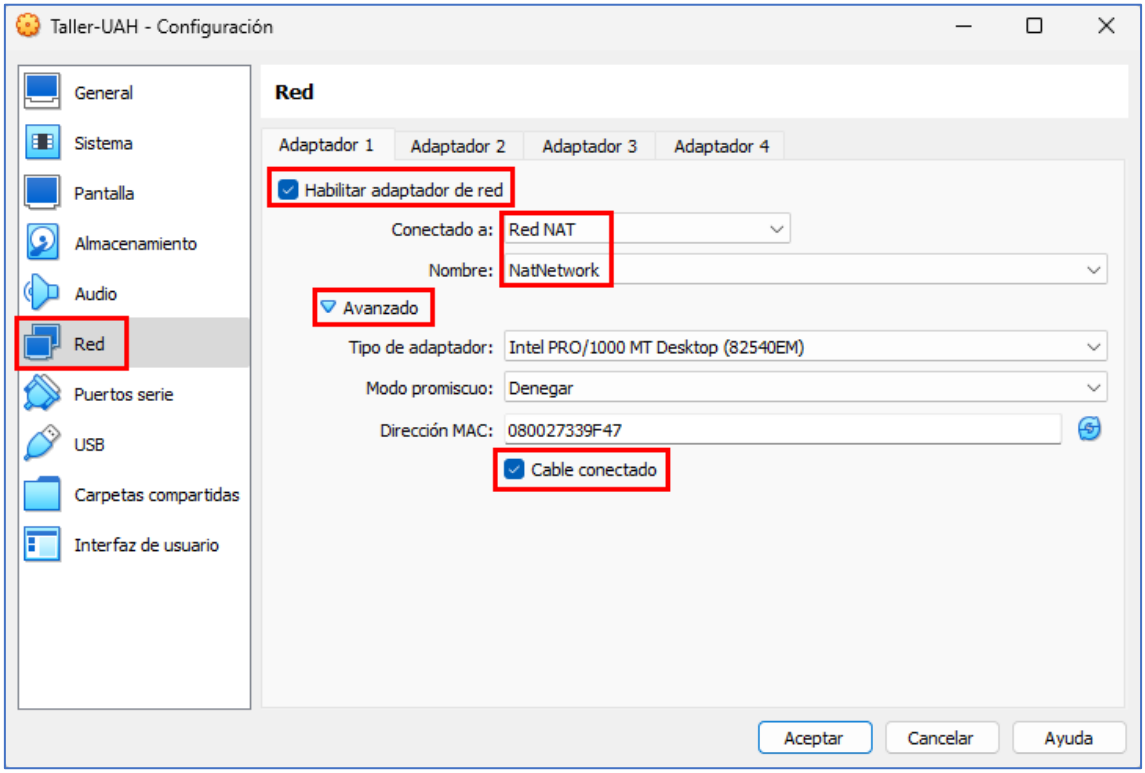
En caso de querer modificar la configuración de la red recién creada, podemos hacer **doble click** sobre la misma o en el botón "**Propiedades**". Debemos asegurar que el servicio DHCP se encuentra habilitado para la red.



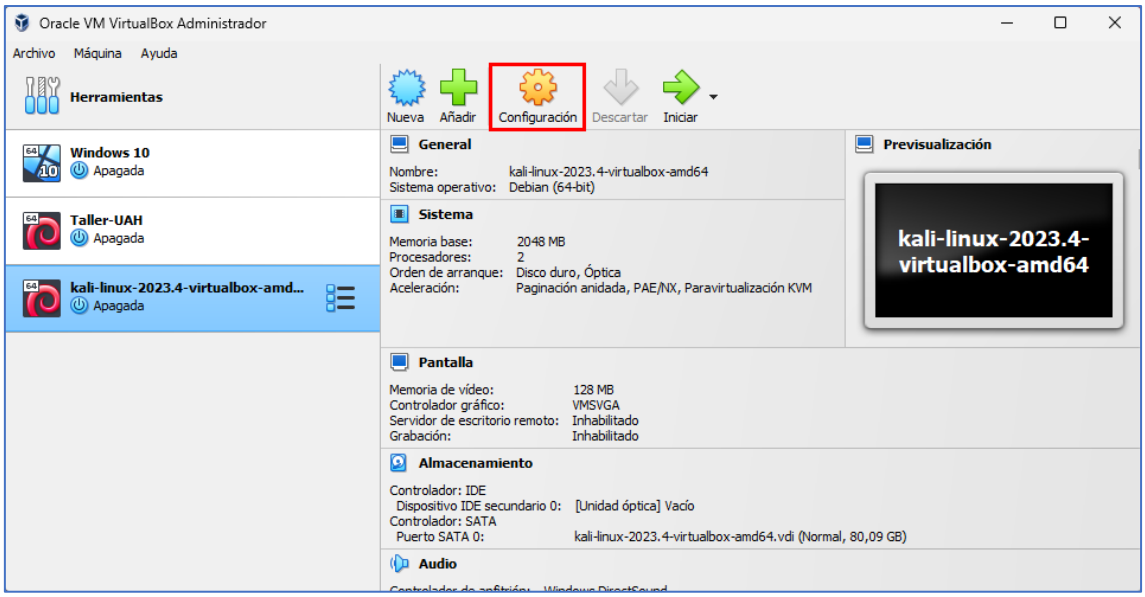
Cambiar la configuración de red de la máquina virtual del taller: seleccionamos la máquina del taller importada y el botón "**Configuración**".

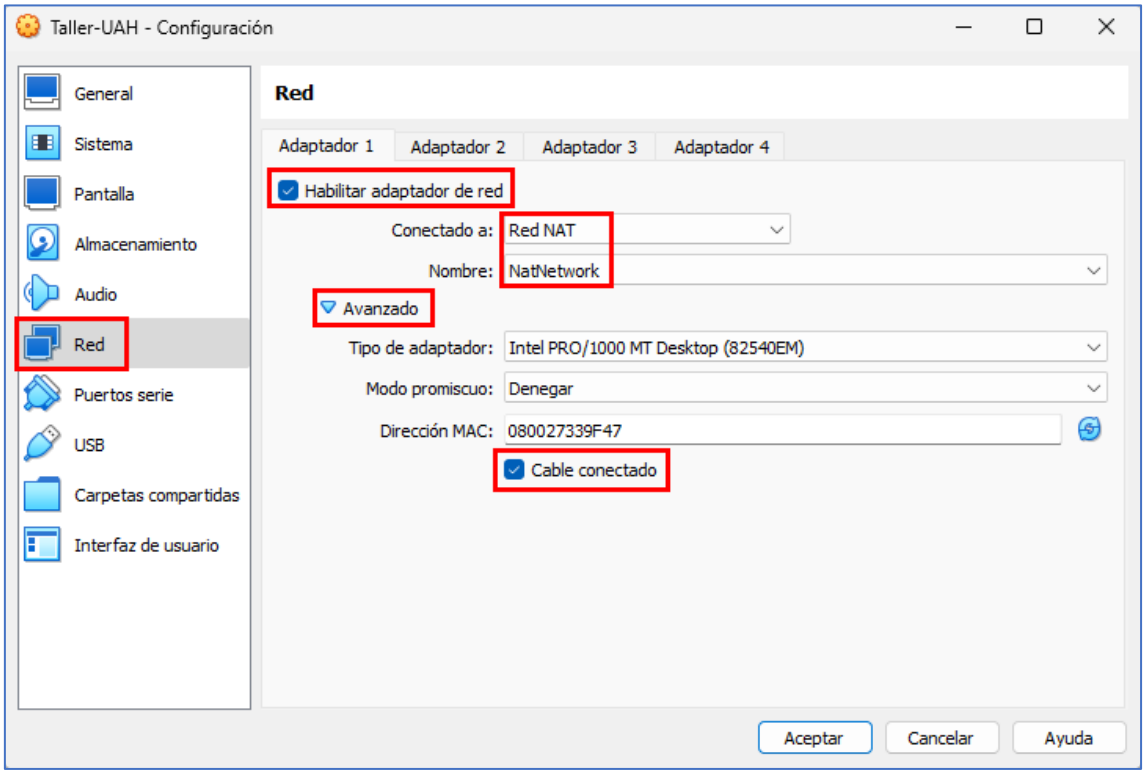


En el menú lateral izquierdo, navegamos a la opción "**Red**" y para el **Adaptador 1**, comprobamos que la configuración se encuentra establecida tal y como se muestra en la captura a continuación.



Repetir los mismos pasos para la máquina virtual Kali:

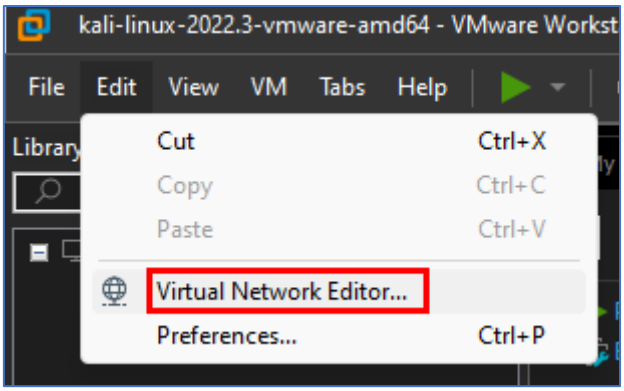




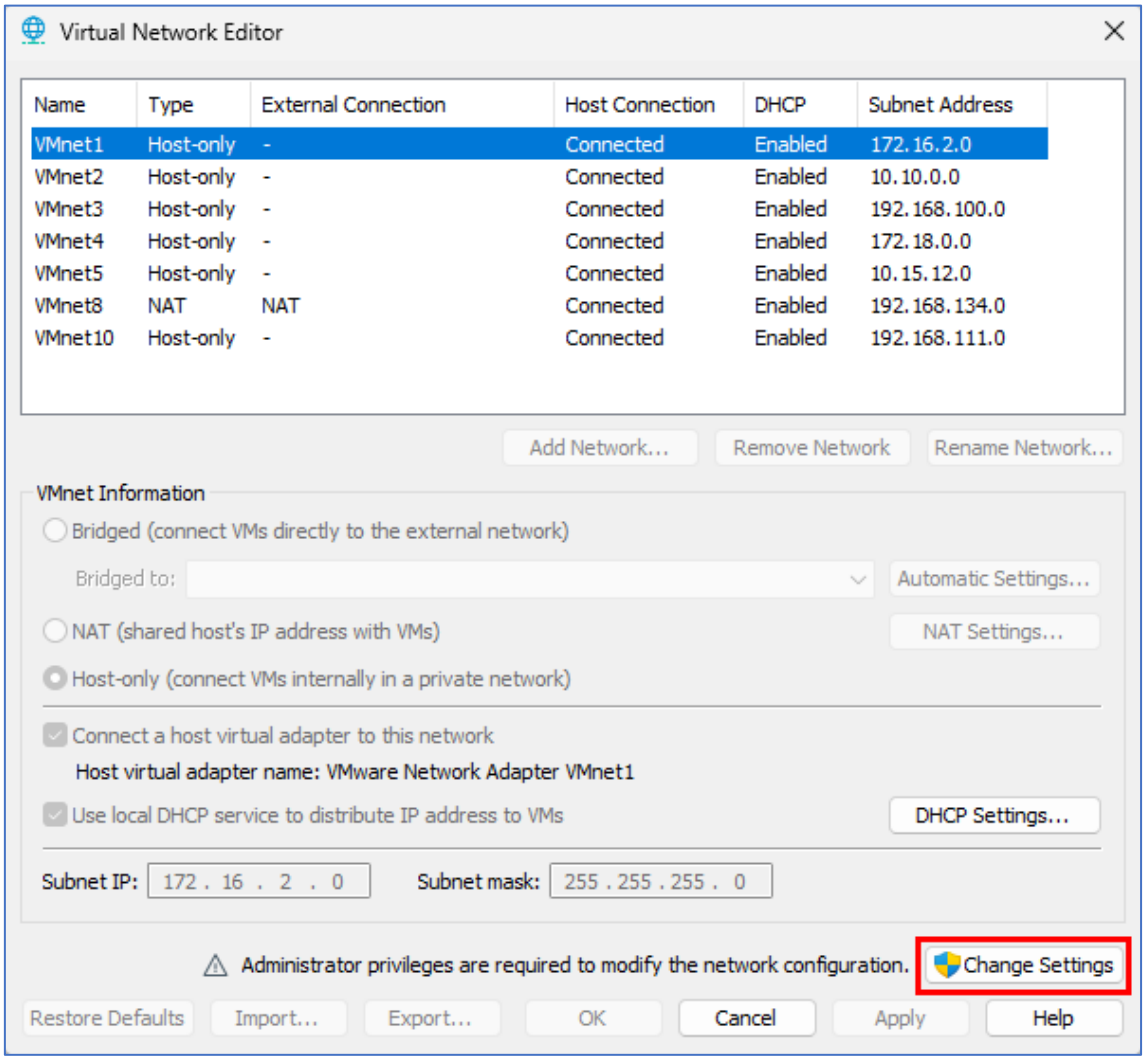
Encender ambas máquinas virtuales (la máquina de Kali puede tardar hasta un par de minutos en iniciarse y mostrar la interfaz gráfica de inicio de sesión).

VMware Pro

Crear la red interna para que las máquinas tengan visión entre sí: navegaremos para ello en la aplicación de Escritorio de VMware Pro, en la barra de menú superior, a **Edit > Virtual Network Editor…**

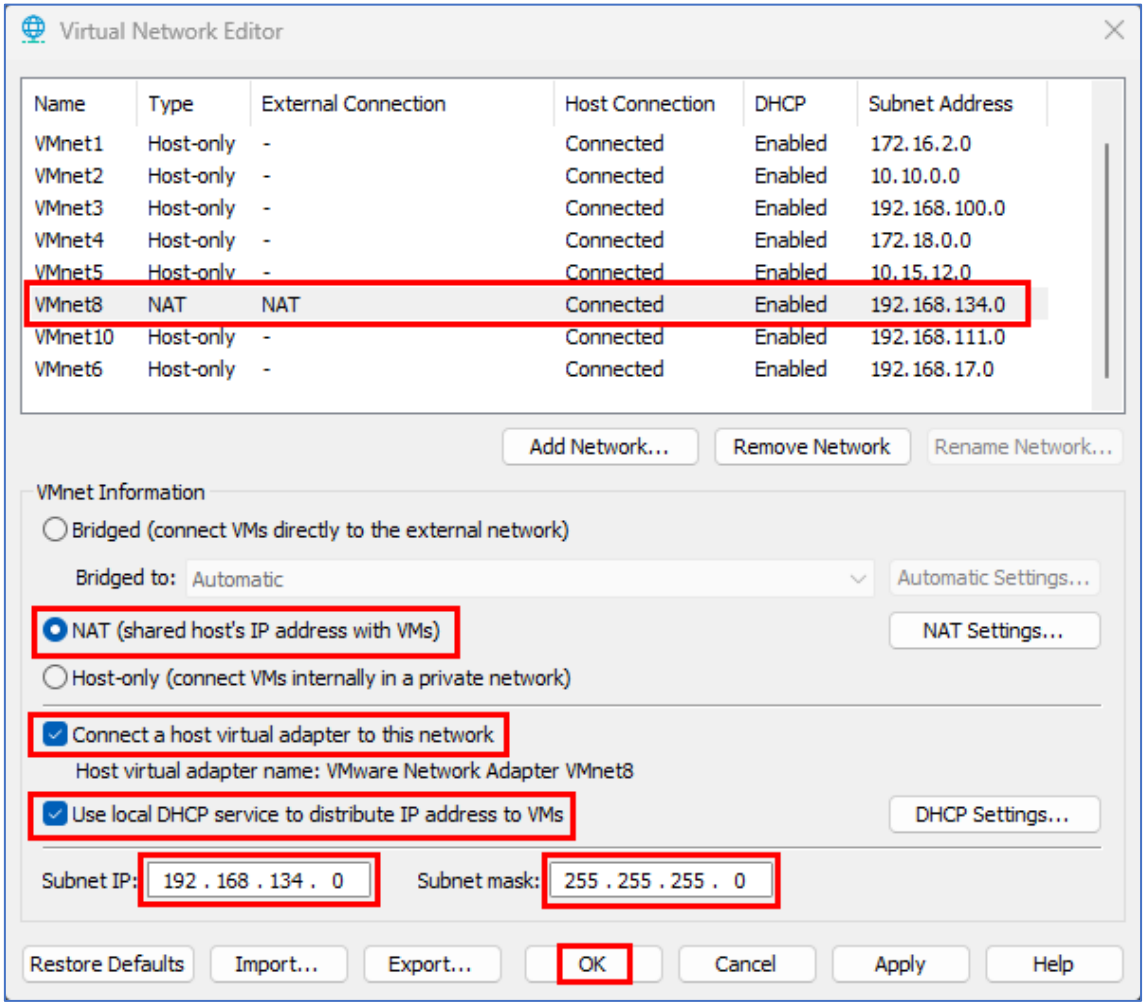


En caso de existir alguna red NAT ya creada (como la VMnet8 que se puede ver en la captura a continuación) con DHCP habilitado y que no se encuentre actualmente en uso en el equipo, se puede utilizar sin necesidad de configurar otra red adicional (en concreto, VMware solo permite tener definida a la vez una única red NAT por lo que, en caso de existir ya una creada, no es posible crear una segunda). En caso contrario, deberá primeramente habilitarse la opción de realizar cambios en la configuración, para lo cual se necesitan privilegios de **administrador**.

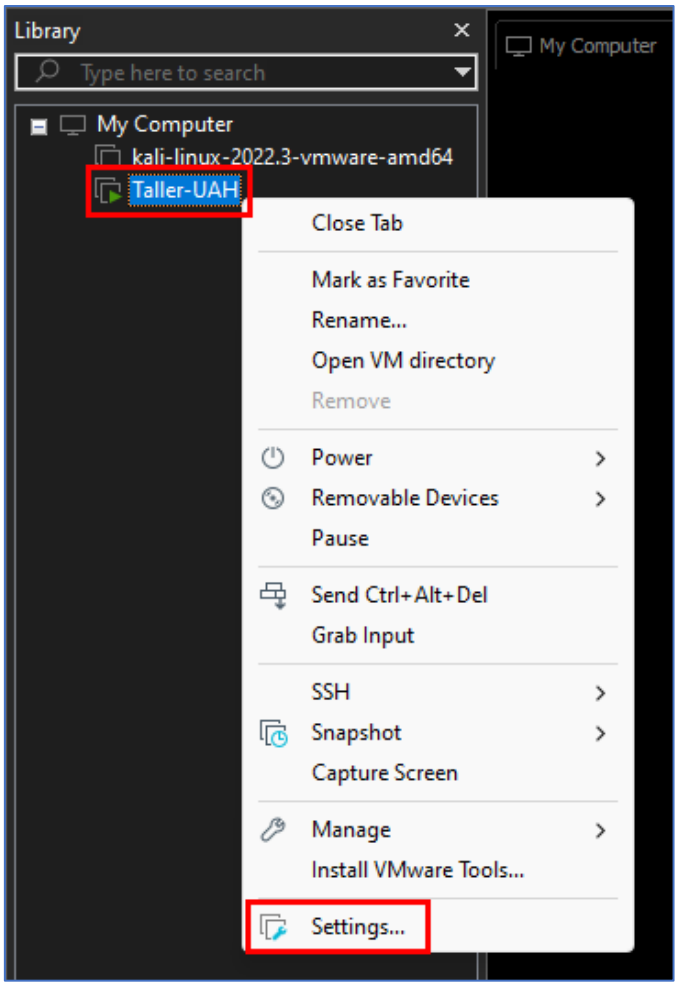


Seleccionamos la opción "**Add Network…**" y en el menú desplegable que se muestre, seleccionamos cualquier nombre disponible.

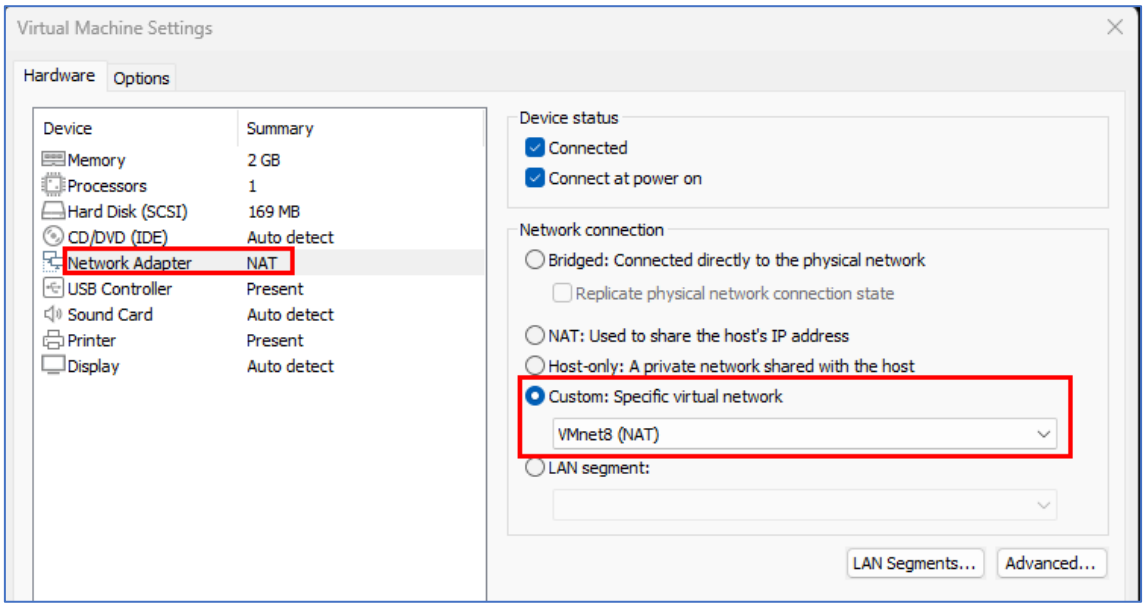
Deberemos asegurar que la configuración que se establezca siga los parámetros definidos en la captura a continuación. Para el caso de la subred IP, puede emplearse cualquiera que se encuentre disponible en nuestro host físico (i.e. con el comando **ipconfig** en una consola de comandos, puede revisarse qué direccionamiento IP tenemos por defecto asignado en nuestra interfaz principal de la tarjeta de red).



Cambiar la configuración de red de la máquina virtual del taller: en este caso, al estar la máquina preparada a partir de un snapshot de la misma en estado de suspensión, **es necesario encender primero la máquina y luego modificar la configuración de red**.



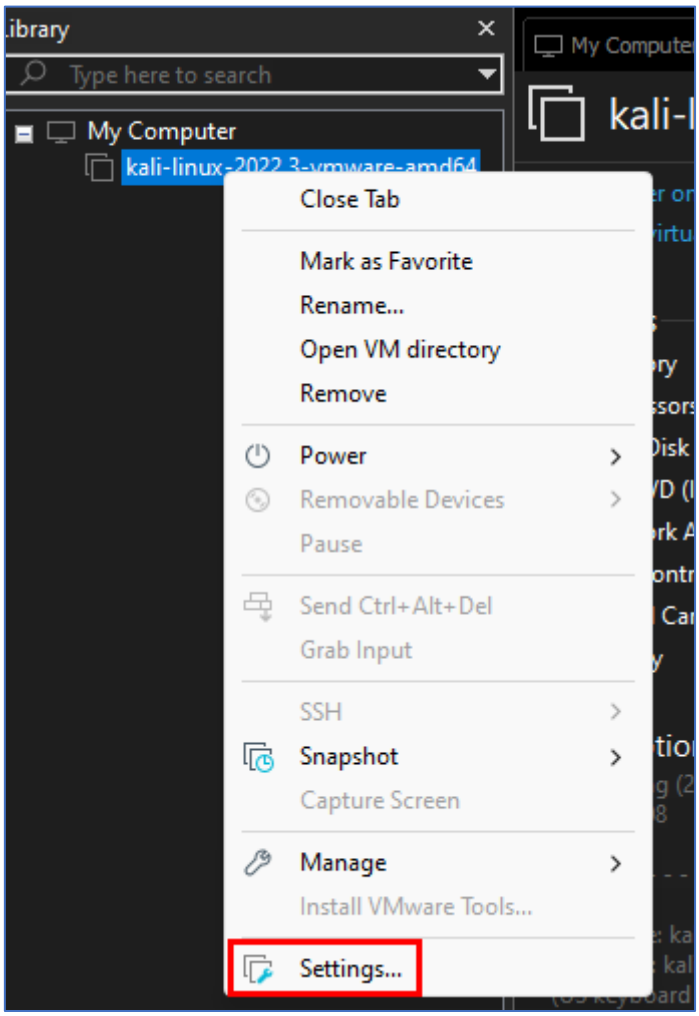
En las opciones del menú lateral izquierdo, seleccionamos "**Network Adapter**", nos aseguramos de que las **casillas** de la configuración del **estado del adaptador** de red se encuentran **habilitadas** y cambiamos el tipo de conexión de red a "**Custom: Specific virtual network**" seleccionando en el desplegado la red creada en el paso anterior (es fácilmente identificable por tener especificado "NAT" entre paréntesis).

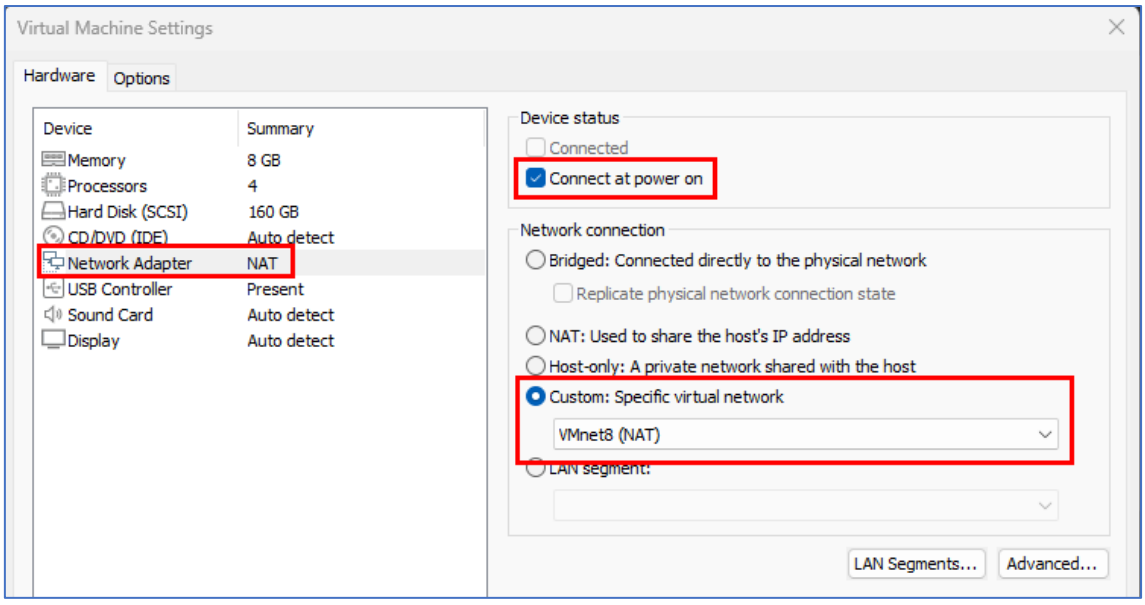


Podemos confirmar fácilmente que se ha cambiado correctamente la configuración ejecutando en la terminal de la máquina virtual del taller el comando "**ip a**" y revisando que, en el adaptador de red por defecto "**eth0**", efectivamente se muestra una dirección IP interna asignada en el rango de red definido para nuestra red virtual NAT en el paso anterior.

```
user@debian:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    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: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOW
N qlen 1000
    link/ether 00:0c:29:2a:a9:76 brd ff:ff:ff:ff:ff:ff
    inet 192.168.134.139/24 brd 192.168.134.255 scope global eth0
    inet6 fe80::20c:29ff:fe2a:a976/64 scope link
       valid_lft forever preferred_lft forever
user@debian:~$ _
```

Repetir los mismos pasos para la máquina virtual Kali: en este caso, no es necesario que la máquina esté encendida para modificar su configuración de red (aunque, al encontrarse el servicio DHCP habilitado, en caso de estar encendida, el cambio será también inmediato).





Encender ambas máquinas virtuales (la máquina de Kali puede tardar hasta un par de minutos en iniciarse y mostrar la interfaz gráfica de inicio de sesión).

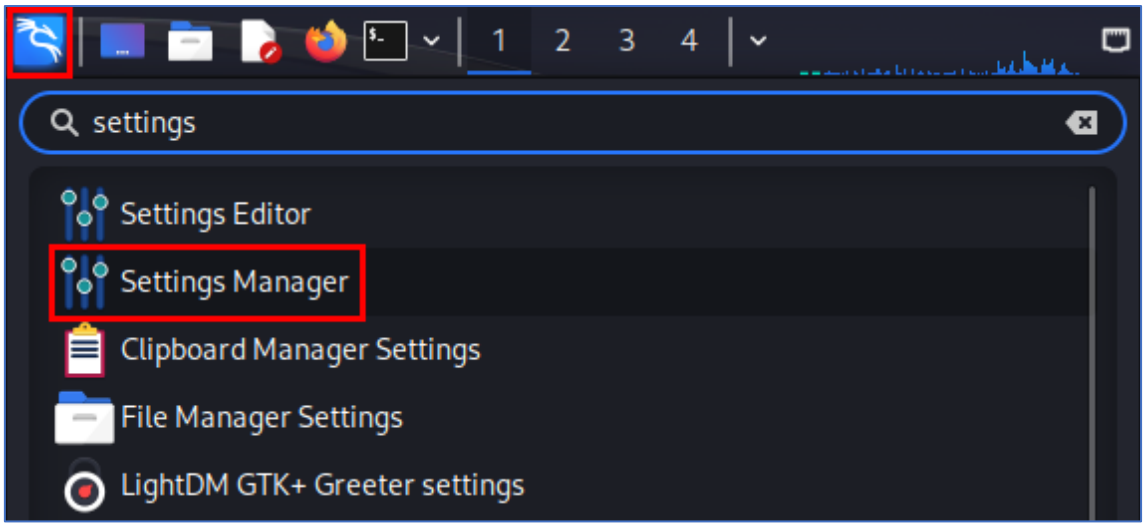
Requisitos previos para Kali Linux

Credenciales por defecto:

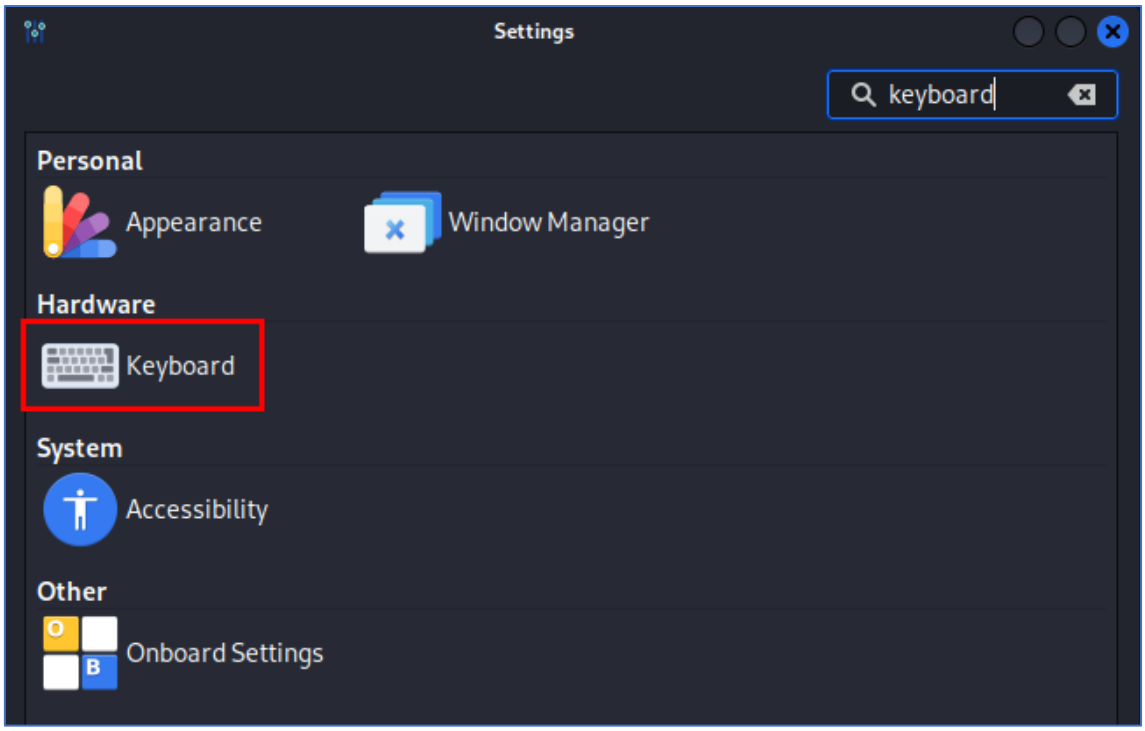
- Usuario: kali
- Contraseña: kali

Cambiar la distribución del teclado

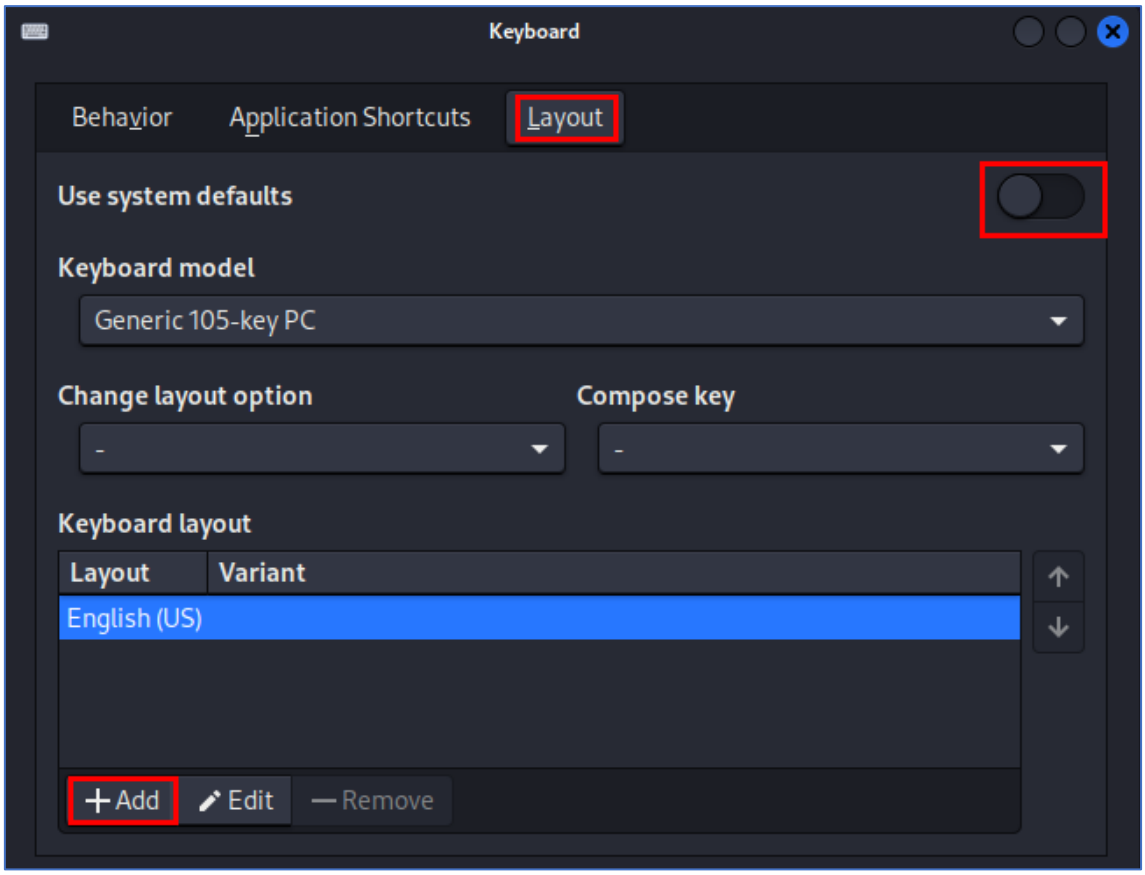
Una vez iniciada sesión, navegaremos al menú de aplicaciones seleccionando el icono superior izquierdo en la barra de menú superior del Escritorio, y buscaremos la aplicación denominada "**Settings Manager**".



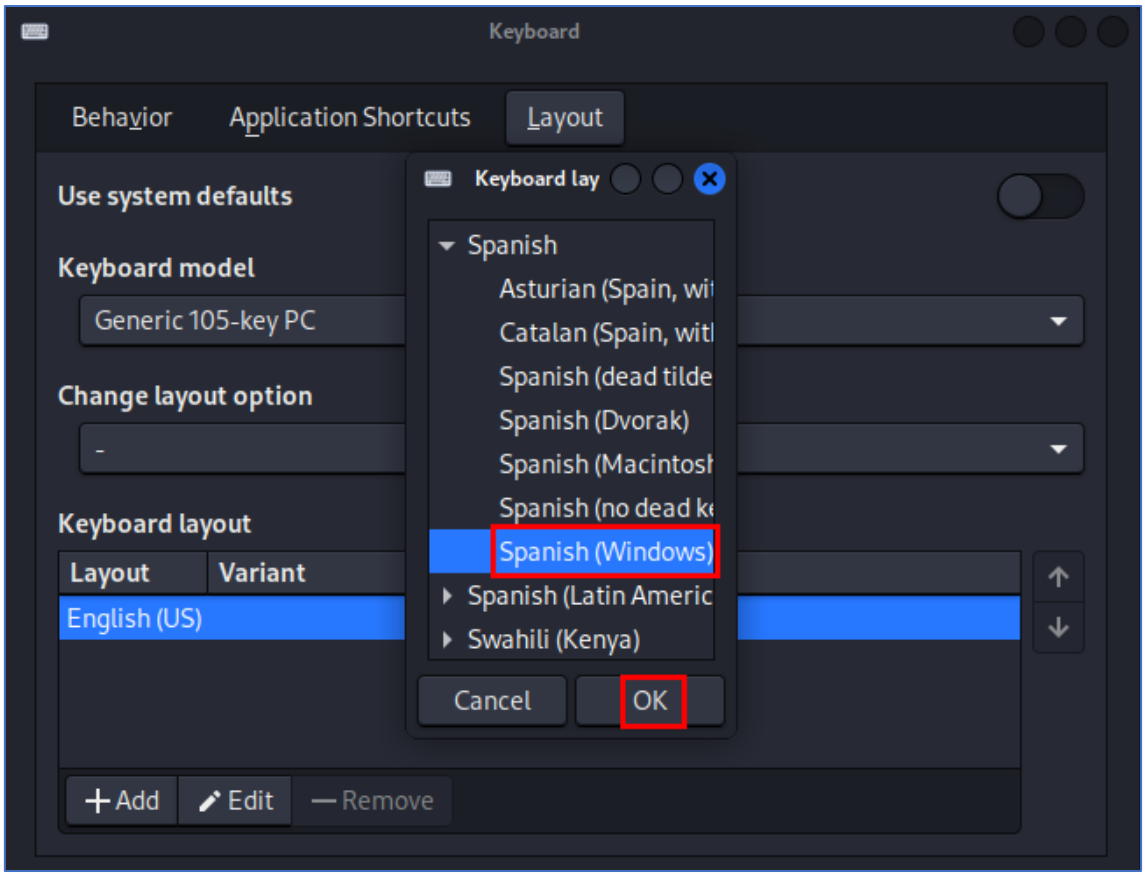
Buscamos la opción de configuración del teclado (i.e. "***keyboard***").



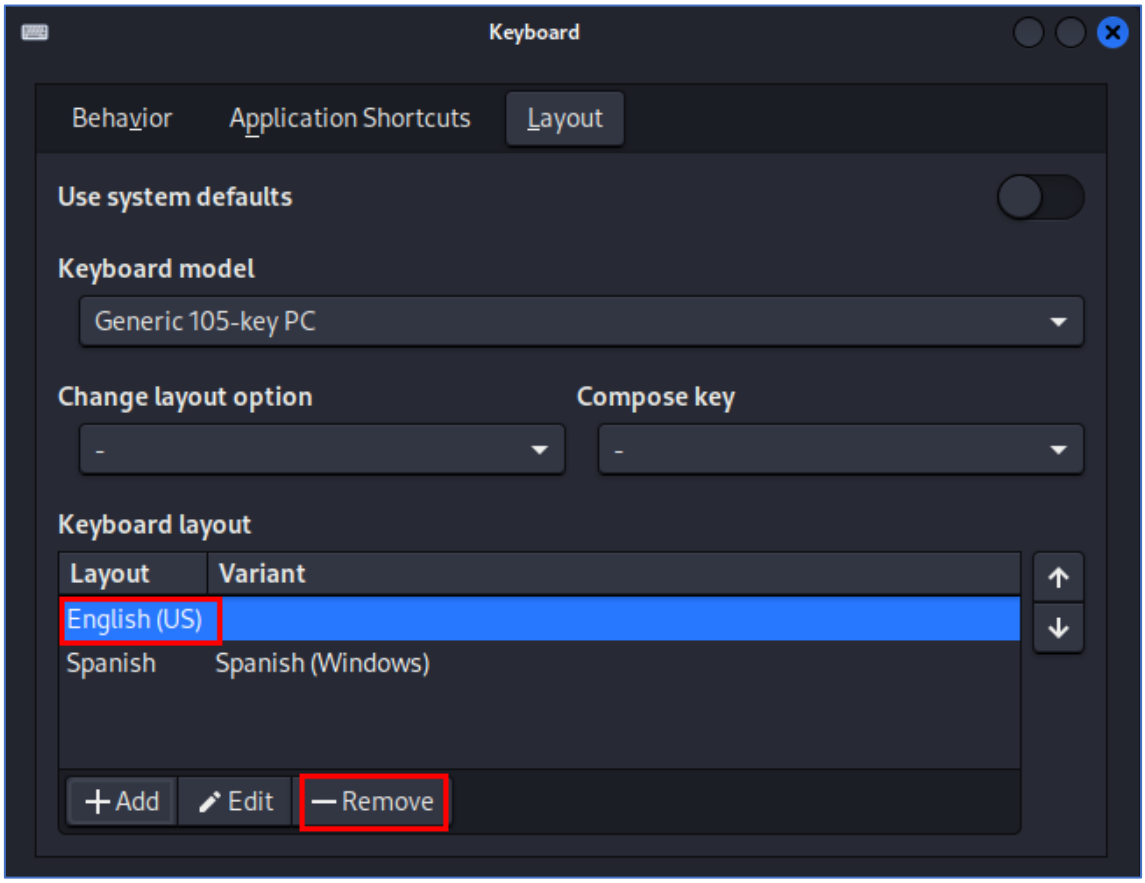
En la pestaña "**Layout**", deseleccionamos la opción inicial "**Use system defaults**" y seleccionamos el botón "**+ Add**" para añadir una nueva distribución de teclado.



A continuación, buscamos y seleccionamos la distribución **Spanish > Spanish (Windows)**.



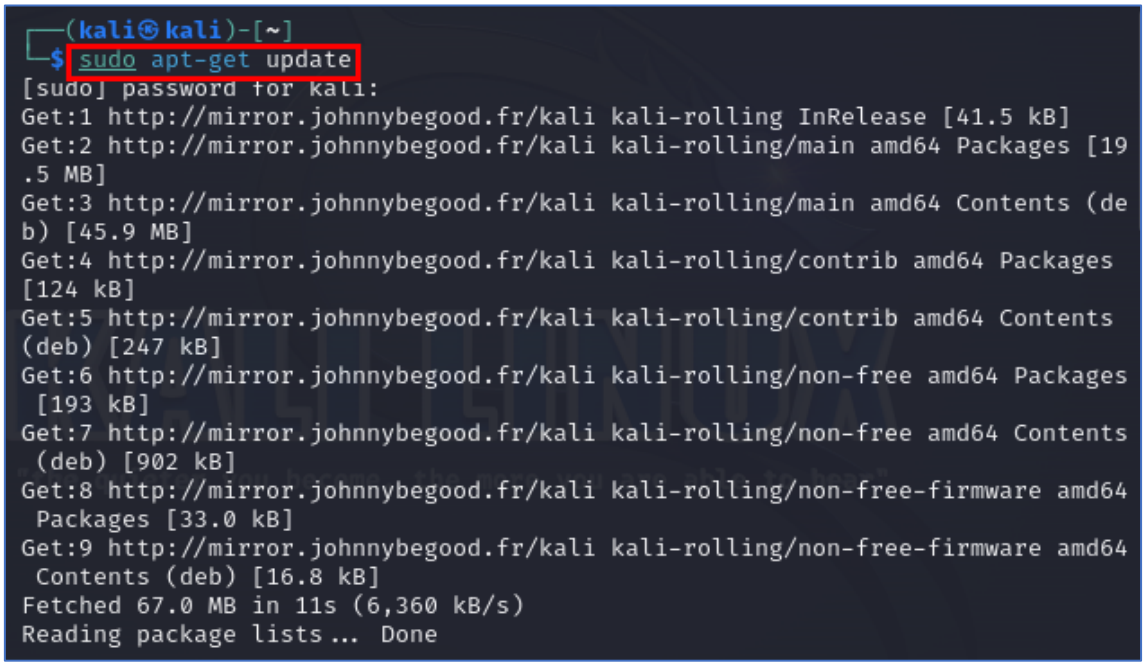
Eliminamos la distribución inglesa, seleccionándola y a continuación el botón "**– Remove**".



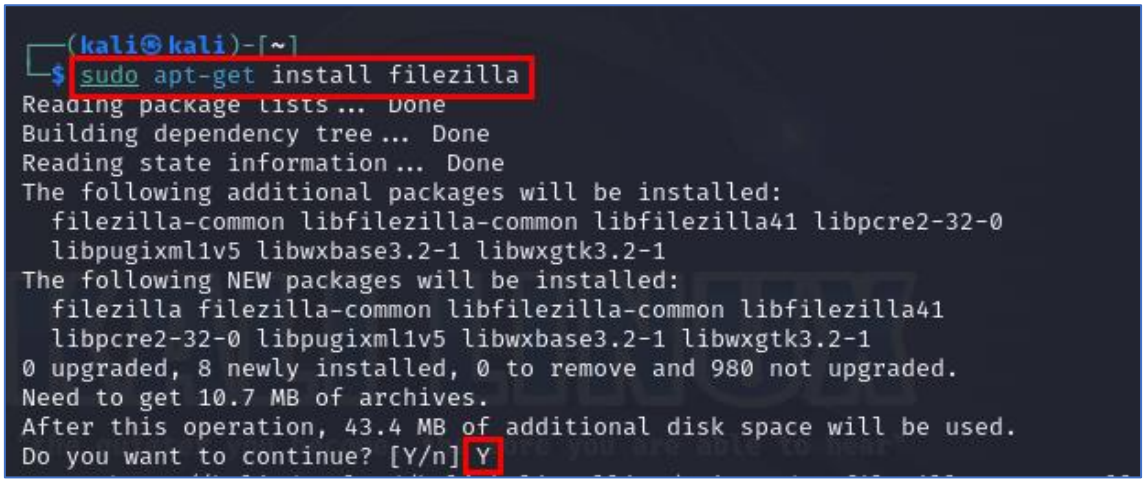
En caso de tener ya una terminal abierta, deberemos cerrarla y abrir una nueva para asegurar que se aplican los cambios en la distribución del teclado de entrada.

Instalar Filezilla como cliente SFTP

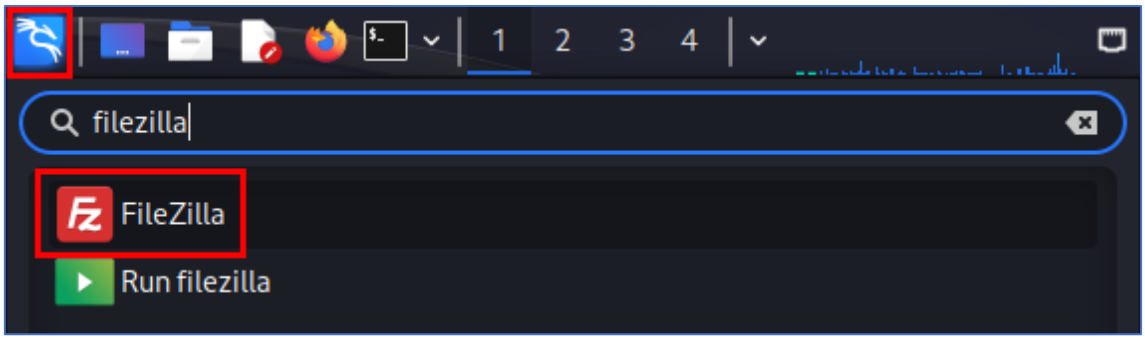
Abrimos una terminal y ejecutamos el comando "**sudo apt-get update**" para actualizar las fuentes del gestor de paquetes *apt*.



Descargamos el programa de intercambio de ficheros Filezilla ejecutando el comando "**sudo apt-get install filezilla**". En el momento en que se solicite por consola confirmación para continuar con el proceso de instalación, introduciremos **Y** (Yes).



Confirmamos que el programa se ha instalado correctamente navegando para ello al menú de aplicaciones y buscando por el nombre de la aplicación "filezilla".


1
2
3
4
filezilla
FileZilla
Run filezilla