MANUAL DE INSTALACION METASPLOITABLE_3 EN VIRTUALBOX

LUIS JADER CUESTA MOYA

SEMESTRE:

VIII

Fecha: 07/08/2025

INTRODUCCIÓN

Metasploitable3 es una máquina virtual diseñada específicamente con vulnerabilidades, creada para que tanto estudiantes como profesionales de la ciberseguridad puedan practicar análisis, explotación y verificación de fallas de seguridad en un ambiente controlado. Esta herramienta, forma parte del conocido Metasploit Framework, muy popular en el mundo de las pruebas de penetración.

Metasploitable3 se apoya en sistemas operativos más modernos (como Windows Server 2008 o Ubuntu) e implica una instalación algo más compleja, utilizando herramientas como Packer, Vagrant, y VirtualBox o VMware. Actualmente la usamos para laboratorio de hacking ético.

Contenido

1. METASPLOITABLE 3

Para esta instalación se presenta un caso nuevo para mí, ya que es primera vez que instalo un sistema por medio de líneas de código y más cuando veo que su instalación compleja requiere de otros programas para lo que se requiere trabajar, como lo es el caso de **VAGRANT** antes de hacer cualquier proceso debí instalar esta herramienta como se mostrara a continuación.

1.1. Vagrant

Es una herramienta de código abierto que permite crear y configurar entornos virtuales de desarrollo de manera sencilla y reproducible.

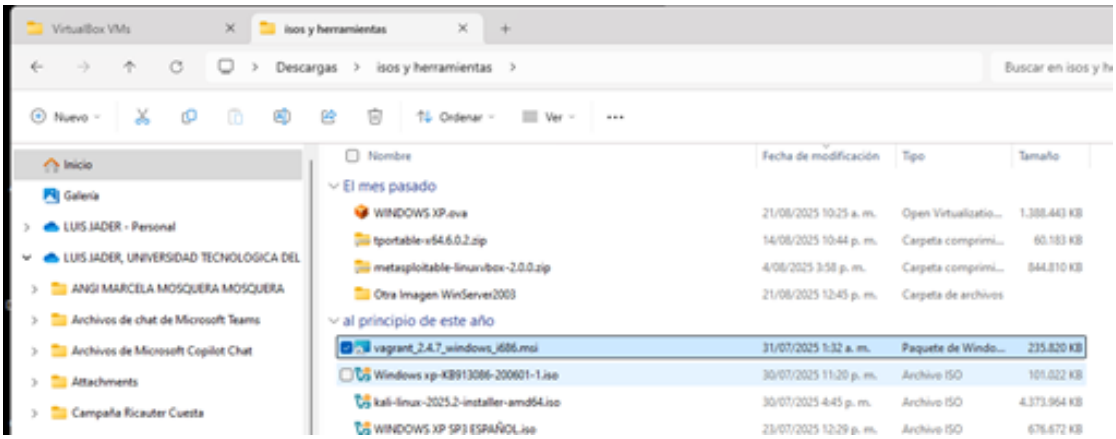

Ilustración 1 archivo de instalacion Vagrant

Al ejecutar el archivo descargado. Se abrirá el asistente de instalación. Aceptar los términos de la licencia marcando la casilla **“I accept the terms in the License Agreement”** y hacer clic en **Install**.

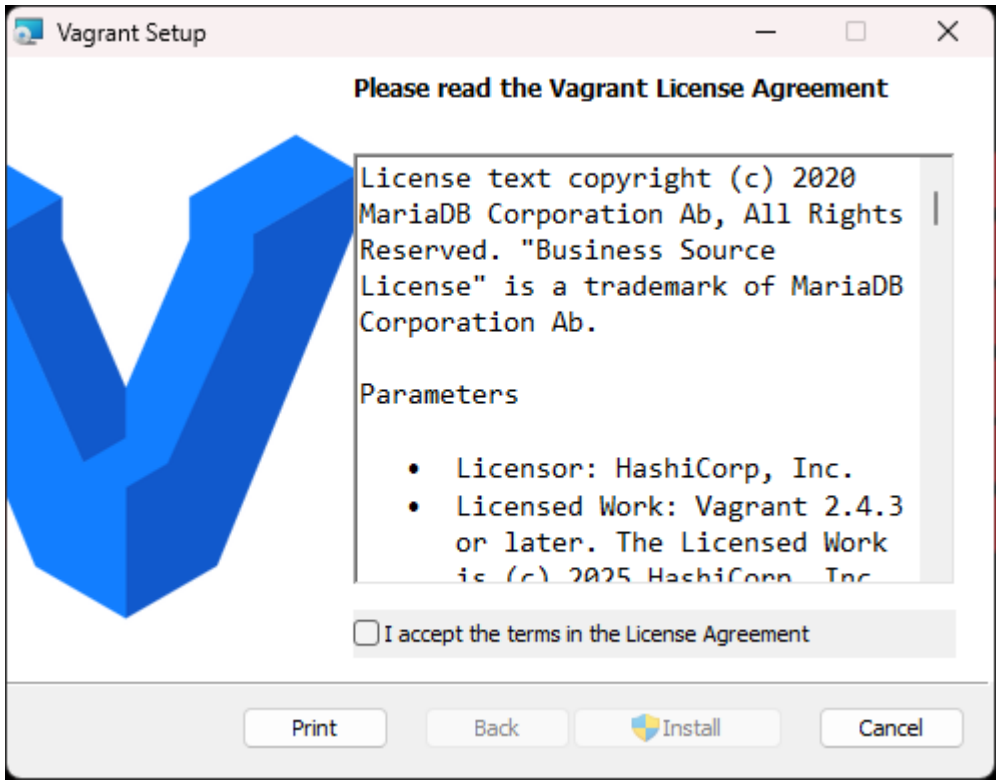

Ilustración 2 proceso de instalacion vagrant

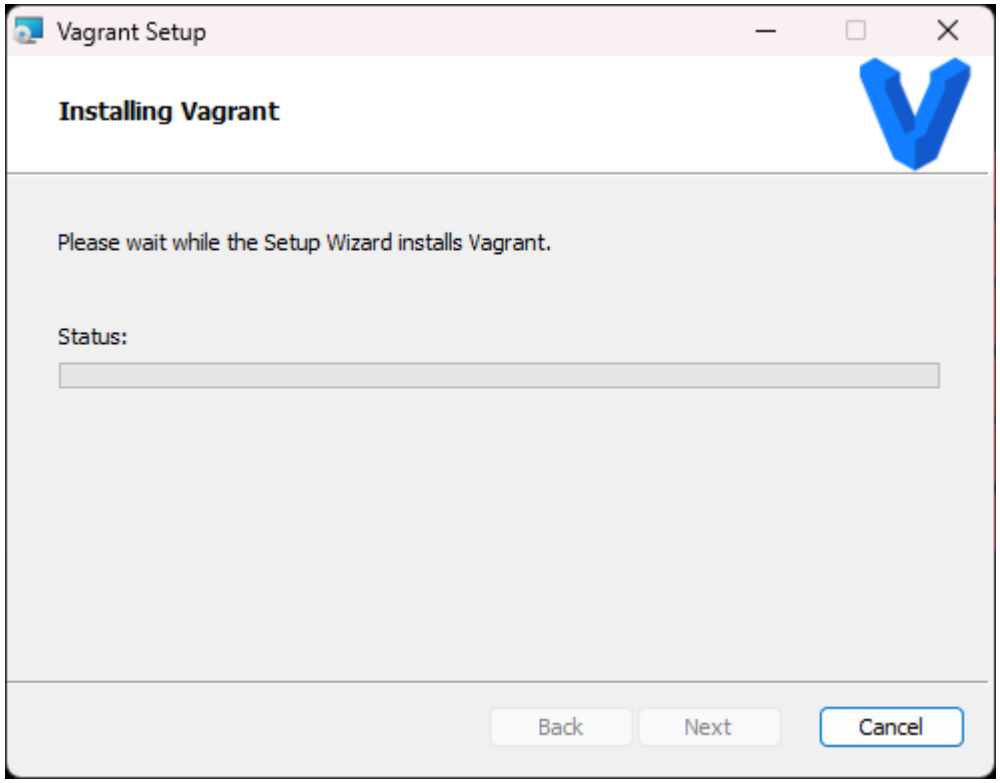

Ilustración 3 estado de carga durante instalacion

Esperar a que finalice la instalación.

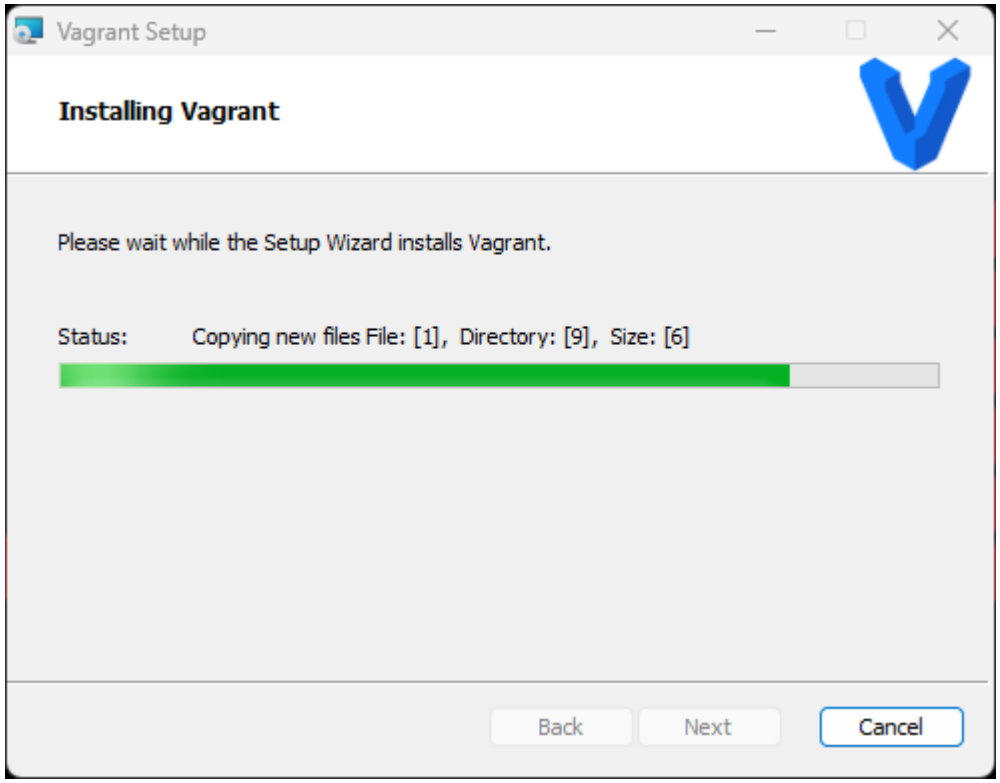

Ilustración 4 estado de carga durante instalacion parte2

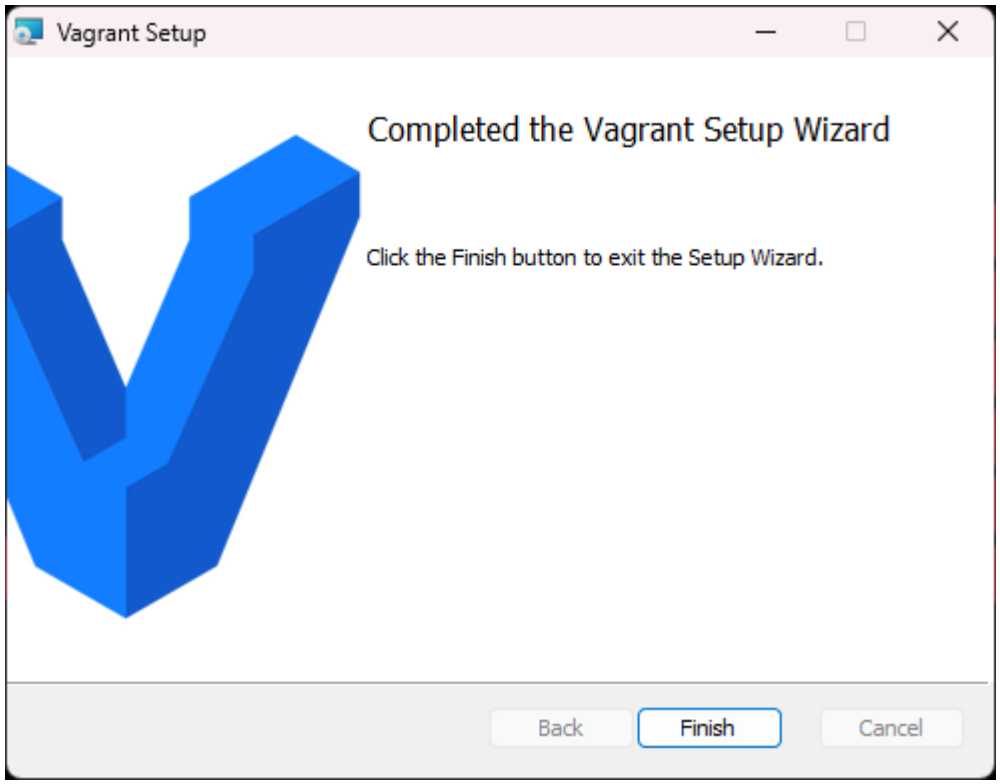

Ilustración 5 finalizacion de instalacion vagrant

Luego presionar **Finish**.

1.2. Instalación de PowerShell 7

Es otro de los requerimientos para tener una buena respuesta de trabajo por Metasploitable3

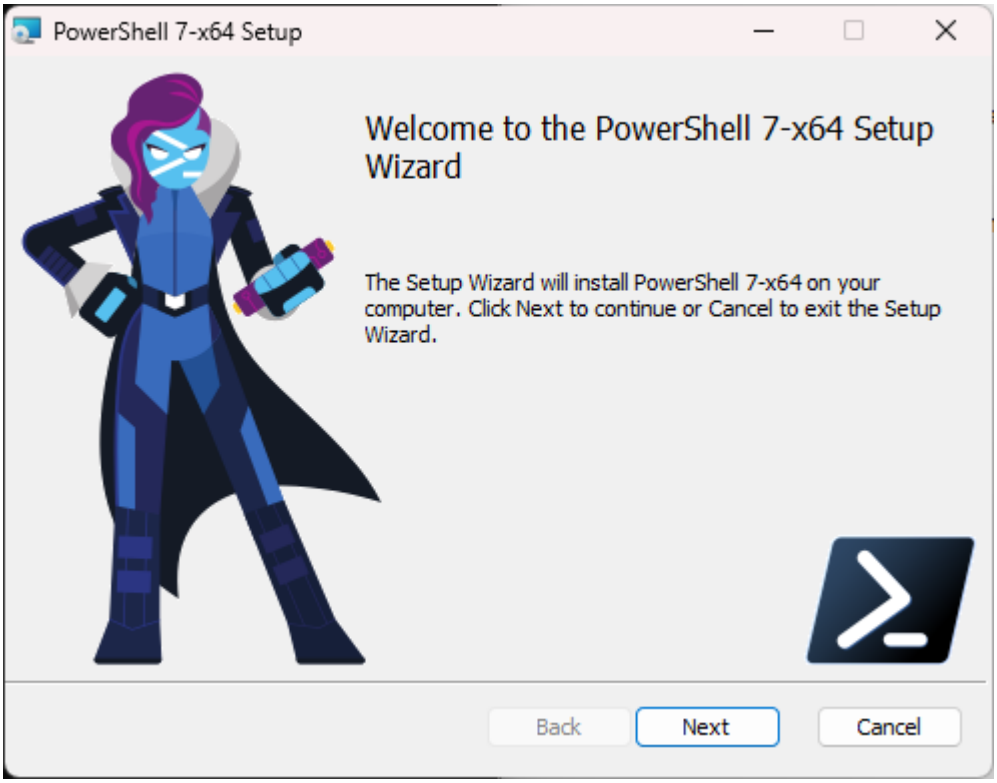

Ilustración 6 Instalación de PowerShell 7

Hacemos clic en **Next** para continuar.

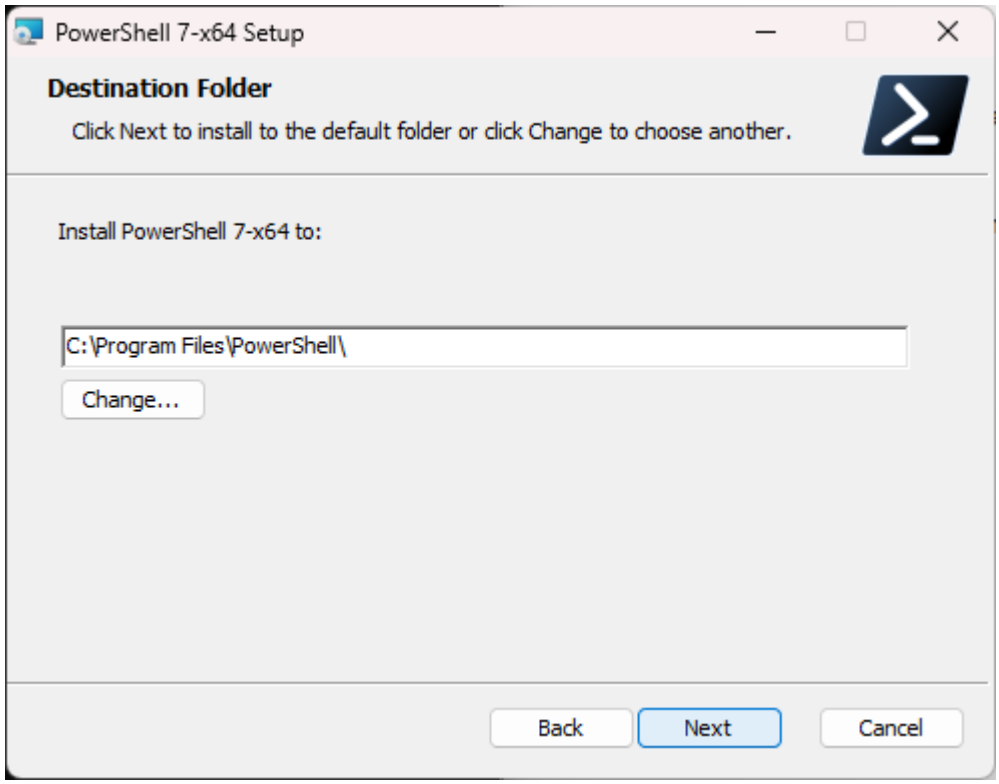

Ilustración 7 selecion de destino donde se instalara

Seleccionamos la carpeta de instalación y dejar la opción por defecto.

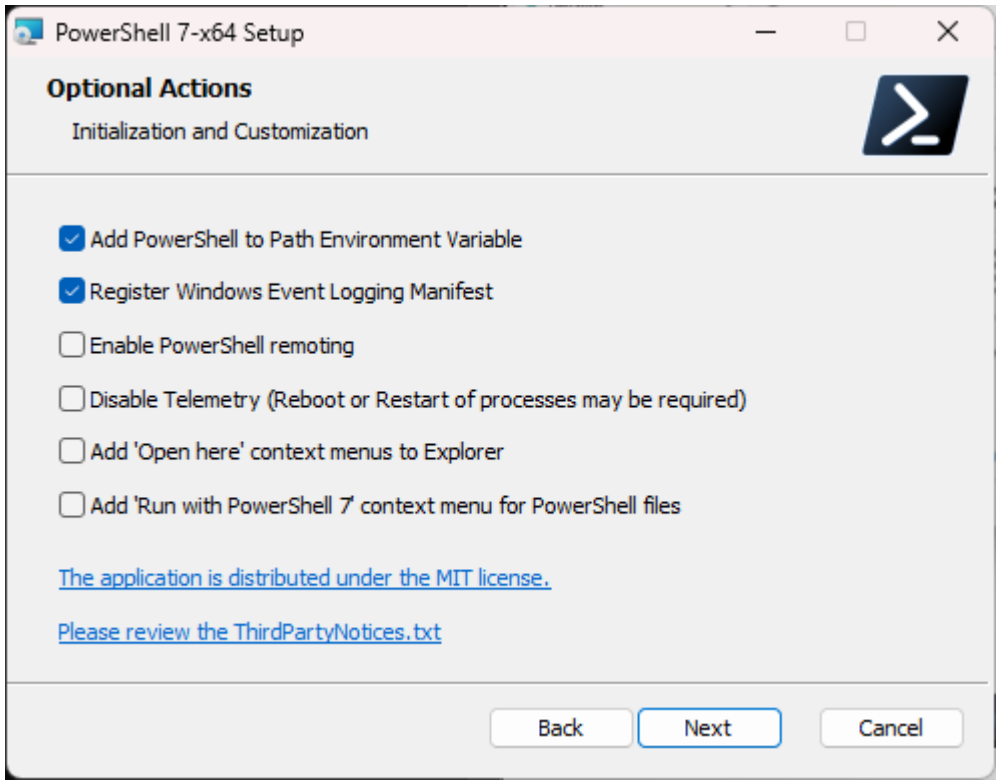

Ilustración 8 selecion de caracteristicas PowerShell al PATH

Debemos activar la casilla para que se agregue **PowerShell al PATH** del sistema, lo que permitirá ejecutarlo desde cualquier terminal.

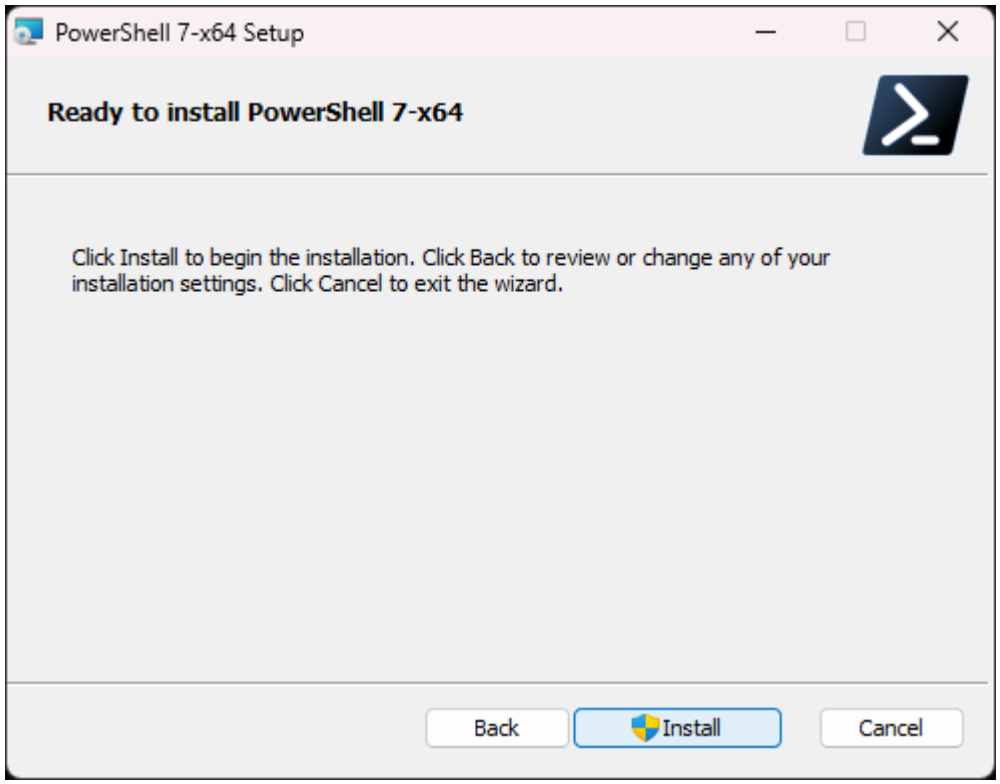

Ilustración 9 instalar para dar marcha a todo el proceso

Hacer clic en **Install** y esperar a que termine la instalación.

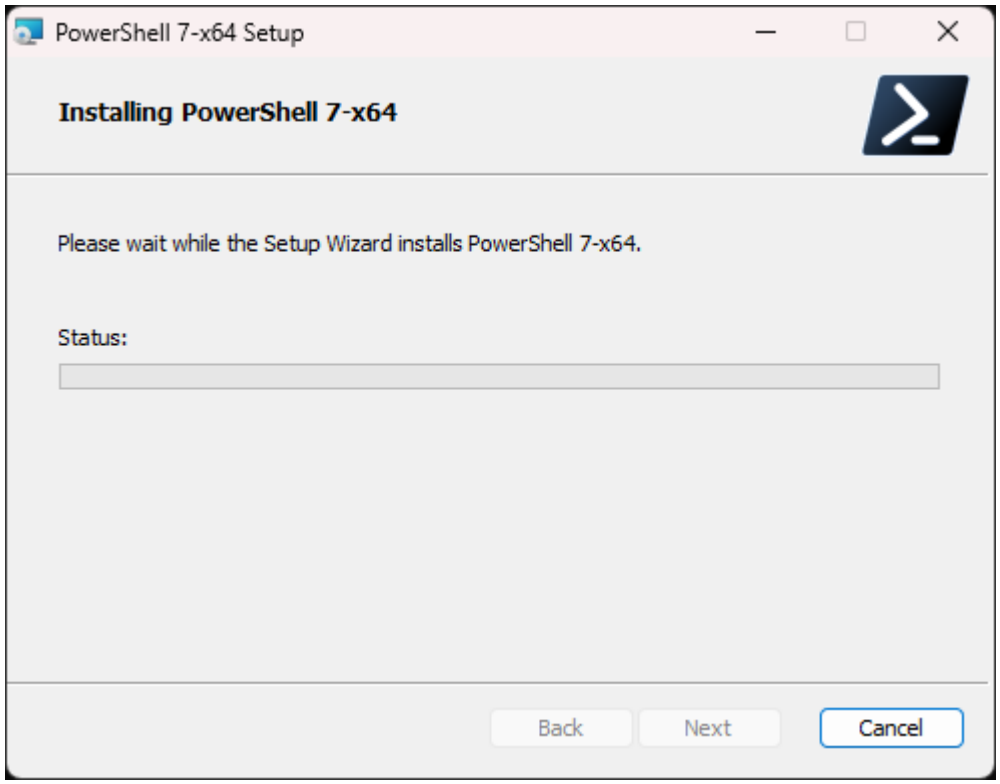

Ilustración 10 estado de carga de la instalacion

Una vez finalizado, presionar **Finish**.

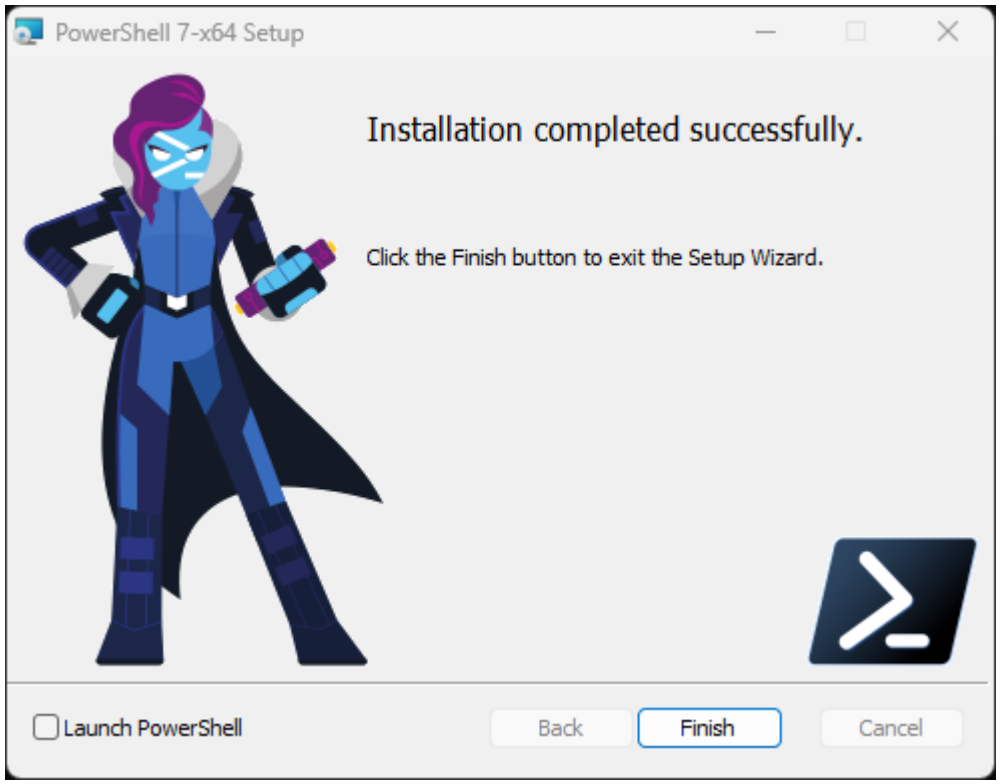

Ilustración 11 proceso de instalacion terminado

2. INSTALACION METASPLOITABLE_3

Ya instaladas las herramientas procedemos ha realiza la instalación de nuestras maquinas **metasploitable_3** por medio de códigos! Luego de haber verificado que nos haya cargado el **vagrant**

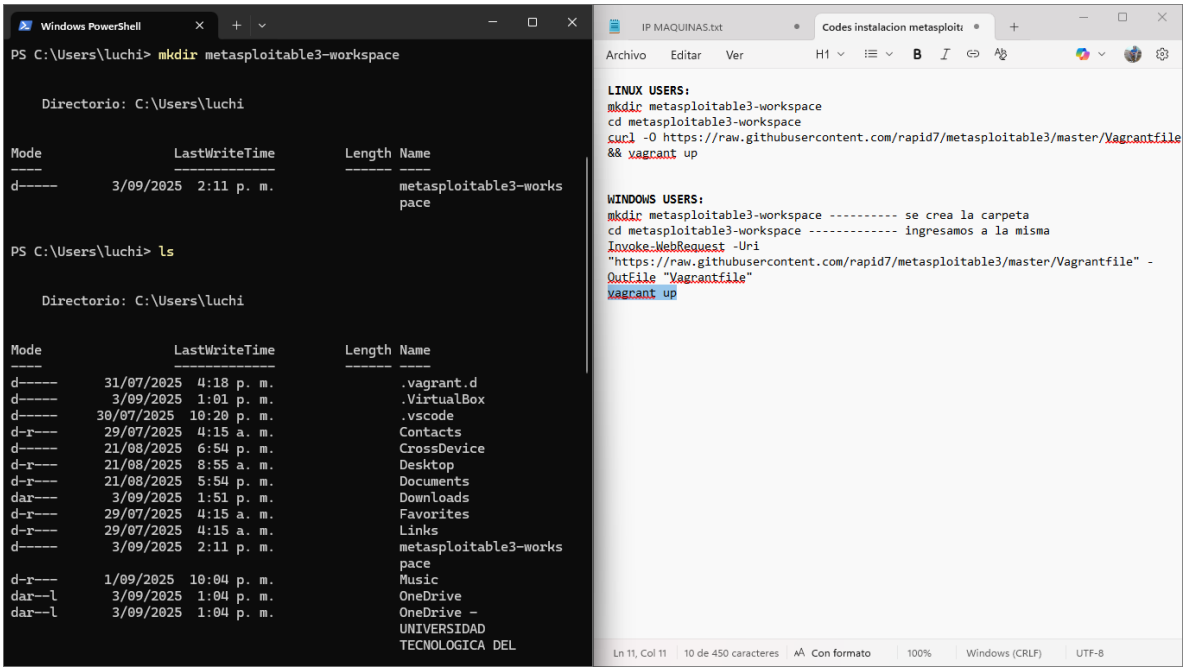

Ilustración 12 confirmacion de la existencia de carpentas

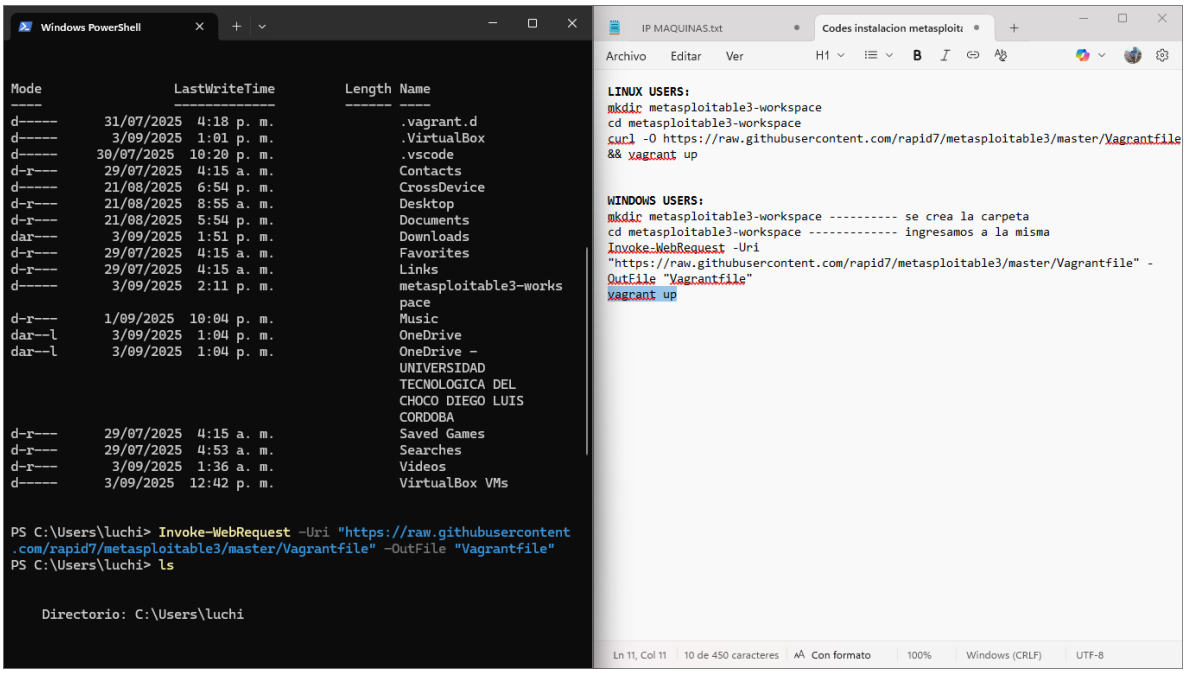

Ilustración 13 carga de codigos en el comando CMD para instalacion metasploit3

Como vemos en la imagen del block de notas, vemos que se encuentran ya documentadas brevemente las cortas líneas del código de instalación. Lo primero es crear la carpeta **metasploitable3-workspace** luego con un **cd metasploitable3-workspace** ingresamos a ella. Para posteriormente ingresar este comando: (**Invoke-WebRequest-Uri"https://raw.githubusercontent.com/rapid7/metasploitable3/master/Vagrantfile" -OutFile "Vagrantfile")** por ultimo **vagrant up** es el más importante en la instalación de **Metasploitable3**, ya que es el que construye y arranca la máquina virtual. Además que es lo que da marcha a:

- Lee la configuración definida en el archivo **Vagrantfile**.
- Descarga las imágenes necesarias (Windows Server 2008 o Ubuntu, dependiendo de la versión de **Metasploitable3**).
- Configura la máquina virtual en VirtualBox (o VMware, si está configurado).
- Instala y levanta los servicios vulnerables dentro de la máquina.

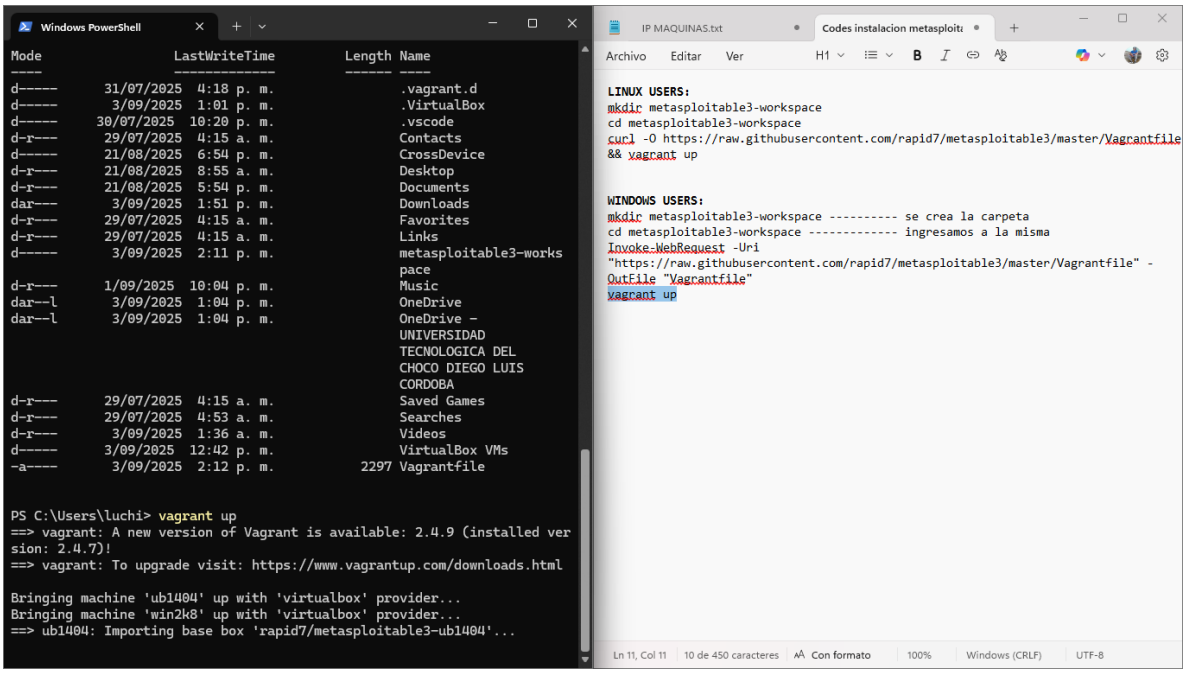

Ilustración 14 vagrant up Instala y levanta los servicios vulnerables dentro de la máquina

Como podemos apreciar aun no cargan las imágenes de las maquinas en el nuestro **virtualbox** porque se está realizando el proceso de carga y descarga

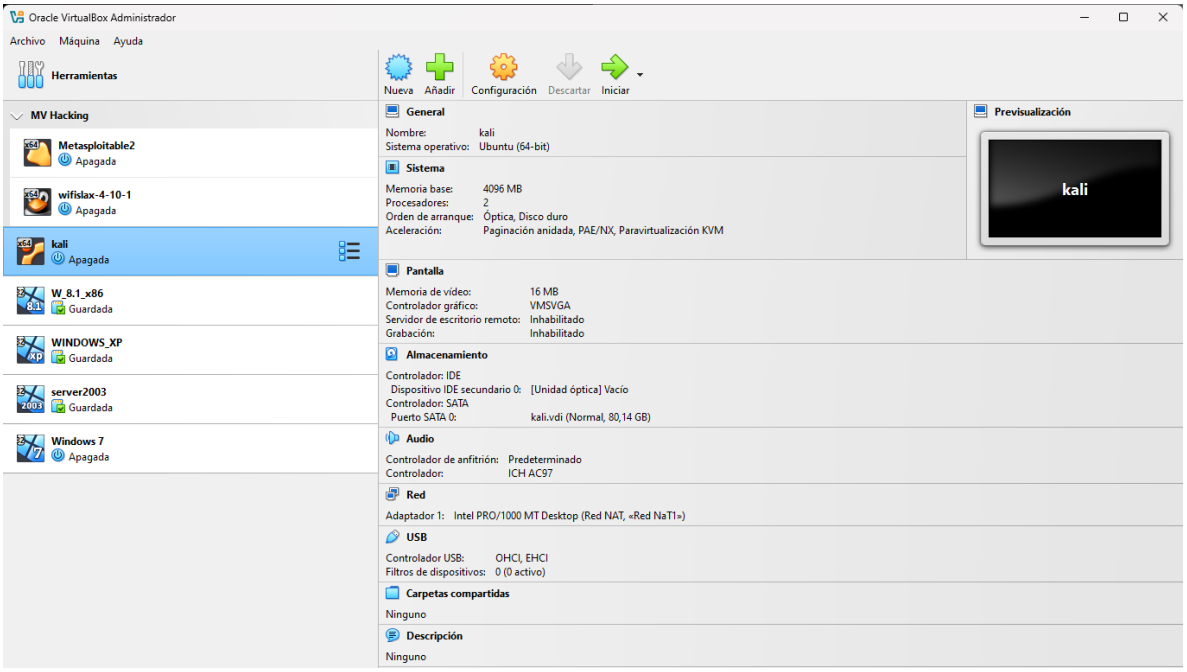

Ilustración 15 verificación de carga de dichos sistemas como máquinas virtuales aun no cargados.

En la siguiente imagen podemos apreciar los diferentes procesos de carga donde **Vagrant está levantando la máquina Metasploitable3** en VirtualBox, mostrando los mensajes de configuración de red, arranque y conexión SSH.

Ilustración 16 puesta en marcha de la carga de sistema Ubuntu y Windows

Cuando termina la carga completamente podemos hacer uso del comando **ls** en **PowerShell** dentro del directorio del usuario, donde ya aparece la carpeta

metasploitable3-workspace y el archivo **Vagrantfile**, lo que confirma que la preparación del entorno está correcta.

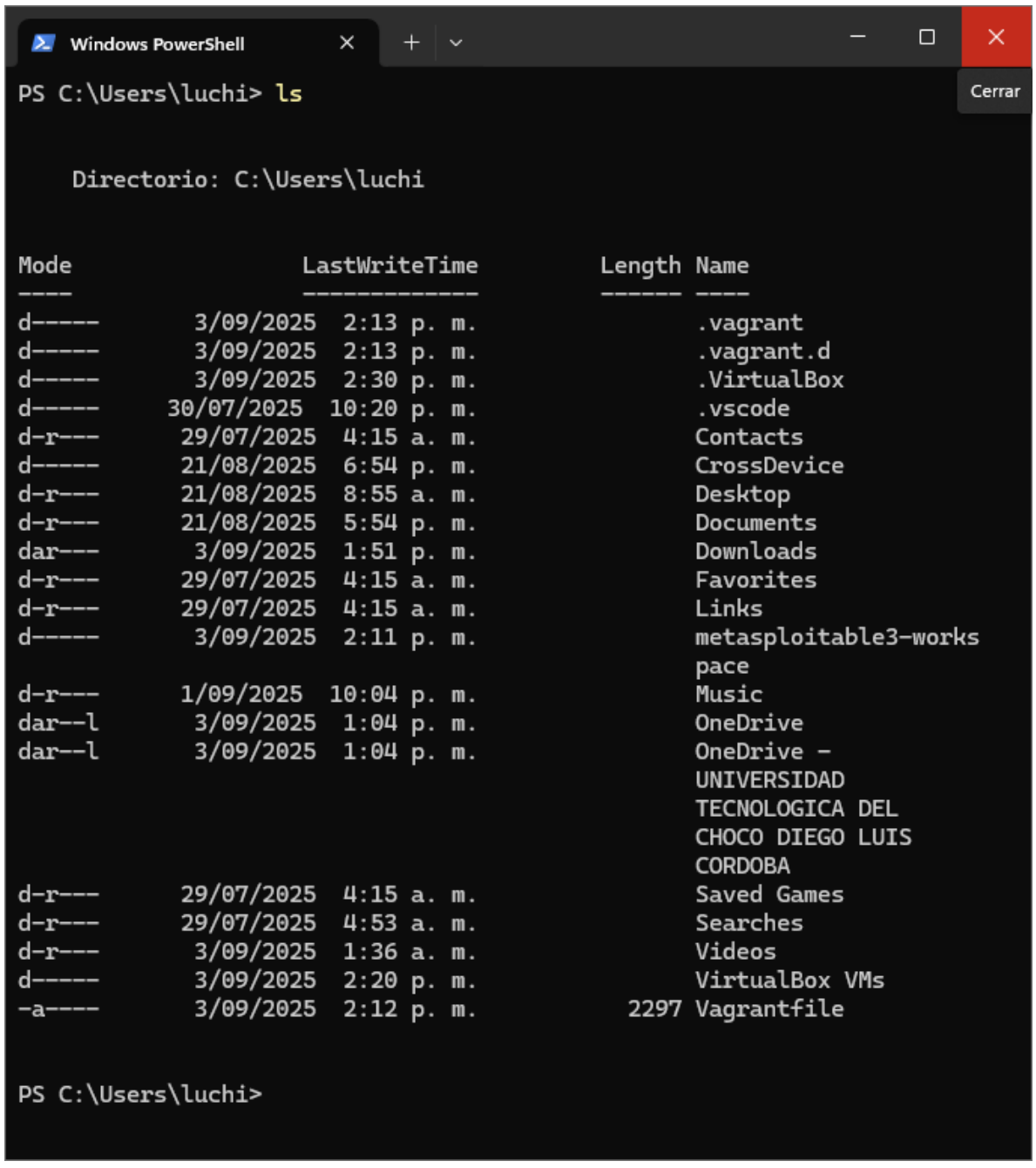

Ilustración 17 Instalacion ya cargada

En esta última imagen ya podemos apreciar las distribuciones de nuestro **METASPLOITABLE_3** ya cargadas en el virtualbox, tanto para **Ubuntu** como para **Windows** ya disponibles para ser usados

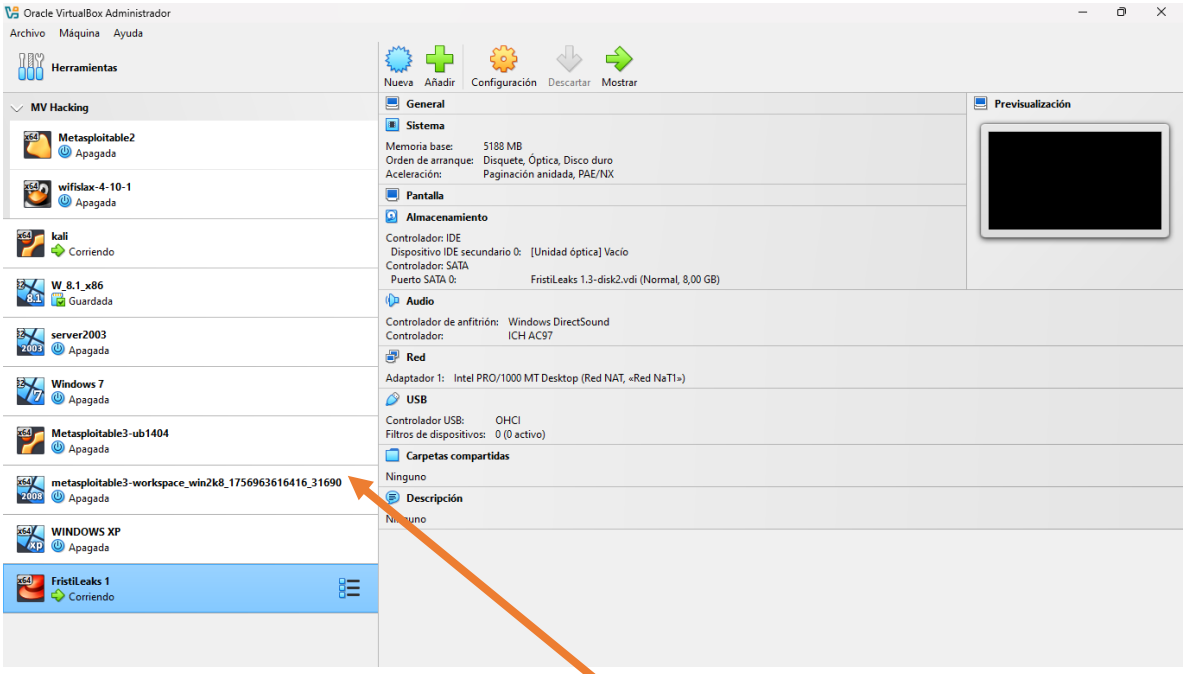

Ilustración 18 ambas maquinas cargadas en virtualbox

3. Conclusiones

Metasploitable3 es una excelente herramienta para practicar pruebas de penetración en un entorno controlado. Su instalación puede ser un reto debido a la necesidad de múltiples herramientas, pero una vez configurada, ofrece una gran variedad de vulnerabilidades ideales para el aprendizaje.