# Manual de la instalación y configuración de Metasploitable 3 en la máquina virtual de VirtualBox.

Asignatura

Seguridad y Auditoría en Redes

Estudiante

Andrés Felipe Asprilla Córdoba

Universidad Tecnológica del Chocó “Diego Luis Córdoba”

Ingeniería de Telecomunicaciones e Informática

Quibdó/Chocó

# Manual de la instalación y configuración de Metasploitable 3 en la máquina virtual de VirtualBox.


Docente

ING Rafael Sandoval Morales

Estudiante

Andrés Felipe Asprilla Córdoba


Asignatura

Seguridad y Auditoría en Redes


Universidad Tecnológica del Chocó “Diego Luis Córdoba”

Ingeniería de Telecomunicaciones e Informática

Quibdó/Chocó

Universidad Tecnológica del Chocó
Diego Luis Córdoba

**Tabla de contenido**

Universidad Tecnológica del Chocó
Diego Luis Córdoba

**Tabla de ilustraciones.**

## Introducción

El presente manual documenta de manera detallada el proceso de instalación y configuración de **Metasploitable 3** en entornos virtualizados, utilizando como principales herramientas **VirtualBox**, **Vagrant** y los recursos disponibles en el repositorio oficial de GitHub. Este procedimiento tiene como propósito fundamental la creación de un entorno controlado y vulnerable, ideal para el desarrollo de pruebas de penetración, auditorías de seguridad informática y ejercicios prácticos de hacking ético.

El despliegue de Metasploitable 3 permite a estudiantes y profesionales de la ciberseguridad experimentar con un laboratorio realista, en el cual se pueden identificar vulnerabilidades, evaluar riesgos y aplicar técnicas de protección frente a ciberataques. De esta manera, se fortalece la comprensión de los mecanismos de defensa, así como la preparación ante escenarios que afectan de manera directa a las pequeñas y medianas empresas (pymes), que suelen ser más vulnerables frente a incidentes de seguridad por limitaciones de recursos tecnológicos.

Este manual constituye, entonces, una guía práctica y estructurada que integra conocimientos de virtualización, automatización y administración de sistemas, ofreciendo una herramienta pedagógica para la formación en **ciberseguridad ofensiva y defensiva**.

# Objetivos

## Objetivo General

Implementar la instalación y configuración de Metasploitable 3 en un entorno virtualizado mediante el uso de VirtualBox y Vagrant, con el fin de disponer de una plataforma controlada que facilite la práctica de pruebas de penetración y la detección de vulnerabilidades en el marco de la ciberseguridad.

### *Objetivos Específicos*

- **Descargar, instalar y configurar VirtualBox** como hipervisor tipo 2 para la gestión de máquinas virtuales.
- **Instalar y configurar Vagrant** como herramienta de automatización en la construcción de entornos virtuales.
- **Implementar el repositorio oficial de Metasploitable 3 desde GitHub**, asegurando su correcta integración con Vagrant y VirtualBox.
- **Verificar y ejecutar las máquinas virtuales vulnerables** (Ubuntu 14.04 y Windows Server 2008) para confirmar la disponibilidad del entorno de pruebas en ciberseguridad.

## Alcances

- El manual ofrece una **guía clara y paso a paso** para la instalación de Metasploitable 3, asegurando que cualquier usuario con conocimientos intermedios en informática pueda reproducir el procedimiento de manera exitosa.
- Permite **comprender el uso de herramientas de virtualización (VirtualBox)** y **automatización de entornos (Vagrant)**, fundamentales en escenarios actuales de infraestructura tecnológica y prácticas de ciberseguridad.
- Brinda un **entorno controlado de laboratorio**, seguro y aislado del sistema operativo principal, para realizar pruebas de penetración y auditorías sin comprometer equipos de producción o datos sensibles.
- Contribuye al **fortalecimiento de competencias en ciberseguridad ofensiva y defensiva**, ya que el entorno desplegado puede ser utilizado para la práctica de técnicas de explotación, detección y mitigación de vulnerabilidades.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

# Instalación y configuración de Metasploitable 3 en VirtualBox

La correcta instalación y configuración de entornos de práctica constituye un paso fundamental en la formación en ciberseguridad. En este apartado se presenta el procedimiento para implementar **Metasploitable 3** dentro de **VirtualBox**, un hipervisor de tipo 2 ampliamente utilizado para la gestión de máquinas virtuales. El propósito es disponer de un entorno vulnerable y controlado que permita la realización de pruebas de penetración, auditorías de seguridad y ejercicios de hacking ético, garantizando que la experimentación se realice sin riesgos para el sistema operativo principal ni para redes de producción.

## Descarga del instalador de VirtualBox

Durante la primera etapa del proceso, accedí a la página oficial de VirtualBox ([https://www.virtualbox.org](https://www.virtualbox.org)) y seleccioné la opción correspondiente al sistema operativo Windows desde la sección "Windows hosts". Esta descarga me permitiría obtener el instalador ejecutable necesario para iniciar la instalación del software de virtualización.

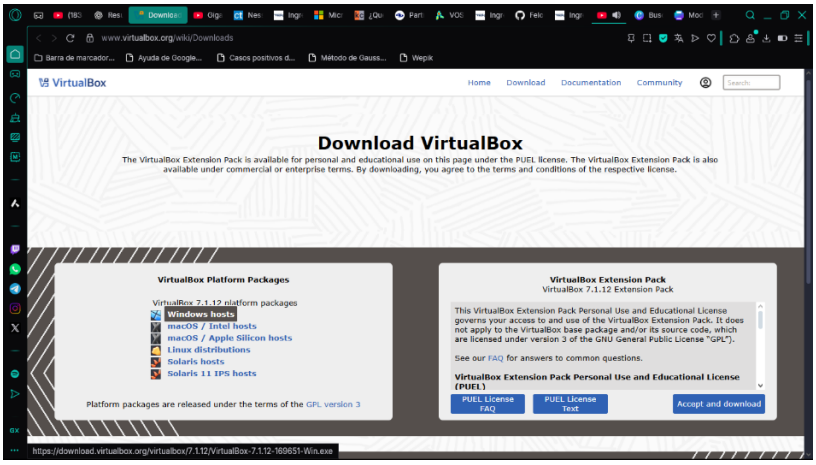


*Ilustración 1Version de virtualBox*

## *Guardando el archivo de instalación*

Una vez seleccionada la versión adecuada para Windows, el navegador me mostró la ventana de descarga. Elegí la carpeta "Descargas" como ubicación para guardar el archivo `VirtualBox-7.1.12-169651-Win.exe`, asegurándome de tener acceso rápido al instalador.

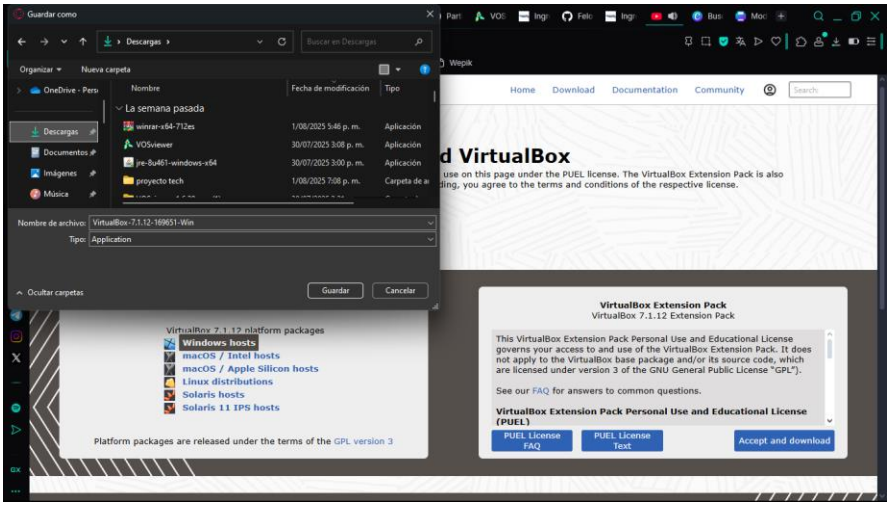


*Ilustración 2Guardando instalador de VirtualBox*

***Inicio del asistente de instalación***

Después de que la descarga finalizara, abrí el instalador. En esta imagen se muestra la pantalla de bienvenida del asistente de instalación de Oracle VirtualBox. Aquí hice clic en “Next” para continuar con la configuración paso a paso.

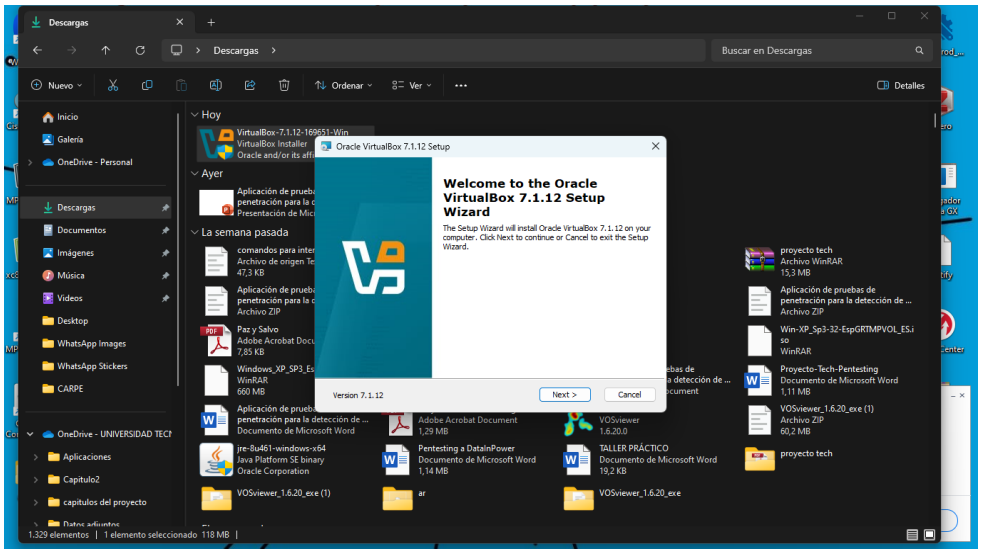


*Ilustración 3Ejecutando el instalador de VirtualBpx*

***Aceptación de los términos de licencia***

El instalador me solicitó aceptar los términos de la licencia GNU GPL v3. Leí los puntos principales y seleccioné la opción "I accept the terms in the License Agreement" para continuar con la instalación del software de forma legal y segura.

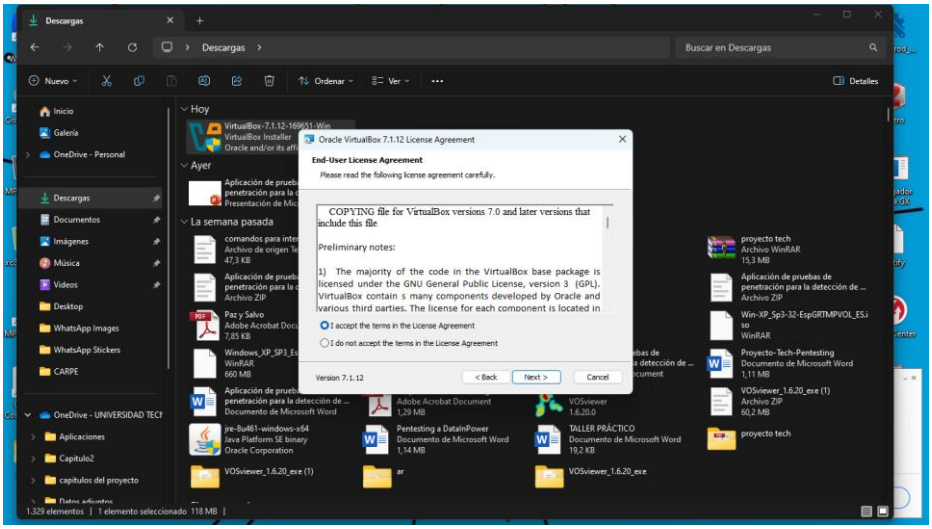


*Ilustración 4Aceptando los términos y condiciones*

## *Configuración personalizada de la instalación*

En esta etapa, revisé las opciones avanzadas de instalación. El instalador permite seleccionar características adicionales como soporte USB, redes virtuales y componentes Python. Opté por dejar la configuración predeterminada para asegurarme de que se instalaran las funciones básicas necesarias para crear y gestionar máquinas virtuales.

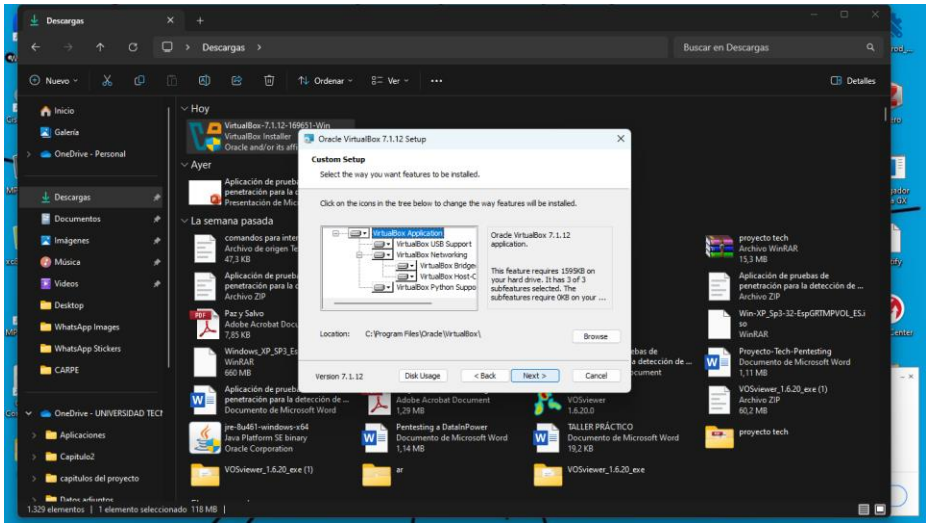


*Ilustración 5Personalizacion de la instalacion de VirtualBox*

## *Advertencia sobre interfaces de red*

Antes de continuar con la instalación final, el instalador mostró una advertencia indicando que las interfaces de red podían reiniciarse temporalmente. Esto es normal cuando se configuran adaptadores de red virtuales. Acepté haciendo clic en "Yes" para continuar sin problemas.

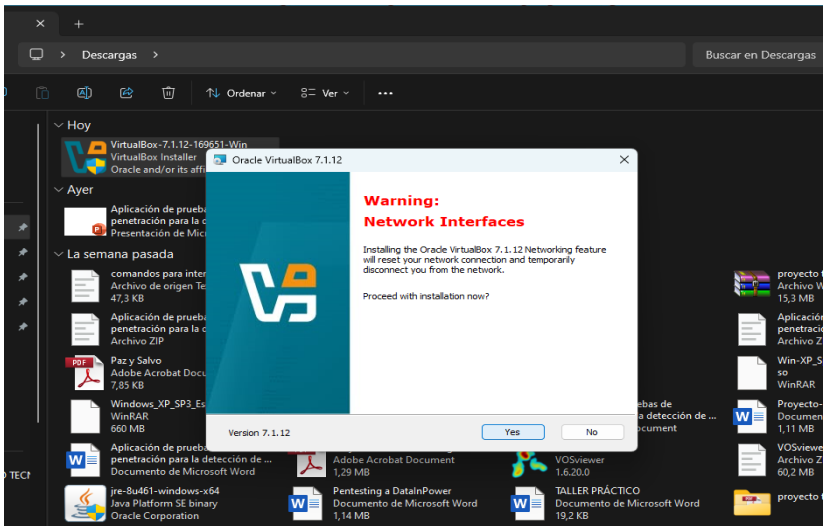


*Ilustración 6advertencia de red*

***crear accesos directos***

En la pantalla de configuración personalizada seleccioné las opciones para crear accesos directos en el menú de inicio, en el escritorio y en la barra de inicio rápido, además de registrar las asociaciones de archivos. Luego, hice clic en Next para continuar con la instalación.

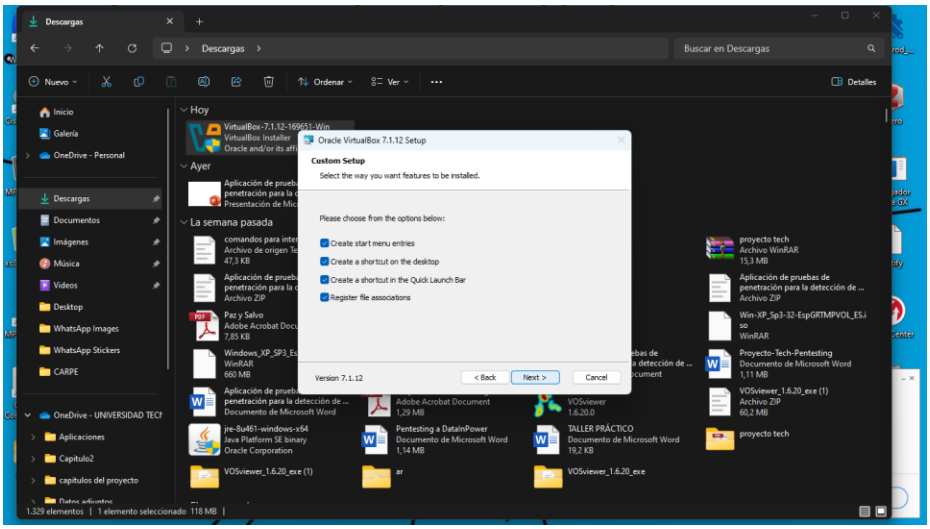


*Ilustración 7crear accesos directos*

***iniciar el proceso de instalación.***

Revisé la configuración final de la instalación de VirtualBox y confirmé que todo estaba listo para proceder. Presioné el botón Install para iniciar el proceso de instalación.

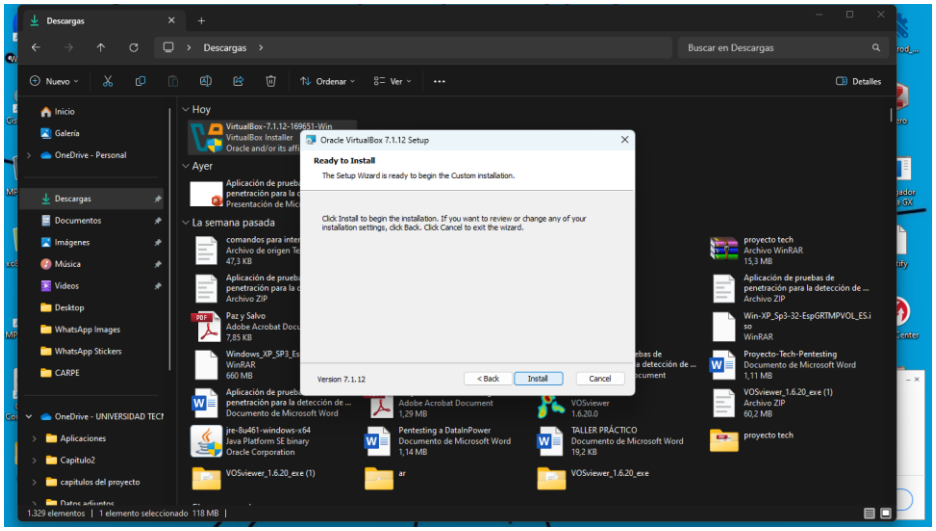


*Ilustración 8iniciar el proceso de instalación.*

## *Cargando instalación*

El asistente comenzó a instalar VirtualBox en mi equipo. En esta etapa, esperé mientras el instalador copiaba los archivos necesarios y configuraba el programa.

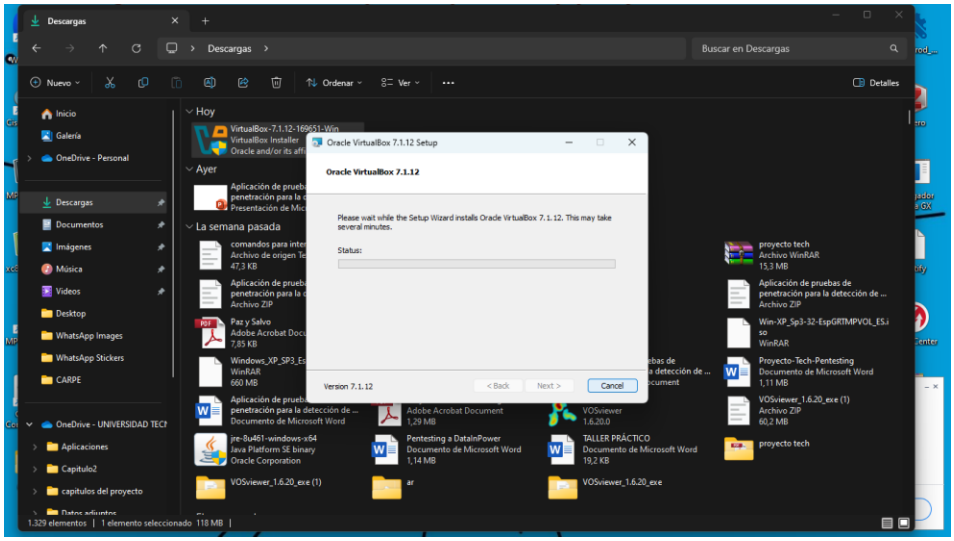


*Ilustración 9Cargando instalación*

***Finalización de la instalación.***

Durante el proceso, la instalación se interrumpió inesperadamente. El asistente me informó que el sistema no había sido modificado y que, si quería instalar el programa más tarde, debía ejecutar nuevamente el instalador. Finalmente, presioné Finish para cerrar el asistente.

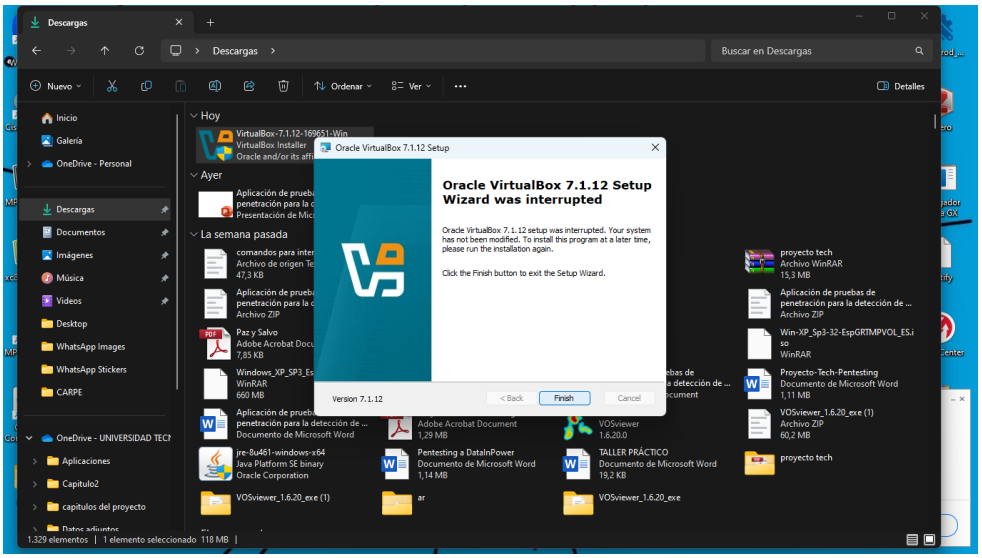


*Ilustración 10Finalizacion de la instalación de VirtualBox*

**Instalación de Vagrant**

En esta parte del proceso me dirigí a la página oficial de **HashiCorp**, específicamente a la sección de descargas de **Vagrant**. Este paso fue necesario porque Vagrant es una herramienta fundamental para la construcción y administración de máquinas virtuales de forma automatizada, lo cual resulta indispensable en la instalación de **Metasploitable 3**.

En la siguiente imagen se observa que seleccioné la versión correspondiente al sistema operativo **Windows (AMD64)** para proceder con la descarga del instalador. Este archivo es el que posteriormente me permitirá instalar Vagrant en mi equipo y garantizar que pueda crear y administrar las máquinas necesarias de manera eficiente.

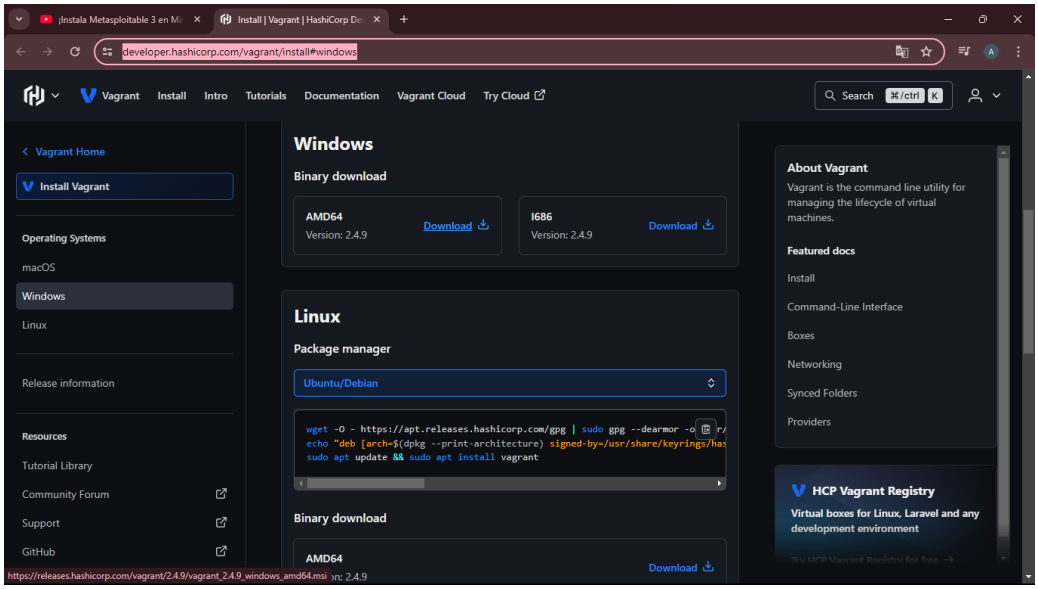


*Ilustración 11la página oficial de HashiCorp*

## *Descarga del instalador de Vagrant*

En este paso procedí a descargar el archivo instalador de **Vagrant** para Windows en su versión **2.4.9**. Tal como se observa en la parte superior derecha de la imagen, la descarga comenzó a ejecutarse y se muestra en el historial de descargas recientes del navegador.

Este procedimiento fue fundamental porque garantiza que tendré el instalador disponible en mi equipo para ejecutarlo más adelante. Es importante destacar que la descarga puede tardar algunos minutos, dependiendo de la velocidad de conexión a internet, ya que el archivo pesa más de 300 MB. Una vez finalizada la descarga, el siguiente paso será abrir este instalador para continuar con la configuración de la herramienta en mi sistema.

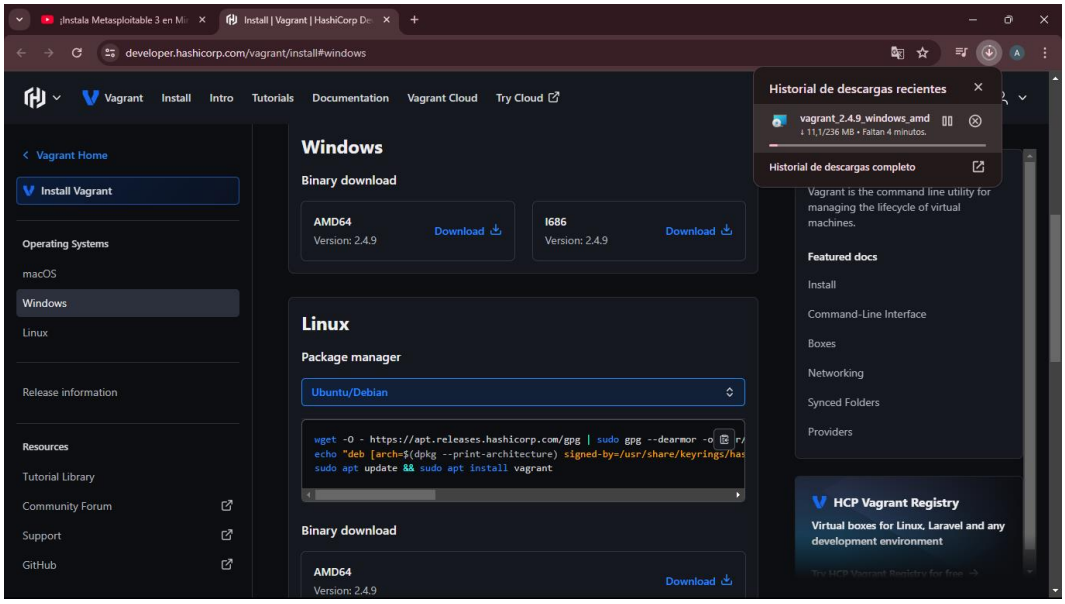


*Ilustración 12a descargar el archivo instalador de Vagrant*

***Instalación de Vagrant – Aceptación de términos de licencia***

En este punto, una vez finalizada la descarga del instalador de **Vagrant**, procedí a ejecutarlo en mi equipo. Como se aprecia en la imagen, se abrió el asistente de instalación en el cual fue necesario aceptar los términos y condiciones de la licencia. Para poder continuar con el proceso marqué la casilla **"I accept the terms in the License Agreement"** y posteriormente seleccioné la opción **Install**.

Este paso es importante porque valida legalmente el uso del software en mi equipo y permite que se inicie la instalación de los archivos necesarios. Sin aceptar este acuerdo, el instalador no permite avanzar. Con ello, se da inicio a la configuración de Vagrant en el sistema operativo Windows, asegurando que la herramienta quede correctamente instalada para la administración de máquinas virtuales.

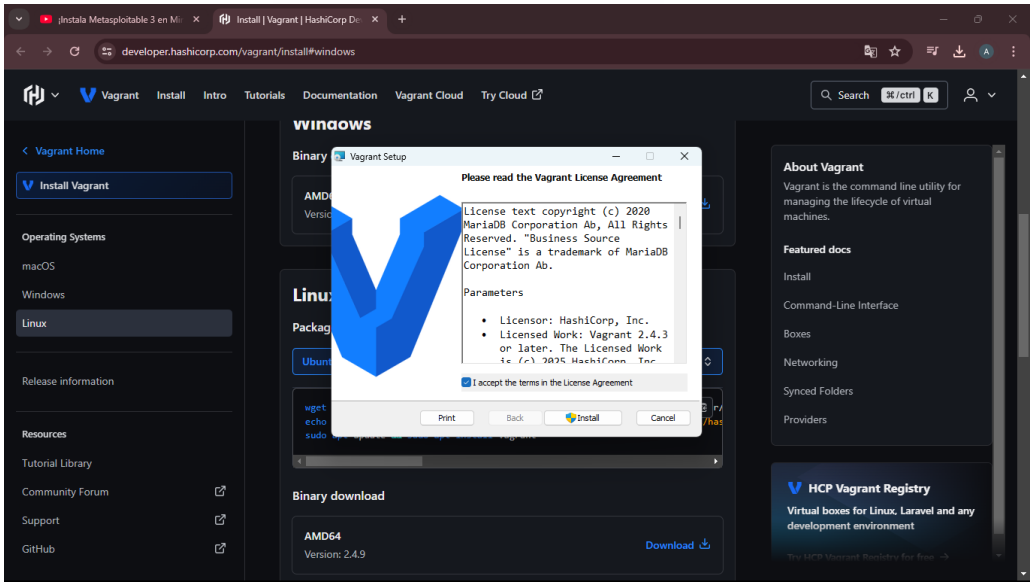


*Ilustración 13Aceptación de términos de licencia*

***Instalación de Vagrant – Proceso en ejecución***

Después de aceptar los términos de la licencia y dar inicio al instalador, comenzó el proceso de instalación de **Vagrant** en mi equipo. En la ventana del asistente, como se observa en la imagen, se muestra la barra de progreso que indica cómo se van copiando los archivos necesarios en el sistema.

Este paso es fundamental porque asegura que todos los componentes de Vagrant se integren correctamente en el sistema operativo. Durante esta fase no es necesario realizar ninguna otra acción más que esperar a que el proceso finalice. Una vez completada la instalación, la herramienta quedará lista para ser utilizada en la configuración y despliegue de la máquina virtual de **Metasploitable 3**.

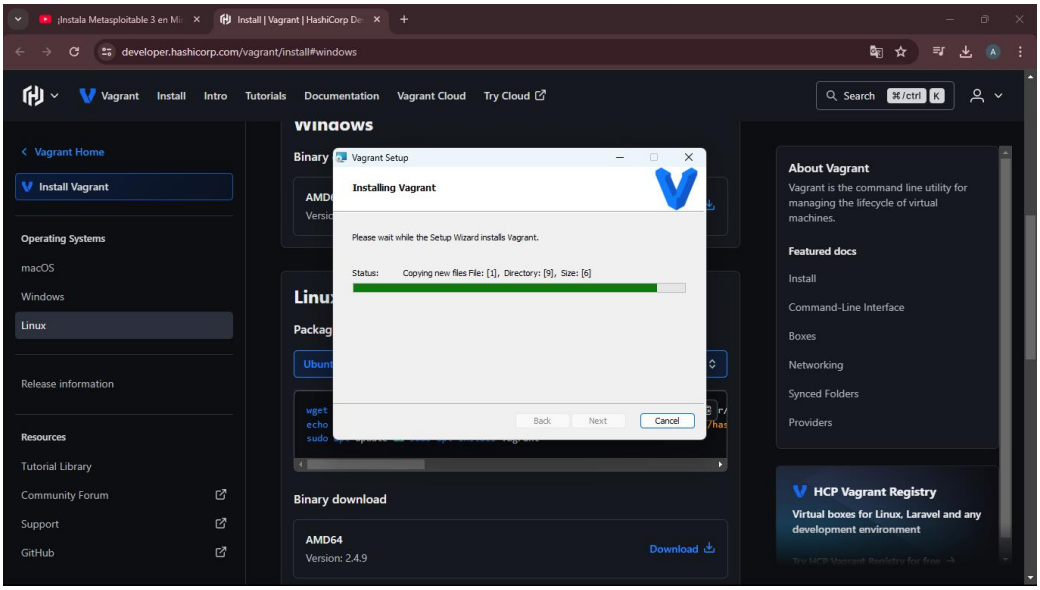


*Ilustración 14Proceso en ejecución*

### *Finalización de la instalación de Vagrant*

Una vez que el proceso de instalación terminó correctamente, el asistente mostró la ventana de finalización, como se aprecia en la imagen. Aquí se confirma que la instalación de **Vagrant** se completó con éxito en el sistema operativo. Para cerrar el asistente simplemente seleccioné la opción **Finish**, con lo cual se da por concluida esta fase.

Con este paso ya cuento con Vagrant instalado en mi equipo, lo que me permitirá continuar con la preparación del entorno necesario para desplegar **Metasploitable 3**. Este cierre marca el final del proceso de instalación básica de la herramienta y abre la posibilidad de avanzar hacia la configuración de otros programas complementarios que forman parte del entorno de pruebas.

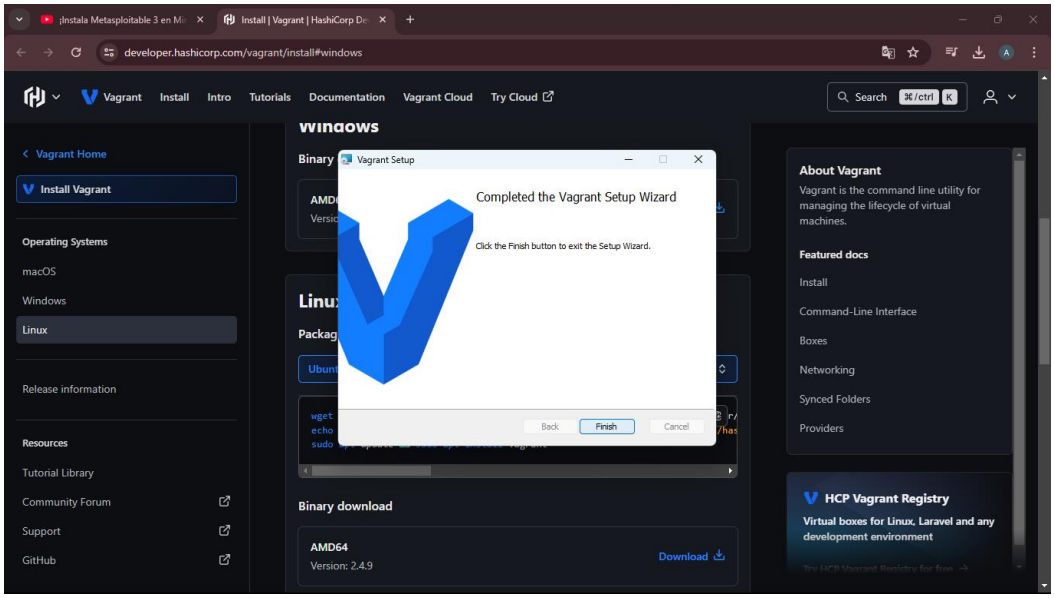


*Ilustración 15Finalización de la instalación de Vagrant*

## Descarga del repositorio de Metasploitable 3

Después de haber instalado correctamente **Vagrant**, el siguiente paso fue dirigirme al repositorio oficial de **Metasploitable 3** en GitHub. En este sitio se encuentran las instrucciones y los archivos necesarios para la creación de la máquina virtual vulnerable que se utilizará con fines de práctica en ciberseguridad.

La página muestra los comandos que deben ejecutarse dependiendo del sistema operativo utilizado. En mi caso, al trabajar sobre **Windows**, se indica la necesidad de crear un directorio llamado *metasploitable3-workspace*, ingresar en él y posteriormente descargar el archivo **Vagrantfile** mediante el comando Invoke-WebRequest. Finalmente, el proceso se completa al ejecutar vagrant up, que es el comando encargado de levantar la máquina virtual.

Este paso resulta clave, ya que conecta directamente Vagrant con los archivos del repositorio oficial y permite que la construcción de la máquina de Metasploitable 3 se realice de manera automatizada, siguiendo la configuración predefinida por los desarrolladores.

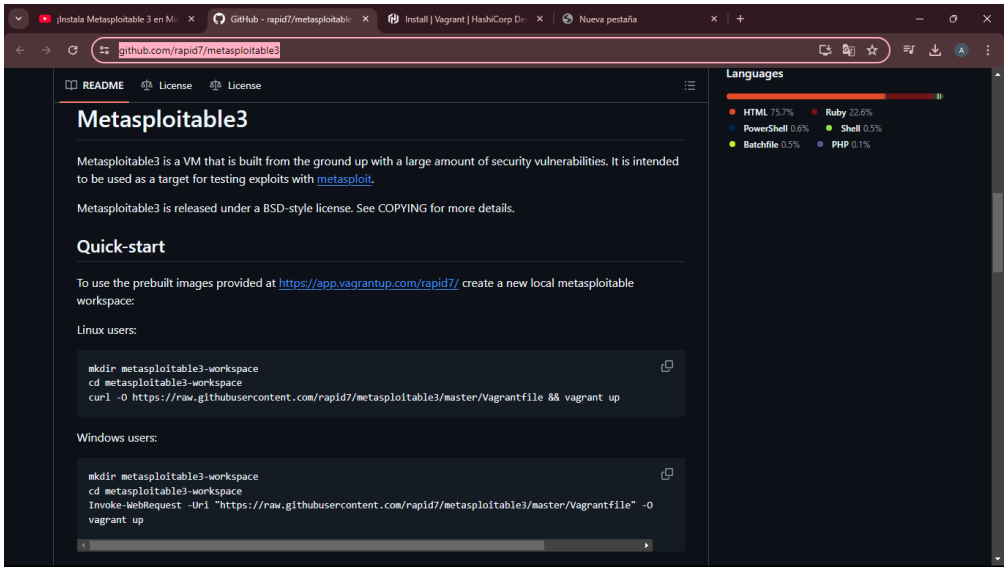


*Ilustración 16pagina de comandos que deben ejecutarse*

### *Apertura del Símbolo del sistema*

En esta parte del proceso, abrí el **Símbolo del sistema (CMD)** en Windows. Para ello, utilicé la barra de búsqueda y escribí “cmd”, lo que me mostró la aplicación correspondiente. Seleccioné la opción de **Ejecutar como administrador**, ya que es necesario contar con permisos elevados para ejecutar ciertos comandos que intervienen en la instalación y configuración de Metasploitable 3.

Este paso es esencial porque desde la terminal se van a ejecutar los comandos proporcionados en el repositorio de GitHub. A través de CMD, se crean las carpetas necesarias,

se descargan los archivos de configuración y finalmente se inicia la construcción de la máquina virtual.

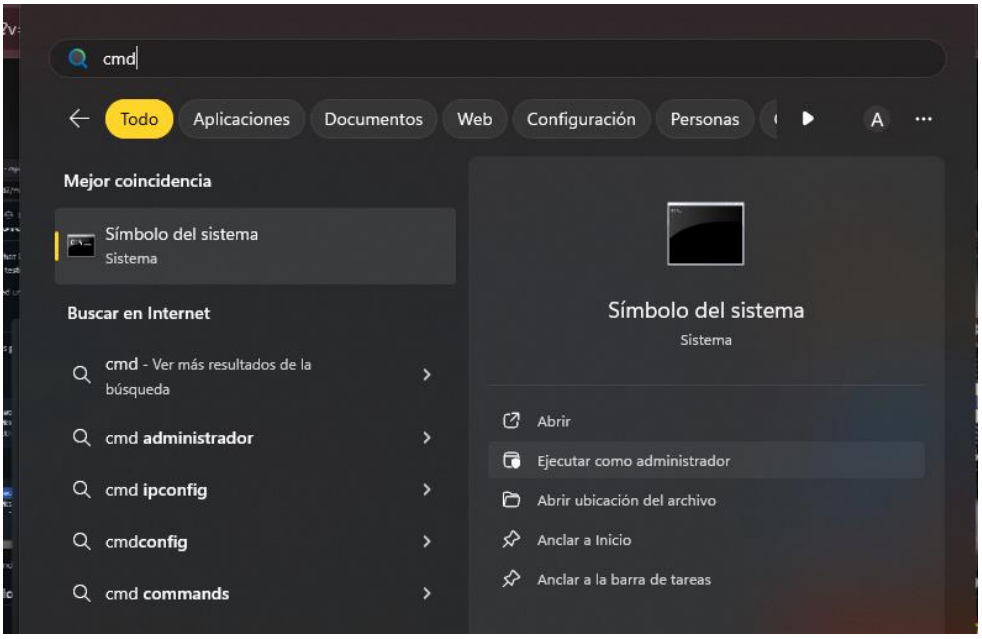


*Ilustración 17CMD*

***Acceso al directorio raíz en CMD***

Una vez abierto el **Símbolo del sistema como administrador**, lo primero que hice fue desplazarme desde la ruta inicial C:\Windows\System32 hacia el directorio raíz del disco (C:\).

Para lograrlo, utilicé el comando cd .., que sirve para retroceder un nivel en la estructura de directorios. Como en este caso estaba dentro de una carpeta del sistema (System32), tuve que ejecutar el comando dos veces para llegar finalmente al nivel principal del disco local **C:**

Este paso es importante porque desde el directorio raíz resulta más sencillo crear la carpeta de trabajo donde se descargarán y configurarán los archivos necesarios para la instalación de **Metasploitable 3**.

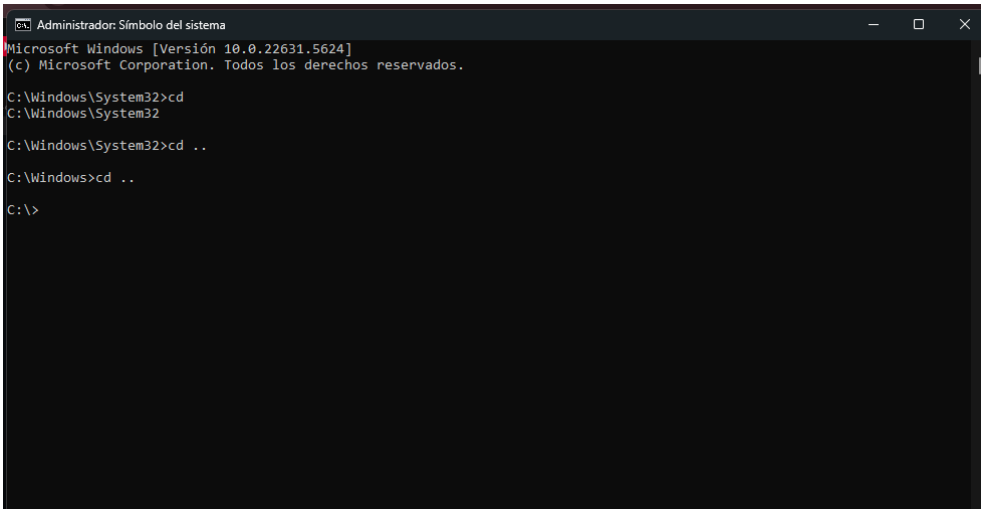


*Ilustración 18Acceso al directorio raíz en CMD*

Con el comando cd .. se retrocede un nivel en la estructura de directorios. Luego, mediante mkdir metasploitable3-workspace se crea una nueva carpeta llamada *metasploitable3-workspace*, la cual será utilizada como espacio de trabajo para organizar todos los archivos necesarios durante la instalación. Finalmente, con el comando cd metasploitable3-workspace se ingresa a la carpeta recién creada, dejando el entorno listo para continuar con los siguientes pasos de la configuración.

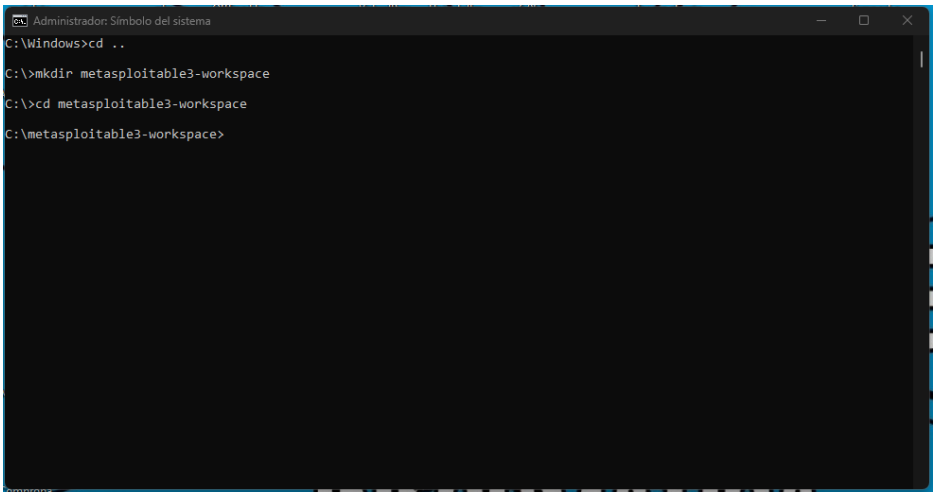


*Ilustración 19Ingreso a la carpeta*

***Windows PowerShell***

En este paso se procede a buscar y abrir **Windows PowerShell**, una herramienta necesaria para ejecutar comandos avanzados durante la instalación de **Metasploitable 3**. Desde el menú de inicio de Windows se escribe “Windows PowerShell” en la barra de búsqueda, lo que permite localizar la aplicación dentro del sistema. Una vez encontrada, se recomienda abrirla con la opción **“Ejecutar como administrador”** para garantizar que los comandos tengan los permisos adecuados y evitar errores durante la instalación y configuración del entorno.

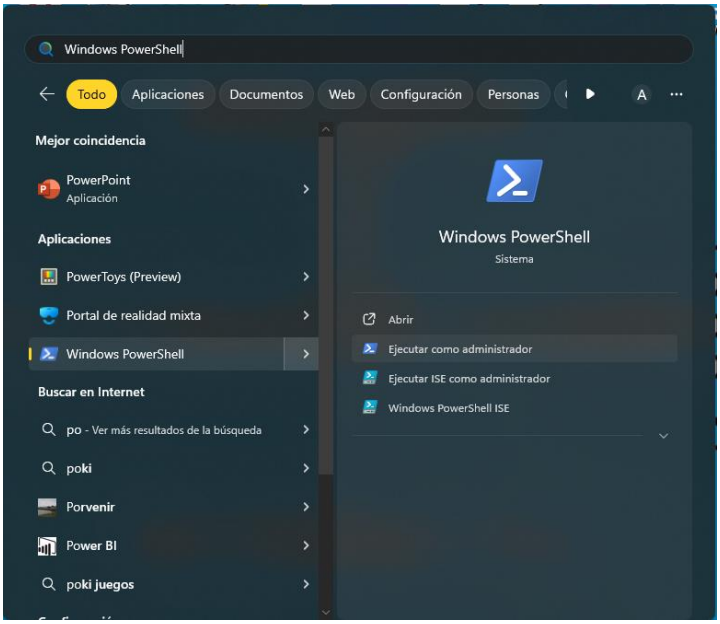


*Ilustración 20Windows PowerShell*

En este punto se utiliza **Windows PowerShell** para continuar con la instalación de **Metasploitable 3**. Primero, con el comando cd .. se retrocede un nivel en la ruta de directorios y posteriormente se accede a la carpeta de trabajo creada anteriormente mediante cd

metasploitable3-workspace. Una vez dentro, se ejecuta el comando Invoke-WebRequest para descargar desde GitHub el archivo **Vagrantfile**, el cual contiene la configuración necesaria para que Vagrant cree y gestione la máquina virtual de Metasploitable 3. El archivo descargado se guarda directamente en el directorio de trabajo con el nombre *Vagrantfile*, dejando lista la base de configuración para los siguientes pasos de la instalación.


*Ilustración 21instalación de Metasploitable 3.*

En este paso se inicia la construcción y levantamiento de las máquinas virtuales necesarias para **Metasploitable 3** utilizando **Vagrant**. Una vez descargado el archivo *Vagrantfile* en el directorio de trabajo, se ejecuta el comando vagrant up.

Este comando indica a Vagrant que inicie el proceso de creación y configuración de las máquinas virtuales definidas en dicho archivo. En este caso, el sistema comienza a levantar dos entornos: uno basado en **Ubuntu 14.04 (ub1404)** y otro en **Windows 2008 (win2k8)**, ambos gestionados con el proveedor **VirtualBox**. Este procedimiento puede tardar varios minutos, ya que implica la descarga de las imágenes necesarias y la configuración automática de cada máquina virtual.

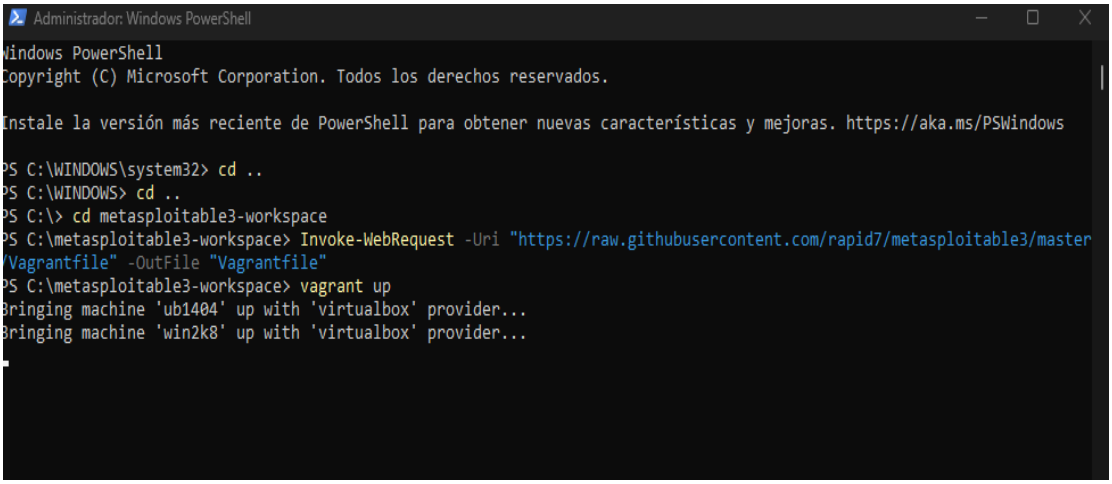


*Ilustración 22construcción y levantamiento de las máquinas virtuales*

En este punto se visualiza el resultado del proceso en **VirtualBox**, donde ya se han creado las máquinas virtuales correspondientes a **Metasploitable 3**. En la lista aparecen las máquinas levantadas desde el *Vagrantfile*: una basada en **Ubuntu 14.04 (ub1404)**, que se encuentra en ejecución, y otra basada en **Windows Server 2008 (win2k8)**, que permanece apagada.

En el panel derecho se muestra la información de configuración de la máquina seleccionada, incluyendo memoria asignada, procesador, almacenamiento, red y demás recursos virtualizados. Con esto se confirma que la instalación y despliegue de Metasploitable 3 a través de Vagrant y VirtualBox se han realizado correctamente, dejando disponibles los entornos vulnerables para pruebas de seguridad y prácticas de hacking ético.

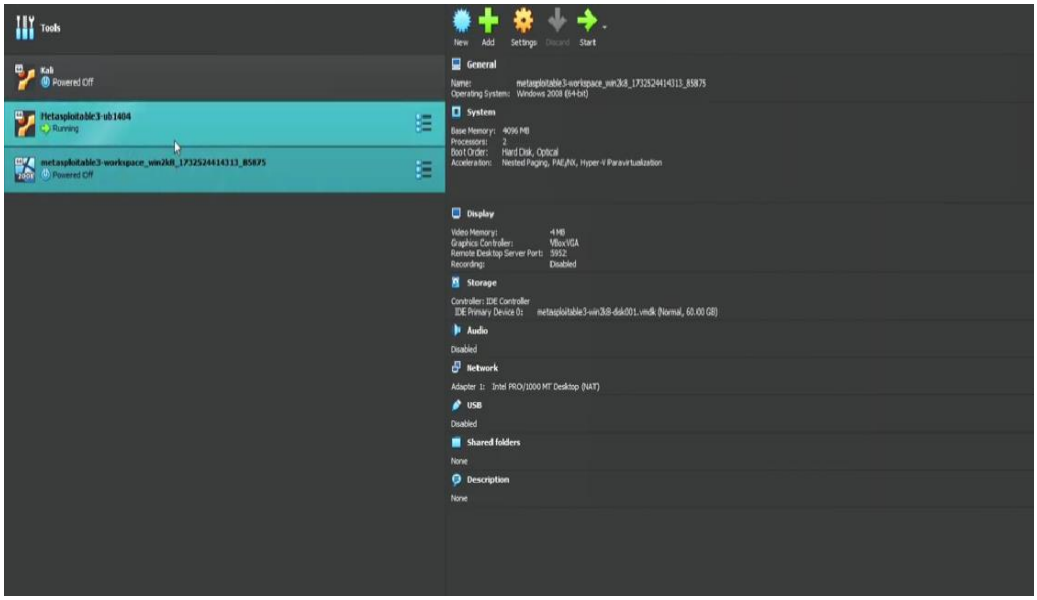


*Ilustración 23visualiza el resultado del proceso en VirtualBox*

En esta etapa se muestra la máquina virtual de **Metasploitable 3 basada en Ubuntu 14.04** ejecutándose dentro de **VirtualBox**. El sistema solicita credenciales de acceso y se realiza el inicio de sesión con el usuario predeterminado **vagrant**, que es el que Vagrant configura por defecto en estas máquinas.

Una vez ingresado, se accede al terminal del sistema operativo, confirmando que la máquina ha iniciado correctamente y que está lista para ejecutar comandos y pruebas de laboratorio. Con esto, la instalación se encuentra finalizada y el entorno de Metasploitable 3 ya puede ser utilizado para prácticas de auditoría y ejercicios de seguridad informática.

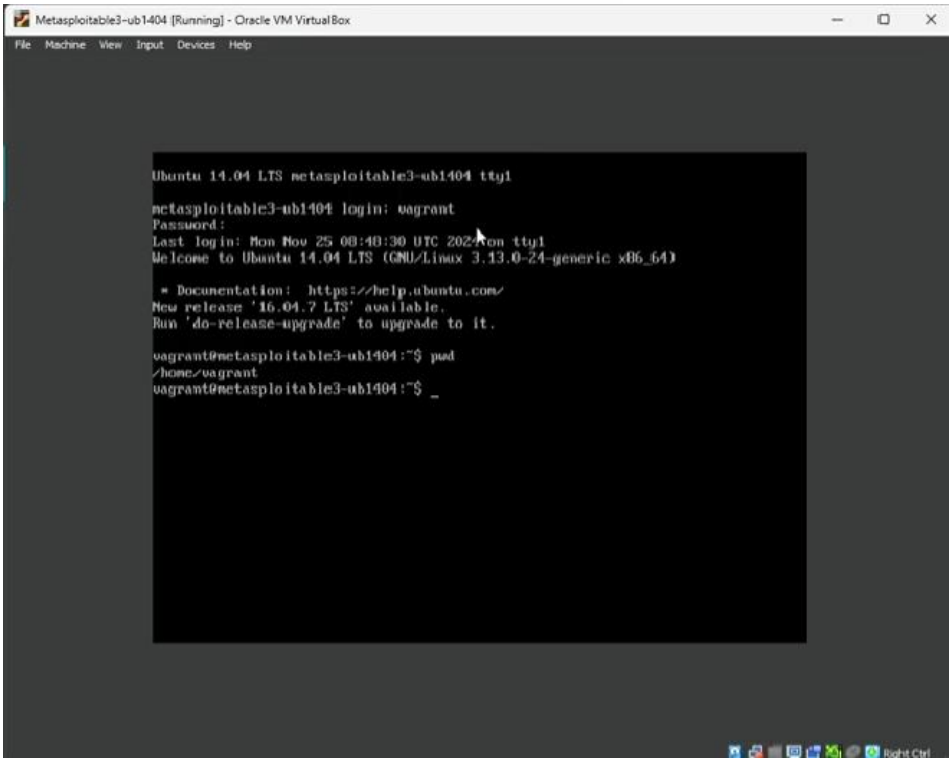


*Ilustración 24máquina virtual de Metasploitable 3 basada en Ubuntu 14.04 ejecutándose dentro de VirtualBox*

En la siguiente imagen se muestra la pantalla de inicio de sesión de **Windows Server 2008 R2 Standard** dentro de la máquina virtual que configuré. Aquí se indica que debo presionar la combinación de teclas **Ctrl + Alt + Supr** para poder acceder al sistema.

Este paso es característico de los servidores Windows y representa una medida de seguridad antes de introducir las credenciales de acceso. En el fondo se aprecia el diseño gráfico gris con líneas blancas propias de esta versión del sistema operativo, mientras que en la parte inferior se observa el logotipo y la edición correspondiente. Esta pantalla confirma máquina virtual se ejecutó correctamente y que está lista para iniciar sesión.


*Ilustración 25Ejecucion de la máquina virtual de Windows Server 2008 (win2k8),*

## Recomendaciones

1. **Revisar los requisitos de hardware** antes de iniciar la instalación, asegurando memoria RAM, almacenamiento y procesador adecuados para la ejecución fluida de las máquinas virtuales.
2. **Ejecutar siempre los comandos en modo administrador** en CMD o PowerShell para evitar errores en la instalación.
3. **Verificar la conexión a internet estable** durante la descarga de VirtualBox, Vagrant y los archivos del repositorio, dado que son de gran tamaño.
4. **Crear un directorio exclusivo para Metasploitable 3**, lo que facilita la organización y evita conflictos con otras instalaciones.
5. **Mantener actualizadas las versiones de VirtualBox y Vagrant**, comprobando compatibilidad con la versión del sistema operativo host.
6. **Utilizar el entorno únicamente con fines académicos y de investigación**, evitando su uso en redes de producción o entornos sensibles.

## Conclusión

La instalación de Metasploitable 3 constituye una herramienta esencial para el aprendizaje y la práctica de la ciberseguridad, ya que provee un entorno vulnerable diseñado específicamente para el entrenamiento en pruebas de penetración. A través del proceso documentado en este manual, se evidencia la relevancia de comprender los fundamentos de la virtualización y la automatización, integrando herramientas como VirtualBox y Vagrant para crear escenarios de práctica profesional.

Uno de los aportes más significativos de este procedimiento es la **posibilidad de experimentar de manera segura con vulnerabilidades reales**, lo que permite a estudiantes y profesionales adquirir habilidades críticas en el manejo de incidentes de seguridad. En un mundo cada vez más digitalizado, donde las pequeñas y medianas empresas son especialmente vulnerables a los ciberataques, este tipo de laboratorios se convierten en un recurso estratégico para el fortalecimiento de las capacidades de defensa.

Además, el manual fomenta el **pensamiento analítico y la resolución de problemas técnicos**, dado que la instalación puede implicar enfrentar errores o incompatibilidades que requieren soluciones prácticas. Esto desarrolla no solo competencias técnicas, sino también una mentalidad resiliente, fundamental en la labor de un especialista en ciberseguridad.