Universidad Tecnológica del Chocó
Diego Luis Córdoba
Ingeniería de Telecomunicaciones
e Informática

INSTALACIÓN METAPOSTAIBLE 3

Natalia Espinosa Mena

Universidad Tecnológica del Choco Diego Luis Córdoba
Facultad de Ingeniería
Telecomunicaciones e Informática
Quibdó – Chocó
2025

Universidad Tecnológica del Chocó
Diego Luis Córdoba
Ingeniería de Telecomunicaciones
e Informática

INSTALACIÓN METAPOSTAIBLE 3

Natalia Espinosa Mena

Docente
Rafael Sandoval Morales
Ingeniero

Universidad Tecnológica del Choco Diego Luis Córdoba
Facultad de Ingeniería
Telecomunicaciones e Informática
Quibdó – Chocó
2025

Tabla de contenido

Lista de ilustraciones

Universidad Tecnológica del Chocó
Diego Luis Córdoba
Ingeniería de Telecomunicaciones
e Informática

Introducción

Metasploitable es una máquina virtual diseñada específicamente para practicar técnicas de hacking ético y pruebas de penetración en un entorno controlado. En el marco de la asignatura **Seguridad y Auditoría de Redes**, se utiliza este tipo de entornos virtuales como herramientas pedagógicas para aplicar de forma práctica los conceptos teóricos abordados en clase.

El presente informe es presentado con el objetivo documentar detalladamente el proceso de instalación de **Metasploitable 3,** de forma que se comprende fácilmente implementación.

Alcance

Esta práctica tiene como alcance realizar el proceso de instalación correcta de **Metasploitable 3**, asegurando que la máquina virtual quede completamente operativa para su uso en entornos de pruebas en la asignatura.

Universidad Tecnológica del Chocó
Diego Luis Córdoba
Ingeniería de Telecomunicaciones
e Informática

Objetivos

General: Instalar correctamente la máquina virtual **Metasploitable 3**.

Específicos:

- Investigar los requisitos y procedimientos necesarios para la instalación de Metasploitable 3.
- Documentar el paso a paso del proceso de instalación de la máquina.

Universidad Tecnológica del Chocó
Diego Luis Córdoba
Ingeniería de Telecomunicaciones
e Informática

Planteamiento del problema

El problema planteado radica en la necesidad de instalar **Metasploitable 3**, una máquina virtual que, a diferencia de otras, **no se distribuye en formato ISO** para una instalación directa. ¿Cómo llevar a cabo correctamente este proceso de instalación sin recurrir a una imagen ISO tradicional?

1 Desarrollo del problema

1.1 ¿Qué es Metasploitable?

Metasploitable 3 es una máquina virtual intencionadamente vulnerable, diseñada para ser utilizada en entornos de laboratorio con fines educativos. Su propósito principal es servir como plataforma para realizar prácticas de hacking ético, pruebas de penetración y análisis de seguridad, utilizando herramientas como Metasploit Framework.

A diferencia de otras versiones, Metasploitable 3 está construida a partir de sistemas operativos como Windows Server 2008 o Ubuntu 14.04, e incluye una variedad de servicios y aplicaciones vulnerables que permiten simular escenarios reales de ataque y defensa en redes.

1.2 Requisitos previos:

Para poder crear y ejecutar correctamente la máquina virtual **Metasploitable 3**, es necesario contar con una serie de herramientas y configuraciones previas en el sistema operativo. Estos requisitos aseguran que el proceso de construcción e instalación se realice sin errores y que la máquina virtual funcione de manera adecuada en un entorno de pruebas.

1.2.1 Vagrant:

Vagrant es una herramienta que permite automatizar la creación, configuración y administración de máquinas virtuales sobre plataformas como **VirtualBox**. En lugar de

realizar configuraciones manuales, Vagrant utiliza archivos de configuración y scripts que definen el entorno virtual deseado, lo que facilita la reproducción de entornos consistentes y estandarizados.

1.2.1.1 ¿Para qué se usó?

Vagrant se utilizó para automatizar el proceso de creación de la máquina virtual **Metasploitable 3**, gestionando la descarga de la imagen base, la configuración del entorno y la provisión de los servicios necesarios

1.2.2 **Repositorio de Git:**

El repositorio oficial de **Metasploitable 3**, disponible en GitHub, contiene todos los archivos necesarios para construir la máquina virtual. Este repositorio incluye los scripts, configuraciones y recursos que permiten automatizar la instalación utilizando herramientas como Vagrant y Packer. Enlace al repositorio: https://github.com/rapid7/metasploitable3

1.2.2.1 ¿Para qué se uso?

Se usó para obtener el archivo Vagrantfile desde el repositorio oficial, el cual permite a Vagrant crear y provisionar la máquina virtual Metasploitable 3.

1.3 Instalar vagrant

Se accede al sitio oficial de Vagrant y se selecciona la descarga correspondiente al sistema operativo Windows.

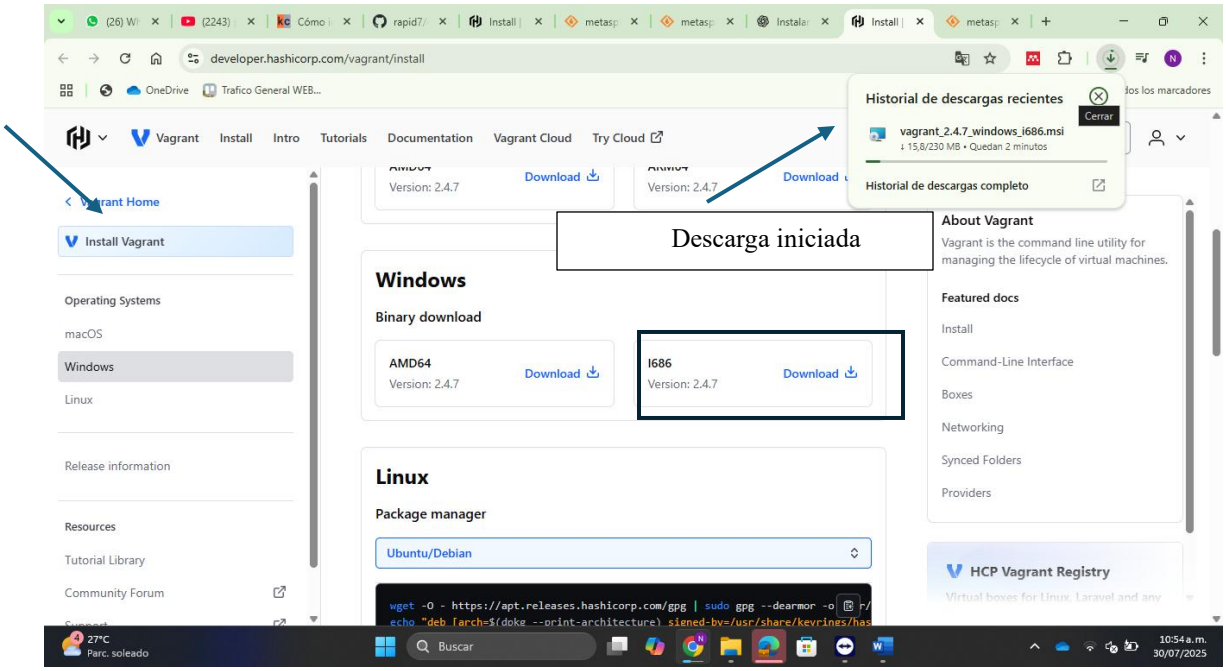


Ilustración 1 Descarga de Vangrant

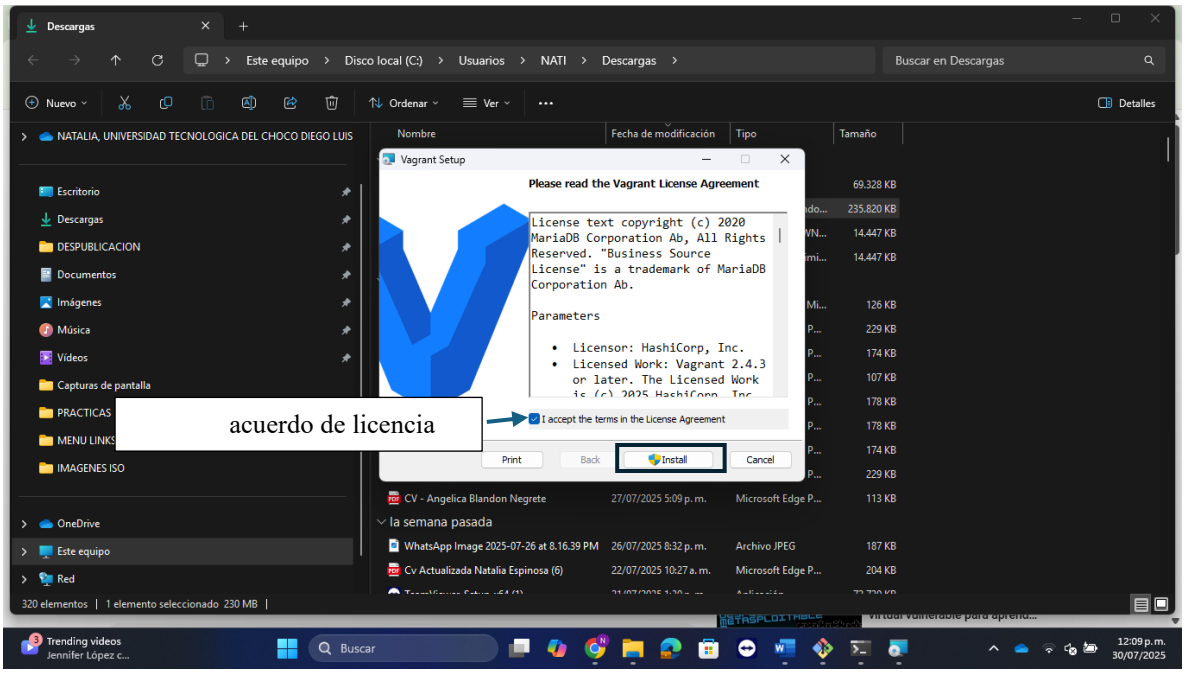


Ilustración 2 Instalación de Vagrant

Una vez completada la descarga, se ejecuta el archivo instalador. Al hacerlo, se mostrará una ventana como la que aparece en la captura.

Se acepta el acuerdo de licencia marcando la casilla correspondiente y, a continuación, se hace clic en el botón **Install**. Luego, se espera a que finalice el proceso de instalación.

Una vez completada la instalación, abrimos la consola **CMD**, nos ubicamos en el disco **C:** y ejecutamos el primer comando indicado en el archivo **README** del repositorio: mkdir metasploitable3-workspace.

Este comando crea el directorio donde se almacenarán los archivos del proyecto. Luego, accedemos a esa carpeta con: cd metasploitable3-workspace

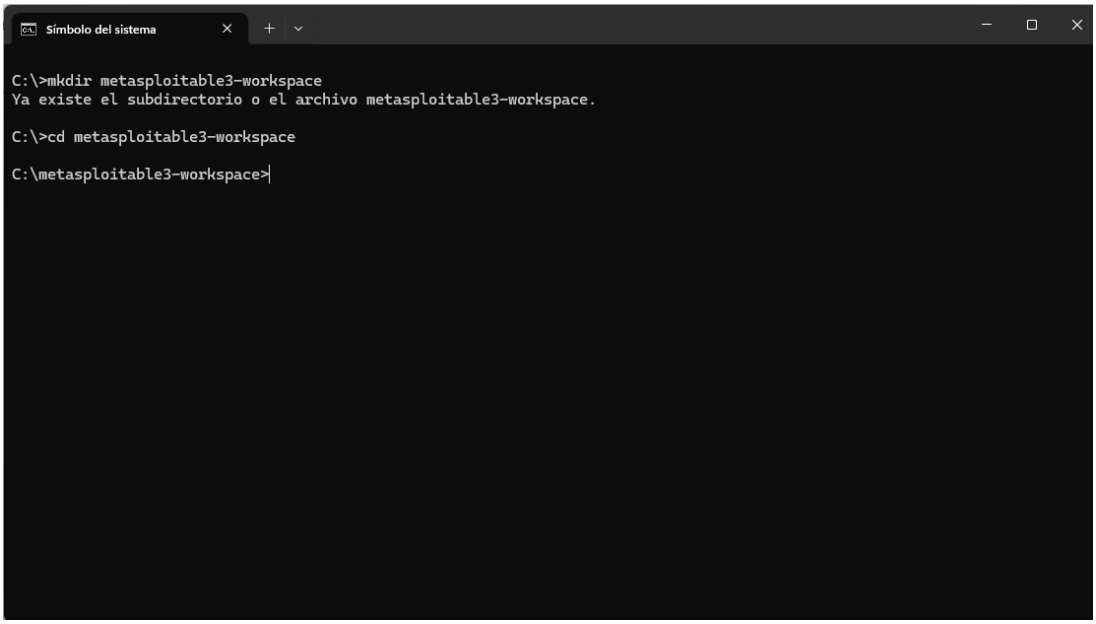


Ilustración 3 Creación del archivo

Nota: En la captura se puede observar que, al ejecutar el primer comando, aparece un mensaje indicando que la carpeta ya fue creada. Esto ocurre porque el comando se ejecutó por segunda vez, es decir, el directorio **ya había sido creado previamente**.

Ahora, tal como se indica en las instrucciones, **abrimos la terminal PowerShell**, accedemos al disco **C:** y nos ubicamos en la ruta del directorio que creamos en el paso anterior (metasploitable3-workspace).

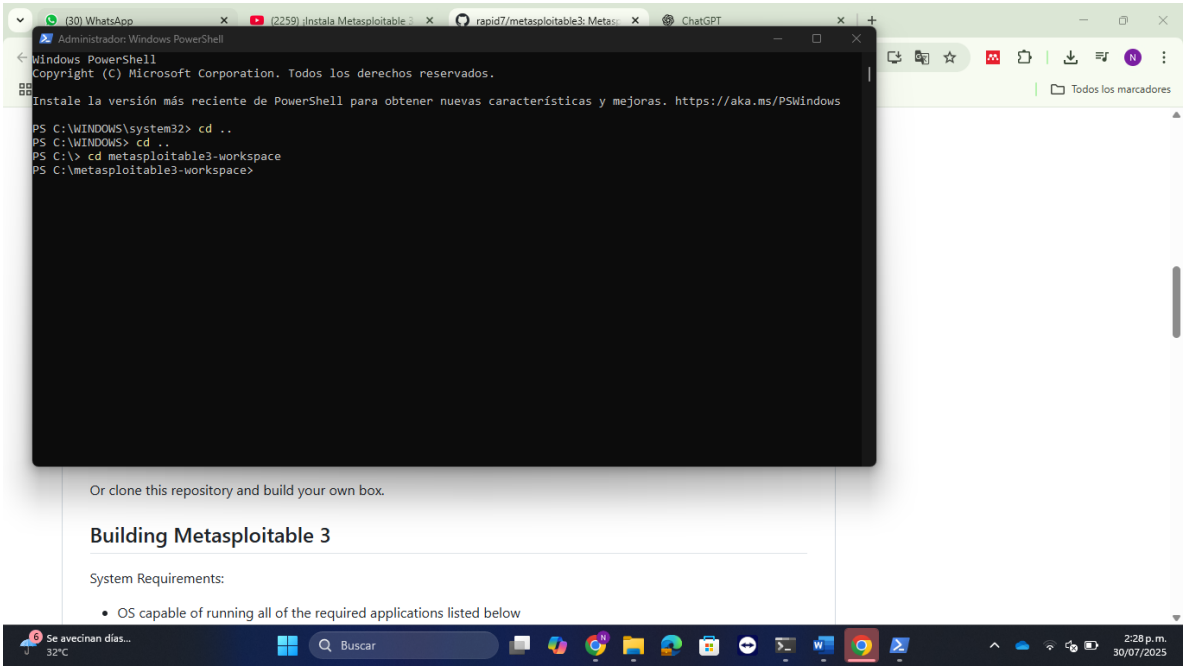


Ilustración 4 Ruta Metasploitable

Una vez dentro de la ruta correcta en PowerShell, **ejecutamos el segundo comando indicado en el archivo README del repositorio oficial**: Invoke-WebRequest -Uri "https://raw.githubusercontent.com/rapid7/metasploitable3/master/Vagrantfile" -OutFile "Vagrantfile"

Este comando descarga el archivo Vagrantfile desde el repositorio oficial de Metasploitable3 y lo guarda en la carpeta actual. El archivo Vagrantfile contiene las

instrucciones necesarias para que Vagrant pueda construir la máquina virtual automáticamente.

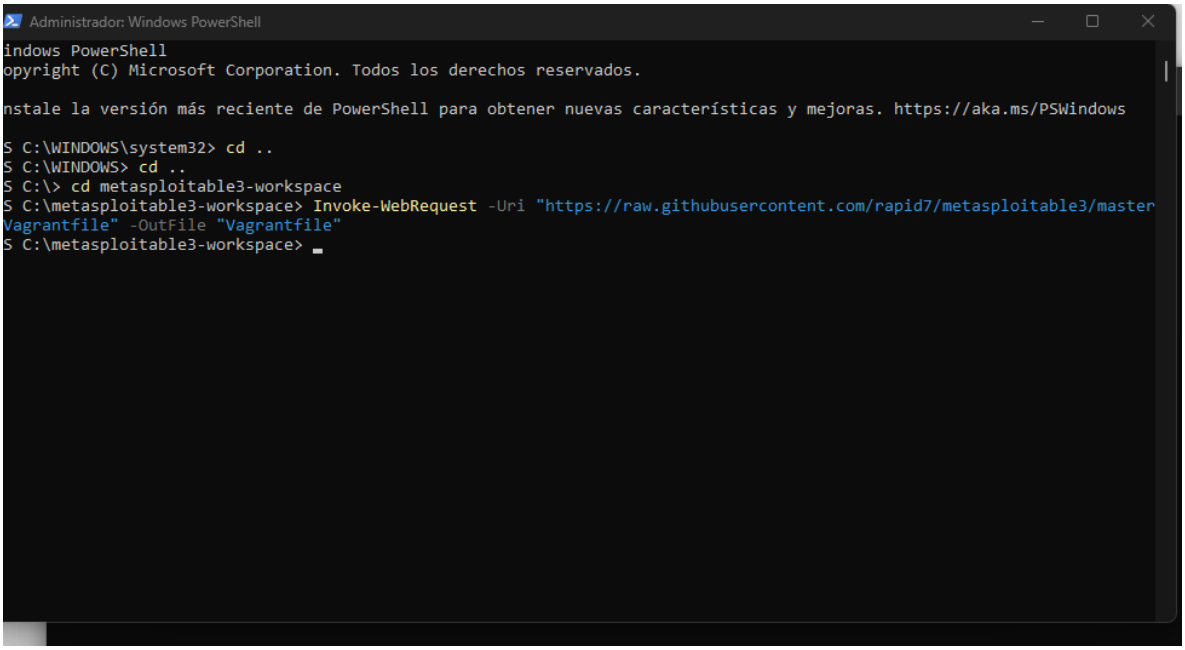


Ilustración 5 Descarga del archivo Vagrantfile

A continuación, ejecutamos el **tercer comando**: vagrant up (ver imagen 6)

Este comando inicia el proceso de creación y configuración automática de la máquina virtual utilizando el archivo Vagrantfile. Durante este paso, Vagrant descarga las imágenes necesarias e instala los servicios y configurará el entorno.

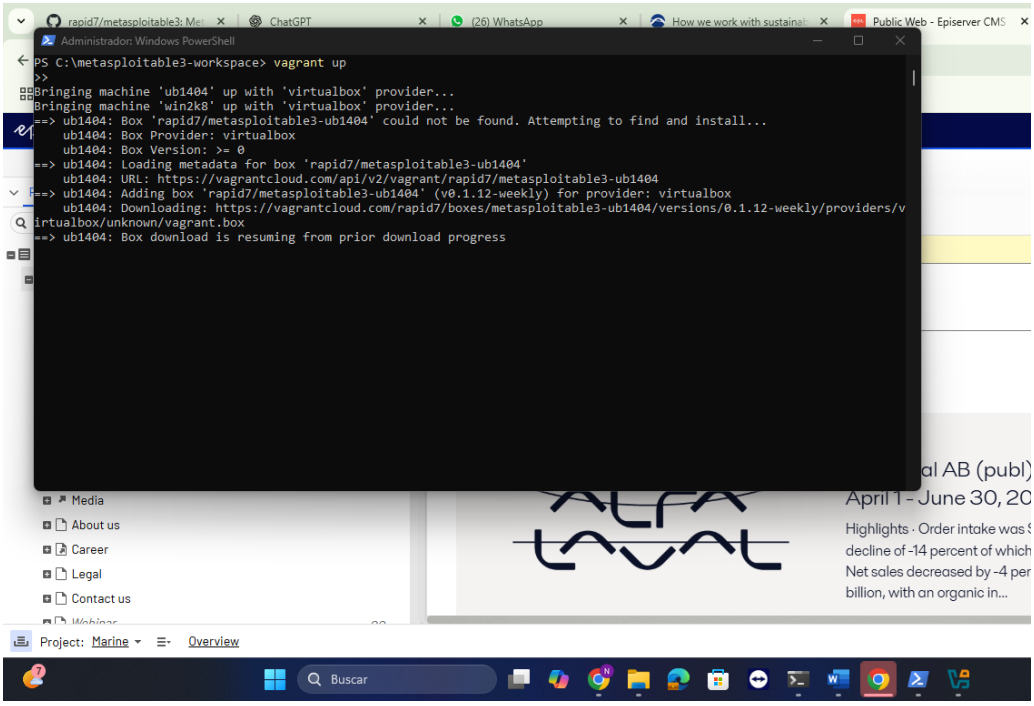


Ilustración 6 Creación de la máquina virtual con vagrant up

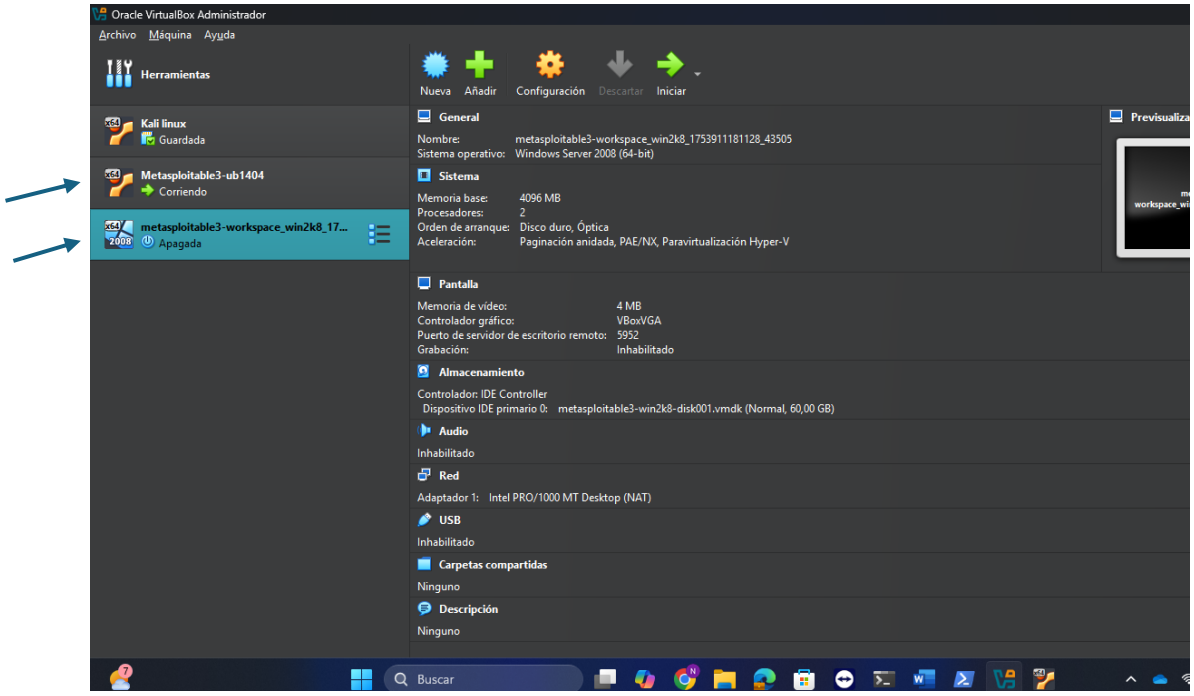


Ilustración 7 Metasploitable

Una vez finalizado el proceso de descarga, tras varios minutos, ya es posible visualizar en VirtualBox las dos máquinas virtuales generadas: una basada en Ubuntu y otra en Windows (ver la imagen 7).

Procedemos a iniciar ambas máquinas virtuales desde VirtualBox y finalizar sus configuraciones iniciales. Las credenciales predeterminadas para acceder a ambas máquinas son:

- **Usuario:** vagrant
- **Contraseña:** vagrant

Se muestra en las siguientes imágenes:

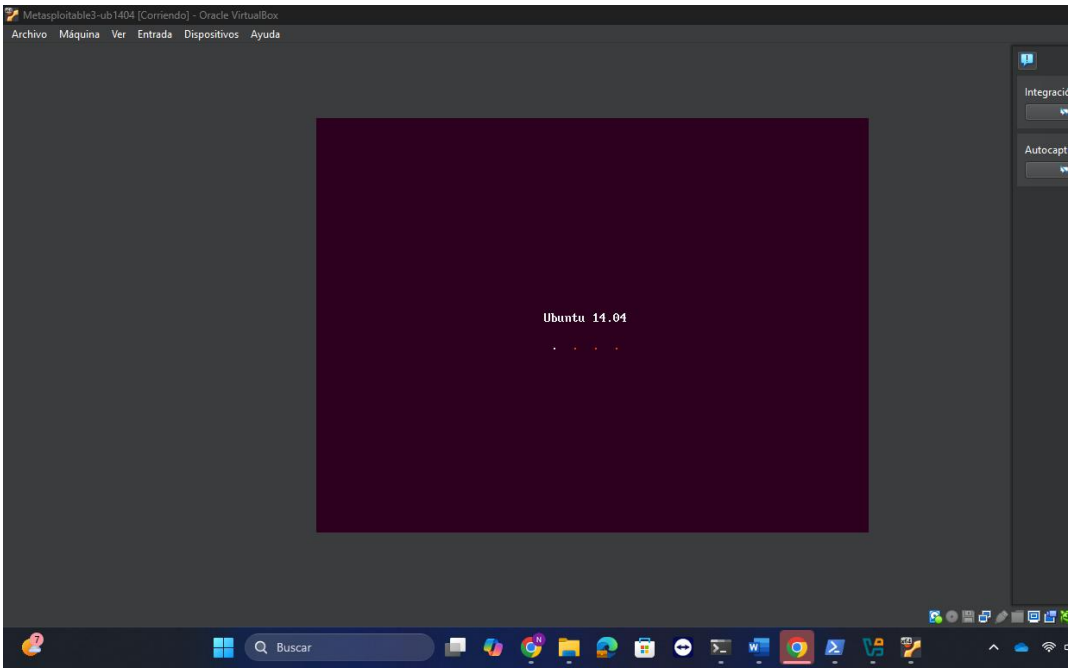
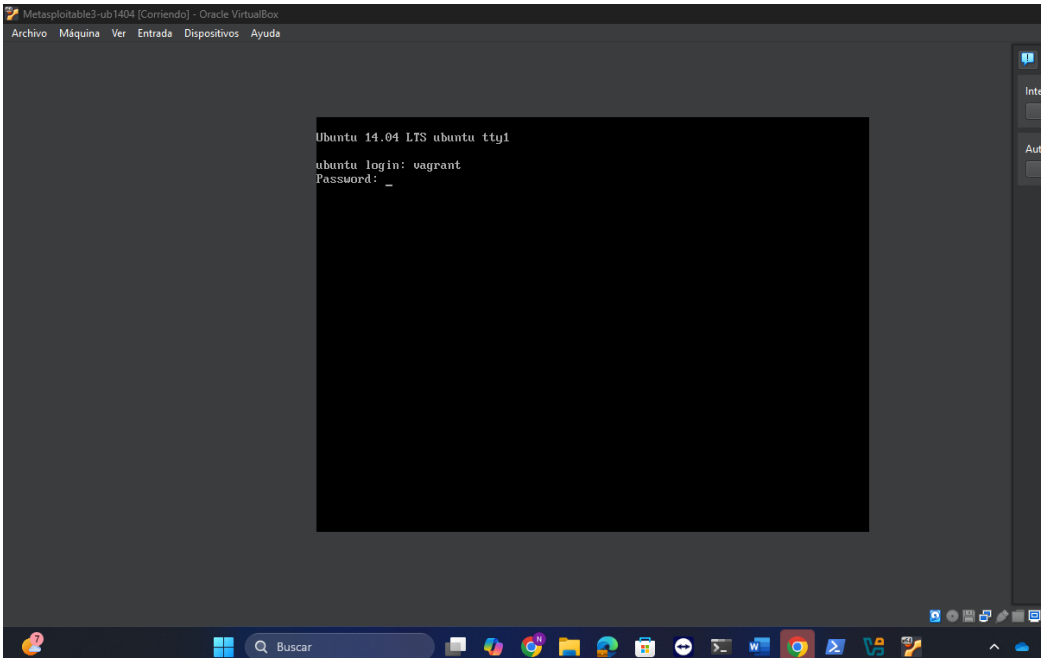
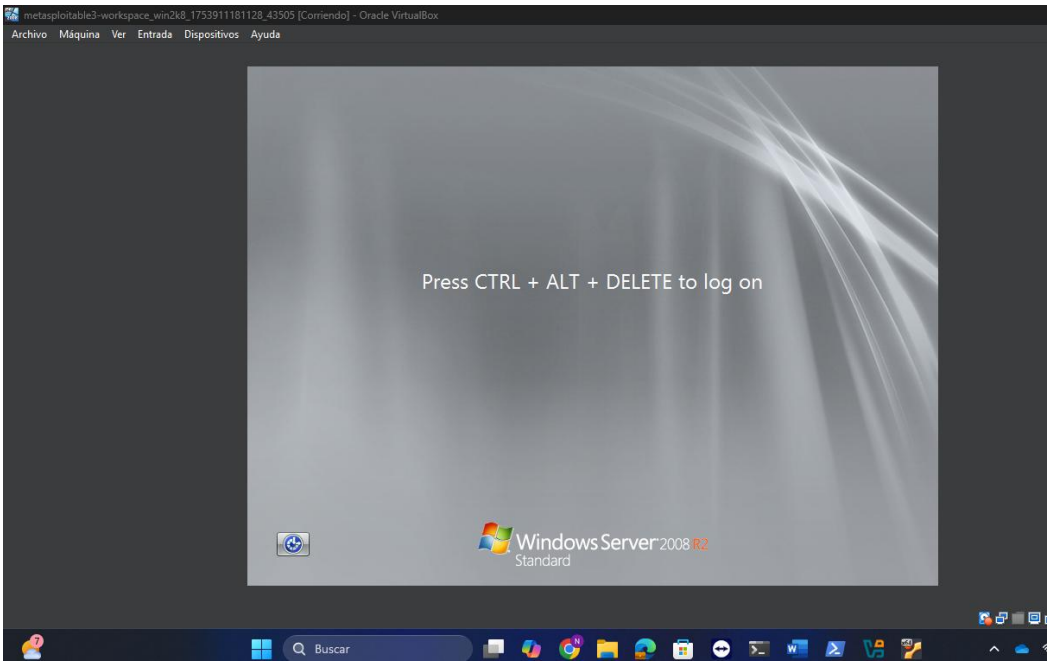
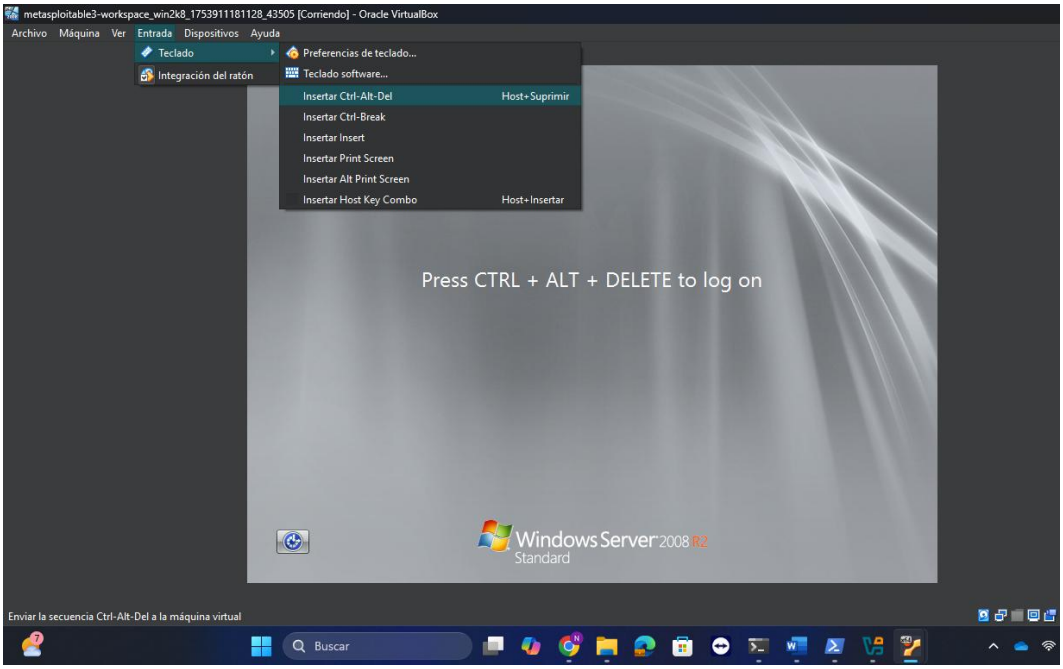


Ilustración 8 Metasploitable Ubuntu


Metasploitable3-ub1404 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Ubuntu 14.04 LTS ubuntu tty1
ubuntu login: vagrant
Password:
Buscar


metasploitable3-workspace_win2k8_1753911181128_43505 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Press CTRL + ALT + DELETE to log on
Windows Server 2008 R2
Standard
Buscar


metasploitable3-workspace_win2k8_1753911181128_43505 [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Teclado
Integración del ratón
Preferencias de teclado...
Teclado software...
Insertar Ctrl-Alt-Del Host+Suprimir
Insertar Ctrl-Break
Insertar Insert
Insertar Print Screen
Insertar Alt Print Screen
Insertar Host Key Combo Host+Insertar
Press CTRL + ALT + DELETE to log on
Windows Server 2008 R2
Standard
Enviar la secuencia Ctrl-Alt-Del a la máquina virtual
Buscar

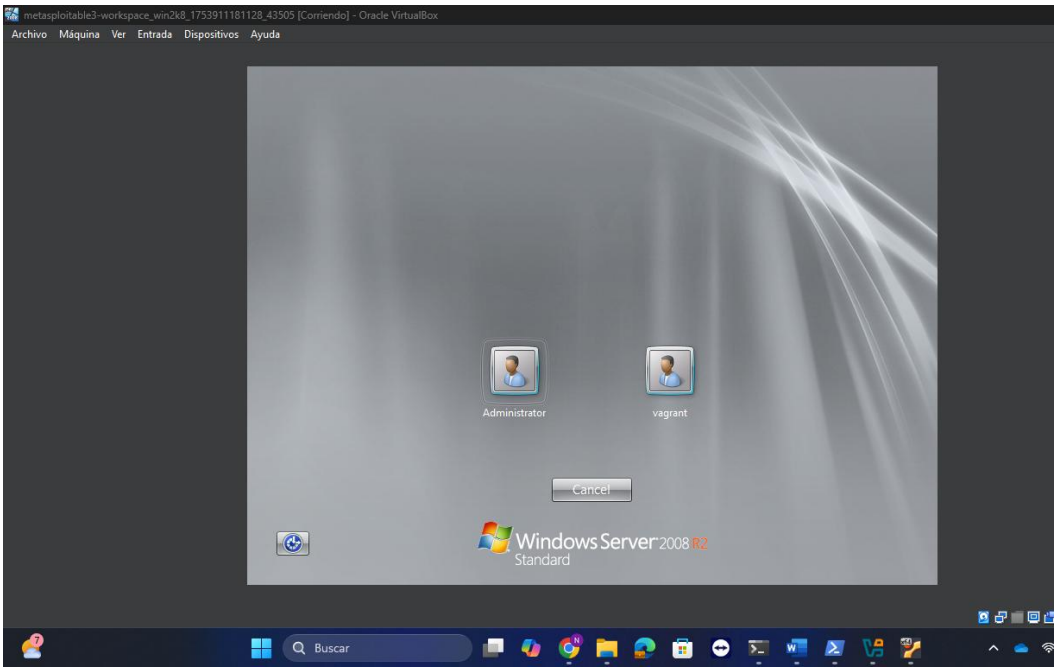
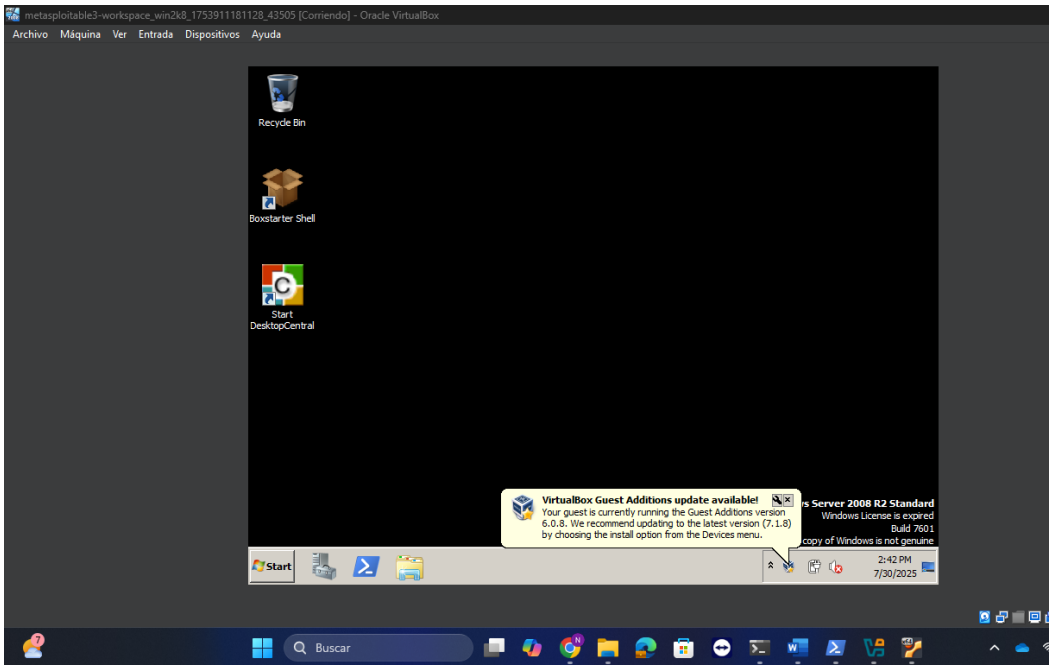


Ilustración 9 Maquina Metasploitable Windows



2 Problemas encontrados

Durante el proceso de instalación se presentaron dos inconvenientes principales:

Conectividad a Internet:

La conexión fue inestable en algunos momentos, lo que generó retrasos en la descarga de archivos y en la ejecución de ciertos comandos necesarios para levantar las máquinas virtuales.

Error con la versión de Windows de Metasploitable 3:

Aunque la versión basada en Ubuntu se instaló correctamente, la versión de Windows presentó fallos al principio.

3 Soluciones de los problemas

Problema de conectividad:

Primeramente, me dirigí a un lugar con mejor conexión a internet. Esto se reflejó en una mejora notable en la velocidad de descarga y ejecución de los comandos necesarios.

Problema con la instalación de la versión de Windows:

Para resolver este inconveniente, se liberó espacio en el equipo. Esto permitió que la versión de Windows de Metasploitable 3 se pudiera instalar correctamente, ya que el problema estaba relacionado con la falta de recursos de almacenamiento del equipo.

4 Recomendaciones

Se recomienda tener en cuenta las capacidades del equipo antes de iniciar el proceso de instalación, especialmente en cuanto a almacenamiento y memoria RAM.

5 Conclusiones

En base a los objetivos planteados, se concluye que fue posible instalar correctamente la máquina virtual Metasploitable 3 utilizando Vagrant como herramienta para su creación y configuración. Este proceso no solo me permitió cumplir con los pasos técnicos necesarios para la correcta instalación, sino que también representó una experiencia de aprendizaje valiosa. Al ser la primera vez que realizo un procedimiento de este tipo por mi cuenta, me siento agradecida por la oportunidad de adquirir nuevos conocimientos que fortalecen mi comprensión sobre entornos virtualizados y prácticas de hacking ético.

6 Bibliografía

Cilleruelo, C. (09 de Julio de 2024). *keepcoding.io/blog*. Obtenido de keepcoding.io: https://keepcoding.io/blog/como-instalar-metasploitable-3/

HashiCorp. (s.f.). *developer.hashicorp.com/vagrant*. Obtenido de developer.hashicorp.com: https://developer.hashicorp.com/vagrant

Rapid7. (s.f.). *Metasploitable3. GitHub*. Obtenido de Metasploitable3. GitHub: https://github.com/rapid7/metasploitable3