

INSTALACIÓN DE METASPLOITABLE 3

EDWARD CAMILO CAICEDO BENITEZ

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERÍA

PROGRAMA DE INGENIERÍA DE TELECOMUNICACIONES E

INFORMÁTICA

SEGURIDAD Y AUDITORIAS EN REDES

DOCENTE

RAFAEL SANDOVAL MORALES

QUIBDÓ-CHOCÓ-COLOMBIA

2025

TABLA DE CONTENIDO

INTRODUCCIÓN	4
OBJETIVO.....	4
METODOLOGÍA	5
INSTALCIONDE DE METASPLOTABLE 3	6
Instalamos vagrant.....	6
Procedemos con la instalación de metasploitable 3	9
Verificamos la instalación de metasploitable 3	12
CONCLUSIÓN	14

INTRODUCCIÓN

En el campo de la ciberseguridad, es fundamental contar con entornos controlados que permitan realizar pruebas de vulnerabilidades sin comprometer sistemas reales. **Metasploitable 3** es una máquina virtual intencionadamente vulnerable, diseñada por Rapid7, que facilita el aprendizaje de técnicas de explotación, análisis forense y prácticas de pentesting. La instalación de esta máquina requiere el uso de herramientas como **Vagrant** y **VirtualBox**, que automatizan la construcción del entorno, simplificando el despliegue de sistemas listos para pruebas de seguridad informática.

OBJETIVO

Implementar la instalación de Metasploitable 3 en un entorno local, utilizando Vagrant y VirtualBox, con el fin de disponer de una máquina vulnerable que sirva como laboratorio de prácticas para pruebas de penetración, identificación de vulnerabilidades y fortalecimiento de habilidades en ciberseguridad.

METODOLOGÍA

Metodología

La instalación de Metasploitable 3 se llevó a cabo siguiendo un proceso estructurado, dividido en varias fases:

1. **Preparación del entorno:**
2. **Creación del espacio de trabajo:**
3. **Despliegue de la máquina virtual:**
4. **Confirmación y acceso:**

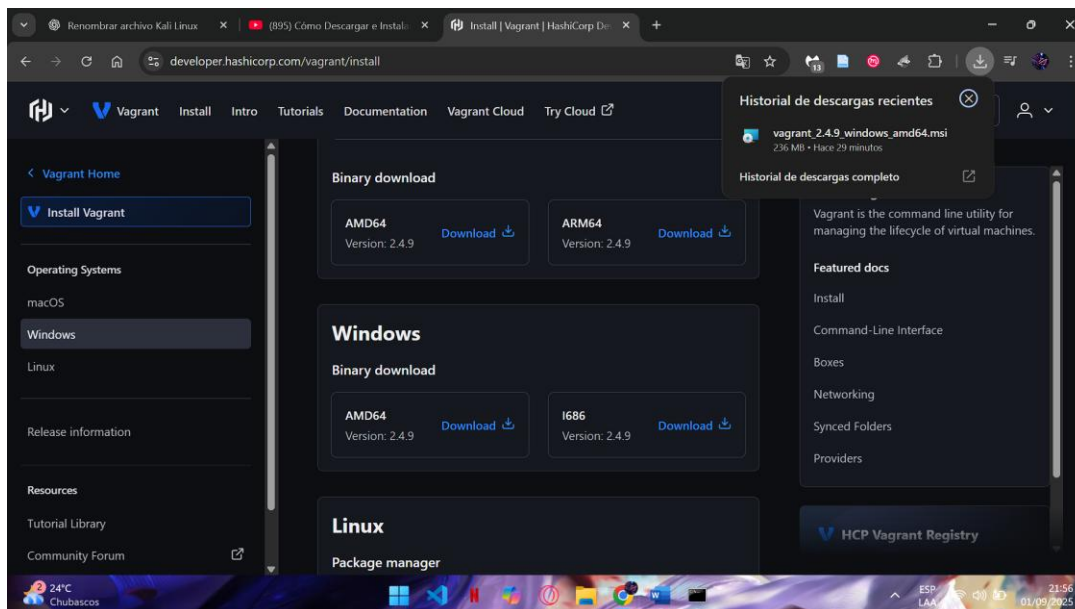
Con esta metodología se asegura la instalación exitosa de Metasploitable 3, dejando operativo un entorno seguro y controlado para el desarrollo de prácticas en seguridad informática

INSTALCIONE DE METASPLOTABLE 3

Instalamos vagrant

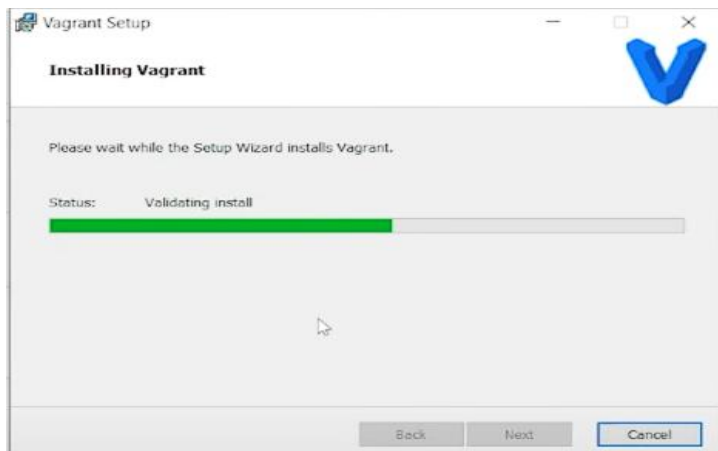
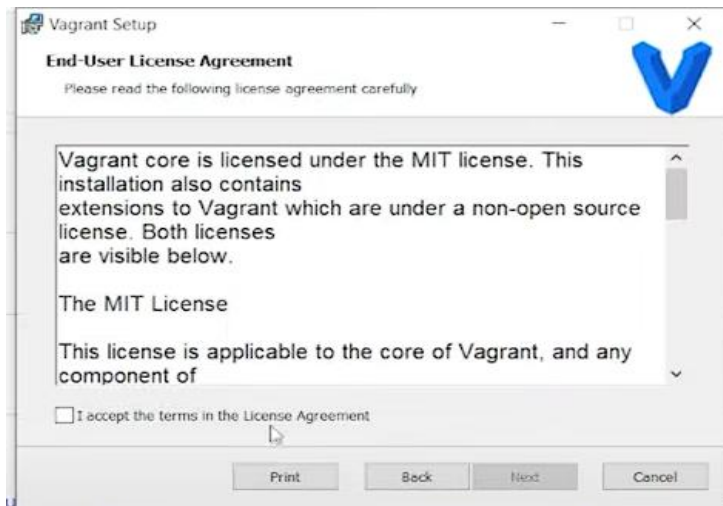
Paso 1 En este primer paso se procede a descargar **Vagrant**, una herramienta necesaria para la creación y administración de entornos virtualizados.

En la imagen se observa la página oficial de descargas de HashiCorp, donde se selecciona el sistema operativo **Windows** y se descarga el instalador correspondiente a la arquitectura **AMD64** (archivo: `vagrant_2.4.9_windows_amd64.msi`). Una vez iniciada la descarga, el archivo queda disponible en el historial del navegador para proceder con la instalación.

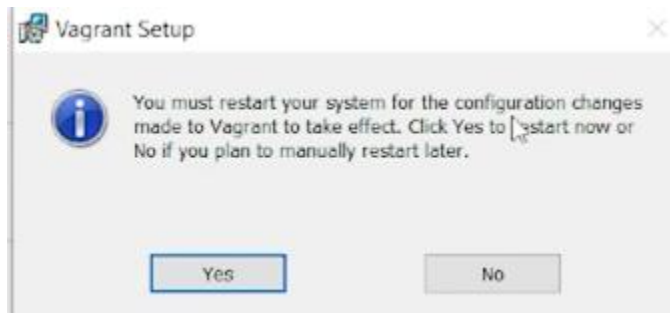


Paso 2: Una vez descargado el instalador, se procede a ejecutar el archivo `.msi`. En la primera ventana del asistente de instalación se presenta el **acuerdo de licencia de usuario final (EULA)**, donde es necesario aceptar los términos para continuar con la instalación.

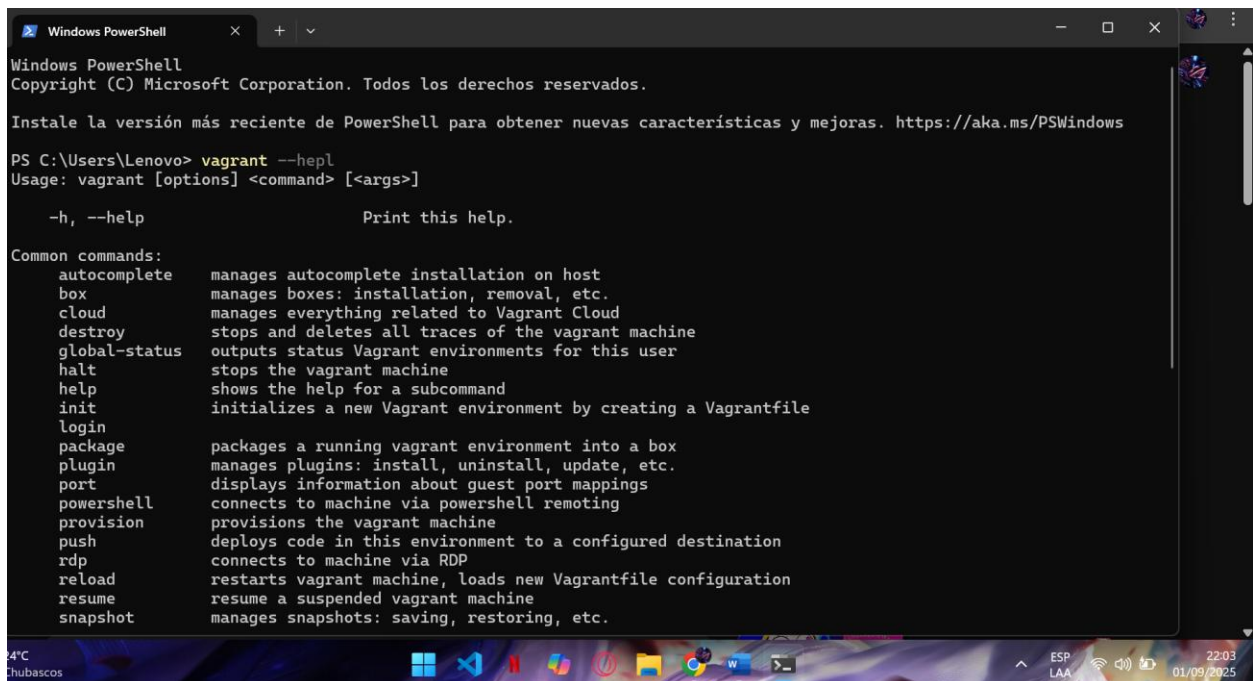
Posteriormente, el asistente comienza a instalar los componentes necesarios de Vagrant. En la imagen se observa el progreso de la instalación, específicamente en la etapa de **validación**, lo que confirma que el software se está configurando correctamente en el sistema.



Y reiniciamos el equipo



Paso 3: Confirmamos la instalación con esta validación, Vagrant queda listo para ser utilizado en la instalación de **Metasploitable 3**.

A screenshot of a Windows PowerShell terminal window. The title bar says "Windows PowerShell". The text inside shows the copyright notice for Microsoft Corporation, a link to the PowerShell website, and the command `vagrant --help` being executed. The output displays the usage and a list of common commands with their descriptions. The taskbar at the bottom shows the system clock as 22:03 on 01/09/2025.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Instale la versión más reciente de PowerShell para obtener nuevas características y mejoras. https://aka.ms/PSWindows

PS C:\Users\Lenovo> vagrant --help
Usage: vagrant [options] <command> [<args>]

    -h, --help                Print this help.

Common commands:
  autocomplete  manages autocomplete installation on host
  box           manages boxes: installation, removal, etc.
  cloud         manages everything related to Vagrant Cloud
  destroy       stops and deletes all traces of the vagrant machine
  global-status outputs status Vagrant environments for this user
  halt         stops the vagrant machine
  help         shows the help for a subcommand
  init         initializes a new Vagrant environment by creating a Vagrantfile
  login
  package      packages a running vagrant environment into a box
  plugin       manages plugins: install, uninstall, update, etc.
  port         displays information about guest port mappings
  powershell  connects to machine via powershell remoting
  provision    provisions the vagrant machine
  push        deploys code in this environment to a configured destination
  rdp         connects to machine via RDP
  reload      restarts vagrant machine, loads new Vagrantfile configuration
  resume      resume a suspended vagrant machine
  snapshot    manages snapshots: saving, restoring, etc.
```

Procedemos con la instalación de metasploitable 3

Paso 1: Creación del directorio de trabajo

El primer paso para instalar **Metasploitable 3** es crear un directorio de trabajo donde se almacenarán los archivos necesarios.

En la imagen se observa el uso del comando:

```
mkdir metasploitable3-workspace
```

Este comando crea la carpeta llamada **metasploitable3-workspace** dentro de C:\Windows\system32.

Posteriormente, se intenta acceder a esta carpeta con:

```
cd metasploitable3-workspace\
```

Sin embargo, se produce un error ya que el comando no se reconoce correctamente por la sintaxis utilizada. El problema se soluciona al ejecutar de nuevo el comando, pero esta vez con la ruta relativa correcta:

```
cd .\metasploitable3-workspace\
```

De esta manera, se logra ingresar sin inconvenientes al directorio creado, lo que confirma que el espacio de trabajo está listo para continuar con la instalación.

```
PS C:\Windows\system32> mkdir metasploitable3-workspace

Directorio: C:\Windows\system32


Mode                LastWriteTime         Length Name
----                -
d-----          01/09/2025   22:18             metasploitable3-workspace

PS C:\Windows\system32> cd
>> \metasploitable3-workspace\
\metasploitable3-workspace\ : El término '\metasploitable3-workspace\' no se reconoce como nombre de un cmdlet,
función, archivo de script o programa ejecutable. Compruebe si escribió correctamente el nombre o, si incluyó una ruta
de acceso, compruebe que dicha ruta es correcta e inténtelo de nuevo.
En línea: 2 Carácter: 1
+ \metasploitable3-workspace\
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (\\metasploitable3-workspace\:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\Windows\system32> cd .\metasploitable3-workspace\
PS C:\Windows\system32\metasploitable3-workspace> █
```

Paso 2: Descarga del Vagrantfile y despliegue inicial

Dentro del directorio de trabajo previamente creado, se procede a descargar el archivo **Vagrantfile** directamente desde el repositorio oficial de Rapid7 en GitHub mediante el comando:

`Invoke-WebRequest -Uri`

`"https://raw.githubusercontent.com/rapid7/metasploitable3/master/Vagrantfile" -OutFile`

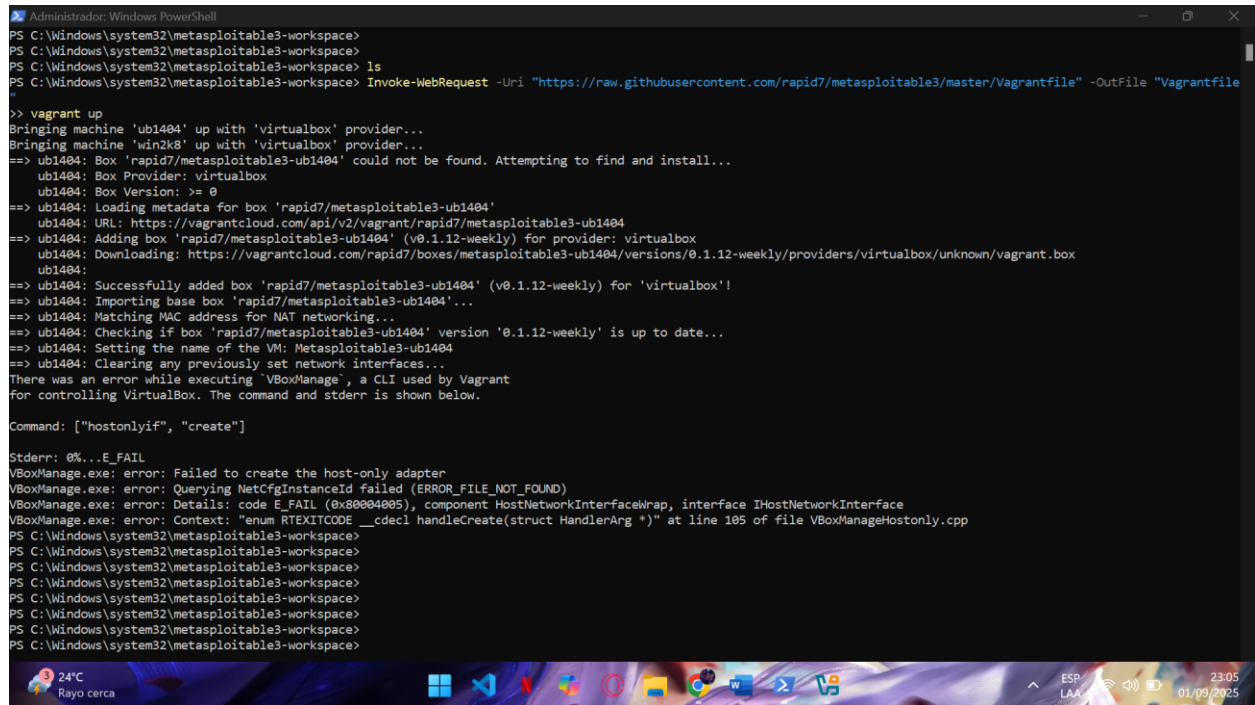
`"Vagrantfile"`

Este archivo contiene la configuración necesaria para que Vagrant construya la máquina virtual de Metasploitable 3.

Posteriormente, se ejecuta el comando:

`vagrant up`

Este inicia el proceso de descarga e instalación de la máquina base (**ub1404**) y la levanta utilizando **VirtualBox** como proveedor. Durante el proceso, Vagrant busca y descarga el box correspondiente desde vagrantcloud.com



```
Administrator: Windows PowerShell
PS C:\Windows\system32\metasploitable3-workspace>
PS C:\Windows\system32\metasploitable3-workspace>
PS C:\Windows\system32\metasploitable3-workspace> ls
PS C:\Windows\system32\metasploitable3-workspace> Invoke-WebRequest -Uri "https://raw.githubusercontent.com/rapid7/metasploitable3/master/Vagrantfile" -OutFile "Vagrantfile"
"
>> vagrant up
Bringing machine 'ub1404' up with 'virtualbox' provider...
Bringing machine 'win2k8' up with 'virtualbox' provider...
==> ub1404: Box 'rapid7/metasploitable3-ub1404' could not be found. Attempting to find and install...
ub1404: Box Provider: virtualbox
ub1404: Box Version: >= 0
==> ub1404: Loading metadata for box 'rapid7/metasploitable3-ub1404'
ub1404: URL: https://vagrantcloud.com/api/v2/vagrant/rapid7/metasploitable3-ub1404
==> ub1404: Adding box 'rapid7/metasploitable3-ub1404' (v0.1.12-weekly) for provider: virtualbox
ub1404: Downloading: https://vagrantcloud.com/rapid7/boxes/metasploitable3-ub1404/versions/0.1.12-weekly/providers/virtualbox/unknown/vagrant.box
ub1404:
==> ub1404: Successfully added box 'rapid7/metasploitable3-ub1404' (v0.1.12-weekly) for 'virtualbox'!
==> ub1404: Importing base box 'rapid7/metasploitable3-ub1404'...
==> ub1404: Matching MAC address for NAT networking...
==> ub1404: Checking if box 'rapid7/metasploitable3-ub1404' version '0.1.12-weekly' is up to date...
==> ub1404: Setting the name of the VM: Metasploitable3-ub1404
==> ub1404: Clearing any previously set network interfaces...
There was an error while executing 'VBoxManage', a CLI used by Vagrant
for controlling VirtualBox. The command and stderr is shown below.

Command: ["hostonlyif", "create"]

Stderr: 0%...E_FAIL
VBoxManage.exe: error: Failed to create the host-only adapter
VBoxManage.exe: error: Querying NetCfgInstanceId failed (ERROR_FILE_NOT_FOUND)
VBoxManage.exe: error: Details: code E_FAIL (0x80004005), component HostNetworkInterfaceWrap, interface IHostNetworkInterface
VBoxManage.exe: error: Context: "enum RTEITCODE __cdecl handleCreate(struct HandlerArg *)" at line 105 of file VBoxManageHostonly.cpp
PS C:\Windows\system32\metasploitable3-workspace>
PS C:\Windows\system32\metasploitable3-workspace>
PS C:\Windows\system32\metasploitable3-workspace>
PS C:\Windows\system32\metasploitable3-workspace>
PS C:\Windows\system32\metasploitable3-workspace>
PS C:\Windows\system32\metasploitable3-workspace>
PS C:\Windows\system32\metasploitable3-workspace>
PS C:\Windows\system32\metasploitable3-workspace>
```

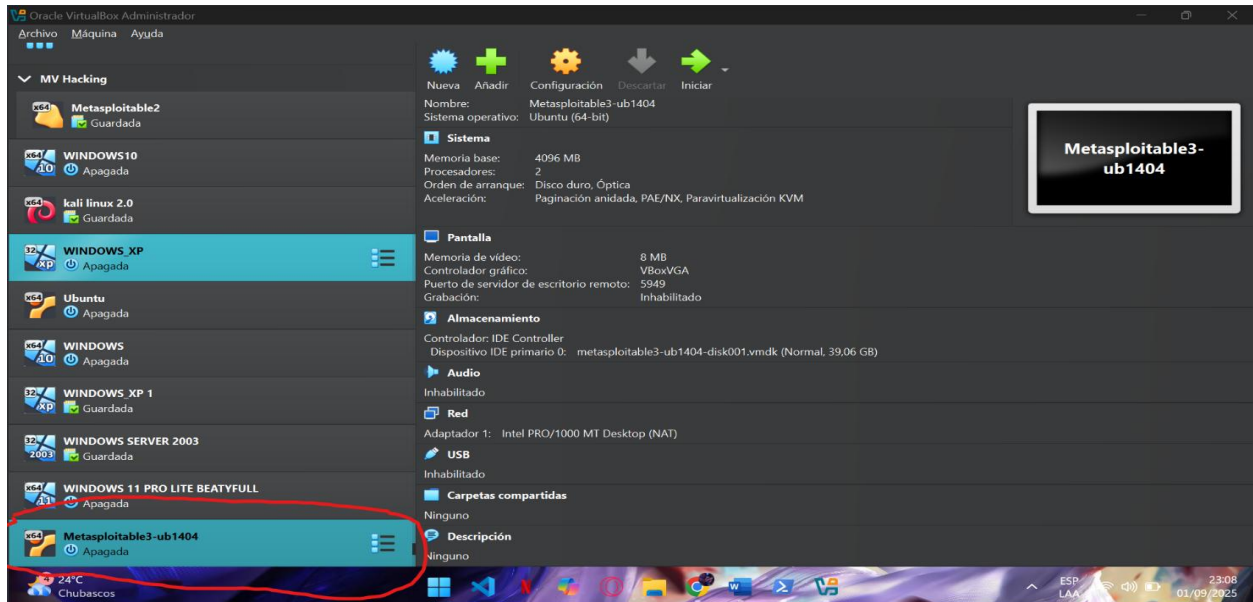
Paso 3: Confirmamos la instalación de metasploitable 3

Paso 3: Confirmación de la instalación en VirtualBox

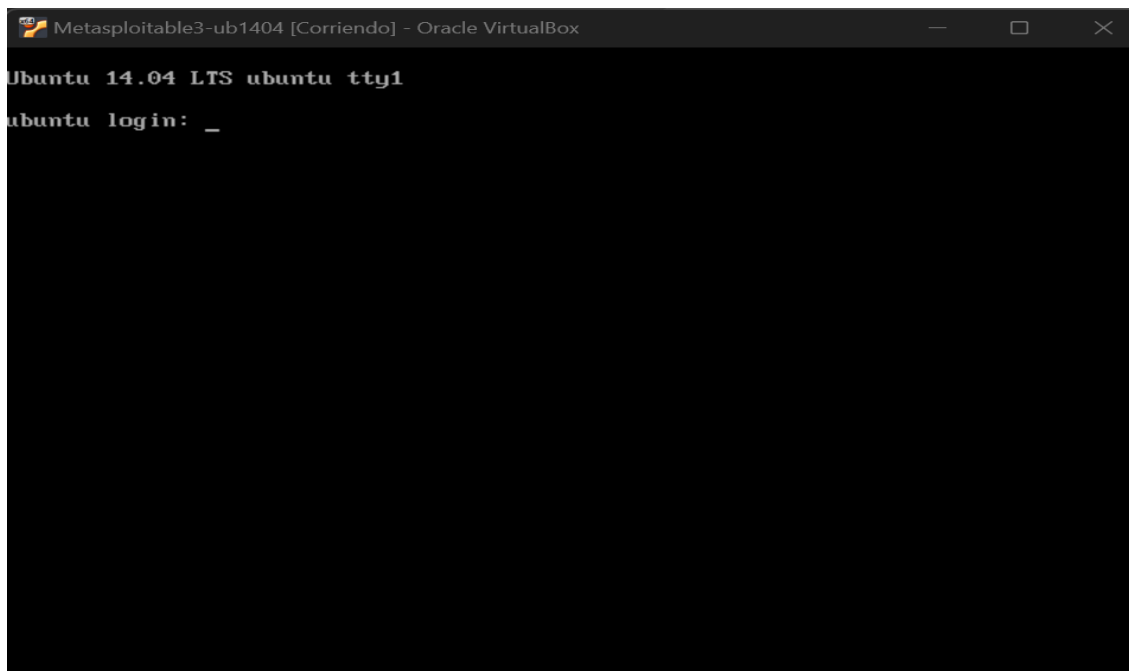
Una vez completada la ejecución del comando `vagrant up`, se verifica en **Oracle VM VirtualBox** la creación de la máquina virtual correspondiente a **Metasploitable 3**.

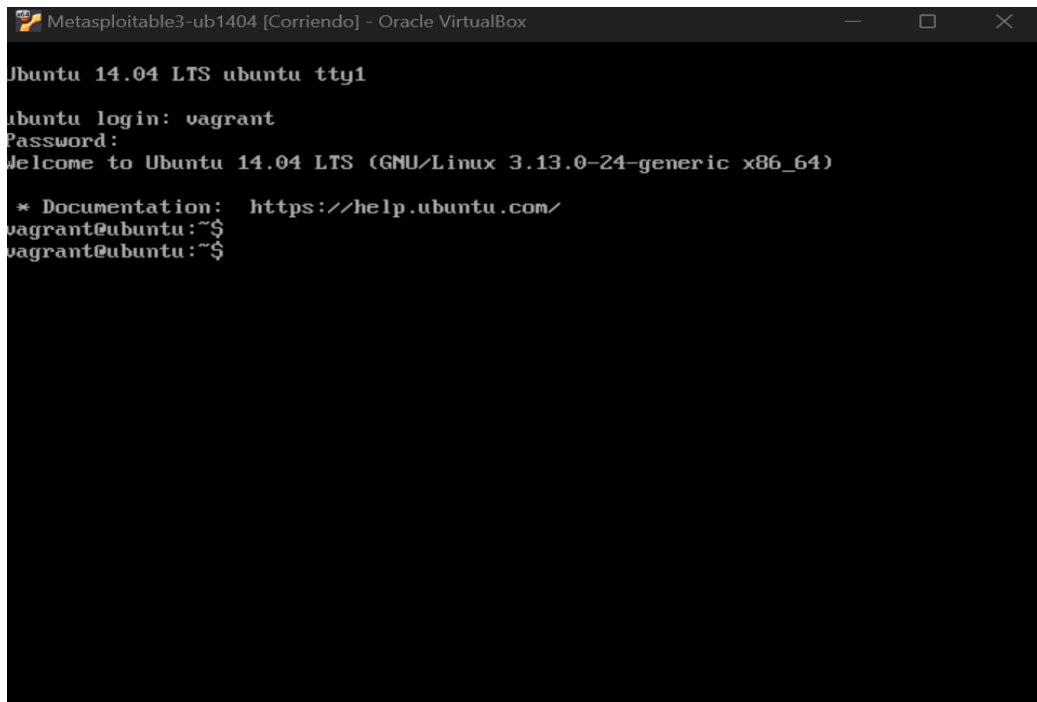
En la imagen se observa la máquina con el nombre **Metasploitable3-ub1404**, que aparece en la lista de entornos virtualizados junto a otros sistemas ya instalados. La máquina se encuentra en estado **Apagada**, lo que significa que la instalación fue exitosa y está lista para iniciarse cuando sea necesario.

Con este paso se confirma que la integración entre **Vagrant** y **VirtualBox** funcionó correctamente, dejando Metasploitable 3 preparado para usarse en pruebas de seguridad y entornos de laboratorio.



Verificamos la instalación de metasploitable 3



A screenshot of a terminal window titled "Metasploitable3-ub1404 [Corriendo] - Oracle VirtualBox". The terminal shows the following text: "Ubuntu 14.04 LTS ubuntu tty1", "ubuntu login: vagrant", "Password:", "Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)", "* Documentation: https://help.ubuntu.com/", "vagrant@ubuntu:~\$", and "vagrant@ubuntu:~\$". The terminal has a black background with white text.

```
Metasploitable3-ub1404 [Corriendo] - Oracle VirtualBox
Ubuntu 14.04 LTS ubuntu tty1
ubuntu login: vagrant
Password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
vagrant@ubuntu:~$
vagrant@ubuntu:~$
```

Finalmente, al iniciar la máquina virtual **Metasploitable3-ub1404** en **Oracle VM VirtualBox**, el sistema arranca con **Ubuntu 14.04 LTS**.

En la pantalla se muestra el inicio de sesión, donde el usuario y contraseña predeterminados son:

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

Una vez autenticado, se accede al sistema operativo Ubuntu, lo que confirma que la máquina virtual se encuentra funcionando correctamente y está lista para ser utilizada en prácticas de seguridad informática y pruebas de pentesting.

CONCLUSIÓN

El proceso de instalación de **Metasploitable 3** requiere la configuración de herramientas como **Vagrant** y **VirtualBox**, las cuales automatizan la creación y despliegue del entorno vulnerable.

A lo largo de los pasos se pudo:

1. Instalar y verificar el correcto funcionamiento de Vagrant.
2. Descargar y configurar el archivo Vagrantfile desde GitHub.
3. Desplegar la máquina virtual Metasploitable3 en VirtualBox.
4. Confirmar el acceso al sistema Ubuntu 14.04 LTS.

Con ello, se dispone de un entorno controlado y vulnerable, ideal para realizar pruebas de seguridad, prácticas de explotación y fortalecimiento de habilidades en ciberseguridad.