



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

Código: F

COPM-11
Versión: 03
Fecha: 22-05-24

SEGURIDAD Y AUDITORIA DE REDES

Ing. Rafael Sandoval

MANUEL INSTRUCTIVO DE DESCARGA E INSTALACIÓN DE METASPLOITABLE 3 SOBRE UNA MAQUINA VIRTUAL

KEVIN STIVEN JARAMILLO CÓRDOBA

UNIVERSIDAD TECNOLÓGICA DEL CHOCO “DIEGO LUIS CÓRDOBA”
FACULTAD DE INGENIERÍA
INGENIERIA DE TELECOMUNICACIONES
SEGURIDAD Y AUDITORIA DE REDES
QUIBDÓ-CHOCO (COLOMBIA) 2025

Vigilada MinEducación



SC CER130675



“UTCH, Compromiso de Todos y para Todos”

Universidad Tecnológica del Chocó Diego Luis Córdoba
Nit. 891680089-4
Carrera 22 No. 18B-10 B. Nicolas Medrano - Ciudadela Universitaria
Conmutador (+57) 4 672 65 65, Línea gratuita: 018000938824
E-mail contactenos@utch.edu.co, Pagina Web: utch.edu.co
Quibdó, Chocó(Colombia)



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

Código: F

COPM-11
Versión: 03
Fecha: 22-05-24

SEGURIDAD Y AUDITORIA DE REDES

Ing. Rafael Sandoval

MANUEL INSTRUCTIVO DE DESCARGA E INSTALACIÓN DE METASPLOITABLE 3 SOBRE UNA MAQUINA VIRTUAL

KEVIN STIVEN JARAMILLO CÓRDOBA
Estudiante, IX semestre

ING. RAFAEL SANDOVAL
Docente de la asignatura

UNIVERSIDAD TECNOLÓGICA DEL CHOCO “DIEGO LUIS CÓRDOBA”
FACULTAD DE INGENIERÍA
INGENIERIA DE TELECOMUNICACIONES
SEGURIDAD Y AUDITORIA DE REDES
QUIBDÓ-CHOCO (COLOMBIA)
2025

Vigilada MinEduación



SC CER130675



“UTCH, Compromiso de Todos y para Todos”

Universidad Tecnológica del Chocó Diego Luis Córdoba
Nit. 891680089-4
Carrera 22 No. 18B-10 B. Nicolas Medrano - Ciudadela Universitaria
Conmutador (+57) 4 672 65 65, Línea gratuita: 018000938824
E-mail contactenos@utch.edu.co, Pagina Web: utch.edu.co
Quibdó, Chocó (Colombia)



SEGURIDAD Y AUDITORIA DE REDES

Ing. Rafael Sandoval

CONTENIDO

	Pág.
1. Introducción.....	5
2. Objetivos	6
2.2 Objetivo General.....	6
2.3 Objetivos Específicos	6
3. Desarrollo del tema	7
3.2 Descarga de Vagrant desde el sitio oficial de HashiCorp	7
4. Conclusión.....	23
5. Bibliográfica	24



SEGURIDAD Y AUDITORIA DE REDES

Ing. Rafael Sandoval

TABLA DE ILUSTRACIÓN

Ilustración 1: Sitio oficial de HashiCorp para descargar Vagrant	7
Ilustración 2: Visualización de la descarga de Vagrant	8
Ilustración 3: Dar permiso para ejecutar el archivo descargado	9
Ilustración 4: Aceptar términos y condiciones de Vagrant	10
Ilustración 5: Finalizar instalación de Vagrant	11
Ilustración 6: Reiniciar para guardar los cambios por Vagrant	12
Ilustración 7: Guía para instalación de Metasploitable 3	13
Ilustración 8: Entorno de trabajo desde el CMD	14
Ilustración 9: Ejecución de comandos desde el CMD	15
Ilustración 10: Evidencia de creación de la carpeta en el disco local	16
Ilustración 11: Ejecución de comandos desde PowerShell	17
Ilustración 12: Inicio de descarga de Metasploitable 3	18
Ilustración 13: Instalación completada	19
Ilustración 14: Maquinas reflejadas en Virtualbox	20
Ilustración 15: Interfaz gráfica de Metasploitable 3	21
Ilustración 16: Acceso a Metasploitable 3 desde la terminal de Ubuntu	22



SEGURIDAD Y AUDITORIA DE REDES

Ing. Rafael Sandoval

1. Introducción

Metasploitable 3 es una herramienta diseñada para el aprendizaje y la práctica de temas relacionados con la seguridad informática. Se trata de una máquina virtual que se instala en el computador y que contiene vulnerabilidades creadas de forma intencional. Estas fallas permiten que estudiantes, profesionales o cualquier persona interesada practiquen cómo detectar y explotar errores de seguridad de forma segura, ética y sin afectar sistemas reales.

En este informe se explica paso a paso cómo instalar Metasploitable 3 en un computador con Windows. Para esto, se usan programas como Vagrant y VirtualBox, que ayudan a crear y manejar máquinas virtuales. La instalación puede parecer complicada al principio, pero siguiendo las instrucciones correctas se puede lograr sin problemas. Esta guía de instalación está pensada para cualquiera persona que lea el documento pueda entender como descargar e instalar correctamente la maquina virtual tanto en entorno grafico como en consola



SEGURIDAD Y AUDITORIA DE REDES

Ing. Rafael Sandoval

2. Objetivos

2.2 Objetivo General

- Instalar y ejecutar correctamente la máquina virtual Metasploitable 3 para usarla como entorno de prácticas para la asignatura de Seguridad y Auditoria de Redes

2.3 Objetivos Específicos

- Descargar e instalar las herramientas necesarias: Vagrant, VirtualBox y Git (en caso necesario).
- Crear y configurar el entorno de trabajo mediante comandos en PowerShell siguiendo las instrucciones del repositorio oficial.
- Verificar que la máquina virtual de Metasploitable 3 se ejecute correctamente tanto en modo gráfico como en consola.



SEGURIDAD Y AUDITORIA DE REDES

Ing. Rafael Sandoval

3. Desarrollo del tema

3.2 Descarga de Vagrant desde el sitio oficial de HashiCorp

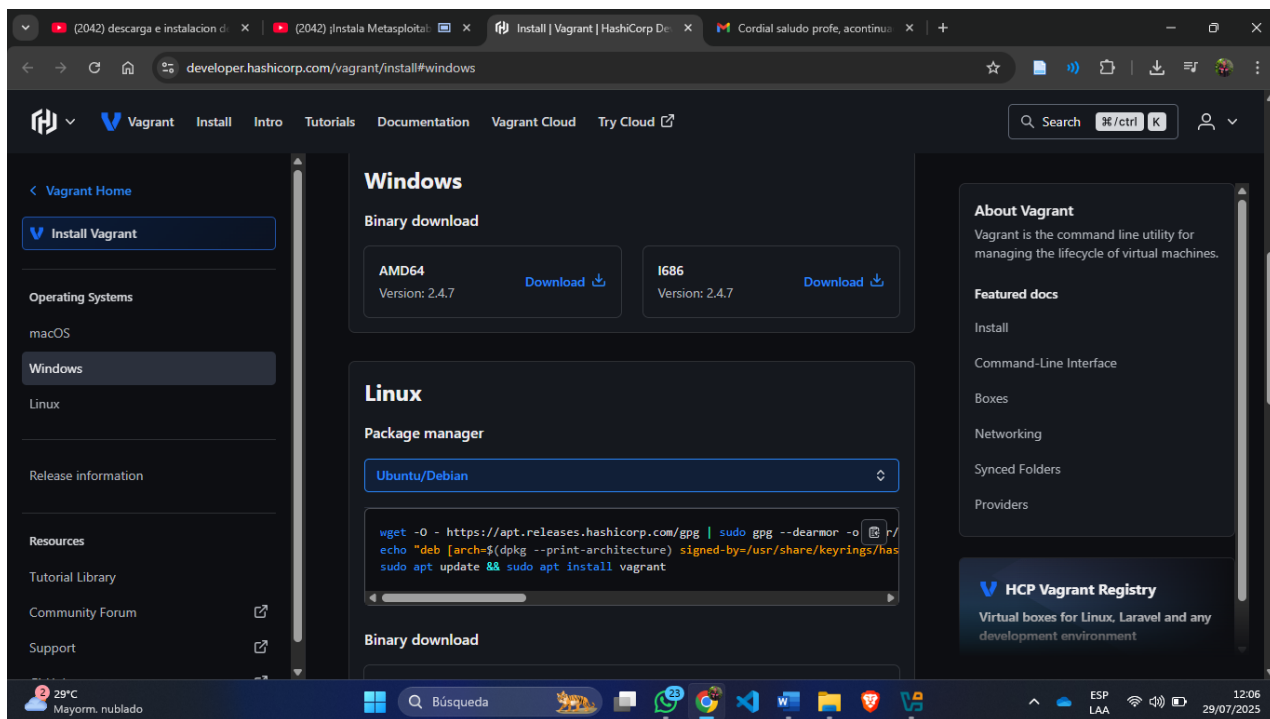


Ilustración 1: Sitio oficial de HashiCorp para descargar Vagrant

En esta imagen se muestra el sitio oficial de HashiCorp desde donde se realiza la descarga de Vagrant, una herramienta fundamental para la gestión de entornos virtuales en el proceso de instalación de Metasploitable 3. Se observa la sección de descarga específica para el sistema operativo Windows, con versiones disponibles para arquitecturas AMD64 e I686. También se presentan instrucciones para la instalación en sistemas Linux (Ubuntu/Debian) mediante el uso de comandos en terminal. Esta etapa es esencial para preparar el entorno donde se ejecutará la máquina virtual vulnerable Metasploitable 3.



SEGURIDAD Y AUDITORIA DE REDES

Ing. Rafael Sandoval

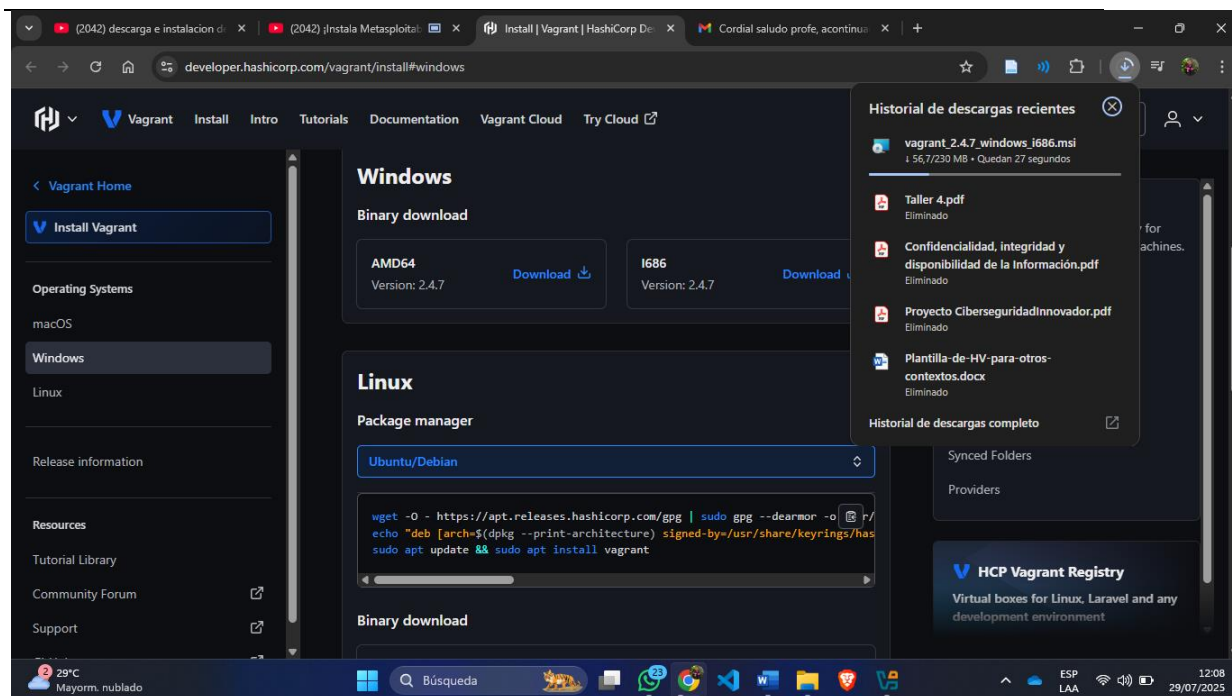


Ilustración 2: Visualización de la descarga de Vagrant



SEGURIDAD Y AUDITORIA DE REDES

Ing. Rafael Sandoval

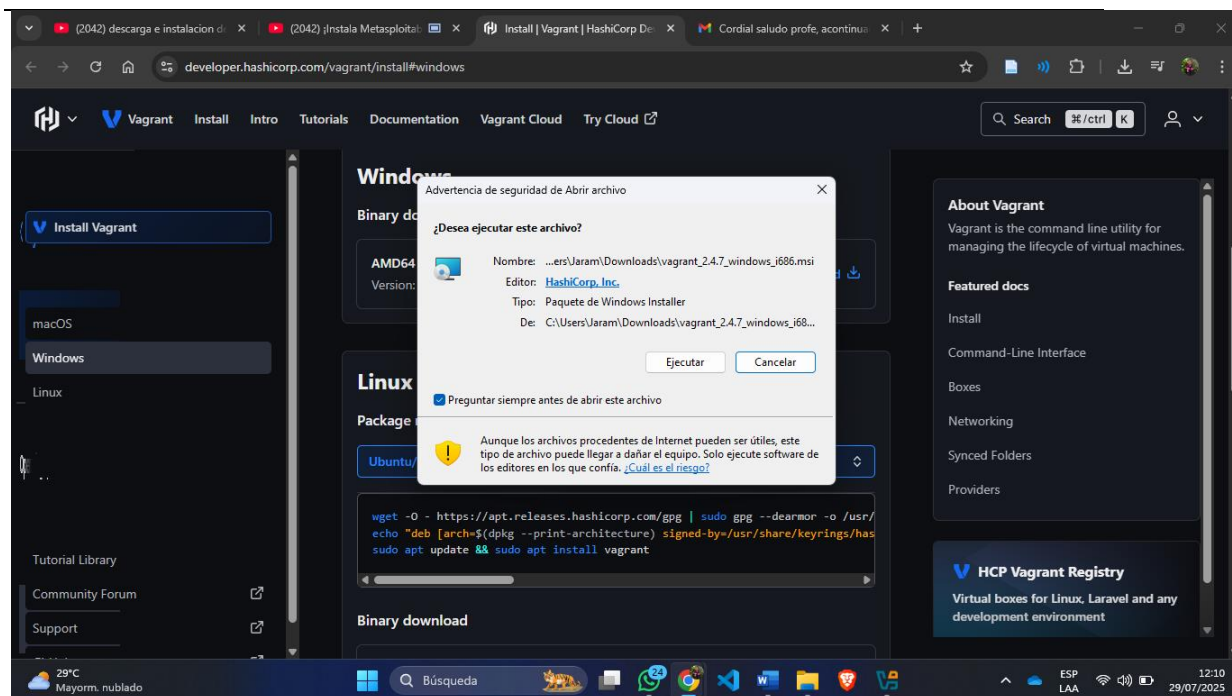


Ilustración 3: Dar permiso para ejecutar el archivo descargado



SEGURIDAD Y AUDITORIA DE REDES

Ing. Rafael Sandoval

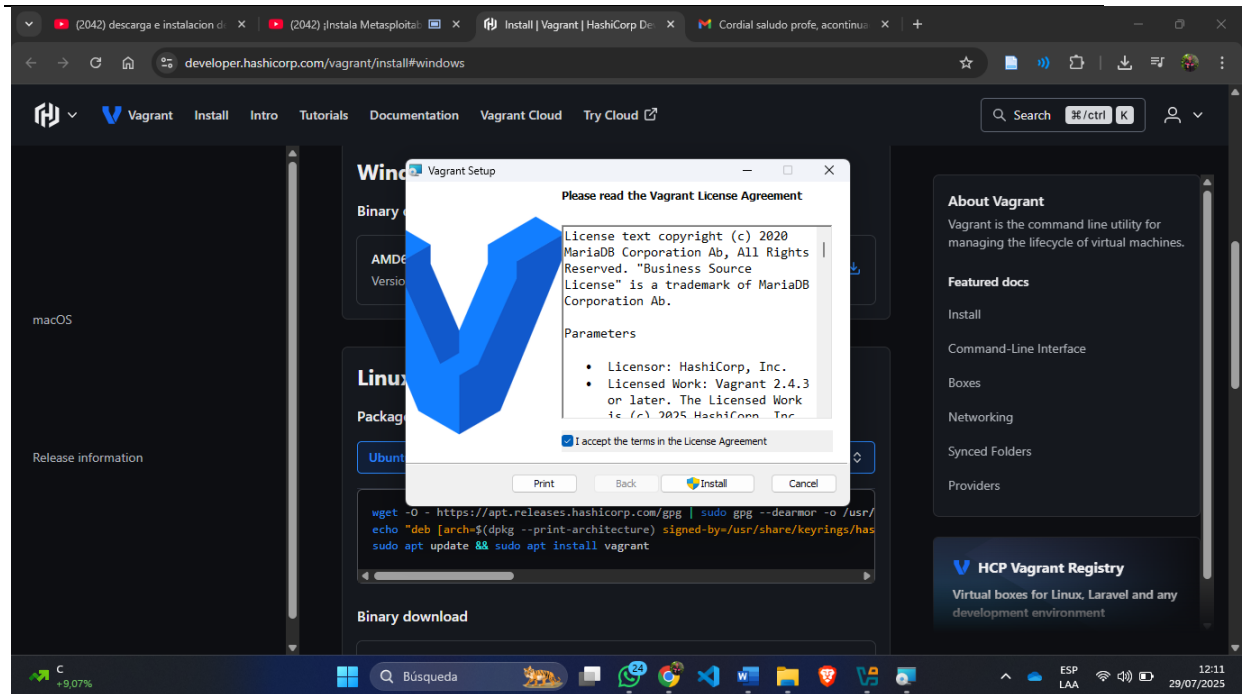


Ilustración 4: Aceptar términos y condiciones de Vagrant



SEGURIDAD Y AUDITORIA DE REDES

Ing. Rafael Sandoval

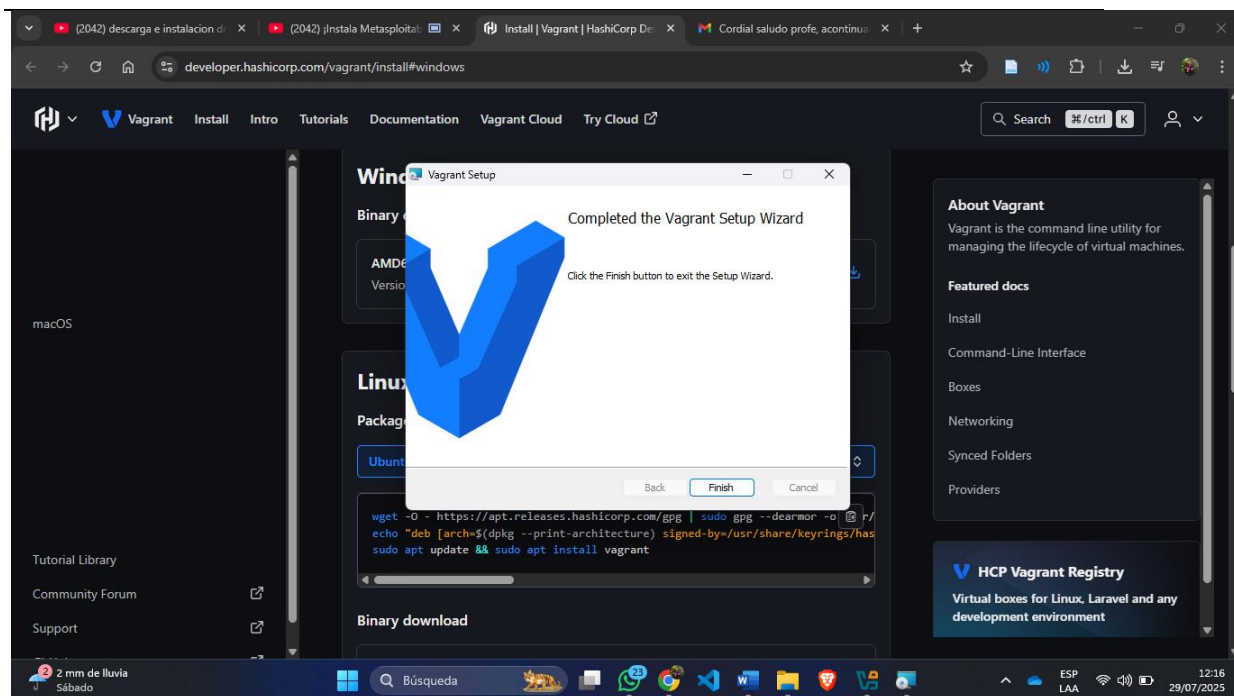


Ilustración 5: Finalizar instalación de Vagrant



SEGURIDAD Y AUDITORIA DE REDES

Ing. Rafael Sandoval

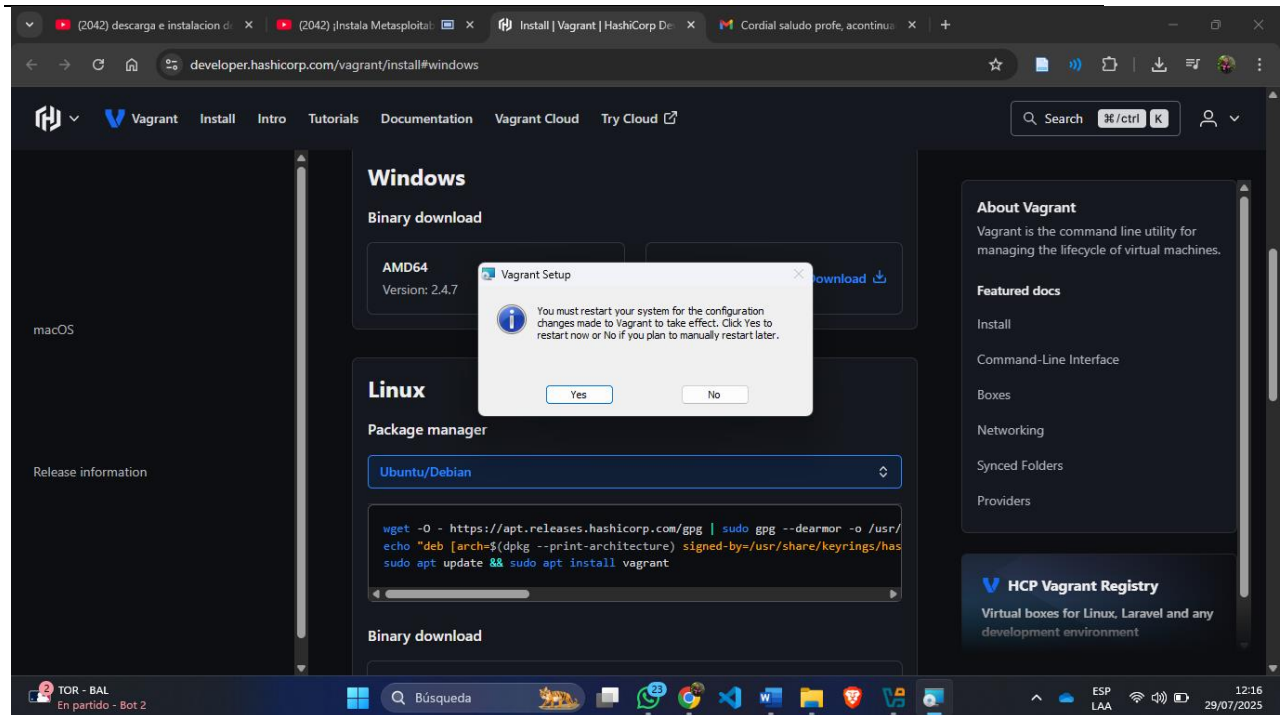


Ilustración 6: Reiniciar para guardar los cambios por Vagrant

Guía de inicio rápido para la configuración de Metasploitable 3



SEGURIDAD Y AUDITORIA DE REDES

Ing. Rafael Sandoval

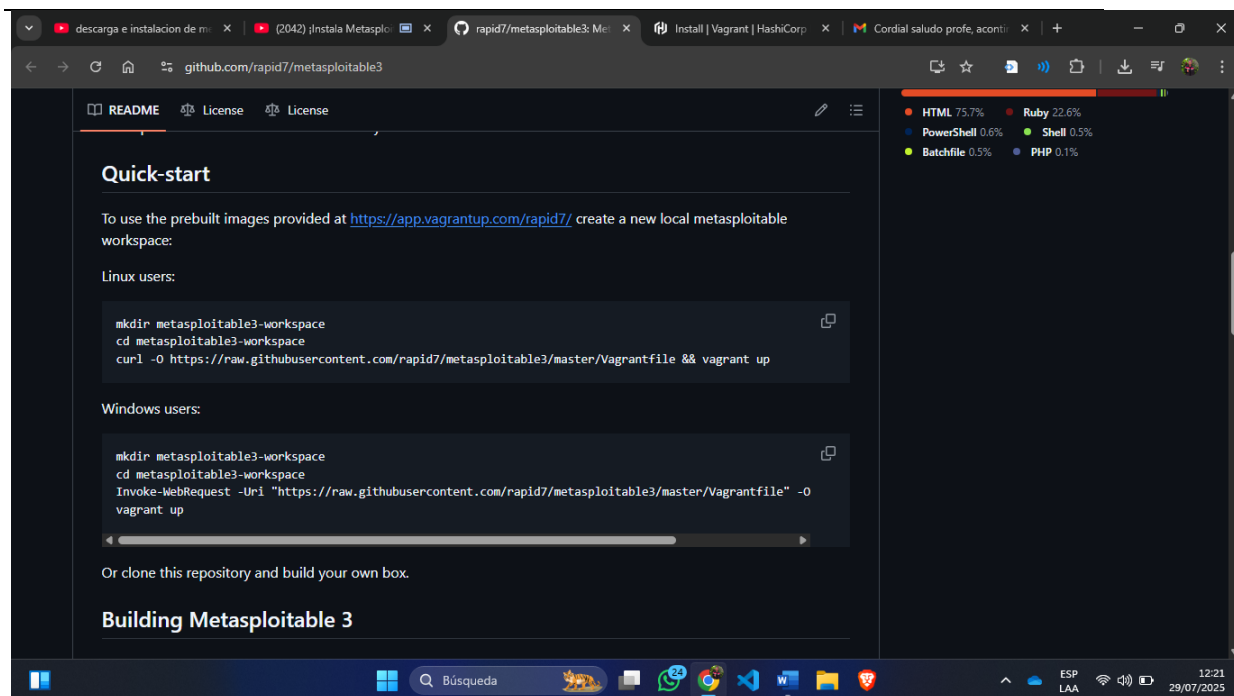


Ilustración 7: Guía para instalación de Metasploitable 3

La imagen muestra la sección "Quick-start" del repositorio oficial de Metasploitable 3 en GitHub. Se detallan los comandos necesarios para crear un entorno de trabajo local utilizando Vagrant, tanto para usuarios de Linux como de Windows. Para Windows, se utiliza PowerShell con `Invoke-WebRequest` para descargar el archivo Vagrantfile, seguido del comando `vagrant up` que inicializa la máquina virtual. Esta etapa es esencial para desplegar Metasploitable 3 de forma automatizada y controlada mediante Vagrant, utilizando imágenes preconstruidas alojadas en Vagrant Cloud.

```
mkdir metasploitable3-workspace
cd metasploitable3-workspace
Invoke-WebRequest -Uri "https://raw.githubusercontent.com/rapid7/metasploitable3/master/Vagrantfile" -OutFile
"Vagrantfile"
vagrant up
```

Creación del directorio de trabajo para Metasploitable 3 en Windows



SEGURIDAD Y AUDITORIA DE REDES

Ing. Rafael Sandoval

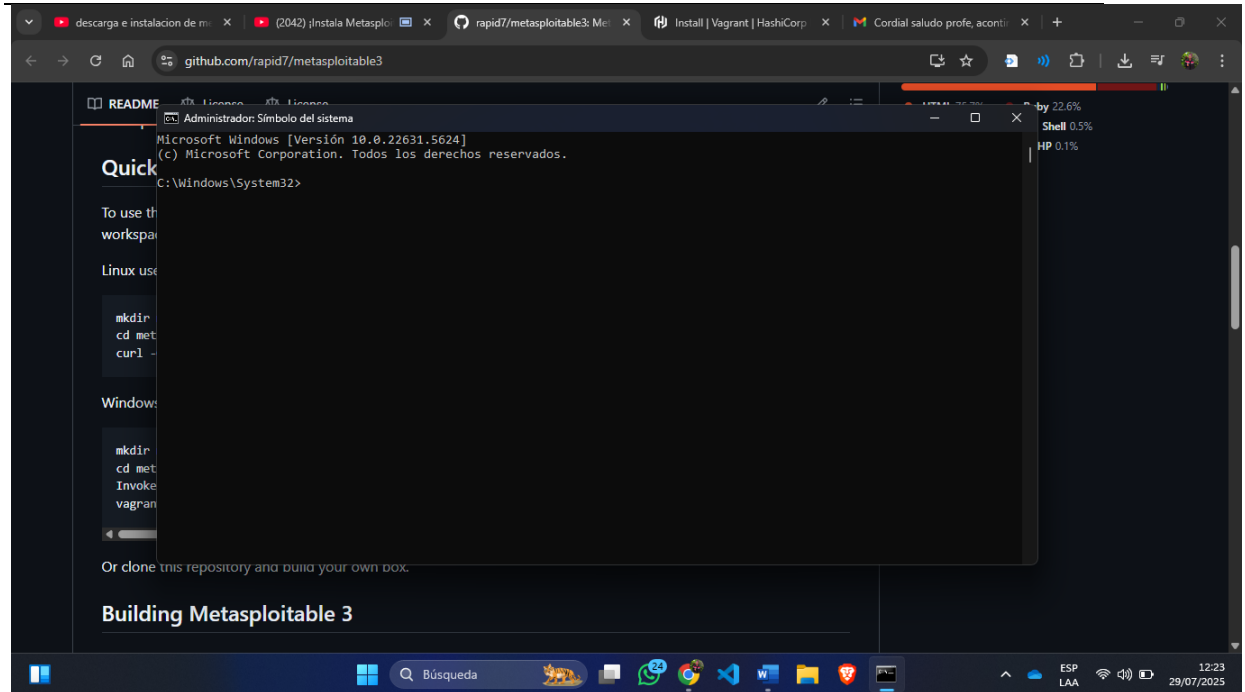


Ilustración 8: Entorno de trabajo desde el CMD

Estas capturas muestran el uso del símbolo del sistema (CMD) en Windows para iniciar la configuración del entorno de Metasploitable 3. En la primera imagen se observa el entorno de terminal listo para ejecutar comandos.



SEGURIDAD Y AUDITORIA DE REDES

Ing. Rafael Sandoval

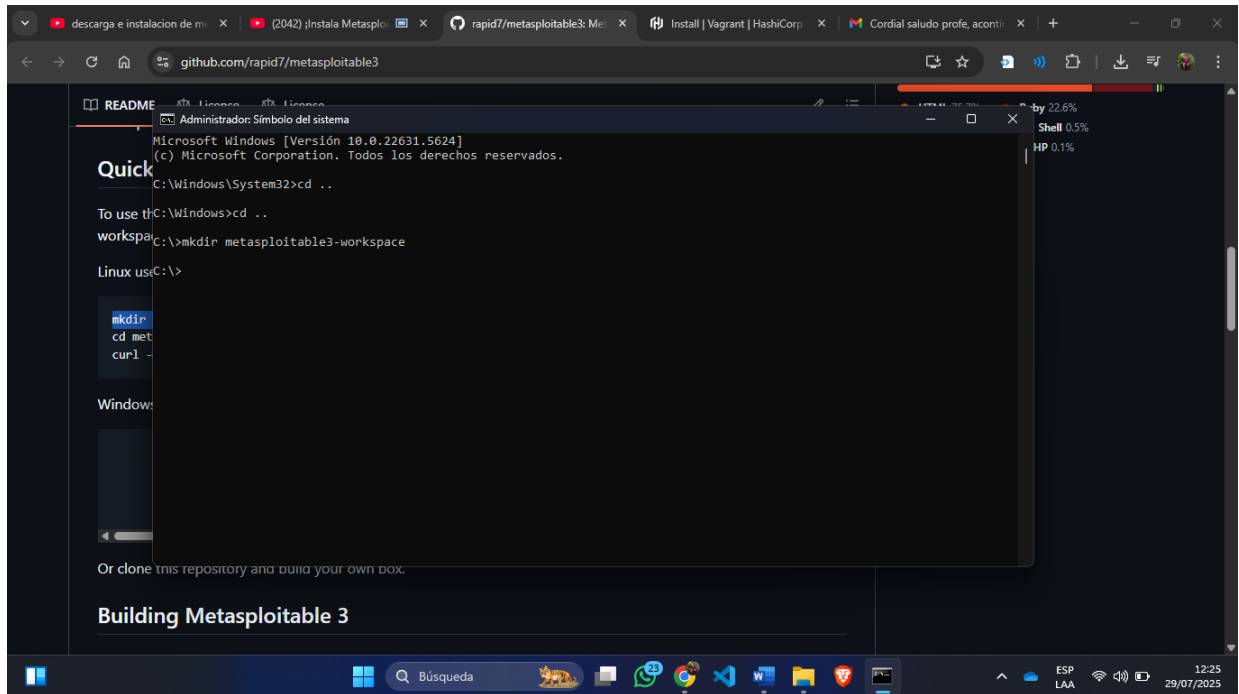


Ilustración 9: Ejecución de comandos desde el CMD

En la segunda imagen, ya se ha ejecutado el comando `mkdir metasploitable3-workspace`, lo que crea un nuevo directorio llamado `metasploitable3-workspace`, y se ha navegado dentro de él usando `cd metasploitable3-workspace`. Este paso es esencial para organizar los archivos del proyecto y continuar con la descarga del archivo Vagrantfile necesario para desplegar la máquina virtual con Vagrant.



SEGURIDAD Y AUDITORIA DE REDES

Ing. Rafael Sandoval

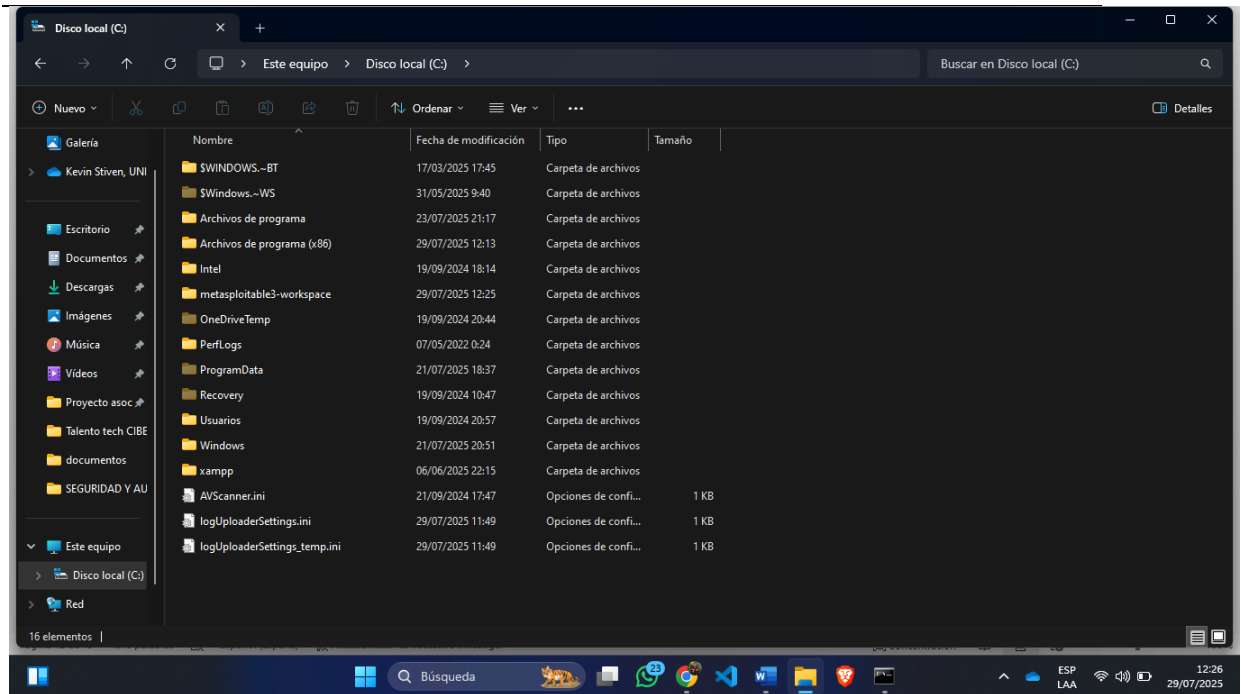


Ilustración 10: Evidencia de creación de la carpeta en el disco local

Aquí se ve reflejado la creación de la carpeta desde el cmd



SEGURIDAD Y AUDITORIA DE REDES

Ing. Rafael Sandoval

Ejecución de comandos para iniciar Metasploitable 3 desde PowerShell

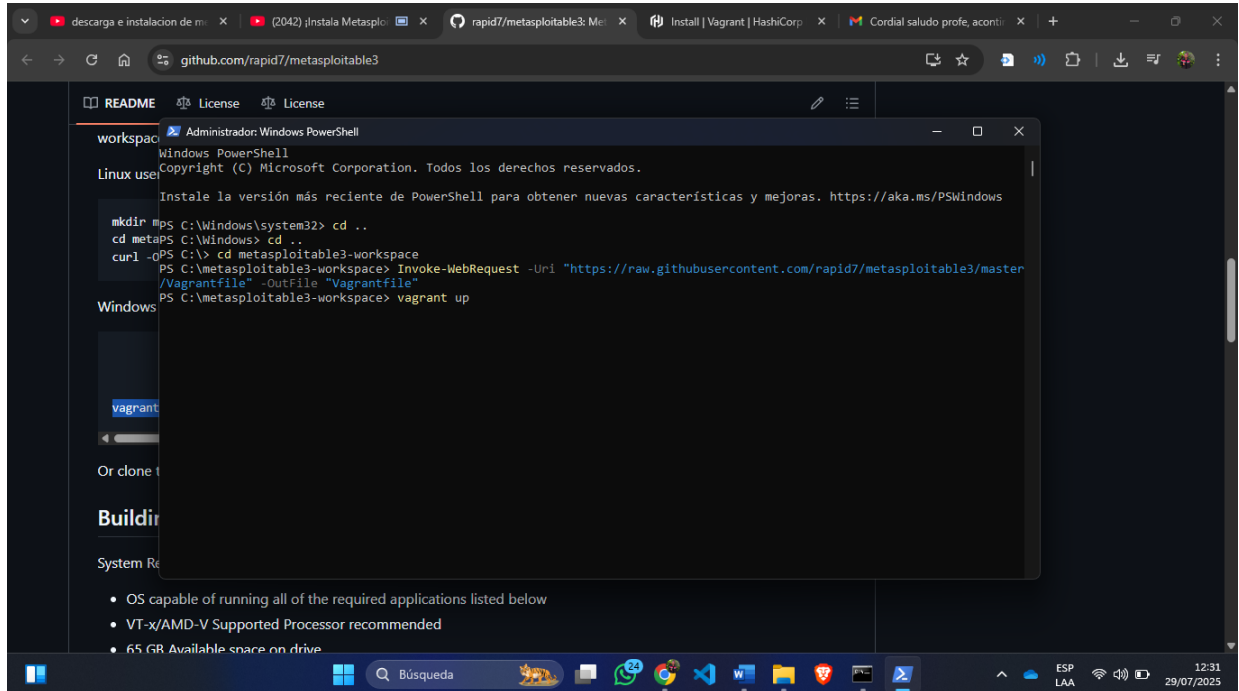


Ilustración 11: Ejecución de comandos desde PowerShell

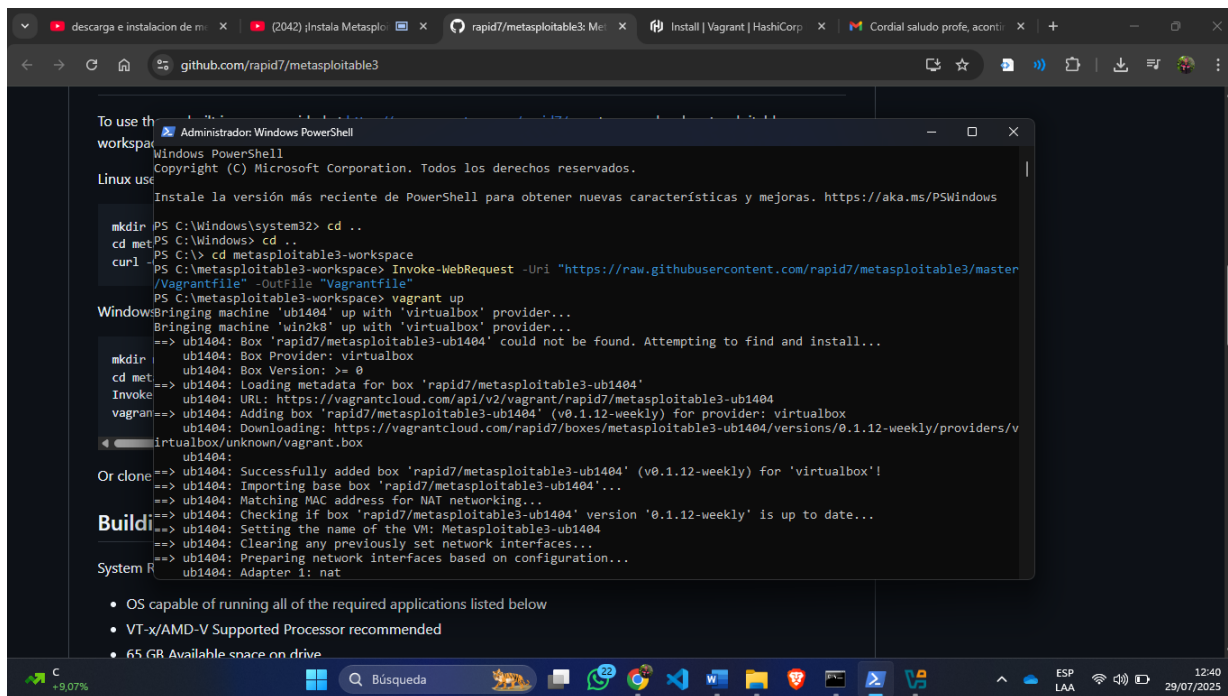
En esta imagen se observa la ejecución de comandos desde Windows PowerShell con privilegios de administrador. El usuario navega hacia el directorio de trabajo metasploitable3-workspace y ejecuta el comando Invoke-WebRequest para descargar el archivo Vagrantfile desde el repositorio oficial de Metasploitable 3 en GitHub. Posteriormente, se utiliza el comando vagrant up para iniciar la construcción y puesta en marcha de la máquina virtual. Este paso automatiza la creación del entorno vulnerable, siendo uno de los momentos clave del proceso de instalación de Metasploitable 3.



SEGURIDAD Y AUDITORIA DE REDES

Ing. Rafael Sandoval

Inicialización automática de la máquina virtual Metasploitable 3 con Vagrant



```
To use the workspace
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:\Windows\system32> cd ..
PS C:\Windows> cd ..
PS C:\> cd metasploitable3-workspace
PS C:\metasploitable3-workspace> Invoke-WebRequest -Uri "https://raw.githubusercontent.com/rapid7/metasploitable3/master/Vagrantfile" -OutFile "Vagrantfile"
PS C:\metasploitable3-workspace> 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: 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...
ub1404: Preparing network interfaces based on configuration...
ub1404: Adapter 1: nat

Or clone
Build
System R
• OS capable of running all of the required applications listed below
• VT-x/AMD-V Supported Processor recommended
• 65 GB Available space on drive
```

Ilustración 12: Inicio de descarga de Metasploitable 3

En esta imagen se muestra la salida generada en PowerShell tras ejecutar el comando `vagrant up`. El proceso automatizado comienza trayendo la máquina virtual base `ub1404` utilizando el proveedor `virtualbox`. Al no encontrar la imagen localmente, Vagrant la descarga desde el repositorio oficial de Vagrant Cloud (`rapid7/metasploitable3-ub1404`). Una vez descargada e importada, se procede a la configuración de la red y demás parámetros necesarios para levantar la máquina virtual. Esta fase es crítica, ya que valida la correcta conexión entre Vagrant y VirtualBox y marca el inicio del despliegue del entorno de pruebas de seguridad.



SEGURIDAD Y AUDITORIA DE REDES

Ing. Rafael Sandoval

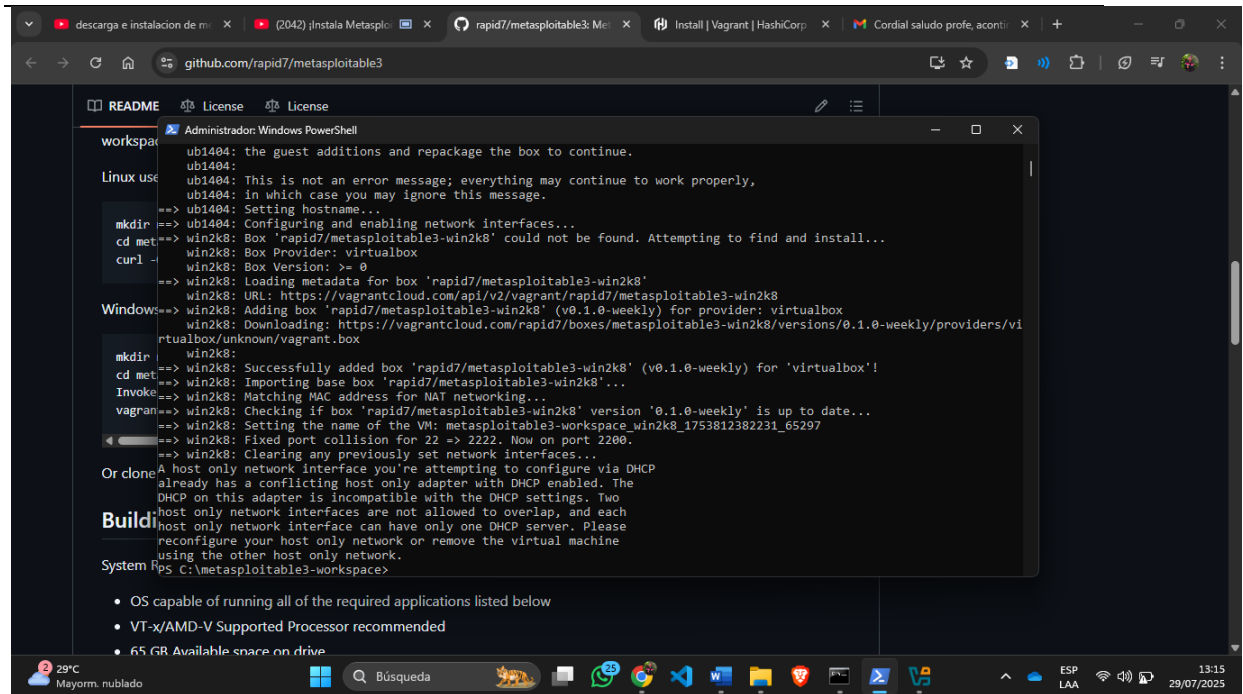


Ilustración 13: Instalación completada

Instalación completada



SEGURIDAD Y AUDITORIA DE REDES

Ing. Rafael Sandoval

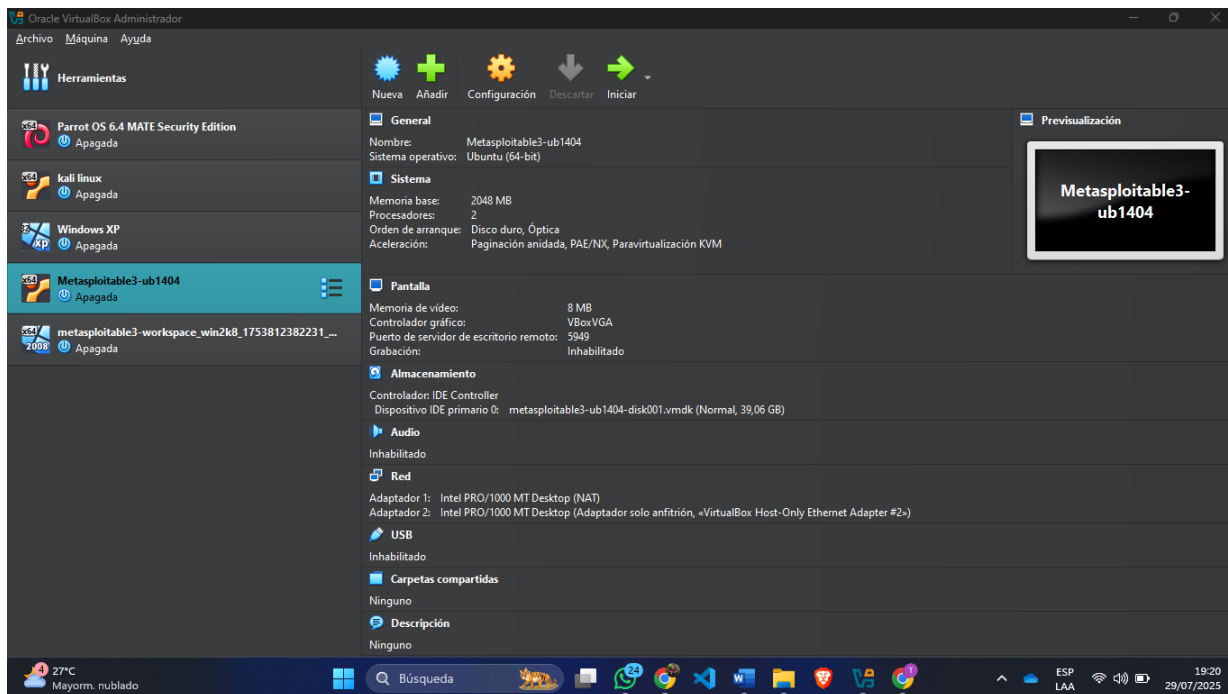


Ilustración 14: Maquinas reflejadas en Virtualbox

Se ven reflejadas las dos maquinas



SEGURIDAD Y AUDITORIA DE REDES

Ing. Rafael Sandoval

Interfaz gráfica de Metasploitable 3 en VirtualBox

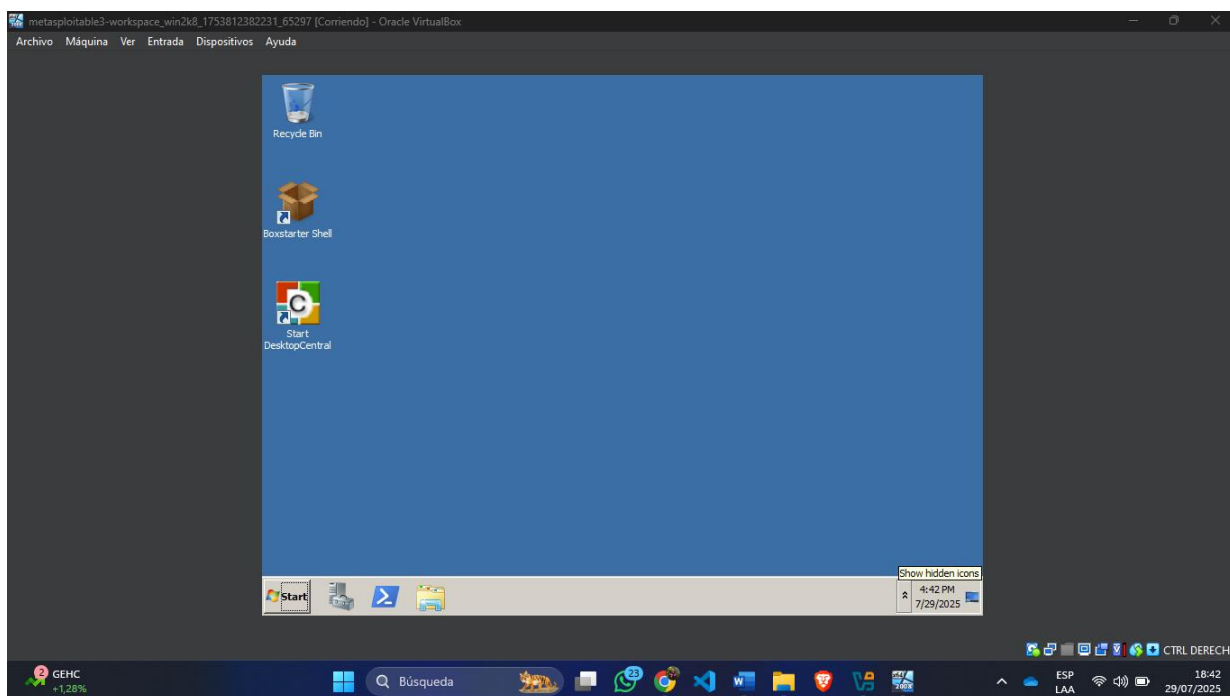


Ilustración 15: Interfaz gráfica de Metasploitable 3

Esta imagen muestra la máquina virtual de Metasploitable 3 ejecutándose en VirtualBox con una interfaz gráfica tipo Windows. Se observan accesos directos en el escritorio como “Boxstarter Shell” y “Start DesktopCentral”, los cuales forman parte del entorno vulnerable intencionalmente configurado con múltiples servicios expuestos. La presencia de este entorno permite realizar pruebas de penetración en condiciones controladas y reproducibles.



SEGURIDAD Y AUDITORIA DE REDES

Ing. Rafael Sandoval

Acceso a Metasploitable 3 (Ubuntu 14.04) mediante terminal

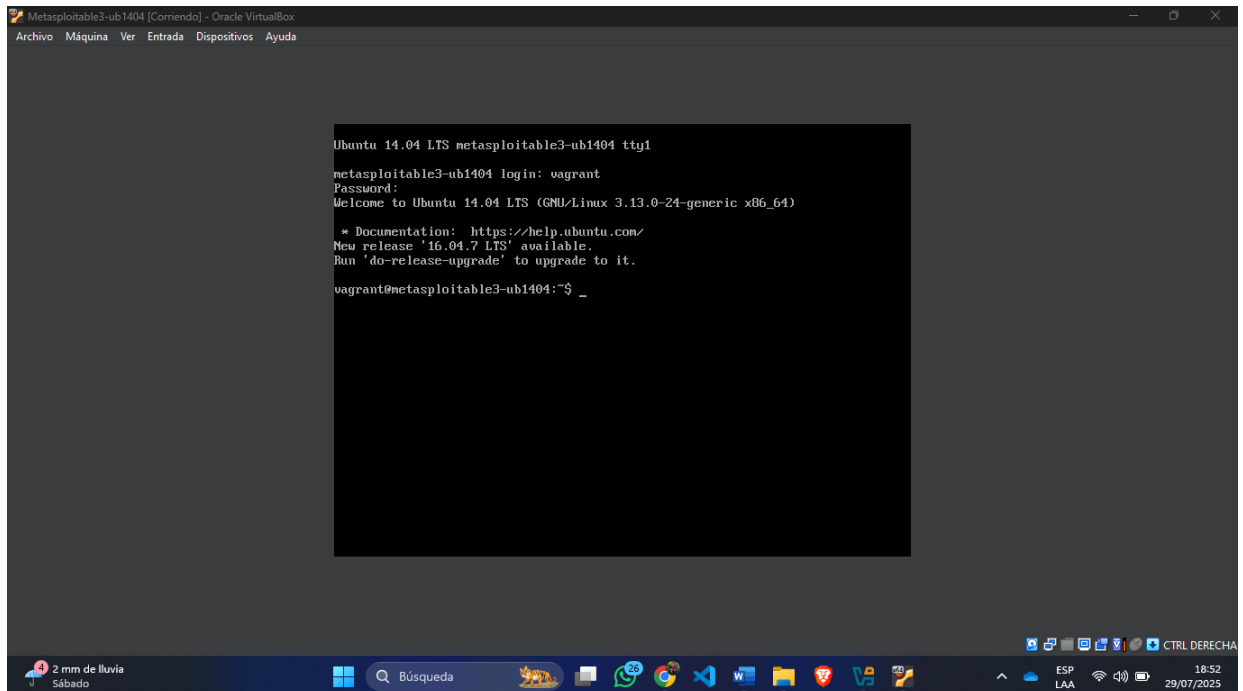


Ilustración 16: Acceso a Metasploitable 3 desde la terminal de Ubuntu

En esta segunda imagen se observa la máquina virtual metasploitable3-ub1404 corriendo en modo consola dentro de VirtualBox. El sistema operativo es Ubuntu 14.04 LTS, y se ha accedido con las credenciales por defecto (vagrant / vagrant). Esta terminal representa el entorno de backend del sistema vulnerable, donde se pueden ejecutar pruebas de seguridad, explotación de vulnerabilidades y análisis forense desde el sistema huésped.



SEGURIDAD Y AUDITORIA DE REDES

Ing. Rafael Sandoval

Recomendaciones

- **Tener conexión a Internet estable:** Algunos paquetes se descargan desde repositorios en línea; si se interrumpe la conexión, puede fallar la instalación.
- **Ejecutar PowerShell como administrador:** Es necesario para que los comandos tengan los permisos adecuados.
- **Espacio en disco:** Asegúrate de tener al menos 65 GB libres, ya que la instalación y creación de la máquina virtual puede ocupar bastante espacio.
- **VirtualBox actualizado:** Una versión desactualizada puede generar errores al importar o ejecutar la máquina virtual.

4. Conclusión

La instalación de Metasploitable 3 permite contar con un entorno de pruebas donde se pueden practicar ataques éticos y técnicas de seguridad sin causar daño a otros equipos. Aunque el proceso tiene varios pasos, es posible completarlo con éxito si se siguen las instrucciones con cuidado y se cuenta con los programas necesarios.

Esta máquina virtual es una excelente opción para aprender de manera práctica sobre vulnerabilidades, ataques comunes y cómo proteger los sistemas. Es ideal para personas en formación del área o cualquier interesado en el mundo de la ciberseguridad. Usar Metasploitable 3 ayuda a mejorar habilidades técnicas, prepararse para retos profesionales y entender mejor cómo defender los sistemas informáticos.



SEGURIDAD Y AUDITORIA DE REDES

Ing. Rafael Sandoval

5. Bibliográfica

Rafael Sandoval Morales (2025). Manual instructivo de descarga e instalación de Metasploitable 3 sobre una máquina virtual