Manual Técnico

INSTALACIÓN DE SOFTWARE

MANUAL TECNICO DE DESCARGA E INSTALACIÓN DE METASPLOIT 3

VICTOR MANUEL LONGA MENA

UNIVERSIDAD TECNOLOGÍA DEL CHOCO "DIEGO LUIS CÓRDOBA"
FACULTAD DE INGENIERÍA
INGENIERIA DE TELECOMUNICACIONES
2720409: SEGURIDAD Y AUDITORIA DE REDES
QUIBDÓ-CHOCO (COLOMBIA)
2025

MANUAL TECNICO DE DESCARGA E INSTALACIÓN DE METASPLOIT 3

VICTOR MANUEL LONGA MENA

Estudiantes, IX semestre

ING. RAFAEL S MORALES

Docente de la asignatura

UNIVERSIDAD TECNOLOGÍA DEL CHOCO "DIEGO LUIS CÓRDOBA"

FACULTAD DE INGENIERÍA

INGENIERIA DE TELECOMUNICACIONES

2720409: SEGURIDAD Y AUDITORIA DE REDES

QUIBDÓ-CHOCO (COLOMBIA)

2025

Tabla de Contenido

Tabla de Figuras

Introducción

El presente manual describe de manera detallada el procedimiento necesario para llevar a cabo la descarga e instalación de Metasploit 3, una de las herramientas más reconocidas en el ámbito de la seguridad informática ofensiva. Su propósito es guiar paso a paso al lector en la correcta obtención e implementación del software dentro de un entorno controlado, garantizando la comprensión de los aspectos técnicos y prácticos relacionados con su instalación inicial.

Este documento está orientado al desarrollo de competencias en auditoría de seguridad y pruebas de penetración, en un marco estrictamente académico y con fines educativos. A lo largo de las instrucciones, se resaltan aspectos esenciales como la preparación del entorno, la configuración de los recursos necesarios y la verificación de la correcta instalación de Metasploit 3. De esta manera, el manual no solo pretende servir como guía técnica para la descarga, sino también como apoyo en la formación de conocimientos básicos de ciberseguridad ofensiva, fomentando la responsabilidad y el uso ético de las herramientas presentadas.

Alcance

Este manual tiene como alcance principal llegar a estudiantes, docentes y profesionales en formación dentro del área de la seguridad informática, con el propósito de proporcionar una guía clara y estructurada sobre el proceso de descarga e instalación de Metasploit 3.

El documento en cuestión se limita exclusivamente a:

- Describir los pasos necesarios para obtener el software de fuentes oficiales.
- Explicar el procedimiento de instalación en un entorno controlado.
- Detallar las configuraciones básicas requeridas para asegurar el correcto funcionamiento de la herramienta.
- Presentar recomendaciones para el uso responsable y ético de Metasploit en contextos académicos y de investigación.

Dentro del manual no se abordara el uso avanzado de Metasploit Framework ni el desarrollo de exploits personalizados, ya que su objetivo principal se centra en la instalación inicial y en la preparación del entorno para posteriores prácticas de auditoría de seguridad.

.

1. Objetivos

1.1.General

Proporcionar una guía clara y estructurada que permita realizar la descarga e instalación de Metasploit 3 de manera correcta, dentro de un entorno controlado, con fines académicos y de formación en seguridad informática.

1.2.Específicos

- Conseguir Metasploit 3 desde fuentes seguras con el fin de evitar posibles descargas de virus maliciosos dentro de nuestros pc.
- Instalarlo en un entorno controlado, como una máquina virtual de VirtualBox o VMware, que son softwares para crear maquinas virtuales-
- Hacer las configuraciones básicas para que el programa funcione correctamente y sin mayores problemas.
- Tener una primera idea de cómo preparar tu entorno para futuras prácticas de auditoría y pruebas de seguridad.

2. Planteamiento Del Problema

En un entorno cada vez más digitalizado e interconectado, las organizaciones, instituciones educativas y usuarios particulares dependen en gran medida de sistemas informáticos que ofrecen múltiples servicios en red. Esta creciente dependencia ha traído consigo una expansión de la superficie de ataque, es decir, el conjunto de puntos vulnerables por donde un atacante podría comprometer la seguridad d En la actualidad, la ciberseguridad se ha convertido en un aspecto esencial para organizaciones, instituciones educativas y usuarios particulares, debido a la creciente dependencia de sistemas informáticos y redes interconectadas. Esta realidad ha generado la necesidad de contar con herramientas que permitan comprender, analizar y mitigar posibles vulnerabilidades antes de que sean aprovechadas por atacantes malintencionados.

En el ámbito académico, uno de los principales retos consiste en brindar a los estudiantes la posibilidad de adquirir experiencia práctica en auditoría de seguridad y pruebas de penetración. No obstante, realizar este tipo de prácticas directamente sobre sistemas reales implica riesgos éticos, legales y técnicos que pueden comprometer la estabilidad de los entornos de trabajo. Por esta razón, el uso de entornos controlados y herramientas específicas se vuelve indispensable para un aprendizaje responsable y seguro.

Metasploit Framework se ha consolidado como una de las herramientas más utilizadas para la explotación de vulnerabilidades en entornos de práctica, ya que facilita la comprensión de conceptos clave de la ciberseguridad ofensiva. Sin embargo, un obstáculo frecuente en los procesos formativos radica en que muchos estudiantes carecen de una guía clara sobre cómo descargar, instalar y configurar correctamente la herramienta, lo que dificulta su aprovechamiento pleno en escenarios educativos.

Este manual surge como respuesta a dicha necesidad, ofreciendo una explicación paso a paso sobre el proceso de descarga e instalación de Metasploit 3 en un entorno controlado. Con ello, se busca garantizar que los estudiantes puedan contar con la herramienta lista para su uso, favoreciendo el desarrollo de competencias prácticas en seguridad informática y fomentando un aprendizaje ético, seguro y estructurado.

3. Elementos Necesarios Para Descargar Metasploitable 3

Lo primero que debemos saber antes de comenzar a descargar Metasploitable 3 es cuales son los elementos y/o aplicaciones necesarias para poder descargar este repositorio. Las condiciones necesarias para descargar metasploitable 3 son:

- Tener descargado VirtualBox o cualquier otro gestor de maquinas virtuales que nos permita tener una o mas maquinas virtuales
- Descargar Vagrant para poder levantar entornos de desarrollo de manera rápida y segura.
- Tener sistema operativo anfitrión compatible que permita descargar lo antes mencionado.
- Tener un pc que cumpla con las características de hardware optimas para poder trabajar con este repositorio. Las características mínimas pueden ser Procesador con al menos 2 núcleos (idealmente 4 o más), 8 GB de memoria RAM (mínimo 4 GB, pero puede quedarse corto), 60 GB de espacio libre en disco duro.
- Tener una conexión a internet estable para la descarga de dependencias y repositorios necesario para trabajar con Metasploitable 3.

4. Paso 1: Descargamos VirtualBox

Si se tiene descargado VirtualBox se puede omitir este paso, de lo contrario lo primero que haremos es ir al enlace https://www.virtualbox.org/wiki/Downloads o seguir el paso a paso que se detallara a continuación.

4.1. ¿ Cómo Descargar VirtualBox?

El paso a paso para descargar VirtualBox es muy sencillo en realidad, lo primero que debemos hacer es desde nuestro navegador buscar la página oficial de Oracle VirtualBox o ingresar al enlace dado anteriormente, si se eligió el enlace

Así.

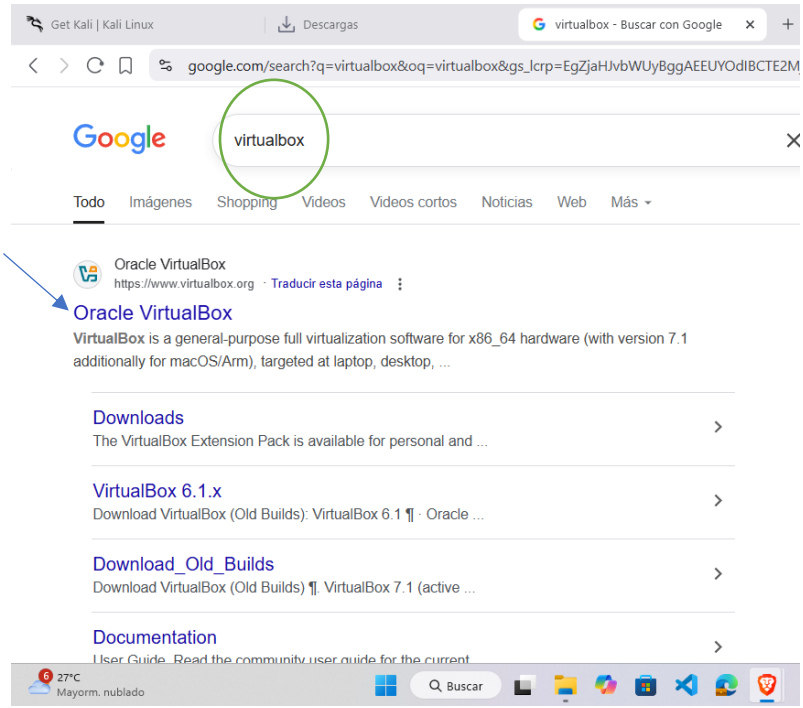

Figura 1. Búsqueda de la Pagina Para Descargar VirtualBox

Luego ingresamos a la página de encontraremos lo siguiente.

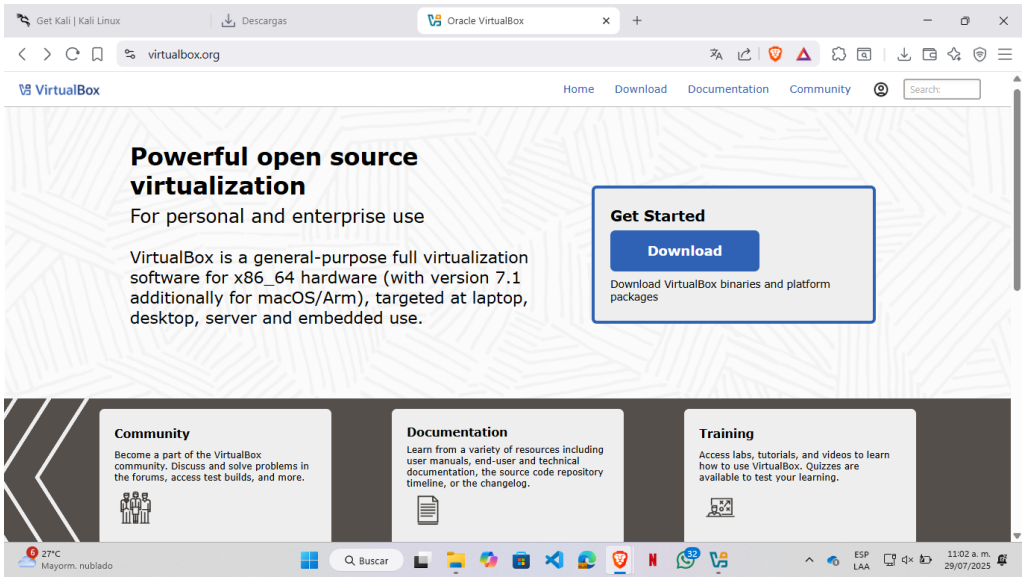

Figura 2. Página Oficial de VirtualBox Para Descargarlo

Estando aquí elegimos el botón azul y fuimos a otra ventana.

Figura 3. Selección Del Sistema en el Que se Usara VirtualBox

En esta ventana, seleccionamos Windows porque es el sistema operativo de nuestro pc. Luego comenzara nuestra descarga. En algunos navegadores tendremos que elegir la carpeta en donde nuestro archivo se guardara, en otro la descarga se guarda automáticamente en la carpeta de descarga, en mi caso elegí la carpeta en donde se guardó mi ISO y ahí guarde el archivo de descarga de VirtualBox.

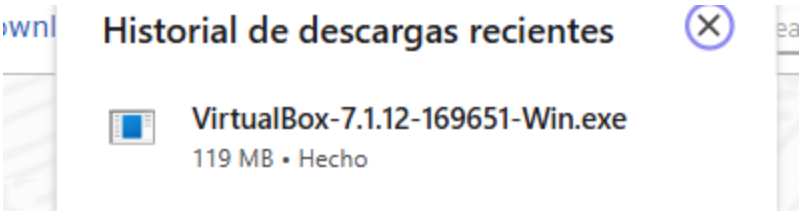

Figura 4. Descarga de VirtualBox terminada

La imagen anterior muestra nuestra descarga terminada.

4.2.Instalación de VirtualBox

Para descargar VirtualBox el proceso es prácticamente el mismo paso que en VMware, primero buscamos el setup.

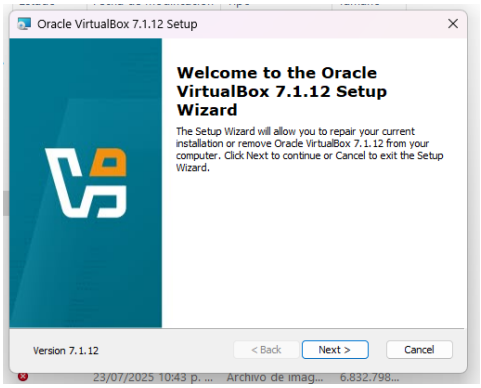

Figura 5. Abrimos el Setup

Luego de ingresar a esta sección le damos en next para ir a la siguiente página.

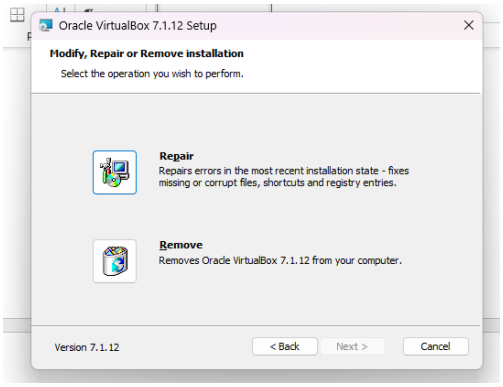

Figura 6. Seleccionamos Nuestra Opcion

Para mi caso, me salen estas opciones porque ya tengo el VirtualBox instalado, pero elegiré la opción de reparar para seguir descargando la aplicación.

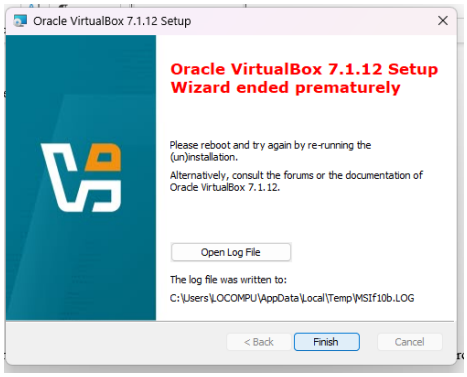

Figura 7. Ventana Final

Si no tiene el VirtualBox descargado simplemente le das siguiente a todas las opciones y ya estaríamos así.

Figura 8. VirtualBox Desde el Escritorio

Aquí podemos ver el software VirtualBox en nuestro escritorio luego de hacer la instalación pertinente.

Según (Oracle, 2024) "*VirtualBox es un software de virtualización completo de propósito general para hardware x86_64 (con la versión 7.1 adicionalmente para macOS/Arm), dirigido a computadoras portátiles, computadoras de escritorio, servidores y uso integrado*."

4.2.1 Características de VirtualBox

Según Oracle las principales características de VirtualBox son:

- Soporte para sistemas operativos invitados como Debian, Ubuntu, Kali Linux, Windows, entre otros.
- Configuración flexible de recursos (memoria, CPU, almacenamiento).
- Compatibilidad con imágenes ISO, instantáneas del sistema, carpetas compartidas, USB y red virtual.
- Comunidad activa y documentación abundante

VirtualBox se destaca por ser gratuito, multiplataforma y fácil de usar, lo que lo convierte en una herramienta educativa ideal para prácticas de sistemas operativos, redes y seguridad informática (Oracle, 2024).

5. Paso 2: Descargamos Vagrant

Para descargar Vagrant lo primero que hacemos es ingresar al siguiente enlace o en su efecto buscamos la página oficial en nuestro navegador https://developer.hashicorp.com/vagrant/install#windows lo que nos abrirá la siguiente página.

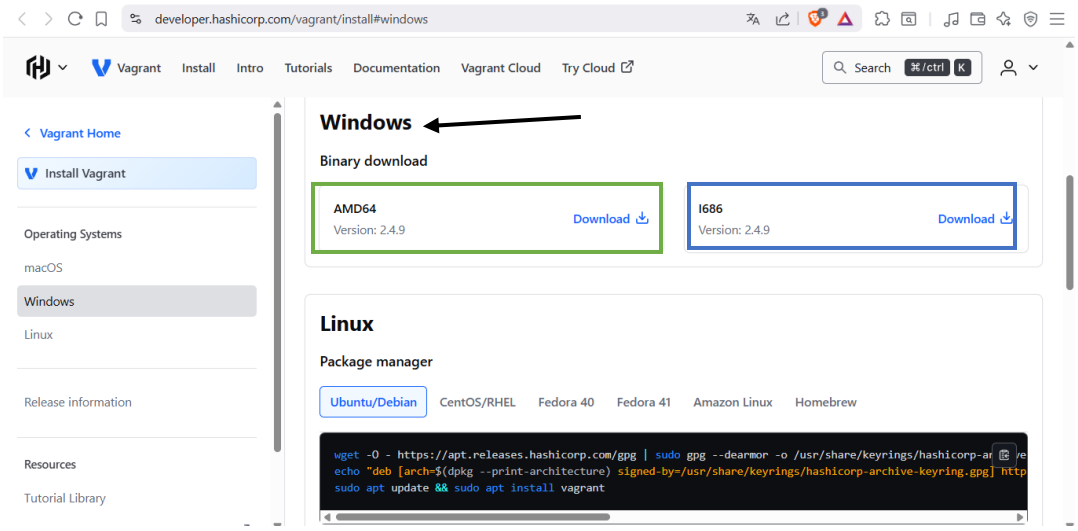

Figura 9.Vista de la Página de Vagrant

Luego de estar en la sección que se mostró anteriormente elegiremos el sistema en donde descargaremos este software (flecha negra) y luego se descargara según el procesador de nuestro pc que puede ser Intel (cuatro verdes) o AMD (cuatro azules) en mi caso tengo un procesador AMD por lo es obvio saber mi elección.

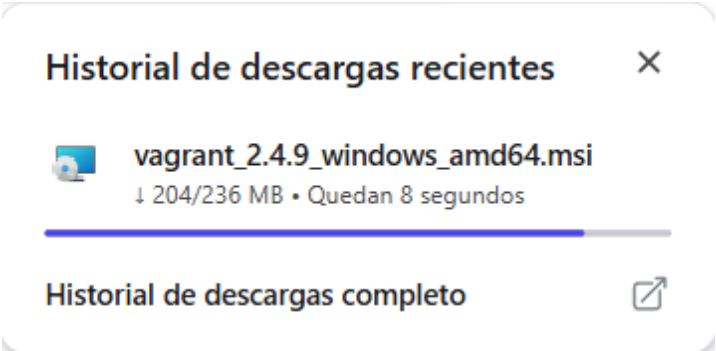

Figura 10. Descarga de Vargrant

La figura 6 (Ver figura 6) muestra cómo se está descarando nuestra aplicación

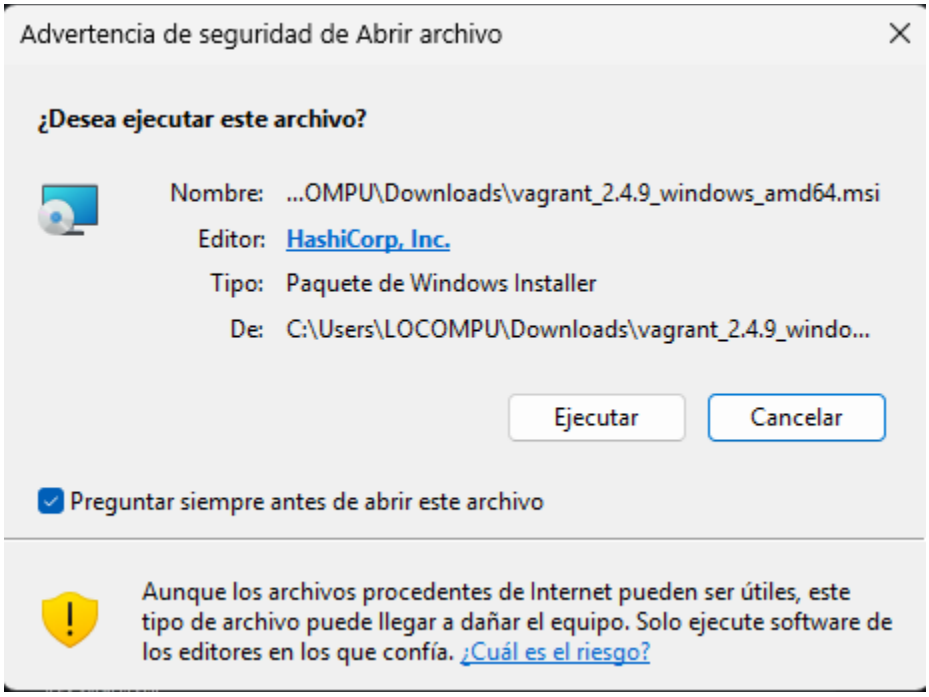

Figura 11. Ejecutamos el Setup Descargado

Luego de que se termine de descargar el setup que descargamos o lo ejecutamos para empezar la instalación de este software.

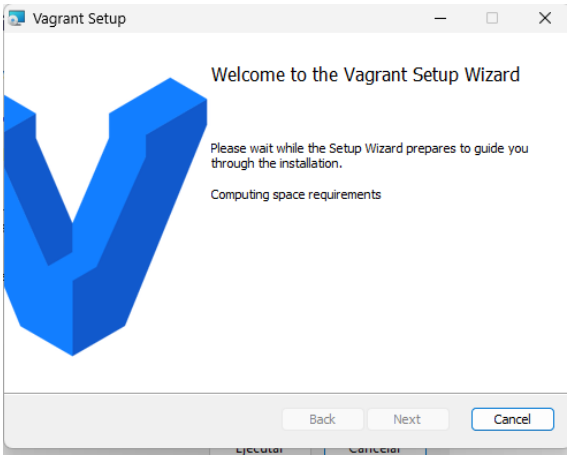

Figura 12. Esperamos a Que se Prepare la Guía de Instalación

Aquí debemos esperar que se nos indique como debemos proceder para descargar este software.

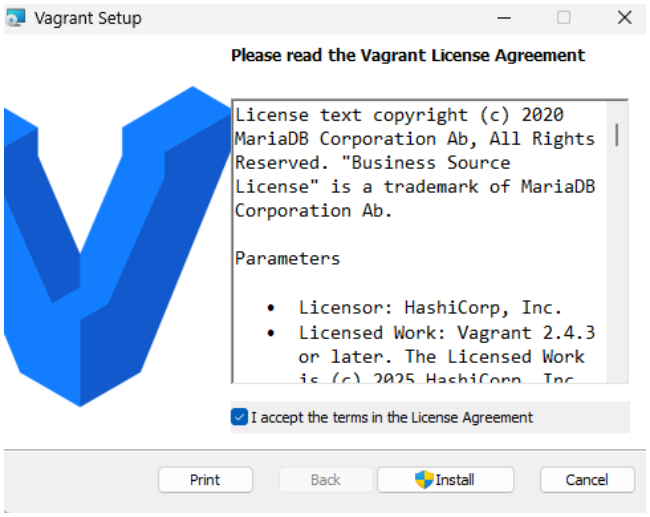

Figura 13. Seguimos la guía de Instalación para Vagrant

A continuación, se sigue la guía de instalación para Vagrant, esto puede tardar algunos minutos. Aquí le damos aceptamos los términos y condiciones (Recomiendo siempre leer estos términos) y le damos instalar

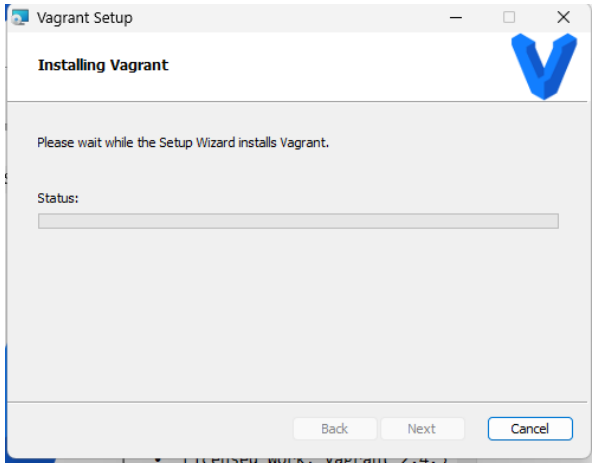

Figura 14. Esperamos Que Termine la Instalación

Aquí ya nos queda esperar que termine la instalación sin dejar de estar pendientes a cualquier permiso que se nos solicite.

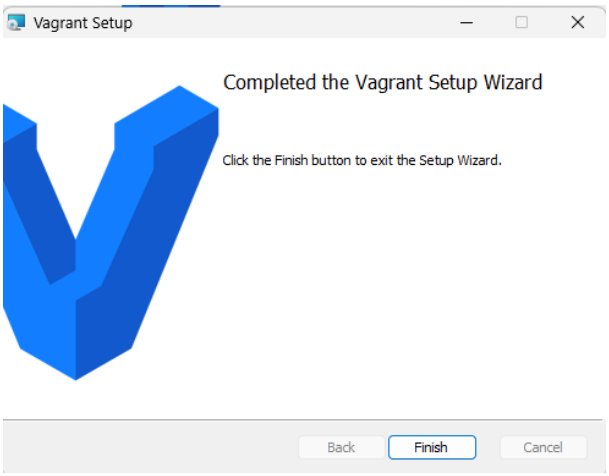

Figura 15. Finaliza la instalación de Vagrant

Luego de que finalice esta instalación y le demos en el botón finish se nos reiniciara el pc y todo quedara listo.

Figura 16. Vagrant Instalado

En esta imagen se muestra como a app ya está instalada en nuestro pc y procedemos a realizar el siguiente paso.

6. Paso 3: Descargamos el repositorio para Metasploitable 3

Para el 3 paso lo que hacemos es ir al enlace del repositorio de GitHub de donde descargaremos Metasploitable 3. El enlace del que lo bajaremos se presenta a continuación.

https://github.com/rapid7/metasploitable3

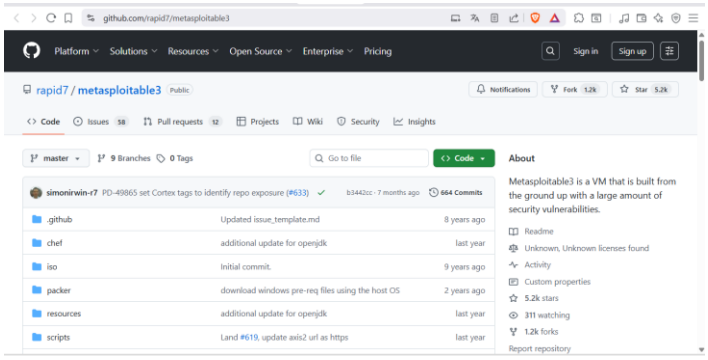

Figura 17. Vista Del Repositorio

De este repositorio lo que realmente necesitamos son los comando que encontraremos aquí, para visualizar esos comandos bajamos un poco y luego realizamos lo que se explicara a continuación.

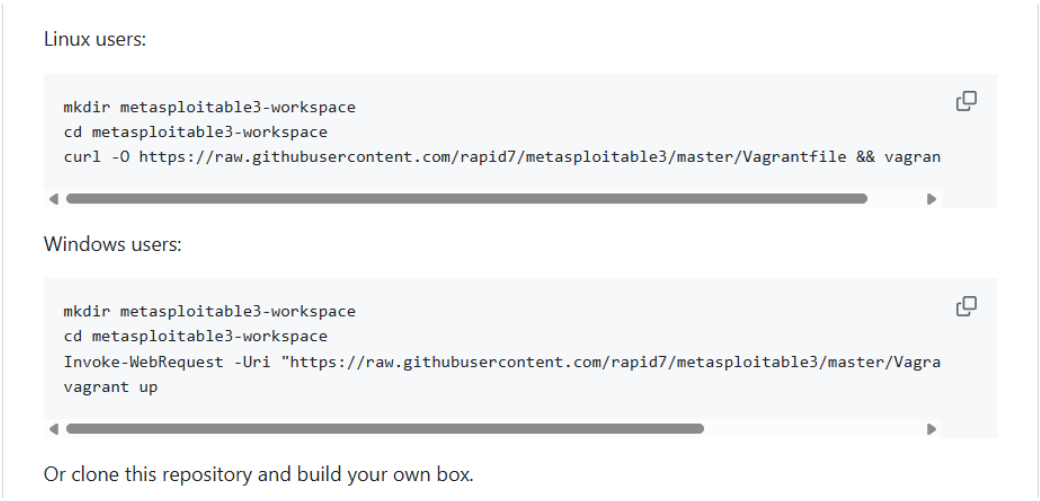

Figura 18. Comandos Necesarios Para Descargar Metasplo

Como vamos a utilizar algunos comados que se muestran aquí necesitamos abrir una consola de comandos o cmd

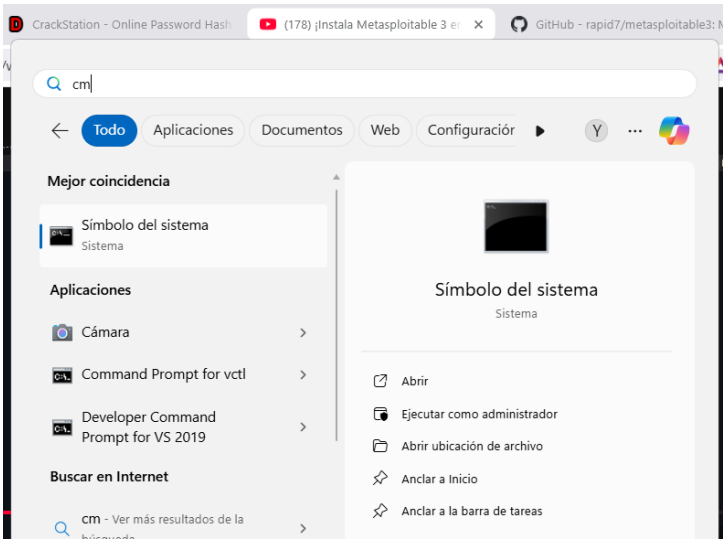

Figura 19. Se Abre el Cmd

Para abril el cmd o la consola de símbolos del sistema lo primero que hacemos es ir al menú de aplicaciones de Windows y escribir Cmd o símbolos del sistema. Otra opción seria utilizar el comando Windows R y en el ejecutar escribimos cmd, para mi caso lo abri desde el menú por que necesitaba ejecutarlo como administrador.

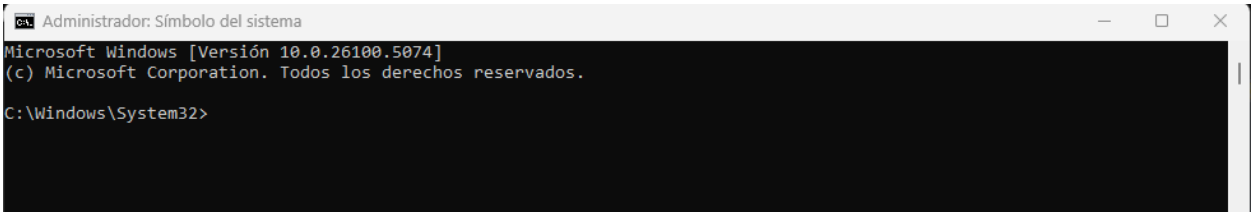

Figura 20. Cmd Abierto

Si ya estamos adentro de la consola cmd, lo siguiente será ejecutar el comando **cd..** comando utilizado para salirnos de la carpeta system32 hacemos esto hasta que lleguemos a la carpeta raíz **C:/**

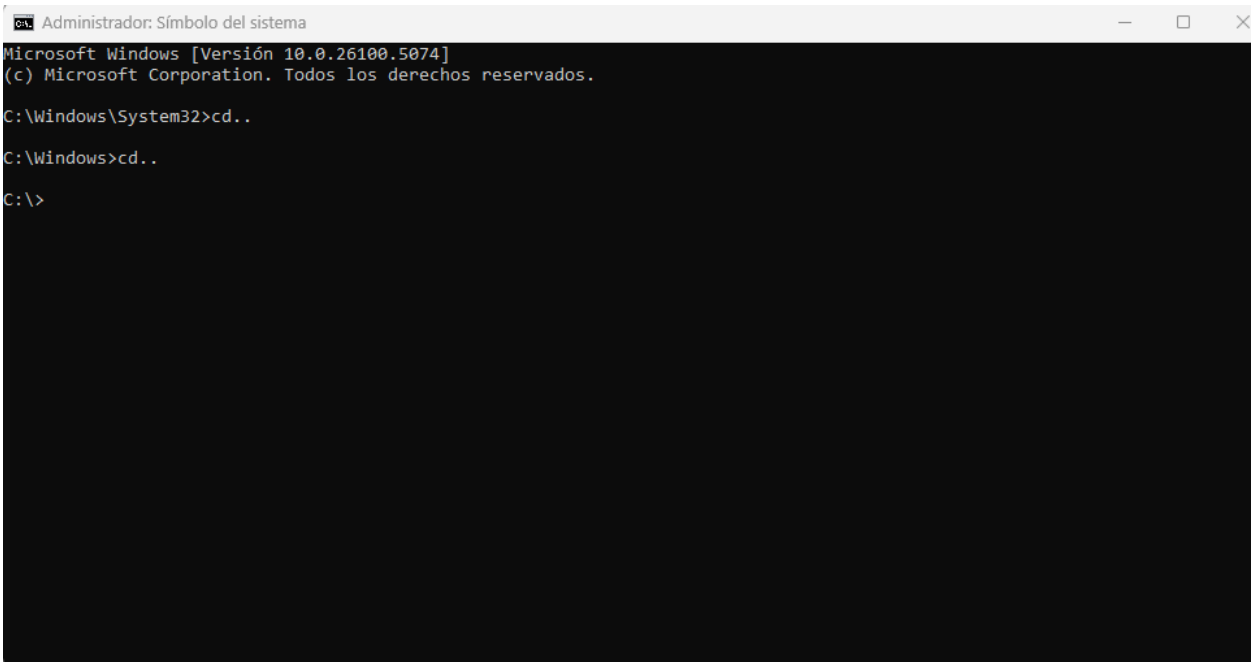

Figura 21. Llegamos a la Carpeta Raíz Usando CD..

Cuando estemos en la carpeta raíz, ingresamos el comando **mkdir metasploitable3-workspace** este comando nos permite crear una carpeta de nombre: **metasploitable3-workspace**, en nuestra carpera raíz

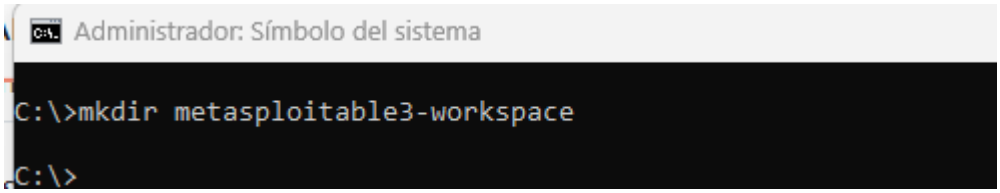

Figura 22. Comandos Mkdir Insertado

Si observan ya ingresamos el comando, las siguientes 2 imágenes que se muestran a continuación muestran como fue el antes y después de la creación de la carpeta

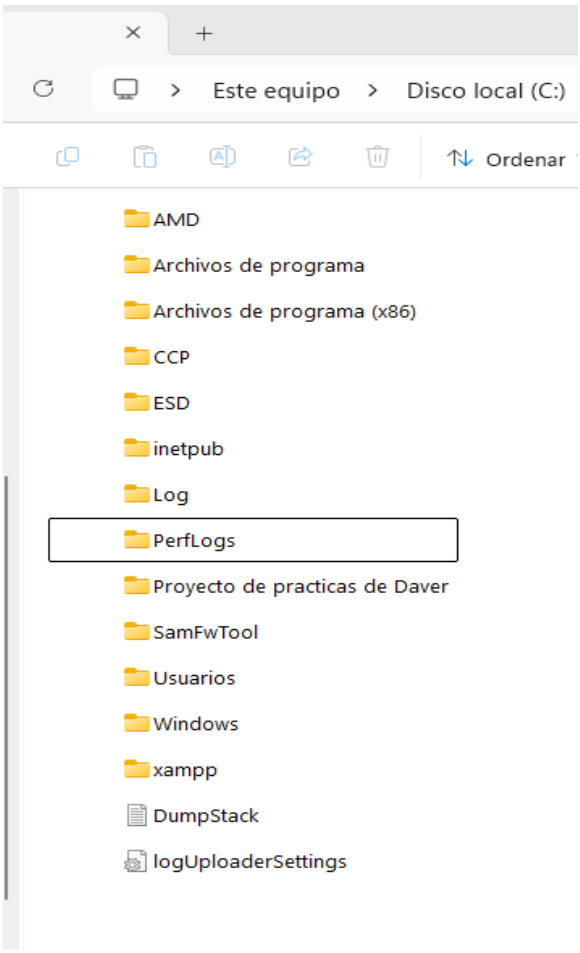

Figura 23. Antes del MKDIR

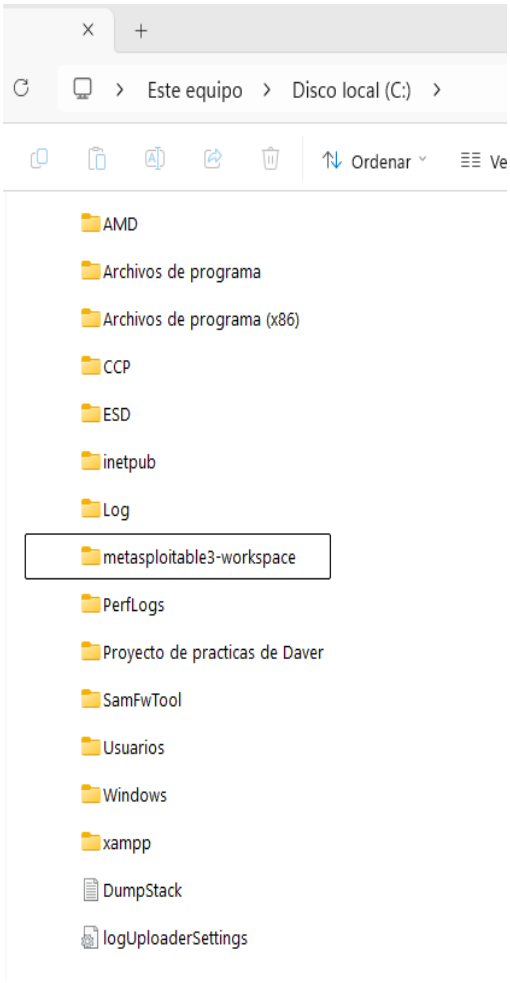

Figura 24. Después del MKDIR

Aquí podemos ver como luego de usar el comando dado anteriormente se crea una carpeta llamada **metasploitable3-workspace**, en nuestra carpera raíz

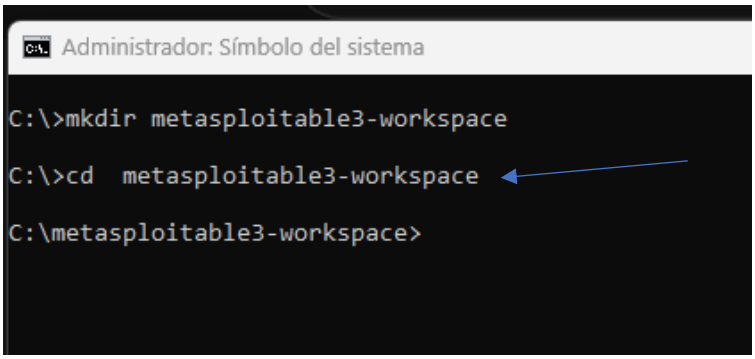

Figura 25. Ingresamos a la Carpeta Usando el Comando CD junto al Nombre de la Carpeta

Después ingresamos el comando **cd metasploitable3-workspace** (fecha azul) esto lo hacemos para verificar que efectivamente si se haya creado la carpeta con ese nombre, luego de esto lo que haremos es abrir una sección en la consola de PowerShell

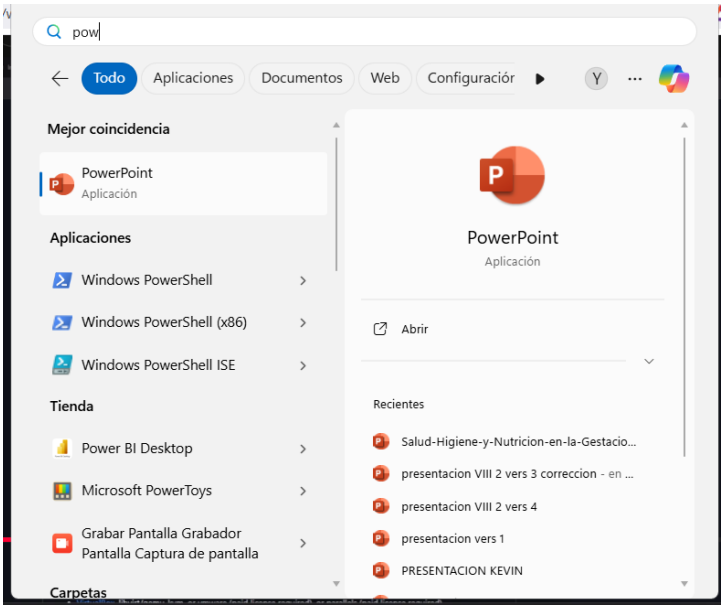

Figura 26. Abrimos la Consola de PowerShell

Para abrir la consola mencionada anteriormente volvemos a abrir el menú de aplicaciones de Windows y buscamos PowerShell, luego la ejecutamos como administrador y nos saldrá esta ventana.

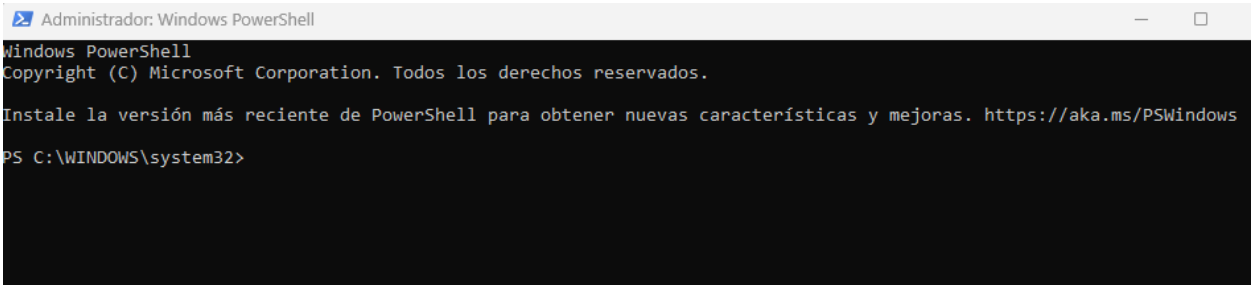

Figura 27. Consola de PowerShell

Luego de que entremos a nuestra consola debemos regresar a la la raíz como hicimos en el cmd, esto lo hacemos usando el comando cd..

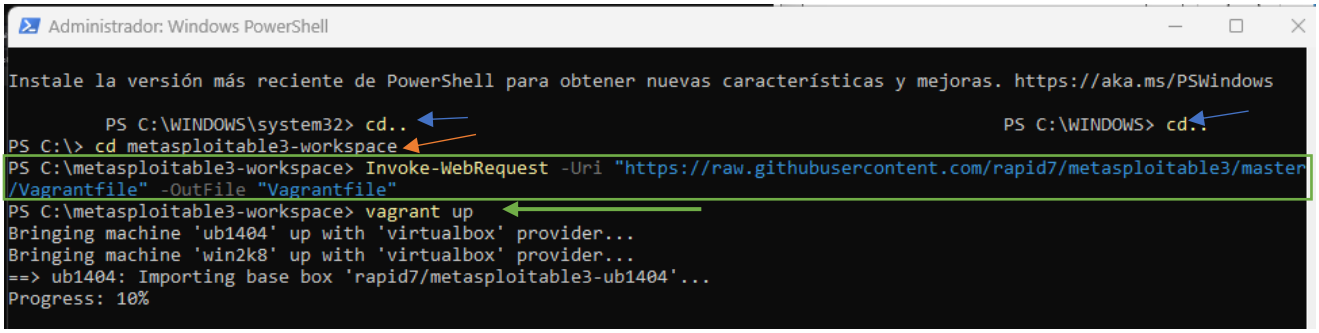

Figura 28. Aplicamos Los Comandos Para Descargar Metasp

Aquí luego de volver a la carpeta raíz con el comando **cd..** (flechas azules) ingresamos a la carpeta de nombre **metasploitable3-workspace** (flecha naranja) cuando ingresemos aquí lo siguiente será escribir el comando:

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

Por último, ingresamos el comando **vagrant up** (flecha verde) este comando es importante por que permite inicializar la descarga de metasploitable.

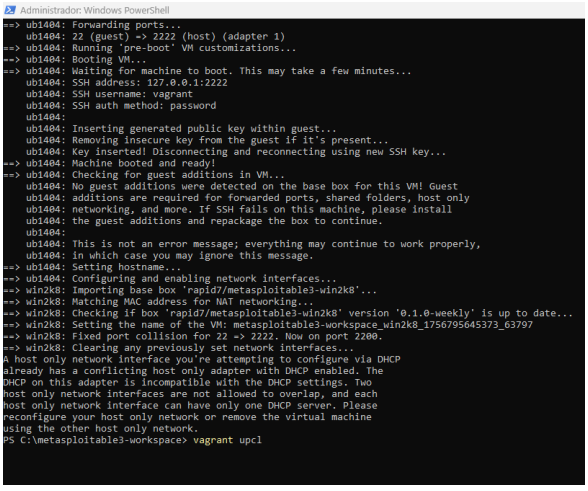

Figura 29. Se visibiliza la Descarga

Después de terminar la descarga nos saldrán 2 maquinas virtuales, una de Ubuntu y otra de Windows, estas máquinas nos permitirán hacer nuestras practicas aquí.

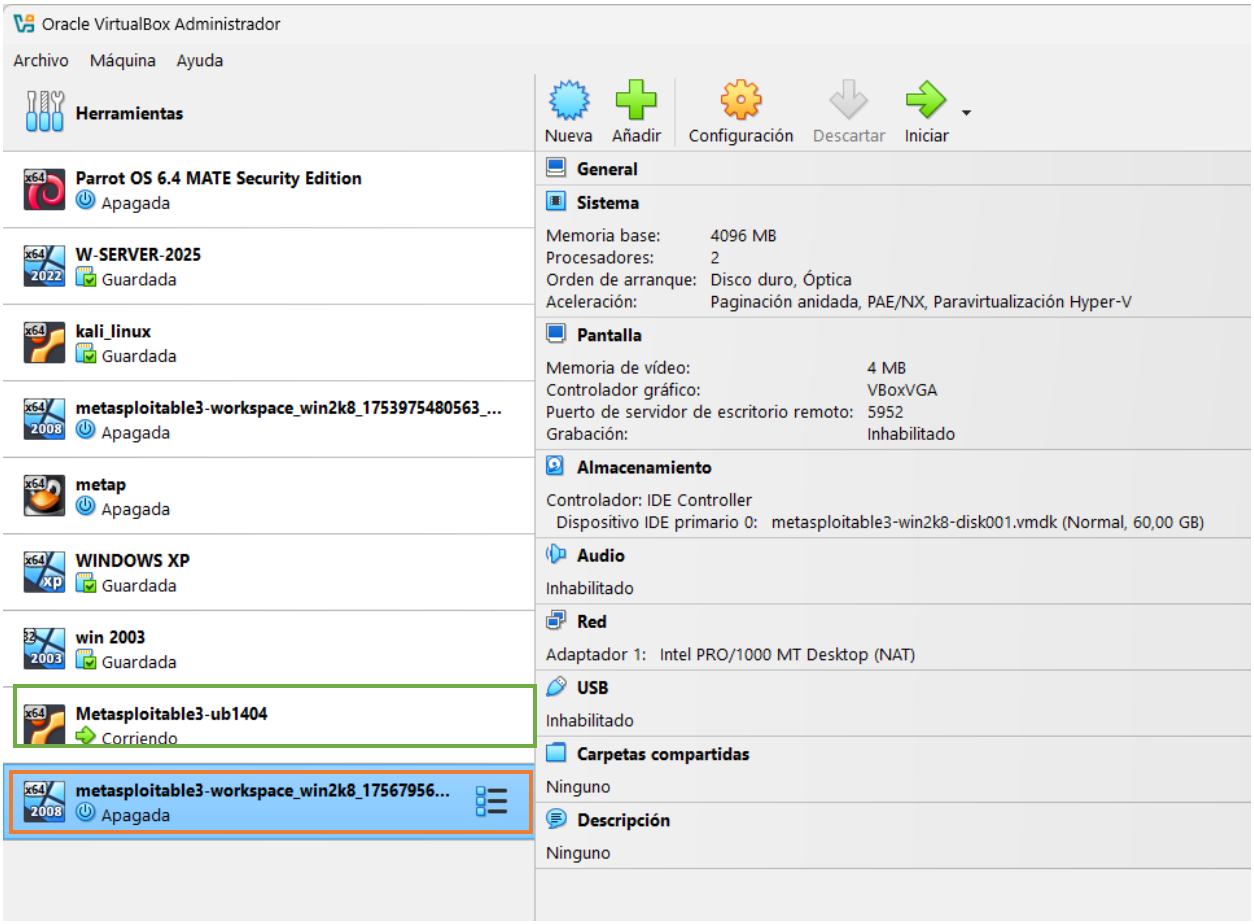

Figura 30. se Visualizan las Maquinas en VirtualBox

Ya llegado a este punto podemos ver como nuestras máquinas virtuales están en virtual box. Los datos de ingreso usuario y contraseña de nuestras máquinas virtuales son:

Usuario: vagrant

Contraseña: vagrant

7. Verificación de la Instalación.

Probamos que lo hecho funcione arrancando las maquinas.

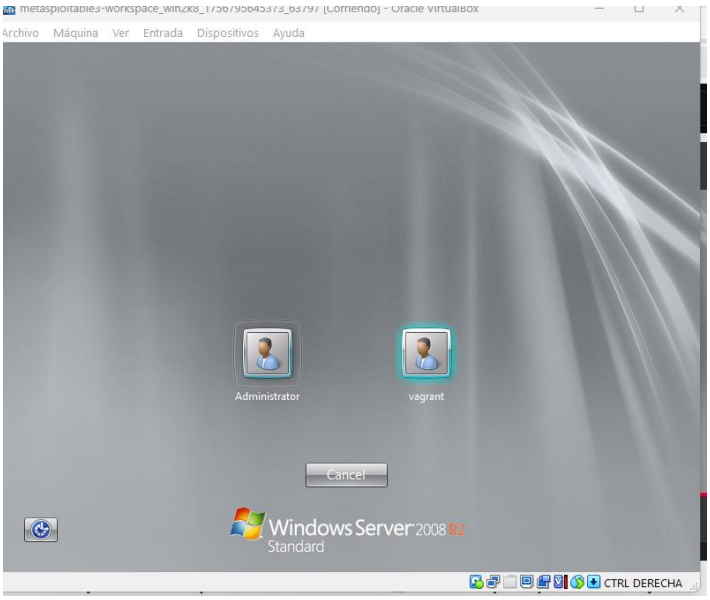

Figura 31. Arrancamos la Máquina Virtual de Windows Server 2008.

Para probar que lo hecho si funciona arrancamos las dos máquinas, en este caso se arranca la máquina de Windows server 2008.

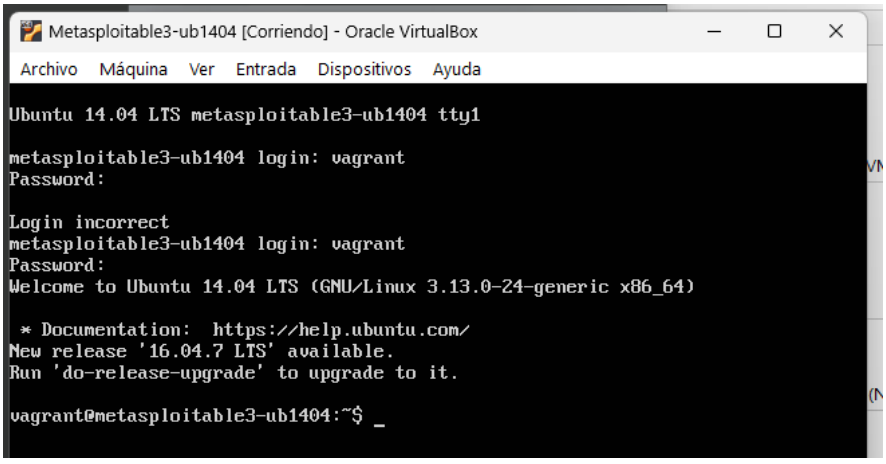

Figura 32. Arranque de Ubuntu

Aquí luego arrancamos la máquina virtual de Ubuntu en este caso si iniciamos sección en Ubuntu servidor. Así termina manual.

Conclusión

La correcta descarga e instalación de Metasploit 3 constituye el primer paso para el desarrollo de prácticas en seguridad informática dentro de un entorno controlado y académico. A través de este manual ofrecemos una guía clara y estructurada que facilita al estudiante la preparación de su equipo de trabajo, garantizando que cuente con todos los elementos necesarios para ejecutar la herramienta de forma adecuada.

El proceso descrito permite comprender la importancia de seguir una metodología ordenada, desde la verificación de los requisitos previos hasta la comprobación final de la instalación, evitando errores comunes que suelen dificultar el aprendizaje inicial.

De esta manera, el manual no solo asegura que Metasploit quede operativo, sino que también promueve el uso responsable y ético de la herramienta, resaltando que su aplicación debe limitarse a contextos académicos y de investigación, siempre con el fin de fortalecer las competencias técnicas en auditoría y pruebas de penetración.

En conclusión, el documento cumple con el propósito de servir como apoyo práctico para quienes inician en el estudio de la ciberseguridad ofensiva, brindando un punto de partida sólido para posteriores ejercicios de exploración y explotación en entornos virtualizados.

Conclusión

Puedo concluir diciendo que la presente práctica permitió aplicar de forma progresiva y estructurada los conocimientos adquiridos sobre análisis de vulnerabilidades y pruebas de penetración en entornos controlados. A través del uso de herramientas especializadas como Nmap y Metasploit Framework, se logró identificar, evaluar y explotar múltiples servicios vulnerables presentes en la máquina virtual Metasploitable, tales como FTP, Telnet, Samba, MySQL, PostgreSQL y DNS.

Cada uno de los pasos realizados, desde el escaneo de red, la detección de servicios, hasta la ejecución de exploits, evidenció la importancia de comprender cómo las configuraciones débiles y las versiones obsoletas pueden ser aprovechadas por un atacante para obtener acceso no autorizado. Asimismo, se fortalecieron competencias técnicas relacionadas con la lectura de banners, el uso de módulos de explotación, la interpretación de errores y la validación de resultados.

En términos generales, la práctica resultó altamente importante para mí ya que me permite poner aprueba lo que vi en clase, tanto desde el punto de vista técnico como metodológico. No solo permitió afianzar los conceptos tratados en clase, sino que también sirvió como preparación efectiva para futuras evaluaciones prácticas y como ejemplo concreto de cómo debe estructurarse una prueba de penetración básica. Se concluye, por tanto, que el desarrollo del informe cumplió satisfactoriamente con los objetivos planteados.

Referencias Bibliográficas

Oracle. (2024). *VirtualBox: Powerful x86 and AMD64/Intel64 virtualization*. Oracle VM VirtualBox. https://www.virtualbox.org/

Simon, I. (2025). *Rapid7/metasploitable3* [HTML]. Rapid7. https://github.com/rapid7/metasploitable3 (Obra original publicada en 2016)

morcor (Director). (2024, diciembre 4). *¡Instala Metasploitable 3 en Minutos! 💻 Guía Completa para Hackers y Pentesters 🔥 2025* [Video recording]. https://www.youtube.com/watch?v=bnKpkW2890M

.