MANUAL DE INSTALACION DE METASPLOITABLE3

DANIEL SAMIR RODRÍGUEZ PALACIOS

Estudiantes, IX semestre

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFORMÁTICA

SEGURIDAD Y AUDITORIA DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

MANUAL DE INSTALACION DE METASPLOITABLE3

DANIEL SAMIR RODRÍGUEZ PALACIOS

Estudiantes, IX semestre

RAFEL SANDOVAL MORALES

Docente de asignatura

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFORMÁTICA

SEGURIDAD Y AUDITORIA DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

TABLA DE CONTENIDO

LISTA DE ILUSTRACIONES

Informe del Laboratorio #2 Manual de instalación de Metasploitable 3

Este informe presenta una guía detallada para la instalación de Metasploitable 3 en un entorno Windows, utilizando herramientas como VirtualBox, Vagrant, Packer y Git. El objetivo es documentar cada paso del proceso, desde la preparación del entorno hasta la construcción de la máquina virtual, asegurando que el lector pueda replicar la instalación de forma autónoma y confiable.

La implementación de este entorno vulnerable no solo facilita la exploración de técnicas ofensivas y defensivas en seguridad informática, sino que también promueve el desarrollo de habilidades críticas en análisis de servicios, detección de vulnerabilidades y aplicación de medidas de mitigación. En el marco del laboratorio académico, esta práctica se alinea con los objetivos formativos del programa de Ingeniería en Telecomunicaciones e Informática, fortaleciendo el dominio técnico en entornos controlados y éticamente responsables.

Objetivo general

Documentar el proceso de instalación de la máquina virtual vulnerable **Metasploitable 3** en un entorno Windows, con fines educativos y de práctica en hacking ético.

Requisitos Previos

Antes de iniciar el proceso, se deben instalar las siguientes herramientas:

Herramienta	**Descripción**	**Enlace de descarga**
VirtualBox	Plataforma de virtualización	virtualbox.org
Vagrant	Automatización de entornos virtuales	vagrantup.com
Packer	Generador de imágenes de máquina	packer.io
Git *(opcional pero recomendado)*	Control de versiones y clonación de repositorios	git-scm.com

Paso 1: Clonar el repositorio oficial

Abrir PowerShell o terminal y ejecutar: mkdir metasploitable3-workspace este comando nos crea una carpeta…

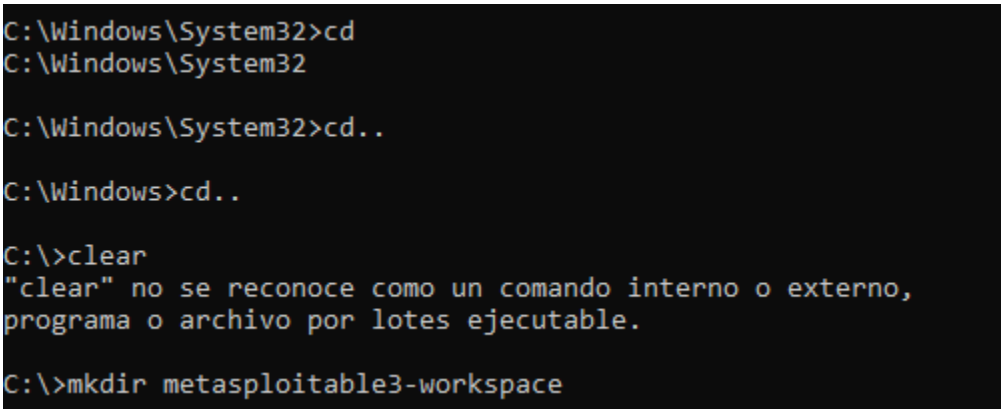
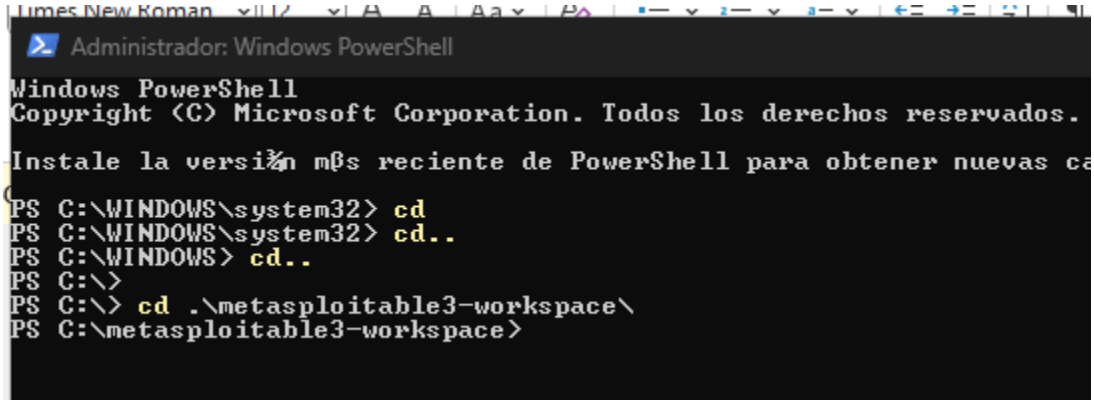


Ilustración 1creacion de la carpeta de metasploitable

Instalación de las maquinas a utilizar…

Luego ejecutamos Power Shell (en modo administrador), ya que esta nos permite instalar de manera correcta las dependencias y los programas a utilizar…



Aquí copiamos los siguientes comandos:

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

Y con este último: vagrant up es que nos instalara todo metasploitable3 y las demás maquinas que necesitamos

Ilustración 2 accediendo a la carpeta de metasploitable3-workspace

Instalación de los paquetes en virtualbox desde power Shell

Eso demora bastante, aun apenas están descargando los paquetes, una vez descargados adjuntare imágenes y pruebas de ellas

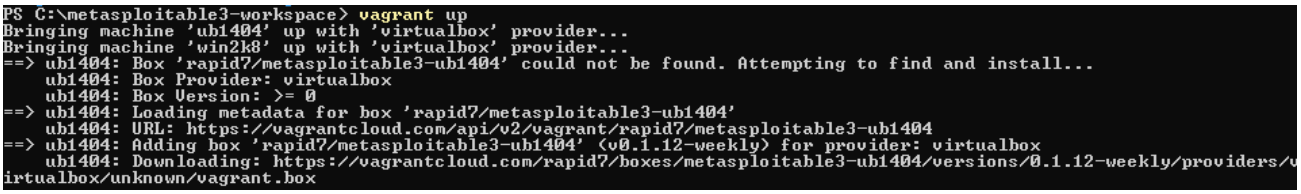


Ilustración 3Instalación de los paquetes

Creación automáticamente

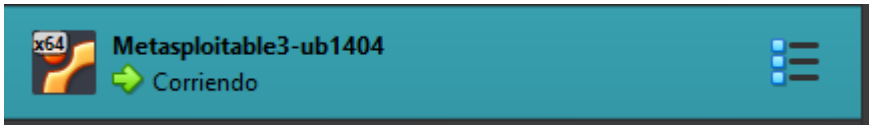


Ilustración 4 creación de las maquinas

Aquí lo que podemos observar es como automáticamente metasploitable3 de va creado por medio de la power Shell

Imágenes de las maquinas corriendo al 100%

1) metasploitable3-workspace_win2k8_1756799443609_27877

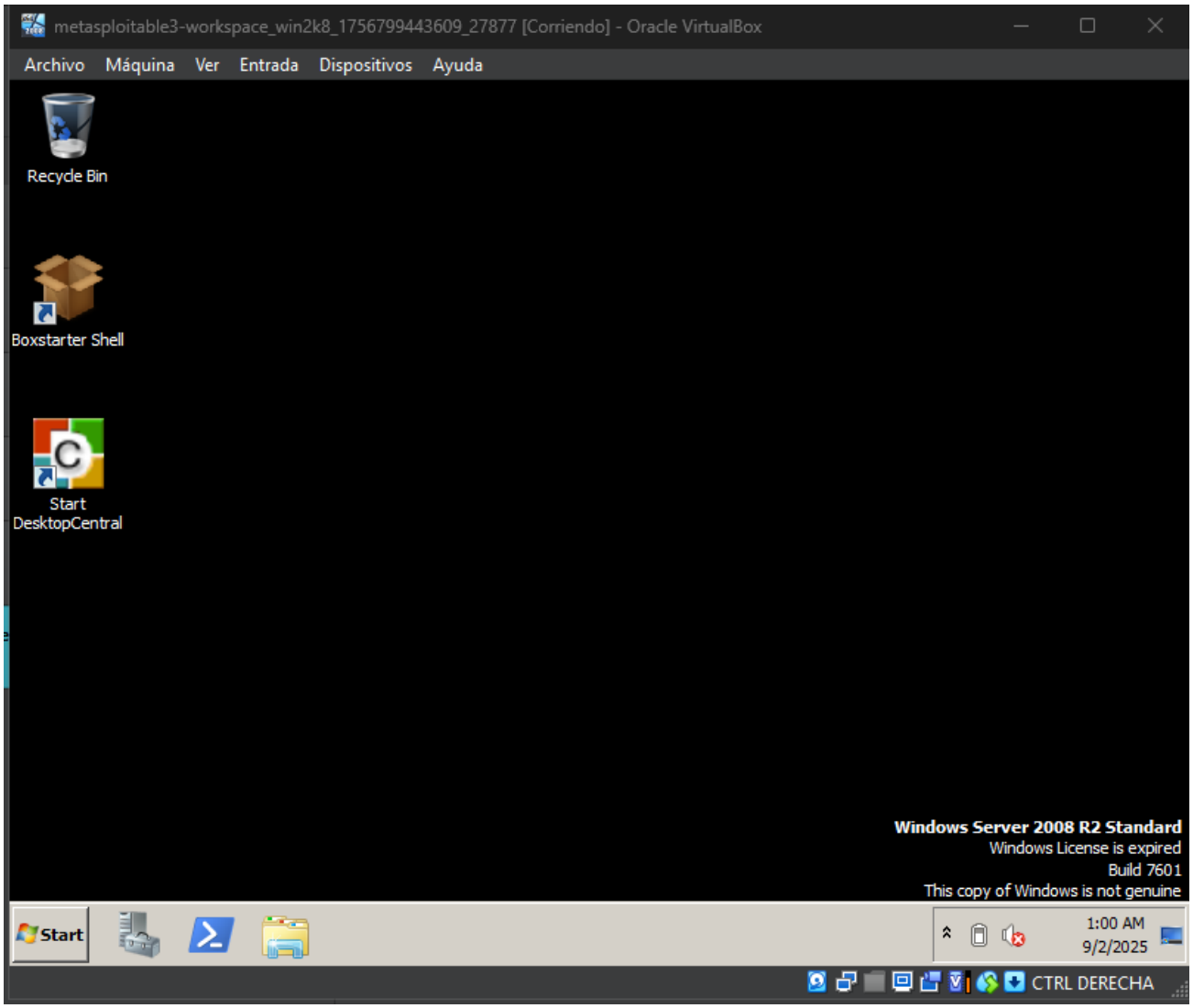


Ilustración 5 metasploitable3-workspace_win2k8_1756799443609_27877

2) Metasploitable3-ub1404

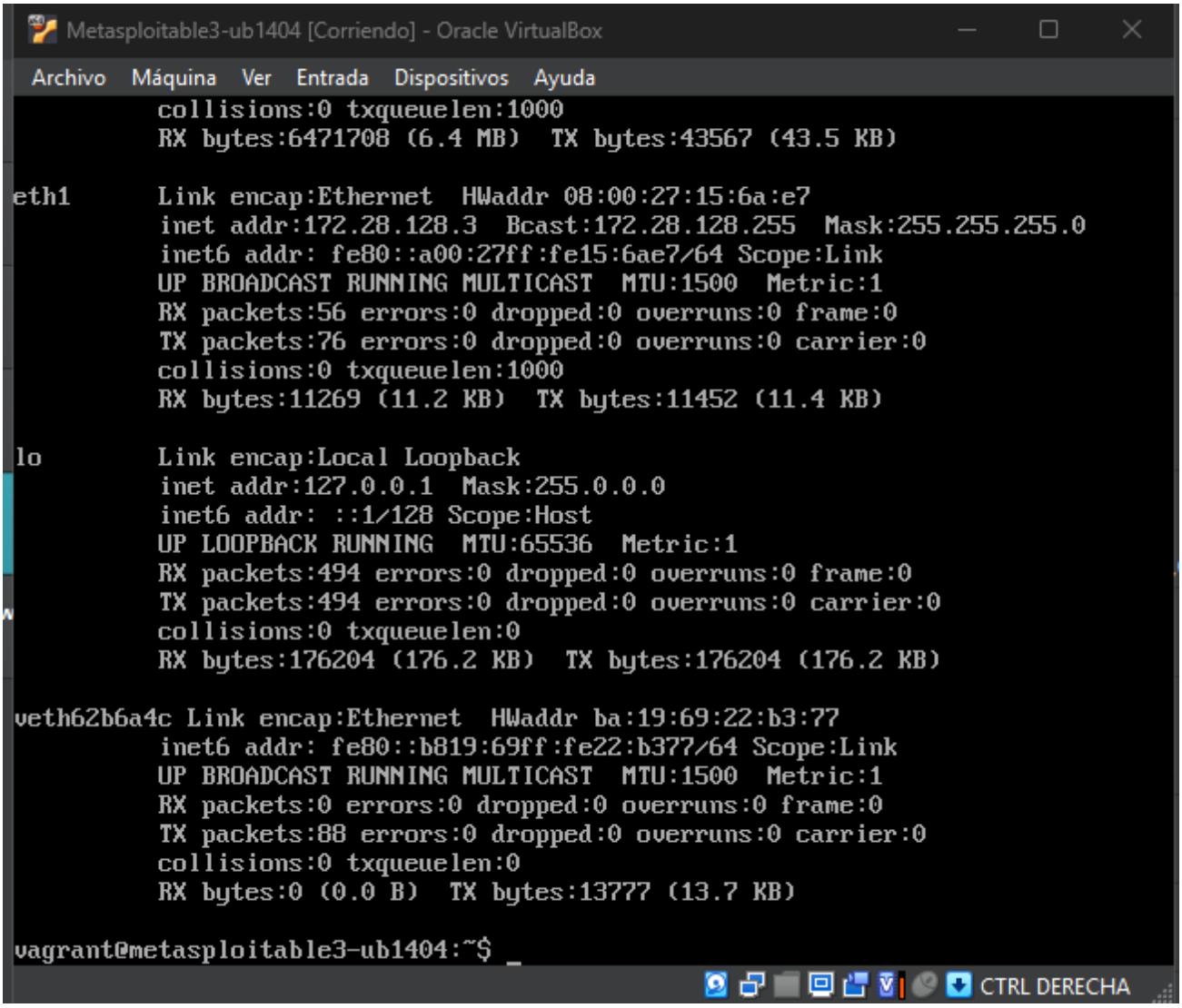


Ilustración 6 Metasploitable3-ub1404

Conclusiones

La instalación de Metasploitable3 en Windows requiere una preparación cuidadosa del entorno y ajustes técnicos precisos. A pesar de los errores iniciales, se logró identificar y corregir los conflictos de versión y rutas, permitiendo avanzar con éxito en la construcción de la máquina virtual

Bibliografía

Morcor

Webgrafía

Metasploitable3 GitHub - rapid7/metasploitable3: Metasploitable3 is a VM that is built from the ground up with a large amount of security vulnerabilities.

Ia.

https://chatgpt.com/