INFORME1 – LABORATORIO DE PENTESTING CON KALI LINUX Y METASPLOITABLE 2

Johely Cordoba Valoyes

Estudiante de Ingeniería en Telecomunicaciones e informática

Universidad Tecnológica de Chocó Diego Luis Cordoba

7 – 08 - 2025

INFORME 1 – LABORATORIO DE PENTESTING CON KALI LINUX Y METASPLOITABLE 2

Johely Cordoba Valoyes

Estudiante de Ingeniería en Telecomunicaciones e Informática

Seguridad y auditoría de redes

Prof. Rafael Sandoval Morales

Universidad Tecnológica de Chocó Diego Luis Córdoba

7 – 08 - 2025

Tabla de contenido

TABLA DE ILUSTRACIONES

INTRODUCCIÓN

El presente informe describe la implementación de un laboratorio de ciberseguridad utilizando como entorno de virtualización VirtualBox 7.0, donde se configuraron dos máquinas virtuales: Kali Linux como sistema atacante y Metasploitable 2 como sistema víctima. El objetivo de esta práctica fue establecer una red virtual segura que permitiera la comunicación entre ambas máquinas, realizar un escaneo de puertos y detectar servicios vulnerables para posteriormente explotarlos en un entorno controlado.

Durante el desarrollo de la práctica se configuró una red en VirtualBox: un adaptador en modo NAT para permitir el acceso a Internet. Posteriormente, se procedió a la instalación y uso de la herramienta Nmap para el descubrimiento de puertos y servicios, y a la utilización de Metasploit Framework y otras técnicas para la explotación de vulnerabilidades presentes en Metasploitable 2.

Esta práctica permite comprender y aplicar conceptos fundamentales de redes, seguridad informática y hacking ético, reforzando el uso de herramientas de auditoría y simulando un escenario real de ataque, siempre dentro de un entorno controlado y con fines académicos.

ALCANCE

El alcance de este laboratorio abarca desde la creación y configuración inicial de las máquinas virtuales hasta la explotación de vulnerabilidades detectadas. Incluye la configuración de adaptadores de red en VirtualBox, la verificación de conectividad entre las máquinas, la ejecución de escaneos de puertos con Nmap, el análisis de los servicios expuestos y la explotación de puertos específicos.

Los puertos explotados durante la práctica fueron los siguientes: 23, 25, 53, 139 y 445, 2121, 3306 y 5432. Cada uno de estos servicios se probó para evidenciar vulnerabilidades como credenciales por defecto, configuraciones inseguras y falta de cifrado.

OBJETIVOS GENERALES

Implementar y documentar un laboratorio de pruebas de penetración utilizando VirtualBox 7.0, Kali Linux y Metasploitable 2, para identificar y explotar vulnerabilidades en un entorno virtual seguro y controlado.

OBJETIVOS ESPECÍFICOS

- Configurar dos máquinas virtuales con sistemas operativos Kali Linux y Metasploitable 2 dentro de VirtualBox 7.0.

- Establecer un esquema de red NAT.

- Realizar un escaneo de puertos con Nmap para detectar servicios activos y versiones.

- Analizar los resultados del escaneo para identificar posibles vulnerabilidades.

- Explotar de forma controlada los servicios vulnerables detectados.

INFORME 1 – LABORATORIO DE PENTESTING CON KALI LINUX Y METASPLOITABLE 2

Para iniciar la práctica, se procedió a crear las dos máquinas virtuales dentro de **VirtualBox 7.0**. La primera máquina, con sistema **Kali Linux**, la segunda máquina, **Metasploitable 2**, se importó a partir de su archivo `.vmdk` official.

En la configuración de red de ambas máquinas, se habilitó un adaptador en modo NAT.

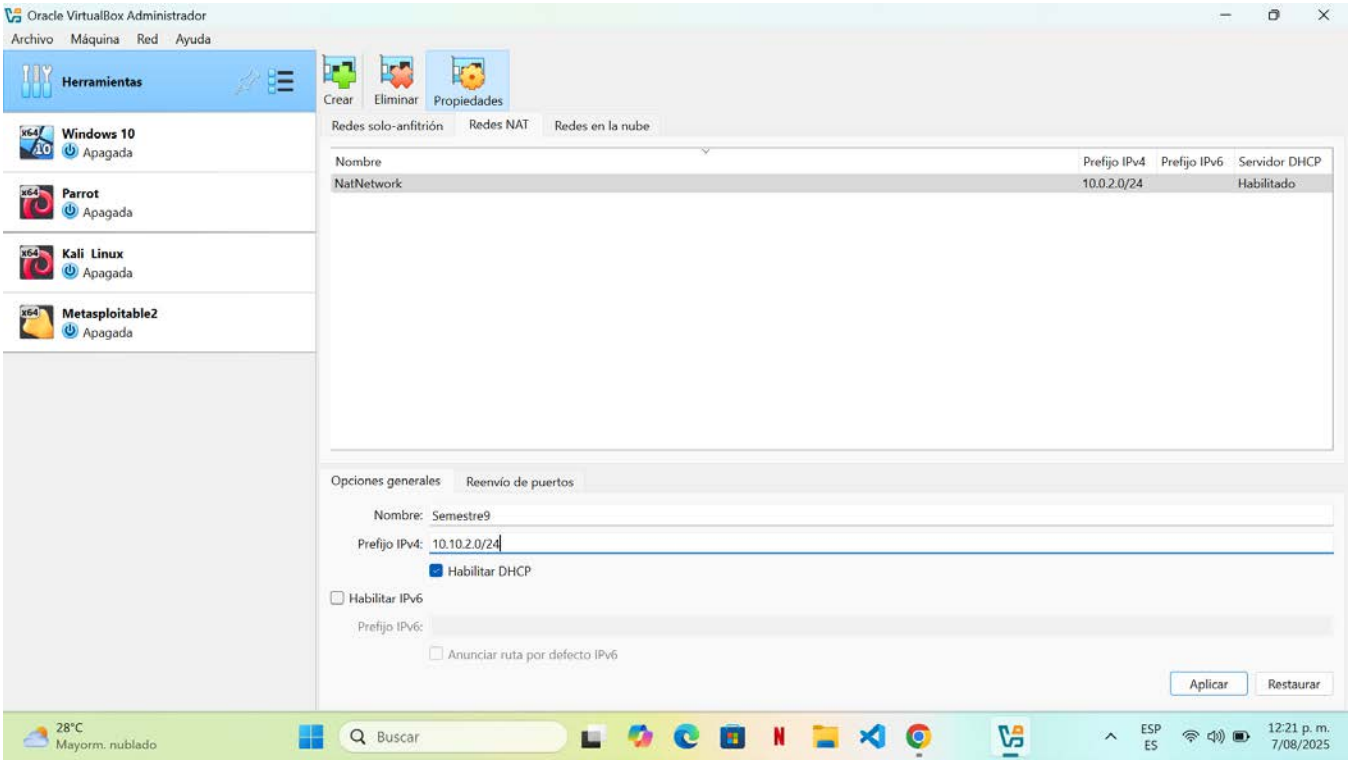

Ilustración 1: Configuración red NAT

Esta configuración se realizó desde la ventana de ajustes de cada máquina en VirtualBox, en la sección “Red”, activando la opción “Habilitar adaptador de red” y seleccionando “Conectado a: Red NAT”. El modo NAT permitió que ambas máquinas virtuales se comunicaran entre sí.

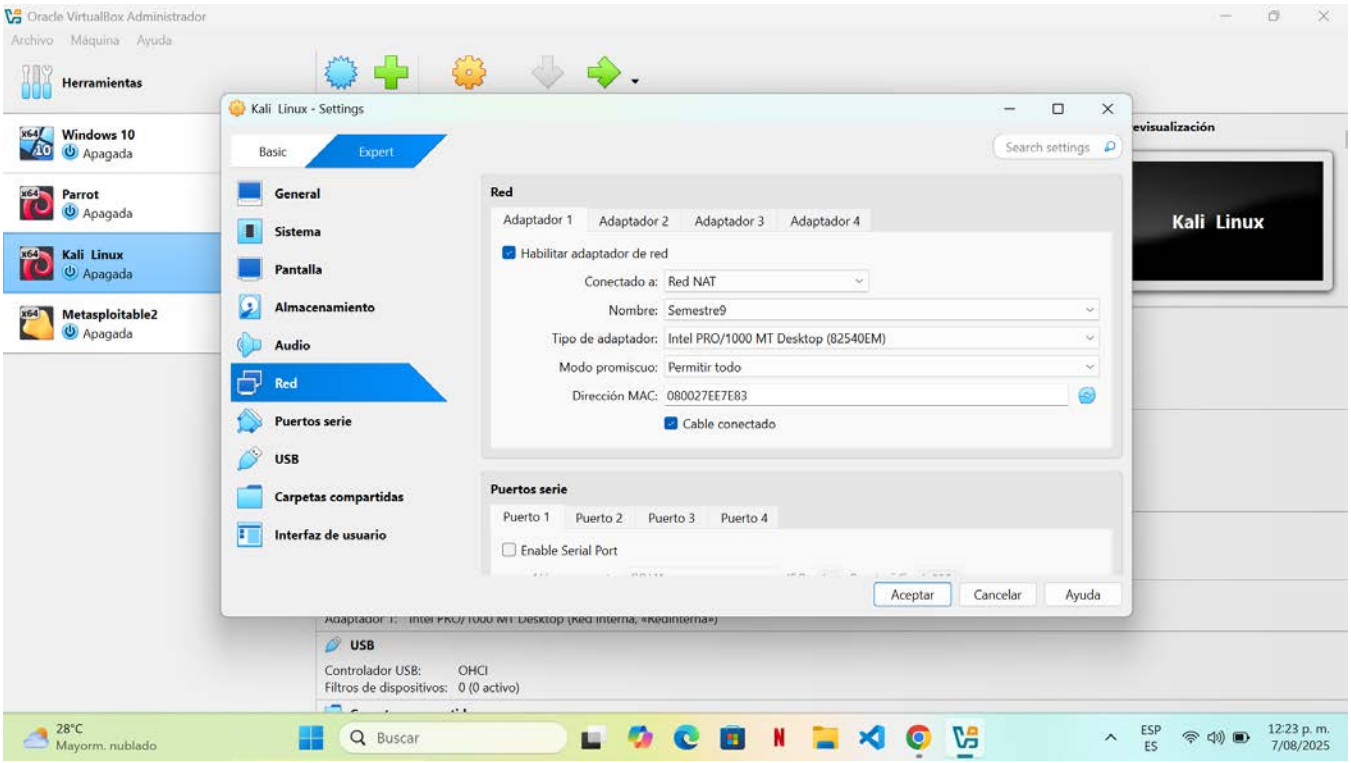

Ilustración 2 Configuración red NAT en Kali Linux

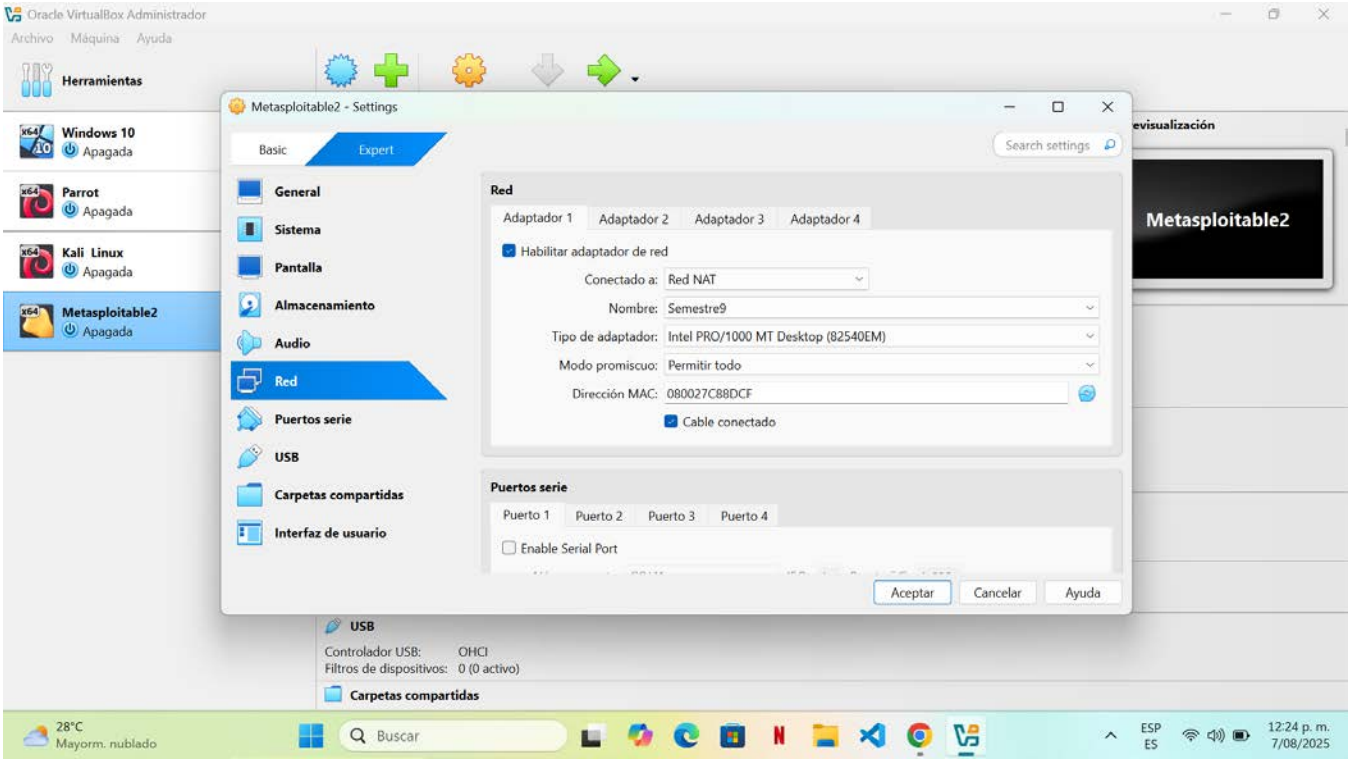

Ilustración 3 Configuración red NAT en Metasploitable2

Una vez configurada la red, se iniciaron las máquinas virtuales y se procedió a verificar las direcciones IP asignadas automáticamente por la red NAT semestre9. Después de identificar las direcciones IP de ambas máquinas, se comprobó la conectividad mediante el comando ping desde Kali hacia la IP de Metasploitable 2. La respuesta exitosa confirmó que la configuración NAT estaba funcionando correctamente y que ambas máquinas podían comunicarse entre sí.

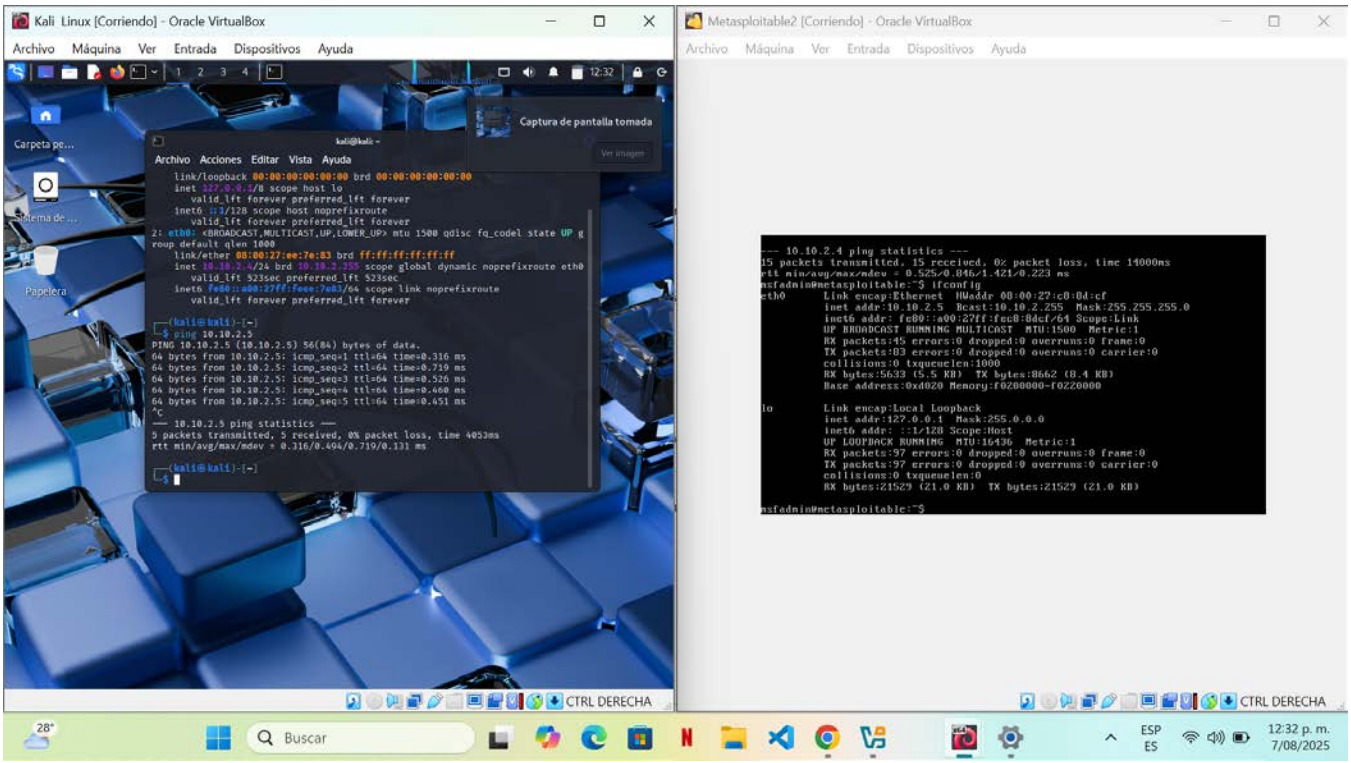

Ilustración 4 Verificación de conexión de red

En primera instancia, se ejecutó Nmap de forma básica, introduciendo únicamente la dirección IP de Metasploitable 2. Este escaneo inicial permitió obtener una lista de los puertos abiertos en la máquina víctima, mostrando el estado de cada uno y su número de puerto.

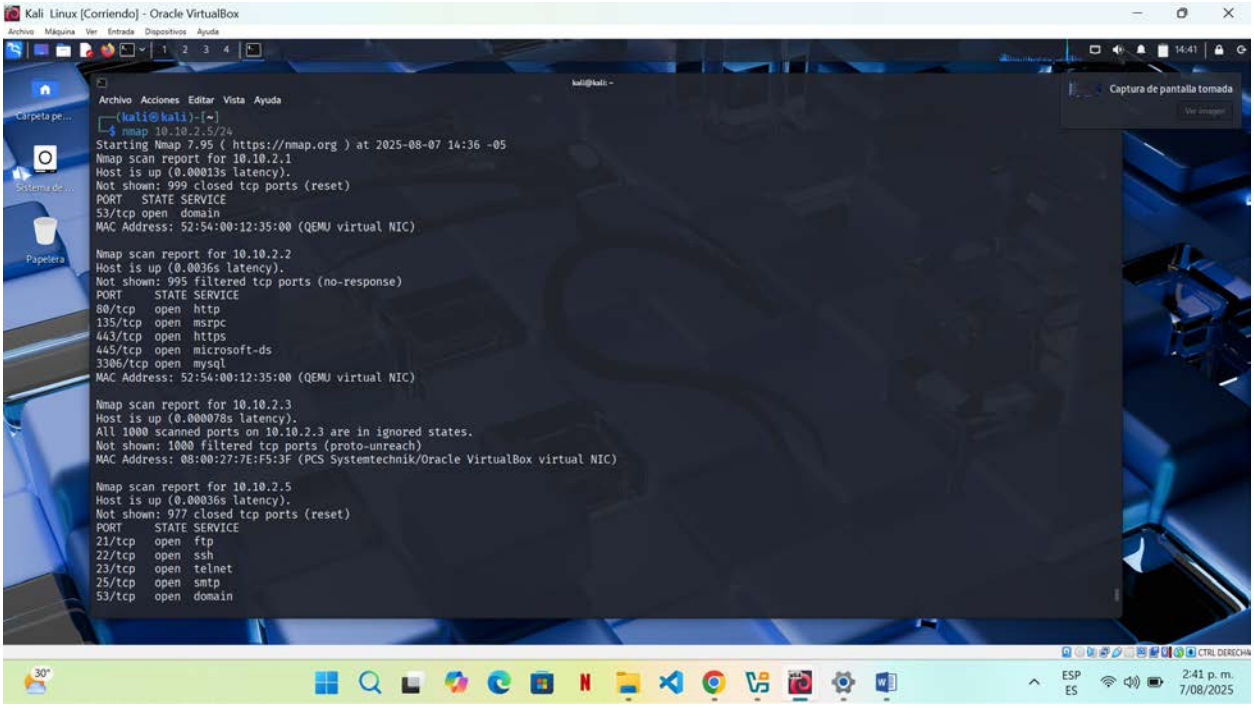

Ilustración 5 Lista de puertos abiertos

Ilustración 6 Lista de puertos abiertos

Posteriormente, para obtener información más detallada, se empleó el parámetro -sV, que ordena a Nmap identificar la versión exacta de los servicios que están activos en cada puerto.

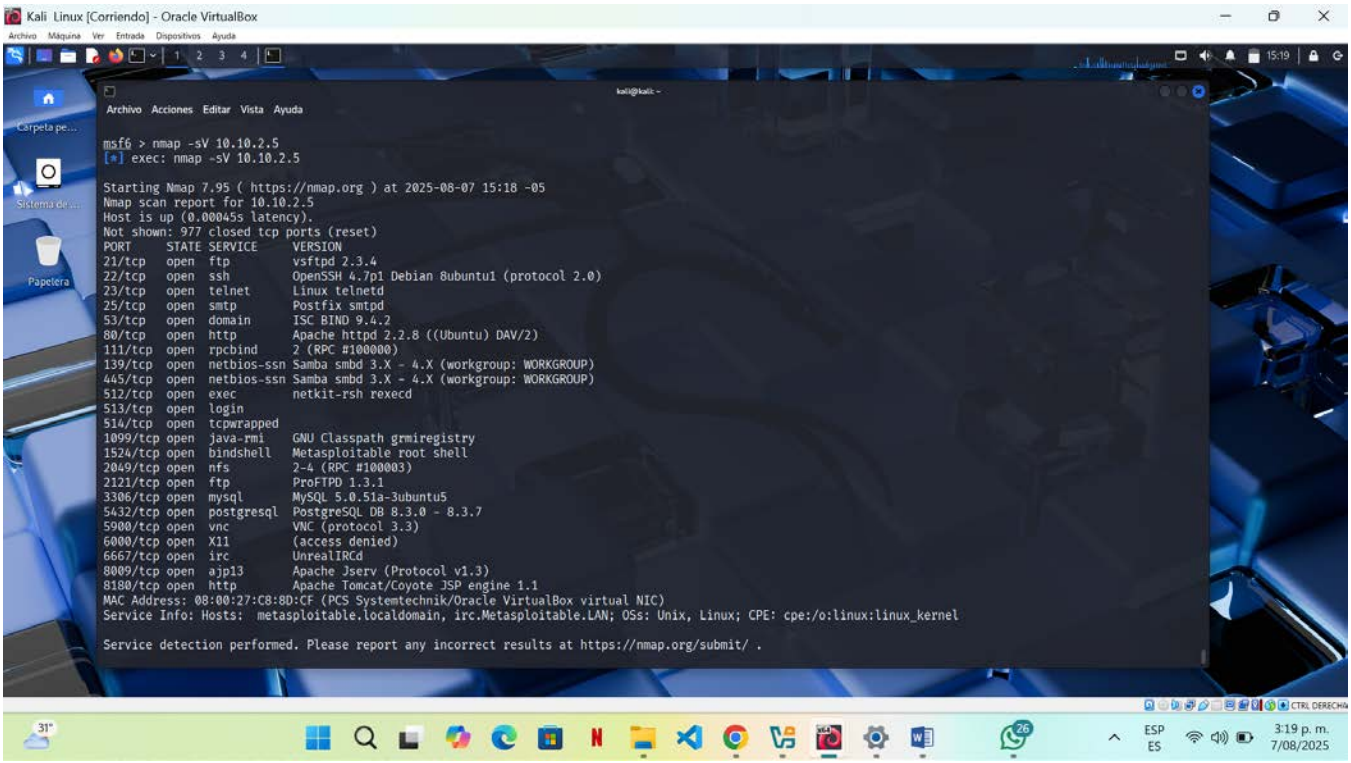

Ilustración 7 Lista de puertos abiertos con versions exactas

Cada vez que se procedió a explorar o explotar un puerto detectado como vulnerable, se utilizó la herramienta Metasploit Framework, que en Kali Linux se inicia con el comando: msfconsole. Este permite buscar exploits específicos mediante el comando search, seleccionar el módulo adecuado con use, y luego configurar los parámetros necesarios como la dirección IP del objetivo (set RHOST) y el puerto correspondiente (set RPORT). De esta manera, para cada servicio identificado en el escaneo con Nmap, se inició msfconsole, se cargó el módulo más

apropiado y se ejecutó el exploit, obteniendo así acceso o información del servicio en cuestión.

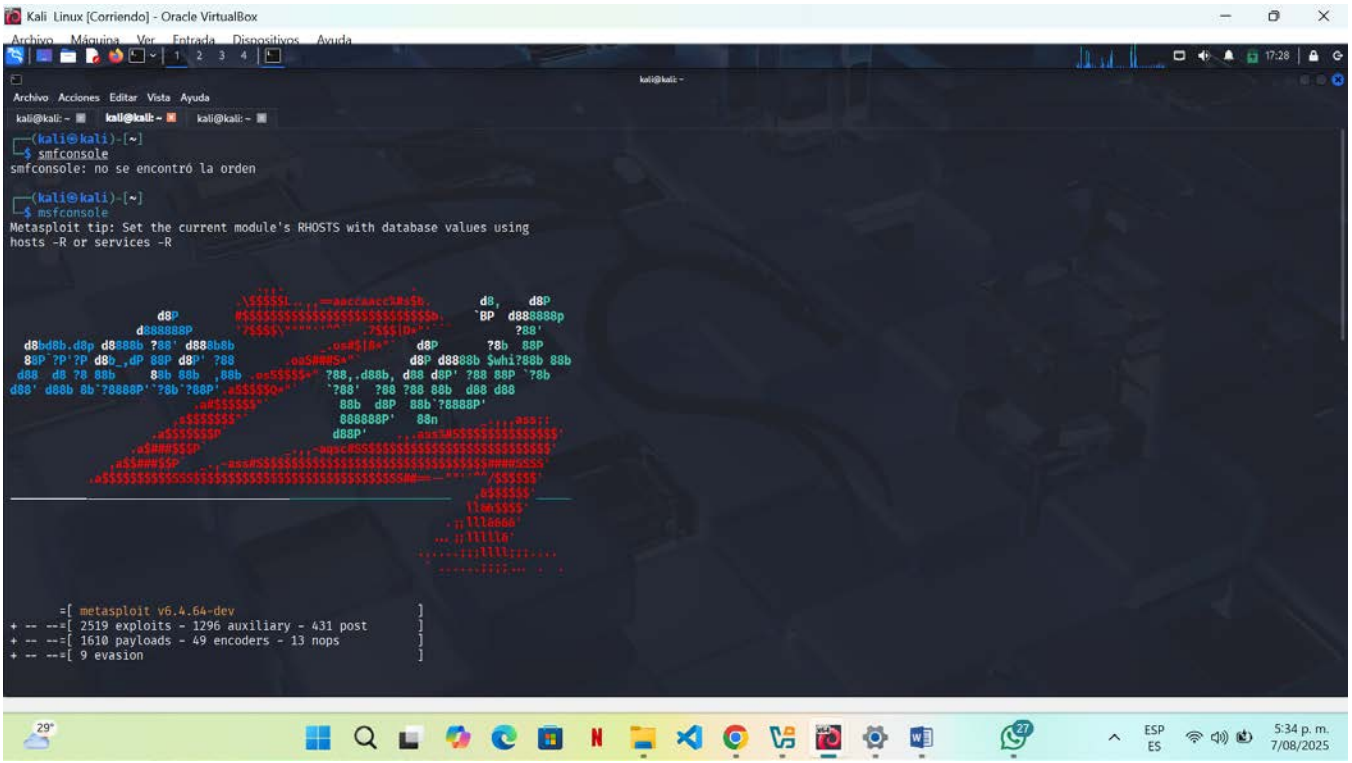

Ilustración 8 msfconsole

PUERTO 23 – TELNET

El puerto 23 corresponde al servicio Telnet, un protocolo de acceso remoto que permite administrar un sistema a través de línea de comandos. Su principal vulnerabilidad radica en que transmite la información, incluidas las credenciales de usuario y contraseña, en texto plano, sin cifrado. En esta práctica, Telnet permitió el acceso remoto a Metasploitable 2 utilizando credenciales por defecto (msfadmin/msfadmin), lo que facilitó el control total del sistema

víctima desde Kali Linux.

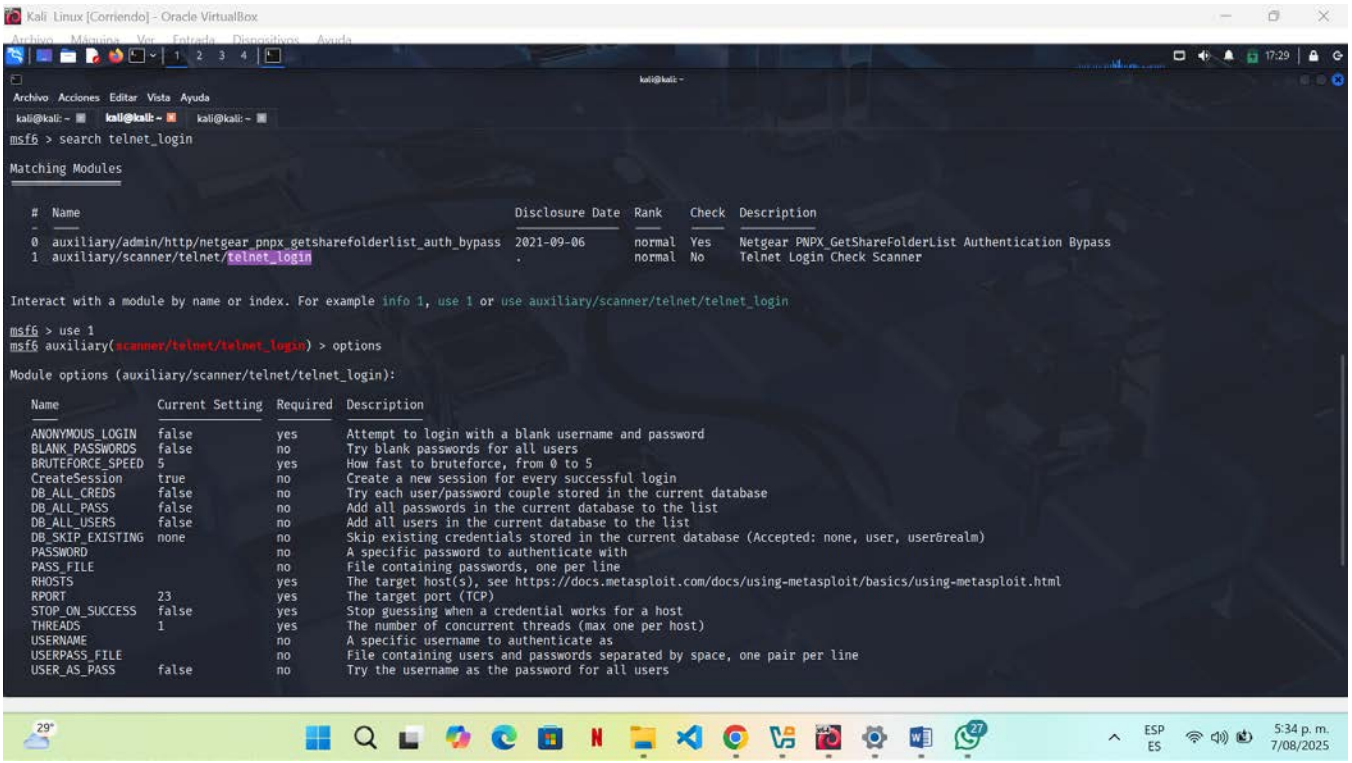

Ilustración 9 PUERTO 23 – TELNET

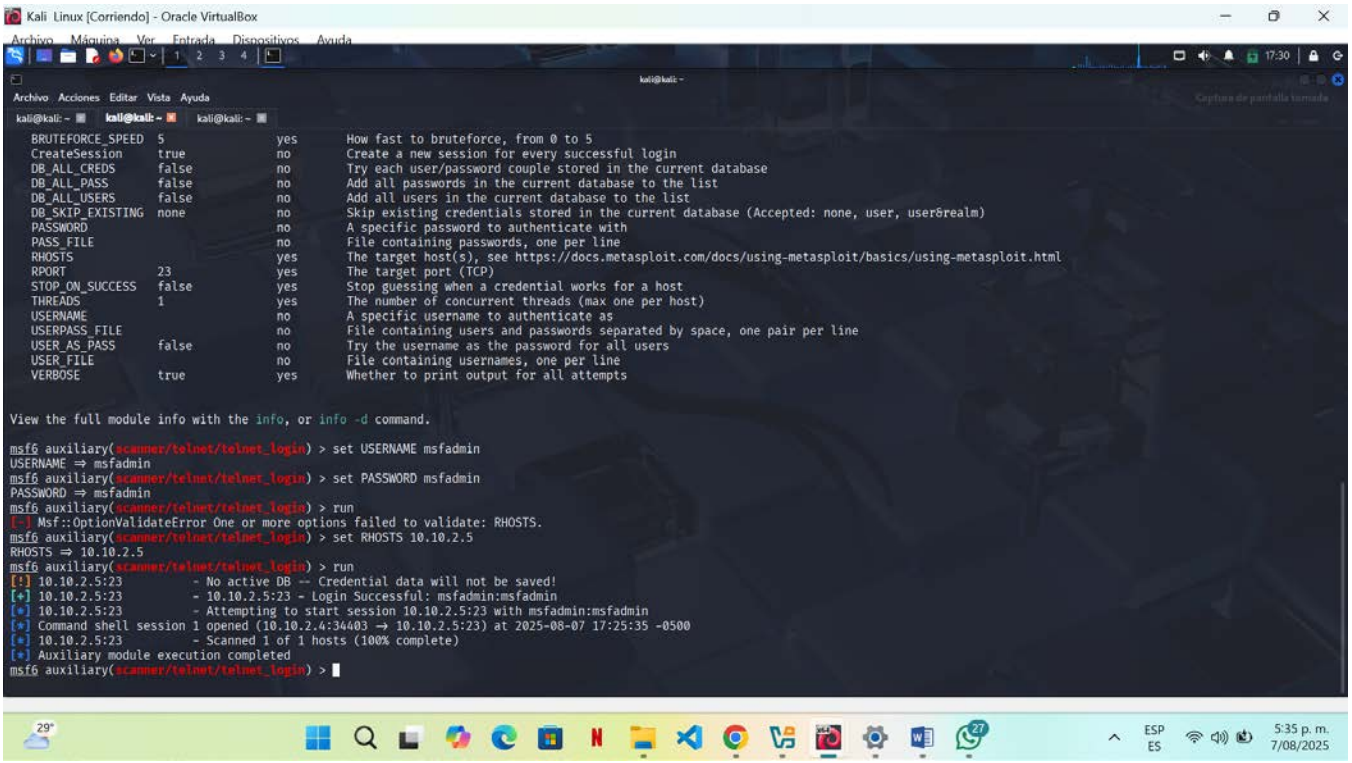

Ilustración 10 PUERTO 23 – TELNET

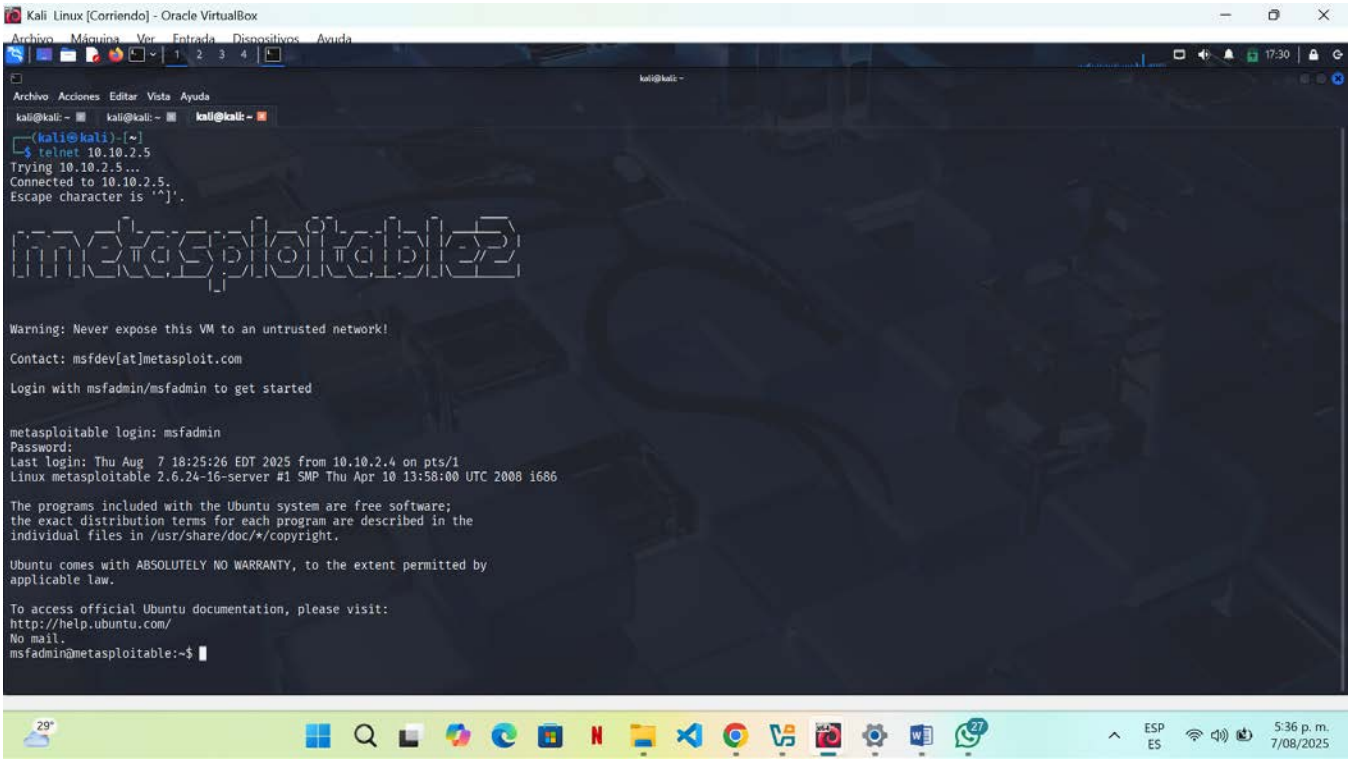

Ilustración 11 PUERTO 23 – TELNET

PUERTO 25 – SMTP

El puerto 25 está asociado al protocolo Simple Mail Transfer Protocol (SMTP), utilizado para el envío de correos electrónicos. Una configuración insegura de este servicio puede permitir ataques de enumeración de usuarios

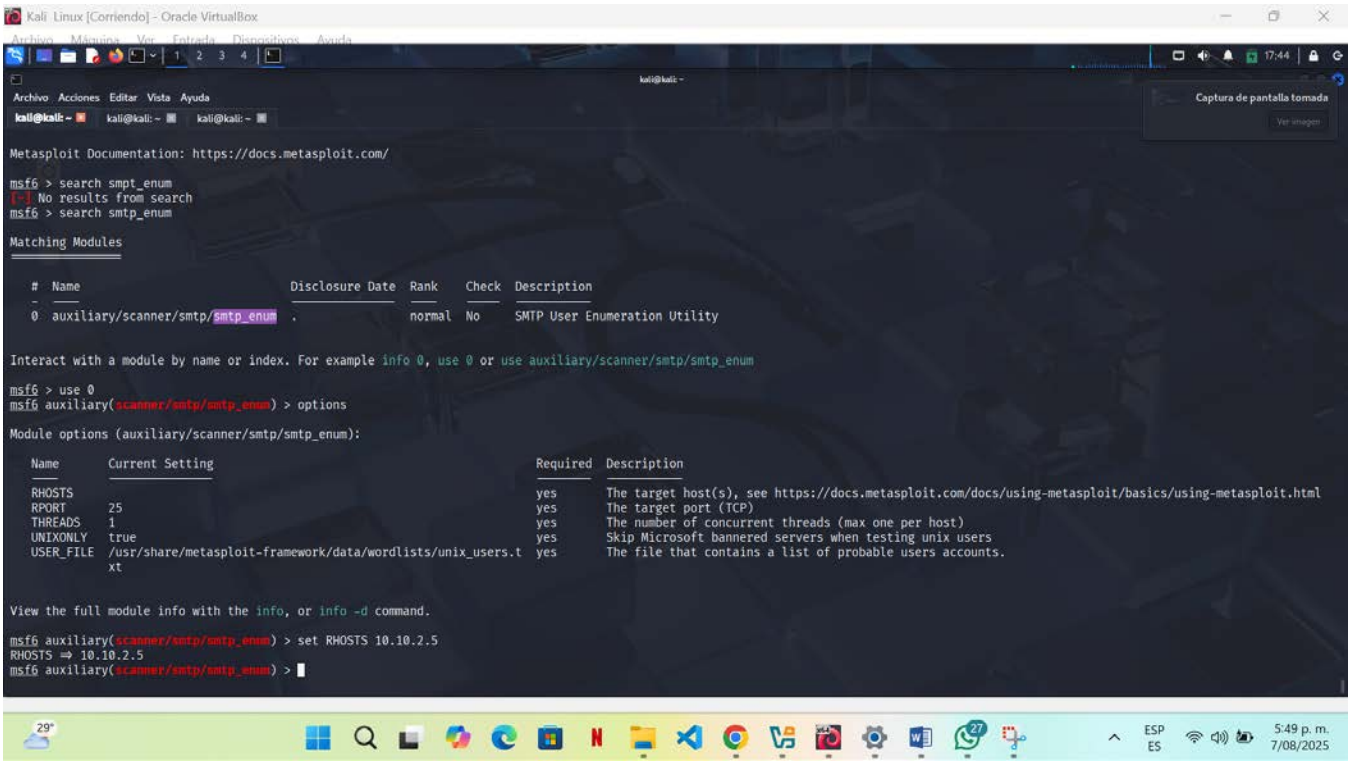

Ilustración 12 PUERTO 25 – SMTP

PUERTO 53: DNS

El puerto 53 corresponde al servicio Domain Name System (DNS), encargado de la resolución de nombres de dominio en direcciones IP. Una configuración incorrecta puede permitir realizar transferencias de zona (zone transfer), revelando información interna como nombres de host y estructura de red. En esta práctica, se logró ejecutar una transferencia de zona

desde Kali Linux, exponiendo datos que en un entorno real serían de gran valor para un atacante.

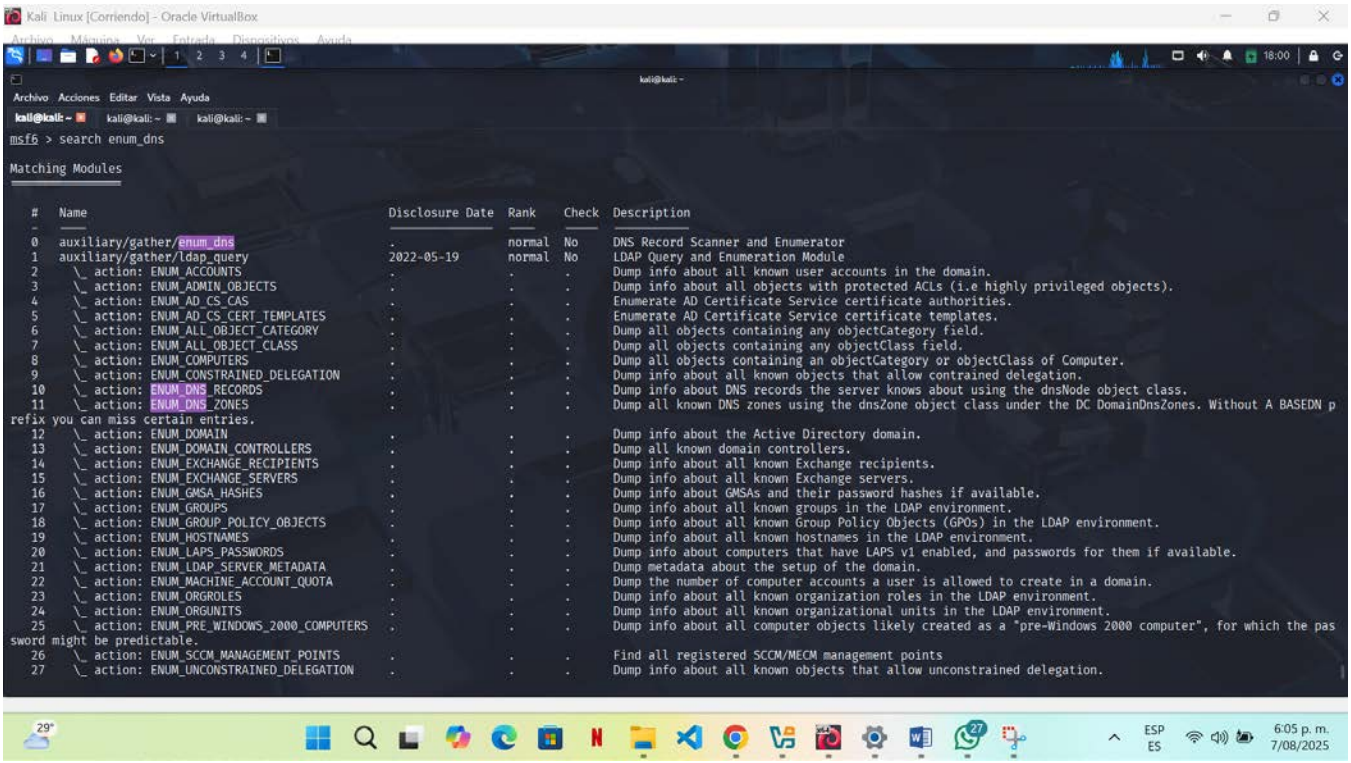

Ilustración 13 PUERTO 53: DNS

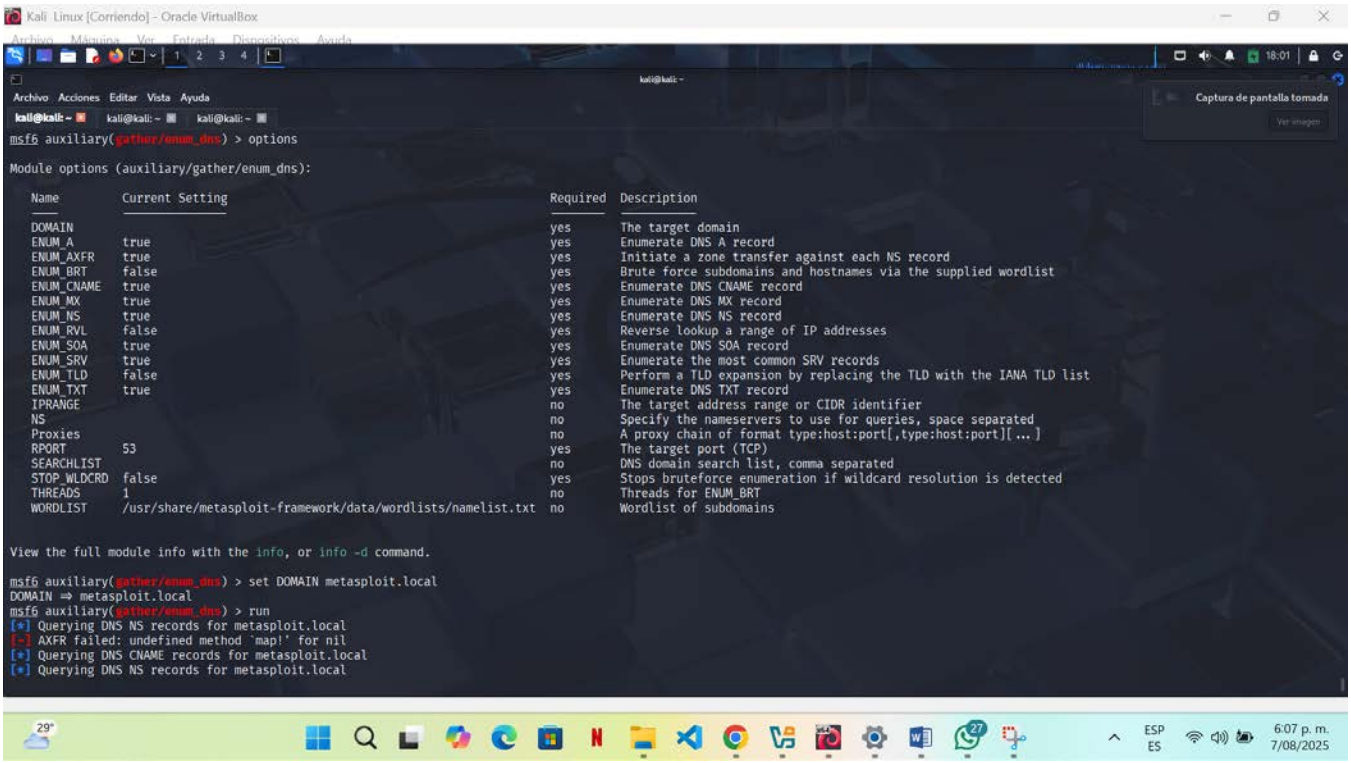

Ilustración 14 PUERTO 53: DNS

PUERTO 139: NETBIOS SESSION SERVICE

El puerto 139 pertenece al servicio NetBIOS sobre TCP/IP, utilizado para compartir archivos e impresoras en redes Windows. Este servicio es conocido por permitir la enumeración de recursos compartidos, usuarios y grupos, especialmente si no está protegido por autenticación robusta. Durante la práctica, se pudo listar información sensible de Metasploitable 2 que podría ser utilizada para escalar privilegios.

PUERTO 445: MICROSOFT-DS (SMB)

El puerto 445 está relacionado con el protocolo Server Message Block (SMB), que permite el intercambio de archivos y recursos en redes Windows.

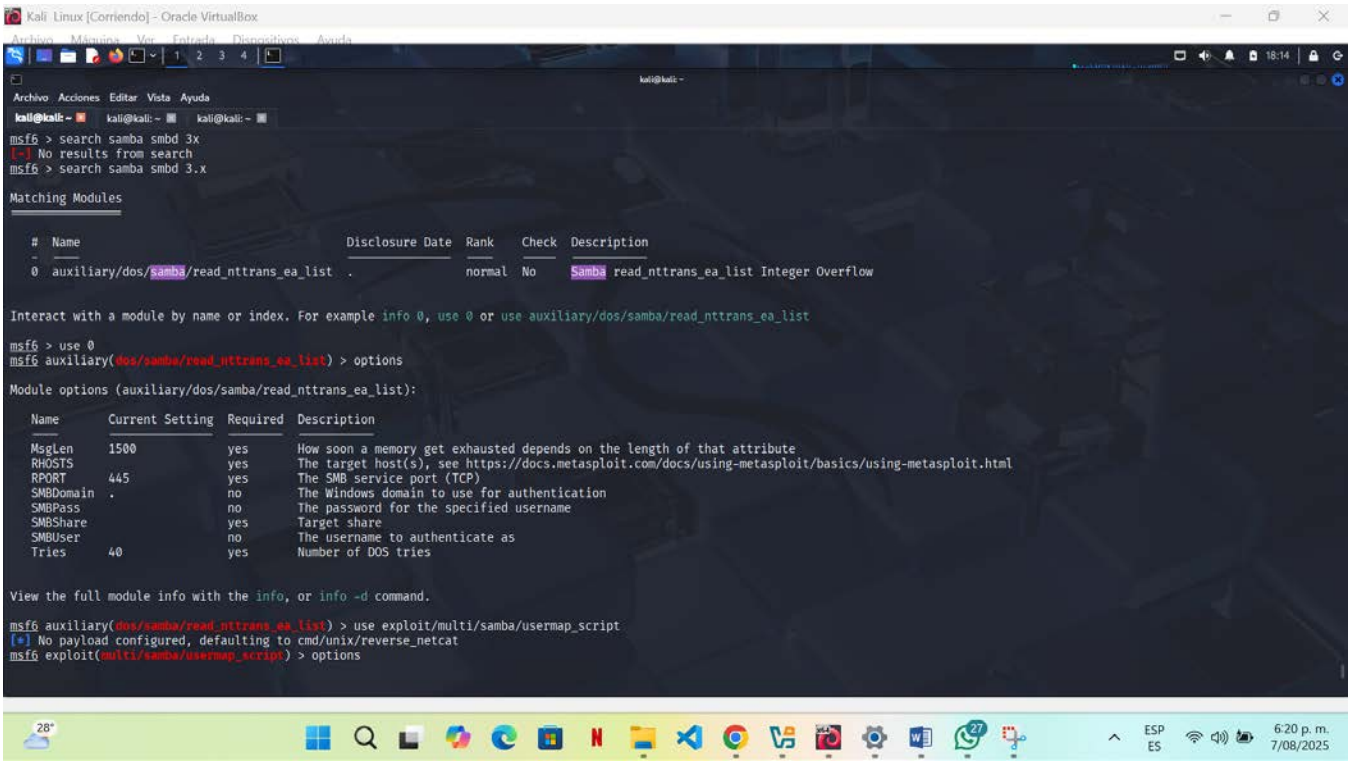

Ilustración 15 puertos 139,145

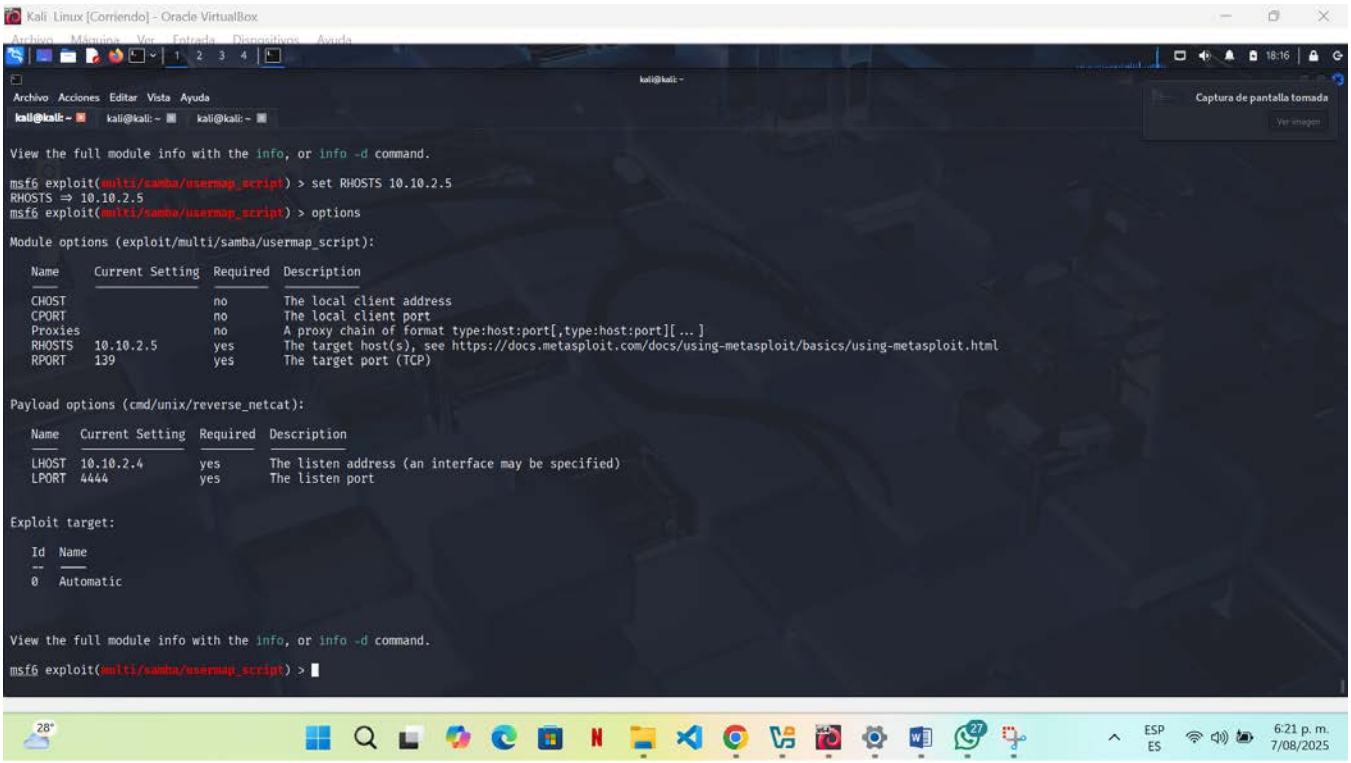

Ilustración 16 puertos 139, 145

PUERTO 2121: FTP ALTERNATIVO

El puerto 2121 corresponde a un servicio FTP configurado en un puerto no estándar. Aunque el cambio de puerto puede confundir a usuarios poco experimentados, no proporciona seguridad real. En la práctica, este servicio aceptó conexiones anónimas sin autenticación, lo que permitió la subida y descarga de archivos libremente, representando un riesgo grave de fuga o

manipulación de información.

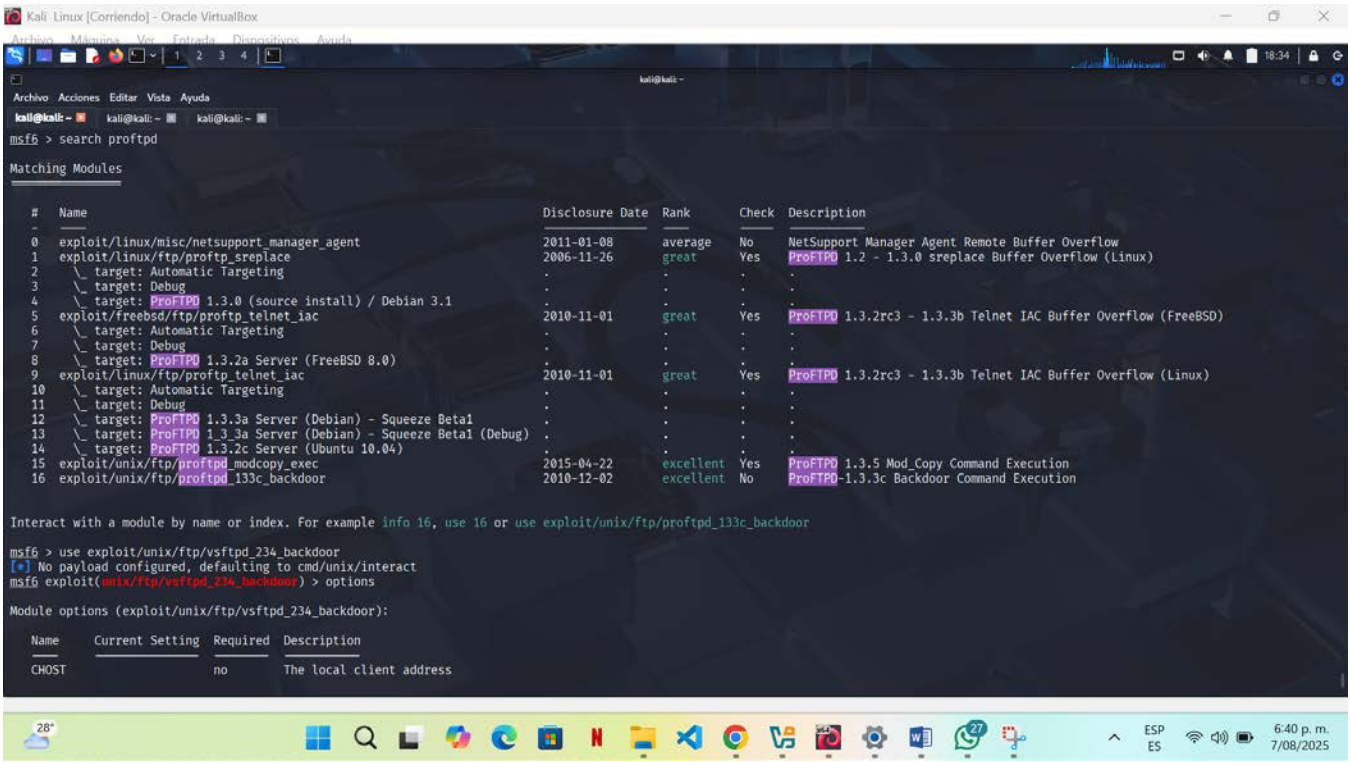

Ilustración 17 PUERTO 2121: FTP ALTERNATIVO

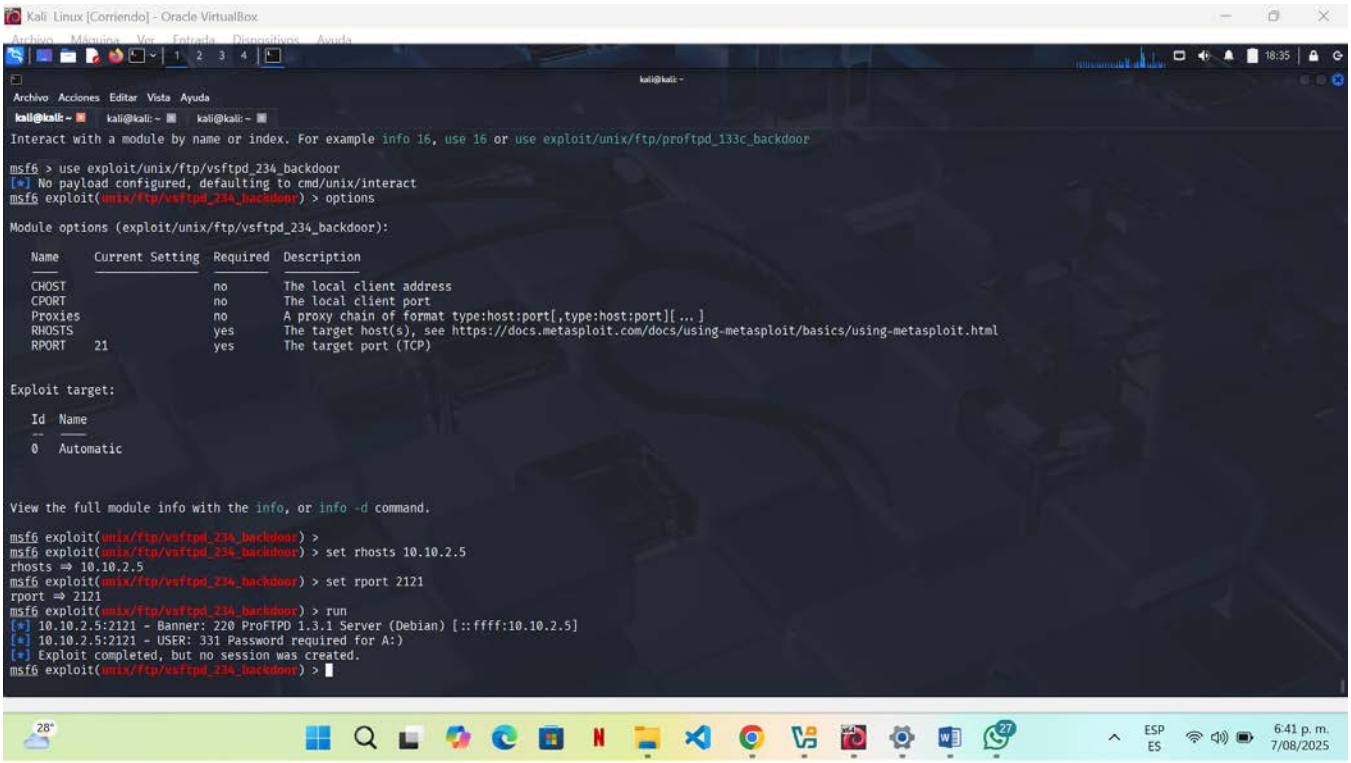

Ilustración 18 PUERTO 2121: FTP ALTERNATIVO

PUERTO 3306: MYSQL

El puerto 3306 es utilizado por el sistema de gestión de bases de datos MySQL. Configuraciones por defecto, como credenciales vacías o de fácil adivinación, representan un riesgo considerable. Durante la práctica, MySQL permitió el acceso con el usuario root sin contraseña, lo que permitió visualizar y extraer bases de datos completas desde Kali Linux, comprometiendo la integridad y confidencialidad de la información.

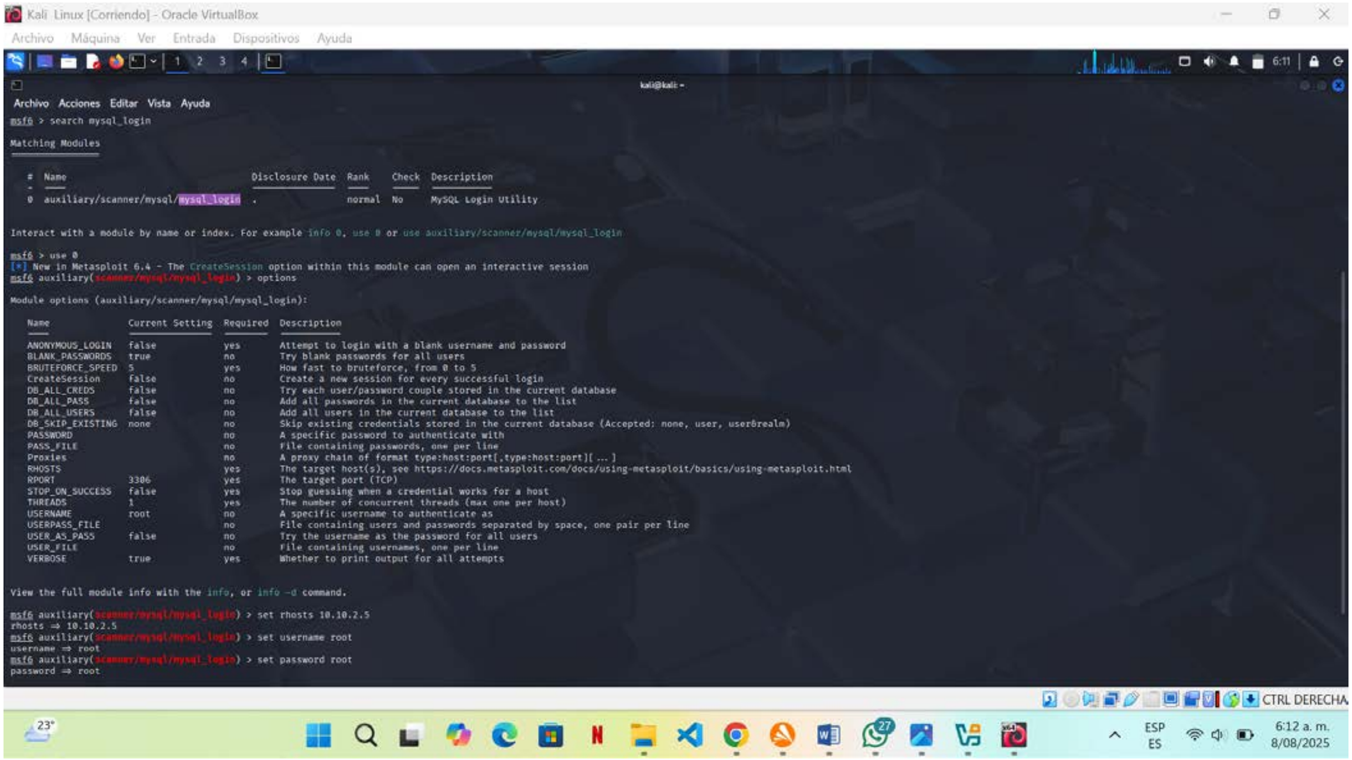

Ilustración 19 PUERTO 3306: MYSQL

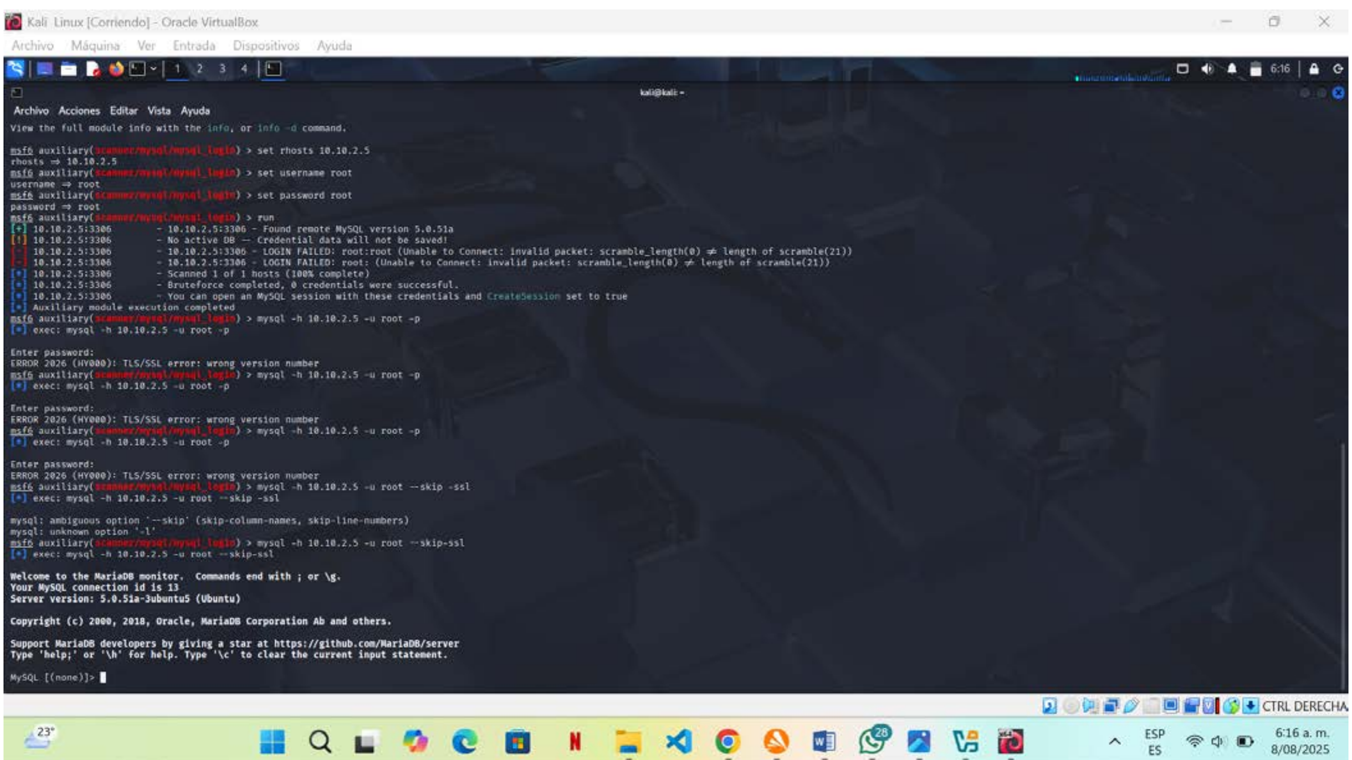

Ilustración 20 PUERTO 3306: MYSQL

PUERTO 5432: POSTGRESQL

El puerto 5432 corresponde a la base de datos PostgreSQL, otro sistema de gestión de bases de datos ampliamente utilizado. Al igual que MySQL, una configuración débil en este servicio puede permitir el acceso no autorizado. En esta práctica, el servicio aceptó credenciales por defecto, permitiendo acceder a todas las bases de datos y ejecutar consultas sin restricción, lo que demuestra una vulnerabilidad crítica en su seguridad.

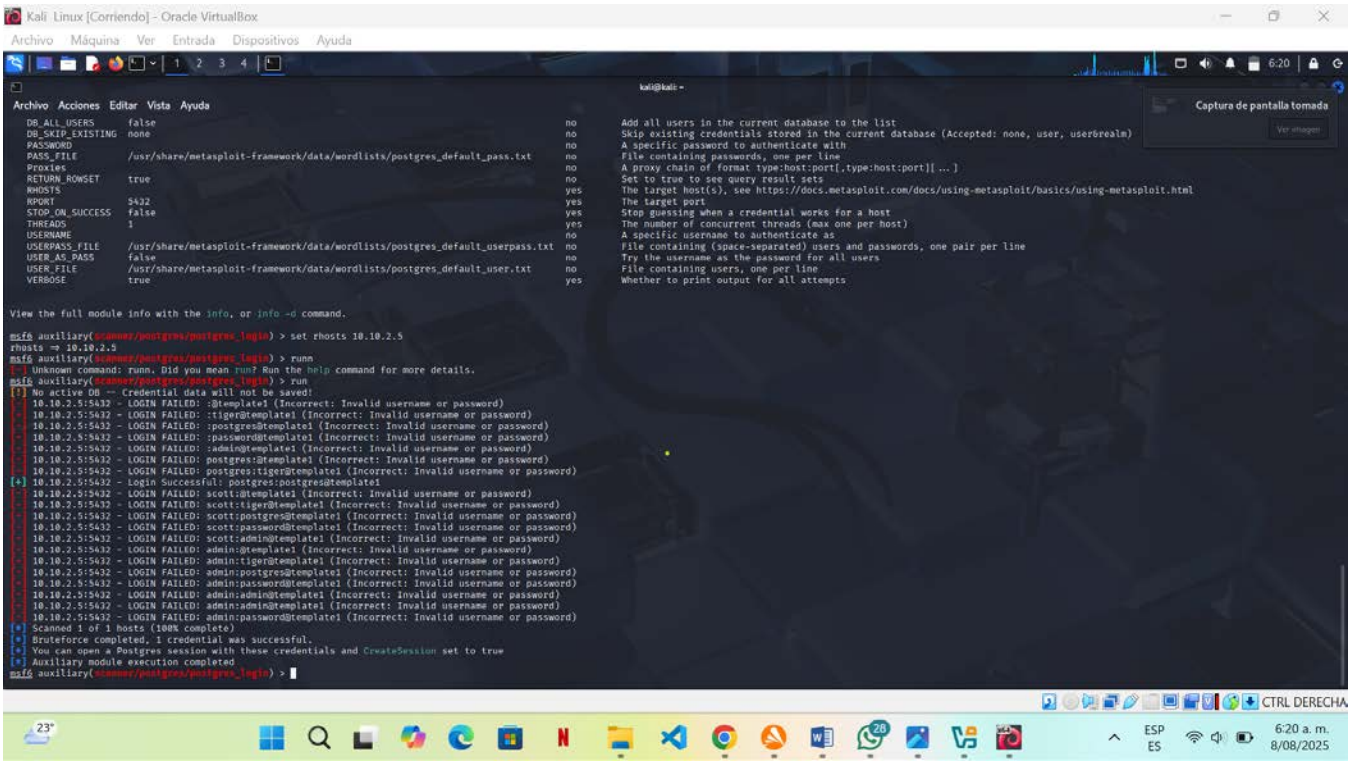

Ilustración 21 PUERTO 5432: POSTGRESQL

GLOSARIO

- Pentesting: también conocido como prueba de penetración, es un proceso de seguridad que simula ataques cibernéticos para identificar vulnerabilidades en sistemas, redes o aplicaciones.

- VirtualBox: Software de virtualización que permite crear y ejecutar máquinas virtuales dentro de un sistema anfitrión, simulando hardware para instalar y utilizar diferentes sistemas operativos.

- NAT (Network Address Translation): Modo de red en máquinas virtuales que traduce las direcciones IP internas a la IP del anfitrión, permitiendo el acceso a Internet sin exponer directamente la VM a la red física.

- Kali Linux: Distribución de Linux especializada en pruebas de penetración y auditorías de seguridad, que incluye una gran cantidad de herramientas para análisis de redes y explotación de vulnerabilidades.

- Metasploitable 2: Máquina virtual intencionalmente vulnerable diseñada para prácticas y aprendizaje de ciberseguridad.

- Nmap: Herramienta de código abierto para el descubrimiento y escaneo de redes, utilizada para identificar hosts, puertos abiertos y servicios activos.

- nmap -sV: Comando de Nmap que, además de detectar puertos abiertos, identifica la versión exacta de los servicios que están activos.

- Telnet: Protocolo de comunicación que permite acceso remoto a un dispositivo mediante línea de comandos, transmitiendo la información sin cifrar.

- SMTP: Protocolo estándar para el envío de correos electrónicos en redes IP.

- DNS: Servicio que traduce nombres de dominio en direcciones IP y viceversa.

- NetBIOS/SMB: Protocolos utilizados para compartir archivos, impresoras y recursos en redes locales, especialmente en entornos Windows.

- FTP: Protocolo de transferencia de archivos entre dispositivos en una red.

- MySQL: Sistema de gestión de bases de datos relacional muy utilizado en aplicaciones web.

- PostgreSQL: Sistema de gestión de bases de datos relacional, reconocido por su estabilidad y funciones avanzadas.

CONCLUSIONES

La realización de esta práctica me permitió comprender de forma más clara cómo se puede estructurar un laboratorio de ciberseguridad utilizando herramientas de virtualización y redes. Pude configurar correctamente la red NAT personalizada semestre9 en VirtualBox, lo que me dio la posibilidad de comunicar Kali Linux con Metasploitable 2 y, al mismo tiempo, mantener el acceso a Internet para instalar y actualizar las herramientas necesarias.

La utilización de Nmap fue una parte clave del proceso, ya que me permitió primero detectar qué puertos estaban abiertos y luego, con la opción -sV, identificar con precisión qué servicios y versiones se encontraban activos. Esta información fue fundamental para decidir qué servicios eran vulnerables y cómo explotarlos.

Durante el análisis encontré varios puertos con configuraciones inseguras o credenciales por defecto, lo que demuestra la importancia de mantener buenas prácticas de seguridad, como deshabilitar servicios innecesarios y reforzar las credenciales de acceso. El ejercicio me ayudó a reforzar mis conocimientos sobre protocolos, vulnerabilidades comunes y la importancia de un correcto aislamiento de entornos de prueba para evitar riesgos en redes reales.

En general, considero que esta práctica fue muy útil para afianzar conceptos teóricos a través de la experiencia directa, y me permitió afinar mi manejo de herramientas fundamentales en el ámbito de la auditoría y seguridad de redes.