INFORME – PRÁCTICA DE EXPLOTACIÓN WINDOWS 2003 Y UBUNTU CON KALI LINUX Y METASPLOIT

Johely Cordoba Valoyes

Estudiante de Ingeniería en Telecomunicaciones e informática

Universidad Tecnológica de Chocó Diego Luis Cordoba

3– 09 - 2025

INFORME – PRÁCTICA DE EXPLOTACIÓN WINDOWS 2003 Y UBUNTU CON KALI LINUX Y METASPLOIT

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

La seguridad informática constituye un eje fundamental en la administración de sistemas y redes. El avance de las amenazas cibernéticas ha obligado a las organizaciones a fortalecer sus mecanismos de defensa, pero también ha generado la necesidad de comprender cómo actúan los atacantes. En este contexto, el uso de laboratorios controlados permite a los estudiantes y profesionales practicar técnicas ofensivas con fines educativos y de investigación.

En el presente trabajo se realizaron dos escenarios de explotación: el primero contra un sistema Windows Server 2003 y el segundo contra una máquina Ubuntu, ambos desde la distribución Kali Linux. Se utilizaron herramientas como Metasploit Framework y msfvenom para generar y ejecutar payloads que permitieron establecer sesiones remotas con Meterpreter.

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 presente informe abarca únicamente la explotación de dos sistemas en un entorno de laboratorio: Windows Server 2003 y Ubuntu. Se limita a la generación de payloads, su ejecución en las máquinas víctimas y el establecimiento de sesiones con Meterpreter para manipular información y procesos. El alcance no incluye la explotación de sistemas en producción ni la ejecución de ataques fuera de un ambiente académico controlado. Tampoco se pretende realizar un análisis exhaustivo de todas las vulnerabilidades existentes, sino demostrar de forma práctica cómo un atacante puede obtener acceso remoto aprovechando malas prácticas de seguridad, como la ejecución de binarios sin verificar su origen.

OBJETIVOS GENERALES

Ejecutar prácticas de explotación controlada contra máquinas Windows Server 2003 y Ubuntu desde Kali Linux desde Oracle VirtualBox, aplicando herramientas de pruebas de penetración, con el fin de comprender las fases de un ataque y reflexionar sobre la importancia de la seguridad defensiva en sistemas operativos.

OBJETIVOS ESPECÍFICOS

- Configurar el entorno de laboratorio en máquinas virtuales para simular un ataque real en condiciones controladas.

- Generar payloads maliciosos adaptados a los sistemas operativos Windows y Linux.

- Ejecutar los payloads y establecer conexiones remotas mediante sesiones de Meterpreter.

- Manipular archivos y procesos en los sistemas comprometidos para demostrar el alcance del control.

- Documentar cada acción con su finalidad y relacionarla con escenarios de seguridad reales.

- Identificar los mecanismos defensivos que podrían haber prevenido o mitigado el ataque.

INFORME – PRÁCTICA DE EXPLOTACIÓN WINDOWS 2003 Y UBUNTU CON KALI LINUX Y METASPLOIT

WINDOWS 2003

1.Preparación del entorno

El primer paso consistió en identificar las direcciones IP de ambos sistemas, ya que esto permitía configurar correctamente la comunicación entre ellos:

- Kali Linux (atacante).
- Windows Server 2003 (víctima).

Verificar las direcciones IP de ambas:

En Kali: ip a

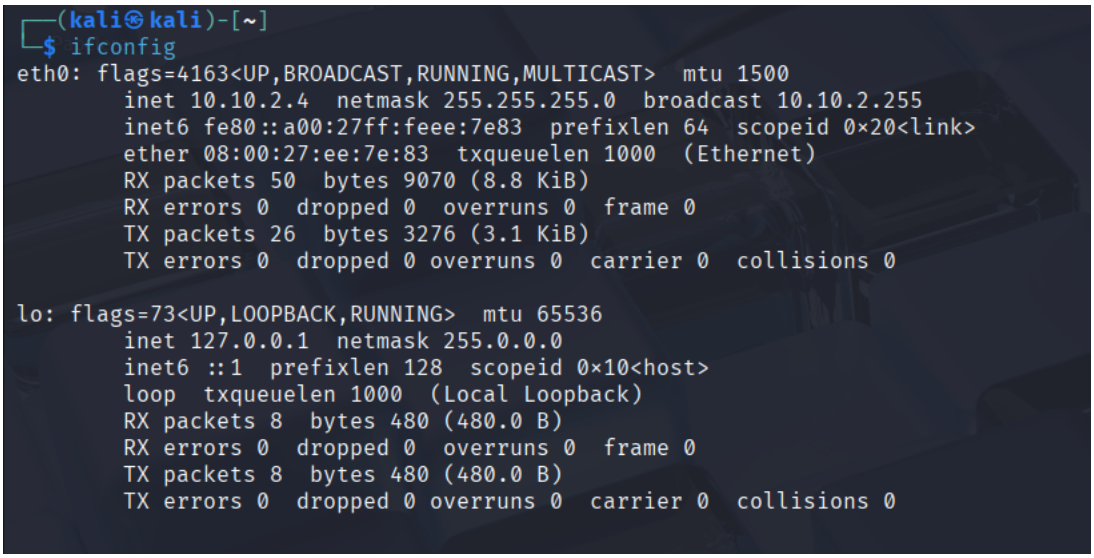

Ilustración 1: Ip atacante

En Windows: ipconfig

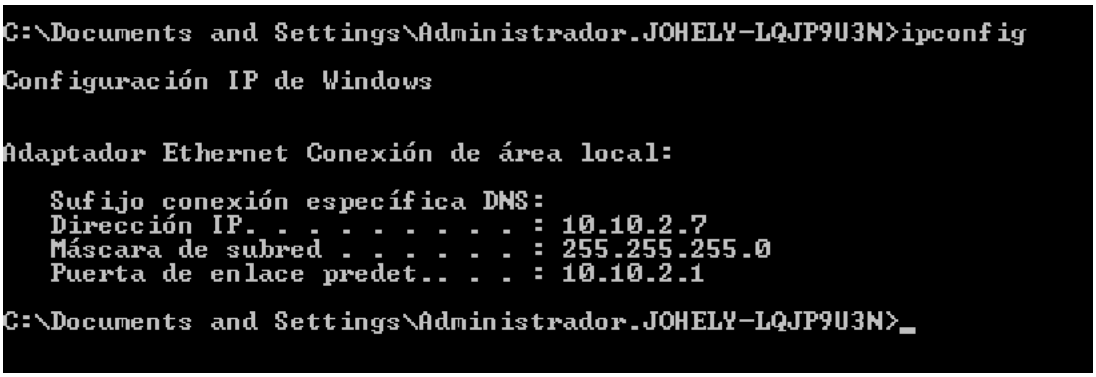

Ilustración 2 Ip atacada

2. Crear el payload malicioso con msfvenom

Posteriormente, en Kali se generó un archivo malicioso con la herramienta msfvenom, indicando como parámetros la dirección IP del atacante y un puerto de escucha. El resultado fue un ejecutable llamado shell.exe, el cual se guardó en la carpeta de Apache para que pudiera ser descargado fácilmente desde el navegador de la víctima.

En Kali:

Ilustración 3 creación de payload

LHOST: dirección IP de Kali.

LPORT: puerto de escucha (ej: 4444).

-f exe: genera archivo ejecutable de Windows.

> /var/www/html/shell.exe: guarda el archivo directamente en la carpeta web de Apache.

3. Activar servidor Apache en Kali

Esto permite compartir el archivo shell.exe con la víctima. Una vez generado el archivo, se levantó el servicio web de Apache en Kali y se verificó que el archivo estuviera disponible en el directorio /var/www/html.

sudo service apache2 start

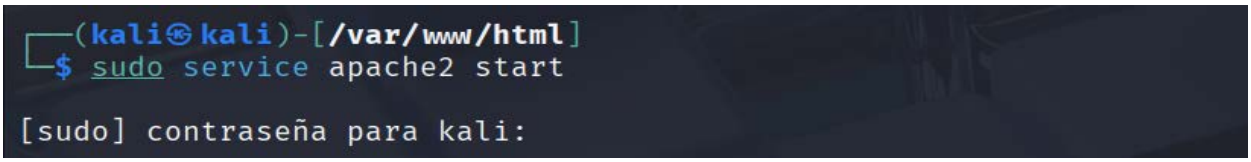

Ilustración 4 activar apache2

sudo service apache2 status

Ilustración 5 apache2 status

4. Configurar Metasploit Handler

Paralelamente, en Metasploit se configuró un módulo handler para escuchar conexiones entrantes. En este módulo se definió el mismo payload utilizado en la creación del ejecutable, junto con la dirección IP y el puerto configurados previamente. En Kali, abrimos Metasploit:

set PAYLOAD windows/meterpreter/reverse_tcp

Ilustración 6 set PAYLOAD windows/meterpreter/reverse_tcp

(El handler queda esperando que la víctima ejecute el archivo malicioso).

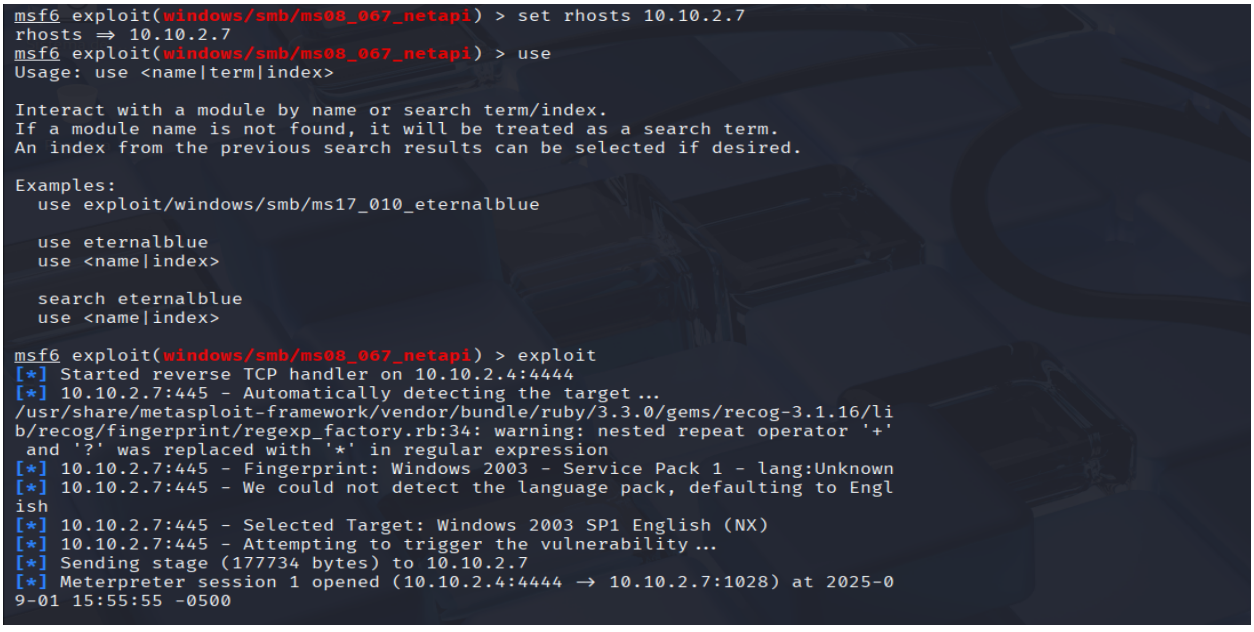

Ilustración 7 exploit windows 2003

5. Descargar y ejecutar payload en Windows

En el servidor Windows 2003, utilizando el navegador Internet Explorer, se accedió a la dirección del atacante y se descargó el archivo shell.exe. Al ejecutarlo, automáticamente se estableció una sesión de Meterpreter en Kali, lo que confirmó la correcta ejecución del ataque. Desde este momento se tuvo control remoto sobre la máquina víctima, pudiendo ejecutar distintos comandos. En Windows (víctima):

Abrir el navegador Internet Explorer.

Acceder a la dirección de Kali para descargar el archivo:

http://10.10.2.4/shell.exe

Ilustración 8 http://10.10.2.4/shell.exe

Guardar el archivo en el escritorio o en C:\.

Ejecutar el archivo shell.exe.

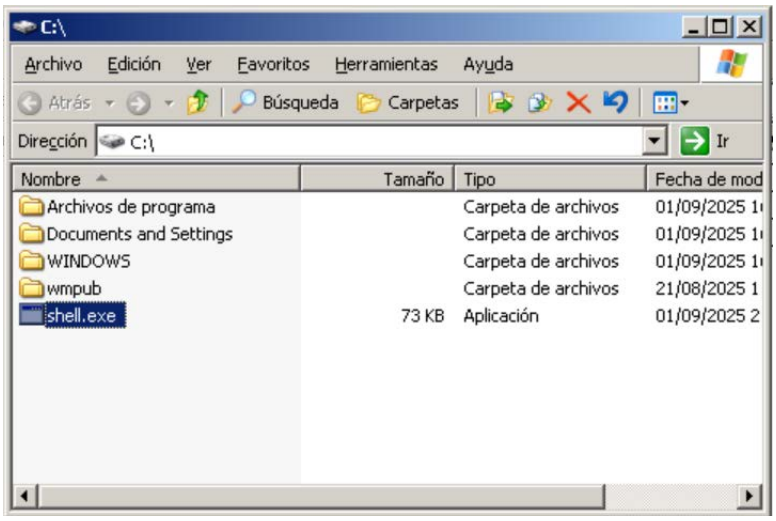

Ilustración 9 shell.exe

En este momento, en Kali (donde está el multi/handler), se abrirá una sesión de Meterpreter.

Comandos básicos en Meterpreter

Sysinfo: Muestra información del sistema

Getuid: Usuario actual

Getsystem: Intenta escalar privilegios a SYSTEM

Hashdump: Extrae los hashes de contraseñas de Windows

Ps: Lista de procesos

migrate PID: Migrar el payload a otro proceso (ej: explorer.exe)

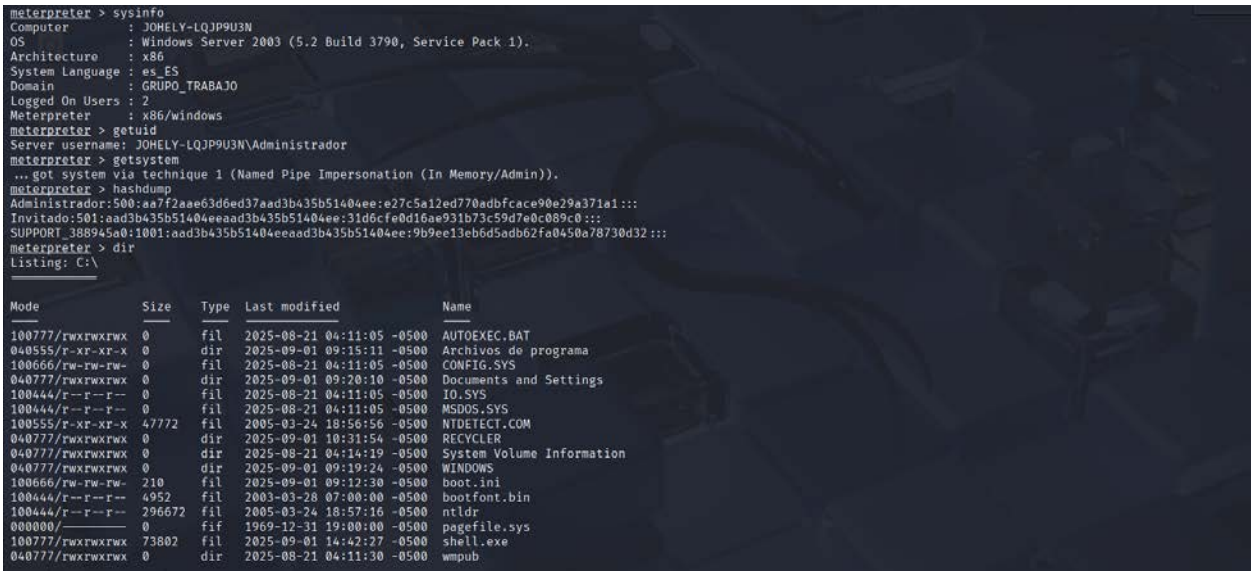

Ilustración 10 comandos de meterpreter para windows 2003

7.Cracking de contraseñas

Si se ejecutó hashdump y se obtuvieron hashes de Windows:

Copiar los hashes.

Pegarlos en Crackstation.net para intentar descifrarlos.

Ilustración 11 Crackstation.net

UBUNTU

1.Primero se comprueba la conectividad y la arquitectura de la víctima. En Kali se verifica la IP con ip a y desde la VM Ubuntu se comprueba la propia IP y la arquitectura.

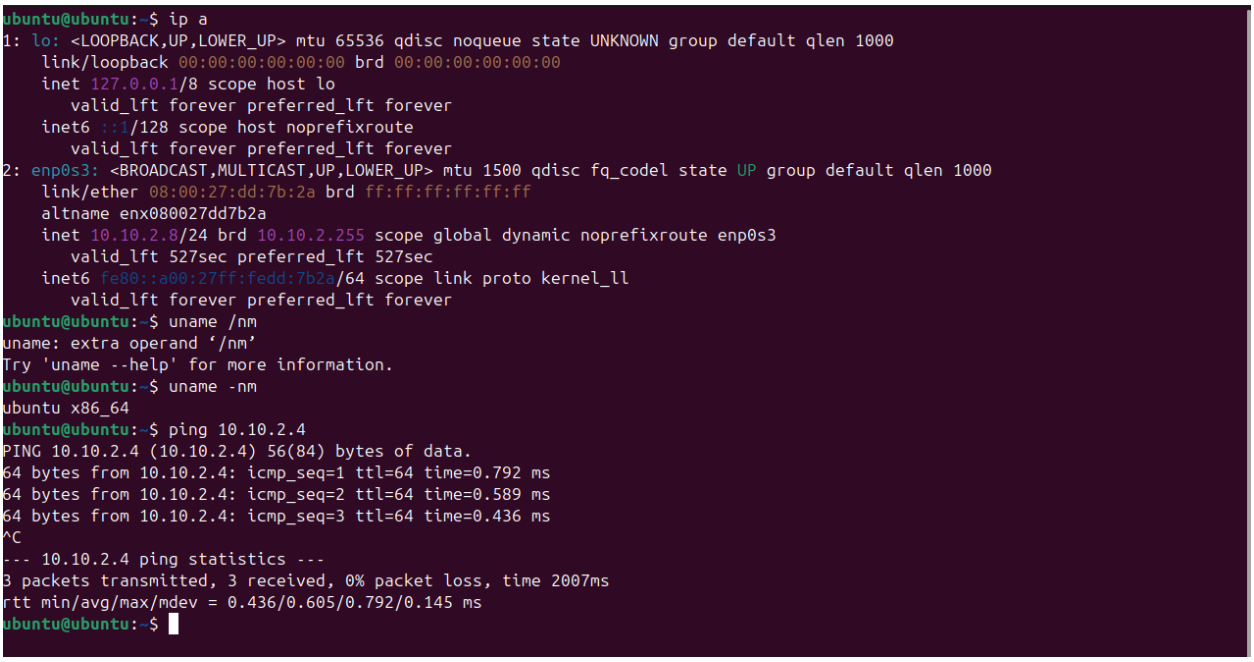

Ilustración 12 ip ubuntu

2. En Kali se genera el payload adaptado a la arquitectura detectada. Si la víctima es 64-bit, se usa el payload Linux x64; si es 32-bit se usa x86. Por ejemplo (cambia 10.10.2.4 por la IP de tu Kali y 4444 por el puerto que uses)

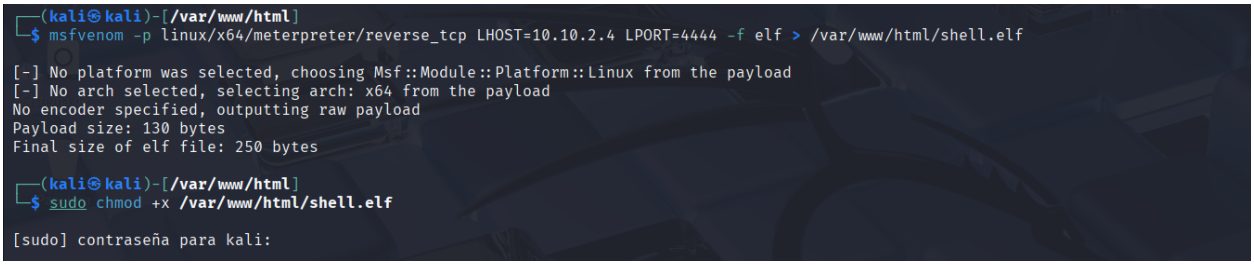

Ilustración 13

3. Se prepara el servidor para distribuir el payload. Si usas Apache en Kali colocaste el archivo en /var/www/html/ (como en el comando anterior); asegúrate de que Apache esté activo.

Ilustración 14

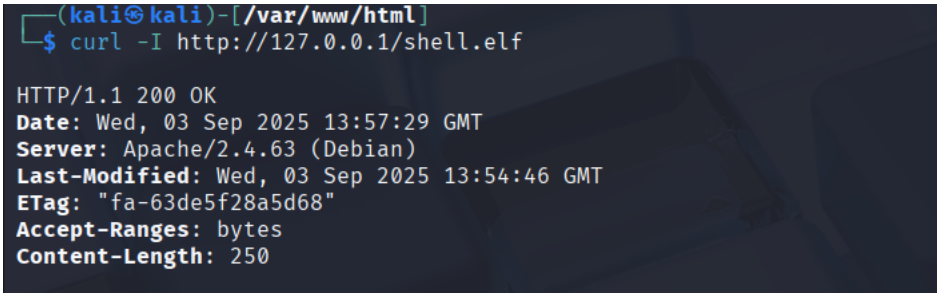

Ilustración 15

4. En Kali se configura el handler en Metasploit para escuchar la conexión inversa que la víctima va a abrir.

Ilustración 16

5. En la máquina Ubuntu (víctima) se descarga el binario desde Kali y se ejecuta. Desde la terminal de Ubuntu.

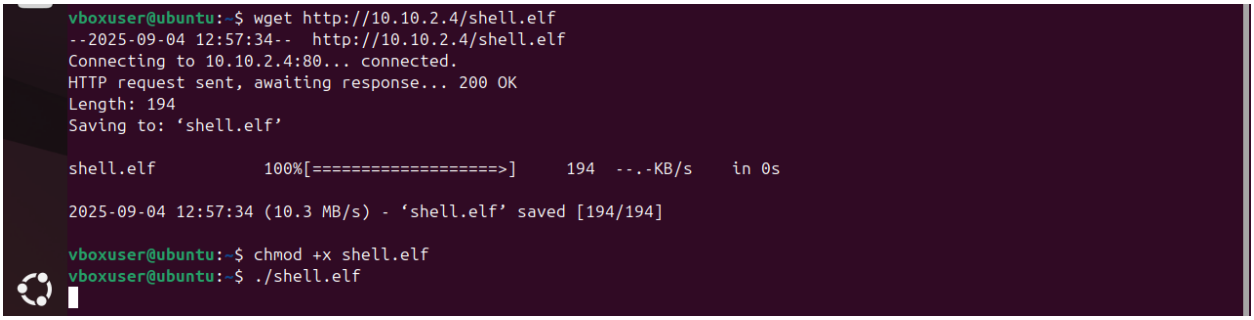

Ilustración 17

6. Al obtener la sesión Meterpreter, se realizan las acciones de reconocimiento y manejo de archivos.

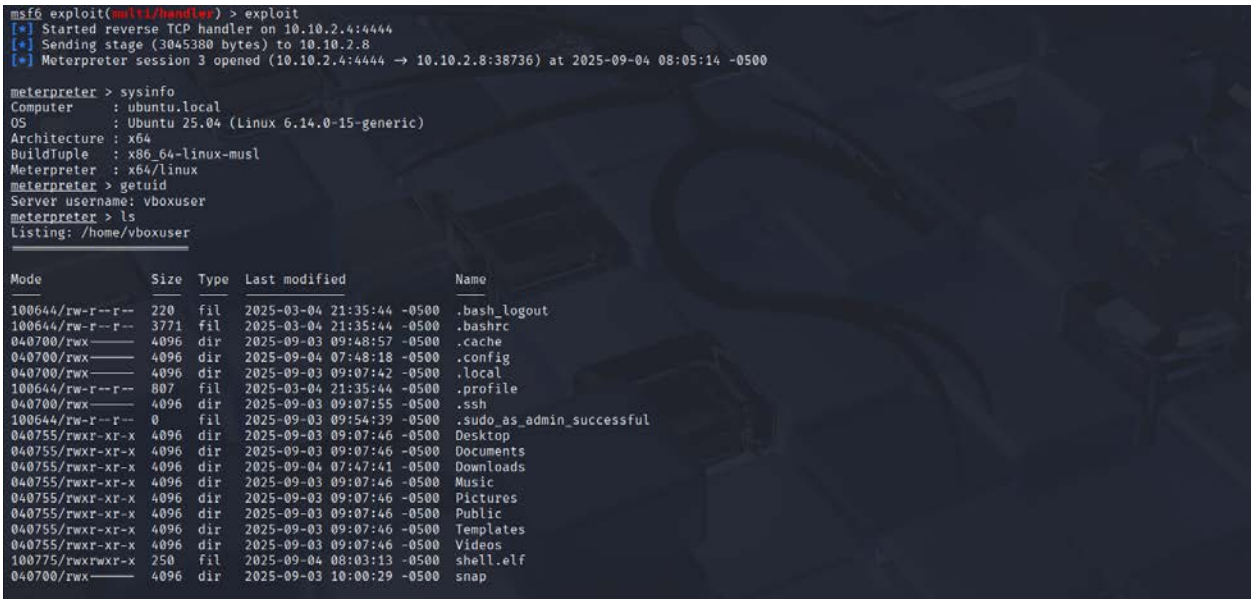

Ilustración 18

7. Ocultar evidencia

IDS / IPS (conceptos vistos en clase)

IDS (Intrusion Detection System): detecta ataques y genera alertas.

IPS (Intrusion Prevention System): bloquea ataques en tiempo real.

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.

- Kali Linux: Distribución de GNU/Linux especializada en pruebas de penetración y auditoría de seguridad.

- Metasploit Framework: Plataforma utilizada para desarrollar, probar y ejecutar exploits contra sistemas remotos.

- msfvenom: Herramienta incluida en Metasploit para generar payloads en distintos formatos.

- Payload: Código malicioso que se ejecuta en el sistema víctima para establecer una conexión o realizar una acción específica.

- Meterpreter: Intérprete avanzado que se ejecuta en la memoria de la máquina víctima y permite al atacante interactuar con ella.

- Reverse TCP: Técnica en la cual la máquina víctima inicia una conexión hacia el atacante, facilitando eludir firewalls.

- Apache2: Servidor web utilizado en Kali Linux para alojar y distribuir archivos hacia las máquinas víctimas.

CONCLUSIONES

La práctica demostró que tanto Windows como Linux son susceptibles a ataques cuando no se aplican medidas básicas de seguridad. La explotación realizada permitió comprender cómo un atacante prepara su entorno, genera el payload, logra la ejecución en la víctima y mantiene el

control remoto mediante sesiones de Meterpreter. Aunque los entornos de laboratorio se realizaron con fines académicos, los resultados reflejan riesgos reales a los que se enfrentan las organizaciones en su operación diaria.

Es fundamental promover una cultura de ciberseguridad que incluya el uso de antivirus, firewalls, actualizaciones constantes y, sobre todo, concientización de los usuarios para evitar la ejecución de archivos de origen desconocido. En conclusión, esta experiencia práctica reafirma que el conocimiento de las técnicas ofensivas es indispensable para diseñar y aplicar estrategias defensivas efectivas.