HACKING PARA LA CREACION DE NUEVOS USUARIOS EN EL SITIO WEB DE LAMPIAO DESDE EL 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

HACKING PARA LA CREACION DE NUEVOS USUARIOS EN EL SITIO WEB DE LAMPIAO DESDE EL 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

En esta práctica trabajamos con Lampiao, una aplicación web usada para aprender sobre seguridad informática. El objetivo fue simular un ataque controlado desde Kali Linux para crear nuevos usuarios en el sitio y así ver qué fallas existen. Durante el ejercicio aplicamos técnicas básicas de reconocimiento, identificación de puntos débiles y ejecución de comandos para explotar vulnerabilidades. Esto nos permitió comprender, paso a paso, cómo un atacante puede aprovechar errores de configuración o código inseguro.

2. Objetivos

2.1. Objetivo General

Aprender a identificar y aprovechar vulnerabilidades en Lampiao usando Kali Linux para identificar y explotar vulnerabilidades que permitan la creación de usuarios.

2.2. Objetivos Específicos

- Identificar vulnerabilidades y puntos de entrada en Lampiao.
- Ejecutar pruebas controladas para crear usuarios y documentar los pasos.
- Proponer recomendaciones para corregir las fallas detectadas.

3. Justificación

La justificación es doble: académica y práctica. Académicamente, la actividad refuerza contenidos vistos en clase (reconocimiento, explotación y documentación). En lo práctico, permite ver los errores comunes que cometen desarrolladores y administradores de sistemas y aprender a mitigarlos. También fomenta la responsabilidad: al practicar en un entorno controlado, entendiendo la diferencia entre usar conocimientos para aprender y hacerlo para causar daño.

4. Planteamiento de la Actividad

En la asignatura de Seguridad y Auditoría de Redes, el profesor planteó como actividad la explotación de vulnerabilidades en Lampiao utilizando Kali Linux. La intención era aplicar los conceptos aprendidos en clase y demostrar la creación de usuarios en el sistema como evidencia de la falla de seguridad.

El problema principal surgió al momento de ejecutar los comandos necesarios para llevar a cabo la práctica. Aunque en teoría se conocían las herramientas y la secuencia de pasos, en la práctica varios comandos no funcionaban, ya sea por errores de sintaxis, falta de parámetros o desconocimiento del uso correcto. Esto generó retrasos, confusión y dificultad para cumplir el objetivo.

.

5. Desarrollo del tema

5.1. Capitulo #1

5.1.1 Escaneo de Red con Nmap

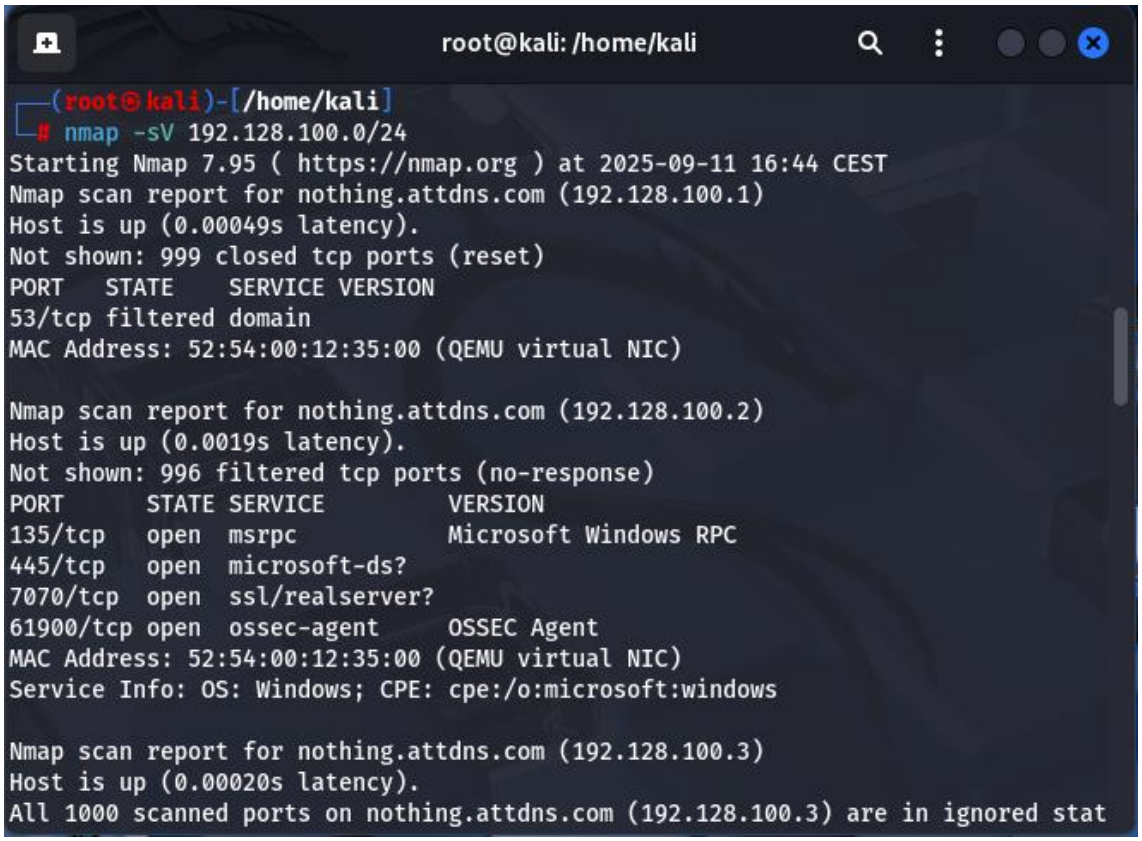

Ilustración 1. Resultado del escaneo de puertos en la red 192.128.100.0/24.

Esta captura de pantalla muestra la ejecución del comando nmap -sV 192.128.100.0/24 desde la terminal de Kali Linux. El objetivo de este paso fue realizar un reconocimiento inicial de la red para identificar hosts activos y los servicios y versiones que se estaban ejecutando en sus puertos abiertos.

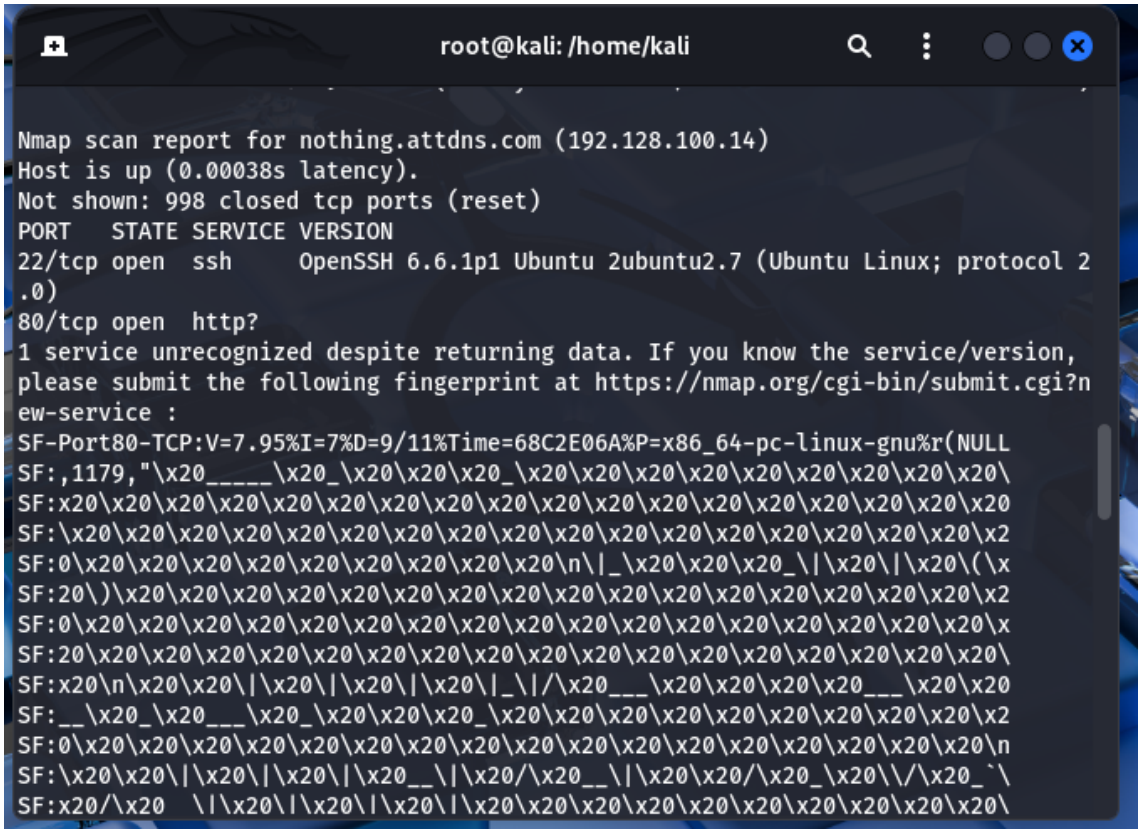

Ilustración 2. Resultado del escaneo de puertos en la red 192.128.100.0/24.

5.1.2 Identificación del Objetivo - Máquina Lampião

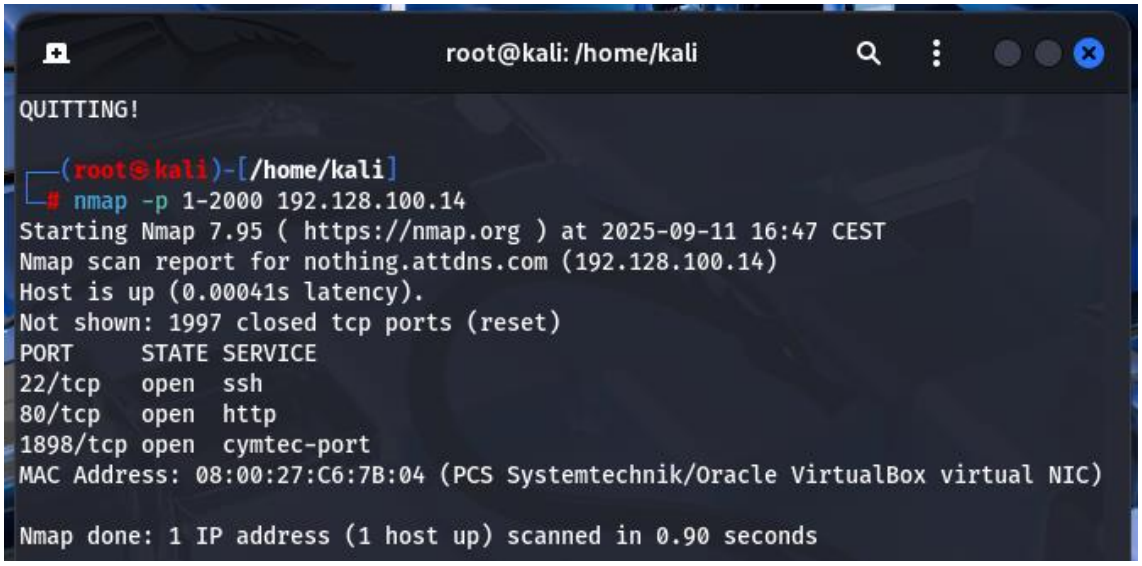

Ilustración 3. Escaneo de puertos dirigido a la IP 192.128.100.14.

Tras el escaneo general de la red, se identificó a la máquina con la dirección IP 192.128.100.14 como el objetivo principal, confirmando que se trata de la máquina virtual de Lampião. El comando nmap -p 1-2000 192.128.100.14 se utilizó para realizar un escaneo más detallado.

5.1.3 Interfaz visual con la IP de Lampiao en el navegador

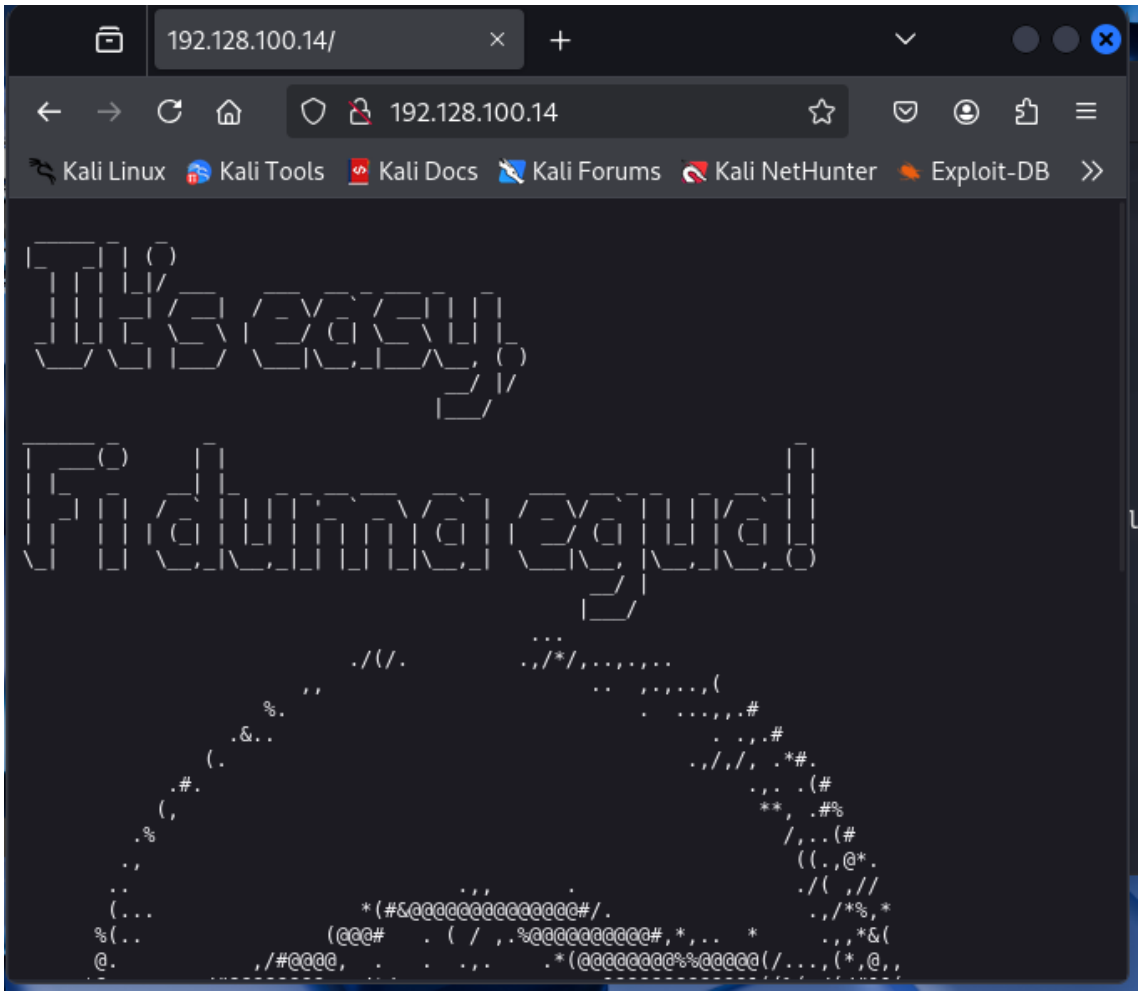

Ilustración 4. Navegación con la IP de Lampia

Una vez de haber identificado a través del escaneo de la red la dirección IP de Lampiao, se pudo ingresar a la interfaz visual de Lampiao sin que esta mostrara el index principal.

5.1.4 Página de Inicio y Login de Lampião

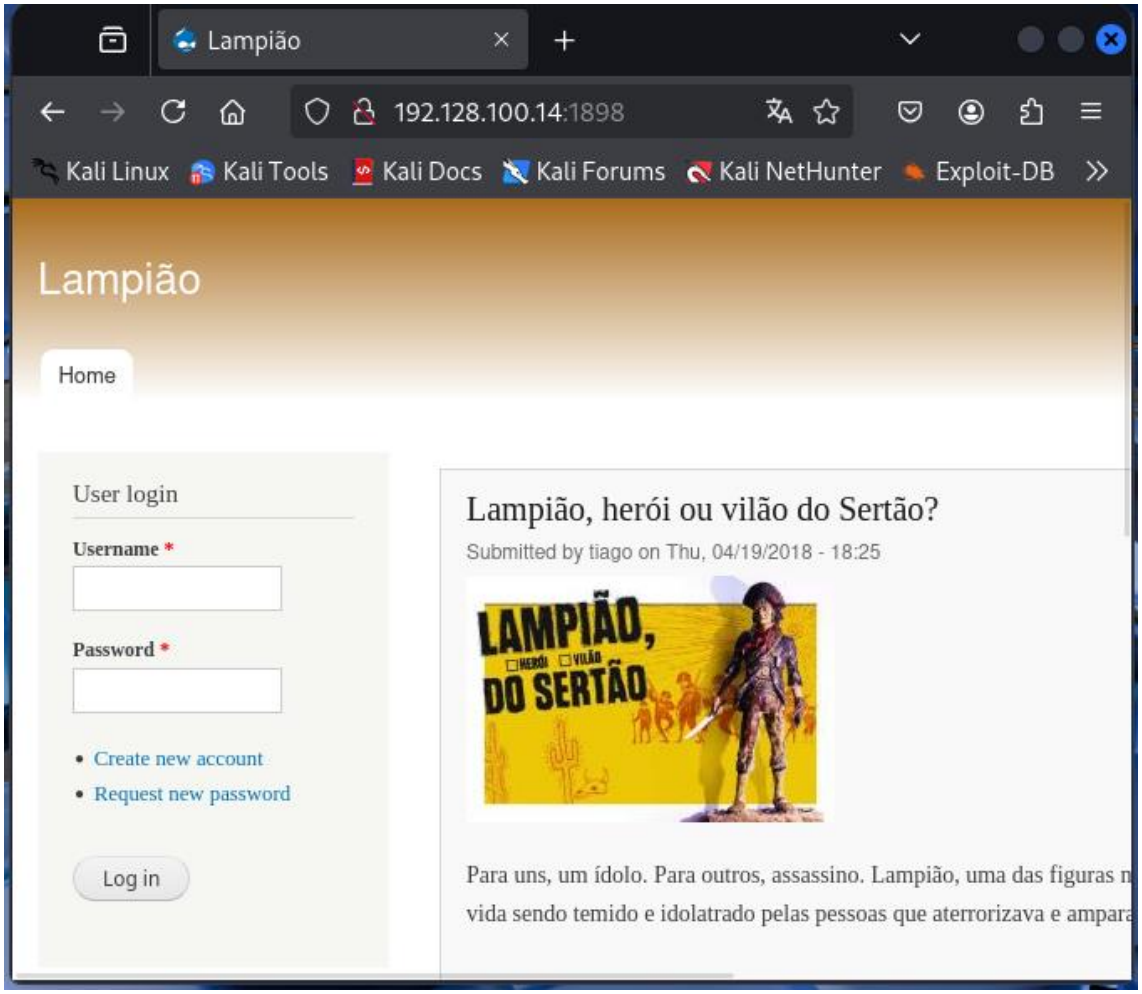

Ilustración 5. Interfaz web principal de la aplicación Lampião

La captura muestra la página de inicio de la aplicación web Lampião, accesible a través de http://192.128.100.14. La interfaz presenta dos elementos principales de interés:

Formulario de Login

Contenido Público

5.1.5 Análisis Detallado del Servicio SSH

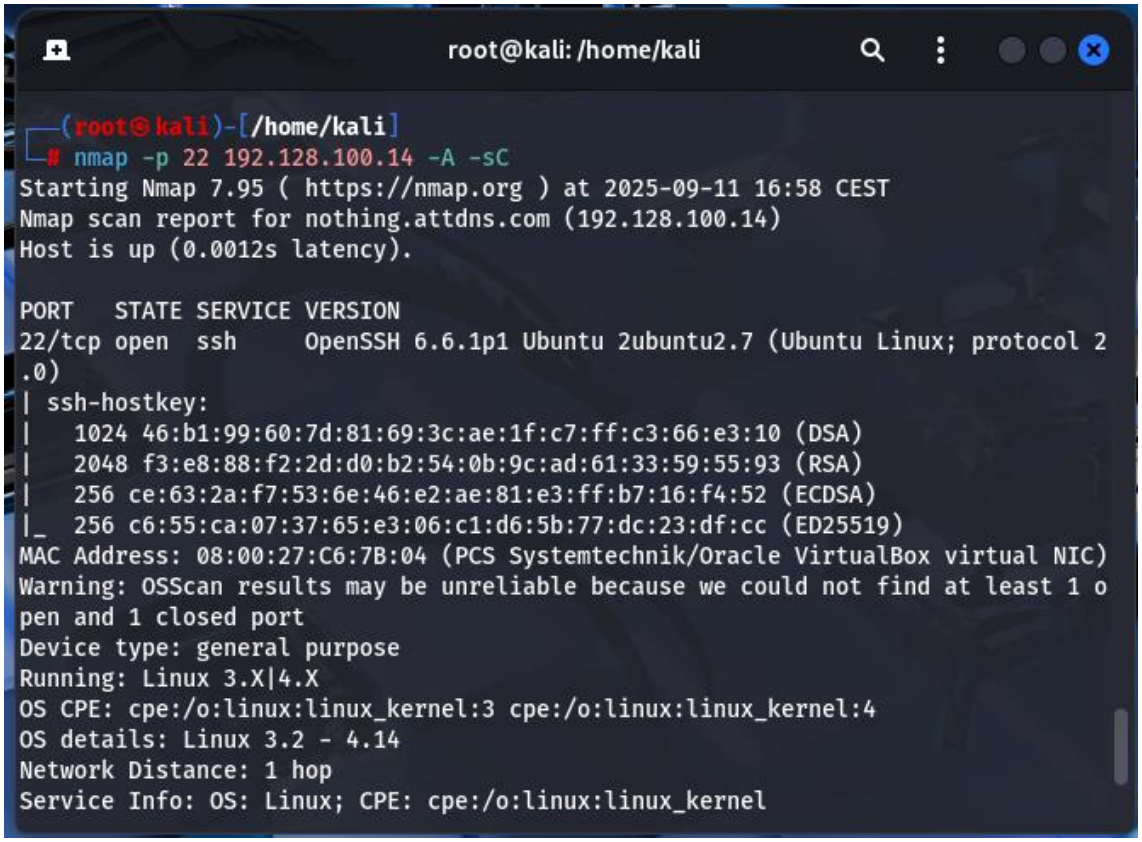

Ilustración 6. Resultado del escaneo con scripts sobre el puerto SSH (22)

El comando nmap -p 22 192.128.100.14 -A -sC se ejecutó para obtener información detallada del servicio SSH identificado previamente.

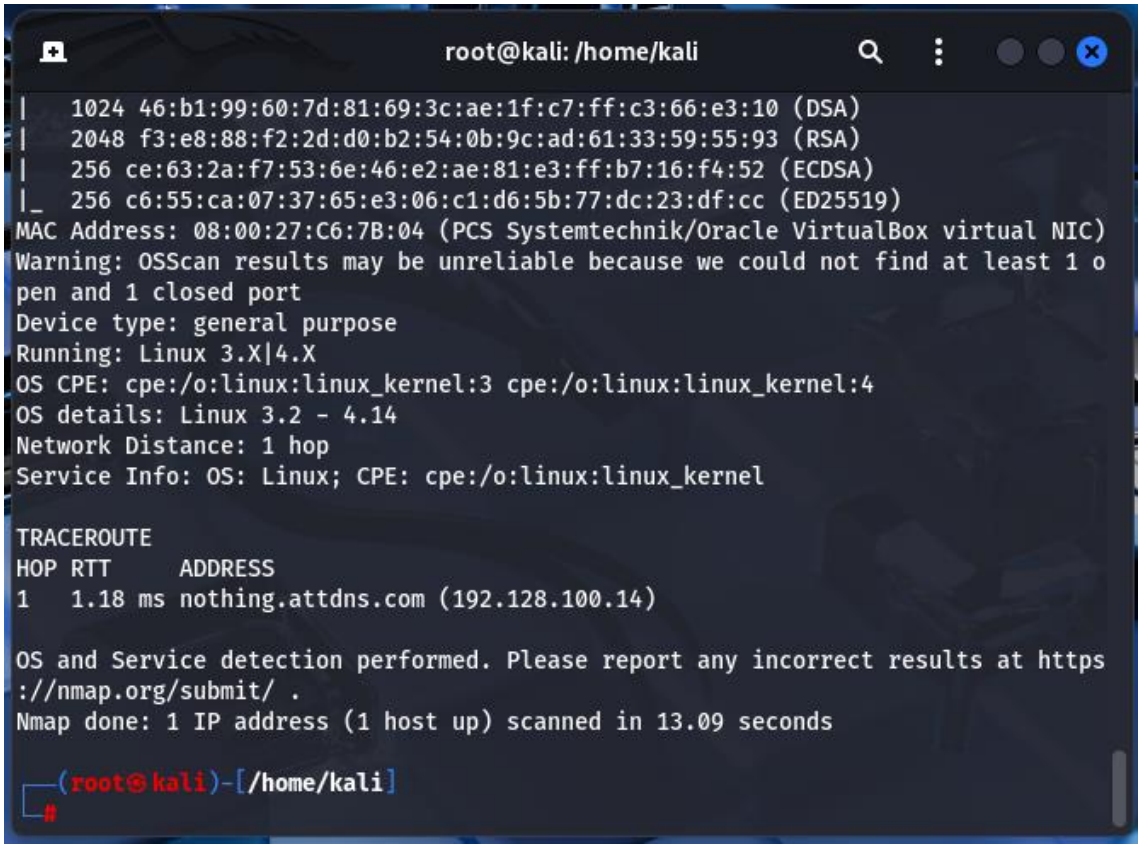

Ilustración 7. Resultado del escaneo con scripts sobre el puerto SSH (22)

Los resultados clave son:

- **Versión del Servicio:** OpenSSH 6.6.1p1
- **Huellas Digitales:** Se recopilaron las claves públicas del host
- **Detección de Sistema Operativo:** Nmap

5.1.6 Descubrimiento de Directorios

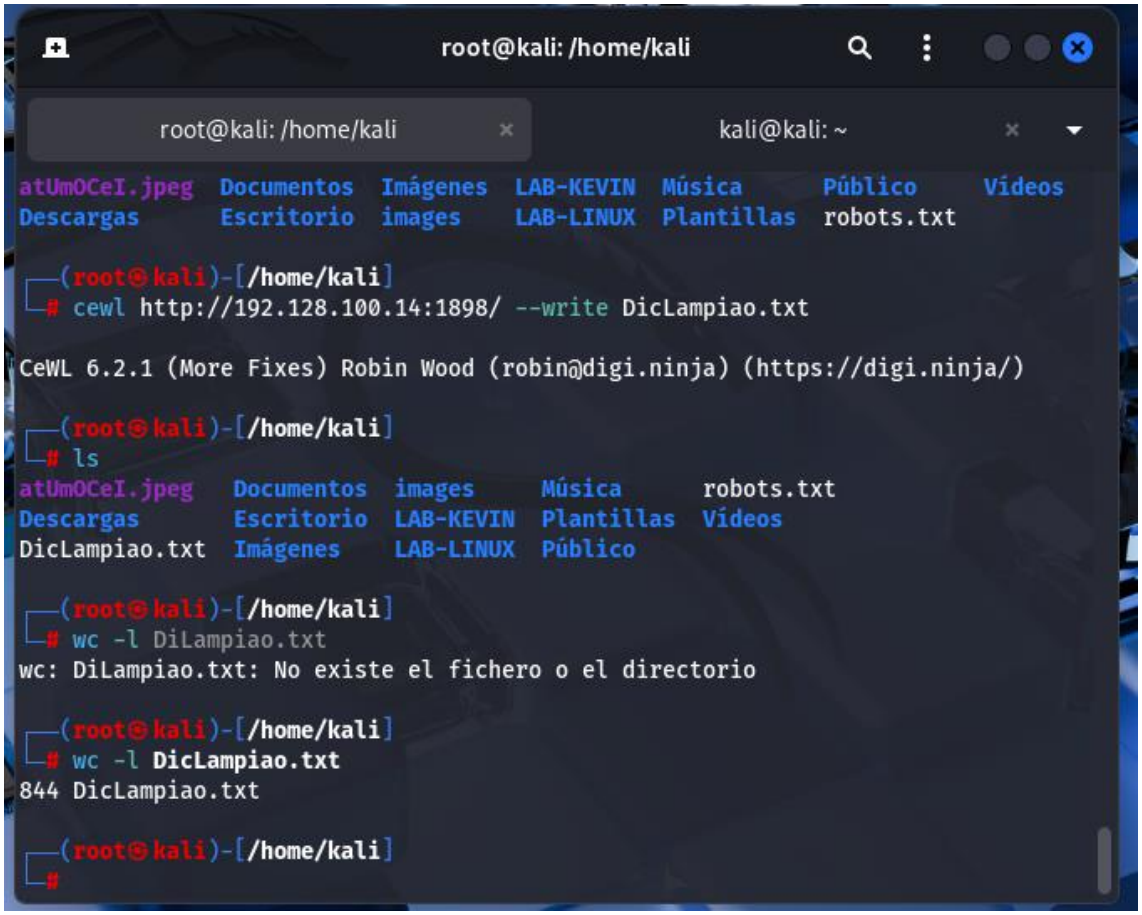

Ilustración 8. Uso de la herramienta cevl para descubrir rutas en el servidor web.

En esta fase se utilizó la herramienta cewl para descubrir directorios y archivos ocultos en el servidor web de Lampiao (http://192.128.100.14:1898/). El comando cewl http://192.128.100.14:1898/ --write DicLampiao.txt ejecutó un escaneo y guardó los resultados en un archivo de texto llamado DicLampiao.txt.

5.1.7 Contenido del Diccionario

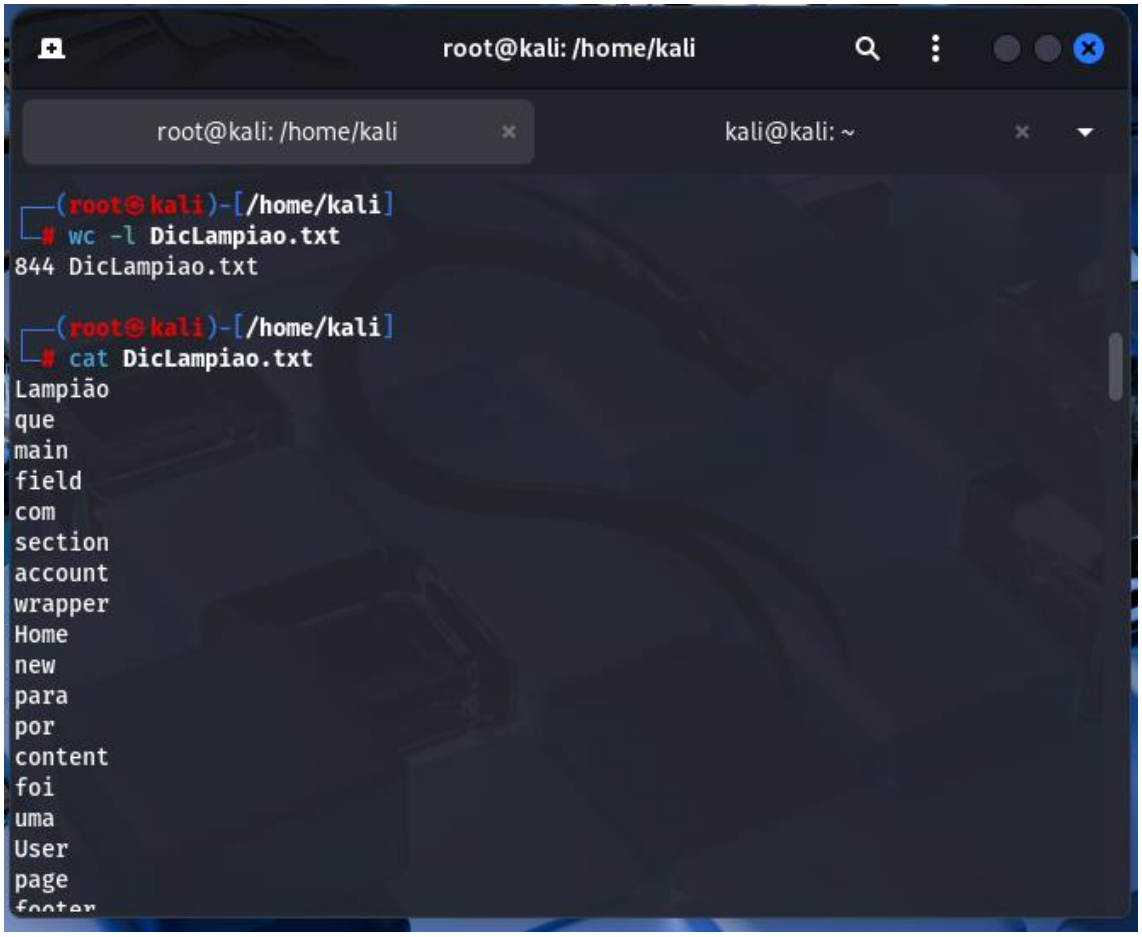

Ilustración 9.Visualización del archivo DicLampiao.txt

Tras el escaneo de directorios, se visualiza el contenido del archivo DicLampiao.txt usando el comando cat. El archivo contiene un listado de palabras y rutas descubiertas en la aplicación web.

5.1.8 Pantalla de ayuda de la herramienta Hydra

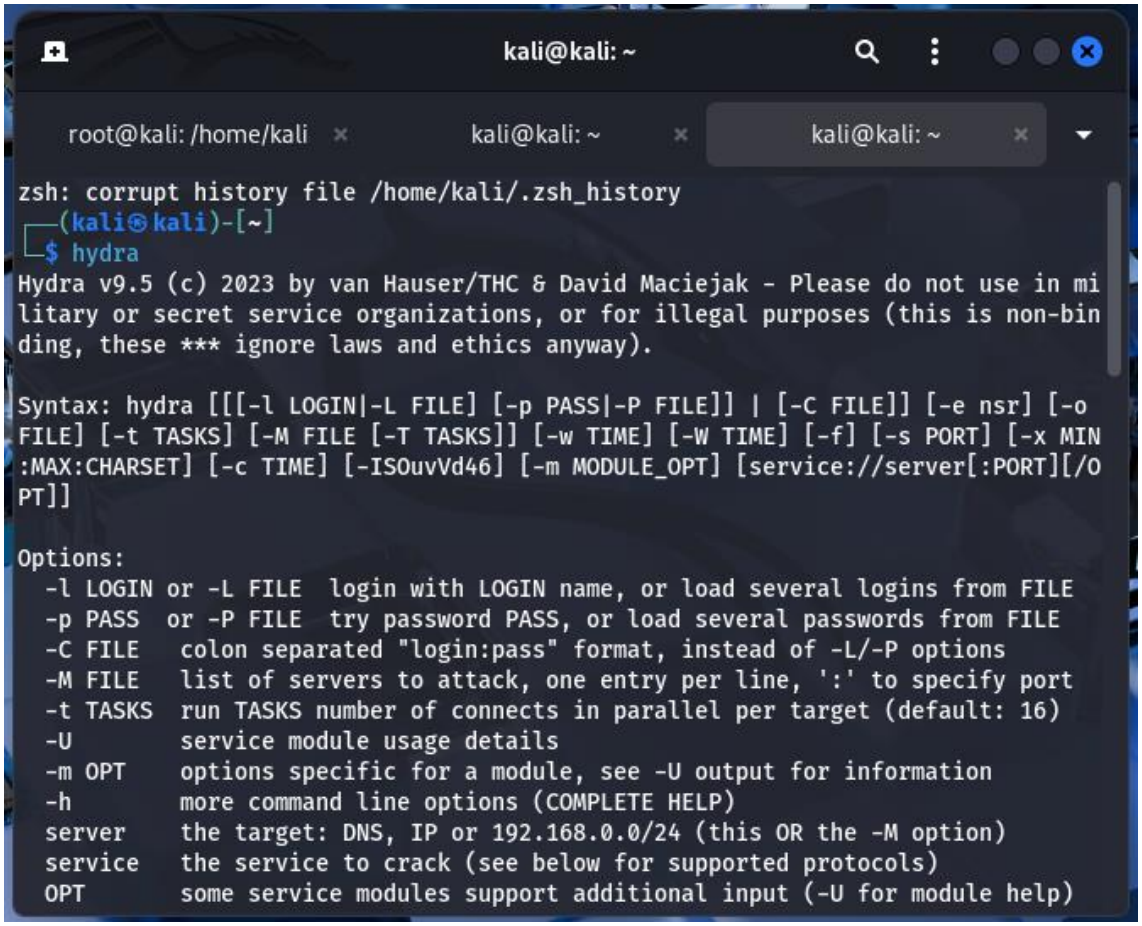

Ilustración 10. Resumen de sintaxis y opciones básicas de Hydra.

Captura de la salida de ayuda del comando hydra en Kali Linux, mostrando la versión, la sintaxis general y las opciones principales para realizar ataques de fuerza bruta (login, password, archivos, módulos y parámetros de conexión).

5.1.9 Ataque SSH con diccionario mediante Hydra

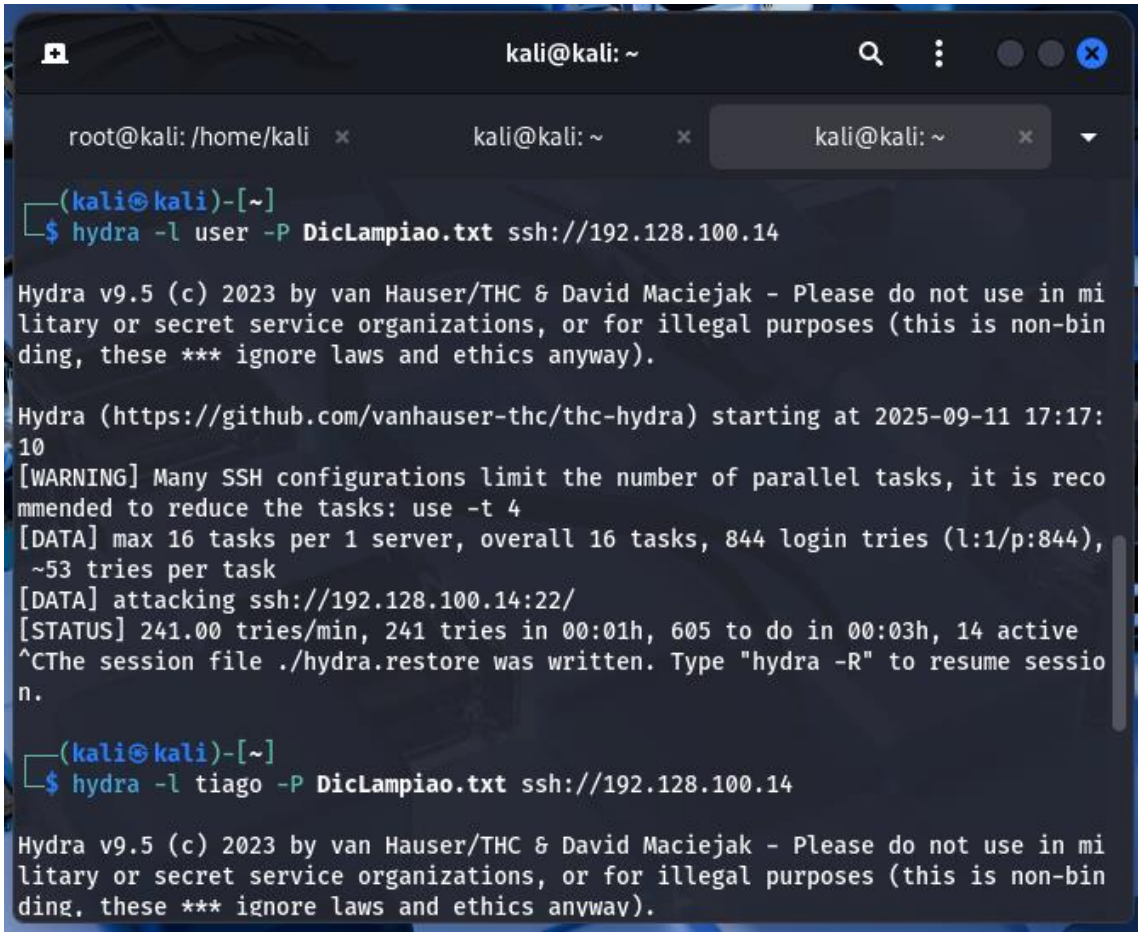

Ilustración 11. Ejecución de Hydra contra SSH en Lampiao.

Captura del terminal donde se ejecuta hydra -l <usuario> -P DicLampiao.txt ssh://192.128.100.14. Se muestran mensajes de inicio de Hydra. También se ve que Hydra creó un archivo de sesión para reanudar el ataque.

5.1.10 Credenciales encontradas por Hydra

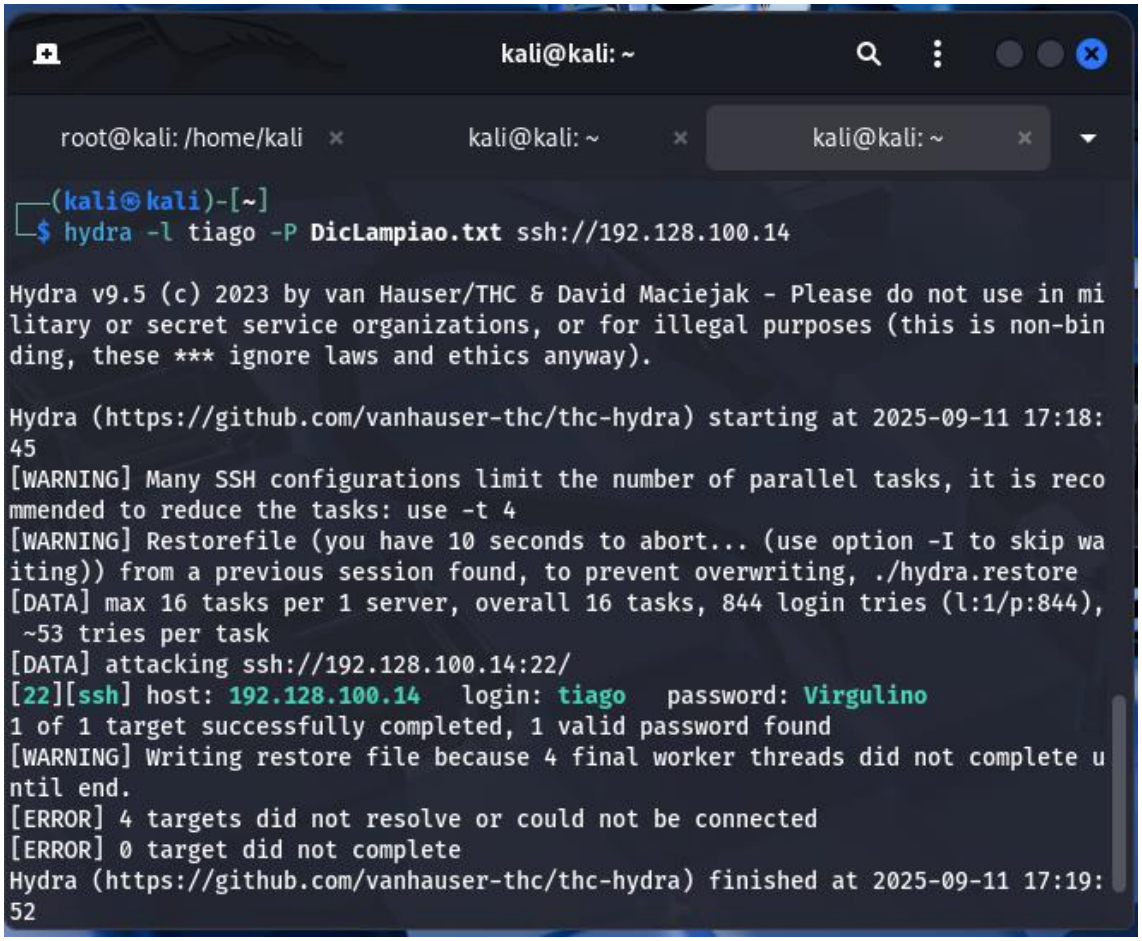

Ilustración 12. Resultado exitoso de fuerza bruta sobre SSH.

Captura del terminal mostrando la ejecución de hydra -l tiago -P DicLampiao.txt ssh://192.128.100.14 y la salida final donde Hydra informa que encontró una credencial válida: usuario tiago y contraseña Virgulino.

5.1.11 Prueba de contraseñas (Hydra)

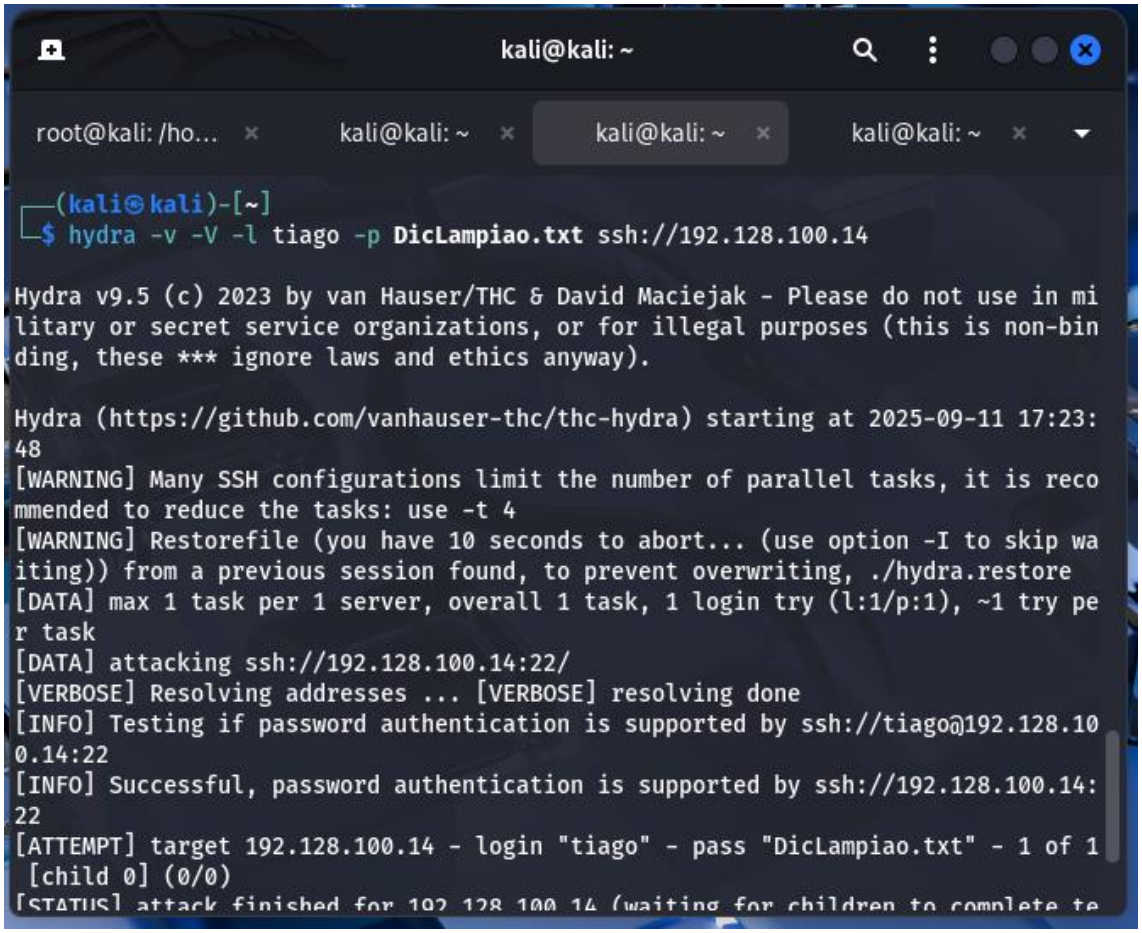

Ilustración 13. Resultado de intento de autenticación.

Captura del terminal mostrando la ejecución hydra -v -V -l tiago -p DicLampiao.txt ssh://192.128.100.14. Se aprecian advertencias sobre la verificación de que la autenticación por contraseña está soportada y el intento de autenticación para el usuario tiago usando el archivo de contraseñas DicLampiao.txt.

5.1.12 Acceso Exitoso vía SSH

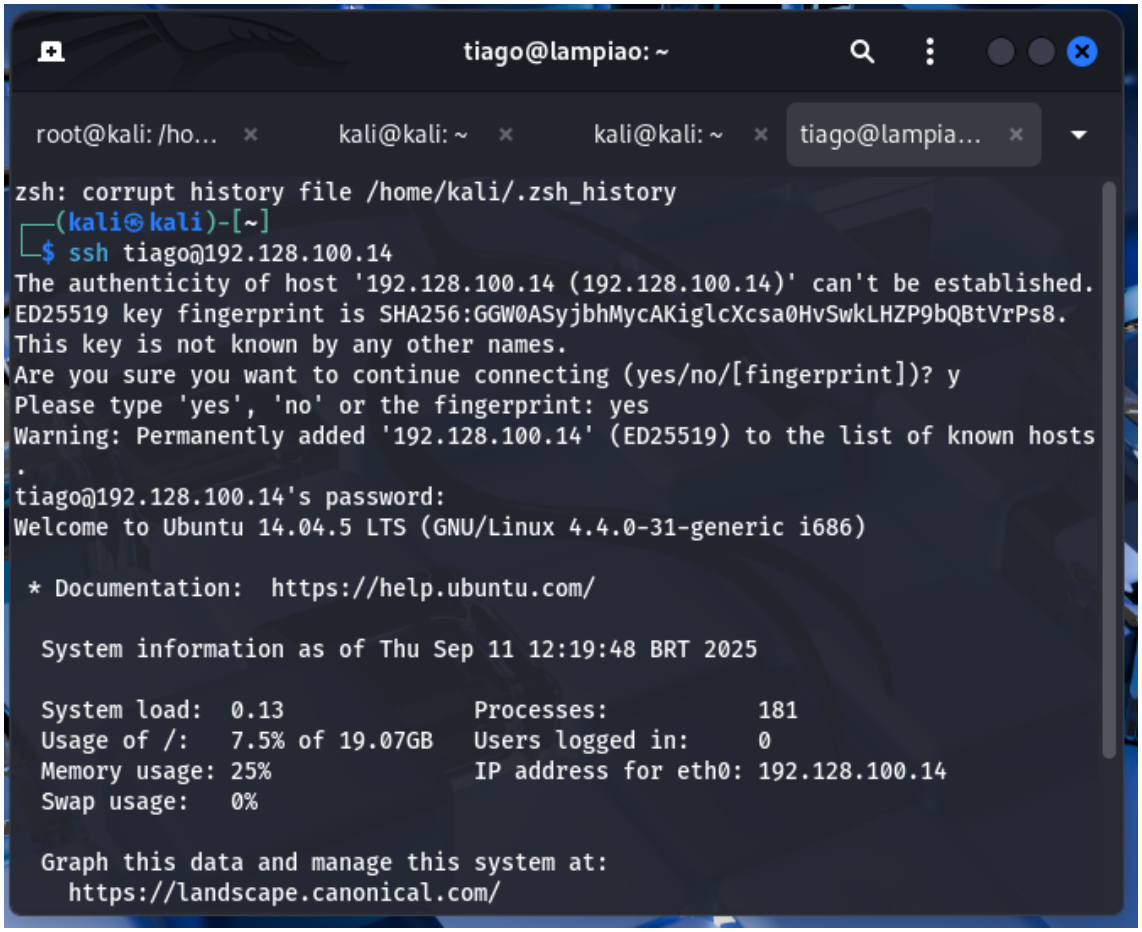

Ilustración 14. Conexión SSH establecida al servidor Lampião

Se logró un acceso inicial al sistema mediante el servicio SSH (puerto 22) utilizando el nombre de usuario tiago descubierto durante la fase de reconocimiento. El comando ssh tiago@192.128.100.14 inició la conexión, que fue autenticada exitosamente con una contraseña.

5.1.13 Descarga de Herramienta de Escalada de Privilegios LinEnum

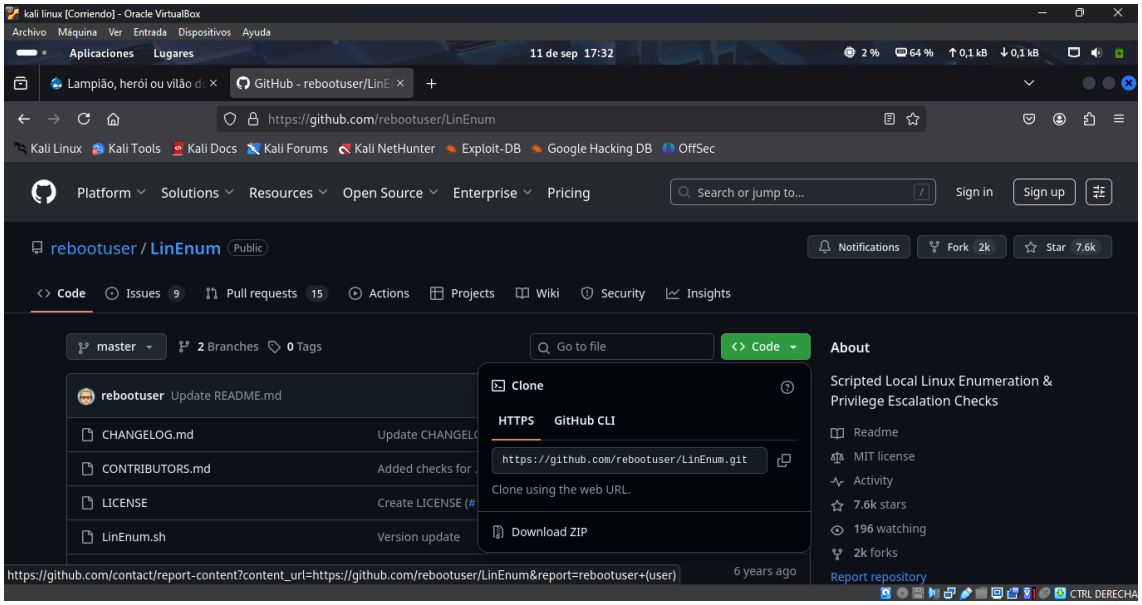

Ilustración 15. Clonación del script LinEnum.sh en GitHub

Visita al repositorio de GitHub rebootuser/LinEnum, que contiene un script de enumeración muy conocido.

LinEnum automatiza la búsqueda común de escalada de privilegios en sistemas Linux

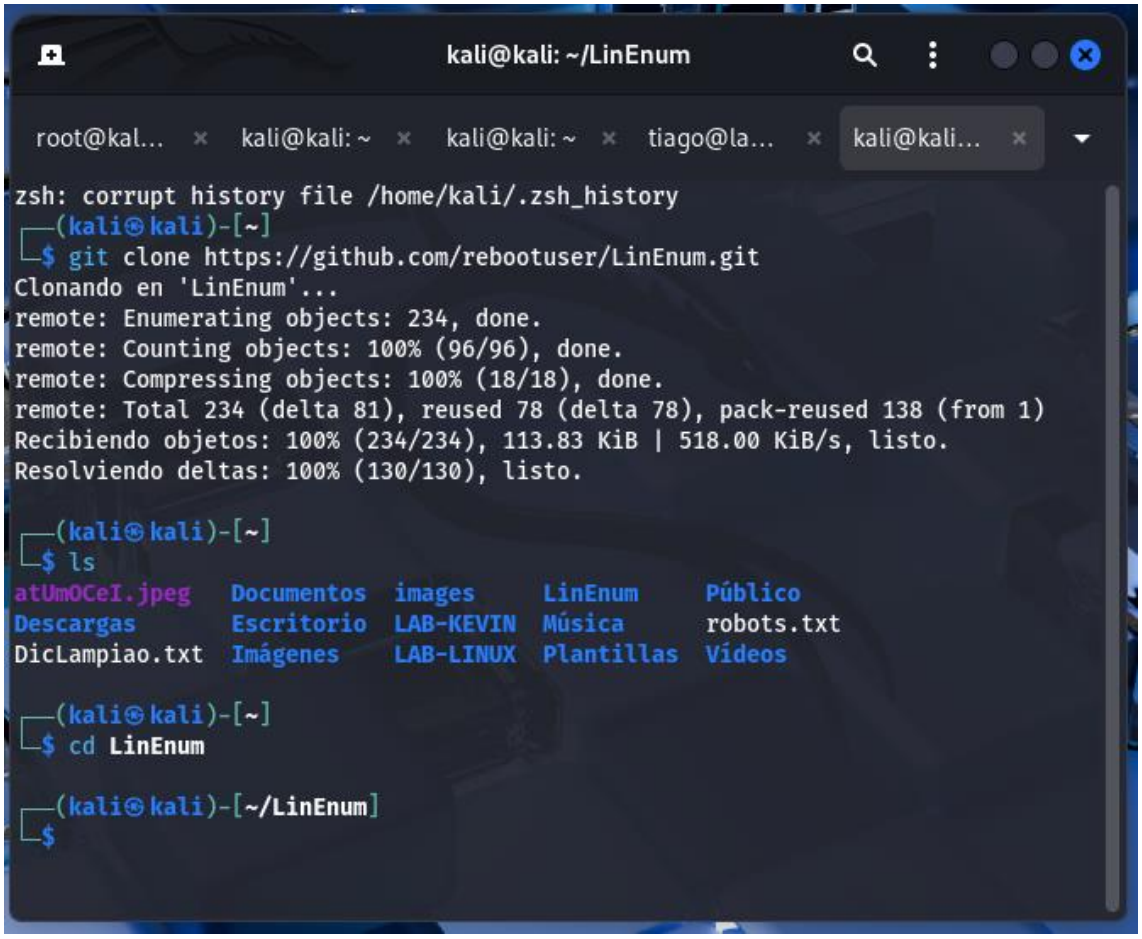

Ilustración 16. Clonación del script LinEnum.sh en la consola

La ejecución del comando git clone https://github.com/rebootuser/LinEnum.git para descargar la herramienta.

5.1.14 Verificación y Preparación del Script LinEnum.sh

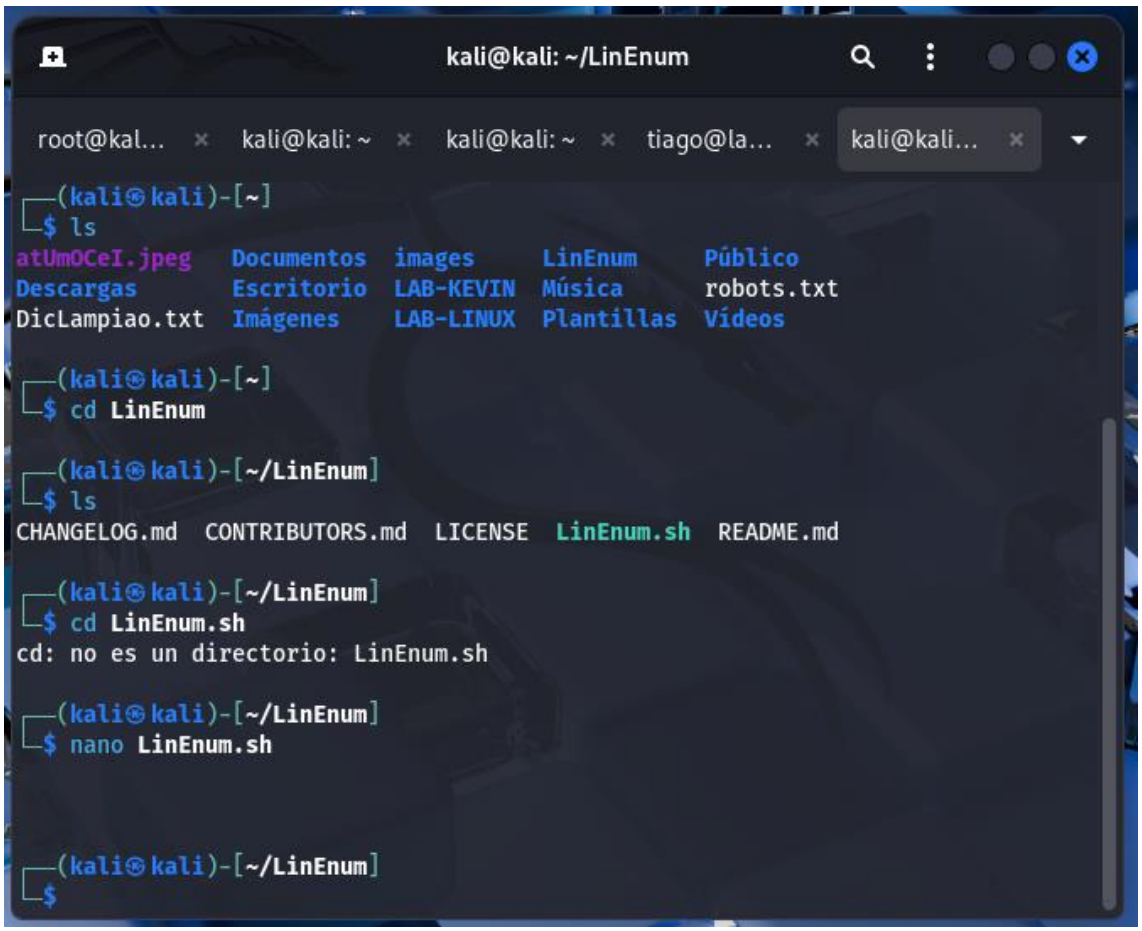

Ilustración 17. Navegación y verificación del contenido del directorio LinEnum

Una vez clonado el repositorio, se verifica su contenido con el comando ls, confirmando la presencia del script principal LinEnum.sh junto con archivos de documentación

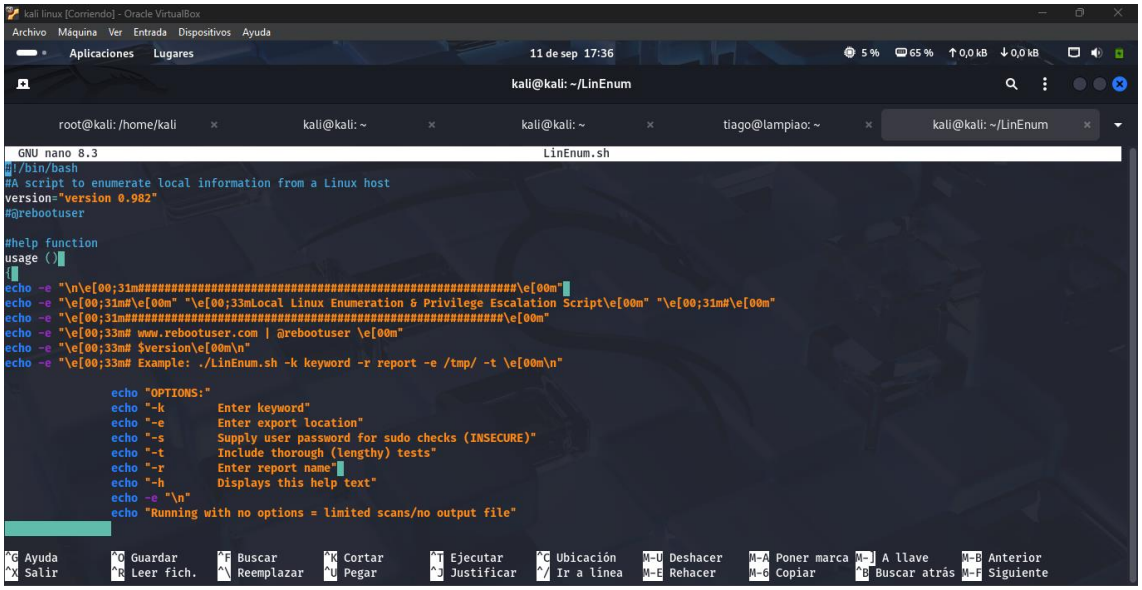

Ilustración 18. Apertura del script principal de LinEnum.sh

Se abre el script con el editor nano usando el comando nano LinEnum.sh. Este paso permite revisar o modificar el código del script antes de transferirlo.

5.1.15 Exploración Inicial del Sistema

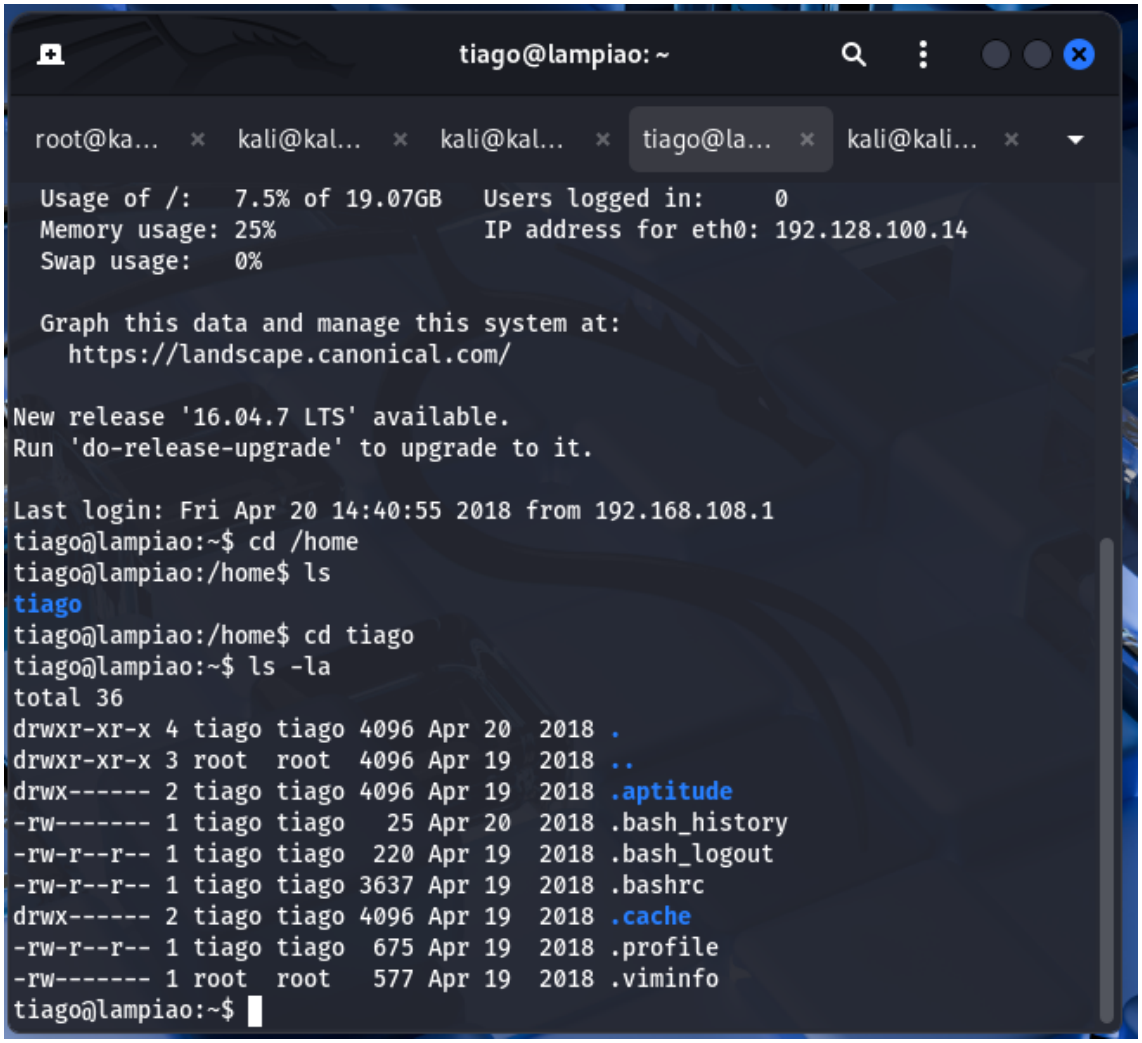

Ilustración 19. listado de directorios críticos en la máquina Lampião

Una vez establecida la sesión SSH como el usuario tiago, se inicia la exploración del sistema de archivos para entender el entorno y buscar información sensible.

El comando ls -la /home/tiago revela archivos ocultos del usuario.

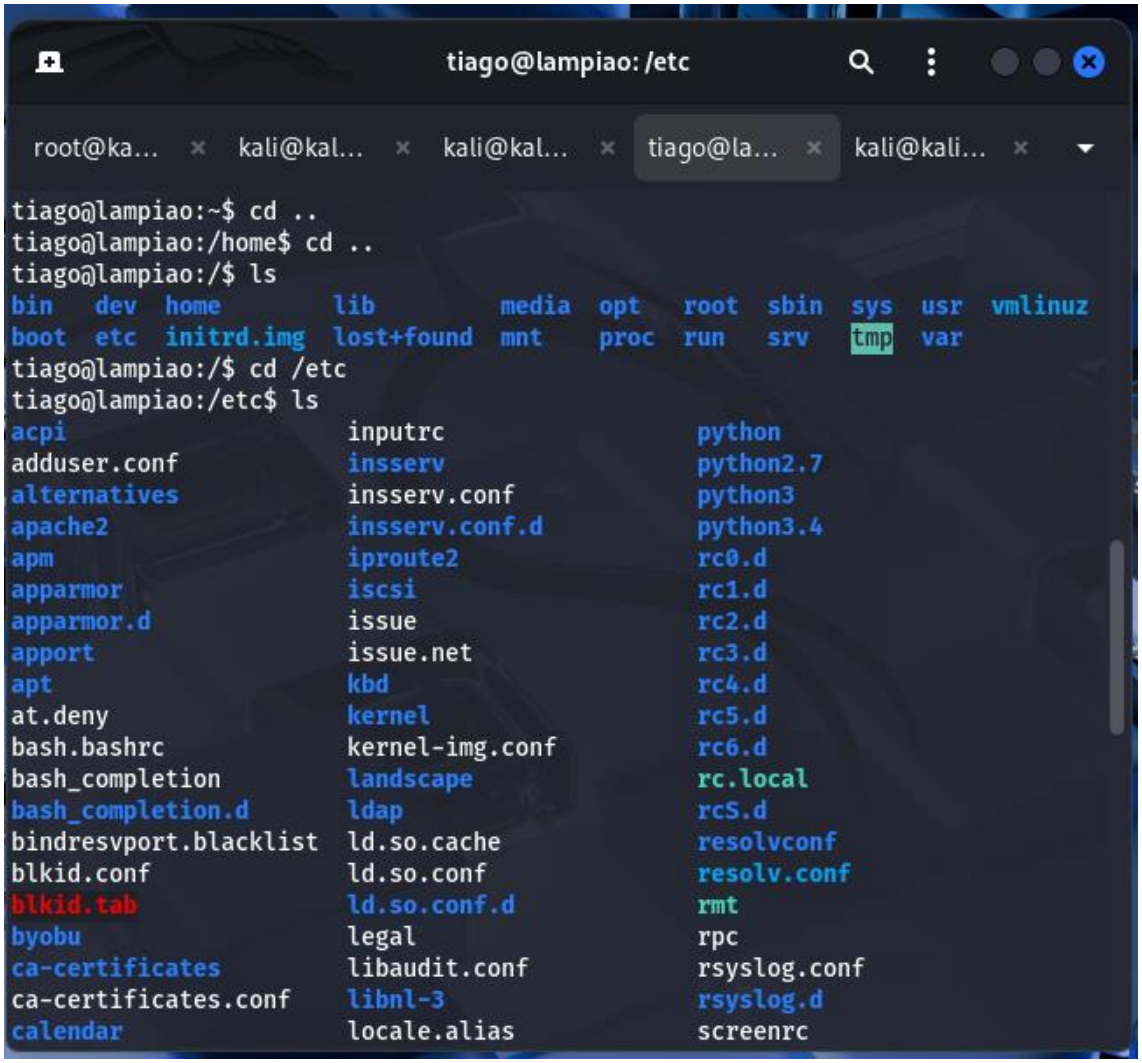

Ilustración 20. Navegación de directorios críticos en Lampião tras el acceso SSH.

Se navega hasta el directorio raíz (/) y se lista su contenido. Luego, se explora el directorio /etc, que contiene archivos de configuración del sistema y de aplicaciones (como apache2, passwd).

5.1.16 Inspección del Archivo /etc/passwd

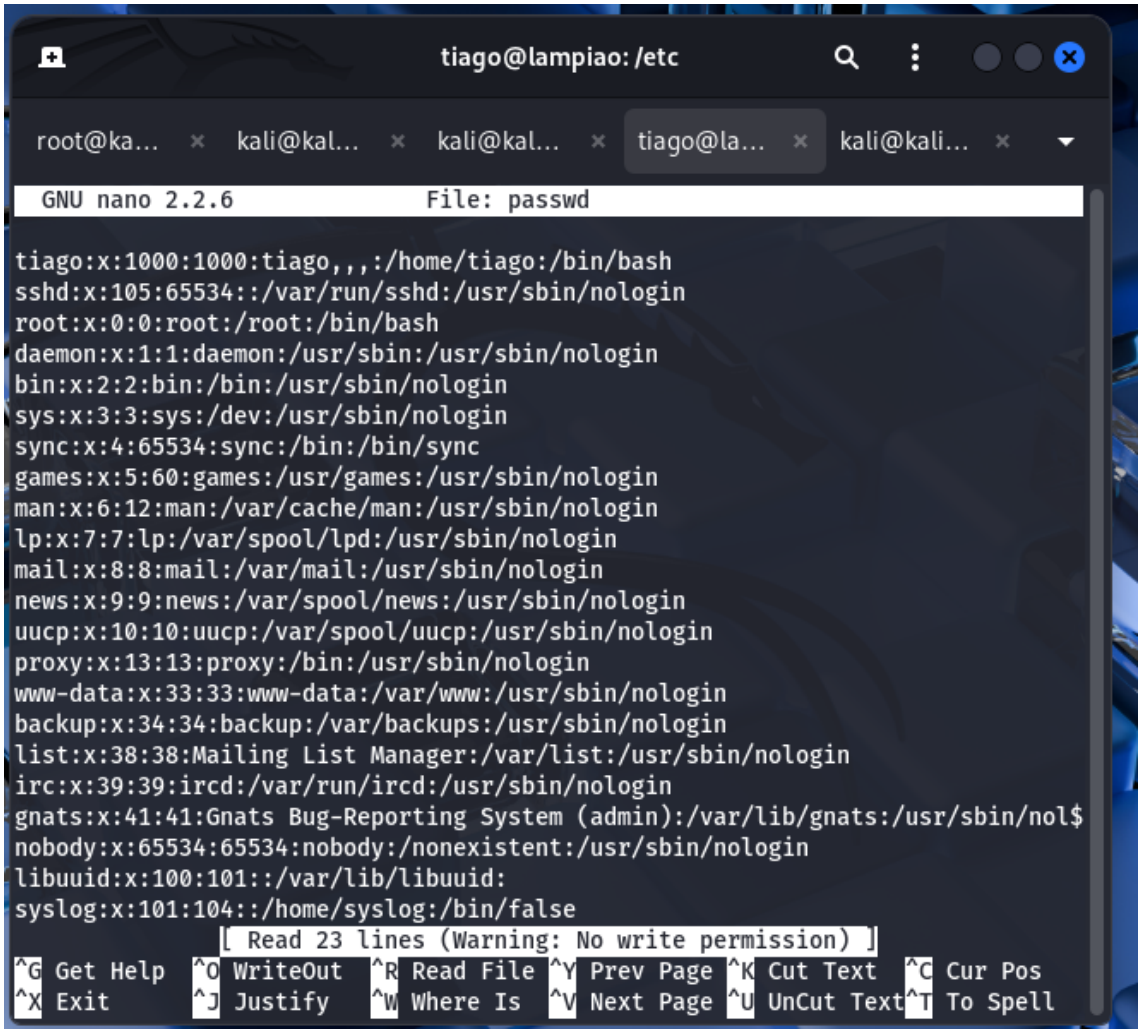

Ilustración 21. Visualización del archivo /etc/passwd

El comando nano /etc/passwd fue utilizado para visualizar su contenido. El archivo lista todos los usuarios del sistema, confirmando la existencia de las cuentas root y Tiago.

5.2.Capitulo #2

5.2.1 Descarga de un Exploit para Escalar Privilegios

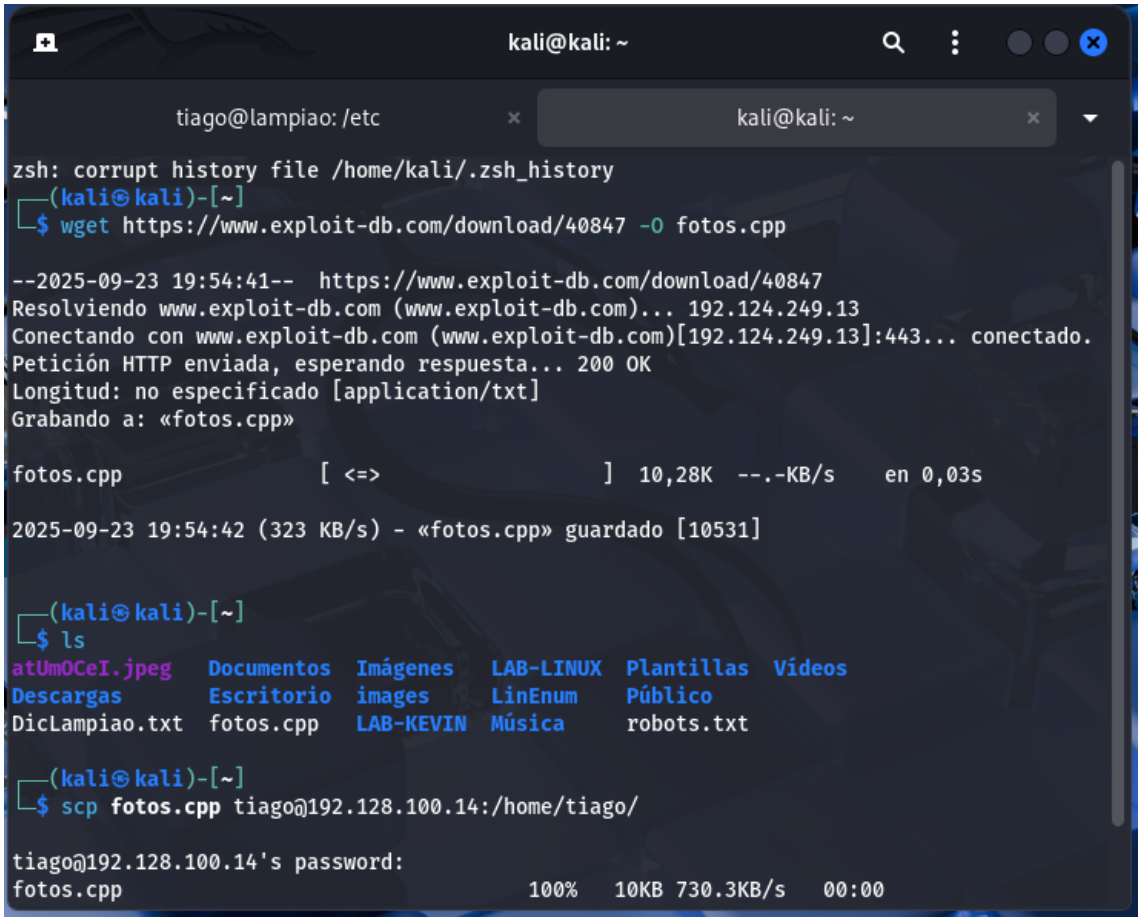

Ilustración 22. transferencia a la máquina Lampião mediante SCP.

Se utiliza wget para descargar el exploit, guardándolo localmente con el nombre fotos.cpp.

El archivo del exploit se transfiere desde la máquina Kali Linux al directorio /home/tiago/ de la máquina Lampião utilizando el comando scp , autenticándose con la contraseña del usuario Tiago.

5.2.2 Explotación Exitosa de la Vulnerabilidad

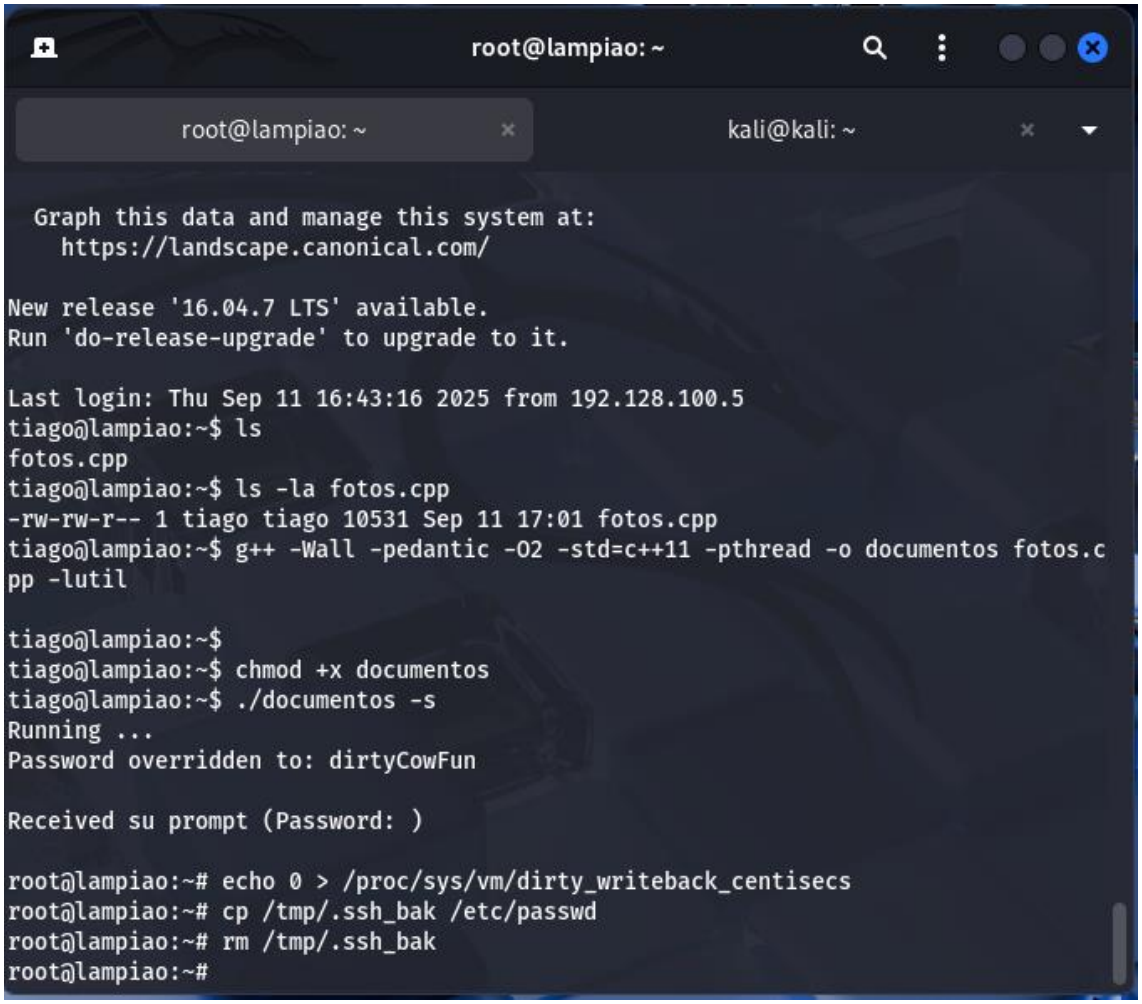

Ilustración 23. Ejecución del exploit Dirty COW y obtención de privilegios.

Esta secuencia documenta la explotación exitosa que concede acceso de root al sistema:

Compilación del Exploit: El comando g++ -Wall -pedantic -O2 -std=c++11 -pthread -o documents fotos.cpp -lutil genera un ejecutable llamado documents.

Ejecución y Escalada: Se dan permisos de ejecución (chmod +x documents) y se ejecuta el exploit (./documents).

5.2.3 Creación de Nuevos Usuarios

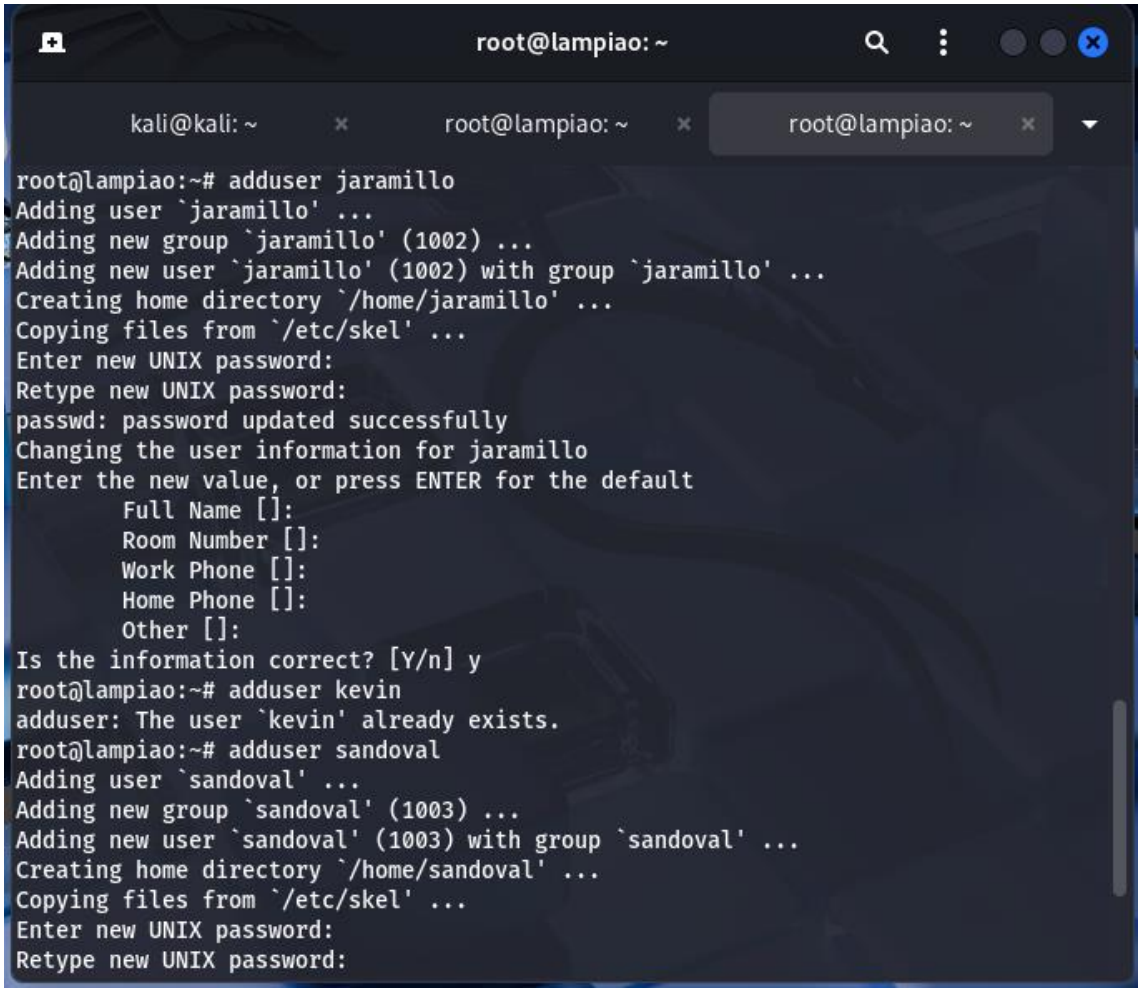

Ilustración 24. Ejecución de adduser para crear nuevas cuentas en el sistema.

Utilizando el comando adduser con los máximos privilegios, se ejecutan las siguientes acciones:

1. Creación de Usuario jaramillo: Se crea exitosamente el usuario jaramillo.
2. Creación de Usuario sandoval**:** Se crea exitosamente el usuario sandoval

5.2.4 Verificación del acceso con los nuevos usuarios

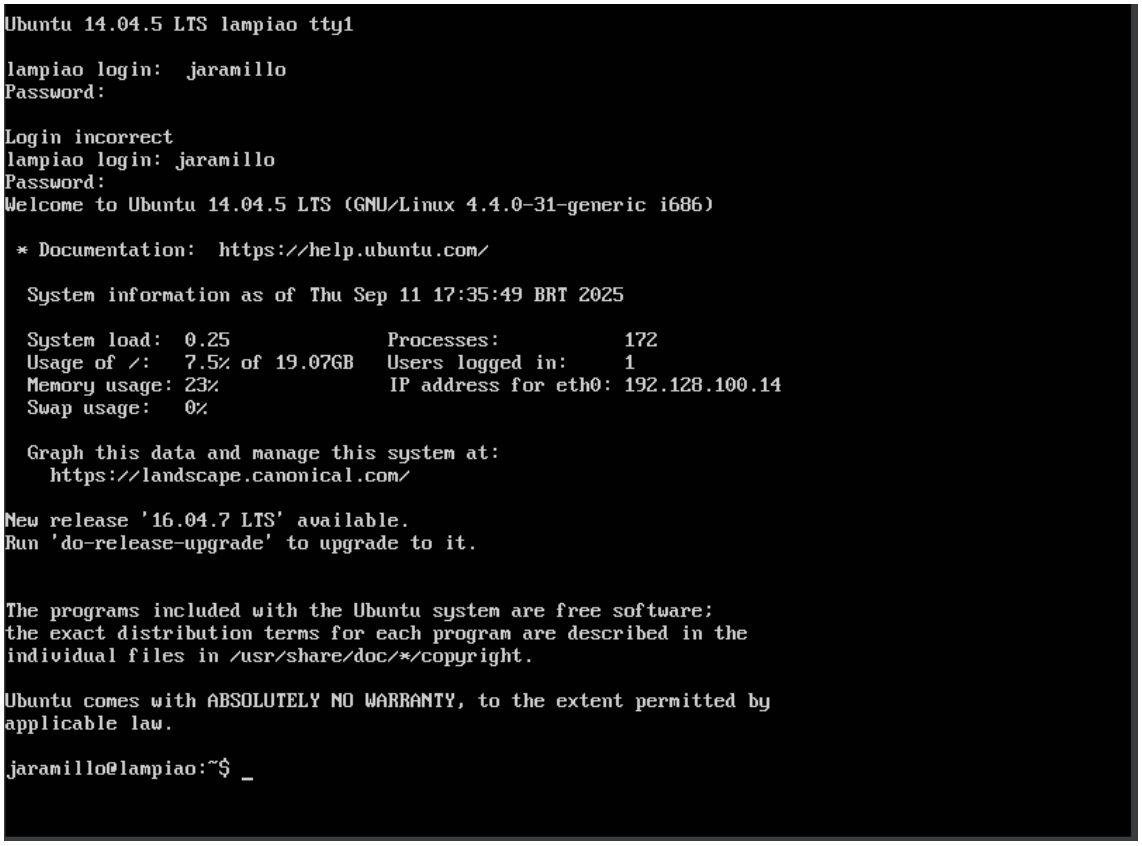

Ilustración 25. Inicio de sesión en el sistema Lampiao utilizando la cuenta jaramillo

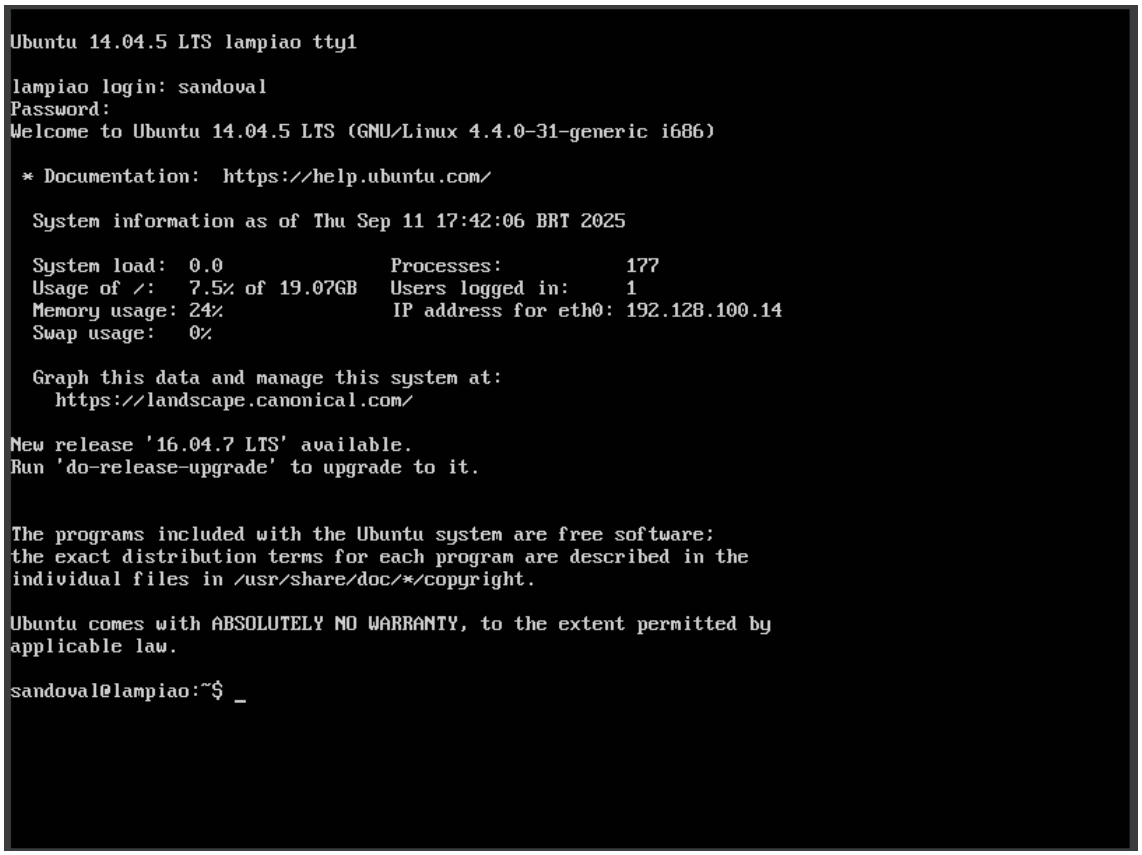

Ilustración 26. Inicio de sesión en el sistema Lampiao utilizando la cuenta Sandoval

La creación de los usuarios jaramillo y sandoval se realizó correctamente.

5.2.5 Exploración del Directorio Web

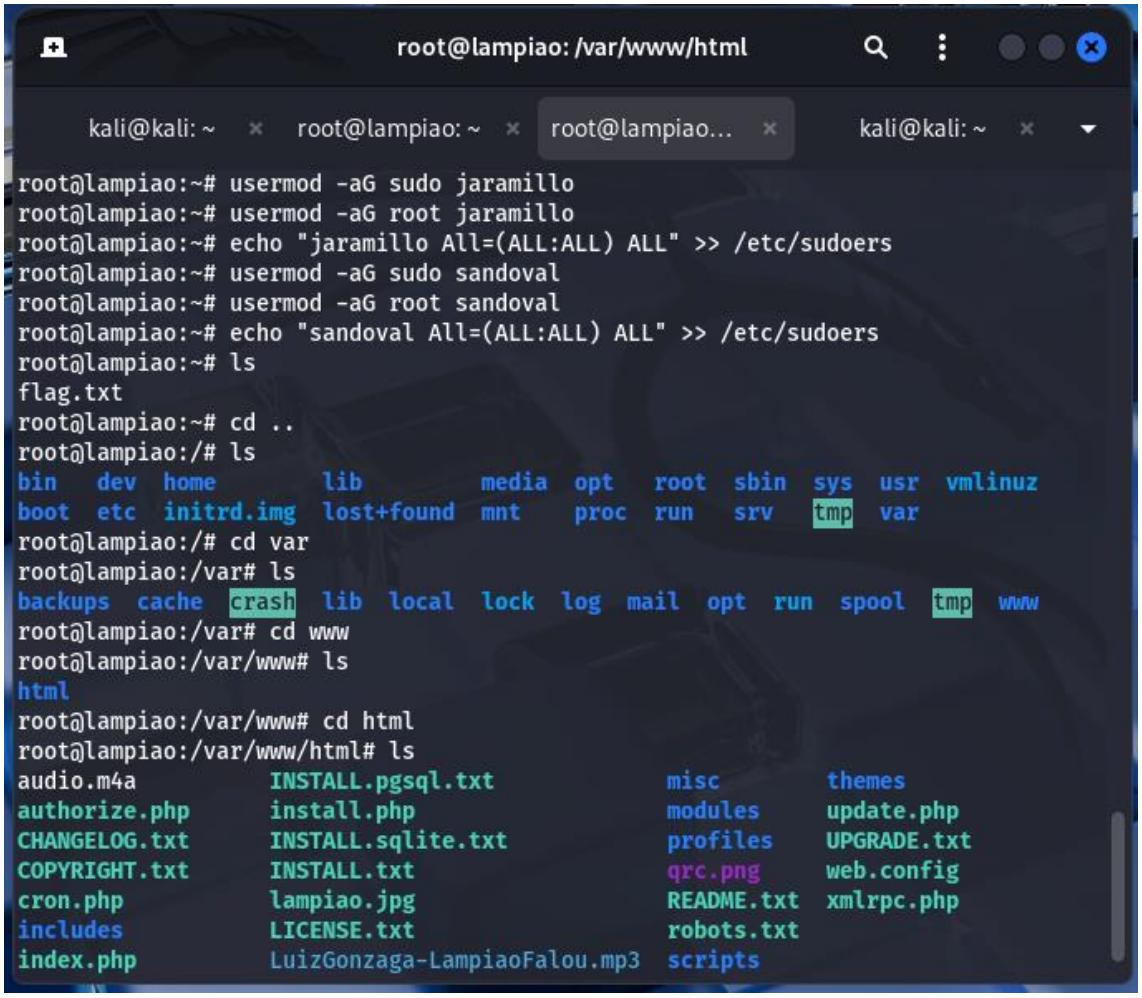

Ilustración 27. Asignación de privilegios de administrador a los nuevos usuarios

Tras obtener el acceso root y crear los nuevos usuarios, se realizan las siguientes acciones:

Escalada de privilegios para los nuevos usuarios: Se utilizan los comandos usermod y se edita el archivo /etc/sudoers para agregar a los usuarios jaramillo y sandoval a los grupos sudo y root para darles permiso

Exploración del servidor web: Se navega hasta el directorio raíz del servidor web en /var/www/html. ls revela la estructura de la aplicación Lampiao.

5.2.6 Exploración de la Base de Datos Drupal

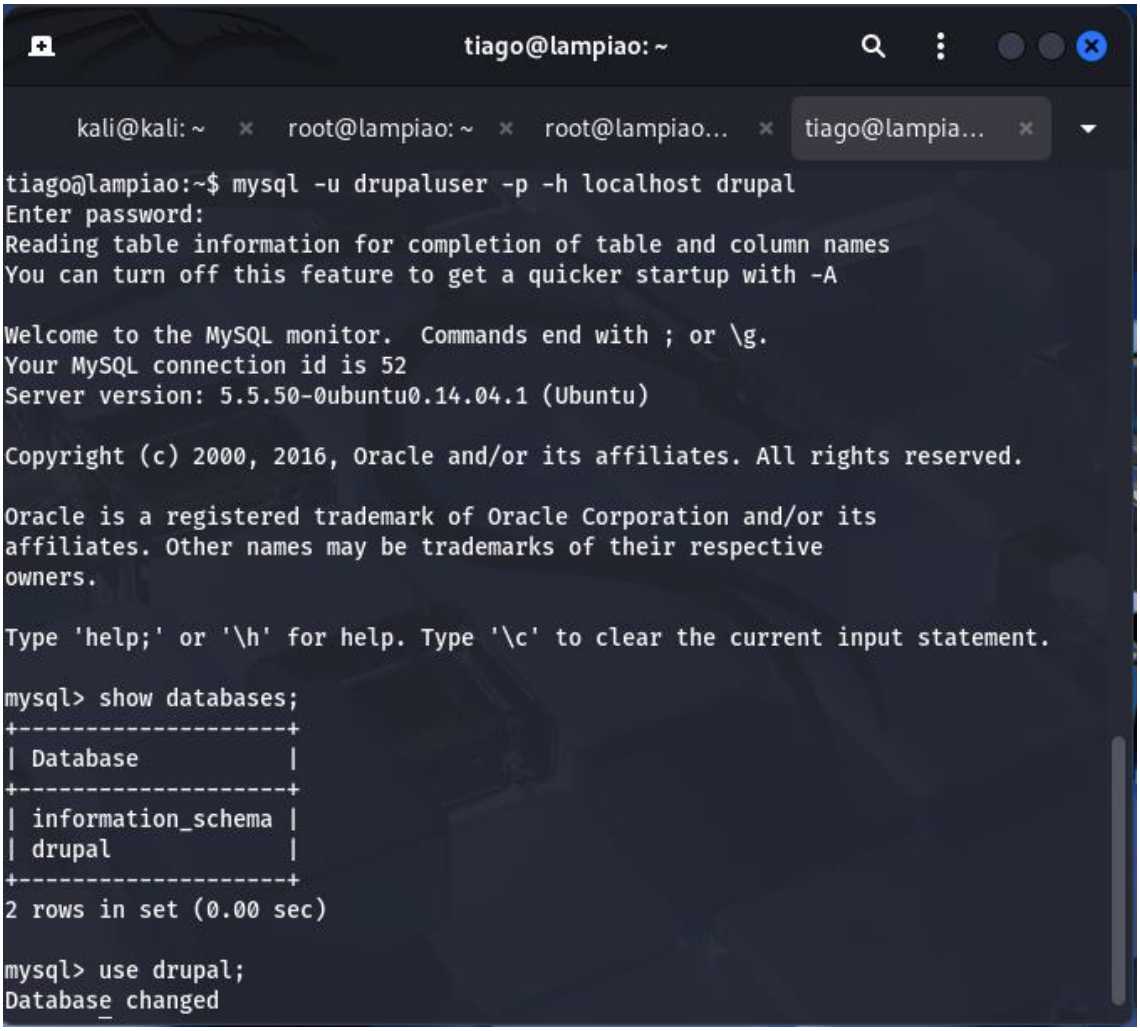

Ilustración 28. Conexión a la base de datos MySQL de Drupal y listado de sus tablas.

Desde la sesión del usuario tiago, se conecta a la base de datos drupal en el servidor local (localhost) utilizando el comando mysql -u drupaluser -p.

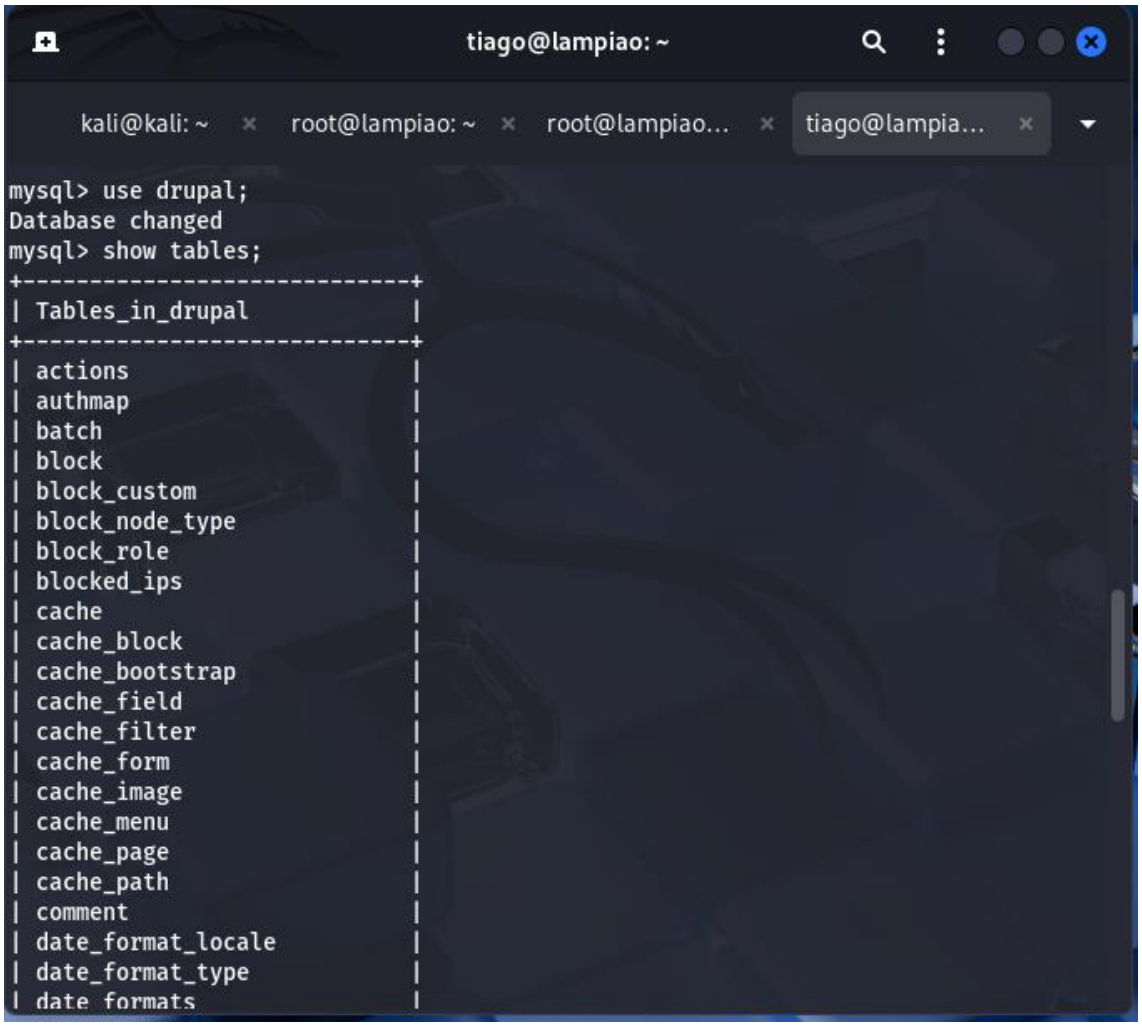

Ilustración 29. Listado de tablas de la base de datos drupal

El comando show databases; confirma la existencia de la base de datos drupal. Al seleccionarla con use drupal; y listar sus tablas (show tables;), se muestra la estructura completa de Drupal.

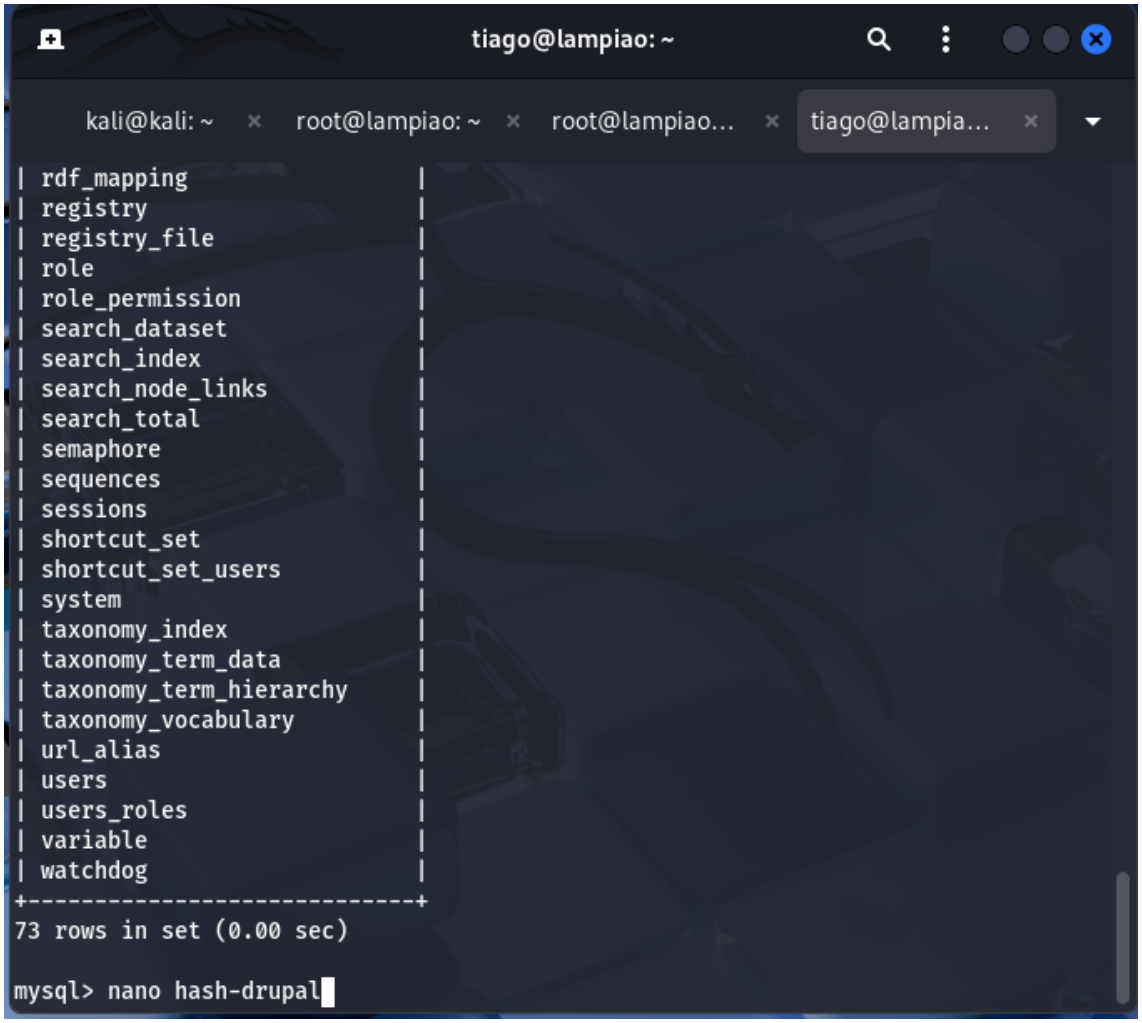

Ilustración 30. Revelación de la estructura completa de la base de datos

5.2.7 Exposición de Credenciales de la Base de Datos

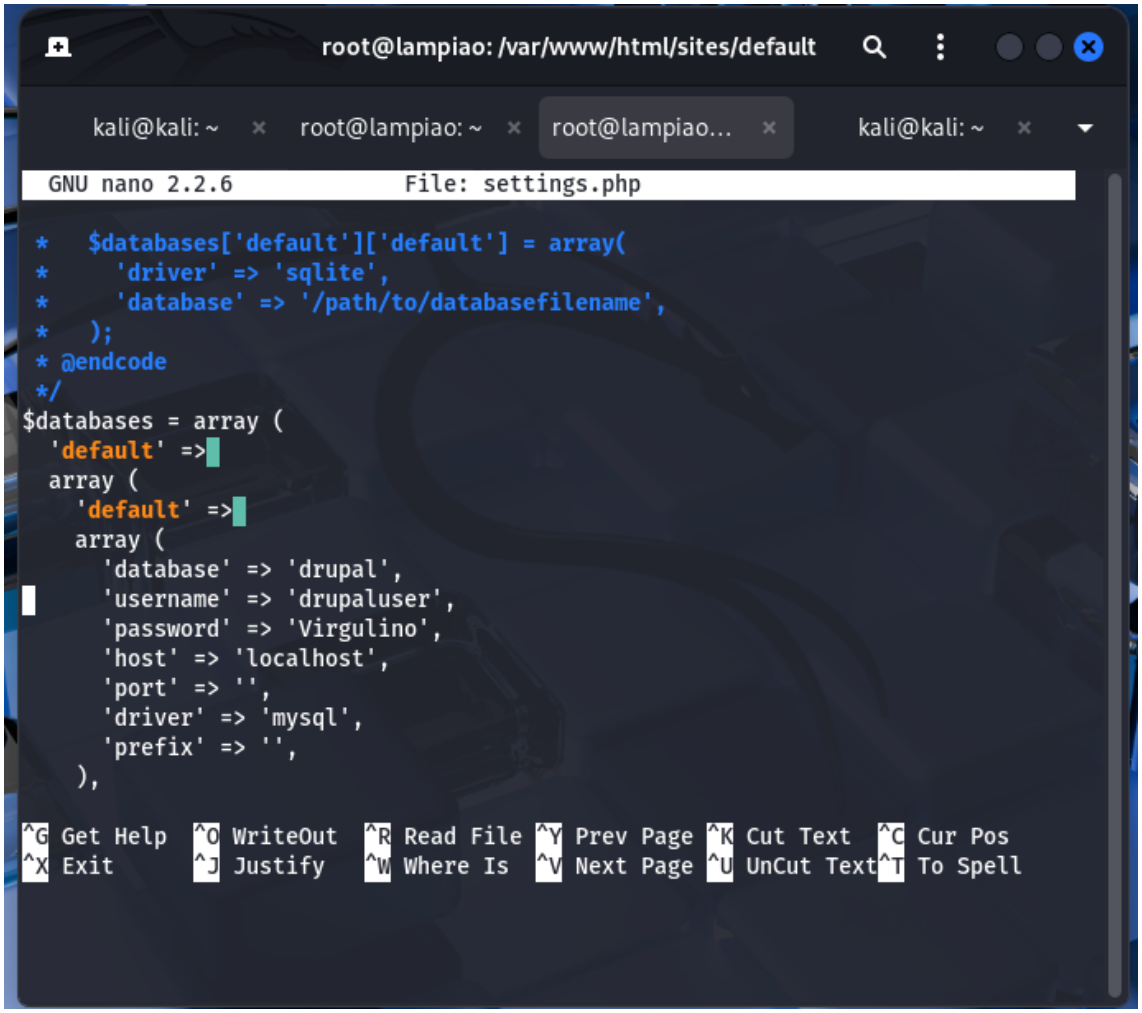

Ilustración 31. Visualización del archivo de configuración settings.php de Drupal

Esta captura revela la exposición de credenciales en el archivo de configuración. El archivo /var/www/html/sites/default/settings.php, que contiene la configuración principal de Drupal, fue abierto con el editor nano. En su contenido se observa las credenciales de acceso:

- Base de datos: drupal
- Usuario: drupaluser
- Contraseña: Virgulino
- Host: localhost

5.2.8 Generación de Hash de Contraseña

Ilustración 32. Creación de un script PHP para generar hashes compatibles con Drupal

Se muestra un script PHP phpass_hash.php que implementa el algoritmo de hash utilizado por Drupal identificado por el prefijo P.

Se ejecuta el script desde la línea de comandos con php phpass_hash.php “MiPass123”, generando el hash para la contraseña MiPass123.

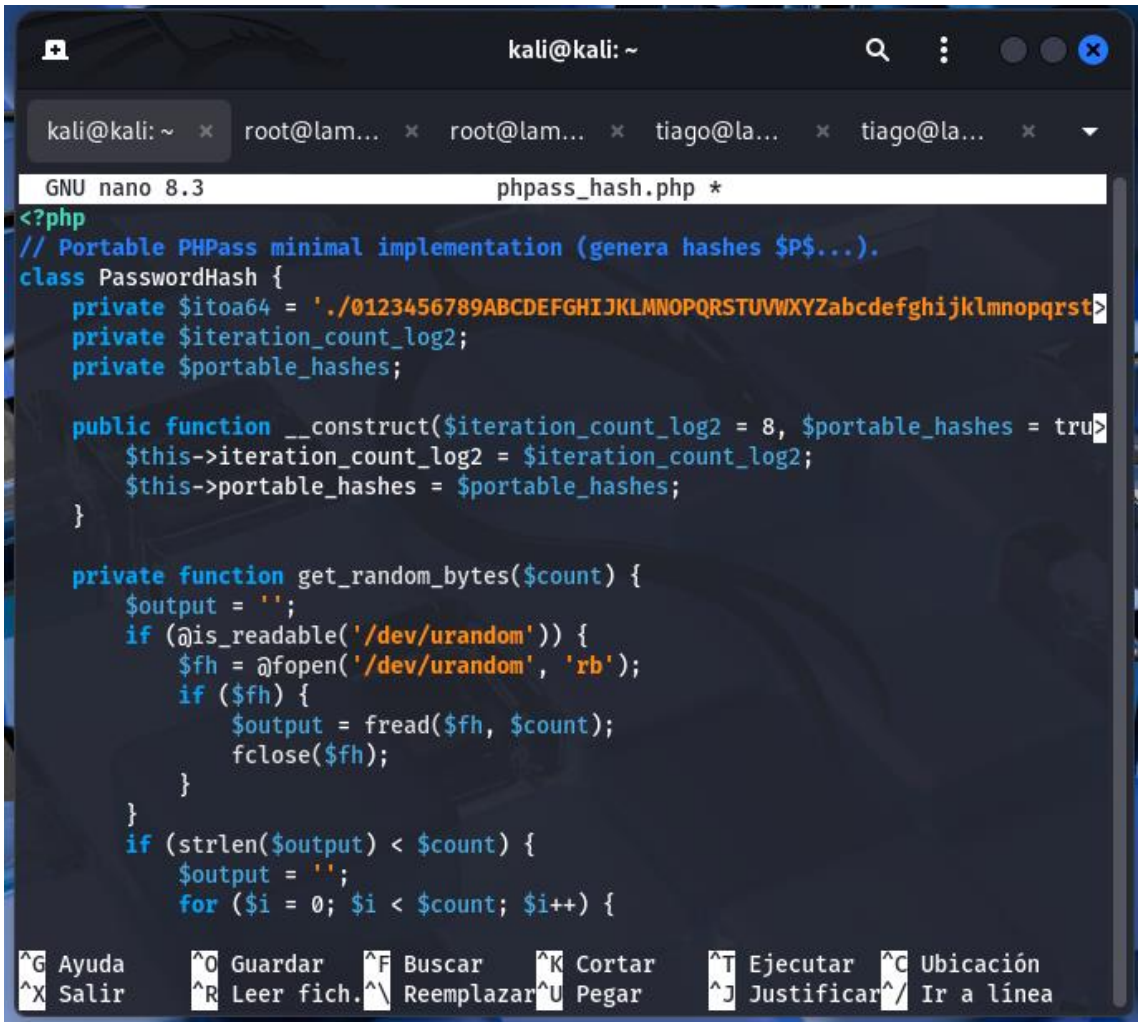

Ilustración 33. Uso de un script PHP para generar hashes compatibles con Drupal.

5.2.9 Creación de Usuarios en la Base de Datos de Drupal

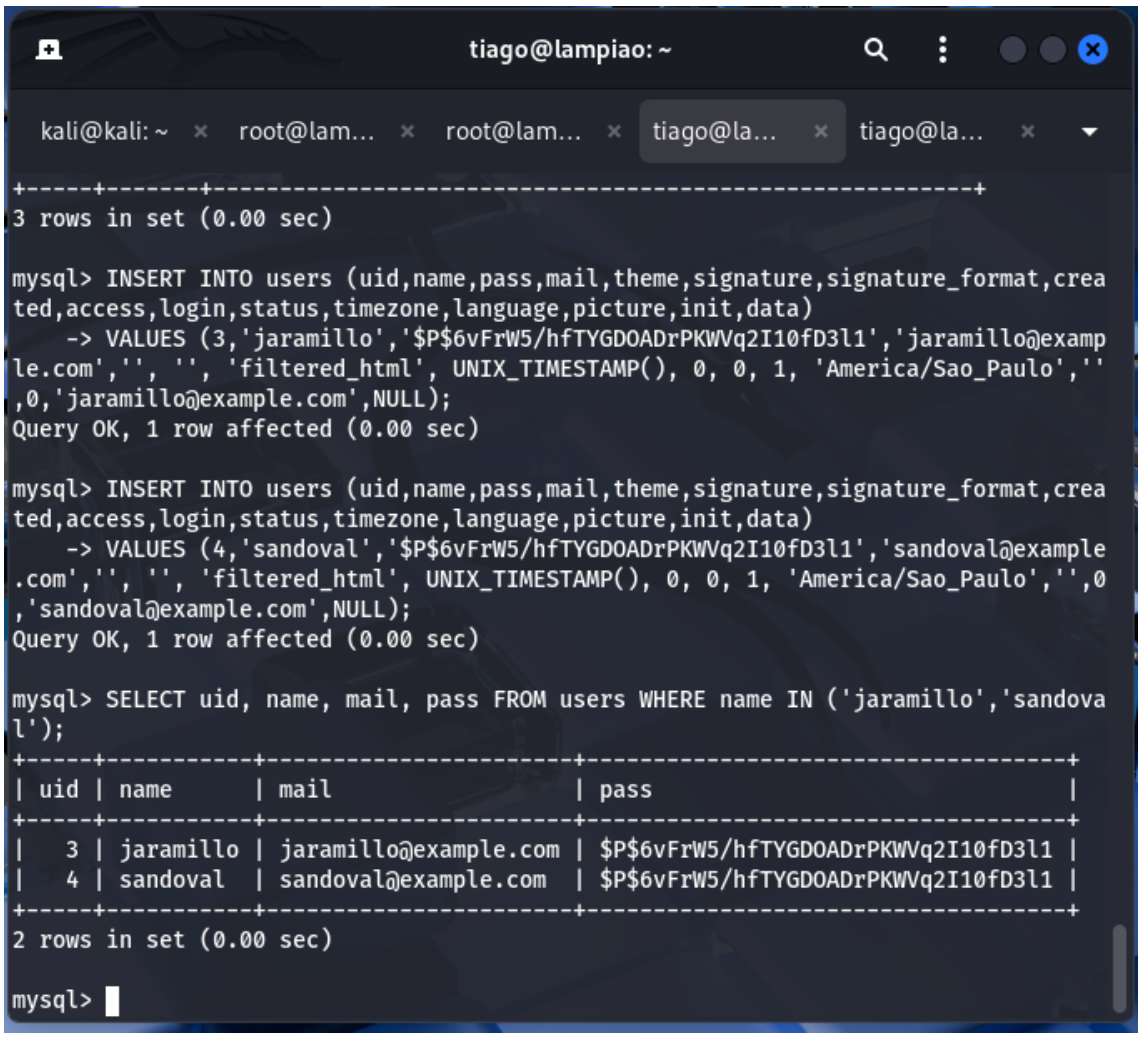

Ilustración 34. Inserción de nuevos usuarios en la tabla users de Drupal

Esta captura demuestra la explotación de la aplicación web. Utilizando el acceso a la base de datos Mysql y el hash de contraseña Drupal generado:

1. Se crean dos nuevos usuarios en la aplicación web:

   Usuario jaramillo y correo jaramillo@example.com y Usuario sandoval y

   correo sandoval@example.com

Ambos utilizan el hash mismo correspondiente a la contraseña MiPass123.

2. La consulta SELECT confirma que los usuarios fueron insertados exitosamente en la base de datos

5.2.10 Usuarios Creados en la Interfaz Web de Drupal - Lampiao

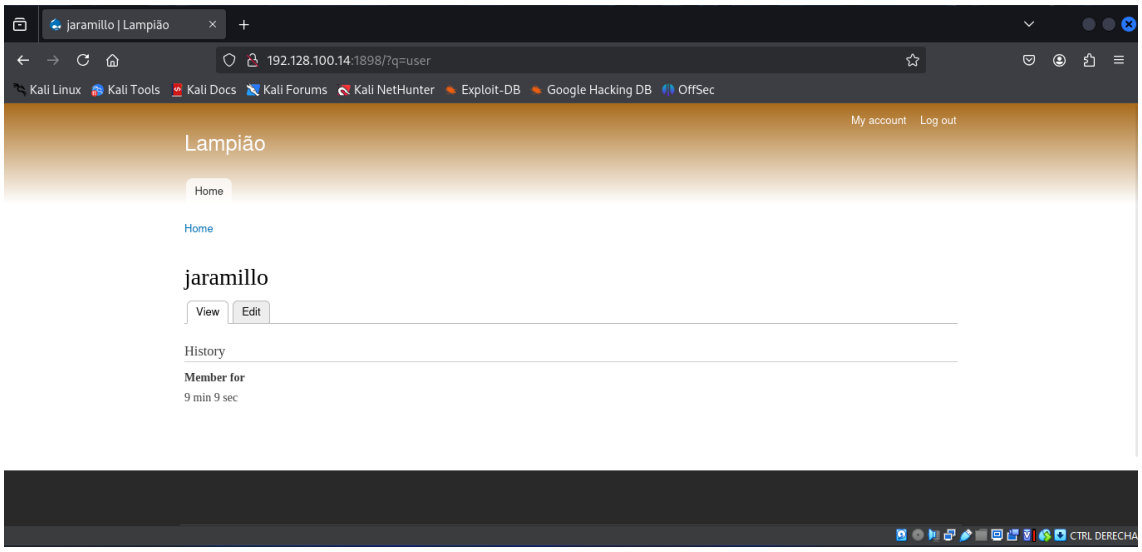

Ilustración 35. Perfil de usuarios jaramillo confirmados en la interfaz de Lampiao.

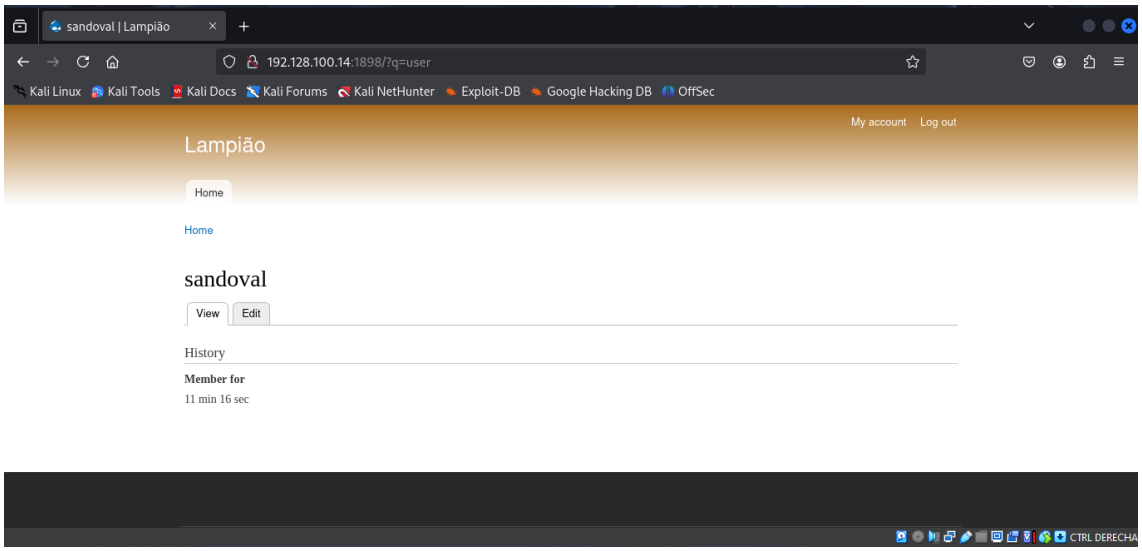

Ilustración 36. Perfil deusuario sandoval confirmados en la interfaz de Lampiao.

Estas capturas de pantalla sirven como la verificación final y concluyente del éxito de la práctica.

La interfaz muestra el nombre de usuario "jaramillo" en donde se confirma que la cuenta fue creada exitosamente.

De igual manera, se confirma la existencia del usuario "sandoval" dentro del sistema Drupal de Lampiao.

6. Problemas encontrados

- En varias ocasiones los comandos fueron escritos con parámetros mal colocados, lo que produjo respuestas de error.

- Había desconocimiento sobre la forma exacta crear los usuarios en Lampiao, lo que llevó a pruebas fallidas.

- Algunos errores no eran claros, lo que complicó identificar la causa real de algunos fallos.

- Gran parte de la práctica se fue en intentar comandos hasta hallar la forma correcta, reduciendo el tiempo para documentar el informe.

7. Recomendaciones

- Verificar sintaxis de comandos
- Anotar los comandos exitosos para replicarlos en futuros escenarios
- Probar comandos paso a paso
- leer los mensajes de error con atención

8. Conclusión

El ejercicio demostró que la teoría vista en clase necesita complemento práctico para ser realmente útil. Sin embargo, el trabajo permitió entender el proceso de explotación y reconocer qué medidas son necesarias para proteger sistemas web como Lampiao. En definitiva, fue una práctica valiosa que dejó lecciones claras sobre la metodología.

9. Bibliográfica

Rafael Sandoval Morales (2025). Hacking para la creación de nuevos usuarios en el sitio web de Lampiao desde el Kali Linux