INFORME #2 LABORATORIO DE SEGURIDAD WEB EN EL PORTAL LAMPIAO

EDWARD CAMILO CAICEDO BENITEZ

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERÍA

PROGRAMA DE INGENIERÍA DE TELECOMUNICACIÓNES E INFORMÁTICA

SEGURIDAD Y AUDITORIAS EN REDES

DOCENTE

RAFAEL SANDOVAL MORALES

QUIBDÓ-CHOCÓ-COLOMBIA

2025

Tabla de contenido

TABLA DE ILUSTRACIONES....3
INTRODUCCIÓN....5
OBJETIVOS....5
Objetivo general....5
Objetivos específicos....5
PLANTEAMIENTO DEL PROBLEMA....6
EXPLOTACIÓN DE LA PÁGINA DE LAMP DESDE KALI LINUX....7
INTALACION DE LAMPIAO....7
Ingresamos por ssh e ingresamos la contraseña de Virgulino....16
Crear dos usuarios....20
Resultados....25
Resultados obtenidos:....26
Posibles causas del fallo:....26
CONCLUCIÓN....28
REFERENCIA BIBLIOGRÁFICA....29

TABLA DE ILUSTRACIONES

1. Importación de lampio desde VirtualBox 7

2. Seleccionado el archivo lampio 8

3. Archivo de lampio seleccionado 8

4. Lampio creado 9

5. Escaneo del segmento de red nat 9

6. Resultados del escaneo de servicios 10

7. Ip de Kali Linux con ifconfig 10

8. Escaneo de puertos 1–2000 en Lampiao 11

9. Accediendo al servicio web 11

10. Portal web de Lampião en el puerto 1898 12

11. Error al intentar crear un usuario 13

12. Escaneo Puerto 22 SSH 13

13. generar diccionario 14

14. contar palabras diccionario 14

15. mostrar contenido diccionario 15

16. herramienta hydra 15

17. ssh login 16

18. buscar linenum 17

19. GitHub linenum 17

20. clonar linenum 18

21. abrir script linenum 18

22. intentar sudo 19

23. explorar home var 19

24ver passwd nnano 20

25. settings php 21

26. Ingreso a MySQL con el usuario drupaluser 21

27. Visualizando las bases de datos existentes 22

28. Consulta de usuarios en la base de datos 22

29. Comprobando el identificador máximo de usuarios 23

30. Inserción de nuevos usuarios en la base de datos 23

31. Nuevo identificador máximo de usuarios 24

32. Asignación de roles a los usuarios creados 24

33. Fallo de inicio de sesión con el usuario admin1 25

34. Fallo de inicio de sesión con el usuario admin2 26

INTRODUCCIÓN

En el presente trabajo se documenta el proceso de análisis y explotación de un entorno controlado con el objetivo de identificar vulnerabilidades en un portal web basado en Drupal, conocido como Lampião. Para ello se siguieron diferentes fases, comenzando con el reconocimiento de servicios, acceso a la base de datos MySQL y manipulación de registros internos para intentar generar usuarios administradores. A través de este proceso se buscó comprender cómo un atacante podría aprovechar configuraciones débiles o fallas en la gestión de credenciales, además de poner en práctica técnicas de auditoría de seguridad en un escenario realista.

OBJETIVOS

Objetivo general

Analizar y documentar las vulnerabilidades presentes en el portal web Lampião, evaluando los riesgos que pueden surgir a partir de configuraciones inseguras y accesos indebidos a la base de datos, con el fin de aplicar conocimientos prácticos de seguridad informática.

Objetivos específicos

1. Realizar un reconocimiento de los servicios expuestos en la máquina víctima.
2. Acceder a la base de datos MySQL y analizar su estructura para localizar información sensible.
3. Intentar la creación y manipulación de cuentas de usuario con privilegios de administrador.
4. Evaluar las respuestas del sistema frente a los intentos de autenticación en el portal Lampião.

5. Identificar las posibles causas por las que los accesos creados en la base de datos no fueron reconocidos por el sistema web.

PLANTEAMIENTO DEL PROBLEMA

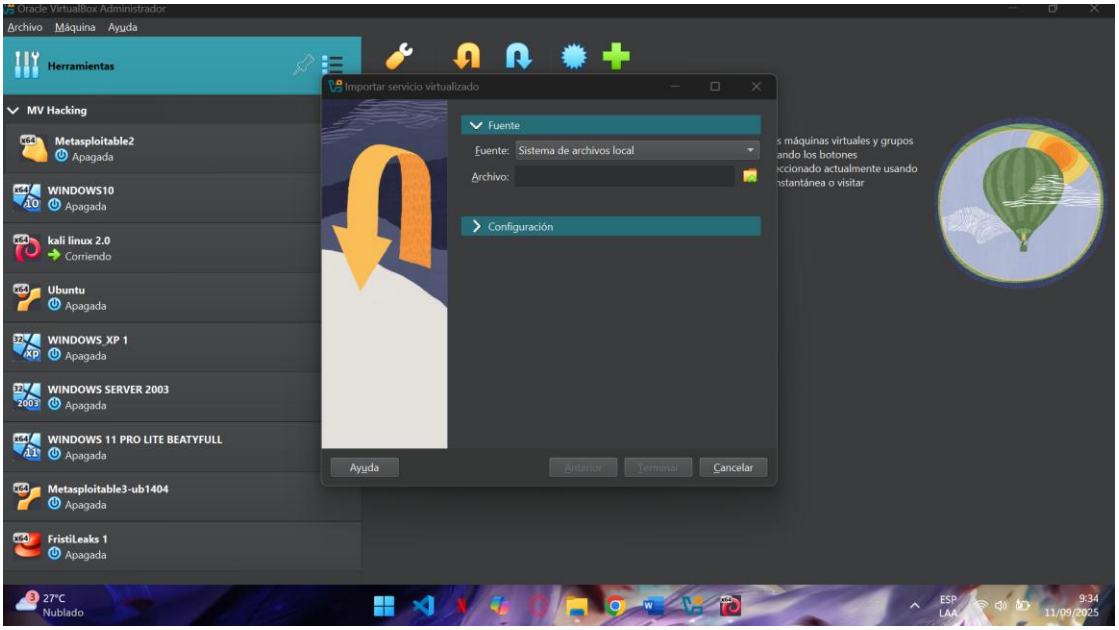
El portal Lampião expone servicios en distintos puertos que podrían contener información sensible o ser utilizados como vectores de ataque. Durante el proceso, se detectó que la base de datos almacenaba usuarios y contraseñas en formato cifrado, lo cual dio la posibilidad de crear cuentas de manera directa desde MySQL. Sin embargo, al intentar iniciar sesión en el portal con esas credenciales, el acceso fue denegado.

Esto plantea un problema de doble naturaleza: por un lado, la exposición de la base de datos representa un riesgo considerable, ya que permite manipular información interna sin pasar por los controles del sistema. Por otro lado, la imposibilidad de autenticar los usuarios creados sugiere que el CMS utiliza un mecanismo de validación adicional que no depende únicamente de los registros en la tabla de usuarios.

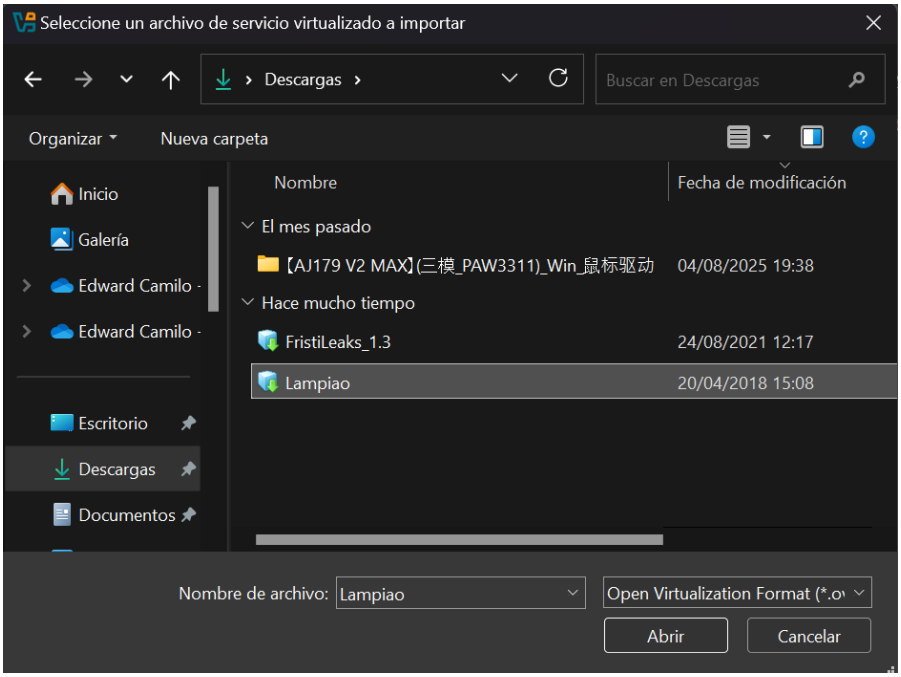
EXPLOTACIÓN DE LA PÁGINA DE LAMP DESDE KALI LINUX

INTALACION DE LAMPIAO

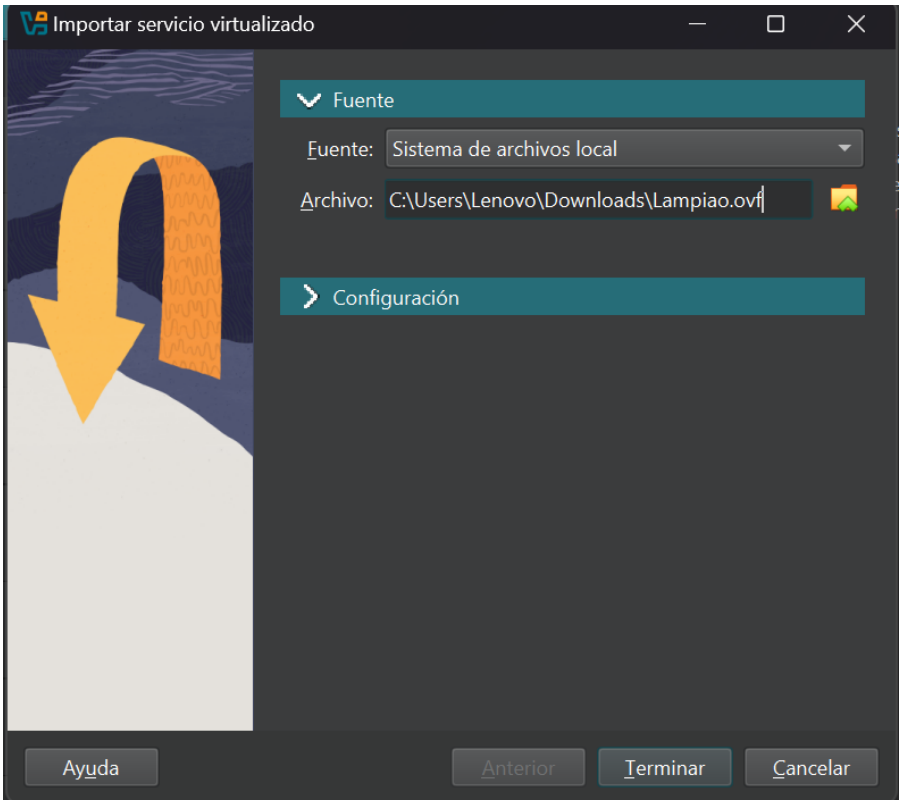
Paso 1: En este primer paso abrí el programa de Oracle VirtualBox y fui a la opción de importar un servicio virtualizado. Esta parte es fundamental porque me permite cargar máquinas virtuales ya creadas en otros entornos, sin tener que instalarlas desde cero. Aquí seleccioné que el archivo lo iba a traer desde el sistema de archivos local, es decir, desde mi propio computador.



1. Importación de lampio desde VirtualBox



2. Seleccionado el archivo lampio

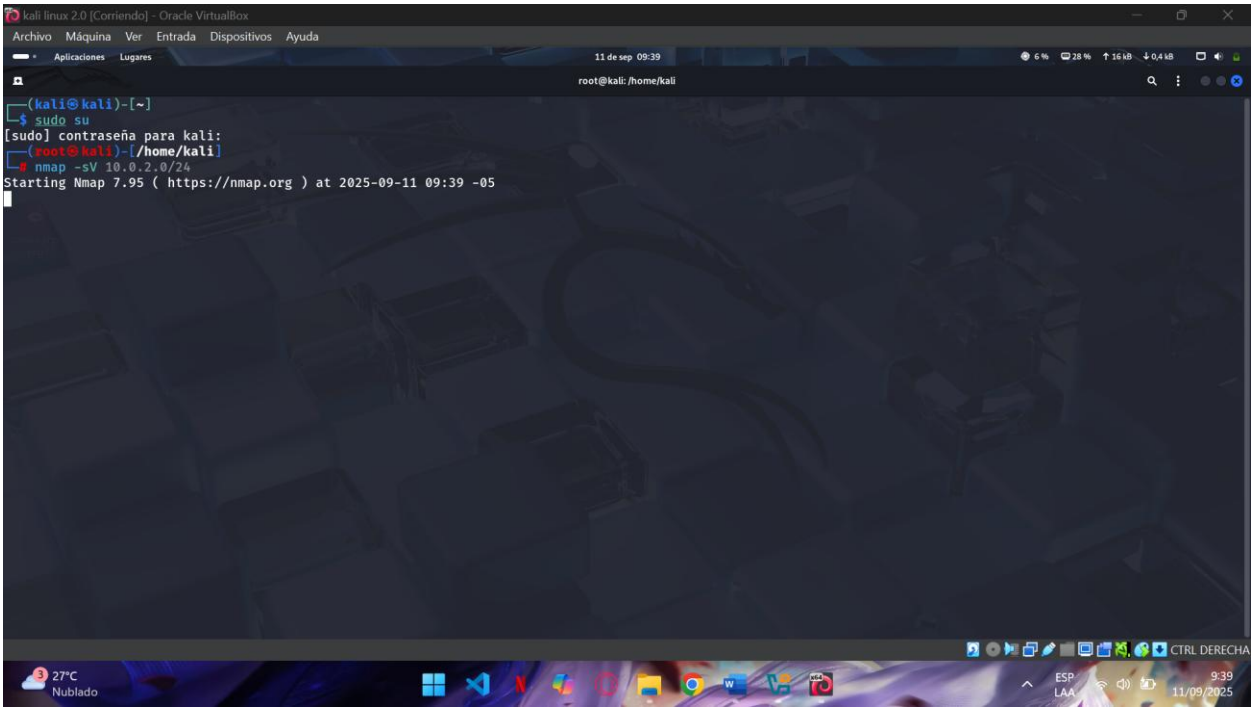


3. Archivo de lampio seleccionado

4. Lampio creado

Paso 2: En este paso utilicé **Kali Linux** para escanear la red y verificar qué dirección IP le fue asignada a la máquina virtual *Lampiao*. Para esto ejecuté el comando nmap -sV 10.0.2.0/24, el cual permite descubrir los equipos activos dentro del rango de red y los servicios que tienen abiertos. Este escaneo es clave porque me da el punto de partida para interactuar con la máquina que quiero analizar.

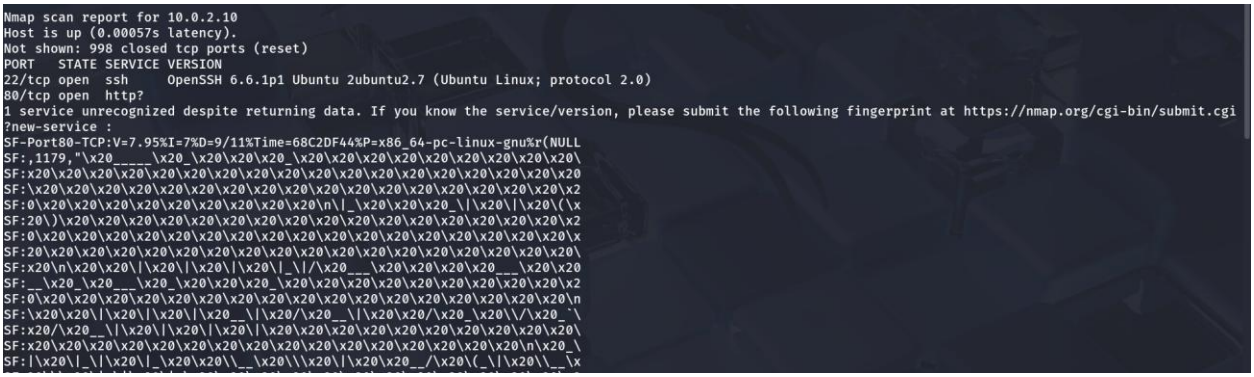
Escaneamos la red para saber que ip cogió lampio



5. Escaneo del segmento de red nat

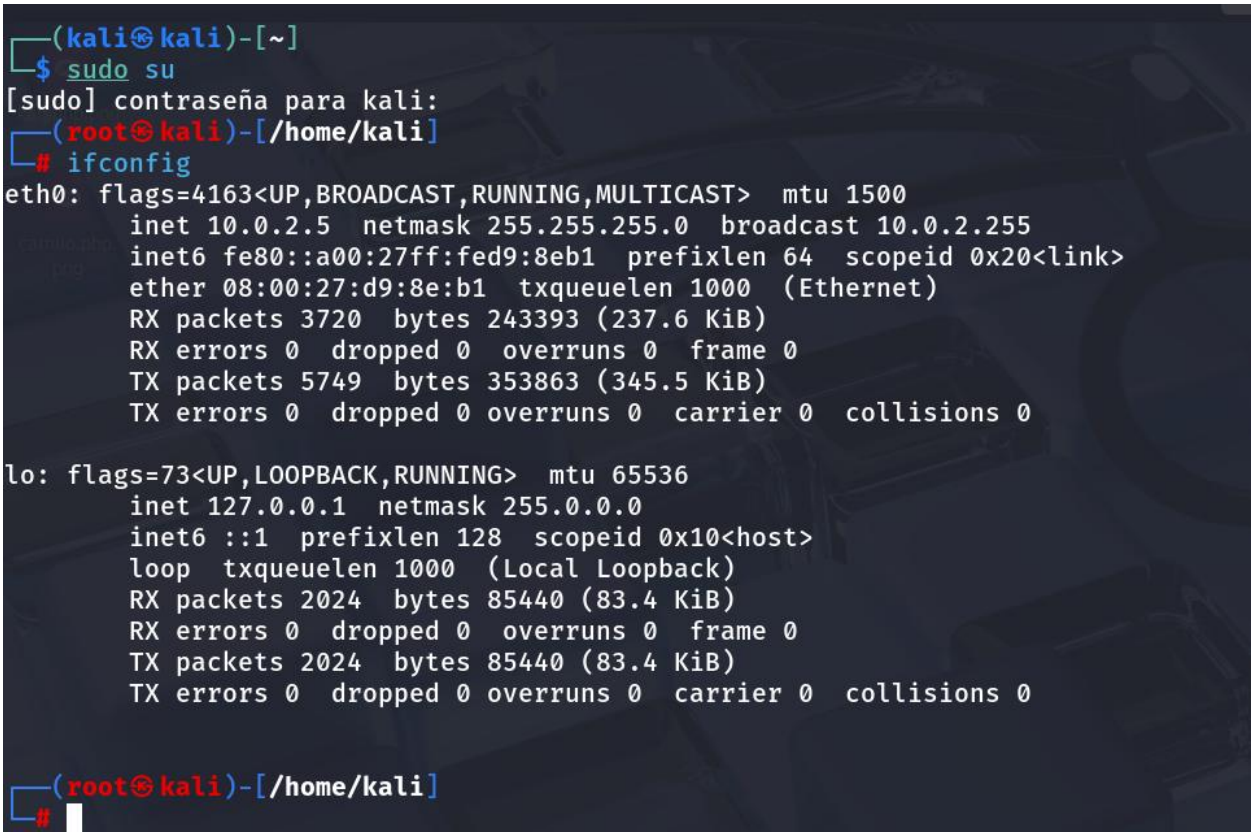
Aquí observamos el resultado del escaneo con **Nmap**. Se detectó que la máquina *Lampiao* tiene activos los puertos **22 (SSH)** y **80 (HTTP)**. El primero permite conexiones remotas seguras y el segundo corresponde a un servidor web. Estos datos son muy importantes porque indican por

dónde podemos empezar a explorar la máquina, ya sea revisando el servicio web o intentando conexiones remotas: Ip victima 10.0.2.10



6. Resultados del escaneo de servicios

ip atacante 10.0.2.5



7. Ip de Kali Linux con ifconfig

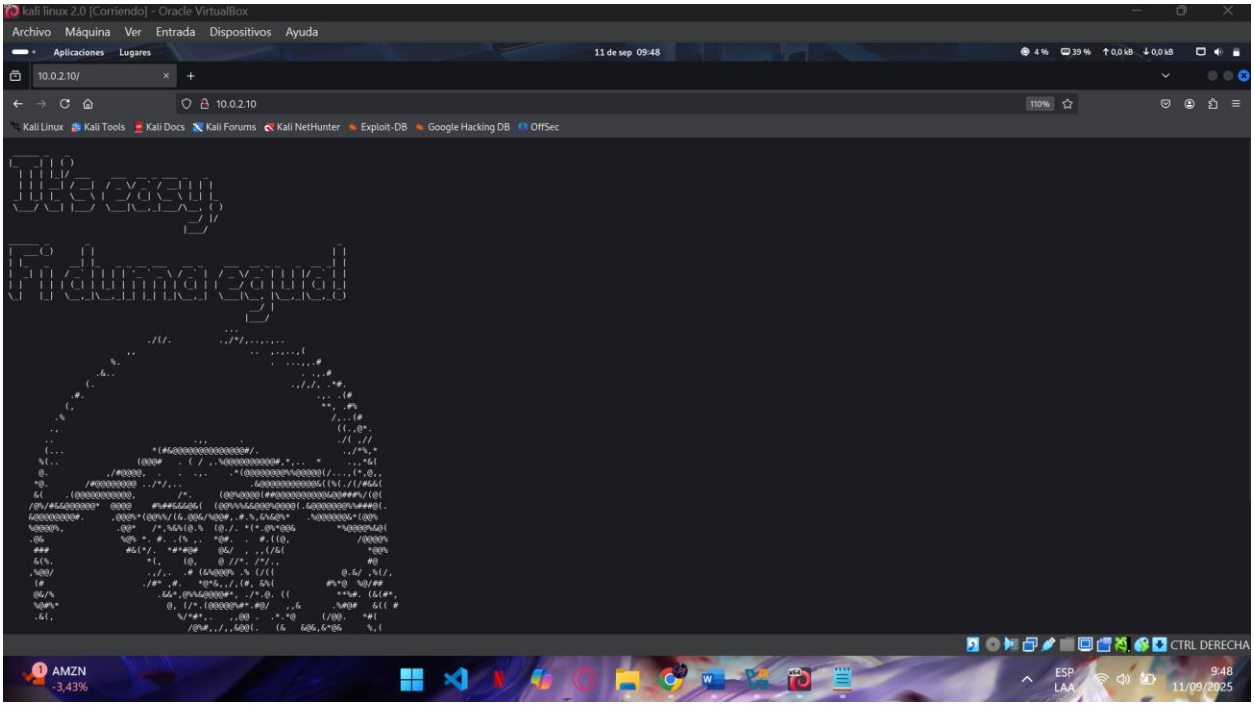
Paso 3: Ejecuté un escaneo más profundo sobre la IP de **Lampiao (10.0.2.10)** usando nmap -p 1-2000 10.0.2.10 para revisar los primeros 2000 puertos TCP. Con esto quería confirmar qué

servicios adicionales estaban escuchando y no quedarme sólo con el escaneo rápido anterior. El resultado mostró nuevamente los puertos **22 (SSH)** y **80 (HTTP)** abiertos, y además apareció el puerto **1898** (etiquetado como cymtec-port), lo que me llamó la atención porque es un servicio menos común: Escaneo de 2000 puerto de lampio ip 10.0.2.10

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 1-2000 10.0.2.10
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-11 09:46 -05
Nmap scan report for 10.0.2.10
Host is up (0.00086s 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: 08:00:27:16:C8:06 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.09 seconds
```

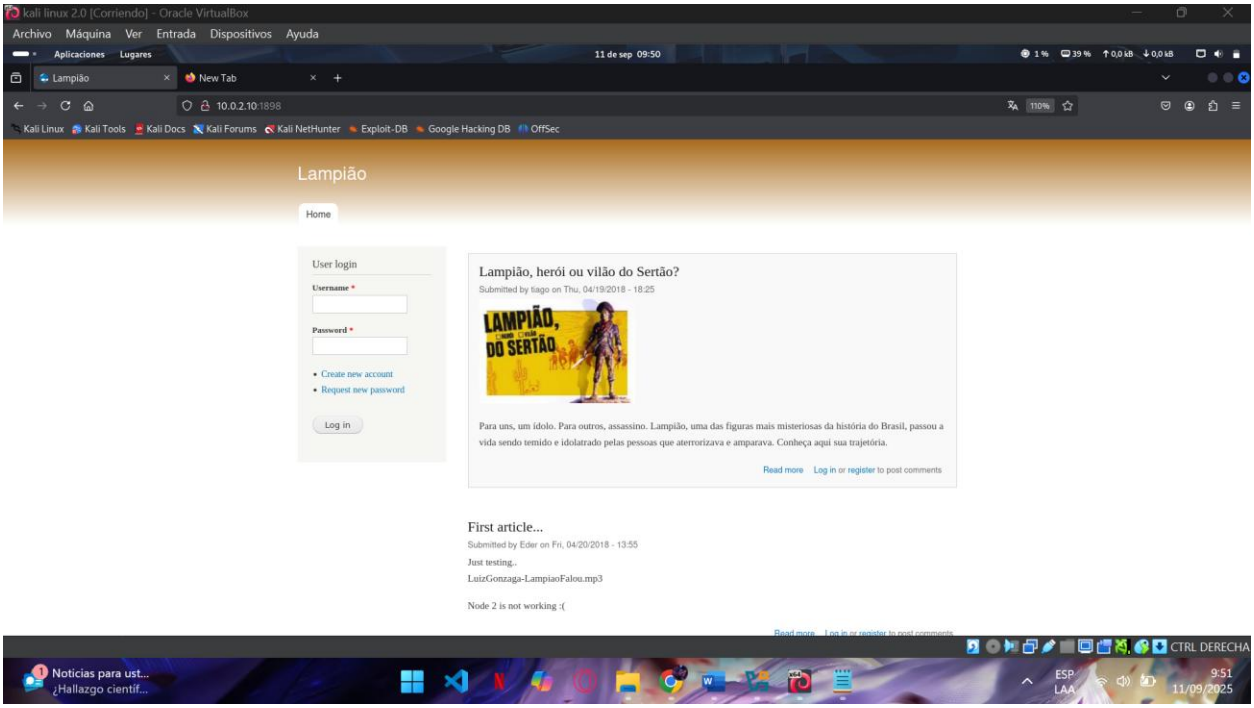
8. Escaneo de puertos 1–2000 en Lampiao

Paso 4: Vamos a vulnerar a página de lampio abrimos el navegador y entré a la dirección **10.0.2.10** en el puerto 80. ¡Allí encontré una página que mostraba un mensaje en ASCII art que decía “It’s easy, Fidu maceguad!”. Esta primera vista me confirmó que el servidor web estaba en funcionamiento y que podría haber pistas escondidas dentro de la página.



9. Accediendo al servicio web

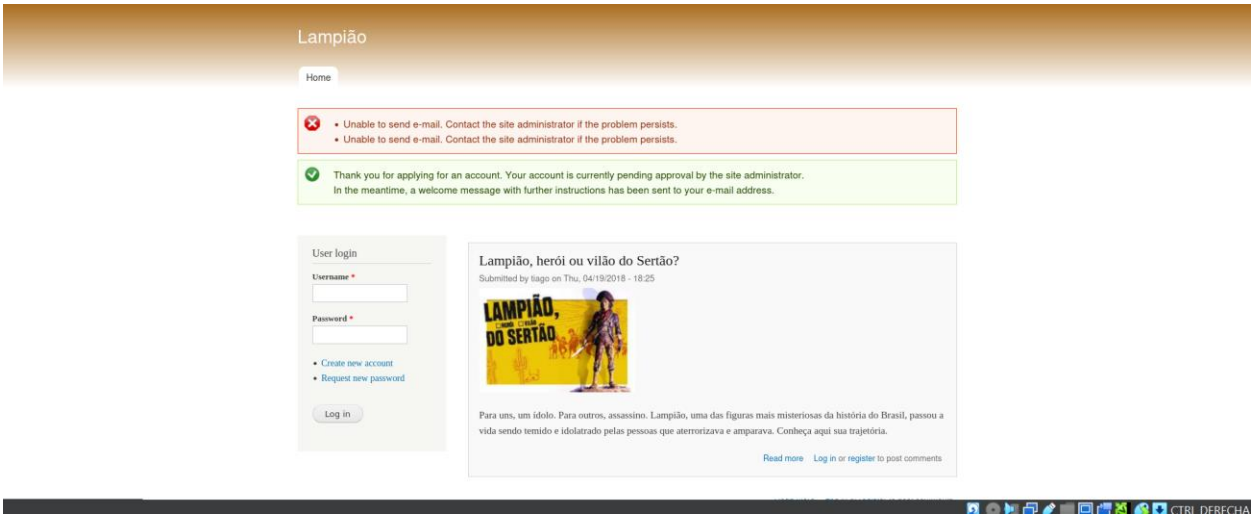
Después probé con el puerto **1898**, que había aparecido en el escaneo anterior. Al acceder, me encontré con una aplicación web llamada **Lampião**, la cual mostraba un portal con opción de inicio de sesión y registro de usuarios. También había artículos publicados con información histórica sobre Lampião. Esto me indicó que la máquina no solo tiene servicios abiertos, sino que además cuenta con un sistema de gestión de contenido donde probablemente se puedan explotar vulnerabilidades.



10. Portal web de Lampião en el puerto 1898

Intenté crear una cuenta nueva dentro del portal de Lampião, pero el sistema arrojó un error al momento de enviar el correo de validación. Aunque el registro parecía haberse enviado, realmente quedó pendiente de aprobación por parte del administrador y no me permitió acceder directamente. Esto me mostró que la opción de crear un usuario no era viable en este momento, por lo que tendría que buscar otro método para ingresar.

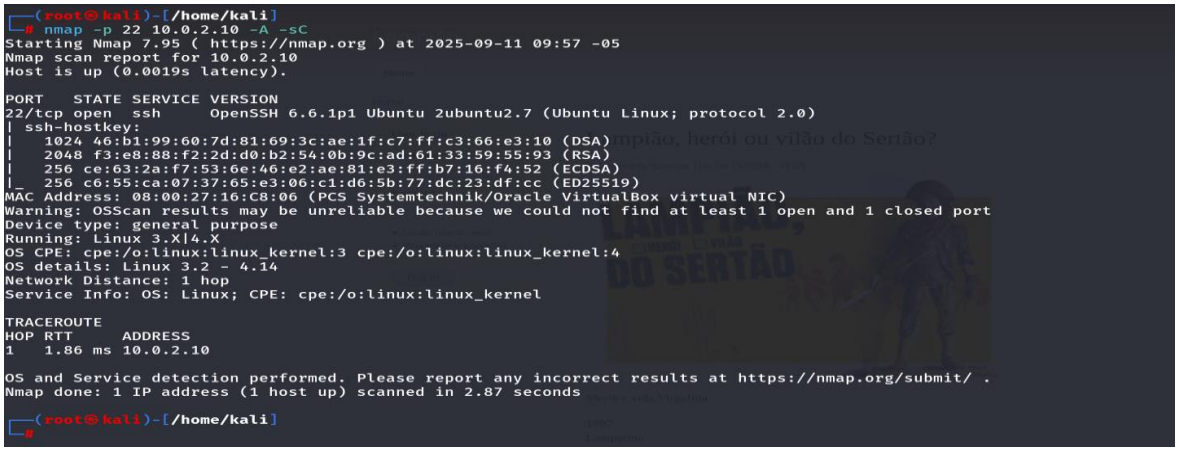
No deja crear usuario



11. Error al intentar crear un usuario

Paso 5: En este paso hice un escaneo al equipo 10.0.2.10 enfocándome en el puerto 22, que es el que se usa normalmente para entrar por SSH. El resultado me mostró que ese puerto está **abierto** y que el servicio SSH está funcionando (es decir, se puede intentar una conexión remota al equipo).

También aparecen las "huellas" de las claves públicas que el servidor muestra al conectarse, y la dirección de hardware detectada sugiere que la máquina es una **máquina virtual** (probablemente VirtualBox). Finalmente, la herramienta asoció el sistema con Linux.



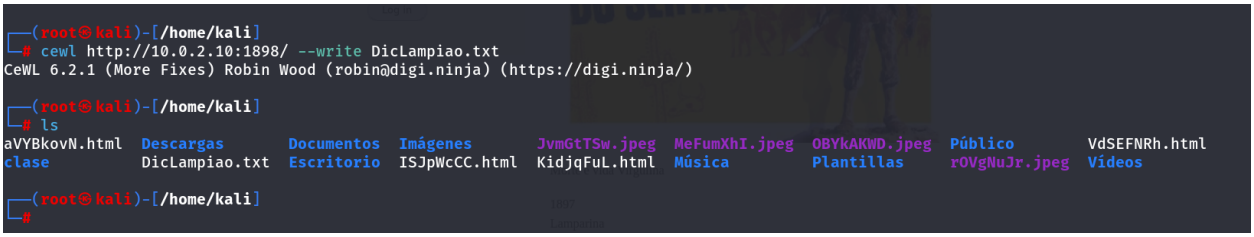
12. Escaneo Puerto 22 SSH

Paso 6: Para crear diccionario utilicé la herramienta **CeWL** para crear un diccionario de posibles contraseñas a partir de la página web que está corriendo en el puerto 1898 del servidor. Guardé ese diccionario en un archivo llamado **DicLampiao.txt**.

Después revisé cuántas palabras se generaron dentro del archivo usando el comando wc -l, y me dio como resultado **844 palabras**. Esto significa que ya tengo una lista bastante amplia de posibles contraseñas que pueden estar relacionadas con el sitio o el sistema.

Luego abrí el archivo con cat para ver algunas de las palabras generadas, y se pueden observar términos relacionados con el contenido del sitio (como “Lampião”, “password”, “user”, etc.).

Finalmente, ejecuté la herramienta **Hydra**, que es la que me va a permitir probar automáticamente las combinaciones de usuario y contraseña a partir del diccionario creado. Esta herramienta es muy útil para pruebas de fuerza bruta en servicios como **SSH**.



13. generar diccionario

14. contar palabras diccionario

```
┌──(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
menu
bando
required
This
password
cangaceiros
era
morte
and
```

15. mostrar contenido diccionario

```
┌──(root㉿kali)-[/home/kali]
└─# hydra &
[1] 3605

┌──(root㉿kali)-[/home/kali]
└─# Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is n
on-binding, 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 M
IN:MAX:CHARSET] [-c TIME] [-ISOuvVd46] [-m MODULE_OPT] [service://server[:PORT][/OPT]]

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)

Supported services: adam6500 asterisk cisco cisco-enable cobaltstrike cvs firebird ftp[s] http[s]-{head|get|post} http[s]-{get|post}-form http-proxy http-prox
y-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|digest}md5][s] memcached mongodb mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres
 radmin2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at;
https://github.com/vanhauser-thc/thc-hydra
```

16. herramienta hydra

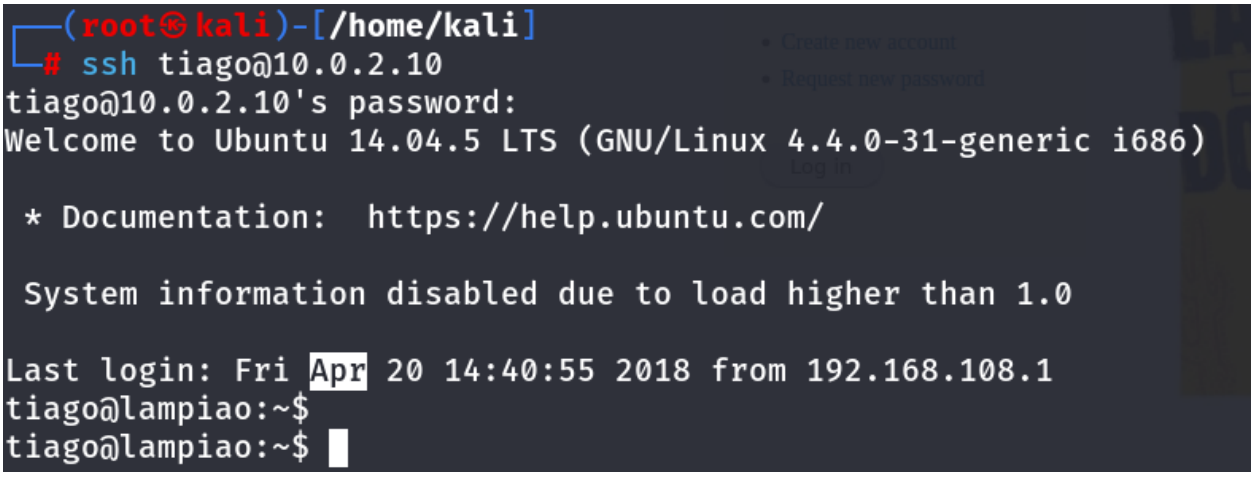
Ingresamos por ssh e ingresamos la contraseña de Virgulino

Paso 7: En este paso me conecté por **SSH** al equipo como el usuario tiago y pude acceder sin problemas; aparece el prompt con la versión de Ubuntu que está corriendo.

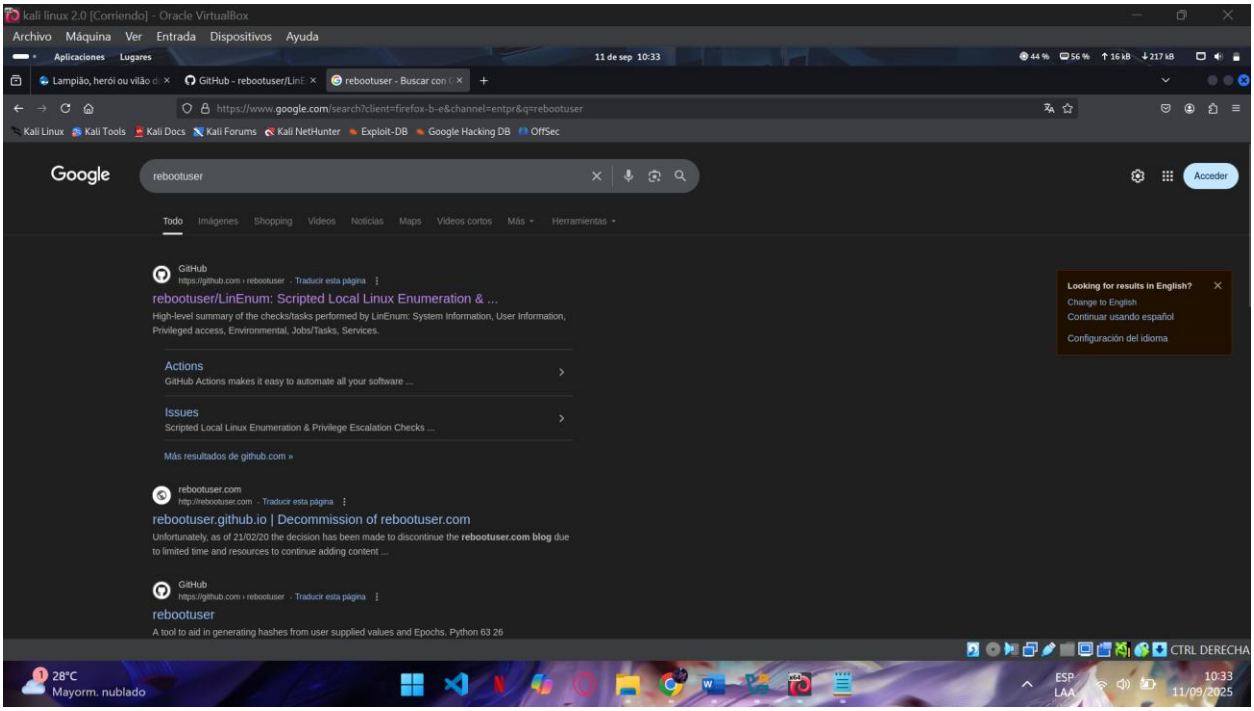
Busqué información sobre herramientas de **enumeración local** y encontré **LinEnum** en GitHub, que es un script que ayuda a recopilar información del sistema para ver posibles vías de escalada de privilegios. Entré a la página del repositorio, lo cloné en mi máquina y abrí el archivo LinEnum.sh para revisar qué hace y ver si puedo usarlo.

Probé ejecutar sudo -l para comprobar si el usuario tiene permisos sudo especiales, pero no tenía permisos adicionales (no se mostró nada útil). Luego navegué por los directorios del usuario (/home/tiago) y di una vuelta por /var para ver si había algún archivo o configuración llamativa. También intenté editar/abrir algunos archivos del sistema, pero no tuve permisos para modificarlos.

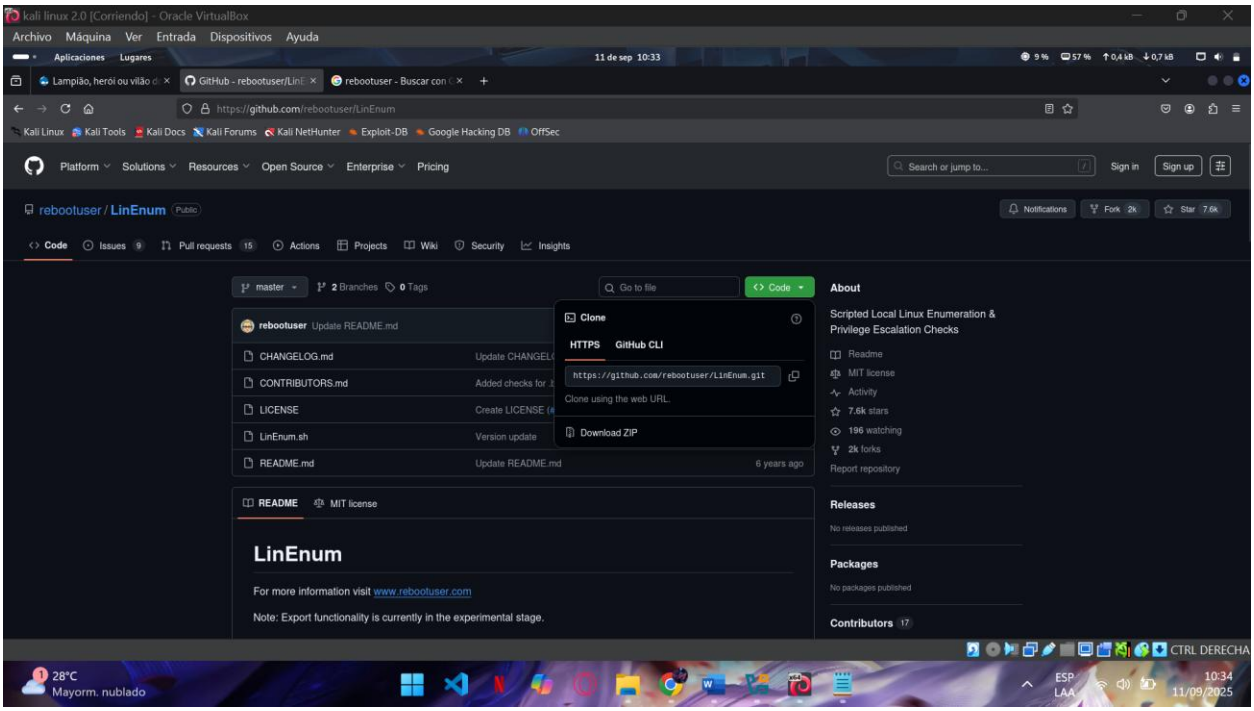
Finalmente revisé el archivo /etc/passwd para ver los usuarios que existen en el sistema (esto es solo lectura y ayuda a entender qué cuentas hay y si alguna parece interesante). En el listado aparecen usuarios del sistema y la cuenta tiago, además del usuario root.



17. ssh login



18. buscar linenum



19. GitHub linenum

```
└─# 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 | 1.06 MiB/s, listo.
Resolviendo deltas: 100% (130/130), listo.

┌──(root㉿kali)-[/home/kali]
└─# ls
aVYBkovN.html  Descargas       Documentos  Imágenes       JvmGtTSw.jpeg  LinEnum         Música          Plantillas  rOVgNuJr.jpeg  Vídeos
clase          DicLampiao.txt  Escritorio  ISJpWcCC.html  KidjqFuL.html  MeFumXhI.jpeg   OBYkAKWD.jpeg   Público     VdSEFNRh.html

┌──(root㉿kali)-[/home/kali]
└─# cd LinEnum

┌──(root㉿kali)-[/home/kali/LinEnum]
└─# ls
CHANGELOG.md  CONTRIBUTORS.md  LICENSE  LinEnum.sh  README.md

┌──(root㉿kali)-[/home/kali/LinEnum]
└─# nano LinEnum

┌──(root㉿kali)-[/home/kali/LinEnum]
└─# nano LinEnum.sh

┌──(root㉿kali)-[/home/kali/LinEnum]
└─# nano LinEnum.sh
```

20. clonar linenum

Pero no se modificó nada

```
 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"

echo -e "\e[00;31m#########################################################\e[00m"
}
header()
                                [ 1352 líneas leídas ]
^G Ayuda      ^O Guardar    ^F Buscar     ^K Cortar     ^T Ejecutar   ^C Ubicación  M-U Deshacer  M-A Poner marca  M-] A llave
^X Salir      ^R Leer fich. ^\ Reemplazar ^U Pegar      ^J Justificar ^/ Ir a línea M-E Rehacer  M-6 Copiar     ^B Buscar atrás
                                                                                                                CTRL DERECHA
```

21. abrir script linenum

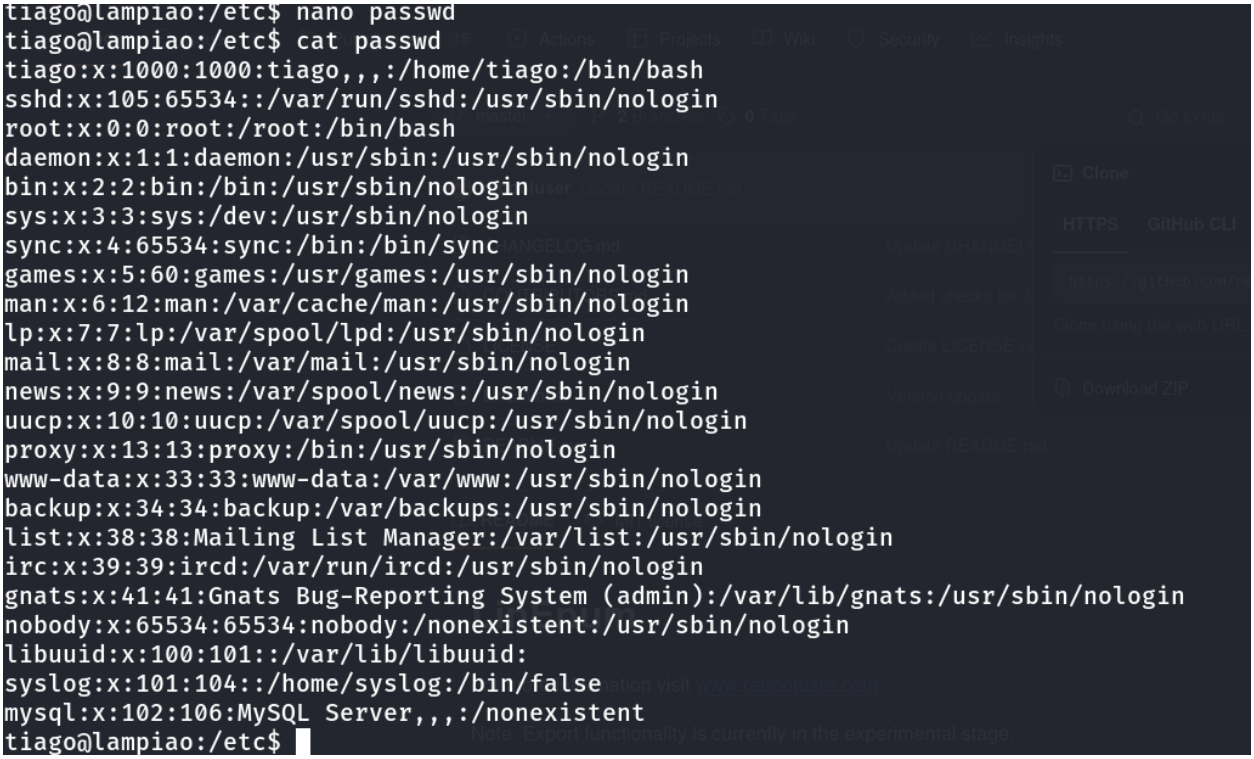
```
[1]+  Stopped                 sudo -l
tiago@lampiao:~$
tiago@lampiao:~$ /home ls
-bash: /home: Is a directory
tiago@lampiao:~$ cd /home
tiago@lampiao:/home$ ls
tiago
tiago@lampiao:/home$ nano tiago
tiago@lampiao:/home$ ls -la
total 12
drwxr-xr-x  3 root  root  4096 Apr 19  2018 .
drwxr-xr-x 21 root  root  4096 Apr 19  2018 ..
drwxr-xr-x  4 tiago tiago 4096 Apr 20  2018 tiago
tiago@lampiao:/home$ cd
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:~$ cd ..
tiago@lampiao:/home$ cd ..
tiago@lampiao:/$ ls
bin  boot  dev  etc  home  initrd.img  lib  lost+found  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var  vmlinuz
tiago@lampiao:/$ cd var
```

22. intentar sudo

Tampoco se modificó nada

```
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
mysql:x:102:106:MySQL Server,,,:/nonexistent


                [ 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
```

23. explorar home var

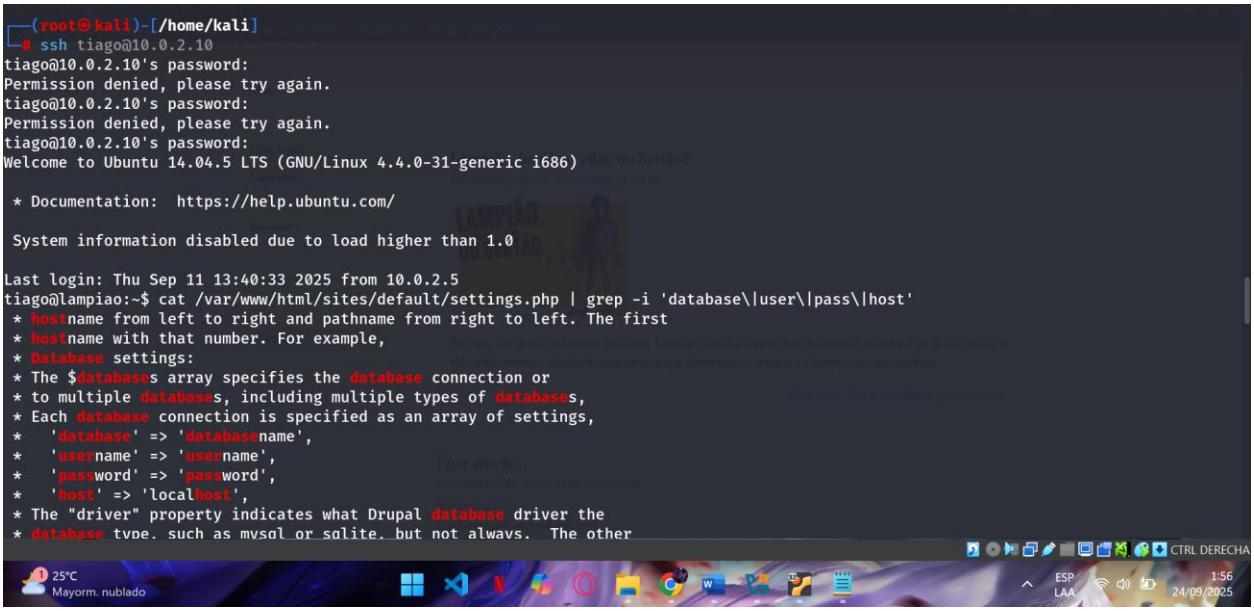


24ver passwd nnano

Crear dos usuarios

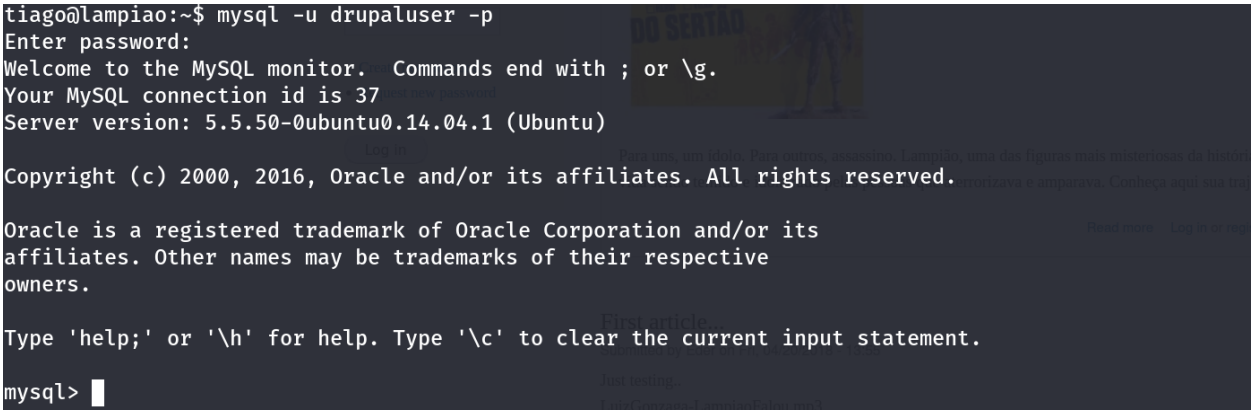
Paso 8 Al conectar por SSH tuve que intentarlo un par de veces hasta que me dejó entrar como tiago; en la cabecera de la sesión se ve la versión de Ubuntu del servidor. Una vez dentro fui directo al árbol del sitio web y abrí el archivo de configuración principal: /var/www/html/sites/default/settings.php. Para no leer todo el archivo usé un comando que filtra por palabras clave relacionadas con la base de datos (database, user, pass, host) y así localizar

rápidamente la sección que define la conexión.



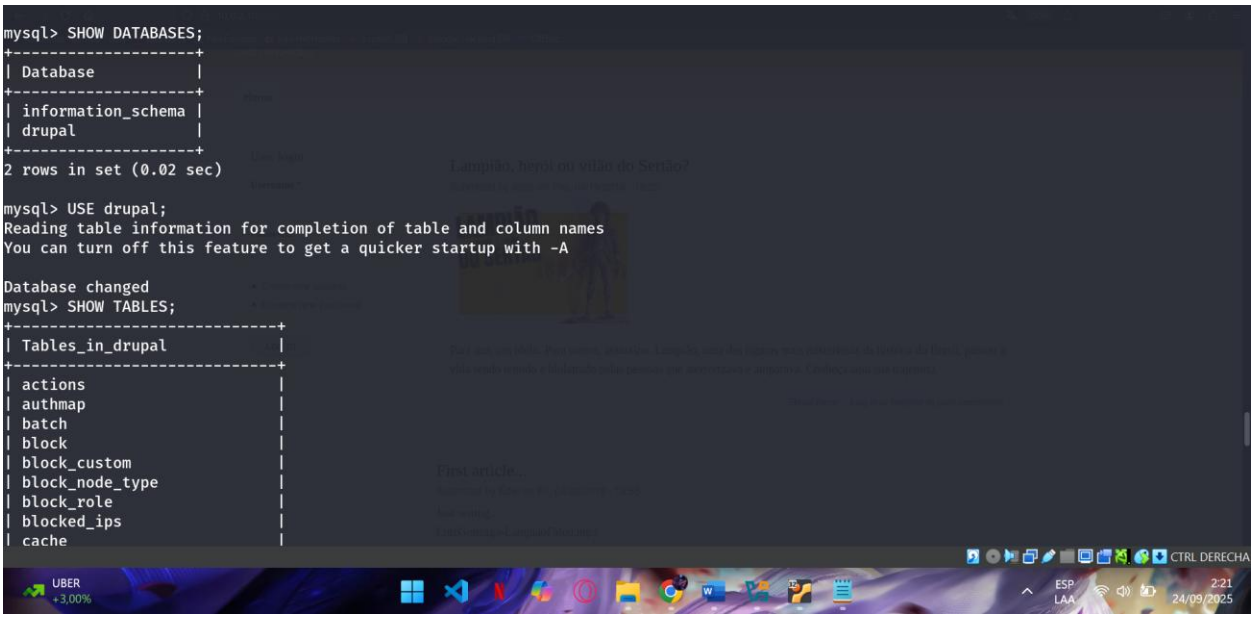
25. settings php

Paso 9: Ingresé a la base de datos usando el usuario drupaluser con el comando mysql -u drupaluser -p. Tras escribir la contraseña correctamente, se abrió la consola de MySQL y pude ver la versión instalada en el servidor. Esto me confirmó que tenía acceso directo al motor de base de datos, lo cual era un avance importante.



26. Ingreso a MySQL con el usuario drupaluser

Dentro de MySQL ejecuté el comando SHOW DATABASES; y se listaron las bases disponibles. Entre ellas encontré la llamada drupal, que es la que resultaba más interesante porque seguramente contenía la información del portal. Después accedí a esa base con USE drupal; y listé todas sus tablas.



27. Visualizando las bases de datos existentes

Al revisar la tabla users, ejecuté una consulta para mostrar los campos uid, name, mail y pass. De esta manera pude obtener los usuarios registrados en el portal Lampião, junto con sus correos y contraseñas en formato cifrado. Esto me dio una idea clara de las cuentas ya existentes en el sistema.

```
mysql> SELECT uid, name, mail, pass FROM users;
+-----+--------+--------------------+-------------------------------------------------------------+
| uid | name   | mail               | pass                                                        |
+-----+--------+--------------------+-------------------------------------------------------------+
|   0 |        |                    |                                                             |
|   1 | tiago  | lampiao@lampiao.com | $S$DNZ5o1k/NY7SUgtJvjPqNl40kHKwn4yXy2eroEnOAlpmT0TJ9Sx8 |
|   2 | Eder   | eder@lampiao.com    | $S$Dv5orvhi7okjmViImnVPmVgfwJ2U..PNK4E9IT/k7Lqz9GZRb7tY |
|   3 | edward | ecabe@gmail.com     | $S$DurKAY/HrzaCKkqXHfrn1v0oDesKkN.LNuUCIJi9PY8IUhUuLa4s |
+-----+--------+--------------------+-------------------------------------------------------------+
4 rows in set (0.01 sec)
```

28. Consulta de usuarios en la base de datos

Para saber cuál era el siguiente identificador de usuario disponible, ejecuté SELECT MAX(uid) FROM users;. El resultado mostró que el valor más alto era 3, lo que significaba que el próximo uid libre sería el 4. Esta información era necesaria para crear nuevos registros en la tabla sin causar conflictos.

```
mysql> mysql> SELECT MAX(uid) FROM users;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right s
yntax to use near 'mysql> SELECT MAX(uid) FROM users' at line 1
mysql> SELECT MAX(uid) FROM users;
+----------+
| MAX(uid) |
+----------+
|        3 |
+----------+
1 row in set (0.00 sec)
```

29. Comprobando el identificador máximo de usuarios

A continuación, realicé inserciones en la tabla users para añadir dos nuevas cuentas con nombres admin1 y admin2. Para la contraseña utilicé la función MD5, lo que generó un hash que se almacenó en la base de datos. Tras ejecutar el comando, confirmé que los nuevos registros se habían agregado correctamente. Con otro SELECT revisé de nuevo la tabla users y comprobé que ahora aparecían las nuevas cuentas junto a las anteriores. En la salida se podían ver los nombres, correos y contraseñas cifradas de admin1 y admin2, lo que confirmó que la inserción había sido exitosa.

```
mysql> INSERT INTO users (uid, name, pass, mail, status, created)
    ->  VALUES (4, 'admin1', MD5('edward'), 'camilo@gmail.com', 1, UNIX_TIMESTAMP());
Query OK, 1 row affected (0.03 sec)

mysql> INSERT INTO users (uid, name, pass, mail, status, created)
    ->     ->  VALUES (4, 'admin1', MD5('edward'), 'camilo@gmail.com', 1, UNIX_TIMESTAMP());
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right s
yntax to use near '->  VALUES (4, 'admin1', MD5('edward'), 'camilo@gmail.com', 1, UNIX_TIMESTAMP())' at line 2
mysql>  INSERT INTO users (uid, name, pass, mail, status, created)
    ->  VALUES (5, 'admin2', MD5('camilo'), 'edward@gmail.com', 1, UNIX_TIMESTAMP());
Query OK, 1 row affected (0.01 sec)

mysql> SELECT uid, name, mail, pass FROM users;
+-----+--------+--------------------+--------------------------------------------------------------+
| uid | name   | mail               | pass                                                         |
+-----+--------+--------------------+--------------------------------------------------------------+
|   0 |        |                    |                                                              |
|   1 | tiago  | lampiao@lampiao.com | $S$DNZ5o1k/NY7SUgtJvjPqNl40kHKwn4yXy2eroEnOAlpmT0TJ9Sx8 |
|   2 | Eder   | eder@lampiao.com    | $S$Dv5orvhi7okjmViImnVPmVgfwJ2U..PNK4E9IT/k7Lqz9GZRb7tY |
|   3 | edward | ecabe@gmail.com     | $S$DurKAY/HrzaCKkqXHfrn1v0oDesKkN.LNuUCIJi9PY8IUhUuLa4s |
|   4 | admin1 | camilo@gmail.com    | a53f3929621dba1306f8a61588f52f55                             |
|   5 | admin2 | edward@gmail.com    | 0aa0b6b3207f0b3839381db1962574a2                             |
+-----+--------+--------------------+--------------------------------------------------------------+
6 rows in set (0.00 sec)
```

30. Inserción de nuevos usuarios en la base de datos

Volví a ejecutar el comando SELECT MAX(uid) FROM users; para validar que el contador de identificadores se había actualizado. El resultado mostró que ahora el valor máximo era 5, lo que reflejaba los dos nuevos registros creados.

```
mysql> SELECT MAX(uid) FROM users;
+----------+
| MAX(uid) |
+----------+
|        5 |
+----------+
1 row in set (0.00 sec)
```

31. Nuevo identificador máximo de usuarios

Finalmente consulté la tabla role para conocer los identificadores de los diferentes roles del sistema, entre ellos el de administrador. Con esos datos, inserté registros en la tabla users_roles asignando el rol de administrador a las cuentas recién creadas. Esto significó que los nuevos usuarios tenían ya permisos elevados dentro del portal.

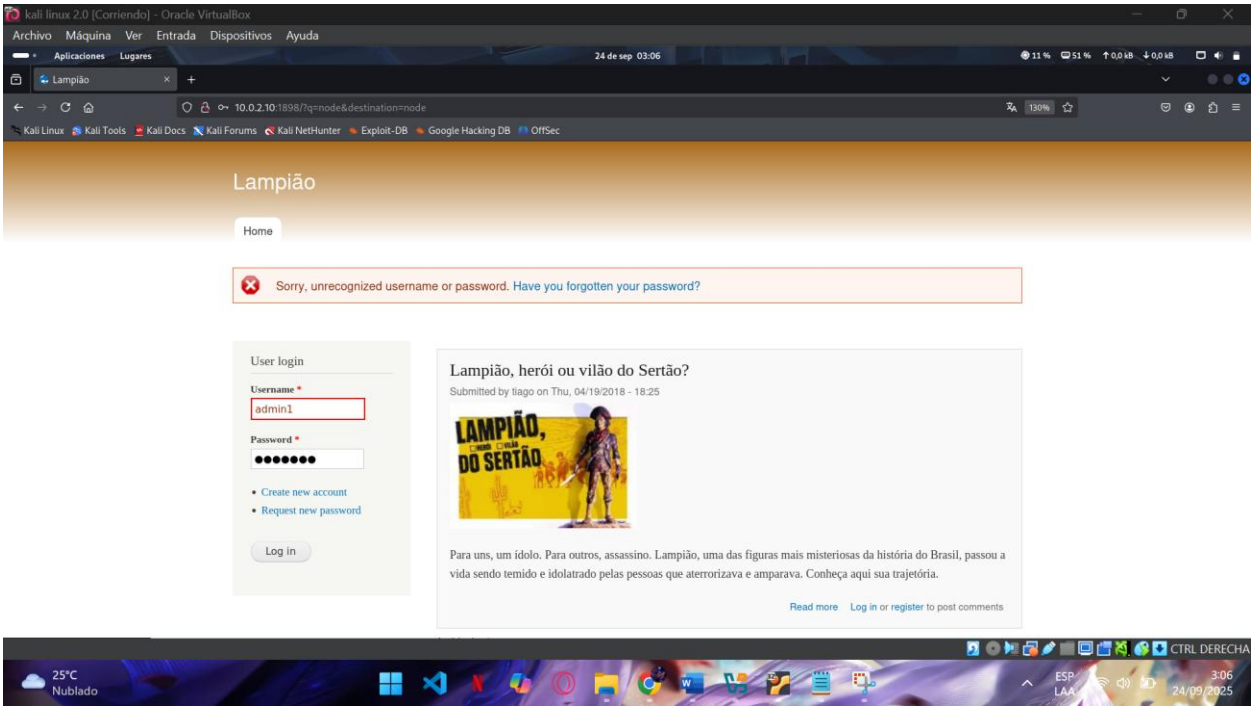
```
mysql> SELECT * FROM role;
+-----+-------------------+--------+
| rid | name              | weight |
+-----+-------------------+--------+
|   3 | administrator     |      2 |
|   1 | anonymous user    |      0 |
|   2 | authenticated user |      1 |
|   4 | writer            |      3 |
+-----+-------------------+--------+
4 rows in set (0.00 sec)

mysql> INSERT INTO users_roles (uid, rid) VALUES (3, 3);
Query OK, 1 row affected (0.02 sec)

mysql> INSERT INTO users_roles (uid, rid) VALUES (4, 3);
Query OK, 1 row affected (0.01 sec)

mysql> INSERT INTO users_roles (uid, rid) VALUES (5, 3);
Query OK, 1 row affected (0.00 sec)

mysql>
```

32. Asignación de roles a los usuarios creados

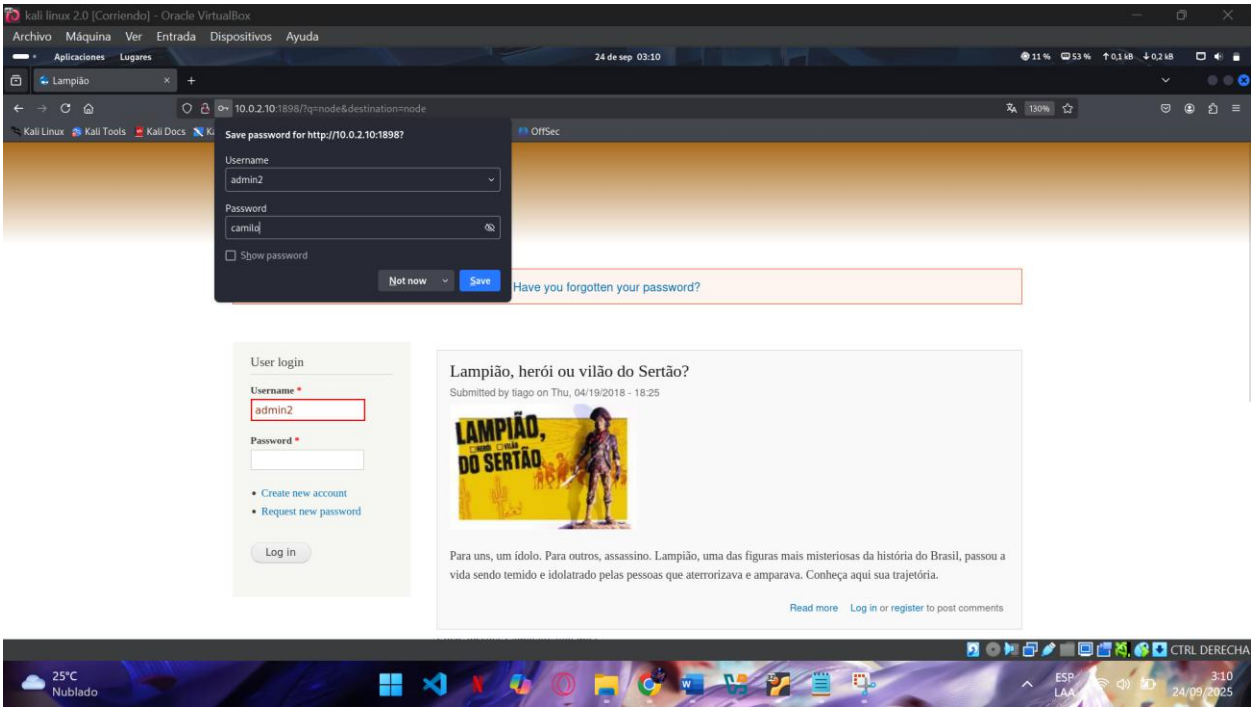
Resultados

En este intento traté de ingresar al portal Lampião usando el usuario admin1 que previamente había creado dentro de la base de datos. Sin embargo, al introducir la contraseña, el sistema devolvió un error indicando que el usuario o la contraseña no eran reconocidos. Esto me dejó claro que, aunque el registro se había insertado correctamente en la base de datos, el portal no lo validaba al momento de iniciar sesión.

Después probé con el usuario admin2, al cual también le había asignado el rol de administrador en la base de datos. Al introducir su contraseña, nuevamente el portal mostró el mismo mensaje de error de credenciales inválidas. Incluso el navegador me ofreció guardar los datos, pero el acceso no fue exitoso.



33. Fallo de inicio de sesión con el usuario admin1



34. Fallo de inicio de sesión con el usuario admin2

Resultados obtenidos:

- Se logró acceder a la base de datos MySQL y crear usuarios nuevos directamente en la tabla users.
- También se asignaron roles de administrador a esos usuarios para darles permisos elevados dentro del sistema.
- A pesar de esto, los intentos de iniciar sesión con dichos usuarios en la interfaz web del portal Lampião fueron fallidos.

Posibles causas del fallo:

1. **Inconsistencias en los hashes de contraseña:** El portal probablemente no utilice directamente MD5 para validar las contraseñas, sino un esquema más complejo (por ejemplo, contraseñas con salto algoritmos específicos de Drupal como phpass).

2. **Campos adicionales no configurados:** Es posible que al crear los usuarios desde la base de datos faltara rellenar otros campos necesarios (por ejemplo, estado de la cuenta, fecha de creación o tokens de validación).
3. **Validación interna del sistema:** El portal puede requerir que los usuarios sean creados desde la interfaz de administración y no directamente desde la base de datos, por lo que no reconoce los registros añadidos manualmente.
4. **Restricciones de seguridad del CMS:** El sistema Lampião (basado en Drupal) podría tener mecanismos para ignorar registros no generados por sus propios procesos de creación de cuentas.

CONCLUCIÓN

El análisis permitió comprobar que, aunque es posible acceder y manipular directamente los registros de la base de datos de Drupal, esto no garantiza automáticamente el acceso al portal web, ya que el sistema emplea métodos más complejos para validar las credenciales y el estado de las cuentas. Entre las posibles causas se encuentran el uso de algoritmos de hash específicos, la falta de campos adicionales requeridos en la creación de usuarios y las restricciones propias del CMS para validar cuentas legítimas.

En términos de seguridad, el ejercicio demostró la importancia de proteger adecuadamente los accesos a la base de datos y de implementar mecanismos robustos de validación de usuarios. A nivel práctico, permitió reforzar el conocimiento sobre técnicas de auditoría y sobre cómo interactúan los distintos componentes de un sistema web vulnerable.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

REFERENCIA BIBLIOGRÁFICA

Ingeniero Rafael Sandoval