INFORME LABORATORIO 04

JESUS ORULA BARCOS PADILLA

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA
FACULTAD DE INGENIERÍA, INGENIERÍA TELECOMUNICACIONES E INFORMÁTICA – IX NIVEL

SEGURIDAD Y AUDITORÍA DE REDES

QUIBDÓ, CHOCÓ, COLOMBIA
2025

INFORME LABORATORIO 04

JESUS ORULA BARCOS PADILLA

INFORME DE EXPLOTACIÓN

RAFAEL SANDOVAL MORALES

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA
FACULTAD DE INGENIERÍA, INGENIERÍA TELECOMUNICACIONES E INFORMÁTICA – IX NIVEL

SEGURIDAD Y AUDITORÍA DE REDES

QUIBDÓ, CHOCÓ, COLOMBIA
2025

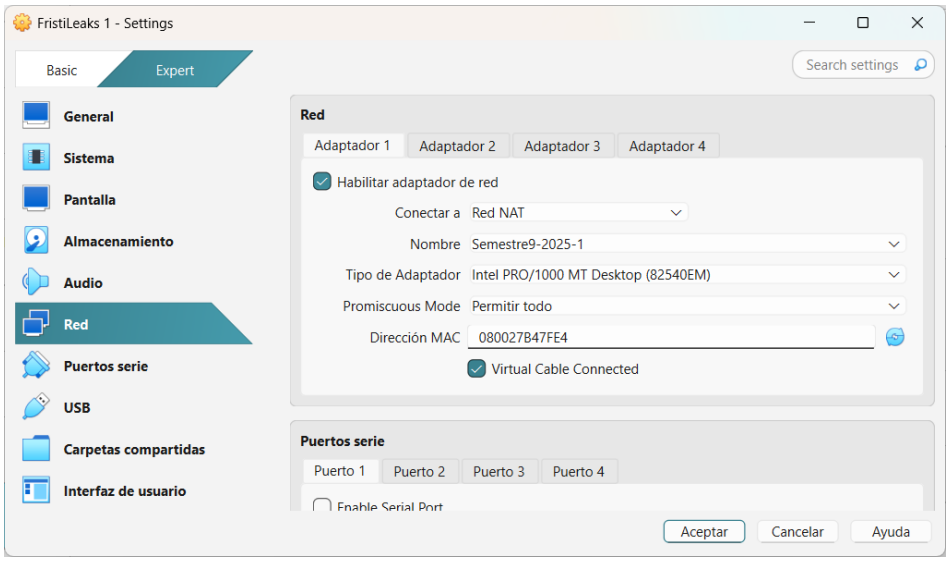
TABLA DE CONTENIDO

TABLA DE ILUSTRACIONES

CONFIGURAR FRISTILEAKS.

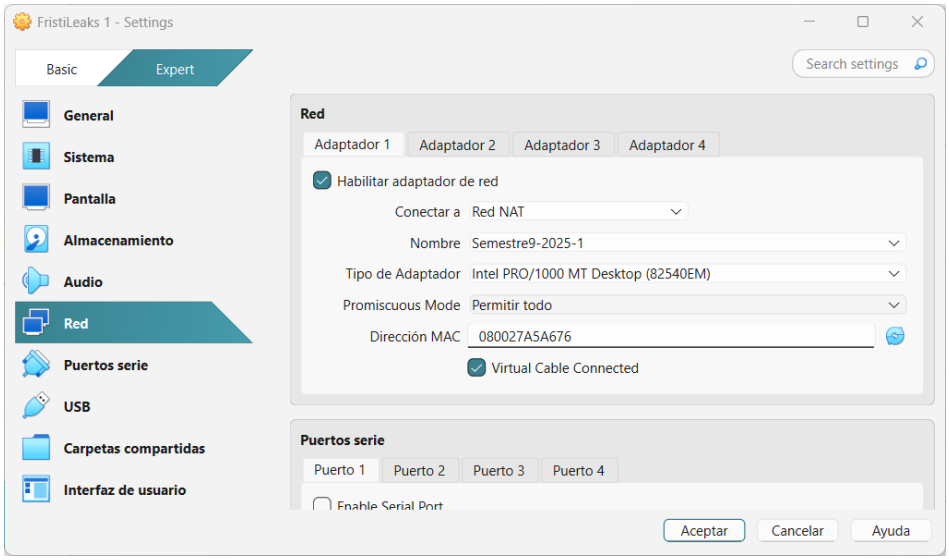
Para iniciar Fristileaks se debe cambiar la dirección Mac que trae por defecto.

Ilustración 1Dirección Mac por defecto.



En este caso la dirección Mac que hay que usar es **00800027A5A676.**

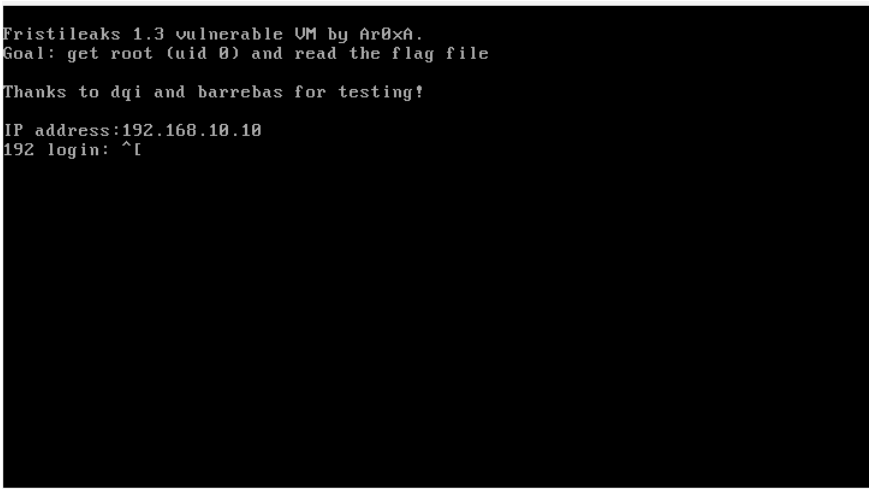
Ilustración 2 Nueva dirección Mac.



ABRIR FRISTILEAKS.

Iniciar la máquina virtual de Fristileaks.

Ilustración 3 Windows 2003.



ABRIR LINUX.

Iniciar la máquina virtual de Linux.

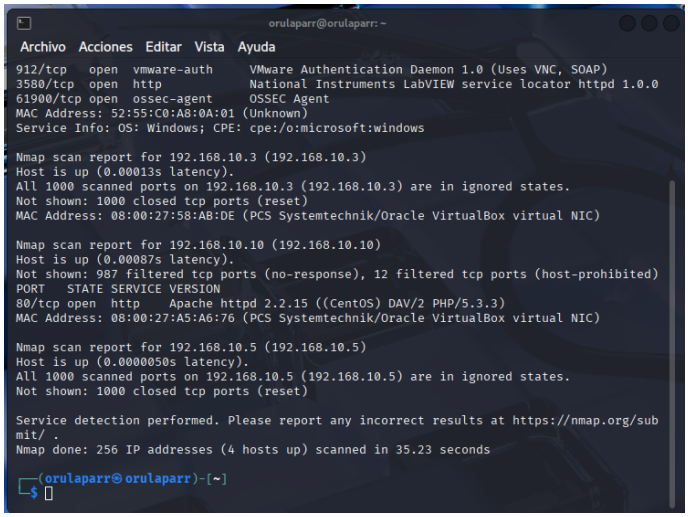
Ilustración 4 Linux.

VULNERAR FRISTILEAKS.

1. Utilizar el comando nmap.

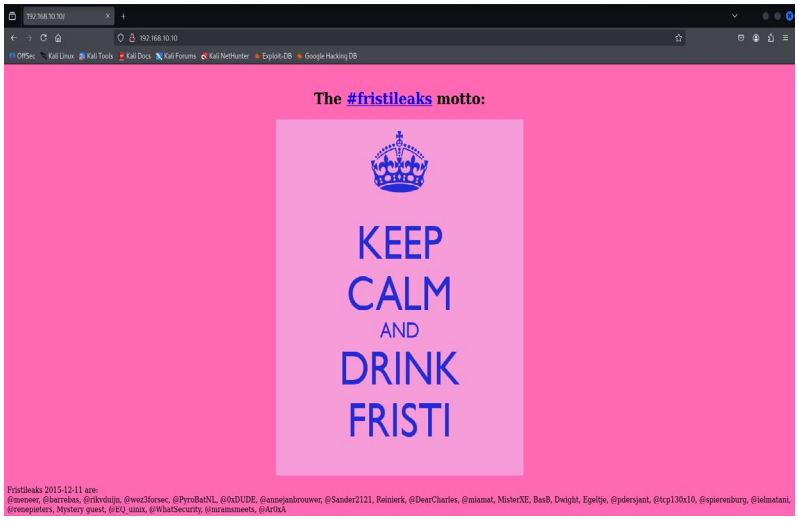
Se utiliza el comando `nmap -sV 192.168.10.0/24` para ver que puertos se pueden vulnerar.

Ilustración 5 Puertos disponibles.



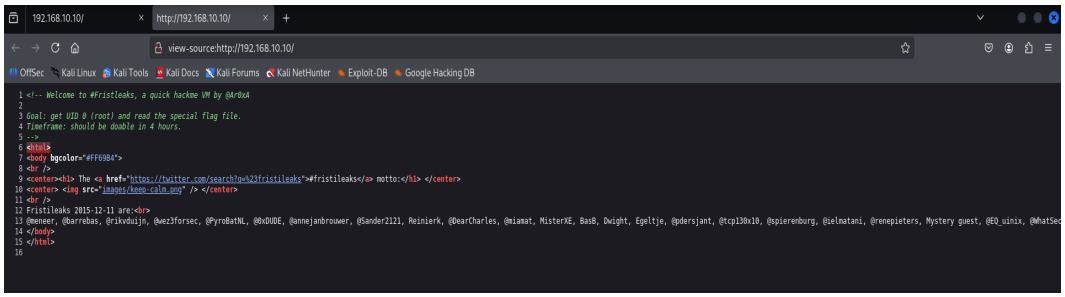
En este caso se puede observar que Fristileaks utiliza un servicio http, es decir, tiene una pagina web. Para ingresar a dicha página web, colocamos la dirección ip de Fristileaks en el navegador.

Ilustración 6 Página web de Fristileaks.



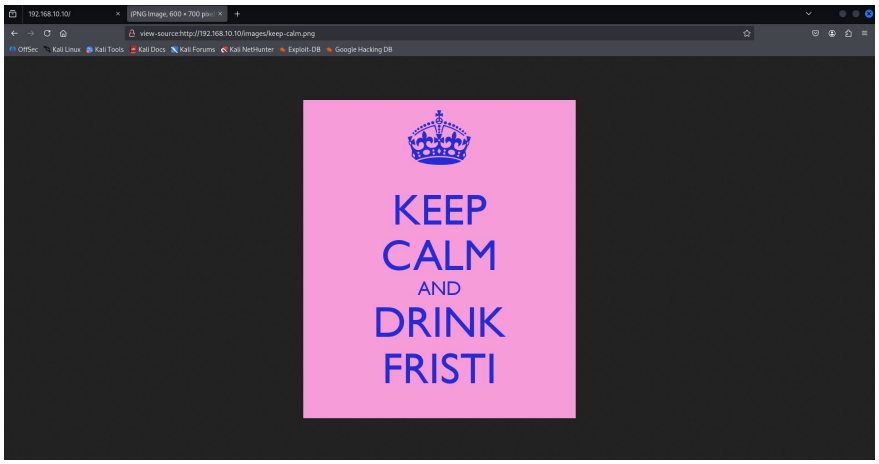
Se puede observar que la página principal no interacción alguna. Entonces se procede a ver el código raíz de esta página, dándole clic derecho y **View Page Source.** A continuación, se podrá observar el código de esta página de donde se puede extraer una URL.

Ilustración 7 HTML.



El URL dirigirá a la imagen que nos aparece en la página principal.

Ilustración 8 Imagen.



2. Utilizar el comando dirb.

Se utiliza el comando `dirb http://192.168.10.10/` para tomar un diccionario de nombres, los va probando uno por uno con la URL que le indicamos y si alguno existe, nos lo reporta.

Ilustración 9 Comando dirb.

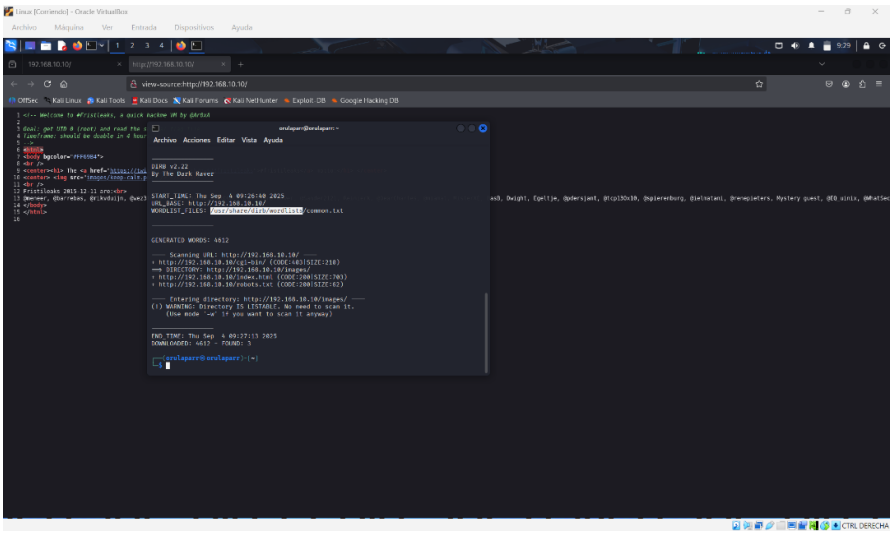


Ilustración 10 Listas dirb.

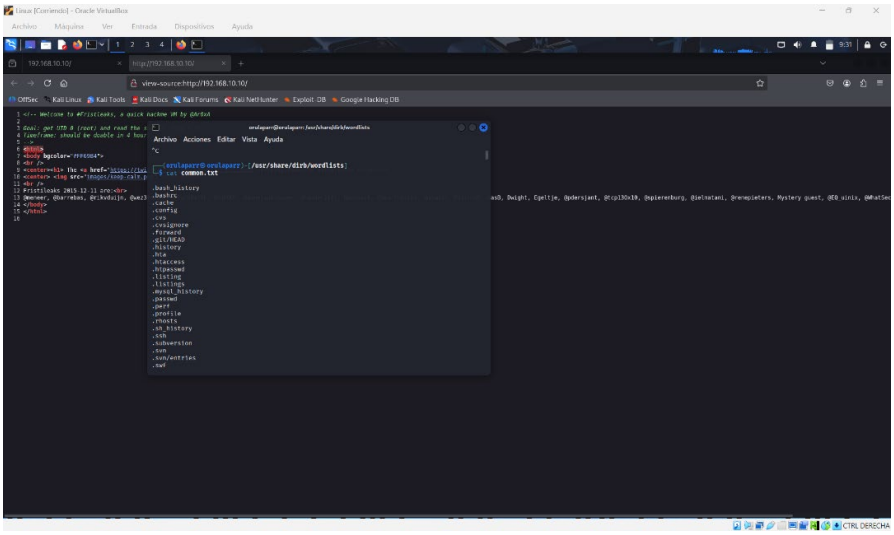


Ilustración 11 Subdominios.

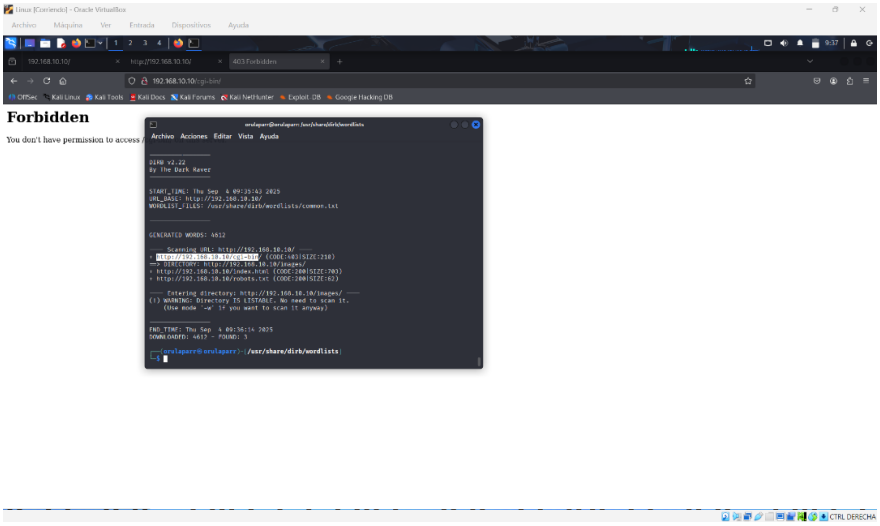


Ilustración 12 Subdominio 1.

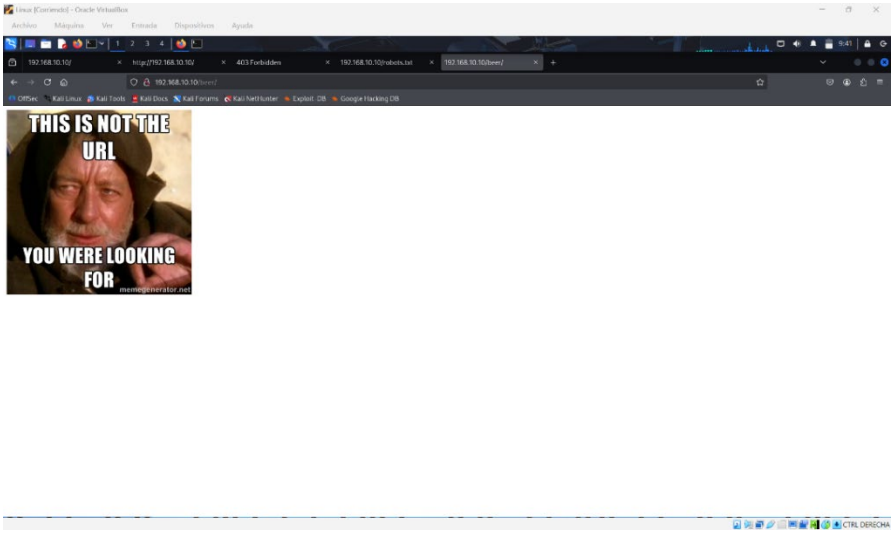


Ilustración 13 Login.

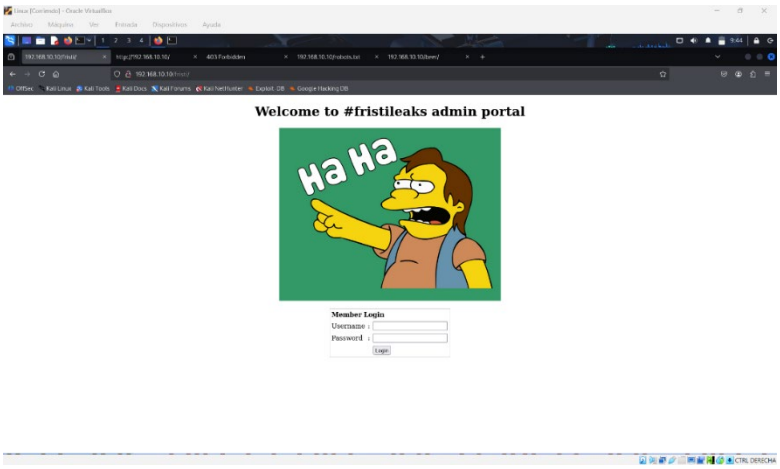


Ilustración 14 HTML 2.

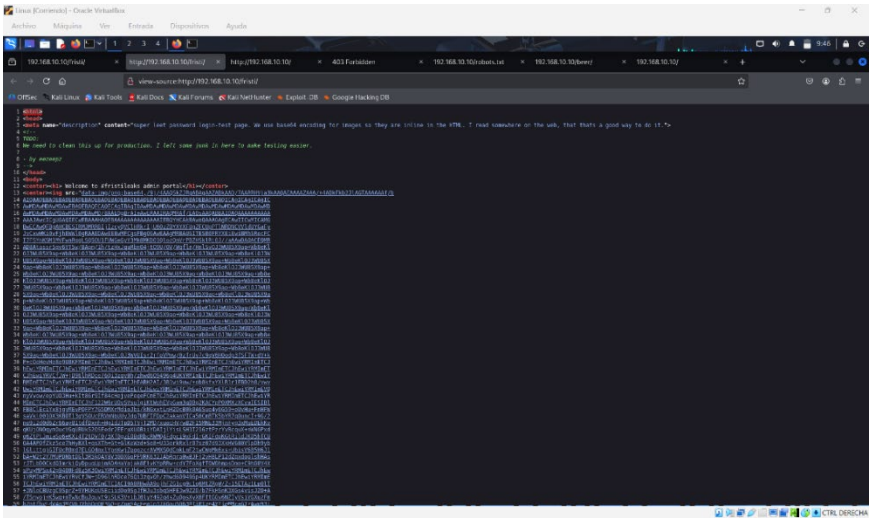
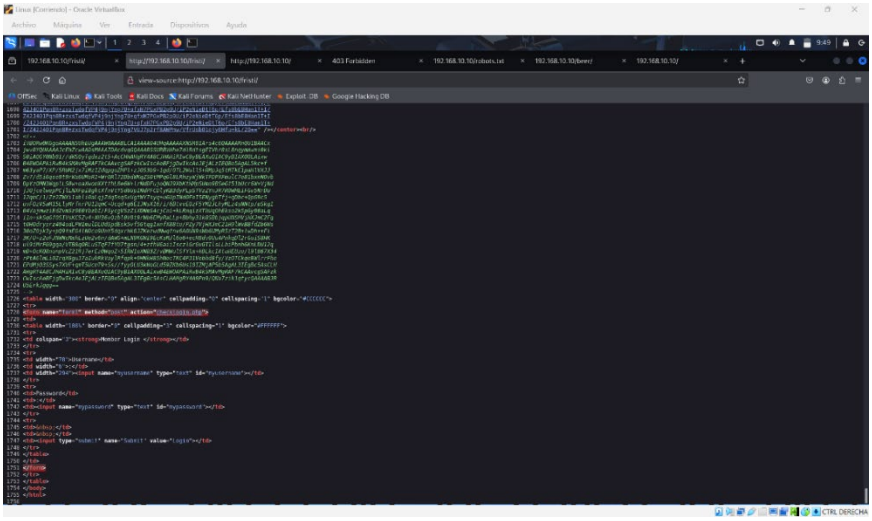


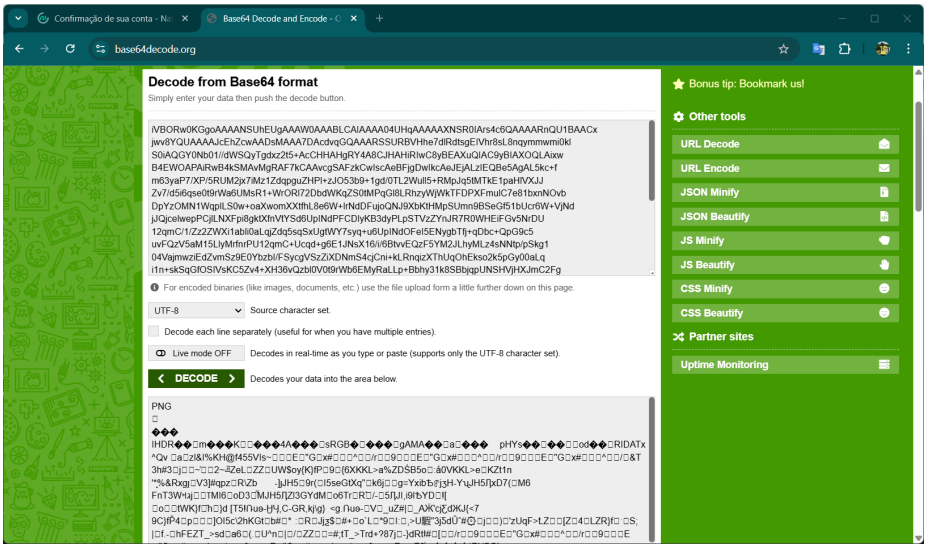
Ilustración 15 HTML 2.1



DESENCRIPTAR TEXTO.

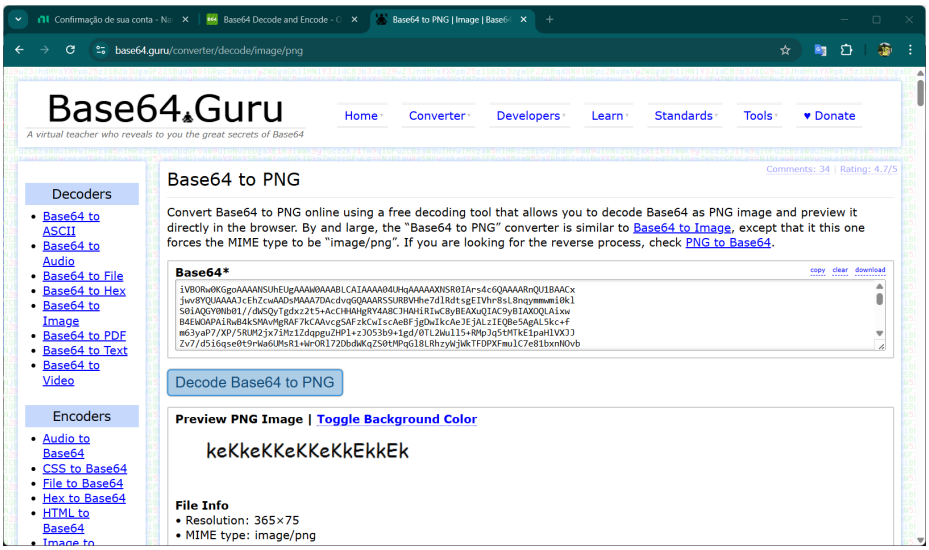
Para desencriptar un texto se debe recurrir a una página desencriptadora de bas64 y colocar el texto.

Ilustración 16 Desencriptar base64.



Este será el resultado del texto de base64 desencriptado.

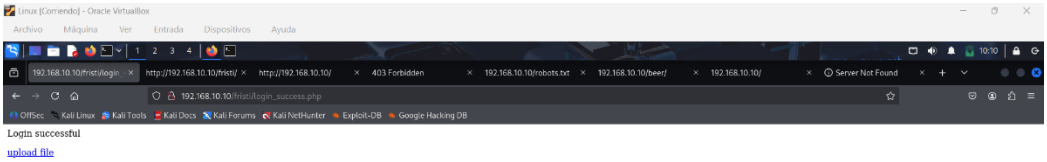
Ilustración 17 Texto desencriptado.



Una vez hecho este proceso se procede a intentar con el **usuario: eezeepz** y la **contraseña: keKkeKKeKKeKkEkkEk.**

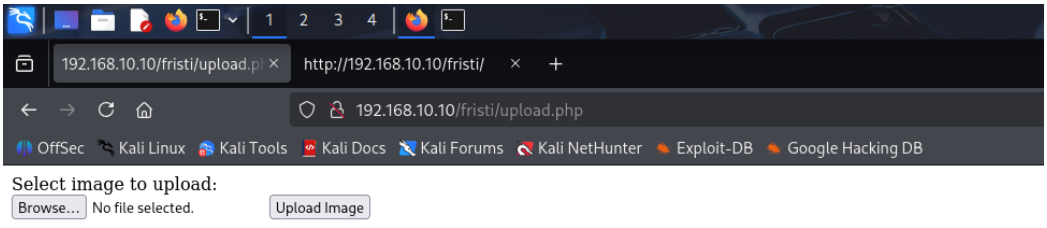
A continuación, se puede observar que tanto el usuario como la contraseña son correctos y pudo iniciar sección. En donde nos va a dar una opción para subir un archivo.

Ilustración 18 Inicio de sección exitoso.



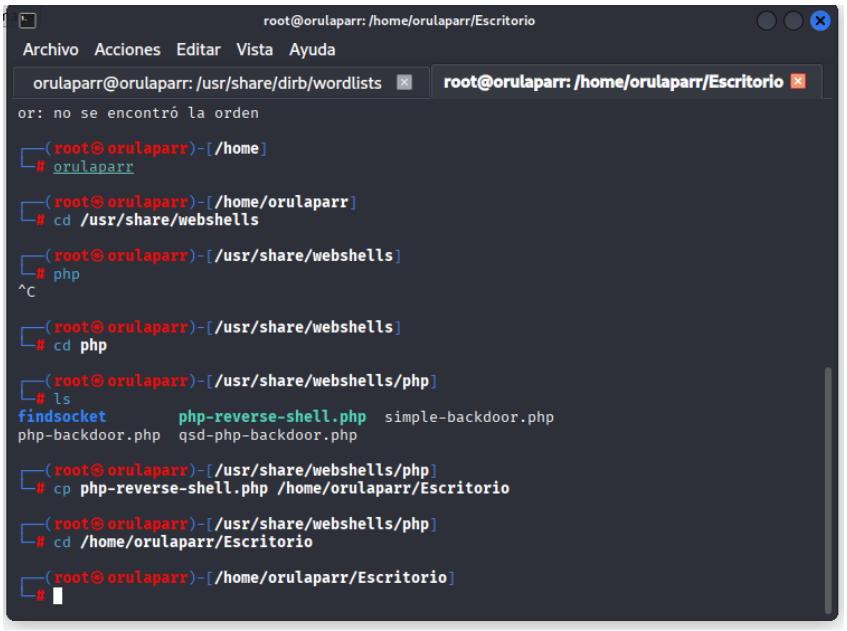
Cuando se le da clic en subir archivo, nos dice que el tipo de archivo permitido es de imagen (.png)

Ilustración 19 Subir png.



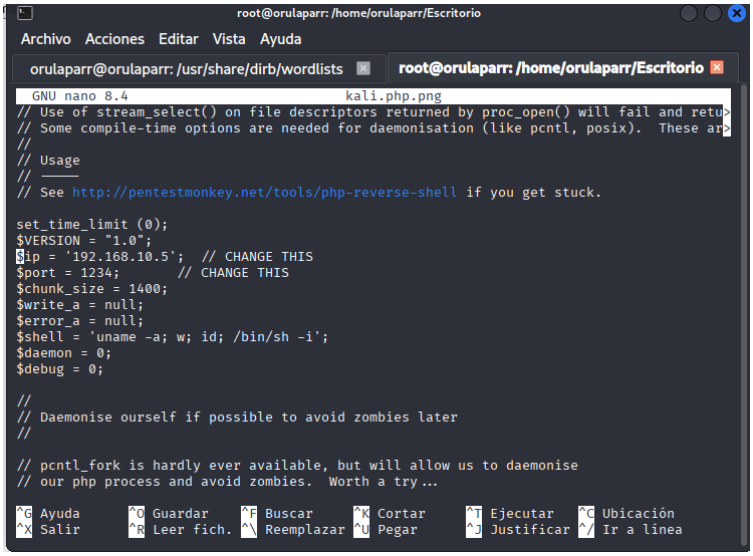
Entonces se procede a crear un archivo malicioso con extensión **.png**

Ilustración 20 Archivo malicioso.



Y se procede a colocarle la IP de nuestro Linux para posteriormente subirlo en la página.

Ilustración 21 Editar archivo.



Selecciona el documento creado y editado recientemente.

Ilustración 22 Seleccionar el documento.

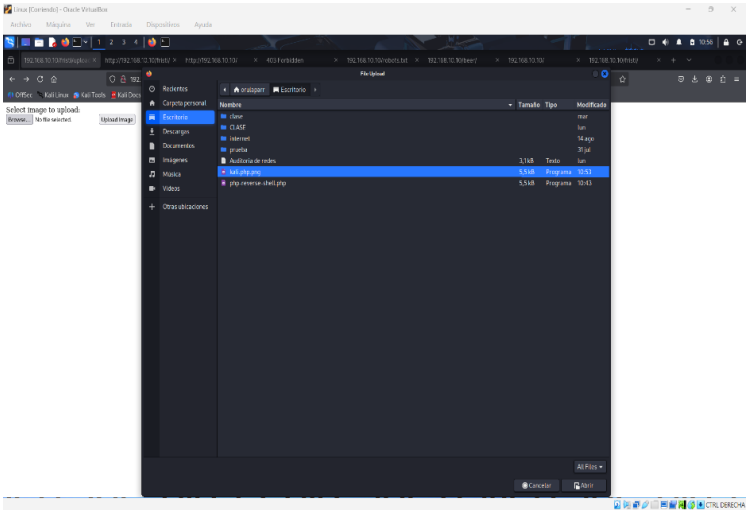
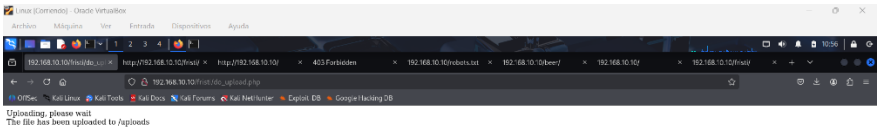


Ilustración 23 Documento subido correctamente.



Una vez subido el documento, se debe acceder a la URL `http://192.168.10.10/fristi//uploads/kali.php.png` y utilizar el comando `nc -lvp 1234`

Ilustración 24 Ingreso con éxito a la máquina virtual.

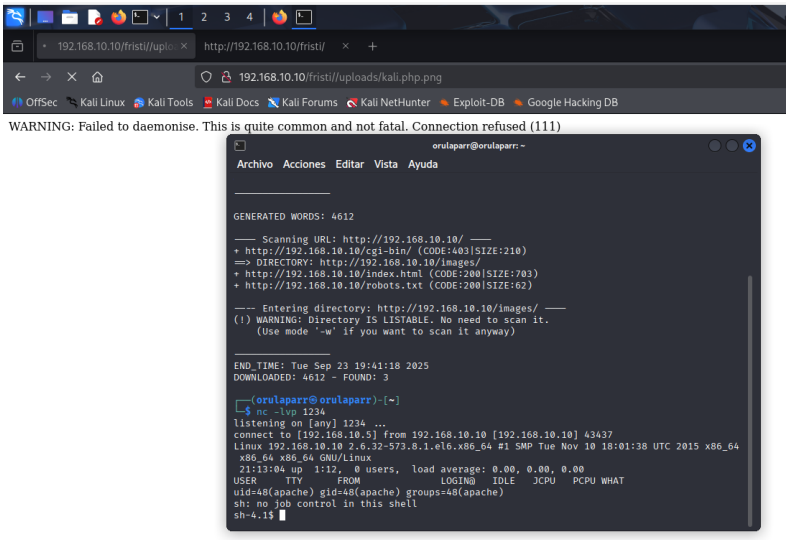


Ilustración 25 Whoami.