Informe 1 – Segundo Parcial

Yadier Stiven Mayoral Palomeque

Facultad de Ingeniería, Universidad Tecnológica del Chocó Diego Luis Córdoba

2720409: Seguridad y Auditoria de Redes

Docente: Rafael Sandoval Morales

Quibdó, Chocó

Septiembre 2025

Tabla de Contenido

Pag.

Tabla de Ilustraciones

Pag.

Introducción

Este es el primer laboratorio del segundo parcial de la asignatura de seguridad y auditoría de redes. El objetivo es simular un entorno controlado que represente una red real, permitiendo poner en práctica técnicas de reconocimiento, análisis y explotación de servicios/puertos vulnerables.

Dentro de este entorno se configuraron diferentes máquinas virtuales, entre ellas Kali Linux como sistema atacante, y FristiLeaks como víctima, además se hizo una configuración en una maquina con sistema operativo Fedora Linux para que solo tomara dirección IP de la red NAT con una dirección MAC anteriormente establecida.

Objetivos

Objetivo General

Simular un entorno controlado que represente una red real mediante el uso de máquinas virtuales en red NAT, con el fin de poner en práctica técnicas de generación y ejecución de archivos maliciosos que permitan obtener acceso remoto a sistemas Linux.

Objetivos Específicos

Crear una red NAT e integrar las máquinas virtuales para establecer un entorno seguro para llevar a cabo el laboratorio.

Escanear la red con Nmap con el fin de identificar dispositivos conectados.

Configurar Fedora para que solo adquiera direcciones IP con una dirección MAC configurada.

Escanear y encontrar vulnerabilidades en FristiLeaks y crear dos usuarios.

Desarrollo

Importación y configuración de FristiLeaks

El primer paso es la importación de FristiLeaks en VirtualBox.

Ilustración 1 Importación de FristiLeaks

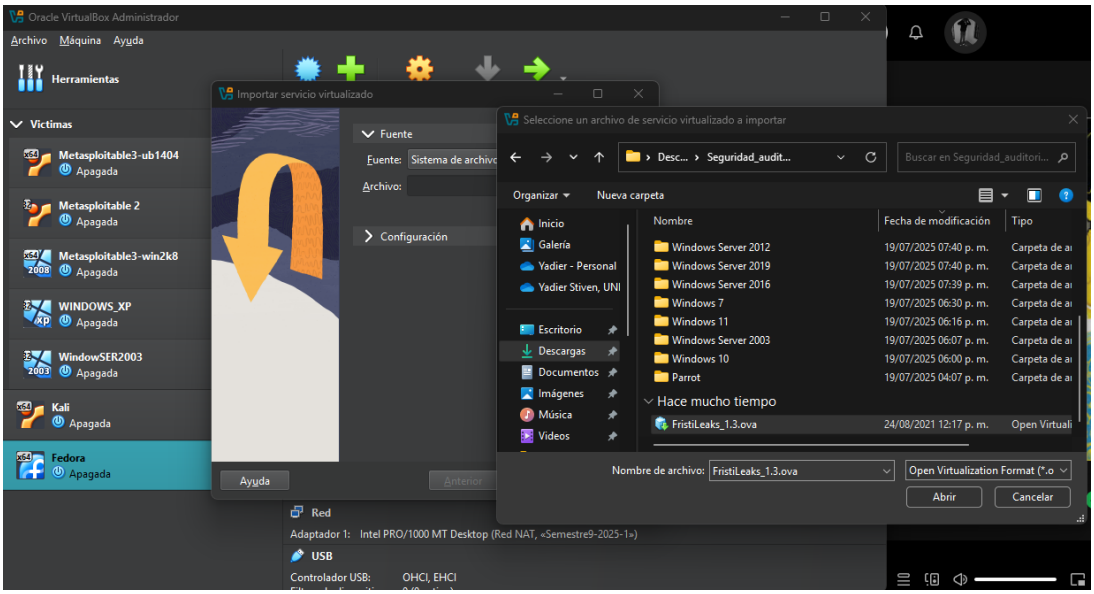
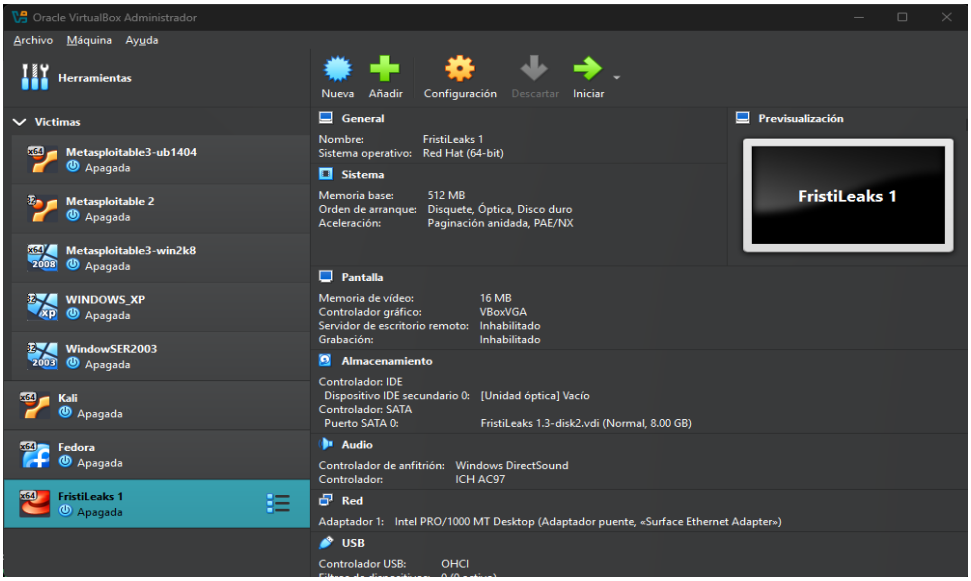


Ilustración 2 FristiLeaks importado



Luego se hacen algunas modificaciones en la configuración por defecto de FristiLeaks.

La primera modificación consiste en poner el portapapeles compartido y la acción de arrastrar y soltar en modo bidireccional.

Ilustración 3 Modo bidireccional

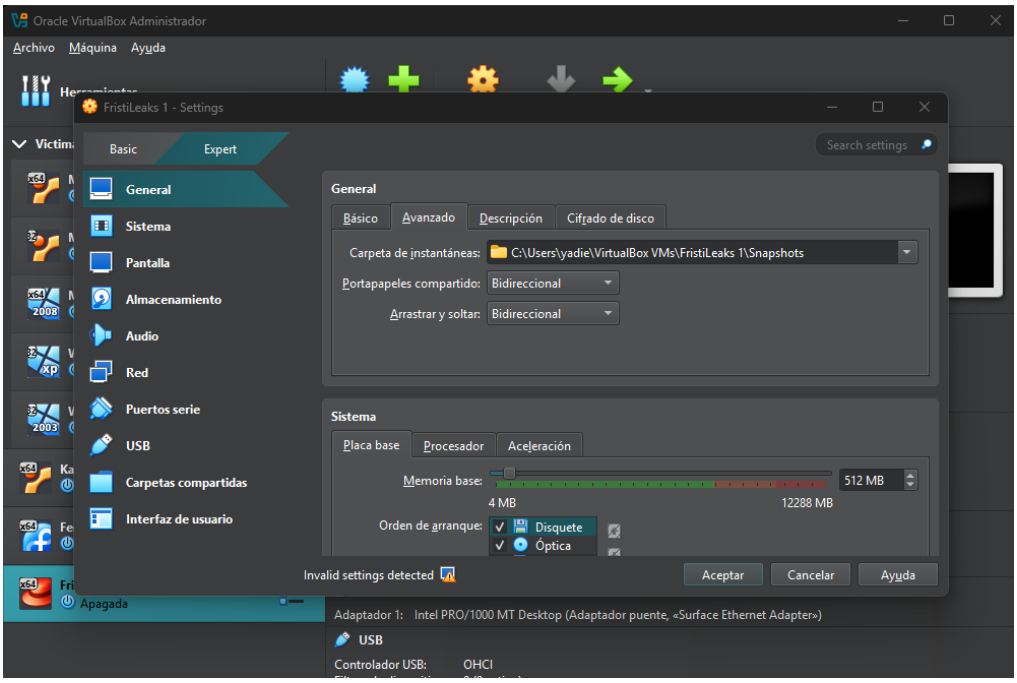


Ilustración 4 Modificación características extendidas

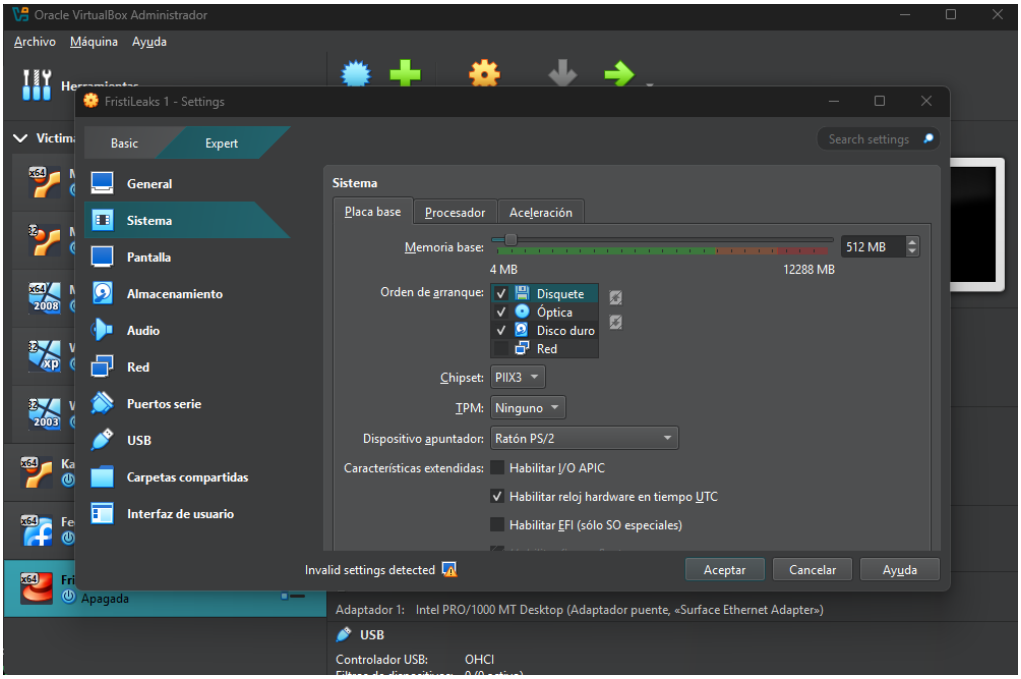
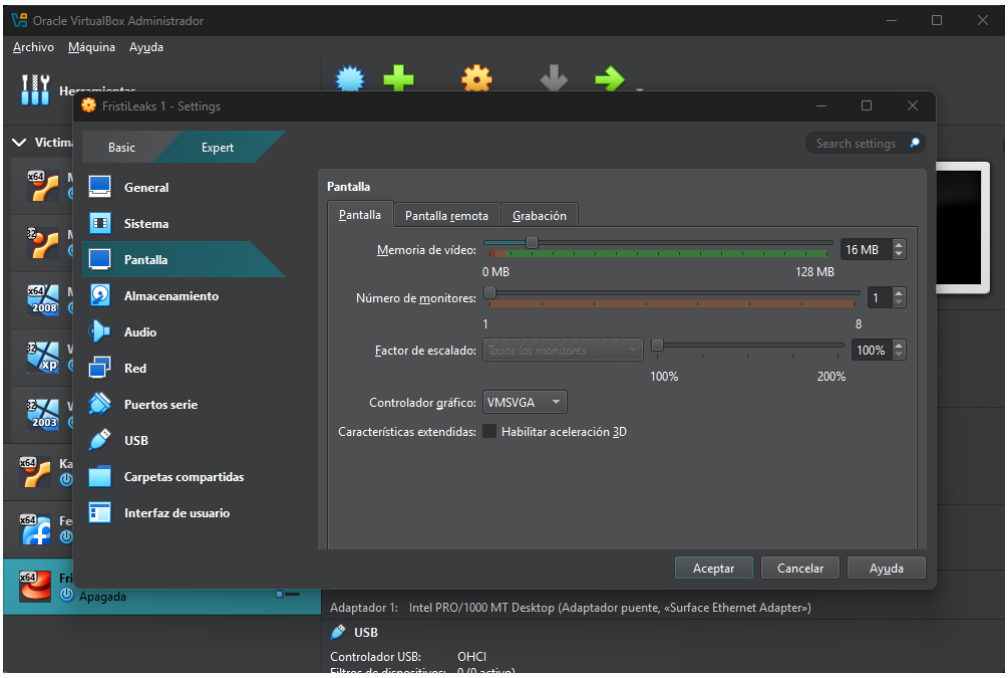
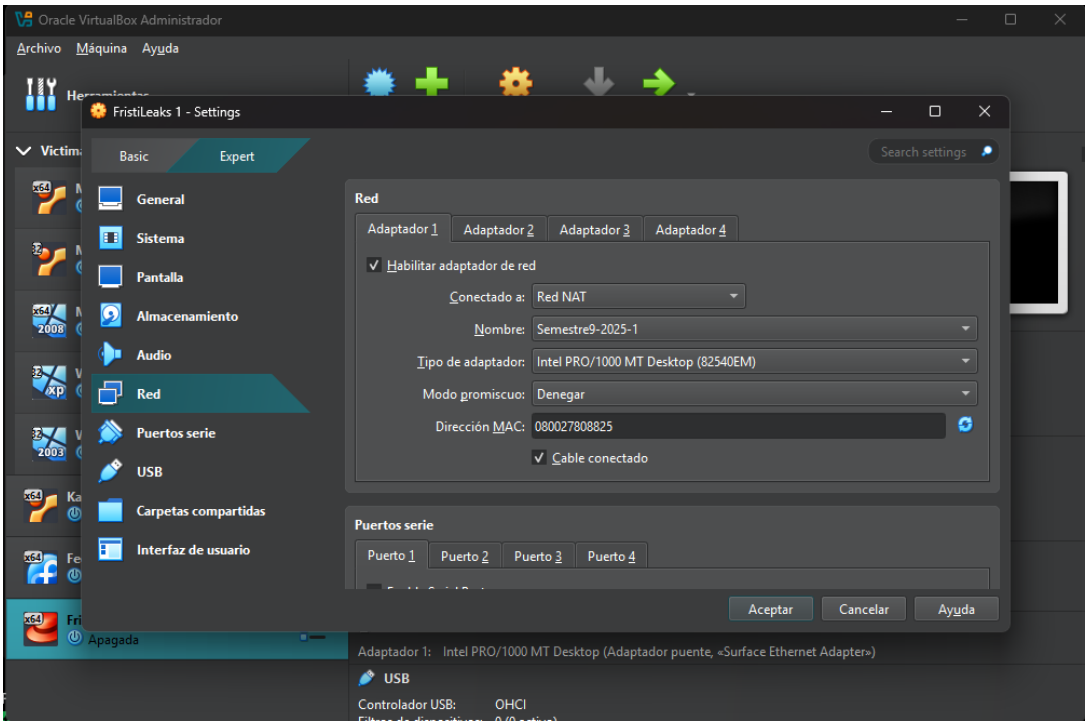


Ilustración 5 Configuración de pantalla



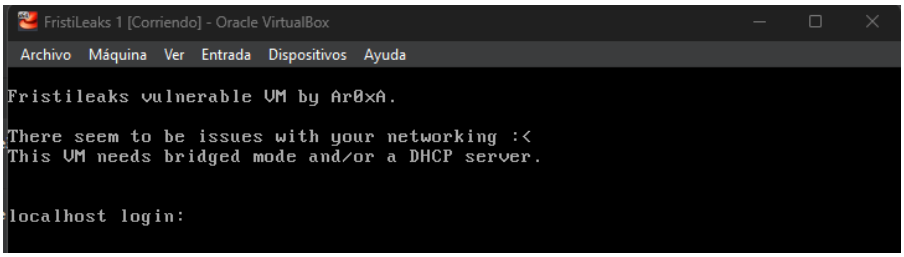
Luego se procede a modificar el adaptador de red, cambiándolo de adaptador puente a Red NAT que es donde están las demás máquinas virtuales.

Ilustración 6 Configuración de red



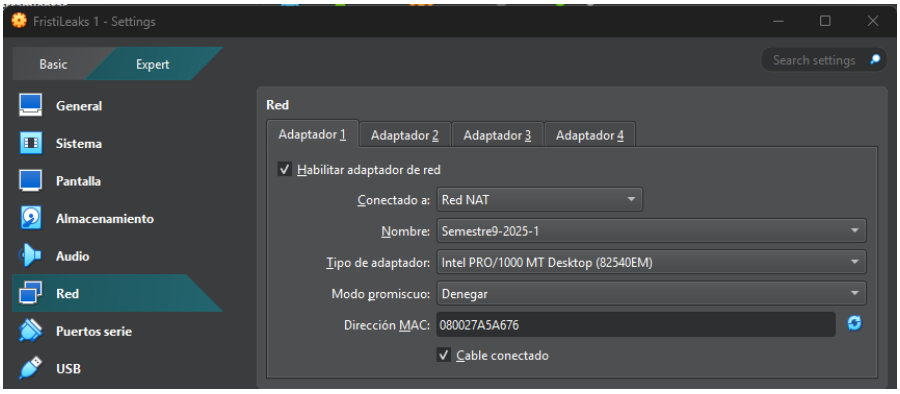
Una vez hecho esto, se inicia la máquina virtual, como se observa aparece un mensaje que indica que FristiLeaks no tiene dirección IP

Ilustración 7 Primer inicio de FristiLeaks



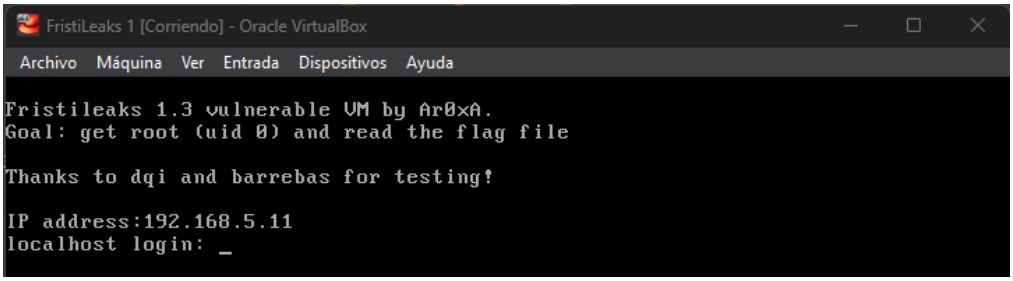
Esto se debe a que para que FristiLeaks pueda obtener una dirección IP, se le debe modificar la dirección MAC que se adquiere por defecto por la siguiente **080027A5A76** esta es una dirección MAC ya establecida.

Ilustración 8 Cambio de dirección MAC FristiLeaks



Luego de la modificación de la dirección MAC se inicia la maquina nuevamente y se observa que esta vez si obtiene dirección IP, que es la siguiente: **192.168.5.11.**

Ilustración 9 Segundo inicio de FristiLeaks



Ping Kali - FristiLeaks

Luego se hace un ping desde Kali para probar conectividad entre Kali y FristiLeaks.

Ilustración 10 Ping Kali-FristiLeaks

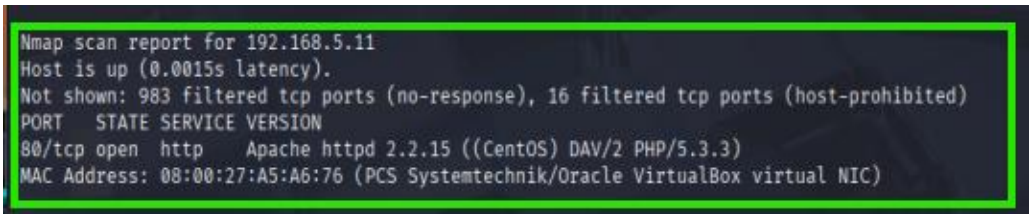
Escaneo y búsqueda de vulnerabilidades

Una vez se tiene conectividad entre ambas máquinas se procede a hacer un escaneo de la red, para verificar puertos y servicios abiertos, esto se hace utilizando el comando: **nmap -sV 192.168.5.0/24**

Ilustración 11 Escaneo de red

Del escaneo resultante se observa que la maquina o dispositivo con la dirección IP **192.168.5.11** que corresponde a FristiLeaks, tiene el puerto 80 (Apache2) abierto.

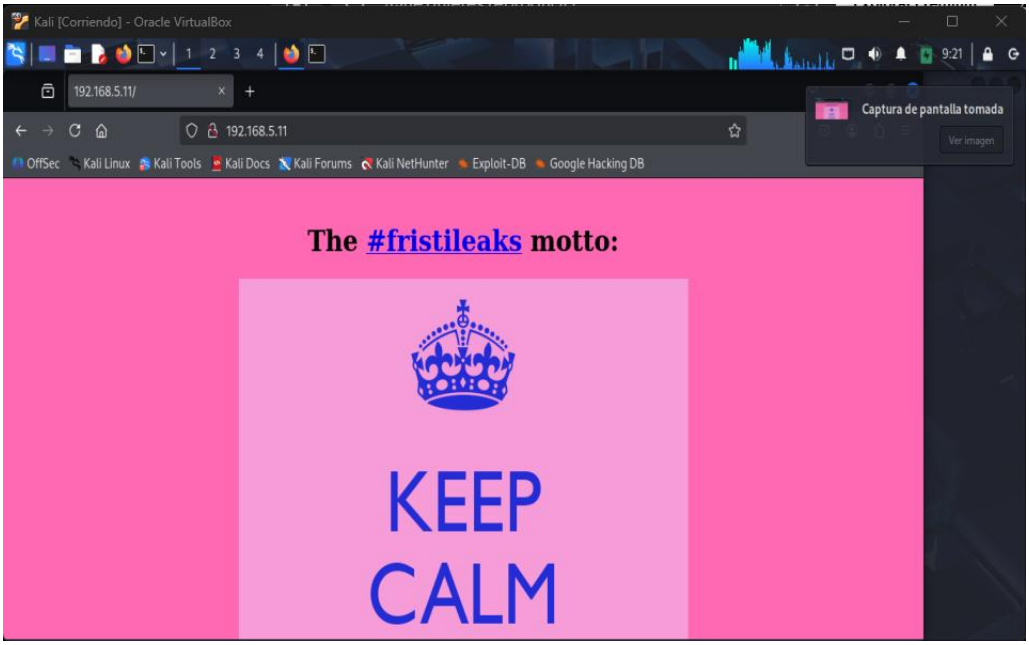
Ilustración 12 Servicios y puertos abiertos FristiLeaks



Ingreso a servicio Apache2 FristiLeaks

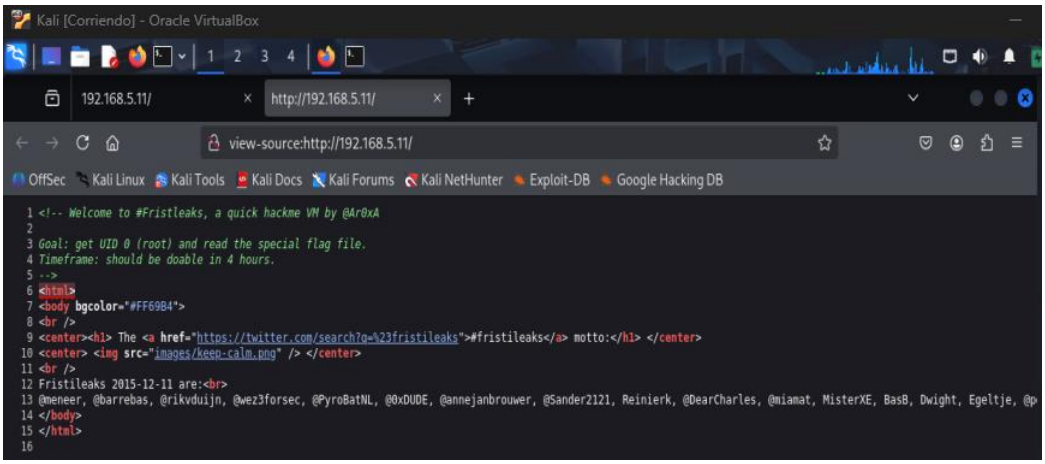
Luego de que se sabe que el puerto 80 está abierto, se procede a ingresar a el navegador de preferencia y en el buscador se ingresa la dirección IP de FristiLeaks y eso lleva a un sitio web que es el siguiente:

Ilustración 13 Sitio web FristiLeaks



Se procede a dar click derecho sobre cualquier parte del sitio web para inspeccionar la estructura de este y ver que vulnerabilidades se encuentran. El resultado es el siguiente:

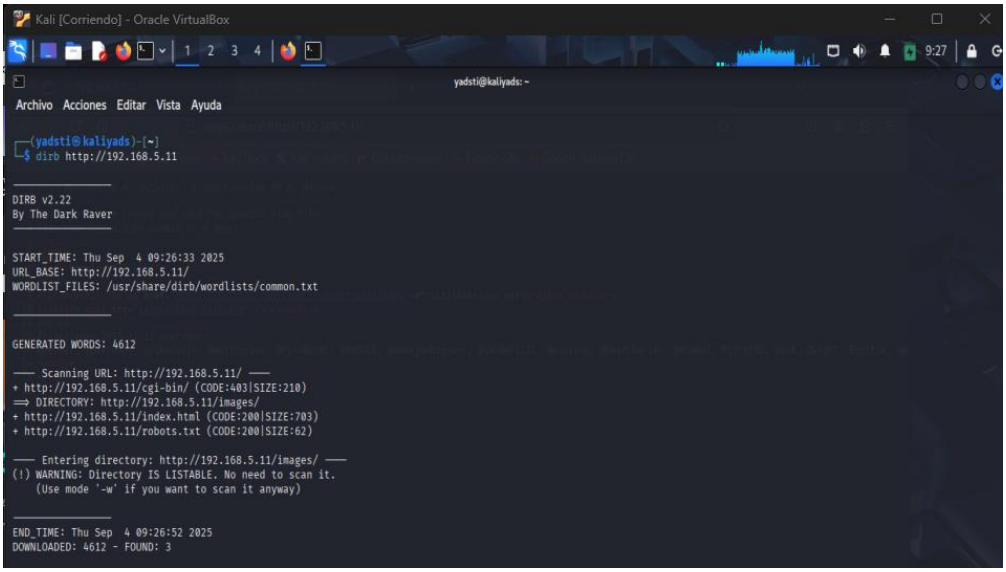
Ilustración 14 Inspección de código



Como se observa en la ilustración anterior no hay mucho que destacar, solo se encuentra información básica del sitio, url de twitter y una url que contiene la imagen que se muestra en el sitio.

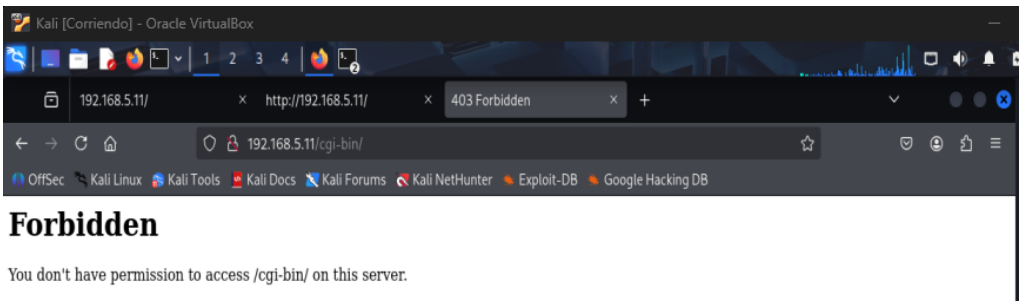
Para escanear un poco más a fondo hay que dirigirse a una terminal en Kali y utilizar el siguiente comando **dirb http://192.168.5.11/** con el fin de identificar subdominios o directorios ocultos, los cuales debido a sus características no se ven a simple vista.

Ilustración 15 Escaneo de subdominios



Como se observa en la ilustración anterior se obtienen 4 subdominios, la tarea ahora consiste en ingresar a cada uno de estos subdominios para ver qué información de utilidad se puede encontrar para ingresar a este sitio web o al sistema donde se aloja.

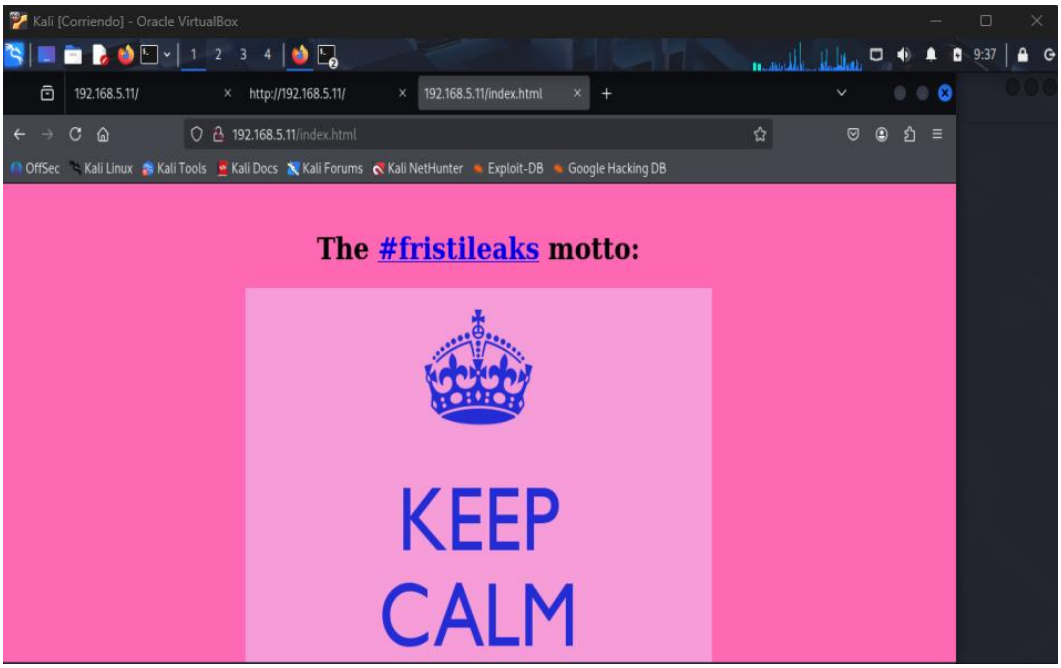
Ilustración 16 Ingreso subdominio cgi-bin/



Se observa en la ilustración anterior que aparece un mensaje que indica que no se tienen permisos para acceder a dicho enlace.

Se prueba con el siguiente.

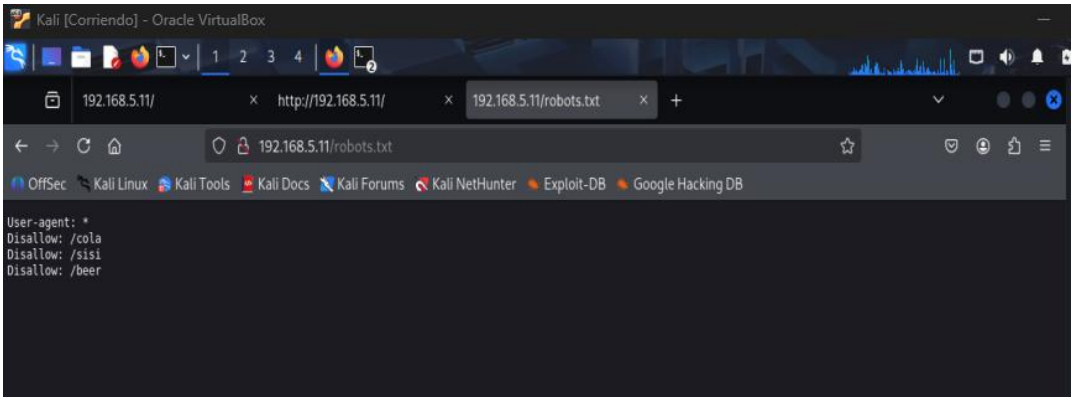
Ilustración 17 Subdominio index.html



El segundo subdominio que en realidad es el princIPal contiene el home page.

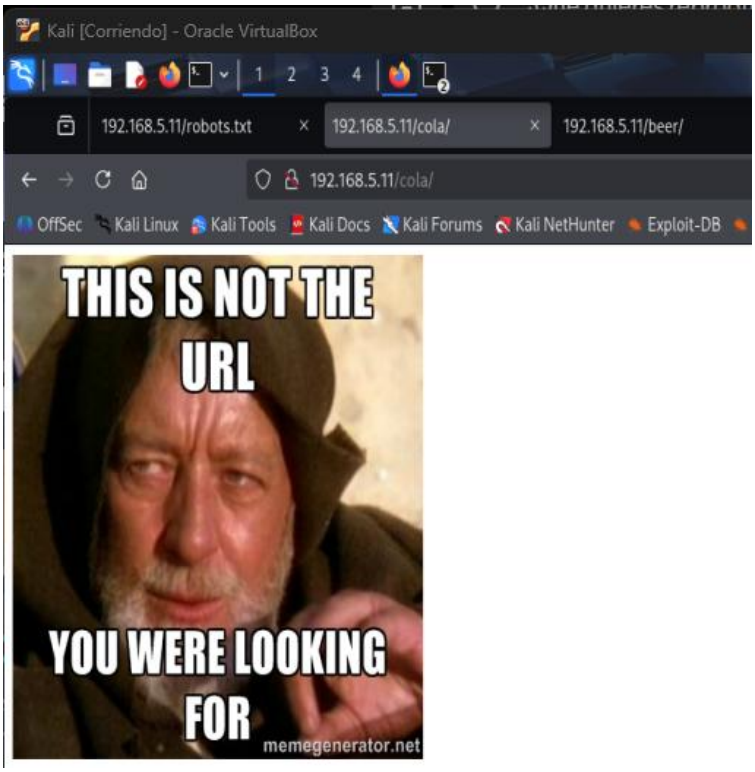
Se prueba el siguiente.

Ilustración 18 Subdominio robots.txt



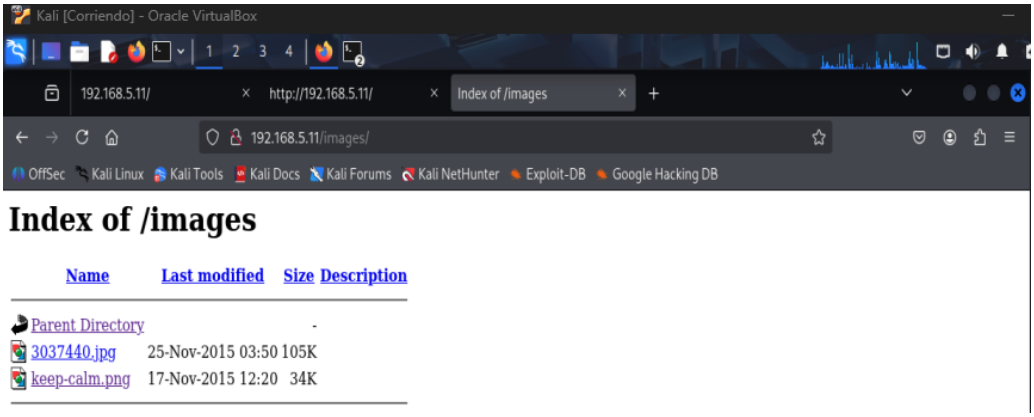
Este subdominio contiene algunos datos que podrían ser subdominios también, solo que están deshabilitados, para salir de dudas se procede a modificar el enlace con cada de uno de estos, al ingresar a cada uno de estos aparece la siguiente imagen en forma de burla.

Ilustración 19 Subdominios robots/cola



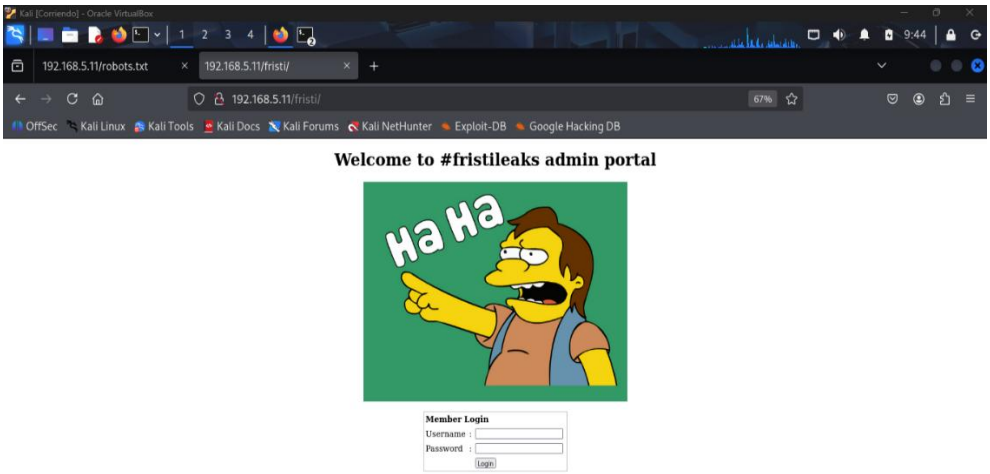
No es nada de importancia, entonces se continua con el siguiente, que como se observa es un directorio de imágenes.

Ilustración 20 Directorio de imágenes



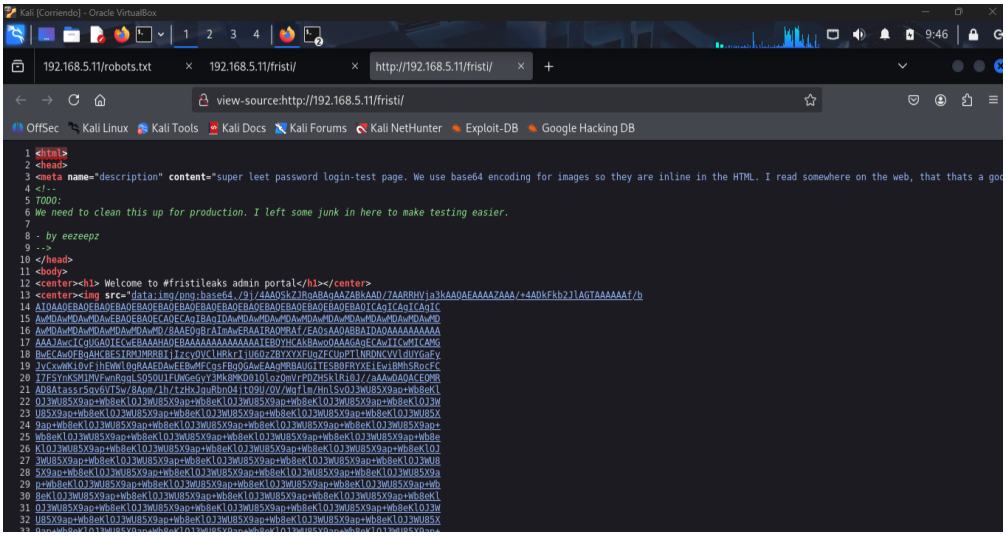
Por último, se intenta con el subdominio **fristi**, como se observa se obtiene acceso al portal administrativo.

Ilustración 21 Portal administrativo



Se intenta iniciar sesión múltIPles veces con usuarios y contraseñas genéricas como: **Admin:Admin, admin:admin, admin123:admin123, admin:password**, entre otros, pero con ninguno se obtiene un acceso satisfactorio, entonces se procede a inspeccionar el código de origen del panel con el fin de encontrar alguna vulnerabilidad o algún dato que pueda ser de ayuda para ingresar al panel administrativo.

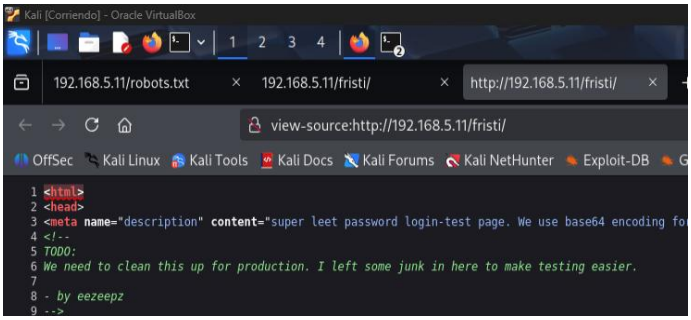
Ilustración 22 Inspección admin panel



Al hacer esta información se encuentra material importante y sustancioso como, por ejemplo:

1. Comentario dejado por un usuario **ezzeepz**

Ilustración 23 Usuario encontrado



2. En la url de la imagen se observa que esta tiene codificación base 64.
3. Comentario cifrado:

Contenido comentario cifrado

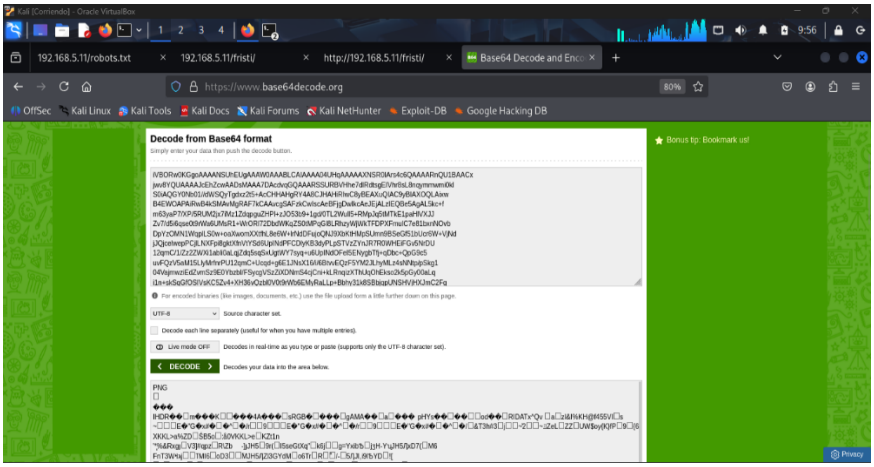
iVBORw0KGgoAAAANSUhEUgAAAW0AAABLCAIAAAA04UHqAAAAAXNSR0I
Ars4c6QAAAARnQU1BAACxjwv8YQUAAAAJcEhZcwAADsMAAA7DAcdvqGQAA
ARSSURBVHhe7dlRdtsgEIVhr8sL8nqymmwmi0klS0iAQGY0Nb01//dWSQyTgdxz2t5
+AcCHHAHgRY4A8CJHAHiRIwC8yBEAXuQIAC9yBIAXOQLEQBe5AgC9yBIAXOQLFjgDwIeB
wB4kSMAvMgRAF7kCAAvcgSAFzkCwIscAeBFjgDwIkcAeJEjALzIEQBe5AgAL5kc
+fm63yaP7/XP/5RUM2jx7iMz1ZdqpguZHPl+zJO53b9+1gd/0TL2Wull5+RMpJq5tMTk
E1paHlVXJJZv7/d5i6qse0t9rWa6UMsR1+WrORl72DbdWKqZS0tMPqGl8LRhzyWjWk
TFDPXFmulC7e81bxnNOvbDpYzOMN1WqplLS0w+oaXwomXXtfhL8e6W+lrNdDFuj
oQNJ9XbKtHMpSUmn9BSeGf51bUcr6W+VjNdjJQjcelwepPCjlLNXFpi8gktXfnVtYSd
6UpINdPFCDlyKB3dyPLpSTVzZYnJR7R0WHEiFGv5NrDU12qmC/1/Zz2ZWXi1abli0
aLqjZdq5sqSxUgtWY7syq+u6UpINdOFeI5ENygbTfj+qDbc+QpG9c5uvFQzV5aM15Ll
yMrfnrPU12qmC+Ucqd+g6E1JNsX16/i/6BtvvEQzF5YM2JLhyMLz4sNNtp/pSkg104Va
jmwziEdZvmSz9E0YbzbI/FSycgVSzZiXDNmS4cjCni+kLRnqizXThUqOhEkso2k5pGy
00aLqi1n+skSqGfOSIVsKC5Zv4+XH36vQzbl0V0t9rWb6EMyRaLLp+Bbhy31k8SBbjq
pUNSHVjHXJmC2FgtOH0drysrz404sdLPW1mulDLUdSpdEsk5vf5Gtqg1xnfX88tu/PZy
7VjHXJmC21H9lWvBBfdZb6Ws30oZ0jk3y+pQ9fnEG4lNOco9UnY5dqxrhk0JZKezwd
Nwqfnv6AOUN9sWb6UMyR5zT2B+lwDh++Fl3K/U+z2uFJNWNcMmhLzUe2v6n/dA
WG+mLN9KGWI9EcKsMJl6o6+ecH8dv0Uu4PnkqDl2rGuiS8HKul9iMrFG9gqa/VTB8
qORLuSTqF7fYU7tgsn/4+zfhV6aiiIsczlGrGvGTIlsLLhIPbnh6KnLDU12qmD+0cKQ8n
unpVcZ21Rj7erEz0WqoZ+5IRW1oXNB3Z/vBMWulSfYlm+hDLkcIAtuHEUzu/l9l867
X34rPtA6lmLi0ZrqX6gu37aIukRkVaylRfqpk+9HNkH85hNocTKC4P31Vebhd8fy/VzO
TCkqeBWlrrFheEPdMjO3SSys7XVF+qmT5UcmT9+Ss//fyyOLU3kWoGLd59ZKb6Us1
0IZMjAP5b5AgAL3IEgBc5AsCLHAHgRY4A8CJHAHiRIwC8yBEAXuQIAC9yBIAX
OQLAixwB4EWOAPAiRwB4kSMAvMgRAF7kCAAvcgSAFzkCwIscAeBFjgDwIkcAeJEj

JEjALzIEQBe5AgAL3IEgBc5AsCLHAHgRY4A8Pn9/QNa7zik1qtycQAAAABJR
U5ErkJggg==

4. Se identifica que el formulario de registro utiliza el método post y además de eso está en un archivo cheklogin.php que puede tener la validación del formulario entre otras cosas.
5. Se identifica el nombre de los campos del formulario con sus id, estos id son importantes porque pueden ser nombres de columnas en la base de datos donde se almacenan los datos.

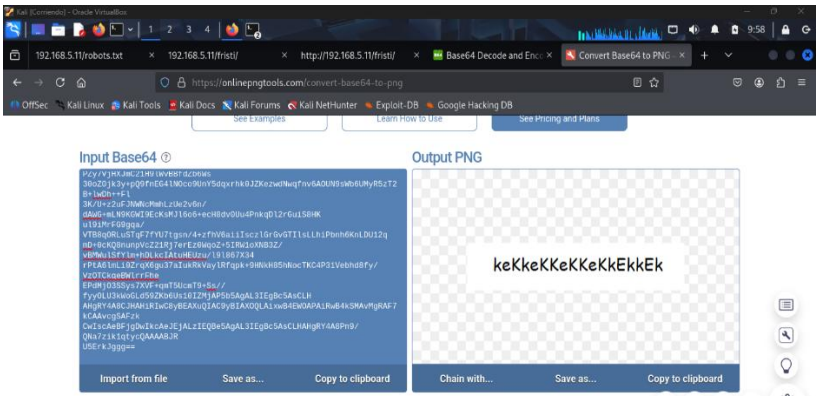
Teniendo esto en cuenta se abre otra pestaña del navegador y se base64 decode, con el fin de decodificar el contenido encontrado en el comentario.

Ilustración 24 Decodificación de comentarios



Al decodificar el contenido del comentario se obtiene que lo que está codificado es un archivo de extensión **.PNG,** sabiendo esto en la barra de búsqueda buscamos un decodificador de base 64 a png.

Ilustración 25 Decodificación de base 64 a PNG



Al descifrar el contenido se obtiene una imagen con un conjunto de caracteres, estos se copian a texto plano = **kekkeKKeKKeKkEkkEk**. Esta podría ser la contraseña del usuario identificado anteriormente.

Se toma el nombre de usuario que dejó el mensaje para producción y el texto que se desencrIPtó de la imagen para iniciar sesión, el inicio sesión es exitoso.

Ilustración 26 Inicio de sesión con credenciales encontradas

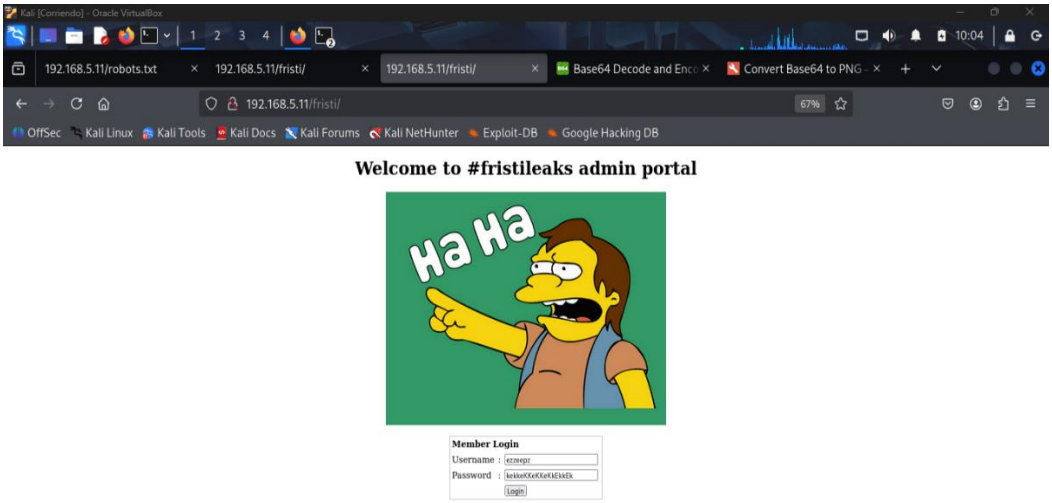
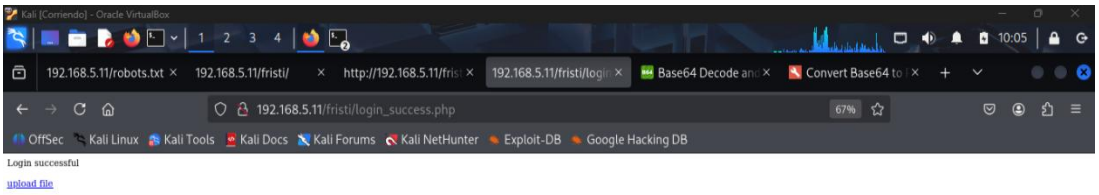
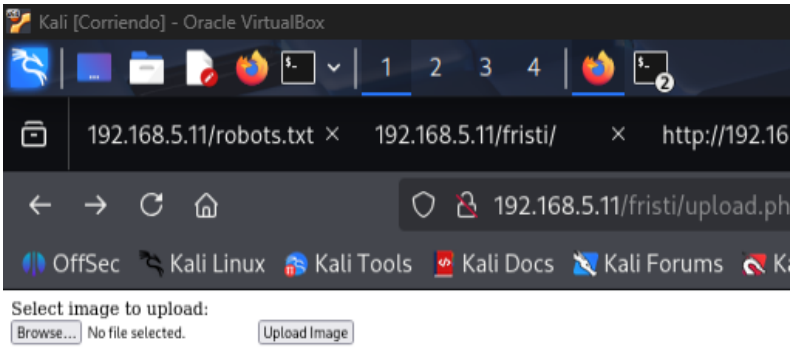
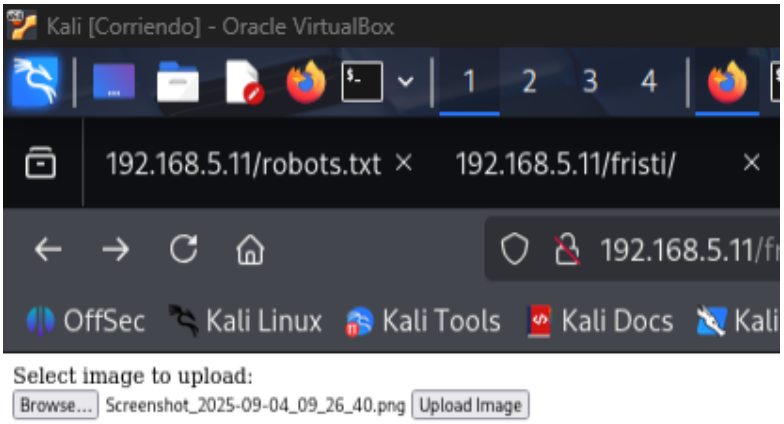


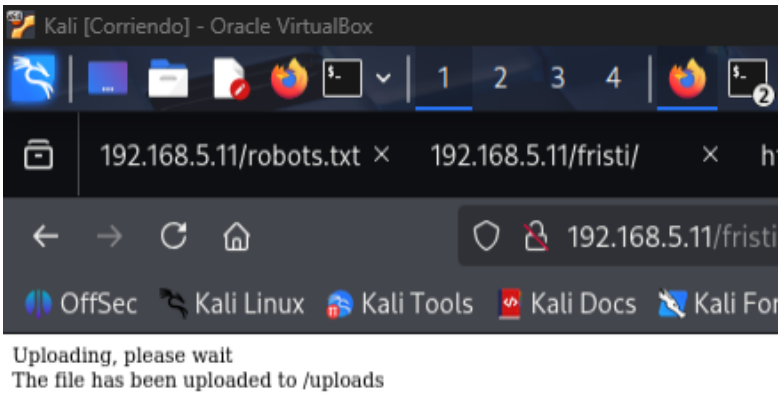
Ilustración 27 Inicio de sesión exitoso



Se observa que al iniciar sesión aparece la opción de cargar archivos, para probar se procede a cargar una imagen.







Se ingresa al subdominio **/uploads** con el fin de verificar que el archivo si se subió, pero cuando se ingresa aparece que no, luego se intenta subiendo un archivo con otra extensión y no es posible, solo se admiten extensiones **.PNG, .GIF, .JPG**, esto es suficiente para ejecutar el ataque.

Ahora se procede a buscar las herramientas y a crear un archivo con terminación en una de esas extensiones para realizar un ataque.

Creación de archivo

Para crear el archivo que se va a subir al portal, es necesario utilizar una de las herramientas o scrIPts preparados que ya trae Kali, en este caso se utilizará el **php-reverse-shell.php,** este al cargarse y ejecutarse da acceso a la máquina donde está alojado el portal.

Ilustración 28 Búsqueda de herramientas

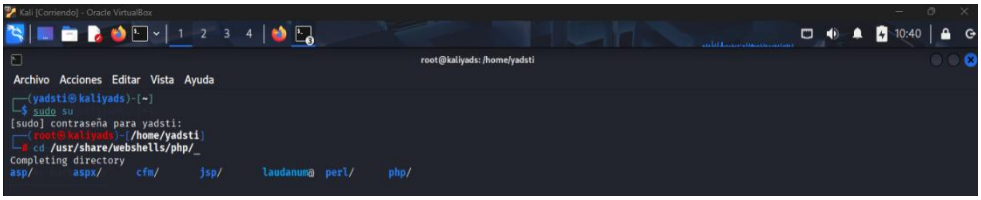


Ilustración 29 Selección de herramienta

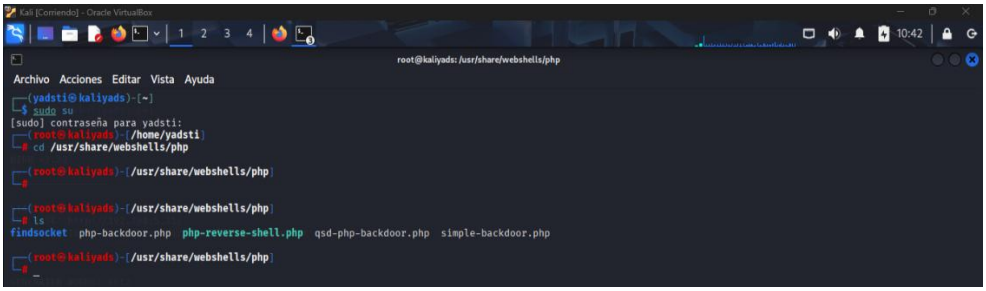
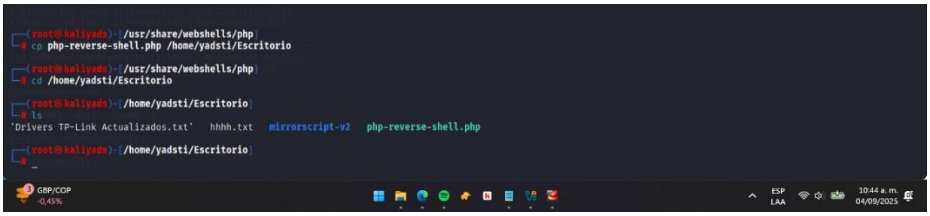
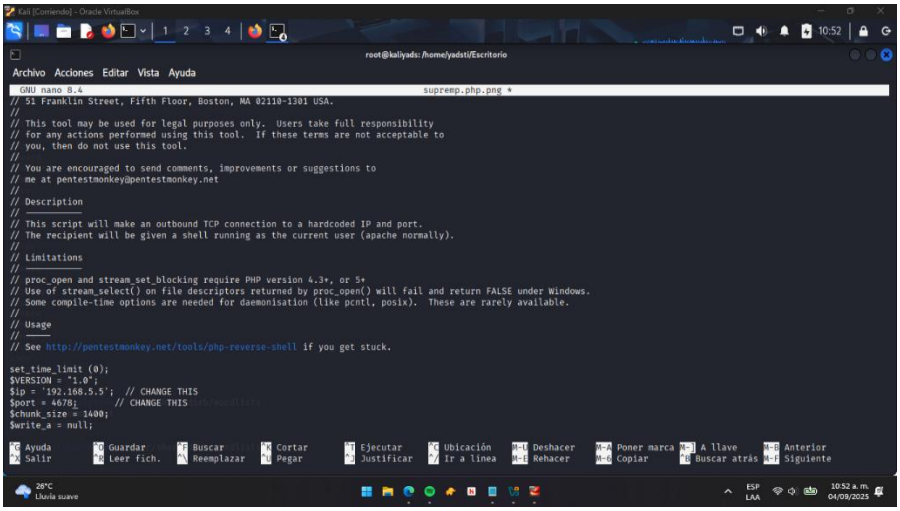


Ilustración 30 Movimiento de herramienta



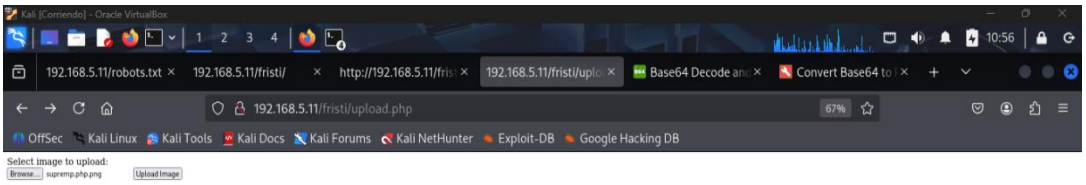
Posteriormente se copia el scrIPt en el escritorio se ingresa al scrIPt y se modifica tanto la dirección IP y como el puerto de escucha, como se evidencia en la siguiente ilustración.

Ilustración 31 Modificación del scrIPt



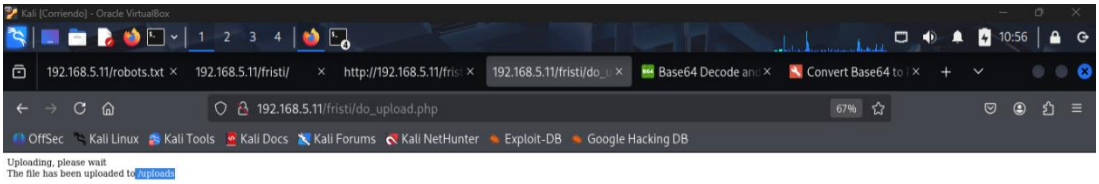
Despues de modificar el scrIPt, este se renombra como **supreme.php.png** y se carga en el portal.

Ilustración 32 Carga de scrIPt en el portal



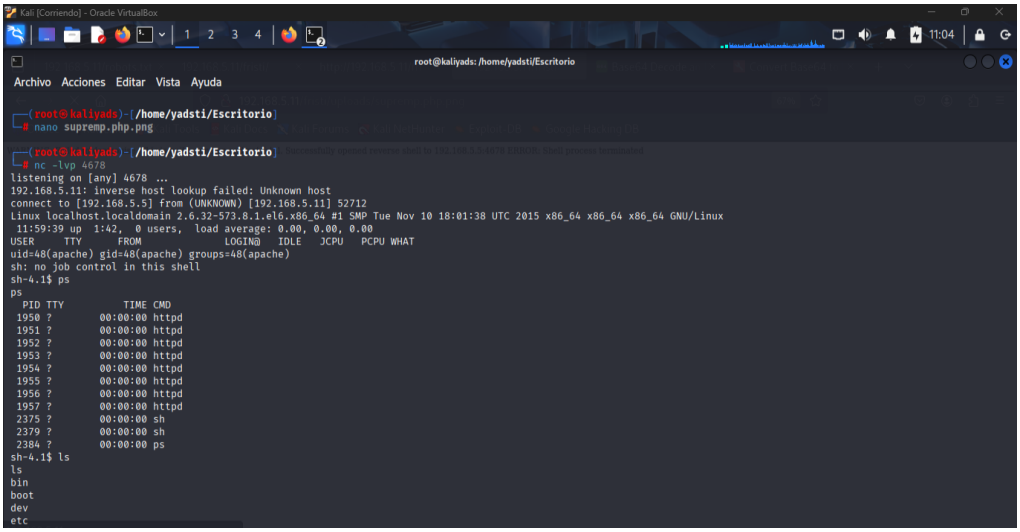
Se observa que el scrIPt enmascarado se cargó.

Ilustración 33 ScrIPt cargado



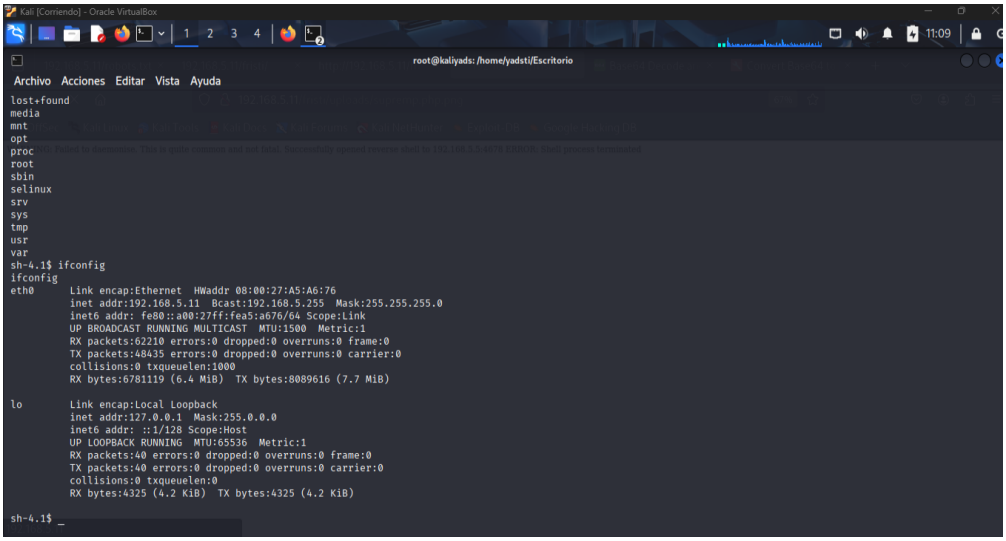
Luego se ingresa a una terminal y se utiliza el comando **nc -lvp 4678** este comando lo que va a hacer es escuchar la comunicación por el puerto anteriormente configurado a espera de que el archivo cargado sea accedido, una vez se accede al archivo se obtiene acceso a la máquina de fristileaks como se evidencia en la siguiente ilustración.

Ilustración 34 Acceso a FristiLeaks



Luego de acceder para verificar que si es la máquina, se verifica la dirección IP y como se evidencia es la correspondiente a FristiLeaks.

Ilustración 35 Verificación dirección IP



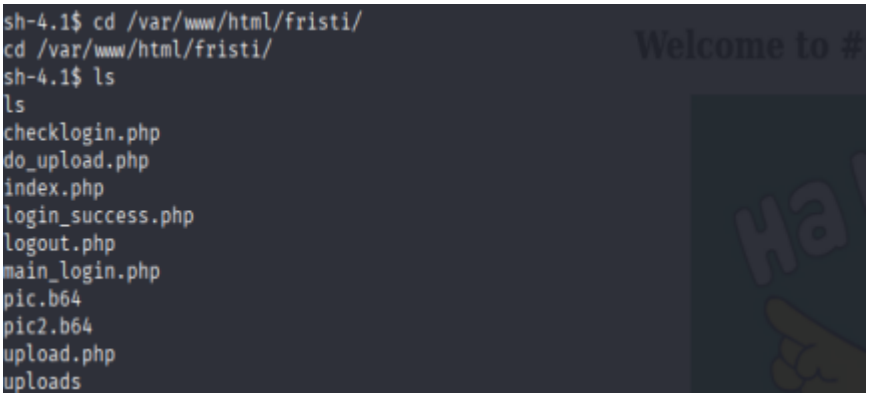
Teniendo acceso a la máquina se procede con la creación de dos usuarios.

Creación de Usuarios en FristiLeaks

Para la creación de los usuarios revisaré el archivo **cheklogin.php** ya que este puede contener información importante como usuario y contraseña del gestor de bases de datos del portal y facilitaría la inserción o creación de los dos usuarios.

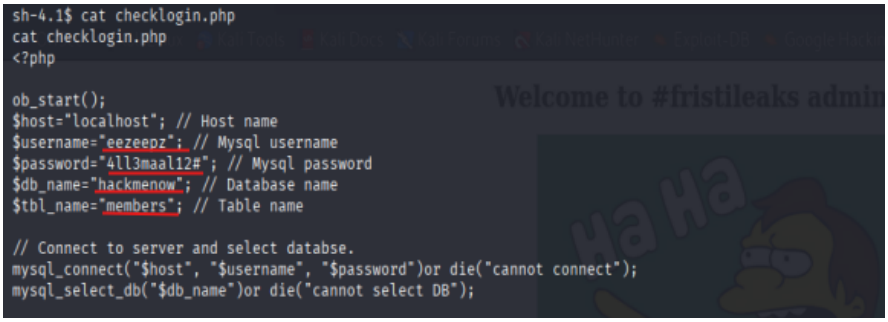
En los servidores apache los sitios webs están alojados en **/var/www/html/carperta** del sitio, en este caso se ingresa a **/var/www/html/fristi** y se observan los archivos.

Ilustración 36 Archivos fristi



Se hace un **cat** al archivo de **cheklogin.php** y como se evidencia en la siguiente imagen, se encuentran el nombre de usuario, el host, la contraseña, el nombre de la base de datos y el nombre de la tabla de donde se almacenan las credenciales, están resaltados en rojo.

Ilustración 37 Cat cheklogin



Con esto, ahora se procede a iniciar sesión en mysql, mirar la estructura de la tabla y crear los dos usuarios.

Ilustración 38 Creación de los dos usuarios

```
sh-4.1$ mysql -u eezeepz -p'4ll3maal12#' -e "USE hackmenow; SELECT * FROM members;"
s;"ql -u eezeepz -p'4ll3maal12#' -e "USE hackmenow; SELECT * FROM member
id      username        password
1       eezeepz keKkeKKeKKeKkEkkEk
sh-4.1$ mysql -u eezeepz -p'4ll3maal12#' -e "USE hackmenow; DESCRIBE members;"
mysql -u eezeepz -p'4ll3maal12#' -e "USE hackmenow; 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
sh-4.1$ mysql -u eezeepz -p'4ll3maal12#' -e "USE hackmenow; INSERT INTO members (username, password) VALUES ('suppra', 'admin123');"
(username, password) VALUES ('suppra', 'admin123');"INSERT INTO members
sh-4.1$ mysql -u eezeepz -p'4ll3maal12#' -e "USE hackmenow; INSERT INTO members (username, password) VALUES ('mayimbu', 'admin123');"
(username, password) VALUES ('mayimbu', 'admin123');"NSERT INTO members
sh-4.1$ mysql -u eezeepz -p'4ll3maal12#' -e "USE hackmenow; SELECT * FROM members;"
s;"ql -u eezeepz -p'4ll3maal12#' -e "USE hackmenow; SELECT * FROM member
id      username        password
1       eezeepz keKkeKKeKKeKkEkkEk
2       suppra  admin123
3       mayimbu admin123
```

Como se observa en la ilustración anterior primero se inicia sesión, se selecciona la base de datos, se ven los registros de la tabla **members** y se observa que solo hay dos, luego se describe la estructura de la tabla para saber que campos tiene la tabla, luego se crean los dos usuarios y se muestran nuevamente los registros de la tabla **members** y ahora hay cuatro.

Se procede a ir al panel administrativo e iniciar sesión con los dos usuarios.

Ilustración 39 Inicio de sesión usuario 1

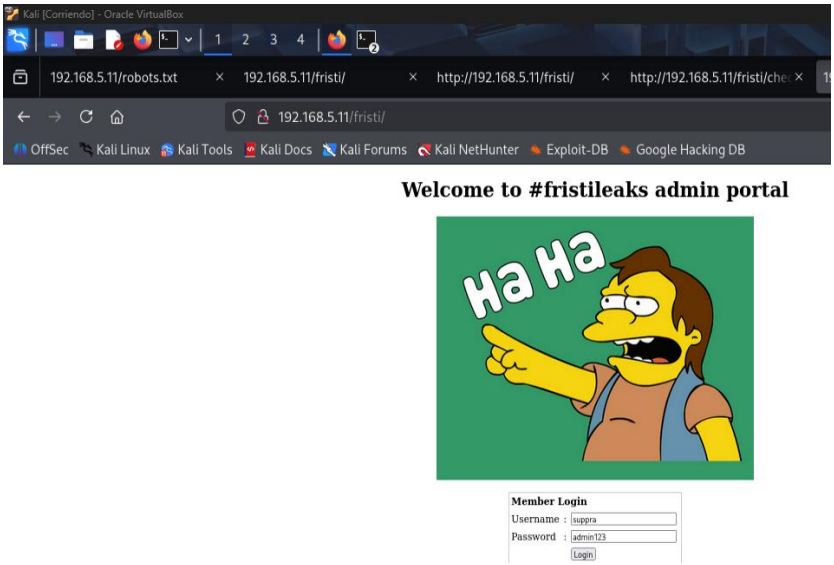


Ilustración 40 Inicio de sesión exitoso 1

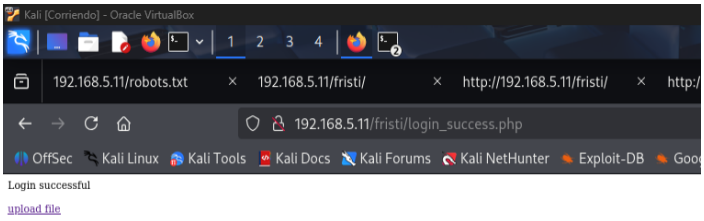


Ilustración 41 Inicio de sesión usuario 2

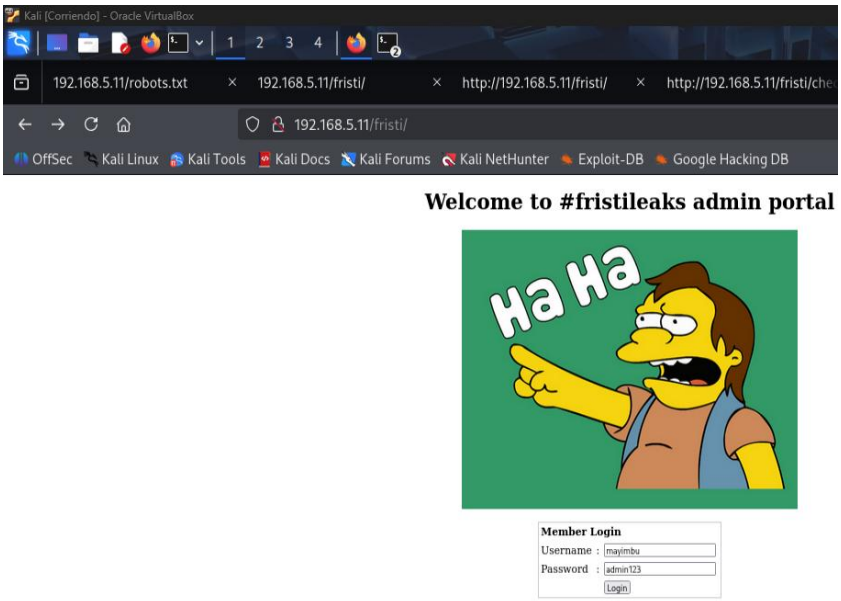
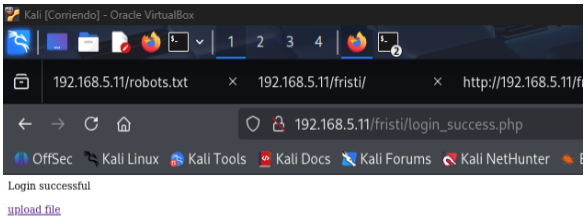


Ilustración 42 Inicio de sesión exitoso 2



De esa forma se puede ingresar a un servidor mal configurado y modificar sus datos, corromper el sistema.

Configuración de Fedora para que solo tome IP con la MAC determinada

En este apartado se configurará Fedora para que tome dirección IP de forma similar a FristiLeaks, ósea que solo tome IP cuando se le asigne una MAC especifica, con cualquier otra MAC no tomará dirección IP.

Ahora se muestra cómo funciona normalmente.

Configuración normal Fedora

En la siguiente ilustración se observa la configuración predeterminada de Fedora, tiene una RED NAT y una dirección MAC por defecto, de esta forma toma dirección IP.

Ilustración 43 Configuración normal Fedora

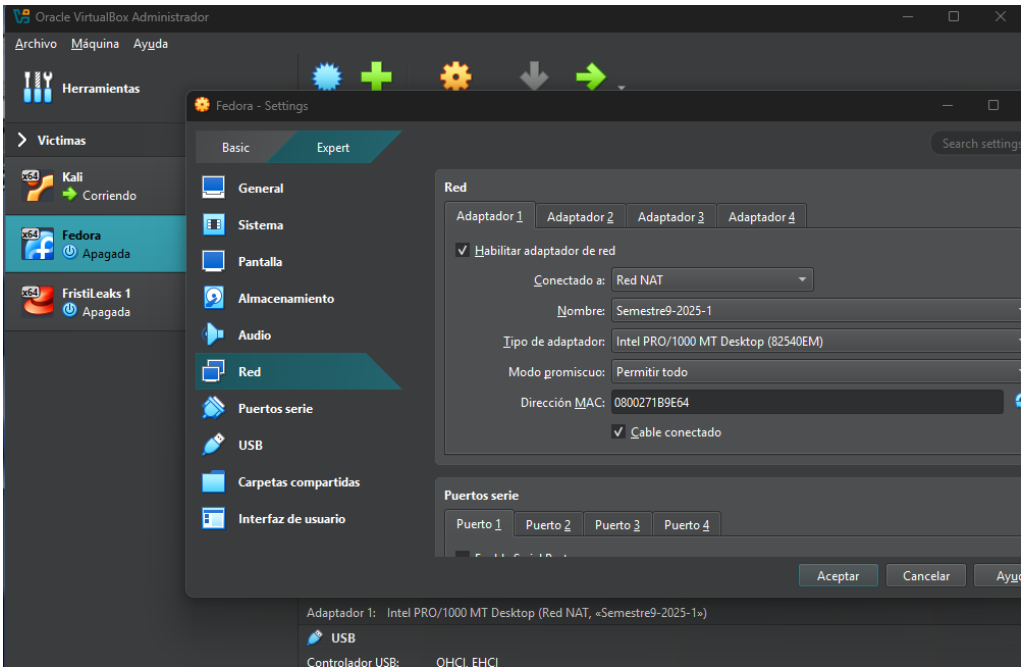
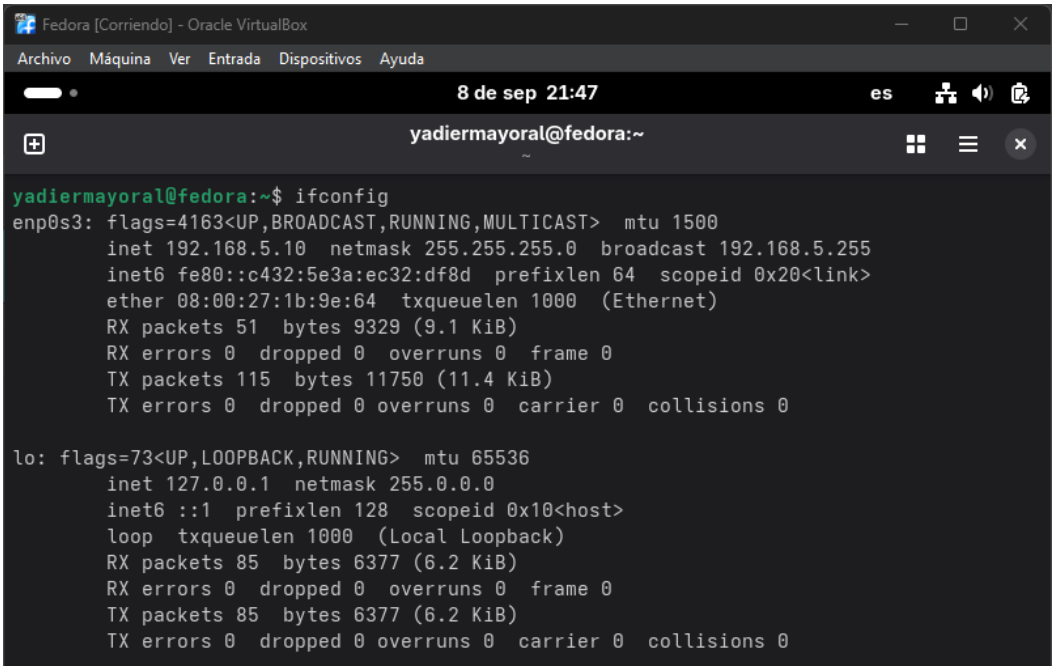


Ilustración 44 Dirección IP con Mac predeterminada



Como se observa toma dirección IP.

Modificación de Fedora

Ahora se procede a modificar Fedora para que solo tome dirección IP de la red Nat cuando la MAC sea **080027A5A76C.**

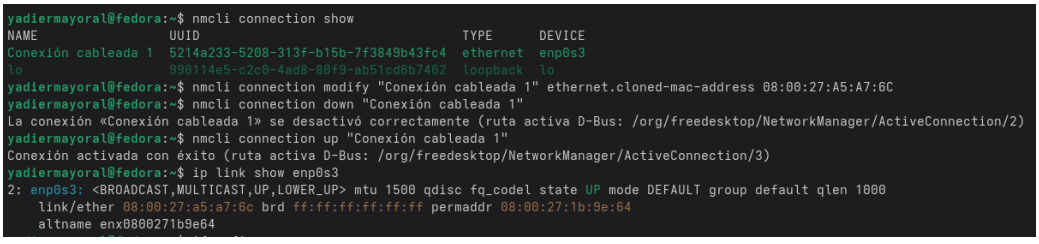
Eso se hace de la siguiente manera:

Lo primero es mostrar el nombre la conexión, en este caso es **Conexión cableada 1**.

Luego se le asigna la Mac anteriormente mencionada con el comando **nmcli connection modify "Conexión cableada 1" ethernet.cloned-mac-address 08:00:27:A5:A7:6C**.

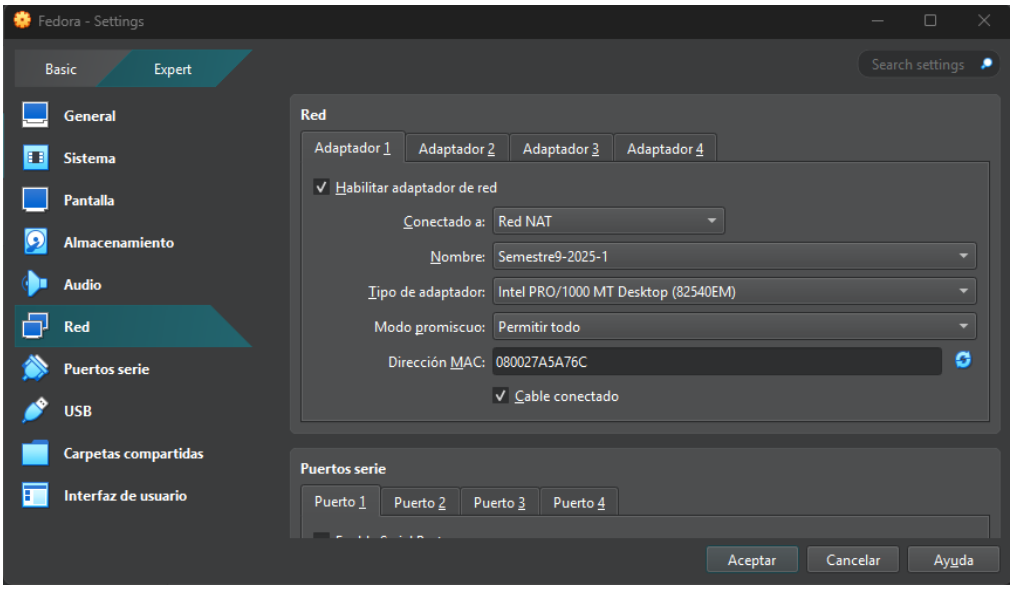
Por ultimo se reinicia la conexión.

Ilustración 45 Modificación de dirección MAC



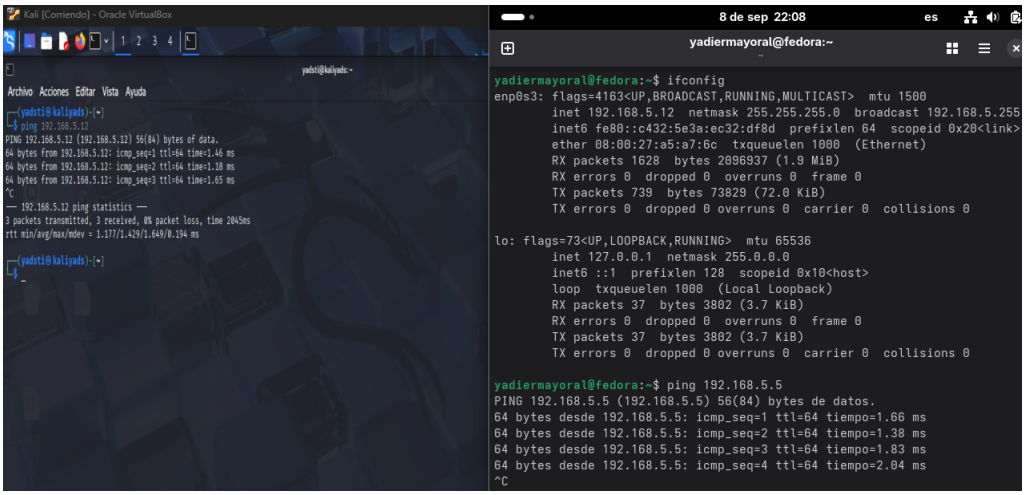
Ahora se procede a apagar la máquina de Fedora y se modifica la MAC.

Ilustración 46 Modificación MAC adaptador



Una vez encendida la maquina como se observa en la siguiente ilustración, ya toma dirección IP y tiene comunicación con Kali que está en la misma red.

Ilustración 47 Ping de confirmación



¿Qué es NC?

Netcat (abreviado NC) es una utilidad Unix que lee y escribe datos a través de la red conexiones mediante protocolo TCP o UDP. Está diseñado para ser una herramienta "back-end" que puede ser utilizada directa o fácilmente manejada por otros programas y scrIPts. Al mismo tiempo, es una red rica en funciones de depuración y exploración, ya que puede crear casi cualquier tIPo de conexión que se necesite y tiene interesantes capacidades.

Se le conoce como la “navaja suiza de las redes” porque es muy flexible y puede simular muchos comportamientos de red.

Tiene los siguientes comandos:

-c comandos de shell como `-e'; usar /bin/sh para ejecutar [¡peligroso!!]

-e archivo programa a ejecutar después de conectar [¡peligroso!!]

-b permitir broadcasts (difusión)

-g gateway punto[s] de salto de enrutamiento de origen, hasta 8

-G num puntero de enrutamiento de origen: 4, 8, 12, ...

-h muestra la ayuda

-i segs intervalo de retraso para líneas enviadas, puertos escaneados

-k establecer la opción keepalive en el socket

-l modo escucha, para conexiones entrantes

-n solo direcciones IP numéricas, sin DNS

-o archivo volcado hexadecimal del tráfico

-p puerto número de puerto local

-r aleatorizar puertos locales y remotos

-q segs salir después de EOF en stdin y retraso de segs

-s dir dirección de origen local

-T tos establecer Type Of Service (TIPo de Servicio)

-t responder negociación TELNET

-u modo UDP

-v modo detallado [usar dos veces para más detalle]

-w segs tiempo de espera para conexiones y lecturas finales de red

-C enviar CRLF como final de línea

-z modo de E/S cero [usado para escaneo]

En pocas palabras, NC sirve para conectar, escuchar y transferir datos en red de forma simple, además de ser muy útil en auditoría, administración de sistemas y pruebas de seguridad.

Comando para Calcular Cuantos Caracteres tiene un Archivo

El comando wc muestra información estadística sobre un archivo, como el número de líneas, palabras y caracteres.

Trivia: wc significa recuento de palabras.

La sintaxis del comando wc es:

wc [options] [files]

El comando wc tiene las siguientes opciones:

- –l: imprime solo el número de líneas
- –w: imprime solo el número de palabras
- -c: imprime solo el número de bytes
- –m: imprime el recuento de caracteres (diferente del número de bytes para archivos que no son de texto)
- –L: Imprime la longitud de la línea más larga del archivo.

- —files0-from=F: obtiene los nombres de los archivos del archivo F (los nombres de los archivos deben estar separados por el carácter NULL)

Conclusión

El desarrollo de este laboratorio de seguridad y auditoría de redes permitió simular un entorno real en el que fue posible aplicar técnicas de generación y ejecución de archivos maliciosos, orientados a obtener acceso remoto. A través de la implementación de una red NAT y el uso de **Kali Linux** como máquina atacante, se logró comprometer a FristiLeaks.

Con este ejercicio se reafirma la importancia de contar con configuraciones seguras y mantener un control constante sobre las aplicaciones, páginas y servicios en los equIPos, ya que incluso la simple ejecución de un archivo descargado puede otorgar control al atacante.

Referencias

Sandoval Morales, R. (2025). *Seguridad y Auditoria de Redes. Quibdó*

netcat | Kali Linux Tools. (n.d.). Kali Linux. https://www.kali.org/tools/netcat/

Davidochobits. (2021, November 4). *Uso del comando Ncat (nc) en Linux con ejemplos - ochobitshacenunbyte*. Ochobitshacenunbyte. https://www.ochobitshacenunbyte.com/2021/11/04/uso-del-comando-ncat-nc-en-linux-con-ejemplos/

Ejemplos de comandos WC: contar el número de líneas, palabras y caracteres. (n.d.). https://es.linux-console.net/?p=20171