INFORME TÉCNICO: ATAQUE CONTROLADO A FRISTILEAKS MEDIANTE SUBIDA DE ARCHIVOS Y REVERSE SHELL EN ENTORNO VIRTUALIZADO

VICTOR MANUEL LONGA MENA

UNIVERSIDAD TECNOLOGÍA DEL CHOCO "DIEGO LUIS CÓRDOBA"
FACULTAD DE INGENIERÍA
INGENIERIA DE TELECOMUNICACIONES
2720409: SEGURIDAD Y AUDITORIA DE REDES
QUIBDÓ-CHOCO (COLOMBIA)
2025

INFORME TÉCNICO: ATAQUE CONTROLADO A FRISTILEAKS MEDIANTE SUBIDA DE ARCHIVOS Y REVERSE SHELL EN ENTORNO VIRTUALIZADO

VICTOR MANUEL LONGA MENA
Estudiantes, IX semestre

ING. RAFAEL S MORALES
Docente de la asignatura

UNIVERSIDAD TECNOLOGÍA DEL CHOCO "DIEGO LUIS CÓRDOBA"
FACULTAD DE INGENIERÍA
INGENIERIA DE TELECOMUNICACIONES
2720409: SEGURIDAD Y AUDITORIA DE REDES
QUIBDÓ-CHOCO (COLOMBIA)
2025

Tabla de Contenido

Tabla de Figuras

Tabla de Tabla

Introducción

En este informe se recoge paso a paso la práctica realizada dentro del laboratorio de auditoría de redes, donde el reto principal fue trabajar con la máquina vulnerable FristiLeaks y aplicar diferentes técnicas de hacking ético. Todo el proceso se llevó a cabo en un entorno controlado de máquinas virtuales, utilizando VirtualBox para simular tanto la máquina víctima como la máquina atacante. De esta manera, se pudo experimentar de manera segura con configuraciones de red, pruebas de vulnerabilidad y explotación de servicios.

La primera parte de la práctica consistió en configurar la red con NAT y modificar la dirección MAC de Edubuntu, con el fin de garantizar que la máquina trabajara únicamente con una dirección fija y que la conectividad quedara bajo control. Este paso inicial fue importante porque sirvió de base para que después todo funcionara correctamente entre las máquinas virtuales y se pudiera realizar la conexión hacia el servidor víctima.

Posteriormente se hizo un reconocimiento de la red empleando herramientas como Nmap, que permitieron descubrir los servicios activos y versiones en ejecución dentro del segmento configurado. A partir de ahí se localizaron puertos abiertos y se identificó el servidor web vulnerable. Con ayuda de Dirb, se exploraron directorios ocultos y se detectaron rutas que más adelante servirían como puerta de entrada.

La parte más interesante vino cuando se trabajó con la subida de archivos maliciosos. Se preparó un archivo de tipo reverse shell en PHP, disfrazado con extensión de imagen, para aprovechar la vulnerabilidad en el sistema de carga del sitio. Al lograr subir y ejecutar este archivo, se estableció una conexión inversa que dio acceso remoto al servidor FristiLeaks, abriendo así la posibilidad de navegar por sus directorios y explorar archivos sensibles.

Finalmente, se consiguió ingresar a la base de datos MySQL del sistema, utilizando credenciales descubiertas en el proceso. Una vez dentro, se identificó la base de datos de la aplicación web y se manipuló la tabla members, insertando nuevos usuarios de prueba. Para verificar el éxito del procedimiento, se probaron las cuentas creadas en el portal de FristiLeaks y efectivamente funcionaron, confirmando que se había logrado el objetivo de comprometer el sistema y tomar control sobre los registros de usuario.

Alcance

El informe abarca un período de trabajo de 4 días, comprendido entre el jueves 4 de agosto de 2025 y el martes 9 de agosto de 2025, fecha en la cual se dio por concluido el proceso de prácticas. Durante este tiempo se llevó a cabo la configuración inicial de las máquinas virtuales en VirtualBox, se realizaron las pruebas de conectividad y escaneo de servicios, y se desarrollaron ejercicios de explotación controlada sobre la máquina vulnerable FristiLeaks. Además, se recopilaron evidencias en forma de capturas de pantalla, salidas de comandos y fragmentos de configuraciones, con el objetivo de documentar de manera clara cada paso del procedimiento. Además de esto, toda la información obtenida fue organizada en este informe, con el propósito de dejar constancia del trabajo realizado y servir como material de consulta y estudio en futuras evaluaciones académicas.

1. Objetivos

1.1.General

. aplicar técnicas de auditoría de seguridad en entornos virtualizados mediante la configuración de red, el uso de comandos en Kali Linux y la explotación controlada de vulnerabilidades en la plataforma FristiLeaks, con el fin de comprender los riesgos asociados y comprobar métodos de acceso y manipulación de datos en sistemas vulnerables.

1.2.Específicos

- Configurar la red en entornos virtualizados (VirtualBox con NAT) y asignar direcciones MAC fijas, garantizando conectividad controlada entre la máquina atacante y la máquina víctima.
- Identificar y escanear servicios activos en la red con Nmap, reconociendo puertos abiertos y posibles puntos de acceso en el servidor vulnerable.
- Subir y ejecutar una reverse shell en PHP disfrazada como archivo de imagen, estableciendo comunicación remota con el sistema víctima.
- Acceder al sistema de gestión de bases de datos MySQL y manipular la información en la tabla members, logrando crear usuarios válidos y comprobar su acceso al portal web.

2. Planteamiento Del Problema

En la actualidad, los sistemas informáticos y las aplicaciones web se enfrentan constantemente a intentos de intrusión que buscan aprovechar fallos de seguridad para acceder de manera no autorizada a información sensible. Muchas organizaciones, por desconocimiento o descuido, mantienen servidores y aplicaciones con vulnerabilidades que pueden ser explotadas fácilmente mediante técnicas conocidas y al alcance de cualquier atacante con conocimientos básicos.

Uno de los principales retos en el ámbito de la seguridad informática es la falta de experiencia práctica de los estudiantes y profesionales en el manejo de herramientas de auditoría, pruebas de penetración y explotación de vulnerabilidades. Si bien existen teorías y marcos conceptuales que explican los riesgos, solo mediante la experimentación en entornos controlados es posible comprender realmente cómo operan los ataques, cuáles son las fases que los componen y qué consecuencias pueden tener.

El problema radica en que, sin un acercamiento práctico, los futuros profesionales de la informática carecen de la capacidad de identificar, prevenir y mitigar riesgos reales en sistemas expuestos a internet. De allí surge la necesidad de desarrollar prácticas con máquinas vulnerables como **FristiLeaks**, que permiten simular de manera ética y segura escenarios de intrusión. Este tipo de ejercicios no solo revelan lo fácil que puede ser vulnerar un sistema mal protegido, sino que también resaltan la urgencia de aplicar medidas preventivas en la administración de servidores y bases de datos.

En este contexto, el presente trabajo busca dar respuesta a la siguiente pregunta central: ¿Cómo aplicar herramientas y técnicas de auditoría informática en un entorno virtualizado

controlado, para comprender el proceso de explotación de vulnerabilidades en aplicaciones web y bases de datos?

3. Capítulo 1: Cambio y Asignación de Dirección MAC en Edubuntu Para la Virtualización con NAT

Para poder realizar el cambio y asignación de mi dirección mac y que solo entregue una ip dhcp o desde una red NAT lo primero que hacemos es ingresar nuestro virtualbox de la siguiente manera.

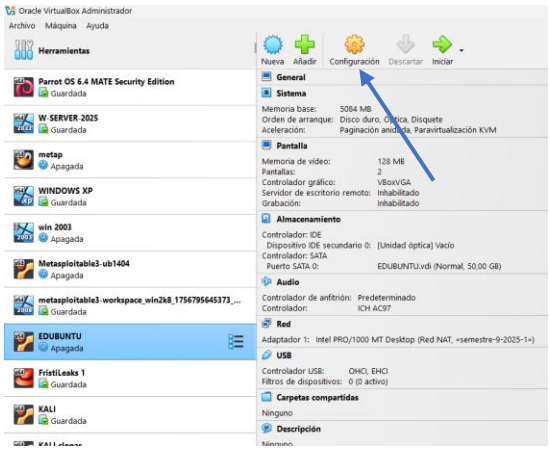


Figura 1. Visualización Virtualbox

Estand en este apartado, seleccionamos nuestra maquina (en este caso será Edubuntu) en la que queremos hacer esto, pero en vez de arrancarla como normalmente hacemos, lo que realizaremos es ir la configuración (Flecha Azul)

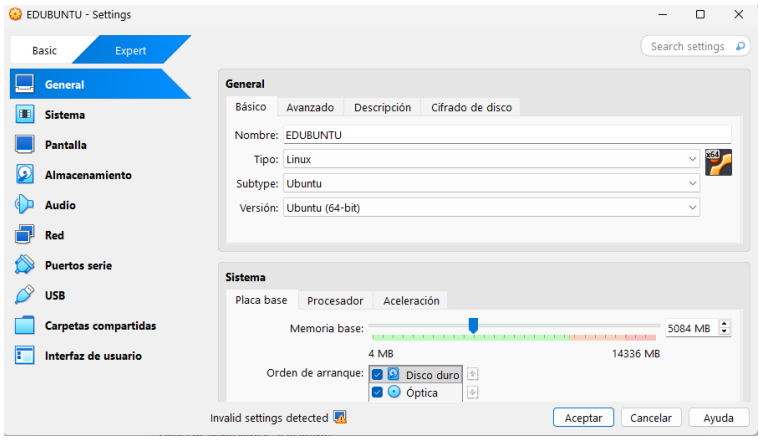


Figura 2. Visualización de la Configuración de Edubuntu

Lo siguiente que se debe hacer es ingresar al apartado de red, como se muestra en la imagen anterior, estando allí lo primero que hacemos es cambiar dirección **Mac 080027FDDA82** (rectángulo negro) que este caso sería la que tiene por defecto esta máquina.

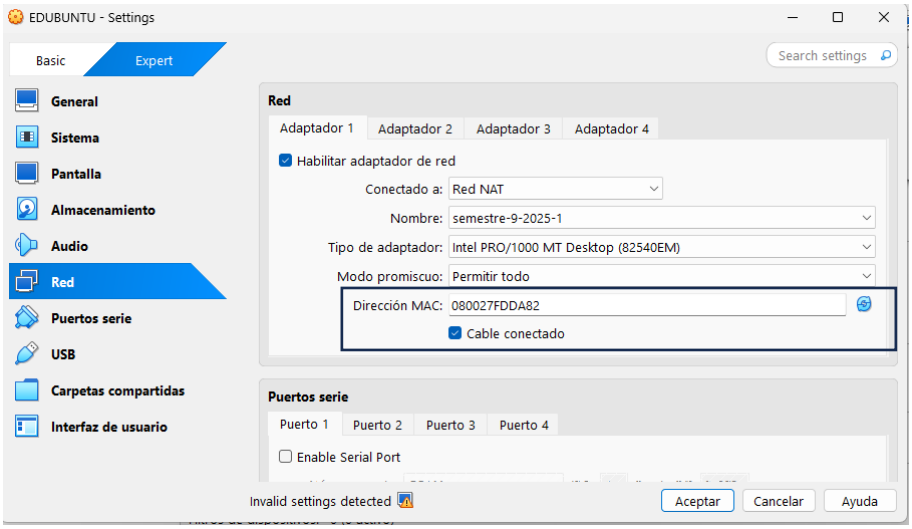


Figura 3. Mac por defecto de la Máquina.

Lugo lo que hacemos es cambiar esa Mac por defecto, por otra Mac fija de nuestra preferencia. La nueva Mac que se asigno fue **08:00:27:AA:BB:CC** (rectángulo negro) al configura esta Mac de forma física, Lo que se hace es evitar que el usuario pueda cambiar la Mac de forma manual desde edubuntu y si llega a hacerlo no podrá navegar en internet.

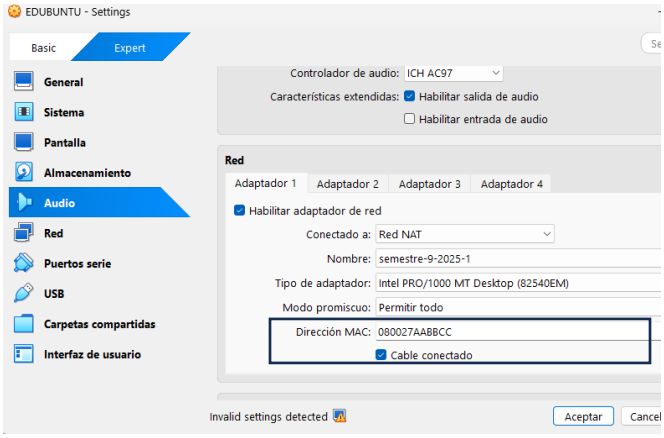
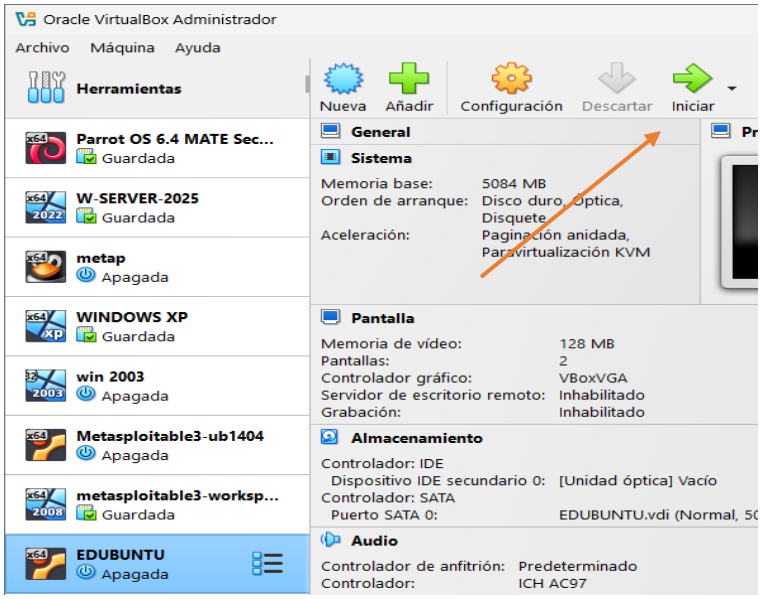


Figura 4. Establecimiento de Una Nueva Mac fija



Cuando luego de darle clic en aceptar iniciamos nuestra maquina nuestra máquina, para esto le damos clic en iniciar (flecha naranjada)

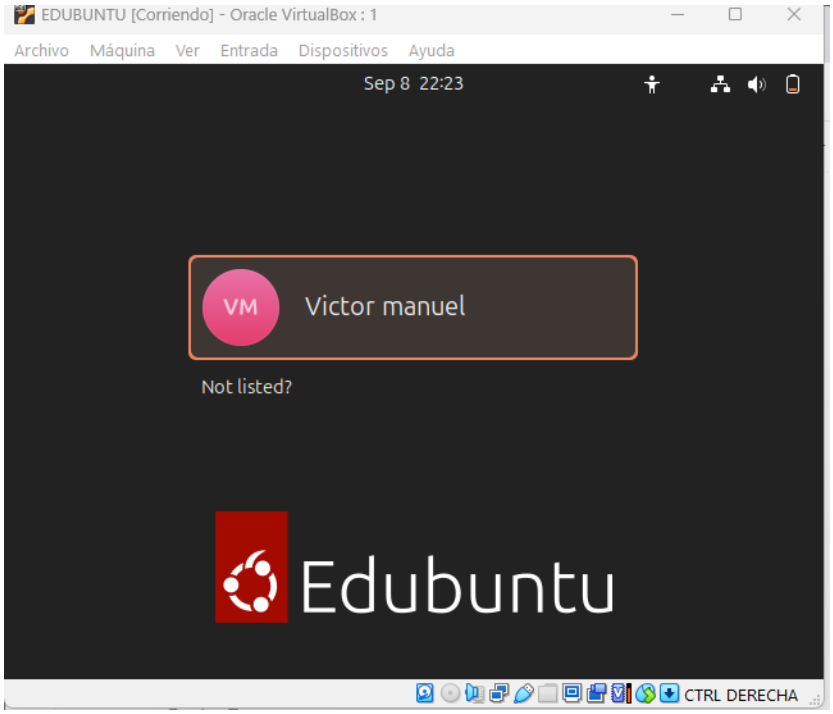


Figura 5. Iniciamos Nuestra Máquina Virtual En Edubuntu

Al iniciar nuestra máquina virtual previamente configurada en VirtualBox , para loguearnos utilizamos la contraseña **Victor123.**

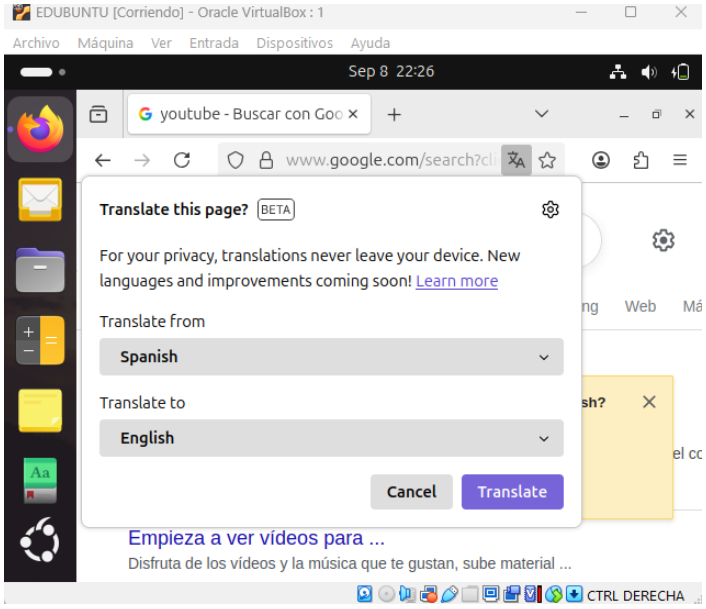
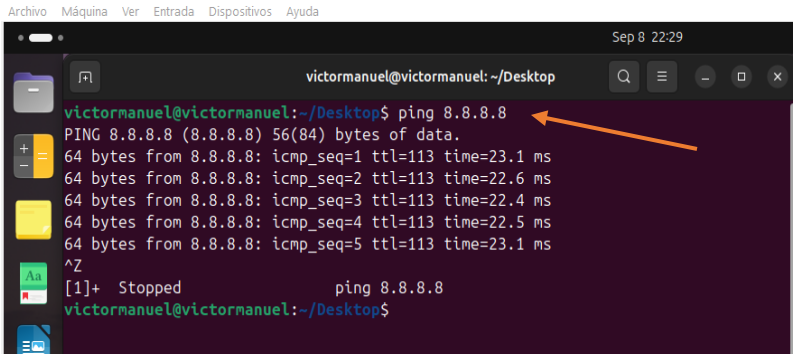


Figura 6. Hacemos la Prueba Con la Mac Que Agregamos

Para probar que la configuración hecha funciona vamos a nuestro navegador dentro de nuestra máquina virtual y buscamos una página cualquiera en este caso busqué YouTube, Otra opción de verificar que nuestra máquina está funcionando o la configuración esté funcionando es abrir la consola de nuestra distribución y mandar un pin A Google con el comando ping 8. 8. 8. 8 con esto deberá salir lo siguiente.



Lo que hicimos aquí fue probar el ping y como Como era evidente nos da pin de forma correcta lo que haremos a continuación será cambiar la Mac de forma manual desde la consola de edubuntu, esto nos permitirá ver si al cambiarla podemos navegar a internet común y corriente de poderse hacer quiere decir que nuestra configuración no fue correcta y la Mac permanente que pusimos no está funcionando.

3.1. Prueba de Que la Configuración Hecha Funciona Correctamente.

Para confirmar que el cambio de dirección MAC en Edubuntu si funciono, y se nos permite navegar con la Mac fija se logra cambiando la mac desde Ubuntu. Lo primro que se hizo fue ingresar al modo super usuario, luego apagar la interfaz de red usando el comando **sudo ip link set dev enp0s3 down**, luego asignamos una nueva dirección física con el comando **sudo ip link set dev enp0s3 address 00:11:22:33:44:55** por último reactivamos la interfaz con el comando **ip link set dev up .** En Edubuntu sobre VirtualBox, al modificar la MAC manualmente y no coincidir con la configurada en el hipervisor, la conexión NAT se interrumpe, impidiendo el acceso a internet.

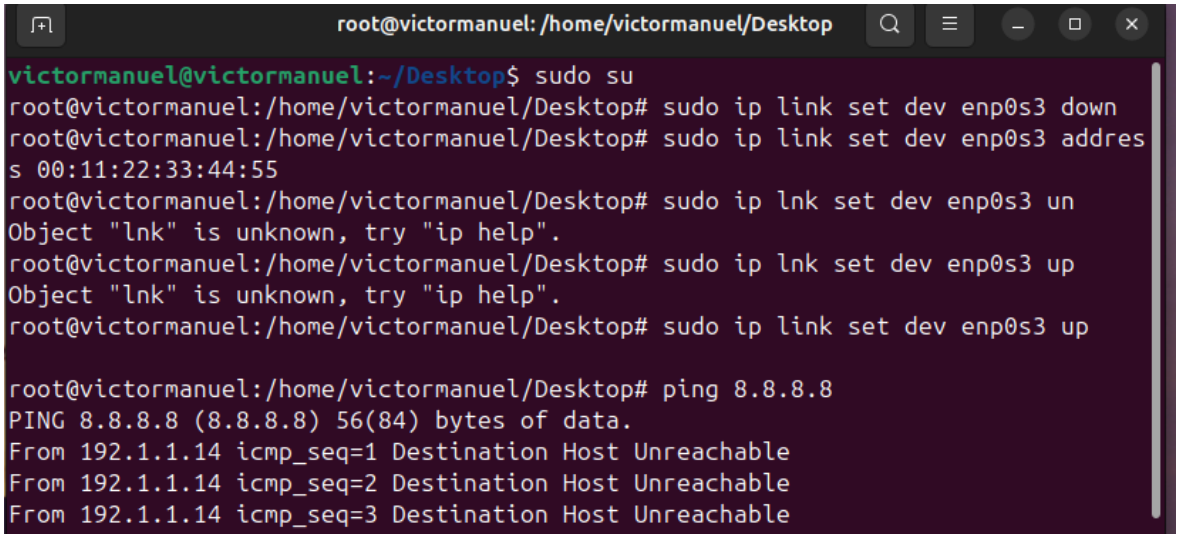


Figura 7. Comandos Realizados en la Prueba en su Respectivo Orden

Después de ingresar los comandos, volvemos a darle ping a Google, pero si notamos bien no se nos permitió salir a internet ya que no se reconoce esa dirección que estamos utilizando.

Luego de la prueba, se realizó el cambio de la Mac por la que configuramos previamente como Mac fija, por lo que no explicar de nuevo ese paso a paso por que s lo mismo que explique anteriormente.

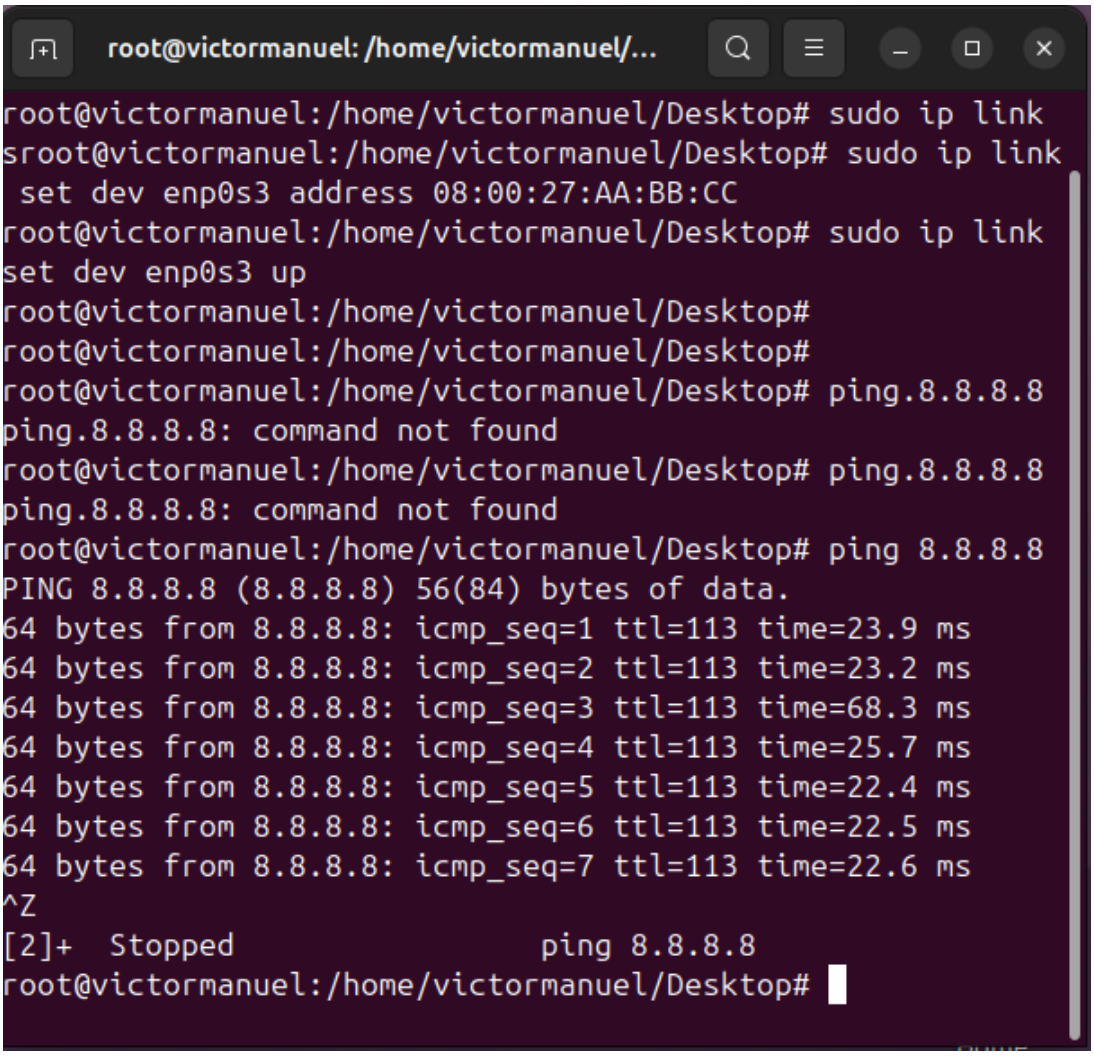


Figura 8. Cambio de la Mac incorrecta Por la Correcta

Al cambiar los datos y dar ping de nuevo a Google Google se evidenciará que todo funciona de forma correcta.

4. Capítulo 2: Comandos en Linux Para Calcular la Cantidad de Caracteres en un Archivo

Según (IONOS, 2023a) El comando de Linux **wc** es aquel que nos permite conocer la cantidad de líneas, palabras y caracteres contenidos en un archivo. Además, puede aplicarse a varios documentos de forma simultánea, mostrando los resultados individuales y el total acumulado.

4.1. ¿Cómo funciona el comando wc?

(IONOS, 2023b) piensa que el comando **wc** en Linux funciona de manera sencilla. Por defecto muestra en la terminal el número de líneas, palabras y caracteres de un archivo, aunque también es posible especificar opciones para ver solo un parámetro. Asimismo, puede aplicarse a varios ficheros a la vez, entregando los resultados individuales de cada uno y la suma total de líneas, palabras y caracteres. Pero a su vez (IBM, 2023) nos dique que El comando wc se utiliza para contar el número de líneas, palabras y bytes en los archivos indicados mediante el parámetro archivo.

Si no se especifica un archivo, el comando toma como entrada la entrada estándar. Los resultados se muestran en la salida estándar, junto con un recuento total cuando se trabajan con varios archivos. Si se emplean banderas, el orden de estas determina la forma en que se presenta la salida. Una palabra se define como una cadena de caracteres delimitada por espacios, tabulaciones o saltos de línea y cuando se especifican archivos en la línea de comandos, sus nombres aparecen junto a los valores obtenidos.

4.2.Ejemplo, opciones de comando y su uso

Las opciones de comando que encontramos las mostraremos a continuación junto con un ejemplo de cómo se aplicarían al hacer una practica tal cual como lo verán a continuación.

Tabla 1. Ejemplo, opciones de comando y su uso

Opción	Descripción	Ejemplo
-c	Muestra el número de **bytes** del archivo	wc -c ejemplo.txt
-l	Muestra el número de **líneas**	wc -l ejemplo.txt
-m	Muestra el número de **caracteres**	wc -m ejemplo.txt
-w	Muestra el número de **palabras**	wc -w ejemplo.txt
-L	Longitud de la **línea más larga** del archivo	wc -L ejemplo.txt

5. Capítulo 3: Creación de Usuarios en la Máquina Fristileaks

El jueves cuatro del mes en curso en la clase de auditoría de redes, realizamos una laboratorio de hacking ético en donde vulneramos una página web por defecto de Fristileaks, este capítulo del informe lo dedicaremos específicamente a replicar dicho laboratorio entendiendo que se descartar algunas cosas hechas en clase.

5.1. Configuración de Fristileaks

Para este paso lo que se hizo fue instalar el archivo punto evo contenedor de una máquina virtual bastante necesaria para esta práctica, lo que se hizo fue ingresar a nuestra VirtualBox, ingresamos en la configuración de red y cambiamos el conectado a Red NAT, luego cambiamos la dirección Mac por la que nos dio el profe. Tal como se ve en la imagen.

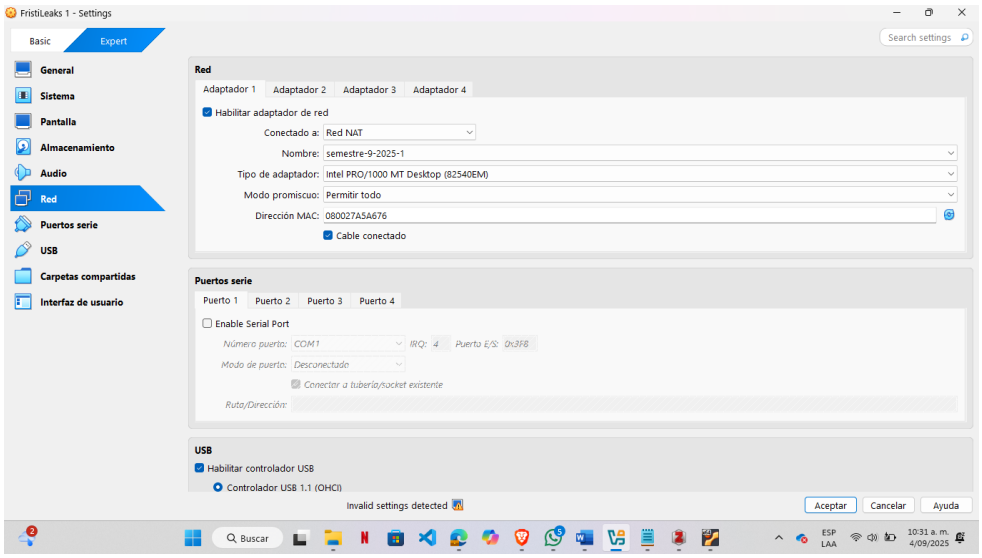


Figura 9. Configuraciones Previas a Nuestro Laboratorio

Luego de este proceso encendimos nuestra máquina de Fristileaks y revisamos que ya nos estuviera dando una dirección ip del segmento Red NAT configurado.

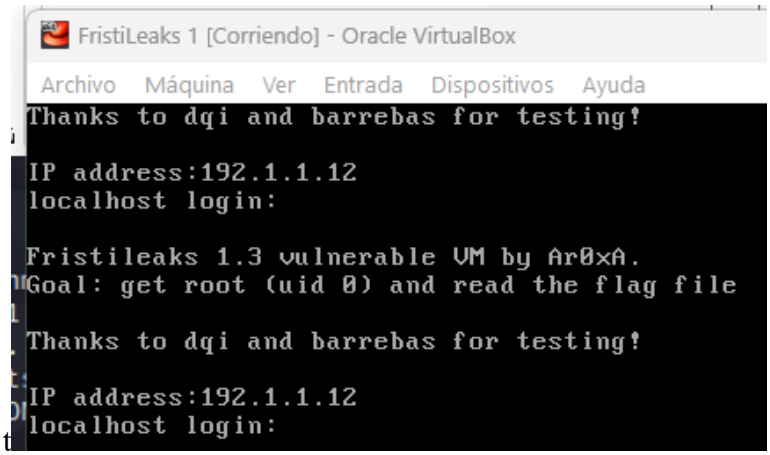


Figura 10. Dirección Obtenida En Fristileaks

Después de obtenida la dirección abrimos nuestro Kali Linux e hicimos el siguiente proceso, se realizo un escaneo de dirección ip con **nmap -Sv** a la dirección ip 192.1.1.0/24, esto nos permitiría obtener una lista de direcciones conectadas a este segmento de red y algunos de sus versiones.

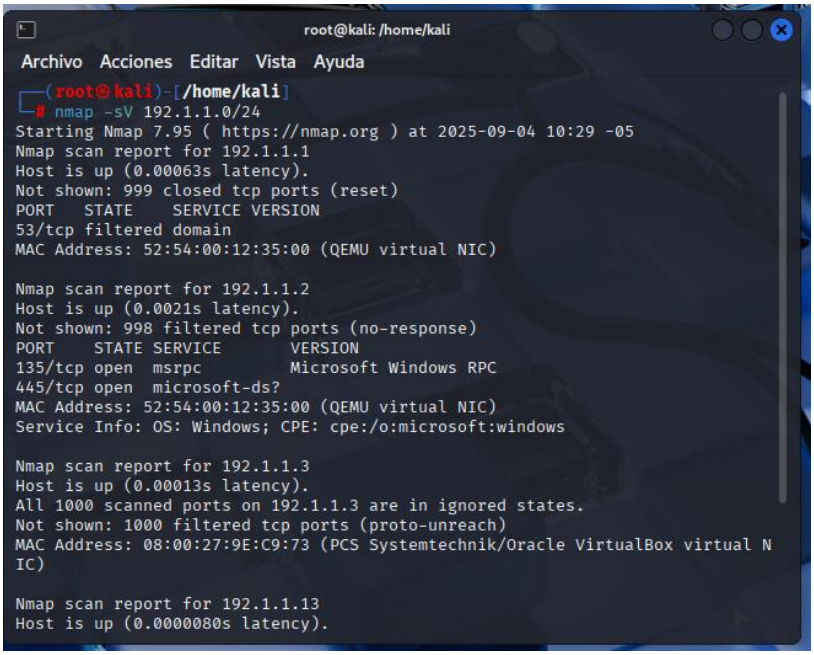


Figura 11. Escaneo de red Con Nmap -sV

```
Nmap scan report for 192.1.1.12
Host is up (0.00035s latency).
Not shown: 986 filtered tcp ports (no-response), 13 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 N
IC)

Nmap scan report for 192.1.1.13
Host is up (0.0000060s latency).
All 1000 scanned ports on 192.1.1.13 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 256 IP addresses (5 hosts up) scanned in 19.90 seconds
```

Figura 12.1 Escaneo de red Con Nmap -sV

Luego de indagar que en la ip **192.1.1.12** estaba corriendo el servicio apache en su puerto predeterminado, abrimos una el navegador de Kali e ingresamos en la barra de búsqueda la ip antes mencionada.

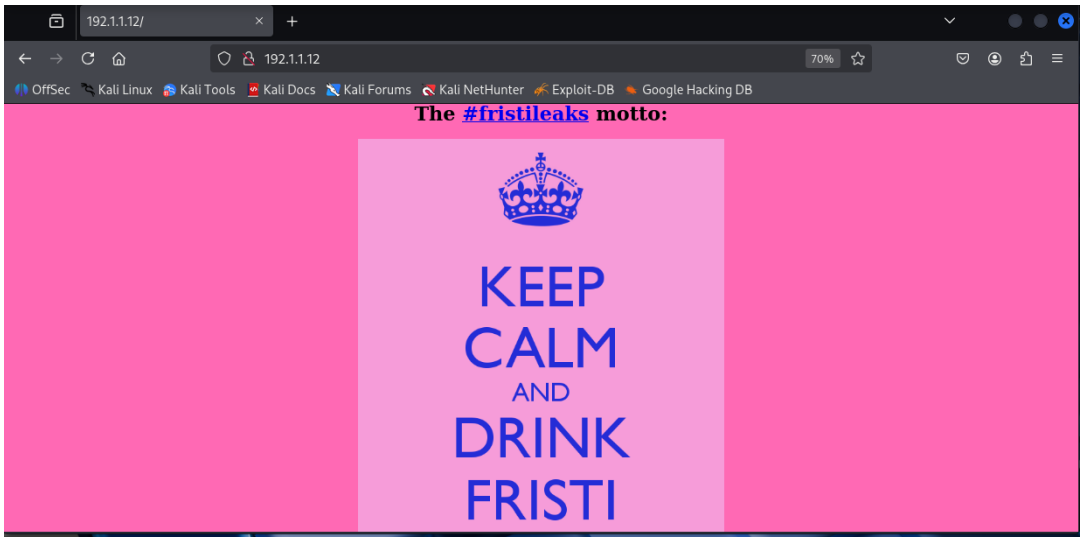


Figura 13. Visualización de la Página por Defecto De Apache.

Luego revisamos el código fuente a ver si encontrábamos algún dato filtrado y al no hallar ninguno se procedió a copiar la url para realizar un mapeo de subdominios que permitirá encontrar aun dado importante dentro de los posibles sub dominios que encontráramos.

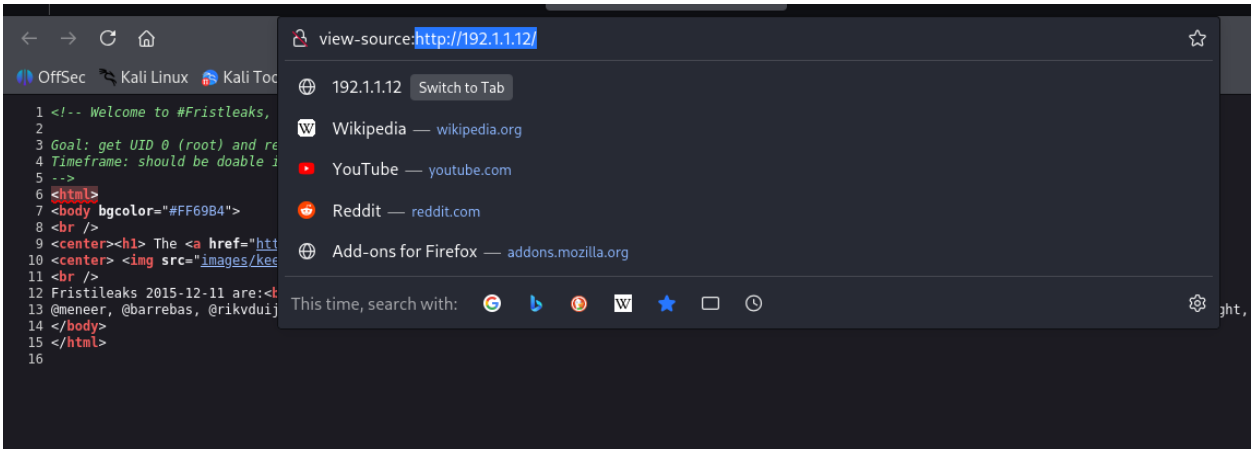
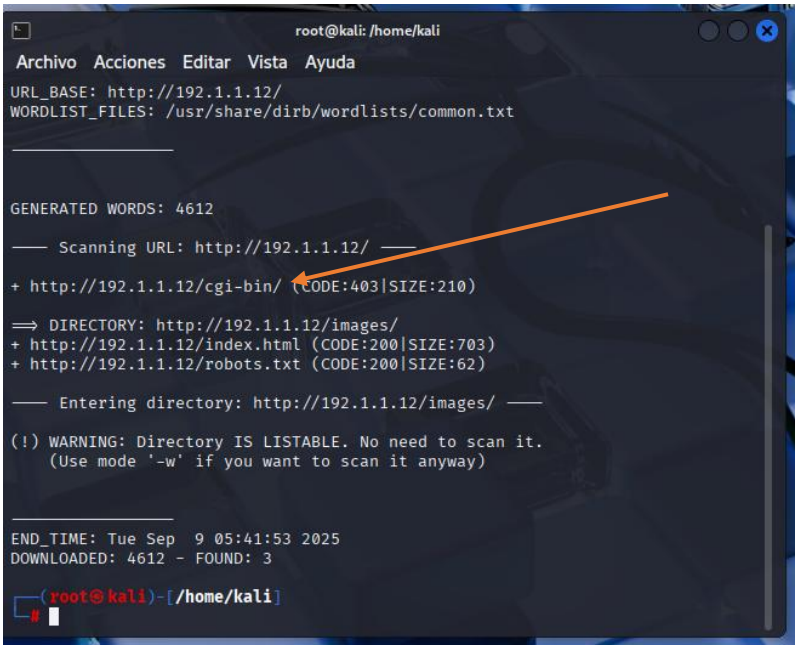


Figura 14. Revisión Del Código Fuente y Copia de la Url Para su Escaneo

Después de que se copió la ruta, fuimos a escanear a ver si existía algún subdomido en esa ip o url para mirar cuantos directorios ocultos pudiese haber para ello lo que hicimos fue emplear diccionario llamado dirb.



Después de ejecutar **dirb** para identificar directorios en el servidor, procedimos a realizar la revisión de algunas presentes en la librería estas listas de palabras que incluye la herramienta en la ruta */usr/share/dirb/wordlists*. Que son diccionarios que el docente decía que nos servían

para realizar un sinfín de hackeos y que incluso podríamos realizar nuestros propios diccionarios ya que algunos como common.txt. contenían palabras comunes en utilizadas en los directorios.

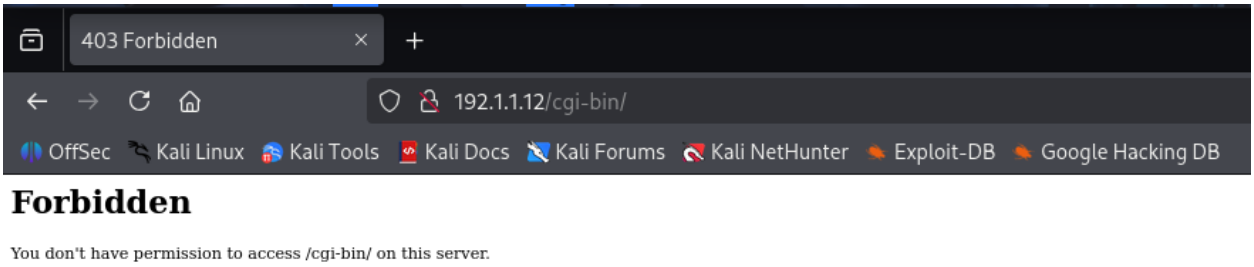


Figura 15. Ingresamos a Una de Las Rutas Encontradas en el Escaneo

Al intentar ingresar de forma directa a la ruta que nos encontremos lo que nos mostró que no teníamos el permiso para poder ingresa a este sitio por lo que se procedió a escáner esta nueva ruta para ver que otras rutas se podrán encontrar y de nuevo nos encontramos con una ruta vacía

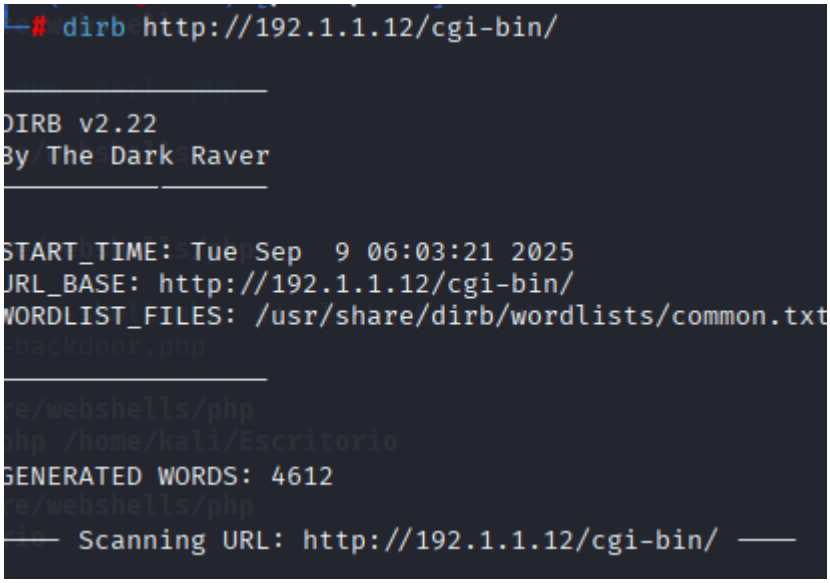


Figura 16.Escaneo de la Nueva Ruta

Se procedió entonces a hacer un mapeo a la ruta anterior pero con un nuevo directorio llamado imagen, que no arrojo nada.

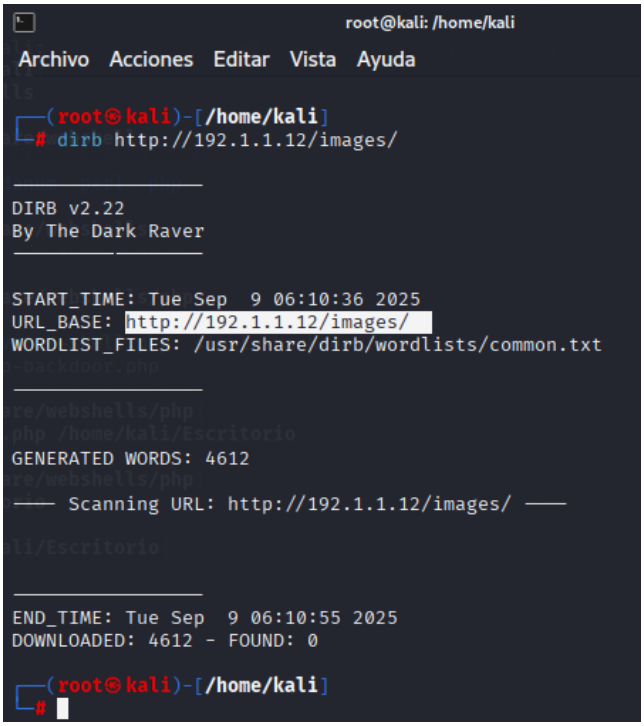


Figura 17. Escaneo e la ruta images

Lo que posterior mente se hizo fue abrir la ruta para comprobar que existiese algún archivo dentro de es ruta, esto derivo en que efectivamente existían dos imágenes en dicha ruta.

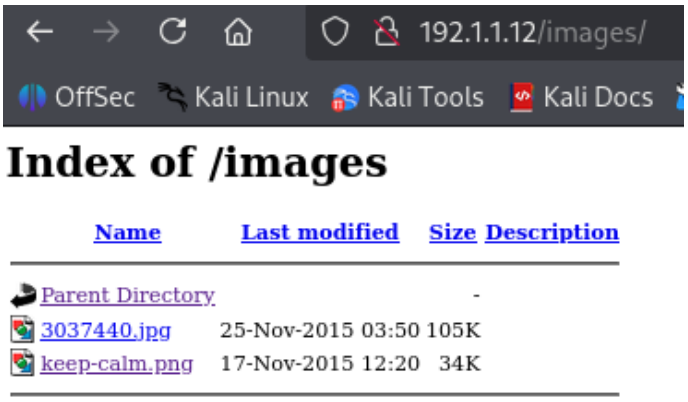


Figura 18. Archivos Encontrados.

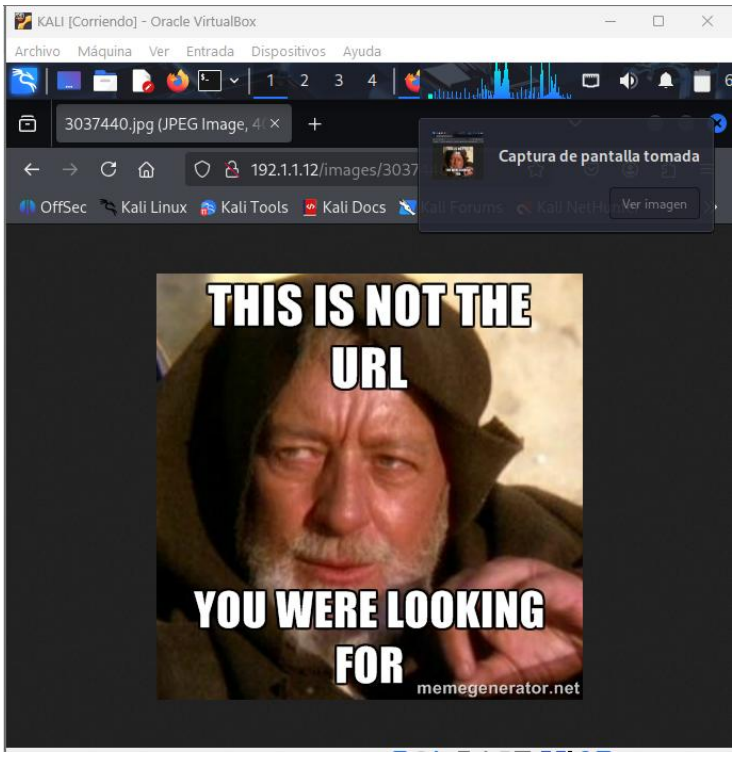


Figura 19. Revisión la Imagen 1 de Los Archivos.

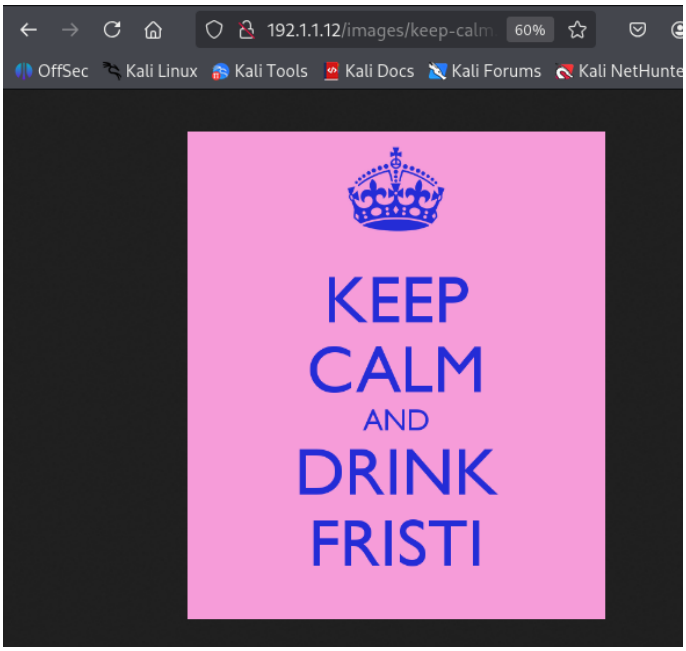


Figura 20. Revisión la Imagen 2 de Los Archivos.

Al revisar estas imágenes no encontramos nada interesante por lo precedí a intentar abrir la ruta **http:192.1.1.12/fristi**

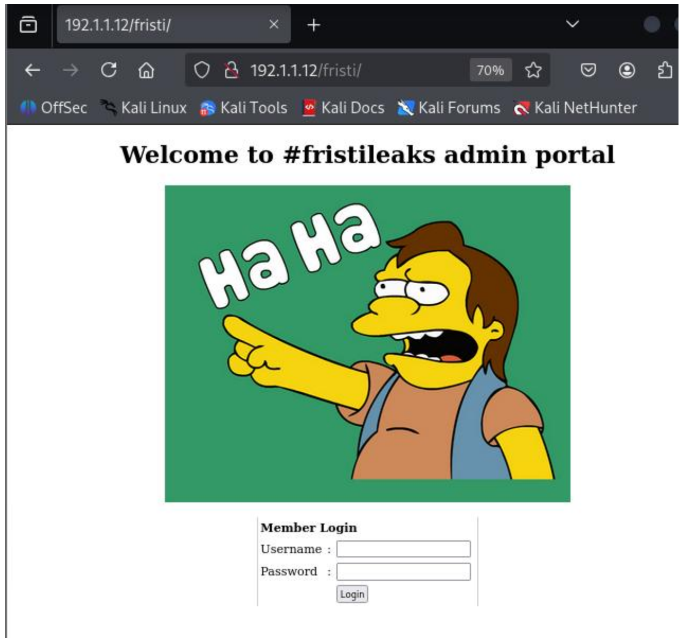


Figura 21. Revisión de la ruta http:192.1.1.12/fristi

Esta ruta nos mostro un login del cual no teníamos ni usuario ni contraseña, lo que nos llevó a intentar conseguir ese usuario y la contraseña necesaria, lo primero que se hizo aquí fue inspeccionar el Código fuente.

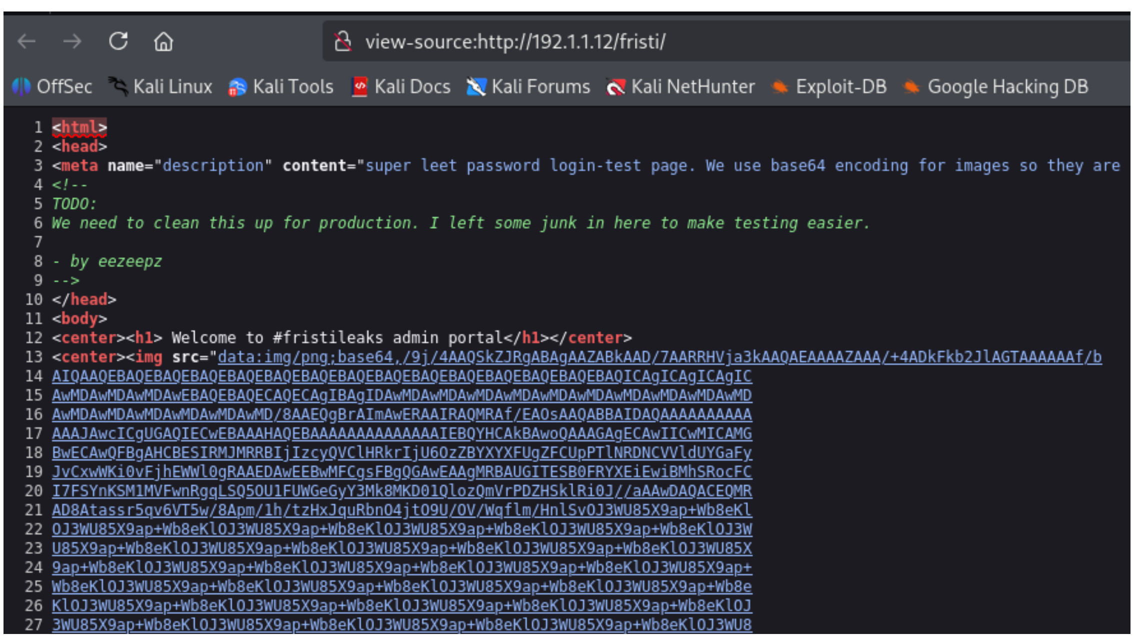


Figura 22. Inspección de la ruta antes mencionada

En esta inspección si tuvimos éxito que encontramos mas datos, ejemplo de ello es que en uno de los comentarios que estaba en el Código fuente encontramos el usuario los datos encontrados los pegamos en un blog de nota.

Figura 23. Imagen Codificada

Aquí nos encontramos una imagen codificada que posiblemente podría contener los datos de usuario contraseña así que lo que se hizo fue intentar encontrar en que formato estaba ya que el texto estaba en formato base 64 y que contenía, debido hace procedimos a buscar las páginas necesarias. Para resumir, luego de probar convertirla de a pnj descubrimos que dicha imagen estaba en formato png.

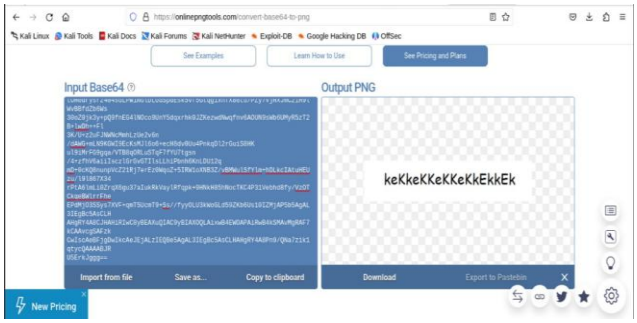


Figura 24. Convertimos de PNG

Aquí ya habíamos encontrado el usuario y la contraseña, lo siguiente fue devolvernos a la ruta **http:192.1.1.12/fristi** y revisar si esta si era las credenciales.

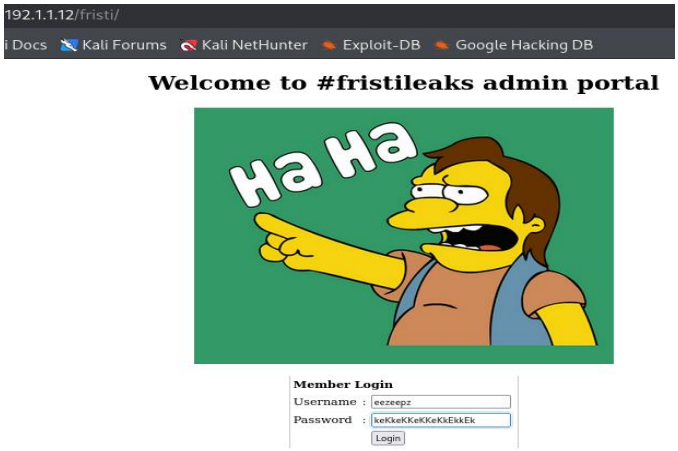


Figura 25. Credenciales Probadas.

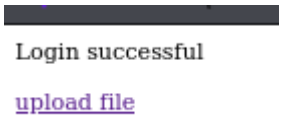


Figura 26. Ingreso Con Dichas Credenciales Exitoso

Al intentar ingresar con dichas credenciales nos encontramos con que, si eran las credenciales correctas, entonces le dimos clic subir archivos y nos llevo a la siguiente pagina

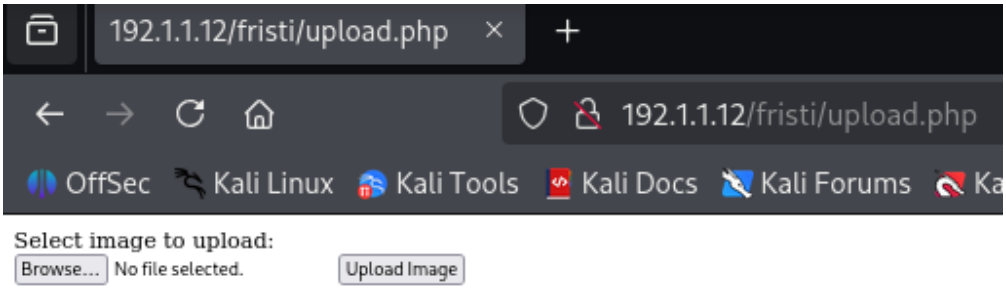


Figura 27. Sección Para Cargar Archivos

La pagina nos mandó a una sección donde podíamos cargar una, el docente Rafael S Morales nos Explico con un ejemplo que en clase que en dicha página no podíamos subir

imágenes en un formato que no fuese de imagen, el ejemplo consistió en subir cualquier archivo que no estuviera en ese formato a ver que pasaba y lo que paso fue esto.

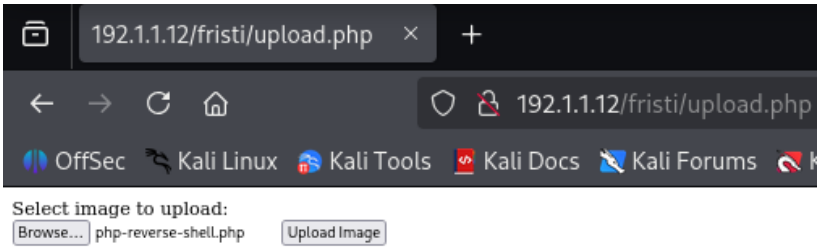


Figura 28. Intento de Subir un Archivo en un Formato Distinto

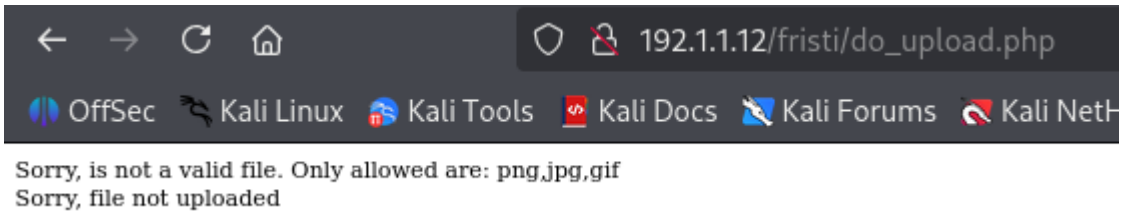


Figura 29. Mensaje Obtenido.

Lo que obtuvimos fue un mensaje de denegación en donde nos decías que no era posible subir ese formato.

5.2. Procesos Realizados en Kali Linux Como vulneración Directa

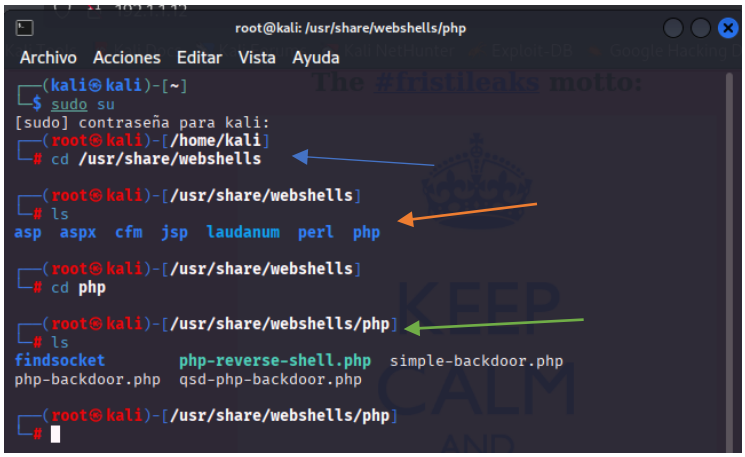


Figura 30. Buscamos Nuestro Archivo php-Reverse

Para comenzar este proceso, lo primero que debemos hacer es ingresar al modo super usuario, luego de estar aquí ingresamos la ruta **/usr/share/webshells/** (flecha azul) , luego de realizar lo que hicimos fue listas con el comando **ls** (flecha naranja) los archivos presentes en esta, utilizando el comando **cd php** (flecha verde) accedimos a este archivo y listamos de nuevo los archivos que tenga este directorio.

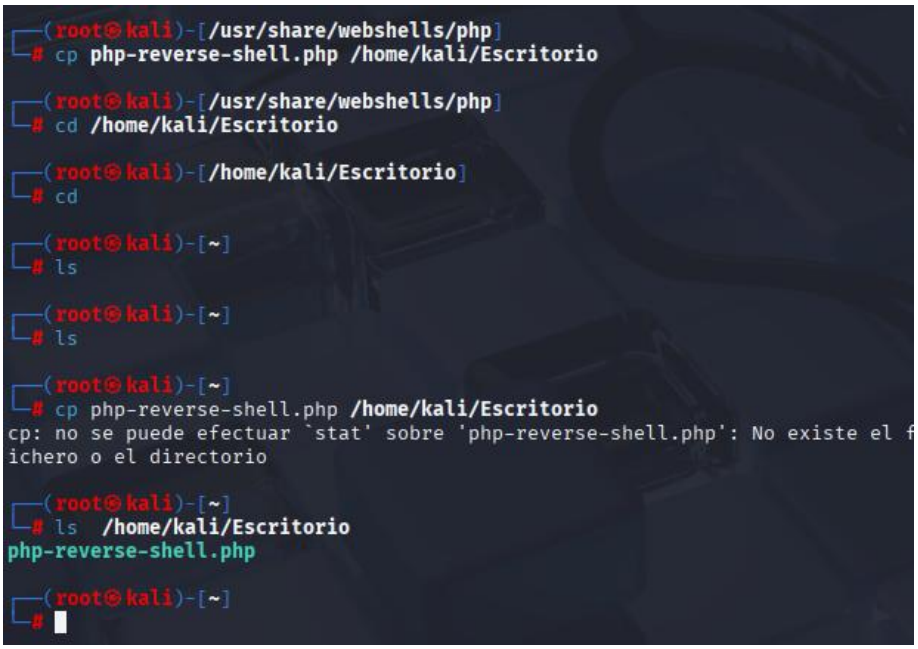


Figura 31. Movemos Nuestro Archivo al Escritorio

Luego de estar en el directorio php y listarlo, movimos el archivo **php-Reverse-shell.php** a nuestro escritorio este archivo nos permite hacer una conexión inversa de maquina a máquina, me refiero a que por medio del archivo vamos a poder tener acceso a la otra maquina

Figura 32. Disfrazar La Shell En PHP Como Si Fuera Una Imagen

Aquí copiamos el archivo **php-reverse-shell.php** y lo guardamos con el nombre **fotohot.php.png**. Esto sirve para **disfrazar la shell en PHP como si fuera una imagen**, lo cual es útil si el sistema víctima solo permite subir imágenes y bloquea archivos Nano

fotohot.php.png

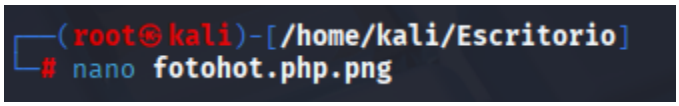


Figura 33. Contenido de la Reverse Shell

Con este comando abrimos el archivo **fotohot.php.png** en el editor de texto **Nano**. Desde aquí podemos modificar el contenido de la reverse Shell, por ejemplo, cambiando la dirección **IP** de nuestra máquina atacante y el **puerto** en el que escucharemos la conexión. Este paso es clave para personalizar el ataque.

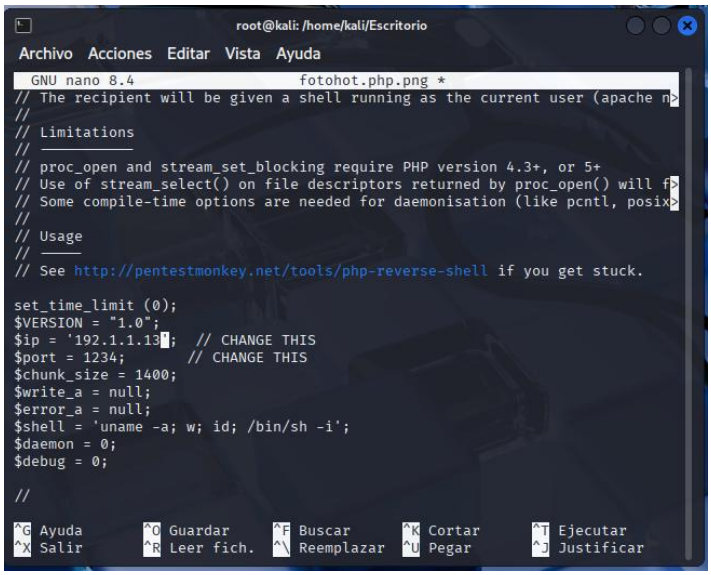


Figura 34. Modificación Del Contenido de la Reverse Shell

Con este comando se abrió el archivo fotohot.php.png en el editor Nano. En su interior se encuentra el código de una reverse shell en PHP. Desde este archivo podemos personalizar la conexión maliciosa, modificando parámetros como la dirección IP **($ip = '192.1.1.13';)** que

corresponde a la máquina atacante y el puerto **($port = 1234;)** donde se recibirá la conexión. Estas modificaciones son esenciales para que el shell inverso se conecte correctamente a nuestro sistema, permitiéndonos obtener acceso remoto al servidor comprometido.

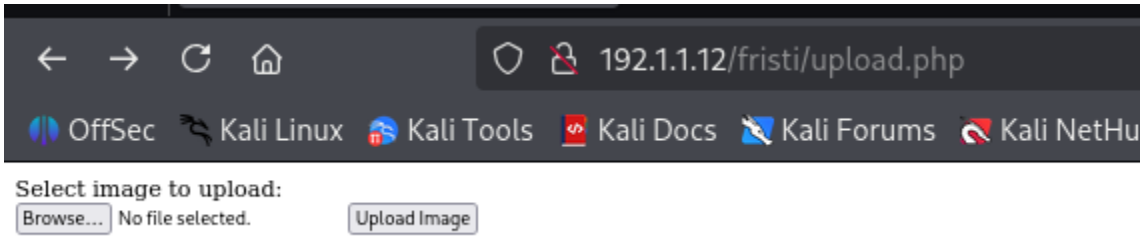


Figura 35. Accedemos a la Página Upload.Php

En este paso accedemos a la página upload.php del servidor víctima, ubicada en la dirección 192.1.1.12/fristi/upload.php. Desde esta interfaz web es posible subir archivos al servidor, lo que representa una vulnerabilidad importante. Aquí se aprovecha la opción de carga de imágenes para subir nuestro archivo malicioso fotohot.php.png, el cual contiene la reverse shell configurada previamente.

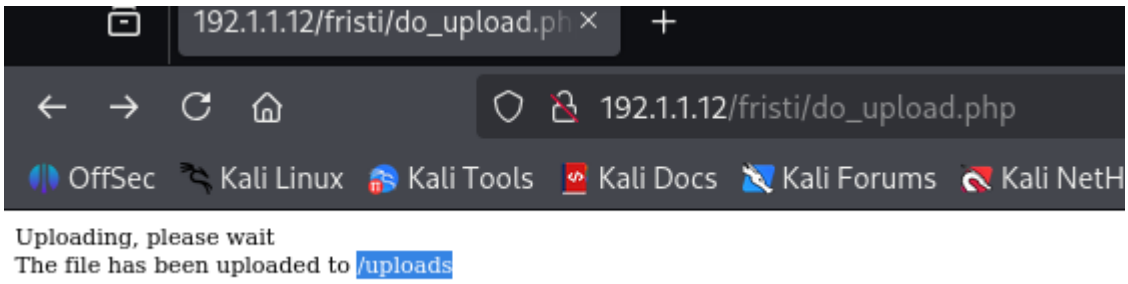


Figura 36. do_upload.php Reemplazamos Por /Uploads

Una vez cargado el archivo malicioso mediante el formulario de subida, el sistema confirma que la operación fue exitosa mostrando el mensaje “The file has been uploaded to /uploads”. Esto significa que nuestro archivo fotohot.php.png se encuentra almacenado en el

directorio /uploads del servidor víctima. Luego lo que hicimos fue copia lo que sombreamos con azul, borramos del navegador hasta el **do_upload.php** y reemplazamos por **/uploads**

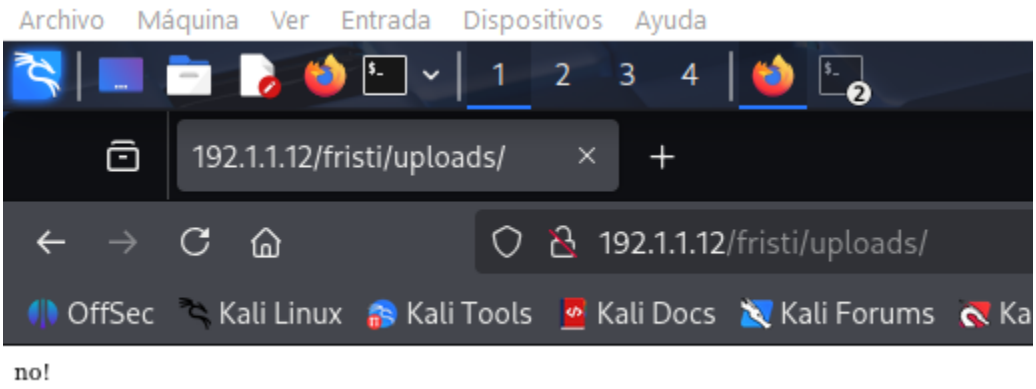


Figura 37. Ejecutamos el archivo

Al intentar acceder directamente al directorio uploads mediante la URL **192.1.1.12/fristi/uploads/,** el servidor responde con el mensaje “no!”. Esto indica que el listado de archivos dentro de esa carpeta está restringido, impidiendo ver qué contenido se ha subido. Sin embargo, esto no significa que el archivo malicioso no esté allí; si hicimos tod el proceso bin aquí ta deberíamos estar dentro de nuestra máquina de fisti, simplemente el directorio no muestra un índice navegable. Luego ejecutamos el comando **nc -l 1234** donde ingresamos el puerto que configuramos en el nano.

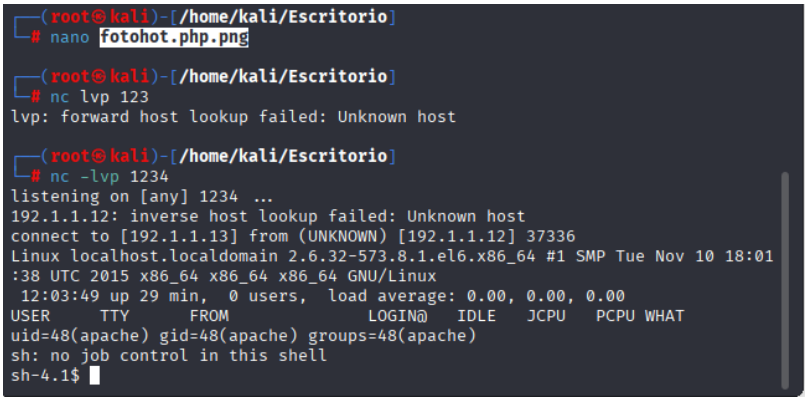


Figura 38. Ingreso FristiLeaks

Con el comando **ls -la** (flecha naranja) listamos todos los archivos y carpetas del directorio actual, incluyendo los ocultos (los que empiezan con "."). La opción -la sirve para mostrar detalles como permisos, propietario y tamaño de cada archivo. Esto nos ayuda a tener una visión completa de qué hay disponible en la carpeta en la que estamos.

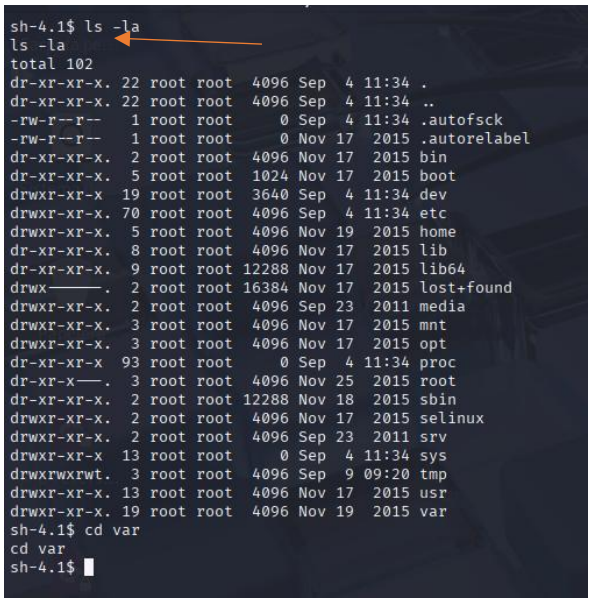


Figura 39.Comando ls -la

Después utilizamos el comando **cd var** Aquí nos movemos al directorio **/var**, que en sistemas Linux suele contener datos y archivos relacionados con servicios, como logs o contenido de servidores we

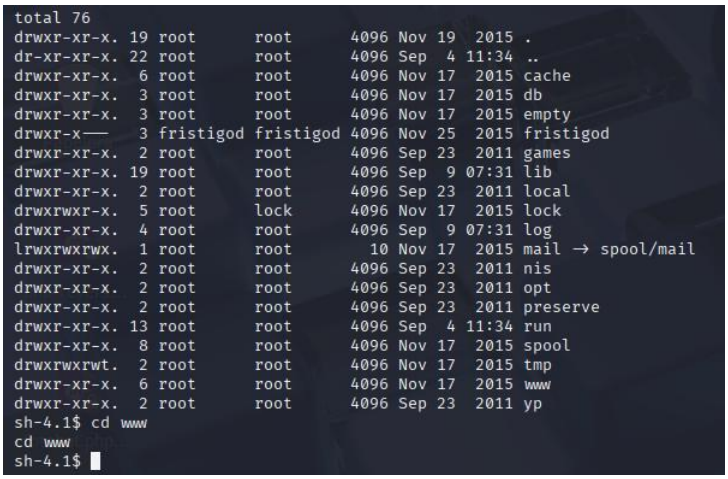


Figura 40. Accedemos A La Carpeta WWW

Dentro de /var, accedemos a la carpeta www usando el comando **cd www** , que normalmente es usada por los servidores web para alojar los sitios y aplicaciones que están en ejecución.

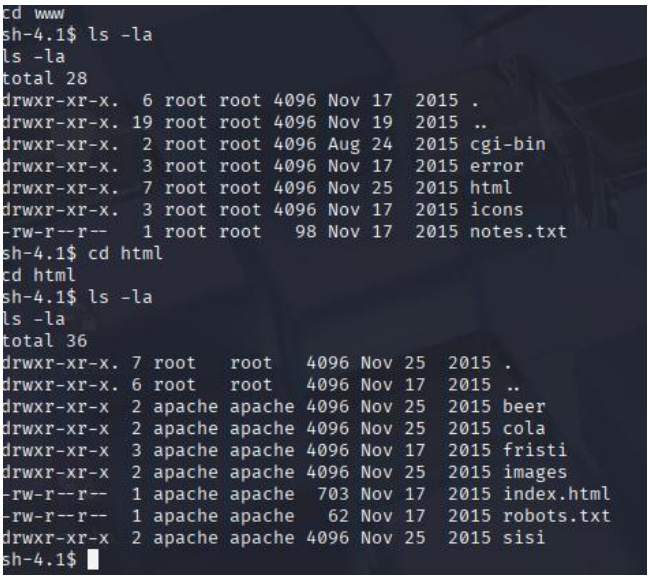


Figura 41. Entramos en HtmL

Después entramos en html, que suele ser la carpeta raíz pública del servidor web. Es aquí donde se guardan los archivos que los usuarios ven cuando acceden al sitio desde el navegador.

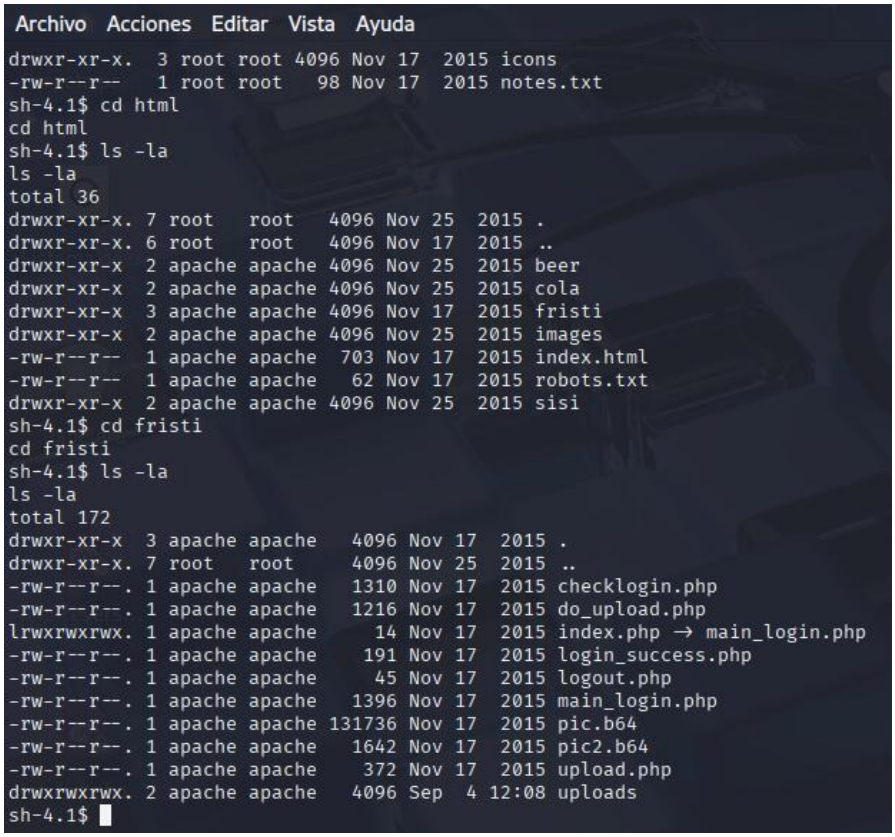


Figura 42. Nos Movemos a la Carpeta Fristi

Nos movemos a la carpeta fristi, que corresponde a la aplicación web FristiLeaks. Este es el directorio específico donde se encuentran los archivos PHP y demás recursos que hacen funcionar el portal vulnerable. Usamos tambien el comando **cat checklogin.php**, con este comando visualizamos el contenido del archivo checklogin.php, que contiene el código encargado de manejar el proceso de inicio de sesión. Revisar este archivo es clave porque nos permite entender cómo se validan las credenciales y por qué es posible manipularlas desde la base de datos.

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

Este comando se usa para mejorar la shell que tenemos. Muchas veces al obtener acceso inicial a un sistema la consola es muy limitada (no soporta atajos, historial, etc.). Con esta instrucción en Python, lo que hacemos es “invocar” una shell interactiva completa de bash, lo que nos da mucho más control.

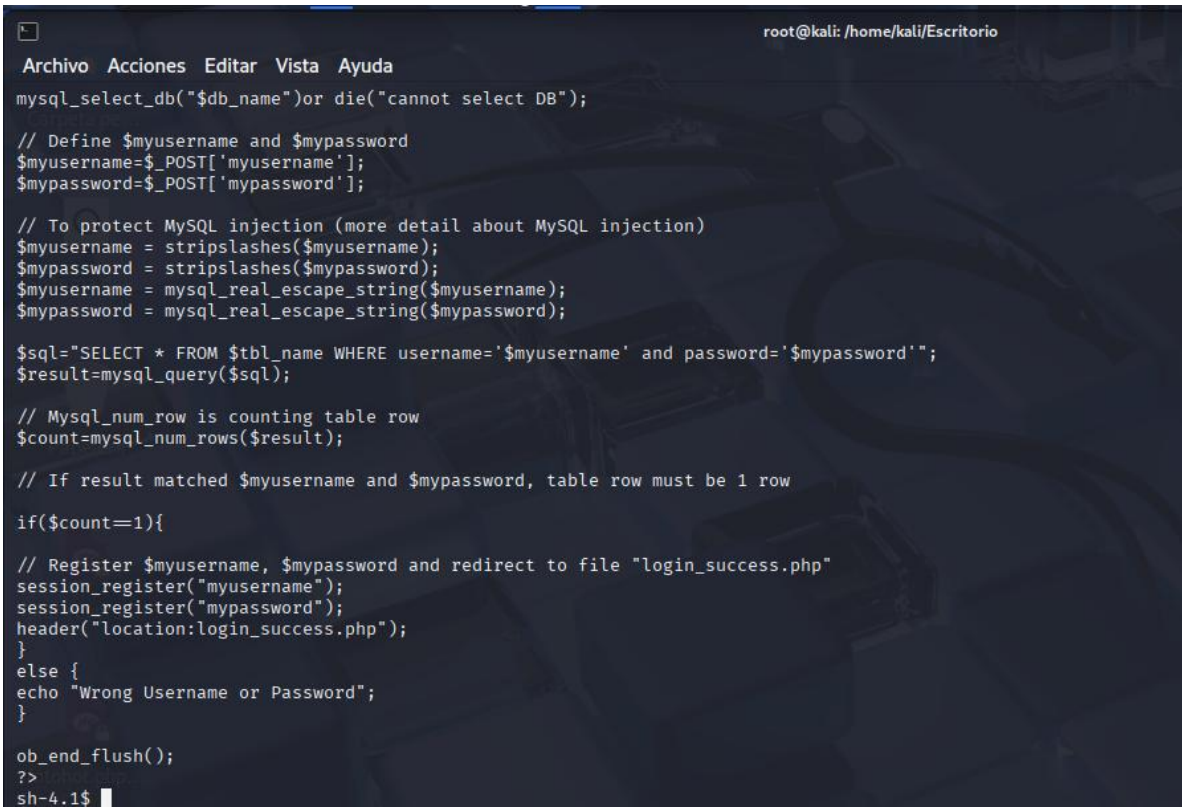


Figura 43. Aquí Tratamos de Entrar al Servicio de Mysql Usando el Usuario Eezeepz

Aquí tratamos de entrar al servicio de MySQL usando el usuario eezeepz. Al usar la opción -p, MySQL nos pedirá la contraseña para autenticar.la contraseña se según el cat que hicimo era 4ll3maal12#. Como último paso introducimos la contraseña 4ll3maal12# para el usuario eezeepz. Con estas credenciales, si son válidas, logramos acceder al gestor de bases de datos y desde ahí manipular directamente la información, como fue el caso de la tabla members.

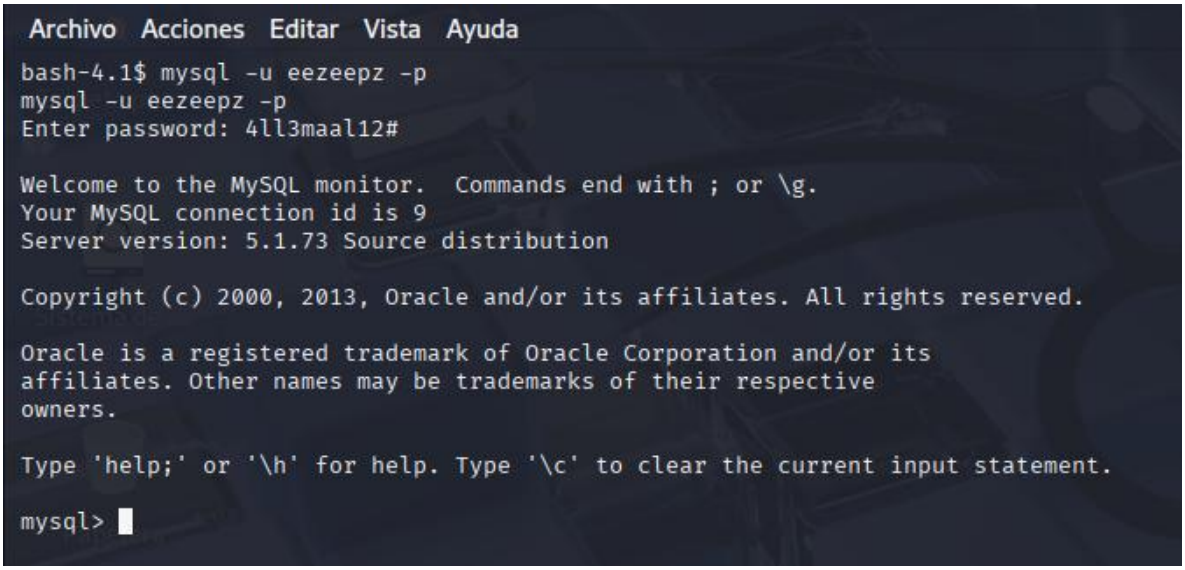


Figura 44. Ingresamos MySQL

Para iniciar este procedimiento, lo primero que se realizó fue ejecutar el comando **show databases;**, el cual permite visualizar todas las bases de datos disponibles en el servidor MySQL. En la imagen se observa cómo el sistema devuelve la lista de bases, entre ellas la llamada **hackmenow**, que será la utilizada en este ejercicio.

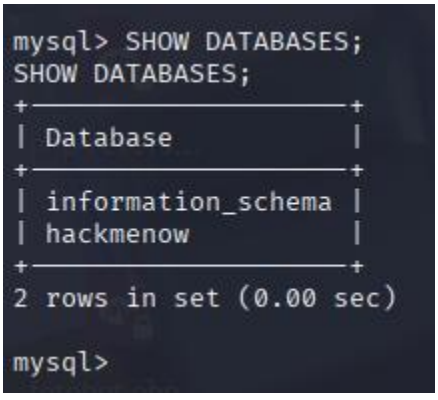


Figura 45. Se Ejecutó El Comando Show Database

Una vez identificada la base de datos, el siguiente paso fue seleccionarla para trabajar sobre ella. Para ello se empleó el comando **USE hackmenow;**, que cambia el contexto actual

hacia dicha base de datos, asegurando que todas las consultas posteriores se realicen en ella, Después de ingresar a la base de datos, se ejecutó el comando **show tables;**, cuyo propósito es mostrar las tablas disponibles en hackmenow. En esta captura se aprecia la tabla **members**, que contiene la información de usuarios y contraseñas.

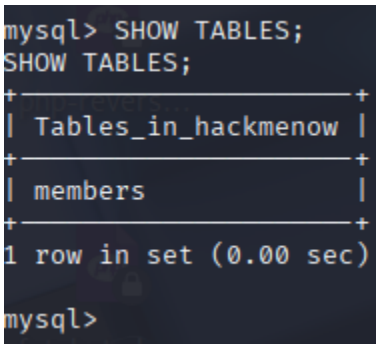


Figura 46. Tabla Obtenida al Ejecutar Show Tables

Para conocer la estructura interna de la tabla encontrada, se utilizó el comando **describe members;**. Este comando detalla los campos que componen la tabla, mostrando que posee columnas como **username y password,** necesarias para el registro y validación de usuarios.

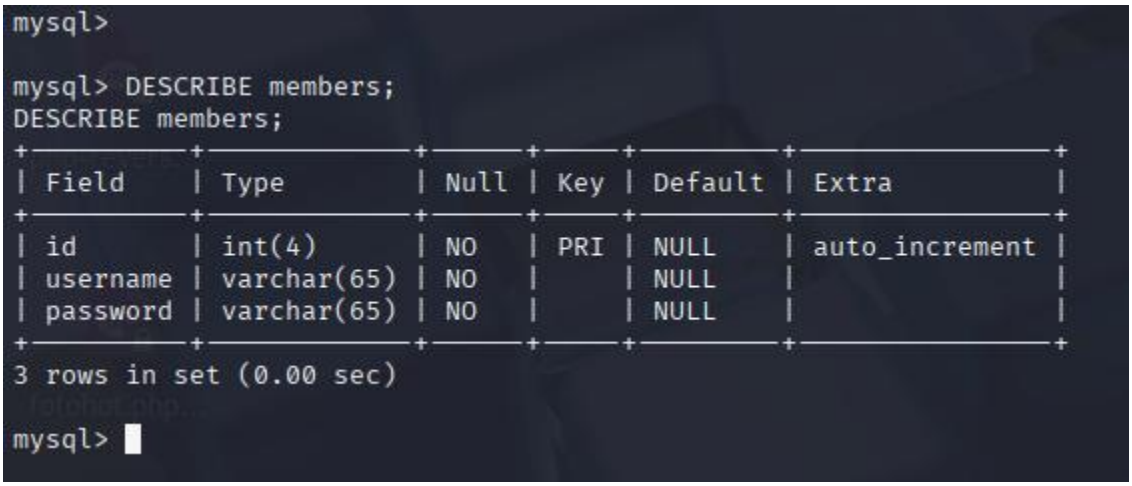


Figura 47. Conoceremos La Estructura Interna De La Tabla Encontrada Usando El Comando Members

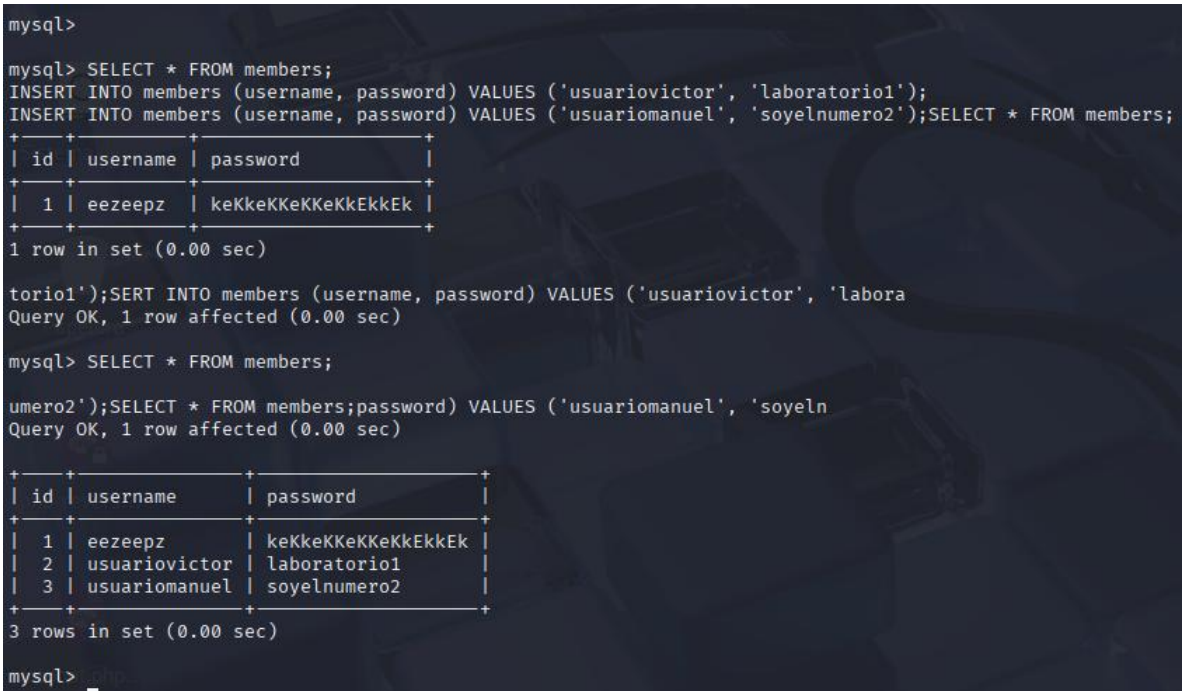


Figura 48. De Observa el Trabajo Dentro de la Tabla Members y Nuestros Usuarios Registrados.

En esta captura se observa el trabajo dentro de la tabla **members** de la base de datos. Inicialmente, se ejecutó el comando **select * from members;** para visualizar los registros existentes, mostrando únicamente el usuario **eezeepz** con su respectiva contraseña cifrada.

Posteriormente, se insertaron nuevos usuarios utilizando el comando **insert into**. El primer registro añadido fue **usuariovictor** con la contraseña **laboratorio1**, seguido de **usuariomanuel** con la contraseña **soyelnumero2**. Cada inserción fue confirmada con el mensaje

Finalmente, se volvió a ejecutar **select * from members;** para verificar los cambios. El resultado muestra ahora tres registros en total: el usuario original **eezeepz** y los dos nuevos usuarios creados (**usuariovictor** y **usuariomanuel**), confirmando que las operaciones de inserción se realizaron correctamente.

5.3. Verificación Del Registro de los Usuarios

Figura 49. Nos logueamos con el 1 usuario

En esta captura se ve la página de inicio de sesión del portal de **FristiLeaks**. Después de haber creado al usuario **usuariovictor** con la contraseña **laboratorio1** directamente en la base de datos, aquí lo estamos probando en el formulario web.

Básicamente, lo que se hizo fue usar esas credenciales nuevas en el login y con esto comprobar que el truco funcionó: los usuarios que insertamos manualmente en la tabla **members** también son aceptados por la aplicación web. Esto demuestra que teníamos control sobre la base de datos y que era posible colar cuentas falsas para entrar al panel de administración.

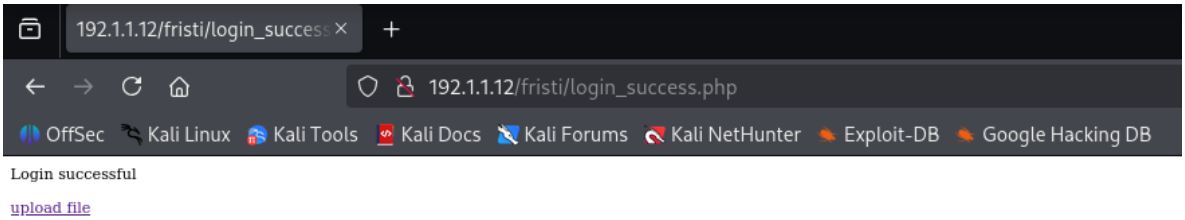


Figura 50. Verificación Exitosa 2 Usuario

Luego de esto mostramos la prueba de lo que se hizo fue correcto ingresando y logueandome

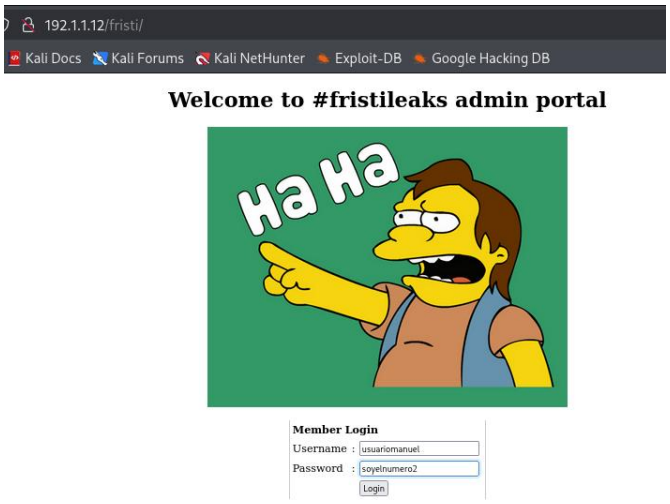


Figura 51. Nos logueamos con el 2 usuario

En esta otra captura estamos probando el segundo usuario que insertamos en la base de datos: **usuariomanuel** con la clave **soyelnumero2**. Igual que en el caso anterior, lo que hacemos es ir al formulario de login de **FristiLeaks** y colocar las credenciales creadas manualmente en la tabla **members**. Esto confirma que no solo funcionó con un usuario, sino que cualquier cuenta que añadamos directamente en la base de datos queda lista para iniciar sesión en la aplicación web. En pocas palabras, teníamos control total para crear accesos "a la medida" dentro del sistema.

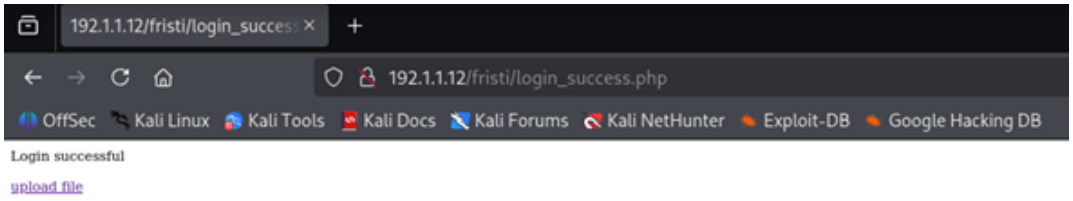


Figura 52. verificación Exitosa 2 Usuario

Por último, mostramos que en este caso también funciono el proceso que hicimos , lo mostramos ingresando a la página web.

Problemas Encontrados al Realizar el Informe

En mi caso el único problema realmente serio fue el tiempo, el trabajo y la salud ya que estos día me sentido un tanto indispuesto, pero e intentando que mi indisposición que no afecte mucho mi responsabilidad, aunque aun así lo hace de forma indirecta, prometo ser un poco mas responsable y apropiarme mas aun de los temas de ahora en lo adelante.

Solución del Problema

Para el problema descrito mi solución fue seguir intentando realizar el trabajo y aunque tarde, cumplir con la responsabilidad de entregarlo prometiendo esforzarme mas de ahora en adelante.

Recomendaciones

Por el momento no tengo una recomendación para el laboratorio como tal, ya que en general me gusto bastante la temática trata. Espero practicar un poco más para dominar el tema que estamos viendo y los temas que veremos más adelante.

Conclusión

Al finalizar esta práctica con la máquina vulnerable FristiLeaks se puede decir que la experiencia fue bastante enriquecedora, ya que permitió recorrer todo el ciclo de un ataque controlado en un entorno seguro. Se inició con la configuración básica de las máquinas virtuales y la red en VirtualBox, lo que aseguró la comunicación adecuada entre la máquina atacante y la víctima. Luego, con herramientas como Nmap y Dirb, se logró realizar un reconocimiento efectivo que dio la base para avanzar en la explotación.

Uno de los puntos más relevantes fue el uso de la reverse shell en PHP, que al ser disfrazada como una imagen y subida al servidor, permitió obtener acceso remoto al sistema. Este logro mostró lo sencillo que puede ser aprovechar una mala configuración en un servicio de carga de archivos. A partir de allí, se tuvo la posibilidad de navegar por los directorios internos, revisar scripts sensibles y encontrar credenciales que abrieron la puerta hacia la base de datos MySQL.

La manipulación de la base de datos, en especial la inserción de nuevos usuarios en la tabla members, confirmó el éxito del ataque, ya que fue posible ingresar al portal web con las credenciales creadas. Esto refleja de manera clara el impacto que puede tener una vulnerabilidad cuando no se toman las medidas necesarias de protección, como validar extensiones, restringir permisos o cifrar adecuadamente las contraseñas.

En definitiva, este ejercicio permitió entender de forma práctica cómo se desarrolla un proceso de hacking ético, desde el reconocimiento hasta la post-explotación. Además, resaltó la importancia de no limitarse a la teoría, sino de enfrentarse a laboratorios que simulen casos reales.

Referencias Bibliográficas

Rafael S Morales (2025) *Aplicación de servicio nmap y metaplotaible en la explotacion y vulneracion de páginas web* -Tema explicados en clase.

IONOS, E. (2023, agosto 11). Comando de Linux wc: Para contar palabras, caracteres y líneas en archivos. *IONOS Digital Guide*.https://www.ionos.com/es-us/digitalguide/servidores/configuracion/comando-de-linux-wc/

IBM. (2023, marzo 24). *Contar palabras, líneas y bytes en archivos (comando wc)*. https://www.ibm.com/docs/en/aix/7.1.0?topic=af-counting-words-lines-bytes-in-files-wc-command