INFORME LABORATORIO FRISTILEAKS Y CAMBIO DE MAC A UBUNTU

Natalia Espinosa Mena

Universidad Tecnológica del Choco Diego Luis Córdoba

Facultad de Ingeniería

Telecomunicaciones e Informática

Quibdó – Chocó

2025

INFORME LABORATORIO FRISTILEAKS Y CAMBIO DE MAC A UBUNTU

Docente

Rafael Sandoval Morales

Ingeniero

Universidad Tecnológica del Choco Diego Luis Córdoba

Facultad de Ingeniería

Telecomunicaciones e Informática

Quibdó – Chocó

2025

Universidad Tecnológica del Chocó
Diego Luis Córdoba

TABLA DE CONTENIDO

Pág.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

LISTA DE ILUSTRACIONES

Pág.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

INTRODUCCIÓN

El presente informe expone el desarrollo del laboratorio compuesto por tres capítulos, realizados en el entorno VirtualBox utilizando los sistemas operativos Kali Linux y Ubuntu. El propósito principal de este trabajo fue fortalecer las competencias prácticas en seguridad informática mediante la aplicación de herramientas y técnicas orientadas al análisis y protección de redes.

En el primer capítulo, se abordó la explotación del portal vulnerable FristiLeaks, donde se aplicaron procedimientos básicos de reconocimiento y análisis para identificar posibles puertas abiertas y comprender cómo estos pueden comprometer la seguridad de un sistema.

El segundo capítulo se centró en la modificación de la dirección MAC en el sistema Ubuntu, con el objetivo de observar cómo esta acción puede alterar la identidad de un dispositivo dentro de una red.

Por último, en el tercer capítulo, se documenta la consulta sobre los comandos de Linux relacionados con el uso de nc y los comandos para contar caracteres en un archivo.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

OBJETIVOS

General: Comprender las vulnerabilidades que pueden presentarse en los sistemas de red y su impacto en la seguridad informática.

Específicos:

- Crear dos usuarios en la VM FristiLeaks.
- Identificar y describir los comandos básicos de nc.
- Investigar y aplicar los comandos necesarios para contar caracteres en un archivo.
- Realizar el cambio de dirección MAC a la VM Ubuntu.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

PLANTEAMIENTO DEL PROBLEMA

En los sistemas de red y en las aplicaciones web pueden existir vulnerabilidades que permiten el acceso no autorizado o la alteración de su funcionamiento, aun cuando aparentan estar protegidos. Estas debilidades representan un riesgo constante para la integridad y seguridad de la información. Durante el desarrollo del laboratorio se evidenció esta problemática a través de actividades donde se detectaron y analizaron fallos presentes en diferentes entornos.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

1 CAPÍTULO 1: EXPLOTACIÓN PAGINA FRISTILEAKS

El laboratorio comenzó cuando el docente compartió el archivo OVA (incluye su sistema operativo y configuraciones predefinidas) de **Fristelaks**, que ya venía listo para usarse. Se copió el archivo al escritorio del computador para tenerlo a la vista.

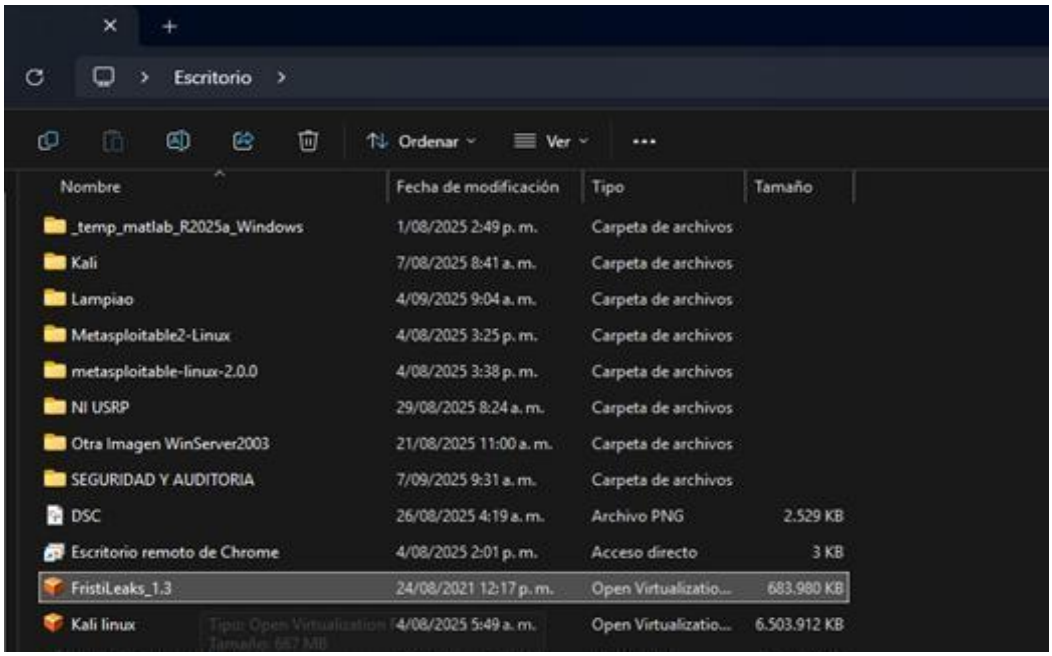


Ilustración 1 Ova FristiLeaks

Una vez ubicado en el Escritorio, se procedió a ejecutar la OVA haciendo doble clic sobre el archivo. Al hacerlo, se abrió automáticamente el asistente de VirtualBox, donde comenzó el proceso para añadir la máquina virtual al programa. La ventana de importación mostro las opciones de configuración básicas del entorno, las cuales se cargan automáticamente al tratarse de una OVA.

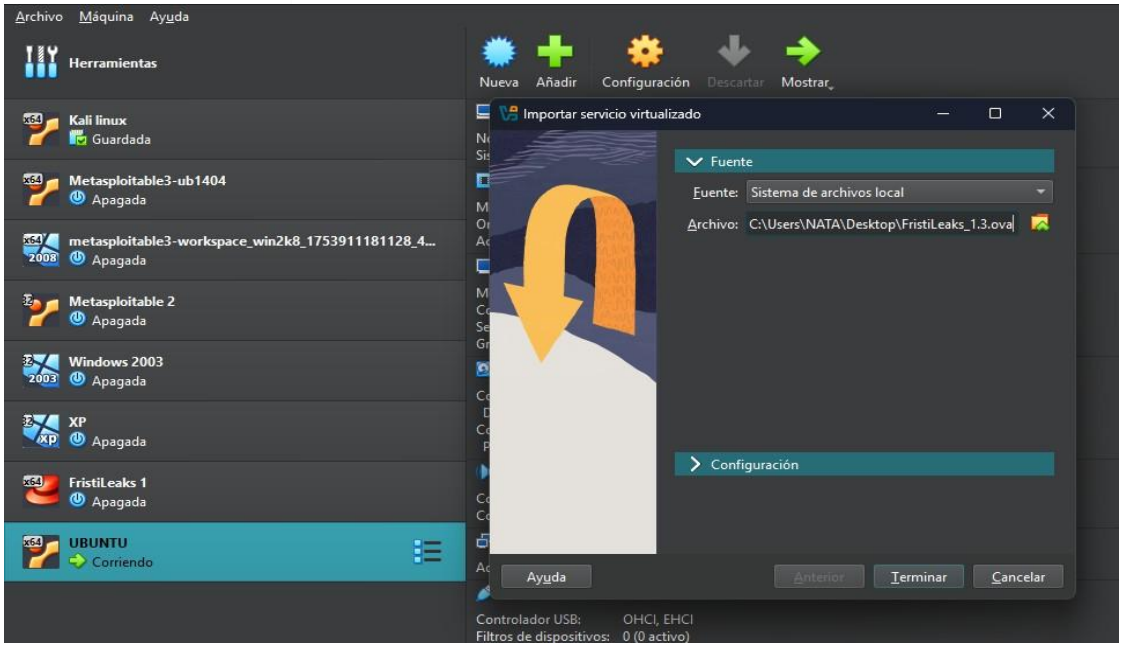


Ilustración 2 Importación de la Ova

En esta ventana cargo automáticamente la Fuente como Sistema de archivos local y se cargó el archivo FristiLeaks_1.3.ova desde la ruta en la que se encuentra el archivo. Luego, se hizo clic en el botón **Terminar** y VirtualBox procedió a registrar la máquina virtual y agregarla a la lista de máquinas disponibles.

Como paso siguiente, la máquina virtual de **FristiLeaks** requería el uso de una dirección MAC específica, ya que, de no configurarse correctamente, el sistema no obtenía una dirección IP por medio de DHCP y, en consecuencia, no podía conectarse a la red del laboratorio.

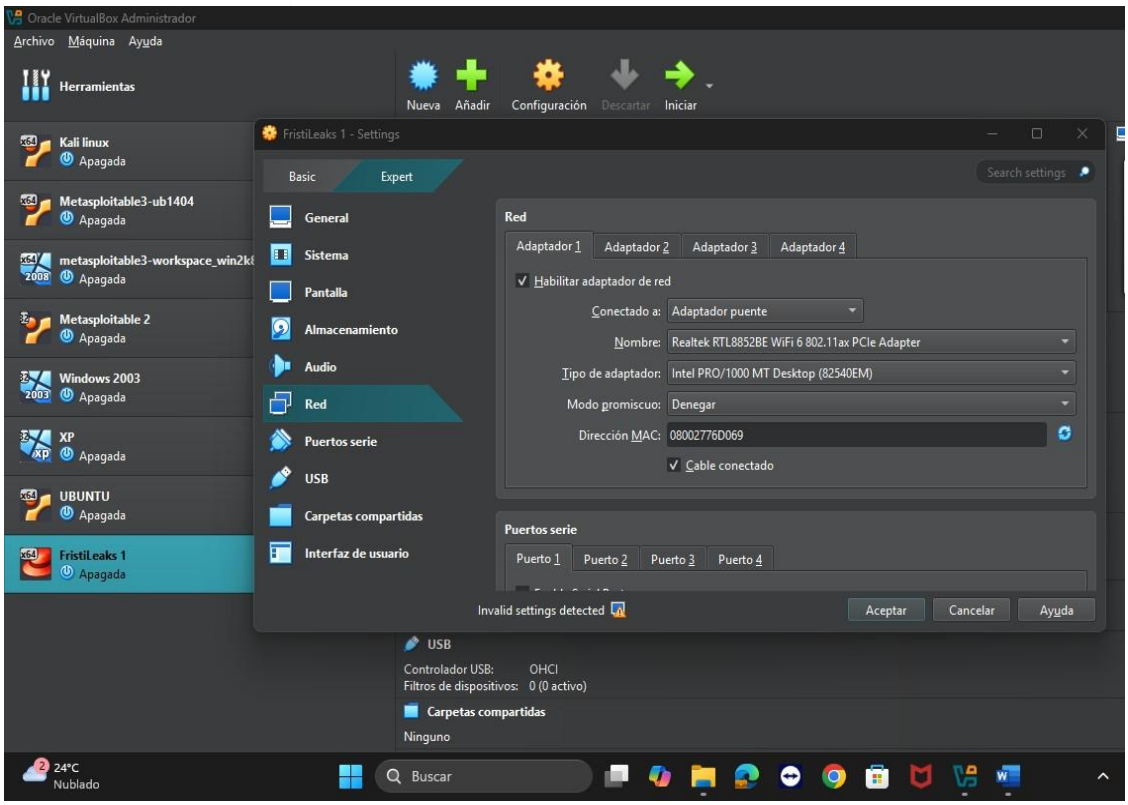


Ilustración 3 Dirección MAC predeterminada en VirtualBox para la OVA FristiLeaks

Para acceder a esta configuración, se seleccionó la máquina virtual Fristelaks dentro de VirtualBox y se hizo clic en el botón **Configuración** ubicado en la parte superior de la ventana principal. En el panel lateral izquierdo, se eligió la opción Red, que permitió visualizar los parámetros relacionados con la conexión del adaptador.

Apareció una pestaña donde se muestra, el apartado correspondiente **al Adaptador 1**, también se visualiza la dirección **MAC** por defecto asignada automáticamente por VirtualBox antes de realizar el cambio requerido.

En esta imagen se muestra el resultado de iniciar la máquina virtual con la dirección MAC predeterminada asignada por VirtualBox. Se observa que, con esta configuración, la máquina no logra adquirir una dirección IP mediante DHCP.

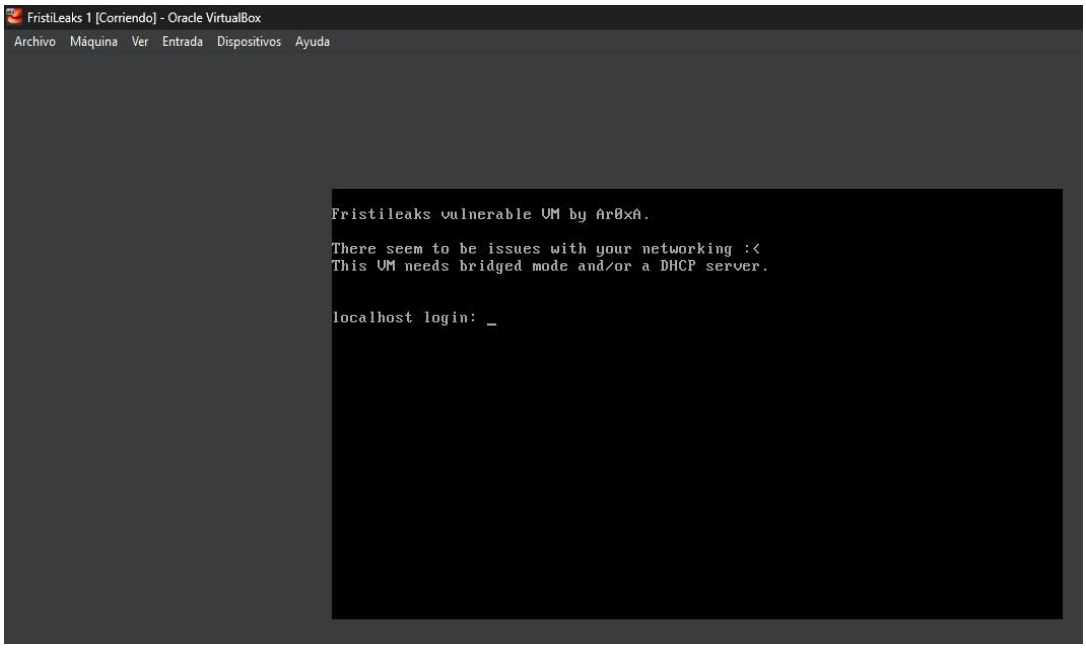


Ilustración 4 Resultado del arranque de FristiLeaks con la MAC predeterminada

Lo que se mostró fue una pantalla indicando problemas con la conexión de red. En el mensaje se señalaba que la máquina necesitaba contar con un servidor DHCP para obtener una dirección IP. Esto mostro que, con la MAC inicial, el sistema no lograba conectarse correctamente a la red que se usó para el laboratorio.

Como esta condición había sido establecida, se modificó de forma manual la dirección MAC del adaptador de red en VirtualBox, usando el valor específico que se había proporcionado para el laboratorio.

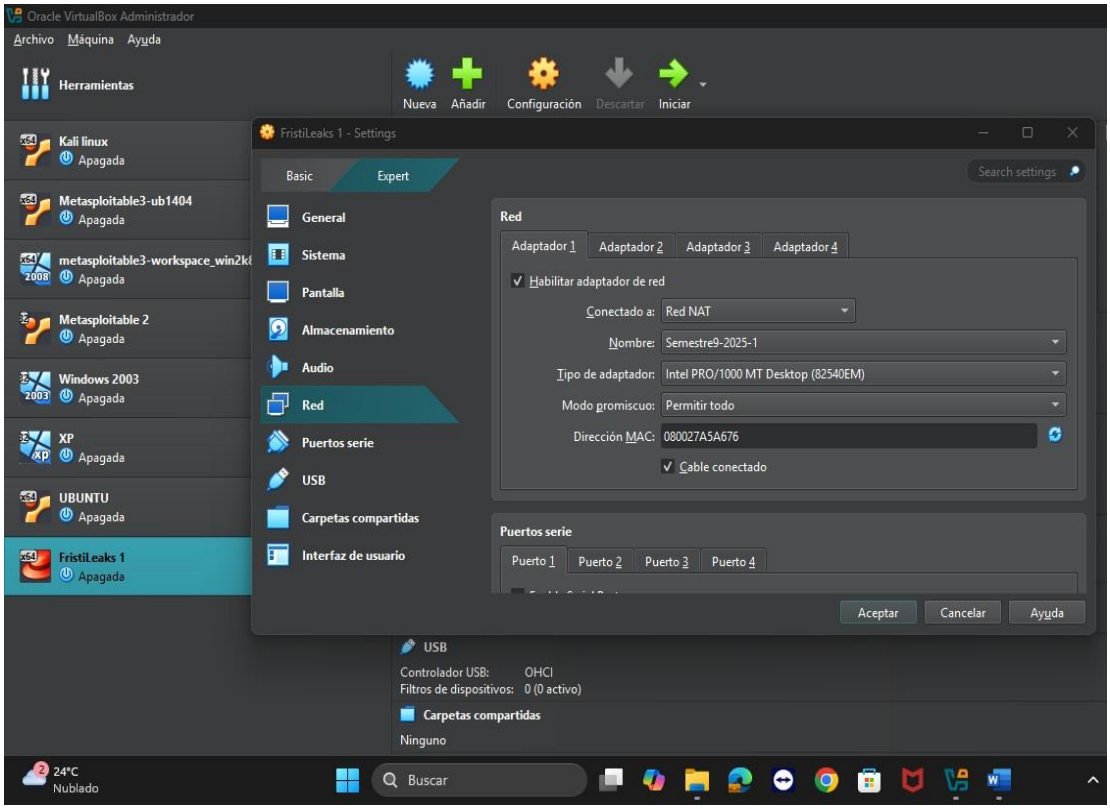


Ilustración 5 Establecimiento de la dirección MAC específica en VirtualBox para la VM FristiLeaks

Para ello se abrió VirtualBox y se seleccionó la máquina Fristelaks en la lista del menú izquierdo. Luego se hizo clic en el botón Configuración del menú superior y, dentro de la ventana que apareció, se ingresó a la **pestaña Red**. En esa pestaña se habilitó el adaptador de red y se comprobó que estuviera conectado a la opción **Red NAT** y en el campo Dirección MAC, se reemplazó el valor predeterminado por un nuevo valor y se confirmó el cambio con el botón **Aceptar** para guardar la configuración.

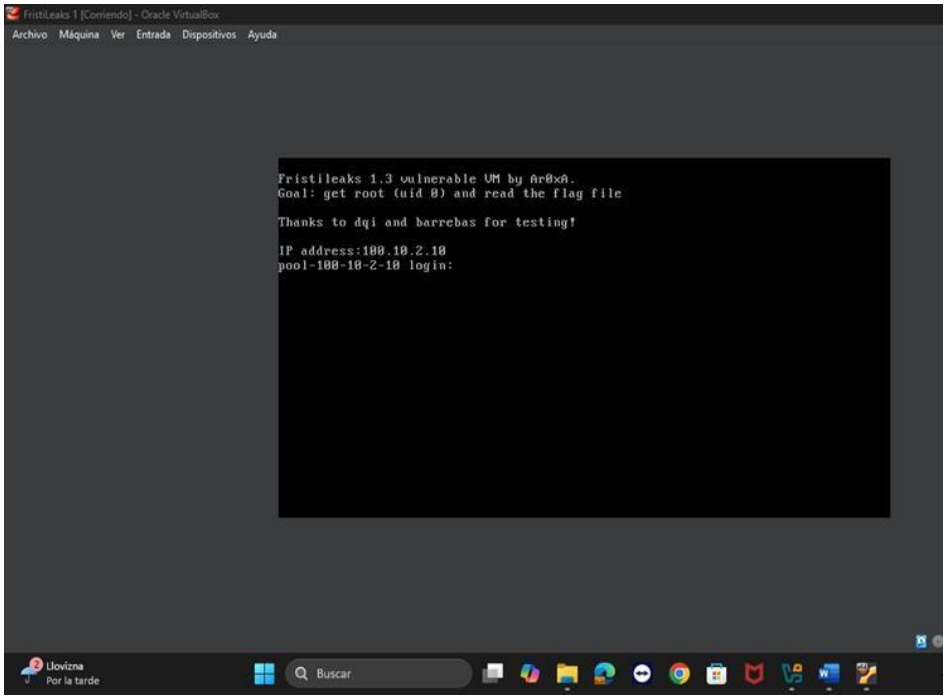
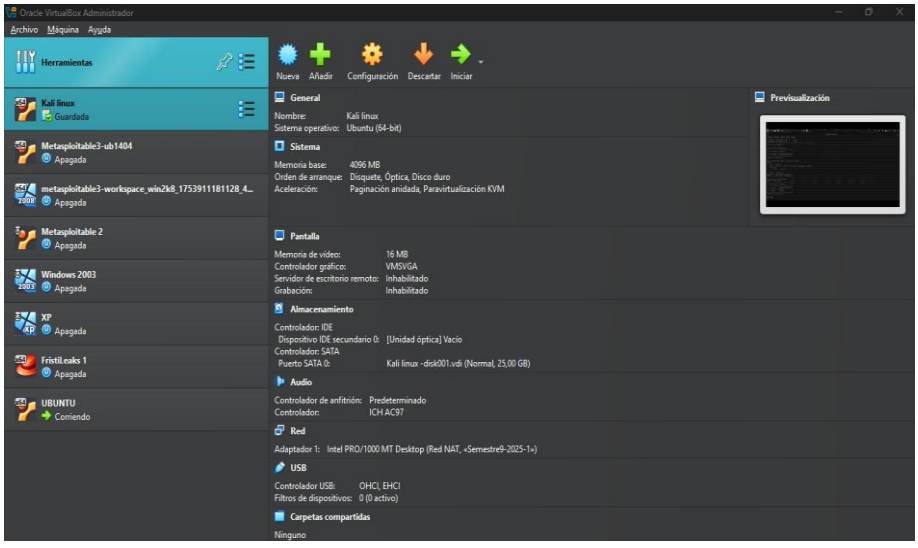


Ilustración 6 Obtención de dirección IP en FristiLeaks tras configurar la MAC

Después de realizar el cambio de la dirección MAC, se inició nuevamente la máquina virtual Fristelaks. En la pantalla se pudo observar que esta vez la conexión de red funcionó correctamente y el sistema obtuvo una dirección IP asignada por DHCP.



Universidad Tecnológica del Chocó
Diego Luis Córdoba

Se inició también la máquina Kali Linux. Para ello, se abrió VirtualBox y, en la lista de máquinas disponibles, se seleccionó la que correspondía a Kali Linux. Luego se hizo clic en el botón Iniciar, ubicado en la parte superior del menú.

Ilustración 7 Resultado del escaneo de red con Nmap

Una vez dentro de Kali Linux, se abrió una nueva terminal para realizar un escaneo general del segmento de red y reconocer los equipos que estaban activos. En la imagen se observa la ejecución del comando nmap -sV 100.10.2.0/24, que permitió obtener información sobre los dispositivos conectados, los puertos abiertos y los servicios que se encontraban en ejecución dentro de la red del laboratorio.

Ilustración 8 Host FristiLeaks

En los resultados del escaneo se identificó un equipo con el puerto 80 abierto, donde se ejecuta un servidor Apache con soporte para PHP. Este host corresponde a la máquina Fristelaks.

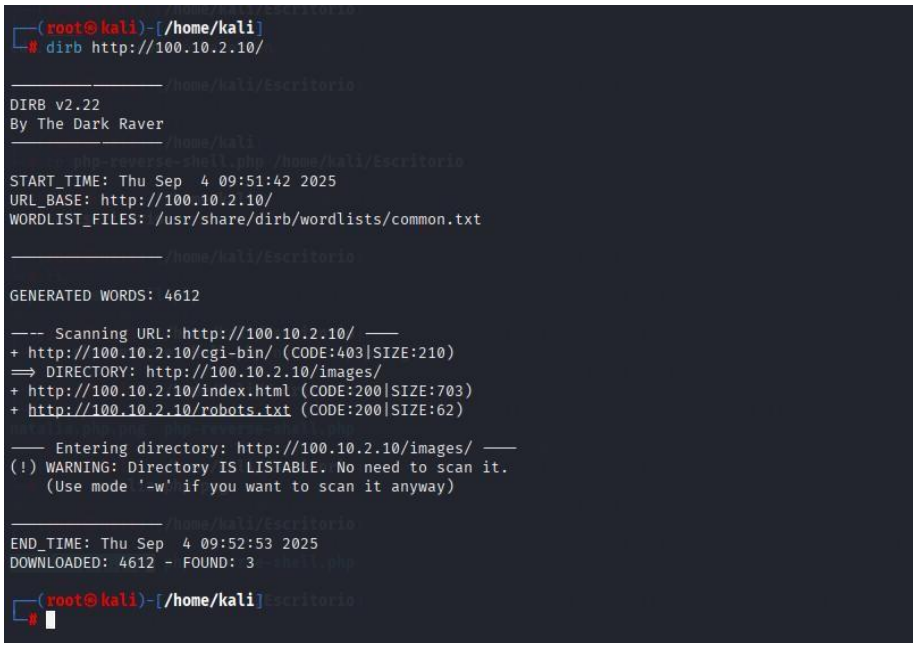


Ilustración 9 Resultados del análisis de fuerza bruta con dirb en el host 100.10.2.10

En este paso se utilizó la herramienta dirb con el fin de realizar un análisis de fuerza bruta sobre la aplicación web de la máquina víctima. El comando empleado fue: dirb http://100.10.2.10/

La función de este comando es comparar las rutas del sitio web con un diccionario de palabras (en este caso common.txt), permitiendo así descubrir directorios y archivos ocultos que no son visibles de forma directa en la navegación.

En el resultado se identificaron varias rutas incesantes como /cgi-bin/, /images/, /index.html y /robots.txt, las cuales fueron navegadas en busca de pistas, pero no hubo resultados exitosos.

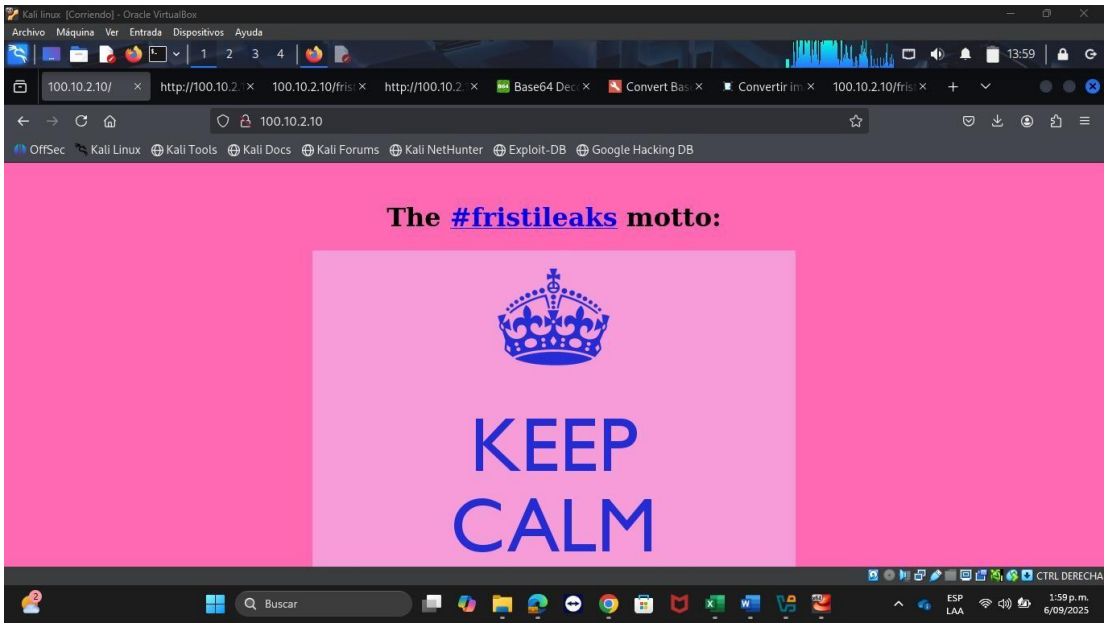


Ilustración 10 Interfaz inicial del servidor Apache

Se accedió desde el navegador a la dirección IP correspondiente a la máquina víctima. En el escaneo se había comprobado que la máquina tenía un servidor Apache activo, el cual muestro una interfaz web inicial. Sobre esta interfaz se procedió a realizar pruebas de seguridad con el objetivo de identificar posibles vulnerabilidades explotables.

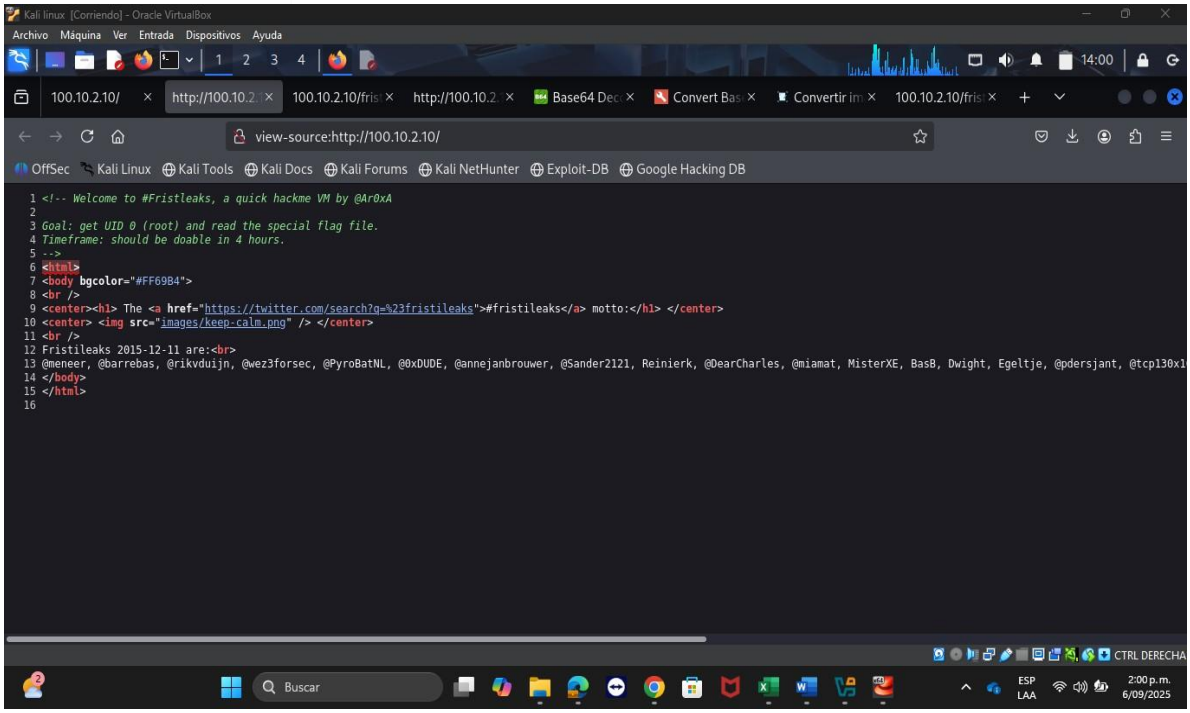


Ilustración 11 Visualización del código fuente de la página web

Como paso siguiente, se procedió a visualizar el código fuente de la página web con el propósito de identificar posibles pistas que pudieran revelar credenciales u otra información sensible.

Para ello, en la interfaz principal se hizo clic derecho sobre la interfaz y se seleccionó la opción

View Page Source (Ver código fuente de la página) pero aquí no se encontraron credenciales. Por ello se siguió navegando por otras rutas:

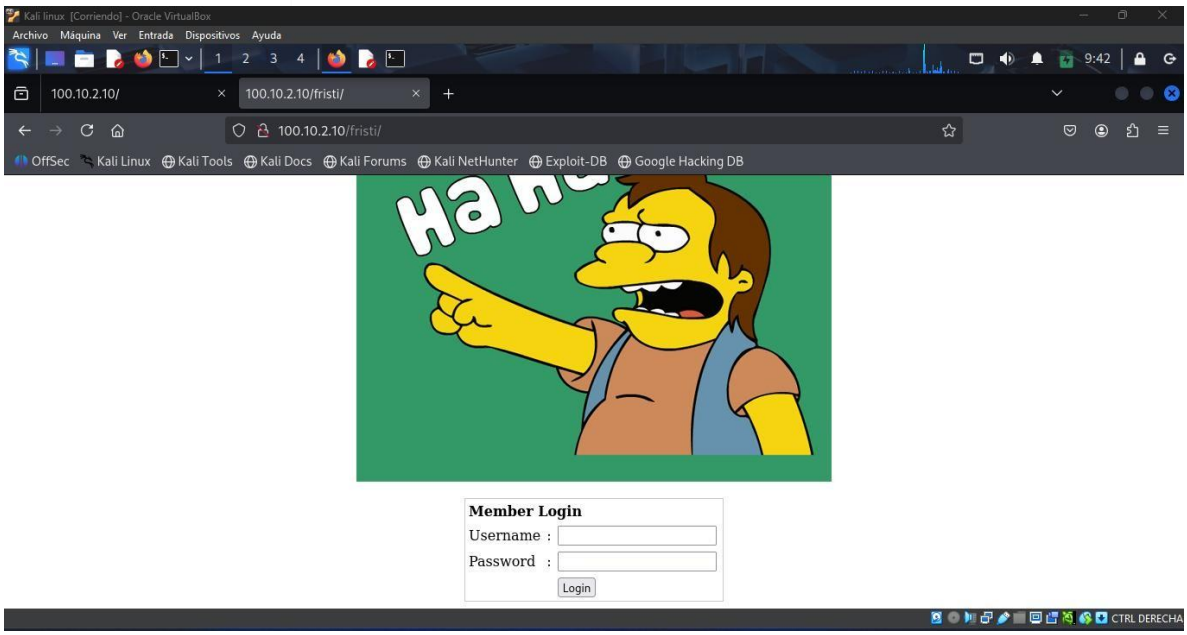


Ilustración 12 Interfaz del Login de la aplicación web FristiLeaks

Una de ellas fue la dirección 100.10.2.10/fristi, se observó una página con una imagen grande y, debajo, un formulario de inicio de sesión. En el formulario aparecían los campos Username y Password, junto con un botón Login, indicando que el acceso a esa sección del sitio estaba protegido mediante autenticación. Esta interfaz fue registrada como un punto de interés para las siguientes etapas de reconocimiento.

Sin embargo, en este punto no se disponía aún con credenciales de acceso válidas. Ante esta situación, se procedió a inspeccionar el código fuente de esta página aplicando el mismo procedimiento: clic derecho sobre la interfaz y selecciono la opción **Ver código fuente**.

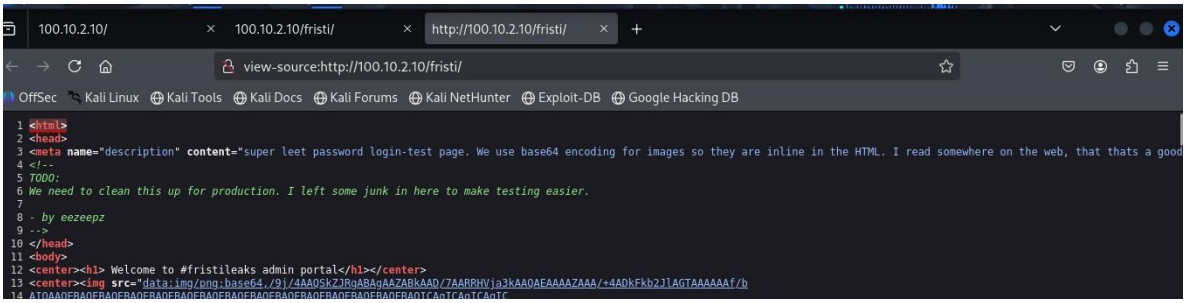


Ilustración 13 Posible usuario en el código fuente del formulario de Login

Al inspeccionar el código fuente del formulario de Login, se identificaron varios elementos de interés. Entre ellos, un posible nombre de usuario referenciado en los comentarios del HTML **eezeepz**, así como una imagen codificada en base64 que podría contener información oculta.

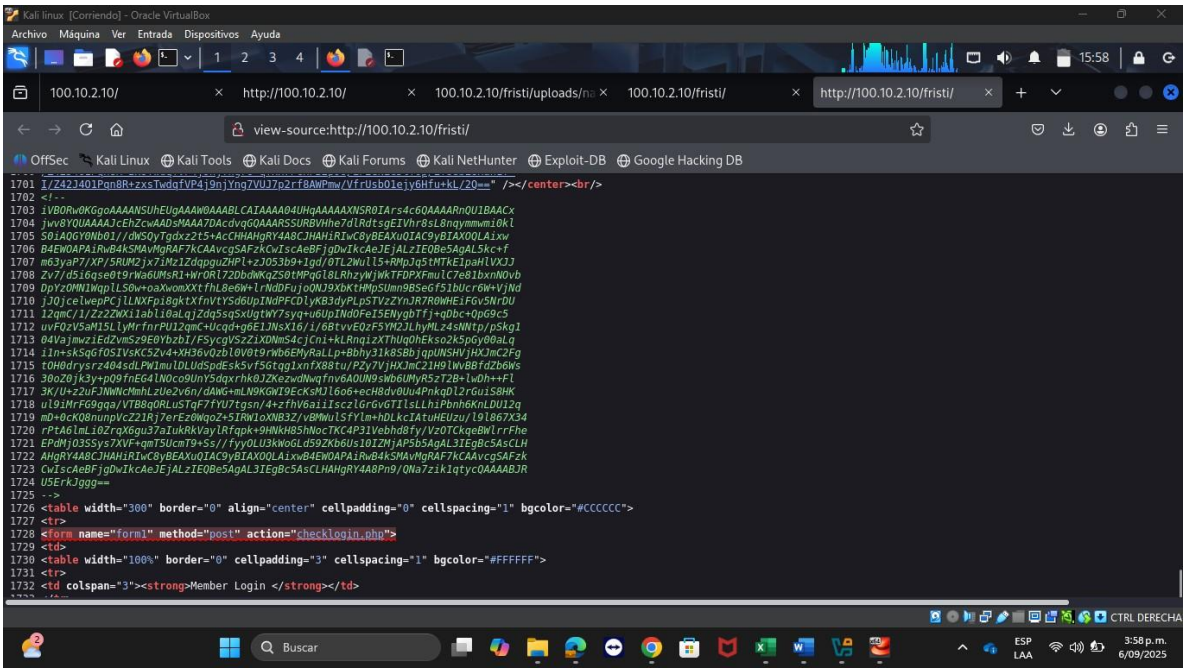


Ilustración 14 Imagen codificada en base64

Se procedió a copiar el bloque de datos codificado en base64 identificado en el código fuente, se utilizó un decodificador de base 64 a binario, accesible desde el navegador. En este se

pegó el código con el objetivo de analizar la información oculta en la imagen. Como se observa en la siguiente imagen.

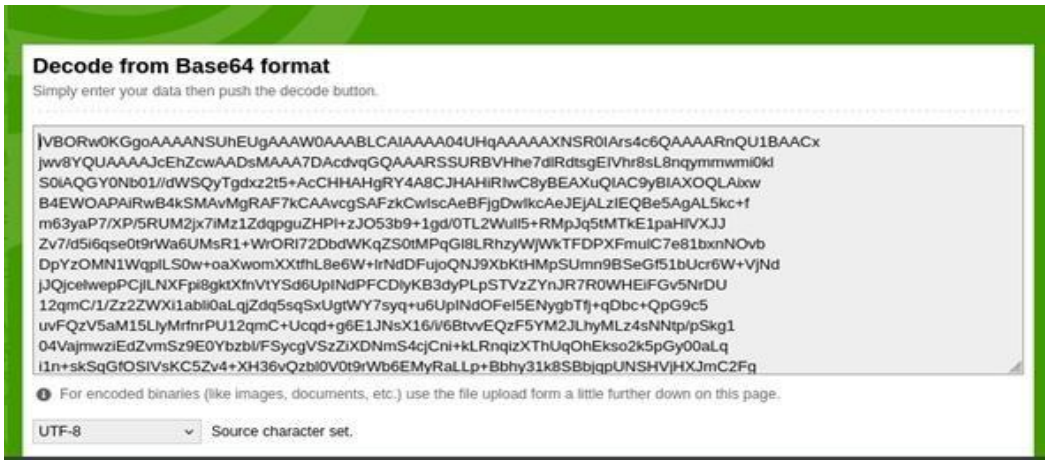


Ilustración 15 Uso de un decodificador online

El resultado de la decodificación fue una imagen en formato PNG. Aquí se evidenció que la aplicación web aceptaba archivos con extensión .png en su proceso de carga. Esta característica abrió la posibilidad de aprovechar dicha funcionalidad para intentar una inyección a través de un archivo manipulado.

Ilustración 16 Decodificación del contenido en base64

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Luego, se realizó la decodificación del contenido base64 a formato PNG, con el objetivo de obtener y visualizar la imagen oculta.

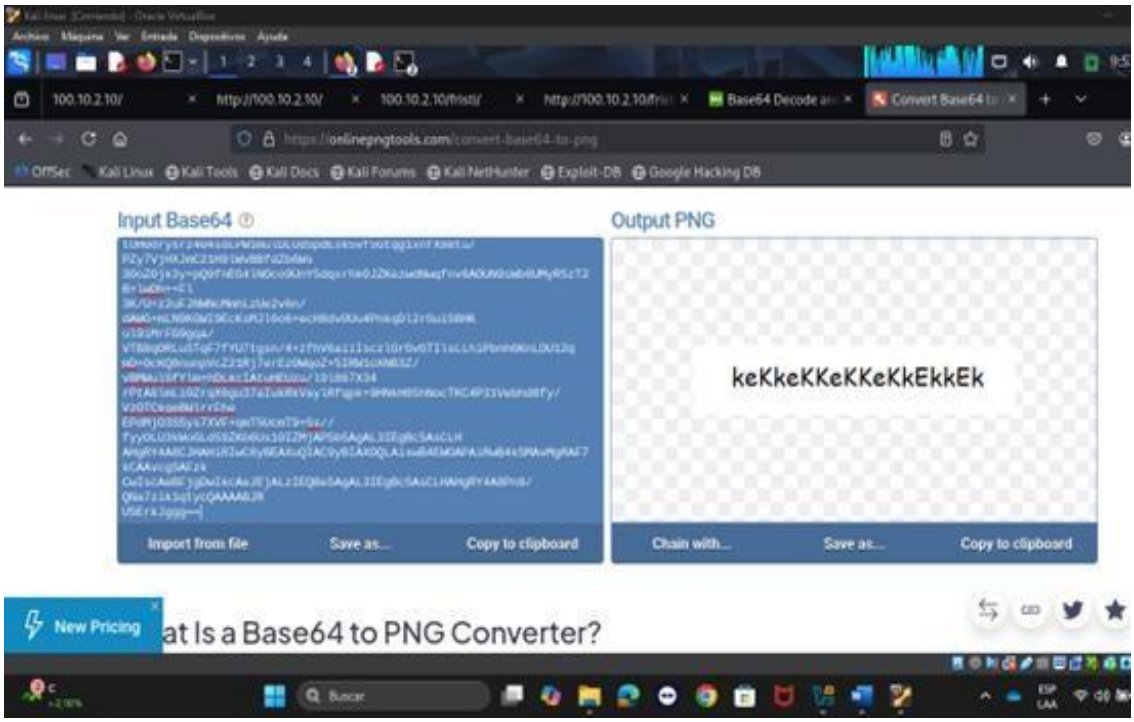


Ilustración 17 Resultado de la decodificación base64 a imagen PNG

El resultado fue una imagen en la que se mostraba una cadena de texto que podría corresponder a una posible contraseña. Aquí ya se encontró un nuevo indicio para intentar acceder al formulario de Login.

Por lo cual, se procedió a probar el usuario identificado y la contraseña extraída como se observa en la siguiente imagen:

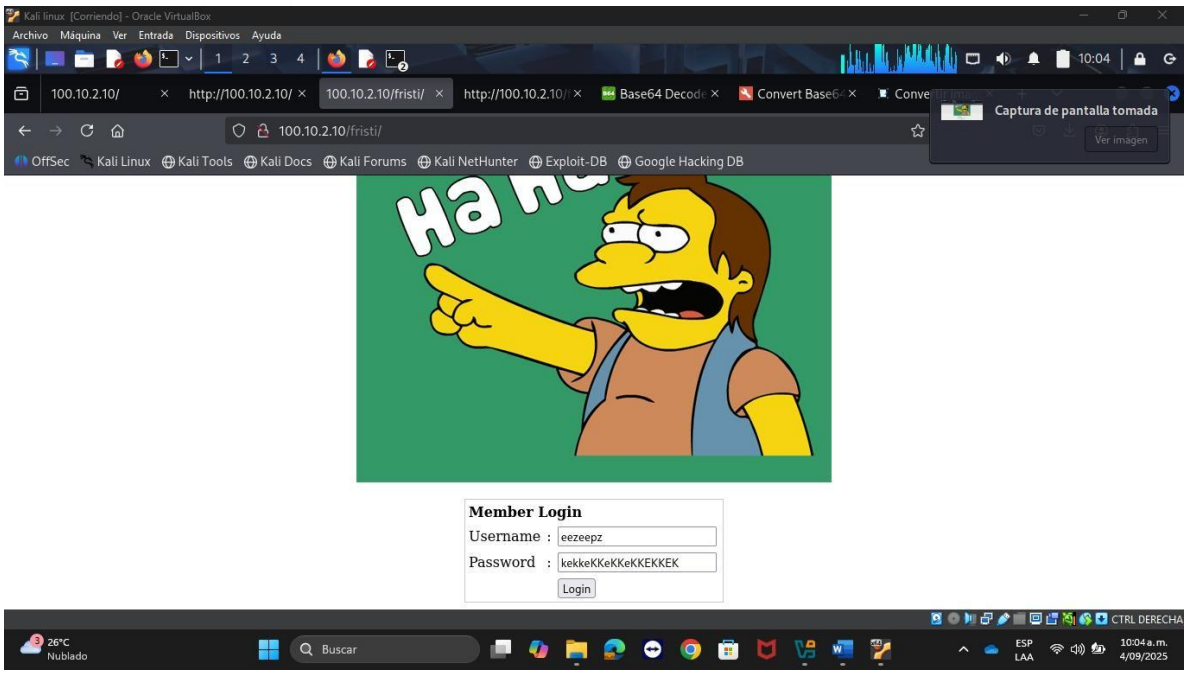


Ilustración 18 Autenticación de credenciales

En esta ventana se ingresaron las credenciales identificadas durante la exploración: el usuario **eezeepz**, hallado como comentario en el código fuente, y la contraseña **kekekeKekKekKEkKEK**, obtenida al decodificar el texto presente en la imagen. Estos datos se introdujeron en los campos **Username y Password** del formulario para probar el acceso al sistema.

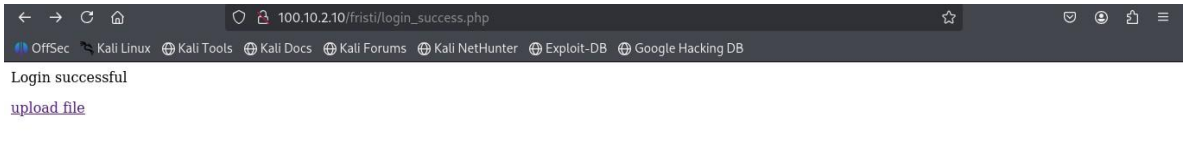


Ilustración 19 Login exitoso

Después de ingresar las credenciales en el formulario, el sistema mostró un mensaje que confirmaba el inicio de sesión exitoso con la frase **Login successful**. Debajo del mensaje apareció

un enlace llamado **Upload file**, indicando que el acceso había sido concedido y que ahora era posible interactuar con una opción para subir archivos.

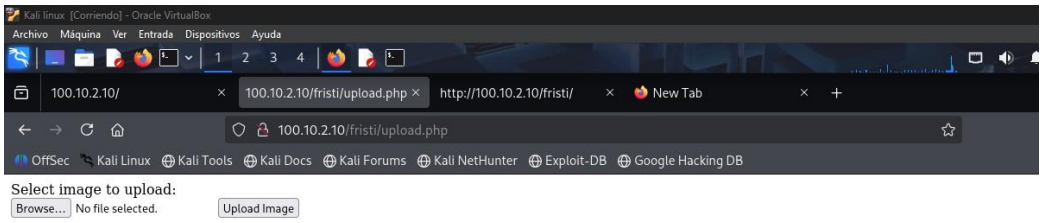


Ilustración 20 Portal de carga de archivos

Al hacer clic en dicho botón, el sistema redirigió a esta ventana específica que permitía realizar la subida de archivos, en específico imágenes ya que se observó el botón de Upload Image.

Allí se realizó una pausa y se regresó a la terminal:

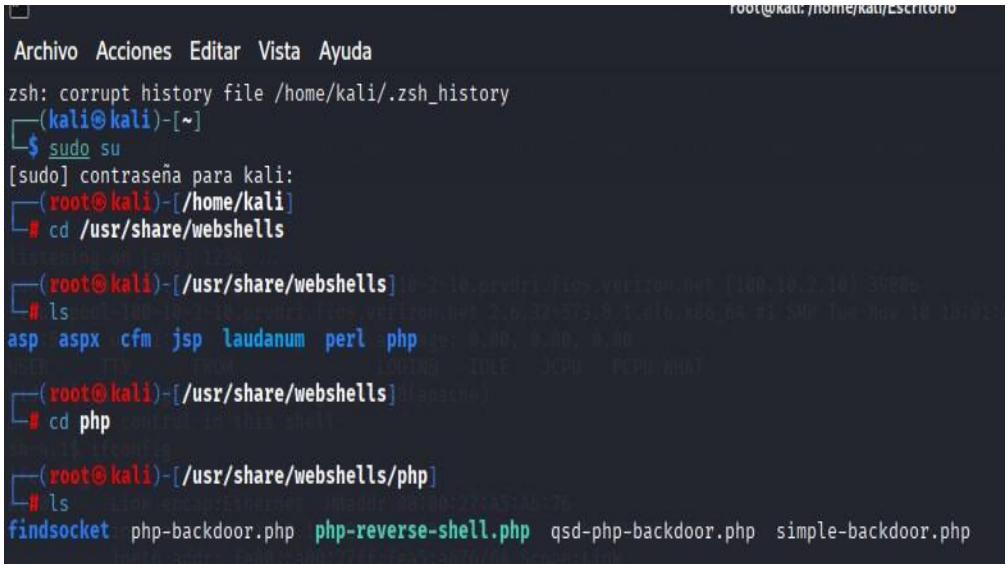


Ilustración 21 Ubicación del archivo php-reverse-shell.php

Aquí se volvió a la terminal y se navegó hasta la carpeta de webshells usando cd /usr/share/webshells/php/. Allí se listaron los archivos con ls y se confirmó que el directorio

contenía varios recursos. Luego, se entró al subdirectorio php usando cd php, se volvió a listar el contenido con ls y se localizó el archivo php-reverse-shell.php

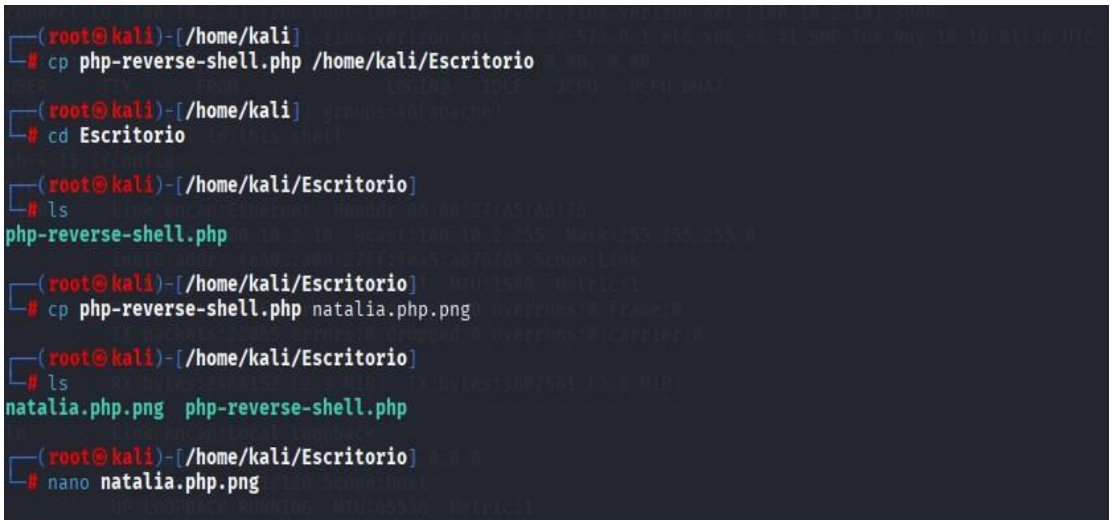


Ilustración 22 Renombrado del archivo reverse

En este paso, se regresó a la carpeta personal con cd /home/Kali y se copió el archivo php-reverse-shell.php al Escritorio, para ello se usó el comando cp php-reverse-shell.php /home/Kali/Escritorio. Como siguiente, se navegó a la ruta del escritorio con **cd Escritorio** y ls para listar los archivos, allí se encontró ya disponible el archivo copiado.

El paso siguiente fue crear una copia del archivo con el nombre natalia.php.png, como se observa en la imagen se usó la instrucción **cp** seguido del nombre del archivo y al lado el nuevo nombre de modo que el archivo adoptara una apariencia de imagen, luego, se abrió ese archivo con el editor de texto nano con el comando **nano natalia.php.png** para revisar y ajustar su contenido y poder adaptarlo a la estructura necesaria para que, a simple vista, pareciera una imagen pero conservara el código preparado para la hacer el **Exploit.**

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Al ejecutar esta instrucción la pestaña que se mostro fue la siguiente:

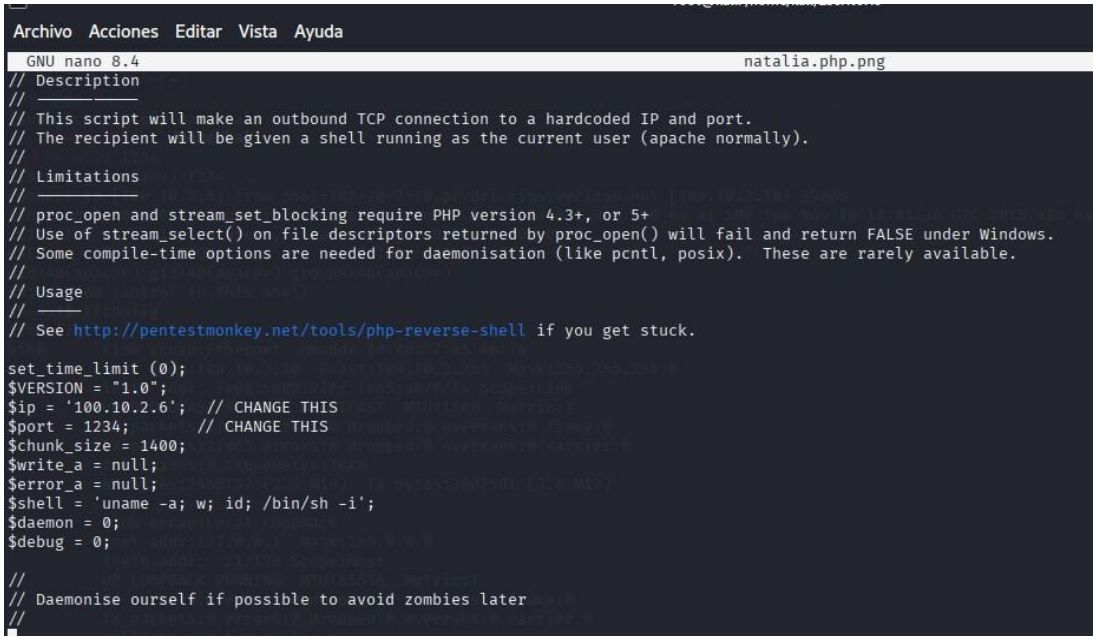


Ilustración 23 Edición del archivo reverse shell

En esta pestaña, del editor se mostró el título GNU nano 8.4 seguido del nombre del archivo natalia.php.png, indicando que el archivo fue abierto con ese editor. En el área de edición aparecieron los comentarios iniciales del script y, justo debajo, las líneas de configuración donde se realizaron los cambios: la variable de la ip quedó establecida en 100.10.2.6 y la del port en 1234: IP del atacante a 100.10.2.6 y Puerto de escucha a 1234. Y se guardaron los cambios del archivo.

Una vez guardados los cambios realizados en el archivo **natalia.php.png**, se regresó al portal web que contenía la opción para subir imágenes.

Ilustración 24 Carga de archivos

En esta ventana recordemos que se mostró el campo Select image to **Upload** junto con los botones Browse y Upload Image. Se hizo clic en el botón Browse, lo que abrió la ventana del sistema para explorar las carpetas del equipo.

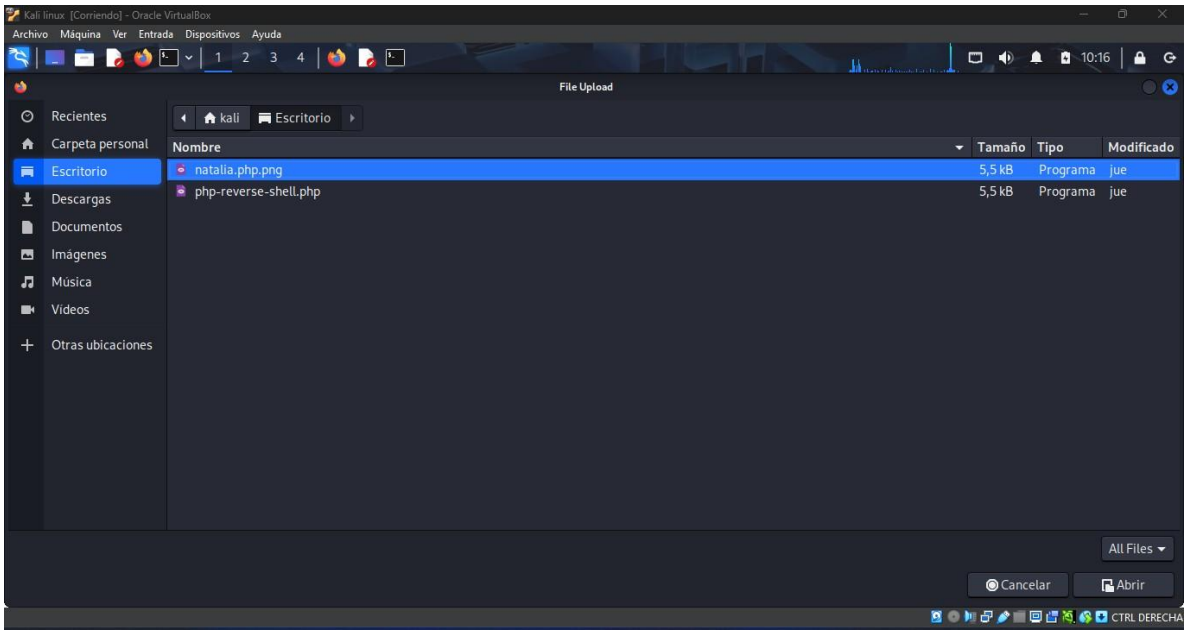


Ilustración 25 Archivo script

En esta ventana de selección de archivos se accedió al directorio **Escritorio**, donde se mostraban los archivos disponibles. Entre ellos, el archivo **natalia.php.png**, el cual se ha

preparado para realizar el **Exploit** en el paso anterior. Se hizo clic sobre dicho archivo para resaltarlo y, se presionó el botón **Abrir** ubicado en la parte inferior derecha de la ventana.

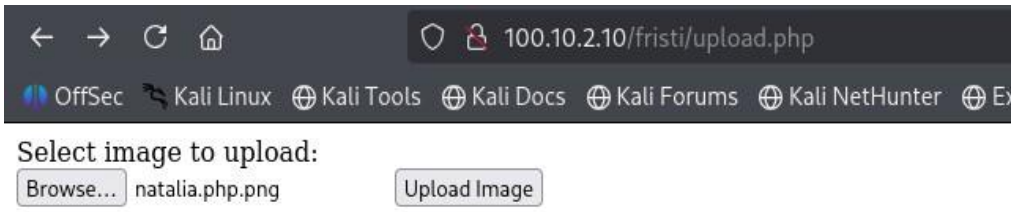


Ilustración 26 Script php cargado

Una vez seleccionado el archivo en la ventana anterior, el navegador mostró nuevamente la interfaz del portal web. En la pantalla se podía ver que junto al botón **Browse** aparecía el nombre del archivo natalia.php.png, lo que confirmaba que había realizado correctamente la selección del archivo.

Con el archivo ya cargado en el campo de selección, el siguiente paso consistió en hacer clic sobre el botón **Upload Image** para enviar el archivo al servidor, se recargo la pagina y mostro la siguiente información:

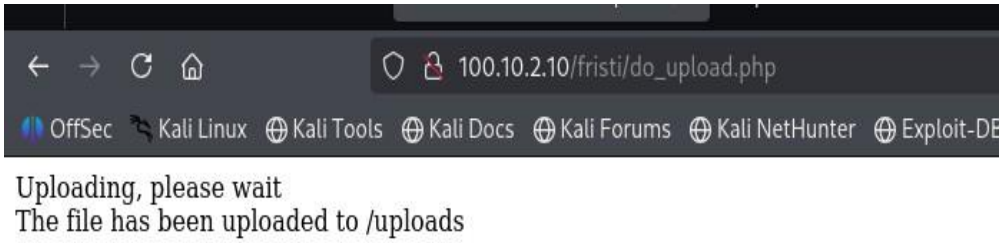


Ilustración 27 Nueva ventana después de la carga del script

Un mensaje en pantalla indicando el progreso de la carga con la frase Uploading, please wait. Luego, al completarse el proceso, apareció el texto The file has been uploaded to /uploads, indicando que el archivo había sido subido a ese directorio /uploads del servidor.

Como paso siguiente, se minimizó el navegador y se volvió a la terminal de Kali Linux para continuar con el proceso. Una vez en la consola, se cambiaron los permisos a usuario administrador utilizando el comando sudo su, ingresando la contraseña correspondiente. Ya con privilegios de superusuario, se ejecutó el comando nc -lvp 1234, con el cual la terminal quedó en estado de escucha en el puerto 1234

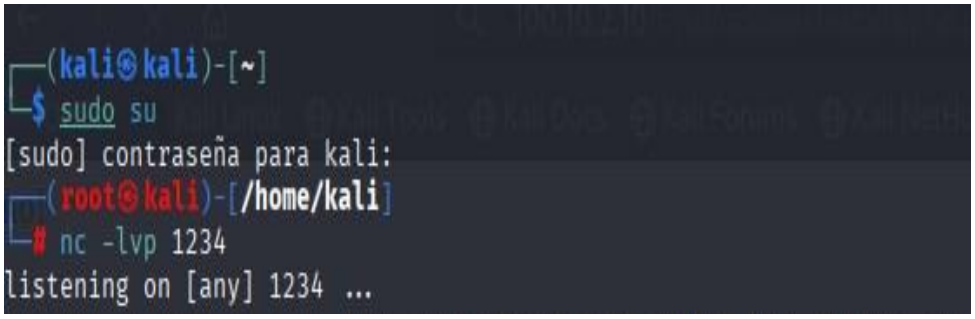


Ilustración 28 Escucha del puerto 1234

Este paso se realizó porque, al momento de editar el archivo natalia.php.png, se había configurado el puerto 1234 como el canal de comunicación, por lo que fue necesario dejar la terminal en escucha en ese mismo puerto para esperar la conexión proveniente de la máquina remota.

De vuelta en el navegador, se accedió a la **ruta /uploads**, tal como se indicó tras la carga del archivo. Al ingresar, el sistema respondió con el mensaje no!

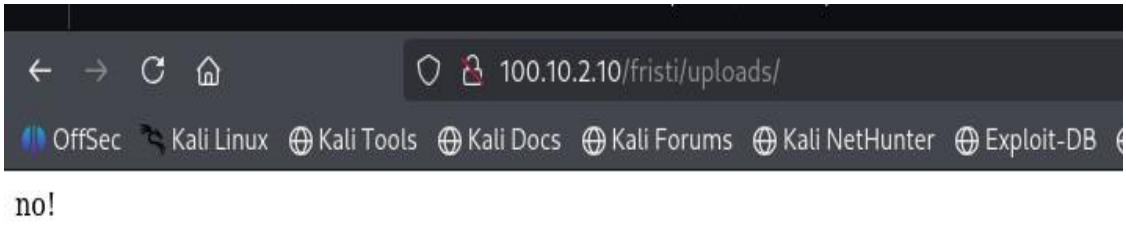


Ilustración 29 Ruta /uploads

Aunque la respuesta inicial de la aplicación mostró el mensaje “no!”, lo que hacía pensar que la carga había fallado, el archivo sí se había almacenado correctamente en el servidor. Para comprobarlo, se ingresó manualmente en el navegador la ruta completa del archivo dentro del directorio de subidas, **100.10.2.10/fristi/uploads/natalia.php.png**

Ilustración 30 Ejecución del archivo

Al ingresar, la página quedo en carga sin mostrar errores visibles, lo que confirmó que el archivo se encontraba alojado en el servidor

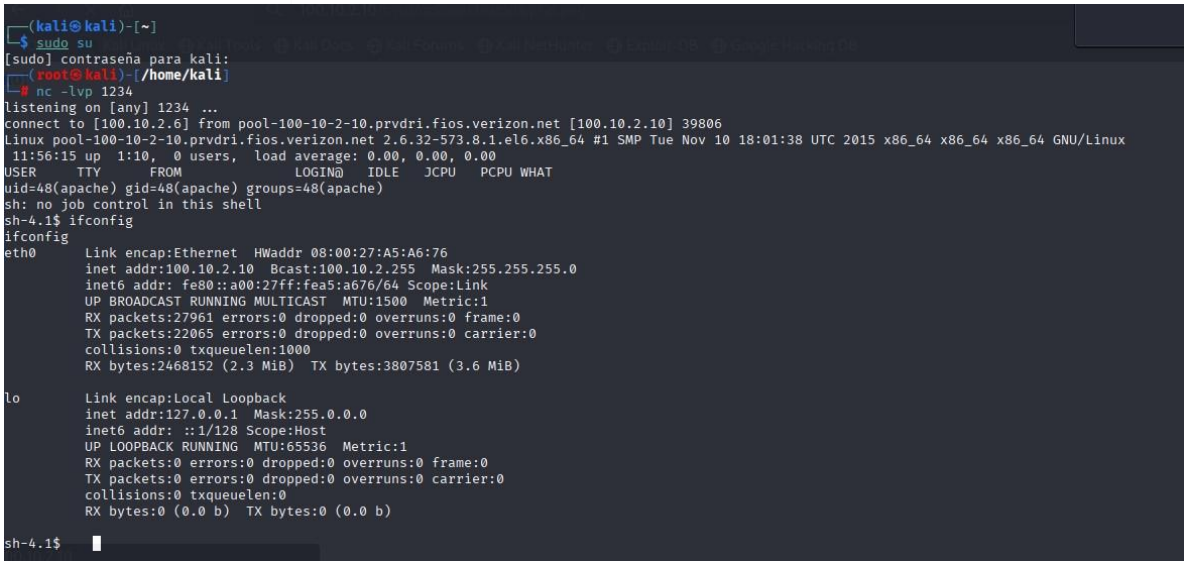


Ilustración 31 Establecimiento de conexión inversa desde la víctima hacia la máquina atacante con netcat

Al volver a la terminal donde estaba en escucha con nc -lvp 1234, se registró inmediatamente una conexión entrante desde la IP de la máquina víctima. Apareció la línea que indicaba **connect from** 100.10.2.10 y, acto seguido, se recibió el banner del sistema remoto.

La sesión remota entregó un intérprete de comandos con el usuario del servicio web (UID 48, apache), tal como lo mostraron las primeras líneas posteriores a la conexión. Desde esa shell se ejecutaron comprobaciones básicas: se observó la información de identidad del usuario conectado y la salida de ifconfig, que mostró la interfaz eth0 con la dirección 100.10.2.1

1.1 CREACIÓN DE DOS NUEVOS USUARIOS A FRISTILEAKS

En la segunda parte del capítulo 1, el propósito fue crear dos nuevos usuarios dentro del sistema FristiLeaks. Aquí se continuo desde la sesión obtenida con anterioridad a FristiLeaks.

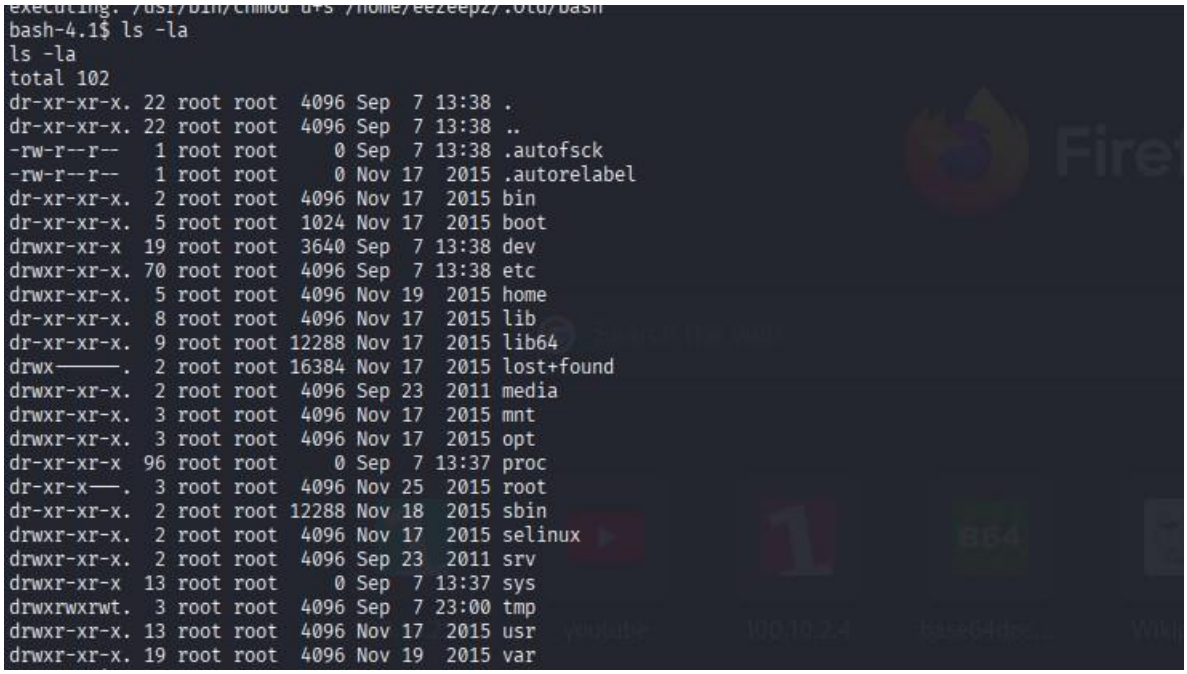


Ilustración 32 Listado de archivos FristiLeaks

Una vez en la sesión interactiva, se utilizó el comando **ls -la** para listar el contenido del directorio raíz (/). Este comando mostró todas las carpetas y archivos principales del sistema junto con sus permisos, propietarios y fechas. En la salida aparecieron rutas importantes como bin, boot, home, lib, opt, root, tmp, usr y var.

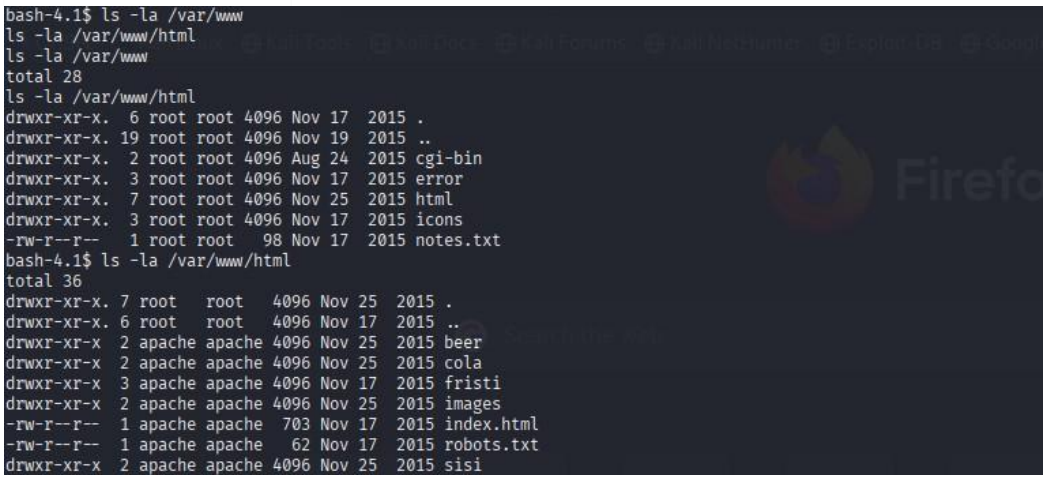


Ilustración 33 Directorio archivos servidor web

En este paso se exploró el sistema para identificar los directorios del servidor web. Para ello, se ejecutó el comando **ls -la /var/www/,** que permitió acceder al contenido de la carpeta principal donde se almacenan los archivos del sitio. Luego, se ingresó a la subcarpeta **html** mediante el comando **ls -la /var/www/html**, donde se observaron varios directorios y archivos, entre ellos beer, cola, fristi, images, index.html, robots.txt y sisi.

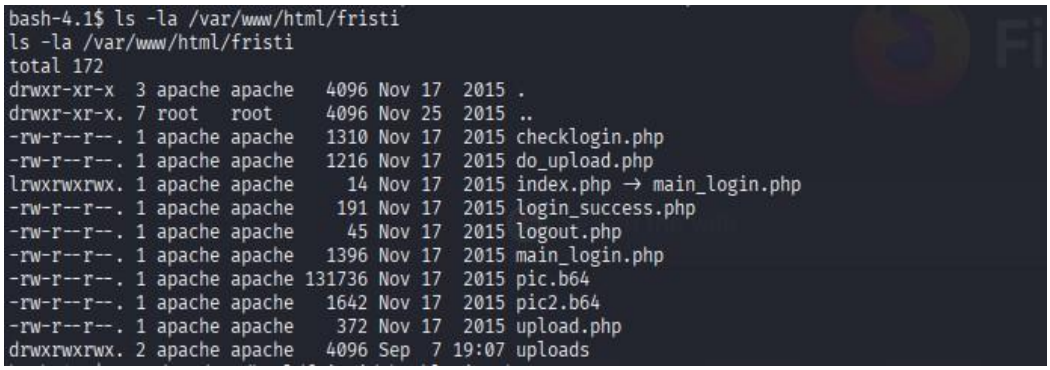


Ilustración 34 Ruta fristi directorio de archivos

Como en pasos anteriores se había encontrado un formulario de inicio de sesión en la ruta **/fristi**, se decidió ingresar a ese mismo directorio dentro del sistema para analizar su estructura

interna. Por eso, se ejecutó el comando **ls -la /var/www/html/fristi**, para revisar los archivos que componían el sitio. En esta ubicación se identificaron varios ficheros importantes, entre ellos checklogin.php, main_login.php, do_upload.php, login_success.php y la carpeta Upload

Como paso siguiente, se eligió navegar el archivo **checklogin.php** porque es el encargado de validar las credenciales de acceso dentro del portal, y se encontraba en la ruta **/var/www/html/fristi/ checklogin.php**.

```
bash-4.1$ cat /var/www/html/fristi/checklogin.php
cat /var/www/html/fristi/checklogin.php
<?php

ob_start();
$host="localhost"; // Host name
$username="eezeepz"; // Mysql username
$password="4ll3maal12#"; // Mysql password
$db_name="hackmenow"; // Database name
$tbl_name="members"; // Table name

// Connect to server and select databse.
mysql_connect("$host", "$username", "$password")or die("cannot connect");
mysql_select_db("$db_name")or die("cannot select DB");

// Define $myusername and $mypassword
$myusername=$_POST['myusername'];
$mypassword=$_POST['mypassword'];

// To protect MySQL injection (more detail about MySQL injection)
$myusername = stripslashes($myusername);
$mypassword = stripslashes($mypassword);
$myusername = mysql_real_escape_string($myusername);
$mypassword = mysql_real_escape_string($mypassword);

$sql="SELECT * FROM $tbl_name WHERE username='$myusername' and password='$mypassword'";
$result=mysql_query($sql);
```

Ilustración 35 Análisis del archivo checklogin.php

Al analizar este archivo **checklogin.php**, se identificaron credenciales de conexión a la base de datos MySQL. Estas credenciales corresponden al usuario **eezeepz**, con la contraseña **4ll3maal12#,** y apuntan a la base de datos **hackmenow**, y a la tabla **members.**

Universidad Tecnológica del Chocó
Diego Luis Córdoba

Con las credenciales halladas en checklogin.php, se estableció conexión al servidor MySQL desde la sesión obtenida. Para ello se ejecutaron el comando: mysql -u eezeepz -p4ll3maal12# -h localhost

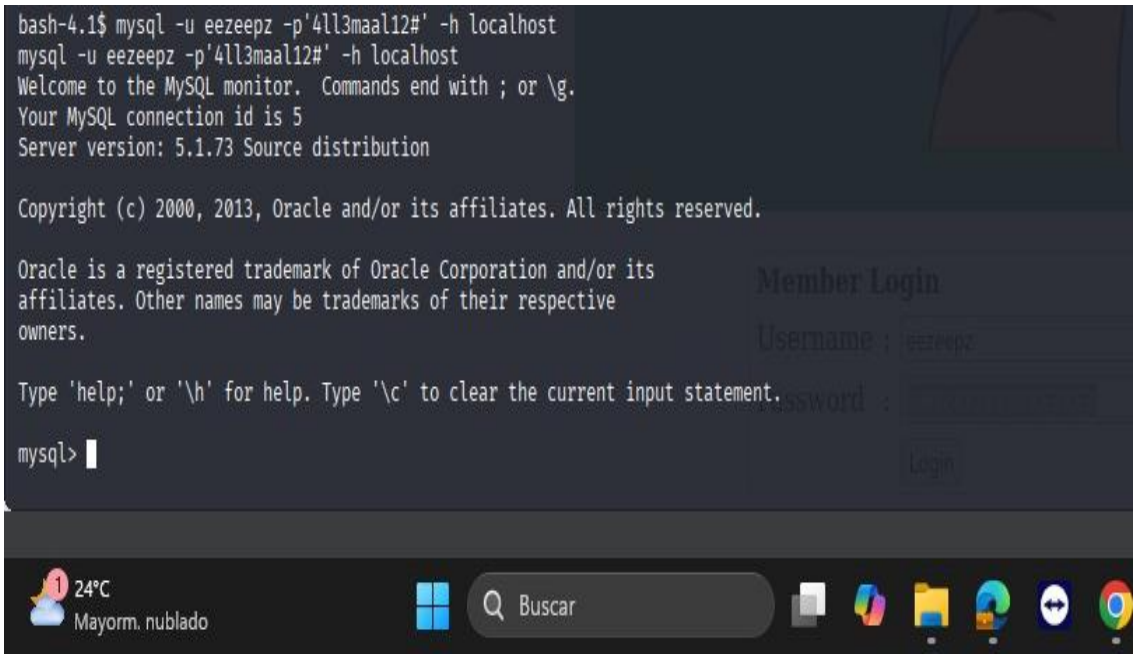


Ilustración 36 Conexión a MySQL

Al ejecutar la instrucción, se abrió el monitor de MySQL, confirmando el acceso directo a la base de datos en localhost. Este acceso confirmó que era posible interactuar con la base de datos **hackmenow**, y permitió realizar insert en la tabla de usuarios (members).

Una vez dentro del motor de base de datos MySQL, se ejecutaron varias consultas para revisar la información almacenada. Primero, se utilizó el comando SELECT * FROM members; para visualizar los registros existentes en la tabla members:

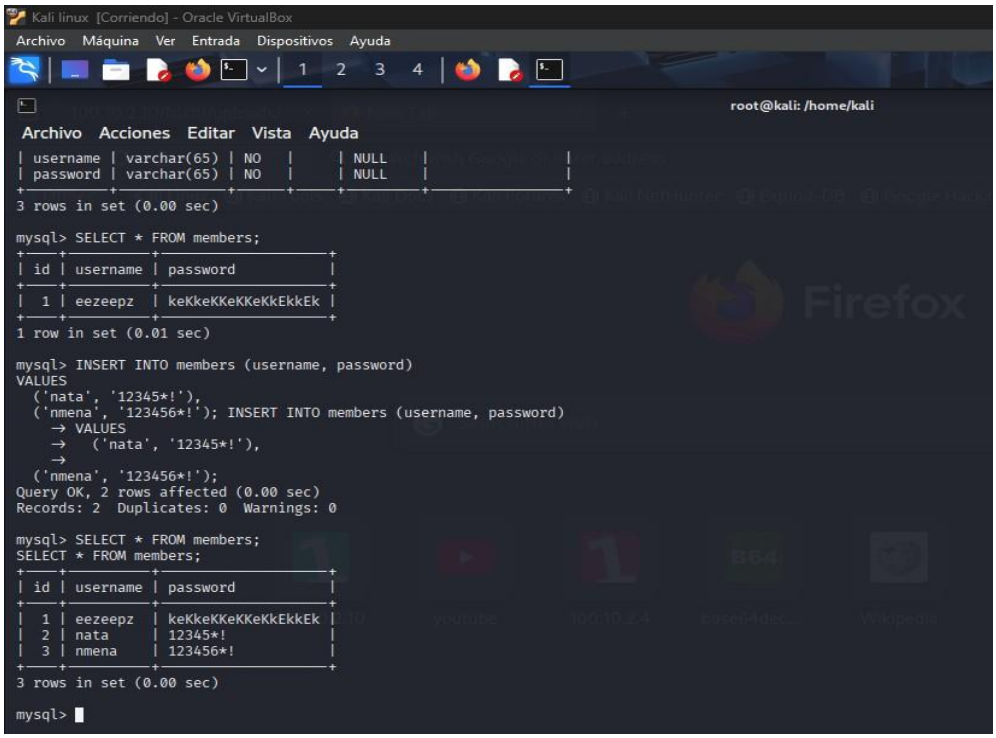


Ilustración 37 Configuraciones en Mysql

Luego, se insertaron dos nuevos registros mediante la instrucción INSERT INTO members (username, password), creando los usuarios **nata y nmena**, ambos con la contraseña 12345*.

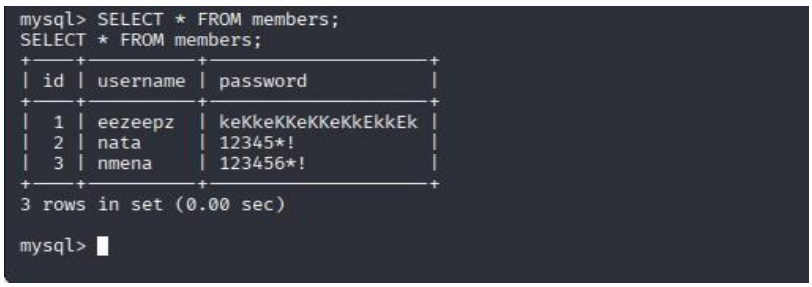


Ilustración 38 Vista de nuevos usuarios

Para verificar que las inserciones se realizaron correctamente, se volvió a ejecutar el comando de consulta y se comprobó que los nuevos usuarios habían sido añadidos exitosamente a la tabla.

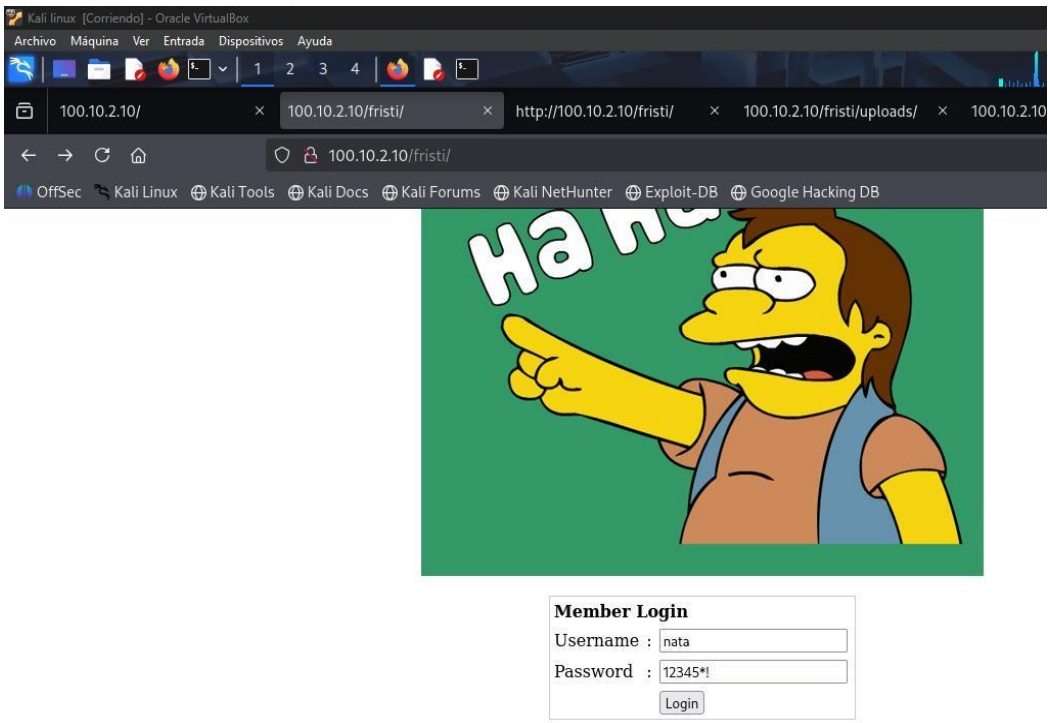
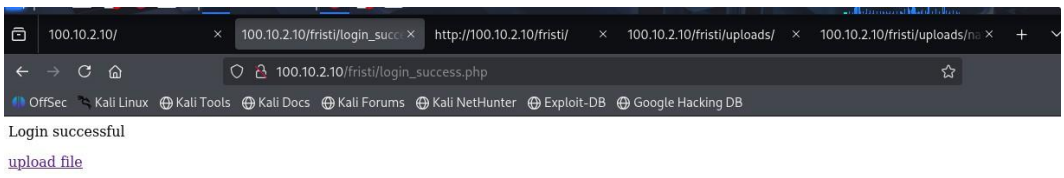


Ilustración 39 Validación de acceso exitoso nata

Después de haber creado los nuevos usuarios en la base de datos, se procedió a comprobar su funcionamiento desde el portal web. Para ello, se accedió nuevamente a la página de inicio de sesión ubicada en la ruta 100.10.2.10/fristi/ y se ingresaron las credenciales del usuario nata con la contraseña 12345*.



Al hacer clic en el botón **Login**, el sistema respondió con el mensaje **Login successful** y mostró el enlace **upload file**, que confirmó que el nuevo usuario había sido registrado correctamente en la base de datos y que su autenticación era válida dentro del portal.

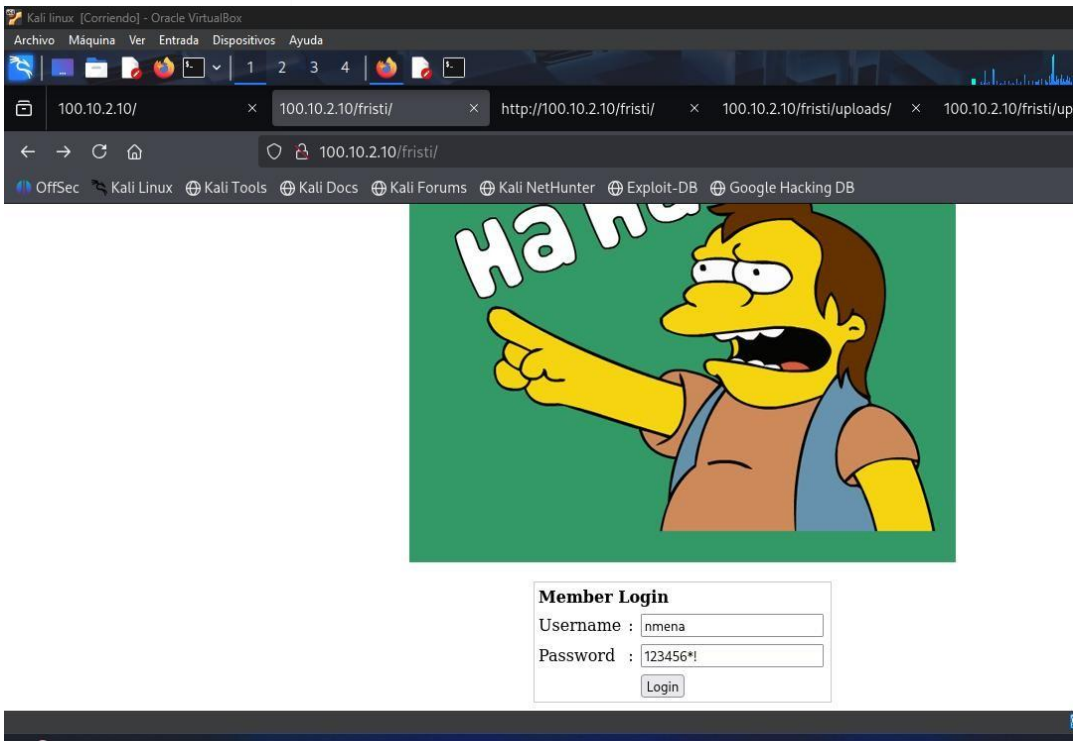
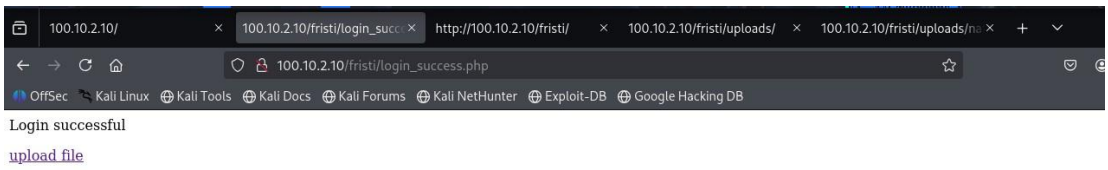


Ilustración 40 Validación de acceso exitoso nmena



El mismo procedimiento se repitió con el segundo usuario creado, **nmena**, utilizando sus respectivas credenciales. Al realizar el inicio de sesión, el sistema mostró nuevamente el mensaje Login successful, confirmando el acceso sin errores.

De esta manera, se verificó que ambos usuarios fueron creados correctamente en la base de datos y que sus credenciales funcionan adecuadamente dentro del portal. Con ello, se da por finalizada esta parte del laboratorio.

2 CAPÍTULO 2: CONFIGURACION DEL DHCP POR MEDIO DE LA MAC A LA MÁQUINA VIRTUAL DE UBUNTU

En este segundo capítulo, el objetivo fue configurar la máquina **Ubuntu** para que solo pudiera recibir una dirección IP por DHCP cuando utilizara una dirección MAC específica.

De esta manera, se buscó garantizar que el acceso a la red estuviera condicionado únicamente al uso de la MAC establecida en la configuración.

Para iniciar el proceso, se encendió la máquina virtual Ubuntu desde VirtualBox, seleccionándola en la lista de sistemas disponibles y haciendo clic en el botón Iniciar. Una vez cargado el sistema operativo, se verificó que la conexión de red estuviera activa y configurada correctamente dentro del entorno virtual.

Luego, se abrió una terminal y se editó el archivo de configuración de **Netplan** en la ruta:

Ilustración 41Archivo ruta Netplan

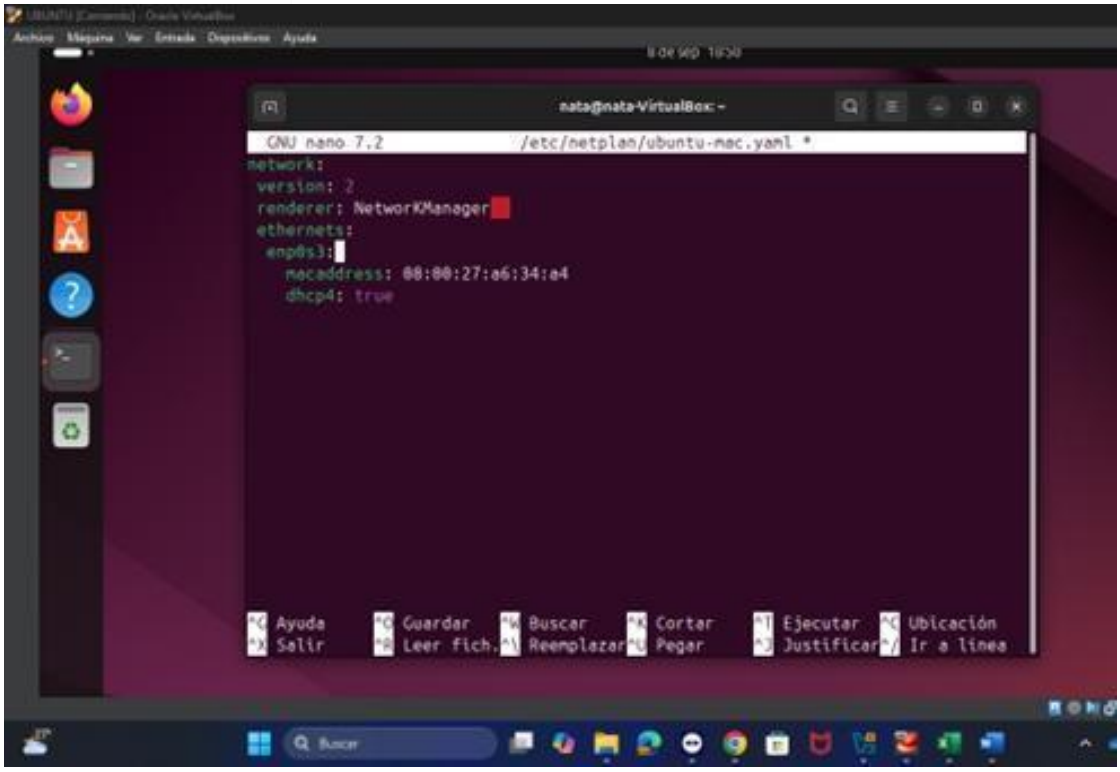


Ilustración 42Edición archivo ruta Netplan

En este archivo se estableció lo siguiente:

Interfaz activa: enp0s3.

Dirección MAC asignada: 08:00:27:a6:34:a4.

Obtención de dirección IP: habilitada mediante dhcp4: true.

Administrador de red: NetworkManager.

El resultado de la configuración puede observarse en la siguiente imagen:

Se procedió a aplicar los cambios realizados en **Netplan** con el siguiente comando:

```
nata@nata-VirtualBox:~$ sudo netplan apply
nata@nata-VirtualBox:~$
```

Ilustración 43Aplicación de la configuración de red con Netplan

Este comando recarga la configuración de red establecida, activando el uso de la dirección MAC configurada para la interfaz enp0s3

Se verificó que la interfaz enp0s3 presentara la dirección MAC configurada, utilizando el comando: ip link show enp0s3

```
nata@nata-VirtualBox:~$ ip link show enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mo
de DEFAULT group default qlen 1000
    link/ether 08:00:27:a6:34:a4 brd ff:ff:ff:ff:ff:ff
nata@nata-VirtualBox:~$
```

Ilustración 44 Comprobación de la dirección MAC en la interfaz enp0s3

Finalmente, se utilizó el comando:

```
nata@nata-VirtualBox:~$ ip addr show enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gr
oup default qlen 1000
    link/ether 08:00:27:a6:34:a4 brd ff:ff:ff:ff:ff:ff
    inet 100.10.2.12/24 brd 100.10.2.255 scope global dynamic noprefixroute enp0
s3
       valid_lft 456sec preferred_lft 456sec
    inet6 fe80::a00:27ff:fea6:34a4/64 scope link
       valid_lft forever preferred_lft forever
nata@nata-VirtualBox:~$
```

Ilustración 45 Asignación de dirección IP por DHCP

Para confirmar que la máquina obtuvo una dirección IP a través del servidor DHCP.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

3 RECOMENDACIONES

Se recomienda documentar cada paso del proceso para evitar confusiones y verificar cuidadosamente las rutas y directorios antes de ejecutar cualquier comando. Asimismo, es fundamental prestar atención a la correcta escritura de los comandos, ya que los errores tipográficos pueden ocasionar fallos en la ejecución. También resulta conveniente investigar y familiarizarse con los comandos básicos de navegación en la terminal, como salir, retroceder o cambiar de directorio,

Universidad Tecnológica del Chocó
Diego Luis Córdoba

4 CONCLUSIÓN

Se cumplieron los objetivos propuestos, ya que los cuatro capítulos del laboratorio pudieron ser desarrollados satisfactoriamente. Durante el proceso se comprendió cómo identificar vulnerabilidades en sistemas web y explotarlas de manera controlada.

El ejercicio resultó útil para comprender que en los sistemas web es fundamental ocultar o proteger archivos y elementos sensibles, ya que, de no hacerlo, estos pueden ser aprovechados por un atacante para obtener credenciales o ejecutar accesos indebidos.

Asimismo, se fortalecieron los conocimientos prácticos sobre el uso de comandos básicos y avanzados, tales como los empleados en la herramienta nc netcat para establecer conexiones de red.

Universidad Tecnológica del Chocó
Diego Luis Córdoba

5 BIBLIOGRAFÍA

IONOS, E. e. (11 de 2023 de Agosto). *ionos.Comando de Linux wc*. Obtenido de ionos.com: https://www.ionos.com/esus/digitalguide/servidores/configuracion/comando-de-linux-wc/