LABORATORIO #4

DANIEL SAMIR RODRÍGUEZ PALACIOS

Estudiantes, IX semestre

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFORMÁTICA

SEGURIDAD Y AUDITORIA DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

LABORAT0ORIO #4

DANIEL SAMIR RODRÍGUEZ PALACIOS

Estudiantes, IX semestre

RAFEL SANDOVAL MORALES

Docente de asignatura

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFORMÁTICA

SEGURIDAD Y AUDITORIA DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

TABLA DE CONTENIDO

LISTA DE ILUSTRACIONES

Informe detallado de despliegue y explotación de satena.exe

El hallazgo de un portal de administración (de la página fristile) nos llevó a la fase de explotación. Primero, preparamos un reverse shell para obtener control del servidor. Luego de conseguir una terminal remota, exploramos el sistema de archivos del servidor para encontrar información sensible. El punto de inflexión fue la obtención de las credenciales de la base de datos a través de un archivo de configuración, lo que nos permitió acceder a la base de datos MySQL. Finalmente, no solo pudimos extraer datos de la tabla members sino también insertar nuevos usuarios, demostrando el control total sobre la información del sitio web.

Objetivo y contexto

El objetivo principal de este proceso de hacking ético es demostrar la vulnerabilidad de una aplicación web en un entorno de laboratorio controlado. A través de una serie de pasos, se busca identificar y explotar las debilidades del sistema para obtener acceso no autorizado y control sobre un servidor y su base de datos.

El contexto es un escenario de prueba realista, donde se utiliza un conjunto de herramientas de seguridad (VirtualBox, Kali Linux, Netcat, Dirb) para simular un ataque.

Nueva dirección Mac de Fristileaks 1.

Aquí en este apartado lo que hicimos fue cambiar la dirección Mac que traía por defecto al momento de montar la ova, ya que cuando le damos en red NAT, no nos permitía adquirir dhcp para esta máquina entonces lo que hicimos fue cambiar la dirección Mac para que ahora sí pudiera adquirir dhcp con la dirección de nosotros.

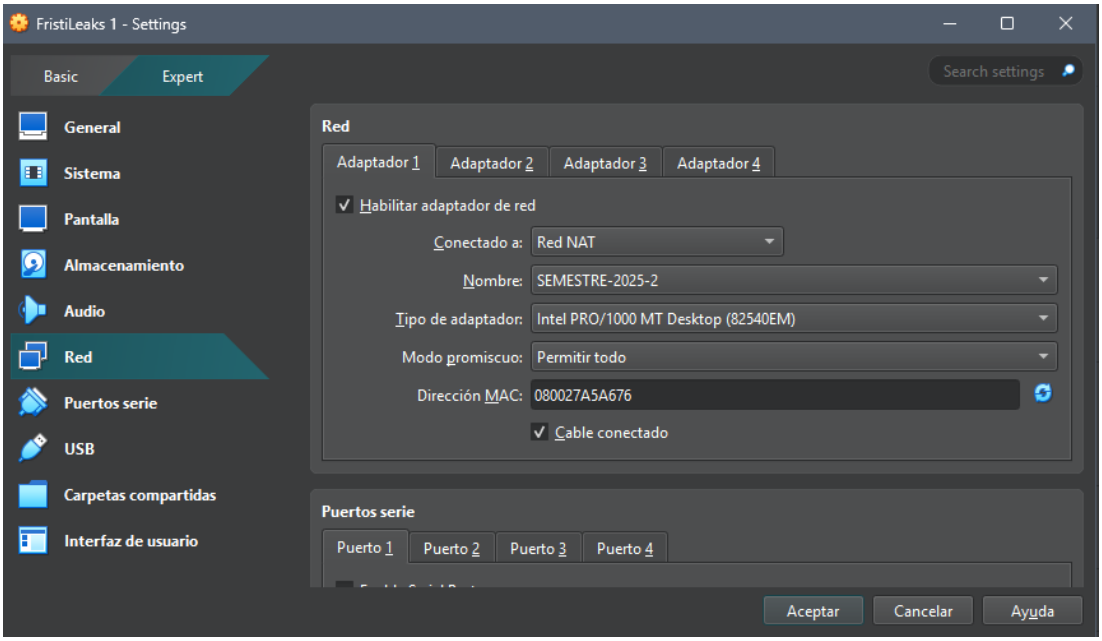


Ilustración 1 Nueva dirección Mac de Fristileaks 1.

Análisis de la pagina

El comando que utilizamos para escanear la página y ver sus archivos o su contenido fue el siguiente, Cómo nos dimos cuenta que esa era la dirección IP porque al insertarle una Mac diferente esa se conectaba a nuestro rango de red que tenemos disponible Y entonces notaba 210.210.200.12

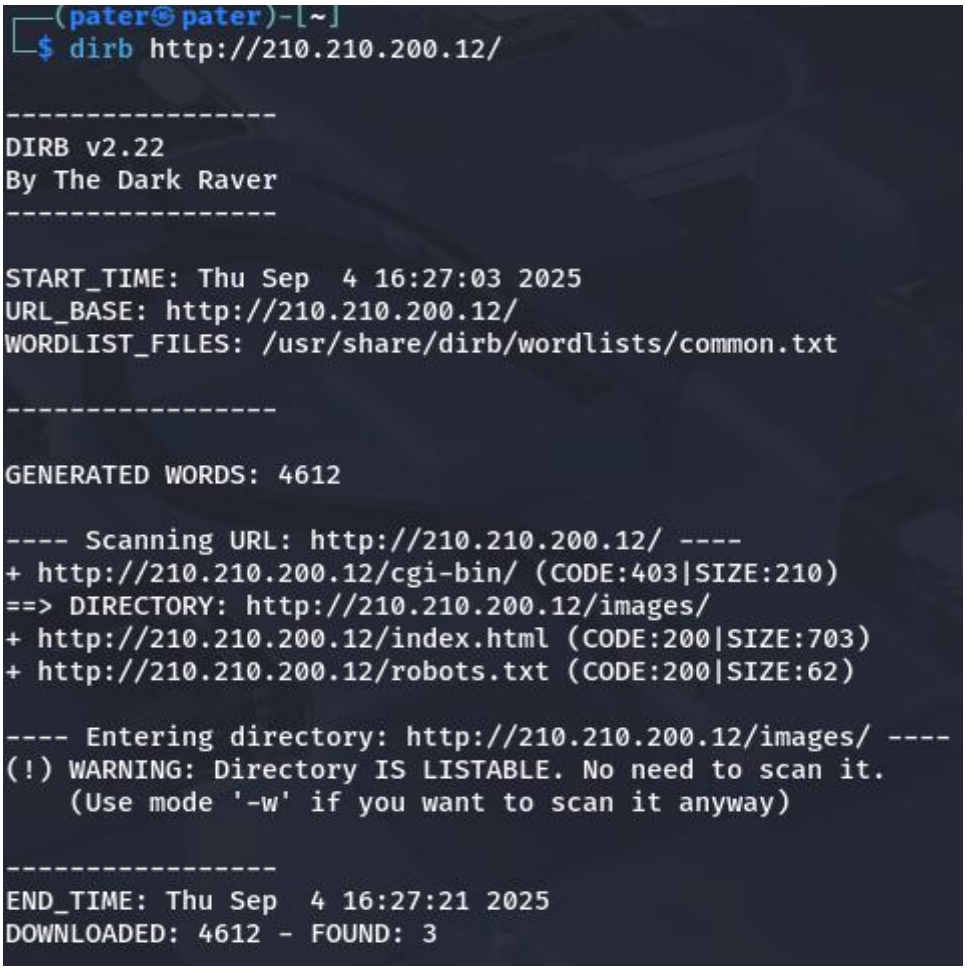


Ilustración 2 Análisis de la pagina

Índex de la página fristileks

Con la dirección IP que ya no sabíamos esa misma ipes la utilizamos para ingresar a la página y nos arrojó este indes

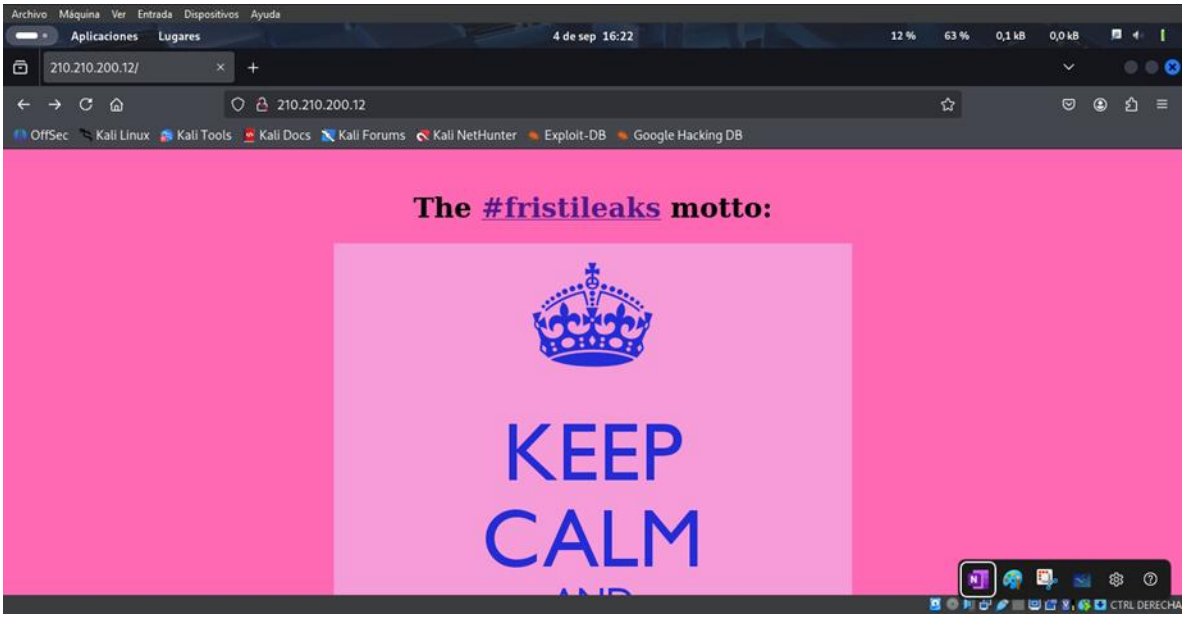


Ilustración 3 Índex de la página fristileks

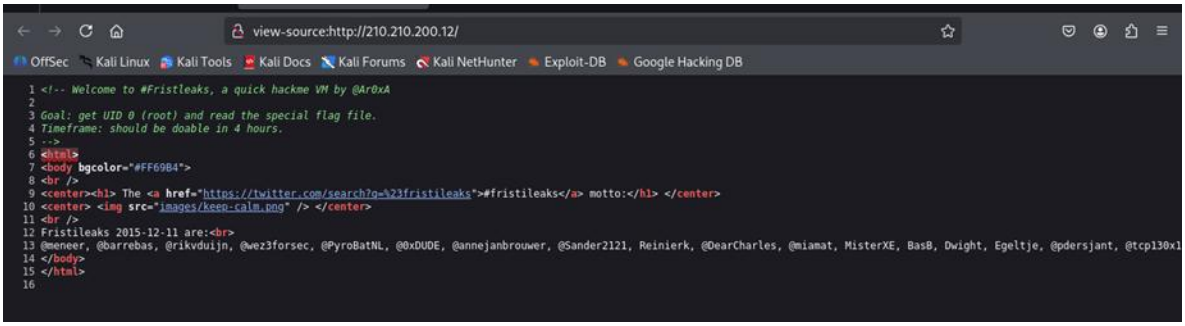


Ilustración 4 código fuente

Luego nos dirigimos a ver el código fuente donde encontramos ciertas cosas en la página que nos sirvieron para continuar con el análisis y la vulnerabilidad de la página freestyle

Lista de los archivos de firsti

Aquí lo que hicimos fue listar la ruta de la página para que nos arrojara esos datos que vemos en pantalla los cuales nos iban a servir más adelante para continuar con la vulnerabilidad a la página

La idea es utilizar una herramienta de ataque como Dirb o Dirbuster para probar cada uno de los nombres de estas listas de palabras contra la página web de Fristileaks, con el fin de descubrir directorios o archivos ocultos que no están enlazados directamente desde la página principal

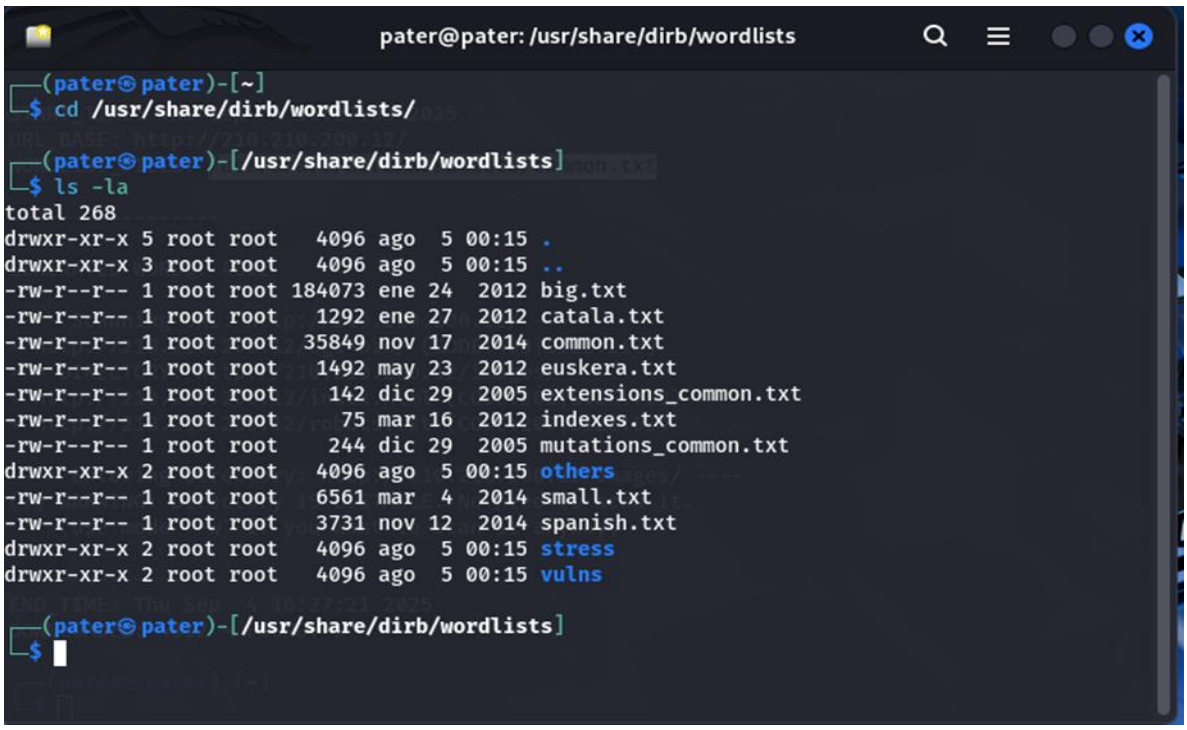


Ilustración 5 Lista de los archivos de firsti

Herramienta Dirb

La imagen muestra la ejecución de la herramienta Dirb para realizar un escaneo de directorios en el servidor web

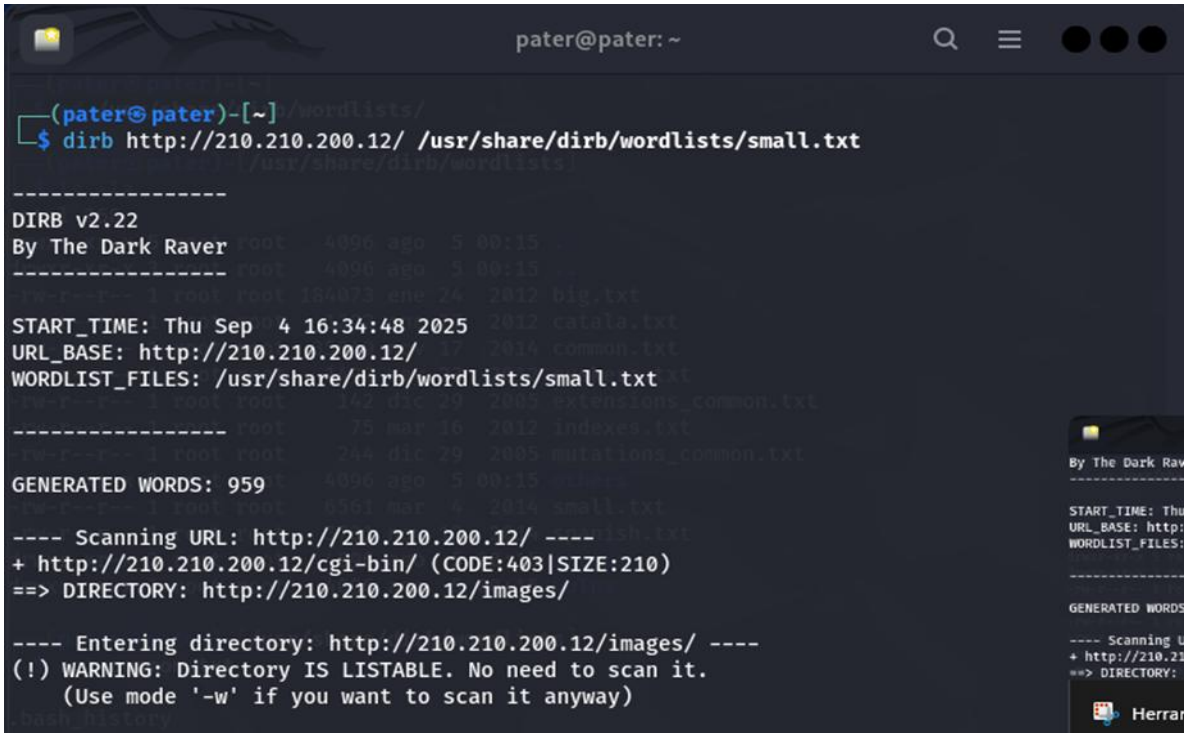


Ilustración 6 herramienta Dirb

Esta imagen muestra un paso crucial en la fase de reconocimiento de un sitio web

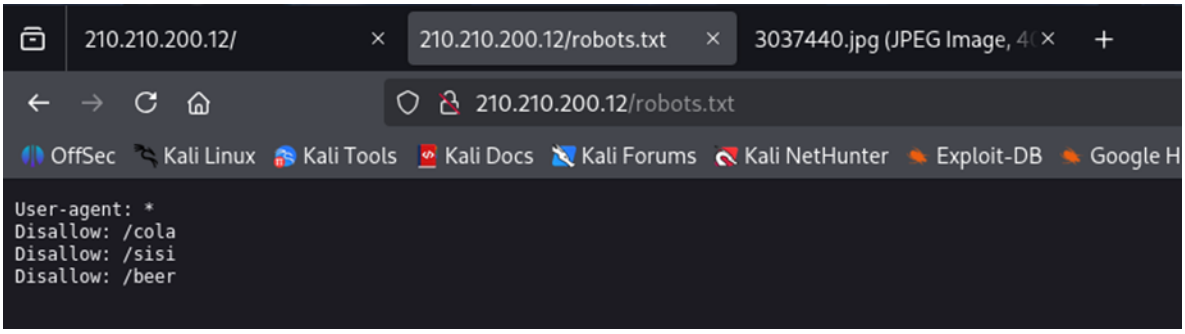


Ilustración 7 robost.txt

Portal de administración

Abrí una nueva pestaña en mi navegador y, basándome en los nombres que encontré en los pasos anteriores, navegué directamente a la dirección http://210.200.200.12/fristileaks/

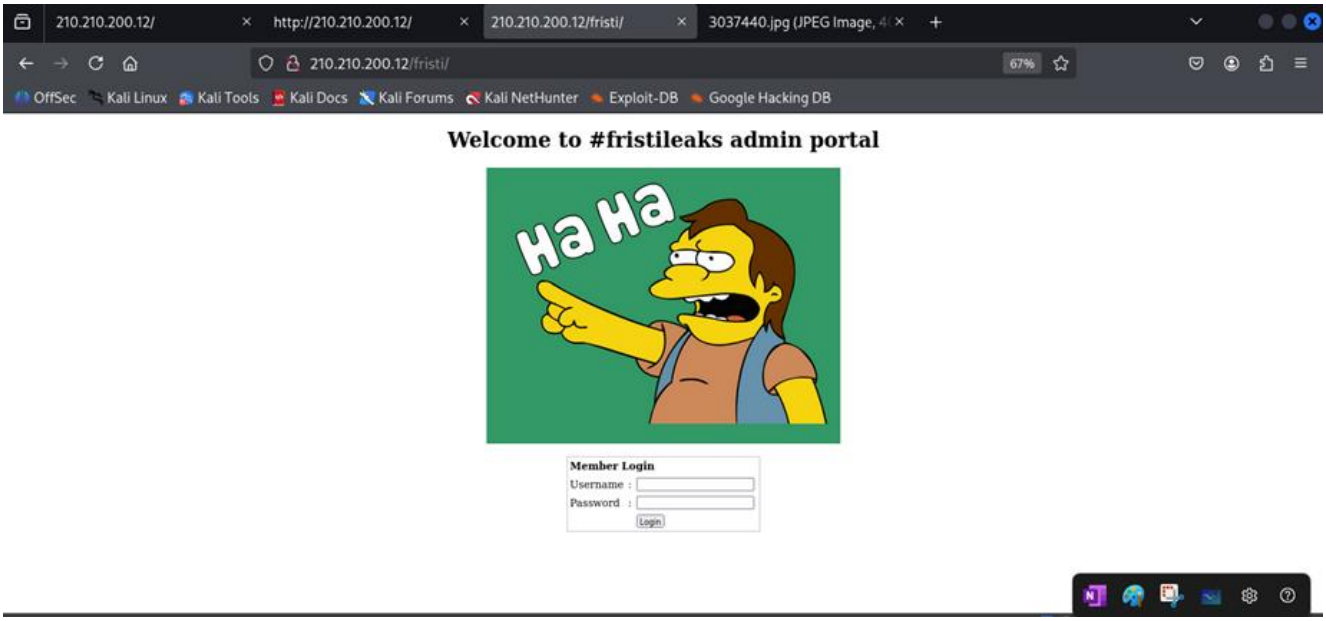


Ilustración 8 Portal de administración

Formato Base64

Esta imagen muestra un paso en el proceso de descifrado, donde se está utilizando una herramienta en línea para decodificar datos en formato Base64

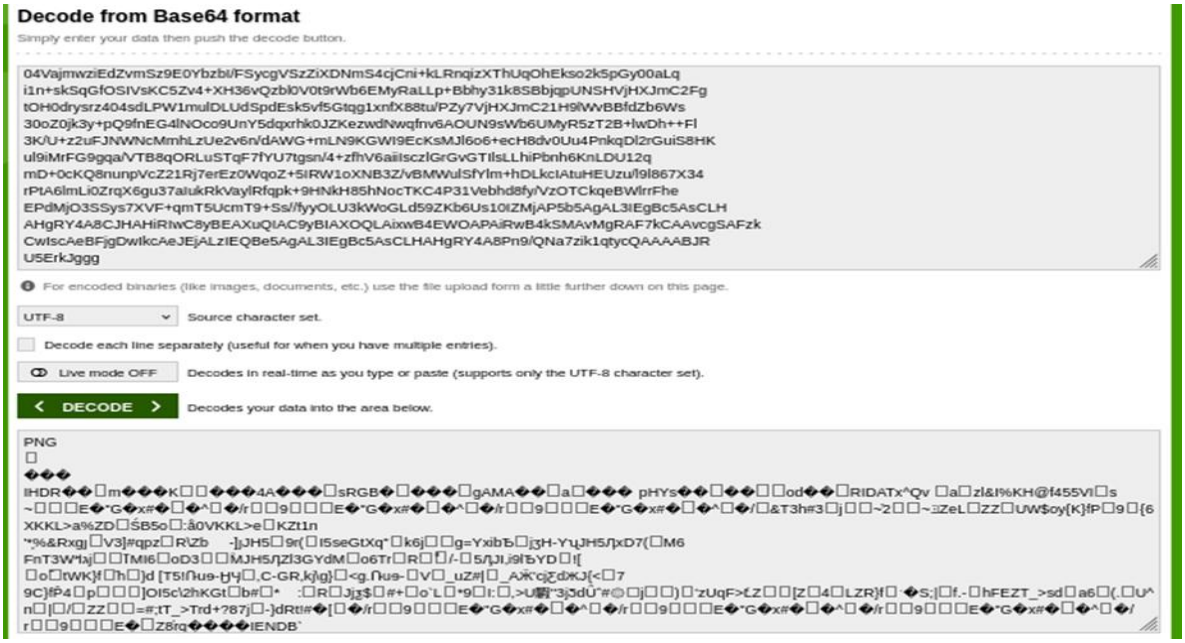


Ilustración 9 Formato Base64

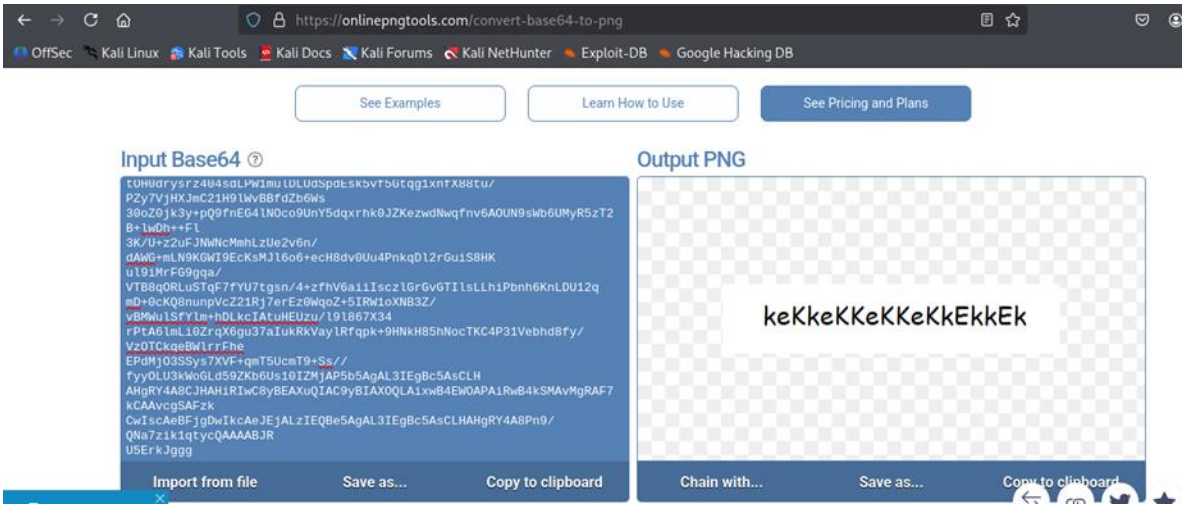


Ilustración 10 descripción

Preparación de un webshell

la preparación de un webshell de tipo reverse shell. Después de encontrar una vulnerabilidad en el sitio, el siguiente paso es preparar una herramienta para explotarla y obtener el control del servidor.

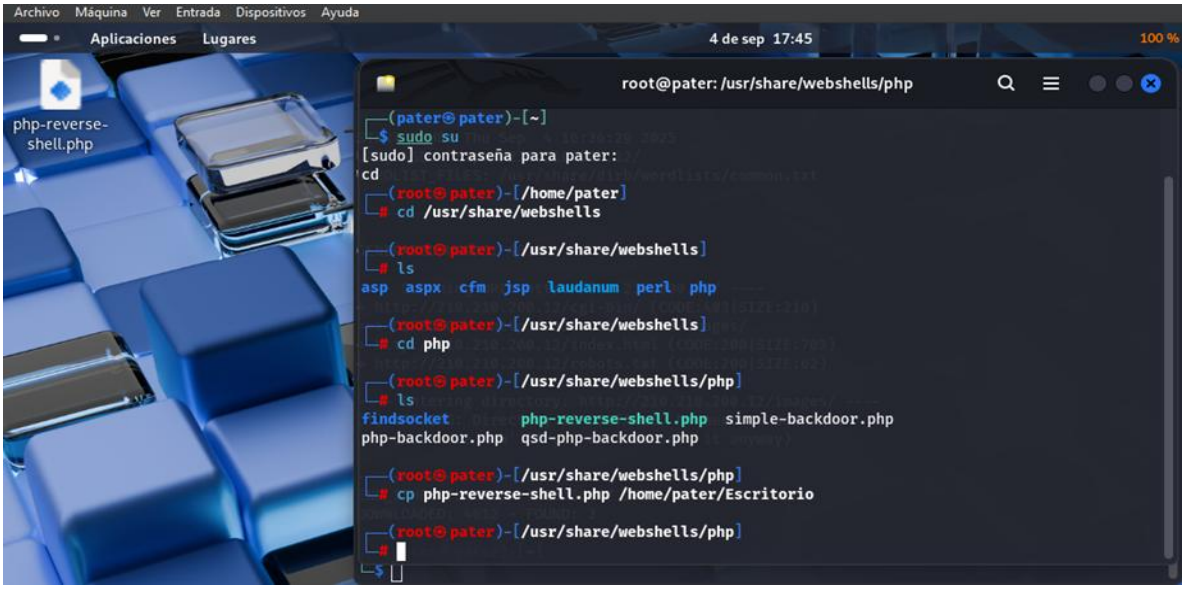


Ilustración 11 Preparación de un webshell

Aquí, me estoy asegurando de que el archivo pueda pasar por cualquier filtro de subida que el servidor web pueda tener, Pero antes se estaba configurando la dirección IP que trae por defecto ese php para que quedara con la dirección IP de nuestra máquina la cual es Kali Linux la atacante

Ilustración 12 configurando la dirección IP

Configuración del Nano Win.php.png

Localicé las líneas marcadas con // CHANGE THIS. Se referían a dos variables clave:
$ip: Cambié el valor de la IP por la dirección de mi máquina, que en este caso es 210.210.200.4. Esta es la dirección a la que el servidor de la víctima intentará conectarse.
$port: Dejé el valor predeterminado 1234. Este es el número de puerto que configuraré en mi máquina para "escuchar" la conexión entrante del reverse shell.

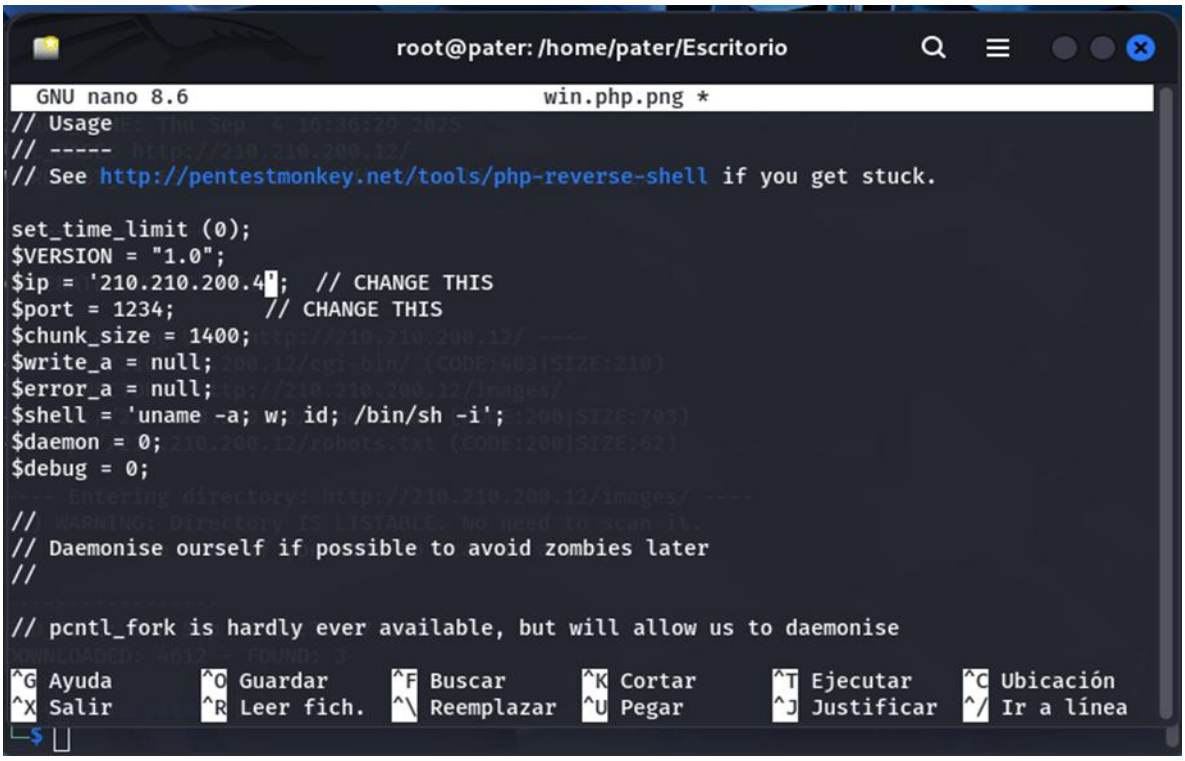
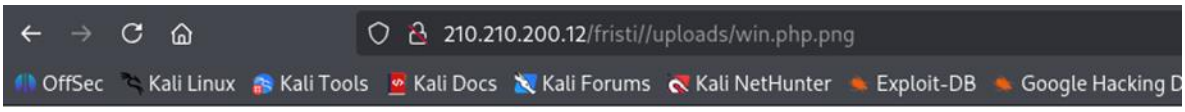


Ilustración 13 Configuración del Nano Win.php.png



WARNING: Failed to daemonise. This is quite common and not fatal. Network is unreachable (101)

Este problema que me aparecía aquí, es porque había puesto mi dirección ip de mi Kali Linux mal

Netcat modo de escucha

Muestra que el reverse shell que preparé y subí al servidor fue ejecutado con éxito, dándome control total sobre la máquina de la víctima.

Antes de intentar ejecutar el webshell en el servidor, en la terminal ejecuté el comando nc -lvp 1234.

nc: Es el comando para Netcat, una herramienta muy versátil que utilicé como "oyente".

-l: Le dije a Netcat que estuviera en modo de escucha (listen).

-v: Le pedí que me diera información detallada (verbose).

-p 1234: Le indiqué que escuchara en el puerto 1234, el mismo que configuré en mi script del reverse shell.

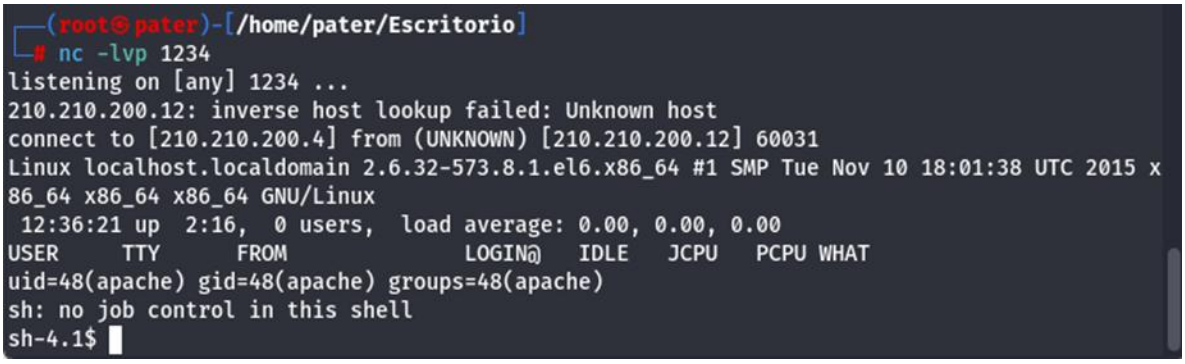


Ilustración 14 Netcat modo de escucha

Pasos para crear los dos usuarios en la base de daros de fristileas

El símbolo del sistema **sh-4.1$** me indica que ya estoy dentro de la máquina del servidor de Fristileaks. Lo primero que hice fue ejecutar un comando básico de exploración: ls -la.

ls: Es el comando estándar para listar el contenido de un directorio.

-l: Muestra la lista en formato largo, lo que me da detalles como permisos, propietario, tamaño y fecha.

-a: Muestra todos los archivos, incluyendo los que están ocultos (los que comienzan con un punto).

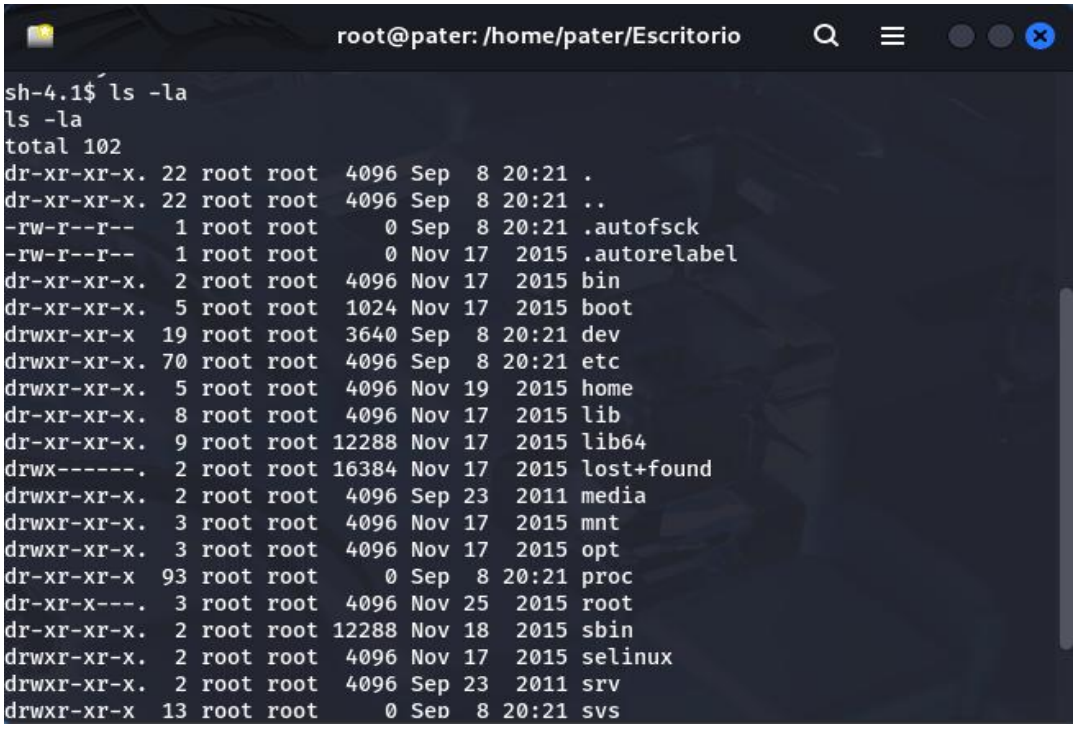


Ilustración 15 símbolo del sistema sh-4.1$

Navegación en los archivos de fristi

Con mi terminal remota **(sh-4.1$),** comencé a moverme por el sistema de archivos usando el comando cd (change directory):

Exploración inicial: Primero, navegué a la carpeta **/var (cd var).** Este es un directorio estándar de Linux para archivos variables del sistema, incluyendo los de los servidores web.

Encontrando la raíz web: Luego, me moví a **/var/www (cd www),** que es una ubicación muy común para los sitios web. Intenté entrar en la carpeta **HTML (cd HTML),** pero recibí un error porque el nombre del directorio era en minúsculas. Corregí el error y entré a **/var/www/html (cd html)**. Esto me confirmó que estaba en el directorio principal del servidor web.

Localizando el sitio específico: Finalmente, sabiendo que el sitio se llamaba "Fristileaks", probé a moverme al directorio **fristi (cd fristi).** El comando fue exitoso, lo que significa que encontré la carpeta que contiene todos los archivos de la página web.

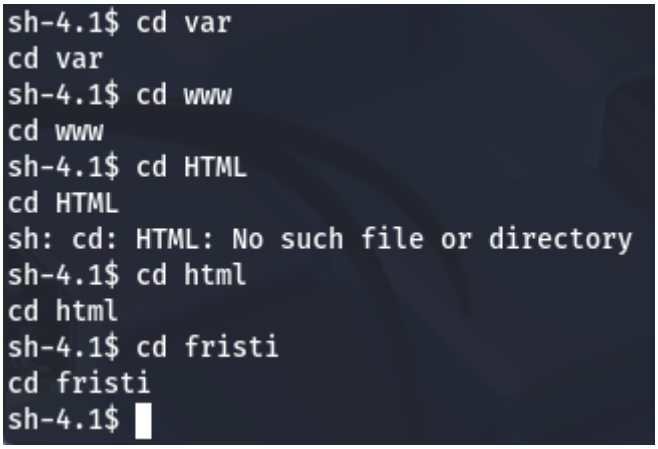


Ilustración 16 mi terminal remota

Revisión de Archivo de Configuración de Login

Utilicé el comando cat checklogin.php para ver el contenido del archivo checklogin.php, que encontré en la carpeta del sitio web.

Credenciales de la base de datos: El script contenía las credenciales para la conexión a la base de datos:

$username: "eezeepz"

$password: "4ll3maal12#"

$db_name: "hackmenow"

```
sh-4.1$ cat checklogin.php
cat 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);

// Mysql_num_row is counting table row
$count=mysql_num_rows($result);

// If result matched $myusername and $mypassword, table row must be 1 row
```

Ilustración 17 Configuración de Login

Obtención de una Terminal Interactiva Mejorada

Aunque ya tenía acceso al sistema a través del reverse shell, el shell inicial (sh-4.1$) era muy básico y carecía de funcionalidades importantes como el historial de comandos, la autocompletación con Tab o la capacidad de manejar Ctrl+C. Para realizar un trabajo más eficiente, necesitaba una terminal más robusta.

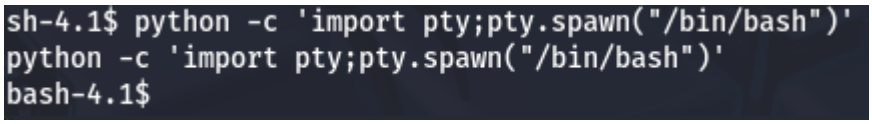


Ilustración 18 Terminal Interactiva Mejorada

Acceso a la Base de Datos con Credenciales Robadas

Después de obtener las credenciales de la base de datos del archivo checklogin.php, ahora estoy usándolas para acceder directamente a la base de datos de la página.

Para lograrlo, ejecuté el comando mysql -u eezeepz -p.

mysql: Es la herramienta de línea de comandos para interactuar con la base de datos MySQL.

-u eezeepz: Le dije a la herramienta que quería conectarme como el usuario eezeepz.

-p: Le indiqué que se me pidiera una contraseña.

Cuando el terminal me pidió la contraseña, ingresé la que había encontrado en el archivo PHP: **4ll3maal12#.**

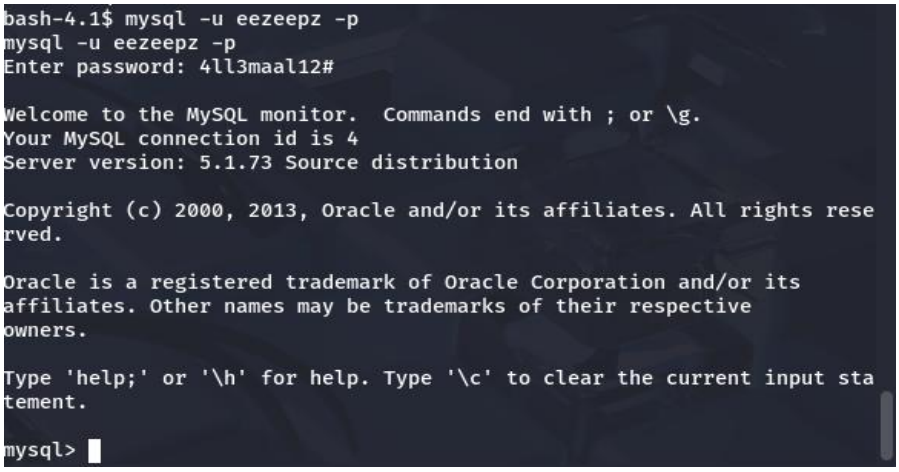


Ilustración 19 Credenciales Robadas

Enumeración y Selección de la Base de Datos

Comandos ejecutados dentro del monitor de MySQL, con el objetivo de identificar y seleccionar la base de datos correcta para la exfiltración de datos.

Listado de bases de datos: Primero, ejecuté el comando SHOW DATABASES;. Este comando me mostró una lista de todas las bases de datos a las que el usuario eezeepz tenía acceso. La lista reveló dos bases de datos: information_schema (una base de datos del sistema) y hackmenow. Este último nombre coincidía con el que encontré en el script PHP, lo que confirmó que esta era la base de datos que contenía la información del sitio web.

Selección de la base de datos: Luego, utilicé el comando USE hackmenow; para seleccionar esa base de datos. El mensaje "Database changed" confirmó que ahora estaba trabajando dentro de la base de datos hackmenow.

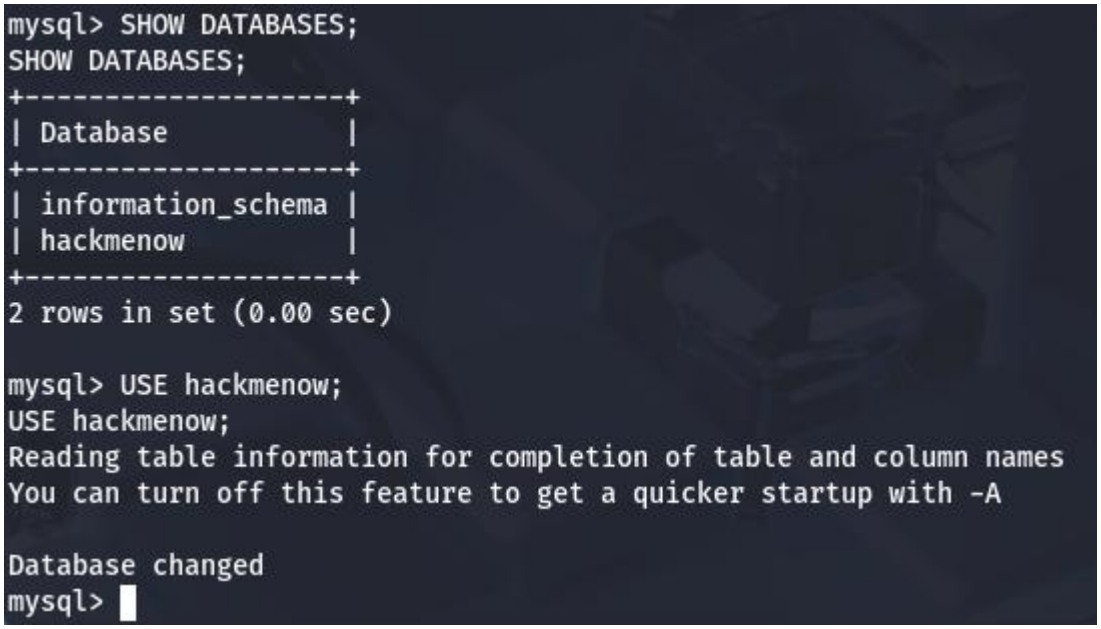


Ilustración 20 Enumeración y Selección de la Base de Datos

Búsqueda de Tablas de Usuarios

Ya dentro de la base de datos hackmenow, mi siguiente paso fue encontrar la tabla que contenía la información de los usuarios. Para ello, ejecuté el comando SHOW TABLES;.

La base de datos me devolvió una única tabla llamada members. Este es el objetivo principal que estaba buscando, ya que su nombre indica que contiene los datos de los miembros del sitio, como nombres de usuario y contraseñas.

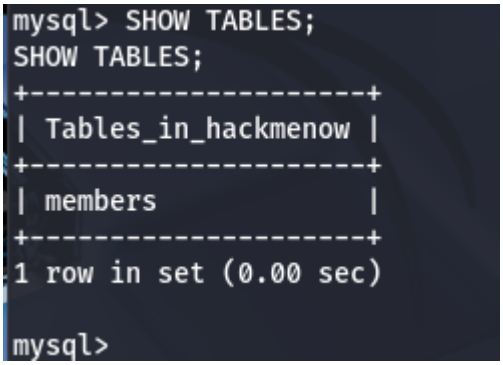


Ilustración 21 Búsqueda de Tablas de Usuarios

Estructura de la Tabla 'members'

Una vez que encontré la tabla members, mi siguiente paso fue entender su estructura para saber dónde se almacenaba la información de los usuarios. Ejecuté el comando DESCRIBE members;.

Este comando me mostró la estructura de la tabla, con sus columnas y tipos de datos:

id: Un número entero que sirve como identificador único.

username: Una cadena de texto (varchar) para los nombres de usuario.

password: Una cadena de texto (varchar) para las contraseñas.

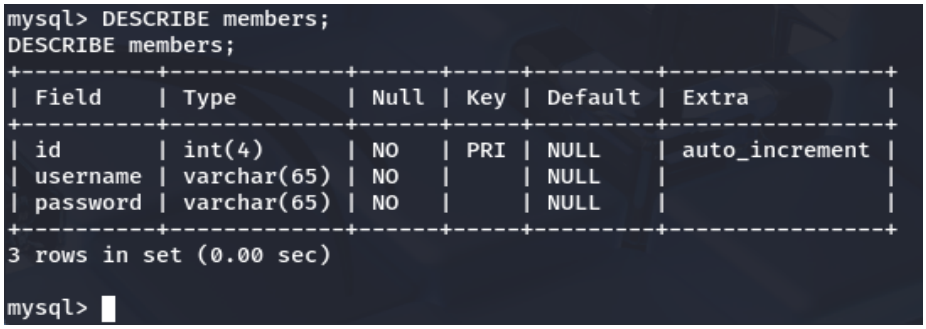


Ilustración 22 Estructura de la Tabla 'members'

Obtención de Credenciales de Usuario

Una vez que entendí la estructura de la tabla, mi objetivo final era extraer la información que contenía. Para ello, ejecuté el comando **SELECT * FROM members;.**

Este comando es una consulta SQL que le dice a la base de datos que seleccione (SELECT) todos (*)los campos de la tabla **members`.**

La terminal me devolvió el contenido de la tabla, que incluía el id, el username y la password. Con esto, obtuve las credenciales de acceso de un usuario:

username: eezeepz

password: keKkeKKeKkeKkEkkEk

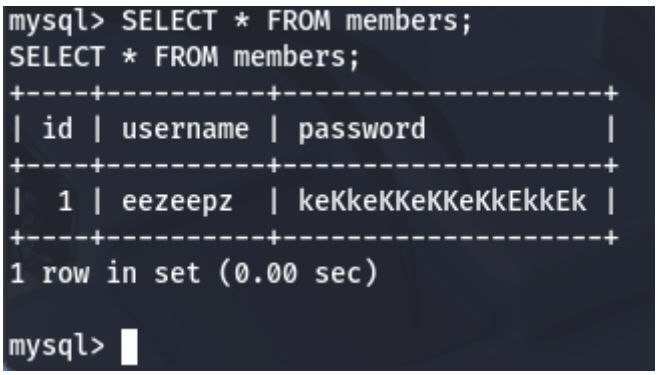


Ilustración 23 Obtención de Credenciales de Usuario

Manipulación de la Base de Datos

Una vez que obtuve las credenciales de un usuario, procedí a manipular la base de datos. Utilicé el comando INSERT INTO para agregar nuevos usuarios a la tabla members.

El objetivo de esta acción no era solo demostrar que podía insertar datos, sino también crear nuevas credenciales de acceso para mí mismo en el sitio.

Primer Usuario: Utilicé el comando INSERT INTO members (username, password) VALUES **('daniel', 'usuario1');** para agregar un usuario con el nombre "daniel" y la contraseña "usuario1".

Segundo Usuario: Luego, agregué un segundo usuario con INSERT INTO members (username, password) VALUES **('samir', 'usuario2');,** con el nombre de usuario "samir" y la contraseña "usuario2".

```
mysql> INSERT INTO members (username, password) VALUES ('daniel', 'usuario
1');
INSERT INTO members (username, password) VALUES ('daniel', 'usuario1');
Query OK, 1 row affected (0.00 sec)

mysql> INSERT INTO members (username, password) VALUES ('samir', 'usuario2
');
INSERT INTO members (username, password) VALUES ('samir', 'usuario2');
Query OK, 1 row affected (0.00 sec)
```

Ambos comandos fueron exitosos, como lo indica el mensaje **"Query OK, 1 row affected".**

Ilustración 24 Manipulación de la Base de Datos

Confirmación de Inserción de Datos

Después de insertar los nuevos usuarios en la base de datos, ejecuté nuevamente el comando SELECT * FROM members; para verificar que la información se había guardado correctamente.

El resultado de la consulta me mostró la tabla completa, que ahora incluye las tres filas:

El usuario original eezeepz.

El usuario que inserté daniel.

El segundo usuario que inserté samir.

Esto demuestra que no solo pude obtener datos de la base de datos, sino que también pude escribir y modificar su contenido.

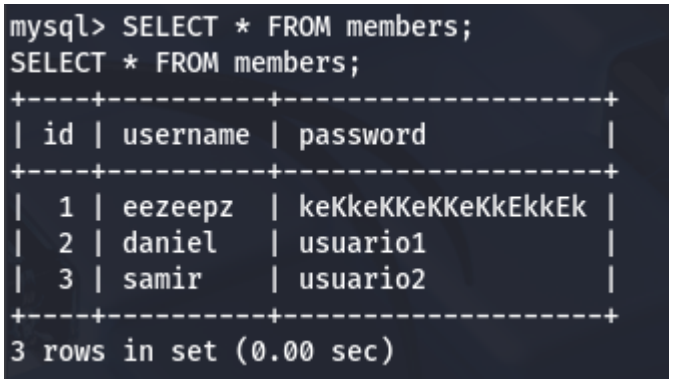


Ilustración 25 Confirmación de Inserción de Datos

Consulta de investigación

Comandos Útiles de Netcat (nc)

El comando Netcat (nc) es una herramienta versátil usada para leer y escribir datos a través de conexiones de red.

-l: (Listen) Pone a Netcat en modo de escucha para esperar una conexión entrante en un puerto específico. Es esencial para crear un "oyente" como se hizo con el reverse shell.

-v: (Verbose) Muestra información detallada sobre la conexión, lo cual es útil para la depuración y para ver el estado de la conexión.

-p <puerto>: (Port) Especifica el puerto de origen o el puerto en el que se va a escuchar.

-z: (Zero-I/O) Entra en modo de escaneo. Solo escanea para ver si un puerto está abierto, sin enviar ningún dato.

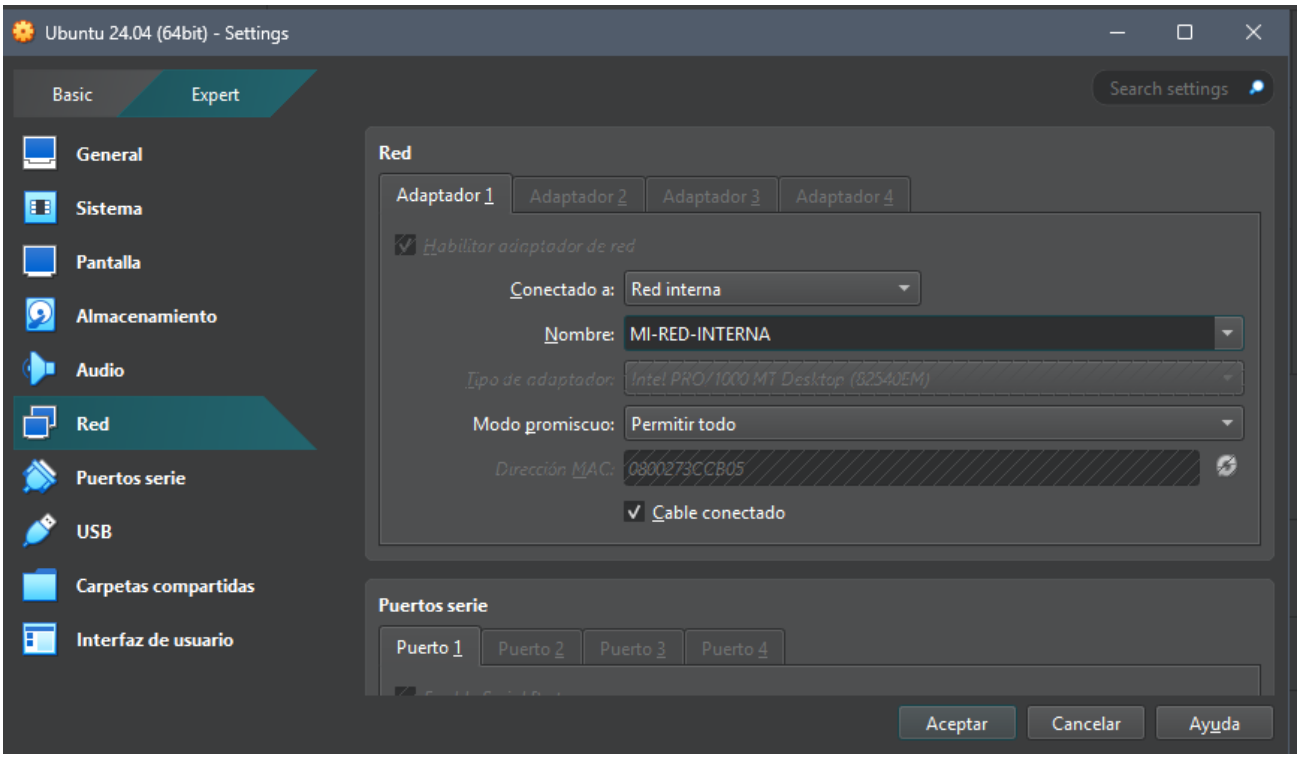
-n: (Numeric) Evita la resolución de DNS, usando solo direcciones IP numéricas. Esto hace que la conexión sea más rápida.

-w <segundos>: (Timeout) Establece un tiempo de espera para las conexiones, lo cual es útil para evitar que se queden atascadas.

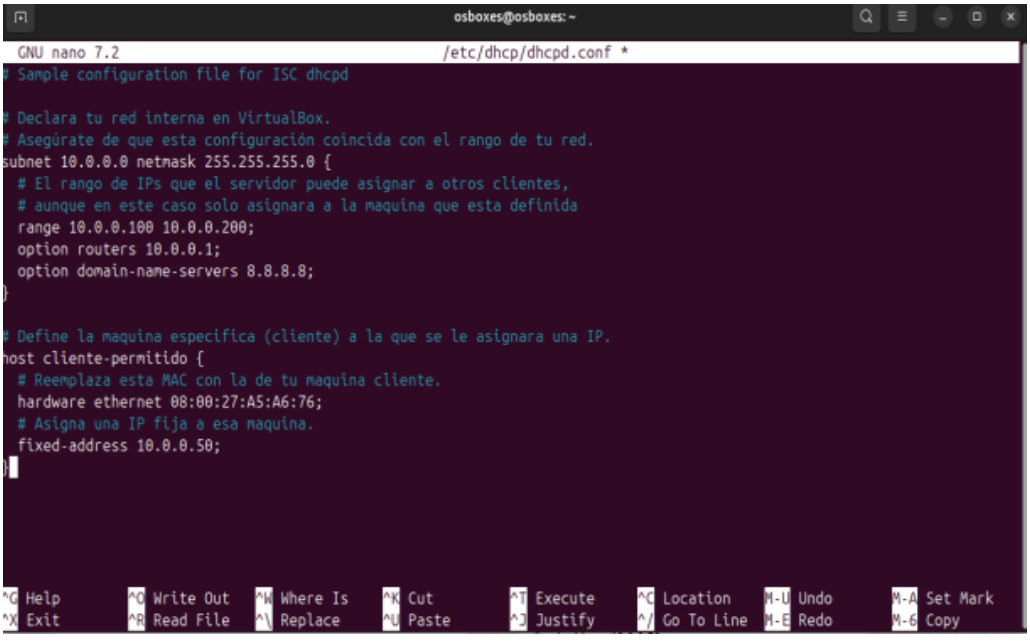
-u: (UDP) Usa el protocolo UDP en lugar del protocolo TCP por defecto.

-e <comando>: (Execute) Ejecuta un programa después de que se establece la conexión. Este comando es clave para obtener un shell remoto.

Cambiar la mac del Ubuntu




```
osboxes@osboxes:~$ sudo nano /etc/dhcp/dhcp.conf
```




osboxes@osboxes:~$ sudo systemctl restart isc-dhcp-server
osboxes@osboxes:~$ sudo systemctl enable isc-dhcp-server
Synchronizing state of isc-dhcp-server.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable isc-dhcp-server
osboxes@osboxes:~$

Dificultades encontradas y soluciones

La principal dificultad del proceso de penetración reside en la fase de reconocimiento y enumeración. Aunque la obtención del reverse shell y la manipulación de la base de datos parecen los pasos más complejos, dependen completamente de encontrar la vulnerabilidad inicial. En un entorno real, los directorios no siempre son tan obvios como /images o /fristileaks, y los archivos de configuración no siempre exponen las credenciales tan fácilmente.

Conclusiones

este ejercicio demostró que una cadena de vulnerabilidades pequeñas puede llevar a un control total del sistema. La falta de protección en los directorios, la exposición de un archivo robots.txt que revelaba directorios sensibles, y la inclusión de credenciales de la base de datos en un archivo de código fuente, actuaron como eslabones débiles. El proceso ilustró que la seguridad de un sistema es tan fuerte como su eslabón más débil, y que una buena defensa requiere atención a cada detalle, desde la configuración de la red hasta el código de la aplicación.Rafel Sandoval Morales

Webgrafía

Ia.

https://chatgpt.com/