PICKLE RICK

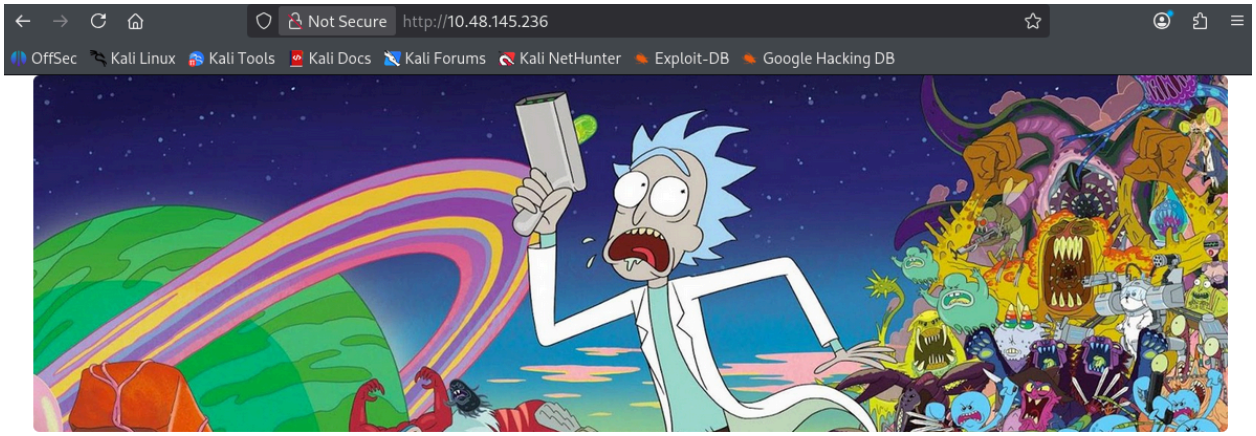
First I started the machine and pinged it using my own machine. Ping was successful.

```
┌──(kali㉿kali)-[~]
└─$ ping 10.48.145.236
PING 10.48.145.236 (10.48.145.236) 56(84) bytes of data.
64 bytes from 10.48.145.236: icmp_seq=1 ttl=62 time=47.6 ms
64 bytes from 10.48.145.236: icmp_seq=2 ttl=62 time=47.7 ms
64 bytes from 10.48.145.236: icmp_seq=3 ttl=62 time=47.0 ms
64 bytes from 10.48.145.236: icmp_seq=4 ttl=62 time=46.9 ms
^C
── 10.48.145.236 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 46.945/47.301/47.725/0.355 ms
```

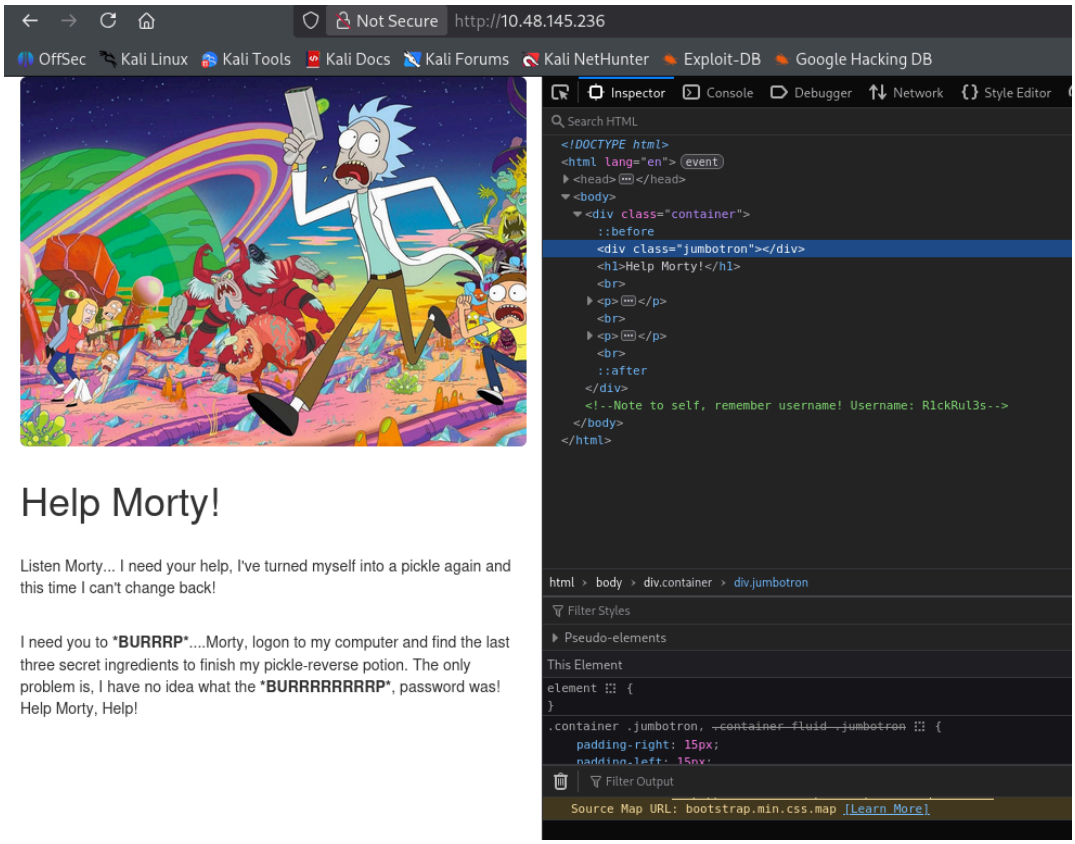
Then ran a nmap scan and found that SSH port 22 and http port 80 were open.

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn -A 10.48.145.236
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-21 08:46 EST
Nmap scan report for 10.48.145.236
Host is up (0.047s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 7a:3f:87:52:d8:70:55:47:df:4a:70:75:3f:44:20:6a (RSA)
|   256 11:7d:15:da:f4:82:5d:4f:7a:f0:16:99:aa:1b:f7:8a (ECDSA)
|_  256 79:9e:9b:4f:70:9e:5d:3d:9b:a2:88:51:d8:b6:43:81 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Rick is sup4r cool
|_http-server-header: Apache/2.4.41 (Ubuntu)
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
Network Distance: 3 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
1   45.91 ms 192.168.128.1
2   ...
3   46.59 ms 10.48.145.236

OS and Service detection performed. Please report any incorrect results at https://nmap.org
/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.68 seconds
```

Then I visited the website. There was nothing much on the website.



Inspected the website and found the Username.



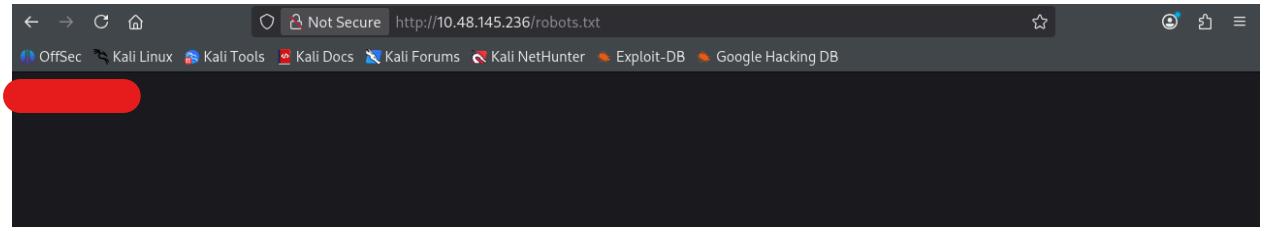
Used ssh but was denied permission because of no public key.

```
┌──(kali㉿kali)-[~]
└─$ ssh R1ckRul3s@10.48.145.236
The authenticity of host '10.48.145.236 (10.48.145.236)' can't be established.
ED25519 key fingerprint is: SHA256:YzAUoqwX8Kdt0nyM6iLEK3S3G2FuLPUb7bxPMnJ7v/k
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.48.145.236' (ED25519) to the list of known hosts.
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
R1ckRul3s@10.48.145.236: Permission denied (publickey).
```

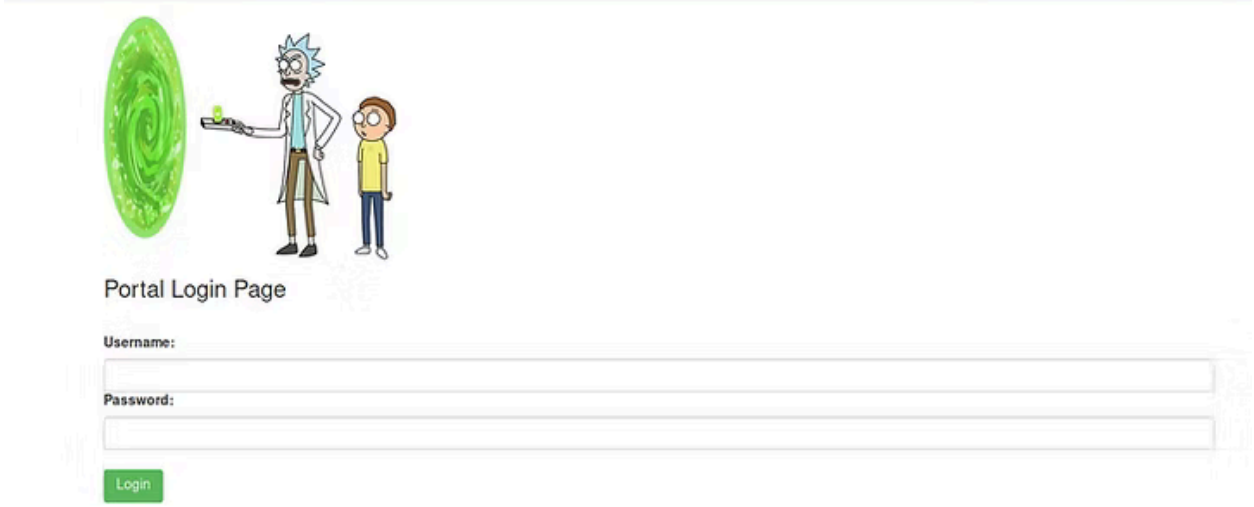
Used gobuster to brute force directory and found login.php, robots.txt

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://10.48.145.236 -w Desktop/gobuster/SecLists/Discovery/Web-Content
/common.txt -t 50 -x php,html,txt
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.48.145.236
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                Desktop/gobuster/SecLists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta.php             (Status: 403) [Size: 278]
/.hta.html            (Status: 403) [Size: 278]
/.hta                 (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htaccess.php        (Status: 403) [Size: 278]
/.hta.txt             (Status: 403) [Size: 278]
/.htaccess.html       (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/.htaccess.txt        (Status: 403) [Size: 278]
/.htpasswd.php        (Status: 403) [Size: 278]
/.htpasswd.html       (Status: 403) [Size: 278]
/.htpasswd.txt        (Status: 403) [Size: 278]
/assets               (Status: 301) [Size: 315] [--> http://10.48.145.236/assets/]
/denied.php           (Status: 302) [Size: 0] [--> /login.php]
/index.html           (Status: 200) [Size: 1062]
/index.html           (Status: 200) [Size: 1062]
/login.php            (Status: 200) [Size: 882]
/portal.php           (Status: 302) [Size: 0] [--> /login.php]
/robots.txt           (Status: 200) [Size: 17]
/robots.txt           (Status: 200) [Size: 17]
/server-status        (Status: 403) [Size: 278]
Progress: 19000 / 19000 (100.00%)
===============================================================
Finished
===============================================================
```

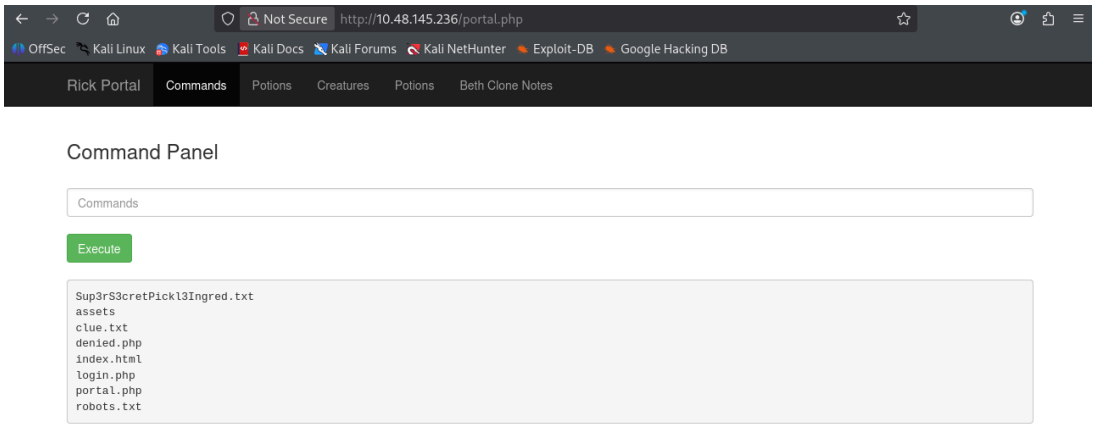
In robots.txt found this interesting text.



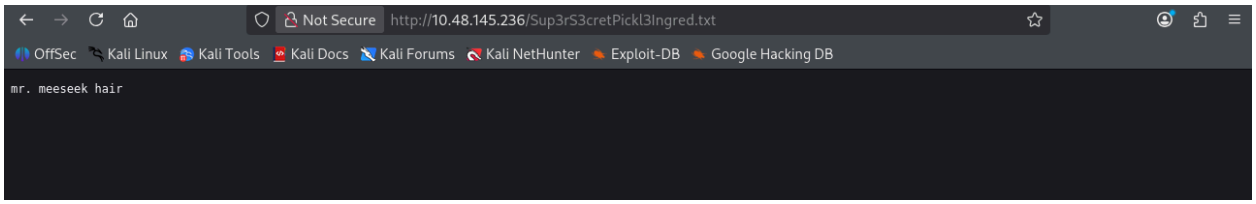
Went to the login page used the username and the text found from robots.txt and it actually worked.



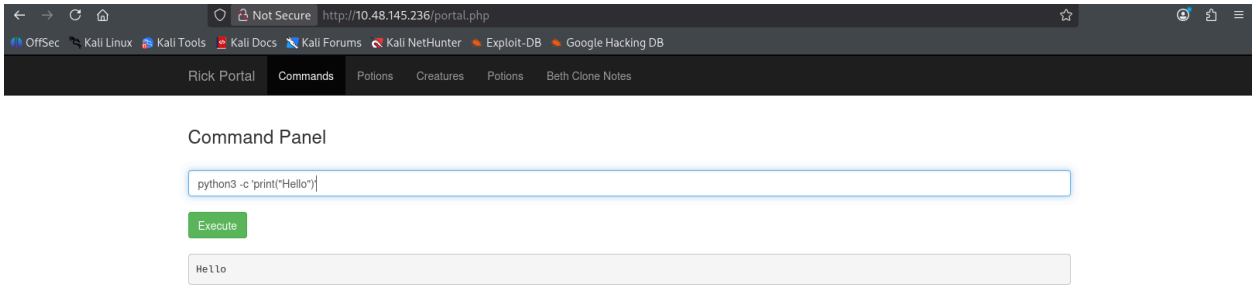
Now we have a command panel that doesn't let us use cat, touch commands. But can use ls ls -la commands.



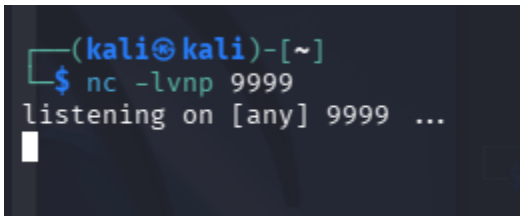
Used Sup3rS3cretPickl3Ingred.txt with the url and found the first ingredient.



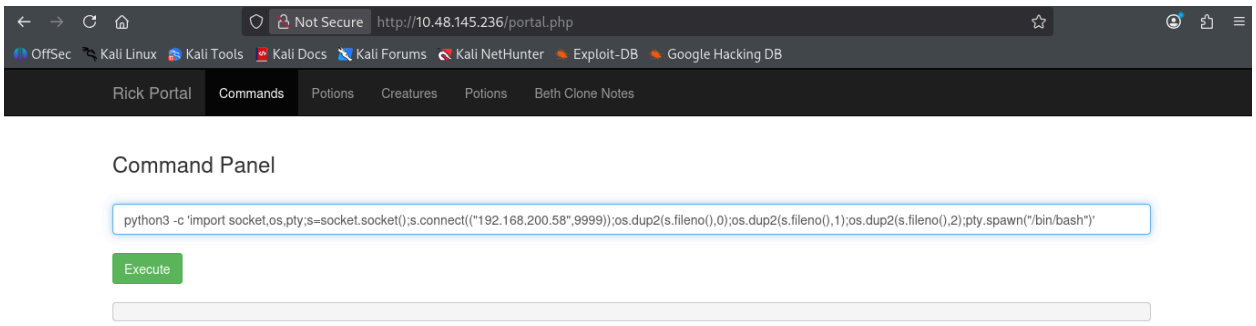
Then nothing was working. And couldn't find anything so checked for the python version. It was python3 .



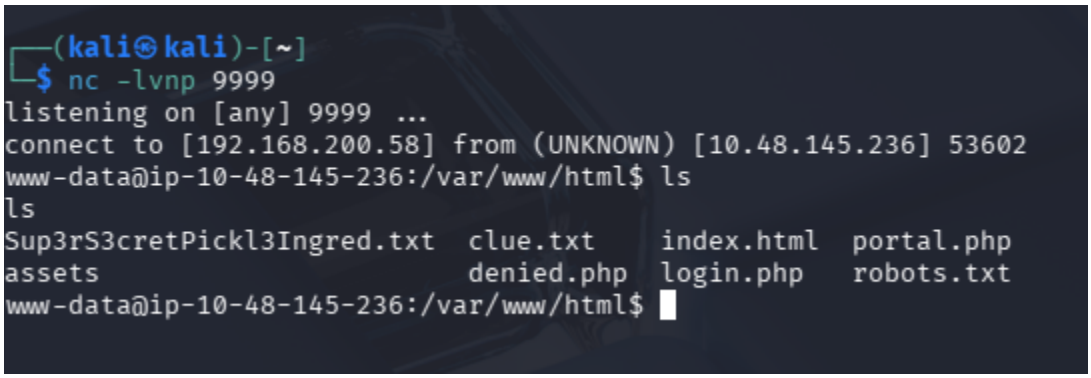
Setup a Netcat listener on kali machine and started it on port 9999



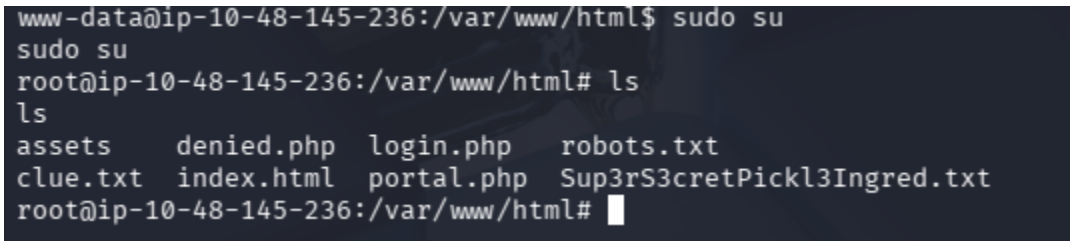
Used oneliner reverse shell code from [Reverse Shell Cheat Sheet | pentestmonkey] with a little modification was able to start a connection.



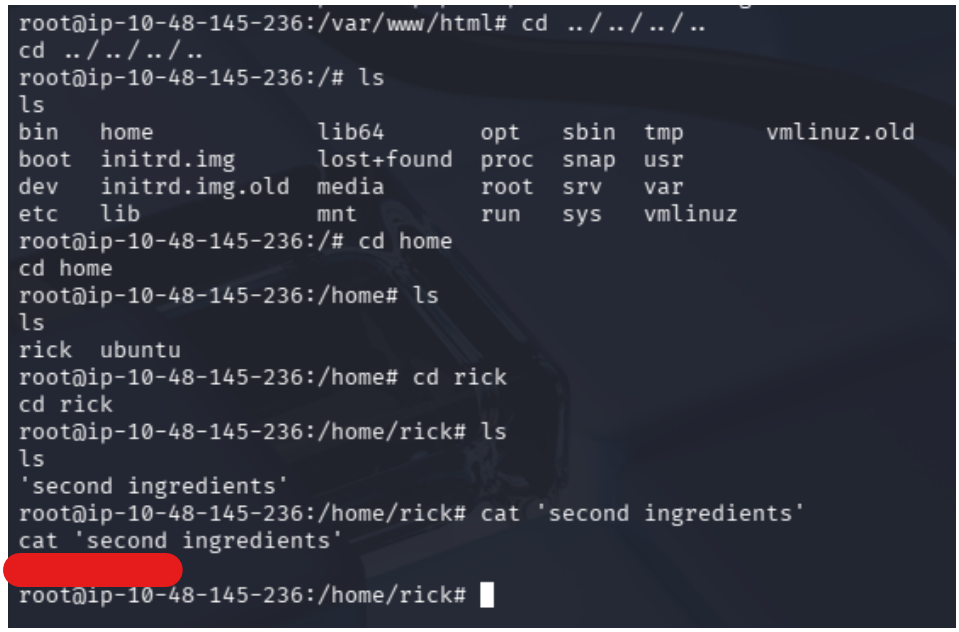
Connection started and got the data.



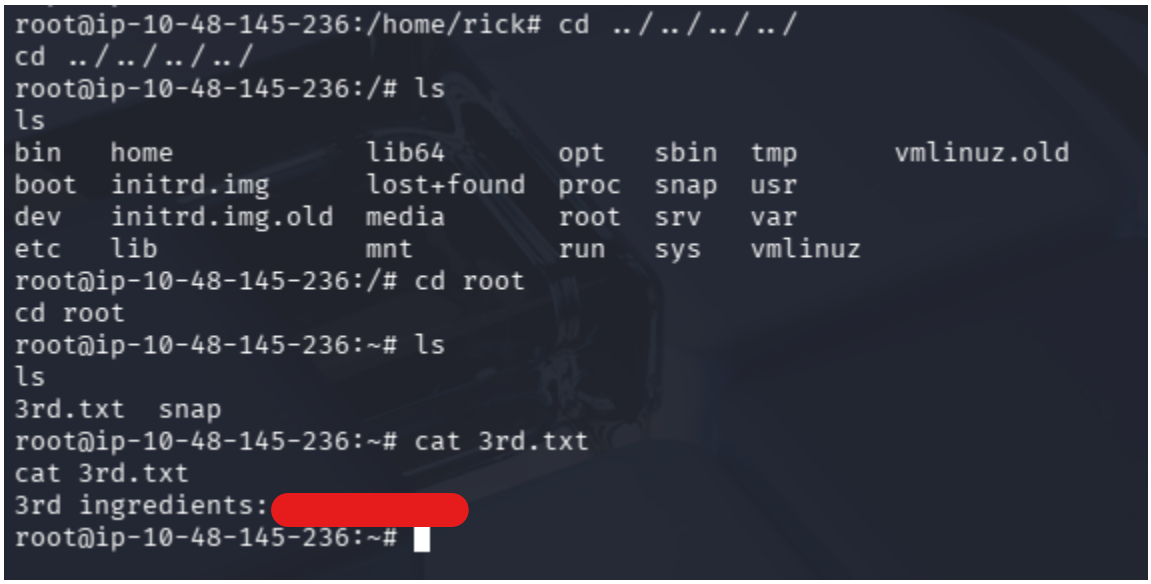
Used sudo su to escalate privilege and it worked without any password what a luck.



Then went back on the directory and searched all one by one and found second ingredient on home/rick/'second ingredients'



Then went back on the directory and searched other directories one by one and found third ingredient on root/3rd.txt



This was my first solved THM actual CTF Lab. That's all for now, thanks for reading :)

- Sk. Md. Rashid Assef Shibly