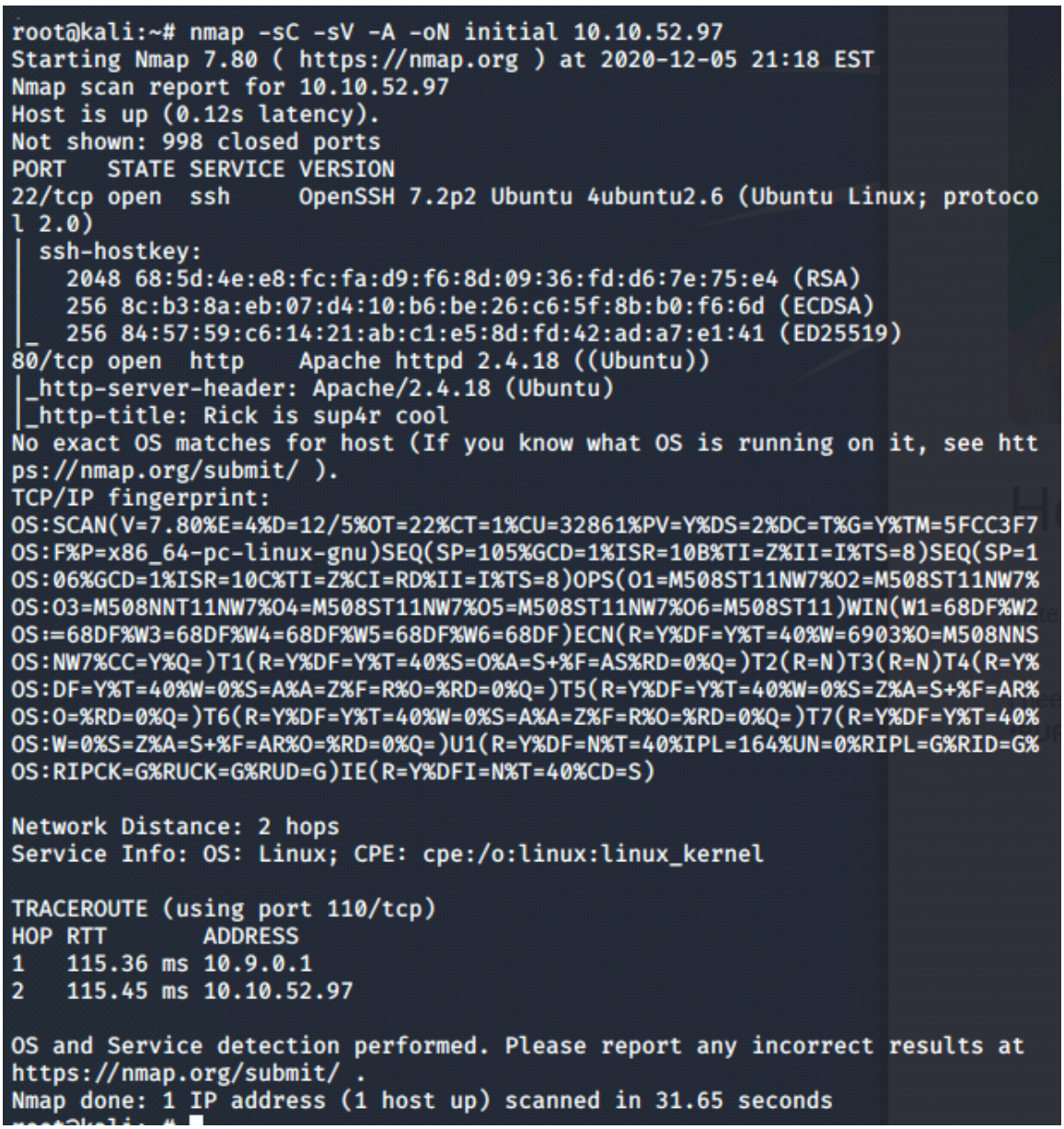
Pickle Rick CTF

First I start off by connecting to the openvpn in my Kali VM

We start off with a nmap scan to find any open ports.



```
root@kali:~# nmap -sC -sV -A -oN initial 10.10.52.97
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-05 21:18 EST
Nmap scan report for 10.10.52.97
Host is up (0.12s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 68:5d:4e:e8:fc:fa:d9:f6:8d:09:36:fd:d6:7e:75:e4 (RSA)
|   256 8c:b3:8a:eb:07:d4:10:b6:be:26:c6:5f:8b:b0:f6:6d (ECDSA)
|_  256 84:57:59:c6:14:21:ab:c1:e5:8d:fd:42:ad:a7:e1:41 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Rick is sup4r cool
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80%E=4%D=12/5%OT=22%CT=1%CU=32861%PV=Y%DS=2%DC=T%G=Y%TM=5FCC3F7
OS:F%P=x86_64-pc-linux-gnu)SEQ(SP=105%GCD=1%ISR=10B%TI=Z%II=I%TS=8)SEQ(SP=1
OS:06%GCD=1%ISR=10C%TI=Z%CI=RD%II=I%TS=8)OPS(O1=M508ST11NW7%O2=M508ST11NW7%
OS:O3=M508NNT11NW7%O4=M508ST11NW7%O5=M508ST11NW7%O6=M508ST11)WIN(W1=68DF%W2
OS:=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN(R=Y%DF=Y%T=40%W=6903%O=M508NNS
OS:NW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%
OS:DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%
OS:O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%
OS:W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%
OS:RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 110/tcp)
HOP RTT       ADDRESS
1   115.36 ms 10.9.0.1
2   115.45 ms 10.10.52.97

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 31.65 seconds
```

After the nmap I run gobuster to find any further knowledge to help.

```
root@kali:~# gobuster dir -u http://10.10.52.97 -w /usr/share/dirb/wordlist
s/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.52.97
[+] Threads:        10
[+] Wordlist:       /usr/share/dirb/wordlists/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2020/12/05 21:22:33 Starting gobuster
===============================================================
/.htpasswd (Status: 403)
/.htaccess (Status: 403)
/.hta (Status: 403)
/assets (Status: 301)
/index.html (Status: 200)
/robots.txt (Status: 200)
/server-status (Status: 403)
===============================================================
2020/12/05 21:23:52 Finished
===============================================================
root@kali:~#
```

Go buster shows us a few pages, one of them being robots.txt.

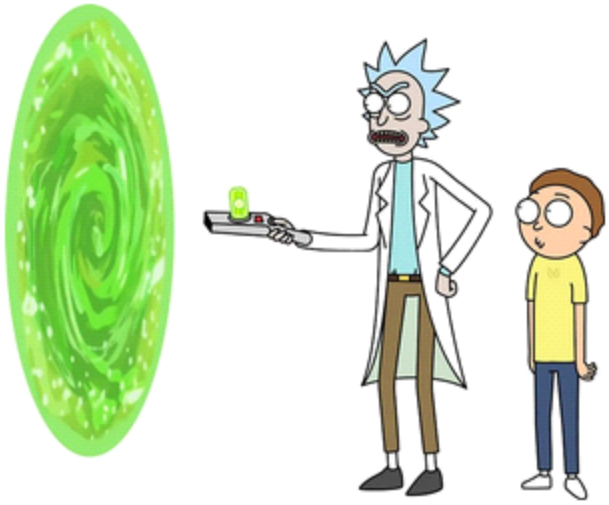
This page includes what seems to be either a username or password.

After inspecting the source code we find the username.

```
<!DOCTYPE html>
<html lang="en"> event
▶ <head> ··· </head>
▼ <body>
  ▶ <div class="container"> ··· </div>
    <!--Note to self, remember username! Username: R1ckRul3s-->
  </body>
</html>
```

Seeing that I have exhausted my other resources I now run nikto on the IP address to possible find a login page.

nikto finds us a login.php extension so we go to it



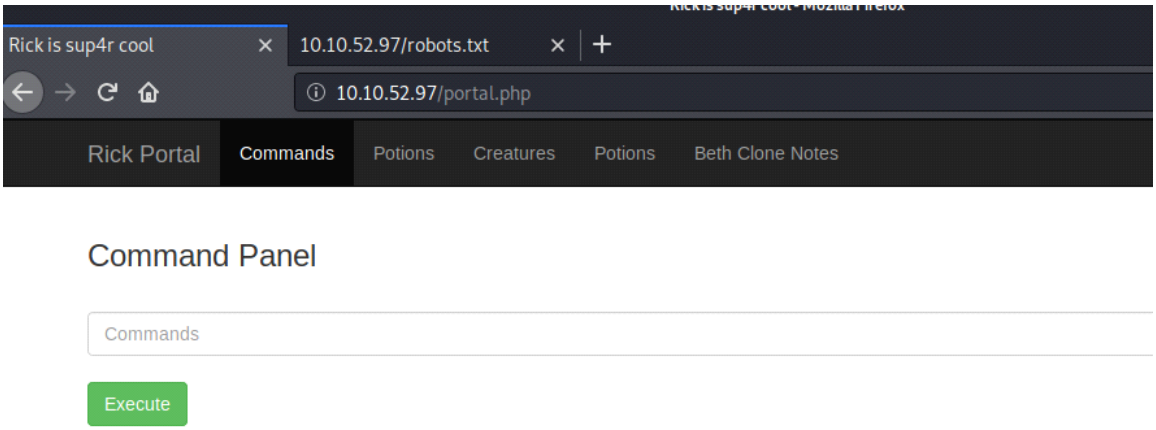
Portal Login Page

Username:

Password:

Login

We have the username from the source code. And the random string from robots.txt so maybe thats the password?



Bingo! we are logged in!

In the command panel we can enter ls command to find a list of txt files.

One of these text files is called Sup3rS3cretPickl3Ingred.txt so we add that to the end of the IP address and it gives us our first ingredient!

Now I tried a lot of commands and evenutally tried the ls /home

This command showed me two users and one of them was rick. So with ls /home/rick/ we find a file for second ingredients so we now use ls /home/rick/second ingredients to get our second flag

However ls wouldnt work so after some research I found out less is used to open files. so I used less /home/rick/second\ ingredients to finally get the second flag.

Now that we know that ls works, I tried sudo ls /root and found out there is a text file named 3rd.txt. Could this be our final ingredient? Lets check by running sudo less ls -la /root/3rd.txt

We are correct! and We have completed this room!

Command Panel

sudo less ls -la /root/3rd.txt

Execute

```
3rd ingredients: fleeb juice
```