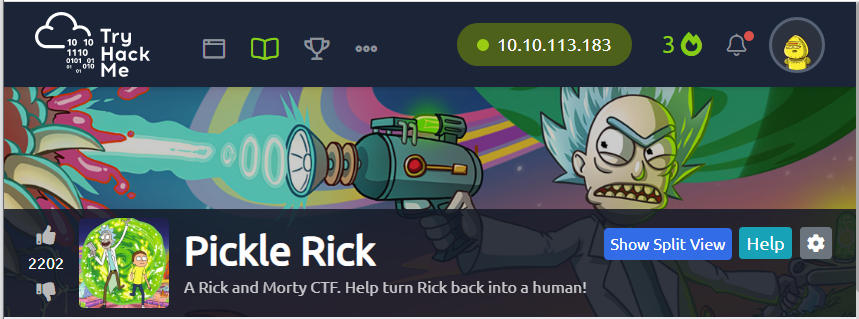
Guilibaldo (Gil) Valles

TryHackMe CTF Write up



# INFORMATION GATHERING

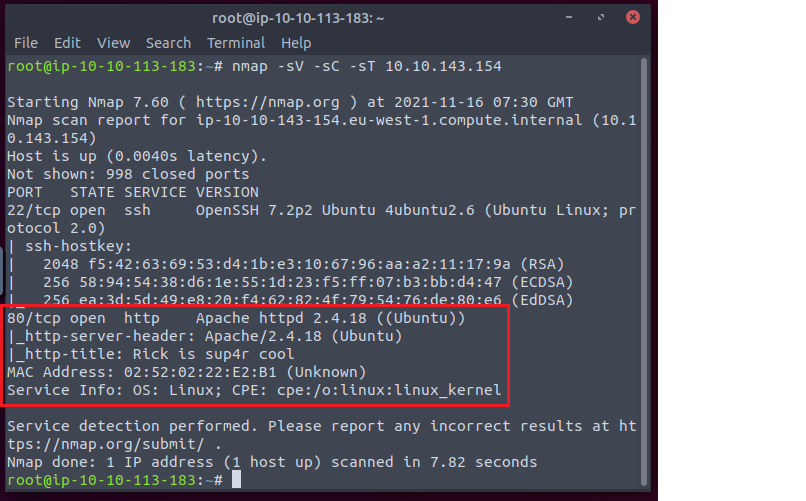
I was given a scope of host(s) from TryHackMe. You can see the network details of that device listed below:

- IP Address: 10.10.143.154

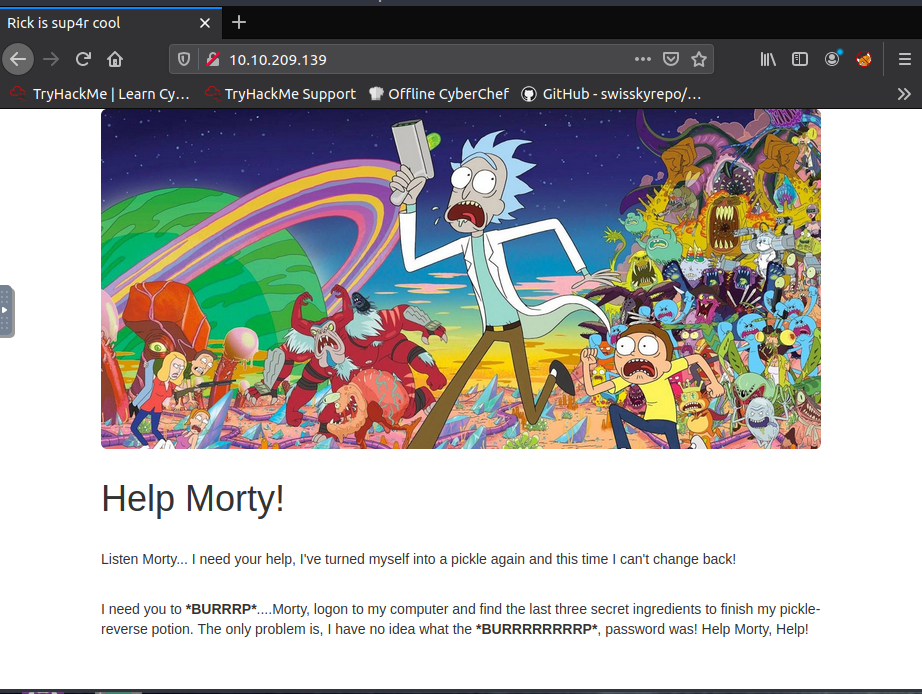
- MAC Address: 02:52:02:22:E2:B1

Enumeration

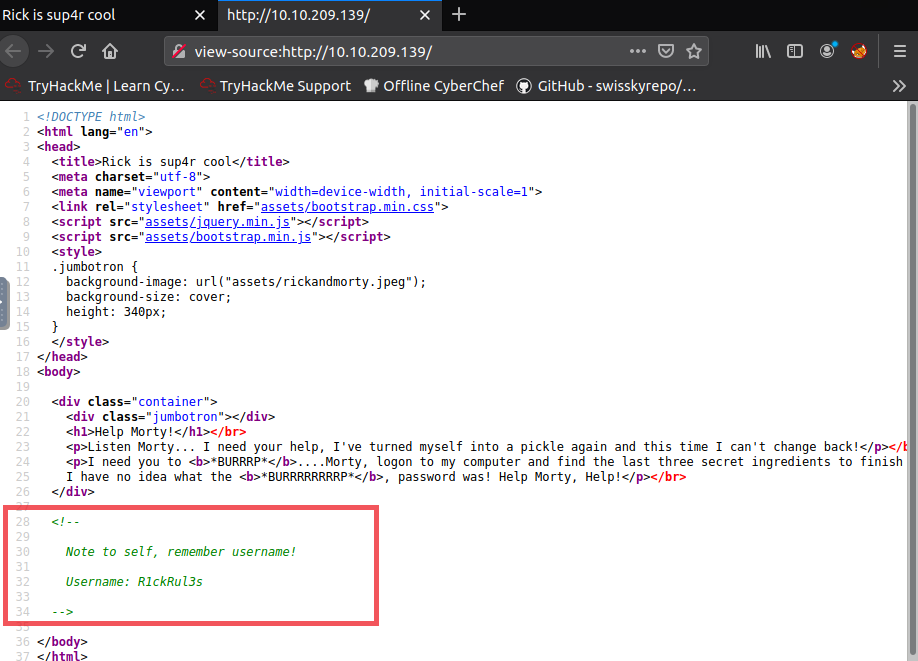
I performed service enumeration to discover information that may reveal critical details that could be leveraged to bypass security and gain an initial foothold into the system. I ran an ***nmap*** scan that revealed TCP port 80 was open.



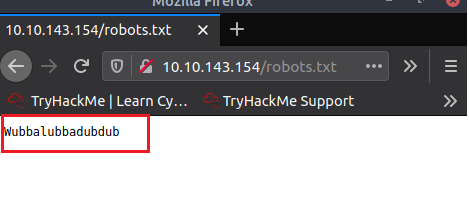
The next step was to browse the web page. The main landing page showed nothing of value.



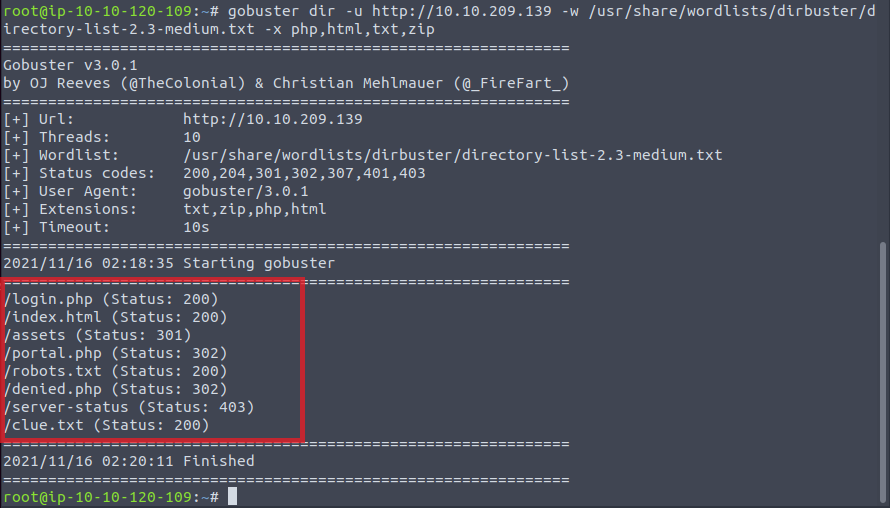
Upon viewing the page’s source, a commented out part of the HTML code revealed the username: *R1ckRul3s*



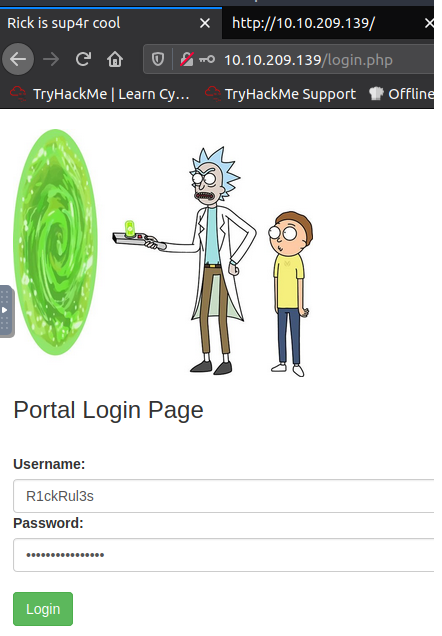
Taking a look at the website’s robot.txt directory simply shows one line of text. This could be a possible password: *Wubbalubbadubdub*



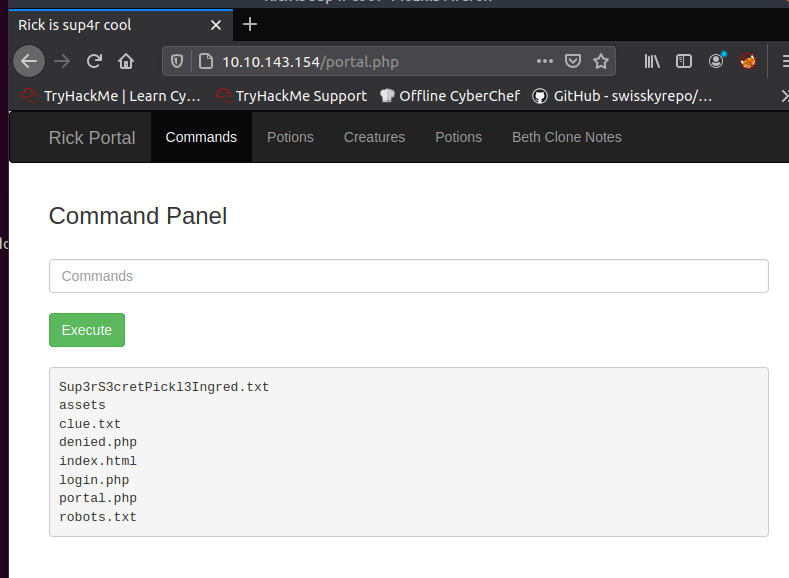
I discovered possible credentials but have yet to find anywhere to enter them. At this point I use ***gobuster*** to try and uncover hidden web directories. Gobuster returned a few interesting pages: *login.php, portal.php, clue.txt, assets*



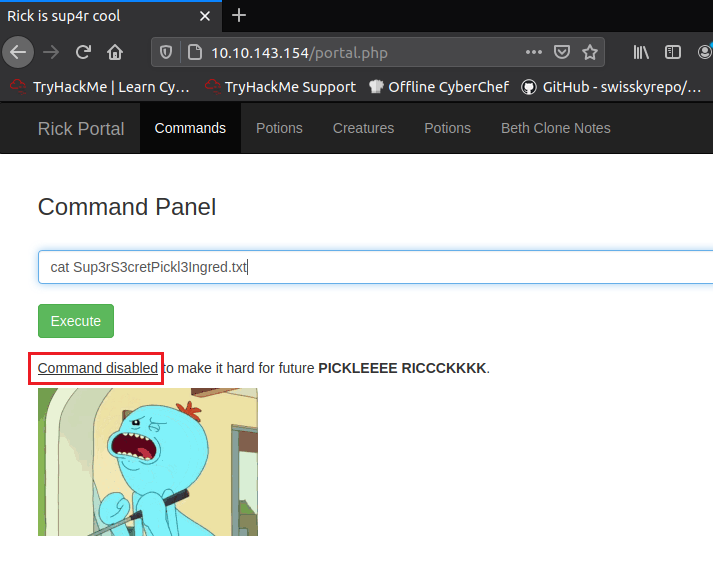
The page portal.php redirects to login.php so I enter the credentials I found.



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

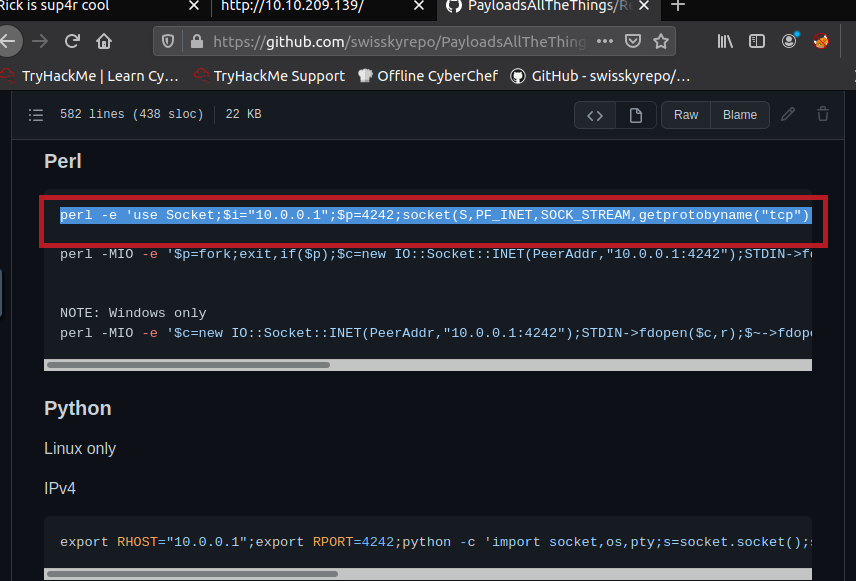


The file *Sup3rS3cretPickl3Ingred.txt* is new and may provide a flag for the TryHackMe questions so I try and ***cat*** the file to show it’s contents but the cat command is dsabled in the web browser command panel.



Exploitation

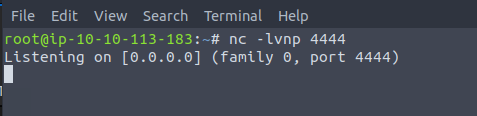
Since I can not run certain commands in the web browser, the next step is to try and obtain a reverse shell. I go to a popular github repo for reverse shell payload to use on the site. I copy a perl based reverse shell.



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



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



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.

