TryHackMe CTF Write-Up

Pickle Rick

Prepared by: NIVEDA S

From the Pickle Rick challenge on TryHackMe, we learn how to bypass a login screen, perform command injection, and gain a reverse shell.

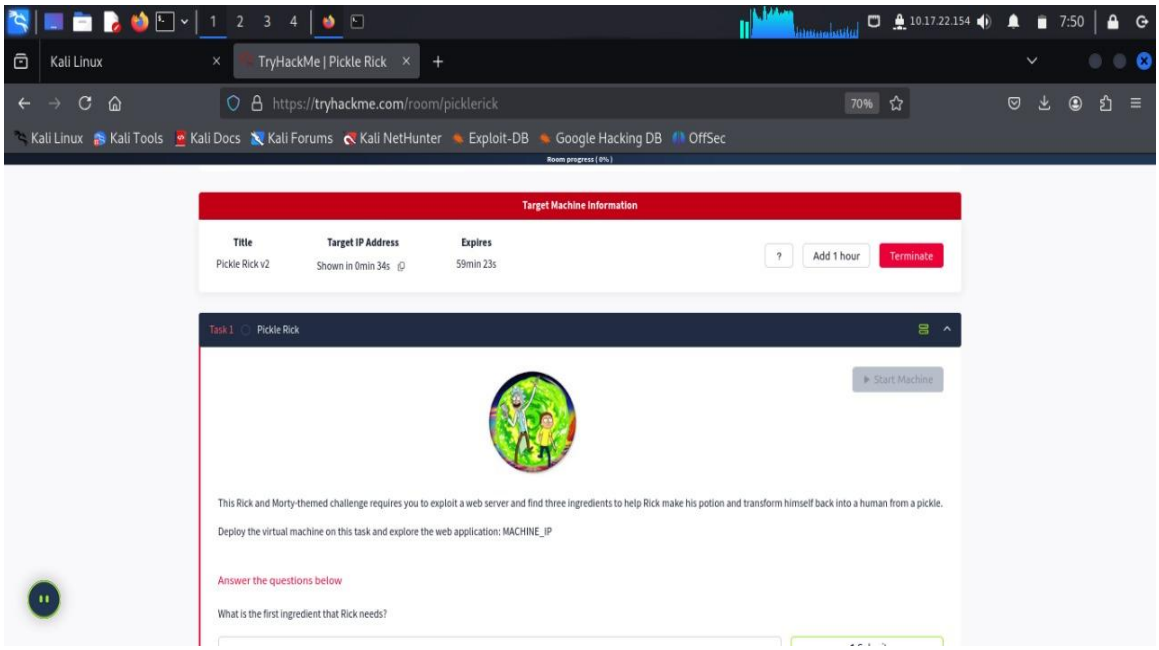
The theme of the challenge is: Rick has turned himself into a pickle and needs to find three ingredients to turn himself back into a human. So our mission is to find these three ingredients.

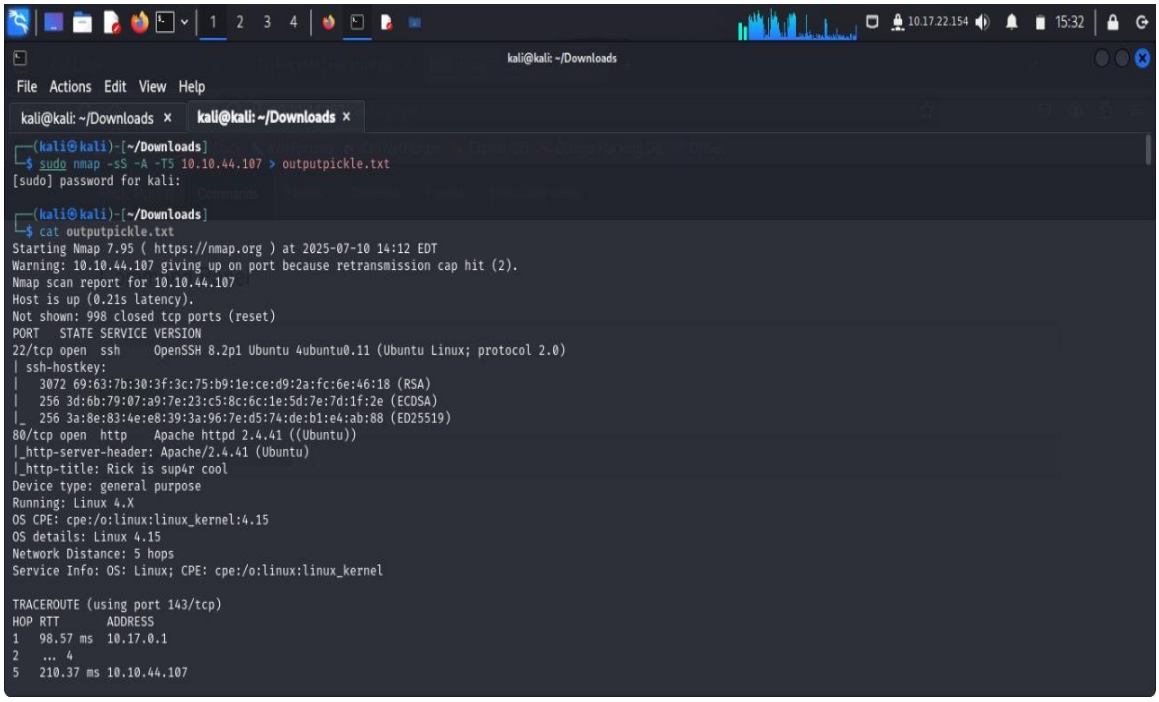
First, I connected TryHackMe with my OpenVPN by downloading the configuration file and using the `sudo openvpn` command.

Step 1: Start the Machine and Scan

We start the machine and get the IP address.
Using `nmap`, we scan the target IP and save the result in a .txt format file. Then, using the `cat` command, we read the file. From the scan result, we find that there is one SSH port and one HTTP port open.

So I paste the IP address into the browser. From this, we can confirm that a web server is running.

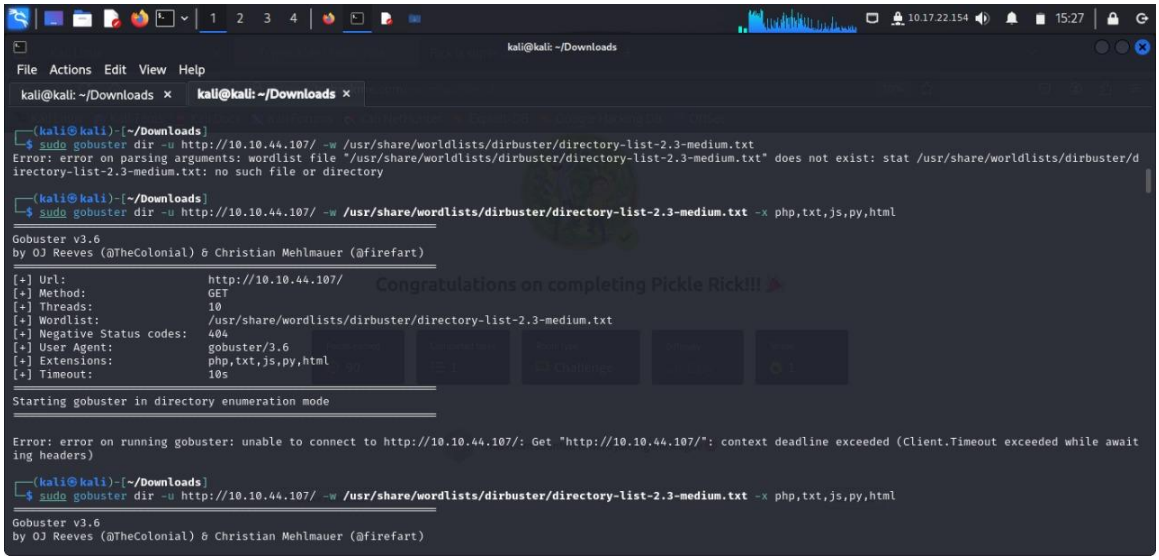




Step 2: Find Login Details

By viewing the source code of the page, we get a username, but there's no login page or password.

Using Gobuster, we discover hidden files. From reading this files `robots.txt`, `login.php`. gives us the password and access to the login portal.
Then, we log in.



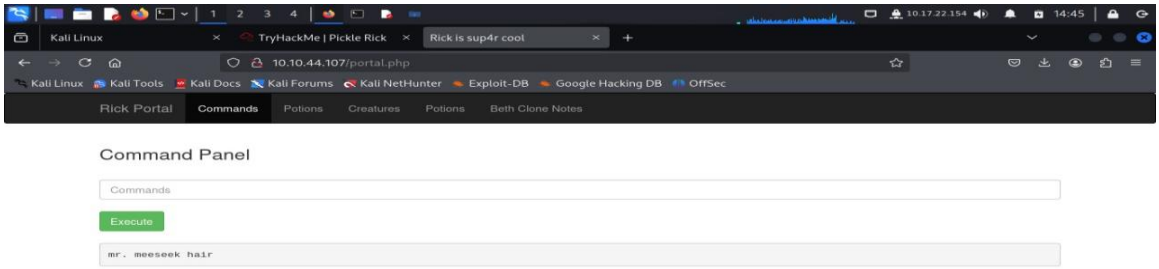
Step 3: Command Panel Access

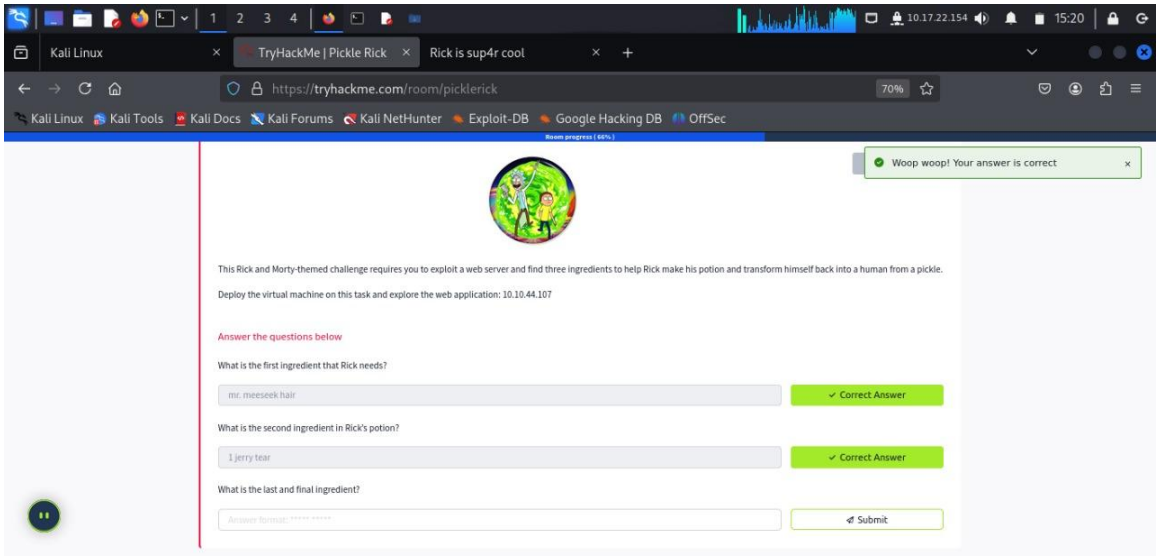
There is a command panel where we can run system commands.
So we try the `ls` command and get a list of all the files.

From the contents of `Sup3rS3cretPickl3Ingred.txt`, I got my first answer.

Then I checked what's in the `/home` directory. There are two users; I checked the `rick`

user and got the second ingredient.



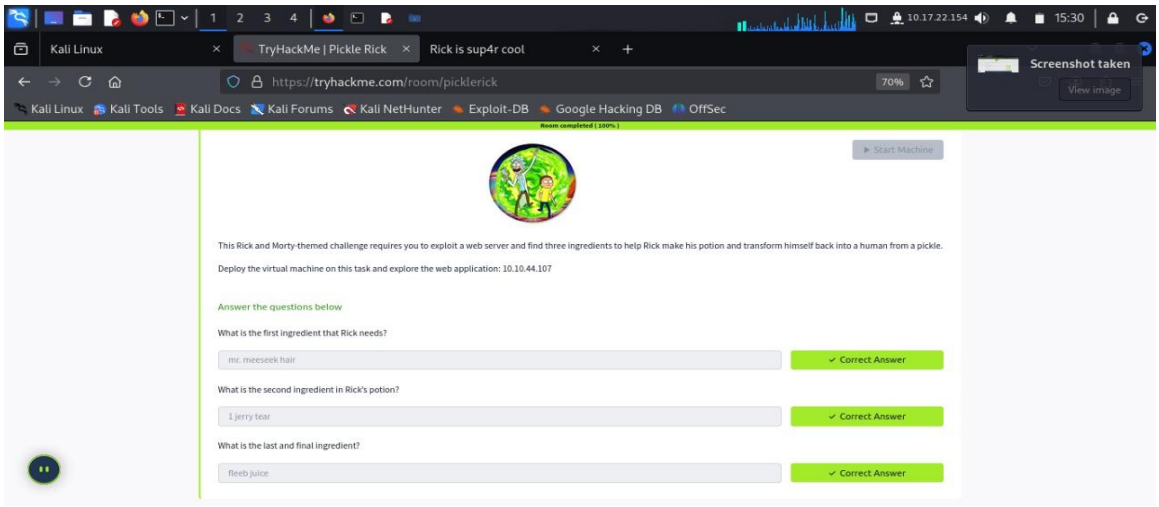


Step 4: Get Root Access for Third Ingredient

To check for the last ingredient under the `/root` directory, we need permission.

So we use the `sudo` command. From there, we get the third ingredient.

Or-For this step, we can use a bash reverse shell and a listener, which gives us access to the server and lets us view the content in the root directory.



Conclusion

We got all three ingredients to turn Rick back into a human and successfully completed the Pickle Rick challenge on TryHackMe.