

TryHackMe CTF Report – Pickle Rick Room

Name : Aiswarya R

Room Name : Pickle Rick

TryHackMe : <https://tryhackme.com/room/picklerick>

Target IP : 10.10.194.149

Objective

The goal of this CTF challenge is to help Rick return to his human form by finding 3 secret ingredients through web enumeration, decoding clues, and command-line interaction on a vulnerable web server.

Tools Used

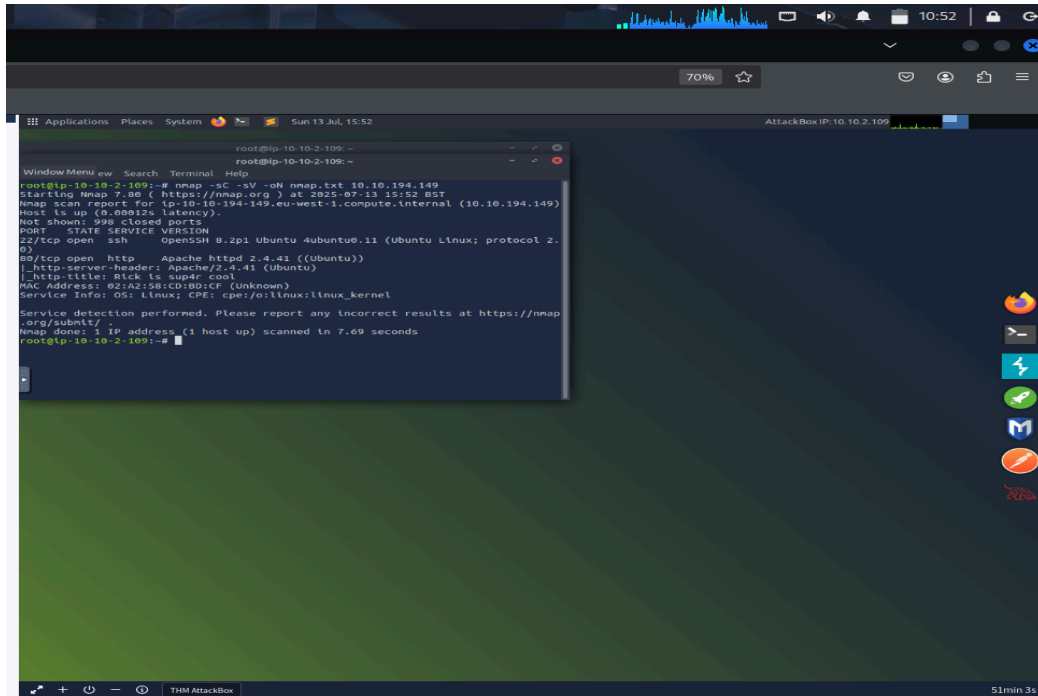
- Nmap (for port scanning)
- Gobuster (for directory enumeration)
- Firefox (web interaction)
- TryHackMe AttackBox / Kali Linux

Steps Followed

1. Scanning with Nmap

Command used:

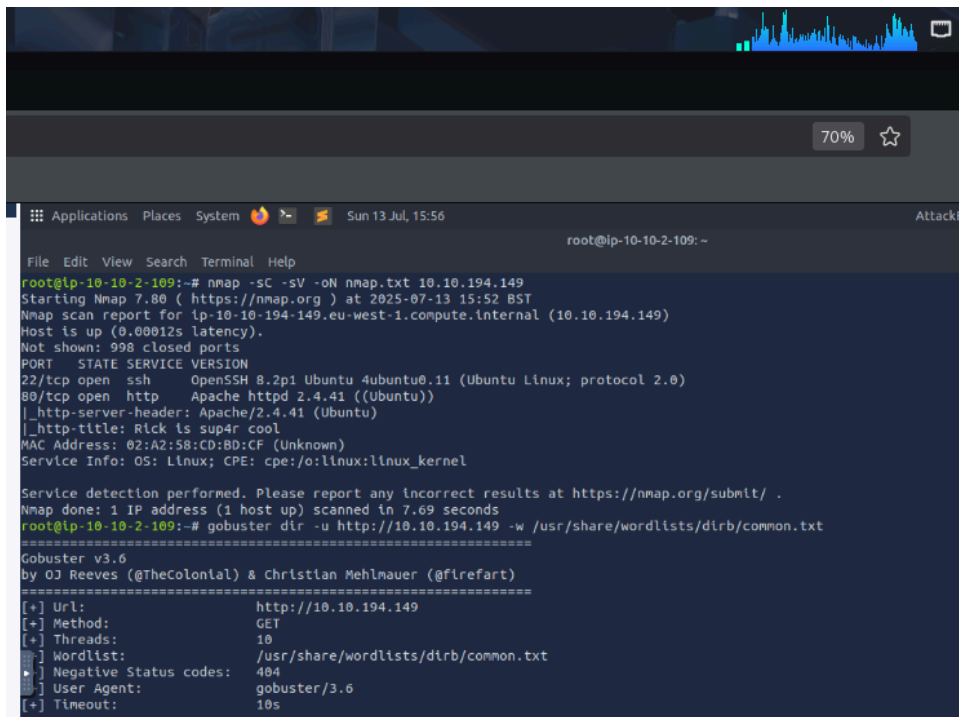
```
nmap -sC -sV -oN nmap.txt 10.10.194.149
```



2. Directory Enumeration with Gobuster

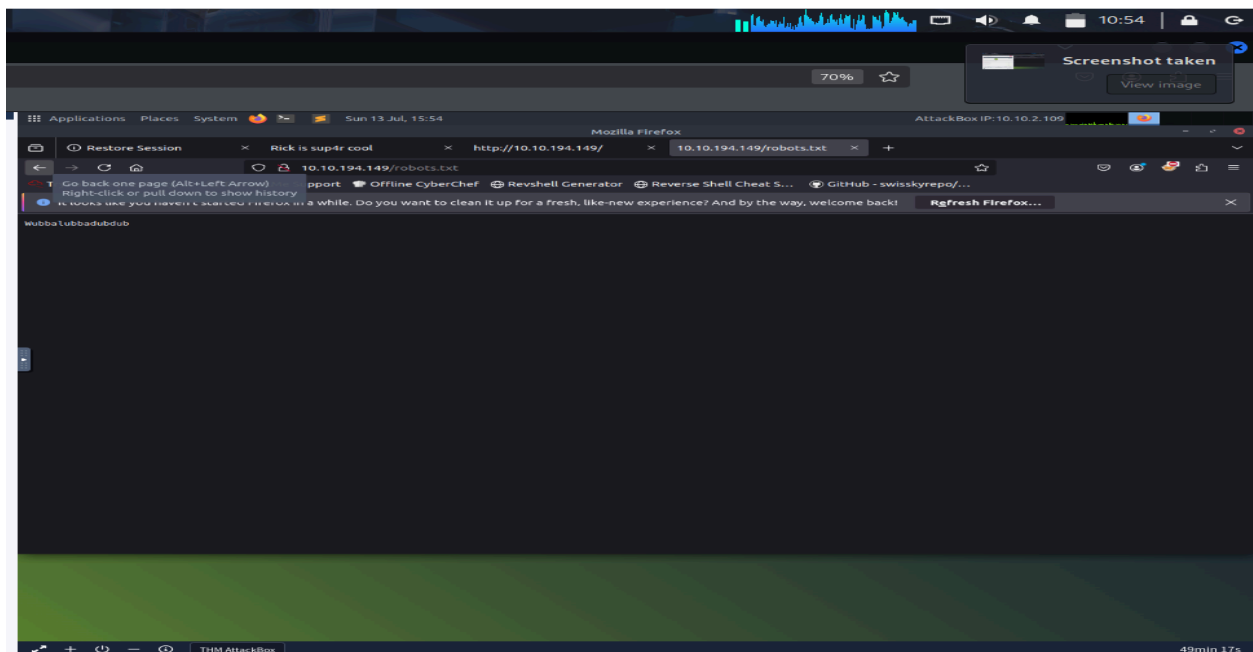
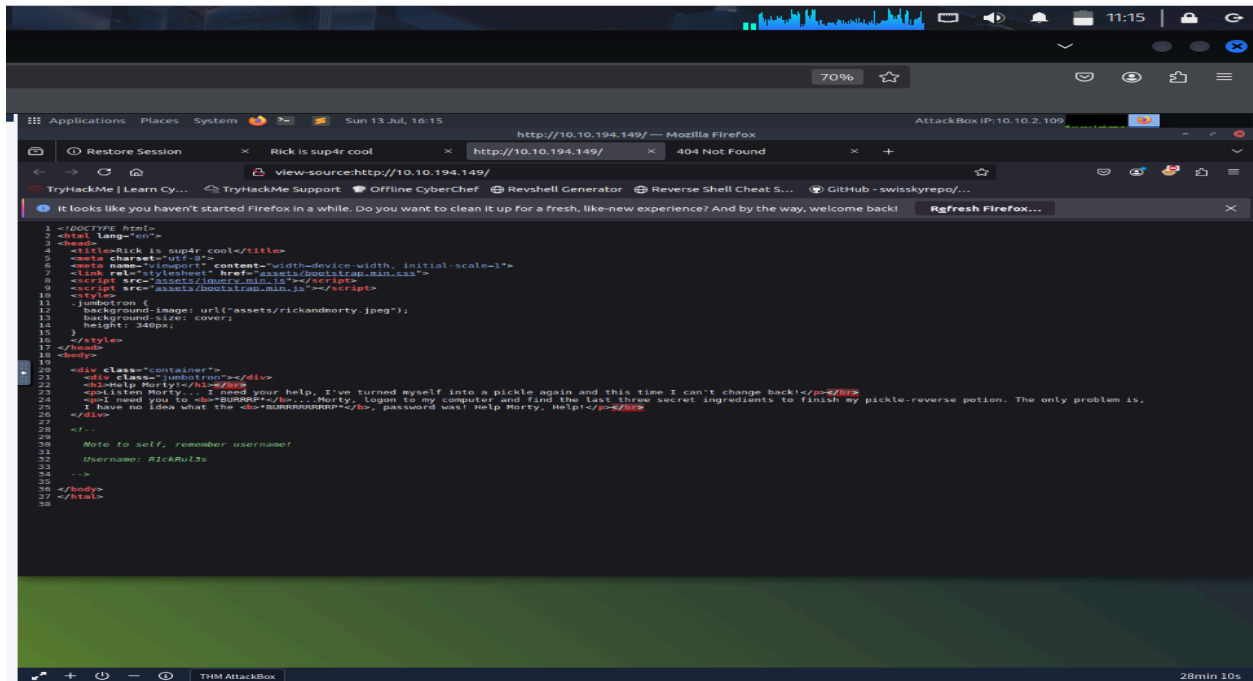
Command used:

```
gobuster dir -u http://10.10.194.149 -w /usr/share/wordlists/dirb/common.txt
```



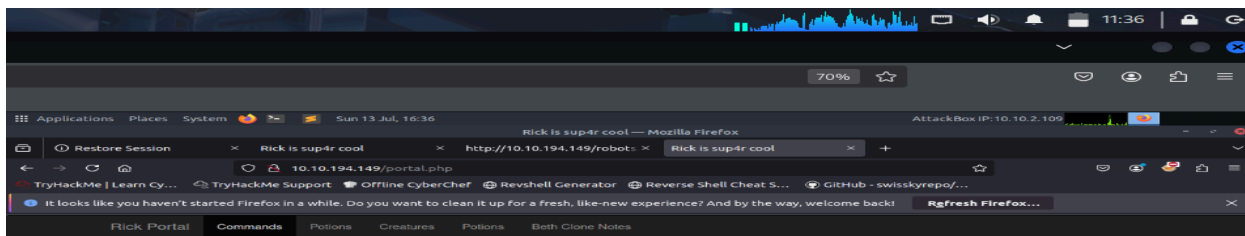
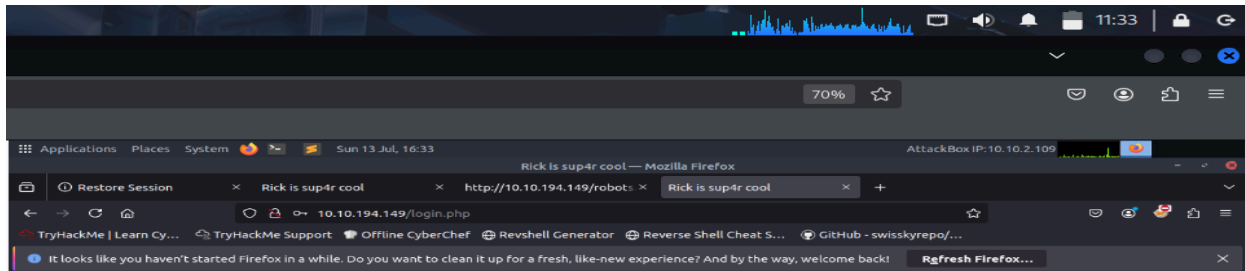
3. Discovering Credentials

- Found username **R1ckRu13s** in page source
- Found password **Wubbalubbadubdub** in **robots.txt**



4. Accessing Hidden Login Panel

- Discovered path: **/login.php**
- Successfully logged into the command interface



5. Extracting the Ingredients

Commands used:

1. `more Sup3rS3cretPickl3Ingred.txt`
2. `more /home/rick/second_ingredient.txt`
3. `more /root/third_ingredient.txt`

6. Final Answers Submitted

Question	Answer
First Ingredient	mr. meeseek hair
Second Ingredient	1 jerry tear
Final Ingredient	fleeb juice

Summary

This task involved basic CTF methodology such as enumeration, hidden path discovery, and web-based command execution. Although the machine had time constraints and some steps were challenging, this was a great learning experience for identifying weaknesses in web applications and practicing real-world enumeration tactics.