

# 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.

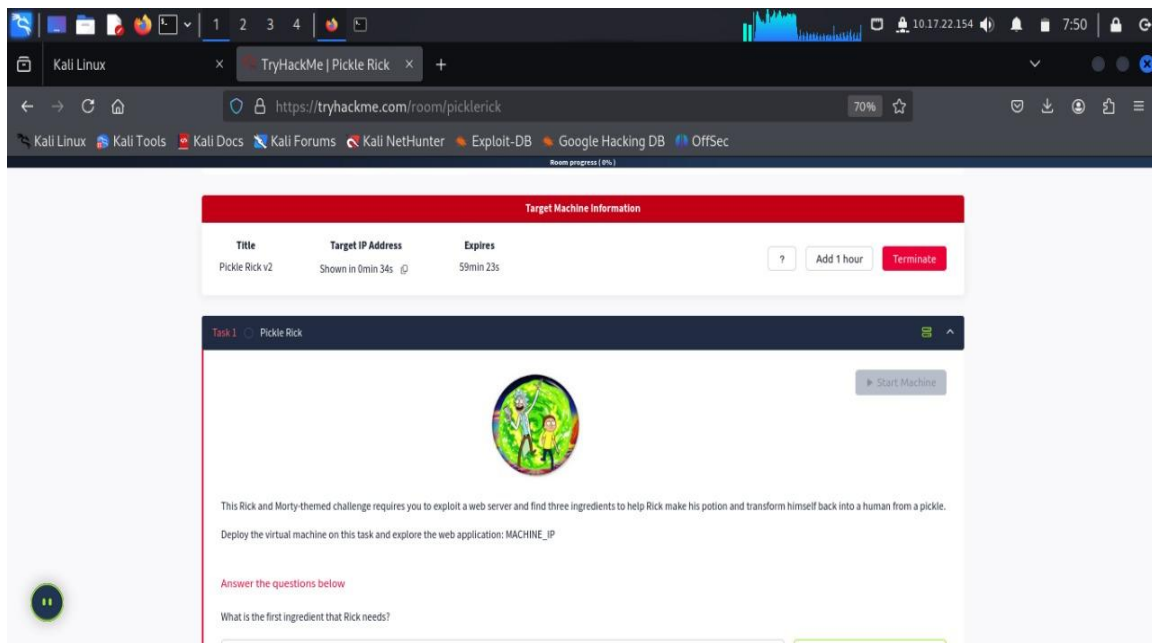
First, I connected TryHackMe with my OpenVPN by downloading the configuration file and using the `sudo openvpn` command.

### 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.



```
kali@kali: ~/Downloads
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~/Downloads x
(kali@kali)~/Downloads
$ sudo nmap -sS -A -T5 10.10.44.107 > outputpickle.txt
[sudo] password for kali:
(kali@kali)~/Downloads
$ cat outputpickle.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-10 14:12 EDT
Warning: 10.10.44.107 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.44.107
Host is up (0.21s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 3072 69:63:7b:30:3f:3c:75:b9:1e:ce:d9:2a:fc:6e:46:18 (RSA)
|_ 256 3d:6b:79:07:a9:7e:23:c5:8c:6c:1e:5d:7e:7d:1f:2e (ECDSA)
|_ 256 3a:8e:83:4e:e8:39:3a:96:7e:d5:74:de:b1:e4:ab:88 (ED25519)
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-title: Rick is sup4r cool
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
Network Distance: 5 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 143/tcp)
HOP RTT      ADDRESS
1   98.57 ms  10.17.0.1
2   ... 4
5  210.37 ms 10.10.44.107
```

## 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.

```
kali@kali: ~/Downloads
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~/Downloads x
(kali@kali)~/Downloads
$ sudo gobuster dir -u http://10.10.44.107/ -w /usr/share/worldlists/dirbuster/directory-list-2.3-medium.txt
Error: error on parsing arguments: wordlist file "/usr/share/worldlists/dirbuster/directory-list-2.3-medium.txt" does not exist: stat /usr/share/worldlists/dirbuster/directory-list-2.3-medium.txt: no such file or directory
(kali@kali)~/Downloads
$ sudo gobuster dir -u http://10.10.44.107/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt,js,py,html
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.44.107/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,txt,js,py,html
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

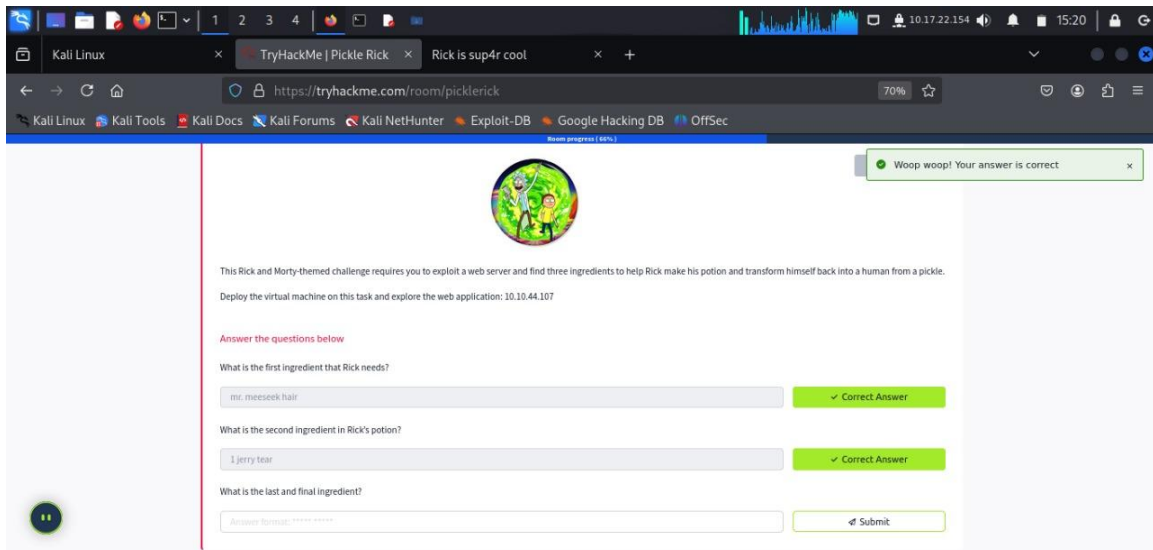
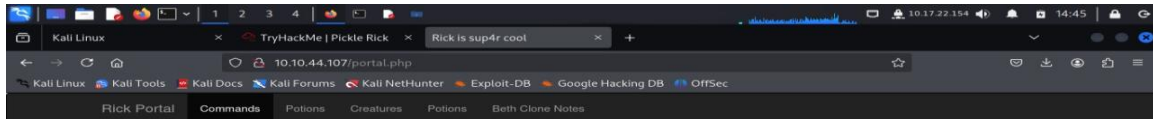
Error: error on running gobuster: unable to connect to http://10.10.44.107/: Get "http://10.10.44.107/": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
(kali@kali)~/Downloads
$ sudo gobuster dir -u http://10.10.44.107/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt,js,py,html
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
```

### 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.

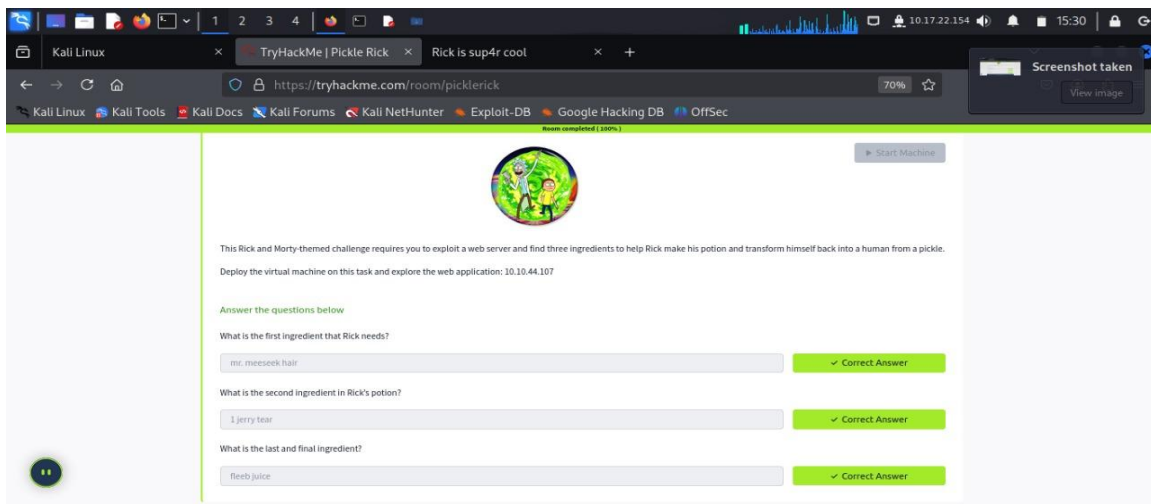


## Step 4: Get Root Access for Third Ingredient

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.

