nmap

parámetros

- -sS : escanea los puertos más normales o los difinidos en `services`
- -p : escanea un puerto determinado (50), un rango (50-60) o todos, poniendo un guión (-p-)
- -Tx : establece el periodo de tiempo que deja pasar para escanear un dispositovo para evitar ser detectado y que el firewall nos mande información falsa. De más espaciado a menos:
  - T0: paranoid
  - T1: sneaky
  - T2: polite
  - T3: normal
  - T4: aggresive
  - T5: insane

+ info

- https://hackertarget.com/nmap-cheatsheet-a-quick-reference-guide/

cut&paste

scan de puertos:

```
nmap -sS -sV -P0 -O <ip o dominio>
```

```
nmap -sS <ip o dominio> -> scan de los puertos más normales o los definidos en ''services''
```

hosts activos de una red:

```
nmap -sP <ip_range>
```

hosts con puerto activo (en este caso, AFP apple):

```
nmap -p 548 <ip> -Pn -n
```

Scan a través de proxies (ver lista más abajo):

```
# nmap -sS -sV -P0 -O --proxies "http://199.193.255.160:3128,http://64.20.45.139:8080,http://64.20.54.211:8080" www.torrelles.cat
```

proxies

- http://proxylist.hidemyass.com/search-1305348#listable
- https://www.sslproxies.org/