

# nmap

## parámetros

- -sS : scanea los puertos más normales o los definidos en services
- -p : scanea un puerto determinado (50), un rango (50-60) o todos, poniendo un guión (-p-)

## cut&paste

scan de puertos:

```
nmap -sS -sR -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
```

From:

<https://miguelangel.torresegea.es/wiki/> - miguel angel torres egea

Permanent link:

<https://miguelangel.torresegea.es/wiki/linux:tcpip:nmap?rev=1322154320>

Last update: **24/11/2011 09:05**

