Eines de xarxa: nmap i nast

Nmap és un escànner de xarxes que serveix per explorar i auditar la seguretat de les xarxes.
Nast és una eina d'anàlisi de xarxes i de captura de les trames de la xarxa (sniffer).

Instal·lació:
apt-get install nast nmap

Si tinc una adreça de xarxa 192.168.1.0/24 i vull llistar els hosts presents en la xarxa amb les seves adreces MAC
nast -m

```
Nast V. 0.2.0

Mapping the Lan for 255.255.255.0 subnet ... please wait

MAC address Ip address (hostname)
==================================
00:03:XX:XX:XX:XX 192.168.1.1 (ROUTER)
00:22:XX:XX:XX:XX 192.168.1.236 (TALLER36) (*)
00:18:XX:XX:XX:XX 192.168.1.223 (TALLER23)

(*) This is localhost
```

També podem obtenir un llistat dels hosts actius amb nmap:
$ nmap -sP 192.168.1.0/24

Si tenim diversos hosts i no tenim clar quin d'ells ens pot proporcionar sortida a la Internet ho podem saber amb la ordre:
nast -g

```
Nast V. 0.2.0

Finding suitable hosts (excluding localhost) -> Done

Trying 192.168.1.1 (00:03:XX:XX:XX:XX)-> Yep!
Trying 192.168.1.223 (00:18:XX:XX:XX:XX) -> Bad!
```

Aquells hosts amb el missatge Yep! confirmen que tenim sortida a la Internet.

Per obtenir informació d'un host, quin sistema operatiu té, i quins ports comuns té oberts podem fer servir l'ordre:
$ sudo nmap -O 192.168.1.223