NMAP

who is online ?

nmap use multiple ways to **specify its targets**.

ip range using **-** if you want to scan all the ip addresses from 192.168.0.1 yo 192.168.0.10 yo can write 192.168.0.1-10.

ip subnet using **/** if you want to scan subnet, you can express it as 192.168.0.1/24 and it was equivalent to 192.168.0.0-255

Hostname you can also specify the target by hostname, for example **example.thm**

Lets say you want to *discover the online hosts on a network.* Nmap offer the **-an** option.

Scanning a "Local" Network

we use local to refer to the network we are directly connected to.

in this example *our ip addres is 192.168.66.89* and we are *scanning the 192.168.66.0/24* network

```
nmap -sn 192.168.66.0/24
```