**nmap** (Abreviatura de **Network Mapper**) es la mejor herramienta de línea de comandos en **Linux** (también disponible para Windows y Mac OS X) para realizar funciones de **auditoría y seguridad de redes**, rastreo y análisis en busca de sistemas para elaborar un **inventario de red**, etc. Todo esto de forma gratuita y bajo licencia open source. Lanzando un escaneo de red con Nmap podemos visualizar una gran cantidad de información: **hosts activos en la red, sistema operativo que están ejecutando, puertos y servicios abiertos a través de la red, tipos de firewall que están utilizando**… para los recelosos de la línea de comandos, existe la opción de utilizar Nmap con GUI, para ello está Zenmap.

Direcciones activas

nmap -sP <Red>

PUertos TCP abiertos

nmap -sT <IP\_Máquina>

Si puerto esta abierto

nmap -p <puerto> <máquina>

nmap -p 80 192.168.1.20

COnocer sisema operative de maquina

nmap -O <ip>

nmap -sS -O -T3 -oA invent <red>

