Escaneo de redes

* **NMAP -**

comandos para verificar red

ya disponible en Linux

se puede realizar un sondeo de flags para determinar puertos abiertos

permite escaneos agresivos, completos

ver ips

ver puertos

ver que nomas tienen con -a -sT

servicios de cada máquina disponible

con nmap -f (se salta los ids e firewalls)

mtu 8

revisar snmp. Netbios

* **angry ip scan**

preferencias y puedo filtrar icmp y protocolos

se ejecuta en Windows

en display permite visualizar solo los que dan ok en el ping

* **megapin**

host discovey

TTl 128 equipo Windows

TTl 64 equipo linux

Cisco solaris aix 255 ttl

* netscantools

manual tools- ping scanner – port scanner

* sxtools

esta en parrot- toca instalar

* hping3

ya instalada en parrot

sudo su Thor

revisar

<https://www.linkedin.com/pulse/ceh-practical-exam-all-you-need-know-xiotz-exzpf/>

* netbios

revisar bios de equipos

* ad explorer

revisión ldap