Guía NMAP:

**Instalación**: apt install nmap

**Ejemplo práctico**:

Nmap –sP –n (Y la ip de la subred que nos encontramos, depende de su red)

s: para hacer un escaneo

P: escaneo ISMP ya que será un escaneo ping a toda la sub red

-n: para evitar la resolución de nombres así será más rápido

Nmap -p- -sV (ip objetivo)

-p-: para que escanee los 65535 puertos en nuestro objetivo

-sV para que nos muestre la versión de los servicios que corren en ese servicio

**Escaneo Básico**: nmap [HOST] o [IP]

**Toda una subred**: nmap 192.168.0.\*

**Excluimos una ip**: nmap 192.168.0.\* --exclude 192.168.0.1

**A diferentes octetos**: nmap 192.168.0.100,101,102

**Lectura de archivo con objetivos**: nmap –iL archivo.txt

**Rangos de ip**: nmap 192.168.0.10-20

**Mayor detalle**: nmap –v [IP]

**Multiple**: nmap [IP] [IP]

**Saber el SO**: nmap –O [IP]

**SO que lo gobierna y traceroute**: nmap –A [IP]

**Detectar Firewall**: nmap –sA [IP]

**Dispositivos encendidos en la red**: nmap –sP 192.168.0.\*

**Escaneo rápido por los puertos más usados**: nmap –F [IP]

**Orden creciente en resultados**: nmap –r [IP]

**Escaneo de puestos específico**: nmap –p 22 [IP]

**Versiones de los servicios**: nmap –sV [IP]

**Escaneo Exhaustivo**: nmap –sS [IP]

**Con análisis de prueba de firewall**: nmap –sN [IP]

**Escaneo de varios puertos**: nmap –p 22,80,25 [IP]

**Por rango de puertos**: nmap –p 1-1000 [IP]

**Escaneo completo exhaustivo**:

Nmap –O –n –v –sS –p 1-65535 192.168.0.0/24

**Para almacenar resultados**: nmap [IP] > resultado.txt