

**Centro de Enseñanza Técnica Industrial**

**Desarrollo de Software**

**Documentación de nmap**

**Jesús Alberto Aréchiga Carrillo**

**22310439 5N**

**Profesor**

**José Francisco Pérez Reyes**

**Noviembre 2024**

**Guadalajara, Jalisco**

## Introducción

El comando nmap (Network Mapper) es una herramienta de código abierto ampliamente utilizada en la auditoría de seguridad y el análisis de redes. Su principal función es descubrir hosts y servicios en una red, lo que permite a los administradores de sistemas y especialistas en seguridad identificar posibles puntos de vulnerabilidad y conocer la infraestructura subyacente.

## Desarrollo

El comando nmap tiene muchas opciones para usarse, en esta práctica se van a usar 10 combinaciones de argumentos y mostrar la función que hacen dichas combinaciones.

1. nmap [IP]A computer screen shot of a black screen

   Description automatically generatedEscanea una subred completa (en este caso, la red de clase C 192.168.1.0) para encontrar hosts activos.
2. nmap -p- [IP]A screen shot of a computer

   Description automatically generated

Escanea todos los puertos de una dirección IP en específico. Es útil para descubrir servicios que no están en los puertos comunes.

1. nmap -p [IP] A computer screen with numbers and letters

   Description automatically generatedEscanea puertos específicos de una dirección IP
2. nmap -sV [IP] A computer screen with white text

   Description automatically generatedEscanea dando las versiones de los servicios que se están ejecutando
3. nmap -sS [IP] A screen shot of a computer

   Description automatically generatedEscanea los puertos de una diercción IP en modo sigiloso (SYN scan), que es más dificil de detectar porque no el handshake TCP.
4. nmap -O [IP] A computer screen with white text

   Description automatically generatedEscanea la dirección IP brindando información del sistema operativo que se está utilizando.
5. nmap -T4 192.168.1.64A screen shot of a computer

   Description automatically generatedEscanea los puertos de una dirección IP en modo rápido. Utiliza el nivel de velocidad T4, que es más rápido que el escaneo normal. Ideal para hacer un escaneo más ágil, pero consume más recursos.
6. nmap -Pn [IP] A screen shot of a computer

   Description automatically generatedEscanea los puertos de una dirección IP sin ping para evitar la detección de ICMP. Útil para escanear dispositivos que bloquean solicitudes ICMP.
7. nmap -sA [IP] A black screen with white text

   Description automatically generatedEscanea puertos de un a dirección IP con detección de firewall o presencia de sistemas de filtrado de paquetes
8. nmap –traceroute [IP] A computer screen with white text

   Description automatically generatedMuestra la ruta que los paquetes siguen para llegar al objetivo, lo que ayuda a identificar los saltos de red y posibles problemas en la ruta.