**2.2 Descripción de la tecnología Nmap**

****

Es una herramienta de código abierto que sirve para efectuar un rastreo de puertos. Fue escrito originalmente por Gordon Lyon (más conocido por su alias Fyodor Vaskovich) y cuyo desarrollo se encuentra hoy a cargo de una comunidad.

Fue creado originalmente para Linux aunque actualmente es multiplataforma. Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una [red](https://es.wikipedia.org/wiki/Red_de_computadores) [informática](https://es.wikipedia.org/wiki/Inform%C3%A1tica), para ello Nmap envía unos paquetes definidos a otros equipos y analiza sus respuestas.

Este software posee varias funciones para sondear [redes de computadores](https://es.wikipedia.org/wiki/Redes_de_computadores), incluyendo detección de equipos, servicios y [sistemas operativos](https://es.wikipedia.org/wiki/Sistemas_operativos). Estas funciones son extensibles mediante el uso de scripts para proveer servicios de detección avanzados, detección de vulnerabilidades y otras aplicaciones. Además, durante un escaneo, es capaz de adaptarse a las condiciones de la [red](https://es.wikipedia.org/wiki/Red_de_computadores) incluyendo [latencia](https://es.wikipedia.org/wiki/Latencia) y [congestión](https://es.wikipedia.org/wiki/Congesti%C3%B3n_de_red) de la misma.

Nmap es reconocido como el scanner de puertos mas poderoso. Fue diseñado para escanear rápidamente grandes redes, aunque funciona bien contra el anfitrión individuales. Se utiliza comúnmente para las auditorías de seguridad, aunque a muchos sistemas y administradores de red les resulta útil para tareas de rutina, tales como inventario de la red, los horarios de actualización de servicio de gestión, monitoreo y anfitrión o un tiempo de servicio, y para recolectar información para futuros ataques (hackers).

Nmap puede funcionar en sistemas operativos basados en Unix (GNU/Linux, Solaris, BSD y Mac OS X) y también en otros sistemas operativos como Microsoft Windows y AmigaOS.

Respecto a su funcionamiento, es capaz se utilizar diferentes técnicas de evasión de detección como escaneo sealth. Soporta escaneos sobre ciertos puertos específicos, entre rangos IP específicos, uso se paquetes Null, FIN, Xmas y ACK, además SYN que es el paquete por defecto. Esto significa que se mandan cierto tipo de paquetes a cada puerto y estos responderán con alguna señal que permitirá a scanner encontrar versiones y servicios.

Sus principales características son las siguientes:

* Descubrimiento de [servidores](https://es.wikipedia.org/wiki/Servidores): Identifica computadoras en una red, por ejemplo listando aquellas que responden [ping](https://es.wikipedia.org/wiki/Ping).
* Identifica [puertos](https://es.wikipedia.org/wiki/Puerto_(computaci%C3%B3n)) abiertos en una [computadora](https://es.wikipedia.org/wiki/Computadora) objetivo.
* Determina qué servicios está ejecutando la misma.
* Determinar qué [sistema operativo](https://es.wikipedia.org/wiki/Sistema_operativo) y versión utiliza dicha computadora, (esta técnica es también conocida como [fingerprinting](https://es.wikipedia.org/wiki/Fingerprinting)).
* Obtiene algunas características del hardware de red de la máquina objeto de la prueba.

Nmap es una gran herramienta de carácter gratuito.

EJEMPLO de uso:

