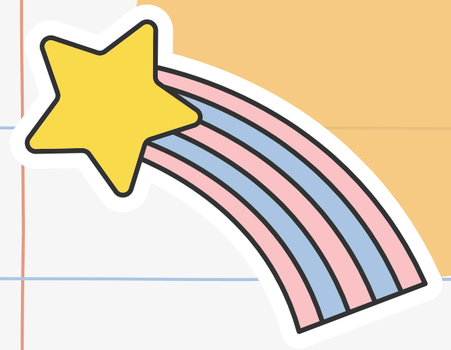
inteligencia Activa



Alexis Valencia Ramirez

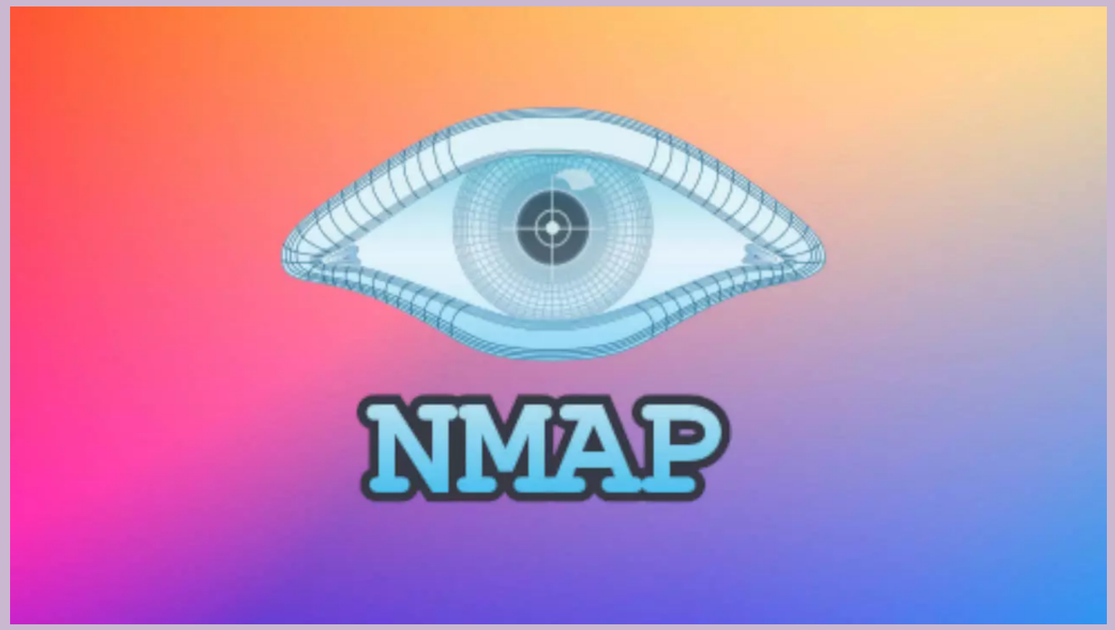
Analisis de dispositivos y puertos con Nmap

Nmap es un software de código abierto que se utiliza para escanear una red y sus puertos con el objetivo de obtener información importante sobre la misma para controlar y gestionar su seguridad. Es una aplicación que se utiliza normalmente para realizar auditorías de seguridad y monitoreo de redes.

- **Ping/Arp son escaneos muy útiles a la hora de conocer qué host se encuentran activos en la red (Ping) o para obtener información específica sobre los host activos (Arp)**
- **TCP Connect sirve para realizar una conexión completa de todos los puertos.**
- **Sondeo de lista tiene la finalidad de obtener los nombres de equipo de los distintos dispositivos conectados a la red, sin la necesidad de enviar un paquete para ello (realiza una resolución inversa de DNS).**
- **FIN sirve para determinar si el host e encuentra tras un cortafuego.**

Parametros opciones de escaneo de nmap

- **Seleccionar objetivos: Direcciones o rangos IP, nombres de sistemas, redes, etc.**
- **Descubrir sistemas.**
- **Técnicas de análisis de puertos.**
- **Puertos a analizar y orden de análisis.**
- **Duración y ejecución:**
- **Detección de servicios y versiones.**
- **Evasión de Firewalls/IDS.**

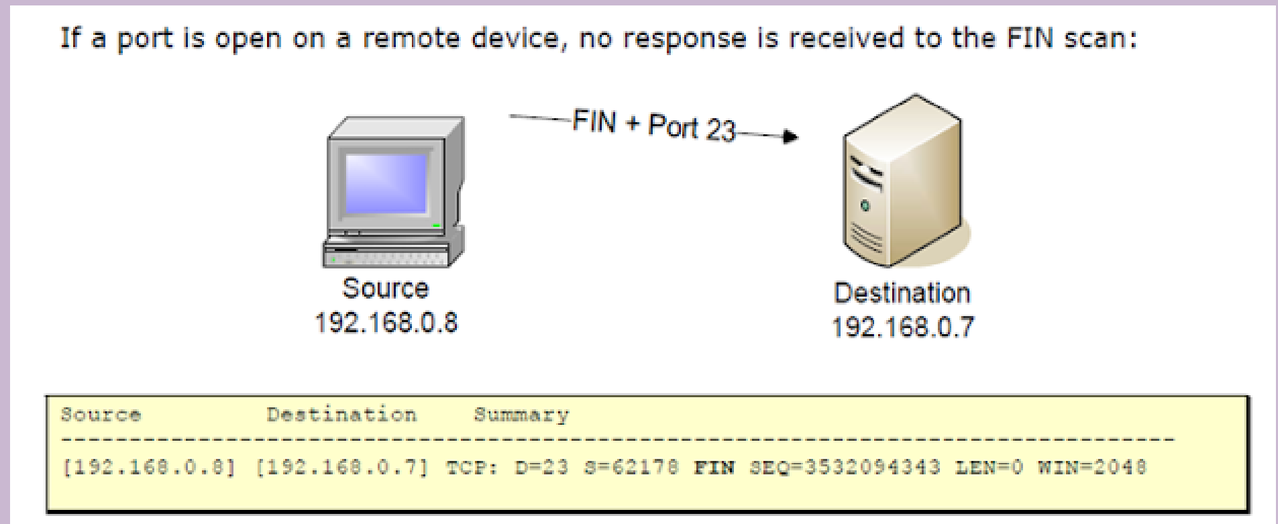


Full TCP scan

Es una técnica de exploración de puertos que consiste en enviar un paquete FIN a un puerto determinado, con lo cual deberíamos recibir un paquete de reset (RST) si dicho puerto esta cerrado. Esta técnica se aplica principalmente sobre implementaciones de pilas TCP/IP de sistemas Unix.

la comunicación entre un host A y B

- **El host A manda una petición FIN al host B**
- **Si Host B responde con una petición RST/ACK, el puerto esta cerrado**
- **Si host B no responde, posiblemente el puerto esta abierto.**



Stelth scan

son aquellos en los que las banderas de paquetes hacen que el sistema de destino responda sin tener una conexión completamente establecida . Los piratas informáticos utilizan el escaneo sigiloso para eludir el sistema de detección de intrusos (IDS), lo que lo convierte en una amenaza importante.

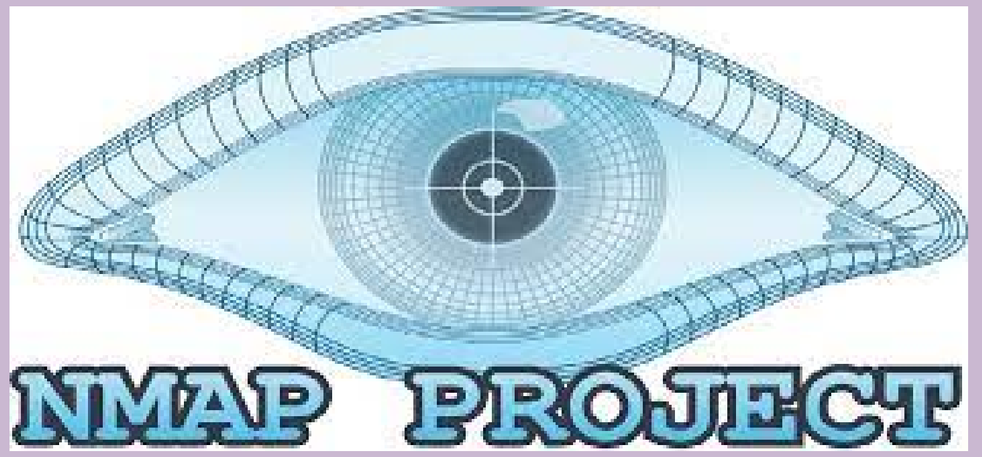
- **Escaneos FIN (terminados). Estos envían paquetes FIN con un conjunto de banderas. Si se devuelve un RST, el puerto se considera abierto; si no se recibe nada, se considera cerrado.**
- **Escaneos NULL. Estos no establecen ningún indicador en el paquete TCP. En otras palabras, el encabezado del indicador TCP se establece en 0 y los protocolos de respuesta son los mismos que los escaneos FIN.**
- **Escaneos de Navidad. Estos utilizan banderas FIN, URG (urgente) y PSH (push), que iluminan el paquete como un árbol de Navidad. Si se recibe un RST empaquetado, el puerto se considera cerrado; ninguna respuesta indica un estado abierto o filtrado. Un error ICMP inalcanzable también indica un puerto filtrado.**

Fingerprintig

es una técnica que permite obtener información de una persona o empresa a través de los sistemas informáticos. Muchas entidades buscan monitorizar la actividad de los usuarios, algunas para realizar un mejor marketing con publicidad personalizada, otras para detectar posibles actividades fraudulentas o delictivas en Internet. A continuación, te ofrecemos una lista de este tipo de actividades que ponen en riesgo tu ciberseguridad y la de tu organización

Zenmap

Es la interfaz gráfica de usuario oficial de Nmap Security Scanner. Es una aplicación multiplataforma (Linux, Windows, Mac OS X, BSD, etc.) gratuita y de código abierto que tiene como objetivo hacer que Nmap sea fácil de usar para los principiantes al tiempo que proporciona funciones avanzadas para usuarios experimentados de Nmap. Los escaneos que se usan con frecuencia se pueden guardar como perfiles para que sean fáciles de ejecutar repetidamente. Un creador de comandos permite la creación interactiva de líneas de comandos de Nmap. Los resultados del escaneo se pueden guardar y ver más tarde. Los resultados de escaneo guardados se pueden comparar entre sí para ver en qué se diferencian. Los resultados de los escaneos recientes se almacenan en una base de datos de búsqueda.



Análisis traceroute

se ejecuta en la consola de símbolo de sistema en los sistemas operativos Windows. Gracias a este comando, podremos seguir la pista a los paquetes que vienen desde un host. Cuando ejecutamos el comando «Tracert» obtenemos una estadística de la latencia de red de esos paquetes, lo que es una estimación de la distancia (en saltos) a la que están los extremos de la comunicación.

TRACEROUTE

Aunque Windows lo denomina «tracert», en sistemas operativos basados en UNIX, el nombre de esta herramienta que viene por defecto se denomina «traceroute». La herramienta traceroute es exactamente la misma que el tracert, pero se denomina de otra forma, aunque internamente puede hacer uso de diferentes protocolos, ya que en algunos sistemas operativos se hace uso del protocolo ICMP Echo Request/reply, y en otros de hace uso de mensajes UDP directamente para comprobar cuántos saltos hay de un equipo a otro.

o