Nmap

**Escaneo silencioso:**

**-sS:** Este es el escaneo de tipo "SYN" o "half-open". En este tipo de escaneo, Nmap no completa el proceso de conexión TCP, lo que lo hace menos probable que sea detectado por los sistemas objetivo.

**-sT:** Este es el escaneo TCP "connect". En este tipo de escaneo, Nmap completa la conexión TCP con el sistema objetivo. Aunque es más "ruidoso" que el escaneo SYN, sigue siendo bastante silencioso en comparación con otros tipos de escaneos.

**-Pn:** Esta opción evita la detección de hosts y se asume que todos los hosts están activos. Esto puede evitar la necesidad de enviar paquetes de ping y potencialmente reducir la visibilidad del escaneo.

**-n:** Esta opción evita la resolución de DNS, lo que puede acelerar el escaneo y reducir la cantidad de tráfico generado.

**-T0 a -T5:** Estas son opciones de tiempo de espera que controlan la velocidad del escaneo. En este caso usamos un -T0

**--min-rate y --max-rate:** Estas opciones permiten controlar la velocidad de envío de paquetes, lo que puede ayudar a ajustar el nivel de "ruido" generado por el escaneo.

**-p-:** Escanea todos los puertos, lo que puede aumentar la cantidad de tráfico pero no necesariamente aumenta el ruido, ya que no se realizan acciones adicionales en los puertos.

**--min-rate 5000:** Establece una tasa mínima de paquetes por segundo, lo que podría acelerar el escaneo sin generar demasiado ruido.

**Escaneo más silencioso posible:**

**nmap -sS -T0 -p- -Pn -n IP**

**-sS:** Se utiliza un escaneo de tipo SYN, que es más silencioso ya que no completa la conexión TCP.

**-T0:** Se establece el nivel de tiempo de espera en el mínimo, lo que ralentiza el escaneo y reduce la probabilidad de ser detectado.

**-p-:** Escanea todos los puertos, lo que podría generar más tráfico pero no necesariamente aumenta el ruido, ya que no se realizan acciones adicionales en los puertos.

**-Pn:** Se evita la detección de hosts, asumiendo que todos los hosts están activos.

**-n:** Se evita la resolución de DNS para reducir la cantidad de tráfico generado y acelerar el escaneo.

Este escaneo es muy discreto ya que utiliza un escaneo SYN, minimiza el tiempo de espera y evita actividades adicionales que podrían llamar la atención de los sistemas objetivo.

**Escaneo medio:**

**nmap -sS -sC -sV -p- -n -Pn -open -open -vvv --min-rate 5000 192.168.0.15**

**-sS:** Utiliza un escaneo de tipo SYN, que es más silencioso ya que no completa la conexión TCP.

**-sC:** Activa scripts de escaneo predeterminados, lo que puede agregar un poco de ruido al escaneo.

**-sV:** Realiza la detección de versiones de servicios, lo que puede generar solicitudes adicionales y aumentar ligeramente el nivel de ruido.

**-p-:** Escanea todos los puertos, lo que puede aumentar la cantidad de tráfico pero no necesariamente aumenta el ruido, ya que no se realizan acciones adicionales en los puertos.

**-n:** Evita la resolución de DNS, lo que puede reducir la cantidad de tráfico generado y acelerar el escaneo.

**-Pn**: Evita la detección de hosts y asume que todos los hosts están activos, lo que puede reducir la visibilidad del escaneo.

**-open:** Filtra los resultados para mostrar solo los hosts con puertos abiertos, lo que puede reducir la cantidad de datos de salida, pero no afecta directamente el nivel de ruido.

-vvv: Establece un nivel de verbosidad muy alto, lo que significa que se mostrará una cantidad significativa de información sobre el progreso del escaneo. Esto no afecta directamente el nivel de ruido del escaneo, pero puede hacer que la salida sea más notable.

--min-rate 5000: Establece una tasa mínima de paquetes por segundo, lo que podría acelerar el escaneo sin generar demasiado ruido.

**Escaneo Ruidoso:**

**nmap -sS -sV -sC -p- -T5 -v -A -PN -d --script-args=unsafe=1 IP**

**-sS:** Utiliza un escaneo de tipo SYN.

**-sV:** Realiza la detección de versiones de servicios.

**-sC:** Activa scripts de escaneo predeterminados.

**-p-:** Escanea todos los puertos.

**-T5:** Establece el nivel de tiempo de espera en el máximo, lo que acelera el escaneo pero aumenta la probabilidad de ser detectado.

**-v:** Establece un nivel de verbosidad alto para obtener una salida detallada.

**-A:** Activa la detección de sistemas operativos y otros detalles avanzados.

**-PN:** Se omite la detección de hosts, asumiendo que todos los hosts están activos.

**-d:** Activa el modo depuración para mostrar detalles adicionales sobre el escaneo.

**--script-args=unsafe=1**: Activa scripts que pueden ser considerados más intrusivos o "peligrosos".

Este escaneo es muy ruidoso porque activa la detección de versiones de servicios, scripts de escaneo, y detección de sistemas operativos, además de establecer un tiempo de espera muy corto y un alto nivel de verbosidad.

-T0: Parada repentina. Este modo ralentiza Nmap a su máximo. Establece un tiempo entre los paquetes extremadamente largo, lo que hace que el escaneo sea muy lento y sigiloso. Es útil cuando la discreción es una prioridad máxima.

-T1: Sigiloso. Un poco más rápido que -T0, pero aún así bastante lento. Adecuado para escenarios donde se necesita un escaneo muy silencioso y no se necesita velocidad.

-T2: Moderado. Este es el valor predeterminado si no se especifica ninguno. Proporciona un equilibrio entre velocidad y sigilo, lo que lo hace útil en la mayoría de los escenarios.

-T3: Ágil. Un poco más rápido que el modo predeterminado, pero aún razonablemente discreto. Adecuado para escaneos en redes donde la velocidad es importante pero la discreción sigue siendo una preocupación.

-T4: Rápido. Mucho más rápido que los modos anteriores, lo que lo hace más ruidoso. Adecuado para escaneos en redes donde la velocidad es prioritaria y el sigilo no es una preocupación importante.

-T5: Insensato. El más rápido y menos sigiloso de todos los modos. Este modo genera una gran cantidad de tráfico y es más probable que sea detectado por dispositivos de seguridad. Adecuado para escenarios donde la velocidad es crítica y no importa la discreción.