Nmap - Control de tiempo y rendimiento

Una de las prioridades durante el desarrollo de Nmap ha sido siempre el rendimiento. Un sondeo por omisión (nmap <nombre_de_sistema>) de cualquier sistema en una red local tarda un quinto de segundo. Esto es menos que el tiempo que uno tarda en parpadear, pero se va sumando al tiempo que se tarda cuando se realiza un sondeo sobre decenas o centenares o miles de equipos.

Además, ciertas opciones de sondeo como puedan ser el sondeo UDP y la detección de versiones pueden incrementar los tiempos de sondeos de forma sustancial. También pueden afectar a este tiempo algunas configuraciones de sistemas cortafuegos, especialmente cuando implementan limitaciones a la tasa de respuestas.

Nmap tiene muchas opciones avanzadas para controlar de una forma granular determinados aspectos que afectan al rendimiento.

Además de estas opciones granulares (que no vamos a tratar en este documento), Nmap permite utilizar plantillas predefinidas, que definen varias de estas opciones, de acuerdo al efecto deseado.

-T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane>

Nmap ofrece seis plantillas de tiempos. Podemos especificar cualquiera de éstas con la opción -T seguido de un número o su nombre. Los nombre de las plantillas son:

paranoico (0), sigiloso (1), amable (2), normal (3), agresivo (4) y loco (5)

(respectivamente "paranoid", "sneaky", "polite", "normal", "aggressive" e "insane").

Las primeras dos se utilizan para evadir IDS. El modo amable reduce el sondeo para que éste utiliza menos ancho de banda y menos recursos de los sistemas analizados. El modo normal es el valor por omisión, así que la opción -T3 no hace nada realmente. El modo agresivo hace que los sondeos sean más rápidos al asumir que está en una red razonablemente más rápida y fiable. En modo loco asume que está en una red extraordinariamente rápida o que está dispuesto a sacrificar fiabilidad por velocidad.

Mientras que puede ser útil evitar alarmas de IDS con -T0 y -T1, éste tardará mucho más tiempo para sondear miles de sistemas o puertos.

Los efectos principales del uso de T0 es la serialización de los sondeos de forma que sólo se

sondea un puerto cada vez, y se espera cinco minutos antes de enviar cada sonda.

Las opciones T1 y T2 son similares pero sólo esperan 15 y 0.4 segundos entre sondas, respectivamente. El comportamiento por omisión de Nmap es T3, que incluye sondeos en paralelo.

Autor: Fabian Martinez Portantier

Fuentes:

- http://incibe.es
- http://seguridadyredes.wordpress.com
- http://nmap.org