Nmap - Evasión de Firewalls e IDS/IPS

Los filtros de red como los cortafuegos pueden hacer muy difícil el análisis de una red. Nmap ofrece varias funcionalidades para ayudar a entender estas redes complejas, y que también sirven para verificar que los filtros funcionan como se espera de ellos. Incluso tiene mecanismos para saltarse las defensas que no hayan sido implementadas del todo correctamente.

Las compañías, además de restringir la actividad de red, están monitorizando cada vez más el tráfico con sistemas de detección o prevención de intrusos (IDS/IPS). Todos los IDS/IPS principales vienen preinstalados con reglas diseñadas para detectar sondeos de Nmap porque, a veces, se realizan sondeos previos a un ataque.

No hay ninguna herramienta mágica (u opción de Nmap) que permita detectar y evitar cortafuegos y sistemas IDS. Esto requiere habilidad y experiencia.

-f ; --mtu

La opción -f hace que el sondeo solicitado (incluyendo los sondeos ping) utilicen paquetes IP fragmentados pequeños. La idea es dividir la cabecera del paquete TCP entre varios paquetes para hacer más difícil que los filtros de paquetes, sistemas de detección de intrusos y otros filtros detecten lo que se está haciendo.

Especificando esta opción una sola vez Nmap dividirá los paquetes en ocho bytes o menos después de la cabecera de IP.

De esta forma, una cabecera TCP de veinte bytes se dividiría en 3 paquetes. Dos con ocho bytes de cabecera TCP y uno con los últimos cuatro. Obviamente, cada fragmento tiene su propia cabecera IP. Especificando la opción -f otra vez podemos utilizar fragmentos de dieciséis bytes (reduciendo la cantidad de fragmentos).

O podemos especificar un propio tamaño con la opción --mtu. No debemos utilizar la opción -f si se utiliza --mtu. El tamaño debe ser múltiplo de ocho. Aunque la utilización de paquetes fragmentados no nos ayudará a saltar los filtros de paquetes y cortafuegos que encolen todos los fragmentos IP (como cuando se utiliza la opción CONFIG_IP_ALWAYS_DEFRAG del núcleo de Linux), algunas redes no pueden tolerar la pérdida de rendimiento que esto produce y deshabilitan esa opción.

Otros no pueden habilitar esta opción porque los fragmentos pueden tomar distintas rutas para entrar en su red.

-D <s1 [,s2],[ME]...>

Realiza un sondeo con señuelos. Esto hace creer que el/los equipo/s que utilice como señuelos están también haciendo un sondeo de la red. De esta manera sus IDS pueden llegar a informar de que se están realizando de 5 a 10 sondeos de puertos desde distintas direcciones IP, pero no sabrán qué dirección IP está realizando el análisis y cuáles son

señuelos inocentes.

Aunque esta técnica puede vencerse mediante el seguimiento del camino de los routers, descarte de respuesta y otros mecanismos activos, generalmente es una técnica efectiva para esconder la dirección IP.

Se debe separar cada equipo de distracción mediante comas, y podemos utilizar ME ("YO") como uno de los señuelos para representar la posición de la verdadera dirección IP.

Si ponemos ME en la sexta posición o superior es probable que algunos detectores de sondeos de puertos habituales ni siquiera muestren nuestra dirección IP. Si no utilizamos ME, Nmap lo pondrá en una posición aleatoria.

Tengamos en cuenta que los equipos que utilicemos como distracción deberían estar conectados o puede que accidentalmente causemos un ataque de inundación SYN a los objetivos.

Además, sería bastante sencillo determinar qué equipo está realmente haciendo el sondeo si sólo uno está disponible en la red. Puede que queramos utilizar direcciones IP en lugar de nombres (de manera que no aparezca en los registros del servidor de nombres de los sistemas utilizados como señuelo).

Se utilizan los señuelos tanto para el sondeo de ping inicial (si se utiliza ICMP, SYN, ACK, o cualquier otro) como durante la fase de sondeo. También se utilizan los señuelos durante la detección de sistema operativo (-O). Los señuelos no funcionarán con la detección de versión o el sondeo TCP connect().

Vale la pena tener en cuenta que utilizar demasiados señuelos puede ralentizar el sondeo y potencialmente hacerlo menos exacto. Además, algunos proveedores de acceso a Internet filtran los paquetes falsificados, aunque hay muchos que no lo hacen.

Autor: Fabian Martinez Portantier

Fuentes:

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