Estados de puertos

Para comprender mejor cómo funcionan los métodos de escaneo es importante conocer primero los posibles estados de un puerto.

Las definiciones de los estados abierto, filtrado y cerrado son comunes entre muchas herramientas de escaneo, pero dependiendo del aplicativo pueden usarse diferentes nombres para referirse a un mismo estado. Por consiguiente, nos basaremos en las definiciones de estados de puertos de la herramienta de escaneo más popular: *NMAP*.

Abierto: un puerto en este estado está disponible y escuchando por conexiones hacia el servicio asociado en dicho puerto.
Por ejemplo, un webserver público podría tener abiertos los puertos TCP/80 (HTTP), TCP/443 (HTTPS), UDP/53 (DNS) y
otros más.

Cerrado: por el contrario, un puerto cerrado, aunque es accesible, no tiene una aplicación o servicio asociado que responda a solicitudes de conexión.

Filtrado: un puerto filtrado no es posible de ser accedido porque existe un dispositivo filtrador de paquetes de por medio que impide al escáner determinar si dicho puerto está abierto o cerrado. El dispositivo intermedio puede ser un router con ACL's implementadas o bien un firewall.

No-filtrado: un puerto en este estado es accesible pero no puede determinarse a ciencia cierta si está abierto o cerrado. Este estado es específico de una técnica de escaneo descrita más adelante en esta misma sección denominada escaneo ACK.

Abierto | Filtrado: este es un estado ambiguo en el cual el escáner no pudo determinar si el puerto se encuentra abierto o filtrado y es factible de obtenerse cuando se usa una técnica de escaneo en la cual un puerto abierto puede no responder.

Cerrado | Filtrado: se da cuando el escáner no puede concluir si el puerto está cerrado o filtrado.

En los casos en que el estado de un puerto no ha podido determinarse con seguridad usando una sola técnica de escaneo, lo recomendable es utilizar uno o varios métodos adicionales que nos permitan sacar una conclusión más firme.

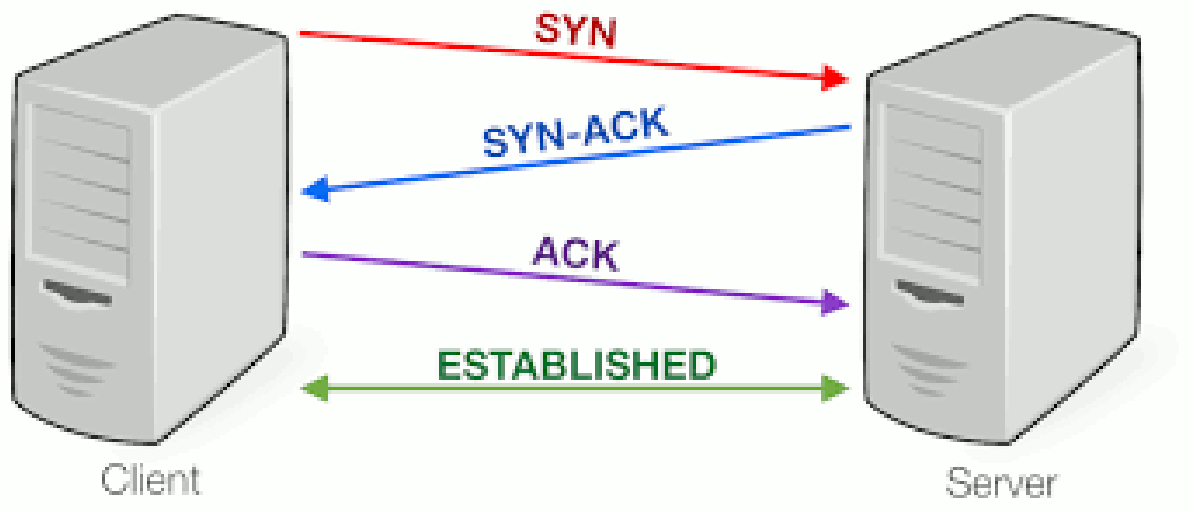
Técnicas de escaneo

Métodos de escaneo más utilizados:

Escaneo SYN o Half-Open (medio abierto)

Este método es utilizado para identificar puertos que tienen servicios asociados que usan como protocolo de transporte a TCP. Como recordarán el protocolo TCP es orientado a conexión y utiliza un "apretón de manos de 3 vías" (*three-way handshake*) para establecer una sesión.

Dicha secuencia es como se ilustra en la Figura:



Esta técnica se basa en el envío de una solicitud de sincronismo (SYN) a la víctima y esperar a recibir como

respuesta un sincronismo y un acuse de recibo (SYN + ACK), pero sin completar la conexión, es decir sin enviar el acuse de recibo final. Debido a esto se le llama escaneo SYN o Half-Open (medio abierto), por el hecho que de la conexión no se completa quedando en estado *embriónico*.
Si se recibe el SYN + ACK el puerto se determina como abierto, si se recibe un reset (RST) se identifica como cerrado y si no se recibe respuesta se coloca como filtrado.
La razón para hacer esto es que, en la mayoría de los sistemas operativos de servidores, estaciones y dispositivos de comunicaciones como firewalls y routers, las conexiones embriónicas se mantienen en memoria durante un tiempo, pero si no se completan simplemente se eliminan y no se registran en los logs de eventos, pasando desapercibidas para los administradores y para los sistemas de prevención de intrusos.
Por este motivo esta técnica se suele utilizar en los escaneos iniciales con el objetivo de no ser detectados.

Escaneo Full o Connect-Scan

Este es otro tipo de escaneo TCP, pero en esta ocasión se completa la conexión con el objetivo. Si bien este método disminuye los falsos positivos, toma más tiempo en ejecutarse y adicionalmente es muy probable que quede un registro de nuestras conexiones en los logs de eventos de los hosts remotos, lo que podría llamar la atención de un sistema de prevención de intrusos (IPS).

Escaneo UDP

Como su nombre indica esta es una técnica usada para el protocolo de transporte UDP. El escaneo consiste en el envío de un paquete UDP a los puertos de los hosts remotos en espera de contestación. Si la respuesta es un mensaje *ICMP port-unreacheable* el puerto es declarado como cerrado; si se recibe otro tipo de error ICMP (tipo 3, códigos 1, 2, 9, 10, ó 13) se coloca como filtrado y si retorna un segmento UDP, entonces el puerto se marca como abierto.

Escaneos especiales: Null-Scan, Fin-Scan, XMAS-Scan

En estos escaneos se manipulan las banderas de la cabecera del segmento TCP para determinar si un puerto remoto está abierto o cerrado. Lo que cambian son las banderas, pero el concepto es el mismo: dado que en todos ellos el segmento inicial no es la usual solicitud de sincronismo (SYN), la respuesta dependerá de la implementación de la pila de TCP/IP del sistema operativo del host remoto.

Null-Scan: todas las banderas apagadas

Fin-Scan: bandera FIN encendida

XMAS-Scan: banderas FIN, URG y PSH encendidas

De acuerdo al *RFC 793*, si un puerto está cerrado la recepción de un segmento que no contenga la bandera reset (RST) ocasionará que el sistema responda con un reset. Por lo

tanto, si se recibe un RST el puerto se marca como cerrado y si no se recibe respuesta se coloca como abierto | filtrado. Pero no todos los fabricantes implementan el *RFC 793* al pie de la letra en las pilas TCP/IP de sus sistemas operativos, por ejemplo *Windows*, versiones del *Cisco IOS*, entre otros, responden con un RST a este tipo de pruebas inclusive si el puerto está abierto, por lo cual se recomienda complementar este tipo de escaneo con otros adicionales para mitigar los falsos negativos.

Escaneo ACK

A diferencia de los métodos previos, el propósito del escaneo ACK no es determinar si un puerto está abierto o cerrado sino comprobar si existe o no un firewall de por medio.
La lógica detrás de esta técnica consiste en enviar un segmento con solo la bandera ACK encendida al puerto destino de la víctima, si la respuesta es un RST esto implica que el puerto no está filtrado, es decir que es accesible independientemente de si el puerto está abierto o cerrado, luego, se coloca como no-filtrado (*unfiltered*), mientras que aquellos puertos de los que no se reciba respuesta o que respondan con mensajes de error ICMP se marcan como filtrados.

Escáner de puertos: *NMAP*

NMAP es sin duda el escáner de puertos más popular entre los profesionales de redes y seguridad informática, en parte por su facilidad de uso, pero principalmente debido a su versatilidad para escanear.

Con *NMAP* se pueden aplicar las técnicas de escaneo descritas anteriormente y otras adicionales que pueden revisarse en la *Guía de Referencia* en el sitio web oficial del proyecto, **http://www.nmap.org/**.

Otra de las ventajas de este escáner es la posibilidad de ejecutarlo desde la línea de comandos además de la interfaz gráfica. De hecho, inicialmente se desarrolló para *Linux* y se ejecutaba exclusivamente en un *shell*, pero posteriormente se agregó la interfaz gráfica *Zenmap* y se portó a la plataforma *Windows*.

Veamos algunas de las opciones más utilizadas de *NMAP*:

Sintaxis: nmap [tipo(s)_de_escaneo] [opciones] {red|host_objetivo}

Opciones:

-sn : ping scan

-sS : syn/half scan

-sT : tcp/connect scan

-sA : ack scan

-sN : null scan

-sU : udp scan

-sF : fin scan

-sX : xmas scan

-sV : detección de versión de servicios

-O : detección de sistema operativo

-T<0-5>: temporizador, el valor más alto es más rápido

-v : salida detallada

Para las pruebas, puede utilizarse el sitio scanme.nmap.org