Definición de Estrategias para Protegerse de los Ataques de Denegación de Servicio TCP SYN

Contenido

Abstracto

Hay un potencial ataque de negación de servicio en los Proveedores de servicios de Internet (IPS) que apuntan a los dispositivos de red.

- **Ataque TCP SYN** Un remitente transmite un volumen de conexiones que no se pueden completar. Esto provoca que las colas de conexión se llenen y denieguen el servicio para usuarios TCP legítimos.

Este documento incluye una descripción técnica sobre cómo se producen los ataques TCP SYN potenciales y sobre los métodos recomendados para utilizar el software Cisco IOS a fin de defenderse de éstos.

Nota: El software Cisco IOS 11.3 tiene una función para prevenir activamente ataques de denegación de servicio TCP. Esta función se describe en el documento Configuración de TCP Intercept (Prevención de Ataques de Negación de Servicio).

Prerequisites

Requirements

No hay requisitos previos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Descripción de problemas

El ataque TCP SYN

Cuando se inicia una conexión TCP normal, un host de destino recibe un paquete SYN (sincronización/inicio) desde un host de origen y envía de regreso un SYN ACK (sincronización de reconocimiento). El host de destino debe escuchar un ACK (reconocimiento) de SYN ACK antes de establecer la conexión. Esto se conoce como el "intercambio de señales de tres vías TCP".

Mientras se espera el ACK en el ACK SYN, una cola de conexión de tamaño finito en el host de destino realiza el seguimiento de las conexiones que están por finalizar. Esta cola normalmente se vacía rápidamente ya que se espera que el ACK llegue unos milisegundos después de SYN ACK.

El ataque TCP SYN explota este diseño haciendo que un host de origen atacante genere paquetes TCP SYN con direcciones de origen aleatorias hacia un host víctima. El host víctima de destino envía un SYN ACK de regreso la dirección de origen aleatoria y le agrega una entrada a la cola de conexión. Como el SYN ACK está destinado a un host incorrecto o inexistente, la última parte del “contacto de tres direcciones” nunca se completa y la entrada permanece en la cola de conexión hasta que se agote un temporizador; por lo general, alrededor de un minuto. Al generar paquetes SYN TCP falsos de direcciones IP aleatorias a una velocidad rápida, es posible llenar la cola de conexión y denegar los servicios TCP (como correo electrónico, transferencia de archivos o WWW) a usuarios legítimos.

No hay una manera fácil de rastrear el autor del ataque porque la dirección IP del origen está falsificada.

Las manifestaciones externas del problema incluyen la incapacidad de obtener correo electrónico, la incapacidad de aceptar conexiones a WWW o servicios FTP, o un gran número de conexiones TCP en su host en el estado SYN_RCVD.

Defensa contra ataques en dispositivos de red

Dispositivos detrás de Firewalls

EL ataque TCP SYN se caracteriza por una entrada de paquetes SYN desde direcciones IP de origen aleatorias. Cualquier dispositivo detrás de un firewall que detiene los paquetes SYN entrantes ya está protegido de este modo de ataque y no se necesita ninguna otra acción. Algunos ejemplos de firewalls incluyen un firewall Cisco Private Internet Exchange (PIX) o un router Cisco configurado con listas de acceso. Para obtener ejemplos de cómo configurar listas de acceso en un router Cisco, consulte el documento Aumento de la seguridad en redes IP.

Dispositivos que ofrecen servicios disponibles de manera pública (servidores de correo, servidores Web públicos)

La prevención de los ataques SYN en dispositivos detrás de un firewall desde direcciones IP aleatorias es relativamente simple, ya que puede usar las listas de acceso para limitar de manera explícita el acceso entrante a unas pocas direcciones IP selectas. Sin embargo, en el caso de un servidor web público o un servidor de correo que se encuentra frente a Internet, no hay forma de determinar qué direcciones IP de origen entrantes son amigables y cuáles son poco amigables. Por lo tanto, no existe una defensa clara contra el ataque de direcciones IP aleatorias. Hay varias opciones para los hosts:

- Aumente el tamaño de la cola de conexión (cola SYN ACK).
- Reduzca el tiempo de espera para el intercambio de señales de tres direcciones.
- Emplee parches de software del proveedor para detectar y evitar el problema (si están disponibles).

Debe ponerse en contacto con su proveedor de host para ver si han creado parches específicos para hacer frente al ataque TCP SYN ACK.

Nota: El filtrado de direcciones IP en el servidor no es efectivo, ya que un atacante puede variar su dirección IP, y la dirección puede o no ser la misma que la de un host legítimo.

Cómo evitar que una red albergue un ataque sin intención

Dado que un mecanismo primario de este ataque de rechazo del servicio es la generación de tráfico originado en direcciones IP aleatorias, se recomienda el filtrado del tráfico destinado a Internet. El concepto básico es descartar paquetes con direcciones IP de origen no válidas a medida que ingresan a Internet. Esto no evita un ataque de denegación de servicio en su red, pero ayudará a que la parte atacada descarte su ubicación como el origen del atacante. Además, hace que su red sea menos atractiva como base para esta clase de ataques.

Cómo evitar la transmisión de direcciones IP no válidas

Al filtrar paquetes en los routers que conectan la red a Internet, puede permitir que únicamente los paquetes con direcciones IP de origen válidas abandonen la red y lleguen a Internet.

Por ejemplo, si la red está formada por la red 172.16.0.0 y el router se conecta al ISP mediante una interfaz serial 0/1, puede aplicar la lista de acceso de la siguiente manera:

```
access-list 111 permit ip 172.16.0.0 0.0.255.255 any
access-list 111 deny ip any any log

interface serial 0/1
ip access-group 111 out
```

Nota: La última línea de la lista de acceso determina si hay tráfico con una dirección de origen no válida entrando en Internet. No es crucial tener esta línea, pero ayudará a localizar el origen de posibles ataques.

Cómo evitar la recepción de direcciones IP no válidas

Para los ISP que proporcionan servicio a las redes finales, recomendamos encarecidamente la validación de los paquetes entrantes de sus clientes. Esto se logra usando filtros de paquete de entrada en los routers de borde.

Por ejemplo, si sus clientes tienen los siguientes números de red conectados al router a través de una interfaz serial denominada "serial 1/0", puede crear la siguiente lista de acceso:

```
The network numbers are 192.168.0.0 to 192.168.15.0, and 172.18.0.0.

access-list 111 permit ip 192.168.0.0 0.0.15.255 any
access-list 111 permit ip 172.18.0.0 0.0.255.255 any
access-list 111 deny ip any any log

interface serial 1/0
ip access-group 111 in
```

Nota: La última línea de la lista de acceso determina si hay tráfico con direcciones de origen no válidas que ingresen a Internet. No es crucial tener esta línea, pero ayudará a localizar el origen del posible ataque.

Este tema se ha tratado con cierto detalle en la lista de correo de NANOG [North American Network Operator1s Group]. Los archivos de la lista se encuentran en: http://www.merit.edu/mail.archives/nanog/index.html

Para obtener una descripción detallada del ataque de denegación de servicio TCP SYN y la suplantación de IP, consulte: http://www.cert.org/advisories/CA-1996-21.html

http://www.cert.org/advisories/CA-1995-01.html

Información Relacionada

- Soporte Técnico - Cisco Systems