Definición de las estrategias para proteger contra los establecimientos de rechazo del 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 pueda ser completado. 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 del Cisco IOS 11.3 tiene una característica para prevenir activamente los ataques de negación del servicio TCP. Esta característica se describe en el documento que configura la Intercepción de tráfico de TCP (prevenga los establecimientos de rechazo del servicio).

prerrequisitos

Requisitos

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. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). 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). La computadora principal de destino debe entonces oír un ACK (reconozca) del SYN ACK antes de que se establezca la conexión. Esto se refiere como la “entrada en contacto 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 vacia típicamente rápidamente puesto que se espera que llegue el ACK algunos milisegundos después del 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. Generando los falsos paquetes SYN TCP de los IP Addresses al azar a una velocidad tan rápida, es posible llenar la cola de conexión y negar los servicios TCP (tales como email, transferencia de archivos, o WWW) a los usuarios legítimos.

No hay forma sencilla de localizar al terminal original del ataque porque la dirección IP de la fuente se forja.

Las manifestaciones externas del problema incluyen la incapacidad para conseguir el email, la incapacidad para validar las conexiones al WWW o a los 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 pare los paquetes SYN entrantes se protege ya contra este modo de ataque y ninguna otra acción es necesario. Los ejemplos de los Firewall incluyen un Firewall del private internet exchange (PIX) de Cisco o a un router Cisco configurado con las Listas de acceso. Por ejemplos de cómo configurar las Listas de acceso en un router Cisco, refiera por favor a

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 de un mail server que hace frente al Internet, no hay manera de determinar que las direcciones de origen del IP entrante son cómodas y que son hostil. 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).
- Disminuya el descanso que espera la entrada en contacto de tres vías.
- Emplee las correcciones del software del proveedor para detectar y para evitar el problema (si está disponible).

Usted debe entrar en contacto a su vendedor del host para ver si han creado las correcciones específicas para dirigir el ataque TCP SYN ACK.

Nota: La filtración de los IP Addresses en el servidor es ineficaz puesto que un atacante puede variar su dirección IP, y el direccionamiento puede o no puede ser lo mismo que el 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 su red menos atractiva como base para esta clase de ataque.

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 su red consiste en la red 172.16.0.0, y su router conecta con su ISP usando una interfaz del serial 0/1, usted puede aplicar la lista de acceso como sigue:

```
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 que ingresa a 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 el servicio para terminar las redes, recomendamos altamente la validación del paquete entrante de sus clientes. Esto se logra usando filtros de paquete de entrada en los routers de borde.

Por ejemplo, si sus clientes tienen los network number siguientes conectados con su router vía una interfaz serial nombrada "serial 1/0", usted puede crear la lista de acceso siguiente:

```
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 existe algún tráfico con direcciones de origen inválidas que entran a Internet. No es crucial tener esta línea, pero ayudará a localizar el origen del posible ataque.

Este tema se ha discutido en un cierto detalle en la lista de correo del [North-american Network Operator1s Group] NANOG. Los archivos de listado se localizan en:
http://www.merit.edu/mail.archives/nanog/index.html

Para una descripción detallada del ataque de negación de servicio y del IP spoofing, vea:
http://www.cert.org/advisories/CA-1996-21.html

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

Información Relacionada

- Soporte Técnico - Cisco Systems