Caracterización y seguimiento de la inundación de paquetes usando routers de Cisco

Contenido

Introducción

Los ataques de rechazo de servicio (DoS) son frecuentes en Internet. El primer paso que se utiliza para responder a dicho ataque es descubrir exactamente qué clase de ataque es. La mayoría de los ataques DOS que se utilizan comúnmente están basados en inundaciones de paquetes de ancho de banda alto o en otras secuencias de paquetes repetitivas.

Los paquetes en muchos flujos de ataque de DoS se pueden aislar cuando se comparan con las entradas de la lista de acceso del software Cisco IOS®. Esto es valioso para filtrar los ataques. También es útil para el momento en que se caracterizan los ataques desconocidos y para el momento en que se rastrean los flujos de paquetes "suplantados" a sus fuentes reales.

Las funciones del router de Cisco tales como el registro de depuración y la contabilidad IP se pueden utilizar a veces con propósitos similares, especialmente ante ataques nuevos o inusuales. Sin embargo, con las versiones recientes del software Cisco IOS, las listas de acceso y el registro de la lista de acceso son las funciones principales para caracterizar y rastrear ataques comunes.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

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

Convenciones

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Los ataques DoS más comunes

Es posible realizar una amplia variedad de ataques de DoS. Incluso si ignora los ataques que utilizan errores de software para apagar sistemas con relativamente poco tráfico, el hecho es que cualquier paquete IP que se pueda enviar a través de la red se puede utilizar para ejecutar un ataque de DoS inundable. Cuando está siendo atacado, siempre debe considerar la posibilidad de que lo que ve es algo que no cae en las categorías usuales.

Sujeto a esa advertencia, también es bueno recordar que muchos ataques son similares. Los atacantes eligen las vulnerabilidades comunes porque son especialmente eficaces, especialmente difíciles de rastrear o porque hay herramientas disponibles. Muchos atacantes de DoS carecen de la habilidad o motivación para crear sus propias herramientas y utilizar los programas que se encuentran en Internet. Estas herramientas tienden a estar o no de moda.

Cuando se escribió este artículo, en julio de 1999, la mayoría de las solicitudes de los clientes para obtener la asistencia de Cisco comprendían el ataque “smurf”. Este ataque tiene dos víctimas: un "objetivo final" y un "reflector". El atacante envía una secuencia de estímulo de peticiones de eco ICMP ("pings") a la dirección de difusión de la subred reflectora. Las direcciones de origen de estos paquetes se falsifican para ser la dirección del destino final. Para cada paquete enviado por el atacante, muchos hosts en la subred reflectora responden. Esto inunda el objetivo final y desperdicia ancho de banda para ambas víctimas.

Un ataque similar denominado "fraggle", utiliza anuncios directos de la misma manera, pero usa solicitudes de eco UDP en lugar de las solicitudes de eco del protocolo de mensajes de control de Internet (ICMP). El ataque Fraggle usualmente logra un menor factor de amplificación que el ataque Smurf, y es mucho menos popular.

Los ataques de Smurf generalmente se notan porque un link de red se sobrecarga. Una descripción completa de estos ataques, y de las medidas de defensa, está en la página Información de Ataques de Negación de Servicio .

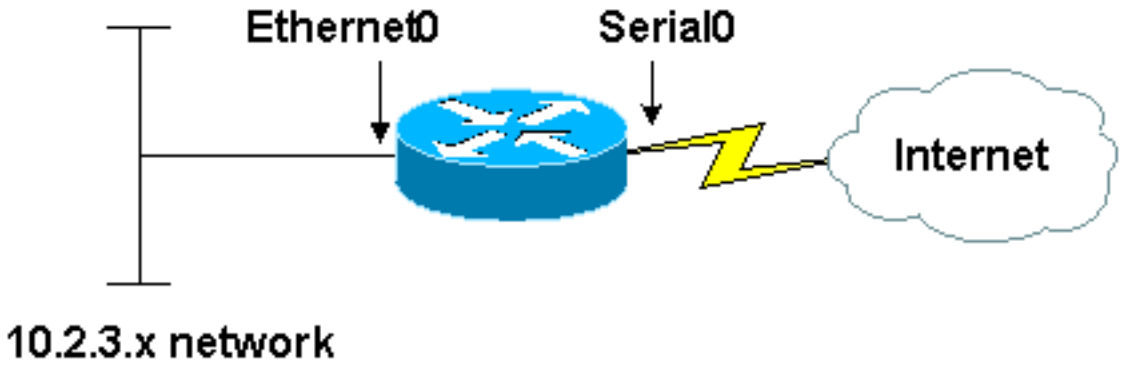
Otro ataque común es la inundación SYN en la que una máquina de destino es inundada con solicitudes de conexión TCP. Las direcciones de origen y los puertos TCP de origen de los paquetes de solicitud de conexión se aleatorizan. El propósito es obligar al host de destino a mantener la información de estado para muchas conexiones que nunca se completan.

Por lo general, se observan ataques de inundación SYN debido a que el host de destino (comúnmente un servidor HTTP o SMTP) se vuelve extremadamente lento, falla o se cuelga. También es posible que el tráfico que regresa del host de destino cause problemas en los routers. Esto se debe a que este tráfico de retorno va a las direcciones de origen aleatorizadas de los paquetes originales, carece de las propiedades de la localidad del tráfico IP "real" y puede desbordar las memorias caché de ruta. En los routers Cisco, este problema a menudo se manifiesta en el router que carece de memoria.

Juntas, las inundaciones smurf y SYN atacan la cuenta en la mayoría de los casos de inundación DoS que registra Cisco; por lo tanto, su rápida detección resulta esencial. Ambos ataques (así como algunos ataques de "segundo nivel", como inundaciones de ping) se reconocen fácilmente cuando se utilizan las listas de acceso de Cisco.

Lista de acceso de caracterización DoS

Imagine un router con dos interfaces. Ethernet 0 se conecta a una LAN interna en un ISP pequeño o empresarial. Serial 0 permite la conexión a Internet a través de ISP ascendente. La velocidad de paquetes de entrada en la serie 0 se "fija" al ancho de banda del link completo y los hosts en la LAN se ejecutan lentamente, se bloquean, se cuelgan o muestran otros signos de un ataque de DoS. El pequeño sitio en el que se conecta el router no tiene analizador de red y las personas de ahí tienen poca o ninguna experiencia en leer rastros de analizador incluso si los rastros están disponibles.



Ahora, suponga que aplica una lista de acceso como muestra este resultado:

```
access-list 169 permit icmp any any echo
access-list 169 permit icmp any any echo-reply
access-list 169 permit udp any any eq echo
access-list 169 permit udp any eq echo any
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
access-list 169 permit ip any any

interface serial 0
ip access-group 169 in
```

Esta lista no filtra ningún tráfico en absoluto; todas las entradas son permisos. Sin embargo, dado que categoriza paquetes de manera útil, la lista se puede utilizar tentativamente para diagnosticar los tres tipos de ataques: smurf, SYN inunda y fraggle.

Destino final de smurf

Si ejecuta el comando **show access-list**, verá un resultado similar al siguiente:

```
Extended IP access list 169
    permit icmp any any echo (2 matches)
    permit icmp any any echo-reply (21374 matches)
    permit udp any any eq echo
    permit udp any eq echo any
    permit tcp any any established (150 matches)
    permit tcp any any (15 matches)
    permit ip any any (45 matches)
```

La mayor parte del tráfico que llega a la interfaz serial consiste en paquetes de respuesta de eco ICMP. Esta es probablemente la firma de un ataque smurf, y nuestro sitio es el objetivo final, más que el reflector. Puede recopilar más información sobre el ataque al revisar la lista de acceso, como muestra este resultado:

```
interface serial 0
no ip access-group 169 in

no access-list 169
access-list 169 permit icmp any any echo
access-list 169 permit icmp any any echo-reply log-input
access-list 169 permit udp any any eq echo
access-list 169 permit udp any eq echo any
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
access-list 169 permit ip any any

interface serial 0
ip access-group 169 in
```

Aquí, el cambio corresponde a que se agrega la palabra clave de entrada de registro a la entrada de lista de acceso que coincide con el tráfico sospechoso. (Las versiones anteriores a 11.2 del software del IOS de Cisco carecen de esta palabra clave. Utilice la palabra clave "**log**" en su lugar). Esto hace que el router registre información sobre los paquetes que coinciden con la entrada de la lista. Si asume que **logging buffered** está configurado, puede ver los mensajes que resultan con el comando **show log** (puede llevar un tiempo que los mensajes se acumulen debido a la limitación de velocidad). Los mensajes aparecen de forma similar a este resultado:

```
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.142
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.113
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.72
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.154
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.15
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.142
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.47
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
```

```
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.35
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.113
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.59
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.82
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.56
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.84
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.47
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.45.35
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet

%SEC-6-IPACCESSLOGDP: list 169 denied icmp 192.168.212.15
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
%SEC-6-IPACCESSLOGDP: list 169 denied icmp 172.16.132.33
(Serial0 *HDLC*) -> 10.2.3.7 (0/0), 1 packet
```

Las direcciones de origen de los paquetes de respuesta de eco se agrupan en los prefijos de dirección 192.168.212.0/24, 192.168.45.0/24 y 172.16.132.0/24. (Las direcciones privadas de las redes 192.168.x.x y 172.16.x.x no estarían en Internet; esta es una ilustración de laboratorio.) Esto es muy característico de un ataque smurf, y las direcciones de origen son las direcciones de los reflectores smurf. Si busca a los propietarios de estos bloques de direcciones en las bases de datos "whois" de Internet adecuadas, puede encontrar a los administradores de estas redes y solicitar su ayuda para hacer frente al ataque.

En este punto en un incidente smurf, es importante recordar que estos reflectores son víctimas, no atacantes. Es sumamente raro que los agresores utilicen sus propias direcciones de origen en los paquetes IP en toda inundación DoS y es imposible que lo hagan en un ataque smurf en funcionamiento. Debería asumirse que toda dirección en un paquete de inundación es completamente falsa, o bien es la dirección de alguna clase de víctima. El enfoque más productivo para el objetivo final de un ataque smurf es ponerse en contacto con los reflectores, ya sea para pedirles que reconfiguren sus redes para apagar el ataque o para pedir su ayuda para rastrear el flujo de estímulo.

Debido a que el daño al objetivo final de un ataque smurf suele deberse a la sobrecarga del link entrante desde Internet, a menudo no hay otra respuesta que ponerse en contacto con los reflectores. Cuando los paquetes llegan a cualquier máquina bajo el control del objetivo, la mayor parte del daño ya se ha hecho.

Una medida provisoria es pedirle al proveedor de la red ascendente que filtre todas las respuestas de eco ICMP o todas las respuestas de eco ICMP que provienen de reflectores específicos. No se recomienda que deje este tipo de filtro en su lugar de forma permanente. Incluso para un filtro temporal, sólo se deben filtrar las respuestas de eco, no todos los paquetes ICMP. Otra posibilidad es que el proveedor ascendente utilice las funciones de calidad de servicio y limitación de velocidad para restringir el ancho de banda disponible para las respuestas de eco. Una limitación razonable del ancho de banda se puede dejar en su lugar indefinidamente. Ambos enfoques dependen de que el equipo del proveedor ascendente tenga la capacidad necesaria, y a

veces esa capacidad no está disponible.

Reflector Smurf

Si el tráfico entrante consiste en solicitudes de eco en lugar de respuestas de eco (en otras palabras, si la primera entrada de la lista de acceso, en lugar de la segunda, contaba muchas más coincidencias de las que cabría razonablemente esperar), sospecharía un ataque smurf en el que la red se estaba utilizando como reflector, o posiblemente una simple inundación de ping. En cualquier caso, si el ataque es un éxito, esperaría que el lado saliente de la línea serial se inundara, así como el lado entrante. De hecho, debido al factor de amplificación, se espera que el lado saliente esté aún más sobrecargado que el lado entrante.

Hay varias maneras de distinguir el ataque smurf de la simple inundación de ping:

- Los paquetes de estímulo Smurf se envían a una dirección de broadcast dirigida, en lugar de a una dirección de unidifusión, mientras que las inundaciones de ping normales casi siempre utilizan unicasts. Puede ver las direcciones que utilizan la palabra clave **log-input** en la entrada de la lista de acceso adecuada.
- Si se utiliza como reflector smurf, hay un número desproporcionado de broadcasts de salida en la pantalla **show interface** en el lado Ethernet del sistema, y normalmente un número desproporcionado de broadcasts enviados en la **visualización show ip traffic**. Una inundación de ping estándar no aumenta el tráfico de broadcast de fondo.
- Si se utiliza como reflector smurf, hay más tráfico saliente hacia Internet que tráfico entrante desde Internet. En general, hay más paquetes de salida que paquetes de entrada en la interfaz serial. Incluso si el flujo de estímulo completa la interfaz de entrada, el flujo de respuesta es mayor que el flujo de estímulo y se cuentan las caídas de paquetes.

Un reflector smurf tiene más opciones que el objetivo final de un ataque smurf. Si un reflector decide apagar el ataque, el uso apropiado de **no ip directed-broadcast** (o comandos equivalentes no IOS) suele ser suficiente. Estos comandos pertenecen a cada configuración, incluso si no hay un ataque activo. Para obtener más información sobre la prevención de que su equipo Cisco se use en un ataque smurf, consulte Mejora de la Seguridad en Routers Cisco. Para obtener información más general sobre los ataques smurf en general, y para obtener información sobre la protección de equipos que no son de Cisco, refiérase a la página Información sobre Ataques de Negación de Servicio.

Un reflector smurf está un paso más cerca del atacante que el destino final y, por lo tanto, está en una mejor posición para rastrear el ataque. Si decide rastrear el ataque, debe trabajar con los ISP involucrados. Si desea que se realice alguna acción cuando complete el seguimiento, debe trabajar con las agencias de aplicación de la ley adecuadas. Si busca rastrear un ataque, se recomienda que involucre a la policía lo antes posible. Consulte la sección Seguimiento para obtener información técnica sobre el seguimiento de ataques por inundación.

Fraggle

El ataque de fraggle es análogo al ataque de smurf, excepto que, para la secuencia de estímulo, se utilizan las solicitudes de eco UDP en lugar de las solicitudes de eco ICMP. Las tercera y cuarta líneas de la lista de acceso se refieren a ataques de fraggle. La respuesta adecuada para las víctimas es la misma, excepto que el eco UDP es un servicio menos importante en la mayoría de las redes que el eco ICMP. Por lo tanto, puede desactivarlos completamente con menos consecuencias negativas.

Inundación SYN

Las líneas quinta y sexta de la lista de acceso son:

```
access-list 169 permit tcp any any established
access-list 169 permit tcp any any
```

La primera de estas líneas coincide con cualquier paquete TCP con el conjunto de bits ACK. Para nuestros fines, esto significa realmente que coincide con cualquier paquete que no sea TCP SYN. La segunda línea coincide sólo con los paquetes que son TCP SYN. Una inundación SYN se identifica fácilmente desde los contadores de estas entradas de lista. En el tráfico normal, los paquetes TCP que no son SYN superan en número a los SYN por al menos un factor de dos, y generalmente más como cuatro o cinco. En un ataque SYN flood, los SYN son generalmente muchas veces mayores en número que los paquetes TCP no SYN.

La única condición de no ataque que crea esta firma es una sobrecarga masiva de pedidos auténticos de conexión. En general, dicha sobrecarga no será inesperada y no involucrará a tantos paquetes SYN como una inundación SYN real. Además, las inundaciones SYN a menudo contienen paquetes con direcciones de origen completamente inválidas; con la palabra clave **log-input**, es posible ver si las solicitudes de conexión provienen de dichas direcciones.

Hay un ataque llamado "ataque en la tabla de procesos" que tiene cierta similitud con la inundación SYN. En el ataque de la tabla de procesos, las conexiones TCP se completan y luego se les permite agotar el tiempo de espera sin tráfico de protocolo adicional, mientras que en la inundación SYN, sólo se envían las solicitudes de conexión iniciales. Debido a que un ataque a la tabla de procesos requiere la finalización del intercambio de señales inicial TCP, generalmente se debe iniciar con el uso de la dirección IP de una máquina real a la que el atacante tiene acceso (por lo general, acceso robado). Por lo tanto, los ataques de la tabla de procesos se distinguen fácilmente de las inundaciones SYN con el uso del registro de paquetes. Todos los SYN en un ataque de tabla de procesos provienen de una o varias direcciones, o como máximo de una o varias subredes.

Las opciones de respuesta para las víctimas de las inundaciones SYN son muy limitadas. El sistema atacado suele ser un servicio importante y el bloqueo del acceso al sistema suele lograr lo que el atacante quiere. Muchos productos de router y firewall, incluidos los de Cisco, tienen funciones que se pueden utilizar para reducir el impacto de las inundaciones SYN. Pero la efectividad de estas características depende del medio ambiente. Para obtener más información, refiérase a la documentación para el Conjunto de Funciones de Cisco IOS Firewall, la documentación para la función Cisco IOS TCP Intercept y Mejora de la Seguridad en los Routers Cisco.

Es posible rastrear inundaciones SYN, pero el proceso de seguimiento requiere asistencia de cada ISP en el trayecto desde el atacante hasta la víctima. Si decide intentar rastrear una inundación SYN, póngase en contacto con las fuerzas del orden desde el principio y trabaje con su propio proveedor de servicios ascendente. Consulte la sección seguimiento de este documento para obtener detalles sobre el seguimiento con el uso de equipos de Cisco.

Otros ataques

Si cree que se encuentra bajo un ataque y puede caracterizar ese ataque utilizando direcciones IP de origen y destino, números de protocolo y números de puerto, puede utilizar listas de acceso para probar su hipótesis. Cree una entrada de lista de acceso que coincida con el tráfico

sospechoso, aplíquela a una interfaz apropiada, y luego, mire los contadores de coincidencias o registre el tráfico.

Advertencias sobre registro y contadores

El contador de una entrada de lista de acceso cuenta todas las coincidencias con esa entrada. Si aplica una lista de acceso a dos interfaces, los recuentos que ve son recuentos agregados.

La lista de acceso al sistema no muestra cada paquete que se corresponde con una entrada. El registro tiene velocidad limitada para evitar la sobrecarga de la CPU. Lo que el registro muestra es una muestra razonablemente representativa, pero no un seguimiento de paquetes completo. Recuerde que hay paquetes que no ve.

En algunas versiones de software, sólo se puede iniciar sesión en la lista de acceso en determinados modos de conmutación. Si una entrada de la lista de acceso cuenta muchas coincidencias, pero no registra nada, intente borrar la memoria caché de ruta para forzar que los paquetes sean conmutados por proceso. Tenga cuidado si lo hace en routers con mucha carga con muchas interfaces. Se puede descartar mucho tráfico mientras se reconstruye la memoria caché. Utilice Cisco Express Forwarding siempre que sea posible.

Las listas de acceso y el registro tienen un impacto en el rendimiento, pero no uno grande. Tenga cuidado en los routers que funcionan con una carga de CPU superior al 80% o cuando aplica listas de acceso a interfaces de alta velocidad.

Rastreo

Las direcciones de origen de los paquetes DoS casi siempre se configuran en valores que no tienen nada que ver con los propios atacantes. Por lo tanto, no son útiles para identificar a los atacantes. La única manera confiable de identificar el origen de un ataque es rastreándolo hacia atrás, salto por salto, a lo largo de la red. Este proceso implica la reconfiguración de los routers y el examen de la información de registro. Se requiere la cooperación de todos los operadores de red a lo largo de la ruta del atacante a la víctima. Para asegurar esa cooperación, suele resultar necesaria la participación de agencias encargadas de velar por el cumplimiento de las leyes, las cuales deben también intervenir si se tomase alguna medida en contra del atacante.

El proceso de seguimiento para las inundaciones DoS es relativamente simple. Partiendo de un router (llamado “A”) que se sabe que es el que lleva el tráfico saturado, se identifica el router (llamado “B”) desde el cual A recibe el tráfico. Luego uno se conecta a B y encuentra el router (denominado "C") del que B recibe el tráfico. Esto continúa hasta que se encuentre la fuente última.

Hay varias complicaciones en este método, que esta lista describe:

- La "fuente final" puede ser una computadora que ha sido comprometida por el atacante, pero que en realidad es propiedad de otra víctima y está operada por ella. En este caso, el seguimiento de la inundación de DoS es sólo el primer paso.
- Los atacantes saben que se les puede rastrear y, por lo general, continúan sus ataques sólo durante un tiempo limitado. Es posible que no haya tiempo suficiente para rastrear la sobrecarga.
- Los ataques pueden provenir de varias fuentes, especialmente si el atacante es relativamente sofisticado. Es importante intentar identificar tantas fuentes como sea posible.

- Los problemas de comunicación ralentizan el proceso de seguimiento. Con frecuencia, uno o más de los operadores de red involucrados no tienen personal debidamente cualificado disponible.
- Las preocupaciones legales y políticas pueden dificultar la acción contra los atacantes incluso si se encuentra a uno.

La mayoría de los esfuerzos para rastrear los ataques de DoS fallan. Debido a esto, muchos operadores de red ni siquiera intentan rastrear un ataque a menos que se les ponga bajo presión. Muchos otros rastrean solamente ataques "severos", con diferentes definiciones de lo que es "severo". Algunos ayudan con un seguimiento sólo si se trata de la aplicación de la ley.

Seguimiento con “entrada de registro

Si decide rastrear un ataque que pasa a través de un router Cisco, la manera más efectiva de hacerlo es construir una entrada de lista de acceso que coincida con el tráfico de ataque, adjuntar la palabra clave **log-input** a él y aplicar la lista de acceso saliente en la interfaz a través de la cual se envía el flujo de ataque hacia su destino final. Las entradas de registro producidas por la lista de acceso identifican la interfaz del router a través de la cual llega el tráfico y, si la interfaz es una conexión multipunto, den la dirección de Capa 2 del dispositivo desde el que se recibe. La dirección de la Capa 2 luego puede ser utilizada para identificar el router siguiente en la cadena, utilizando por ejemplo el comando show ip arp mac-address.

Inundación SYN

Para rastrear una inundación SYN, puede crear una lista de acceso similar a esta:

```
access-list 169 permit tcp any any established
access-list 169 permit tcp any host victim-host log-input
access-list 169 permit ip any any
```

Esto registra todos los paquetes SYN destinados al host de destino, incluidos los SYNs legítimos. Para identificar el trayecto real más probable hacia el atacante, examine las entradas de registro en detalle. En general, la fuente de la inundación es la fuente desde la que llega el mayor número de paquetes coincidentes. Las direcciones IP de origen no significan nada. está buscando interfaces de origen y direcciones MAC de origen. A veces es posible distinguir los paquetes de inundación de los paquetes legítimos porque los paquetes de inundación pueden tener direcciones de origen no válidas. Cualquier paquete cuya dirección de origen no sea válida puede ser parte de la inundación.

La inundación puede provenir de múltiples fuentes, aunque esto es relativamente inusual para las inundaciones SYN.

Estímulo Smurf

Para rastrear un flujo de estímulo smurf, utilice una lista de acceso como esta:

```
access-list 169 permit icmp any any echo log-input
access-list 169 permit ip any any
```

Observe que la primera entrada no se restringe a los paquetes destinados para la dirección reflectora. La razón para esto es que muchos ataques smurf usan redes de reflector múltiple. Si no está en contacto con el objetivo final, es posible que no conozca todas las direcciones del

reflector. A medida que su seguimiento se acerca al origen del ataque, puede comenzar a ver solicitudes de eco que van a más y más destinos; esta es una buena señal.

Sin embargo, si trata con una gran cantidad de tráfico ICMP, esto puede generar demasiada información de registro para que pueda leerla fácilmente. Si esto sucede, puede restringir la dirección de destino para que sea uno de los reflectores que se sabe que se utilizará. Otra táctica útil es usar una entrada que aprovecha el hecho de que las mascarillas de red de 255.255.255.0 son muy comunes en Internet. Y, debido a la forma en la que los atacantes encuentran reflectores smurf, es más probable que las direcciones del reflector que en realidad se usan coincidan con esa máscara. Las direcciones de host que terminan en .0 o .255 son muy poco comunes en Internet. Por lo tanto, puede construir un reconocedor relativamente específico para los flujos de estímulo smurf como muestra este resultado:

```
access-list 169 permit icmp any host known-reflector echo log-input access-list 169 permit icmp any 0.0.0.255 255.255.255.0 echo log-input access-list 169 permit icmp any 0.0.0.0 255.255.255.0 echo log-input access-list 169 permit ip any any
```

Con esta lista, puede eliminar muchos de los paquetes de "ruido" de su registro, mientras aún tiene una buena oportunidad de notar flujos de estímulo adicionales a medida que se acerca al atacante.

Seguimiento sin “entrada de registro”

Existe la palabra clave de entrada de registro en la versión 11.2 del software del IOS de Cisco y versiones posteriores, y en algunos software basados en 11.1 creados especialmente para el mercado de proveedor de servicios. El software anterior no admite esta palabra clave. Si utiliza un router con software antiguo, tiene tres opciones viables:

- Cree una lista de acceso sin registro, pero con entradas que coincidan con el tráfico sospechoso. Aplique la lista en el lado de *entrada* de cada interfaz y observe los contadores. Busque interfaces con altas velocidades de coincidencia. Este método tiene una sobrecarga de rendimiento muy pequeña y es bueno para la identificación de interfaces de origen. La desventaja más importante es que no provee direcciones de origen de la capa del link y, por lo tanto, es mucho más útil para líneas punto a punto.
- Cree entradas de lista de acceso con la contraseña de registro (en oposición a la entrada de registro). Una vez más, aplique la lista al lado entrante de cada interfaz a la vez. Este método todavía no proporciona direcciones MAC de origen, pero puede ser útil para ver datos IP. Por ejemplo, para verificar que un flujo de paquetes realmente es parte de un ataque. El impacto en el rendimiento puede ser de moderado a alto y el software más reciente funciona mejor que el software anterior.
- Utilice el comando **debug ip packet detail** para recopilar información sobre los paquetes. Este método proporciona direcciones MAC, pero puede tener un impacto negativo en el rendimiento. Es fácil cometer un error con este método y hacer que un router sea inutilizable. Si utiliza este método, asegúrese de que el router conmute el tráfico de ataque en modo rápido, autónomo u óptimo. Utilice una lista de acceso para restringir la depuración sólo a la información que realmente necesita. Registre la información de depuración para la memoria intermedia de registro local, pero desactive el registro de información de depuración para las sesiones Telnet y la consola. En lo posible, coloque a alguien cerca del router, de modo que esta persona pueda realizar a un ciclo de encendido del router toda vez que fuese necesario.Recuerde que el comando **debug ip packet** no muestra información sobre los

paquetes de conmutación rápida. Debe ejecutar el comando **clear ip cache** para capturar información. Cada **comando clear** le da uno o dos paquetes de salida de debug.

Información Relacionada

- Kerberos
- Soporte Técnico y Documentación - Cisco Systems