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 muchas secuencias de ataque DOS pueden ser aislados cuando usted las hace juego contra las entradas de lista de acceso del software de Cisco IOS®. Esto tiene valor para filtrar hacia fuera los ataques. Es también útil para cuando usted caracteriza los ataques desconocidos, y para cuando usted rastrea las secuencias de paquetes del “spoofed” a sus verdaderos orígenes.

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 Cisco IOS Software, las Listas de acceso y el registro de la lista de acceso son las funciones principales para cuando usted caracteriza y localiza los ataques comunes.

prerrequisitos

Requisitos

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

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

Los ataques DoS más comunes

Una amplia variedad de ataques DOS son posibles. Incluso si usted ignora los ataques que utilizan los bug de software para apagar los sistemas con relativamente poco tráfico, el hecho sigue siendo que cualquier paquete del IP que se pueda enviar a través de la red se puede utilizar para ejecutar un ataque el inundar DOS. Cuando usted está bajo ataque, usted debe considerar siempre la posibilidad que lo que usted ve es algo que no entra en las categorías habituales.

Sujeto a esa advertencia, también es bueno recordar que muchos ataques son similares. Los atacantes eligen los exploits comunes porque son determinado eficaces, determinado duro localizar, o porque las herramientas están disponibles. Muchos atacantes DOS faltan la habilidad o la motivación para crear sus propias herramientas, y utilizan los programas encontrados 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 “último destino” 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. Falsifican a las direcciones de origen de estos paquetes para ser el direccionamiento del último destino. Para cada paquete enviado por el atacante, muchos host en la subred reflectora responden. Esto inunda el último destino y pierde el 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 smurf se notan generalmente porque un link de red se sobrecarga. Una descripción completa de estos ataques, y de las medidas de la defensa, está en la página de información de los establecimientos de rechazo del servicio .

Otro ataque común es la inundación SYN en la que una máquina de destino es inundada con solicitudes de conexión TCP. Seleccionan al azar a las direcciones de origen y los puertos TCP de la fuente de los paquetes de pedido de conexión. El propósito es forzar al host de destino a

mantener la información del estado para muchas conexiones que nunca se completen.

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. Es también posible para el tráfico ese las devoluciones del host de destino para causar el problema en el Routers. Esto es porque este tráfico de retorno va a las direcciones de origen asignadas en forma aleatoria de los paquetes originales, él falta las propiedades de localidad del tráfico IP “real”, y puede desbordar 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 la “segunda grada”, tales como inundaciones de ping) se reconocen fácilmente cuando usted utiliza las Listas de acceso de Cisco.

Lista de acceso de caracterización DoS

Represente a un router con dos interfaces. El ethernet0 está conectado con un LAN interno en un negocio o un pequeño ISP. Serial 0 permite la conexión a Internet a través de ISP ascendente. La tarifa del paquete de entrada en el serial0 “se fija” en el ancho de banda de link completo, y los host en el LAN se ejecutan lentamente, causan un crash, cuelgan, o muestran otras muestras de un ataque DOS. El pequeño sitio en el cual el router conecta no tiene ningún analizador de red, y la gente allí tiene poco o nada de experiencia en las trazas del analizador de la lectura incluso si las trazas están disponibles.

Ahora, asuma que usted aplica una lista de acceso mientras que esta salida muestra:

```
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 hacia fuera 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, inundaciones SYN, y fraggle.

Destino final de smurf

Si usted publica el **comando show access-list**, usted ve la salida similar a esto:

```
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 en la interfaz serial consiste en los paquetes de respuesta del

eco de ICMP. Ésta es probablemente la firma de un ataque smurf, y nuestro sitio es el último destino, bastante que el reflector. Usted puede recopilar más información sobre el ataque cuando usted revisa la lista de acceso, pues esta salida muestra:

```
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 de Cisco IOS Software de 11.2 faltan anterior esta palabra clave. Utilice la palabra clave del "**registro**" en lugar de otro.) Esto causa al router a la información de registro sobre los paquetes que hacen juego la entrada de la lista. Si usted asume que la **registración mitigada** está configurada, usted puede ver los mensajes que resultan con el **comando show log** (pueden tardar un rato para que los mensajes acumulen debido a la tarifa que limita). Los mensajes aparecen similares a esta salida:

```
%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
```

Agrupan a las direcciones de origen de los paquetes de respuesta de eco en los prefijos de dirección 192.168.212.0/24, 192.168.45.0/24, y 172.16.132.0/24. (Las direcciones privadas en las redes 192.168.x.x y 172.16.x.x no estarían en Internet; esto es una ilustración de laboratorio.) Esto es muy característico de un ataque smurf, y las direcciones de origen son los direccionamientos de los reflectores smurfes. Si usted mira para arriba a los propietarios de estos bloqueos de dirección en las bases de datos apropiadas de Internet “WHOIS”, usted puede encontrar a los administradores de estas redes, y pide su ayuda haciendo 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 acercamiento más productivo para el último destino de un ataque smurf es entrar en contacto los reflectores, para pedirlos para configurar de nuevo sus redes para apagar el ataque, o para pedir su ayuda en localizar la secuencia de estímulo.

Porque el daño al último destino de un ataque smurf es causado generalmente sobrecargando del link entrante de Internet, no hay a menudo respuesta con excepción de para entrar en contacto los reflectores. Para el momento en que los paquetes lleguen cualquier máquina bajo el control de la blanco, la mayor parte del daño se ha hecho ya.

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 usted deja esta clase de filtro en el lugar permanentemente. Incluso para un filtro temporal, solamente las Respuestas de eco se deben filtrar, no todos los paquetes icmp. Otra posibilidad es tener la calidad de servicio del uso del proveedor ascendente y valorar la limitación de las características para restringir el ancho de banda disponible para las Respuestas de eco. Una limitación de ancho de banda razonable se puede dejar en el lugar indefinidamente. Ambos acercamientos dependen del equipo del proveedor ascendente que tiene la capacidad necesaria, y esa capacidad no está a veces disponible.

Reflector Smurf

Si el tráfico entrante consiste en los pedidos de eco bastante que las Respuestas de eco (es decir si la primera entrada de lista de acceso, bastante que la segunda, contara muchas más coincidencias que podría razonablemente ser esperado), usted sospecharía un ataque smurf en el cual la red era utilizada como reflector, o posiblemente una simple inundación de ping. En ambos casos, si el ataque es un éxito, usted esperaría que hundieran al lado de salida de la línea serial, así como al lado entrante. De hecho, debido al factor de amplificación, usted esperaría que sobrecargaran al lado de salida aún más 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 dirigido, bastante

que a una dirección de Unicast, mientras que las inundaciones de ping ordinarias utilizan casi siempre el unicasts. Usted puede ver los direccionamientos que utilizan la **palabra clave de entrada de registro** en la entrada de lista de acceso apropiada.
- Si le utilizan como reflector smurf, hay un número desproporcionado de broadcasts de la salida en la visualización de la **interfaz de la demostración** en el lado Ethernet del sistema, y generalmente un número desproporcionado de broadcasts enviados en la visualización del **tráfico del IP de la demostración**. Una inundación de ping estándar no aumenta el tráfico de broadcast de fondo.
- Si le utilizan como reflector smurf, hay más tráfico saliente hacia Internet que el tráfico entrante de Internet. Hay generalmente más paquetes de salida que los paquetes de entrada en la interfaz serial. Incluso si la secuencia de estímulo llena totalmente la interfaz de entrada, la secuencia de la respuesta es más grande que la secuencia de estímulo, y se cuentan las caídas de paquetes.

Un reflector smurf tiene más opciones que el último destino de un ataque smurf. Si un reflector elige apagar el ataque, el uso apropiado de **ningún broadcast dirigido del IP** (o de los comandos equivalentes del no IOS) es suficiente generalmente. Estos comandos pertenecen en cada configuración, incluso si no hay ataque activo. Para más información sobre la prevención de su equipo de Cisco de ser utilizado en un ataque smurf, refiera a mejorar la Seguridad en los routeres Cisco. Para más información general sobre los ataques smurf generalmente y para la información sobre la protección equipo no Cisco, refiera a la página de información de los establecimientos de rechazo del 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 usted elige localizar el ataque, usted necesita trabajar con los ISP implicados. Si usted desea tener acción realizada cuando usted completa la traza, usted necesita trabajar con las autoridades competentes apropiadas. Si usted intenta localizar un ataque, se recomienda que usted implica el cumplimiento de la ley cuanto antes. 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 apropiada para las víctimas es lo mismo, salvo que la generación de eco UDP es un servicio menos importante en la mayoría de las redes que el eco ICMP. Por lo tanto, usted puede inhabilitarlas totalmente con menos consecuencias negativas.

Inundación SYN

Las quintas y sextas líneas de la lista de acceso son:

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

El primer de estas líneas hace juego 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 hace juego solamente los paquetes que son TCP SYN. Una inundación SYN se identifica fácilmente de los contadores en estas entradas de la lista. En el tráfico normal, los paquetes TCP NON-SYN exceden en número los SYN por por lo menos un factor de dos, y generalmente más bién 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. También, las inundaciones SYN contienen a menudo los paquetes con totalmente las direcciones de origen no válidas; usando la **palabra clave de entrada de registro**, es posible ver si los pedidos de conexión venir de tales direccionamientos.

Hay un ataque llamado un “ataque de tabla al proceso” que lleve una cierta semejanza a la inundación SYN. En el ataque de tabla al proceso, se completan, después se permiten las conexiones TCP medir el tiempo hacia fuera sin el tráfico de protocolo adicional, mientras que en la inundación SYN, sólo se envían las peticiones de conexión inicial. Porque un ataque de tabla al proceso requiere la realización de la entrada en contacto inicial con TCP, debe ser iniciado generalmente con el uso de la dirección IP de una Máquina real a la cual el atacante tenga acceso (acceso generalmente robado). Los ataques de tabla al proceso por lo tanto se distinguen fácilmente de las inundaciones SYN con el uso del registro del paquete. Todos los SYN en un ataque de tabla al proceso vienen a partir de un o algún direccionamientos, o a lo más a partir de una o alguna subredes.

Las opciones de respuesta para las víctimas de las inundaciones SYN son muy limitadas. El sistema bajo ataque es generalmente un servicio importante, y el bloqueo del acceso al sistema logra generalmente lo que quiere el atacante. Mucho el router y los productos de escudo de protección, incluyendo Cisco, tienen características que se puedan utilizar para reducir el impacto de las inundaciones SYN. Pero, la eficacia de estas características depende del entorno. Para más información, refiera a la documentación para el conjunto de funciones del Cisco IOS Firewall, la documentación para la característica de la Intercepción de tráfico de TCP del Cisco IOS, y mejorar la Seguridad en los routeres 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 usted decide intentar localizar una inundación SYN, entre en contacto el cumplimiento de la ley a principios de, y trabaje con su propio proveedor del servicio ascendente. Vea la sección de seguimiento de este documento para los detalles en el seguimiento con el uso del equipo de Cisco.

Otros ataques

Si usted cree que usted está bajo ataque, y si usted puede caracterizar ese ataque usando el IP de origen y las direcciones destino, los números de protocolo, y los números del puerto, usted puede utilizar las 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 en una entrada de lista de acceso cuenta todas las coincidencias contra esa entrada. Si usted aplica una lista de acceso a dos interfaces, las cuentas que usted ve son cuentas globales.

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. Qué registro muestra usted es razonablemente un ejemplo representativo, pero no una traza del paquete completa. Recuerde

que hay los paquetes que usted 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 lista de acceso cuenta muchas coincidencias, pero no registra nada, intente borrar memoria caché de ruta para forzar los paquetes para ser proceso conmutado. Tenga cuidado si usted hace esto en pesadamente los routeres cargados con muchas interfaces. Mucho tráfico puede conseguir caído mientras que se reconstruye el caché. Utilice el Cisco Express Forwarding siempre que sea posible.

Las Listas de acceso y el registro tienen un impacto del rendimiento, pero no grande. Tenga cuidado en el Routers que se ejecuta en más que cerca de 80 porcentaje de la CPU cargan, o cuando usted aplica las Listas de acceso mismo a las interfaces de velocidad alta.

Rastreo

Fijan a las direcciones de origen de los paquete DoS casi siempre a los valores que no tienen nada hacer con los atacantes ellos mismos. Por lo tanto, no son útil en la identificación de 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 del Routers y el examen de la información de registro. La cooperación de todos los operadores de la red a lo largo de la trayectoria del atacante a la víctima se requiere. 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 última” puede ser un ordenador que ha sido comprometido por el atacante, pero que es poseído y actuado realmente por otra víctima. En este caso, localizar la inundación DOS es solamente el primer paso.
- Los atacantes saben que pueden ser localizados, y continúan generalmente sus ataques solamente por un tiempo limitado. Es posible que no haya tiempo suficiente para rastrear la sobrecarga.
- Los ataques pueden venir de las fuentes múltiples, especialmente si el atacante es relativamente sofisticado. Es importante intentar identificar tantas fuentes como sea posible.
- Los problemas de comunicación retrasan el proceso de seguimiento. Uno o más de los operadores de la red implicados no tienen con frecuencia apropiadamente el personal capacitado disponible.
- Las preocupaciones legales y políticas pueden hacerlo difícil actuar contra los atacantes incluso si se encuentra uno.

La mayoría de los esfuerzos para localizar el fall de los ataques DOS. Debido a esto, muchos operadores de la red ni siquiera intentan localizar un ataque a menos que estén colocados bajo presión. Muchos otros localizan solamente los ataques “severos”, con las definiciones de diferenciación de cuál es “severo.” Una cierta ayuda con una traza solamente si el cumplimiento de la ley está implicado.

Seguimiento con “entrada de registro

Si usted elige localizar un ataque que pase a través de un router Cisco, la mayoría de la manera eficaz de hacer esto es construir una entrada de lista de acceso que haga juego el tráfico del ataque, asocia la **palabra clave de entrada de registro a** ella, y aplica la lista de acceso saliente en la interfaz a través de la cual la secuencia de ataque se envía hacia su último destino. Las entradas de registro producidas por la lista de acceso identifican la interfaz del router a través de la cual el tráfico llega, y, si la interfaz es una conexión multipunto, dan el direccionamiento de la capa 2 del dispositivo del cual 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 localizar una inundación SYN, usted puede crear una lista de acceso similar a esto:

```
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 para el host de destino, incluyendo los SYN legítimos. Para identificar la ruta de acceso real más probable hacia el atacante, examine las entradas de registro detalladamente. La fuente de la inundación es generalmente la fuente de la cual el número más grande de paquetes que corresponden con llega. Las dirección IP de origen ellos mismos no significan nada. está buscando interfaces de origen y direcciones MAC de origen. Es a veces posible distinguir los paquetes de inundación de los paquetes legítimos porque los paquetes de inundación pueden tener las direcciones de origen no válidas. Cualquier paquete cuya dirección de origen no sea válida puede ser parte de la inundación.

La inundación puede venir de las fuentes múltiples, aunque ésta sea relativamente inusual para las inundaciones SYN.

Estímulo Smurf

Para localizar una secuencia de estímulo del smurf, utilice una lista de acceso como esto:

```
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
```

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 usted no está en contacto con el último destino, usted no puede conocer todos los direccionamientos del reflector. Mientras que su traza consigue más cercano a la fuente del ataque, usted puede comenzar a ver los pedidos de eco el ir cada vez más a los destinos; esto es un buen síntoma.

Sin embargo, si usted se ocupa de mucho tráfico ICMP, esto puede generar demasiada información de ingreso al sistema para que usted lea fácilmente. Si sucede esto, usted puede restringir a la dirección destino para ser uno de los reflectores que se sabe para ser utilizado. Otra táctica útil es utilizar una entrada que se aproveche del hecho de que las máscaras 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

infrecuentes en Internet. Por lo tanto, usted puede construir un reconocedor relativamente específico para las secuencias de estímulo del smurf mientras que esta salida muestra:

```
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
```

Con esta lista, usted puede eliminar muchos de los paquetes del “ruido” de su registro, mientras que usted todavía tiene una buena ocasión de notar las secuencias de estímulo adicionales mientras que usted consigue más cercano 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 usted utiliza a un router con un más viejo software, usted tiene tres opciones viables:

- Cree una lista de acceso sin la registración, pero con las entradas que hacen juego el tráfico sospechoso. Aplique la lista en el *lado de entrada de* cada interfaz a su vez, y mire los contadores. Busque las interfaces con las altas tarifas de la coincidencia. Este método tiene una recarga de rendimiento muy pequeña, y es bueno para la identificación de las 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 da los MAC Address de origen, sino puede ser útil para considerar los datos IP. Por ejemplo, verificar que una secuencia de paquetes sea realmente parte de al ataque. El impacto del rendimiento puede ser medio a alto y un más nuevo software realiza mejor que un más viejo software.
- Utilice el **comando debug ip packet detail** de recoger la 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 usted utiliza este método, aseegurese que los switches del router el tráfico del ataque en rápido, autónomo, o el modo óptimo. Utilice una lista de acceso para restringir el debugging solamente a la información que usted necesita realmente. 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 no lo hace el **comando debug ip packet** mostrar información sobre los paquetes de Switching rápido. Usted necesita publicar el **comando clear ip cache** para capturar la información. Cada **comando clear** le da uno o dos paquetes de salida de los debugs.

Información Relacionada

- Kerberos
- Soporte Técnico y Documentación - Cisco Systems