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

Contenido

Introducción

Los ataques de la negación de servicio (DOS) son comunes en Internet. El primer paso que se utiliza para responder a dicho ataque es descubrir exactamente qué clase de ataque es. Muchos de los ataques de uso general DOS se basan en las inundaciones de paquetes del ancho de banda alto, o en otras secuencias repetitivas de paquetes.

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 “spoofed” a sus verdaderos orígenes.

Las características del router de Cisco tales como registro de debug y estadísticas IP se pueden utilizar a veces para los propósitos similares, especialmente con los nuevos o inusuales ataques. 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 rastrea 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

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

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 a los sistemas cerrados con relativamente poco tráfico, el hecho sigue siendo que cualquier paquete 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.

Conforme a esa advertencia, sin embargo, es también bueno recordar que muchos ataques son similares. Los atacantes eligen los exploits comunes porque son determinado eficaces, determinado duro rastrear, 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 caer dentro y fuera de la moda.

A la hora de esta escritura, en julio 1999, la mayoría de los pedidos del cliente la asistencia de Cisco implican el ataque del “smurf”. Este ataque tiene dos víctimas: un “último destino” y un “reflector.” El atacante envía una secuencia de estímulo de peticiones de la generación de eco ICMP (“pings”) a la dirección de broadcast 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, llamado “fraggle,” utiliza los broadcastes dirigidos de la misma manera, pero utiliza las peticiones de la generación de eco UDP en vez de las peticiones de la generación de eco del Internet Control Message Protocol (ICMP). Fraggle alcanza generalmente un factor de amplificación más pequeño que el 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 ataques de la negación de servicio .

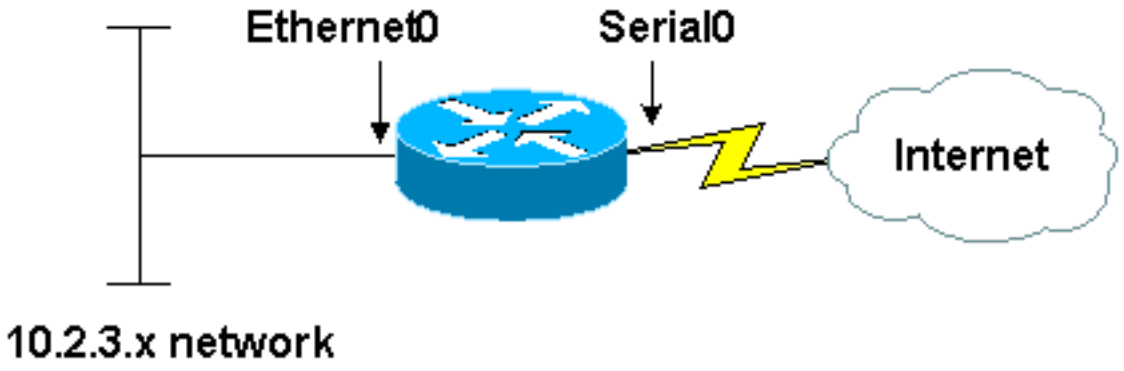
Otro ataque común es la inundación del SYN, en la cual una máquina de destino se inunda con las peticiones de conexión TCP. Seleccionan al azar a las direcciones de origen y los puertos de la fuente TCP de los paquetes de pedidos de la conexión. El propósito es forzar al host de destino a mantener la información del estado para muchas conexiones que nunca se completen.

Los ataque de tipo flood de congestión del servidor SYN se notan generalmente porque el host de destino (con frecuencia un HTTP o un servidor SMTP) llega a ser extremadamente lento, causa un crash, o 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 “real” IP, y puede desbordar los cachés de la ruta. En el Routers de Cisco, este problema se manifiesta a menudo en el router que se ejecuta de la memoria.

Junto, el smurf y los ataque de tipo flood de congestión del servidor SYN explican al amplia mayoría de los ataques DOS que inundan señalados a Cisco, y el reconocimiento de ellos es rápidamente muy importante. 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.

Una lista de acceso del caracterización DoS

Represente a un router con dos interfaces. El Ethernet 0 está conectado con un LAN interno en un negocio o una pequeña ISP. El serial 0 proporciona a una conexión de Internet vía una ISP por aguas arriba. La tarifa del paquete de entrada en el serial 0 “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 los rastros del analizador de la lectura incluso si los rastros 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, porque categoriza los paquetes en las formas útiles, la lista se puede utilizar para diagnosticar provisional los tres tipos de ataques: smurf, inundaciones del 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 en serie 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
```

El cambio aquí es que la **palabra clave de entrada de registro** está agregada a la entrada de lista de acceso que hace juego el tráfico sospechoso. (Las versiones de software del Cisco IOS de 11.2 faltan anterior esta palabra clave. Utilice la palabra clave del "**registro**" en lugar de otro.) Esto hace al router registrar la información sobre los paquetes que hacen juego la entrada de la lista. Si usted asume que la **registración protegida** 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 la 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.

Es importante a este punto en un incidente de smurf recordar que estos reflectores son víctimas también, no los atacantes. Es extremadamente raro para que los atacantes utilicen a sus propias direcciones de origen en los paquetes IP en cualquier inundación DOS, e imposible para que hagan tan en un ataque smurf de trabajo. Cualquier direccionamiento en un paquete de inundación se debe asumir para ser falsificado totalmente, o el direccionamiento de una víctima de una cierta clase. El acercamiento más productivo para el último destino de un ataque smurf es entrar en contacto con los reflectores, para pedirlos para configurar de nuevo sus redes para cerrar el ataque, o para pedir su ayuda en rastrear 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 con 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 del substituto es pedir el proveedor de red ascendente para filtrar hacia fuera todas las Respuestas de eco ICMP, o todas las Respuestas de eco ICMP de los 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 las peticiones de la generación 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 del estímulo de Smurf se envían a una dirección de broadcast dirigido, bastante que a un direccionamiento del unicast, mientras que las inundaciones de ping ordinarias utilizan casi siempre los 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 difusiones de la salida en la visualización del **interfaz de la demostración** en el lado de los Ethernetes del sistema, y generalmente un número desproporcionado de difusiones enviadas en la visualización del **tráfico 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 en serie. 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 los descensos del paquete.

Un reflector smurf tiene más opciones que el último destino de un ataque smurf. Si un reflector elige cerrar el ataque, el uso apropiado de **ningún broadcast dirigido 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 el Routers de 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 ataques de la negación de servicio .

Un reflector smurf es un paso más cercano al atacante que el último destino, y está por lo tanto en una mejor posición para rastrear el ataque. Si usted elige rastrear el ataque, usted necesita trabajar con las ISP implicadas. Si usted desea tener acción realizada cuando usted completa el rastro, usted necesita trabajar con las autoridades competentes apropiadas. Si usted intenta rastrear un ataque, se recomienda que usted implica el cumplimiento de la ley cuanto antes. Vea la sección de seguimiento para información técnica sobre los ataques de la inundación que rastrean.

Fraggle

El ataque de fraggle es análogo al ataque smurf, salvo que las peticiones de la generación de eco UDP se utilizan para la secuencia de estímulo en vez de las peticiones de la generación de eco ICMP. Las terceras y cuartas líneas de la lista de acceso identifican los 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 la generación de 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 del bit ACK. Para nuestros propósitos, qué éste significa realmente es que hace juego cualquier paquete que no sea un SYN TCP. La segunda línea hace juego solamente los paquetes que son TCP SYNs. Una inundación del SYN se identifica fácilmente de los contadores en estas entradas de la lista. En el tráfico normal, los paquetes del no-SYN TCP exceden en número SYNs por por lo menos un factor de dos, y generalmente más bién cuatro o cinco. En una inundación del SYN, SYNs excede en número típicamente los paquetes del no-SYN TCP muchas veces encima.

La única condición del no-ataque que crea esta firma es una sobrecarga masiva de las peticiones de conexión auténticas. Tal sobrecarga no vendrá generalmente inesperado, y no implicará tantos paquetes SYN como inundación real del SYN. También, las inundaciones del 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 las peticiones de conexión venir de tales direccionamientos.

Hay un ataque llamado un “ataque de tabla al proceso” que lleve una cierta semejanza a la inundación del 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 del 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 puesto en marcha 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 del SYN con el uso del registro del paquete. Todo el SYNs en un ataque de tabla al proceso viene 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 del 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 los Productos del router y del Firewall, incluyendo Cisco, tienen características que se puedan utilizar para reducir el impacto de las inundaciones del SYN. Pero, la eficacia de estas características depende del entorno. Para más información, refiera a la documentación para el conjunto de la característica del Firewall Cisco IOS, la documentación para la característica de la Intercepción de tráfico de TCP del Cisco IOS, y mejorar la Seguridad en el Routers de Cisco.

Es posible rastrear las inundaciones del SYN, pero el proceso de seguimiento requiere la ayuda de cada ISP a lo largo de la trayectoria del atacante a la víctima. Si usted decide intentar rastrear una inundación del SYN, entre en contacto con 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 rastrear 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 los direccionamientos de 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 haga juego el tráfico sospechoso, lo aplican a un interfaz apropiado, y mire a los contadores de coincidencias o registre el tráfico.

Registro y Advertencias del contador

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.

El registro de la lista de acceso no muestra cada paquete que haga juego una entrada. El registro es tarifa-limitado evitar sobrecarga de la CPU. Qué registro muestra usted es razonablemente un ejemplo representativo, pero no un rastro completo del paquete. Recuerde que hay los paquetes que usted no ve.

En algunas versiones de software, el registro de la lista de acceso trabaja solamente en ciertos modos de la transferencia. Si una entrada de lista de acceso cuenta muchas coincidencias, pero no registra nada, intente borrar el caché de la ruta para forzar los paquetes para ser proceso cambiado. Tenga cuidado si usted hace esto en pesadamente los routeres cargados con muchos interfaces. Mucho tráfico puede conseguir caído mientras que se reconstruye el caché. Utilice la expedición expresa de Cisco 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 la fuente de un ataque es rastrearlo salto-por-salto a través de la red. Este proceso implica la reconfiguración del Routers y el examen de la información del registro. La cooperación de todos los operadores de red a lo largo de la trayectoria del atacante a la víctima se requiere. La sujeción de esa cooperación requiere generalmente la implicación de las autoridades competentes, que deben también estar implicadas si se va alguna acción a ser tomada contra el atacante.

El proceso de seguimiento para las inundaciones DOS es relativamente simple. Comenzando en un router (nombrado “A”) que se sabe para llevar el tráfico inundado, uno identifica al router (nombrado “B”) de quien A está recibiendo el tráfico. Entonces los registros uno en B, y encuentran al router (nombrado “C”) de quien B está recibiendo 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, rastrear la inundación

DOS es solamente el primer paso.

- Los atacantes saben que pueden ser rastreados, y continúan generalmente sus ataques solamente por un tiempo limitado. Puede no haber bastante tiempo de rastrear realmente la inundación.
- 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 red implicados no tienen con frecuencia apropiadamente el personal capacitado disponible.
- Las preocupaciones legales y políticas pueden hacerla difícil actuar contra los atacantes incluso si se encuentra uno.

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

Seguimiento con “entrada de registro

Si usted elige rastrear un ataque que pase a través de un router de Cisco, la mayoría del modo 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** él, y aplica la lista de acceso saliente en el interfaz a través del cual la secuencia de ataque se envía hacia su último destino. Las entradas de registro producidas por la lista de acceso identifican el interfaz del router a través del cual el tráfico llega, y, si el interfaz es una conexión multipunto, dan el direccionamiento de la capa 2 del dispositivo del cual se recibe. El direccionamiento de la capa 2 se puede entonces utilizar para identificar al router siguiente en el encadenamiento, usando, por ejemplo, el **comando show ip arp mac-address**.

Inundación SYN

Para rastrear una inundación del 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 SYNs legítimo. 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. Los IP Addresses ellos mismos de la fuente no significan nada. Usted está buscando las interfaces de origen y los direccionamientos del 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 sea inválida es probable ser parte de la inundación.

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

Estímulo Smurf

Para rastrear 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 el direccionamiento del reflector. La razón de esto es que la mayoría de los ataques smurf utilizan las redes reflectoras múltiples. Si usted no está en contacto con el último destino, usted no puede conocer todos los direccionamientos del reflector. Mientras que su rastro consigue más cercano a la fuente del ataque, usted puede comenzar a ver las peticiones de la generación 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 el direccionamiento de 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 manera que los atacantes encuentran los reflectores smurfes, los direccionamientos del reflector usados realmente para los ataques smurf son aún más probables hacer juego 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”

La palabra clave de entrada de registro existe en los Cisco IOS Software Release 11.2 y Posterior, y en cierto software 11.1-based creado específicamente 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 los 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. Su desventaja más grande es que no da a las direcciones de origen de la capa de link, y es por lo tanto útil sobre todo para las líneas Point-to-Point.
- Cree las entradas de lista de acceso con la palabra clave del **registro** (en comparación con la registro-**entrada**). De nuevo, aplique la lista al lado entrante de cada interfaz a su vez. Este método todavía no da los direccionamientos del MAC 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 da las direcciones MAC, pero puede tener impacto negativo en el rendimiento. Es fácil incurrir en una equivocación con este método y hacer a un router inutilizable. Si usted utiliza este método, asegúrese de que el router cambie el tráfico del ataque en rápido, autónomo, o modo óptimo. Utilice una lista de acceso para restringir el depuración solamente a la información que usted necesita realmente. Registre la información de debugging al búfer del registro local, pero dé vuelta a cierre de la sesión de la información de la depuración a las sesiones de Telnet y a la consola. Si es posible, arregle para que alguien esté físicamente cerca del router, de modo que pueda ser potencia completada un ciclo cuanto sea necesario.Recuerde que no lo hace el **comando debug ip packet** mostrar información sobre los paquetes rápido-cambiados. Usted necesita publicar el **comando clear ip cache** para capturar la información. Cada **comando clear** le da uno o dos paquetes de salida de la depuración.

Información Relacionada

- Kerberos
- Soporte Técnico y Documentación - Cisco Systems