Caracterizando e Rastreando Inundações de Pacote com Uso de Cisco Routers

Índice

Introdução

Os ataques de negação de serviço (DoS) são comuns na Internet. O primeiro passo para responder a tal ataque é saber exatamente de que tipo é o ataque. Muitos dos ataques de DoS usados com freqüência baseiam-se em inundações de pacotes de largura de banda elevada ou em outros fluxos de pacotes repetitivos.

Os pacotes em muitos fluxos de ataque do dos podem ser isolados quando você os combina contra entradas de lista de acesso do software de Cisco IOS®. Isto é valioso para filtrar para fora ataques. É igualmente útil para quando você caracteriza ataques desconhecidos, e para quando você segue correntes de pacote de informação “falsificado” de volta a seus origens reais.

Os recursos do roteador Cisco, como log de depuração e contabilidade IP também podem ser usados para finalidades semelhantes, particularmente com ataques novos ou incomuns. Contudo, com versões recentes do Cisco IOS Software, as Listas de acesso e o registro da lista de acessos são os recursos principais para quando você caracteriza e segue ataques comuns.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Os ataques mais comuns de DoS

Uma ampla variedade de ataques DoS é possível. Mesmo se você ignora os ataques que usam Bug de Software aos sistemas fechados com relativamente pouco de tráfego, o fato permanece que algum pacote IP que puder ser enviado através da rede pode ser usada para executar um ataque inundar DoS. Quando você está sob o ataque, você deve sempre considerar a possibilidade que o que você vê é algo que não cai nas categorias comum.

Sujeito a caveat, contudo, vale lembrar que muitos ataques são semelhantes. Os atacantes escolhem façanhas comuns porque são particularmente eficazes, particularmente duro seguir, ou porque as ferramentas estão disponíveis. Muitos atacantes DoS faltam a habilidade ou a motivação para criar suas próprias ferramentas, e usam os programas encontrados no Internet. Essas ferramentas tendem a ficar e sair na moda.

No momento em que este documento foi escrito, em julho de 1999, a maioria das solicitações dos clientes por assistência da Cisco envolvia o ataque "smurf". Este ataque tem duas vítimas: um "destino final" e um "refletor". O invasor envia um fluxo de estímulo de solicitações de eco ICMP ("pings") ao endereço de transmissão da sub-rede refletora. Os endereços de origem destes pacotes são falsificados para ser o endereço do destino final. Para cada pacote enviado pelo atacante, muitos anfitriões na sub-rede de refletor respondem. Isto inunda o destino final e desperdiça a largura de banda para ambas as vítimas.

Um ataque semelhante, chamado fraggle, utiliza difusões direcionadas da mesma forma, mas usa solicitações de eco de UDP em vez de solicitações de eco do Protocolo de mensagens de controle da Internet (ICMP). O ataque fraggle normalmente obtém um fator de amplificação menor e é muito menos popular que o smurf.

Os ataques de smurf são observados geralmente porque um link de rede se torna sobrecarregado. Uma descrição completa destes ataques, e de medidas da defesa, está na página de informação do ataque de recusa de serviço .

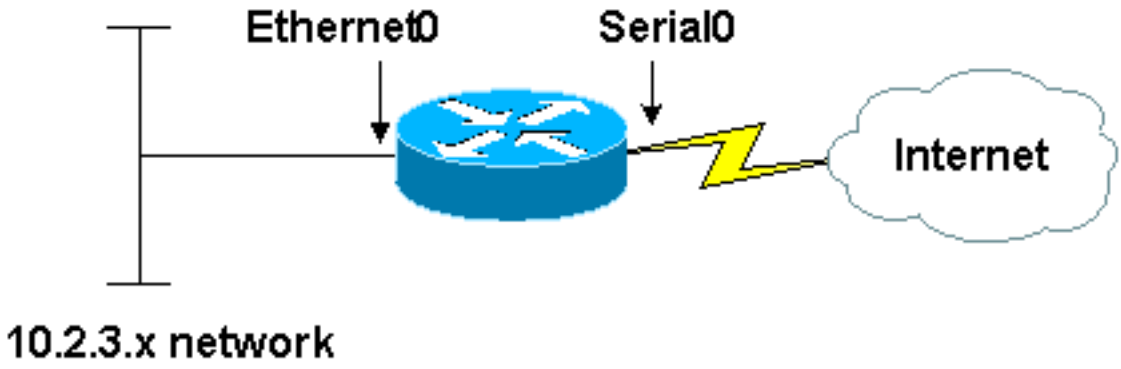
Outro ataque comum é a inundação de SYN, na qual uma máquina de destino é inundada com requisições de conexão de TCP. Os endereços de origem e as portas TCP da fonte dos pacotes de pedido de conexão randomized. A finalidade é forçar o host de destino a manter a informação de estado para muitas conexões que são terminadas nunca.

Geralmente, os ataques de inundações SYN são percebidos porque o host alvo (quase sempre um servidor HTTP ou SMTP) torna-se extremamente lento, sofre travamento ou fica suspenso. É igualmente possível para o tráfego que retorna do host de destino para causar o problema no Roteadores. Isto é porque este tráfego de retorno vai aos endereços de origem aleatório dos pacotes originais, ele falta as propriedades de localidade do tráfego IP “real”, e pode transbordar caches de rota. Nos Cisco routers, esse problema muitas vezes se manifesta quando o roteador está com falta de memória.

Juntos, programas de ataque smurf e de inundação de SYN são responsáveis pela grande maioria dos ataques de inundação de DoS reportados à Cisco e o rápido reconhecimento deles é muito importante. Ambos os ataques (assim como alguns da “ataques segunda série”, tais como inundações de ping) são reconhecidos facilmente quando você usa Listas de acesso de Cisco.

Uma lista de acesso de caracterização de DoS

Represente um roteador com duas relações. O ethernet0 é conectado a uma LAN interna em um negócio ou em um ISP pequeno. A serial 0 fornece uma conexão à Internet via um upstream do ISP. A taxa do pacote de entrada no serial0 “é cavilhada” na largura de banda de enlace completa, e os anfitriões no LAN são executado lentamente, causam um crash, penduram, ou mostram outros sinais de um ataque DoS. O local pequeno em que o roteador conecta não tem nenhum analisador de rede, e os povos lá tem quase nenhuma experiência em traços do analisador da leitura mesmo se os traços estão disponíveis.



Agora, supõe que você aplica uma lista de acessos enquanto esta saída mostra:

```
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 não filtra para fora nenhum tráfego de todo; todas as entradas são licenças. Entretanto, por categorizar os pacotes de maneiras úteis, a lista pode ser usada para tentar diagnosticar todos os três tipos de ataque: smurf, inundações de SYN, e fraggle.

Destino final do smurf

Se você emite o **comando show access-list**, você vê a saída similar a esta:

```
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)
```

A maioria do tráfego que chega na interface serial consiste em pacotes de resposta eco ICMP. Esta é provavelmente a assinatura de um ataque de smurf, e nosso local é o destino final, um pouco do que o refletor. Você pode recolher mais informação sobre o ataque quando você revisa a lista de acessos, porque esta saída mostra:

```
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
```

A alteração aqui é que a palavra-chave log-input foi adicionada à entrada da lista de acesso que corresponde ao tráfego suspeito. (Os Cisco IOS Software Release mais cedo de 11.2 faltam esta palavra-chave. Use a palavra-chave do "**log**" pelo contrário.) Isto causa o roteador à informação de registro sobre os pacotes que combinam a entrada de lista. Se você supõe que **registrar protegido** está configurado, você pode ver as mensagens que resultam com o **comando show log** (podem tomar um quando para que as mensagens acumulem devido à taxa que limita). As mensagens parecem similares a esta saída:

```
%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
```

Os endereços de origem dos pacotes de resposta de eco são aglomerados nos prefixos de endereço 192.168.212.0/24, 192.168.45.0/24, e 172.16.132.0/24. (Os endereços privados nas redes 192.168.x.x e 172.16.x.x não estariam no Internet; esta é uma ilustração de laboratório.) Isto é muito característico de um ataque de smurf, e os endereços de origem são os endereços dos refletores de smurf. Se você olha acima os proprietários destes blocos de endereço nos bases de dados apropriados do Internet “WHOIS”, você pode encontrar os administradores destas redes, e pede sua ajuda ao lidar com o ataque.

Éimportante, nessa altura de um incidente de smurf, lembrar que esses refletores são vitimas semelhantes e não atacantes. É extremamente raro ter os invasores utilizando os próprios endereços de origem em pacotes IP em qualquer inundação de DoS e impossível que eles façam isso em um ataque smurk em funcionamento. Qualquer endereço em um pacote de inundações deve ser assumido como sendo completamente falsificado ou o endereço de um tipo de vítima. A aproximação a mais produtiva para o destino final de um ataque de smurf é contactar os refletores, para pedi-los para reconfigurar suas redes para fechar o ataque, ou para pedi-lo seu auxílio em seguir o fluxo de estímulo.

Porque o dano ao destino final de um ataque de smurf é causado geralmente sobrecarregando do link recebido do Internet, não há frequentemente nenhuma resposta a não ser para contactar os refletores. Antes que os pacotes chegarem em toda a máquina sob o controle do alvo, a maioria do dano tem sido feito já.

Uma medida paliativa é solicitar ao provedor de rede upstream para que filtre todas as respostas de eco de ICMP ou todas as respostas de eco de ICMP de refletores específicos. Não se recomenda que você deixa isto meio o filtro no lugar permanentemente. Mesmo para um filtro provisório, somente as respostas de eco devem ser filtradas, não todos os pacotes ICMP. Uma outra possibilidade é ter o uso Qualidade de Serviço do provedor de upstream e avaliar a limitação de características para restringir a largura de banda disponível às respostas de eco. Uma limitação de largura de banda razoável pode ser deixada no lugar indefinidamente. Both of these aproximações dependem do equipamento do provedor de upstream que tem a capacidade necessária, e às vezes essa capacidade não está disponível.

Refletor do smurf

Se o tráfego de entrada consiste em requisições de eco um pouco do que respostas de eco (ou

seja se a primeira entrada de lista de acesso, um pouco do que a segunda, estava contando muito mais fósforos do que poderia razoavelmente ser esperado), você suspeitaria um ataque de smurf em que a rede era usada como um refletor, ou possivelmente uma inundação de ping simples. Em qualquer dos casos, se o ataque é um sucesso, você esperaria o lado de saída da linha de série ser inundado, assim como o lado de entrada. De fato, devido ao fator de ampliação, você esperaria o lado de saída ser sobrecarregado ainda mais do que o lado de entrada.

Há diversas maneiras de distinguir o ataque de smurf da inundação de ping simples:

- Os pacotes de estímulo de Smurf são enviados a um endereço de broadcast direcionado, um pouco do que a um endereço de unicast, visto que as inundações de ping ordinárias usam quase sempre unicasts. Você pode ver os endereços que usam as **palavras-chave de registro de entrada na** entrada de lista de acesso apropriada.
- Se você é usado como um refletor de smurf, há um número desproporcional de transmissões da saída no indicador da **relação da mostra no** lado de Ethernet do sistema, e geralmente um número desproporcional de transmissões enviadas no indicador do **tráfego da mostra IP**. Uma inundação de ping padrão não aumenta o tráfego de transmissão de background.
- Se você é usado como um refletor de smurf, há mais tráfego que parte para o Internet do que o tráfego entrante do Internet. Geralmente, há mais pacotes de saída do que pacotes de entrada na interface serial. Mesmo se o fluxo de estímulo enche completamente a interface de entrada, o córrego da resposta é maior do que o fluxo de estímulo, e as quedas de pacote de informação são contadas.

Um refletor de smurf tem mais opções do que o destino final de um ataque de smurf. Se um refletor escolhe fechar o ataque, o uso apropriado de **nenhuma transmissão direcionada IP** (ou de comandos não-IOS equivalentes) basta geralmente. Estes comandos pertencem em cada configuração, mesmo se não há nenhum ataque ativo. Para obter mais informações sobre da prevenção de seu equipamento da Cisco da utilização em um ataque de smurf, refira o melhoramento da Segurança em roteadores Cisco. Para obter mais informações gerais sobre dos ataques de smurf geralmente, e para obter informações sobre do equipamento que não é da Cisco de proteção, refira a página de informação do ataque de recusa de serviço .

Um refletor smurf está um passo mais próximo do invasor que é o destino final e, portanto, está em uma melhor posição para rastrear o ataque. Se você escolhe seguir o ataque, você precisa de trabalhar com os ISP envolvidos. Se você deseja ter alguma ação tomada quando você termina o traço, você precisa de trabalhar com agências de execução de lei apropriadas. Se você procura seguir um ataque, recomenda-se que você envolve a execução de lei o mais cedo possível. Consulte a seção de rastreio para obter informações técnicas sobre ataques de inundação de rastreio.

Fraggle

O ataque de fraggle é análogo ao de smurf, exceto pelo fato de que são usadas requisições de eco UDP (e não requisições de eco ICMP) para o fluxo de estímulo. A terceira e quarta linhas da lista de acesso identificam os ataques frágeis. A resposta apropriada para as vítimas é a mesma, salvo que o eco UDP é um serviço menos importante na maioria de redes do que é o eco ICMP. Consequentemente, você pode desabilitá-los completamente com menos consequências negativas.

Inundações de SYN

As quintas e sextas linhas da lista de acessos são:

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

O primeiro destas linhas combina todo o pacote de TCP com o jogo do bit ACK. Para nossas finalidades, o que importa realmente é que isso corresponde a qualquer pacote que não seja um TCP SYN. A segunda linha combina somente os pacotes que são TCP SYN. Uma inundação de SYN é identificada facilmente dos contadores nestas entradas de lista. No tráfego normal, os pacotes de TCP NON-SYN ultrapassam SYN pelo menos por um fator de dois, e geralmente mais como quatro ou cinco. Em uma inundação de SYN, os SYNs normalmente superam muito os pacotes de TCP não SYN.

A única condição de não-ataque que cria essa assinatura é uma sobrecarga maciça de requisições genuínas de conexão. Em geral, tal sobrecarga não chega inesperadamente e não envolve tantos pacotes SYN quanto a inundação SYN real. Também, as inundações de SYN contêm frequentemente pacotes com completamente endereços de origem inválido; usando as **palavras-chave de registro de entrada**, é possível ver se pedidos de conexão para vir de tais endereços.

Há um ataque chamado um “ataque de tabela de processo” que carregue alguma similaridade à inundação de SYN. No ataque de tabela de processo, as conexões de TCP são terminadas, a seguir permitidas cronometrar para fora sem um tráfego de protocolo mais adicional, visto que na inundação de SYN, simplesmente os pedidos de conexão inicial são enviados. Porque um ataque de tabela de processo exige a conclusão do handshake inicial do TCP, deve geralmente ser lançado com o uso do endereço IP de Um ou Mais Servidores Cisco ICM NT de uma máquina real a que o atacante tem o acesso (acesso geralmente roubado). Os ataques de tabela de processo consequentemente são distinguidos facilmente das inundações de SYN com o uso do registro do pacote. Todos os SYN em um ataque de tabela de processo vêm de um ou algum endereço, ou no máximo de uma ou alguma sub-rede.

As opções de resposta para as vítimas das inundações de SYN são muito limitadas. O sistema sob o ataque é geralmente um serviço importante, e obstruir o acesso ao sistema realiza geralmente o que o atacante quer. Muito o roteador e os produtos de firewall, incluindo Cisco, têm as características que podem ser usadas para reduzir o impacto das inundações de SYN. Mas, a eficácia destas características depende do ambiente. Para mais informação, refira a documentação para o Cisco IOS Firewall Feature Set, a documentação para os recursos de interceptação de TCP do Cisco IOS, e o melhoramento da Segurança em roteadores Cisco.

Épossível rastrear inundações de SYN, mas o processo de rastreamento exige a assistência de cada ISP ao longo do caminho, do atacante até a vítima. Se você decide tentar seguir uma inundação de SYN, contacte a execução de lei cedo sobre, e trabalhe com seu próprio fornecedor de serviço upstream. Veja a seção traça deste documento para detalhes no seguimento com o uso do equipamento da Cisco.

Outros ataques

Se você acredita que você está sob um ataque, e se você pode caracterizar esse ataque usando o origem de IP e os endereços de destino, os números de protocolo, e os números de porta, você pode usar Listas de acesso para testar sua hipótese. Crie uma entrada de lista de acesso que corresponda ao tráfego suspeito, aplique-a em uma interface apropriada e observe os contadores de correspondência ou registre o tráfego.

Caveats de registro e contador

O contador em uma entrada de lista de acesso conta todos os fósforos contra essa entrada. Se você aplica uma lista de acessos a duas relações, as contagens que você vê são contagens agregadas.

O registro de lista de acesso não mostra cada pacote que corresponde a uma entrada. O registro tem taxa limitada para evitar sobrecarga de CPU. Que registro mostra você é razoavelmente um exemplo representativo, mas não um rastreamento de pacotes completo. Recorde que há os pacotes que você não vê.

Em algumas versões de software, o registro de lista de acesso funciona somente em certos modos de switching. Se uma entrada de lista de acesso conta muitos fósforos, mas não registra nada, tente cancelar o cache de rota para forçar pacotes para ser processo comutado. Seja cuidadoso se você faz este pesadamente em roteadores carregados com muitas relações. Muito tráfego pode obter deixado cair quando o esconderijo for reconstruído. Use o Cisco Express Forwarding sempre que possível.

As Listas de acesso e o registro têm um impacto no desempenho, mas não grande. Seja cuidadoso no Roteadores que é executado mais do que na carga do percentual de CPU aproximadamente 80, ou quando você aplica Listas de acesso muito às interfaces de alta velocidade.

Rastreamento

Os endereços de origem dos pacotes DOS são ajustados quase sempre aos valores que não não têm nada fazer com os atacantes eles mesmos. Consequentemente, não são úteis na identificação dos atacantes. A única maneira confiável de identificar a origem de um ataque é rastreá-lo nó a nó através da rede. Este processo envolve a reconfiguração de roteadores e o exame da informação de registro. A cooperação por todos os operadores de rede ao longo do trajeto do atacante à vítima é exigida. A garantia dessa cooperação geralmente exige o envolvimento de órgãos de imposição da lei, que também deverão se envolver se for necessário tomar qualquer medida contra o atacante.

O processo de rastreamento para inundações DoS é relativamente simples. Partindo de um roteador (chamado "A") que sabidamente está transportando tráfego de inundação, é possível identificar o roteador (chamado de "B") a partir do qual A está recebendo o tráfego. Em seguida, faz-se login em B, e o roteador (designado como "C"), a partir do qual B está recebendo o tráfego, é localizado. Isso continua até a origem final ser encontrada.

Há diversas complicações neste método, que esta lista descreve:

- O “origem final” pode ser um computador que sejam comprometidos pelo atacante, mas que realmente é possuído e operado por uma outra vítima. Neste caso, seguir a inundação DoS é somente a primeira etapa.
- Os atacantes sabem que podem ser seguidos, e continuam geralmente seus ataques somente por um período limitado. Talvez não haja tempo suficiente para rastrear de verdade a inundação.
- Os ataques podem vir dos origens múltipla, especialmente se o atacante é relativamente sofisticado. É importante tentar identificar o máximo de origens possível.
- Os problemas de comunicação retardam o processo de traçado. Frequentemente uns ou

vários dos operadores de rede envolvidos não têm apropriadamente o grupo de trabalho capacitado disponível.
- Os interesses legais e políticos podem fazê-lo difícil atuar contra atacantes mesmo se se é encontrado.

A maioria de esforços para seguir a falha dos ataques DoS. Devido a isto, muitos operadores de rede tentam nem sequer seguir um ataque a menos que colocado sob a pressão. Muitos outro ataques “severos” do traço somente, com definições de deferimento do que é “severo.” Alguma assistência com um traço somente se a execução de lei é involvida.

Rastreando com "registro de entrada"

Se você escolhe seguir um ataque que passe através de um roteador Cisco, a maioria de maneira eficaz fazer isto é construir uma entrada de lista de acesso que combine o tráfego do ataque, anexa-lhe as **palavras-chave de registro de entrada**, e aplica-à lista de acessos de partida na relação através de que o fluxo de ataque é enviado para seu destino final. As entradas de registro produzidas pela lista de acessos identificam a interface do roteador através de que o tráfego chega, e, se a relação é uma conexão multiponto, dão o endereço da camada 2 do dispositivo de que é recebido. É possível então usar o endereço da camada 2 para identificar o próximo roteador na cadeia, utilizando-se, por exemplo, o comando show ip arp mac-address.

Inundação de SYN

A fim seguir uma inundação de SYN, você pode criar uma lista de acessos 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
```

Isto registra todos os pacotes SYN destinados para o host de destino, incluindo SYN legítimos. A fim identificar o trajeto real mais provável para o atacante, examine as entradas de registro em detalhe. Geralmente, a fonte da inundação é a fonte de que o número o maior de pacotes de harmonização chega. Os endereços IP de origem eles mesmos não significam nada. você está procurando interfaces e endereços MAC de origem. Às vezes é possível distinguir pacotes de inundação dos pacotes legítimos porque os pacotes de inundação podem ter endereços de origem inválido. Qualquer pacote cujo endereço de origem não for válido será provavelmente parte da inundação.

A inundação pode vir dos origens múltipla, embora esta seja relativamente incomum para inundações de SYN.

Estímulo de smurf

A fim seguir um fluxo de estímulo do smurf, use uma lista de acessos como este:

```
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 a primeira entrada não se restringe a pacotes destinados ao endereço de refletor. A razão para isto é que a maioria dos ataques de smurf utiliza redes refletoras múltiplas. Se você não é em contato com o destino final, você não pode conhecer todos os endereços do refletor. Enquanto seu traço obtém mais perto da fonte do ataque, você pode começar a ver requisições de eco ir cada vez mais aos destinos; este é um bom sinal.

Contudo, se você trata muito tráfego ICMP, isto pode gerar demasiada informação de registro para que você leia facilmente. Se isto acontece, você pode restringir o endereço de destino para ser um dos refletores que é sabido para ser usado. Uma outra tática útil é usar uma entrada que se aproveite do fato de que os netmasks de 255.255.255.0 são muito comuns no Internet. E, devido à forma como os atacantes localizam refletores de smurf, a probabilidade de os endereços de refletor efetivamente utilizados para ataques de smurf coincidirem com a máscara é muito maior. Os endereços de host que terminam em .0 ou em .255 são muito raros no Internet. Consequentemente, você pode construir um identificador relativamente específico para fluxos de estímulo do smurf enquanto esta saída mostra:

```
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
```

Com esta lista, você pode eliminar muitos dos pacotes do “ruído” de seu log, quando você ainda tiver uma boa possibilidade de observar fluxos de estímulo adicionais enquanto você obtém mais perto do atacante.

Rastreamento sem "registro de entrada"

A palavra-chave log-input está presente no Cisco IOS Software Releases 11.2 e posteriores e em determinados softwares com base no Release 11.1 criados especificamente para o mercado de provedores de serviços. Software mais antigo não suporta essa palavra-chave. Se você usa um roteador com software mais velho, você tem três opções viáveis:

- Crie uma lista de acessos sem registrar, mas com as entradas que combinam o tráfego suspeito. Aplique a lista no *lado de entrada de* cada relação por sua vez, e olhe os contadores. Procure relações com taxas altas do fósforo. Este método tem uma carga adicional de desempenho muito pequena, e é bom para a identificação das interfaces de origem. Sua maior desvantagem é que os endereços de origem da camada do enlace não são fornecidos e, portanto, tem maior utilidade para as linhas ponto-a-ponto.
- Crie entradas de lista de acesso com a palavra-chave registro (em oposição a registro de entrada). Aplique novamente a lista ao lado de entrada da cada interface em questão. Este método ainda não dá endereços MAC de origem, mas pode ser útil para considerar dados IP. Por exemplo, para verificar que uma corrente de pacote de informação é realmente parte de um ataque. O impacto no desempenho pode ser médio a elevado e um software mais novo executa um software melhor do que mais velho.
- Use o **comando debug ip packet detail** recolher a informação sobre pacotes. Esse método fornece endereços MAC, mas pode ter graves impactos no desempenho. É muito fácil errar com esse método e deixar um roteador sem condições de uso. Se você usa este método, certifique-se de que os switch do roteador o tráfego do ataque em rápido, em autônomo, ou o modo ótimo. Use uma lista de acessos para restringir a eliminação de erros somente à informação que você precisa realmente. Registre as informações de depuração no buffer de registro local, mas desligue o registro dessas informações nas sessões Telnet e no console. Se possível, faça com que alguém esteja fisicamente próximo ao roteador, para que ele possa ter o ciclo de energia necessário.Recorde que o **comando debug ip packet** não faz Exibir informação sobre pacotes comutados rapidamente. Você precisa de emitir o **comando clear ip cache** a fim capturar a informação. Cada **comando clear** dá-lhe um ou dois pacotes de resultado do debug.

Informações Relacionadas

- Kerberos
- Suporte Técnico e Documentação - Cisco Systems