Caracterizando e Rastreando Inundações de Pacote com Uso de Cisco Routers

Contents

Introduction

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 doS podem ser isolados quando você os compara às entradas da lista de acesso do software Cisco IOS®. Isso é valioso para filtrar ataques. Também é útil para quando você caracteriza ataques desconhecidos e para quando rastreia fluxos de pacotes "falsificados" de volta para suas fontes 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. No entanto, com versões recentes do software Cisco IOS, as listas de acesso e o registro da lista de acesso são os principais recursos para quando você caracteriza e rastreia ataques comuns.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

Conventions

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

Os ataques mais comuns de DoS

Uma grande variedade de ataques de DoS é possível. Mesmo que você ignore ataques que usam bugs de software para desligar sistemas com tráfego relativamente pequeno, o fato é que qualquer pacote IP que possa ser enviado pela rede pode ser usado para executar um ataque de inundação de DoS. Quando você está sob ataque, deve sempre considerar a possibilidade de que o que você vê é algo que não se enquadra nas categorias habituais.

Sujeito a caveat, contudo, vale lembrar que muitos ataques são semelhantes. Os invasores escolhem explorações comuns porque são particularmente eficazes, particularmente difíceis de rastrear ou porque as ferramentas estão disponíveis. Muitos invasores de DoS não têm habilidade ou motivação para criar suas próprias ferramentas e usar programas encontrados na 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 desses pacotes são falsificados para serem o endereço do destino final. Para cada pacote enviado pelo invasor, muitos hosts na sub-rede refletora respondem. Isso inunda o objetivo final e desperdiça 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 geralmente são notados porque um link de rede fica sobrecarregado. Uma descrição completa desses ataques e das medidas de defesa está na página Informações de Recusa de Ataques de Serviço.

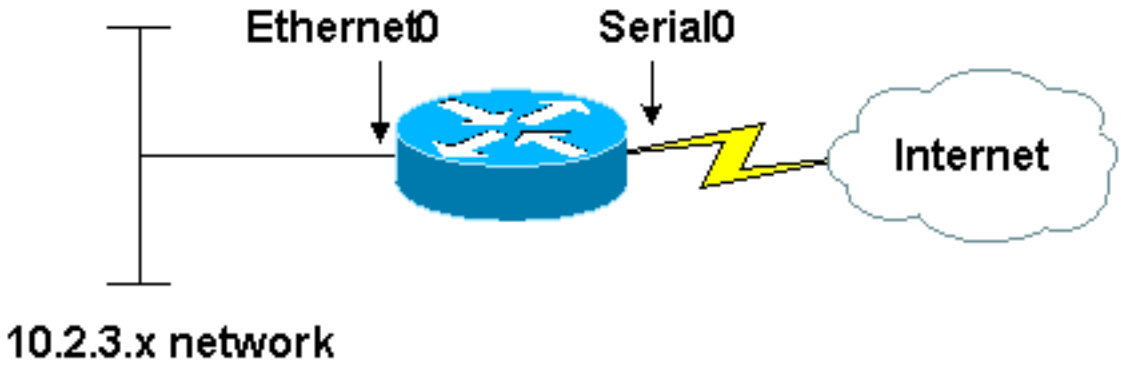
Outro ataque comum é a inundação de SYN, na qual uma máquina de destino é inundada com requisições de conexão de TCP. Os endereços de origem e as portas TCP de origem dos pacotes de solicitação de conexão são aleatórios. A finalidade é forçar o host de destino a manter informações de estado para muitas conexões que nunca foram concluídas.

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. Também é possível que o tráfego que retorna do host de destino cause problemas nos roteadores. Isso ocorre porque esse tráfego de retorno vai para os endereços de origem randomizados dos pacotes originais, ele não tem as propriedades locais do tráfego IP "real" e pode estourar caches de rotas. 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 ataques de "segundo nível", como inundações de ping) são facilmente reconhecidos quando você usa listas de acesso da Cisco.

Uma lista de acesso de caracterização de DoS

Imagine um roteador com duas interfaces. A Ethernet 0 está conectada a uma LAN interna em uma empresa ou em um pequeno ISP. A serial 0 fornece uma conexão à Internet via um upstream do ISP. A taxa de pacote de entrada na serial 0 é "pegged" (indexada) na largura de banda do link completo e os hosts na LAN são executados lentamente, travam, travam ou mostram outros sinais de um ataque de DoS. O pequeno local no qual o roteador se conecta não tem um analisador de rede e as pessoas lá têm pouca ou nenhuma experiência em ler rastreamentos do analisador, mesmo que os rastreamentos estejam disponíveis.



Agora, suponha que você aplique uma lista de acesso como 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 nenhum tráfego; todas as entradas são permissões. Entretanto, por categorizar os pacotes de maneiras úteis, a lista pode ser usada para tentar diagnosticar todos os três tipos de ataque: smurf, SYN flood e fraggle.

Destino final do smurf

Se você executar o comando **show access-list**, verá uma saída semelhante 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 maior parte do tráfego que chega na interface serial consiste em pacotes de resposta de eco ICMP. Esta é provavelmente a assinatura de um ataque smurf, e o nosso site é o alvo final, em vez do refletor. Você pode coletar mais informações sobre o ataque ao revisar a lista de acesso, como mostrado nesta saída:

```
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. (As versões do software Cisco IOS anteriores à 11.2 não têm essa palavra-chave. Use a palavra-chave "**log**".) Isso faz com que o roteador registre informações sobre pacotes que correspondem à entrada da lista. Se você supor que o **registro armazenado em buffer** está configurado, você pode ver as mensagens que resultam com o comando **show log** (pode levar um tempo para que as mensagens sejam acumuladas devido à limitação de taxa). As mensagens são semelhantes 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 agrupados 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 na Internet; esta é uma ilustração de laboratório.) Isso é muito característico de um ataque smurf, e os endereços de origem são os endereços dos refletores smurf. Se você procurar os proprietários desses blocos de endereços nos bancos de dados apropriados "whois" da Internet, poderá encontrar os administradores dessas redes e pedir ajuda para 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 abordagem mais produtiva para o alvo final de um ataque de smurf é entrar em contato com os refletores, seja para pedir que eles reconfigurem suas redes para desligar o ataque, ou para pedir assistência para rastrear o fluxo de estímulo.

Como o dano ao alvo final de um ataque smurf é geralmente causado pela sobrecarga do link de entrada da Internet, geralmente não há outra resposta além de entrar em contato com os refletores. Quando os pacotes chegam a qualquer máquina sob controle do destino, a maior parte dos danos já foi feita.

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 é recomendável que você deixe este tipo de filtro no lugar permanentemente. Mesmo para um filtro temporário, apenas as respostas de eco devem ser filtradas, não todos os pacotes ICMP. Outra possibilidade é fazer com que o provedor de upstream use recursos de qualidade de serviço e limitação de taxa para restringir a largura de banda disponível para respostas de eco. Uma limitação razoável de largura de banda pode ser mantida indefinidamente. Ambas as abordagens 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 solicitações de eco em vez de respostas de eco (em outras palavras, se a primeira entrada da lista de acesso, em vez da segunda, estivesse contando muito mais correspondências do que seria razoavelmente esperado), você suspeitaria de um ataque de smurf no qual a rede estava sendo usada como refletor, ou possivelmente uma simples inundação de ping. Em ambos os casos, se o ataque for um sucesso, você esperaria que o lado de saída da linha serial fosse trocado, assim como o lado de entrada. Na verdade, devido ao fator de amplificação, você esperaria que o lado de saída fosse ainda mais sobrecarregado do que o lado de entrada.

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

- Os pacotes de estímulo de smurf são enviados para um endereço de broadcast direcionado, em vez de para um endereço unicast, enquanto as inundações de ping comuns quase sempre usam unicasts. Você pode ver os endereços que usam a palavra-chave **log-input** na entrada da lista de acesso apropriada.
- Se você for usado como um refletor smurf, haverá um número desproporcional de broadcasts de saída na tela **show interface** no lado Ethernet do sistema e, geralmente, um número desproporcional de broadcasts enviados na tela **show ip traffic**. Uma inundação de ping padrão não aumenta o tráfego de broadcast de segundo plano.
- Se você for usado como um refletor smurf, há mais tráfego de saída para a Internet do que tráfego de entrada da Internet. Em geral, há mais pacotes de saída do que pacotes de entrada na interface serial. Mesmo que o fluxo de estímulo preencha completamente a interface de entrada, o fluxo de resposta é maior que o fluxo de estímulo, e as quedas de pacote são contadas.

Um refletor smurf tem mais opções do que o alvo final de um ataque smurf. Se um refletor optar por desligar o ataque, o uso apropriado de **no ip directed-broadcast** (ou comandos não IOS equivalentes) geralmente é suficiente. Esses comandos pertencem a todas as configurações, mesmo que não haja ataque ativo. Para obter mais informações sobre a prevenção do uso do equipamento da Cisco em um ataque smurf, consulte Melhorando a Segurança em Cisco Routers. Para obter informações mais gerais sobre ataques de smurf em geral, e para obter informações sobre como proteger equipamentos que não são da Cisco, consulte a página Informações sobre Ataques de Negação 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 optar por rastrear o ataque, precisará trabalhar com os ISPs envolvidos. Se você deseja que alguma ação seja tomada quando você concluir o rastreamento, você precisa trabalhar com as agências de polícia apropriadas. Se você procura rastrear um ataque, é recomendável que você envolva a aplicação da lei o mais rápido 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,

exceto que o eco UDP é um serviço menos importante na maioria das redes do que o eco ICMP. Portanto, você pode desativá-los completamente com menos consequências negativas.

Inundações de SYN

A quinta e a sexta linhas da lista de acesso são:

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

A primeira dessas linhas corresponde a qualquer pacote TCP com o bit ACK definido. Para nossas finalidades, o que importa realmente é que isso corresponde a qualquer pacote que não seja um TCP SYN. A segunda linha corresponde somente aos pacotes que são TCP SYNs. Uma inundação de SYN é facilmente identificada dos contadores nessas entradas da lista. No tráfego normal, os pacotes TCP não-SYN superam os SYNs em pelo menos 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. Além disso, as inundações SYN geralmente contêm pacotes com endereços de origem completamente inválidos; usando a palavra-chave **log-input**, é possível ver se as solicitações de conexão vêm desses endereços.

Há um ataque chamado "ataque à tabela de processos" que tem alguma semelhança com a inundação SYN. No ataque da tabela de processos, as conexões TCP são concluídas e, em seguida, é permitido o tempo limite sem nenhum tráfego de protocolo adicional, enquanto na inundação SYN, somente as solicitações de conexão inicial são enviadas. Como um ataque de tabela de processo requer a conclusão do handshake inicial do TCP, ele deve geralmente ser iniciado com o uso do endereço IP de uma máquina real à qual o invasor tem acesso (geralmente acesso roubado). Os ataques à tabela de processos são, portanto, facilmente diferenciados das inundações SYN com o uso de registro de pacotes. Todos os SYNs em um ataque de tabela de processo vêm de um ou alguns endereços ou, no máximo, de uma ou algumas sub-redes.

As opções de resposta para as vítimas das inundações SYN são muito limitadas. O sistema sob ataque é geralmente um serviço importante, e bloquear o acesso ao sistema normalmente realiza o que o invasor deseja. Muitos produtos de roteador e firewall, incluindo os da Cisco, têm recursos que podem ser usados para reduzir o impacto de inundações SYN. Mas a eficácia desses recursos depende do ambiente. Para obter mais informações, consulte a documentação do conjunto de recursos do Cisco IOS Firewall, a documentação do recurso Cisco IOS TCP Intercept e Melhorando a Segurança em Cisco Routers.

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 decidir tentar rastrear uma inundação SYN, entre em contato com a aplicação da lei no início e trabalhe com seu próprio provedor de serviços upstream. Consulte a seção de rastreamento deste documento para obter detalhes sobre como rastrear o uso de equipamentos Cisco.

Outros ataques

Se você acredita que está sob um ataque e se puder caracterizar esse ataque usando endereços IP de origem e destino, números de protocolo e números de porta, poderá 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 da lista de acesso conta todas as correspondências em relação a essa entrada. Se você aplicar uma lista de acesso a duas interfaces, as contagens vistas serão 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. O registro mostra que você é uma amostra razoavelmente representativa, mas não um rastreamento de pacote completo. Lembre-se de que há 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 da lista de acesso conta muitas correspondências, mas não registra nada, tente limpar o cache da rota para forçar os pacotes a serem comutados no processo. Tenha cuidado se fizer isso em roteadores altamente carregados com muitas interfaces. Muito tráfego pode ser descartado enquanto o cache é recriado. Use o Cisco Express Forwarding sempre que possível.

As listas de acesso e o registro têm um impacto no desempenho, mas não um impacto grande. Tenha cuidado com roteadores que executam com mais de 80% de carga da CPU ou quando aplica listas de acesso a interfaces de alta velocidade.

Rastreamento

Os endereços de origem dos pacotes DoS são quase sempre definidos como valores que não têm nada a ver com os próprios invasores. Portanto, eles não são úteis na identificação dos invasores. A única maneira confiável de identificar a origem de um ataque é rastreá-lo nó a nó através da rede. Esse processo envolve a reconfiguração dos roteadores e o exame das informações de log. É necessária a cooperação de todos os operadores de rede ao longo do caminho do invasor até a vítima. 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 várias complicações neste método, que esta lista descreve:

- A "fonte final" pode ser um computador que foi comprometido pelo invasor, mas que na verdade é de propriedade e operado por outra vítima. Nesse caso, rastrear a inundação do DoS é apenas o primeiro passo.
- Os invasores sabem que podem ser rastreados e, em geral, continuar seus ataques por um tempo limitado. Talvez não haja tempo suficiente para rastrear de verdade a inundação.
- Os ataques podem vir de várias fontes, especialmente se o invasor for relativamente

sofisticado. É importante tentar identificar o máximo de origens possível.
- Problemas de comunicação retardam o processo de rastreamento. Frequentemente, um ou mais dos operadores de rede envolvidos não têm pessoal adequadamente qualificado disponível.
- Preocupações jurídicas e políticas podem dificultar a ação contra os invasores, mesmo que se encontrem.

A maioria dos esforços para rastrear ataques de DoS falha. Por causa disso, muitos operadores de rede nem sequer tentam rastrear um ataque a menos que estejam sob pressão. Muitos outros rastreiam apenas ataques "graves", com definições diferentes do que é "grave". Alguns assistem com um rastreamento apenas se a aplicação da lei estiver envolvida.

Rastreando com "registro de entrada"

Se você optar por rastrear um ataque que passa por um roteador Cisco, a maneira mais eficaz de fazer isso é construir uma entrada da lista de acesso que corresponda ao tráfego de ataque, anexar a palavra-chave **log-input** a ele e aplicar a lista de acesso de saída na interface através da qual o fluxo de ataque é enviado para seu destino final. As entradas de log produzidas pela lista de acesso identificam a interface do roteador através da qual o tráfego chega e, se a interface for uma conexão multiponto, fornecem o endereço da Camada 2 do dispositivo do qual ele 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

Para rastrear uma inundação SYN, você pode criar uma lista de acesso semelhante 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
```

Registra todos os pacotes SYN destinados ao host de destino, incluindo SYNs legítimos. Para identificar o caminho real mais provável para o invasor, examine as entradas de log em detalhes. Em geral, a origem da inundação é a origem da qual o maior número de pacotes correspondentes chega. Os próprios endereços IP de origem não significam nada. você está procurando interfaces e endereços MAC de origem. Às vezes, é possível distinguir pacotes de inundação de pacotes legítimos porque os pacotes de inundação podem ter endereços de origem inválidos. Qualquer pacote cujo endereço de origem não for válido será provavelmente parte da inundação.

A inundação pode vir de várias fontes, embora isso seja relativamente incomum para inundações SYN.

Estímulo de smurf

Para rastrear um fluxo de estímulo smurf, use uma lista de acesso como esta:

```
access-list 169 permit icmp any any echo 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 estiver em contato com o destino final, talvez não saiba todos os endereços do refletor. À

medida que seu rastreamento se aproxima da origem do ataque, você pode começar a ver solicitações de eco indo para mais e mais destinos; este é um bom sinal.

No entanto, se você lidar com uma grande quantidade de tráfego ICMP, isso pode gerar muita informação de registro para que você leia facilmente. Se isso acontecer, você poderá restringir o endereço de destino para ser um dos refletores conhecidos por serem usados. Outra tática útil é usar uma entrada que aproveite o fato de que as máscaras de rede 255.255.255.0 são muito comuns na 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 .255 são muito incomuns na Internet. Portanto, você pode criar um reconhecedor relativamente específico para fluxos de estímulos de smurf conforme mostrado nesta saída:

```
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
```

Com essa lista, você pode eliminar muitos dos pacotes de "ruído" do seu registro, enquanto ainda tem uma boa chance de notar fluxos de estímulo adicionais à medida que se aproxima do invasor.

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 antigo, você tem três opções viáveis:

- Crie uma lista de acesso sem registro, mas com entradas que correspondam ao tráfego suspeito. Aplique a lista no lado *de entrada* de cada interface e observe os contadores. Procure interfaces com altas taxas de correspondência. Esse método tem uma sobrecarga de desempenho muito pequena e é bom para a identificação de 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. Esse método ainda não fornece endereços MAC de origem, mas pode ser útil para ver dados IP. Por exemplo, para verificar se um fluxo de pacotes realmente faz parte de um ataque. O impacto no desempenho pode ser moderado a alto e o software mais novo tem melhor desempenho do que o software mais antigo.
- Use o comando **debug ip packet detail** para coletar informações 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 usar esse método, certifique-se de que o roteador comute o tráfego de ataque no modo rápido, autônomo ou ideal. Use uma lista de acesso para restringir a depuração somente às informações de que você realmente precisa. 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.Lembre-se de que o comando **debug ip packet** não exibe informações sobre pacotes comutados rapidamente. Você precisa emitir o comando **clear ip cache** para capturar informações. Cada comando **clear** fornece um ou dois pacotes de saída de

depuração.

Informações Relacionadas

- Kerberos
- Suporte Técnico e Documentação - Cisco Systems