Definindo estratégias para proteger contra o ataque de recusa de serviço TCP SYN

Índice

Resumo
Pré-requisitos
Requisitos
Componentes Utilizados
Convenções
Descrição do problema
O ataque TCP SYN
Defendendo-se contra ataques nos dispositivos da rede
Dispositivos atrás de firewalls
Dispositivos que oferecem serviços disponíveis publicamente (servidores de e-mail, servidores públicos da Web)
Evitando que uma rede hospede inconscientemente um ataque
Evitando a transmissão de endereços IP inválidos
Evitando recebimento de endereços de IP inválidos
Informações Relacionadas

Resumo

Existe um ataque de serviço potencial em provedores de serviço de Internet (ISPs) direcionado a dispositivos de rede.

- Ataque SYN de TCP: Um remetente transmite um volume de conexões que não possa ser terminado. Isso faz com que as filas de conexões sejam preenchidas e, conseqüentemente, o atendimento aos usuários TCP legítimos seja recusado.

Este documento contém uma descrição técnica de como possíveis ataques TCP SYN ocorrem e os métodos sugeridos para utilização do Cisco IOS Software como defesa.

Nota: O software do Cisco IOS 11.3 tem uma característica para impedir ativamente ataques do serviço de recuso do TCP. Esta característica é descrita no documento que configura o TCP Intercept (impeça ataques de recusa de serviço).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Convenções

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

Descrição do problema

O ataque TCP SYN

Quando uma conexão de TCP normal é iniciada, um host de destino recebe um pacote SYN (sincronização/início) a partir de um host de origem e envia de volta um SYN ACK (Reconhecimento de sincronização). O host de destino deve então ouvir um ACK (reconheça) do SYN ACK antes que a conexão esteja estabelecida. Isto é referido como “o cumprimento de três vias TCP.”

Enquanto aguarda o ACK para o SYN ACK, uma fila de conexão de tamanho finito no host de destino mantém o controle das conexões aguardando conclusão. Esta fila esvazia tipicamente rapidamente desde que o ACK é esperado chegar alguns milissegundos após o SYN ACK.

O ataque SYN em TCP explora esse projeto ao fazer um host de origem de ataque gerar pacotes SYN no TCP com endereços de origem aleatórios em direção ao host de uma vítima. O host de destino da vítima envia um SYN ACK de volta ao endereço de origem aleatório e adiciona uma entrada à fila de conexão. Como o SYN ACK está destinado para um host incorreto ou inexistente, a última parte do "handshake de três vias" nunca é concluída e a entrada permanece na fila de conexão até que o temporizador expire, geralmente em torno de um minuto. Gerando pacotes SYN de TCP falsos dos endereços IP de Um ou Mais Servidores Cisco ICM NT aleatórios em uma taxa rápida, é possível encher acima a fila de conexão e negar serviços TCP (tais como o email, a transferência de arquivo, ou o WWW) aos usuários legítimos.

Não há nenhuma maneira fácil seguir o autor do ataque porque o endereço IP de Um ou Mais Servidores Cisco ICM NT da fonte é forjado.

As manifestações externas do problema incluem a incapacidade receber o email, a incapacidade aceitar conexões ao WWW ou aos serviços de FTP, ou as um grande número conexões de TCP em seu host no estado SYN_RCVD.

Defendendo-se contra ataques nos dispositivos da rede

Dispositivos atrás de firewalls

O ataque TCP SYN é caracterizado por um influxo de pacotes SYN dos endereços IP de origem aleatória. Todo o dispositivo atrás de um Firewall que pare pacotes SYN de entrada é protegido já deste modo de ataque e de nenhuma ação mais adicional é precisado. Os exemplos dos Firewall incluem um Firewall do intercâmbio de Internet privada (PIX) de Cisco ou um roteador Cisco configurado com Listas de acesso. Para exemplos de como estabelecer Listas de acesso em um roteador Cisco, refira por favor

Dispositivos que oferecem serviços disponíveis publicamente (servidores de e-mail, servidores públicos da Web)

Impedir ataques SYN de endereços IP aleatórios em dispositivos protegidos por firewalls é relativamente simples, uma vez que você pode usar listas de acesso para limitar explicitamente os acessos recebidos para alguns endereços IP selecionados. Contudo, no caso de um servidor de web público ou de um mail server que enfrentam o Internet, não há nenhuma maneira de determinar que endereços de origem do IP recebido são amigáveis e quais são hostis. Portanto, não há nenhuma defesa de corte contra um ataque de endereço de IP aleatório. Várias opções estão disponíveis para hosts:

- Aumente o tamanho da fila de conexão (fila SYN ACK).
- Diminua o intervalo que espera o cumprimento de três vias.
- Empregue correções de programa do software de fornecedor para detectar e contornar o problema (se disponível).

Você deve contactar seu vendedor do host para ver se criaram correções de programa específicas para endereçar o ataque TCP SYN ACK.

Nota: Filtrar endereços IP de Um ou Mais Servidores Cisco ICM NT no server é ineficaz desde que um atacante pode variar seu endereço IP de Um ou Mais Servidores Cisco ICM NT, e o endereço pode ou não pode ser o mesmo que aquele de um host legítimo.

Evitando que uma rede hospede inconscientemente um ataque

Como o principal mecanismo desse ataque de recusa de serviço é a geração de tráfego originário de endereços IP aleatórios, recomendamos a filtragem do tráfego destinado à Internet. O conceito básico é desativar pacotes que tenham endereços IP de origem inválidos quando eles entrarem na Internet. Isso não impede um ataque de negação de serviço na rede, mas ajudará a excluir as partes atacadas a excluir o seu local como a fonte do ataque. Além, faz sua rede menos atrativa como uma base para esta classe de ataque.

Evitando a transmissão de endereços IP inválidos

Ao filtrar pacotes nos seus roteadores que conectam sua rede à Internet, você pode permitir que apenas pacotes com endereços IP de origem válidos saiam da sua rede e entrem na Internet.

Por exemplo, se sua rede consiste na rede 172.16.0.0, e seu roteador conecta a seu ISP usando uma relação da série 0/1, você pode aplicar a lista de acessos como segue:

```
access-list 111 permit ip 172.16.0.0 0.0.255.255 any
access-list 111 deny ip any any log

interface serial 0/1
ip access-group 111 out
```

Nota: A última linha da lista de acesso determina se há tráfego de entrada na Internet com endereço de origem inválido. Não é crucial ter esta linha, mas ela ajudará a localizar a origem de possíveis ataques.

Evitando recebimento de endereços de IP inválidos

Para os ISP que proporcionam o serviço para terminar redes, nós recomendamos altamente a validação de pacote de entrada de seus clientes. Isso pode ser obtido pelo uso de filtros de pacotes de entrada nos roteadores de borda.

Por exemplo, se seus clientes têm os seguintes network number conectados a seu roteador através de uma interface serial nomeada "serial 1/0", você pode criar a seguinte lista de acessos:

```
The network numbers are 192.168.0.0 to 192.168.15.0, and 172.18.0.0.

access-list 111 permit ip 192.168.0.0 0.0.15.255 any
access-list 111 permit ip 172.18.0.0 0.0.255.255 any
access-list 111 deny ip any any log

interface serial 1/0
ip access-group 111 in
```

Nota: A última linha da lista de acesso determina se existe tráfego com endereços de origem inválidos entrando na Internet. Não é crucial ter esta linha, mas ajudará a localizar a origem de um possível ataque.

Este assunto foi discutido em algum detalhe na lista de endereços do [North-american Network Operator1s Group] NANOG. Os arquivos de lista são encontrados em: http://www.merit.edu/mail.archives/nanog/index.html

Para uma descrição detalhada do ataque do seviço da recusa do TCP SYN e da falsificação de IP, veja: http://www.cert.org/advisories/CA-1996-21.html

http://www.cert.org/advisories/CA-1995-01.html

Informações Relacionadas

- Suporte Técnico - Cisco Systems