Definição de estratégias para proteção contra ataques de negação de serviço TCP SYN

Contents

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 podem ser concluídas. 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.

Observação: o software Cisco IOS 11.3 tem um recurso para impedir ativamente ataques de negação de serviço TCP. Este recurso é descrito no documento Configurando a interceptação TCP (Impedir ataques de negação de serviço).

Prerequisites

Requirements

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. All of the devices used in this document started with a cleared (default) configuration. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Conventions

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 ouvir um ACK (confirmação) do SYN ACK antes de estabelecer a conexão. Isso é conhecido como "handshake triplo do 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. Essa fila normalmente esvazia rapidamente, pois espera-se que o ACK chegue 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. Ao gerar pacotes SYN de TCP falsos de endereços IP aleatórios em uma taxa rápida, é possível preencher a fila de conexão e negar serviços TCP (como e-mail, transferência de arquivos ou WWW) a usuários legítimos.

Não há maneira fácil de rastrear o originador do ataque porque o endereço IP da origem é forjado.

As manifestações externas do problema incluem incapacidade de obter e-mail, incapacidade de aceitar conexões com serviços WWW ou FTP ou um grande número de conexões 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. Qualquer dispositivo por trás de um firewall que interrompa pacotes SYN de entrada já está protegido contra esse modo de ataque e nenhuma ação adicional é necessária. Exemplos de firewalls incluem um firewall Cisco Private Internet Exchange (PIX) ou um roteador Cisco configurado com listas de acesso. Para obter exemplos de como configurar listas de acesso em um roteador Cisco, consulte o documento Aumentando a segurança em redes IP.

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. No entanto, no caso de um servidor web público ou de um servidor de correio com acesso à Internet, não há como determinar quais endereços IP de origem recebidos 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 tempo limite de espera pelo handshake triplo.
- Utilize patches de software do fornecedor para detectar e contornar o problema (se disponível).

Você deve entrar em contato com o fornecedor do host para ver se eles criaram patches específicos para lidar com o ataque TCP SYN ACK.

Observação: a filtragem de endereços IP no servidor não é eficaz, pois um invasor pode variar seu endereço IP e o endereço pode ou não ser o mesmo 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 disso, torna sua rede menos atraente como base para essa 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 se conecta ao ISP usando uma interface serial 0/1, você pode aplicar a lista de acesso da seguinte maneira:

```
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
```

Observação: a última linha da lista de acesso determina se há tráfego com um endereço de origem inválido entrando na Internet. 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 ISPs que fornecem serviço para redes finais, recomendamos altamente a validação de pacotes 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 tiverem os seguintes números de rede conectados ao roteador através de uma interface serial chamada "serial 1/0", você poderá criar a seguinte lista de acesso:

```
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
```

Observação: a última linha da lista de acesso determina se há 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 tópico foi discutido em alguns detalhes na lista de discussão do NANOG [North American Network Operator1s Group]. Os arquivos da lista estão localizados em: http://www.merit.edu/mail.archives/nanog/index.html

Para obter uma descrição detalhada do ataque de negação de serviço TCP SYN e falsificação de IP, consulte: http://www.cert.org/advisories/CA-1996-21.html

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

Informações Relacionadas

- Suporte Técnico - Cisco Systems