Définition de stratégies par rapport aux attaques par déni de service TCP SYN

Contenu

Résumé

Il existe une attaque de déni de service potentielle chez les fournisseurs d'accès à Internet (FAI) qui cible les périphériques réseau.

- **Attaque SYN TCP** : Un expéditeur transmet un volume de connexions qui ne peut pas être terminé. Cela entraîne le remplissage des files d'attente de connexion, refusant ainsi le service aux utilisateurs TCP légitimes.

Ce document contient une description technique de la manière dont se produit l'attaque TCP SYN potentielle et des méthodes suggérées pour utiliser le logiciel Cisco IOS pour se défendre contre cette attaque.

Remarque : le logiciel Cisco IOS 11.3 dispose d'une fonctionnalité permettant d'empêcher activement les attaques par déni de service TCP. Cette fonctionnalité est décrite dans le document Configuration de l'interception TCP (Empêcher les attaques par déni de service).

Conditions préalables

Conditions requises

Aucune condition préalable spécifique n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Description du problème

Attaque TCP SYN

Lorsqu'une connexion TCP normale démarre, un hôte de destination reçoit un paquet SYN (synchronisation/démarrage) d'un hôte source et renvoie un ACK SYN (synchronisation de l'accusé de réception). L'hôte de destination doit alors entendre un accusé de réception (accuser réception) de l'accusé de réception SYN avant l'établissement de la connexion. On parle alors de « connexion TCP en trois étapes ».

En attendant l'ACK vers l'ACK SYN, une file d'attente de connexion de taille limitée sur l'hôte de destination conserve le suivi des connexions en attente d'achèvement. En règle générale, cette file d'attente se vide rapidement, car l'ACK devrait arriver quelques millisecondes après l'ACK SYN.

L'attaque SYN TCP exploite cette conception en demandant à un hôte source d'attaque de générer des paquets SYN TCP avec des adresses source aléatoires vers un hôte victime. L'hôte de destination de la victime renvoie un ACK SYN à l'adresse source aléatoire et ajoute une entrée à la file d'attente de connexion. Puisque l'ACK SYN est destiné à un hôte incorrect ou inexistant, la dernière partie de la « connexion en trois étapes » n'est jamais terminée et l'entrée reste dans la file d'attente de connexion jusqu'à l'expiration d'un compteur, généralement pendant environ une minute. En générant rapidement des paquets SYN TCP factices à partir d'adresses IP aléatoires, il est possible de remplir la file d'attente de connexion et de refuser les services TCP (tels que les e-mails, le transfert de fichiers ou le WWW) aux utilisateurs légitimes.

Il n'existe aucun moyen simple de retracer l'auteur de l'attaque car l'adresse IP de la source est falsifiée.

Les manifestations externes du problème incluent l'incapacité d'obtenir des e-mails, l'incapacité d'accepter les connexions aux services WWW ou FTP, ou un grand nombre de connexions TCP sur votre hôte dans l'état SYN_RCVD.

Protection contre les attaques sur les périphériques réseau

Périphériques derrière les pare-feu

L'attaque SYN TCP se caractérise par un afflux de paquets SYN provenant d'adresses IP source aléatoires. Tout périphérique derrière un pare-feu qui arrête les paquets SYN entrants est déjà protégé contre ce mode d'attaque et aucune autre action n'est nécessaire. Parmi les pare-feu, citons un pare-feu PIX (Private Internet Exchange) ou un routeur Cisco configuré avec des listes d'accès. Pour obtenir des exemples de configuration des listes d'accès sur un routeur Cisco, reportez-vous au document Renforcer la sécurité sur les réseaux IP.

Périphériques Offrant Des Services Publics (Serveurs De Messagerie, Serveurs Web Publics)

Empêcher les attaques SYN sur les périphériques derrière les pare-feu à partir d'adresses IP aléatoires est relativement simple car vous pouvez utiliser des listes d'accès pour limiter explicitement l'accès entrant à quelques adresses IP sélectionnées. Cependant, dans le cas d'un serveur Web public ou d'un serveur de messagerie faisant face à Internet, il n'y a aucun moyen de déterminer quelles adresses IP source entrantes sont conviviales et lesquelles ne le sont pas. Par conséquent, il n'existe aucune défense claire contre une attaque à partir d'une adresse IP aléatoire. Plusieurs options sont disponibles pour les hôtes :

- Augmenter la taille de la file d'attente de connexion (file d'attente SYN ACK).
- Réduire le délai d'attente pour la connexion en trois étapes.
- Utilisez les correctifs logiciels du fournisseur pour détecter et contourner le problème (le cas échéant).

Contactez le fournisseur de votre hôte pour savoir s'il a créé des correctifs spécifiques pour répondre à l'attaque TCP SYN ACK.

Remarque : le filtrage des adresses IP sur le serveur est inefficace car un pirate peut modifier son adresse IP et l'adresse peut être identique ou non à celle d'un hôte légitime.

Empêcher un réseau d'héberger involontairement une attaque

Étant donné qu'un mécanisme principal de cette attaque par déni de service est la génération du trafic provenant d'adresses IP aléatoires, nous recommandons de filtrer le trafic destiné à Internet. Le concept de base est de jeter les paquets avec des adresses IP source non valides lorsqu'ils pénètrent sur Internet. Cela n'empêche pas une attaque par déni de service sur votre réseau, mais aide les parties attaquées à exclure votre emplacement en tant que source de l'attaquant. En outre, il rend votre réseau moins attrayant en tant que base de cette classe d'attaque.

Prévention de la transmission d'adresses IP non valides

En filtrant les paquets sur vos routeurs qui connectent votre réseau à Internet, vous pouvez autoriser uniquement les paquets avec des adresses IP source valides à quitter votre réseau et à accéder à Internet.

Par exemple, si votre réseau se compose du réseau 172.16.0.0 et que votre routeur se connecte à votre FAI à l'aide d'une interface série 0/1, vous pouvez appliquer la liste d'accès comme suit :

```
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
```

Remarque : La dernière ligne de la liste d'accès détermine s'il y a un trafic avec une adresse source non valide entrant sur Internet. Il n'est pas essentiel d'avoir cette ligne, mais elle aidera à localiser la source des attaques possibles.

Prévention de la réception d'adresses IP non valides

Pour les FAI qui fournissent des services aux réseaux finaux, nous recommandons fortement la validation des paquets entrants de vos clients. Pour ce faire, vous pouvez utiliser des filtres de paquets entrants sur vos routeurs périphériques.

Par exemple, si vos clients ont les numéros de réseau suivants connectés à votre routeur via une interface série nommée « serial 1/0 », vous pouvez créer la liste d'accès suivante :

```
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
```

Remarque : La dernière ligne de la liste d'accès détermine s'il y a un trafic avec des adresses source non valides qui pénètre sur Internet. Il n'est pas essentiel d'avoir cette ligne, mais elle aidera à localiser la source de l'attaque possible.

Ce sujet a été abordé en détail dans la liste de diffusion NANOG [North American Network Operator1s Group]. Les archives de la liste se trouvent à l'adresse : http://www.merit.edu/mail.archives/nanog/index.html

Pour obtenir une description détaillée de l'attaque par déni de service SYN TCP et de l'usurpation d'adresse IP, reportez-vous à la section : http://www.cert.org/advisories/CA-1996-21.html

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

Informations connexes

- Support technique - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.