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

Contenu

Abstrait

Il y a une attaque de refus de service potentielle aux fournisseurs de services d'Internet (ISP) des périphériques de ce réseau de cibles.

- **Attaque de synchronisation de TCP** : Un expéditeur transmet un volume de connexions qui ne peuvent pas être terminées. Ceci fait remplir les files d'attente de connexion, refusant de ce fait le service pour légitimer des utilisateurs de TCP.

Ce document contient une description technique de la façon dont l'attaque potentielle de synchronisation de TCP se produit et a suggéré des méthodes pour l'usage du logiciel de Cisco IOS pour défendre contre lui.

Remarque: Le logiciel du Cisco IOS 11.3 a une caractéristique pour empêcher activement des attaques par déni de service de TCP. Cette caractéristique est décrite dans le document configurant l'Interception TCP (empêchez les attaques par déni de service).

Conditions préalables

Conditions requises

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

Composants utilisés

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. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). 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

L'attaque de synchronisation de TCP

Quand les débuts normaux d'une connexion TCP, une destination host reçoit une synchronisation (synchronisez/paquet de début) d'un hôte de source et renvoyez une synchronisation ACK (synchronisez reconnaissent). La destination host doit alors entendre un ACK (reconnaissez) de la synchronisation ACK avant que la connexion soit établie. Ceci désigné sous le nom du « connexion TCP à trois. »

Tout en attendant l'ACK à la synchronisation ACK, une file d'attente de connexion de taille finie sur la destination host maintient des connexions attendant d'être terminé. Cette file d'attente vide typiquement rapidement puisqu'on s'attend à ce que l'ACK arrive quelques millisecondes après la synchronisation ACK.

L'attaque de synchronisation de TCP exploite cette conception en ayant un hôte de attaque de source génèrent des paquets de synchronisation de TCP avec des adresses sources aléatoires vers un hôte victime. Le hôte de destination victime envoie une synchronisation ACK de nouveau à l'adresse source aléatoire et ajoute une entrée à la file d'attente de connexion. Puisque la synchronisation ACK est destinée à un hôte incorrect ou inexistant, la dernière partie de la « connexion en trois étapes » n'est jamais terminée et l'entrée demeure dans la file d'attente de connexion jusqu'à ce qu'un temporisateur expire, typiquement pour environ une minute. En générant de faux paquets de synchronisation de TCP des adresses IP aléatoires à une vitesse rapide, il est possible de remplir la file d'attente de connexion et de refuser des services de TCP (tels que le courrier électronique, le transfert de fichiers, ou le WWW) aux utilisateurs légitimes.

Il n'y a aucune méthode facile de tracer le créateur de l'attaque parce que l'adresse IP de la source est modifiée.

Les manifestations externes du problème incluent l'incapacité d'obtenir le courrier électronique, l'incapacité de recevoir des connexions aux services de WWW ou de FTP, ou un grand nombre de connexions TCP sur votre hôte dans l'état SYN_RCVD.

Défense contre des attaques sur des périphériques de réseau

Périphériques derrière des Pare-feu

L'attaque de synchronisation de TCP est caractérisée par un afflux des paquets de synchronisation des adresses IP aléatoires de source. N'importe quel périphérique derrière un Pare-feu qui arrête les paquets d'arrivée de synchronisation est déjà protégé contre ce mode d'attaque et d'aucune action supplémentaire est nécessaire. Les exemples des Pare-feu incluent un Pare-feu du Private Internet Exchange de Cisco (PIX) ou un routeur de Cisco configuré avec des Listes d'accès. Pour des exemples de la façon installer des Listes d'accès sur un routeur de Cisco, référez-vous s'il vous plaît à la Sécurité croissante de document sur des réseaux IP.

Périphériques offrant publiquement - des services disponibles (serveurs de messagerie, serveurs Web publics)

L'empêchement des attaques de synchronisation sur des périphériques derrière des Pare-feu des adresses IP aléatoires est relativement simple puisque vous pouvez employer des Listes d'accès pour limiter explicitement l'accès entrant à une minorité d'adresses IP. Cependant, dans le cas d'un web server ou d'un serveur de messagerie public faisant face à l'Internet, il n'y a aucune manière de déterminer quelles adresses entrantes de source IP sont amicales et ce qui sont peu amicales. Par conséquent, il n'y a aucune défense définie contre une attaque à partir d'une adresse IP aléatoire. Plusieurs options sont disponibles aux hôtes :

- Augmentez la taille de la file d'attente de connexion (file d'attente de synchronisation ACK).
- Diminuez la minuterie attendant la connexion en trois étapes.
- Utilisez les correctifs de logiciel constructeur pour détecter et éviter le problème (si disponible).

Vous devriez contacter votre constructeur d'hôte pour voir s'ils ont créé les correctifs spécifiques pour adresser l'attaque de la synchronisation ACK de TCP.

Remarque: Le filtrage des adresses IP au serveur est inefficace puisqu'un attaquant peut varier son adresse IP, et l'adresse peut ou peut ne pas être identique que cela d'un hôte légitime.

Empêchant un réseau d'accueillir inconsciemment une attaque

Puisqu'un mécanisme primaire de cette attaque par déni de service est la génération du trafic originaire des adresses IP aléatoires, nous recommandons le trafic de filtrage destiné pour l'Internet. Le concept de base est de jeter des paquets avec des adresses IP de source non valide car ils entrent dans l'Internet. Ceci n'empêche pas une attaque par déni de service sur votre réseau, mais aidera les interlocuteurs attaqués à éliminer votre emplacement comme source de l'attaquant. En outre, il rend votre réseau moins attrayant comme base pour cette classe d'attaque.

Empêchement de la transmission des adresses IP non valides

En filtrant des paquets sur vos Routeurs qui connectent votre réseau à l'Internet, vous pouvez permettre seulement à des paquets avec les adresses IP valides de source pour laisser votre réseau et pour l'entrer dans l'Internet.

Par exemple, si votre réseau se compose du réseau 172.16.0.0, et votre routeur se connecte à votre ISP utilisant une interface de l'interface série 0/1, vous peut 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 n'importe quel trafic avec une adresse source incorrecte entrant dans l'Internet. Il n'est pas crucial d'avoir cette ligne, mais il aidera à identifier la source des attaques possibles.

Empêchement de la réception des adresses IP non valides

Pour les ISP qui fournissent le service pour finir des réseaux, nous recommandons fortement la validation des paquets entrant de vos clients. Ceci peut faire en employant des filtres de paquets entrant sur vos Routeurs de cadre.

Par exemple, si vos clients ont les network number suivants connectés à votre routeur par l'intermédiaire d'une interface série nommée la « interface série 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 n'importe quel trafic avec des adresses sources incorrectes entrant dans l'Internet. Il n'est pas crucial d'avoir cette ligne, mais il aidera à identifier la source d'attaque possible.

Ce thème a été discuté de manière assez détaillée sur la liste de diffusion NANOG [groupe nord-américain de réseau Operator1s]. Les archives de liste se trouvent à : http://www.merit.edu/mail.archives/nanog/index.html

Pour une description détaillée de l'attaque par déni de service et d'usurpation d'adresse IP de synchronisation de TCP, voyez : http://www.cert.org/advisories/CA-1996-21.html

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

Informations connexes

- Support technique - Cisco Systems