Caractérisation et suivi des inondations de paquets à l'aide de routeurs Cisco

Contenu

Introduction

Les attaques de déni de service sont courantes sur Internet. La première étape à suivre pour répondre à une telle attaque est de découvrir le type exact de l'attaque. Plusieurs des attaques de déni de service utilisées généralement sont basées sur l'envoi massif de paquets de bande passante élevée, ou sur d'autres flux répétitifs de paquets.

Les paquets de nombreux flux d'attaque DoS peuvent être isolés lorsque vous les comparez aux entrées de liste d'accès du logiciel Cisco IOS®. Cela est utile pour le filtrage des attaques. Il est également utile lorsque vous caractérisez des attaques inconnues et lorsque vous retracez des flux de paquets « usurpés » vers leurs sources réelles.

Les fonctions des routeurs Cisco telles que la journalisation des débogages et la comptabilité IP peuvent parfois être utilisées à des fins similaires, en particulier avec des attaques nouvelles ou inhabituelles. Cependant, avec les versions récentes du logiciel Cisco IOS, les listes d’accès et la journalisation des listes d’accès sont les principales fonctionnalités pour caractériser et suivre les attaques courantes.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

Conventions

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

Les attaques DoS les plus courantes

Une grande variété d'attaques DoS est possible. Même si vous ignorez les attaques qui utilisent des bogues logiciels pour arrêter les systèmes avec relativement peu de trafic, le fait demeure que tout paquet IP pouvant être envoyé sur le réseau peut être utilisé pour exécuter une attaque DoS inondée. Lorsque vous êtes attaqué, vous devez toujours envisager la possibilité que ce que vous voyez est quelque chose qui ne tombe pas dans les catégories habituelles.

Toutefois, sous réserve de cette mise en garde, il est également bon de se rappeler que de nombreuses attaques sont similaires. Les pirates choisissent les attaques courantes parce qu'elles sont particulièrement efficaces, particulièrement difficiles à retracer, ou parce que des outils sont disponibles. De nombreux pirates DoS n'ont pas les compétences ou la motivation nécessaires pour créer leurs propres outils et utiliser les programmes trouvés sur Internet. Ces outils ont tendance à tomber dans la mode.

Au moment de la rédaction du présent document, en juillet 1999, la plupart des demandes d'assistance Cisco concernaient l'attaque « smurf ». Cette attaque a deux victimes : une « cible ultime » et un « réflecteur ». Le pirate envoie un flux de stimulation de requêtes d'écho ICMP (« ping ») à l'adresse de diffusion du sous-réseau du réflecteur. Les adresses source de ces paquets sont falsifiées pour être l'adresse de la cible finale. Pour chaque paquet envoyé par le pirate, de nombreux hôtes du sous-réseau du réflecteur répondent. Cela inonde la cible ultime et gaspille de la bande passante pour les deux victimes.

Une attaque similaire, appelée « fraggle », utilise les diffusions dirigées de la même manière, mais utilise des requêtes d'écho UDP au lieu de requêtes d'écho ICMP (Internet Control Message Protocol). Fragle atteint généralement un facteur d'amplification plus faible que smurf, et est beaucoup moins populaire.

Les attaques par brouillards sont généralement remarquées car une liaison réseau est surchargée. Une description complète de ces attaques et des mesures de défense est disponible sur la page Informations sur les attaques par déni de service.

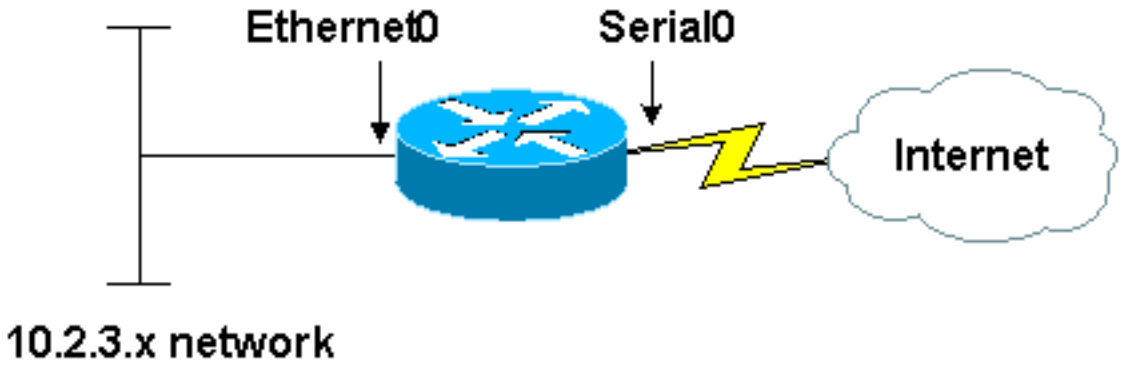
Une autre attaque courante est l'inondation SYN, dans laquelle une machine cible est inondée de requêtes de connexion TCP. Les adresses source et les ports TCP source des paquets de demande de connexion sont randomisés. L'objectif est de forcer l'hôte cible à conserver les informations d'état pour de nombreuses connexions qui ne sont jamais terminées.

Les attaques par inondation SYN sont généralement remarquées car l'hôte cible (souvent un serveur HTTP ou SMTP) devient extrêmement lent, tombe en panne ou se bloque. Il est également possible que le trafic qui revient de l'hôte cible cause des problèmes sur les routeurs. Ceci est dû au fait que ce trafic de retour va aux adresses source aléatoires des paquets d'origine, qu'il manque les propriétés de localisation du trafic IP « réel » et qu'il peut déborder des caches de route. Sur les routeurs Cisco, ce problème se manifeste souvent dans le manque de mémoire du routeur.

Ensemble, les attaques smurf et SYN représentent la grande majorité des attaques DoS d'inondation signalées à Cisco, et la reconnaissance rapide de ces attaques est très importante. Les deux attaques (ainsi que certaines attaques de deuxième niveau, telles que les inondations de requêtes ping) sont facilement reconnues lorsque vous utilisez les listes d'accès Cisco.

Liste d'accès de personnalisation DoS

Imaginez un routeur avec deux interfaces. Ethernet 0 est connecté à un réseau local interne d'une entreprise ou d'un petit FAI. Serial 0 fournit une connexion Internet via un FAI en amont. Le débit des paquets d'entrée sur la série 0 est « fixé » à la bande passante de la liaison complète et les hôtes du réseau local s'exécutent lentement, se bloquent, se bloquent ou montrent d'autres signes d'attaque DoS. Le petit site auquel le routeur se connecte n'a pas d'analyseur de réseau et les personnes qui y sont présentes n'ont que peu ou pas d'expérience de la lecture des traces de l'analyseur, même si les traces sont disponibles.



Maintenant, supposez que vous appliquez une liste d'accès comme le montre ce résultat :

```
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
```

Cette liste ne filtre aucun trafic ; toutes les entrées sont des permis. Cependant, comme elle classe les paquets de manière utile, la liste peut être utilisée pour diagnostiquer provisoirement les trois types d'attaques : smurf, inondations SYN et fraggle.

Cible Ultime Smurf

Si vous émettez la commande **show access-list**, vous voyez une sortie similaire à celle-ci :

```
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)
```

La plupart du trafic qui arrive sur l'interface série est constitué de paquets de réponse d'écho ICMP. C'est probablement la signature d'une attaque de smurf, et notre site est la cible ultime, plutôt que le réflecteur. Vous pouvez collecter plus d'informations sur l'attaque lorsque vous modifiez la liste de contrôle d'accès, comme le montre ce résultat :

```
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
```

La modification ici est que le mot clé **log-input** est ajouté à l'entrée de la liste d'accès qui correspond au trafic suspect. (Les versions du logiciel Cisco IOS antérieures à 11.2 ne contiennent pas ce mot clé. Utilisez le mot clé "**log**" à la place.) Le routeur enregistre ainsi les informations relatives aux paquets qui correspondent à l'entrée de la liste. Si vous supposez que **logging buffered** est configuré, vous pouvez voir les messages qui résultent de la commande **show log** (il peut prendre un certain temps pour que les messages s'accumulent en raison de la limitation de débit). Les messages apparaissent comme suit :

```
%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
```

Les adresses source des paquets de réponse d’écho sont mises en grappe dans les préfixes d’adresse 192.168.212.0/24, 192.168.45.0/24 et 172.16.132.0/24. (Les adresses privées des réseaux 192.168.x.x et 172.16.x.x ne se trouveraient pas sur Internet ; ceci est une illustration de travaux pratiques.) Ceci est très caractéristique d'une attaque smurf, et les adresses source sont les adresses des réflecteurs smurf. Si vous recherchez les propriétaires de ces blocs d'adresses dans les bases de données Internet whois appropriées, vous pouvez trouver les administrateurs de ces réseaux et demander leur aide pour gérer l'attaque.

Il est important à ce stade d'un incident de brouillard de se rappeler que ces réflecteurs sont d'autres victimes, pas des agresseurs. Il est extrêmement rare que les pirates utilisent leurs propres adresses source sur des paquets IP lors d'une inondation de déni de service, et il leur est impossible de le faire lors d'une attaque par brouillard. Toute adresse d’un paquet d’inondation doit être supposée être soit complètement falsifiée, soit l’adresse d’une victime d’une sorte ou d’une autre. L'approche la plus productive pour la cible ultime d'une attaque smurf est de contacter les réflecteurs, soit pour leur demander de reconfigurer leurs réseaux pour arrêter l'attaque, soit pour leur demander de les aider à retracer le flux de stimulation.

Comme les dommages causés à la cible finale d'une attaque smurf sont généralement causés par une surcharge de la liaison entrante depuis Internet, il n'y a souvent pas d'autre réponse que de contacter les réflecteurs. Au moment où les paquets arrivent sur n'importe quelle machine sous le contrôle de la cible, la plupart des dégâts ont déjà été faits.

Une mesure de blocage consiste à demander au fournisseur de réseau en amont de filtrer toutes les réponses d’écho ICMP ou toutes les réponses d’écho ICMP provenant de réflecteurs spécifiques. Il n'est pas recommandé de laisser ce type de filtre en place de façon permanente. Même pour un filtre temporaire, seules les réponses d’écho doivent être filtrées, pas tous les paquets ICMP. Une autre possibilité consiste à faire en sorte que le fournisseur en amont utilise des fonctionnalités de qualité de service et de limitation de débit pour limiter la bande passante disponible pour les réponses d’écho. Une limite raisonnable de bande passante peut être maintenue indéfiniment. Ces deux approches dépendent de l'équipement du fournisseur en amont

ayant la capacité nécessaire, et parfois cette capacité n'est pas disponible.

Réflecteur Smurf

Si le trafic entrant se compose de requêtes d'écho plutôt que de réponses d'écho (en d'autres termes, si la première entrée de la liste d'accès, plutôt que la seconde, comptait beaucoup plus de correspondances qu'il n'est raisonnable de s'y attendre), vous suspecterez une attaque smurf dans laquelle le réseau était utilisé comme réflecteur, ou peut-être une simple inondation ping. Dans les deux cas, si l'attaque est une réussite, vous vous attendez à ce que le côté sortant de la ligne série soit submergé, ainsi que le côté entrant. En fait, en raison du facteur d'amplification, on s'attendrait à ce que le côté sortant soit encore plus surchargé que le côté entrant.

Il existe plusieurs façons de distinguer l'attaque smurf de la simple inondation ping :

- Les paquets de stimulation Smurf sont envoyés à une adresse de diffusion dirigée, plutôt qu'à une adresse de monodiffusion, alors que les inondations ping ordinaires utilisent presque toujours des monodiffusions. Vous pouvez voir les adresses qui utilisent le mot clé **log-input** sur l'entrée de liste d'accès appropriée.
- Si vous êtes utilisé comme réflecteur smurf, il y a un nombre disproportionné de diffusions de sortie dans l'affichage **show interface** du côté Ethernet du système, et généralement un nombre disproportionné de diffusions envoyées dans l'affichage **show ip traffic**. Une inondation ping standard n'augmente pas le trafic de diffusion en arrière-plan.
- Si vous êtes utilisé comme réflecteur smurf, il y a plus de trafic sortant vers Internet que de trafic entrant depuis Internet. En général, il y a plus de paquets de sortie que de paquets d'entrée sur l'interface série. Même si le flux de relance remplit complètement l'interface d'entrée, le flux de réponse est plus grand que le flux de relance, et les pertes de paquets sont comptées.

Un réflecteur de brouillard offre plus d'options que la cible ultime d'une attaque de brouillard. Si un réflecteur choisit d'arrêter l'attaque, l'utilisation appropriée de **no ip directed-broadcast** (ou de commandes non IOS équivalentes) est généralement suffisante. Ces commandes appartiennent à chaque configuration, même s'il n'y a pas d'attaque active. Pour plus d'informations sur la prévention de l'utilisation de votre équipement Cisco lors d'une attaque smurf, référez-vous à Amélioration de la sécurité sur les routeurs Cisco. Pour plus d'informations générales sur les attaques smurf en général et pour plus d'informations sur la protection des équipements non Cisco, consultez la page Informations sur les attaques par déni de service.

Un réflecteur smurf est un pas plus proche du pirate que la cible ultime et est donc mieux placé pour suivre l'attaque. Si vous choisissez de suivre l'attaque, vous devez travailler avec les FAI concernés. Si vous souhaitez que des mesures soient prises lorsque vous terminez la trace, vous devez travailler avec les organismes d'application de la loi appropriés. Si vous cherchez à retracer une attaque, il est recommandé d'impliquer les forces de l'ordre dès que possible. Reportez-vous à la section Suivi pour obtenir des informations techniques sur le suivi des attaques par inondation.

Fragmenter

L'attaque de fragmentation est analogue à l'attaque smurf, sauf que les requêtes d'écho UDP sont utilisées pour le flux de stimulation au lieu des requêtes d'écho ICMP. Les troisième et quatrième lignes de la liste d'accès identifient les attaques fragmentées. La réponse appropriée pour les victimes est la même, sauf que l'écho UDP est un service moins important dans la plupart des

réseaux que l'écho ICMP. Par conséquent, vous pouvez les désactiver complètement avec moins de conséquences négatives.

Inondations SYN

Les cinquième et sixième lignes de la liste d’accès sont les suivantes :

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

La première de ces lignes correspond à n’importe quel paquet TCP avec le bit ACK défini. Pour nos besoins, cela signifie vraiment qu'il correspond à n'importe quel paquet qui n'est pas un SYN TCP. La deuxième ligne correspond uniquement aux paquets qui sont des SYN TCP. Une inondation SYN est facilement identifiée à partir des compteurs de ces entrées de liste. Dans le trafic normal, les paquets TCP non SYN dépassent le nombre de SYN d'au moins un facteur deux, et généralement plus de quatre ou cinq. Dans une inondation SYN, les SYN dépassent souvent le nombre de paquets TCP non SYN.

La seule condition de non-attaque qui crée cette signature est une surcharge massive de demandes de connexion authentiques. En général, une telle surcharge ne se produira pas de manière inattendue et n'impliquera pas autant de paquets SYN qu'une véritable inondation SYN. En outre, les inondations SYN contiennent souvent des paquets avec des adresses source complètement incorrectes ; en utilisant le mot clé **log-input**, il est possible de voir si les requêtes de connexion proviennent de ces adresses.

Il y a une attaque appelée « attaque de table de processus » qui présente une certaine similitude avec l'inondation SYN. Lors de l'attaque de la table de processus, les connexions TCP sont terminées, puis autorisées à expirer sans trafic de protocole supplémentaire, alors que dans le flux SYN, seules les requêtes de connexion initiales sont envoyées. Étant donné qu'une attaque de table de processus nécessite l'achèvement de la connexion TCP initiale, elle doit généralement être lancée à l'aide de l'adresse IP d'une machine réelle à laquelle le pirate a accès (accès généralement volé). Les attaques de table de processus se distinguent donc facilement des inondations SYN avec l'utilisation de la journalisation des paquets. Tous les SYN d’une attaque de table de processus proviennent d’une ou de quelques adresses, ou tout au plus d’un ou de quelques sous-réseaux.

Les options d'intervention pour les victimes des inondations SYN sont très limitées. Le système attaqué est généralement un service important, et le blocage de l'accès au système accomplit généralement ce que le pirate veut. De nombreux routeurs et pare-feu, dont ceux de Cisco, offrent des fonctionnalités qui peuvent être utilisées pour réduire l'impact des inondations SYN. Mais l'efficacité de ces caractéristiques dépend de l'environnement. Pour plus d'informations, référez-vous à la documentation du jeu de fonctions de pare-feu Cisco IOS, à la documentation de la fonction d'interception TCP de Cisco IOS et à l'amélioration de la sécurité sur les routeurs Cisco.

Il est possible de suivre les inondations SYN, mais le processus de suivi nécessite l'assistance de chaque FAI le long du chemin entre l'attaquant et la victime. Si vous décidez d'essayer de suivre une inondation SYN, contactez les services de police dès le début et travaillez avec votre propre fournisseur de services en amont. Reportez-vous à la section traçage de ce document pour plus de détails sur le traçage avec l'utilisation de l'équipement Cisco.

Autres attaques

Si vous croyez être victime d'une attaque et que vous pouvez la caractériser à l'aide d'adresses IP source et de destination, de numéros de protocole et de numéros de port, vous pouvez utiliser des listes d'accès pour tester votre hypothèse. Créez une entrée de liste d'accès qui correspond au trafic suspect, appliquez-la à une interface appropriée et observez les compteurs de correspondance ou enregistrez le trafic.

Consignation et contre-cavités

Le compteur d'une entrée de liste d'accès compte toutes les correspondances par rapport à cette entrée. Si vous appliquez une liste d'accès à deux interfaces, les nombres que vous voyez sont des nombres agrégés.

La journalisation de la liste d'accès n'affiche pas tous les paquets qui correspondent à une entrée. La journalisation est limitée au débit pour éviter la surcharge du processeur. Ce que la journalisation vous montre est un échantillon raisonnablement représentatif, mais pas une trace de paquet complète. N'oubliez pas qu'il y a des paquets que vous ne voyez pas.

Dans certaines versions logicielles, la journalisation des listes d'accès fonctionne uniquement dans certains modes de commutation. Si une entrée de liste d'accès compte beaucoup de correspondances, mais ne consigne rien, essayez d'effacer le cache de route pour forcer les paquets à être commutés par processus. Faites attention si vous effectuez cette opération sur des routeurs lourdement chargés avec de nombreuses interfaces. Une grande partie du trafic peut être abandonnée lors de la reconstruction du cache. Utilisez Cisco Express Forwarding dans la mesure du possible.

Les listes d'accès et la journalisation ont un impact sur les performances, mais pas sur les grandes. Soyez prudent sur les routeurs qui fonctionnent avec une charge CPU supérieure à 80 % ou lorsque vous appliquez des listes d'accès à des interfaces à très haut débit.

Suivi

Les adresses source des paquets DoS sont presque toujours définies sur des valeurs qui n'ont rien à voir avec les agresseurs eux-mêmes. Par conséquent, ils ne sont pas utiles pour identifier les agresseurs. La seule façon fiable d'identifier la source d'une attaque consiste à la retracer saut par saut sur le réseau. Ce processus implique la reconfiguration des routeurs et l'examen des informations de journal. Tous les opérateurs de réseau doivent coopérer sur le chemin entre l'attaquant et la victime. Pour garantir cette coopération, il faut généralement faire intervenir les services de détection et de répression, qui doivent également être impliqués si l'on veut prendre des mesures contre l'agresseur.

Le processus de suivi des inondations par déni de service est relativement simple. À partir d'un routeur (appelé « A ») connu pour acheminer le trafic d'inondation, on identifie le routeur (appelé « B ») à partir duquel A reçoit le trafic. L'un se connecte ensuite à B et trouve le routeur (appelé « C ») à partir duquel B reçoit le trafic. Cela se poursuit jusqu'à ce que la source ultime soit trouvée.

Cette méthode comporte plusieurs complications, décrites dans cette liste :

- La « source ultime » peut être un ordinateur qui a été compromis par l'attaquant, mais qui est en fait la propriété et l'exploitation d'une autre victime. Dans ce cas, le suivi de l'inondation DoS n'est que la première étape.
- Les hackers savent qu'ils peuvent être retracés et ne poursuivent généralement leurs

attaques que pendant une durée limitée. Il n'y aura peut-être pas assez de temps pour suivre les inondations.
- Les attaques peuvent provenir de sources multiples, surtout si le pirate est relativement sophistiqué. Il est important d'essayer d'identifier autant de sources que possible.
- Les problèmes de communication ralentissent le processus de suivi. Souvent, un ou plusieurs des opérateurs de réseau concernés ne disposent pas de personnel qualifié approprié.
- Les préoccupations juridiques et politiques peuvent rendre difficile l'action contre les agresseurs, même si l'on en trouve.

La plupart des tentatives de suivi des attaques DoS échouent. De ce fait, de nombreux opérateurs de réseau ne tentent même pas de détecter une attaque, à moins qu'elle ne soit soumise à des pressions. Beaucoup d'autres ne retracent que des attaques « graves », avec des définitions différentes de ce qui est « grave ». Certains aident à tracer une trace seulement si les forces de l'ordre sont impliquées.

Suivi avec « log-input »

Si vous choisissez de tracer une attaque qui passe par un routeur Cisco, la façon la plus efficace d'y parvenir est de construire une entrée de liste de contrôle d'accès qui correspond au trafic d'attaque, de lui attacher le mot clé **log-input** et d'appliquer la liste de contrôle d'accès en sortie sur l'interface par laquelle le flux d'attaque est envoyé vers sa cible finale. Les entrées du journal produites par la liste d'accès identifient l'interface du routeur par laquelle le trafic arrive et, si l'interface est une connexion multipoint, indiquent l'adresse de couche 2 du périphérique à partir duquel il est reçu. L'adresse de couche 2 peut ensuite être utilisée pour identifier le routeur suivant de la chaîne, en utilisant, par exemple, la commande **show ip arp** ***mac-address.***

Inondation SYN

Afin de suivre une inondation SYN, vous pouvez créer une liste d'accès similaire à ceci :

```
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
```

Cela consigne tous les paquets SYN destinés à l'hôte cible, y compris les SYN légitimes. Afin d'identifier le chemin le plus probable vers le pirate, examinez les entrées du journal en détail. En général, la source de l'inondation est la source à partir de laquelle le plus grand nombre de paquets correspondants arrive. Les adresses IP source elles-mêmes ne signifient rien. Vous recherchez des interfaces source et des adresses MAC source. Il est parfois possible de distinguer les paquets inondés des paquets légitimes, car les paquets inondés peuvent avoir des adresses source non valides. Tout paquet dont l'adresse source n'est pas valide est susceptible de faire partie de l'inondation.

L'inondation peut provenir de sources multiples, bien que ce soit relativement inhabituel pour les inondations SYN.

Stimulus de Schtroumpf

Afin de tracer un flux de relance smurf, utilisez une liste d'accès comme celle-ci :

```
access-list 169 permit icmp any any echo log-input
```

```
access-list 169 permit ip any any
```

Notez que la première entrée ne se limite pas aux paquets destinés à l'adresse du réflecteur. La raison en est que la plupart des attaques smurf utilisent plusieurs réseaux de réflecteurs. Si vous n'êtes pas en contact avec la cible finale, vous ne connaissez peut-être pas toutes les adresses du réflecteur. À mesure que votre trace se rapproche de la source de l'attaque, vous pouvez commencer à voir des requêtes d'écho se dirigeant vers de plus en plus de destinations ; c'est un bon signe.

Cependant, si vous gérez une grande partie du trafic ICMP, cela peut générer trop d'informations de journalisation pour que vous puissiez les lire facilement. Si cela se produit, vous pouvez limiter l'adresse de destination à l'un des réflecteurs connus pour être utilisés. Une autre tactique utile consiste à utiliser une entrée qui tire parti du fait que les masques réseau 255.255.255.0 sont très courants sur Internet. Et, en raison de la manière dont les pirates trouvent les réflecteurs smurf, les adresses de réflecteur réellement utilisées pour les attaques smurf sont encore plus susceptibles de correspondre à ce masque. Les adresses d'hôte qui se terminent par .0 ou .255 sont très rares sur Internet. Par conséquent, vous pouvez créer un outil de reconnaissance relativement spécifique pour les flux de stimulus smurf comme le montre ce résultat :

```
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
```

Avec cette liste, vous pouvez éliminer un grand nombre de paquets « bruit » de votre journal, tout en ayant encore une bonne chance de remarquer des flux de stimulation supplémentaires lorsque vous vous rapprochez du pirate.

Suivi sans « log-input »

Le mot clé **log-input** existe dans les versions 11.2 et ultérieures du logiciel Cisco IOS et dans certains logiciels basés sur 11.1 créés spécifiquement pour le marché des fournisseurs de services. Des logiciels plus anciens ne prennent pas en charge ce mot clé. Si vous utilisez un routeur avec un logiciel plus ancien, vous disposez de trois options viables :

- Créez une liste d'accès sans journalisation, mais avec des entrées correspondant au trafic suspect. Appliquez la liste sur le côté *entrée* de chaque interface à tour de rôle et observez les compteurs. Recherchez des interfaces avec des taux de correspondance élevés. Cette méthode a une surcharge de performances très faible et est bonne pour l'identification des interfaces source. Son principal inconvénient est qu'il ne donne pas d'adresses source de couche de liaison et est donc surtout utile pour les lignes point à point.
- Créez des entrées de liste d'accès avec le mot clé **log** (par opposition à **log-input**). Une fois de plus, appliquez la liste au côté entrant de chaque interface à tour de rôle. Cette méthode ne donne toujours pas d'adresses MAC source, mais peut s'avérer utile pour voir les données IP. Par exemple, pour vérifier qu'un flux de paquets fait réellement partie d'une attaque. L'impact sur les performances peut être modéré à élevé et les logiciels plus récents offrent de meilleures performances que les anciens logiciels.
- Utilisez la commande **debug ip packet detail** pour collecter des informations sur les paquets. Cette méthode donne des adresses MAC, mais peut avoir un impact sérieux sur les performances. Il est facile de faire une erreur avec cette méthode et de rendre un routeur inutilisable. Si vous utilisez cette méthode, assurez-vous que le routeur commute le trafic d'attaque en mode rapide, autonome ou optimal. Utilisez une liste d'accès pour limiter le débogage aux informations dont vous avez vraiment besoin. Consignez les informations de

débogage dans la mémoire tampon du journal local, mais désactivez la journalisation des informations de débogage dans les sessions Telnet et sur la console. Si possible, faites en sorte que quelqu'un se trouve physiquement à proximité du routeur, afin qu'il puisse être mis hors tension si nécessaire.N'oubliez pas que la commande **debug ip packet** n'affiche pas d'informations sur les paquets à commutation rapide. Vous devez émettre la commande **clear ip cache** afin de capturer les informations. Chaque commande **clear** vous donne un ou deux paquets de sortie de débogage.

Informations connexes

- Kerberos
- Support et documentation techniques - Cisco Systems