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

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Conventions](#)
[Les attaques DoS les plus communes](#)
[Une liste d'accès de caractérisation DOS](#)
[Cible finale de Smurf](#)
[Réflecteur de surcharge](#)
[Fraggle](#)
[Inondations de synchronisation](#)
[Autre attaques](#)
[Se connecter et contre- mises en garde](#)
[Découverte](#)
[Découverte avec la « log-entrée »](#)
[Inondation de synchronisation](#)
[Stimulus de Smurf](#)
[Découverte sans « log-entrée »](#)
[Informations connexes](#)

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 dans beaucoup de flots d'attaque DoS peuvent être isolés quand vous les appariez contre des entrées de liste d'accès de logiciel de Cisco IOS®. C'est valeur pour filtrer des attaques. Il est également utile pour quand vous caractérisez des attaques inconnues, et pour quand vous tracez les flux de paquets « charriés » de nouveau à leurs vraies sources.

Des caractéristiques de routeur de Cisco telles que le debug logging et l'ip accounting peuvent parfois être utilisés pour les buts semblables, particulièrement avec de nouvelles ou peu communes attaques. Cependant, avec des versions récentes de Cisco IOS logiciel, les Listes d'accès et se connecter de liste d'accès sont les caractéristiques de première pour quand vous caractérisez et tracez des attaques communes.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Les attaques DoS les plus communes

Une grande variété d'attaques DoS sont possibles. Même si vous ignorez les attaques qui utilisent des erreurs de programmation aux systèmes arrêtés avec relativement peu de trafic, le fait demeure que tout paquet IP qui peut être envoyé à travers le réseau peut être utilisé pour exécuter une attaque DoS d'inondation. Quand vous êtes soumise aux attaques, vous devez toujours considérer la possibilité que ce que vous voyez est quelque chose qui ne se range pas dans les catégories habituelles.

Sujet à cette mise en garde, cependant, il est également bon de se souvenir que beaucoup d'attaques sont semblables. Les attaquants choisissent des exploits communes parce qu'ils sont particulièrement efficaces, particulièrement dur pour tracer, ou parce que les outils sont disponibles. Beaucoup d'attaquants DOS manquent de la compétence ou de la motivation pour créer leurs propres outils, et utilisent des programmes trouvés sur l'Internet. Ces outils tendent à tomber dans et hors de la mode.

Au moment de cette écriture, en juillet 1999, la plupart des requêtes du client pour l'assistance de Cisco comportent l'attaque de « smurf ». Cette attaque a deux victimes : « une cible finale » et un « réflecteur. » L'attaquant envoie un flux de stimuli des requêtes d'écho d'ICMP (« pings ») à l'adresse d'émission du sous-réseau réflecteur. Les adresses sources de ces paquets sont falsifiées pour être l'adresse de la cible finale. Pour chaque paquet envoyé par l'attaquant, beaucoup d'hôtes sur le sous-réseau réflecteur répondent. Ceci inonde la cible finale et gaspille la bande passante pour les deux victimes.

Une attaque semblable, appelée le « fraggle, » utilise des diffusions dirigées de la même manière, mais utilise des requêtes d'écho d'UDP au lieu des requêtes d'écho de Protocole ICMP (Internet Control Message Protocol). Fraggle réalise habituellement un plus petit facteur d'amplification que le smurf, et est beaucoup moins populaire.

Des attaques smurf sont habituellement notées parce qu'une liaison réseau devient surchargée. Une description complète de ces attaques, et des mesures de la défense, est sur la page d'information d'attaques par déni de service .

Une autre attaque commune est l'inondation de synchronisation, en laquelle une machine cible est inondée avec des demandes de connexion TCP. Les adresses sources et les ports TCP de

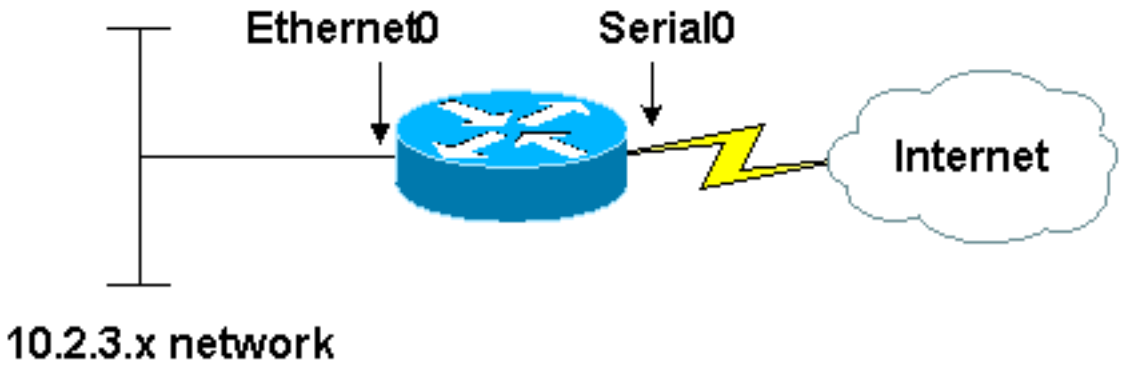
source des paquets de demandes de connexion sont sélectionnés de façon aléatoire. Le but est de forcer l'hôte de cible pour mettre à jour les informations d'état pour beaucoup de connexions qui ne sont jamais terminées.

Des attaques par inondation SYN sont habituellement notées parce que l'hôte de cible (fréquemment un HTTP ou un serveur SMTP) devient extrêmement lent, tombe en panne, ou s'arrête. Il est également possible au trafic qui retourne de l'hôte de cible pour entraîner le problème sur des Routeurs. C'est parce que ce trafic de retour va aux adresses sources sélectionnées de façon aléatoire des paquets d'origine, il manque des propriétés de localité du « vrai » trafic IP, et peut déborder des caches d'artère. Sur des Routeurs de Cisco, ce problème se manifeste souvent dans l'exécution de routeur hors de la mémoire.

Ensemble, le smurf et les attaques par inondation SYN expliquent l'immense majorité des attaques DoS d'inondation signalées à Cisco, et l'identification de elles est rapidement très importante. Les deux attaques (aussi bien que quelques attaques de « deuxième niveau », telles que des inondations pings) sont facilement identifiées quand vous utilisez des Listes d'accès de Cisco.

Une liste d'accès de caractérisation DOS

Décrivez un routeur avec deux interfaces. L'Ethernet 0 est connecté à un RÉSEAU LOCAL interne à une entreprise ou à un petit ISP. L'interface série 0 fournit une connexion Internet par l'intermédiaire d'un ISP d'en amont. Le débit de paquet en entrée sur l'interface série 0 « est chevillé » à la pleine bande passante de lien, et les hôtes sur le RÉSEAU LOCAL fonctionnent lentement, tombent en panne, arrêtent, ou affichent d'autres signes d'une attaque DoS. Le petit site auquel le routeur se connecte n'a aucun analyseur de réseau, et les personnes là ont peu ou pas d'expérience dans des suivis d'analyseur de lecture même si les suivis sont disponibles.



Maintenant, supposez que vous appliquez une liste d'accès pendant que cette sortie affiche :

```
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 du tout ; toutes les entrées sont des autorisations. Cependant,

parce qu'elle classe des paquets par catégorie des moyens utiles, la liste peut être utilisée pour diagnostiquer à titre d'essai chacun des trois types d'attaques : smurf, inondations de synchronisation, et fraggle.

Cible finale de Smurf

Si vous émettez la **commande access-list d'exposition**, vous voyez la sortie semblable à ceci :

```
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 majeure partie du trafic qui arrive sur l'interface série se compose des paquets de réponse d'écho d'ICMP. C'est probablement la signature d'une attaque smurf, et notre site est la cible finale, plutôt que le réflecteur. Vous pouvez recueillir plus d'informations au sujet de l'attaque quand vous mettez à jour la liste d'accès, car cette sortie affiche :

```
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 liste d'accès qui apparie le trafic suspect. (Les versions du logiciel Cisco IOS plus tôt que 11.2 manquent de ce mot clé. Utilisez le mot clé de « **log** » à la place.) Ceci fait connecter le routeur des informations sur les paquets qui apparient l'entrée de la liste. Si vous supposez que le **logging buffered** est configuré, vous pouvez voir les messages qui résultent avec le **show log command** (il peut prendre un moment pour que les messages s'accumulent en raison de la limitation de débit). Les messages ressemblent à cette sortie :

```
%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 sources des paquets de réponse d'écho sont groupées dans les préfixes d'adresse 192.168.212.0/24, 192.168.45.0/24, et 172.16.132.0/24. (Les adresses privées dans les réseaux 192.168.x.x et 172.16.x.x ne seraient pas sur l'Internet ; c'est une illustration de laboratoire.) C'est très caractéristique d'une attaque smurf, et les adresses sources sont les adresses des réflecteurs de surcharge. Si vous consultation les propriétaires de ces blocs d'adresses dans bases de données appropriées de l'Internet les « WHOIS », vous pouvez trouver les administrateurs de ces réseaux, et demandez leur aide en faisant face à l'attaque.

Il est important en ce moment dans un incident de smurf de se souvenir que ces réflecteurs sont les victimes semblables, pas des attaquants. Il est extrêmement rare pour que les attaquants utilisent leurs propres adresses sources sur des paquets IP en n'importe quelle inondation DOS, et impossible pour qu'ils fassent ainsi dans une attaque smurf fonctionnante. On devrait assumer que n'importe quelle adresse dans un paquet d'inondation est complètement falsifiée, ou l'adresse d'une victime d'un certain tri. L'approche la plus productive pour la cible finale d'une attaque smurf est d'entrer en contact avec les réflecteurs, pour leur demander pour modifier leurs réseaux pour arrêter l'attaque, ou pour demander leur assistance pour tracer le flux de stimuli.

Puisque les dommages à la cible finale d'une attaque smurf sont habituellement provoqués par la surcharge du lien entrant de l'Internet, il n'y a souvent aucune réponse autre que pour entrer en contact avec les réflecteurs. Avant que les paquets arrivent à n'importe quel ordinateur sous le contrôle de la cible, la majeure partie des dommages a été déjà faite.

Une mesure de bouche-trou est de demander au fournisseur de services réseau en amont pour filtrer toutes les réponses d'écho d'ICMP, ou à tous réponses d'écho d'ICMP des réflecteurs spécifiques. On ne le recommande pas que vous laissiez ce tri de filtre en place de manière permanente. Même pour un filtre provisoire, seulement des réponses d'écho devraient être filtrées, non tous les paquets d'ICMP. Une autre possibilité est d'avoir les caractéristiques en amont de qualité de service et de limitation de débit d'utilisation de fournisseur pour limiter la bande passante disponible aux réponses d'écho. Une limite de bande passante raisonnable peut être laissée en place indéfiniment. Chacun des deux approches dépendent du matériel du

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

Réflecteur de surcharge

Si le trafic entrant se compose des requêtes d'écho plutôt que des réponses d'écho (en d'autres termes, si la première entrée de liste d'accès, plutôt que la deuxième, comptait beaucoup plus de correspondances que pourrait raisonnablement être prévu), vous suspecteriez une attaque smurf dans laquelle le réseau était utilisé comme réflecteur, ou probablement une simple inondation de ping. Dans l'un ou l'autre de cas, si l'attaque est un succès, vous vous attendriez le côté sortant de la ligne série à inonder, aussi bien qu'au côté entrant. En fait, en raison du facteur d'amplification, vous vous attendriez au côté sortant à surcharger bien plus que le côté entrant.

Il y a plusieurs manières de distinguer l'attaque smurf de la simple inondation de ping :

- Des paquets de stimulus de Smurf sont envoyés à une adresse de diffusion dirigée, plutôt qu'à une adresse de monodiffusion, tandis que les inondations pings ordinaires utilisent presque toujours des unicasts. 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 de surcharge, il y avez un nombre disproportionné d'émissions de sortie dans l'affichage d'**interface d'exposition du** côté Ethernet du système, et habituellement un nombre disproportionné d'émissions introduites l'affichage de **show ip traffic**. Une inondation ping standard n'augmente pas le trafic de diffusion complémentaire.
- Si vous êtes utilisé comme réflecteur de surcharge, il y a plus de trafic sortant vers l'Internet que le trafic entrant de l'Internet. Généralement il y a plus de paquets en sortie que des paquets en entrée sur l'interface série. Même si le flux de stimuli remplit complètement interface d'entrée, le flot de réponse est plus grand que le flux de stimuli, et des pertes de paquets sont comptées.

Un réflecteur de surcharge a plus d'options que la cible finale d'une attaque smurf. Si un réflecteur choisit d'arrêter l'attaque, l'utilisation appropriée sans **ip directed-broadcast** (ou commandes non-IOS équivalentes) suffit habituellement. Ces commandes appartiennent dans chaque configuration, même s'il n'y a aucune attaque active. Pour plus d'informations sur la prévention de votre matériel de Cisco d'être utilisé dans une attaque smurf, référez-vous à améliorer la Sécurité sur des Routeurs de Cisco. Pour plus d'informations générales sur des attaques smurf généralement et pour des informations sur protéger le matériel de non-Cisco, référez-vous à la page d'information d'attaques par déni de service .

Un réflecteur de surcharge est une étape plus près de l'attaquant qu'est la cible finale, et est donc en meilleure position pour tracer l'attaque. Si vous choisissez de tracer l'attaque, vous devez travailler avec les ISP impliqués. Si vous souhaitez faire prendre n'importe quelle action quand vous vous terminez le suivi, vous devez travailler avec les organismes d'application de la loi compétents. Si vous recherchez à tracer une attaque, il est recommandé que vous comportez l'application de la loi dès que possible. Voyez la partie traçage pour des informations techniques sur des attaques par engorgement de suivi.

Fraggle

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

réseaux qu'est l'écho d'ICMP. Par conséquent, vous pouvez les désactiver complètement avec moins conséquences négatives.

Inondations de synchronisation

Les cinquièmes et sixièmes lignes de la liste d'accès sont :

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

Le premier de ces lignes apparie n'importe quel paquet TCP avec le positionnement de bit ACK. À nos fins, ce que signifie vraiment ceci est qu'il apparie n'importe quel paquet qui n'est pas une synchronisation de TCP. La deuxième ligne apparie seulement les paquets qui sont des synchronisations de TCP. Une inondation de synchronisation est facilement identifiée des compteurs sur ces entrées de la liste. Dans le trafic normal, les paquets TCP de non-synchronisation dépassent des synchronisations en nombre par au moins un facteur de deux, et habituellement plutôt quatre ou cinq. Dans une inondation de synchronisation, les synchronisations dépassent typiquement des paquets TCP en nombre de non-synchronisation plusieurs fois.

Le seul état de non-attaque qui crée cette signature est une surcharge massive des demandes de connexion véritables. Généralement une telle surcharge ne sera pas livré inopinément, et n'impliquera pas autant de paquets de synchronisation comme vraie inondation de synchronisation. En outre, les inondations de synchronisation contiennent souvent des paquets avec complètement des adresses sources incorrectes ; utilisant le **mot clé log-input**, il est possible de voir si des demandes de connexion provenir tels des adresses.

Il y a une attaque appelée une « attaque contre la table de traitement » qui soutient une certaine similitude à l'inondation de synchronisation. Dans l'attaque contre la table de traitement, les connexions TCP sont terminées, puis permises pour chronométrer sans davantage de trafic de protocole, tandis que dans l'inondation de synchronisation, seulement les demandes de connexion initiale sont envoyées. Puisqu'une attaque contre la table de traitement exige la fin de la prise de contact d'initiale de TCP, elle doit généralement être lancée avec l'utilisation de l'adresse IP d'un vrai ordinateur auquel l'attaquant a accès (accès habituellement dérobé). Des attaques contre la table de traitement donc sont facilement distinguées des inondations de synchronisation avec l'utilisation de se connecter de paquet. Toutes les synchronisations dans une attaque contre la table de traitement proviennent une ou quelque adresses, ou tout au plus d'un ou quelque sous-réseaux.

Les options de réponse pour les victimes des inondations de synchronisation sont très limitées. Le système sous l'attaque est habituellement un important service, et le blocage de l'accès au système accomplit habituellement ce que l'attaquant veut. Beaucoup le routeur et les produits pare-feux, y compris Cisco, ont des caractéristiques qui peuvent être utilisées pour réduire l'incidence des inondations de synchronisation. Mais, l'efficacité de ces caractéristiques dépend de l'environnement. Le pour en savoir plus, se rapportent à la documentation pour l'ensemble de fonctionnalités du pare-feu Cisco IOS, la documentation pour la caractéristique d'Interception TCP de Cisco IOS, et améliorer la Sécurité sur des Routeurs de Cisco.

Il est possible de tracer des inondations de synchronisation, mais le processus de suivi a besoin de l'assistance de chaque ISP le long du chemin de l'attaquant à la victime. Si vous décidez d'essayer de tracer une inondation de synchronisation, entrez en contact avec l'application de la loi dès l'abord, et fonctionnez avec votre propre fournisseur de service ascendant. Voyez la partie traçage de ce document pour des détails sur le suivi avec l'utilisation du matériel de Cisco.

Autre attaques

Si vous croyez que vous êtes soumise à des attaques, et si vous pouvez caractériser cette attaque utilisant des adresses d'origine et destination IP, des nombres de protocole, et des numéros de port, vous pouvez employer des Listes d'accès pour évaluer votre hypothèse. Créez une entrée de liste d'accès qui apparie le trafic suspect, l'appliquent à une interface appropriée, et observez les compteurs de correspondance ou connectez-vous le trafic.

Se connecter et contre- mises en garde

Le compteur sur une entrée de liste d'accès compte toutes les correspondances contre cette entrée. Si vous appliquez une liste d'accès à deux interfaces, les comptes que vous voyez sont des comptes d'agrégat.

Se connecter de liste d'accès n'affiche pas chaque paquet qui apparie une entrée. Se connecter est débit-limité pour éviter la surcharge CPU. Quel se connecter affiche vous est un échantillon raisonnablement représentatif, mais pas un tracé de paquets complet. Souvenez-vous qu'il y a des paquets que vous ne voyez pas.

Dans quelques versions de logiciel, liste d'accès se connectant des travaux seulement en certains modes de commutation. Si une entrée de liste d'accès compte beaucoup de correspondances, mais ne se connecte rien, essai pour effacer le cache d'artère pour forcer des paquets pour être commuté par processus. Faites attention si vous faites ceci sur les Routeurs fortement chargés avec beaucoup d'interfaces. Beaucoup de trafic peut obtenir relâché tandis que le cache est reconstruit. Utilisation Cisco Express Forwarding autant que possible.

Les Listes d'accès et se connecter ont une incidence des performances, mais pas grande. Faites attention sur les Routeurs qui fonctionnent au chargement CPU de plus qu'environ 80 pour cent, ou quand vous appliquez des Listes d'accès aux interfaces très ultra-rapides.

Découverte

Les adresses sources des paquets DOS sont presque toujours placées aux valeurs qui n'ont rien à faire avec les attaquants eux-mêmes. Par conséquent, ils ne sont pas utiles dans l'identification des attaquants. La seule manière fiable d'identifier la source d'attaque est de la tracer de retour saut par saut par le réseau. Ce processus implique la reconfiguration des Routeurs et l'examen des informations de log. La coopération par tous les opérateurs réseau le long du chemin de l'attaquant à la victime est exigée. Sécuriser cette coopération exige habituellement l'implication des organismes d'application de la loi, qui doivent également être impliqués si n'importe quelle action doit être prise contre l'attaquant.

Le processus de suivi pour des inondations DOS est relativement simple. Commençant à un routeur (nommé « A ») qui est connu pour être le trafic de propagation de transport, on identifie le routeur (dont nommé « B ») A reçoit le trafic. On se connecte alors dans B, et trouve le routeur (dont nommé « C ») B reçoit le trafic. Ceci continue jusqu'à ce que la source finale soit trouvée.

Il y a plusieurs complications dans cette méthode, que cette liste décrit :

- « La source finale » peut être un ordinateur qui a été compromis par l'attaquant, mais qui est possédé et actionné réellement par une autre victime. Dans ce cas, la découverte de l'inondation DOS est seulement la première étape.

- Les attaquants savent qu'ils peuvent être tracés, et continuent habituellement leurs attaques seulement pendant un certain temps une durée limitée. Il peut ne pas y avoir assez de temps de tracer réellement l'inondation.
- Les attaques peuvent provenir de plusieurs sources, particulièrement si l'attaquant est relativement sophistiqué. Il est important d'essayer d'identifier autant de sources comme possible.
- Les problèmes de communication ralentissent le processus de suivi. Fréquemment un ou plusieurs des opérateurs réseau impliqués n'a pas convenablement le personnel compétent disponible.
- Les soucis juridiques et politiques peuvent le rendre difficile à agir contre des attaquants même si un est trouvé.

La plupart des efforts de tracer l'échouer d'attaques DoS. Pour cette raison, beaucoup d'opérateurs réseau ne tentent pas même de tracer une attaque à moins que placés sous pression. Beaucoup d'autres attaques « graves » de suivi seulement, avec des définitions différentes de ce qui est « grave. » Une certaine aide avec un suivi seulement si l'application de la loi est impliquée.

Découverte avec la « log-entrée »

Si vous choisissez de tracer une attaque qui traverse un routeur de Cisco, la plupart de façon efficace de faire ceci est de construire une entrée de liste d'accès qui apparie le trafic d'attaque, relient le **mot clé log-input à** elle, et appliquent la liste d'accès sortante sur l'interface par laquelle le flot d'attaque est envoyé vers sa cible finale. Les entrées de journal produites par la liste d'accès identifient l'interface de routeur par laquelle le trafic arrive, et, si l'interface est une connexion multipoint, donnent l'adresse de la couche 2 du périphérique duquel elle est reçue. L'adresse de la couche 2 peut alors être utilisée pour identifier le prochain routeur dans la chaîne, utilisant, par exemple, la commande de *mac-address de* **show ip arp**.

Inondation de synchronisation

Afin de tracer une inondation de synchronisation, vous pouvez créer une liste d'accès semblable 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
```

Ceci se connecte tous les paquets de synchronisation destinés pour l'hôte de cible, y compris des synchronisations légitimes. Afin d'identifier le chemin réel le plus susceptible vers l'attaquant, examinez les entrées de journal en détail. Généralement la source de l'inondation est la source dont le plus grand nombre de paquets assortis arrive. Les adresses IP de source elles-mêmes ne signifient rien. Vous recherchez des interfaces et des adresses MAC sources de source. Parfois il est possible de distinguer des paquets d'inondation des paquets légitimes parce que les paquets d'inondation peuvent avoir des adresses sources incorrectes. N'importe quel paquet dont l'adresse source est non valide est susceptible de faire partie de l'inondation.

L'inondation peut provenir de plusieurs sources, bien que ce soit relativement peu commune pour des inondations de synchronisation.

Stimulus de Smurf

Afin de tracer un flux de stimuli de smurf, utilisez une liste d'accès comme 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
```

Notez que la première entrée ne se limite pas aux paquets destinés pour l'adresse de réflecteur. La raison pour ceci est que la plupart des attaques smurf utilisent de plusieurs réseaux de réflecteur. Si vous n'êtes pas en contact avec la cible finale, vous ne pouvez pas connaître toutes les adresses de réflecteur. Pendant que votre suivi obtient plus près de la source d'attaque, vous pouvez commencer à voir des requêtes d'écho allant de plus en plus aux destinations ; c'est un bon signe.

Cependant, si vous traitez beaucoup de trafic d'ICMP, ceci peut générer trop d'informations de journalisation pour que vous lisiez facilement. Si ceci se produit, vous pouvez limiter l'adresse de destination pour être l'un des réflecteurs qui est connu pour être utilisé. Une autre tactique utile est d'utiliser une entrée qui tire profit du fait que les netmasks de 255.255.255.0 sont très communs en Internet. Et, en raison de la manière que les attaquants trouvent des réflecteurs de surcharge, les adresses de réflecteur réellement utilisées pour des attaques smurf sont bien plus pour apparier ce masque. Les adresses d'hôte qui finissent dans .0 ou .255 sont très rares en Internet. Par conséquent, vous pouvez établir un système de reconnaissance relativement spécifique pour des flux de stimuli de smurf pendant que cette sortie affiche :

```
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
```

Avec cette liste, vous pouvez éliminer plusieurs des paquets de « bruit » de votre log, alors que vous avez toujours une bonne possibilité de noter les flux de stimuli supplémentaires pendant que vous obtenez plus près de l'attaquant.

Découverte sans « log-entrée »

Le mot clé log-input existe dans le Logiciel Cisco IOS versions 11.2 et plus tard, et dans certain logiciel 11.1-based créé spécifiquement pour le marché des fournisseurs de service. Des logiciels plus anciens ne prennent pas en charge ce mot clé. Si vous utilisez un routeur avec un logiciel plus ancien, vous avez trois alternatives viables :

- Créez une liste d'accès sans se connecter, mais avec les entrées qui apparient le trafic suspect. Appliquez la liste du *côté entrée de* chaque interface à leur tour, et observez les compteurs. Recherchez les interfaces avec des débits élevés de correspondance. Cette méthode a un temps système très petit de représentation, et est bonne pour l'identification des interfaces de source. Son plus grand inconvénient est qu'il ne donne pas des adresses sources de couche de liaison, et est donc utile en grande partie pour les lignes point par point.
- Créez les entrées de liste d'accès avec le **mot clé de journal** (par opposition à la log-**entrée**). De nouveau, appliquez la liste au côté entrant de chaque interface à leur tour. Cette méthode ne donne toujours pas des adresses MAC sources, mais peut être utile pour voir des données IP. Par exemple, pour vérifier qu'un flux de paquets fait partie vraiment d'une attaque. L'incidence des performances peut être moyenne à élevée et un plus nouveau logiciel exécute un logiciel mieux que plus ancien.
- Utilisez la commande de **détail de debug ip packet** de collecter des informations au sujet des paquets. Cette méthode donne des adresses MAC, mais peut avoir l'incidence importante 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. Employez une liste d'accès pour limiter l'élimination des imperfections seulement aux informations que vous avez besoin vraiment. Connectez-vous les informations de débogage à la mémoire tampon de log locale, mais arrêtez se connecter de mettent au point les informations aux sessions de telnet et à la console. Si possible, assurez quelqu'un pour être physiquement près du routeur, de sorte que ce puisse être alimentation faite un cycle selon les besoins.Souvenez-vous que la commande de **debug ip packet** n'affiche pas des informations sur des paquets à commutation rapide. Vous devez émettre la commande de **clear ip cache** afin de saisir les informations. Chaque commande **claire** te donne un ou deux paquets de sortie de débogage.

Informations connexes

- Kerberos
- Support et documentation techniques - Cisco Systems