Groupe de travail du réseauP . Ferguson
Demande de commentaires : 2827Cisco Systems, Inc.
Obsolètes : 2267 D. Senie
BCP : 38Amaranth Networks Inc.
Catégorie : Meilleure pratique actuelleMai 2000

Filtrage des entrées réseau : Vaincre les attaques par déni de service qui utilisent l'usurpation d'adresse IP

Statut de ce mémo

Ce document spécifie les meilleures pratiques actuelles pour la communauté Internet, et demande une discussion et des suggestions d'amélioration. La diffusion de ce mémo est illimitée.

Avis de droit d'auteur

Résumé

Les récents cas de diverses attaques par déni de service (DoS) utilisant de fausses adresses sources se sont révélés être un problème préoccupant pour les fournisseurs de services Internet et la communauté Internet dans son ensemble. Ce document présente une méthode simple, efficace et directe pour utiliser le filtrage du trafic entrant afin d'interdire les attaques par déni de service qui utilisent de fausses adresses IP à propager "derrière" le point d'agrégation d'un fournisseur de services Internet (ISP).

Table des matières

1. Introduction

La recrudescence des attaques par déni de service [1] visant diverses cibles sur l'internet a engendré de nouveaux défis au sein des communautés des fournisseurs de services internet (ISP) et de la sécurité des réseaux afin de trouver des méthodes nouvelles et innovantes pour atténuer ces types d'attaques. Les difficultés pour atteindre cet objectif sont nombreuses ; certains outils simples existent déjà pour limiter l'efficacité et la portée de ces attaques, mais ils n'ont pas été largement mis en œuvre.

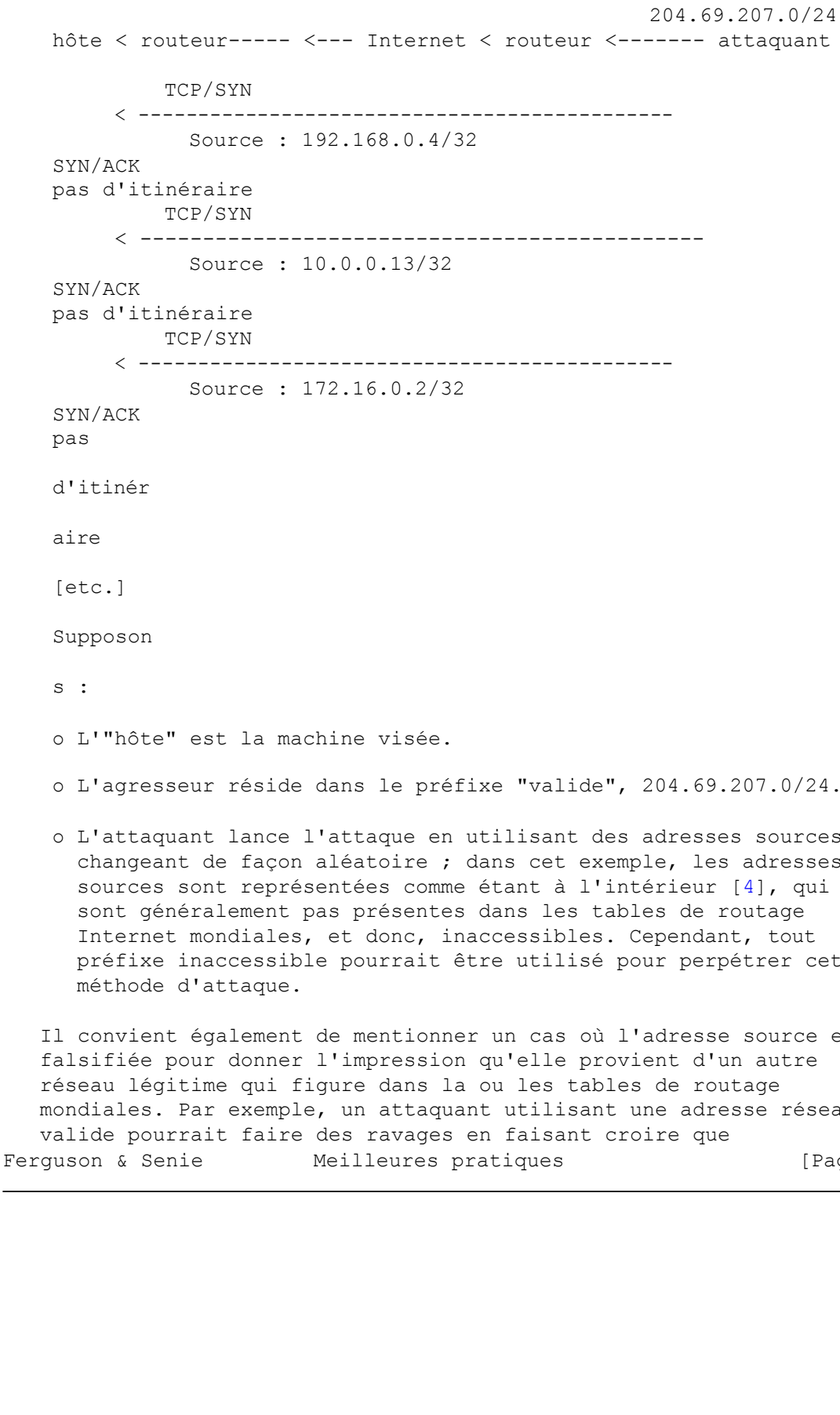
Cette méthode d'attaque est connue depuis un certain temps. Cependant, la défense contre cette méthode est une préoccupation constante. Bill Cheswick est cité dans [2] comme disant qu'il avait tiré un chapitre de son livre, "Firewalls and Internet Security" [3], à la dernière minute parce qu'il n'y avait aucun moyen pour un administrateur du système attaqué de défendre efficacement le système. En mentionnant la méthode, il s'est soucié d'encourager son utilisation.

Bien que la méthode de filtrage discutée dans ce document ne fasse absolument rien pour protéger contre les attaques par flooding qui proviennent de préfixes valides (adresses IP), elle interdira à un attaquant au sein du réseau d'origine de lancer une attaque de cette nature en utilisant de fausses adresses sources qui ne sont pas conformes aux règles de filtrage d'entrée. Tous les fournisseurs de connectivité Internet sont invités à mettre en œuvre le filtrage décrit dans le présent document afin d'interdire aux attaquants d'utiliser de fausses adresses sources qui ne résident pas dans une gamme de préfixes légitimement annoncés. En d'autres termes, si un FAI regroupe des annonces de routage pour plusieurs réseaux en aval, un filtrage strict du trafic devrait être utilisé pour interdire le trafic qui prétend provenir de l'extérieur de ces annonces regroupées.

Un avantage supplémentaire de la mise en œuvre de ce type de filtrage est qu'il permet de retrouver facilement la véritable source de l'auteur, puisque l'attaquant devra utiliser une adresse source valide et légitimement accessible.

2. Contexte

Un schéma simplifié du problème d'inondation du TCP SYN est présenté ci-dessous :



- L'"hôte" est la machine visée.
- L'agresseur réside dans le préfixe "valide", 204.69.207.0/24.
- L'attaquant lance l'attaque en utilisant des adresses sources changeant de façon aléatoire ; dans cet exemple, les adresses sources sont représentées comme étant à l'intérieur [4], qui ne sont généralement pas présentes dans les tables de routage Internet mondiales, et donc, inaccessibles. Cependant, tout préfixe inaccessible pourrait être utilisé pour perpétrer cette méthode d'attaque.

Il convient également de mentionner un cas où l'adresse source est falsifiée pour donner l'impression qu'elle provient d'un autre réseau légitime qui figure dans la ou les tables de routage mondiales. Par exemple, un attaquant utilisant une adresse réseau valide pourrait faire des ravages en faisant croire que

ue provient d'une organisation qui n'est pas à l'origine de l'attaque et qui est totalement innocente. Dans de tels cas, l'administrateur d'un système attaqué peut être enclin à filtrer tout le trafic provenant de la source apparente de l'attaque. L'ajout d'un tel filtre entraînerait alors un déni de service pour

des systèmes finaux légitimes et non hostiles. Dans ce cas, l'administrateur du système attaqué devient involontairement complice de l'attaquant.

Pour compliquer encore les choses, les attaques par flood TCP SYN entraînent l'envoi de paquets SYN-ACK à un ou plusieurs hôtes qui n'ont pas participé à l'attaque, mais qui deviennent des victimes secondaires. Cela permet à l'attaquant d'abuser de deux ou plusieurs systèmes à la fois.

Des attaques similaires ont été tentées en utilisant les inondations de l'UDP et de l'ICMP. La première attaque (UDP flooding) utilise de faux paquets pour essayer de connecter le service UDP de charge au service UDP d'écho à un autre site. Les administrateurs de systèmes ne doivent JAMAIS permettre aux paquets UDP destinés aux ports de diagnostic système provenant de l'extérieur de leur domaine administratif d'atteindre leurs systèmes. Cette dernière attaque (ICMP flooding), utilise une fonctionnalité insidieuse dans la mécanique de réplication de la diffusion des sous-réseaux IP. Cette attaque repose sur un routeur desservant un grand réseau de diffusion à accès multiples pour encadrer une adresse de diffusion IP (telle qu'une adresse destinée à 10.255.255.255) dans une trame de diffusion de couche 2 (pour ethernet, FF:FF:FF:FF:FF:FF). Le matériel NIC Ethernet (matériel de la couche MAC, en particulier) n'écoute qu'un nombre limité d'adresses en fonctionnement normal. La seule adresse MAC que tous les appareils partagent en fonctionnement normal est la diffusion du média, ou FF:FF:FF:FF:FF:FF:FF. Dans ce cas, un appareil prendra le paquet et enverra une interruption pour le traitement. Ainsi, une inondation de ces trames de diffusion consommera toutes les ressources disponibles sur un système final [9]. Il est peut-être prudent que les administrateurs système envisagent de s'assurer que leurs routeurs de frontière n'autorisent pas par défaut la transmission de paquets de diffusion dirigée par leurs routeurs.

Lorsqu'une attaque TCP SYN est lancée en utilisant une adresse source injoignable, l'hôte cible tente de réserver des ressources en attendant une réponse. L'attaquant change constamment la fausse adresse source sur chaque nouveau paquet envoyé, épuisant ainsi les ressources supplémentaires de l'hôte.

Par ailleurs, si l'attaquant utilise l'adresse d'hôte valide d'une autre personne comme adresse source, le système attaqué enverra un un grand nombre de paquets SYN/ACK à ce qu'il croit être l'auteur de la séquence d'établissement de la connexion. De cette manière, l'attaquant endommage deux systèmes : le système cible de

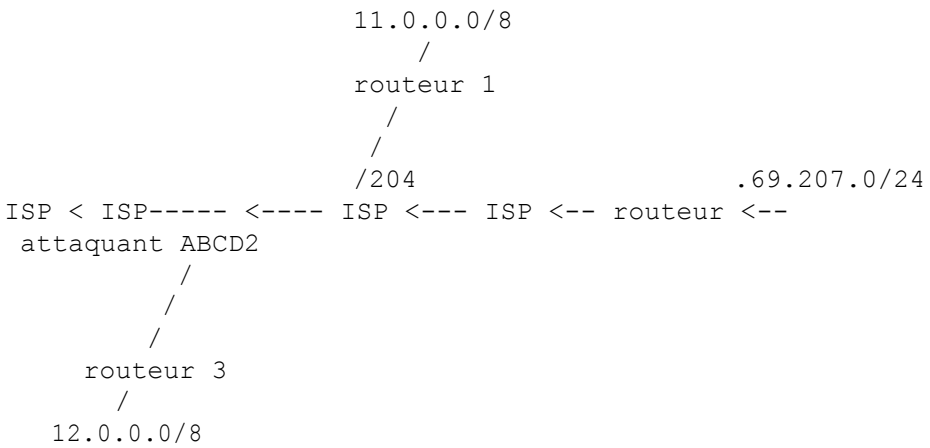
destination et le système qui utilise effectivement l'adresse usurpée dans le système de routage global.

Les deux méthodes d'attaque ont pour résultat une dégradation extrême des performances ou, pire, un crash du système.

En réponse à cette menace, la plupart des fournisseurs de systèmes d'exploitation ont modifié leurs logiciels pour permettre aux serveurs ciblés de supporter des attaques avec des taux de tentatives de connexion très élevés. C'est une partie bienvenue et nécessaire de la solution au problème. Le filtrage des intrusions prendra du temps pour être mis en œuvre de manière généralisée et être pleinement efficace, mais les extensions des systèmes d'exploitation peuvent être mises en œuvre rapidement. Cette combinaison devrait s'avérer efficace contre l'usurpation d'adresse source. Voir [1] pour des informations sur les mises à jour des logiciels des fournisseurs et des plates-formes.

3. Limiter le trafic de faux

Les problèmes rencontrés avec ce type d'attaque sont nombreux, et impliquent des lacunes dans les implémentations des logiciels hôtes, les méthodologies de routage, et les protocoles TCP/IP eux-mêmes. Toutefois, en limitant le trafic de transit provenant d'un réseau en aval à des préfixes connus et intentionnellement annoncés, le problème de l'usurpation d'adresse source peut être pratiquement éliminé dans ce scénario d'attaque.



Dans l'exemple ci-dessus, l'attaquant réside dans le préfixe 204.69.207.0/24, qui est fourni par le FAI D. Un filtre de trafic d'entrée sur le lien d'entrée (input) du "routeur 2", qui fournit la connectivité au réseau de l'attaquant, restreint le trafic pour n'autoriser que le trafic provenant d'adresses sources situées dans le préfixe 204.69.207.0/24, et interdit à un attaquant d'utiliser des adresses sources "invalides" qui résident en dehors de cette plage de préfixes.

En d'autres termes, le filtre d'entrée sur le "routeur 2" ci-

dessus serait vérifié : l'adresse source du paquet IF à

partir de 204.69.207.0/24
Ensuite, le cas échéant

L'adresse source d'IFpacket est tout
autre chose THENdeny packet

Les administrateurs de réseau doivent consigner les informations relatives aux paquets qui sont abandonnés. Cela permet ensuite de surveiller toute activité suspecte.

4. Autres possibilités d'équipement de mise en réseau

Des fonctions supplémentaires devraient être envisagées pour les futures mises en œuvre de la plate-forme. La suivante mérite d'être signalée :

- Mise en place d'un filtrage automatique sur les serveurs d'accès à distance.
  Dans la plupart des cas, un utilisateur qui se connecte à un serveur d'accès est un utilisateur individuel sur un seul PC. La SEULE adresse IP source valide pour les paquets provenant de ce PC est celle attribuée par le FAI (qu'elle soit attribuée statiquement ou dynamiquement). Le serveur d'accès à distance pourrait vérifier chaque paquet en entrée pour s'assurer que l'utilisateur n'usurpe pas l'adresse source des paquets dont il est à l'origine. Bien entendu, des dispositions doivent également être prises pour les cas où le client attache légitimement un réseau ou un sous-réseau via un routeur distant, mais cela pourrait certainement être mis en œuvre en tant que paramètre facultatif. Nous avons reçu des informations selon lesquelles certains fournisseurs et certains FAI commencent déjà à mettre en œuvre cette possibilité.

Nous avons envisagé de suggérer que les routeurs valident également l'adresse IP source de l'expéditeur comme suggéré dans [8], mais cette méthodologie ne fonctionnera pas bien dans les réseaux réels actuels. La méthode suggérée consiste à rechercher les adresses sources pour voir si la voie de retour vers cette adresse passerait par la même interface que celle où le paquet est arrivé. Avec le nombre de routes asymétriques sur Internet, cela serait clairement problématique.

5. Passif

Ce type de filtrage est susceptible de briser certains types de services "spéciaux". Il est toutefois dans l'intérêt du FSI offrant ces types de services spéciaux d'envisager d'autres

méthodes de mise en œuvre de ces services pour éviter d'être affecté par le filtrage du trafic entrant.

L'IP mobile, tel que défini dans [6], est spécifiquement affecté par le filtrage du trafic entrant. Comme spécifié, le trafic vers le nœud mobile est tunnelisé, mais le trafic en provenance du nœud mobile ne l'est pas. Il en résulte que les paquets provenant du ou des nœuds mobiles ont des adresses sources qui ne correspondent pas au réseau où la station est connectée. Pour tenir compte du filtrage des entrées et d'autres préoccupations, le groupe de travail sur l'IP mobile a élaboré une méthodologie pour les "tunnels inversés", spécifiée dans [7]. Celle-ci prévoit une méthode pour que les données transmises par le nœud mobile soient acheminées vers l'agent d'origine avant d'être transmises à l'internet. Le système de tunnels inversés présente des avantages supplémentaires, notamment une meilleure gestion du trafic de multidiffusion. Les personnes qui mettent en œuvre des systèmes IP mobiles sont encouragées à appliquer cette méthode de tunnelage inverse.

Comme mentionné précédemment, si le filtrage du trafic entrant réduit considérablement le succès de l'usurpation d'adresse source, il n'empêche pas un attaquant d'utiliser une fausse adresse source d'un autre hôte dans la plage de filtrage autorisée par le préfixe. Il garantit toutefois que lorsqu'une attaque de cette nature se produit effectivement, un administrateur de réseau peut être sûr que l'attaque provient effectivement des préfixes connus qui sont annoncés. Cela simplifie la recherche du coupable et, au pire, l'administrateur peut bloquer une série d'adresses sources jusqu'à ce que le problème soit résolu.

Si le filtrage d'entrée est utilisé dans un environnement où le DHCP ou le BOOTP est utilisé, l'administrateur réseau serait bien avisé de s'assurer que les paquets avec une adresse source de 0.0.0.0 et une destination de 255.255.255.255 sont autorisés à atteindre l'agent de relais dans les routeurs, le cas échéant. La portée de la réplication de la diffusion dirigée devrait cependant être contrôlée et ne pas être transmise arbitrairement.

6. Résumé

Le filtrage du trafic d'entrée à la périphérie des réseaux connectés à Internet réduira l'efficacité des attaques de déni de service par usurpation d'adresse source. Les fournisseurs de services et les administrateurs de réseaux ont déjà commencé à mettre en œuvre ce type de filtrage sur les routeurs périphériques, et il est recommandé à tous les fournisseurs de services de le faire dès que possible. En plus d'aider la communauté Internet dans son ensemble à vaincre cette méthode d'attaque, elle peut également aider les fournisseurs de services à localiser la source de l'attaque si les fournisseurs de services peuvent démontrer catégoriquement que leur réseau dispose déjà d'un filtrage d'entrée sur les liens des clients.

Les administrateurs de réseaux d'entreprise devraient mettre en place un filtrage pour s'assurer que leurs réseaux d'entreprise ne sont pas la source de tels problèmes. En effet, le filtrage pourrait être utilisé au sein d'une organisation pour s'assurer que les utilisateurs ne causent pas de problèmes en connectant incorrectement les systèmes aux mauvais réseaux.

Le filtrage pourrait également, en pratique, bloquer un employé mécontent des attaques anonymes.

Il est de la responsabilité de tous les administrateurs de réseau de s'assurer qu'ils ne deviennent pas la source involontaire d'une attaque de cette nature.

7. Considérations de sécurité

L'objectif premier de ce document est d'améliorer les pratiques de sécurité et la sensibilisation de la communauté Internet dans son ensemble ; à mesure que les fournisseurs d'accès à Internet et les administrateurs de réseaux d'entreprise mettront en œuvre le filtrage d'intrusion, la possibilité pour un attaquant d'utiliser de fausses adresses sources comme méthode d'attaque diminuera considérablement. Le suivi de la source d'une attaque est simplifié lorsque la source est plus susceptible d'être "valable". En réduisant le nombre et la fréquence des attaques dans l'ensemble de l'internet, on disposera de plus de ressources pour suivre les attaques qui se produisent en fin de compte.

8. Remerciements

L'ensemble du groupe North American Network Operators Group (NANOG) [5] mérite un crédit particulier pour avoir discuté ouvertement de ces questions et cherché activement des solutions possibles. Nous remercions également Justin Newton [Priori Networks] et Steve Bielagus [IronBridge Networks] pour leurs commentaires et leurs contributions.

9. Références

[1] Avis du CERT CA-96.21 ; attaques par inondation du TCP SYN et par usurpation d'adresse IP ; 24 septembre 1996.

[2] B. Ziegler, "Hacker Tangles Panix Web Site", Wall Street Journal, 12 septembre 1996.

[3] "Pare-feu et sécurité sur Internet : Repelling the Wily Hacker" ; William R. Cheswick et Steven M. Bellovin, Addison-Wesley Publishing Company, 1994 ; ISBN 0-201-63357-4.

[4] Rekhter, Y., Moskowitz, R., Karrenberg, D., de Groot, G. et E. Lear, "Address Allocation for Private Internets", RFC 1918,

février 1996.

[5] Le Groupe des opérateurs de réseaux nord-américains ; http://www.nanog.org.

[6] Perkins, C., "IP Mobility Support", RFC 2002, octobre 1996.

[7] Montenegro, G., "Reverse Tunneling for Mobile IP", RFC 2344, mai 1998.

[8] Baker, F., "Requirements for IP Version 4 Routers", RFC1812, juin 1995.

[9] Grâce à : Craig Huegen ; Voir : http://www.quadrunner.com/~chuegen/smurf.txt.

10. Adresses des auteurs

Paul Ferguson
Cisco Systems, Inc.
13625 Dulles Technology Dr.
Herndon, Virginie20170 USA

Courriel :

ferguson@cisco.com

Daniel Senie
Amaranth Networks Inc.
324 Still River
Road Bolton, MA
01740 USA

Courriel : dts@senie.com

11. Déclaration complète sur le droit d'auteur

Remerciements

Le financement de la fonction d'éditeur RFC est actuellement assuré par l'Internet Society.