La protection des reseaux contre les attaques DoS

Amarir Hakim Danes Adrien Doffe Sidney

Mai 2009

Table des matières

Introduction

De nos jours les réseaux informatiques sont de plus en plus présents dans les milieux professionnels ainsi que chez les particuliers. Ces dix dernières années ont vu l' avènement de l' internet, et son apparition dans la plupart des foyers, du moins dans les pays développés. Cette évolution a favorisée la communication, l' expansion du commerce, l' accès à l'information et de nombreuses sociétés dépendent maintenant entièrement de leur réseaux. Les particuliers utilisent de plus en plus l' internet pour échanger des données sensibles telles que des informations de paiement en ligne.

Toutes ces innovations ont permis de faciliter la vie de tout à chacun mais ont aussi contribué au développement de nouveaux risques que sont les attaques informatiques. Les méthodes de piratages sont de plus en plus nombreuses et perfectionnées, elles peuvent se traduire par des vols d'informations confidentielles, des destructions de données numériques, des coupures de services voire même des dégâts matériels. Nous nous intéresserons ici à un type d'attaque assez répandu : le Déni de Service ou DoS. Cette attaque bien que peu dangereuse pour l'intégrité des données peut s'avérer très pénalisante pour une société car elle vise a rendre indisponible une ressource réseau. Ainsi une société de e-commerce ne peut se permettre de perdre son site internet même pour quelques minutes car elle perdrait des milliers voire des millions d'euros.

Nous allons tout d'abord définir les attaques DoS, pour mieux comprendre d'où elles proviennent, comment elles sont exécutées et quelles en sont les principales conséquences. Nous verrons ensuite comment détecter et contrer de telles attaques dans un réseau en se penchant sur l'efficacité des solutions existantes. Puis nous tenterons de proposer une solution adaptée pour les détecter.

1 Une vulnérabilité connue : le Déni de Service

1.1 D'ou proviennent les attaques et pourquoi ?

1.1.1 Que sont les attaques DoS ?

Les attaques par déni de services (denial of service en anglais ou DoS) sont des attaques qui visent à rendre une machine ou un réseau indisponible durant une certaine période. En apparence une telle attaque peut sembler inoffensive si elle vise un réseau ou un ordinateur particulier, mais elle peut s'avérer redoutable lorsqu'elle vise un serveur ou des ressources matérielles appartenant à une grande société dépendante de son infrastructure réseau.

Ce genre d'attaque est très répandue sur les réseaux car elle est assez simple à mettre en oeuvre mais peut néanmoins avoir des conséquences désastreuses. De plus la détection et la prévention de ces attaques sont très difficiles car elles peuvent prendre des formes très variées, quasiment tout les systèmes informatiques sont vulnérable et même des équipements coûtant des milliers de dollar ne peuvent parfois rien faire contre de telles attaques.

C'est pour ces raisons que les dénis de service sont utilisés dans de multiples situations et par des personnes très variées, allant de l'adolescent curieux voulant s'essayer au piratage informatique, jusqu' aux multinationales attaquant leurs concurrents pour prendre la tête dans la course au pouvoir. Les équipements touchés peuvent être des routeurs, des serveurs web, des serveur DNS des serveurs mails...

Tous ces équipements sont critiques, la surcharge d'un routeur entraînera un retard important des décisions de routage voire une impossibilité totale de router les paquets sur un réseau le rendant totalement inefficace à communiquer avec d'autres. Les surcharges de serveurs empêcheront les utilisateurs d'accéder aux services tels que les mails, ou l' internet, ils subiront des délais d'attente considérables et seront même parfois dans l'impossibilité de joindre leur ressource.

Le principe général des attaques DoS, consiste à envoyer des données ou des paquets dont la taille ou le contenu est inhabituel, ceci à pour effet de provoquer des réactions inattendues du réseau ou de la machine cible, pouvant aller jusqu'à l'interruption du service.

1.1.2 Les conséquences

Une attaque par DoS peut avoir de nombreuses formes qui engendrent chacune de nombreuses conséquences, représentant une palette de risques très variées. Les attaques les plus dévastatrices peuvent amener, que ce soit de manière directe ou indirecte, à des pertes d'argents colossales

pour une société dont la principale activité est basée sur un flux d'informations Internet. Dans un monde où un grand nombre des entreprises utilisent leurs sites internet comme leur principale vitrine, et où leur chiffre d'affaires dépend de ce même site, les attaques contres celui-ci peuvent amener à des pertes d'argent colossales.

Une attaque par déni de service étant, le plus souvent temporaire, les auteurs utilisent allègrement le chantage pour extorquer des fonds aux entreprises. Il est clair que pour une société d'e-commerce par exemple, un blocage de son site pourrait lui faire perdre plusieurs millions par heure. Payer les auteurs peut donc parfois s'avérer être une solution beaucoup moins coûteuse, même si cela signifie céder au chantage, et que rien ne garantit que l'auteur de l'attaque ne récidivera pas. On remarque, au fil des années, que ce genre de pratique est de plus en plus utilisé dans le monde du cyber-terrorisme, puisque ces attaques sont relativement simples à mettre en place, et que toutes les sociétés dépendantes d'internet sont menacées.

1.1.3 Historique

Comme on a pu le voir auparavant, le déni de service est une attaque qui peut occasionner d'importantes conséquences. En voici quelques exemples qui furent tous considérées comme importants :

- En juin 1998, L'attaque Syndrop basé sur Teardrop en TCP avec le bit SYN et des champs invalides tel que le numéro de séquence, la taille de fenêtre, etc. L'impact est de bloquer les stations Windows NT4 SP3 par un Freeze.

- En Aout 2005, l'Américain Jasmine Singh, âgé de 17 ans, a étè condamné à cinq ans de prison et 35000$ d'amende pour avoir, à 5 reprises, rendus injoignables les sites Internet Jersey-Joe.com et Distant Replays. Il agissait pour le compte du propriétaire d'une société concurrente, âgé lui de 18 ans. Les plaignants ont estimés le préjudice à 1,5 millions de dollars. Il utilisait pour cela un virus pour se créer un réseau de botnet, puis utiliser celui-ci pour lancer son attaque.

- Les 21 et 22 octobre 2002, Une attaque de type Ping Flood a été réalisé en mode distribuée sur les 13 serveurs racines DNS de l'Internet. Seulement 4 à 6 serveurs (selon les sources) sur 13 sont restés disponibles. Malgré le succès relatif de cette attaque, aucune perturbation au niveau mondial n'a été observé.Ceci démontre la puissance de ces serveurs, et que seul un petit nombre de ces serveurs est nécessaire pour assurer le fonctionnement des DNS au niveau mondial !

- En août 2003, Le virus Blaster, était programmé pour effectuer une attaque de déni de service distribué sur le site de mise à jour Windows. Mais le reverse engineering effectué à permis de

comprendre son fonctionnement et sa cible. Microsoft a donc fait migré son serveur sur une autre adresse pour contrer la future attaque. Microsoft avait par ailleurs désactivé l'entrée DNS sur www.windowsupdate.com le temps de l'attaque, ce qui a considérablement atténué les effets.

- Le 25 janvier 2003, L'attaque Slammer s'enclencha à 5h30 UTC. Plusieurs vols aériens sont annulés, il y a des perturbations pour les paiements par cartes de crédit et les guichets automatiques subissent eux aussi des problèmes, plusieurs grandes entreprises voient leurs réseaux inutilisables. C'est le résultat du virus SLAMMER qui provoqua un déni de service généralisé. Basé sur UDP, il s'est propagé en moins de 30 minutes sur plus de 75 000 ordinateurs connectés à Internet.

- En 2004, Huit ans de prison ont été prononcé pour un groupe de trois russes qui ont attaqué le site DoubleClick, le 28 juillet 2004, entraînant le site de ses clients, qui dépendent de sa technologie pour gérer leurs bannières de publicité. Leurs sites furent fortement ralentis ou complètement paralysés pendant de longues heures. Ils ont extorqués plus de 4 millions d'Euros repartis sur plus de 54 sites WEB d'une trentaine de pays. Cette peine est la plus lourde prononcée en Russie, car la justice a considéré l'affaire comme relevant de l'extorsion en bande organisée et non du seul piratage informatique.

- Fin septembre 2004, aux Etats-Unis, la société Authorize.net qui fournit une solution de paiement par carte bancaire à 91.000 e-détaillants, a subi une attaque d'une ampleur inégalée ; il avait reçu au préalable une lettre d'extorsion.

- Le 12 août 2008, la presse internationale rapporte que des pirates russes ont lancé une cyber-attaque massive contre de nombreux sites et serveurs géorgiens alors même que le président russe Dimitri Medvedev avait donné l'ordre le matin de cesser les hostilités sur le terrain. Les firewall de la société ont bloqué la plupart de ces attaques mais le site est devenu plusieurs fois inaccessible. La Shadowserver Foundation basée aux Etats-Unis, qui traque les attaques sur Internet, a déclaré avoir remarqué pendant le week-end que des ordres d'attaque avaient été donnés par des ordinateurs "zombies" en réseau, des "Botnets" détournés par des pirates. Lundi, Shadowserver a ajouté que les hackers avaient pris le contrôle du site du Parlement de Géorgie ainsi que le Ministère géorgien des Affaires étrangères et y avaient remplacé les photos officielles par des images montrant le président en Nazi, dressant un parallèle entre le président Saakachvili et Adolf Hitler.

1.2 Les différentes attaques DoS

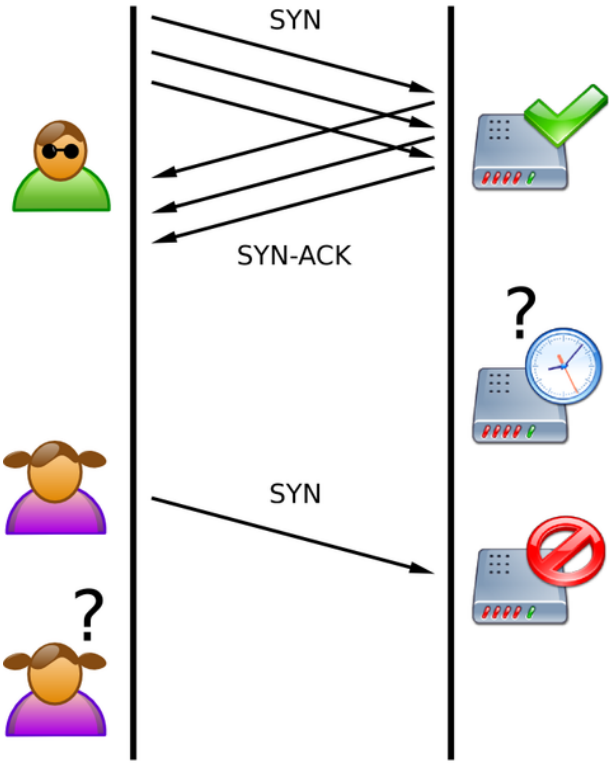
Les attaques DoS prennent de multiple formes et utilisent de nombreuse méthodes différentes pour mettre hors service une ressource réseau, nous allons essayer de définir ici de manière non exhaustive les différentes attaques connues et répandues.

1.2.1 Les attaques par surcharge

Une des méthode les plus répandue et une des plus simple a mettre en oeuvre est de surcharger complètement la cible de requêtes de toutes sortes. On distingue quatre grands type d'attaques utilisant différents protocoles et couches réseaux.

Le SYN flood Cette attaque utilise des paquets TCP contenant le flag SYN. Ce flag signifie à la cible que l'on veut initier une connexion avec elle. En envoyant un nombre très important de ces paquets, on oblige le serveur à démarrer une socket de connexion pour chaque requête, il enverra donc des paquets contenant les flag SYN,ACK pour établir la connexion mais ne recevra jamais de réponses. Le serveur aura donc un grand nombre de connexion en attente et arrivera à saturation jusqu'à ne plus pouvoir répondre aux connexions légitimes des utilisateurs.

Pour éviter de se faire repérer la source peut combiner cette attaque avec le changements du champs IP source des paquets envoyés ce qui redirigera les réponses de la cible vers une autre destination. Ce type d'usurpation est aussi appelé attaque en aveugle car les réponses venant de la cible ne pourront être reçu par l'attaquant, il exécute l'attaque mais ne peut pas vérifier son efficacité autrement qu'en essayant une connexion légitime au serveur.



Le PING flood Une des attaque les plus simple à mettre en place. Elle consiste à simplement envoyer un nombre maximal de PING simultané jusqu'à saturer la victime. On utilise généralement la commande ping sous Linux mais une des conditions pour que l'attaque soit efficace est de posséder plus de bande passante que la victime.

Le Smurf Les attaques Smurf profite d'une faiblesse de IPv4 et d'une mauvaise configuration pour profiter des réseaux permettant l'envoi de paquets au broadcast. Le broadcast est une adresse IP qui permet de joindre toutes les machines d'un réseau. L'attaquant envoie au broadcast des paquets contenant l'IP source de la victime ainsi chaque machine sur le réseau va répondre a la cible a chaque requête de l'attaquant. On se sert ainsi du réseau comme un amplificateur pour perpétrer l'attaque, cette méthode porte aussi le nom d'attaque réfléchie permettant à l'attaquant de couvrir ces traces et de rendre l'attaque plus puissante.

Ces attaques peuvent être vraiment très efficaces c'est pourquoi une association Smurf Amplifier Registry existe pour aider les opérateurs à détecter les réseaux mal configurer. Les particuliers peuvent aussi demander à leurs opérateurs de désactiver le broadcast dirigé pour éviter ce type de désagréments

1.2.2 Les attaques par failles

Un autre moyen de réaliser un DoS consiste à exploiter les nombreuses failles présentes dans les systèmes d'informations. Au lieu de chercher à surcharger la cible, on va simplement la forcer a réagir de façon bien définit en lui soumettant des informations qu'elle ne peut gérer. Les systèmes Microsoft Windows sont par exemple très vulnérables à ce genre d'attaques. De nombreux moyens existent afin de tromper le système pour l'exploiter. Néanmoins ces attaques sont de moins en moins nombreuses et de moins en moins efficaces car les systèmes d'exploitations actuels sont de plus en plus sécurisés.

Teardrop Attack Elle consiste à envoyer des paquets IP invalides à la cible, ces paquets peuvent être fragmentés, ou contenir des données corrompues ou qui dépassent la taille réglementaire. Sur certains systèmes comme les Windows avant 98 ou les Linux avant 2.0.32, ces paquets ne peuvent être interprétés et rendrons la machine inopérante.

Ping of Death Elle reprend le principe de l'attaque Teardrop mais avec des paquets ICMP. Les paquets ICMP possèdent généralement un champ data de 56 octets. Certains systèmes deviennent vulnérables en envoyant des PING avec un champs de données plus important. Les systèmes en général ne sont pas prévus pour recevoir des paquets ICMP plus gros que les paquets IP traditionnels (64K), mais les PING peuvent être fragmentés. Cependant, une fois rassemblée, ces paquets causeront une saturation de la mémoire tampon . Cette attaque est de nos jours obsolète car la majorité des systèmes ont été corrigé. Elle touchait tous les systèmes d'exploitations et même les équipements réseaux tels que les routeurs et les imprimantes.

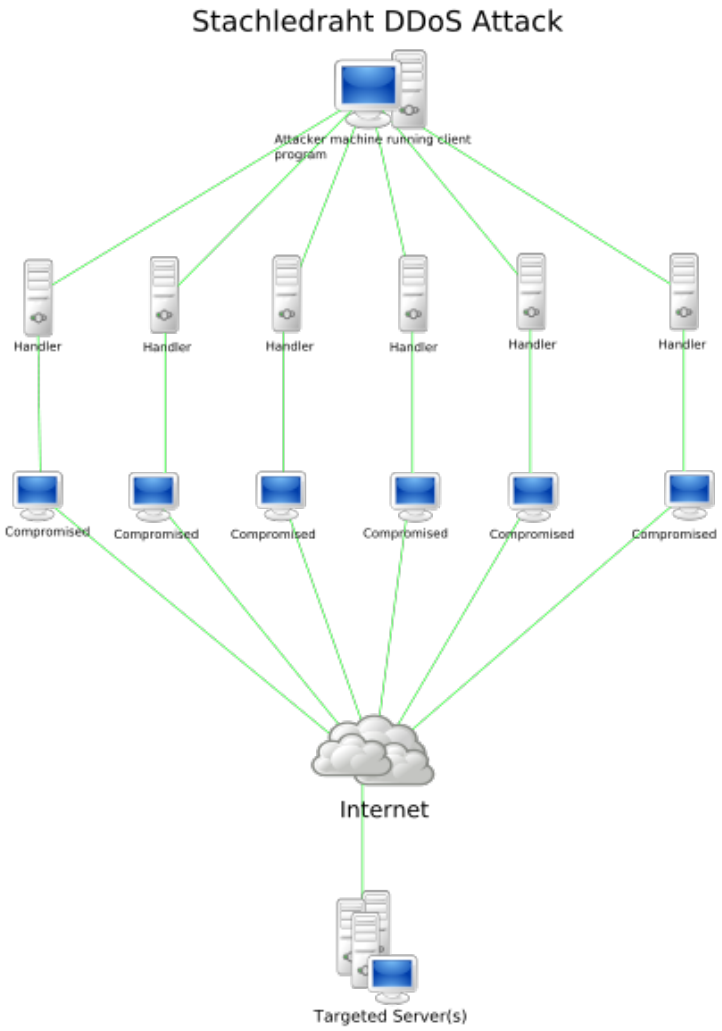
Permanent DoS Ces attaques peuvent s'avérer très dangereuses car elles permettent à l'attaquant d'altérer le matériel de la victime de façon irréversible nécessitant le remplacement des équipements. Elles utilisent des failles dans les pilotes matérielles pour changer les firmwares matériels et ainsi mettre hors service les machines.

Failles applicative De nos jours, les systèmes d'exploitations sont de plus en plus sécurisés et les failles sont de moins en moins courantes. Par contre, de nombreuses applications, installé par l'utilisateur, peuvent se révéler faible et présenter des moyen d'exploiter une machine. L'attaquant utilise ces failles pour ensuite perpétrer des actions visant a rendre la machine indisponible. Il peut par exemple saturer le disque dur jusqu'à ce que la cible ne puisse plus fonctionner. Il peut exécuter un code créant des processus se dédoublant l'infini aussi appeler des fork bomb. On peut encore rediriger toutes les connections sortantes d'une machine sur elle même pour qu'elle se sature toute seule.

1.2.3 Les attaques distribuées

La plupart des attaques, cité plus haut, peuvent être exécutés de manière distribuée, on parle alors de DDoS pour Distributed Denial of Service. Les attaques distribuées se basent sur ce fait : attaquer une cible toute seule se traduit souvent par un échec, alors que si un grand nombre de machines s'attaquent à la même cible alors l'attaque a plus de chance de réussir.

Il y a deux grandes façons d'exécuter un DDoS. on peut tout d'abord utiliser un groupe de personnes en connivence et convenir d'un moment et d'une façon bien précise de mener l'attaque. Ce n'est pas la méthode la plus simple et elle nécessite beaucoup d'organisations et de logistiques. L'autre façon est de disposer d'un nombre important de machines corrompues à travers le monde et de les utiliser pour perpétrer l'attaque. Ceci nécessite au préalable une grande préparation pour corrompre les machines et les maintenir sous contrôle, mais présente aussi un avantage certain de pouvoir accomplir l'attaque seul.



1.2.4 Les attaques par usurpation

ARP spoof L' ARP spoof est une attaque très puissante qui permet, en général, de sniffer le trafic sur le réseau en s'interposant entre une ou des victimes et la passerelle. Elle permet même de sniffer et récupérer des mots de passes sur des connexions sécurisés SSL. L'attaque inonde le réseau avec des trames ARP liant l'adresse physique de l'attaquant avec la passerelle. De cette manière, le cache ARP des victimes est corrompu et tout le trafic est redirige vers le poste de l'attaquant.

Dans le cadre d'un déni de service, on peut utiliser l'ARP spoof en détournant un peu son utilisation classique. Au lieu de se faire passer pour la passerelle, l'attaquant corrompt la table

ARP de la victime avec une route invalide, ce qui va avoir pour effet de couper la victime du réseau. Elle sera complètement isolée et restera inutilisable tant que le cache ARP sera corrompu.

DNS spoof De la même manière, on peut corrompre le DNS d'une victime. Normalement, ceci permet de rediriger la victime vers des sites pirates que l'on contrôle mais dans le cadre d'un déni service, on corrompt le cache DNS de fausse informations qui rendront impossible l'accès aux sites web.

1.3 Les outils d'attaques

Il existe de nombreux outils servant à perpétrer des dénis de services selon le système, que l'on soit sous Windows, Linux ou autres systèmes d'exploitations. Linux reste qu'en même le système comportant le plus d'outils dont nous détaillerons quelques fonctions.

1.3.1 Hping

La simple commande ping peut déjà se révéler assez utile si l'on dispose de beaucoup de bande passante et de bonnes options. Mais il existe un programme, hping qui est bien plus puissant. Il ne se contente pas d'envoyer des paquets ICMP, il gère aussi les paquets TCP, UDP et permet en plus de modifier certains champs des en-têtes de ces paquets. Il comporte aussi un traceroute et des capacités à détecter les systèmes d'exploitations d'une cible.

Quelque commandes utiles :

- hping 192.168.0.1 -1 : le ping classique
- hping 192.168.0.1 -a 192.168.0.11 : l'option -a définit l'adresse source du ping et donc l'adresse qui recevra les réponse en provenance de la cible
- hping 192.168.0.1 -i u10 : pour envoyer 1 paquet toutes les 10 s'avérer

Cet outil peut s'avérer très puissant et peut être utilisé par exemple pour effectuer une attaque SYN flood, Ping flood et Smurf.

Exemple d'attaques SYN flood

- hping 192.168.0.1 -S –fast : pour envoyer 10 paquets par secondes contenant le flag SYN

– hping 192.168.0.1 -S –fast -a 192.168.0.100 : pour effectuer la même attaque en fesant passer la machine 192.168.0.100 pour l'attaquant

Exemple d'attaques PING flood

– hping 192.168.0.1 -1 –fast : pour envoyer 10 pings par secondes

– hping 192.168.0.1 -1 –fast -a 192.168.0.100 : pour effectuer la même attaque en fesant passer la machine 192.168.0.100 pour l'attaquant

Exemple d'attaque Smurf

– hping 192.168.0.255 -1 –fast -a 192.168.0.1 : pour envoyer 10 pings par secondes au broadcast qui répondra a la cible 192.168.0.1

Hping peut être utilise dans beaucoup de situations pour analyser et effectuer des audits de réseaux informatique ainsi que leurs configurations.

1.3.2 TFN2K

Ce programme est destine aux attaques DDoS aussi appelées attaques distribuées. Il est complexe et très difficile à contrer. En effet, il utilise un système client serveur communiquant de façon crypté pour échanger des données sur l'attaque. Il permet d'attaquer plusieurs client de façon aléatoire grâce a des paquets ICMP, TCP, ou UDP.

1.3.3 Dsniff

Dsniff est une suite d'outils destiné aux attaques de type man-in-the-middle qui permet entre autres de mettre en pratique l'arp-spoof aussi appeler arp poisoning. La suite est constituée de arpspoof, dsniff, msgsnarf, urlsnarf qui permettent de sniffer le réseaux, une fois l'attaque mise en place. Dans le cas d'une attaque DoS par arp poisoning, le but recherché est de corrompre la table ARP de la victime pour l'empêcher d'avoir accès au réseau. Pour se faire, on peut utiliser la commande arpspoof -i eth0 192.168.0.1 et se faire passer pour la passerelle du réseau, ainsi tous les paquets du réseau seront reçus par la machine de l'attaquant et ne seront plus router vers l'internet. La commande utilise des trames ARP-reply de niveau 2 envoyées au broadcast FF :FF :FF :FF :FF :FF pour stipuler que l' adresse de la passerelle se trouve a l'adresse MAC de l'attaquant.

1.3.4 Ettercap

Ettercap est un analyseur de réseau qui permet aussi de mettre en place des attaques DoS par surcharge ou par ARP poisoning, mais cette fois de façon graphique. Il contient des plugins pour isoler des machines sur le réseau et de les rendre inefficaces.

2 Les moyens de se prémunir

2.1 Les modes de détections

Comme on a pu le voir dans la partie précédente, il est très important de se prémunir contre ces attaques faciles à réaliser et pouvant provoquer de graves dégâts. Le problème est qu'il est très dur de les détecter efficacement, car elles ne sont pas évidentes à différencier des autres attaques. En effet, il faut réussir à différencier un grand nombre de connexions légitimes d'une attaque afin de détecter le minimum possible de faux positives tout en ne laissant passer aucunes attaques ! Parfois, un déni de service peut même résulter de la popularité soudaine d'un site web sans qu'il y est d'attaquant mal intentionné, dans ce cas comment proposer une méthode de détection efficace dans toutes les situations. Il existe plusieurs moyens, plus ou moins efficace, permettant de détecter et/ou de bloquer ces attaques.

2.1.1 Les mise a jours systèmes

La première chose à faire, pour éviter les dénis de services applicatifs, est de maintenir tous les logiciels de son système à jour puisque les mises à jours permettent souvent de corriger des failles logicielles, qui peuvent etre utilisées par un attaquant, pour mettre l'application (Par exemple un serveur web) hors service, ou pire, le serveur. Il est donc impératif de mettre son système à jour très régulièrement C'est un moyen très simple à mettre en place pour se protéger des attaques applicative, mais les administrateurs effectuent souvent ces mise à jour irrégulièrement. Une autre chose sur laquelle il faut porter l'attention : la configuration de ces serveurs. Une mauvaise configuration de ces serveurs peut donner accès à des fichiers importants. Mais cette fois-ci, il est beaucoup plus dur de mettre en place une configuration bien sécurisée car il faut penser à beaucoup de choses. De plus, lorsque qu'on exécute une modification sur son serveur, il faut penser si celle-ci n'a pas d'impact sur les autres services, et donc sur la sécurité du serveur.

Aujourd'hui, des systèmes tels que Linux intègrent des moyens primitifs de protections. Par exemple, on peut éditer des options dans le fichier sysctl.conf, généralement placer dans /etc. Ces systèmes de protections sont notamment, le SYNCookie. Cette méthode stocke des données concernant chaque connexion reçu par la machine telle que l'adresse IP source, le numéro de port, l'âge de la connexion. En analysant ces données, on peut trouver des comportements suspects et se prémunir de certains types d'attaques. Les attaques n'ont pas les même conséquences suivants les systèmes et les configurations utilisées.

2.1.2 Les sondes IDS/IPS

Une manière supplémentaire de se protéger des attaques par déni de service est d'installer des IDS (Intrusion Détection Systèmes) et ou IPS (Intrusion Protection Systèmes). Les premiers systèmes de détection d'intrusion ont été développé par la sécurité américaine puis par les entreprises possédant des données sensibles. Maintenant, il existe plusieurs logiciels IDS, que ce soit des solutions open source comme Snort, ou des produits proposés par des entreprises spécialisées en sécurité comme Cisco, Symantec ...

Les IDS Un IDS est un ensemble de logiciel et/ou de matériel, qui a pour rôle de surveiller tous les paquets qui transitent sur un système, dans le but de détecter toutes tentatives d'intrusions et qui peuvent déclencher différentes alertes en fonction du trafic et de sa configuration. C'est un système qui doit fonctionner en temps réel, et qui requiert beaucoup de ressources, aussi bien en CPU pour traiter chaque paquet, qu'en bande passante. C'est la raison pour laquelle il est preferable de l'installer sur un système dédié.

Il y a deux grandes famille d'IDS :

Les NIDS Un NIDS (Network IDS) est un système qui va écouter en temps réel, et de manière passive, tous les flux transitant sur un réseau afin de détecter les intrusions. Un NIDS capture donc tout le trafic réseau, l'analyse, et génère des alertes lorsque des paquets suspects sont détectés. Un NIDS requiert donc une bande passante capable de supporter tout le trafic du réseau, et un équipement assez puissant pour analyser tout ce trafic en temps réel.

1ere étapes : la capture Pour la capture des paquets, la plupart des IDS utilisent la librairie libpcap qui existe sur toutes les plate-formes, ce qui permet aux IDS d'être compatible sur toutes les plates-formes Son fonctionnement est de copier tous les paquets arrivant sur la couche liaison de données, puis de leur appliquer un filtre (BPF, Berkley Packet Filter) permettant de récupérer les informations nécessaires à l'analyse de celui ci. Le trafic capturé par l'IDS n'est donc pas forcement le même qui arrive sur le système d'exploitation puisque l'IDS agit sur un niveau inférieur de celui du pare-feu.

2eme étapes : Analyse Comme nous l'avons vu précédemment, il existe différents types d'attaques, opérant à différents niveaux (applicatifs, réseaux ..), il est donc nécessaire de disposer de différents techniques de détections :
-Analyse par scénario :

Tous comme les antivirus, qui utilisent des base de signature de virus pour effectuer leurs détections ; les IDS utilisent des bases de signatures d'attaque pour detecter les intrusions. Il

est aussi possible de personnaliser cette base de signature, en rajoutant nos propres règles. L'inconvénient de l'utilisation de signatures pour la détection des attaques est qu'il est nécessaire de connaître toutes les différentes attaques possibles. Or ceci pose problème pour les attaques nouvellement decouvertes .Il est donc important de mettre a jour ses bases de signature très régulièrement, mais souvent pas suffisant. L'analyse par scénario peut aussi verifier la conformité des flux par rapport à leur utilisation normal décrite dans les RFC (Request For Comment). Par exemple, dans le cas d'un déni de service de type Ping of death, l'IDS remarque que l'on reçoit un paquet ICMP n'ayant pas une taille conforme à la RFC et peut donc émettre une alerte.
Il existe aussi l'analyse heuristique, qui permet de générer une alarme quand le nombre de sessions à destination d'un port donné dépasse un seuil dans un intervalle de temps prédéfini. c'est la methode que l'on va utiliser pour notre script de detection de deni de service.

-Analyse par comportement :

Il existe aussi d'autre méthodes de détections telles que l'analyse comportementale, qui consiste à détecter les intrusions en fonction des habitudes de l'utilisateurs. Les habitudes des utilisateurs peuvent être mesurer a l'aide de différentes données comme la charge CPU, l'utilisation mémoire... Mais cette technique est très contraignante car il faut enregistrer toutes les habitudes des utilisateurs. De plus, elle n'est pas très efficace car elle génère un grand nombre de faux positifs des que les utilisateurs modifient leurs habitudes d'utilisation. Cependant, si un pirate attaque pendant la phase d'apprentissage, son attaque ne sera alors jamais détecté car elle sera considéré comme normal.

3eme étapes : Alertes Généralement, les alertes sont stockées dans le gestionnaire de journalisation du système, tels que Syslog ou Metalog. Mais il est aussi possible de formater les alertes sous la norme IDMEF (Intrusion Détection Message Exchange Format) afin de pouvoir les faire interoperer avec d'autres logiciels de sécurité. Les alertes de sécurité peuvent être remonté par email sur la plupart des IDS.

Les HIDS Contrairement à un NIDS, un HIDS (Host IDS) est dédié à une machine en particulier, il analyse seulement le trafic entrant et sortant de cette machine, vérifier ses fichiers de logs.. Il demande donc beaucoup moins de bande passante, et de CPU qu'un NIDS. Un inconvénient des HIDS est qu'il soit installé sur un système sain, puisque le HIDS utilise l'état du système au moment ou il est installé pour détecter les activités suspectes. Un autre inconvénient : un grand nombre de postes a installer nécessite l'installation du HIDS sur chacun de ces postes. L'avantage des HIDS est qu'il y a détecte très peu de faux positifs.

Les IPS Les IPS (Intrusion Prevention System) sont, à la différences des IDS, un ensemble de matériel et de logiciel ayant pour but d'empêcher les intrusions ou autres activités suspectes détectés. Les IPS sont donc des outils actifs permettant de stopper toutes activités suspectes, contrairement aux IDS qui ne font que les détecter.

Les IPS agissent a plusieurs niveaux :

- Niveau applicatif : L'IPS surveille chaque processus d'un système et les arrête des qu'il se comporte anormalement.

- Niveau Transport / Session : Si une session suspecte est détecté, il peut la clore avec un TCP Reset (Flag RST).

- Niveau Réseau : Il peut bloquer le trafic s'il est utilisé en tant que routeur, ou peut interagir avec les autres équipements réseaux.

Ce système est très efficace mais il possède plusieurs inconvénients :

- Puisqu'il s'occupe directement de bloquer ce qui lui semble suspect sans intervention de l'être humain, il arrive souvent que les IPS bloquent du trafic légitime (faux positif). Par exemple, lorsque le réseau est exceptionnellement très fortement utilisé, l'IPS peut, en fonction de sa configuration, considérer ce trafic comme un déni de service et donc bloquer toutes ces connexions légitimes.

- Un autre inconvénient non négligeable des IPS est qu'ils peuvent être utilisé par les attaquants pour réaliser un déni de service. Par exemple, si quelqu'un attaque le réseau par déni de service tout en ayant pris soin de modifier son adresse IP par celle d'un équipement indispensable au fonctionnement du réseau, l'IPS détectera l'attaque et bloquera l'attaquant, et par conséquent l'équipement réseau en question. Il existe maintenant des techniques pour contrer ces problèmes telles que la mise en place de "white list" qui permettent de définir les adresses des équipements qui ne devront jamais être banni.

- De plus les IPS sont facilement repérables par un attaquant. Une attaque lancée est directement détecte et bloquée. Une fois l'IPS repéré, l'attaquant essaye de trouver une faille de l'IPS afin de la contourner.

  C'est pour toutes ces raisons, que les IDS sont beaucoup plus utilisés que les IPS, bien que certains IDS sont maintenant dotés de fonction permettant de réagir et donc de bloquer

certaines attaques.

2.1.3 Les firewalls

Les firewalls sont des équipements réseaux qui permettent de filtrer les paquets entrants et sortants afin de prévenir toutes attaques de l'extérieur. Ils se basent sur un fonctionnement séquentiel et un ensemble de règles pour autoriser seulement les connexions légitimes. Dans le cadre des DoS, le problème majeur est que les attaquant utilisent des connexions légitimes pour perpétrer leurs attaques. De plus, les firewalls ne peuvent pas efficacement différencier les connexions légitimes et illégitimes. Par contre ils peuvent se révéler très efficace pour contrer un attaquant. En se basant sur les informations fournits par des équipements de détections, on peut appliquer des règles très précises qui bloqueront uniquement les connexions malfaisantes, en se basant sur le protocole, l'IP ou le port.

De nombreux firewalls hardware ou software permettent de se prémunir contre les attaquants. Parmi eux, un des plus courant est le firewall intégré au noyau Linux : Netfilter et son interface iptables. Il présente l'avantage d'être open source donc gratuit et d'être assez facile à appréhender. De plus, cela n'a aucune influence sur sa puissance et sa modularité.

Quelques exemple de règles simple pour bloquer certaines attaques :

- iptables -I INPUT 1 -p tcp -s 192.168.0.1 -j DROP : bloquer les connexions TCP provenant de l'attaquant 192.168.0.1
  Pour se prémunir d'un SYN flood.

- iptables -I INPUT 1 -p icmp -s 192.168.0.1 -J DROP : bloquer les PING provenant de l'attaquant 192.168.0.1
  Pour se prémunir des PING flood.

Bien maîtriser un firewall peut être une très bonne protection contre la majorité des attaques et des attaquants. Il est nécessaire de surveiller les connexions qui transitent sur son réseau pour être capable de bien se protéger contre toutes menaces.

2.2 Comment améliorer la détection et la prévention

2.2.1 Une combinaison de protections

La détection et la prévention des attaques DoS est une science en permanente évolution qui vise toujours à réduire l'écart qui sépare l'avance des pirates et les contre-mesure existantes. Les principales solutions pour améliorer les chances de détections et de préventions sont de se tenir au courant des dernières avancées dans la matière et de mettre en place des systèmes sécurises comportant des sondes de détections, des serveurs configurer de manière sécurisée , coupler à des bon firewall.

2.2.2 Pour Voir plus loin

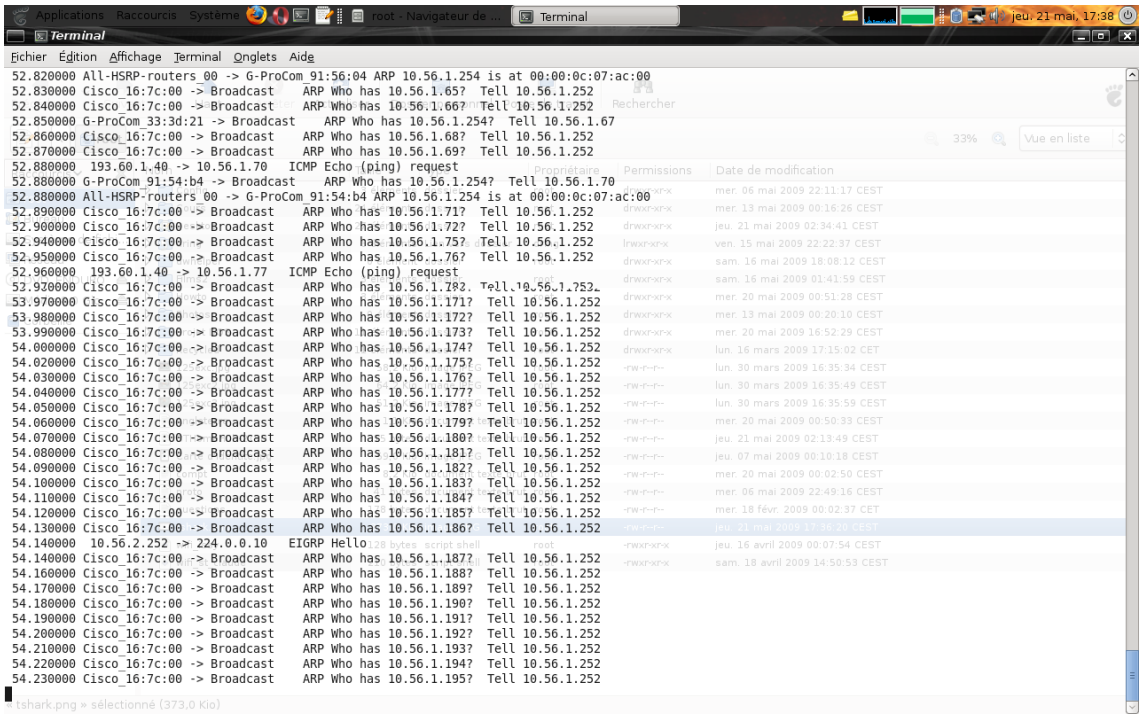
Des personnes sont aussi allé plus loin dans la lutte contre de telles attaques. Aujourd'hui, il existe des programme RID, gag, Zombie Zapper... qui permettent la recherche d'hôtes Zombies sur les réseaux.On rapelle que les hôtes zombies sont des machines corrompues par des attaquants et sur lesquelles tourne un programme permettant aux pirates de relayer des attaques DoS. Il en existe un nombre incalculable sur Internet car leurs propriétaires ne se rendent même pas compte qu'ils sont infectes et qu'ils peuvent être à la source d'attaques distribuées. Les programmes de détection de machines zombies luttent de la meilleure façon possible pour détecter et essayer de supprimer ces machines zombies mais leur nombre est tellement important que la tache est presque vaine.

3 Un script pour détecter et contrer les attaques DoS

Pour illustrer les détections d'attaques, nous avons développé un script bash tournant sous Linux permettant de détecter et de contrer quelques attaques connues.

3.1 Base sur tshark

Nous avons décider de développer le script en se basant sur la sortie du programme tshark. Tshark est un programme de la suite wireshark qui est très similaire a tcpdump mais dont la sortie est plus plus facilement interprétable par un script. Le script s'appuie directement sur la sortie de tshark et la parse de façon à trouver des irrégularités.
Ci dessous un exemple d'anomalies ARP détectées sur un réseau.



L' output générer par tshark est assez simple à analyser car il se base sur un schéma en colonnes assez pratique à parser. Chaque information telle que l'adresse source, l'adresse destination le protocole peuvent être extraites rapidement et facilement.

3.2 Mode opératoire

Une fois la sortie de tshark redirige dans le script, toutes les information sont parsées ligne par ligne avec l'aide d'un buffer pour détecter des éventuelles attaques. Il permet de filtrer tout

d'abord les types de paquets : TCP, ICMP...
Suivant ces types, il effectue différentes actions. Ceci permet entre autre de pouvoir détecter plusieurs types d'attaques se déroulant en simultanées.

Contrer l'attaque SYN flood Pour le SYN flood, on analyse les paquets TCP en les comparant pour déterminer si la même IP essaye d'envoyer plusieurs paquets SYN. Si 3 de ces paquets sont reçus de la même adresse IP, dans la même seconde alors une alerte est déclenchée. Puis, une règle de firewall est crée pour contrer l'attaquant. Dans la vie courante, il est plutôt rare que trois paquets SYN en provenance de la même source soit reçu dans la même seconde, ce qui évite de bloquer un utilisateur effectuant des opérations légitimes comme des requêtes HTTP pour consulter un site web.
Les actions réalisés dans la boucle de lecture des paquets sont les suivantes :

```
#Récupération du type de paquet
type=‘echo $paquet | cut -f 5 -d " "‘;
case $type in
#Le paquet est de type TCP
TCP)
tmp=‘echo $paquet | cut -f 2 -d [‘;
#On test pour détecter si il s’agit d’un paquet avec le flag SYN
if [ ${tmp:0:1} = "S" ]; then
ip=‘echo $paquet | cut -f 2 -d " "‘;
ip2=‘echo $paquet_tcp_precedent | cut -f 2 -d " "‘;
#On compare l’IP source avec l’IP du paquet dans le buffer
if [ $ip = $ip2 ]; then
ts=‘echo $paquet | cut -f 1 -d .‘;
ts2=‘echo $paquet_tcp_precedent | cut -f 1 -d .‘;
#On confirme que les paquets on été reçu dans la même seconde
if [ $ts = $ts2 ]; then
nombre_tcp_syn=$[$nombre_tcp_syn+1];
#Si le nombre de paquets SYN depasse 3 par seconde on déclenche l’alerte et on lance la règle de
if [ $nombre_tcp_syn -gt 3 ]; then
echo "Tentative de SYN FLOOD!!!!!!";
‘iptables -I INPUT 1 -p tcp -s $ip -j DROP‘
nombre_tcp_syn=0;
paquet_tcp_precedent="fff f ";
fi
```

```
fi
fi
paquet_tcp_precedent=$paquet;
fi
;;
```

Contrer l'attaque PING flood Les attaques par PING flood sont contrées de la même manière. Le script repose sur l'analyse séquentielle des requête ICMP pour détecter des comportement anormaux. On analyse seulement les paquets contenant des 'echo request' puis on les comparent pour savoir si l'IP source est la même. De la même manière que pour le SYN flood, lorsque le nombre de paquets à la seconde dépasse une certaine valeur (ici 3), on lance une règle de firewall interdisant l'accès de la machine à l'attaquant.

```
#Le paquet est de type TCP
ICMP)
tmp=‘echo $paquet | cut -f 8 -d " "‘;
if [ $tmp = "request" ]; then
ip=‘echo $paquet | cut -f 2 -d " "‘;
ip2=‘echo $paquet_icmp_precedent | cut -f 2 -d " "‘;
#On compare l'IP source avec l'IP du paquet dans le buffer
if [ $ip = $ip2 ]; then
ts=‘echo $paquet | cut -f 1 -d .‘;
ts2=‘echo $paquet_icmp_precedent | cut -f 1 -d .‘;
#On confirme que les paquets on ete recu dans la meme seconde
if [ $ts = $ts2 ]; then
nombre_icmp=$[$nombre_icmp+1];
#Si le nombre de paquets PING depasse 3 par seconde on declanche l'alerte et on lance la regle
if [ $nombre_icmp -gt 3 ]; then
echo "Tentative de PING FLOOD!!!!!!";
‘iptables -I INPUT 1 -p icmp -s $ip -j DROP‘
nombre_icmp=0;
paquet_icmp_precedent="fff f "
fi
fi
fi
```

```
paquet_icmp_precedent=$paquet;
fi
;;
```

Dans l'état actuel, le script permet de détecter des attaques simultanées mais il est axée sur les attaques par surcharge. Dans le cas des attaques par failles, elle sont de moins en moins courantes et la plupart des systèmes sont maintenant patcher pour éviter d'être pénalisés.

Conclusion

Les attaques par déni de service existent depuis longtemps et se sont développées au fur et à mesure de l'évolution des systèmes informatiques. Etant simples d'accès, elles sont très utilisées dans de nombreuses situations,et deviennent même parfois politique. Ces attaques sont très modulables et bien que la détection fait d'énormes progrès, elles restent toujours très compliques à mettre en place de manière efficace. Il ne suffit pas de multiplier les outils de préventions et d'enrichir ses connaissances. Il faut surtout être réactif et se préparer à toutes les éventualités. Il faut aussi voir l'aspect financier de ces attaques et adapter le budget de protections aux risques encourus. Mais le risque zéro ne sera jamais atteint et plus les technologies évolues, plus les pirates auront accès à des ressources importantes. Les attaques seront alors très compliquées, voire impossible à contrer avec les méthodes actuelles. La course contre les pirates ne s'arrêtera jamais.

Annexe

```
#!/bin/bash
nombre_tcp_syn=0;
nombre_icmp=0;
nombre_arp=0;
paquet_tcp_precedent="fdfd f ";
paquet_icmp_precedent="fdfd f ";
paquet_arp_precedent="fdfd f ";
while read paquet;
do
type=‘echo $paquet | cut -f 5 -d " "‘;
case $type in
TCP)
tmp=‘echo $paquet | cut -f 2 -d [‘;
if [ ${tmp:0:1} = "S" ]; then
ip=‘echo $paquet | cut -f 2 -d " "‘;
ip2=‘echo $paquet_tcp_precedent | cut -f 2 -d " "‘;
if [ $ip = $ip2 ]; then
ts=‘echo $paquet | cut -f 1 -d .‘;
ts2=‘echo $paquet_tcp_precedent | cut -f 1 -d .‘;
if [ $ts = $ts2 ]; then
nombre_tcp_syn=$[$nombre_tcp_syn+1];
if [ $nombre_tcp_syn -gt 3 ]; then
echo "Tentative de SYN FLOOD!!!!!!";
‘iptables -I INPUT 1 -s $ip -j DROP‘
nombre_tcp_syn=0;
paquet_tcp_precedent="fff f "
fi
fi
fi
paquet_tcp_precedent=$paquet;
fi
;;
ICMP)
tmp=‘echo $paquet | cut -f 8 -d " "‘;
if [ $tmp = "request" ]; then
```

```
ip=‘echo $paquet | cut -f 2 -d " "‘;
ip2=‘echo $paquet_icmp_precedent | cut -f 2 -d " "‘;
if [ $ip = $ip2 ]; then
ts=‘echo $paquet | cut -f 1 -d .‘;
ts2=‘echo $paquet_icmp_precedent | cut -f 1 -d .‘;
if [ $ts = $ts2 ]; then
nombre_icmp=$[$nombre_icmp+1];
if [ $nombre_icmp -gt 3 ]; then
echo "Tentative de PING FLOOD!!!!!!";
‘iptables -I INPUT 1 -s $ip -j DROP‘
nombre_icmp=0;
paquet_icmp_precedent="fff f "
fi
fi
fi
paquet_icmp_precedent=$paquet;
fi
;;
*)
echo Autre traffic
;;
esac
done <&0
```