L'attaque par déni de service

Travail réalisé par NITARD Hugo,

De la section de technicien supérieur en services informatiques aux organisations

De septembre à décembre 2016

Sommaire

1) Introduction à la veille

Dans cette veille technologique, je vais vous présenter différentes parties, concernant le déni de service.

Premièrement, je définirai avec vous ce qu'est une attaque par déni de service, suivi de différentes techniques utilisées jusqu'aujourd'hui, des plus dépassées aux plus modernes, et en dernière partie, je vous montrerai différents moyens afin de se protéger contre les attaques par déni de service.

Nous terminerons ensuite par une conclusion sur le sujet, contenant mon avis personnel sur la veille, ainsi qu'un petit bilan sur l'ensemble de la veille et de son contenu.

Faire une veille technologique sur ce sujet me paraît important parce que j'ai dû, premièrement m'informer du mieux que je pouvais sur les dénis de services. Cela m'a donc permis d'avoir une approche plus professionnelle sur le sujet d'Internet, le fonctionnement du réseau, d'un serveur, et tout ce qui peut toucher à la partie réseau.

Cette veille m'a donc été très utile pour mon projet professionnel, car je souhaite devenir, à la date du 12 décembre 2016, Développeur Web, ou au moins équivalent dans le domaine du Web.

2) Qu'est-ce qu'une attaque par déni de service ?

Une attaque par déni de service (*DoS attack* en anglais pour *denial-of-service attack*) est une attaque se déroulant sur Internet ; l'attaquant essayant de faire tomber une infrastructure connectée, et à la rendre momentanément indisponible à tous. Il faut savoir que cet acte est passible dune peine de cinq ans d'emprisonnement (entrave au fonctionnement d'un système de traitement automatisé) et d'une amende pouvant aller jusque 150 000€.

Une attaque par déni de service permet de saturer la bande passante de la machine disposant de l'IP attaquée, ce qui la rend soit inaccessible, soit difficile d'accès.

Le DoS a rapidement donné naissance au DDoS (*Distributed denial-of-service*) impliquant alors un système de maîtres-zombies. Le hackeur s'introduit alors dans plusieurs ordinateurs et y laissent un petit programme qui sommeille. Lorsque le hackeur lance le top a un maître (qui est aussi un ordinateur piraté), le maître contacte alors les zombies en réveillant le programme, et les adresses IP des zombies sont alors utilisées afin d'attaquer le service voulu. Le hackeur est du coup beaucoup plus dur à tracer car ce n'est pas lui qui donne l'ordre aux zombies directement.

La RFC 4732 (*Request For Comments*, littéralement Demande De Commentaires, c'est-à-dire une série de documents numérotés, officiels, concernant Internet) clarifie le fond et la forme des attaques par déni de service.

Du fait de sa nature, le DDoS est beaucoup plus violent et puissant que le DoS.

3) Différentes techniques de déni de service

Les premières attaques DoS eurent lieu dans les années 1980.

3.1 Paquets ICMP

Les plus courantes utilisaient les failles présentes à l'époque, notamment le fait que les paquet ICMP (un protocole fondamental d'Internet, littéralement *Internet Control Message Protocol*, est utilisé pour transporter des messages d'erreur) soient limités à 65 535 octets. De ce fait, envoyer un message d'au moins 65 536 octets se poursuivait par des erreurs UDP (*User Datagram Protocol*, aussi un protocole principal d'Internet, permettant la transmission de données entre deux adresses IP) car les piles IP (Un ensemble de protocoles que l'on peut appelé modèle internet, ou TCP/IP) ne pouvaient pas les gérer de manière propre.

3.2 Attaque SYN Flood

Quand un client essaie de se connecter à un serveur, il lui envoie une demande (le message SYN pour *synchronize*), s'en suit de l'autorisation du serveur en renvoyant un message au client (le message SYN-ACK pour *synchronize-aknowledgment*) et le dernier message qui part du client vers le serveur (un message acknowledgment). Suite à ces 3 messages, la connexion est alors établie entre le client et le serveur.

Le but de l'attaque SYN Flood est d'envoyer des requêtes à un serveur, mais de ne pas répondre son message SYN-ACK, ce qui réservait et mettait en file d'attente les autres requêtes, ce qui devenait vite ingérable. Les premières période durant lesquelles le serveur attendait une réponse ACK étaient de 75 secondes. Cela coûtait très cher, car le processeur du serveur travaillait pendant ce temps là, et cela prenait beaucoup de mémoire.

Ce type d'attaque est très simple grâce au spoofing (ou usurpation) d'adresses IP. A chaque message envoyé, l'adresse IP de provenance n'était pas la même.

3.3 UDP Flooding

L'UDP Flooding se repose sur le trafic paquets UDP, qui est prioritaire à celui des paquets TCP. Au lieu d'attaquer une adresse IP, l'UDP Flooding se repose sur la congestion du réseau, c'est-à-dire l'augmentation de trafic au sein d'un réseau. Cette attaque provoque donc la saturation d'une connexion entre deux machines. Du fait de la priorité du trafic UDP, TCP a de moins en moins de bande passante, ce qui peut donc aller jusqu'à l'arrêt total d'un réseau.

3.4 Smurfing

Le smurfing utilise le protocole ICMP, vu précédemment, ainsi que l'adresse de broadcast du réseau (on utilise ici des ping ICMP ECHO). Cela démultiplie les messages vers tous les hôtes (comme on envoie les ping à l'adresse de broadcast). Pour reprendre en d'autres termes, le fait d'envoyer un flux continu de ping à l'adresse de broadcast.

3.5 Attaque par fragmentation

L'attaque par fragmentation (ou *teardrop* / *fragment* attack) repose sur le principe de la fragmentation du protocole IP, c'est-à-dire lorsqu'un paquet IP est trop long, il est fragmenté en plusieurs paquets IP, chacun étant identifié de manière séquentielle, et à l'intérieur de cette séquence, une identification commune (afin de savoir que ces paquets divisés font à la base parti du même paquet IP). A la réception de ses paquets, ils sont rassemblés originalement grâce aux valeurs de décalage appelées *offset*.

La plus connue étant l'attaque *teardrop*. Cette attaque constituait à introduire, dans les paquets fragmentés, des informations concernant l'*offset*. Bien entendu, les informations introduites étaient des décalages erronés. Cela provoquait, lors de l'assemblage, des vides, appelés recoupements (ou *overlapping*), ce qui peut provoquer des instabilités systèmes.

Les systèmes actuels ne sont plus vulnérables à ce type d'attaques.

3.6 Attaque par déni de service d'une ligne téléphonique

L'attaque par déni de service d'une ligne téléphonique (ou *TDoS* pour

Telephony Denial-of-Service) consiste à saturer une ligne téléphonique d'appels, suivis de redirections sur des lignes non-désirées. On parle de *DoS* car le *TDoS* utilise la technologie du *VoIP* (*Voice over IP* pour Voix sur IP est une technique utilisant les paquets IP afin de transmettre la voix à travers des flux audio ou vidéo). La technologie VoIP est très proche d'une autre, la *ToIP* (*Telephony over IP* pour Téléphonie sur l'IP. Cette technologie est utilisée par les standardistes, afin de démarcher par téléphone, et de joindre des lignes téléphoniques.

Ce type d'attaque permet, à l'image du DOS, de rendre hors-ligne la ligne téléphonique de la cible.

3.7 Déni de service involontaire

Le déni de service involontaire n'est pas issu de la volonté de quelqu'un, mais simplement d'un pic de trafic que le serveur n'arrive pas à gérer. Ce phénomène est très présent dans le cas où un site très populaire envoie le lien d'un site un peu plus « rural ». Ce site, n'a pas l'habitude de recevoir autant de requêtes, par conséquent, le site chute, et devient indisponible jusqu'au redémarrage du serveur.

4) Comment se protéger contre les attaques DOS/DDOS ?

Comme les attaques devenaient de plus en plus diverses et variées, différents moyens ont été mis au point afin de contrer les attaques par déni de service le plus rapidement possible.

- La première solution est d'adopter pour un pare-feu, cela bloquera les attaques les plus simples. On utilisera alors une règle dans ce pare-feu, qui va bloquer le trafic entrant, (si l'on a pas l'adresse IP de l'attaquant), ou simplement, mettre en liste noire l'adresse de l'attaquant, ce qui l'empêchera de nuire.

- Certains routeurs incluent une liste de contrôle d'accès. Cette dernière attribue des droits, en fonction des utilisateurs. Donc si l'attaquant ne figure pas dans cette liste, son attaque sera simplement inefficace, car le routeur (ou switch), va rediriger l'attaque vers ce qu'on appelle une « null route ». C'est-à-dire une route entrée dans la table de routage qui ne va nulle part. Les paquets sont donc ignorés. On peut aussi appeler ceci un filtrage trou noir.

- Une autre technique, appelée « upstream filtering » (ou filtrage en amont) s'assure de la provenance des paquets IP avant de les transmettre au serveur se situant juste après ce point de passage. Un proxy est généralement muni de ce service. Plusieurs fournisseurs de filtrage existe, mais un ami m'a recommandé Arbor Networks, spécialisé dans la protection DDOS pour entreprise.

- La dernière solution, nommée Système de detection d'intrusion (ou IDS pour Intrusion Detection Sytem) est très efficace. Ce dernier utilise son propre matériel, et à la puissance nécessaire pour détecter et gérer seul des attaques DDOS. Il analyse le réseau entrant, à la recherche de modèles connu de DDOS, de manière continue et bloque le flux s'il le trouve suspect.

5) Conclusion

Avant de conclure, j'aimerais donner mon avis sur cette veille.

Je l'ai trouvée très intéressante, autant d'un point de vue informatif, car j'ai vraiment appris beaucoup de choses en la faisant, mais aussi d'un point de vue méthode, car ce n'est pas quelque chose que j'avais fait auparavant. C'était donc une nouvelle expérience positive pour moi, même si je pense avoir fait une description de tout, avec une petite touche un peu plus poussée par moments.

Au sein de cette veille, nous avons d'abord expliqué ce qu'était une attaque par déni de service. Cette définition est générale, et s'applique à toutes, malgré certaines vraiment spécialisées et poussées.

Suivant cette définition, nous avons vu les différentes attaques les plus réputées, allant de la plus ancienne aux plus récentes (notamment l'attaque par déni de service d'une ligne téléphonique, ceci-dit, elle est de moins en moins fréquente avec l'omniprésence d'Internet, qui commence à pénétrer tous les marchés, ainsi que tous les domaines, rendant le téléphone et le courrier obsolètes).

Et avant de terminer cette veille, nous avons vu différents moyens de se protéger contre les attaques DOS et DDOS. Différents moyens ont été mis au point, mais certains restent au-dessus. Mais une bonne protection contre le DOS et DDOS coûte très cher, mais assurera une continuité dans les services proposés par l'entreprise ou l'association.

Cette veille n'est qu'une ébauche de ce que pourrait être mon travail en 2 ans. J'ai eu 8 fois moins de temps afin de produire ceci, soit 3 mois. Certaines recherches m'ont demandées de remonter assez loin, notamment au niveau des RFC.