REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
ECOLE NATIONALE SUPERIEURE D'INFORMATIQUE

CS 1 **Année 2019 / 2020**

Module : SEC

Les attaques par déni de service distribué (DDoS)

REALISE PAR :
AZIZ Rezak
BEN MESSAOUD Mohammed Issam Daoud

ENCADRE PAR :
Ens ANANE Mohamed

Section : B

Groupe N° : 08

Table des matières

I. Introduction générale :

Avec le développement de l'utilisation de l'internet, les entreprises et les particuliers optent souvent à développer leurs business sur internet. Cela, donc, les a menés à ouvrir leurs systèmes d'informations à leurs partenaires et leurs fournisseurs. Cette démarche a ces avantages en faisant que le business de l'entreprise s'accroît, mais elle a aussi des risques qui sont fatals dans certain cas, on parle de problèmes de sécurités.

Les données partagées à travers internet sont exposées à plusieurs menaces par des malfaiteurs qui exploite des vulnérabilités pour s'infiltrer dans les systèmes d'informations pour plusieurs objectifs : espionnage, vol, prise de système en otage, et ils peuvent arriver même à la destruction du système.

Pour exploiter les vulnérabilités d'un système et le détruire les pirates utilisent plusieurs techniques : en injectant un virus, en exploitant des vulnérabilités dans le système pour y avoir accès, on parle alors d'attaques. Dans notre cas on s'intéresse principalement à un seul type d'attaque : "Attaque par déni de service DDoS".

On va étudier principalement l'attaque et son principe, ses types, les outils utilisés pour la faire, comment prévenir cette attaque et que faire si on est face à cette attaque.

II. DDoS : Définitions et principe :

1. Définition DoS :

On ne peut pas parler de DDoS (attaque par déni de service distribué) sans parler de l'attaque DoS.

"Le "Denial-of-service" ou déni de service est une attaque très évoluée visant à rendre muette une machine en la submergeant de trafic inutile." (D'après le site securiteinfo)

Pour mieux expliquer, d'après Cybersecurity and Infrastructure Security Agency (CISA), Une attaque par déni de service (DoS) se produit lorsque des utilisateurs légitimes ne peuvent pas accéder aux systèmes d'information, aux appareils ou à d'autres ressources réseau en raison des actions d'un acteur malveillant. Les services concernés peuvent inclure le courrier électronique, les sites Web, les comptes en ligne (par exemple, les services bancaires) ou d'autres services qui dépendent de l'ordinateur ou du réseau affecté.

2. Définition de DDoS :

Le but de DDoS est le même que le DoS, c'est à dire il vise à rendre muette une machine en la submergeant de trafic inutile. Donc on se pose la question suivante : Quel est la différence entre DDoS et DoS ?

On peut dire que DDoS est un type d'attaque DoS. Une attaque par déni de service distribué (DDoS) se produit lorsque plusieurs machines (Zombies) fonctionnent ensemble pour attaquer une cible, d'où le terme distribué.

Par exemple, Au début du mois septembre 2019, Wikipedia a subi une attaque qui a touché ses infrastructures européennes. Les versions espagnoles, françaises, polonaises, croates, autrichiennes, allemandes, britanniques et russes n'étaient plus totalement accessibles. En parallèle, Blizzard, l'éditeur du jeux vidéo World of Warcraft a signalé un DDoS ciblant la version Classic du MMORPG. Là encore, les utilisateurs ne pouvaient se connecter pendant plusieurs heures. Ici, les structures visées n'ont pas une importance vitale. Cependant, cela entraîne de fortes pertes économiques. Dans certains cas, les cibles sont des hôpitaux ou des administrations qui gèrent des données sensibles ou opèrent des services critiques.

3. Principe :

Le principe d'une attaque par déni de service est simple, il s'agit d'inonder l'hôte ou le réseau ciblé de trafic jusqu'à ce que ce dernier ne puisse pas répondre ou se bloque.

On peut illustrer ça comme un embouteillage sur l'autoroute, empêchant le trafic régulier d'arriver à sa destination souhaitée.

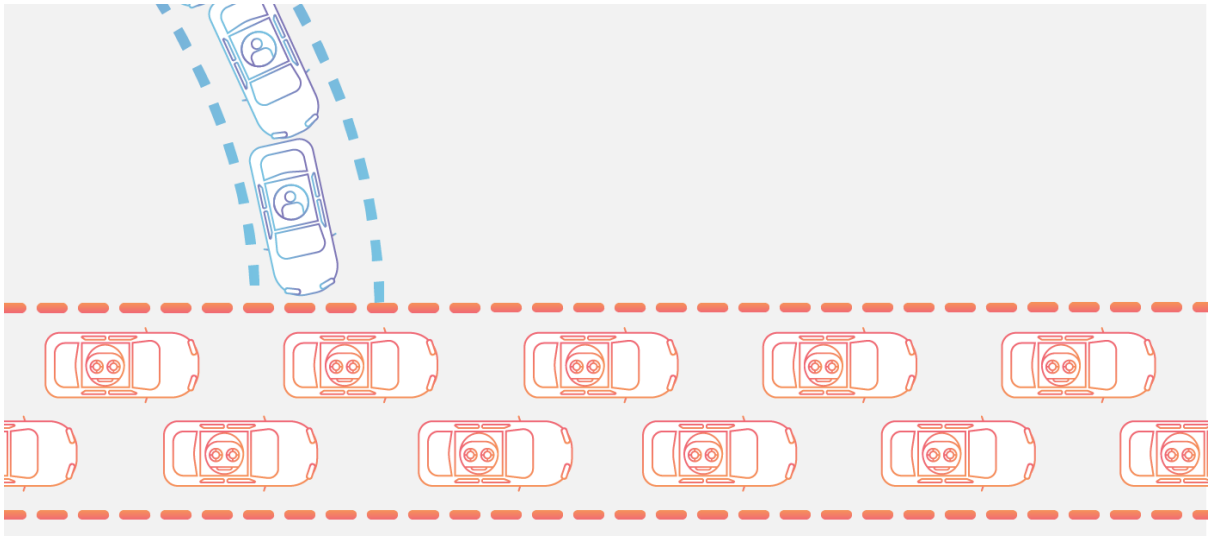


Figure 1: Source https://www.cloudflare.com/fr-fr/learning/ddos/what-is-a-ddos-attack/

Les DDoS se sont démocratisées depuis 2-3 ans. En effet dans les premiers temps, cette attaque restait assez compliquée et nécessite de bonnes connaissances de la part des attaquants ; mais ceux-ci ont alors développé des outils pour organiser et mettre en place l'attaque. Ainsi le processus de recherche des hôtes secondaires (ou zombies) a été automatisé. On cherche en général des failles courantes (buffer overflows sur wu-ftpd, les RPCs...) sur un grand nombre de machines sur Internet et l'attaquant finit par se rendre maître (accès administrateur) de centaines voire de milliers de machines non protégées. Il installe ensuite les clients pour l'attaque secondaire et essaye également d'effacer ses traces (corruption des fichiers logs, installation de rootkits). Une fois le réseau en place, il n'y a plus qu'à donner l'ordre pour inonder la victime finale de paquets inutiles.

Il est intéressant de noter que les victimes dans ce type d'attaques ne sont pas que celles qui subissent le déni de service ; tous les hôtes secondaires sont également des machines compromises jusqu'au plus haut niveau (accès root), tout comme l'hôte maître.

La menace provient du fait que les outils automatisant le processus ont été très largement diffusés sur Internet. Il n'y a plus besoin d'avoir des connaissances pointues pour la mettre en place, il suffit de "cliquer" sur le bouton.

Ce principe est illustré dans la figures ci-dessous,

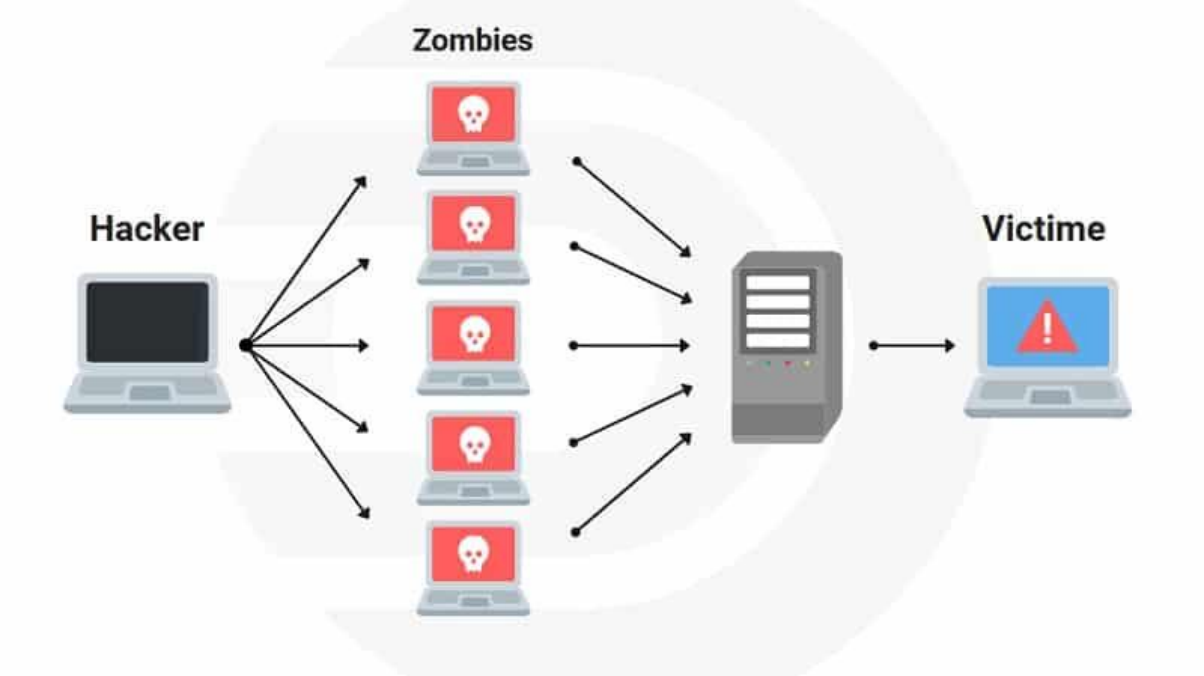


Figure 2 Source:https://www.opportunites-digitales.com/protection-anti-ddos

4. Qui peut être visé :

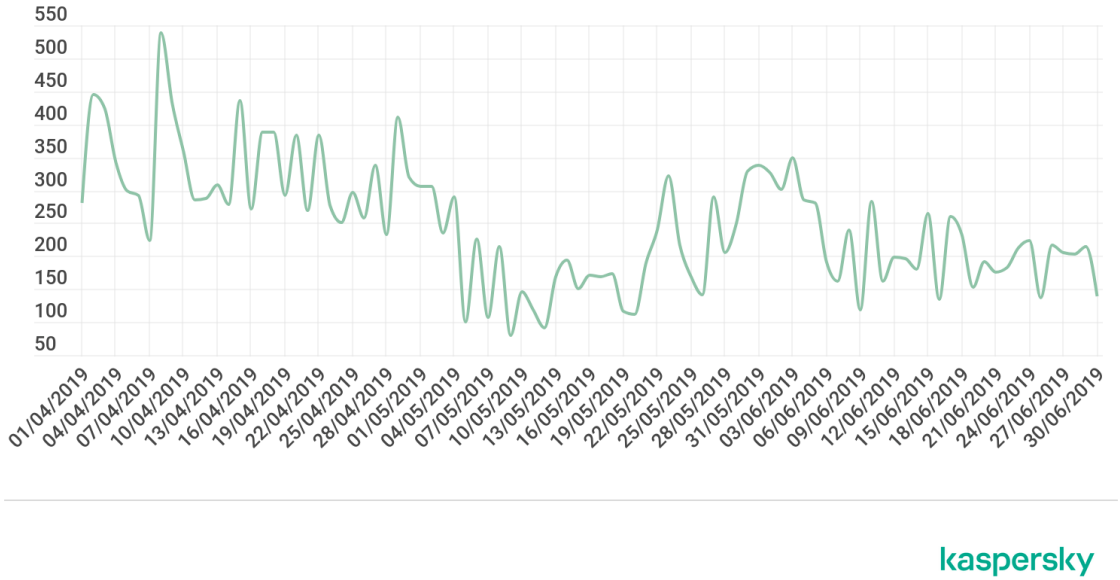
Toute entité dont l'activité dépend d'une infrastructure réseau connecté à internet peut être la cible d'une attaque DDoS. Les objectifs de attaquants sont divers (revendication idéologique, vengeance, et même pour s'amuser). Par ailleurs, certaines autres attaques sont menées afin de détourner l'attention pour couvrir d'autres actions illégales comme des transactions bancaires frauduleuses.

Plusieurs entités sont ciblées de cette attaque mais on peut dire que le e-commerce, les institutions financières, les gouvernements et les structures d'hébergement informatiques sont le plus visé par les DDoS.

Les attaques DDoS aujourd'hui sont très fréquentes. Pour parler des dernières années : 2018 semblait être synonyme de déclin des attaques DDoS. Pourtant, une nouvelle étude de Kaspersky Lab tend à montrer un retour en force de ces attaques par déni de service, qui ont considérablement augmenté pour ce premier trimestre 2019. En effet, la croissance est de 84% par rapport au quatrième trimestre 2018.

Comme le montre ce graphe fait par Kaspersky Lab pour l'année 2019, l'évolution est imprévisible ça peut diminuer comme ça peut augmenter tout dépend de nombres de cible non préparé

Source : Kaspersky Lab



Comme exemple d'attaque on peut citer l'attaque qui ciblait Cedexis, une société française spécialisée dans l'optimisation de la performance web. [Plusieurs centaines de clients de Cedexis ont été touchés, dont de nombreux sites français. Parmi les sites impactés, on relève des sites d'actualité (FranceTélévisions, L'Equipe, Le Figaro, Le Monde, 20 Minutes...), mais aussi des réseaux sociaux (LinkedIn, Slack...) ou encore des sites de grandes marques (Microsoft, Lenovo...). En une heure, l'équipe technique de la société est parvenue à rétablir le service. "C'est une performance compte-tenu de la violence de l'attaque que nous avons subie. Nous avons reçu en une heure l'équivalent de 75 fois le trafic que nous gérons en général en une journée", estime Julien Coulon, cofondateur et directeur général de Cedexis.

L'attaque provenait d'Asie. Au total, Cedexis aurait identifié 6,5 millions d'adresses IP inconnues mobilisées pour lancer le DDoS. "Sur nos 5 réseaux, trois ont pris cher. Nous estimons qu'environ 200 sites ont pu être touchés », précise Julien Coulon. Deux des trois réseaux touchés ont enregistré des taux de disponibilité de 80% (soit une requête sur cinq qui ne passait pas). "Quatre requêtes sur cinq étaient bloquées sur le troisième réseau touché. Or, c'est un réseau très utilisé pour les sites [de nos clients] français", explique Julien Coulon.

"Nous avions prévu une marge très importante, et plusieurs redondances réseaux. Mais dans le cas actuel, nous avons fait face à une attaque gigantesque, sans doute l'une des plus violentes jamais absorbée."]

[Extrait d’un article d’après journaldunet.com]

En parlant de la durée des attaques elles peuvent durée de quelques minutes à plusieurs jours, tout dépend de l’objectif de l’attaquant et la performance de l’équipe technique. Les attaques qui dure des jours visent principalement à extraire des données.

III. DDos : Types et outils :

1. Les types d'attaques DDoS les plus courants :

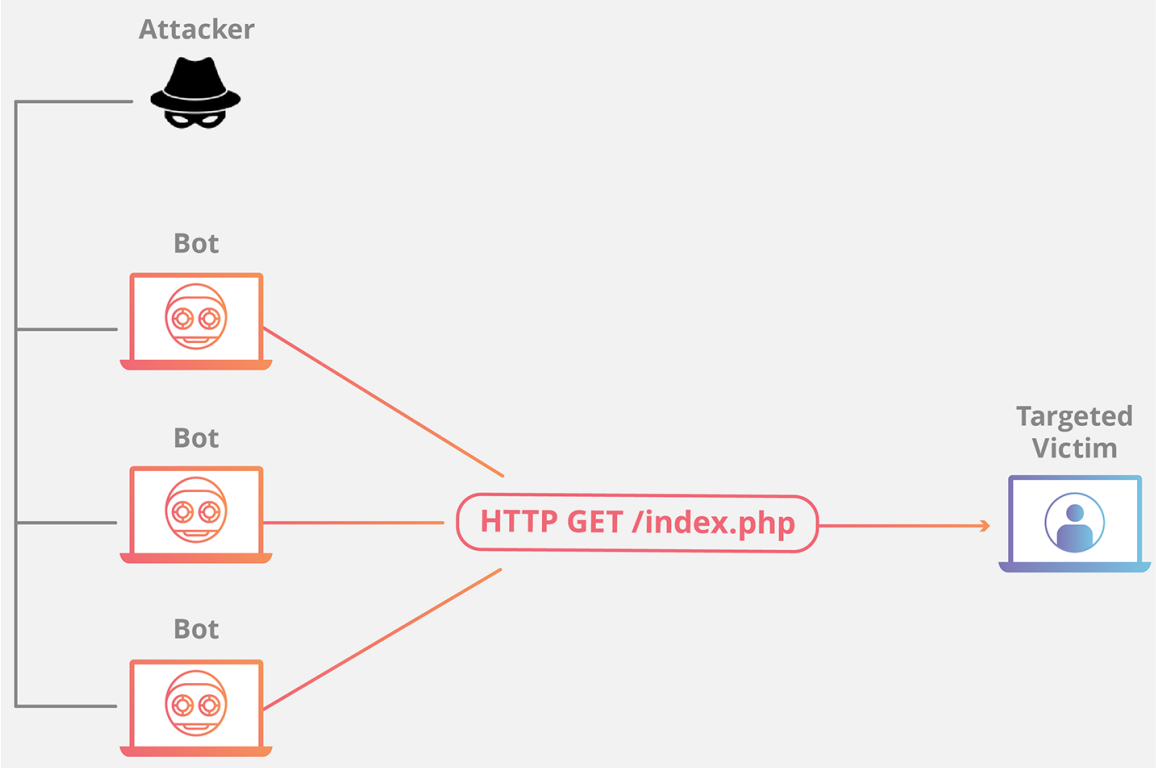
Différents vecteurs d'attaque DDoS ciblent des composants distincts d'une connexion réseau. Si la majorité des attaques DDoS impliquent de submerger de trafic une unité ou un réseau cible, ces attaques peuvent toutefois être divisées en trois catégories. Un pirate informatique peut utiliser un ou plusieurs vecteurs d'attaque différents, ou appliquer des vecteurs d'attaque selon un cycle potentiellement déterminé par les contre-mesures prises par la cible.

Les trois grandes familles d'attaques DDoS sont les suivantes :

- Attaques au niveau des applications (couche 7 du modèle OSI)
- Attaques au niveau des protocoles (couches 3 et 4 du modèle OSI)
- Attaques au niveau de la volumétrie (attaques par amplification)

A. Attaques sur la couche d'application

Parfois appelées attaques DDoS de la couche 7 (en référence à la 7e couche du modèle OSI), l'objectif de ces attaques est d'épuiser les ressources de la cible. Les attaques ciblent la couche où les pages Web sont générées sur le serveur et fournies en réponse aux requêtes HTTP (c'est-à-dire la couche d'application). Une seule requête HTTP est simple à faire côté client mais elle peut coûter cher au serveur car il doit souvent charger plusieurs fichiers et d'exécuter des requêtes des bases de données. Les attaques de la couche 7 sont difficiles à contrecarrer, car il peut être difficile d'identifier le trafic comme malveillant.



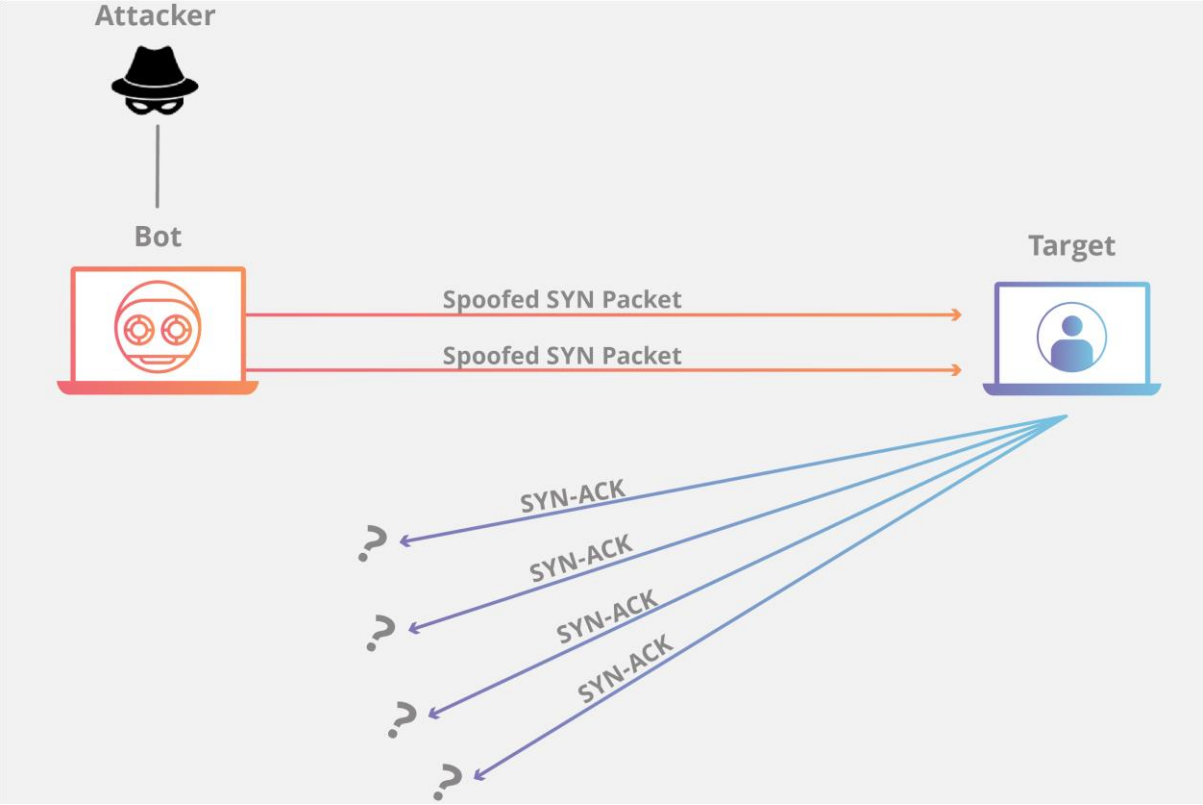
B. Attaques protocolaires

Les attaques protocolaires exploitent des faiblesses des couches 3 et 4 de la pile du modèle OSI pour rendre la cible inaccessible. Ces attaques, également connues sous la notion d'attaques par épuisement des tables d'état (state-exhaustion attacks), provoquent une interruption de service en consommant toute la capacité des tables d'état des serveurs d'application Web ou des ressources intermédiaires comme les pare-feu et les équilibreurs de charge.

i. SYN Flood :

Un SYN Flood ressemble à un travailleur dans une salle d'approvisionnement recevant des demandes de l'avant du magasin. Le travailleur reçoit une demande, va chercher le colis et attend la confirmation avant de le mettre en avant. L'employé reçoit alors beaucoup plus de demandes de colis sans confirmation jusqu'à ce qu'il ne puisse plus transporter de colis, qu'il soit débordé et que les demandes commencent à rester sans réponse.

Cette attaque exploite la négociation TCP en envoyant à une cible un grand nombre de paquets SYN TCP « Initial Connection Request» avec des adresses IP source fausses. La machine cible répond à chaque demande de connexion, puis attend la dernière étape de confirmation (l'acquittement), qui ne se produit jamais, épuisant les ressources de la cible dans le processus.



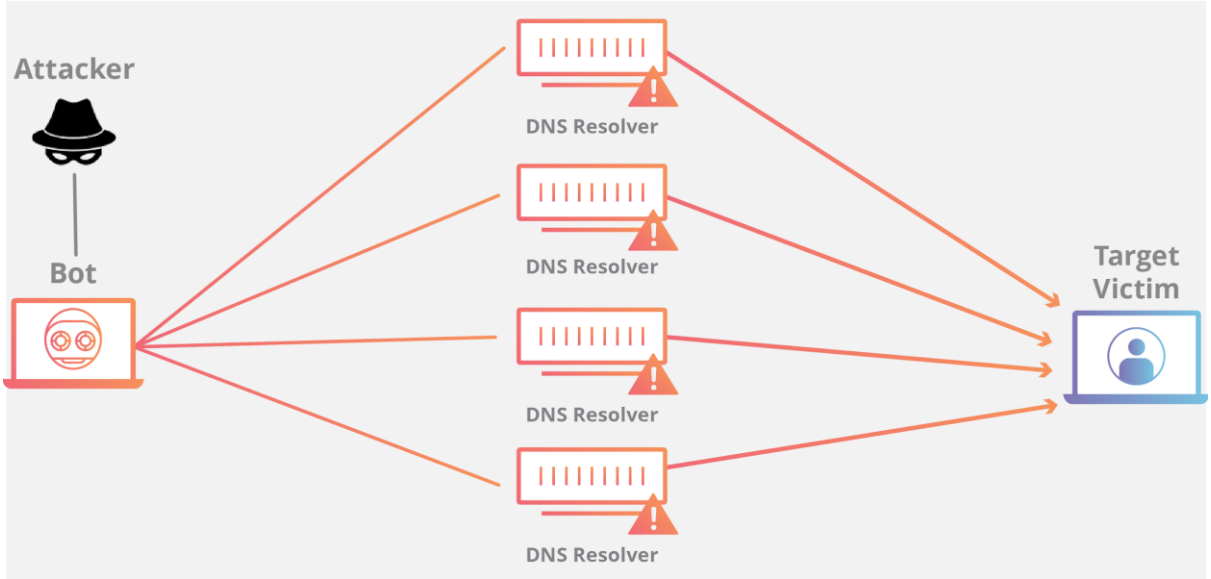
C. Attaques volumétriques

Cette catégorie d'attaques tente de créer une saturation en consommant toute la bande passante disponible entre la cible et Internet. De grandes quantités de données sont envoyées vers la cible en utilisant une forme d'amplification ou un autre moyen de créer un trafic massif, comme des demandes provenant d'un botnet.

ii. Amplification DNS :

Une amplification DNS, c'est comme si quelqu'un appelait un restaurant et disait "J'aurai l'un de tout, rappelez-moi et dites-moi toute ma commande", où le numéro de téléphone de rappel qu'ils donnent est le numéro de la cible. Avec très peu d'effort, une longue réponse est générée.

En faisant une demande à un serveur DNS ouvert avec l'adresse IP réelle de la cible, l'adresse IP cible reçoit alors une réponse du serveur. L'attaquant structure la demande de telle sorte que le serveur DNS réponde à la cible avec une grande quantité de données. En conséquence, la cible reçoit une amplification de la requête initiale de l'attaquant.



2. Les outils d'attaques DDoS les plus utilisés :

Voici quelques outils couramment utilisés :

- ✓ **Low Orbit Ion Cannon (LOIC)**

  Le LOIC est une application open-source de test de stress. Il permet de réaliser des attaques des couches protocoles TCP et UDP à l'aide d'une interface WYSIWYG facile à utiliser. En raison de la popularité de l'outil d'origine, des dérivés ont été créés pour permettre le lancement d'attaques à l'aide d'un navigateur Web.

- ✓ **High Orbit Ion Cannon (HOIC)**

  Cet outil d'attaque a été créé pour remplacer le LOIC en augmentant ses capacités et en ajoutant des personnalisations. En utilisant le protocole HTTP, le HOIC est en mesure de lancer des attaques ciblées qu'il est difficile d'atténuer. Le logiciel est conçu pour qu'un minimum de 50 personnes travaillent ensemble dans un effort d'attaque coordonné.

- ✓ **Slowloris**

  En plus d'être un primate lent, Slowloris est une application conçue pour déclencher une attaque faible et lente sur un serveur ciblé. L'élégance de Slowloris réside dans la quantité limitée de ressources dont il a besoin pour créer un effet néfaste.

✓ **R.U.D.Y (R-U-Dead-Yet)**

R.U.D.Y. est un autre outil d'attaque faible et lent conçu pour permettre à l'utilisateur de lancer facilement des attaques à l'aide d'une simple interface pointer-cliquer. En ouvrant plusieurs requêtes HTTP POST et en maintenant ces connexions ouvertes aussi longtemps que possible, l'attaque vise à submerger lentement le serveur ciblé.

IV. DDos : Comment prévenir les attaques DDoS:

On ne peut pas empêcher un attaquant de d'envoyer un trafic sur un serveur et cela parce que le serveur est destiné à recevoir de trafic. Mais on peut toujours se préparer pour éviter la surcharge.

1. Contrôler le trafic :

Cela revient à dire il faut savoir le volume normal de trafic, faible et élevé de votre organisation. Donc on doit être en possession de plusieurs informations :

- Connaître la valeur supérieure de trafic que votre serveur peut accepter. Cela va permettre de mettre un " rate limiting". Le serveur n'acceptera alors que le nombre de requêtes qu'il est capable de gérer.
- Avoir des informations statistiques sur les tendances de trafic circulant. Cela va permettre de détecter les problèmes plus rapidement.
- Il faut savoir que le trafic peut être augmenter ou diminuer selon les circonstances donc il faut être préparé à gérer les pointes de trafic. Un trafic légitime peut causer le même effet qu'une attaque DDoS. Et un arrêt de serveur peut causer des pertes considérables même si la source était légitime.

2. Avoir plus de bande passante :

Une fois que vous une idée sur le trafic maximal que le serveur peut supporter, vous devez avoir une bande passante plu large que cette valeur. Le fait d'obtenir plus de bande passante que nécessaire s'appelle l'over-provisioning ».

Cela vous permet de gagner du temps en cas d'attaque DDoS avant que votre site internet, serveur ou application ne soit complètement surchargé.

3. Filtrage par operateur de transit :

L'intervention de l'opérateur de transit est parfois nécessaire, en particulier lorsque le lien réseau mis à disposition du client est saturé. Les opérateurs permettent souvent d'effectuer du blackholing de trafic basé sur la destination. Il convient de noter que cette mesure, parfois nécessaire, rend le déni de service effectif. L'opérateur peut également offrir un service de filtrage de trafic. Dans le cas où ce service est opéré par

le client, ce dernier doit s'assurer de maîtriser la configuration des différentes contre-mesures offertes par la plate-forme.

4. Utilisez un réseau de diffusion de contenu (CDN)

Le but d'une attaque DDoS est de surcharger votre serveur d'hébergement. Une des solutions est donc de stocker vos données sur plusieurs serveurs répartis dans le monde entier.

C'est exactement ce que permet un réseau de diffusion de contenu (CDN).

Les CDN servent votre site internet ou des données aux utilisateurs depuis un serveur situé à proximité de l'utilisateur afin d'offrir de meilleures performances. Mais l'utilisation d'un CDN vous permet également d'être moins vulnérable à une attaque, car en cas de surcharge d'un serveur, de nombreux autres restent opérationnels.

V. Que faire si vous êtes la cible d'une attaque DDoS

Aujourd'hui, les attaques DDoS sont sophistiquées et puissantes qu'il peut être très difficile de les régler seul. C'est pourquoi la meilleure ligne de défense contre une attaque sera de disposer des bonnes mesures de prévention.

Mais si vous êtes la cible d'une attaque et votre serveur n'est plus en ligne, voici ce que vous pouvez faire :

1. Mettre rapidement en place des mesures défensives

Si vous avez une bonne idée de ce à quoi ressemble un trafic normal, vous devriez pouvoir identifier assez rapidement une attaque DDoS.

Vous verrez un flux massif de requêtes serveur ou de trafic web provenant de sources suspectes. Mais vous pouvez disposer d'un peu de temps avant la surcharge totale et le plantage de vos serveurs.

Configurez dès que possible le « rate limiting » et supprimez vos journaux de serveur afin de libérer de l'espace.

2. Contactez votre hébergeur

Si quelqu'un d'autre possède et administre le serveur abritant vos données, informez-le de l'attaque immédiatement.

Il pourrait être capable de faire disparaître le trafic (« black hole ») jusqu'à ce que l'attaque cesse, ce qui signifie que les requêtes arrivant au serveur seront simplement écartées, qu'elles soient légitimes ou non. C'est dans son intérêt d'agir ainsi, afin que les serveurs de ses clients ne plantent pas.

À partir de là, il réacheminer probablement le trafic vers un « épurateur » pour filtrer le trafic illégitime et laisser passer les requêtes ordinaires.

3. Contactez un spécialiste

Si vous subissez une attaque de grande ampleur ou si vous ne pouvez pas vous permettre la moindre interruption de votre site internet ou application, vous devriez envisager de contacter un expert DDoS.

Il peut détourner votre trafic vers ses énormes serveurs capables de gérer la charge et de tenter d'épurer les requêtes illégitimes.

4. Attendre

Engager un professionnel pour rediriger et épurer votre trafic web est une opération onéreuse.

La plupart des attaques DDoS cessent après quelques jours (même si dans les cas les plus graves, elles peuvent durer plus longtemps), vous avez donc toujours la possibilité d'accepter cette perte et d'être mieux préparé la prochaine fois.

VI. Comment éviter de participer à un DDoS ?

Il est indispensable de veiller à anticiper les attaques DDoS, mais il est aussi indispensable de veiller à ne pas participer à des attaques DDoS en étant un vecteur pour mener ce type d'attaque. Il faut donc avoir de bonnes pratiques et les mettre en place sur nos machines

1. Les services inutilisés doivent être désactivés au niveau des serveurs. Par ailleurs, une entité hébergeant des services exploitables peut mettre en place des règles permettant de limiter le trafic à la bordure de son réseau, voire de le filtrer afin d'interdire l'interrogation de tels services.
2. Le durcissement des systèmes d'exploitation en limitant les privilèges et en utilisant les anti-virus
3. Restreindre la configuration des services aux seules fonctions nécessaires
4. Les applications web peuvent être exploitées pour mener des attaques par déni de service distribué. Les Framework, les CMS (Content Management System) et les greffons utilisés doivent être maintenus à jour. Par ailleurs, le développement de ces applications doit respecter les bonnes pratiques.
5. L'accès aux services d'une entité doit être restreint afin de n'autoriser que les réseaux internes à celle-ci. Par ailleurs, la mise en place de règles de ratelimiting peut réduire une éventuelle participation à une attaque par déni de service. Enfin, le trafic sortant de l'entité doit être filtré afin de bloquer l'envoi de trafic pour lequel les adresses IP sources sont usurpées.

VII. Conclusion

Comme tout le reste dans l'informatique, les attaques DDoS évoluent et deviennent plus destructrices pour les entreprises. Ces attaques utilisent de nouvelles techniques pour atteindre leurs énormes nombres de bande passante telle que l'exploitation des appareils Internet des objets (IoT) pour créer un botnet, comment serait-il amusant que votre réfrigérateur fasse partie d'un botnet !

Les attaques DDoS peuvent être très coûteuses, en particulier pour les entreprises qui fournissent des services via Internet en raison de l'interruption de ces services. De même, contrer une attaque DDoS pourrait s'avérer très coûteux. Combien de personnes devront consacrer leurs efforts à lutter contre l'attaque au lieu de s'occuper des activités informatiques essentielles de votre entreprise ? Combien de temps faudra-t-il pour redémarrer vos applications ou vos serveurs, puis les tester afin d'en vérifier le bon fonctionnement ? Et si des données sont perdues ? Si, par exemple, votre serveur plante pendant qu'une transaction est en cours, tout le disque pourrait être corrompu en raison d'une erreur de lecture et d'écriture.

De nos jours, chaque entreprise mature doit mettre en place et exploiter des mécanismes pour répondre à de telles attaques dévastatrices.

VIII. Bibliographie :

Partie Définition et principe :

- https://www.lebigdata.fr/
- https://www.securiteinfo.com/
- journaldunet.com
- Kaspersky Lab

Partie Types et outils :

- https://www.cloudflare.com/
- https://www.imperva.com/
- « Distributed Denial of Service Attack and Defense » De Shui Yu.

Partie Comment prévenir les attaque DdoS, Que faire si vous etes cible d'une attaque, comment éviter de participer à une attaque DDoS:

- https://www.securiteinfo.com/
- Comprendre et anticiper les attaques DDoS- ANSSI Agence nationale de la sécurité des systèmes informatiques
- https://www.kaspersky.fr/