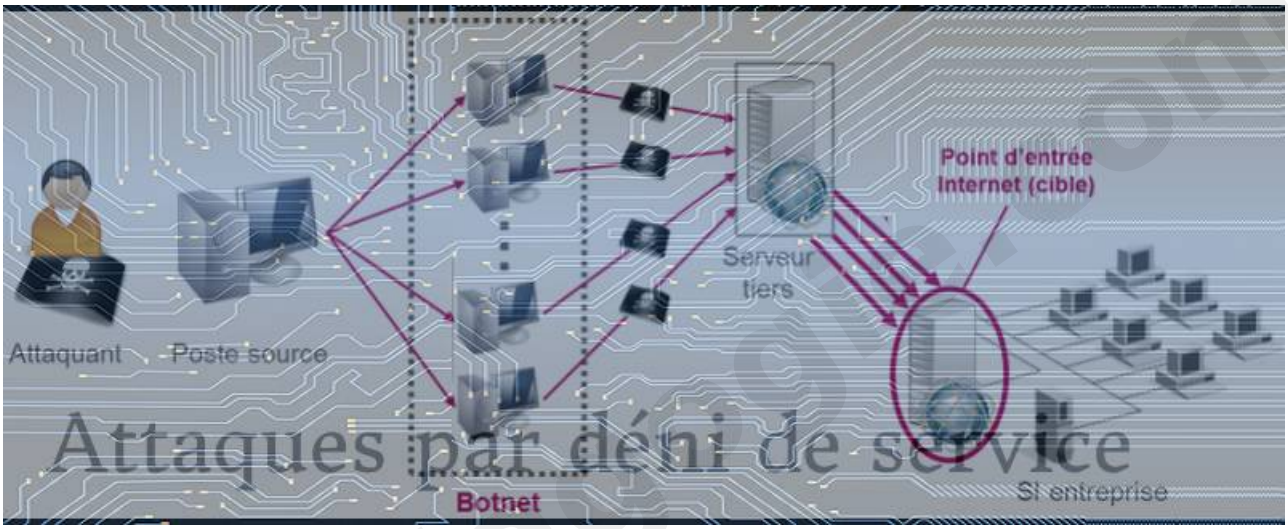
Attaques par déni de service

1. **Objectifs**

- Connaitre les attaques par déni de service

- **Présentation**



- Une attaque par déni de service (abr. DoS attack pour Denial of Service attack en anglais) est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. À l'heure actuelle la grande majorité de ces attaques se font à partir de plusieurs sources, on parle alors d'attaque par déni de service distribuée (abr.**DDoS** attack pour **D**istributed **D**enial **o**f **S**ervice attack). Il peut s'agir de :
- Une **attaque par déni de service** (**DoS**, **D**enial **o**f **S**ervice) est un type d'attaque visant à rendre indisponible pendant un temps indéterminé les services ou ressources d'une organisation.
- Il s'agit la plupart du temps d'attaques à l'encontre des serveurs d'une entreprise, afin qu'ils ne puissent être utilisés et consultés.
- Une attaque DDoS, aussi appelée attaque par déni de service, est une technique assez basique de piratage qui noie les serveurs d'un site Internet sous de (trop) nombreuses connexions, pour le rendre rapidement inaccessible. Le ou les pirates ont recours à des "**botnets**", armée d'ordinateurs infectés qui envoient des requêtes en boucles. Les smartphones ainsi que les appareils connectés, c'est-à-dire tout ce qui peut se connecter à un site Internet, composent de plus en plus ces botnets.

- Les attaques par déni de service sont un fléau pouvant toucher tout serveur d’entreprise ou tout particulier relié à Internet. Le but d’une telle attaque n’est pas de récupérer ou d’altérer des données, mais de nuire à la réputation de sociétés ayant une présence sur Internet et éventuellement de nuire à leur fonctionnement si leur activité repose sur un système d’information.
- **On distingue deux types d’attaques** : non distribuées et distribuées.

Différents types d’attaques DDOS (Source ANSSI)

- **Les botnets**
  - Les attaques **DDoS** peuvent être lancées à partir de réseaux de machines compromises appelés botnets.
  - "**Botnet**" est une contraction des termes "robot" et "network" (réseau). Les cyber-criminels utilisent des chevaux de Troie spéciaux pour violer la sécurité des ordinateurs de différents utilisateurs, prendre le contrôle de chacun de ces ordinateurs infectés et les regrouper au sein d'un réseau de "bots" gérables à distance.
    Un botnet (contraction de l'anglais "robot net" : "réseau de robots") est un réseau de bots informatiques, des programmes connectés à Internet qui communiquent avec d'autres programmes similaires pour l'exécution de certaines tâches.
  - De nombreux outils accessibles en ligne permettent d’exploiter des botnets. Au cours des dernières années, des services de DDoS en ligne, couramment appelés booter ou stresser, ont fait leur apparition. Ces services proposent des tarifs autorisant leur usage par des particuliers, et permettent à un utilisateur de lancer des attaques contre la cible de son choix. Par ailleurs, certains booter proposent de tester le service gratuitement pendant quelques minutes.
  - La diversité des outils et services permettant de lancer des attaques par déni de service distribué contribue à l’augmentation du nombre de ces attaques.
- **Attaque par réflexion**
  - La technique dite attaque par réflexion (smurf) est une attaque par déni de service basée sur l'utilisation de serveurs de diffusion (broadcast) pour paralyser un réseau. Un serveur broadcast est un serveur capable de dupliquer un message et de l’envoyer à toutes les machines présentes sur le même réseau.
  - Le scénario d’une telle attaque est le suivant :

apcpedagogie.com

        - La machine attaquante envoie une requête ping (ping est un outil exploitant le protocole ICMP, permettant de tester les connexions sur un réseau en envoyant un paquet et en attendant la réponse) à un ou plusieurs serveurs de diffusion en falsifiant l'adresse IP source (adresse à laquelle le serveur doit théoriquement répondre) et en fournissant l'adresse IP d'une machine cible.
        - Le serveur de diffusion répercute la requête sur l'ensemble du réseau.
        - Toutes les machines du réseau envoient une réponse au serveur de diffusion.
        - Le serveur broadcast redirige les réponses vers la machine cible.
    - Ainsi, lorsque la machine attaquante adresse une requête à plusieurs serveurs de diffusion situés sur des réseaux différents, l'ensemble des réponses des ordinateurs des différents réseaux vont être routées sur la machine cible.
    - De cette façon l'essentiel du travail de l'attaquant consiste à trouver une liste de serveurs de diffusion et à falsifier l'adresse de réponse afin de les diriger vers la machine cible.

- **Attaque par amplification**

    - L'attaque par amplification est une variante de l'attaque par réflexion. Ces attaques n'utilisent pas une adresse de broadcast
      mais des mécanismes réseau plus complexes (les adresses de broadcast sont très surveillées par les pare-feu, et un réseau bien configuré ne permet plus d'exploiter ce genre de procédé).
    - L'actualité récente (2015) a mis en avant une attaque très efficace qui consiste à utiliser des serveurs dont la réponse à une requête renvoie bien plus de données que la requête originale.
    - C'est par exemple le cas des serveurs NTP (Network Time Protocol). Ces derniers sont chargés de donner l'heure sur le réseau (indispensable pour de nombreuses tâches des systèmes).
    - Chaque serveur peut fournir une liste des ordinateurs qui sont connectés à lui. Il suffit pour cela d'envoyer une commande. En forgeant une demande avec une adresse d'origine falsifiée, on peut très facilement générer un gros volume de données (environ 200 fois la taille du paquet original). En multipliant ces demandes et en faisant envoyer la réponse à la victime de l'attaque, on génère un flux très important. Ce type d'amplification a déjà été utilisé sur les protocoles DNS et SMTP avec des taux d'amplification allant jusqu'à 650 fois le flux original.

- **Attaque du ping de la mort**

apcpedagogie.com

- L'attaque du ping de la mort (ping of death) est une des plus anciennes attaques de déni de service.
- Le principe du ping de la mort consiste tout simplement à créer un datagramme IP dont la taille totale excède la taille maximum autorisée (65 536 octets).
- Un tel paquet envoyé à un système possédant une pile TCP/IP vulnérable, provoquera un plantage.
- Plus aucun système récent n'est vulnérable à ce type d'attaque.

- **Attaque par fragmentation**

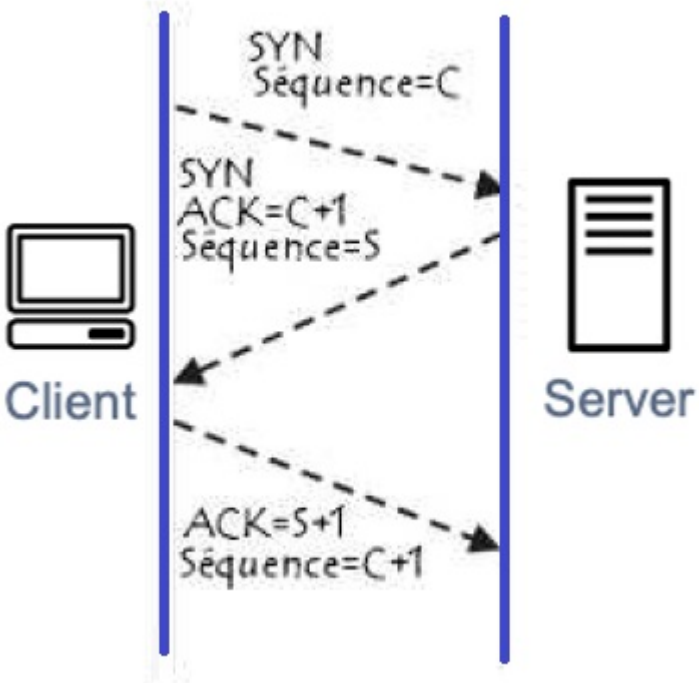
  - Une attaque par fragmentation (fragment attack) est une attaque réseau par saturation (déni de service) exploitant le principe de fragmentation du protocole IP.
  - En effet, le protocole IP est prévu pour fragmenter les paquets de taille importante en plusieurs paquets IP possédant chacun un numéro de séquence et un numéro d'identification commun. À réception des données, le destinataire réassemble les paquets grâce aux valeurs de décalage (offset) qu'ils contiennent.
  - L'attaque par fragmentation la plus célèbre est l'attaque Teardrop. Son principe consiste à insérer dans des paquets fragmentés des informations de décalage erronées. Ainsi, lors du réassemblage il existe des vides ou des recoupements (overlapping), pouvant provoquer une instabilité du système. À ce jour, les systèmes récents ne sont plus vulnérables à cette attaque.

- **Attaque LAND**

  - L'attaque LAND est une attaque réseau par déni de service datant de 1997, utilisant l'usurpation d'adresse IP afin d'exploiter une faille de certaines implémentations du protocole TCP/IP dans les systèmes vulnérables. Le nom de cette attaque provient du nom donné au premier code source diffusé permettant de mettre en oeuvre cette attaque : land.c.
  - L'attaque LAND consiste ainsi à envoyer un paquet possédant la même adresse IP et le même numéro de port dans les champs source et destination des paquets IP.
  - Dirigée contre des systèmes vulnérables, cette attaque avait pour conséquence de faire planter les systèmes ou de les conduire à des états instables. Les systèmes récents ne sont aujourd'hui plus vulnérables à ce type d'attaque.

- **Attaque SYN**

apcpedagogie.com



- L’attaque SYN (appelée également TCP/SYN Flooding) est une attaque réseau par saturation (déni de service) exploitant le mécanisme de poignée de mains en trois temps (Three-ways handshake) du protocole TCP.
- Le mécanisme de poignée de main en trois temps est la manière selon laquelle toute connexion « fiable » à Internet (utilisant le protocole TCP) s’effectue.
- Lorsqu’un client établit une connexion à un serveur, le client envoie une requête SYN, le serveur répond alors par un paquet SYN/ACK et enfin le client valide la connexion par un paquet ACK (acknowledgement, qui signifie accord ou remerciement).
- Une connexion TCP ne peut s’établir que lorsque ces trois étapes ont été franchies. L’attaque SYN consiste à envoyer un grand nombre de requêtes SYN à un hôte avec une adresse IP source inexistante ou invalide. Ainsi, il est impossible que la machine cible reçoive un paquet ACK.
- Les machines vulnérables aux attaques SYN mettent en file d’attente, dans une structure de données en mémoire, les connexions ainsi ouvertes, et attendent de recevoir un paquet ACK. Il existe un mécanisme d’expiration permettant de rejeter les paquets au bout d’un certain délai. Néanmoins, avec un nombre de paquets SYN très important, si les ressources utilisées par la machine cible pour stocker les requêtes en attente sont épuisées, elle risque d’entrer dans un état instable pouvant conduire à un plantage ou un redémarrage.

- **Attaque de la faille TLS/SSL**

apcpedagogie.com

- Une faille découverte en novembre 2009 par le chercheur Marsh Ray sur la gestion du protocole de sécurité SSL a permis d'élaborer des attaques DDOS très efficaces contre des cibles utilisant le protocole HTTPS et ayant des moyens matériels conséquents.
- Le principe est d'envoyer de nombreuses demandes de renégociation du protocole SSL. Le client demande au serveur de générer une nouvelle clé de chiffrement pour la connexion en cours.
- Ces demandes créent une grande consommation de ressources CPU sur le serveur web. La dissymétrie entre les capacités de l'attaquant et celle de la cible est telle qu'une seule machine peut rendre inaccessible un site : la charge générée est, en effet, environ quinze fois plus importante pour le serveur que pour le client.
- Il est à noter que cette attaque a été tellement efficace que le document (RFC) décrivant le protocole TLS a été modifié dès janvier 2010 pour supprimer cette vulnérabilité.

- **Attaque par downgrade**

  - Une **attaque par repli**, **attaque par rétrogradation** ou **négociation à la baisse** (en anglais : **downgrade attack**) est une attaque informatique consistant à passer d'un fonctionnement sécurisé à un fonctionnement moins sécurisé.
  - L'attaque par downgrade (aussi appelée par abaissement de version) consiste à profiter d'une option de compatibilité de certains programmes réseau (serveur web notamment) : l'attaquant demande au serveur d'utiliser une version d'un protocole plus ancienne afin d'exploiter les failles qu'elle comporte.
  - Ce type d'attaques est revenu sur le devant de la scène en 2014 avec la faille appelée POODLE1 (Padding Oracle On Downgraded Legacy Encryption).
  - La faille POODLE consistait à demander au serveur l'utilisation du protocole SSL 3 – qui comporte une faille – au lieu de versions plus récentes. L'attaquant pouvait alors déchiffrer plus facilement les communications dans le cadre d'une attaque man in the middle.
  - Cette attaque par downgrade peut s'effectuer sur toutes les applications réseau qui comportent des fonctionnalités de compatibilité avec d'anciennes versions. C'est notamment le cas de SSH1, PPTP, ou encore des protocoles de sécurité WiFi (certaines bornes permettent d'utiliser à la demande soit WPA2 soit WPA).

- **Attaque par requêtes élaborées**

  - Une variante de l'attaque DoS consiste à envoyer en masse, non pas des paquets sans objet ou exploitant des failles mais des requêtes légitimes (attaque sur la couche 7 – applicative – du modèle OSI).

apcpedagogie.com

- L’idée de l’attaquant est de rendre inaccessible un site web ou un service en lui faisant traiter des demandes qui sollicitent beaucoup la base de données.
- Ce type d’attaque demande une analyse fine de la cible : pages html qui ne sont pas en cache et qui sollicitent directement la base de données, pages générant des demandes de données très importantes ou créant des erreurs sur le serveur, module du site connu pour une faille particulière... Ce type d’attaque a pour principal avantage d’être très difficilement détectable. La parade est d’autant plus complexe que les requêtes seront pertinentes et variées.

Exercice d'application

[h5p id="53"]

Sommaire du cours Administration et sécurité des sites web

Source : https://apcpedagogie.com/attaques-par-deni-de-service · téléchargé le 04/11/2026 · © APC Pédagogie · apcpedagogie.com

apcpedagogie.com