Exemple de problème « Deny of Service ». (DoS)

L’attaque par déni de service

Une attaque par déni de service (DoS attack pour Denial of Service attack en anglais) est une attaque informatique ayant pour but de rendre indisponible un service ou d'empêcher les utilisateurs légitimes d'un service de l'utiliser.

Il peut s'agir de :

- l’inondation d’un réseau afin d'empêcher son fonctionnement ;
- la perturbation des connexions entre deux machines, empêchant l'accès à un service particulier ;
- l'obstruction d'accès à un service pour une personne en particulier ;
- Empêcher la distribution de courriel dans une entreprise
- Ou simplement l’impossibilité pour un utilisateur de prendre un rendez-vous par informatique.

L'attaquant n'a pas forcément besoin de matériel sophistiqué. Ainsi, certaines attaques DoS peuvent être exécutées avec des ressources limitées contre un réseau de taille plus importante et plus moderne.

Recherche de la cause et résolution :

1 Analyse anti-virus.

Si vous devez rechercher un problème de « Deny of Service ».
Vous devez, <u>bien sûr, en premier</u>, analyser <u>tous</u> vos serveurs et vos postes pour chercher les virus.

2 Analyse réseau. (Saturation du réseau)

2A Saturation des liaisons informatiques.

Il vous faut donc tester le débit de la ou des cartes réseaux du ou des serveurs, puis, si tout est ok, vous intéresser à votre box ou vos routeurs pour voir si la saturation vient de l’extérieure.
Si problème : rechercher l’adresse IP de l’attaquant, sans oublier que cela peut-être une panne de type : carte réseau bavarde ou routeur interne défectueux.
Exemple de panne routeur : une de lame du routeur central n’a pas le même niveau de microcodes que les autres lames. Cela crée des collisions Ethernet, donc des arbitrages etc... (Voir le Protocole Ethernet).

2B Vérifier la configuration des routeurs.

Analyser les passerelles et les protocoles de routages pour vérifier s’ils n’ont pas été modifiés.
Il peut s’agir simplement d’un port de communication effacé dans un routeur ou d’une modification de la DMZ ou d’un par feu d’un serveur.

2C Tester le service en passant par l'extérieur.

Ne pas oublier de tester de l'extérieur, votre réseau informatique y compris en utilisant un smartphone avec le Wifi désactivé.

3 « DoS » pour une personne en particulier ou un groupe de personne.

Il faut utiliser la machine incriminée ou avoir une copie des identifiants de la personne.
Le ou les problèmes peuvent être multiples en commençant par l'active directories.
Par exemple : le problème peut être lié au poste de travail, a l'adresse IP ou seulement une mauvaise configuration des serveurs ou des routeurs.

4 « DoS » pour le courriel de l'entreprise.

Comme pour un DoS pour une personne vu au-dessus, les actions à mener pour identifier le problème sont trop nombreuses pour toutes les citer ici.

5 Impossibilité pour un utilisateur de prendre un rendez vous informatique ou un autre service client.

Ce « DoS » est très fréquent dans les services informatiques des administrations.
Ce n'est souvent pas une vraie panne mais simplement la saturation d'un service par une trop grande demande.
C'est par exemple une ou des associations qui remplissent (volontairement) tous les créneaux horaires disponibles d'une administration, de faux rendez-vous pour être sur d'avoir des créneaux horaires disponibles pour leurs adhérents.
Mais cela peut être aussi seulement une personne mécontente qui veut nuire à une Mairie ou une autre administration.

Conclusion.

Comme tout dépannage rechercher les causes d'un « DoS » dans un système informatique demande de bien cerner le problème avant de commencer. Et de ne pas partir avec des idées préconçues.

Si le problème est bien une attaque extérieure il ne faut pas hésiter à porter plainte auprès de la gendarmerie, celle-ci est actuellement équipée pour retrouver l'adresse IP, donc l'adresse réel du coupable.

CAS d'une attaque extérieure.

Si c'est une attaque « DoS » multiple on change de domaine de compétence.

« Attaque par Déni de service distribué (ou attaque par effet de levier) »
C'est un groupe de personnes ou de serveurs qui attaquent un service ou une entreprise.
Souvent la cause est politique, sociale, financière ou seulement pour nuire à un concurrent industriel. Cette attaque peut provenir d'états ou de mercenaires informatiques. Dont le but est de nuire un autre état ou de faire payer une entreprise.

Dans ce cas l'attaquant utilise un botnet soit un certain nombre de pc connectés ensemble pour saturer l'adresse IP de la cible.

Le botnet peut être des PC loués pour l'occasion ou plus probablement un groupe de PC infectés par un virus qui répondrons aux sollicitations de l'attaquant pour créer ce botnet.

Mais dans la plupart des cas une attaque DOS venant de l'extérieur est une attaque payée par quelqu'un, ce n'est pas de l'amateurisme.

L'attaque par elle-même est souvent très simple.

Exemple :

On demande à chaque à chaque PC du botnet d'envoyer une commande PING modifiée à la cible. Au lieu d'envoyer un PING classique de 4 bytes (que la cible doit renvoyer) on lui envoie un Ping de 40 000 bytes ou plus. Et si tous les PC du botnet font la même chose, en même temps, le serveur cible n'arrivera même pas à répondre aux PING et donc ne répondra plus à personne.

MIRAI est le logiciel le plus populaire qui peut préparer (infester) et mobiliser sont réseau de botnets pour lancer une attaque DDoS.