Agir contre une attaque par déni de service

Les objectifs de l'attaque

Rendre indisponible un service en ligne pour porter directement atteinte à l'image de son propriétaire et à la confiance que peuvent avoir les utilisateurs.

Une attaque par déni de service ou en déni de service distribué (DDoS pour Distributed Denial of Service en anglais) vise à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à le saturer ou par l'exploitation d'une faille de sécurité afin de provoquer une panne ou un fonctionnement fortement dégradé du service.

Mesures de réaction

Identifier la ou les origines de l'attaque ainsi que la méthode utilisée. Il faut s'assurer qu'il s'agit réellement d'un DOS ou d'un DDOS :

- **Identifier** où se situe le crash ou la saturation de la machine (ou des machines)
- **Identifier** la cible de l'attaquant
- **Déconnecter** le service si besoin durant les recherches

Si l'attaque vise les **couches applicatives** (basée sur l'exploitation d'une vulnérabilité / erreur de configuration) :

- **Appliquer les derniers correctifs** de l'équipement / système / application
- **Durcir la configuration** de l'équipement / système et/ou utiliser des applications spécifiques contre les attaques DOS
- **Surveiller** l'équipement / l'application (utilisation de Nagios, etc.). Attention au déchiffrement du trafic SSL.
- **Auditer** l'application / équipement visé(e) et réaliser régulièrement des scans

Si l'attaque consiste **à saturer le réseau** :

- **Utiliser un équipement de type pare-feu ou répartiteur de charge**. Attention même si ces équipements permettent d'améliorer la résistance à une attaque par déni de service, ils ne sont en général pas suffisants.
- **Utiliser un équipement de protection spécifique aux attaques DOS**. En plus de posséder des capacités de traitement adaptées, ces équipements possèdent des fonctionnalités de filtrage spécifique Anti-DOS.
- **Solliciter l'opérateur de transit ou le fournisseur d'accès à Internet** afin de filtrer le trafic en amont
- **Recourir à des services** de Content Delivery Network (CDN)
- Etudier si l'équipement / application visé peut être hébergé(e) dans le « cloud »
- **Planifier régulièrement** des tests de charge

LIENS UTILES ANSSI

Comprendre et anticiper les attaques DDOS
Dénis de service - Prévention et réaction