

Comprendre et Anticiper les **Dénis de Service**





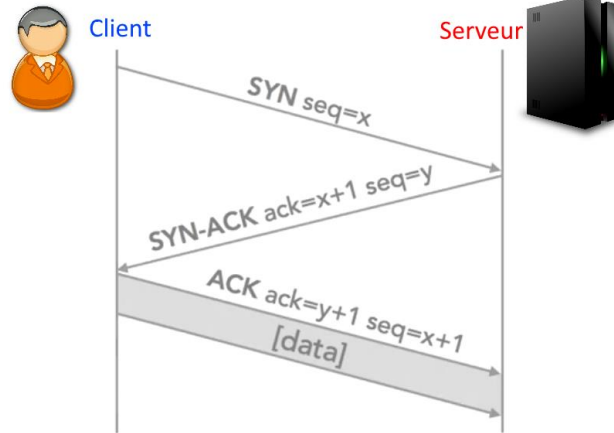
Qu'est-ce qu'un **Déni de service** ?

- ⦿ Bloquer la **disponibilité** d'un service
- ⦿ **En ligne** : sites web
- ⦿ **Hors ligne** : ransomwares
- ⦿ Déni de service **simple** (DOS) VS déni de service **distribué** (*DDOS*)
- ⦿ Autre type : attaque par amplification (utilisation de service légitime)



Attaques basées sur le **réseau**

- TCP SYN Flood
- Smurf (ICMP) flood
- UDP flood
- ARP Flood
- DNS Reflection
- Attaques sur les réseaux sans-fil, HTTP, FTP...Etc





Démonstration avec hping



Comment s'en prémunir

- ⦿ Difficile mais pas impossible
- ⦿ Mitigation à travers le design : **filtrage**, gestion des **priorités**, **blocage**
- ⦿ Mitigation « *opérationnelle* » : Vérification des adresses IP, détection trafic malveillant
- ⦿ Utiliser des **services de mitigation** : *Cloudflare*, *OVH*...etc