DOS UN SERVEUR TCP

VELOZZI Mathieu - FINOT Guillaume - CROZET Gabin

Start

SOMMAIRE

1. C’est quoi une attaque par déni de service ?

2. Démonstration et explications d’une attaque DoS de type SYN Flood

3. Comment l’attaque fonctionne-t-elle ?

C'EST QUOI UNE ATTAQUE DOS

1. Que signifie DoS ?

DoS (Denial of Service attack), désigne toute les attaques ayant pour objectif de saturer un serveur pour le rendre indisponible

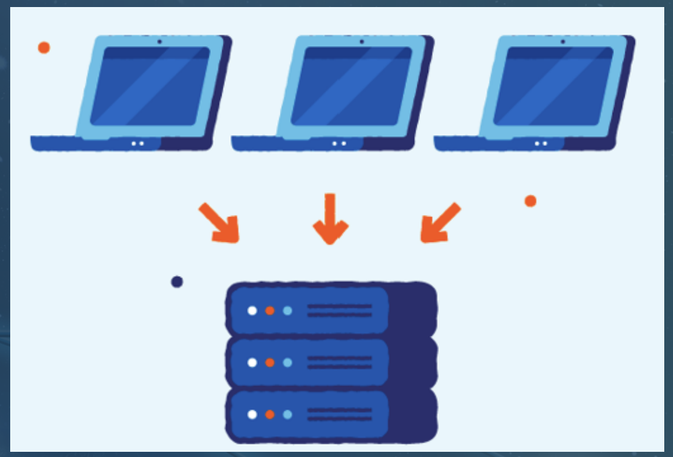
2. C'est quoi une attaque SYN Flood ?

Attaque DoS visant à émettre un nombre suffisant de demande de synchronisation TCP incomplète avec un serveur pour le rendre hors service

3. Historique du DoS

L'attaque par déni de service a vu le jour dans les années '80. Mais très vite un autre type d'attaque similaire et plus puissant a vu le jour, le DDoS

DOS VS DDOS



- Appareil source unique
- Fausses requêtes
- Se produit à petite échelle

- Appareil source multiple
- Vraies requêtes
- Peut se produire à grande échelle

HPING 3

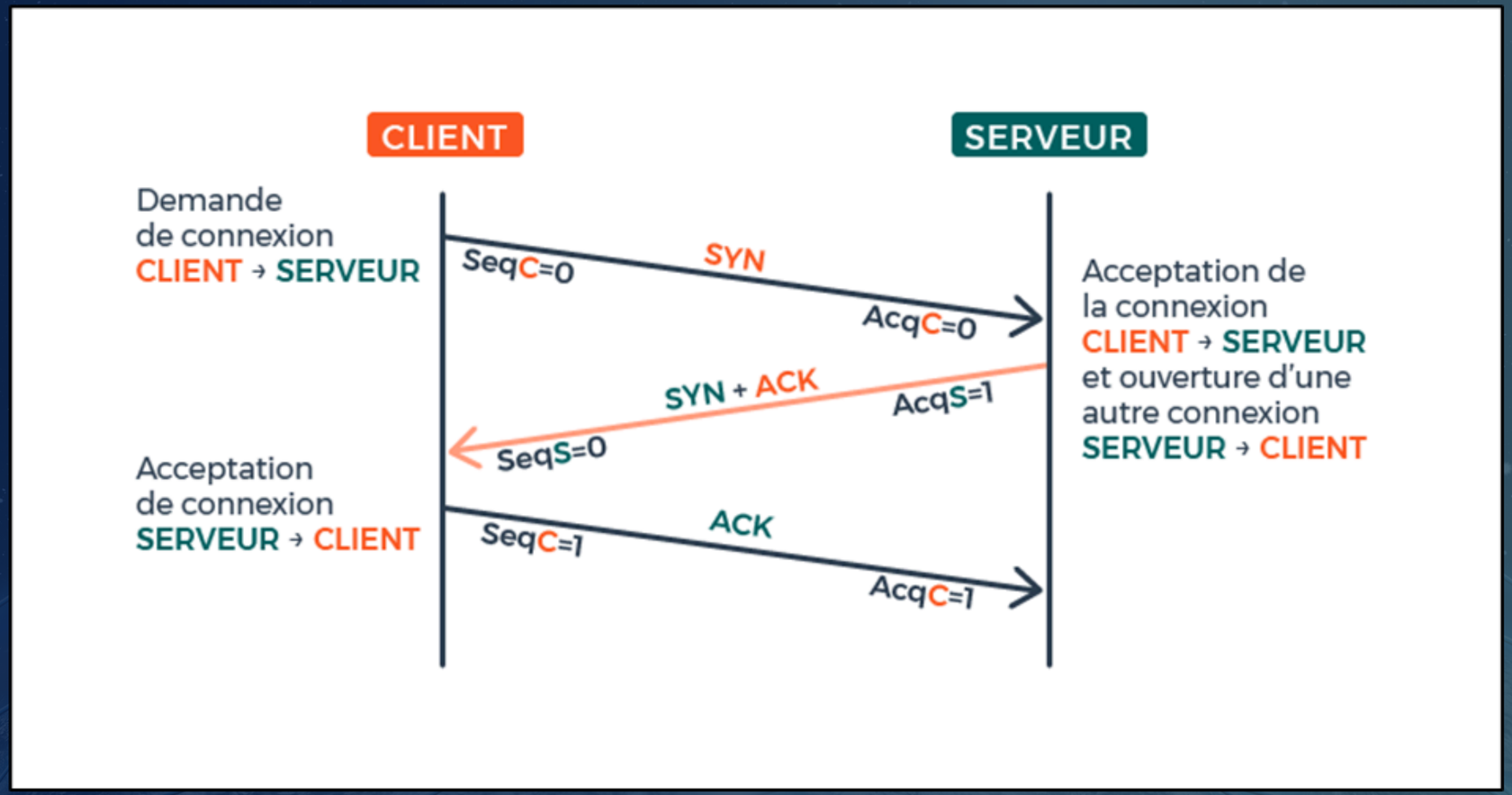
- Outils de cybersécurité
- Scan de port
- Socket raw
- Attaque par SYN flood
- Forge de paquets

COMMANDES HPING3

- hping3 --scan [IP]
  [plage IP]
- hping3 -[flag] [IP] -p [port] --rand-source
  -S -t [TTL] --flood
  -R -f [frag]
  -A

PLACE À LA DÉMO !

SYNCOOKIE


CLIENT
SERVEUR
Demande de connexion CLIENT → SERVEUR
SeqC=0
SYN
AcqC=0
Acceptation de la connexion CLIENT → SERVEUR et ouverture d'une autre connexion SERVEUR → CLIENT
SYN + ACK
AcqS=1
SeqS=0
Acceptation de connexion SERVEUR → CLIENT
ACK
SeqC=1
AcqC=1

SYNCOOKIE

encodage

$$syncookie = H(s_1, sa, sp, da, dp) + ISN_c + (t \times 2^{24}) + (H(s_2, sa, sp, da, dp, t) \bmod 2^{24}) + MSS_i$$ [11]

décodage

$$MSS_{i_2} = acknum - seqnum - t \times 2^{24} - H(s_1, sa, sp, da, dp) - (H(s_2, sa, sp, da, dp, t) \bmod 2^{24})$$ [11]

AVANTAGES

1. Protège contre les attaques DoS de type SYN flood

2. Permet d’éviter de stocker les connexions semi-ouvertes

3. Maintient de la disponibilité du serveur

INCONVENIENT

1. Consommation des resources CPU

2. Falsification des SYN Cookie

PLACE À LA DÉMO !

CONCLUSION