3TI
Sécurité des réseaux informatiques
2015-2016

Les attaques par déni de service

V.Van den Schrieck

Brainstorming

- Qu'est ce qu'un déni de service?
- Quelles sont les conséquences d'une telle attaque?
- Quel débit les attaques DDoS peuvent-elles atteindre?

DoS : Impact BW

2010

100 GBps

2002
400 MBps

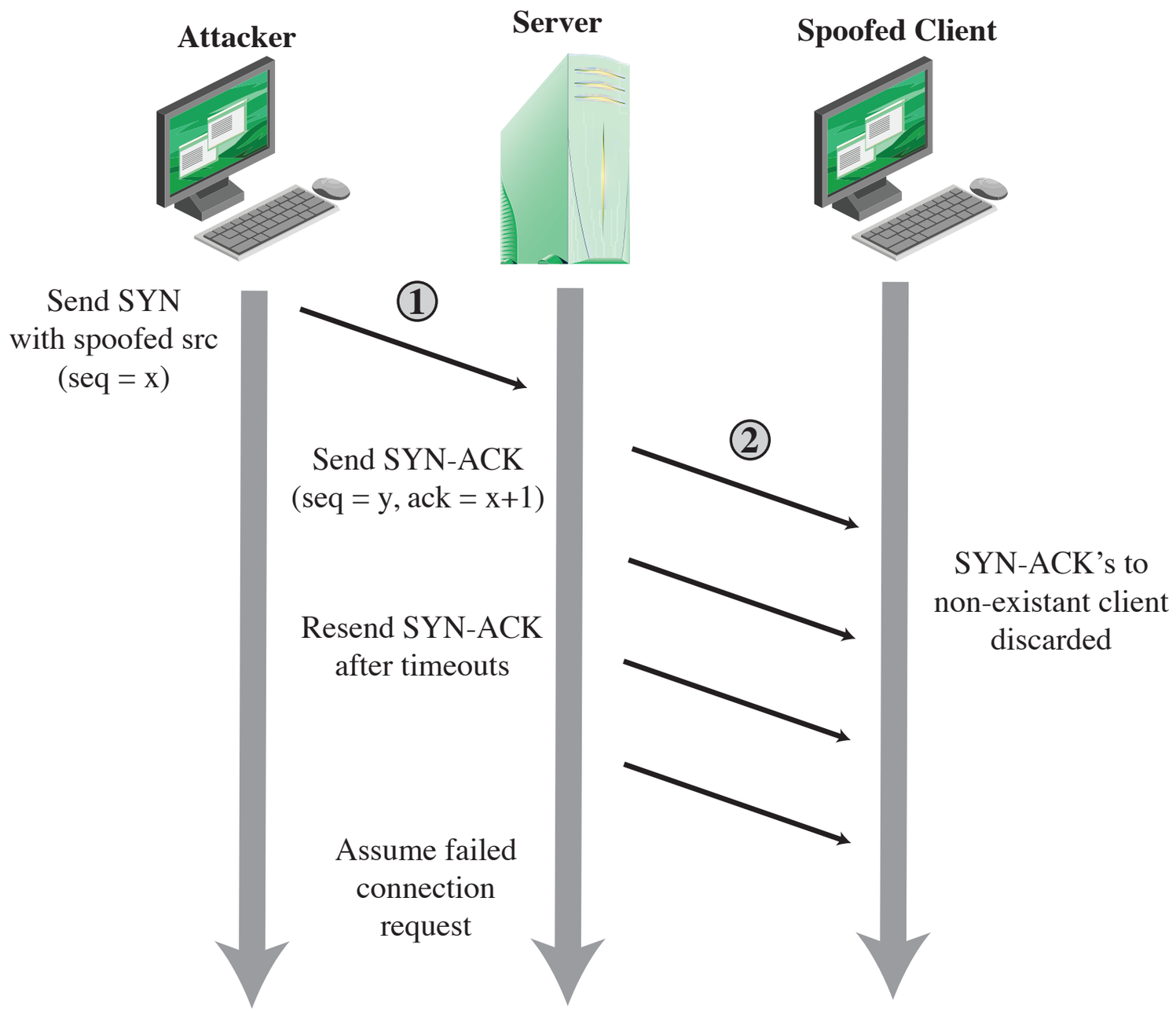
2013

Spamhaus
300 GBps

Mécanismes DoS

- BW réseau (ex : Ping flooding)
- Ressources système (ex : SYN spoofing ou poison packet)
- Ressources applicatives (ex : cyberslam)

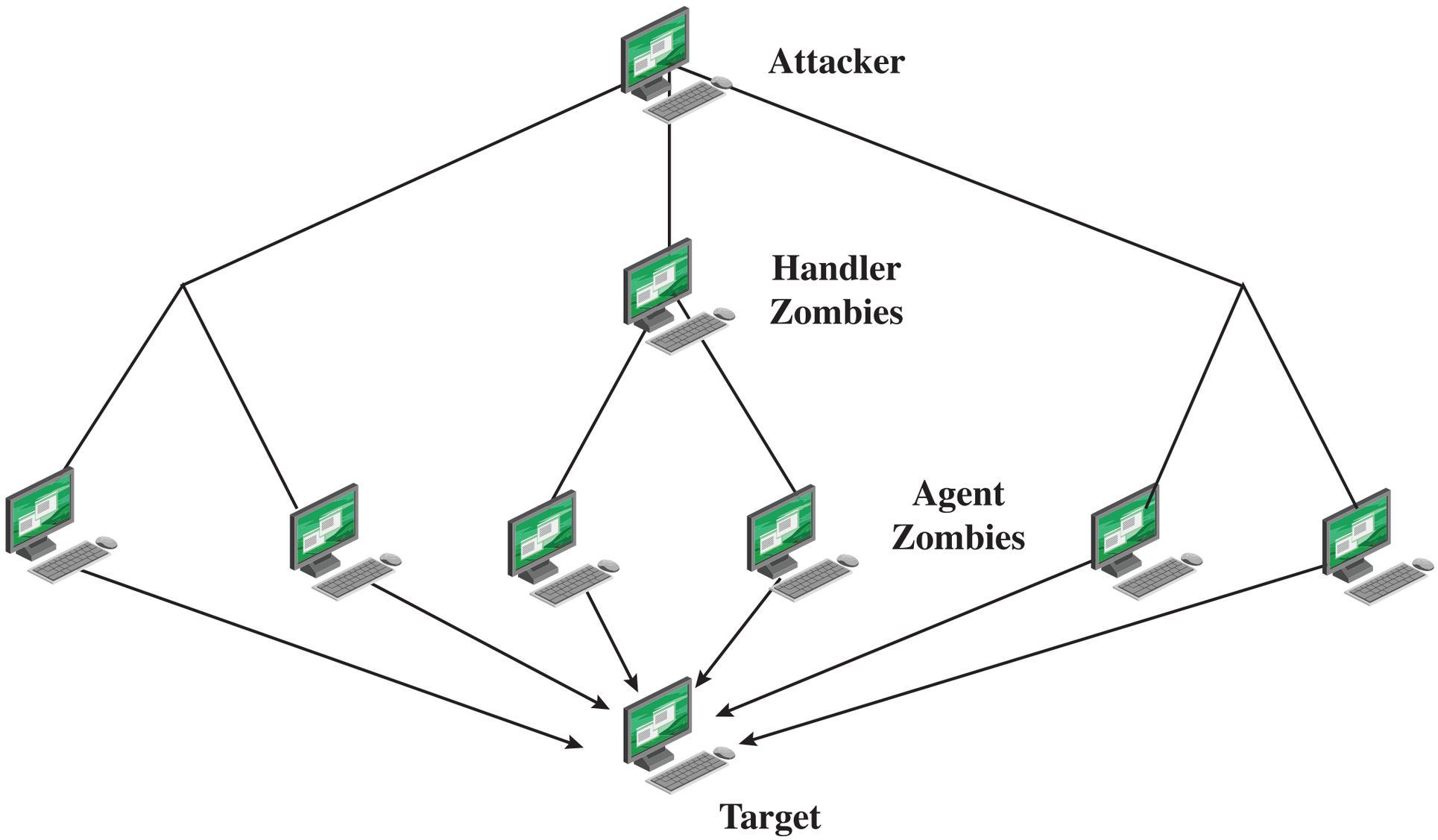
SYN spoofing :



Attaque par flooding

- ICMP flood
- UDP flood
- TCP SYN Flood

DDoS



DDos : Exemple

Recherche : Quels sont les mécanismes utilisés par l'outil DDoS Tribe Flood Network (et ses évolutions)

DoS applicatifs

Objectif : forcer la cible à exécuter des opérations couteuses en ressources, disproportionnées par rapport au coût de l'attaque

SIP Flood

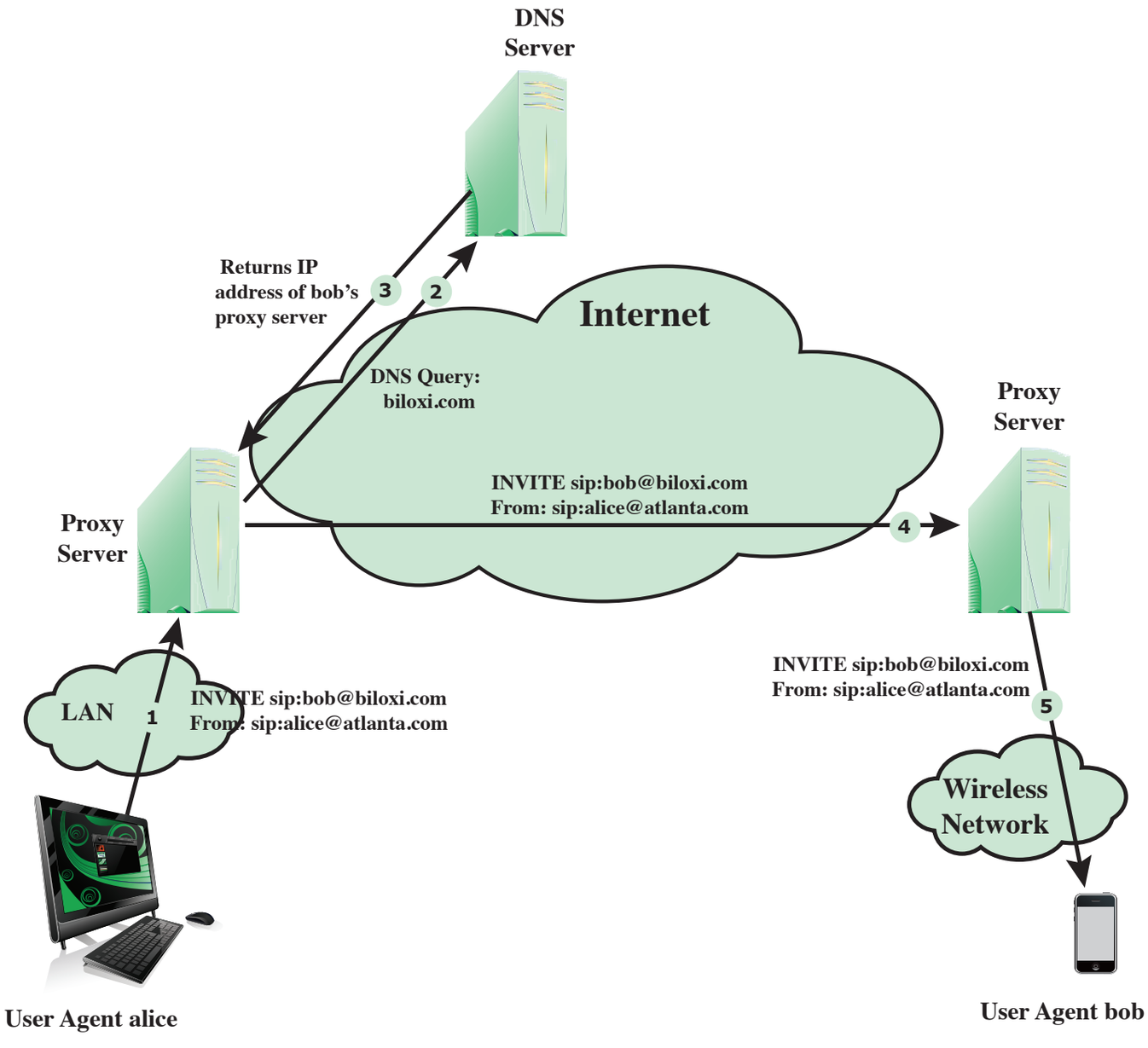


Figure 7.5 SIP INVITE Scenario

HTTP flood

- Requête pour de gros fichiers
- Recursive HTTP flood / spidering
- Slowloris

Réflexion et amplification

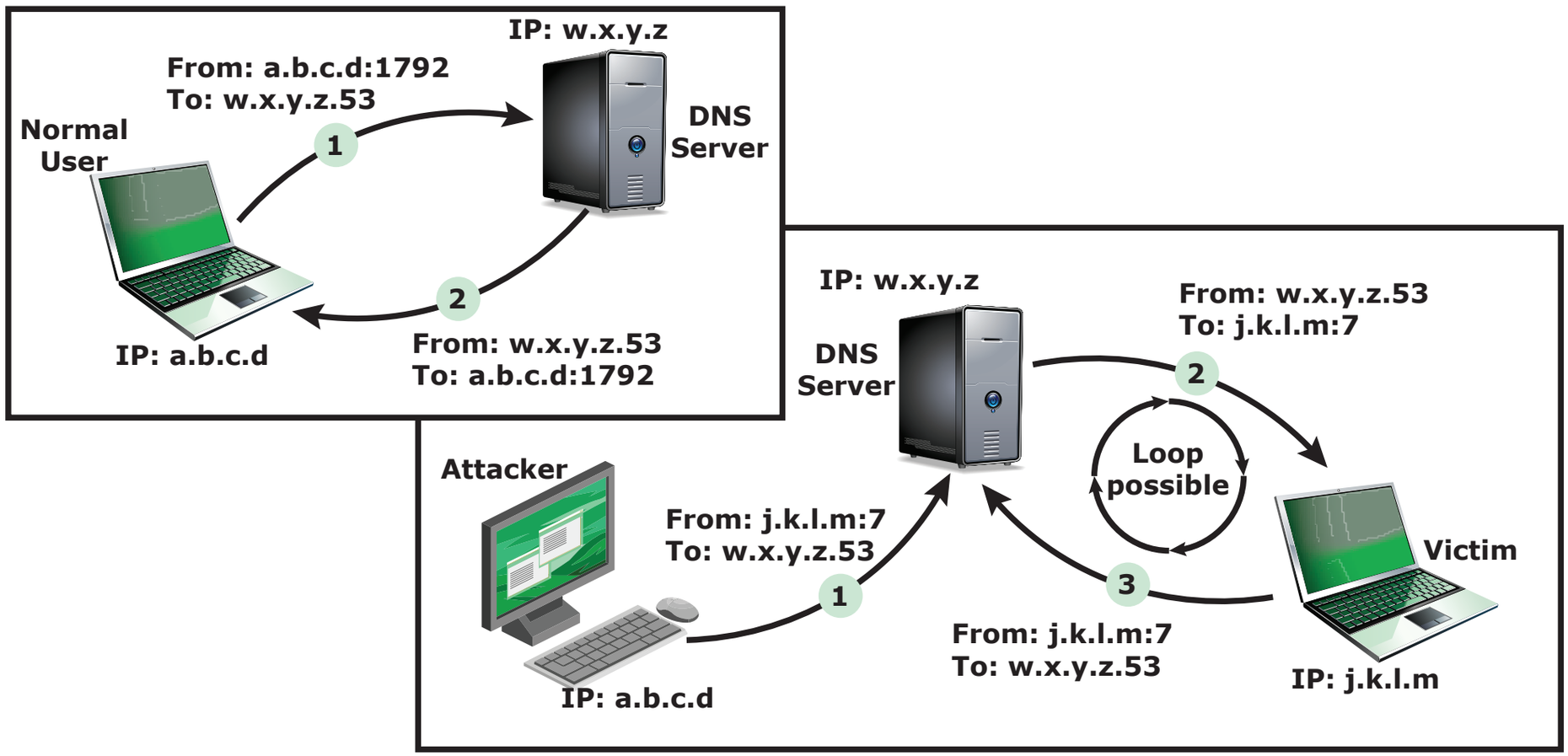
Principe : On n'utilise pas des intermédiaires compromis (botnets), mais des hôtes légitimes comme relais pour les attaques

=> Spoofing de l'adresse de la cible en tant qu'adresse source de paquets envoyés à des machines/serveurs légitimes

Attaques par réflexion

- Outils :
  - Service générant des réponses plus larges que les requêtes (Services UDP classiques : DNS, SNMP, NTP…)
  - Systèmes intermédiaires : Réseaux à large BW
    - Génération de larges volumes de trafic possible
    - Attaque dissimulée dans un large volume de trafic régulier

Attaque par réflexion DNS



Attaque par réflexion TCP/SYN

- Variante du SYN spoofing => SYN flood :
  - Envoi de paquets SYN avec l'adresse source de la cible au système intermédiaire
  - Le système intermédiaire renvoie des SYN +ACK à la cible
  - La cible est surchargée de paquets TCP

Attaques par réflexion

- : Très efficace
  Difficile de remonter à la source

+ : Facile à filtrer (combinaisons de ports improbables)

Attaques par amplification

- Variante de la réflexion : Une requête génère plusieurs réponses
  - Ex : Requête ping envoyée à une adresse de broadcast
- Ex : smurf, fraggle

Attaque par amplification DNS

- Principe : Générer une requête DNS dont la réponse sera de taille importante
  - Ex : requête de 60 octets, réponse = RR de 512 octets (en IPv6 : Max autorisé = 4ko!)
- Variante : Exploitation des requêtes récursives
- Prévention : Bloquer l'utilisation du spoofing d'adresse source, encore une fois!

Défense contre les DoS

- **Prévention** : Contrôle des ressources, backup, mécanismes structurels, …
- **Détection et filtrage** : Pour minimiser l'impact et y répondre rapidement
- **Traçage** de la source de l'attaque
- **Réaction** à l'attaque et restauration du service

Prévention

- Limitation du spoofing d'adresses source
- Limitation du taux d'acceptation de paquets d'un certain type (ICMP, UDP vers des services de diagnostic, …)
- SYN cookie, random drop sur la table des connexions TCP ou modification des paramètres de la table TCP (timeout, nombre de connexions, …)
- Blocage des broadcast entrant
- Attaques applicatives : Captcha, interactions avec l'utilisateurs…
- Prévention contre la compromission des systèmes! (zombies)

Réponse aux DoS

- Plan de réponse à l'incident!
  - Contacter l'ISP par un autre médium que le réseau
  - Répartition de la réaction entre l'ISP et la cible
- Monitoring du réseau et connaissance du pattern de trafic
- Identification de l'attaque et de la réponse appropriée => network analysis tools
- …