Sécurité des Systèmes d'Information

(Vulnérabilité, menace et attaque informatique)

Partie 3: attaque DOS/DDOS

université d'Alger 1 -
Benyoucef Benkhedda

Attaque DOS

Définition:

Denial of Service (Dénie de Service)

Une attaque réseau dont le but est d'arrêter un système, bloquer une connexion ou interdire l'accès à une ressources

Vise généralement des serveurs web

Simple exemple:

Possédant un ordinateur avec faible RAM (voir 1Go) et un système d'exploitation 64bits

Attaque DDOS

Définition:

Distributed Denial Of Service (Dénie de Service Distribué)

Une attaque DOS évoluée en utilisant un ensemble de machines comme sources d'attaque

Difficile à contrer par rapport au DOS

Utilise ce qu'on appel un ensemble de « Botnet »

Dit aussi « PC Zombie ». Est un ordinateur piraté et contrôlé par un attaquant en utilisant un cheval de Troie.

Méthodes d’attaque DOS/DDOS

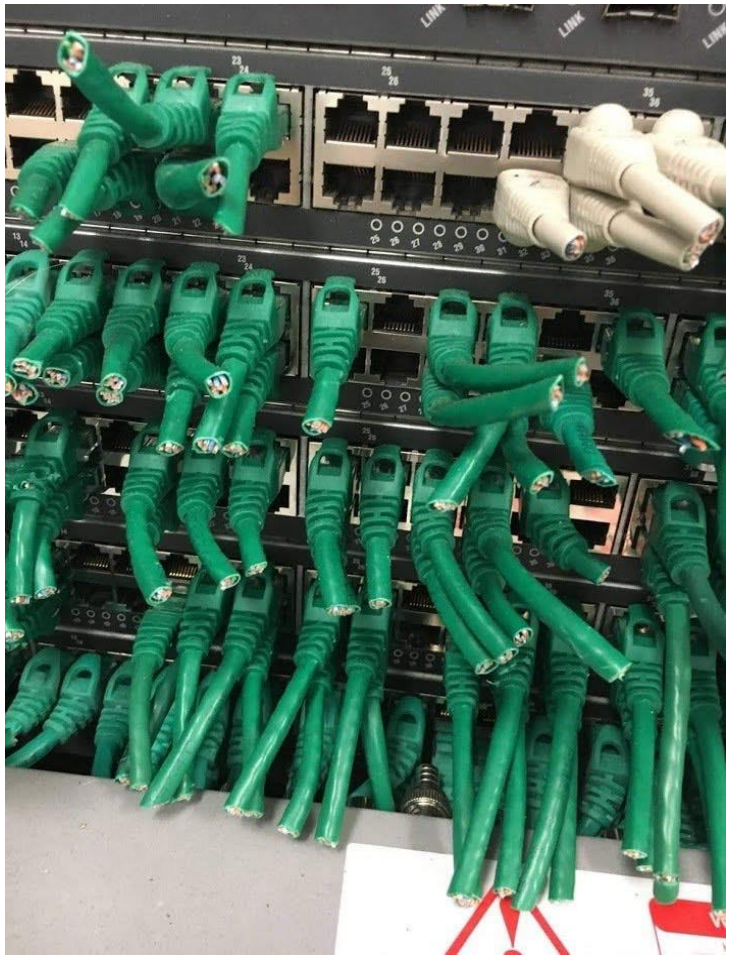
- Blocage du trafic réseau en inondant ce dernier par de nombreux paquets
- Blocage d’un serveur web en envoyant un nombre de requête plus qu’il peut traiter
- Blocage d’une machine en encombrant sa RAM principalement ou occupant d’autres ressources (espace disque, processeur…etc.)
- Changeant ou vidant la table de routage
- Retarder les tâche importante dans un système en occupant les ressources de calcul

Types d’attaque DOS/DDOS

Plusieurs types:

- Chacun réagisse sur un protocole web spécifique

- Parfois, DOS peut être physique
  - ➢ Un ingénieur malveillant coupe tous les câbles Ethernet liés aux différents switch dans la salle informatique



Types d’attaque DOS/DDOS

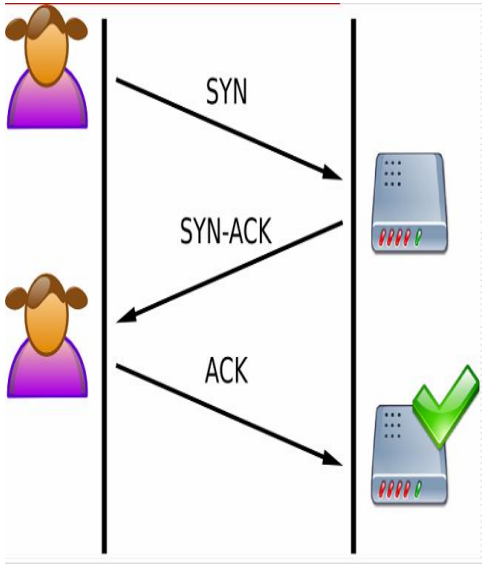
Plusieurs types:

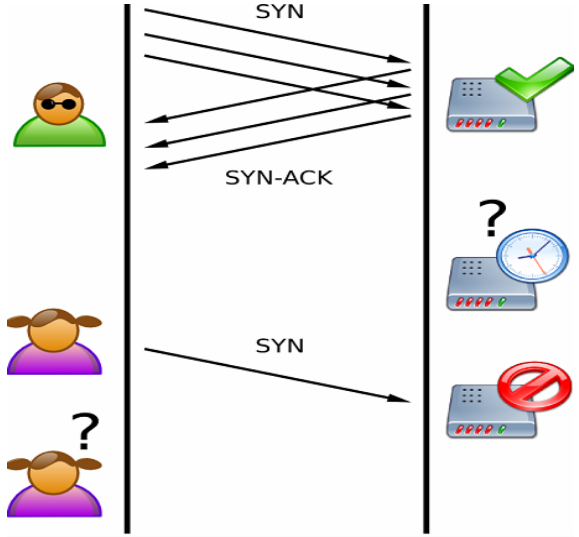
- **SYN flooding:**

Se base sur le protocole d’authentification « TCP Three Way Handshake »

Consiste à inonder le réseau par des paquets « SYN » sans répondre au paquet « SYN-ACK » venant des adresses IP falsifiées

Un nombre important des connexion en attente bloque le serveur en empêchant des connexions normales





Types d’attaque DOS/DDOS

Plusieurs types:

- **Smurfing :**

Se base sur le protocole ICMP

Consiste à installer un smurf via un compte volé afin de permettre l’envoie de plusieurs paquets « ping » via l’adresse broadcast dans un réseau => réseau encombré par les paquets

Utilise des adresses sources falsifiées

Types d’attaque DOS/DDOS

Plusieurs types:

- **LAND :**

Principe simple, forcer une machine à envoyer un nombre important de paquet SYN à elle-même. Par conséquence, la machine va répondre à tous les paquets jusqu’à crasher

- **FRAGGLE :**

Similaire à l’attaque smurfing

Utilise le protocole UDP pour envoyer un nombre important des paquets UDP à l’adresse broadcast.

Types d’attaque DOS/DDOS

Les attaques DDOS peuvent être assurés en utilisant certains outils.

Ces outils se basent en générale sur le modèle « master/slave » similaire au modèle « client/serveur ».

Un programme dite « master » permet de communiquer à plusieurs agents dites « slaves » afin de lancer plusieurs attaques DOS à la fois de plusieurs sources différentes parfois même appartenant à plusieurs réseaux différents.

Le réseau d’attaque est appelé « réseau de zombies »

Exemples: Trinoo, Tribal Flood Network (TFN), Stacheldraht…etc.

Quelques attaques connues (exemples)

- **MAFIABOY, faite par un garçon de 16 ans**
  - 7 Février 2000
  - CNN.com, Amazon, eBay, et Yahoo

- **ROOT DNS Server, faite par plusieurs attaquants**
  - 21 Octobre 2002
  - Tous les 13 DNS connus des serveurs à travers le monde

- **Estonia Cyberattack, faite par plusieurs attaquants**
  - Avril 2007, intérêt politique
  - Tous les serveurs de gouvernement, finance et media en ligne de l'Estonie

Quelques attaques connues (exemples)

- **Projet Chanology, faite par Anonymous**
  - Janvier 2008, réponse à suppression de vidéo de scientologie de Tom Cruise
  - Tous les serveurs de l'église de scientologie

- **L'opération Ababil, faite par le groupe Izz Ad-Dine Al-Qassam**
  - Décembre 2012 à Janvier 2013
  - Bank of America, Capitale One, Chase City Bank, PNC Bank, Wells Fargo et d'autres

- **MIRAI IoT botnet, faite par Anonymous**
  - Octobre 2016, réponse à suppression de vidéo de scientologie de Tom Cruise
  - Des sites web d'achat et social (airbnb, github,netflix, reddit, twitter,et autres)