LES ATTAQUES RÉSEAUX

SOURCES D'ATTAQUES « EXTERNES »

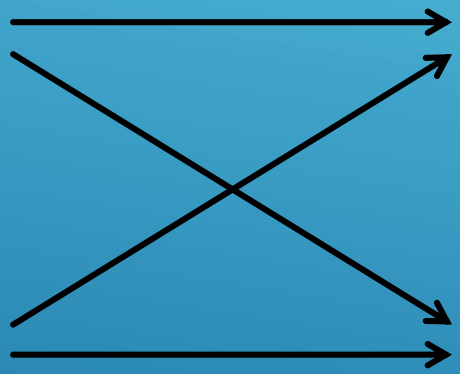
- **Intrusion via le réseau**
- **Diffusion de virus**
- **Elles sont médiatisées, connues**
- **Nécessites pare-feu, la surveillance du réseau, isolation des zones sensibles ...**

SOURCES D'ATTAQUES « INTERNES »

- **Le cas typique est l'employé pas content.**
- **Ce sont les plus efficaces.**
- **Lutte complexe.**
- **Employer des serveurs distincts.**

SOURCES D'ATTAQUES

- **Attaque externes**
- **Attaque internes**



- **Attaque non-structurées**
- **Attaque structurées**

TYPE D'ATTAQUES

- **Attaques de reconnaissance:**
  - **Scan des ports**
  - **Sniffer des paquets (Filaire ou Sans fil)**
  - **Analyse du trafic**
- **Attaques d'accès**
  - **Equipement**
  - **Logiciels**
- **Dénie de service (DoS)**
  - **Disponibilité**
- **Virus, vers & chevaux de trois**
  - **Les plus connus (attaque les OS)**
- **Les attaques physiques**
  - **Vole, endommagement de matériel, coupure de câbles …**

MÉTHODES UTILISÉES

Écoute :

- **Écoute passive et clandestine sur le réseau dans le but de récupérer des informations.**
- **Exemples d'attaques : analyseurs de réseau, sondes …**

Intrusion :

- **exploitation des vulnérabilités du système pour exécuter des commandes non autorisées.**
- **Exemples d'attaques : exploitation des erreurs de configuration(Satan, Cops), exploitation des bugs : Network Scanning, Sendmail, INN …**

Abus de droits légitimes :

- **Utilisation d'une fonctionnalité du système de façon abusive.**
- **Exemples d'attaques : diffusions de logiciels sur des comptes ftp anonymes, trop de requêtes pour saturer un serveur, sniffer des ports.**

Action physique :

- **Destruction, altération ou changement physique d'un composant.**
- **Exemples d'attaques : destruction d'un câble, débranchement d'une prise électrique…**

Usurpation d'identité :

- **Utilisation d'une fausse identité pour abuser un système ou un utilisateur.**
- **Exemples d'attaques : changer d'adresse IP pour tromper le système : IP spoofing…**

Injection de code :

- **Installation et exécution d'un module clandestin sur un système.**
- **Exemples d'attaques : virus, bombes logiques, cheval de Troie, cookies, ver…**

CLASSIFICATION DES ATTAQUES *(ATTAQUES PASSIVES)*

Ne modifient pas le comportement du système, et peuvent ainsi passer inaperçues.

- ***Attaques sur la confidentialité :***
  - **Objectifs : obtention d'informations sur un système, sur un utilisateur ou un projet.**
- **Méthodes possibles :**
  - **Ecoute**
  - **Injection de code**
  - **Usurpation d'identité**
  - **Intrusion**
  - **Abus de droits**

CLASSIFICATION DES ATTAQUES *(ATTAQUES ACTIVES)*

Modifient le contenu des informations du système ou le comportement du système. Elles sont en général plus critique que les passives. Exemple:

- ***Attaques sur l'intégrité :***

  Objectifs : modification ou destruction de données ou de configurations.

  Méthodes possibles :

  - **Injection de code**
  - **Action physique**
  - **Intrusion**

- ***Attaques sur la disponibilité :***

  Objectifs : perturbation d'un échange par le réseau, d'un service ou d'un accès à un service.

  Méthodes possibles :

  - **Abus de droits**
  - **Action physique**
  - **Intrusion**

EXEMPLE D'ATTAQUES DE RECONNAISSANCE

PORT SCAN *(EXEMPLES)*

- Exemple de site Web
- **Extensions de navigateur :**
  - **Wappalizer (détection des outils utilisé pour le développement d'un site web)**
  - **LightBeam (Ce n'est un outil d'attaque, mais vous permet de démasquer les sites tierces qui espionnes vos activités sur le web : Tracking)**
- **Logiciels:**
  - Advanced IP Scanner
  - Look@LAN
  - NMAP (avancé)

ANALYSEUR DE TRAFIQUE *(EXEMPLES)*

- **Wireshark : *www.wireshark.org***
- **tcpDump : *www.tcpdump.org***
- **…**

ATTAQUES D'ACCÈS

ATTAQUE PHYSIQUE

- **Accès physique au équipements**
  - **Destruction (disponibilité)**
  - **Vole de HDD (Confidentialité)**
- **Utilisation des drones**
- **Utilisation des caméras cachées**
- **…**

LES ATTAQUES PAR PROTOCOLE

- **IP Spoofing**
- **TCP-SYN/Flooding**
- **Attaque par le protocole RIP**
- **Attaque par requêtes ARP**
- **Attaques ICMP**
- **Attaques par fragmentation**
- **Attaques UDP**
- **Attaques par inondation de messages**
- **Attaque par débordement de tampon**
- **…**

LES PARASITES

- **Les virus**
- **Les vers**
- **Trojans (chevaux de Troie)**

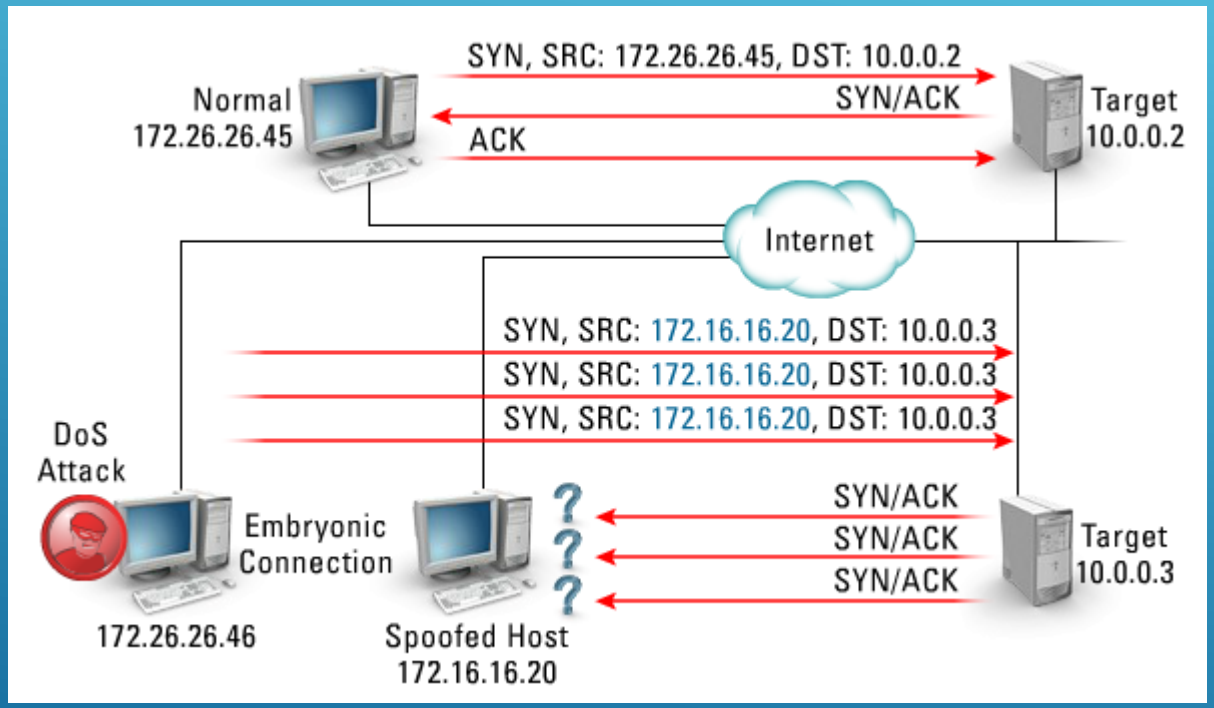
EXEMPLES D'ATTAQUES

TCP-SYN/FLOODING 1 (DOS)

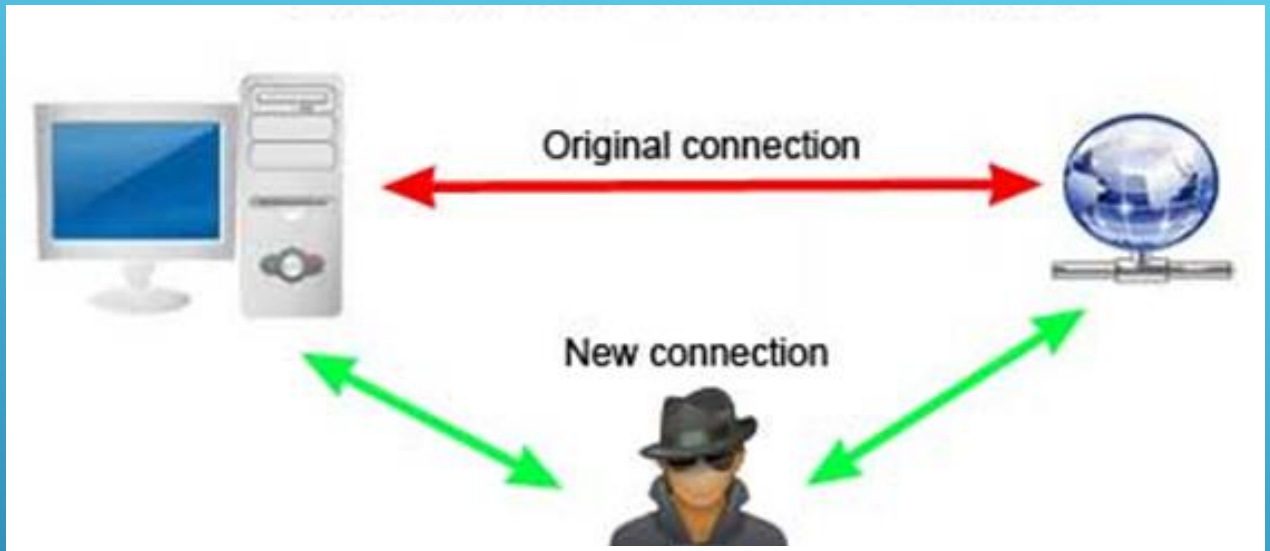
- **Etablissement d'une connexion TCP entre client/serveur :**
  - **Connexion incomplète**
  - **Backlog: longueur de la file d'attente SYN.**
  - **Timeout? ➔ envoyer des paquets plus vite que le temps d'expiation**
  - **La <u>localisation de l'attaque</u> ?**

➔ **complexe car les adresses contenues dans les paquets SYN envoyés sont falsifiées**

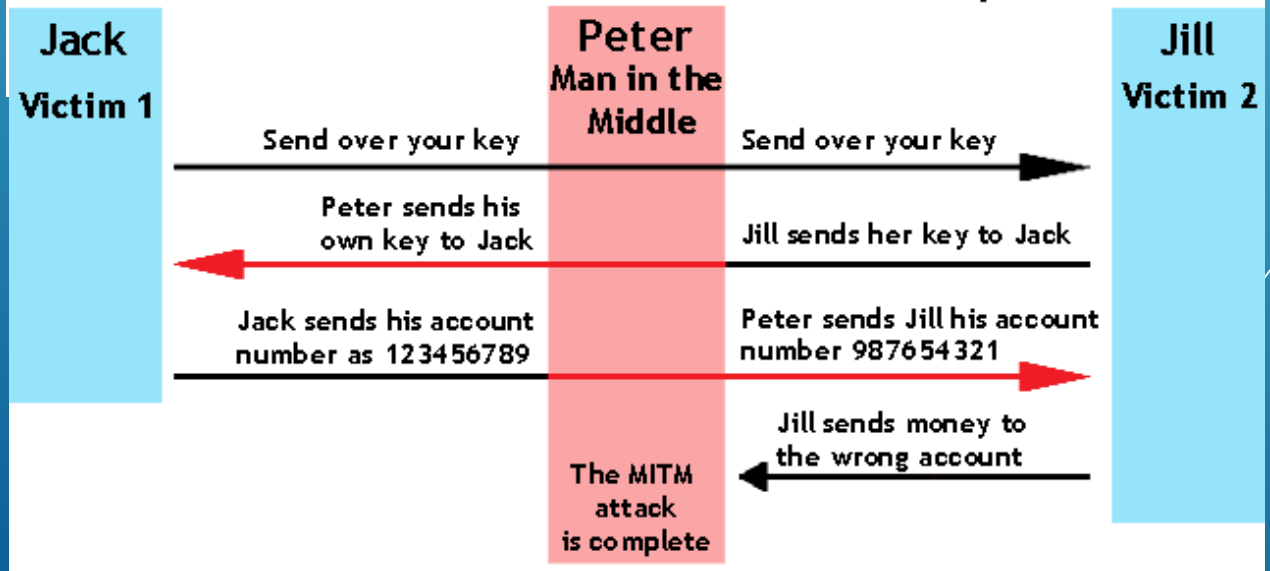
TCP-SYN/FLOODING 2 (DOS)



MAN IN THE MIDDLE



Man-in-the-Middle Attack Example



QUELQUES PRINCIPAUX ACTES CYBERCRIMINELS RECENSÉS EN 2015

- **30/09/2015 : Les sites Web du gouvernement thaïlandais attaqués**
- **12/09/2015 : Cyberattaque contre le site officiel de la Commission électorale centrale (CEC) de Russie**
- **05/08/2015 : La SNCB victime d'un piratage**
- **25/07/2015 : Le Pentagone visé par une cyber-attaque russe**
- **28/07/2015 : Les e-mails de hauts gradés de l'armée américaine piratés**
- **18/07/2015 : Piratage du site de rencontres adultères Ashley Madison**
- **06/07/2015 : Hacking Team, société d'espionnage informatoque hacké**
- **19/05/2015 : Un hacker a modifié en vol la puissance d'un réacteur**
- **14/05/2015 : Un ordinateur de Merkel touché par la cyberattaque contre le Bundestag**
- **14/05/2015 : Des hôtels suisses victimes d'un piratage informatique**
- **12/05/2015 : Kaspersky annonce être victime d'une Cyberattaque**
- **05/05/2015 : Arnaque aux faux virement : Vol de 15 millions d'euros à Intermarché**
- **29/04/2015 : Des pirates informatiques volent 5 millions de dollars à Ryanair**
- **10/04/2015 : Lufthansa victime d'une cyberattaque**
- **05/05/2015 : Les états -Unis (Office of Personnal Management) victime de piratage. Plus de 4 millions de données personnelles de personnels fédéraux piratées;**
- **09/04/2015 : Arte victime d'une attaque informatique**
- **08/04/2015 : La chaîne TV5 Monde victime d'un piratage de grande ampleur par des individus se réclamant du groupe Etat Islamique | Le Net Expert Informatique**
- **02/2015 : Thales aurait été la cible d'une cyberattaque**
- **02/01/2015 : Les données de deux millions d'abonnés du site de TF1 ont été piratées. Les hackers détiennent les RIB et autres informations sensibles de ces internautes.**

Source : ici

MINI-PROJETS

- **Attaques par protocole.**
- **DoS et DDoS**
- **Attaques sur les systèmes/services/Applications/cloud**
- **Attaques sur l'authentification**
- **Parasites : virus, vers, Trojans (chevaux de Troie)**
- **Ransomwares**
- **L'ingénierie Sociale**
- **Attaques sur les objets connectés**
- **…**