Université de M'sila
Faculté des Mathématiques et de l'Informatique
Département d'informatique
Spécialité: Master RTIC

Attaques Réseaux

Université de M'sila
Département d'informatique:2020-2021
Niveau : master2
Préparé et présenté par: SAOUDI Lalia

Attaque Informatique

- Une attaque peut être définit comme toute action ou ensemble d'actions qui peut porter atteinte la sécurité des informations d'un système ou d'un réseau informatique.

Objectifs des attaques

- Désinformer
- Empêcher l'accès à une ressource
- Prendre le contrôle d'une ressource
- Récupérer de l'information présente sur le système
- Constituer un réseau de « botnet » (ou réseau de machines zombies

Faut-il apprendre les attaques?
من تعلم لغة قوم أمن شرهم

- avant de sécuriser un système, il faut faire des tests de pénétration (appelés Pen-Test) pour cibler les failles…
- De plus pour contrer efficacement une personne, il faut soit penser comme elle, soit connaître ses limites.
- En gros pour sécuriser un système, il faut se mettre à la place d'un pirate.

Les hackers

- Mais alors qui sont ces hackers ? et comment s'organisent-ils ?
- 1- les newbies (débutants) : ce sont généralement des adolescents fascinés par les exploits de certains hackers.
- **2- les Whites Hat Hackers**: des élites en hacking qui programment à longueur de journée et ne font que rechercher des failles dans les systèmes, logiciels…
- **3- les Blacks Hat Hackers:** des élites qui préfèrent détruire tout
- système qui leur tombent sous la main.
- **4-les crackers :** ce sont des personnes piratant les logiciels payants de façon à pouvoir les utiliser indéfiniment sans dépenser d'argent.
- **les hacktivistes :** ce sont des hackers utilisant leurs connaissances pour défendre ce en quoi il pensent et se battre pour un but (les droits de l'homme, la non commercialisation de l'Internet…).

Les « botnets »
(réseau de machines zombies)

- Réseau de machines contrôlées par un « bot herder » ou « botmaster ».
- Un quart des ordinateurs du monde, dont, probablement, le vôtre, serait compromis à l'insu de leurs propriétaires, et exploités par des cybercriminels qui les regrouppent pour former de puissants réseaux d'attaques.
- " Bot " est un raccourci pour " Robot " et désigne l'agent logiciel implanté (le parasite).
- " Net " signifie " réseau " en anglais.
- " Botnet " est l'ensemble, actif à un instant, de tous les exemplaires d'un agent logiciel donné, constituant un réseau communiquant.
- " Zombie " est un terme qualifiant un ordinateur compromis car il n'est plus sous le contrôle de son propriétaire mais sous celui d'un tiers inconnu à cause de l'agent logiciel (le virus, le malware) implanté.

Cible des pirates

- Les états
- Serveurs militaires
- Banques
- Universités
- Tout le monde

II.Classification des attaques

- *II.1- Interne- externe:*
- Un système informatique peut être attaqué soit par un utilisateur interne , soit par un utilisateur externe.

II.2ème classification

C’est la classification la plus classique, elle regroupe quatre types d’attaques. Ainsi une attaque peut porter atteinte à :

- la ***confidentialité des informations:*** *en brisant des règles privées,*
- l’***intégrité,*** *en altérant les données,*
- l’***authenticité des données,***
- la ***disponibilité,*** *en rendant un système ou réseau informatique indisponible. On* parle alors d’attaque de ***déni de service***

II.3ème classification

les attaques passives / les attaques actives.

1. ***Les attaques passives*** regroupent les attaques portant atteinte à la confidentialité. Il en existe deux types :

• la lecture de contenus de messages confidentiels : courrier électronique, fichier transféré ;

• l'analyse de trafic pour déterminer la nature d'une communication : identité des "hosts" communiquant, fréquence et longueur des messages échangés.

Les attaques passives ne sont pas facilement détectables car elles n'impliquent aucune altération des informations.

2. Les attaques actives concernent celles qui entraînent une modification des données ou création de données incorrectes. Autrement dit, celles qui portent atteinte à l'intégrité, l'authenticité et la disponibilité. On retrouve alors quatre types d'attaques actives :

• l'usurpation : c'est lorsqu'une entité se fait passer pour une autre,

• le rejeu : retransmission de messages capturés lors d'une communications, et cela à des fins illégitimes,

• la modification de messages,

• le déni de service.

II.4 4ème classification

Attaques réseaux / Attaques système

- ***attaques réseaux*** *: leur but principal est d'empêcher les utilisateurs d'utiliser* une connexion réseau, de rendre indisponible un service et de surveiller le trafic réseau dans le but de l'analyser et d'en récupérer des informations pertinentes.
- ***attaques systèmes :*** *ce sont des attaques qui portent atteinte au système, comme* par exemple effacer des fichiers critiques (tel que le fichier "password") ou modifier la page web d'un site dans le but de le discréditer ou tout simplement le ridiculiser.

Attaques Réseaux: Méthodologie d'une attaque

- Nous ne connaissons rien sur le système cible, ni l'architecture, ni les services, ni l'organisme.
- 1-Collecte des informations:
- 2-Repérage de failles.
- 3- Intrusion
- 4-Exploitation

1. Attaques permettant d'écouter le trafic réseau

- Cette technique est généralement utilisée par les pirates pour capturer les mots de passe.
- Lorsqu'on se connecte à un réseau qui utilise le mode broadcast, toutes les données en transit arrivent à toutes les cartes réseau connectées à ce réseau.
- En temps normal, seules les trames destinées à la machine sont lues, les autres étant ignorées.

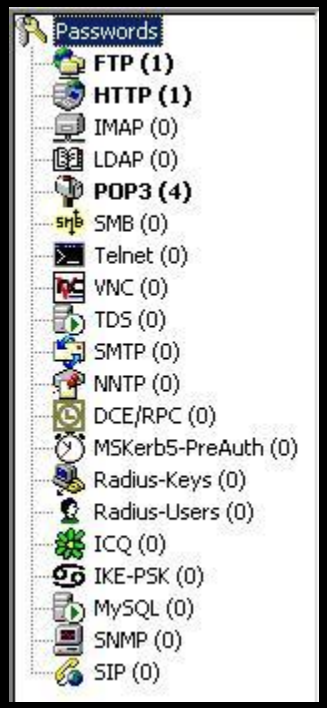
Attaque par sniffing

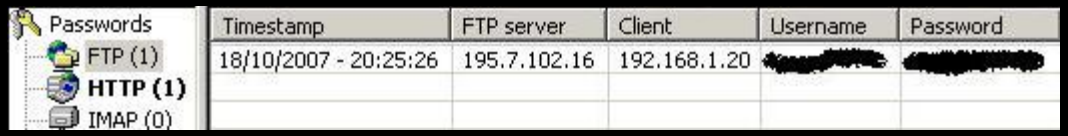
- **Définition**: Les sniffers réseau sont très souvent utilisés par les administrateurs réseau pour capturer le trafic à des fins d'archives (pour une analyse future) ou d'analyse de problèmes. Mais ces outils sont également utilisés par des pirates à des fins bien moins éthiques, comme le vol de mot de passe .

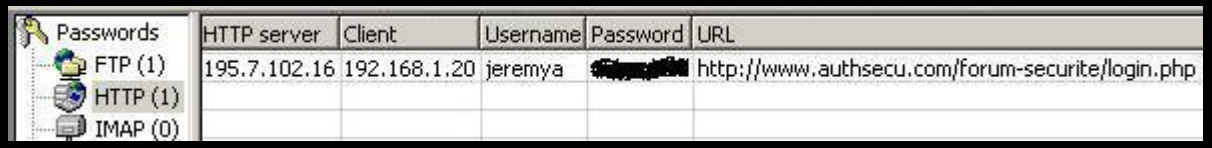
- Le système pirate se situe sur le réseau local et capture tous les paquets réseau transitant sur ce réseau afin d'obtenir des mots de passe, etc.

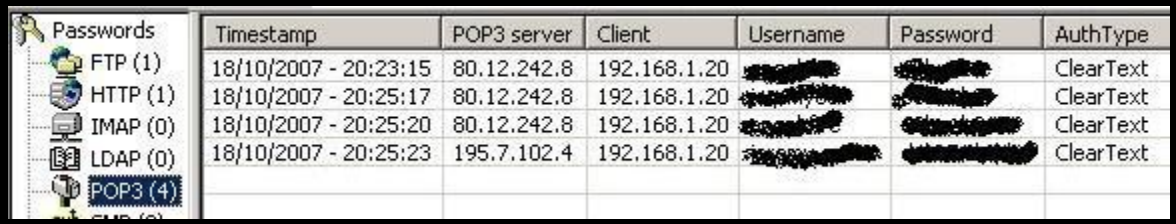
- Grâce à des outils tels qu'Ethereal ou WinDump/TCPDump, le sniffer peut analyser tous les paquets IP ainsi que les protocoles contenus dans les données du paquet.
- En revanche, lorsque le réseau s'appuie sur une étoile commutée,(switch) les choses deviennent un peu plus difficiles.

Exemple:cain









Attaque par sniffing

- **1- Wireshark**
  Wireshark (anciennement Ethereal) est un logiciel libre d'analyse de protocole, ou « packet sniffer » sous linux et windows, utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro-ingénierie, mais aussi le piratage.

Attaque par sniffing

- **2 Kismet**
- Kismet est un logiciel libre de détection de réseaux, un sniffeur, et un système de détection d'intrusion pour réseau sans fil 802.11. Kismet fonctionne avec les cartes réseau qui supportent le mode moniteur, et tout protocole 802.11 (802.11a, 802.11b, 802.11g et 802.11n)

Attaque par sniffing

- **3- TCPdump**

  tcpdump est un sniffer de Paquets en ligne de commande. Il permet d'obtenir le détail du trafic visible depuis une interface réseau.
  C'est un outil de mise au point apprécié pour sa puissance ; les nombreuses informations qu'il faut trier conduisent à utiliser le filtre BPF.

Attaque par sniffing

- **4 Cain et Abel**

  Cain & Abel est un outil gratuit de récupération de mot de passe fonctionnant sous Windows. Il permet la récupération facile de divers genres de mots de passe en sniffant le réseau, cassant des mots de passe hachés en utilisant des attaques par dictionnaire, par recherche exhaustive ou encore via des tables arc-en-ciel. Son code source n'est pas fourni.

Attaque par sniffing

- **5 Ettercap**

  Ettercap est un logiciel libre d'analyse du réseau informatique. Il est capable d'intercepter le trafic sur un segment réseau, de capturer les mots de passe, et de réaliser des attaques dites de l'homme du milieu (Man In The Middle) contre un certain nombre de protocoles de communication usuels tels que HTTP, FTP et certains protocoles chiffrés.

2 Attaque d'un commutateur

- le commutateur gère une table dynamique des adresses MAC physiques des machines situées sur chaque port. Lorsque la donnée part d'une machine A vers une machine B, le commutateur reçoit en fait un paquet destiné à une adresse MAC particulière.
- Un intrus branché sur un commutateur ne doit voir que :
  - les données qui sont destinées à une machine branchée sur le même port que lui, donc lui-même ou une autre s'il est branché sur un répéteur branché au commutateur ;
  - les données envoyées sous forme de broadcast ou multicast. Dans ce cas, le commutateur envoie les données à tous les ports hébergeant des machines.

2 Attaque d'un commutateur

a-Le switch jamming

- **Saturation de la mémoire d'un switch**
- Pour router le trafic, les switches maintiennent une table de correspondance appelée Content Adressable Memory (CAM). Il est possible d'exploiter un dépassement de mémoire de certains équipements en saturant la table d'adresses MAC, afin de capturer les paquets.
- lorsque la mémoire est pleine, certains switches se comportent en hubs et envoient les paquets à tous les hôtes connectés.

Attaque d'un commutateur

b- La reconfiguration du port moniteur/SPAN

- La plupart des commutateurs permettent à des ports d'être configurés en tant que port moniteur (ou SPAN) et de copier une partie ou la totalité du trafic transitant par le commutateur, dans un but d'administration.
- ces ports sont conçus pour exécuter des sniffers de paquets lorsque l'administrateur réseau doit résoudre un problème.

- Beaucoup de commutateurs sont installés par défaut. Un intrus peut donc faire un Telnet sur le commutateur ou le reconfigurer avec le protocole SNMP, dans le but d'assigner ce type de port au numéro de port sur lequel le pirate est branché.

C- La manipulation des tables de commutation (les tables CAM)

- Le principe est simple : envoyer une trame avec pour adresse source MAC l'adresse MAC de la victime. Ou encore plus simple : changer sa propre adresse MAC en l'adresse MAC de la victime avant de se connecter au switch.
- cette technique est très limitée. D'abord parce que la victime émet encore des paquets, ce qui place le commutateur face à un conflit .

- Cette technique est donc inutilisable pour écouter une connexion entre deux hôtes. Mais, elle est très intéressante dans le cas d'une attaque de déni de service - La machine victime ne pourra plus communiquer avec le réseau- .

3. Spoofing (mystification)

- Définition: le spoofing est une attaque d'usurpation d'identité, lorsqu'une machine se présente comme étant une autre.
- Spoofing des adresses MAC
  - Modification de l'adresse MAC de la carte réseau
  - Difficile d'être capturé.

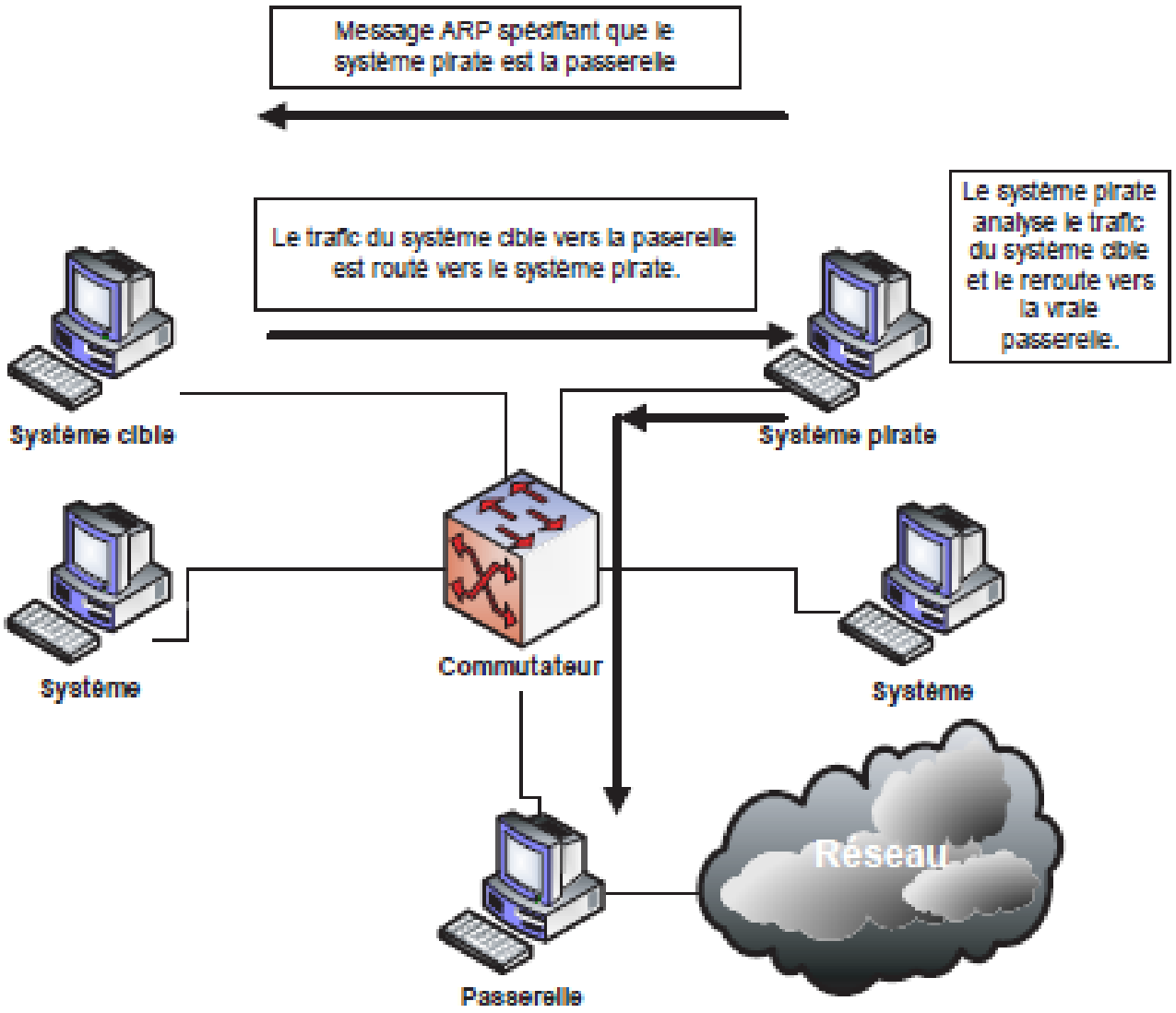
3.1 ARP Spoofing (mystification)

- l’attaque ARP spoofing s’appuie sur le protocole ARP(Address Resolution Protocol), qui implémente le mécanisme de résolution d’une adresse IP (32 bits) en une adresse MAC (48 bits) pour rediriger le trafic réseau de un ou plusieurs systèmes vers le système pirate.
- Lorsqu’un système désire communiquer avec ses voisins sur un même réseau (incluant la passerelle d’accès à d’autres réseaux), des messages ARP sont envoyés afin de connaître l’adresse MAC des systèmes voisins et d’établir ainsi une communication avec un système donné.

3.1 ARP Spoofing (mystification)

- Sachant que chaque système possède localement une table de correspondance entre les adresses IP et MAC des systèmes voisins.
- ARP permet à un système pirate d'envoyer des paquets ARP réponse au système cible indiquant que la nouvelle adresse MAC correspondant à l'adresse IP d'une passerelle est la sienne.
- Le système du pirate reçoit donc tout le trafic à destination de la passerelle. Il lui suffit d'écouter ou de modifier passivement le trafic et de router ensuite les paquets vers leur véritable destination, comme l'illustre la figure

3.1 ARP Spoofing (mystification)



3.2 *Attaque IP spoofing*

- La plupart des moyens d'authentification s'appuyant de nos jours sur les adresses IP, ce moyen faible d'authentification peut entraîner de graves problèmes de sécurité si l'authentification ne recourt qu'à ce mécanisme.
- Si un système peut donner des privilèges particuliers à un ensemble d'adresses IP sources, un paquet IP forgé avec une telle adresse IP est reçu par ce système avec les privilèges associés.
- L'attaque IP spoofing consiste à se faire passer pour un autre système en falsifiant son adresse IP.
- Le pirate commence par choisir le système qu'il veut attaquer. Après avoir obtenu le maximum de détails sur ce système cible, il détermine les systèmes ou adresses IP autorisés à se connecter au système cible

3.2 *Attaque IP spoofing*

- Ce type d’attaque s’utilise de deux manières différentes :
  - La première utilité de l'IP Spoofing est la falsification de la source d'une attaque, lors d'une attaque de type déni de service.
  - La seconde utilisation de l'IP Spoofing permet de profiter d'une relation de confiance entre deux machines pour prendre la main sur l'une des deux

Questions de cours6

- Q1:Pourquoi attaquer un réseau informatique?
- Q2: Faut-il apprendre les attaques?
- Q3: Qu'est ce qu’un bot net?
- Q4: Donner les différentes classification des attaques
- Q5: Expliquer le sniffing
- Q6: Comment attaquer un switch
- Q7: Pourquoi les attaquants font le spoofing dans leurs attaques (IP spoofing ou ARP spoofing)