Les attaques

De qui se protéger

Une attaque est une menace réalisée par des gens :

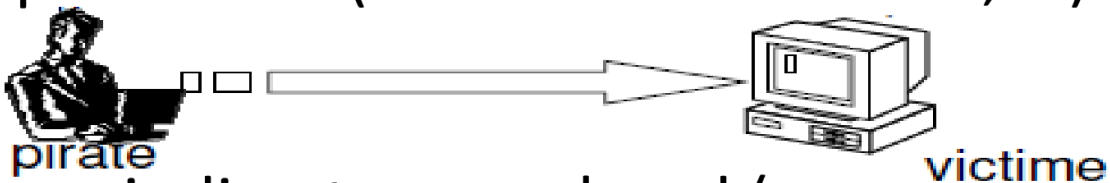
- **Pirates informatiques « Hackers »** : qui s'amusent d'accéder à des systèmes d'info d'autres personnes. Certains se contentent simplement de laisser leur « empreinte ». D'autres appelés « braqueurs » mettent en panne les systèmes, volent ou endommagent les données ou interrompent l'activité.
- **Personnel non avisé** : être involontairement la source des failles de sécurité (contamination par virus, installation des logiciels, …)
- **Utilisateurs mécontents** : abusent de leur droit et causent l'endommagement de certains services.

Méthode d'attaque

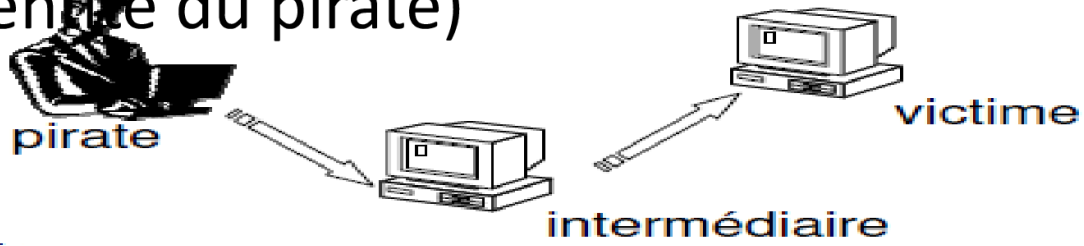
- 1. Recherche de la machine par : ping, …
- 2. Déterminer les nœuds intermédiaires : traceroute, ..
- 3. Recherche des services actifs : TCP SCAN, SYN SCAN, UDP SCAN
- 4. Identification des machines et des logiciels, champ ID, Stack finger print, obtention de la version et de la configuration des logiciels, obtention d'informations via les services accessibles.
- 5. Tentative d'exploitations des vulnérabilités : débordement du buffer, attaques sur les services web, chevaux de trois ….
- 6. Attaque de la cible

Types d'attaques

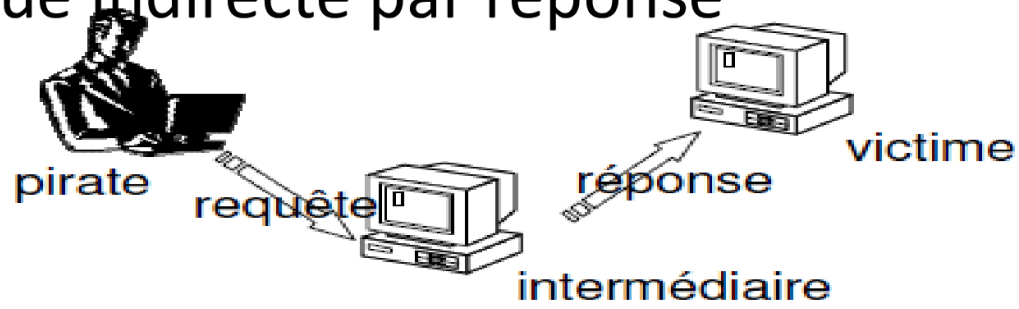
- Attaque directe (commandes directes, …)



- Attaque indirecte par rebond (masque l'identité du pirate)

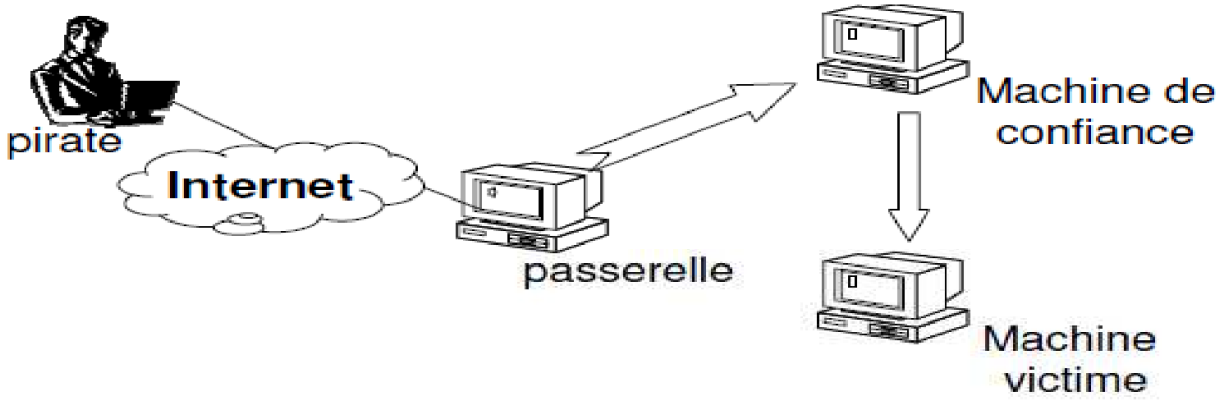


- Attaque indirecte par réponse



Vulnérabilités courantes

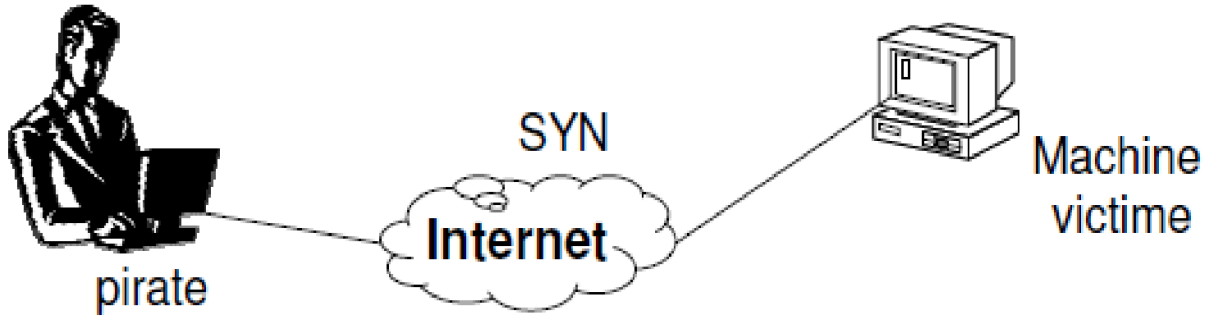
- Protocole TCP/IP



- **IPSpoofing** : établissement d'une communication avec la machine victime en se faisant passer pour la machine de confiance (en créant un message truqué contenant artificiellement l'adresse source de la machine de confiance)

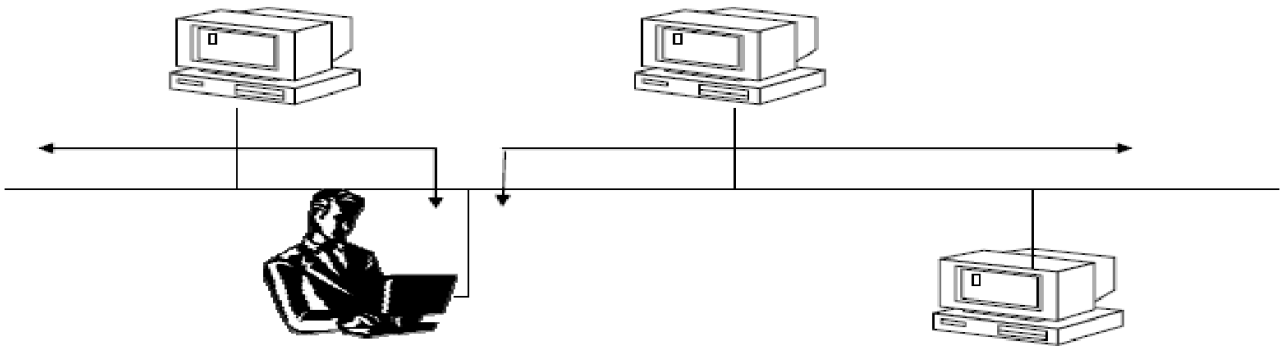
SYN flooding

envoie d'un paquet TCP avec le flag SYN armé semblant venir d'une machine non accessible, éteinte ou inexistante. La machine victime envoie donc le second paquet pour l'ouverture de la connexion et attend la réponse de la machine non accessible, qui ne viendra jamais. (monopolisation de la connexion)

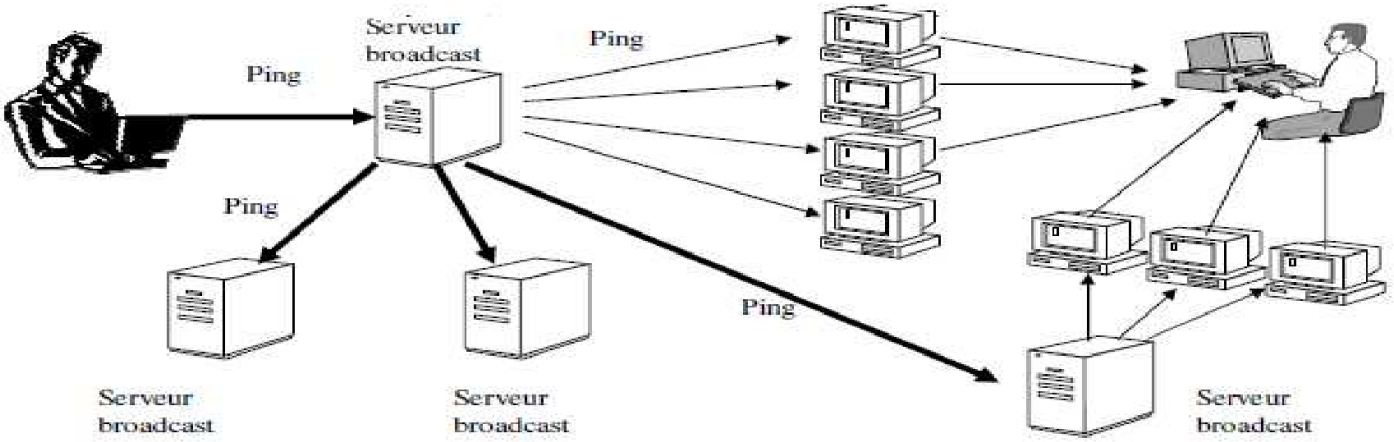


Snifing

- Le reniflement (Snifing) : capturer toutes les informations provenant des machines du réseau passant par la machine en question. Il permet d'analyser le trafic pour obtenir des mots de passe et des données sensibles.



Protocole ICMP: ping



Attaque par réflexion (Smurfing) : (1) récupération de l'adresse IP de la cible par spoofing ; (2) envoi d'un ping à plusieurs serveurs broadcast en changeant l'adresse source par celui de la machine victime ; (3) Les serveurs broadcast s'adressent à toutes les machines de leurs réseaux ; (4) La machine victime va recevoir autant de réponses au ping qu'il y a de machines sur les réseaux des serveurs broadcast et finira par perdre toute sa bande

Protocole UDP:UDP Flood

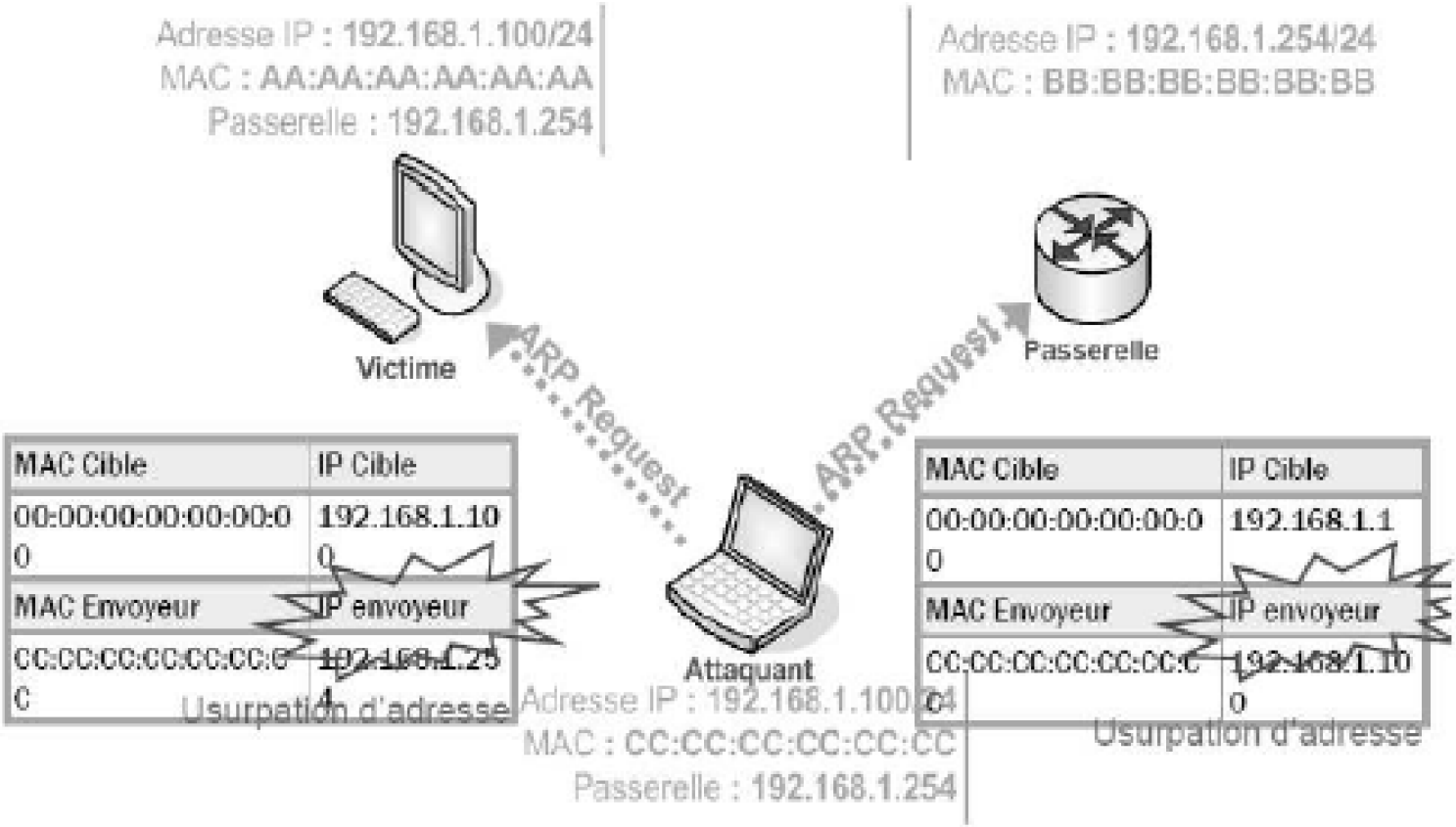
de la même manière que pour le SYN Flooding, l'attaquant envoie un grand nombre de requête UDP sur une machine.

Le trafic UDP étant prioritaire sur le trafic TCP. Ce type d'attaque peut rapidement troubler et saturer le trafic transitant sur le réseau.

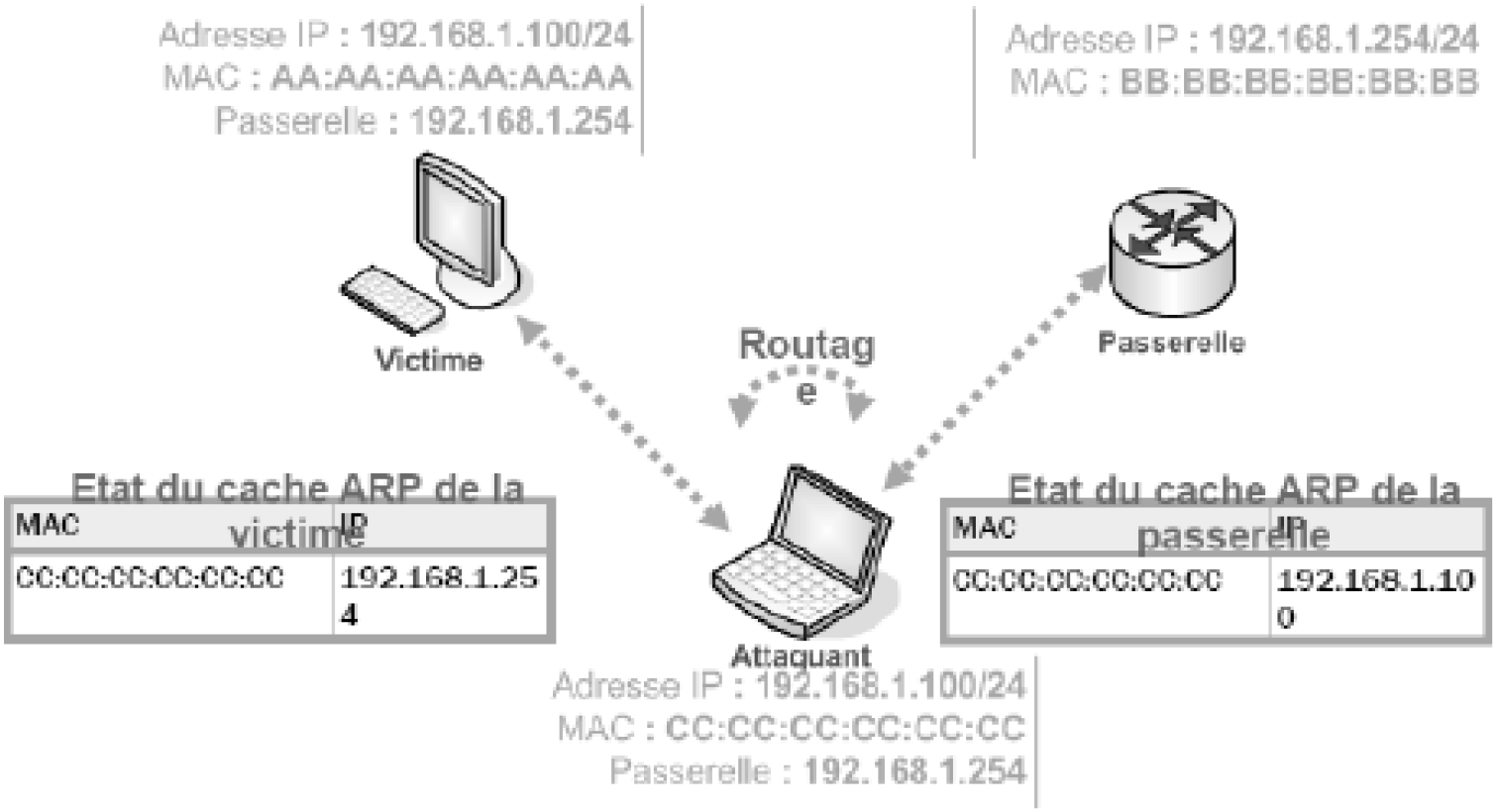
Protocole ARP: Spoofing ARP

consiste à s'attribuer l'@ IP de la machine cible, en faisant correspondre son @ IP à l'@ MAC de la machine pirate dans les tables ARP des machines du réseau. (envoi régulier des paquets ARP_reply en broadcast, contenant l'@ IP cible et la fausse adresse MAC. Cela a pour effet de modifier les tables dynamiques de toutes les machines du réseau. Celles-ci enverront donc leur trames Ethernet à la machine pirate tout en croyant communiquer avec la cible

ARP Poisoning



ARP Poisoning+ routage



Service messagerie: SMTP

- **Le Mail Bombing** : consiste à envoyer un grand nombre d'emails avec des fichiers attachés (plusieurs milliers par exemple) à un ou à des destinataires
- **Spamming** : consiste à envoyer plusieurs e-mails identiques (souvent de type publicitaire) à un grand nombre de personnes sur le réseau. Le but premier du spamming est de faire de la publicité à moindre coût

Service Web: HTTP

- **Les cookies** : information permettant aux serveurs de reconnaître tout visiteur qui s'est déjà connecté à ce service. Ces informations peuvent être utilisées par un pirate ou par des sites commerciaux.
- **JavaScript** : Diverses failles de sécurité dues à des erreurs dans les butineurs sont détectées:
  - relire des informations du disque dur de l'utilisateur et retransmettre l'information vers un autre site du réseau
  - retransmettre l'adresse électronique de l'utilisateur, ainsi que les adresses de documents visités
  - espionner les pages que l'utilisateur visitera par la suite
- **Les applets Java ou les composants ActiveX**

Les virus

- **Virus de boot :** remplacent l'amorce d'un disque par leur propre code, pour se charger ensuite en mémoire centrale .
- **Virus Programme** : ajoutent leur codes source au programme en EXE, COM, BAT, ils détruisent le fichier, et se chargent en mémoire centrale .
- **Virus de Macro** : se trouvent dans les fichiers qui utilisent des macro commandes, comme Word, Excel, etc. Lorsque la macro sera lancée, le virus sera en action.
- **Virus de Partition** : se logent dans la table de partition, et n'ont pas besoin d'un fichier infecté pour être chargés en mémoire
- **Les virus flibustiers** (Bounty hunters) : visent directement les antivirus en les modifiant pour les rendre impuissants, ce genre des virus sont très rares mais très efficaces.

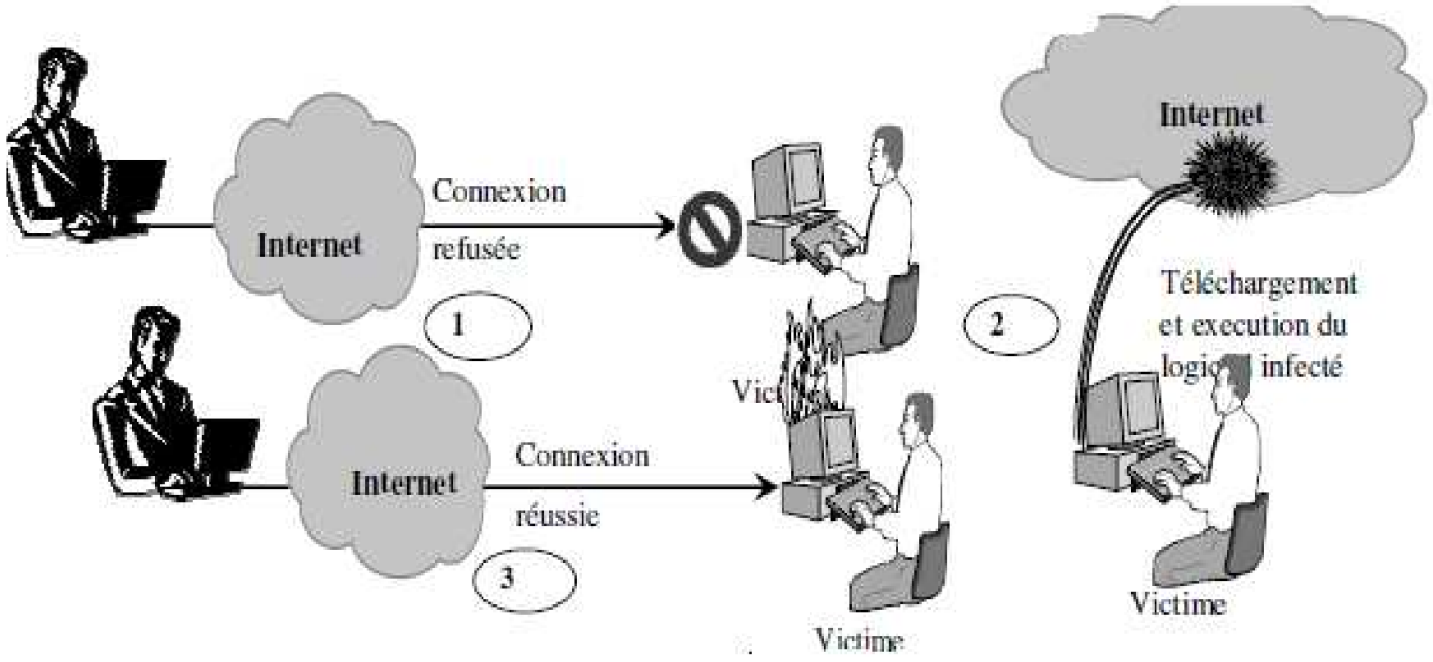
Les vers

- ne peut pas se greffer à un autre programme et donc l'infecter, il se copie via un réseau ou Internet, d'ordinateur en ordinateur.

- Réplication
  ==>
  - ✓affecter un ordinateur
  - ✓dégrader les performances du réseau

Chevaux de trois

programme ou un code malveillant qui fait autre chose en plus de sa fonction déclarée



Les logiciels d’espionnage (Spyware)

- Un outil infecté par un spyware peut représenter une très grande menace pour la sécurité du système d'information infecté.
- En effet plusieurs routines successives peuvent permettre la détection de mots de passe encryptés et les craquages de ces informations

Vulnérabilité des systèmes d'exploitation

- Les logiciels (systèmes d'exploitation et applications) sont presque tous livrés avec des erreurs. Ces erreurs sont souvent bénignes, mais parfois elles peuvent créer des trous de sécurité sur notre système, trous que des personnes mal intentionnées peuvent utiliser pour l'attaquer

outils d'attaque et d'analyse du trafic d'un réseau informatique

- Analyseurs de trames (sniffer)
  tcpdump: analyseur en mode texte
  wireshark: analyseur en mode graphique
  tshark: comme wireshark mais en mode texte
  dsniff: recherche de mode passe
- Balayeur de ports (scanner)
  telnet: scanner de port du pauvre
  nmap: scanner de ports …
- Détecteurs d'intrusion (IDS)
  snort, chkrootkit, portsentry

tcpdump

- Tcpdump [options] [expression]
- Options:

-i interface

-w fichier: stocke le résultat dans le fichier

-F fichier :expression de filtrage est lue à partir du fichier

-n : ne pas convertir les adresses en noms

-a : convertit les adresse en nom

-N: n'affiche pas le nom de domaine des machine

-c n: s'arrete après n paquets

-v : plus de detail (TTL, ToS …)

-vv: mode plus verbeux

-e: affiche les donnée en couche liaison (adress MAC)

-s n: concerve/affiche les n premiers octets d'un paquet

-S: affiche les numéros de séquences TCP

- Expressions:

Les quantificateurs de type: host, net, port

Les quantificateurs de direction: src, dst, src and dst, src or dst, src net, dst port …

Les quantificateurs de protocole: ether, fddi, ip, icmp, arp, rarp, tcp, udp, ip proto …

Les quantificateurs spéciaux: broadcast, gateway, less, greater, not (ou !), or (ou ||), and (ou &&), <,>,<=, <=, <> ,=, !=

exemple

- $tcpdump // capture sur la sortie standard
- $tcpdump –i eth0 –w fichier

//visualiser les paquets web

- $tcpdump tcp port 80
- $tcpdump host 192.168.1.23
- $tcpdump ip proto 1 ⇔ $tcpdump icmp
- $tcpdump 'tcp and (port 21 or port 80)'

nmap

- $nmap [type_analyse] [options] (hote|réseau)
- Type_analyse:

-sS: balaye les port TCP par envoi de SYN

-sF: utilise un paquet FIN et attend RST

-sX: utilise un paquet FIN avec les drapeaux URG, PUSH

-sU: balaye les ports UDP

-s0: balaye IP

-sA: balaye TCP en utilisant ACK

-sL: liste les noms des machines d'un réseau

nmap

- $nmap [type_analyse] [options] (hote|réseau)
- Options

-p <domaine>: spécifie les domaines de port, par défaut 1-1024 on peut spécifier –p 578, -p 24-56,234-550

-O: essaye de determiner le système d'exploitation du cible

-A: détermine OS et les applications

-sV: détermine les version des applications

-v mode bavard

-S <addresse> fixe l'adresse source (spoofing)

exemple

- $nmap lion
- $nmap –v –sP 192.168.1.0/24
- $nmap –p 443 192.168.1.44

//port UDP de lion

- $nmap –sU lion

//affiche le nom OS et les applications

- $nmap –A lion

//lister les ports ouverts TCP inferieurs à 1024

- $nmap –sT –p 1-1024 lion

Autres attaques

- Ettercap
- Arpspoof
- dnsspoof
- Dsniff

Ettercap

- Ettercap permet l'analyse du réseau informatique. Il est capable d'intercepter le trafic sur un segment réseau.
- placé l'attaquant dans une situation de man in the middle
- En empoisonnant le cache arp du host (routeur) et de la victime, ettercap a fait croire au routeur qu'il était la victime et il a fait croire a la victime qu'il était le routeur . Ainsi l'attaquant maitrise totalement sa victime, en plus de pouvoir les sniffer, il peut modifier à sa guise toutes les données qui transitent.

arpspoof

arpspoof -t target host

où :

– **target** est la machine client que nous souhaitons attaquer

– **host** est la machine serveur pour laquelle nous souhaitons nous faire passer

dnsspoof

- **dnsspoof** [**-i** *interface*] [**-f** *hostsfile*] [*expression*]
- **-f** *hostsfile* specifie le fichier qui contient les faux noms |adresse de la même forme que hosts (de la forme adresse nom ou adresse *.nom)
- Expression : sont des expression comme celles de tcpdump (src, host, dst , port …)

dsniff

- Dsniff est à la fois une suite d'utilitaire et un utilitaire lui-même d'audit réseau permettant aisément de sniffer les passwords circulants en clair, dans des protocoles non sécurisés: FTP, telnet, SMTP, HTTP, POP, NNTP, IMAP, SNMP, LDAP, rlogin, RIP, OSPF …
- dsniff -i interface [-f services] [-w savefile] [expression]
- Exemple:
- dsniff -i eth0 -w pass.txt
- dsniff -i eth0 -f ftp
- dsniff src 192.168.1.18