



Université  
De Boumerdes



Université  
De Limoges

---

Département d'informatique  
M2

# Attaques et vulnérabilités des réseaux

*Réalisé par :* Dr RIAHLA

Docteur de l'université de Limoges (France)

Maitre de conférences à l'université de Boumerdes



Université  
De Boumerdes



Université  
De Limoges

---

**Département de physique/Infotronique  
IT/S6**

# **Introduction**

# Introduction

## *Hacker et cracker*

---

### *Hacker*

Une communauté de programmeurs expérimentés et des spécialistes des réseaux, ont créé le mot "***hacker***".

Ces informaticiens sont:

- Généralement discrets
- Anti-autoritaristes
- Motivés par la curiosité.

# Introduction

## *Hacker et cracker*

---

### ***cracker***

- Personnes qui s'autoproclament des "hackers".
- Adolescents de sexe masculin
- S'introduisant à distance dans les systèmes informatiques
- piratent des systèmes téléphoniques.
- Utilisent des outils écrit par d'autres personnes (trouvés sur Internet).

# Introduction

## *Hacker et cracker*

---

Les vrais hackers appellent ces gens des ***crackers***.

Les vrais hackers pensent que les crackers sont:

- Des gens *paresseux*,
- *Irresponsables et*
- *Pas très brillants.*

# Introduction

## Objectifs des attaques

---

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

# Introduction

## Motivations des attaques

---

- Vol d'informations
- Modifications d'informations
- Vengeance/rancune
- Politique/religion
- Défis intellectuels

# Introduction

## Cible des pirates

---

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





Université  
De Boumerdes



Université  
De Limoges

# Définitions

# Définitions

---

## **Nœud malicieux:**

- Unité malveillante (écoute puis attaque)

## **Attaquant actif-n-m:**

- Attaquant qui possède  $m$  nœuds malicieux et qui compromet  $n$  nœuds

## **Attaques externes :**

- Attaques lancées par un nœud qui n'appartient pas au réseau ou bien qui n'est pas autorisé à y accéder

# Définitions

---

## Attaques internes:

- Attaques lancées par des nœuds internes compromis ou malveillants.
- C'est le type de menace le plus sévère
- Les mécanismes proposés pour lutter contre les attaques externes sont inefficaces devant ce type d'attaques

# Définitions

## (Définitions: **Attaques passives**)

---

- Écoute des lignes
- Analyse de trafic
- Plus facile avec le sans fil
- C'est une préparation d'une attaque active

### **La Solution doit:**

- **Assurer la confidentialité des échanges.**

# Définitions

## (Définitions: **Attaques actives**)

---

- **Détruire** des messages
- **Injecter** des messages erronés
- **Modifier** des messages et **usurper l'identité** d'un nœud.
- ...etc

**La Solution doit:**

- **Assurer la disponibilité, l'intégrité, l'authentification et la non répudiation**



Université  
De Boumerdes



Université  
De Limoges

# Rappels TCP/IP

# Rappels sur le concept d'IP

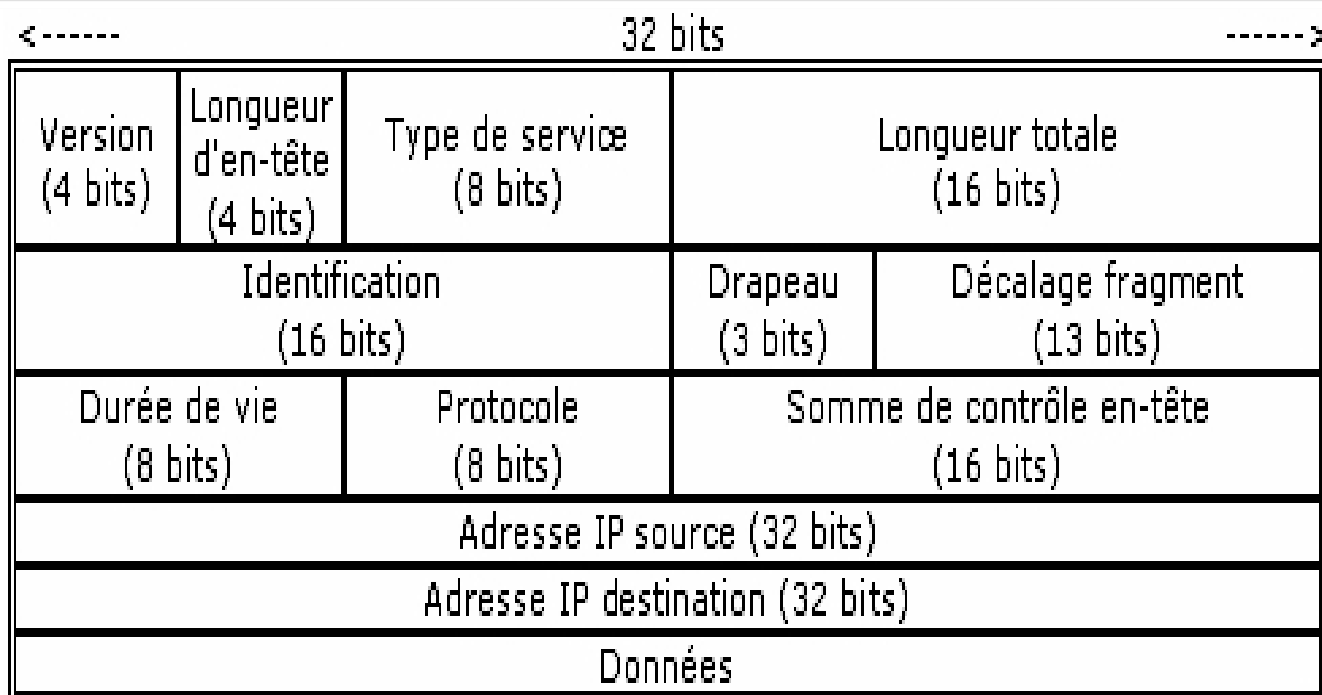
## Anatomie d'une adresse IP

---

- Adresse logique des machines
- Représentée sur 32 Bits
- **ICANN**, Institution chargée d'affecter les numéros IP dans le monde afin d'éviter les conflits

# Datagramme IP:

L'unité de base des données circulant sur Internet



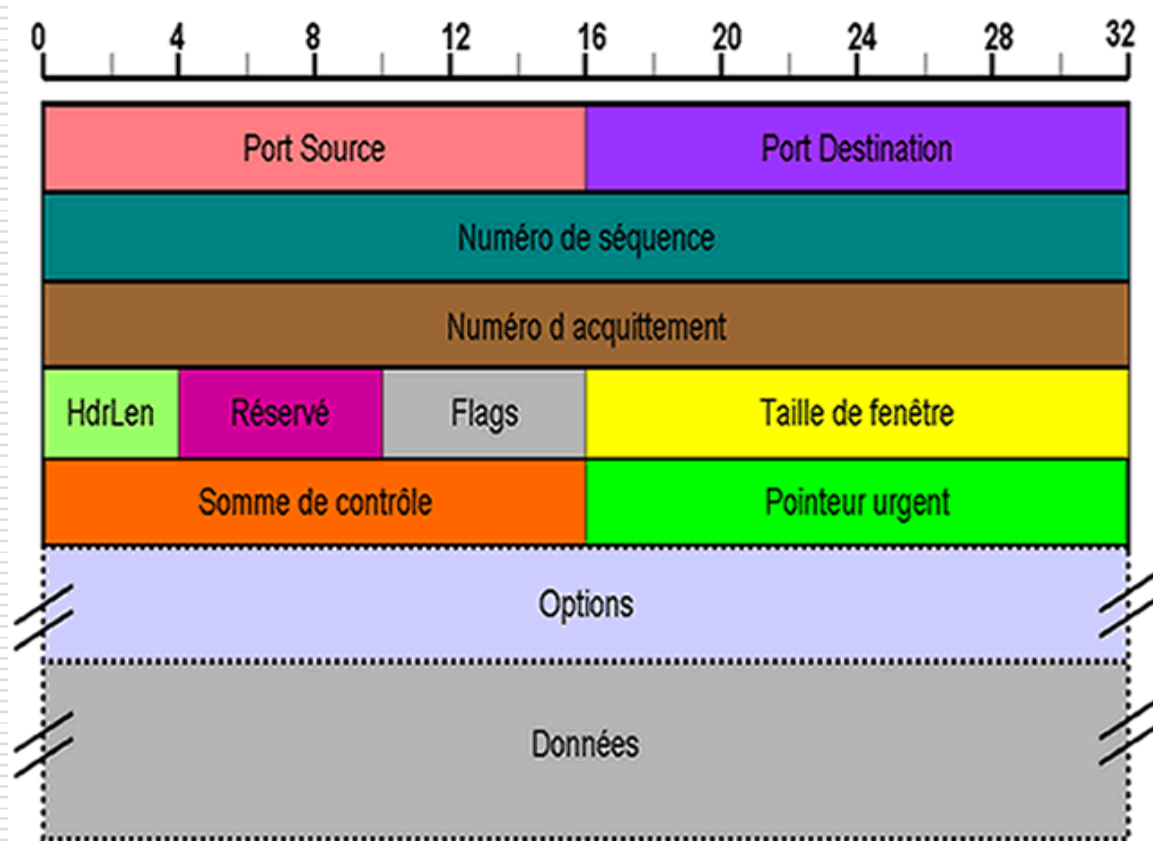


# Message UDP

---

<b>Port UDP source</b>	<b>Port UDP destination</b>
<b>Longueur message UDP</b>	<b>Somme de contrôle</b>
<b>Données ...</b>	

# Segment TCP



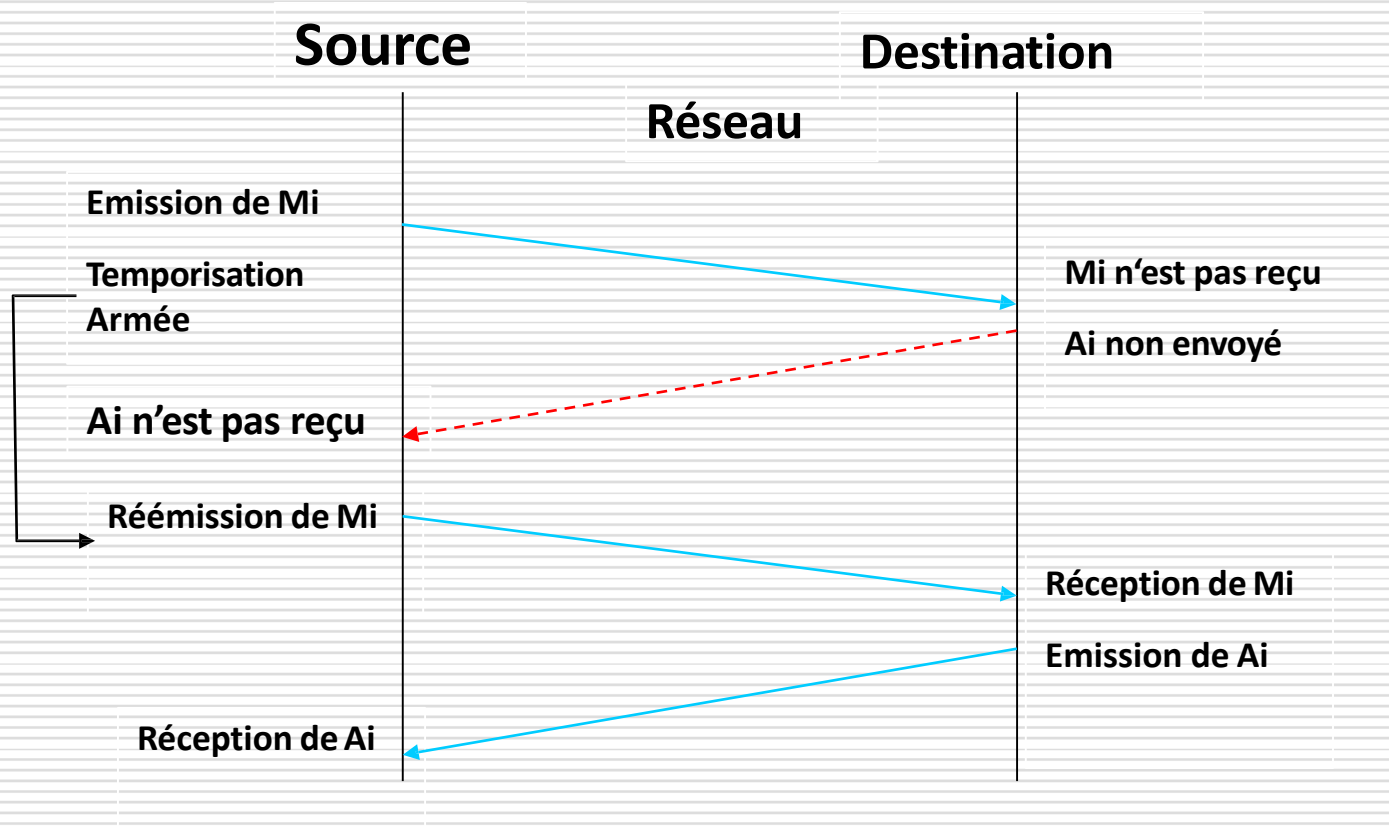
# Segment TCP

## Le champ Flags

---

- **ACK:** Le paquet est un accusé de réception
- **FIN :** L'émetteur a atteint la fin de son flot de données.
- **RST:** Réinitialiser la connexion.
- **SYN:** Synchroniser les numéros de séquence pour initialiser une connexion.
- **PSH:** Fonction push.

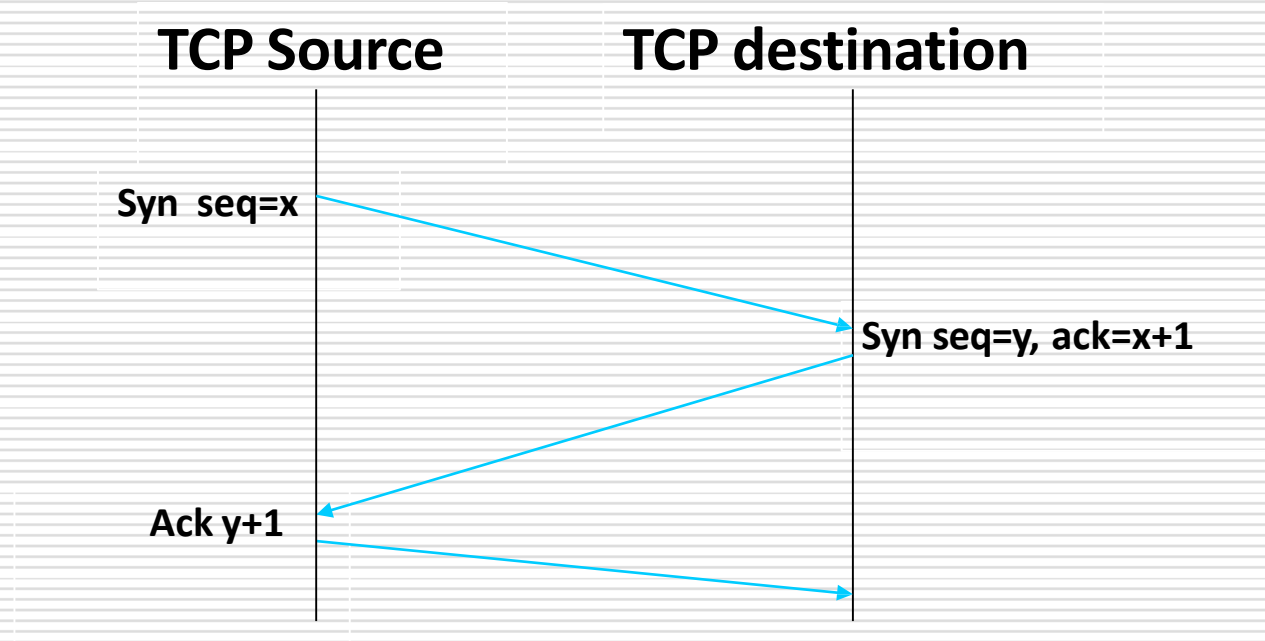
# Segment TCP Acquittements



# Segment TCP

## Ouverture de connexion

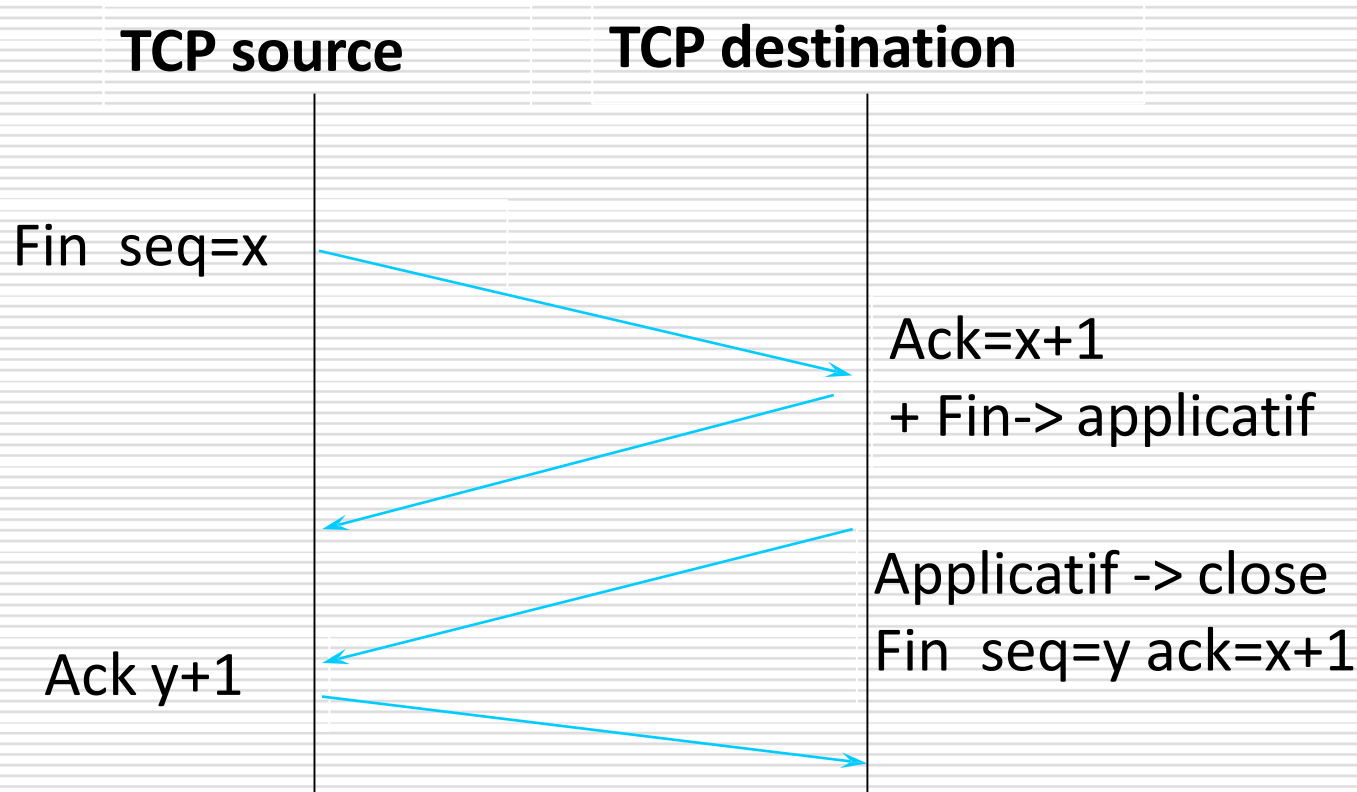
---



# Segment TCP

## Fermeture de connexion

---



# Segment TCP

## Autres types de connexions

---

### **Transfert de données**

==> ACK=1 - SeqNum=101 - AckNum=301 - Data=30 octets

<== ACK=1 - SeqNum=301 - AckNum=131 - Data=10 octets

==> ACK=1 - SeqNum=131 - AckNum=311 - Data=5 octets

<== ACK=1 - SeqNum=311 - AckNum=136 - Data=10 octets

### **Fermeture brutale de connexion**

==> ACK=1 - RST=0 - SeqNum=200 - AckNum=400

<== ACK=0 - RST=1 - SeqNum=400 - ACKNum=xxx



Université  
De Boumerdes



Université  
De Limoges

# Attaques réseaux





Université  
De Boumerdes



Université  
De Limoges

---

Les réseaux peuvent être vulnérables:

- Par une mauvaise implémentation des piles udp/ip et tcp/ip.
- Par des faiblesses des protocoles

# IP Spoofing: Introduction (Usurpation d'adresse IP)

---

➤ Dans certains cas, l'adresse IP source est utilisée pour autoriser une connexion (Systèmes sur lesquels l'authentification est fondée sur l'adresse IP).

**IP Spoofing:** On fait croire que la requête provient d'une machine autorisée.

# IP Spoofing: Principe

---

- **IP Spoofing:** Forger l'adresse source d'un paquet et à abusez de la confiance de cette source.
- Plus facile à utiliser avec les protocoles basés sur **UDP**.
- Pour **TCP** ???

# IP Spoofing: Attaques à base de TCP

---



# IP Spoofing: Attaques à base de TCP

---

- TCP est un protocole en mode connecté, il utilise des acquittements et des numéros de séquence
- Pour éviter d'utiliser les mêmes numéros de séquence, un numéro de séquence initial aléatoire (ISN) est choisi pour chaque nouvelle connexion
- **Exemple d'attaque:** les protocoles **rlogin**, **rsh** sur les machines à numéro de séquence TCP prévisible.



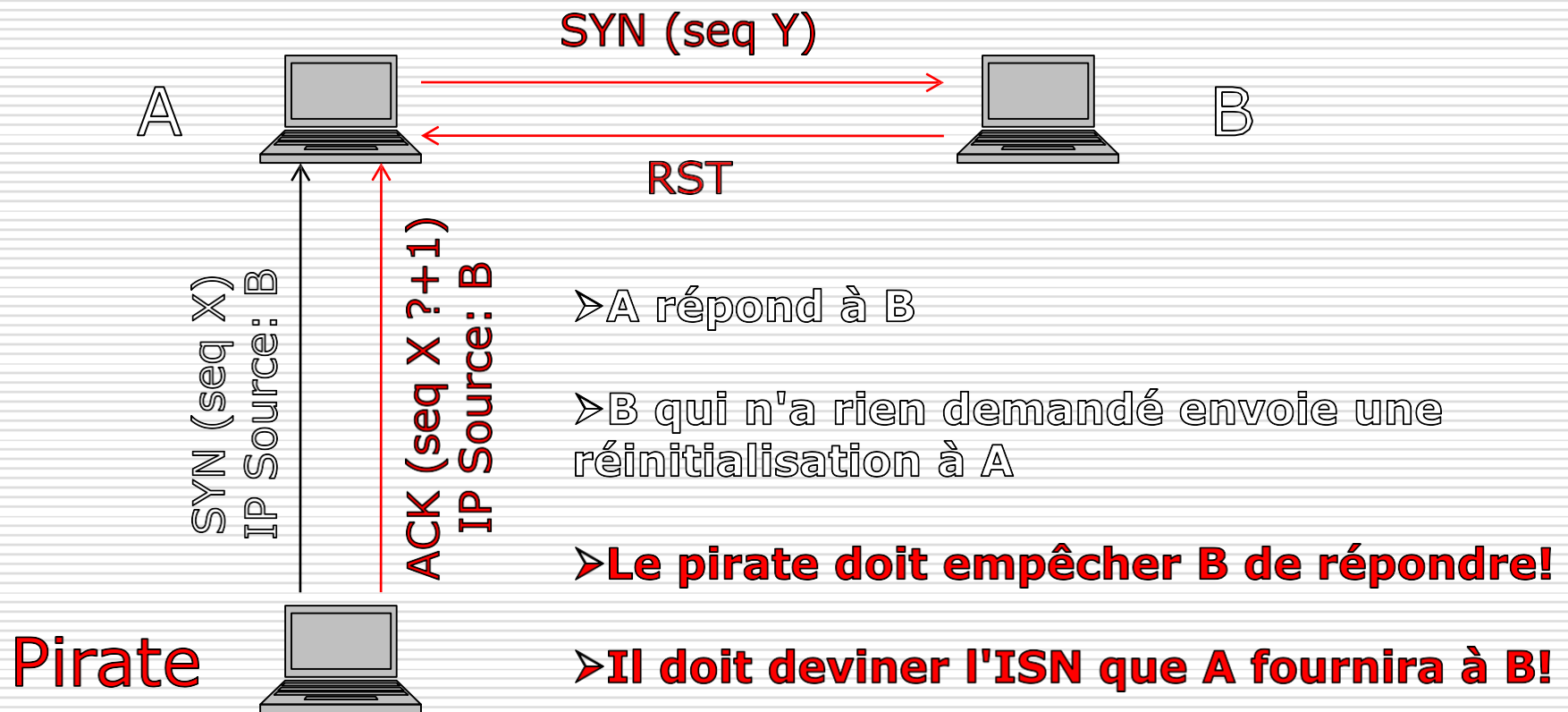
Université  
De Boudoules



Université  
De Limoges

**Mais...**

# IP Spoofing: Attaque à base de TCP



- 
- **Comment deviner l'ISN d'une machine?**
  - **Comment empêcher une machine répondre! ?**



# TCP ISN generation

---

Dans certaines implémentations de pile TCP/IP prochain ISN peut que soit prédit.

Un pirate procède comme suite:

# TCP ISN generation

---

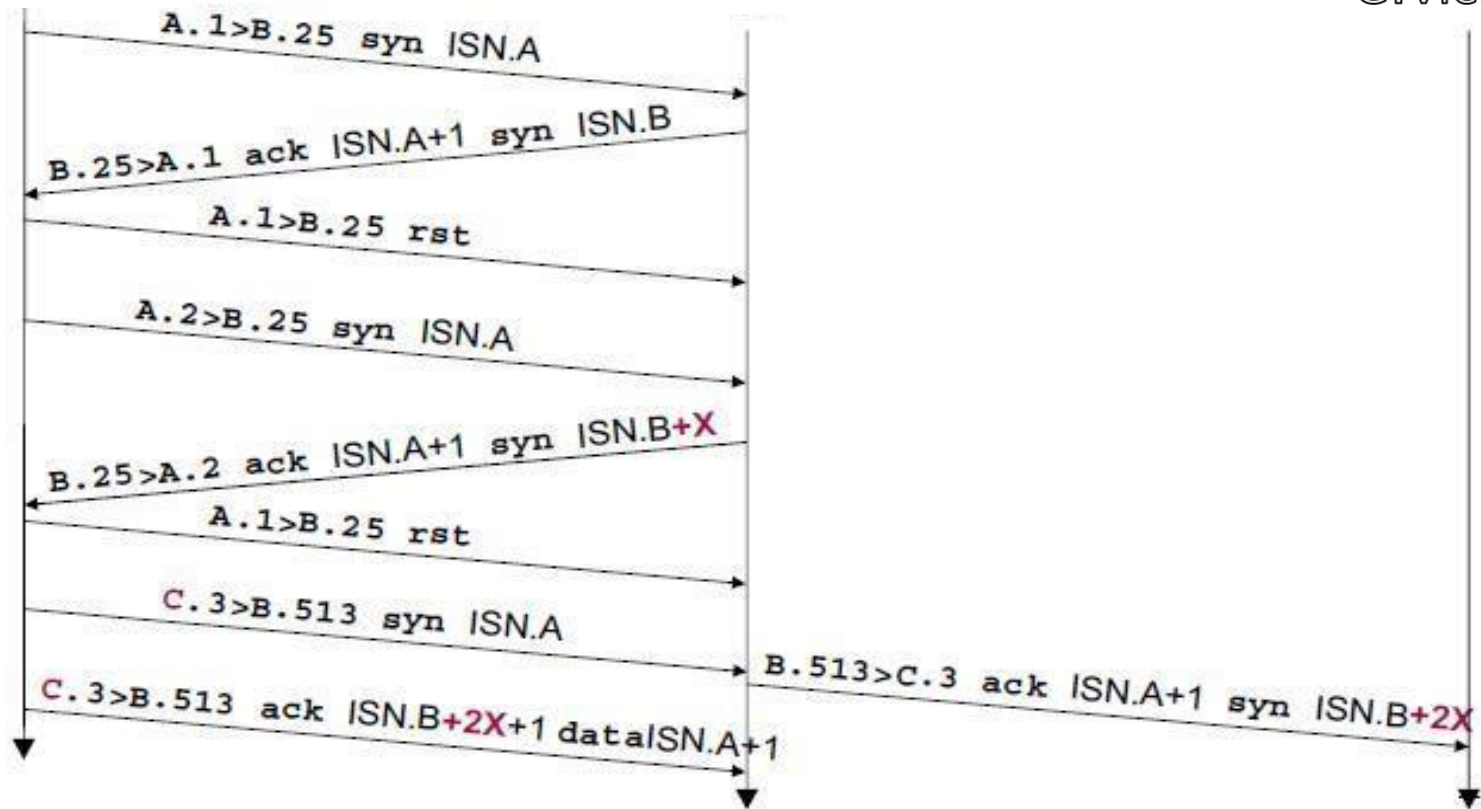
- Il ouvre quelques connexions (par exemple SMTP) pour obtenir les ISN courants et leurs méthodes d'incrémentation.
- Il lance sa connexion forgée qui utilise le dernier ISN incrémenté selon la méthode détectée.
- Il peut lancer des connexions forgées multiples avec différentes augmentations en espérant qu'au moins une est correcte.

# Exemple

A: Pirate

B: serveur

C: victime



---

➤ **Comment empêcher une machine de répondre?**

# DOS (dédi de service)

---

- Attaque destinée à empêcher l'utilisation d'une machine ou d'un service.
- Plus souvent utilisé pour saturer un routeur ou un serveur.
- Ce type d 'attaque peut engendrer des pertes très importantes pour une entreprise.
- Attaque très simple à mettre en œuvre (outils faciles à trouver) et très difficile à empêcher.

# DOS

---

## **DOS local**

- **Epuisement des ressources**
- Saturation de l'espace disque
- répertoires récursifs
- boucle infinie de fork ()
- ...etc

## **DOS par le réseau**

- **Consommation de bande passante**
  - SYN flood
  - *mailbombing.*
  - ...etc
-

# DOS: Exemple SYN Flood

---

- Attaque par inondation de SYN avec une adresse source usurpée (spoofée) et inaccessible.
- La machine cible doit gérer une liste de connexions dans l'état SYN\_RECV .
- Le pirate sature cette liste.
- La machine victime ignore les prochaines connexions
- **Attaque visible si la commande *netstat -an* indique un grand nombre de connexions**

# Se protéger de SYN Flood

---

➤ Une file FIFO (file circulaire)



# DOS: Outils

---

- *Ping 'O Death*
- *Land - Blat*
- *Jolt*
- *TearDrop – SynDrop*
- *Ident Attack*
- *Bonk – Boink*
- *Smurf*
- *WinNuke*

# ARP Spoofing

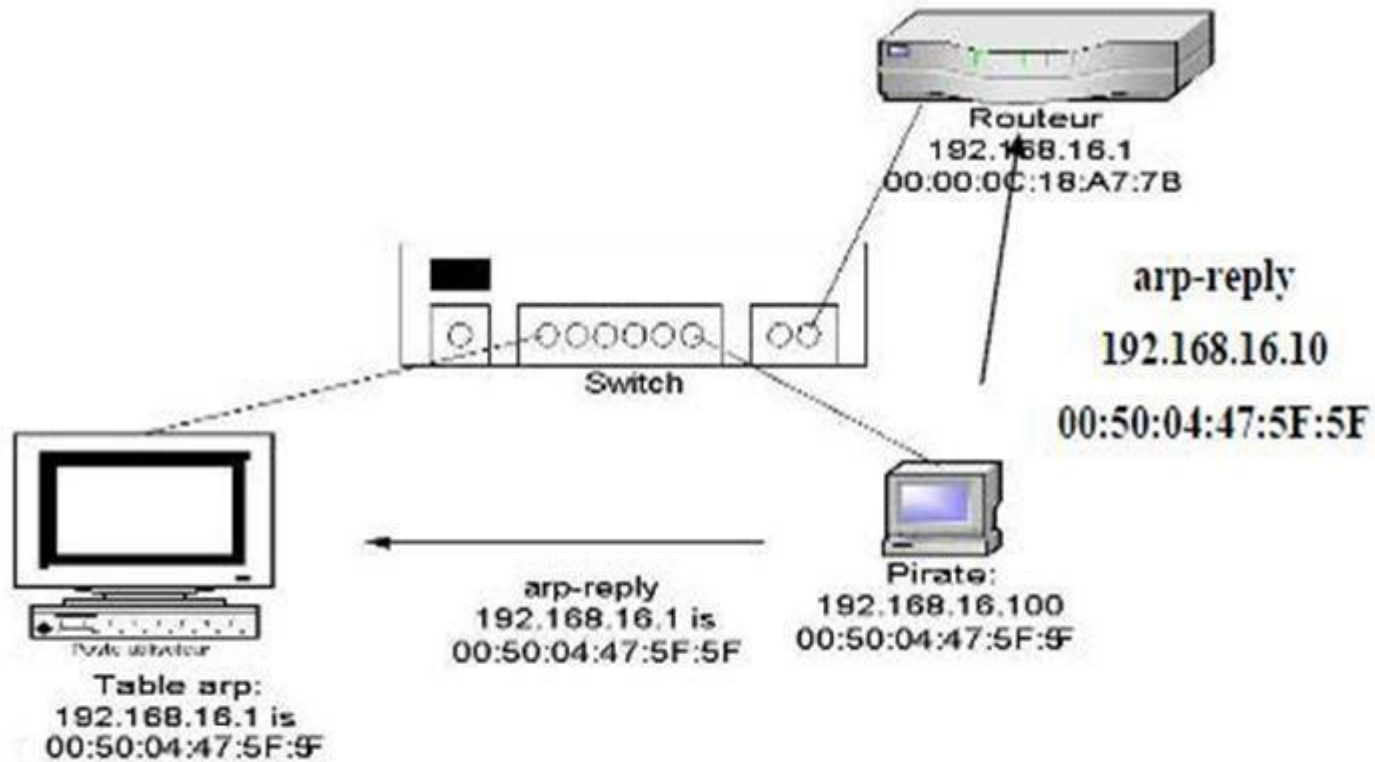
---

- Pollution des caches arp avec de fausses associations adresse mac/adresse IP.
- Permet des attaques de type "man in the middles."

## Outils:

- arp-sk (unix) winarp-sk (windows)  
<http://www.arp-sk.org>
- WinArpSpoof <http://nextsecurity.net>

# ARP Spoofing



# Se protéger contre ARP Spoofing

---

- Utiliser des associations statiques
- Surveiller les changements d'association:

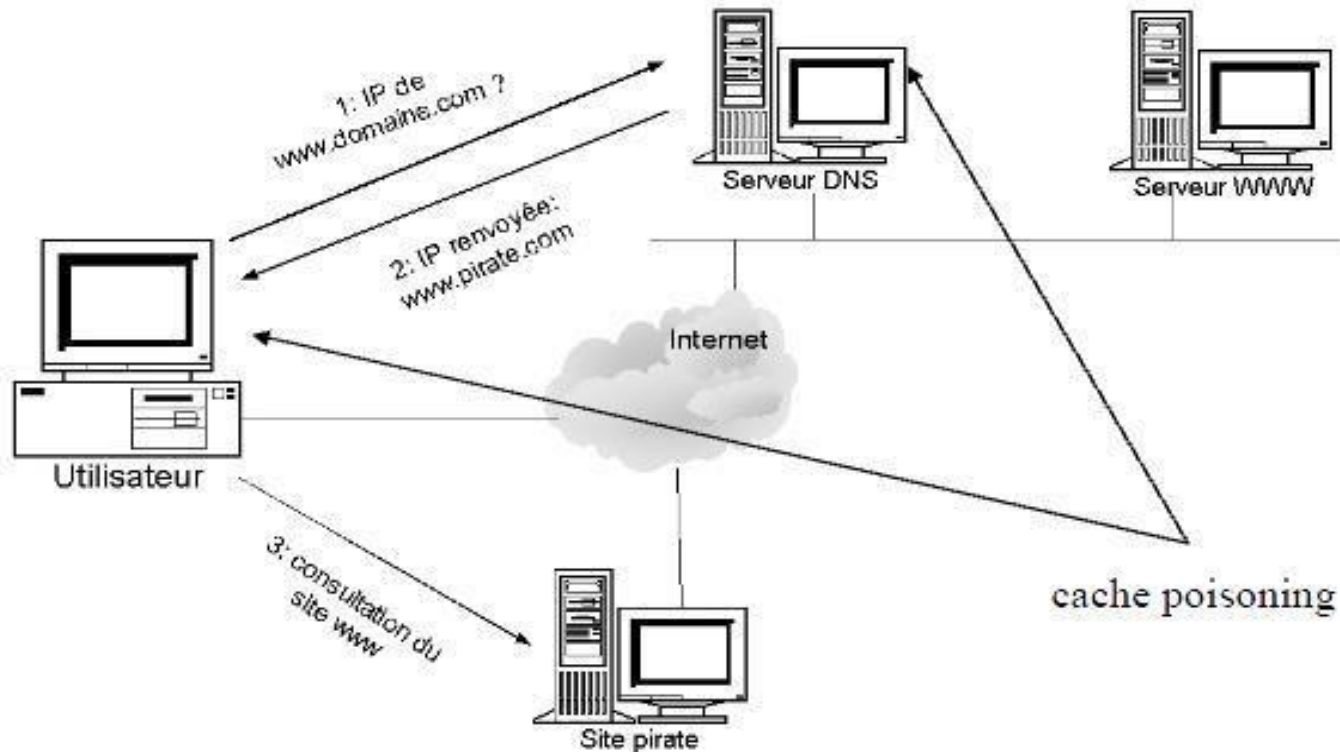
- **arpwatch** (unix)

<http://www.securityfocus.com/data/tools/arpwatch.tar.Z>

- **WinARP Watch** (Windows)

<http://www.securityfocus.com/data/tools/warpwatch.zip>

# DNS Cache poisoning



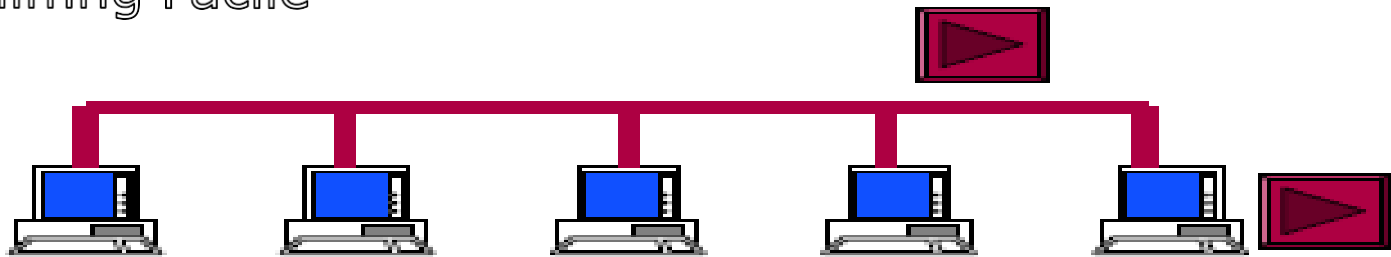
# Sniffer

---

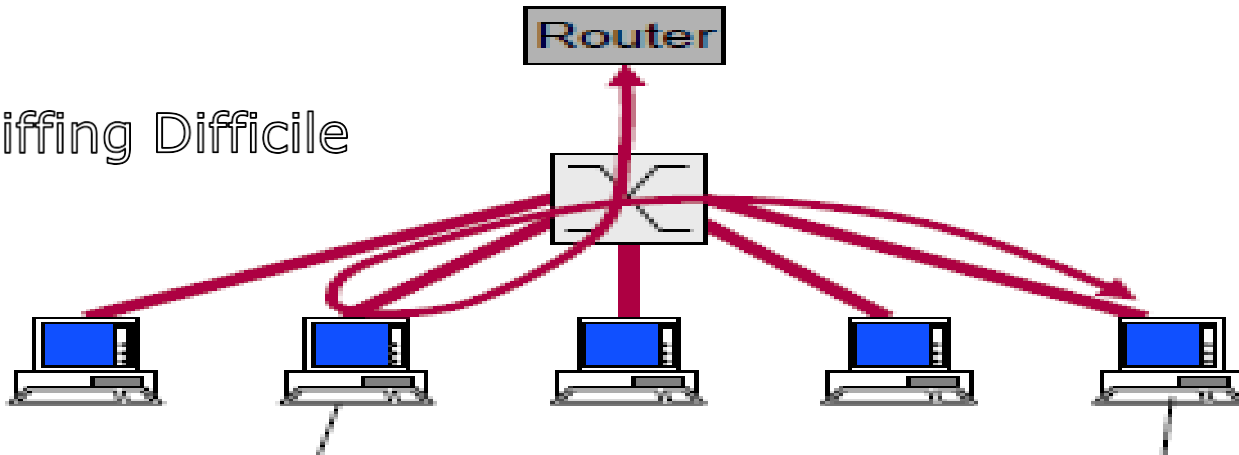
- De nombreux protocoles utilisent une authentification en texte clair
- En visualisant la circulation sur un réseau, nous pouvons obtenir les noms d'utilisateurs et les mots de passe == **sniffer**
- Les sniffers Utilisent des sockets en mode « promiscuous »
- `socket (AF_INET,SOCK_RAW,IPPROTO_RAW)`

# Sniffer

Sniffing Facile



Sniffing Difficile



# Sniffing: Examples

---

Les protocoles d'authentification dont l'échange de données est en text clair:

- telnet
- rsh, rlogin, rexec
- ftp
- http (with basic authentication)
- pop, imap (with default authentication)



# Sniffing: Outils

---

➤ Le sniffer de base pour unix: **tcpdump**.

**tcpdump host e450 and port 25**

➤ Sniffer multi-plateforme: **ethereal**

(<http://www.ethereal.com>) devenu wireshark

(<http://www.wireshark.org>)

➤ Cain & Abel

# Smurf

---

Envoie d'une trame ICMP "echo request « ping » sur une adresse de diffusion.

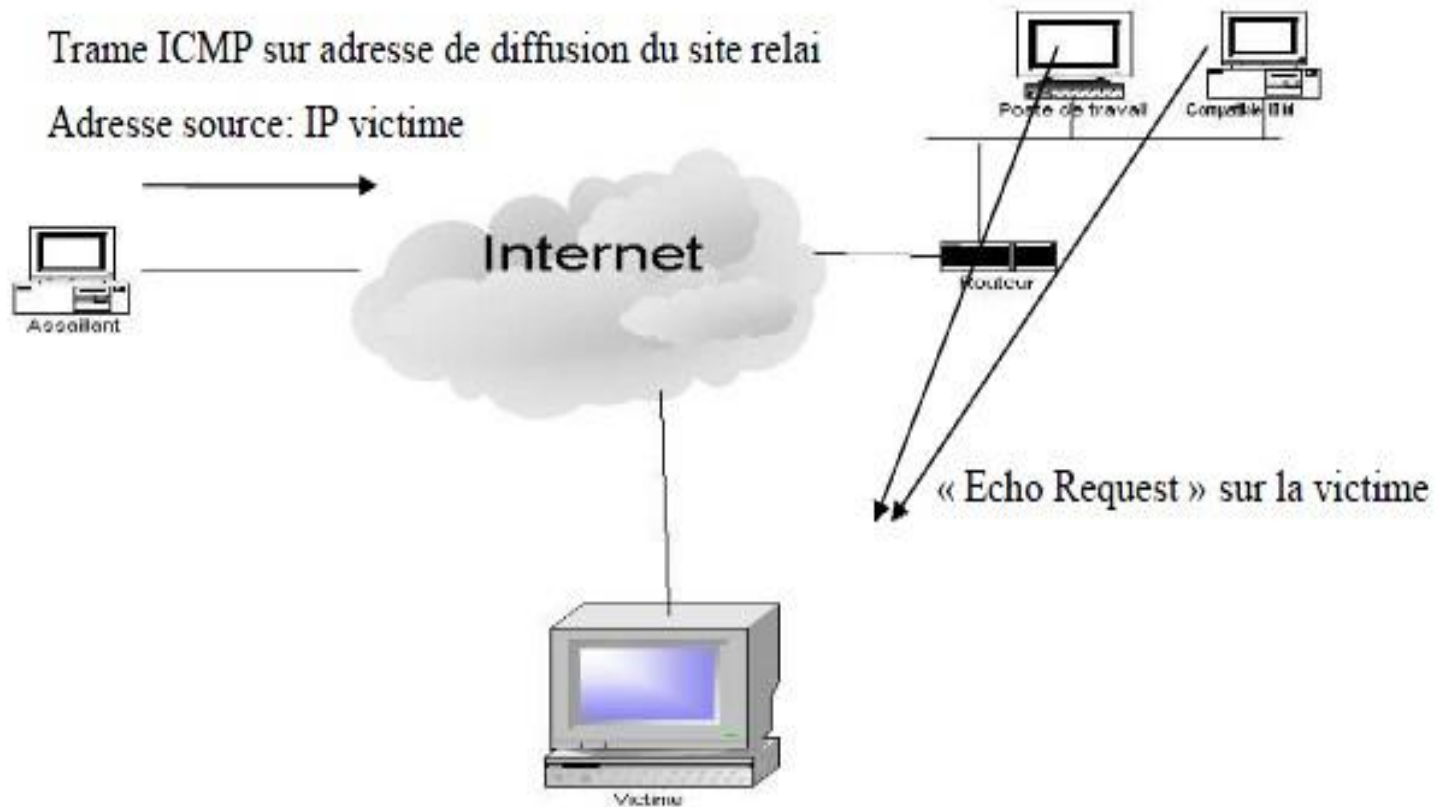
- **Exemple:** *ping 193.49.200.255*

## Objectif

- Utilisée pour déterminer les machines actives sur une plage IP donnée.
- Ecrouler une machine

# Smurf

## Ecrouter une machine



# Se protéger Contre Smurf

---

Interdire la réponse aux trames ICMP sur les adresses de diffusion:

- Au niveau routeur
- Au niveau machine

# L'ingénierie sociale

---

- Il n'y a généralement pas d'attaques réussies sans relations humaines
- basée sur quatre grands principes:
  - **Le contexte** (l'organigramme de l'entreprise)
  - **L'audace** ou le **bluff** (avoir connaissance et savoir parler)
  - **La chance**
  - **La patience calculée**

# Réussite de l'attaque ingénierie sociale

---

- Les personnes ne sont pas formées à la notion de sécurité informatique

Comment ça!!!!!!!!!!:



- *Disquettes ou sauvegardes jetées à la poubelle*
- *Papiers ou l'on note ses mots de passe jetés à la poubelle*
- *Echange de mot de passe par MSN!!!!!!*



# DDOS

---

- Distributed Denial Of Service.
- Type d 'attaque très à la mode.
- L 'objectif est d 'écrouler une machine et/ou saturer la bande passante de la victime.
- Nécessite plusieurs machines corrompues.

# DDOS

## Distributed Denial Of Service.

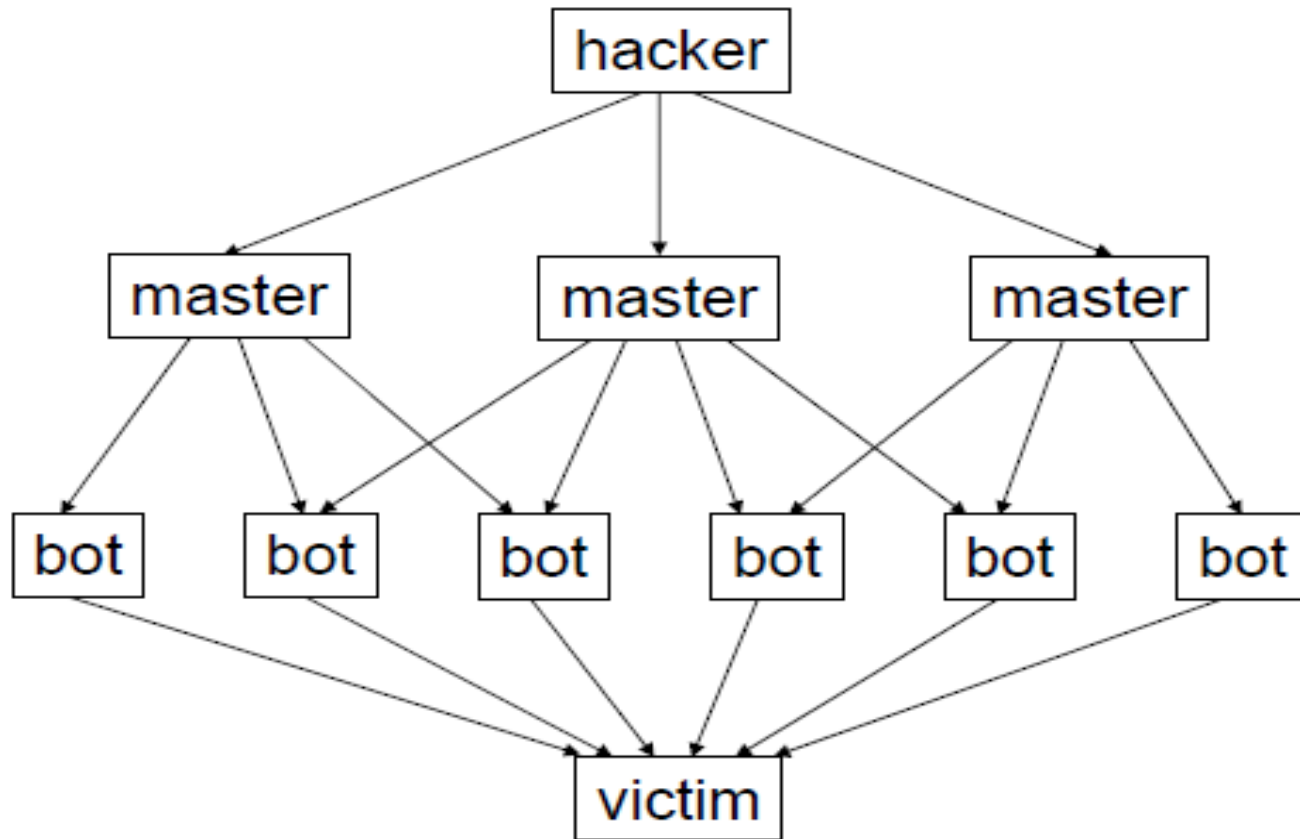
---

- Attaque popularisée le 14 février 2000 sur quelques sites .com renommés (ebay, cnn, amazon, microsoft, ...). Le coupable « Mafiaboy », 15 ans, est arrêté au Canada le 15 avril et condamné à 8 mois de détention. Il a causé des pertes estimées à 1,2 milliards de dollars en 24 heures.



# DDOS

## Distributed Denial Of Service.



# DDOS

## Exemples

---

- Tribe Flood Network (TFN)
- Trinoo
- TFN2K
- Trinity (utilise les serveurs irc)..etc

### **Se protégé contre DDOS:**

- Etre attentif aux ports ouverts
- find\_ddos sur <http://www.nipc.gov>

# But d'une attaque DDOS

---

- Un botnet de 1000 machines peut saturer la bande passante d'une grande entreprise ( $1000 * 128\text{Kb/s} = 128\text{ Mb/s}$ ).
- Une entreprise peut acheter les services d'un « bot herders » pour attaquer un concurrent.
- « Ddos extortion »: des pirates peuvent menacer des sites de commerce en ligne (Exemple: la société Canbet en Angleterre).

# Les « botnets »

---

- Début des années 1990.
- Réseau de machines contrôlées par un « bot herder » ou « botmaster ».

**Selon une estimation:** une machine sur quatre fait partie d'un botnet, soit environ 154 millions de machines.

# Les « botnets » (Utilisation)

---

- Envoyer du spam
- Vol d'informations sensibles (keylogger).
- Installer des spywares.
- **Paralyser un réseau en déni de services (ddos)**
- Installer un site web malicieux (phishing)
- Truquer les statistiques de sites webs.

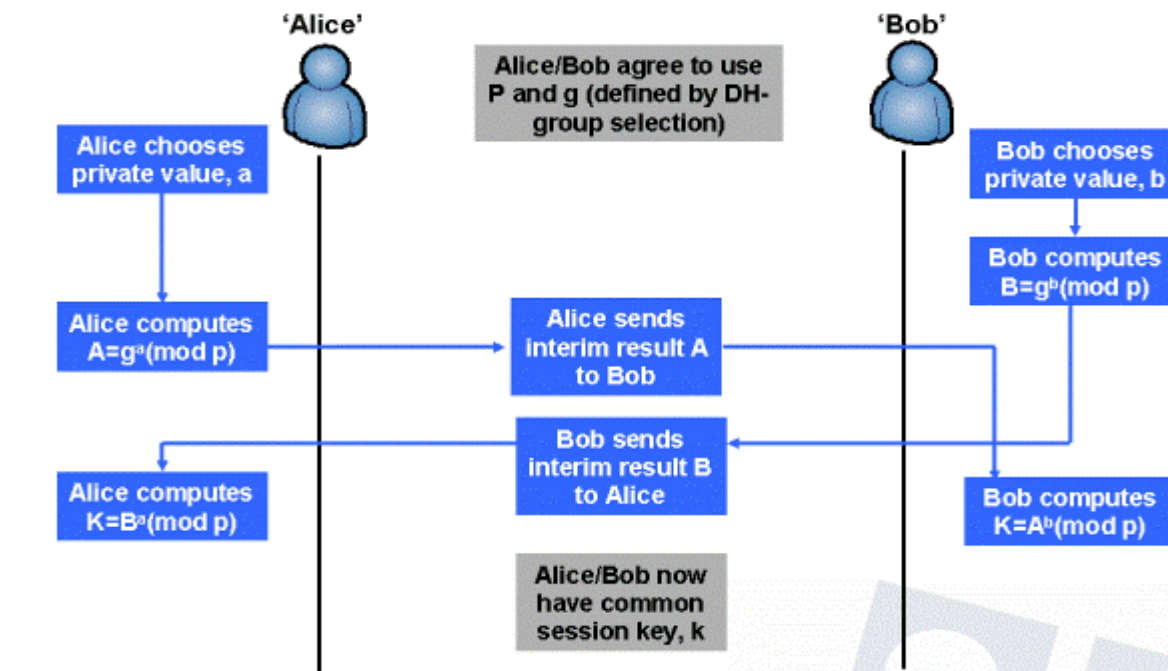
— ...

# ***L'homme du milieu*** ***man in the middle***

---

- **DHCP**
- **ARP**
- **ICMP**
- **RIP**
- **DNS**
- **Proxy HTTP**
- **Virus**

## Diffie-Helman Key Generation/Exchange



# ***Intrusion***

---

## **Attaque :**

- Découverte systématique d'informations.
- Tentative d'intrusion ou de déni de service.

## **Intrusion :**

- Prise de contrôle totale ou partielle d'un système distant



# ***Intrusion***

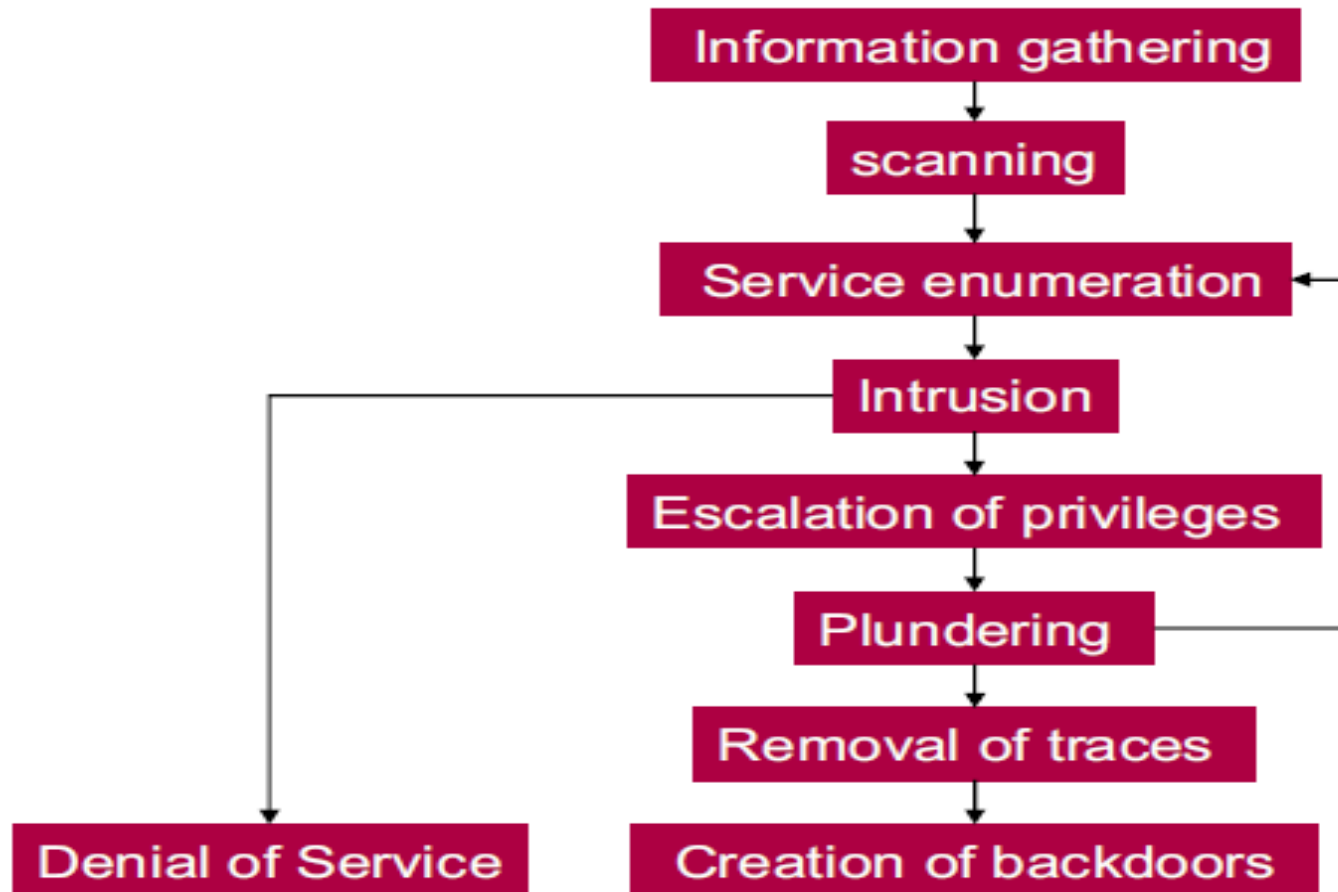
---

- la réalisation d'une menace (c 'est une attaque).
- Les conséquences peuvent être catastrophiques : vol, fraude, incident diplomatique, chantage...etc

## **Solution:**

- Firewall et systèmes de détection d'intrusion ( étudier dans les prochaines parties)

# La méthode des hackers



# ***Collecte d'information***

---

Utilitaires utilisés par les pirates pour préparer leurs attaques.

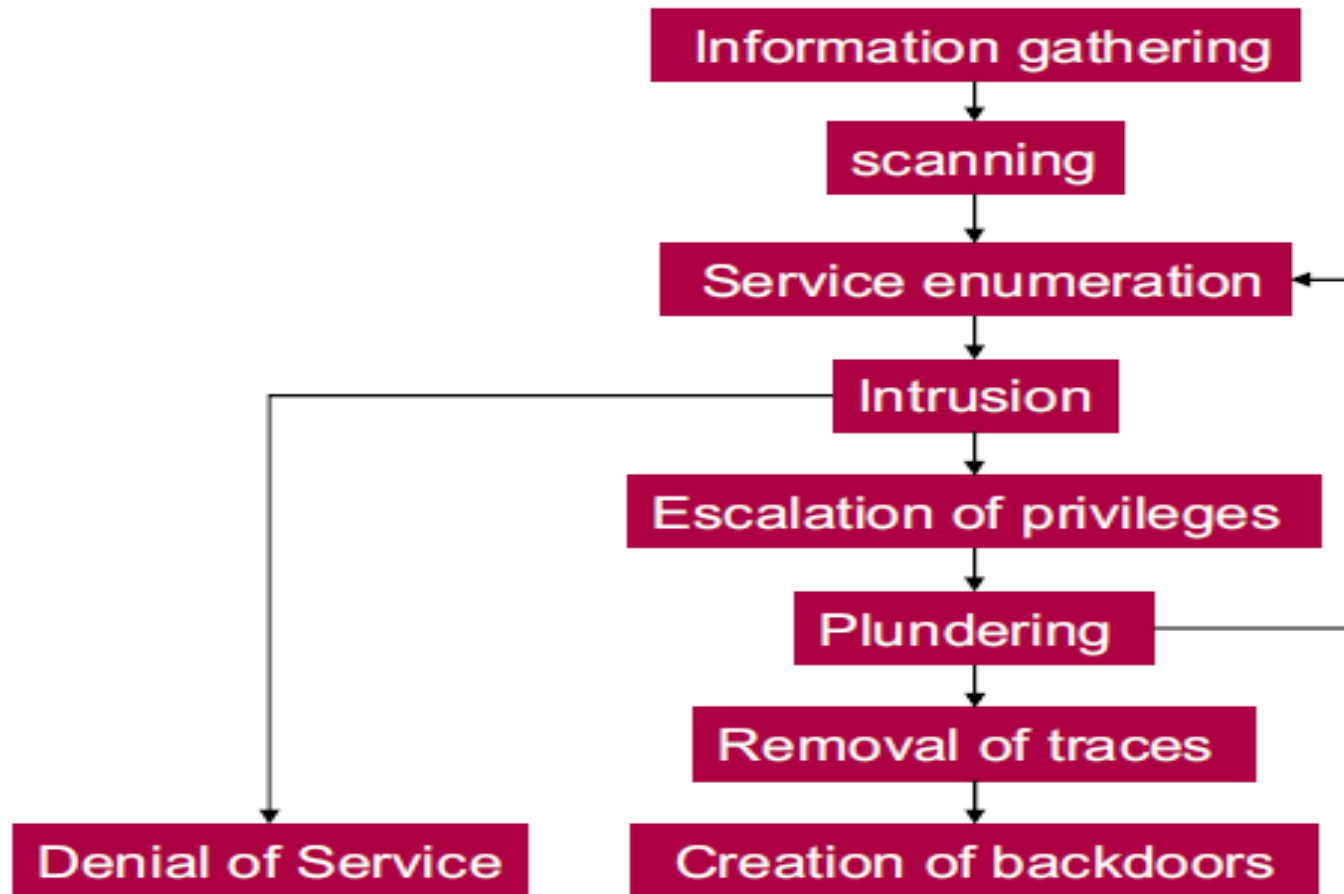
- Détermination des champs d'activités(site web): Téléphone, Implantation Emails, politique de sécurité, liens vers d'autres serveurs WEB, Code source HTML
- Recensement des éléments du réseau (Identifier les noms de domaines et les réseaux associés d'une organisation: BDD INTERNIC, ARIN,...etc)

# ***Collecte d'information***

---

- Interrogation des serveurs DNS  
(**outil**: nslookup www.google.fr)
- Cartographie du réseau (Détermination de la topologie de chaque réseau : **traceroute**)
- Utiliser aussi les techniques d'**Ingénierie sociale**

# La méthode des hackers



# Balayage systématique

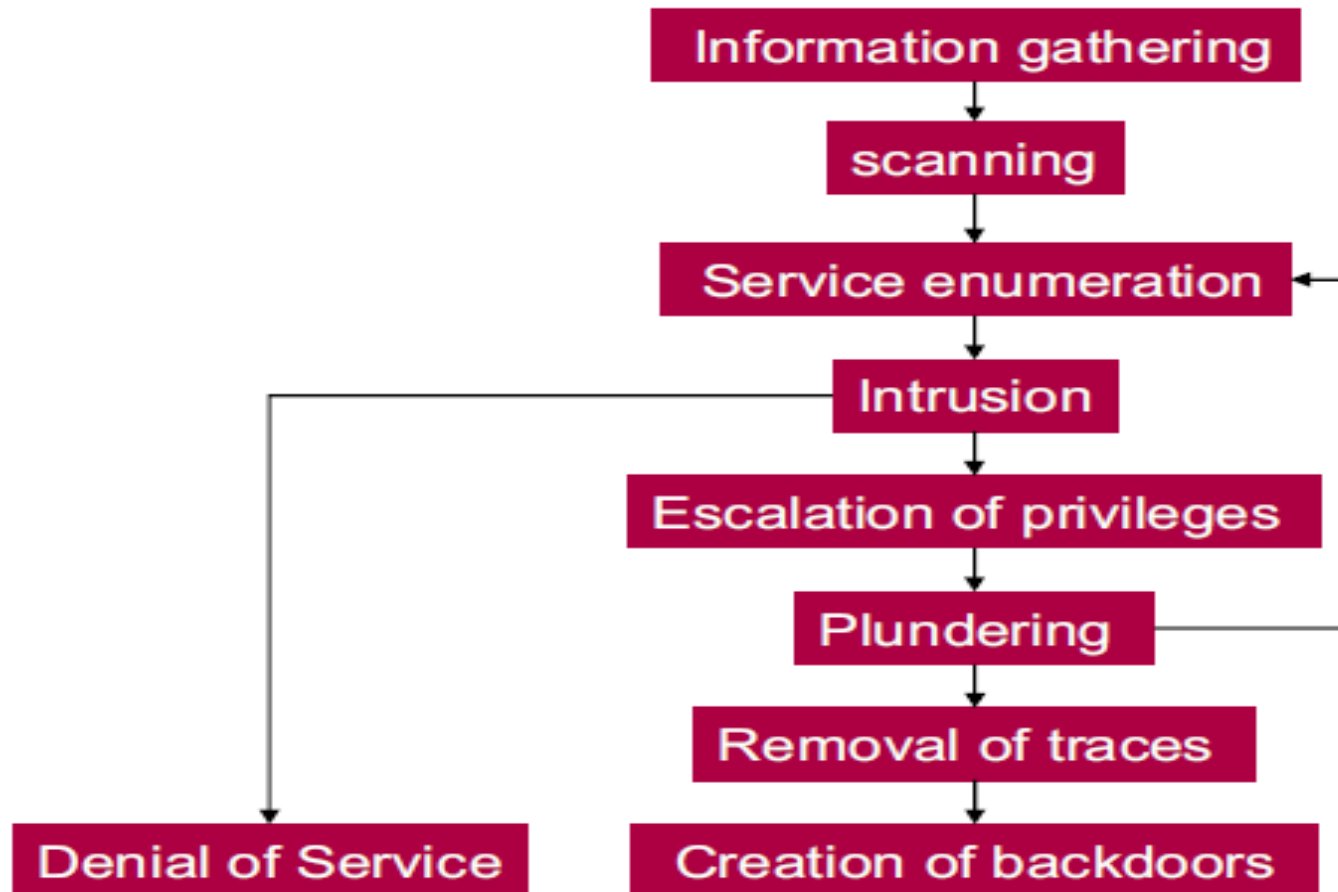
## Scanner

---

Frapper contre tous les murs dans l'espoir de trouver les portes et les fenêtres du réseau cible.

- En connaissant les adresses IP, nous pouvons lancer un scan pour trouver des cibles intéressantes
- Le scanner va essayer de se connecter à tous les services voulu sur toutes les machines appartenant à une plage d'adresses
- **Résultat**: liste des machines accessibles, des ports ouverts sur ces machines (**Outil**: nmap)

# La méthode des hackers



# Enumération des services

---

➤ Dans cette phase, il faut trouver des informations sur les services disponibles (TCP et UDP).

➤ Chercher aussi des:

Systèmes d'exploitation

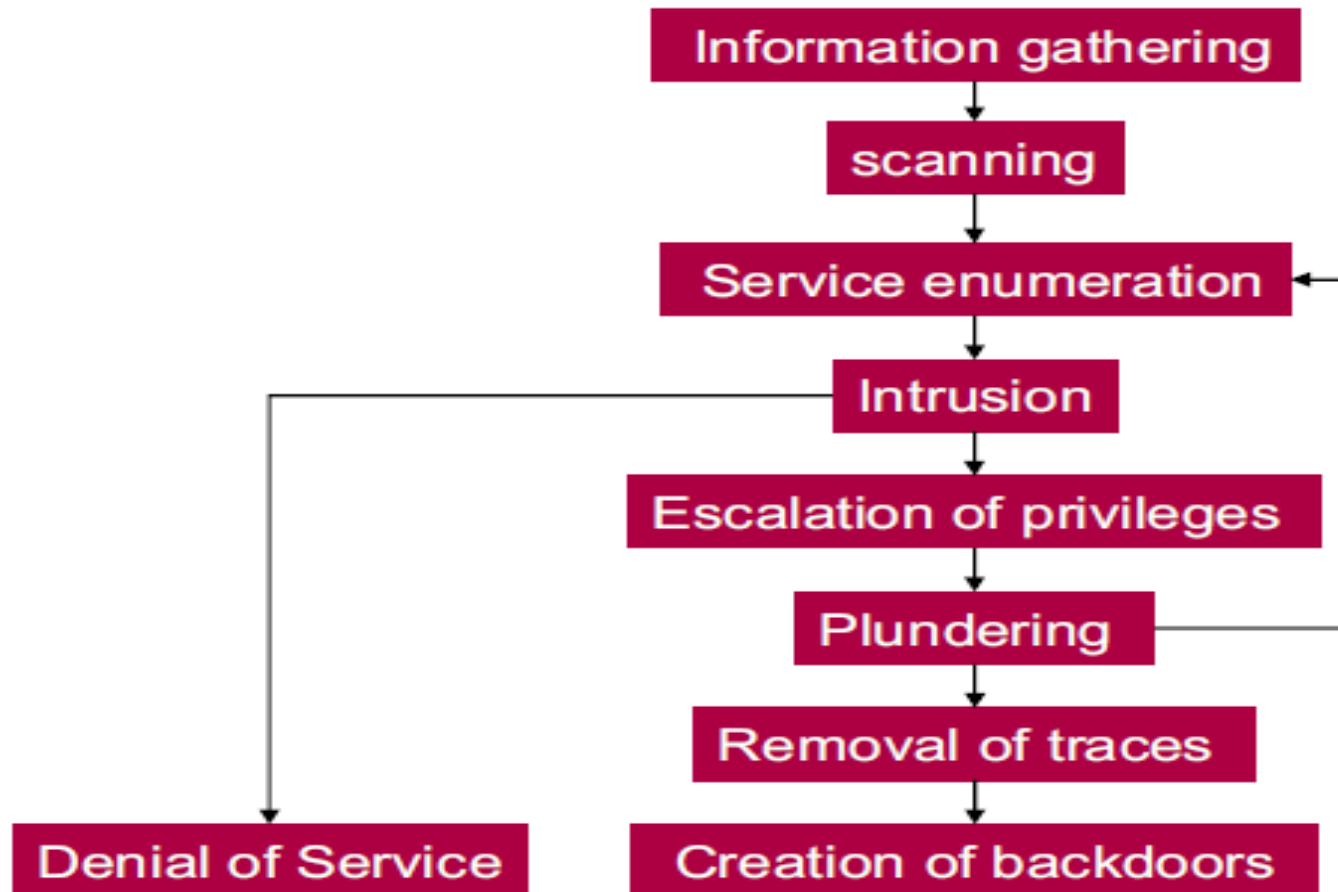
Fournisseur d'un logiciel

Version d'un logiciel (ou service)

**Outils de scan** : *nmap, strobe, udp\_scan, netcat,*



# La méthode des hackers

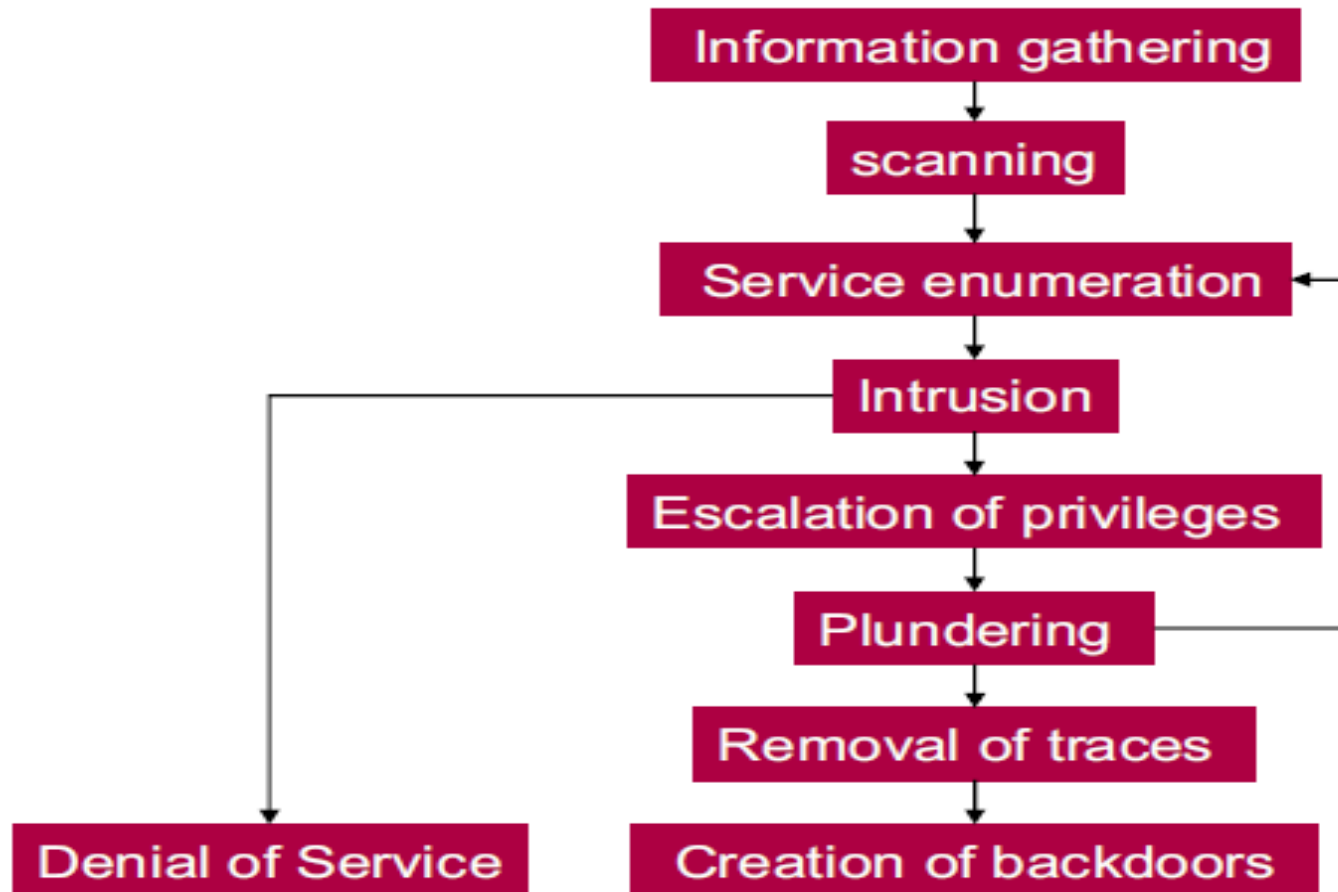


# Intrusion

---

- Par la recherche d'une vulnérabilité connue qui n'a pas encore été corrigé (patcher), nous pouvons pénétrer dans un système.
- Des failles connues peuvent être trouvées sur des sites web: **securityfocus.com, secunia.com**
- Les vulnérabilités les plus récentes sont publiées dans des mailing-listes

# La méthode des hackers



# Suite des étapes

---

## **Escalation (extension) of privileges**

- Chercher à augmenter ses privilèges
- Par exemple l'installation d'un petit script que l'administrateur exécute par erreur .
- Le pirate peut installer un sniffeur

# Suite des étapes

---

## **Plundering**

- Le vol de mots de passe.
- La recherche des informations, des documents ou des emails contenant des mots de passe

# Suite des étapes

---

## **Effacer la trace**

- Correction de logs avec des outils automatiques
- Dissimulation d'intrusion à l'aide de rootkits pour masquer la présence du hacker

## **Installation d'un backdoor**

# Conclusion

---

Après quelques minutes, n'importe qui est capable d'apprendre la manière de hacker votre site

Ce n'est pas parce que vous n'êtes pas connu que vous ne serez pas attaqué

## **Il faut donc:**

- installer les correctifs de sécurité (patches) quand ils sont publiés
- installer seulement les modules logiciels strictement nécessaires pour vos serveurs.

# Conclusion

---

Lorsque les compétences au sein de l'entreprise ne sont pas suffisantes pour mener à bien cette opération, il convient de faire réaliser un audit par une société spécialisée dans la sécurité informatique.





# Merci