




Sécurité



Menaces et attaques

Objectifs

- ▶ Type de menaces
- ▶ Panorama des accidents et erreurs
- ▶ Type des attaques
- ▶ Panorama des attaques
- ▶ Attaques les plus connues

Types des menaces

Menaces

Accidents

Erreurs

Malveillance

pertes de services essentiels

pannes d'origine interne

événements naturels

accidents physiques

erreurs de conception

erreurs d'utilisation

vols ou disparitions

infection par virus

divulgations

attaques logiques

actes de dénigrement ou atteinte
à l'image

sabotages physiques

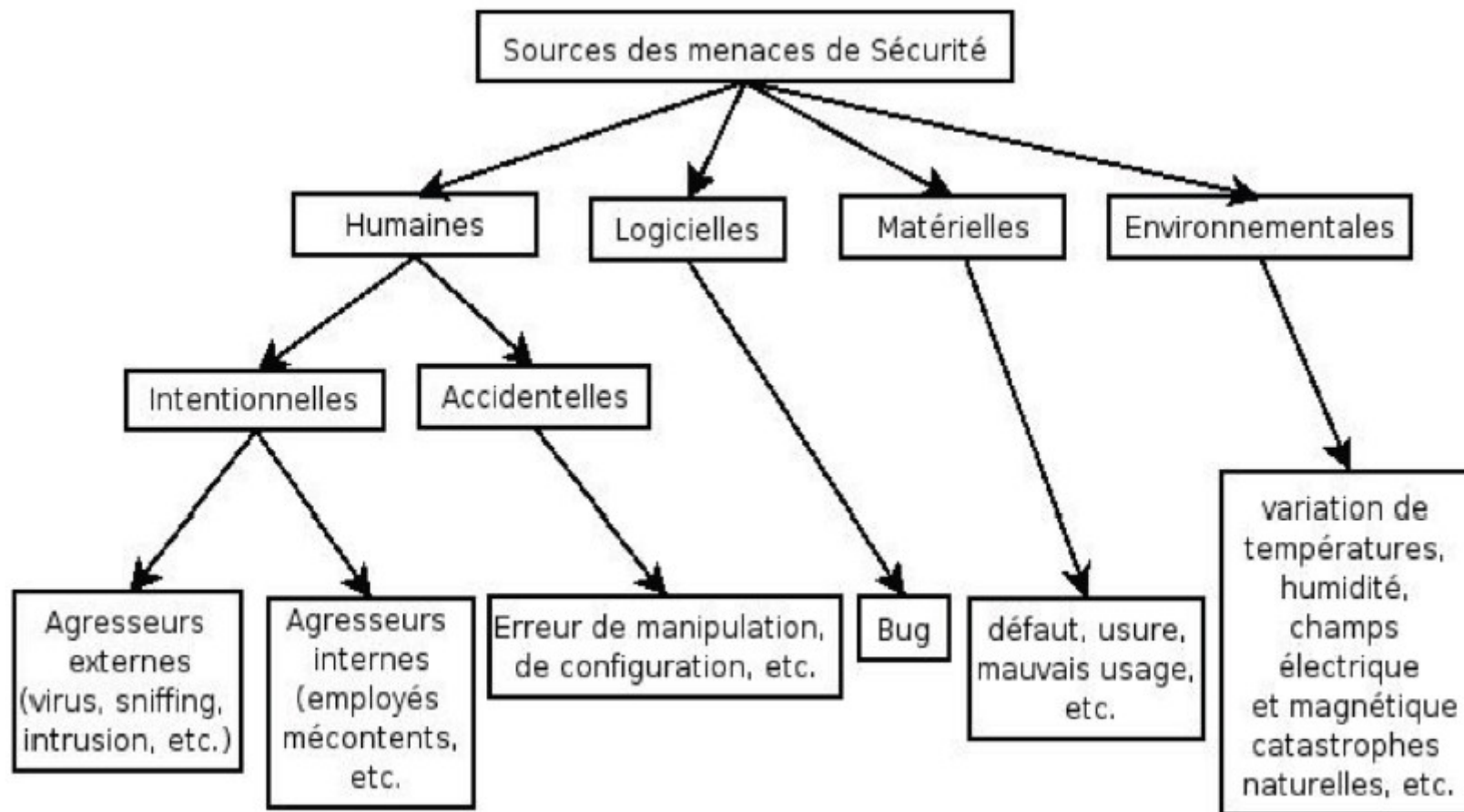
intrusions sur les SI

fraudes informatiques

chantage, extorsion informatique

intrusions, accès par un dispositif
sans fil

Sources des menaces



Vecteurs d'attaques

Vecteur	Exemple
Infrastructure exposée à Internet et infrastructure interne de l'organisation	Systèmes soutenant les applications, notamment les pare-feu, les routeurs, les commutateurs, les points d'accès et les serveurs pour les services accessibles de l'extérieur du périmètre de sécurité ⁹ .
Application	Produits applicatifs de type client lourd ¹⁰ , Web, mobiles, services Web, qu'ils soient conçus maison ou achetés (logiciels et progiciels).
Solution de sécurité	Systèmes ayant pour objectif de protéger les infrastructures ou les applications ¹¹ .
Bâtiment (sécurité physique)	Cartes d'accès, jetons, processus d'accès au bâtiment, processus de demande d'accès, absence de gardiens de sécurité pour surveiller l'accès au bâtiment, etc.
Humain	Comprend particulièrement l'ingénierie sociale. Par exemple, une personne malveillante pourrait abuser de la confiance d'un employé ou d'un dirigeant. Elle pourrait aussi mettre à l'épreuve un gardien de sécurité, un membre du personnel de l'entretien ménager, etc.

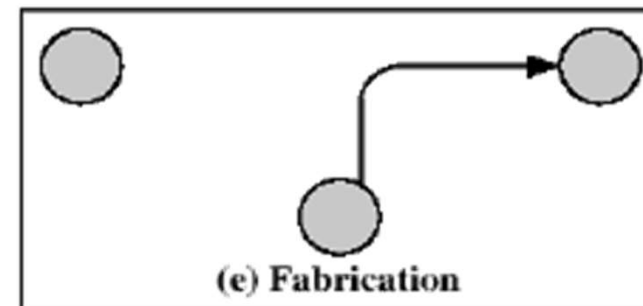
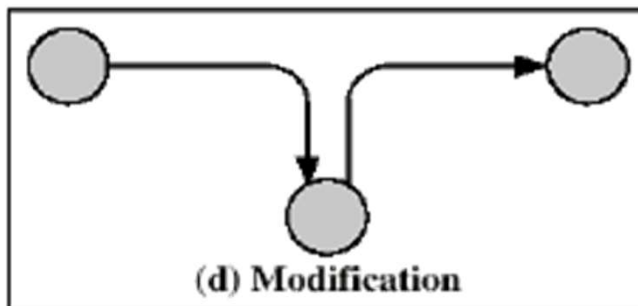
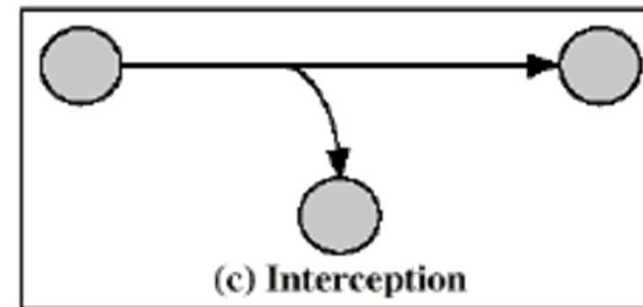
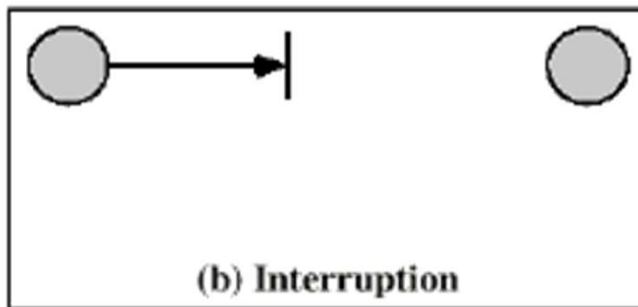
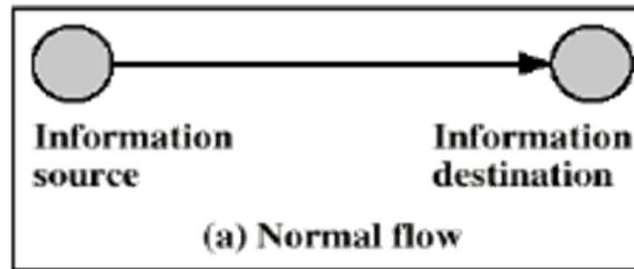
Panorama des accidents

- ▶ Incendie, explosion, implosion
- ▶ Dégât des eaux
- ▶ Problème d'intégrité du bâtiment
- ▶ Catastrophes naturelles
- ▶ Pannes
 - ▶ Internes (composant)
 - ▶ Logiciel de base
 - ▶ Externes (ex : climatisation, alimentation, ...)
- ▶ Arrêt de services (STEG, Télécommunications, eau, ...)
- ▶ Choc, collision, chute, pollution, rayonnement, ...

Panorama des erreurs

- ▶ Erreurs de saisie, de transmission de données
- ▶ Erreurs d'exploitation
- ▶ Erreurs de conception dans la réalisation ou la mise en œuvre des :
 - ▶ logiciels
 - ▶ procédures
- ▶ Disponibilité des personnes

Type des attaques



Attaques passives / actives

Attaques passives

- Divulgation de contenu
- Analyse de trafic

Attaques actives

- Mascarade
- Rejeu
- Modification de contenu
- Déni de service

Définition : Vulnérabilité

► Vulnérabilité :

- est une faute accidentelle ou intentionnelle (avec ou sans volonté de nuire), dans la spécification, la conception ou la configuration du système, ou dans la façon selon laquelle il est utilisé.
- peut être exploitée pour créer une intrusion.

Définition : Attaque

▶ Attaque :

- ▶ est une faute d'interaction malveillante visant à violer une ou plusieurs propriétés de sécurité
- ▶ est une faute externe créée avec l'intention de nuire
- ▶ peut être ou non réalisée par des outils automatiques

Définition : Intrusion

- ▶ Intrusion :

- ▶ est une faute malveillante interne, mais d'origine externe, résultant d'une attaque qui a réussi à exploiter une vulnérabilité.

Panorama des attaques

- ▶ Logiciels malveillants
- ▶ Attaques forgées

Logiciels malveillants

- ▶ Programmes qui exploitent les vulnérabilités du Système appelés “*malware*”
 - ▶ fragments de programmes nécessitant un programme hôte (virus, bombe logique, porte dérobée)
 - ▶ programmes autonomes indépendants (vers, robot) pouvant se répliquer ou non

Malware : Porte dérobée ("*backdoor*")

- ▶ Fonction d'un programme non autorisée et qui ne participe en rien aux objectifs officiels d'un programme
 - ▶ à priori malveillante
 - ▶ d'aucune utilité autre que pour son concepteur
 - ▶ s'exécute à l'insu de l'utilisateur

Malware : Cheval de Troie ("*Tojan*")

- ▶ Programme, jeu, commande ayant une fonction annoncée et en réalisant une autre (illicite)
 - ▶ attaque classique
 - ▶ s'exécute à l'insu de l'utilisateur

Malware : Bombe logique

- ▶ Action malveillante généralement différée
 - ▶ chantage
 - ▶ racket

Malware : Virus

- ▶ Programme illicite qui s'insère dans des programmes légitimes appelés hôtes
 - ▶ se reproduit automatiquement, se transmet,
 - ▶ peut avoir des actions retardées
 - ▶ se répand au travers d'internet, de disquettes, de clés USB
- ▶ Se compose de :
 - ▶ mécanisme d'infection : permet la réplication
 - ▶ déclenchement : évènement qui rend la charge active
 - ▶ charge du virus : ce qu'il fait, action malveillante

Malware : Virus / Structure

```
program V :=  
  
{goto main;  
 1234567;  
  
  subroutine infect-executable :=  
    {loop:  
      file := get-random-executable-file;  
      if (first-line-of-file = 1234567)  
        then goto loop  
        else prepend V to file; }  
  
  subroutine do-damage :=  
    {whatever damage is to be done}  
  
  subroutine trigger-pulled :=  
    {return true if some condition holds}  
  
main:  main-program :=  
      {infect-executable;  
      if trigger-pulled then do-damage;  
      goto next;}  
  
next:  
  
}
```

Malware : Virus / Type

- ▶ virus d'amorçage
- ▶ virus programme
- ▶ virus de macro
- ▶ virus e-mail
- ▶ virus chiffré
- ▶ virus furtif
- ▶ virus polymorphe
- ▶ virus métamorphique

Malware : Vers ("*Worm*")

- ▶ Processus parasite qui consomme, détruit et se propage sur le réseau
 - ▶ n'a pas besoin d'un programme hôte pour se reproduire (contrairement au virus)
 - ▶ se reproduit par ses propres moyens sans contaminer de programme hôte
 - ▶ souvent écrits sous forme de script intégrés dans un e-mail, une page html

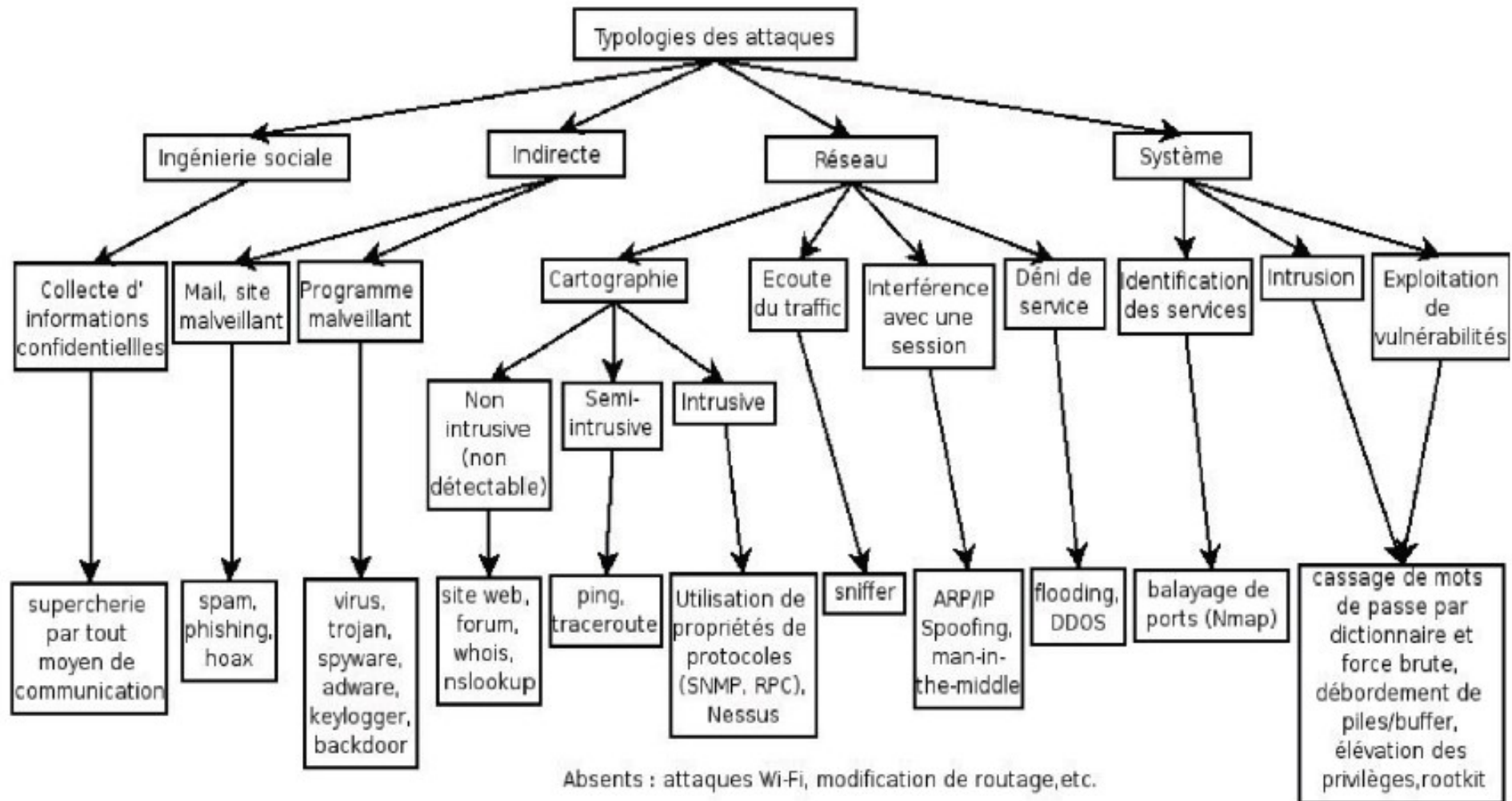
Malware : Canular ("*Hoax*")

- ▶ Messages diffusant :
 - ▶ de fausses alertes au virus
 - ▶ des rumeurs
- ▶ Visant à :
 - ▶ Encombrer les boîtes aux lettres
 - ▶ Encombrer le réseau
 - ▶ Ralentir l'activité normale sur le système

Attaque forgée

- ▶ ou attaque par manipulation
- ▶ attaque basée sur la manipulation des éléments de la communication afin d'en tirer profit ou de nuire

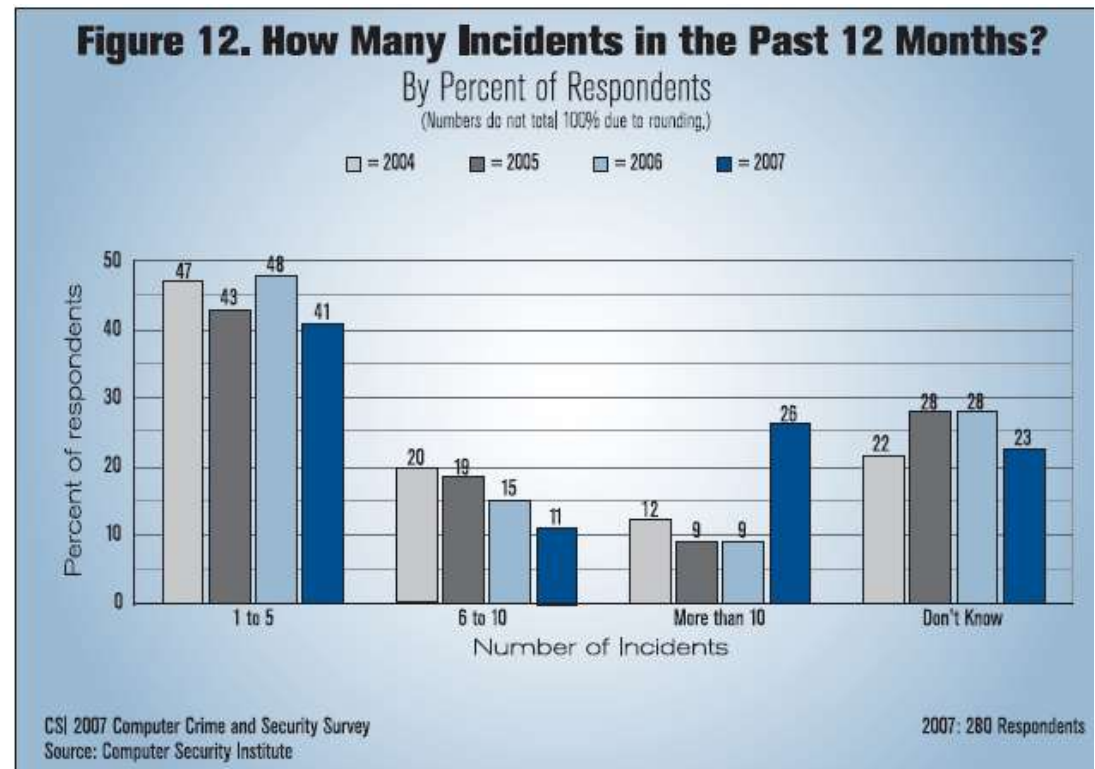
Typologie des attaques



Sécurité des systèmes informatiques

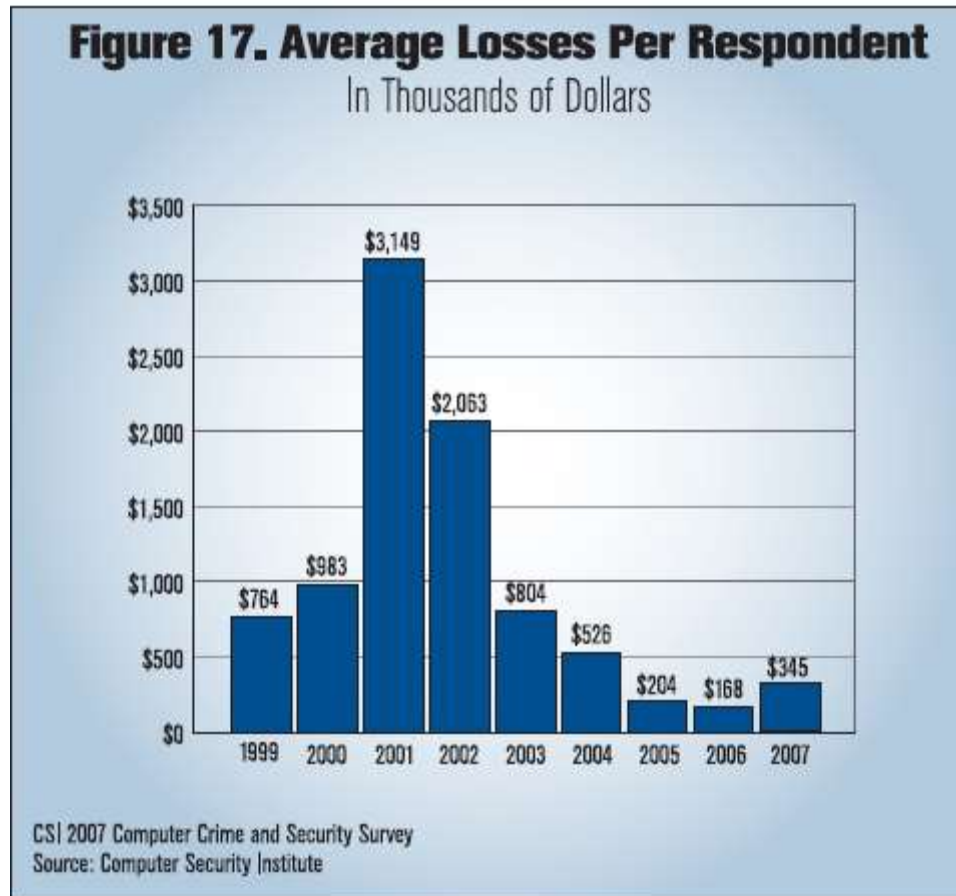
Enjeux pour les entreprises

- ▶ Attaque et intrusion : comportements hostiles dirigés au sein du réseau.
- ▶ Confidentialité de l'information
- ▶ Intégrité
- ▶ Disponibilité
- ▶ Non répudiation



Sécurité des systèmes informatiques

Enjeux pour les entreprises



> Perte de capitaux pour les entreprises.

> Palmarès des systèmes de sécurité mis en œuvre :

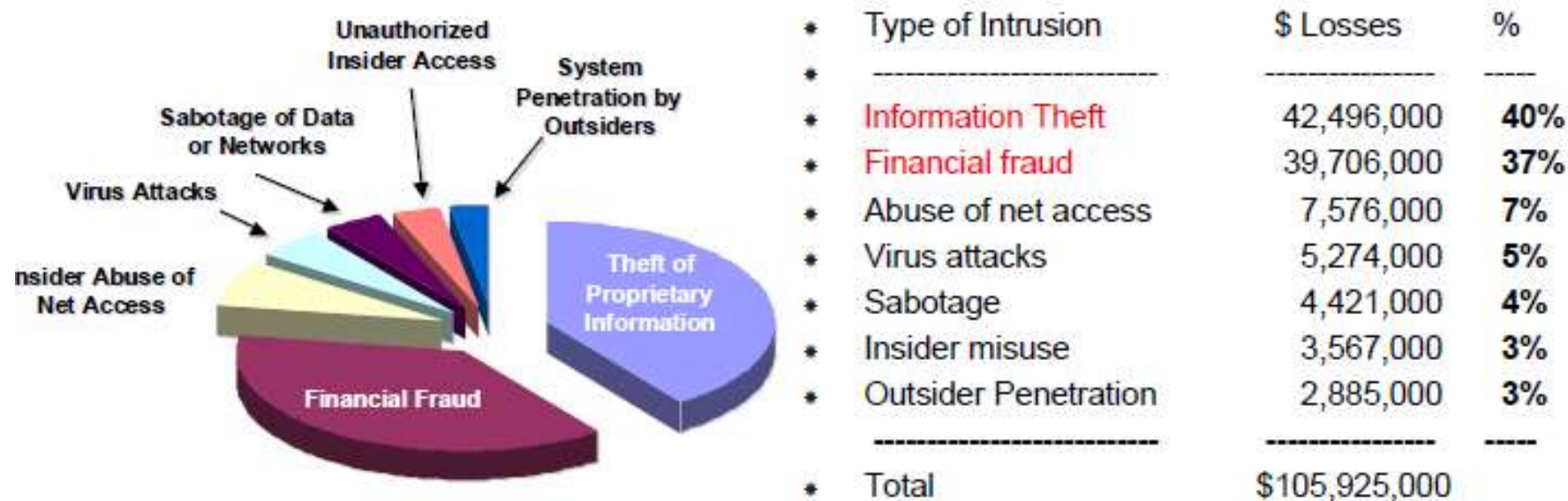
- 1. Firewall.
- 2. Antivirus.
- 3. VPN.
- 4. IDS.



Nécessité de se prémunir contre les attaques.

Sécurité des systèmes informatiques

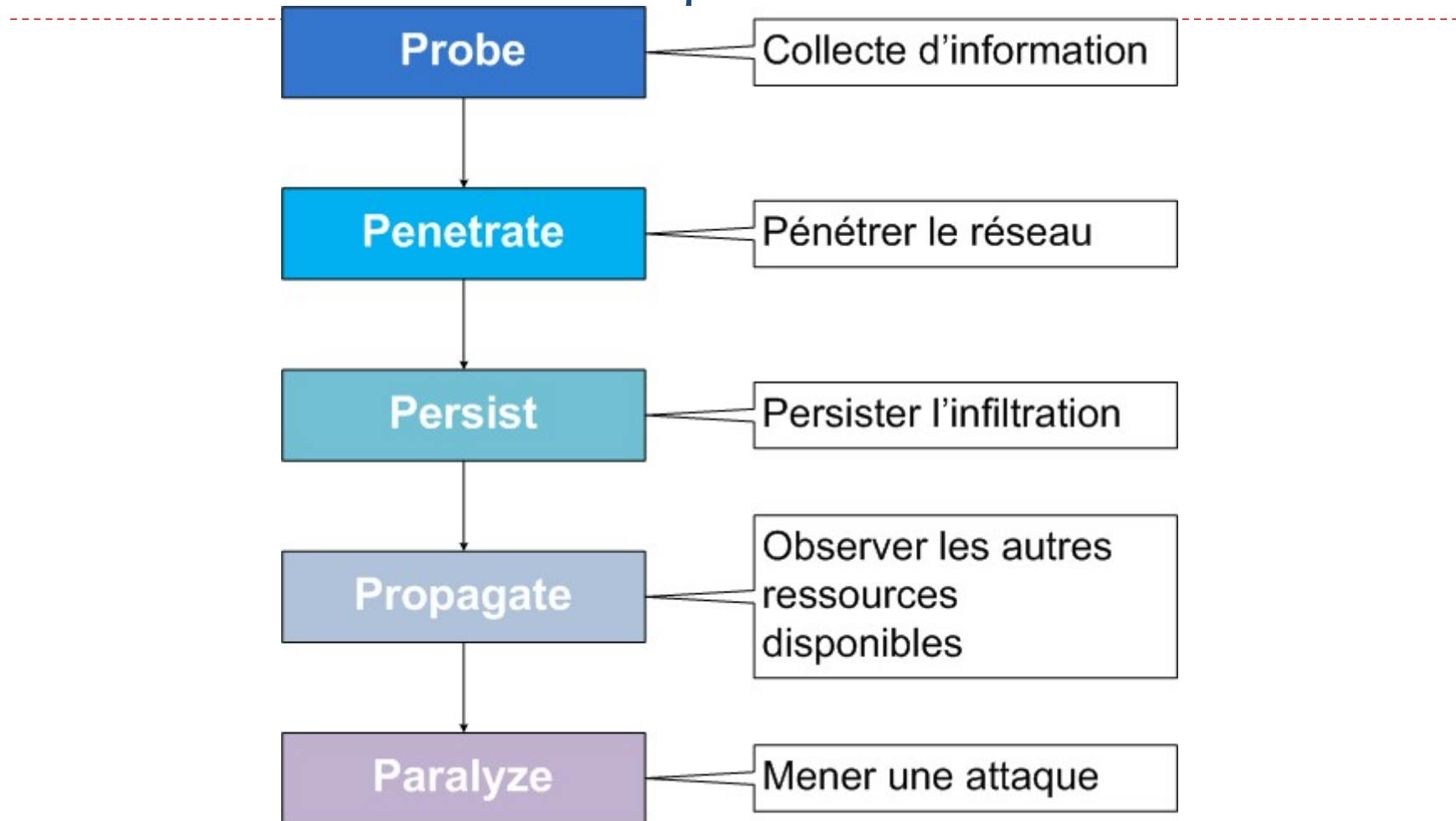
Enjeux pour les entreprises



Source: "1999 CSI/FBI Computer Crime and Security Survey" Computer Security Institute - www.gocsi.com/losses.htm

Sécurité des systèmes informatiques

Anatomie d'une attaque



Les 5 « P ».

Phase 1 : collecte d'informations

- ▶ Collecte passive
- ▶ Collecte active

Collecte passive : Whois

- ▶ La base Whois est une base renseignée par les registrars Internet.
- ▶ Whois est normalisé par la RFC 3912
- ▶ Elle renseigne sur l'appartenance d'une adresse IP ou de noms de domaines :
 - ▶ Nom de domaine
 - ▶ Registrar (organisme s'occupant de la gestion de nom de domaine)
 - ▶ URL du serveur Whois de ce registrar
 - ▶ URL du site du registrar
 - ▶ Serveurs DNS (dans la base Internic)
 - ▶ Date de dernière modification
 - ▶ Adresse du propriétaire du nom de domaine
 - ▶ Adresse de l'administrateur du nom de domaine
 - ▶ Adresse du contact technique du nom de domaine
 - ▶ Date de modification, création, et expiration du nom de domaine
 - ▶ Serveurs DNS (dans la base du registrar)

Collecte passive : Whois, exemple

Résultats pour le domaine "google.fr"

```
%  
% This is the AFNIC Whois server.  
%  
% complete date format : DD/MM/YYYY  
% short date format : DD/MM  
% version : FRNIC-2.5  
%  
% Rights restricted by copyright.  
% See https://www.afnic.fr/en/products-and-services/services/whois/whois-  
special-notice/  
%  
% Use '-h' option to obtain more information about this service.  
%  
% [151.80.122.100 REQUEST] >> -V Md5.1 google.fr  
%  
% RL Net [#####] - RL IP [#####.]  
%  
  
domain: google.fr  
status: ACTIVE  
hold: NO  
holder-c: GIH6-FRNIC  
admin-c: GIH5-FRNIC  
tech-c: CP4370-FRNIC  
zone-c: NFC1-FRNIC  
nsl-id: NSL4386-FRNIC  
registrar: MARKMONITOR Inc.  
Expiry Date: 30/12/2017
```

Collecte passive : nslookup exemple

C:\ Invite de commandes

```
Microsoft Windows [version 10.0.14393]
(c) 2016 Microsoft Corporation. Tous droits réservés.

C:\Users\DELL>nslookup www.google.fr
Serveur : UnKnown
Address: 192.168.1.1

Réponse ne faisant pas autorité :
Nom : www.google.fr
Addresses: 2a00:1450:4002:807::2003
           216.58.205.67
```


Collecte passive : RIPE

Responsible organisation: [OVH SAS](#)
Abuse contact info: abuse@ovh.net

inetnum: [188.165.48.0 - 188.165.55.255](#)
netname: OVH
descr: OVH SAS
country: FR
admin-c: [OK217-RIPE](#)
tech-c: [OTC2-RIPE](#)
status: ASSIGNED PA
mnt-by: [OVH-MNT](#)
created: 2016-06-13T09:44:27Z
last-modified: 2016-06-13T09:44:27Z
source: RIPE

role: OVH Technical Contact
address: OVH SAS
address: 2 rue Kellermann
address: 59100 Roubaix
address: France
e-mail: noc@ovh.net
admin-c: [OK217-RIPE](#)
tech-c: [GM84-RIPE](#)
tech-c: [SL10162-RIPE](#)
nic-hdl: [OTC2-RIPE](#)

Collecte passive : moteur de recherche

- ▶ Permettre la récupération d'informations.
- ▶ Exemple :
 - ▶ Permettre de connaître des noms de machines
 - ▶ En déduire une logique de noms afin de découvrir d'autres noms d'hôtes
 - ▶ Récupérer simplement des adresses e-mail qui sont souvent liés à de simple nom d'utilisateur.
- ▶ Google dork :
 - ▶ Inurl
 - ▶ Filetype
 - ▶ Intitle
 - ▶ ...

Collecte passive : sniffing

- ▶ Réseau de type "broadcast"
- ▶ Re-direction de flux permettrait de récupérer pendant un instant un trafic illégitime.
- ▶ Sniffing de trames (ou écoute de trames) peut permettre de récupérer des informations sensibles. Exemples :
 - ▶ des mots de passes
 - ▶ des logins
- ▶ Outils :
 - ▶ Tcpdump
 - ▶ Ethereal

Recherche active : récupération des informations DNS

- ▶ La commande `host` permet de récupérer sur le serveur DNS laissant sortir trop d'informations au public des informations sur la topologies d'un réseau.

- ▶ Exemple :

`host -a -l cible`

permet de lister tous les hôtes d'un domaine.

- ▶ La plupart du temps, les serveurs DNS sont bien configurés et les requêtes de transferts de zones sont filtrées aux hôtes légitimes (comme les serveurs DNS secondaires).

Recherche active : firewalking

- ▶ Le firewalking est un ensemble de techniques permettant de faire une cartographie du réseau et d'en déduire la présence des points de protection tels que les firewalls.
- ▶ Il est basé sur les techniques utilisant le champs TTL des datagrammes IP tels que
 - ▶ traceroute
 - ▶ hping

Recherche active : firewalking

traceroute

- ▶ Principe de fonctionnement :
 - ▶ envoyer des paquets UDP (TCP / ICMP) avec un paramètre Time-To-Live (TTL) de plus en plus grand (en commençant à 1)
 - ▶ chaque routeur qui reçoit un paquet IP en décrémente le TTL avant de le transmettre
 - ▶ lorsque le TTL atteint 0, le routeur émet un paquet ICMP d'erreur Time to live exceeded vers la source
 - ▶ traceroute découvre ainsi les routeurs de proche en proche
- ▶ Exemple :
 - ▶ Windows :
 - ▶ C:\WINDOWS>tracert fr.wikipedia.org
 - ▶ Linux :
 - ▶ traceroute fr.wikipedia.org

Recherche active : firewalking

hping

- ▶ Hping permet de :
 - ▶ Forger soit même ses propres paquets.
 - ▶ Simuler le comportement de l'utilitaire traceroute en utilisant des paquets TCP au lieu de l'UDP ou de l'ICMP.
 - ▶ Permet de passer un firewall qui bloquerai juste les requêtes ICMP ou UDP.
 - ▶ L'option -t permet de modifier le champs TTL d'un paquet IP.
 - ▶ L'option -p permet de spécifier le port TCP à utiliser , avec les flags voulu (-A : Ack, -S : Syn, -R : Reset, -F Fin).

Recherche active : firewalking

scan des ports

- ▶ Un scan de ports permet :
 - ▶ de déterminer les ports ouverts sur une machine
 - ▶ de déterminer le système d'exploitation d'une machine (par le fingerprinter de sa pile TCP/IP)
- ▶ L'outil de référence pour le scan de port est **Nmap**.

Recherche active : firewalking

scan des ports

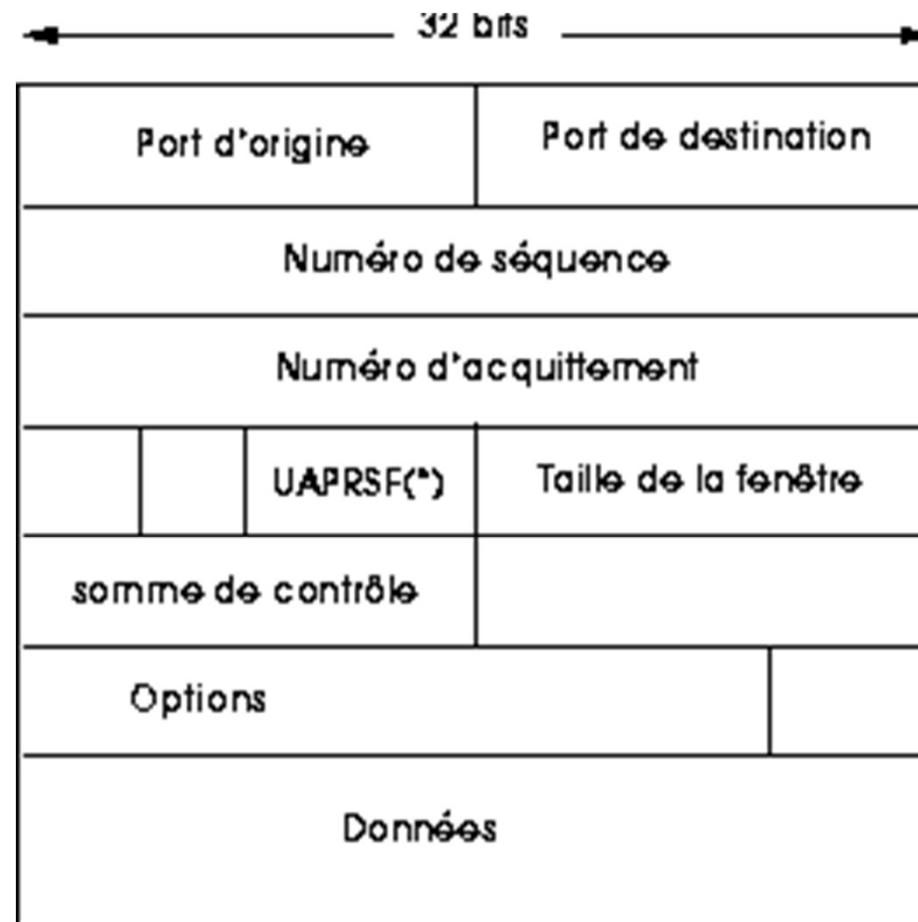
► Exemple de capture avec nmap :

```
# nmap 192.168.0.1

Starting nmap 3.81 ( http://www.insecure.org/nmap/ ) at 2006-01-23 00:49 CET
Interesting ports on 192.168.0.1:
(The 1652 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
81/tcp    open  hosts2-ns
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
893/tcp   open  unknown
913/tcp   open  unknown
2049/tcp  open  nfs
3128/tcp  open  squid-http
MAC Address: 00:04:76:24:D0:DF (3 Com)

Nmap finished: 1 IP address (1 host up) scanned in 0.802 seconds
```

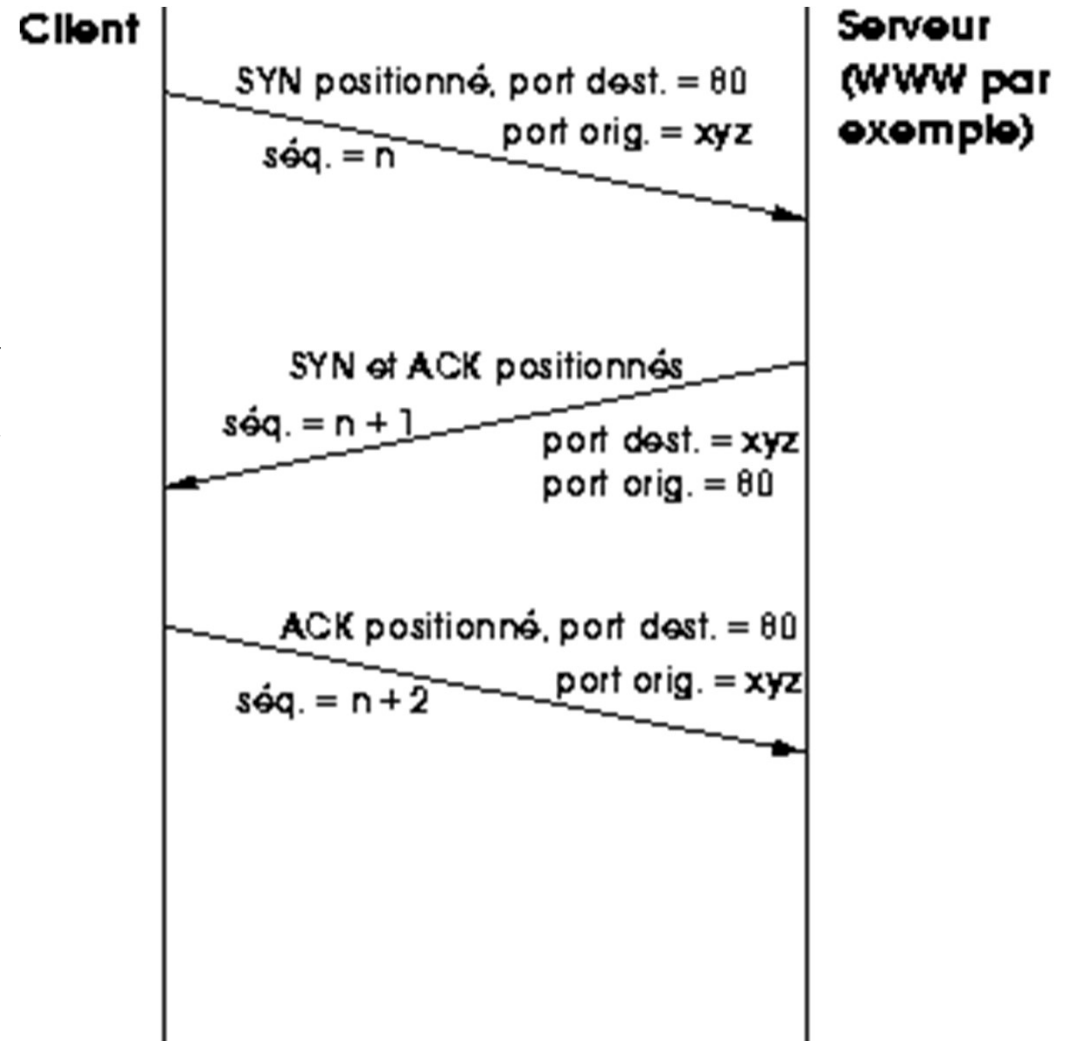
Rappel : Communication TCP



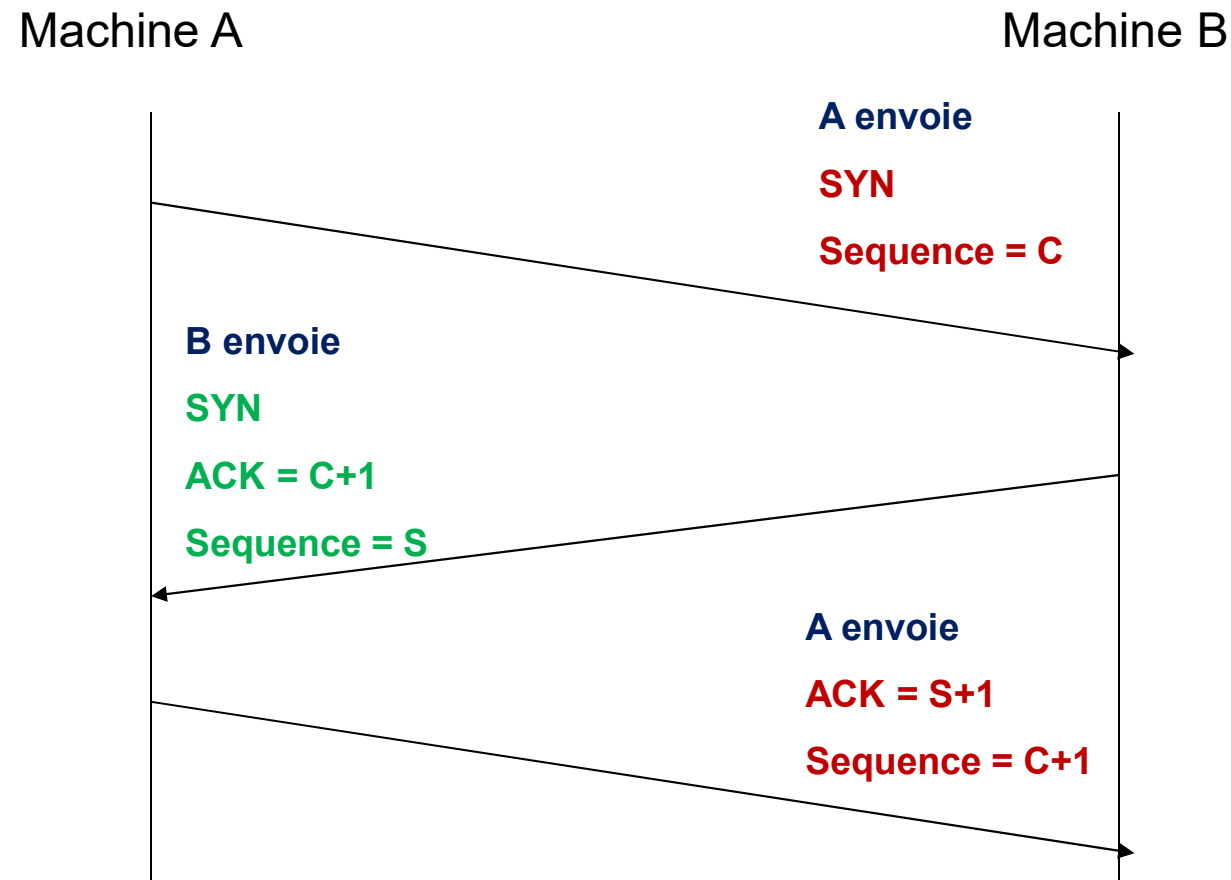
(*) UAPRSF : champs de 6 bits de contrôle :
URG ACK PSH RST SYN FIN

Rappel : Communication TCP

- ▶ Avant tout transfert de données, TCP ouvre donc une connexion, ce qui se passe selon la procédure suivante appelée poignée de main en trois étapes (*three-way handshake*)



Rappel TCP: Etablissement d'une connexion



Rappel : Communication TCP

- ▶ Le nœud à l'origine de la demande de communication (appelé communément le client) émet un segment TCP avec le bit SYN positionné, le numéro de port du serveur avec lequel le client veut communiquer dans le champ port de destination de l'en-tête de segment, un numéro de port arbitraire dans le champ port d'origine, les adresses d'origine et de destination convenables dans l'en-tête de datagramme. Le numéro de séquence est également initialisé dans l'en-tête de segment.
- ▶ Le serveur répond en acquittant ce message au moyen d'un segment dont le bit SYN est lui aussi positionné, le bit ACK positionné également, les numéros de ports et adresses d'origine et de destination logiquement inversés par rapport au segment du client.
- ▶ Le client acquitte lui-même ce message en renvoyant un segment avec le bit ACK positionné. À l'issue de cet échange en trois temps, client et serveur sont réputés s'être mis d'accord sur les numéros de ports nécessaires à l'établissement de la connexion.

Rappel : signification des drapeaux

- ▶ Drapeaux (flags) (6x1 bit): Les drapeaux représentent des informations supplémentaires :
- ▶ URG: si ce drapeau est à 1 le paquet doit être traité de façon urgente.
- ▶ ACK: si ce drapeau est à 1 le paquet est un accusé de réception.
- ▶ PSH (PUSH): si ce drapeau est à 1, le paquet fonctionne suivant la méthode PUSH.
- ▶ RST: si ce drapeau est à 1, la connexion est réinitialisée.
- ▶ SYN: Le Flag TCP SYN indique une demande d'établissement de connexion.
- ▶ FIN: si ce drapeau est à 1 la connexion s'interrompt.

Le scan

- ▶ Permet de découvrir les protocoles et ports ouverts sur les différents équipements réseaux
- ▶ Peut être comparé à un cambrioleur qui frappe contre toutes les portes et fenêtres de la maison pour savoir si l'une d'entre elle est ouverte, fermée ou protégée
- ▶ TCP et UDP utilisent les numéros de ports pour identifier les services des couches supérieures

Exemples de scan furtif (1)

▶ SYN/ACK scan

- ▶ Machine A envoie un SYN/ACK
- ▶ Machine B répond par RST si le port est ouvert et ne renvoie rien si le port est fermé

▶ TCP FIN

- ▶ En principe, le segment FIN est envoyé pour fermer une connexion TCP ouverte
- ▶ Machine A envoie un segment FIN
- ▶ Machine B
 - ▶ N'envoie rien si le port est ouvert ou actif, il ignore le packet FIN puisqu'il n'y a pas une connexion
 - ▶ Envoie un RST si le port est fermé
 - ▶ Dans le cas de l'OS Windows, FIN=RST

Exemple de scan furtifs (2)

- ▶ Le NULL scanning
 - ▶ Suppression de tous les indicateurs dans l'entête TCP (ACK, FIN, RST, SYN, URG, PSH)
 - ▶ La RFC 793 dit qu'il faut envoyer un RST si le port est fermé, ne rien envoyer si le port est ouvert
- ▶ Le XMAS scanning (balayage de Noël)
 - ▶ Opposé du Null Scanning, le hacker envoie un entête ayant tous les flag
 - ▶ La RFC 793 dit qu'il faut renvoyer un RST pour tous les ports fermés, ne rien envoyer si le port est ouvert
 - ▶ Ne fonctionne que sur les machines UNIX

UDP ICMP PORT Unreachable Scanning

- ▶ UDP n'est pas orienté connexion
 - ▶ Plus difficile à scanner que TCP
 - ▶ Les ports UDP ne sont pas tenus à répondre à des sondage
- ▶ Si port fermé = renvoie d'une erreur ICMP (port_unreachable)
- ▶ Si pas de réponse, le port est actif

Scanners de ports (1)

- ▶ L'outil le plus utilisé : nmap
 - ▶ Ne scanne pas l'ensemble des ports mais uniquement 3,5%, soit 172 ports
 - ▶ Utilise un balayage furtif par défaut
 - ▶ Capable de traverser les filtres, pare-feu et routeurs
 - ▶ Capable d'apparaître comme un trafic occasionnel de réseau

- ▶ `[root@localhost ~]# nmap 192.168.1.3`

Starting Nmap 4.00 (<http://www.insecure.org/nmap/>) at 2009-05-17 20:17 CET

Interesting ports on 192.168.1.3:

(The 1671 ports scanned but not shown below are in state: closed)

PORT	STATE	SERVICE
------	-------	---------

3306/tcp	open	mysql
----------	------	-------

Nmap finished: 1 IP address (1 host up) scanned in 13.296 seconds

Scanners de ports (2)

- ▶ Utiliser cette règle dans votre firewall et 80% des scans de ports seront bloqués sur le FW

- ▶ **[root@localhost ~]# iptables -I INPUT -p tcp --tcp-option ! 8 -j DROP**

- ▶ **[root@localhost ~]# nmap 192.168.1.3**

Starting Nmap 4.00 (<http://www.insecure.org/nmap/>) at 2009-05-17 20:24 CET

All 1672 scanned ports on 192.168.1.3 are: filtered

Nmap finished: 1 IP address (1 host up) scanned in 351.355 seconds

A retenir

- ▶ La règle fondamentale de la sécurité des applications est de désactiver tout service TCP/UDP non utilisé car tout service offre aux personnes mal intentionnées une possibilité de pénétrer dans le coeur du système d'information

Les RPCs (1)

- ▶ Lorsqu'un service RPC est découvert, il fournit une liste de services disponibles
- ▶ Interrogeable à l'aide du programme **rpcinfo**
- ▶ Exemple:
 - ▶ **rpcinfo -p 192.168.10.2**
- ▶ Le service RPC est utilisé par les serveurs NFS pour l'export de ressources (partage du SF)

Les RPCs (2): ce qu'il faut vérifier

- ▶ S'assurer que seuls les PCs autorisés ont droit à accéder aux services RPC
 - ▶ Exemple sous linux: Vérifier l'entrée relative au *portmap* dans le fichier `/etc/hosts.allow`
- ▶ Pour le cas des serveurs NFS, s'assurer que les répertoires sont exportés aux PCs autorisés avec l'option “**read only**”
 - ▶ Exemples de configuration dans le fichier `/etc/exports`:
 - ▶ `/tmp * (ro)`
 - ▶ `/usr/local/man *.archinet.edu (ro, insecure)`

Manipulation : Hameçonnage ("*Phishing*")

- ▶ Action visant à piéger l'utilisateur en lui faisant croire qu'il s'adresse à un tiers de confiance pour lui soutirer des informations confidentielles :
 - ▶ Mot de passe
 - ▶ Numéro de carte de crédit
 - ▶ Tout type d'informations pouvant être réutilisées dans une attaque future

Manipulation : Craquage ("*Cracking*")

- ▶ craquage des mots de passe pour un accès ou une utilisation non autorisée :
 - ▶ à l'aveuglette
 - ▶ comparaison du chiffrement de mots de passe supposés et de mots chiffrés dans le fichier des mots de passe

Manipulation : Renfilage ("*Sniffing*")

- ▶ Analyse du trafic pour récupérer des informations confidentielles
 - ▶ sondes placées sur le réseau pour écouter et récupérer des informations à la volée

Manipulation : Mascarade ("*Spoofing*")

- ▶ Utilisation de l'adresse IP d'une machine afin d'en usurper l'identité.
 - ▶ récupération de l'accès à des informations en se faisant passer la machine dont l'identité a été usurpée
 - ▶ création de paquets IP avec une adresse IP source appartenant à quelqu'un d'autre

Manipulation : "*Smurfing*"

- ▶ Attaque du réseau IP par l'envoi d'un message à une adresse IP inexistante
- ▶ Provoque la saturation et le blocage du réseau

Manipulation : Dénie de service (DOS)

- ▶ Rendre une application informatique incapable de répondre aux requêtes des utilisateurs
- ▶ Différentes attaque possibles:
 - ▶ débranchement physique d'un serveur
 - ▶ saturation d'un élément chargé d'animer l'application

Manipulation : Dénie de service distribué (DDoS)

- ▶ Repose sur la multiplication d'attaques DoS menées simultanément par plusieurs systèmes