Chapitre II :

Vulnérabilité d'un système d'information

Préparé par : Hajer Gahbiche

Plan

- Vulnérabilité d’un système d’information
  - Vulnérabilité des utilisateurs
  - Vulnérabilité des réseaux
  - Vulnérabilité du Web

Vulnérabilité d’un système d’information

- Les virus informatique
- Le cycle de vie d’un virus
- Classification des virus

Les virus informatique

➢Définition

Un virus informatique est un programme capable d'infecter d'autres programmes en les modifiant pour y inclure une copie de lui-même.

Le virus ne peut pas fonctionner d'une manière indépendante, l'exécution d'un programme hôte est nécessaire pour son activation Fred Cohen

Les virus informatique

Un virus informatique peut être :

- simple
- auto-producteur

Les virus informatique: simple

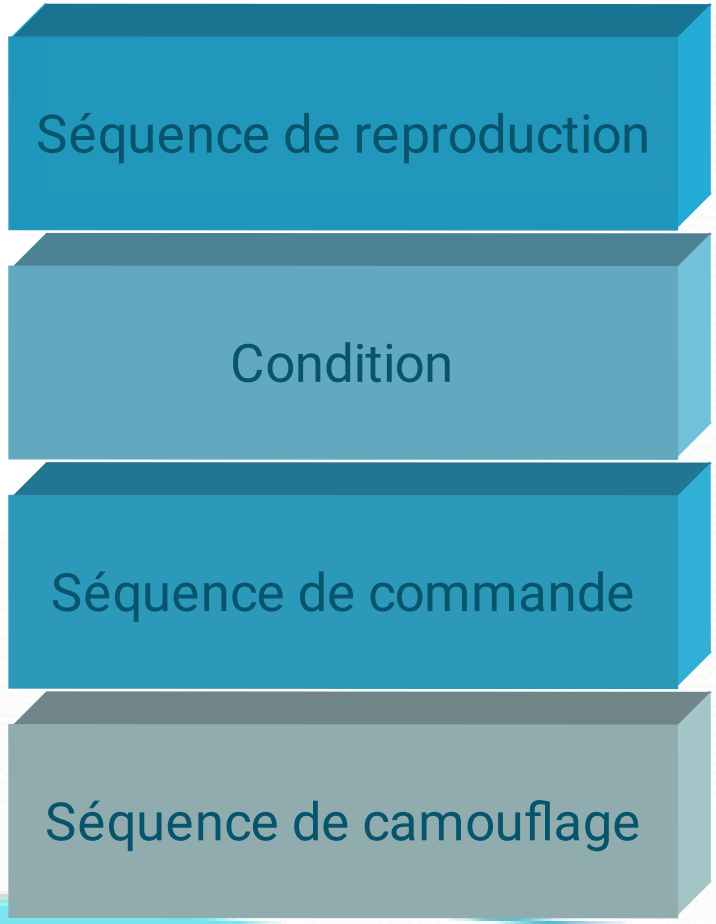
- Il contient une fonctionnalité malveillante qui se déclenche lors de son excusions.
- Il n’y a pas de propagation.
- L’action induite par ce virus peut avoir une action destructive ou perturbatrice.
- Elle peut être retardé ou immédiate dans le temps.

Les virus informatique: auto-producteur

- Le but d’un programme auto-producteur est celle d’un programme simple : destruction ou perturbation
- Il y a une propagation
- À sa première exécution le programme cherche à se reproduire et à se propager. Ces actions peuvent causer plusieurs ennuis.
- La fonction malveillante, si elle existe, peut être effectuée dans un délai très court, sur un critère bien défini.

Les virus informatique

➢ Composantes d'un virus [1]



Vulnérabilité d'un système d'information

- Les virus informatique
- Le cycle de vie d'un virus
- Classification des virus

Le cycle de vie d'un virus (1/2)

- **La création** : c'est la période pendant laquelle le programmeur va développer un virus.

- **La gestation** : c'est la période pendant la quel le virus est copié dans un endroit stratégique (CD-ROM, DVD, Serveur Web, Serveur VoD…) à fin que sa diffusion soit le rapide que possible.

- **La reproduction (l'infection)** : le virus cherche à se reproduire un nombre de fois important avant son activation.

- **L'activation** : il s'agit de la condition d'activation (réveil) du virus. Cette condition peut être un événement, une date…

Le cycle de vie d’un virus (2/2)

- **La découverte** : il s’agit du moment dans le quel quelqu'un se rend compte de l’existence d’un virus et arrive à l'isoler.

- **L’assimilation :** Les éditeurs des antivirus essaie de trouver des moyens de parer le virus.

- **L’irradiation** : Cette phase consiste à supprimer complètement un virus. Cette phase n’est possible que si tous les utilisateurs admettent l’antivirus adéquat (capable de détecter ce virus et qui est mis à jours).

Le cycle de vie d'un virus (1/2)

- **La création** : c'est la période pendant la quel le programmeur va développer un virus.

- **La gestation** : c'est la période pendant la quel le virus est copié dans un endroit stratégique (CD-ROM, DVD, Serveur Web, Serveur VoD…) à fin que sa diffusion soit le rapide que possible.

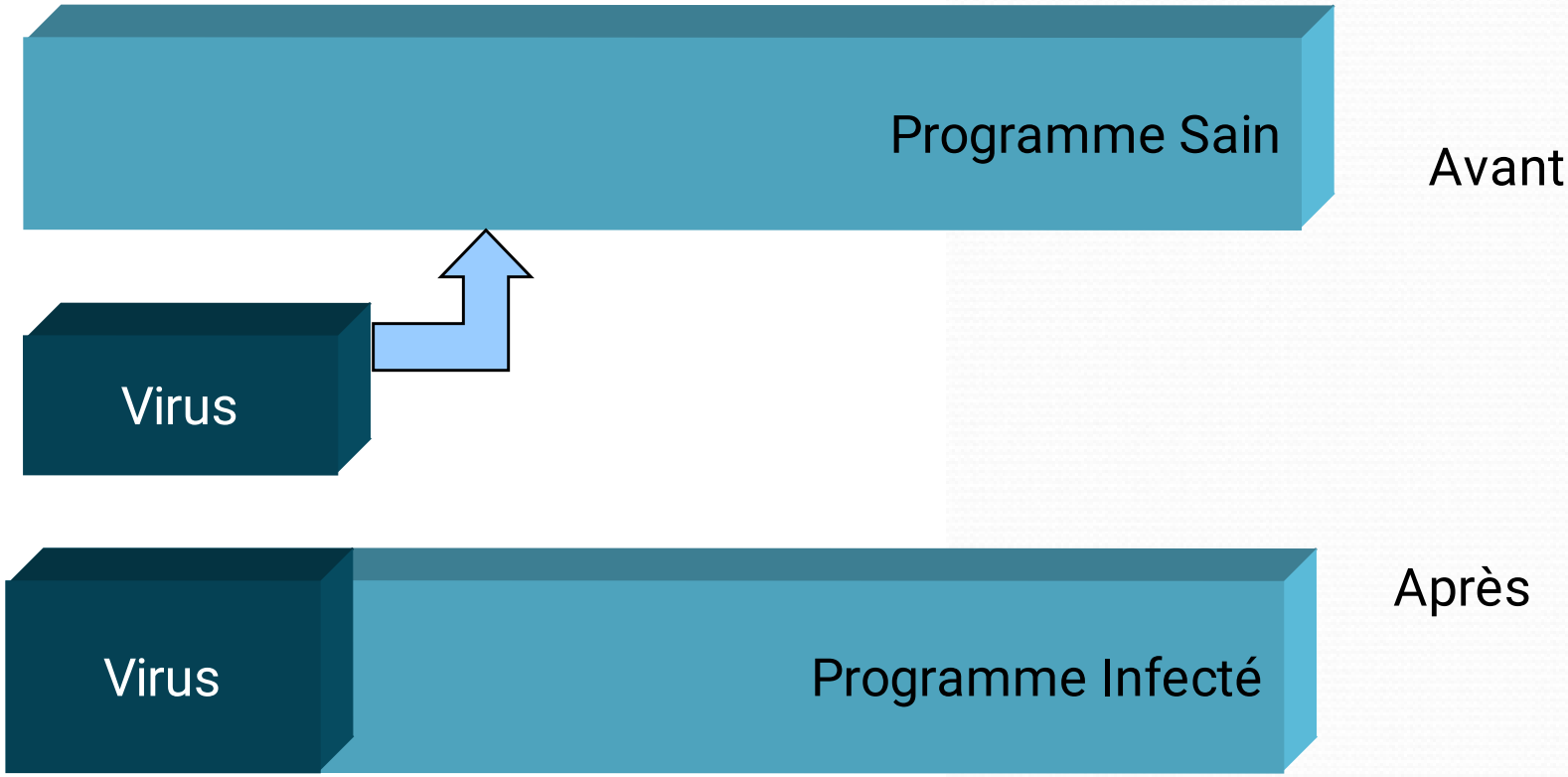
- **La reproduction (l'infection)** : le virus cherche à se reproduire un nombre de fois important avant son activation.

- **L'activation** : il s'agit de la condition d'activation (réveil) du virus. Cette condition peut être un événement, une date…

Le cycle de vie d’un virus : La reproduction [2]

- Recouvrement
- Ajout
- Cavité
- Par virus Compagnon

La reproduction : Recouvrement

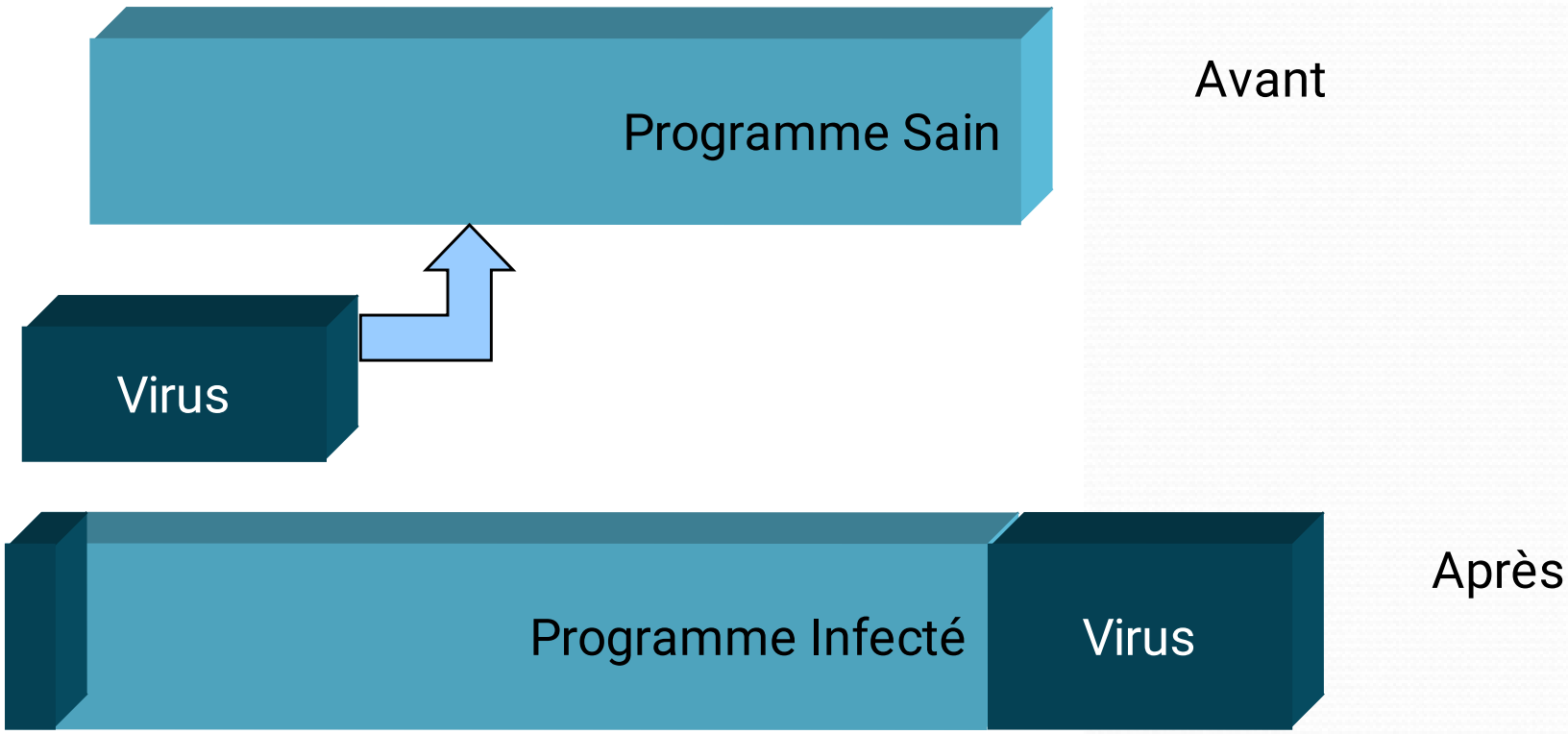


- Le virus écrase une partie du programme, ou bien totalement un programme.
- Il rend son irradiation impossible.
- La taille du programme originale n'est pas modifié.

Le cycle de vie d’un virus : La reproduction

- Recouvrement
- Ajout
- Cavité
- Par virus Compagnon

La reproduction : Ajout



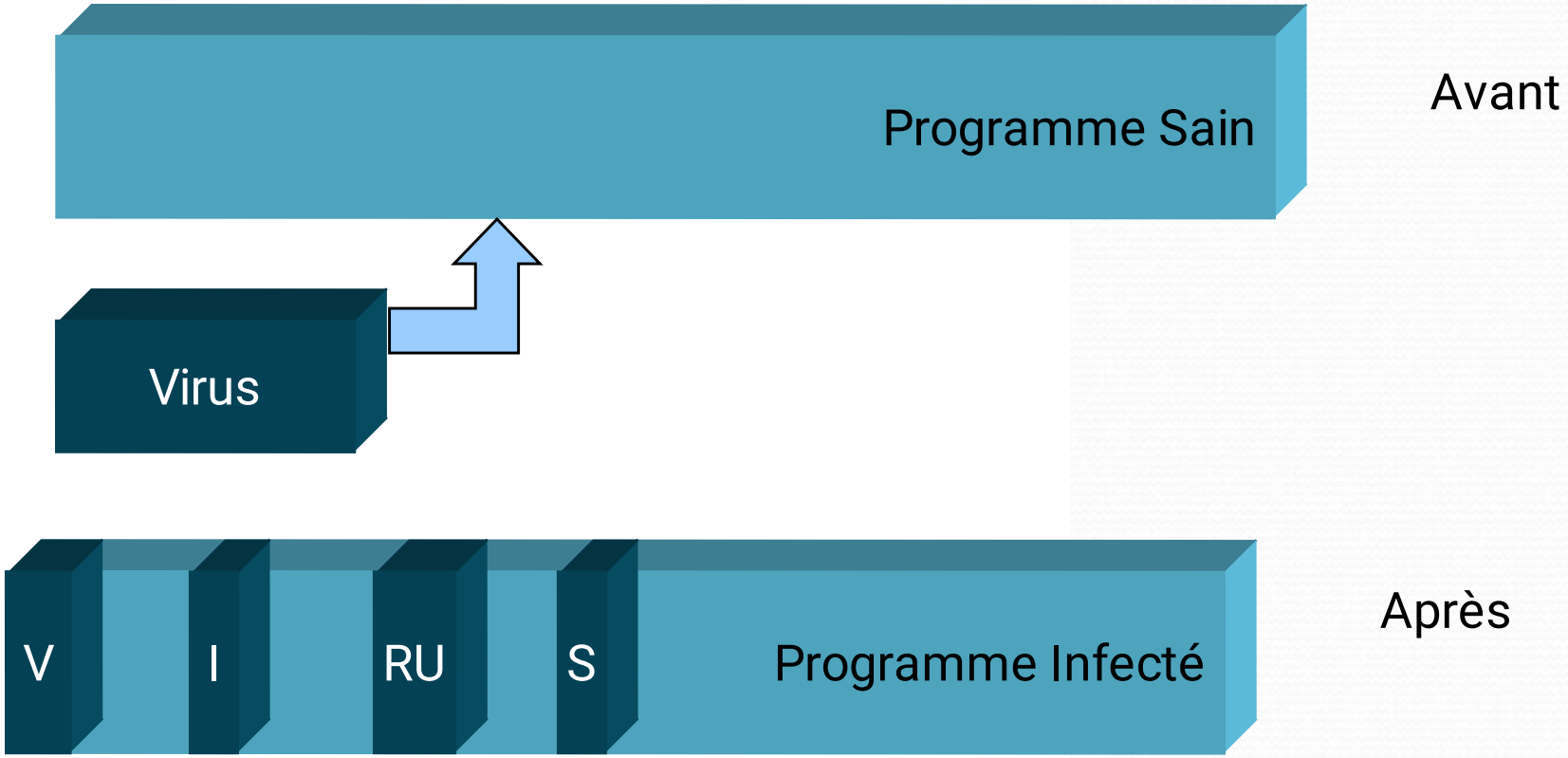
- Cette technique modifie un programme sans le détruire.

-Le virus s'exécute chaque fois que le programme est lancé.

Le cycle de vie d’un virus : La reproduction

- Recouvrement
- Ajout
- Cavité
- Par virus Compagnon

La reproduction : Cavité



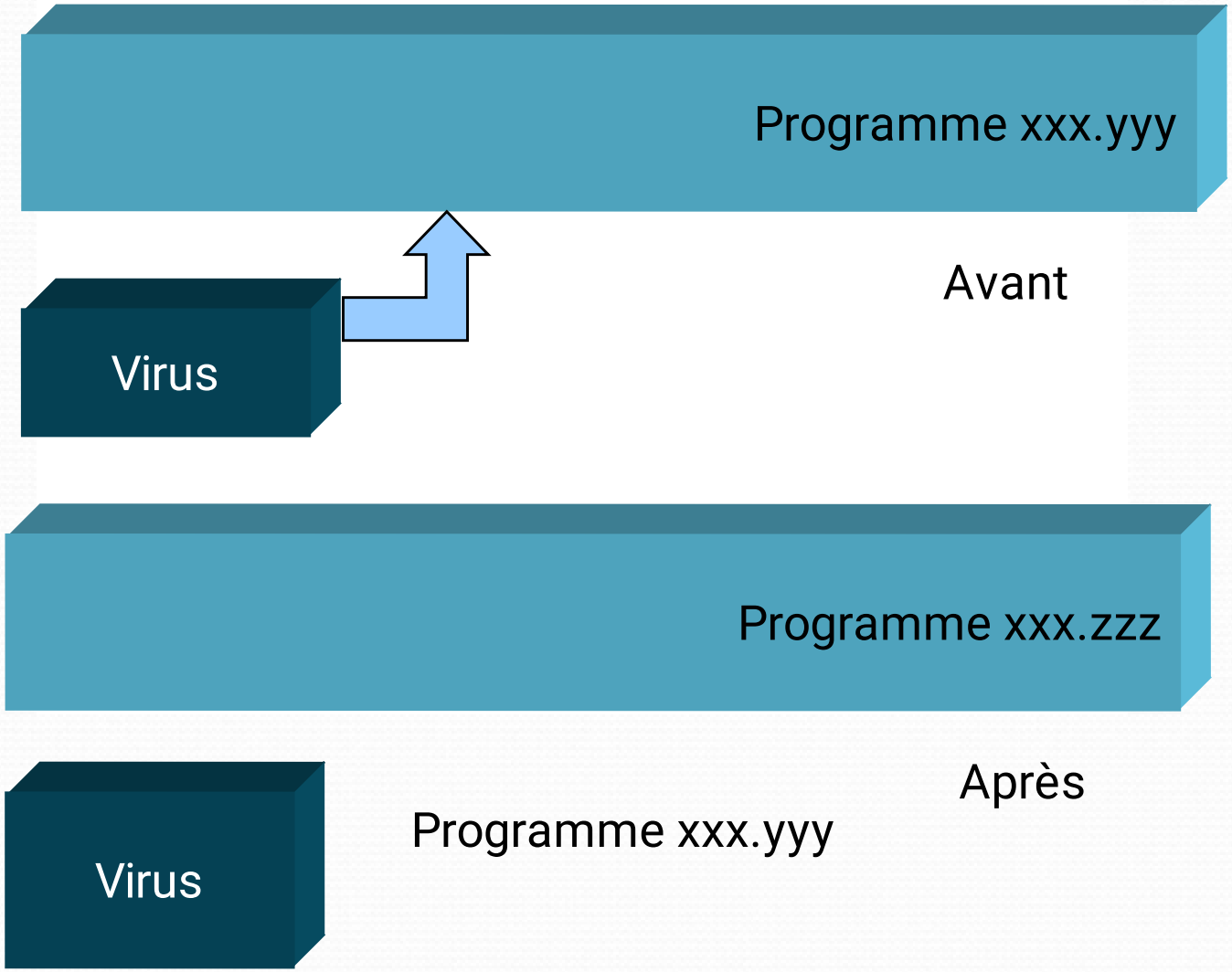
- Le virus insère tout ou une partie de son code dans différentes zones non utilisées.

-Il pourrait se situer entre le bloc de code, de données ou bien de la pile.

Le cycle de vie d’un virus : La reproduction

- Recouvrement
- Ajout
- Cavité
- Par virus Compagnon

La reproduction : Par virus Compagnon



- Le virus compagnon va créer un fichier du même nom que le fichier cible, mais avec une nouvelle extension (BAT, EXE, . COM).

- C'est le code viral qui est exécuté en premier, avant de lancer le programme désiré.

Vulnérabilité d'un système d'information

- Les virus informatique
- Le cycle de vie d'un virus
- Classification des virus

Classification des virus

- Les virus programme
- Les virus système
- Les virus interprétés
- “Les virus réseau” : Les vers

Les virus programme

- Ils cherchent à infecter des exécutables binaires compilé.

- Leurs principe de fonctionnement :
  - Le virus est présent dans un fichier exécutable, il contamine alors un ou plusieurs autre fichier exécutable.

  - Il peut se produire à travers différentes méthodes (Recouvrement, ajout, cavité, virus compagnon)

  - Il peut résider dans la mémoire et infecter d'autre fichier lors de leur exécution, ou simplement lors de leur manipulation.

Les virus système

- Ils infectent les zones systèmes des disques durs:
  - Secteur de partition (MBR : Master Boot Record)
  - Secteur d'amorce (Boot : Dos Boot Record)

- Le mode de fonctionnement de ce virus est le suivant :
  - Le virus est généralement présent dans le secteur de démarrage d'un support de stockage
  - Il contamine le PC lorsque le BIOS exécute le code
  - Il écrase le code originale du BOOT ou du MBR et le remplace par son code
  - Dés lors à chaque démarrage il peut infecter d'autre support de stockage.

Classification des virus

- Les virus programme
- Les virus système
- Les virus interprétés
- “Les virus réseau” : Les vers

Les virus interprétés

- La sophistication :
  - Des outils de bureautique (Word, Excel…)
  - Des langages de script (VBScript, JavaScript)
  - Des langages de programmation (Java, C++…)

A permis de “transformer” tout fichier inoffensif, en un fichier potentiellement DANGEUREUX

Classification des virus

- Les virus programme
- Les virus système
- Les virus interprétés
- “Les virus réseau” : Les vers

“Les virus réseau” : Les vers

- Les vers sont des programmes autonomes.
- Ils se propagent de machine en machine à travers le réseau
- Ils ne modifient pas le code relatif à un programme, par contre ils peuvent transporter des portions de codes nocifs.

Plan

- Vulnérabilité d’un système d’information
  - Vulnérabilité des utilisateurs
  - Vulnérabilité des réseaux
  - Vulnérabilité du Web

Vulnérabilité des utilisateurs

- Les Chevaux de Troie
- Les Bombes logiques
- Les spywares/adware
- Les virus polymorphes
- Les macro virus

Les Chevaux de Troie

- Il s'agit d'un "programme" qui est caché au niveau d'un logiciel d'apparence légitime.

- Il se compose de 2 parties:
  - Partie cliente : chez le pirate
  - Partie Serveur : Chez la victime, présente sous forme de mise à jours, d'amélioration d'un logiciel (MSN, Adobe…)

Les Chevaux de Troie

- Le cheval de Troie peut s'installer :
  - Dans l'éditeur de registre,
  - Dans l'autoexec de démarrage
- Une fois le cheval de Troie installé et démarré le pirate peut prendre le contrôle de l'ordinateur à distance, à travers l'utilisation des portes dérobées.

Les portes dérobées:

Les portes dérobées représentent l'un des éléments d'une application client/serveur qui permettent la prise de contrôle d'un poste à distance.

Les Chevaux de Troie

- A travers les chevaux de Troie, les hackers peuvent :
  - Voler des mots de passe
  - Copier des données
  - Exécuter des commandes à distance
  - Activer la WebCam
  - Imprimer des documents

Les Chevaux de Troie (3/3)

- Les symptômes d'infection par un cheval de Troie:
  - Activité anormale du modem ou de la carte réseau
  - Des réactions anormales de la souris
  - Des plantages à répétition
  - Des ouvertures imprévues de programmes

- Exemple de chevaux de Troie:
  - Back Orifice, SubSeven, ByteVerify…

Vulnérabilité des utilisateurs

- Les Chevaux de Troie
- Les Bombes logiques
- Les Spywares/Adwares
- Les virus polymorphes
- Les macro virus

Les Bombes logiques

- Les bombes logiques sont programmés pour s'activer quand un événement survient.

- Il s'agit d'un code qui est ajouté à un programme hôte. Ce dernier fonctionnera de façon normale jusqu'à l'arrivé d'un événement bien définit.

- Exemple de Bombe logique : Tchernobyl qui s'est déclenché le 26 Avril 1999, 13 d'anniversaire de la catastrophe nucléaire de Tchernobyl. Ce virus a fait des ravage jusqu'à 2002.

Vulnérabilité des utilisateurs

- Les Chevaux de Troie
- Les Bombes logiques
- Les spywares/adware
- Les virus polymorphes
- Les macro virus

Vulnérabilité des utilisateurs

- Les Chevaux de Troie
- Les Bombes logiques
- Les spywares/adwares
- Les virus polymorphes
- Les macro virus

Les Spywares

- Il s'agit d'un programme qui collecte des informations sur :
  - Ces habitudes de navigation
  - La configuration de son système d'exploitation
  - Les login/mots de passe utilisées

- Ce programme s'installe en même temps qu'un logiciel, qu'une mise à jours téléchargé à partir d'Internet (codec DivX, ActiveX, plugin…)

- Il n'est pas destiné, **généralement**, a endommagé une machine.

Les Adwares

- Ce sont des logiciels publicitaires qui s'installent de la même manière que les Spyware.

- Ils enregistrent souvent les habitudes de surf d'un utilisateur pour lui envoyer des e-mail publicitaires ciblés.

- Les risques des Spyware/ Adware :
  - Espionnage des données confidentielles (mots de passe, login..)
  - Mise en danger des données privées
  - La publicité non sollicité

Les virus polymorphes

- Ce virus change sa signature (séquence d'octet qui identifie un virus), pour qu'il ne puisse pas être détecté par un antivirus .

- La signature du virus peut changer de deux manières différentes :
  - Chiffrement : à chaque infection le virus change de code.
  - Métamorphisme: à chaque infection , il y a une insertion de séquence de bourrage différente à la séquence initial du virus.

Vulnérabilité des utilisateurs

- Les Chevaux de Troie
- Les Bombes logiques
- Les spywares/adwares
- Les virus polymorphes
- Les macro virus

Les macro virus

- Il s'agit d'une macro malveillante.

- Les macrovirus peuvent réaliser différentes actions:
  - Ouverture d'un ensemble de fichier en même temps,
  - Interruption de l'enregistrement de fichiers,
  - Destruction des données
  - Formatages de disque
  - Envoi de document qui se trouve au niveau de votre disque à tous vos contact …

- La propagation d'une macro virus se fait à travers la propagation du document contenant cette macro

Définition d’une macro

- Une macro est:
  - Intégrée dans des documents de bureautiques (Word, Excel…)pour exécuter une liste d’actions successives.
  - Développée en VBA (Visual Basic for application).

retour

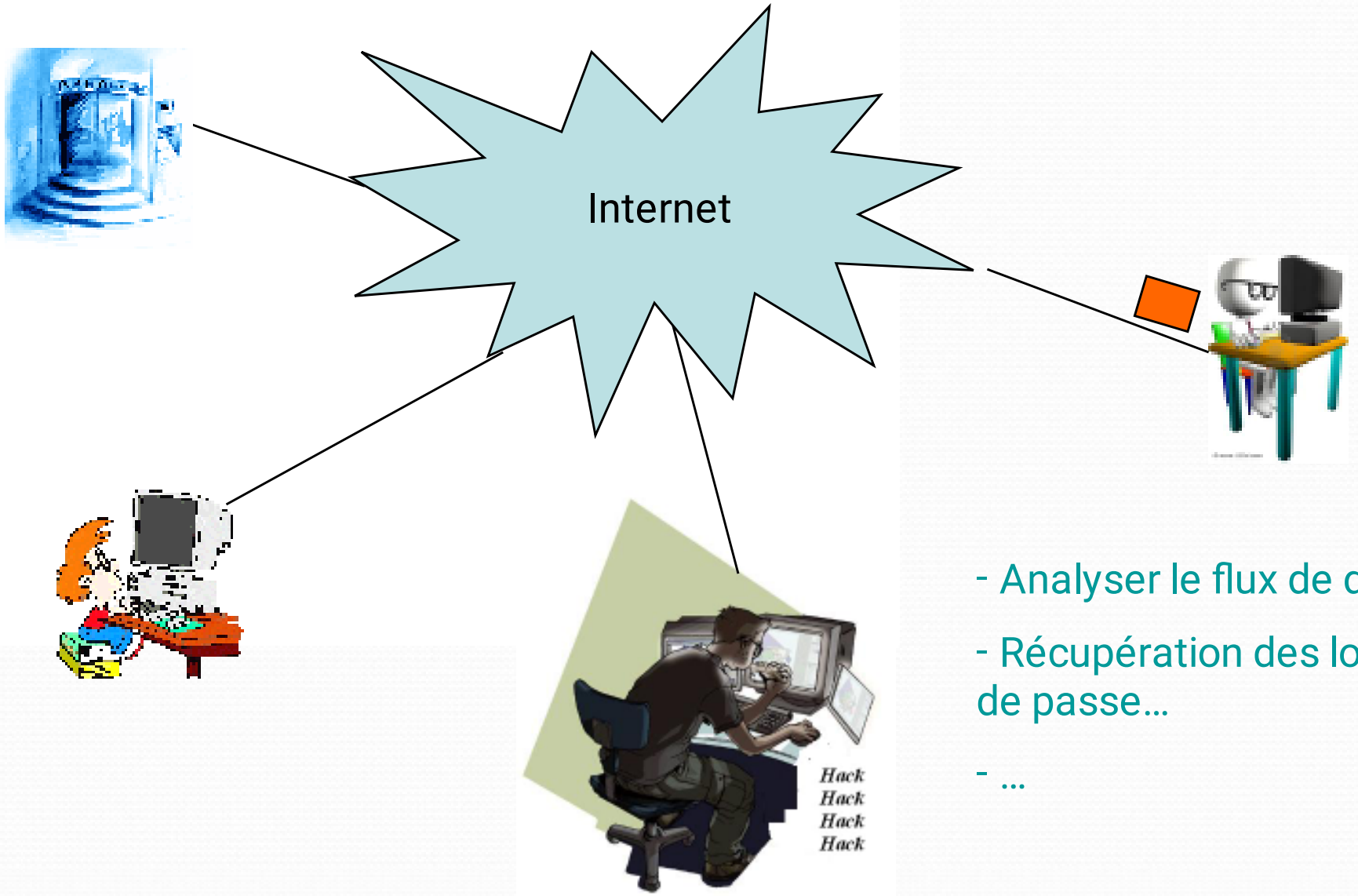
Plan

- Vulnérabilité d’un système d’information
  - Vulnérabilité des utilisateurs
  - Vulnérabilité des réseaux
  - Vulnérabilité des sites Web

Vulnérabilité des réseaux

- Deni of Service (DoS)
- IP spoofing
- DNS poisoning

Attaques Passives



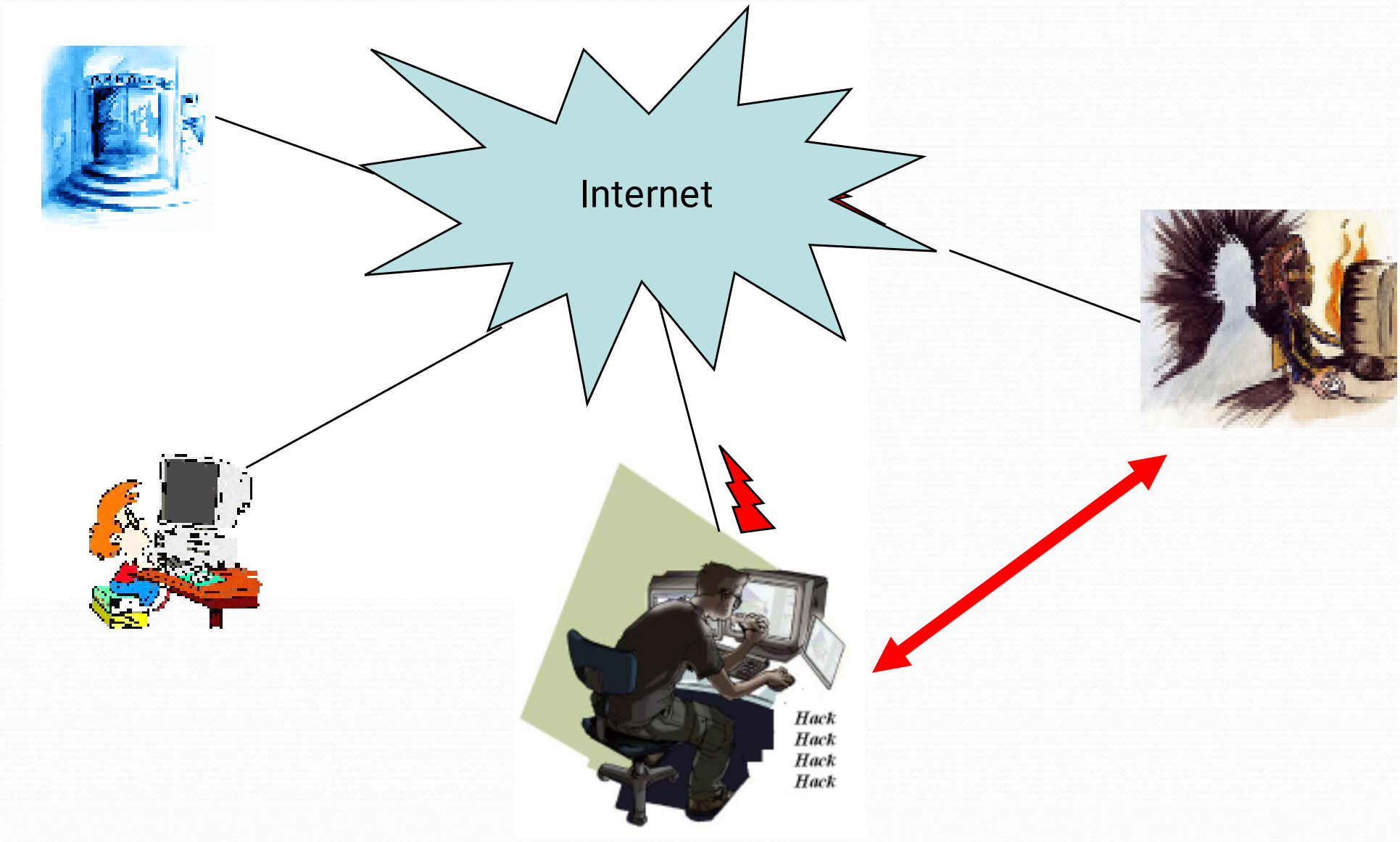
- Analyser le flux de données
- Récupération des login/mots de passe…
- …

Attaques actives

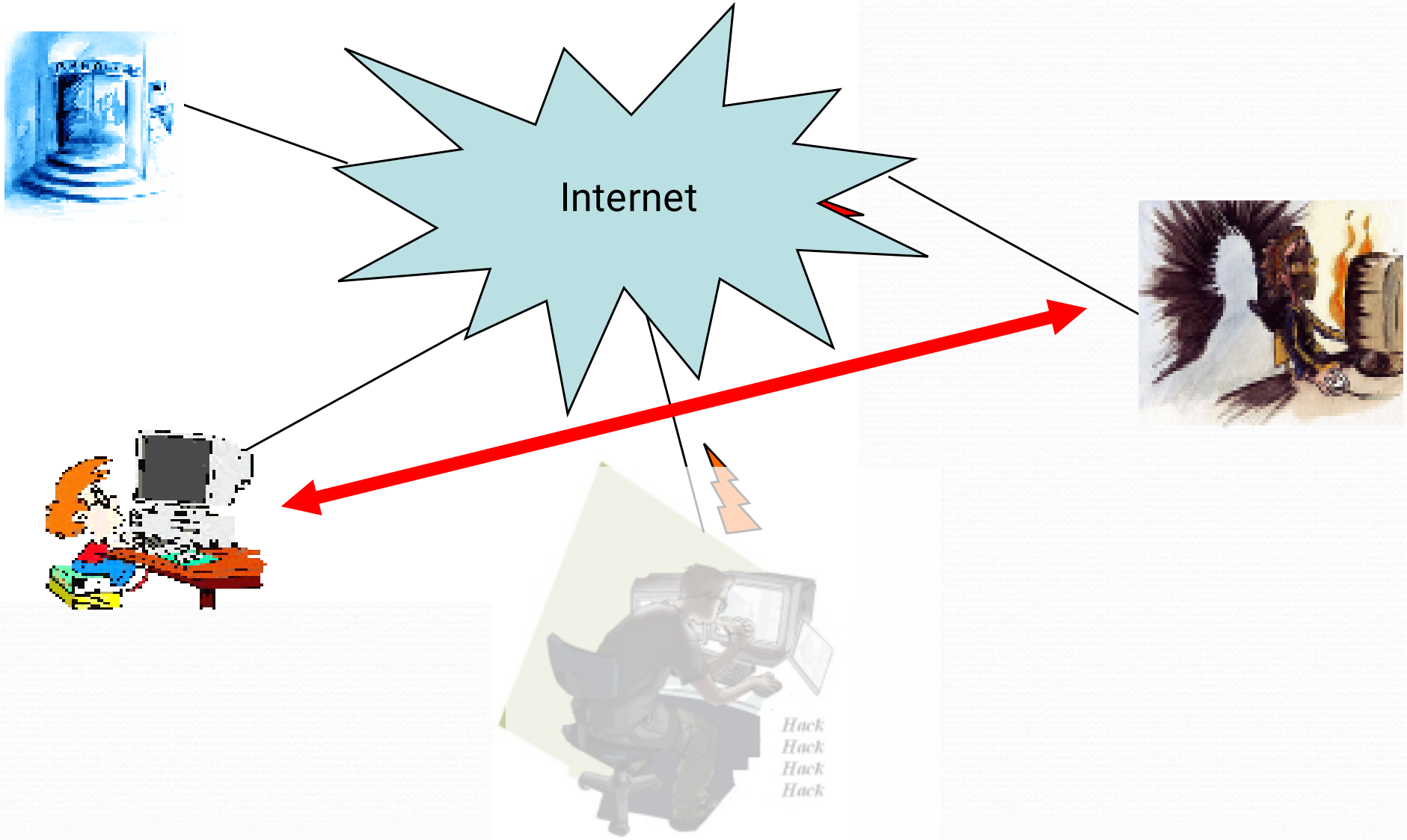
Internet

- Envoi de commandes
- Utilisation des chevaux de Troie, des vers…
- Dépassement de tampon
- Déni de service

Attaques directes



Attaques indirectes (par rebondissement)



Deni of Service (DoS)

- Cette attaque a pour but de bloquer, rendre impossible l'accès à une machine (serveur FTP, un serveur web,…)

- Ceci peut être réaliser de différente manière:
  - Inondation d'un réseau par un trafic "inutile"
  - La perturbation de la connexion entre différentes machines
  - Interdire l'accès à une machine

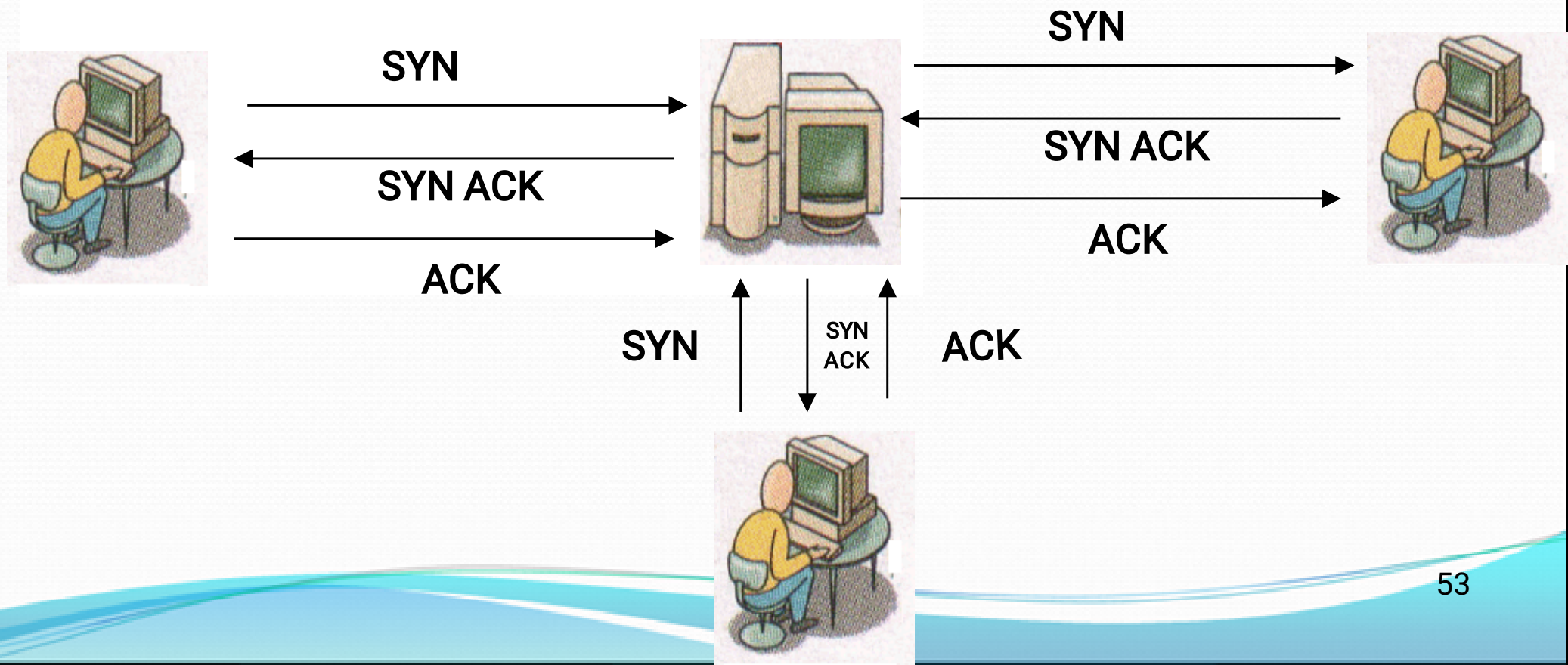
Deni of Service (DoS)

- Cette attaque a évolué ces dernières années pour donner une nouvelle attaque nommée: DDoS (Distributed DoS)
- Au niveau de cette attaque plusieurs machines participent à l'attaque.

- Différentes techniques sont utilisées pour causé un déni de service :
  - SYN Flood
  - Smurfing
  - ..

Deni of Service (DoS): SYN Flood

- Cette technique se base sur l'émission d'un nombre important de demande de synchronisation avec un serveur



Deni of Service (DoS):Smurfing

- Cette technique utilise le protocole ICMP (Internet Control Message Protocol).

- Au niveau de cette technique :

  - L'attaquant usurpe l'adresse IP de la cible

  - Il envoi au nom de la cible un paquet EchoRequest vers toute les machines du réseau

  - Ces machines vont répondre par un paquet EchoReply vers la cible. Ceci va causer la mise hors service de cette machine cible.

Le protocole ICMP

- Il s’agit d’un protocole de la couche 3 (réseau) du modèle OSI.
- Il permet l’échange de message de contrôle de connexion entre différente machine.
- Ce protocole utilise différent type de paquet: EchoRequest, EchoReply….
- Le paquet Echo request est généré à travers l’utilisation de la commande ping

Vulnérabilité des réseaux

- Deni of Service (DoS)
- DNS poisoning
- IP spoofing

DNS poisoning

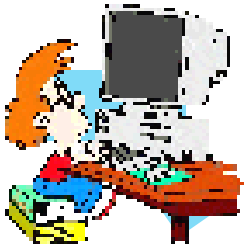
- Cette technique consiste à mettre hors service un serveur DNS (voir glossaire).
- Cette attaque se déroule de la manière suivante :
  - L'attaquant met hors service le serveur DNS
  - L'attaquant prend l'adresse IP de ce serveur DNS.
  - Lorsque un client demande une page Web (www.monsite.fr) cette demande va passer vers l'attaquant. Et au lieu de recevoir l'adresse IP correcte (60.96.1.34) de www.monsite.fr, il recevra une autre fausse adresse IP (98.30.46.32) d'un autre site web (www.sitedelattaquant.com).

Vulnérabilité des réseaux

- Deni of Service (DoS)
- DNS poisoning
- IP spoofing

IP spoofing

- Au niveau de cette attaque l'attaquant
  - Met hors service une destination, en premier lieu
  - Ensuite, il usurpe/prend l'adresse IP de cette machine, dans le but d'intercepter des données qui ne lui sont pas destiné.



Source

Destination

DESTINATION

Plan

- Vulnérabilité d’un système d’information
  - Vulnérabilité des utilisateurs
  - Vulnérabilité des réseaux
  - Vulnérabilité du Web

Vulnérabilité du Web

- Hoax
- Spam
- Phishing
- Injection SQL

Hoax (canular)

- Il s'agit d'un e-mail propageant une fausse information.
- Le contenu de cet e-mail pousse son récepteur de propagateur la fausse nouvelle.

- Les conséquences des canulars sont multiples:
  - L'encombrement du réseau par un flux de données inutile.
  - L'occupation d'espace au niveau des serveur mail.
  - ….

Spam (pollupostage)

- Cette technique se base sur un envoie massif d’email.
- Ces e-mail ne sont pas « désirés » par leur récepteur.
- Les spam peuvent incorporer des chevaux de Troie, comme pièce jointe.

Phishing (hameçonnage)(1/3)

- Cette technique se base sur l'envoie massif des e-mail (spam)
- Les e-mail envoyé par le pirate contiennent [3]:
  - Des objets trompeurs
    Exemple ; Subject: "eBay Member Billing Information Updates"
  - De fausses adresses d'expédition
    Exemple : SecretService@ebay.com
  - Des corps du message incitateurs et menacant :
    - Demande d'informations sur l'utilisateur pour la "Sécurisation" de son compte.
    - Suppression imminente du compte si pas de mise à jour
    - Débit imminent si pas d'annulation d'une transaction de vente..

Phishing (hameçonnage) (2/3)

- Ces e-mail contiennent des liens hypertexte (texte ou image), qui réalise une redirection automatique vers un site sous contrôle de l'attaquant.

- Le but du phishing est la récupération d'information privées telque : login/mots de passe, numéro de la carte bancaire, date de validité de la carte bancaire…

Phishing (hameçonnage) (3/3)

- Comment peut-on connaître et identifier une tel attaque ?
  - L'adresse apparente au niveau de la barre d'adresse est celle qui existe au niveau de la propriété de la page. Au niveau de l'image présenté ci-dessous on remarque l'absence de l'adresse URL dans la propriété de la page, et que cette adresse est remplacé par l'adresse IP du serveur de l'attaquant .
  - L'absence du verrou de sécurité, indice d'un échange sécurisé de données.

Adresse URL de la page

Verified by Visa

Protect your Visa card online with a personal password

Activate Now for Verified by Visa

Properties

General

Protocol: HyperText Transfer Protocol

Type: File

Connection: Not Encrypted

Address (URL): http://280.251.252.10/verified/

Size: 20018 bytes

Created: 14.12.2004

Modified: 14.12.2004

Certificates

OK Cancel Apply

Absence de l'URL de la page
et
présence d'une adresse IP

Absence du verrou de sécurité

Injection SQL (1/3)

- Cette attaque visent les serveurs Web, les serveurs d'email utilisant une base de données, dont la quelle il y a un stockage d'un ensemble d'identifiant : Login et mots de passe.
- Au niveau de cette attaque, il est possible à un attaquant de modifier, supprimer et d'accéder au contenu de la base de données du serveur Web.
- Cette attaque se base sur l'utilisation d'une séquence qui est ignorer lors de l'exécution de la requête SQL

Injection SQL (2/3)

- Voici un exemple pour comprendre cette attaque.
- Soit le formulaire présenté par l'image suivante.

Parmi l'un des codes SQL qui est exécuté au niveau de cette page est la commande SQL suivante :

```
SELECT * FROM utilisateurs WHERE nom="$name";
```

Cette commande rendra tous les champs de la table utilisateurs, lorsque le champ nom est égale à « name ».

name : le nom du champ qui est présenté au niveau du formulaire

Injection SQL (3/3)

- Lorsque l'attaquant fait entrer au niveau du champs name la valeur suivante :

  « toto" OR 1=1 OR nom ="titi »

La commande SQL serait alors :

SELECT * FROM utilisateurs WHERE nom="toto" OR 1=1 OR nom ="titi";

Dans ce cas de figure la condition après le terme WHERE est toujours vrai, et donc cette commande rendra la totalité de la table utilisateurs

Vulnérabilité du Web

- Au niveau de cette partie nous avons présenté quelques vulnérabilités relatifs au Web. Toutefois, il existe d'autre vulnérabilité. Parmi ces derniers on cite:
  - L'exploitation des cookies
  - Les attaques CGI (Common Gateway Interface)

Annexe

Serveur DNS

- La conversion entre adresse IP (68.98.12.34) et nom de domaine (www.google.fr) est assuré par un serveur DNS.
- Le mode de fonctionnement du serveur DNS est le suivant:

PC

1. Demande d'accès au site : www.monsite.fr

Serveur DNS

2. Recherche de l'adresse IP de www.monsite.fr

3. Envoi de l'adresse IP (60.96.1.34) du serveur ayant l'adresse URL : www.monsite.fr

4. Connexion à l'adresse IP 60.96.1.34

5.Envoi de la page d'accueil du site demandé: www.monsite.fr/index.html

Serveur Web

Références

- [1] http://tecfa.unige.ch/staf/staf-j/diego/staf14/ex8/virus.html
- [2] Dossier technique, «Les virus Informatiques », 2005, disponibles dans ; http://www.clusif.asso.fr/fr/production/ouvrages/pdf/virusinformatiques.pdf,
- [3] Document de formation de l'Agence National de Sécurité Informatique, 2005, en partie disponible dans http://www.ansi.tn/fr/documentations/publications.html