



Festivités du 19ème anniversaire du changement

-Novembre 2006-

« Initiation à la sécurité Informatique »



Plan

- **Introduction**
- **Les Menaces informatiques et comment se protéger...**
 - Virus
 - Ver
 - Cheval de Troie
 - Bombe Logique
 - Spywares
 - Hoax
 - Spamming
- **Radioscopie des attaques**
- **Quelques exemples d'attaques passives :**
 - Balayage du réseau (scan)
 - Observation du trafic réseau
 - Capture de Mot de Passe
 - Capture d'E-Mail
- **Attaque d'un serveur Web**
 - Modification d'un site
 - Arrêt forcé (déni) de service
- **Déni de service**
 - Exemple
- **Vol d'adresse (spoof)**
- **Recommandations générales et Contacts importants**



Introduction

DEGATS INFORMATIQUES (Source : DataPro) :

- Causes Communes de dommages :
 - **Erreurs Humaines : 52%**,
 - Malhonnêteté : 10%,
 - Sabotage 10%,
 - Feu 15%,
 - Eau 10%
 - Terrorisme 3%.
- Source :
 - **Employés : 81%**,
 - **Externes : 13%**,
 - Anciens employés 6%.
- Types de dommages :
 - **Détournement de fonds: 44%**,
 - Dommage aux logiciels 16%,
 - Perte d'informations 16%,
 - Altération de données 12%,
 - Altération des services 10%,
 - **Faillite 2%**.



Les menaces Informatiques

- Virus
- Ver
- Cheval de Troie
- Bombe Logique
- Spywares
- Hoax
- Spamming



Les menaces informatiques

Les virus





Virus

« Tout programme d'ordinateur capable d'infecter un autre programme d'ordinateur en le modifiant de façon à ce qu'il puisse à son tour se reproduire. »

- Les virus mutants
- Les virus polymorphes
- Les rétrovirus
- Les virus de secteur d'amorçage
- Les virus trans-applicatifs (virus macros)



Virus

Les moyens de propagation :

- Les disques durs
- Les disquettes
- Flash disk
- Cd Rom
- Le partage de fichiers réseau
- Email
- P2p

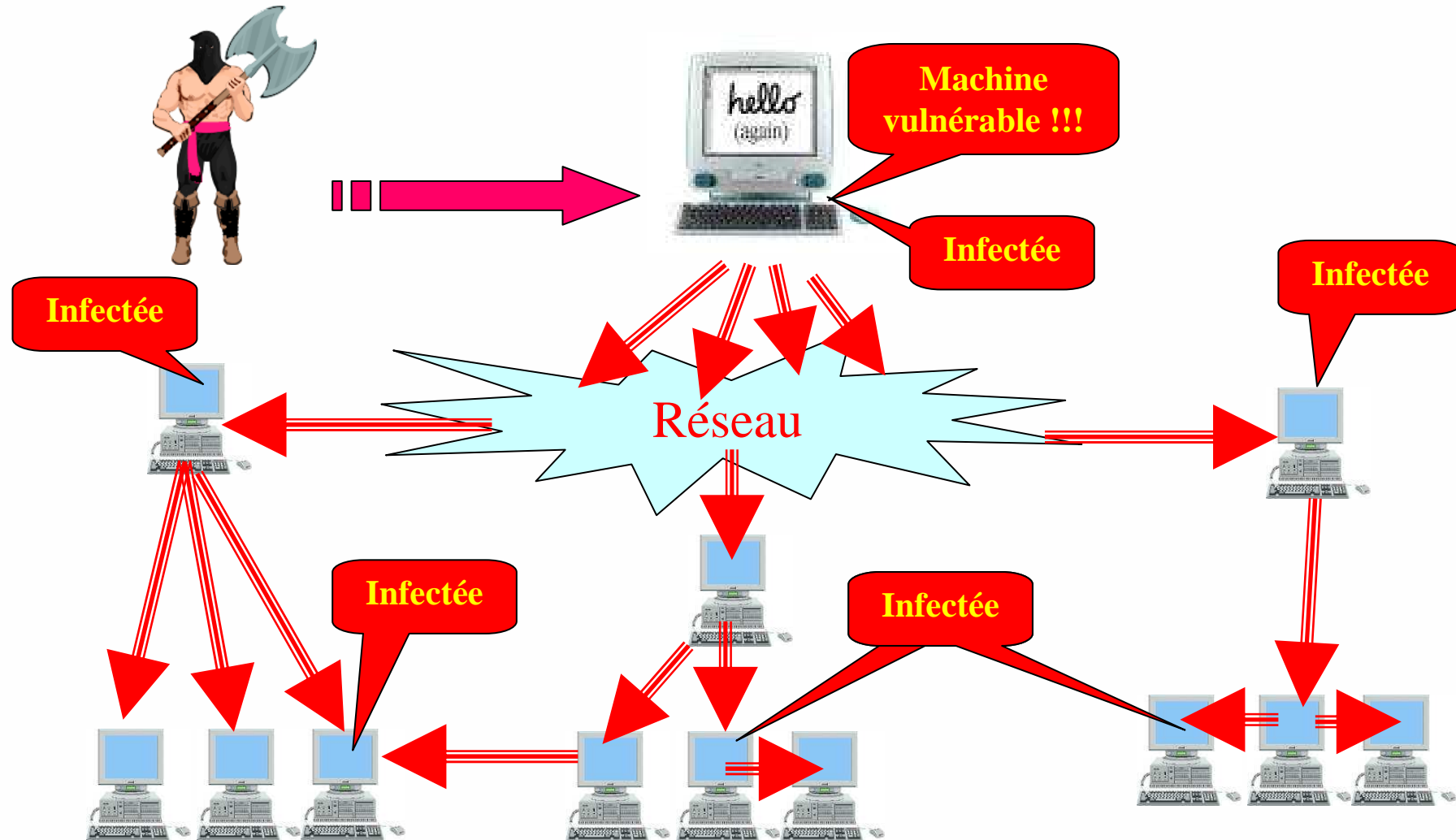


Les menaces informatiques



Les vers
(ou virus réseau)

Un ver est un programme qui peut s'auto-reproduire et se déplacer en utilisant des mécanismes réseau, sans avoir réellement besoin d'un support physique ou logique (disque dur, programme hôte, fichier ...) pour sa propagation, un ver est donc un virus réseau.





Dommmages dus aux virus

Enquête officielle DTI” britannique, (Mai 2004 , 1 000 entreprises)

-Augmentation de 25 % des atteintes virales en une année

-68% des grandes entreprises ont été atteintes par des vers et ont été sujettes à des attaques actives (DDos)

Quelques chiffres sur les dégâts dus aux derniers vers :

- 2004 : Le ver (virus réseau) MyDoom → 38 Millions \$US
- Le Ver SirCam →1.15 Milliards \$US,
- Le ver Code Red (Toutes les variantes) → 2.62 Milliards \$US
(250 000 systèmes infectés en moins de 9 heures)
- Le Ver NIMDA → 635 Million \$US



(50 Milliards de dégâts en 2003, selon des enquêtes de constructeurs d'anti-virus)

Les menaces Informatiques

Cheval de Troie





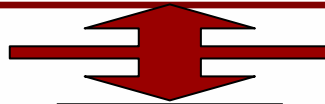
Attaque par cheval de Troie

- Un cheval de Troie est un programme qui, une fois installé sur une machine, permet de créer un troue qui donne aux pirates le contrôle total d'une machine.
- Une machine peut être infecté en téléchargement un programme d'Internet ou par un e-mail.
- Il est également appelé Tojan, il peut avoir le comportement d'un virus, il a la capacité de se cacher et de se dissimuler dans un fichier : Audio, Video, Word,...
- Les Trojans les plus connues sont : NetBus, Sub7, Back Orifice.

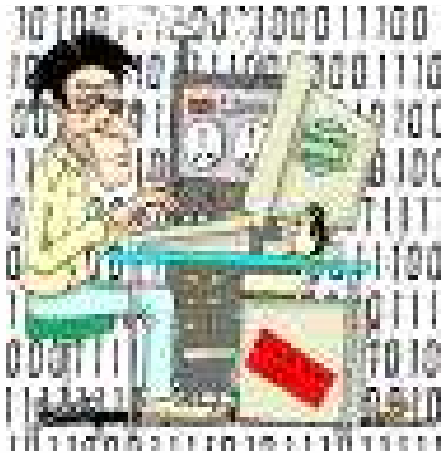


Email

De : ami@fsi.com
A : internaute@fsi.com
Sujet : Ma photo
Message : xxxxxxxxxxxx
Attachement : photo.jpg



**Réception
d'un Email
d'un ami**



Contrôle



total



Téléchargement & infection



Contrôle total

- Ouvrir/Fermer le CD-ROM.
- Afficher des images BMP/JPG.
- Désactiver les boutons de la souris.
- Exécuter des applications. Lancer un fichier wav.
- Contrôler la souris.
- Afficher différents types de messages.
- Fermer Windows.
- Télécharger/Envoyer/Effacer des fichiers.
- Exécuter une URL.
- Désactiver des touches de clavier.
- Visualiser les touches appuyées sur le clavier et insérer des caractères.
- Faire une capture d'écran.
- Contrôler le volume du son.
- Enregistrer du son à l'aide du Microphone.
- Faire des sons chaque fois qu'une touche est appuyée.



Solution contre les chevaux de Troie

- **Anti-Virus** : Un antivirus peut de détecter la présence d'un Trojan sur une machine et l'éliminer.
- **Firewall personnel** : permet de détecter les accès illicites d'une machine externe vers la machiné protégé par ce Firewall.
- **Détecteur d'intrusion** (Host IDS ou Network IDS): peut identifier le comportement d'un cheval de Troie sur le réseaux ou sur la machine et il génère une alerte.
- Quelques liens d'outils sont disponibles sur le site de l'Agence Nationale de la Sécurité informatique
http://www.ansi.tn/fr/outils/outils_domestique.htm (*)

(*) Ces outils sont gratuits uniquement à usage Personnel



Les menaces Informatiques



**Les bombes
logiques**



Les Bombes Logiques

- Ce sont les dispositifs programmés dont le déclenchement s'effectue à un moment déterminé en exploitant la date du système, le lancement d'une commande, ou n'importe quel appel au système.
- Ainsi ce type de virus est capable de s'activer à un moment précis sur un grand nombre de machines (on parle alors de *bombe à retardement* ou de *bombe temporelle*), par exemple le jour de la Saint Valentin, ou la date anniversaire d'un événement majeur : la bombe logique Tchernobyl s'est activée le 26 avril 1999, jour du 13ème anniversaire de la catastrophe nucléaire ...
- Les bombes logiques sont généralement utilisées dans le but de créer un déni de service en saturant les connexions réseau d'un site, d'un service en ligne ou d'une entreprise



Les menaces Informatiques

**Les spywares
(ou logiciels espions)**





Les Spywares

Un spyware est un programme chargé de recueillir des informations sur l'utilisateur de l'ordinateur sur lequel il est installé afin de les envoyer à la société qui le diffuse pour lui permettre de dresser le profil des internautes.

Les récoltes d'informations peuvent ainsi être :

- Voire des informations personnelles,
- la traçabilité des URL des sites visités,
- le traquage des mots-clés saisis dans les moteurs de recherche,
- ...



Les Spywares

Les spywares peuvent également être une source de nuisances diverses :

- consommation de mémoire vive,
- utilisation d'espace disque,
- mobilisation des ressources du processeur,
- plantages d'autres applications,
- gêne ergonomique (par exemple l'ouverture d'écrans publicitaires ciblés en fonction des données collectées),
- ...



Les menaces Informatiques

Les Hoax
(ou faux virus)





Les Hoax

→ On appelle hoax ou canular un email propageant de fausses informations en les passant pour vraies. Généralement le destinataire du courrier se voit incité à diffuser cette nouvelle à toutes ses connaissances.

→ Le but des hoax est de provoquer la satisfaction de la personne l'ayant envoyé d'avoir trompé des millions de personnes. Leurs conséquences sont nombreuses :

- Ils encombrant les boîtes mail et donc nous font perdre du temps de téléchargement lors de la réception des mails
- Ils engorgent les réseaux en consommant inutilement de la bande passante et des ressources serveur.
- Ils véhiculent de fausses informations en les faisant passer pour vraies.



Exemple d'Hoax: COUPE du MONDE

- **Objet : VIRUS TRES DANGEREUX**

Soyez très vigilants dans les jours à venir!

N'ouvrez aucun message avec un dossier appelé COUPE du MONDE 2006, indépendamment de qui que ce soit qui vous l'envoie. Ce virus viendra d'une personne connue qui a votre nom dans son carnet d'adresse, pour ça vous devez envoyer ce message à tous vos contacts. Il est préférable de le recevoir 25 Fois que de subir le virus en l'ouvrant. Si vous recevez un message appelé COUPE du MONDE 2006 : ne l'ouvrez pas et éteignez l'ordinateur immédiatement!

Il s'agit du pire virus que l'on ait jamais connu, CNN a annoncé son existence dans le journal télévisé; Microsoft l'a classé comme le plus ravageur qu'il n'y ait jamais existé.

Le virus a été découvert très récemment par McAfee et il n'existe pas d'antivirus. Le virus détruit le Secteur Zéro du Disque Dur, dans lequel on garde les informations vitales pour leur fonctionnement.

ENVOYEZ LA COPIE DE CET E-MAIL à TOUS VOS AMIS ET COLLEGUES ET CONTACTS. EN LE FAISANT CIRCULER, NOUS NOUS AIDONS TOUS.



→ Pour éviter de se faire piéger par les hoax et distinguer les faux mails des vrais, voici quelques notions simples :

- Toute information reçue par mail qui ne contient pas de lien hypertexte ou de mail de contact doit être reléguée au rang de hoax.
- Tout mail insistant dans le message sur le fait qu'il est très important de donner l'information à toutes vos connaissances (ex : "n'oubliez pas d'avertir vos connaissances en leur envoyant une copie du message") sont à bannir.
- N'hésitez pas à vérifier l'information sur un site spécialisé ou d'actualités ou contactez directement le CERT/TCC de l'ANSI pour plus de vérification à l'adresse cert-tcc@ansi.tn ou par téléphone **Numéro vert 80100267** ou 71843200 disponible 7j/7j



Les menaces Informatiques

Le Spamming
Dit communément « Spam »





Le Spamming

- Le spamming consiste à envoyer massivement des e-mails généralement de type publicitaire (dit aussi "**junk mail**"), à un grand nombre de personnes n'ayant pas sollicité ce type d'envoi publicitaire, engorgeant ainsi les serveurs de messagerie et vos boîtes à lettres de messages publicitaires inutiles, non sollicités et généralement mensongers. Les e-mails "spammés" constituent actuellement la quasi-moitié des e-mails "circulant" à l'échelle planétaire.
- Le but premier du spam est généralement de faire de la publicité à moindre coût. Toutefois, il est aussi source de tentatives d'abus, via des offres alléchantes (vous avez gagné ...) et bien sûres mensongères, dont le but est de vous attirer à acheter un produit ou un service douteux, ou bien d'essayer d'abuser de vous, en vous estorquant de l'argent surtout si vous possédez des cartes de crédit en devises.
- Il est aussi parfois question de publicité "politique" ou "religieuse" dangereuses pour les enfants (par exemple : l'église de la Scientologie avait récemment envoyé 1200 spams en 15 jours sur un groupe de discussion). Toutes les récentes enquêtes réalisées depuis 2003 montrent que le pourcentage de propagation du SPAM représente la plus grande part de l'ensemble d'EMAILS à l'échelle mondiale.



Réaction à avoir contre le Spam

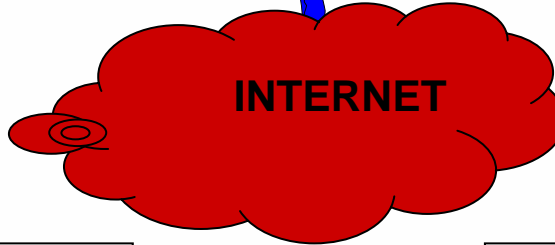
- **Ne pas répondre aux messages de spam** (même pour les menacer, ...), car cela ne ferait qu'empirer les choses, puisque cela assurera aux spammeurs que vous receviez bien leur e-mails et ainsi que vous êtes réceptif à ce genre de messages.
- **Configurer votre client de messagerie.** En effet plusieurs logiciels de messagerie et certains services webmail, permettent de bloquer l'accès aux expéditeurs indésirables. De plus, certains clients de messagerie suppriment systématiquement les emails en question.
- **Ne pas donner votre adresse e-mail sur des formulaires de sites douteux**, car beaucoup de ces sites communiquent ces adresses aux spammeurs. **Il serait même utile d'avoir deux ou plusieurs adresses mails dont vous spécifieriez une pour vous identifier sur le web, ou dans les groupes de discussion.**
- **Protéger votre adresse de messagerie:** Ceci minimiserait la probabilité de la voir récupérée par les robots collecteurs d'adresses et de recevoir de nombreux mails non sollicités. Ainsi à la place de publier votre adresse sous votrenom@fournisseur.tn vous la publierez sous astuce_spam_votrenom@fournisseur.tn. Ceci obligerait votre correspondant à corriger l'adresse avant de vous envoyer un message et éviter ainsi les robots collecteurs.
- **Prévenir votre administrateur** et surtout votre FSI, en cas d'amplification de ce phénomène. Ceci leur permettra de certifier l'ampleur du spam et de prendre les mesures nécessaires (blocage de l'origine de ces messages, via les outils anti-spam, ...).



Radioriscope des Attaques



S
O
N
D
A
G
E



Attaques

P
A
S
S
I
V
E
S



Ciblés

Automatiques

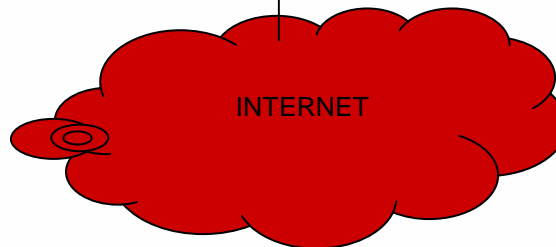


•Exploits spécifiques

Sondage de
TOUTES les
Failles
connues



E
S
P
I
O
N
N
A
G
E



« Sniffeurs »



- Analyse des Flux
- Récolte de Passwords
- Récolte de séquences à Rejouer
-



DECEPTION

“Social ENGINEERING”



ANALYSE → Edification

et **TEST** “sans risque” et “le Temps qu’il faut”

d’Attaques **Combinées** et **Bien Planifiées**



Corruption

- Confidentialité,
- Intégrité
- Disponibilité
- Autorisation, Non-Repudiation, Compabilisation (Log)



Atteinte à la CONFIDENTIALITE : “Vol” (lecture) de Données, Implantation d’outils de capture de flux (“ Sniffeurs”),

Atteinte à l’INTÉGRITÉ : Modification (non détectable) des Données

• **Atteinte à la DISPONIBILITE** :IMMOBILISATION sélective ou GLOBALE de Serveurs ou/et du RESEAU (DENI DE SERVICE)



• **Atteinte aux mécanismes d’autorisation/ Non-répudiation** :
Usurpation de droits et abus des interlocuteurs



• **Atteinte aux mécanismes de Comptabilisation (log)** : Corruption des outils de Log (effacent leurs traces, via l’Implantation de codes malicieux (Chevaux de Troie, ..).



Implantation de “portes dérobées”, codes malicieux (verss, troyens, ...), Canaux Cachés (entités d’espionnage)



Exemples des attaques passives :

Scan du réseau

(Balayage du réseau)



Scan (ou balayage) du réseau

- Le scan permet de collecter des informations concernant :
 - Le type de système
 - Les applications qui tournent
 - Les ports ouverts
 - Les vulnérabilités existantes
- Il constitue la première étape de reconnaissance pour attaquer un système, le scan d'un réseau a pour but d'identifier les machines, les routeurs, les firewalls et les serveurs.



Exemples des attaques passives :

Observation du trafic réseau

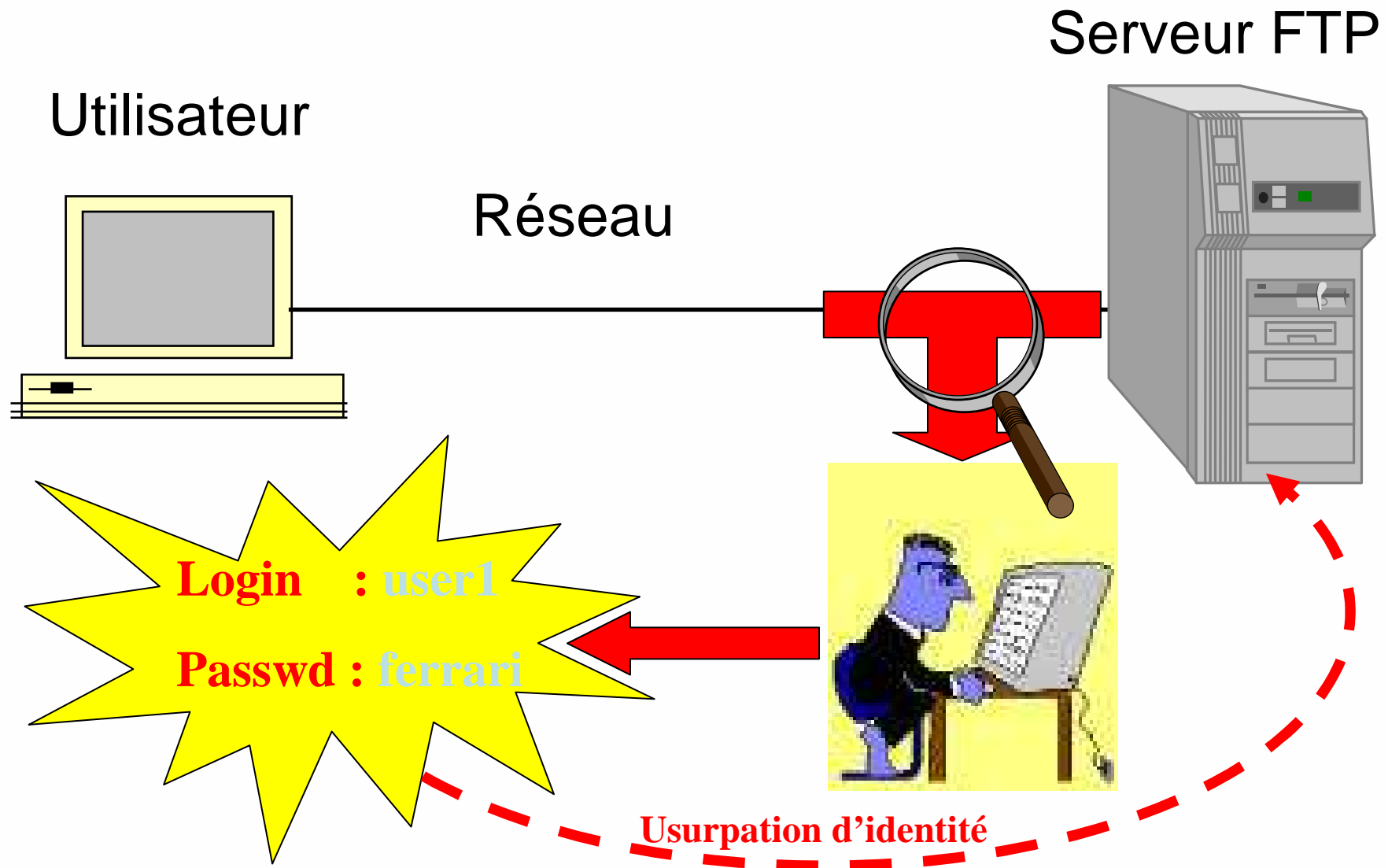
Capture de Mot de Passe



Observation du trafic réseau

- Sur un réseaux local (non-switché), pour envoyer des données d'une machine à une autre, le hub d'interconnexion envoie ces données à toutes les machines du même segment, seule la machine destinataire lit les données les autres les rejettent.
- Certains protocoles envoient toutes les données en claire comme : Telnet, FTP, POP3, SMTP,...
- Un utilisateur mal-intentionné, ne rejette pas ces données, les analyses et extrait d'informations qui l'intéresse comme un mot de passe ou un E-Mail.

Capture de Mot de Passe



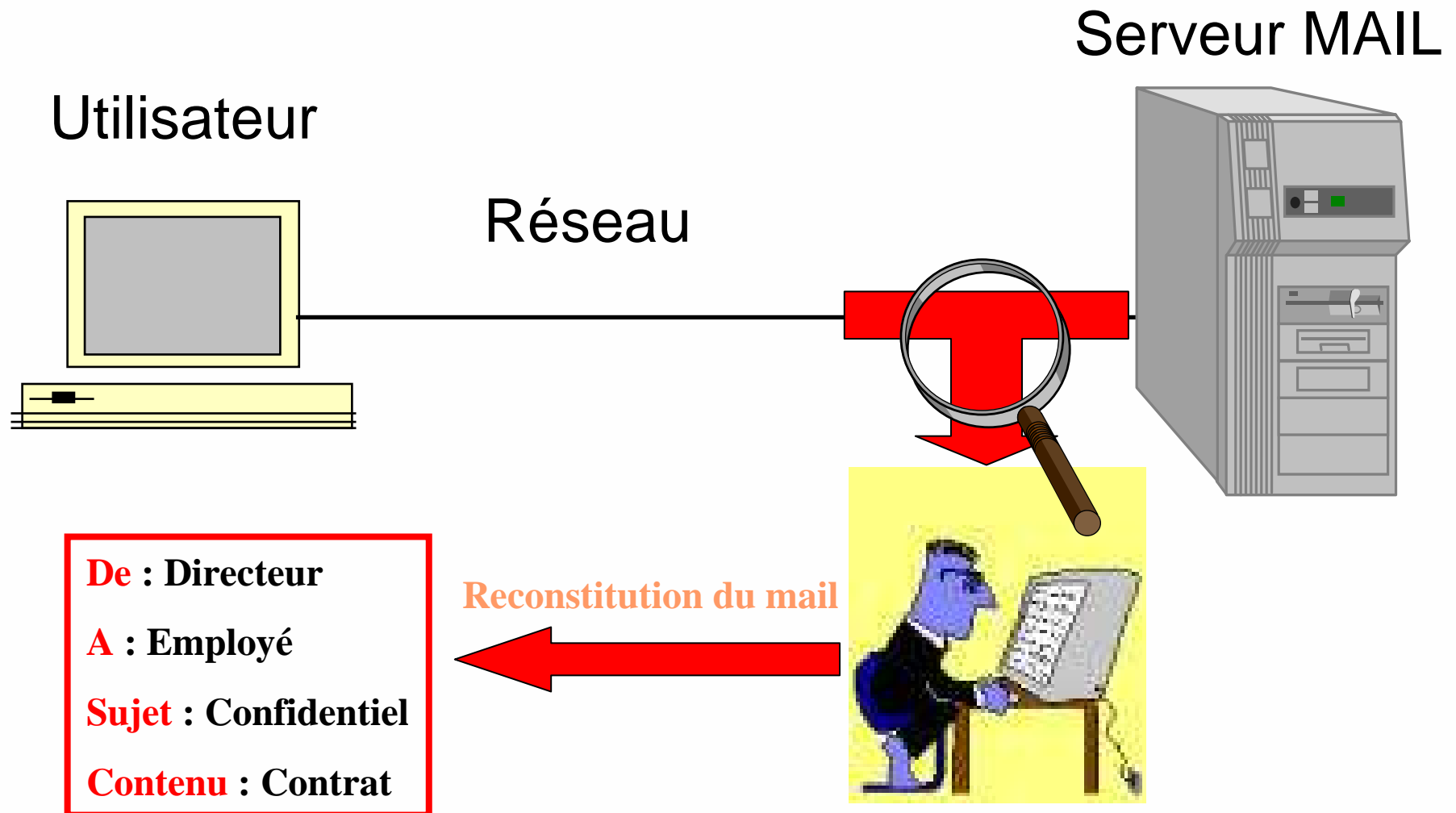


Exemples des attaques passives :

Observation du trafic réseau

Capture d'E-Mail

Capture d'E-Mail





Solution contre l'observation du trafic réseau

- **Switch** : Le remplacement d'un Hub et l'utilisation d'un Switch qui permet d'éviter la diffusion des informations vers toutes les machines, seule la destination indiquée reçoit les données.
- **Cryptage** : le cryptage est la solution inévitable pour garder la confidentialité des données, les données passent cryptées sur le réseau seule la destination peut les déchiffrer et lire le contenu.
- **Anti-Sniff** : Permet de lancer un scan sur le réseau pour identifier les machines qui travaillent en mode de capture de trafic

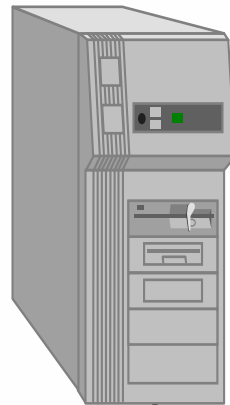


Attaque d'un serveur Web



Changement de la page d'accueil

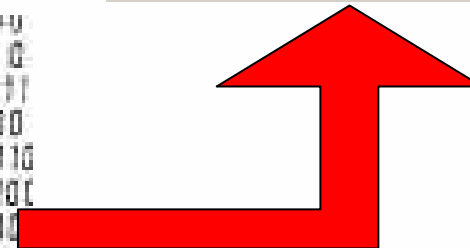
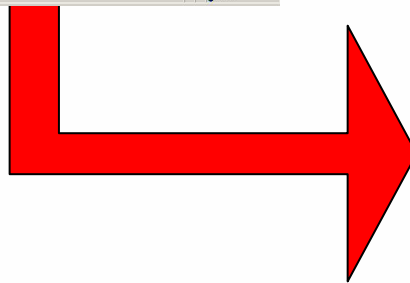
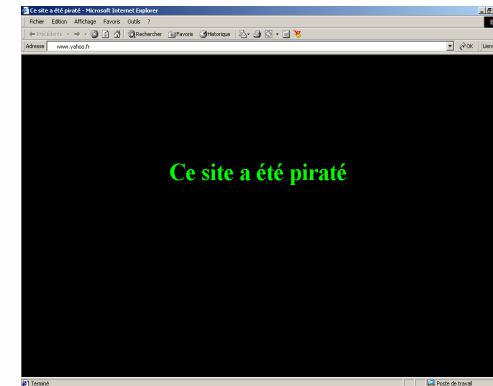
Serveur Web



Ancienne page d'accueil

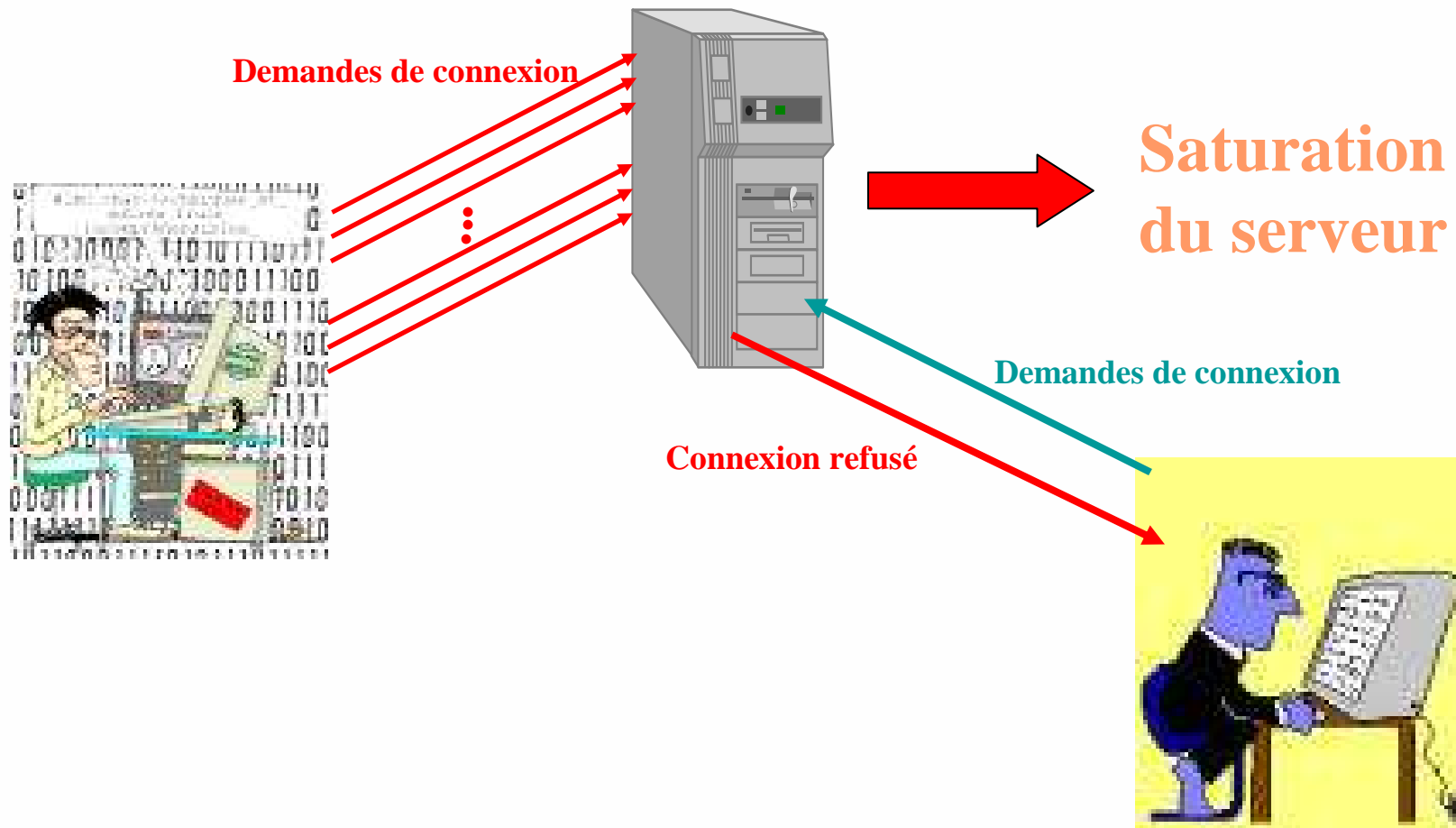


Nouvelle page d'accueil



Déni de service (arrêt forcé de service)

Serveur Web





UNICEF - United Nations Children's Fund - Microsoft Internet Explorer

Fichier Edition Affichage Favoris Outils ?

Précédente → Recherche Favoris Historique

Adresse http://www.unicef.org/

Special Session on Children / Employment / Contact / UN Links / Copyright / Français / Español 13 December 2002

unicef
Why Children Must Be Heard
11 December 2002
What's New

MUHAMMAD ALI IN AFGHANISTAN

CARDS AND GIFTS

SOUTHERN AFRICA CRISIS

GIRLS' EDUCATION

**For every child
Health, Education, Equality, Protection
ADVANCE HUMANITY**

UNICEF in Action

Highlights

Information Resources

Donations, Greeting Cards, & Gifts

Press Centre

Voices of Youth

About UNICEF

THE STATE OF THE WORLD'S CHILDREN 2003

UNICEF's flagship publication, *The State of the World's Children 2003*, examines the largely unexplored issue of child participation.

Search

Netscape: UNICEF/DAMM Coalition

Back Forward Reload Home Search Guide Images Print Security Stop

NetSite: http://www.unicef.org/

unicef
United Nations Children's Fund
and DAMM bring you....

STARVIN' 4 KEVIN

(i'm hungry!)

meat!!!



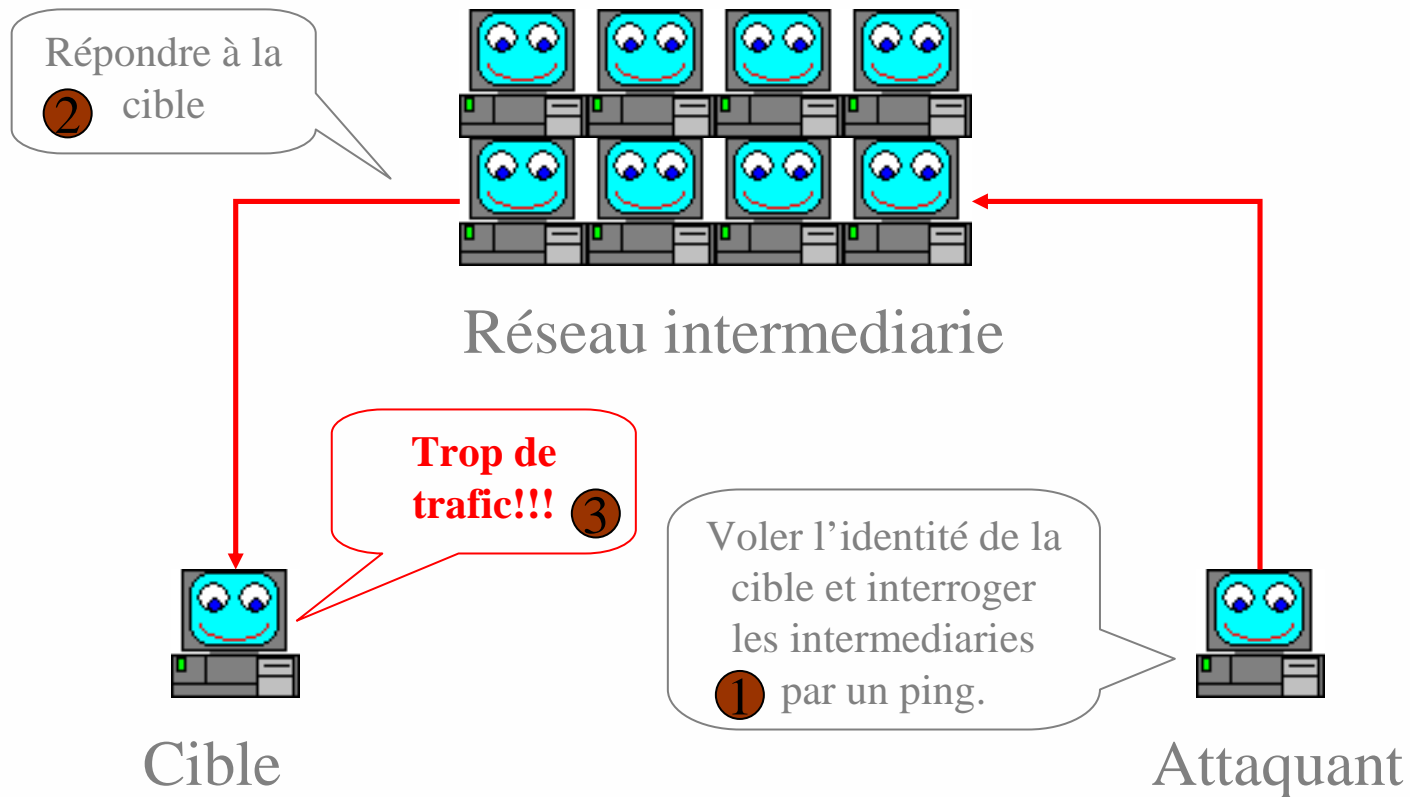
The screenshot shows a Mozilla Firefox browser window with the address bar displaying `http://www.microsoft.com/france/`. The page content is a black overlay with the word **HACKED!** in large white letters. Below this, the text reads: `Hi Master (: Your System OwNed By Turkish Hackers!`, followed by `redLine & rudeb0y & Ejder & The_Bekir & SaCRe0SeeR & ASH owNed you!`, `next target: microsoft.com`, and `TiTHack.CoM & SauSaK.CoM`. The browser's address bar in the foreground shows `http://experts.microsoft.fr/`. The background page includes a navigation menu with sections like 'Produits' (Windows, Office, Serveurs, etc.) and 'Ressources' (Téléchargement, Windows Update, etc.). The system tray at the bottom shows the time as 20:28 and the status 'Chargé'.



Déni de service

(arrêt forcé de service)

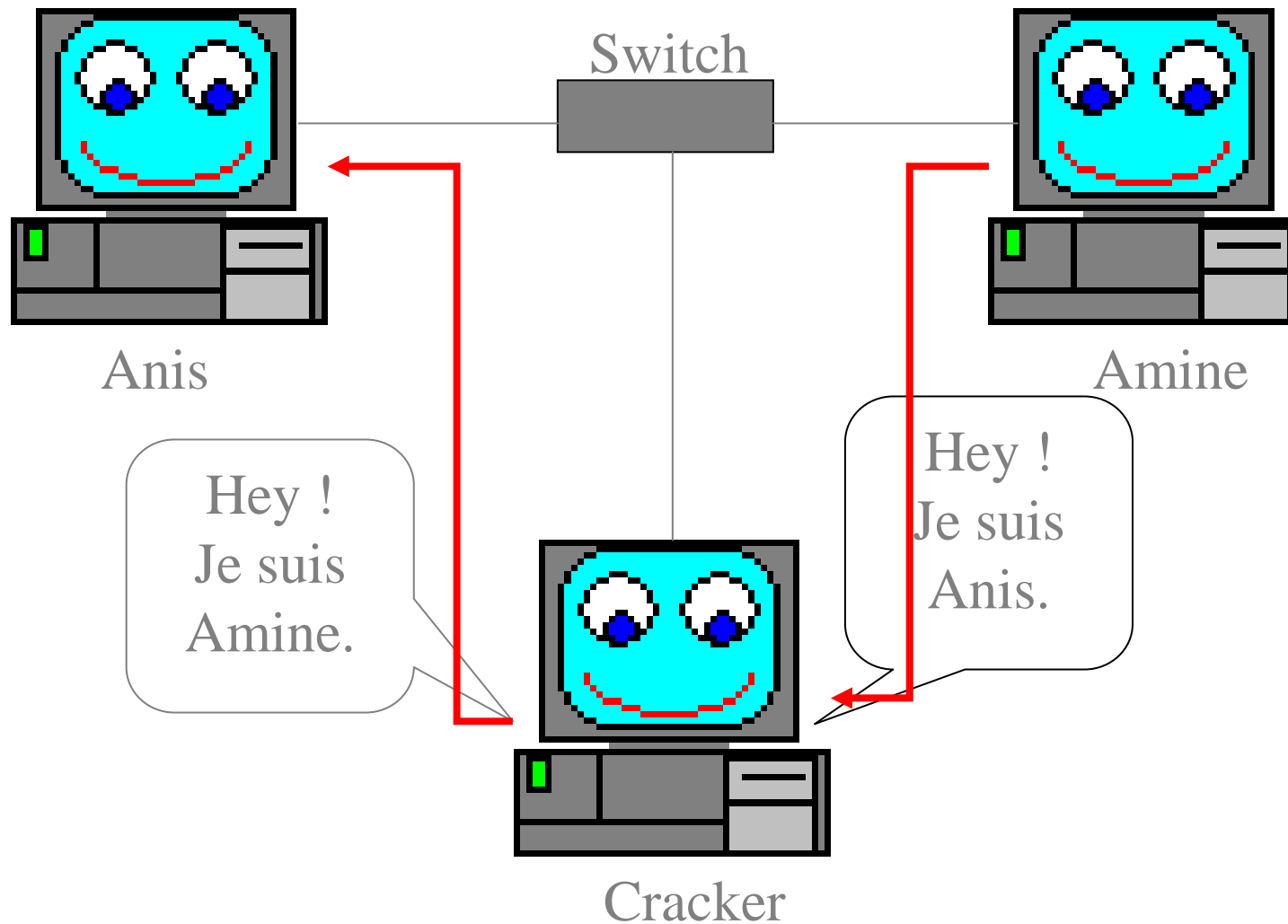
Exemple





Le Vol (ou spoof) d'adresse

Attaque Man in the Middle





Recommandations

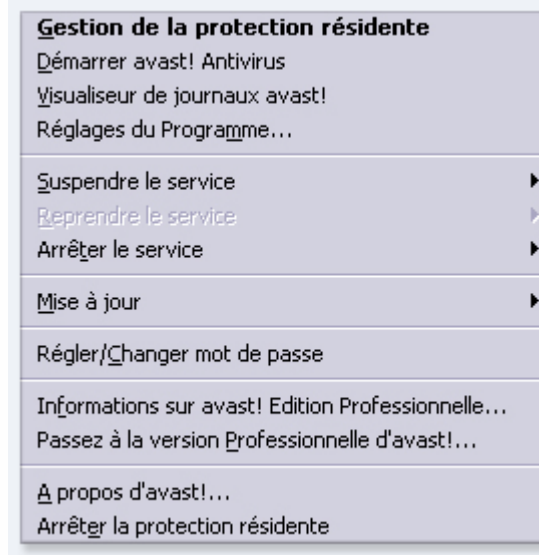
Générales



1. Utiliser un antivirus et garder-le à jour

Avast!: Antivirus gratuit à usage domestique

Cliquez droit sur l'icone avast de la **barre des taches** pour afficher le menu contextuel d'avast:



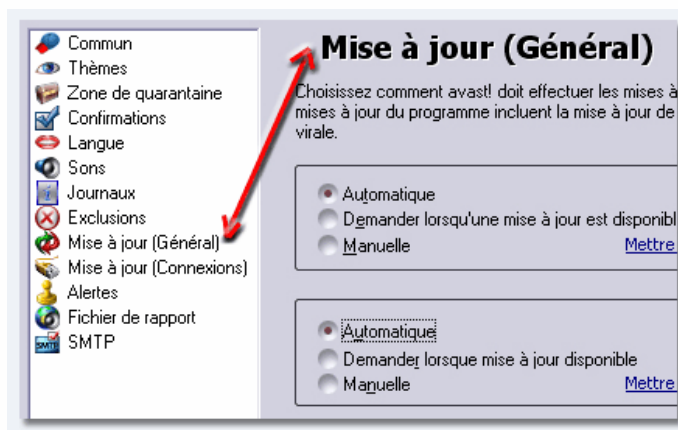
Toujours avec le clic droit, avast vous donne la possibilité de suspendre ou d'arrêter les différents services de protection



Avast!: Antivirus gratuit à usage domestique

Choisissez l'option "*Réglage du programme*", vous accédez à l'interface d'**administration**. Pour activer les mises à jour automatiques: cliquer sur le menu concerné et cocher "**Automatique**".

Celles-ci sont réalisées **quotidiennement** ou à défaut lors de chaque connexion:

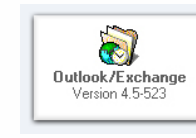


Attaquons-nous au choses sérieuses, démarrez Avast! Antivirus:



Avast!: Antivirus gratuit à usage Personnel

Accédez à la gestion de la protection résidente d'un clic droit dans la barre des tâches, dans cette fenêtre vous pouvez affiner le réglage de **protection** de votre PC:



Plusieurs solutions s'offrent à vous, sélectionner de préférence **réparer** puis si c'est impossible, supprimer où mettre en quarantaine. Ces alertes apparaissent sans que vous ayez à activer le scan. C'est tout l'intérêt d'une **protection résidente** pas besoin de penser à lancer l'antivirus il le fait tout seul. (Ce qui ne vous empêche pas de scanner minutieusement votre PC de temps en temps)





2. Soyez attentifs lorsque vous naviguez sur le net

– **Méfiez vous des messages électroniques trop attractifs**

– **Des extensions dangereuses**

386, ACE, ACM, ACV, ARC, ARJ, ASD, ASP, AVB, AX, BAT, BIN, BOO, BTM, CAB, CLA, CLASS, CDR, CHM, CMD, CNV, COM, CPL, CPT, CSC, CSS, DLL, DOC, DOT DRV, DVB, DWG, EML, EXE, FON, GMS, GVB, HLP, HTA, HTM, HTML, HTA, HTT, INF, INI, JS, JSE, LNK, MDB, MHT, MHTM, MHTML, MPD, MPP, MPT, MSG, MSI, MSO, NWS, OBD, OBJ, OBT, OBZ, OCX, OFT, OV?, PCI, PIF, PL, PPT, PWZ, POT, PRC, QPW, RAR, SCR, SBF, SH, SHB, SHS, SHTML, SHW, SMM, SYS, TAR.GZ, TD0, TGZ, TT6, TLB, TSK, SP,VBE, VBS, VBX, VOM, VS?,

VWP, VXE, VXD, WBK, WBT, WIZ, WK?, WPC, WPD, WML, WSH, WSC, XML, XLS, XLT, ZIP

- **Réglez le niveau de sécurité de votre navigateur (Internet Explorer, Netscape, FireFox, ...)**



3. Ne pas ouvrir d'email ou de pièce jointe dont la source est inconnue (susceptible de contenir un virus). Être suspicieux à la réception d'une pièce jointe à un email même si celui-ci apparaît être parvenu d'une source connue.



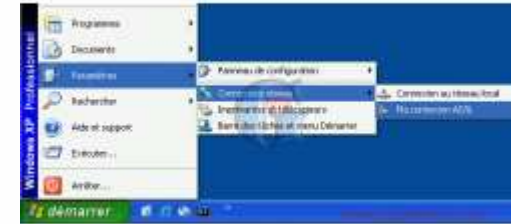
4. Protéger son ordinateur contre les intrusions provenant d'Internet – utiliser un « Firewall ».

Firewall de Windows XP

Activez le Firewall intégré à Windows XP :

Pour activer la protection de votre PC sous Windows XP, faites comme indiqué sur les photos suivantes (nous supposons ici que votre connexion ADSL ou Câble est déjà installée et opérationnelle).

Cliquez sur "Démarrer", "Connexions", sélectionnez votre connexion ADSL ou câble et cliquez droit dessus, choisissez alors "Propriétés".



Vous devriez alors obtenir la fenêtre suivante (allez dans l'onglet "Avancé") Si ce n'est déjà fait, vous n'avez qu'à cliquer sur : "Protéger mon ordinateur et le réseau en limitant ou interdisant l'accès à cet ordinateur à partir d'Internet" pour activer le firewall de Windows XP.



Zoom

Firewall de Windows XP

Configurer le firewall:

Votre firewall est maintenant actif mais il est possible de le configurer plus finement qu'il ne l'est par défaut. Sur la fenêtre précédente, cliquez sur "Paramètres...".

Dans l'onglet "Services", vous pourrez spécifier quels services ou applications seront autorisés à accéder à Internet.

Il est bien entendu possible d'en rajouter en cliquant sur "Ajouter...".

C'est d'ailleurs ici que vous pourrez ouvrir spécifiquement des ports, c'est à dire permettre à des applications bien définies de passer à travers votre firewall.

Ceci peut être en effet très utile si votre firewall se montre un peu trop restrictif en bloquant certaines de vos applications comme Netmeeting ou Messenger !



Zoom

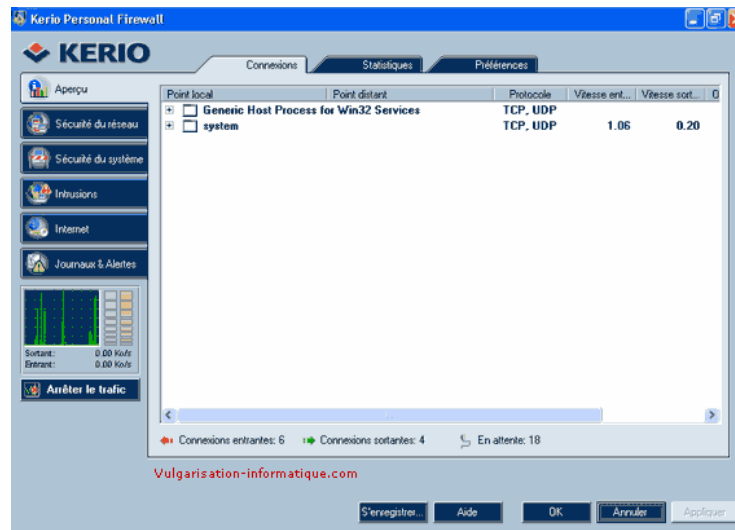


Zoom

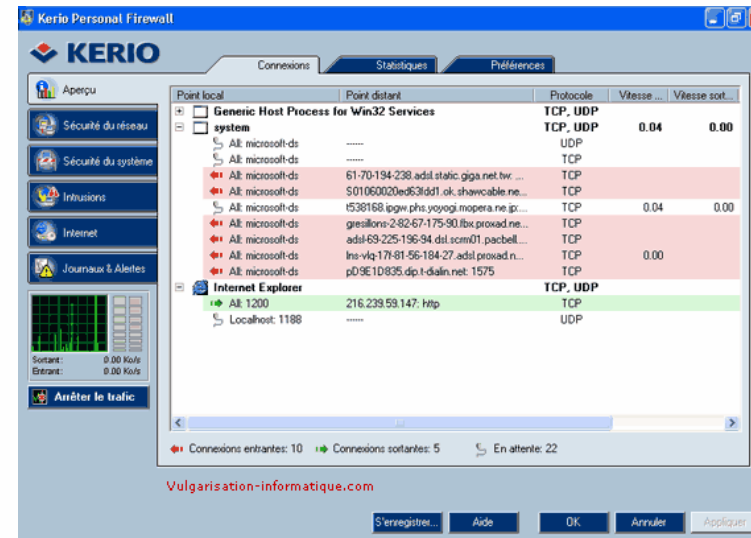
Kerio: Firewall gratuit à usage Personnel

Kerio personal firewall

. Il dispose d'une interface claire et simple à appréhender. Vous pouvez commencer par télécharger kerio Sélectionnez **anglais** pour la langue d'installation, et installez kerio. Redémarrez ensuite votre PC. Une icône est ensuite visible dans le systray (à côté de l'horloge)



Cliquez sur **configuration**. Vous avez alors accès à toutes les options disponibles. L'écran d'accueil de kerio se présente sous cette form



Cliquez sur un élément (ici **system**) pour afficher la liste des connexions entrantes et sortantes ainsi que les ports associés à ces connexions.

Kerio: Firewall gratuit à usage Personnel

Cliquez ensuite sur l'onglet **préférences**. Vous pouvez ici configurer les options de base du logiciel. Cochez la case **Mettre à jour automatiquement** et décochez celle nommée **Vérifier les versions Beta**. Si vous souhaitez protéger la configuration de votre firewall, cochez la case **Activer la protection par mot de passe**.



Cliquez ensuite sur **Sécurité du réseau**. Les choses un peu plus sérieuses commencent. Cochez tout d'abord la case **Activer le module de sécurité réseau**. Vous pouvez ici pour chaque application listée (ou toutes les autres en cliquant sur **autres applications**) refuser sa communication localement ou à travers internet





5. Télécharger régulièrement les mise à jour de sécurité et les « patch » pour le système d'exploitation et les autres applications utilisées.



I) les étapes à suivre pour appliquer les patches critiques des systèmes Windows

1- Se connecter au site WindowsUpdate (cliquer sur le lien ci-contre) :www.windowsupdate.com (ou sélectionner depuis votre bureau :

"*Démarrer*" --> "*WindowsUpdate*")

2- Une fenêtre s'affichera, incluant le lien suivant :---> Rechercher des mises à jour

3- Cliquer dessus, afin de rechercher automatiquement la liste des patches relatifs à votre système. Cette opération peut prendre quelques minutes, selon le nombre de correctifs nécessités et la vitesse de votre connexion.

4- Une fois cette opération terminée (patches identifiés), une nouvelle fenêtre incluant le lien suivant s'affichera :--->Examiner les mises à jour et les installer

5- Cliquer dessus, afin d'examiner la liste complète des patches relatifs à votre PC (Ou Cliquer dans la sous-fenêtre de gauche sur "Mises à jour Critiques, service Pack")

6- Une fenêtre incluant en haut, le message suivant apparaît : [Installer Maintenant] Total :.....= Mo, Minutes

Ceci spécifie le Nombre Total des Patches nécessaires, la taille totale (en Mega Octets) et le temps moyen (en minutes nécessaires pour finaliser cette opération).

Si vous voulez appliquer tous les patches en une seule fois : Cliquer sur [*Installer Maintenant*] Sinon

Si vous voulez réaliser cette opération en plusieurs fois (temps nécessité trop long, ...). sélectionner uniquement quelques mises à jour à installer tout de suite,

en : Retirant de la liste ceux non désirés maintenant (ceux de grande taille),

En cliquant sur [*Supprimer*] (ou sur certaines versions, cliquez sur Ajouter en regard de la mise à jourchoisie). Puis cliquer sur : [*Installer Maintenant*]

Il faudra alors reprendre cette procédure autant de fois que nécessaire, jusqu'à appliquer la totalité des Patches.

7- Attendez la fin de la mise à jour automatique et selon le cas(type de patch), il sera parfois nécessaire de Redémarrer votre PC pour finaliser l'opération (voir le message affiché)



II) Les étapes à suivre pour appliquer les patches critiques des outils Office

1- Se connecter au site OfficeUpdate : www.officeupdate.com

2- Une fenêtre s'affichera, incluant un carré qui contient le lien suivant :

---> **Rechercher des Mise à Jour**

3- Cliquer sur Rechercher des Mise à Jour , afin de rechercher automatiquement la liste des patches relatifs à votre version d'Office. Cette opération peut prendre quelques dizaines de minutes, selon le nombre de correctifs nécessités et la vitesse de votre connexion.

4- Une fois cette opération terminée (patches identifiés), une nouvelle fenêtre incluant le lien suivant s'affichera :

Mises à jour sélectionnées : (Nombre de patches nécessaires)

Taille de téléchargement : **Ko** (Taille des Patches)

Temps de téléchargement : **min** (Temps moyen pour compléter l'opération de "patching [**Accepter et Démarrer l'Installation**]

5- Cliquer sur le bouton [**Accepter et Démarrer l'Installation**], pour appliquer automatiquement les patches.

6- Attendez la fin de la mise à jour automatique et selon le cas(type de patch), il sera parfois nécessaire de Redémarrer votre PC pour finaliser l'opération (voir le message affiché)



6. Installer un anti-spyware et mettez le régulièrement à jour

Spybot: gratuit à usage Personnel

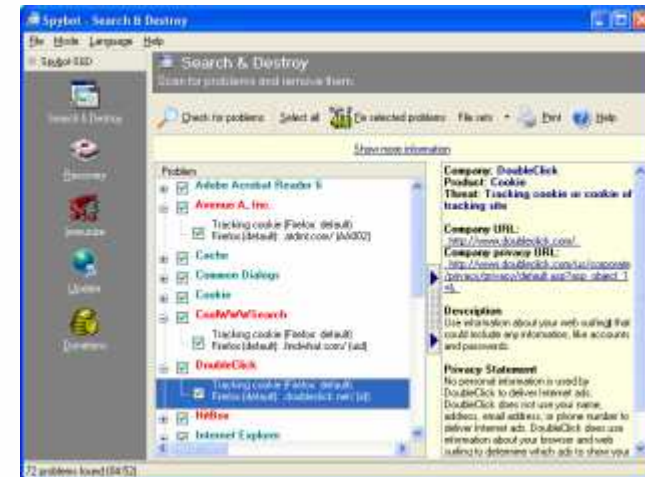
Installer spybot

La première fois que vous lancez Spybot-S&D, il affichera un *Assistant*, une petite fenêtre qui vous aidera dans vos premiers pas. Celle-ci vous donne la possibilité d'ajouter ou d'enlever les icônes que vous avez ou non créées pendant l'installation, par exemple. Disons que vous les voulez, et passons à la page suivante.



Balayer le système

Le premier bouton de cette barre d'outils s'appelle Vérifier tout - c'est le bouton sur lequel vous devez cliquer pour lancer le balayage. Appuyez-vous sur votre dossier et regardez la progression de la recherche. La première chose est de faire la distinction entre les lignes en rouge, qui représentent le spyware et les menaces similaires, et les lignes en vert, qui sont des traces d'utilisation.



Utiliser le bouton *Corriger les problèmes pour supprimer toutes les menaces sélectionnées*



7. Utiliser des mots de passe difficile à deviner. Combiner des majuscules, des minuscules, des chiffres, et autres caractères spéciaux, et s'assurer que la taille du mot de passe dépasse les huit caractères.



- Si nous prenons le mot **"asselema"** , il s'agit d'un mot de 8 lettres facile à retenir et qui n'existe dans aucun dictionnaire. Seulement, tel que présenté, il ne constitue pas un mot de passe fort car il ne contient aucun chiffre, aucune majuscule et aucun caractère spécial. Seulement, avec quelques manipulations, nous pourrions aboutir à un mot de passe plus robuste:
 - Ajouter des chiffres : par exemple, en ajoutant un "3" en tête de mot et en remplaçant le "s" par un "5", nous obtenons au mot **"3a55elema"**,
 - Ajouter des majuscules : aussi, en remplaçant certaines lettres minuscules en majuscules, nous pourrions obtenir le mot **"3a55eleMA"**,
 - Ajouter des caractères spéciaux : enfin, nous pouvons remplacer le "l" par un point d'exclamation "!" et le "a" par "@" ce qui permettrait d'aboutir à un bon mot de passe : **"3@55e!eMA"**.



8. Sauvegarder régulièrement les données de son ordinateur sur des disques ou sur des CDs (Back-up).



9. Ne pas partager l'accès à son ordinateur avec tout le monde. Apprendre les risques du partage de fichiers.



10. Se déconnecter de l'Internet, si c'est non utilisé.



11. Verrouillez ou fermer l'ordinateur en quittant.



12. Sensibiliser les membres de la famille et/ou ses collègues sur les bonnes réactions dans le cas où l'ordinateur est infecté.



Agence Nationale de La Sécurité Informatique

Cert-TCC

Computer Emergency Response Team / Tunisian Coordination Center



- Call Center: 71 843 200
- Fax: 71 846 363
- Site web : www.ansi.tn
- Emails: cert-tcc@ansi.tn
 - pour l'assistance : Assistance@ansi.tn
 - pour la déclaration (confidentielles) d'incidents : incident@ansi.tn
 - Enfants et Parents:enfants@ansi.tn
 - pour l'abonnement à la mailing-list de sécurité : Abonnement@ansi.tn
- Bureau d'accueil du citoyen : N°94, Avenue Jugurtha Mutuelle-Ville, CP 1002, Tunis