# Documentation A2IMP-Windows

Version 2007-03-15 pour la boîte à outils *a2impWin* v5 (version du 15 mars 2007)
Adaptée pour Capitoul le 31 mars 2009


Auteurs : Marie-Claude Quidoz <Marie-Claude.Quidoz@urec.cnrs.fr>
Contributions : Denis Pugnère <d.pugnere@ipnl.in2p3.fr>
Relectures : Nicole Dausque <Nicole.Dausque@urec.cnrs.fr>,
François Morris < Francois.Morris@impmc.jussieu.fr >



**Résumé :**

Cette documentation a été réalisée pour décrire comment utiliser la boîte à outils *a2impWin* (Aide à l'Acquisition d'Information sur une Machine Piratée – version Windows). Cette documentation contient les commandes indispensables pour réaliser l'étape d'acquisition de traces sur une machine piratée, dans le but de pouvoir analyser ultérieurement ces traces. L'analyse de traces ne sera pas abordée dans ce document.


**Information :**
Ce document propose une méthode. Compte-tenu des spécificités du site, qui doivent être privilégiées, il se peut que cette méthode ne puisse être suivie à la lettre.

**Sommaire**

# 1 Avant de commencer

- Gérer les priorités :
  - identifier les services impactés,
  - informer sa hiérarchie,
  - informer les utilisateurs
- Isoler la machine du réseau ou filtrer le trafic via les équipements réseaux (*routeur*, *firewall*, *switch*...) : geler la situation. Nous déconseillons de débrancher le câble réseau de la machine compromise. En donnant ce conseil, nous faisons l'hypothèse que vous êtes totalement opérationnel et que cette machine ne restera connecté au réseau que le temps nécessaire à la sauvegarde des informations volatiles de la machine compromise donc dans les faits peu de temps. Remarque : en fonction de votre environnement, il est possible que vous ne puissiez pas isoler vous-même votre machine. Dans ce cas, discutez-en au préalable avec votre CRI.
- Se munir de documentation (celle ci est un bon début !)
- Avoir la boîte à outils *A2IMP-linux* gravée sur CD
- Disposer d'un *switch* ou *hub* rapide (100Mb/s est le minimum en fonction de l'espace à sauvegarder) : compter 2 minutes par Go
- Posséder des cordons *RJ45* droits et/ou croisés
- Avoir à disposition un espace de stockage suffisant :
  - soit un PC (portable ou autre) branché (via switch, hub, cordon croisé) disposant de la commande *nc* présente sur le CD *A2IMP-linux* et pouvant recevoir les données,
  - soit un disque externe à brancher sur la machine compromise (attention aux risques relatifs à l'intégrité des données que l'on va enregistrer sur ce disque puisqu'il sera accessible directement en écriture par tout le système compromis),
  - il existe des boîtiers spécifiques dédiés à la copie qui sont plus rapides (et plus chers)

NB :

- Ne pas hésiter à s'appuyer sur les compétences locales, régionales (coordinateurs) et nationales (CERT-Renater, CERTA, experts)

Conseil :
Il est vivement conseiller de tester et de valider régulièrement les procédures employées pour être à même de les appliquer efficacement et sereinement en situation de crise.

# 2 Principes de base

- Ne pas faire de modifications sur le système en cours d'acquisition d'informations
- Ne pas faire confiance aux outils installés sur le système en cours d'acquisition d'informations
- Garder une trace horodatée des actions réalisées
- Récupérer les informations et les enregistrer :
  - volatiles :
    - l'image de la mémoire *RAM*,
    - processus en cours d'exécution,

    - fichiers ouverts,
    - la liste des communications ouvertes,
    - l'état du système (variables d'environnement, modules, liste des utilisateurs...)
  - non volatiles :
    - les informations sur le système de fichiers (partitions...)
    - les partitions utilisées

- Penser également à recenser et récupérer les traces laissées sur le système d'information en bordure de cette machine (*logs* et filtres des *routeurs*, métrologie, contrôles d'accès...)
- Sauvegarder les informations sur un support externe, d'une manière fiable
- S'assurer que les informations sauvegardées sont intègres
- S'assurer qu'aucune modification n'a été faite ou ne peut se faire sur les informations sauvegardées.

# 3 Disposer de moyens d'écoute du trafic réseau

En théorie, enregistrer le trafic émis par une machine peut être fait à différents endroits :

- directement sur la machine compromise,
- à partir d'une autre machine saine connectée sur le même hub que la machine compromise,
- au niveau du switch sur laquelle la machine compromise est connectée,
- au niveau d'un élément extérieur (routeur, garde-barrière, commutateur, IDS, ...).

Pour avoir une analyse plus complète de chaque solution, reportez-vous à l'annexe 2.

La solution idéale correspondrait à la quatrième possibilité : au niveau extérieur. Cependant, il est impératif de tester, au préalable, sa faisabilité dans votre propre environnement et d'avoir documenté la procédure utilisée.

Remarque : le choix de la première possibilité peut conduire à ne pas respecter le principe de base : « il ne faut pas écrire sur la machine compromise ».

Dans la suite de ce document, nous utiliserons la troisième possibilité.

# 4 Vérifier l'existence des DLL

Deux DLL sont nécessaires pour le bon fonctionnement de l'utilitaire netcat. Il s'agit des DLL : Msvcr70.dll et Msvcp70.dll. Vérifiez leur présence dans le répertoire c:\windows\system32 et cela sur les deux machines : celle compromise et celle qui permet de sauvegarder.

Si ces DLL ne sont pas présentes, il faut les copier au préalable dans le répertoire c:\windows\system32 de vos deux machines. Elles sont disponibles dans la boîte à outils Windows (répertoire DLLWIN2000).

# 5 Méthode

Cette méthode détaille les commandes à utiliser pour réaliser la phase d'acquisition de données en tenant compte des principes de base décrits dans le document « documentation A2IMP-Linux ».

Voici le déroulement de la méthode :

- Création de la main courante
- Insertion de la boîte à outils *a2impWin* (disponible sur le CDROM)
- Vérification de la date et de l'heure sur le système compromis
- Sauvegarde des informations volatiles
  - Enregistrement du trafic émis
  - Sauvegarde de la mémoire RAM
  - Obtention des informations sur l'état du système (script a2imp-win.bat)
- Arrêt de la machine proprement
- Démarrage avec le CDROM fourni
- Sauvegarde de l'espace de stockage

⇒ Nous allons supposer que la machine compromise s'appelle « compro » et qu'elle a comme adresse IP 10.1.1.1. Le prompt de la machine compromise sera :

```
[root@compro] #
```

⇒ Nous allons aussi supposer que la machine où l'on va sauvegarder les informations s'appelle « sauvegarde » et qu'elle a comme adresse IP 10.2.2.2. Le prompt de cette machine sera :

```
[user@sauvegarde] #
```

OPERATIONS « A CHAUD » (ONLINE)

## *5.1 Création de la main courante*

Cette main courante peut être traditionnelle (stylo + papier) ou électronique (édition d'un fichier sur un système sûr). Le principe est de noter chaque action réalisée et la date et l'heure à laquelle elle a été lancée.

> ⇒ À partir de maintenant, on va donc noter sur la main courante chaque action et l'horodatée.

## *5.2 Mise à disposition de la boite à outils a2impwin (CDROM)*

Sur la machine compromise, nous allons rendre accessible la boîte à outil *a2impWin* disponible sur le CDROM

À partir de maintenant, toutes les commandes tapées sur la machine compromise devront l'être à partir du répertoire courant de la boîte à outils *a2impWin*. Attention cependant, ces outils ne sont pas sûrs à 100 % car ils font appel aux DLL du système compromis.

⇒ On va prendre l'hypothèse que le CDROM est monté sur le lecteur D: et que l'on accède à cet espace par l'explorateur Windows. Une fois localisé dans le dossier a2impWin, il suffit de cliquer sur l'icone « cmd.exe ».

## *5.3 Vérification de la date et de l'heure sur le système compromis*

La première action est de vérifier date et heure du système compromis et de noter le delta par rapport à une source sûre (serveur *NTP* ou horloge parlante (numéro de téléphone : 3699)).

```
[machine compro D:\a2impWin>] date /T & time /T
```

## *5.4 Sauvegarde des informations volatiles*

### 5.4.1 Sauvegarde de la mémoire RAM

⇒ Attention, pour certaines versions (Windows 2003 SP1 et Vista ), la sauvegarde de la RAM n'est pas possible.

Deux étapes :

Ouverture d'un socket sur la machine de sauvegarde « sauvegarde »
Sauvegarde de la partition RAM

Ouverture d'un socket sur la machine de sauvegarde
Sur la machine de sauvegarde : ouverture d'un port en écoute (ici 1234) pour sauvegarder les informations transmises depuis la machine compromise à l'aide de la commande *nc* (*netcat*)

Remarque : ne vous connectez pas à la machine de sauvegarde depuis la machine compromise, vous risquez d'utiliser des commandes piratées et surtout vous allez modifier l'état initial de la machine compromise.

```
[root@machine sauvegarde] ./nc -l -p 1234 > sauvegarde-RAM
```

⇒ S'assurer qu'aucun filtre de paquets ne bloque le flux qui sera envoyé sur ce port, car si c'est le cas, aucune information ne pourra être enregistrée sur la machine de sauvegarde.

Remarque : on peut s'assurer que le port spécifié est bien mis à l'écoute par la commande « netstat -a »

Sauvegarde de la partition RAM
Sur la machine compromise, exécuter la commande dd contenu sur le CDROM. Le résultat doit être transmis sur la machine de sauvegarde à l'aide de la commande *nc* (*netcat*).

```
[machine compro D:\a2impWin>] dd if=\\.\PhysicalMemory | nc 10.2.2.2 1234
```

*Création de la somme de contrôle (hash) sur la machine de sauvegarde*

```
[root@machine sauvegarde] ./md5sum sauvegarde-RAM> sauvegarde-RAM.md5
```

Remarque : sur la machine compromise, il est inutile de créer la somme de contrôle (hash). Et cela pour deux raisons : ce hash ne sera jamais égal à celui effectué sur la RAM sauvegardée (machine « online ») et moins on fait d'opérations sur la machine compromise, mieux c'est.

### 5.4.2 Obtention des informations sur l'état du système

Deux étapes :
Ouverture d'un socket sur la machine de sauvegarde « sauvegarde »
Collecte des informations sur « compro » la machine piratée

Ouverture d'un socket sur la machine de sauvegarde
Sur la machine de sauvegarde : ouverture d'un port en écoute (ici 1234) pour sauvegarder les informations transmises depuis la machine compromise à l'aide de la commande *nc* (*netcat*)

```
[root@machine sauvegarde] ./nc -l -p 1234 > sauvegarde-info.txt
```

Collecte des informations sur la machine piratée
Sur la machine compromise « compro », exécuter le script « a2imp-win.bat » existant dans la boîte à outils *a2impWin* du CDROM. Il lance des commandes qui permettent d'obtenir des informations sur l'état du système : connexions réseaux, liste des processus, partitions,

environnement, modules. Pour ne pas modifier les données de la machine compromise, ces données doivent être transmises sur la machine de sauvegarde à l'aide de la commande *nc* (*netcat*). Mais avant d'exécuter ce script, il faut se positionner dans une nouvelle instance de l'interpréteur de commande de Windows.

```
[machine compro D:\a2impWin>] a2imp-win.bat | nc 10.2.2.2 1234
```

Ces informations nous seront utiles par la suite, pour rechercher, sans stress, des traces de compromission.

Remarque : pour acquérir des informations plus complètes sur le disque de la machine compromise, nous avons besoin d'écrire des fichiers temporaires sur le support contenant la boîte à outils. Cela est possible si le script s'exécute à partir d'un support sur lequel l'écriture est autorisé (par exemple une clef usb). C'est pour cette raison que nous avons défini un deuxième script plus complet « a2imp-win-all.bat ».

*Création de la somme de contrôle (hash) sur la machine de sauvegarde*

```
[root@machine sauvegarde] ./md5sum sauvegarde-info.txt > sauvegarde-info.txt.md5
```

Remarque : sur la machine compromise, il est impossible de créer la somme de contrôle (hash) et cela pour la bonne raison qu'il n'existe pas l'équivalent du fichier sauvegarde-info.txt.

## *5.5 Arrêt de la machine*

Une fois les informations volatiles sauvegardées, un arrêt de la machine compromise est nécessaire, via la procédure standard (shutdown).

Conseil : avant de redémarrer la machine compromise, il faut l'isoler du réseau et la connecter via un câble croisé ou un mini hub/switch à la machine de sauvegarde.

## *5.6 Redémarrage avec le CDROM Linux*

À partir de maintenant, nous allons utiliser sur la machine « compro » un système extérieur. Vérifier que vous pouvez redémarrer sur votre CDROM, sinon changer l'option de démarrage lors du démarrage de la machine compromise.

Le compte utilisateur de ce CDROM est root et il n'y a pas de mot de passe. Vérifier la connexion réseau avant d'aller plus loin « service network start ».

Remarque : dans un environnement sans DHCP, il faut attribuer une adresse IP à la machine compromise et il faut indiquer l'adresse IP de la passerelle.

```
[root@machine compro] ifconfig eth0 xxx.xxx.xxx.xxx netmask 255.255.255.xxx
[root@machine compro] ifconfig lo 127.0.0.1
[root@machine compro] route add default gw xxx.xxx.xxx.xxx
```

## *5.7 Sauvegarde de l'espace de stockage*

Le partitionnement des disques durs peut être obtenu par la commande « fdisk -l »

```
[root@machine compro] /a2impUnix/fdisk -l
```

```
Disk /dev/hda: 30.0 GB, 30005821440 bytes
255 heads, 63 sectors/track, 3648 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot      Start         End      Blocks   Id  System
/dev/hda1               1           6       48163+  de  Dell Utility
/dev/hda2   *           7        3647    29246332+   7  HPFS/NTFS
```

Cependant, même si le disque est partitionné, sur un système windows, il est recommandé de sauvegarder le disque en totalité car ainsi vous pourrez redémarrer virtuellement votre système.

Deux étapes :

Ouverture d'un socket sur la machine de sauvegarde « sauvegarde »
Sauvegarde de l'ensemble du disque dur

Ouverture d'un socket sur la machine de sauvegarde

Sur la machine de sauvegarde : ouverture d'un port en écoute (ici 1234) pour sauvegarder les informations transmises depuis la machine compromise à l'aide de la commande *nc* (*netcat*)

Remarque : ne vous connectez pas à la machine de sauvegarde depuis la machine compromise.

```
[root@machine sauvegarde] ./nc -l -p 1234 > sauvegarde-disque-dur
```

Sauvegarde de l'ensemble du disque dur

Sur la machine compromise, exécuter la commande dd contenu sur le CDROM. Le résultat doit être transmis sur la machine de sauvegarde à l'aide de la commande *nc* (*netcat*).

```
[root@machine compro] /a2impUnix/dd if=/dev/hda | /a2impUnix/nc 10.2.2.2 1234
```

Création de la somme de contrôle (hash) sur la machine compromise et sur celle de sauvegarde

Les deux résultats devront être stockés sur la machine de sauvegarde. Donc de nouveau il faut ouvrir un port en écoute (ici 1234) pour sauvegarder les informations transmises depuis la machine compromise à l'aide de la commande *nc* (*netcat*)

```
[root@machine sauvegarde] ./nc -l -p 1234 > compro-disque-dur.md5
```

Sur la machine compromise, exécuter la commande md5sum contenu sur le CDROM. Le résultat doit être transmis sur la machine de sauvegarde à l'aide de la commande *nc* (*netcat*).

```
[root@machine compro] /a2impUnix/md5sum /dev/hda | /a2impUnix/nc 10.2.2.2 1234
```

Remarque : le checksum est reçu sur la machine de sauvegarde quand est affiché rnleft=yy

Création de la somme de contrôle (hash) sur la machine de sauvegarde

```
[root@machine sauvegarde] ./md5sum sauvegarde-disque-dur >
                                        sauvegarde-disque-dur.md5
```

Remarque : Windows dispose d'une mémoire virtuelle, souvent appelée fichier d'échange. Il s'agit d'un mécanisme semblable à celui du *fichier de swap* UNIX. La taille par défaut du fichier d'échange de la mémoire virtuelle (Pagefile.sys) créé durant l'installation est 1,5 fois supérieure à la capacité de mémoire vive de votre ordinateur. Par défaut, ce fichier est situé à la racine du disque dur (commande dir pagefile.sys /a H)

# *6* Boîte à outils *a2impWin*

Elle a été construite à partir de la boîte à outils « Forensic Acquisition Utilities » auquel nous avons rajouté quelques binaires. Tous les binaires de cette boîte à outils s'utilisent en ligne de commande dans une fenêtre "cmd".

**Forensic Acquisition Utilities**
(disponible sur le site http://users.erols.com/gmgarner/forensics/)

Cette boîte à outils contient les binaires suivants :

- 1. dd.exe: A modified version of the popular GNU dd utility program
- 2. md5sum.exe: A modified version of Ulrich Drepper's MD5sum utility.
- 3. Volume_dump.exe: An original utility to dump volume information
- 4. wipe.exe: An original utility to sterilize media prior to forensic duplication.
- 5. nc.exe: A modified version of the netcat utility by Hobbit.

http://www.microsoft.com/technet/sysinternals/utilitiesindex.mspx

- 1. psinfo.exe
- 2. pslist.exe
- 3. psloggedon.exe
- 4. psservice.exe
- 5. listdlls.exe

http://www.foundstone.com/

- 1. fport.exe
- 2. ntlast.exe

Les binaires windows ajoutés dans le but de rendre la boîte à outils plus sûre sont :

- 1. cmd.exe
- 2. diskpart.exe
- 3. hostname.exe
- 4. ipconfig.exe
- 5. net.exe
- 6. netstat.exe
- 7. reg.exe

ainsi que l'utilitaire awk.exe pour rendre le script a2impWin.bat plus générique

Dans cette boîte à outils, nous avons ajouté deux DLL (msvcr70.dll et msvcp70.dll dans le répertoire DLLWIN2000) qui sont nécessaires au bon fonctionnement de la commande « netcat ».

## Annexe 1 : scripts a2imp-win

### Script a2imp-win.bat

```
@echo script d'automatisation de collecte d'information
@echo ################################

@echo Modification du prompt pour l'horodatage et le path étendu
set prompt_ini=%PROMPT%
PROMPT $p$_$d-$t$g

@echo date : Verification  et affichage de la date du systeme
cmd.exe /c date /T
@echo date : Verification  et affichage de l'heure locale du systeme
cmd.exe /c time /T
@echo ver : système et version du kernel en cours d execution
cmd.exe /c ver
@echo hostname : nom de la machine
hostname

@echo psloggedon : liste des personnes connectees (locale et ressources partagees)
psloggedon
@echo nlast : liste des dernieres connexions sur ce systeme
ntlast

@echo ipconfig /all : liste des interfaces reseau
ipconfig /all
@echo arp -a : Table ARP
arp -a
@echo netstat -s : statistiques des protocoles reseaux
netstat -s
@echo netstat -nr : table de routage
netstat -nr
@echo netstat -r : table de routage
netstat -r
@echo netstat -ano : liste des connexions reseau
netstat -ano
@echo netstat -ban : liste des connexions reseau avec les DLL utilises
netstat -ban
@echo fport : liste des connexions reseau
fport.exe

@echo psservice : liste des services avec leur permission
psservice.exe security
@echo pslist : liste des processus
pslist.exe
```

*@echo pslist -t : arborescence des processus*
*pslist.exe -t*
*@echo listdlls : liste des DLLs charges (par processus)*
*listdlls.exe*

*@echo path : liste des variables d'environnement*
*set*
*@echo net share : liste des partages offerts*
*net share*
*@echo net use : liste des disques montes*
*net use*
*@echo diskpart : liste des volumes, des disques et des partitions*
*diskpart -s listdisk.txt*

*@echo restauration du prompt d'origine*
*set PROMPT=%prompt_ini%*

**Script a2imp-win-all.bat**

*@echo script d'automatisation de collecte d'information*
*@echo ################################*

*@echo Modification du prompt pour l'horodatage et le path étendu*
*set prompt_ini=%PROMPT%*
*PROMPT $p$_$d-$t$g*

*@echo date : Verification  et affichage de la date du systeme*
*cmd.exe /c date /T*
*@echo date : Verification  et affichage de l'heure locale du systeme*
*cmd.exe /c time /T*
*@echo ver : système et version du kernel en cours d execution*
*cmd.exe /c ver*
*@echo hostname : nom de la machine*
*hostname*

*@echo psloggedon : liste des personnes connectees (locale et ressources partagees)*
*psloggedon*
*@echo nlast : liste des dernieres connexions sur ce systeme*
*ntlast*

*@echo ipconfig /all : liste des interfaces reseau*
*ipconfig /all*
*@echo arp -a : Table ARP*
*arp -a*
*@echo netstat -s : statistiques des protocoles reseaux*
*netstat -s*

```
@echo netstat -nr : table de routage
netstat -nr
@echo netstat -r : table de routage
netstat -r
@echo netstat -ano : liste des connexions reseau
netstat -ano
@echo netstat -ban : liste des connexions reseau avec les DLL utilises
netstat -ban
@echo fport : liste des connexions reseau
fport.exe

@echo psservice : liste des services avec leur permission
psservice.exe security
@echo pslist : liste des processus
pslist.exe
@echo pslist -t : arborescence des processus
pslist.exe -t
@echo listdlls : liste des DLLs charges (par processus)
listdlls.exe

@echo path : liste des variables d'environnement
set
@echo net share : liste des partages offerts
net share
@echo net use : liste des disques montes
net use
@echo diskpart : liste des volumes, des disques et des partitions
diskpart -s listdisk.txt > res.txt
@echo list disk > info-sur-disque.txt
@echo list volum >> info-sur-disque.txt
awk -f script.awk res.txt >> info-sur-disque.txt
diskpart -s info-sur-disque.txt

@echo restauration du prompt d'origine
set PROMPT=%prompt_ini%
```

## Annexe 2 : enregistrement du trafic réseau émis par une machine

**Si on veut faire la trace depuis une machine saine dans un réseau « switché», cas le plus courant actuellement, il y a trois possibilités :**

**1. Recopie de port au niveau du swicth : en principe, indolore pour la machine piratée et pour le réseau.**

La recopie de ports supposent :
- avoir des switches qui supportent cette fonctionnalité
- pouvoir avoir accès à la configuration du switch ce qui n'est pas possible lorsque comme cela est assez fréquent le réseau est géré par une autre entité
- connaître sur quel port est connecté la machine concernée, ce qui suppose de disposer d'un plan de câblage à jour
- avoir physiquement accès au switch et y avoir un port libre pour pouvoir connecter la machine d'analyse. Certes il est possible sur certains types de matériel de recopier un port sur un autre switch du réseau, ce qui est sûrement la situation la plus confortable car on n'a pas à déplacer une machine, par contre cette disposition n'est pas supportée par tous les switches et cela reste plus ou moins propriétaire.
- avoir noté et testé auparavant la séquence de commandes à effectuer le jour venu. Ce n'est pas toujours trivial et d'un matériel à l'autre et même d'une version à l'autre cela change pas mal.

**2. Recopie de port au niveau du firewal : en principe, indolore pour la machine piratée et pour le réseau.**

Certes cela ne permet pas de détecter ce que ferait une machine pour infecter une autre machine sur le réseau. Mais généralement le firewall est plus accessible que le switch auquel est reliée la machine, il est donc plus facile d'analyser le trafic à ce niveau.

Plusieurs possibilités sont envisageables :

- On a déjà un IDS qui écoute le trafic, il suffit alors de le reconfigurer pour enregistrer le trafic lié à la machine suspecte.
- Sur certains firewalls comme ceux construits à partir de système Linux ou BSD, il est possible de lancer une commande (dumpcap, tcpdump...) qui va permettre d'enregistrer le trafic.
- Il reste toujours la possibilité de faire une recopie de port du firewall ou de connecter un boîtier intermédiaire. Réserver un port sur un switch et le configurer une fois pour toute en recopie du port du firewall est parfaitement envisageable car ne demande pas beaucoup de ressources supplémentaires. Le jour où l'on veut analyser le trafic il suffit de brancher une machine sans à avoir à changer une quelconque configuration avec les risques que cela comportent surtout en période de stress.

Mais faut-il écouter en amont ou en aval du firewall ?

Pour un IDS il est probablement plus judicieux de regarder uniquement les attaques qui ont traversé le firewall car cela limite le nombre d'alertes.

Pour écouter une machine piratée c'est moins évident. Si on écoute côté externe on verra tout ce que qu'envoie l'attaquant mais pas forcément tout le trafic de la machine piratée vers l'extérieur qui peut en partie être filtré par le firewall. Si on écoute sur le réseau interne ce sera l'inverse.

**3. Insertion d'un hub qui relira la machine saine et la machine piratée : pas indolore pour la machine piratée, car il faut insérer entre la machine et la prise murale, un hub. Pendant un laps de temps court la machine piratée n'est plus connecté au réseau.**

Le fait de couper la liaison, d'introduire un hub puis de reconnecter va déclencher sur le switch et sur la machine une renégociation des paramètres de la connexion :

- on va passer de full duplex à half duplex
- éventuellement le switch va faire du spanning tree pour déterminer qui est connecté derrière lui et s'assurer qu'il n'y a pas de boucle. Cela peut-prendre plusieurs dizaines de secondes
- on peut avoir aussi à refaire une authentification 802.1X ce qui est loin d'être innocent

Mais est-ce si grave ? Généralement les protocoles de niveau plus élevé se récupèrent assez bien en cas d'erreur de la couche réseau.

**Si on veut faire la trace depuis la machine piratée,**

**Windump (le portage tcpdump sous windows) : indolore si WinPCap est déja installé mais pas indolore sinon.**

Solution pas très réaliste. L'installation après piratage de l'outil va prendre trop de temps, modifier trop de choses en mémoire et sur le disque. Quant à l'installer systématiquement sur toutes les machines pour le cas où interviendrait un piratage ne me semble pas une bonne idée. Tout d'abord les produits d'analyse ne sont pas eux-mêmes exempts de failles de sécurité. Ensuite il ne faut jamais perdre de vue que l'objectif premier est de faire fonctionner des machines avec le maximum de sécurité mais de pas de créer un réseau de pots de miel.

## Annexe 3 : image complète de la mémoire RAM

Par défaut, Windows ne génère d'image complète de la mémoire qu'en cas de problème système majeur. Une fonctionnalité de 2000 et de XP permet d'aboutir à cet état manuellement, à condition de l'avoir prévu en avance et de provoquer un « crash » de la machine. Cette solution n'est pas à conseiller, car le fichier « dump » est créé sur le disque de la machine compromise.

*Pour programmer un Dump de la RAM (*http://www.labo-microsoft.com/t/1745/ *)*

1. *Aller dans Démarrer >> Paramètres >> Panneau de configuration >> Système*
2. *Choisir l'onglet Avancé puis Paramètres du menu Démarrage et récupération*
3. *Sélectionner le type de dump "Image mémoire complète" et le fichier cible (obligatoirement sur une unitée montée afin de ne pas altérer les données du système audité ; la taille d'un dump est légèrement supérieur à la taille de la mémoire )*
4. *Via regedit, ajouter dans HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\i8042prt\Parameters la clef CrashOnCtrlScroll de type REG_DWORD et de valeur 1*
5. *"Rebooter"*

*Pour créer un Dump de la RAM à la demande (*http://www.labo-microsoft.com/t/1745/ *)*

1. *Maintenir la touche CTRL (à droite de la barre d'espace) enfoncée puis appuyer deux fois sur SCROLL LOCK*
2. *Le système "plante" et le dump est généré à l'emplacement prévu*