Documentation A2IMP-Linux

Version 2007-01-23 pour la boîte à outils *A2IMP-linux* v0.6
Adaptée pour Capitoul le 31 mars 2009

Auteurs : Denis Pugnère <d.pugnere@ipnl.in2p3.fr>
Contributions : Cédric Hillembrand <Cedric.Hillembrand@cesr.fr>
Christophe Dubois <Christophe.Dubois@certa.ssi.gouv.fr>
Marie-Claude Quidoz <Marie-Claude.Quidoz@urec.cnrs.fr>
Relectures : Nicole Dausque <nicole.dausque@urec.cnrs.fr>

Résumé :

Cette documentation a été réalisée pour décrire comment utiliser la boîte à outils A2IMP-linux (Aide à l'Acquisition d'Information sur une Machine Piratée – version Linux). Cette documentation contient les références, conseils et commandes utiles 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 2
2 Principes de base 2
3 Disposer de moyens d'écoute du trafic réseau 3
4 Méthode 4
4.1 Vérification de la date et de l'heure sur le système compromis 5
4.2 Création de la main courante 5
4.3 Montage de la boîte à outils (CDROM) 5
4.4 Sauvegarde des informations volatiles 5
4.4.1 Ouverture d'un socket sur la machine de sauvegarde 5
4.4.2 Enregistrement continu des informations saisies par la commande « script » 6
4.4.3 Sauvegarde de la mémoire RAM 6
4.4.4 Obtention des informations sur l'état du système 7
4.5 Arrêt – redémarrage de la machine 8
4.6 Sauvegarde de l'espace de stockage 8
4.6.1 Sauvegarde de l'espace de stockage SWAP 9
4.6.2 Sauvegarde de l'espace de stockage des partitions système 10
4.7 Vérification des images 11
4.8 Arrêt de la session 11
5 Références 12

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 Méthode

Cette méthode détaille les commandes à taper pour réaliser la phase d'acquisition de données en tenant compte des principes de base précédemment décrits. Nous posons l'hypothèse que nous avons une machine propre « de sauvegarde » connectée en réseau à la machine compromise via un câble croisé ou un mini *switch*, cette machine de sauvegarde recevra les données pour les stocker sur le disque local, elle contiendra les commandes « *nc* » et « *md5sum* » fournies.

Voici le déroulement de la méthode :

- Vérification de la date et de l'heure sur le système compromis
- Création de la main courante
- Montage de la boîte à outils (CDROM)
- Sauvegarde des informations volatiles à l'aide des commandes de la boîte à outils
  - Ouverture d'un socket sur la machine de sauvegarde
  - Enregistrement continu des informations saisies par la commande « *script* »
  - Sauvegarde de la mémoire RAM
  - Obtention des informations sur l'état du système
- Arrêt-redémarrage de la machine à partir du CD bootable
- Sauvegarde de l'espace de stockage
  - Sauvegarde de l'espace de stockage SWAP
  - Sauvegarde de l'espace de stockage des partitions système
- Vérification de la signature des images
- Arrêt de la session

⇒ 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)

4.1 *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.

Cette opération peut se réaliser de plusieurs manières :

- on peut utiliser la commande *date* (présente sur le CD *A2IMP-linux*), à comparer avec une source sûre : serveur *NTP* ou alors l'horloge parlante (numéro de téléphone : 3699)
- pour vérifier éventuellement que le système est synchronisé avec une source réseau précise (par exemple ntp) : commandes *ntpstat* ou *ntpdc*

Il ne faut pas modifier l'heure du système, si une modification est faite, il faut noter cette modification dans la main courante pour pouvoir en tenir compte par la suite.

4.2 *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. Le résultat de cette commande pourra être stocké à part.

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

4.3 *Montage de la boîte à outils (CDROM)*

Sur la machine compromise, nous allons monter le CDROM *A2IMP-linux* sur le point de montage */mnt/cdrom* (on utilise les outils système pour cela, on ne peut pas faire autrement) :

```
[root@compro] # mkdir /mnt/cdrom
[root@compro] # mount /dev/cdrom /mnt/cdrom
[root@compro] # cd /mnt/cdrom
```

À partir de maintenant, toutes les commandes que l'on tapera sur la machine compromise seront celles réputées sûres car exécutées depuis le CDROM, en spécifiant le chemin d'accès aux commandes, par exemple :

```
[root@compro] # /mnt/cdrom/date
```

4.4 *Sauvegarde des informations volatiles*

4.4.1 Ouverture d'un socket sur la machine de sauvegarde

Sur la machine de sauvegarde : ouverture d'un port en écoute (ici 10000) pour sauvegarder les informations sur les commandes tapées sur la machine compromise à l'aide de la commande *nc* (*netcat*):

```
[user@sauvegarde] # nc -l -p 10000 > session.txt
```

⇒ S'assurer qu'aucun filtre de paquets (*iptables, ipchains, pf, ipfilter*...) ne bloque le

flux qui sera envoyé sur ce port, car si c'est le cas, aucune information ne sera enregistrée sur la machine de sauvegarde.

4.4.2 Enregistrement continu des informations saisies par la commande « script »

Sur la machine compromise, on ne doit pas modifier les informations sur le disque et donc avoir un minimum d'impact sur les informations volatiles. De plus on doit garder une trace des actions réaliser pour pouvoir par la suite expliquer les éventuelles modifications systèmes.

Pour réaliser cette action, nous créons une *fifo.* Puis nous utiliserons la commande « *script* » qui enverra tout ce qui a été tapé en local dans la *fifo*, *et nous utiliserons la* commande *nc* pour l'envoi sur la machine de sauvegarde.

Création de la *fifo* (ici, le fichier *fifo* est /tmp/session-a2imp, on peut aussi créer cette fifo sur une disquette ou sur une clé USB préalablement montées) :

```
[root@compro] # /mnt/cdrom/mkfifo /tmp/session-a2imp
```

On prépare l'envoi à distance (à l'adresse IP 10.2.2.2, port tcp 10000) via la commande *nc*) de tout ce qui sera envoyé dans la fifo :

```
[root@compro] # /mnt/cdrom/cat /tmp/session-a2imp | /mnt/cdrom/nc 10.2.2.2 10000
```

Depuis un autre *terminal*, lancer la commande « script » qui enregistre tout ce qui est lancé et tous les résultats dans la *fifo* précédemment créée :

```
[root@compro] # /mnt/cdrom/script -f /tmp/session-a2imp
```

⇒ Maintenant, grâce à la commande « *script* », tout ce qui est tapé et affiché **dans ce terminal** sera envoyé à distance (sur le port 10000) sur la machine de sauvegarde.

4.4.3 Sauvegarde de la mémoire RAM

⇒ Dans certains cas la sauvegarde de la *RAM* n'est pas possible. Par exemple, si la protection *SELinux* est activée, celle ci empêche de lire le contenu de la *RAM* avec la commande dd. L'option *SELinux* est activée par défaut sur les systèmes *Redhat Entreprise Linux v4* (voir le fichier */etc/selinux/config* et le code de retour de la commande *selinuxenabled*).

On va sauvegarder le contenu de la *RAM* en exécutant un « *nc* » qui écoute sur un port (ici *9000*) sur la machine de sauvegarde (ne pas réutiliser le port *10000* toujours en cours d'utilisation pour l'enregistrement des commandes tapées dans le terminal). Le *dump* envoyé depuis la machine compromise sera reçu sur la machine de sauvegarde et sera enregistré dans le fichier *compro-RAM.dd.*

Création de la socket de réception sur la machine de sauvegarde et enregistrement des informations reçues dans le fichier *compro-RAM.dd* :

```
[user@sauvegarde] # nc -l -p 9000 > compro-RAM.dd
```

⇒ S'assurer (comme précédemment) qu'aucun filtre de paquets (*iptables, ipchains, pf, ipfilter*...) ne bloque le flux qui sera envoyé sur ce port, car si c'est le cas, aucune information ne sera enregistrée sur la machine de sauvegarde.

Maintenant, on sauvegarde le contenu de la *RAM* à l'aide de la commande *dd* : La mémoire RAM est accessible par les fichiers */dev/mem* ou */proc/kcore*

Horodatage :

```
[root@compro] # /mnt/cdrom/date
```

Puis la sauvegarde :

```
[root@compro] # /mnt/cdrom/dd if=/dev/mem | /mnt/cdrom/nc 10.2.2.2 9000
[root@compro] # CTRL + C
```

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

```
[user@sauvegarde] # md5sum compro-RAM.dd >  compro-RAM.dd.md5
```

4.4.4 Obtention des informations sur l'état du système

Maintenant que l'on a sauvegardé le contenu de la RAM, on peut exécuter le script « *a2imp-auto.sh* » existant sur le CDROM. Il lance des commandes qui permettent d'obtenir des informations sur l'état du système : connexions réseaux, liste des processus, partitions, environnement, modules. On peut l'exécuter avec la commande :

```
[root@compro] # /mnt/cdrom/a2imp-auto.sh
```

Ces informations (qui seront sauvegardées dans la main courante) nous seront utiles pour rechercher des traces de compromission par la suite.

4.5 Arrêt – redémarrage de la machine

Pour minimiser les risques d'incohérences, il est préférable de réaliser l'opération de sauvegarde de l'espace de stockage depuis les systèmes de fichiers démontés. Il faut tout d'abord stopper la machine proprement en utilisant la procédure habituelle (par exemple, la commande *shutdown*).

Il faut noter que cette opération présente quelques risques : l'opération d'arrêt d'une machine *Unix* est une opération qui exécute séquentiellement plusieurs dizaines de scripts et exécutables, qui modifie plusieurs fichiers (notamment les fichiers de *logs* systèmes et applicatifs). Cette opération laisse donc des traces importantes dans les fichiers systèmes.

La procédure d'arrêt de la machine va couper la session d'enregistrement des commandes tapées (cf paragraphe 3.4.2), il faudra donc ouvrir une nouvelle session pour enregistrer la suite des opérations.

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
```

4.6 Sauvegarde de l'espace de stockage

Pour la sauvegarde, il y a plusieurs manières de réaliser cette opération :

- On peut redémarrer la machine sans démonter physiquement le disque système en utilisant un CD bootable ou autre (clé USB...) qui reconnaît les périphériques, contrôleurs et disques du système, mais qui ne fait aucune modification sur les partitions (exemple de l'option *noswap* au *boot Linux* d'une knoppix). D'autre part, il faut que le CD :
  - contienne le support des pilotes des cartes Ethernet et contrôleurs disques (*SATA, SCSI*...)
  - supporte les systèmes de fichiers (*ext2, ext3, xfs, reiserfs*...) ou de partitionnement utilisés par le système (*LVM, EVMS*)
  - contienne également les commandes nécessaires pour la sauvegarde (*dd, nc, date*...)
- On peut aussi extraire physiquement le disque dur et utiliser un boîtier spécialisé pour réaliser la sauvegarde des partitions ou du disque dans son intégralité.

Le partitionnement des disques durs peut être obtenu par des commandes comme « *fdisk -l* » ou *df*. Les informations sur les systèmes de fichiers montés, sur les disques et partitions ont été relevées par le script *a2imp-auto.sh* précédemment lancé. Voir le fichier *session.txt* présent sur le système de sauvegarde.

Exemple : pour connaître la liste des partitions :

```
[root@compro] # /a2impUnix/date
[root@compro] # /a2impUnix/fdisk -l
```

```
Disk /dev/sda: 18.3 GB, 18373349376 bytes
255 heads, 63 sectors/track, 2233 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot    Start       End    Blocks   Id  System
/dev/sda1   *         1      1275  10241406   83  Linux
/dev/sda2          1276      1657   3068415   82  Linux swap
/dev/sda3          1658      2233   4626720   83  Linux

Disk /dev/sdb: 18.3 GB, 18373349376 bytes
255 heads, 63 sectors/track, 2233 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

   Device Boot    Start       End    Blocks   Id  System
/dev/sdb1   *         1       637   5116671   83  Linux
/dev/sdb2           638      1019   3068415   83  Linux
```

On voit ici qu'il y a des partitions Linux de type systèmes de fichiers et SWAP.

4.6.1 Sauvegarde de l'espace de stockage SWAP

Il est important de sauvegarder l'espace SWAP, car il révèle potentiellement des informations sur des processus précédemment lancés. Il est important de réaliser cette opération à froid pour ne pas le modifier pendant le déroulement de sa sauvegarde.

Linux peut utiliser le *SWAP* sur une partition dédiée ou utiliser un « *fichier swap* ». Le script « *a2imp-auto.sh* » précédemment lancé contient la commande « `cat /proc/swaps` » qui permet de connaître les espaces de swap utilisés par le système.

Pour sauvegarder le contenu de chaque zone *SWAP*, on exécute d'abord un « *nc* » qui écoute sur le port *9000* sur la machine de sauvegarde, le *dump* qui sera reçu sera enregistré dans le fichier *compro-SWAP-sda2.dd* :

```
[user@sauvegarde] # nc -l -p 9000 > compro-SWAP-sda2.dd
```

Horodatage :

```
[root@compro] # /a2impUnix/date
```

Maintenant, on sauvegarde le contenu du *SWAP* de la partition /dev/sda2 :

```
[root@compro] # /a2impUnix/dd if=/dev/sda2 | /a2impUnix/nc 10.2.2.2 9000
[root@compro] # CTRL + C
```

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

```
[user@sauvegarde] # md5sum compro-SWAP-sda2.dd > compro-SWAP-sda2.dd.md5
```

Il peut arriver que certaines zones du disque soient endommagées (donc illisibles) et empêchent la copie par *dd* : dans ce cas, on peut ajouter les options « *conv=noerror,sync* » qui permettent de remplacer dans l'image les zones illisibles par une suite de zéros. Exemple :

```
[root@compro] # /a2impUnix/dd if=/dev/sda2 conv=noerror,sync | /a2impUnix/nc 10.2.2.2 9000
```

> ⇒ Si vous utilisez les options « conv=noerror,sync » sur un disque qui a des secteurs défectueux, il faudra bien penser à créer une signature de l'image, par contre il sera impossible de vérifier l'intégrité de l'image prise par rapport à l'original (disque physique ou partition).

4.6.2 Sauvegarde de l'espace de stockage des partitions système

Les partitions que l'on va sauvegarder sont principalement les partitions systèmes, c'est-à-dire celles où un intrus aurait pu déposer ses outils utilisés pour la compromission. Dans la plupart des cas, cela ne sert à rien de sauvegarder les partitions utilisateurs (généralement /home), mais c'est à apprécier au cas par cas.

La sauvegarde des disques ou partitions systèmes est à répéter pour chaque partition et/ou disque à sauvegarder. Dans la liste des partitions données par la commande *fdisk*, nous avons */dev/sda1*, */dev/sda3*, */dev/sdb1* et */dev/sdb2*

Exemple pour sauvegarder la partition */dev/sda1* :

```
[user@sauvegarde] # nc -l -p 9000 > compro-dd-sda1
```

Horodatage :

```
[root@compro] # /a2impUnix/date
[root@compro] # /a2impUnix/dd if=/dev/sda1 | /a2impUnix/nc 10.2.2.2 9000
[root@compro] # CTRL + C
```

ou
Pour sauvegarder l'ensemble du disque (ici /dev/sda) en « morceaux » de 2Go :

```
[user@sauvegarde] # nc -l -p 9000 | split -d -b 2000m - compro-dd-sda.split
```

Horodatage :

```
[root@compro] # /a2impUnix/date
[root@compro] # /a2impUnix/dd if=/dev/sda | /a2impUnix/nc-10.2.2.2 9000
[root@compro] # CTRL + C
```

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

sauvegarde de la partition */dev/sda1*) :

```
[user@sauvegarde] # md5sum compro-dd-sda1 >  compro-dd-sda1.md5
```

Il est aussi possible de compresser les images des partitions ou du *SWAP* pendant ou après le transfert sur la machine de sauvegarde, exemple :

```
[user@sauvegarde] # nc -l -p 9000 > compro-dd-sda1.gz
[root@compro] # /a2impUnix/date
[root@compro] # /a2impUnix/dd if=/dev/sda1 | /a2impUnix/gzip -c | /a2impUnix/nc-
10.2.2.2 9000
[root@compro] # /a2impUnix/date
[root@compro] # /a2impUnix/md5sum /dev/sda1
[user@sauvegarde] # md5sum compro-dd-sda1.gz >  compro-dd-sda1.gz.md5
```

> ⇒ Si vous compressez les images des partitions ou des disques, penser à créer à la fois une signature de l'original mais aussi une signature de l'image compressée.

4.7 Vérification des images

Nous avons créé des images du *SWAP*, des disques ou des partitions, nous avons également pris le soin de créer des signatures de ces images.

Exemple :

```
[user@sauvegarde] # md5sum -c compro-SWAP.dd.md5
compro-SWAP.dd: OK
```

Dans ce cas, la signature est bonne car la somme de contrôle de l'image correspond à la somme de contrôle calculée précédemment.

Autre exemple :

```
[user@sauvegarde] # md5sum -c compro-SWAP.dd.md5
compro-SWAP.dd: : FAILED
md5sum: WARNING: 1 of 1 computed checksum did NOT match
```

Dans ce cas précis, la signature de l'image ne correspond pas à la signature, on en déduit que l'image a été modifiée, elle est à considérer comme non valide.

4.8 Arrêt de la session

Depuis le *terminal* où a été lancée la commande « *script* » qui enregistre tout ce qui est lancé, il faut taper « exit » ou la combinaison de touches Control-D pour arrêter l'enregistrement de la session

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

5 Références

Note CERTA-2002-INF-002-002 : Les bons réflexes en cas d'intrusion sur un système d'information http://www.certa.ssi.gouv.fr/site/CERTA-2002-INF-002

RFC 3227 : Guidelines for Evidence Collection and Archiving http://www.ietf.org/rfc/rfc3227.txt

Annexe : contenu du script a2imp-auto.sh de la boîte à outils a2imp-linux

```
#!/bin/bash
echo "script d'automatisation de collecte d'information sur un systeme a l'aide"
echo "de la boite a outils A2IMP-linux"
echo "(c) CNRS / D.Pugnere 11/09/2006"
echo "################################################################################"
echo -e "### => date : Verification  et affichage de l'heure locale du systeme"
./date
echo -e "\n### => uname -a : version du kernel en cours d execution"
./uname -a
echo -e "\n### => cat /proc/sys/kernel/hostname : hostname"
./cat /proc/sys/kernel/hostname
echo -e "\n### => cat /proc/sys/kernel/osrelease : version du kernel"
./cat /proc/sys/kernel/osrelease
echo -e "\n### => uptime"
./uptime
echo -e "\n### => who : liste des personnes connectées"
./who
echo -e "\n### => w : liste des personnes et leur activité"
./w
# echo -e "\n### => last : liste des dernières connexions sur ce système"
# ./last
echo -e "\n### => lsmod : liste des modules du kernel"
./lsmod
echo -e "\n### => cat /proc/modules : liste des modules du kernel"
./cat /proc/modules
echo -e "\n### => dmesg : Logs du kernel depuis le boot"
./dmesg
echo -e "\n### => ifconfig -a : liste des interfaces reseau"
./ifconfig -a
echo -e "\n### => arp -an : Table ARP"
./arp -an
echo -e "\n### => netstat -s : statistiques des protocoles reseaux"
./netstat -s
echo -e "\n### => netstat -nr : table de routage"
./netstat -nr
echo -e "\n### => route -Cn : table de routage"
./route -Cn
echo -e "\n### => netstat -anp : liste des connexions reseaux"
./netstat -anp
echo -e "\n### => lsof -n -i4 : liste des connexions reseau IPv4"
./lsof -n -i4
echo -e "\n### => lsof -n -i6 : liste des connexions reseau IPv6"
./lsof -n -i6
echo -e "\n### => ps -eaxf : liste des processus"
./ps -eaxf
echo -e "\n### => pstree : arborescence des processus"
./pstree
echo -e "\n### => lsof -n -P -l : liste de tous les processus, des librairies et des fichiers
ouverts"
./lsof -n -P -l
echo -e "\n### => sysctl -a : liste de toutes les variables du kernel"
./sysctl -a
echo -e "\n### => printenv : liste des variables d'environnement"
./printenv
echo -e "\n### => df : liste des montages actifs vus par la commande df"
./df
echo -e "\n### => cat  /proc/mounts : liste des montages vus par le kernel"
./cat /proc/mounts
echo -e "\n### => cat  /proc/partitions : liste des partitions des disques detectés par le kernel"
./cat /proc/partitions
echo -e "\n### => cat  /proc/swaps : liste des espaces swap utilisés par le système"
./cat /proc/swaps
echo -e "\n### => fdisk -l /dev/(h|s)d[a-z] : liste des partitions des disques par fdisk"
for disk in `./tail -n+3 /proc/partitions | ./grep -E " (h|s)d[a-z]\b" | ./tr -s ' ' ' ' | ./cut -
d" " -f 5`; do  ./fdisk -l /dev/$disk; done
echo -e "\n### => ifpromisc : verification du mode PROMISC sur les interfaces ethernet"
./ifpromisc
echo -e "\n### => chkproc : verification des processus cachés dans ps"
./chkproc
echo -e "\n### => listps : "
./listps
```