Analyses forensiques

Outillages libres/ouverts au service de l'analyse des supports informatiques

Michel Roukine
m.roukine@gmail.com

RéSIST -- 25 septembre 2007

A propos de cette présentation

- Son objectif est de survoler l'essentiel de l'outillage libre disponible pour l'analyse forensique des supports informatiques:

- 1 - Linux et les outils GNU
- 2 - Outils d'acquisition des données
- 3 - Outils d'analyse des systèmes de fichiers
- 4 - Outils spécifiques

Linux et les outils GNU

- Une boîte à outils simple et puissante
- Acquisition de données
- Examen de la table des partitions
- Exploration des systèmes de fichiers
- Recherches dans l’espace non alloué

Acquisition d’une image

- Examen des paramètres du disque dur
  - dmesg | grep hd # informations de démarrage
  - hdparm
    - hdparm -I /dev/hdx # informations identification
    - hdparm -g /dev/hdx # géométrie du disque dur
  - fdisk -l /dev/hdx # affiche la table des partitions

Créer une image avec dd

dd est une commande de base commune à tous les systèmes Unix. dd permet de copier un fichier (sous Unix/Linux tout est fichier ... ou processus) en effectuant éventuellement des opérations de conversion

- Exemple 1 : copie d'une partition de disque dur
  - dd if=/dev/hdg1 of=/.../pièce_x-part1.dd
- Exemple 2 : copie d'un CD comportant des secteurs erronés
  - dd conv=noerror,sync if=/dev/hdc of=/.../CD18.dd
- A l'aide de la commande netcat (nc) il est possible de copier disques et partitions au travers d'un réseau

Monter une partition à partir d’une image

Il est possible, en utilisant les "loop devices" de monter l’image d’une partition créée avec dd

- Exemple :
  - mount -o loop,ro /.../image.dd /mnt/hdtemp

Rechercher un fichier

La commande find permet de rechercher des fichiers en combinant de multiples critères : nom, taille, dates MAC, ... c'est une commande très puissante qui peut elle-même faire appel à d'autres commandes

- Exemple 1 : recherche des fichiers .txt
  - find /.../Content.IE5 -iname "*.txt"
- Exemple 2 : recherche des fichiers .txt dont la taille soit inférieure à 50 octets
  - find /.../Content.IE5 -iname "*.txt" -size -50c

Rechercher une chaîne (grep)

La commande grep recherche, dans les fichiers spécifiés, les occurences d'une expression régulière (ou rationnelle)

- exemple : rechercher un mot à l'orthographe incertaine dans un fichier
  - grep -i 'po(e|u)lvorde?' acteurs.txt
- attention à l'encodage des chaînes recherchées (voir notamment la commande strings)

Examiner en hexadécimal

Plusieurs commandes permettent d’examiner des fichiers en affichant leur contenu en hexadécimal : xxd, hexdump

Rechercher une chaîne (strings)

strings permet d'extraire de tout fichier, notamment binaire, des chaînes de caractères

- exemple : obtenir les chaînes ascii (8bits) contenues dans une partition
  - strings -e S </dev/hdg2 >/home/expert/hdg2.strings
- exemple : afficher les chaînes unicodes (16 bits) contenues dans un fichier word
  - strings -e b grosDocumentSuspect.doc

Déterminer le type d’un fichier

la commande file essaie de deviner le type d’un fichier à partir d’informations (magic numbers) contenues au début et à la fin de ce fichier

- Exemple : afficher le type des fichiers contenus dans un répertoire indépendamment de leur extension.
  - file * |less

Outils d’acquisition des données

- Sous Linux les trois outils d’acquisition les plus répandus sont:
- 1 - dd : l’outil d’origine, à la fois simple, puissant et incontesté
- 2 - dcfldd : cette version de dd permet notamment le calcul des clés md5 ou sha au moment de l’acquisition
- 3 - sdd : il s’agit là d’une version de dd qui privilégie la vitesse d’acquisition.
- Enfin, il y a lieu de mentionner "netcat" (nc) qui, bien que n’étant pas un outil d’acquisition à proprement parler, permet d’effectuer des acquisitions au travers d’un réseau

Outils d’analyse des systèmes de fichiers

- Quelles sont les principales ressources ?
- 1 - Sleuthkit : la référence en matière d’outil libre d’analyse forensique
- 2 - Autopsy : il s’agit essentiellement d’une interface graphique pour Sleuthkit
- 3 - Outils de récupération (hors Sleuthkit) : Fatback, Foremost, Ntfsundelete
- 4 - De nombreux outils spécifiques (galetta, pasco, rifiuti, ...)

Sleuthkit

Sleuthkit est un ensemble de commandes qui permettent :

- d'analyser, entre autres, les systèmes de fichiers FAT et NTFS
- d'analyser les disques et les partitions aux formats DOS, BSD, Sun et Mac
- de récupérer des données supprimées
- d'établir une chronologie des accès MAC aux fichiers
- de trier les fichiers exitants et récupérés en fonction de leur clé MD5 ou SHA et de leur type

Sleuthkit : sorter et mactime

- sorter trie les fichiers supprimés (et récupérables) ou présents dans une image en fonction du type du fichier : exec, text, document, archive, audio, image, video, system, ...
- mactime produit une chronologie des accès MAC aux fichiers dont les méta-données n’ont pas été détruites

Récupération de fichiers

- Fatback pour les systèmes de fichier FAT, en modes interactif ou automatique
- Foremost travaille directement à partir d'une image (disque, partition, dd, enCase, safeBack ...) et récupère les fichiers en "reconnaissant" leur début et leur fin
- Ntfsundelete comme son nom l'indique. Fonctionne selon les modes : scan, undelete et copy.

Outils libres de Foundstone

Ces outils peuvent fournir leurs résultats sous un format "tabulé" et s’exécutent sous Win32(cygwin), Linux, Mac OS X et BSD’s

- Galleta analyse les "cookies" d’IE
- Pasco reconstitue le contenu du fichier index.dat du cache d’IE
- Rifiuti reconstitue le contenu du fichier INFO2 de la corbeille

CD amorçables (LiveCDs)

Deux CD amorçables sont adaptés à l'analyse technico-légale sous Linux:

- Le "FCCU GNU/Linux Forensic Boot CD" de Christophe Monniez et Geert Van Acker

http://www.lnx4n6.be

- Le "Helix LiveCD" de e-fense.com

http://www.e-fense.com/helix/

Webographie

- www.sleuthkit.org
  - Sleuthkit & autopsy : forensic tools for linux and other unixes
- www.opensourceforensics.org
  - Open source digital forensics
- www.forensicswiki.org
  - Forensics Wiki
- www.e-evidence.info
  - The electronic evidence information center
- www.forensicfocus.com
  - Computer forensics news, information and community