Formation A2IMP

Présentation Boîtes à outils et TP

Capitoul

Cédric Hillembrand (CESR) – mars 2009

D’après les diapositives de D. Pugnère (IN2P3)

Boîtes à Outils et TP - Plan

- ***Les Boîtes à outils***
  - Le concept
  - Les fonctionnalités générales
  - Les différentes boîtes à outils
  - La boîte à outils : A2IMP
- ***Les TP***
  - Organisation
  - Méthodologie
  - Particularités Linux
  - Particularités Windows

Boîtes à Outils – Concept

- ***Approche différente suivant la situation***
  - Système (encore) fonctionnel : online
    - Utilisation d'utilitaires statiques depuis le support amovible,
    - Analyse du système.
  - Système stoppé : offline
    - Démarrage sur un système qui permet d'accéder au stockage,
    - Dump images disques ou des partitions disponibles.

Boîtes à Outils – Fonctionnalités

- Boite à outils statique (indépendante de la machine hôte),
- Elle permet :
  - Copie disques, RAM et swap,
  - Énumération des processus,
  - Énumération des connexions ouvertes,
  - Énumération de l'environnement (configuration),
  - Détection du type et des propriétés des fichiers,
  - Recouvrement des données effacées,
  - Suivi de l’activité du système,
  - Capture réseau.
- Transfert des données vers un site distant via le réseau,
- Contrôle de l'intégrité (calcul du hash).

Boîtes à Outils – Différentes BàO

- ***Orientées sécurité et Forensics :***
  - ***Knoppix std (security tools distribution)***
  - ***Fire***
  - ***Helix***
  - ***…***
- ***Notre choix :***
  - ***Mandriva***

Boîtes à Outils – A2IMP

- ***Pourquoi ce choix :***
  - Outils compilés en statique pour l'utilisation sur un système Linux online à disposition,
  - Création d'un CD bootable Linux de type LiveCD
    - Utilisation sur système Linux et Windows offline,
    - Intégration des utilitaires dédiés à l'acquisition de données :
      - Utilitaires binaires statiques a2imp-linux,
      - Utilitaires binaires statiques a2imp-windows.
    - Modification des scripts de démarrage :
      - Eviter l'altération de l'espace de stockage.

Boîtes à Outils – Outils

- ***Tct (The Coroner's Toolkit): www.porcupine.org/forensics/tct.html***
  - Collection d'outils d'analyse de systèmes de fichiers.
- ***Sleuthkit : www.sleuthkit.org/sleuthkit/desc.php***
  - Ensemble d'outils permettant d'analyser différents types de systèmes de fichiers (NTFS, FAT, UFS1, UFS2, EXT2, EXT3, ISO9660),
  - reconnaît différents types de partitions (DOS, BSD, MAC, SUN),
  - Plate-formes : Linux, Mac OSX, Open&FreeBSD, Solaris, CYGWIN.
- ***Autopsy : www.sleuthkit.org/autopsy/desc.php***
  - Interface graphique (html) à la boite à outils Sleuthkit.
- ***Scalpel, foremost :foremost.sourceforge.net & digitalforensicssolutions.com/Scalpel***
  - détection / récupération de fichiers sur images disques.

TP – Organisation

- ***Contexte :***
  - Un client / un serveur
  - IP Serveur : 10.2.2.2 & IP Client (DHCP)
  - Ports : 10100 à 10409 de 10 en 10 sur serveur
  - Users : user10 à user40
  - Password : !a2imp
  - Commandes nc et md5sum copiées dans le répertoire utilisateur
  - Pour le boot du LiveCD : user root, no passwd

TP – Méthodologie Windows

- ***Etape 1 : Horodatage***
- ***Etape 2 : Création main courante***
- ***Etape 3 : Actions à chaud***
  - Montage du CDROM
  - Copie de la RAM vers le serveur via nc
  - Exécution du script d'analyse du système (a2imp-win.bat)
- ***Etape 4 : Actions à froid***
  - Boot sur CDROM + commande script
  - Copie DD (clé USB) vers le serveur via nc

TP – Méthodologie Linux

- ***Etape 1 : Horodatage***
- ***Etape 2 : Création main courante***
- ***Etape 3 : Lancement commande script dans FIFO***
- ***Etape 4 : Actions à chaud***
  - Montage du CDROM
  - Copie de la RAM vers le serveur via nc
  - Exécution du script d'analyse du système (a2imp-auto.sh)
- ***Etape 5 : Actions à froid***
  - Boot sur CDROM + commande script
  - Copie SWAP vers le serveur via nc
  - Copie DD (clé USB) vers le serveur via nc

TP – Particularités Windows

- Pas de commande « script »,
- Manipulation difficile à réaliser pour le dump de la RAM, qu'il faut anticiper sur toutes les machines dès le départ,
- Dumper l'ensemble du disque dur.

TP – Particularités Linux

- Utilisation de la commande « script » pour tracer l'ensemble des commandes,
- Difficultés d'accéder à la RAM avec certains noyaux,
- Attention à relancer le FIFO script lors du reboot.

TP – Conclusion

- A vous de jouer…

TP – Organisation

- ***Contexte :***
  - Un client / un serveur
  - IP Serveur : 10.2.2.2 & IP Client (DHCP)
  - Ports : 10100 à 10409 de 10 en 10 sur serveur
  - Users : user10 à user40
  - Password : !a2imp
  - Commandes nc et md5sum copiées dans le répertoire utilisateur
  - Pour le boot du LiveCD : user root, pwd root