Formation A2IMP

Systèmes Linux

Capitoul

Cédric Hillembrand (CESR)– mars 2009

D’après les diapositives de F.Bongat (DR5)

Systèmes Linux - Plan

- Comment gérer un incident ?
- La chaîne de confiance
- Un peu d'aide extérieure
- Procédure :
  - Horodatage et main courante,
  - Montage de la boîte à outils,
  - Sauvegarde des différents types de données,
  - Sauvegarde des données par réseau
  - Somme de contrôle,
  - Enregistrement continu des informations saisies,
  - Collecte d'informations (commandes),
  - Récupération des données.
- Conclusion

Systèmes Linux – Gestion Incident

- ***Aspects organisationnels et objectifs :***
  - Effectuer une analyse réfléchie et minutieuse,
  - Récupérer un maximum d'informations,
  - Préserver ces informations,
  - Reconstruire la succession d'évènements.
  - ➢ Il est important d'avoir :
    - Un plan ou une procédure,
    - Des outils d'analyse,
    - Des connaissances dans les systèmes à explorer.

Systèmes Linux – Gestion Incident

- ***Méthodologie :***
  - Filtrer le trafic via les équipements réseaux ou firewalls externes,
  - Se référer au trafic réseau (logs routeur / firewall, snort, ntop) pour obtenir des informations,
  - Préparer un organe externe chargé de collecter les informations
    - périphérique USB,
    - connexion privilégiée avec un serveur sain.
  - Analyser avec précaution le système « online » munis des bons outils.

Systèmes Linux – Chaîne de confiance

- Quelle est-elle ?
  - le shell (inclus les variables d'environnement),
  - les commandes,
  - les bibliothèques dynamiques,
  - les drivers des périphériques,
  - le noyau.
- Quelle confiance peut-on avoir dans les données du système ?
- Que se passe t'il lorsque l'on exécute un binaire ?
- On veut essayer de faire le moins de modifications sur le système en cours d'analyse.

Systèmes Linux – Aide extérieure

- ***Grâce à une boîte à outils compilée en statique :***
  - Pour savoir si un binaire est monté en statique :

```
[root@pc-3 a2impUnix]# ldd /bin/ps                                    Local
        linux-gate.so.1 =>  (0x00235000)
        libproc-3.2.7.so => /lib/libproc-3.2.7.so (0x00376000)
        libdl.so.2 => /lib/libdl.so.2 (0x00532000)
        libc.so.6 => /lib/libc.so.6 (0x00868000)
        /lib/ld-linux.so.2 (0x00e46000)
[root@pc-3 a2impUnix]#
[root@pc-3 a2impUnix]#
[root@pc-3 a2impUnix]# ldd /mnt/cdrom/a2impUnix/ps                    CDROM
        not a dynamic executable
```

  - Toujours lancer les commandes avec ‘./’ :
    - Exemple : *./ps -eaf*

Systèmes Linux – Procédure

- ***Déroulement :***
  - Comparaison de la date,
  - Création d'une main courante (manuelle ou automatique),
  - Montage de la boite à outils (CD),
  - Sauvegarde des mémoires, et des disques,
  - Calcul des sommes de contrôle,
  - Collecte d'informations sur le système.

Systèmes Linux – Procédure

- ***Date et main courante :***
  - Vérification de la date et de l'heure sur le système compromis :
    - Utiliser la commande *date* (Boite à Outils),
    - Comparer l'heure à une source sûre.
  - Création de la main courante :
    - Avec un stylo et du papier…
    - Via l'édition d'un fichier sur un système sûr :
      - Noter chaque action réalisée, ainsi que l'heure à laquelle elle a été lancée,
      - Le résultat des différentes commandes peut être stocké à part.

Systèmes Linux - Procédure

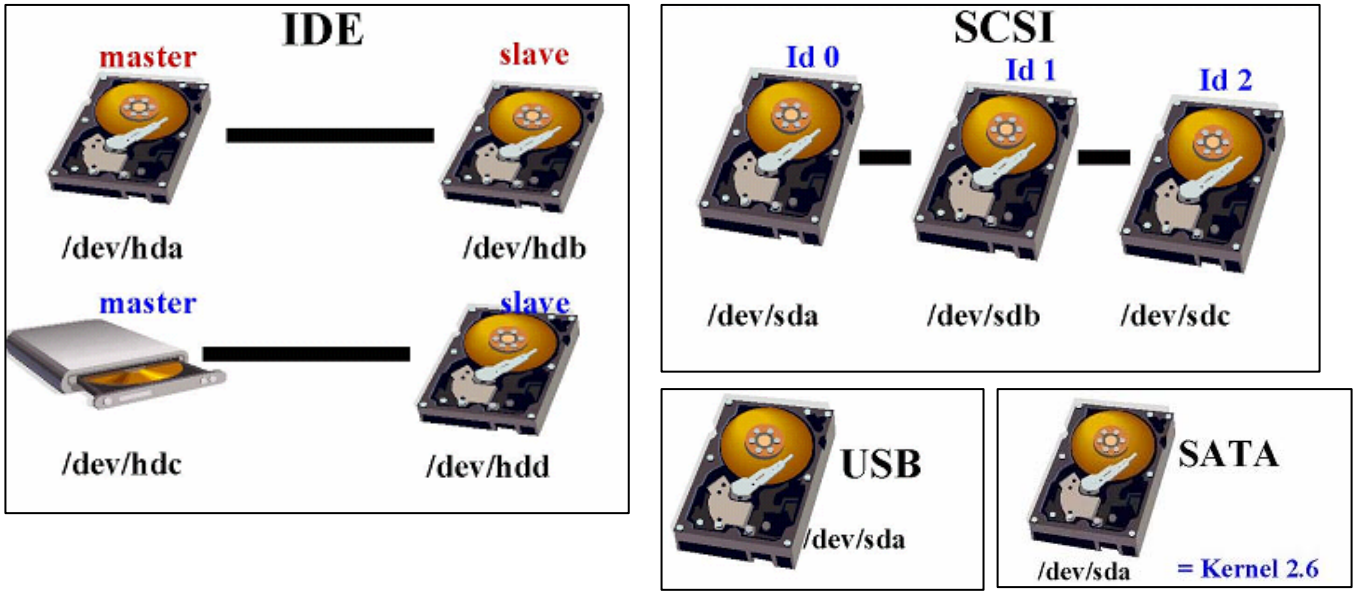
- ***Montage de la boîte à outils (CDROM) :***
  - *mount /dev/cdrom /mnt/cdrom*
  - A partir de maintenant, toutes les commandes que l'on tapera sur la machine compromise seront celles réputées sûres car exécutées depuis le CDROM.
  - Rappel : ne pas oublier de spécifier le chemin d'accès aux commandes :
    - */mnt/cdrom/ls –altF /etc*
    - *cd /mnt/cdrom; ./ls –altF /etc*

Systèmes Linux - Procédure

- ***Sauvegarde des mémoires :***
  - Sauvegarde de la mémoire :
    - */mnt/cdrom/dd if=/dev/mem of=file-ram.dd*
    - */mnt/cdrom/dd if=/proc/kcore of=file-ram.dd*
  - Sauvegarde de la swap :
    - Recherche de la swap :
      - */mnt/cdrom/cat /proc/swaps => on en déduit le /dev/XdY*
    - Copie de la swap :
      - */mnt/cdrom/dd if=/dev/XdY of=file-swap.dd*

Systèmes Linux - Procédure

- ***Sauvegarde des disques :***
  - Nommage des périphériques :



Systèmes Linux - Procédure

- ***Sauvegarde des disques :***
  - Déterminer la structure d'un disque **:**
    - */mnt/cdrom/fdisk –l /dev/XdY > fdisk.disk1*
  - Sauvegarder les disques ou les partitions **:**
    - Copie de disque à disque :
      - */mnt/cdrom/dd if=/dev/XdY of=/dev/XdZ*
    - Copie de disque vers un fichier :
      - */mnt/cdrom/dd if=/dev/XdY of=file-devXdY.dd*
    - Découpage des partitions en fichiers de tailles finies :
      - */mnt/cdrom/dd if=/dev/hda1 | /mnt/cdrom/split –d –b 2000m – image.split*

Systèmes Linux - Procédure

- ***Sauvegarde des disques, remarques :***
  - Cas lors d'erreurs dans la copie
    - A cause de blocs défectueux, la copie peut s'arrêter dès qu'elle rencontre un problème :
      - option *conv=noerror*
    - Le système de fichiers fonctionne par adressage. Par défaut, *dd* ne remplace pas les blocs défectueux :
      - D'où un décalage des adresses lors de la reconstruction du système de fichiers et des fichiers incohérents,
      - option *conv=sync* (remplace les blocs défectueux par des octets nuls, ce qui conserve l'adressage).
    - *./mnt/cdrom/dd if=/dev/XdY conv=noerror,sync of=file.dd*

Systèmes Linux - Procédure

- ***Sauvegarde par réseau pour export données :***
  - Utiliser *netcat* comme outil (simple et puissant, il est le plus utilisé par les hackers !!). Ouverture d'un socket sur le serveur sain :
    - *nc –l –p 5555 > /usr/local/save/image.dd*
  - Sauvegarde depuis le client compromis vers le serveur sain *:*
    - */mnt/cdrom/dd if=/dev/XdY | /mnt/cdrom/nc server 5555*
  - S'assurer qu'aucun filtre de paquets (iptables, ipchains, pf, ipfilter...) ne bloque le flux.

Systèmes Linux - Procédure

- ***Création de la somme de contrôle :***
  - Vérification de l'intégrité des données transférées :

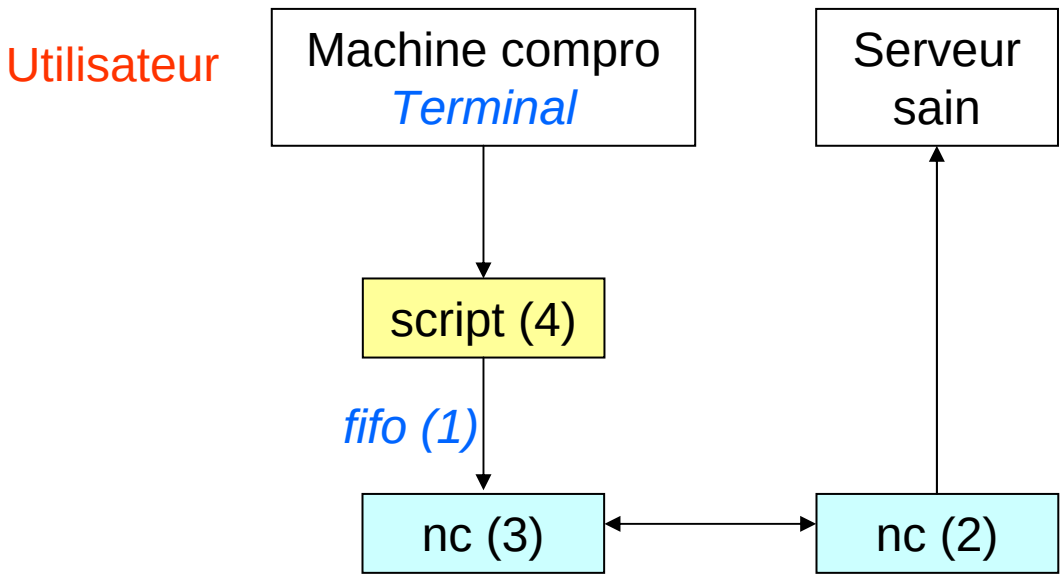
    /mnt/cdrom/md5sum file-devXdY.dd > file-devXdY.dd.md5
  - A faire sur le serveur et la machine compromise pour comparaison.

Systèmes Linux - Procédure

- ***Enregistrement continu des commandes :***
  - On veut avoir un minimum d'impact sur les informations volatiles,
  - On doit garder une trace des actions réalisées pour pouvoir ensuite expliquer les éventuelles modifications systèmes,
  - On redirige les commandes passées vers un serveur sain.

Systèmes Linux - Procédure

- ***Enregistrement continu des commandes :***
  - Méthode :
    - Création d'un *fifo*, d'une communication réseau via *nc*, utilisation de la commande *script*.



Systèmes Linux - Procédure

- ***Enregistrement continu des commandes :***
  - Création du fifo :
    - */mnt/cdrom/mkfifo /tmp/session-client*
  - On prépare l'envoi à distance via la commande «nc» de tout ce qui sera envoyé dans le fifo :
    - */mnt/cdrom/cat /tmp/session-client* | */mnt/cdrom/nc server 5555*
  - Depuis un autre terminal, on lance la commande «script» qui enregistre tout ce qui est lancé et tous les résultats dans le fifo précédemment créé :
    - */mnt/cdrom/script -f /tmp/session-client*
  - Maintenant, tout ce qui est saisi et affiché dans ce terminal est envoyé vers le serveur sain.

Systèmes Linux - Procédure

- ***Collecte d'informations :***

  Liste des commandes pouvant être utilisées pour analyser la partie ***réseau*** :

  - arp –a : liste des entrées de la table arp
  - netstat –s : statistiques des protocoles (IP,TCP,UDP,ICMP…)
  - netstat –nr : affichage des tables de routage
  - netstat –nap : liste des connexions réseau actives
  - ifconfig –a : configuration des interfaces réseau
  - lsof –i –n –i4(6) : connexions réseau et fichiers ouverts Ipv4(6)
  - sysctl –a : configurations des paramètres du noyau à chaud
  - ifpromisc : vérification mode PROMISCUS sur interface eth (chkrootkit)

Systèmes Linux - Procédure

- ***Collecte d'informations :***

  Liste des commandes pouvant être utilisées pour analyser la partie ***système*** :

  - ps –eaf : ensemble des processus en mémoire
  - uptime : charge de la machine, temps de vie, nombre d'utilisateurs connectés
  - who, w, last : utilisateurs sur le système
  - ldd : analyse des dépendances entre librairies partagées
  - strace : affiche chaque appel système réalisé par un programme
  - stat : informations et statistiques sur un fichier
  - ls –alituR : listing complet des fichiers

Systèmes Linux - Procédure

- ***Collecte d'informations :***
  - du : calcul de la taille d'un répertoire
  - df : calcul des quantités d'espace disque occupées
  - chkproc : vérification des processus cachés dans ps (chkrootkit)
  - lsof -nPl : liste de tous les processus, des librairies et des fichiers ouverts
  - lsmod : liste des modules chargé par le noyau en mémoire
  - uname –a : version du noyau
  - rpm –qa : liste des paquetages installés
  - printenv : liste des variables d'environnement

Systèmes Linux - Procédure

- ***Récupération des données :***
  - Montage des images sur le système sain :
    - *mount –t proc –o loop,ro file_mem.dd /mnt/mem (mémoire)*
    - *mount –t swap –o loop,ro file_swap.dd /mnt/swap*
    - *mount –t ext3 –o loop,ro image_disk1.dd /mnt/disk1*

Systèmes Linux - Conclusion

- Bien connaître l'environnement de ses serveurs (HDD, Swap, commandes),
- Avoir une machine serveur saine prête,
- Tester la boîte à outils avant pour se familiariser et valider son fonctionnement,
- Penser à horodater, « scripter », et à lancer les commandes depuis le CDROM,
- Et rester calme !!

Questions ?