A2IMP - Acquisition de données

Boris Valera
(boris.valera@insa-toulouse.fr)
d'après Christophe Dubois

31 mars 2009

Principe de base

- Face à un système piraté, il faut :
  - une méthodologie afin de faire face au problème de manière calme et réfléchie
  - une boîte à outils permettant l'acquisition des données système intéressantes pour l'analyse
  - un support pour stocker les données récoltées

Principe de base

- Un système compromis implique :
  - ne pas faire de modifications sur le système à analyser
  - ne pas faire confiance aux outils installés sur ce système
  - récupérer les traces récoltées par les équipements en bordure de la machine (logs du routeur, firewall, système de métrologie)
  - vérifier que les données sauvegardées sont identiques à la source et ne pourront être altérées

Objectif

- Conserver des traces les plus complètes possibles en vue d'une analyse.

  Traces ce qui est visible et invisible

Objectif de l'analyse

- Le but de l'analyse est de répondre aux 4 questions :
  - Qui ?
  - Quand ?
  - Comment ?
  - Pourquoi ?

Analyse : répondre aux questions

- Qui ?
  - La réponse à cette question intéresse typiquement les services de police
    - Cas particulier : malveillance interne
  - En général, la réponse se trouve dans les journaux

Analyse : répondre aux questions

- Quand ?
  - La réponse à cette question intéresse également les services de police
    - qui + quand = identification possible
  - Parfois utile pour comprendre quelle vulnérabilité a été utilisée
  - En général, la réponse se trouve dans les journaux et sur les dates des fichiers

Analyse : répondre aux questions

- Comment ?
  - La réponse à cette question intéresse les CSIRT (CERT-RENATER et CERTA) et la victime
    - Conséquences sur l'administration de la machine
  - En général, la réponse se trouve dans les journaux

Analyse : répondre aux questions

- Pourquoi ?
  - La réponse à cette question intéresse les CSIRT (CERT-RENATER et CERTA) et la victime
    - Permet parfois de découvrir des faiblesses sur le réseau
    - Permet, dans certains cas, de comprendre comment a eu lieu l'intrusion
  - En général, pour répondre à cette question il est nécessaire d'analyser tout le disque

Temps de l'analyse

- Répondre aux questions qui, quand et comment est rapide (quelques heures voire quelques minutes)
- Répondre à la question pourquoi peut prendre plusieurs jours voire plusieurs semaines
- L'analyse d'un incident permet parfois de mettre en évidence d'autres attaques éventuellement réussies

La méthode à employer

Elle dépend

- Du système d'exploitation
- De l'état du système
  - à froid : on arrête le système ou le sysème a été arrêté
    - On perd les informations volatiles
  - à chaud : la machine continue de fonctionner
    - On cherche à conserver les informations volatiles
- Du support de sauvegarde disponible

Ce que l'expert attend

- Tout élément qui permettrait de répondre aux 4 questions
- Dans l'ordre d'importance (du point de vue du CERTA)
  - Copie du disque dur (signée pour éviter toute contestation)
  - Journaux du réseau
  - Main courante
  - Copie du swap
  - Informations volatiles

Préparation

- Gérer les priorités :
  - identifier les services impactés
  - informer sa hierarchie
  - informer les utilisateurs
- Se munir de documentation
- Avoir la boîte à outils
- Avoir un espace de stockage suffisant :
  - disque dur, bande magnétique
  - une machine ou un serveur pour faire la copie via le réseau

Méthodologie

- Créer une main courante
- Analyse des processus et du système
- Récupération des informations volatiles (RAM, liste des processus, connexions, environnement)
- Isoler la machine du réseau ou la stopper proprement
  - Connecter la machine à une autre sur un switch dédié
  - Démarrer sur un support externe (LiveCD A2IMP) sans toucher au disque dur et sauvegarder les partitions (SWAP et données)
- Signer les informations sauvegardées

Noter le temps

- Penser à préciser le décalage entre l'heure du système et l'horloge parlante
- Dans l'idéal, tous les systèmes sont synchronisés via NTP avant l'incident

Main courante (1)

- Noter toutes les opérations effectuées et les communications échangées
  - particulèrement utile en cas de dépôt de plainte $\longrightarrow$ la police demande la meilleure précision possible lors de l'audition
  - les incidents engendrent souvent des situations de stress $\longrightarrow$ tendance à l'oubli de ce que l'on fait
  - permet, dans certains cas, lors de l'analyse, de distinguer les actions du pirate des actions de l'administration

Main courante (2)

- Horodater chacune des opérations effectuées en se synchronisant avec l'horloge parlante (3699)
- En croisant les dates de la main courante avec celles du système, on arrive parfois à horodater les actions de l'intrus (encadrement des actions dans un intervalle de temps)
- Inclure des éléments de contexte dans la main courante, comme les messages électroniques relatifs à l'incident (ex : message du CERT-RENATER) et retranscrire les éléments les plus pertinents des conversations téléphoniques

Copie Physique ou logique ?

- Problème des copies logiques :
  - ne copie pas le "slackspace" (fin de fichiers)
  - ne copie pas les blocs de données non utilisés (fichiers effacés)
  - souvent réalisé sur le disque compromis $\rightarrow$ écrase des traces
- Nécessité absolue de faire des copies physiques !

Sauvegarde du SWAP

- Le swap est soit un fichier sur le disque (pagefile.sys) soit une partition
- Contient énormément d'informations, mais celles-ci son non datées et non classées
- Pas d'outils permettant une analyse efficace du swap → utilisation de *strings* et de *grep* en général
- Il est fréquent de retrouver l'adresse IP d'un intrus (lors d'une compilation par exemple)

→ intéressant mais pas facilement exploitable

Mémoire volatile

- Instantané de la mémoire
- Pas forcément représentatif de l'activité récente de la machine
- Pas le plus important, mais peu coûteux à récupérer (sur les machines Unix)

Arrêt de la machine

Deux écoles

- Arracher le câble d'alimentation
  - risque de mettre le système dans un état instable
  - risque d'endommager le disque physiquement
- Arrêter proprement la machine avec les commandes système
  - risque que ces commandes aient été sabotées, mais le risque est peu probable

Au CERTA, préférence pour l'arrêt propre du système

Faire une signature numérique

- La signature permet de vérifier l'état de la copie et d'éviter certaines contestations
- De nombreux outils natifs pour le faire : md5sum, sha1sum, etc
- Signature de l'original stocké dans un fichier puis on vérifie la copie
- Exemple :
  - `md5sum /dev/hda1 > /mnt/disk/hda1.md5sum`
  - `md5sum /mnt/dis/hda1.dd`
- Si le résultat est différent, la copie est ratée
- Si on n'arrive pas à obtenir une copie identique ou que l'on utilise `conv=noerror,sync`, il est important de le préciser dans la main courante
- Inutile d'essayer de signer une copie faite à chaud → impossible de vérifier si la copie a réussi

Objectifs de la sauvegarde

- Sauver les données afin d'établir une continuité de service : une archive suffit
- Récupérer des données en vue d'une analyse : image faite bloc par bloc pour conserver les données effacées

Dans chaque cas, il faut essayer d'éviter une altération des données du système

Utilisation d'un LiveCD

- Permet de démarrer dans un mode sain pour différents systèmes d'exploitation
- N'importe quelle distribution, nécessite de prendre en compte le support de sauvegarde et la commande *dd* et *md5sum*
- Inconvénients :
  - n'est pas vraiment universel, il dépend de l'architecture matérielle
  - doit correspondre au besoin
  - Dans le cas d'une compromission, il doit être équipé d'une boîte à outils pour l'analyse

Quelques LiveCD

- Operator
  - `http://www.ussysadmin.com/operator/`
  - complet
  - binaires Linux et Windows
- INSERT
  - `http://www.inside-security.de/insert_en.html`
  - anti-virus
  - orienté récupération de données
- Knoppix std
  - `http://s-t-d.org/`
  - assez complet
  - maintenu
- LiveCD A2IMP
  - outils pour Windows et Linux

Outils pour la copie

- De nombreux outils permettent de faire des copies de disque, mais certains créent des images propriétaires (ex : Encase) qui nécessite le même outil pour relire l'image → risque de ne pas pouvoir exploiter l'image
- Un bon outil gratuit et natif sur les LiveCDs et les systèmes Unix : *dd*
- Variante de dd : *dcfldd*

Support de sauvegarde

- On va faire l'acquisition des données en fonction du support disponible et de la quantité des données $\rightarrow$ bien calibrer le support
- Déterminer la possibilité de connecter le support au système compromis
- Utilisation du réseau si possible afin de transférer l'image sur une autre machine

Intérêt du disque dur

- Reconnu facilement quelque soient les systèmes
- Bon rapport qualité/prix au niveau espace de stockage (surtout IDE et SATA)
- Connectique "universelle" et adaptateur nombreux
  - IDE ou SATA en interne
  - SCSI (nécessite une carte)
  - USB ou FireWire : le moyen le plus simple

Les autres supports

- Sur clé USB
  - problème de taille
  - problème de fiabilité
- Sur bande
  - demande un lecteur spécifique $\longrightarrow$ peut poser un problème pour le tiers en charge de l'analyse

Questions ?