



Forensics sous Windows

Date: 07/09/2007

Cet exemple d'analyse forensique est typiquement un cas d'étude que vous pouvez retrouver au cours de la formation "FORENSICS SOUS WINDOWS" que nous proposons. Cette formation d'une durée de quatre jours est assurée par un expert en sécurité informatique présentant une forte expérience dans le domaine du forensics. On y apprend entre autres les techniques permettant d'acquérir et d'analyser les données tout en cernant les informations potentiellement intéressantes à chercher et où les chercher. Retrouvez les détails de cette formation sur notre site (<http://www.lexfo.fr>) ou bien contactez nous à tout moment en envoyant un mail à l'adresse formations@lexfo.fr si vous souhaitez de plus amples renseignements.

Introduction aux techniques forensics

Le terme anglais Forensics [1] désigne les recherches effectuées sur une machine suite à sa compromission par exemple, afin d'en déterminer les causes et de juger de l'étendue des dommages. Une définition plus formelle pourrait être : l'action d'acquérir, de recouvrer, de préserver, et de présenter des informations traitées par le système d'information et stockées sur des supports informatiques.

Ces investigations suivent généralement 3 grandes étapes :

1) l'acquisition de données

Cette étape consiste à récupérer les données d'une machine dans le but de les analyser. Il faut évidemment éviter toute modification du système et des informations elles-mêmes. L'approche sera différente suivant que le système est en cours d'exécution ou arrêté. Trois types de collecte peuvent alors être détaillés, à savoir le "dead" forensics (analyse de disque), le "live" forensics (analyse du système opérationnel) et le "mixed" forensics (collecte et analyse de la mémoire physique).

2) le recouvrement de données

Un fichier effacé sur un disque dur l'est rarement de façon sécurisée. Les informations concernant ce fichier y restent souvent physiquement. Il est donc généralement possible de recouvrer ces fichiers à partir de l'image d'un disque dur. On emploiera par exemple la technique dite "file carving" [2] qui consiste à faire une recherche sur l'image disque par rapport au type des fichiers.

3) l'analyse de données

Une fois les données récupérées, il faut les analyser ; la facilité de l'analyse est étroitement liée aux compétences du pirate. Certains ne tenteront pas de se dissimuler, laissant des traces voyantes un peu partout sur le système (dans les journaux systèmes, les fichiers de traces applicatives, etc ...). D'autres auront pris soin d'effacer un maximum d'éléments pouvant trahir leur présence ou leur identité jusqu'à ne rien écrire sur le disque (intrusion par Meterpreter par exemple [3]).

Exemple d'analyse sous Windows

La récupération des journaux d'évènements (ou event logs) sur un système Windows est un exemple concret d'analyse forensique. Ces journaux peuvent par exemple avoir été supprimés par une personne s'étant introduite sur votre système afin d'effacer ses traces. Dans ce cas précis, la connaissance du format des journaux d'évènements est nécessaire pour mener à bien l'analyse.

Le format des event logs (différent sur Windows Vista)

Il est possible sur un système Windows de visualiser les event logs grâce à l'application Event Viewer. Cette application regroupe en fait plusieurs sources d'informations:

1) l'event log record enregistré dans un fichier .evt (AppEvent.evt pour le journal des applications, SecEvent.evt pour la sécurité et SysEvent.evt pour le système) présent dans le répertoire C:\windows\system32\config.

L'event log record a le format suivant :

```
typedef struct _EVENTLOGRECORD {
    DWORD Length;
    DWORD Reserved;
    DWORD RecordNumber;
    DWORD TimeGenerated;
    DWORD TimeWritten;
    DWORD EventID;
    WORD EventType;
    WORD NumStrings;
    WORD EventCategory;
    WORD ReservedFlags;
    DWORD ClosingRecordNumber;
    DWORD StringOffset;
    DWORD UserSidLength;
    DWORD UserSidOffset;
    DWORD DataLength;
    DWORD DataOffset;
}EVENTLOGRECORD
```

La description de chaque champ est donnée sur le site de Microsoft [4]. Le champ Reserved reste cependant très important et va servir à la reconstruction des event logs. Il a toujours pour valeur ELF_LOG_SIGNATURE (0x654c664c), soit en ascii "eLfl". Il est aussi appelé magic number. Le champ Length quant à lui va servir à connaître la taille exacte de l'event record de manière à ne pas récupérer plusieurs event record à la fois.

2) les clés de registre

```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Eventlog\
```

Elles fournissent comme informations les fichiers (des fichiers .dll) contenant les messages associés aux event records.

3) les message files en question

Le message affiché va dépendre de l'event id. Certains messages contiennent des variables. Les valeurs sont présentes à la suite de la structure EVENTLOGRECORD définies comme telles :

```
WCHAR SourceName[]
WCHAR Computername[]
SID UserSid
WCHAR Strings[]
BYTE Data[]
CHAR Pad[]
DWORD Length
```

Plus de détails sur ces valeurs peuvent également être trouvés sur le site de Microsoft [5].

L'acquisition des données

C'est la première étape de notre analyse forensique. Elle consiste à récupérer le contenu du disque dur du système à analyser. Pour éviter toute modification des données de ce dernier, nous choisirons d'agir le système éteint et de faire une copie intégrale (bits à bits) du contenu du disque dur à l'aide de l'outil dd [6] que l'on ne présente plus.

Le recouvrement des données

Muni d'une image du disque, la seconde étape de l'analyse consiste à récupérer les événements effacés. En fait, lorsque les événements d'un journal sont nettoyés via l'application Event Viewer, le fichier .evt correspondant est vidé. Mais comme n'importe quelles données effacées sur un disque, les données des journaux sont toujours en partie présentes sur le disque dur. La procédure est alors simple. Elle consiste à rechercher à partir de notre image toutes les occurrences de la chaîne de caractères "LfLe". La taille de l'event log record étant présente à "(offset de "LfLe") - 4", il est alors facile de reconstruire l'évènement à chaque occurrence de la chaîne "LfLe" trouvée.

L'analyse des données

La dernière étape de notre analyse. A ce stade, nous avons pu récupérer tous les événements potentiellement présents sur le disque dur. Pour connaître ensuite la signification exacte de chaque événement (pour représenter à peu de choses prêtes les informations fournies par l'Event Viewer), il suffit par exemple d'interroger le site Eventid [7] muni de l'event id et de la source de l'évènement.

Références

- [1] <http://en.wikipedia.org/wiki/Forensic>
- [2] <http://www.forensicswiki.org/wiki/Carving>
- [3] <http://www.metasploit.com/projects/Framework/docs/meterpreter.pdf>
- [4] <http://msdn2.microsoft.com/en-us/library/aa363646.aspx>
- [5] <http://msdn2.microsoft.com/en-us/library/aa363646.aspx>
- [6] <http://www.gmgsystemsinc.com/fau/>
- [7] <http://www.eventid.net>