

Dans le cadre de

SECURIDAY 2010

Et sous le thème de

Computer Forensics Investigation



VOUS PRÉSENTE L'ATELIER :

Analyse des fichiers LOG

Chef Atelier : **Tarek LABIDI (RT3)**

- **Mongia BEN HAMMOUDA (RT5)**
- **Mariem MABROUK (RT3)**
- **Mariem BEN FADHL (RT4)**



1. Computer Forensics :

Une discipline émergente de la collection et de l'analyse de l'information concernant les ordinateurs et les réseaux d'ordinateurs pour détecter les activités suspectes ou malicieuses en vue de l'utiliser comme des preuves dans la cour de la loi. C'est l'art de découvrir et d'extraire l'information prouvant l'occurrence d'un crime informatique de telle façon à le rendre admissible dans le tribunal .

Computer Forensics est une nouvelle science qui est apparue comme une réaction au crime informatique. Elle permet d'appliquer la loi à l'informatique, en employant les techniques d'investigation pour identifier la cause origine d'un crime informatique.

Un crime informatique peut être une attaque, une intrusion ou toute activité malicieuse.

2. L'importance des fichiers logs: Composant vital pour Forensics

Les fichiers logs tracent tous les événements qui arrivent pendant l'activité d'un système. Ils peuvent contenir la preuve en détail de toute activité exceptionnelle, suspecte ou non désirée. Les fichiers logs issus des différents composants d'un réseau peuvent indiquer si la sécurité du réseau est compromise ou en voie de compromission. Ils sont la seule information que l'attaquant laisse derrière lui après son introduction dans un réseau, ils représentent l'empreinte de l'attaquant. Lors d'une attaque, l'information contenue dans les fichiers logs peut être vérifiée pour définir les traces de l'attaque et aboutir à une preuve accusatrice.

=>donc le but de cet atelier est de mieux structurer les fichiers logs et les centraliser afin de faciliter le processus d'investigation tout en analysant les différents composants de sécurité d'un réseau.

3. Présentation de l'atelier et de l'outil :

L'acquisition et l'analyse des données à Partir du réseau permettent:

- De savoir comment l'intrus a pénétré dans le réseau
- De montrer le chemin suivi par l'intrus
- De révéler les techniques d'intrusion
- La collecte des traces et des preuves



Sous UNIX il existe plusieurs outils. Le plus fameux est Syslog qui représente Un service de journalisation se reposant sur les deux démons « syslogd » et « klogd ».

3.1 Syslogd :

Le démon syslogd existe par défaut sous UNIX. Mais ces fonctionnalités sont néanmoins limitées. Lors de son lancement, « syslogd » lit le fichier « /etc/syslog.conf » afin de pouvoir ensuite décider le milieu d'enregistrement de chaque message. Il représente plusieurs inconvénients :

- > Utilisation de protocole UDP.
- > Fonctions de filtrage très simplifiées.
- > Si le système est indisponible, les messages réacheminés par les clients seront perdus.
- > Consommateur de CPU.

Afin de résoudre ces difficultés on a recours à Syslog-ng qui offre plus de qualités.

3.2 Syslog-ng :

C'est le système standard de journalisation de nouvelle génération disponible au format source et binaire, il est libre. Son principal avantage est sa grande flexibilité et sa simplicité dans sa configuration. En effet il permet :

- > Filtrage des messages par leur contenu et selon plusieurs critères (contenu, gravité...)
- > Transport des journaux via le protocole TCP et UDP
- > Une large portabilité
- > Sécurité du transport des données par le cryptage
- > Synchronisation des horloges avec un client NTP
- > Compatible IPV6

SECURINETS



Club de la sécurité informatique

INSAT

Voici un tableau comparatif qui montre la différence entre syslogd et syslog-ng :

Syslog-ng	Syslogd
permet de séparer les sources d'événement réseaux et les segmenter en plusieurs fichiers, chacun correspondant à une source bien précise	stocke l'intégralité des journaux dans le même fichier sans distinction.
Utilise le protocole TCP en plus que l'UDP	Utilise seulement le protocole UDP

-> L'export des logs reçu vers un serveur mySQL

-> L'utilisation de macros (instruction) possible pour le nom des logs

Remarque :

Le format d'un message syslog est édité comme l'exemple suivant:

```
Jan 19 14:09:09 hostname dhcp service [warning] 110 corps_message
```

Il comprend alors:

- la date et l'heure
- le hostname
- une information sur le processus
- le niveau de sévérité du log
- un corps de message.

->Les niveaux de priorité : indiquent l'urgence du message.

Exemple: erreur, warning...

SECURINETS



Club de la sécurité informatique

Priorités :	signification :
emerg (emergency)	Message urgent. Le système est inutilisable ou risque de le devenir à très court terme.
alert (alerte)	Message alertant l'administrateur système qu'une action de sa part est requise.
crit (critique)	Message critique.
err (erreur)	Message d'erreur.
Warning(ou warn) (avertissement)	Message d'avertissement.
notice (note)	Message de fonctionnement normal, sans gravité particulière.
nfo (Information)	Message à titre informatif.
debug (debogage)	Message de débogage

->Les "facility" : Ce sont les applications ou les composants du système pouvant générer un message.

Exemple: Kernel, cron, syslog...

Facility :	signification :
auth, authpriv, security	authentification et sécurité
cron	service cron (exécution périodique de commandes)
daemon	processus démons, càd qui tournent en arrière-plan
ftp	service ftp
kern	pour kernel (noyau)
mail	service email
syslog	service syslogd
user	processus lancés par les utilisateurs, excepté root
local0 local7	à messages du noyau, en fonction de leur niveau



3.4 EventLog :

C'est un outil pour le balayage, stockage, et manipulation des événements sur une machine dans un LAN. Il stocke les événements de toutes les machines sur une base de données puissante, où on peut récupérer tous les détails tels que l'identification d'événement, type, catégorie, source, SID des utilisateurs, suivi de message et de date d'événement.

Windows a 3 types de logs, un serveur en a plus :

Types de log :	Description :	Emplacement :
Log Application :	les événements rapportés par les différentes applications installées sur votre PC. Celles peuvent être des applications non Microsoft.	%SystemRoot%\System32\Config\AppEvent.evt
Log sécurité :	qui contient les événements audités ainsi que ceux concernant la sécurité.	%SystemRoot%\System32\Config\SecEvent.evt
Log système :	les événements rapportés par les composants système (processes, kernel, drivers...)	%SystemRoot%\System32\Config\SysEvent.evt

Chaque log peut contenir 5 types d'événements :

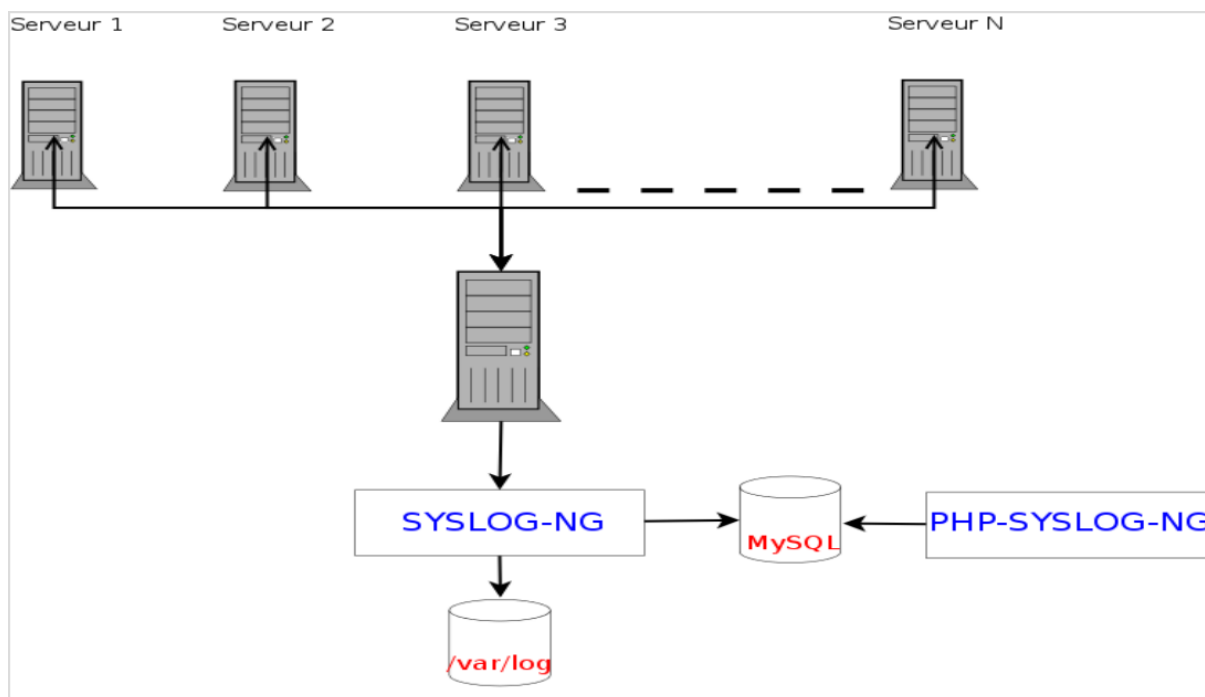
Type :	Description :
Information	Cet événement indique, par exemple, qu'une application, un driver, ou un service a démarré correctement. Un événement de type information sera écrit dans le log.
Erreur	Cet événement indique un problème, une perte de fonctionnalité ou une erreur pendant le démarrage. Par exemple, si un service ne démarre pas au démarrage, un événement de type erreur sera écrit dans le log.
Avertissement	Cet événement non nécessairement significatif, peut indiquer un futur problème. Par exemple, si l'espace disque devient trop restreint, un message d'avertissement apparaîtra dans le log.



Audit Succès	des	Ce type d'événement apparaît dans le log Sécurité lors d'un login par exemple.
Audit Echecs	des	Ce type d'événement apparaît dans le log Sécurité lors d'un login par exemple, si un mot de passe erroné a été entré.

4. Environnement logiciel :

Pour assurer le bon fonctionnement de syslog-ng on a recours à plusieurs outils :



4.1 Syslog-ng :

Disponible sur la plupart des distributions sous forme de paquet (Debian, Red Hat, Mandriva ...).

En téléchargement (format tar.gz) sur SOURCEFORGE (<http://sourceforge.net/projects/php-syslogng/>) ou chez BALABIT (<http://www.balabit.com/downloads/files/syslog-ng/sources/stable/>)



4.2 Apache2 :

Configurer apache afin de créer un site virtuel ou pour avoir accès à <http://localhost/php-syslog-ng/>. En effet il permet de créer une interface web.

4.3 Php :

Ça nécessite d'installer non seulement php car il fallait télécharger aussi php5, php5-cli, php5-gd, php5-mysql. Il faut récupérer php-syslog-ng à partir de sourceforge.net ou The Home php-syslog-ng (site du php). On le télécharge à partir de ce lien <http://code.google.com/p/php-syslogng/downloads/list> Version (Mai 2008) : php-syslog-ng-2.9.8 ou selon une autre version qui soit équivalente.

4.4 Mysql:

Ça permet de stocker les différents événements dans une base de données Mysql pour une utilisation ultérieure. Ainsi il faut la mettre à jour lors de la configuration du système.

4.5 Snare:

Pour la collecte de donnée à partir des machines windows on utilise snare comme étant un client syslog qui envoie ses logs au serveur.

5 Installation et configuration :

5.1 Syslog-ng :

C'est une implémentation open source qui se base sur le protocole syslog. En utilisant UBUNTO on procède ainsi :

Tout d'abord on tape la commande « `sudo aptitude install syslog-ng` »
Une fois fait on modifie quelques instructions suivant nos besoins dans le fichier de configuration `/etc/syslog-ng/syslog-ng.conf` en jouant sur les paramètres suivants:

-> « **option** »

Définit les paramètres généraux de syslog-ng

-> « **source** »

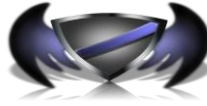
Définit la provenance des logs reçus par syslog-ng

-> « **destination** »

Transforme les logs

-> En requête SQL grâce à un système de template

-> à une destination classique



-> «filter»

Créer des règles de filtrage

Exemple:

On garde le message si le niveau est 'info', 'notice' ou 'warn' et si la facilité n'est pas 'cron'.

-> «log»

Applique toutes les sections définies précédemment.

Ensuite on redémarre syslog-ng :

```
sudo /etc/init.d/syslog-ng restart
```

5.2 Apache :

L'utilisation d'un serveur virtuel n'est pas nécessaire. il suffit donc de taper « sudo aptitude install apache2 ». on édite ensuite le fichier de configuration de apache sudo « vi /etc/apache2/apache2.conf » afin de pouvoir changer le nom du serveur :

```
ServerRoot "/etc/apache2" <<- Existing line
```

```
ServerName (nom du serveur)
```

Puis on redémarre le serveur « sudo /etc/init.d/apache2 restart »

5.3 PHP :

Sur la console on utilise la commande « sudo aptitude install php5 php5-cli php5-gd php5-mysql » puis on édite le fichier ini.php afin de faire quelques modifications qui seront utiles lors de la connexion au serveur apache : sudo vi /etc/php5/apache2/php.ini

On change ensuite les paramètres suivants :

```
memory_limit = 16M ->memory_limit = 128M
```

```
max_execution_time = 30->max_execution_time = 300
```

Puis on redémarre le serveur apache pour utiliser php:

```
sudo /etc/init.d/apache2 restart
```

5.4 L'interface web :

On accède à un root web en créant le répertoire suivant : « sudo su - mkdir -p /www && cd /www » et après avoir téléchargé le package php-syslog-ng on le décompresse ou on le décompacte à l'aide de la commande « tar xzvf php-syslog-ng-2.9.8.tgz » dans notre cas on utilise cette version mais on peut bien évidemment utiliser d'autres.

SECURINETS



Club de la sécurité informatique

On crée ensuite notre répertoire de logs :
mkdir -p /var/log/php-syslog-ng

Et enfin il faut activer apache avec la commande « /etc/init.d/apache2 reload »

On se connecte ensuite sur <http://localhost/php-syslog-ng/> afin de :

- Créer une base de données "syslog" avec les comptes utilisateurs adéquats
- paramétrer le site (mot de passe admin, adresse ...)

Une fois qu'on a terminé toutes les étapes de l'installation on démarre le php-syslog-ng en cliquant sur le bouton « view site » :

Php-Syslog-NG 2.9.1 Unstable [cdukes] 16-Jun-2006 16:00 EST Wednesday December 31st, 2008 - 15:35:24
Your IP: 127.0.1.1

Network Syslog Monitor

Login Help About

LOGIN:

Username:

Password:

Executed in 0.00478005409241 seconds

Php-Syslog-NG 2.9.1 Unstable [cdukes] 16-Jun-2006 16:00 EST Wednesday December 31st, 2008 - 16:00
Your IP: 127.0.1.1

Network Syslog Monitor

Logout Search Config Help About

USING TABLE: logs

USING CACHE TO POPULATE HOST AND FACILITY FIELDS.
Cache last updated on 2006-06-15 18:25:54.

<p>HOSTS: 2</p> <p>Include <input type="radio"/></p> <p>Exclude <input checked="" type="radio"/></p> <p>Hostname like <input type="text"/></p> <p>====AND====</p> <p>as-3550-2</p> <p>srv-www-001</p>	<p>SYSLOG FACILITY:</p> <p>Include <input type="radio"/></p> <p>Exclude <input checked="" type="radio"/></p> <p>daemon</p> <p>kern</p> <p>mail</p>	<p>SYSLOG PRIORITY:</p> <p>Include <input type="radio"/></p> <p>Exclude <input checked="" type="radio"/></p> <p>debug</p> <p>info</p> <p>notice</p> <p>warning</p> <p>err</p> <p>crit</p> <p>alert</p> <p>emerg</p>
---	---	--

<p>DATE</p> <p>From: <input type="text"/> <input type="button" value="aa"/></p> <p>To: <input type="text"/> <input type="button" value="aa"/></p>	<p>RECORDS PER PAGE 100</p> <p>ORDER BY datetime</p> <p>SEARCH ORDER DESC</p>
---	---

SEARCH MESSAGE:

Exclude AND

Exclude AND



Cette interface présente les différents champs du message log tel que :

- les priorités
- les facilités
- la date (on trouve la date de début et la date de fin)
- l'heure (on trouve l'heure de début et l'heure de fin)
- le nom de l'utilisateur
- le contenu même du message.....

Ces valeurs sont utilisées afin de pouvoir filtrer les journaux, on trouve aussi l'ordre du filtrage (croissant, décroissant..) ainsi que le paramètre utilisé.

Exemple : un filtrage suivant la date dans l'ordre décroissant.

La requête SQL sera affichée dans un champ spécifique comme suit :

The screenshot shows the Syslog-NG web interface. At the top, it displays 'Php-Syslog-NG 2.9.1 Unstable [cdukes] 16-Jun-2006 16:00 EST' and 'Wednesday January 14th, 2009 - 22:10:36'. Below this is a navigation bar with 'Logout Search Config Help About'. A search query is entered in a text box: 'SELECT SQL_CALC_FOUND_ROWS * FROM logs ORDER BY facility DESC LIMIT 0, 100'. Below the query is a table with columns: SEQ, HOST, FACILITY, DATE TIME, MESSAGE. The table contains three rows of log entries. At the bottom right, it says 'Executed in 0.0065369319916 seconds'.

SEQ	HOST	FACILITY	DATE TIME	MESSAGE
3	as-3550-2	mail-warning	2006-06-15 22:25:36	Line protocol on Interface FastEthernet0/7, changed state to up
2	as-3550-2	kern-info	2006-06-15 22:25:34	Duplicate address 10.10.2.2 on Vlan20
1	srv-www-001	daemon-warning	2006-06-15 22:25:32	%AAA-3-IPILLEGALMSG: Fan 1 had a rotation error reported.

Remarque :

syslog_mysql.sh est un script lancé lors de démarrage de syslog-ng il vérifie que le pipe (un canal) existe sinon il le crée.

La configuration du serveur peut contenir d'autres étapes suivant les besoins de l'utilisateur ainsi que la modification du fichier de configuration.

SECURINETS



Club de la sécurité informatique
INSAT

5.5 EventLog Analyser :

Une fois les fichiers log sont collectés, alors il nous reste qu'à faire l'analyse de ces fichiers à l'aide de l'outil EventLog Analyser.

ManageEngine
EventLog Analyzer 6

You have been successfully logged out

ManageEngine
Powering IT ahead

- Centralized Event Management
- Historical Trending
- Compliance Reporting
- Scheduled Event Reporting
- Built-in Database
- Totally Web-based access

Sign In here

User Name

Password

Keep me signed in

Login

First time users use 'admin' as User Name and 'admin' as Password to login.

Best viewed in IE 5.5+ or Mozilla 1.5+ or Netscape 7.0+ at a screen resolution of 1024 X 768 pixels.

© 2009 ZOHIO Corp. All Rights Reserved. E-mail : eventloganalyzer-support@manageengine.com
Website : www.eventloganalyzer.com

ManageEngine
EventLog Analyzer 6

Tell a friend Upgrade License Help Feedback About Logout (admin)

Home Reports Alerts Settings Ask MF Support

Create New Host New Alert Profile New Report New Filter Import Logs Advanced Search Bookmarks

From: 2010-02-03 00:00:00
To: 2010-04-16 22:20:00

Dashboard

Total Events Per Host Group

Total Events Per Event Type

Hosts

All Hosts Search Add New Host

Showing: 1 to 1 of 1 Page: [1] View per page: 5 [10] 20 25 50 75 100 150 200

HostName	HostGroup	Status	Error	Warning	Failure	Others	Total
sweet-7U8cQeU51	WindowsGroup		33	10	0	145	188



7. Conclusion

D'après cette étude sur la journalisation et l'analyse des logs on a pu connaître des outils performants avec une souplesse de configuration et une comptabilité sous de diverses plateformes. Ainsi on a pu trier en détail les messages de log par le biais des filtres qui jouent un rôle important pour informer l'administrateur sur le degré d'importance des événements en cours et conserver la trace des différents utilisateurs qui se connectent dans un réseau pendant une période bien déterminée. Toutefois, l'abondance des journaux échangés cause un « éclatement » de traces, de plus pour syslog-ng on a eu recours à plusieurs outils afin de pouvoir percevoir son utilité et son bon fonctionnement.