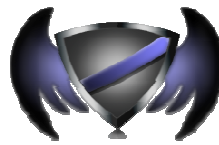


Dans le cadre de *SECURIDAY 2009*

SECURINETS



*Présente*

# Atelier : OSSIM

## Formateurs:

1. BOUCHRIHA Aymen
2. BOURGUIBA Mouna
3. EL GARES Afef
4. OUERGHI Manel

## 1. Présentation :

OSSIM est une solution offrant une infrastructure pour le monitoring de la sécurité réseau. Ses objectifs consistent à :

- Fournir un cadre centralisé
- Fournir une console d'organisation
- Améliorer la détection et l'affichage des alarmes de sécurité

## 2. Outils utilisés :

Les outils utilisés sont :

- un serveur OSSIM version 1.0.6 téléchargeable à partir du site :  
<http://www.ossim.net/docs/INSTALL.Debian.quick.html>
- L'agent PADS
- L'agent TCPTRACK
- L'agent POF
- L'agent SNORT
- L'agent NTOP

Les dernières versions de ces agents peuvent être installées à l'aide de la commande : atp-get install.

## 3. Architecture OSSIM :

L'architecture d'OSSIM est divisée en 2 principaux étages :

- **Pré-processing** : remontée d'événements des moniteurs et détecteurs dans une base de données commune.
- **Post- processing** : analyse centralisée.

La figure ci-dessous illustre le fonctionnement en 2 étages. Nous remarquons que ces deux étages disposent de différentes bases de données permettant la sauvegarde des informations intermédiaires (corrélées).

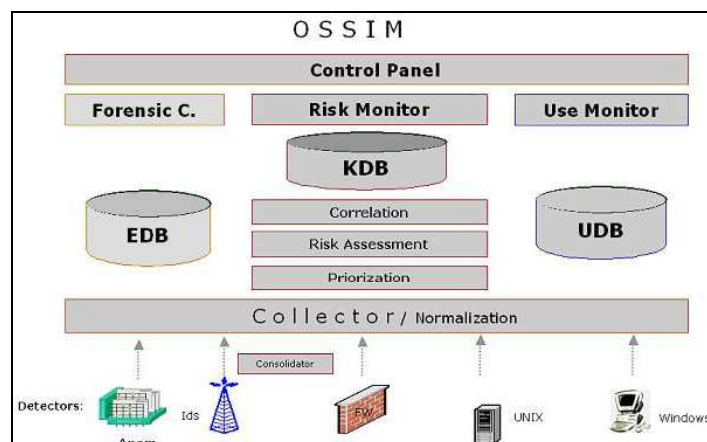
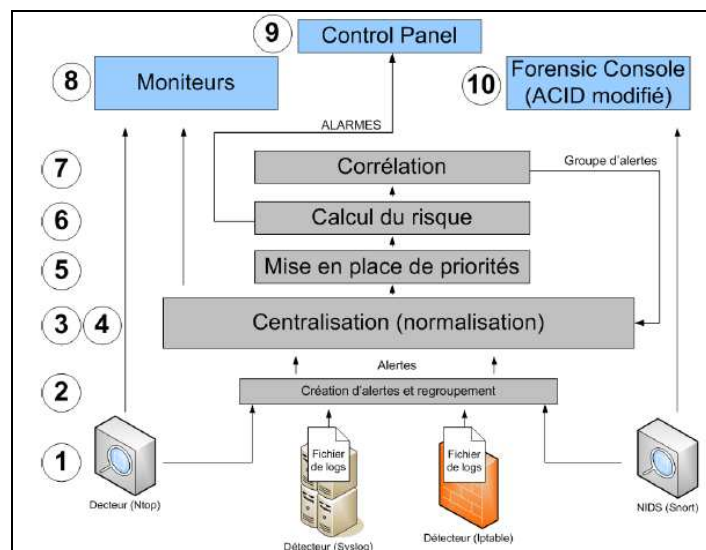


Figure 1 : Architecture OSSIM

Définitions des bases de données :

- **EDB** : La base de données des événements (la plus grande), stockant toutes les alarmes individuelles.
- **KDB** : La base de données des connaissances, sauvegardant les configurations établies par l'administrateur en charge de la sécurité.
- **UDB** : La base de données des profils, stockant toutes les informations du moniteur de profile.

Nous détaillons l'acheminement d'une alarme dans l'architecture définie par la figure ci-dessus.



**Figure 2. Data flow du serveur OSSIM**

1. Détection d'un événement suspect par un détecteur (par signatures ou par l'heuristique).
2. Si nécessaire, des alarmes seront regroupées (par le détecteur) afin de diminuer le trafic réseau.
3. Le collecteur reçoit la/les alarme(s) via différents protocoles de communications ouverts.
4. Le parser normalise et sauve les alarmes dans la base de données d'événements (EDB).
5. Le parser assigne une priorité aux alarmes reçues en fonction de la configuration des polices de sécurité définies par l'administrateur sécurité.
6. Le parser évalue le risque immédiat représenté par l'alarme et envoie si nécessaire une alarme interne au Control panel
7. L'alerte est maintenant envoyée à tous les processus de corrélation qui mettent à jour leurs états et envoient éventuellement une alerte interne plus précise (groupe d'alerte provenant de la corrélation) au module de centralisation.
8. Le moniteur de risque affiche périodiquement l'état de chaque risque calculé par CALM.

9. Le panneau de contrôle affiche les alarmes les plus récentes et met à jour les indices des états qui sont comparés aux seuils définis par l'administrateur. Si les indices sont supérieurs aux seuils configurés, une alarme interne est émise.
10. Depuis le panneau de contrôle, l'administrateur a la possibilité de visualiser et rechercher des liens entre les différentes alarmes à l'aide de la console forensic.

#### 4. Fonctionnement logiciel de l'architecture :

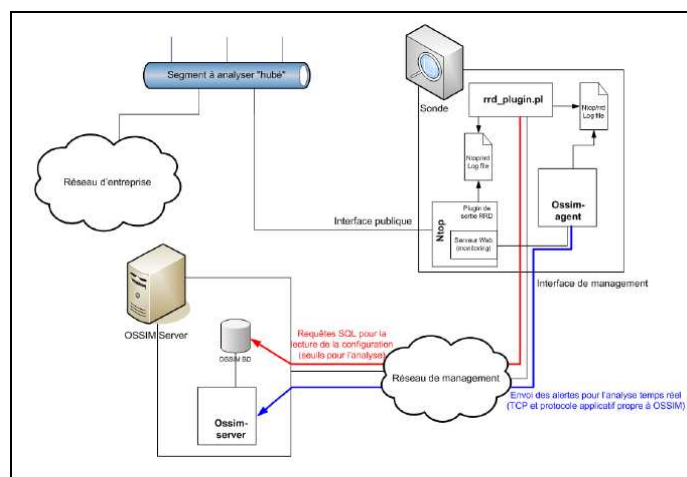
##### a. Les applications Ossim-server et Ossim-agent :

- **Ossim-agent** : récupère simplement les informations des fichiers de logs des plugins et les envoie directement au serveur Ossim permettant ainsi le traitement temps réel de celles-ci. De plus, l'agent Ossim s'occupera de la mise en marche et de l'arrêt des différentes sondes qui lui sont connectées.
- **Ossim-server** : constitue le noyau de l'architecture. En effet, celui-ci comporte les modules d'analyse et de corrélation des données ainsi qu'un serveur Web permettant l'interaction avec l'utilisateur (administrateur réseau).

##### b. Fonctionnement avec une sonde Ntop :

Ce logiciel analyse en temps réel le trafic réseau et met à disposition une liste de compteurs, permettant le monitoring ainsi que le calcul de statistiques. La sonde Ntop met en place un serveur Web permettant le son monitoring ainsi que la sa configuration à distance. Le plugin de sortie RRD est nécessaire pour l'intégration de Ntop dans Ossim. Celui-ci permet l'enregistrement des données sous forme de tourniquet.

Le principe de communication d'une sonde Ntop avec le serveur OSSIM est illustré par la figure ci dessous.



**Figure 3 : Principe de communication entre une sonde Ntop et le serveur d'OSSIM**

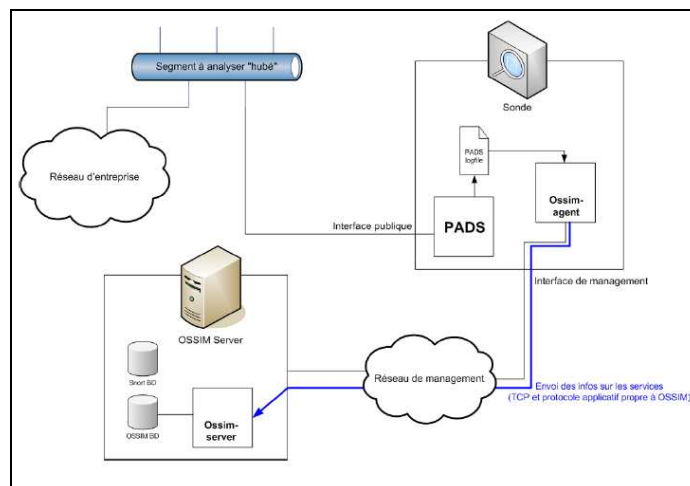
Le script Perl rrd plugin.pl effectue la liaison entre Ntop et l'agent Ossim. Celui-ci interroge périodiquement la « base de donnée » RRD à l'aide de l'outil RRDtool. Il récupère les seuils des compteurs définis par l'administrateur réseau à l'aide du framework de configuration et les compare aux données précédemment récupérées.

Les éventuels dépassements des seuils sont ensuite stockés dans un fichier de log (/var/log/ossim/rrd plugin.log) qui sera récupéré par l'agent Ossim afin de permettre l'envoi temps réel des informations au serveur. La corrélation des ces informations peut ensuite être effectuée sur le serveur.

### c. Fonctionnement de l'architecture avec une sonde PADS :

PADS va permettre d'identifier les machines (adresses IP et MAC) ainsi que leurs services uniquement en sniffant le réseau. Il permettra l'affichage des services d'une machine sans avoir à opérer un scan actif. Il permettra l'affichage des services d'une machine configurée sur Ossim sans opérer un scan actif.

Le principe de communication d'une sonde PADS avec le serveur OSSIM est illustré par la figure ci-dessous.



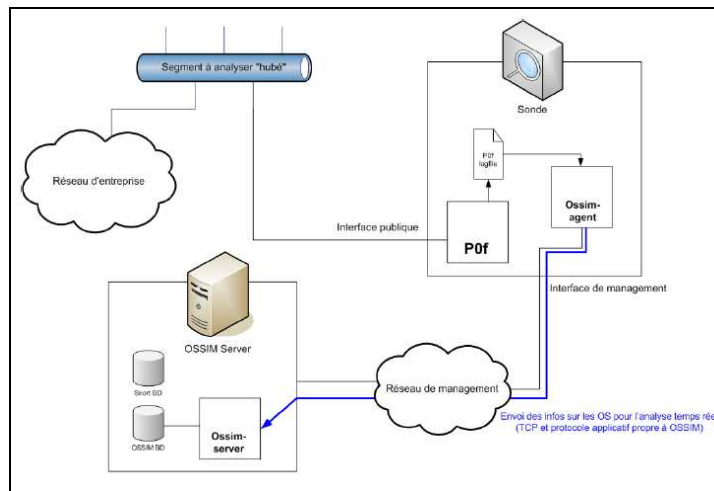
**Figure4 : Principe de communication entre une sonde PADS et le serveur d'OSSIM**

Le logiciel PADS reportera simplement toutes les informations récoltées dans le fichier de log /var/log/ossim/pads.csv (indiqué dans la configuration du plugin, fichier /etc/ossim/agent/plugins/pad.xml). L'agent Ossim se chargera ensuite de les récolter et de les envoyer de manière temps réel au serveur.

### d. Fonctionnement avec une sonde P0f :

P0f est un logiciel de détection de système d'exploitation passif. Il analyse les trames transitant sur le réseau (le segment analysé) et les compare avec une base de données des caractéristiques de chaque OS (prise d'empreintes) afin d'en retrouver l'OS correspondant. P0f est totalement passif. Il ne génère aucun trafic réseau supplémentaire.

Le principe de communication d'une sonde P0f avec le serveur OSSIM est illustré par la figure ci-dessous.



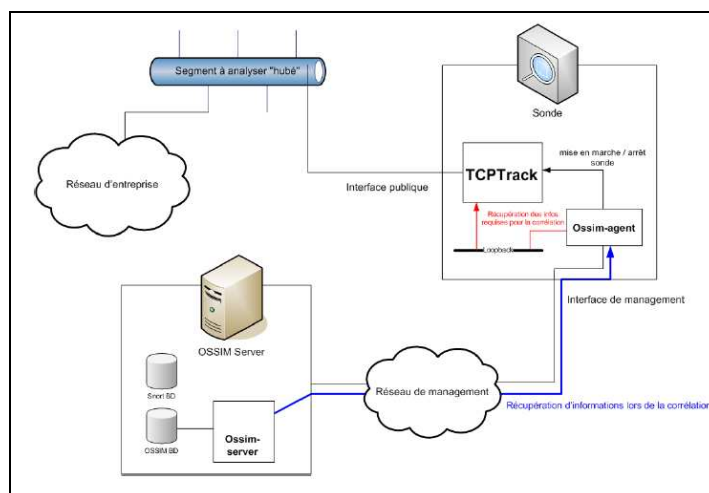
**Figure 5 : Principe de communication entre une sonde P0f et le serveur d'OSSIM**

Celui-ci est assez simple. P0f écrit ses logs dans le fichier `/var/log/ossim/p0f.log` (chemin fournit à P0f par l'agent Ossim lors du lancement de P0f). Ce chemin se trouve donc dans la configuration du plugin P0f (`/etc/ossim/agent/plugins/p0f.xml`) de l'agent. Le daemon agent (`ossim-agent`) s'occupera ensuite de les récupérer afin de les envoyer au serveur Ossim pour une analyse temps réel.

### e. Fonctionnement avec une sonde TCPTrack :

TCPTrack est un sniffer affichant des informations sur les connexions TCP qu'il rencontre sur une interface. Il détecte passivement les connexions TCP sur l'interface à analyser et affiche les informations. Il permet l'affichage des adresses source et destination, de l'état de la connexion, du temps de connexion ainsi que de la bande passante utilisée.

Le principe de communication d'une sonde TCPTrack avec le serveur OSSIM est illustré par la figure ci-dessous.



**Figure 6 : Principe de communication entre une sonde TCPTrack et le serveur d'OSSIM**

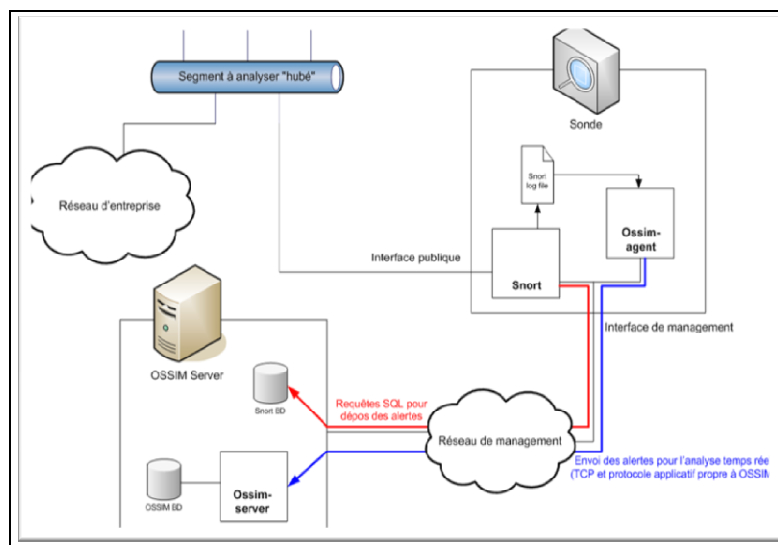
TCPTrack fonctionne d'une manière similaire à l'affichage Web des informations de Ntop. En effet, aucune information n'est spontanément envoyée vers le serveur Ossim. TcpTrack ouvre simplement un port serveur sur la loopback de l'agent. C'est ensuite le serveur Ossim, qui lors du procédé de corrélation, interrogera si nécessaire l'agent afin qu'il interroge à son tour TCPTrack). Une fois les informations récoltées par l'agent, celui-ci se chargera de les remettre au serveur qui les utilisera pour la corrélation. L'agent joue donc un rôle d'intermédiaire entre le serveur et le sonde TCPTrack.

#### **f. Fonctionnement de l'architecture avec une sonde Snort :**

**Snort** est un système de détection d'intrusions réseau en Open Source, capable d'effectuer l'analyse du trafic en temps réel. On l'utilise en général pour détecter une variété d'attaques et de scans. Il peut être configuré pour fonctionner en plusieurs modes.

Dans la cadre de l'architecture d'OSSIM, Snort fonctionne en mode NIDS. En effet, il analyse le trafic du réseau, compare ce trafic à des règles déjà définies par l'utilisateur et établit des actions à exécuter.

Le principe de communication d'une sonde Snort avec le serveur OSSIM est illustré par la figure ci-dessous :



**Figure 7 : Principe de communication entre une sonde SNORT et le serveur d'OSSIM**

Nous remarquons que l'IDS Snort est indépendant du programme client d'OSSIM (nommé : ossim-agent) et que deux flux d'informations sont émis en direction du serveur.

## 5. Installation et configuration

### a. Server OSSIM :

On télécharge et on installe le serveur OSSIM à partir du site officiel d'OSSIM

<http://www.ossim.org/OSSIM/Downloads.html>

### b. Agent OSSIM:

On installe avec apt-get install ossim-agent:

```
# apt-get install ossim-agent
```

On configure l'agent ossim en effectuant des modifications sur son fichier /etc/ossim/agent/config.cfg:

```
# vi /etc/ossim/agent/config.cfg
```

```
sensor = 127.0.0.1
interface = eth0 # interface from where the event has come
date_format = %Y-%m-%d %H:%M:%S ; format, not date itself
ossim_dsn=mysql:localhost:ossim:root:yoursecretpassword
```

```
enable = True
ip = 127.0.0.1
port = 40001
```

```
GRANT ALL PRIVILEGES ON *.* TO 'snort_database_user'@'sensor_ip' identified
by 'mysql_password';
```

### c. Outils supplémentaires :

- NTOP :

```
# apt-get install librrd2 ntop
# ntop -u ntop
>> Please enter the password for the admin user:
# ^C
# /etc/init.d/ntop start
```

**S E C U R I N E T S**  
**Club de la sécurité informatique**  
**I N S A T**

- PADS :

```
# apt-get install pads
```

- P0F :

```
# apt-get install p0f
```

- TCPTRACK :

```
# apt-get install tcptrack
```

Après chaque installation on utilise la commande suivante pour activer l'outil chez l'agent :

```
# dpkg-reconfigure ossim-agent
```

Pour plus de renseignement veuillez consulter notre site :

[http://securinets.souayeh.com/index.php?option=com\\_docman&task=cat\\_view&gid=90&Itemid=56](http://securinets.souayeh.com/index.php?option=com_docman&task=cat_view&gid=90&Itemid=56)