

HIMS

Host Intrusion Monitoring System

Nicolas Greneche

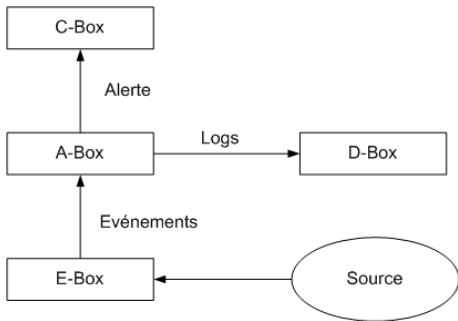
MAPMO
Projet SDS

Mathrice Rouen 2008

- 1 Introduction
- 2 Osiris
- 3 Samhain
 - Architecture
 - Installation
 - Politiques de protection
 - Déploiement

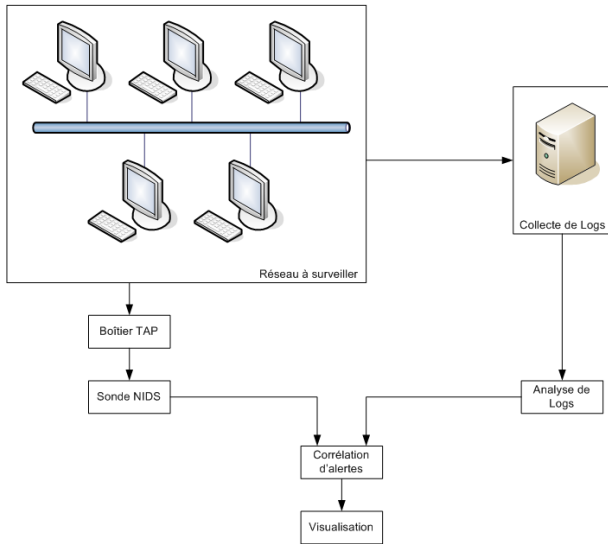
- IDS : Intrusion Detection System

- IDS : Intrusion Detection System



Introduction à la détection d'intrusions

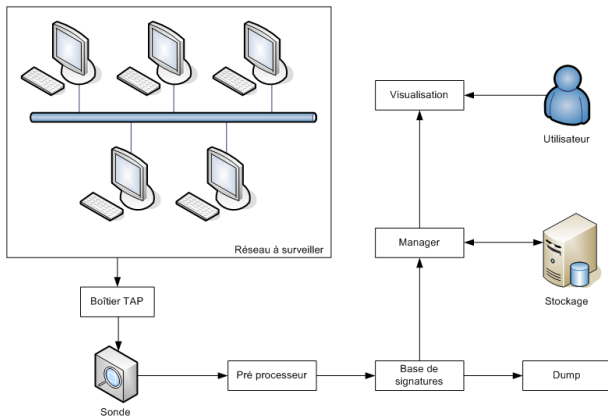
- IDS : Intrusion Detection System



- NIDS : Network Intrusion Detection System

Introduction à la détection d'intrusions

- NIDS : Network Intrusion Detection System



Discussion :

- Temps nécessaire à l'analyse des alertes
- L'attaque est-elle un succès ?
- Systèmes basés sur des signatures (SNORT)
- Techniques d'évasion

Ne peut-on rien faire côté réseaux ?

Ne peut-on rien faire côté réseaux ?

Analyse de flux

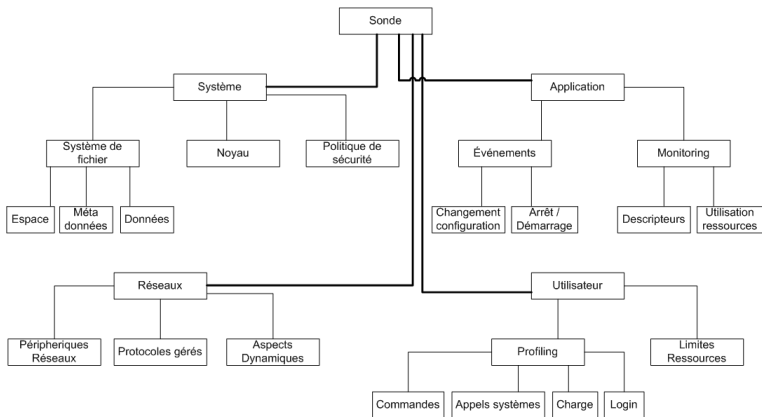
Ne peut-on rien faire côté réseaux ?

Analyse de flux

- Netflow / Sflow : informations précises (réplication des trames transmises sur les ports des équipements de commutation et routage), connexions non gérées et gros volume de données
- Argus : Orienté connexions, rapidité d'acquisition, petit volume de données, pas de payload

- HIDS : Host Intrusion Detection System

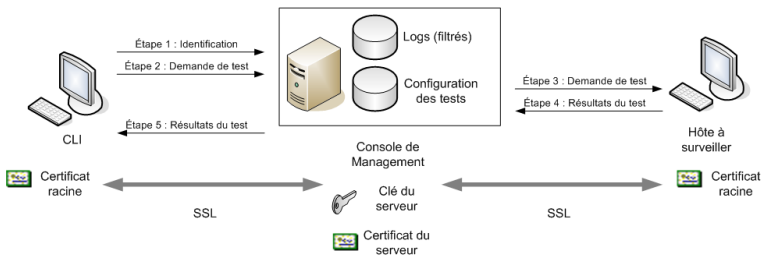
- HIDS : Host Intrusion Detection System



- HIMS : Host Intrusion Monitoring System
 - Intégrité des fichiers (données et métas)
 - Intégrité du noyau (table des appels systèmes)
 - Architecture distribuée
 - Acteurs historiques : Integrit, AIDE, Tripwire
 - Actualité : OSIRIS, Samhain

- Architecture

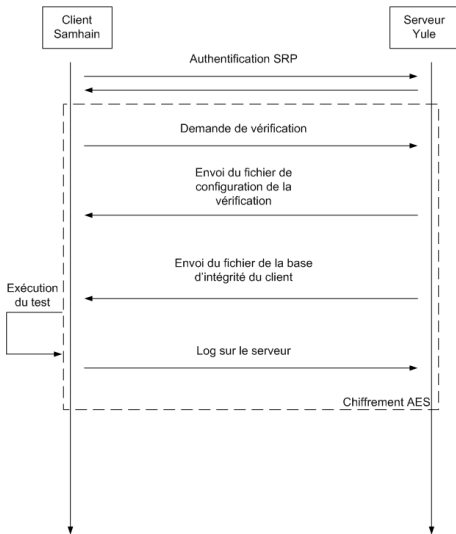
- Architecture



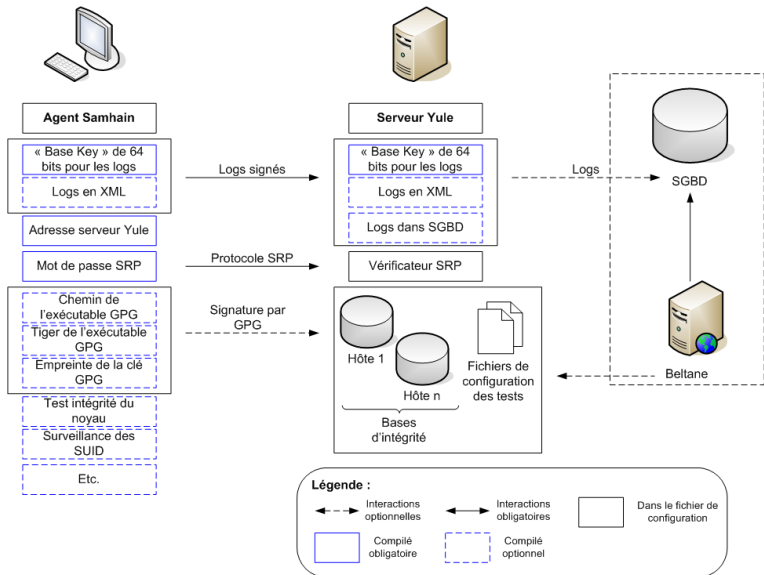
- Mode PUSH : Le serveur donne les instructions à l'agent sur les tests à effectuer sur le client
- Compatible OSSIM
- Plus ergonomique et simple à configurer que Samhain
- Beaucoup plus compliqué à distribuer que Samhain

- Yule : serveur contenant les bases d'intégrité
- Samhain : agent côté client
- Peut aussi fonctionner en "standalone"

Samhain - architecture



Samhain - architecture



```
./configure --enable-network=server --with-database=mysql  
--enable-xml-log
```

samhain has been configured as follows :

System binaries : /usr/local/sbin

Configuration file : /etc/yulerc

Manual pages : /usr/local/man

Data : /var/lib/yule

PID file : /var/run/yule.pid

Log file : /var/log/yule/yule_log

Base key : 1348296752,6012908

```
make && make install && make install-boot
```

- Configuration file (/etc/yulerc) : emplacement du fichier de configuration de Yule
- Data (/var/lib/yule) : répertoire qui va accueillir les bases d'intégrité et les fichiers de configuration des hôtes sous la surveillance de Samhain
- Log file (/var/log/yule/yule_log) : fichier contenant les logs remontés au serveur Yule. Ces logs seront présentés au format XML

```
./configure --enable-network=client --enable-mounts-check  
--enable-suid-check  
--with-kcheck=/boot/System.map-2.6.18-3-686  
--with-logserver=192.168.1.100 --enable-xml-log  
--with-config-file=REQ_FROM_SERVER/etc/samhainrc  
--with-data-file=REQ_FROM_SERVER/etc/samhain_file  
--enable-base=1348296752,6012908 --enable-static
```

samhain has been configured as follows :

System binaries : /usr/local/sbin

Configuration file : REQ_FROM_SERVER/root/.sam/samhainrc

Manual pages : /usr/local/man

Data : /root/.sam

PID file : /root/.sam/samhain.pid

Log file : /root/.sam/samhain_log

Base key : 1348296752,6012908

make && make install && make install-boot

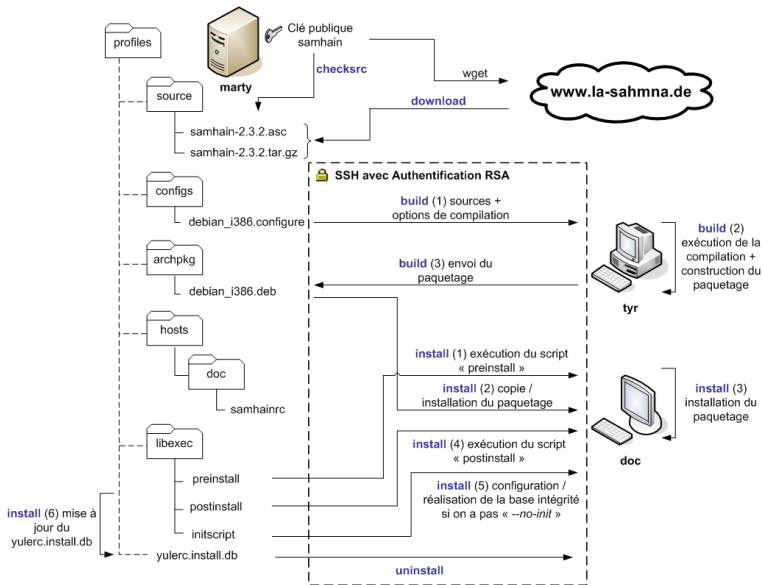
Granularité :

- Checksum des fichiers (CHK)
- Traiter les liens (LNK / HLN)
- Traiter les inodes (INO)
- Propriétaire, Groupe (USR / GRP)
- Mtime, Atime et Ctime (MTM / ATM / CTM)
- Taille des fichiers (SIZ)
- Major / Minor pour les fichiers de /dev (RDEV)
- Permissions (MOD)
- Prelink (PRE)
- Autorise uniquement les fichiers à grossir (SGROW)

Protections supplémentaires :

- Fichiers SUID / SGID (Quarantaine ou suppression)
- Dissimulation de Samhain (khide)
- Protection noyau contre les hooks d'appels systèmes
- Utilisation de GnuPG pour signer les échanges avec le serveur Yule

Samhain - déploiement



Grandement simplifié avec beltane !