Logiciel d'empreinte système

tripwire est un logiciel permettant de prendre une empreinte du système et de vérifier, controler l'intégrité d'un système de fichiers

- ***Le principe*** : est de créer une image (snapshot) du système de fichier à un temps ”t0”. On recrée chque jour des images qu'on compare à l'image de départ. On trouve ainsi immédiatement tous les fichiers modifiés

Initialisation de tripwire

première étape : créer une base de données de départ. Cette BD est un ”snapshot” du file system complet, qui servira de base de comparaison pour les contrôle d'intégrité futurs

Initialisation de tripwire - Fichiers de config

A l'installation tripwire génére une paire de clé cryptographique quivont servir a signer et chiffrer les fichiers d'empreinte

```
ll  /etc/tripwire/
-rw------- 1 root root  931 2009-01-24 19:30 libes-local.key
-rw------- 1 root root  931 2009-01-24 19:28 site.key
-rw-r--r-- 1 root root 4586 2009-01-24 19:30 tw.cfg
-rw-r--r-- 1 root root  486 2007-04-30 20:10 twcfg.txt
-rw-r--r-- 1 root root 4159 2009-01-24 19:30 tw.pol
-rw-r--r-- 1 root root 6057 2007-04-30 20:10 twpol.txt
```

- Tripwire lit le fichier de ”policy” */etc/tripwire/twpol.txt* pour faire son empreinte.. cette empreinte est signée cryptographiquement avec des clés générées lors de l'install
- Tripwire conserve sa configuration dans une base de données chiffrée qui est générée, par défaut, à partir de /etc/tripwire/twcfg.txt.

Génération de l'empreinte

- Génération de l'empreinte : *tripwire --init --verbose*

```
Opening configuration file: /etc/tripwire/tw.cfg
This file is encrypted.
Opening key file: /etc/tripwire/site.key
Opening key file: /etc/tripwire/libes-maison-local.key
Please enter your local passphrase:
...Wrote database file: /var/lib/tripwire/libes-maison.twd
```

- À l'issue de la commande, L'empreinte système est faite et chiffrée

- Pour imprimer l'empreinte en clair :
  - */usr/sbin/twprint -m d*
- la base de données est située dans */var/lib/tripwire.* Cet emplacement doit être protégés en écriture

Modification des fichiers de config.

- si on veut affiner l'empreinte prise par tripwire, il faut éditer et modifier le fichier le fichier /etc/tripwire/twpol.txt (qui est la version texte du fichier tw.pol)...
- Modifier ce fichier texte et le rechiffrer par la suite avec twadmin pour refaire une image binaire chiffrée de ce fichier par la commande
  - tripwire --update-policy

Tripwire : Les contrôles subséquents

- Le but est de recalculer régulièrement (cron) une empreinte du système et de la comparer à l'empreinte originale.
  - Les calculs d'empreinte se font par la commande
    - */usr/sbin/tripwire –check*

```
/usr/sbin/tripwire --check
Parsing policy file: /etc/tripwire/tw.pol
*** Processing Unix File System ***
Performing integrity check...
```

- Lors des controles subséquents, la base de données initiale sert de point de comparaison. Le diagnostic donne les éléments du file system qui ont été touchés/modifiés entre les 2 controles.
- la commande */usr/sbin/tripwire --check* produit un fichier de rapport chiffré qui se trouve dans */var/lib/tripwire/report*

Tripwire : exploitation des fichiers de rapport

- La commande twprint affiche le contenue de la database et des fichiers de rapport en texte clair
- $ ls -l /var/lib/tripwire/report/
- `-rw-r--r-- 1 root root 11126 2009-01-24 23:26 libes-maison-20090124-232258.twr`
- Ce fichier de rapport binaire peut etre lu avec la commande *twprint*
  - `$ twprint -m r --twrfile /var/lib/tripwire/report/libes-maison.twr`

Tripwire : Exploitation des rapports

	Rule Name	SeverityLevel	Added	Removed	Modified
	Invariant Directories	66	0	0	0
*	Tripwire Data Files	100	1	0	0
	Other binaries	66	0	0	0
	Tripwire Binaries	100	0	0	0
	Other libraries	66	0	0	0
*	Root file-system executables	100	1	0	2
	System boot changes	100	0	0	0
	Root file-system libraries	100	0	0	0

Added object name: /bin/.hack
Modified object name: /bin/ps

Mise à jour de l'empreinte système

- Toute modification (volontaire, ou intrusive) du file system va être détectée par tripwire --check. Destruction, création, mais également modification des inodes de fichiers (dates, propriétaires..)
- Si on installe des logiciels apres la 1ere empreinte faite par tripwire, les controles par tripwire --check vont s'avérer positifs
- Au cours de la vie du système il faut donc mettre a jour l'empreinte initiale après certaines opérations maitrisées par l'ASR
  - `/usr/sbin/tripwire --update`
    - `--dbfile /var/lib/tripwire/compc32.com.univ-mrs.fr.twd`
    - `--twrfile /var/lib/tripwire/report/compc32.com.univ-mrs.fr-20090124-23322.twr`