Université Paris Descartes
UFR Mathématiques et Informatique

Master RIP filière Réseaux

Tutorial Tripwire

Lynda TLILI

lynda.tlili@gmail.com

Sécurité des réseaux 2011/2012

Tutoriel Tripwire

Dans ce tutoriel, on apprendra qu'est ce que Tripwire, comment l'installer et comment l'utiliser. On apprendra les bases nécessaires à la simple surveillance des fichiers sensibles sur une machine.

Sommaire

1 Introduction

2 Qu'est ce que Tripwire ?

3 Fonctionnement

4 Téléchargement

5 Installation et configuration

6 Utilisation

7 Conclusion

1 Introduction

Tripwire est un outil de détection d'intrusion qui permet de vérifier l'intégrité de fichiers, grâce à une prise *d'empreinte* effectuée dès l'installation du système. Cette empreinte est basée sur la taille, la date, et le contenu des fichiers. Il suffit donc de lancer une vérification de ces fichiers au moment où vous le demandez, ou bien, à chaque fois que vous l'avez programmé.

2 Qu'est ce que Tripwire ?

Tripwire est un *HIDS* (*HostBased Intrusion Detection System*) qui surveille l'état de la sécurité des fichiers et des répertoires sensibles au niveau d'un hôte qui tourne sous Linux.

Tripwire surveille et détecte toute modification non autorisée :

- Les fichiers ajoutés.
- Les fichiers modifiés.
- Ce qui est modifié dans les fichiers.
- Qui a effectué les modifications.
- Quand les modifications ont-elles eu lieu.

3 Fonctionnement

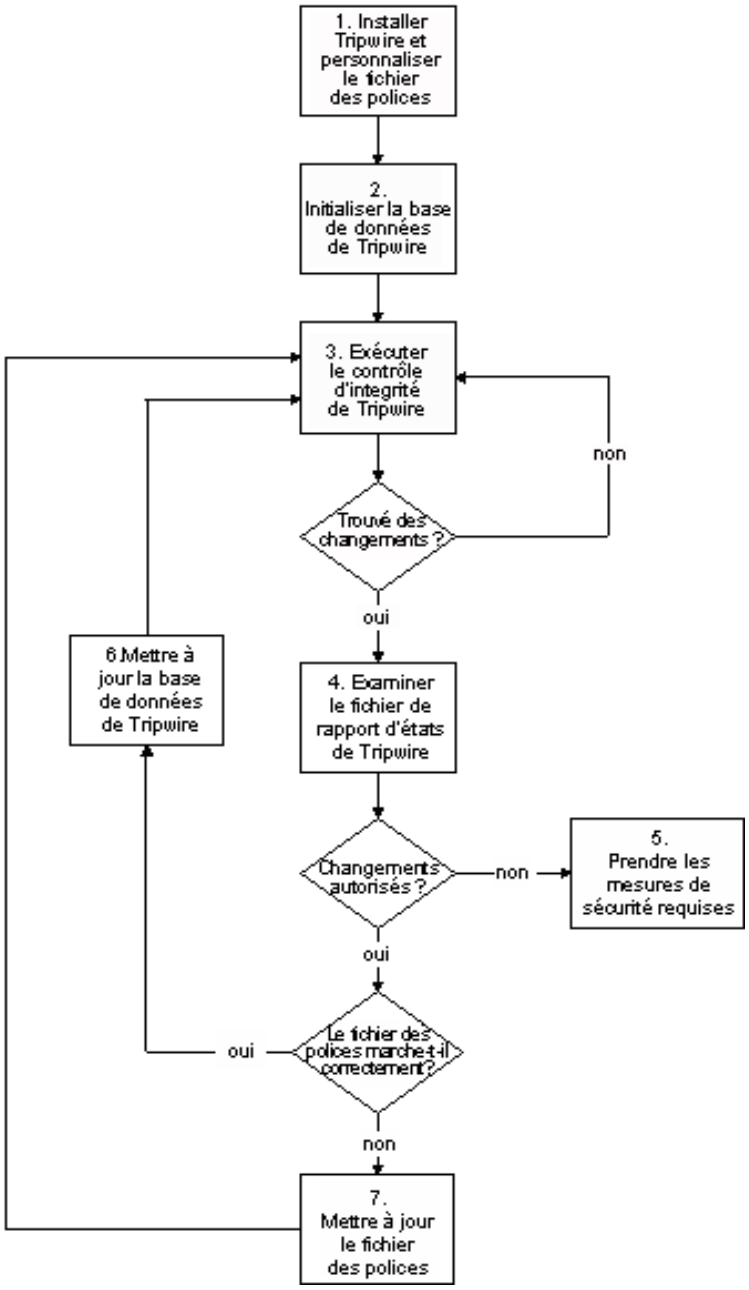


Figure. Schéma de fonctionnement de Tripwire.

1. Installer Tripwire et personnaliser les fichiers de politiques.
2. Initialiser la base de données.
3. Exécuter la vérification d'intégrité des fichiers.
4. Examinez le fichier de rapport.
5. Si des violations d'intégrité non autorisés surviennent, prendre les mesures de sécurité appropriées.

6. Si les modifications de fichier sont valides, vérifier et mettre à jour le fichier de base de données.
7. Si la vérification échoue, mettre à jour le fichier des règles.

4 Téléchargement

Récupérer la dernière version de Tripwire Open source (*tripwire 2.4.2.2)* au format compressé *bz2* à partir de : http://sourceforge.net/projects/tripwire/.

5 Installation et configuration

Il est important de souligner que l'installation de Tripwire doit se faire sur un système ou une machine *propre* (non infecté), car il serait inutile de sécuriser un système déjà infecté.

5.1 Installation

Décompresser l'archive téléchargée dans le répertoire `/usr/src`.

```
# tar xjvf tripwire-2.4.2.2-src.tar.bz2
```

Se placer dans le répertoire de Tripwire.

```
# cd tripwire-2.4.2.2-src
```

Spécifier le répertoire d'installation avec l'option préfixe (exemple : répertoire `tw`).

```
# ./configure -- prefix =/tw/tripwire
```

Chercher le programme exécutable d'installation (fichier *install.sh)*.

```
# make
```

Lancer l'installation de Tripwire.

```
# make install
```

– L'invite de commande demande de lire la licence du logiciel Tripwire.

Après avoir lu la licence, tapez `accept`.
Confirmer l'installation avec `y` pour poursuivre l'installation.

– Par la suite, on obtient les messages suivants :

`Enter the site keyfile passphrase` entrez un "mot de passe" pour le site

Entrer un mot de passe pour le site afin de créer la clé pour crypter les fichiers de configuration et des règles (*tw.cfg* et *tw.pol).*

`Enter the local keyfile passphrase` entrez un "mot de passe" local

Entrer un mot de passe local pour crypter le fichier de la base de données et les rapports.

```
Wrote configuration file: /etc/tripwire/tw.cfg
```

Entrer le mot de passe du site pour crypter le fichier des règles *tw.pol*

```
Please enter your site passphrase
Wrote policy file: /etc/tripwire/tw.pol
```

entrez le "mot de passe" pour le site

5.2 Configuration

Pour la première utilisation de Tripwire, il faut initialiser sa base de données. La base de données servira de référence pour la comparaison. Elle contient l'image des fichiers originaux.

- **Initialisation de la base de données**

Se placer dans le répertoire contenant le fichier exécutable d'initialisation de la base de données.

```
# cd /tw/tripwire/sbin/
```

Lancer l'initialisation de la base de données.

```
# ./tripwire -- init
```

Le système vous demande alors le mot de passe locale pour crypter le fichier de règles.

– Le fichier crée `/rep/lib/tripwire/IDS.twd` est l'image des fichiers sensibles de la machine (IDS étant à remplacer par votre nom de machine). Il est recommandé de copier ce fichier et de réaliser une sauvegarde.

- **Mise à jour de la base de données**

Si des fichiers sont ajoutés ou modifiés volontairement par l'administrateur, Tripewire génère des alertes et/ou des erreurs dans les rapports. Pour éviter cela, il suffit de mettre à jour votre base.

```
# tripwire --update --twrfile /var/lib/tripwire/report/nomdurapport.twr
```

Cette commande ouvre l'éditeur de texte *nano* avec votre rapport, en ajoutant le symbole « x » devant les modifications.

- **Génération du rapport**

Pour effectuer la vérification et le contrôle des modifications sur les fichiers surveillés, il suffit de générer le rapport de Tripwire et passer en revue les fichiers corrompus.

```
# cd /tw/tripwire/sbin/
#./tripwire --check
```

Le rapport est créé dans le répertoire `/var/lib/tripwire/` et sous la forme : *`nomdemachine-date-heure`*`.twr`, la date et l'heure sont celles du système lors de la génération du rapport.

Les rapports générés sont cryptés, pour les visualiser il faut taper la commande suivante :

```
# cd /tw/tripwire/sbin/
# ./twprint -m r -r /opt/tripwire/lib/tripwire/report/nomdurapport.twr
```

- **Le fichier des règles de sécurité**

Les règles de sécurité (mesures de sécurité) à appliquer après une modification sont sauvegardées dans le fichier `/etc/tripwire/tw.pol`.

Le fichier des règles est crypté mais il est possible de générer une copie au format txt avec la commande suivante :

```
# twadmin --create-polfile -S site.key /etc/tripwire/twpol.txt
```

Si l'utilisateur apporte des modifications dans fichier de règles, il faut mettre à jour le fichier des règles, réinitialiser la base de données puis supprimer le fichier txt.

```
# ./tripwire - update-policy - secure-mode bass ../etc/twpol.txt
```

Tous les paramètres des règles de sécurité sont disponibles dans le fichier `/rep/tripwire/doc/tripwire/policyguide.txt`.

- **Le fichier de configuration**

Le fichier de configuration `tw.cfg` est aussi un fichier crypté qui contient, entre autres, tous les paramètres de configuration de Tripwire à savoir :

- localisation du répertoire root de tripwire,
- localisation du répertoire de règles de sécurité,
- localisation du répertoire de la BdD,
- localisation du répertoire des rapports,
- localisation du répertoire des clés,
- localisation du répertoire de l'éditeur de texte (vi),
- …etc.

Pour « sécuriser » un peu plus l'outil Tripwire, il est conseillé de modifier les chemins par défaut de ces fichiers.

Pour recréer une copie du fichier `tw.cfg` en format texte, il suffit de lancer la commande suivante :

```
# twadmin --create-cfgfile -S site.key /etc/tripwire/twcfg.txt
```

Après modification du fichier `/etc/tripwire/twcfg.txt`, il faut relancer une initialisation de la base de données et supprimer le fichier txt généré.

6 Utilisation

On va manipulation l'outil Tripwire pour surveiller un fichier sensible sur le système et empêcher toute modification sur ce dernier.

1. Soit *test.txt* le fichier sensible à surveillé par Tripwire.
2. Protéger le fichier *test.txt* et autoriser seulement la lecture.
3. Modifier le fichier des règles et ajoute la nouvelle règle de vérification

Editer le fichier des règles.

```
# cd /tw/tripwire/etc/
# nano twpol.txt
```

Ajouter la nouvelle règle qui autorise que la lecture seule du fichier *test.txt.*

```
(
    rulename=''test'';
)
{
    /test.txt ->$(readOnly);
}
```

4. Visualiser le fichier des règles et vérifier que la nouvelle règle à bien été ajouté.

```
# cd /tw/tripwire/etc/
# cat twpol.txt
```

5. Réinitialiser la base de données.

```
# cd /tw/tripwire/sbin/
# ./tripwire --init
```

6. Éditer le fichier surveillé et apporter des modifications.

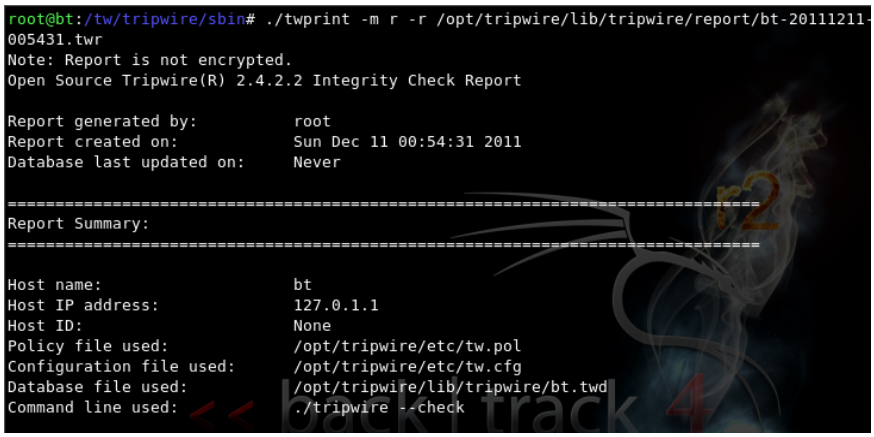
```
# nano test.txt
```

7. Générer le nouveau rapport de vérification de l'intégrité des fichiers.

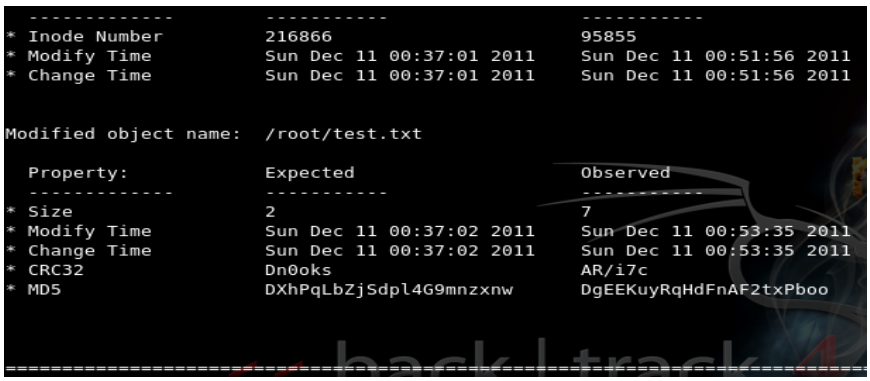
```
# cd /tw/tripwire/sbin/
# ./tripwire --check
```

8. Visualiser le rapport et vérifier si des fichiers ont été modifiés depuis le dernier control.

```
# cd /tw/tripwire/sbin/
#./twprint -m r -r/opt/tripwire/lib/tripwire/report/bt-20111211-005431.twr
```



– La partie **«** Rule Summary », montre quel fichier a été modifié (fichier *test.txt*) et quelles sont les modifications apportées en les marquant d'un astérisque (*).



7 Conclusion

Tripwire constitue un des premiers éléments de protection passive pour une station ou un serveur. Il n'est qu'une petite partie d'un processus de sécurisation, et doit être utilisé avec d'autres logiciels permettant de mettre en œuvre une protection plus importante.

Sa mise en place et son fonctionnement sont simples, et son mode de fonctionnement de type une règle par fichier, permet de cibler exactement les besoins. Sa configuration s'adresse à des utilisateurs ayant connaissance des principes de fonctionnement d'un système UNIX, au moins pour le choix des règles de sécurité.