THIERRY MEYER
SÉCURITÉ INFORMATIQUE

LA CRYPTOGRAPHIE APPLIQUÉE AUX SYSTÈMES ET RÉSEAUX
Travaux pratiques : lab n°1 – ½ journée

Le contrôle d'intégrité d'un système de fichiers
Installation et configuration du HIDS sur un serveur web Linux Debian

1 Aperçu du lab :

A travers ce TP vous allez effectuer une partie de la sécurisation d'un serveur Linux Debian, en mettant en œuvre des mécanismes de contrôle d'intégrité de son système de fichiers. Pour cela vous utiliserez l'Host Based Intrusion Detection System (HIDS) Aide[1].

Vous serez amené à installer et configurer cet outil afin de remonter des alertes en cas de modification inattendue des fichiers systèmes sous « surveillance ». Dans la dernière partie du TP vous aurez l'occasion de mettre en œuvre les méthodes qui vous permettront de pérenniser votre installation, en réfléchissant aux bonnes pratiques et en rédigeant la procédure à suivre en cas de mise à jour du système.

Pour réaliser toutes les tâches qui vous sont demandées par la suite, vous travaillerez en binôme et disposerez d'un serveur Linux Debian virtualisé sur lequel Apache sera installé pour faire tourner un blog Wordpress.

Vous travaillerez de façon totalement autonome, vous devrez donc consulter toute la documentation **officielle[2] (et uniquement)** à votre disposition pour comprendre les options que vous utiliserez et les décrire. Pensez comme toujours à bien documenter vos manipulations.

Vous avez le temps de faire toutes les manipulations dans le temps imparti.

2 Objectifs du lab :

Le premier objectif de ce lab est de vous faire découvrir une application concrète de la cryptographie sur les systèmes, à savoir le Contrôle d'intégrité. Il présente également l'intérêt de compléter par la pratique les notions théoriques abordées en cours.

C'est également l'occasion pour vous de découvrir l'HIDS `Aide`, qui est un outil relativement léger et simple mais particulièrement efficace si employé correctement. Avec ce premier contact il vous sera alors plus facile de prendre en main d'autres solutions et notamment `tripwire`[3] dont la syntaxe des fichiers de configuration est relativement proche.

Le dernier objectif de ce lab est de vous faire réfléchir aux moyens de pérenniser votre installation en préparant des procédures à suivre en cas de modifications prévues du système. Ce travail peut prendre du temps la première fois, mais s'il est effectué correctement, il vous permettra d'en gagner lorsque vous devrez modifier votre système par la suite.

1 http://sourceforge.net/projects/aide/

2 man aide, man aide.conf et http://www.cs.tut.fi/~rammer/aide/manual.html

3 http://www.tripwire.org/

3 Les consignes :

3.1 Découverte de l'outil

3.1.1 Installation de Aide :

Le projet `Aide` se trouve dans les dépôts officiels de Debian, vous pourrez donc l'installer simplement en tapant la commande suivante :

```
apt-get install aide
```

3.1.2 Rappels théoriques sur la détection d'intrusion :

- Expliquez ce qu'est un HIDS. En quoi est-ce différent d'un IDS classique ?
- `Aide` utilise les techniques de contrôle d'intégrité sur le système de fichiers sous surveillance. Expliquez comment la cryptographie permet cela. Quels sont les mécanismes et algorithmes cryptographiques qui interviennent lors du contrôle d'intégrité.

3.1.3 Découverte de aide :

`Aide` dispose de deux fichiers de configuration:

- `/etc/aide/aide.conf` et,
- `/etc/aide/aide.conf.d`.

Les commandes `man aide` et `man aide.conf` ainsi que la page web http://aide.sourceforge.net/stable/manual.html, constituent les principales sources de documentation du projet. Elles sont suffisamment explicites et vous donneront tous les détails sur la façon d'utiliser et configurer `aide`.

Après avoir consulté la documentation, expliquez le fonctionnement de `Aide`.

3.2 Configuration de l'outil

3.2.1 Préparation du fichier de configuration :

La configuration par défaut de `Aide` est adaptée à la plupart des systèmes. Consultez le fichier `aide.conf` et expliquez quels sont les fichiers surveillés ainsi que les attributs sous surveillance.

Lorsque vous avez saisi le fonctionnement de ce fichier, vous pouvez passer à l'étape suivante : l'exécution de l'HIDS

- générez votre première base de données,
- forcez l'exécution du contrôle d'intégrité de `Aide` en précisant l'option `-check`. Vérifiez que celui-ci s'exécute correctement.
- si tout se passe comme vous le souhaitez repérez le `PID`, puis stoppez le processus.
- Vous allez maintenant tester le bon fonctionnement de votre nouvelle protection :
  - Modifiez un des fichiers sous surveillance.
  - Reproduisez la manipulation.

Que constatez-vous ? Expliquez en détail **toutes** vos manipulations.

3.2.2 Personnalisation de la configuration :

Si tout s'est passé correctement à l'étape précédente, vous allez pouvoir maintenant passer à une utilisation

concrète de votre HIDS : la surveillance de votre blog.

- Vérifiez le bon fonctionnement du service nouvellement installé et modifiez la configuration de `Aide` pour correspondre à votre nouveau besoin de sécurité. L'objectif ici est de vérifier que les fichiers sources de votre blog ne sont pas modifiés, hormis les seuls répertoires en écriture pour l'utilisateur internet.
- Effectuez un nouveau test d'intégrité.
- Expliquez en détail vos modifications et justifiez vos choix.

3.3 Renforcement de la sécurité de l'HIDS : utilisation de la cryptographie pour signer la base de données.

Comme vous le savez, il peut arriver que la mise en œuvre d'une mesure de sécurité génère une nouvelle faille dans votre système. Aussi vous devez prendre toutes les mesures nécessaires pour que votre nouveau système de protection ne devienne pas une nouvelle vulnérabilité.

Outre les mesures classiques (mises à jour de sécurité, …), il est important de garantir la fiabilité des résultats obtenus par le contrôle d'intégrité, par conséquent il est primordial de s'assurer que la base de données de référence ne soit pas corrompue.

Pour cela `Aide` permet de signer la base de données et le fichier de configuration. On peut alors forcer le processus `Aide` à contrôler la signature de la base avant le contrôle et refuser toute base de données ayant une signature invalide.

Vous allez donc maintenant mettre en œuvre ces mécanismes :

- générez une nouvelle base de données,
- signez la base de données et le fichier de configuration,
- configurez `Aide` pour qu'il vérifie les signatures avant de s'exécuter.
- Expliquez en détail vos manipulations et justifiez vos choix.

Quelle autre mesure indispensable prendriez-vous par exemple pour vous assurer que la base de données ne soit pas altérée ?

3.4 Automatisation des tâches :

Maintenant que tout fonctionne comme vous le souhaitez, vous allez faire en sorte d'automatiser les vérifications de votre blog par `Aide`. Pour cela créez une nouvelle tâche `CRON`, celle-ci devra exécuter `Aide` (en forçant le contrôle de la signature de la base).

Expliquez en détails vos manipulations.

Dans quels cas ces contrôles d'intégrité pourraient présenter des faux positifs ? Rédigez alors une procédure simple permettant de prévenir ces faux positifs.

4 Les livrables :

A l’issue de ce TP, vous devrez me présenter vos résultats, et prouvez le bon fonctionnement de vos travaux. Votre présentation devra contenir également les réponses aux éventuelles questions théoriques posées.

La note tiendra compte de vos résultats, l’implication de votre équipe sur le lab, ainsi que la clarté de vos explications.