SÉCURITÉ DES SYSTEMES ET RÉSEAUX
(B3)
Projet sécurité systèmes et réseaux : 40h

Renforcement de la sécurité d'une application web
Détection d'intrusion sur les sources d'un site internet

---

1 Aperçu du lab :

Un client, hébergeur de sites internet, vous a commandé une prestation de réalisation d'un utilitaire de sécurité pour protéger les sites de ses clients. Cet utilitaire, de type `HIDS`[1], doit permettre de lever des alertes en cas de détection de modifications des sources sur des sites internet sous surveillance.

Vous allez donc développer cet outil à l'aide du langage `Python` en respectant les consignes du cahier des charges de la partie 3.

Vous travaillerez de façon totalement autonome en groupe de 2 ou 3 **maximum**. Vous devrez donc consulter toute la documentation officielle à votre disposition pour comprendre les options que vous utiliserez et les décrire.

2 Objectifs du lab :

Ce projet a été réalisé avec en tête l'objectif suivant :

- Vous faire découvrir une autre application de la cryptographie :
  - le contrôle d'intégrité d'un système de fichiers, en réalisant un outil de détection d'intrusions de type `HIDS`,

1 *Host Based Intrusion Detection System*

3 Les consignes :

3.1 Conception d'un outil de détection d'intrusions :

3.1.1 Rappels théoriques sur le contrôle d'intégrité :

Les fonctions de hachage permettent de créer des empreintes numériques de longueur fixe supposées représentatives de la donnée initiale. Compte tenu de cette propriété, cette technique est très souvent utilisée pour vérifier l'intégrité d'un système de fichiers de la façon suivante :

1. l'empreinte de chaque fichier est calculée puis stockée en lieu sûr, c'est à dire sur un support non modifiable. Dans l'idéal sur un support placé ensuite en lecture seule,
2. à intervalle régulier, les empreintes de chaque fichiers sont recalculées et comparées aux empreintes qui ont été calculées initialement et conservées dans la base de référence. Si une empreinte ne correspond pas, c'est que le fichier en question a été modifié, une alerte est alors émise.

Afin que cette mesure soit efficace, il est primordial de respecter quelques règles parmi lesquelles :

- utiliser un algorithme de hachage suffisamment robuste, c'est à dire qui présente peu de collisions, mais pas trop consommateur de ressources[2],
- stocker la base d'empreintes dans un endroit sûr, afin de garantir son intégrité. Elle pourra être signée pour plus de sécurité. Un hash pourra être calculé à chaque fois qu'elle sera générée.

Ce type d'outil est communément appelé `Host Based Detection Intrusion System (HIDS)`

3.1.2 Fonctionnalités de l'HIDS :

Afin de protéger les applications web de vos clients, vous allez développer un utilitaire de ce type. Pour développer votre HIDS, vous utiliserez le langage de programmation Python, ainsi que les différents langages nécessaires à la conception d'une interface graphique web (HTML, CSS, Javascript, …)

Votre solution devra impérativement respecter les règles suivantes :

- elle fonctionnera de la façon suivante :
  - Votre HIDS pourra se lancer automatiquement à intervalle régulier, lorsque le site distant le permettra, ou
  - Recevoir automatiquement les résultats d'une analyse déclenchée automatiquement sur un site, via une tâche `CRON`.

  Attention, afin d'éviter qu'un acteur malveillant ne puisse forger des requêtes à destination de votre outil, vous devrez mettre en œuvre un mécanisme qui garantira l'identité du site avec lequel votre outil est en contact.

- votre `HIDS` devra disposer d'un fichier ou d'une interface de configuration, qui permettra de choisir les fichiers et répertoires à inclure ou a exclure de l'analyse. Il sera également possible de configurer l'intervalle de temps entre deux analyses. Ce fichier de configuration permettra de surveiller tout type de site, et notamment ceux développés avec les CMS courants. (Wordpress, Joomla, Prestashop, ...)

- En cas de détection d'activité malveillante, c'est à dire modification, suppression ou ajout d'un fichier dans les sources du site, il devra pouvoir envoyer une alerte détaillée de l'incident par mail. Cette alerte vous permettra de réagir rapidement.

- Il devra également disposer d'une interface Web d'administration qui permettra entre autre :
  - d'afficher la liste des analyses effectuées par sites avec leurs rapports,
  - de forcer le lancement d'une analyse sur un ou plusieurs sites.

  Cette interface Web devra être accessible **uniquement** en `HTTPs`.

2 *Par exemple SHA1*

4 Les livrables :

A l'issue du projet, vous présenterez votre solution en soutenance. Vous devrez me remettre un rapport détaillé de votre travail, présentant notamment les fonctionnalité de votre outil. Ce rapport devra être correctement rédigé et remis au moins une semaine avant la date de la soutenance.

Pour chacun des points à traiter vous fournirez l'explication détaillée des manipulations que vous avez effectué (commandes et résultats). Vous joindrez les résultats que vous avez obtenus, votre interprétation, ainsi que vos éventuelles remarques et constats. N'hésitez pas également à indiquer vos interrogations sur des résultats.

Pour finir, la note tiendra compte de votre analyse et de la qualité de la rédaction.