SÉCURITÉ DES SYSTEMES ET RÉSEAUX

**Renforcement de la sécurité d'une application web**

I - Présentation du projet

II – Solution d’infrastructure

III – Solution de scripting

IV – Solution Web

Présentation du projet :

L’objectif du projet est de sécurisé des sites internet appartenant à des clients et ce via un utilitaire de type HIDS. Cette utilitaire permettra de lever des alertes en cas de détection de modifications des sources sur les sites internet mis sous surveillance.

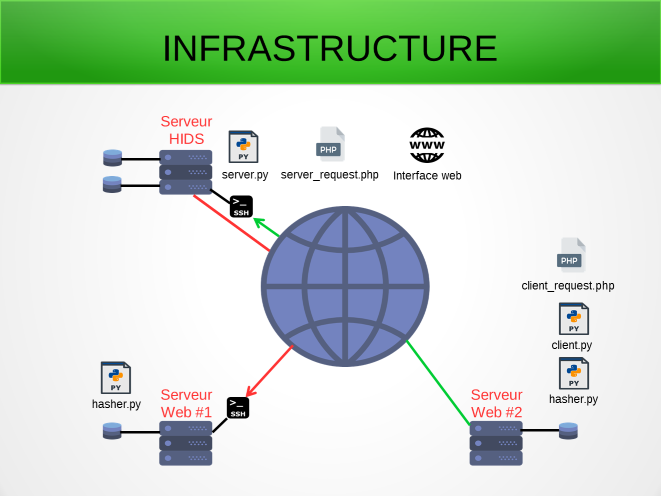
Afin d’atteindre l’objectif du projet nous avons mis en place des solutions adaptées aux besoin définis dans ce dernier.

Voici un bref résumé des solutions mise en place, nous entrerons dans les détails dans la suite de la présentation.

Ainsi nous avons :

* Trois machines virtuelles tournant sous l’OS Debian 9 et virtualisé sur Virtual Box, ces trois VM joueront respectivement le rôle du serveur HIDS et des deux serveurs Web.
* Trois script Python qui gèreront les requêtes du serveurs et des clients et permettront de hasché les fichiers sources des sites.
* Deux scripte PHP qui permettront de récupéré les requêtes des serveur Web et lancer les scripte Python (et ??)
* Une interface Web qui permettra d’accédé a un certain nombre de données concernant les sites surveillés et également de lancer des analyses manuellement.

Voici la conception de notre projet de manière schématique :



II - Solution d’infrastructure

Le serveur HIDS :

Notre serveur HIDS est une machine tournant sous l’OS Debian 9, elle sera le point central du projet et sera en relation avec tout les autres serveurs Web.

Deux base de données sont implémenté (?) sur le serveur, la base de données des sites et la base de données des requêtes.

On y trouvera également le script Python server.py et le script PHP server\_request.php.

L’interface web d’administration sera également accessible depuis le serveur HIDS et uniquement depuis ce dernier ( ?).

Sur le serveur HIDS sont installer les rôles suivants :

* Apache
* SSH
* ? ? ?

? ? ?

III – Solution Web

Afin de pouvoir administrer les sites sous surveillance de manière sécurisé et pratique nous avons mis en place une interface Web qui nous permettra d’avoir un visu direct sur un grand nombre de données.

L’accès a l’interface Web se fera par une connexion sécurisée avec des identifiants/mot de passe.

L’interface Web permettra également d’accéder aux sites analysés et aux logs des analyses.

Il sera également possible de lancer manuellement des analyses depuis l’interface Web.

IV – Solution de scripting

Notre solution comporte plusieurs scriptes qui ont chacun leur utilité.

On distinguera deux types de scriptes, les scriptes Python et les scriptes PHP.

**hasher.py :**

Le scripte hasher.py analyse le fichier CSV permettant de générer les empreintes. Il génère également un fichier CSV d’empreintes et permet d’envoyer son état au serveur HIDS via le script request\_server.php.

**server.py :**

Le scripte permet de se connecter en SSH aux différents serveur Web qui sont sous surveillance et de copier des fichiers sur ces serveurs.

Le scripte se lance au démarrage du serveur et fonctionne en arrière-plan. Il consulte et analyse la base de données des requêtes et des sites. Il peut également consulter et modifier la base de données des empreintes.

Les requêtes sont envoyées via le client\_request.php .

**client.py :**

Ce script permet d’envoyer les fichier d’empreinte via le protocole SCP qui est le protocole utilisé pour les transferts sécurisé.

Ce script servira également a définir des taches CRON.

**client\_request.php :**

Ce script PHP permet d’analyser les demande de l’HIDS. Il permet également de lancer le script client.py et le script hasher.py

**server\_request.php :**

Ce script récupère les requêtes des serveurs web et ajoute les requêtes à la base de données des requêtes.