AIST 21 – Compte-rendu hebdomadaire

Compte-rendu Lundi 18/03/2024

En ce début de semaine, j'ai réalisé une configuration **SSL/TLS** pour le serveur **Zulip** en déployant des certificats autosignés. Après avoir généré les certificats et déplacé les fichiers **ca.crt**, **ca.key**, **zulip.crt**, **zulip.csr**, et **zulip.key** dans les répertoires **/etc/ssl/certs/** et **/etc/ssl/private/** respectivement, j'ai tenté d'intégrer ces certificats dans la configuration de **Nginx**. Cependant, une erreur est survenue lors de la tentative d'ajout de la **phrase secrète** à la configuration de **Zulip**. Pour résoudre ce problème, j'ai opté pour une approche différente en déchiffrant la **clé privée** chiffrée à l'aide d'**OpenSSL**, puis en l'incorporant dans la configuration de **Nginx**. Cette méthode a évité l'utilisation de la phrase secrète dans la configuration **Nginx**, garantissant ainsi le bon fonctionnement du serveur **Zulip** avec des connexions **HTTPS** sécurisées.

J'ai donc choisi d'utiliser **OpenSSL** pour les certificats au lieu de **Let's encrypt**, d'abord pour tester une autre façon de faire mais surtout avec **OpenSSL**, j'ai un contrôle absolu sur la génération et la gestion des certificats **SSL/TLS**, me permettant de personnaliser les paramètres selon les besoins. De plus, en utilisant **OpenSSL**, je ne dépends pas d'un service tiers comme **Let's Encrypt**, ce qui me donne une autonomie totale sur vos certificats et évite toute dépendance externe.

D'ailleurs, j'avais déjà pu faire cette manipulation-là en fin de semaine dernière pour notre serveur **Wazuh**.

Compte-rendu Mardi 19/03/2024 & Mercredi 20/03/2024 & Jeudi 21/03/2024

Durant ces trois jours, je me suis penché en détail sur les fonctionnalités de **Wazuh** : d'abord **VirusTotal**, il s'agit d'un service en ligne de **Google** qui permet l'analyse de fichiers suspects et facilite la détection rapide des virus, vers, chevaux de Troie et toutes sortes de logiciels malveillants détectés par les moteurs antivirus.

J'ai donc configuré le fichier **ossec.conf** du serveur **Wazuh** pour pouvoir utiliser ce service qui permet de remonter les alertes de virus ou logiciels malveillants dans **Wazuh**.

Ensuite, j'ai configuré et activé la surveillance de l'intégrité des fichiers dans le fichier **ossec.conf** et tester avec le fichier de test **Eicar** avec comme contenu une chaîne de caractères, écrite dans un fichier informatique, destiné à tester le bon fonctionnement des logiciels antivirus, notamment pour tester **VirusTotal**.

Compte-rendu Vendredi 22/03/2024

Aujourd'hui, j'ai documenté tout ce que j'ai pu mettre en place le jour précédent, j'ai surtout activé une option qui permet de détecter des vulnérabilités sur les hôtes supervisés par **Wazuh** (option dans **ossec.conf** désactivée par défaut par **Wazuh**). J'ai pu voir dès l'activation, des vulnérabilités sur un des hôtes de tests supervisée par **Wazuh.**

J'ai configuré le serveur **Wazuh** et les agents **Wazuh** avec **Whodata** qui permet de notifier qui a modifié tels ou tels fichiers système (par exemple un utilisateur faisant partie du groupe **sudoers** et qui modifier un fichier dans **/etc** grâce aux privilèges **sudo** et avec un tel éditeur (test réalisé sous **Linux**)).

J'ai testé aussi une petite configuration qui permet de détecter des manipulations des comptes : le répertoire **.ssh/authorized_keys** des distributions **Linux** est surveillé et lorsqu'une clé est ajoutée dans ce fichier, alors une notification est générée.

J'ai testé **Yara**, un outil similaire à **VirusTotal** qui permet de détecter si un fichier ou logiciel malveillant est installé, j'ai testé en configurant la surveillance sur le répertoire **/root** et j'ai testé en téléchargeant **Mirai** ou **Xbash** et une alerte est générée sur l'interface **Wazuh**.

Compte-rendu général de cette semaine :

Cette semaine a été axée sur l'amélioration de la sécurité et des fonctionnalités des hôtes surveillés par **Wazuh**.

J'ai mis en place avec succès un système **SSL/TLS** pour le serveur Zulip en utilisant des certificats autosignés avec **OpenSSL**, offrant ainsi un contrôle total sur la gestion des certificats.

Parallèlement, j'ai exploré les capacités de **Wazuh**, en configurant la détection de virus via **VirusTotal** et en activant la surveillance de l'intégrité des fichiers. Des mesures de détection de vulnérabilités et de modifications suspectes des fichiers système ont également été mises en place, renforçant ainsi la sécurité globale de nos systèmes.

Enfin, j'ai documenté toutes les configurations mises en œuvre, assurant ainsi une traçabilité et une compréhension claire des mesures de sécurité adoptées. Cette semaine a été marquée par des progrès significatifs dans la sécurisation de l'infrastructure de tests et dans l'optimisation de leurs fonctionnalités.