AIST 21 – Compte-rendu hebdomadaire

Compte-rendu Lundi 26/02/2024

Découverte du lieu du stage, remise d'un badge personnel pour toute la durée du stage pour accéder aux lieux interdits au public, (salle déjeuné, certains bureaux, etc.) et présentation des équipes (RH, télécommunication etc.)

Présentation des activités de la journée:

- Mise en place de l'outil **Wazuh**, une plateforme de gestion de la sécurité des informations et des événements (SIEM). Il a pour rôle d'assister à mieux gérer la sécurité des systèmes d'information.Il permet de détecter, de répondre et de prévenir les incidents de sécurité informatique.
- Création des agents compatibles en fonction du SE:
  - **wazuh-agent** : pour 2 VM **Linux** : **test1-wazuh** et la vm **guacamol** (agent créé depuis l'interface web de **Wazuh**).
  - Pour une VM **Windows10** : installation de l'agent depuis : Télécharger et configurer l'agents Wazuh sur les points de terminaison pour Windows

Source: IT-admin : Installer Wazuh sous Linux - Ubuntu

- Mise en place d'une solution **Guacamole** / **Téléporte** et configuration des clés **Yubikey** avec **Keepass** pour l'authentification.

Compte-rendu Mardi 27/02/2024

Reprise de réinstallation et de la configuration de **Wazuh**, ainsi que la rédaction de documentation concernant **Wazuh**, résolution de bug au niveau de l'installation de **VirtualBox** sur la machine physique.

A noter que **Wazuh** peut être installé et configuré sur une VM avec **Debian 12 Bookworm**, mais cela n'est pas recommandé d'âpres le site officiel, celui-ci à tendance à buguer et l'interface web ne s'affiche plus, même avec redémarrage de l'agent en ligne de commande.

Réinstallation alors de **Wazuh** sur **Ubuntu 22.04 Live Server TSL**.

Remontée de deux hôtes dans **Wazuh** avec la génération d'un agent « client » depuis l'interface de **Wazuh**.

Compte-rendu Mercredi 28/02/2024

Le bug de **VirtualBox** s'est répété avec la même erreur concernant le démarrage d'une machine virtuelle : **"VirtualBox – Erreur dans supR3HardenedWiReSpawn"** et après avoir cliqué sur **OK**, une autre erreur apparaît indiquant **"Échec de l'ouverture d'une session pour le virtuel".**

Je l'ai corrigé avec :
CORRECTIF : Erreur VirtualBox dans supR3HardenedWiReSpawn – Erreur lors de la relance du processus 5 de la VM VirtualBox (résolu)

J'ai ajouté de nouvelles fonctionnalités dans **Wazuh**, notamment la gestion des alertes avec **Slack** (Formation WAZUH : Comment envoyer des alertes sur Slack avec Wazuh (Vidéo) - Alphorm), la gestions des logs avec **syslogs**.

D'ailleurs **Wazuh** peut être déployer sous **Docker** ou sur **Kubernets,** ou automatique avec **Ansible,** ou encore sous **Pfsense.**

Source : Administration du serveur Wazuh

AIST 21 – Compte-rendu hebdomadaire

Compte-rendu Jeudi 29/02/2024

Toujours sur le serveur **Wazuh**, j'ai assuré la gestion des agents, en créant des groupes.

Source : Formation WAZUH : Comment gérer des groupes d'agents Wazuh (Vidéo) - Alphorm

Actualisation et mise à jour du portefiolio.

Compte-rendu Vendredi 01/03/2024

Toujours sur le serveur **Wazuh**, j'ai essayé de configurer une règles qui permet de détecter l'exécution de **PowerShell** sur les postes Windows.

Source : Formation WAZUH : Comment détecter l'exécution de PowerShell avec les règles Wazuh (Vidéo) – Alphorm

Compte-rendu général de cette semaine :

Cette semaine a été consacrée à des activités diverses dans le cadre du stage, principalement axées sur la mise en place et la configuration de l'outil de gestion de la sécurité des informations et des événements (SIEM) appelé **Wazuh**.

Les tâches ont inclus la découverte du lieu de stage et l'attribution de badges personnels pour accéder aux zones restreintes, la présentation des équipes et des activités prévues.

Parmi les activités hebdomadaires, la configuration de **Wazuh** sur différents systèmes d'exploitation tels que **Linux** et **Windows** a été une priorité, suivie de la création d'agents compatibles.

Des solutions complémentaires, comme l'authentification via les clés **Yubikey** et **Keepass** avec **Guacamole** / **Téléporte**, ont également été mises en place.

En parallèle, des efforts ont été déployés pour résoudre les problèmes techniques rencontrés, tels que des bugs lors de l'installation de **VirtualBox** et des erreurs spécifiques à **Wazuh**, nécessitant des corrections et des recherches approfondies.

Des vidéos informatives de la chaîne YouTube Alphorm ont été suivies pour améliorer la compréhension et l'utilisation des fonctionnalités de **Wazuh**, notamment la gestion des alertes avec **Slack** et des logs avec **syslogs** ou encore **sysmon**.

Enfin, des travaux de documentation, d'actualisation et de mise à jour du **portfolio** ont complété les activités de la semaine, offrant ainsi une vue d'ensemble des progrès accomplis et des compétences acquises dans le domaine de la sécurité informatique et de la gestion des événements.