Installation de l'HIDS Wazuh

Présentation

Wazuh est un système open source de détection d'intrusion basé sur l'hôte (**HIDS**). Il offre une variété de fonctionnalités pour renforcer la sécurité et la surveillance des systèmes.

Wazuh HIDS

Wazuh est un système de détection d'intrusion qui s'exécute au niveau de l'hôte (sur chaque machine) et combine des technologies basées sur les anomalies et les signatures pour détecter les intrusions ou les abus de logiciels.

Fonctionnalités

- **Analyse des journaux : Wazuh** surveille les journaux système, les journaux d'application et les journaux de sécurité pour détecter les activités suspectes.
- **Surveillance de l'intégrité des fichiers :** Il vérifie si les fichiers système ont été modifiés de manière inattendue.
- **Détection des rootkits et des vulnérabilités : Wazuh** identifie les **rootkits** et les vulnérabilités connues.
- **Évaluation de la configuration système :** Il surveille les paramètres de configuration pour détecter les anomalies.
- **Utilisation : Wazuh** est couramment déployé avec la pile **Elastic** pour une analyse de sécurité plus approfondie.

Phases d'installation :

Wazuh s'installe en 3 temps :

W.indexer :
- L'**indexeur Wazuh** est un moteur de recherche en texte intégral hautement évolutif. Il gère l'indexation des données et fournit des fonctionnalités avancées telles que l'alerte, la gestion des index et l'analyse des performances.

W.server :
- Le **serveur Wazuh** collecte, analyse et stocke les données provenant des agents **Wazuh**. Il est essentiel pour le fonctionnement du système.

W.dashboard :
- Le **tableau de bord Wazuh** est une interface Web permettant de visualiser les alertes du serveur **Wazuh** et les événements archivés.

Source pour la procédure d'installation : IT-admin : Installer **Wazuh** sous Linux Debian - Ubuntu

Recommandations pour les tests, (à ajuster en fonction des besoins) pour la mise en place dans une entreprise :

→ Ubuntu 22.04.4 Live Server TLS
→ 4 Go de RAM (au moins)
→ 2 cœurs (au moins)
→ 25 Go d'espace disque (au moins)

NOTE : Il existe une **OVA** téléchargeable sur le site de **Wazuh** préconfigurée.

Pour gérer les groupes d'agents :

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

Pour configurer les notifications avec Slack :

Source : Formation **WAZUH** : Comment envoyer des alertes sur Slack avec **Wazuh** (Vidéo) - Alphorm