Installation de Wazuh

NOM: KOUASSI

PRENOM: GLOHNDY

ETABLISSEMENT: ORT TOULOUSE

Travaux Pratiques : Installation de Wazuh

1. Introduction

Wazuh est une plateforme open-source de gestion des informations et événements de sécurité (SIEM). Elle permet :

Détection des menaces

La détection des menaces et la réponse aux incidents.

Surveillance FIM

La surveillance de l’ intégrité des fichiers (FIM).

Visibilité complète

Une visibilité complète sur l’ infrastructure informatique.

Ce TP a pour objectif de mettre en place un environnement Wazuh complet sur un système Debian 64 bits, comprenant le serveur, l’ indexeur et le tableau de bord.

2. Présentation de Wazuh

2.1 Les composants de Wazuh

Wazuh Server

Analyse les données collectées par les agents et génère les alertes.

Wazuh Indexer

Stocke et indexe les logs pour la recherche et la corrélation (basé sur Elasticsearch/OpenSearch).

Wazuh Agent

Collecte les événements sur chaque machine (Windows, Linux, macOS).

Wazuh Dashboard

Interface graphique (basée sur Kibana) pour visualiser et gérer les alertes.

3. Installation de Wazuh

3.1 Pré-requis

Avant de commencer, assurez-vous d'avoir :

- Un système Debian 64 bits (ou Ubuntu équivalent),
- Un accès root / sudo,
- Les paquets `curl` et `gpg` installés.

> 💡 **Si curl n'est pas disponible :**
>
> ```
> sudo apt install curl gpg
> ```

3.2 Étape 1 : Ajouter la clé GPG

```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg
```

Explication :

- `curl -s` : télécharge silencieusement la clé GPG depuis le dépôt Wazuh.
- `gpg --import` : importe la clé dans le trousseau.
- `chmod 644` : ajuste les permissions pour lecture système.

3.3 Étape 2 : Ajouter le dépôt Wazuh

```
echo "deb \[signed-by=/usr/share/keyrings/wazuh.gpg\] https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list
```

Explication :

- Ajoute le dépôt officiel de Wazuh dans la liste des sources APT.
- `signed-by` sécurise la signature avec la clé importée.

3.4 Étape 3 : Mettre à jour et installer les dépendances

```
sudo apt update && sudo apt upgrade && sudo apt-get install debconf adduser procps curl gnupg apt-transport-https filebeat debhelper libcap2-bin
```

Explication :

- `apt update` : met à jour la liste des paquets.
- `apt upgrade` : applique les dernières mises à jour.
- La commande installe plusieurs outils nécessaires à Wazuh.

3.5 Étape 4 : Télécharger les scripts de configuration

```
curl -sO https://packages.wazuh.com/4.8/wazuh-certs-tool.sh
curl -sO https://packages.wazuh.com/4.8/config.yml
```

Explication :

- Télécharge deux fichiers :
- `wazuh-certs-tool.sh` : script pour générer les certificats SSL.
- `config.yml` : fichier de configuration contenant les IP et noms des nœuds.

3.6 Étape 5 : Modifier config.yml

```
nano config.yml
```

Explication :

- Ouvre le fichier dans l'éditeur `nano`.
- Remplace les IP du serveur, de l'indexeur et du dashboard par l'adresse de ta machine (mode single node).

3.7 Étape 6 : Générer les certificats

```
bash ./wazuh-certs-tool.sh -A
tar -cvf ./wazuh-certificates.tar -C ./wazuh-certificates/ .
rm -rf ./wazuh-certificates
```

Explication :

- Exécute le script de génération (`-A` = tous les certificats).
- Archive les certificats générés dans un fichier `.tar`.
- Supprime le dossier temporaire.

3. Installation de Wazuh (Suite)

3.8 Étape 7 : Installer les composants principaux

```
sudo apt install wazuh-indexer wazuh-manager wazuh-dashboard -y
```

Explication :

Installe les 3 paquets :

- `wazuh-indexer` (base de données Elasticsearch),
- `wazuh-manager` (serveur d'analyse),
- `wazuh-dashboard` (interface web).

3.9 Étape 8 : Configurer l'indexeur

```
nano /etc/wazuh-indexer/opensearch.yml
```

Modifier `network.host` avec l'adresse IP du serveur.

3.10 Étape 9 : Déployer les certificats de l'indexeur

```
NODE\_NAME=node-1
mkdir /etc/wazuh-indexer/certs
tar -xf ./wazuh-certificates.tar -C /etc/wazuh-indexer/certs/ ./$NODE\_NAME.pem ./$NODE\_NAME-key.pem
./admin.pem ./admin-key.pem ./root-ca.pem
mv -n /etc/wazuh-indexer/certs/$NODE\_NAME.pem /etc/wazuh-indexer/certs/indexer.pem
mv -n /etc/wazuh-indexer/certs/$NODE\_NAME-key.pem /etc/wazuh-indexer/certs/indexer-key.pem
chmod 500 /etc/wazuh-indexer/certs
chmod 400 /etc/wazuh-indexer/certs/\*
chown -R wazuh-indexer:wazuh-indexer /etc/wazuh-indexer/certs
```

Explication :

- Crée le répertoire des certificats.
- Extrait et renomme les fichiers SSL pour l'indexeur.
- Ajuste les permissions pour sécuriser les fichiers.

3.11 Étape 10 : Démarrer wazuh-indexer

```
sudo systemctl daemon-reload
sudo systemctl enable wazuh-indexer
sudo systemctl start wazuh-indexer
```

Explication :

- Recharge les services, active et démarre le service au démarrage.

3.12 Étape 11 : Initialiser et tester le cluster

```
/usr/share/wazuh-indexer/bin/indexer-security-init.sh
sudo curl -k -u admin:admin https://:9200
curl -k -u admin:admin https://:9200/\_cat/nodes?v
```

Explication :

- Initialise la sécurité de l'indexeur.
- Vérifie la connectivité avec `curl` en utilisant les identifiants par défaut.

3. Installation de Wazuh (Suite)

3.13 Étape 12 : Installer et configurer le Wazuh Manager

```
sudo systemctl daemon-reload
sudo systemctl enable wazuh-manager
sudo systemctl start wazuh-manager
sudo systemctl status wazuh-manager
```

Explication :

- `daemon-reload` : recharge la configuration systemd pour que les nouveaux services soient reconnus.
- `enable` : active le démarrage automatique du service au boot.
- `start` : démarre le service Wazuh Manager.
- `status` : vérifie que le service est actif et fonctionne correctement.

Configuration de Filebeat et des Certificats

3.14 Étape 13 : Installer et configurer Filebeat

```
apt install filebeat
curl -so /etc/filebeat/filebeat.yml https://packages.wazuh.com/4.8/tpl/wazuh/filebeat/filebeat.yml
nano /etc/filebeat/filebeat.yml
```

Explication :

- `apt install filebeat` : installe Filebeat, outil pour transférer les logs vers l'indexeur.
- `curl -so` : télécharge le fichier de configuration spécifique à Wazuh.
- `nano` : ouvre le fichier pour remplacer l'adresse IP localhost par celle de l'indexeur.

3.15 Étape 14 : Créer le keystore et ajouter les identifiants

```
filebeat keystore create
echo admin | filebeat keystore add username --stdin --force
echo admin | filebeat keystore add password --stdin --force
```

Explication :

- Crée un keystore sécurisé pour stocker les informations sensibles (login/mot de passe).
- `echo | filebeat keystore add` : ajoute le nom d'utilisateur et le mot de passe par défaut (`admin`) dans le keystore.

3.16 Étape 15 : Télécharger le template d'alertes pour Wazuh Indexer

```
curl -so /etc/filebeat/wazuh-template.json
https://raw.githubusercontent.com/wazuh/wazuh/v4.8.2/extensions/elasticsearch/7.x/wazuh-template.json
chmod go+r /etc/filebeat/wazuh-template.json
```

Explication :

- Télécharge le template JSON pour Wazuh, utilisé par Filebeat et l'indexeur.
- `chmod go+r` : donne les permissions de lecture pour le groupe et les autres utilisateurs.

3.17 Étape 16 : Installer le module Wazuh pour Filebeat

```
curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-0.4.tar.gz | tar -xvz -C /usr/share/filebeat/module
```

Explication :

- Télécharge et extrait le module Wazuh pour Filebeat dans le répertoire des modules.
- Permet à Filebeat de comprendre les logs Wazuh et de les transférer correctement vers l'indexeur.

3.18 Étape 17 : Déployer les certificats pour Filebeat

```
NODE\_NAME=wazuh-1
mkdir /etc/filebeat/certs
tar -xf ./wazuh-certificates.tar -C /etc/filebeat/certs/ ./$NODE\_NAME.pem ./$NODE\_NAME-key.pem ./root-
ca.pem
mv -n /etc/filebeat/certs/$NODE\_NAME.pem /etc/filebeat/certs/filebeat.pem
mv -n /etc/filebeat/certs/$NODE\_NAME-key.pem /etc/filebeat/certs/filebeat-key.pem
chmod 500 /etc/filebeat/certs
chmod 400 /etc/filebeat/certs/\*
chown -R root:root /etc/filebeat/certs
```

Explication :

- Crée le dossier pour les certificats Filebeat.
- Extrait les certificats nécessaires et les renomme pour Filebeat.
- Ajuste les permissions et la propriété pour sécuriser les fichiers.

3.19 Étape 18 : Démarrer et vérifier Filebeat

```
sudo systemctl daemon-reload
sudo systemctl enable filebeat
sudo systemctl start filebeat
filebeat test output
```

Explication :

- Redémarre et active Filebeat comme service.
- `filebeat test output` : vérifie que Filebeat peut se connecter à l'indexeur et transmettre les logs correctement.

Configuration et Démarrage du Dashboard

3.20 Étape 19 : Configurer le Wazuh Dashboard

```
nano /etc/wazuh-dashboard/opensearch\_dashboards.yml
```

Explication :

- Ouvre le fichier de configuration du dashboard.
- Remplace l'adresse IP de `opensearch.hosts` par l'adresse de ton indexeur.

3.21 Étape 20 : Déployer les certificats du Dashboard

```
NODE\_NAME=dashboard
mkdir /etc/wazuh-dashboard/certs
tar -xf ./wazuh-certificates.tar -C /etc/wazuh-dashboard/certs/ ./$NODE\_NAME.pem ./$NODE\_NAME-key.pem
./root-ca.pem
mv -n /etc/wazuh-dashboard/certs/$NODE\_NAME.pem /etc/wazuh-dashboard/certs/dashboard.pem
mv -n /etc/wazuh-dashboard/certs/$NODE\_NAME-key.pem /etc/wazuh-dashboard/certs/dashboard-key.pem
chmod 500 /etc/wazuh-dashboard/certs
chmod 400 /etc/wazuh-dashboard/certs/\*
chown -R wazuh-dashboard:wazuh-dashboard /etc/wazuh-dashboard/certs
```

Explication :

- Même principe que pour Filebeat : création du dossier, extraction des certificats et sécurisation.

3.22 Étape 21 : Démarrer et vérifier le Dashboard

```
sudo systemctl daemon-reload
sudo systemctl enable wazuh-dashboard
sudo systemctl start wazuh-dashboard
sudo systemctl status wazuh-dashboard
sudo systemctl status wazuh-manager
sudo systemctl status wazuh-indexer
```

Explication :

- Recharge systemd et active le dashboard.
- Vérifie que tous les services essentiels (dashboard, manager, indexer) sont actifs et fonctionnels.

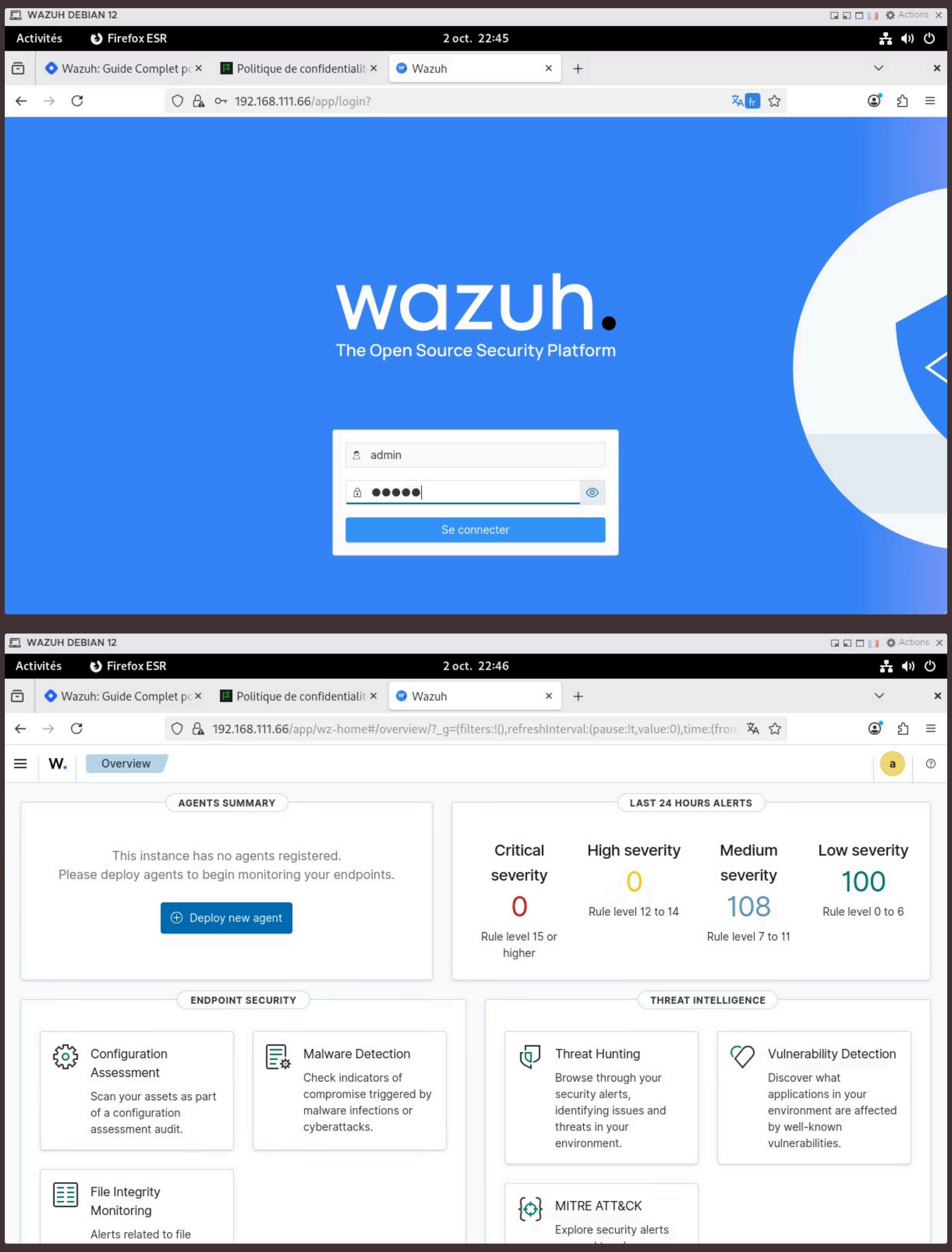
Accès et Conclusion

4. Accès à l’ interface Wazuh

Ouvrir un navigateur et se connecter à :

> https://<IP_DU_SERVEUR>:5601

Authentification : `admin/admin` (par défaut).



Interface prête pour gérer et visualiser les alertes.

5. Conclusion

L’ installation complète du serveur Wazuh, indexeur, Filebeat et dashboard est terminée.

Sécurité SSL

Les certificats SSL sont en place pour sécuriser les communications.

Prêt à l'emploi

Le serveur est prêt à recevoir des agents et à centraliser les logs.

Prochaine étape : déployer les agents sur les machines clientes et configurer le FIM.