Rapport

System Information Event and Management

Déploiement d'une Plateforme SIEM Open Source avec Wazuh et Simulation d'Attaques Réelles

Students :
Simon Lignac
Hugo Dubouchet
Jokebelle Coulibaly

Professeur :
Patrick Hebrard

Promotion 2027 Aéro 4
Vendredi 4 mars 2026
Année 2025–2026

Sommaire

Chapter 1

Introduction

Dans un contexte où les infrastructures informatiques sont de plus en plus connectées et exposées à Internet, les entreprises doivent faire face à une augmentation constante des cyberattaques. Prenons l'exemple d'une entreprise disposant d'un serveur accessible à distance afin de permettre à ses employés de travailler via le protocole RDP. Ce type d'accès, bien que pratique pour l'administration et le télétravail, constitue également une cible privilégiée pour les attaquants. Un individu malveillant peut, par exemple, commencer par scanner le réseau afin d'identifier les services actifs sur la machine. Une fois le port RDP détecté, l'attaquant peut tenter de réaliser une attaque par force brute afin de deviner les identifiants d'accès.

Sans système de supervision adapté, ces tentatives d'intrusion peuvent passer inaperçues pendant un certain temps.

Les plateformes de type SIEM (Security Information and Event Management) permettent de centraliser les journaux d'événements provenant de différentes machines et d'analyser ces données afin de détecter des comportements anormaux ou suspects.

Dans le cadre de ce projet, une plateforme SIEM basée sur la solution open source Wazuh a été déployée afin de superviser une infrastructure virtuelle composée de plusieurs machines. L'objectif est de simuler différentes attaques, telles qu'un scan de ports ou une tentative de brute force, et d'observer comment le système de supervision détecte ces activités malveillantes.

Chapter 2

Présentation de Wazuh

Wazuh est une plateforme open source de supervision et de détection d'intrusion. Elle permet de collecter et d'analyser les journaux de sécurité provenant de différents systèmes afin d'identifier les activités suspectes.

L'architecture de Wazuh repose sur plusieurs composants principaux :
-**Wazuh Manager** : serveur central qui analyse les logs et applique les règles de détection.
-**Wazuh Indexer** : base de données permettant de stocker et d'indexer les événements.
-**Wazuh Dashboard** : interface web permettant de visualiser les alertes et l'activité du système.
-**Agents Wazuh** : logiciels installés sur les machines surveillées pour envoyer les logs au serveur.

Cette architecture permet une supervision centralisée de l'infrastructure informatique et facilite l'identification des incidents de sécurité.

Chapter 3

Architecture du laboratoire

Afin de tester les capacités de détection du SIEM, une infrastructure virtuelle a été mise en place à l'aide de machines virtuelles. L'environnement comprend trois machines principales :
- Un serveur Ubuntu hébergeant la plateforme Wazuh.
- Une machine Windows 10 utilisée comme cible et équipée de l'agent Wazuh.
- Une machine Kali Linux utilisée pour simuler les attaques.

Le serveur Wazuh collecte les événements provenant de la machine Windows et les analyse afin de détecter des comportements suspects.

Une fois installé, le serveur est accessible via l'interface web Wazuh permettant d'observer l'activité des agents et les alertes de sécurité.

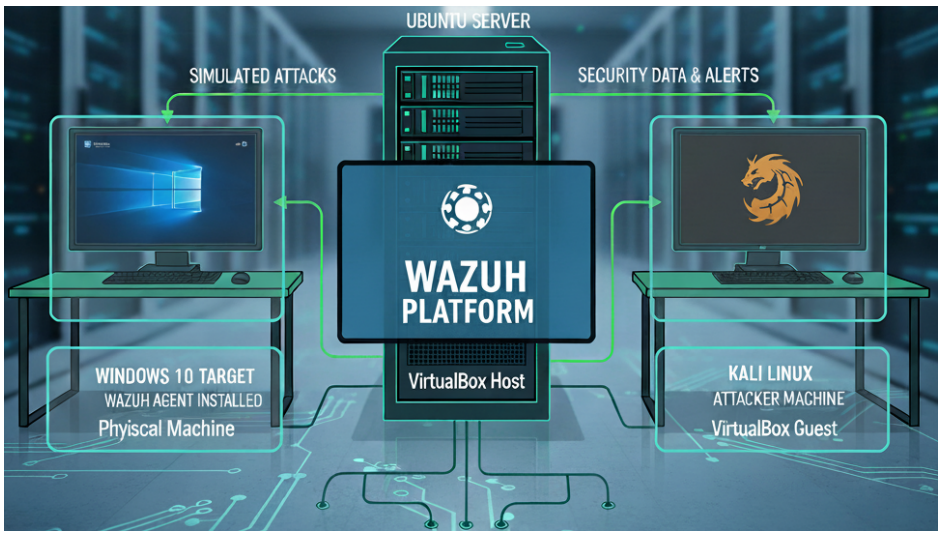

Figure 3.1: Schéma de notre architecture

Chapter 4

Mise en place de la plateforme

La première étape consiste à créer une machine virtuelle Ubuntu Server destinée à héberger la plateforme SIEM. Le serveur est configuré avec les caractéristiques suivantes :
- 4 Go de mémoire RAM
- 3 processeurs
- Ubuntu Server 64 bits

Une fois le système installé, plusieurs étapes de configuration sont réalisées :
Mise à jour du système avec la commande :

```
sudo apt update
sudo apt upgrade
```

-Installation du serveur SSH :

```
sudo apt install openssh-server
```

-Installation de Wazuh avec le script officiel :

```
curl -sO https://packages.wazuh.com/4.8/wazuh-install.sh
sudo bash wazuh-install.sh -a
```

Après l'installation, l'interface web Wazuh est accessible depuis un navigateur via l'adresse du serveur.
Un agent Wazuh est ensuite installé sur la machine Windows afin de transmettre les événements de sécurité au serveur. Une fois l'ensemble installé, l'activation de ssh et wazuh doit être effectuée.

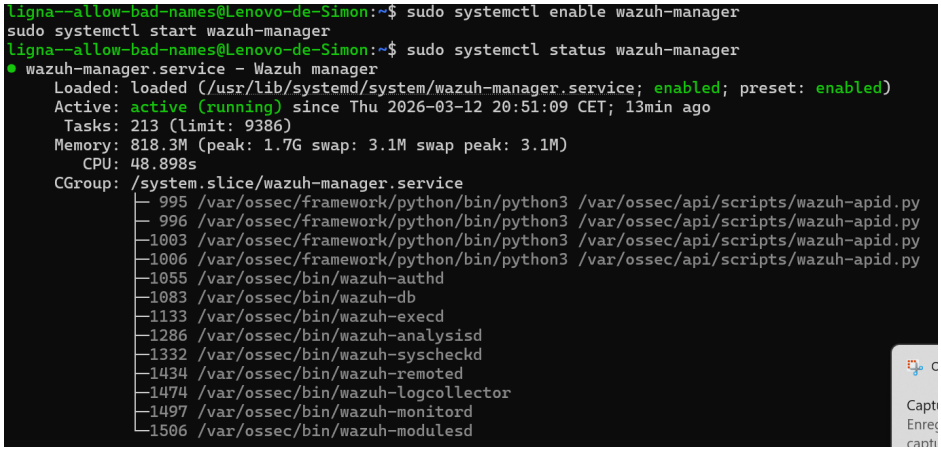

Figure 4.1: Wazuh est activé

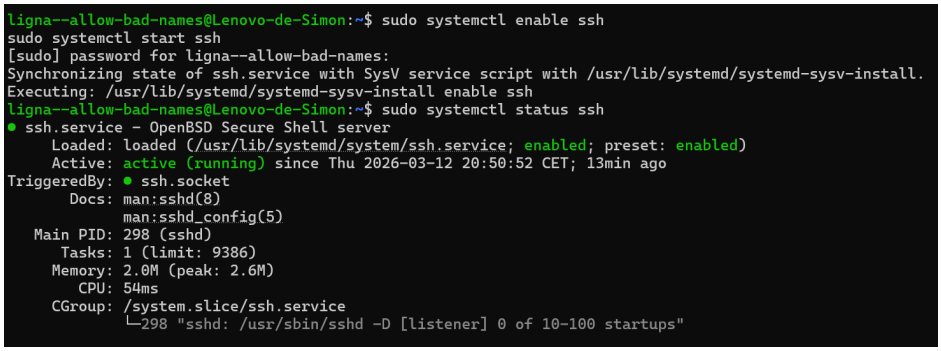

Figure 4.2: ssh est activé

Après l'installation et la configuration, l'interface web de Wazuh est accessible depuis un navigateur via l'adresse IP du serveur. L'agent Wazuh installé sur la machine WSL permet de collecter et d'envoyer les événements de sécurité au serveur.

Les captures d'écran montrent que les services `Wazuh` et `SSH` sont bien actifs. Cela confirme que la plateforme fonctionne correctement et que l'environnement est prêt pour la détection et l'analyse des attaques.

Chapter 5

Simulation d'attaques

Une fois l'infrastructure en place, plusieurs attaques sont simulées depuis la machine Kali Linux afin de tester les capacités de détection du SIEM.

5.1 Scan de ports

La première attaque consiste à effectuer un scan de ports à l'aide de l'outil **Nmap** :

```
nmap -sV 172.21.229.93
```

Cette commande permet d'identifier les services actifs sur la machine cible. Le scan révèle notamment l'ouverture du port 3389, utilisé pour le protocole RDP.
Le SIEM Wazuh détecte cette activité et enregistre les événements correspondants dans le tableau de bord.

5.2 Attaque par force brute

Une attaque par brute force est ensuite réalisée à l'aide de l'outil Hydra afin de tenter de deviner les identifiants d'accès au service RDP :

```
hydra -t 4 -V -L users.txt -P rockyou.txt rdp://172.21.229.93
```

Cette attaque génère un grand nombre de tentatives de connexion.

Le SIEM détecte alors plusieurs échecs d'authentification et génère une alerte indiquant une activité suspecte.

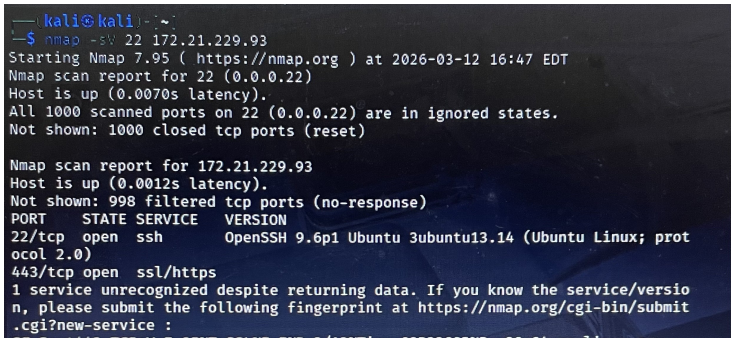

Figure 5.1: Utilisation de l'attaque Nmap

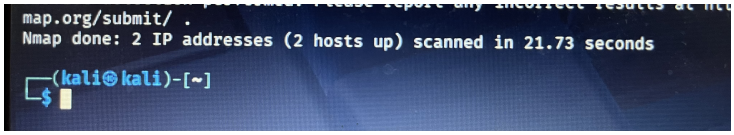

Figure 5.2: Nmap effectué

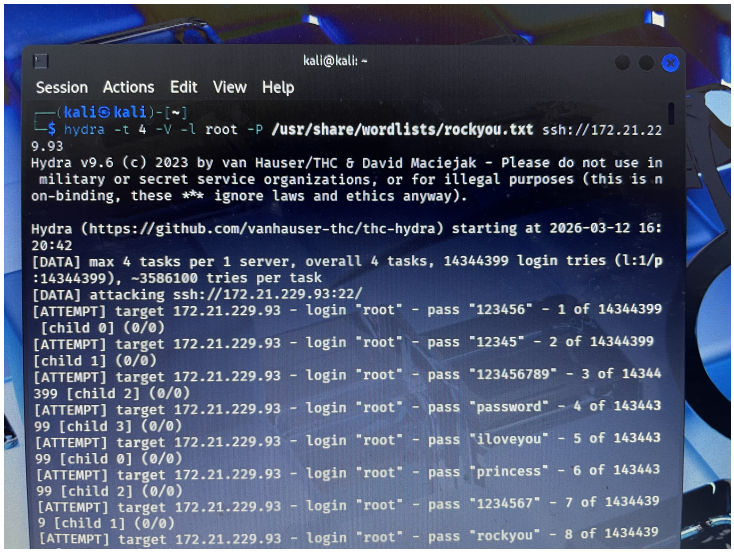

Figure 5.3: attaque hydra avec kali linux

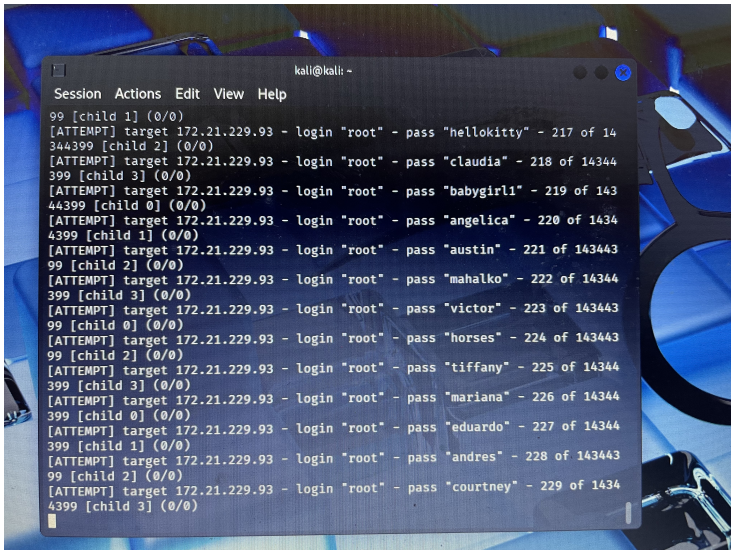

Figure 5.4: Mots de passe générés avec la bibliothèque RockYou

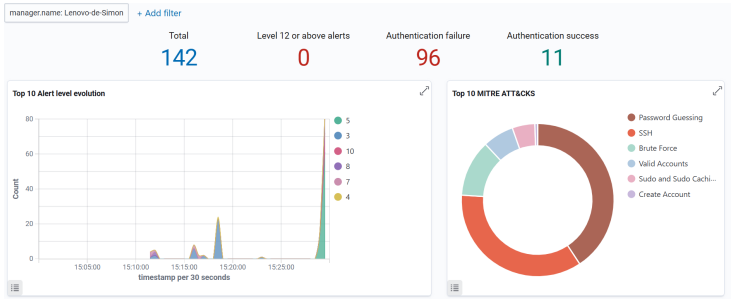

Figure 5.5: Détection des tentatives de connexion sur le tableau de bord Wazuh.

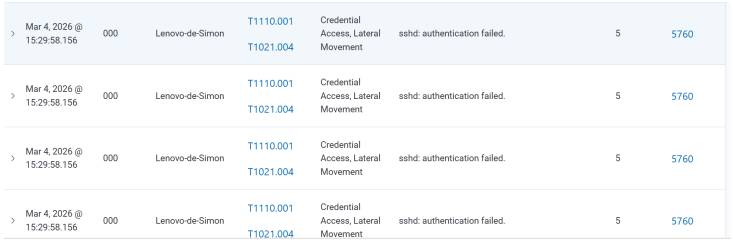

Figure 5.6: Détection de tentatives avec une fréquence très élevée

Chapter 6

Analyse des résultats

Les résultats observés montrent que la plateforme Wazuh est capable de détecter efficacement les activités malveillantes.

Les principales détections réalisées sont :
-Scan de ports effectué avec Nmap
-Tentatives de brute force sur le service RDP
-Échecs multiples d'authentification
-Connexion réussie après authentification

Ces événements sont centralisés dans le tableau de bord Wazuh, ce qui permet d'obtenir une vue globale de l'activité de sécurité sur l'infrastructure.

Chapter 7

Difficultés rencontrées

7.1 Kali Linux

Kali Linux est une distribution Linux utilisée pour réaliser des tests d'intrusion. Lors de l'installation, quand on télécharge l'image Kali pour VirtualBox et qu'on l'importe ensuite dans notre machine virtuelle, elle s'importe avec sa propre configuration, dont certains éléments ne peuvent être modifiés comme on le souhaite.

Figure 7.1: Configuration initiale de Kali sous VirtualBox

Nous avons rencontré ce problème de configuration et pour le résoudre, nous avons téléchargé le fichier ISO afin de l'ajouter dans la configuration de stockage de notre machine virtuelle.

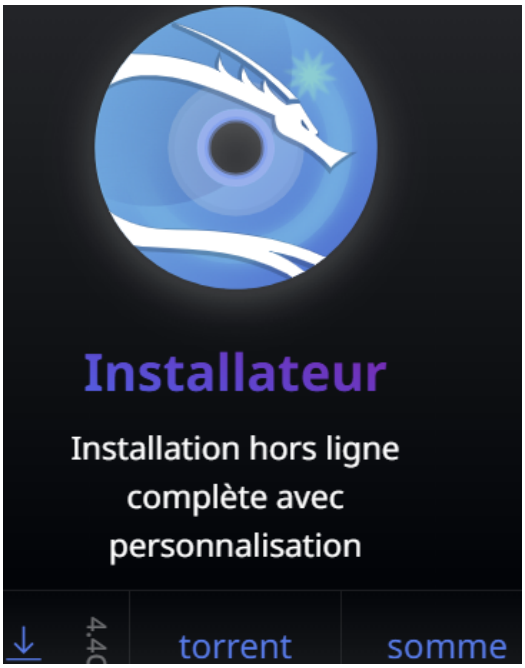

Figure 7.2: Ajout du fichier ISO dans la configuration

Ainsi, nous avons pu effectuer les modifications nécessaires comme demandé dans le rapport d'installation que nous avions. En revanche, la connexion par pont ne fonctionnait pas ; nous sommes donc restés en NAT, ce qui ne nous a nullement gênés dans notre travail.

De plus, l'installation de l'agent Wazuh a nécessité plusieurs tentatives en raison de différents problèmes de configuration et de compatibilité de versions. Ces difficultés nous ont amenés à désinstaller et réinstaller Wazuh à plusieurs reprises afin d'obtenir une version fonctionnelle et assurer la communication correcte entre l'agent et le serveur.

Chapter 8

Conclusion

Ce projet a permis de mettre en place une plateforme de supervision de sécurité basée sur la solution open source Wazuh.

L'infrastructure mise en place permet de centraliser les journaux d'événements, d'analyser les activités du système et de détecter les tentatives d'intrusion.

Les tests réalisés à l'aide d'outils de pentesting comme Nmap et Hydra ont démontré l'efficacité du SIEM pour identifier les activités suspectes.

Ce type de solution constitue un outil essentiel pour la surveillance et la protection des infrastructures informatiques dans les environnements professionnels.