



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

1	Introduction	1
2	Présentation de Wazuh	2
3	Architecture du laboratoire	3
4	Mise en place de la plateforme	4
5	Simulation d'attaques	6
5.1	Scan de ports	6
5.2	Attaque par force brute	6
6	Analyse des résultats	9
7	Difficultés rencontrées	10
7.1	Kali Linux	10
8	Conclusion	12

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.

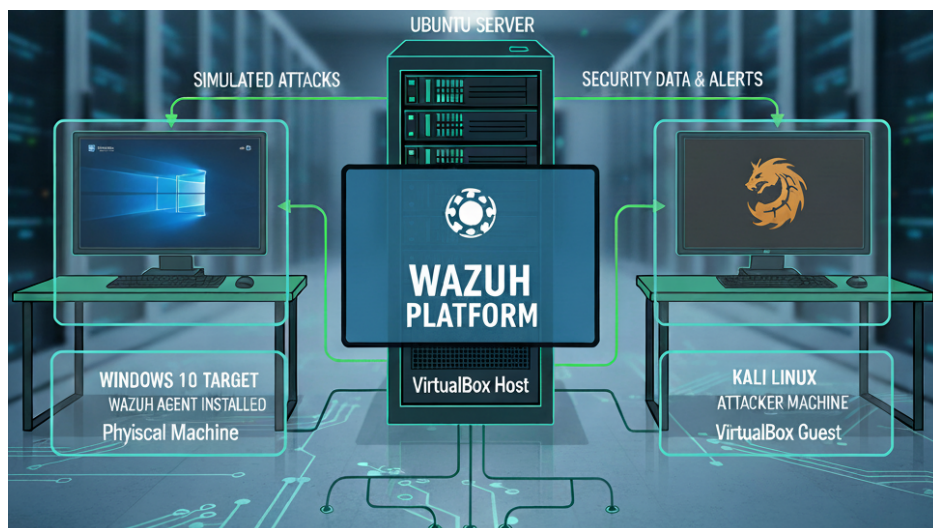


Figure 3.1: Schéma de notre architecture

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 -s0 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.

```

ligna--allow-bad-names@Lenovo-de-Simon:~$ sudo systemctl enable wazuh-manager
sudo systemctl start wazuh-manager
ligna--allow-bad-names@Lenovo-de-Simon:~$ sudo systemctl status wazuh-manager
● wazuh-manager.service - Wazuh manager
   Loaded: loaded (/usr/lib/systemd/system/wazuh-manager.service; enabled; preset: enabled)
   Active: active (running) since Thu 2026-03-12 20:51:09 CET; 13min ago
     Tasks: 213 (limit: 9386)
    Memory: 818.3M (peak: 1.7G swap: 3.1M swap peak: 3.1M)
       CPU: 48.898s
    CGroup: /system.slice/wazuh-manager.service
            └─ 995 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
               996 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
              1003 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
              1006 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
              1055 /var/ossec/bin/wazuh-authd
              1083 /var/ossec/bin/wazuh-db
              1133 /var/ossec/bin/wazuh-execd
              1286 /var/ossec/bin/wazuh-analysisd
              1332 /var/ossec/bin/wazuh-syscheckd
              1434 /var/ossec/bin/wazuh-remoted
              1474 /var/ossec/bin/wazuh-logcollector
              1497 /var/ossec/bin/wazuh-monitord
             1506 /var/ossec/bin/wazuh-modulesd

```

Figure 4.1: Wazuh est activé

```

ligna--allow-bad-names@Lenovo-de-Simon:~$ sudo systemctl enable ssh
sudo systemctl start ssh
[sudo] password for ligna--allow-bad-names:
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
ligna--allow-bad-names@Lenovo-de-Simon:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
   Active: active (running) since Thu 2026-03-12 20:50:52 CET; 13min ago
 TriggeredBy: ● ssh.socket
              Docs: man:sshd(8)
                  man:sshd_config(5)
    Main PID: 298 (sshd)
      Tasks: 1 (limit: 9386)
     Memory: 2.0M (peak: 2.6M)
        CPU: 54ms
    CGroup: /system.slice/ssh.service
            └─ 298 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

```

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.

```
kali@kali:~$ nmap -sV 22 172.21.229.93
Starting Nmap 7.95 ( https://nmap.org ) at 2026-03-12 16:47 EDT
Nmap scan report for 22 (0.0.0.22)
Host is up (0.0070s latency).
All 1000 scanned ports on 22 (0.0.0.22) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap scan report for 172.21.229.93
Host is up (0.0012s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 9.6p1 Ubuntu 3ubuntu13.14 (Ubuntu Linux; prot
ocol 2.0)
443/tcp   open  ssl/https
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
```

Figure 5.1: Utilisation de l'attaque Nmap

```
map.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 21.73 seconds
(kali@kali)-[~]
```

Figure 5.2: Nmap effectué

```
kali@kali:~$ hydra -t 4 -V -l root -P /usr/share/wordlists/rockyou.txt ssh://172.21.229.93
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-03-12 16:20:42
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://172.21.229.93:22/
[ATTEMPT] target 172.21.229.93 - login "root" - pass "123456" - 1 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.21.229.93 - login "root" - pass "12345" - 2 of 14344399 [child 1] (0/0)
[ATTEMPT] target 172.21.229.93 - login "root" - pass "123456789" - 3 of 14344399 [child 2] (0/0)
[ATTEMPT] target 172.21.229.93 - login "root" - pass "password" - 4 of 14344399 [child 3] (0/0)
[ATTEMPT] target 172.21.229.93 - login "root" - pass "iloveyou" - 5 of 14344399 [child 0] (0/0)
[ATTEMPT] target 172.21.229.93 - login "root" - pass "princess" - 6 of 14344399 [child 2] (0/0)
[ATTEMPT] target 172.21.229.93 - login "root" - pass "1234567" - 7 of 14344399 [child 1] (0/0)
[ATTEMPT] target 172.21.229.93 - login "root" - pass "rockyou" - 8 of 14344399
```

Figure 5.3: attaque hydra avec kali linux

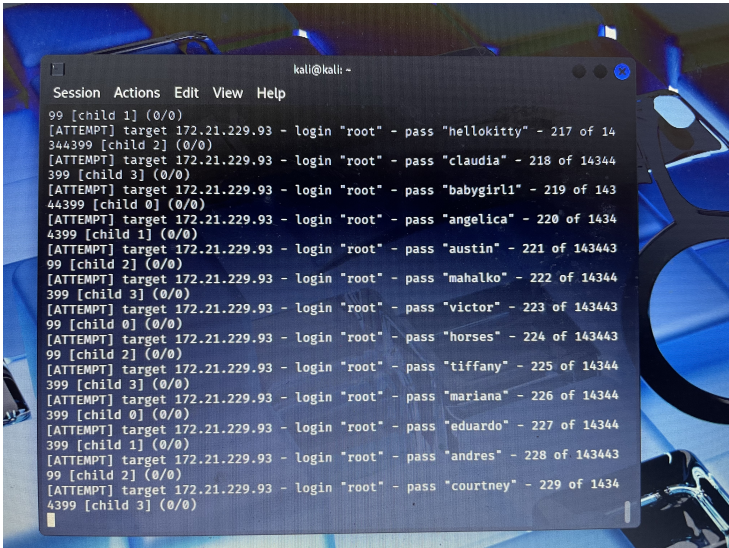


Figure 5.4: Mots de passe g n r s avec la biblioth que RockYou

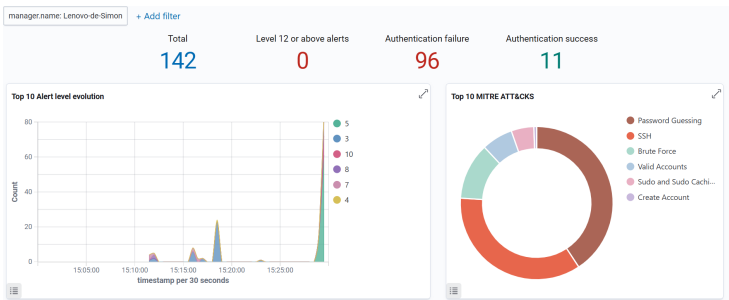


Figure 5.5: D t ction des tentatives de connexion sur le tableau de bord Wazuh.

>	Mar 4, 2026 @ 15:29:58.156	000	Lenovo-de-Simon	T1110.001	Credential Access, Lateral Movement	sshd: authentication failed.	5	5760
				T1021.004				
>	Mar 4, 2026 @ 15:29:58.156	000	Lenovo-de-Simon	T1110.001	Credential Access, Lateral Movement	sshd: authentication failed.	5	5760
				T1021.004				
>	Mar 4, 2026 @ 15:29:58.156	000	Lenovo-de-Simon	T1110.001	Credential Access, Lateral Movement	sshd: authentication failed.	5	5760
				T1021.004				
>	Mar 4, 2026 @ 15:29:58.156	000	Lenovo-de-Simon	T1110.001	Credential Access, Lateral Movement	sshd: authentication failed.	5	5760
				T1021.004				

Figure 5.6: D t ction de tentatives avec une fr quence tr s  lev e

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.

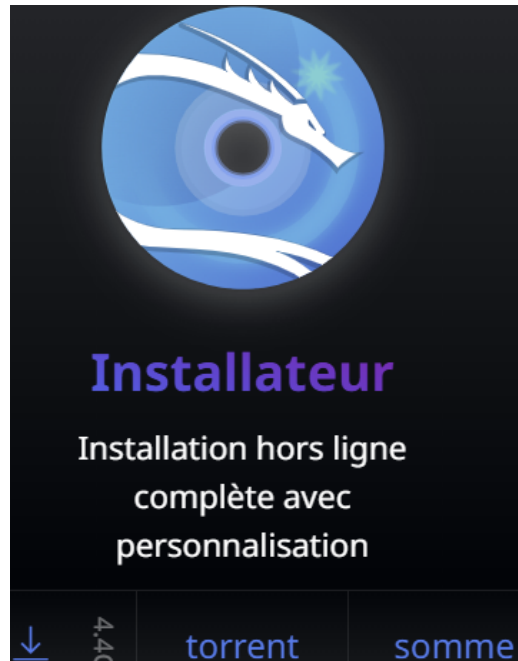


Figure 7.2: Ajout du fichier ISO dans la configuration

Ainsi, nous avons pu effectuer les modifications nécessaires comme demandé dans le rapport d'installation que nous avons. 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.