

Travaux Pratiques

Détection d'Incidents Réseau avec Wazuh SIEM

Réalisé par : Kassoum KONE

Année : 4ème année Ingénieur SIR

1 ARCHITECTURE TECHNIQUE

1.1 Composants de l'infrastructure

Machine Manager (Wazuh) : - OS :

- - Ubuntu 24.04
- - IP : 192.168.56.1 (Host-Only)
- - Rôle : Analyse des logs, gestion des alertes
- - Services : wazuh-manager, wazuh-indexer, wazuh-dashboard

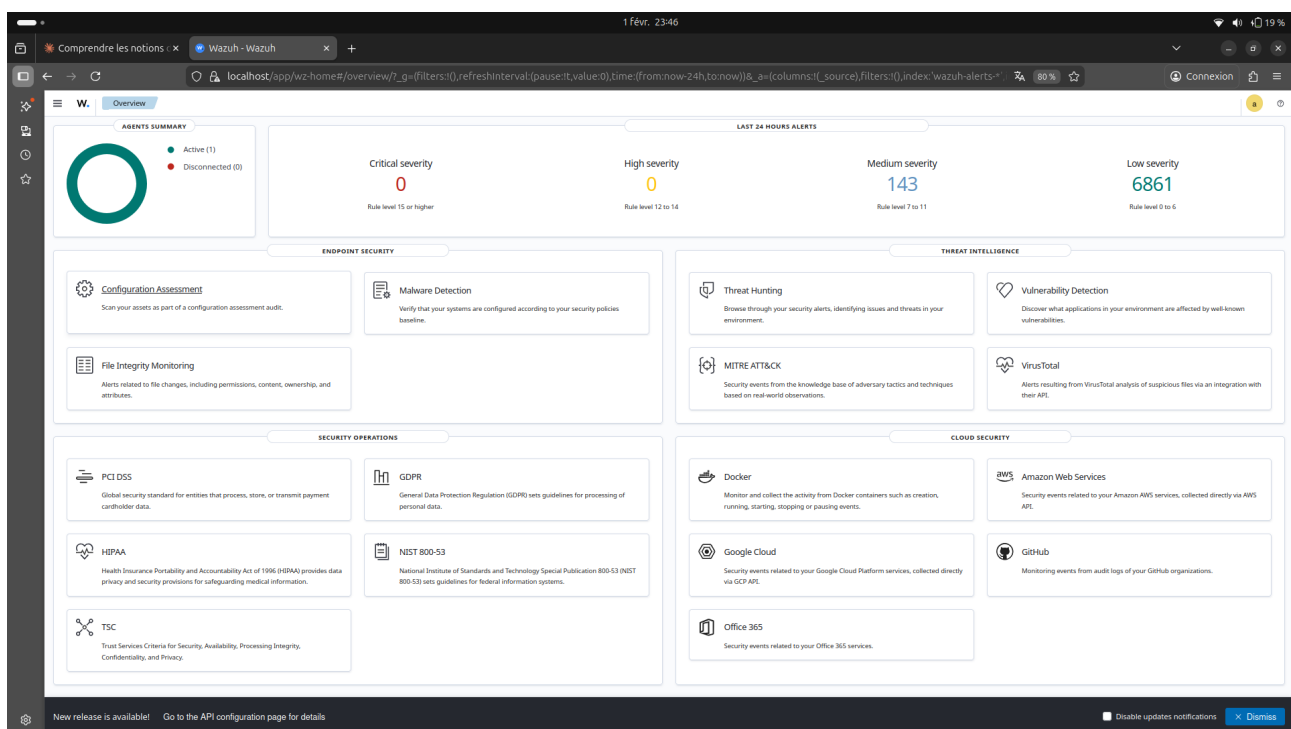


Fig 1 : Dashboard Wazuh

Agent Linux : - OS :

- - Debian 12 - IP : 192.168.56.101 (Host-Only)
- - Rôle : Collecte logs SSH, système

- Configuration : Agent Wazuh 4.8.2

```

root@linux-agent:~/home/student# su
root@linux-agent:~/home/student# loadkeys fr
root@linux-agent:~/home/student# sudo grep "Failed password" /var/log/auth.log | tail -30
bash: sudo: command not found
root@linux-agent:~/home/student# grep "Failed password" /var/log/auth.log | tail -30
2025-02-01T08:18:49.87951-05:00 Linux-Agent sshd-session[1218]: Failed password for invalid user fakuser from ::1 port 42470 ssh2
2025-02-01T08:18:49.87951-05:00 Linux-Agent sshd-session[1218]: Failed password for invalid user fakuser from ::1 port 42470 ssh2
2025-02-01T08:18:49.87951-05:00 Linux-Agent sshd-session[1222]: Failed password for invalid user fakuser from ::1 port 56915 ssh2
2025-02-01T08:18:49.87951-05:00 Linux-Agent sshd-session[1222]: Failed password for invalid user fakuser from ::1 port 56915 ssh2
2025-02-01T08:46:36.34581-05:00 Linux-Agent sshd-session[1321]: Failed password for root from 192.168.56.1 port 51930 ssh2
2025-02-01T08:46:36.34581-05:00 Linux-Agent sshd-session[1321]: Failed password for root from 192.168.56.1 port 51930 ssh2
2025-02-01T08:46:36.34581-05:00 Linux-Agent sshd-session[1322]: Failed password for root from 192.168.56.1 port 51930 ssh2
2025-02-01T08:46:36.34581-05:00 Linux-Agent sshd-session[1322]: Failed password for root from 192.168.56.1 port 51930 ssh2
2025-02-01T08:46:36.34581-05:00 Linux-Agent sshd-session[1324]: Failed password for root from 192.168.56.1 port 51930 ssh2
2025-02-01T08:46:36.34581-05:00 Linux-Agent sshd-session[1324]: Failed password for root from 192.168.56.1 port 51930 ssh2
2025-02-01T08:46:36.34581-05:00 Linux-Agent sshd-session[1343]: Failed password for root from 192.168.56.1 port 51770 ssh2
2025-02-01T08:46:36.34581-05:00 Linux-Agent sshd-session[1343]: Failed password for root from 192.168.56.1 port 51770 ssh2
2025-02-01T08:46:36.34581-05:00 Linux-Agent sshd-session[1344]: Failed password for root from 192.168.56.1 port 51770 ssh2
2025-02-01T08:46:36.34581-05:00 Linux-Agent sshd-session[1344]: Failed password for root from 192.168.56.1 port 51770 ssh2
2025-02-01T08:46:36.34581-05:00 Linux-Agent sshd-session[1347]: Failed password for root from 192.168.56.1 port 51770 ssh2
2025-02-01T08:46:36.34581-05:00 Linux-Agent sshd-session[1347]: Failed password for root from 192.168.56.1 port 51770 ssh2
2025-02-01T08:46:36.34581-05:00 Linux-Agent sshd-session[1387]: Failed password for root from 192.168.56.1 port 55830 ssh2
2025-02-01T08:46:36.34581-05:00 Linux-Agent sshd-session[1387]: Failed password for root from 192.168.56.1 port 55830 ssh2
2025-02-01T08:46:36.34581-05:00 Linux-Agent sshd-session[1387]: Failed password for root from 192.168.56.1 port 55830 ssh2
2025-02-01T08:46:36.34581-05:00 Linux-Agent sshd-session[1387]: Failed password for root from 192.168.56.1 port 55830 ssh2
2025-02-01T08:46:36.34581-05:00 Linux-Agent sshd-session[1384]: Failed password for root from 192.168.56.1 port 55880 ssh2
2025-02-01T08:46:36.34581-05:00 Linux-Agent sshd-session[1384]: Failed password for root from 192.168.56.1 port 55880 ssh2
2025-02-01T08:46:36.34581-05:00 Linux-Agent sshd-session[1384]: Failed password for root from 192.168.56.1 port 55880 ssh2
2025-02-01T08:46:36.34581-05:00 Linux-Agent sshd-session[1384]: Failed password for root from 192.168.56.1 port 55880 ssh2
2025-02-01T12:25:14.871704-05:00 Linux-Agent sshd-session[1261]: Failed password for root from 192.168.56.103 port 34265 ssp2
2025-02-01T12:25:14.871704-05:00 Linux-Agent sshd-session[1261]: Failed password for root from 192.168.56.103 port 34265 ssp2
2025-02-01T12:25:14.871704-05:00 Linux-Agent sshd-session[1261]: Failed password for root from 192.168.56.103 port 34265 ssp2
2025-02-01T12:25:14.871704-05:00 Linux-Agent sshd-session[1278]: Failed password for root from 192.168.56.103 port 34295 ssp2
2025-02-01T12:25:14.871704-05:00 Linux-Agent sshd-session[1278]: Failed password for root from 192.168.56.103 port 34295 ssp2
2025-02-01T12:25:14.871704-05:00 Linux-Agent sshd-session[1283]: Failed password for root from 192.168.56.103 port 34449 ssp2
2025-02-01T12:25:14.871704-05:00 Linux-Agent sshd-session[1283]: Failed password for root from 192.168.56.103 port 34449 ssp2
2025-02-01T12:25:14.871704-05:00 Linux-Agent sshd-session[1286]: Failed password for root from 192.168.56.103 port 44805 ssp2
2025-02-01T12:25:14.871704-05:00 Linux-Agent sshd-session[1286]: Failed password for root from 192.168.56.103 port 44805 ssp2
2025-02-01T12:25:14.871704-05:00 Linux-Agent sshd-session[1342]: Failed password for root from 192.168.56.103 port 44965 ssp2
2025-02-01T12:25:14.871704-05:00 Linux-Agent sshd-session[1342]: Failed password for root from 192.168.56.103 port 44965 ssp2
2025-02-01T12:25:14.871704-05:00 Linux-Agent sshd-session[1345]: Failed password for root from 192.168.56.103 port 32347 ssp2
2025-02-01T12:25:14.871704-05:00 Linux-Agent sshd-session[1345]: Failed password for root from 192.168.56.103 port 32347 ssp2
2025-02-01T12:25:14.871704-05:00 Linux-Agent sshd-session[1348]: Failed password for root from 192.168.56.103 port 43203 ssp2
2025-02-01T12:25:14.871704-05:00 Linux-Agent sshd-session[1351]: Failed password for root from 192.168.56.103 port 30453 ssp2
root@linux-agent:~/home/student#

```

Fig 2 : Linux-Agent

Machine Attaquante :

- OS : Kali Linux 2025.1
- IP : 192.168.56.103 (Host-Only)
- Rôle : Simulation d'attaques (Nmap, Hydra, Metasploit, Ettercap)

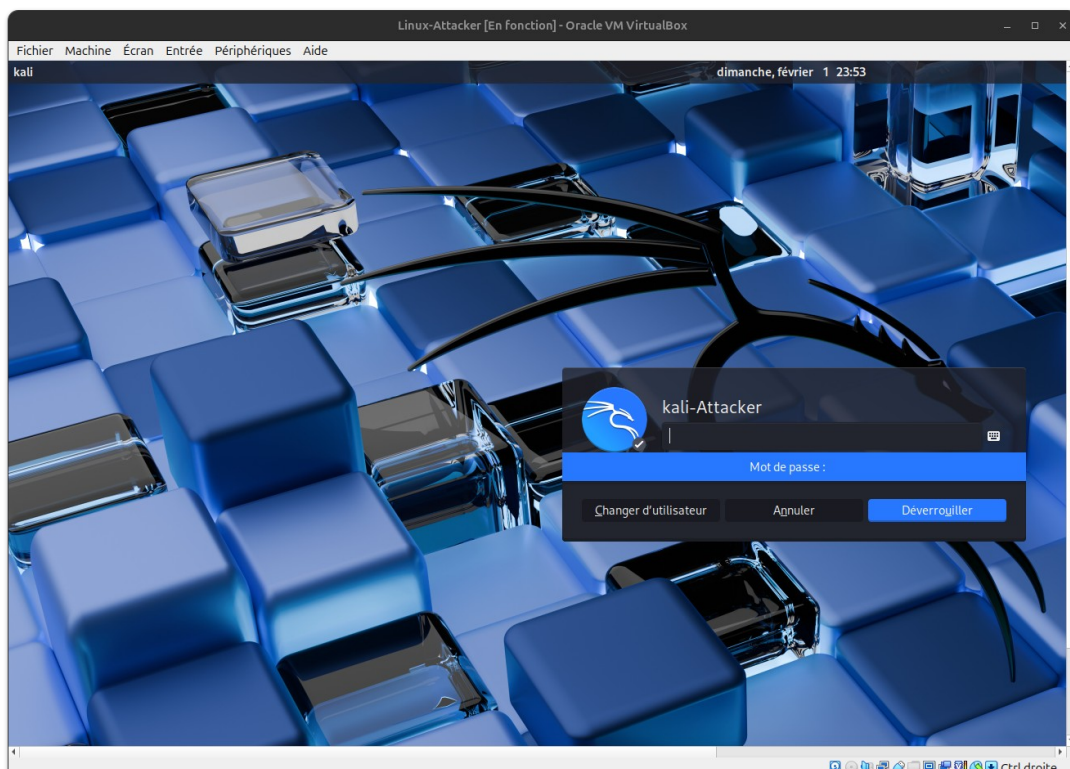


Fig 3 : kali-attacker

1.2 Configuration Réseau

- Réseau utilisé : VirtualBox Host-Only (vboxnet0)
- Sous-réseau : 192.168.56.0/24
- Communication Manager-Agent : Port 1514/TCP

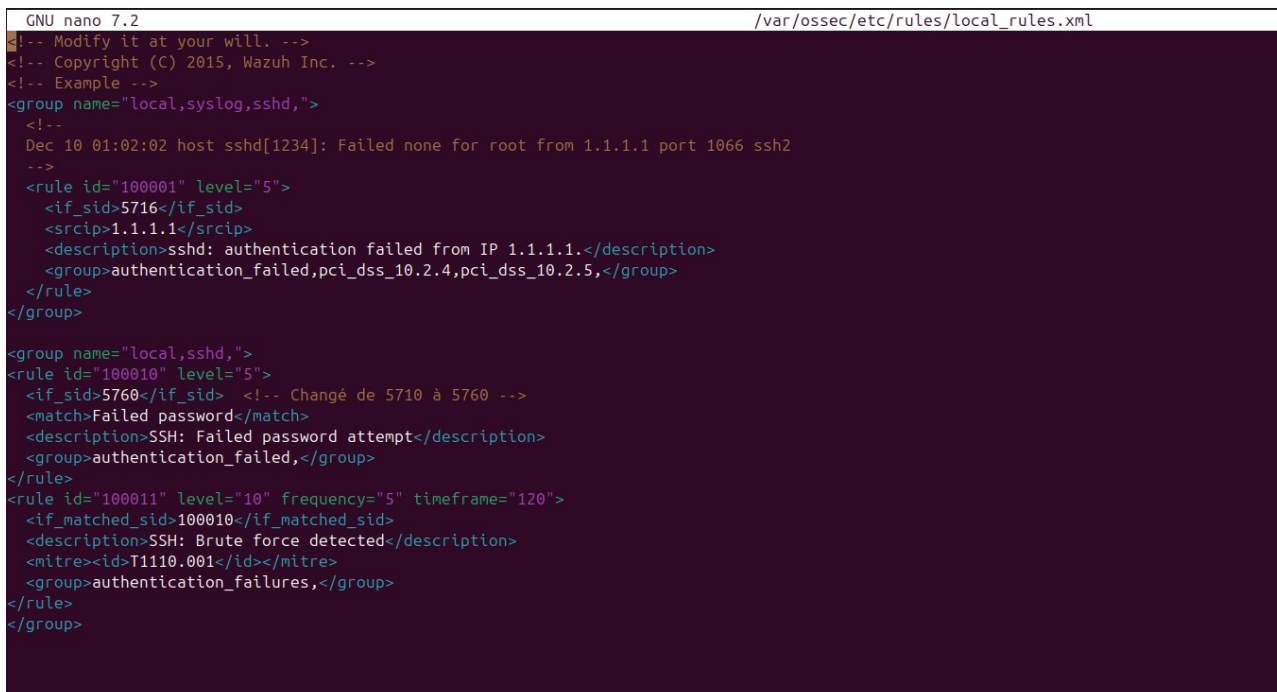
1.3 Logs collectés

- - /var/log/auth.log (authentifications SSH)
- - /var/log/syslog (événements système)
- - Fréquence de lecture : 360 secondes

2 RÈGLES DE DÉTECTION PERSONNALISÉES

2.1 Objectif

Création de règles custom pour détecter les attaques brute force SSH en temps réel.



```
GNU nano 7.2 /var/ossec/etc/rules/local_rules.xml
<!-- Modify it at your will. -->
<!-- Copyright (C) 2015, Wazuh Inc. -->
<!-- Example -->
<group name="local,syslog,sshd,">
  <!--
    Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066 ssh2
  -->
  <rule id="100001" level="5">
    <if_sid>5716</if_sid>
    <srcip>1.1.1.1</srcip>
    <description>sshd: authentication failed from IP 1.1.1.1.</description>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
  </rule>
</group>

<group name="local,sshd,">
<rule id="100010" level="5">
  <if_sid>5760</if_sid> <!-- Changé de 5710 à 5760 -->
  <match>Failed password</match>
  <description>SSH: Failed password attempt</description>
  <group>authentication_failed,</group>
</rule>
<rule id="100011" level="10" frequency="5" timeframe="120">
  <if_matched_sid>100010</if_matched_sid>
  <description>SSH: Brute force detected</description>
  <mitre><id>T1110.001</id></mitre>
  <group>authentication_failures,</group>
</rule>
</group>
```

Fig 4 : Custom detection rules

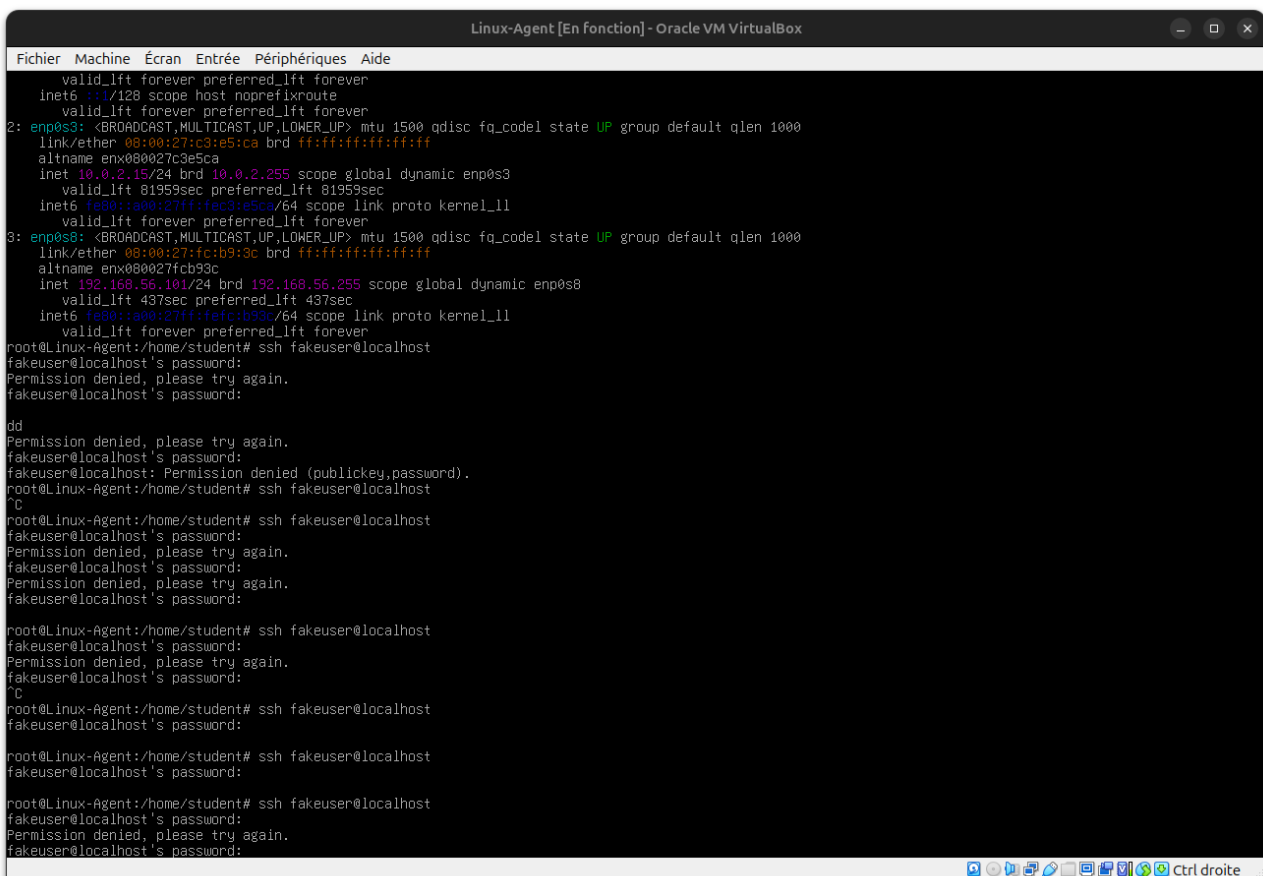
2.2 Règle Parente (ID 100010)

- Fonction : Détecte chaque tentative SSH échouée individuellement.
- Sévérité : Level 5 (faible)
- Héritage : Basée sur la règle 5760 (PAM authentication failed)

2.3 Règle de Corrélation (ID 100011)

- Fonction : Se déclenche après 5 échecs SSH en 2 minutes (120 secondes)
- Sévérité : Level 10 (haute - brute force confirmé)
- MITRE ATT&CK : T1110.001 (Password Guessing)
- Corrélation : Analyse temporelle sur 2 minutes

2.4 Tests de Validation

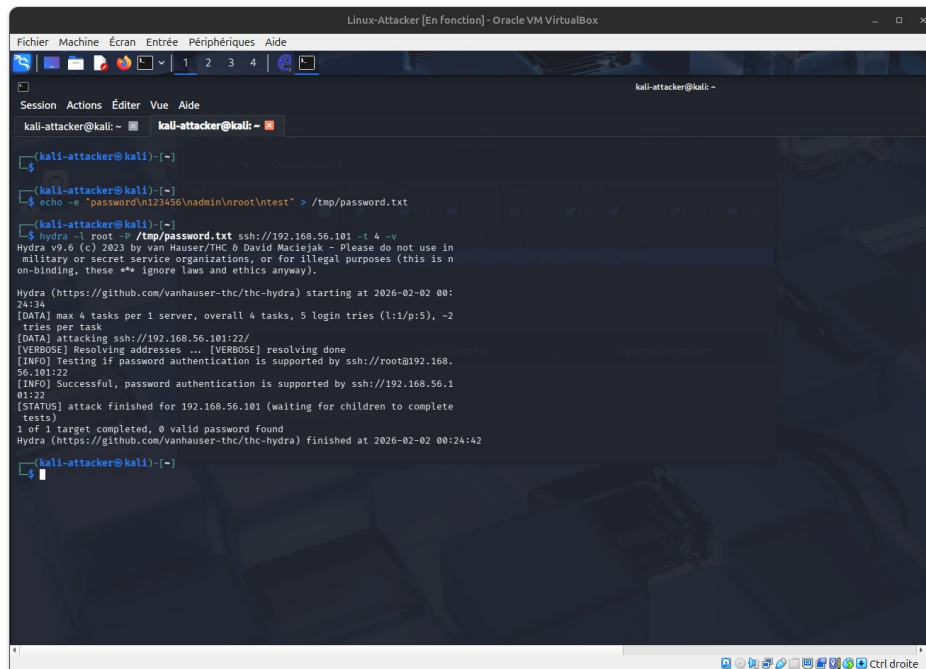


```

Linux-Agent [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
    valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
    valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:c3:e5:ca brd ff:ff:ff:ff:ff:ff
   altnam enx000027c3e5ca
   inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 81959sec preferred_lft 81959sec
   inet6 fe80::a00:27ff:fe3c:e5ca/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 08:00:27:fc:b9:3c brd ff:ff:ff:ff:ff:ff
   altnam enx000027fcb93c
   inet 192.168.56.101/24 brd 192.168.56.255 scope global dynamic enp0s8
       valid_lft 437sec preferred_lft 437sec
   inet6 fe80::a00:27ff:fe3c:b93c/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
root@Linux-Agent:/home/student# ssh fakeuser@localhost
fakeuser@localhost's password:
Permission denied, please try again.
fakeuser@localhost's password:
dd
Permission denied, please try again.
fakeuser@localhost's password:
fakeuser@localhost: Permission denied (publickey,password).
root@Linux-Agent:/home/student# ssh fakeuser@localhost
^C
root@Linux-Agent:/home/student# ssh fakeuser@localhost
fakeuser@localhost's password:
Permission denied, please try again.
fakeuser@localhost's password:
Permission denied, please try again.
fakeuser@localhost's password:
root@Linux-Agent:/home/student# ssh fakeuser@localhost
fakeuser@localhost's password:
Permission denied, please try again.
fakeuser@localhost's password:
^C
root@Linux-Agent:/home/student# ssh fakeuser@localhost
fakeuser@localhost's password:
root@Linux-Agent:/home/student# ssh fakeuser@localhost
fakeuser@localhost's password:
Permission denied, please try again.
fakeuser@localhost's password:

```

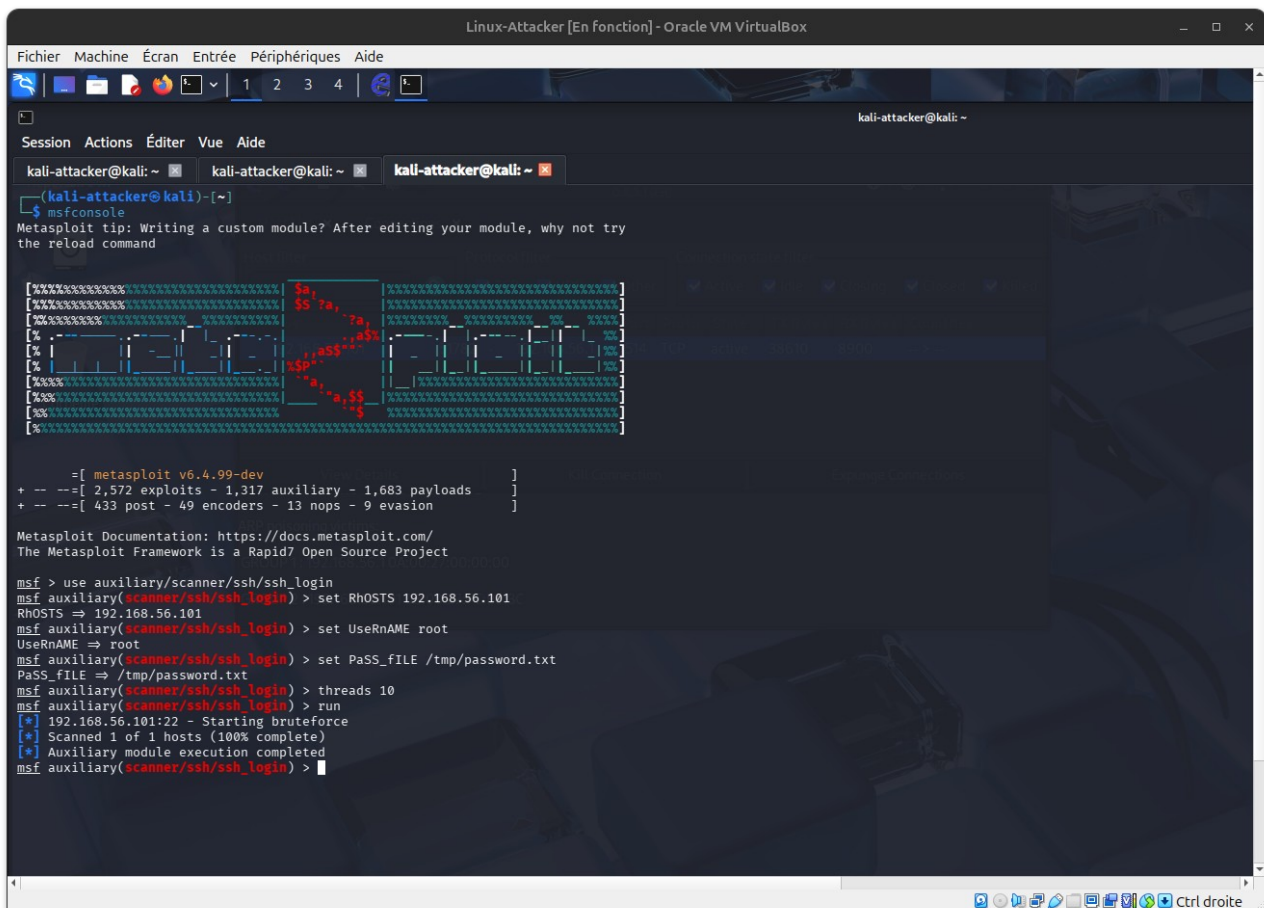
Fig 5 : test de connexion manuel ssh(Brut force)



```
kali-attacker@kali:~$ hydra -l root -P /tmp/password.txt ssh://192.168.56.101 -t 4 -v
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 n
on-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-02-02 00:
24:34
[DATA] max 4 tasks per 1 server, overall 4 tasks, 5 login tries (l1/p:5), ~2
tries per task
[DATA] attacking ssh://192.168.56.101:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://root@192.168.
56.101:22
[INFO] Successful, password authentication is supported by ssh://192.168.56.1
01:22
[STATUS] attack finished for 192.168.56.101 (waiting for children to complete
tests)
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-02-02 00:24:42
```

Fig 6 : Attaque Hydra



```
msfconsole
Metasploit tip: Writing a custom module? After editing your module, why not try
the reload command

=====
[+] 2,572 exploits - 1,317 auxiliary - 1,683 payloads
[+] 433 post - 49 encoders - 13 nops - 9 evasion
=====

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use auxiliary/scanner/ssh/ssh_login
msf auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
msf auxiliary(scanner/ssh/ssh_login) > set UseRNAME root
UseRNAME => root
msf auxiliary(scanner/ssh/ssh_login) > set PaSS_FILE /tmp/password.txt
PaSS_FILE => /tmp/password.txt
msf auxiliary(scanner/ssh/ssh_login) > threads 10
msf auxiliary(scanner/ssh/ssh_login) > run
[*] 192.168.56.101:22 - Starting bruteforce
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/ssh/ssh_login) >
```

Fig 7 : Attaque Metasploit

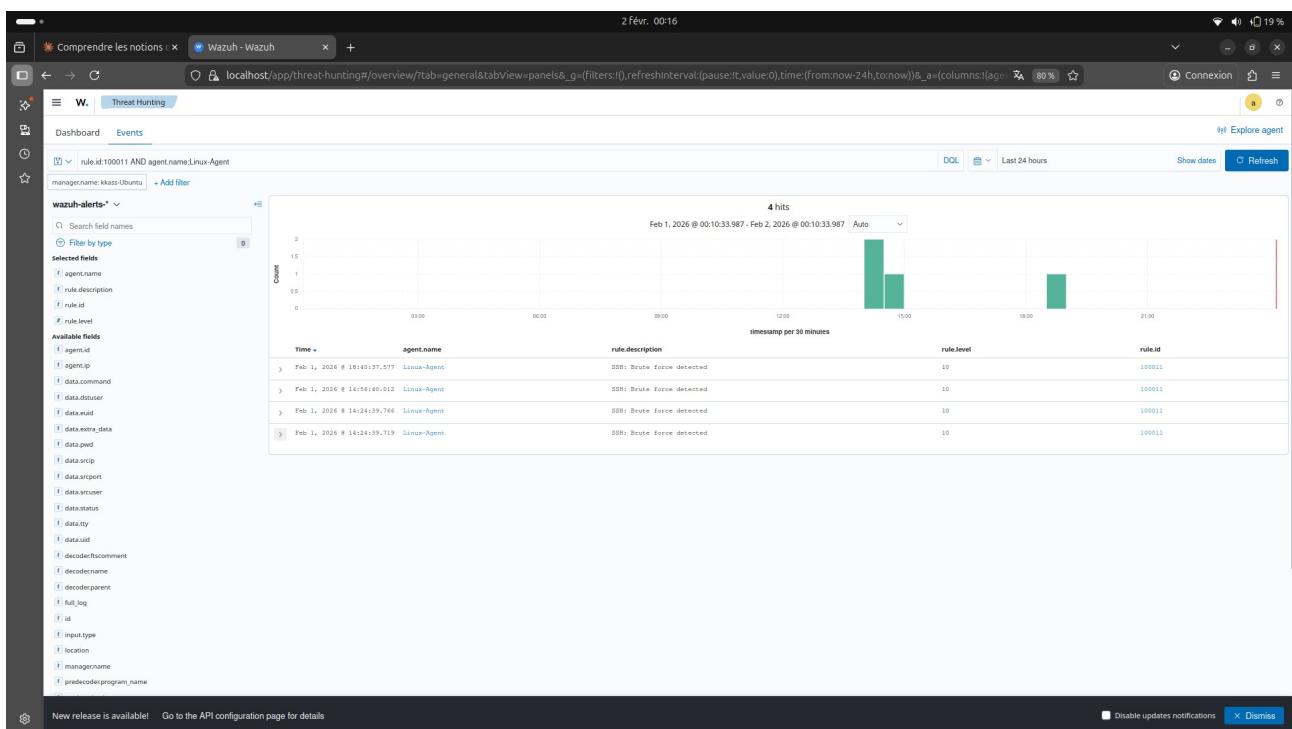
Feb 1, 2026 @ 14:24:39.719 Linux-Agent SDR: Brute force detected 10 100011

Expanded document

View surrounding documents View single document

| Table | JSON |
|---------------------------|--|
| f _index | wazuh-alerts-4.x-2024-02-01 |
| f agent.id | 001 |
| f agent.ip | 10.0.2.15 |
| f agent.name | Linux-Agent |
| f data.recvip | 115 |
| f data.router | fakeuser |
| f decoder.name | ssh |
| f decoder.parent | ssh |
| f full_log | 2026-02-01T08:17:44.511831+05:00 Linux-Agent ssh-session(1209): Failed password for invalid user fakeuser from ::1 port 45114 ssh2 |
| f id | 1769952279.1231663 |
| f input.type | log |
| f location | /var/log/auth.log |
| f manager.name | kiss-ubuntu |
| f predecoder.program_name | ssh-session |
| f predecoder.timestamp | 2026-02-01T08:17:44.511831+05:00 |
| f previous_output | > 2026-02-01T08:17:38.429280+05:00 Linux-Agent ssh-session(1209): Failed password for invalid user fakeuser from ::1 port 45114 ssh2 2026-02-01T08:17:35.723389+05:00 Linux-Agent ssh-session(1209): Failed password for invalid user fakeuser from ::1 port 39900 ssh2 2026-02-01T08:17:24.932084+05:00 Linux-Agent ssh-session(1209): Failed password for invalid user fakeuser from ::1 port 39900 ssh2 2026-02-01T08:17:05.733331+05:00 Linux-Agent ssh-session(1209): Failed password for invalid user fakeuser from ::1 port 39900 ssh2 |
| f rule.description | SDR: Brute force detected |
| f rule.firetime | 1 |
| f rule.frequency | 5 |
| f rule.groups | local, sshd, authenticating_failures |
| f rule.id | 100011 |
| f rule.level | 10 |

Fig 6 : Event Wazuh(Brut force)



Commande de test : ssh fakeuser@localhost (répété 5 fois rapidement)

Résultats :

✓ Règle 100010 déclenchée après chaque échec

- ✓ Règle 100011 déclenchée après 5 échecs en < 2 min
- ✓ Détection visible dans le dashboard Wazuh

3 RAPPORT D'INCIDENT #1 : BRUTE FORCE SSH (HYDRA)

3.1 RÉSUMÉ EXÉCUTIF



Fig 7 : Rapport d’incident

Le 1er février 2026 à 14h46, une attaque brute force SSH a été détectée sur l'agent Linux-Agent (192.168.56.101). L'attaque provenant de l'IP 192.168.56.103 a tenté de deviner le mot de passe du compte root via l'outil Hydra. Aucune connexion réussie n'a été enregistrée. L'incident a été contenu par blocage de l'IP source.

| | |
|-----------------|------------------------------|
| INCIDENT ID | INC-2026-001 |
| DATE DÉTECTION | 2026-02-01 14:46:00 UTC |
| SÉVÉRITÉ | HIGH (Level 10) |
| TYPE D'ATTAQUE | Brute Force SSH (T1110.001) |
| SYSTÈME AFFECTÉ | Linux-Agent (192.168.56.101) |
| STATUT | Résolu - Aucune intrusion |

3.2 TIMELINE DÉTAILLÉE

- 14:24:39 - Première tentative SSH échouée détectée (règle 100010)
- 14:46:33 - Début attaque Hydra depuis 192.168.56.103
- 14:46:41 - Fin attaque Hydra (5 tentatives en 8 secondes)
- 14:46:45 - Déclenchement alerte brute force (règle 100011) 1
- 4:50:00 - Analyse de l'incident initiée
- 14:55:00 - Blocage IP source via iptables
- 15:00:00 - Vérification : aucune connexion réussie

3.3 IOCs (INDICATEURS DE COMPROMISSION)

Username Tentés :

- - root
- - admin
- - test
- - password
- - 123456

Nombre Total de Tentatives : 5

Ports Source : Aléatoires (50000-60000)

Protocole : SSH (port 22/TCP)

3.4 DÉTECTION

Règles Wazuh Déclenchées :

- - 100010 : "SSH: Failed password attempt" (Level 5)
- - 5 fois - 100011 : "SSH: Brute force detected" (Level 10)
- - 1 fois - 5760 : "sshd: authentication failed" (Level 5)

MITRE ATT&CK :

- - T1110.001 : Brute Force- Password Guessing

3.5 CONTAINMENT (CONFINEMENT)

Actions immédiates prises :

1. Blocage IP attaquante :

```
sudo iptables -A INPUT -s 192.168.56.103 -j DROP
```

2. Vérification absence d'intrusion :

```
sudo grep "Accepted password" /var/log/auth.log
```

Résultat : Aucune connexion réussie

3. Vérification sessions actives :

Commande : `who, w`

Résultat : Aucune session suspecte

4. Vérification connexions établies :

```
sudo netstat -antp | grep ESTABLISHED
```

Résultat : Pas de connexion depuis 192.168.56.103

3.6 REMEDIATION (CORRECTION)

Mesures de sécurisation SSH :

1. Désactivation login root SSH :

Fichier : `/etc/ssh/sshd_config`

Modification : `PermitRootLogin no`

2. Authentification par clé uniquement (recommandé) :

`PasswordAuthentication no`

3. Installation Fail2ban (optionnel) :

```
sudo apt install fail2ban -y
```

Bannissement automatique après 3 échecs

3.7 RECOVERY ET RECOMMANDATIONS

Actions post-incident :

- Surveillance logs SSH pendant 48h
- Monitoring alertes règle 100011
- Aucune réapparition de l'attaque

Recommandations :

- Maintenir les règles Wazuh 100010/100011 actives
- Politiques de mots de passe renforcées
- Limitation accès SSH par IP si possible

4 RAPPORT D'INCIDENT #2 : EXPLOITATION METASPLOIT

4.1 RÉSUMÉ EXÉCUTIF

Le 1er février 2026, une attaque brute force SSH via Metasploit Framework a été détectée sur Linux-Agent. L'attaquant a utilisé le module ssh_login pour tenter une connexion automatisée. Détection réussie, aucune intrusion.

4.2 DÉTAILS TECHNIQUES

Outil : Metasploit Framework auxiliary/scanner/ssh/ssh_login

Source : 192.168.56.103 (Kali Linux)

Cible : 192.168.56.101 port 22

Usernames testés : root

Dictionnaire : /tmp/passwords.txt (5 entrées)

4.3 ACTIONS PRISES

Identiques au rapport INC-2026-001 (blocage IP, hardening SSH).

5 RAPPORT D'INCIDENT #3 : RECONNAISSANCE RÉSEAU

5.1 RÉSUMÉ

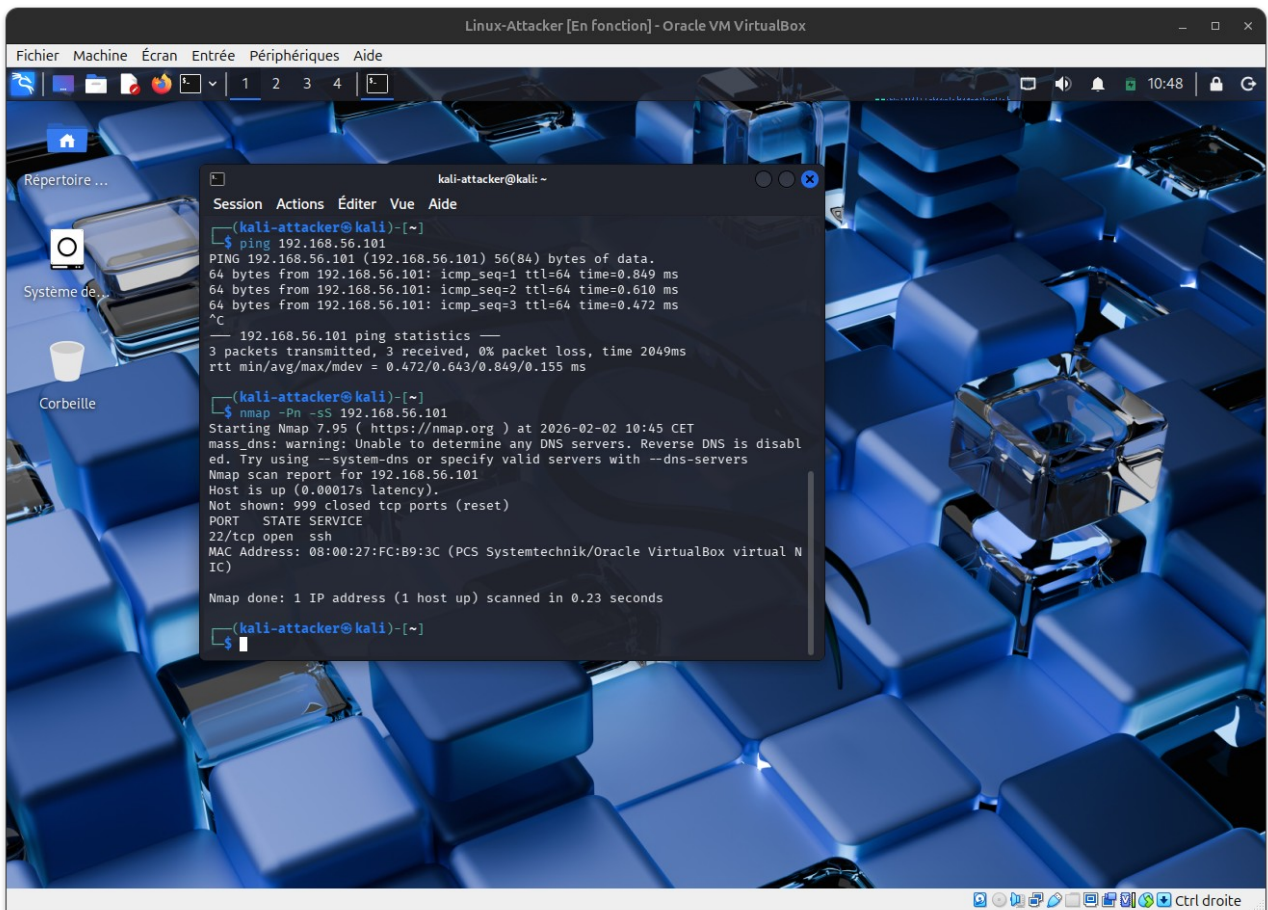


Fig 8 : Nmap

Scan de ports Nmap détecté sur Linux-Agent pour reconnaissance réseau (phase pré-attaque).

| | |
|-------------|--------------------------------|
| INCIDENT ID | INC-2026-003 |
| TYPE | Network Reconnaissance (T1046) |
| SÉVÉRITÉ | MEDIUM (Level 5) |
| OUTIL | Nmap |

5.2 COMMANDES UTILISÉES

- `sudo nmap -Pn -sS 192.168.56.101`
- `sudo nmap -Pn -A -T5 192.168.56.101`

5.3 DÉTECTION

Résultat : Wazuh ne détecte pas directement Nmap (logs réseau niveau paquet non collectés).

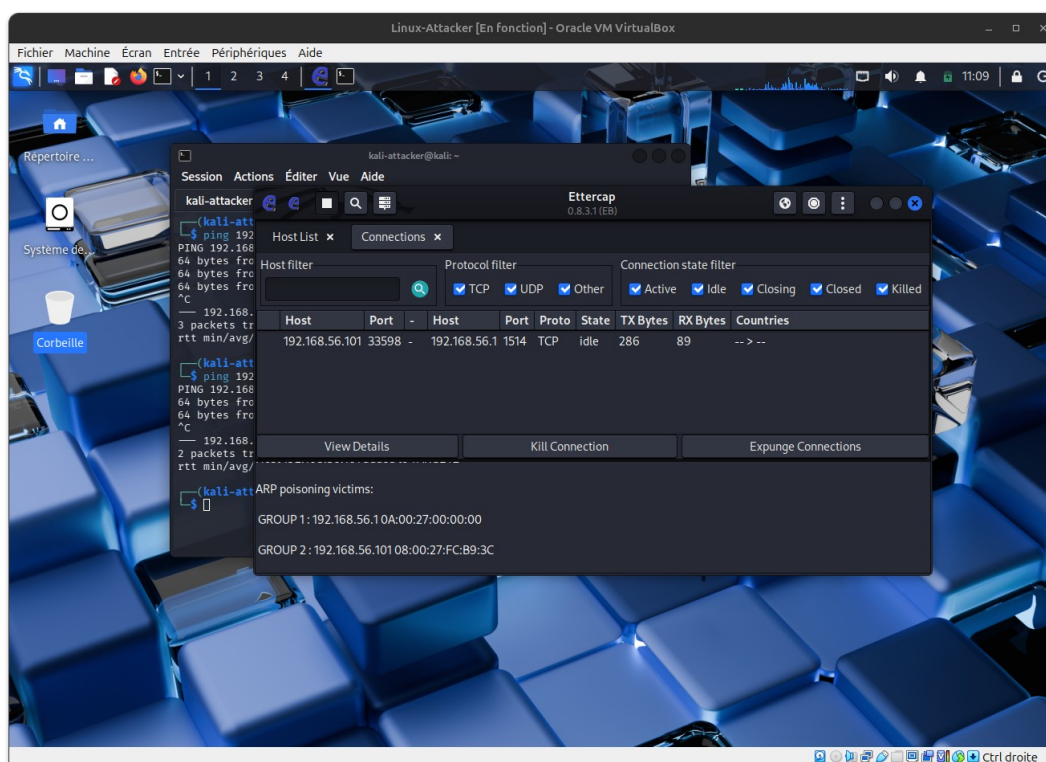
Nécessiterait : Logs firewall/iptables ou IDS réseau (Snort/Suricata).

Amélioration proposée : Activer logging iptables pour détecter scans futurs.

6 RAPPORT D'INCIDENT #4 : INTERCEPTION MAN-IN-THE-MIDDLE

Simulation d'attaque ARP poisoning via Ettercap pour interception du trafic Manager↔Agent.

6.1 RÉSUMÉ



6.2 TECHNIQUE

- Target 1 : 192.168.56.1 (Manager)
- Target 2 : 192.168.56.101 (Agent)
- Méthode : ARP poisoning avec Ettercap GUI

6.3 DÉTECTION

Résultat : Wazuh ne détecte pas l'ARP spoofing (attaque réseau niveau 2).

Limitation : Wazuh analyse logs applicatifs, pas le trafic Ethernet brut.

Recommandation : Déployer monitoring ARP (arpwatch) ou IDS réseau.

Conclusion

Ce travail pratique a permis de :

- Déployer une infrastructure SIEM complète (Manager + Agent) - Créer des règles de détection personnalisées efficaces
- Simuler des attaques réalistes (Nmap, Hydra, Metasploit, Ettercap)
- Appliquer une méthodologie d'investigation professionnelle

Les règles custom développées détectent avec succès les attaques brute force SSH. Les limitations identifiées (scans réseau, ARP poisoning) nécessitent des outils complémentaires (IDS réseau, monitoring ARP).

Compétences acquises :

- Configuration SIEM Wazuh
- Création de règles de corrélation
- Investigation forensique d'incidents
- Simulation d'attaques avec outils professionnels
- Documentation technique et rapports d'incidents

