S9 – L3 EXTRA

Installazione e primo utilizzo di Wazuh (SIEM/XDR) in ambiente di laboratorio

---

Introduzione

In questo esercizio ho configurato un sistema SIEM/XDR basato su **Wazuh** all'interno di un ambiente di laboratorio controllato.
L'obiettivo è stato installare la Wazuh Virtual Machine (OVA), collegarla alla rete del laboratorio, installare e configurare il Wazuh Agent su una macchina Kali Linux e verificare la corretta raccolta delle prime informazioni di sicurezza, in linea con i concetti di monitoraggio, logging centralizzato e incident response.

Prerequisiti e sicurezza

Prima di iniziare:

- Avvio esclusivamente macchine virtuali di laboratorio
- Utilizzo una rete isolata (Host-Only)
- Evito qualunque attività su sistemi reali

---

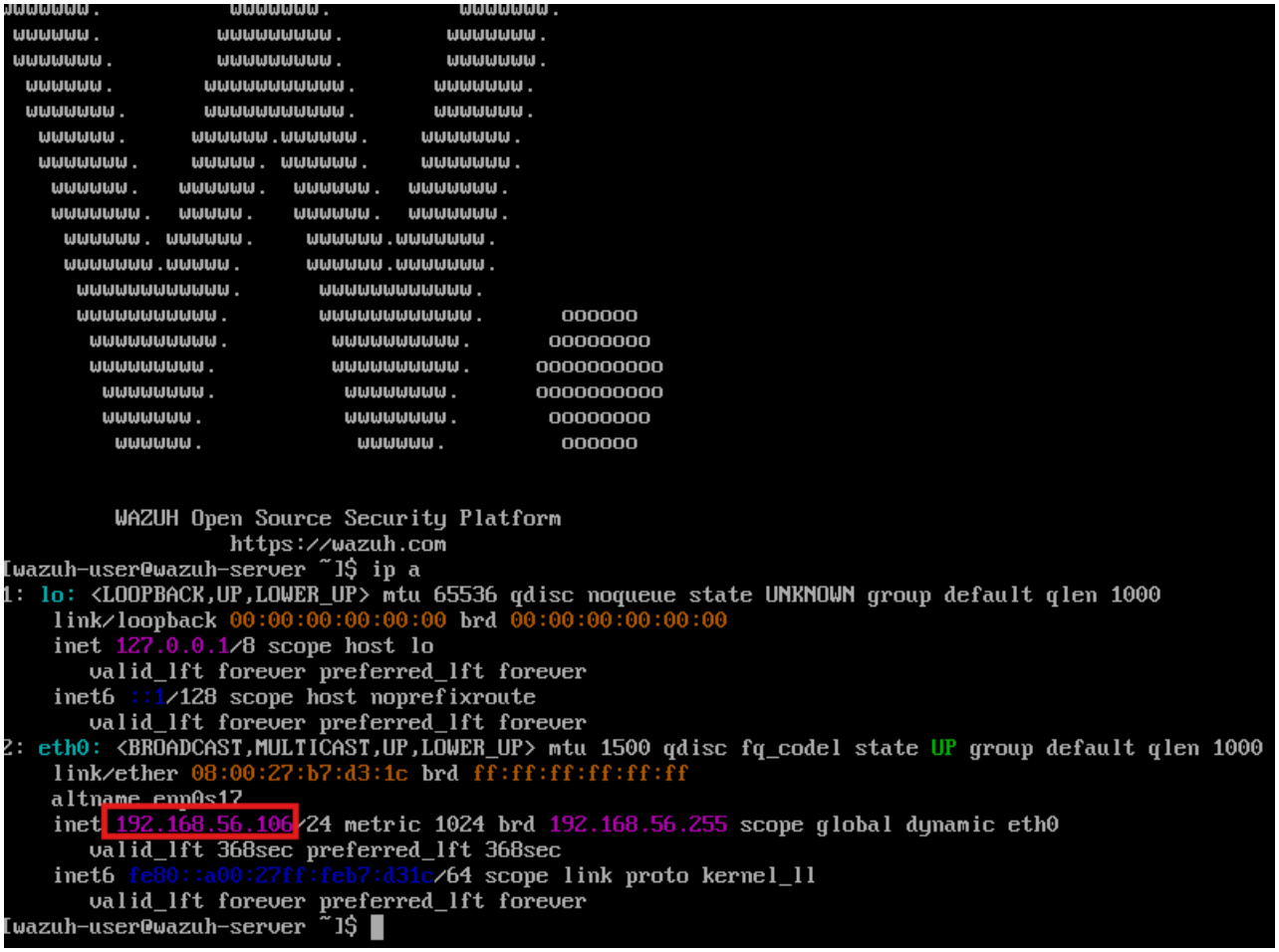
1) Configurazione di rete VM Kali e Wazuh

1. Imposto la scheda di rete della VM **Wazuh** utilizzando lo stesso tipo di rete della VM **Kali Linux** (Host-Only).
2. Avvio entrambe le macchine virtuali.
3. Su **Kali Linux** verifico l'indirizzo IP con:

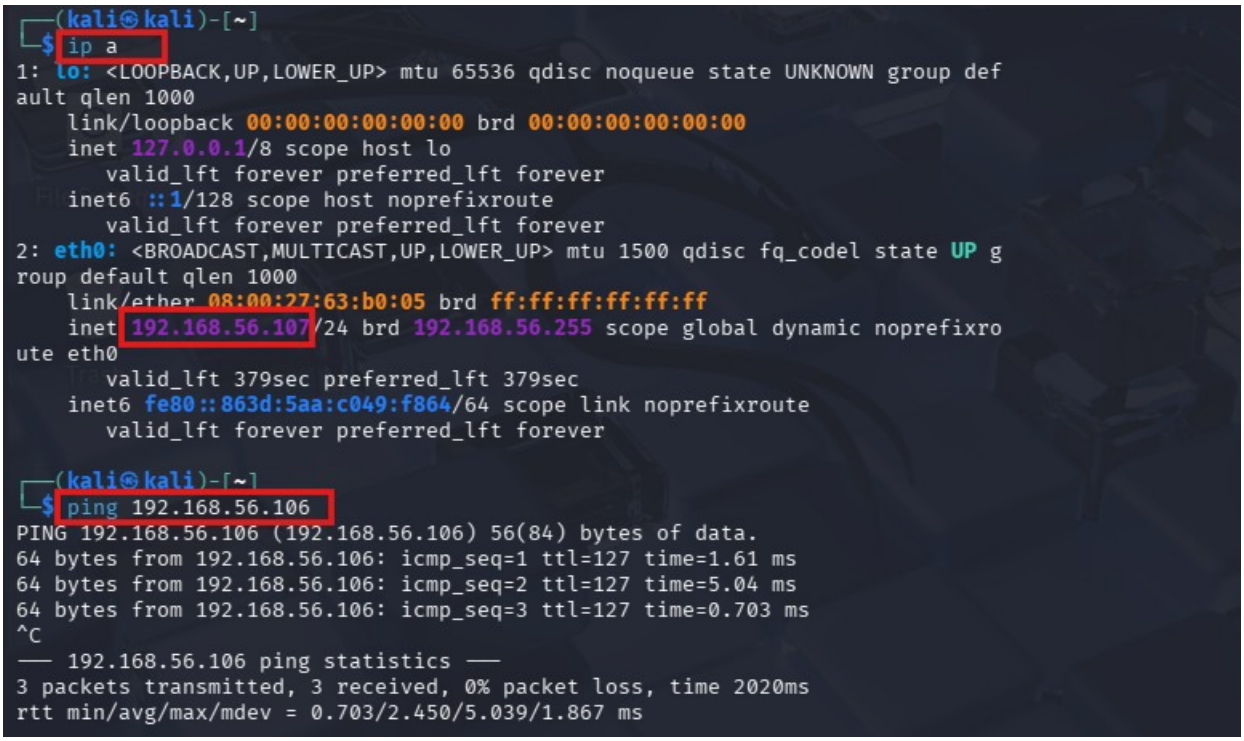
   ```
   ip a
   ```

4. Sulla **Wazuh VM** individuo l'indirizzo IP mostrato a console dopo il login effettuato.
5. Da Kali verifico la raggiungibilità della Wazuh VM:

   ```
   ping 192.168.56.106 (IP_WAZUH)
   ```



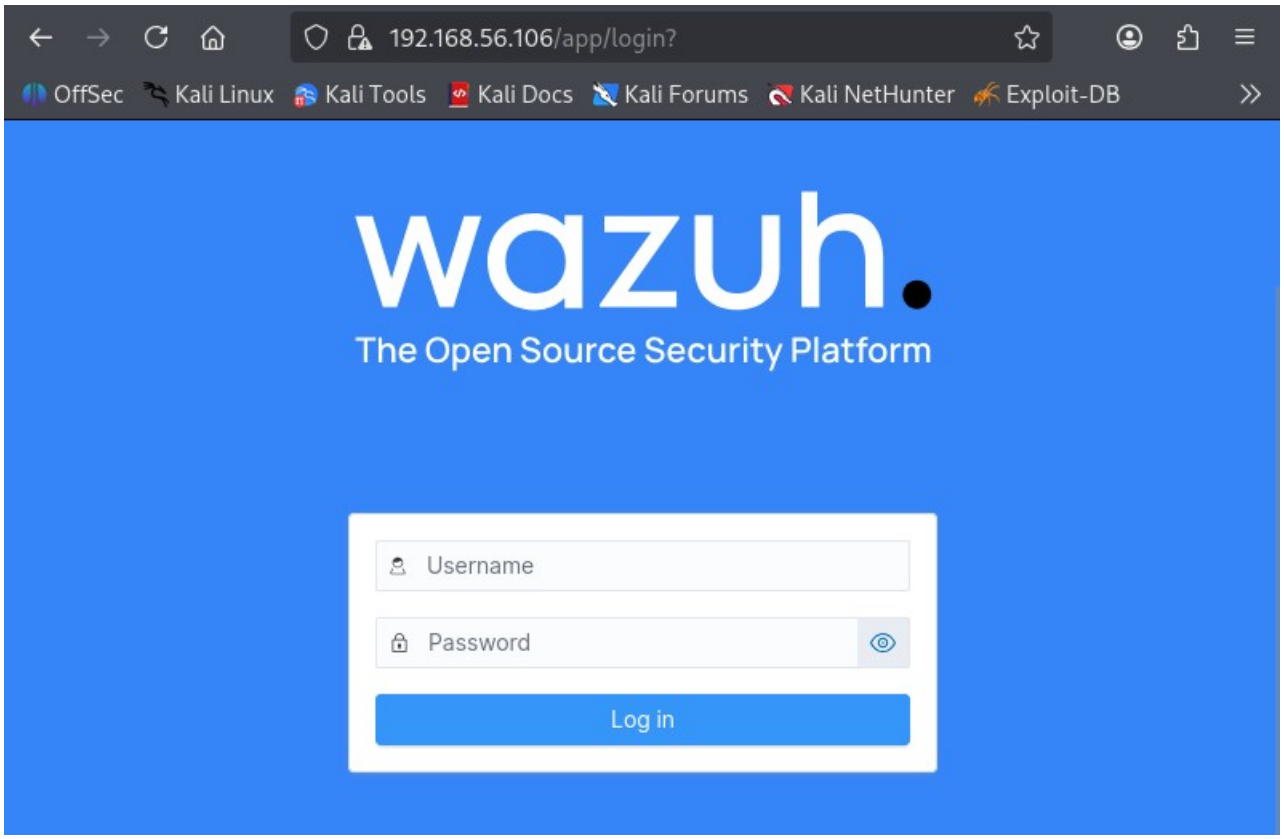
- Output IP Wazuh: **192.168.56.106** dopo il comando **ip a**
- Accesso con user **wazuh-user** e password **wazuh**



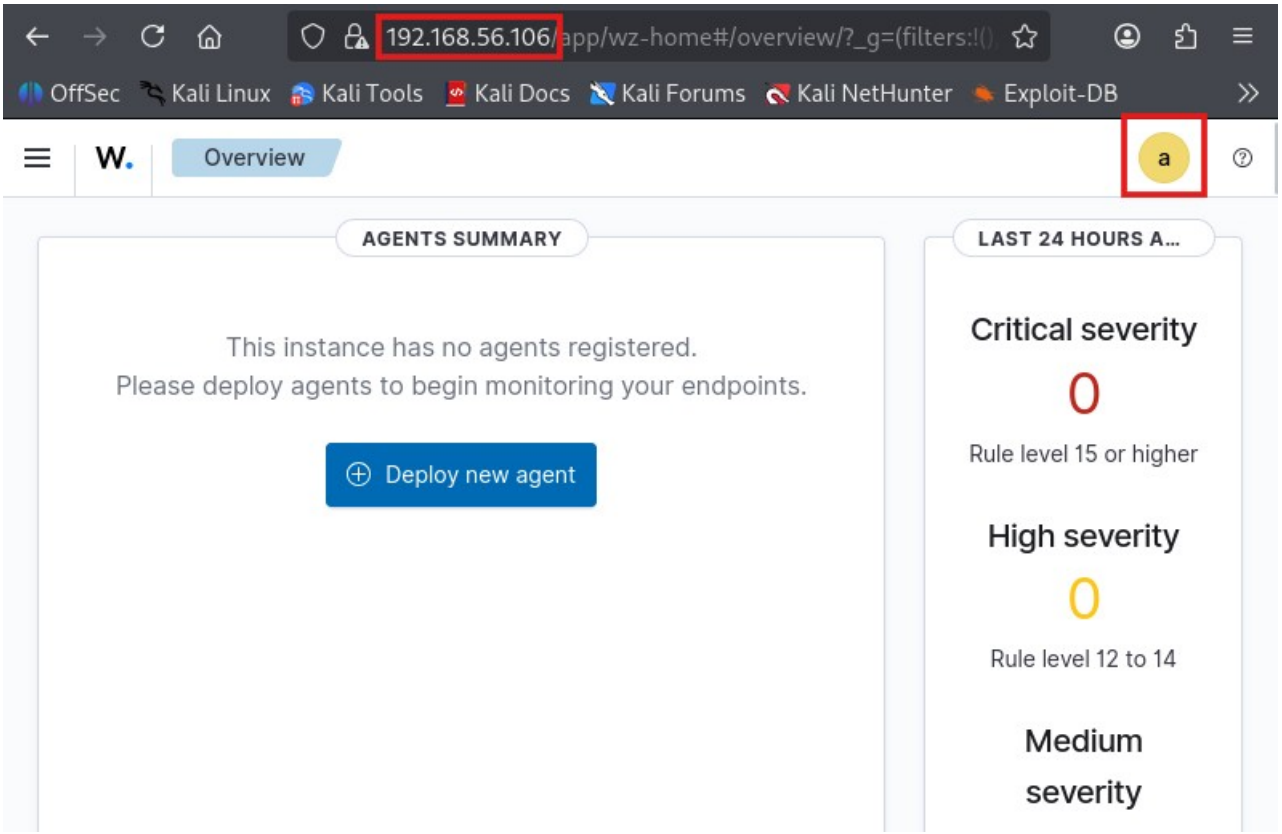
La comunicazione tra le due macchine risulta corretta.

2) Accesso alla dashboard Wazuh

1. Apro il browser su **Kali Linux**.
2. Accedo alla dashboard Wazuh tramite browser utilizzando l'indirizzo:
   https://192.168.56.106 (IP WAZUH)



3. Effettuo il login utilizzando le **credenziali fornite dalla documentazione ufficiale della Wazuh OVA**.
4. Verifico il corretto accesso alla dashboard principale di Wazuh
5. Username: **admin** e Password: **admin**



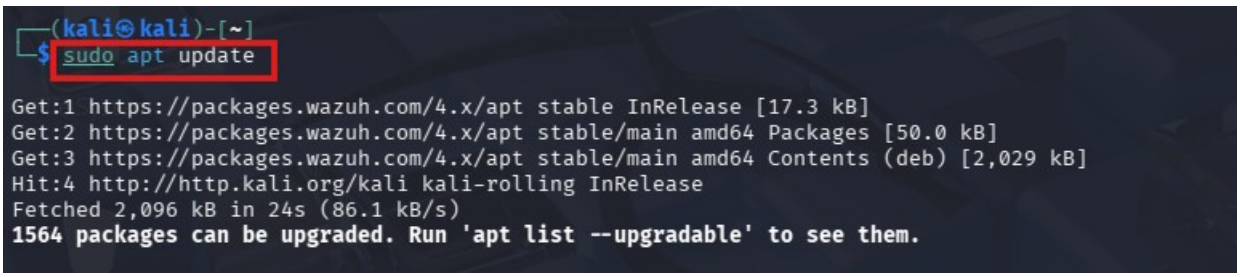
Output dopo il login effettuato con user e passowrd admin

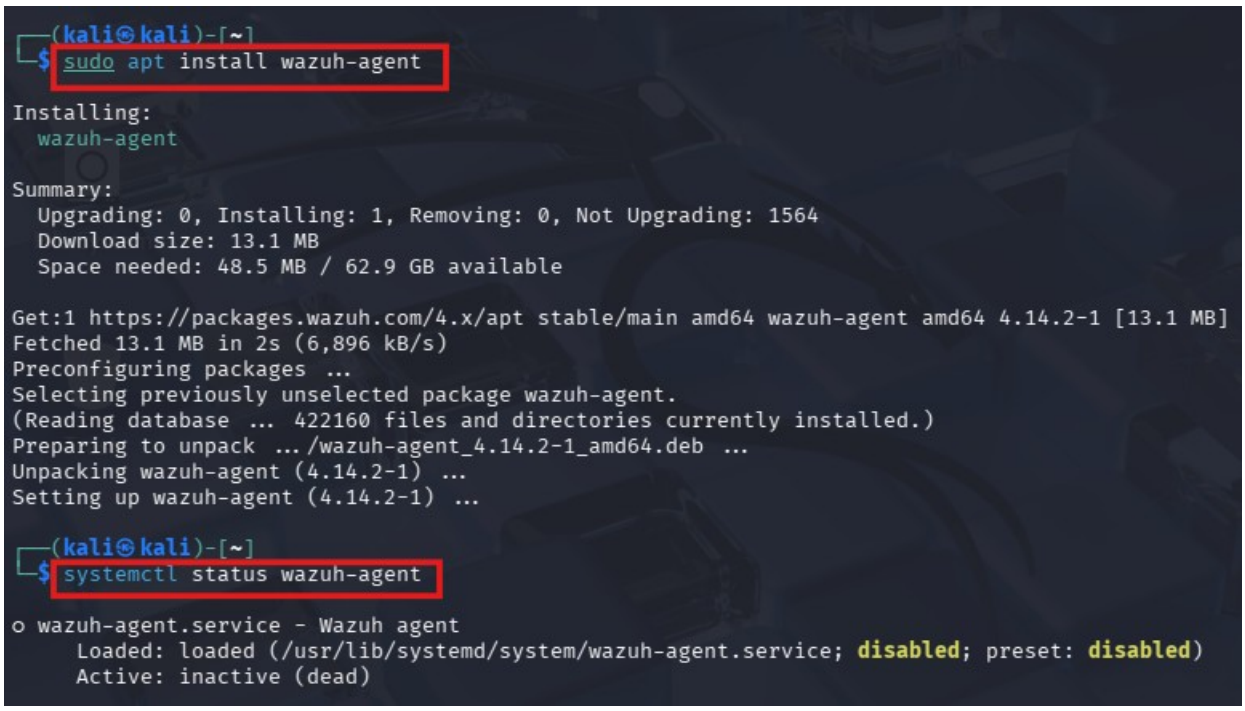
---

3) Installazione del Wazuh Agent su Kali Linux

1. Seguo la guida ufficiale per l'installazione dell'agent Wazuh su sistemi Linux tramite **APT e systemd**.
2. Aggiorno i repository e installo l'agent:

```
sudo apt update
sudo apt install wazuh-agent
```





3. Verifico la presenza del servizio:

   `systemctl status wazuh-agent`

Il Wazuh Agent è stato installato correttamente sulla macchina Kali Linux. Subito dopo l'installazione, **il servizio risulta inattivo, come previsto, in attesa della configurazione del collegamento al manager e della registrazione dell'agent.**

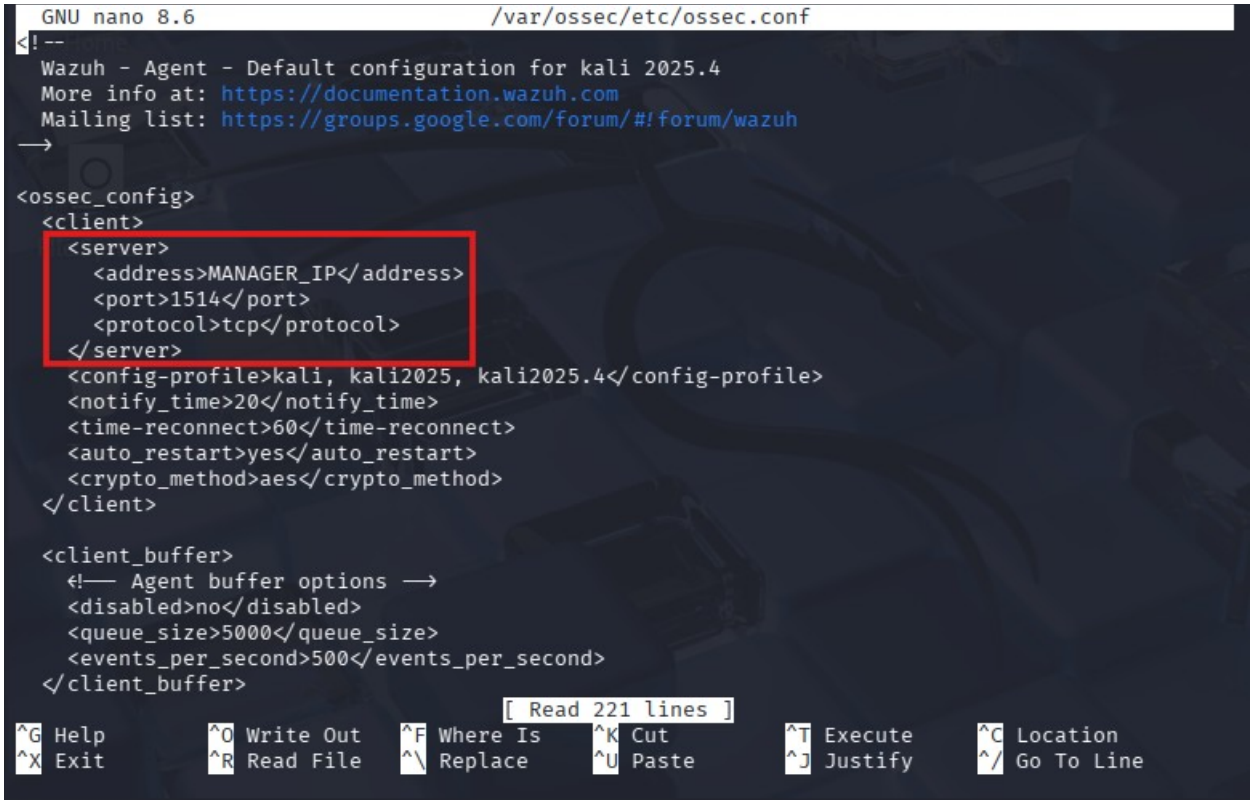
---

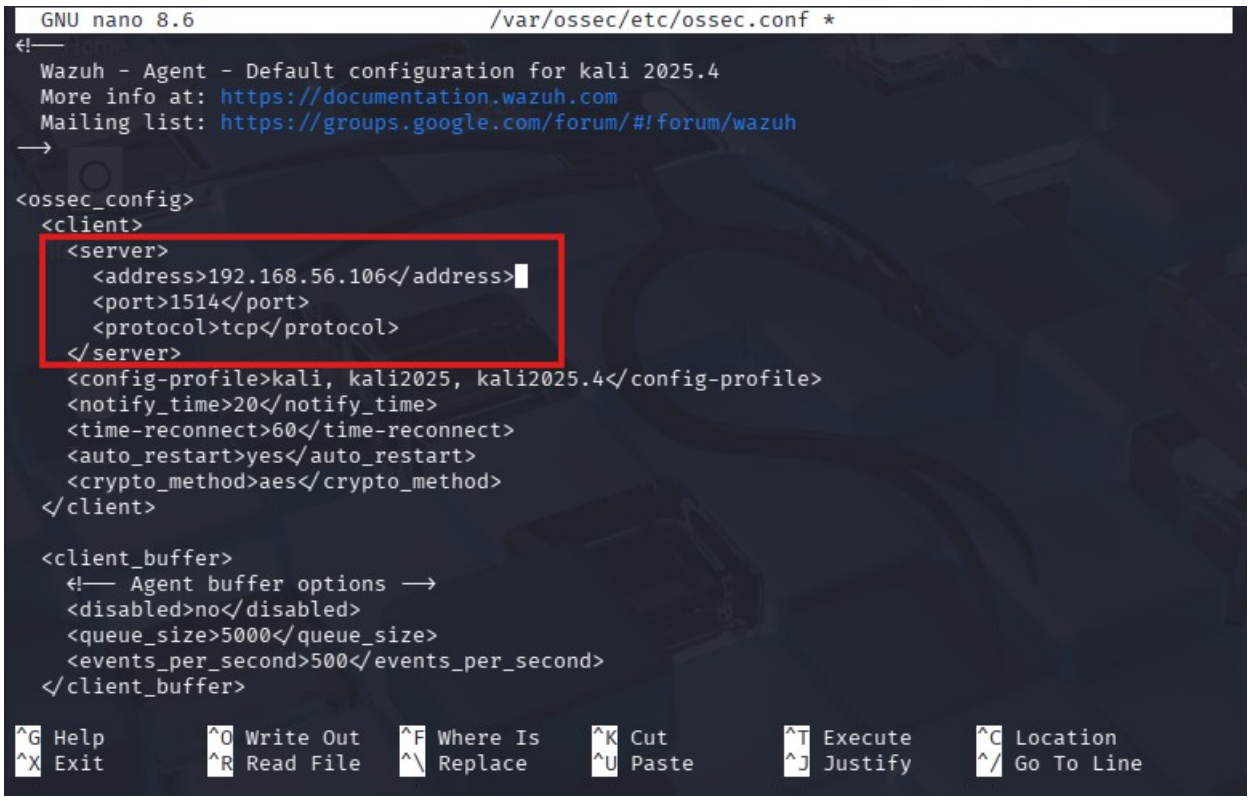
4) Configurazione dell’agent (collegamento al manager)

1. Modifico il file di configurazione dell’agent:

   `sudo nano /var/ossec/etc/ossec.conf`

2. Inserisco l’indirizzo IP della **Wazuh VM** come manager.





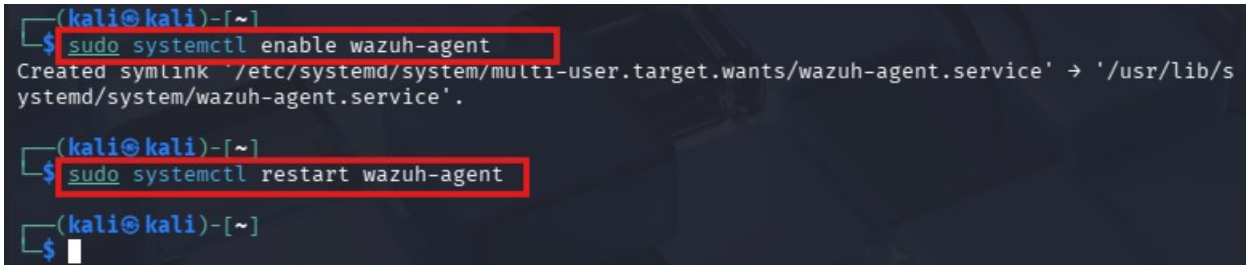
3. Salvo la configurazione ed esco (**Ctrl + O** poi **Invio** poi **Ctrl + X**)

---

5) Enrollment e avvio del Wazuh Agent

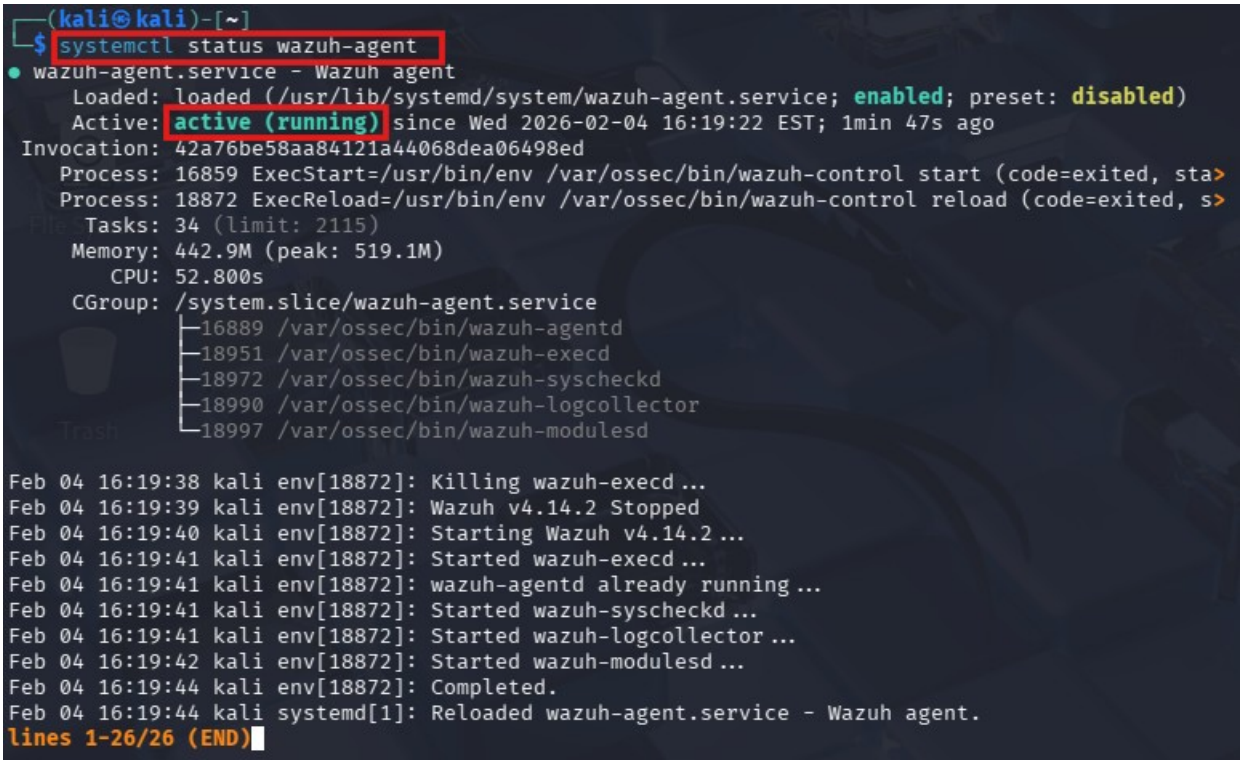
1. Procedo con la registrazione (enrollment) dell'agent seguendo la procedura prevista per endpoint Linux.
2. Avvio e abilito il servizio:

```
sudo systemctl enable wazuh-agent
sudo systemctl restart wazuh-agent
```



3. Verifico che l'agent sia correttamente in esecuzione:

```
systemctl status wazuh-agent
```

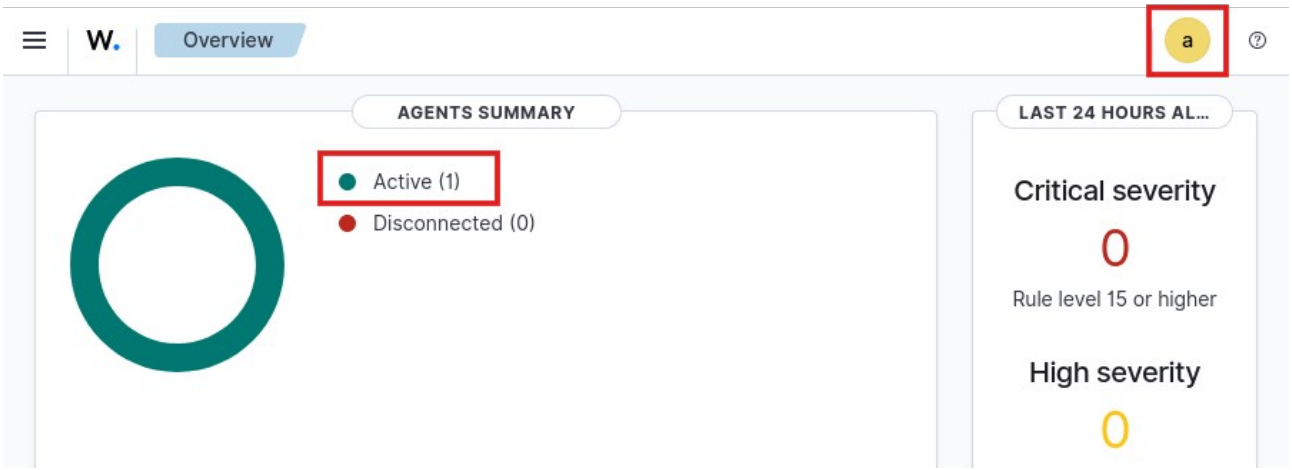


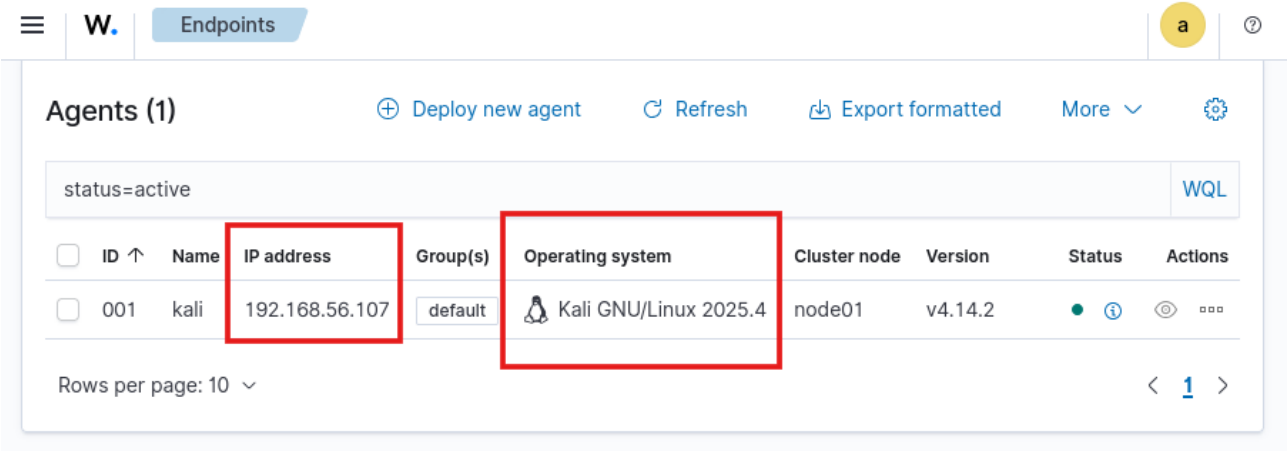
Output dell’agent correttamente in esecuzione

---

6) Verifica dell’agent nella dashboard Wazuh

1. Accedo nuovamente alla dashboard Wazuh (User e Password admin)
2. Apro la sezione **Agents**.
3. Verifico che l’agent installato su Kali Linux risulti:
    - Presente
    - Attivo (status *Active*)
    - Con informazioni coerenti su sistema operativo e indirizzo IP





---

7) Analisi delle prime informazioni raccolte

1. Osservo le informazioni iniziali fornite da Wazuh:
    - Stato dell'agent
    - Dati di inventario del sistema
    - Eventi di base e log di sistema
2. Genero attività lecite su Kali Linux (aggiornamento pacchetti, creazione di file) per stimolare la raccolta di eventi:

```
sudo apt update
echo "test wazuh" | sudo tee /tmp/wazuh_test.txt
```

3. Verifico nella dashboard Wazuh la comparsa dei primi eventi associati all'agent Kali.

Come previsto, la quantità di informazioni iniziali è limitata e richiederebbe configurazioni avanzate aggiuntive non richieste dall'esercizio.

Conclusioni

In questo esercizio ho installato e configurato correttamente un sistema **Wazuh SIEM/XDR** in ambiente di laboratorio.

Ho collegato una macchina **Kali Linux** come endpoint monitorato tramite Wazuh Agent, verificandone lo stato attivo e la corretta comunicazione con il manager.

L'attività ha permesso di comprendere il funzionamento di base di una soluzione SIEM/XDR, il ruolo degli agent e l'importanza della raccolta centralizzata dei log e degli eventi di sicurezza, in linea con i concetti di monitoraggio e incident response affrontati.