Report

Realised by :

ELKADI Ayoub

Executive Summary

This project aimed to design and deploy a Mini SOC environment using Wazuh as a SIEM on a Docker Swarm cluster.

The solution integrates automation with Ansible, Docker Swarm, and Traefik for reverse proxy and SSL termination.

The goal was also to implement a custom Wazuh rule to detect suspicious SSH login patterns.

While the Wazuh Indexer and Manager were deployed successfully in Docker Swarm,

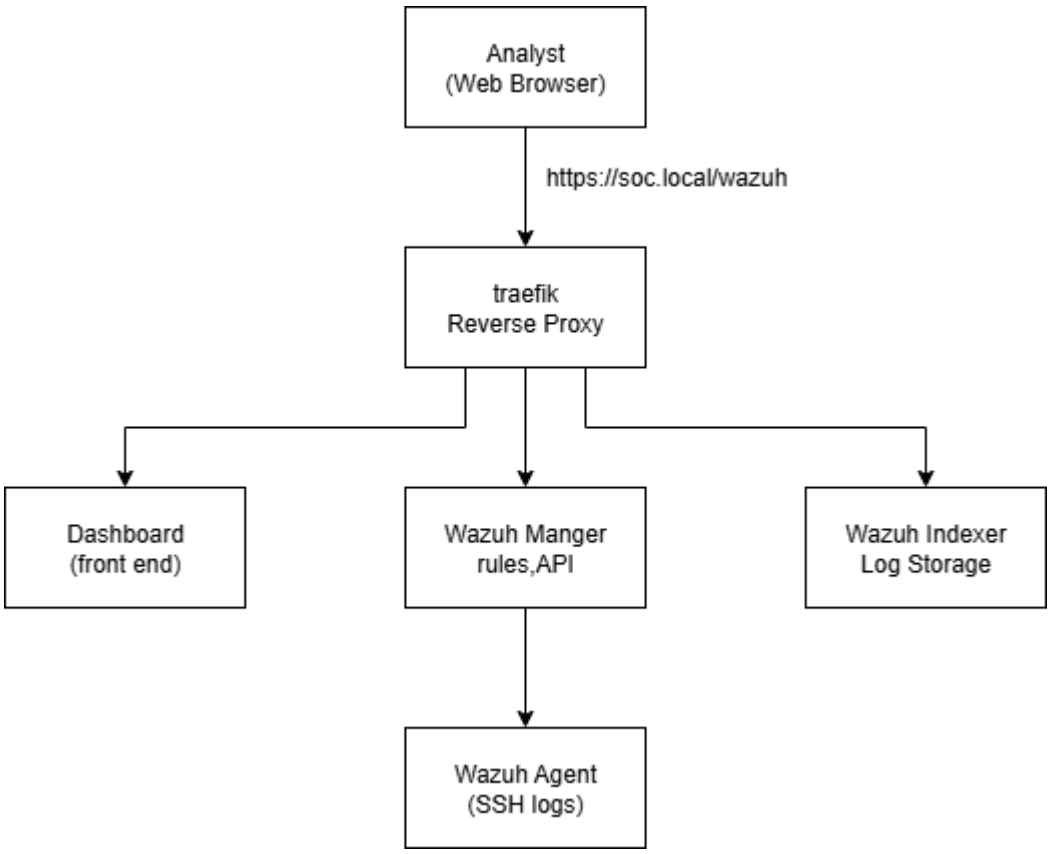
an issue with the OpenSearch security index prevented full initialization of the Wazuh Dashboard.

As a result, the custom detection rule could not be tested in the interface.

Nevertheless, the project demonstrates a functional CI/CD pipeline,

deployment automation, and strong architectural design.

Future work involves resolving the indexer issue and validating detection rules.



Architecture Overview

The architecture consists of a Docker Swarm cluster running the following services:

- Wazuh Indexer (OpenSearch)

- Wazuh Manager

- Wazuh Dashboard

- Traefik (reverse proxy with SSL)

Automation is managed with Ansible playbooks (deploy and teardown).

Certificates for secure communication were generated and mounted into containers.

Workflow:

Developer → GitHub Repository (CI/CD) → Ansible → Docker Swarm → Wazuh Stack

Technical Walkthrough:

I. Part One – Mini SOC Deployment

Used Ansible to automate deployment:

ansible/playbooks/deploy.yml

ansible/playbooks/teardown.yml

```
manager1                   : ok=8    changed=1    unreachable=0    failed=0
skipped=0    rescued=0    ignored=0
```

```
(venv) ayoub@ayoub-VMware-Virtual-Platform:~/Desktop/mini-soc-wazuh-final$ ansi
ble-playbook ansible/playbooks/deploy.yml -i ansible/inventories/hosts.ini

PLAY [Bootstrap Swarm and deploy stack] ************************************
*

TASK [Gathering Facts] *****************************************************
*
ok: [manager1]

TASK [Ensure Docker is running] ********************************************
*
ok: [manager1]

TASK [Initialize Docker Swarm (if not already)] ****************************
*
ok: [manager1]

TASK [Ensure overlay network exists] ***************************************
*
ok: [manager1]
```

Docker Swarm stack file (stack/wazuh-stack.yml) defines services:

Wazuh Indexer with SSL

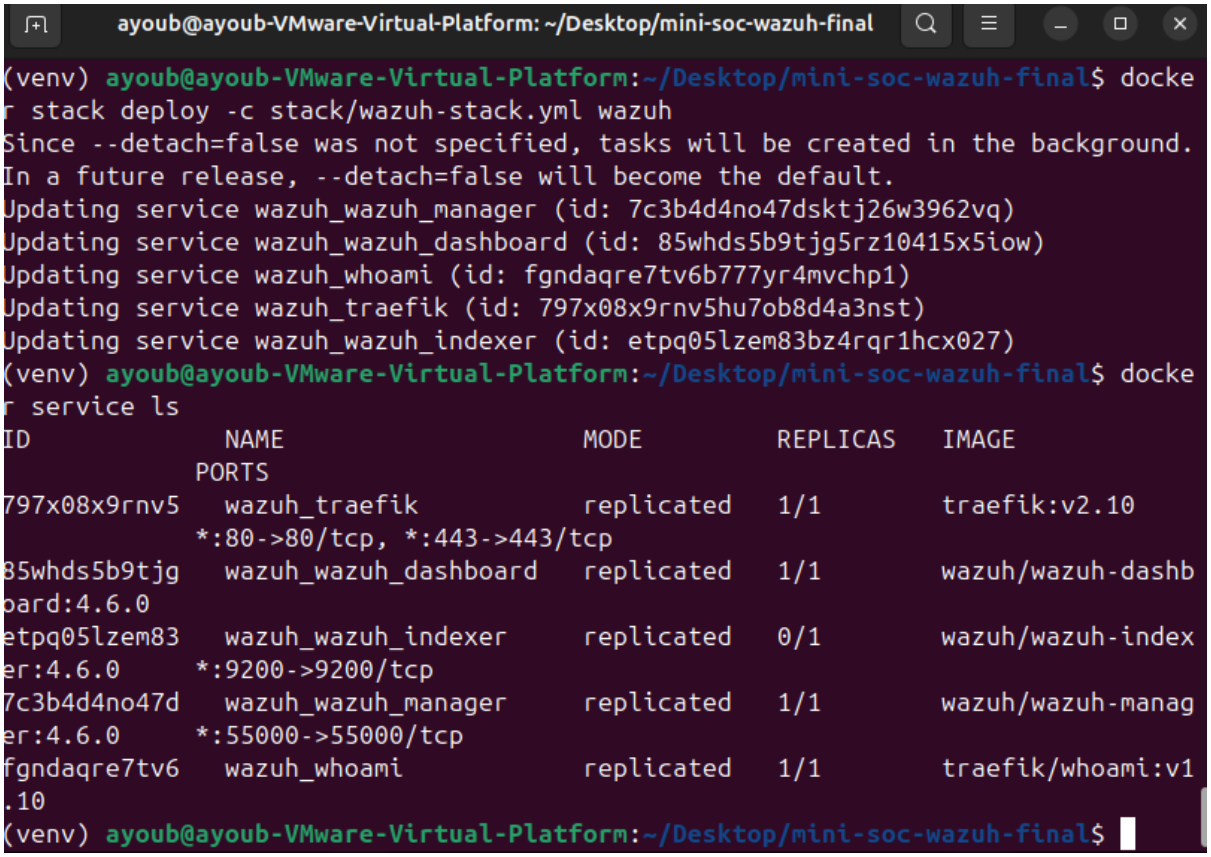
Wazuh Manager

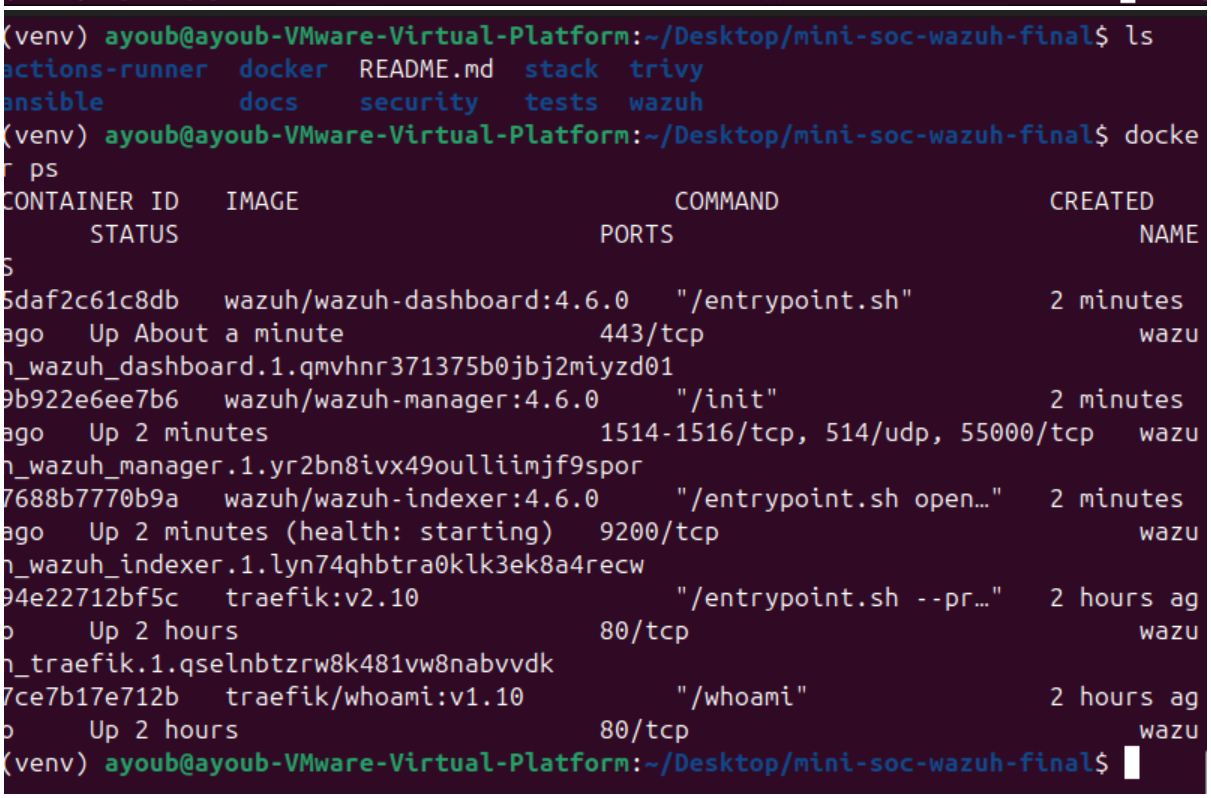
Wazuh Dashboard

Traefik for HTTPS routing

Certificates generated under stack/config/wazuh_indexer_ssl_certs/

Deployment tested with: docker stack deploy -c stack/wazuh-stack.yml wazuh


ayoub@ayoub-VMware-Virtual-Platform: ~/Desktop/mini-soc-wazuh-final
(venv) ayoub@ayoub-VMware-Virtual-Platform:~/Desktop/mini-soc-wazuh-final$ docke
r stack deploy -c stack/wazuh-stack.yml wazuh
Since --detach=false was not specified, tasks will be created in the background.
In a future release, --detach=false will become the default.
Updating service wazuh_wazuh_manager (id: 7c3b4d4no47dsktj26w3962vq)
Updating service wazuh_wazuh_dashboard (id: 85whds5b9tjg5rz10415x5iow)
Updating service wazuh_whoami (id: fgndaqre7tv6b777yr4mvchp1)
Updating service wazuh_traefik (id: 797x08x9rnv5hu7ob8d4a3nst)
Updating service wazuh_wazuh_indexer (id: etpq05lzem83bz4rqr1hcx027)
(venv) ayoub@ayoub-VMware-Virtual-Platform:~/Desktop/mini-soc-wazuh-final$ docke
r service ls
ID NAME MODE REPLICAS IMAGE
PORTS
797x08x9rnv5 wazuh_traefik replicated 1/1 traefik:v2.10
*:80->80/tcp, *:443->443/tcp
85whds5b9tjg wazuh_wazuh_dashboard replicated 1/1 wazuh/wazuh-dashb
oard:4.6.0
etpq05lzem83 wazuh_wazuh_indexer replicated 0/1 wazuh/wazuh-index
er:4.6.0 *:9200->9200/tcp
7c3b4d4no47d wazuh_wazuh_manager replicated 1/1 wazuh/wazuh-manag
er:4.6.0 *:55000->55000/tcp
fgndaqre7tv6 wazuh_whoami replicated 1/1 traefik/whoami:v1
.10
(venv) ayoub@ayoub-VMware-Virtual-Platform:~/Desktop/mini-soc-wazuh-final$


(venv) ayoub@ayoub-VMware-Virtual-Platform:~/Desktop/mini-soc-wazuh-final$ ls
actions-runner docker README.md stack trivy
ansible docs security tests wazuh
(venv) ayoub@ayoub-VMware-Virtual-Platform:~/Desktop/mini-soc-wazuh-final$ docke
r ps
CONTAINER ID IMAGE COMMAND CREATED
STATUS PORTS NAME
S
5daf2c61c8db wazuh/wazuh-dashboard:4.6.0 "/entrypoint.sh" 2 minutes
ago Up About a minute 443/tcp wazu
h_wazuh_dashboard.1.qmvhnr371375b0jbj2miyzd01
9b922e6ee7b6 wazuh/wazuh-manager:4.6.0 "/init" 2 minutes
ago Up 2 minutes 1514-1516/tcp, 514/udp, 55000/tcp wazu
h_wazuh_manager.1.yr2bn8ivx49oulliimjf9spor
7688b7770b9a wazuh/wazuh-indexer:4.6.0 "/entrypoint.sh open…" 2 minutes
ago Up 2 minutes (health: starting) 9200/tcp wazu
h_wazuh_indexer.1.lyn74qhbtra0klk3ek8a4recw
94e22712bf5c traefik:v2.10 "/entrypoint.sh --pr…" 2 hours ag
o Up 2 hours 80/tcp wazu
h_traefik.1.qselnbtzrw8k481vw8nabvvdk
7ce7b17e712b traefik/whoami:v1.10 "/whoami" 2 hours ag
o Up 2 hours 80/tcp wazu
(venv) ayoub@ayoub-VMware-Virtual-Platform:~/Desktop/mini-soc-wazuh-final$

```
(venv) ayoub@ayoub-VMware-Virtual-Platform:~/Desktop/mini-soc-wazuh-final$ cat
stack/securityconfig/internal_users.yml | head -n 20
_meta:
  type: "internalusers"
  config_version: 2

admin:
  hash: "$2y$12$yF6hWBV7p9oVj2OD4lM9oeH5jk7GoJ3YFwp4XZJkksGdiyMy9HbRu" # passwo
rd: admin
  reserved: true
  backend_roles:
    - "admin"
  description: "Admin user"
```

Part Two – Threat Detection Rule :

The goal was to create a Wazuh custom rule to detect suspicious SSH login behavior:

- Multiple failed attempts from the same source

- Followed by a successful login with a new user

The rule was prepared in the Wazuh Manager configuration but could not be validated due to the dashboard issue.

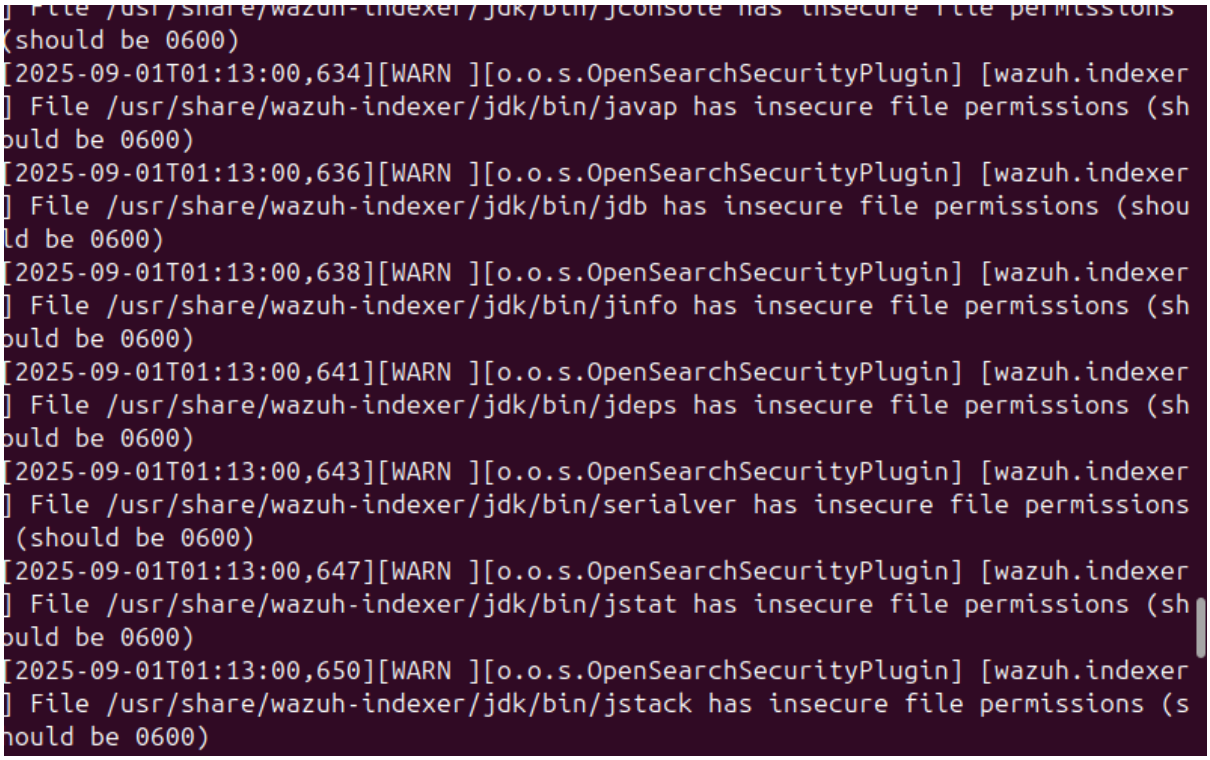
```
(venv) ayoub@ayoub-VMware-Virtual-Platform:~/Desktop/mini-soc-wazuh-final/wazuh/
rules$ cat local_rules.xml
<group name="local,ssh,">
  <!-- Detect multiple failed SSH login attempts -->
  <rule id="100001" level="5">
    <if_sid>5710</if_sid>
    <frequency>3</frequency>
    <timeframe>120</timeframe>
    <description>Multiple failed SSH login attempts detected</description>
    <group>authentication_failed,</group>
  </rule>

  <!-- Detect a successful login after failed attempts -->
  <rule id="100002" level="10">
    <if_sid>5712</if_sid>
    <predec_rule>100001</predec_rule>
    <description>Suspicious SSH activity: failed logins followed by success</des
cription>
    <group>authentication_success,</group>
  </rule>
</group>
```

Issues Faced:

- Wazuh Indexer failed with ".opendistro_security index missing".
- This blocked Wazuh Dashboard from starting correctly.

- Limited time to troubleshoot indexer security initialization.



Next Steps:

- Run securityadmin.sh to initialize OpenSearch security index.
- Validate custom SSH detection rule.
- Add Trivy scanning in pipeline.
- Complete end-to-end SOC workflow with alerts visible in dashboard.

Conclusion:

Despite the dashboard issue, the project demonstrates:

- Infrastructure as Code (Ansible + Docker Swarm)

- Secure deployment with certificates

- CI/CD-ready GitHub repo

- Understanding of SOC architecture and detection logic

Future debugging will enable full alert validation.