National College of Ireland

Configuration Manual

MSc Research Project
MSC Cyber Security

Ayush Dharmesh Shah
Student ID: X23272741

School of Computing
National College of Ireland

Supervisor: Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Ayush Dharmesh Shah		
Student ID:	X23272741		
Programme:	MSC cybersecurity	**Year:**	2024-2025
Module:	MSC Research Project		
Lecturer:	Vikas Sahni		
Submission Due Date:	11th Aug 2025		
Project Title:	Zero trust architecture a proactive defence framework to mitigate phishing based ransomware attacks		
Word Count:	1226 words	**Page Count:**	14

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Ayush Dharmesh Shah

Date: 11th August 2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Ayush Dharmesh Shah
Student ID: x23272741

1 Introduction

This configuration manual documents the configuration steps which are necessary for implementing a practical approach of ZTA environment and focuses on preventing and detecting phishing ransomware attacks. While the environmental setup covers core core component like ZTA controller (Keycloak+Pomerium), SIEM monitor (Wazuh), Attack Simulation (Kali Linux), and victim (Windows Server).

2 System Overview

Components	**Description**	**CPU**	**RAM**	**Storage**	**OS**	**Network Adaptors**
ZTA Controller	Ubuntu Linux VM with pomerium for ZTNA VPN access, key cloak (Identity access management provider)	4	8 GB	60 GB	Ubuntu 22.04 LTS	**Adaptor 1:** Internal Network **Adaptor 2:** Internal network **Adaptor 3:** NAT
SIEM Monitor	Ubuntu Linux VM with Wazuh Manager and Dashboard	4	8 GB	100 GB	Ubuntu 22.04 LTS	**Adaptor 1:** Internal Network **Adaptor 2:** Internal network **Adaptor 3:** NAT
Attacker VM	Kali Linux with tools like Hydra	2	4 GB	40 GB	Kali Linux 2024.03	**Adaptor 1:** Internal Network **Adaptor 2:** Internal network **Adaptor 3:** NAT

Victim VM	Windows server with Wazuh agent	2	4 GB	40 GB	Windows Server 2022 21H2	**Adaptor 1:** Internal Network **Adaptor 2:** Internal network **Adaptor 3:** NAT

3 Environmental Setup

3.1 Installation and configuration of Keycloak on ZTA controller VM

The installation process of key cloak primarily involved updating of server packages installation of Java JDK downloading the key cloak latest version from GitHub extraction of the file and configuring the key cloak server after which key cloak service was and service was started.

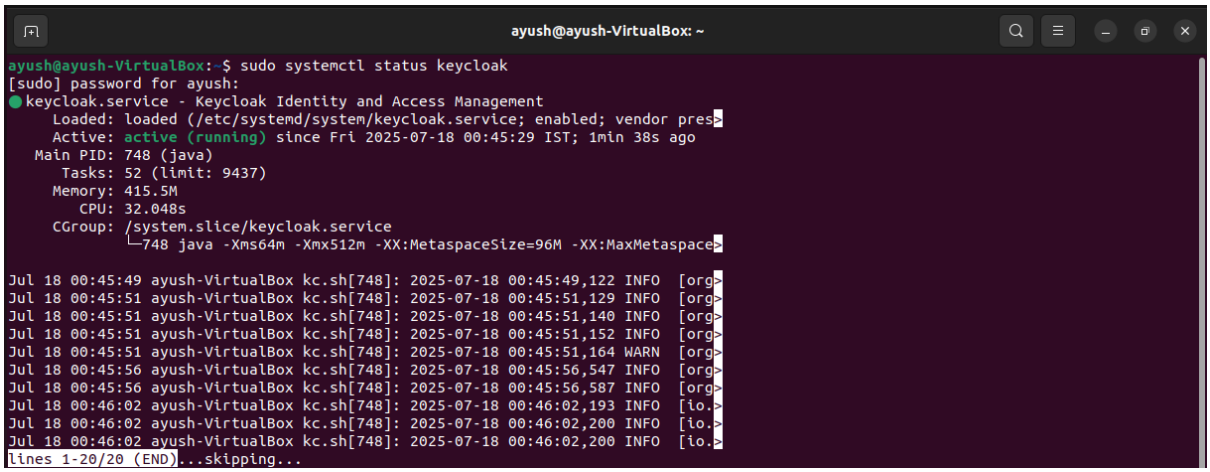

Figure 1 Successful installation of Keycloak

Configurations:

Step 1 Realm Creation:

1. Log in to the Admin Console as the admin user.
2. In the top-left realm selector, click Add realm.
3. Enter Realm Name: zero-trust-realm and click Create.
4. Under Realm Settings → General, verify:
   - User registration: Off
   - Email verification: On
   - Forgot password: On
   - Remember me: Off
   - Login with email: Off
5. Save changes.

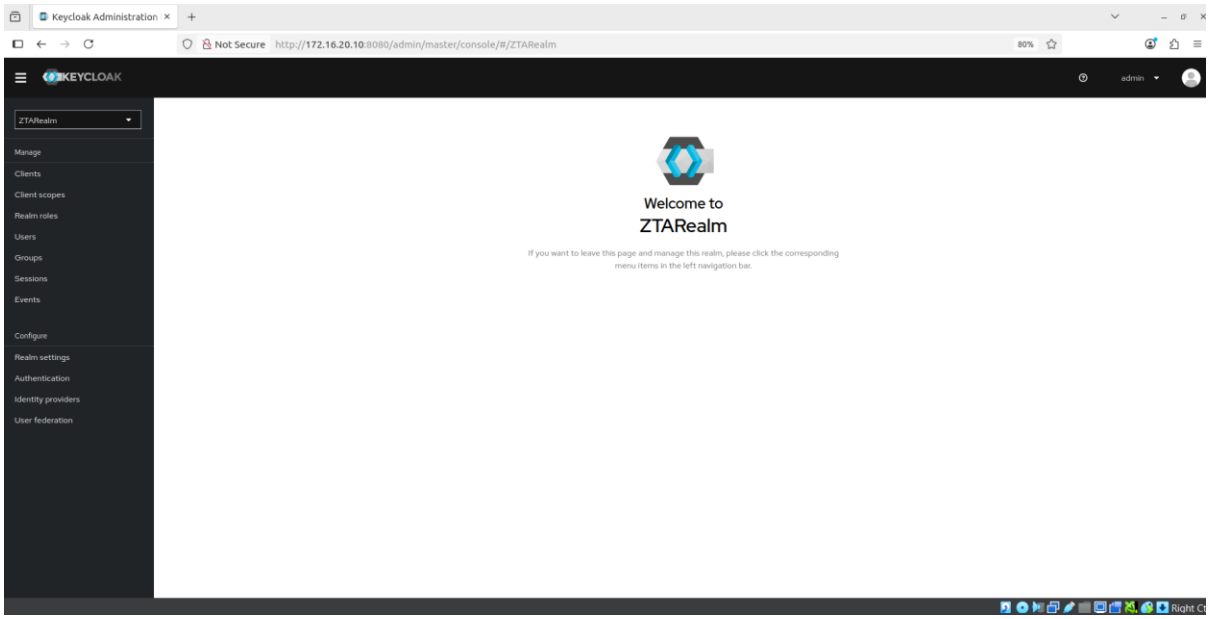

Figure 2 ZTA Realm Creation

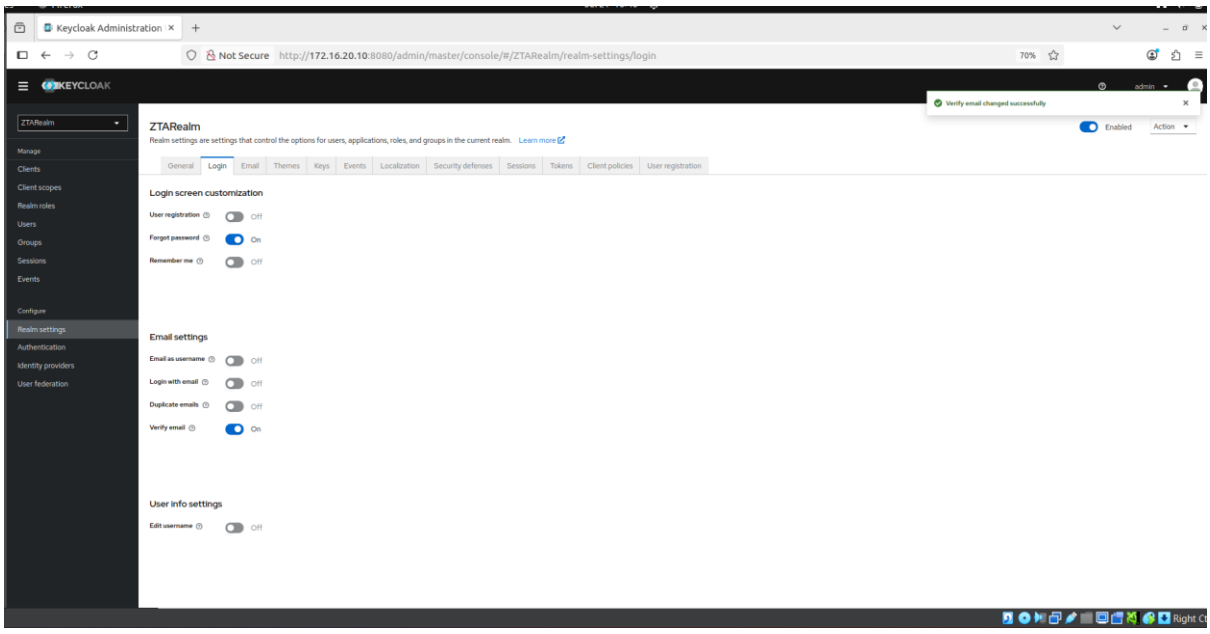

Figure 3 General Setting Configuration

Step 2: Enforce Secure HTTP headers

Realm Settings → Security Defences → Headers.

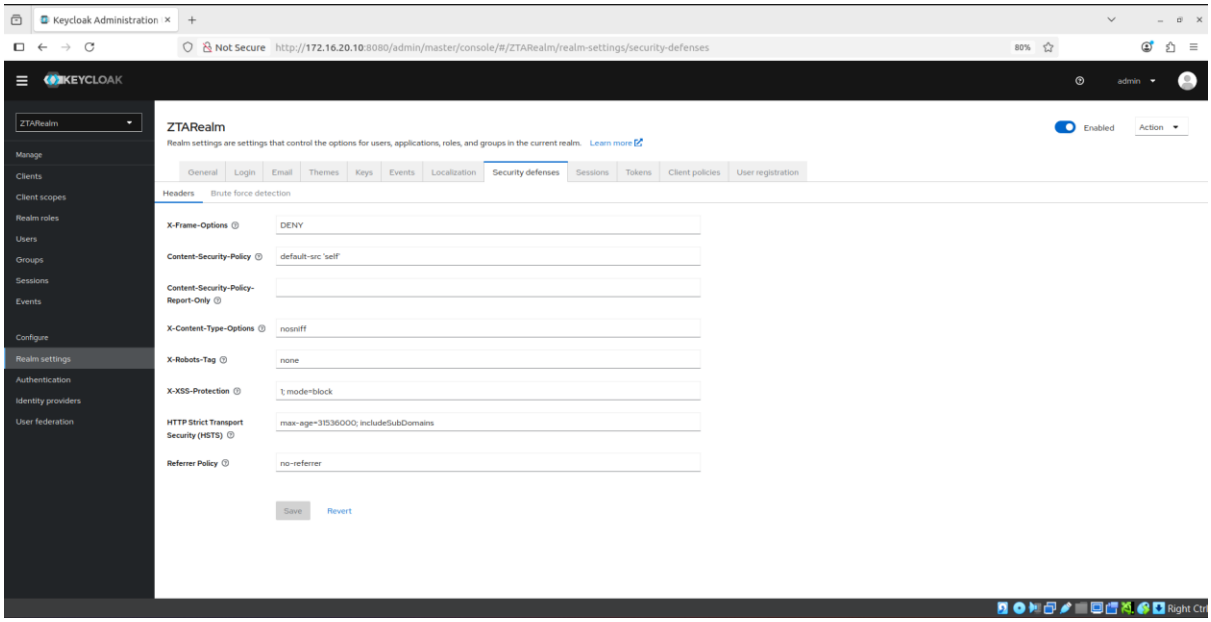

Figure 4 HTTP Header Configuration

Step 3: Configuring MFA

Go to Authentication → Required Actions, enable Configure OTP, then click Save.

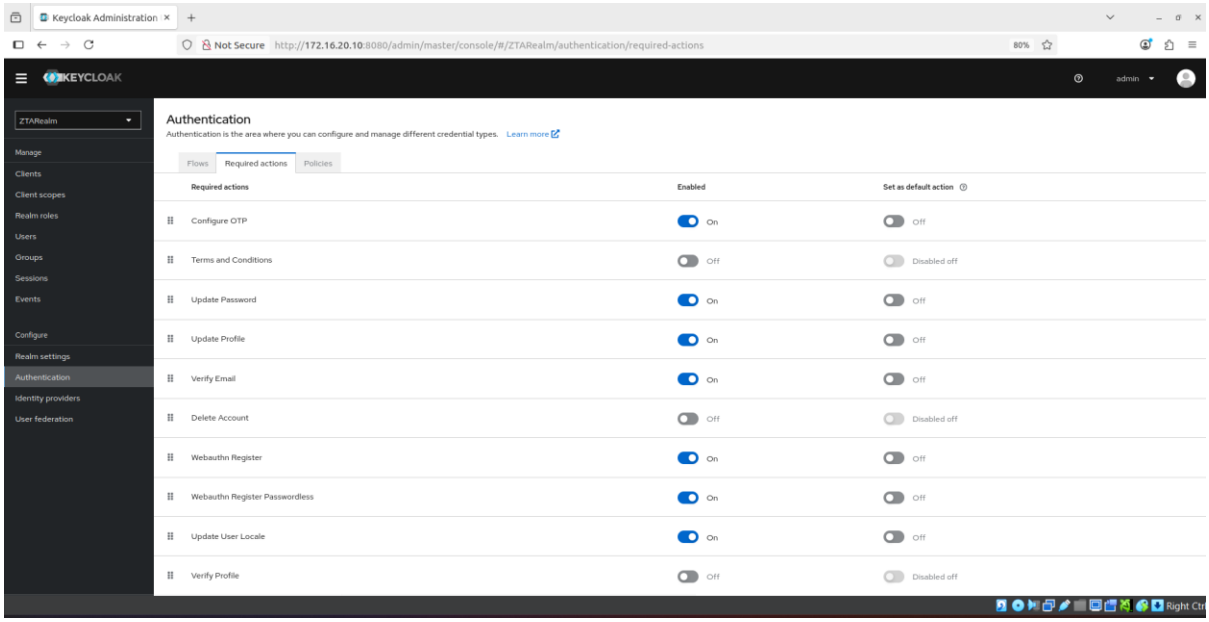

Figure 5 MFA Enablement

Multifactor authentication browser flow created

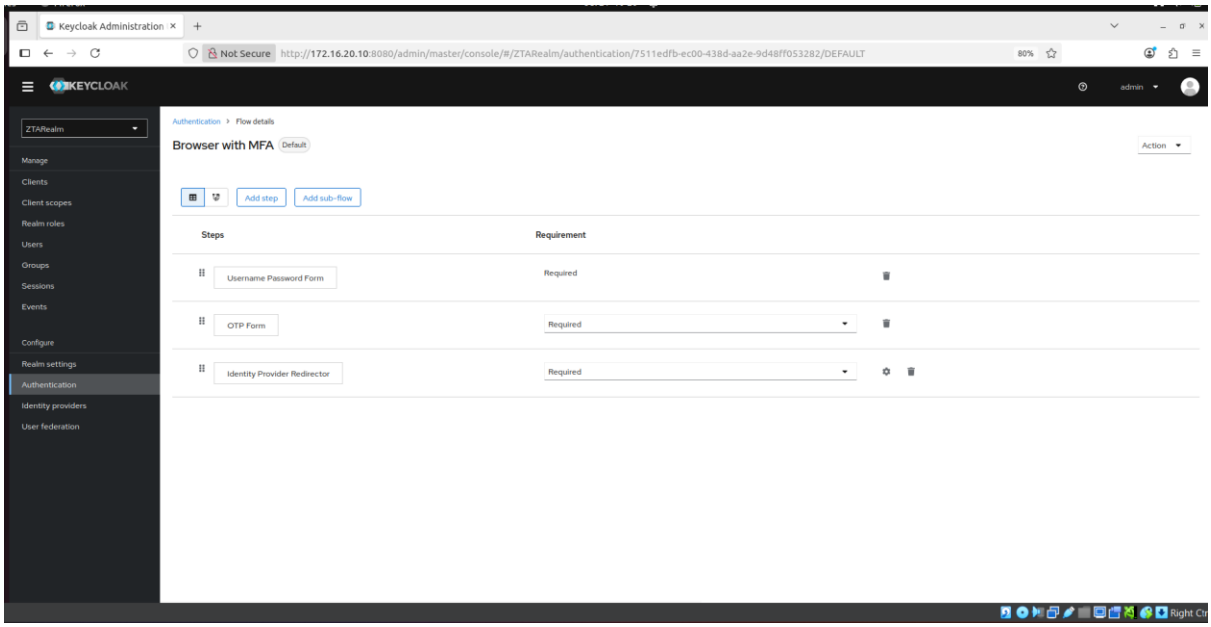

Figure 6 Browser with MFA flow

Step 4: Enforcing strong password policies

Navigate to Authentication → Password Policy.

- Minimum Length: 12
- Digits: 2
- Lowercase Characters: 2
- Uppercase Characters: 2
- Special Characters: 2
- Not Recent Reuse: 5
- Expire Password: 90 days
- Not Username and Not Email (prevent trivial passwords)

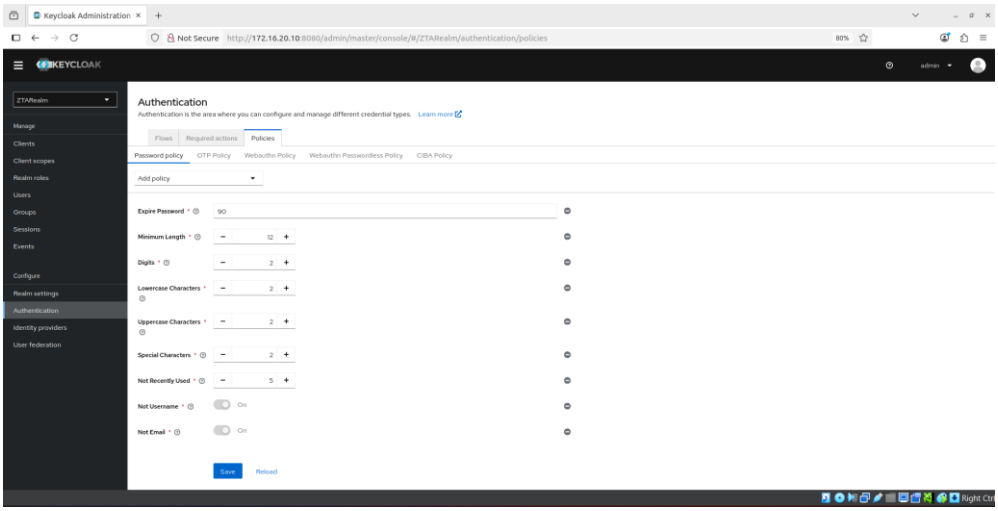

Figure 7 Password Policy Configuration

Step 5: Enabling Brute force Protection

1. Go to Realm Settings → Security Defenses → Brute Force Detection.
2. Toggle Enabled to On and configure:

- Max Login Failures: 5
- Wait Increment (seconds): 60
- Minimum Quick Login Wait (ms): 1000
- Maximum Wait (seconds): 900
- Failure Reset Time (seconds): 3600
- Click Save

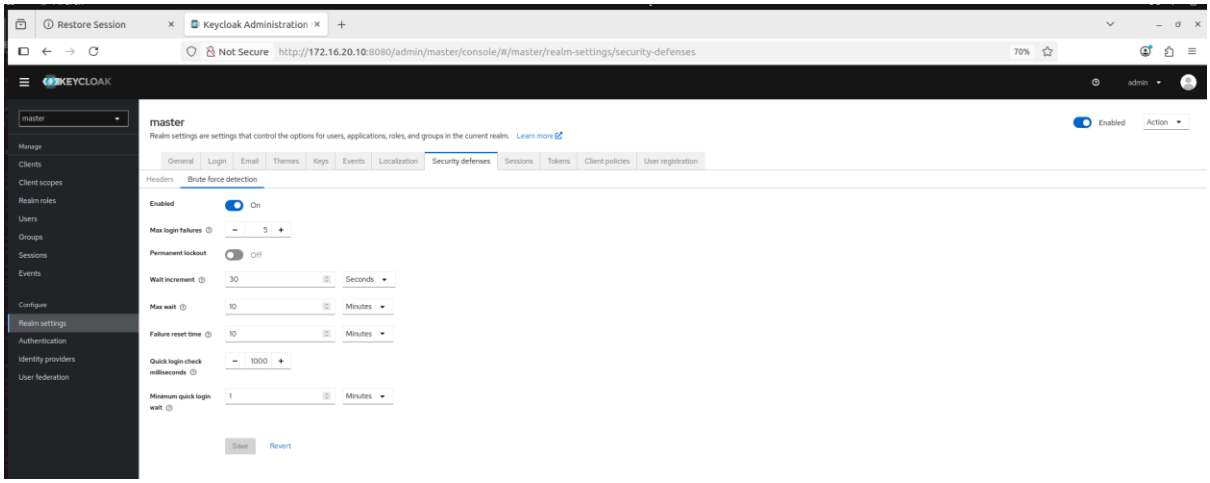

Figure 8 Brute Force Configuration

3.2 Installation and configuration of pomerium on ZTA controller VM

For Installation of pomerium I firstly updated the system and installed its dependencies on the Ubuntu VM , then I added Pomerium official repository on my system and imported its GPG key and installed pomerium

Configuration:

Step 1 : Generating the required secret keys like shared secret , cookie secret for pomerium config yaml file

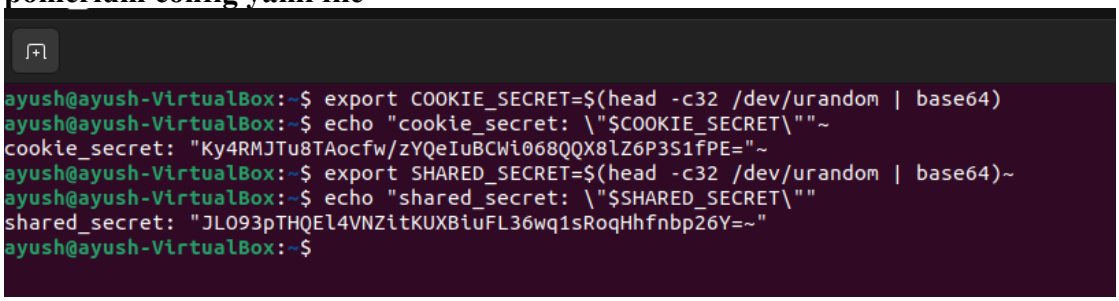

Figure 9 Extraction of Secret keys

Step2 : Adding the required informantion in the config.yaml file of pomerium and configuring it as per requirements

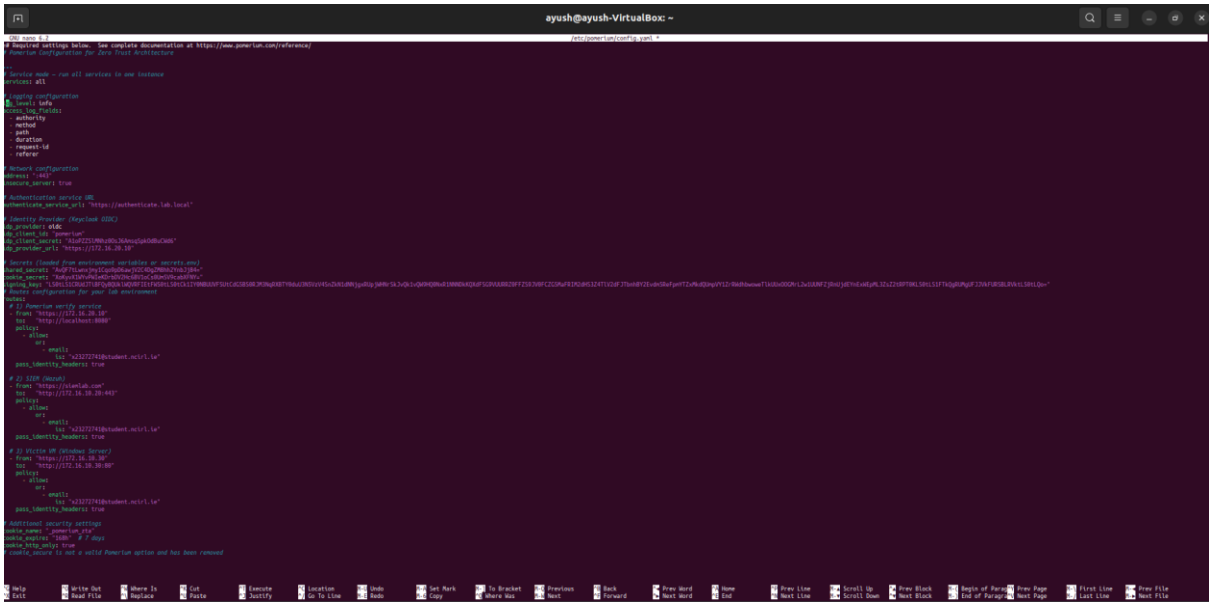

Figure 10 Pomerium Config File

Step 3:After editing the config file the agent was restrated and status was active and running

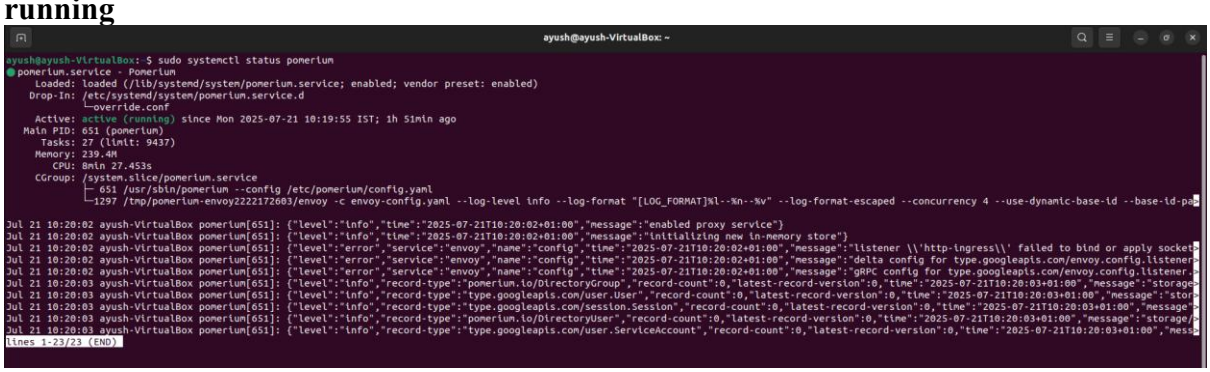

Figure 11 Pomerium Is Up and running

3.3 Installation and configuration of Wazuh SIEM

Step 1 : Installation of wazuh on ubuntu VM

With this command from wazuh official documentation I was able to install wazuh on my SIEM monitor VM

Command: curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh && sudo bash ./wazuh-install.sh -a

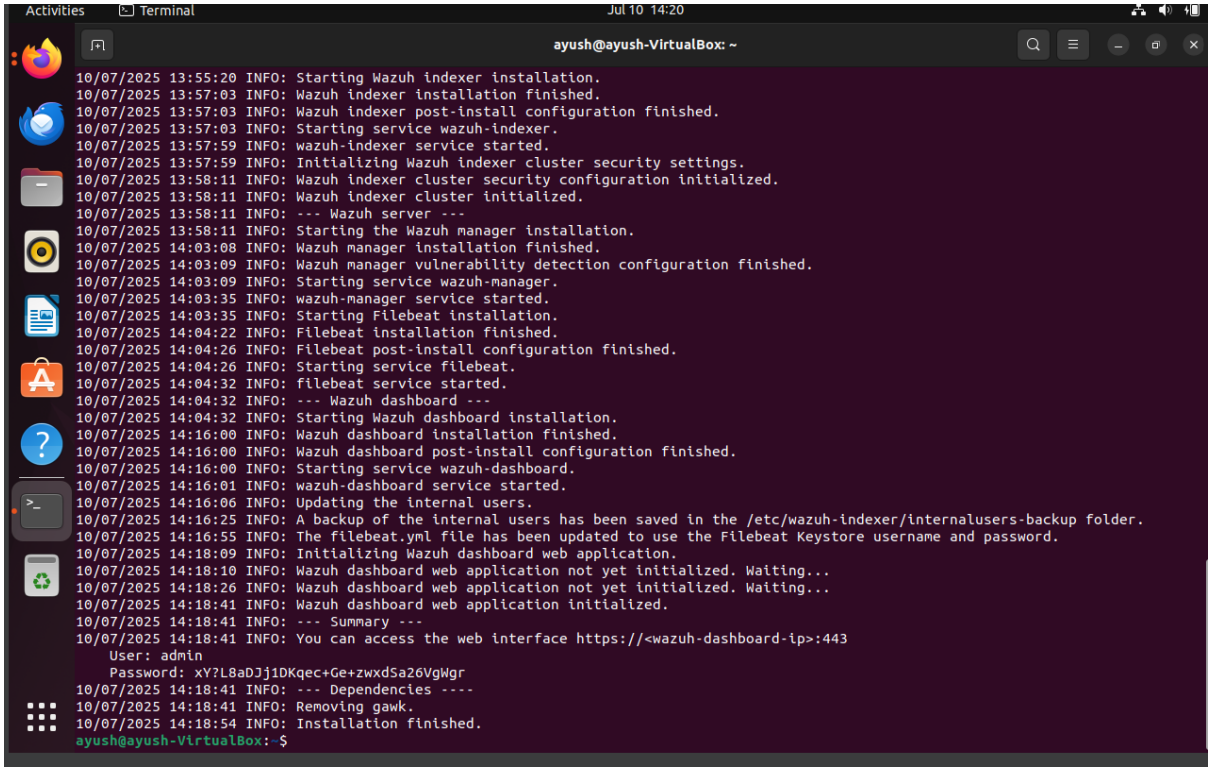

Figure 12 Successful Installation of Wazuh

Step 2: Checking wazuh components like wazuh manager , wazuh dashboard , wazuh indexer is active and running

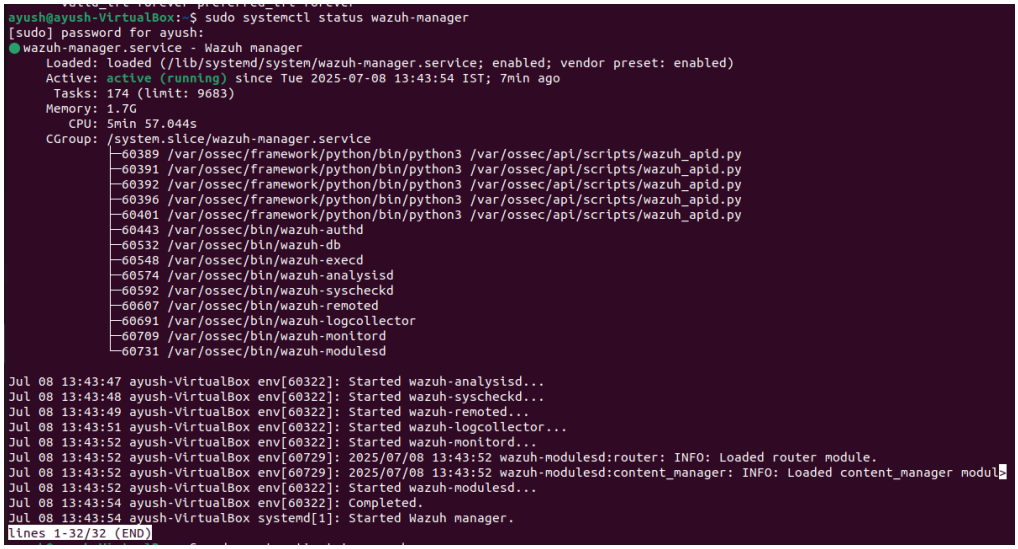

Figure 13 Wazuh Manager Active

```
ayush@ayush-VirtualBox:~$ sudo systemctl status wazuh-indexer
● wazuh-indexer.service - wazuh-indexer
     Loaded: loaded (/lib/systemd/system/wazuh-indexer.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2025-07-08 13:22:16 IST; 30min ago
       Docs: https://documentation.wazuh.com
   Main PID: 6315 (java)
      Tasks: 86 (limit: 9683)
     Memory: 1.4G
        CPU: 7min 6.282s
     CGroup: /system.slice/wazuh-indexer.service
             └─6315 /usr/share/wazuh-indexer/jdk/bin/java -Xshare:auto -Dopensearch.networkaddress.cache.ttl=60 -Dopensearch.networ>

Jul 08 13:21:43 ayush-VirtualBox systemd-entrypoint[6315]: WARNING: System::setSecurityManager has been called by org.opensearch.bo>
Jul 08 13:21:43 ayush-VirtualBox systemd-entrypoint[6315]: WARNING: Please consider reporting this to the maintainers of org.opense>
Jul 08 13:21:43 ayush-VirtualBox systemd-entrypoint[6315]: WARNING: System::setSecurityManager will be removed in a future release
Jul 08 13:21:45 ayush-VirtualBox systemd-entrypoint[6315]: Jul 08, 2025 1:21:45 PM sun.util.locale.provider.LocaleProviderAdapter <>
Jul 08 13:21:45 ayush-VirtualBox systemd-entrypoint[6315]: WARNING: COMPAT locale provider will be removed in a future release
Jul 08 13:21:46 ayush-VirtualBox systemd-entrypoint[6315]: WARNING: A terminally deprecated method in java.lang.System has been cal>
Jul 08 13:21:46 ayush-VirtualBox systemd-entrypoint[6315]: WARNING: System::setSecurityManager has been called by org.opensearch.bo>
Jul 08 13:21:46 ayush-VirtualBox systemd-entrypoint[6315]: WARNING: Please consider reporting this to the maintainers of org.opense>
Jul 08 13:21:46 ayush-VirtualBox systemd-entrypoint[6315]: WARNING: System::setSecurityManager will be removed in a future release
Jul 08 13:22:16 ayush-VirtualBox systemd[1]: Started wazuh-indexer.
lines 1-21/21 (END)
```

Figure 14 Wazuh Indexer Active

```
ayush@ayush-VirtualBox:~$ sudo systemctl status wazuh-dashboard
● wazuh-dashboard.service - wazuh-dashboard
     Loaded: loaded (/etc/systemd/system/wazuh-dashboard.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2025-07-08 13:44:02 IST; 9min ago
   Main PID: 61463 (node)
      Tasks: 11 (limit: 9683)
     Memory: 187.2M
        CPU: 1min 1.262s
     CGroup: /system.slice/wazuh-dashboard.service
             └─61463 /usr/share/wazuh-dashboard/node/bin/node --no-warnings --max-http-header-size=65536 --unhandled-rejections=war>

Jul 08 13:44:50 ayush-VirtualBox opensearch-dashboards[61463]: {"type":"log","@timestamp":"2025-07-08T12:44:50Z","tags":["info","pl>
Jul 08 13:44:51 ayush-VirtualBox opensearch-dashboards[61463]: {"type":"log","@timestamp":"2025-07-08T12:44:51Z","tags":["listening>
Jul 08 13:44:52 ayush-VirtualBox opensearch-dashboards[61463]: {"type":"log","@timestamp":"2025-07-08T12:44:52Z","tags":["info","ht>
Jul 08 13:44:52 ayush-VirtualBox opensearch-dashboards[61463]: {"type":"log","@timestamp":"2025-07-08T12:44:52Z","tags":["info","pl>
Jul 08 13:44:52 ayush-VirtualBox opensearch-dashboards[61463]: {"type":"log","@timestamp":"2025-07-08T12:44:52Z","tags":["info","pl>
Jul 08 13:45:01 ayush-VirtualBox opensearch-dashboards[61463]: {"type":"log","@timestamp":"2025-07-08T12:45:01Z","tags":["error","o>
Jul 08 13:45:01 ayush-VirtualBox opensearch-dashboards[61463]: {"type":"log","@timestamp":"2025-07-08T12:45:01Z","tags":["info","pl>
Jul 08 13:45:03 ayush-VirtualBox opensearch-dashboards[61463]: [agentkeepalive:deprecated] options.freeSocketKeepAliveTimeout is de>
Jul 08 13:45:03 ayush-VirtualBox opensearch-dashboards[61463]: {"type":"log","@timestamp":"2025-07-08T12:45:03Z","tags":["info","pl>
Jul 08 13:45:06 ayush-VirtualBox opensearch-dashboards[61463]: {"type":"response","@timestamp":"2025-07-08T12:45:03Z","tags":[],"pi>
lines 1-20/20 (END)
```

Figure 15 Wazuh Dashboard Active

3.3.1 Wazuh Agent installation on ZTA controller and Windows Victim

1) ZTA controller agent installation confirmation

```
ayush@ayush-VirtualBox: ~
ayush@ayush-VirtualBox:~$ sudo systemctl status wazuh-agent
[sudo] password for ayush:
● wazuh-agent.service - Wazuh agent
     Loaded: loaded (/lib/systemd/system/wazuh-agent.service; enabled; vendor preset: enabled)
     Active: active (running) since Mon 2025-07-21 10:20:03 IST; 4h 47min ago
    Process: 914 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
      Tasks: 30 (limit: 9437)
     Memory: 75.1M
        CPU: 1min 952ms
     CGroup: /system.slice/wazuh-agent.service
             ├─1034 /var/ossec/bin/wazuh-execd
             ├─1126 /var/ossec/bin/wazuh-agentd
             ├─1176 /var/ossec/bin/wazuh-syscheckd
             ├─1187 /var/ossec/bin/wazuh-logcollector
             └─1195 /var/ossec/bin/wazuh-modulesd

Jul 21 10:19:58 ayush-VirtualBox env[914]: Deleting PID file '/var/ossec/var/run/wazuh-syscheckd-10111.pid' not used...
Jul 21 10:19:58 ayush-VirtualBox env[914]: Deleting PID file '/var/ossec/var/run/wazuh-agentd-10097.pid' not used...
Jul 21 10:19:58 ayush-VirtualBox env[914]: Deleting PID file '/var/ossec/var/run/wazuh-execd-10086.pid' not used...
Jul 21 10:20:00 ayush-VirtualBox env[914]: Started wazuh-execd...
Jul 21 10:20:01 ayush-VirtualBox env[914]: Started wazuh-agentd...
Jul 21 10:20:01 ayush-VirtualBox env[914]: Started wazuh-syscheckd...
Jul 21 10:20:01 ayush-VirtualBox env[914]: Started wazuh-logcollector...
Jul 21 10:20:01 ayush-VirtualBox env[914]: Started wazuh-modulesd...
Jul 21 10:20:03 ayush-VirtualBox env[914]: Completed.
Jul 21 10:20:03 ayush-VirtualBox systemd[1]: Started Wazuh agent.
ayush@ayush-VirtualBox:~$
```

Figure 16 Wazuh Agent confirmation On ZTA controller

2) Windows Victim wazuh agent installation

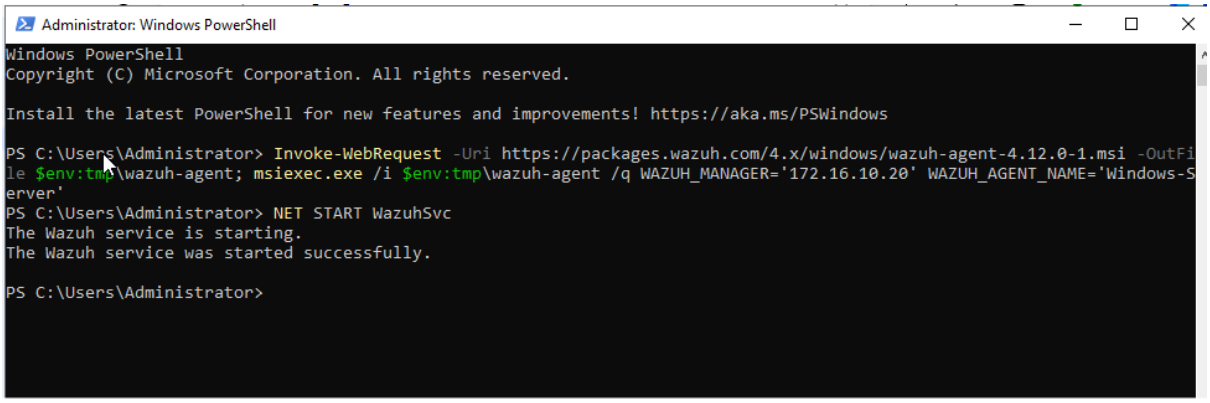

Figure 17 Wazuh Agent confirmation on Windows server

1. 3.3.2 Log Archival Service configuration on wazuh

   Go to **/var/ossec/etc/ossec.conf on the terminal and edit line**

   <logall>yes</logall>
   <logall_json>yes</logall_json>

   The above two lines were changed from no to yes for turning on log archival service on widows server

   After which the wazuh dashboard was accessed and the below mentioned steps were performed to get real time logs
   1.In the Wazuh Dashboard, click the menu icon (☰) and navigate to Dashboard management → Index patterns.

2. Click Create index pattern.
3. Enter wazuh-archives-* as the index pattern name.
4. Choose timestamp (not @timestamp) as the Time field.
5. Click Create index pattern to save

.

View Archive Logs in Discover

1. Click the menu icon (☰) and select Discover.
2. From the index pattern dropdown (top left), choose wazuh-archives-*.
3. Use the time picker to set your desired time range.

```
<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>yes</logall>
    <logall_json>yes</logall_json>
    <email_notification>no</email_notification>
    <smtp_server>smtp.example.wazuh.com</smtp_server>
    <email_from>wazuh@example.wazuh.com</email_from>
    <email_to>recipient@example.wazuh.com</email_to>
    <email_maxperhour>12</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
    <agents_disconnection_time>10m</agents_disconnection_time>
    <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
    <update_check>yes</update_check>
  </global>
```

3.4 Kali Linux Tool installation

1)Hydra : Hydra comes as a preinstalled toll on kali linux and it was used for initiating brute force attacks

Figure 18 Hydra Brute Force attack Manual

3.5 Windows server tool installation

Ransim was downloaded on the windows server to simulate ransomware type behaviour on the windows server to generate file encryption logs on wazuh SIEM

References

Pomerium.com. (2025). *What is Pomerium? | Pomerium*. [online] Available at: https://www.pomerium.com/docs [Accessed 21 Jul. 2025].

Wazuh (n.d.). *Quickstart · Wazuh Documentation*. [online] documentation.wazuh.com. Available at: https://documentation.wazuh.com/current/quickstart.html.

www.keycloak.org. (n.d.). *Keycloak - Documentation*. [online] Available at: https://www.keycloak.org/documentation.