

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)	<input type="checkbox"/>
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	<input type="checkbox"/>
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.	<input type="checkbox"/>

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.

```

ayush@ayush-VirtualBox: ~
ayush@ayush-VirtualBox:~$ sudo systemctl status keycloak
[sudo] password for ayush:
● keycloak.service - Keycloak Identity and Access Management
   Loaded: loaded (/etc/systemd/system/keycloak.service; enabled; vendor prese
   Active: active (running) since Fri 2025-07-18 00:45:29 IST; 1min 38s ago
     Main PID: 748 (java)
       Tasks: 52 (limit: 9437)
      Memory: 415.5M
         CPU: 32.048s
    CGroup: /system.slice/keycloak.service
            └─748 java -Xms64m -Xmx512m -XX:MetaspaceSize=96M -XX:MaxMetaspace
Jul 18 00:45:49 ayush-VirtualBox kc.sh[748]: 2025-07-18 00:45:49,122 INFO [org
Jul 18 00:45:51 ayush-VirtualBox kc.sh[748]: 2025-07-18 00:45:51,129 INFO [org
Jul 18 00:45:51 ayush-VirtualBox kc.sh[748]: 2025-07-18 00:45:51,140 INFO [org
Jul 18 00:45:51 ayush-VirtualBox kc.sh[748]: 2025-07-18 00:45:51,152 INFO [org
Jul 18 00:45:51 ayush-VirtualBox kc.sh[748]: 2025-07-18 00:45:51,164 WARN [org
Jul 18 00:45:56 ayush-VirtualBox kc.sh[748]: 2025-07-18 00:45:56,547 INFO [org
Jul 18 00:45:56 ayush-VirtualBox kc.sh[748]: 2025-07-18 00:45:56,587 INFO [org
Jul 18 00:46:02 ayush-VirtualBox kc.sh[748]: 2025-07-18 00:46:02,193 INFO [io.
Jul 18 00:46:02 ayush-VirtualBox kc.sh[748]: 2025-07-18 00:46:02,200 INFO [io.
Jul 18 00:46:02 ayush-VirtualBox kc.sh[748]: 2025-07-18 00:46:02,200 INFO [io.
lines 1-20/20 (END)...skipping...

```

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.

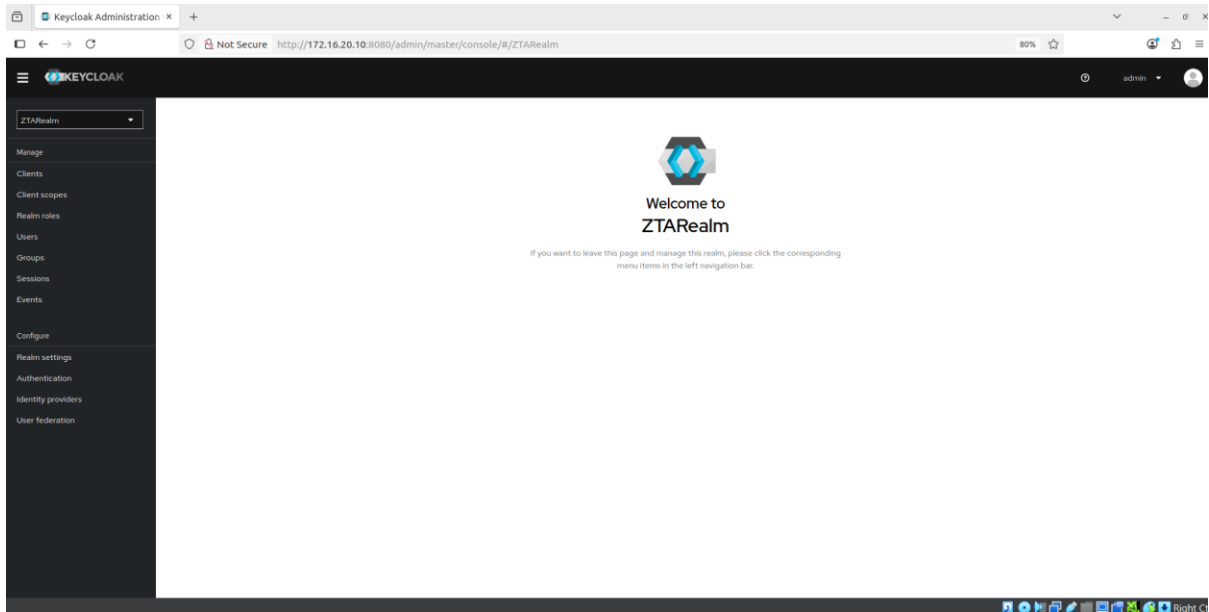


Figure 2 ZTA Realm Creation

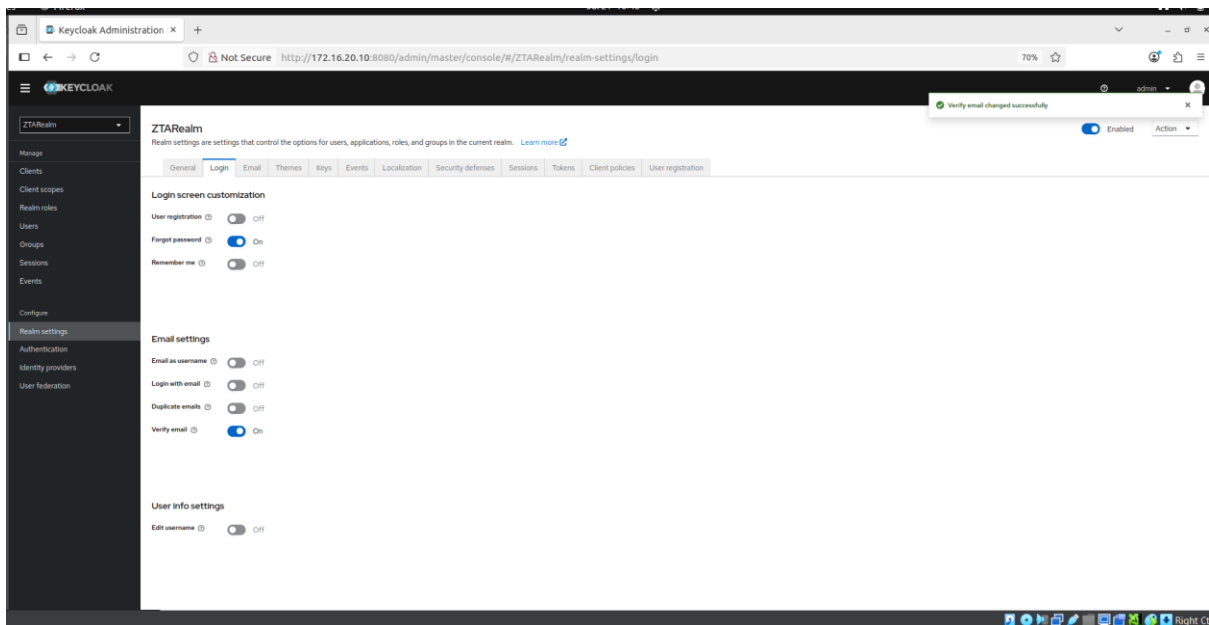


Figure 3 General Setting Configuration

Step 2: Enforce Secure HTTP headers

Realm Settings → Security Defences → Headers.

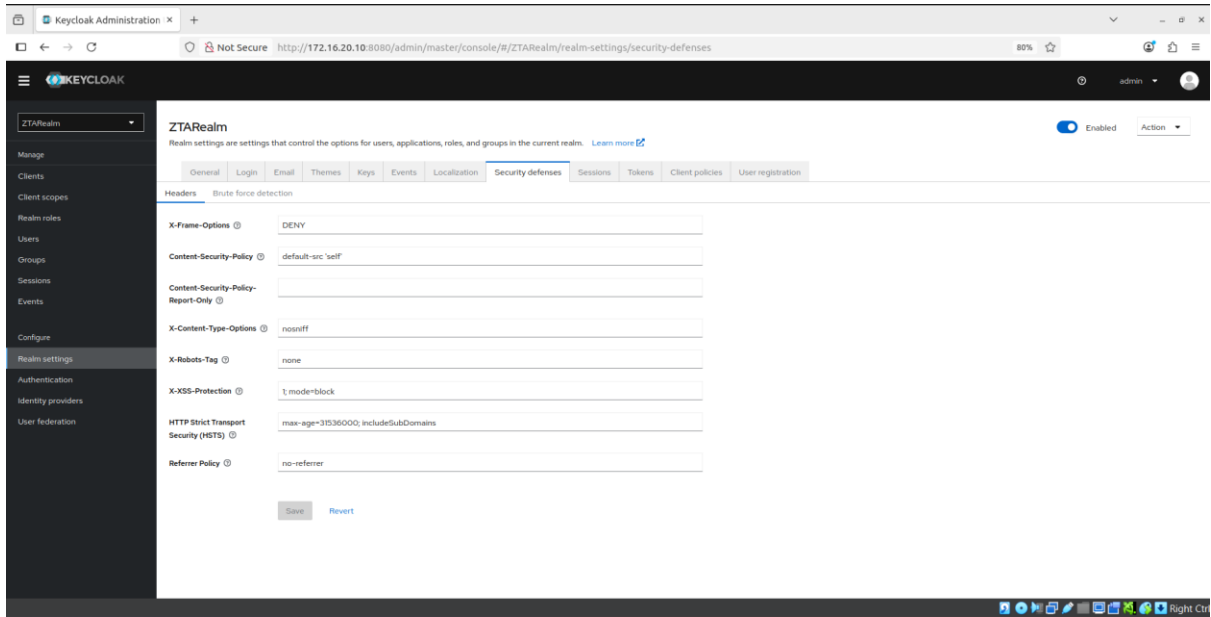


Figure 4 HTTP Header Configuration

Step 3: Configuring MFA

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

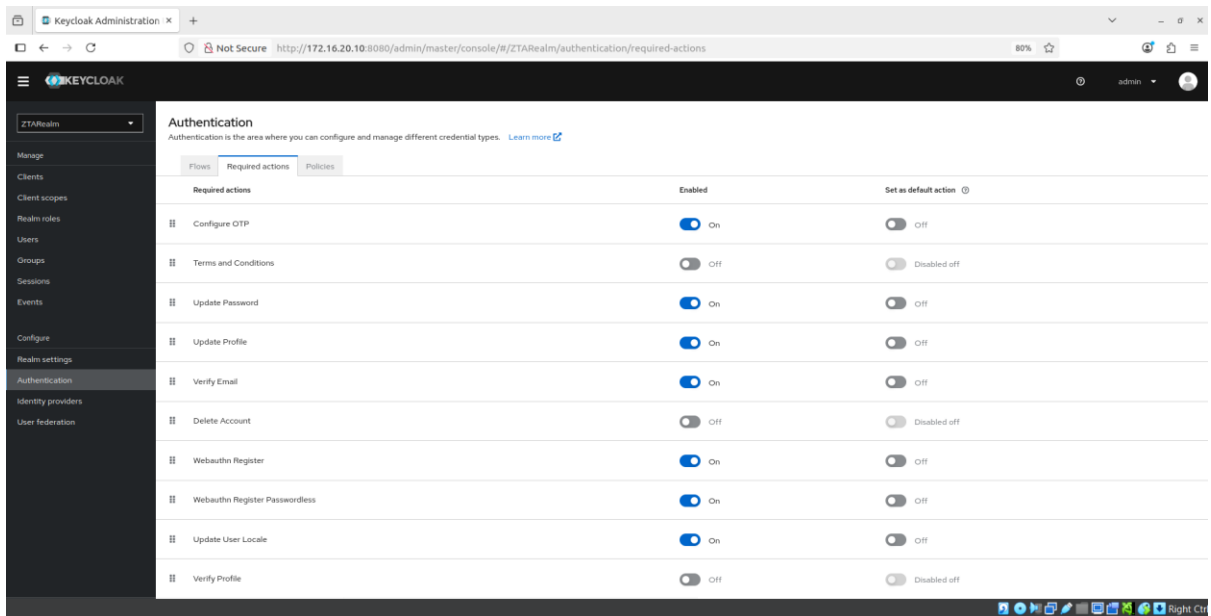


Figure 5 MFA Enablement

Multifactor authentication browser flow created

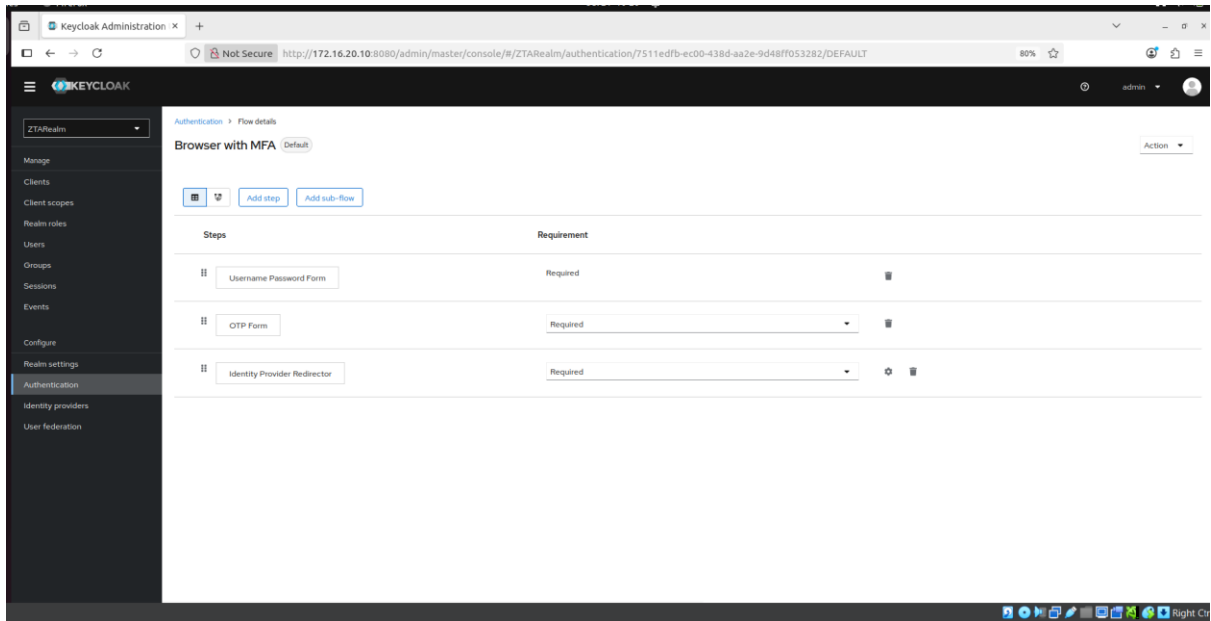


Figure 6 Browser with MFA flow

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)

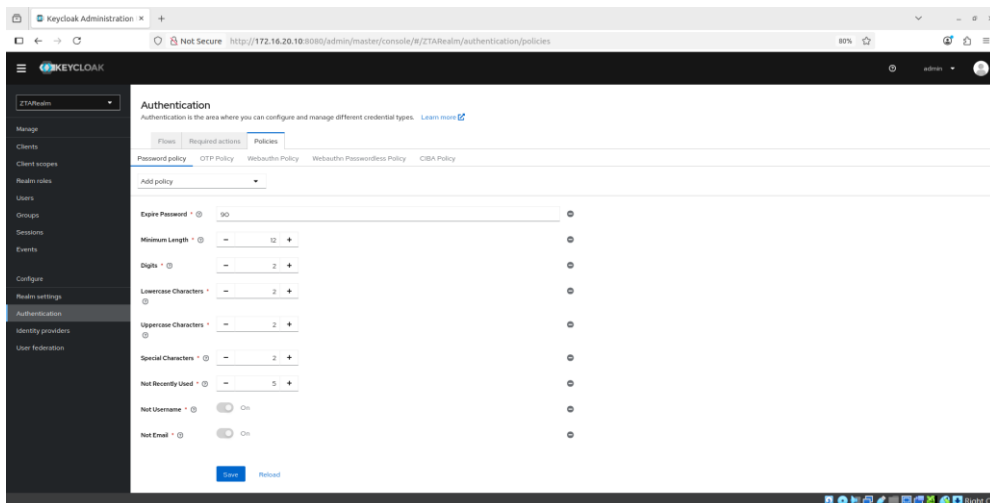


Figure 7 Password Policy Configuration

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

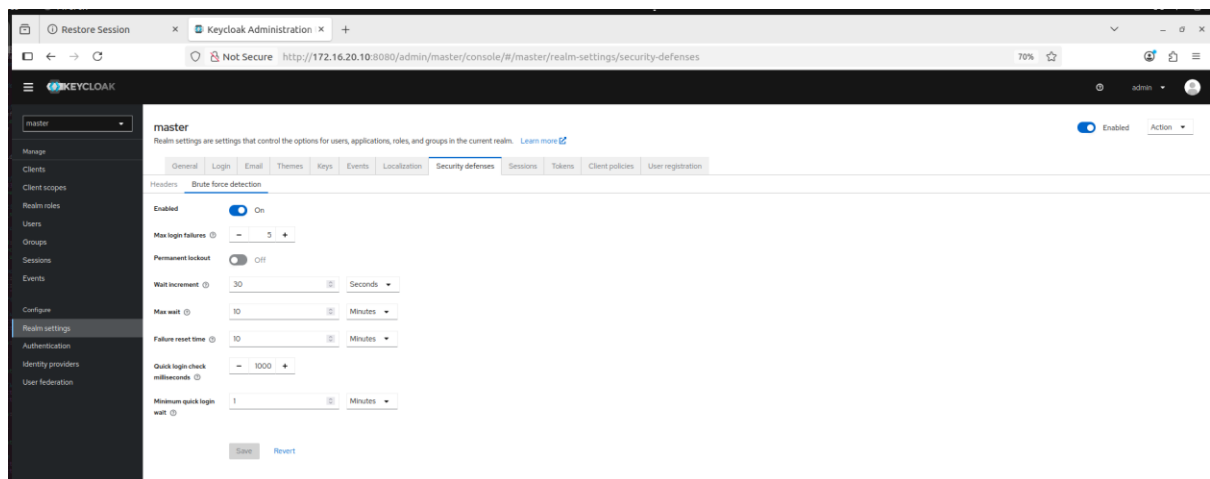


Figure 8 Brute Force Configuration

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

```
ayush@ayush-VirtualBox:~$ export COOKIE_SECRET=$(head -c32 /dev/urandom | base64)
ayush@ayush-VirtualBox:~$ echo "cookie_secret: \"\$COOKIE_SECRET\""
cookie_secret: "Ky4RMJTU8TAocfw/zYQeIuBCWi068QX8Lz6P3S1fPE=~"
ayush@ayush-VirtualBox:~$ export SHARED_SECRET=$(head -c32 /dev/urandom | base64)
ayush@ayush-VirtualBox:~$ echo "shared_secret: \"\$SHARED_SECRET\""
shared_secret: "JL093pTHQEL4VNZitKUXBiuFL36wq1sRoqHhfnbp26Y=~"
ayush@ayush-VirtualBox:~$
```

Figure 9 Extraction of Secret keys


```

Activities Terminal Jul 10 14:20
ayush@ayush-VirtualBox: ~
10/07/2025 13:55:20 INFO: Starting Wazuh indexer installation.
10/07/2025 13:57:03 INFO: Wazuh indexer installation finished.
10/07/2025 13:57:03 INFO: Wazuh indexer post-install configuration finished.
10/07/2025 13:57:03 INFO: Starting service wazuh-indexer.
10/07/2025 13:57:59 INFO: wazuh-indexer service started.
10/07/2025 13:57:59 INFO: Initializing Wazuh indexer cluster security settings.
10/07/2025 13:58:11 INFO: Wazuh indexer cluster security configuration initialized.
10/07/2025 13:58:11 INFO: Wazuh indexer cluster initialized.
10/07/2025 13:58:11 INFO: --- Wazuh server ---
10/07/2025 13:58:11 INFO: Starting the Wazuh manager installation.
10/07/2025 14:03:08 INFO: Wazuh manager installation finished.
10/07/2025 14:03:09 INFO: Wazuh manager vulnerability detection configuration finished.
10/07/2025 14:03:09 INFO: Starting service wazuh-manager.
10/07/2025 14:03:35 INFO: wazuh-manager service started.
10/07/2025 14:03:35 INFO: Starting Filebeat installation.
10/07/2025 14:04:22 INFO: Filebeat installation finished.
10/07/2025 14:04:26 INFO: Filebeat post-install configuration finished.
10/07/2025 14:04:26 INFO: Starting service filebeat.
10/07/2025 14:04:32 INFO: filebeat service started.
10/07/2025 14:04:32 INFO: --- Wazuh dashboard ---
10/07/2025 14:04:32 INFO: Starting Wazuh dashboard installation.
10/07/2025 14:16:00 INFO: Wazuh dashboard installation finished.
10/07/2025 14:16:00 INFO: Wazuh dashboard post-install configuration finished.
10/07/2025 14:16:00 INFO: Starting service wazuh-dashboard.
10/07/2025 14:16:01 INFO: wazuh-dashboard service started.
10/07/2025 14:16:06 INFO: Updating the internal users.
10/07/2025 14:16:25 INFO: A backup of the internal users has been saved in the /etc/wazuh-indexer/internalusers-backup folder.
10/07/2025 14:16:55 INFO: The filebeat.yml file has been updated to use the Filebeat Keystore username and password.
10/07/2025 14:18:09 INFO: Initializing Wazuh dashboard web application.
10/07/2025 14:18:10 INFO: Wazuh dashboard web application not yet initialized. Waiting...
10/07/2025 14:18:26 INFO: Wazuh dashboard web application not yet initialized. Waiting...
10/07/2025 14:18:41 INFO: Wazuh dashboard web application initialized.
10/07/2025 14:18:41 INFO: --- Summary ---
10/07/2025 14:18:41 INFO: You can access the web interface https://<wazuh-dashboard-ip>:443
User: admin
Password: xY?L8aDJj1DKqec+Ge+zxwD5a26VgWgr
10/07/2025 14:18:41 INFO: --- Dependencies ---
10/07/2025 14:18:41 INFO: Removing gawk.
10/07/2025 14:18:54 INFO: Installation finished.
ayush@ayush-VirtualBox: $

```

Figure 12 Successful Installation of Wazuh

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

```

ayush@ayush-VirtualBox: ~$ sudo systemctl status wazuh-manager
[sudo] password for ayush:
● wazuh-manager.service - Wazuh manager
   Loaded: loaded (/lib/systemd/system/wazuh-manager.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2025-07-08 13:43:54 IST; 7min ago
     Tasks: 174 (limit: 9683)
    Memory: 1.7G
       CPU: 5min 57.044s
   CGroup: /system.slice/wazuh-manager.service
           └─00389 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
             └─00391 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
               └─00392 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
                 └─00396 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
                   └─00401 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
                     └─00443 /var/ossec/bin/wazuh-authd
                       └─00532 /var/ossec/bin/wazuh-db
                         └─00548 /var/ossec/bin/wazuh-execd
                           └─00574 /var/ossec/bin/wazuh-analysisd
                             └─00592 /var/ossec/bin/wazuh-syscheckd
                               └─00607 /var/ossec/bin/wazuh-remoted
                                 └─00691 /var/ossec/bin/wazuh-logcollector
                                   └─00709 /var/ossec/bin/wazuh-monitord
                                     └─00731 /var/ossec/bin/wazuh-modulesd

Jul 08 13:43:47 ayush-VirtualBox env[60322]: Started wazuh-analysisd...
Jul 08 13:43:48 ayush-VirtualBox env[60322]: Started wazuh-syscheckd...
Jul 08 13:43:49 ayush-VirtualBox env[60322]: Started wazuh-remoted...
Jul 08 13:43:51 ayush-VirtualBox env[60322]: Started wazuh-logcollector...
Jul 08 13:43:52 ayush-VirtualBox env[60322]: Started wazuh-monitord...
Jul 08 13:43:52 ayush-VirtualBox env[60729]: 2025/07/08 13:43:52 wazuh-modulesd:router: INFO: Loaded router content.
Jul 08 13:43:52 ayush-VirtualBox env[60729]: 2025/07/08 13:43:52 wazuh-modulesd:content_manager: INFO: Loaded content_manager module.
Jul 08 13:43:52 ayush-VirtualBox env[60322]: Started wazuh-modulesd...
Jul 08 13:43:54 ayush-VirtualBox env[60322]: Completed.
Jul 08 13:43:54 ayush-VirtualBox systemd[1]: Started Wazuh manager.
lines 1-32/32 (END)

```

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 call
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":["error"],"ob
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

```

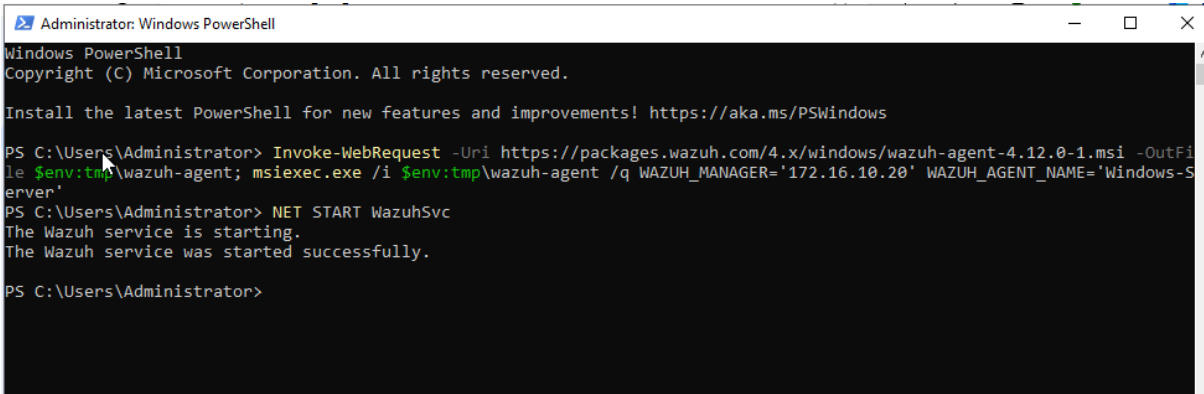
ayush@ayush-VirtualBox:~$ sudo systemctl status wazuh-agent
[sudo] password for ayush:
● wazuh-agent.service - Wazuh agent
   Loaded: loaded (/lib/systemd/system/wazuh-agent.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2025-07-21 10:20:03 IST; 4h 47min ago
     Process: 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 10:20:02 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



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Administrator> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.12.0-1.msi -OutFile $env:tmp\wazuh-agent; msisexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='172.16.10.20' WAZUH_AGENT_NAME='Windows-Server'
PS C:\Users\Administrator> NET START WazuhSvc
The Wazuh service is starting.
The Wazuh service was started successfully.

PS C:\Users\Administrator>
```

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 windows 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

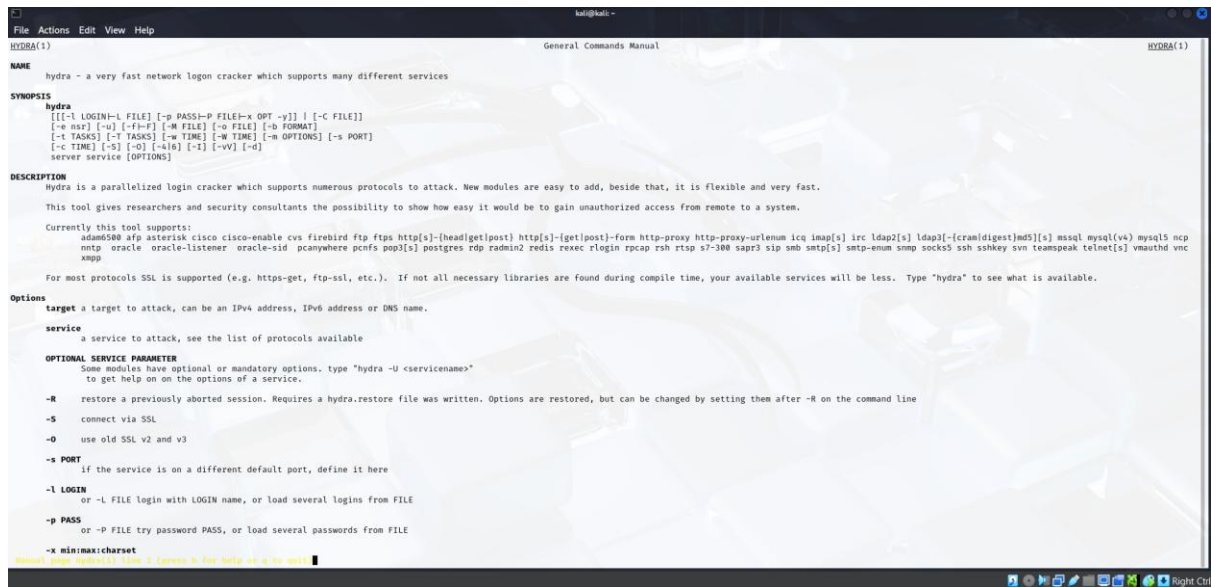


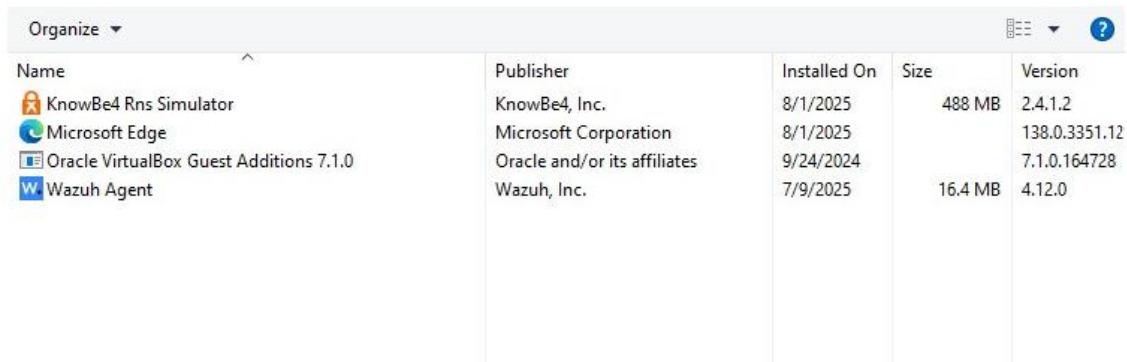
Figure 18 Hydra Brute Force attack Manual

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

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.



The screenshot shows the 'Uninstall or change a program' window in Windows. The window title is 'Organize'. It contains a table with the following columns: Name, Publisher, Installed On, Size, and Version. The table lists four programs: KnowBe4 Rns Simulator, Microsoft Edge, Oracle VirtualBox Guest Additions 7.1.0, and Wazuh Agent.

Name	Publisher	Installed On	Size	Version
 KnowBe4 Rns Simulator	KnowBe4, Inc.	8/1/2025	488 MB	2.4.1.2
 Microsoft Edge	Microsoft Corporation	8/1/2025		138.0.3351.12
 Oracle VirtualBox Guest Additions 7.1.0	Oracle and/or its affiliates	9/24/2024		7.1.0.164728
 Wazuh Agent	Wazuh, Inc.	7/9/2025	16.4 MB	4.12.0

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>.