Configuration Manual

MSc Research Project
MSc in Cybersecurity

Nirav Ratilal Patel
Student ID: x23268859@student.ncirl.ie

School of Computing
National College of Ireland

Supervisor: Joel Aleburu

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Nirav Ratilal Patel
Student ID:	x23268859@student.ncirl.ie
Programme:	MSc in Cybersecurity **Year:** 2024-2025
Module:	MSc Research Project
Lecturer:	Joel Aleburu
Submission Due Date:	11/08/2025
Project Title:	Implementing Zero Trust Architecture in Detecting and Mitigating Threats: An APT Focused ZTA Framework
Word Count:	2031 **Page Count:** 24

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: Nirav Ratilal Patel

Date: 11/08/2025

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

Implementing Zero Trust Architecture in Detecting and Mitigating Threats: An APT Focused ZTA Framework

Nirav Ratilal Patel
X23268859@student.ncirl.ie

1. Introduction

This configuration manual goes through and introduces about the lab designed which comprises of the five VM setup which demonstrates the zero trust principles for the detection and mitigation of the APT attacks through the open source Wazuh SIEM. The attack simulation is performed through Kali Linux virtual machines and demonstrated real world exploits using different tools like Hydra, Metasploit, Wireshark and other tools and the victims are Ubuntu server and the windows server 2022 and the illustration of detection and response process against these APT threats. This configuration manual provides step by step process starting from the network setup configuration and also all the tools installation process along with the attack scenarios.

2. System Specifications

2.1 The following is the hardware configurations of the machine.

- CPU: Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz 2.59 GHz
- Operating System: 64-bit operating system, x64-based processor
- Memory: 16GB RAM
- Drive: 1 TB SSD

2.2 Network design and Lab architecture and tools Installation

Below are the details about the virtual machines and their configurations.

Virtual Machine	**Operating System**	**RAM**	**Storage**	**IP address**
Ubuntu for SIEM	Ubuntu 22.04	8 GB	100 GB	192.168.1.86
Kali Linux for Attack machine	Kali Linux	4 GB	40 GB	192.168.1.76

Ubuntu for ZTA controller	Ubuntu	4 GB	60 GB	192.168.1.81
Windows server for victim machine	Windows server 2022	4 GB	60 GB	192.168.1.72
Ubuntu Server for Victim machine	Ubuntu server 22.04	2 GB	40 GB	192.168.1.77

2.3 Tools Installation on different virtual machines

1. **Ubuntu Desktop: Installation of Wazuh SIEM 4.12.0.** It is an opensource tool for monitoring of all the events has threat detection capabilities which is used mainly for the detection of abnormal behaviours in the infrastructure in different environments. It has different features such as Active response, File integrity monitoring, Vulnerability detection, Log analysis and corelation and provides real time alerts and Incident response. IT consists of three major components which are Wazuh Manager, Wazuh Indexer, Wazuh, Dashboard.

   The command for Installing Wazuh is "**curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh && sudo bash ./wazuh-install.sh -a"**

   - **Wazuh Manager:** It is basically the central component of the of the whole system which receives and processes the data and also analyses the data from all the agents which are deployed. It performs real time log processing and many other different functions.

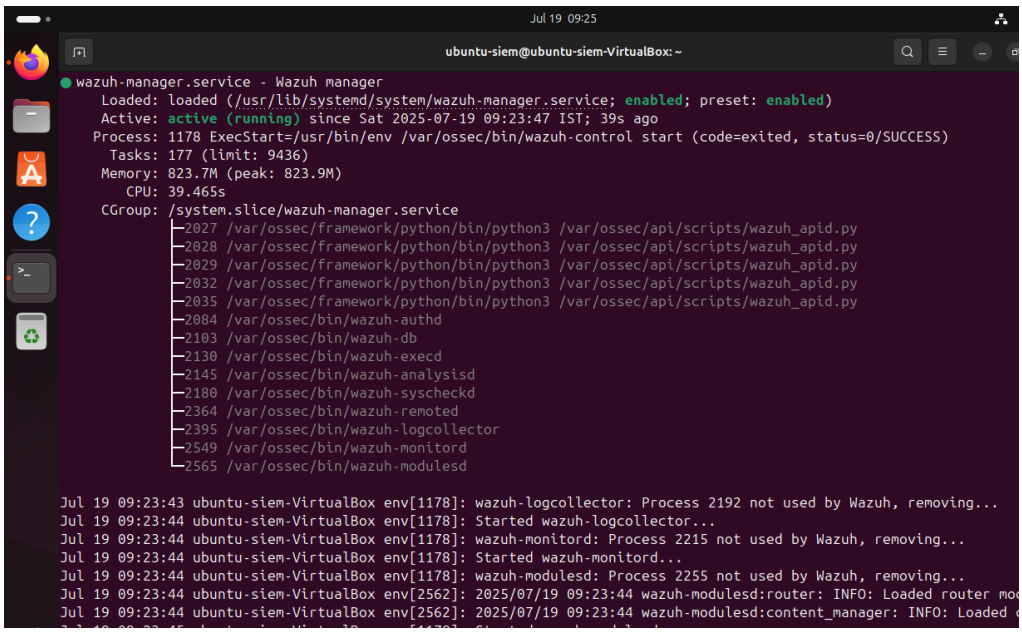


Figure 1: Wazuh manager

- **Wazuh Indexer:** It is based on the functions like handling the data storage and indexing and other search capabilities which can help for faster data retrieval and other data retention capabilities.

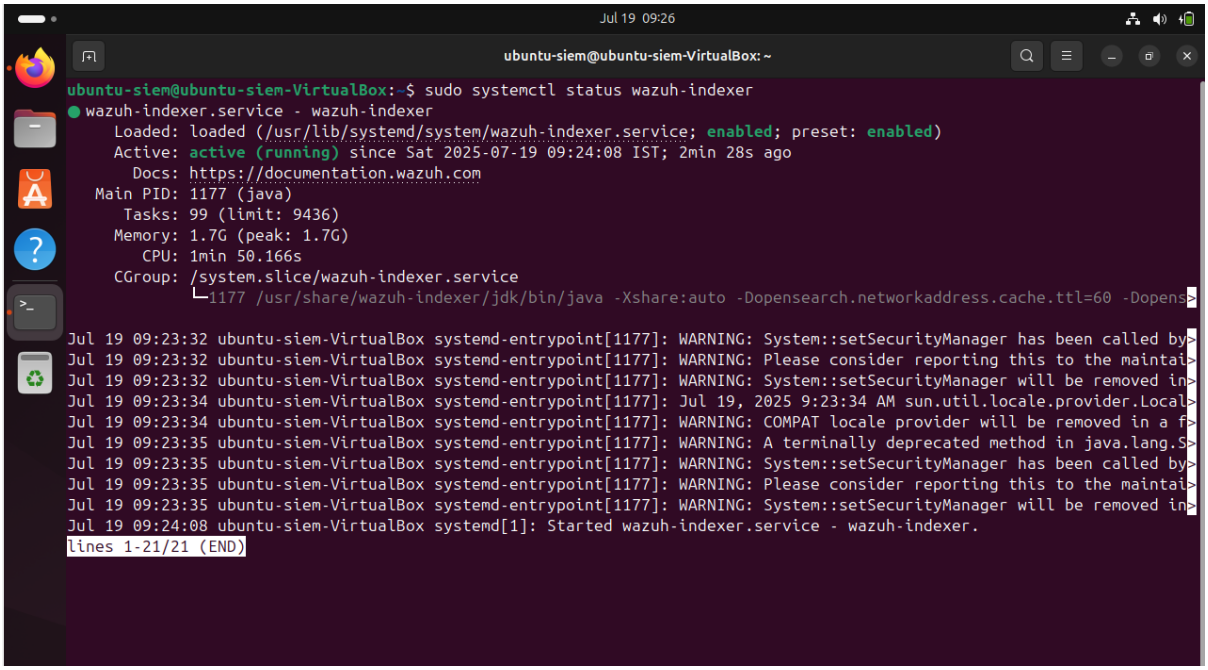


Figure 2:Wazuh Indexer

- **Wazuh Dashboard:** It is wazuh's web interface which is used for the real time monitoring and management. It is mainly used for the managing the alerts and proactive threat hunting and management of different users and its access and permission.

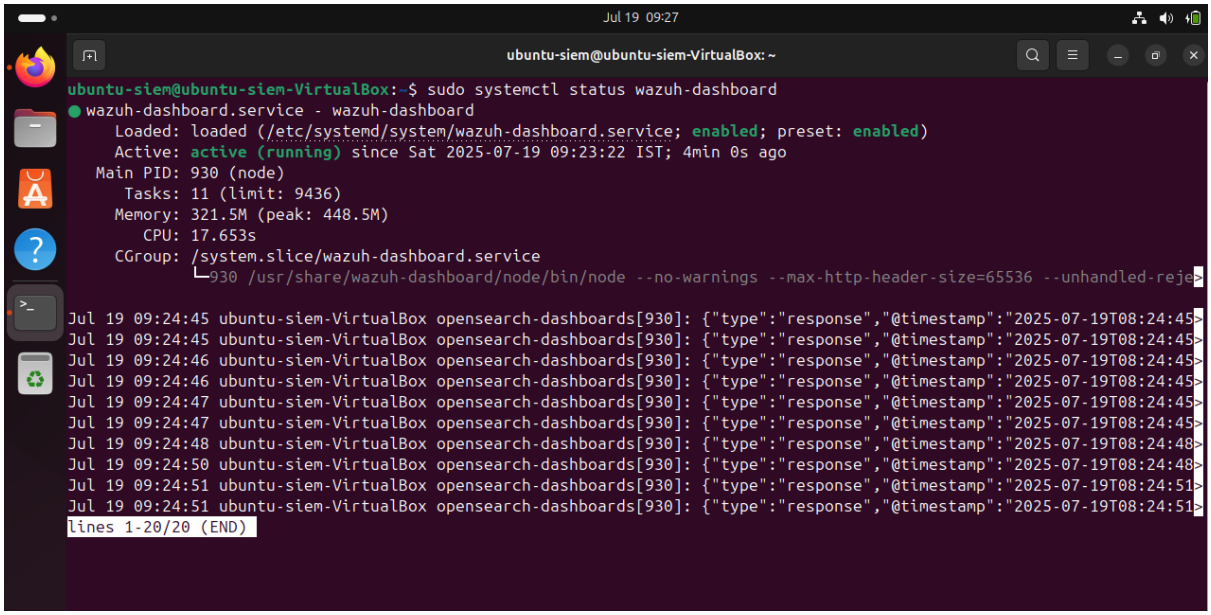


Figure 3: Wazuh Dashboard

Wazuh Manager Configuration: For leveraing the full event logging and also checking the location of the logs, we need to make some changes in the configuraiton file which is "/var/ossec/etc/ossec.conf". Perform the below steps and add the <global> section in the conf file.

- Go to sudo nano /var/ossec/etc/ossec.conf
- Add the below steps in the file and save it.
- **<global>**
  <logall>yes</logall>
  <logall_json>yes</logall_json>
  </global>

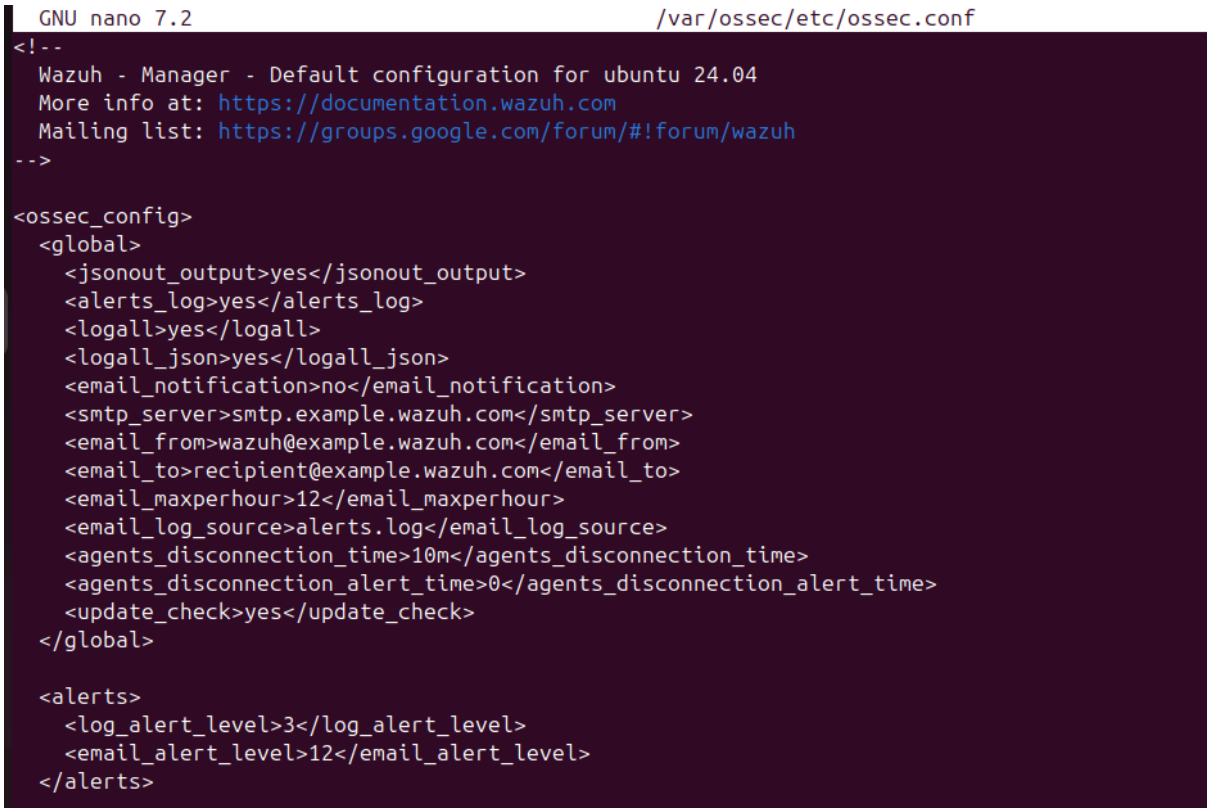


Figure 4: ossec.conf file

For log parsing and processing, we need to make some changes in the filebeat modules due to which we can enable all the alerts and archives in wazuh logs. It is the vital setting for integrating and visualizing the alerts in Wazuh's console.
Navigate to the filebeat.yml file by "**sudo nano /etc/filebeat/filebeat.yml**" and make the folliwing changes. We need to make sure that the alerts and archives both are "true".

- filebeat.modules:
  - module: wazuh
    alerts:
      enabled: true
    archives:
      enabled: true

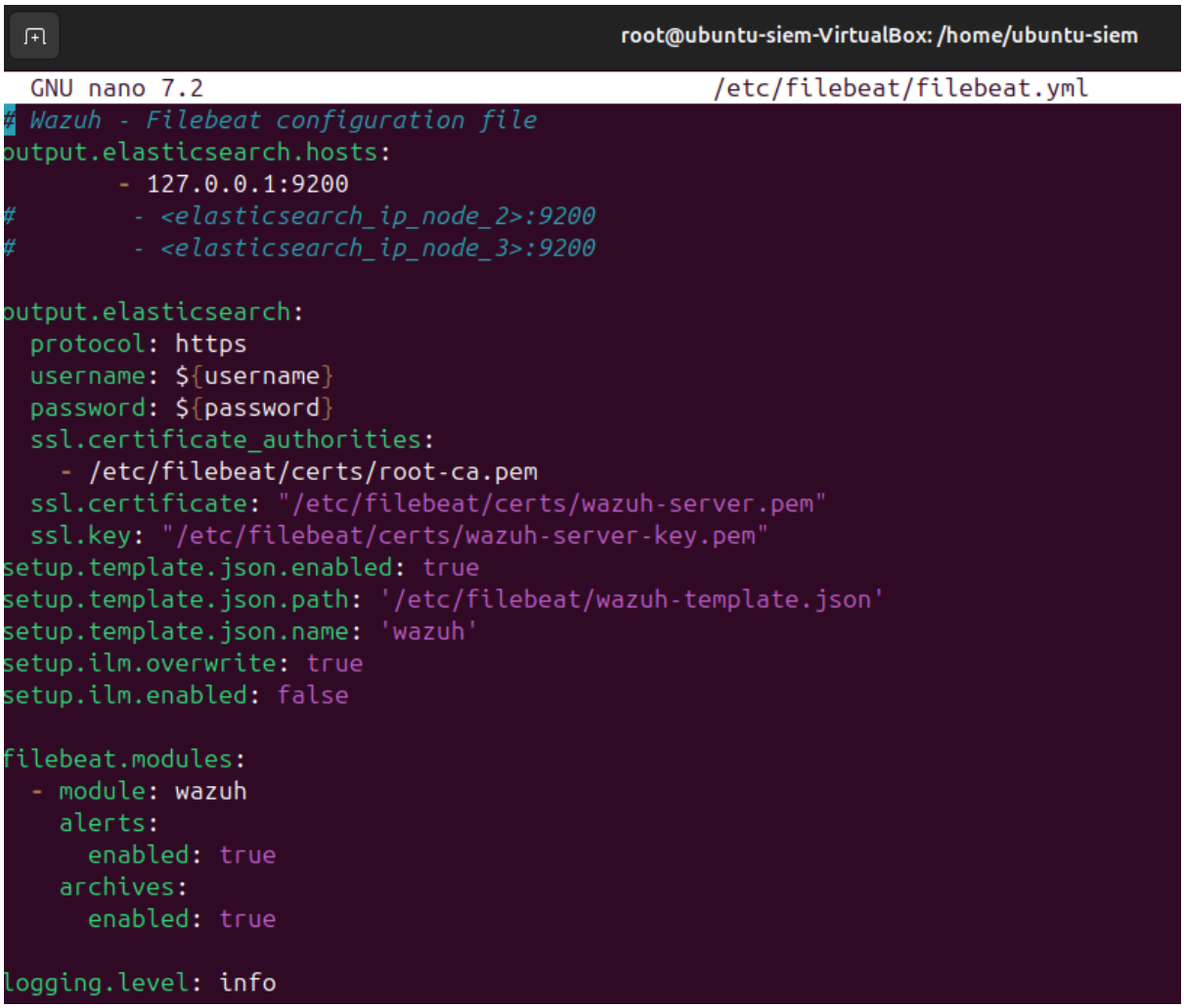


Figure 5: Filebeat.yml file

Log Inestion in Wazuh: Creation of the archeive index pattern in wazuh dashboard for recognizing all the seaches in the logs and selecting the timestamps which will enable all the time fields.

- Go to the Wazuh dashboard, and click on the menu Icon and select the Dashbaord management and go to index patterns.
- Click on the “create index pattern” and add wazuh-archives-* as the index pattern.
- Next, choose timestamp as the time field.
- Click on the create indext pattern to save it.

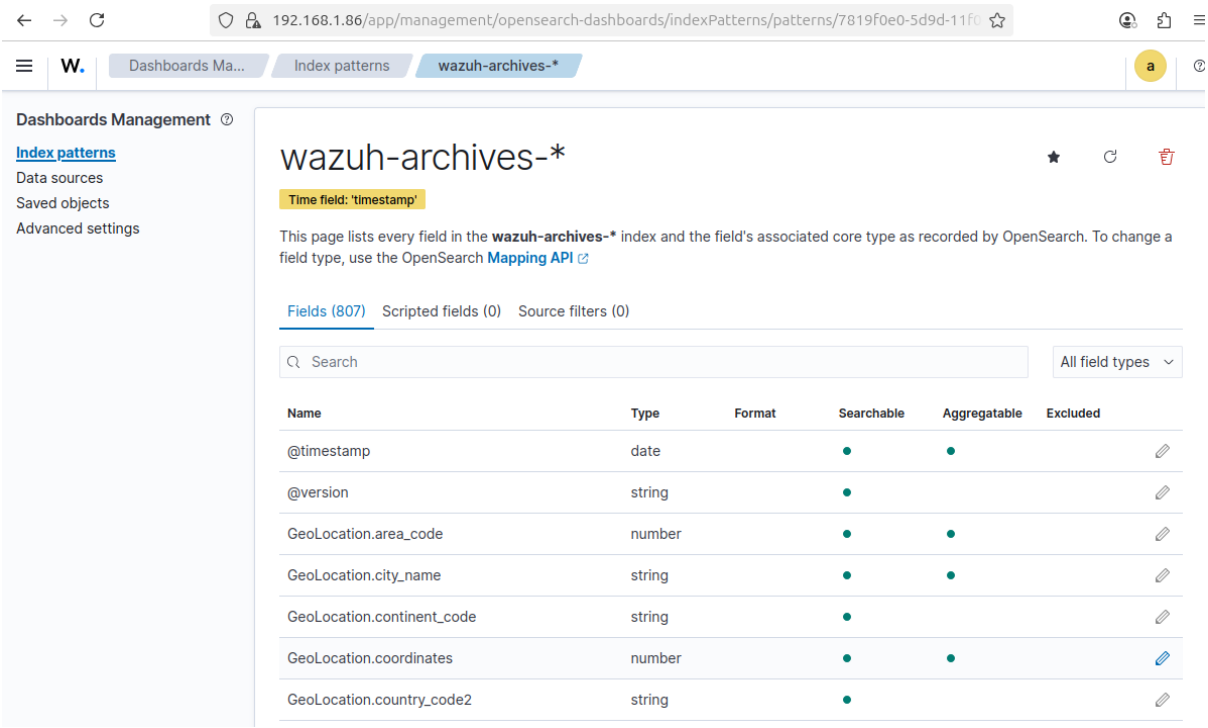


Figure 6: Log ingestion

For vewing the logs in the Dashboard,

- Go to the Discover section and from the index pattern dropdown, choose the **wazuh-archives-*** option and see the all the raw logs which are being sent by the agent.

2. Ubuntu for ZTA Controller:

Installation of spire server which will work as the foundation of the zero trust architecture in out environments. Basically it comprises of the two main components, one is Spire server and other is spire agent. The installation steps are mentioned below. [4]

Initially, we will update all the dependencies and required packeges.

- **sudo apt update && sudo apt upgrade -y**
- **sudo apt install curl wget git unzip build-essential -y**

Now, we will create a separate directory for spire.

- **mkdir -p ~/zta-lab/spire/{bin,conf,data/{server,agent},logs}**
- **cd ~/zta-lab/spire**

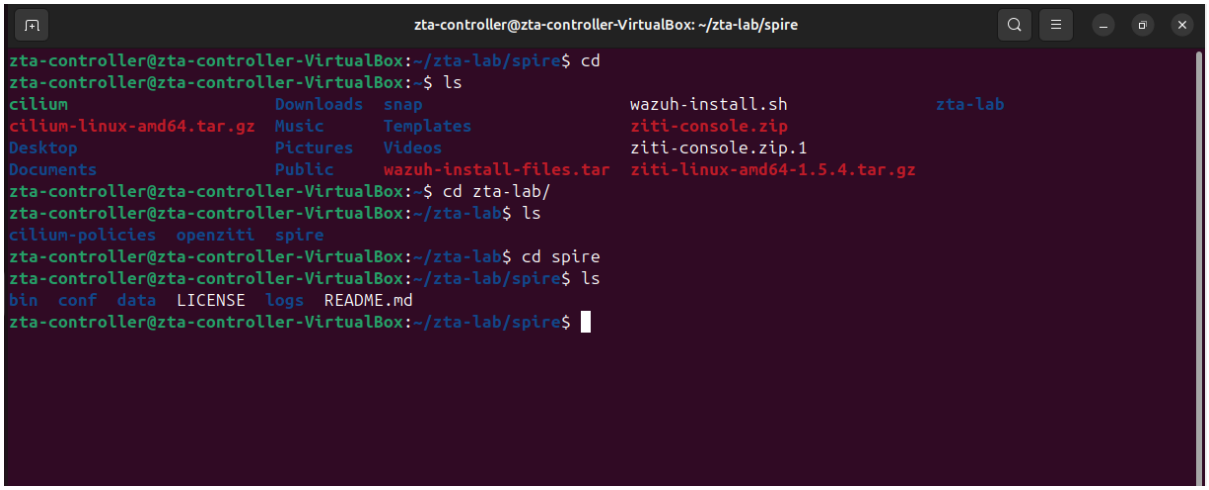


Figure 7: Create a directory for spire

Now, we will download the latest release version for spire and install it. The version which is the latest is version 1.12.3. The commands for the intallaiton are given below.

- wget https://github.com/spiffe/spire/releases/download/v1.12.3/spire-1.12.3-linux-amd64-musl.tar.gz

Now, we will verify and extract the binaries.

- **tar -xzf spire-1.12.3-linux-amd64-musl.tar.gz**
- **mv spire-1.12.3/* .**
- **rm -rf spire-1.12.3 spire-1.12.3-linux-amd64-musl.tar.gz**

Configiration of Spire Server:

We will do the confgiuration in the nano text editor and below is the configuration of that.

- **nano ~/zta-lab/spire/conf/server/server.conf**

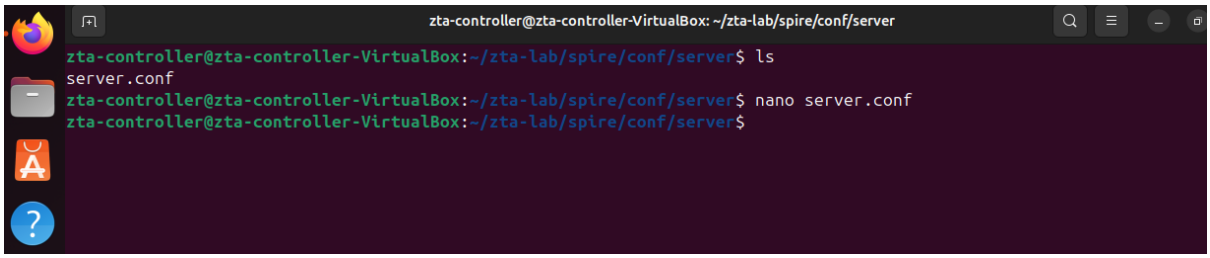


Figure 8: Make server.conf file

Now add all the configuration in the "**server.conf**" file.

Figure 9: Spire server configuration

Configuration of Spire Agent: For this configuration navigate to the same file location and make a new file called “agent.conf”. The location should be, “**nano ~/zta-lab/spire/conf/agent/agent.conf”**.

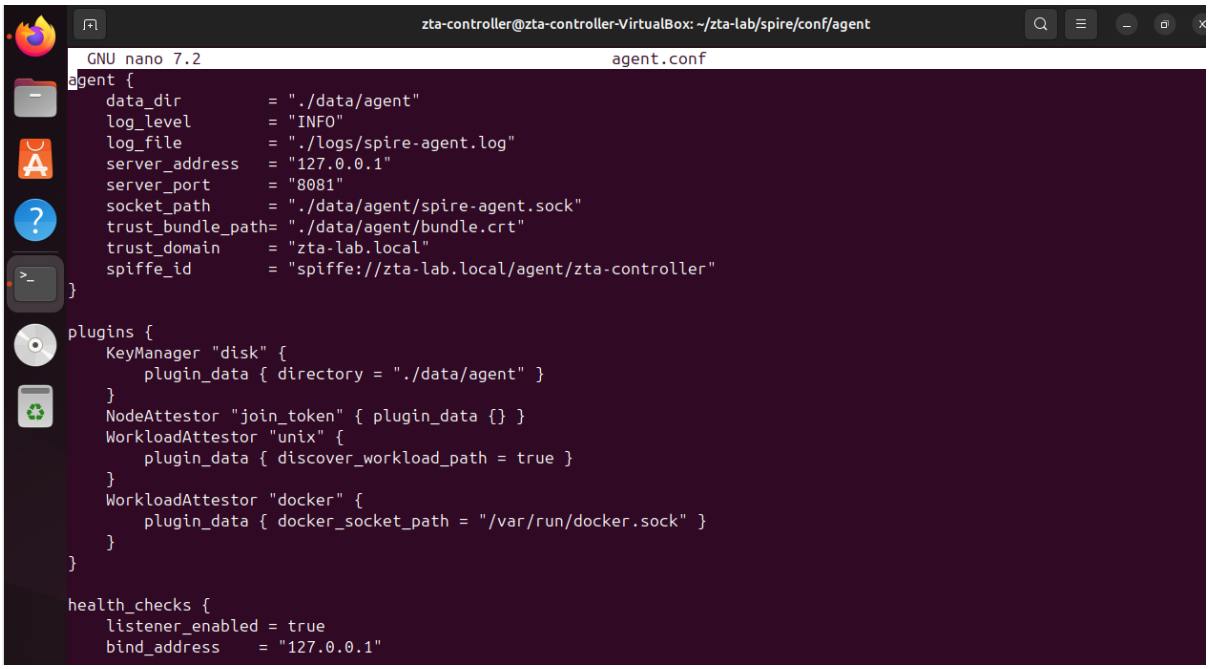


Figure 10: Spire agent

Now, we are going to create a systemd service for both spire service as well as spire agent. Below are the steps for spire service and spire agent.

Spire Server Service: "**sudo nano /etc/systemd/system/spire-server.service**"

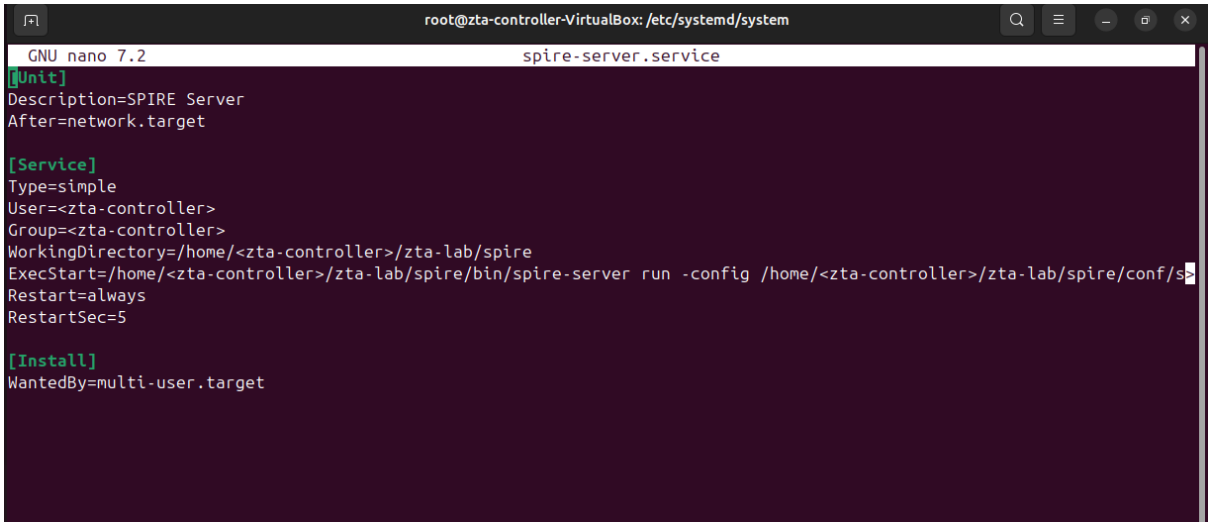


Figure 11: Spire server service

Spire Agent Service: "sudo nano /etc/systemd/system/spire-agent.service"

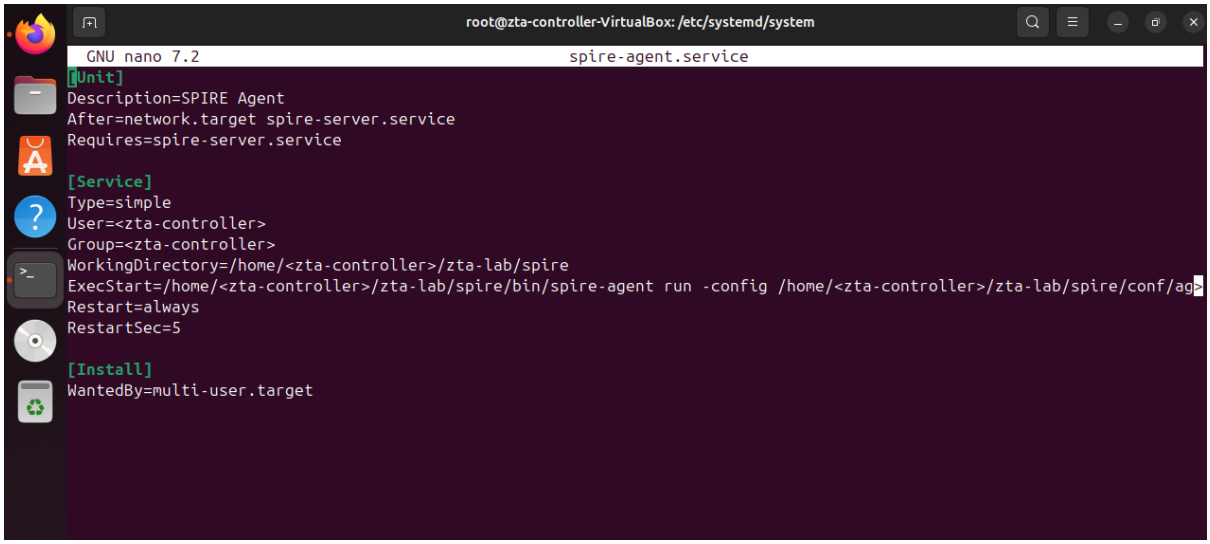


Figure 12: Spire Agent Service

The spire server and spire agent is set up now. We will enable the services and check the status of the services.

- **sudo systemctl daemon-reload**
- **sudo systemctl enable spire-server spire-agent**
- **sudo systemctl start spire-server**
- **sleep 5**
- **sudo systemctl start spire-agent**

Environment Configuration and adding variables to the user profile

- nano ~/.bashrc
- Appnend the following command in the end of the file:
- **export SPIRE_SERVER_ADDRESS=127.0.0.1:8081**
- **export SPIFFE_ENDPOINT_SOCKET=unix:///home/<your_user>/zta-lab/spire/data/agent/spire-agent.sock**
- Now, Save and reload it using "**source ~/.bashrc**"

Installtion of Cilium

Now, we will move forward with the cilium installation, we will download Cilum form github and below are the commands for it.Also, the extraction and installation commands are provided below.

- **curl -L --remote-name-all https://github.com/cilium/cilium-cli/releases/latest/download/cilium-linux-amd64.tar.gz**

- **tar -xzf cilium-linux-amd64.tar.gz sudo mv cilium /usr/local/bin/**

- **cilium version –client**

Also, the deployment of the cilium is done with zero trust configuration below are the commands and snippets for it.

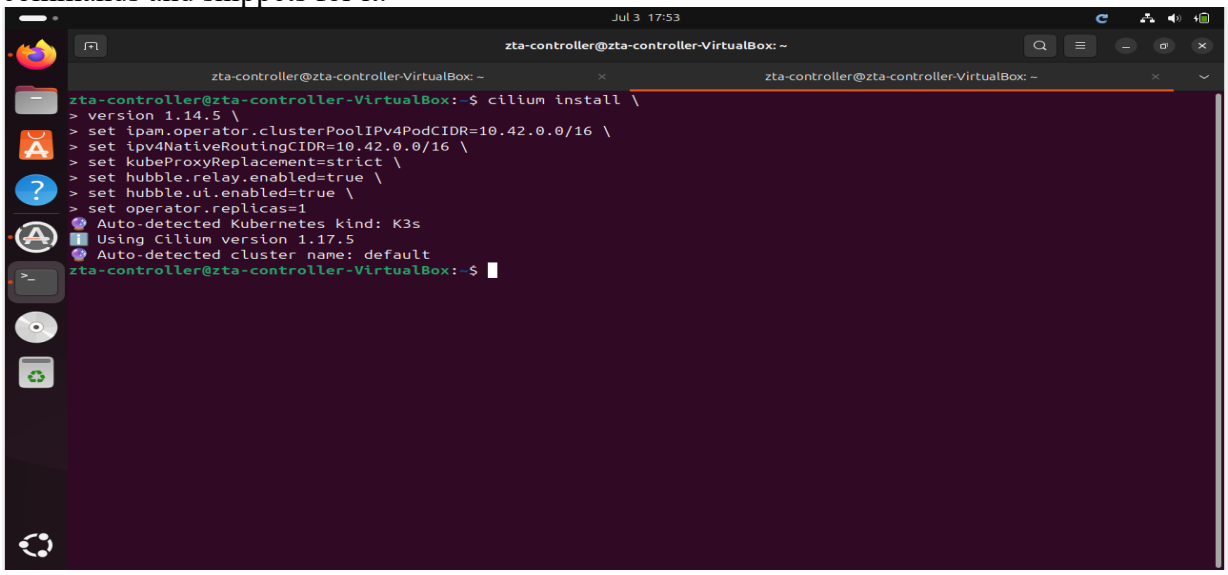


Figure 13: Cilium installation

For checking the cilium status, use the command "**cilium version --wait**"

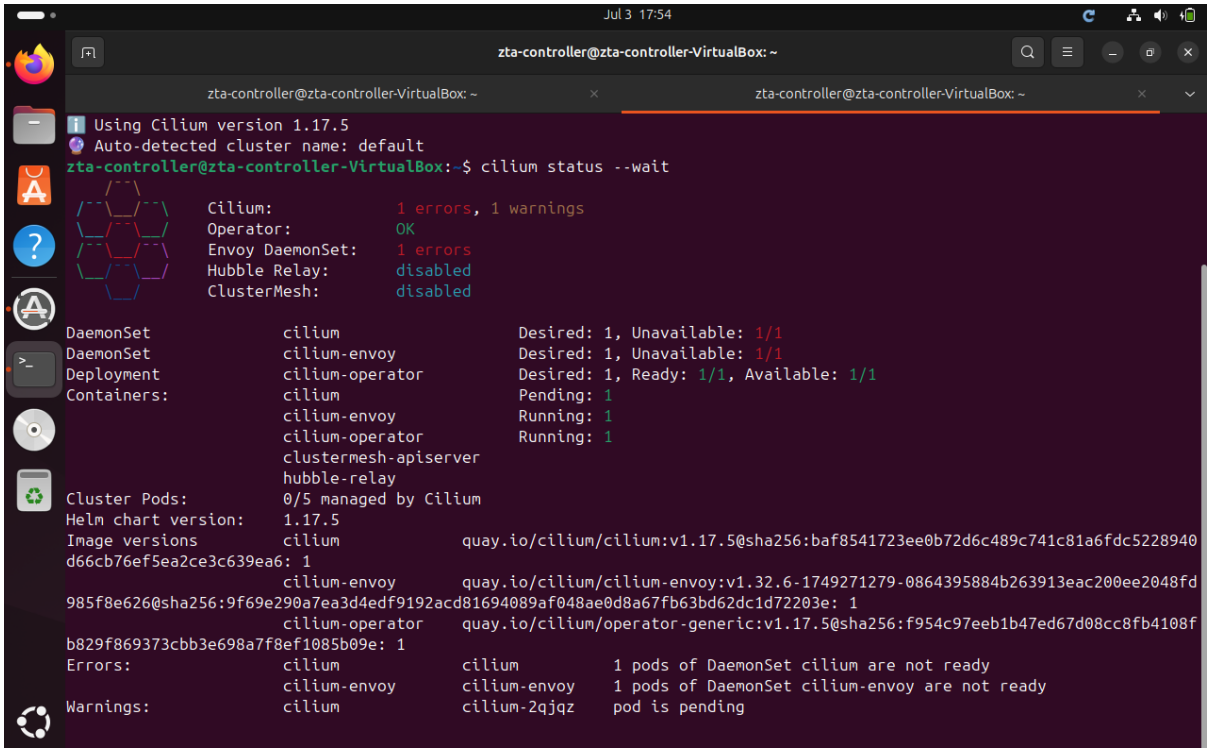


Figure 14: Cilium status

Configuration of Zero Trust Network Policies:

- mkdir -p ~/zta-lab/cilium-policies
- nano default-deny-policy.yaml

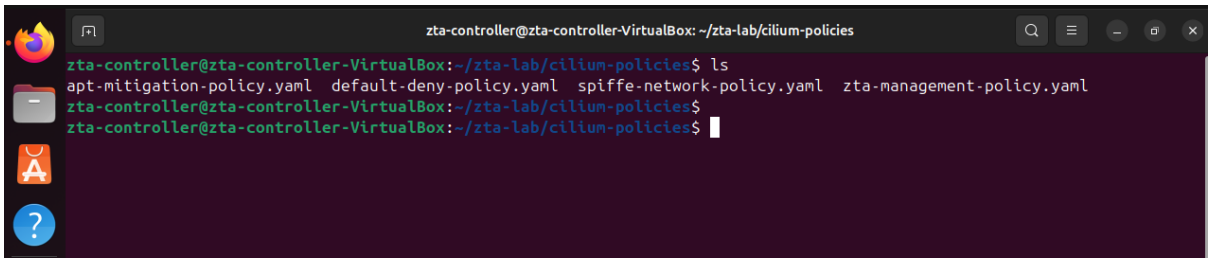


Figure 15: Policies

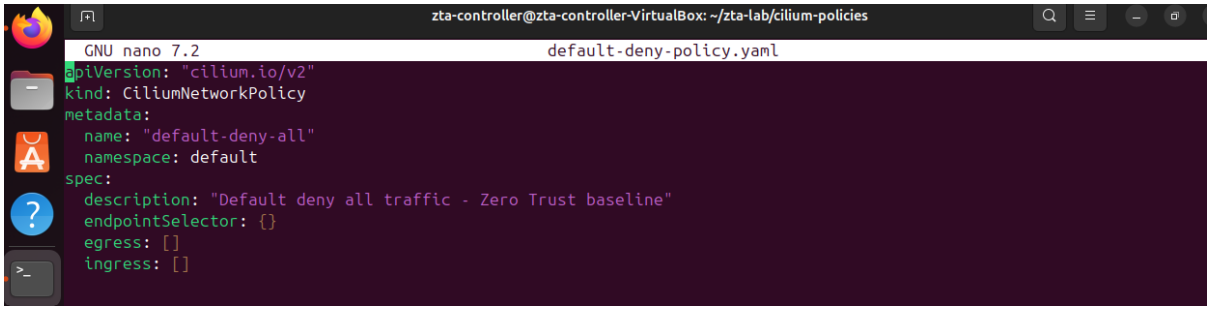


Figure 16: Default -deny policy

Now, we can create **ZTA management policy:**

- Go to terminal and use the command “nano zta-management-policy.yaml” and edit the file.
- Apply the changes and save it. “kubectl apply -f zta-management-policy.yaml”

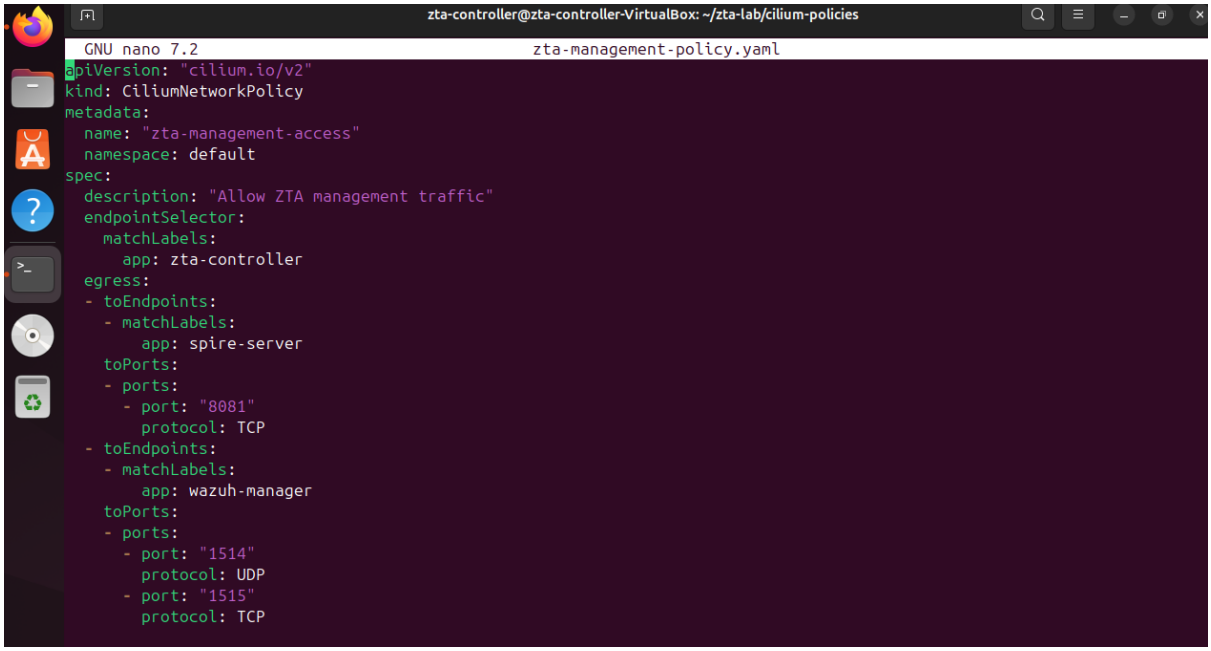


Figure 17: ZTA-management policy

Cilium policy for APT Mitigation:

- Go to the terminal and create policy using the nano editor. “nano apt-mitigation-policy.yaml”
- Apply the policy and save it. “kubectl apply -f apt-mitigation-policy.yaml”

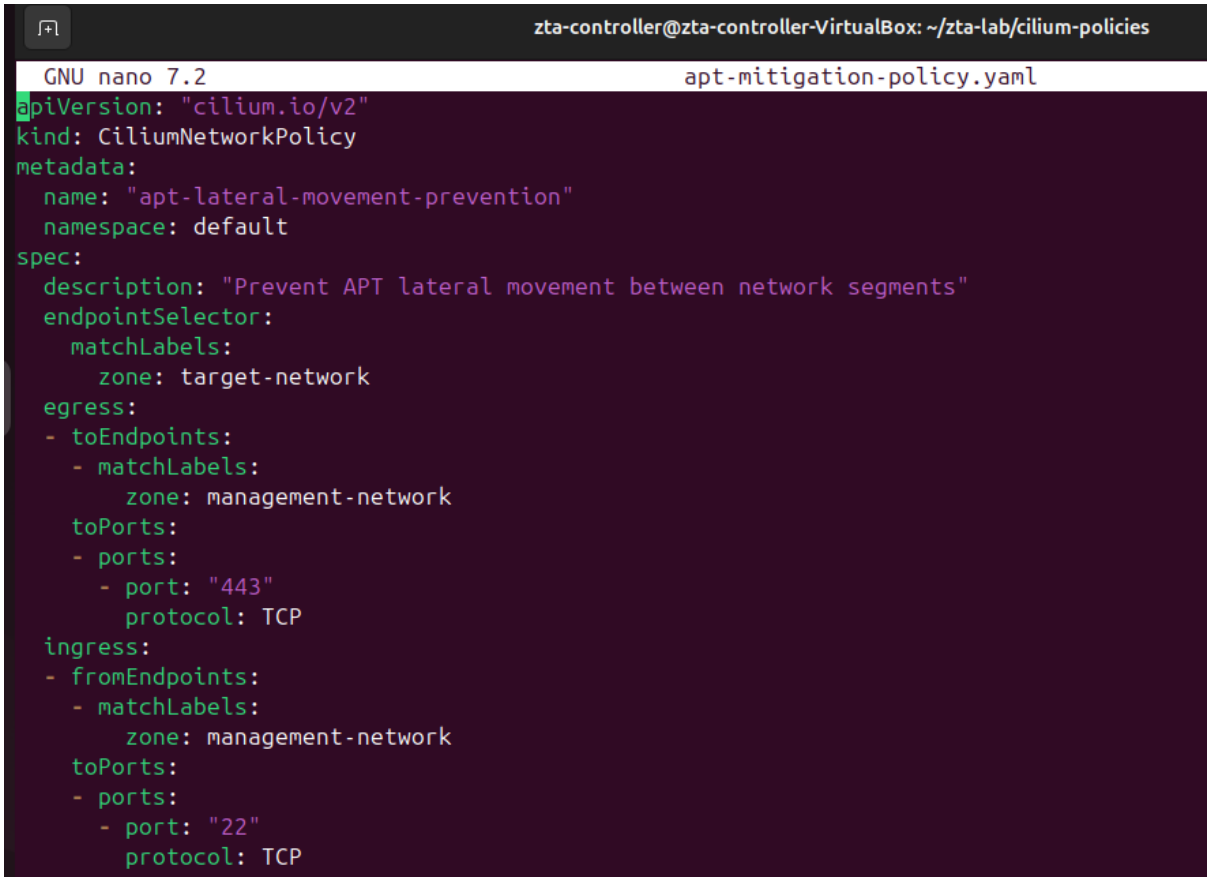


Figure 18: Cilium policy

Now, we move forward with creating system service for monitoring which basically creates a service for monitoring cilium,

- Go to the terminal and type “sudo nano /etc/systemd/system/cilium-monitor.service” and save the file.

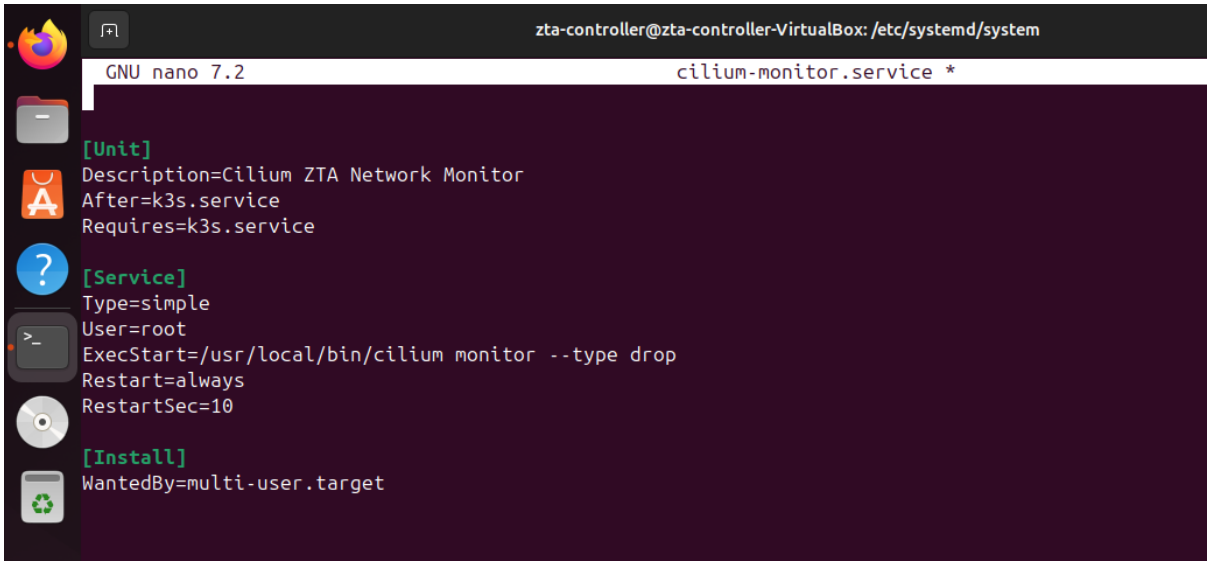


Figure 19: cilium service

3. Installation of Tools in Kali Linux

- We will install Metasploit and Hydra in kali linux for the attack scenario purpose:

Below is the installation of the tools.

- Sudo apt install Metasploit-framework
- systemctl enable --now postgresql
- systemctl status postgresql
- msfdb init
- msfconsole

Figure 20: Metasploit

Figure 21: Hydra

4. Installation of Wazuh Agent in Ubuntu server (Victim Machine)

Below is the commands for installation of agent.

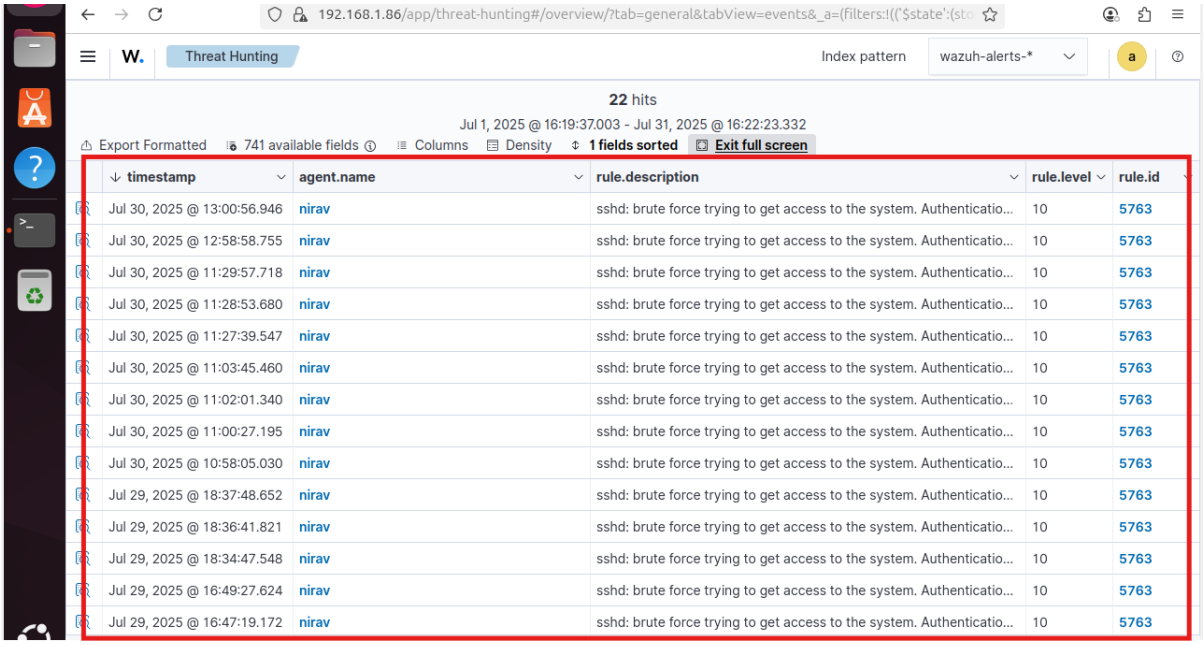
- Initially, Install the GPG Key by using the following command
  Command : “curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg”.

- Add the repository by usung the following command
  Command: echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list.

- Update the current package:
  Command: **apt-get update**

Below is the attack simluations of all the attack scenarios.

1. **SSH Brute Force Attack**: Detection of the SSH brutefore attacks whene therer is 8 or more then 8 failed login from the same IP address in the time span of 120 seconds.



timestamp	agent.name	rule.description	rule.level	rule.id
Jul 30, 2025 @ 13:00:56.946	nirav	sshd: brute force trying to get access to the system. Authenticatio...	10	5763
Jul 30, 2025 @ 12:58:58.755	nirav	sshd: brute force trying to get access to the system. Authenticatio...	10	5763
Jul 30, 2025 @ 11:29:57.718	nirav	sshd: brute force trying to get access to the system. Authenticatio...	10	5763
Jul 30, 2025 @ 11:28:53.680	nirav	sshd: brute force trying to get access to the system. Authenticatio...	10	5763
Jul 30, 2025 @ 11:27:39.547	nirav	sshd: brute force trying to get access to the system. Authenticatio...	10	5763
Jul 30, 2025 @ 11:03:45.460	nirav	sshd: brute force trying to get access to the system. Authenticatio...	10	5763
Jul 30, 2025 @ 11:02:01.340	nirav	sshd: brute force trying to get access to the system. Authenticatio...	10	5763
Jul 30, 2025 @ 11:00:27.195	nirav	sshd: brute force trying to get access to the system. Authenticatio...	10	5763
Jul 30, 2025 @ 10:58:05.030	nirav	sshd: brute force trying to get access to the system. Authenticatio...	10	5763
Jul 29, 2025 @ 18:37:48.652	nirav	sshd: brute force trying to get access to the system. Authenticatio...	10	5763
Jul 29, 2025 @ 18:36:41.821	nirav	sshd: brute force trying to get access to the system. Authenticatio...	10	5763
Jul 29, 2025 @ 18:34:47.548	nirav	sshd: brute force trying to get access to the system. Authenticatio...	10	5763
Jul 29, 2025 @ 16:49:27.624	nirav	sshd: brute force trying to get access to the system. Authenticatio...	10	5763
Jul 29, 2025 @ 16:47:19.172	nirav	sshd: brute force trying to get access to the system. Authenticatio...	10	5763

Figure 22: SSH Brute Force Attack

2. **SQL Injection Attack:** The SQL injection attempt has been detetected all the attempts which were targeting web application and has the near real time detection.

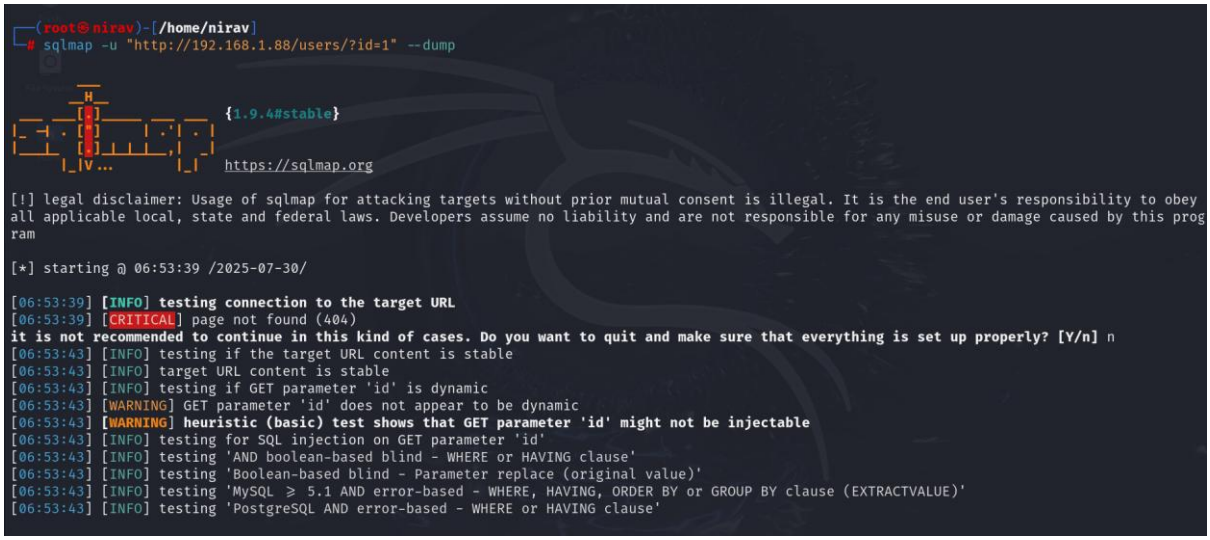


Figure 23: SQL Map

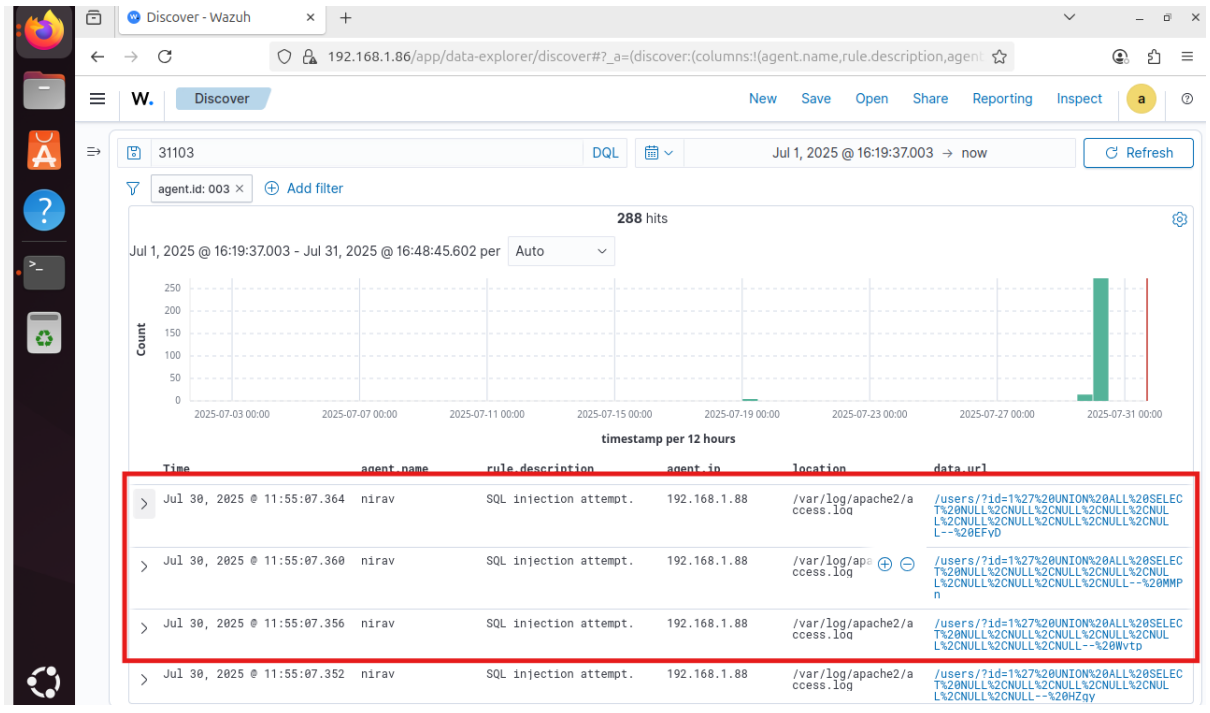


Figure 24: SQL Injection Attempt

3. **File Integrity Monitoring:** This usecase detects any creation of file or any modeificaiotns in the file system, using the checksum values for monitoring.

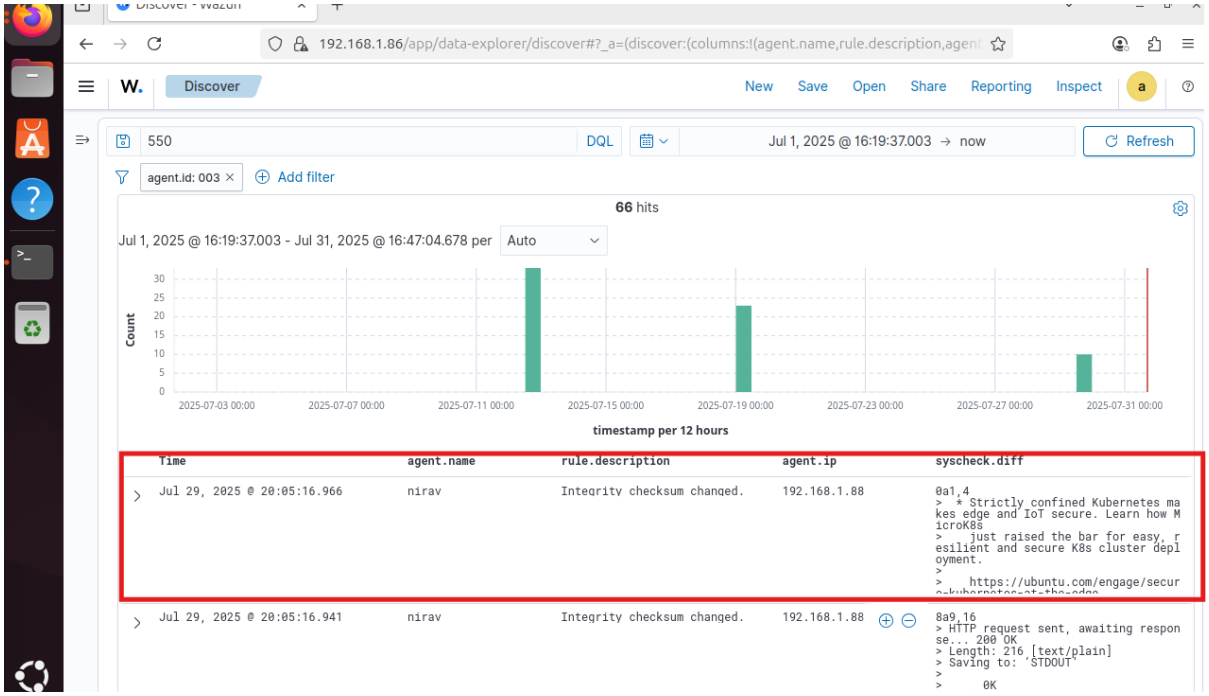


Figure 25: FIM

4. **Detection of Shellshock Attack:** This identifies the shellshock vulenabilty in the insfrasstruture and detects it in near real time.

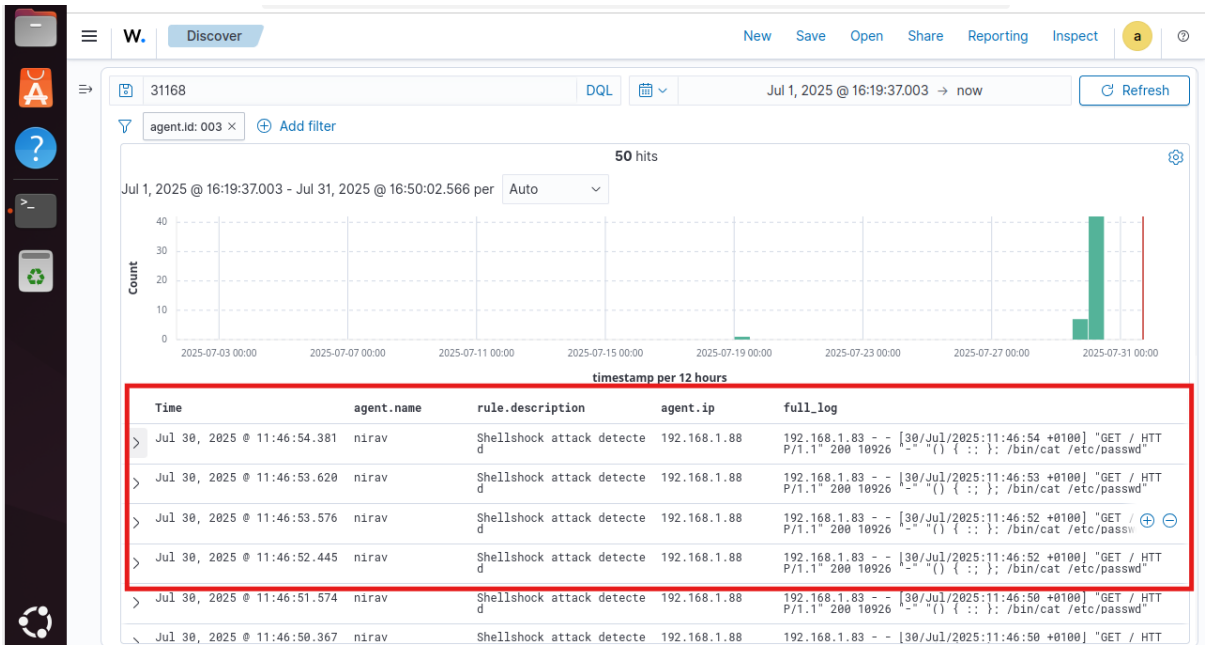


Figure 26: Shell Shock Attack detection

5. **Detection of the Unauthorized Processess:** This policy detects the unautorized network tools such as netcat sessions which is on listening and is the indication of the reverse shell scripts.

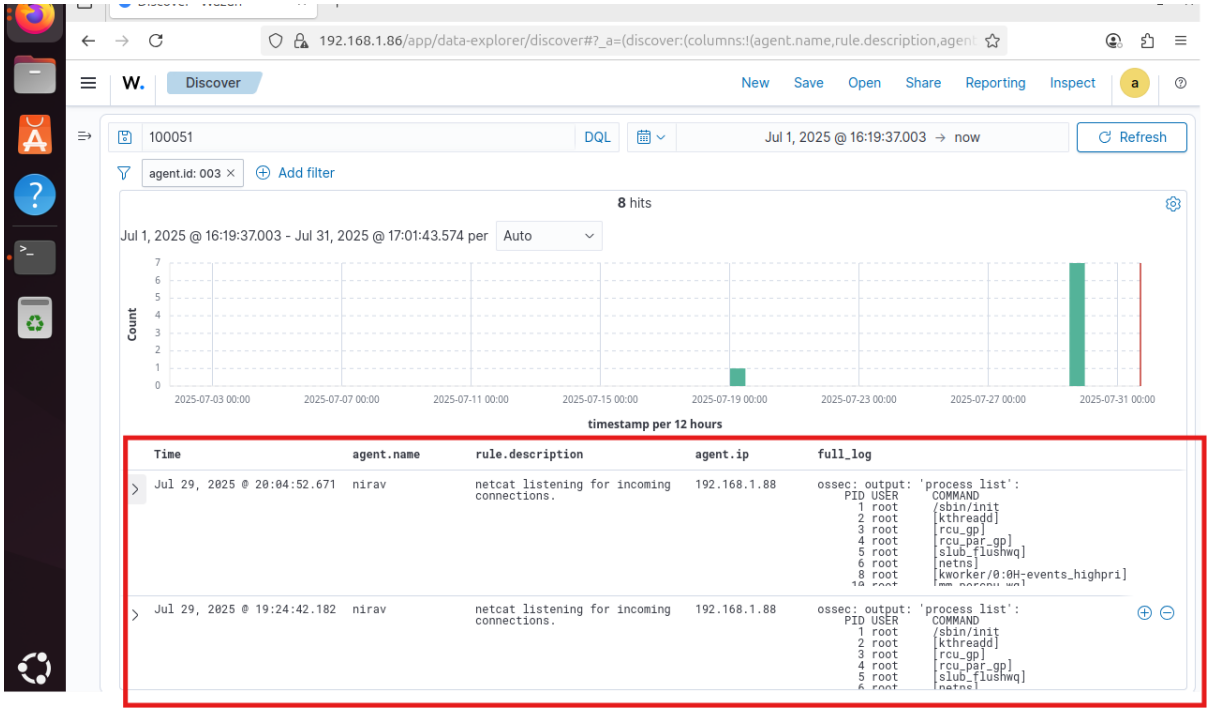


Figure 27: Unauthorized process

6. **Multiple Authentication Failures:** This rule triggers as there are lot of multiple authentication failures with in the short span of time in around 120 seconds.

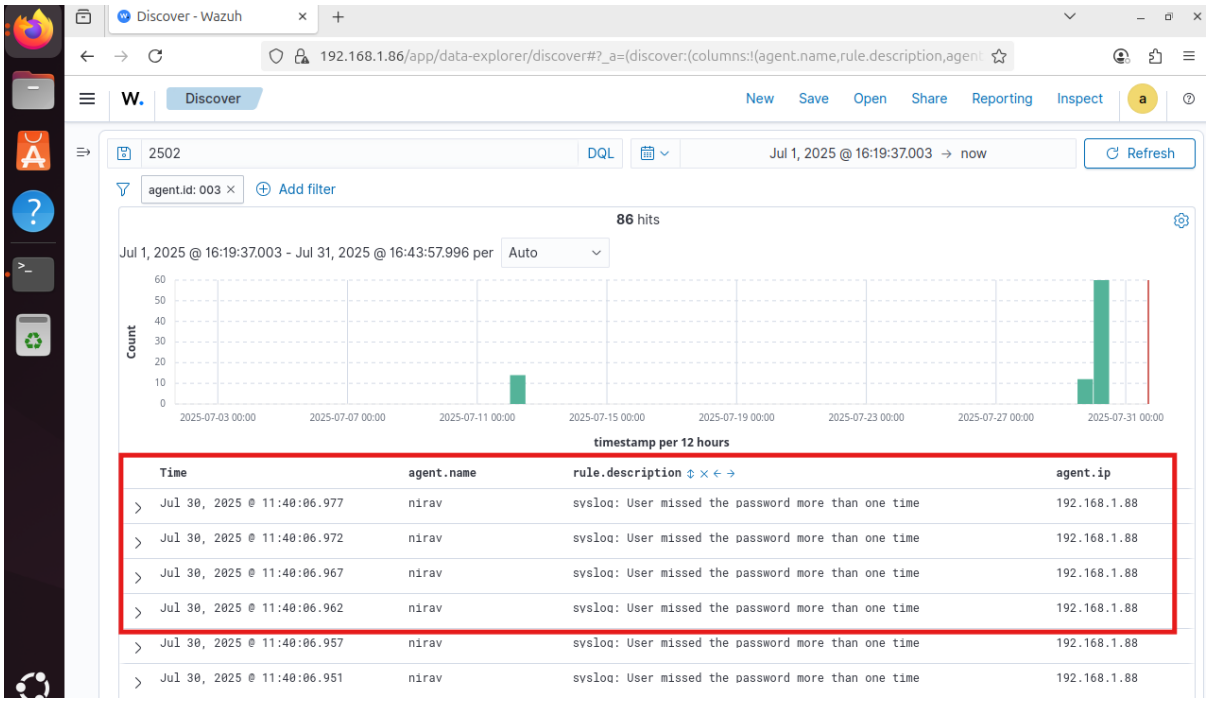


Figure 28: Multiple authentication Failure

7. **Non Existing User login attempts:** This rule is designed for detecting the adversaries reconnaissance techniques as they try to login using multiple usernames.

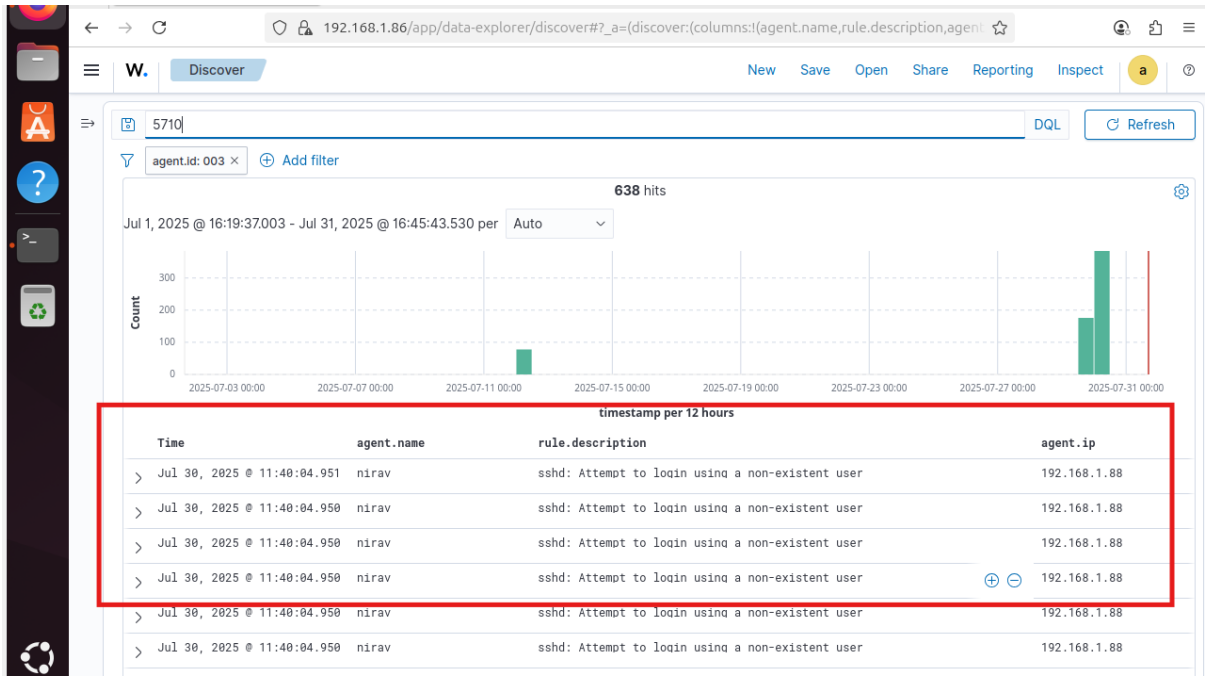


Figure 29: Non Existing User Login

8. **Successful login after the multiple failed attempts**: The rule triggers when there is successful login after the lots of failed login attempts in around time span of 240 seconds.

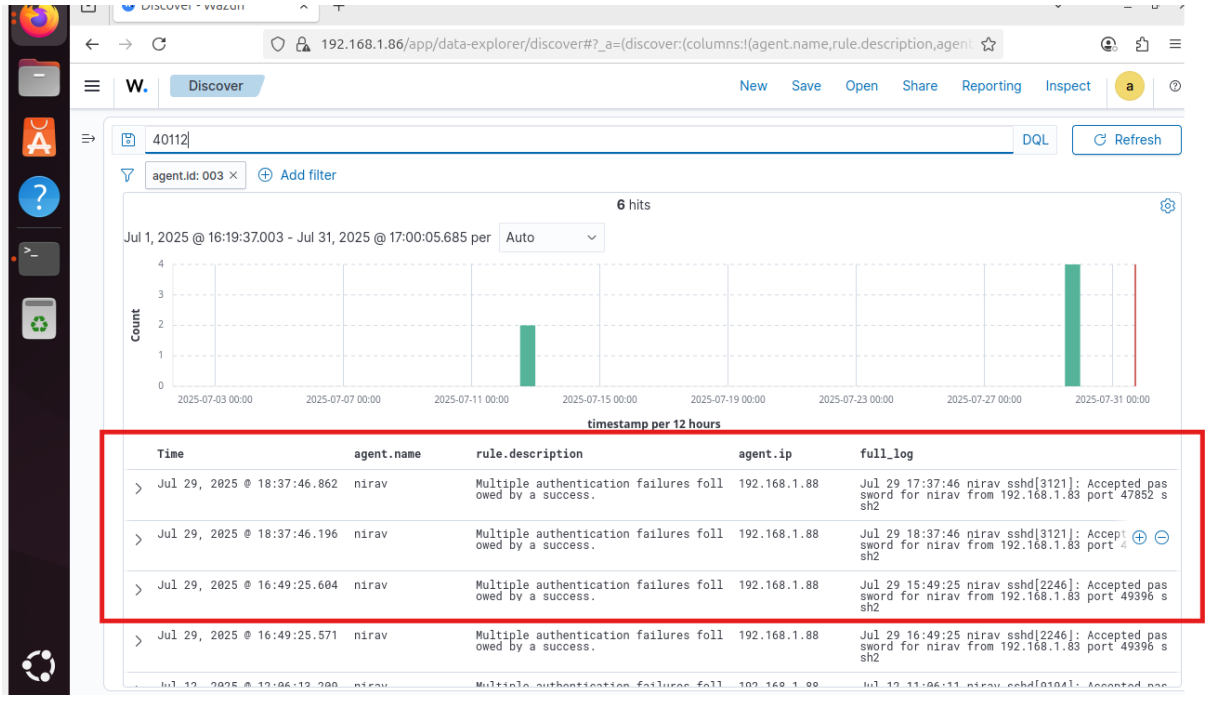


Figure 30: Successful Login after multiple failed Attempts

References

Spiffe.io. (2025). SPIFFE | Install the SPIRE Server. [online] Available at: https://spiffe.io/docs/latest/deploying/install-server/ [Accessed 21 Jul. 2025].

Wazuh (n.d.). Deploying Wazuh agents on Linux systems - Wazuh agent. [online] documentation.wazuh.com. Available at: https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-linux.html.

Wazuh (2024). Installing the Wazuh server step by step - Wazuh server. [online] Wazuh.com. Available at: https://documentation.wazuh.com/current/installation-guide/wazuh-server/step-by-step.html.