wazuh.

Name: Tehreem Amna

Internship Title: SOC Internship Program

Task Title: Wazuh Installation and File Integrity Monitoring (FIM)

Date: 30 July 2025

Task Objective:

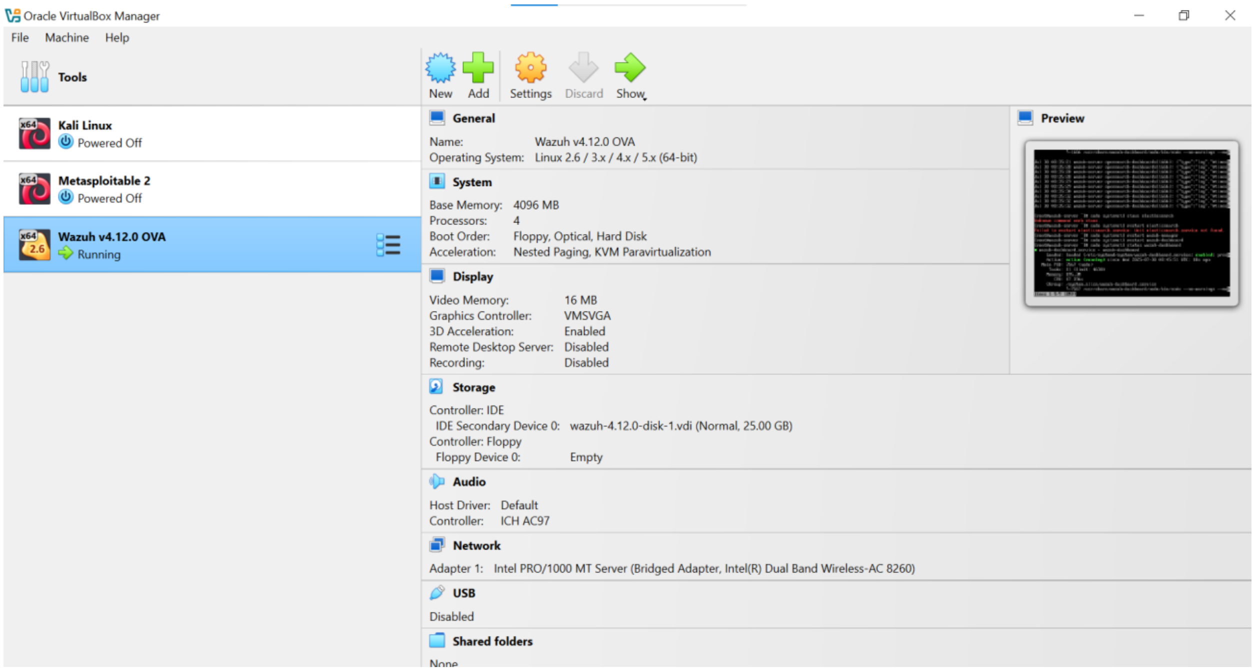
In this task, I installed Wazuh in a virtual environment and set up its File Integrity Monitoring (FIM) feature. The main idea was to make sure any unauthorized changes to files like creating, editing, or deleting could be detected in real time. This setup is a crucial first step, as it forms the foundation for more advanced monitoring and traffic analysis later on.

Part A: Wazuh Installation

Component	Description
Platform	VMware / VirtualBox
OS	Wazuh All-in-One VM (Ubuntu-based)
Agent Machine	Windows 10 (with Wazuh agent)

Installation Steps:

1. Import the Wazuh appliance into VirtualBox to set up the environment.



General

Name: Wazuh v4.12.0 OVA
Operating System: Linux 2.6 / 3.x / 4.x / 5.x (64-bit)

System

Base Memory: 4096 MB
Processors: 4
Boot Order: Floppy, Optical, Hard Disk
Acceleration: Nested Paging, KVM Paravirtualization

Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
3D Acceleration: Enabled
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: wazuh-4.12.0-disk-1.vdi (Normal, 25.00 GB)
Controller: Floppy
Floppy Device 0: Empty

Audio

Host Driver: Default
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Server (Bridged Adapter, Intel(R) Dual Band Wireless-AC 8260)

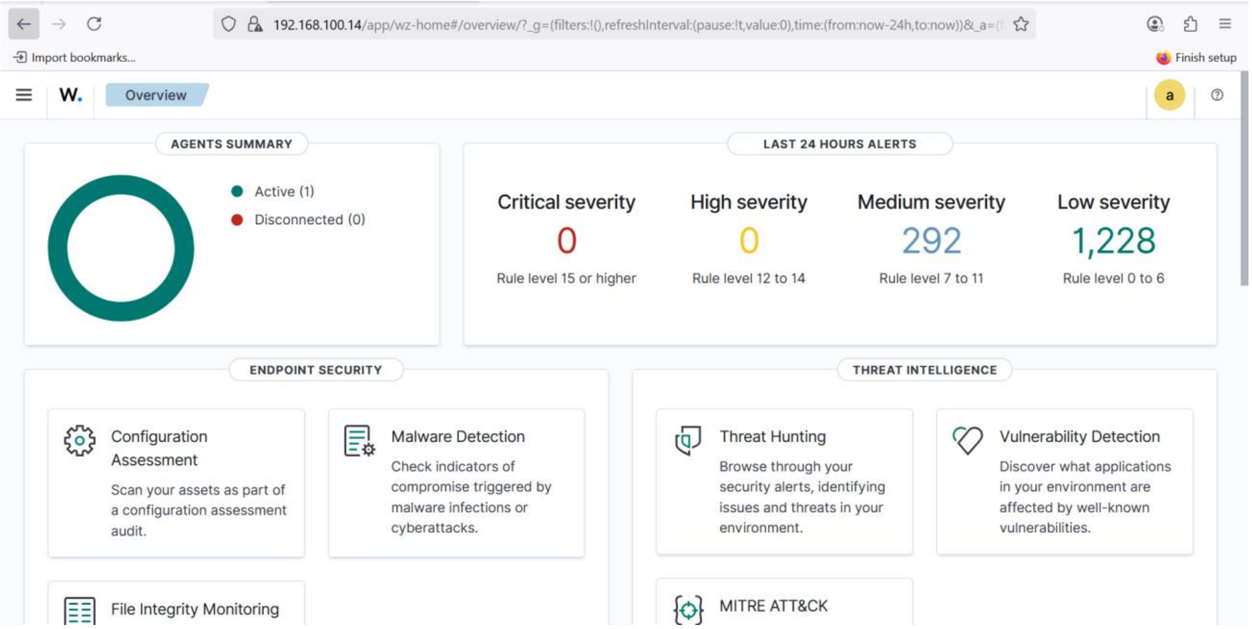
USB

Disabled

Shared folders

None

2. Assign enough RAM and CPU cores to ensure smooth performance.
3. Starting the virtual machine, I accessed the Wazuh Dashboard through my browser using the IP address of the VM.


192.168.100.14/app/wz-home#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(
Import bookmarks...
Finish setup
W.
Overview
a

AGENTS SUMMARY

● Active (1)
● Disconnected (0)

LAST 24 HOURS ALERTS

Critical severity	High severity	Medium severity	Low severity
0	0	292	1,228
Rule level 15 or higher	Rule level 12 to 14	Rule level 7 to 11	Rule level 0 to 6

ENDPOINT SECURITY

Configuration Assessment
Scan your assets as part of a configuration assessment audit.

Malware Detection
Check indicators of compromise triggered by malware infections or cyberattacks.

File Integrity Monitoring

THREAT INTELLIGENCE

Threat Hunting
Browse through your security alerts, identifying issues and threats in your environment.

Vulnerability Detection
Discover what applications in your environment are affected by well-known vulnerabilities.

MITRE ATT&CK

4. Finally, I created a Windows Agent and connected it to the Wazuh Manager using the “Manage Agents” option in the dashboard.

Part B: File Integrity Monitoring (FIM) Configuration

Monitored Path:

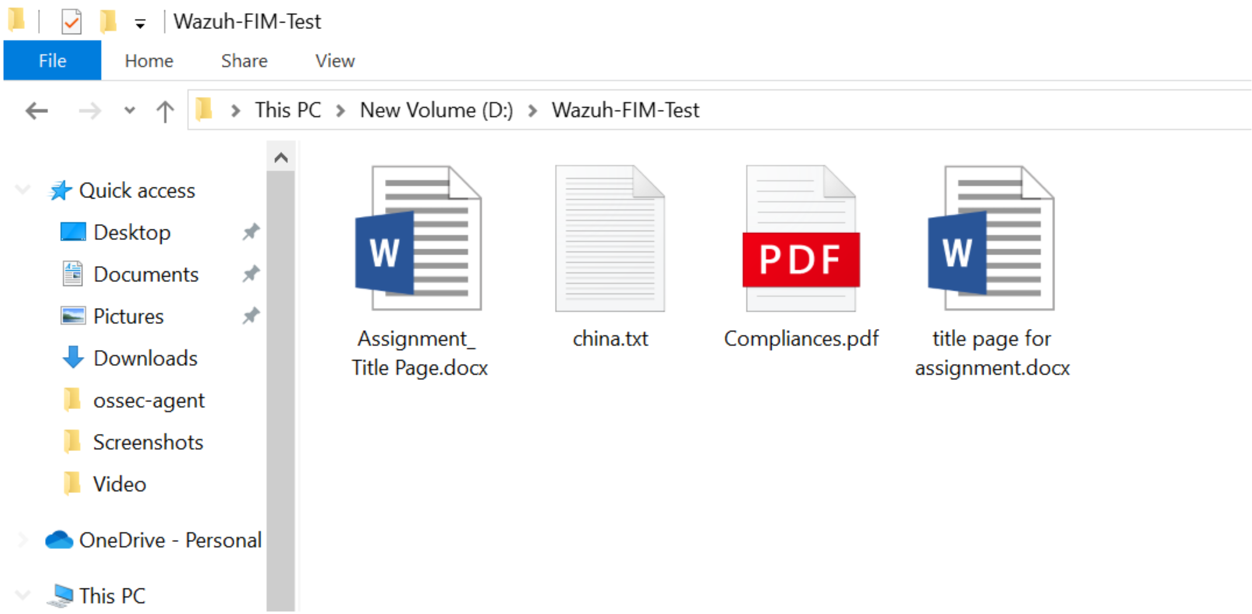
D:\Wazuh-FIM-Test

Agent-Side Configuration (ossec.conf):

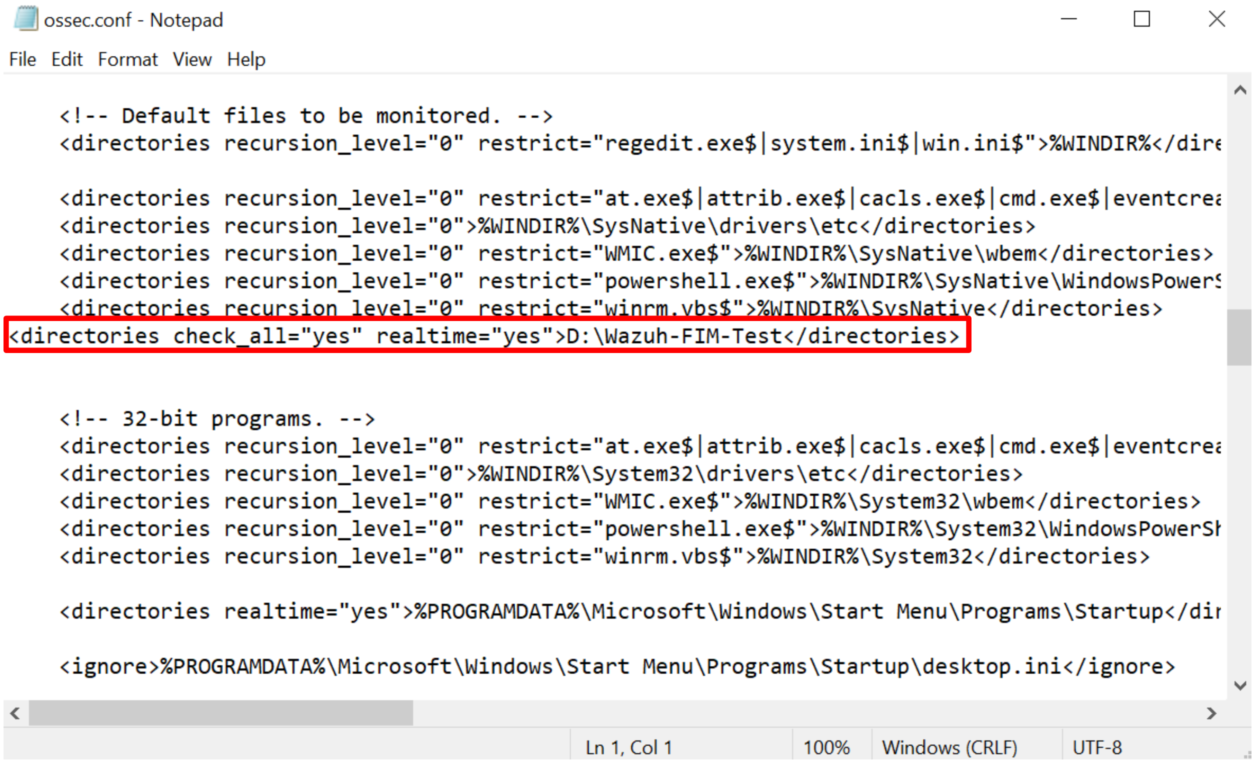
```
<syscheck>

  <directories check_all="yes"> D:\Wazuh-FIM-Test</directories>

</syscheck>
```

Procedure:

1. Created a folder Wazuh-FIM-Test in D drive.



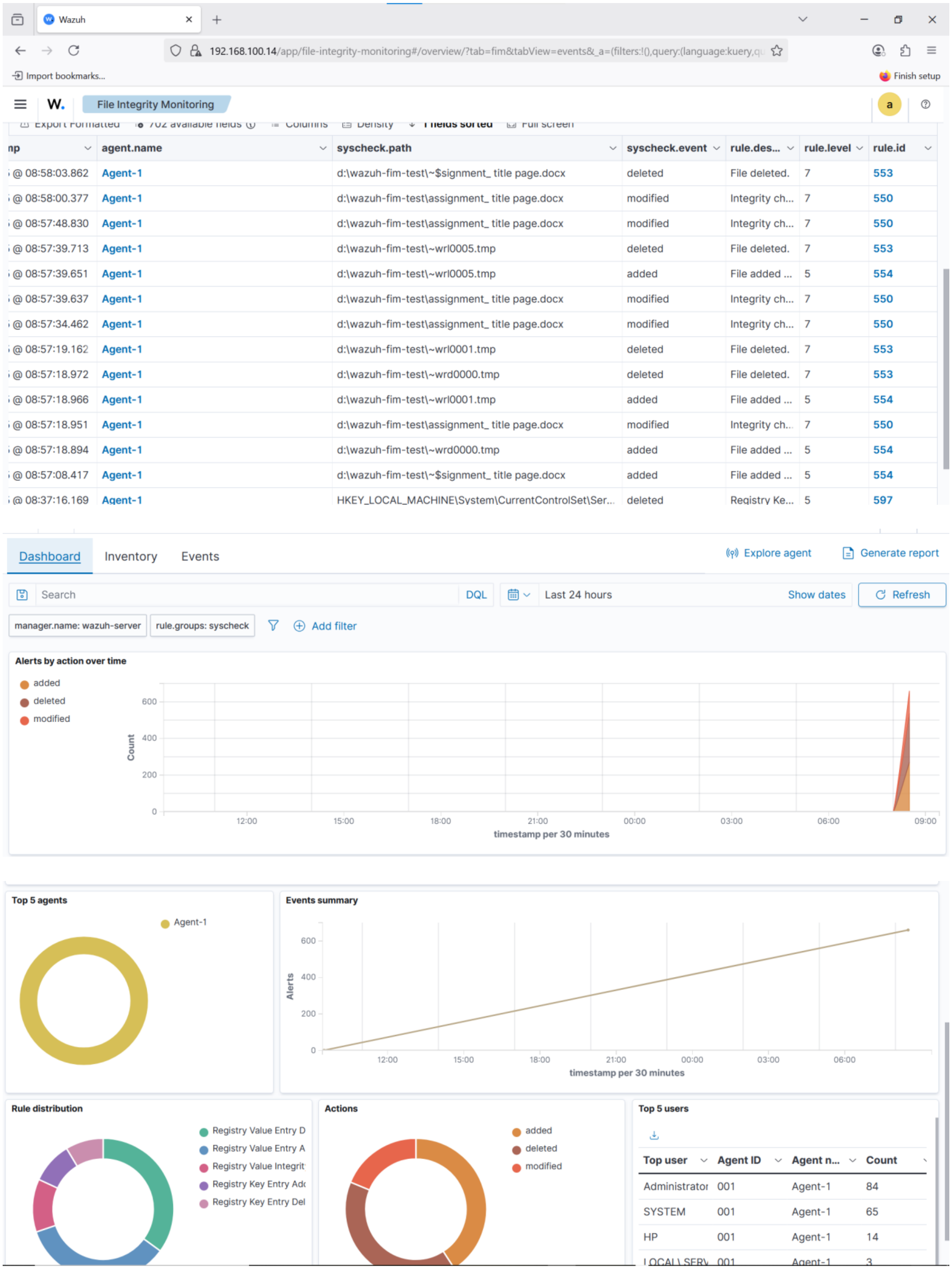
2. Edited ossec.conf file on agent side to include the folder.



```
    <!-- Default files to be monitored. -->
    <directories recursion_level="0" restrict="regedit.exe$|system.ini$|win.ini$">%WINDIR%</dire

    <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcrea
    <directories recursion_level="0">%WINDIR%\SysNative\drivers\etc</directories>
    <directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\SysNative\wbem</directories>
    <directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\SysNative\WindowsPowerS
    <directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\SysNative</directories>
<directories check_all="yes" realtime="yes">D:\Wazuh-FIM-Test</directories>


    <!-- 32-bit programs. -->
    <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcrea
    <directories recursion_level="0">%WINDIR%\System32\drivers\etc</directories>
    <directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\System32\wbem</directories>
    <directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\System32\WindowsPowerSh
    <directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\System32</directories>

    <directories realtime="yes">%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup</dir

    <ignore>%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini</ignore>
```

3. Restart Wazuh Agent.
4. Perform the different operations like Create, Modify, Delete, Added on files.

Part C: Observations on Wazuh Dashboard



Wazuh
192.168.100.14/app/file-integrity-monitoring#/overview/?tab=fim&tabView=events&_a=(filters:!(),query:(language:kuery,qu
Import bookmarks...
Finish setup
W.
File Integrity Monitoring
a
Export Formatted
702 available fields
Columns
Density
1 fields sorted
Full screen

mp	agent.name	syscheck.path	syscheck.event	rule.des...	rule.level	rule.id
@ 08:58:03.862	Agent-1	d:\wazuh-fim-test\~$signment_ title page.docx	deleted	File deleted.	7	553
@ 08:58:00.377	Agent-1	d:\wazuh-fim-test\assignment_ title page.docx	modified	Integrity ch...	7	550
@ 08:57:48.830	Agent-1	d:\wazuh-fim-test\assignment_ title page.docx	modified	Integrity ch...	7	550
@ 08:57:39.713	Agent-1	d:\wazuh-fim-test\~wrl0005.tmp	deleted	File deleted.	7	553
@ 08:57:39.651	Agent-1	d:\wazuh-fim-test\~wrl0005.tmp	added	File added ...	5	554
@ 08:57:39.637	Agent-1	d:\wazuh-fim-test\assignment_ title page.docx	modified	Integrity ch...	7	550
@ 08:57:34.462	Agent-1	d:\wazuh-fim-test\assignment_ title page.docx	modified	Integrity ch...	7	550
@ 08:57:19.162	Agent-1	d:\wazuh-fim-test\~wrl0001.tmp	deleted	File deleted.	7	553
@ 08:57:18.972	Agent-1	d:\wazuh-fim-test\~wrd0000.tmp	deleted	File deleted.	7	553
@ 08:57:18.966	Agent-1	d:\wazuh-fim-test\~wrl0001.tmp	added	File added ...	5	554
@ 08:57:18.951	Agent-1	d:\wazuh-fim-test\assignment_ title page.docx	modified	Integrity ch...	7	550
@ 08:57:18.894	Agent-1	d:\wazuh-fim-test\~wrd0000.tmp	added	File added ...	5	554
@ 08:57:08.417	Agent-1	d:\wazuh-fim-test\~$signment_ title page.docx	added	File added ...	5	554
@ 08:37:16.169	Agent-1	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Ser...	deleted	Registry Ke...	5	597

Alerts by action over time

Top 5 agents

Events summary

Rule distribution

Actions

Top 5 users

Top user	Agent ID	Agent n...	Count
Administrator	001	Agent-1	84
SYSTEM	001	Agent-1	65
HP	001	Agent-1	14
LOCAL SERV	001	Agent-1	3

Part D: Tuning & Alert Filtering:

To reduce unnecessary alerts and cut down on false positives, I made a few important adjustments:

- I used the check_all="yes" attribute, which helps Wazuh focus only on actual content changes instead of triggering alerts for every minor file update.
- I also looked into setting up rules to ignore temporary or system files since these changes often and usually aren't a real threat.

Conclusion:

In this task, I successfully installed Wazuh and explored how its File Integrity Monitoring (FIM) module works. After setting everything up, I tested the system by creating, modifying, and deleting some files. Wazuh was able to detect all these changes in real-time, just as expected. This confirmed that the monitoring setup was working properly. I also learned that with a bit of fine-tuning, it's possible to minimize false alerts while still keeping strong visibility into what's happening on the system.