Linux File Integrity Monitoring using Wazuh

BY: GOKUL KRISHNA K

OBJECTIVE

The objective of this project is to implement a File Integrity Monitoring (FIM) system on a Linux environment using Wazuh to detect, track, and alert on any unauthorized or suspicious changes made to critical files and directories. This project aims to strengthen system security by ensuring that any modification to important files is immediately identified, logged, and investigated.

TOOLS USED

UBUNTU SERVER

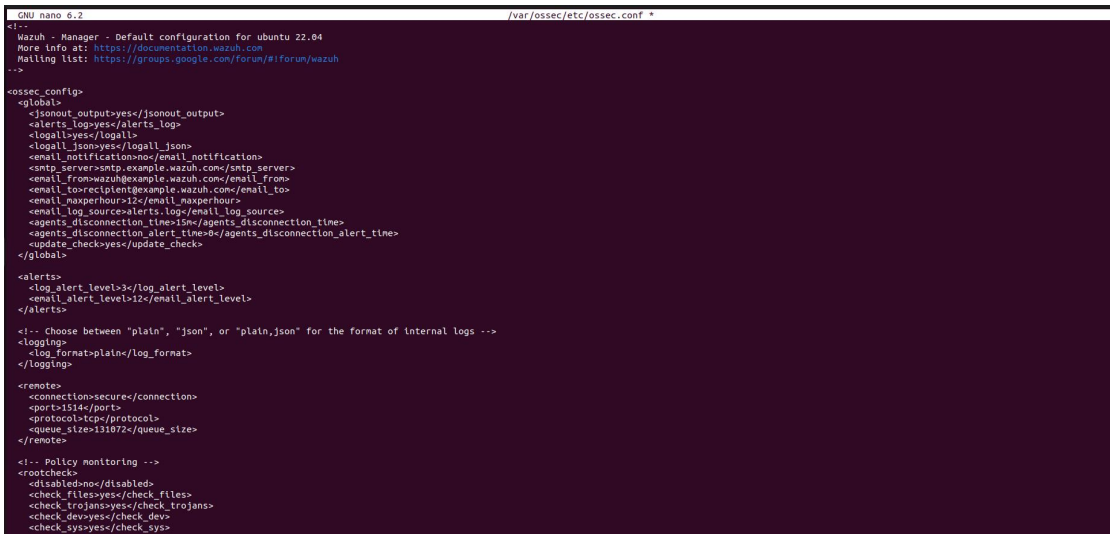
UBUNTU DESKTOP

VRITUALBOX

WAZUH SERVER

WAZUH AGENT

Wazuh Server Setup

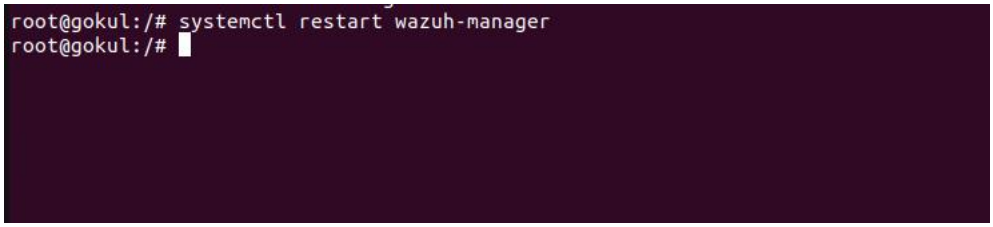


I opened server configuration file for some modifications and I enabled both <logall> and <logall_json> in the Wazuh configuration to ensure complete logging and structured storage of all events.logall allows the agent to record every activity, which is essential for detailed File Integrity Monitoring.logall_json stores these logs in JSON format, making them easier to analyze, parse, and visualize in the Wazuh dashboard or any SIEM.

Command: sudo nano /var/ossec/etc/ossec.conf

1.<logall>yes</logall> — Enables Full Logging

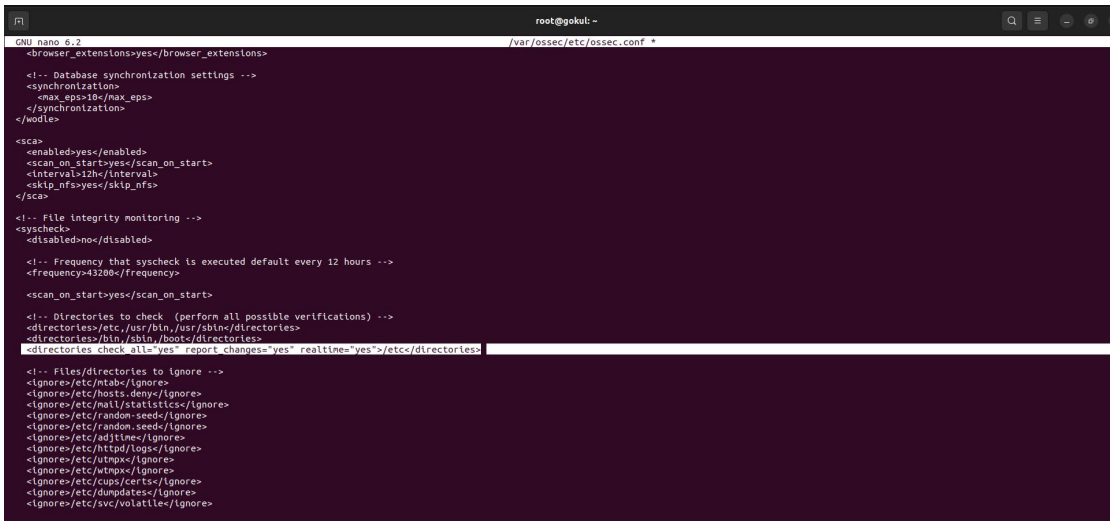
2. <logall_json>yes</logall_json> — Enables JSON Format Logging



I restarted wazuh manager

Command: sudo systemctl restart wazuh-manager

Wazuh Agent Setup



I opend the agent configuration file same like server configuration file and I added <directories check_all="yes" report_changes="yes" realtime="yes">/etc</directories> inside configuration file of wazuh agent.This configuration line in Wazuh File Integrity Monitoring (FIM) tells Wazuh to monitor the /etc directory for security-related file changes.This directive is used to enable File Integrity Monitoring on the /etc directory.
It instructs Wazuh to:

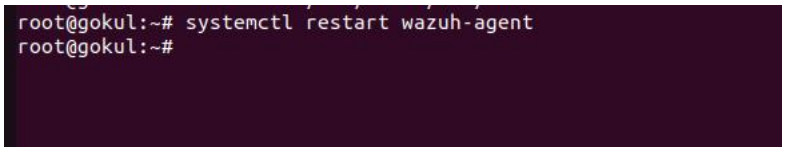
check_all="yes" → Monitor all types of changes, including file creation, deletion, modification, and permission changes.

report_changes="yes" → Generate detailed reports showing what exactly changed inside a file (diff output).

realtime="yes" → Detect and alert on changes immediately using real-time monitoring instead of periodic scans.

By applying this configuration, Wazuh continuously tracks any unauthorized or suspicious modifications in the /etc directory, which is one of the most critical locations in a Linux system because it contains system configurations, user account details, and security settings.

Command : <directories check_all="yes" report_changes="yes" realtime="yes">/etc</directories>

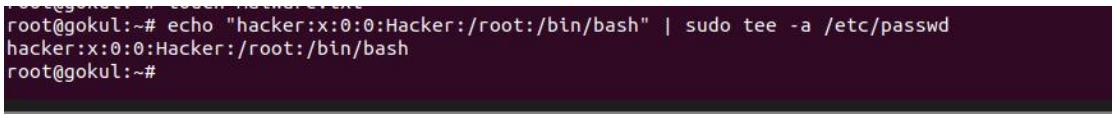


I restart wazuh agent for getting fresh start

Command: sudo systemctl restart wazuh-agent

My First Attack Simulation

Append a fake root user into /etc/passwd:



I had run the echo "hacker:x:0:0:Hacker:/root:/bin/bash" | sudo tee -a /etc/passwd command this is for adds a malicious backdoor user with root privileges, which is commonly used in attacks.This will trigger Wazuh FIM alerts because /etc/passwd is a monitored file and the system's integrity is compromised.

Command: echo "hacker:x:0:0:Hacker:/root:/bin/bash" | sudo tee -a /etc/passwd

My Second Attack Simulation

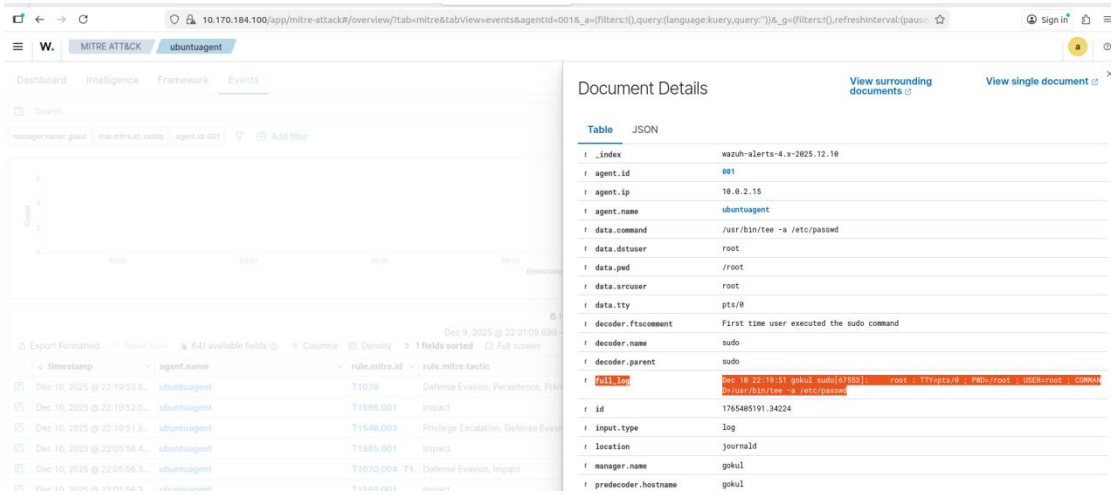
Modify SSH configuration to allow root login:

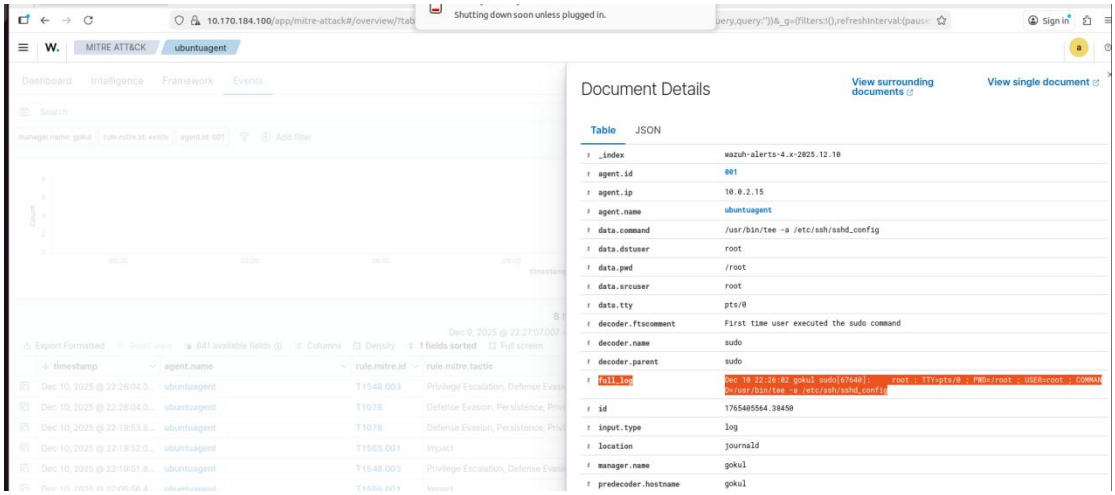
```
root@gokul:~# echo "PermitRootLogin yes" | sudo tee -a /etc/ssh/sshd_config
PermitRootLogin yes
root@gokul:~#
```

It enables remote login as root using SSH (which is normally disabled for security reasons).I appended the line PermitRootLogin yes to the SSH configuration file /etc/ssh/sshd_config.
This change enables SSH login for the root account, which is a high-risk security setting.Wazuh File Integrity Monitoring detects this modification and generates a security alert indicating that a critical system configuration file was altered.

Command: echo "PermitRootLogin yes" | sudo tee -a /etc/ssh/sshd_config

I accessed the Wazuh server to review the security alerts triggered by the attack I performed





Both alerts were visible on the Wazuh server during my analysis.

CONCLUSION

The implementation of File Integrity Monitoring (FIM) using Wazuh successfully demonstrated how critical system files in a Linux environment can be continuously monitored for unauthorized changes. By configuring Wazuh agents to track directories such as /etc, the system was able to detect and alert on high-risk activities, including modifications to /etc/passwd and /etc/ssh/sshd_config. These actions simulated real-world attack scenarios such as privilege escalation and insecure configuration changes.