



## **Task No: 01**

### **Wazuh Installation & FIM Monitoring**

**Name**

**Saad Naveed**

**Team**

**SOC Phi**

**Duration**

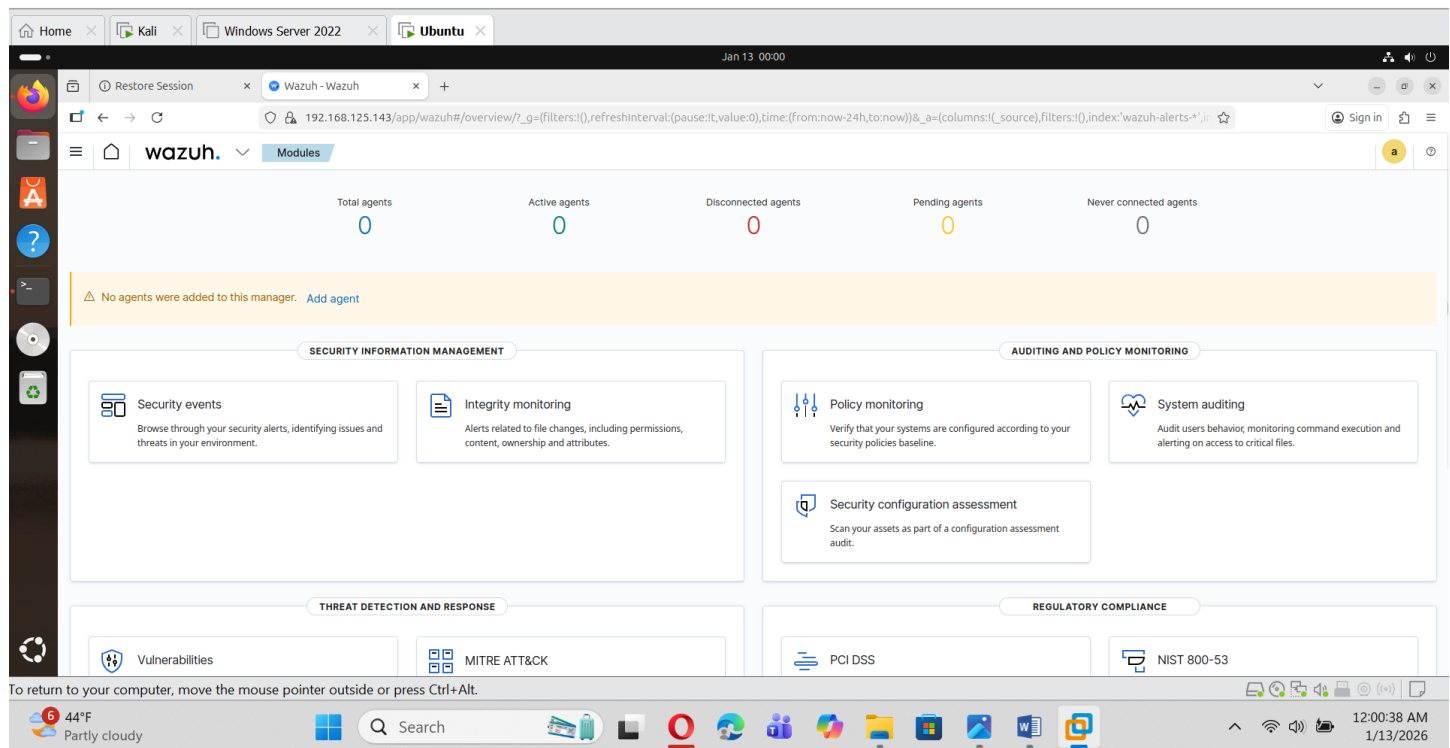
**10 days**

## Goal:

- Wazuh setup
- Start real-time log collection
- Configure **File Integrity Monitoring (FIM)**
- Generate alerts
- Reduce false positives

## Step 1:

I have successfully install & set-up wazuh in Ubuntu.



WAZUH SERVER IP = 192.168.125.143

## Step: 02

Configure Kali Linux Agent

On kali linux terminal & Install wazuh agent

```
(syrian@kali) - [~/Desktop]
$ sudo apt install wazuh-agent -y

wazuh-agent is already the newest version (4.14.1-1).
The following packages were automatically installed and are no longer required:
  curlftpfs libboost-chrono1.83.0t64 libgirepository-1.0-1 libradare2-5.0.0t64 python3-pysmi
  gir1.2-girepository-2.0 libboost-program-options1.83.0 libgnome-rr-4-2t64 libsqlcipher1 tini
  libarmadillo14 libgdal37 libobjc-14-dev linux-image-6.12.25-amd64
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1195

(syrian@kali) - [~/Desktop]
$ sudo nano /var/ossec/etc/ossec.conf

(syrian@kali) - [~/Desktop]
$
```

## Register Kali Agent with Manager:

```
(syrian@kali) - [~/Desktop]
$ sudo systemctl daemon-reload

(syrian@kali) - [~/Desktop]
$ sudo systemctl enable wazuh-agent

(syrian@kali) - [~/Desktop]
$ sudo systemctl start wazuh-agent

(syrian@kali) - [~/Desktop]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:55:4f:b6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.125.133/24 brd 192.168.125.255 scope global dynamic noprefixroute eth0
        valid_lft 1227sec preferred_lft 1227sec
    inet6 fe80::20c:29ff:fe55:4fb6/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:9d:4a:3d:39 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever

(syrian@kali) - [~/Desktop]
$
```

## Wazuh-Agent showing in Wazuh-Manager (Ubuntu)

The screenshot shows the Wazuh Manager web interface running in a browser. The URL is `192.168.125.131/app/endpoints-summary#/agents-preview/`. The interface displays three summary cards: 'AGENTS BY STATUS' showing 1 Active agent, 'TOP 5 OS' showing 'kali' as the top OS, and 'TOP 5 GROUPS' showing 'default' as the top group. Below these is a table titled 'Agents (1)' with a search filter 'status=active'. The table contains one entry for the 'kali' agent, which is active and belongs to the 'default' group. The table has columns for ID, Name, IP address, Group(s), Operating system, Cluster node, Version, Status, and Actions.

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	kali	192.168.125.133	default	Kali GNU/Linux 2025.4	node01	v4.14.1	active	

The screenshot shows the Wazuh dashboard interface. At the top, there's a navigation bar with tabs for 'Endpoints', 'kali', and 'Wazuh'. Below this, a table lists system details for agent 'kali (001)':

ID	Status	IP address	Version	Group	Operating system	Cluster node	Registration date	Last keep alive
001	active	192.168.125.133	Wazuh v4.14.1	default	Kali GNU/Linux 2025.4	node01	Jan 14, 2026 @ 03:10:38.000	Jan 14, 2026 @ 03:21:38.000

Below the table, the 'System inventory' section displays hardware details:

- Cores: 2
- Memory: 3.8GB
- CPU: Intel(R) Core(TM) i7-8565U CPU @ 1.80GHz
- Host name: kali
- Serial number: None

The 'Events count evolution' section shows a line graph with 'Count' on the y-axis (0 to 200) and 'timestamp per 30 minutes' on the x-axis (08:00 to 00:00). The 'MITRE ATT&CK' section lists top tactics: Defense Evasion (2), Privilege Escalation (2), Credential Access (1), Initial Access (1), and Persistence (1). The 'Compliance' section shows a donut chart for PCI DSS with scores: 2.2 (192), 10.6.1 (9), 10.2.5 (4), 10.2.4 (2), and 10.2.7 (1).

## Enable FIM on the Wazuh Agent (Kali)

### Generate FIM Alerts

The screenshot shows a terminal window on a Kali Linux system. The user 'syrian' is at the prompt. The following commands are executed:

```
(syrian@kali) - [~/Desktop]
$ sudo touch /etc/fim_test.txt

(syrian@kali) - [~/Desktop]
$ ls
ALHacking  blackbird  cred.txt  Facad  flag.txt  Info  pandora  phishing  scanning  venv
AndroRAT  BTC        CTF       FASTCTF  Geo-Phone  osint  payload_android  profiles.csv  splunk  zphisher
atm       confidential.pdf  EmailForensics  file  india  osmedeus  PCCCTF  RIUCTF  task

(syrian@kali) - [~/Desktop]
$ echo "test" | sudo tee /etc/fim_test.txt
test

(syrian@kali) - [~/Desktop]
$ sudo rm /etc/fim_test.txt

(syrian@kali) - [~/Desktop]
$
```

### Check Alerts in Wazuh Dashboard:

HomeKaliUbuntu

Jan 18 23:27

New TabWazuh

192.168.125.131/app/endpoints-summary#/agents?tab=welcome&agent=001

Wazuh

Endpointskali

Threat HuntingFile Integrity MonitoringConfiguration AssessmentMITRE ATT&CKVulnerability DetectionMore...

kali (001)StatsConfiguration

ID	Status	IP address	Version	Group	Operating system	Cluster node	Registration date	Last keep alive
001	active	192.168.125.133	Wazuh v4.14.1	default	Kali GNU/Linux 2025.4	node01	Jan 14, 2026 @ 03:10:38.000	Jan 18, 2026 @ 23:27:24.000

System inventory

Cores2


Memory3.8GB

CPUIntel(R) Core(TM) i7-8565U CPU @ 1.80GHz

Host namekali

Serial numberNone

Events count evolution



MITRE ATT&CK

Top Tactics

Defense Evasion45

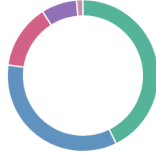
Privilege Escalation40

Initial Access20

Persistence20

Compliance

POI DSS



10.2.5 (62)

10.6.1 (50)

10.2.2 (20)

10.2.6 (11)

10.2.7 (2)

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

System tray icons

```
syrian@kali: ~/Desktop
syrian@kali: /etc/FIM

(syrian@kali) - [/etc]
$ cd FIM

(syrian@kali) - [/etc/FIM]
$ ls
saad.txt

(syrian@kali) - [/etc/FIM]
$ nano saad.txt

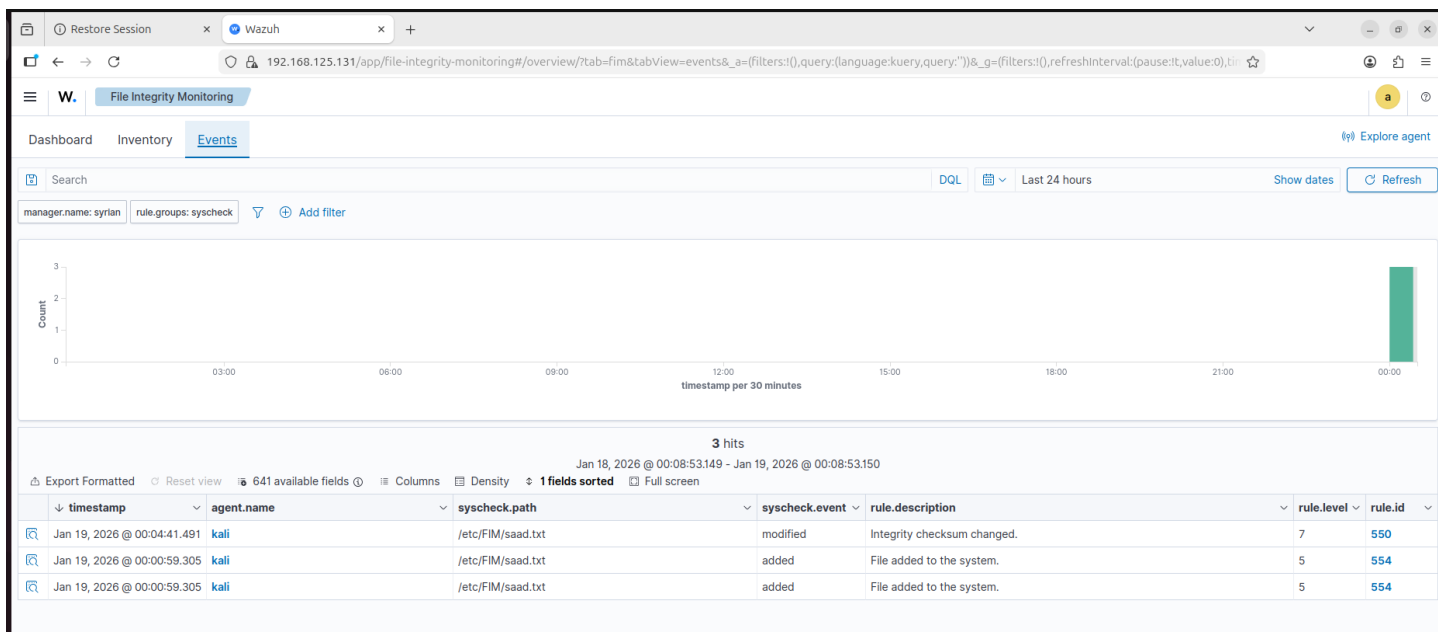
(syrian@kali) - [/etc/FIM]
$ sudo saad.txt
sudo: saad.txt: command not found

(syrian@kali) - [/etc/FIM]
$ sudo nano saad.txt

(syrian@kali) - [/etc/FIM]
$ ls
saad.txt

(syrian@kali) - [/etc/FIM]
$ cat saad.txt
this is my file!

(syrian@kali) - [/etc/FIM]
$
```



I configured File Integrity Monitoring using the syscheck module to monitor critical Linux directories such as /etc, /bin, and /usr/sbin. I validated the configuration by simulating file creation, modification, and deletion, and successfully observed real-time alerts in the Wazuh dashboard.

