Task No: 01

Wazuh Installation & FIM Monitoring

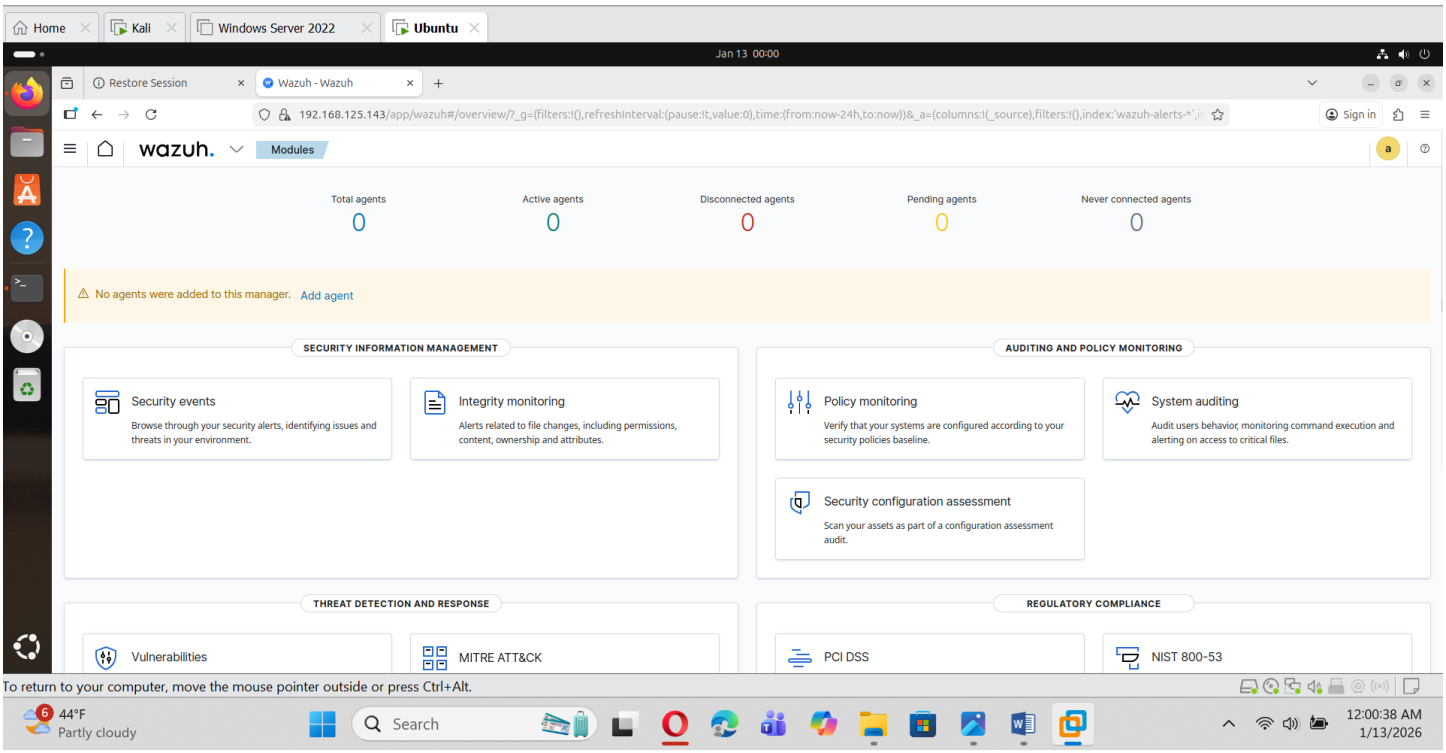
Name	**Saad Naveed**
Team	**SOC Phi**
Duration	**10 days**

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

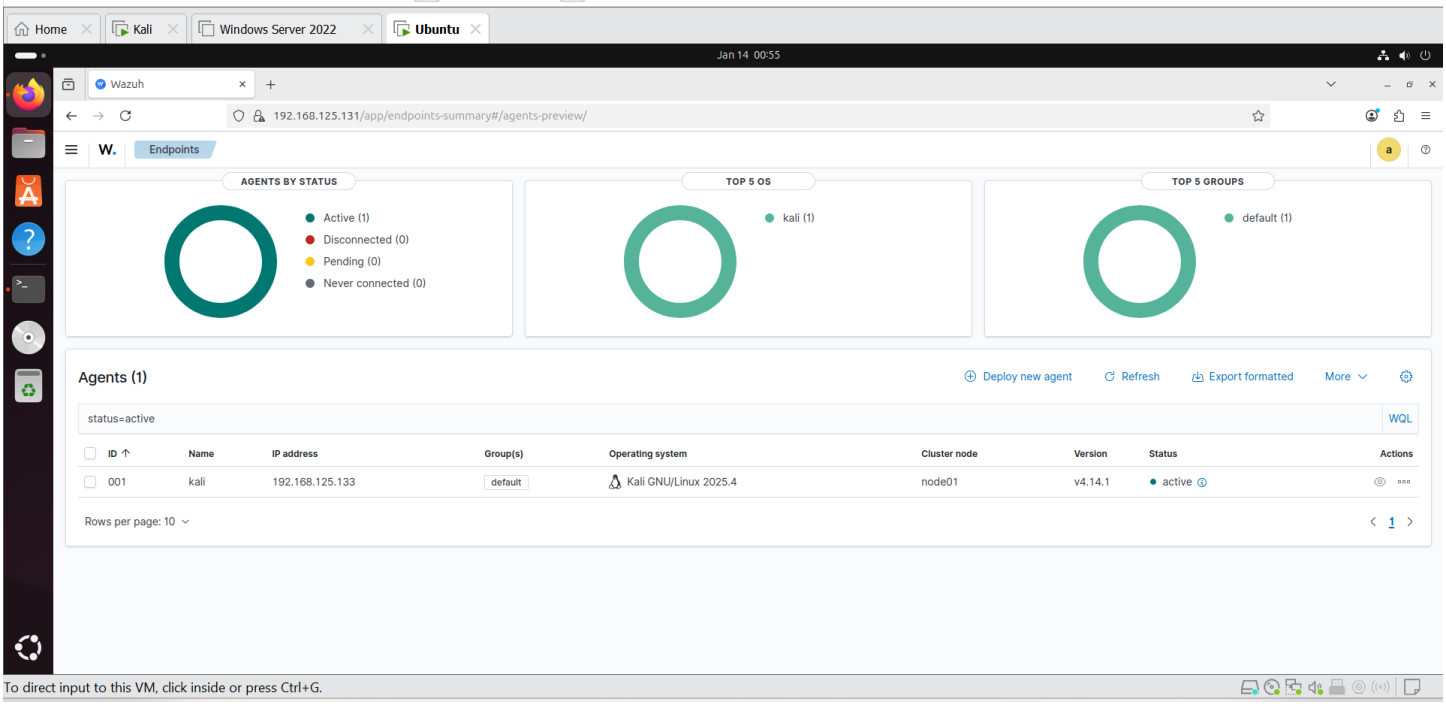
On kali linux terminal & Install wazuh agent

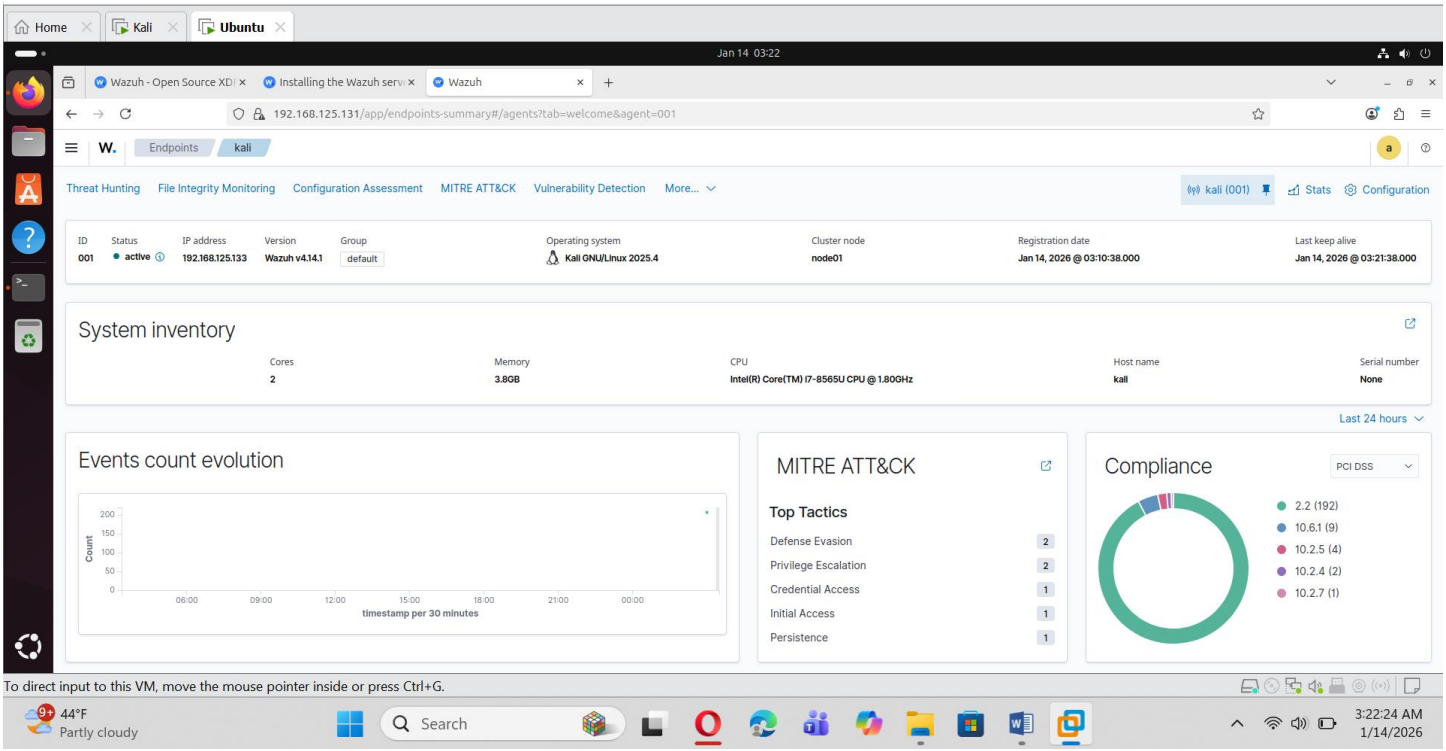
```
┌──(syrian㉿kali)-[~/Desktop]
└─$ sudo apt install wazuh-agent -y

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]
└─$
```

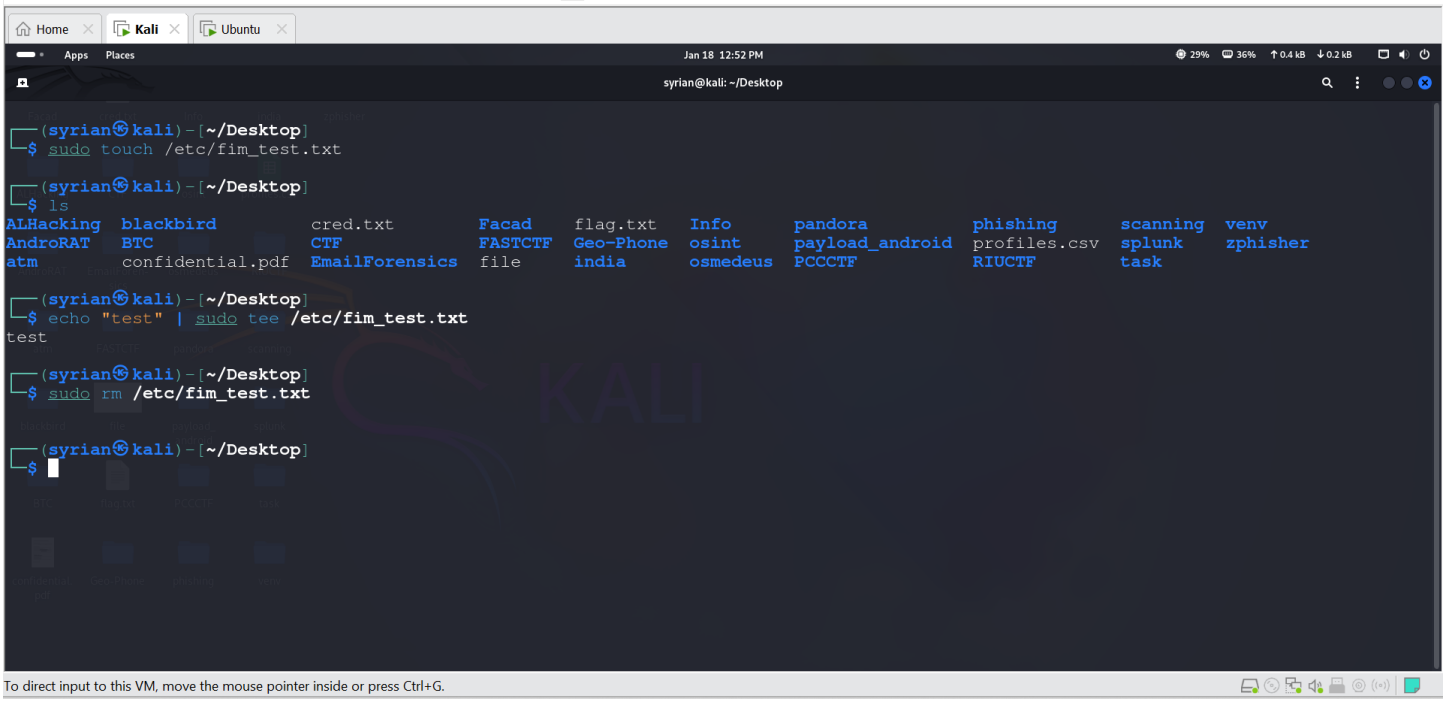
Wazuh-Agent showing in Wazuh-Manager (Ubuntu)



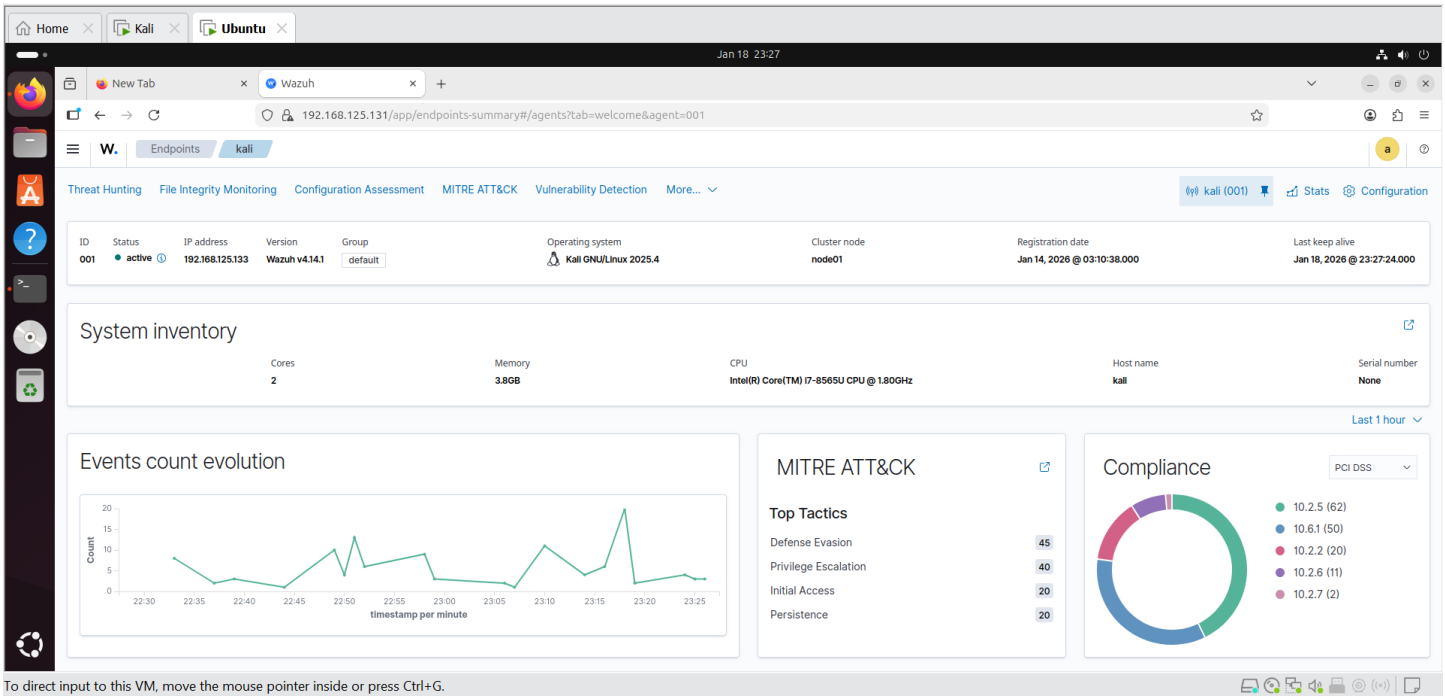


Enable FIM on the Wazuh Agent (Kali)

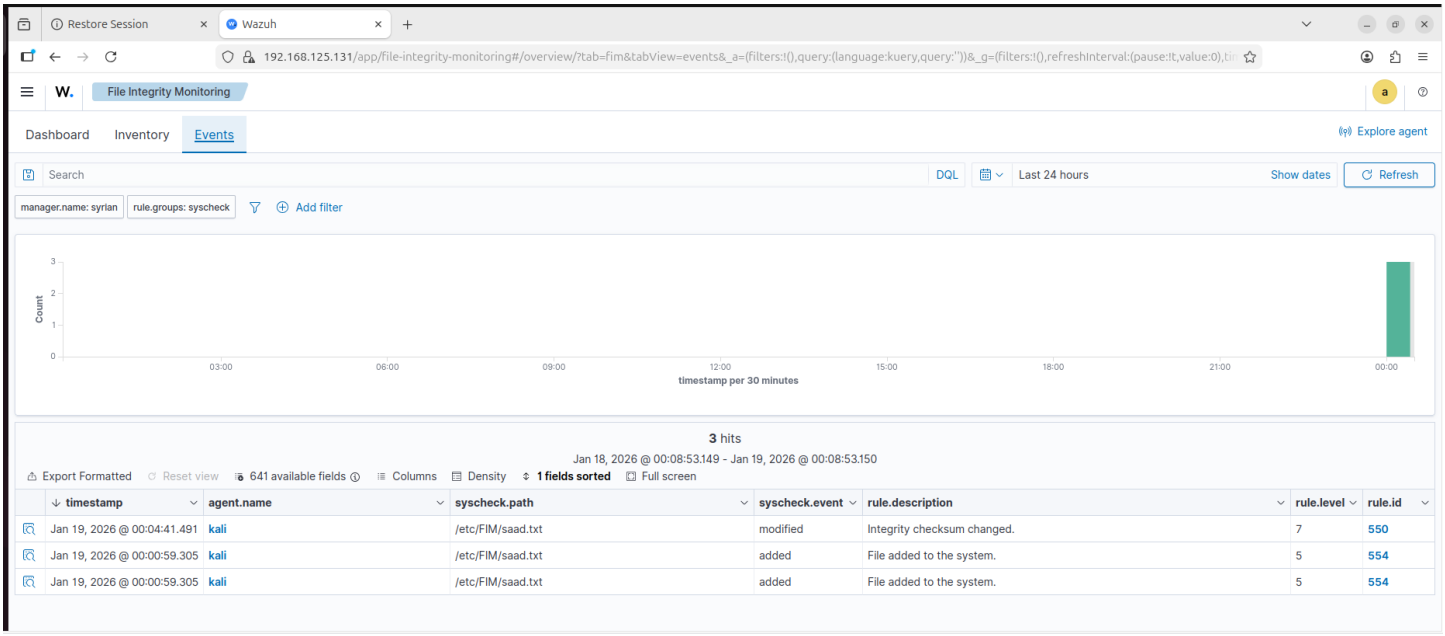
Generate FIM Alerts



Check Alerts in Wazuh Dashboard:



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



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.