



## Task No: 01

### Wazuh Installation & FIM Monitoring

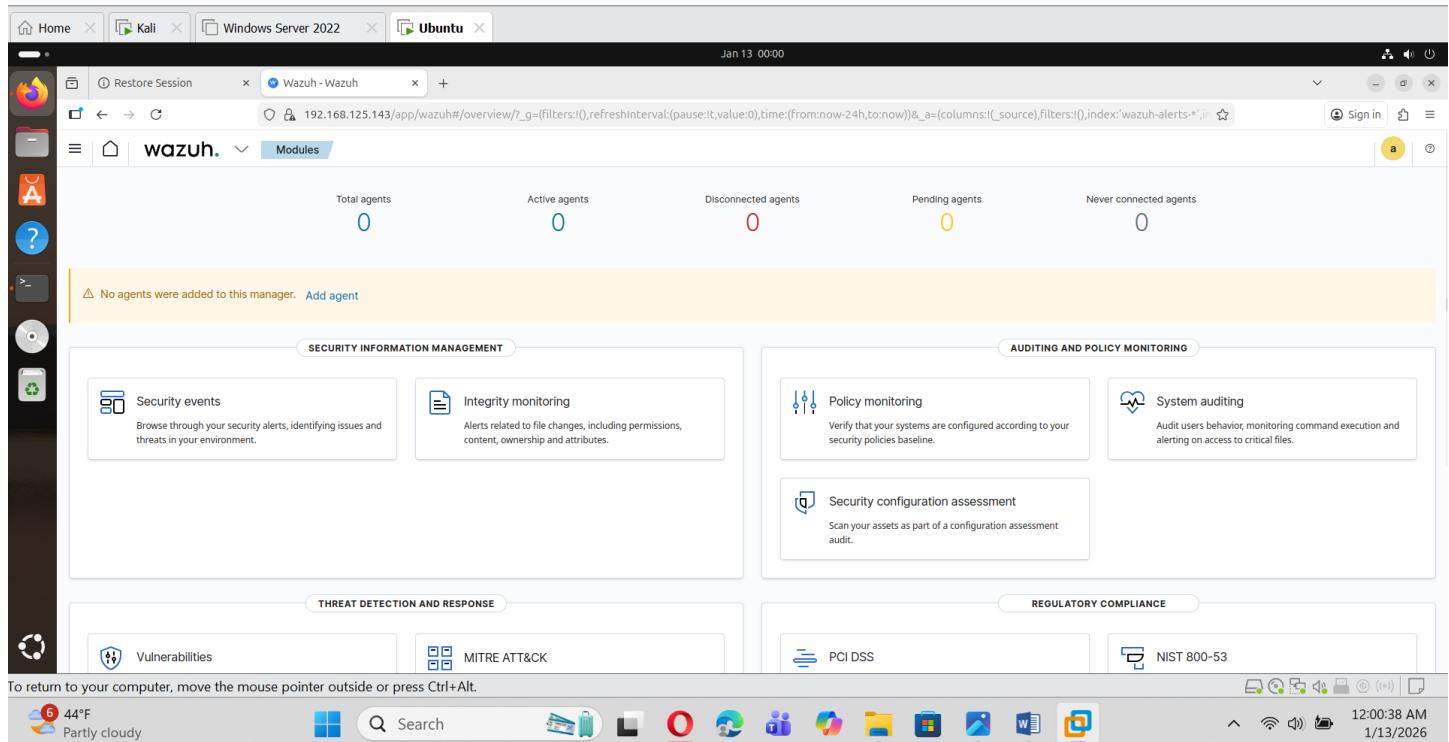
Name	Saad Naveed
Team	SOC Phi
Duration	10 days

## 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
  libbamadillo14    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 interface running on an Ubuntu host. The top navigation bar includes tabs for Home, Kali, Windows Server 2022, and Ubuntu. The main content area is titled 'Wazuh' and displays the 'Endpoints' tab. Key visual elements include three donut charts: 'AGENTS BY STATUS' (all active), 'TOP 5 OS' (kali), and 'TOP 5 GROUPS' (default). Below these charts is a table titled 'Agents (1)' showing the details of the registered agent. The agent listed is 'kali' with IP address 192.168.125.133, belonging to the 'default' group, running Kali GNU/Linux 2025.4, and connected to cluster node 'node01'. The table includes 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	<a href="#">Edit</a>

The screenshot shows a Linux desktop environment with a window manager like Unity. The top bar includes icons for Home, Kali, and Ubuntu. The main window is a browser displaying the Wazuh endpoint monitoring interface at <http://192.168.125.131/app/endpoints-summary#/agents?tab=welcome&agent=001>. The page shows details for a single endpoint (ID 001) and a system inventory table. Below the browser are three panels: 'Events count evolution' (a line chart), 'MITRE ATT&CK' (a list of tactics with counts), and 'Compliance' (a donut chart).

Wazuh - Open Source XD | Installing the Wazuh server | Wazuh

Jan 14 03:22

Endpoints kali

Threat Hunting File Integrity Monitoring Configuration Assessment MITRE ATT&CK Vulnerability Detection More... [kali \(001\)](#) Stats Configuration

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

### System inventory

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

Last 24 hours

### Events count evolution

Count

0 50 100 150 200

06:00 09:00 12:00 15:00 18:00 21:00 00:00

timestamp per 30 minutes

### MITRE ATT&CK

#### Top Tactics

Tactic	Count
Defense Evasion	2
Privilege Escalation	2
Credential Access	1
Initial Access	1
Persistence	1

### Compliance

PCI DSS

Level	Count
2.2 (192)	192
10.6.1 (9)	9
10.2.5 (4)	4
10.2.4 (2)	2
10.2.7 (1)	1

## Enable FIM on the Wazuh Agent (Kali)

## Generate FIM Alerts

```
(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:

Jan 18 23:27

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

Endpoints kali

Threat Hunting File Integrity Monitoring Configuration Assessment MITRE ATT&CK Vulnerability Detection More... [kali \(001\)](#) Stats Configuration

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

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

Events count evolution

MITRE ATT&CK

Top Tactics

Defense Evasion	45
Privilege Escalation	40
Initial Access	20
Persistence	20

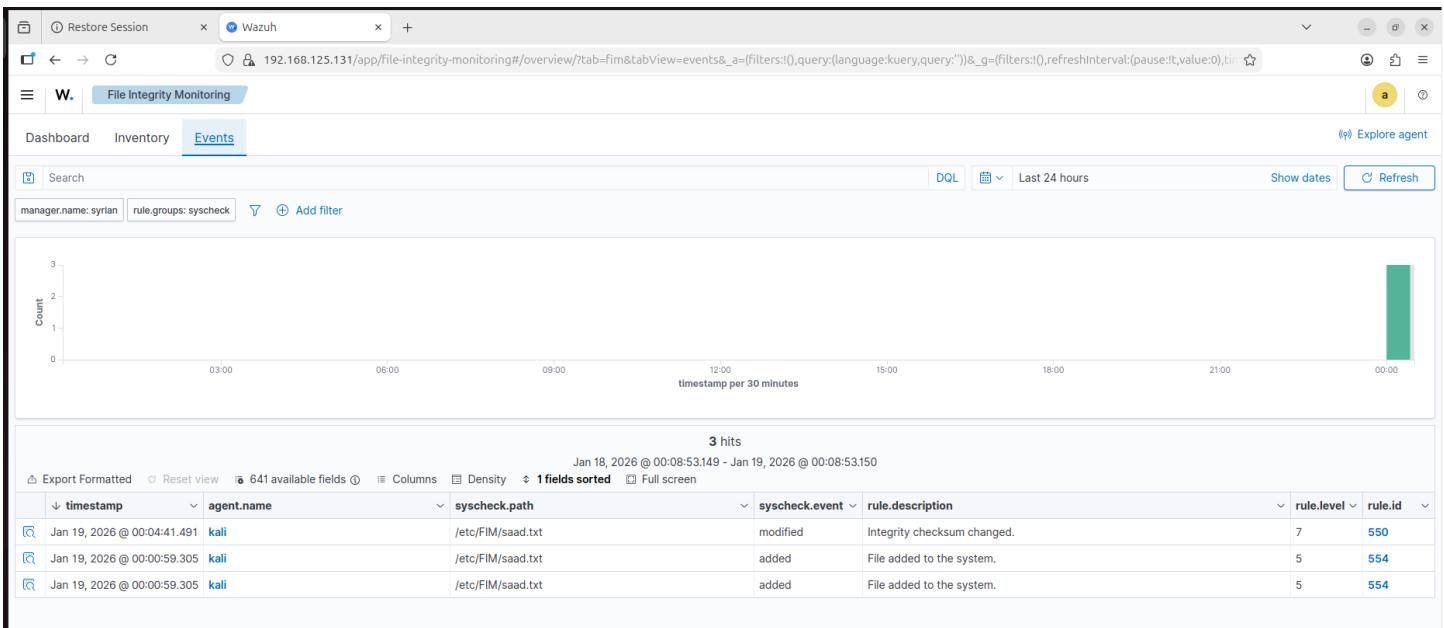
Compliance

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

```

syrian@kali: ~/Desktop
└─$ cd FIM
└─$ ls
saad.txt
└─$ nano saad.txt
└─$ sudo saad.txt
sudo: saad.txt: command not found
└─$ sudo nano saad.txt
└─$ ls
saad.txt
└─$ cat saad.txt
this is my file!
└─$ 

```



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.

