

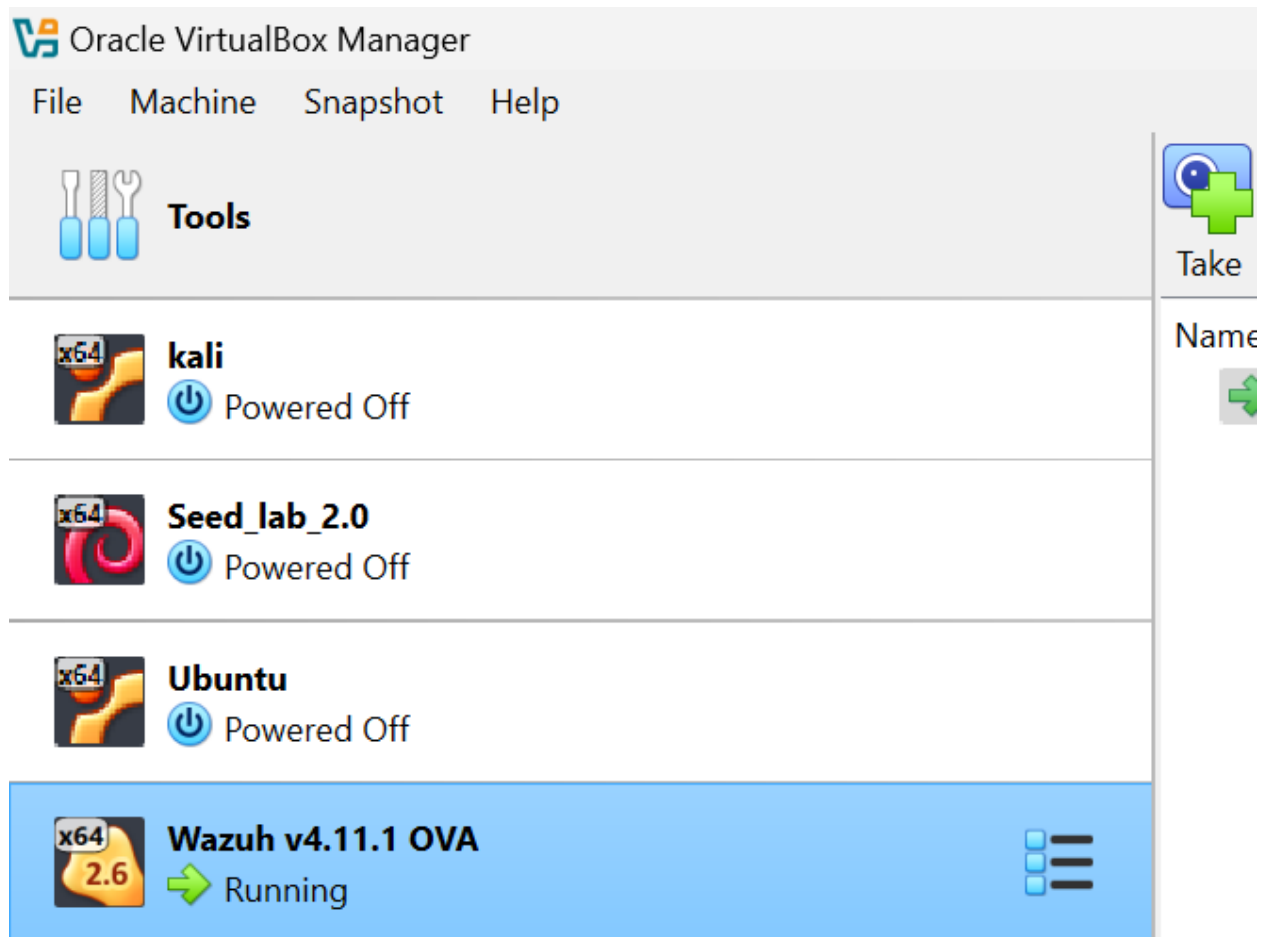
Task 1 Submission

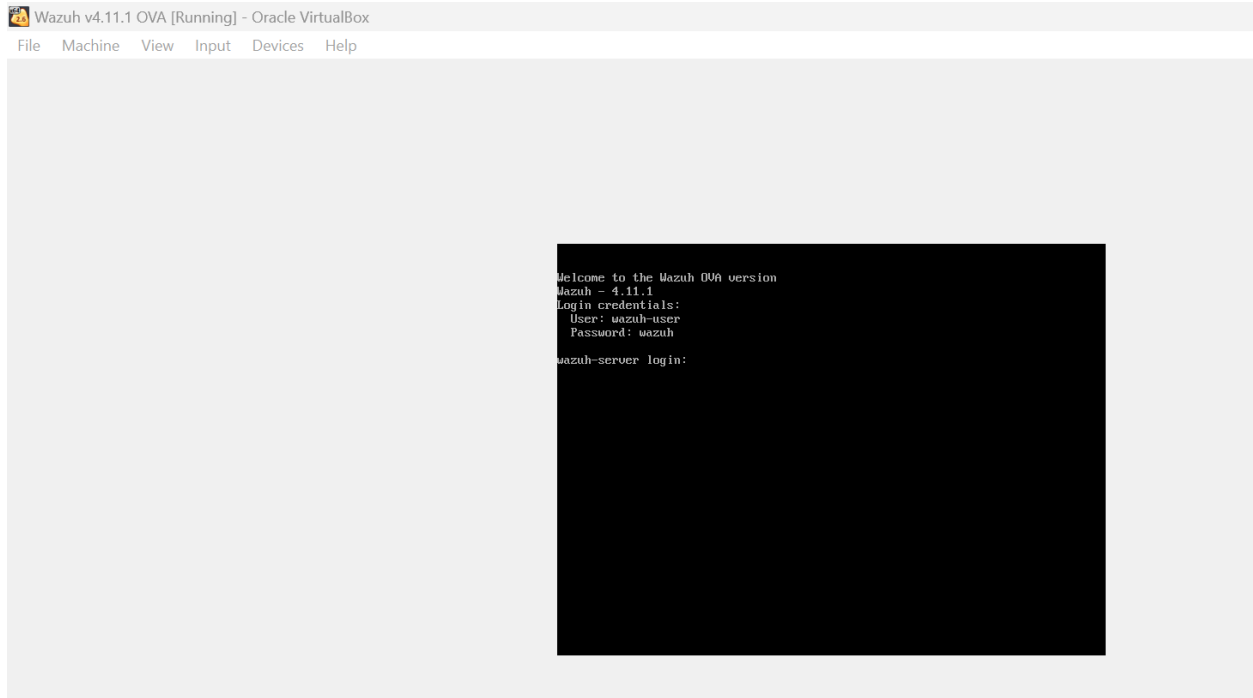
Syed Hasa Raza Rizvi

Questions:

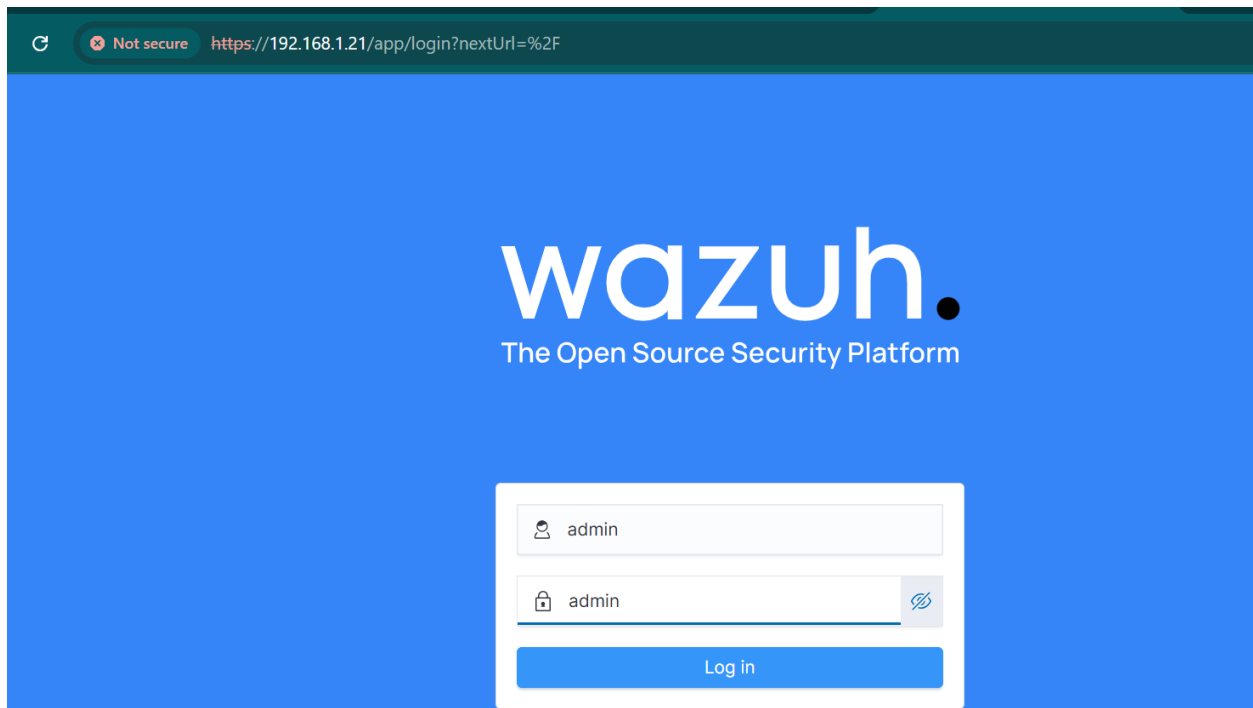
1. Import the Wazuh OVA file into VirtualBox or VMware and start the Wazuh Manager.
2. Access the Wazuh web interface and take a screenshot of the dashboard login page.
3. Install the Wazuh agent on a Windows machine and connect it to the Wazuh Manager.
4. Install the Wazuh agent on an Ubuntu machine and connect it to the Wazuh Manager.
5. Enable File Integrity Monitoring (FIM) on the Ubuntu agent for the /etc directory.
6. Enable FIM on the Windows agent for the C:\Windows\System32 directory.
7. Create or modify a file in both monitored directories and verify FIM alerts in the Wazuh dashboard.

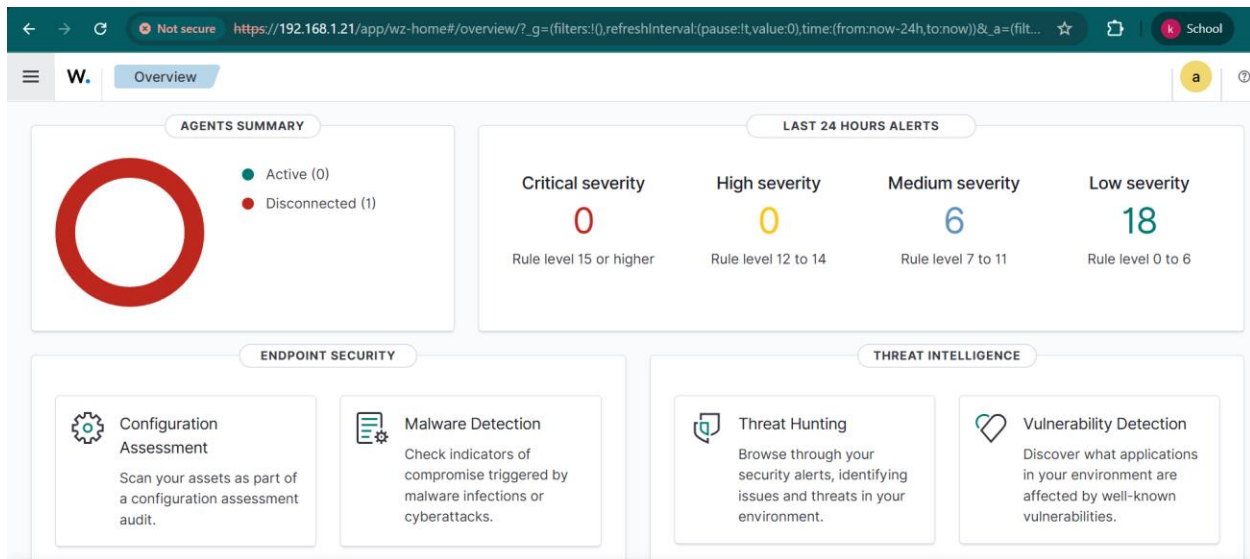
Question1:





Question 2:





Question 3:

Deploying a new agent on windows

The screenshot shows the 'Deploy new agent' page in the Wazuh interface. The 'Endpoints' tab is active, and the 'Deploy new agent' sub-tab is selected. The page is divided into three main sections for different operating systems:

- LINUX:** Offers four options: RPM amd64, RPM aarch64, DEB amd64, and DEB aarch64.
- WINDOWS:** Offers one option: MSI 32/64 bits (selected).
- Apple:** Offers two options: Intel and Apple silicon.

Below these sections, there is a link: "For additional systems and architectures, please check our [documentation](#)".

Server address: This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

Assign a server address ⓘ

192.168.1.21

☐ Remember server address



Optional settings:

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the f

Assign an agent name: [?](#)

hasan-raza

[i](#) The agent name must be unique. It can't be changed once the agent has been enrolled. [?](#)

Run this command in windows power shell(as administrator):

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.11.1-1.msi -OutFile $env:tmp\wazuh-agent; msixec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.1.21' WAZUH_AGENT_NAME='hasan-raza'
```

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

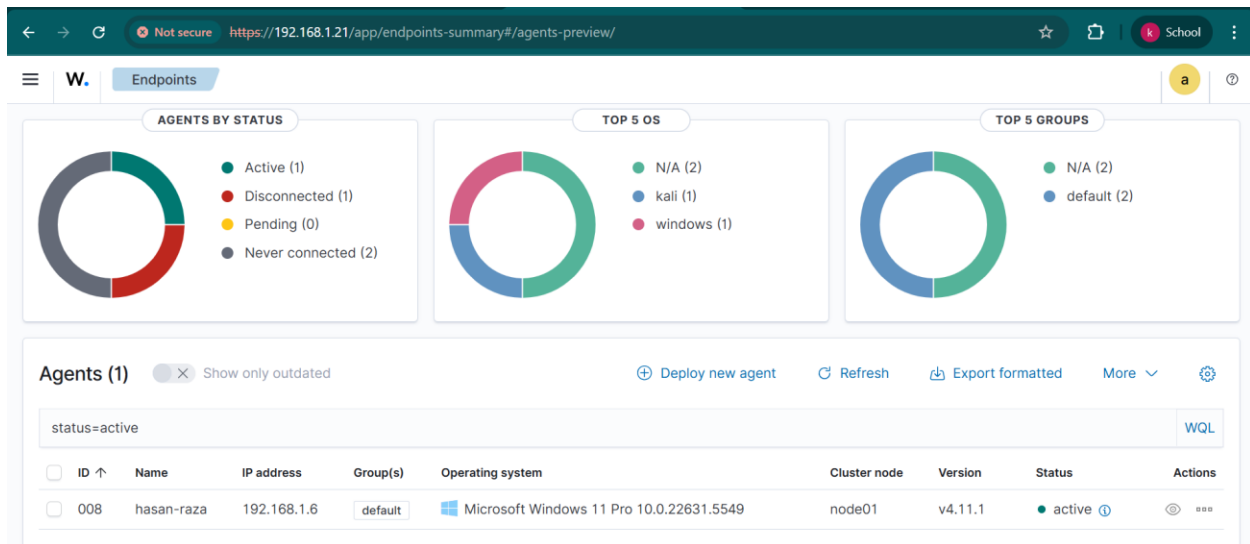
PS C:\WINDOWS\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.11.1-1.msi -OutFile $env:tmp\wazuh-agent; msixec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.1.21' WAZUH_AGENT_NAME='hasan-raza'
PS C:\WINDOWS\system32>
```

Then run this command to start the service:

```
PS C:\WINDOWS\system32> NET START WazuhSvc
The Wazuh service is starting.
The Wazuh service was started successfully.

PS C:\WINDOWS\system32> _
```

Successfully added the agent:



Question 6 for Windows:

Run this command to open the file:

```
PS C:\WINDOWS\system32> notepad "C:\Program Files (x86)\ossec-agent\ossec.conf"
>>
```

Then added this line in the file:

```
<directories realtime="yes" check_all="yes">C:\Windows\System32</directories>
```

Question 7:

For FIM:

```
PS C:\WINDOWS\system32> "Hello" | Out-File -FilePath "C:\Windows\System32\wazuh-test.txt"
>> Start-Sleep -Seconds 10
>> "Updated" | Add-Content -Path "C:\Windows\System32\wazuh-test.txt"
>>
PS C:\WINDOWS\system32>
```

Jul 2, 2025 @ 02:52:03.135 - Jul 3, 2025 @ 02:52:03.136						
Export Formatted 719 available fields Columns Density Sort fields Full screen						
	agent.name	syscheck.path	syscheck.event	rule.des...	rule.level	rule.id
@ 02:45:56.628	hasan-raza	c:\windows\system32\wazuh-test.txt	modified	Integrity ch...	7	550
@ 02:45:56.642	hasan-raza	c:\windows\system32\wazuh-test.txt	modified	Integrity ch...	7	550
@ 02:22:20.974	hasan-raza	c:\windows\system32\wazuh-test.txt	added	File added ...	5	554

Question 4: For “KALI”

Installing the Wazuh agent on Kali machine and connecting it to the Wazuh Manager:

Adding the Wazuh APT repository:

```
(hasanraza@kali)-[~]
$ curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo gpg --dearmor -o /usr/share/keyrings/wazuh.gpg
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | sudo tee /etc/apt/sources.list.d/wazuh.list
deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main
```

```
(hasanraza@kali)-[~]
$ sudo apt update

Get:1 https://packages.wazuh.com/4.x/apt stable InRelease [17.3 kB]
Get:2 https://packages.wazuh.com/4.x/apt stable/main i386 Packages [13.2 kB]
Get:3 https://download.docker.com/linux/debian bullseye InRelease [43.3 kB]
Get:4 https://packages.wazuh.com/4.x/apt stable/main amd64 Packages [46.2 kB]
Get:5 https://packages.wazuh.com/4.x/apt stable/main i386 Contents (deb) [5804 B]
Get:6 https://packages.wazuh.com/4.x/apt stable/main amd64 Contents (deb) [1952 kB]
Get:7 https://download.docker.com/linux/debian bullseye/stable amd64 Packages [57.9 kB]
Get:8 https://download.docker.com/linux/debian bullseye/stable amd64 Contents (deb) [1392 B]
Get:9 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Err:9 http://kali.download/kali kali-rolling InRelease
       Sub-process /usr/bin/sq returned an error code (1). error message is: Missing key 827C8569F25
```

Installing the Wazuh agent:

```
(hasanraza@kali)~$ sudo apt install wazuh-agent -y

The following packages were automatically installed and are no longer required:
docker-buildx-plugin libavfilter9 libgeos3.12.2 libgsfapi0 libiparser1 libpostproc57 librdmacm164 python3-hatch-vcs python3-trove-classifiers samba-vfs-modules
docker-compose-plugin libboost-iostreams1.83.0 libgfsapi0 libgtk2.0-0t64 libjsoncpp25 libpython3.11-dev libslirp0 python3-hatchling python3-trove-classifiers slirp4netns
fontconfig libboost-thread1.83.0 libgfsapi0 libgtk2.0-bin liblvm2 libpython3.11-minimal libusbmuxd python3-hatchling python3.11 python3.11-dev slirp4netns
hydra-gtk libcephfs2 libgtk2.0-common liblvm2 libpython3.11-stdlib libusbmuxd python3-hatchling python3.11 python3.11-dev slirp4netns
libverbs-providers libgail-common libglapi-mesa libibverbs1 libplacebo338 libpython3.11t64 openjdk-17-jre-headless python3-hatchling python3.11 python3.11-dev slirp4netns
libassuan0 libgail18t64 libglapi-mesa libglusterfs0 libimobiledevice6 libplist3 librados2 pigz python3-hatchling python3.11 python3.11-dev slirp4netns
Use 'sudo apt autoremove' to remove them.

Upgrading:
wazuh-agent

Summary:
Upgrading: 1, Installing: 0, Removing: 0, Not Upgrading: 2039
Download size: 12.0 MB
Space needed: 4353 kB / 2172 MB available

Get:1 https://packages.wazuh.com/4.x/apt/stable/main amd64 wazuh-agent amd64 4.12.0-1 [12.0 MB]
Fetched 12.0 MB in 6s (2111 kB/s)
Preconfiguring packages ...
(Reading database ... 456635 files and directories currently installed.)
Preparing to unpack .../wazuh-agent_4.12.0-1_amd64.deb ...
Unpacking wazuh-agent (4.12.0-1) over (4.11.1-1) ...
Setting up wazuh-agent (4.12.0-1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
```

Accessed the file through this command:

```
(hasanraza@kali)~$ sudo nano /var/ossec/etc/ossec.conf
```

Changed the ip address in the ossec file:

```
File Actions Edit View Help
GNU nano 8.1
Wazuh - Agent - Default configuration for kali 2024.3 and check IP address
More info at: https://documentation.wazuh.com
Mailing list: https://groups.google.com/forum/#!forum/wazuh
→
<ossec_config>
  <client>
    <server>
      <address>192.168.56.105</address>
      <port>1514</port>
      <protocol>tcp</protocol>
    </server>
```

```
(hasanraza@kali)~$ sudo /var/ossec/bin/agent-auth -m 192.168.56.105 -A Hasanraza-kali

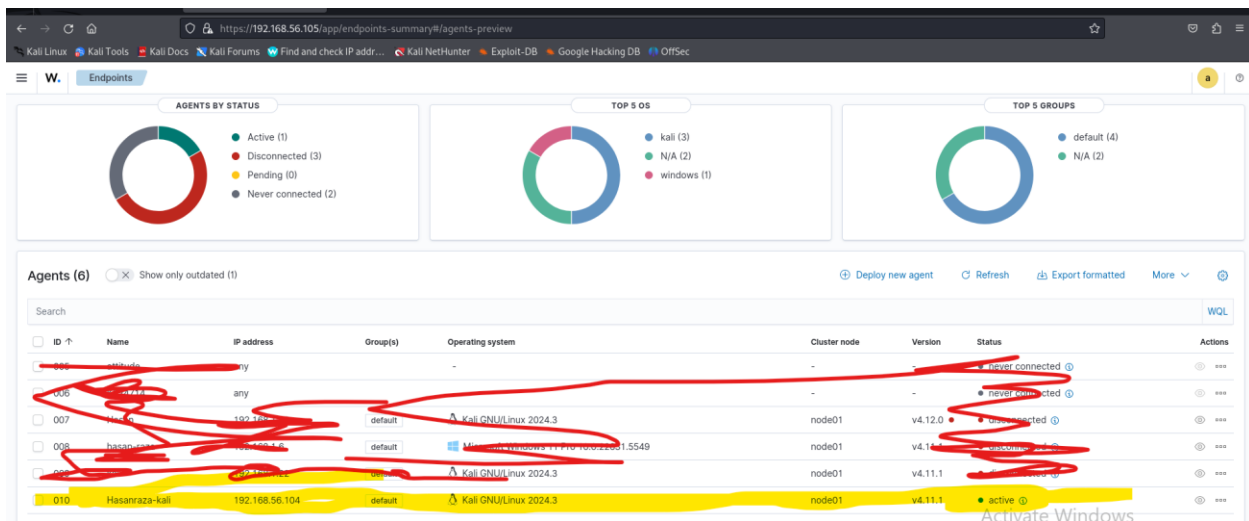
2025/07/03 16:12:47 agent-auth: INFO: Started (pid: 8625).
2025/07/03 16:12:47 agent-auth: INFO: Requesting a key from server: 192.168.56.105
2025/07/03 16:12:47 agent-auth: INFO: No authentication password provided
2025/07/03 16:12:47 agent-auth: INFO: Using agent name as: Hasanraza-kali
2025/07/03 16:12:47 agent-auth: INFO: Waiting for server reply
2025/07/03 16:12:47 agent-auth: INFO: Valid key received
```


Agent added:

```
*****
* Wazuh v4.11.1 Agent manager.          *
* The following options are available: *
*****
(A)dd an agent (A).
(E)xtract key for an agent (E).
(L)ist already added agents (L).
(R)emove an agent (R).
(Q)uit.
Choose your action: A,E,L,R or Q: L

Available agents:
ID: 005, Name: attitude, IP: any
ID: 006, Name: K224714, IP: any
ID: 007, Name: Hasan, IP: any
ID: 008, Name: hasan-raza, IP: any
ID: 009, Name: kali, IP: any
ID: 010, Name: Hasanraza-kali, IP: any
```

Successfully agent deployed from kali:



Question 6 for KALI:

Also made this change:

```
File Actions Edit View Help
GNU nano 8.1
<!-- Check the file, but never compute the diff -->
<nodiff>/etc/ssl/private.key</nodiff>

<skip_nfs>yes</skip_nfs>
<skip_dev>yes</skip_dev>
<skip_proc>yes</skip_proc>
<skip_sys>yes</skip_sys>

<!-- Nice value for Syscheck process -->
<process_priority>10</process_priority>

<!-- Maximum output throughput -->
<max_eps>50</max_eps>

<directories_check_all="yes" realtime="yes">/etc</directories>
```

Added this file and modified it:

```
(hasanraza@kali)-[~]
$ sudo touch /etc/test-fim-kali.txt

(hasanraza@kali)-[~]
$ echo "changed" | sudo tee -a /etc/test-fim-kali.txt
changed
```

Question 7: for KALI

FIM:

FIM: Recent events

Time	Path	Action	Rule description	Rule Lev...	Rule Id
Jul 3, 2025 @ 16:53:25.754	/etc/test-fim-kali.txt	modified	Integrity checksum changed.	7	550

https://192.168.56.105/app/file-integrity-monitoring#/overview?tab=fim&tabView=events&agentId=010&_a=(filters:[]&query:(language:query,query:))&_g=(filters:[]&refreshInterval:(pause:it,va...

Wazuh File Integrity Monitoring - Hasanraza-kali

DashboardInventoryEvents

SearchDQLLast 24 hoursShow datesRefresh

manager.name: wazuh-serverrule.group: syscheckagent.id: 010Add filter

Count

timestamp per 30 minutes

2 hits

Export Formatted719 available fieldsColumnsDensity1 fields sortedFull screen

timestamp	agent.name	syscheck.path	syscheck.event	rule.description	rule.level	rule.id
Jul 3, 2025 @ 16:53:25.754	Hasanraza-kali	/etc/test-fim-kali.txt	modified	Integrity checksum changed.	7	550
Jul 3, 2025 @ 16:53:09.385	Hasanraza-kali	/etc/test-fim-kali.txt	modified	Integrity checksum changed.	7	550