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.

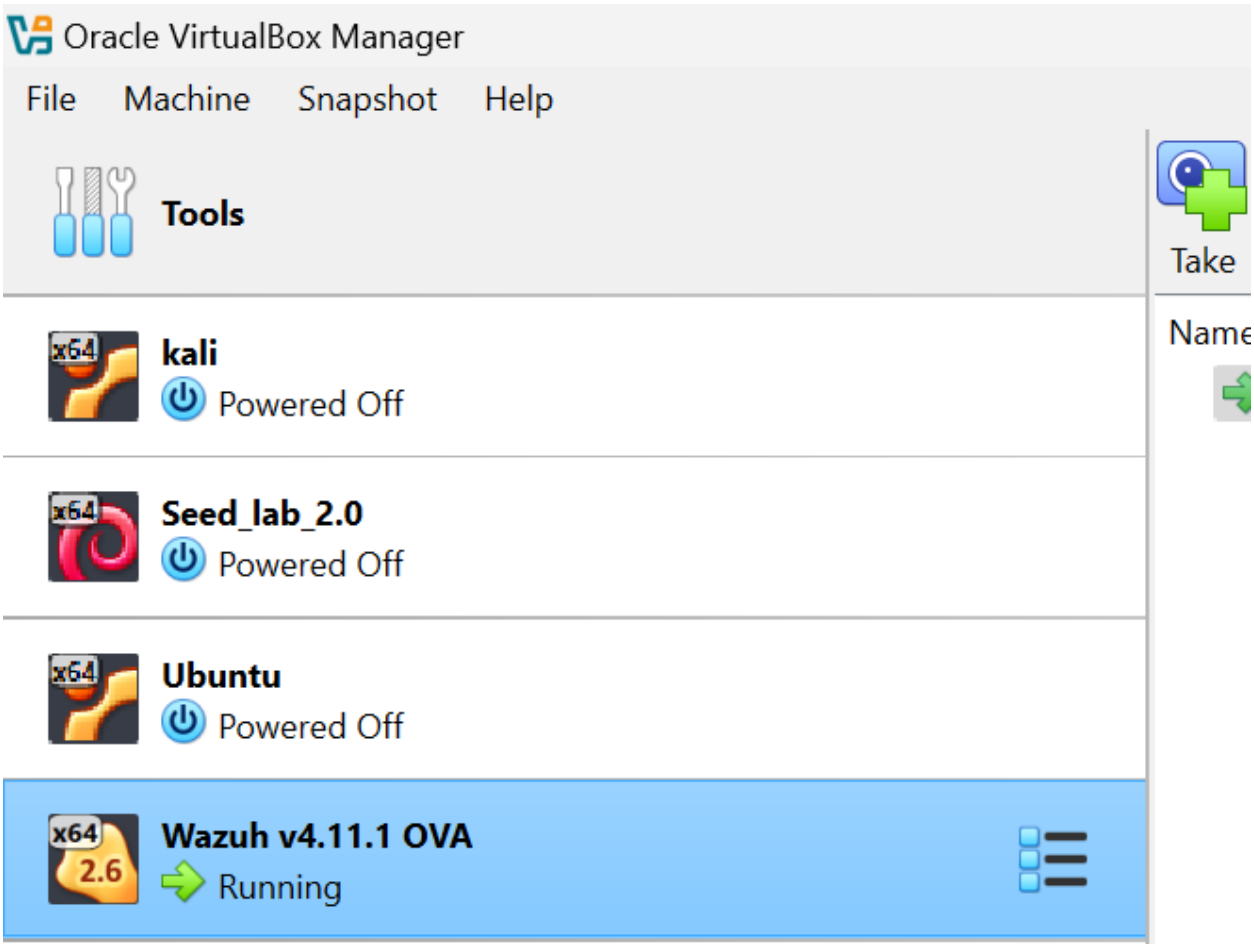
4. Install the Wazuh agent on an Ubuntu machine and connect it to the Wazuh Manager.

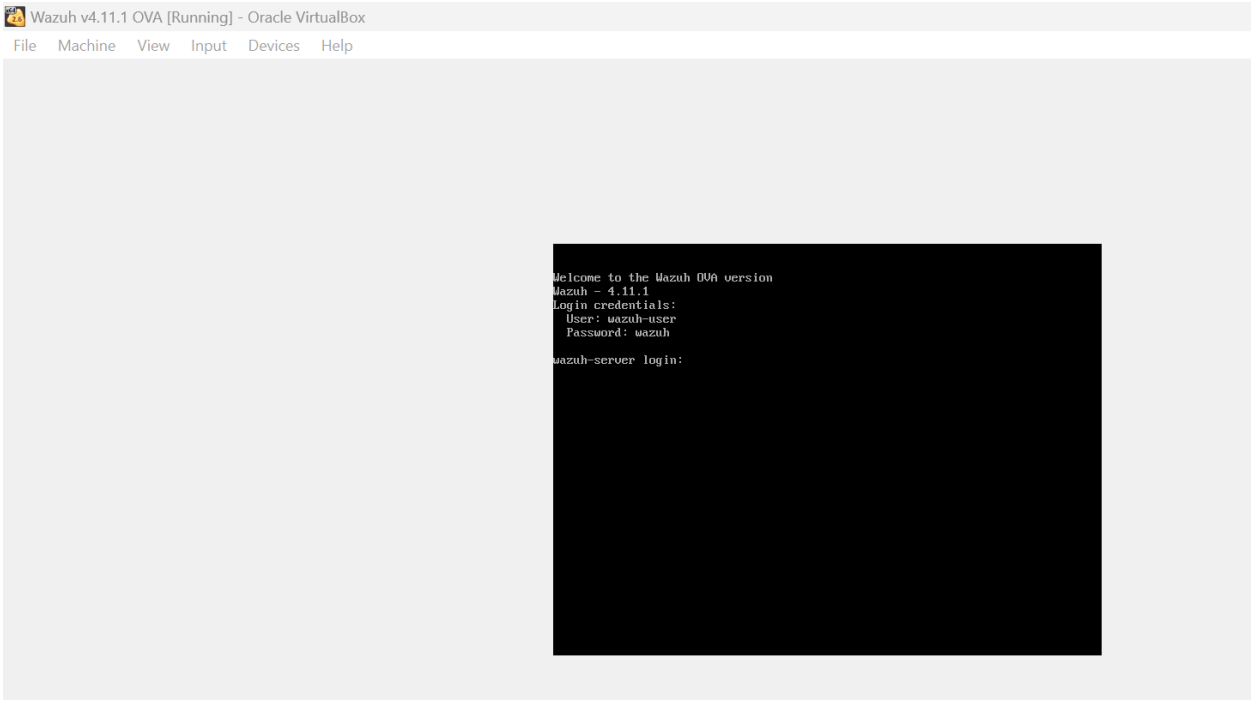
5. Enable File Integrity Monitoring (FIM) on the Ubuntu agent for the /etc directory.

6. Enable FIM on the Windows agent for the C:\Windows\System32 directory.

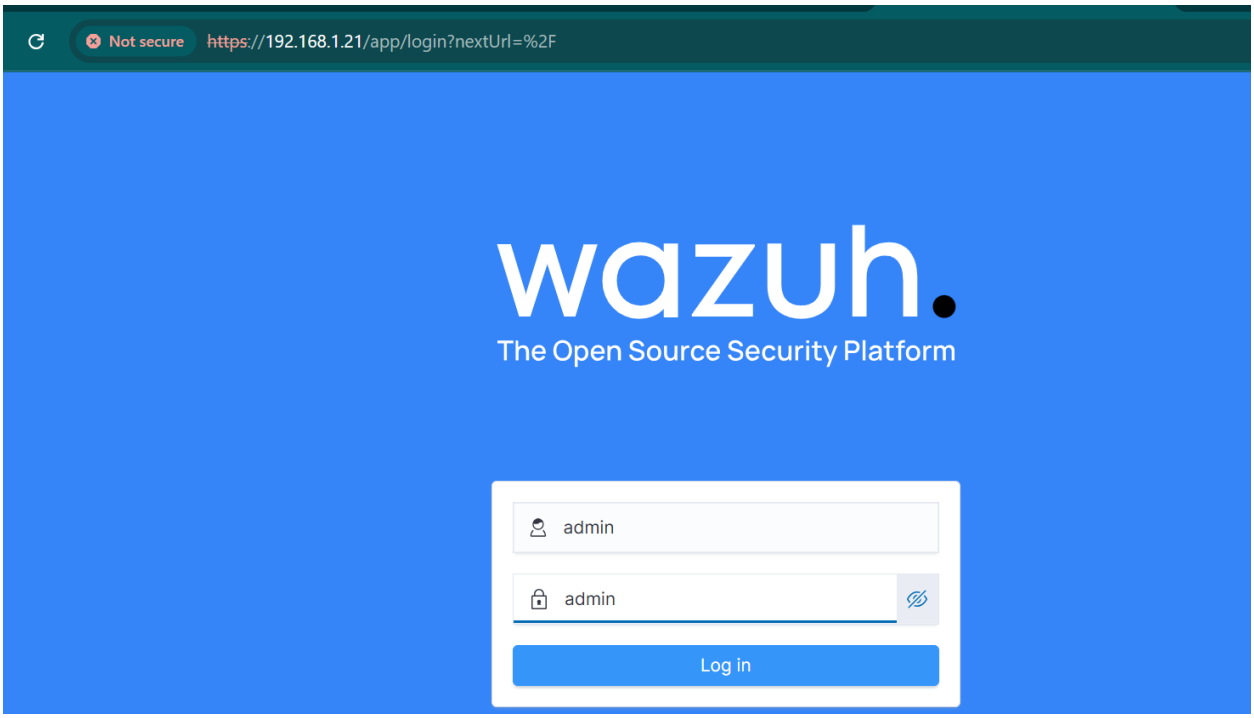
7. Create or modify a file in both monitored directories and verify FIM alerts in the Wazuh dashboard.

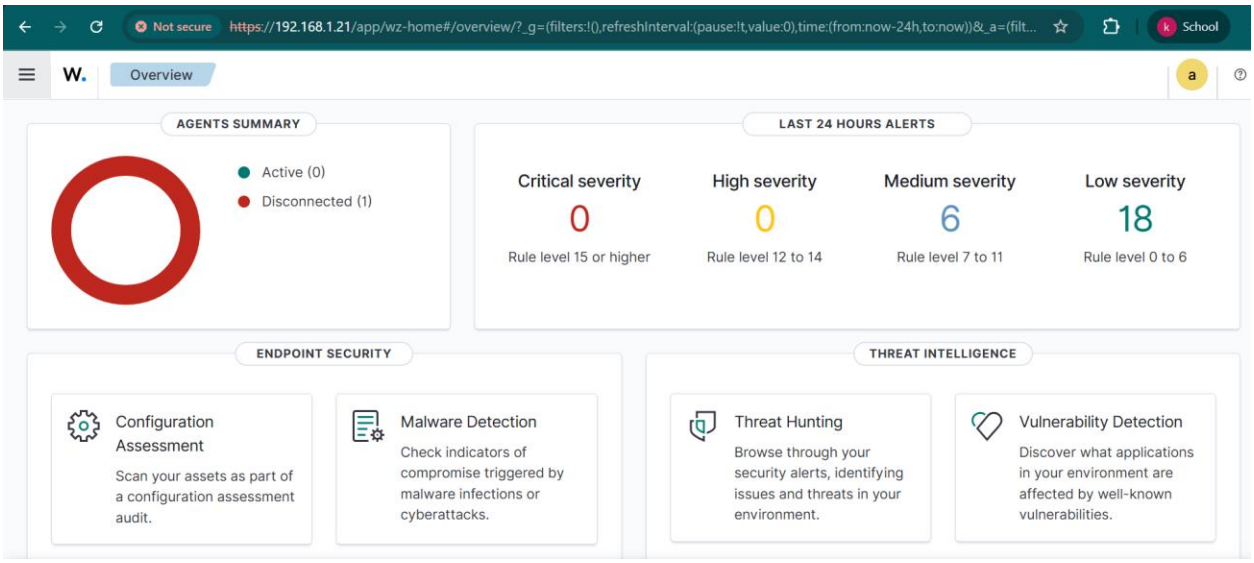
Question1:


Oracle VirtualBox Manager
File
Machine
Snapshot
Help
Tools
Take
Name
kali
Powered Off
Seed_lab_2.0
Powered Off
Ubuntu
Powered Off
Wazuh v4.11.1 OVA
Running


Wazuh v4.11.1 OVA [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Welcome to the Wazuh OVA version
Wazuh - 4.11.1
Login credentials:
User: wazuh-user
Password: wazuh
wazuh-server login:

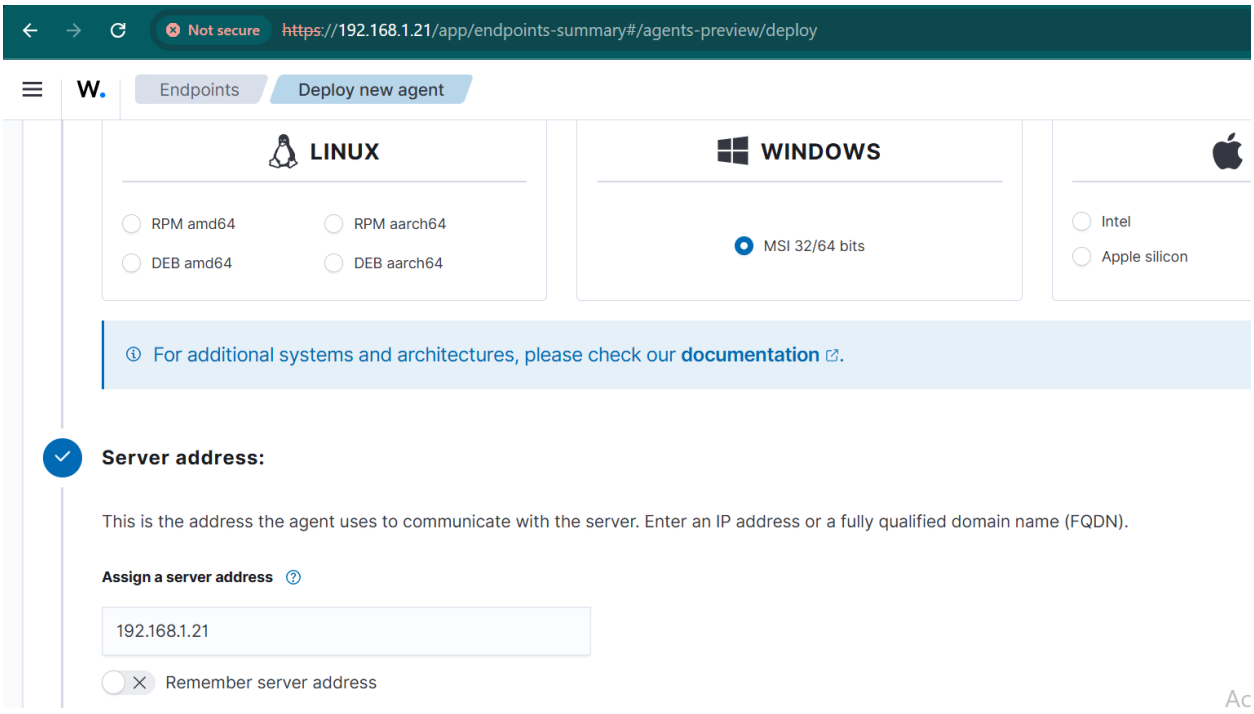
Question 2:


Not secure
https://192.168.1.21/app/login?nextUrl=%2F
wazuh.
The Open Source Security Platform
admin
admin
Log in



Question 3:

Deploying a new agent on windows



Optional settings:

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

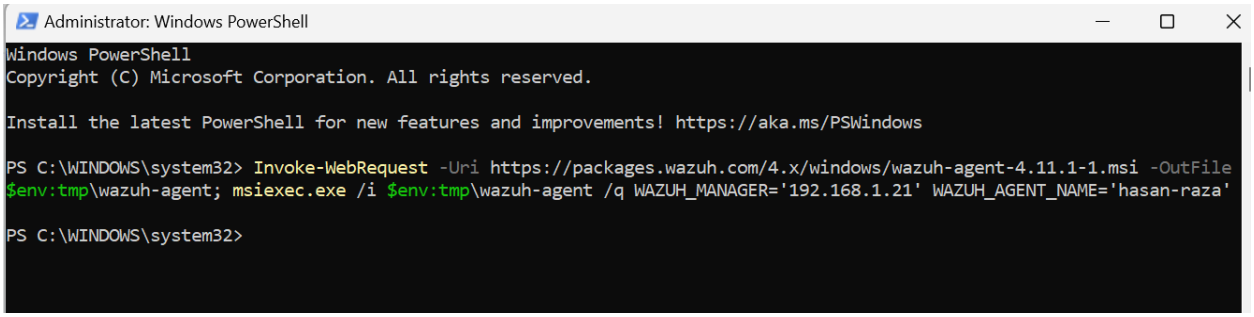
Assign an agent name:

hasan-raza

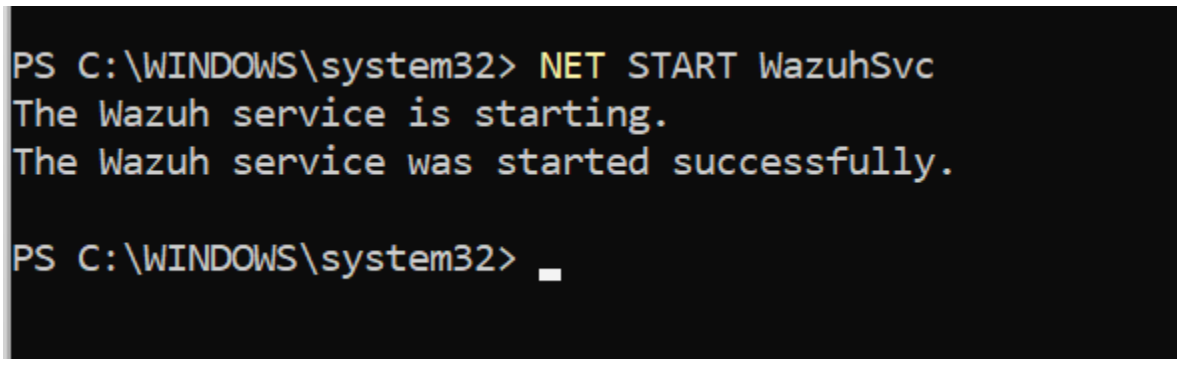
The agent name must be unique. It can't be changed once the agent has been enrolled.

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

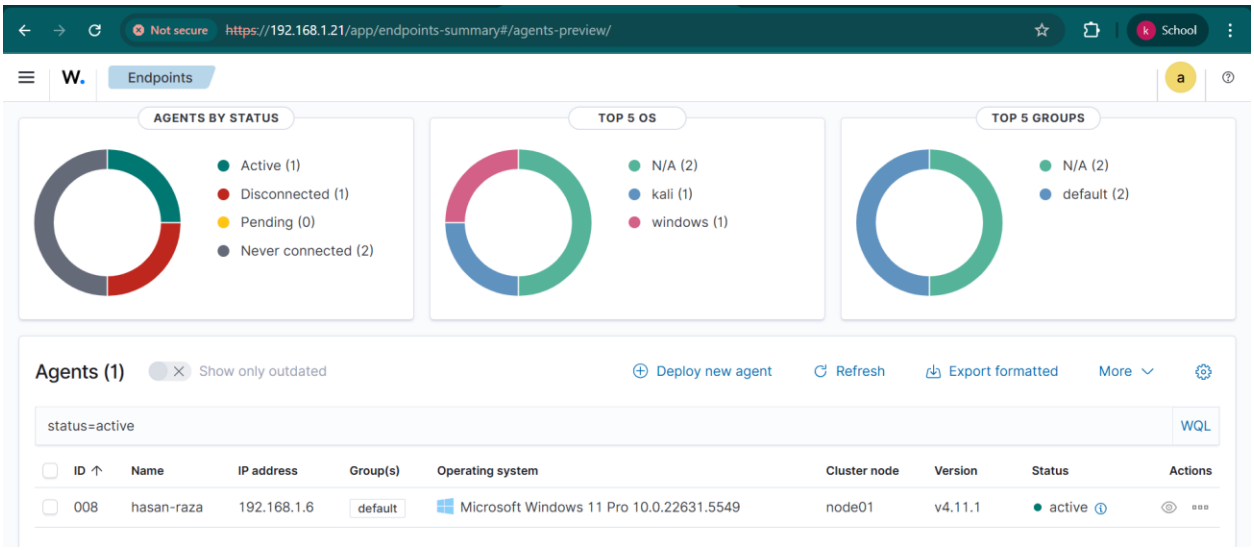
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.11.1-1.msi -OutFile $env:tmp\wazuh-agent; msiexec.exe /i $env:tmp\wazuh-agent /q WAZUH_MANAGER='192.168.1.21' WAZUH_AGENT_NAME='hasan-raza'



Then run this command to start the service:



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/sqv returned an error code (1), error message is: Missing key 827C8569F25
```

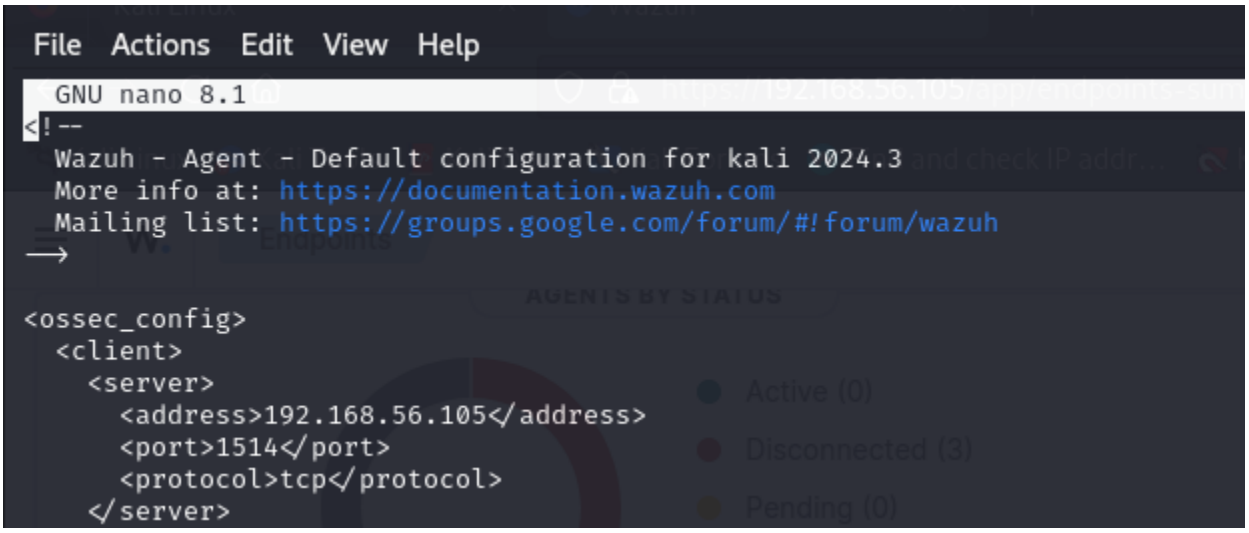
Installing the Wazuh agent:

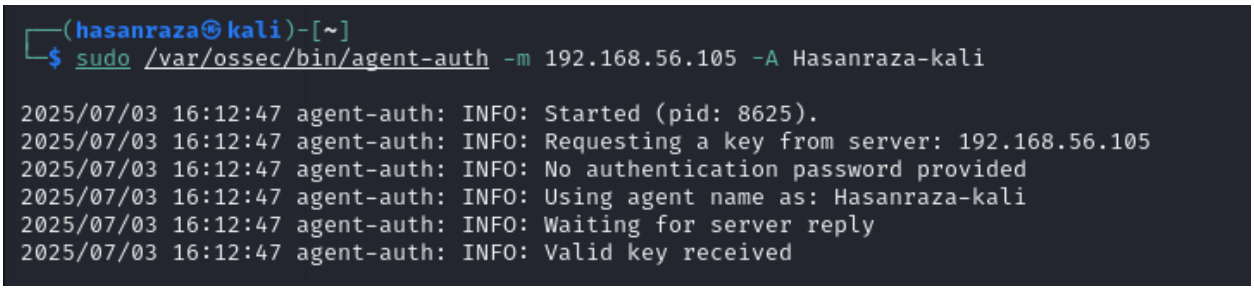
Accessed the file through this command:

┌──(hasanraza㉿kali)-[~]

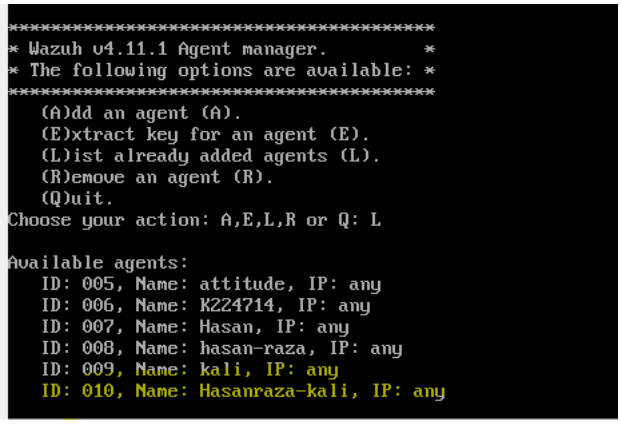
└─$ sudo nano /var/ossec/etc/ossec.conf

Changed the ip address in the ossec file:

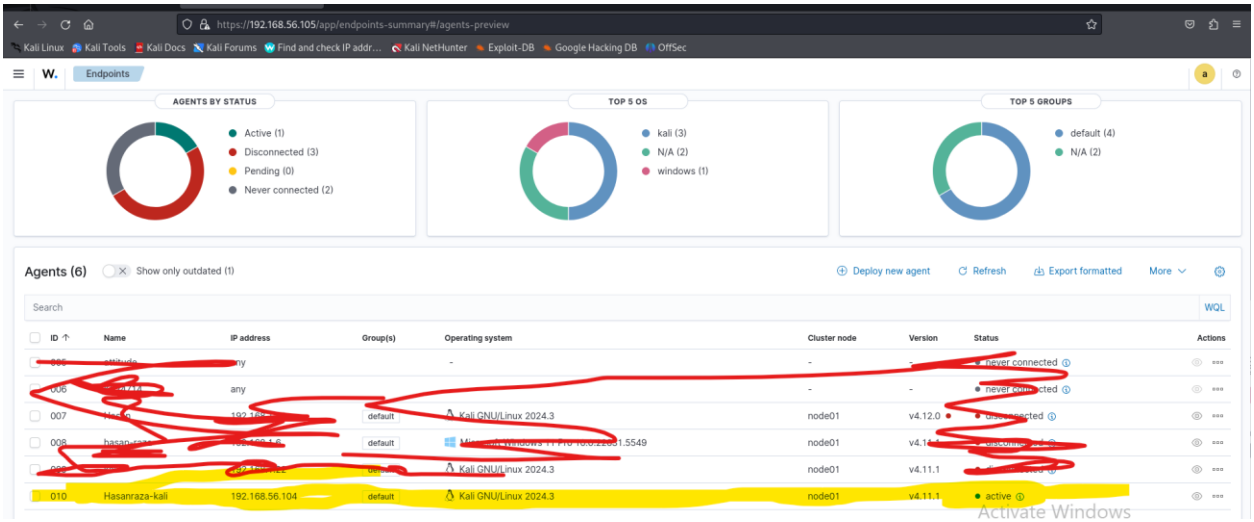




Agent added:

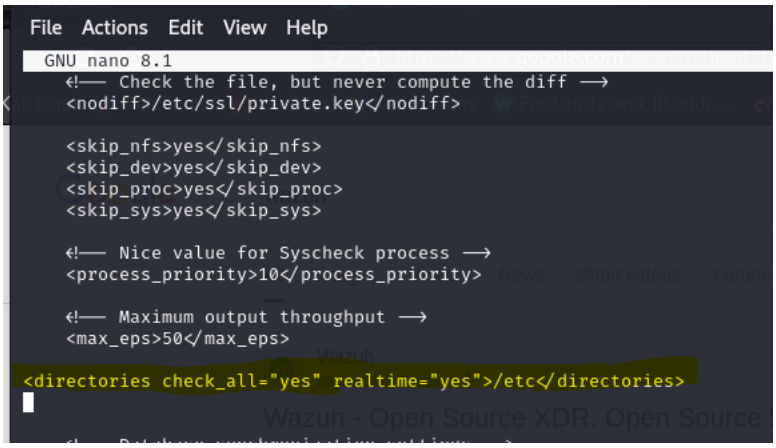


Successfully agent deployed from kali:



Question 6 for KALI:

Also made this change:



Added this file and modified it:

Question 7: for KALI

FIM: