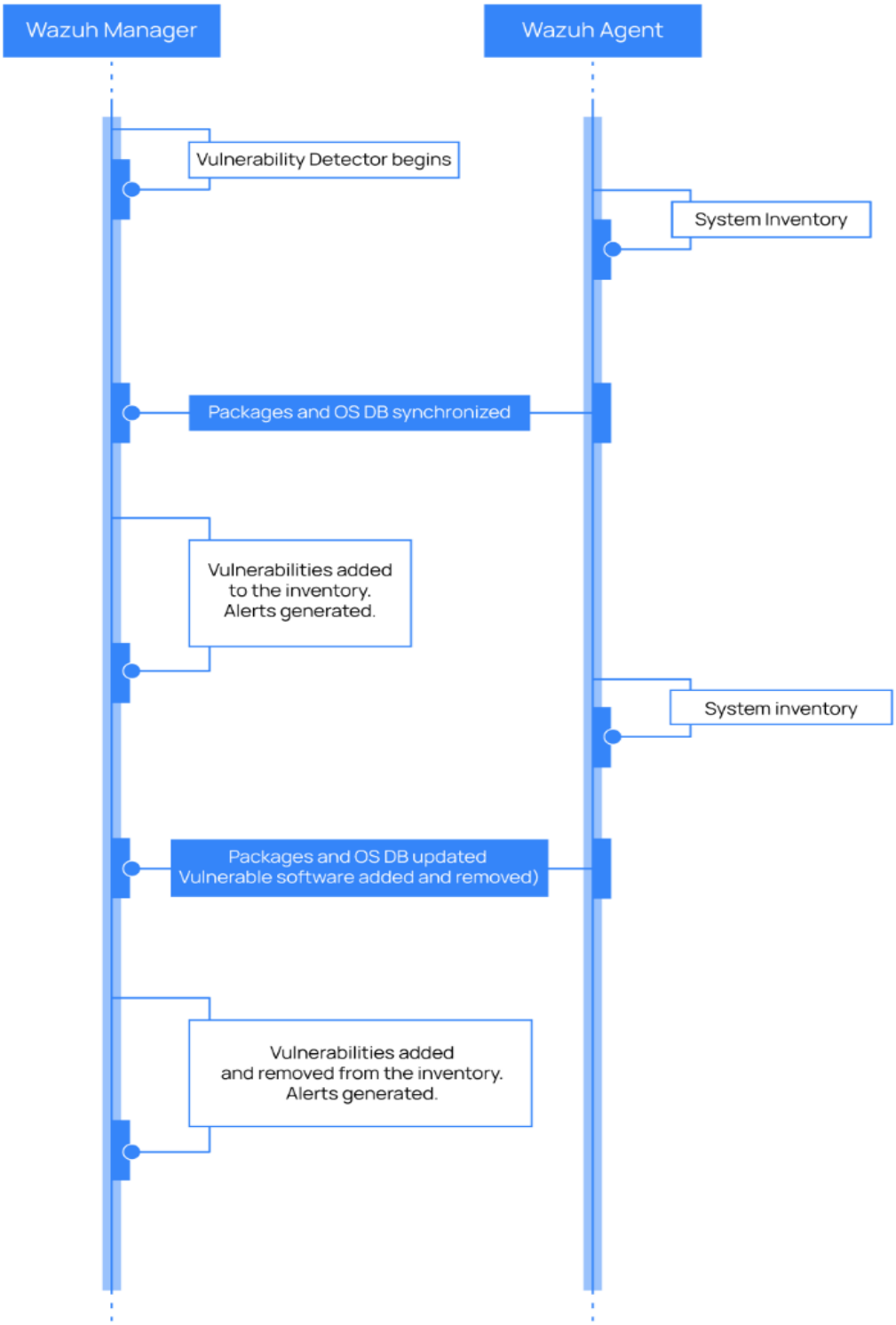
Wazuh Vulnerability Detection {Threat detection and response}

Vulnerabilities are security flaws in computer systems that threat actors can exploit to gain unauthorized access to these systems. After exploitation, malware and threat actors may be able to perform remote code execution, exfiltrate data, and carry out other malicious activities. Therefore, organizations must have strategies or security solutions that promptly detect vulnerabilities in their network before bad actors exploit them. Prompt detection and remediation of vulnerabilities in a network help to strengthen its overall security posture.

The Wazuh Vulnerability Detection module helps users discover vulnerabilities in the operating system and applications installed on the monitored endpoints.

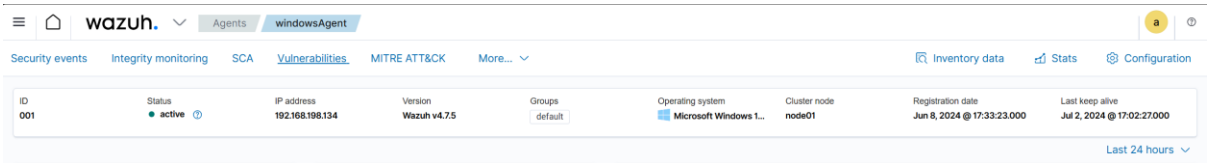
To detect vulnerabilities, Wazuh agents collect a list of installed applications from monitored endpoints and send it periodically to the Wazuh server. Local SQLite databases in the Wazuh server store this list. Within the Wazuh server, the Vulnerability Detection module correlates the software inventory data with vulnerability content documents to detect vulnerable software on the monitored endpoint. These documents are Common Vulnerabilities and Exposures (CVE) records that are available in Cyber Threat Intelligence (CTI) platform.



Setup:

Here, I have accessed my Wazuh console via SSH in kali

Access your Wazuh-dashboard.



Now you need to configure your ossec.conf file,

nano /var/ossec/etc/ossec.conf

Now, search for the System Inventory block. The below reference gives the default configuration.

```
<!-- System inventory -->
<wodle name="syscollector">
  <disabled>no</disabled>
  <interval>1h</interval>
  <scan_on_start>yes</scan_on_start>
  <hardware>yes</hardware>
  <os>yes</os>
  <network>yes</network>
  <packages>yes</packages>
  <ports all="no">yes</ports>
  <processes>yes</processes>
```

```
<vulnerability-detector>
  <enabled>no</enabled>
  <interval>5m</interval>
  <min_full_scan_interval>6h</min_full_scan_interval>
  <run_on_start>yes</run_on_start>

  <!-- Ubuntu OS vulnerabilities -->
  <provider name="canonical">
    <enabled>no</enabled>
    <os>trusty</os>
    <os>xenial</os>
    <os>bionic</os>
    <os>focal</os>
    <os>jammy</os>
    <update_interval>1h</update_interval>
  </provider>
```

Now, you need to enable certain functionalities in order to automate the process of finding vulnerabilities.

Such that

```
<!-- System inventory -->
<wodle name="syscollector">
  <disabled>yes</disabled>
  <interval>1h</interval>
  <scan_on_start>yes</scan_on_start>
  <hardware>yes</hardware>
  <os>yes</os>
  <network>yes</network>
  <packages>yes</packages>
  <ports all="no">yes</ports>
  <processes>yes</processes>

  <!-- Database synchronization settings -->
  <synchronization>
    <max_eps>10</max_eps>
  </synchronization>
</wodle>

<sca>
  <enabled>yes</enabled>
  <scan_on_start>yes</scan_on_start>
  <interval>12h</interval>
  <skip_nfs>yes</skip_nfs>
</sca>
```

```
<vulnerability-detector>
  <enabled>yes</enabled>
  <interval>5m</interval>
  <min_full_scan_interval>6h</min_full_scan_interval>
  <run_on_start>yes</run_on_start>

  <!-- Ubuntu OS vulnerabilities -->
  <provider name="canonical">
    <enabled>yes</enabled>
    <os>trusty</os>
    <os>xenial</os>
    <os>bionic</os>
    <os>focal</os>
    <os>jammy</os>
    <update_interval>1h</update_interval>
  </provider>
```

```
  <!-- Ubuntu OS vulnerabilities -->
  <provider name="canonical">
    <enabled>yes</enabled>
    <os>trusty</os>
    <os>xenial</os>
    <os>bionic</os>
    <os>focal</os>
    <os>jammy</os>
    <update_interval>1h</update_interval>
  </provider>

  <!-- Debian OS vulnerabilities -->
  <provider name="debian">
    <enabled>yes</enabled>
    <os>buster</os>
    <os>bullseye</os>
    <os>bookworm</os>
    <update_interval>1h</update_interval>
  </provider>
```

```
  <!-- Windows OS vulnerabilities -->
  <provider name="msu">
    <enabled>yes</enabled>
    <update_interval>1h</update_interval>
  </provider>
```

After this, there one more important step, this configuration enables the vulnerability database will start downloading after restart wazuh-manager

```
<!-- Aggregate vulnerabilities -->
<provider name="nvd">
  <enabled>yes</enabled>
  <update_interval>1h</update_interval>
</provider>
```

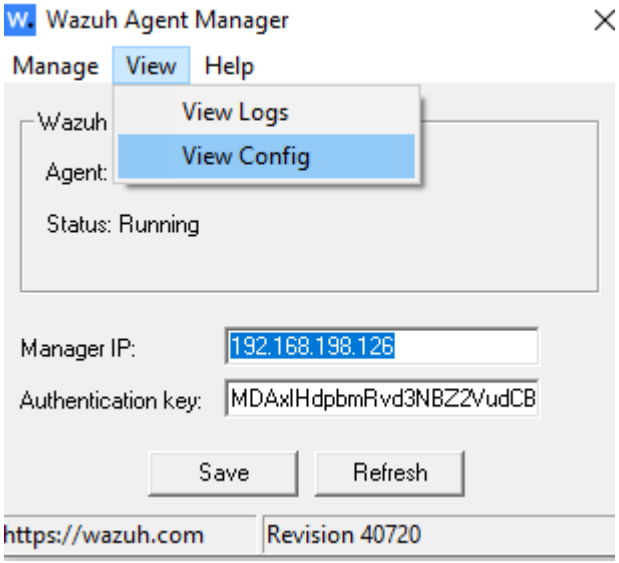
After this, try to restart your wazuh-manger in order to save the updates

Command:

sudo systemctl restart wazuh-manager

After successful restart try to update the configurations in the endpoint (i.e., windows in my case)

Access Manage Agent → view → view config

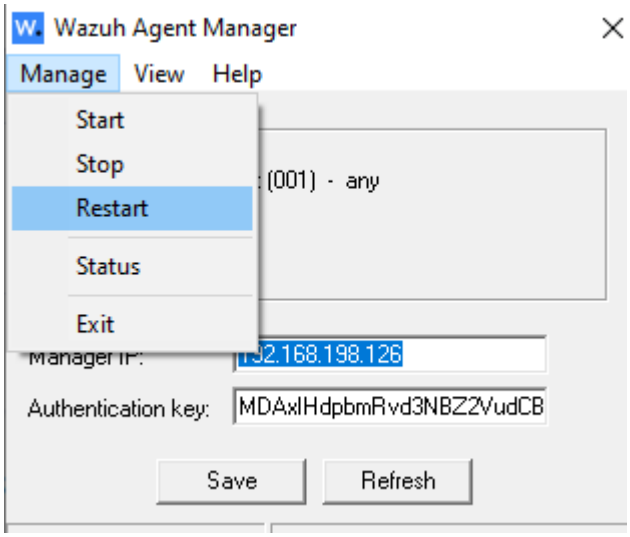


In that, under System inventory block, I have added the line

<hotfixes>yes</hotfixes>

```
<!-- System inventory -->
<wodle name="syscollector">
  <disabled>no</disabled>
  <interval>1h</interval>
  <scan_on_start>yes</scan_on_start>
  <hardware>yes</hardware>
  <os>yes</os>
  <network>yes</network>
  <packages>yes</packages>
  <hotfixes>yes</hotfixes>
  <ports all="no">yes</ports>
  <processes>yes</processes>
```

After that, try to restart the wazuh-agent manager



Thus, your setup is ready for testing