Wazuh – Vulnerability Detection

THREAT DETECTION AND RESPONSE

Lab Created By: MUHAMMAD MOIZ UD DIN RAFAY

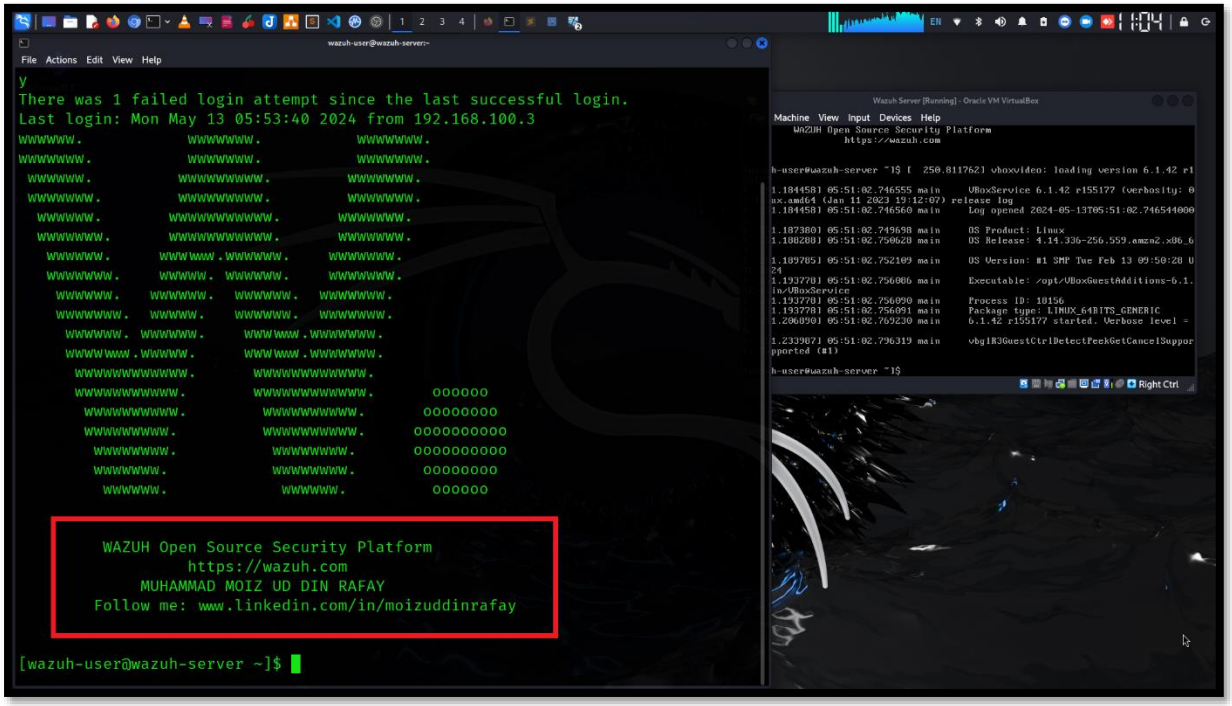
Follow Me: linkedin.com/in/moizuddinrafay

Wazuh is an open-source security platform that provides threat detection, integrity monitoring, and security analytics. It's designed to help organizations detect and respond to security incidents effectively. One of its key functionalities is vulnerability detection, which plays a crucial role in maintaining the security posture of systems and networks.

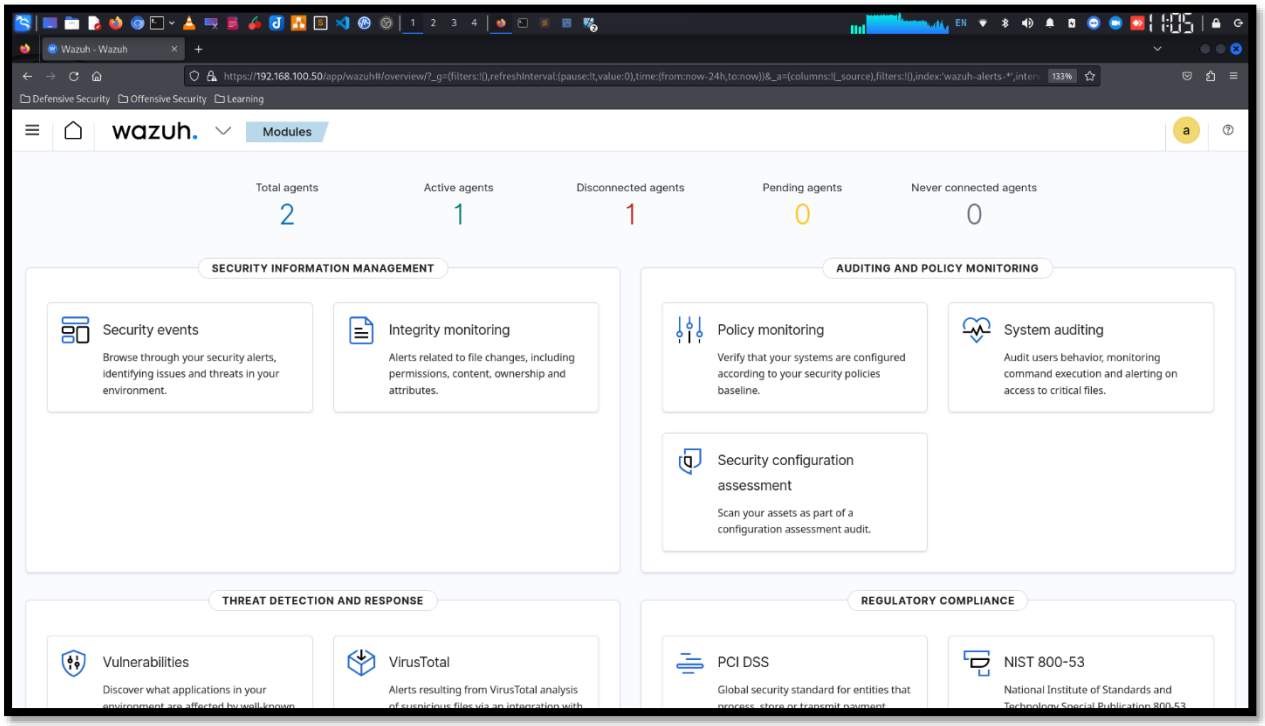
Wazuh employs several techniques for vulnerability detection:

1. **Vulnerability Scanning**: Wazuh integrates with popular vulnerability scanning tools such as OpenVAS and Nessus. These tools scan the network and systems for known vulnerabilities by comparing their configurations and installed software versions against a database of known vulnerabilities.
2. **Asset Inventory**: Wazuh maintains an inventory of assets within the organization's network, including hardware devices, software applications, and their respective versions. By continuously monitoring this inventory, Wazuh can identify discrepancies or outdated software versions that may be vulnerable to known exploits.
3. **Behavioural Analysis**: In addition to scanning for known vulnerabilities, Wazuh monitors system and network behaviour for anomalies that could indicate potential security issues. For example, sudden spikes in network traffic or unexpected changes in system configurations may suggest the presence of an exploit or vulnerability.
4. **Real-time Alerts**: Wazuh generates real-time alerts when vulnerabilities are detected, providing administrators with immediate notification of potential security threats. These alerts include detailed information about the vulnerability, affected systems, and recommended remediation steps.
5. **Customization and Extensibility**: Wazuh is highly customizable and extensible, allowing organizations to tailor vulnerability detection capabilities to their specific needs. Administrators can define custom rules and policies for detecting vulnerabilities based on their unique environment and security requirements.

Here is Wazuh Server running on my lab environment. I access Wazuh console via SSH connection.

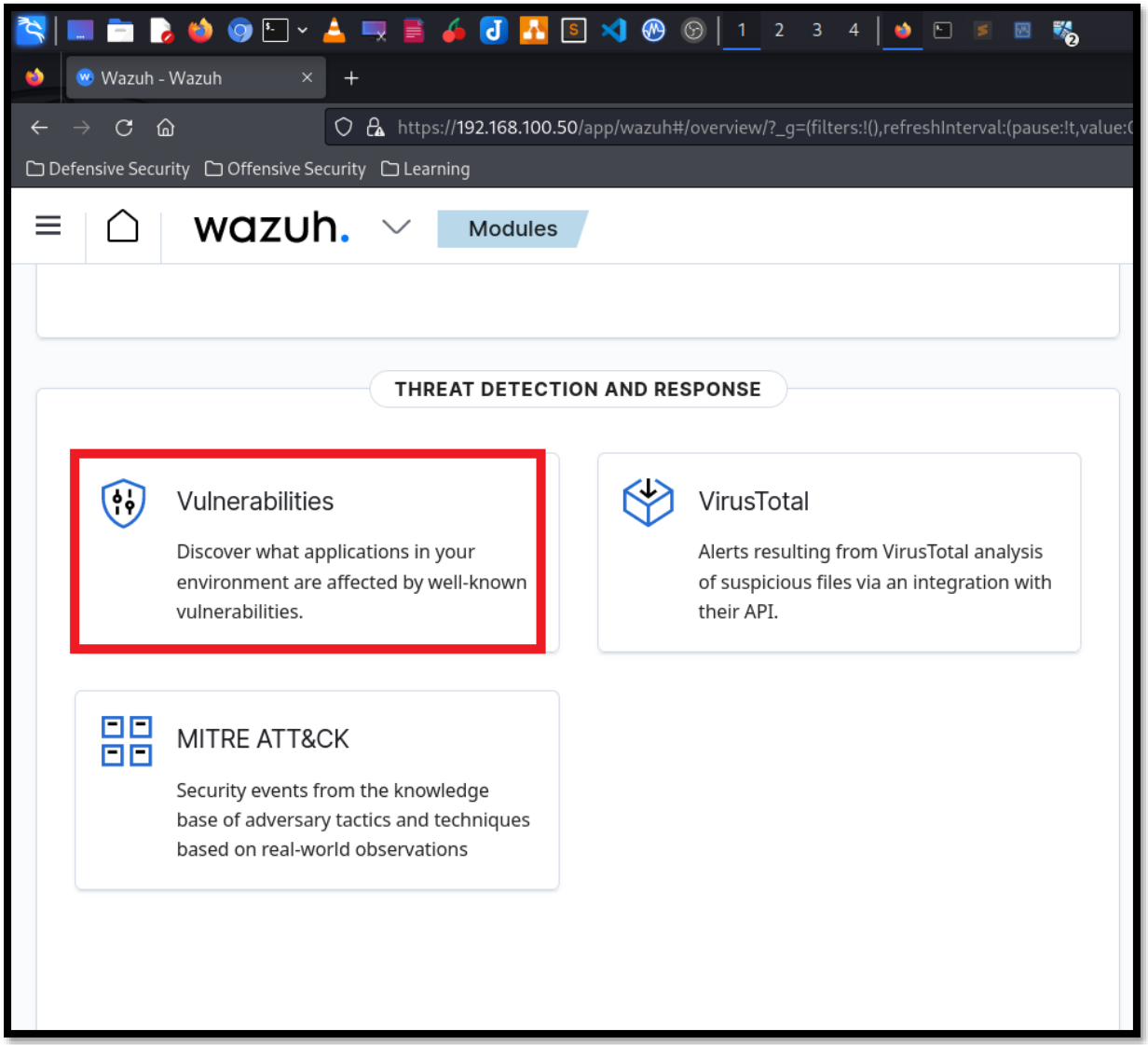


Here is Wazuh Server dashboard.

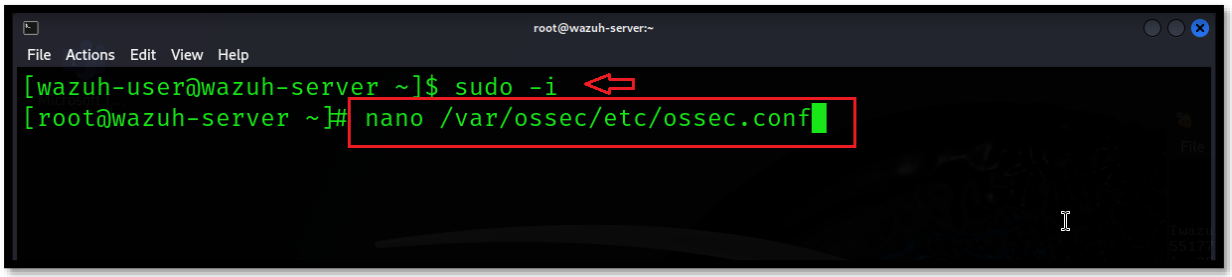


Selecting the Active agent (Windows 11)

Scroll down and go to “THREAT DETECTION AND RESPONSE” > “Vulnerabilities” options is available.



Now we have to configure vulnerability scanner.
Edit: “nano /var/ossec/etc/ossec.conf” file.



Here is in “ossec.conf” look at “System inventor” this configuration already there, we will add these configuration in to Windows-agent “ossec.conf” later.

```
root@wazuh-server:~
File  Actions  Edit  View  Help
  GNU nano 2.9.8              /var/ossec/etc/ossec.conf


<!-- virustotal integration -->

<integration>
  <name>virustotal</name>
  <api_key>08dcbc18314a0afd2ce8b2f9e12a282545de7f0b24f1570e9a0faf22e212d432 <$
  <group>syscheck</group>
  <alert_format>json</alert_format>
</integration>

  <!-- 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>

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

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell
```

Note: These configuration we will add in to Agent ossec.conf file.

<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>

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

Now scroll down and see there is “vulnerability-detector” not enabled. Also some OS vulnerabilities configuration is set to not enabled.

```
root@wazuh-server:~
File  Actions  Edit  View  Help
GNU nano 2.9.8                /var/ossec/etc/ossec.conf

  </wodle>

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

  <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>
```

We have to enabled configuration here follow as shown in figure.

```
root@wazuh-server:~
File  Actions  Edit  View  Help
  GNU nano 2.9.8              /var/ossec/etc/ossec.conf              Modified

  </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>

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell
```

```
<!-- 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>
```

Now we have to enable “Aggregate Vulnerabilities” option. When you enable this option the vulnerability database will start downloading after restart wazuh manager.

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

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

</vulnerability-detector>
```

Now restart wazuh manager
Command: systemctl restart wazuh-manager

```
[wazuh-user@wazuh-server ~]$ sudo -i
[root@wazuh-server ~]# nano /var/ossec/etc/ossec.conf
[root@wazuh-server ~]# systemctl restart wazuh-manager
[root@wazuh-server ~]#
```

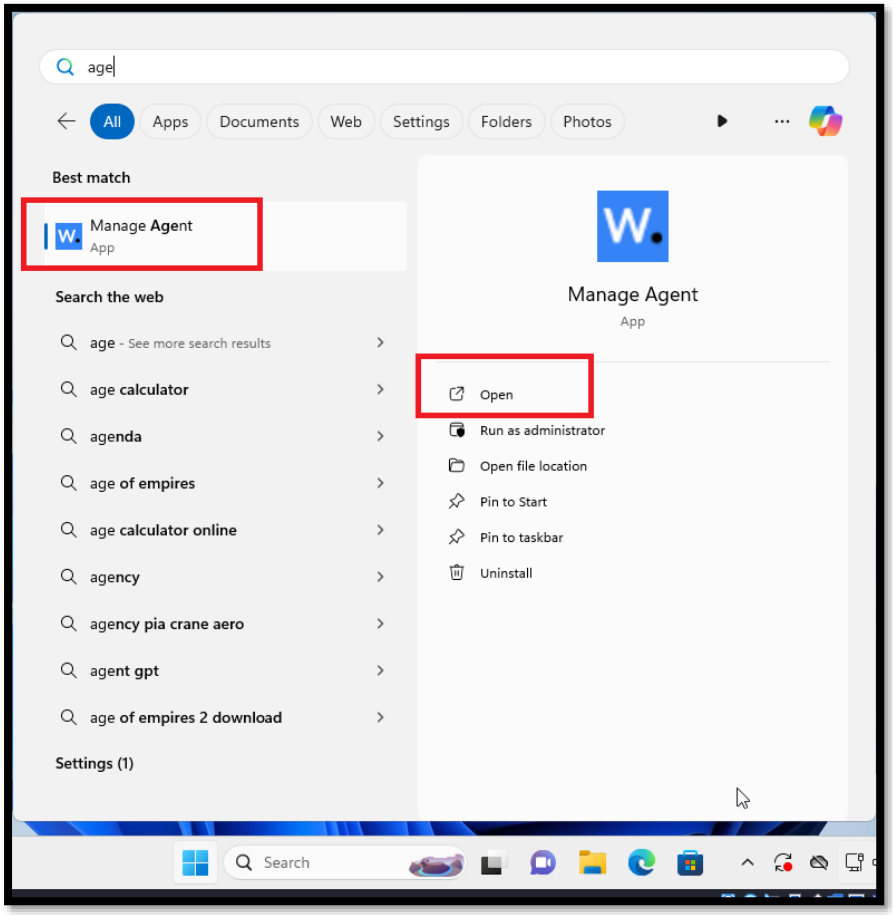
Now check the logs of “ossec.log” file
Command: cat /var/ossec/logs/ossec.log

```
[root@wazuh-server logs]# cat /var/ossec/logs/ossec.log
```

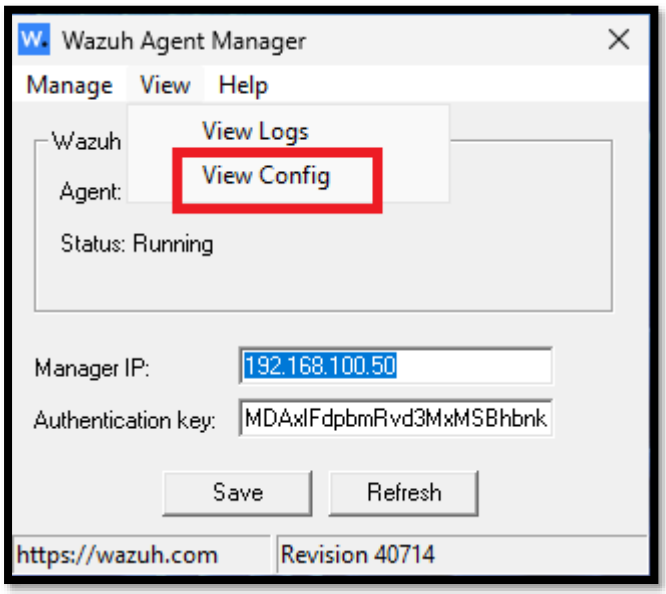
Vulnerability database is updating and starting scanning. So this vulnerability database is download form: https://nvd.nist.gov/vuln/data-feeds

```
wazuh-modulesd:vulnerability-detector: INFO: (5400): Starting 'Ubuntu Focal' database update.
rootcheck: INFO: Ending rootcheck scan.
wazuh-modulesd:vulnerability-detector: INFO: (5430): The update of the 'Ubuntu Focal' feed finished succes

wazuh-modulesd:vulnerability-detector: INFO: (5400): Starting 'Ubuntu Jammy' database update.
wazuh-modulesd:vulnerability-detector: INFO: (5430): The update of the 'Ubuntu Jammy' feed finished succes

wazuh-modulesd:vulnerability-detector: INFO: (5400): Starting 'Debian Buster' database update.
wazuh-modulesd:vulnerability-detector: INFO: (5430): The update of the 'Debian Buster' feed finished succe

wazuh-modulesd:vulnerability-detector: INFO: (5400): Starting 'Debian Bullseye' database update.
wazuh-modulesd:vulnerability-detector: INFO: (5430): The update of the 'Debian Bullseye' feed finished suc

wazuh-modulesd:vulnerability-detector: INFO: (5400): Starting 'Debian Bookworm' database update.
wazuh-modulesd:vulnerability-detector: INFO: (5430): The update of the 'Debian Bookworm' feed finished suc

wazuh-modulesd:vulnerability-detector: INFO: (5400): Starting 'National Vulnerability Database' database u

wazuh-modulesd:vulnerability-detector: INFO: (5430): The update of the 'National Vulnerability Database' f
sfully.
wazuh-modulesd:vulnerability-detector: INFO: (5400): Starting 'Microsoft Security Update' database update.
wazuh-modulesd:vulnerability-detector: INFO: (5430): The update of the 'Microsoft Security Update' feed fi
.
wazuh-modulesd:vulnerability-detector: INFO: (5431): Starting vulnerability scan.
```

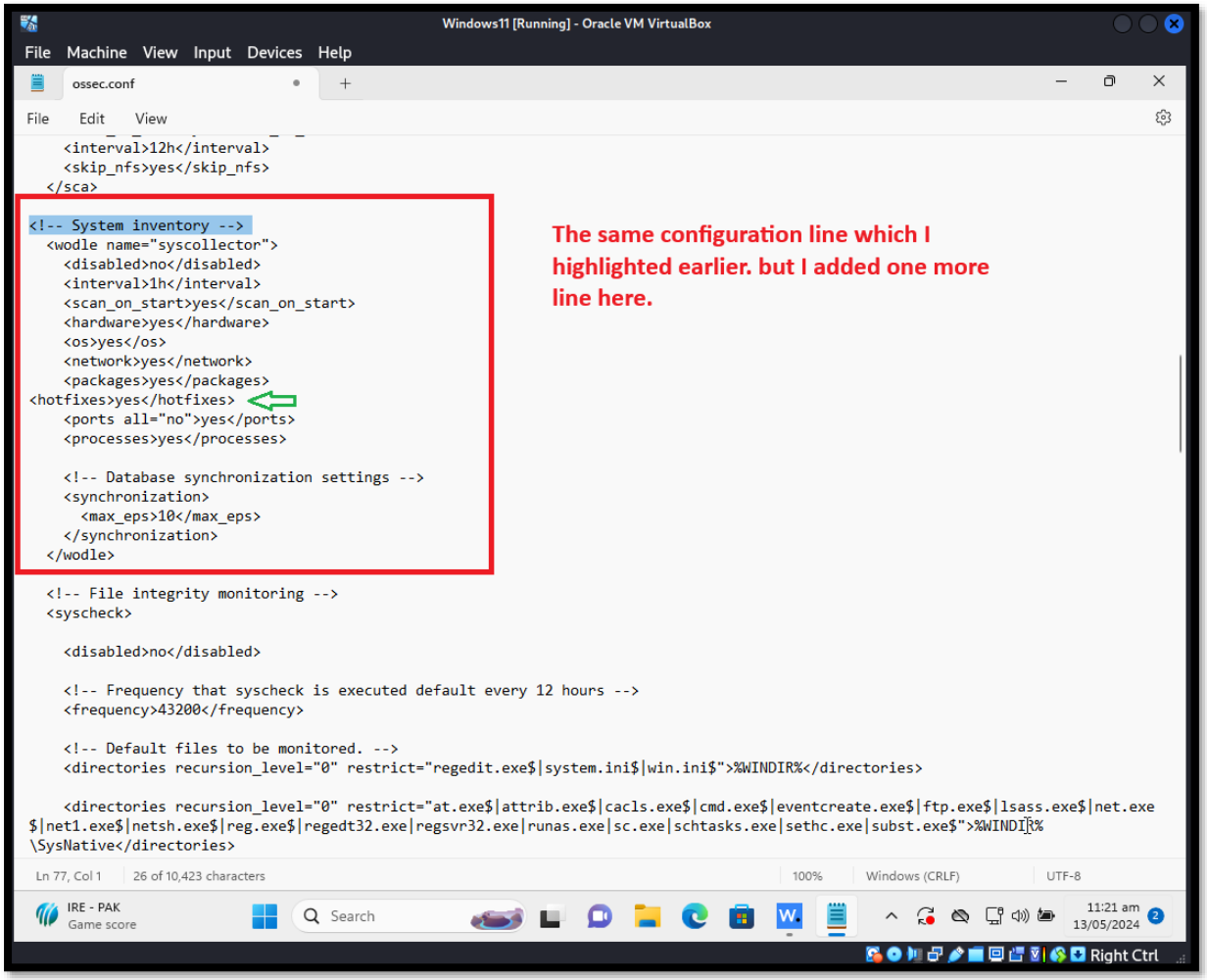
Now we have to edit configuration in Windows-agent “ossec.conf: file open wazuh-agent.



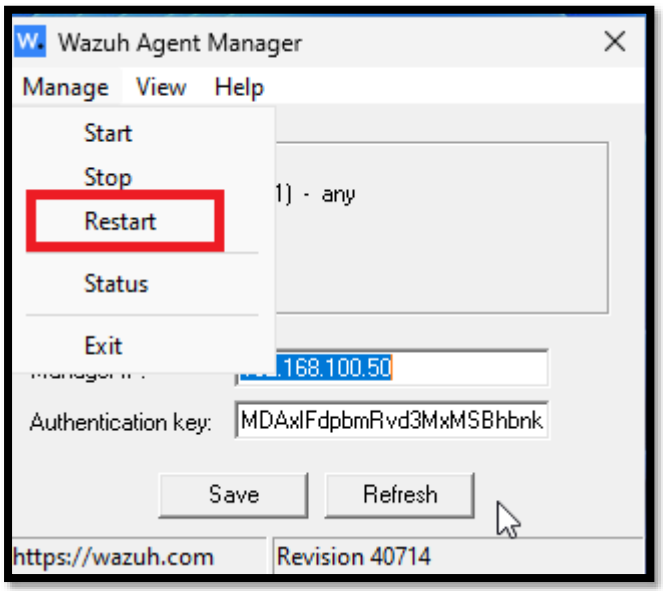
Now go to View > View Config



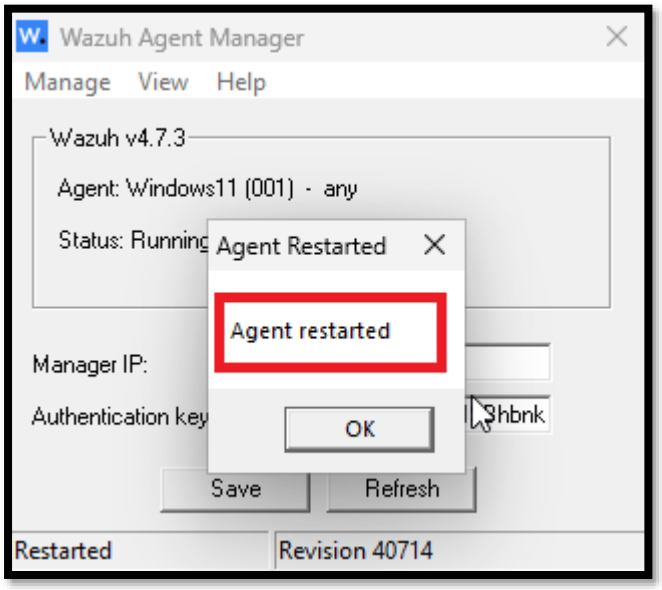
Add the following configuration line here.
I am adding here one extra line: <hotfixes>yes</hotfixes>



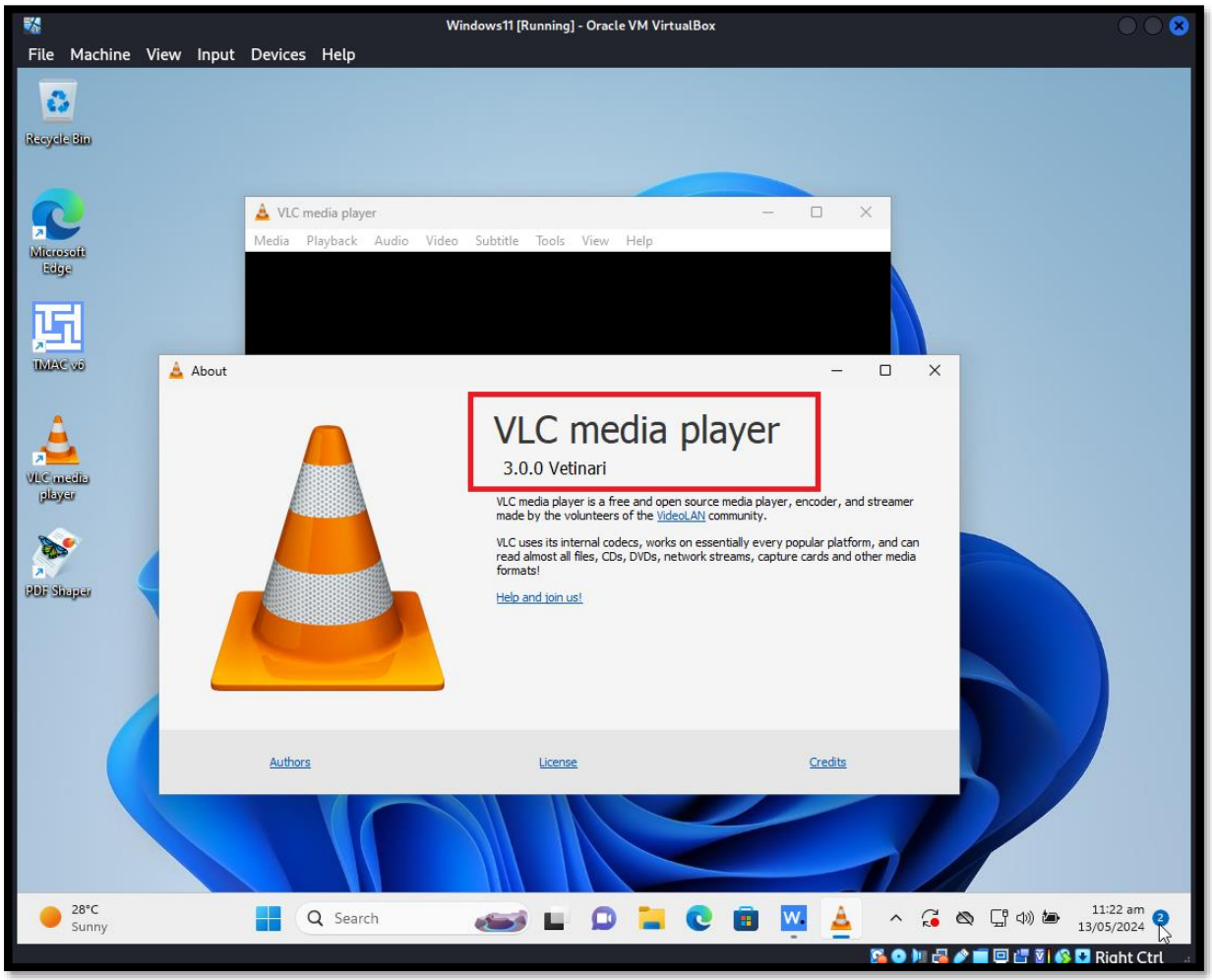
After adding configuration we have to restart wazuh agent.



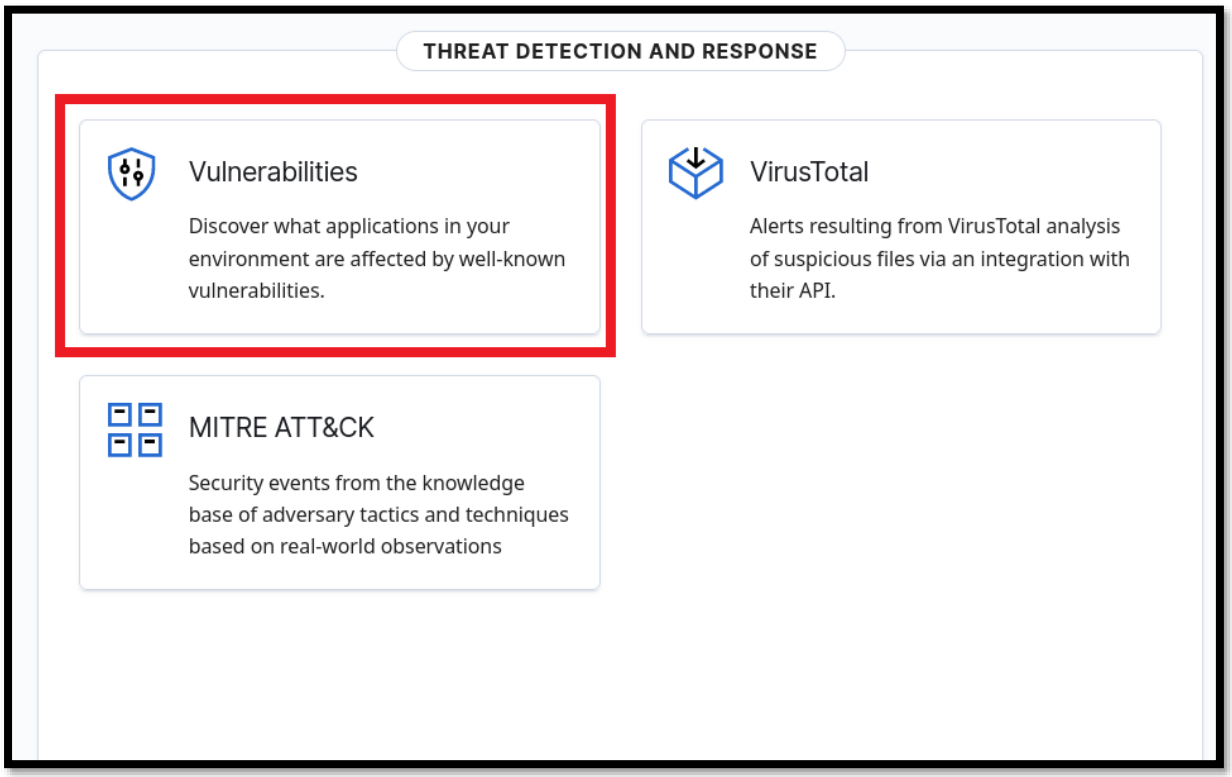
Wazuh-agent is restarted.



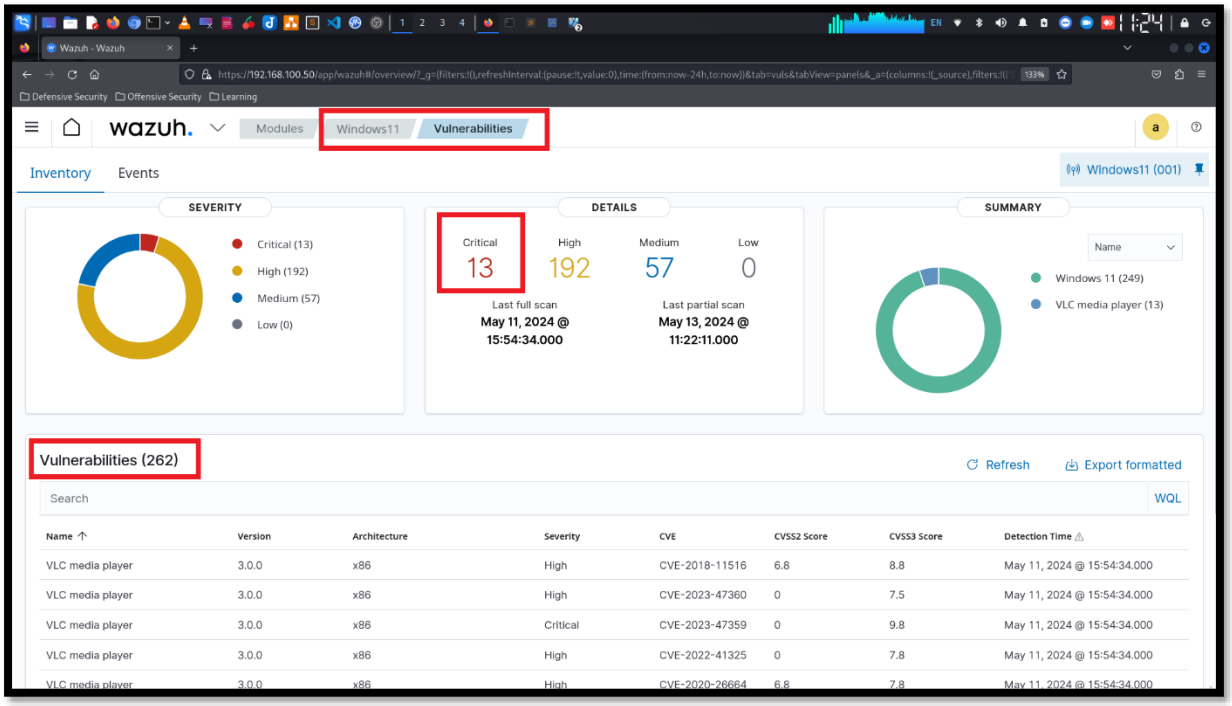
Here is vulnerable VLC media player installed on my Windows 11 machine.



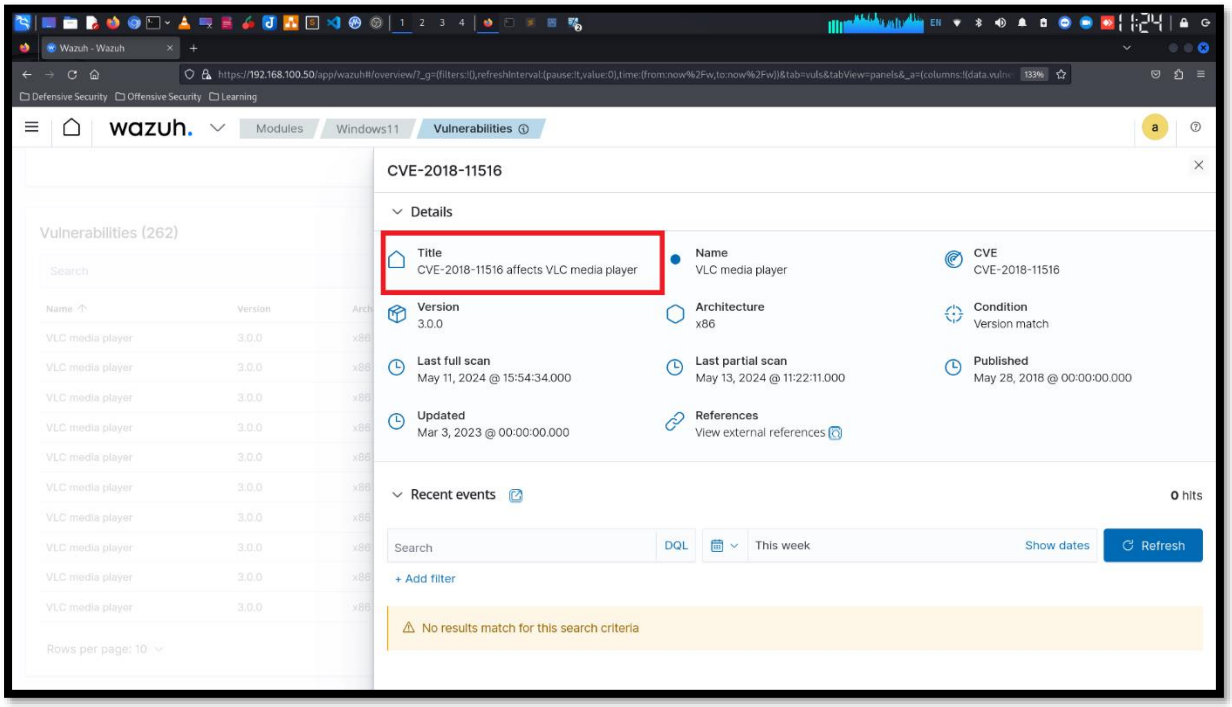
Now click on “Vulnerabilities” again.



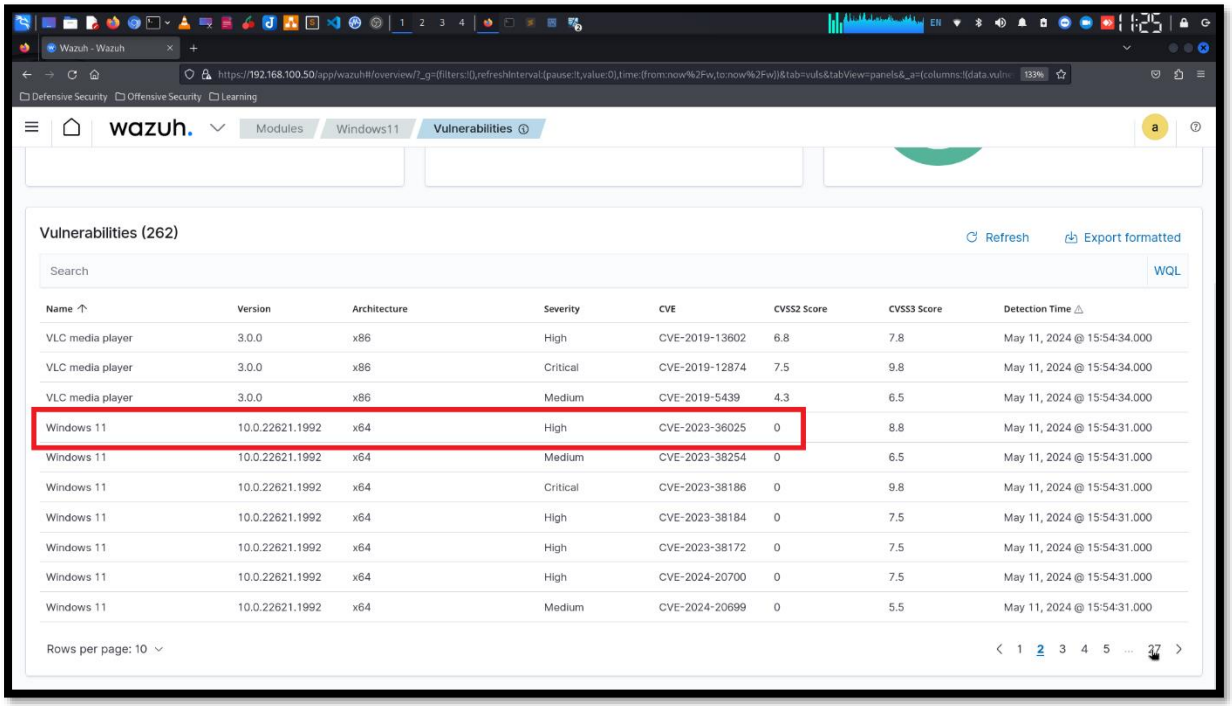
Here is **Vulnerabilities Detected!!**



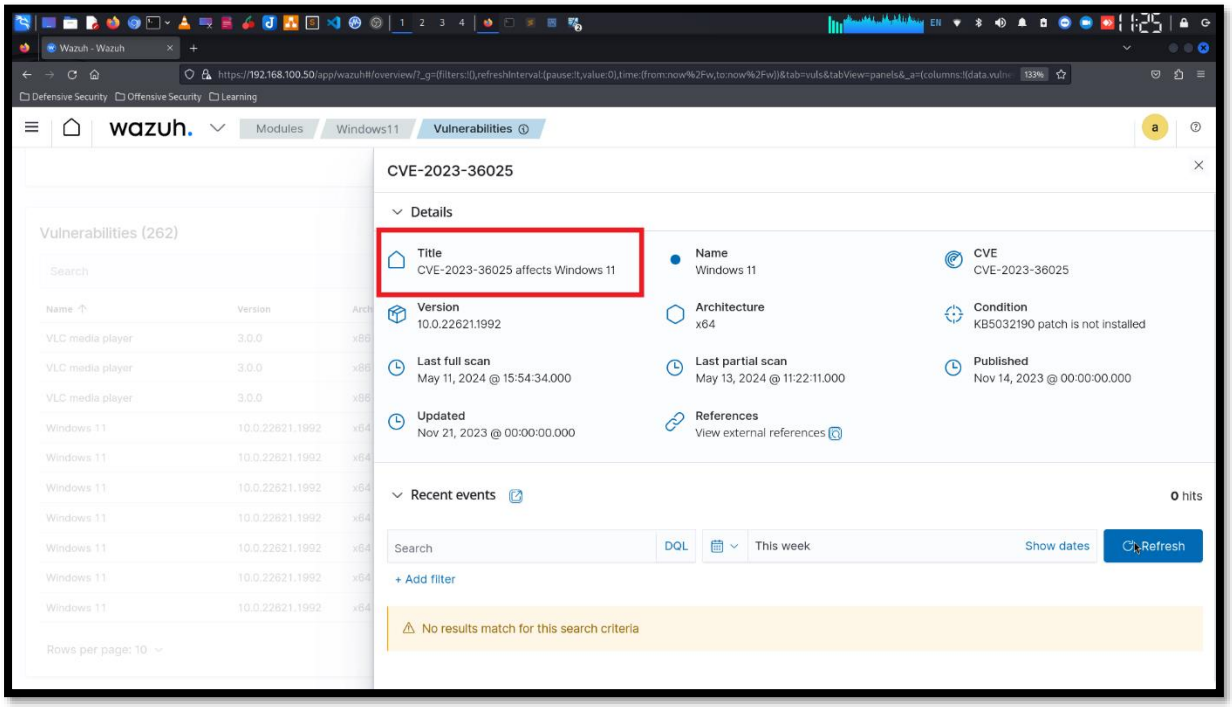
Let’s see the vulnerability details. Here is the vulnerability in VLC Media Player.



We have 2 major vulnerabilities in our windows 11.



Windows 11 Vulnerability details.



SUMMARY

In summary, Wazuh's vulnerability detection capabilities help organizations proactively identify and mitigate security risks, thereby strengthening their defence against cyber threats and ensuring the integrity and availability of their systems and data.