Vulnerability Detection
Wazuh

Vulnerability Detection using Wazuh

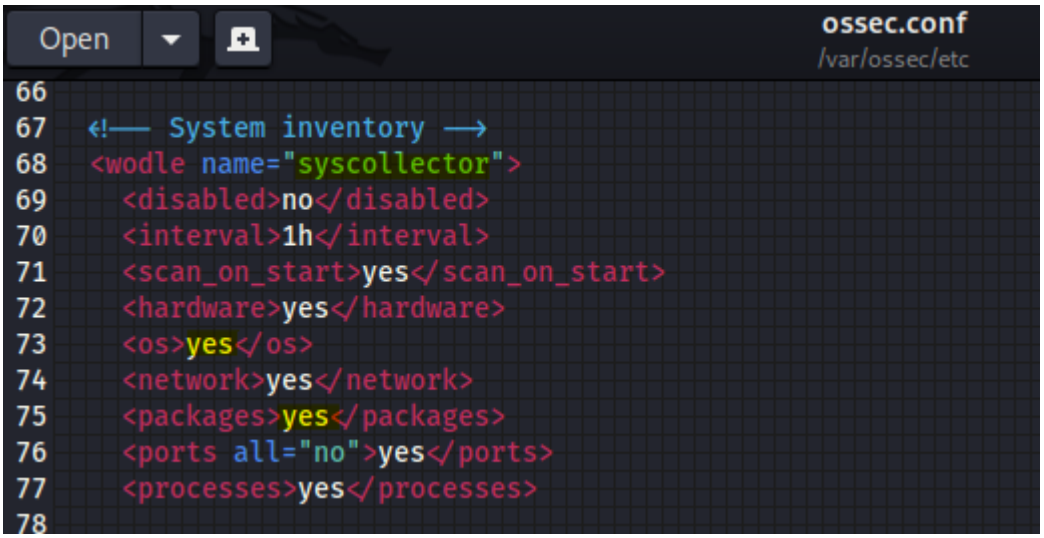
To detect vulnerabilities, Wazuh agents collect a list of installed applications from monitored endpoints and send it periodically to the Wazuh server. Local SQLite databases in the Wazuh server store this list. Also, the Wazuh server builds a global vulnerability database from publicly available CVE repositories. It uses this database to cross-correlate this information with the application inventory data of the agent.

How to configure

Configure Agent

For this task we have installed an agent in Kali Linux which is running on a VM.
After the installation configure the Agent's config file.

1. Location for the config file is `/var/ossec/etc/ossec.conf`
2. Edit the config file using any editor & look for System inventory.
3. In the System inventory section you will find sys collector, make sure it's **Enable.**
4. `<os>` tag used to detect Operating systems running on the Agent. This should be set to `YES`
5. There is a `<packages>` tag used to read all the package information present in the agent. This also should be set to `YES`
6. Save & exit



Now restart your wazuh agent service using a command mentioned below:

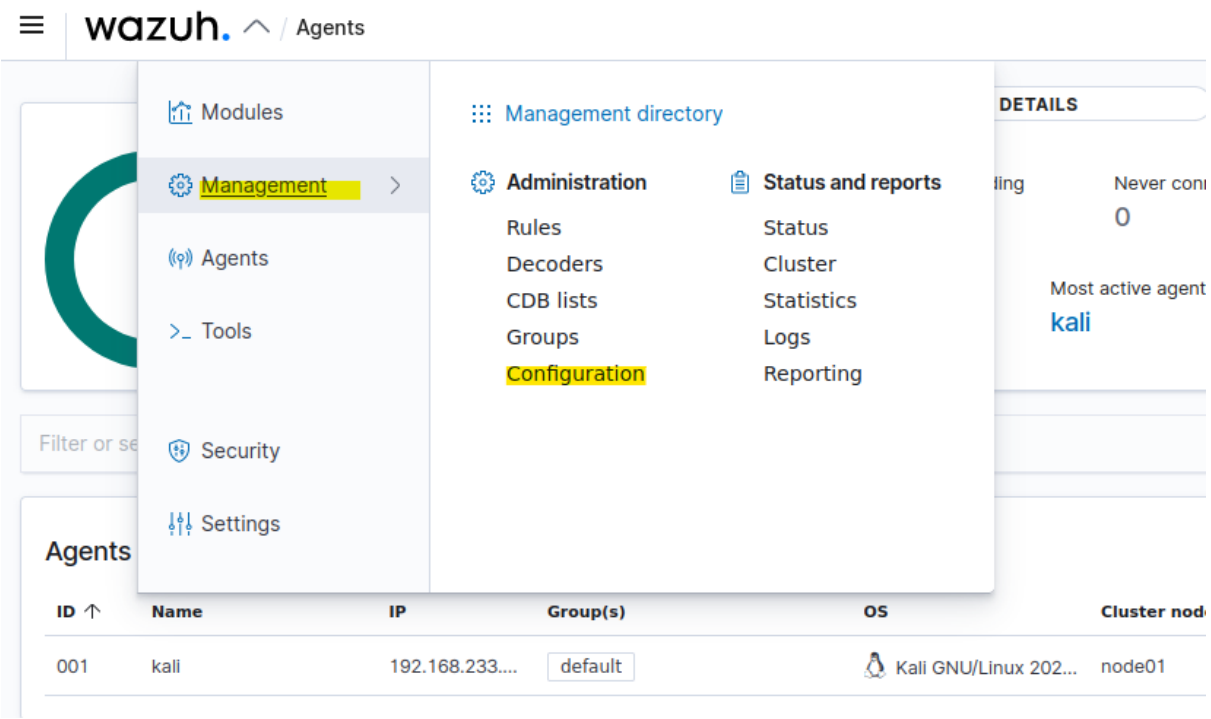
```
# service wazuh-agent restart
```

Now let’s move to the Wazuh managers dashboard

Configure Manager

Step 1

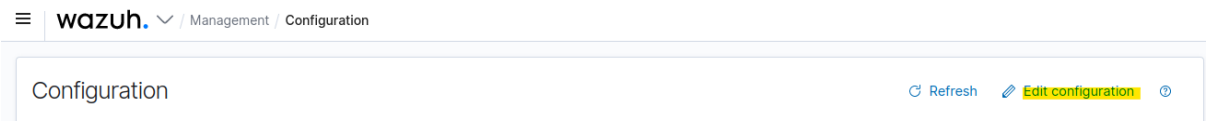
Configure manager for vulnerability management
Follow the steps click on `wazuh management > configuration`



Step 2

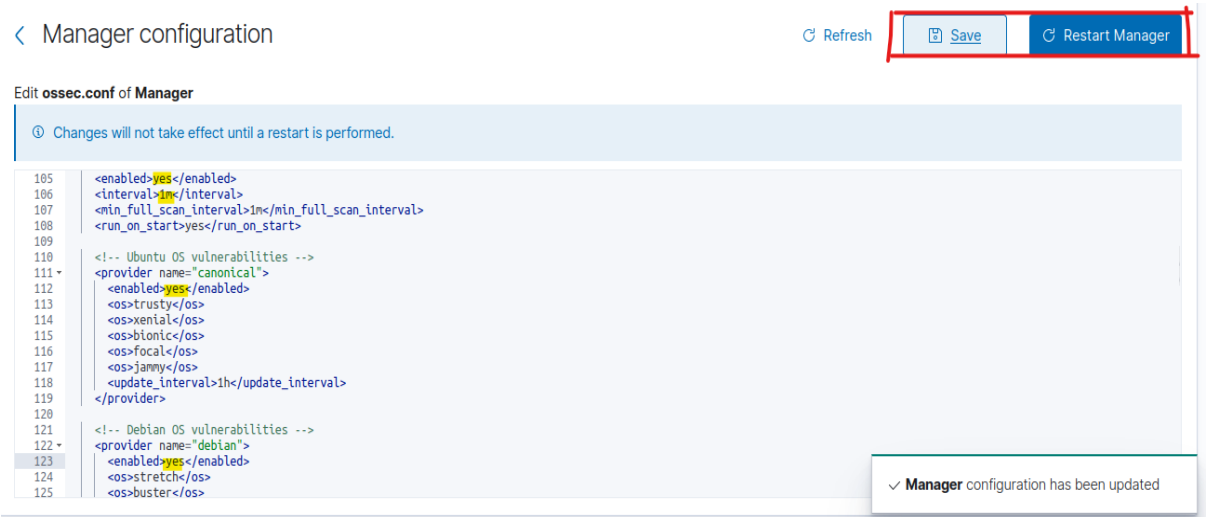
When you land in configuration page you can find `Edit configuration` on right top corner.

Now we have to edit the configuration click on that.



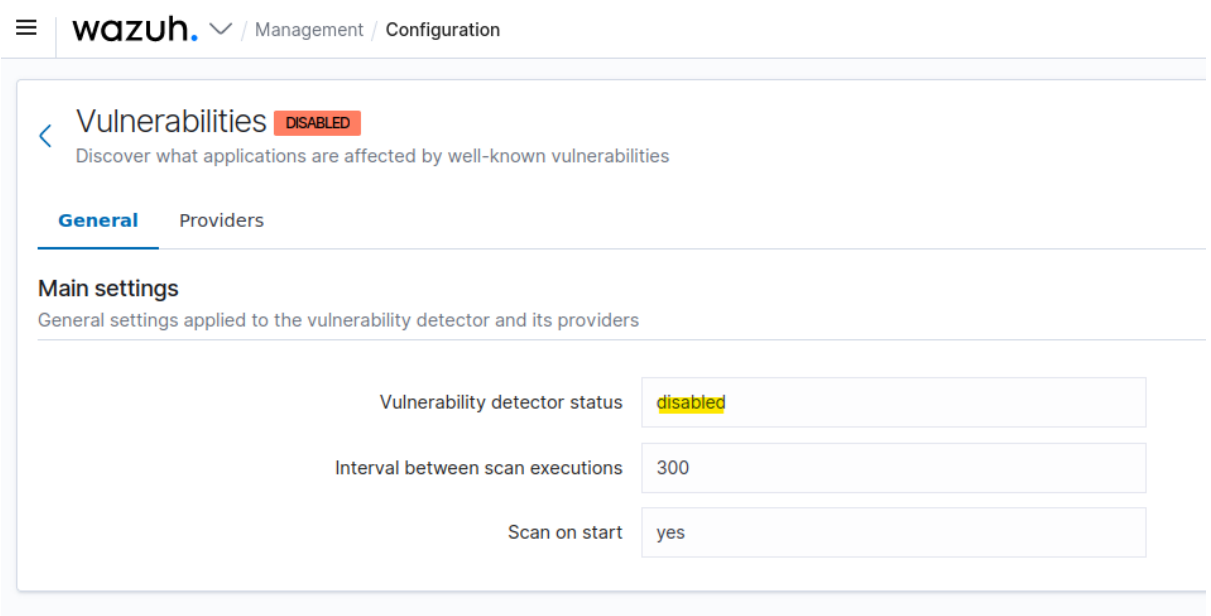
Step 3

1. Enable vulnerability Detection option
2. You can set a time **interval** to get a vulnerability updates in each specified time.
3. Enable specific **os**, in which you want to detect vulnerability.
4. **Save** configuration and **Restart the manager.**



Step 4 (optional)

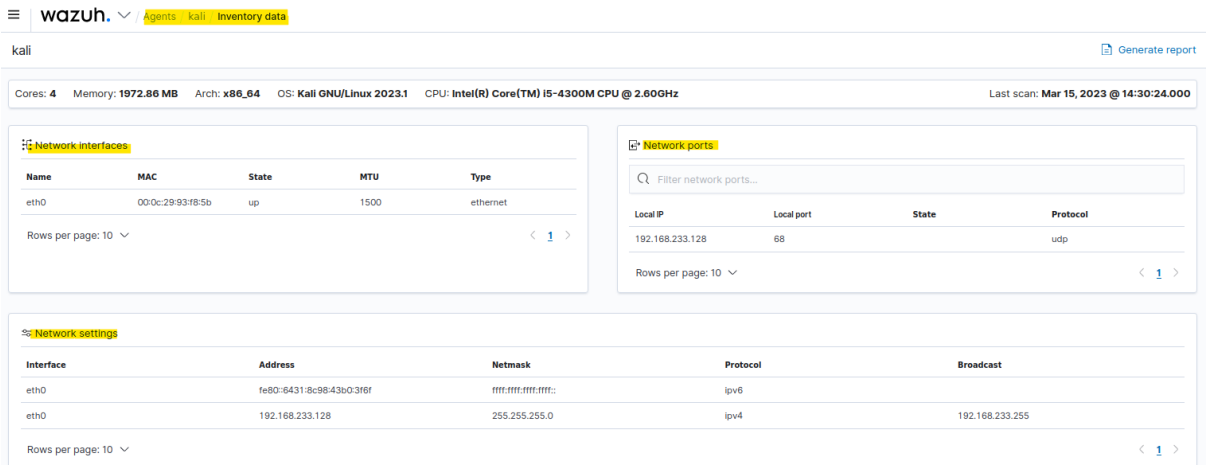
You can also check if vulnerability detection is enabled or not. If not, you have to configure it as I mentioned in the **Step 3.**



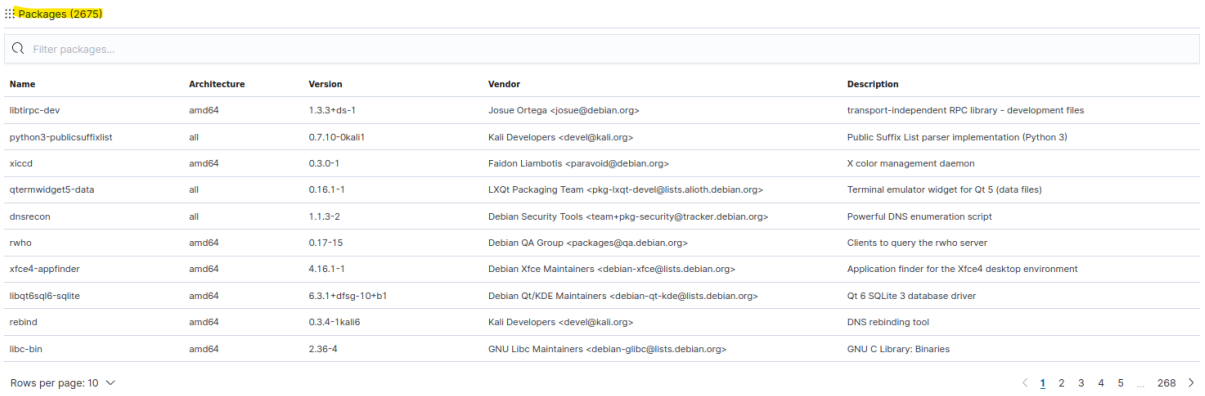
Step 5

At this point setup & configuration is Done. Now let's check the agent's inventory.
By going to `agent > selected agent > Inventory.`

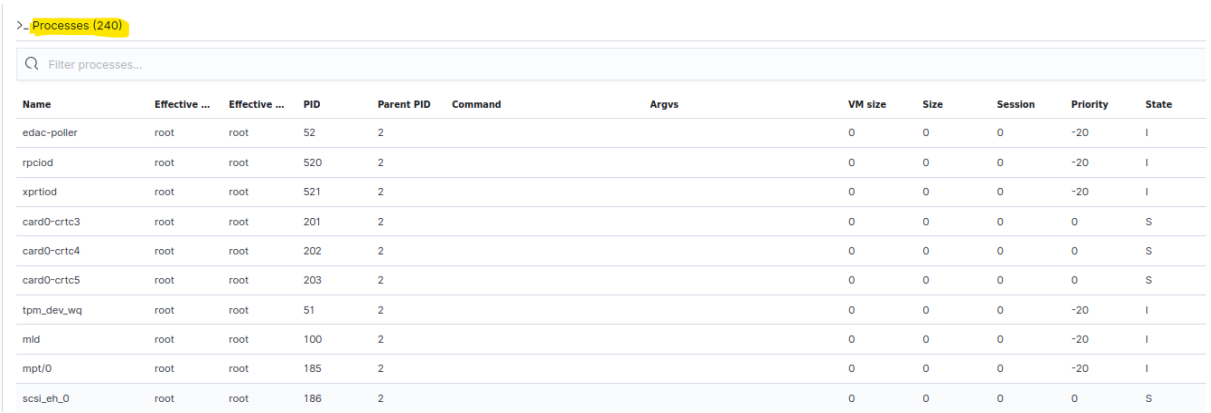
- In inventory it shows all the available data of agents collected.



- You can see all the packages installed on the agent's operating system.

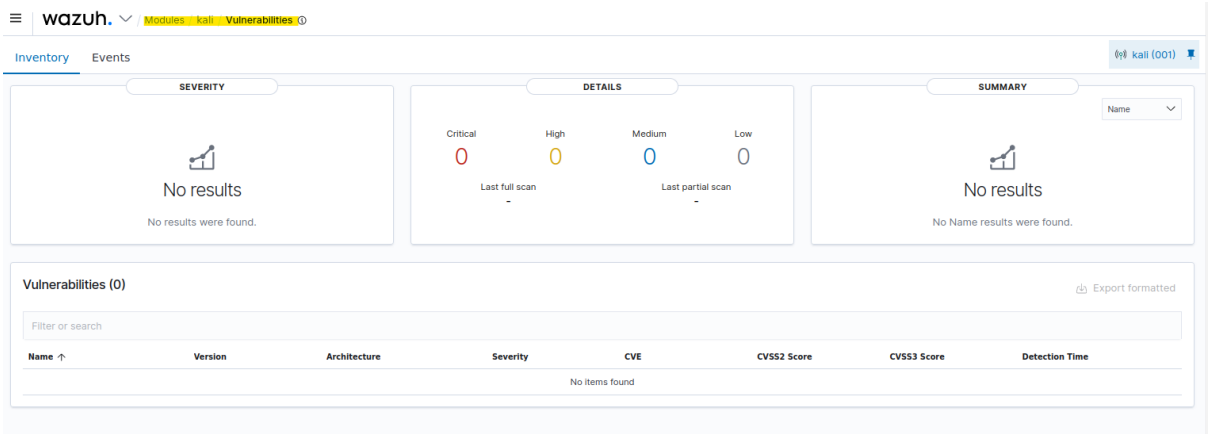


- You can also see all the processes which are running on the agent's operating system.



Step 6

Now let’s check the vulnerability detection Dashboard. What we found here



We found 0 Vulnerability. Because the agent I used is kali linux & it is up to date. Hence, there is no vulnerability.

—----------EOD—----------