

Vulnerability Detection

Wazuh

Vulnerability Detection using Wazuh

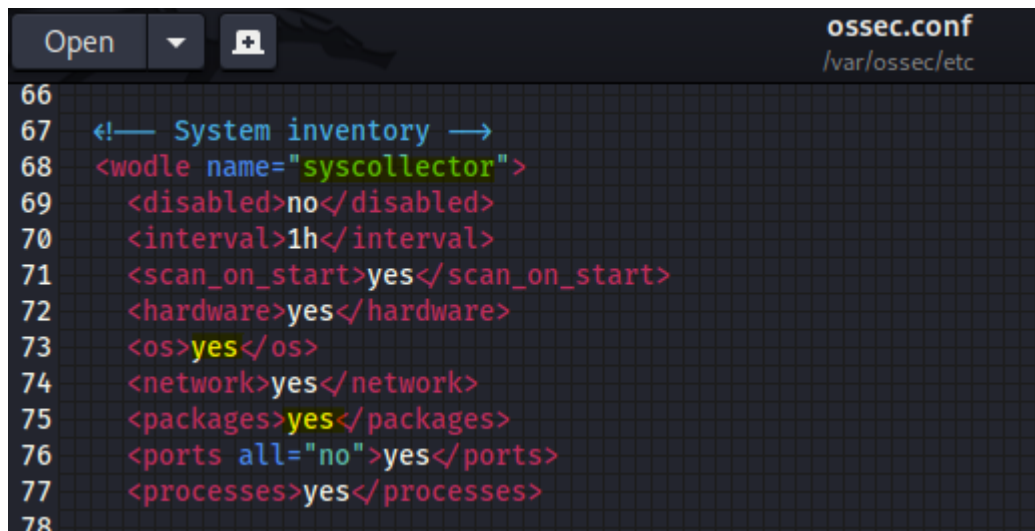
To detect vulnerabilities, Wazuh agents collect a list of installed applications from monitored endpoints and send it periodically to the Wazuh server. Local SQLite databases in the Wazuh server store this list. Also, the Wazuh server builds a global vulnerability database from publicly available CVE 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



```
66
67 <!-- System inventory -->
68 <wodle name="syscollector">
69   <disabled>no</disabled>
70   <interval>1h</interval>
71   <scan_on_start>yes</scan_on_start>
72   <hardware>yes</hardware>
73   <os>yes</os>
74   <network>yes</network>
75   <packages>yes</packages>
76   <ports all="no">yes</ports>
77   <processes>yes</processes>
78
```

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

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

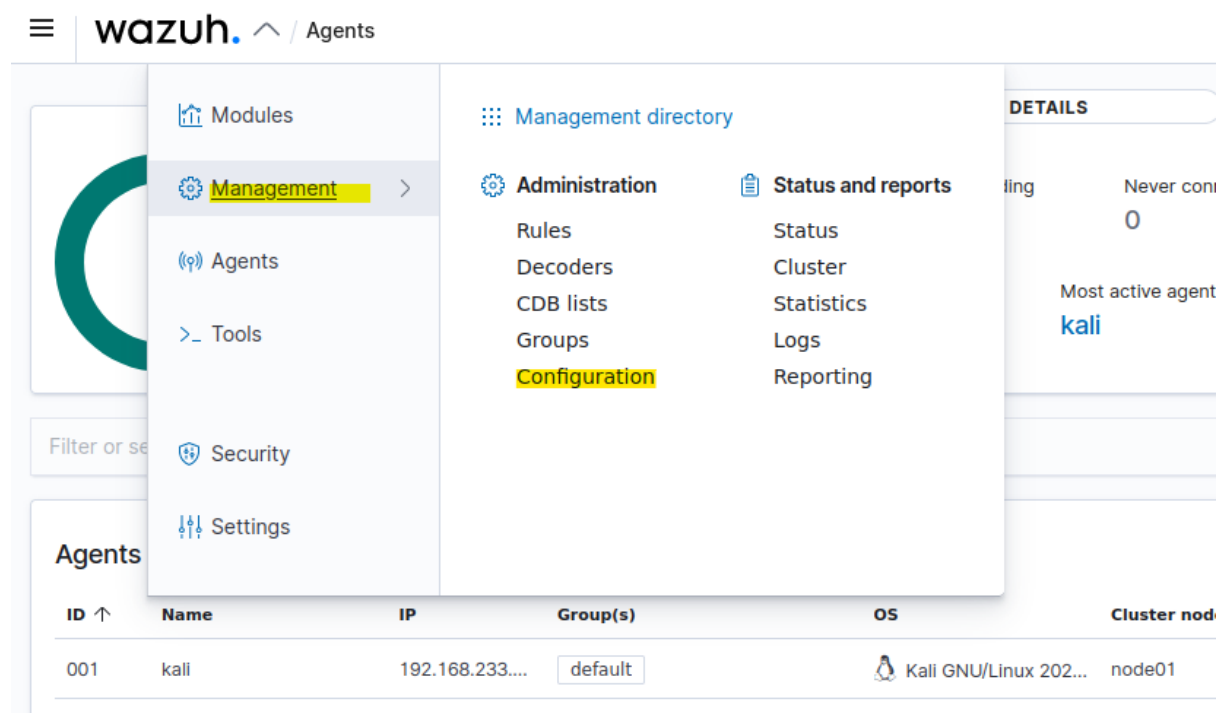
Now let's move to the Wazuh managers dashboard

Configure Manager

Step 1

Configure manager for vulnerability management

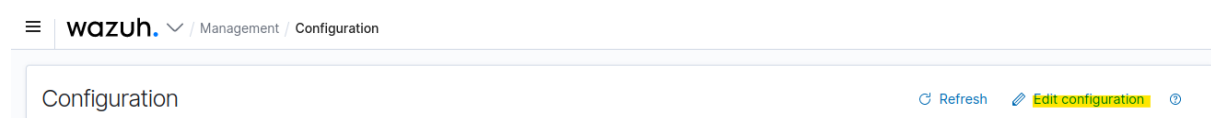
Follow the steps click on `wazuh management > configuration`



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**.

Manager configuration

Refresh Save Restart Manager

Edit ossec.conf of Manager

Changes will not take effect until a restart is performed.

```
105 <enabled>yes</enabled>
106 <interval>1m</interval>
107 <min_full_scan_interval>1m</min_full_scan_interval>
108 <run_on_start>yes</run_on_start>
109
110 <!-- Ubuntu OS vulnerabilities -->
111 <provider name="canonical">
112   <enabled>yes</enabled>
113   <os>trusty</os>
114   <os>xenial</os>
115   <os>bionic</os>
116   <os>focal</os>
117   <os>jammy</os>
118   <update_interval>1h</update_interval>
119 </provider>
120
121 <!-- Debian OS vulnerabilities -->
122 <provider name="debian">
123   <enabled>yes</enabled>
124   <os>stretch</os>
125   <os>buster</os>
```

✓ Manager configuration has been updated

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**.

Management / Configuration

Vulnerabilities DISABLED

Discover what applications are affected by well-known vulnerabilities

General Providers

Main settings

General settings applied to the vulnerability detector and its providers

Vulnerability detector status	disabled
Interval between scan executions	300
Scan on start	yes

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.

Wazuh interface showing the inventory of a Kali Linux agent.

Network interfaces

Name	MAC	State	MTU	Type
eth0	00:0c:29:93:f8:5b	up	1500	ethernet

Rows per page: 10

Network ports

Local IP	Local port	State	Protocol
192.168.233.128	68		udp

Rows per page: 10

Network settings

Interface	Address	Netmask	Protocol	Broadcast
eth0	fe80::6431:8c98:43b0:3f6f	ffff:ffff:ffff::	ipv6	
eth0	192.168.233.128	255.255.255.0	ipv4	192.168.233.255

Rows per page: 10

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

Wazuh interface showing the list of installed packages on the Kali Linux agent.

Packages (2675)

Name	Architecture	Version	Vendor	Description
libtirpc-dev	amd64	1.3.3+ds-1	Josue Ortega <josue@debian.org>	transport-independent RPC library - development files
python3-publicsuffixlist	all	0.7.10-0kali1	Kali Developers <devel@kali.org>	Public Suffix List parser implementation (Python 3)
xiccd	amd64	0.3.0-1	Faidon Liambotis <paravoid@debian.org>	X color management daemon
qtermwidget5-data	all	0.16.1-1	LXQt Packaging Team <pkg-lxqt-devel@lists.ubuntu.com>	Terminal emulator widget for Qt 5 (data files)
dnsrecon	all	1.1.3-2	Debian Security Tools <team+pkg-security@tracker.debian.org>	Powerful DNS enumeration script
rwho	amd64	0.17-15	Debian QA Group <packages@qa.debian.org>	Clients to query the rwho server
xfce4-appfinder	amd64	4.16.1-1	Debian Xfce Maintainers <debian-xfce@lists.debian.org>	Application finder for the Xfce4 desktop environment
libqt6sql-sqlite	amd64	6.3.1+dfsg-10+b1	Debian Qt/KDE Maintainers <debian-qt-kde@lists.debian.org>	Qt 6 SQLite 3 database driver
rebinder	amd64	0.3.4-1kali6	Kali Developers <devel@kali.org>	DNS rebinding tool
libc-bin	amd64	2.36-4	GNU Libc Maintainers <debian-glibc@lists.debian.org>	GNU C Library: Binaries

Rows per page: 10

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

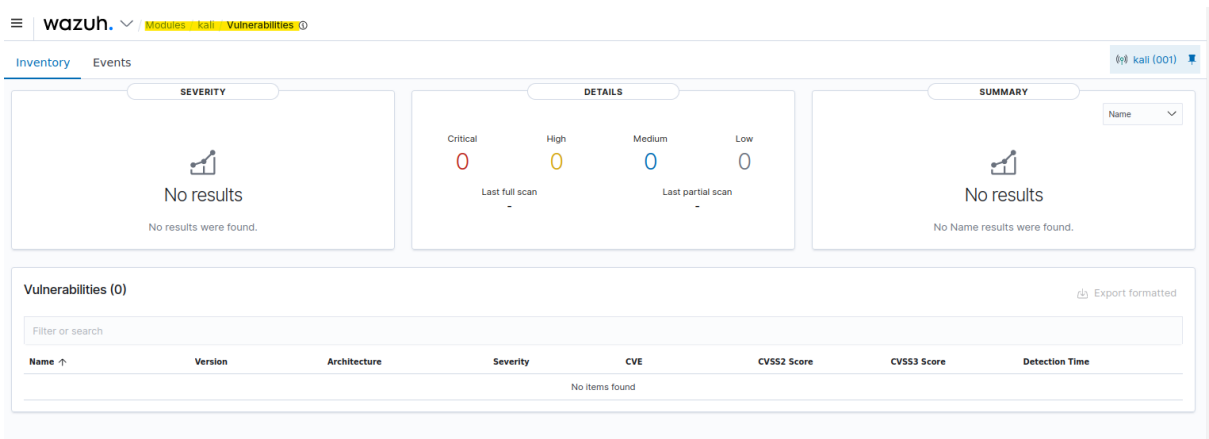
Wazuh interface showing the list of running processes on the Kali Linux agent.

Processes (240)

Name	Effective ...	Effective ...	PID	Parent PID	Command	Argvs	VM size	Size	Session	Priority	State
edac-poller	root	root	52	2			0	0	0	-20	I
rpciod	root	root	520	2			0	0	0	-20	I
xprtiod	root	root	521	2			0	0	0	-20	I
card0-crtc3	root	root	201	2			0	0	0	0	S
card0-crtc4	root	root	202	2			0	0	0	0	S
card0-crtc5	root	root	203	2			0	0	0	0	S
tpm_dev_wq	root	root	51	2			0	0	0	-20	I
mld	root	root	100	2			0	0	0	-20	I
mptj0	root	root	185	2			0	0	0	-20	I
scsi_ah_0	root	root	186	2			0	0	0	0	S

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-----