Enabling Vulnerability Detection and Email Alerts

SAMEER HASSAN

Wazuh lab-03

Github-link: GitHub - sameerhassancode/Wazuh-

Linkedin: https://www.linkedin.com/in/sameer-hassan-15a428255/

Wazuh is an open-source security platform offering **threat detection, integrity monitoring, and security analytics** to help organizations respond to security incidents. A key feature is **vulnerability detection**, achieved through:

1. **Vulnerability Scanning** – Integrates with OpenVAS and Nessus to identify known vulnerabilities.
2. **Asset Inventory** – Maintains a record of hardware/software to spot outdated or vulnerable systems.
3. **Behavioral Analysis** – Monitors system and network activity for anomalies suggesting security threats.
4. **Real-time Alerts** – Provides instant notifications about detected vulnerabilities with remediation steps.
5. **Customization & Extensibility** – Allows tailored security rules to suit organizational needs.

Start the Wazuh

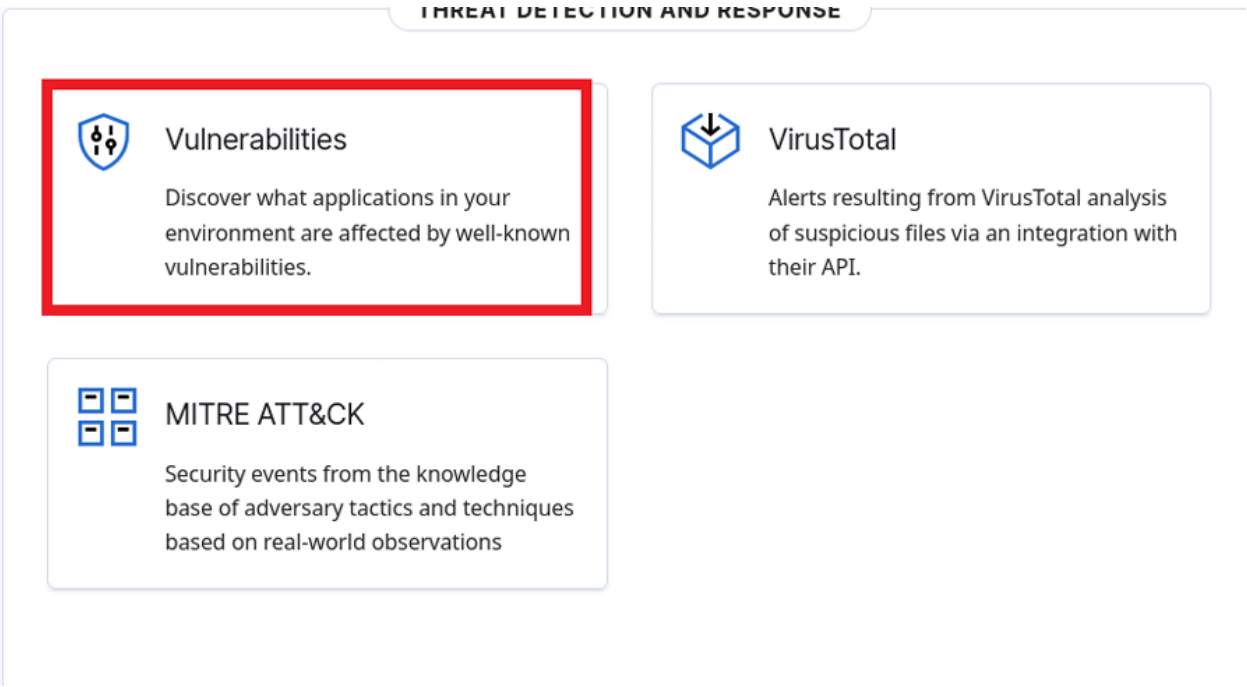
After starting Wazuh get SSH access for easy configuration!

```
Microsoft Windows [Version 10.0.26100.4202]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Shifat>ssh wazuh-user@192.168.100.205
wazuh-user@192.168.100.205's password:

A newer release of "Amazon Linux" is available.
  Version 2023.7.20250428:
  Version 2023.7.20250512:
  Version 2023.7.20250527:
Run "/usr/bin/dnf check-release-update" for full release and version update info
```

Now Access the wazuh server dashboard and you will see the Vulnerablity in the threat intelligence section.

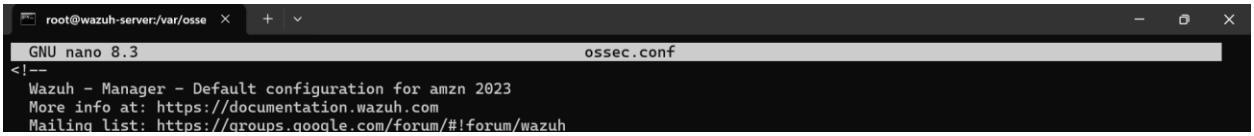


Now let’s configure Vulnerability scanner

Get admin permission with sudo -i

Then Goto file path : /var/ossec/etc/ossec.conf

And open the file with nano ossec.conf.



After opening the file locate this section

```
<vulnerability-detection>
  <enabled>yes</enabled>
  <index-status>yes</index-status>
  <feed-update-interval>60m</feed-update-interval>
</vulnerability-detection>
```

After location this code copy and paste this below code snippet and save the file.

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

 <!-- Canonical feed: Debian/Ubuntu -->
 <provider>
  <name>canonical</name>
  <enabled>yes</enabled>
  <os>debian,ubuntu</os>
 </provider>

 <!-- Microsoft feed: Windows -->
 <provider>
  <name>msu</name>
  <enabled>yes</enabled>
  <os>windows</os>
 </provider>

 <!-- NVD feed: General vulnerabilities for all OS -->
 <provider>
  <name>nvd</name>
```

```
  <enabled>yes</enabled>

  <update_interval>1h</update_interval>

 </provider>

</vulnerability-detector>
```

Save the file with CTRL + O → Enter → CRTL + X

After that run this command cat /var/ossec/logs/ossec.log and you will notice our vulnerability scanner is started!!

```
2025/06/10 08:55:17 wazuh-modulesd:vulnerability-scanner: INFO: Vulnerability scanner module started.
2025/06/10 08:55:17 wazuh-modulesd:syscollector: INFO: Evaluation finished.
2025/06/10 08:55:19 wazuh-syscheckd: INFO: (6009): File integrity monitoring scan ended.
2025/06/10 08:55:19 wazuh-syscheckd: INFO: FIM sync module started.
2025/06/10 08:55:29 sca: INFO: Evaluation finished for policy '/var/ossec/ruleset/sca/cis_amazon_linux_2023.yml'
2025/06/10 08:55:29 sca: INFO: Security Configuration Assessment scan finished. Duration: 14 seconds.
2025/06/10 08:55:56 rootcheck: INFO: Ending rootcheck scan.
[root@wazuh-server etc]#
```

Database source: [NVD - Data Feeds]

Now after that verify the vulnerability with this command

tail -f /var/ossec/logs/ossec.log | grep vuln

```
[root@wazuh-server etc]# tail -f /var/ossec/logs/ossec.log | grep vuln
2025/06/10 09:05:17 indexer-connector: INFO: IndexerConnector initialized successfully for index: wazuh-states-vulnerabilities-wazuh-
server.
2025/06/10 09:05:18 wazuh-modulesd:vulnerability-scanner: INFO: Vulnerability scanner module started.
```

Our Vulnerability Scanner is configured and working now let's enable email notification for IDS and new vulnerability

Again Open Ossec.conf file and at the top you will see the <global > tag and inside you will also notice some Email tags.

```
  GNU nano 8.3                                                    ossec.conf
<!--
  Wazuh - Manager - Default configuration for amzn 2023
  More info at: https://documentation.wazuh.com
  Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>no</logall>
    <logall_json>no</logall_json>
    <email_notification>no</email_notification>
    <smtp_server>smtp.example.wazuh.com</smtp_server>
    <email_from>wazuh@example.wazuh.com</email_from>
    <email_to>recipient@example.wazuh.com</email_to>
    <email_maxperhour>12</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
    <agents_disconnection_time>10m</agents_disconnection_time>
    <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
    <update_check>yes</update_check>
  </global>
```

Just make below changes!

```
<global>
<jsonout_output>yes</jsonout_output>
<alerts_log>yes</alerts_log>
<logall>no</logall>
<logall_json>no</logall_json>
<email_notification>yes</email_notification>
<smtp_server>smtp.gmail.com</smtp_server>
<email_from>sameerkhan1214110@gmail.com</email_from>
<email_to>sameerishassan@gmail.com</email_to>

<email_maxperhour>12</email_maxperhour>
<email_log_source>alerts.log</email_log_source>
<agents_disconnection_time>10m</agents_disconnection_time>
<agents_disconnection_alert_time>0</agents_disconnection_alert_time>
<update_check>yes</update_check>
</global>
```

Note wazuh doesnot support SMPT tags like Email_pass so to bypass this error we will install ssmpt with given command! sudo yum install ssmtp

```
[root@wazuh-server etc]# sudo yum install ssmtp
Last metadata expiration check: 1 day, 2:45:46 ago on Mon Jun  9 07:33:55 2025.
Dependencies resolved.
=================================================================================================================================
 Package                    Architecture               Version                                  Repository                       Size
=================================================================================================================================
Installing:
 ssmtp                      x86_64                     2.64-26.amzn2023.0.2                     amazonlinux                      48 k

Transaction Summary
=================================================================================================================================
Install  1 Package

Total download size: 48 k
Installed size: 79 k
Is this ok [y/N]: y
Downloading Packages:
```

After intalling the ssmpt change directory to ssmpt and then you will ssmpt.conf file

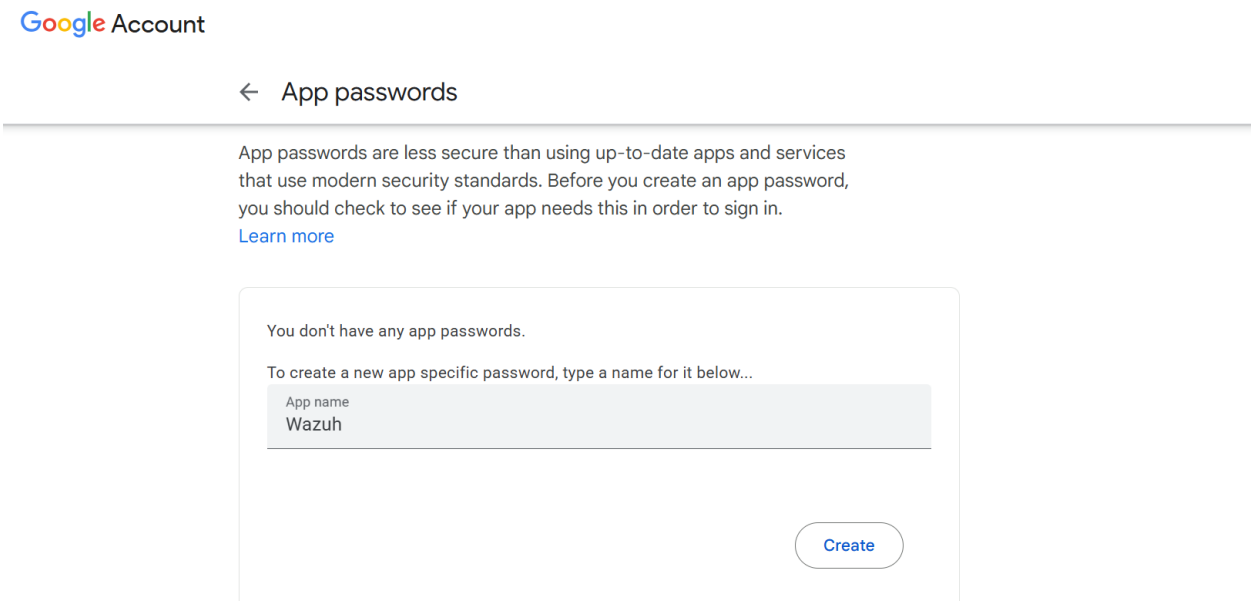
Inside the file you will see this code

```
  GNU nano 8.3
root=postmaster
mailhub=smtp.gmail.com:587
AuthUser=sameerkhan1214110@gmail.com
AuthPass=[redacted]
UseSTARTTLS=YES
FromLineOverride=YES
```

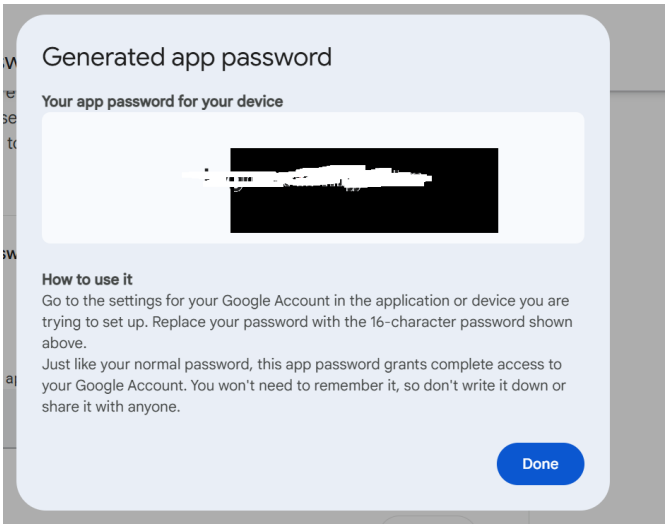
Ok now let's obtain the email authpass key! Open you Gmail account on web browser and goto this link! https://myaccount.google.com/apppasswords

After opening you will see this

Enter any name I entered name Wazuh!



After that hit click and you will see the app password copy the app password and paste it in the ssmpt.conf file in authpass tag



Paste it under authpass Now save the file and run this command to test it

cat /var/ossec/etc/logs/ossec.log

```
2025/06/10 10:15:52 wazuh-maild: INFO: Getting alerts in log format.
2025/06/10 10:15:53 wazuh-syscheckd: INFO: (6206): Ignore 'file' entry '/etc/mail/statistics'
2025/06/10 10:30:53 wazuh-maild: INFO: (1225): SIGNAL [(15)-(Terminated)] Received. Exit Cleaning.
2025/06/10 10:31:06 wazuh-maild: INFO: Started (pid: 51582).
2025/06/10 10:31:06 wazuh-maild: INFO: Getting alerts in log format.
2025/06/10 10:31:07 wazuh-syscheckd: INFO: (6206): Ignore 'file' entry '/etc/mail/statistics'
[root@wazuh-server logs]#
```

Now you your system found any new vulnerability it will send you alert through the email notification

summary:

Wazuh's vulnerability detection feature proactively identifies security weaknesses in your systems, allowing organizations to take action before threats can be exploited. This strengthens overall cybersecurity by ensuring system integrity, availability, and compliance. Additionally, configuring email alerts (via tools like ssmtp) allows Wazuh to notify administrators in real time about critical security events. This immediate awareness enhances response time and minimizes potential damage from threats.