Rootkit Detection, **Detect Failed SSH Login Attempts**,

and **Enable Active Responses**

using **Wazuh**

-R.M.Naren Adithya

6. Rootkit Detection with Wazuh

- Unauthorized file changes

A. Ensure Rootcheck is Enabled

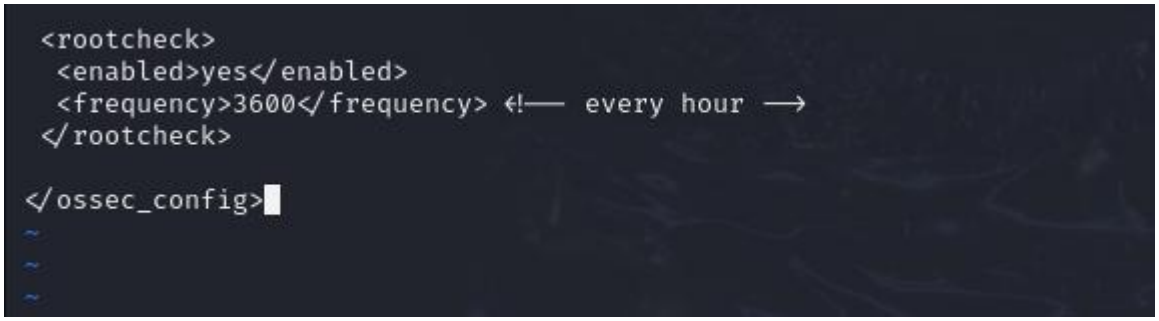
On the agent (/var/ossec/etc/ossec.conf), ensure:

<rootcheck>

<enabled>yes</enabled>

<frequency>3600</frequency> <!-- every hour -->

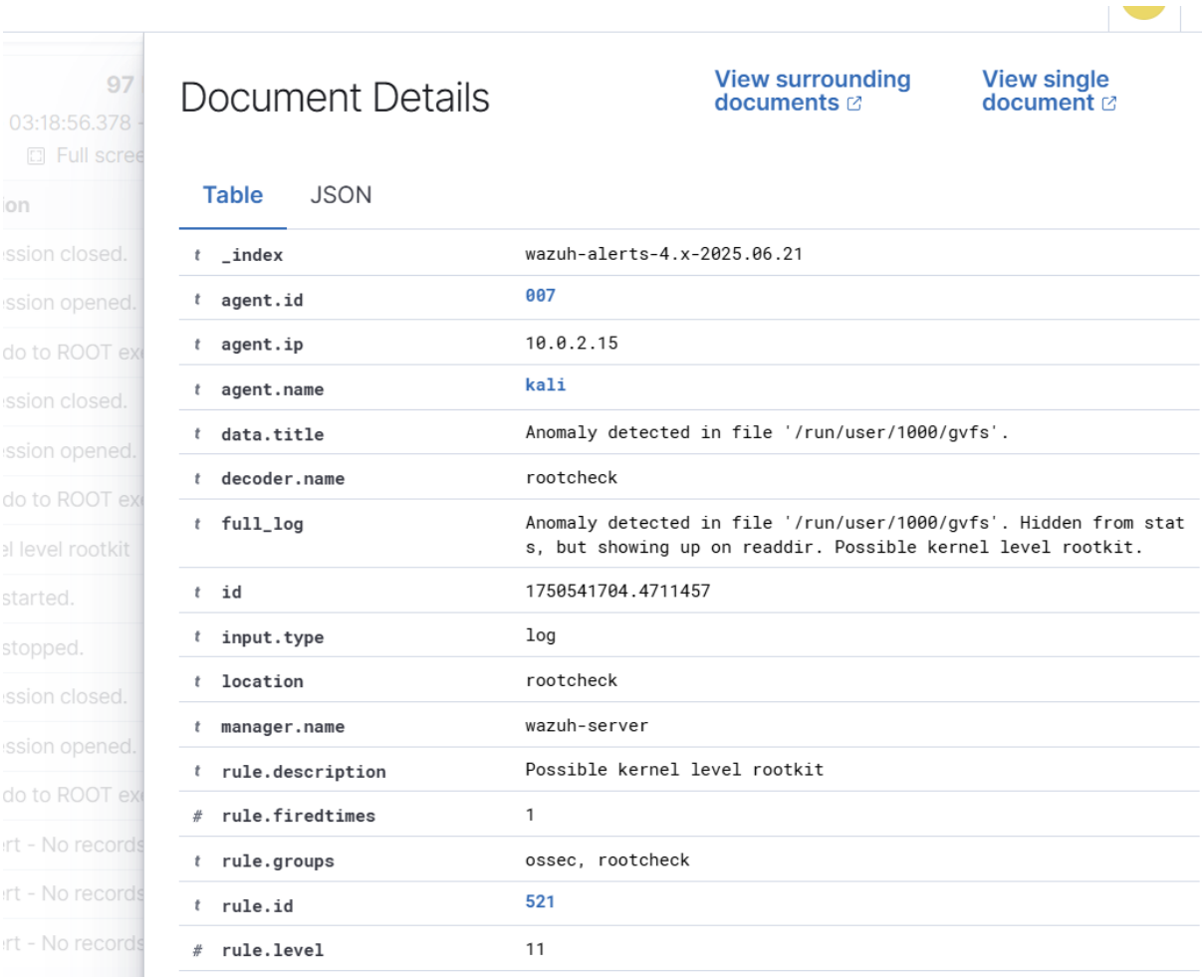
</rootcheck>



B. View Results in Wazuh Dashboard

Go to:

- **Wazuh Dashboard > Modules > Rootcheck**



7. Detect Failed SSH Login Attempts (Brute Force)

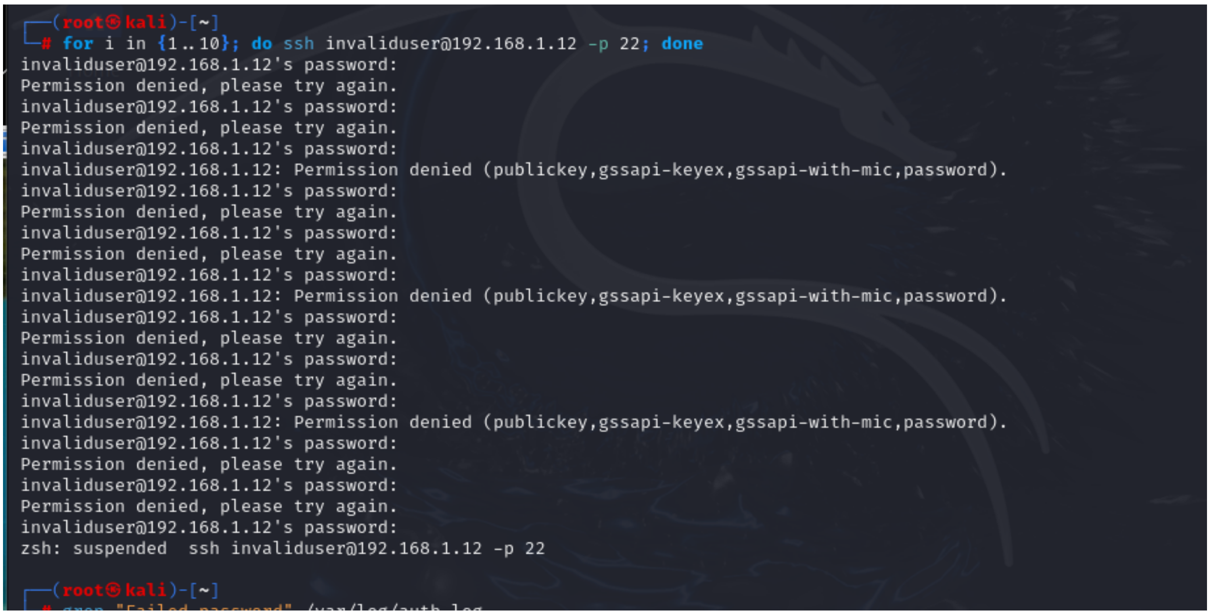
A. Simulate Brute-force SSH Attempts

From any other machine or within the same network:

for i in {1..15}; do

ssh invaliduser@<WAZUH_AGENT_IP> -o StrictHostKeyChecking=no

done



You'll see repeated failed attempts in /var/log/auth.log (Linux), which Wazuh will pick up.

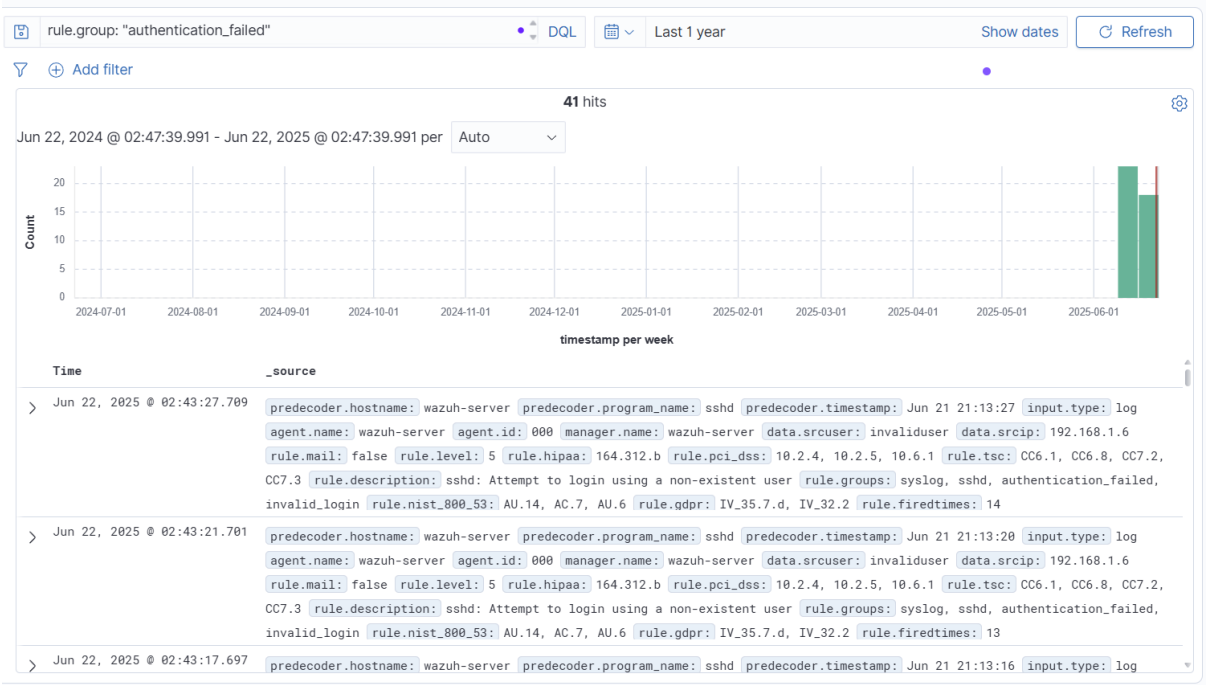
B. View Alerts

Go to:

- **Wazuh Dashboard > Security Events**
- Search: rule.group: "authentication_failed" OR rule.id: 5710 OR rule.id: 5712 OR rule.id: 5715

You'll see alerts like:

- **"sshd: authentication failed"**
- **"Multiple failed SSH login attempts"**



---

8. Active Responses (e.g., IP Blocking)

A. Enable Active Response in ossec.conf

On Wazuh **Manager** (/var/ossec/etc/ossec.conf):

<active-response>

<command>firewalldrop</command>

<location>local</location>

<rules_id>5712</rules_id>

<timeout>600</timeout>

</active-response>

<command>

<name>firewalldrop</name>

<executable>firewalldrop</executable>

<timeout_allowed>yes</timeout_allowed>

</command>

```
</ossec_config>

<ossec_config>
 <active-response>
  <command>firewall-drop</command>
  <location>local</location>
  <rules_id>5712</rules_id> <!-- SSH brute-force rule -->
  <timeout>600</timeout> <!-- Block for 10 minutes -->
 </active-response>

 <command>
  <name>firewall-drop</name>
  <executable>firewall-drop.sh</executable>
  <expect>srcip</expect>
 </command>
</ossec_config>
"/var/ossec/etc/ossec.conf" 367L, 10063B
```

B. Restart Wazuh Agent/Manager

sudo systemctl restart wazuh-manager

sudo systemctl restart wazuh-agent

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

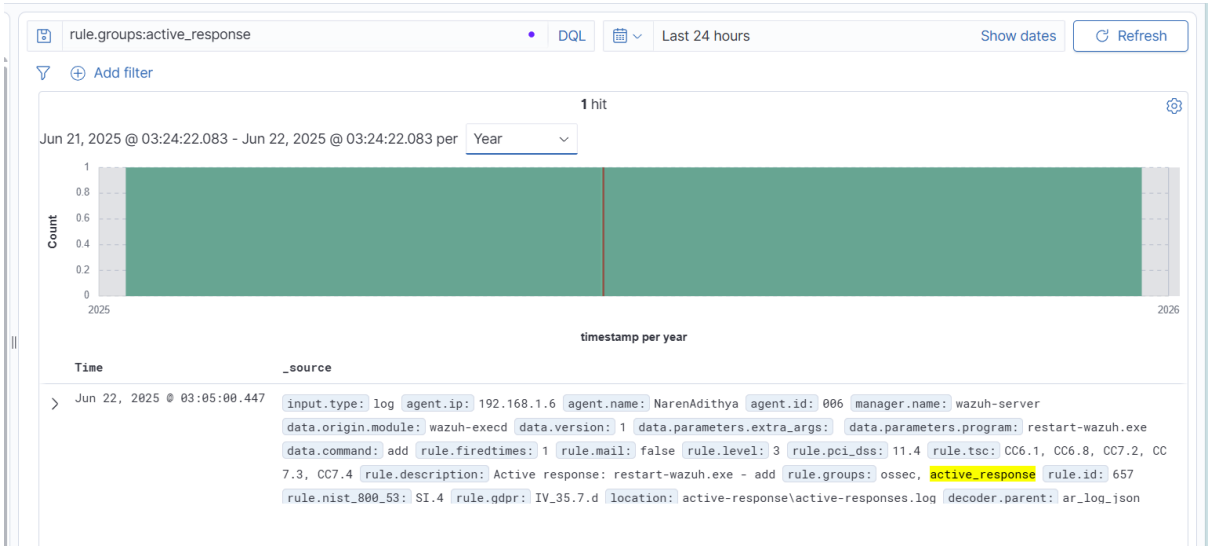
C. Trigger Brute-force Again

Repeat:

for i in {1..15}; do

ssh invaliduser@<WAZUH_AGENT_IP>

done



Configure the Active Response module to block the malicious IP address[Permalink to this headline]

1. Add a custom rule to trigger a Wazuh active response script. Do this in the Wazuh server /var/ossec/etc/rules/local_rules.xml custom ruleset file:

```
<group name="attack,">
  <rule id="100100" level="10">
    <if_group>web|attack|attacks</if_group>
    <list field="srcip" lookup="address_match_key">etc/lists/blacklist-alienvault</list>
    <description>IP address found in AlienVault reputation database.</description>
  </rule>
</group>
```

2. Edit the Wazuh server /var/ossec/etc/ossec.conf configuration file and add the etc/lists/blacklist-alienvault list to the <ruleset> section:

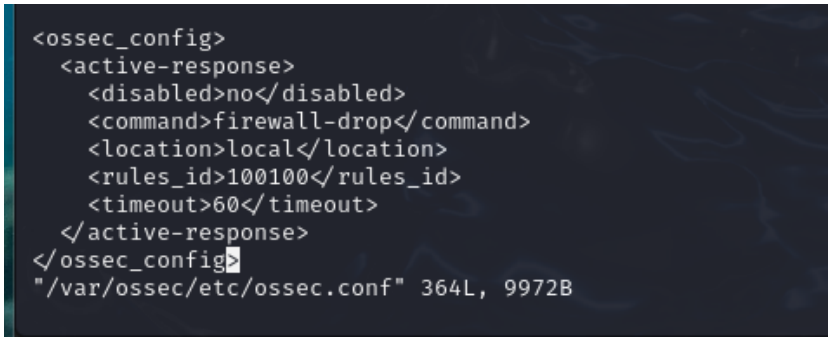
```
<ossec_config>
  <ruleset>
    <!-- Default ruleset -->
    <decoder_dir>ruleset/decoders</decoder_dir>
    <rule_dir>ruleset/rules</rule_dir>
    <rule_exclude>0215-policy_rules.xml</rule_exclude>
    <list>etc/lists/audit-keys</list>
    <list>etc/lists/amazon/aws-eventnames</list>
    <list>etc/lists/security-eventchannel</list>
    <list>etc/lists/blacklist-alienvault</list>

    <!-- User-defined ruleset -->
    <decoder_dir>etc/decoders</decoder_dir>
    <rule_dir>etc/rules</rule_dir>
  </ruleset>

</ossec_config>
```

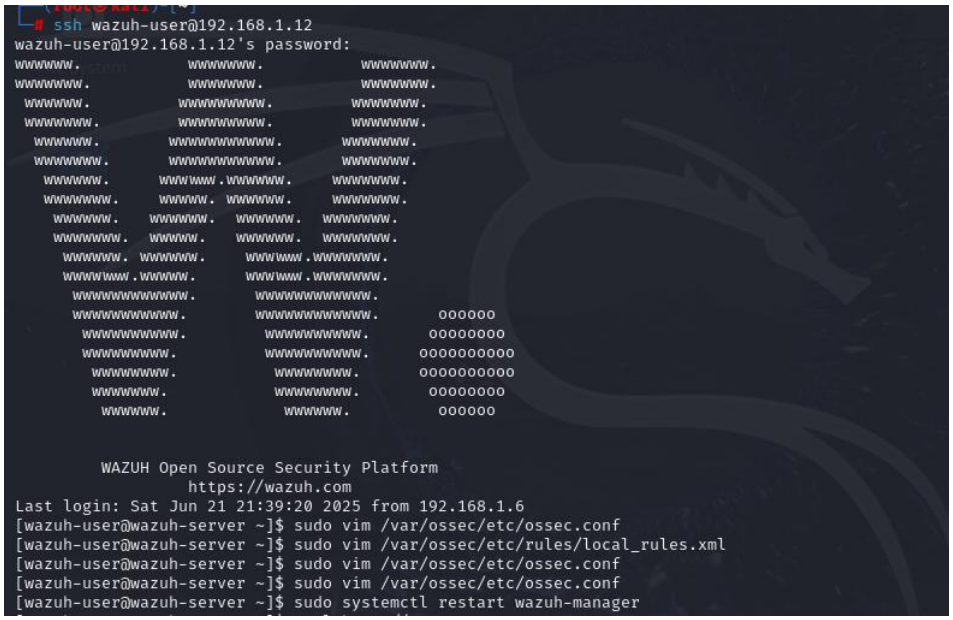
3. Add the Active Response block to the Wazuh server /var/ossec/etc/ossec.conf file:

```
<ossec_config>
  <active-response>
    <disabled>no</disabled>
    <command>firewall-drop</command>
    <location>local</location>
    <rules_id>100100</rules_id>
    <timeout>60</timeout>
  </active-response>
</ossec_config>
```



4. Restart the Wazuh manager to apply the changes:

   $ sudo systemctl restart wazuh-manager



Attack emulation

Access any of the web servers from the RHEL endpoint using the corresponding IP address. Replace <WEBSERVER_IP> with the appropriate value and execute the following command from the attacker endpoint:

$ curl http://<WEBSERVER_IP>

The attacker endpoint connects to the victim's web servers the first time. After the first connection, the Wazuh Active Response module temporarily blocks any successive connection to the web servers for 60 seconds.

Visualize the alerts

You can visualize the alert data in the Wazuh dashboard. To do this, go to the **Threat Hunting** module and add the filters in the search bar to query the alerts.

- Ubuntu - rule.id:(651 OR 100100)