Response to a brute-force attack

Contents

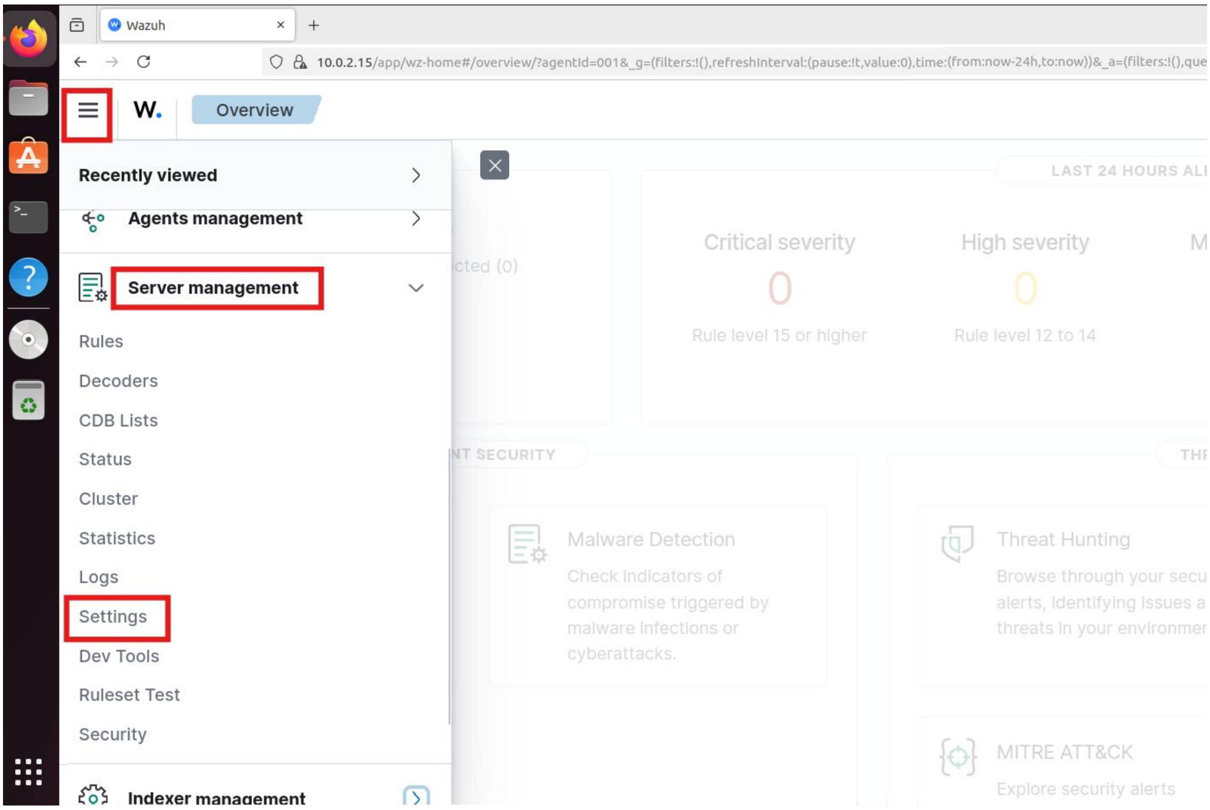
Machines Used:

1. Ubuntu with wazuh installed (Server)
2. Ubuntu with wazuh agent installed (Client)
3. Kali linux (Attacker)

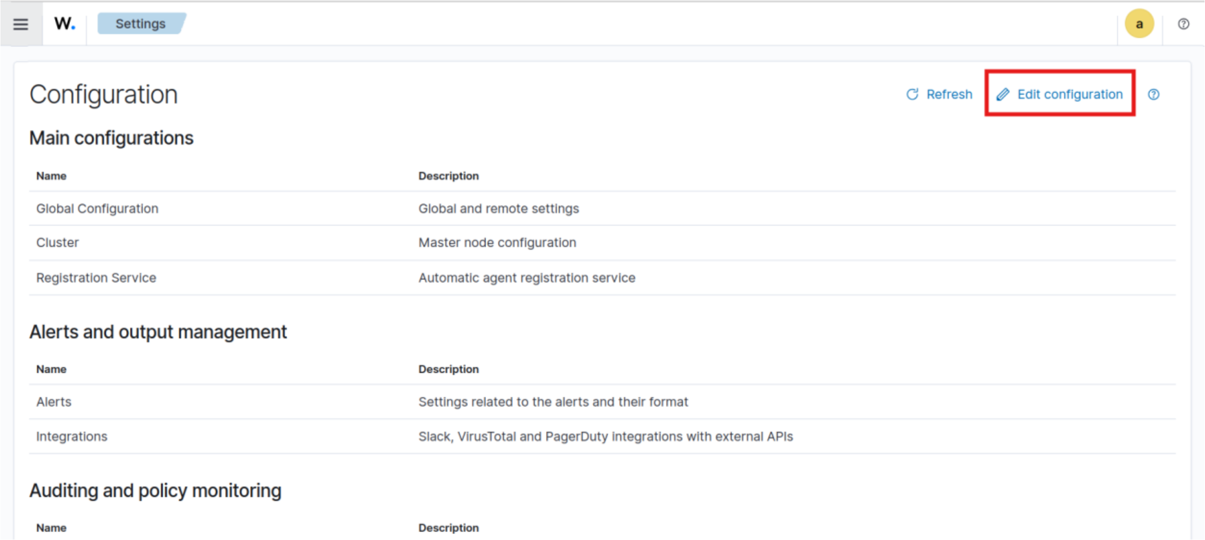
Configuring wazuh Active response capabilities

We are configuring wazuh to drop the brute force requests and block the requests for a certain period.

1. Login to wazuh dashboard.
2. Click on menu -> server management -> settings.



3. Click on edit configuration.



Configuration

Main configurations

Name	Description
Global Configuration	Global and remote settings
Cluster	Master node configuration
Registration Service	Automatic agent registration service

Alerts and output management

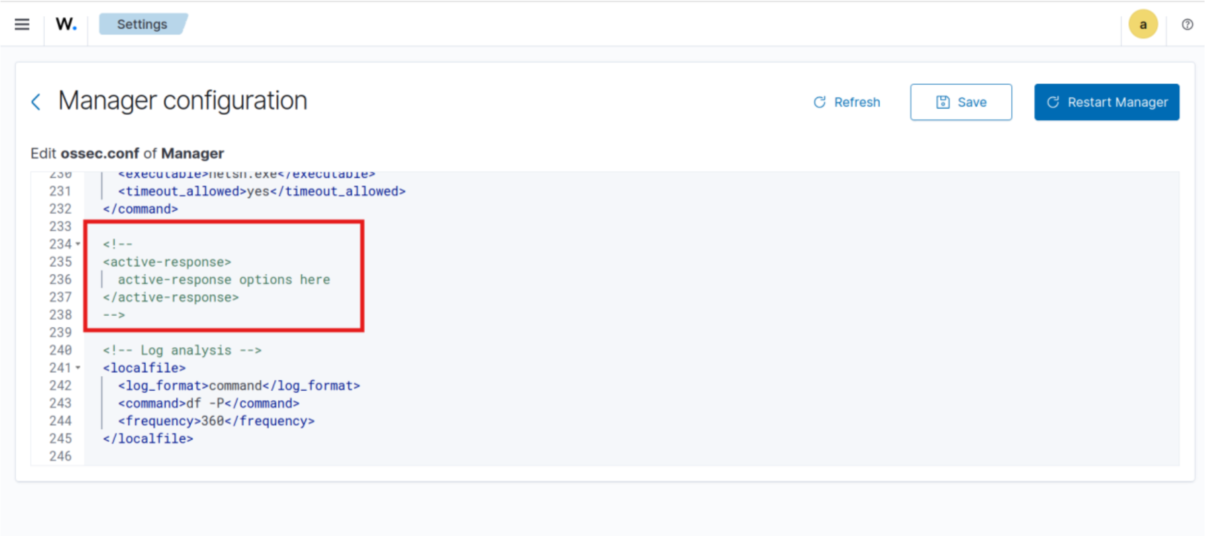
Name	Description
Alerts	Settings related to the alerts and their format
Integrations	Slack, VirusTotal and PagerDuty integrations with external APIs

Auditing and policy monitoring

Name	Description

4. In the manager configuration look for this block

```
<!--
<active-response>
  active-response options here
</active-response>
-->
```



Manager configuration

Edit **ossec.conf** of **Manager**

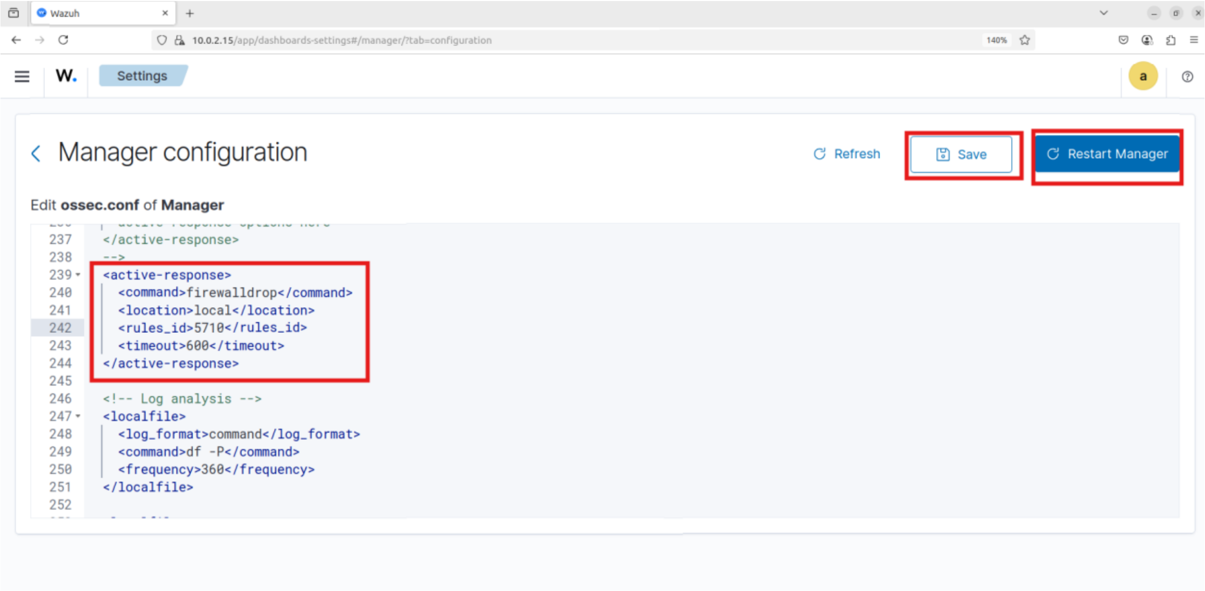
```
  <executable>netsh.exe</executable>
  <timeout_allowed>yes</timeout_allowed>
</command>

<!--
<active-response>
  active-response options here
</active-response>
-->

<!-- Log analysis -->
<localfile>
  <log_format>command</log_format>
  <command>df -P</command>
  <frequency>360</frequency>
</localfile>
```

5. Add this under the above block to configure the active response.

```
<active-response>
  <command>firewall-drop</command>
  <location>local</location>
  <rules_id>5710</rules_id>
  <timeout>600</timeout> <!-- Block IP for 10 minutes -->
</active-response>
```

Rule id 5710: Attempt to login using a non-existent user

6. Click Save and Restart manager.



Edit **ossec.conf** of **Manager**

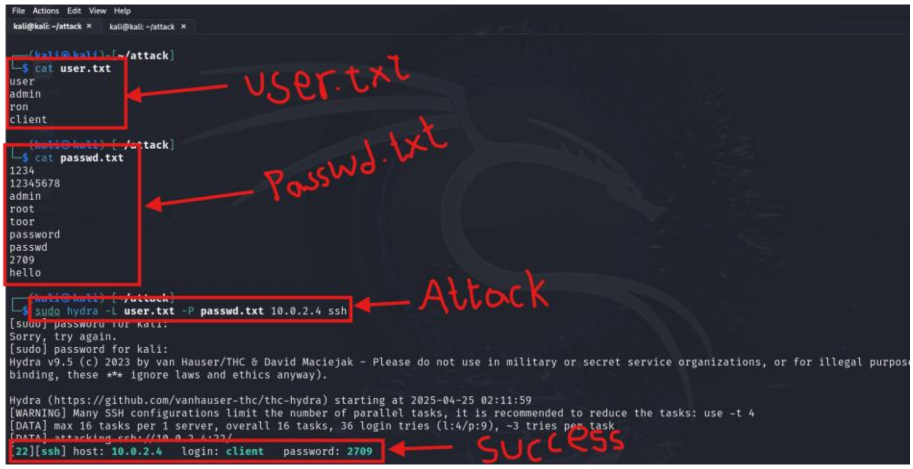
```
</active-response>
-->
<active-response>
  <command>firewalldrop</command>
  <location>local</location>
  <rules_id>5710</rules_id>
  <timeout>600</timeout>
</active-response>

<!-- Log analysis -->
<localfile>
  <log_format>command</log_format>
  <command>df -P</command>
  <frequency>360</frequency>
</localfile>
```

Attack simulation

1. Start the kali machine for attacking.
2. Download or create common usernames and passwords files. Add username and password of the client machine in the respective files.
3. Run the following command to start the attack.

```
sudo hydra -L <USER_LIST.txt> -P <PASSWD_LIST.txt> <IP> ssh
```

The following image shows the usenames and passwords and successful ssh brute force attack.

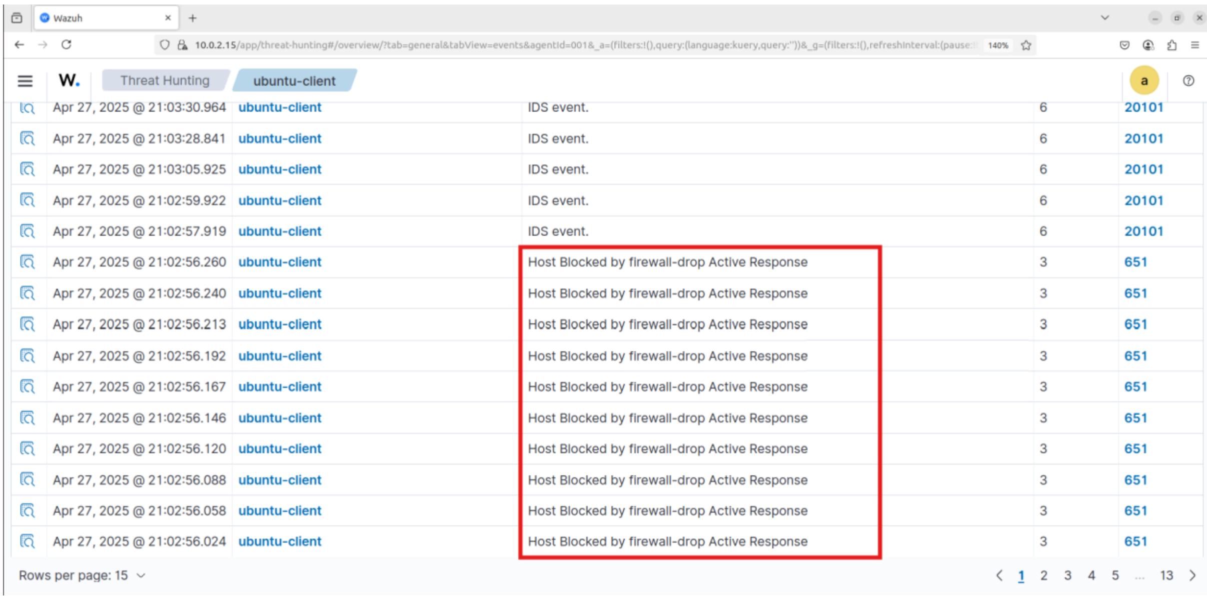


```
┌──(kali㉿kali)-[~/attack]
└─$ cat user.txt
user
admin
ron
client

┌──(kali㉿kali)-[~/attack]
└─$ cat passwd.txt
1234
12345678
admin
root
toor
password
passwd
2709
hello

┌──(kali㉿kali)-[~/attack]
└─$ sudo hydra -L user.txt -P passwd.txt 10.0.2.4 ssh
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purpos
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-04-25 02:11:59
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 36 login tries (l:4/p:9), ~3 tries per task
[DATA] attacking ssh://10.0.2.4:22/
[22][ssh] host: 10.0.2.4   login: client   password: 2709
```

4. Now if you try to login using ssh you cannot be able access for 10 minutes.

Visualization of alerts

To visualize the alerts in wazuh dashboard go to Threat Hunting and following alerts are generated.


Wazuh
10.0.2.15/app/threat-hunting#/overview/?tab=general&tabView=events&agentId=001&_a=(filters:!(),query:(language:kuery,query:''))&_g=(filters:!(),refreshInterval:(pause:
140%
W.
Threat Hunting
ubuntu-client
a

Apr 27, 2025 @ 21:03:30.964	ubuntu-client	IDS event.	6	20101
Apr 27, 2025 @ 21:03:28.841	ubuntu-client	IDS event.	6	20101
Apr 27, 2025 @ 21:03:05.925	ubuntu-client	IDS event.	6	20101
Apr 27, 2025 @ 21:02:59.922	ubuntu-client	IDS event.	6	20101
Apr 27, 2025 @ 21:02:57.919	ubuntu-client	IDS event.	6	20101
Apr 27, 2025 @ 21:02:56.260	ubuntu-client	Host Blocked by firewall-drop Active Response	3	651
Apr 27, 2025 @ 21:02:56.240	ubuntu-client	Host Blocked by firewall-drop Active Response	3	651
Apr 27, 2025 @ 21:02:56.213	ubuntu-client	Host Blocked by firewall-drop Active Response	3	651
Apr 27, 2025 @ 21:02:56.192	ubuntu-client	Host Blocked by firewall-drop Active Response	3	651
Apr 27, 2025 @ 21:02:56.167	ubuntu-client	Host Blocked by firewall-drop Active Response	3	651
Apr 27, 2025 @ 21:02:56.146	ubuntu-client	Host Blocked by firewall-drop Active Response	3	651
Apr 27, 2025 @ 21:02:56.120	ubuntu-client	Host Blocked by firewall-drop Active Response	3	651
Apr 27, 2025 @ 21:02:56.088	ubuntu-client	Host Blocked by firewall-drop Active Response	3	651
Apr 27, 2025 @ 21:02:56.058	ubuntu-client	Host Blocked by firewall-drop Active Response	3	651
Apr 27, 2025 @ 21:02:56.024	ubuntu-client	Host Blocked by firewall-drop Active Response	3	651

References

- https://documentation.wazuh.com/current/user-manual/capabilities/active-response/index.html