Detection & Response to RDP brute-force attack

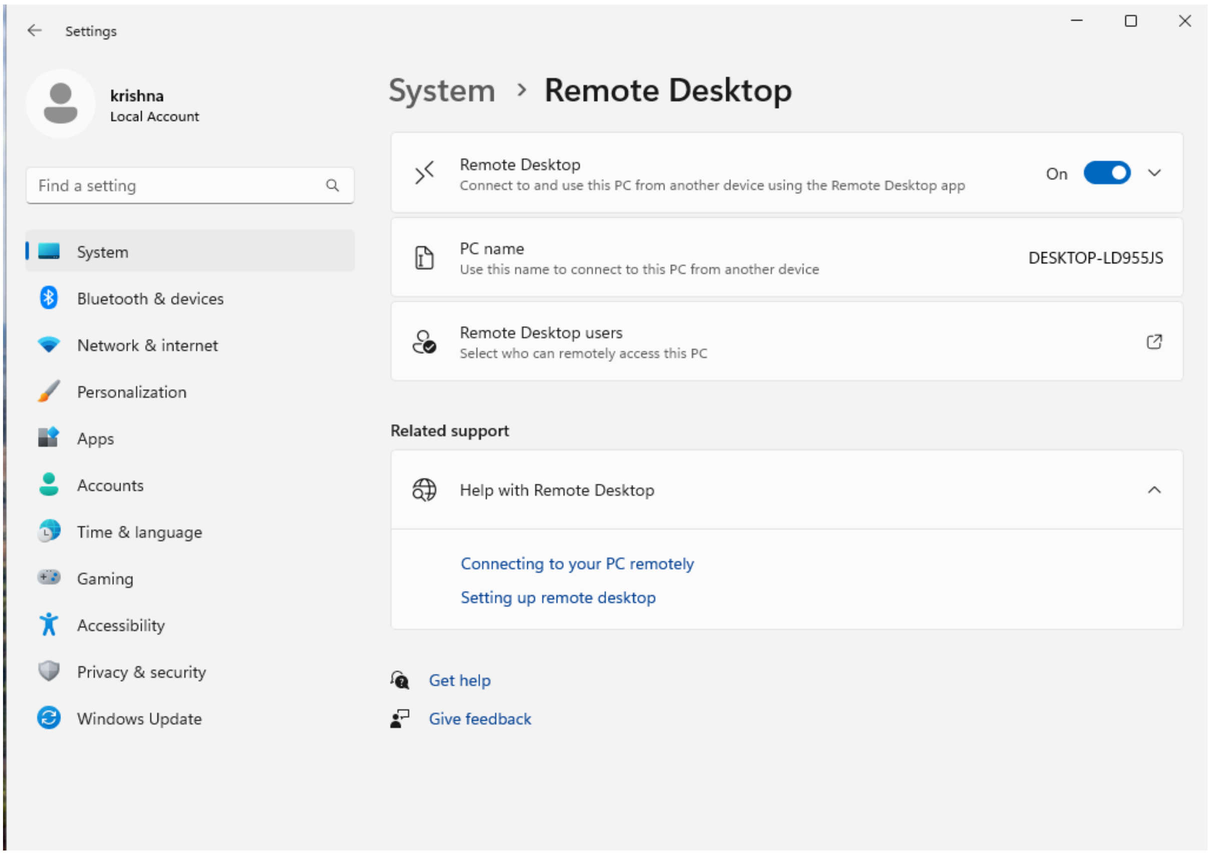
Contents

Machines Used:

1. Ubuntu with wazuh 4.10 installed (Server)
2. Windows 11 Enterprise with wazuh agent installed (Client)
3. Kali linux (Attacker)

Setting up Remote Desktop (RDP)

1. Open settings -> remote desktop -> Toggle on -> Enable.



System > Remote Desktop

Remote Desktop
Connect to and use this PC from another device using the Remote Desktop app
On

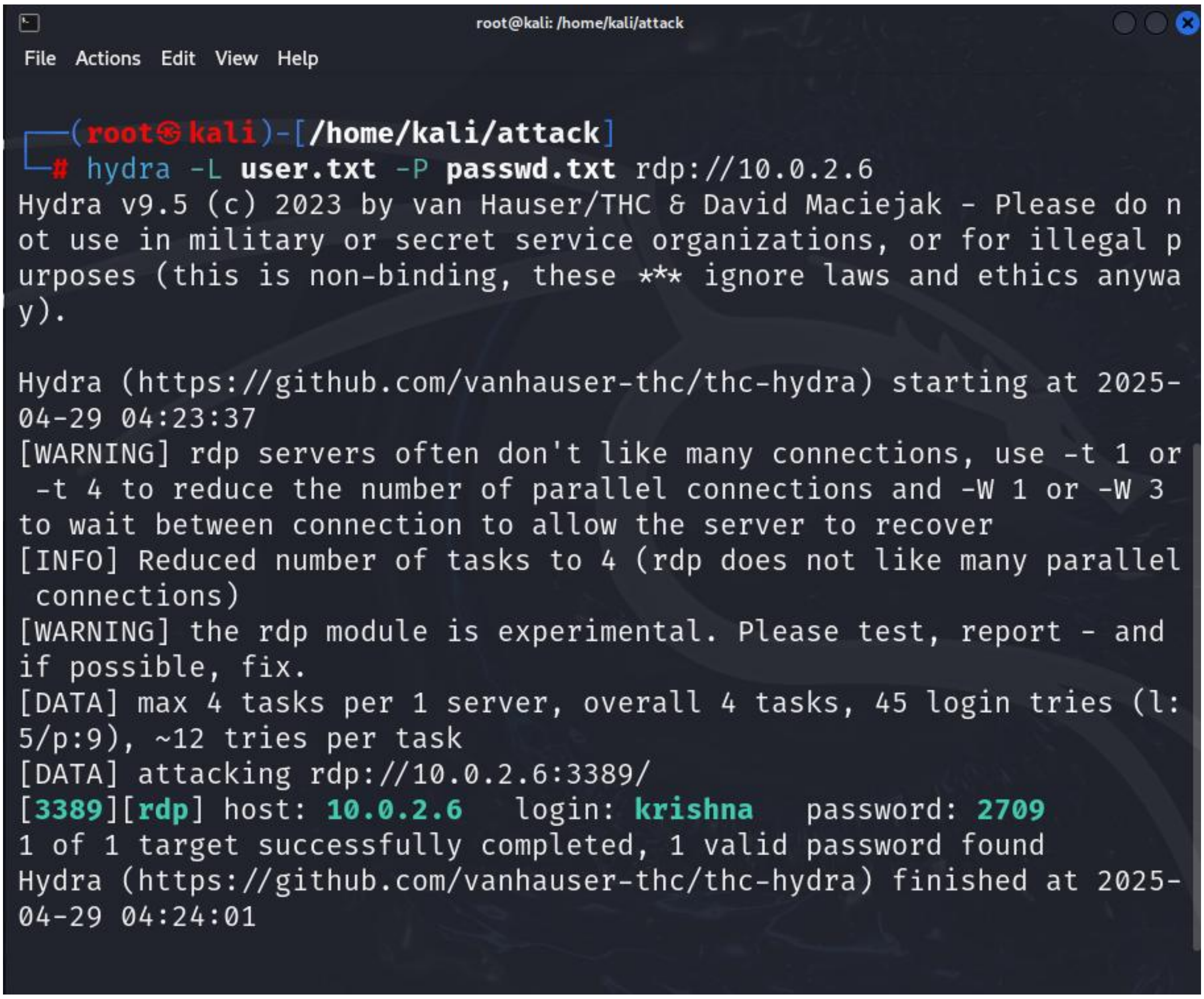
PC name
Use this name to connect to this PC from another device
DESKTOP-LD955JS

Remote Desktop users
Select who can remotely access this PC

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> rdp://<WINDOWS_IP>
```

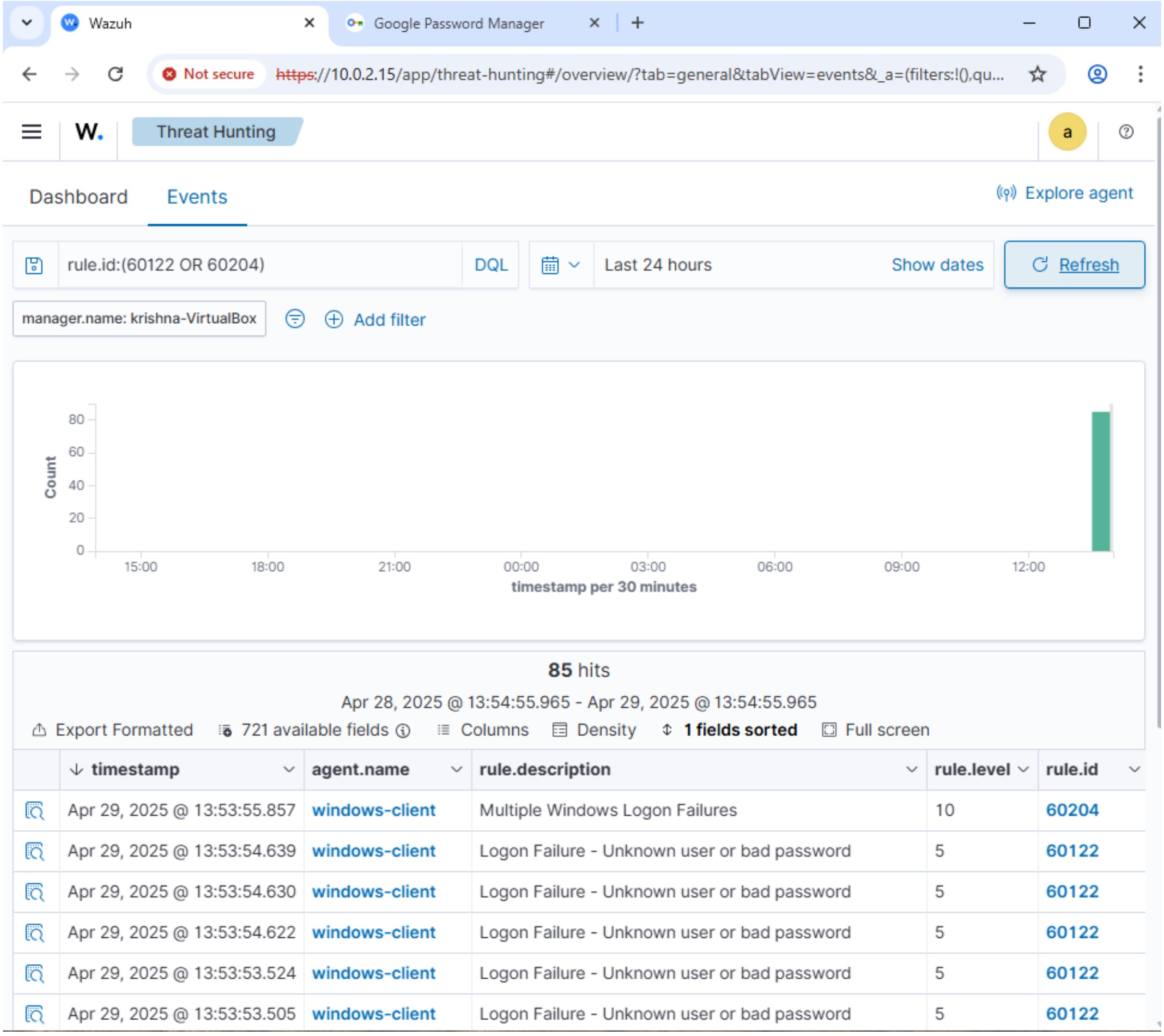


```
┌──(root㉿kali)-[/home/kali/attack]
└─# hydra -L user.txt -P passwd.txt rdp://10.0.2.6
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do n
ot use in military or secret service organizations, or for illegal p
urposes (this is non-binding, these *** ignore laws and ethics anywa
y).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-
04-29 04:23:37
[WARNING] rdp servers often don't like many connections, use -t 1 or
 -t 4 to reduce the number of parallel connections and -W 1 or -W 3
to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel
 connections)
[WARNING] the rdp module is experimental. Please test, report - and
if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 45 login tries (l:
5/p:9), ~12 tries per task
[DATA] attacking rdp://10.0.2.6:3389/
[3389][rdp] host: 10.0.2.6   login: krishna   password: 2709
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-
04-29 04:24:01
```

Visualization of alerts

To visualize the alerts in wazuh dashboard go to Threat Hunting and search the following filter in the search bar.

```
rule.id:(60122 OR 60204)
```



rule.id:(60122 OR 60204)

Last 24 hours

manager.name: krishna-VirtualBox

85 hits

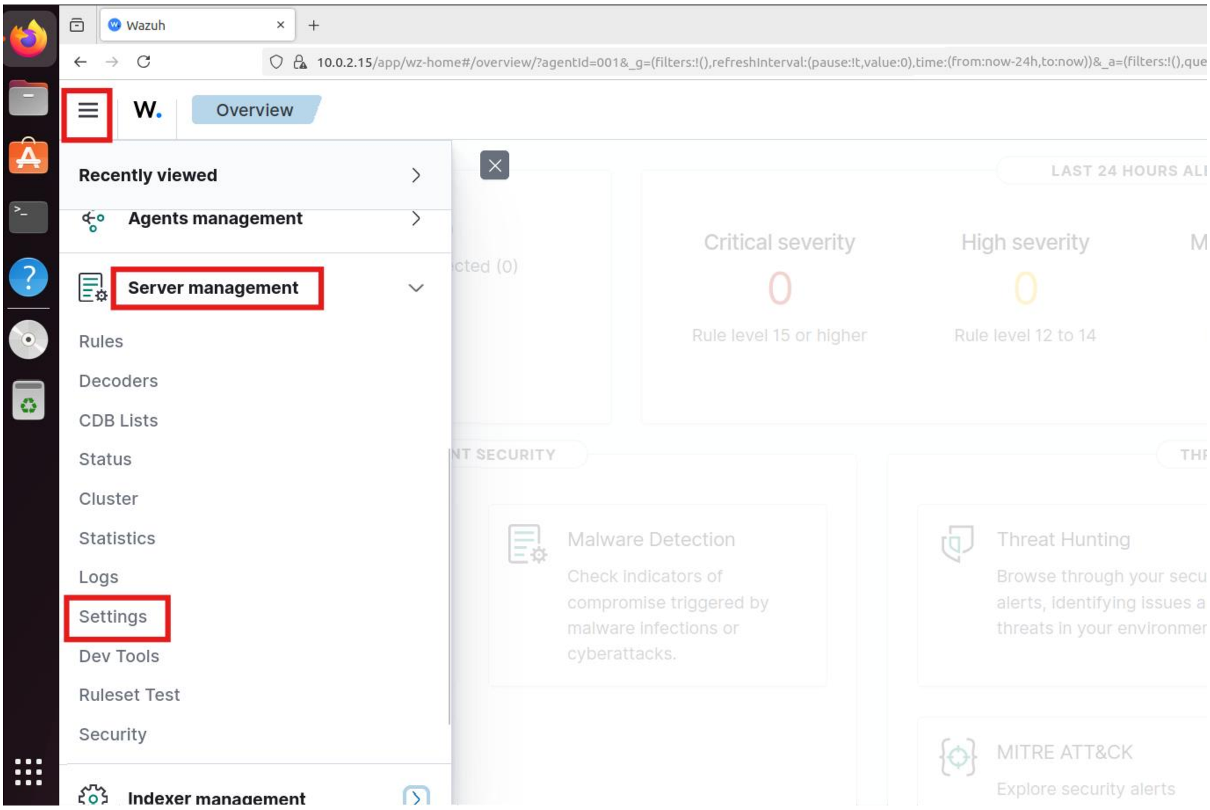
Apr 28, 2025 @ 13:54:55.965 - Apr 29, 2025 @ 13:54:55.965

timestamp	agent.name	rule.description	rule.level	rule.id
Apr 29, 2025 @ 13:53:55.857	windows-client	Multiple Windows Logon Failures	10	60204
Apr 29, 2025 @ 13:53:54.639	windows-client	Logon Failure - Unknown user or bad password	5	60122
Apr 29, 2025 @ 13:53:54.630	windows-client	Logon Failure - Unknown user or bad password	5	60122
Apr 29, 2025 @ 13:53:54.622	windows-client	Logon Failure - Unknown user or bad password	5	60122
Apr 29, 2025 @ 13:53:53.524	windows-client	Logon Failure - Unknown user or bad password	5	60122
Apr 29, 2025 @ 13:53:53.505	windows-client	Logon Failure - Unknown user or bad password	5	60122

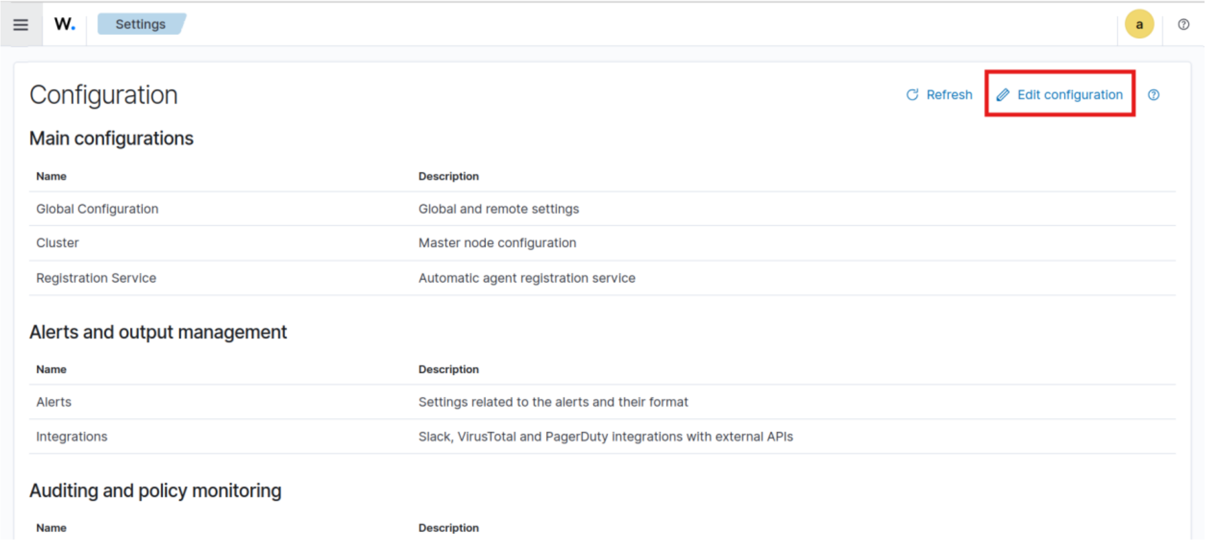
Configuring wazuh Active response capabilities

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

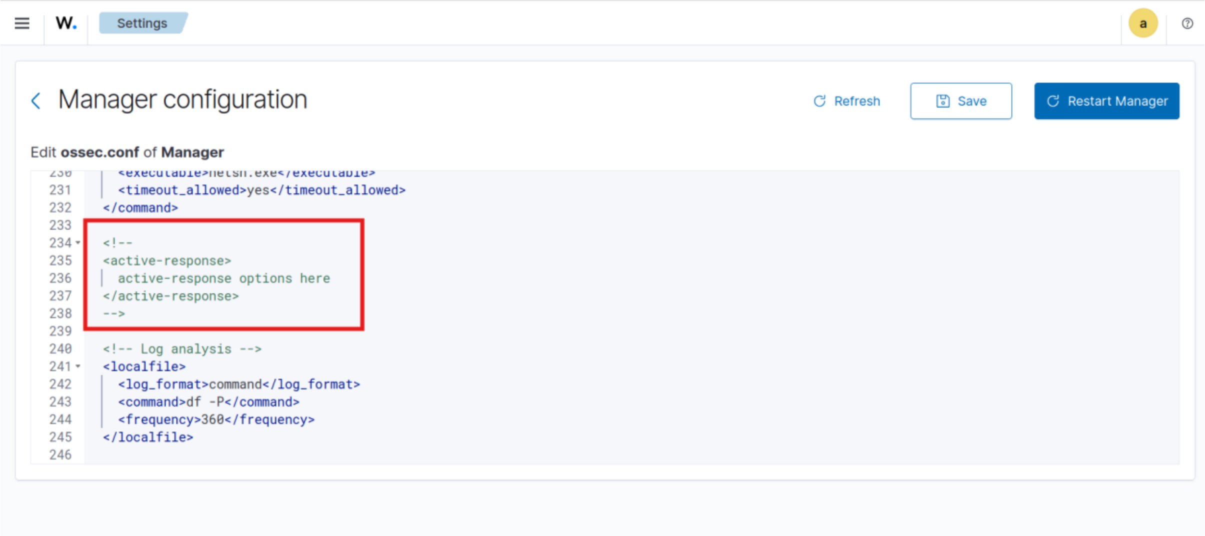
Name	Description
Alerts	Settings related to the alerts and their format
Integrations	Slack, VirusTotal and PagerDuty integrations with external APIs

Auditing and policy monitoring

Name	Description

4. In the manager configuration look for this block

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



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

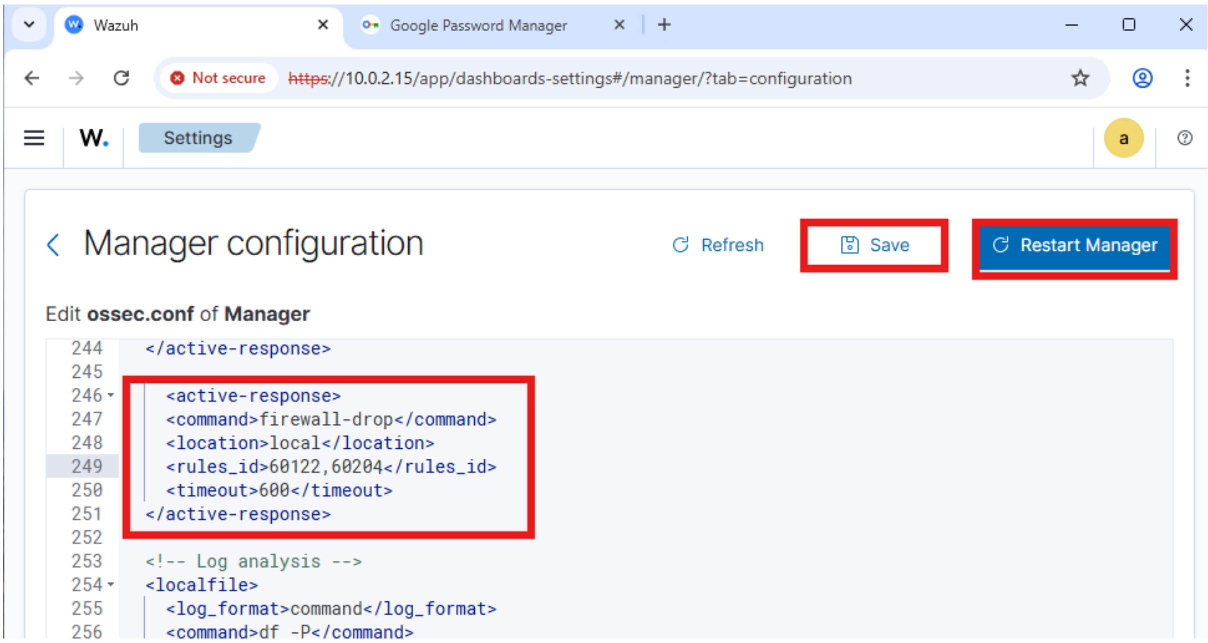
```
    <executable>netsh.exe</executable>
    <timeout_allowed>yes</timeout_allowed>
  </command>

  <!--
  <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>server</location>
  <rules_id>60122,60204</rules_id>
  <timeout>600</timeout> <!-- Block IP for 10 minutes -->
</active-response>
```

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

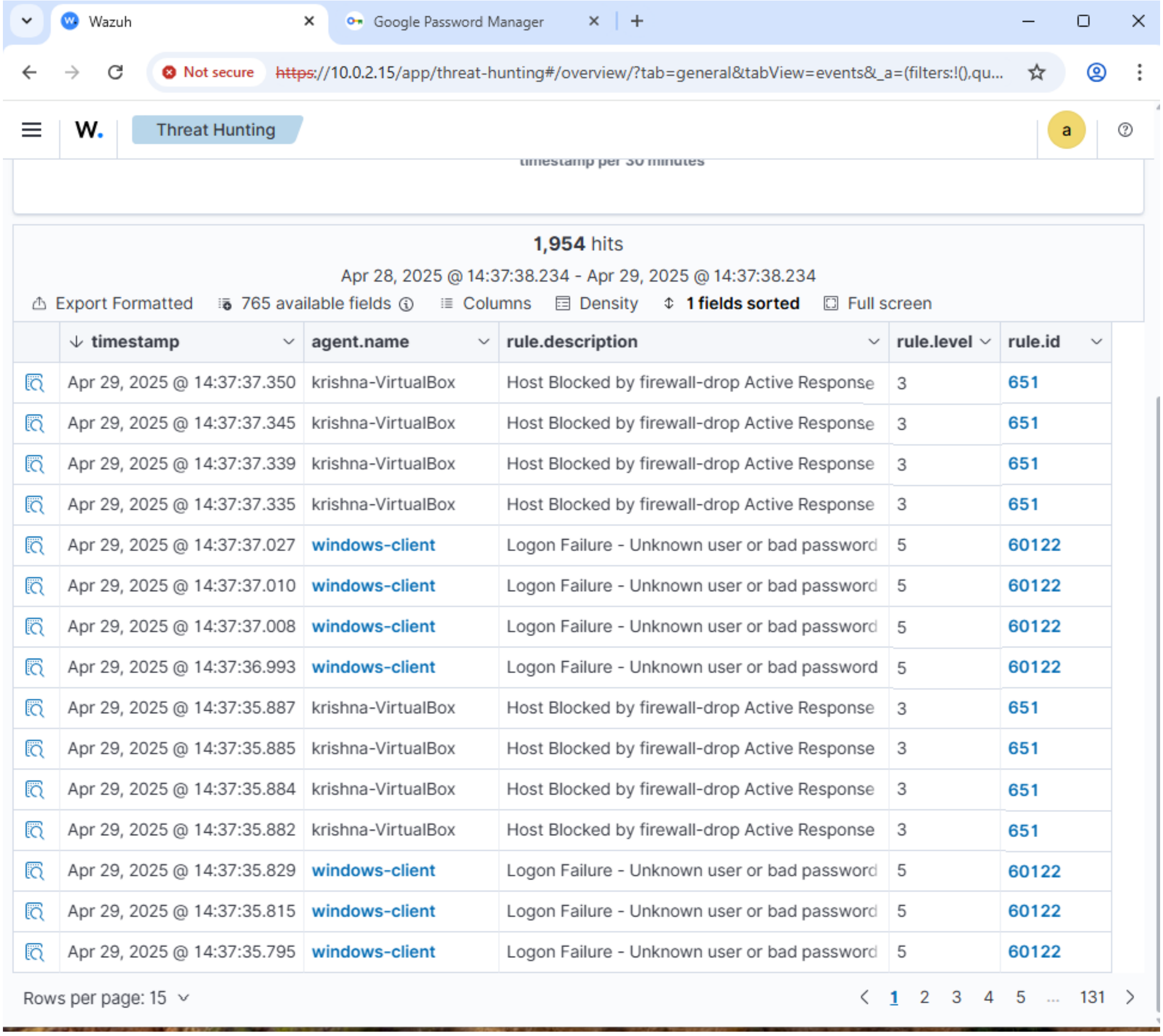
6. Click Save and Restart manager.



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

```
  </active-response>

    <active-response>
    <command>firewall-drop</command>
    <location>local</location>
    <rules_id>60122,60204</rules_id>
    <timeout>600</timeout>
  </active-response>

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

Now perform the attack again and visualize the alerts again.



Wazuh
Google Password Manager
Not secure
https://10.0.2.15/app/threat-hunting#/overview/?tab=general&tabView=events&_a=(filters:!(),qu...
W.
Threat Hunting
a
timestamp per 30 minutes

1,954 hits

Apr 28, 2025 @ 14:37:38.234 - Apr 29, 2025 @ 14:37:38.234

Export Formatted · 765 available fields · Columns · Density · 1 fields sorted · Full screen

timestamp	agent.name	rule.description	rule.level	rule.id
Apr 29, 2025 @ 14:37:37.350	krishna-VirtualBox	Host Blocked by firewall-drop Active Response	3	651
Apr 29, 2025 @ 14:37:37.345	krishna-VirtualBox	Host Blocked by firewall-drop Active Response	3	651
Apr 29, 2025 @ 14:37:37.339	krishna-VirtualBox	Host Blocked by firewall-drop Active Response	3	651
Apr 29, 2025 @ 14:37:37.335	krishna-VirtualBox	Host Blocked by firewall-drop Active Response	3	651
Apr 29, 2025 @ 14:37:37.027	windows-client	Logon Failure - Unknown user or bad password	5	60122
Apr 29, 2025 @ 14:37:37.010	windows-client	Logon Failure - Unknown user or bad password	5	60122
Apr 29, 2025 @ 14:37:37.008	windows-client	Logon Failure - Unknown user or bad password	5	60122
Apr 29, 2025 @ 14:37:36.993	windows-client	Logon Failure - Unknown user or bad password	5	60122
Apr 29, 2025 @ 14:37:35.887	krishna-VirtualBox	Host Blocked by firewall-drop Active Response	3	651
Apr 29, 2025 @ 14:37:35.885	krishna-VirtualBox	Host Blocked by firewall-drop Active Response	3	651
Apr 29, 2025 @ 14:37:35.884	krishna-VirtualBox	Host Blocked by firewall-drop Active Response	3	651
Apr 29, 2025 @ 14:37:35.882	krishna-VirtualBox	Host Blocked by firewall-drop Active Response	3	651
Apr 29, 2025 @ 14:37:35.829	windows-client	Logon Failure - Unknown user or bad password	5	60122
Apr 29, 2025 @ 14:37:35.815	windows-client	Logon Failure - Unknown user or bad password	5	60122
Apr 29, 2025 @ 14:37:35.795	windows-client	Logon Failure - Unknown user or bad password	5	60122

Rows per page: 15 · < 1 2 3 4 5 ... 131 >

References

- https://documentation.wazuh.com/current/proof-of-concept-guide/detect-brute-force-attack.html
- https://documentation.wazuh.com/current/user-manual/capabilities/active-response/index.html