Detecting a brute-force attack

Contents

Configuration for monitoring Auth log files

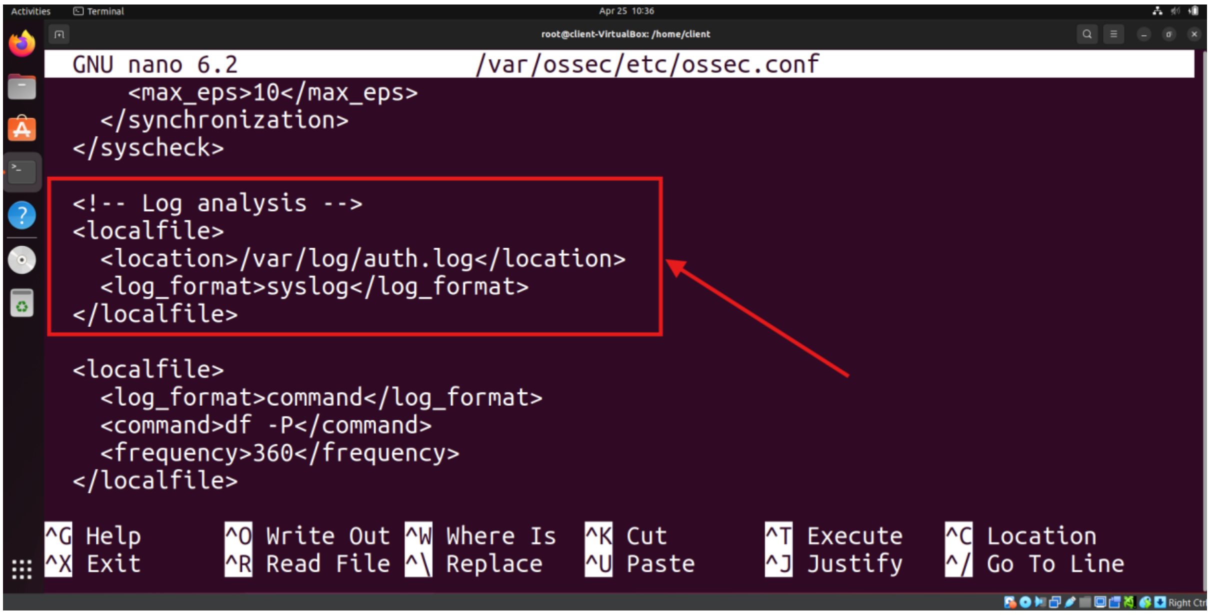
To monitor auth logs of a client configure the Wazuh agent ossec.conf file on linux(ubuntu) endpoint

1. Edit Wazuh agent configuration file.

```
sudo nano /var/ossec/etc/ossec.conf
```

2. Add the following lines in between <ossec_config> tags in config file.

```
<localfile>
  <location>/var/log/auth.log</location>
  <log_format>syslog</log_format>
</localfile>
```



```
  GNU nano 6.2                    /var/ossec/etc/ossec.conf
      <max_eps>10</max_eps>
    </synchronization>
  </syscheck>

  <!-- Log analysis -->
  <localfile>
    <location>/var/log/auth.log</location>
    <log_format>syslog</log_format>
  </localfile>

  <localfile>
    <log_format>command</log_format>
    <command>df -P</command>
    <frequency>360</frequency>
  </localfile>

^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line
```

3. Restart the Wazuh agent.

```
sudo systemctl restart wazuh-agent
```

Setting up ssh server

Install and setup ssh server on the client machine.

1. Installing openssh using apt.

```
sudo apt install openssh-server
```

2. Enable and start the ssh.

```
sudo systemctl enable ssh
sudo systemctl start ssh
```

3. Go to attacker machine and check ssh is working.

```
ssh user@ip
```

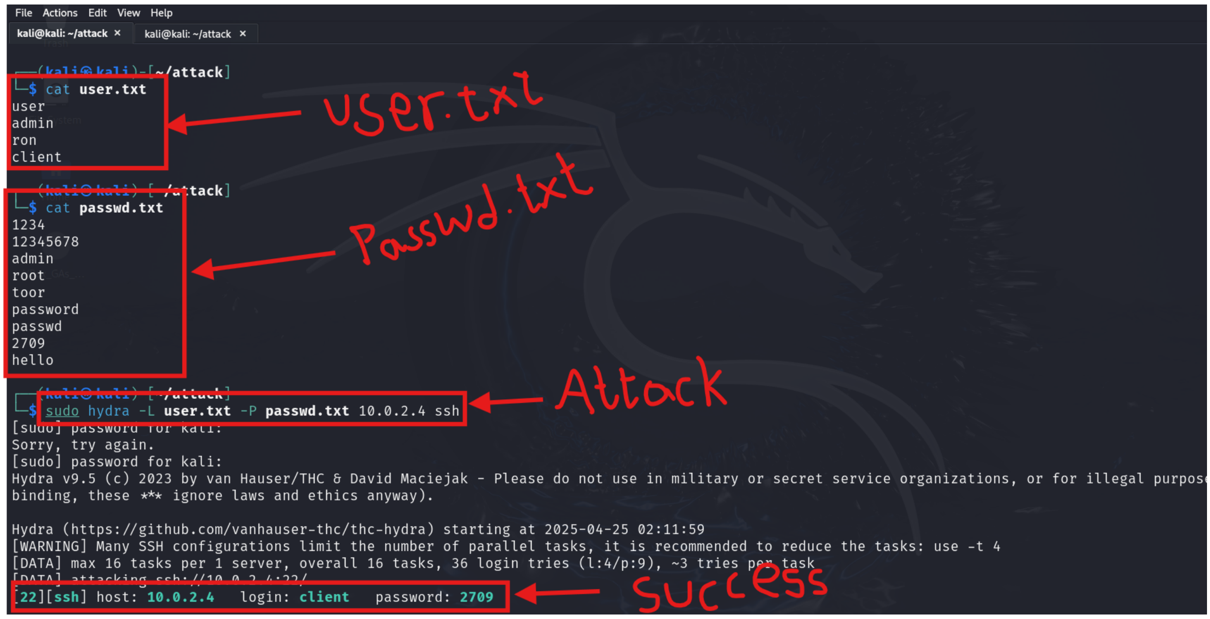
Accept the fingerprint and enter password.

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 purpose
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
```

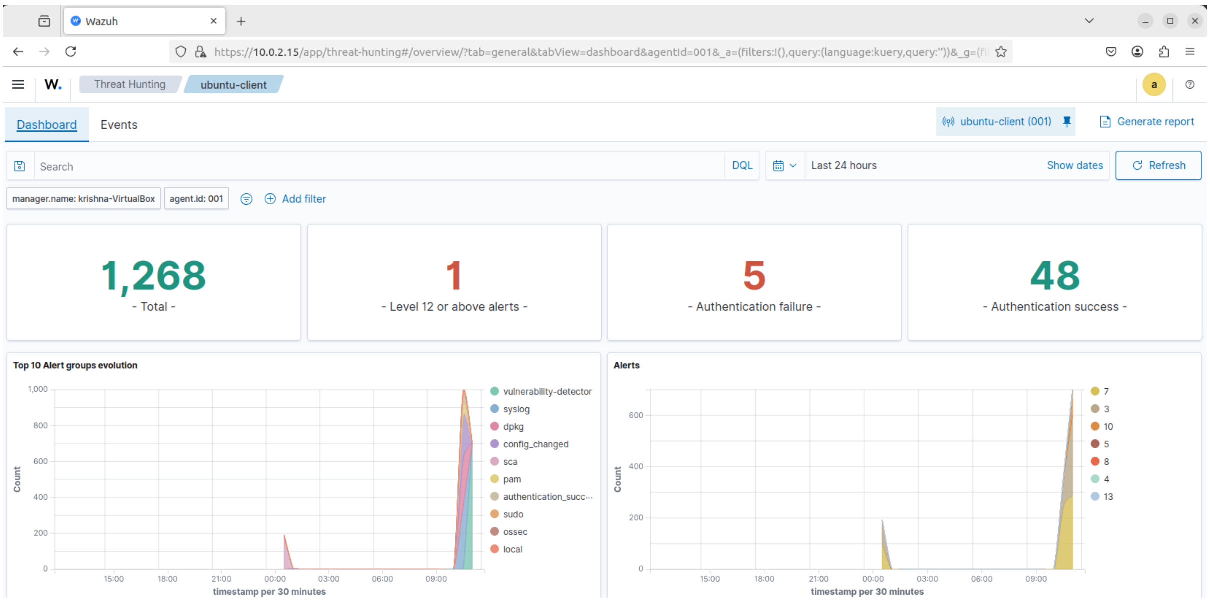
user.txt

Passwd.txt

Attack

success

This is the screenshot of wazuh dashboard before attack which shows 5 authentication failures.



Wazuh
https://10.0.2.15/app/threat-hunting#/overview/?tab=general&tabView=dashboard&agentId=001&_a=(filters:!(),query:(language:kuery,query:''))&_g=(fil
W.
Threat Hunting
ubuntu-client
a
Dashboard
Events
ubuntu-client (001)
Generate report
Search
DQL
Last 24 hours
Show dates
Refresh
manager.name: krishna-VirtualBox
agent.id: 001
Add filter

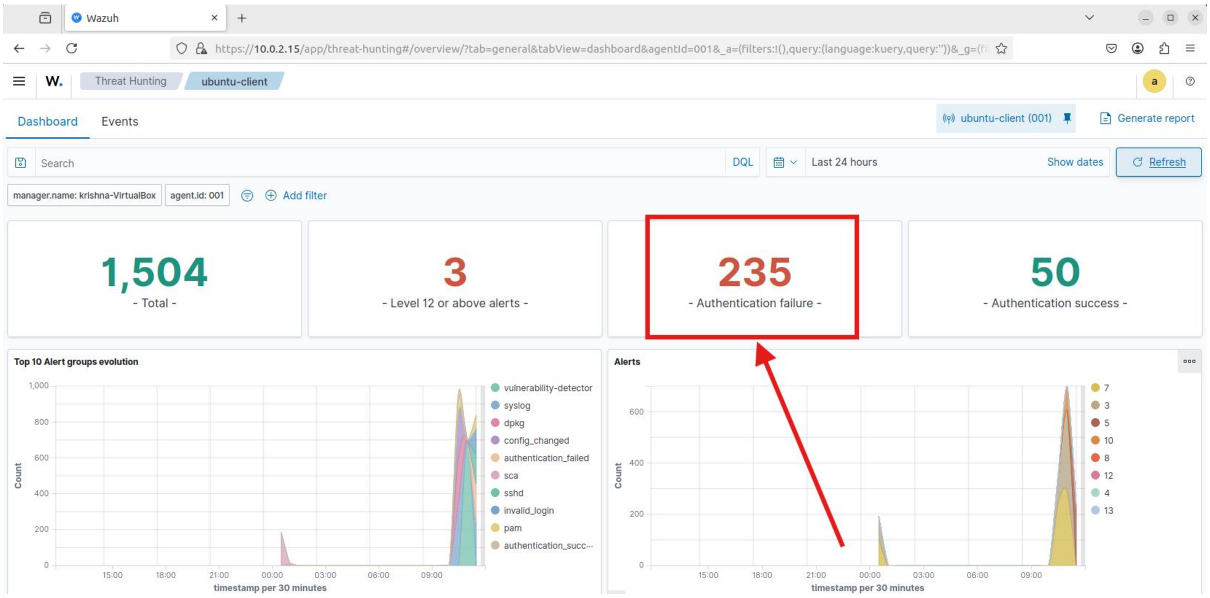
1,268
- Total -

1
- Level 12 or above alerts -

5
- Authentication failure -

48
- Authentication success -

This is the screenshot of wazuh dashboard before attack which shows 235 authentication failures.

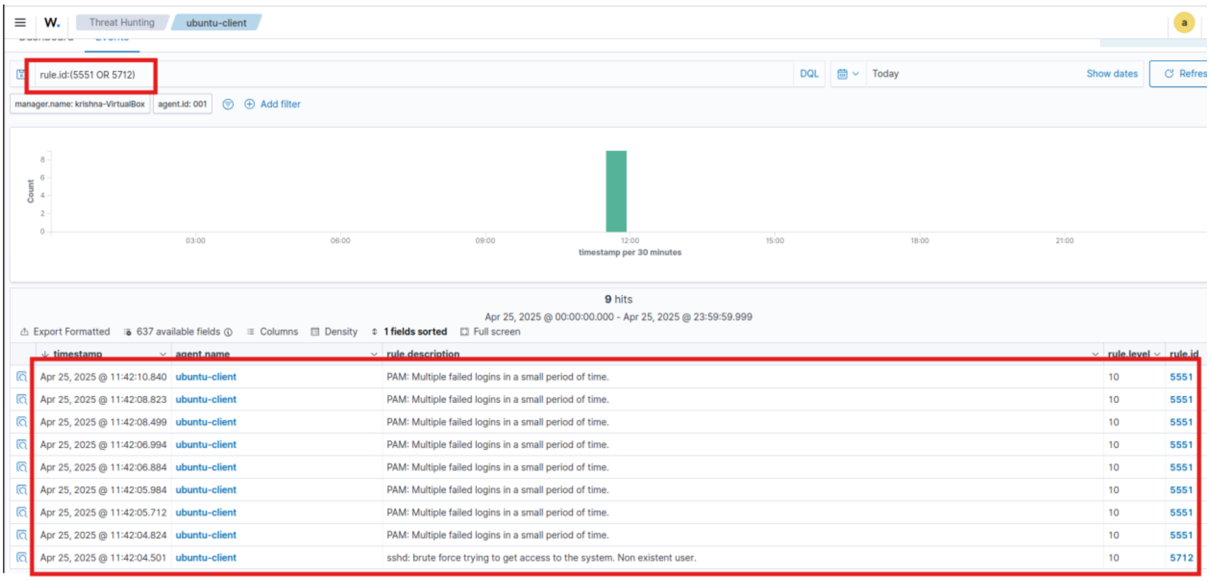


Visualization of alerts

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

```
rule.id:(5551 OR 5712)
```

we ca also search other login related rules are 5710, 5711, 5716, 5720, 5503, 5504.



rule.id:(5551 OR 5712)

manager.name: krishna-VirtualBox | agent.id: 001

9 hits

Apr 25, 2025 @ 00:00:00.000 - Apr 25, 2025 @ 23:59:59.999

timestamp	agent.name	rule.description	rule.level	rule.id
Apr 25, 2025 @ 11:42:10.840	ubuntu-client	PAM: Multiple failed logins in a small period of time.	10	5551
Apr 25, 2025 @ 11:42:08.823	ubuntu-client	PAM: Multiple failed logins in a small period of time.	10	5551
Apr 25, 2025 @ 11:42:08.499	ubuntu-client	PAM: Multiple failed logins in a small period of time.	10	5551
Apr 25, 2025 @ 11:42:06.994	ubuntu-client	PAM: Multiple failed logins in a small period of time.	10	5551
Apr 25, 2025 @ 11:42:06.884	ubuntu-client	PAM: Multiple failed logins in a small period of time.	10	5551
Apr 25, 2025 @ 11:42:05.984	ubuntu-client	PAM: Multiple failed logins in a small period of time.	10	5551
Apr 25, 2025 @ 11:42:05.712	ubuntu-client	PAM: Multiple failed logins in a small period of time.	10	5551
Apr 25, 2025 @ 11:42:04.824	ubuntu-client	PAM: Multiple failed logins in a small period of time.	10	5551
Apr 25, 2025 @ 11:42:04.501	ubuntu-client	sshd: brute force trying to get access to the system. Non existent user.	10	5712

References

- https://documentation.wazuh.com/current/user-manual/capabilities/log-data-collection/monitoring-log-files.html
- https://documentation.wazuh.com/current/proof-of-concept-guide/detect-brute-force-attack.html