

Detecting a brute-force attack

Contents

Configuration for monitoring Auth log files	1
Setting up ssh server	2
Attack simulation	2
Visualization of alerts	4
References.....	4

Machines Used:

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

Configuration for monitoring Auth log files

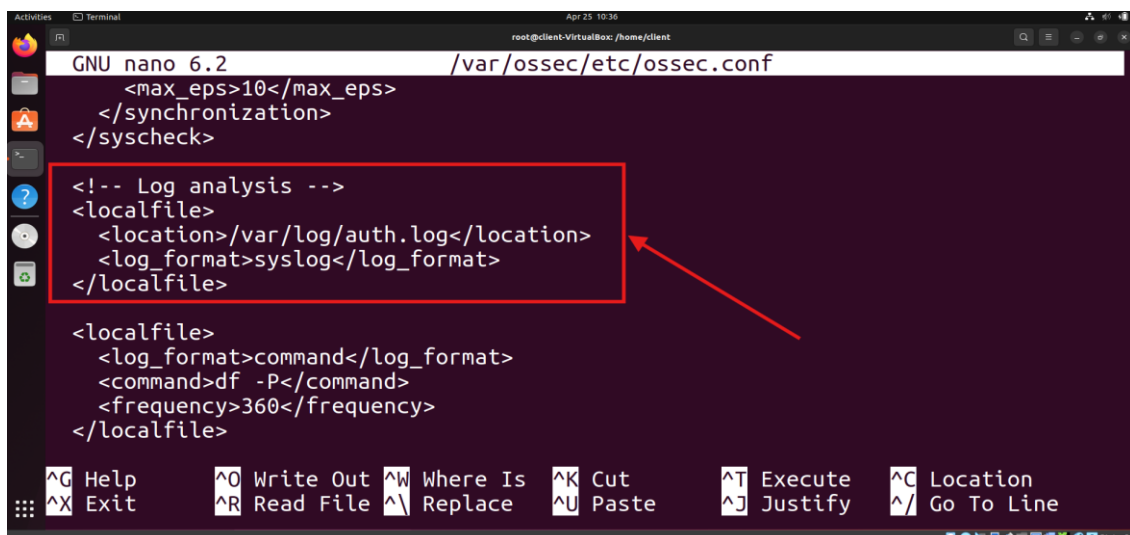
To monitor auth logs of a client configure the Wazuh agent ossec.conf file on linux(ubuntu) endpoint

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>
```

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
```

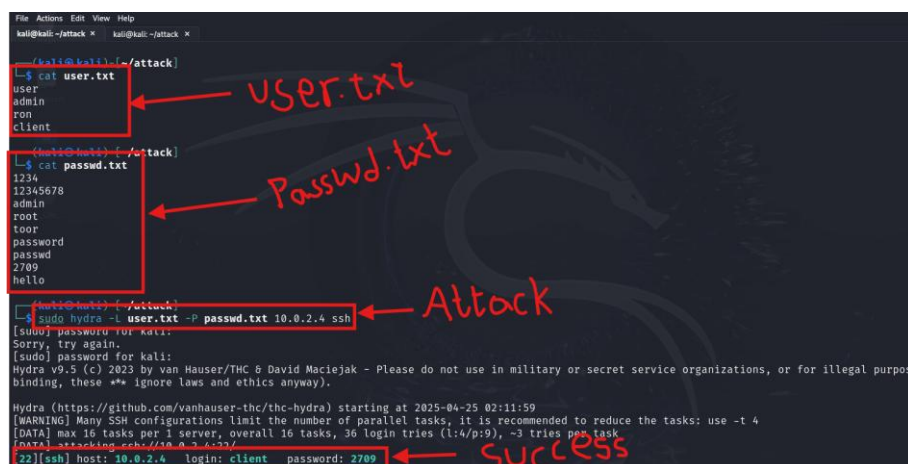
Accept the fingerprint and enter password.

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 usernames and passwords and successful ssh brute force attack.

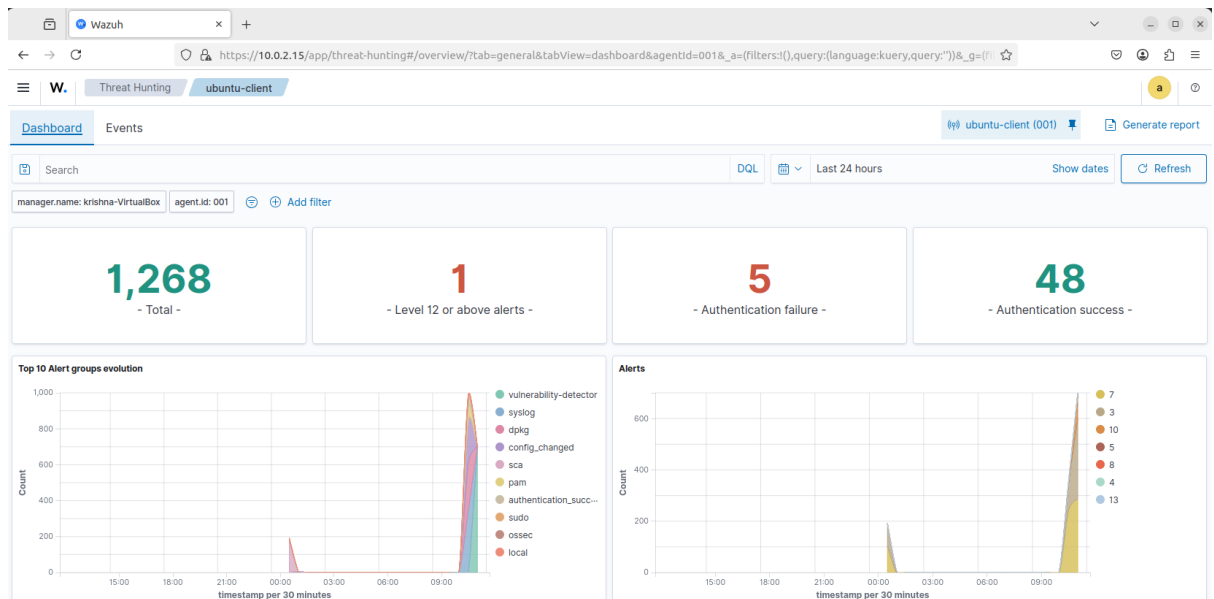


The screenshot shows a Kali Linux terminal with three red boxes and arrows highlighting key steps:

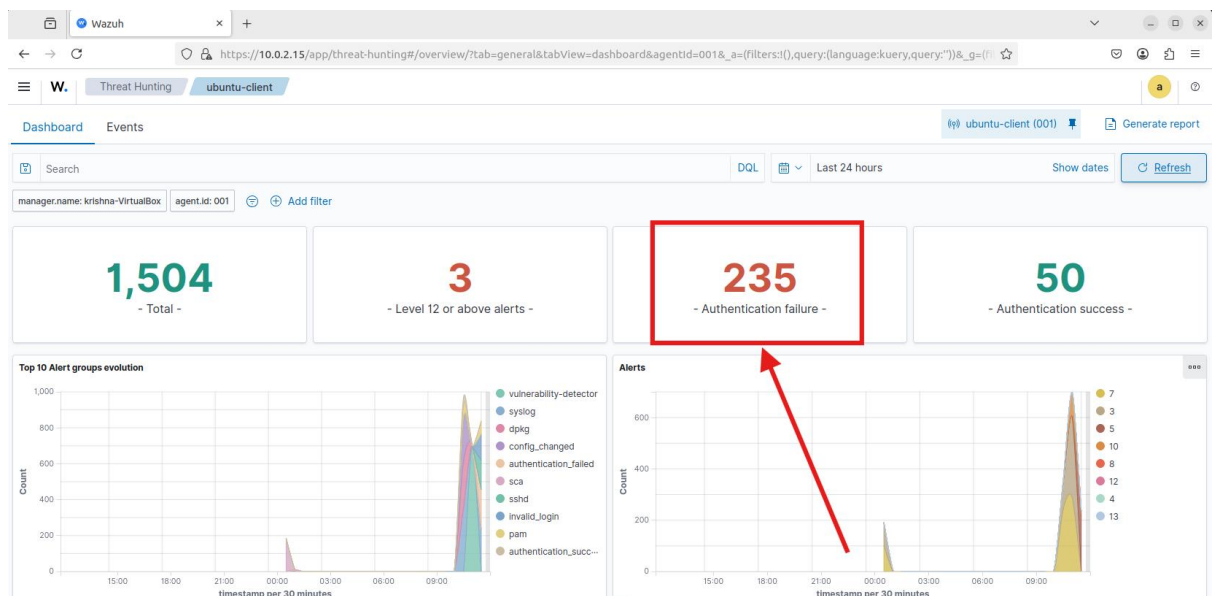
- USER.txt**: A box around the command `cat user.txt` and its output: `user`, `admin`, `ron`, and `client`.
- Passwd.txt**: A box around the command `cat passwd.txt` and its output: `1234`, `12345678`, `admin`, `root`, `toor`, `password`, `passwd`, `2709`, and `hello`.
- Attack**: A box around the command `sudo hydra -L user.txt -P passwd.txt 10.0.2.4 ssh`.

The terminal output shows the Hydra attack in progress, including a warning about SSH configurations, data about tasks and login tries, and a final success message: `[22][ssh] host: 10.0.2.4 login: client password: 2709`. A red arrow points to this line with the label **Success**.

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



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

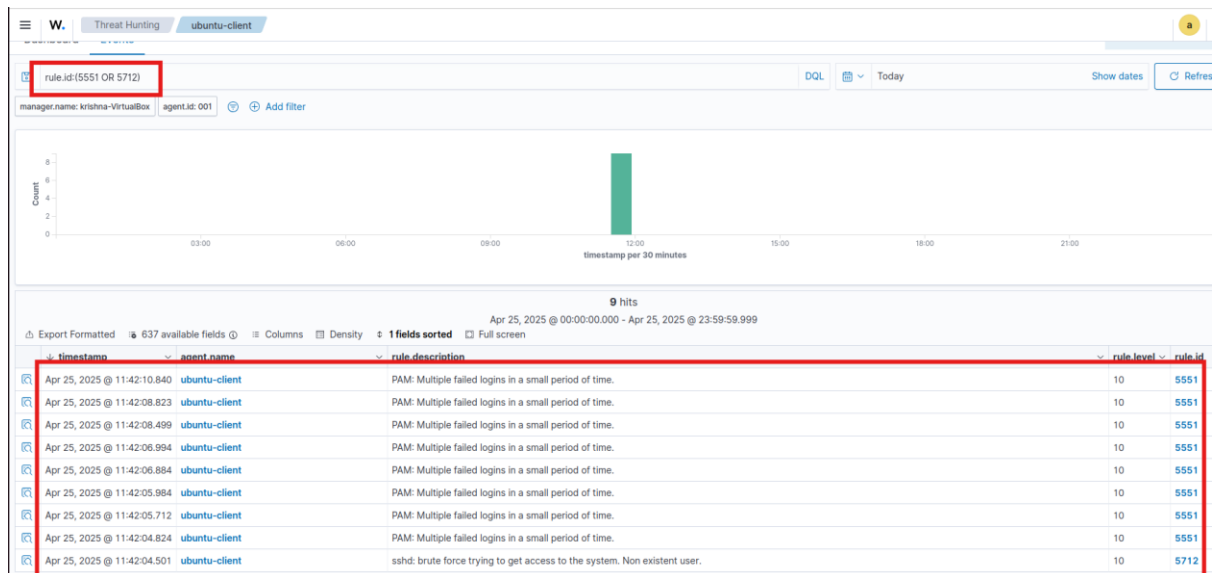


Visualization of alerts

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



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>