PREPARED BY: MUHAMMAD ABDUL REHMAN KHAN

LAB OUTLINE:

- What is Brute Force Attack?
- Requirement
- Setting up Wazuh Manager
- Adding Ubuntu Agent to Wazuh
- Setting up Brute Force Attack
- Visualizing Alerts
- Conclusion

What is BRUTE FORCE ATTACK?

A brute force attack is a method used by attackers to guess a password, encryption key, or PIN by systematically trying all possible combinations until the correct one is found. It relies on trial and error and can target online accounts, encrypted files, or network services. While simple, brute force attacks can be effective if passwords are weak, short, or commonly used. However, they can often be detected and blocked by security measures like account lockouts, CAPTCHA, or intrusion detection systems. Strengthening passwords, enabling multi-factor authentication, and monitoring for repeated login attempts are key defenses against these attacks.

REQUIREMENTS:

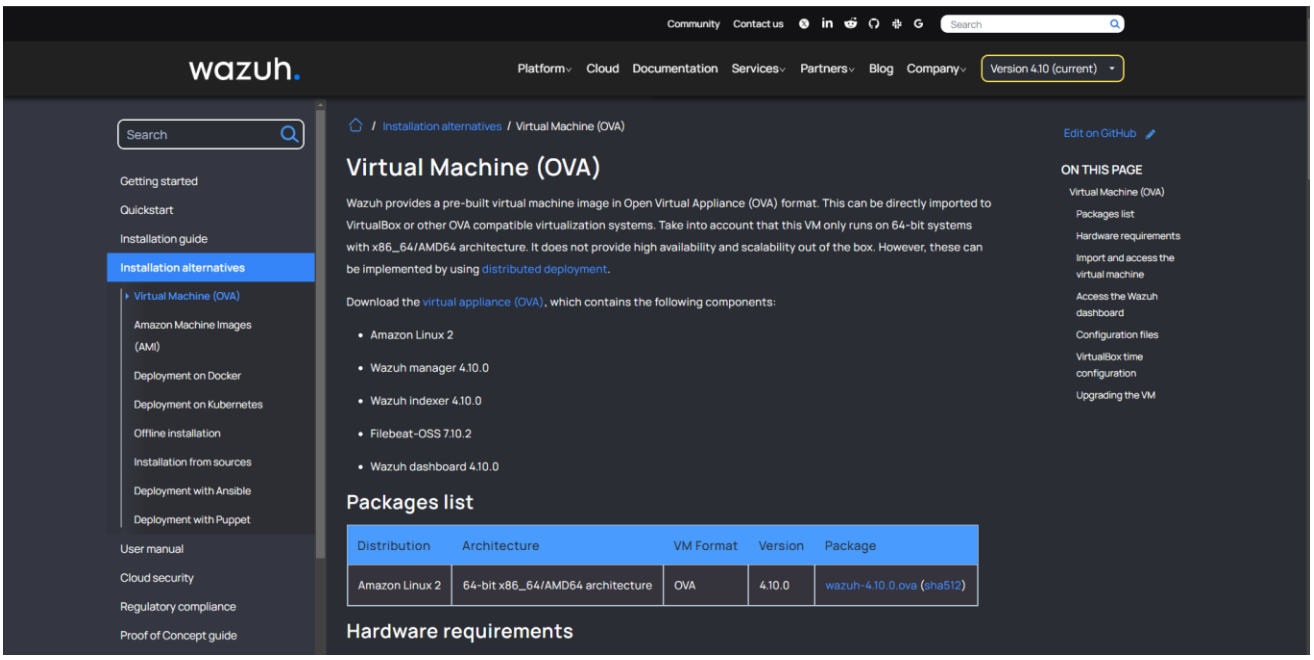
To set up our Home-lab, we need platforms and tools as mentioned below:

- VirtualBox
- Ubuntu 22.04 VM
- Kali Linux
- Wazuh OVA File

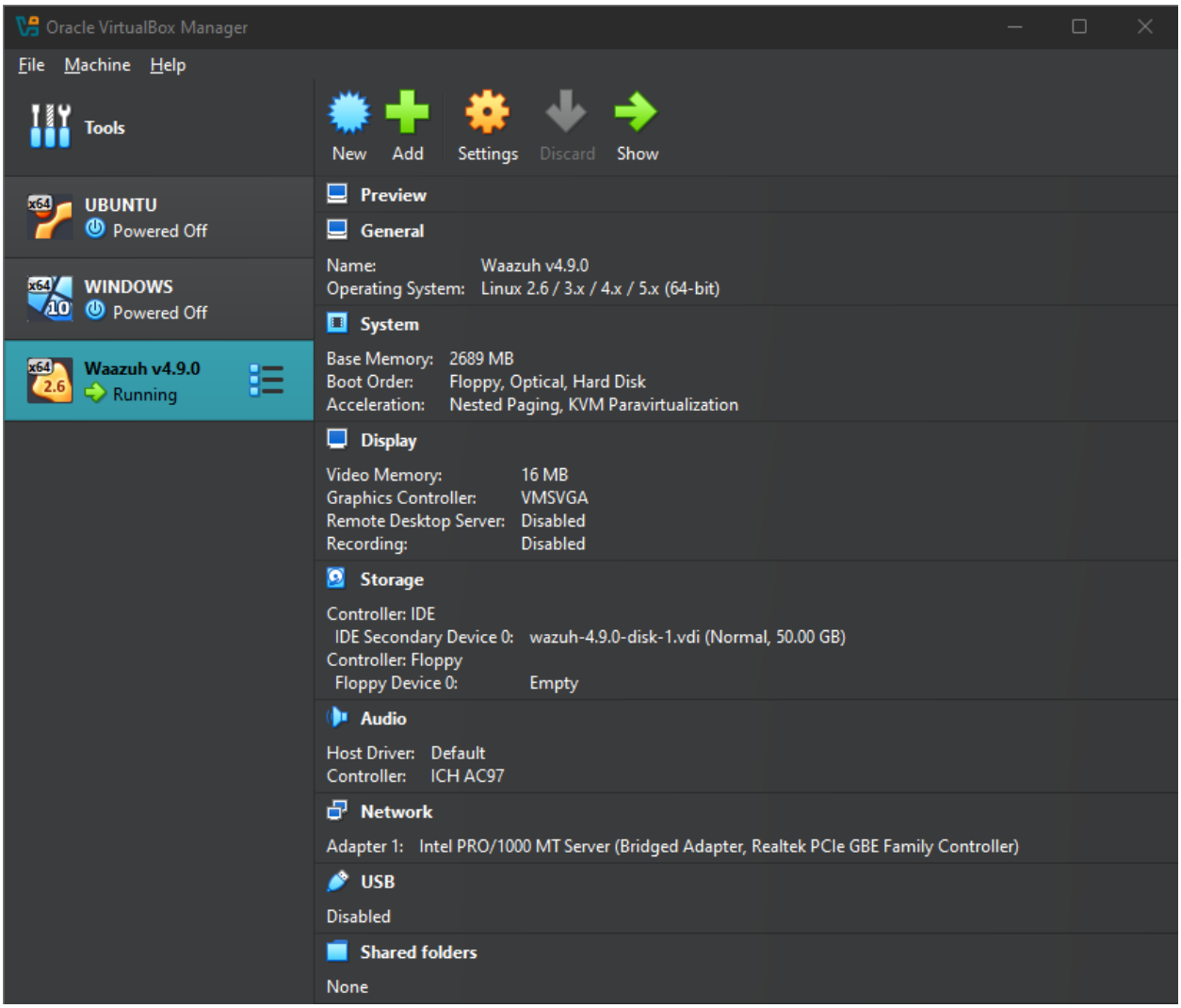
SETTING UP WAZUH MANAGER:

For Home-lab, it is convenient to use Wazuh OVA file. Visit their official website the file

(*https://documentation.wazuh.com/current/deployment-options/virtual-machine/virtual-machine.html*)



Open the file in VirtualBox and start the Virtual Machine



Now, log in to Wazuh CLI and run ***ifconfig*** to get the IP address. The default Wazuh CLI credential is:

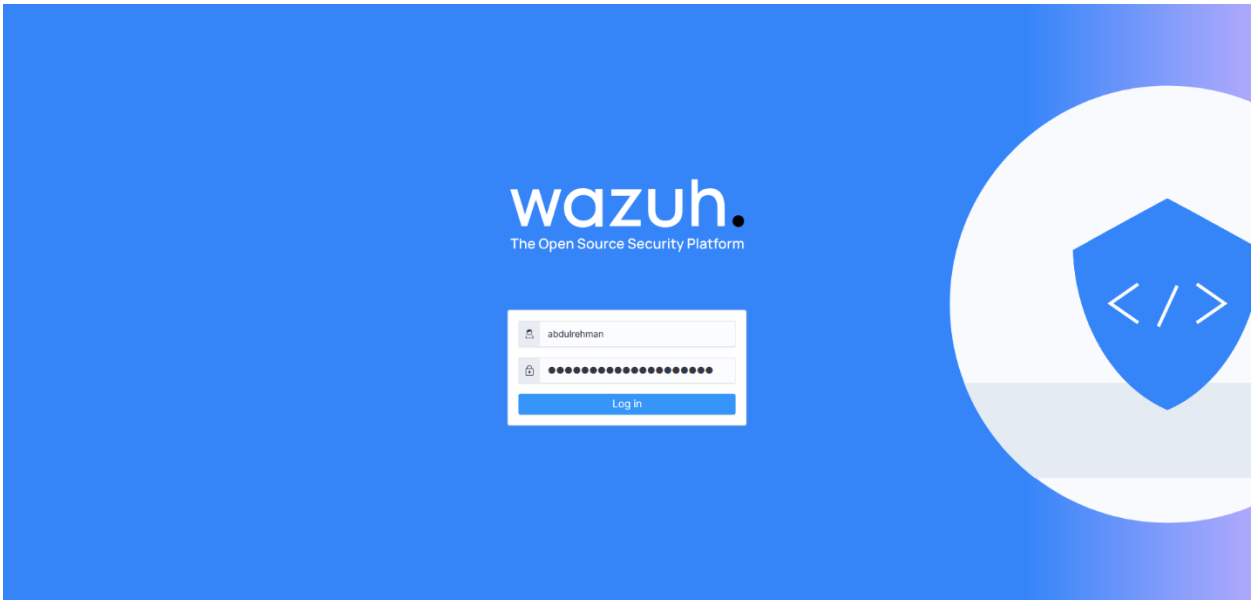
- **username:** *wazuh-user*
- **password:** *wazuh*

Once, you have the IP address, open your favourite browser and submit the URL:

- ***https://<WAZUH_IP_ADDRESS>***

Next, enter the Wazuh GUI credential as shown below

- **username:** *admin*
- **password:** *admin*

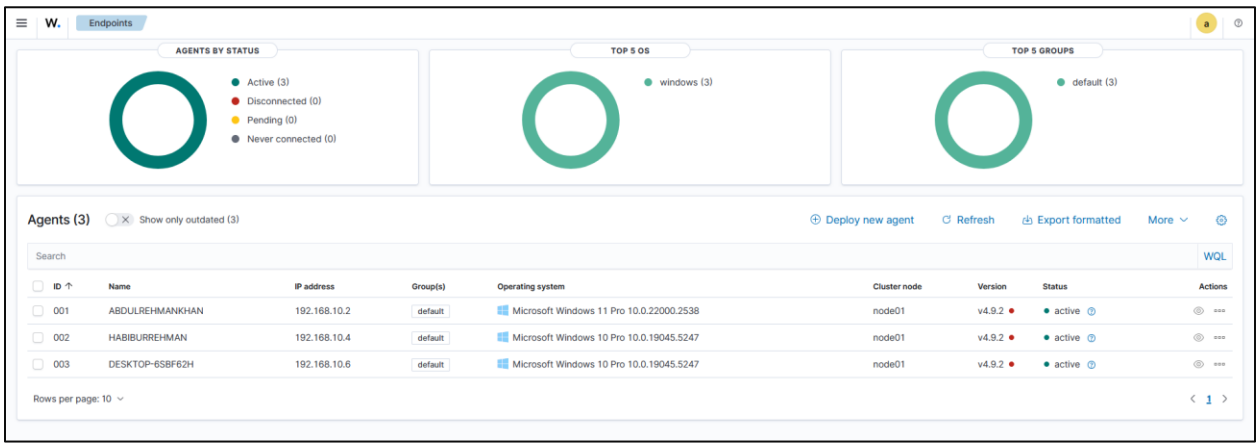


You are successfully logged-in to your WAZUH dashboard.

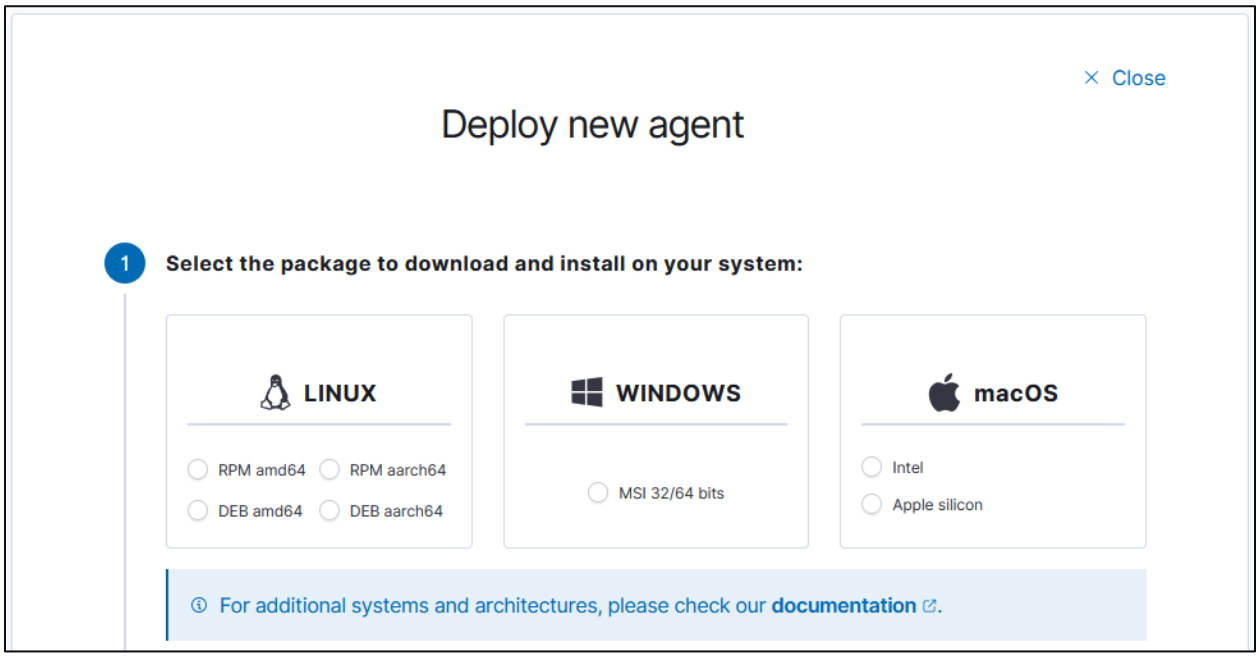
ADDING UBUNTU MACHINE TO WAZUH:

If your host OS is Ubuntu, you can go for installing locally or else you can download the Ubuntu 22.04.05 LTS Edition from Ubuntu's official ***website***.

Step1: Once your Ubuntu 22.04 machine is ready, visit the Wazuh platform using GUI. Go to Agents and click on Deploy new agent, as shown below.



Step2: Next, select an Operating system, enter your Wazuh Server address, and set your agent name as shown below.



2 **Server address:**

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

Assign a server address

Server address

Remember server address

3 **Optional settings:**

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Assign an agent name:

Agent name

The agent name must be unique. It can't be changed once the agent has been enrolled.

Select one or more existing groups:

Default

Step3: In the end, you will get a Shell Bash script & a command to start the Wazuh service on your agent, as shown below.

4 **Run the following commands to download and install the agent:**

```
wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.9.0-1_amd64.deb &&
sudo WAZUH_MANAGER='172.168.526.266' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='UBUNTU' dpkg -i
./wazuh-agent_4.9.0-1_amd64.deb
```

Requirements

- You will need administrator privileges to perform this installation.
- Shell Bash is required.

Keep in mind you need to run this command in a Shell Bash terminal.

5 **Start the agent:**

```
sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

Step4: Next, go to your Ubuntu 22.04 Machine and the script in your Shell Bash Terminal.

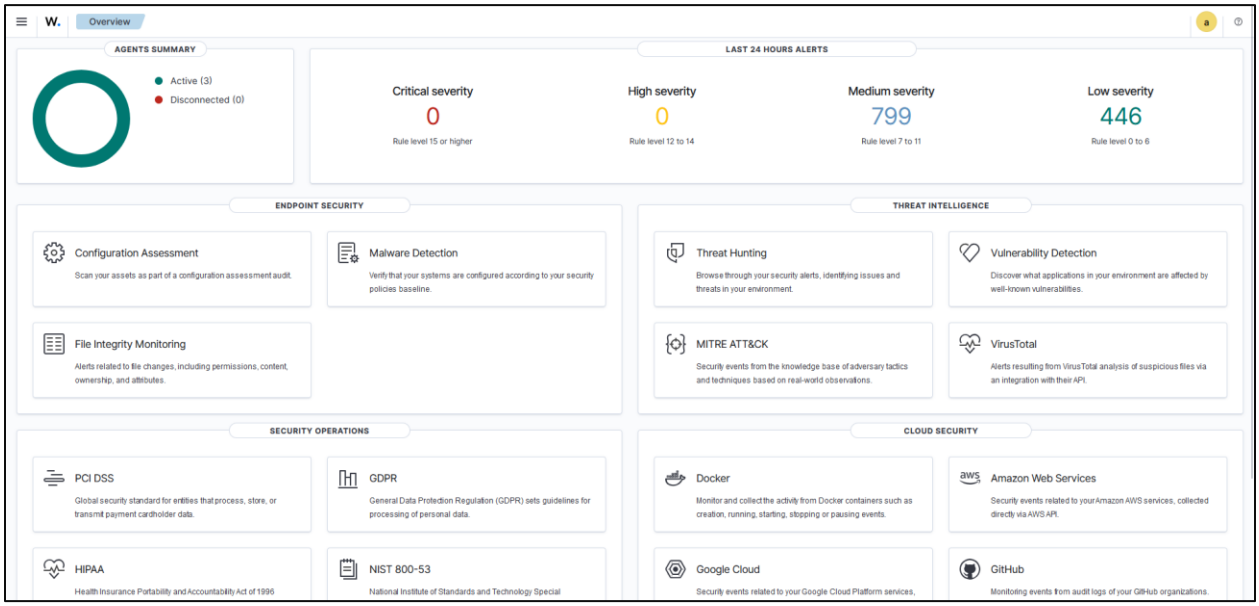
```
abdullah@m4rk-tech: ~
abdullah@m4rk-tech:~$ wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.9.0-1_amd64.deb && sudo WAZUH_MANAGER='192.168.10.212' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='UBUNTU' dpkg -i ./wazuh-agent_4.9.0-1_amd64.deb
```

Step5: Next, start the Wazuh service.

```
abdullah@m4rk-tech: ~
abdullah@m4rk-tech:~$ sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
```

Step6: Finally, come back to your Wazuh platform and go to Agents; you should see your newly on boarded Ubuntu agent here.

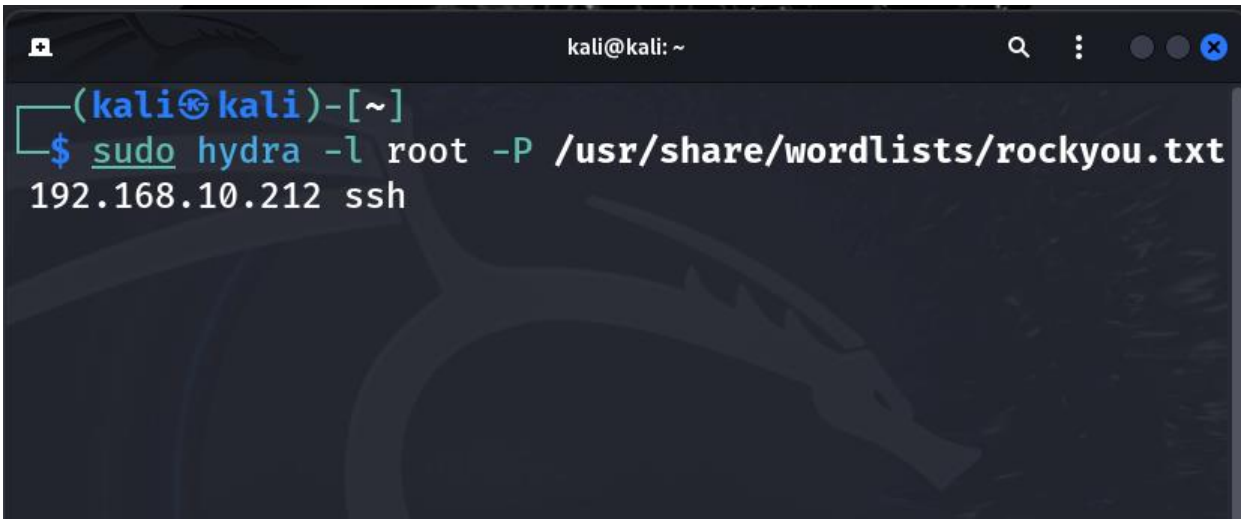
You have successfully boarded a new UBUNTU agent on your WAZUH



dashboard.

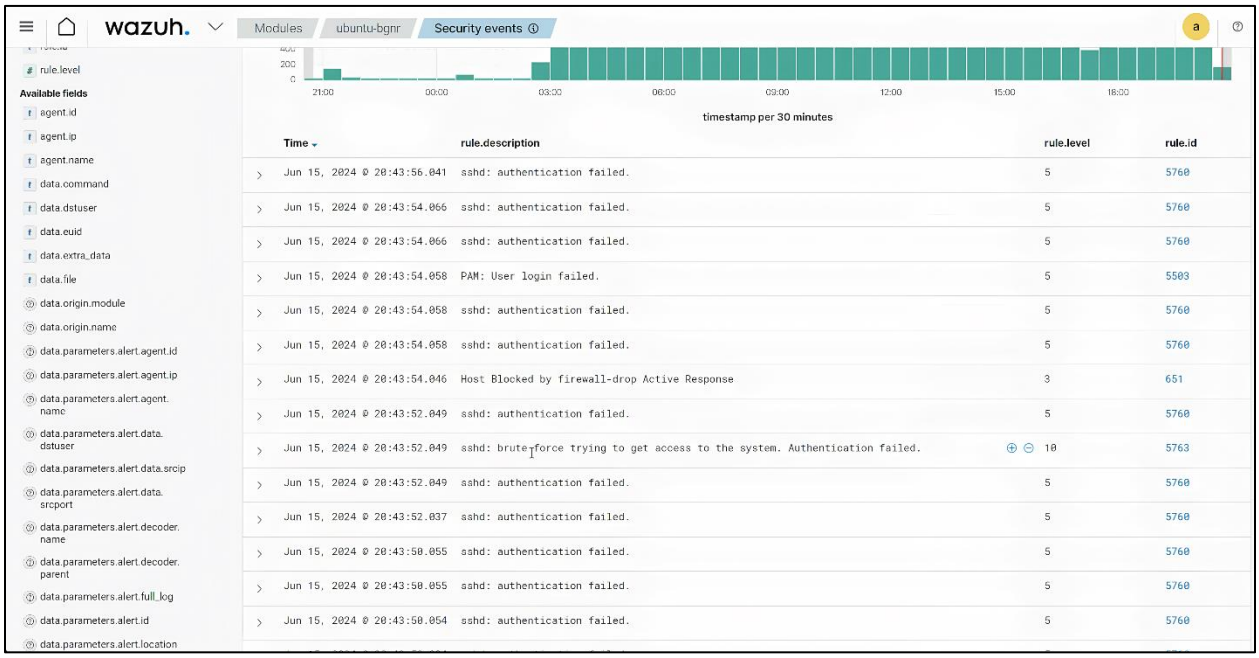
SETTING UP BRUTE FORCE ATTACK:

To simulate a brute force attack in your lab, we will use Hydra, a powerful tool designed for password-cracking via various protocols. In this lab, we are targeting SSH port.



VISUALIZING ALERTS:

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



DETECTING BRUTE FORCE ATTACK OVERVIEW:

A brute force attack is a method attackers use to guess passwords by systematically trying multiple combinations until successful. Detecting such attacks is crucial for securing systems against unauthorized access. Tools like Wazuh play a vital role in monitoring endpoints for unusual activity, such as repeated login failures, rapid login attempts, or unauthorized access attempts. By setting up proper monitoring rules and leveraging log analysis, Wazuh can generate real-time alerts, enabling swift detection and response to brute force attacks. This capability is essential in understanding attack patterns, mitigating threats, and strengthening overall system security.

CONCLUSION:

In this lab, we explored the process of detecting brute force attacks using Wazuh, showcasing its effectiveness in monitoring and securing systems. By simulating a brute force attack, we demonstrated how repeated login attempts and unauthorized access attempts can be identified through log analysis and real-time alerts. This exercise emphasized the importance of proactive detection tools like Wazuh in mitigating security risks, enhancing system defenses, and ensuring a strong cybersecurity posture against such threats.