Building a Wazuh lab that runs in VirtualBox to simulate threat detection + active response. It simulate a brute-force SSH attack and configure Wazuh to automatically block the attacker’s IP

**Lab Setup Overview**

We’ll use 3 VMs in VirtualBox:

1. Wazuh Manager (OVA file) → Collects logs, applies rules, triggers responses.

2. Ubuntu Desktop/Server (Victim with Wazuh Agent) → Target machine to be brute-forced.

3. Kali Linux (Attacker) → Runs brute-force attack with hydra.

Step 1. Deploy Wazuh Manager

1. Download Wazuh OVA from Wazuh website.

2. Import into VirtualBox:

Network mode: “Internal Network” (so all 3 VMs can see each other).

Assign hostname: wazuh-manager.

Default web UI: https://{wazuh-ip:192.168.10.53}

Step 2. Setup Victim Machine (Ubuntu Desktop/Server)

1. Install Ubuntu Desktop.

2. Enable SSH:

***sudo apt update && sudo apt install openssh-server -y***

***sudo systemctl enable ssh && sudo systemctl start ssh***

3. Create a test user:

***sudo adduser victim***

4. Install Wazuh Agent:

From Wazuh dashboard, copy the agent installation command (it includes manager IP & key).

Run on Ubuntu:

curl -so wazuh-agent.sh https://packages.wazuh.com/4.x/wazuh-agent.sh

sudo bash wazuh-agent.sh --register --server wazuh-manager-ip

sudo systemctl enable wazuh-agent && sudo systemctl start wazuh-agent

5. Confirm connection in Wazuh Dashboard → Agents → should show Ubuntu agent as active.

Step 3. Setup Attacker Machine (Kali Linux)

1. Install Kali Linux in VirtualBox.

2. Ensure it’s on the same Internal Network as Ubuntu and Wazuh Manager.

3. Install hydra (if not preinstalled):

***sudo apt update && sudo apt install hydra -y***

Step 4. Configure Active Response on Wazuh

1. On Wazuh Manager, edit ossec.conf:

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

2. Add active response block (inside <ossec\_config>):

***<active-response>***

***<command>firewalld</command>***

***<location>local</location>***

***<rules\_id>5710, 5712, 5715</rules\_id>***

***<timeout>600</timeout>***

***</active-response>***

* 5710, 5712, 5715 → SSH brute-force rule IDs.
* firewalld → blocks attacker’s IP.
* timeout = 600 sec (unblocks after 10 min).

3. Restart Wazuh Manager:

***sudo systemctl restart wazuh-manager***

Step 5. Simulate Brute-force Attack

1. From Kali Attacker, run Hydra against Ubuntu victim:

***hydra -l victim -P /usr/share/wordlists/rockyou.txt ssh://<victim-ip>***

* Replace <victim-ip> with Ubuntu’s IP.{192.168.10.53}
* This floods SSH with failed logins.

2. On Wazuh Dashboard:

* Navigate to Security events.
* You should see alerts: SSH brute-force detected.

3. Active response kicks in:

* Attacker’s IP gets blocked by firewall.
* Check on victim machine:

***sudo iptables -L -n | grep <kali-ip>***

* You should see Kali’s IP blocked.

Step 6. Verify & Test

* Try SSH from Kali again → should be blocked.
* After timeout (10 min), the block is removed automatically.

Logs:

***tail -f /var/ossec/logs/active-responses.log***

Shows:

Active response: Firewall drop -> Attacker IP {192.168.10.55}

What You Achieved

* Detection: Wazuh spotted brute-force SSH attempts.
* Response: Wazuh auto-blocked attacker’s IP with firewall rules.
* Verification: Confirmed IP block in logs + firewall rules.