Project 2 WEEK 3

🛡️ WEEK-3: ACTIVE RESPONSE (IPS)

“Active response was configured to automatically mitigate SSH brute-force attacks. Upon detecting multiple failed login attempts, Wazuh triggered a firewall-drop action that blocked the attacker IP for one hour, demonstrating real-time IPS capabilities.”

🎯 Goal (Evaluator / Interview Ready)

Detect SSH brute-force attacks and automatically block attacker IP using firewall rules.

🧱 Lab Architecture (Simple)

- **Wazuh Manager** → Detection + decision
- **Linux Agent (Target Server)** → SSH service
- **Attacker Machine (Kali)** → Hydra brute force
- **Active Response** → Firewall auto-block

Kali (Hydra attack)

↓

Linux Agent (SSH logs)

↓

Wazuh Manager (Detect brute force)

↓

Active Response triggered

↓

iptables rule added on Linux Agent

🔹 STEP 1: Verify SSH Log Collection (Agent)

On **Linux Agent**:

First install ssh on agent if not installed:

sudo apt update

sudo apt install openssh-server -y

Then:

sudo systemctl start ssh

sudo systemctl enable ssh

then:

sudo systemctl status ssh

sudo ss -tulnp | grep ssh

sudo grep -i ssh /var/log/auth.log | tail

Agar logs aa rahe hain → SSH monitoring OK ✅

On Windows Agent:

Open **PowerShell as Administrator** on Windows Server 2022:

wevtutil qe Security /c:5 /rd:true /f:text

If output aa raha hai → **Windows Security logging OK** ✅

- **Filter Only RDP / Logon Failures**

Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4625} -MaxEvents 5

✅ Agar events aa rahe hain → **Brute-force detection possible**

- **Agent Is Sending Logs**

Get-Service WazuhSvc

Expected:

Status   : Running

Name   : WazuhSvc

Restart if needed:

Restart-Service WazuhSvc

- **Check Wazuh Agent Log (Windows):**

type "C:\Program Files (x86)\ossec-agent\ossec.log" | more

expected output:

Connected to manager

Sending event logs

🔹 **Ensure RDP Is Enabled (Target Exposure)**

```
Set-ItemProperty `
 'HKLM:\System\CurrentControlSet\Control\Terminal Server' `
 -Name "fDenyTSConnections" -Value 0
```

🔹 Allow RDP through firewall:

```
Enable-NetFirewallRule -DisplayGroup "Remote Desktop"
```

Verify:

```
netstat -ano | findstr 3389
```

🔹 **STEP 2: Ensure SSH Brute Force Rules Enabled (Manager)**

Check default rules (already enabled usually):

```
sudo grep -R "sshd" /var/ossec/ruleset/rules/
```

🔍 Expected Output (Examples)

Tumhe aise rules dikhenge:

/var/ossec/ruleset/rules/sshd_rules.xml

/var/ossec/ruleset/rules/sshd_rules.xml:<description>SSH authentication failed</description>

/var/ossec/ruleset/rules/sshd_rules.xml:<mitre>T1110</mitre>

Important Rule IDs:

5710 – SSH auth failure

5712 – Multiple failures

5715 – SSH brute force (Active Response trigger)

🧠 Why We Checked This (SOC Logic)

“Before enabling active response, we verified that SSH brute-force detection rules were already present and mapped to MITRE ATT&CK T1110.”

🔹 **STEP 3: Enable Active Response (Manager)**

Check Available Active Response Scripts

Run:

sudo ls /var/ossec/active-response/bin/

Tumhe kuch aise scripts dikhenge:

```
agent@agent-virtual-machine:~$ sudo ls /var/ossec/active-response/bin/
default-firewall-drop  firewall-drop   ipfw          npf         restart-wazuh
disable-account        host-deny       kaspersky     pf          route-null
firewalld-drop         ip-customblock  kaspersky.py  restart.sh  wazuh-slack
```

firewall-drop

👉 **Jo bhi firewall related script ho — wahi use karna hai.**

- **Register firewall-drop Command (MANDATORY)**

Wazuh me rule hai: Active-response command tabhi valid hota hai jab pehle `<command>` section me registered ho.

Open config:

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

For linux agent Add this once (outside active-response block):

<command>

<name>firewall-drop</name>

<executable>firewall-drop</executable>

<timeout_allowed>yes</timeout_allowed>

</command>

🔹 **Configure Active Response Rule for linux agent**

Add this block:

<active-response>

<command>firewall-drop</command>

<location>local</location>

<level>10</level>

<timeout>3600</timeout>

</active-response>

🔹 **For Windows Agent add this once (outside active-response block):**:

<command>

<name>block-ip-windows</name>

<executable>block-ip.cmd</executable>

<timeout_allowed>yes</timeout_allowed>

</command>

🔹 **Configure Active Response Rule for windows agent**

<active-response>

<command>block-ip-windows</command>

<location>any</location>

<rules_id>100001</rules_id>

<timeout>600</timeout>

</active-response>

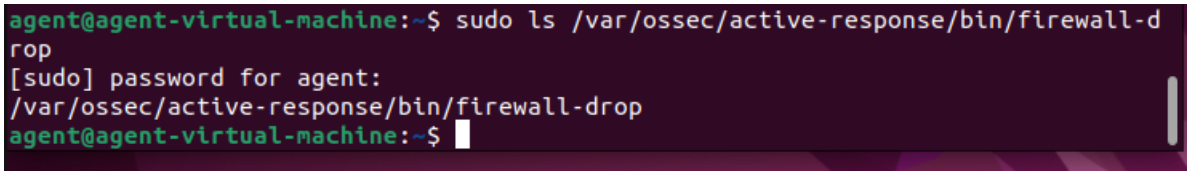
📌 Meaning:

- Level ≥10 alerts only
- Auto block attacker IP
- 1 hour timeout
- firewall-drop → IP block karega
- level 10 → sirf high-severity alerts pe
- timeout 3600 → 1 hour ban

🔹 **STEP 4: Enable Firewall Command**

Verify command exists:

sudo ls /var/ossec/active-response/bin/firewall-drop



If present → OK ✅

- **STEP 5: Restart & Validate**

sudo /var/ossec/bin/wazuh-analysisd -t

sudo systemctl restart wazuh-manager

systemctl status wazuh-manager

Expected:

Active: active (running)

- **STEP 6: Simulate Brute Force Attack (Attacker Kali linux)**

For Linux Agent:

ssh root@192.168.48.129

You should see:

Permission denied

Now Launch Hydra (use agent ip as < TARGET_IP>)

hydra -l root -P /usr/share/wordlists/rockyou.txt ssh://<TARGET_IP>

Let it run for **30–60 seconds**.

For windows:

METHOD 1: Manual RDP Attempts (Simple but Slow)

❌ Try logging in via RDP with **wrong password** multiple times from another windows machine.

Win + R → mstsc

- Enter Windows Server IP
- Use **wrong password 5–10 times**

📌 This still generates **4625 events** (works fine for demos).

METHOD 2: Hydra (Sometimes Unstable for RDP)

echo -e "admin123\npassword\nwelcome123\nP@ssw0rd\nfgs32\ndrdr443\nhack@me\nkjjhfu45\nijhsfd67\nhygf87\nhggf6\n6fffjy" > pass.txt

hydra -t 4 -V -f -l administrator -P pass.txt rdp://192.168.1.20

⚠️ Note:
Hydra RDP module can be unstable

Rule ID Description

60122 Windows login failure

60123 Multiple login failures

60204 RDP brute-force detected

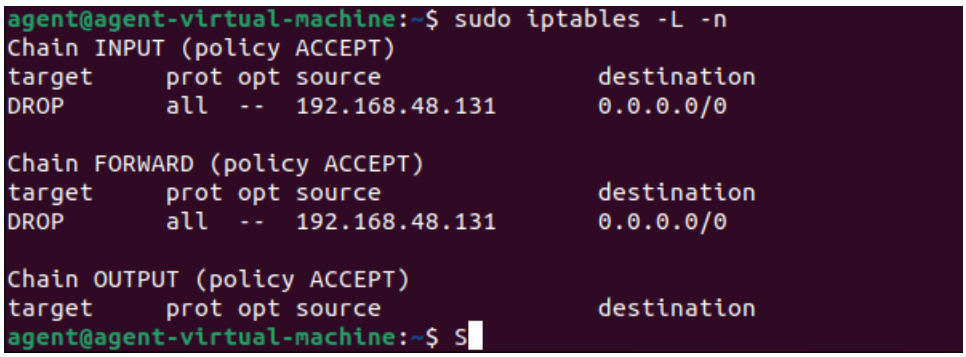
60205 Authentication attack

60206 MITRE T1110 (Brute Force)

🔹 **STEP 7: Verify Auto IP Block (Target Agent)**

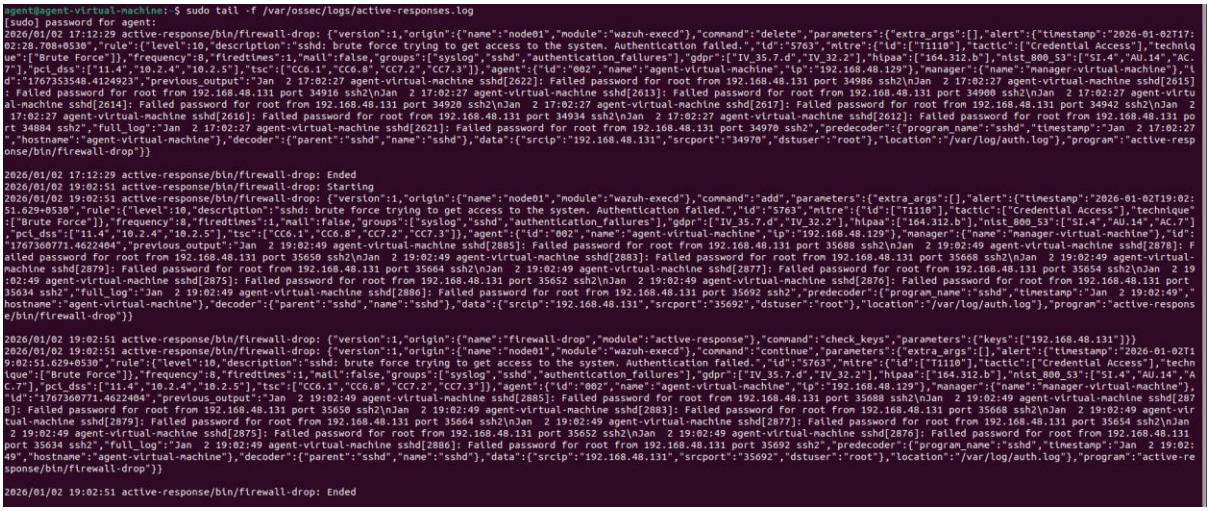
sudo iptables -L -n

Expected:



➢ Also verify logs:

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



🎯 **SUCCESS: Active Response triggered**

🔹 **STEP 8: Verify Alert in Dashboard**

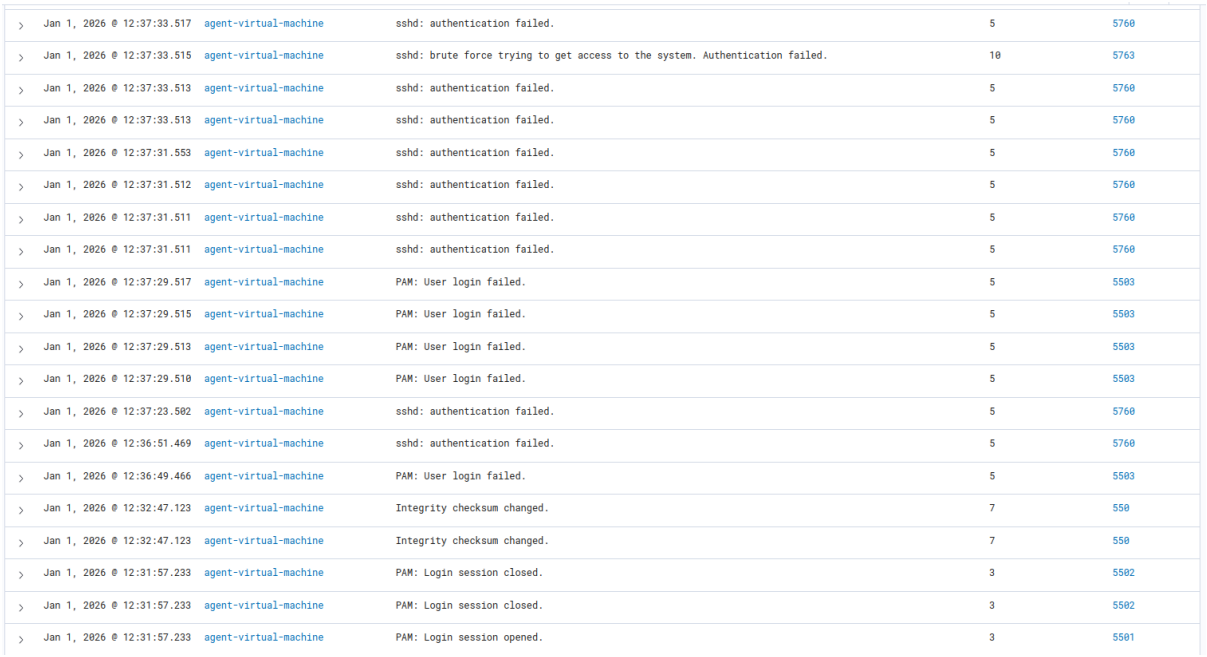
Dashboard → Security Events

Filter:

rule.id:5760,60106

You should see:

- SSH brute force detected
- Source IP
- Active response executed

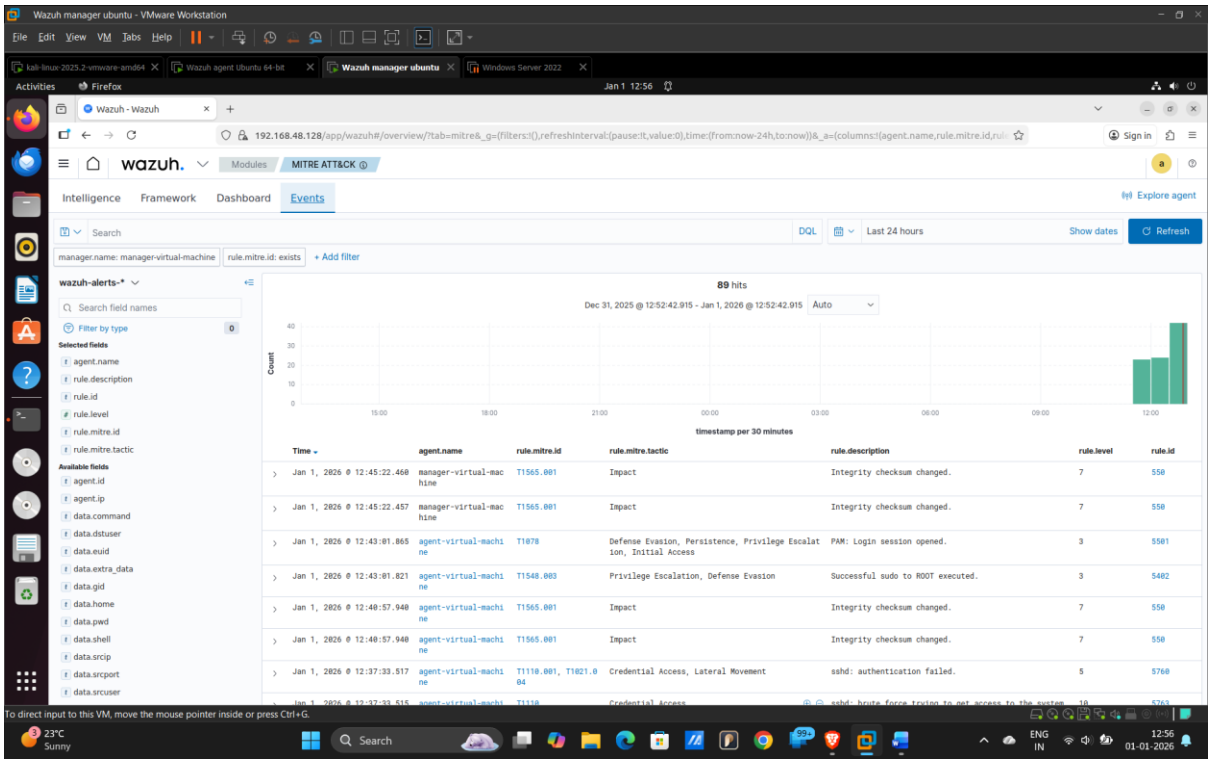


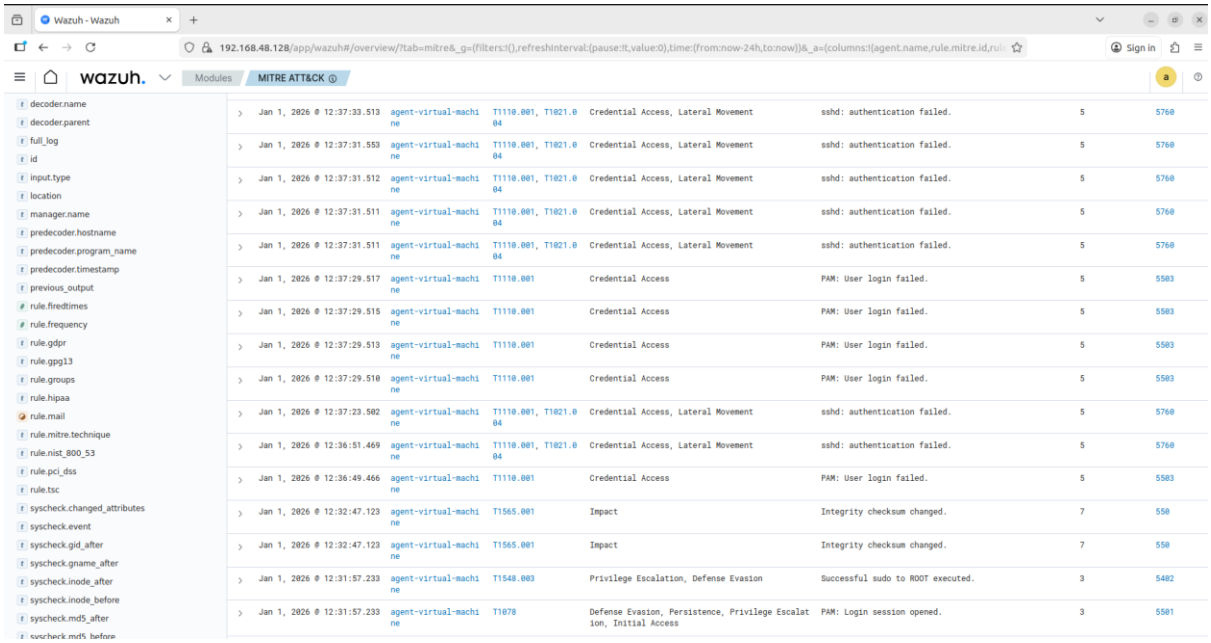
Jan 1, 2026 @ 12:37:33.517	agent-virtual-machine	sshd: authentication failed.	5	5760
Jan 1, 2026 @ 12:37:33.515	agent-virtual-machine	sshd: brute force trying to get access to the system. Authentication failed.	10	5763
Jan 1, 2026 @ 12:37:33.513	agent-virtual-machine	sshd: authentication failed.	5	5760
Jan 1, 2026 @ 12:37:33.513	agent-virtual-machine	sshd: authentication failed.	5	5760
Jan 1, 2026 @ 12:37:31.553	agent-virtual-machine	sshd: authentication failed.	5	5760
Jan 1, 2026 @ 12:37:31.512	agent-virtual-machine	sshd: authentication failed.	5	5760
Jan 1, 2026 @ 12:37:31.511	agent-virtual-machine	sshd: authentication failed.	5	5760
Jan 1, 2026 @ 12:37:31.511	agent-virtual-machine	sshd: authentication failed.	5	5760
Jan 1, 2026 @ 12:37:29.517	agent-virtual-machine	PAM: User login failed.	5	5503
Jan 1, 2026 @ 12:37:29.515	agent-virtual-machine	PAM: User login failed.	5	5503
Jan 1, 2026 @ 12:37:29.513	agent-virtual-machine	PAM: User login failed.	5	5503
Jan 1, 2026 @ 12:37:29.510	agent-virtual-machine	PAM: User login failed.	5	5503
Jan 1, 2026 @ 12:37:23.502	agent-virtual-machine	sshd: authentication failed.	5	5760
Jan 1, 2026 @ 12:36:51.469	agent-virtual-machine	sshd: authentication failed.	5	5760
Jan 1, 2026 @ 12:36:49.466	agent-virtual-machine	PAM: User login failed.	5	5503
Jan 1, 2026 @ 12:32:47.123	agent-virtual-machine	Integrity checksum changed.	7	550
Jan 1, 2026 @ 12:32:47.123	agent-virtual-machine	Integrity checksum changed.	7	550
Jan 1, 2026 @ 12:31:57.233	agent-virtual-machine	PAM: Login session closed.	3	5502
Jan 1, 2026 @ 12:31:57.233	agent-virtual-machine	PAM: Login session closed.	3	5502
Jan 1, 2026 @ 12:31:57.233	agent-virtual-machine	PAM: Login session opened.	3	5501

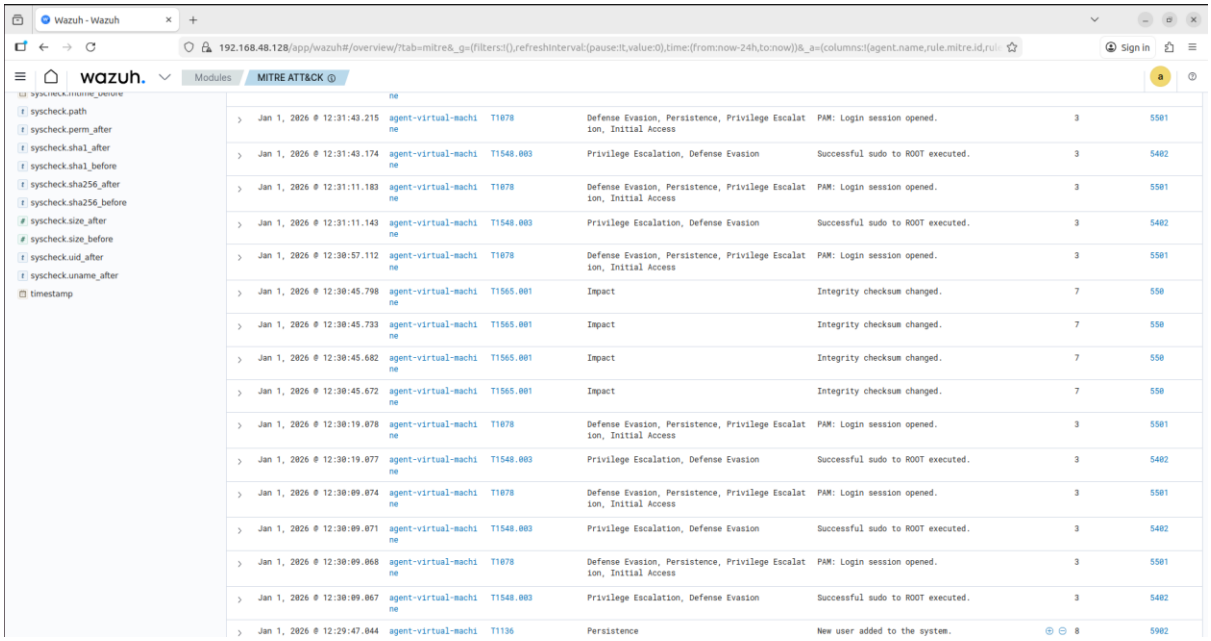
◆ STEP 9: MITRE ATT&CK Mapping (Final)

Activity / Detection	**MITRE ATT&CK Technique**	**Technique ID**	**Explanation**
SSH Brute-Force Attack	Remote Services (SSH)	**T1021.004**	Attacker attempts to gain remote access via SSH using automated tools such as Hydra.
Repeated SSH Login Failures	Password Guessing	**T1110.001**	Multiple failed SSH authentication attempts indicate brute-force password guessing.
Successful SSH Login (if occurred)	Valid Accounts	**T1078**	Attacker successfully authenticates using valid credentials obtained via brute-force.
Privilege Escalation via Sudo	Abuse Elevation Control Mechanism (Sudo)	**T1548.003**	Attacker attempts privilege escalation by abusing sudo permissions after login.
Configuration / File Integrity Changes	Stored Data Manipulation	**T1565.001**	Unauthorized modification of system or configuration files detected by FIM.

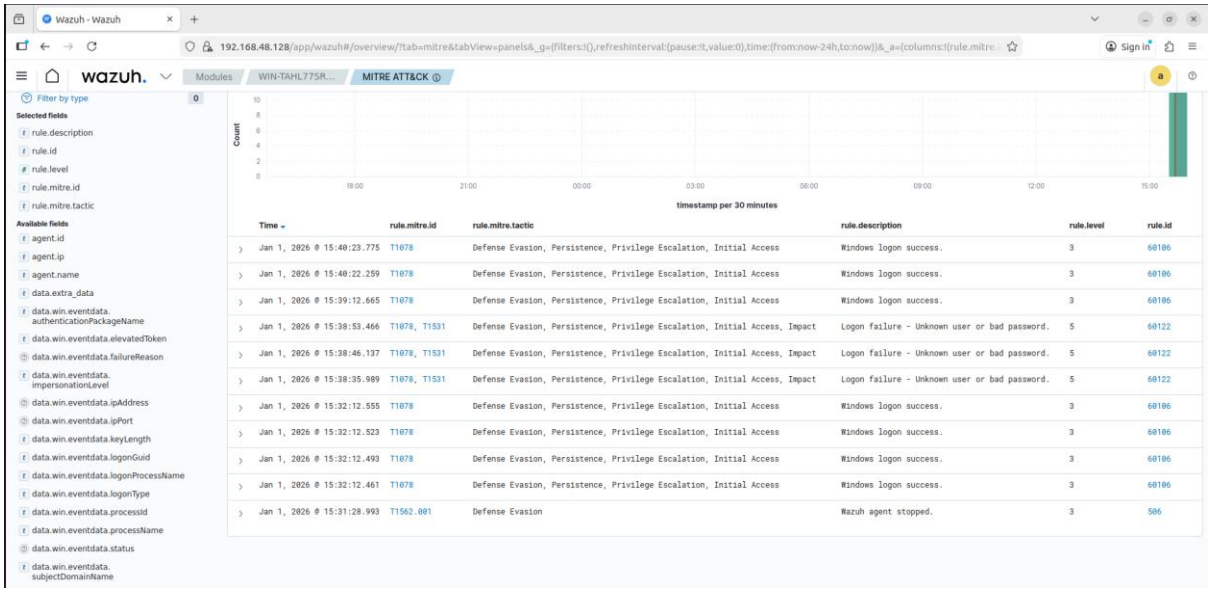
Activity / Detection	MITRE ATT&CK Technique	Technique ID	Explanation
Automated IP Blocking (Active Response)	Network Traffic Filtering (Mitigation)	**M1037**	Firewall rules dynamically block malicious source IPs to contain the attack.



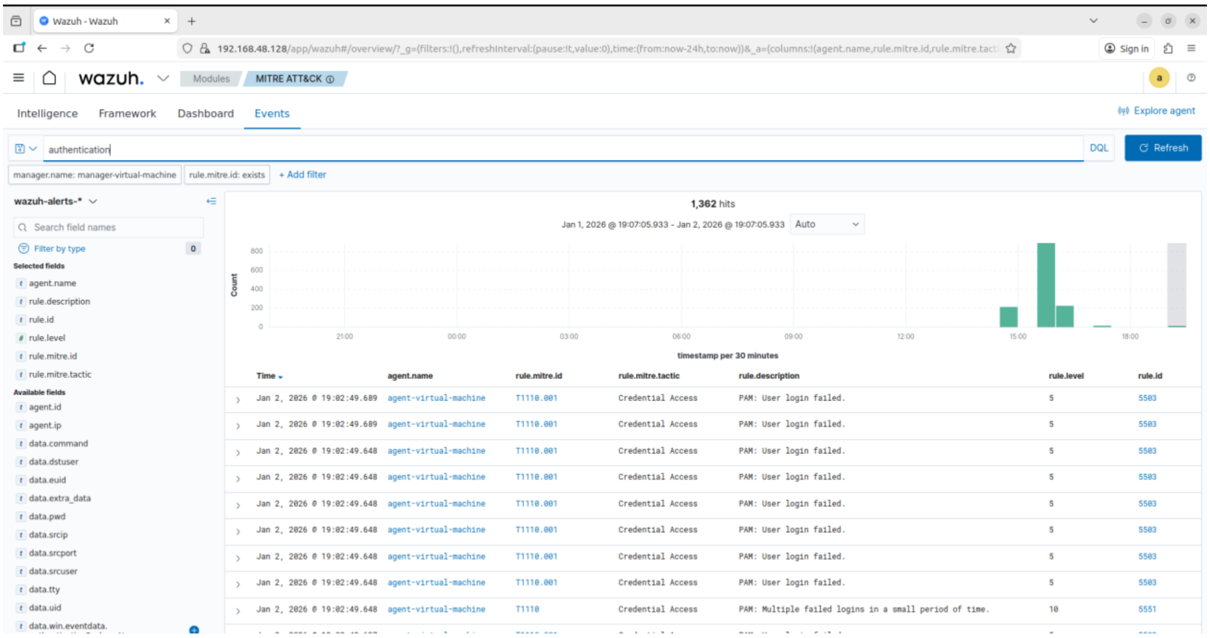




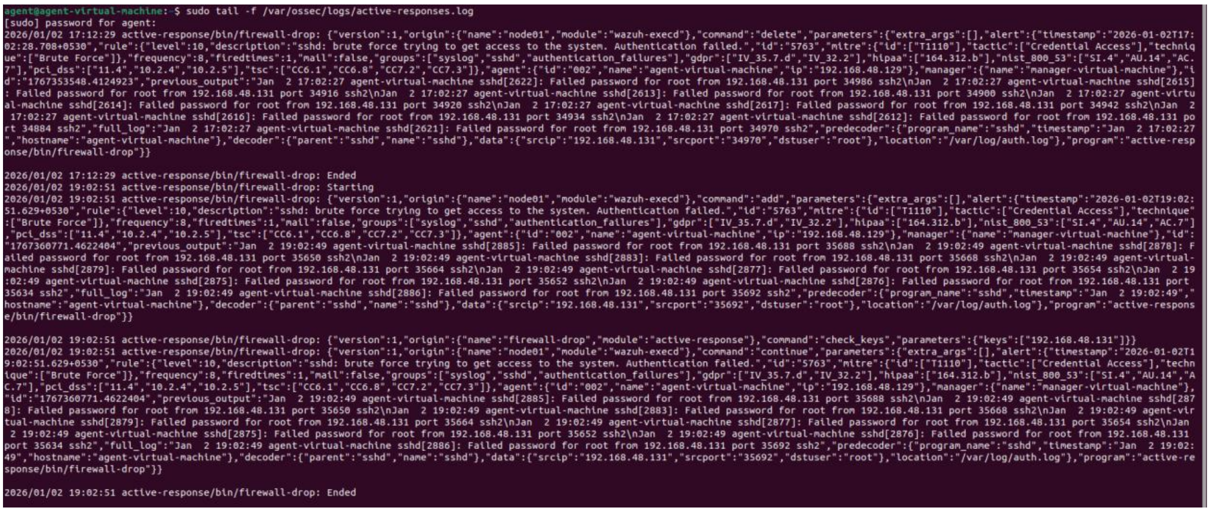
WINDOWS AGENT



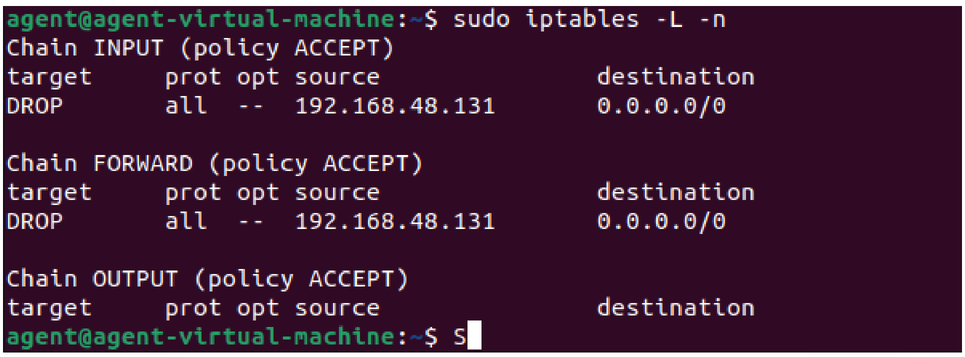
Wazuh-alert.png



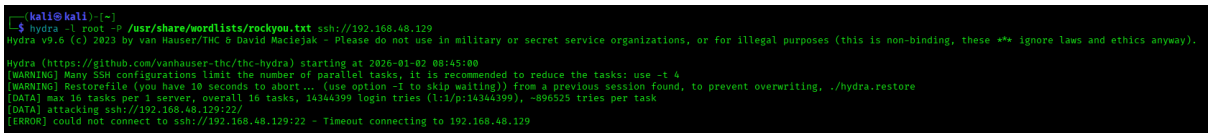
active-response-log.png



iptables-drop-rule.png



attacker-blocked.png



🧠 One-Line Explanation (For Viva / Interview)

“The SSH brute-force attack maps to MITRE ATT&CK technique **T1110**, and the automated firewall-based active response aligns with mitigation technique **M1037**, effectively preventing further credential access attempts.”

“The detection and response pipeline demonstrates alignment with the MITRE ATT&CK framework, enabling standardized threat classification and response validation.”

🏁 Week-3 Status

- ✅ Brute-force attack simulated
- ✅ Detection via Wazuh SSH rules
- ✅ Active Response executed
- ✅ MITRE mapping completed

🔥 **WEEK-3 = COMPLETE**