Incident Ticket – SSH Brute Force Attempt

Incident Title

[Medium] SSH Brute Force Authentication Failure on VM2

Incident ID

INC-002

Date & Time

07 January 2026, 17:47:39

Reported By

Wazuh SIEM

Affected Asset

- Hostname: kkk-VMware-Virtual-Platform
- Agent Name: kkk
- Agent IP: 192.168.247.135
- Operating System: Ubuntu Linux

Incident Category

Unauthorized Access Attempt / Brute Force Attack

Severity

Medium
(Rule Level: 10)

Status

Open

Incident Description

Multiple failed SSH authentication attempts were detected on the endpoint system (VM2). The Wazuh agent identified repeated password failures through the SSH daemon, indicating a potential brute-force attack targeting the SSH service. The event was generated from system logs monitored via journald and decoded by the SSHD decoder.

No successful authentication was observed during this activity.

Detection Details

- Detection Source: Wazuh Agent
- Decoder Name: sshd
- Log Source: journald
- Rule ID: 2502
- Rule Description: User missed the password more than one time

- Rule Groups: syslog, access_control, authentication_failed

Indicators of Compromise (IOCs)

- Source IP Address: 127.0.0.1
- Target Service: SSH
- Authentication Method: Password-based login
- Log Message: PAM authentication failure detected

MITRE ATT&CK Mapping

- Tactic: Credential Access
- Technique ID: T1110
- Technique Name: Brute Force

Initial Assessment

The incident represents an attempted brute-force authentication attack against the SSH service. Although no successful login was recorded, the repeated authentication failures suggest malicious or unauthorized activity. The impact is currently limited, and no system compromise has been identified.

Recommended Actions

- Continue monitoring SSH authentication logs for further attempts

- Enforce account lockout policies for repeated login failures
- Review SSH configuration and restrict access where possible
- Escalate to Tier 2 SOC if activity persists or escalates

Assigned To

SOC Analyst – Tier 1