Incident Ticket – SSH Brute Force Attempt

Incident Title

[Medium] SSH Brute Force Authentication Failures on Alpha VM

Incident ID

INC-003

Date & Time

06 January 2026, 12:46:29

Reported By

Wazuh SIEM

Affected Asset

- Hostname: it-VMware-Virtual-Platform
- Agent ID: 001
- Agent IP: 172.20.10.5
- Operating System: Ubuntu Linux

Incident Category

Unauthorized Access Attempt / Brute Force Attack

Severity

Medium
(Rule Level: 10)

Status

Open

Incident Description

Wazuh detected multiple failed SSH authentication attempts on the Alpha Ubuntu virtual machine. The alerts indicate repeated password failures recorded by the SSH daemon, suggesting a brute-force attack against the SSH service. The activity was identified through system authentication logs and analyzed by the Wazuh manager.

No successful SSH login was observed during the incident timeframe.

Detection Details

- Detection Tool: Wazuh Agent
- Decoder Name: sshd
- Log Source: /var/log/auth.log
- 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 System IP: 172.20.10.5
- Target Service: SSH
- Authentication Method: Password-based login
- Log Evidence: PAM authentication failure messages

MITRE ATT&CK Mapping

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

Initial Assessment

This incident represents an attempted brute-force attack against the SSH service. Although repeated authentication failures were detected, there is no evidence of a successful login or system compromise. The activity suggests probing or unauthorized access attempts with limited impact at this stage.

Recommended Actions

- Continue monitoring SSH authentication logs
- Enforce strong password and account lockout policies
- Restrict SSH access to trusted IP addresses
- Escalate to Tier 2 SOC if repeated attempts continue

Assigned To

SOC Analyst – Tier 1

Next Review

Pending further investigation if additional alerts are triggered