Incident Ticket

Incident Title

SSH Brute Force Authentication Failures Detected

Incident ID

INC-SSH-2502-001

Detection Source

Wazuh SIEM

Date & Time (IST)

21 January 2026, 18:36:19 IST

Affected Asset

- **Hostname:** kkk-VMware-Virtual-Platform
- **Agent Name:** kkk
- **Agent ID:** 001
- **Operating System:** Ubuntu Linux

Alert Description

Multiple SSH authentication failures were detected on the monitored Ubuntu endpoint. The alert was generated after repeated failed login attempts within a short time interval, indicating potential brute-force activity against the SSH service.

Technical Details

- **Decoder:** sshd
- **Log Source:** journalld
- **Log File:** /var/log/auth.log
- **Rule ID:** 2502
- **Rule Level (Severity):** 10
- **Rule Description:** User missed the password more than one time

---

Indicators of Compromise (IOCs)

- **Source IP Address:** 127.0.0.1
- **Service Targeted:** SSH
- **Event Type:** Authentication failure

MITRE ATT&CK Mapping

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

Threat Intelligence Enrichment

- **VirusTotal:** No malicious reputation found
- **AlienVault OTX:** No associated threat pulses detected
- **Assessment:** Source IP is localhost; activity likely generated internally for testing or misconfiguration

---

Analyst Assessment

The alert represents a **True Positive** event as multiple authentication failures were recorded. However, the source IP being localhost indicates that the activity originated from the same system, suggesting either intentional testing or improper authentication attempts rather than an external attack.

Incident Severity

Medium

Response Actions Taken

- Alert reviewed and validated
- Authentication logs analyzed
- Threat intelligence checks performed
- No containment action required at this stage

Recommendations

- Monitor SSH authentication attempts for recurrence
- Enforce strong authentication policies
- Consider enabling key-based SSH authentication
- Implement account lockout or fail2ban if repeated failures continue

---

Incident Status

Closed – Monitoring Recommended
