Security Operations Center (SOC) - Triage Report

1. Alert Identification

- **Alert ID: 1767808061.2639867**
- **Timestamp: Jan 07 17:47:39**
- **Agent Name: kkk**
- **Agent ID: 001**

---

2. Alert Technical Details

Field	Value
Rule Level	10 (High Severity)
Rule ID	2502
MITRE ATT&CK ID	T1110 (Brute Force)
MITRE Tactic	Credential Access
Log Location	journald

Full Log	Jan 07 17:47:39 kkk-VMware-Virtual-Platform sshd[10466]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1

---

3. Triage Documentation Table

Alert ID	Description	Source IP	Target	Severity	Analyst Verdict
1767808061.2639867	SSH brute-force authentication failure	127.0.0.1	kkk-VMware-Virtual-Platform	Medium	True Positive

---

4. Analyst Triage Decision & Reasoning

Verdict: True Positive

Detailed Reasoning:

- Authentication Activity: The system recorded multiple failed attempts within a short window, as evidenced by the "PAM 2 more authentication failures" log entry.
- Brute-Force Confirmation: The alert triggered Rule ID 2502, which specifically flags repeated authentication failures.
- Source Analysis: The rhost is identified as 127.0.0.1, indicating that the failed login attempts are originating from the local host itself.
- Analyst Decision: This is a True Positive because real failed logins occurred. The severity is classified as Medium because while the activity is suspicious, it is confined to a local source and no successful login was observed**.**