

Security Operations Center (SOC) - Triage Report

1. Alert Identification

- Alert ID: 1767811589.252398
- Timestamp: 2026-01-07 18:46:29
- Agent Name: alpha-VMware-Virtual-Platform
- 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 | /var/log/auth.log |
| Full Log | 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 |
|----------|--|-----------|---------------------|----------|-----------------|
| 003 | SSH brute-force authentication failure | 127.0.0.1 | VM2 (alpha-VMware) | Medium | True Positive |

4. Analyst Triage Decision & Reasoning

Verdict: True Positive

Detailed Reasoning:

- **Authentication Activity:** The logs explicitly show multiple failed login attempts (`rule.firedtimes: 8`) via SSH.
- **Verification:** The `full_log` field confirms that the Pluggable Authentication Module (PAM) triggered an alert for repeated authentication failures.
- **Source Analysis:** The source IP is `127.0.0.1` (localhost), suggesting the attempts may be originating from an internal script, a user already on the system, or a misconfigured service on the local machine.
- **Impact Assessment:** While the attempts were unsuccessful (no compromise detected), the activity is confirmed as a real brute-force pattern and not a system glitch, justifying the "True Positive" classification.