SSH Brute Force Attack Detection & Analysis

Incident ID

SOC-SPL-SSH-2026-001

Report Date

25 January 2026

Incident Classification

Unauthorized Access Attempt / Brute Force Attack

Severity Level

High

Status

Closed – Mitigated

Prepared By

PATHAN FARHANA
SOC Analyst – L1

---

1. Executive Summary

This incident report documents the detection and investigation of an **SSH brute force attack** identified using **Splunk SIEM**. The attack involved repeated failed SSH login attempts originating from a single external IP address, followed by a successful authentication attempt, indicating a potential account compromise.

The detection was performed by analyzing **OpenSSH authentication logs** ingested into Splunk. Correlation of failed and successful login events confirmed brute force behavior. Immediate

containment actions were taken to mitigate further risk.

---

2. Incident Overview

Field	Details
Attack Type	SSH Brute Force
Detection Tool	Splunk SIEM
Log Source	OpenSSH Authentication Logs
Affected System	Linux Server
Attack Vector	SSH (Port 22)
Incident Impact	Credential Compromise Risk

---

3. Incident Timeline

Time (UTC)	Event Description
09:10:22	Multiple failed SSH login attempts detected
09:12:45	Failed login threshold exceeded
09:13:10	Successful SSH login after failures
09:15:00	SOC Analyst initiated investigation
09:18:00	Attacker IP identified
09:20:00	Firewall rule applied
09:25:00	Incident closed

---

4. Detection Methodology

Splunk Search Queries Used

Failed SSH Login Detection

```
index=linux_logs "Failed password"
```

Attacker IP & Username Correlation

```
index=linux_logs "Failed password"
| stats count by src_ip user
| sort -count
```

Brute Force Threshold Detection

```
index=linux_logs "Failed password"
| stats count by src_ip
| where count > 10
```

Successful Login After Failures

```
index=linux_logs ("Accepted password" OR "Failed password")
| stats count by src_ip action
```

---

5. Evidence Analysis

Observed Indicators

- Repeated failed SSH login attempts from the same IP
- Targeting of multiple usernames
- High-frequency authentication attempts
- Successful login immediately after failures

Screenshot Evidence

- Raw SSH log events
- Failed login count by IP
- Brute force threshold detection
- Timeline visualization
- Successful login correlation

(Screenshots attached in Appendix A)

---

6. Indicators of Compromise (IOCs)

IOC Type	Value	Description
Source IP	`182.63.140.253`	Brute force attacker
Destination Port	22	SSH
Protocol	TCP	Authentication
Username	Multiple	Credential guessing
Log Signature	"Failed password"	Brute force indicator

---

7. Impact Assessment

Security Pillar	Impact
Confidentiality	High
Integrity	Medium
Availability	Low
Overall Risk	High

Potential Risks:

- Unauthorized system access
- Lateral movement
- Privilege escalation
- Data exfiltration

---

8. Response & Mitigation Actions

Immediate Actions

- Blocked attacker IP at firewall
- Disabled affected user account
- Forced password reset

SOC Actions

- Preserved log evidence
- Documented IOCs
- Updated detection rules

---

9. Root Cause Analysis

The root cause of the incident was:

- Weak password policy
- SSH service exposed to public access
- Absence of login rate limiting

---

10. Recommendations

Short-Term

- Enforce strong password policy
- Enable account lockout after failed attempts
- Disable SSH password authentication

Long-Term

- Implement SSH key-based authentication
- Enable MFA for remote access
- Integrate alerts into SIEM
- Deploy Fail2Ban

---

11. Lessons Learned

- Brute force attacks are easily detectable with proper log analysis
- Correlation between failed and successful events is critical
- SIEM-based monitoring significantly reduces response time

---

12. Conclusion

This incident highlights the importance of centralized log monitoring using **Splunk SIEM**. Early detection and rapid response prevented further compromise. Improved security controls and monitoring rules have been implemented to reduce future risks.

---

13. Appendices

Appendix A – Screenshots

- Raw SSH Logs
- Failed Login Events
- Brute Force Detection
- Timeline Visualization

Appendix B – SPL Queries

- Included in Section 4

Appendix C – Log Source Details

- OpenSSH Authentication Logs