

SOC INCIDENT INVESTIGATION REPORT

Title: Brute Force Attack Detection and Analysis Using Splunk

Analyst: Jacob John

Company Type: IT Services Firm

Date: 08 November 2025

1. Executive Summary

On 25 October 2025, the Security Operations Center (SOC) of the IT Services Firm identified multiple failed authentication attempts against a Windows domain controller. These events were detected through Splunk correlation rules configured to monitor abnormal login behaviors. Upon further investigation, the incident was confirmed to be a brute-force attack originating from an external IP address. No data exfiltration or privilege escalation occurred. The threat was contained, and mitigation steps were implemented.

2. Tools and Frameworks Used

Category	Tool / Framework	Purpose
SIEM	Splunk Enterprise	Log ingestion, parsing, detection, and analysis
Endpoint Logs	Windows Event Viewer	Authentication log collection
Network Analysis	Wireshark	Network packet inspection
Threat Intel	AbuseIPDB / VirusTotal	IP reputation and threat context
Framework	MITRE ATT&CK	Attack technique mapping

3. Incident Description

3.1. Detection Summary

- **Detection Source:** Splunk Correlation Search (Failed Logon Spike Rule)
- **Alert Triggered:** Multiple failed login attempts detected within a short time frame.
- **Event Count:** 142 failed logins within 10 minutes.
- **Source IP:** 45.177.23.61 (external, suspicious)
- **Target Host:** WIN-SRV01 (Domain Controller)
- **Timeframe:** 25 Oct 2025 – 02:05 AM to 02:15 AM IST

3.2. Event Details

Timestamp	Event ID	Account Name	Source IP	Status
2025-10-25 02:05:12	4625	admin01	45.177.23.61	Failed
2025-10-25 02:05:23	4625	admin01	45.177.23.61	Failed
2025-10-25 02:07:44	4625	admin01	45.177.23.61	Failed
2025-10-25 02:10:08	4624	admin01	45.177.23.61	Success

4. Investigation Process

Step 1: Log Retrieval

Splunk collected Windows Security logs from the domain controller through Universal Forwarder agents. Event IDs 4625 (failed logons) and 4624 (successful logons) were filtered for analysis.

Step 2: Query Execution

A search query was executed in Splunk:

```
sourcetype="WinEventLog:Security" EventCode=4625 OR EventCode=4624 | stats count by Account_Name, IPAddress, EventCode
```

The results revealed abnormal login spikes from a single external IP address.

Step 3: Threat Intelligence Lookup

IP **45.177.23.61** was analyzed using **AbuseIPDB** and **VirusTotal**, showing historical brute-force and SSH scanning activity across multiple networks.

Step 4: MITRE ATT&CK Mapping

Tactic	Technique ID	Technique Name
Credential Access	T1110	Brute Force
Initial Access	T1078	Valid Accounts
Defense Evasion	T1070	Indicator Removal on Host

Step 5: Correlation and Verification

Splunk correlation rules confirmed that the login attempts originated externally, targeting administrative accounts. No lateral movement or privilege escalation activity was observed.

5. Findings and Impact Assessment

- Findings:**
- Attack Type: Brute-force authentication attempt.
 - Attack Source: External IP 45.177.23.61.
 - Target Account: admin01.
 - Success Level: Single login succeeded after multiple failed attempts.
 - Privilege Escalation: Not detected.
 - Data Exfiltration: None.

Impact Assessment: | Category | Level | Description | |-----| -----|-----| | System Compromise | Low | Contained early, limited to login attempt | | Business Impact | Medium | Attack targeted administrative credentials | | Risk Level | Medium | Could escalate if persistent attempts succeeded |

6. Mitigation and Recommendations

1. **Enable Account Lockout Policy:** Lock accounts after 5 failed attempts within 10 minutes.
 2. **Implement Multi-Factor Authentication (MFA):** Require secondary verification for all privileged users.
 3. **Restrict External Access:** Limit RDP/SSH access to internal VPN only.
 4. **Blacklist IP Addresses:** Block known malicious IPs at the firewall level.
 5. **Continuous Monitoring:** Maintain real-time alerting for login spikes.
 6. **Patch Management:** Ensure OS and SIEM agents are up to date.
-

7. Conclusion

The SOC successfully identified and contained a brute-force attack targeting an administrative account. Proactive Splunk correlation searches enabled early detection before system compromise. Strengthening authentication policies and implementing MFA will significantly reduce similar threats in the future.

Final Status: Incident Contained – No Further Malicious Activity Observed.

8. Appendix

Sample Log Snippet:

Event ID: 4625
Account Name: admin01
Failure Reason: Unknown user name or bad password
Source Network Address: 45.177.23.61
Logon Type: 3 (Network)

IP Reputation Lookup Summary:

- **45.177.23.61** → Reported for RDP brute force (score: 98/100)

References:

- MITRE ATT&CK v14 – Credential Access: Brute Force (T1110)
- Microsoft Event ID documentation
- Splunk Security Essentials playbooks