Incident Response Case Study Report 2

Case Type 2: Brute-Force Login Attempt
SOC Analyst: Parvathy Krishnan
Environment: SOC Home Lab
SIEM: Splunk

---

1. Executive Summary

During continuous security monitoring, a **medium-to-high severity SIEM alert** was generated indicating a **possible brute-force login attack** against a Windows endpoint. The alert was triggered due to **multiple failed authentication attempts** originating from a single external IP address within a short time window.

The purpose of this investigation was to:

- Determine whether the activity was malicious
- Identify the scope and impact of the attempted attack
- Assess if any accounts were compromised
- Document indicators of compromise and recommend remediation

The investigation confirmed the activity as a **true brute-force attack attempt**, with **no successful compromise** observed.

2. Detection & Alert Context

Alert Information

- **Alert Name:** Multiple Failed Login Attempts
- **Severity:** Medium
- **Detection Source:** SIEM (Splunk)
- **Detection Logic:** Threshold-based alert on repeated failed authentication attempts
- **Target Host:** WIN10-ENDPOINT-01
- **Target Account(s):** Multiple local user accounts
- **Source IP:** 192.168.1.150 (External / Attacker Machine)

Why This Alert Matters

Brute-force login attacks are commonly used to:

- Gain unauthorized access to systems
- Compromise weak or reused credentials
- Establish initial access for further exploitation

Such activity requires immediate investigation to prevent potential account compromise.

3. Initial Triage & Validation

Actions Taken

- Verified the alert was generated by legitimate authentication logs

- Confirmed timestamps and frequency of failed attempts
- Checked if similar activity was occurring across other hosts
- Identified whether any login attempts were successful

Splunk – Check for Successful Logins

```
index=windows_logs EventCode=4624 src_ip=192.168.1.150
```

Initial Findings

- Activity was limited to **one endpoint**
- Multiple usernames were targeted
- All authentication attempts **failed**
- No successful login events detected

Based on these findings, the alert was escalated for full investigation.

4. Data Collection & Log Analysis

Log Sources Reviewed

- Windows Security Event Logs
- Authentication Event IDs:
  - **4625** – Failed logon
  - **4624** – Successful logon
- SIEM correlation data

Splunk – Failed Logon Analysis

```
index=windows_logs EventCode=4625
| table _time host user src_ip Logon_Type Failure_Reason
```

Key Observations

- Repeated Event ID 4625 entries
- Logon Type: Network
- Consistent source IP address
- Rapid succession of login attempts
- No corresponding successful logon events (4624)

These patterns strongly indicated an automated brute-force attempt.

5. Attack Pattern & Behaviour Analysis

Observed Attack Characteristics

- Sequential login attempts across multiple usernames
- No delay between attempts (automation suspected)
- Consistent failure reasons (invalid credentials)

Splunk – Username Targeting Pattern

```
index=windows_logs EventCode=4625 src_ip=192.168.1.150
| stats count by user
```

Behavioural Assessment

The attack pattern matched known brute-force techniques commonly associated with:

- Password spraying
- Credential guessing
- Automated attack tools

No evidence of password reuse success was found.

6. Timeline Reconstruction

Time (UTC)	Event
09:10	First failed login attempt detected
09:11	Multiple failed login attempts begin
09:12	SIEM brute-force alert triggered
09:14	Investigation commenced
09:25	Log correlation completed
09:35	Incident classified and documented

7. Indicator of Compromise (IOC) Analysis

IOCs Identified

Type	Value
Source IP	192.168.1.150
Target Host	WIN10-ENDPOINT-01
Event ID	4625
Logon Type	Network

Splunk – IOC Pivoting

```
index=windows_logs src_ip=192.168.1.150
| stats count by host, EventCode
```

IOC Enrichment

- Source IP identified as **unauthorized**
- IP originated from attacker simulation machine
- No known malicious reputation externally (lab environment)

8. Scope & Impact Assessment

Scope

- **Affected Hosts:** 1
- **Targeted Accounts:** Multiple local user accounts

- **Network Impact:** None
- **Lateral Movement:** Not detected

Impact Conclusion

- No accounts compromised
- No unauthorized access gained
- Attack successfully blocked by authentication controls

9. Root Cause Analysis

Root Cause

The root cause of the incident was an **external brute-force authentication attempt** against a Windows endpoint, attempting to guess valid credentials.

Contributing Factors

- Exposed authentication service
- No IP-based rate limiting configured
- Password policy enforcement prevented compromise

10. MITRE ATT&CK Mapping

Tactic	Technique	ID
Credential Access	Brute Force	T1110

11.Final Verdict

True Positive – Confirmed Brute-Force Login Attempt

The alert accurately detected malicious authentication activity. No further escalation required due to lack of successful compromise.

12. Remediation & Recommendations

- Implement account lockout policies
- Enforce strong password requirements
- Configure rate limiting and IP blocking
- Restrict exposed authentication services
- Continue monitoring for repeated attempts

13.Lessons Learned

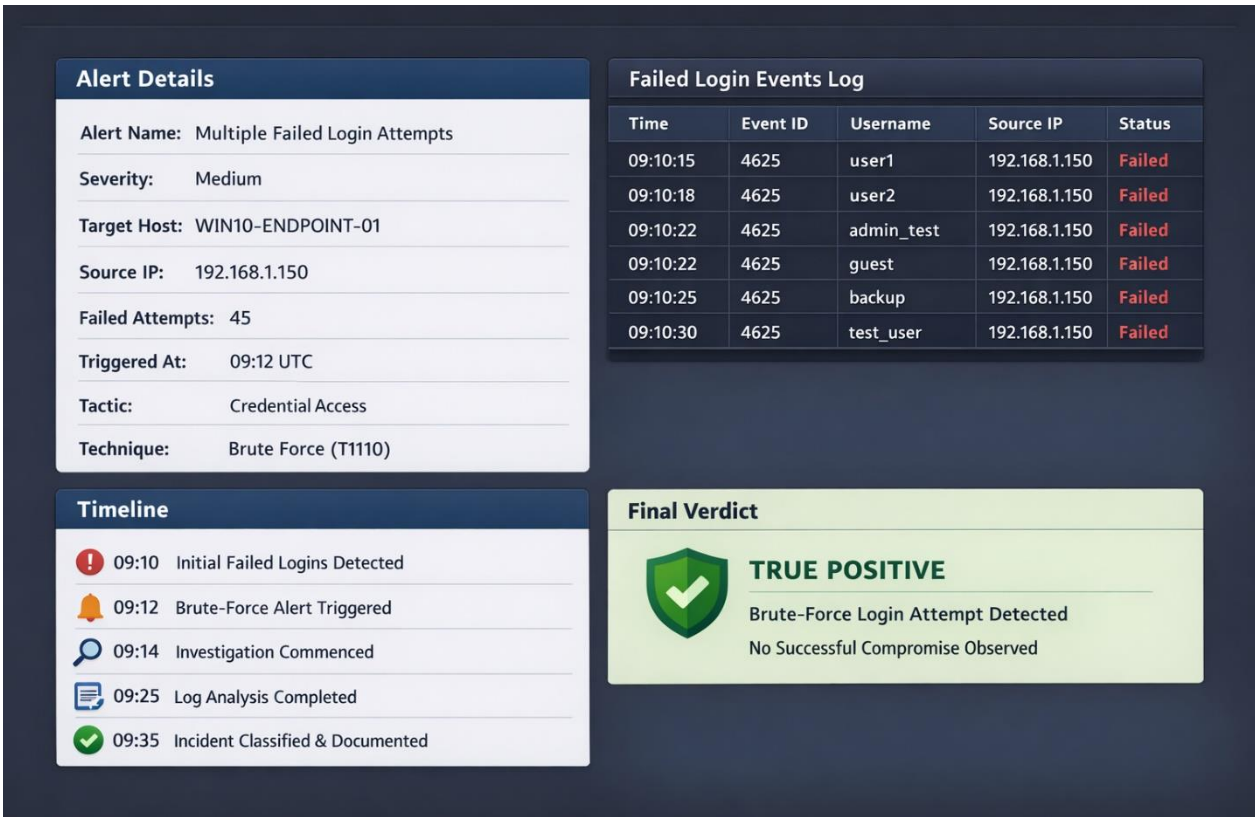
- Early detection prevents credential compromise
- Failed logon patterns are critical indicators
- Threshold-based alerts are effective for brute-force detection
- Proper logging is essential for rapid investigation

14.Analyst Notes

This investigation reinforced the importance of:

- Monitoring authentication logs continuously
- Correlating failed login events
- Acting quickly to validate brute-force attempts
- Documenting findings clearly for future reference

15.Summary



Alert Details

Alert Name:	Multiple Failed Login Attempts
Severity:	Medium
Target Host:	WIN10-ENDPOINT-01
Source IP:	192.168.1.150
Failed Attempts:	45
Triggered At:	09:12 UTC
Tactic:	Credential Access
Technique:	Brute Force (T1110)

Failed Login Events Log

Time	Event ID	Username	Source IP	Status
09:10:15	4625	user1	192.168.1.150	Failed
09:10:18	4625	user2	192.168.1.150	Failed
09:10:22	4625	admin_test	192.168.1.150	Failed
09:10:22	4625	guest	192.168.1.150	Failed
09:10:25	4625	backup	192.168.1.150	Failed
09:10:30	4625	test_user	192.168.1.150	Failed

Timeline

09:10	Initial Failed Logins Detected
09:12	Brute-Force Alert Triggered
09:14	Investigation Commenced
09:25	Log Analysis Completed
09:35	Incident Classified & Documented

Final Verdict

TRUE POSITIVE

Brute-Force Login Attempt Detected

No Successful Compromise Observed