SOC Use Case Investigation Report

UC-001: Brute Force Detection (SOC L1 Workflow)

Author: Abishek V
Date: 22 January 2026

Series: SOC Use Case Playbook Series (50 Use Cases)

Purpose

This report documents a complete SOC L1 approach for handling a brute force alert: how it is detected, triaged, investigated, classified (TP/BTP/FP), and documented using a structured playbook.

Environment Type	Home SOC Lab (VirtualBox VMs)
Log Sources	Windows Security Logs + Sysmon (optional)
SIEM View	SIEM-style triage + evidence checklist
Target OS	Windows 10 (victim endpoint)
Attacker OS	Kali Linux

This document is written in SOC operational style for portfolio and investigation practice.

1 Use Case Summary

Use Case ID:	UC-001
Use Case Name:	Detecting Brute Force Attacks
Category:	Authentication / Account Attack
SOC Tier:	L1 (Alert triage + investigation + escalation)
Severity Guideline:	Medium → High (based on account type and success login)

Short description: A brute force alert triggers when a single account (or multiple accounts) receives repeated failed login attempts within a short time window. The L1 objective is to quickly determine if this is user error/noise or a real attack attempt, and most importantly confirm whether the attacker succeeded.

2 Scenario (Lab Story)

To keep this investigation realistic, the following lab scenario was used:

- **Victim endpoint:** Windows 10 VM
- **Endpoint user:** `clair`
- **Attacker machine:** Kali Linux VM
- **Attacker username:** `kali`

Lab IP Addressing (Trusted internal range)

- Windows 10 endpoint: `192.168.56.110`
- Kali attacker: `192.168.56.120`
- SIEM/Log collector: `192.168.56.100` (optional)

SOC note: Even though this is a lab, the same checklist applies in production. Brute force alerts are high-volume alerts in SOC, so the investigation must be fast, evidence-driven, and documented clearly.

3 Telemetry and Evidence Requirements

3.1 Primary telemetry

- **Windows Security Event Logs**

3.2 Key Windows Event IDs

4625	Failed logon attempt
4624	Successful logon
4740	Account locked out (if policy exists)

3.3 Evidence expected during brute force

Typical evidence seen during brute force investigation:

- A burst of **4625** events within a few minutes
- Common source IP repeatedly attempting authentication

- Same username targeted OR multiple usernames targeted (spray)
- Potential lockouts if account policy is configured

4 Detection Logic (How the Alert is Triggered)

4.1 Detection objective

Generate an alert when failed logins exceed a threshold within a short time window.

4.2 Simple SOC threshold baseline

- **10 failed logins within 5 minutes** for a normal user
- **5 failed logins within 5 minutes** for privileged/admin accounts

4.3 What the SOC alert should include

- Target username: `clair`
- Source IP: `192.168.56.120`
- Target host: `192.168.56.110`
- Failure count + time range
- Logon type + failure reason/status (if available)

5 SOC L1 Playbook (Step-by-step Analyst Workflow)

This section documents the exact L1 flow used to handle the alert.

5.1 Phase A: Triage (2–5 minutes)

1. Open the brute force alert and confirm:
   - alert timestamp
   - number of failed attempts
   - user/host/IP included in the alert
2. Check for duplication:
   - verify if there is already an open ticket for the same user/IP/time window
3. Quick risk judgement:
   - Is the target an admin/service account?
   - Is the target a server/DC?
   - Is the source internal or external?

5.2 Phase B: Investigation (10–20 minutes)

Step 1: Attack pattern identification

- If a single user is targeted: brute force attempt
- If many users are targeted: password spraying (higher risk)

Step 2: Success check (mandatory)

This is the most important step.

- Search for **4624 (successful logon)** after the burst of 4625 failures.

- If a 4624 exists after failures, treat this alert as **potential compromise** and escalate.

Step 3: Source validation

- Validate the source IP: `192.168.56.120`
- Confirm whether source is:
  - known internal system / scanner (benign)
  - unknown internal workstation (suspicious)
  - external address (suspicious)

Step 4: Impact confirmation

- Confirm if the account was locked (4740)
- Confirm whether attempts stopped naturally or continued
- Check whether other accounts were attacked from same IP

6 Quick Evidence Timeline (Example)

Time (IST)	Event ID	Entity	Observation
09:42:10	4625	clair / 192.168.56.120	Failed logon attempt begins
09:42:10–09:44:55	4625 (x28)	clair / 192.168.56.120	Burst of failed logons (high frequency)
09:45:01	4740	clair	Account lockout (policy enabled)
09:45:20	–	–	Attempts stopped after lockout

Outcome (This run): No successful login (4624) was observed after the failed attempts. Based on the evidence, the activity was classified as **True Positive (Brute Force attempt)** but **no confirmed compromise**.

7 False Positive / Benign Checklist

Before closing, L1 must validate common benign reasons:

- user typing wrong password repeatedly
- password manager using an old password
- cached credentials repeatedly failing (email/mobile client)
- internal scanner activity

8 Verdict Criteria

8.1 True Positive (TP)

- High-volume 4625 failures in short window
- Repeat attempts from same source
- No legitimate reason identified

8.2 Benign True Positive (BTP)

- confirmed scanner/test activity OR confirmed user behaviour with supporting evidence

8.3 Critical escalation condition

If a **4624 success** appears after the failed attempts, L1 should escalate immediately as suspected account compromise.

9 SOC Response Actions (Recommended)

In a real SOC environment, the recommended actions include:

- block the attacking source IP at firewall/VPN (if external and confirmed malicious)
- reset password for the impacted user (`clair`)
- enforce MFA on the account
- review exposure: RDP/VPN portals, lockout policy, password policy

10 Ticket Documentation (SOC Notes Template)

Ticket Title: UC-001 Brute Force Attempts – user clair – src 192.168.56.120
Severity: Medium (elevate to High if admin/service account targeted)
Verdict: True Positive (attempted brute force)
Compromise status: Not confirmed (no 4624 success observed)

Example analyst notes (human SOC style)

- Observed 28 failed logon attempts (Event ID 4625) targeting user `clair` from source IP `192.168.56.120` within approximately 3 minutes.
- Reviewed for successful logons (Event ID 4624) after the failure burst; none identified.
- Account lockout observed (Event ID 4740). Attempts stopped after lockout.
- Classified as brute force attempt. Recommended password reset and MFA enforcement.

End of Report — UC-001