SOC Incident Response Report

Title: Brute Force Attack Detection & Investigation
Environment: Lab Simulation (Controlled)
Prepared by: Preetha Paindupal Ramadoss

Executive Summary

A simulated brute-force attack targeted the user account **TestAccount** on the Active Directory Domain Controller **DC01**.
Splunk SIEM generated alerts for **failed login attempts (4625)** and an **account lockout (4740)**.
The attack originated from **Kali Linux** with ~200 login attempts in 2 minutes.
This was a lab exercise; no production systems were affected and everything was performed in a controlled environment.

Key Outcomes:

- No successful authentication occurred
- No lateral movement or data compromise detected
- Account lockout and SIEM detection effectively contained the attack
- Lessons learned were documented, and SOC workflows and preventive controls were updated

This exercise demonstrates the **full NIST 800-61 Incident Response lifecycle**, including Preparation, Detection & Analysis, Containment/Eradication/Recovery, and Post-Incident Review.

1. Incident Details

Field	Information
Incident Title	Brute Force Attack Detection – Windows Authentication
Incident ID	IR-2025-SAMPLE-001
Detected By	Splunk SIEM – Authentication Failure Alert, Account Lockout
Source System	Kali Linux Attacker
Target System	Domain Controller (DC01)
Target Account	TestAccount
Classification	Unauthorized Access Attempt
Severity Level	Medium (No compromise)
MITRE ATT&CK Technique	**T1110 – Brute Force**

2. NIST 800-61 IR Phases Mapping

Phase	Actions / Lab Alignment
Preparation	Lab setup, Splunk deployment, AD lockout policies, password/MFA policies configured
Detection & Analysis	SIEM alerts on 4625 & 4740; log analysis; source IP and target account identified; MITRE T1110 mapped
Containment	AD account automatically locked; attack source identified; verified activity ceased
Eradication & Recovery	Password reset, account unlocked, no persistence found, SIEM thresholds updated, IP block rules added
Post-Incident Activity / Lessons Learned	Lessons documented, runbooks updated, preventive controls strengthened

3. Detection Summary

- **Alert 1 – Brute Force Attempt Detected**: >200 failed login attempts (4625) in <2 minutes
- **Alert 2 – Account Lockout Event**: Event 4740 triggered automatic lockout
- Attacker Host: Kali Linux machine (internal lab attacker)
- Target account: TestAccount

4. Analysis & Investigation Findings

Field	Result
Source IP / Host	Kali Linux
Target Account	TestAccount
Event IDs Observed	4625 (failures), **No 4624 (success)**, 4740 (lockout)
Attempt Rate	~200 attempts in 2 minutes
Attack Method	Hydra password brute-force (simulated lab attack)
Lateral Movement	None detected
Persistence Indicators	None found

Conclusion: Attack unsuccessful; AD lockout prevented compromise.

5. Containment Actions

- AD account automatically locked (4740)
- Analyst verified activity cessation
- No system isolation required

6. Eradication & Recovery Actions

- Password reset and unlocked TestAccount
- Verified no persistence mechanisms
- Updated Splunk SIEM alert thresholds
- Added preventive firewall/IP rules

---

7. Impact Assessment

- No unauthorized access
- No lateral movement
- No data compromise
- Fully contained

Impact Level: Low

---

8. Lessons Learned

Technical Lessons

- Effective log forwarding is essential
- SIEM thresholds must reflect real attack behavior
- Account lockout policies mitigate brute-force attacks
- Event ID correlation strengthens detection accuracy
- No successful logons confirmed attack containment

Operational / SOC Process Lessons

- SOC analysts must validate alerts
- Internal IPs can still represent threat sources
- Runbooks streamline SOC workflows

Configuration & Policy Lessons

- Strong password policies reduce brute-force success
- MFA significantly enhances security
- SIEM dashboards improve authentication visibility

Strategic Lessons

- Automated attacks require behavioral detection
- Defense must be multi-layered
- Post-incident hardening improves overall resilience

---

9. Final Status

Incident Closed – No compromise detected.
The brute-force attempt was unsuccessful and contained by AD lockout and SIEM detection.
Security controls, SOC workflows, and runbooks have been updated to strengthen future resilience.

References

All supporting steps, screenshots, and lab documentation for this use case are available in the GitHub repository: Brute-Force Detection Project Github Link