SIEM Log Analysis — Brute Force Attack Investigation

Author: Alexander T. Ramos | Date: 2025-10-04 | Case ID: SOC-2025-001

1. Summary

Splunk generated a “Multiple Failed Login Attempts” alert from a domain controller. Analysis of Event ID 4625 logs revealed repeated failed logins for the 'admin' account, originating from the same IP. A subsequent successful login (4624) occurred minutes later followed by new account creation (4720).

2. Log Data Extracts

```
EventCode: 4625
Account Name: admin
Source Network Address: 192.168.1.45
Failure Reason: Unknown user name or bad password
Logon Type: 3
Time: 2025-10-02 09:32:44
```

```
EventCode: 4624
Account Name: admin
Source Network Address: 192.168.1.45
Logon Type: 10
Time: 2025-10-02 09:35:06
```

```
EventCode: 4720
A user account was created.
New Account: backup_admin
Creator: admin
Time: 2025-10-02 09:36:12
```

3. Timeline of Events

Time (PST)	Event ID	Description	Source IP	Outcome
09:32	4625	Failed login attempt (x9)	192.168.1.45	Failed
09:35	4624	Successful admin login	192.168.1.45	Success
09:36	4720	New admin user created	192.168.1.45	Success

4. Technical Findings

```
- Attack Type: Brute Force → Privilege Escalation
- Impacted Account: admin
- Malicious IP: 192.168.1.45
- Event IDs: 4625, 4624, 4720
- Detection Source: Splunk correlation rule 'Multiple Failed Logons'
```

5. Analysis

The attacker executed a brute-force attack using repeated password attempts until successful authentication. Upon success, they created a privileged account 'backup_admin' to maintain persistence. MITRE ATT&CK; Mapping: T1110: Brute Force T1136: Create Account T1078: Valid Accounts

6. Recommendations

```
- Implement account lockout after 5 failed attempts.
- Restrict RDP access via firewall rules.
- Review administrative account privileges and disable unused ones.
- Deploy MFA for all privileged users.
- Enhance SIEM rule to auto-escalate repeated 4625 events and notify Tier 2.
```

7. Lessons Learned

- Adjust Splunk alert thresholds for failed logons to detect brute-force earlier. - Document detection response workflow for Tier 1 analysts. - Increase monitoring on administrative account changes and account creation events.

Portfolio: GitHub Repo (replace with your repo URL) | LinkedIn: Your LinkedIn (replace with your profile URL)