SOC Incident Report – Brute Force Authentication Attempt

Date: 01/05/2026
Prepared By: Danial
SIEM Tool: Splunk Enterprise
Severity: High
Status: Closed (Simulated Lab)

Summary

A brute-force authentication attempt was detected on a Windows endpoint through monitoring of Windows Security Event Logs using Splunk SIEM. Multiple failed login attempts occurred within a short time window. No successful compromise was observed.

Detection Details

- **Log Source:** Windows Security Event Log
- **Event ID:** 4625 (Failed Logon)
- **Detection Method:** SIEM alert based on failed login threshold

SPL Query Used:

```
index=* EventCode=4625
| stats count by Account_Name
| where count > 5
```

Evidence

- Repeated Event ID 4625 entries
- Multiple failed authentication attempts against a single account
- Automated alert triggered in Splunk

Impact Assessment

- **Attack Type:** Credential access attempt
- **Successful Login:** No
- **System Compromise:** No

MITRE ATT&CK Mapping

- **Tactic:** Credential Access
- **Technique: T1110 – Brute Force**

Response & Mitigation

- Monitor authentication failures
- Enforce account lockout policies
- Implement multi-factor authentication (MFA)

Conclusion

The Splunk SIEM successfully detected suspicious authentication behavior and generated an alert, demonstrating effective log monitoring and detection capabilities.