SOC Incident Response Report

Prepared by: Sachin Madhumitha Sree D
Date: 10-June-2025
SIEM Tool Used: Splunk (Free Trial Version)

1. Executive Summary

On June 10, 2025, a brute-force attack was detected targeting the admin account on AuthServer01. The attacker gained access through repeated failed login attempts, escalated privileges, accessed a sensitive financial report, and initiated an outbound connection to an external IP. The SOC team detected the anomaly via the SIEM (Splunk) and initiated an incident response protocol to contain and remediate the threat.

2. Incident Details

- **Incident ID:** IR-2025-001
- **Detection Time:** 10-June-2025, 01:13 UTC
- **Detection Source:** SIEM Alert (Splunk)
- **Affected System:** AuthServer01
- **Business Impact:** Potential exposure of confidential financial data

3. Timeline of Events

01:13:20 — Multiple failed login attempts detected (Event ID: 4625)

01:13:45 — Successful login to `admin` account (Event ID: 4624)

01:14:10 — Privilege escalation activity performed (Event ID: 4672)

01:15:20 — Sensitive file accessed: /finance/reports/Q2_Confidential.pdf

01:16:55 — Outbound connection to external IP `203.0.113.10` using HTTPS (Event ID: 5156)

4. Indicators of Compromise (IOC)

- **Attacker IP:** 185.22.55.91
- **Destination IP (exfiltration server):** 203.0.113.10
- **Targeted File:** Q2_Confidential.pdf
- **Account Compromised:** admin

5. Incident Classification

- **Type:** Unauthorized Access and Data Exfiltration
- **Category:** Category 2 — Threat to Sensitive Data
- **Severity:** Critical
- **Threat Actor:** External (Unknown)

6. Root Cause Analysis

The attack succeeded due to a weak password on the `admin` account and the absence of Multi-Factor Authentication (MFA). The attacker leveraged brute-force methods to gain access, which was not blocked due to lack of login rate-limiting or account lockout policies.

7. Forensic Investigation

- Reviewed Splunk logs (Event IDs: 4625, 4624, 4672, 5156)
- Verified IP logs and file access trails
- Found no signs of lateral movement to other systems
- Confirmed single-system compromise with outbound exfiltration activity

8. Remediation Actions

- Blocked IP `185.22.55.91` at the firewall
- Reset all admin credentials
- Enabled MFA on privileged accounts
- Applied account lockout policy after 5 failed attempts
- Reviewed access control permissions and hardened the server
- Conducted a malware scan and integrity verification

9. Damage and Cost Assessment

- **Data Exposure:** Access to confidential quarterly report
- **Data Loss:** None confirmed
- **Estimated Cost:** ~$8,000 (investigation + remediation time)

10. Lessons Learned and Recommendations

- Enforce stronger password policies
- Deploy MFA across all user accounts
- Update SIEM alerting rules for faster brute-force detection
- Schedule quarterly penetration testing
- Improve internal awareness and IR response playbooks

11. Evidence Preservation

- Archived logs from SIEM
- Exported screenshots of key events
- Timeline and session IDs recorded
- Stored forensic data for legal and audit use