**Incident Report- Brute Force Login Attempts**

Date: September 28, 2025

Time: 9:55AM EST and 12:50PM EST

Prepared by: Singh H.- SOC Analyst

Incident ID: INC-001

1. **Executive Summary**:

On September 28, 2025, multiple failed login attempts were detected from a single external IP address- 203.0.113.77. The attack pattern indicated a brute-force attempt targeting the admin account. Defensive actions included monitoring the attack source and preparing to block the IP if activity persisted. No successful compromise was observed.

1. **Incident Details**:

* **Type of Incident:** Brute Force Attack
* **Date:** September 28, 2025
* **Time Detected:** 09:55AM EST and 12:50PM EST
* **Source:** IP 203.0.113.77
* **Target:** User admin account on system the Macintosh Server (Macbook)
* **Indicators:**
  + 225 failed login attempts in the first attack at 09:55AM EST
  + 15 failed login attempts in the second attack at 12:50PM EST
  + Event logs from Elasticsearch/Kibana (screenshot attached)

1. **Impact Analysis**:

 **Status:** Contained (no compromise detected)

 **Affected Accounts:** None successfully breached

 **Business Impact:** Low (detected in a lab/test environment, no production assets affected)

1. **Response Action Taken**:

 Monitored failed login activity in Kibana dashboard

 Correlated activity to a brute-force pattern

 No escalation required

1. **Recommendations**:

* Implement **IP blocking for IP address: 203.0.113.77**
* **Rate limiting** for repeated failed login attempts- no more than 3 attempts per account
* Enable **Multi-Factor Authentication (MFA)** for privileged accounts
* Add **alert rules in Kibana** to notify SOC staff when login failures exceed a threshold

1. Attachments:

Screenshot from Kibana Dashboard

**Bar Graph**: Authentication Outcomes Over Time:

A graph with numbers and a number of days

AI-generated content may be incorrect.

**Pie Chart**: Authentication Attempts by Source IP

A red circle with numbers and a number of percentages

AI-generated content may be incorrect.

**Screenshot of Log Table- Detailed Table in the attached .xlsx file**:

A screenshot of a computer

AI-generated content may be incorrect.