Incident Report – Brute Force Attack Detection

1. Executive Summary

This report documents the detection of a potential brute-force attack identified through security event logs. The investigation highlights patterns of repeated failed login attempts followed by a successful login, suggesting possible unauthorized access.

2. Incident Details

Field	Details (Fill In)
Date & Time Detected	
Detected By	SIEM (Splunk / Sentinel / Elastic)
Event IDs	4625 (Failed Login), 4624 (Successful Login)
Affected User/Account	
Source IP Address	
System/Server Impacted	

3. Investigation Findings

Analysis of the security logs revealed multiple failed login attempts from the same source IP address within a short timeframe, followed by a successful login. This behavior is consistent with brute-force attack patterns.

4. Impact Assessment

If successful, this attack could provide unauthorized access to the affected system. Potential consequences include data theft, privilege escalation, or further compromise of the corporate network.

5. Recommended Actions

1. Block or monitor the identified source IP address.
2. Enforce Multi-Factor Authentication (MFA) for the affected account.
3. Reset the compromised user credentials.
4. Review and harden password policies to prevent weak credentials.
5. Continue monitoring for similar suspicious activities.

6. Lessons Learned

This incident highlights the importance of proactive monitoring, effective password policies, and layered defenses such as MFA. Maintaining robust detection rules in the SIEM is crucial for timely identification of brute-force attempts.