Incident Response Report – Task 16

By : NROUPSINH GOHIL

1. Incident Summary

On 13/02/2026, multiple failed login attempts were detected on the local system. The activity indicated a possible brute-force attack targeting a user account.

2. Detection

The incident was identified by reviewing Windows Security Logs (Event ID 4625) Multiple failed login attempts were observed within a short time period.

3. Incident Classification

- Type: Brute Force Attack Attempt
- Severity: Medium
- Affected System: Local machine
- Target: User account

4. Containment Actions

- Account temporarily locked
- Password reset performed
- Login attempt monitoring enabled
- Account lockout policy verified

5. Eradication

- Verified no successful unauthorized login
- Reviewed system for unusual processes
- Confirmed system integrity

6. Recovery

- Account restored with strong password
- Monitoring continued for suspicious activity

7. Root Cause Analysis

The incident occurred due to multiple incorrect login attempts. The system lacked strict account lockout enforcement before multiple failures.

8. Preventive Measures

- Enable MFA
- Enforce strong password policy
- Configure automatic account lockout
- Continuous log monitoring