CYBER SECURITY INTERNSHIP

Task 16: Incident Response & Security Breach Simulation

1. Introduction

This report presents a simulated security incident involving repeated failed login attempts and unauthorized access attempts detected through system authentication logs. The objective is to demonstrate practical understanding of incident response procedures.

2. Incident Description

A suspicious pattern of multiple failed login attempts was observed on a Linux system. The logs indicated repeated authentication failures from a specific IP address, suggesting a possible brute force attack.

3. Incident Classification

- Attack Type: Brute Force Attack
- Target: User authentication system
- Severity Level: Medium to High (due to repeated login attempts)
- Impact: Risk of unauthorized account access

4. Incident Response Phases

- Identification: Detected abnormal login failures in system logs.
- Containment: Blocked suspicious IP address and temporarily locked affected account.
- Eradication: Reset passwords and removed unauthorized access attempts.
- Recovery: Restored system access with stronger authentication controls.
- Lessons Learned: Recommended multi-factor authentication and log monitoring.

5. Incident Timeline

Time	Event
10:15 AM	Multiple failed login attempts detected
10:25 AM	Log analysis confirmed brute force pattern

10:35 AM	Suspicious IP address blocked
10:45 AM	Passwords reset and system monitored
11:00 AM	System restored to secure state

6. Root Cause Analysis

The root cause was weak password protection combined with lack of account lockout policy. Insufficient monitoring allowed repeated login attempts before detection.

7. Recommendations

- Enable multi-factor authentication (MFA).
- Implement account lockout after multiple failed attempts.
- Regular monitoring of system and authentication logs.
- Deploy intrusion detection systems (IDS).
- Conduct regular security awareness training.