🔐 Task 16 – Incident Response & Security Breach Simulation

📌 Objective

To simulate a security incident (Repeated Failed Login Attack), analyze logs, classify the incident, contain the threat, remove root cause, restore systems, and document the entire response process.

📄 1️⃣ INCIDENT RESPONSE REPORT

1. Incident Overview

- **Incident Type:** Brute Force Login Attack
- **Target System:** Ubuntu Linux (Test VM)
- **Log Source:** /var/log/auth.log
- **Attack Vector:** Repeated failed SSH login attempts
- **Date of Simulation:** [Enter Date]
- **Severity Level:** Medium to High

---

2. Incident Description

A simulated brute force attack was performed against an SSH service by attempting multiple failed login attempts using incorrect passwords.

The logs showed repeated authentication failures from a suspicious IP address.

---

3. Evidence Collection

🔍 Linux Log Analysis

Command used:

```
sudo cat /var/log/auth.log | grep "Failed password"
```

Sample Log Entries:

```
Feb 26 10:12:01 kali sshd[2145]: Failed password for invalid user admin from 192.168.1.50 port 54321 ssh2
Feb 26 10:12:03 kali sshd[2145]: Failed password for invalid user admin from 192.168.1.50 port 54322 ssh2
Feb 26 10:12:05 kali sshd[2145]: Failed password for invalid user admin from 192.168.1.50 port 54323 ssh2
```

🔎 **Suspicious Indicators Identified:**

- Multiple login failures within seconds
- Same source IP address
- Attempting common usernames (admin, root, user)

---

4. Incident Classification

Category	Classification
Attack Type	Brute Force
Threat Level	Medium (if internal lab) / High (if production)
Affected Service	SSH
Impact	Unauthorized access attempt

---

5. Containment Actions

Immediate actions taken:

✅ **Block Suspicious IP**

```
sudo ufw deny from 192.168.1.50
```

OR

```
sudo iptables -A INPUT -s 192.168.1.50 -j DROP
```

✅ **Lock Target Account**

```
sudo passwd -l admin
```

---

6. Eradication (Removing Root Cause)

- Installed and configured Fail2Ban
- Changed SSH port
- Disabled root login

- Enforced strong password policy

Install Fail2Ban:

```
sudo apt install fail2ban
```

---

7. Recovery

- Restarted SSH service
- Verified no active malicious sessions
- Monitored logs for additional suspicious activity

```
sudo systemctl restart ssh
```

---

8. Lessons Learned

- Weak authentication mechanisms are vulnerable
- Monitoring logs is critical
- Brute force attacks are common
- Preventive controls must be proactive

📜 2️⃣ INCIDENT TIMELINE DOCUMENT

Time	Event
10:10 AM	Suspicious failed login attempts detected
10:12 AM	Log analysis started
10:15 AM	Identified repeated attempts from same IP
10:18 AM	IP address blocked
10:20 AM	Target account locked
10:30 AM	Fail2Ban installed
10:45 AM	System verified and restored
11:00 AM	Incident documentation completed

🛡️ 3️⃣ PREVENTIVE SECURITY RECOMMENDATIONS

1. Enable Multi-Factor Authentication (MFA)
2. Use SSH Key Authentication instead of passwords
3. Install Fail2Ban
4. Enable firewall (UFW)
5. Regular log monitoring
6. Strong password policy
7. Disable root login
8. Use intrusion detection systems

🎯 FINAL OUTCOME

✔ Understood complete incident handling lifecycle
✔ Learned log analysis
✔ Practiced containment techniques
✔ Implemented preventive security controls
✔ Documented incident professionally

🎤 Interview Questions – Answers

❓ What is Incident Response?

Incident Response (IR) is a structured approach used to detect, analyze, contain, eradicate, and recover from cybersecurity incidents.

❓ Phases of Incident Response?

According to National Institute of Standards and Technology (NIST):

1. Preparation
2. Detection & Analysis
3. Containment
4. Eradication

5. Recovery
6. Lessons Learned

❓ Why Containment is Important?

Containment prevents the attack from spreading further and minimizes damage to systems and data.

❓ Role of Logs in Incident Response?

Logs help:

- Detect suspicious activity
- Trace attacker IP
- Build timeline
- Collect digital evidence

Without logs, investigation becomes impossible.