

Task 16: Incident Response & Security Breach Simulation

1. Introduction

Incident response is the process of identifying, managing, and resolving security incidents in an organized manner. A security breach can occur due to unauthorized access, malware infection, or repeated failed login attempts.

This task focuses on simulating a basic security incident and applying proper incident response steps to handle the situation effectively.

2. Objectives

- Simulate a basic security incident
 - Analyze logs to identify suspicious activity
 - Classify the incident
 - Contain the affected system
 - Remove the threat
 - Restore the system to a secure state
 - Document the incident timeline
 - Recommend preventive measures
-

3. Tools Used

- Linux Logs
- Windows Event Viewer

- TheHive (Community Edition – Alternative)
-

4. Incident Simulation

A basic security incident was simulated in a controlled lab environment.

Example scenario:

- Multiple failed login attempts detected
- Unauthorized login attempt from unknown IP
- Suspicious user activity

This simulation helped in understanding how real security incidents occur.

5. Identification of Suspicious Activity

System and authentication logs were analyzed to detect abnormal behavior such as:

- Repeated failed login attempts
- Login attempts at unusual times
- Access from unknown IP addresses

Log analysis helped confirm the presence of suspicious activity.

6. Incident Classification

The incident was classified based on:

- Type of attack (Brute-force attempt)

- Severity level (Medium/High depending on impact)
- Affected system components

Proper classification helps determine the response priority.

7. Containment

The affected account/system was isolated to prevent further damage.

Containment actions included:

- Temporarily locking user account
 - Blocking suspicious IP address
 - Disconnecting affected system from network (if required)
-

8. Eradication

The root cause of the incident was identified and removed.

Actions taken:

- Reset compromised passwords
 - Remove malicious files (if any)
 - Update system patches
-

9. Recovery

After removing the threat, the system was restored to normal operation.

Steps included:

- Re-enabling secure user access
 - Monitoring logs for further suspicious activity
 - Verifying system stability
-

10. Incident Documentation

An incident timeline was created including:

- Date and time of detection
- Description of suspicious activity
- Actions taken for containment
- Remediation steps
- Final resolution status

Documentation is important for auditing and future reference.

11. Preventive Recommendations

To prevent similar incidents in the future, the following measures were recommended:

- Enable multi-factor authentication
 - Implement strong password policies
 - Configure account lockout policies
 - Regular log monitoring
 - Enable firewall and intrusion detection systems
-

12. Conclusion

This task provided practical understanding of incident handling and response procedures. It improved knowledge of log analysis, containment strategies, and proper documentation of security incidents.

RIFAH RESLIN MANIYODAN LATHEEF