Introduction

Incident Response is the process of identifying, analyzing, and responding to security incidents such as unauthorized access or repeated failed login attempts. The main goal is to minimize damage, stop the attack, and restore systems to a secure state as quickly as possible.

Incident Simulation

A basic security incident is simulated to understand real-world attack scenarios.

Example incidents:

- Multiple failed login attempts
- Unauthorized access attempt
- Suspicious authentication behavior

This helps in learning how incidents appear in system logs.

Log Analysis & Detection

System logs are analyzed to detect suspicious activity.

Log sources:

- Linux authentication and system logs
- Windows Event Viewer (Security logs)

Suspicious signs include:

- Repeated failed logins
- Unknown IP addresses
- Login attempts at unusual times

Incident Identification & Classification

After detecting suspicious activity, it is confirmed as an incident.

Incident types:

- Brute-force attack
- Unauthorized access

Severity levels:

- Low
- Medium
- High

Classification helps decide response priority.

Containment

Containment limits the impact of the incident.

Containment actions:

- Lock or disable affected accounts
- Block malicious IP addresses
- Isolate affected systems

Quick containment prevents further damage.

Eradication & Root Cause

The threat is removed and the cause is identified.

Actions include:

- Resetting passwords
- Removing malicious activity
- Applying missing patches

Root cause analysis helps prevent future incidents.

Recovery

Systems are restored to a secure and normal state.

Recovery steps:

- Restore from clean backups
- Verify system integrity
- Monitor systems after recovery

Documentation & Timeline

All actions taken during the incident are documented.

Documentation includes:

- Incident description
- Detection time
- Actions taken
- Resolution time

An incident timeline shows the sequence of events clearly.

Preventive Recommendations

Steps are suggested to avoid similar incidents.

Recommendations:

- Strong password policies
- Account lockout mechanisms
- Regular log monitoring
- Security awareness training

Final Outcome

This task provides practical understanding of incident detection, response, containment, recovery, and documentation. It builds essential skills required to handle real security incidents effectively.

Prepared by:

Megaraj S