WEEK-3

Asad Muhammad Channar

DHC-56

TASK-2

Incident Response Fundamentals:

Required:

- Learn the process of detecting, analyzing, and responding cybersecurity incident.
- Create an incident response plan to handle breaches effectively.

Incident Response Plan

Introduction

An Incident Response Plan (IRP) outlines the steps and procedures for detecting, responding to, and recovering from cybersecurity incidents. The IRP ensures that all stakeholders understand their roles and responsibilities in managing an incident to minimize impact and ensure a swift recovery.

1. Detection

The detection phase involves identifying signs of a cybersecurity incident. Early detection helps reduce the potential damage and allows for faster recovery. Detection can occur through monitoring tools, security alerts, reports from staff, or external sources.

Key Activities:

- Monitor systems and network traffic for abnormal behavior or alerts.
- Review system logs for unauthorized access attempts or unusual activity.
- Respond to alerts generated by intrusion detection systems (IDS) or antivirus software.

2. Response

The response phase is initiated once an incident is detected. The goal is to contain the breach and prevent it from causing further harm. This step includes gathering information to assess the scope of the incident and executing predefined actions to mitigate its effects.

Key Activities:

- Isolate affected systems to prevent further spread of the attack.
- Notify the Incident Response Team (IRT) and initiate communication protocols.
- Conduct an initial investigation to understand the extent and impact of the incident.
- Gather and preserve forensic evidence for further investigation.

3. Recovery

The recovery phase focuses on restoring systems to normal operation and ensuring that vulnerabilities have been addressed. Depending on the nature of the incident, this may involve system reconfigurations, patching, or full data restoration from backups.

Key Activities:

- Restore affected systems from backups.
- Patch security vulnerabilities or reconfigure compromised systems.
- Test systems to verify they are fully operational and free from threats.
- Monitor systems closely for any signs of recurring issues.

4. Roles and Responsibilities

• Incident Response Team (IRT): Responsible for coordinating the entire response process, from detection to recovery.
• IT Department: Assists with technical aspects of the incident, including containment, investigation, and recovery.
• Legal Department: Ensures legal compliance and provides advice on regulatory matters related to data breaches or information disclosure.
• Communication Team: Manages internal and external communication, ensuring timely updates to affected parties and stakeholders.

5. Escalation Procedures

Escalation procedures are in place to ensure that incidents are properly managed based on their severity and potential impact. In cases of critical incidents, higher levels of management and external authorities may be involved.

• Low-Severity Incidents: Handled by the IT department with no further escalation.
• Medium-Severity Incidents: Requires Incident Response Team (IRT) involvement and department head notification.
• High-Severity Incidents: Immediate escalation to executive leadership and external stakeholders if needed.

6. Communication Strategy

A well-structured communication plan is essential during an incident to ensure that accurate and timely information is shared with the appropriate stakeholders, both internally and externally. This helps minimize confusion and maintain trust during a crisis.

• Internal Communication: Keep all team members, including management, informed about the incident status and response progress.
• External Communication: Notify affected parties, regulatory authorities, and customers if necessary.
• Media Communication: Handle public relations carefully, ensuring only authorized personnel provide information to the media.