Week-5

Asad Muhammad Channar

DHC-56

Task-3:

Incident Response Drill

- Simulate a cybersecurity incident and execute the incident response plan developed in Week 4.

Incident Response Drill: Mock Cybersecurity Incident

Introduction

Conducting regular incident response drills is essential to ensure preparedness for real-world cybersecurity incidents. This document outlines the steps taken to simulate a cybersecurity incident and execute the incident response plan developed in Week 4. The mock drill aims to identify gaps in the response plan, improve team coordination, and enhance overall incident response capabilities.

Incident Scenario

A simulated phishing attack has been launched against the organization's email system. Several employees have reported receiving suspicious emails with attachments that, when opened, install malware on their computers. The malware aims to exfiltrate sensitive data and disrupt business operations.

Preparation

1. Define Objectives

1.1 Test the effectiveness of the incident response plan.
1.2 Assess the team's ability to detect, respond to, and recover from a cybersecurity incident.
1.3 Identify areas for improvement in the incident response process.

2. Assemble the Response Team

2.1 Incident Commander: Oversees the response efforts.
2.2 IT Security Team: Investigates and contains the incident.
2.3 Communication Team: Manages internal and external communications.
2.4 Legal and Compliance Team: Ensures adherence to legal and regulatory requirements.

Execution

1. Detection and Analysis

1.1 Monitor email systems for phishing indicators.
1.2 Analyze the suspicious emails and attachments.
1.3 Identify affected systems and users.

2. Containment, Eradication, and Recovery

2.1 Containment: Isolate affected systems to prevent further spread of malware.
2.2 Eradication: Remove the malware from affected systems.
2.3 Recovery: Restore systems to normal operation and monitor for any signs of re-infection.

3. Communication

3.1 Internal Communication: Notify employees about the phishing attack and provide guidance on how to handle suspicious emails.
3.2 External Communication: If necessary, issue a public statement to inform stakeholders about the incident and the steps being taken to address it.

Post-Drill Activities

1. Debriefing

1.1 Conduct a debriefing session with all participants to discuss what went well and what could be improved.
1.2 Document the lessons learned and any gaps identified in the incident response plan.

2. Plan Updates

2.1 Update the incident response plan based on the findings from the drill.
2.2 Ensure all team members are aware of the changes and conduct additional training if necessary.

Appendices

Appendix A: Tools and Resources

1. Email Security Tools: Tools used for monitoring and analyzing email threats.
2. Malware Analysis Tools: Tools used for analyzing and removing malware from affected systems.
3. Communication Templates: Predefined templates for internal and external communication during an incident.