Incident Response Simulation

Scenario: The phishing incident unfolded as an employee unknowingly interacted with a deceptive email, further emphasizing the need for vigilance in scrutinizing incoming messages.

Context: In the interconnected world of our organization, a carefully orchestrated phishing campaign has been unleashed. Employees start receiving seemingly legitimate emails with convincing content, concealing a hidden threat. The aim of the attackers is to exploit unsuspecting individuals and potentially gain unauthorized access to sensitive information.

Objectives:

- Evaluate the incident response team's efficiency in promptly detecting and responding to a phishing attempt.
- Assess the effectiveness of the incident response plan in containing and mitigating the incident.
- Test the coordination and communication among team members during the unfolding crisis.

Scope:

- Focus on the impact of the phishing attempt on employee credentials and potentially compromised information.
- Simulate the potential for the phishing attack to lead to unauthorized access or further cyber threats.

Simulation Flow:

1.Incident Detection:

- Interns assume various roles within the incident response team.
- Simulate the detection of phishing emails using monitoring tools and simulated logs.
- Craft convincing phishing emails with varying levels of sophistication to test the team's discernment.

2.Response Plan Execution:

- Incident Responder triggers the incident response plan upon detecting the phishing attempt.
- Predefined roles and procedures are activated for swift containment and mitigation.
- Isolate affected accounts and initiate password resets to prevent unauthorized access.
- Communication Coordinator informs employees about the phishing attempt and provides precautionary measures.
- IT Support plays a vital role in technical aspects of containment.

3.Forensic Analysis:

- Forensic Analyst conducts a thorough analysis of compromised accounts and systems.
- Identify the entry point of the phishing attempt and trace its origin.
- Simulate the discovery of potential lateral movement or additional malware within the network.
- Gather evidence and logs for a comprehensive post-incident analysis.

4.Post-Incident Assessment:

- Evaluate the efficiency of the response plan and actions taken.
- Assess the coordination and communication among team members during the crisis.
- Analyse the potential impact on business operations and customer trust.

5.Areas for Improvement:

- Identify weaknesses or delays in the response process.
- Pinpoint areas for improvement in detection, communication, and education on phishing awareness.
- Gather feedback from participants to enhance the effectiveness of the simulation.