Task 2: Incident Response Simulation

1. Scenario Creation:

Scenario Outline: A phishing attack has been launched against the company's employees, resulting in several individuals inadvertently disclosing their login credentials to a fraudulent website. As a result, unauthorized access to sensitive company data has been detected.

Context: The company is a medium-sized technology firm with approximately 200 employees. The phishing attack targeted employees across various departments, including finance, human resources, and engineering. The attack occurred during regular working hours, and initial indications suggest that multiple accounts may have been compromised.

Objectives:

- Identify the extent of the unauthorized access and compromised accounts.
- Contain and mitigate the impact of the phishing attack on company systems and data.
- Conduct a thorough forensic analysis to determine the root cause of the incident and prevent future occurrences.
- Communicate effectively with internal stakeholders and external parties, if necessary, to manage the incident.

Scope: The incident response team will focus on investigating the compromised accounts, assessing the potential data exfiltration, and implementing measures to prevent further unauthorized access. The scope includes reviewing system logs, conducting forensic analysis, and implementing remediation measures to address the incident.

2. Incident Detection:

Roles within the Incident Response Team:

- Incident Manager: Oversees the overall incident response process and coordinates communication among team members.
- Technical Analyst: Utilizes monitoring tools and log analysis to identify suspicious activities and determine the scope of the incident.
- Forensic Investigator: Conducts detailed forensic analysis of affected systems and data to determine the root cause of the incident.
- Communication Liaison: Manages communication with internal stakeholders and external parties, providing regular updates on the incident response efforts.

Simulation of Incident Detection: Utilize monitoring tools such as SIEM (Security Information and Event Management) systems, intrusion detection systems (IDS), and endpoint detection and response (EDR) solutions to identify suspicious activities. Analyze system logs, network traffic, and email headers to identify indicators of compromise (IoCs) associated with the phishing attack.

3. Response Plan Execution:

Initiation of Incident Response Plan: Upon detection of the phishing attack, the Incident Manager will activate the incident response plan. The team will assemble, and roles and responsibilities will be assigned based on predefined procedures.

Containment and Mitigation:

- Disable compromised accounts to prevent further unauthorized access.
- Reset passwords for affected users and enforce multi-factor authentication to enhance security.
- Conduct a thorough review of access logs to identify any unauthorized activities and anomalous behavior.
- Implement network segmentation to isolate compromised systems and prevent lateral movement by the attacker.

4. Forensic Analysis:

Performing Forensic Analysis: The Forensic Investigator will conduct a detailed examination of affected systems and data. This includes:

- Analyzing system logs, registry entries, and file system metadata.
- Examining email headers and message contents to trace the source of the phishing emails.
- Identifying any malware artifacts or suspicious files on compromised systems.

Gathering Evidence: Collect relevant evidence and logs to support the forensic analysis and aid in post-incident analysis. This may include:

- Network traffic captures to identify communication with malicious servers.
- System snapshots or memory dumps for volatile data analysis.
- Email server logs to track the propagation of phishing emails within the organization.

5. Post-Incident Assessment:

Review of Response Effectiveness: Evaluate the effectiveness of the response plan and actions taken in containing and mitigating the phishing attack. Identify any shortcomings or areas for improvement in the incident response process, communication protocols, or technical controls.

Lessons Learned: Document lessons learned from the simulation exercise, including strengths and weaknesses of the incident response team's performance. Identify opportunities for enhancing incident response capabilities through additional training, procedural improvements, or technological enhancements.