Task 2: Incident Response Simulation

Scenario Creation:

Scenario Outline: A sophisticated phishing attack has been executed against our company's employees. This has led to several employees unknowingly providing their login credentials to a fraudulent website. Consequently, unauthorized access to sensitive company data has been detected.

Context: Our company is a medium-sized technology firm with a diverse workforce of approximately 200 employees. The phishing attack was not department-specific and targeted employees across various departments, including finance, human resources, and engineering. The attack was strategically launched during regular working hours, and initial indications suggest that multiple accounts may have been compromised.

Objectives: Our primary objectives are to:

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.

Incident Detection:

Roles within the Incident Response Team:

Incident Manager: This role oversees the overall incident response process and coordinates communication among team members.

Technical Analyst: This role utilizes monitoring tools and log analysis to identify suspicious activities and determine the scope of the incident.

Forensic Investigator: This role conducts detailed forensic analysis of affected systems and data to determine the root cause of the incident.

Communication Liaison: This role manages communication with internal stakeholders and external parties, providing regular updates on the incident response efforts.

Simulation of Incident Detection: We will 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. We will 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 immediately 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.

◌ Increase monitoring on all systems to detect any further suspicious activity.

Recovery and Lessons Learned: After the incident has been contained and mitigated, we will focus on recovery and learning from the incident. This includes restoring systems to normal operation, confirming that all threats have been eliminated, and conducting a post-incident review to learn from the incident and improve future response efforts.

4. Forensic Analysis:

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

◌ Analyzing system logs, registry entries, and file system metadata to trace the attacker's activities.

◌ Examining email headers and message contents to trace the source of the phishing emails and understand the attacker's tactics.

◌ Identifying any malware artifacts or suspicious files on compromised systems to understand the tools used by the attacker.

Gathering Evidence: The team will collect all 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 and understand the attacker's network activities.

◌ System snapshots or memory dumps for volatile data analysis to capture the state of the system at the time of the attack.

◌ Email server logs to track the propagation of phishing emails within the organization and identify potential victims.

5. Post-Incident Assessment:

Review of Response Effectiveness: The team will evaluate the effectiveness of the response plan and actions taken in containing and mitigating the phishing attack. This includes identifying any shortcomings or areas for improvement in the incident response process, communication protocols, or technical controls. The goal is to understand what worked well and what needs to be improved.

Lessons Learned: The team will document lessons learned from the simulation exercise, including strengths and weaknesses of the incident response team's performance. This will help identify opportunities for enhancing incident response capabilities through additional training, procedural improvements, or technological enhancements. The lessons learned will be shared with the entire organization to improve overall security awareness and preparedness.

Continuous Improvement:

Updating Incident Response Plan: Based on the lessons learned, the incident response plan will be updated to incorporate new strategies and tactics to deal with similar incidents in the future.

Training and Awareness: Regular training sessions will be conducted for all employees to increase their awareness about phishing attacks and how to respond to them. This will help in reducing the chances of such incidents in the future.

Regular Audits and Drills: Regular audits of the systems will be conducted to identify any potential vulnerabilities. Also, regular incident response drills will be conducted to ensure that the team is well-prepared to handle such incidents.