Nama : Rizqi Hendra Ardiansyah
Kelas : SIB-4C
NIM : 2141762145

Lab - Incident Handling

Objectives

Apply your knowledge of security incident handling procedures to formulate questions about given incident scenarios.

Background / Scenario

Computer security incident response has become a vital part of any organization. The process for handling a security incident can be complicated and involve many different groups. An organization must have standards for responding to incidents in the form of policies, procedures, and checklists. To properly respond to a security incident, the security analyst must be trained to understand what to do and must also follow all of the guidelines outlined by the organization. There are many resources available to help organizations create and maintain a computer incident response handling policy. The NIST Special Publication 800-61r2 is specifically cited in the Understanding Cisco Cybersecurity Operations Fundamentals (200-201 CBROPS) exam topics.

Instructions

Scenario 1: Worm and Distributed Denial of Service (DDoS) Agent Infestation

Study the following scenario and discuss and determine the incident response handling questions that should be asked at each stage of the incident response process. Consider the details of the organization and the CSIRC when formulating your questions.

This scenario is about a small, family-owned investment firm. The organization has only one location and less than 100 employees. On a Tuesday morning, a new worm is released; it spreads itself through removable media, and it can copy itself to open Windows shares. When the worm infects a host, it installs a DDoS agent. It was several hours after the worm started to spread before antivirus signatures became available. The organization had already incurred widespread infections.

The investment firm has hired a small team of security experts who often use the diamond model of security incident handling.

Preparation:

1. Would the organization consider the worm's spread and the resulting DDoS activity as a security incident? Which policies might this breach (e.g., acceptable use policy, incident response policy)?
2. What preventative measures, like employee training or endpoint security, were established before the incident? How effective were these measures?
3. Does the organization have existing protocols for the use of removable media?

Detection and Analysis:

1. What early warning signs (e.g., unusual network traffic patterns, antivirus alerts) could have suggested an issue before the incident?
2. Which specific indicators of compromise (IoCs) should the organization be monitoring (e.g., unusual file access, spikes in CPU usage)?
3. What additional detection tools (e.g., intrusion detection systems, network monitoring tools) could improve the organization’s capability to identify similar incidents in the future?

4. How will the team prioritize this incident compared to other ongoing incidents? What criteria will guide the prioritization?

Containment, Eradication, and Recovery:

1. What containment strategy should be applied (e.g., isolating infected devices, disabling removable media ports), and what is the rationale behind it?
2. What tools (e.g., malware removal utilities, forensic software) are necessary for effectively containing and eradicating the worm?
3. Which teams or personnel (e.g., IT support, security team) need to be involved in the response, and what roles will each fulfill?
4. What evidence must be gathered (e.g., logs, infected devices), and what processes will ensure its integrity and maintain a proper chain of custody? How long should this evidence be preserved?

Post-Incident Activity:

1. What actions (e.g., updates to security policies, improved user training) can be implemented to prevent similar incidents in the future?
2. How can detection methods be enhanced to identify similar incidents earlier, such as by refining alert thresholds or deploying honeypots?

Scenario 2: Unauthorized Access to Payroll Records

Study the following scenario. Discuss and determine the incident response handling questions that should be asked at each stage of the incident response process. Consider the details of the organization and the CSIRC when formulating your questions.

This scenario is about a mid-sized hospital with multiple satellite offices and medical services. The organization has dozens of locations employing more than 5000 employees. Because of the size of the organization, they have adopted a CSIRC model with distributed incident response teams. They also have a coordinating team that watches over the security operations team and helps them to communicate with each other.

On a Wednesday evening, the organization's physical security team receives a call from a payroll administrator who saw an unknown person leave her office, run down the hallway, and exit the building. The administrator had left her workstation unlocked and unattended for only a few minutes. The payroll program is still logged in and on the main menu, as it was when she left it, but the administrator notices that the mouse appears to have been moved. The incident response team has been asked to acquire evidence related to the incident and to determine what actions were performed.

The security teams practice the kill chain model and they understand how to use the VERIS database. For an extra layer of protection, they have partially outsourced staffing to an MSSP for 24/7 monitoring.

Preparation:

1. Would unauthorized access to the payroll system qualify as an incident? Which specific policies (e.g., access control policy, data protection policy) might have been violated?
2. What existing security measures (e.g., physical security controls, user access policies) were intended to prevent this type of incident? How effective were they?

Detection and Analysis:

1. What signs (e.g., access logs, security camera footage) could act as early indicators, suggesting that unauthorized access might happen?
2. What specific indicators of unauthorized access should be monitored (e.g., unusual login times, failed login attempts)?
3. What additional tools (e.g., log analysis software, camera systems) might be required to conduct a thorough investigation of this incident?

4. How should the incident be prioritized, and what factors should be considered when making that decision?

Containment, Eradication, and Recovery:

1. What immediate containment actions should be implemented (e.g., locking down the payroll system, reviewing access controls)?
2. What tools or resources (e.g., forensic tools, security software) are required for an effective response?
3. Which personel (e.g., IT security, HR) should be involved in the investigation and remediation process, and what specific roles will they fulfill?

What evidence (e.g., system logs, user activity reports) needs to be collected and preserved, and what protocols should be followed to ensure proper handling of this evidence?

Post-Incident Activity:

1. What policy or procedural changes could help prevent unauthorized access incidents in the future (e.g., stricter access controls, employee training)?
2. How can the organization enhance its monitoring and detection capabilities to more effectively identify unauthorized access attempts in the future?