Syahira Azizah Rendra Putri

SIB 4C – 18

2141762059

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.

Jawab :

- **Incident Response Team Readiness**

- Do we have a dedicated incident response team (CSIRC) in place with defined roles and responsibilities?
- Are team members adequately trained in handling security incidents, particularly those related to malware and DDoS attacks?

- **Incident Response Plan**

- Is there a documented incident response plan that includes procedures for identifying, containing, and eradicating malware infections?
- Have we regularly reviewed and updated the incident response plan to reflect current threats, technologies, and lessons learned from previous incidents?

- **Risk Assessment**

- What specific vulnerabilities exist in our network that could be exploited by a worm or similar malware?
- Have we conducted a recent risk assessment to identify critical assets and the potential impact of their compromise?

- **Preventive Measures**

- What security controls (e.g., firewalls, endpoint protection, network segmentation) are currently in place to prevent malware infections?
- Do we have policies regarding the use of removable media and the sharing of files over the network?

- **Monitoring and Detection**

- Are we utilizing effective monitoring tools to detect unusual activity or unauthorized access on our network?
- How quickly can we respond to alerts regarding malware or suspicious behavior on our systems?

- **Communication Plan**

- Is there a clear communication plan for informing employees about potential threats, as well as guidelines for reporting suspected incidents?
- Have we established communication channels with external partners (e.g., antivirus vendors, law enforcement) for assistance during an incident?

- **Employee Training and Awareness**

- Have we conducted training sessions to educate employees about safe computing practices, such as avoiding suspicious downloads and recognizing phishing attempts?
- Do employees understand the importance of reporting incidents immediately to the incident response team?

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.

Jawab :

1. Preparation Phase

- **Incident Response Readiness**

    - **Is there a clearly defined incident response plan that includes procedures for physical security incidents?**
    - **Are all members of the incident response teams trained in the kill chain model and familiar with their roles during an incident?**
- **Evidence Handling**
    - **Do we have established protocols for acquiring and preserving evidence in physical security incidents?**
    - **Are incident response team members trained in chain-of-custody procedures for collected evidence?**
- **Coordination with MSSP**
    - **What specific roles does the MSSP play in incident detection and response?**
    - **How do we ensure effective communication and coordination between in-house teams and the MSSP?**

2. Identification Phase

- **Incident Detection**
    - **How was the incident detected? Were there any alerts from monitoring systems or reports from staff?**
    - **Have we verified that there are no additional threats or incidents occurring simultaneously?**
- **Incident Confirmation**
    - **What evidence do we currently have that confirms unauthorized access occurred in the payroll administrator's office?**
    - **Have we interviewed the payroll administrator and any other potential witnesses to gather more information?**

3. Containment Phase

- **Immediate Actions**
    - **What steps can we take immediately to contain the incident and prevent further unauthorized access (e.g., locking down systems, notifying security)?**
    - **Do we need to notify employees in the area to ensure their safety and prevent potential interference with the investigation?**
- **Temporary Measures**
    - **What temporary measures can we implement to secure sensitive information in the payroll system while the investigation is ongoing?**
    - **Should we change passwords or access controls related to the payroll program?**

4. Eradication Phase

- **Removing Threats**
    - **What steps do we need to take to ensure that any unauthorized access is fully removed from our systems?**
    - **Do we need to conduct a broader investigation to identify any additional vulnerabilities that may have been exploited during this incident?**
- **Evidence Analysis**
    - **How will we analyze the evidence collected (e.g., logs, surveillance footage) to determine what actions were performed during the unauthorized access?**
    - **Are there any forensic tools or techniques we should employ to assess the extent of the breach?**

5. Recovery Phase

- **System Restoration**
    - **What steps do we need to take to safely restore access to the payroll program and ensure its integrity?**
    - **How can we verify that no malicious software or tools were left on the system after the incident?**

- **Monitoring and Review**
    - **What monitoring measures should we put in place to detect any signs of recurring unauthorized access or similar incidents?**
    - **Are there lessons learned from this incident that we should incorporate into future incident response training and preparation?**

6. Lessons Learned Phase

- **Incident Review**
    - **What did we learn from this incident regarding our physical security protocols and response procedures?**
    - **Are there areas for improvement in our incident response plan that should be addressed to better prepare for similar incidents in the future?**
- **Communication Improvements**
    - **How effective was the communication between different teams (physical security, incident response, MSSP) during the incident?**
    - **What feedback can we gather from all parties involved to improve coordination and response in future incidents?**