Nama : Sasmita Rachmawati

Absen : 15

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:

Answer:

- **Would the worm infection qualify as a security incident under the firm's policies?**
- **What security controls are in place to detect and prevent the spread of worms via removable media?**
- **Are all staff members aware of safe practices for handling removable media?**
- **Is there an incident response plan that addresses similar threats (e.g., malware spread through shares)?**

Detection and Analysis:

Answer:

- **What indicators (e.g., unusual network traffic) might reveal the presence of the worm before AV signatures are available?**
- **Can we determine the first infected host, or the point of initial infection?**
- **How would the CSIRC team differentiate this worm's DDoS activity from legitimate network traffic?**
- **What tools might enhance detection and analysis, such as network monitoring software or host-based malware detection?**

Containment, Eradication, and Recovery:

Answer:

- **What immediate containment actions are necessary (e.g., disconnecting infected machines or disabling open shares)?**
- **Are there backup systems or redundancy to limit the impact of infected systems going offline?**
- **What roles would be assigned to each member of the incident response team during containment and recovery?**
- **How should we acquire and store evidence, and for how long, in case legal action is required?**

Post-Incident Activity:

Answer:

- **What measures could reduce the risk of similar incidents (e.g., restricting removable media use or enhancing endpoint protection)?**

- **How could detection capabilities be improved, such as integrating behavior-based threat detection?**
- **Are there additional training needs identified through this incident for staff and incident response members?**

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:

Answer:

- **Does this incident align with definitions of security incidents in hospital policy? What policies were breached?**
- **What physical and system-based controls are in place to prevent unauthorized access to payroll data?**
- **Is there a policy requiring administrators to lock workstations when unattended?**

Detection and Analysis:

Answer:

- **Are there logs or access records that could indicate if any data was accessed or altered?**
- **What indicators of suspicious activity should the incident response team look for in system and security logs?**
- **What additional tools or support might be required to analyze this incident effectively (e.g., audit logs or forensic software)?**
- **How should this incident be prioritized given the sensitivity of payroll data?**

Containment, Eradication, and Recovery:

Answer:

- **What containment measures should be implemented to secure the payroll system (e.g., password reset, workstation reconfiguration)?**
- **What personnel need to be involved, including IT, security, and payroll departments?**
- **How should evidence (e.g., access logs, video footage) be collected and stored? What is the retention policy for evidence?**
- **Should the MSSP be engaged to assist in monitoring for any additional unauthorized access attempts?**

Post-Incident Activity:

Answer:

- **What measures could prevent similar incidents, such as stronger physical security or enhanced login/logout procedures?**
- **How could detection processes be improved to identify unauthorized physical access attempts more swiftly?**
- **Should additional training or awareness sessions be conducted for payroll staff on securing sensitive systems?**