Nama : Winda Umi Fatimatus Sa’diyah

NIM : 2141762055

Absen : 19

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:

- Would the organization classify this as a significant incident, and which specific protocols or response plans does it activate?
- What baseline security policies are designed to prevent the spread of such worms? Are those policies up-to-date and enforced?
- What measures, such as removable media controls and network share restrictions, does the firm already have in place to mitigate risk?

Detection and Analysis:

- What signs or anomalies could signal the start of the worm's spread, such as sudden network traffic spikes or increased use of removable media?

- What potential indicators would alert IT staff to suspicious DDoS activity or malware infection on affected devices?
- Are the current monitoring and antivirus tools equipped to identify the worm's behavior before updates are available? What additional measures, such as behavioral analysis tools, would be beneficial?
- How will the team decide which systems to prioritize for analysis based on business impact?

Containment, Eradication, and Recovery:

- What immediate steps should be taken to isolate infected machines from the network to prevent further spread?
- Would employing a segmented network structure improve the ability to contain such outbreaks?
- What combination of software tools and manual techniques should be used to eradicate the worm from all affected systems?
- Who in the organization should be responsible for evidence collection, and what format should it be documented in to maintain chain-of-custody?
- Where should the evidence be secured, and what is the protocol for data retention to support possible legal or compliance requirements?

Post-Incident Activity:

- How could the organization enhance its incident response playbooks to handle similar malware more effectively in the future?
- What gaps were identified during this incident that should be addressed, such as training, tools, or communication protocols?
- Would implementing more frequent patch updates or deploying stronger endpoint protection mitigate similar threats in the future?

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:

- Would this event be categorized as an internal security incident, and what protocols are invoked under the organization's incident management plan?

- What security practices are in place to prevent unauthorized physical access, and do they include workstation locking and authentication policies?
- Are employees regularly trained on data handling and access policies to mitigate such risks?

Detection and Analysis:

- What precursors might have indicated suspicious behavior, such as unusual movements detected by security cameras or previous access attempts in the area?
- What specific indicators would point to unauthorized use, such as changes in user account logs or mouse and keyboard activity when the administrator was not present?
- What digital forensics tools could assist in identifying whether data was accessed or transferred during this incident?
- How does the response team prioritize incidents involving potential breaches of sensitive financial data?

Containment, Eradication, and Recovery:

- What immediate measures should be taken to secure the payroll system and prevent further access, such as account lockdowns or session terminations?
- What additional personnel, such as legal or human resources, need to be involved to address the potential insider threat?
- What processes should be followed to secure video footage and logs for analysis, ensuring they are stored securely and retained per the organization's retention policies?

Post-Incident Activity:

- What can be learned from the incident to prevent similar cases, such as reinforcing physical security or enhancing user training on locking workstations?
- How could internal processes for monitoring and response be improved, including communication between physical security and IT teams?
- Would implementing stricter access control or two-factor authentication for sensitive workstations improve security.