Name   : Rizqi Zamzami Jamil

Class   : SIB-4C

NIM   : 2141762089

Lab - Incident Handling

Objectives

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

Background / Scenario

Computer security incident response has become a vital part of any organization. The process for handlinga 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 alsofollow 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 organizationand 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 installsa 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 ofsecurity incident handling.

Preparation:

> **Answer:**
> 1. Are all antivirus software and security tools up to date?
> 2. Do we have an incident response plan for malware outbreaks?
> 3. What backup systems are in place for critical investment data?

Detection and Analysis:

> **Answer:**
> 1. How many systems have been infected by the worm?
> 2. What is the primary vector of infection through the network?
> 3. What are the symptoms of infected systems?

Containment, Eradication, and Recovery:

Answer:
1. How can we isolate infected systems from the network?
2. What steps are needed to remove the worm and DDoS agent?
3. How can we verify systems are clean before reconnecting them?

Post-Incident Activity:

Answer:
1. What security controls need to be improved to prevent future infections?
2. How can we better protect against removable media threats?
3. What lessons were learned from this incident?

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 theCSIRC 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 havea 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 payrollprogram is still logged in and on the main menu, as it was when she left it, but the administrator noticesthat 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. Foran extra layer of protection, they have partially outsourced staffing to an MSSP for 24/7 monitoring.

Preparation:

Answer:
1. What physical security measures are in place?
2. Are there logging mechanisms for payroll system access?
3. Do we have clear workstation locking policies?

Detection and Analysis:

Answer:
1. What actions were performed in the payroll system?
2. Are there security cameras that captured the intruder?
3. What audit logs are available from the payroll system?

Containment, Eradication, and Recovery:

Answer:
1. Should we temporarily disable remote payroll system access?
2. What changes need to be made to physical access controls?
3. How can we verify if any data was stolen?

Post-Incident Activity:

Answer:
1. How can we improve workstation security policies?
2. What additional physical security measures are needed?
3. Should we implement additional access monitoring?