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.

****TASK 1****

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.

****ANSWER****

Preparation:

- Do we have an updated and tested incident response plan (IRP) in place?
- Are all employees trained on safe use of removable media and cybersecurity awareness?
- Are our endpoint detection and antivirus solutions up-to-date and centrally managed?
- Is our CSIRC (Computer Security Incident Response Capability) team equipped with tools and procedures to follow the diamond model?
- Do we have backup and recovery plans that are tested regularly?

- Are there logging and monitoring mechanisms in place for early detection?

Detection and Analysis:

- When and how was the worm first detected?
- What systems or data have been infected or affected?
- How did the worm initially enter the network? (e.g., removable media, open share)
- What are the indicators of compromise (IOCs)?
- Which antivirus or EDR (Endpoint Detection and Response) systems identified the worm? Were any alerts generated earlier but overlooked?
- Has the worm contacted any external Command and Control (C2) servers?

Containment, Eradication, and Recovery:

- Can we quickly isolate infected machines from the network?
- Have we disabled or restricted access to open Windows shares temporarily?
- What is the plan to identify and remove all instances of the worm?
- Do we have clean backups available to restore affected systems?
- Have we updated antivirus signatures and applied them across all systems?
- What patches or configuration changes (like disabling autorun) need to be implemented?
- How do we verify that no DDoS agents remain active in the network?

  Have we monitored and restored any critical business applications or investor?

Post-Incident Activity:

- What could be done to prevent similar incidents from occurring in the future?
- What could be done to improve detection of similar incidents?
- What updates should we make to the incident response plan?

TASK 2

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.

****ANSWER****

Preparation:

- Does the hospital have a policy regarding locking or securing unattended workstations?
- Are employees regularly trained on physical and information security practices?
- What are the access control policy within organization?
- Are workstation access logs or screen recording solutions available?

Detection and Analysis:

- What are the exact details reported by the payroll administrator?
- Did any surveillance footage capture the intruder entering or exiting the premises?
- Did any data access logs or system event logs show unusual activity (e.g., opening sensitive employee files)?
- Was any data exfiltrated, modified, or deleted?

Containment, Eradication, and Recovery:

- Should access to the affected payroll system be temporarily suspended?
- Should other similar systems across the hospital be monitored for similar access patterns?
- Was malware or backdoor software installed on the payroll workstation?
- Were any unauthorized accounts or changes created on the system?
- How should affected employees be notified, especially if payroll data was accessed?
- Can the hospital recover from this event without affecting upcoming payroll processing?

Post-Incident Activity:

- What gaps in physical security controls or endpoint protections were identified?
- Should the hospital implement workstation auto-lock policies or proximity-based screen locking?

- Does the CSIRC need to update response playbooks for physical-digital incident overlap?
- What new controls or training measures should be implemented to reduce recurrence?
- Should this incident be logged into the VERIS database for threat intelligence sharing and statistical analysis?