Name : Selly Amelia Putri

Class : SIB 4C

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:

1. Preparation

- Does the firm have clear policies for incident handling?
- Are there preventative security measures in place?
- Are employees trained on secure practices, especially with removable media?

2. Identification

- How was the worm detected, and how many systems are infected?
- Are there common traits in the infected systems?
- Is there evidence of data theft or other risks?

3. Containment

- What steps are needed to stop the worm's spread?
- Should we isolate infected systems or restrict file sharing?
- Are there critical systems we need to protect first?

4. Eradication

- Has antivirus updated to remove the worm?
- What tools are needed to fully clean infected systems?
- How can we ensure the worm is fully gone?

5. Recovery

- When can systems safely reconnect to the network?
- How will we monitor for reinfection?
- Are backups needed, and is everything functioning well?

6. Lessons Learned

- Where did detection and response fall short?
- What can be done to prevent similar incidents?
- How can employee awareness be improved for future prevention?

Answers will vary especially based upon the cybersecurity operation team. Examples:

Would the organization consider this activity to be an incident? If so, which of the organization's policies does this activity violate?
What measures are in place to attempt to prevent this type of incident from re-occurring, or to limit its impact?

Detection and Analysis:

1. Precursors:

   Were there any early signs like unusual file sharing or device activity that might've warned us?

2. Indicators:

   What symptoms, like network spikes or abnormal file copies, indicate an infection?

3. Tools Needed:

   Do we need any special tools, like advanced malware detectors, to spot this kind of incident?

4. Prioritization:

   How serious is this incident, and which systems should we secure first to minimize damage?

Answers will vary especially based upon the cybersecurity operation team. Examples:

What precursors of the incident, if any, might the organization detect? Would any precursors cause the organization to take action before the incident occurred?
What indicators of the incident might the organization detect? Which indicators would cause someone to think that an incident might have occurred?
What additional tools might be needed to detect this particular incident?
How would the team prioritize the handling of this incident?

Containment, Eradication, and Recovery:

1. Containment Strategy:

   Should we isolate infected systems from the network to stop the spread? This strategy is quick and minimizes further infection.

2. Tools Needed:

   Do we need specific malware removal tools or updated antivirus solutions for cleanup?

3. Involved Personnel:

   Which team members (IT, security, or external experts) will handle containment, cleaning up, and restoring systems?

4. Evidence Gathering:

   Should we collect logs, affected files, and network data? We'd store them securely for analysis and keep them for as long as policy requires for any future investigations.

Answers will vary especially based upon the cybersecurity operation team. Examples:

What strategy should the organization take to contain the incident? Why is this strategy preferable to others?
What additional tools might be needed to respond to this particular incident?
Which personnel would be involved in the containment, eradication, and/or recovery processes?
What sources of evidence, if any, should the organization acquire? How would the evidence be acquired? Where would it be stored? How long should it be retained?

Post-Incident Activity:

1. Prevention:

   Train employees on safe media use and improve security rules.

2. Detection:

   Use alerts for unusual activity and add better monitoring tools.

Answers will vary based upon the cybersecurity operation team. Examples:

What could be done to prevent similar incidents from occurring in the future?
What could be done to improve detection of similar incidents?

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:

1. Incident Classification:

   Does this count as an incident, and which policies does it break?

2. Preventive Measures:

   Are there rules about locking workstations and security checks in sensitive areas?

3. Response Capabilities:

   Is there a process for handling physical security breaches like this?

4. Communication:

   How will the teams (CSIRC and MSSP) coordinate, and who needs to be informed?

Answers will vary based upon the cybersecurity operation team. Examples:

Would the organization consider this activity to be an incident? If so, which of the organization's policies does this activity violate?
What measures are in place to attempt to prevent this type of incident from occurring or to limit its impact?

Detection and Analysis:

1. Precursors: Any signs of suspicious behavior before this?
2. Indicators: What shows unauthorized access (like moved mouse or logs)?
3. Tools: Do we need tools like video footage or activity logs?
4. Prioritization: How urgent is this, and which areas should be secured first?

Answers will vary based upon the cybersecurity operation team. Examples:

What precursors of the incident, if any, might the organization detect? Would any precursors cause the organization to take action before the incident occurred?
What indicators of the incident might the organization detect? Which indicators would cause someone to think that an incident might have occurred?
What additional tools might be needed to detect this particular incident?
How would the team prioritize the handling of this incident?

Containment, Eradication, and Recovery:

1. **Containment:**

   Lock down the workstation and check recent access.

2. **Tools:**

   Gather video footage, access logs, or use forensic tools.

3. **Personnel:**

   Involve IT, security, and CSIRC for investigation.

4. **Evidence:**

   Collect logs and footage, store them securely, and keep as needed.

Answers will vary based upon the cybersecurity operation team. Examples:

What strategy should the organization take to contain the incident? Why is this strategy preferable to others?

What additional tools might be needed to respond to this particular incident?
Which personnel would be involved in the containment, eradication, and/or recovery processes?
What sources of evidence, if any, should the organization acquire? How would the evidence be acquired? Where would it be stored? How long should it be retained?

Post-Incident Activity:

1. Prevention:

   Implement stricter policies for locking workstations and increase staff awareness.

2. Improved Detection:

   Use cameras or monitoring tools to catch unauthorized access faster.

Answers will vary based upon the cybersecurity operation team. Examples:

What could be done to prevent similar incidents from occurring in the future?
What could be done to improve detection of similar incidents?