Nama : Yusufa Haidar

Kelas : SIB – 4C

Absen : 21

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:

- Is this activity considered an incident according to the organization's incident response policy?
- Which organizational policies does this activity violate?
- What measures are in place to prevent or limit the impact of such an incident?
- How trained and prepared is the staff to recognize and handle such incidents?

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 organizationâ€™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:

- How was the worm detected, and how quickly after the initial infection?
- Which systems and networks were affected?
- What is the scope of the infection in terms of affected devices and systems?
- Are there any patterns or indicators that can help identify how the worm entered the system?
- What tools and resources are available to analyze and respond to this incident?

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:

- What immediate steps can be taken to contain the spread of the worm?
- How can infected systems be isolated to prevent further spreading?
- What is the plan for eradicating the worm from infected systems?
- What backups or recovery procedures are in place to restore systems to a secure state?
- How can the organization ensure the worm and any associated threats are completely removed?

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:

- What lessons can be learned from this incident?
- How effective were the existing policies and procedures in responding to the incident?
- What changes or improvements can be made to prevent similar incidents in the future?
- Are there any additional security measures or tools that should be implemented?

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 organizationâ€™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:

- Does the organization consider this activity to be an incident? Which organizational policies does this acti vity violate?
- What preventive measures are in place to avoid unauthorized access to workstations?
- Are there any specific training programs for staff regarding physical and data security?
- How effective are the current communication and coordination strategies among the distributed incident r esponse teams and the coordinating team?

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 organizationâ€™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:

- What are the precursors of this incident? Could any precursors have triggered preventive action before th e incident occurred?
- Which indicators might reveal the presence of the unauthorized individual or actions performed on the pa yroll system?
- How quickly was the incident detected, and by whom?
- What additional tools or logs (such as physical security cameras, access control systems, or software log s) might be needed to detect and analyze this incident?
- How should the team prioritize the handling of this incident, considering its potential impact on sensitive p ayroll data?

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:

- What immediate steps can be taken to contain the incident and prevent further unauthorized access?
- Which personnel (e.g., IT security team, physical security team, forensic investigators) are involved in con tainment, eradication, and recovery processes?

- What additional tools or resources are required to respond effectively to this incident?
- What sources of evidence should be acquired (e.g., security camera footage, access logs, workstation log s)? How will this evidence be collected, stored, and retained?
- What is the plan for eradicating any potential threats and ensuring that the payroll system and workstation are secure?
- Are there existing backups to restore systems and ensure the integrity of payroll data?

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:

- What lessons can be learned from this incident, and how effective were the existing policies and procedur es?
- What measures can be implemented to prevent similar incidents in the future (e.g., stricter access control s, additional staff training)?
- How can the organization improve the detection of similar incidents (e.g., enhanced monitoring tools, mor e frequent security audits)?
- How well did the coordination between the incident response teams and the MSSP work during this incide nt?

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?