Semba Wijaya | SIB4C | KSI

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:

Answer Area

- **Would the organization consider this activity to be an incident? If so, which of the organization's policies does this activity violate?**

- Yes, this would be considered an incident as it involves unauthorized access and infection of systems. It likely violates the organization's policies on cybersecurity and acceptable use of removable media.

- **What measures are in place to attempt to prevent this type of incident from re-occurring, or to limit its impact?**
  - Implementing endpoint protection solutions, restricting the use of removable media, regular antivirus updates, and user training on cybersecurity best practices.

Detection and Analysis:

Answer Area

- **What precursors of the incident, if any, might the organization detect? Would any precursors cause the organization to take action before the incident occurred?**
  - Signs of abnormal network traffic or unexpected file sharing activity could serve as precursors. Monitoring logs for unusual access patterns might trigger a preemptive response.

- **What indicators of the incident might the organization detect? Which indicators would cause someone to think that an incident might have occurred?**
  - Indicators could include multiple reports of system slowdowns, DDoS traffic patterns, and unusual behavior from infected machines. Alerts from intrusion detection systems may signal an ongoing attack.

- **What additional tools might be needed to detect this particular incident?**
  - Network traffic analysis tools, advanced threat detection software, and enhanced logging capabilities to monitor user activities.

- **How would the team prioritize the handling of this incident?**
  - Prioritize based on the criticality of affected systems, the scope of the infection, and potential impact on business operations.

Containment, Eradication, and Recovery:

Answer Area

- **What strategy should the organization take to contain the incident? Why is this strategy preferable to others?**
  - The organization should isolate infected machines from the network to prevent further spread. This is preferable as it limits the impact while containment measures are deployed.

- **What additional tools might be needed to respond to this particular incident?**

- Incident response tools for forensic analysis, malware removal tools, and network segmentation solutions.

- **Which personnel would be involved in the containment, eradication, and/or recovery processes?**
    - The incident response team, IT staff, and external security experts if needed.
- **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?**
    - Evidence could include logs from firewalls, intrusion detection systems, and affected endpoints. Evidence should be acquired through proper forensic methods, stored securely in a chain-of-custody manner, and retained for a period determined by organizational policy, often several months to years.

Post-Incident Activity:

Answer Area

- **What could be done to prevent similar incidents from occurring in the future?**
    - Regular security training for employees, strict access controls, and a review of security policies and procedures to identify weaknesses.
- **What could be done to improve detection of similar incidents?**
    - Enhancing monitoring capabilities, adopting advanced threat detection technologies, and regularly updating antivirus definitions and signatures.
    -

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:

Answer Area

- **Would the organization consider this activity to be an incident? If so, which of the organization's policies does this activity violate?**
    - o Yes, this is considered an incident as it involves unauthorized access to sensitive payroll information. It likely violates data protection and access control policies.
- **What measures are in place to attempt to prevent this type of incident from occurring or to limit its impact?**
    - o Implementing strict access controls, requiring strong authentication measures, and training staff to avoid leaving workstations unlocked.

Detection and Analysis:

Answer Area

- **What precursors of the incident, if any, might the organization detect? Would any precursors cause the organization to take action before the incident occurred?**
    - o Precursors might include suspicious physical security alerts, such as unauthorized access attempts or alerts from security cameras.
- **What indicators of the incident might the organization detect? Which indicators would cause someone to think that an incident might have occurred?**
    - o Indicators include unauthorized access logs, movements captured by security cameras, and any unusual activity in payroll records.
- **What additional tools might be needed to detect this particular incident?**
    - o Physical security monitoring systems, access control logs, and surveillance camera footage.
- **How would the team prioritize the handling of this incident?**
    - o The incident would be prioritized based on the sensitivity of the payroll information, potential impact on employee privacy, and regulatory implications.

Containment, Eradication, and Recovery:

Answer Area

- **What strategy should the organization take to contain the incident? Why is this strategy preferable to others?**
    - o The organization should secure the affected systems, review access logs, and change access credentials. This strategy helps prevent further unauthorized access while investigating the incident.

- **What additional tools might be needed to respond to this particular incident?**

- Forensic analysis tools, tools for reviewing and auditing access logs, and incident tracking systems.

- **Which personnel would be involved in the containment, eradication, and/or recovery processes?**
  - The incident response team, IT staff, physical security personnel, and possibly legal counsel.

- **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?**
  - Evidence may include access logs, surveillance footage, and user authentication records. Evidence should be gathered using proper forensic techniques, stored securely, and retained in accordance with the organization's data retention policy.

Post-Incident Activity:

Answer Area

- **What could be done to prevent similar incidents from occurring in the future?**
  - Regular security training for employees, implementation of stronger authentication methods, and physical security audits.

- **What could be done to improve detection of similar incidents?**
  - Investing in advanced surveillance technologies, regular security assessments, and enhancing the incident reporting mechanisms for employees.