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:

Ask when was the system last used(workday) and was their any sign or compromise then, try to get an exact timing of the attack
Ask if they keep any logs or have HIDS or NIDS service.
Ask who is incharge of physical security of the devices
Ask if they have any suspicion on anyone

Detection and Analysis:

Try and gather all logs from active devices and networks.
Based on the timeline try to sort through the data and try to figure out the attack life cycle

Containment, Eradication, and Recovery:

try to identify the malware and point of breach. update security on all devices and figure out what vulnerabilty was attack by the malware. Is it a popular malware or specially crafted 0 day

Post-Incident Activity:

Prepare a report and present to the business. Talk about backup and recovery§

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:

Contact all required security teams and get information about the device usage.
From the call we can get estimated time of attack, contact on site security to try to get description of unknown person.

Detection and Analysis:

Disconnect administrator account from main network or set up firewall to disallow requests from this particular device.
Log out administrator and change password as well.
Start analysing the device and account history/future actions

Containment, Eradication, and Recovery:

Better on site security
personnel training to not leave devices unlocked

Post-Incident Activity: