Rossi Dea Agatha
SIB 4C – 2141762112

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. Would the organization consider this activity to be an incident? If so, which of the organization's policies does this activity violate?
   - Ya, ini dianggap insiden karena mengancam keamanan jaringan. Aktivitas ini melanggar kebijakan keamanan organisasi tentang penggunaan dan keamanan jaringan internal.

2. What measures are in place to attempt to prevent this type of incident from re-occurring, or to limit its impact?
   - Organisasi mungkin sudah memiliki perangkat lunak antivirus, pemantauan jaringan, dan pembatasan penggunaan media yang dapat dilepas. Meningkatkan frekuensi pembaruan antivirus juga dapat membantu.

Detection and Analysis:

1. **What precursors of the incident, if any, might the organization detect? Would any precursors cause the organization to take action before the incident occurred?**
   - Tanda awal mungkin berupa perlambatan jaringan atau aktivitas mencurigakan di Windows share.

2. **What indicators of the incident might the organization detect? Which indicators would cause someone to think that an incident might have occurred?**
   - Terdeteksi worm yang menyebar ke beberapa host melalui media yang dapat dilepas atau Windows share yang terbuka.

3. **What additional tools might be needed to detect this particular incident? How would the team prioritize the handling of this incident?**
   - IDS (Intrusion Detection System) dan alat pemantauan jaringan untuk mendeteksi aktivitas tidak wajar dalam lalu lintas data.
4. **How would the team prioritize the handling of this incident?**
   - Berdasarkan skala penyebaran worm dan dampaknya terhadap layanan. Dampak pada ketersediaan layanan utama harus menjadi prioritas utama.

Containment, Eradication, and Recovery:

1. **What strategy should the organization take to contain the incident? Why is this strategy cmcv,dgdf,fgyh.preferable to others?**
   - Mengisolasi perangkat yang terinfeksi dari jaringan utama untuk mencegah penyebaran lebih lanjut.

2. **What additional tools might be needed to respond to this particular incident?**
   - Alat untuk menghapus worm secara massal dari perangkat yang terinfeksi serta firewall yang membatasi akses ke Windows share.

3. **Which personnel would be involved in the containment, eradication, and/or recovery processes?**
   - Tim keamanan siber, administrator jaringan, dan personel TI yang berfokus pada perangkat yang terinfeksi.

4. **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?**
   - Log dari perangkat yang terinfeksi, catatan aktivitas jaringan, dan bukti keberadaan worm disimpan dalam sistem yang aman selama jangka waktu sesuai kebijakan retensi.

Post-Incident Activity:

1. **What could be done to prevent similar incidents from occurring in the future?**
   - Mengimplementasikan kebijakan pembatasan perangkat media yang dapat dilepas dan meningkatkan perlindungan jaringan serta respons cepat pada ancaman baru.

2. **What could be done to improve detection of similar incidents?**
   - Menambahkan IDS yang secara otomatis memberi peringatan saat aktivitas mencurigakan di Windows share terdeteksi.

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. **Would the organization consider this activity to be an incident? If so, which of the organization's policies does this activity violate?**
   - Ya, ini dianggap insiden karena ada akses tidak sah ke catatan gaji. Aktivitas ini melanggar kebijakan keamanan terkait akses data sensitif.

2. **What measures are in place to attempt to prevent this type of incident from occurring or to limit its impact?**
   - Kebijakan tentang penguncian otomatis perangkat yang tidak aktif dan pemantauan CCTV mungkin sudah ada, tetapi perlu diperketat.

Detection and Analysis:

1. **What precursors of the incident, if any, might the organization detect? Would any precursors cause the organization to take action before the incident occurred?**
   - Indikasi aktivitas fisik mencurigakan oleh pihak yang tidak dikenal di area sensitif dan pergerakan mouse yang berbeda dari kondisi sebelumnya.

2. **What indicators of the incident might the organization detect? Which indicators would cause someone to think that an incident might have occurred?**
   - itemukan pergerakan mouse dan program gaji yang masih aktif.

3. **What additional tools might be needed to detect this particular incident?**
   - Sistem pemantauan CCTV dan perangkat lunak log aktivitas perangkat.

4. **How would the team prioritize the handling of this incident?**
   - Karena ini melibatkan data pribadi karyawan, insiden ini harus segera ditangani untuk mencegah kebocoran data lebih lanjut.

Containment, Eradication, and Recovery:

1. **What strategy should the organization take to contain the incident? Why is this strategy preferable to others?**
   - Memastikan area kerja aman dengan memperbaiki kebijakan kunci layar otomatis dan memperketat keamanan fisik.

2. **What additional tools might be needed to respond to this particular incident?**
   - Log akses perangkat dan CCTV untuk mengidentifikasi pelaku.

3. **Which personnel would be involved in the containment, eradication, and/or recovery processes?**
   - Tim keamanan fisik, staf TI, dan administrator system.

4. **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?**
   - Rekaman CCTV, log perangkat, dan data sistem disimpan secara aman sesuai kebijakan retensi data.

Post-Incident Activity:

1. **What could be done to prevent similar incidents from occurring in the future?**
   - Menerapkan kebijakan penguncian otomatis perangkat yang tidak digunakan dan meningkatkan pengawasan area dengan data sensitif.

2. **What could be done to improve detection of similar incidents?**
   - Memasang sensor aktivitas di area sensitif dan memperketat kontrol akses.