Nama : Mochammad Aldo Rizky

Kelas : SIB4C

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

In responding to this incident scenario, several specific questions need to be addressed at each stage of the incident response process to ensure thorough handling and containment. Here’s a breakdown of questions that should be considered for each stage, tailored to a small investment firm like the one described:

1. Preparation

Would the organization consider this activity to be an incident?

Which policies or procedures does this activity violate (e.g., malware prevention, acceptable use, removable media policies)?

What existing security measures (e.g., endpoint protection, firewall rules, network segmentation) are in place to prevent the spread of malware and worms?

Are regular backups of critical data performed, and are they isolated from the main network to prevent infection?

Is there an incident response (IR) plan, and are employees aware of their roles in it?

How often are incident response exercises or training conducted for employees?

2. Identification

How was the worm identified (e.g., antivirus alert, network traffic anomaly)?

Which hosts or systems show signs of infection, and are there any patterns in how it has spread?

What indicators of compromise (IoCs) are associated with this worm, such as file hashes, network traffic, or system behaviors?

Which systems are most at risk (e.g., those with open Windows shares or removable media usage)?

What is the extent of the infection across systems and departments?

3. Containment

What immediate containment measures can be taken to isolate infected systems from the network (e.g., disconnecting affected devices, disabling Windows shares)?

Should network-wide sharing or removable media use be temporarily disabled to prevent further infection?

What short-term containment actions can prevent the DDoS agent from activating and causing further damage?

Are there any systems or data that need to be prioritized for containment or protection, such as financial systems or customer data?

Can remote systems or employee devices connecting from home pose an additional risk to containment efforts?

4. Eradication

Are the antivirus signatures or security patches now available to remove the worm from infected systems?

How will the IT team ensure complete removal of the worm across all infected hosts?

Is any custom scripting or additional software needed to thoroughly clean the infected systems?

Have any backdoors or other malware been installed as part of the infection, and how will those be identified and removed?

Is there a process to re-scan the entire network post-eradication to confirm no residual infections remain?

5. Recovery

When is it safe to reconnect cleaned systems to the network?

What tests will be conducted to verify that the worm and DDoS agent have been fully removed and that normal operations can safely resume?

What safeguards, such as monitoring or updated antivirus definitions, will be implemented during recovery?

Are there particular business-critical systems that need priority for restoration?

How will the team verify that the DDoS agent has not left residual changes or vulnerabilities that might impact network stability?

6. Lessons Learned

How did the worm initially penetrate the firm’s defenses, and are there specific vulnerabilities that need to be addressed?

What aspects of the incident response plan were effective, and where were there gaps?

Could the incident have been detected or contained sooner, and what improvements can help with faster response in the future?

What updates are necessary for the firm’s policies on removable media, network sharing, or endpoint protection to prevent future incidents?

Is additional employee training needed regarding malware, handling of removable media, or other relevant areas?

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

In the Detection and Analysis stage, questions should focus on recognizing early signs of the incident, understanding specific indicators, evaluating detection capabilities, and determining priorities. Here's a set of tailored questions for the scenario:

1. Precursors

What precursors of the incident, if any, might the organization detect?

Were there any abnormal network activities, such as unusual traffic patterns or failed connection attempts, that could have signaled the worm's spread before widespread infection?

Did any logs indicate attempts to access shared files or drives in unusual ways?

Was there any increase in unusual removable media use among employees, which could be a sign of a potential worm entry point?

Would any precursors cause the organization to take action before the incident occurred?

If there were early indicators of abnormal activity on the network, would the organization have isolated those systems to prevent potential spread?

Are there specific alerts or anomaly thresholds that would have prompted security personnel to investigate more thoroughly and proactively?

2. Indicators

What indicators of the incident might the organization detect?

Infected systems might exhibit unexpected CPU or network load, signs that a DDoS agent or other malicious processes are active.

Unusual or unauthorized files in shared drives or removable media used across multiple systems.

Suspicious processes running on multiple hosts, possibly linked to malware activity, and flagged by antivirus alerts once signatures become available.

Which indicators would cause someone to think that an incident might have occurred?

Alerts from antivirus, endpoint protection, or intrusion detection systems (IDS) indicating a new worm or abnormal system behavior.

Anomalies in network logs showing high volumes of unusual connections or traffic spikes indicative of a DDoS agent's activity.

Reports from employees or IT noticing significant slowdowns or erratic behavior on workstations.

3. Detection Tools

What additional tools might be needed to detect this particular incident?

Endpoint Detection and Response (EDR) tools for deeper visibility into malware behavior on endpoints, especially for identifying worm spread and process anomalies.

Network monitoring or intrusion detection systems (IDS/IPS) to identify unusual traffic patterns and detect the DDoS agent's traffic.

A Security Information and Event Management (SIEM) system for consolidating and correlating logs, which can help spot early indicators of a worm and alert security staff sooner.

4. Incident Prioritization

How would the team prioritize the handling of this incident?

Given the potential for widespread infection, the incident should likely be classified as high priority due to the risk of further spread and impact on business operations.

Systems critical to business functions (e.g., financial data servers or customer records) should be prioritized to minimize data compromise.

Based on the DDoS component, systems that could be leveraged in external attacks should be handled quickly to prevent damage to external entities and reduce liability.

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

During the Containment, Eradication, and Recovery phase, key questions address strategies for controlling the spread, eliminating threats, and restoring normal operations. Here's a breakdown tailored to the investment firm scenario:

1. Containment Strategy

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

Immediate Isolation: Disconnect infected systems from the network to stop further spread of the worm. This can include disabling network shares and restricting access to removable media temporarily.

Segmented Containment: Use network segmentation to isolate critical systems and prevent cross-infection, prioritizing containment of systems most critical to business operations.

Preferred Strategy: Immediate isolation is preferable because it quickly halts the worm's propagation, while segmented containment ensures that critical data is protected even as less critical systems are treated.

2. Tools for Response

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

Endpoint Detection and Response (EDR) Tools: For identifying, isolating, and analyzing infected hosts.

Network Segmentation Tools: Such as VLANs or firewall rules, to create secure zones and prevent further spread.

Digital Forensics Tools: To analyze worm behavior, DDoS agent installation, and potential lingering vulnerabilities.

Backup and Restore Solutions: If necessary, to restore data and system configurations to a pre-infection state on affected machines.

3. Personnel Involvement

Which personnel would be involved in the containment, eradication, and/or recovery processes?

Security Incident Response Team (CSIRC): To oversee containment and provide specialized response actions, including monitoring for worm reemergence.

IT Operations Team: Responsible for implementing network isolation, disabling Windows shares, and ensuring availability of backup solutions.

Forensics Team: For investigating the worm's behavior and documenting evidence related to infection methods and spread.

Management and Communication Team: To inform employees and possibly clients of the situation, ensuring clear communication regarding any service interruptions or security concerns.

4. Evidence Collection

What sources of evidence, if any, should the organization acquire?

System Logs: Logs from infected hosts and network devices, to trace the worm's origin, spread, and any actions taken by the DDoS agent.

Removable Media Samples: Any removable drives involved in the spread should be isolated and analyzed.

Network Traffic Captures: To document suspicious connections and actions taken by the DDoS agent.

How would the evidence be acquired?

Use forensic imaging tools to capture snapshots of infected systems and devices, ensuring that evidence is preserved in a forensically sound manner.

Collect logs from firewalls, intrusion detection systems, and endpoint protection tools to gain a comprehensive view of the attack.

Where would it be stored?

Evidence should be stored in a secure, access-controlled digital evidence repository, typically managed by the forensics or CSIRC team, with only authorized personnel able to access it.

How long should it be retained?

Retention periods depend on regulatory and organizational policies; however, in this case, evidence should be kept for at least 1-3 years to meet compliance requirements and support any potential legal or insurance needs.

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:

In the Post-Incident Activity phase, the organization can focus on lessons learned, prevention, and improved detection to strengthen its defenses. Here are some targeted questions and actions:

1. Prevention of Similar Incidents

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

Restrict Removable Media Use: Implement stricter policies or controls around removable media, such as disabling USB access on critical systems or enforcing encrypted, organization-owned drives only.

Enhanced Network Segmentation: Apply network segmentation to limit worm propagation, isolating critical systems from those more prone to infection.

Regular Patching and Updates: Establish a timely patching routine to reduce vulnerabilities in operating systems and applications, minimizing exposure to worms and other malware.

User Awareness Training: Conduct regular training on malware risks, including the safe handling of removable media and recognizing phishing attempts that may introduce malware.

2. Improving Detection

What could be done to improve detection of similar incidents?

Deploy Advanced Threat Detection: Use Endpoint Detection and Response (EDR) solutions that monitor unusual activities on endpoints, which can help detect worms and similar threats early.

Enhance SIEM Correlation Rules: Update SIEM (Security Information and Event Management) rules to identify signs of worm-like activity, such as excessive network file-sharing, unexpected removable media access, or DDoS agent patterns.

Implement Network Anomaly Detection: Use Intrusion Detection/Prevention Systems (IDS/IPS) to detect unusual traffic patterns or spikes that indicate malware spread or DDoS agent activity.

Strengthen Endpoint Monitoring: Enable alerts for unapproved USB devices or executable files running from removable media, which can act as a precursor to worm infection.

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:

In the Preparation stage of the incident response process, the organization’s security team should assess the potential policy violations, preventive measures, and incident classification criteria based on the hospital’s specific context. Here are key questions to consider:

1. Incident Classification

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

Classification: Does this unauthorized access to a payroll administrator’s workstation and potentially sensitive payroll data meet the organization’s criteria for an incident? Given the access to personal and financial data, it likely qualifies.

Policy Violation: Which specific policies does this breach? This may include policies on workstation security, user access management, and physical security protocols that require workstations to be locked when unattended, especially in sensitive areas.

2. Preventive Measures

What measures are in place to attempt to prevent this type of incident from occurring or to limit its impact?

Access Controls and Physical Security: Is there a policy requiring workstations with sensitive access to automatically lock after a short period of inactivity? Are there surveillance cameras in place, especially near high-risk areas like payroll?

User Training and Awareness: Do employees receive regular training on security awareness, emphasizing the importance of locking workstations when leaving them unattended?

Enhanced Identity Verification: For access to sensitive areas, are there badge readers or key cards in place to monitor access to sensitive sections of the building? Are physical security and ID checks regularly enforced?

Technical Controls: Does the payroll software have an automatic logout feature after a period of inactivity, especially on unattended sessions?

3. Incident Readiness and CSIRC Preparedness

How prepared is the incident response team to respond to incidents of this nature?

Policy and Procedure Availability: Are there documented procedures and guidelines specifically for handling potential data breaches or unauthorized physical access incidents?

Communication and Coordination: How are communication lines managed between distributed CSIRC teams and the central coordinating team? Is there an established protocol for notifying key stakeholders, including legal and compliance teams, when unauthorized access is suspected?

Integration with MSSP: Is the MSSP adequately informed of physical security incidents, or do they only monitor cybersecurity events? How quickly can they collaborate on incident resolution in cases involving physical breaches?

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:

In the Detection and Analysis stage, the hospital's incident response team should focus on identifying potential signs of the incident, determining which tools may aid in detection, and assessing the priority level for response. Here are essential questions to guide this stage:

1. Precursors

What precursors of the incident, if any, might the organization detect?

Physical Security Logs: Previous logs or surveillance footage might show unauthorized attempts to access sensitive areas, like the payroll office.

Access Attempts: If other employees noticed or reported unusual behavior, such as an unknown individual accessing restricted areas, this could signal increased security risk.

Would any precursors cause the organization to take action before the incident occurred?

Unusual Badge Activity: If the individual used a cloned or stolen access badge, this may have triggered alerts for unusual badge activity, allowing security to investigate sooner.

Repeated Security Breaches: If the organization had recent attempts or breaches in physical security, this may have led to an escalation or investigation, prompting more robust access monitoring or additional employee reminders to secure workstations.

2. Indicators

What indicators of the incident might the organization detect?

Physical Indicators: Surveillance footage from the hallway or office could capture the unknown individual's movement.

System Indicators: Logs from the payroll system, including timestamps and user actions, may show any transactions or access that the individual may have attempted.

Forensic Evidence on the Workstation: Mouse movements, accessed files, or attempts to copy data could be logged on the workstation or monitored through any endpoint protection solutions in place.

Which indicators would cause someone to think that an incident might have occurred?

Unusual Activity on the Payroll System: If payroll data or configuration settings were modified, added, or accessed at an unusual time, this would be a strong indicator.

Unexpected System Access: An unexpected log-in session, access time, or command history on the payroll software could signal unauthorized access.

Physical Security Alert: Reports of a suspicious individual in a restricted area would trigger a physical security alert, prompting further investigation.

3. Tools for Detection

What additional tools might be needed to detect this particular incident?

Endpoint Detection and Response (EDR): An EDR solution could capture details about any processes or data access on the payroll administrator's workstation during the suspicious timeframe.

Physical Surveillance Systems: Cameras with enhanced analytics could automatically flag unauthorized individuals or suspicious movements.

System Access Monitoring: Detailed logging on the payroll system and additional access management systems (e.g., SIEM) would provide insights into unusual activity patterns.

Forensic Imaging Tools: Tools to capture a forensic image of the workstation would allow for thorough post-incident analysis of any system changes.

4. Incident Prioritization

How would the team prioritize the handling of this incident?

High Priority: Given the potential for a sensitive data breach, this incident would be classified as high priority. Payroll data often includes personal and financial information, making it both sensitive and critical to safeguard.

Consideration of Compliance and Legal Ramifications: The potential access to confidential data elevates the priority to ensure compliance with data protection regulations (e.g., HIPAA, GDPR).

Risk to Reputation and Trust: Since it involves a physical breach and potential data compromise, the incident's response is essential to maintain trust with employees and avoid reputational damage.

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:

In the Containment, Eradication, and Recovery phase, the hospital's incident response team will develop and implement a plan to manage and mitigate the incident, gather evidence, and restore normal operations. Here are some critical questions to guide this phase:

1. Containment Strategy

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

Immediate Physical and Digital Containment: Physically secure the payroll office and remove unauthorized personnel to prevent further access. Lock down the payroll system account and initiate a forced logout to prevent further unauthorized actions.

Network Segmentation and Endpoint Isolation: If there is concern that malware was introduced, isolate the affected workstation from the network to prevent lateral movement or data exfiltration.

Rapid System Lockdown: Employ immediate short-term containment by restricting access to the payroll system temporarily while investigating further.

Rationale: These measures quickly prevent additional unauthorized access, contain potential digital threats, and protect sensitive payroll data without causing excessive downtime.

2. Tools for Response

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

Forensic Analysis Tools: Tools like EnCase or FTK to capture and analyze a forensic image of the payroll workstation.

SIEM and EDR: SIEM (Security Information and Event Management) and Endpoint Detection and Response tools to gather logs, check for malware, and detect any suspicious activity that may have been initiated.

Access Management System: Logs from access control systems or badging systems to determine physical entry history.

Network Traffic Analysis Tools: To verify if data was sent outside the organization, especially from the affected workstation.

3. Involved Personnel

Which personnel would be involved in the containment, eradication, and/or recovery processes?

Incident Response Team (IRT): Responsible for digital containment, forensic investigation, and monitoring systems during recovery.

Physical Security Team: To secure the area, review surveillance footage, and track unauthorized access.

IT Support Staff: To assist with account lockdown, workstation isolation, and secure system configurations post-incident.

HR and Legal Teams: Involved for potential legal proceedings, employee interviews, and compliance with regulatory requirements.

External MSSP (Managed Security Service Provider): If the MSSP provides 24/7 monitoring, they may support detection and digital containment efforts.

4. Evidence Collection and Retention

What sources of evidence, if any, should the organization acquire?

Workstation Forensic Image: Capture an exact copy of the affected workstation for later analysis, preserving the state of applications, open sessions, and any suspicious files.

Access Logs: Collect logs from the payroll system, network access points, physical security systems, and badge systems.

Surveillance Footage: Retrieve any camera footage showing the unauthorized individual’s actions and movement.

System and Network Logs: Retain logs from the payroll application and any associated network activity logs that might indicate data access or movement.

How would the evidence be acquired? Where would it be stored? How long should it be retained?

Acquisition Process: Evidence should be gathered using proper forensic protocols, ensuring all data is time-stamped and hash-verified to maintain integrity. Use write-blockers when capturing images of hard drives.

Storage and Security: Evidence should be securely stored in a dedicated evidence storage server or secure repository with access restricted to authorized personnel only.

Retention Duration: Evidence should be retained in accordance with regulatory requirements (such as HIPAA for healthcare data), internal policies, and any legal counsel recommendations. Retention could range from one year to several years based on regulatory and legal mandates.

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:

In the Post-Incident Activity phase, the hospital’s security and incident response teams focus on evaluating the response process, identifying improvements, and implementing changes to prevent similar incidents in the future. Here are key questions to guide this stage:

1. Prevention of Similar Incidents

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

Enhanced Security Awareness Training: Provide employees with ongoing training that emphasizes the importance of locking workstations and secure physical access protocols, especially in sensitive areas.

Automatic Session Locking: Implement technical controls to ensure that all workstations automatically lock after a short period of inactivity, particularly those with access to sensitive data.

Strengthened Physical Security: Add measures such as badge-in/out requirements and monitor surveillance in sensitive areas, like payroll or records offices, to detect unauthorized access attempts.

Access Policy Review: Review and possibly update policies around physical and digital access control, ensuring that only necessary personnel have access to high-risk areas.

Multi-Factor Authentication (MFA): Apply MFA to critical systems and applications to provide additional layers of access security, especially if a session is resumed on an unlocked workstation.

2. Improving Detection

What could be done to improve detection of similar incidents?

Implement Enhanced Monitoring Tools: Deploy additional monitoring solutions, such as DLP (Data Loss Prevention) software or privileged access monitoring tools, that can detect unusual activity on sensitive accounts and workstations.

Regular Log Audits: Increase the frequency of access and activity log audits in sensitive areas, ensuring that unusual activities are detected promptly.

Behavioral Analytics: Use advanced threat detection solutions capable of identifying anomalous behavior patterns on user accounts or devices, which can detect physical and digital threats early.

Integration with Physical Security Systems: Strengthen the integration between physical and digital security systems, ensuring that the CSIRC can view alerts from both digital endpoints and physical access points in real-time.

Engage MSSP for Proactive Monitoring: Ensure the Managed Security Service Provider (MSSP) is fully integrated into physical and cybersecurity monitoring so they can assist in real-time detection of similar incidents around the clock.

3. Documentation and Lessons Learned

Conduct an After-Action Review (AAR): Hold a post-incident review meeting involving all relevant teams to document the incident, response actions, and any gaps or challenges encountered.

Update Incident Response Playbooks: Revise existing incident response plans and playbooks to incorporate lessons learned from this incident, addressing identified gaps and outlining improved response steps.

Regular Testing and Drills: Schedule regular incident response drills that simulate similar incidents, combining physical and digital response activities to improve readiness.

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?