Name: Enid Shilwatso

Student ID: 671055

Lab4Instructor: Professor Dennis Kaburu

Assignment: Lab 28.4.13 - Incident Handling

Title: Advanced Information System Security

Course: ISC6120

Due: Summer 2025

Scenario 1: Worm and Distributed Denial of Service (DDoS) Agent Infestation

Preparation:

- What incident response plan (IRP) is in place for malware outbreaks and DDoS attacks?
- Are all employees trained on identifying suspicious removable media and safe file-sharing practices?
- Are regular backups performed, and are they tested for restorability?
- Is there an inventory of all systems and their configurations?
- Are endpoint detection and response (EDR) solutions deployed on all workstations?
- Are network segmentation strategies in place to limit the spread of malware?
- What are the communication protocols with external security experts?
- Are baseline network traffic patterns established to identify anomalies?
- Are sufficient resources allocated for incident response, including personnel and tools?

Detection and Analysis:

- How was the worm initially detected (e.g., user reports, antivirus alerts, network anomalies)?
- What is the scope of the infection? How many systems are affected?
- What specific files or processes are associated with the worm and the DDoS agent?
- What is the entry point of the worm into the network (e.g., specific removable media, exploited share)?
- Is the DDoS agent active, and if so, what targets is it attempting to attack?
- What is the timeline of the infection spread?
- Are there any indicators of compromise (IoCs) that can be used for further detection?
- What data has been exfiltrated or compromised by the worm or DDoS agent?
- What are the potential business impacts of the widespread infection and potential DDoS activity?

Containment, Eradication, and Recovery:

- What immediate steps can be taken to contain the worm's spread (e.g., disconnecting infected systems, disabling shares, blocking malicious IPs)?

- How will the DDoS agent be neutralized on infected hosts?
- What is the priority for system restoration based on business criticality?
- What is the process for cleaning infected systems, and will it involve re-imaging or specialized tools?
- How will data integrity be ensured during the recovery process?
- Are there any forensic images that need to be taken before remediation?
- How will systems be brought back online to minimize disruption?
- What steps will be taken to prevent re-infection?
- Are the external security experts actively involved in the eradication and recovery phases?

Post-Incident Activity:

- What lessons were learned from this incident?
- How can the incident response plan be improved based on this experience?
- Were the existing security controls effective, and what new controls are needed?
- Was the communication plan effective during the incident?
- What specific training should be provided to employees to prevent similar incidents?
- What changes need to be made to vulnerability management and patching processes?
- How will long-term monitoring be enhanced to detect similar threats?
- Was there any regulatory or legal reporting requirement for this incident?
- What documentation needs to be updated following this incident?

Scenario 2: Unauthorized Access to Payroll Records

Preparation:

- What physical security policies are in place for securing workstations and sensitive areas?
- Are employees regularly trained on workstation security, including locking their screens when unattended?
- What access controls are in place for the payroll system and related data?

- Is there a clear incident response plan for physical security breaches and unauthorized access to sensitive data?
- What agreements are in place with the MSSP regarding incident detection, reporting, and initial response?
- Are surveillance systems (CCTV) in place and properly monitored in critical areas like offices with sensitive data?
- What is the protocol for reporting suspicious physical activities?
- Are forensic tools and capabilities readily available to the distributed incident response teams?
- How does the coordinating team facilitate communication and collaboration among distributed teams and the MSSP?

Detection and Analysis:

- What is the exact timeline of events, from the administrator leaving the workstation to the physical security team's call?
- What specific actions were performed on the payroll program, if any, after the administrator left?
- Were there any other systems or applications accessed from the compromised workstation?
- Are there logs (e.g., system logs, application logs, security logs) that can provide evidence of activities on the workstation?
- Can the identity of the unknown person be determined from physical security footage or other means?
- What payroll records or sensitive data could have been accessed or exfiltrated?
- How will evidence be acquired and preserved according to forensic best practices?
- What is the potential impact of this unauthorized access on employee privacy and regulatory compliance (e.g., HIPAA)?
- How will the Kill Chain model be applied to understand the adversary's actions and intent?

Containment, Eradication, and Recovery:

- What immediate steps need to be taken to secure the compromised workstation and the payroll system (e.g., changing passwords, disabling accounts)?
- How will potential data exfiltration be contained (e.g., network monitoring, blocking suspicious outbound connections)?
- What steps are required to ensure the integrity and confidentiality of the payroll data?
- Does the workstation need to be isolated for forensic analysis?
- How will access to the payroll system be re-secured and monitored going forward?
- What actions are needed to "eradicate" the threat, including removing any potential backdoors or unauthorized access methods?
- What is the recovery plan for any compromised payroll data or systems?
- Are there any legal or HR implications that need to be addressed immediately?
- How will the distributed incident response teams and the coordinating team work together to contain and recover?

Post-Incident Activity:

- What changes are needed to physical security policies and procedures?
- How can employee training on workstation security be enhanced to prevent recurrence?
- Were the existing access controls for the payroll system sufficient, and what improvements are needed?
- How effective was the coordination between the physical security team, the distributed IR teams, the coordinating team, and the MSSP?
- What improvements can be made to the incident response plan, particularly for physical security incidents?
- What legal and regulatory reporting requirements need to be met (e.g., data breach notifications)?
- What follow-up actions are required to ensure the long-term security of payroll records?
- How will the VERIS database be used to document and analyze this incident for future reference?
- What post-incident review and debriefing sessions will be conducted?