CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #12 - Option C

Team: Project Team 11
Participants: Sohal Patel, Erika Maglasang, Nathan Moran, Gabriel Rolink, and Tyler Samuelson

Logistics

A. Get together with other students on your assigned team in person and virtually.
B. Review the three options available and decide on only one to pursue as a team.
C. Discuss and complete this assignment in a collaborative manner. Don't just assign different problems to each teammate as that defeats the purpose of team-based learning.
D. Choose a scribe to prepare a final document to submit via Blackboard for grading, changing the file name provided to denote the number of your assigned **Team**.

Problem 1
Digital forensics are often used for two key purposes, investigating allegations of digital malfeasance and performing root-cause analysis. Compare and contrast these purposes. *(10 points)*

Answer
Digital Forensics: "Investigations that involve the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and root cause analysis. Like traditional forensics, digital forensics follows clear, well-defined methodologies but still tends to be as much an art as a science."
Digital forensics is used to make an in-depth investigation of a specific incident that occurs. The incident is preserved, identified and documented, similar to how regular forensic operations operate. Digital Forensics leads to investigation of cybercrimes during and after a digital crime occurs. Here are the two key purposes of digital forensics:

- **Investigating allegations of digital malfeasance:** "Such an investigation requires digital forensics to gather, analyze, and report the findings. This is the primary mission of law enforcement in investigating crimes that involve computer technologies or online information."
    - Digital malfeasance is when the computer is the source of the crime or the object of it. This operates similarly to a criminal investigation. Key actors in the incident will be questioned about where they were and what they were doing on the computer. The systems logs will be accessed and looked over. These documents into account for the remainder of the investigation. These investigations occur after a theft or damage to the system has happened. In every crime criminals' clues are left and digital forensics will find these clues.
- **Root Cause Analysis:** " If an incident occurs and the organization suspects an attack was successful, digital forensics can be used to examine the path and methodology used to gain unauthorized access, and to determine how pervasive and successful the attack was. This type of analysis is used primarily by incident response teams to examine their equipment after an incident."

- A Root cause analysis is used to detect how the intruder made it to the system. The analysis will also reveal what method they used when they broke into the system. The incident response plan of the organization will be put into effect after the analysis has been conducted.

Problem 2

The handling of data acquired during a digital forensics' investigation requires special care. During an audit of your organization, potential evidence of fraud and embezzlement are uncovered in the accounting information system. Your digital forensics team is brought in to acquire and analyze the relevant data. Describe any special responsibilities your team has related to the handling of this data given the potential need for legal use in a later prosecution. Be sure to address the chain of custody (chain of evidence) and how your team will demonstrate that any analyzed copy or image of the data is a true and accurate replica of the source evidentiary material. *(15 points)*

Answer:

The chain of evidence: "The detailed documentation of the collection, storage, transfer, and ownership of evidence from the crime scene through its presentation in court."

The chain of evidence can be described as a detailed documentation following where the evidence goes from person to person. If the evidence is tracked and stored correctly; the potential risk of the incident occurring again will be reduced.

These are the five steps that our team should take:

1. Identify relevant evidentiary material.
2. Acquire the evidence without alteration or its damage.
3. Take steps to assure that the evidence is verifiably authentic at every step and is unchanged from the time it was seized.
4. Analyze the data without risking modification or unauthorized access.
5. Report the findings to the proper authority.

We will: identify the evidence, acquire the evidence for our investigation, Store the evidence in a safe location so that it is not accessed by unauthorized personnel, analyze the data being sure not to change or alter it, and report our findings to the appropriate authorities so that future actions can be taken. During our investigation process we will be documenting every instance where the evidence is accessed through the use of digital logs. Two factor authentication will be used to access the evidence. Finally, more than one person must be present when accessing the evidence to ensure that no one alters it. Having another person in the room will ensure everyone's actions are accounted for.

Work Cited

Whitman, M. E., & Mattord, H. J. (2018). Chapter 12 Information Security Maintenance. In Principles of information security (pp. 478- 480). Australia: Cengage Learning.