CIS 481 – Intro to Information Security

IN-CLASS EXERCISE # 12

Names of team members: **Trisia Baltazar, Adrian Boone, Savanah Kennedy, Ryan Smith**

Logistics

A. Get into your regular team

B. Discuss and complete the assignment together. Don't just assign different problems to each teammate! That defeats the purpose of team-based learning.

C. Choose a recorder to prepare the final copy to submit to instructor in Blackboard.

Problem 1

List and briefly describe the five domains of the security maintenance model recommended by the text. See Figure 12-4 on p. 651 of the text for an overview. (10 pts.)

1. **External Monitoring: The component of the maintenance model that focuses on evaluating external threats to the organization's information assets.**
2. **Internal Monitoring: The component of the maintenance model that focuses on identifying, assessing, and managing the configuration and status of information assets in an organization.**
3. **Planning and Risk Assessment: The component of the maintenance model that focuses on identifying and planning ongoing information security and activites and identifying and managing risks introduced through IT information security projects.**
4. **Vulnerability assessment and remediation: The component of the maintenance model focused on identifying specific, documented vulnerabilities and remediating them in a timely fashion.**
5. **Readiness and review: Ensures that the information security program is functioning as designed and keep improving it over time.**

Problem 2

Is the term *ethical hacker* truly an oxymoron? What's the difference between a pen tester and a hacker? See pp. 667-669 of the text for more information. (7 pts.)

Yes the term ethical hacker is an oxymoron. A hacker under the modern definition goes against all values an information security professional is supposed to have. The major difference between a pen tester and a hacker is authorization. Pen testers are hired by an organization and actually serve to improve the information security. A hacker does the exact opposite and attacks the organization to harm it. The intentions between a pen tester and a hacker are vastly different. An attack from a pen tester will result in a positive for the organization, while an attack from a hacker will be a negative.

Problem 3

Describe the basic methodology involved in most all digital forensics investigations (listed on p. 680). (8 pts.)

1. **Identify relevant evidentiary material. This means relevant items that fit the description on the authorization can be seized. Item descriptions help ensure critical evidence is not overlooked. Thorough descriptions also help make sure items are not wrongly included as EM. Investigators need to know what they are looking for if they ever expect to find it, since people can own terabytes of data.**
2. **Acquire (seize) the evidence without alteration or damage. When a file is modified, even slightly by just opening it, the integrity or authenticity of the evidence could be questioned by attorneys. This can cause a jury to suspect the evidence was planted. It is important to acquire evidence without alteration or damage to prevent that. Data can be acquired online or offline.**
3. **Take steps to assure that the evidence is verifiably authentic at every step and is unchanged from the time it was seized. This is important for preserving integrity and authenticity. Investigators must track and document the movements, storage, and access of evidence once they have acquired it until the resolution of the event or case. This is accomplished through chain of evidence procedures. Digital media is stored in a specially designed environment that can be secured, so it does not have unauthorized access.**
4. **Analyze the data without risking modification or unauthorized access. Applications such as Guidance Software's EnCase and AccessData Forensics Tool Kit can be used. Open-source alternatives such as Autopsy and The Sleuth Kit could also be used. Each tool supports an investigation and assists management of the entire case. The first component of the analysis phase is indexing. Many investigatory tools create an index of all text found on the drive, including deleted files and file slack space. The index can be used to locate specific documents or document fragments. Indexing organizes files into categories, such as documents and images. Indexing is time and processor consuming, however. Password cracking tools like AccessData Password Recovery Tool Kit can be used to assist investigators.**
5. **Report the findings to the proper authority. Once the copies or images have been analyzed and potential EM has been identified, investigators can tag it and it it to their case files. Once they have found, what they consider to be, a suitable amount of information they can summarize their findings with a synopsis of their investigatory procedures in a report submitted to the appropriate authority. This could be law enforcement or management. Reporting methods and formats vary among organizations. They should be specified in digital forensic policies. The report should be detailed enough so that a similarly trained person can repeat the analysis and achieve similar results.**