CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #12 - Option A

Team: 3
Participants: Brandon Crosier, Aaron Gordon, Kitrina Justus, Sam Steele, Marvin Weaver

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
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 points)*

The five domains of the security maintenance model are external monitoring, planning and risk assessment, internal monitoring, readiness and review, and vulnerability assessment and remediation.
External monitoring focuses on evaluating external threats to the organization. These include hackers, other companies, other governments, and so on. It provides early awareness of new and upcoming threats and threat agents, as well as new vulnerabilities. This ensures the company can come up with a plan of defense.

Planning and risk assessment focuses on identifying ongoing information security activities and managing the risks associated with them. For example, if a certain practice, such as password storage, is analyzed and revealed to leave the company vulnerable to attack, this step analyzes how to reform the practice to mitigate the risk.

Internal monitoring focuses on identifying the state of the organization's networks, information systems, and defenses. They look at their current system and where there may be vulnerabilities that need to be addressed, such as a backdoor. This way, the company can protect itself internally.

Readiness and review focuses on the continuance of the information security program and the continued improvement of it. This includes policy and program reviews to ensure everything is accurate and offers the needed protection. They also rehearse the measures they have taken to see if they are falling short and need to be improved.

Vulnerability assessment and remediation focuses on remediating the vulnerabilities identified in the rest of the maintenance process. It works to solve these vulnerabilities in a timely manner so that the company is not at risk for long. This involves penetration testing so that the company can see where the system is vulnerable and then work to rectify that.

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 points)*

With the modern-day definition of a hacker, the phrase ethical hacker is an oxymoron as being a hacker means gaining unauthorized access to a computer system. However, the practice of an ethical hacker is legitimate and not an oxymoron as the original definition of a hacker is simply a computer enthusiast who uses uncommon techniques. It is entirely possible to remain ethical, but just unique in how you accomplish tasks. Unfortunately, the societal definition of a hacker forces the phrase to be oxymoronic. Since a modern hacker does not abide by the rules and standards set by the information technology industry, they cannot act ethically.

A penetration tester, or pentester, acts in a similar way to a hacker, except they have permission to do what they do. A pen tester finds vulnerabilities in an information system by adopting the techniques of a hacker, including trying to access backdoors and bypass security measures. They are hired by the company to see where the company falls short in security that way they can prepare for a real threat by a real hacker. The company knows pentesters are trying to bypass the security of the system, and encourages it to show them where they have vulnerabilities. A hacker is not contracted by the company, thus making them act illegally.

Problem 3

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

Step one in a digital forensics investigation is to identify relevant evidentiary material. An affidavit or search warrant must be obtained in order to search for such evidence. Only the items that fit the description on the authorization can be seized. Items that are seized that don't match the description could jeopardize the investigation.

Step two of the investigation is to acquire the evidence without altering or damaging it. There are two ways of doing so: online and offline. Offline requires the removal of the power supply and the use of a device to make a copy of the hard drive. This is done using bitstream, where the drives are copied sector by sector to ensure that any hidden or deleted files are captured. In online data acquisition, investigators use network-based tools to acquire a protected copy of the information. The only difference between online and offline is that the system cannot be taken offline. The tools used in online acquisition must also be good enough to avoid altering the system during the process.

Step three is to authenticate the evidence. The copy is transferred to the lab for the next stage of authentication. In the lab, cryptographic hash tools are used to authenticate the copy is true and an accurate replica of the source EM.

The fourth step is to analyze the data. The first step in the most complex part of the investigation is indexing. During this step, investigatory tools create an index of all the text found on the drive, including all data found in deleted files. The index is then used by investigators to locate specific documents or partial documents. FIles during this stage are categorized, typically into files type. If password-protected files are found, commercial password tools are used to crack the files.

The final step is to report the findings. Files, images, and any other copies or EMs are added to case files as they are analyzed. After a suitable amount of evidence has been gathered and analyzed, a summary can be written about their findings as well as a synopsis of their procedures and processes that led them to that point. This report and summary is then submitted to the proper authority. A suitable amount of evidence is circumstantial determined by the investigators. Reporting methods and formats can vary among organizations and should follow their forensic policies, but, in general, the report should be sufficiently detailed to allow a similarly trained person to duplicate the procedures and achieve a similar result.