CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #12 - Option A

Team: 5
Participants: James Hoagland

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 *(10 points)*
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.

The five domains of the security maintenance model are external monitoring, internal monitoring, planning and risk assessment, vulnerability assessment and remediation, and readiness and review.
External monitoring domain is the component of the maintenance model that focuses on evaluating external threats to the organization's information assets.
Internal monitoring domain is the component of the maintenance model that focuses on identifying, assessing, and managing the configuration and status of information assets.
Planning and Risk Assessment is the component of the maintenance model that focuses on identifying and planning ongoing information security activities and identifying and managing risks introduced through IT information security projects.
Vulnerability and Remediation is the component of the maintenance model focused on identifying specific, documented vulnerabilities and remediating them in a timely fashion.
Readiness and Review is the component of the maintenance model that details how a threat is to be handled and then reviewed for effectiveness.

Problem 2 *(7 points)*
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.

Yes, the term ethical hacker is truly an oxymoron, because it is now generally accepted that a hacker has no regard for polices, rules, and regulations involved with the ethical use of computer resources. However, there is a difference between hacking and pen testing, which is the actions taken by an information security professional to thoroughly test and assess an organization's data, information assets, and their security posture which would involve allowing access to the root information and data by bypassing security controls. Most professional information security organizations feature pen testing, and lots of information security professionals even receive training in the art.

Problem 3 *(8 points)*

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

Digital forensics are investigations that involve the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and root cause analysis. When it comes to the basic methodology involved with digital forensics investigations it goes as follows:

1) Identify relevant EM: the affidavit or warrant that authorizes a search must identify what items of evidence can be seized and where they are located. EM that fits a certain description can only be seized.

2) Acquire the evidence without alteration or damage: the response team is responsible for acquiring the information without altering it. You can acquire evidence from a system by the offline model or through online / live data acquisition.

3) Verify and authenticate recovered evidence: evidence is transferred to a lab for the next stage of the authentication process. The lab will use hash tools to be able to demonstrate that any analyzed copy or image is true and accurate.

4) Analyze the data: here we are analyzing the copy or image for potential EM in one of the most complex parts of the investigation. You can either do it manually or use applications such as: Guidance Software's EnCase, AccessData Forensics Tool Kit, OSForensics, etc. From there you must index what you have gathered.

5) Report findings: investigators will examine the analyzed copies or images in which they can tag it and/or add it to their case files. Investigators will then summarize their findings and submit them to the appropriate authority.