**CIS 481 – Intro to Information Security**

**CLASS EXERCISE # 12**

Grading ID: A7386

**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.)

External monitoring: Used to provide awareness of new and emerging threats, vulnerabilities, and attacks so that a defense can be mounted in advance.

Internal monitoring: Used to ensure that vulnerabilities that occur within the company are found and repaired before they can be exploited.

Planning and Risk assessment: Used to identify and plan ongoing security activities that reduce risk and protect primary assets. Important assets are identified and strategies for protecting them are formulated and implemented.

Vulnerability assessment and remediation: Identification of specific, documented vulnerabilities and their timely remediation. Involves tracking vulnerabilities once they are identified, monitoring their status, and ensuring the proper level of management is involved so that they are made aware and a fix can be implemented.

Readiness and review: Used to ensure that a company is prepared in the event of an attack and that individuals responsible for the response and recovery to that attack are trained and up-to-date on the procedures that take place in that event.

**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.)

Ethical hacker can be considered an oxymoron, but there are cases where the term applies. White hat hackers are known for hacking into systems in order to expose vulnerabilities, but instead of exploiting them, they present them to the owner of the system for review. These types of hackers are often contracted or act as consultants for companies. A pen tester is an employee within a company that simulates an attack to detect vulnerabilities within a system, while a hacker commits a real attack in order to exploit the vulnerabilities.

**Problem 3**

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

Digital forensics is used to document what happened during an attack and how it occurred. Most investigations involve the preservation, identification, extraction, documentation, and interpretation of digital media for evidentiary and root-cause analysis. This process ensures that the material is not tampered with or altered, and remains in the same state that it was in following the attack. By following these steps, investigators can ensure that the evidence found is credible and accurate.