**CIS 481 – Intro to Information Security**

**IN-CLASS EXERCISE # 12**

Names of team members:

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.)

*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.*

***The 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 in an  
organization.*

***Planning and Risk Assessment Domain*** *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 Assessment and Remediation Domain*** *is the component of the maintenance model  
focused on identifying specific, documented vulnerabilities and remediating them in a timely  
fashion.*

***Readiness and Review Domain*** *is to keep the information security program 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.)

*The book specifies that ethical hacker is an oxymoron and makes a specific distinction between penetration testers and hackers. Though we can see where they are coming from and why they would make this separation, we aren’t certain that penetration testing is the only useful or ethical activity. The industry consensus seems to be that only authorized penetration testing is ethical. Though that argument is sound, a more utilitarian view of the situation lends one to see that there is greater benefit from the exposure of previously unknown vulnerabilities from unauthorized activities. It is our opinion that allowing the danger to companies and consumers from these vulnerabilities to persist is unethical, as there are neither enough funds or qualified penetration testers to test for all possible vulnerabilities. Searching for them is the main goal of hackers, however, and if they are allowed to discover it and exploit it first, that is unacceptable.*

**Problem 3**

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

**Identify relevant EM**: This usually requires a warrant, and only EM that fits the warrant  
description is liable to be seized. Include thorough item descriptions.

**Acquire evidence without alteration or damage**: Unnecessary modifications of the files  
can be portrayed as tampering or planted evidence, thus it is important to access the files   
without triggering a user or system state change beyond what is actually required to get  
the files.

**Take steps to ensure that the evidence is verifiably authentic at every step and is  
unchanged from time of seizure**: This uses hash tools to illustrate that the file is  
unchanged, proving the authenticity of the duplicate.

**Analyze the data without risking modification/unauthorized access**: To do this, there are  
a few tools and steps. First is indexing, which is functionally a search tool, but takes days  
on large images. You also must get around password protected files.

**Report findings to proper authority**: This step involves tagging and adding findings to  
case files, then reporting it to management or law enforcement.