CIS-481: Introduction to Information Security

Module 12 - Information Security Maintenance

Exercise #12

Team: 5
Participants: Charles Degboe, Sam Martin, Abril Beascoechea, Ricardo Portillo, Nicholas Zhang

Logistics

A. Get together with other students on your assigned **Team** in person and/or virtually.
B. 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 and may impact your performance on assessments, especially with respect to the essay questions.
C. 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. Reference Figure 12-4 on page 470 of the text for an overview.

External monitoring - External monitoring focuses on identifying and mitigating external threats to the organization's network.

Internal monitoring - Internal monitoring focuses its efforts on identification and mitigation of internal threats

Planning and risk assessment - This is a disaster preparedness technique that focuses its efforts on the identification, classification, and mitigation of risk.

Vulnerability assessment and remediation - This domain is involved with analyzing an information system to identify and mitigate vulnerabilities that may be exploited to hurt Confidentiality, Integrity, and Availability.

Readiness and review - This domain is concerned with consistently revising an information system to check its viability in the face of attacks.

Problem 2 *(7 points)*

Is the term *ethical hacker* truly an oxymoron? What's the difference between a pen tester and a hacker? Reference pages 483-484 of the text for details.
The term ethical hacker is not an oxymoron. An ethical hacker is someone who uses their hacking skills for positive purposes, such as identifying security vulnerabilities in systems and networks so that they can be fixed before malicious hackers exploit them. These people are usually hired by companies. A hacker has malicious intent, a pen tester works to find the exploits and fix them.

Problem 3 *(8 points)*
Your text describes three elements that must be present for a fire to ignite and continue to burn. Newer research suggests a fourth element is required, too. See:

https://www.firesafe.org.uk/information-about-the-fire-triangletetrahedron-and-combustion/

Name and describe each of the four elements of the "fire tetrahedron" in this article. How do fire suppression systems manipulate these four elements to quell fires?

1. Heat: sufficient heat to raise the material to its ignition temperature.
2. Oxygen: presence of oxygen in order for a rapid oxidation to occur.
3. Fuel: a combustible material.
4. Chemical Chain Reaction: an exothermic chemical chain reaction in the material.

All four of the elements need to be present for fire to occur. The fire can be extinguished by taking away one or more of the elements in the fire tetrahedron. For example, using a foam to create a barrier between the combustible material and oxygen as well as reducing heat. By applying water to reduce its temperature below the ignition point. Or "mopping up" the free radicals in the chemical reaction using BCF and other halon extinguishers.