**CIS-481: Introduction to Information Security**

**Module 12 - Information Security Maintenance**

**Exercise #12**

**Team: 2**

**Participants: Carter Rowe, Megan Tharp, Madison Heil, Andrea Ballena, Addison Phillips**

**Logistics**

1. Get together with other students on your assigned **Team** in person and/or virtually.
2. 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.
3. 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: This first domain focuses on any external threats to an organization. This type of monitoring aims to be proactive and focuses on catching new threats and vulnerabilities early so that they can more easily be defended against. There are a couple of different sources when it comes to threats, such as the vendors, CERT organizations, the internet / other public sources, and membership sites. All this information is compiled and fed into a database. The information must be analyzed in relation to the organization’s security environment so that it can be appropriately used.

Internal monitoring: This second domain is internal monitoring, which is the part of the maintenance model that looks at information assets that are within an organization. The goal of this domain is to increase awareness on the state of the organization’s internal components, such as their networks, information systems, and security defenses. Internal monitoring involves a couple of activities, such as monitoring IT activities in real time and monitoring the organization’s networks and systems. Organizations should also keep track of their hardware, software, network devices, and communication channels for their monitoring.

Planning and risk assessment: The third domain is the planning and risk assessment domain, which watches over the entirety of the information security program. One of the largest parts of what this domain does is risk assessment, so they focus on identifying activities, or making modifications to activities in order to reduce risk within the organization. They are heavily involved in doing reviews within multiple sectors for assessment purposes – and risk assessment plays into this as well. The information that they collect and analyze helps the executives in the organization make informed decisions about multiple issues such as funding / budgeting, projects, and large organizational changes.

Vulnerability assessment and remediation: The fourth domain is the vulnerability assessment and remediation domain, which focuses on vulnerabilities that have already been identified so that they can work to get them resolved as soon as possible. Lots of information regarding the vulnerability itself along with background information is collected so that a vulnerability assessment can occur, along with the associated procedures. There is always an associated risk level with vulnerabilities in relation to what it compromises, and what the time to resolution means for the organization, which is included in this domain. There are four vulnerability assessment processes as well, which are internet VA, intranet VA, platform security validation, and wireless VA. These processes help the organization balance the intrusiveness that comes with the VA with the need for a stable production environment.

Readiness and review: The fifth domain is the readiness and review domain, which focuses on keeping the information security section running and evolving as needed. As with most other programs in the world, they must continuously evolve to keep up with external and internal threats. For the review and readiness domain, they accomplish this by doing policy reviews, program reviews, and rehearsals. Policy reviews are conducted to ensure that they’re still reliable and functioning as they should. Program reviews are conducted as an independent review to focus on what’s working, and what’s not – and whatever parts that may not be working must be improved upon. Lastly, the rehearsals occur to ensure that the current procedures work, and if they don’t, they help us identify how they could change. A type of rehearsal is a war game, which is a simulation exercise within a test environment – this assists in making the rehearsal more realistic and may be better suited to identifying shortcomings.

**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.

Although the words themselves are an oxymoron, an ethical hacker is not truly one. When people think of hackers, they automatically think of someone who is dangerous, and is trying to use their skills negatively. With today’s world, organizations have so much sensitive data that they need to protect, and they are subject to hackers. Ethical hackers use their hacking skills to help keep information safe. In fact, many organizations will hire white hat hackers to hack into their systems in order to see where they need to improve security. This hacker is not stealing any data or harming the company. They are helping them to see the vulnerabilities, and it is in fact a job. This hacker helps to deter attacks and malicious behavior and is very useful.

A pen tester is someone who does a set of security tests that make it seem as though a hacker is attacking. It is part of a full security audit. The pen tester goes as far into the company's data as they can, identifying weaknesses in the system security and networks. They then present these vulnerabilities in a detailed report to the systems owner. Pen testing can be done in 1 of 2 ways: black box and white box. Black box pen testing is also called blind testing and is where the “attacker” does not have any knowledge of the system or network before they “attack” it. White box testing is also called full-disclosure testing and is where the organization gives the “attacker” information about the system in order to make the testing faster and more focused. The difference between a pen tester and a hacker is authorization. Pen testers get permission to investigate a system and recommend solutions for the faults they identify. Pen testers must document what they find. Hackers, comparatively, do not have any obligation to help the organization. They have motives to benefit only themselves. The motivation and intent are what truly matters.

**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?

The text describes the temperature of the ignition source, fuel, and oxygen as the three elements that must be present for a fire to ignite and burn. Different materials have varying flame points. Paper, a fuel source, is the most common of these materials in an office and can be ignited from cigarettes, electrical malfunctions, or on purpose. However, fires cannot occur without oxygen which is why certain suppression systems let out carbon dioxide to rid fire of oxygen.

The fourth element introduced is a chemical chain reaction. This is the combination of the previous three elements. Fires start through the process of rapid oxidation (a chemical reaction). This process occurs when a reducing agent and oxidizing agent are present, and heat is added. If one element is missing a chemical chain reaction cannot occur. For this reason, fire suppression systems target one or all the elements listed. Extinguishers cut off the supply of oxygen and reduce the heat of the fire by creating a barrier. Water will lower the temperature of the ignition source to one that is below the flame point. Using halon or BCF extinguishers would prevent chemical reactions from occurring all together.