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

**In-Class Exercise #2 - Option A**

Names of team members: Elise Timmons, Trevor Rawleigh, Samantha Conway, Noah Smith

Logistics

A. Get together with other students on your assigned team

B. Discuss and complete the assignment together. Don’t just assign different problems to each teammate as that defeats the purpose of team-based learning.

C. Choose a scribe to prepare a final document to submit via Blackboard for grading, changing the file name to denote the number of your assigned team.

**Problem 1**

Why is information security a management problem? What can management do that technology alone cannot? *(5 points)*

Information Security is a management problem because management is responsible for dealing with all issues that may arise from the organization, including Information Security. Technology and information is needed to run the company and therefore any threats to that need is a problem that management must be aware of.

**Problem 2**

Why do employees constitute one of the greatest threats to information security that an organization may face? *(5 points)*

Employees have access to all of the information that their company has. This level of responsibility can lead to human errors that result in losses or corruption of that information. A company can spend all of the money they have for the best Information Security and yet if an employee can be convinced or just decide to use their level of access for malicious intent no protective system can stop them.

**Problem 3**

How can dual controls, such as two-person confirmation, reduce the threats from acts of human error and failure? Describe two other controls that can also reduce this threat? *(5 points)*

Dual Controls reduce the threats from acts of human error and failure because while one person could create an error and continue without knowledge, with two people, or double authentication, to check modifications there is an increase in chance that one or the other will catch any human error.

Other controls include risk training and ongoing awareness activities that help keep employees informed of all threats that could happen and what an employee can do to prevent and protect their organization. Having a well-aware team helps to reduce mistakes that lead to information losses.

**Problem 4**

What is the difference between a regular denial of service (DoS) attack and a distributed denial of service (DDoS) attack? Which is harder to combat? Why? *(5 points)*

A regular denial of service (DoS) is a single attack that attempts to prevent authorized access to incoming communications to delay time-critical operations. While a distributed denial of service (DDoS) is a multitude of hosts that proceed to attack the legitimate users in a coordinated stream of attacks. The DoS attack is much easier to rectify because the attack is not coming from multiple IP addresses and is therefore easier to track or block. DDoS is harder to combat because the attacks can be organized in waves and from many bots/zombies.

**Problem 5**

Briefly describe the types of password attacks addressed in Chapter 2 of your text? Describe three controls a systems administrator can implement to protect against them? *(5 points)*

Brute Force Attacks – These attacks create every single possible combination of a password and try to forcefully make their way into a system.

Dictionary Attacks – This type of password attack is similar in style to a brute force attack, except that it attempts to find words within a password dictionary, narrowing their attempts from the regular brute force direction. These password dictionaries can be personal to the intended target but could also be more commonly known/used passwords.

Rainbow Table Attacks – This password attack is the most complicated of the three mentioned. Precomputed tables of hash values and corresponding plaintext possible passwords. A system’s encrypted password files is needed to implement this.

A system administrator can implement a multi-factor authentication to make attacks take more time because of complications.

They could also implement a 10.4 Password Rule throughout the organization. This would create stronger passwords that would discourage attacks.

Lastly and possibly the simplest way to protect against these attacks is through password input limits. This would stop brute force attacks after three tries and shut the attack down.