CIS-481: Introduction to Information Security

Module 2 - The Need for Information Security

Exercise #2

Team: 4
Participants: Aneesa Bell, Paige Hensley, Patrick Nguyen, Logan Whaley, Emily Wyland

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

> **Through management, security policies are made and enforced. Technology cannot do that. Management also deals with risk management and chooses the technology for disaster recovery. Additionally, management handles the training and policies applied to the staff who use the technology, such as anti-phishing training, company best practices, and what to do in a security breach.**

Problem 2 *(5 points)*
Why do employees constitute one of the greatest threats to information security that an organization may face?

> **Humans are often more prone to mistakes than technology. This is especially true for social engineering-based attacks which rely almost entirely on human error and susceptibility.**

Problem 3 *(5 points)*
How can dual controls, such as two-person confirmation (sometimes referred to as the two-man rule), reduce the threats from acts of human error and failure? [You've probably seen an example of this in a movie that shows how a nuclear weapon requires two keys, held by two different people, to be launched.]

> **Dual control requires that two people review something before initiating it. An example could be that a group of workers are attempting to submit highly confidential data. The potential of data loss could have a tremendous impact on the organization if human error is made. The use of dual control allows for multiple people to review the information to ensure that no mistakes are made.**

Describe two other common controls that can also reduce this threat.

Two other controls are requiring the user to type a command twice and verifying commands by a second party. Requiring a user to type a command twice ensures that the user can verify that their command isn't going to violate confidentiality with the data. Mistakes can occur and the user may type a command with unintended information in it. As for verifying commands by a second party, this allows for another person to look over the command to ensure confidentiality isn't violated.

Problem 4 *(5 points)*
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?

As the name would imply, DDoS involves multiple "users" across multiple locations as opposed to a single location DoS. With the increased number of users in DDoS, it becomes exponentially more difficult to track/block the attacker, thus making it far more difficult to combat.

Problem 5 *(5 points)*
Briefly describe the types of password attacks addressed in Module 2 of the text. Describe three controls a systems administrator can implement to protect against one or more of these types of password attacks.

The types of password attacks addressed in Module 2 are brute force, dictionary, rainbow table, and social engineering. Brute force password attacks involve trying every possible password combination. Dictionary password attacks occur when a hacker uses a dictionary of common passwords and personal information when attempting to guess a password. Rainbow table attacks involve a table of hash values and their corresponding plaintext values that can be used to look up the password. These types of attacks occur if a hacker was able to steal the system's encrypted password file. Lastly, password attacks by social engineering occur when a hacker poses as a trusted individual (IT professional) when communicating with the potential victim. The hacker will extract the password from the individual during their conversation.

Three controls that system administrators often use are: 10.4 password rule, using dictionaries to block common passwords and words, two-factor authentication.

To begin, the 10.4 password rule is an industry recommendation for password structure and strength. This control requires that passwords should be, at minimum, 10 characters long and contain an uppercase letter, lowercase letters, one number, and one special character. This is useful for brute force password attacks. As for the next control, users often create passwords that closely relate to themselves or words that are common in the dictionary. Organizations can use dictionaries to disallow certain passwords. Lastly, two-factor authentication is another control. This control requires that a user verifies their login credentials through an app or a code. In the instance

that someone can access an account without authorization, this helps prevent that person from logging.