CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #2 - Option A

Team: 6
Participants: Kelsey Beeler, Regis Wilson, Mahendra Khanal, Anthony Combs

Logistics

A. Get together with other students on your assigned team in person and virtually.
B. Review the two options available and decide on only one to pursue as a team.
C. 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.
D. 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
Why is information security a management problem? What can management do that technology alone cannot? *(5 points)*

In order to protect their company, management must take into consideration all of the information security needs. They must pair this with laws, regulations, and technology capacity. Taking all of this into account they must then create policies for the organization to follow and ensure they are constantly implemented and followed.
Even the best technologies cannot remove all factors of human behavior. This can include errors in technology programming or failure to follow the procedures set my management. Most technology has a narrow focus or objective and needs a wider human perspective to ensure successful implementation.

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

Human error is nearly impossible to totally erase. Simple neglect or lazy behavior can result in a loss in data integrity, resulting in errors. Technology also relies on the employees as the users, which leaves the system open to bad actors. These users have access to sensitive or critical data that can be manipulated or erased either through error or intentional actions. Many security systems are built to protect against outside actors and attacks but have failed to address internal threats.

Problem 3
How can dual controls, such as two-person confirmation, reduce the threats from acts of human error and failure? Describe two other common controls that can also reduce this threat? *(5 points)*

Due to the common nature of human error, dual controls can be implemented to reduce the likelihood of one person's ability to affect a system. This works by requiring commands to be verified by a second user. This does not only cut down on common errors but also makes it harder for bad actors to succeed in their efforts.

Limited access is another helpful tool that seeks to achieve the same goal by restricting access to only data pertinent to a user's job. Backups can be put in place to help secure data integrity should a control system fail.

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 DoS attack utilizes a single computer with internet connection to then target a system or resource. A DDoS attack utilizes several computers to attack a targeted source. A DDoS attack is harder to defend against because the requests are coming from multiple places. For a DoS, a simple defense is blocking the lone IP address.

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)*

- *Password attacks are categorized under trespass or espionage while lock-picking falls under breaking and entering.*
- *Brute Force attack is the use of computing and network resources to attempt all possible password combinations.*
- *Cracking is the attempt to reverse calculate a password or simply guessing.*
- *Dictionary is a form of a brute force attack that uses a dictionary of commonly used passwords related to the user being targeted. This can include pet names, important dates, or personal identifiable information.*
- *Rainbow Table is used for cracking password hash. It uses a table for cryptographic hash functions.*
- *Social Engineering is the process of manipulating an employee and gaining their trust. Once this is achieved, you can use them to act on your behalf or use the information you gained from them to attack a system.*

Three control systems administrators can implement to protect against them:

1. *Limiting the amounts of incorrect passwords, a user can input before locking down their credentials. This is especially effective against cracking attacks.*
2. *Secondary authentication is a great way to defend against many types of security threats. It is a quick way to alert another user of a possible issue or attack.*
3. *Having complex rules for passwords ensures that certain attacks such as a dictionary are not effective. It also avoids the use of commonly used passwords or overly simple ones.*