CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #2 - Option A

Team: 3
Participants: Brandon Crosier, Marvin Weaver, Kitrina Justus, Sam Steele, Aaron Gordon

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)*

Information security falls into the hands of the management of a company because management is responsible for facilitating security programs. Secondly, businesses rely on management to perform risk assessments. Furthermore, companies are spending hundreds of thousands of dollars daily to ensure that their company is safe from outside threats. Management is responsible for the implementation of information security for a company, technology alone cannot protect the well being of an organization's day-to-day functions. Management can also implement best practices and host training to ensure the employees know how to safely use their technology.

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

Employees can constitute a great threat to a company's information security via human error. These include acts that were performed without malicious intent or in ignorance; this is often caused by inexperience, improper training, or incorrect assumptions. A mistake made by an employee can easily lead to the: leaking of classified data, entry of erroneous data, deletion or modification, or data being stored in an unprotected area.

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)*

Dual controls reduce the threats from human error because the task or information being worked on is being passed through multiple levels of "security", different people reading and working on the task. With multiple eyes checking for faults or errors the probability of mistake being made. A couple of common controls systems have built-in are: requiring confirmation for every execution the user wants to make by requiring them to enter it twice or requiring a password and an RSA token.

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 attack is an attack that prevents authorized access to resources or delays time-critical operations. A distributed denial of service attack is a similar technique to a DoS attack except it is done by multiple hosts. It is much harder to combat a DDoS attack because it is coming from numerous IP addresses.

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)*

The types of password attacks are cracking, brute force, dictionary, rainbow tables, and social engineering. Cracking is the attempt to reverse calculate a password. The brute force attack occurs when a hacker tries every potential sequence of options as a possible password using computing and network resources. A dictionary attack uses a list of commonly used passwords to target specific accounts. Dictionary attacks can also include information related to the target user, such as phone numbers, addresses, and Social Security numbers. Rainbow table attacks use a table of plaintext values associated with hash values that can be used to lookup passwords if the hacker has access to the password file. Social engineering occurs when the hacker uses social skills to convince employees to reveal confidential information, like passwords.

One way to combat against a brute force attack and a dictionary attack is to increase the password complexity. Increasing the complexity of the password adds more characters making it more difficult for these two kinds of attacks because there are more characters that have to be guessed in the correct sequence. A way to increase password complexity is the addition of case sensitive or special characters. However, the most effective way to combat a brute force attack is to limit the number of attempts to get the correct password. The reason this is the most effective way to combat a brute force attack is that the attacker can not guess the correct sequence efficiently. Another way to combat these attacks is to use two-factor authentication. This strategy is the best way to defend against a rainbow table attack because, with this kind of attack, the attacker already has access to the encrypted password file. However, without the additional authentication method, they would not have access. The best way to combat social engineering is by educating your employees on security measures and ways to avoid getting compromised.