**CIS 481 – Intro to Information Security**

**IN-CLASS EXERCISE # 2**

Names of team members: Corey Cooley, Taylor Payne, Will Brown, & John Hopson

Logistics

A. Get into your regular team

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

C. Choose a recorder to prepare the final copy to submit to instructor in Blackboard.

**Problem 1**

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

*Information Security is a management problem because technology cannot control the user in the same way management must. Through management, there are policies and procedures that must be put in place in order to properly train and educate employees. Management has the authority to institute policies and procedures as well as fund and authorize training and education events and is why the top-down approach is most likely to succeed. Another reason management and training is important is due to the excess number of online attacks that target large companies and their employees in order to access sensitive information. These attacks include things like phishing or email spam. Organizations must protect their assets, and technology is the helper, but the employees hold the key to the safe.*

**Problem 2**

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

*Employees constitute one of the greatest threats to information security because after all, they’re only human. Employees are generally the closest to the organization’s data, and can make mistakes that lead to exposure of sensitive information, false data entry, accidental modification or deletion of information, and failure to protect information. These can all happen through hacking attacks like phishing, or just by employee ignorance or lack of proper training. Many of these threats can be prevented with training, ongoing awareness activities, and controls. That is why employee management in regards to information security is so important.*

**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 pts.)

*Dual controls ensure that a second set of eyes and a second brain are part of a process. This can help prevent errors and failures by making sure a conspiracy is required to carry out intentional attacks, but more likely adds an extra layer of caution to prevent unintentional harm. For instance, requiring two confirmations before deleting tables in a production database can help prevent someone from accidentally deleting real data when they think they are in a QA database.*

*Training is an essential control element to reduce the risk of human error and failure. Initial training is key, but ongoing training is critical to the mission of maintaining a secure digital environment. In this way, common errors and mistakes can be identified to new users as well as how to prevent them. By taking the time to reiterate the training reinforces proper policies and procedures.*

*Principle of least privilege is a concept that limits an employee’s privileges to only those accesses necessary to perform their job or role. This can prevent unauthorized employees from say, accidentally deleting or changing information in a database or from spilling their coffee onto a server rack.*

**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 pts.)

*A denial-of-service (DoS) attack is when a large number of connection or information requests are sent to a target, usually in TCP packets, from one or a block of IP addresses. So many requests are made to the one server, that it overloads and cannot respond to any legitimate requests either. This may cause a system to crash or fail to perform ordinary functions due to the overloading. Because the origin of the attack is easy to spot, it is easy for automated response systems to respond to a DoS attack.*

*A distributed denial-of-service (DDoS) attack is a coordinated stream of requests that are launched against a particular target from many locations at the same time. DDoS attacks use compromised systems called Bots or Zombies, which are attacked as part of a preparation phase and are then used remotely by the attacker. DDoS attacks are much more difficult to defend against because of the multitude of computers and networks being used to target and attack the system. For instance, Microsoft’s servers are constantly fielding these type of requests from global IP addresses, so it would be difficult, initially, to even detect a DDoS attack was under way and there would be no easy way to determine legitimate requests and attacks. Once the attack is identified, there is no feasible way to block all of the IP addresses responsible for the attack. Currently there are no controls any single organization can apply to protect themselves.*

**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 pts.)

*There were five password attacks described within Chapter 2. The first being cracking, this method simply involves reverse-engineering. The hacker makes an attempt to find a way around the password or to remove the access control in order to gain access to the software or objects which they were seeking. The second password attack is called brute force. In this technique a hacker uses computing power to simply guess the account's password using every letter and number combination possible. This can take either a few seconds to many many years depending on the complexity of one’s password.*

*The third is known as dictionary, where computing resources are again used to guess combinations that could represent the user’s password. In this attack, however, it guesses common dictionary terms and utilizes personal information about the targeted individual to better guess possible passwords until it is cracked. The fourth password attack is called rainbow tables. These tables contain hashed values that correlate to plaintext passwords. If a hacker is able to gain access to a file containing encrypted passwords that are presented in the hashed format, one can use the rainbow tables to then easily convert the encrypted password to usable text. The fifth attack involves social engineering. This can include the act of an individual impersonating an internal IT employee or using personal skills/liking to gain pertinent information allowing exposure of confidential details. If the attacker is able to successfully convince the user they are within the organization’s IT staff they may be able to obtain passwords which they can then use to give them greater access to the overall system.*

*One control that can be implemented is the 10.4 Password Rule, this rule is the current recommendation for password requirements stating that they should be at least 10 characters in length with at least 1 uppercase, lowercase, number, and special character. These requirements will ensure passwords take much longer to crack, providing enhanced security.*

*Another control that can be used is Training Protocols, these would be used in attempts to thwart social engineering attacks. The employees are always the weakest link in security, so if you train on what to look out for during a possible social engineering attack it could prevent them from providing confidential information to outsiders.*

*A final control that would help protect from password attacks is change control. This would be a policy implemented by IT personnel for all users on the system requiring passwords to be changed every so often (ex. 90 days) and not allowing a previous password to be used again. This would protect against an attacker who may have possibly cracked a user’s previous passwords and attempts to use them again to access the system.*