Rodrigo Brasil 11/2023

1. You have been made responsible for the company’s file server. How would you preserve the three elements of the CIA triad?
   1. I would implement strong access controls to ensure that only authorized personnel can access sensitive files. File integrity checks using hashing algorithms by regularly generating and comparing hash values for files to detect any unauthorized modifications and redundancy measures using RAID to the server storage.
2. Explain how hashing verifies data integrity using non-technical terms.
   1. Using the analogy of a letter, When I write a letter, I want to make sure it reaches the recipient exactly as I intended. I seal the envelope, and if someone tries to open it during transit then I would know that the letter has been tampered with. applying this analogy to data, having a piece of data, be it a file or something else, i want to ensure it hasn't been changed or corrupted. Instead of sealing an envelope, I would use something called a "hash function." This function takes the data and turns it into a unique, fixed-size string of characters like a "fingerprint." If the data changes, even by a tiny bit, the fingerprint changes completely. identifying that it has been tampered with.
3. How is hashing and encryption different?
   1. While hashing and encryption are both cryptographic techniques used to secure data, they serve different purposes and have distinct characteristics.
   2. The primary purpose of hashing is to generate a fixed-size string of characters (hash) from input data used to check if a piece of data has been tampered with and is irreversible.
   3. Encryption is a two-way process that transforms data into an unreadable format using an algorithm and a key. Its key purpose is to keep data confidential and also it is reversible.