COSC130 Fundamentals of Cybersecurity and Privacy

Tutorial Week 6

1. For each of the following ways to store passwords, comment on how secure they are and how efficiently then can be performed.
   a. Store passwords in plaintext
   b. Encrypt all passwords using the same key, and store the cyphertexts; store the encryption key in a separate database requiring higher privileges to access
   c. Encrypt each password using a unique key; for each password store the cyphertext, and the unique key used for that password
   d. Hash all the passwords, and store hash codes
   e. Append the same salt to each password, hash it and store the hash codes; store the salt in a different, more secure database
   f. Append a unique salt to each password and hash it; for each password, store the obtained hash, and the unique salt used
   g. For each password create a salt that is the same as the d=first two characters in the password; append salts to passwords and hash them; for each password, store the obtained hash
   h. Append a unique salt to each password and hash it; for each password, store the obtained hash, and a ciphertext of the unique salt used; all salts and encrypted with the same key, which is stored in a different secure database

2. Rank the following passwords by their strength; justify your ranking.
   a. Bnjd^57j&*
   b. apple1
   c. Dfgnua
   d. 000000
   e. G56&hk
   f. Apples

3. Whose responsibility is to protect against cybercrime? Select the best answer.
   a. Federal police
   b. Local police
   c. Cybersecurity professionals
   d. Everybody
   e. Government

4. Which one of the following can be used as an attack on passwords?
   a. Looking over someone shoulder while they are withdrawing money from an ATM
   b. Dictionary attack
   c. Brute Force attack
   d. All of the above
   e. None of the above

5. Research password managers available in 2024. Identify features that are commonly supported. Create a table to compare at least 5 password managers in respect to price and identified features.