CYBER SECURITY INTERNSHIP

Task 4: Password Security & Authentication Analysis

1. Hashing vs Encryption in Password Storage

Hashing is a one-way process used to store passwords securely. The original password cannot be obtained from the hash value. The same password always produces the same hash. Hashing becomes more secure when salt and slow algorithms are used.

Encryption is a two-way process where data can be converted back to its original form using a key. It is mainly used to protect data during storage or transmission. Encryption should not be used for storing passwords.

Passwords should always be stored using hashing, not encryption.

2. Types of Hashing Algorithms

MD5 produces a 32-character hash and is considered insecure due to collisions.
SHA-1 generates a 40-character hash and is also broken.
SHA-256 is stronger than MD5 and SHA-1 but is still fast and needs salting.
bcrypt is a secure password hashing algorithm because it is slow and includes salt.

3. Password Hash Generation

Password hashing converts a plain-text password into a fixed-length hash value.
Hash generation can be done using operating system commands or programming languages.
The original password is never stored in the database.

4. Cracking Weak Hashes Using Wordlists

A dictionary attack uses a list of common passwords to crack hashes.
Each word from the list is hashed and compared with the target hash.
This attack is successful when weak passwords and fast hashing algorithms are used.

5. Brute Force vs Dictionary Attacks

Brute force attack tries all possible combinations of characters and is slow but effective.

Dictionary attack uses predefined password lists and is faster but limited to known words.

6. Reasons Why Weak Passwords Fail

Weak passwords are short, predictable, and commonly used.

Passwords without symbols or reused across multiple websites are easily cracked.

Attackers take advantage of leaked password databases and automation tools.

7. Multi-Factor Authentication (MFA)

Multi-Factor Authentication requires more than one method of verification.

It combines something the user knows, has, or is.

Even if a password is compromised, MFA prevents unauthorized access.

8. Recommendations for Strong Authentication

Strong passwords should be long and complex.

Each account should have a unique password.

Password managers should be used to store credentials securely.

Multi-Factor Authentication should be enabled wherever possible.

Secure hashing algorithms like bcrypt should be used for password storage.