Task 4: Password Security & Authentication Analysis

1. How Passwords Are Stored (Hashing vs Encryption)

Passwords are never stored in plain text in secure systems. Instead, they are stored using hashing. Hashing is a one-way process that converts a password into a fixed-length value. Encryption is a two-way process and is not used for password storage because encrypted data can be decrypted.

2. Types of Hashing Algorithms

Common hashing algorithms include MD5, SHA-1, and bcrypt. MD5 and SHA-1 are outdated and insecure. bcrypt is a secure hashing algorithm because it uses salting and is slow, making brute-force attacks difficult.

3. Generating Password Hashes

Sample passwords such as 'password123' or 'admin@123' can be converted into hash values using online hash generators. This step helps in understanding how plain-text passwords are transformed into hashes. Only dummy passwords are used for learning purposes.

4. Understanding Weak Password Cracking

Attackers attempt to crack weak passwords using wordlists that contain commonly used passwords. Tools such as Hashcat and John the Ripper are used by attackers to automate this process. Weak passwords are cracked quickly because they already exist in leaked password databases.

5. Brute Force vs Dictionary Attacks

A dictionary attack uses a list of common passwords and is very fast. A brute-force attack tries all possible combinations of characters and takes more time. Strong and long passwords can resist both attack methods.

6. Why Weak Passwords Fail

Weak passwords fail because they are short, predictable, reused across multiple platforms, and often found in leaked databases. Attackers take advantage of common human behavior rather than guessing randomly.

7. Multi-Factor Authentication (MFA)

Multi-Factor Authentication adds an additional layer of security by requiring more than one verification method. This may include a password and a one-time password (OTP) or biometric verification. MFA prevents preventing unauthorized access even if a password is compromised.

8. Recommendations for Strong Authentication

Strong authentication practices include using long passwords (12–16 characters), unique passwords for each platform, enabling MFA, avoiding common patterns, and using password managers.

Conclusion

This task helped in understanding how password security works, common attack methods, and best practices to protect user accounts. Strong passwords combined with MFA provide effective defense against cyber threats.