Task-6

What makes a password strong?
→ A strong password is long (at least 12 characters) and includes uppercase, lowercase, numbers, and symbols. It avoids common words and personal details.

What are common password attacks?
→ Common attacks include brute force, dictionary, phishing, and credential stuffing attacks.

Why is password length important?
→ Each additional character exponentially increases the time and effort required to crack a password.

What is a dictionary attack?
→ A method where attackers use precompiled lists of common words or passwords to guess user credentials.

What is multi-factor authentication (MFA)?
→ MFA adds an extra layer of security by requiring two or more verification factors (e.g., password + OTP).

How do password managers help?
→ Password managers securely store passwords and generate complex ones, reducing the risk of reuse or weak passwords.

What are passphrases?
→ Passphrases are long combinations of random words (e.g., “BlueCarpetSkyTrain”) that are easier to remember yet highly secure.

What are common mistakes in password creation?
→ Using personal info, short passwords, common words, reusing passwords, or avoiding special characters.

1. **Observations and Best Practices Identified:**

→ Passwords with **mixed case letters, numbers, and special characters** are harder to crack.
Longer passwords (12+ characters) significantly increase security.
Avoid using **personal information** or common words.
Unique passwords should be used for every account.
Use a **password manager** to safely store and generate passwords.
Passphrases (random words strung together) are both secure and memorable.