Task 6 - Interview Questions

1. What makes a password strong?

A strong password is **hard to guess or brute-force**. It usually:

- Has **at least 12–16 characters**.
- Includes a mix of **uppercase, lowercase, numbers, and special symbols**.
- Avoids using **dictionary words**, names, or predictable patterns.
- It is **unique** — not reused across multiple accounts.
  Strong passwords increase the time and computational effort required for attackers to crack them.

---

2. What are common password attacks?

Common password attacks include:

- **Brute-force attack:** Trying every possible combination of characters until the correct password is found.
- **Dictionary attack:** Using lists of common passwords or words from dictionaries to guess the password.
- **Phishing:** Tricking users into revealing their passwords through fake websites or emails.
- **Credential stuffing:** Using leaked username-password pairs from other breaches to access multiple accounts.
- **Keylogging:** Recording keystrokes to capture passwords entered by the user.

---

3. Why is password length important?

Password length significantly increases the **number of possible combinations** an attacker must try.
For example, every additional character exponentially increases complexity — making brute-force attacks much slower.
Longer passwords (or passphrases) are generally **more secure,** even if they use simpler characters, because they're much harder to crack by computational means.

---

4. What is a dictionary attack?

A dictionary attack is when an attacker uses a **precompiled list of likely passwords or words** (like "password," "123456," or "qwerty") to attempt logins.
It's faster than brute-force because it targets **commonly used or predictable passwords** instead of testing all possible combinations.
Defenses include enforcing strong password policies, account lockout mechanisms, and using salted password hashing.

---

5. What is multi-factor authentication (MFA)?

Multi-Factor Authentication (MFA) adds an **extra layer of security** by requiring users to provide **two or more verification factors** to log in.
These factors can be:

- **Something you know** (password or PIN)
- **Something you have** (smartphone, hardware token)
- **Something you are** (fingerprint, face scan)
  Even if a password is compromised, MFA helps prevent unauthorized access.

---

6. How do password managers help?

Password managers securely **store and encrypt all your passwords** in one place, requiring only a single master password to access them.
They help by:

- Generate **strong, unique passwords** for each account.
- Reducing **password reuse** and human error.
- Auto-filling login details safely, preventing phishing by verifying the domain.
  This improves both **security and convenience** for users.

---

7. What are passphrases?

A passphrase is a **longer, easy-to-remember sequence of random words** instead of a single complex password.
Example: “**PurpleSunset!RunsFast@River**”
Passphrases are secure because their **length and randomness** make them resistant to brute-force and dictionary attacks, while being **easier for humans to remember** than random character strings.

---

8. What are common mistakes in password creation?

Common mistakes include:

- Using **short or simple passwords** like “123456” or “password”.
- Reusing the **same password across multiple accounts**.
- Including **personal information** (name, birthdate, pet’s name).
  Ignoring **password change reminders** after breaches.
- Writing passwords down or storing them in **unsecured notes**.
  Avoiding these mistakes greatly improves overall account security.