Interview Questions & Answers

1. What makes a password strong?

A strong password is designed to withstand modern password-cracking techniques by being long, unpredictable, and unique for each account. It uses a variety of character types to make guessing more difficult, while avoiding personal or easily guessed details. Such passwords reduce the risk of compromise through brute force, dictionary attacks, or credential stuffing.

- Minimum of 12–16 characters.
- Mix of uppercase, lowercase, numbers, and special symbols.
- Avoids dictionary words and personal information.
- Unique for every account you use.

2. What are common password attacks?

Password attacks are techniques used by hackers to gain access to accounts. Some rely on computing power to guess the password, while others exploit human mistakes or stolen data. Understanding these attacks helps in designing better defenses.

- Brute force – tries every possible combination.
- Dictionary – uses common words or leaked passwords.
- Credential stuffing – tests stolen credentials on other sites.
- Phishing – tricks users into revealing passwords.
- Keylogging – records keystrokes to capture login details.

3. Why is password length important?

Length is a key factor in password security because each extra character exponentially increases the number of possible combinations. A long password, especially when combined with complexity, is much more resistant to brute force attacks and automated cracking tools.

- Short passwords are guessed quickly.
- Long passwords take exponentially longer to crack.
- 6 lowercase letters → seconds to crack.
- 12 mixed characters → centuries to crack.

4. What is a dictionary attack?

A dictionary attack is a targeted guessing method where attackers test likely passwords instead of all possible combinations. This approach is faster than brute force because it focuses on predictable human choices, especially common or weak passwords.

- Faster than brute force.
- Targets common and predictable passwords.
- Avoidable by using random characters instead of full words.

5. What is multi-factor authentication (MFA)?
MFA adds an extra layer of protection by requiring more than one type of authentication before granting access. Even if a password is stolen, MFA ensures the attacker still cannot log in without the second factor.

- Something you know – password/PIN.
- Something you have – OTP, phone, or security key.
- Something you are – fingerprint or face scan.

6. How do password managers help?
Password managers provide a secure way to store and manage all your login credentials. They not only save time but also help you maintain strong, unique passwords for every account without having to memorize them.

- Store passwords in an encrypted vault.
- Generate strong, unique passwords automatically.
- Reduce password reuse and human errors.

7. What are passphrases?
Passphrases are longer forms of passwords made up of multiple random words. They are easier to remember than complex random strings, yet still provide excellent security due to their length and unpredictability.

- Memorable but hard to guess.
- Secure due to length and randomness.
- Example: `BlueElephant#SingsAtNight42`.

8. What are common mistakes in password creation?
Weak password habits make it easy for attackers to compromise accounts. These mistakes often result from convenience or lack of awareness about security risks.

- Choosing short or simple passwords.
- Reusing the same password across accounts.
- Using personal details like names or birth dates.

- Following predictable patterns (e.g., `Password@2025`).