Report: Password Strength Analyzer Tool

1. Introduction:

The Password Strength Analyzer tool evaluates the strength of a user's password based on common security standards. The tool uses a graphical interface built with Python's tkinter, applies pattern matching using regular expressions (re), and hashes the password using the SHA-256 encryption algorithm from the hashlib library. The effectiveness of the tool lies in its ability to evaluate a password's compliance with key security criteria.

2. Password Strength Algorithm:

The strength of a password is evaluated using five security criteria:

1. Length (>= 8 characters): Passwords less than 8 characters are considered weak.
2. Uppercase Letter: The presence of at least one uppercase letter enhances security.
3. Lowercase Letter: The presence of at least one lowercase letter adds complexity.
4. Digit: Having at least one number improves strength.
5. Special Character: Using symbols (e.g., @, #, !) makes the password harder to guess.

Password Scoring:

- The algorithm assigns 1 point for every criterion the password meets.
- The total strength score ranges from 0 to 5, with 5 being the strongest.

Effectiveness:

- This method is effective for basic password security checks, ensuring that users create passwords that are hard to guess or crack. Each criterion contributes to making the password more resistant to common attacks, such as brute-force and dictionary attacks.

3. Hashing Algorithm (SHA-256):

To enhance security, the tool hashes the entered password using the SHA-256 algorithm. Hashing ensures that even if passwords are stored or transmitted, they are not stored in plain text, making them harder to retrieve in case of a data breach.

How Hashing Works:

- SHA-256 converts the password into a unique fixed-size string (64 characters long), making it almost impossible to reverse-engineer the original password.
- Each unique password produces a different hash.

Effectiveness:

- SHA-256 is highly secure and widely used in the industry. It is resistant to pre-image and collision attacks, meaning attackers cannot easily generate the original password from the hash or create two different passwords with the same hash.

4. Conclusion:

The Password Strength Analyzer tool is a basic yet effective solution for improving password security. By guiding users to create strong, complex passwords and securing them with SHA-256 hashing, it protects against common attack vectors. The tool is simple to use, making it suitable for beginner users, and provides clear, actionable feedback on password quality.