Task 6 Report: Password Strength Evaluation

Name: Keerthivasan E

Role: Intern at Elevate Labs

File Name: task6\_sol.docx

Objective:

To understand the factors that contribute to password strength by generating and evaluating passwords using online password strength tools.

# Tools Used:

- PasswordMeter.com – for evaluating password strength and receiving feedback.

# 1. Password Generation:

|  |  |
| --- | --- |
| Password | Description |
| apple123 | Lowercase + numbers, simple word |
| Apple123 | Capitalized + numbers |
| ApPlE@123 | Mixed case + symbols + numbers |
| @Pp!e\_2025 | Strong symbol + mixed + future year |
| Keerthi@E1 | Custom name pattern + symbol + number |
| K!9fG%r2X# | Randomized characters with symbols |
| 12345678 | Common number-only password |
| Keerthi123 | Phrase with symbol + numbers |

# 2. Password Strength Check:

|  |  |  |
| --- | --- | --- |
| Password | Strength Score | Feedback Summary |
| apple123 | 34% | Too common, lacks complexity |
| Apple123 | 45% | Slight improvement due to capitalization |
| ApPlE@123 | 71% | Good mix of elements |
| @Pp!e\_2025 | 84% | Strong – good symbol and structure |
| Keerthi@E1 | 76% | Strong but pattern-based |
| K!9fG%r2X# | 95% | Very strong – randomized elements |
| 12345678 | 5% | Extremely weak – commonly used |
| LetMe!n123 | 66% | Medium strength – dictionary word pattern |

# 3. Tips Learned:

- Avoid using personal information or common sequences (e.g., 123456).

- Passwords with 8+ characters, mixed case, symbols, and numbers score higher.

- Using randomized combinations is much better than readable words.

- Symbols and non-dictionary words significantly boost strength.

# 4. Research: Common Password Attacks

• Brute Force Attack: Tries all possible combinations until the password is found. Longer and complex passwords slow this down.

• Dictionary Attack: Uses common words or phrases from dictionaries. Avoiding real words helps prevent this.

# 5. Summary: Password Complexity vs. Security

Stronger passwords are those that combine length with character variety. They are more resistant to automated tools and dictionary attacks. Using a password manager can help maintain strong and unique passwords without the need to memorize each one.

# Conclusion:

Creating strong passwords requires avoiding predictability and embracing randomness, length, and character diversity. Tools like PasswordMeter can guide users toward building better security habits.