Task 6: Create a Strong Password and Evaluate Its Strength

# Objective:

Understand what makes a password strong and test multiple examples using an online password strength checker.

# Tools Used:

• Website: https://www.passwordmeter.com

# Password Testing

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Password | Components | Length | Score (%) | Feedback |
| Password974 | lowercase + numbers | 11 | 26% | Very weak, predictable |
| P@ssw0rdd | upper + lower + number + symbol | 8 | 60% | Better, but still common |
| Srishti@0987 | upper + lower + number + symbol | 13 | 81% | Strong, less predictable |
| !0am#uP5^wQa%zL0 | all character types + long | 16 | 100% | Excellent, very strong |

# Observations:

• Simple passwords like 'password123' are extremely weak.

• Adding symbols, uppercase letters, and increasing length boosts the score.

• Random characters with high length gave the best results.

• Even some complex passwords like 'P@ssw0rd' are common and easily guessable.

# Tips for Creating Strong Passwords:

• Use 12–16+ characters.

• Mix uppercase, lowercase, numbers, and symbols.

• Avoid using names, dictionary words, or keyboard patterns.

• Use unpredictable phrases like: Mango$Dance99!

• Don't reuse passwords on multiple websites.

• Use a password manager for remembering complex ones.

# Common Password Attacks:

|  |  |
| --- | --- |
| Attack Type | Description |
| Brute Force | Tries every possible combination until it finds the correct password. |
| Dictionary Attack | Uses a list of common words and passwords to guess quickly. |
| Credential Stuffing | Uses leaked passwords from other sites to try logging into your account. |

# Why Password Complexity Matters:

• Longer & complex passwords increase the total number of possible combinations.

• This makes brute-force attacks almost impossible within a realistic timeframe.

• Symbols and randomness make passwords unpredictable, defeating pattern-based guessing.

• Overall, complexity = more time and effort to crack = better protection.

# Conclusion:

Through this task, I understood how different elements of a password impact its strength. Online tools like PasswordMeter help evaluate our choices. Strong passwords are long, complex, and unpredictable — and are the first line of defense against many cyberattacks.