Task 6: Password Strength Analysis Report

# Objective:

Understand what makes a password strong and test it against password strength tools.

# Tools Used:

Password strength checker: https://passwordmeter.com

# Password Strength Results:

|  |  |  |
| --- | --- | --- |
| Password | Score (%) | Feedback |
| hello123 | 40% | Needs uppercase & symbols |
| Hello@123 | 85% | Strong password |
| H3ll0!Th1s!$Str0ng | 100% | Very strong |
| Pass | 13% | Too short and simple |

# Best Practices for Creating Strong Passwords:

- Use at least 12 characters.

- Combine uppercase, lowercase, numbers, and symbols.

- Avoid dictionary words or personal information.

- Use passphrases (e.g., MyCat$Eats2Much!).

# Common Password Attacks:

- Brute Force: Tries every possible combination.

- Dictionary Attack: Tries common passwords/words.

- Credential Stuffing: Uses leaked credentials.

# Summary:

I created multiple passwords with different strengths and evaluated them using passwordmeter.com. I learned that password strength improves with longer lengths, use of symbols, and character variety. Weak passwords like 'hello123' are easy to guess, while complex ones like 'H3ll0!Th1s!$Str0ng' are secure. This task increased my awareness of strong password creation and common attack types.

# Screenshot:

Pass : Very weak

H3ll0!Th1s!$Str0ng : Very strong

