📝 Task 6 Report: Create a Strong Password and Evaluate Its Strength

1. **Introduction**

In this task, the objective was to understand what makes a password strong and evaluate different passwords using online password strength checkers. The purpose of this exercise is to recognize the best practices in password creation and improve security awareness against common attack methods like brute-force and dictionary attacks.

2. **Passwords Tested**

|  |  |  |
| --- | --- | --- |
| Password | Score | Feedback from Tool |
| TheAvengers@2012 | 85% | Strong password. Good use of uppercase, lowercase, number, and symbol. |
| Dubai2025@dfc | 80% | Medium-strong. Could improve by adding more symbols or increasing length. |
| KarthiyaniAmma@123 | 88% | Strong. Contains a long phrase, uppercase, lowercase, symbol, and numbers. |
| BarrywedsIris2017!@# | 92% | Very strong. Long and includes multiple character types. Good complexity. |
| Hog123Rider!@# | 90% | Strong. Uses uppercase, lowercase, numbers, and multiple special characters. |

3. **Analysis**

* Password length greatly improves strength (longer = harder to crack).
* Combining character types (uppercase, lowercase, numbers, and symbols) increases entropy.
* Avoiding dictionary words or combining them with complex characters is helpful.
* Passwords that mimic personal information (e.g., names or years) can still be guessed if not complex enough.

4. **Best Practices for Creating Strong Passwords**

* Use at least 12–16 characters.
* Include uppercase, lowercase, numbers, and special characters.
* Avoid using real names, birthdates, or common phrases.
* Use random combinations or passphrases.
* Don’t reuse passwords across multiple sites.
* Use a password manager to generate and store strong passwords.
* Regularly update passwords, especially for critical accounts.

5. **Tips Learned from Evaluation**

* Adding multiple symbols (like !@#) drastically increases the score.
* Length combined with complexity (e.g., "BarrywedsIris2017!@#") offers the highest strength.
* Simple passwords, even with numbers (e.g., Dubai2025@dfc), can still be medium-strong but may not withstand targeted attacks.

6. **Common Password Attacks**

1. **Brute-force attack**: Tries all possible combinations. Long, complex passwords take exponentially more time to crack.
2. **Dictionary attack**: Uses a list of common words and variations. Avoid using common phrases, names, or dictionary words.

7. **Conclusion: Password Complexity vs Security**

Password complexity is directly linked to security. A complex password—long and filled with different character types—is significantly harder for attackers to crack. Strong passwords protect personal data, prevent unauthorized access, and are critical in defending against both brute-force and dictionary attacks.