Task 6 - Password Strength Evaluation Report

The purpose of this exercise is to understand the characteristics of strong passwords, evaluate various passwords using an online password strength checker, and summarize best practices for password creation and security.

Methodology

- Multiple passwords were created with varying complexity, length, and character types.
- Each password was tested using passwordmeter.com, a recognized online password strength evaluation tool.
- The scores and feedback were recorded.
- Best practices and common password attack methods were researched and summarized.

3. Passwords Tested and Results

Password	Length	Complexity Used	Score (%)	Feedback from Tool
password	8	Lowercase only	10	Very weak; common word; lacks complexity
Password1	9	Upper, lower, number	35	Needs symbols; longer length recommended
Passw0rd!	9	Upper, lower, number, !	70	Good, but could be longer
1qaz@WSX	8	Upper, lower, number, @	80	Strong, but could be longer
S!mpl3x@mpl3Pwd	14	Upper, lower, number, !@	95	Very strong; good use of length and complexity
9&uY#z3!Qw@Lp$4	13	All character types	100	Excellent; very strong and complex

Best Practices for Creating Strong Passwords

Based on the evaluation and tool feedback, the following best practices are recommended:

- **Length:** Use at least 12–16 characters.
- **Complexity:** Combine uppercase letters, lowercase letters, numbers, and special symbols.
- **Unpredictability:** Avoid dictionary words, names, or easily guessable patterns.
- **Uniqueness:** Use a unique password for each account or service.
- **Passphrases:** Consider using a passphrase (a sequence of unrelated words with added complexity).
- **Password Managers:** Utilize a reputable password manager to generate and store strong passwords.

5. Common Password Attacks

- **Brute Force Attack:** Attempts every possible combination. Longer and more complex passwords are exponentially harder to crack.
- **Dictionary Attack:** Uses lists of common words and phrases. Passwords based on dictionary words are vulnerable.
- **Credential Stuffing:** Uses previously leaked username/password pairs to gain access to other accounts.

6. Impact of Password Complexity on Security

Password complexity and length significantly increase the difficulty of successful brute force or dictionary attacks. Each additional character and character type increases the number of possible combinations, making the password more secure. Unique and complex passwords help prevent unauthorized access, even in the event of a data breach.

The evaluation demonstrates that password strength is directly related to length, complexity, and unpredictability. Adhering to best practices and using password management tools greatly enhances security and reduces the risk of compromise.