
Task 6: Create a Strong Password and Evaluate Its Strength

Objective

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

Tools Used

- PasswordMeter :- https://passwordmeter.com/

- Any other free password strength checker

Steps Performed

1. Created multiple passwords with varying complexity (simple, medium, strong).

2. Included variations:

  - Uppercase & lowercase letters

  - Numbers

  - Special characters

  - Different lengths

3. Tested each password using PasswordMeter.

4. Recorded strength scores and tool feedback.

5. Identified best practices for creating strong passwords.

6. Documented tips and insights from the evaluation.

7. Researched common password attacks:

  - Brute force

  - Dictionary attacks

8. Summarized how password complexity affects security.

Findings

- Short or simple passwords are easily guessable.

- Mixing uppercase, lowercase, numbers, and symbols significantly improves strength.

- Longer passwords (12+ characters) are **more resistant** to brute-force attacks.

- Avoid dictionary words or predictable patterns.

Best Practices

- Use at least 12 characters.

- Combine uppercase, lowercase, numbers, and special characters.

- Avoid personal information and dictionary words.

- Use passphrases for better memorability.

Outcome

Gained practical knowledge on:

- Password strength evaluation

- Importance of complexity and length

- Defense against brute force & dictionary attacks