📝 Summary – Task 6: Password Strength Evaluation

In this task, I explored how to create strong, secure passwords and evaluated their effectiveness using an online password strength checker (https://passwordmeter.com). I created multiple passwords with different levels of complexity — including combinations of uppercase letters, lowercase letters, numbers, symbols, and varying lengths.

Each password was tested on the tool, and the results (strength score and feedback) were recorded. I observed how password strength improves with better character variety and length.

Additionally, I studied common password attacks such as brute force and dictionary attacks. I learned why longer, more complex passwords are significantly harder to crack, and how tools like password managers and multi-factor authentication improve overall security.

This task helped me understand real-world password vulnerabilities and best practices for strong password creation.

☑️ Key Learnings:

- ✔ Use long passwords (12+ characters).
- ✔ Mix uppercase, lowercase, numbers, and special symbols.
- ✔ Avoid personal info (name, DOB, etc.).
- ✔ Use password managers.
- ✔ Enable multi-factor authentication.