Task 6 – Password Strength Evaluation Report

1. Objective

To understand the importance of password complexity and test various passwords using online password strength checkers.

2. Tools Used

- PasswordMeter.com
- Security.org Password Checker

3. Method

1. Created multiple passwords with different complexities.
2. Tested each one using online password strength tools.
3. Recorded scores, cracking times, and feedback.
4. Compared and analyzed the results.

4. Results Table

Password	Strength	Time to Crack	Feedback
kabilesh123	Weak	2 seconds	Add uppercase and symbols
Kabilesh@2025	Medium	4 hours	Increase length
K@b!2025learn#	Strong	5 years	Good complexity
Sunrise$at!Beach2025	Very Strong	40+ years	Very secure

5. Observations

- Passwords with symbols and mixed cases are significantly stronger.
- Length plays a major role in password security.
- Passphrases offer a good balance between memorability and strength.

6. Common Attacks

- **Brute Force Attack:** tries all possible combinations.
- **Dictionary Attack:** uses common words and passwords.
- **Phishing:** tricking users into revealing passwords.

7. Best Practices

- Use at least 12–16 characters.
- Combine letters, numbers, and symbols.
- Avoid reusing passwords.
- Use MFA (Multi-Factor Authentication) for extra protection.
- Store passwords securely with password managers.

8. Conclusion

This activity demonstrated that password strength increases with length and complexity. Using online tools provided insights into how attackers exploit weak passwords and how users can protect themselves.

9. Screenshot

Attach the screenshot named **password_results.png** showing your password strength test results from PasswordMeter.com or Security.org.