Task 6: Password Strength Evaluation Report

Objective: Understand what makes a password strong and evaluate it using online tools.

Password	Score (%)	Time to Crack	Feedback
password123	20%	Less than 1 second	Too short, dictionary word used
Myp@ssword	55%	Few hours	Add more symbols & length
T!m3T0W!n#2025	90%	Centuries	Strong mix of characters
G^r8z&J7@!lQpW4mR2	100%	Millions of years	Excellent — long, random, varied chars

Best Practices for Strong Passwords:

1. Use at least 12–16 characters.
2. Mix uppercase, lowercase, numbers, and special characters.
3. Avoid dictionary words and personal information.
4. Use passphrases for better memorability.
5. Change passwords regularly.

Common Password Attacks:

- Brute Force: Tries all possible combinations until the correct one is found.
- Dictionary Attack: Uses a list of common words and passwords to guess quickly.
- Credential Stuffing: Uses leaked username-password pairs from previous breaches.

Conclusion: Longer passwords with high complexity greatly improve security against brute force and dictionary attacks. Using passphrases and password managers is highly recommended.