Task 6 Report – Password Security

1. Objective

To create strong passwords, evaluate their strength using online tools, and understand best practices for secure authentication.

2. Methodology

- Created multiple passwords with varying complexity.
- Tested them using **PasswordMeter** and **Kaspersky Password Checker**.
- Compared scores and feedback.
- Researched password attacks and prevention.

3. Results

Password Example	Tool Used	Strength	Estimated Crack Time
password123	PasswordMeter	Very Weak	Seconds
Password2025	Kaspersky	Weak	Hours
P@ssw0rd!2025	PasswordMeter	Strong	Years
Gr33n_Tree$2025!SecureLife	Kaspersky	Very Strong	Centuries+

*(*Attach screenshots of test results in your repo under /screenshots*)*

4. Best Practices for Strong Passwords

1. Use 12+ characters.
2. Mix letters, numbers, and special symbols.
3. Avoid personal info & dictionary words.
4. Use passphrases (easy to remember, hard to guess).
5. Enable multi-factor authentication (MFA).
6. Use a password manager for complex/unique passwords.

5. Common Password Attacks

- **Brute Force Attack**: Tests all combinations.
- **Dictionary Attack**: Uses pre-compiled lists of common words.
- **Credential Stuffing**: Uses leaked credentials across websites.

6. Conclusion

This task demonstrated how password complexity and length affect security. Testing across tools proved that simple passwords are easily cracked, while longer, complex passphrases offer strong protection. Combined with MFA and password managers, this ensures robust authentication practices.