Password Strength Evaluation Report

Prepared by Jefrin Correya

1. Objective

The objective of this task is to understand what makes a password strong, analyze password strength using free online tools, and gain awareness of password security best practices and common attack methods.

2. Methodology

1. Created multiple passwords with different levels of complexity.
2. Tested each password using an online password checker (passwordmeter.com).
3. Recorded feedback and scores.
4. Compared results and identified key password strength factors.
5. Additionally, tested them using my own HTML-based password strength checker website developed by me.

3. Password Strength Evaluation Results

The following table summarizes the password strength evaluation results:

Password	Strength Score	Feedback
jefrin123	25	Weak - too short, lacks symbols & uppercase
Jefrin@123	50	Medium - better mix, but short
J3fr!n_C0rr3ya	75	Strong - good complexity
J3fr!nC0rr3ya2025#	90	Very Strong - complex and long
Cyber$ecure_P@ssword2025	100	Excellent - strong, long, and unique

4. My Own Password Strength Checker

In addition to using online tools, I created my own password strength checker website using HTML. The tool analyzes password complexity by checking for factors like length, uppercase, lowercase, numbers, and symbols. This gave me practical understanding of how password strength evaluation algorithms work.

The password strength checker website is designed to provide real-time feedback on password quality, helping users create more secure passwords. It evaluates various criteria including minimum length requirements, character diversity, and common password patterns.

Demo Website: https://password-strength-checker-alpha.vercel.app

5. Common Password Attacks

- Brute Force Attack: Tries every possible combination until it finds the password.
- Dictionary Attack: Uses a precompiled list of common passwords or words.
- Phishing Attack: Tricks users into revealing passwords through fake websites or emails.
- Credential Stuffing: Reuses stolen passwords across multiple accounts.

6. Best Practices for Strong Passwords

- Use at least 12-16 characters.
- Include uppercase, lowercase, numbers, and symbols.
- Avoid personal information or dictionary words.
- Use unique passwords for each account.
- Enable multi-factor authentication (MFA) for additional security.
- Consider using a trusted password manager.

7. Conclusion

This task helped in understanding password complexity, evaluating strength using tools, and developing a hands-on understanding by creating a personal password strength checker. Strong passwords play a crucial role in defending against brute force and dictionary attacks. By following best practices and using tools to evaluate password strength, users can significantly improve their online security posture and protect their digital assets from unauthorized access.