Task 6 Report: Password Strength Evaluation

1. Objective and Evaluation Methodology

The objective of this task was to understand the characteristics of a strong password and evaluate its strength using a simulated testing process, based on the principles used by online password strength checkers.

2. Password Creation and Strength Evaluation

Password Category	Example Password	Length	Complexity Factors Used	Strength Score / Feedback
Very Weak	password123	11	Lowercase, Numbers	Very Weak
Weak	soccergame	10	Lowercase	Weak (Dictionary word)
Moderate	MyDogBuster21	13	Upper, Lower, Numbers	Fair (Common phrase)
Strong	W3@kL1nk!sN0m0r3	17	Upper, Lower, Numbers, Symbols	Strong (High entropy)

Analysis showed that password length and character diversity significantly improved password strength, while dictionary words and predictable patterns made them weak.

3. Best Practices for Creating Strong Passwords

- Use at least 12-16 characters; longer is better.
- Include uppercase, lowercase, numbers, and symbols.
- Use passphrases with random, unrelated words.
- Avoid personal information, patterns, or sequential numbers.

4. Common Password Attacks

Brute-Force Attack: Attempts every combination. Defense: Longer passwords.
Dictionary Attack: Uses common word lists. Defense: Avoid dictionary words and predictable substitutions.

5. Summary: Password Complexity and Security

Password complexity directly increases security by expanding the keyspace and entropy, making brute-force and dictionary attacks impractical.

6. Outcome

Password security depends most on length and diversity. Unique, long passphrases with mixed characters are recommended to resist attacks.