Task 6 — Password Evaluation Report

This report reflects on the process of testing different types of passwords and analysing their strengths. Through this exercise, I learned how password structure impacts security, and I noted down key practices to follow in daily use.

Best Practices for Strong Passwords:
1. Use at least 12–16 characters in every password.
2. Mix uppercase, lowercase, numbers, and special characters.
3. Prefer long passphrases made from random words for memorability.
4. Avoid dictionary words, birthdays, or predictable patterns.
5. Do not reuse passwords across different accounts.
6. Store complex passwords in a trusted password manager.
7. Always enable multi-factor authentication where possible.

Tips Learned from Evaluation:
- Even small improvements (adding digits, changing case) increase strength, but *length matters the most*.
- A passphrase with simple words can be stronger than a short complex password.
- Randomly generated high-entropy passwords provide maximum security but require a manager to store safely.

Common Password Attacks:
- **Brute Force:** Every possible combination is tried. Longer passwords make this almost impossible.
- **Dictionary Attack:** Uses lists of common words and leaked passwords. Simple words or names are easily cracked.
- **Hybrid Attacks:** Mix of dictionary + slight variations (e.g., replacing 'a' with '@').

Impact of Password Complexity:
Password security grows exponentially with length and variety of characters. For example, an 8-character password may be broken in hours or days with modern hardware, while a 12–16 character password with mixed types may take millions of years to guess by brute force. This shows why complexity and length together are essential for security.

— End of Report —