Create a Strong Password and Evaluate Its Strength

Objective

The goal of this task is to understand how password complexity affects security by creating, testing, and analyzing multiple passwords of varying strength.

Guidelines for Creating a Strong Password

1. Length and Complexity

- Use at least 12–16 characters.
- Include a mix of uppercase letters, lowercase letters, numbers, and special symbols (e.g., @, #, $).

2. Avoid Common Pitfalls

- Do not use personal information such as names, birthdays, or phone numbers.
- Avoid dictionary words, common patterns, or easy sequences like 12345 or qwerty.

3. Techniques for Strong Passwords

- Use passphrases made of random, unrelated words (e.g., BlueSky!Pizza#42).
- Consider using randomly generated strings for stronger protection.

4. Unique Passwords for Each Account

- Use a different password for every account.
- This prevents one compromised password from affecting other accounts.

5. Use a Password Manager

A password manager can create, store, and manage all your passwords securely.

6. Enable Multi-Factor Authentication (MFA)

Always turn on MFA or 2FA for an extra layer of security beyond the password.

🧰 Tools & Resources Used

- Bitwarden Password Strength Checker – https://bitwarden.com/password-strength/
- Kali linux terminal – for performing local analysis

Screenshots of the passwords tested