**Password Strength Evaluation Report**

**Task:** Task 6 – Create a Strong Password and Evaluate Its Strength  
**Submitted By:** Aryanshu Saha  
**Date:** 1/07/2025  
**Department/Project:** [Optional – Security Awareness / Internal Audit / Internship Task]

1. **Objective**

To demonstrate understanding of secure password creation techniques by designing multiple passwords with varying complexities and evaluating their strength using online password testing tools. The task also includes a review of password security best practices and common attack vectors.

1. **Tools & Resources Used**
2. [PasswordMeter.com](https://passwordmeter.com) – Complexity scoring & analysis
3. NordPass Password Strength Checker
4. Bitwarden Password Strength Tester
5. Kali Linux 2025.2 (used for research and reference)

**Methodology: Step-by-Step Execution**

**Step 1: Created Password Samples**

* Designed 4 passwords of increasing complexity.
* Incorporated different character types (uppercase, lowercase, numbers, symbols) and varied the length.

**Step 2: Tested Each Password**

* Used all three password strength evaluation tools.
* Recorded scores, feedback, and estimated crack times.

**Step 3: Analyzed Results**

* Compared strength ratings across tools.
* Summarized tool recommendations and scoring factors.

**Step 4: Documented Best Practices**

* Reviewed suggestions provided by each tool.
* Cross-referenced with cybersecurity guidelines (e.g., NIST, OWASP).

**Step 5: Researched Password Attacks**

* Studied brute-force, dictionary, and credential stuffing attacks.
* Evaluated how complexity impacts resistance to these attacks.

**Password Testing Results**

| **Password** | **Complexity** | **Length** | **Tools Used** | **Result** | **Tool Feedback** |
| --- | --- | --- | --- | --- | --- |
| password123 | lowercase + digits | 11 | All | **Weak** | Common, easily guessed |
| Passw0rd! | mixed case + symbol | 9 | All | **Medium** | Some complexity, still predictable |
| P@55w0rd!2024 | upper + lower + numbers + symbols | 13 | All | **Strong** | Secure, not easily guessable |
| R$Xf8L!pG@72x#yB | random full mix | 16 | All | **Very Strong** | Excellent entropy and resistance |

**Best Practices for Strong Passwords**

* **Minimum Length:** Use **12+ characters** (preferably 16+).
* **Mix Characters:** Combine uppercase, lowercase, numbers, and special characters.
* **Avoid Predictable Patterns:** No dictionary words, birthdays, or reused phrases.
* **Use Passphrases:** Four or more random words, optionally separated by symbols.
  + Example: Glass!Rocket$Tiger#Train7
* **Never Reuse Passwords:** Use unique passwords for every account.
* **Store Securely:** Use a password manager (e.g., Bitwarden, KeePass).
* **Enable MFA:** Always pair passwords with multi-factor authentication.

**Common Password Attack Types**

| **Attack Type** | **Description** | **Password Defense** |
| --- | --- | --- |
| **Brute Force** | Tries every possible combination | Long, complex passwords exponentially increase crack time |
| **Dictionary Attack** | Uses lists of common words/phrases | Avoid real words, add randomness |
| **Credential Stuffing** | Uses leaked credentials on multiple sites | Unique passwords prevent this |
| **Phishing/Keylogging** | Tricks user or logs keystrokes | Use 2FA, cautious email behavior |

**Summary**

This task illustrated the significance of strong password hygiene in digital security. Using modern password checkers, we confirmed that length and character diversity are the most effective ways to strengthen password protection. Secure passwords, combined with 2FA and responsible storage, can mitigate most forms of credential-based attacks.