Task 6 Report – Password Creation & Strength Evaluation

Prepared by : Sakshi Patil

Date : 6 June 2025

# 1. Introduction

Passwords remain the first—and often only—line of defence between an attacker and protected data. Modern cracking hardware has dramatically reduced the time required to brute-force weak credentials, making proper password hygiene essential. This exercise evaluates multiple passwords of increasing complexity against industry-standard strength-checking tools and extracts best-practice guidance.

# 2. Methodology

1. Generated five candidate passwords that range from very weak to very strong.  
2. Tested each password using PasswordMeter, Kaspersky Password Checker, and NordPass.  
3. Recorded scores and analyzed character diversity and length impact.  
4. Researched modern attack methods and current recommendations.

# 3. Tested Passwords & Tool Results

|  |  |  |  |
| --- | --- | --- | --- |
| Password | PasswordMeter Score | Kaspersky Est. Time to Crack | NordPass Rating |
| password123 | 24 % | Instantly | Very Weak |
| Sakshi@2025 | 55 % | 2 Hours | Weak |
| Xyz@!78pQr | 84 % | 2 Years | Strong |
| W3!rD#P@55w0rdZ | 94 % | 800 Centuries | Very Strong |
| Pizza@Moon88Dance! | 92 % | 200 Centuries | Very Strong |

# 4. Analysis

1. Length dramatically increases password strength.  
2. Including symbols, numbers, and mixed-case characters improves resistance.  
3. Common words and personal information reduce effectiveness.  
4. Passphrases like 'Pizza@Moon88Dance!' are both memorable and secure.

# 5. Common Attack Vectors & Mitigations

- Brute Force: Tries all combinations. Counter: long, complex passwords.  
- Dictionary Attack: Uses known passwords. Counter: avoid dictionary words.  
- Credential Stuffing: Uses reused passwords. Counter: unique passwords per site.

# 6. Best-Practice Recommendations

1. Use at least 12-15 characters.  
2. Mix uppercase, lowercase, numbers, and symbols.  
3. Avoid names, dates, and personal info.  
4. Use a password manager.  
5. Enable Two-Factor Authentication (2FA).

# 7. Conclusion

Password strength depends heavily on length and character variety. Testing shows that long, complex passwords can resist modern cracking tools for centuries. Adopting best practices is essential for individual and organizational security.