# 🔐 Password Strength Evaluation Report

## 🎯 Objective

The objective of this task is to understand what makes a password strong and to evaluate password strength using online tools like passwordmeter.com.

## 🧠 Methodology

1. Created multiple passwords with varying levels of complexity.  
2. Tested each password using passwordmeter.com.  
3. Recorded feedback, scores, and analysis.  
4. Researched common password attacks.  
5. Identified best practices for creating strong passwords.

## 📋 Password Test Results

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Password | Complexity | Length | Strength Score | Feedback |
| delta123 | Low | 8 | 20% | Simple word + numbers, easily guessed. |
| Delta@2025 | Medium | 10 | 55% | Includes uppercase & symbol but predictable. |
| G@te#Way!789 | High | 12 | 90% | Strong mix of characters, hard to guess. |
| Z!9p@Q#xRt$3 | Very High | 12 | 100% | Randomized and extremely strong. |

## ⚙️ Analysis

Passwords with higher complexity, longer length, and more randomness are significantly stronger. Short and predictable passwords are vulnerable to brute-force and dictionary attacks.

## 🧩 Best Practices Learned

• Use 12–16 characters or more.  
• Combine uppercase, lowercase, numbers, and symbols.  
• Avoid names, dates, or dictionary words.  
• Use password managers for secure storage.  
• Do not reuse passwords across different accounts.

## ⚔️ Common Password Attacks

1. Brute Force – Tries every possible combination.  
2. Dictionary Attack – Uses common words and patterns.  
3. Phishing – Tricks users into revealing credentials.  
4. Credential Stuffing – Reuses leaked passwords from other sites.

## ✅ Conclusion

The strongest password was 'Z!9p@Q#xRt$3'. It demonstrates that a long, random mix of characters provides the highest security. Password complexity directly impacts resistance to attacks.