Password Strength Evaluation Report

July 1, 2025

1 Objective

The objective of this task is to create multiple passwords with varying complexity, test their strength using an online password strength checker (Password Meter at https://passwordmeter.com), and analyze the results to identify best practices for creating strong passwords. Additionally, this report examines common password attacks and discusses how password complexity enhances security.

2 Password Creation

Four passwords were created to test different levels of complexity, incorporating uppercase letters, lowercase letters, numbers, symbols, and varying lengths:

1. **Password 1**: simple123
2. **Password 2**: Password2025
3. **Password 3**: Tr0ub4dor3xplor3r
4. **Password 4**: K9mP$zL8qW@2vN$!

3 Password Strength Evaluation

Each password was evaluated using Password Meter (https://passwordmeter.com), which provides a score (0–100) and feedback based on factors like length, character variety, and complexity. The results are summarized below:

Table 1: Password Strength Test Results

Password	Score	Feedback
simple123	28	Weak: Too short, lacks uppercase and symbols.
Password2025	56	Medium: Decent length, has uppercase and numbers, but predictab
Tr0ub4dor&3xplor3r	92	Very Strong: Good length, mixed characters, but includes dictionar
K9#mP$zL8qW@2vN!	98	Very Strong: Excellent length, diverse characters, no dictionary wo

3.1 Analysis of Results

- **Password 1 (simple123)**: Scored low due to its short length (9 characters) and lack of uppercase letters and symbols. It is vulnerable to brute force and dictionary attacks.
- **Password 2 (Password2025)**: Improved score due to longer length (12 characters) and inclusion of uppercase and numbers, but lacks symbols and uses a predictable word ("Password"), making it susceptible to dictionary attacks.
- **Password 3 (Tr0ub4dor&3xplor3r)**: High score due to 18 characters, mixed character types, and symbols. However, it incorporates dictionary words ("troubadour" and "explorer" with substitutions), which slightly weakens it against sophisticated attacks.
- **Password 4 (K9#mP$zL8qW@2vN!)**: Near-perfect score due to 16 characters, diverse character types (uppercase, lowercase, numbers, symbols), and no recognizable words, making it highly resistant to attacks.

4 Best Practices for Creating Strong Passwords

Based on the evaluation, the following best practices ensure strong passwords:

1. **Length**: Use at least 12–16 characters. Longer passwords are harder to crack.
2. **Diversity**: Include uppercase letters, lowercase letters, numbers, and symbols to increase complexity.
3. **Avoid Predictable Patterns**: Do not use dictionary words, common phrases, or personal information (e.g., names, birthdays).
4. **Randomness**: Use random character sequences or password managers to generate unpredictable passwords.
5. **Uniqueness**: Avoid reusing passwords across different accounts to limit the impact of a breach.

5 Tips Learned from Evaluation

- Longer passwords significantly improve strength, even with fewer character types.
- Symbols and mixed case greatly enhance scores, as seen in Passwords 3 and 4.
- Dictionary words, even with substitutions (e.g., "0" for "o"), reduce security.
- Password Meter penalizes repetitive characters and predictable patterns, emphasizing randomness.
- Regularly updating passwords and using two-factor authentication (2FA) complements strong passwords.

6 Common Password Attacks

Two prevalent password attacks were researched:

- **Brute Force Attack**: Attackers systematically try all possible character combinations to guess a password. Short passwords like “simple123” are highly vulnerable due to fewer combinations (e.g., $36^9 \approx 10^{14}$ for a 9-character password using letters and numbers). Longer passwords like Password 4 ($94^{16} \approx 10^{31}$) are exponentially harder to crack.

- **Dictionary Attack**: Attackers use lists of common words, phrases, or leaked passwords. Passwords 1 and 2 are susceptible due to dictionary words (“simple” and “Password”). Passwords 3 and 4 are more resistant, especially Password 4, which avoids recognizable words.

7 Impact of Password Complexity on Security

Password complexity directly impacts resistance to attacks:

- **Length**: Each additional character exponentially increases the time required for brute force attacks. For example, a 16-character password is 36^7 times harder to crack than a 9-character password (assuming a 36-character set of letters and numbers).

- **Character Variety**: Using multiple character types (e.g., symbols, uppercase) increases the character set size (e.g., 94 vs. 36), making brute force attacks more computationally intensive.

- **Randomness**: Avoiding dictionary words or patterns thwarts dictionary attacks and social engineering. Password 4s random structure makes it nearly impervious to such attacks.

- **Entropy**: Higher entropy (randomness) passwords, like Password 4, have more possible combinations, enhancing security. Entropy for Password 4 is approximately $\log_2(94^{16}) \approx 105$ bits, compared to $\log_2(36^9) \approx 46$ bits for Password 1.

Complex passwords, combined with 2FA and secure storage (e.g., password managers), significantly reduce the risk of unauthorized access.

8 Conclusion

The evaluation demonstrates that passwords with long lengths, diverse characters, and no dictionary words (e.g., Password 4: K9#mP$zL8qW@2vN!) offer the highest security. Password Meter scores reflect this, with Password 4 scoring 98/100. Best practices include prioritizing length, randomness, and character variety while avoiding predictable patterns. Understanding brute force and dictionary attacks underscores the importance of complexity in thwarting unauthorized access. Implementing these practices ensures robust password security in an increasingly threat-prone digital landscape.