Report on Creating a Strong Password and Evaluate Its Strength.

Report Type: Manual

Performer: Aditya Kamble

Tool: Passwordmeter.com

Date: 04/06/2025 Wednesday

Password Strength Evaluation Report

Objective

This report aims to understand the components of a strong password and evaluate password strength using online tools.

Tools Used

- Online free password strength checkers, specifically passwordmeter.com.

Password Creation and Evaluation

- To assess password strength, multiple passwords with varying complexity were designed and tested. The results from passwordmeter.com are documented below:

Password	**Length**	**Character Mix (Uppercase, Lowercase, Numbers, Symbols)**	**Score**	**Feedback/Time to Crack**
password123	11	Lowercase, numbers	49%	Instant/Very Fast
Summer2025	10	Uppercase, lowercase, numbers	83%	Seconds to Minutes
Th!sIsAStr0ngP@ssw0rd!	24	Uppercase, lowercase, numbers, symbols	100%	Years to Centuries
G0ldF!sh_Sw!m_!n_Wat3r$	25	Uppercase, lowercase, numbers, symbols, passphrase-like	100%	Centuries to Millennia
zXcvBnm7_!@#$54321	19	Uppercase, lowercase, numbers, symbols, random	100%	Centuries to Millennia

Analysis and Best Practices

Based on the evaluation, several factors significantly contribute to password strength:

1. **Length:** Longer passwords are inherently more secure. Passwords with 15+ characters, especially passphrases, drastically increase the time required for an attacker to crack them.
2. **Complexity/Character Mix:** Incorporating a diverse range of characters—uppercase letters, lowercase letters, numbers, and symbols—greatly enhances strength. This makes it harder for attackers to guess or brute-force the password.
3. **Randomness:** Passwords that appear random and do not contain easily identifiable words or patterns are much stronger. Avoid sequential characters or common substitutions.
4. **Uniqueness:** Using unique passwords for each account prevents credential stuffing attacks, where a breach on one site compromises other accounts.

Tips Learned from Evaluation

- **Prioritize Length:** When in doubt, make your password longer. A long passphrase is often easier to remember and more secure than a complex, short password.
- **Mix It Up:** Always combine different character types. Simply adding a number to a common word provides minimal security.
- **Avoid Personal Information:** Do not use personal details like birth dates, names, or addresses.
- **Don't Reuse:** Never reuse passwords across multiple accounts.
- **Consider Passphrases:** Passphrases, which are sequences of random or unrelated words, can be both strong and memorable.

Common Password Attacks

Understanding common password attacks helps in creating more resilient passwords:

- **Brute Force Attack:** In a brute force attack, an attacker systematically tries every possible combination of characters until the correct password is found. The longer and more complex a password, the more time and computational power a brute force attack requires.
- **Dictionary Attack:** A dictionary attack uses a list of common words, phrases, and previously leaked passwords to guess a password. This is why avoiding common words or easily guessable phrases is crucial

How Password Complexity Affects Security

- Password complexity directly correlates with the time and resources an attacker needs to crack it. A simple, short password can be cracked almost instantly with modern computing power, often through brute force or dictionary attacks. As complexity (length, character variety, randomness) increases, the number of possible combinations grows exponentially, making it computationally infeasible for attackers to guess or brute-force the password within a reasonable timeframe. This significantly enhances the security of online accounts and sensitive information

Key Concepts

- **Password Strength:** A measure of how difficult it is for an unauthorized person or program to guess or crack a password.
- **Brute Force Attack:** An attack method that tries every possible password combination.
- **Dictionary Attack:** An attack method that tries common words and phrases from a list.
- **Authentication:** The process of verifying the identity of a user.
- **Best Practices:** Recommended guidelines for creating secure passwords.
- **Multi-Factor Authentication (MFA):** An additional layer of security beyond just a password, often requiring a second verification method (e.g., a code from a phone).
- **Password Managers:** Tools that securely store and generate complex, unique passwords for all your online accounts.