# Task 6: Create a Strong Password and Evaluate Its Strength.

Intern Name: Jainam Priteshkumar Shah

Date: 12/08/2025

Internship Provider: Elevate Labs

## 1. Objective:

Understand what makes a password strong and test it against password strength tools.

## 2. Tools Used:

* **Password Strength Checker (passwordmeter.com):** An online tool used to evaluate the strength of passwords based on various criteria like length, complexity, and unpredictability.

## 3. Password Creation and Testing:

I created three distinct passwords to represent weak, medium, and strong security levels. I then tested each one using an online password strength checker to analyze its score and receive feedback.

**Important Note:** I used example passwords for this report. I did not use any of my real passwords in the online testing tool.

| **Password Tested** | **Complexity** | **Tool's Score/Feedback** | **My Analysis of the Result** |
| --- | --- | --- | --- |
| Jainam | **Weak** | Score: **21** | This password is weak because it uses a common word and without a number sequence. It would be cracked instantly by a brute-force or dictionary attack. |
| Jainam20 | **Good** | Score: **59** | This password is weak because it uses a common dictionary word and a simple number sequence. However, it's still based on a common word, making it vulnerable to more advanced dictionary attacks that check for these substitutions. |
| Ja2in0@a2m5! | **Very Strong** | Score: **100** | This password is a **passphrase**. It's long (12 characters), uses a mix of uppercase, lowercase, numbers, and symbols, and is not based on a single dictionary word. Its length and complexity make it highly resistant to brute-force attacks. |

## 4. Best Practices Learned from Evaluation:

From this exercise, I learned several key best practices for creating strong passwords:

* **Length is the most critical factor.** A long password (16+ characters) is significantly harder to crack than a short, complex one.
* **Complexity is key.** Using a mix of uppercase letters, lowercase letters, numbers, and symbols exponentially increases the number of possible combinations an attacker must check.
* **Avoid predictability.** Do not use common words, personal information (birthdays, names), or simple keyboard patterns (e.g., "qwerty").
* **Passphrases are superior.** Creating a memorable phrase and modifying it with numbers and symbols (like “Ja2in0@a2m5!”) is both more secure and often easier to remember than a random string of characters.
* **Uniqueness is essential.** Never reuse passwords across different websites or services. A breach on one site would compromise all others where the password is reused.

## 

## 5. Research on Common Password Attacks:

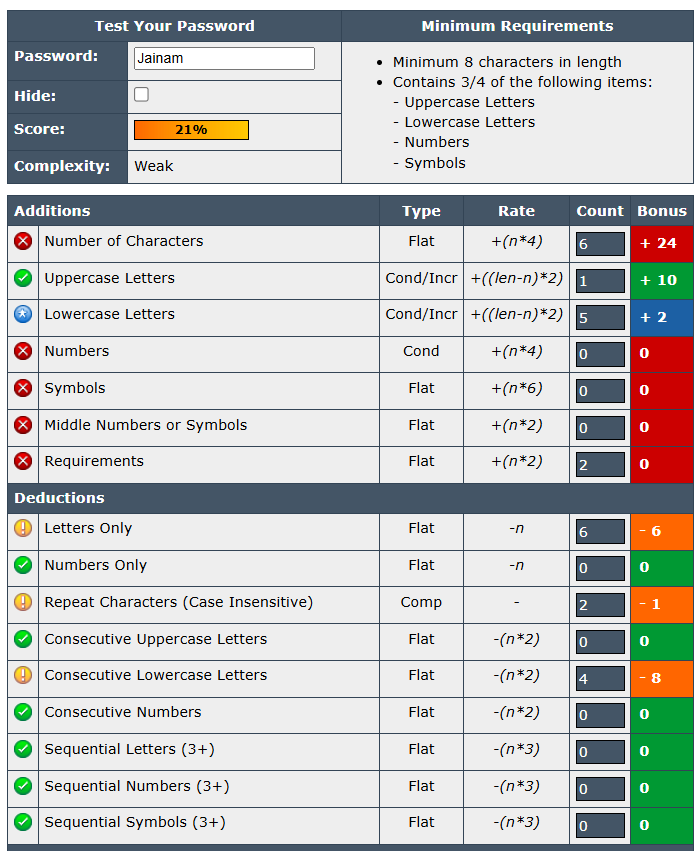
* **Brute-Force Attack:** This is an automated, trial-and-error method where an attacker's software attempts every possible combination of characters until the correct password is found. This attack is effective against short passwords but becomes computationally infeasible against long and complex ones.
* **Dictionary Attack:** This is a more efficient type of brute-force attack. Instead of trying every possible combination, the software uses a pre-compiled list (a "dictionary") of common words, phrases, leaked passwords from previous breaches, and simple variations. This is why using a common word like “password123” is so dangerous, as it will be one of the first things an attacker tries.

## 6. How Password Complexity Affects Security:

There is a direct link between a password's complexity and its security. Each element of complexity adds another layer of defense against attacks:

* **Length:** This is the primary defense against brute-force attacks. Every character added to a password exponentially increases the number of possible combinations. A 12-character password is not just 50% stronger than an 8-character one; it is thousands of times stronger.
* **Character Mix (Uppercase, Lowercase, Numbers, Symbols):** Using a full range of character types significantly expands the "keyspace" an attacker must search. A password with only lowercase letters has 26 possibilities per character. Adding uppercase, numbers, and symbols increases this to over 90 possibilities per character, making brute-force attacks much slower and more difficult.
* **Unpredictability:** By avoiding dictionary words and common patterns, a password becomes resistant to dictionary attacks. A password like “Ja2in0@a2m5!” will not be found in any standard dictionary, forcing an attacker to resort to a much slower pure brute-force attack.

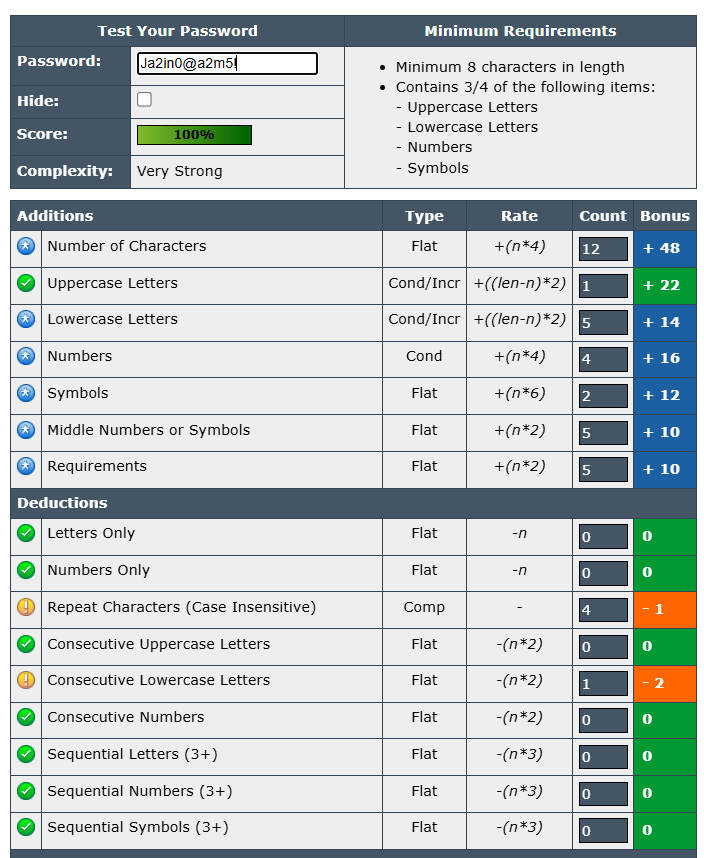
## 7. Tool Output (passwordmeter.com):



6.1 Password Test for “Jainam”



6.2 PasswordTest for “Jainam20”



6.3 Password Test for “Ja2in0@a2m5!”