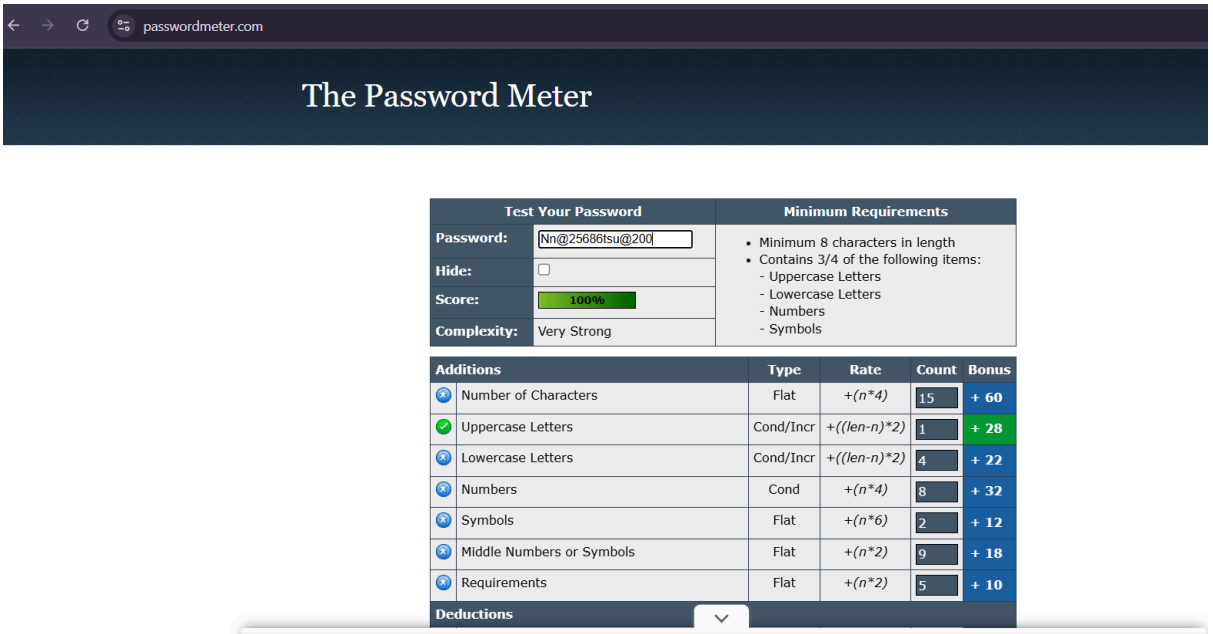
Task 6

Create a Strong Password and Evaluate Its Strength.
Objective: Understand what makes a password strong and test it against password strength tools.
Tools: Online free password strength checkers (e.g., passwordmeter.com).
Deliverables: Report showing password strength results and explanation.

Solution:
While creating password ,The minimum requirements of creating password is Minimum 8 characters in length

- Contains 3/4 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols

You can check the accuracy of password using passwordmeter.



What's a Brute Force Attack?

A brute force attack uses trial-and-error to guess login info, encryption keys, or find a hidden web page. Hackers work through all possible combinations hoping to guess correctly.

These attacks are done by ‘brute force’ meaning they use excessive forceful attempts to try and ‘force’ their way into your private account(s).

This is an old attack method, but it's still effective and popular with hackers. Because depending on the length and complexity of the password, cracking it can take anywhere from a few seconds to many years.

What is a dictionary attack?

A dictionary attack is a method of breaking into a password-protected computer, network or other IT resource by systematically entering every word in a dictionary, or word list, as a password. A dictionary attack can also be used in an attempt to find the key necessary to decrypt an encrypted message or document.

Dictionary attacks work because many computer users and businesses insist on using ordinary words as passwords. Modern dictionary attacks use a wordlist as a base then try combinations of words and permutations with common substitutions, such as replacing an "e" with a "3." These tools can even find unique passwords if they are simple enough.

Results

- A sample password **“Nn@2566tsu@200”** was created and tested on *passwordmeter.com*.
- **Strength Score:** 100% (Very Strong)
- **Analysis:**
    - ✔ Meets minimum length (more than 8 characters)
    - ✔ Contains uppercase, lowercase, numbers, and special symbols
    - ✔ Not a dictionary word
    - ✔ Resistant to brute force and dictionary attacks due to complexity and uniqueness

Conclusion

The experiment demonstrated that a strong password must be long, complex, and unique. Passwords that include a combination of uppercase letters, lowercase letters, numbers, and symbols are significantly harder to crack. While brute force attacks can eventually succeed, the time required to break a strong password increases exponentially with its complexity. Similarly, dictionary attacks are ineffective when the password does not rely on common words or predictable patterns.

Therefore, creating and regularly updating strong passwords is an essential security practice to protect personal and organizational accounts against cyberattacks.