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

1.Create multiple passwords with varying complexity.

2.Use uppercase, lowercase, numbers, symbols, and length variations.

3.Test each password on password strength checker.

4.Note scores and feedback from the tool.

5.Identify best practices for creating strong passwords.

6.Write down tips learned from the evaluation.

7.Research common password attacks (brute force, dictionary).

8.Summarize how password complexity affects security

**1.Create multiple passwords with varying complexity.**

1. Basic Complexity (Not Recommended — Easy to Guess)

Shashank123

Sam2025

2. Medium Complexity (Better but Still Crackable)

Djw@2025

Wwe#5

3. Strong Complexity (Hard to Crack)

G8beP3#Kwb

O@wqlP\*442hY%q

4. Very Strong Passphrases (Long and Secure)

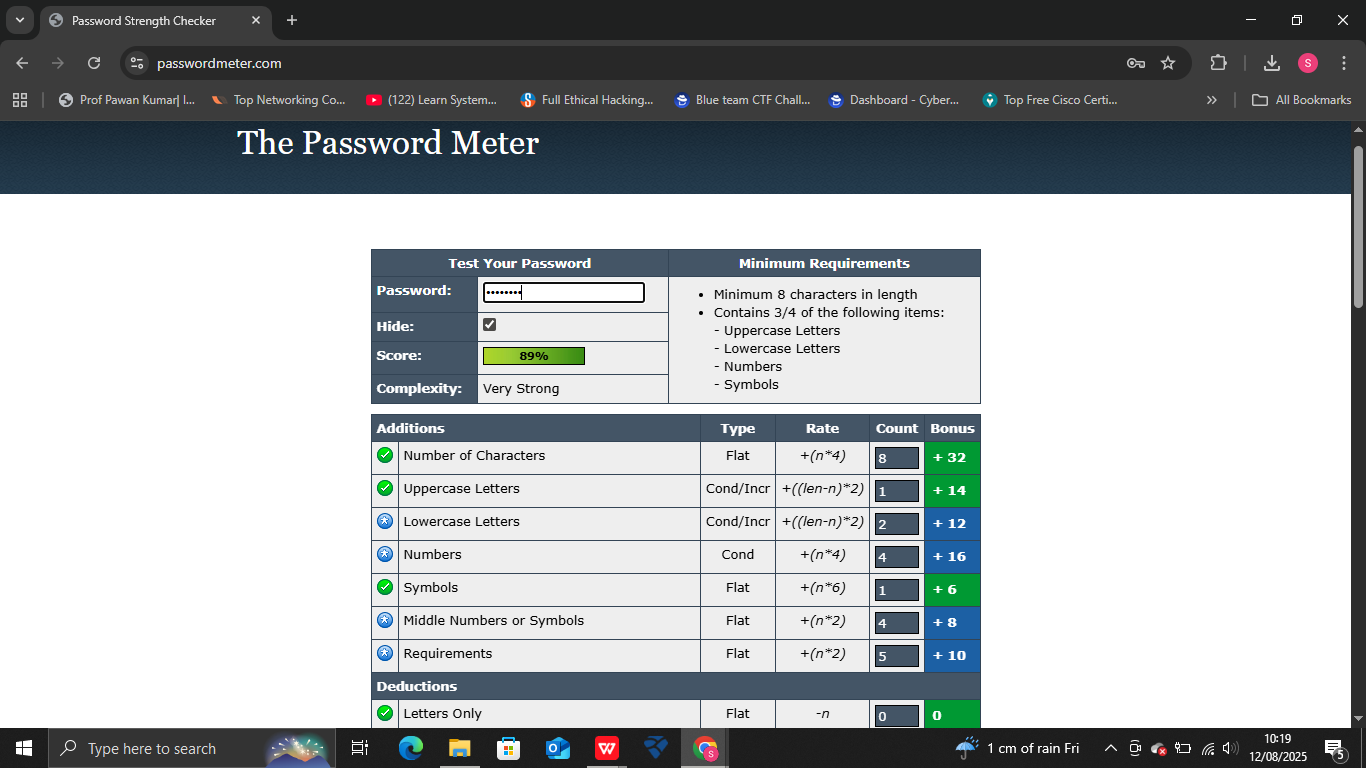
Thebrownfoxjupsoverthebluedog1231#32@

1. **Test each password on password strength checker.**

**4.Note scores and feedback from the tool.**



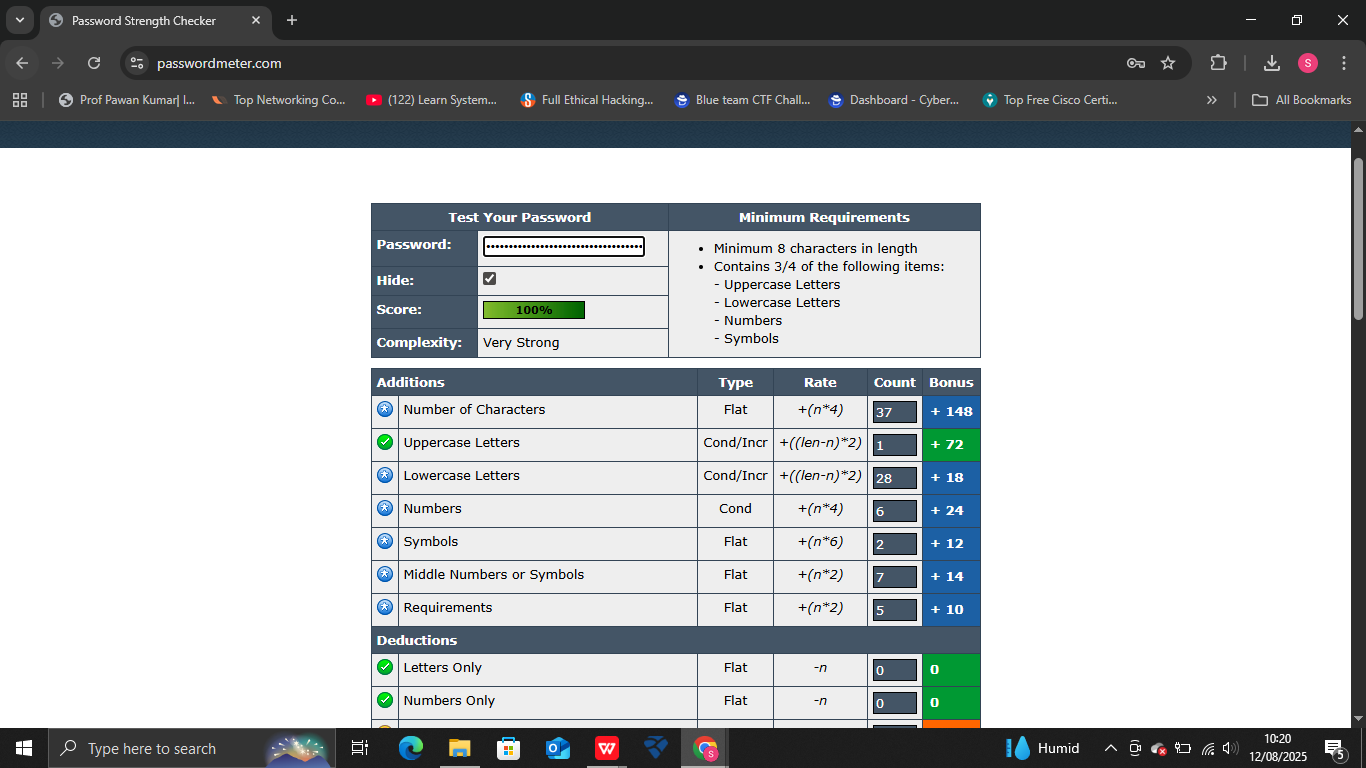
**Shashank123** have the 76% strength



**Djw@2025** have the 89% strength



**G8beP3#Kwb** have 91 % strength



**Thebrownfoxjupsoverthebluedog1231#32@** have the 100% strength.

**5.Identify best practices for creating strong passwords.**

1. Use Long Passwords

At least 12–16 characters; longer is better.

Increases resistance to brute-force attacks exponentially.

2. Mix Character Types

Include uppercase, lowercase, numbers, and symbols.

Example: G#7kL!x9P$2

3. Avoid Personal Information

Don’t use your name, birthday, phone number, or pet’s name.

Hackers often find this in social media or public data.

4. Use Unique Passwords for Every Account

Prevents credential stuffing if one account is breached.

5. Consider Passphrases

Use a random sequence of words or a sentence with numbers/symbols.

Example: Sunset!On4GreenHills

**6.Write down tips learned from the evaluation.**

**Tips from Password Evaluation**

Length matters — longer passwords scored higher in the strength checker.

Strong passwords require unpredictability — avoid predictable substitutions like @ for “a”

Variety of characters (uppercase, lowercase, numbers, and symbols) improves password strength significantly.

Avoid using personal information like names or birth years, as they make passwords easier to guess.

Passphrases are powerful — long, random word combinations with symbols scored the highest.

Medium complexity passwords are still vulnerable — even if they score well, they may be guessable with targeted attacks.

**7.Research common password attacks (brute force, dictionary).**

**Common Password Attacks**

**1. Brute-Force Attack**

Definition:

A method where attackers try every possible combination of characters until they find the correct password.

How It Works:

Starts from short combinations and moves to longer ones.

Uses automated tools that can test millions of passwords per second.

Weakness Exploited:

Short passwords and ones with limited character variety are easier to crack.

Example:

If your password is cat12, a brute-force tool will eventually guess it after trying all 5-character combinations.

Prevention:

Use long, complex passwords.

Enable account lockout after repeated failed attempts.

**Use multi-factor authentication (MFA).**

**2. Dictionary Attack**

Definition:

An attack that uses a precompiled list (dictionary) of common words, passwords, and variations to guess the password.

How It Works:

Instead of trying every possible character combination, the tool checks likely passwords from a list.

Lists often include leaked passwords, common words, and predictable variations like password123 or qwerty!.

Weakness Exploited:

Many people use simple or common passwords that are part of known breach data.

Example:

If your password is Football2025, it might already be in a hacker’s dictionary file.

Prevention:

Avoid real words or common phrases.

Use random combinations of words, numbers, and symbols.

Consider password managers to generate unique passwords.

**8.Summarize how password complexity affects security**

**Impact of Password Complexity on Security**

Higher Complexity = More Possible Combinations

Adding length, character variety, and randomness increases the total number of possible password combinations, making brute-force attacks take significantly longer.

Better Resistance to Dictionary Attacks

Complex passwords that don’t use common words or predictable substitutions are less likely to appear in hacker password lists.

Slows Automated Cracking Tools

Each additional character or symbol exponentially increases cracking time, making automated attacks impractical.