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.

---

1). Password is: - #Password@9091*

The Password Meter

Test Your Password		Minimum Requirements
Password:	•••••••••••••••	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☑	
Score:	100%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	15	+ 60
Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 28
Lowercase Letters	Cond/Incr	+((len-n)*2)	7	+ 16
Numbers	Cond	+(n*4)	4	+ 16
Symbols	Flat	+(n*6)	3	+ 18
Middle Numbers or Symbols	Flat	+(n*2)	5	+ 10
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	4	- 1
Consecutive Uppercase Letters	Flat	-(n*2)	0	0

---

2). Password is :- @9qwe%Vinay087.in

Tips Learned from the Evaluation:

- Use a mix of uppercase and lowercase letters.
- Include numbers and special characters (e.g., !, @, #, $).
- Make the password at least 12 characters long.
- Avoid using dictionary words or common phrases.
- Do not reuse passwords across multiple sites.
- Random combinations of characters are more secure than meaningful words.
- Consider using a passphrase made up of unrelated words for better memorability and strength.

Common Password Attacks:

- **Brute Force Attack**:
  The attacker tries every possible combination of characters until the correct password is found. Short and simple passwords are easier to crack this way.
- **Dictionary Attack**:
  This method uses a list of common words and password combinations (like "password123" or "qwerty") to guess the password. Passwords made of real words are especially vulnerable.
- **Credential Stuffing**:
  Attackers use leaked usernames and passwords from one service to try and log into others, assuming people reuse passwords.
- **Phishing**:
  Users are tricked into revealing their passwords through fake websites or emails.

How Password Complexity Affects Security:

Password complexity makes it significantly harder for attackers to guess or crack your password. A strong password that includes:

- Random combinations of letters, numbers, and symbols,
- Sufficient length (typically 12+ characters),
- No predictable patterns or dictionary words,

...can resist both brute force and dictionary attacks. The more complex and unique your password, the more time and computing power it takes to crack it—often making it impractical for attackers.