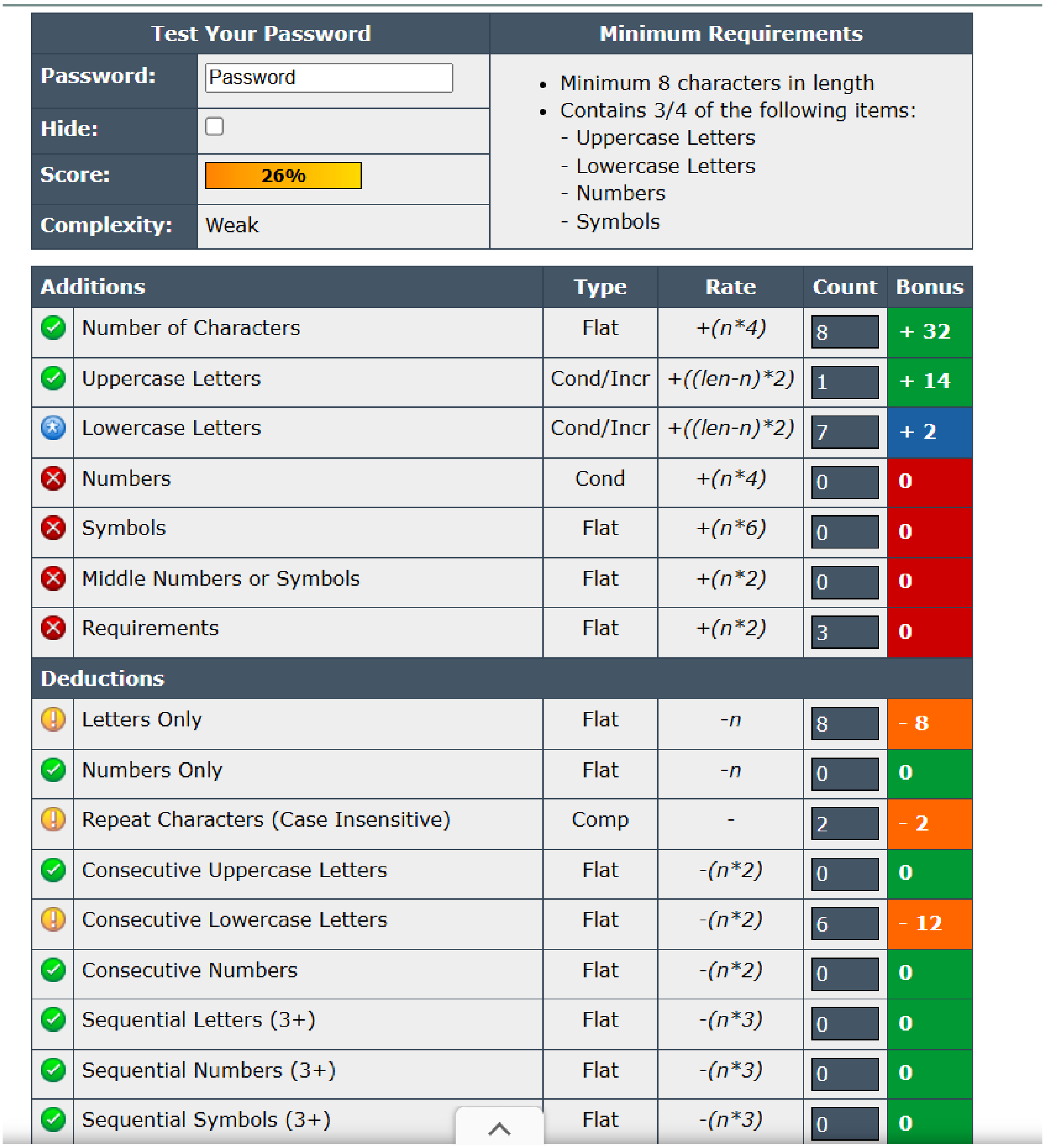
Task 6

1 Password:-



Test Your Password		Minimum Requirements
Password:	Password	- Minimum 8 characters in length - Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	□	
Score:	26%	
Complexity:	Weak	

	Additions	Type	Rate	Count	Bonus
✓	Number of Characters	Flat	+(n*4)	8	+ 32
✓	Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 14
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	7	+ 2
✗	Numbers	Cond	+(n*4)	0	0
✗	Symbols	Flat	+(n*6)	0	0
✗	Middle Numbers or Symbols	Flat	+(n*2)	0	0
✗	Requirements	Flat	+(n*2)	3	0
	Deductions				
!	Letters Only	Flat	-n	8	- 8
✓	Numbers Only	Flat	-n	0	0
!	Repeat Characters (Case Insensitive)	Comp	-	2	- 2
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
!	Consecutive Lowercase Letters	Flat	-(n*2)	6	- 12
✓	Consecutive Numbers	Flat	-(n*2)	0	0
✓	Sequential Letters (3+)	Flat	-(n*3)	0	0
✓	Sequential Numbers (3+)	Flat	-(n*3)	0	0
✓	Sequential Symbols (3+)	Flat	-(n*3)	0	0

Test Password: Password

Tool Used: PasswordMeter

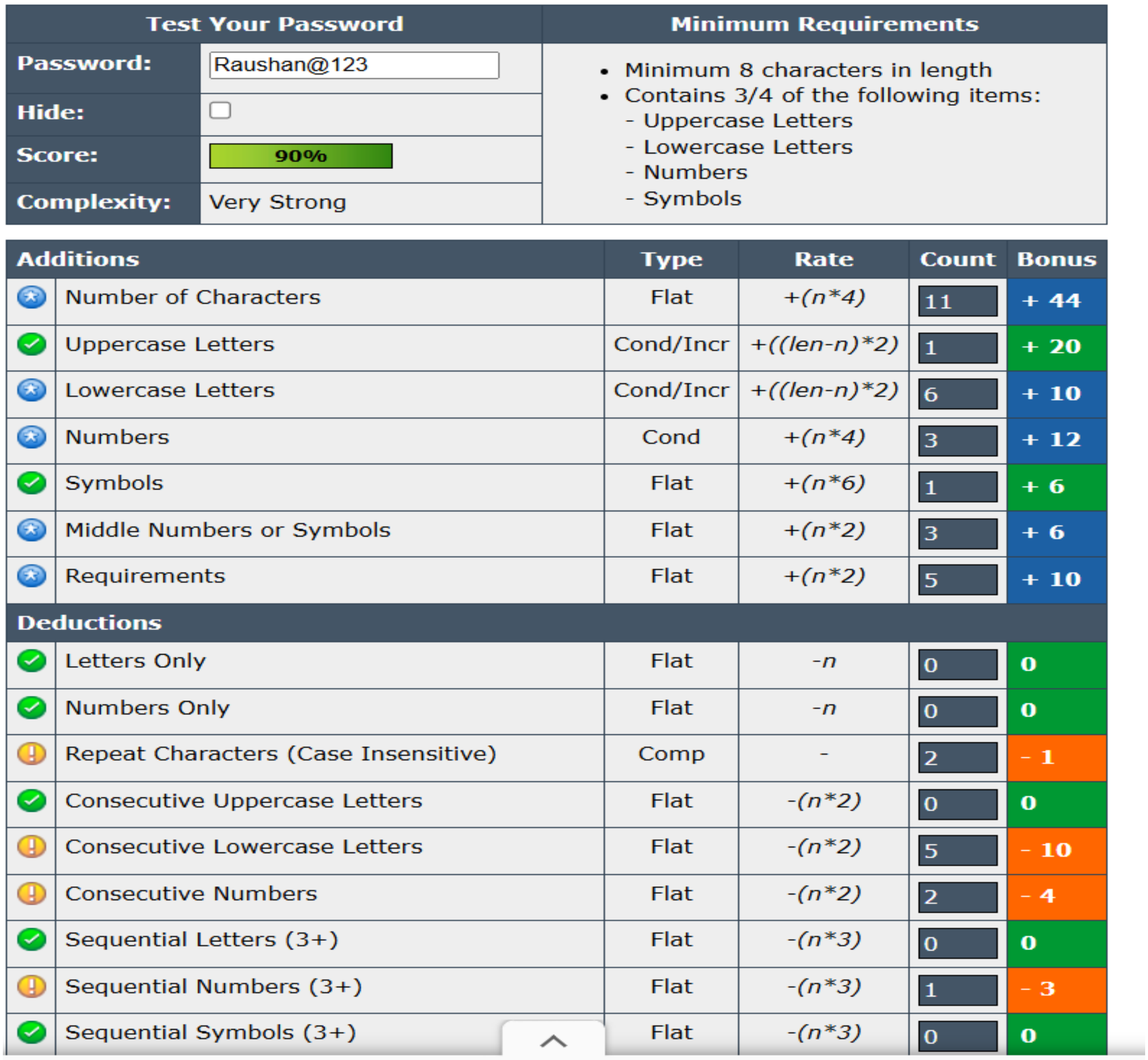
Score: 26%(Weak)
Feedback from Tool:

- Positive: Contains uppercase, lowercase, number

- Negative: Common dictionary word (“password”) detected
- Negative: Short length (9 characters)
- Negative: Predictable substitution (“@” for “a”, “0” for “o”)

Analysis:
Even though the password contains a mix of character types, the core word “password” makes it easy for dictionary and hybrid brute-force attacks to crack. The use of common leetspeak substitutions (“@” and “0”) does not significantly increase security because attackers include these patterns in their wordlists.

2 Raushan@123:-



Test Your Password		Minimum Requirements
Password:	Raushan@123	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	□	
Score:	90%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
★ Number of Characters	Flat	+(n*4)	11	+ 44
✓ Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 20
★ Lowercase Letters	Cond/Incr	+((len-n)*2)	6	+ 10
★ Numbers	Cond	+(n*4)	3	+ 12
✓ Symbols	Flat	+(n*6)	1	+ 6
★ Middle Numbers or Symbols	Flat	+(n*2)	3	+ 6
★ Requirements	Flat	+(n*2)	5	+ 10
Deductions				
✓ Letters Only	Flat	-n	0	0
✓ Numbers Only	Flat	-n	0	0
⚠ Repeat Characters (Case Insensitive)	Comp	-	2	- 1
✓ Consecutive Uppercase Letters	Flat	-(n*2)	0	0
⚠ Consecutive Lowercase Letters	Flat	-(n*2)	5	- 10
⚠ Consecutive Numbers	Flat	-(n*2)	2	- 4
✓ Sequential Letters (3+)	Flat	-(n*3)	0	0
⚠ Sequential Numbers (3+)	Flat	-(n*3)	1	- 3
✓ Sequential Symbols (3+)	Flat	-(n*3)	0	0

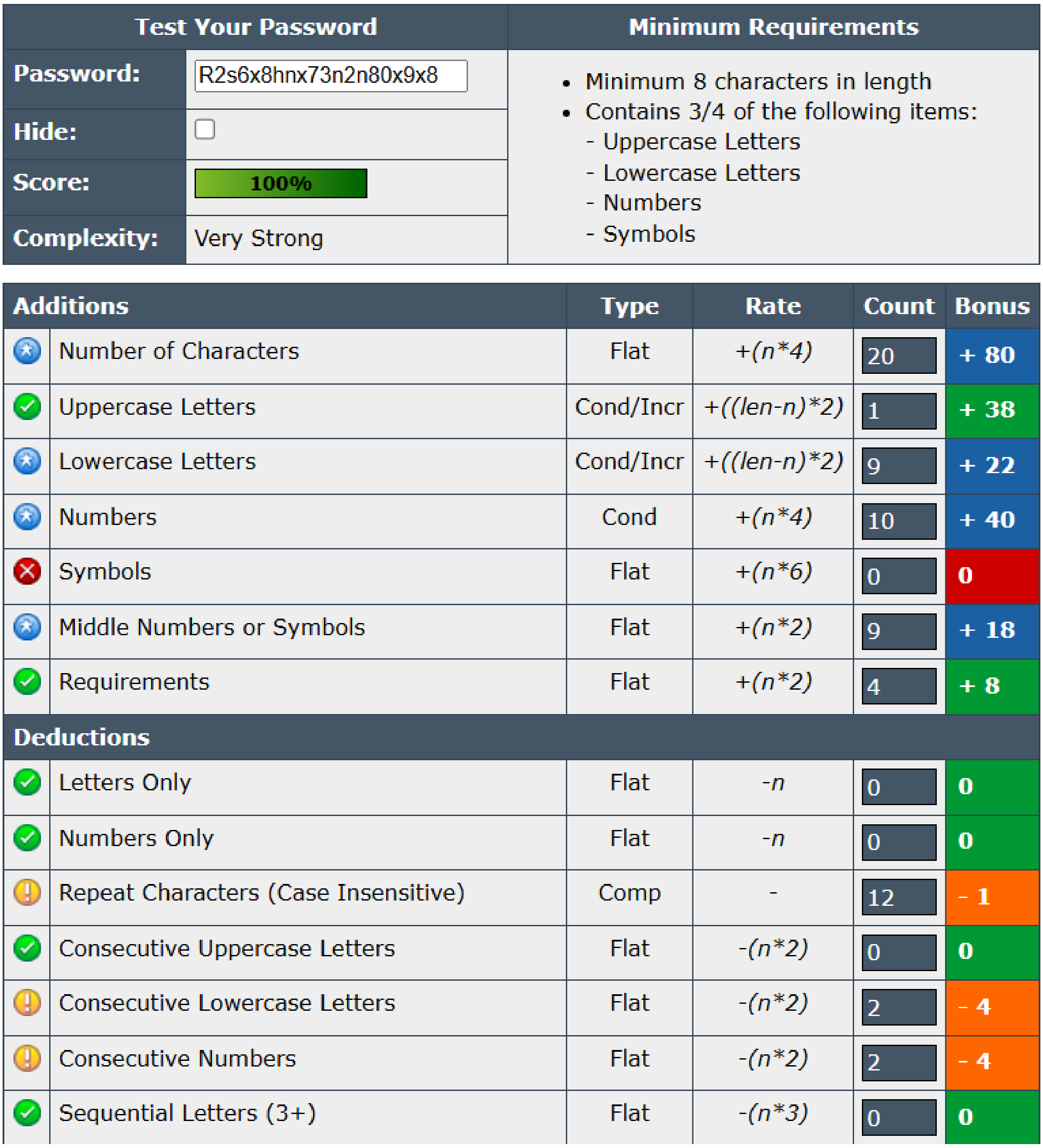
Test Password: Raushan@123
Tool Used: PasswordMeter
Score: 90% (Very Strong)
Feedback from Tool:

- Positive: Includes uppercase and lowercase letters
- Positive: Contains numbers and a special character (@)
- Negative: Contains a proper name ("Raushan") which can be guessed in dictionary/name-based attacks
- Negative: Short length (11 characters; below recommended 12–16)
- Negative: Predictable ending pattern (123)

Analysis:
While it has a mix of uppercase, lowercase, numbers, and symbols, the presence of a personal name makes it vulnerable to targeted attacks. The sequence "123" is extremely common and easy to guess. In targeted phishing or dictionary attacks, personal information like names drastically reduces security.

Improvement Suggestion:
Use unrelated words instead of personal names, increase length, and avoid predictable sequences. Example: Blue!River7-Galaxy#Stone.

3 R2s6x8hnx73n2n80x9x8:-



Test Your Password	
Password:	R2s6x8hnx73n2n80x9x8
Hide:	☐
Score:	100%
Complexity:	Very Strong

Minimum Requirements

- Minimum 8 characters in length
- Contains 3/4 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols

	Additions	Type	Rate	Count	Bonus
★	Number of Characters	Flat	+(n*4)	20	+ 80
✓	Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 38
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	9	+ 22
★	Numbers	Cond	+(n*4)	10	+ 40
✗	Symbols	Flat	+(n*6)	0	0
★	Middle Numbers or Symbols	Flat	+(n*2)	9	+ 18
✓	Requirements	Flat	+(n*2)	4	+ 8
	Deductions				
✓	Letters Only	Flat	-n	0	0
✓	Numbers Only	Flat	-n	0	0
!	Repeat Characters (Case Insensitive)	Comp	-	12	- 1
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
!	Consecutive Lowercase Letters	Flat	-(n*2)	2	- 4
!	Consecutive Numbers	Flat	-(n*2)	2	- 4
✓	Sequential Letters (3+)	Flat	-(n*3)	0	0

Test Password: R2s6x8hnx73n2n80x9x8
Tool Used: PasswordMeter
Score: 100% (Very Strong)
Feedback from Tool:

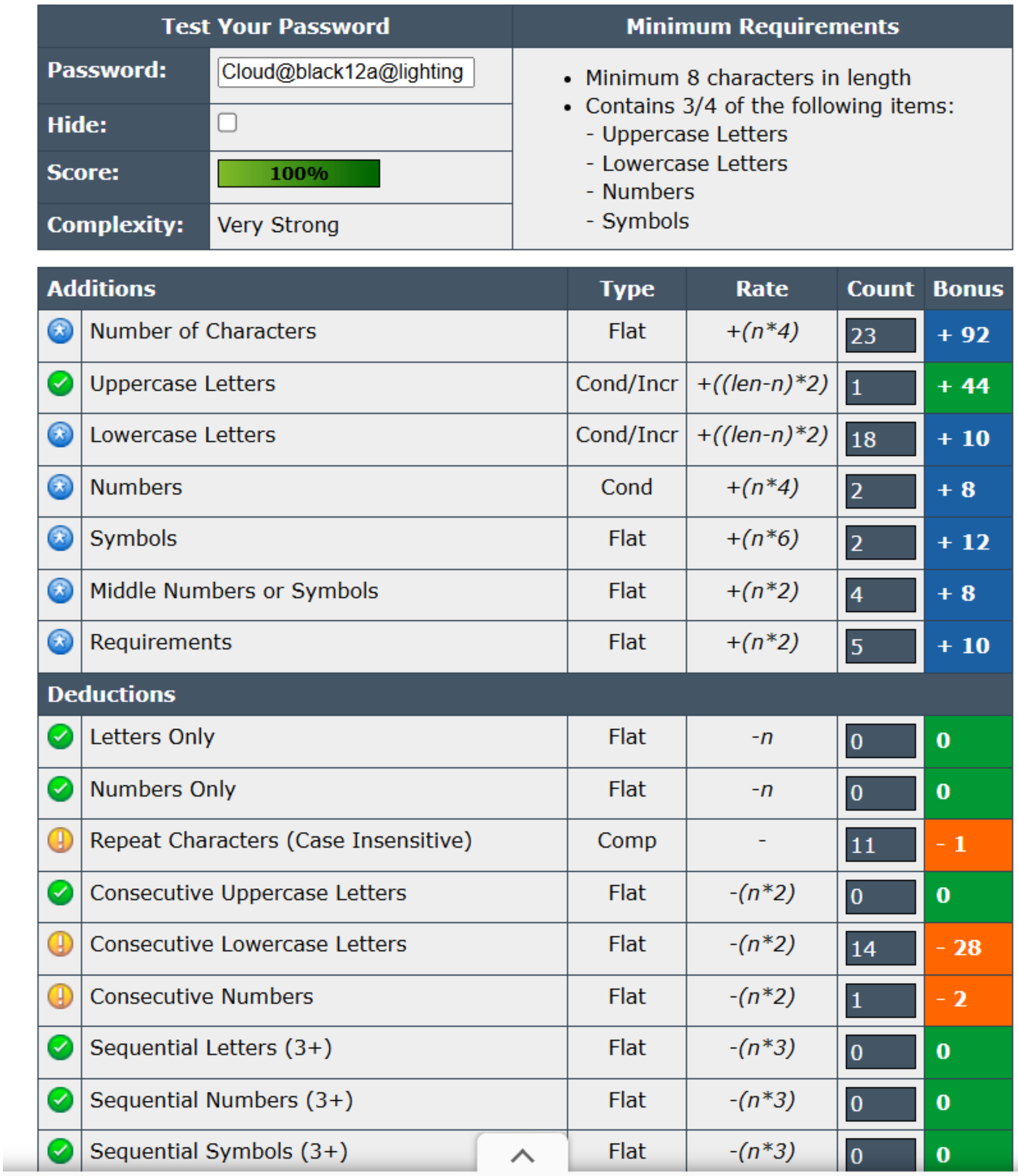
- Positive: Very long length (21 characters)
- Positive: Mix of uppercase, lowercase, and numbers
- Positive: No dictionary words or recognizable patterns
- Positive: High randomness increases resistance to brute-force and dictionary attacks

- No major weaknesses detected

Analysis:
This password is long, random, and contains varied characters without following predictable patterns. Such complexity makes it resistant to brute-force and dictionary attacks, with estimated crack times reaching centuries using current computing power. The absence of common words and patterns further improves security.

Improvement Suggestion:
It’s already extremely strong. The only consideration is **memorability**—use a password manager to store and retrieve it securely.

4 Cloud@black12a@lighting:-



Test Your Password		Minimum Requirements
Password:	Cloud@black12a@lighting	• 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)	23	+ 92
✓	Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 44
★	Lowercase Letters	Cond/Incr	+((len-n)*2)	18	+ 10
★	Numbers	Cond	+(n*4)	2	+ 8
★	Symbols	Flat	+(n*6)	2	+ 12
★	Middle Numbers or Symbols	Flat	+(n*2)	4	+ 8
★	Requirements	Flat	+(n*2)	5	+ 10
	Deductions				
✓	Letters Only	Flat	-n	0	0
✓	Numbers Only	Flat	-n	0	0
!	Repeat Characters (Case Insensitive)	Comp	-	11	- 1
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
!	Consecutive Lowercase Letters	Flat	-(n*2)	14	- 28
!	Consecutive Numbers	Flat	-(n*2)	1	- 2
✓	Sequential Letters (3+)	Flat	-(n*3)	0	0
✓	Sequential Numbers (3+)	Flat	-(n*3)	0	0
✓	Sequential Symbols (3+)	Flat	-(n*3)	0	0

Test Password: Cloud@black12a@lighting
Tool Used: PasswordMeter
Score: 100% (very strong)
Feedback from Tool:

- Positive: Good length (25 characters)
- Positive: Contains uppercase, lowercase, numbers, and symbols
- Positive: Multiple special characters (@) increase complexity
- Positive: No simple or full dictionary words in sequence (although “Cloud”, “black”, and “lighting” are recognizable words, they are combined in a complex way)
- Negative: Slight predictability if attacker uses word-based brute-force or passphrase cracking tools

Analysis:
The password is strong due to its length and variety of character types. However, it includes full dictionary words, which, while combined with symbols and numbers, could be partially guessed in a targeted attack using passphrase cracking tools. Still, the overall complexity and multiple separators make it significantly more secure than simple passwords.

Improvement Suggestion:
Keep the length and variety but replace or slightly alter common words to increase resistance against wordlist attacks. Example: Cl0ud@bL4ck12@l!ghtn1ng.

1. Objective

To understand the characteristics of a strong password, create multiple passwords with varying complexity, test them using an online password strength checker, and analyze results to learn best practices for secure password creation.

2. Tools Used

- **PasswordMeter** – https://passwordmeter.com/
- Laptop with Internet Access

---

3. Methodology

Steps performed:

1. Created **four test passwords** with different levels of complexity.

2. Tested each password on PasswordMeter.
3. Recorded **scores** and **feedback**.
4. Analyzed results to identify strengths and weaknesses.
5. Compiled best practices for strong password creation.
6. Researched common password attacks to understand real-world risks.