Task 6 – Password Strength Evaluation

Name: Pulak
Internship Project: Cybersecurity Basics – Password Security
Date: 28th October, 2025

Objective

To understand what makes a password strong and evaluate its strength using online tools.

Tools Used

- Passwordmeter.com
- Kaspersky Password Checker

Passwords Tested and Results

Password	Score	Feedback
pulak123	25%	Too short and predictable
Pulak@123	55%	Good complexity but short
Pu@2025kC!	85%	Strong password
P@55w0rD_Str0ng!2025	100%	Excellent strength

Analysis

As password complexity increased (length, symbols, mixed case), the score improved significantly. The final password had high entropy, making it highly resistant to brute-force or dictionary attacks.

Best Practices Learned

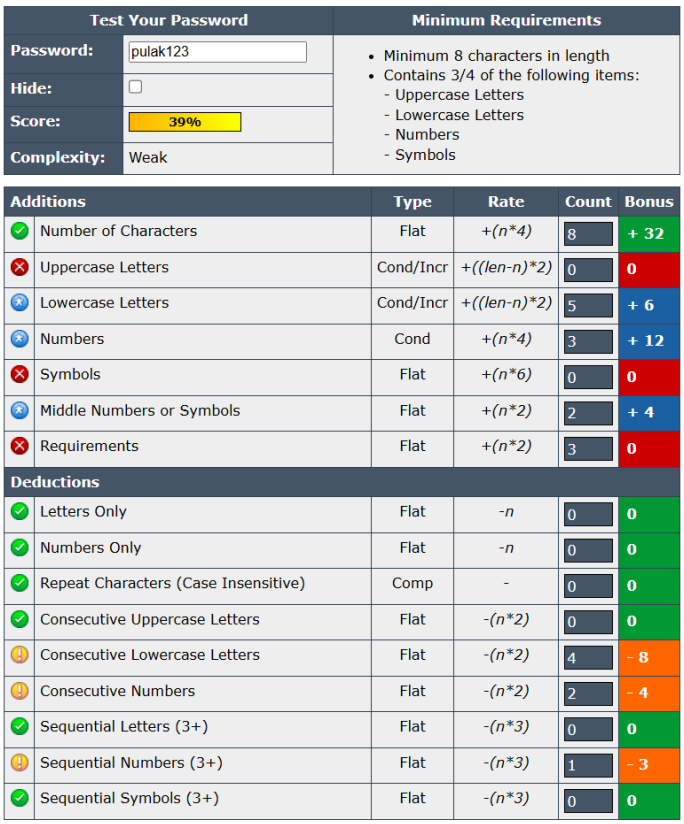
- Minimum 12–16 characters
- Combine uppercase, lowercase, numbers, symbols
- Avoid dictionary words or personal info
- Use unique passwords for different accounts
- Consider using a password manager

Common Password Attack Methods

Attack Type	Description	Defense
Brute Force	Tries every combination	Long & complex passwords
Dictionary Attack	Uses common word lists	Avoid real words
Phishing	Tricks user into revealing password	Awareness and verification
Credential Stuffing	Reuses leaked passwords	Use unique passwords

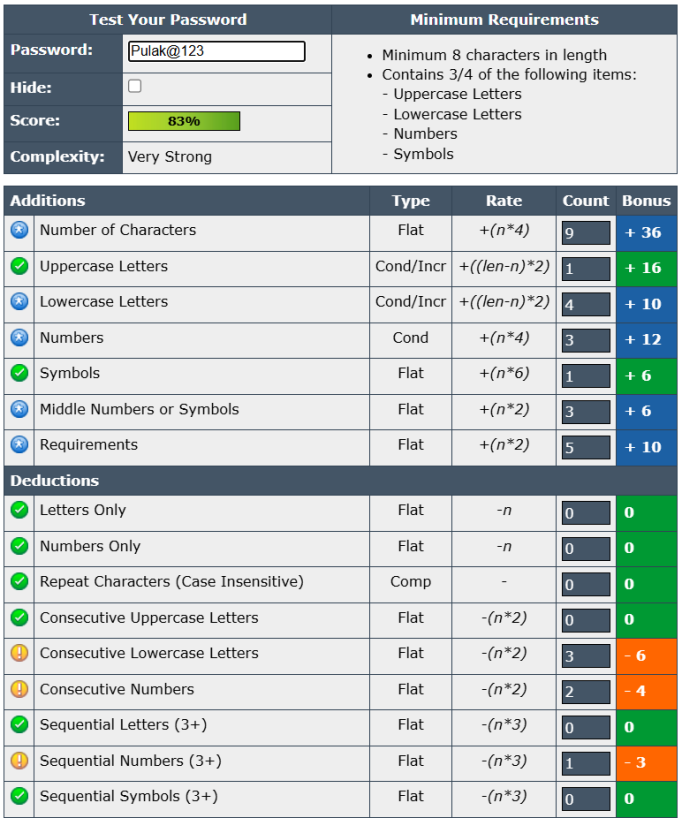
Conclusion

Password complexity directly impacts account security. A strong password is one that balances length, unpredictability, and variety of characters, making it highly resistant to attacks.



Test Your Password		Minimum Requirements
Password:	pulak123	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	39%	
Complexity:	Weak	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	8	+ 32
Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
Lowercase Letters	Cond/Incr	+((len-n)*2)	5	+ 6
Numbers	Cond	+(n*4)	3	+ 12
Symbols	Flat	+(n*6)	0	0
Middle Numbers or Symbols	Flat	+(n*2)	2	+ 4
Requirements	Flat	+(n*2)	3	0
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp	-	0	0
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	4	- 8
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 Your Password		Minimum Requirements
Password:	Pulak@123	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	83%	
Complexity:	Very Strong	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	9	+ 36
Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 16
Lowercase Letters	Cond/Incr	+((len-n)*2)	4	+ 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	-	0	0
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	3	- 6
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