6th Task SUBMISSION REPORT OF ELEVATE LABS CYBERSECURITY INTERNSHIP

NAME	**ADARSH SHARMA**
Submitted to:	**Elevate Labs**
Name of the Academic Institute	**Ganpat University**

REPORT SUBMITTED TO

As part of the Cyber Security Internship, I have completed "Task 6th: Create a Strong Password and Evaluate Its Strength" by following all steps as instructed. Below is a detailed summary of each step followed during the task:

Task 6th: Create a Strong Password and Evaluate Its Strength

Task 4 Report: Create a Strong Password and Evaluat Its Strength

Objective

To create a strong password using best practices in cybersecurity, evaluate its strength using online tools, and understand how complexity contributes to password security.

Step-by-Step Task Execution
1 Create multiple passwords with varying complexity.

Password	Complexity Level
password123	Weak
Passw0rd	Moderate
P@ssw0rd!	Strong
QwErTy2025	Moderate
G!9x#1zB$vK8	Very Strong
aB3!cD5#EfGhIjKl	Extremely Strong

2 Use uppercase, lowercase, numbers, symbols, and length variations.
Each password varies by:

- **Length (from 8 to 16+ characters)**
- **Character types:**
  - **Uppercase (A–Z)**
  - **Lowercase (a–z)**
  - **Numbers (0–9)**
  - **Symbols (!@#$%^&*)**

3 Test each password on password strength checker.
Use online tools like:

- **HowSecureIsMyPassword.net**
- **Password Monster**
- **NordPass Strength Checker**
- **passwordmeter.com**

Task 6th: Create a Strong Password and Evaluate Its Strength

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:	43%	
Complexity:	Good	

Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	*+(n*4)*	11	+ 44
Uppercase Letters	Cond/Incr	*+((len-n)*2)*	0	0
Lowercase Letters	Cond/Incr	*+((len-n)*2)*	8	+ 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	-	2	- 2
Consecutive Uppercase Letters	Flat	*-(n*2)*	0	0
Consecutive Lowercase Letters	Flat	*-(n*2)*	7	- 14
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

Legend

Exceptional: Exceeds minimum standards. Additional bonuses are applied.
Sufficient: Meets minimum standards. Additional bonuses are applied.
Warning: Advisory against employing bad practices. Overall score is reduced.
Failure: Does not meet the minimum standards. Overall score is reduced.

Task 6th: Create a Strong Password and Evaluate Its Strength

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)*	12	+ 48
✪	Uppercase Letters	Cond/Incr	*+((len-n)*2)*	3	+ 18
✪	Lowercase Letters	Cond/Incr	*+((len-n)*2)*	3	+ 18
✪	Numbers	Cond	*+(n*4)*	3	+ 12
✪	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	-	0	0
✓	Consecutive Uppercase Letters	Flat	*-(n*2)*	0	0
✓	Consecutive Lowercase Letters	Flat	*-(n*2)*	0	0
✓	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

Legend

✪ **Exceptional:** Exceeds minimum standards. Additional bonuses are applied.
✓ **Sufficient:** Meets minimum standards. Additional bonuses are applied.
! **Warning:** Advisory against employing bad practices. Overall score is reduced.
✗ **Failure:** Does not meet the minimum standards. Overall score is reduced.

Task 6th: Create a Strong Password and Evaluate Its Strength

4 Note scores and feedback from the tool.

Password	Estimated Crack Time	Feedback
password123	< 1 second	Very weak, too common
Passw0rd	A few minutes	Better, but still guessable
P@ssw0rd!	Hours to days	Stronger due to symbol & case mix
QwErTy2025	Hours	Predictable pattern
G!9x#1zB$vK8	Billions of years	Very strong
aB3!cD5#EfGhIjKl	Practically uncrackable	Excellent – long, random, mixed

5 Identify best practices for creating strong passwords.

- **Use at least 12–16 characters**
- **Include upper & lower case, numbers, symbols**
- **Avoid dictionary words or common patterns**
- **Do not reuse passwords across accounts**
- **Consider using a password manager**
- **Enable 2-Factor Authentication (2FA) when possible**

6 Write down tips learned from the evaluation.

- **Longer passwords are significantly harder to crack.**
- **Randomness is more secure than predictable patterns.**
- **Combining unrelated words or using passphrases can be effective.**
- **Avoid personal info (birthdays, names) in passwords.**
- **Even a small change (like adding a symbol) can exponentially increase security.**

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

Attack Type	Description
Brute Force	Tries all combinations of characters until it guesses the password
Dictionary	Uses a list of common passwords and words to guess the password
Credential Stuffing	Uses stolen username/password combinations from previous breaches
Phishing	Tricks users into revealing passwords through fake websites or emails
Keylogging	Records keystrokes to steal passwords

8 Summarize how password complexity affects security.

- **Simple passwords (short, common words) are easily cracked in seconds by brute force or dictionary attacks.**
- **Complex passwords (long, random, with symbols and case variation) may take billions of years to break with current technology.**
- **Complexity = Security: The more complex and unique your password, the less likely it will be compromised.**