TASK-6

Elevate Labs Internship

Task 6 – Password Strength Evaluation

Mothe Anurag Reddy

1. Create multiple passwords with varying complexity

Password	Reason
anurag	All lowercase, common keyboard pattern, extremely easy to guess
anurag1212	Adds numbers but still predictable and commonly used
Anur@g	Mix of uppercase, lowercase, number, symbol but short in length
Anur4g@1	Increased length, good use of numbers and symbols
A1nurag@13	9 characters, high randomness, strong mix of characters
A1n4r@g@5@!@22064	16 characters, fully randomized, includes all character types

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

All passwords above are created with a variety of:

* Uppercase letters

* Lowercase letters

* Numbers

* Special characters

* Different lengths (6 to 16+ characters)

3. Test each password on password strength checker

Tools Used:

PasswordMeter

Kaspersky Password Checker

4. Note scores and feedback from the tool

Password Strength Level	**Score (%)**	**Feedback / Reason**
Very Weak	8%	All lowercase, name-based, short and guessable
Good	53%	Predictable pattern, repetition, personal name
Moderate	42%	Uppercase/special chars but too short
Strong	78%	Good mix, 8 chars, minimum security standard
Very Strong	87%	Higher randomness, mixed char types
Ultra Secure	100%	Excellent complexity, resists brute force

5. Identify best practices for creating strong passwords

* Use at least 12-16 characters

* Include uppercase, lowercase, numbers, and symbols

* Avoid using personal data like name, DOB, mobile number

* Do not use keyboard patterns (e.g., asdf, qwerty)

* Avoid common words and passwords found in breach lists

* Use password managers to generate and store complex passwords

* Enable Two-Factor Authentication (2FA)

* Use passphrases like Monkey$Climbs^OrangeTree2025

6. Tips learned from the evaluation

* Longer passwords are stronger

* Randomness matters more than symbols

* Predictable passwords are still weak

* Reusing passwords is risky

* Use tools like Bitwarden or NordPass

* 2FA adds a strong second layer

7. Common password attacks

Attack Type	**Description / Prevention**
Brute Force	Try every combo - Use complex, long passwords
Dictionary Attack	Avoid common words and personal info
Credential Stuffing	Use unique passwords for every account
Phishing	Always verify URLs, avoid unknown links
Keylogging	Use antivirus, avoid suspicious downloads

8. Password complexity affects security

Simple passwords like 'anurag' are easy to guess.

Complex passwords like 'A1n4r@g@5@!@22064' are highly secure.

Use a mix of all character types and avoid predictable patterns.

Tools show strong passwords are resistant to most attacks.