Elevate Labs Internship
Task 6 – Password Strength Evaluation

1. Create multiple passwords with varying complexity

Password	Reason
`kishan`	All lowercase, common keyboard pattern, extremely easy to guess
`kishan1212`	Adds numbers but still predictable and commonly used
`Kish@n`	Mix of uppercase, lowercase, number, symbol but short in length
`Kish4n@1`	Increased length, good use of numbers and symbols
`K1shan@13`	9 characters, high randomness, strong mix of characters
`K1sh4n@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

I tested six self-created passwords using online password strength checkers (PasswordMeter and Kaspersky Password Checker) on Kali Linux using Firefox browser. Below is a detailed table showing the strength level, score, and feedback for each:

Password	Strength Level	Score (%)	Feedback / Reason
`kishan`	Very Weak	8%	- All lowercase letters only- Name-based and very short- Easily guessable and common
`kishan1212`	Good	53%	- Includes numbers, but predictable pattern- Repetition lowers security- Still based on personal name
`Kish@n`	Moderate	42%	- Uses uppercase and special character- Still too short (only 6 characters)- Vulnerable to brute-force attacks

`Kish4n@1`	Strong	78%	- 8 characters, good mix of numbers, letters, and symbol- Better unpredictability- Satisfies minimum security standards
`K1shan@13`	Very Strong	87%	- 9 characters- Higher randomness- Strong use of mixed character types and placement
`K1sh4n@5@!@22064`	Ultra Secure	100%	- 16 characters long- Excellent complexity with numbers, uppercase, lowercase, multiple symbols- Hard to guess and resists dictionary/brute force attacks

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) for additional security
- Consider using passphrases with uncommon word combinations

6. Write down tips learned from the evaluation

From my testing and research:

- Longer passwords are significantly stronger

- Randomness matters more than just using special characters
- Short but complex passwords can still be weak due to predictability
- Reusing passwords across sites is a major security risk
- Passphrases like `Monkey$Climbs^OrangeTree2025` are both memorable and secure
- Tools like Bitwarden or NordPass help manage unique passwords for every site
- 2FA adds an essential layer of defense beyond just passwords

7. Research common password attacks

Attack Type	Description	Prevention
Brute Force	Tries every possible combination	Use long, complex passwords
Dictionary Attack	Uses list of common passwords or words	Avoid dictionary words and personal info
Credential Stuffing	Uses leaked credentials from data breaches to access other accounts	Use unique passwords for every account
Phishing	Tricks users into entering passwords on fake sites or through fake messages	Always verify URLs, don't click unknown links
Keylogging	Malware captures keystrokes to steal passwords	Use updated antivirus, avoid suspicious downloads

8. Summarize how password complexity affects security

Password strength greatly depends on length and character complexity. Simple passwords like `kishan` are easy to guess, while longer, more complex ones like `K1sh4n@5@!@22064` are highly secure. By using a mix of uppercase, lowercase, numbers, and special characters, and avoiding predictable patterns, the strength increases significantly. Tools like PasswordMeter and Kaspersky Password Checker showed that strong, random passwords score much higher and are far more resistant to brute-force and dictionary attacks. Strong passwords are essential for basic cybersecurity protection.