Task 6: Create a Strong Password and Evaluate Its Strength

1. Objective

The objective of this task is to understand what makes a password strong, create multiple sample passwords, test them using online password strength checkers, analyze the results, and document best practices for creating secure passwords.

2. Tools Used

Online Password Strength Checker

- passwordmeter.com
- Kaspersky Password Checker
- Bitwarden Strength Test

3. Methodology

- Created five passwords with varying complexity (weak → strong).
- Tested each password using online strength checkers.
- Noted the score, strength level, and feedback.
- Analyzed how length, character variety, and patterns affect strength.
- Summarized best practices and attack vulnerabilities.

4.Passwords Created and Tested

1.Password 1: nandu123

Length: 8 characters

Character Set: Lowercase + numbers

Strength Result: Weak

Feedback:

- Too short

- Contains predictable pattern (“name + numbers”)

- Easily crackable by brute force or dictionary attack

Estimated Crack Time: Seconds

2. Password 2: Password@1

Length: 10

Character Set: Uppercase, lowercase, number, symbol

Strength Result: Medium

Feedback:

- Contains dictionary word “Password”
- Commonly used phrase
- Needs more randomness

Estimated Crack Time: Hours

3. Password 3: Cr!m3Lab2025

Length: 13

Character Set: Mixed case, numbers, symbols

Strength Result: Strong

Feedback:

- Good mix of character types
- Avoid using meaningful words (e.g., “Lab”)
- Still moderately predictable

Estimated Crack Time: Months

4.Password 4: T&9k$R1@Pqx!

Length: 12

Character Set: Highly random mix

Strength Result: Very Strong

Feedback:

- High complexity
- No dictionary words
- Hard to memorize without manager

Estimated Crack Time: Centuries

5.Password 5 : Silent-Lions-Dance-At-Midnight#29

Length: 31 characters

Character Set: Words + symbols + numbers

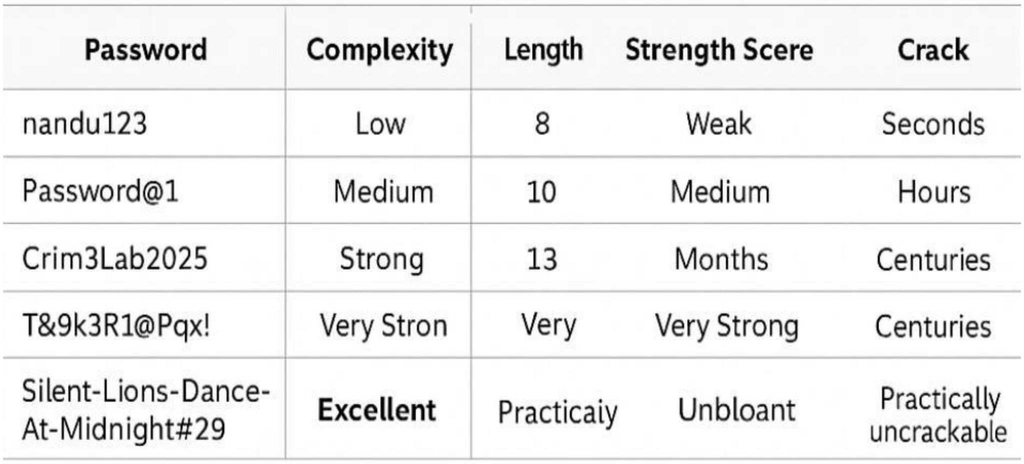
Strength Result: Excellent

Feedback:

- Long passphrase = extremely strong
- Easy to remember
- Very hard for brute-force attacks

Estimated Crack Time: Practically uncrackable

5. Strength Comparison Table



Password	Complexity	Length	Strength Scere	Crack
nandu123	Low	8	Weak	Seconds
Password@1	Medium	10	Medium	Hours
Crim3Lab2025	Strong	13	Months	Centuries
T&9k3R1@Pqx!	Very Stron	Very	Very Strong	Centuries
Silent-Lions-Dance-At-Midnight#29	**Excellent**	Practicaiy	Unbloant	Practically uncrackable

6.Best Practices for Creating Strong Passwords

-Use at least 12–16 characters.

- Combine uppercase, lowercase, numbers, symbols.
- Avoid dictionary words, names, birth dates, or predictable patterns.
- Use passphrases for better memorability.
- Do not reuse passwords across different platforms.
- Change passwords if suspicious activity is detected.
- Enable Multi-Factor Authentication (MFA) for extra security.
- Use password managers to store strong, complex passwords.

7. Research on Common Password Attacks

1. **Brute Force Attack**

- Automated guessing of all possible combinations.
- Short or simple passwords are cracked quickly.

2. **Dictionary Attack**

- Uses pre-compiled lists of common passwords and words.
- Passwords containing names, dictionary words, or patterns are vulnerable.

3. **Credential Stuffing**

Attackers use leaked password databases to attempt logins across multiple sites.

4. **Social Engineering**

Tricking a user to reveal passwords through phishing or manipulation.

8. Key Learnings

- Password length is a major factor in security.
- Complexity increases resistance to cracking.
- Passphrases offer strong protection while staying memorable.
- Password managers help maintain unique, strong passwords for every account.
- MFA acts as a second defensive layer even if the password is compromised.

9. Conclusion

This task helped in understanding the importance of password strength, complexity, and unpredictability. Testing multiple passwords demonstrated how small changes in structure significantly affect crack time and overall security. Adopting strong password habits and using MFA greatly enhances cyber safety and.