**TASK-6**

**Create a Strong Password and Evaluate Its Strength**

**🔹 Step 1: Create Password Samples**

We’ll make passwords with increasing complexity:

1. 123456789→ weak (common + only digits)
2. Password1234 → weak (uppercase + lowercase + digits)
3. MyPassword@1234! → weak (uppercase + lowercase + digits + symbols but very common)
4. Gracy@1605 → weak (uppercase + lowercase + digits)
5. PAssw0rdISP@$$w0→ strong (longer, mix of types, less predictable)
6. #India@is@my@country!! → strong (longer, mix of types, less predictable)
7. 4ryw2wgW4C@j@rYq → very strong (long, random, mix of all character sets)

**🔹 Step 2: Test with Password Strength Tool**

Example tool: **passwordmeter.com**

The below are the screenshots of test results of the password strength test:

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer screen

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.A screenshot of a computer screen

AI-generated content may be incorrect.A screenshot of a computer

AI-generated content may be incorrect.

**🔹 Step 3: Best Practices for Strong Passwords**

From the test, we learn:

* Use **at least 12–16 characters**.
* Mix **uppercase, lowercase, numbers, and symbols**.
* Avoid dictionary words or personal info (like names, DOB).
* Longer + more random = harder to crack.
* A **passphrase** can also be very strong and easier to remember.

**🔹 Step 4 : Common Password Attacks**

1. **Brute Force Attack**
   * The attacker tries every possible combination of characters until the correct password is found.
   * Speed depends on password length and complexity. Short or simple passwords can be cracked in seconds or minutes.
   * Example: A 6-character lowercase password can be cracked in less than a minute, while a 12+ character complex password can take centuries.
2. **Dictionary Attack**
   * Uses a precompiled list of common passwords and words.
   * Targets predictable passwords and common phrases (e.g., 123456, password, qwerty, letmein).
   * More efficient than brute force because it focuses on likely candidates rather than all possibilities.
3. **Credential Stuffing**
   * Hackers use leaked username/password combinations from one site to try logging into other sites.
   * Exploits the habit of password reuse.
   * Can be prevented by using unique passwords for every account and enabling multi-factor authentication (MFA).
4. **Phishing Attacks**
   * Tricking users into giving their passwords via fake websites, emails, or messages.
   * Even strong passwords can be stolen if the user is tricked.
   * Defense: Be cautious of links, verify URLs, and enable MFA.
5. **Keylogging**
   * Malware records keystrokes and sends them to an attacker.
   * Can capture passwords regardless of complexity.
   * Defense: Use antivirus software, keep systems updated, and avoid untrusted downloads.
6. **Rainbow Table Attack**
   * Uses precomputed tables of hashed passwords to crack password hashes faster.
   * Strong passwords with salt values make rainbow table attacks ineffective.
   * Defense: Use password managers and hashed/salted password storage.
7. **Social Engineering**
   * Manipulating people into revealing passwords.
   * Examples: impersonating IT support, asking for password resets, or exploiting trust.
   * Defense: Awareness training, never share passwords, and verify requests.

**🔹 Conclusion**

Password complexity increases the time and resources required for attackers to crack a password. Longer passwords with mixed character types and randomness significantly improve security, reducing vulnerability to brute force and dictionary attacks while protecting sensitive data from common hacking methods. Strong, unique passwords combined with good cyber hygiene and additional security measures like multi-factor authentication (MFA) are essential for protecting digital accounts and preventing breaches.