# Cyber Security Internship – Task 6

# Create a Strong Password and Evaluate Its Strength

---

## Objective

Understand the factors that contribute to a strong password and test various passwords using online password strength checkers.

---

## Tools Used

- Online password strength checker: passwordmeter.com (or any free online tool)

---

## Step-by-Step Process

### 1. Create Multiple Passwords with Varying Complexity

- Start by creating simple passwords (e.g., "password123").
- Gradually increase complexity by adding:
  - Uppercase letters (e.g., "Password123")
  - Numbers (e.g., "Password1234")
  - Special characters (e.g., "Password@123")
  - Increasing length (e.g., "Passw0rd@2025!")
- Include passphrases with multiple words and symbols.

### 2. Test Each Password Using a Password Strength Checker

- Visit passwordmeter.com or another tool.
- Enter each password and review the score and feedback.
- Note down the password, the strength score/grade, and suggestions given.

### 3. Record Scores and Feedback

- Document the strength, weaknesses, and areas to improve for each password.
- Compare how different elements (length, symbols, numbers, lowercase/uppercase) affect strength.

### 4. Identify Best Practices for Strong Passwords

- Use a mix of uppercase, lowercase, numbers, and special characters.
- Use longer passwords (12+ characters).
- Avoid common words, common substitutions, or repeated characters.
- Consider using passphrases (series of random words).

**5. Research Common Password Attacks**

- Understand methods like:
  - Brute Force Attack: Trying every possible combination until the correct password is found.
  - Dictionary Attack: Using lists of common words and passwords to guess.
- Reflect on how password complexity mitigates these attacks.

**6. Write Tips Learned from the Evaluation**

- Emphasize length and complexity are key.
- Strong passwords are less vulnerable to guessing or automated attacks.
- Using password managers helps generate and safely store complex passwords.

**7. Summarize How Password Complexity Affects Security**

- Explain how combination of length, character variety, and unpredictability improves security.
- Show how weak passwords fail checks quickly and are vulnerable.

---

**Passwords and Strength Evaluation Table**

| Password | Strength (Score/Grade) | Notes |
|---|---|---|
| password123 | Weak | Common word and numbers, very weak |
| Password123 | Fair | Added uppercase, still predictable |
| Password@123 | Good | Added special character improves strength |
| P@ssw0rd2025! | Strong | Mix of cases, symbols, numbers, and length |
| mydog$and$cat$123 | Very Strong | Passphrase style with symbols and numbers |

---

**Conclusion**

Creating strong passwords by emphasizing length, complexity, and unpredictability significantly improves security against brute-force and dictionary attacks. Using password strength checkers aids in evaluating and improving password quality.