Task 6 – Strong Password Creation & Evaluation

Date: 21-11-2025
Subject: Cyber Security Internship – Task Report

Objective:
Learn how to create strong passwords, evaluate them using tools, and understand password security best practices.

Tools Used:
1. password.kaspersky.com
2. passwordmeter.com
3. security.org/how-secure-is-my-password

Steps Performed:
1. Created five different passwords:
   a. “hello123”
   b. “Hello@123”
   c. “Rk@2025#Secure”
   d. “LongPassPhraseIsBetter@2025”
   e. “Pa$$w0rD!%Secure”

2. Tested each password using online strength checkers.
3. Noted:
   - Strength score
   - Crack time
   - Security suggestions provided
4. Researched how brute force and dictionary attacks work.
5. Learned how password length and randomness improve protection.

Results Table:

Password | Strength | Crack Time | Remarks
hello123 | Weak | Few seconds | Common password
Hello@123 | Medium | Hours | Needs more length
Rk@2025#Secure | Strong | Millions of years | Good complexity
LongPassPhraseIsBetter@2025 | Very Strong | Impossible | Best as passphrase

What Makes a Password Strong:
- Minimum 12–16 characters
- Use uppercase, lowercase, numbers, symbols
- Avoid patterns (1234, abcd)
- Avoid date of birth, names, phone number
- Use MFA for all accounts

Types of Attacks:
- Brute Force Attack: Tries all combinations
- Dictionary Attack: Uses common passwords/words

- Phishing: Tricks user to enter password
- Keylogger: Captures keystrokes

Conclusion:
A longer passphrase is the most secure option. Password managers and MFA help in maintaining safety of accounts.