Password Strength Evaluation and Security Report

Name: Hemanth.A.S

Date: June 03, 2025

Tool Used: Online password strength checker (e.g., passwordmeter.com)

Objective: Understand what makes a password strong and evaluate password strength using online tools.

Steps Taken

1. Created multiple passwords with varying complexity.
2. Used combinations of uppercase, lowercase, numbers, symbols, and different lengths.
3. Tested each password using the passwordmeter.com checker.
4. Recorded the scores and feedback provided by the tool.
5. Identified the best practices for creating strong and secure passwords.
6. Noted down helpful tips based on the feedback from the tool.
7. Researched common types of password attacks such as brute force and dictionary attacks.
8. Summarized how password complexity plays a crucial role in overall password security.

Summary of Findings

Passwords Tested and Scores (from passwordmeter.com):

1. Password: "hello123" – Score: 35%
   - Feedback: Too short, lacks complexity, easily guessable.

2. Password: "Hello@2024" – Score: 72%
   - Feedback: Better complexity with uppercase, lowercase, and special character. Moderate strength.

3. Password: "G@l@xyT!m3#29" – Score: 92%
   - Feedback: Excellent strength, long and complex. Resistant to brute-force attacks.

Best Practices Identified:
- Use a mix of character types (uppercase, lowercase, numbers, symbols).
- Aim for longer passwords (at least 12–16 characters).
- Avoid dictionary words, personal info, and predictable patterns.

- Consider using a password manager for generating and storing strong passwords.

Common Password Attacks Researched:
- Brute Force: Tries all possible combinations; long and complex passwords help prevent success.
- Dictionary Attack: Uses common words; unique character combinations defend against this.

Conclusion:
Password complexity significantly enhances security. Strong passwords are essential to resist automated and manual attacks. Adopting best practices ensures better protection of accounts and personal data.