CYBER SECURITY INTERNSHIP

TASK 6 – PASSWORD STRENGTH EVALUATION REPORT

Submitted by: Muthukumaran R

---

1) AIM / OBJECTIVE

To understand what makes a password strong by creating multiple passwords with varying complexity and evaluating their strength using an online password strength checker.

2) TOOL USED

Website: https://passwordmeter.com

3) METHODOLOGY / PROCEDURE

• Created five passwords with different complexity levels (weak → strong)

• Checked each password in the passwordmeter.com tool

• Noted strength rating, estimated cracking time, and feedback

• Compared results and extracted best practices

4) OBSERVATION AND RESULTS

Password 1: muthu123

• Strength: Weak (< 1 second to crack)

• Reason: Very short, predictable, common pattern

[Screenshot Placeholder: Insert screenshot of result here]

Password 2: Muthu@2003

• Strength: Medium

• Reason: Mixed characters but uses name and year (predictable)

[Screenshot Placeholder]

Password 3: Muthu@2003!

• Strength: Strong

• Reason: Better complexity with extra special character but still pattern-based

[Screenshot Placeholder]

Password 4: MuthuKumaran@2003#

• Strength: Strong / Very Strong

• Reason: Long length improves security but contains personal info

[Screenshot Placeholder]

Password 5: My$ecureP@ssw0rd!2025

• Strength: Very Strong

• Reason: Long, random, mixed charset, not based on personal identity

[Screenshot Placeholder]

5) ANALYSIS / DISCUSSION

From the experiment, it is clear that:

• Length is a major factor in resisting brute-force attacks

• Removing personal info prevents targeted and dictionary attacks

• Special characters + numbers + upper/lowercase increases entropy

• Passphrases or random strings are more secure than names + years

6) COMMON PASSWORD ATTACKS

- Brute Force Attack – Tries all combinations until correct
- Dictionary Attack – Uses known password wordlists
- Credential Stuffing – Uses leaked passwords from breaches
- Phishing Attack – Tricks user to reveal password

7) BEST PRACTICES

- Use 12–16+ characters minimum
- Avoid names, years, dictionary words
- Use a mix of uppercase, lowercase, numbers, and symbols
- Do not reuse passwords for different accounts
- Enable Multi-Factor Authentication (MFA)
- Use password managers for strong unique passwords

8) CONCLUSION

Password strength depends on complexity, unpredictability, and length.
Strong, unique passwords combined with MFA provide effective protection against brute-force, dictionary, and credential-based attacks.

9) REFERENCES

- https://passwordmeter.com
- https://owasp.org