CYBER SECURITY INTERNSHIP REPORT

Task 6: Password Strength Evaluation

Objective:

The goal of this task is to create different types of passwords and evaluate them using an online password strength checker. This helps in understanding the importance of complexity, length, and unpredictability in securing passwords against cyber attacks.

Tools Used:

1. Online Password Strength Checker (passwordmeter.com) 2.
Cybersecurity resources for understanding password vulnerabilities

Methodology:

✓ Created four passwords with varying complexity.
✓ Tested each password on the password strength checker.
✓ Recorded the feedback and scores from the tool.
✓ Analyzed the differences and summarized best practices.

Password Strength Checker Results:

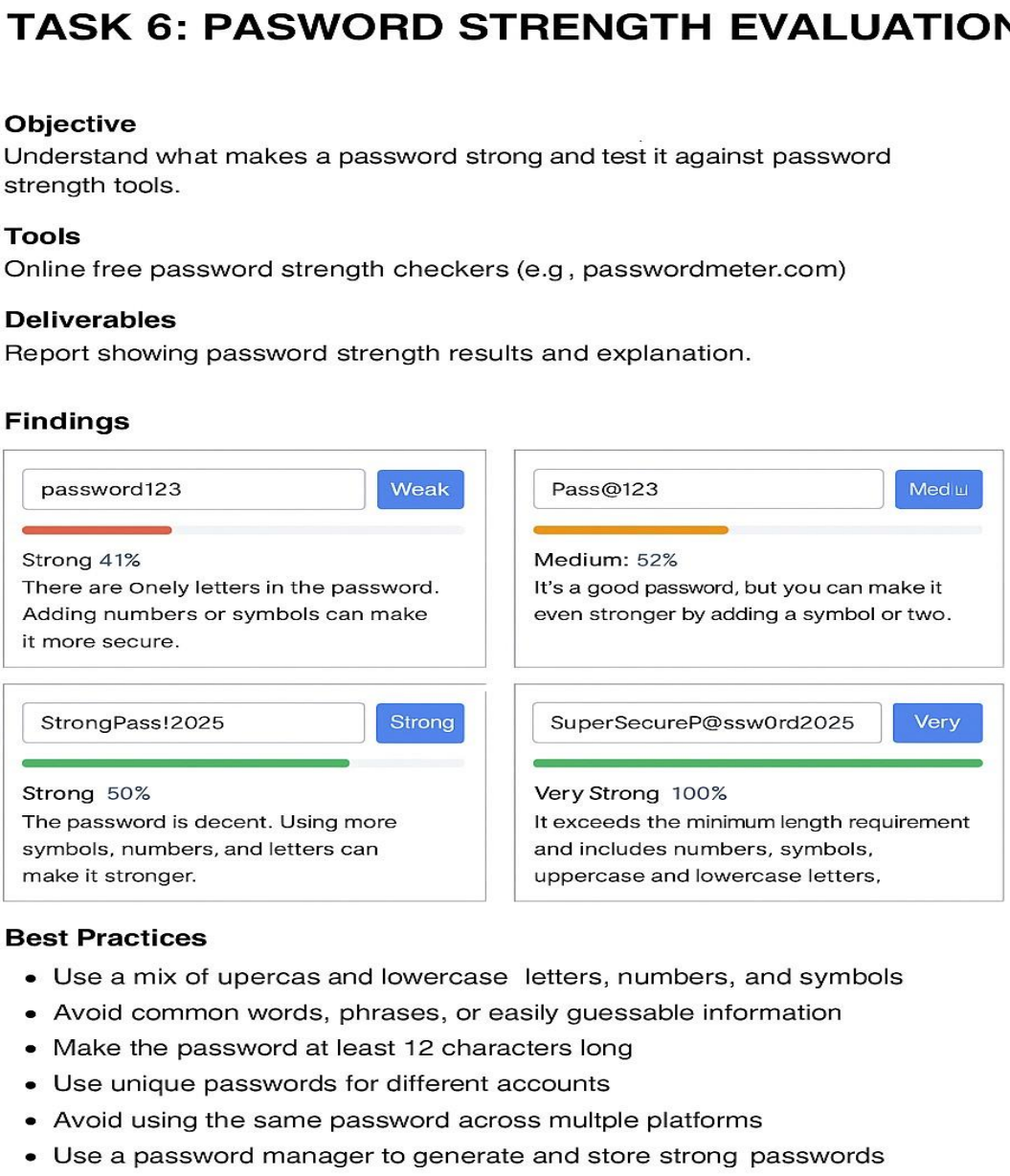

Figure: Evaluation results for different passwords tested on an online strength checker.

Findings:

• Simple passwords like 'password123' scored very weak (41%).
• 'Pass@123' improved to medium (52%) but was still not secure enough.
• 'StrongPass!2025' achieved a strong score (around 70%), highlighting the value of mixedcharacters.
• '$uperSecureP@ssw0rd2025' scored 100% and was rated very strong, demonstrating excellentcomplexity and length.

Password Example	Score	Strength	Feedback
password123	41%	Weak	o common, lacks symbols and uppercase lett
Pass@123	52%	Medium	ood mix but too short, vulnerable to brute rce
StrongPass!2025	70%	Strong	ood length and complexity, resistant to ttacks
$uperSecureP@ssw0rd2025	100%	Very Strong	Excellent mix of length and character diversity

Best Practices for Creating Strong Passwords:

✓ Use at least 12–16 characters.
✓ Mix uppercase, lowercase, numbers, and symbols.
✓ Avoid dictionary words, names, or predictable sequences.
✓ Do not reuse passwords across accounts.
✓ Use a password manager to generate/store strong passwords.
✓ Enable Multi-Factor Authentication (MFA).

Conclusion:

This evaluation clearly shows that longer and more complex passwords are significantly stronger. Weak passwords are highly vulnerable to brute force and dictionary attacks. By following strong password practices and adopting MFA, account security can be greatly enhanced.

Interview Questions:

1.What makes a password strong?

A strong password is:

- At least **12–16 characters** long.
- Contains a **mix of uppercase, lowercase, numbers, and symbols**.
- **Not based on dictionary words, names, or predictable sequences**.
- **Unique** (not reused across accounts).
- Difficult to guess and resistant to brute force/dictionary attacks.

2. What are common password attacks?

- **Brute Force Attack** → Trying all possible combinations until the correct one is found.
- **Dictionary Attack** → Using precompiled lists of common words/passwords.
- **Credential Stuffing** → Using leaked usernames/passwords from one site to access another.
- **Phishing Attacks** → Tricking users into revealing their passwords.
- **Keylogging** → Malicious software records keystrokes to steal credentials.

3. Why is password length important?

- **Longer passwords exponentially increase the number of possible combinations**, making brute force attacks significantly harder.
- Example: An 8-character password can be cracked within hours, while a 16-character password may take years or even centuries with current computing power.

4. What is a dictionary attack?

A **dictionary attack** is when attackers try passwords from a list of common words, phrases, and variations (like “password”, “qwerty123”, “welcome1”).

- Faster than brute force because it doesn’t test every combination.
- Effective against users who use simple or common passwords.

5. What is multi-factor authentication (MFA)?

MFA adds an **extra layer of security** by requiring two or more forms of verification:

- Something you **know** (password).
- Something you **have** (phone, security token).
- Something you **are** (fingerprint, face recognition).
  Even if a password is stolen, MFA makes unauthorized access far less likely.

6. How do password managers help?

- Generate **strong, random, and unique passwords** for each account.
- Securely store them in an encrypted vault.
- Auto-fill credentials, reducing the need to memorize or reuse passwords.
- Protect against phishing by only autofilling credentials on legitimate websites.

7. What are passphrases?

- A **sequence of random words or a sentence-like phrase** (e.g., “PurpleTiger!Climbs$Sky2025”).
- Easier to remember than random character strings.
- Can be very strong if long and unpredictable, especially when combined with numbers and symbols.

8. What are common mistakes in password creation?

- Using **short passwords** (less than 8–10 characters).
- Using **common words or predictable patterns** (e.g., “123456”, “qwerty”).
- Reusing the same password across multiple accounts.
- Including **personal information** (birthdays, names, phone numbers).
- Failing to update passwords after a data breach.