Task 6: Create a Strong Password and Evaluate Its Strength

Task Deliverable

Prepared By: Mumuksha Kashyap

Date: 13/08/2025

Objective

The objective of this task is to understand what makes a password strong, evaluate different password complexities using online password strength checkers, and summarize best practices for creating secure passwords.

Tools Used

- passwordmeter.com - howsecureismypassword.net

Methodology

1. Created multiple passwords with varying complexity.
2. Tested each password on online password strength tools.
3. Recorded scores, estimated crack time, and feedback.
4. Identified best practices for creating strong passwords.
5. Researched common password attacks and their prevention.

Password Testing Results

Password	Score (%)	Estimated Crack Time	Feedback
sunny123	22%	Instant	Too short, common word
Sunny@2025	58%	4 hours	Add more length & symbols
S@feTyNet_99	84%	14 years	Strong password, could be longer
W@terM!l0n_#786	95%	340 centuries	Excellent – good mix of characters
8u#RzT!cQp2Lx$	100%	Trillions of years	Very strong – random characters

Best Practices for Creating Strong Passwords

1. Use at least 12–16 characters.
2. Include uppercase, lowercase, numbers, and symbols.
3. Avoid dictionary words or common phrases.
4. Use random combinations instead of predictable patterns.
5. Never reuse passwords across accounts.
6. Consider using a passphrase (e.g., Mango!River$Sky88).
7. Use a password manager for safe storage.

Common Password Attacks & Prevention

- **Brute Force Attack:** Trying all combinations until the correct one is found.
  - Prevention: Long and complex passwords.
- **Dictionary Attack:** Using lists of common words and variations.
  - Prevention: Avoid real words or predictable substitutions.
- **Phishing:** Tricking users into revealing their password.
  - Prevention: Verify sites and avoid clicking suspicious links.

Conclusion

Password complexity directly impacts security. Weak passwords can be guessed in seconds, while strong 16+ character passwords with random characters can take billions of years to crack, making them far more secure.