Task 6 : Create a Strong Password and Evaluate Its Strength

Objective: Understand what makes a password strong and test it against password strength tools.
Tools: Online free password strength checkers (e.g., passwordmeter.com).
Deliverables: Report showing password strength results and explanation.

Objective:

Understand how password complexity impacts security and document findings using strength-checking tools.

🔧 Tools Needed:

- Free online password strength checkers:
  - https://www.passwordmeter.com/
  - https://howsecureismypassword.net/

📝 Step-by-Step Instructions:

🔹 1. Create Sample Passwords

Generate a set of 6–10 passwords with different characteristics:

Password	Type
apple123	Simple (lowercase + digits)
Apple123	Mixed case + digits
Apple@123	+ symbol
A1@pple2025!	Strong + long
qwerty	Weak/common
P@$$w0rD!	Complex but guessable

🔹 2. Test Each Password

- Open the websites mentioned above one by one.
- Input each password and note:
  - Strength rating or score (e.g., “Weak”, “Strong”, 70%)
  - Estimated crack time (e.g., “10 years” or “Instantly”)
  - Any feedback/tips the site gives

Create a table like this:

Password	Strength	Crack Time	Feedback
apple123	Weak	Instant	Too short, no symbols
Apple123	Medium	Few seconds	Add symbol
Apple@123	Strong	2 days	Use more characters
A1@pple2025!	Very Strong	100+ years	Excellent complexity
qwerty	Very Weak	Instantly	Common password
P@$$w0rD!	Medium	Minutes	Guessable pattern

🔹 3. Analyze What Makes a Password Strong

From the tools and results:

- Length: Longer = stronger
- Character diversity:
  - Mix of uppercase, lowercase, numbers, and symbols
- Avoid:
  - Common words (e.g., qwerty, password)
  - Patterns or substitutions (e.g., P@ssw0rd is still guessable)

🔹 4. Document Best Practices

Use your test results to define good password rules:

✅ Use at least 12–16 characters
✅ Include uppercase, lowercase, digits, and symbols
✅ Avoid dictionary words, names, dates
✅ Don't reuse passwords
✅ Use a password manager for unique passwords

🔹 5. Research Password Attack Techniques

Understand how hackers try to crack passwords:

- Brute Force: Tries every combination; weak passwords fall quickly.
- Dictionary Attack: Uses a list of common passwords and words.
- Credential Stuffing: Uses leaked passwords on other sites.

- Rainbow Tables: Precomputed hash maps of passwords.

📝 6. Write Your Report (Example Format)

Password Strength Report

Date: July 2, 2025

Tools Used:

- passwordmeter.com

- howsecureismypassword.net

- security.org password tester

Tested Passwords & Results:

---

1. apple123 – Weak – Instantly crackable

2. Apple123 – Medium – Cracked in seconds

3. Apple@123 – Strong – Cracked in days

4. A1@pple2025! – Very Strong – 100+ years

5. qwerty – Very Weak – Instantly

6. P@$$w0rD! – Medium – Minutes

🧠 Lessons Learned:

- Length improves security.

- Symbols and mixed cases help.

- Common passwords are still weak, even with substitutions.

- Avoid real words or names.

⚔️ Common Attacks:

- Brute force and dictionary attacks are fast on short/simple passwords.

- Using common patterns (e.g., "Password123") is very risky.

✅ Tips for Creating Strong Passwords:

- Minimum 12 characters
- Use a combination of: UPPERCASE + lowercase + numbers + symbols
- Don’t use the same password on different sites
- Consider using a passphrase or password manager

Conclusion:

Password complexity and randomness significantly reduce vulnerability to password cracking tools and a