# Cyber Security Internship

**Task 6**

**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.

**1.Create multiple passwords with varying complexity.**

Create at least 5 passwords of different complexity levels:

1. apple123 – Simple, lowercase + digits
2. Apple@123 – Medium complexity, mixed case + symbol
3. A!pL3#9xT&z – High complexity, mixed characters
4. P@$$w0rD2025! – Obfuscated common word + numbers/symbols
5. CorrectHorseBatteryStaple – Long passphrase (very strong)

**2.Use uppercase, lowercase, numbers, symbols, and length variations.**

| Password Example | Complexity Level | Composition |
| --- | --- | --- |
| apple123 | Low | Lowercase + numbers |
| Apple@123 | Medium | Uppercase + lowercase + numbers + symbol |
| A!pL3#9xT&z | High | Mixed case + multiple symbols + numbers |
| P@$$w0rD2025! | High | Obfuscated letters + symbols + numbers |
| CorrectHorseBatteryStaple | Very High | Long phrase with capitalized words (passphrase) |

**3.Test each password on password strength checker.**

Used a online tool: “Security.org” Password Checker

Copy paste or type the password in the search box and it will give the details like how weak or strong your password, How much time it will take for an attacker to crack your password, etc…

**4.Note scores and feedback from the tool.**

1. apple123: It would take a computer about 1 day to crack your password.
2. Apple@123: It would take a computer about 3 weeks to crack your password.
3. A!pL3#9xT&z: It would take a computer about 4 hundred years to crack your password.
4. P@$$w0rD2025!: It would take a computer about 2 million years to crack your password.
5. CorrectHorseBatteryStaple: It would take a computer about 6 septillion years to crack your password.

**5.Identify best practices for creating strong passwords.**

From testing, I learn:

* Use 12+ characters
* Mix upper/lowercase, numbers, and symbols
* Avoid dictionary words or obvious patterns
* Use unique passwords for every site
* Long passphrases can be secure and memorable

**6.Write down tips learned from the evaluation.**

**Strong Password Tips:**

* Combine randomness with memorability: T!mB3r\*Sun$72
* Use a password manager (e.g., Bitwarden, 1Password)
* Don’t use personal info (birthdays, names)
* Don’t repeat passwords on different sites
* Add random words or symbols to increase strength

**7.Research common password attacks (brute force, dictionary).**

Some of the common password attacks are:

* BruteForce – Tries every combo (slow, but works on short/simple passwords)
* Dictionary Attack – Uses common passwords/words to guess
* Credential Stuffing – Reuses stolen passwords on many sites
* Phishing – Tricks users into giving passwords
* Keylogging – Malware records what you type

**8.Summarize how password complexity affects security**

* Complex passwords take longer & harder to crack — strong defense against brute-force attacks or dictionary attacks.
* Adding length + randomness makes them significantly safer.
* Passphrases are more secure and easier to remember than random strings.
* Password strength matters most against automated and offline attacks.
* Complexity reduces predictability, **thwarting automated attacks**.
* Security relies not just on complexity but also on **user behavior**, like avoiding reuse and storing credentials safely.