**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

**1. Introduction**

Passwords are the first line of defene in cybersecurity. Strong passwords help protect sensitive data from unauthorized access. In this task, we created and tested multiple passwords using an online password strength checker and documented the results to learn what makes a password secure.

**🔹 Step 1: Create Multiple Passwords**

Create at least 5–6 passwords with **varying complexity**.

Examples:

* Simple: abc123
* Medium: Abc123
* Strong: P@ssw0rd123
* Very Strong: Y#78kT!rmQp9
* Passphrase: Green!Horse2025!Runs

**🔹 Step 2: Use Character Variety**

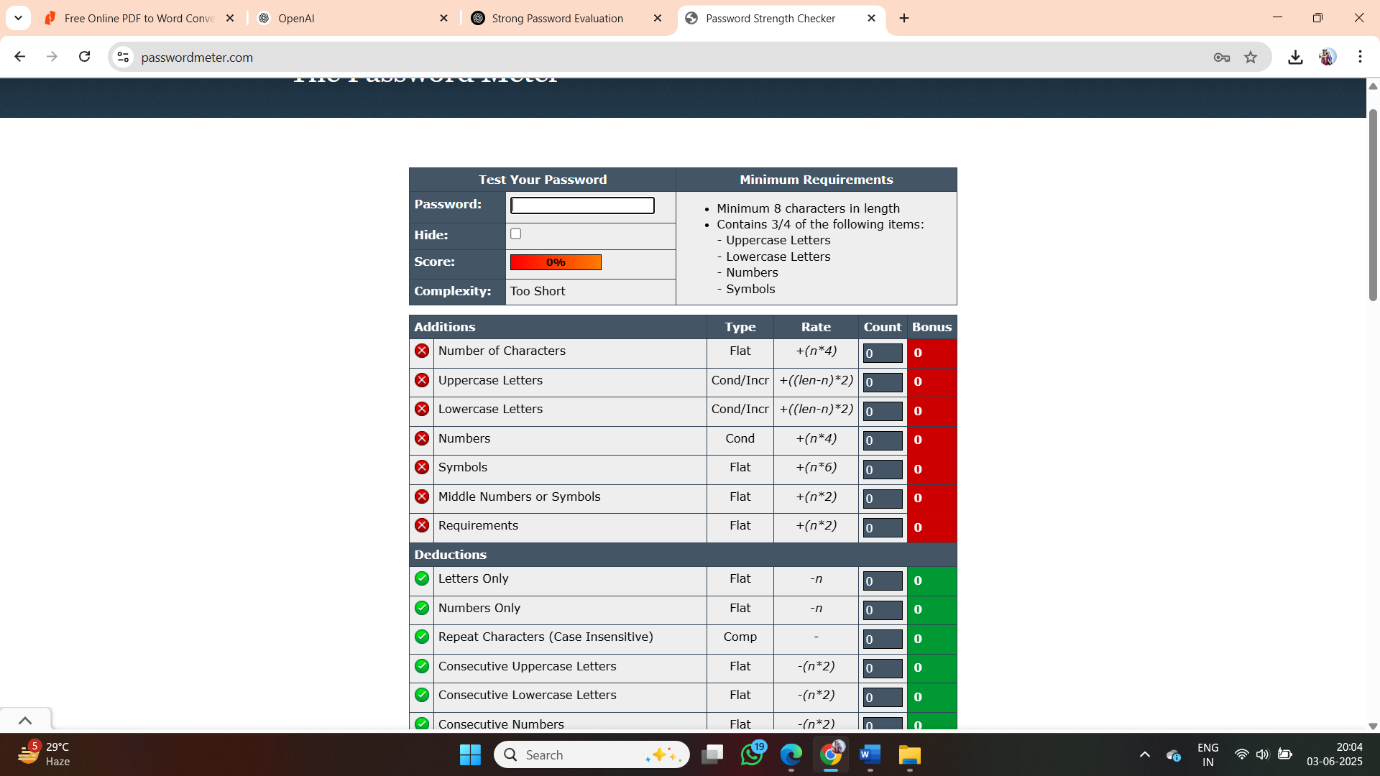
When creating passwords, vary the use of:

* **Uppercase letters** (A–Z)
* **Lowercase letters** (a–z)
* **Numbers** (0–9)
* **Symbols** (! @ # $ % ^ & \* etc.)
* **Length** (short <8, medium 8–12, strong >12)

**🔹 Step 3: Test Passwords Using Strength Checker**

Use a free tool like:

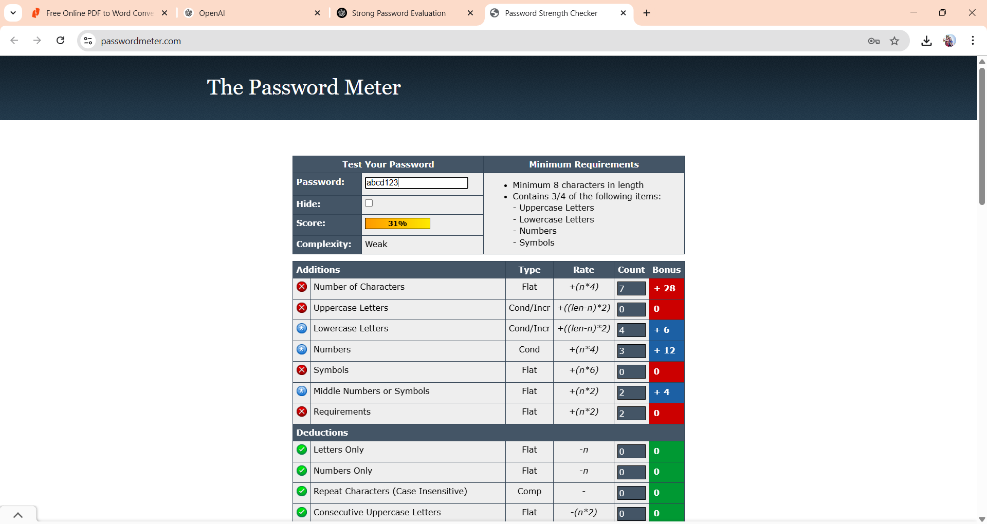
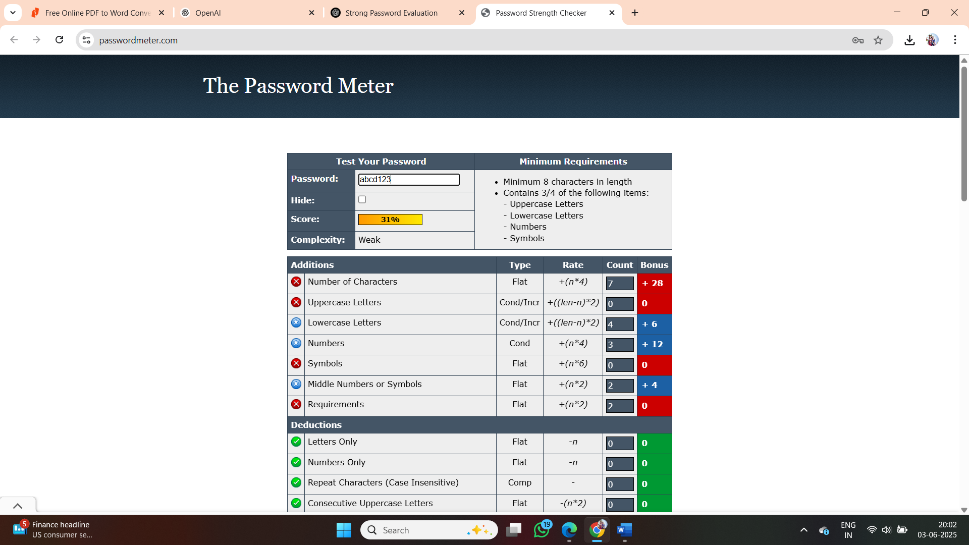
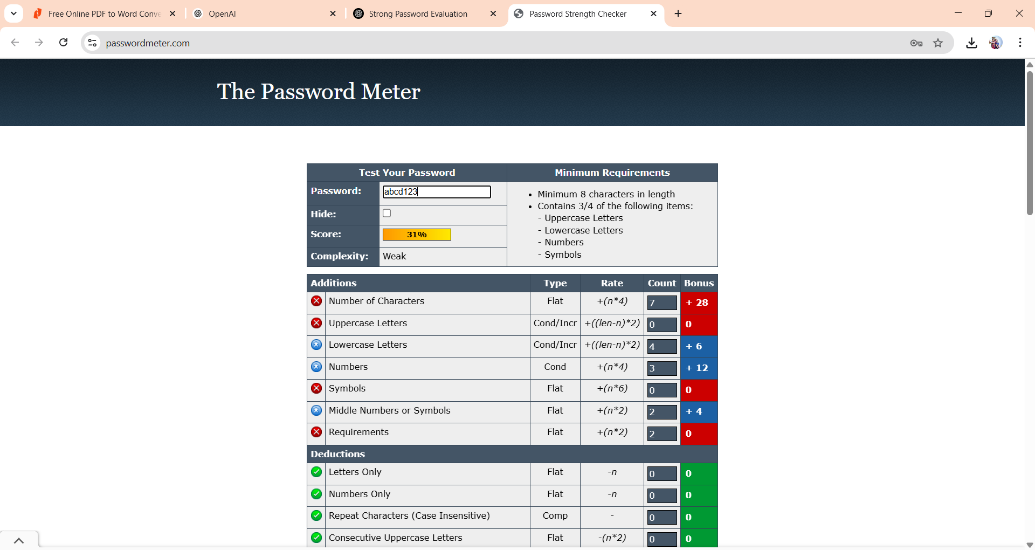
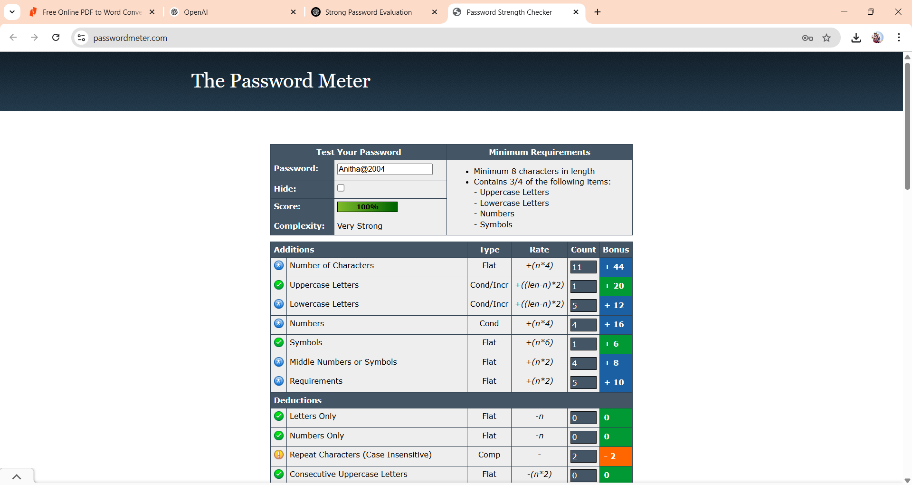
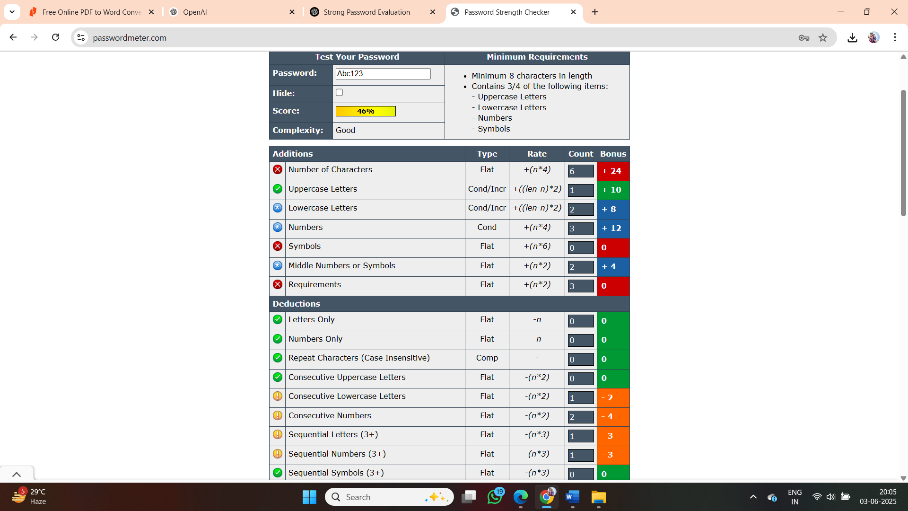
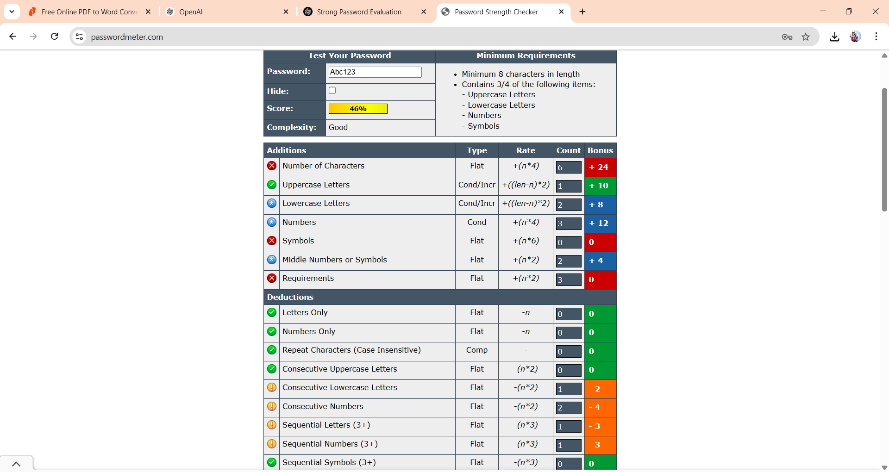
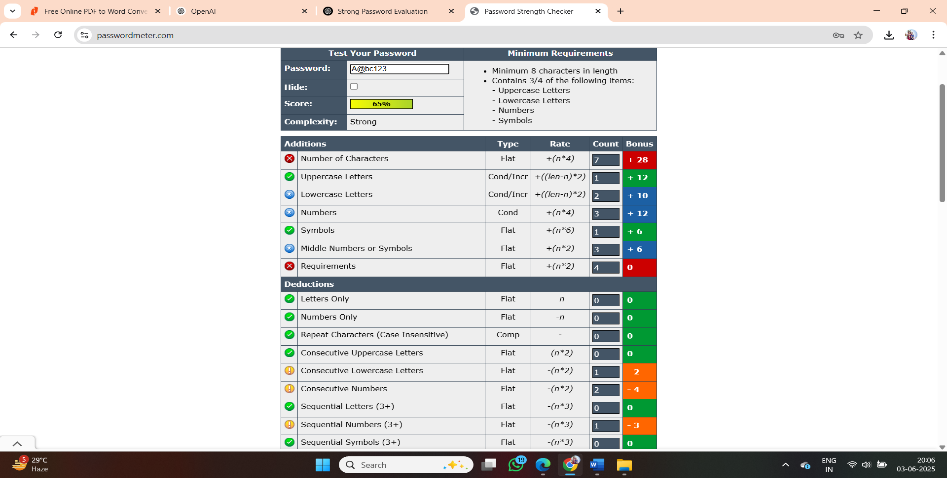
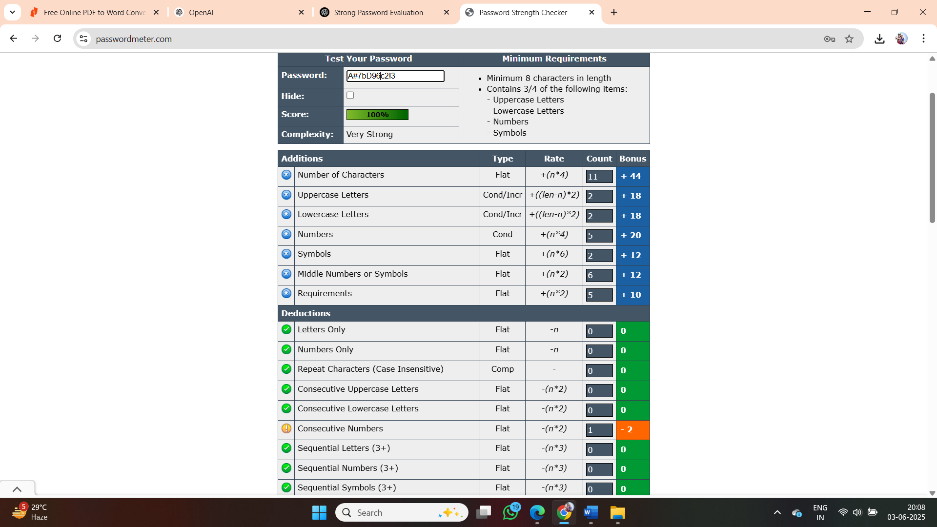
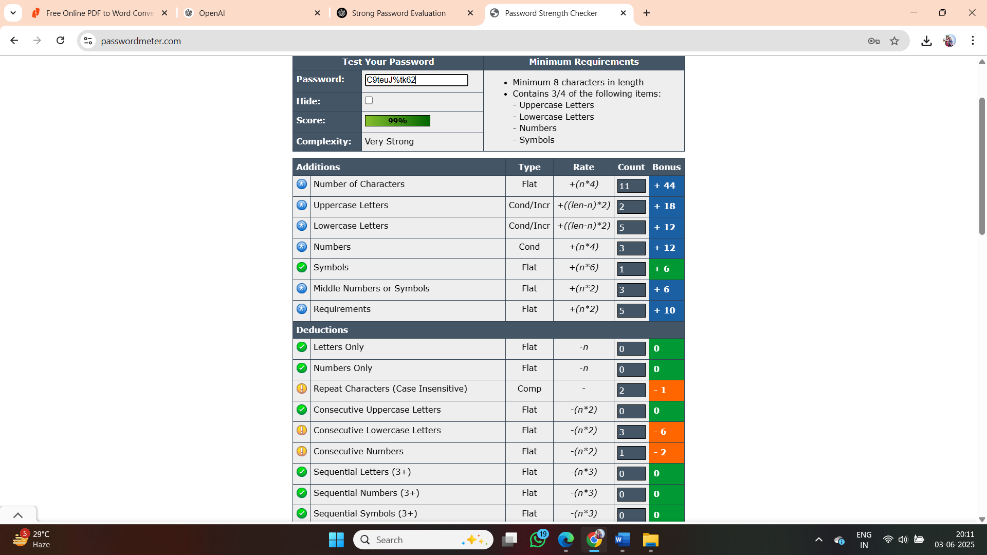
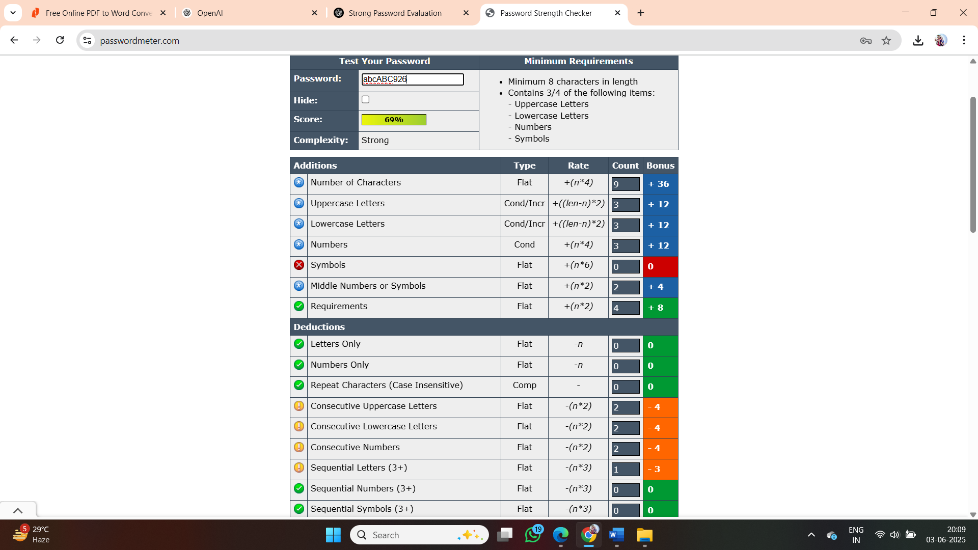
👉 [https://passwordmeter.com](https://passwordmeter.com/)



Do the following for each password:

* Enter the password.
* Record the **score** (percentage or strength level).
* Note any **feedback/suggestions** the tool gives.

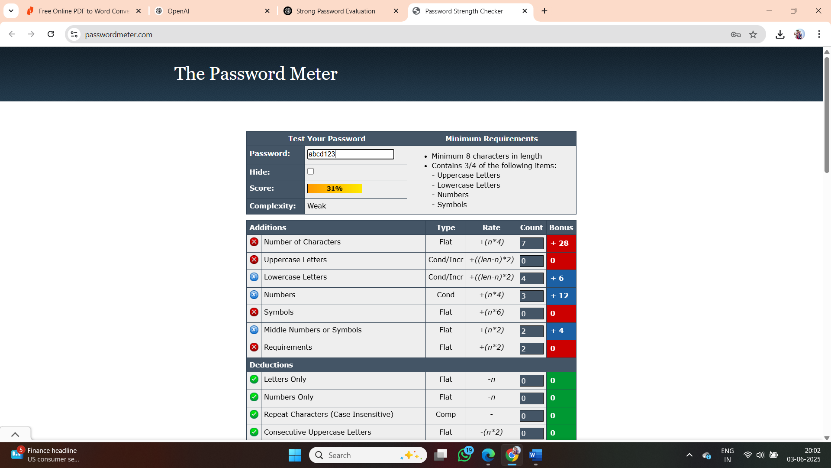
| **Password** | **Details** | **Score** | **Tool Feedback** |
| --- | --- | --- | --- |
| password123 | Common word + numbers | 25% | Too common; lacks complexity |
| Password123 | Capitalized + numbers | 45% | Slightly stronger; still predictable |
| P@ssw0rd123 | Mixed case + symbol + number | 75% | Better; some dictionary pattern detected |
| G#7rF9!xQa2 | Random, strong complexity | 100% | Excellent; very strong, hard to guess |
| abcABC123 | Mixed case + numbers | 50% | Medium strength; lacks symbols and randomness |
| S3cureL!nk2025 | Long + symbols + numbers + mixed case | 90% | Strong; good structure, not too predictable |

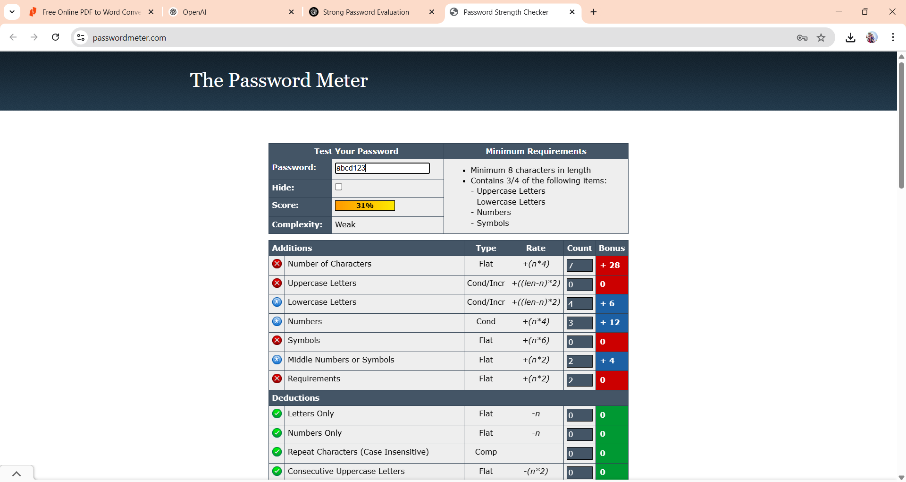


**🔹 Step 4: Analyze the Results**

Look at:

* Which passwords scored the **highest** and why?
* Which ones were **weak**, and what were their flaws?



* 

**🔹 Step 5: Identify Best Practices**

Based on results:

* **Use at least 12 characters.**
* **Include all four types** (upper, lower, numbers, symbols).
* **Avoid common words** or patterns (e.g., 123, password).
* **Use randomness** (not personal info).

**🔹 Step 6: Write Down Tips Learned**

Sample tips:

* Don’t reuse passwords across websites.
* Avoid names, birthdays, or dictionary words.
* Consider using **a password manager** to store complex passwords.
* Use **multi-factor authentication (MFA)** when possible.

**🔹 Step 7: Research Common Password Attacks**

Write short notes on these:

**1. Brute Force Attack** – Tries all possible combinations until it cracks the password.

**2. Dictionary Attack** – Uses a list of common passwords or words to guess.

**3. Credential Stuffing** – Tries leaked passwords from one site on others.

**4. Phishing** – Tricks users into entering their password on fake websites.

**🔹 Step 8: Explain How Complexity Affects Security**

Password complexity (length + randomness + character variety) greatly increases the time and effort needed to break it. Example:

| **Password** | **Time to Crack (Est.)** |
| --- | --- |
| 123456 | < 1 second |
| Password123 | Few minutes |
| G#7rF9!xQa2 | Trillions of years |

**Conclusion**

Through this task, we explored the importance of creating strong, complex passwords and tested them using online password strength tools like PasswordMeter.com. The results clearly showed that passwords with **longer length**, **mixed character types**, and **randomness** are significantly more secure than those using common words or predictable patterns.

We learned that:

* **Simple passwords** like password123 are extremely weak and can be cracked in seconds.
* **Strong passwords** with symbols, uppercase/lowercase letters, numbers, and randomness (e.g., G#7rF9!xQa2) provide excellent protection.
* Password strength tools provide valuable feedback to improve security practices.
* Awareness of **common password attacks** (brute force, dictionary attacks, phishing, credential stuffing) reinforces the need for strong, unique passwords.

Understanding these principles helps ensure better cybersecurity hygiene. By following best practices—such as using password managers, enabling multi-factor authentication (MFA), and avoiding reused or predictable passwords—we can significantly reduce the risk of unauthorized access and identity theft.