**Task 6: Create a Strong Password and Evaluate Its Strength**

**Objective**

To understand what makes a password strong by creating multiple passwords of varying complexity, testing them using an online password strength checker, and analyzing the results.

**Step-by-Step Process**

1. **Understanding Strong Passwords**
   * Minimum 12–16 characters
   * Combination of uppercase & lowercase letters
   * Inclusion of numbers and symbols
   * Avoid dictionary words, patterns, or personal details
2. **Passwords Created**

| **No.** | **Password (Test)** | **Complexity Level** |
| --- | --- | --- |
| 1 | password123 | Simple |
| 2 | HelloWorld2025 | Medium |
| 3 | H3llo\_W0rld! | Strong |
| 4 | T!g#rL!0n\_2025 | Very Strong |
| 5 | V@9X#pL2qW$r8Z!tM1 | Extremely Strong |

*(Note: These are sample test passwords, not actual personal passwords.)*

1. **Testing Method**
   * Tool used: <https://passwordmeter.com>
   * Each password was entered into the checker.
   * Recorded: **Score**, **Time to Crack**, and **Feedback** from the tool.
2. **Results Table**

| **Password** | **Score** | **Feedback** |
| --- | --- | --- |
| password123 | 43% | Too common, lacks symbols, short length |
| HelloWorld2025 | 99% | Needs more symbols, predictable pattern |
| H3llo\_W0rld! | 98% | Strong, could be slightly longer |
| T!g#rL!0n\_2025 | 90% | Very strong, good length & randomness |
| V@9X#pL2qW$r8Z!tM1 | 100% | Extremely strong, highly random & complex |



**Best Practices Identified**

* Use at least **12–16 characters**.
* Mix uppercase, lowercase, numbers, and symbols.
* Avoid dictionary words and personal information.
* Make the password random, not based on patterns.
* Longer passwords greatly increase time to crack.

**Common Password Attacks**

* **Brute Force Attack** – Tries every possible combination until correct.
* **Dictionary Attack** – Tries common words and password lists.
* **Credential Stuffing** – Uses leaked username-password combinations from breaches.

**Impact of Complexity on Security**

Password complexity directly affects resistance to attacks. A short, simple password can be cracked in seconds, while a long, random, and complex password may take centuries. The combination of length, character variety, and unpredictability is crucial for maximum security.