**Title: Task 5 – Password Strength Evaluation Report**

**1. Objective:**  
**To evaluate different passwords based on strength and learn best practices for creating secure passwords.**

**2. Tested Passwords:**

| **Password** | **Strength Result (from tool)** | **Score (%)** | **Feedback** |
| --- | --- | --- | --- |
| hello123 | Weak | 37 % | Add symbols and uppercase letters |
| Hello123 | Medium | 63 % | Add special characters |
| Hello@123 | Strong | 81 % | Increase length |
| HeLlo@123456! | Very Strong | 100 % | Excellent |
| V9!h&KwLz@28%w | Extremely Strong | 100 % | Ideal complexity and length |

**3. Tips Learned:**

* Use at least 12 characters.
* Include uppercase, lowercase, numbers, and symbols.
* Avoid dictionary words and personal information.
* Random combinations are more secure.

**4. Common Password Attacks (Briefly Explained):**

* **Brute Force:** Tries all possible combinations.
* **Dictionary Attack:** Tries common or known passwords.
* **Phishing:** Tricking users to give passwords via fake sites.
* **Credential Stuffing:** Using leaked passwords across accounts.

**5. Conclusion:**  
Password complexity significantly increases resistance to cracking methods. Random, long, and complex passwords are most secure.