**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)

**1. Create Multiple Passwords**

Make at least 3–4 passwords with different complexity:

1. Password → simple, weak.
2. hello12345 → Good
3. hello@1234 → Strong (has lowercase, number, symbol)
4. Hello@123 → Very Strong(has uppercase, lowercase, number, symbol)
5. Hell0@Guys#Cyb3r!$ → very strong (long, random, diverse).

**2. Test Password Strength**

Go to a password checker like:  
🔗 <https://passwordmeter.com>

A screenshot of a computer

AI-generated content may be incorrect.

* **Exceptional:** Exceeds minimum standards. Additional bonuses are applied.
* **Sufficient:** Meets minimum standards. Additional bonuses are applied.
* **Warning:** Advisory against employing bad practices. Overall score is reduced.
* **Failure:** Does not meet the minimum standards. Overall score is reduced.

1) Password-**Password**

Score-**26%** and Complexity-**Weak**

A screenshot of a computer

AI-generated content may be incorrect.

2)Password-**hello12345**

Score-**51%** and Complexity-**Good**

A screenshot of a computer screen

AI-generated content may be incorrect.

3)Password-**hello@1234**

Score-**66%** and Complexity-**Strong**

A screenshot of a computer

AI-generated content may be incorrect.

4)Password-**Hello@123**

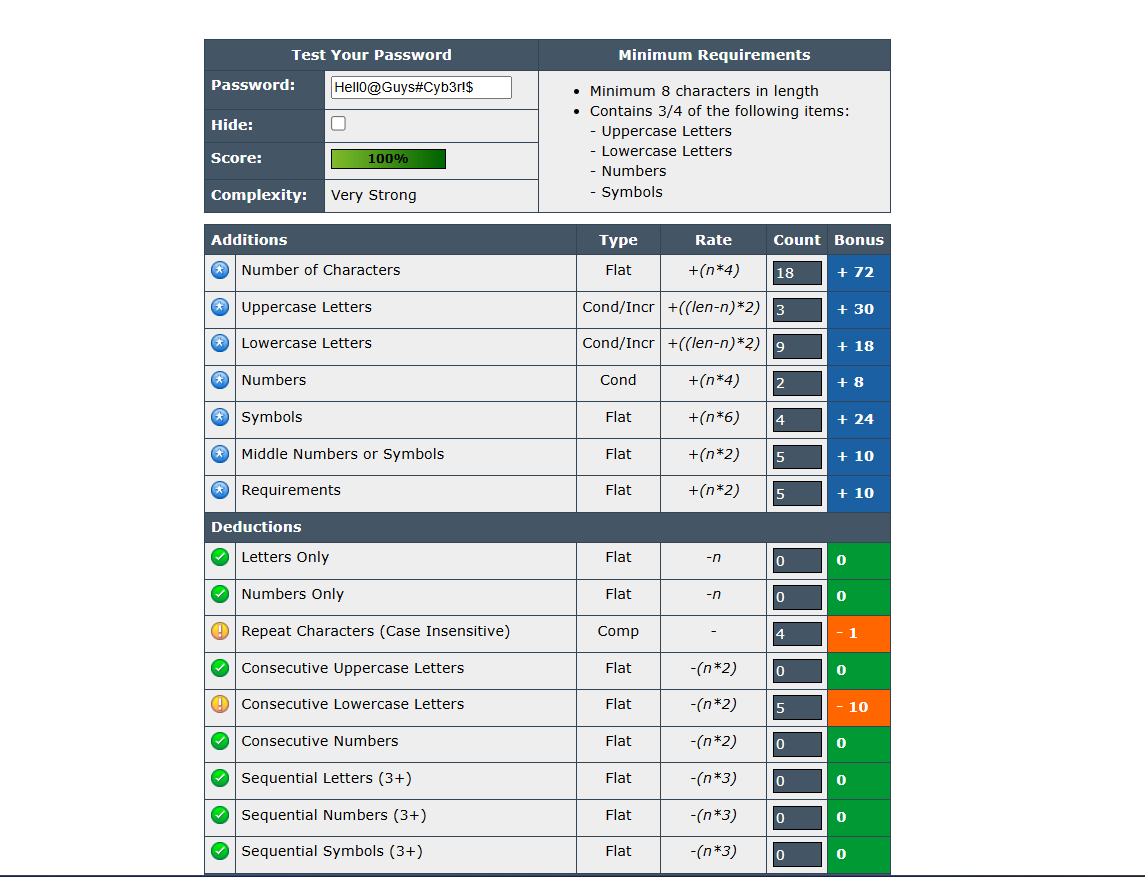
Score-**89%** and Complexity-very **Strong**

**A screenshot of a computer

AI-generated content may be incorrect.**

5)Password-Hell0@Guys#Cyb3r!$

Score-**100%** and Complexity-**very** **Strong**

****

**3. Compare Results**

|  |  |  |  |
| --- | --- | --- | --- |
| **Password** | **Score (%)** | **Strength** | **Tool Feedback** |
| Password | 26% | Weak | Too short, only lowercase + uppercase |
| hello12345 | 51% | Good | Better but still short |
| hello@1234 | 66% | Strong | Good length, multiple char sets |
| Hello@123 | 81% | Very Strong | uppercase + lowercase + symbol + Number |
| Hell0@Guys#Cyb3r!$ | 100% | Very Strong | Very Difficult to crack |

**4. Identify Best Practices**

From testing, strong passwords should:

* Be at least **12–16 characters** long.
* Use **upper + lower case letters, numbers, symbols**.
* Avoid dictionary words, names, or birthdates.
* Be **unique per account**.
* Use a **password manager** for complex passwords.

**5. Research Common Password Attacks**

1. **Brute Force Attack:** Tries every possible combination until it finds the password.
2. **Dictionary Attack:** Uses a list of common words or leaked passwords.
3. **Credential Stuffing:** Uses previously leaked credentials on other accounts.
4. **Social Engineering:** Tricks the user into revealing the password

**6. Summarize**

Password complexity **directly impacts security**:

* Simple passwords (hello123) can be cracked in seconds.
* Complex, long passwords (Hell0@Guys#Cyb3r!$)may take centuries with brute force.
* Strong password practices reduce the risk of hacking and improve overall cybersecurity hygiene.