**ELEVATE LABS – CYBER SECURITY INTERNSHIP**

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

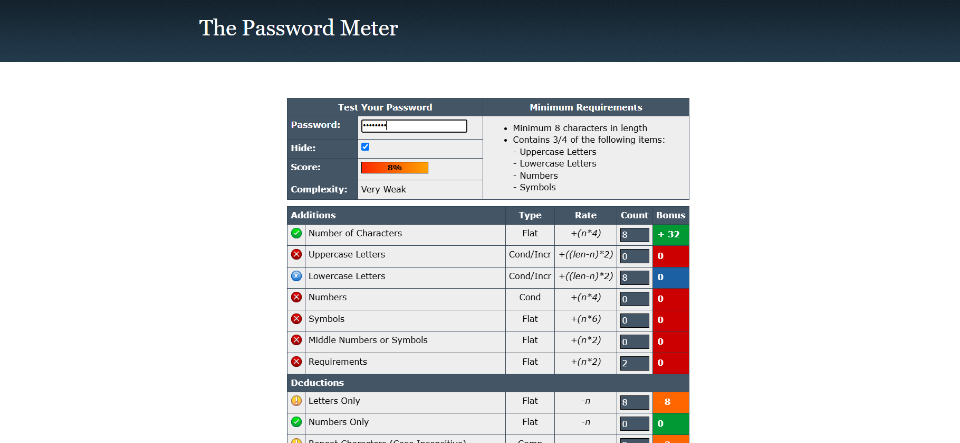
**Objective:  
The goal of this task is to create passwords with different levels of complexity and evaluate their strength using an online password checker. This helps in understanding the factors that make a password strong or weak and how to improve password security.**

**List the Passwords Tested:-**

**Insert the screenshot from passwordmeter.com showing that password’s strength result.**

* Password

Result:-



* Password123

Result:-



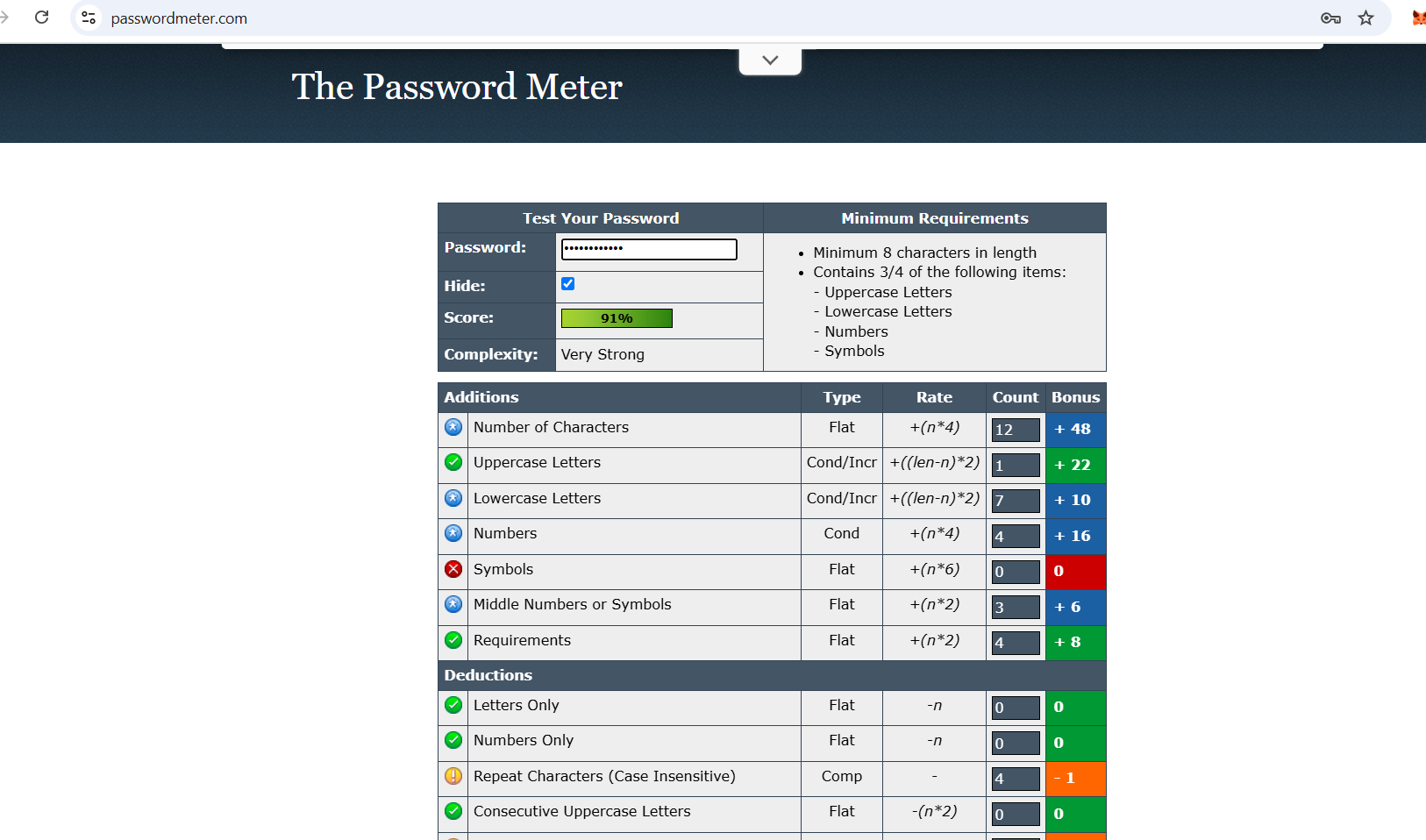
* P@ssw0rd!

Result:-



* Rakshita2025

Result:-



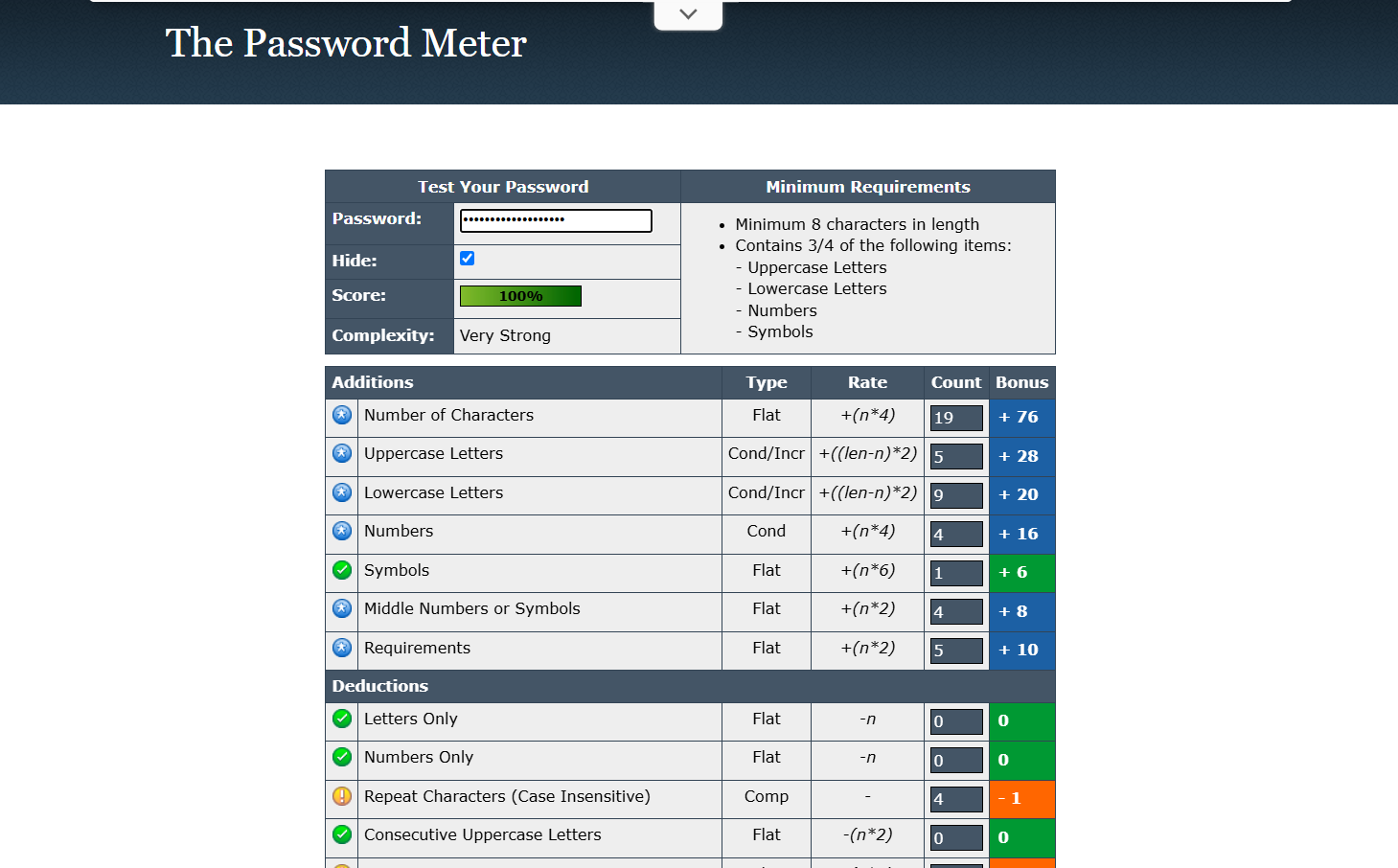
* R@k5h!ta

Result:-



* MyDogNameIsRax!2025

Result:-





**Conclusion:**

Longer passwords and passphrases are significantly stronger than short complex passwords.  
Adding numbers, symbols, and capital letters helps, but **length** and **unpredictability** are the most important factors.  
Using a **password manager** and **multi-factor authentication (MFA)** ensures better protection against attacks like brute-force and dictionary attacks.

**Learning Outcome:**  
I learned how to analyze password strength, identify weak passwords, and understand what makes a password secure. This task helped me realize the importance of using strong, unique passphrases and MFA for better account protection.