**Day 6**

**Tool Used**

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

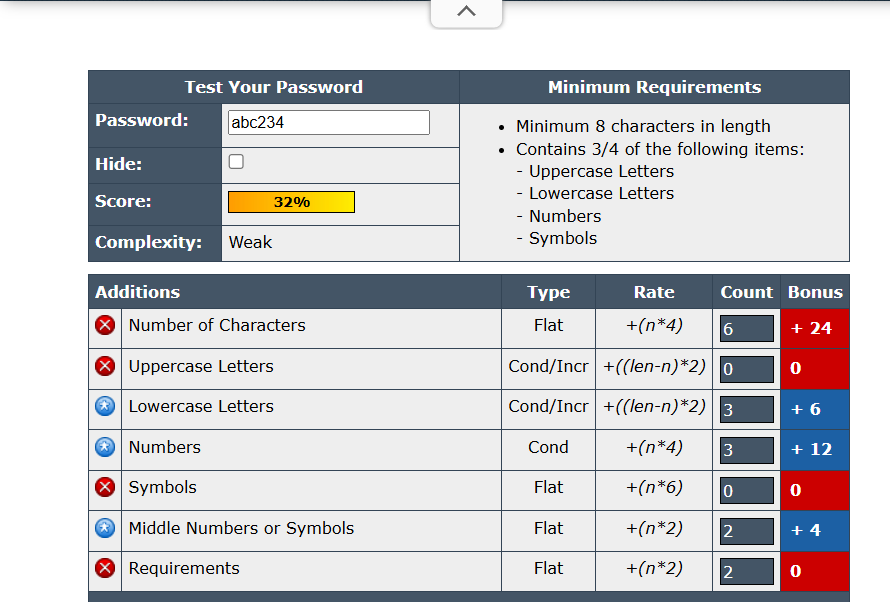
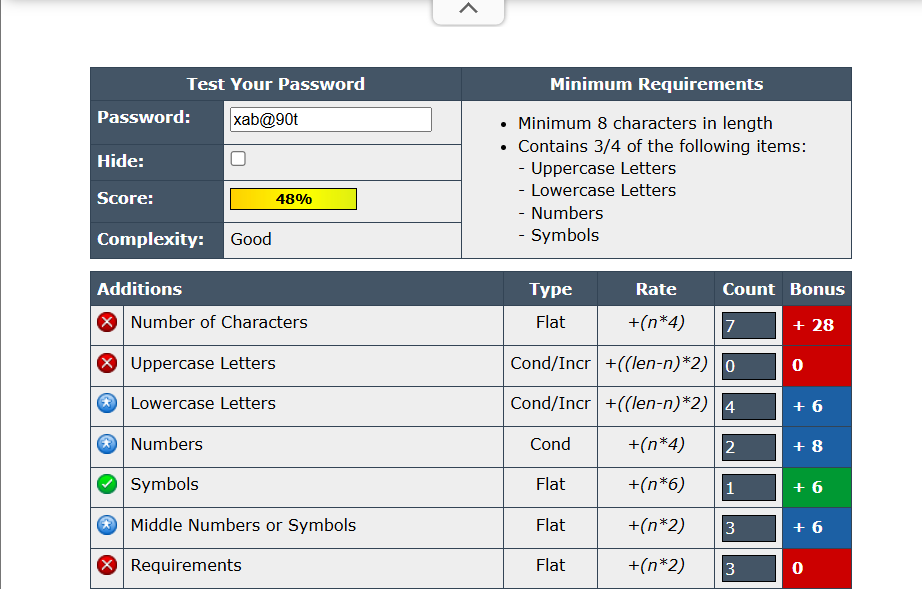
**Objective :-**

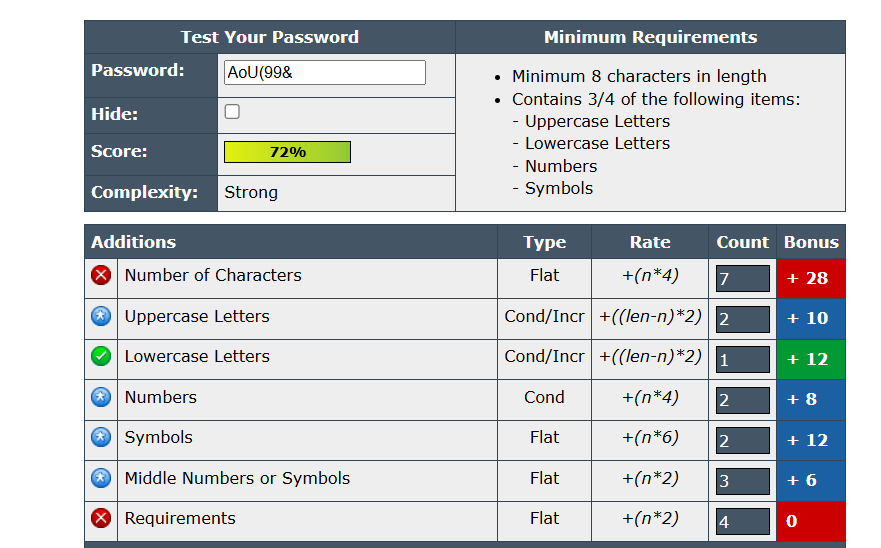
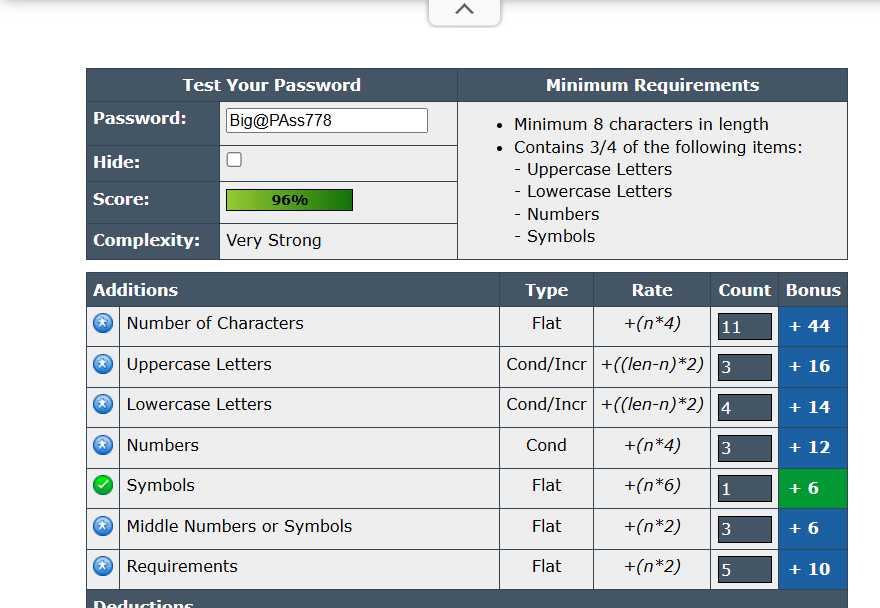
* To assess password strength and document best security practices

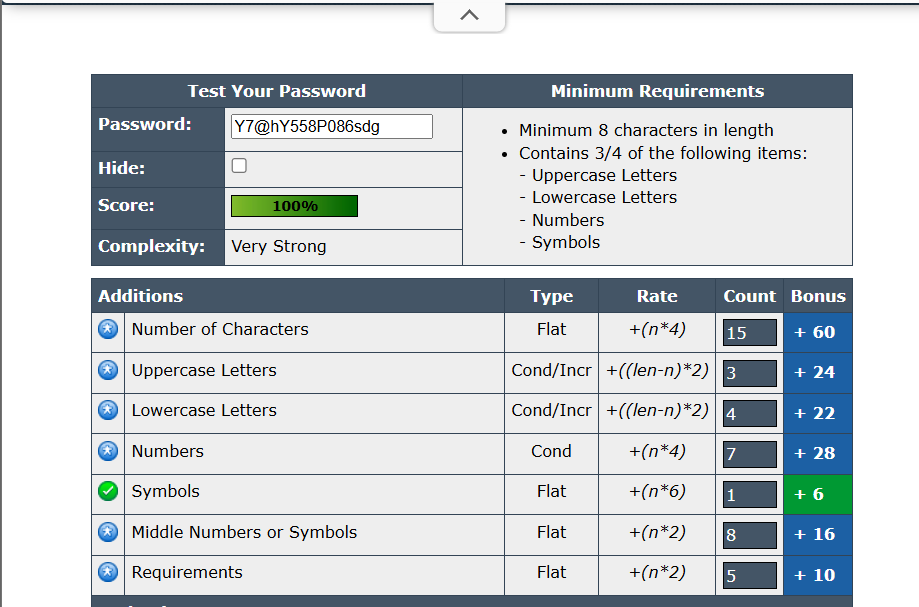
**Sample of Passwords Tested :-**

| **Password** | **Score/Rating** | **Tool Used** | **Feedback/Suggestions** |
| --- | --- | --- | --- |
| Abc234 | Weak (32%) | PasswordMeter | Too short, lacks symbols |
| xab@90t | Good (48%) | PasswordMeter | Needs longer length |
| AoU(99&) | Strong (72%) | PasswordMeter | Very strong, good length |
| Big@PAss778 | Very Strong (96%) | PasswordMeter | Excellent complexity, length |
| Y7@hY558P086sdg | Max (100%) | PasswordMeter | Extremely strong, random |

**Screenshots :-**

** **

** **

****

**Analysis :-**

* Password which are atleast 8 characters are shown as strong password.
* In strong password you need to put symbols to strengthen your password.
* If you add UpperCase and LowerCase characters it is very good and strong.
* Add numbers in your password for more complexity.

**Best Practice Tips :-**

* Use 12+ character password which is mix of Upper case and Lower case, Symbol, and Numbers, so the password will be very strong.
* Avoid Personal information. (e.g., Birth date, Name,etc.)
* Never use same password for different accounts.
* Use password manager for storage.

**Common Password Attacks :-**

* Brute Force Attack :

A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys. It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations' systems and networks.

* Dictionary Attack :

A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys. It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations' systems and networks.

* Credential Stuffing Attack :

Credential stuffing is a cyberattack method in which attackers use lists of compromised user credentials to breach into a system. The attack uses bots for automation and scale and is based on the assumption that many users reuse usernames and passwords across multiple services.

**Summary :-**

Password are very important in this era of hacking and phishing. Building strong password is very important. Because anybody can stole your personal data.

It is like when we go out from our home at that time we lock our main door of house. So nobody can enter in our house. Passwords are like that lock on the main door so nobody can see your personal data.

Passwords are need to be created stronger with the help of Upper case, Lower case charcters, using symbols and numbers. Length of password is atleast 8-12 characters. So, its is difficult to breach your password. Don’t enter your personal information. (e.g., Birth date, Name,etc.)