Report

Name : sharayu Jadhav

Class : SY BSc Cyber Security

Create a Strong Password and Evaluate Its Strength

* Password strength result

Criteria Details

1.password winter@sky123

2.length 13 character

3.upper case no

4.lower case yes

5.symbol yes

6.strength score(passwordmeter) 71%(strong)

Criteria Details

1.Password B00k@shelf98!!

2.length 14 characters

3.Upper case yes

4.Lower case yes

5.symbol yes

6.strength score(passwordmeter) 100%(very strong)

* Best Practises to Identify
* Use at least 12 characters
* Combine uppercase, lowercase, symbols and numbers.
* Avoid predict pattern
* Never reuse password
* Tips learned from Evaluation
* Avoid reuse : unique password for every site
* Don’t use personal info(birthday,name).
* Longer : Password length significantly increase strength
* Common password attacks

1.Brute force attack

Tries every possible combination until the correct password is found.

2.Diticinory attack

Tries passwords from a list of common words and variations

3. Phishing attack

Tricking users into entering passwords on fake websites or through fake emails.

* How complexity affect security

 **Complex passwords exponentially increase time required to crack them**, making brute- force and dictionary attacks impractical.

* Passwords should be **both complex and unique** to defend against modern cyber threats.