CYBER SECURITY INTERNSHIP

Task 6: Create a Strong Password and Evaluate Its Strength

Objective

To understand what makes a password strong and test it against password strength tools.

Tools Used

Online free password strength checker (www.passwordmeter.com)

Passwords Created

Password	Length	Characters Used	Strength Score	Feedback
abc123	6	Lowercase + Numbers	18%	Weak
abc@123	7	Lowercase + Number + Symbol	35%	Medium
Abc@1234	8	Upper + Lower + Num + Sym	62%	Strong
A@b9#Xy7!	9	Mixed Characters	96%	Very Strong

Best Practices for Creating Strong Passwords

- Use at least 8–12 characters.
- Include uppercase and lowercase letters.
- Include numbers and special symbols.
- Avoid personal information.
- Avoid dictionary words.
- Avoid predictable sequences.
- Use random combinations of characters.

Tips Learned

- Longer passwords are more secure.
- Symbols improve password strength.
- Mixed characters increase complexity.
- Random passwords are harder to guess.
- Do not reuse passwords for multiple accounts.

Common Password Attacks

Brute Force Attack: Tries every possible combination until the correct password is found.

Dictionary Attack: Uses a predefined list of common passwords to gain access.

Impact of Password Complexity on Security

Password Type	Time to Crack	Security Level
Simple	Few Seconds	Low

Medium	Few Minutes	Moderate
Complex	Years	High

Conclusion

Password complexity plays an important role in cybersecurity. Stronger passwords with mixed characters and longer length provide better protection against brute force and dictionary attacks. Therefore, strong passwords help in securing user accounts and sensitive information from unauthorized access.