CYBER SECURITY INTERNSHIP

Task 6: Password Strength Evaluation Report

Objective: Understand what makes a password strong and test it against password strength tools.

Tool Used: passwordmeter.com (or similar)

Date: 01 July 2025

Passwords Tested & Feedback:

- 123456: Weak - Very common and short.
- Qwerty123: Weak - Common pattern, lacks symbols.
- Krishna@2025: Strong - Mix of upper/lowercase, symbol, number.
- $Vsk_98&Secure#: Very Strong - Long, mixed charset.

Best Practices for Creating Strong Passwords:

- Use at least 12 characters
- Include uppercase, lowercase, numbers, and symbols
- Avoid dictionary words or personal information
- Use unique passwords for each service
- Consider using a password manager

Common Password Attacks:

- Brute Force Attack: Tries all combinations
- Dictionary Attack: Uses common words/phrases
- Phishing: Tricks user into revealing passwords

Interview Questions & Answers:

Q: What makes a password strong?

A: Length, complexity, unpredictability.

Q: What are common password attacks?

A: Brute force, dictionary attacks, phishing.

Q: Why is password length important?

A: Longer passwords take exponentially more time to crack.

Q: What is a dictionary attack?

A: An attack using a list of common words.

Q: What is multi-factor authentication?

A: An added layer of security requiring more than just a password.

Q: How do password managers help?

A: They generate, store, and autofill secure passwords.

Q: What are passphrases?

A: Combinations of random words, often easier to remember.

Q: Common mistakes in password creation?

A: Using short, predictable, reused passwords.