Password Strength Evaluation Report

Eleyate Cyber Security Internship - Task 6

Prepared by: Sujay Vegi

Date: June 04, 2025

1. Introduction

This report presents an evaluation of password strength using online password checking tools as part of Task 6 for the Eleyate Cyber Security Internship. The objective was to learn how password complexity affects security and how to create strong passwords resistant to attacks.

2. Methodology

1. Several passwords of varying complexity were created.

2. Passwords were tested using online tools like passwordmeter.com.

3. Scores, weaknesses, and recommendations were recorded.

4. Strong and weak patterns were analyzed to identify best practices.

5. Research on common attacks and security measures was conducted.

3. Password Evaluation Summary

Example Passwords Tested:

- 'password123': Weak (Common, lacks symbols or case variation)

- 'P@ssw0rd!2024': Strong (Good mix of characters, length >12)

- 'LetMe!n789': Moderate (Improved with symbols and caps)

Best Practices Learned:

- Use at least 12 characters.

- Include uppercase, lowercase, numbers, and symbols.

- Avoid common words or predictable patterns.

- Use passphrases for better memorability and strength.

4. Interview Questions and Answers

1. What makes a password strong?

A strong password includes a combination of uppercase, lowercase, numbers, and special characters, and is at least 12 characters long.

2. What are common password attacks?

Brute force attacks, dictionary attacks, phishing, and credential stuffing are common password attacks.

3. Why is password length important?

Longer passwords are harder to crack because the number of possible combinations increases exponentially.

4. What is a dictionary attack?

It is an attack that uses a list of common words and combinations to guess a password.

5. What is multi-factor authentication?

It is a security method that requires two or more verification steps, such as a password and a one-time code.

6. How do password managers help?

They store and generate strong, unique passwords for each site, reducing reuse and human error.

7. What are passphrases?

A passphrase is a sequence of words or a sentence used as a password, often longer and easier to remember.

8. What are common mistakes in password creation?

Using common words, short lengths, personal information, and reusing passwords across platforms.