# Cyber Security Internship – Task 4

## Password Security & Authentication Analysis

## 1. Introduction

Passwords are the most common method of authentication. Weak passwords can be easily attacked, leading to data breaches. This task focuses on understanding password security, hashing, attacks, and protection methods.

## 2. How Passwords Are Stored

Passwords are not stored in plain text. Instead, they are stored as **hashes**.

- **Hashing:** Converts passwords into fixed-length values.
- **Encryption:** Converts data into a secret form that can be decrypted.

Hashing is preferred for passwords because it cannot be reversed.

## 3. Common Hash Types

- **MD5:** Fast but insecure
- **SHA-1:** Better than MD5 but still weak
- **bcrypt:** Slow and secure, commonly used today

## 4. Password Hash Generation

Password hashes can be generated using tools or online hash generators.
The same password always produces the same hash (for most algorithms).

## 5. Password Cracking Techniques

### Brute Force Attack

Tries all possible combinations.
Very slow but effective against short passwords.

### Dictionary Attack

Uses common passwords from wordlists.
Faster and effective against weak passwords.

## 6. Why Weak Passwords Fail

- Short length
- Common words (123456, password)
- No symbols or numbers

Attackers can easily crack such passwords using wordlists.

## 7. Multi-Factor Authentication (MFA)

MFA adds an extra layer of security.

Examples:

- OTP
- Authenticator apps
- Biometrics

Even if a password is compromised, MFA protects the account.

## 8. Recommendations for Strong Authentication

- Use long passwords (12+ characters)
- Mix letters, numbers, and symbols
- Avoid common words
- Enable MFA
- Use password managers

## 9. Conclusion

This task helped me understand how password security works, common attack methods, and the importance of strong authentication practices.