# CYBER SECURITY INTERNSHIP – Task 4

Password Security & Authentication Analysis

This report explains password storage mechanisms, password cracking techniques, and strong authentication practices.

## Introduction

Weak passwords are one of the main causes of cyber security breaches.

## Password Storage

Passwords should be stored using hashing instead of plain text or encryption.

## Hashing vs Encryption

Hashing is irreversible while encryption can be reversed using a key.

## Common Hash Types

MD5 and SHA-1 are weak.
SHA-256 offers better security.
bcrypt is slow, salted, and secure.

## Password Attacks

Dictionary attacks use common passwords.
Brute force attacks try all combinations.

## Why Weak Passwords Fail

Short length, common words, and reused passwords are easy to crack.

## Multi-Factor Authentication (MFA)

MFA adds additional verification layers for better security.

## Strong Authentication Recommendations

Use long unique passwords.
Enable MFA.
Use bcrypt hashing.
Avoid password reuse.

## Interview Questions

What is hashing?
Difference between hashing and encryption?
What is dictionary attack?
Why is bcrypt secure?
What is MFA?

## Final Outcome

Knowledge of password attacks and authentication defenses.