

Cyber Security Internship – Task 4

Password Security & Authentication Analysis

1. Introduction

Passwords are one of the most common methods of authentication, but they are also one of the weakest if not implemented properly. In this task, I learned how passwords are stored, how attackers attempt to crack weak passwords, and why strong authentication methods like MFA are important.

2. How Passwords Are Stored

Passwords should never be stored in plain text. Instead, they are stored using **hashing**.

- **Hashing** converts a password into a fixed-length value.
- The same password always produces the same hash.
- Hashes cannot be reversed back to the original password.

This ensures that even if a database is leaked, actual passwords are not directly visible.

3. Hashing vs Encryption

- **Hashing**
 - One-way process
 - Cannot be reversed
 - Used for password storage
- **Encryption**
 - Two-way process
 - Can be decrypted using a key
 - Used for protecting data in transit or storage

Passwords should always be hashed, not encrypted.

4. Common Hash Types

Some commonly used hash algorithms include:

- **MD5** – Fast but insecure and easily crackable
- **SHA-1** – Stronger than MD5 but now considered weak
- **bcrypt** – Secure and slow, designed specifically for password hashing

Modern systems prefer bcrypt or similar algorithms because they resist brute-force attacks.

5. Password Cracking Concepts

Attackers try to crack password hashes using different methods.

Dictionary Attack

Uses a list of common passwords or leaked password databases to guess passwords quickly.

Brute Force Attack

Tries every possible password combination until the correct one is found. This method is slow but effective against weak passwords.

Weak passwords fail because they are short, common, or predictable.

6. Why Weak Passwords Are Dangerous

Weak passwords such as 123456, password, or admin123 can be cracked very quickly using automated tools. Once cracked, attackers can gain unauthorized access to systems and sensitive data.

7. Multi-Factor Authentication (MFA)

MFA adds an extra layer of security by requiring more than one authentication factor, such as:

- Password
- OTP or authenticator app
- Biometric verification

Even if a password is compromised, MFA helps prevent account takeover.

8. Strong Password & Authentication Recommendations

Good password and authentication practices include:

- Using long and complex passwords
- Avoiding common or reused passwords
- Using password managers
- Enabling Multi-Factor Authentication
- Using secure hashing algorithms like bcrypt
- Implementing account lockout policies

9. Summary

This task helped me understand how passwords are stored securely, how attackers exploit weak passwords, and how strong authentication methods like MFA protect systems. Proper password security is essential to prevent unauthorized access and data breaches.