Task 4: Password Security & Authentication Analysis

1. Introduction

Password security is a critical part of cyber security. Most systems protect user passwords by converting them into hashes instead of storing them as plain text. Weak passwords can be cracked easily using password-cracking techniques.
This task focuses on understanding how passwords are stored, how attackers crack weak passwords, and how strong authentication methods protect systems.

---

2. How Passwords Are Stored (Hashing vs Encryption)

Hashing

- Hashing converts a password into a fixed-length string called a **hash**.
- Hashing is **one-way**, meaning the original password cannot be directly recovered.
- Same password always produces the same hash.
- Used by websites and applications to store passwords securely.

Example:
password123 → 482c811da5d5b4bc6d497ffa98491e38

Encryption

- Encryption is **two-way**.
- Data can be decrypted back using a key.
- Encryption is **not recommended** for password storage.

✅ **Conclusion:**
Passwords should always be **hashed**, not encrypted.

---

3. Common Hash Types

Hash Type	Description	Security Level
MD5	Fast and outdated hashing algorithm	❌ Weak
SHA-1	Slightly better than MD5 but broken	❌ Weak
SHA-256	Secure but fast (needs salting)	⚠ Medium
bcrypt	Slow and salted hashing	✅ Strong

---

4. Password Hash Generation

Passwords are converted into hashes using hashing algorithms.

Example Passwords and Hashes:

Password	Hash Type	Example Hash
123456	MD5	e10adc3949ba59abbe56e057f20f883e
admin	SHA-1	d033e22ae348aeb5660fc2140aec35850c4da997
P@ssw0rd!	bcrypt	$2b$12$...

---

5. Password Cracking Techniques

Dictionary Attack

- Uses a list of common passwords.
- Very effective against weak passwords.
- Fast and efficient.

Brute Force Attack

- Tries **all possible combinations**.
- Takes more time.
- Effective if password length is short.

---

6. Why Weak Passwords Fail

Weak passwords fail because:

- They are short (less than 8 characters)
- They use common words (admin, password, 123456)
- No mix of uppercase, lowercase, numbers, and symbols
- Reused across multiple websites

Example of Weak Passwords:

- password
- admin123
- qwerty
- 12345678

---

7. Multi-Factor Authentication (MFA)

What is MFA?

MFA adds **extra security layers** beyond passwords.

Types of MFA

1. **Something you know** – Password or PIN
2. **Something you have** – OTP, mobile, security token
3. **Something you are** – Fingerprint, face recognition

Why MFA is Important

- Prevents unauthorized access
- Even if password is cracked, login is blocked
- Protects sensitive systems and accounts

---

8. Password Attacks vs Defenses

Attack	Defense
Dictionary attack	Strong passwords

Attack	Defense
Brute force	Account lockout
Hash cracking	bcrypt hashing
Credential stuffing	MFA
Phishing	User awareness

---

9. Recommendations for Strong Authentication

- Use **minimum 12-character passwords**
- Combine uppercase, lowercase, numbers, and symbols
- Avoid common words
- Use **bcrypt** for password hashing
- Enable **Multi-Factor Authentication**
- Do not reuse passwords
- Use password managers
- Apply account lockout after failed attempts

---

10. Conclusion

This task helped in understanding how passwords are stored securely using hashing algorithms. Weak passwords are vulnerable to cracking through dictionary and brute force attacks. Strong hashing methods, long passwords, and Multi-Factor Authentication are essential for protecting user accounts and systems.