Task 4: PASSWORD SECURITY & AUTHENTICATION ANALYSIS

1. Introduction

Passwords are the most common method of authentication used in digital systems. However, weak passwords are vulnerable to attacks such as brute force and dictionary attacks. This report analyzes password security mechanisms, hashing techniques, common attacks, and the importance of Multi-Factor Authentication (MFA).

---

2. What is Hashing?

Hashing is a **one-way cryptographic process** that converts plaintext passwords into fixed-length strings called hashes. Once hashed, the original password cannot be retrieved.

Example:

password123 → 482c811da5d5b4bc6d497ffa98491e38

---

3. Hashing vs Encryption

Hashing	**Encryption**
One-way process	Two-way process
Cannot be reversed	Can be decrypted
Used for password storage	Used for data protection
Example: bcrypt	Example: AES

---

4. Common Hash Types

Hash Algorithm	**Security Level**
MD5	Weak
SHA-1	Weak

SHA-256	Moderate
bcrypt	Strong

bcrypt is considered secure because it uses **salting and cost factors**, making cracking difficult.

---

5. Password Hash Generation

Password hashes can be generated using tools such as:

- Linux terminal
- Online hash generators
- OpenSSL

Example command:

echo -n "password123" | md5sum

---

6. Password Cracking Techniques

Brute Force Attack

A brute force attack tries **every possible combination** until the correct password is found. It is time-consuming but effective against short passwords.

Dictionary Attack

A dictionary attack uses **predefined wordlists** containing common passwords. It is faster and very effective against weak passwords.

---

7. Cracking Weak Hashes (Educational Purpose)

Tools used:

- **Hashcat**
- **John the Ripper**

Example (John the Ripper):

john hash.txt --wordlist=rockyou.txt

Weak passwords like 123456 and password are cracked within seconds.

---

8. Why Weak Passwords Fail

- Short length
- Predictable patterns
- No special characters
- Reused across platforms
- Stored using weak hashing algorithms

---

9. Multi-Factor Authentication (MFA)

What is MFA?

MFA requires users to provide **two or more authentication factors**:

1. Something you know (password)
2. Something you have (OTP, mobile device)
3. Something you are (biometrics)

Why MFA is Important

- Prevents unauthorized access
- Protects even if passwords are compromised
- Reduces impact of phishing attacks

---

10. Recommendations for Strong Authentication

- Use **bcrypt or Argon2**
- Password length ≥ **12 characters**

- Enable **MFA**
- Use account lockout mechanisms
- Avoid password reuse
- Use password managers

---

11. Conclusion

Weak passwords remain one of the biggest cybersecurity threats. Using strong hashing algorithms, enforcing strong password policies, and implementing MFA significantly reduce the risk of unauthorized access.