Task 4: Password Security & Authentication Analysis

1. Objective

The objective of this task is to understand password security mechanisms, analyze how passwords are stored using hashing techniques, study common password attack methods, and evaluate the importance of strong authentication practices such as Multi-Factor Authentication (MFA).

2. Tools Used

- **Primary Tools:** Hashcat, John the Ripper
- **Alternative Tools:** Online Hash Identifier tools
- **Environment:** Kali Linux

3. Concepts Studied

- Password hashing vs encryption
- Common hash algorithms (MD5, SHA-1, bcrypt)
- Brute force and dictionary attacks
- Weak vs strong passwords
- Multi-Factor Authentication (MFA)

4. Hashing vs Encryption

- **Hashing** is a one-way process used to securely store passwords. Once hashed, the original password cannot be retrieved.
- **Encryption** is a two-way process where data can be encrypted and later decrypted using a key.

Hashing is preferred for password storage because it prevents password recovery even if the database is compromised.

5. Hash Types Identified

- **MD5:** Fast but insecure and vulnerable to attacks
- **SHA-1:** Better than MD5 but no longer considered secure
- **bcrypt:** Strong and secure due to salting and adaptive cost

6. Password Hash Generation

Sample passwords were converted into hashes using hashing tools. Weak passwords such as simple words or numeric patterns were chosen to demonstrate how easily they can be cracked.

7. Password Cracking Techniques

- **Dictionary Attack:** Uses a predefined list of common passwords
- **Brute Force Attack:** Tries all possible character combinations

Weak passwords were successfully cracked using dictionary attacks, proving their vulnerability.

8. Why Weak Passwords Fail

- Predictable patterns (123456, password)
- Short length
- Lack of symbols and mixed characters
- Reuse across multiple platforms

9. Multi-Factor Authentication (MFA)

MFA adds an extra layer of security by requiring:

- Something you know (password)
- Something you have (OTP, mobile)
- Something you are (biometrics)

Even if a password is compromised, MFA prevents unauthorized access.

10. Recommendations for Strong Authentication

- Use passwords with at least **12 characters**
- Combine **uppercase, lowercase, numbers, and symbols**
- Avoid personal information
- Enable **MFA** wherever possible
- Use a **password manager**
- Never reuse passwords across platforms

12. Final Outcome

This task provided hands-on knowledge of password security, common attack techniques, and defensive mechanisms. It emphasized the importance of strong passwords and multi-factor authentication in modern cybersecurity systems.