Task 4: Password Security & Authentication Analysis

1. How Passwords Are Stored (Hashing vs Encryption)

- **Hashing** converts a password into a fixed-length value (hash).
  - One-way process (cannot be reversed).
  - Used for storing passwords securely.
- **Encryption** converts data into unreadable form but **can be reversed** using a key.
  - Used for data protection, **not ideal for passwords**.

Example
Password: admin123
Hashed value (MD5): 0192023a7bbd73250516f069df18b500

---

2. Types of Password Hashes

- **MD5** – Very fast, weak, easily cracked
- **SHA-1** – Better than MD5 but broken
- **SHA-256** – Stronger but fast (needs salt)
- **bcrypt** – Slow and secure, best for passwords .

---

3. Generating Password Hashes

Hashes can be generated using:

- Linux tools (openssl)
- Online hash generators
- Security tools like **Hashcat**

Example

```
echo -n password | md5sum
```

---

4. Cracking Weak Password Hashes

- Weak hashes can be cracked using:
  - **Wordlists** (common passwords)

    - **Rainbow tables**
- Tools:
    - Hashcat
    - John the Ripper

Example

- Hash: 5f4dcc3b5aa765d61d8327deb882cf99
- Result: password

---

5. Brute Force vs Dictionary Attacks

Attack Type	Description
Brute Force	Tries all combinations (slow but guaranteed)
Dictionary	Uses known password lists (fast and effective)

---

6. Why Weak Passwords Fail

Weak passwords:

- Are short
- Use common words
- Reuse passwords

Examples of weak passwords

- 123456
- password
- admin

These are found easily in wordlists.

---

7. Multi-Factor Authentication (MFA)

MFA adds an extra security layer:

- Password + OTP

- Password + fingerprint
- Password + security key

Even if a password is stolen, MFA **blocks attackers**.

---

8. Recommendations for Strong Authentication

- Use long passwords (12+ characters)
- Combine letters, numbers, symbols
- Use unique passwords for each site
- Enable MFA
- Use password managers

Password Security Analysis Report

Introduction

Password security is a critical part of cybersecurity. Weak passwords are one of the main reasons for data breaches. This report explains how passwords are stored, attacked, and protected.

Password Storage

Passwords should always be stored as hashes instead of plain text or encrypted form. Hashing ensures that even if a database is leaked, passwords cannot be easily recovered.

Password Attacks

Attackers use dictionary and brute-force attacks to crack passwords. Weak hashing algorithms like MD5 and SHA-1 make attacks easier.

Defense Mechanisms

Using strong hashing algorithms such as bcrypt, adding salts, enabling MFA, and educating users are effective defenses against password attacks.

Final Outcome

This study provides knowledge about:

- Password hashing
- Password cracking techniques

- Why weak passwords fail
- How to secure authentication systems