Task 4: Password Security & Authentication Analysis

1. Learn how passwords are stored (hashing vs encryption)

Hashing

- Converts password into a fixed-length value (hash)
- One-way process (cannot be reversed)
- Used for password storage

Encryption

- Two-way process
- Can be decrypted using a key
- Used for data transmission, not passwords

2. Identify different hash types

- MD5, SHA-1,SHA-256, bcrypt,Argon2.

Hash Type	Security
MD5	Very Weak
SHA-1	Weak
SHA-256	Medium
Bcrypt	Strong
Argon2	Very Strong

3. Generate password hashes

Step 1: Generate a Password Hash (Linux)

Open terminal:

```
echo -n "password123" | md5sum
```

Output:

377ffddcf3a279ae4d77de1d0235ab08

Step 2: Identify Hash Type

Use:

https://www.tunnelsup.com/hash-analyzer/

Paste hash → It tells **MD5 / SHA-1 / SHA-256**

4. Attempt cracking weak hashes using wordlists.

Step 1: Crack Weak Hash (John the Ripper)

Install:

sudo apt install john

Create hash file:

nano hash.txt

Paste hash:

377ffddcf3a279ae4d77de1d0235ab08

Run attack:

john hash.txt

If password is weak, it cracks and generates the hashes.

5. Understand brute force vs dictionary attacks.

Dictionary Attack

- Uses common passwords list
- Faster

Brute Force Attack

- Tries all combinations
- Slow but effective

6. Analyze why weak passwords fail.

- Short length
- Common words (password, admin, 123456)
- No special characters
- Reused passwords

7. Study MFA and its importance.

MFA(Multi-Factor Authentication)

MFA = More than one verification

Examples:

- Password + OTP
- Password + Fingerprint
- Password + Authenticator App

8.Write recommendations for strong authentication.

- At least 12 characters
- Uppercase + lowercase
- Numbers + symbols
- Not reused