Task 4: Password Security & Authentication Analysis

1️⃣Understand How Passwords Are Stored

(Hashing vs Encryption)

Hashing

- One-way process (cannot be reversed).
- Same input → same output.
- Used for password storage.
- Examples: **MD5, SHA-1, SHA-256, bcrypt**

Encryption

- Two-way process (can be decrypted).
- Used for data confidentiality, **not passwords**.

📌 **Conclusion to write**:

> Passwords should always be **hashed, not encrypted**, because hashing prevents password recovery even if the database is leaked.

2️⃣Identify Different Hash Types

You can identify hashes by:

- **Length**
- **Format**
- **Prefix**

Hash Type	Length	Example
MD5	32 chars	`5f4dcc3b5aa765d61d8327deb882cf99`
SHA-1	40 chars	`356a192b7913b04c54574d18c28d46e6395428ab`
bcrypt	60 chars	`$2b$12$eImiTXuWVxfM37uY4JANjQ==`

📌 Tool:

- Hashcat
- John the Ripper
- Online hash identifier

3️⃣ Generate Password Hashes

Example passwords:

```
password123
admin123
welcome
```

You can generate hashes using:

- Linux `openssl`
- Python
- Online generators

Example (MD5):

`password123 → 482c811da5d5b4bc6d497ffa98491e38`

📌 **Add this to your report as a demonstration.**

4️⃣ Crack Weak Password Hashes (Dictionary Attack)

Method:

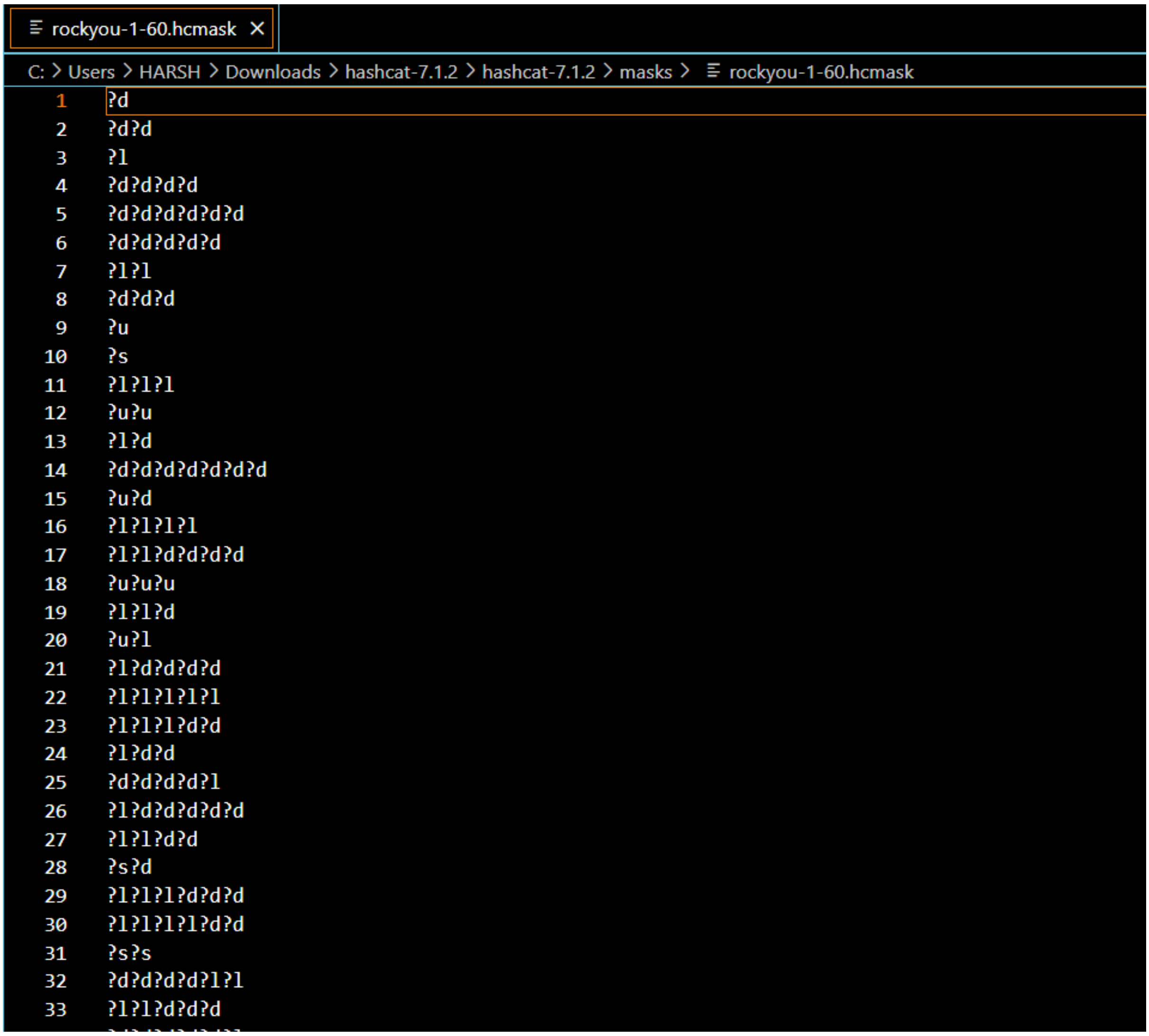
- Use **wordlist attack**
- Common wordlist: `rockyou.txt`

Tools:

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

Example explanation:

Using a dictionary attack, common passwords like `password123` were cracked within seconds, showing the weakness of predictable passwords.


rockyou-1-60.hcmask
C: > Users > HARSH > Downloads > hashcat-7.1.2 > hashcat-7.1.2 > masks > rockyou-1-60.hcmask

```
?d
?d?d
?l
?d?d?d?d
?d?d?d?d?d?d
?d?d?d?d?d
?l?l
?d?d?d
?u
?s
?l?l?l
?u?u
?l?d
?d?d?d?d?d?d?d
?u?d
?l?l?l?l
?l?l?d?d?d?d
?u?u?u
?l?l?d
?u?l
?l?d?d?d?d
?l?l?l?l?l
?l?l?l?d?d
?l?d?d
?d?d?d?d?l
?l?d?d?d?d?d
?l?l?d?d
?s?d
?l?l?l?d?d?d
?l?l?l?l?d?d
?s?s
?d?d?d?d?l?l
?l?l?d?d?d
```

⚠️ **Important**:
You only **explain the process**, not perform illegal cracking.

5️⃣ Brute Force vs Dictionary Attack

Attack Type	Description	Speed

Dictionary	Uses known passwords	Fast
Brute Force	Tries all combinations	Slow

📌 Write:

Dictionary attacks are more efficient against weak passwords, while brute force attacks are computationally expensive but guaranteed over time.

6️⃣ Why Weak Passwords Fail

Reasons:

- Short length
- Common words
- No symbols
- Reused passwords

Example:

```
admin
123456
password
```

📌 Conclusion:

Weak passwords can be cracked quickly due to limited entropy and predictable patterns.

7️⃣ Multi-Factor Authentication (MFA)

What is MFA?

- Password + OTP / biometric / security key

Why MFA is important:

- Even if password is stolen, attacker cannot log in.

Examples:

- OTP via SMS
- Authenticator apps
- Fingerprint / Face ID

📌 Write:

> MFA significantly reduces account compromise even when passwords are leaked.

8️⃣ Recommendations for Strong Authentication

Include these points:

✔ Use bcrypt / Argon2
✔ Minimum 12–16 character passwords
✔ Use symbols, numbers, uppercase
✔ Enable MFA

✔ Prevent password reuse
✔ Implement rate limiting