■■ Task 4: Password Security & Authentication Analysis

1. Introduction

This report details the mechanics of password storage, the practical application of password cracking tools, and the implementation of strong authentication defenses. The goal is to demonstrate how weak security configurations lead to system compromises.

2. Hashing vs. Encryption

It is a common misconception that passwords are encrypted. In professional security, passwords should be hashed.

Feature	Hashing	Encryption
Process	One-way (Non-reversible)	Two-way (Reversible)
Logic	Data is turned into a fixed fingerprint	Data is locked with a key
Use Case	Verifying passwords	Protecting private data files

Why Hashing?
When a user logs in, the system hashes the entered password and compares it to the hash stored in the database. If they match, access is granted. The system never needs to know the actual plaintext password.

3. Common Hash Types

- **MD5:** Very fast but now considered broken and vulnerable.
- **SHA-1:** An older standard no longer secure against advanced attacks.
- **bcrypt:** A slow algorithm designed for secure password storage.

4. Attack Methodology & Tool Analysis

A. Dictionary Attack (Using Hashcat)

- **Tool Command:** hashcat -m 0 -a 0 hash.txt rockyou.txt
- **Mechanism:** Hashes each word in the wordlist and compares it.
- **Finding:** Common passwords are cracked instantly.

B. Brute Force Attack (Using John the Ripper)

- **Tool Command:** john --incremental --format=raw-md5 hash.txt
- **Mechanism:** Tries all possible character combinations.
- **Finding:** Time increases exponentially with password length.

5. Why Weak Passwords Fail

- **Length:** Short passwords are cracked quickly.
- **Commonality:** Common passwords appear first in wordlists.
- **Reuse:** One breach compromises multiple accounts.

6. Strong Authentication Recommendations

- **Multi-Factor Authentication (MFA):** Adds an extra security layer.
- **Modern Algorithms:** Use bcrypt or Argon2.

- **Password Length:** Minimum of 12 complex characters.
- **Password Managers:** Ensure unique passwords for every account.

7. Conclusion

This analysis proves that weak passwords and outdated hashing algorithms can be compromised in seconds. Implementing MFA and modern password hashing techniques is essential to protect user data from dictionary and brute-force attacks.