Task 04: Password Security & Authentication Analysis

By : NROUPSINH GOHIL

1. Introduction

Passwords are the most common method of authentication used in digital systems. This task focuses on understanding how passwords are stored, how attackers crack weak passwords, and what security mechanisms are used to protect user accounts.

---

2. Hashing vs Encryption

Hashing

Hashing is a **one-way process** used to convert a password into a fixed-length value called a hash. The original password **cannot be recovered** from the hash.

- Used for storing passwords
- Irreversible
- Example algorithms: MD5, SHA-1, bcrypt

Encryption

Encryption is a **two-way process** where data can be converted back to its original form using a key.

- Used for protecting data in transit or storage
- Reversible using a secret key
- Not recommended for password storage

Conclusion: Passwords should always be stored using hashing, not encryption.

---

3. Types of Hashing Algorithms

MD5

- Produces a 32-character hash
- Very fast and insecure
- Easily cracked using dictionary attacks

Example:
Password: admin
MD5 Hash: 21232f297a57a5a743894a0e4a801fc3

SHA-1

- Produces a 40-character hash
- More secure than MD5 but now broken

- Not recommended for password storage

---

bcrypt

- Designed specifically for passwords
- Uses salting and multiple rounds
- Slow and resistant to brute force attacks
- Considered secure

---

4. Generating Password Hashes

Password hashes were generated using online hash generators by entering simple passwords and observing their MD5 and SHA-1 outputs. This demonstrates how plaintext passwords are converted into irreversible hash values before storage.

---

5. Cracking Weak Hashes Using Wordlists (Online Hash Identifier)

Weak password hashes were tested using **online hash identifier tools**. These tools identify the hash type and compare it against common password wordlists.

Example:
MD5 Hash: 21232f297a57a5a743894a0e4a801fc3
Cracked Password: admin

This proves that weak passwords present in common wordlists can be cracked easily.

---

6. Brute Force vs Dictionary Attacks

Dictionary Attack

- Uses a predefined list of common passwords
- Very fast
- Effective against weak passwords

Brute Force Attack

- Tries all possible combinations
- Slower but guaranteed to succeed eventually
- Ineffective against long and complex passwords

---

7. Why Weak Passwords Fail

Weak passwords fail due to:

- Short length
- Common usage
- Predictable patterns
- Presence in leaked password databases
- Lack of salting

Once cracked, the same password can be reused to access multiple accounts.

---

8. Multi-Factor Authentication (MFA)

Multi-Factor Authentication adds an extra layer of security by requiring more than one verification method, such as:

- Password (something you know)
- OTP or mobile device (something you have)
- Biometrics (something you are)

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

---

9. Recommendations for Strong Authentication

- Use long and complex passwords
- Avoid password reuse
- Enable MFA on all important accounts
- Use password managers
- Avoid common patterns and predictable passwords

---

10. Conclusion

This task demonstrates how weak password practices expose systems to attacks and how strong hashing algorithms, MFA, and proper password hygiene can significantly improve authentication security.