Cyber Security Internship Report

Cyber Security Internship – Task 4

Password Security Analysis Report

Submitted by: Hetal Antala

Date : 20 / 01 / 2026

1. Introduction

Passwords are the most widely used authentication mechanism in digital systems.

However, weak password practices expose systems to unauthorized access and cyberattacks.

This report analyzes how passwords are stored, common password attack techniques,

and the importance of strong authentication mechanisms such as Multi-Factor Authentication (MFA).

2. What is hashing ?

Hashing is a cryptographic process that converts plain-text data into a fixed-length

string called a hash. Hashing is a one-way function, meaning the original data cannot

be retrieved from the hash. Password hashing ensures that actual passwords are never

stored in plain text.

3. Difference Between Hashing and Encryption

Hashing	Encryption
One-way process	Two-way process
Cannot be reversed	Can be decrypted using a key
Used for password storage	Used for data confidentiality
Example: MD5, SHA-1	Example: AES, RSA

---

4. Common Hash Types

****MD5**:** Fast but insecure and vulnerable to attacks.

****SHA-1**:** More secure than MD5 but now considered weak.

****bcrypt**:** Slow and secure; recommended for password storage due to salting and key stretching.

---

5. Password Cracking Techniques

5.1 Dictionary Attack

A dictionary attack uses a predefined list of commonly used passwords to attempt to match password hashes. Weak and commonly used passwords are easily cracked using this method.

5.2 Brute Force Attack

A brute force attack attempts every possible combination of characters until the correct password is found. While effective, it is time-consuming and computationally expensive.

---

6. Practical Demonstration

- In this task, password hashes were generated using MD5 and SHA-1 algorithms.
- John the Ripper was used to perform a dictionary attack on these hashes using a custom wordlist.

- Weak passwords were successfully cracked, demonstrating the vulnerability of poor password choices.

---

7. Why Weak Passwords Fail

Weak passwords fail because:

- They are short and predictable
- They use common words or patterns
- They are reused across multiple platforms
- They lack complexity

Such passwords can be cracked quickly using automated tools.

---

8. Multi-Factor Authentication (MFA)

Multi-Factor Authentication adds an additional layer of security by requiring multiple forms of verification such as:

- Something you know (password)
- Something you have (OTP, authenticator app)
- Something you are (biometrics)

MFA significantly reduces the risk of account compromise even if passwords are leaked.

---

9. Recommendations for Strong Authentication

- Use long and complex passwords
- Avoid password reuse
- Store passwords using bcrypt or Argon2
- Enable Multi-Factor Authentication

- Implement account lockout policies
- Educate users on password hygiene

---

10. Conclusion

This analysis demonstrates that weak passwords pose a serious security risk.

Using strong hashing algorithms and enabling Multi-Factor Authentication are essential defenses against password-based attacks. Organizations must adopt secure authentication practices to protect user data effectively.
