CYBER SECURITY INTERNSHIP

Task 4 : Password Security & Authentication Analysis

Name: Jeffrina V
Internship Organization: Elevate Labs
Domain: Cyber Security
Task: Task 4
Date: 20 January 2026

PASSWORD SECURITY & AUTHENTICATION ANALYSIS

1. Introduction

Passwords are the most commonly used method for user authentication. However, weak passwords can easily be compromised using various attack techniques. This report analyzes password security, different hashing methods, password attack techniques, and the importance of strong authentication mechanisms.

2. Hashing vs Encryption

Hashing and encryption are two different techniques used to protect data.

Hashing is a one-way process where a password is converted into a fixed-length hash value. The original password cannot be retrieved from the hash.

Encryption is a two-way process where data can be encrypted and later decrypted using a key.

Passwords are always stored using hashing, not encryption, to improve security.

3. Common Password Hash Types

Different hash algorithms are used to store passwords:

- **MD5:** Fast and outdated, vulnerable to attacks.
- SHA-1: More secure than MD5 but still weak.
- **Bcrypt:** Slow and secure, widely used.
- Argon2id: Modern and highly secure, resistant to brute-force attacks.

4. Password Hash Generation

Passwords such as 123456, password123, and P@ssW0rd!9X#24 were tested using an online hash generator. The generator produced MD5 and SHA-1 hashes for each password.

Example:

Password: 123456

MD5 Hash: e10adc3949ba59abbe56e057f20f883e

5. Password Attacks

Two common password attack techniques are:

Dictionary Attack

This attack uses a predefined list of common passwords. If the password exists in the list, it can be cracked quickly.

Brute Force Attack

This attack tries all possible combinations of characters. It is slower but effective against short or simple passwords.

6. Weak Password Analysis

Passwords like 123456 and password123 are considered weak because:

- They are short and predictable
- They are commonly used
- They lack special characters
- Their hashes can be easily identified and reversed using online tools

This makes them vulnerable to dictionary and brute-force attacks.

7. Strong Password Analysis

The password P@ssW0rd!9X#24 is considered a strong password because:

✔ It is longer than 12 characters

✔ It contains uppercase letters, lowercase letters, numbers, and symbols

✔ It does not follow a predictable pattern

✔ Its hash cannot be easily reversed

Even though MD5 is weak, the password itself is strong due to its complexity.

8. Multi-Factor Authentication (MFA)

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

▯ Password + OTP

▯ Password + biometric verification

▯ Password + authenticator app

MFA prevents unauthorized access even if the password is compromised.

9. Recommendations for Strong Authentication

- Use passwords with at least 12–16 characters
- Include uppercase, lowercase, numbers, and symbols
- Avoid common words and personal information
- Use secure hashing algorithms like bcrypt or Argon2
- Enable Multi-Factor Authentication
- Use password managers to store passwords securely

10. Conclusion

Weak passwords are a major security risk and can be easily cracked using simple attack techniques. Strong passwords combined with secure hashing algorithms and Multi-Factor Authentication significantly improve system security. Proper password policies are essential to protect user accounts and sensitive information.

Final Outcome

This task provided practical knowledge about password hashing, password attack methods, weak and strong password identification, and modern authentication defenses.