

Password Analysis Challenge

1. Decrypting the Encrypted Passwords

The encrypted passwords appear to be MD5 hashes. Here's the decrypted output:

1. 5f4dcc3b5aa765d61d8327deb882cf99** → ` password
2. 6cb75f652a9b52798ee0e17941b2c76b** → ` 123456
3. d8578edf8458ce06fbc5bb76a58c5ca4** → qwerty

2. Analyzing Password Strength

Extracted Passwords:

- Password
- 123456
- Qwerty

Strength Analysis:

- Weaknesses:
 - All three passwords are extremely weak and commonly used.
 - They lack complexity (use of uppercase letters, special characters, and numbers).
 - They are short in length, making them easier to crack.

Potential Vulnerabilities:

-Common Passwords: These passwords are easily guessable and are likely found in password databases, making them susceptible to dictionary attacks.

-No unique password :They lack variety, which reduces entropy and increases predictability.

3. Suggestions to Improve Password Strength

To enhance password security, consider the following methods:

1. Aim for at least 12-16 characters.
2. Include a mix of uppercase and lowercase letters, numbers, and special characters.
3. Refrain from using easily guessable passwords such as "password," "123456," or keyboard patterns like "qwerty."
4. Create a memorable phrase or a combination of unrelated words.
5. Use a password manager to generate and store complex passwords securely.
6. Implement second factor security to provide an additional layer of security beyond just the password.

Conclusion:

Understanding how to decrypt and analyze passwords highlights the importance of using strong, unique passwords and employing best practices for password management. By implementing the suggested methods, users can significantly enhance their security posture against potential attacks.