Goldman Sachs - Virtual Internship

Date: 19-08-2024 **Day:** Monday

Overview

In this assessment, I analysed and cracked several leaked passwords using the Hashcat tool. The passwords were hashed using the MD5 algorithm, a widely known but outdated and insecure method. The following are the results of my findings:

Cracked Passwords

- e10adc3949ba59abbe56e057f20f883e: 123456
- d8578edf8458ce06fbc5bb76a58c5ca4: qwerty
- 3f230640b78d7e71ac5514e57935eb69: qazxsw
- fcea920f7412b5da7be0cf42b8c93759: 1234567
- f6a0cb102c62879d397b12b62c092c06: bluered
- 5f4dcc3b5aa765d61d8327deb882cf99: password
- 8d763385e0476ae208f21bc63956f748: moodie00
- 25f9e794323b453885f5181f1b624d0b: 123456789

Hashing Algorithm and Protection Level

- The passwords were hashed using the MD5 algorithm. MD5 is a poor choice for password hashing due to its speed and efficiency, which allows attackers to compute the hash of a large number of passwords in a short amount of time. As a result, MD5 provides minimal protection against password cracking.

Recommendations for Improved Password Security

1. **Use Stronger Hashing Algorithms**: Replace MD5 with stronger algorithms like SHA-256 or bcrypt. These algorithms are more secure and less susceptible to cracking.

2. **Implement Salting**: Always use salts with hashes where feasible. Salting adds a unique value to each password before hashing, making it more difficult for attackers to crack passwords using precomputed hash tables (rainbow tables).

Observations on Organization's Password Policy

- Weak Hash Functions: The use of MD5 without salting is a significant vulnerability.

- Common Passwords: Many users employ simple, common passwords that are easily guessed or cracked.
- Lack of Complexity: The passwords lack a combination of capital letters, numbers, and special symbols, making them less secure.

Suggested Changes to Password Policy

1. Increase Password Length: Require a minimum password length of 12 characters. Longer passwords are harder to crack using brute-force attacks.

2. Avoid Common Phrases: Discourage the use of common phrases or simple patterns as passwords. Instead, enforce the use of mixed characters, including uppercase, lowercase, numbers, and special symbols.

3. Utilize Password Strength Checkers: Encourage users to check their password strength using password strength checker tools and websites to ensure they create robust passwords.

Summary

The current password security practices, especially the use of MD5 without salting and reliance on common passwords, present significant vulnerabilities. By implementing stronger hashing algorithms, enforcing password complexity, and increasing password length, the organization can greatly enhance its password security and reduce the risk of unauthorized access.

- Vishwas Chakilam