This report analyzes the results of a password hashing vulnerability and explores methods to strengthen password security.

**Hashing Algorithm and Protection Level:**

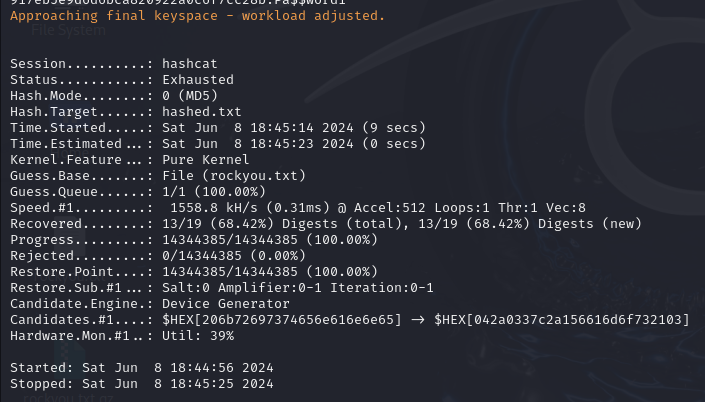
Using hash-identifier, I could identify the type of hashed password. MD5 is outdated and considered weak due to their susceptibility to brute-force attacks. Modern algorithms like bcrypt and Argon2id are much stronger due to techniques like salting (adding random data) and adjustable work factors (increasing the time needed to crack a hash).

**Insights from Cracked Passwords:**

The number of cracked passwords suggests potentially weak password policies. Short passwords with limited character types are easier to crack. Key space refers to the total number of possible password combinations. Enforcing password length requirements and character diversity (uppercase, lowercase, numbers, symbols) exponentially increases the key space, making brute-forcing much harder. It is observed that sequential keyboard patterns that hackers often try during password cracking attempts. They are easily guessable and offer minimal security. Repetitive Characters makes it very weak and vulnerable to guessing.

**Recommendations for Stronger Password Policy:**

* **Minimum Password Length:** Enforce a minimum password length of 12-14 characters.
* **Character Diversity:** Require passwords to include a combination of uppercase, lowercase, numbers, and symbols.
* **Password Disallowances:** Disallow common dictionary words, keyboard patterns, and personal information (birthdays, names) in passwords.
* **Multi-Factor Authentication:** Implement multi-factor authentication (MFA) as an additional security layer. MFA requires a second verification factor besides the password, significantly reducing the risk of unauthorized access.



A screenshot of a computer screen

Description automatically generated

1. experthead:e10adc3949ba59abbe56e057f20f883e 🡪 **123456**
2. interestec:25f9e794323b453885f5181f1b624d0b🡪 **123456789**
3. ortspoon:d8578edf8458ce06fbc5bb76a58c5ca4 🡪 **qwerty**
4. reallychel:5f4dcc3b5aa765d61d8327deb882cf99 🡪 **password**
5. simmson56:96e79218965eb72c92a549dd5a330112 🡪 **111111**
6. bookma:25d55ad283aa400af464c76d713c07ad 🡪 **12345678**
7. popularkiya7:e99a18c428cb38d5f260853678922e03 🡪 **abc123**
8. eatingcake1994:fcea920f7412b5da7be0cf42b8c93759 🡪**1234567**
9. heroanhart:7c6a180b36896a0a8c02787eeafb0e4c 🡪 **password1**
10. edi\_tesla89:6c569aabbf7775ef8fc570e228c16b98 🡪 **password!**
11. liveltekah:3f230640b78d7e71ac5514e57935eb69 🡪**qazxsw**
12. blikimore:917eb5e9d6d6bca820922a0c6f7cc28b 🡪 **Pa$$word1**
13. johnwick007:f6a0cb102c62879d397b12b62c092c06🡪 **bluered**