**Password Cracking Exercise Report**

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

**Exercise Objective**

The goal of this exercise was to crack the following password hashes using any preferred tool or method:

* 5f4dcc3b5aa765d61d8327deb882cf99
* e99a18c428cb38d5f260853678922e03
* 8d3533d75ae2c3966d7e0d4fcc69216b
* 0d107d09f5bbe40cade3de5c71e9e9b7
* 5f4dcc3b5aa765d61d8327deb882cf99 *(duplicate)*

**Tool Used**

John the Ripper – A widely known password-cracking tool.

**Steps Performed**

1. Hash File Preparation
   * Saved all hashes in a text file named hashes.txt.
2. Running John the Ripper
   * Executed the following command:

john --format=Raw-MD5 --incremental hashes.txt

* + Command Breakdown:
    - --format=Raw-MD5: Specifies the hash format (MD5 in this case).
    - --incremental: Performs a brute-force attack, testing all possible character combinations.

1. Displaying Cracked Passwords
   * After completion, the following command was used to show the results:

john --show --format=Raw-MD5 hashes.txt

* + This displayed each hash alongside its cracked plaintext password.

**Results**

John the Ripper successfully cracked all provided hashes. The findings were:

* 5f4dcc3b5aa765d61d8327deb882cf99 → password
* e99a18c428cb38d5f260853678922e03 → abc123
* 8d3533d75ae2c3966d7e0d4fcc69216b → charley
* 0d107d09f5bbe40cade3de5c71e9e9b7 → letmein
* 5f4dcc3b5aa765d61d8327deb882cf99 → password *(duplicate, already cracked)*

**Conclusion**

Using John the Ripper with an incremental brute-force attack proved highly effective in cracking all provided MD5 hashes. This exercise highlights:

* The vulnerability of weak hashing algorithms like MD5.
* The importance of using stronger password storage methods (e.g., bcrypt, Argon2).
* The necessity of enforcing complex passwords to resist brute-force attacks.