Computer Science Department
University of Crete

CS-455: Password Cracking
Spring 2022 - 2023

Assignment 3
Password Cracking

Uploaded: 19/03/2023
Deadline: 02/04/2023

Introduction

In this assignment you will learn about different types of password encryption and hashing and also how to crack them.

Notes

- For every question, you need to provide all the necessary commands used with adequate explanation of the command and the relevant result/output.
- **To demonstrate your work, use screenshots extensively**!
  Useful tools: hashID, John The Ripper (JTR), hashcat, crackstation, cupp, Mentalist.

Questions

1. **[10%] Hash Identification**
   - You are given the following hashes:
     - 491fe2ec1b129dc19210e65931f4c23f
     - 1a7f2a5ad77128b2f81feddac78df213
     - ec65a740f5a00cafe7c7fb6de725fe369c87f0de
   - For the above hashes use hashID to identify the type of the hash.

2. **[10%] Hash Cracking**
   - Based on what you learned from Q1 (i.e., the hash algorithm used), crack the same hashes using JTR or hashcat.

- You can use crackstation afterwards to check your work performed in the previous step.

3. **[20%] Cupp**
   - Based on the information listed in the annex below, use cupp to create a wordlist with candidate passwords.
   - Using the word list that you just created crack the following hash:
     - b2dc8ecffffcea20441ff72290dd9684
   - For the cracking step use either JTRor hashcat.

4. **[20%] Mentalist**
   - Based on the wordlist created in Q3, use mentalist to produce a larger one.
   - Use the following two rules: (a) append one digit number at the end of each word, (b) change every candidate password so that it starts with an uppercase letter while the rest of the characters are lowercase.
   - Use the new wordlist to crack the following hash:
     - 0f0859c50d27cb7bfd41854245df2b95
   - For the cracking step use either JTR or hashcat.

5. **[20%] Cracking a rar password**
   - Find the password the flag.txt.rar file is encrypted with.
   - Describe the process you followed and list the contents of the file.
   - For the cracking step use either JTR or hashcat and rockyou.txt

6. **[20%] Cracking based on known patterns**
   - Configure JTR to search for specific patterns, for example passwords that are exactly N (e.g. 8) characters long and are composed only of numbers (0, …, 9).
   - Demonstrate JTR's configuration is correct by creating such a password and then cracking it.

7. **[5%] BONUS**
   - Demonstrate how to speed up hashcat or JTR's performance by using a GPU, multiple cores or other techniques.

Submission

- Submit a pdf document including all the information requested above.
- Submissions will be done through eLearn.
- This assignment is an individual creative process and students must submit their own work. You are not allowed, under any circumstances, to copy another person's work. You must also ensure that your work won't be accessible to others.
- You are encouraged to post any questions you may have in the eLearn forum. If however you believe that your question contains part of the solution or spoilers for the other students you can communicate directly with the course staff at hy455@csd.uoc.gr.

Annex

Name: john
Last Name: arakas
Nickname: jhot
Birthday: 26/11/1998

Disclaimer

It is **ILLEGAL** to attempt any type of attack against a target (individual, network, public/private entity, etc.) without authorization / explicit permission. Such actions are **prohibited and punished by law and university policies**.