Stony Brook University

CSE331: Computer Security Fundamentals

Assignment 2: Access Control

In this assignment, you will implement a password cracker!

Notes

- The password database will be provided to your program as a CSV file. The structure of the CSV file will be the following:

```
USERNAME1, PASSWORD1, SALT1
USERNAME2, PASSWORD2, SALT2
…
USERNAMEnm PASSWORDn, SALTn
```

- For output, your code should create a new file named task#.csv (where # is the task number) with the following format:

```
USERNAME1, PASSWORD1
USERNAME2, PASSWORD2
…
USERNAMEn, PASSWORDn
TOTALTIME [seconds]
SUCCESSRATE [xx.xx%]
```

- Assume the passwords only contain lowercase and uppercase English letters or numbers (a-z,A-Z,0-9).
- Assume the salt is a string of length 4.
- If you were unable to crack a certain password, output "FAILED" in the corresponding line.
- The hashing algorithm used is MD5.

- When hashing with salt, assume that the system will concatenate the password and salt (i.e., PASSWORDSALT).
- Record the success rate and time taken by each method and report them in the final lines.

Task 1: Implement a brute-force password cracker

Write a program to attempt to crack a list of hashed (unsalted) passwords using brute force. Only target passwords that are no longer than four characters.

Task 2: Implement a dictionary attack

Write a program to attempt to crack a list of hashed (unsalted) passwords using this list of 10,000 common passwords.

Task 3: Implement a rainbow table

Simulate a rainbow table attack by creating a pre-computed table of hash values for common passwords and use it to crack a list of hashed (unsalted) passwords.

Task 4: Crack a salted password database

Using rainbow tables and the list of common passwords, crack a salted password database.

Task 5: Implement a hybrid password cracker

Combine the ideas from the above 4 tasks to implement a hybrid password cracker. A hybrid password cracker starts with a predefined list of common passwords and applies transformation rules to each dictionary word. These rules modify the base words by introducing common password variations that users often create to meet password complexity requirements.
The rules you should consider are:
- Adding digits to the end of the word (e.g., "password" becomes “password1"). (assume the length will be no longer than four digits)
- Replacing certain characters with numbers or symbols (e,o,t become 3,0,7).
- Changing the case of certain letters (e.g., "password" becomes "Password" or "PaSsWoRd").

What to submit

Submit a tarball to Brightspace, using your student ID number as its name (e.g. "123456789.tar.gz"). The tarball should contain:

- A report, describing your code and how you accomplished each task in PDF format titled "**report.pdf**". In the report, provide a comparison of success rate and time taken by each method.
- Your codes.
- Shell script to run each of the tasks. These files should be named "**taskN.sh**" where N is the task number (e.g., "task1.sh"). Out autograder will use these scripts to run and grade your code so make sure they are functioning correctly.

Lateness

Assigned work is due on 11:59PM on the dates listed in the class calendar. We strongly recommend that you get started early. Late submissions will be penalized by 10% of the maximum attainable score, plus an additional 10% every 4 hours until received. The instructors may grant individual extensions, but only under extraordinary circumstances.

Collaboration

Acts of cheating, plagiarism, and unacceptable collaboration will be reported to the Academic Judiciary. Cheating is when you copy, with or without modification, someone else's work that is not meant to be publicly accessible. Plagiarism is the practice of taking someone else's work or ideas and passing them off as one's own without providing attribution. Unacceptable collaboration is the knowing exposure of your own solutions, or the use of someone else's answers or solutions.

At the same time, we encourage students to help each other learn the course material. As in most courses, there is a boundary separating these two situations. You may give or receive help on any of the concepts covered in lecture. You are allowed to consult with other students about the

conceptualization of a project, or the general approach for solving problems. However, all work, whether in scrap or final form, must be done by you.

If you have any questions as to what constitutes unacceptable collaboration or exploitation of prior work, please talk to an instructor right away. You are expected to exercise reasonable precautions to protect your own work, including not posting solutions publicly.