CS2107 Self-Exploration Activity 4

Notes:

In Activity 4, you can optionally perform the following:

1. To inspect the **password file** as well as the corresponding password shadow file in Linux.
2. To experiment with **John the Ripper** in cracking weak passwords contained in a password file.

Task 1: Inspecting Password File and the Corresponding Password Shadow File in Linux

First, you want to **investigate** the *password file* and its corresponding *password shadow file* on a Linux system.

Open your terminal, and then **print out** the content of `/etc/passwd` and `/etc/shadow` files as follows:

```
$ cat /etc/passwd
$ sudo cat /etc/shadow
```

Next, you can **create a new user** named `test`, and then set its password to `testtest` (i.e. double "`test`") by invoking the following command:

```
$ useradd -m test
```

After providing the information of the newly-added user, you can check whether the password and password shadow files now **contain** a new line for the user. Also **inspect** the user's *hashed-salted password* entry stored in the password shadow file.

Task 2: Experimenting with John the Ripper for Offline Password Cracking

To perform an offline password guessing, you can **install** John the Ripper (https://www.openwall.com/john/), which is a very popular password cracker, by running: `sudo apt-get install john`. You can refer to the following documentation page to find out how you can use John the Ripper: https://www.openwall.com/john/doc/EXAMPLES.shtml.

To crack (offline guess) the password of your newly-added user `test1`, you can first ***unshadow*** your password and password shadow files by invoking:

```
$ unshadow /etc/passwd /etc/shadow > combined.txt
```

Then, **run** John , but limit the usernames to be cracked to `test` as follows:

```
$ john --users=test combined.txt
```

Check how much time did John need to crack the set password?

You can further explore John by creating some other new users and setting their passwords with different strength, and then cracking the passwords again. To **print out all passwords** that have been cracked by John so far, you can run:

```
$ john --show combined.txt
```

Before your complete your exploration, do **delete** your unused newly-added users, for instance `test`, by invoking:

```
$ deluser test
```

Lastly, do **remove** John's *$JOHN*/`john.pot` file, which stores the cracked password information as follows:

```
$ rm ~/.john/john.pot
```