

Name: Souhardya Das Chowdhury
Roll-1801cs51

1)Implement a Honeyword Based System

Atfirst run the ib1.cpp file to implement the Honeywell Based System.

For adding users:

Give input of k(number of honeywords needed).

Then,input username and password.[count is 10.You can increase 10 to any number you want).

(I took an assumption,there are 10 users in my system.This number 10 can be changed to anything you want)

Note:Instead of hardcoding username and password,I am asking user to input it,and based on those inputs,I am creating the database.

For logging in:

Type username and password

For exit-

Press anything else

Outputs(For users add) are:

File f1.txt : It contains username and a list of honeyword set index (Contains the correct index and other k-1 shuffled,random index).

File hashFile.txt : It contains the index and corresponding hashed password.

For hashing: I used md5 hash function.

File f3.txt : It contains the index and the corresponding username of the person.

Command to run: g++ ib1.cpp -lcrypto -lssl

Execution: ./a.out

```
souhardya@souhardya-HP-Laptop-15g-dr0xxx:~/Desktop/assign2$ g++ ib1.cpp -lcrypto -lssl
souhardya@souhardya-HP-Laptop-15g-dr0xxx:~/Desktop/assign2$ ./a.out
Type 1 for adding 10 users
Type 2 for logging in
Any other number to exit
1
Please enter the number of honeywords to be generated : 6
I have taken 10 users.Now in order to create the username and password file,enter 10 usernames and 10 passwords
Format : Username Password
Ram Ramshyan
Shyam Shyam56789
Jadu 123456yytfyt
Madhu Beyonce1qw
Souhardya Agartala
Somenath Kolkata1
Ammaar parkcircus
Ayush kanpurup
Iitpatna BihtaPatna
Neels kolkatabehl
Type 1 for adding 10 users
Type 2 for logging in
Any other number to exit
2
Please enter username:Madhu
Please enter password:Beyonce1qw
Successfully Login

Type 1 for adding 10 users
Type 2 for logging in
Any other number to exit
2
Please enter username:Jadu
Please enter password:Agartala1a
Wrong Password.But No threat
Type 1 for adding 10 users
Type 2 for logging in
Any other number to exit
```

Fig:Run the ib1.cpp file to generate the database for honeywell.

#f1.txt: Below is the picture of f1.txt(the 1st password file,It contains the name of the user and the honeywell set).

```
Ram 6 4 8 9 1
Shyam 5 7 1 2 3
Jadu 2 6 1 3 9
Madhu 2 9 4 8 1 10
Souhardya 3 5 8 6 10 1
Somenath 3 6 9 5 8
Ammaar 1 10 7 9 2 8
Ayush 9 10 1 8 4
iitpatna 3 10 6 9 5 7
Neels 6 8 4 1 5 10 |
```

#hashCode.txt: Below is the picture of hashCode.txt(It contains the index - password hashcode).

```
|1 3437b71959824df555ebb9ed9c6668f3
2 a2eee363e6572fe186c30e1918dcd7b4
3 3adb8955c33ee0c7215aefc130e566fb
4 9ac45c27322e1d92bbdb52fcd0df3527
5 5998bb76483bff3009b18cb20a4f8cef
6 5aaf0d89d1d98ae28a4ceb455b81c556
7 16f79c8976a0ec60bd46480ee19b03ab
8 c77075958b560d8d85e4cc4485c6406b
9 1da58e1ab82662b49615d98710a39cb0
10 6cbc4c0485da54136334b158bcf954e6
```

#f3.txt:Below is the picture of f3.txt(It contains the name and index number of each user).

```
Ram 1
Shyam 2
Jadu 3
Madhu 4
Souhardya 5
Somenath 6
Ammar 7
Ayush 8
iitpatna 9
Neels 10
```

Hence,Honeywell based system is designed.[Combination of f1.txt,hashCode.txt,and f3.txt].

[[An additional file f0.txt is here,which only contains the hashed values of hashCode.txt]]

2)Here,whatever was said in question,at first I did that in order to test the John tool.

I meant atfirst do `sudo apt-get install john`

Then Change user to root

Create test folder ,and change its permission to 777 by typing:

`Cd test`

`Chmod test 777`

We download the wordlist dictionary by :

`Wget`

<http://scrapmaker.com/data/wordlists/dictionaries/rockyou.txt>
command.

Now, use `su` command and change to root. After then, create a folder named `test`. Change its permission to 777 by using `chmod` command.Now, go to `test` folder and get a wordlist dictionary. You can use the following command to get a dictionary of wordlist.

`Wget`

<http://scrapmaker.com/data/wordlists/dictionaries/rockyou.txt>

If it is available in the wordlist file then it should show the corresponding password against the username. To perform this, following command I used

Add user alice

Password: alice

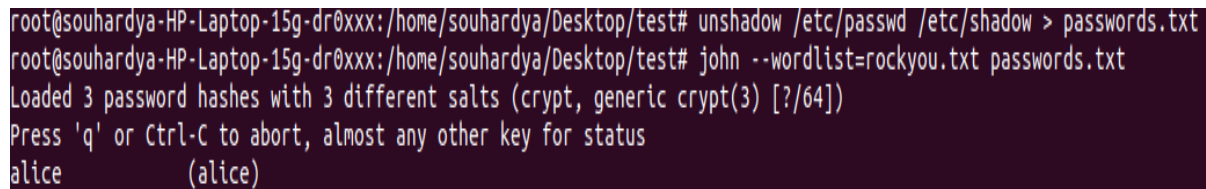
```
unshadow /etc/passwd /etc/shadow > passwords.txt
```

```
john --wordlist=rockyou.txt passwords.txt
```

In order to show the hashed password, I followed:

```
sudo john --show hashFile.txt
```

The end.



```
root@souhardya-HP-Laptop-15g-dr0xxx:/home/souhardya/Desktop/test# unshadow /etc/passwd /etc/shadow > passwords.txt
root@souhardya-HP-Laptop-15g-dr0xxx:/home/souhardya/Desktop/test# john --wordlist=rockyou.txt passwords.txt
Loaded 3 password hashes with 3 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
alice          (alice)
```

After I used `john --wordlist=rockyou.txt hashFile.txt`:

Screenshot attached below-

After I used `sudo john --show hashFile.txt`, Screen shot attached below.

Thank You.

Problems faced:

John didn't work as expected.

A lot of time, I faced errors like No hashes loaded.

Solutions:

Changed the properties of the file and made it utf-8 encoded.