

Shadows and Hashing

What I did was parsing the users' salt and hashes.

And use the salt with words in nltk.corpus to find a match with the user's hash. And print out the output. The thing I found interesting was how long it took to crack those passwords. I was cracking passwords with salt, meaning I grouped people with the same salt. And for every salt, start a new timer, the timer's unit is in seconds.

My Source code:

```
from bcrypt import hashpw
from nltk.corpus import words
import time

class User:
    def __init__(self, name, salt, hash):
        self.name = name
        self.salt = salt
        self.hash = hash

def process_user():
    users = list()
    with open('shadow.txt', 'r') as f:
        for line in f:
            name = line.split(':')[0]
            salt = line.split(':')[1][:29].encode('utf-8')
            hash = line.split(':')[1].strip().encode('utf-8')
            # print(name, salt, hash)
            users.append(User(name, salt, hash))
    return users

def crackPassword(users):
    word_combination = [w.encode("utf-8") for w in words.words() if len(w) >=6 and len(w) <= 10]
    user_map = dict()
    for user in users:
        if user.salt in user_map.keys():
            user_map[user.salt].append(user)
        else:
            user_map[user.salt] = [user]

    for salt in user_map.keys():
        st = time.time()
```

```

for word in word_combination:
    hash_pass = hashpw(word, salt)
    for user in user_map[salt]:
        if hash_pass == user.hash:
            et = time.time()
            print(f'{user.name} password: {str(word)} time: {et-st}')

if __name__ == '__main__':
    users = process_user()
    crackPassword(users)

```

My output:

```

○ hanktsai@Hanks-MacBook-Air Lab4 % python3 shadow.py
Thorin password: b'diamond' time: 4371.018795967102
Bilbo password: b'welcome' time: 8250.74572300911
Gandalf password: b'wizard' time: 8279.887720823288
Fili password: b'desire' time: 3816.0317418575287
Kili password: b'ossify' time: 8446.742583036423
Fili password: b'desire' time: 12543.101666927338
Dwalin password: b'drossy' time: 2082.8579881191254
Balin password: b'hangout' time: 4911.648394823074
Oin password: b'ispaghul' time: 5383.666654825211
Dori password: b'indoxylic' time: 14329.950358867645
Gloin password: b'oversave' time: 26599.65172290802
Nori password: b'swagsman' time: 40877.956803798676
Ori password: b'airway' time: 1068.820188999176
Bifur password: b'corrosible' time: 15898.028846263885
Bofur password: b'libellate' time: 34148.89047908783

```