Network Security HW1: Password Cracking

Due: Thursday, March 15 at 11:59 PM

2171056 강승연

프로그램 구조

crack_salt.py 파일을 실행시켜 salt를 찾은 뒤 salt.txt에 저장한다.

crack_program.py 을 실행시켜 salt.txt에 저장된 salt 로 pw를 crack한다.

Crack한 salt 값 : n5ec

crack_salt.py

```
8   #txt 파일 파싱
9   cwd = os.getcwd()
10  filepath_hashed = os.path.join(cwd, '1MillionPassword_hashed.txt')
11  filepath_wordlist = os.path.join(cwd, '1MillionPassword_wordlist.txt')
12
13  df = pd.DataFrame(columns= ['hash', 'word'])
14
15  hashed_f = open(filepath_hashed)
16  wordlist_f = open(filepath_wordlist)
17  hash_list = []
18  word_list = []
19
20  for line in hashed_f.readlines():
21      line = line.replace('\n', '')
22      hash_list.append(line)
23
24  for line in wordlist_f.readlines():
25      line = line.replace('\n', '')
26      word_list.append(line)
```

Txt 파일을 파싱 후 리스트로 변한한다

```python
#salt 찾기
chars = list(string.ascii_lowercase) + list(string.digits)
length = 4

salts = itertools.product(chars, repeat=length)
ans_salt = 0

for salt in salts:
    word_salt = word_list[0]+''.join(salt)
    print(word_salt+"에 대응하는 해시 찾는중")
    word_salt = word_salt.encode('utf-8')
    md5 = hashlib.md5()
    md5.update(word_salt)
    hash_salt = md5.hexdigest()
    if hash_list[0] == hash_salt:
        ans_salt = ''.join(salt)
        break

print(ans_salt)
```

Salt를 찾는다.

1. 가능한 모든 salt 경우의 수를 리스트로 저장한다.
2. 가능한 모든 salt 경우의 수에 대하여, word에 salt를 붙인 뒤 이를 해싱해 해시값과 비교한다.
3. 일치할 시 해당 salt값을 salt 로 간주한다.

이 과정에서 word 파일의 맨 위 단어와 hash 파일의 맨 위 해시 값이 일치할 것을 가정한다.

```
123456n5d9에 대응하는 해시 찾는중
123456n5ea에 대응하는 해시 찾는중
123456n5eb에 대응하는 해시 찾는중
123456n5ec에 대응하는 해시 찾는중
n5ec
```

crack_program.py

```python
#import
import os
import hashlib
```

os는 파일 오픈을 위해, hashlib 는 해싱을 위해 import 한다.

```
#저장된 salt 불러오기
cwd = os.getcwd()
salt_file = "salt.txt"

file = open(salt_file, 'r')
salt = file.read()
file.close()
```

저장된 salt를 불러온다.

```
13  #pw 파일 열기
14  filepath_wordlist = os.path.join(cwd, '1MillionPassword_wordlist.txt')
15  wordlist_f = open(filepath_wordlist)
16
17  #crack
18  idx = 1
19  for line in wordlist_f.readlines():
20    pw = line.replace('\n', '')
21    word_salt = pw+''.join(salt)
22    pw_encode = word_salt.encode('utf-8')
23    md5 = hashlib.md5()
24    md5.update(pw_encode)
25    hash = md5.hexdigest()
26    print(str(idx)+'/'+'1000000 password has been cracked, hashed: '+hash+', cracked: '+str(pw))
27    idx += 1
```

pw 파일을 연 뒤 salt를 붙여 crack한다.