**Gotta Catch em All**

***Password Cracking***

**Challenge:**

Our team has found a set of encrypted messages. They seemed to have figured out that the passwords consists of a pokemon followed by some numbers. Can you decrypt them?

Hashes:

fbf5496a008165f6db865a23b3da8d89

8d4244cb30f5aff30b2327eb439dea05

3c19b01733e53bd0bf860c59aa2c1c6f

ba351835bcc91d880881d05725ae399d

ff097d17d99af6a74612e9d2784be70d

**Approach:**

Upon checking with an online identifier, we come to know that the provided hash is md5. I went to crackstation.net and feeded the data…no luck.

If you google up you’ll see there’s a pokemon names list consisting of around 700+ pokemon names in it.

Downloaded it, and created a python script to append 1-10000000 numbers after it and hash it to check if that hash is one of the 5 hashes we are given.

Below is my python script. I'm sure there could be more optimized ways to implement or better scripts but this worked well for me.

import hashlib

hashfound = 0

def hashcheck(instring):

for itr in range(100000):

string = instring + str(itr)

khash = hashlib.md5(string.encode('utf-8')).hexdigest()

if khash in hashes:

print(string+" "+khash)

global hashfound

hashfound +=1

break

poklist = open('pokemon-list.txt','r').read()

poklist = poklist.split('\n')

print(len(poklist))

hashes = ['fbf5496a008165f6db865a23b3da8d89', '8d4244cb30f5aff30b2327eb439dea05', '3c19b01733e53bd0bf860c59aa2c1c6f', 'ba351835bcc91d880881d05725ae399d', 'ff097d17d99af6a74612e9d2784be70d']

for k in poklist:

hashcheck(k)

if(hashfound==5):

break

I’m aware of the different brute forcing tools like john, hashcat, etc but i just love to script :)

**Flag:**

**golduck467**

**pikachu866**

**gengar420**

**dratini13**

**charizard13478**

Congrats!!

Happy Hacking!