
Audit & Ethical Hacking

31 MARCH 2020

Bucharest University of Economic Studies
CSIE Faculty, IT&C Security Master Program
Authored by: Ionescu Radu Ștefan



Social Engineering - User credentials generation

Known user information



Image 1 Popescu Ion

First name: Ion

Last name: Popescu

Hometown: Daia, Giurgiu, Romania

Further information gathering

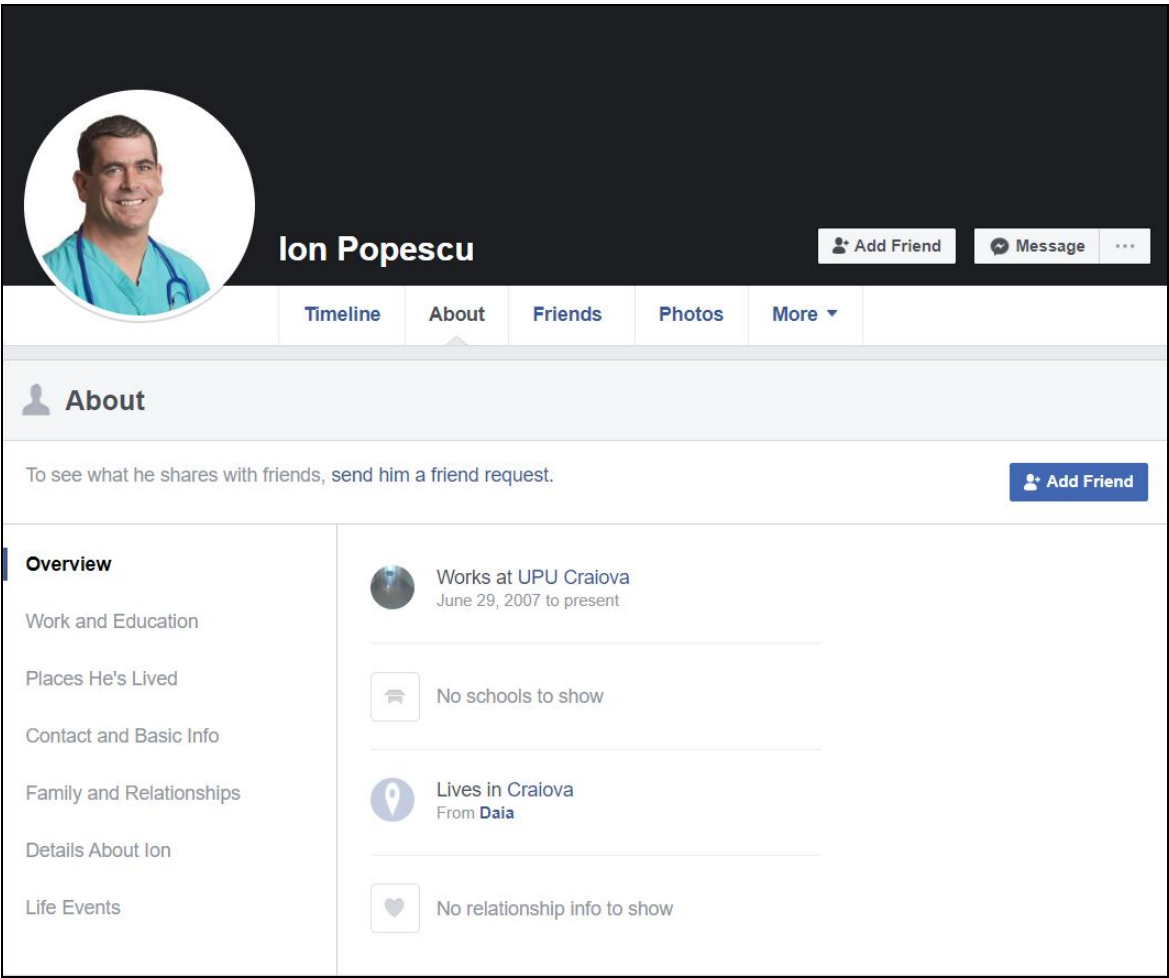


Image 2 Popescu Ion Facebook Page

Source: Facebook Profile Page

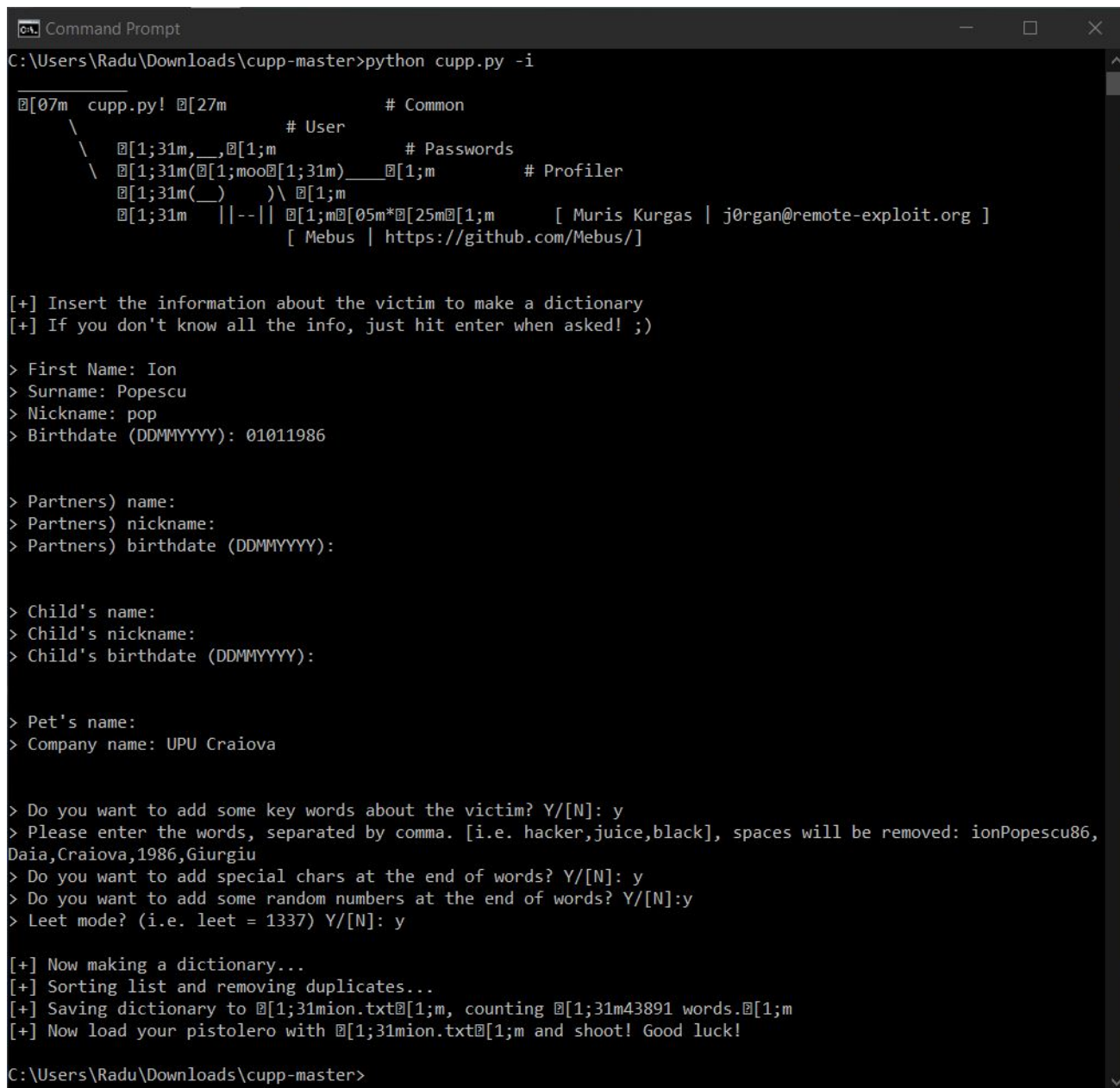
Current city: Craiova

Work: UPU Craiova

Facebook page: <http://facebook.com/ionPopescu86>

Possible birth year: 1986

Possible emails and passwords generation



```

C:\Users\Radu\Downloads\cupp-master>python cupp.py -i

[07m cupp.py! [27m          # Common
    \          # User
    \  [1;31m,__,[1;m          # Passwords
    \  [1;31m([1;moo[1;31m)____[1;m          # Profiler
      [1;31m(____) \ [1;m
      [1;31m  |--|| [1;m[05m*[25m[1;m      [ Muris Kurgas | j0rgan@remote-exploit.org ]
                                   [ Mebus | https://github.com/Mebus/]

[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: Ion
> Surname: Popescu
> Nickname: pop
> Birthdate (DDMMYYYY): 01011986

> Partners) name:
> Partners) nickname:
> Partners) birthdate (DDMMYYYY):

> Child's name:
> Child's nickname:
> Child's birthdate (DDMMYYYY):

> Pet's name:
> Company name: UPU Craiova

> Do you want to add some key words about the victim? Y/[N]: y
> Please enter the words, separated by comma. [i.e. hacker,juice,black], spaces will be removed: ionPopescu86,
Daia,Craiova,1986,Giurgiu
> Do you want to add special chars at the end of words? Y/[N]: y
> Do you want to add some random numbers at the end of words? Y/[N]:y
> Leet mode? (i.e. leet = 1337) Y/[N]: y

[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to [1;31mion.txt[1;m, counting [1;31m43891 words.[1;m
[+] Now load your pistolero with [1;31mion.txt[1;m and shoot! Good luck!

C:\Users\Radu\Downloads\cupp-master>
```

Image 3 cupp tool

Creating a dictionary for our target user, Popescu Ion, using the Common User Passwords Profiler (cupp) tool from Mebus. Using all the gathered information, by feeding it to the cupp tool, we create a dictionary for Popescu Ion, containing 43,891 words, saved in “ion.txt” file. Then we use this dictionary with Mentalist and some rules, like adding something before or after the words, modifying letter case and substituting some characters with others, to generate another, bigger word list for our target.

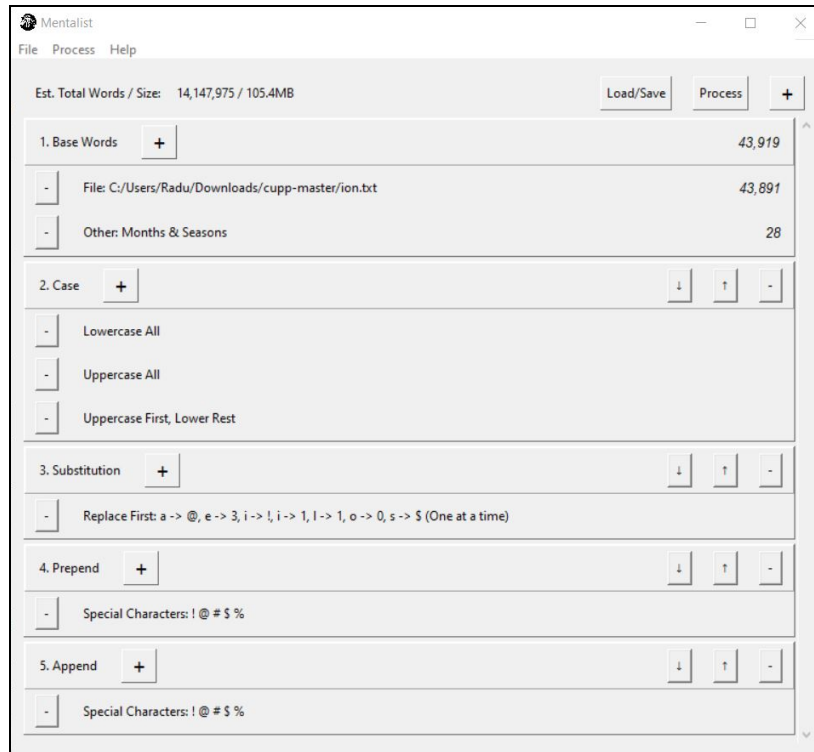


Image 4 Mentalist tool

The Mentalist tool generates a list of 3,648,750 words, saved as “*ion_mentalist.txt*”. We will use this big list to extract the best 100 candidates for the email and for the password.

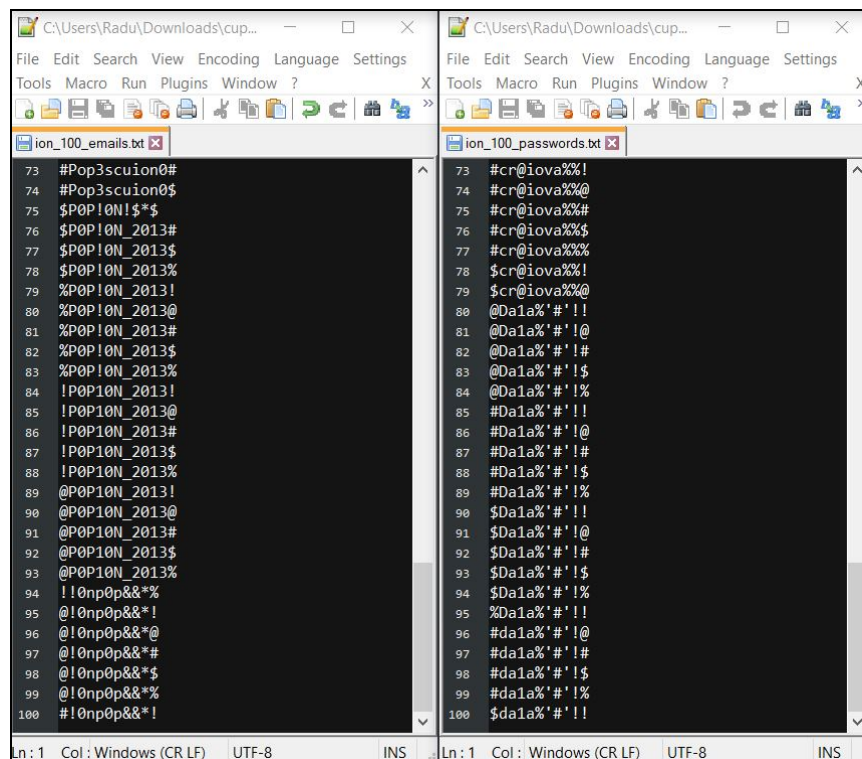


Image 5 Final list of emails and passwords