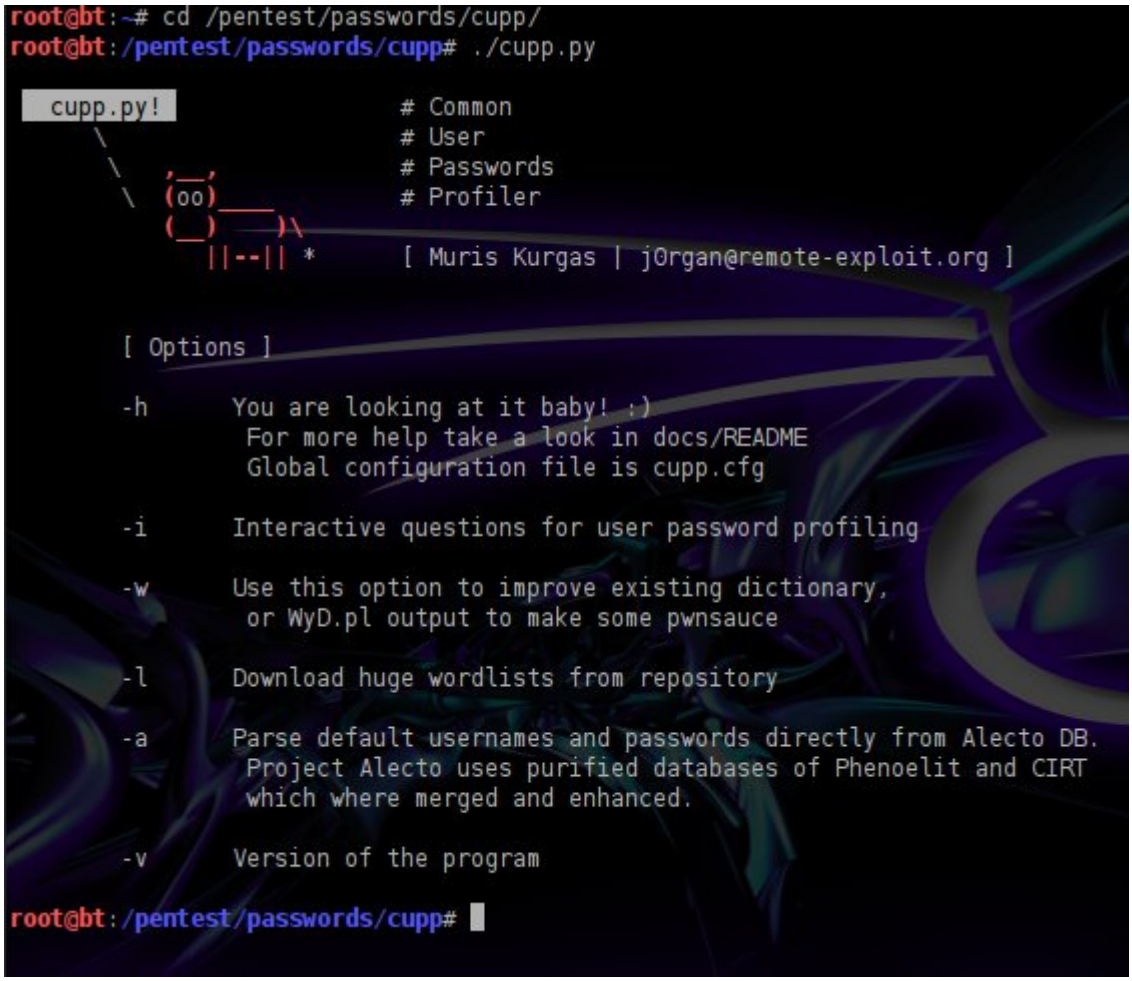
Common User Passwords Profiler

pentestlab.blog/category/social-engineering/page/9

March 6, 2012



There are a lot of social engineering techniques that you can try in order to retrieve personal information from users that can help you to identify their passwords.However people have different personalities like many people are not willing to talk to strangers about the so as penetration tester that performs social engineering attacks you may find some obstacles.

Not all the people are open for discussions so there will be times that you may unable to retrieve the information that you want.So the only thing that you can do is to have a good password list related to the interests of this person.

The aim of the CUPP is to generate common passwords based on the input that you will give for your target.For example:

- Name
- Birthday
- Pet name
- Company
- Interests

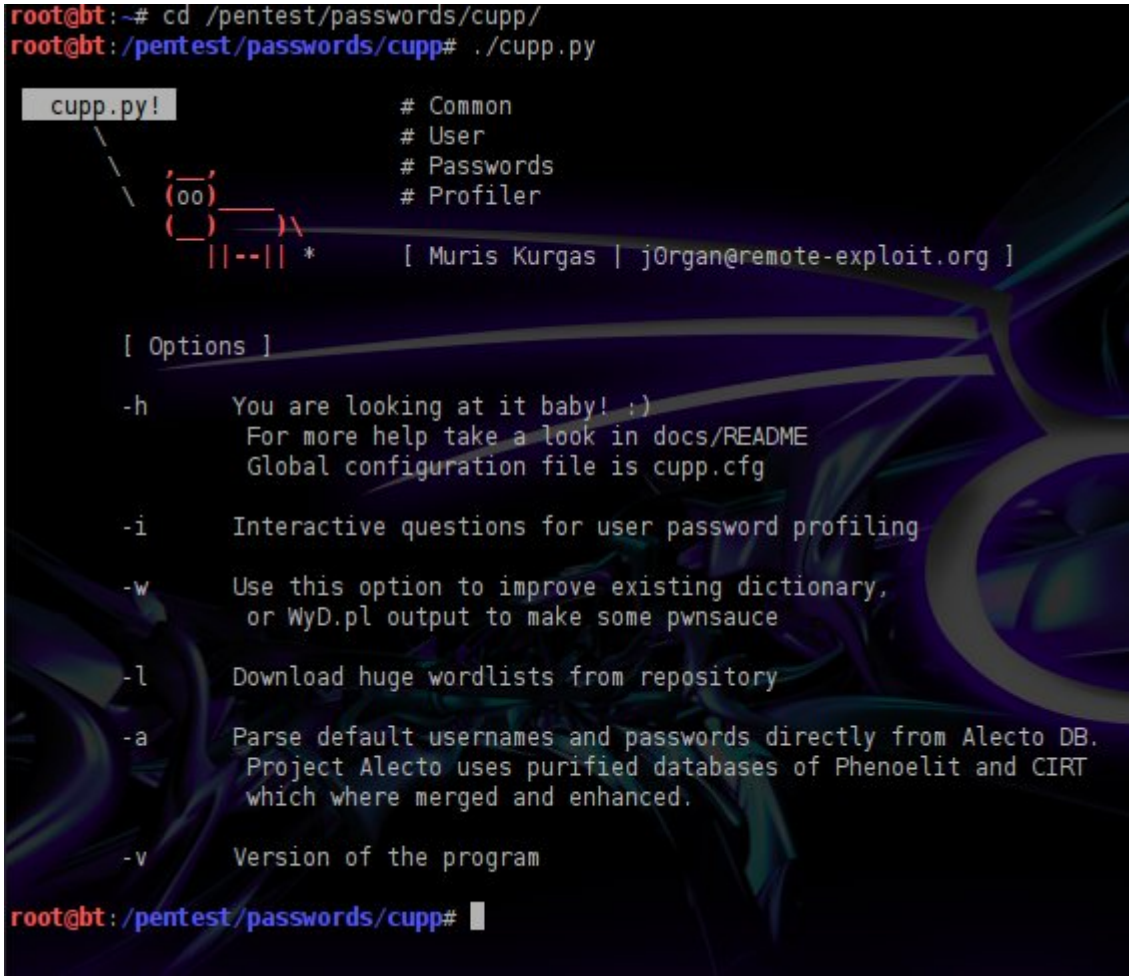
- Hobbies
- Likes

To start CUPP you need to execute the commands below:

#cd /pentest/passwords/cupp

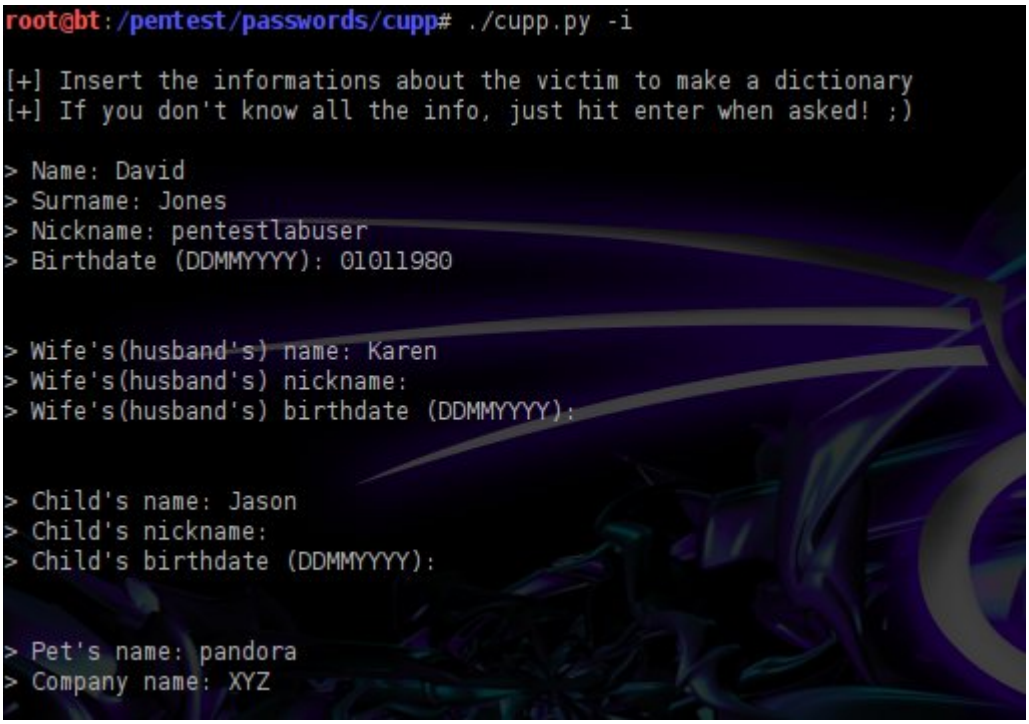
 # ./cupp.py

You can see in the image below the options that you have when you start the program:



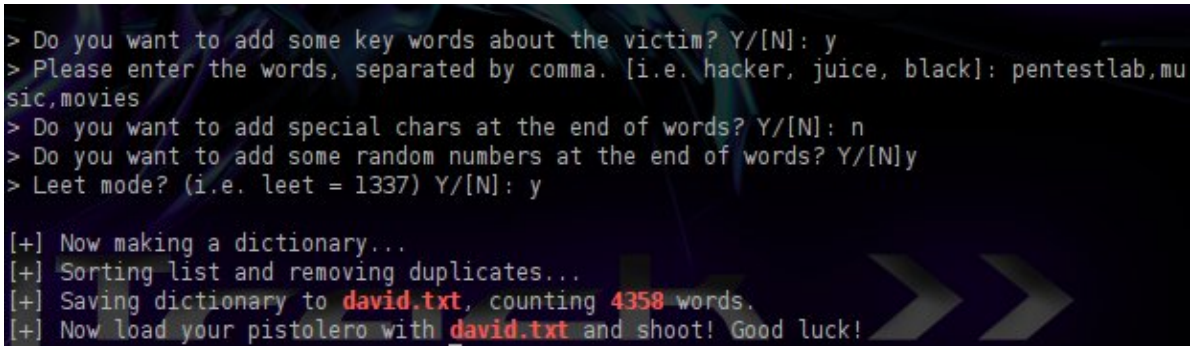
CUPP Options

When we have as much information as possible for the interests,names,nicknames,hobbies etc of our victim it is time to use the cupp in order to fill in the information that we have for the creation of the password list.



Inserting the information in CUPP

Except of the information you can choose also if the list will include and leet words or random numbers at the end of the words,special characters and keywords.



Generating the passwords

Now the CUPP has generate the password list and we can use it in order to see if any password on the list is valid.

Conclusion

Most common passwords are birthdays,names,interests,mobile numbers and generally events from people's real life.The reason behind that is of course that people need to use something that they can remember especially in nowadays that everyone possess many accounts.

CUPP proves that sharing details in the social media or with someone who is not your friend could be dangerous.Besides social engineering is a very effective way for malicious users to discover passwords fast so it is a very common attack.

So every user must know that the choice of the passwords is very important and something that needs constantly evaluation.CUPP generates passwords from users social life so in order to avoid having our password to someone’s CUPP wordlist we can share false information to the social media or we should choose passwords that are irrelevant from our real life events.