

Forum:[Hack Forums](#)

Thread: [\[TUT\] How to use a password profiler](#)

?pth?n - August 13, 2013, 12:43 pm

Welcome

NOTE: This tutorial is for educational purpose only. Thinking about things in theory is fine, but don't use your knowledge to harm others. I am not reliable for any harm that is done with the information I cover in this tutorial.

Table of contents

- I. Introduction
- II. Starting CUPP
- III. How to use CUPP

I. Introduction:

A lot of people are trying to crack facebook, gmail, youtube accounts or even .rar files with a simple bruteforce attack. This will take a while! You can use wordlists, but sometimes a wordlist won't help you since the password isn't covered in it.

This is why we are going to use the Common User Password Profiler (CUPP). CUPP is a program which is made to create a wordlist with the most common passwords a person uses.

A lot of people are using their name, boy- or girlfriends name, birthday, hobbies, etc. for their passwords.

CUPP will create a wordlist which contains possible passwords of your target.

The personalized wordlist can be used to get access to an account way faster than using one of the common methods (bruteforcing, wordlist).

II. Starting CUPP:

CUPP is written for linux distributions.

Luckily, it is preinstalled on Backtrack and Kali linux.

If you want to download it, there you go: [cupp.py](#)

Simply type in Code `cd /pentest/passwords/cupp python cupp.py` to get a quick overview over the tool.

If you want to start directly, just type in:

Code `cd /pentest/passwords/cupp python cupp.py -i`

III. How to use CUPP:

This should be self-explaining.

If you started CUPP you should press enter and go through the following fields. If you don't know what to fill in, just press enter to skip it.

Quote:Name:

Surname:

Nickname:

Birthdate:

wife's(husband's) name:

wife's(husband's) nickname:

wife's(husband's) birthdate:

Child's name:

Child's nickname:

Child's birthdate:

Pets' name:

Company name:

Do you want to add some key words about the victim Y/[N]:

Do you want to add some special chars at end of words? Y/[N]:

Do you want to add some random numbers at end of words? Y/[N]:

Leet mode? (i.e. leet = 1337) Y/[N]:

The first fields are the most important ones.

A lot of people are using a password like John1990 or JohnDoe1990, so it's important to fill these out correctly.

I highly suggest you to add hobbies, crushes, citys, clubs, sport teams and so on to the key words!

Leet mode will generate passwords in l33t sp34k aswell. It's up to you to use this. Personally I doubt that many people are using something like this for their passwords.

Congratulations!

You should see a new wordlist.txt (filename based on what you entered as name before) in /pentest/passwords/cupp/

The next step would be, to test your fresh wordlist using Hydra for example. If you don't know how to do this, check out this thread:

[How to perform bruteforce/dict attack on Hotmail/MSN with Hydra](#)

Final words:

Thank you for reading my tutorial!

I hope someone learned something new reading it. If you got any questions, feel free to PM me or post on the thread.

If you found any bigger mistakes, let me know.

Have a nice day everyone.

Fyton. - August 13, 2013, 1:35 pm

This looks nice, bookmarked it. thankyou OP

?pth?n - August 17, 2013, 10:26 am

(Aug 13, 2013 01:35 PM)Fyton. Wrote: [\[CITE\]](#) This looks nice, bookmarked it. thankyou OP
Thank you ;)

Best success with whatever you are going to do!

???RSA - May 14, 2016, 4:09 pm

Damn, another HQ tutorial. Maybe if I can get linux to work, I can actually do this.

#Bookmarked.