ZIP PASSWORD CRACKER

NOEL MOSES MWADENDE

ABOUT THE AUTHOR

Noel Moses Mwadende is currently 2 year Computer Science and Information Security student at University of Dodoma , Data Scientist and well specialized in python for ethical hacking ,Penetration Tester, Malware Analiyisist, Hacking tools writer already written “KEYLOGGER” and “INFORMATION GATHERING TOOL” mostly used for penetration testing phases of Information Gathering and Reconnaisance,writer of different books about programming language,hacking, malware and Computer security in general also a member of Udom CyberSec lab, After making several experiments in Udom CyberSec lab , Noel started to write different books concern security with great passion starting with his book of "WIFI HACKING IN FEWS STEPS" ,"PANDAS TOOL FOR DATA SCIENTIST","HOW TO MAN IN THE MIDDLE ATTACK",”MAKING OUR ANDROID TROJAN HORSE”,”MY WIN TROJAN-HORSE” and "WRITE VIRUS BY BATCH PROGRAMMING" , but I also want to alert you that I will bring you the book about how to exploiting SQL INJECTION , whereby I will use my self-made tool for the early stages of information gathering and the tool is called “INFORMATION GATHERING TOOL” , so while reading other books to forget to get prepared about exploiting SQL INJECTION with demonstration and web spidering with python, where we will make our own spiders by using Beautifulsoup, scapy and selenium I hope you will enjoy as am here to make you so happy.

ACKNOWELDGEMENT

Thanks to Prof Leonard James Mselle the author of “C++ programming in RAM diagrams under MTL-1” for your support in security issues, to be honest you are our father in Forensic and security in general and my lab instructor currently Phd holder Sir Ramadhani Rais, for giving chance of being security lab member wherein I learned a lot of issues of security together with my brother Joachim Mahole and co.

Thanks to my former head of department Doctor Masoud Masoud, currently lecture at DIT, as my program of CIS was under you plus full control about it, you are the one gave me this opportunity of studying computer Science and Information security.

Thanks to my computer security instructor Sir L Mutembei and Sir Godless Minja, you have been my pillars in security, insipering CIS students to carry out different security practical, do not get tired to insist and give us more experience, as you are greatest in computer security.

Thanks to my security lab members Mr Jackson Bakari, Andy Walters Kawa and Rashid Mtali I know how your cooperation have playing a vital role in my security learning skills.

Thanks to you everyone, I hope without you reader no book can exist in this world.

TABLE OF CONTENT

1. INTRODUCTION

To be honest am human being , and i must speak the truth , the greatest positive response from my last little book which was about "WIFI HACKING IN FEW STEPS" has made tiredless to writing more books or articles about hacking , the knowledge is free and am not selfish about sharing what i know with you my reader.

Sometimes life become annoying , it may sometimes happen that you spent more 10 GB downloading something online in .zip format , but as soon as the download complete you try to extract it and you be prompted to put password ???? , how you feel like ? , on my side i become more than annoyed , now look that to get 10 GB it may cost you a lot, internet i use tend to reward me 1GB for Tsh 1500 , so to get 10 GB it might cost me Tsh 15'000 and the downloaded zip folder has password which i don't know , i remember Mr Joachim Mawole had downloaded hacking tutorials from certain website owned by Indian Profession hacker , it costed him a lot of GB and when he tried to extract zipped folder , it prompted him to put password , OMG he felt bad and i felt very sorry for him and that was the starting point of this my little book when i thought why can't i find some way for cracking zipped password folder and in this book is what we do.

2. WHY WE NEED TO ZIP PASSWORD CRACKER

1. Cracking downloaded zipped folder from Internet

There some sites consist of a lot tutorial zipped by password, to get the password you have to pay some amount of USD Dollars or Tsh whatever, while you're pockets are empty, by owning this zipPasswordCracker.py life become simple and your password are on your fingerprint.

2. You may forget your password

It may happen that you put password on you zipped folder for protecting unauthorized people from accessing it, but unfortunately you forget your own password, who will remind you ?, zipPasswordCracker.py will make your life easy.

3. Cracking for the fun

As the issues concern Computer security and all about hacking we sometimes do it for the fun, just being capable of cracking zipped file, you become happy, i remember a certain Data Scientist said that owning or knowing may data, you become powerful and makes you happy.

4. For Education Purposes

Nowadays Cyber Security is growing too fast, and for those who are taking Computer Security studies, this might be part and parcel of your owned skill and after reading and practicing on this book.

3. REQUIREMENTS NEEDED

1. You will need to have any linux machine, as the file is made up python programming language and python is by default installed in linux machine, am using Parrot Security.

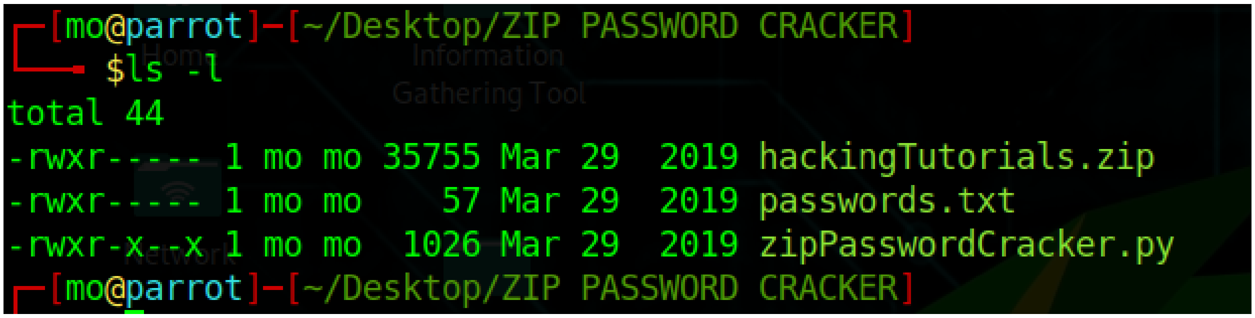
2. A piece of code for cracking, that is zipPasswordCracker.py

3. Zipped folder with password , for begining make your own zipped folder and put for experiment , try to crack own zipped folder with different dictionary , after being advanced then make it real .

4. LET'S GET STARTED

A. command : ls -l

B. command : output



```
┌─[mo@parrot]─[~/Desktop/ZIP PASSWORD CRACKER]
└──╼ $ls -l
total 44
-rwxr----- 1 mo mo 35755 Mar 29  2019 hackingTutorials.zip
-rwxr----- 1 mo mo    57 Mar 29  2019 passwords.txt
-rwxr-x--x 1 mo mo  1026 Mar 29  2019 zipPasswordCracker.py
┌─[mo@parrot]─[~/Desktop/ZIP PASSWORD CRACKER]
```

you can see the file named zipPasswordCracker.py, this is the file that contain our codes for cracking zip password, an extension .py means that this zipPasswordCracker.py is made of python programming language, and we usually call it Python for ethical hacking.

NOTE: In some case you may find that zipPasswordCracker.py is not in executable mode so you must make it executable by command below

MAKING zipPasswordCracker.py into executable mode

A. **command : sudo chmod +x zipPasswordCracker.py**

HOW TO SEE IF PYTHON IS BY DEFAULT INSTALLED IN LINUX

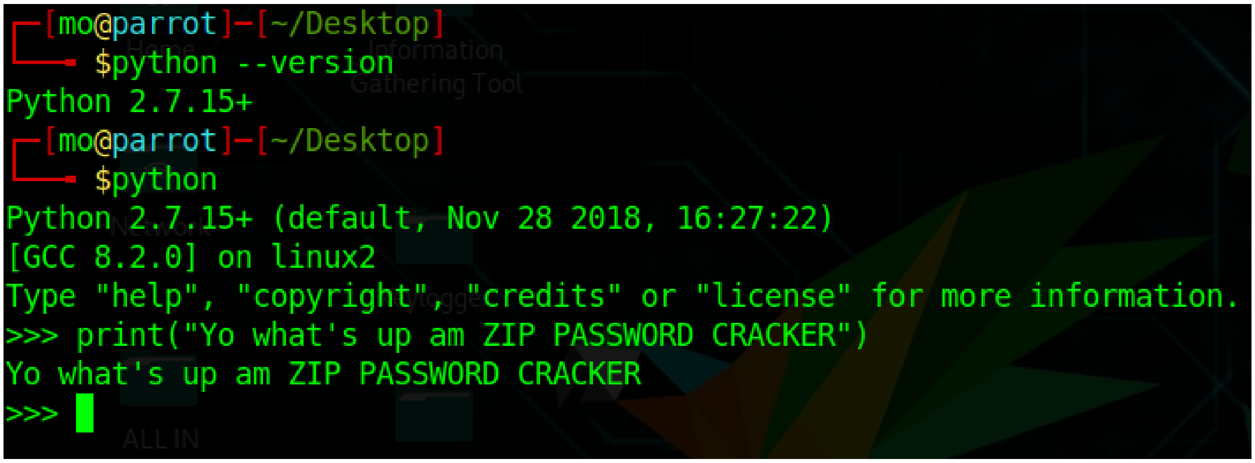
Python is by default installed in linux , and this has aided different hackers to use Python for ethical hacking , and different hacking tools in Kali linux , Parrot , Samurai , Pentoo and Fedora are developed by python.

A. commands

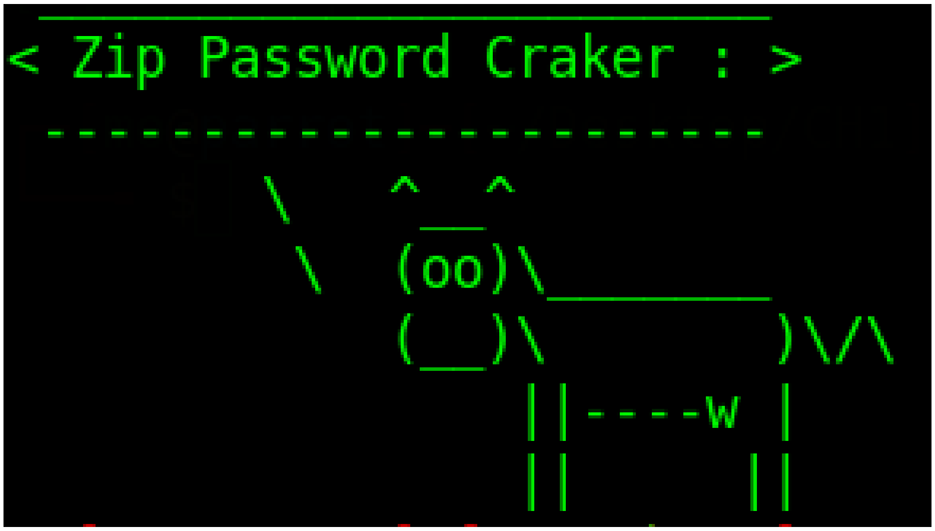
```
- python
-print("Yo what's up am ZIP PASSWORD CRACKER")
-python --version
```

try the above commands and everything is simple

B. **output**

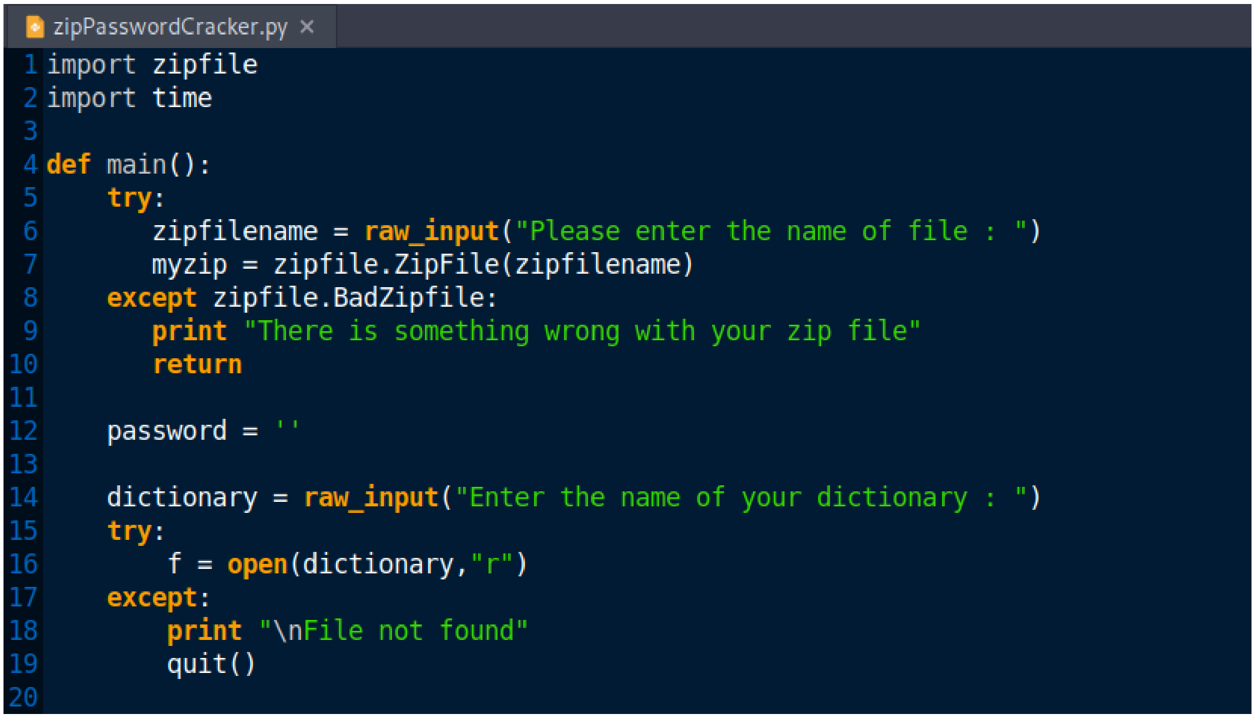


```
┌─[mo@parrot]─[~/Desktop]
└──╼ $python --version
Python 2.7.15+
┌─[mo@parrot]─[~/Desktop]
└──╼ $python
Python 2.7.15+ (default, Nov 28 2018, 16:27:22)
[GCC 8.2.0] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> print("Yo what's up am ZIP PASSWORD CRACKER")
Yo what's up am ZIP PASSWORD CRACKER
>>> 
```

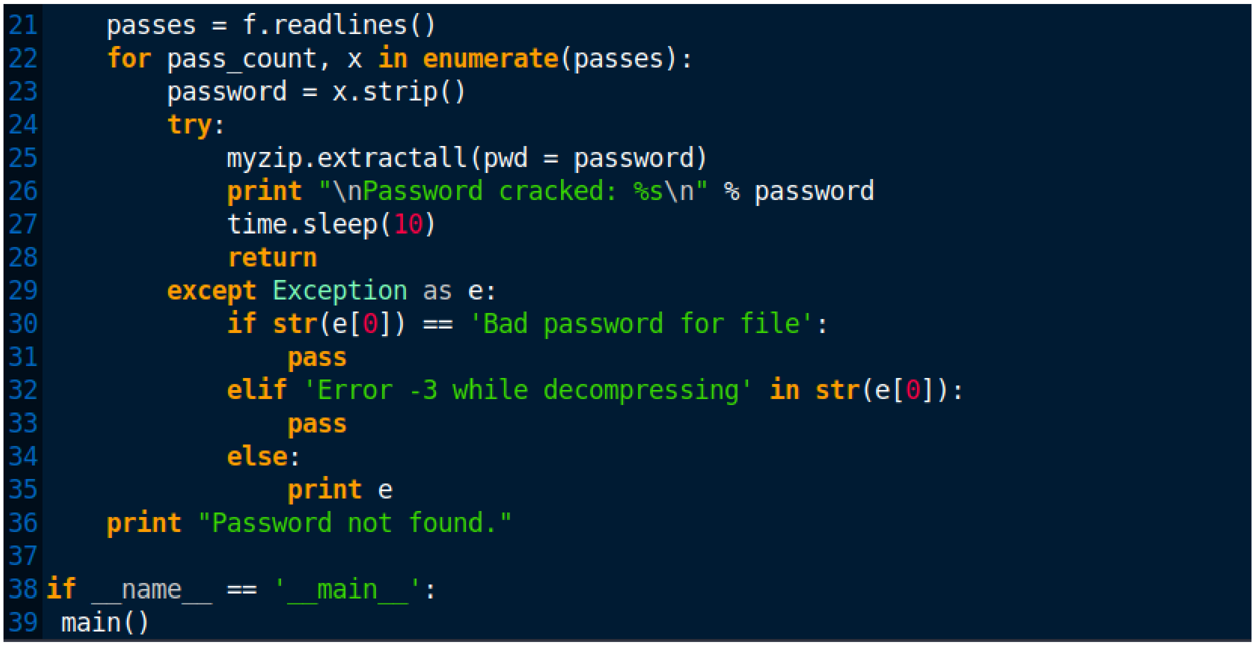


```
 _______________________
< Zip Password Craker : >
 -----------------------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
```

zipPasswordCracker.py SOURCE CODE



```python
import zipfile
import time

def main():
    try:
       zipfilename = raw_input("Please enter the name of file : ")
       myzip = zipfile.ZipFile(zipfilename)
    except zipfile.BadZipfile:
       print "There is something wrong with your zip file"
       return

    password = ''

    dictionary = raw_input("Enter the name of your dictionary : ")
    try:
        f = open(dictionary,"r")
    except:
        print "\nFile not found"
        quit()

```



```python
    passes = f.readlines()
    for pass_count, x in enumerate(passes):
        password = x.strip()
        try:
            myzip.extractall(pwd = password)
            print "\nPassword cracked: %s\n" % password
            time.sleep(10)
            return
        except Exception as e:
            if str(e[0]) == 'Bad password for file':
                pass
            elif 'Error -3 while decompressing' in str(e[0]):
                pass
            else:
                print e
    print "Password not found."

if __name__ == '__main__':
 main()
```

5. HOW zipPasswordCracker.py WORKS

import zipfile

As you can see above we have imported zipfile module "import zipfile" - The zifile module is used to manipulate ZIP Archives files, where by importing zipfile module we can read and write ZIP Archives , so without importing this module it won't work as python will fail To read the zipped file

import time

In python we have module time for handling different time operations

def main():

def main( ): , this is python function , function block begin with keyword def followed by the function name and parentheses (), so here our function name is main , that is the main function, any parameters or arguments should be placed inside those parentheses , remember that function should end with :

```
zipfilename = raw_input("Please enter the name of file")
```

- meaning of the line above, shows that the program can receive input from user , and type of input received is by default a string .

In python we can use two function to receive user input

```
  =>  input("Your message to user")
   =>  raw_input("Your message to user")
```

let's if you want to receive integer input if python your code would look like this,

```
   ip_address = int ( input ("Enter the ip address you want to scan"))
```

but filename is like reference variable which will store the name of zip file you want to crack

as you can see from the code you might have understood how python input method work, at the line above the ip address will be received as string then the int method will convert it into integer as we know thatinput method in python is by default treating all input as string.

```
def main():
   try:
      zipfilename = raw_input("Please enter the name of file : ")
      myzip = zipfile.ZipFile(zipfilename)
```

zipfile.ZipFile() this is the class for reading and writing zip file but you must pass the name of that zip file, as in our case we want python zipfile module to read the name of our zip file, if you see underneath of try: you can see that the name of our zip file received from user is stored in zipfilename variable.

```
def main():
```

This is the python main function

try

and

except

if program execute clear without error that is part of try block, but if any error occur that is part of exception, that is the block where errors are captured

```
except zipfile.BadZipfile:
    print "There is something wrong with your zip file"
    return
```

-From above we use zipfile.BadZipfile to catch the exception will appear if your file got any error the line below it will be printed, as we know that zipfile.BadZipfile is an exeception in zipfile module we imported from the first line of our file, its function is to raise if zip file got any error for example zip file is corrupted or it is bad type of zip file.

```
dictionary = raw_input("Enter the name of your dictionary : ")
```

i know now you understand what is raw_input() and input() function as i just want to memorize you that these two functions works the same and are used to take user input in form of string, so above code of line will take the name of dictionary which is the file consist of all possible password.

```
try:
        f = open(dictionary,"r")
    except:
        print "\nFile not found"
        quit()
```

inoder to open file for writing or reading you need to use open() function in python , it is common sense that you can’t read or write to a file without opening it, as we know that dictionary is the file which consist of passwords so we need to open it so that we can read the passwords it contain the function takes two parameters first one is the name of file and the second one is the mode of file, that is ether r for reading mode or w for writing mode, for our case we put r as we just want to read the file, if the file will be found then underneath of try: will be executed if not that means the file is not found in your working directory, so you can solve this by adding dictionary file to your working directory, then what happen if dictionary file is not found , nothing to carry on , the program should quit.

```
    passes = f.readlines()
    for pass_count, x in enumerate(passes):
        password = x.strip()
```

we know that f is the variable in which the dictionary read password are at it, now we want to read dictionary file line by line as we know that password should be tested one by one, the function to be used is readlines(), and those password which are read line by line are sent to passes

- strip() will strip away everything (remove leading and trailing space of the string), those are the whitespace from the beginning and at the end of the word and will return empty string and that empty string will be stored in password as know above password = x.srtip()

- for pass_count, x in enumerate() that loop over something and have automatic loop, and here passes which has line by line of password from dictionary are

looped and counted.

```
try:
        myzip.extractall(pwd = password)
```

as we know myzip has already read zip file represented by zipfilename at he beginning of this explanation pwd = password , this will be taking password and extract a zipped file

```
print "\nPassword cracked: %s\n" % password
        time.sleep(10)
        return
```

It will print the found password if present in dictionary, time.sleep(10) here is when you should know why we imported time module it is like for such wait.

```
 except Exception as e:
          if str(e[0]) == 'Bad password for file':
             pass
          elif 'Error -3 while decompressing' in str(e[0]):
             pass
          else:
             print e
   print "Password not found."
```

```
if __name__ == '__main__':
 main()
```

the rest part is for handling errors in may the dictionary file is bad or there is any error in decompressing it as you know that these rar/zipped file are compressed.

```
 if __name__ == '__main__':
```

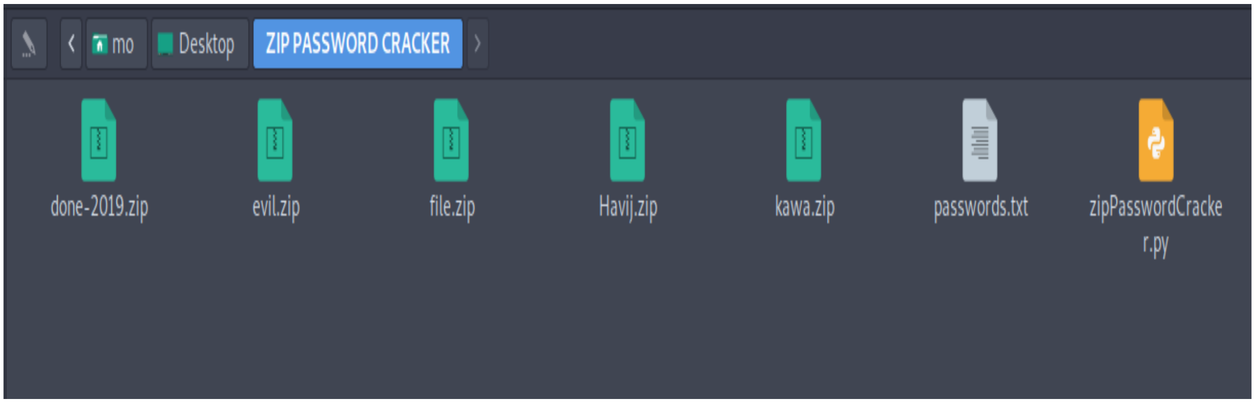
, this allows you to run python files either as reusable modules or standalone program, you must declare the call function "if __name__ == '__main__':",

```
main()
```

the main function is called.

6. CRACKING BY USING DICTIONARY ATTACK

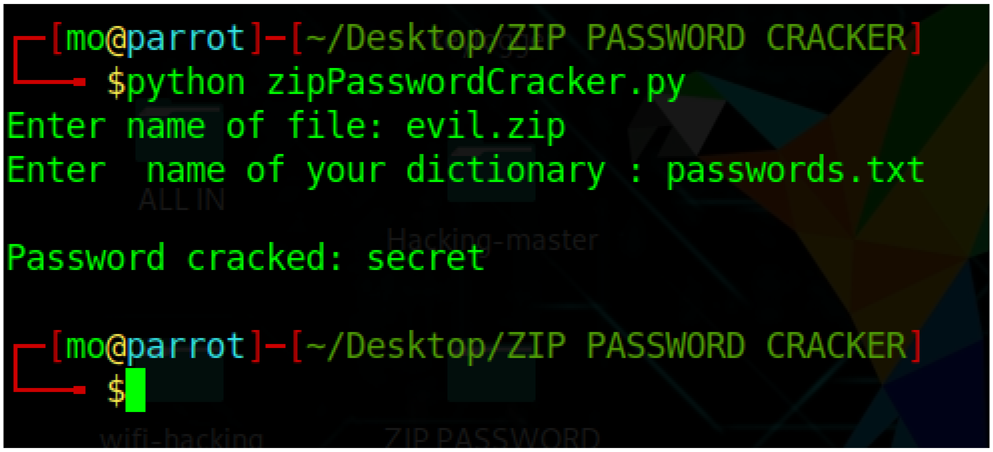
The following below are the zipped files with password, and we are going to crack them one after another.



Before starting to crack our zipped files, the destination folder or working directory looks that way, it has the following zipped file, file.zip,kawa.zip ,done-2019 which contain cs227 notes from my instructor Sir L Mutembei, Havij.zip it contain havij.exe for windows , I bet those who got experience on this field of hacking they have passed across this tool,evil.zip , and file.zip all above zip file got the password , as long as you try to open them , you're prompted to put password, so we will track them one another , so that we can we sure with our tool being using.

1. Cracking evil.zip

Our cracker is simple to use , you just write python zipPasswordCracker.py as the rule of running python scripts on the terminal, then press enter, after that you will prompted to put the name of zipped file you want to crack, then after you will be prompted to enter the name of your dictionary that is combination of all possible passwords used to cracking or bruteforcing.

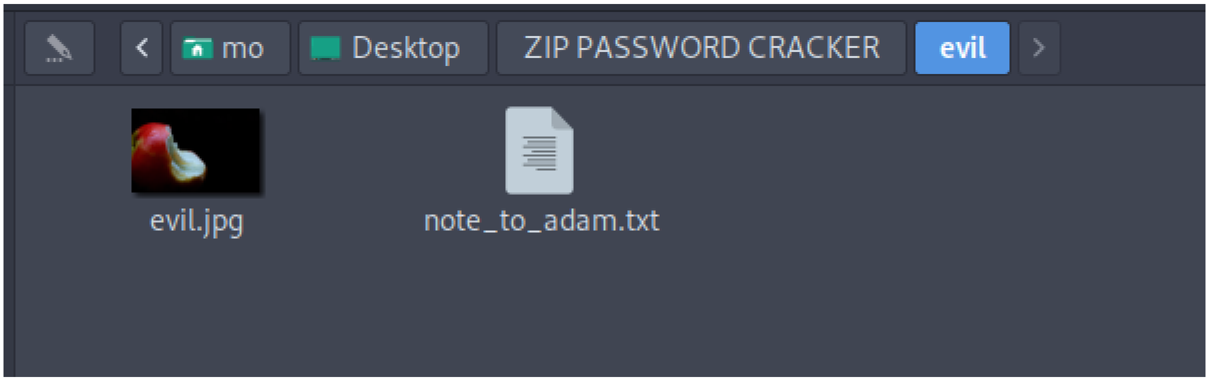


```
┌─[mo@parrot]─[~/Desktop/ZIP PASSWORD CRACKER]
└──╼ $python zipPasswordCracker.py
Enter name of file: evil.zip
Enter  name of your dictionary : passwords.txt

Password cracked: secret

┌─[mo@parrot]─[~/Desktop/ZIP PASSWORD CRACKER]
└──╼ $
```

From above you can see that the password is already cracked, as it finish to crack the found password, zip file extract it'self, after going back to the destination folder, you will be the fil has already.

After evil.zip file has been successfully cracked I tried to visit inside the folder to see what is inside, those are the content of evil.zip, though evil.jpg has been embedded something inside it, for those who have come across steganography, science of hiding text or words inside images.

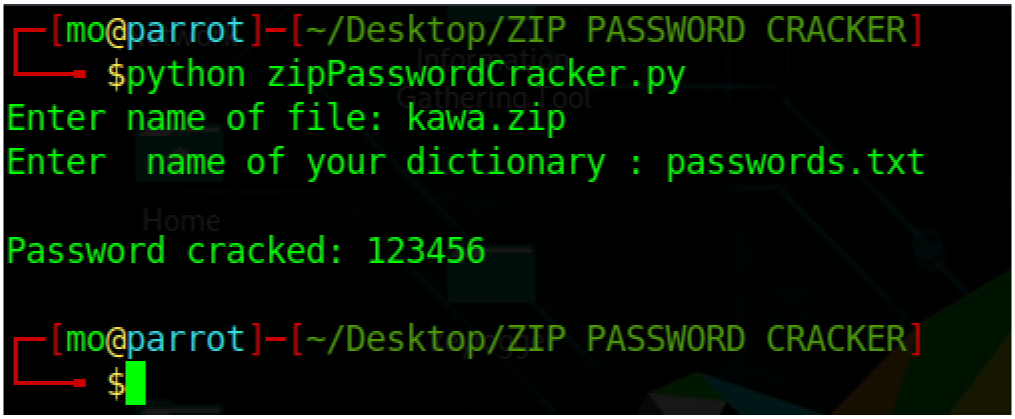
Content of evil.zip



That was then end of cracking evil.zip and it over the password is found.

2. Cracking kawa.zip

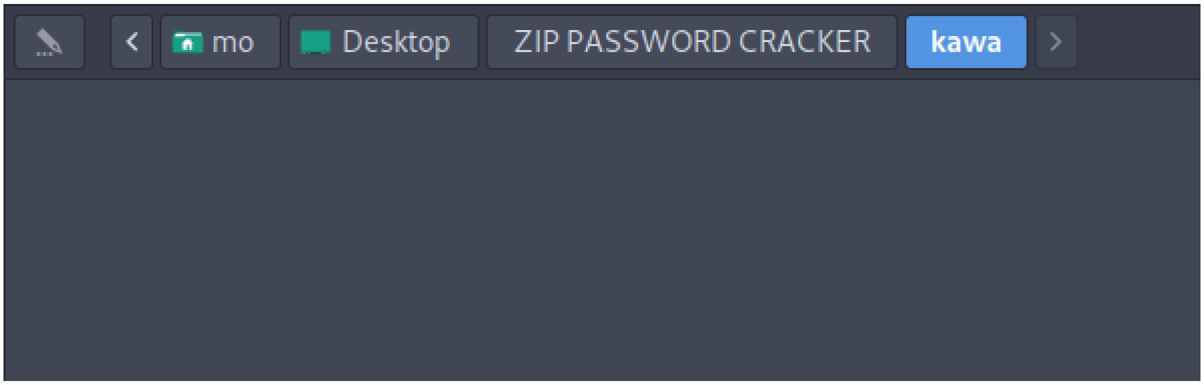
python zipPasswordCracker.py run it on your terminal enter the name of the file to be racked which is kawa.zip, finally write the name of your dictionary, press enter.



```
┌─[mo@parrot]─[~/Desktop/ZIP PASSWORD CRACKER]
└──╼ $python zipPasswordCracker.py
Enter name of file: kawa.zip
Enter  name of your dictionary : passwords.txt

Password cracked: 123456

┌─[mo@parrot]─[~/Desktop/ZIP PASSWORD CRACKER]
└──╼ $
```

Password used in kawa.zip was very simple as it is found in many dictionary, so it had to be cracked, always avoid using password which are commonly found in dictionary.

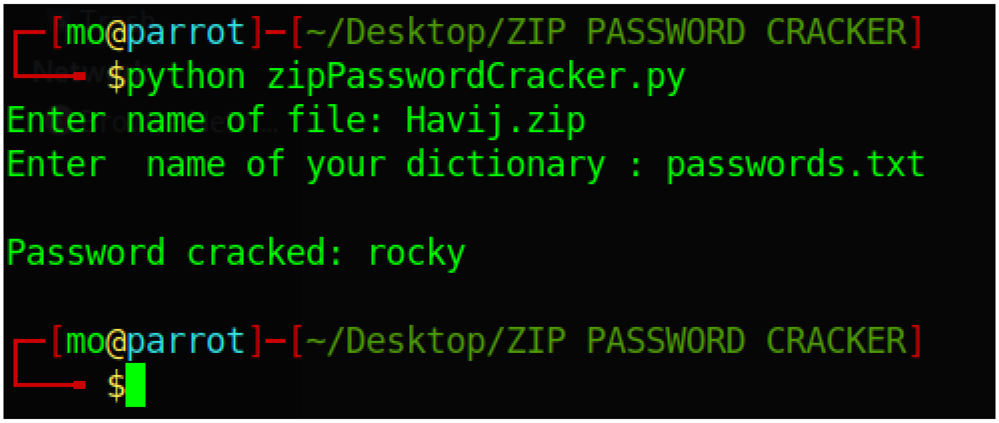
Content of kawa.zip



Oooh you can see kawa.zip was empty file zipped with password, I know this scenario have happened to someone, you download something, after extracting it you see nothing inside, sometime they are embedded with malware and set to execute as long as extraction finishes.

3. Cracking Havij.zip

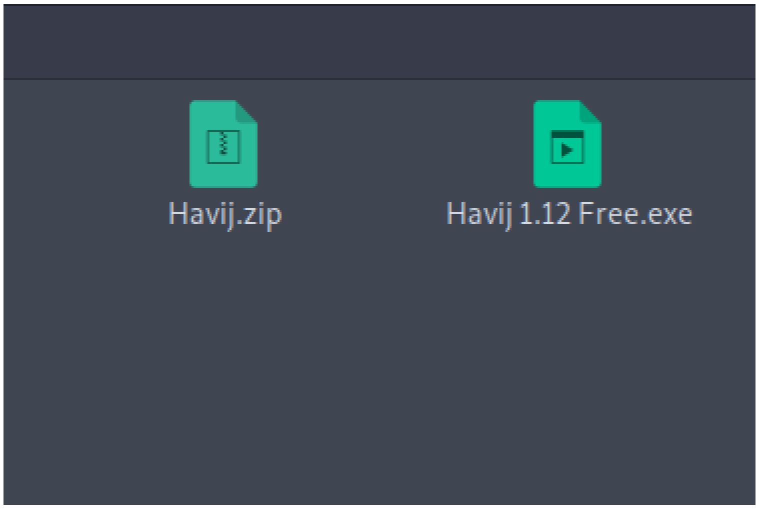
python zipPasswordCracker.py run it on your terminal enter the name of the file to be racked which is kawa.zip, finally write the name of your dictionary, press enter.



```
┌─[mo@parrot]─[~/Desktop/ZIP PASSWORD CRACKER]
└──╼ $python zipPasswordCracker.py
Enter name of file: Havij.zip
Enter  name of your dictionary : passwords.txt

Password cracked: rocky

┌─[mo@parrot]─[~/Desktop/ZIP PASSWORD CRACKER]
└──╼ $
```

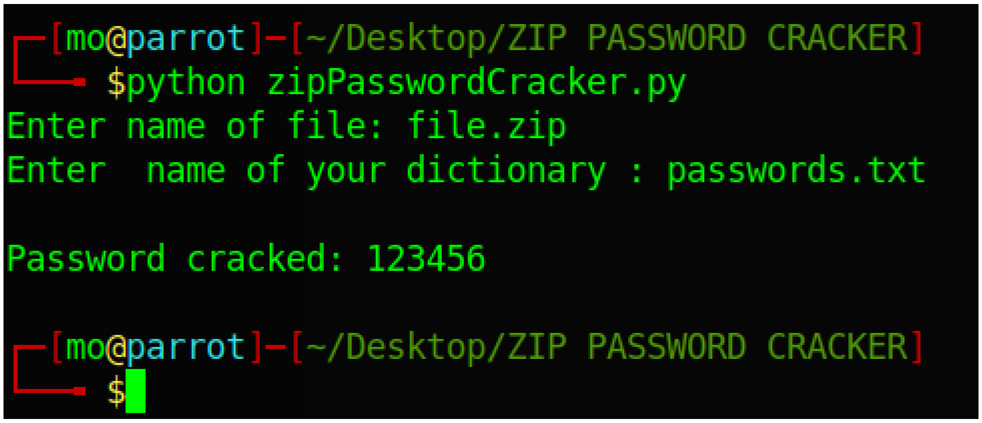
It has successfully cracked lets it’s content.

Content of Havij.zip



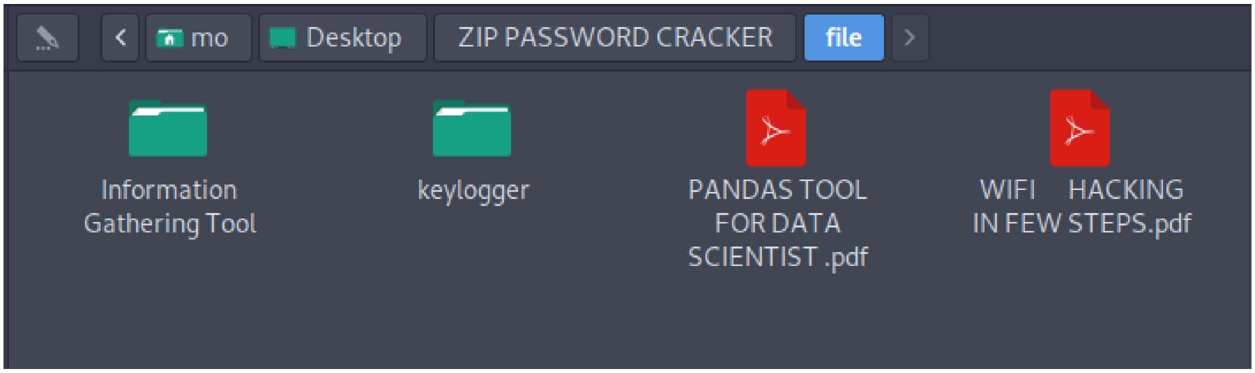
As you can see from above that inside Havij.zip, it had one content and that is Havij 1.12 Free.exe, that is free trial for user, and it work only in wins operating system as you can see it is .exe program.

4. Cracking file.zip



```
┌─[mo@parrot]─[~/Desktop/ZIP PASSWORD CRACKER]
└──╼ $python zipPasswordCracker.py
Enter name of file: file.zip
Enter  name of your dictionary : passwords.txt

Password cracked: 123456

┌─[mo@parrot]─[~/Desktop/ZIP PASSWORD CRACKER]
└──╼ $
```

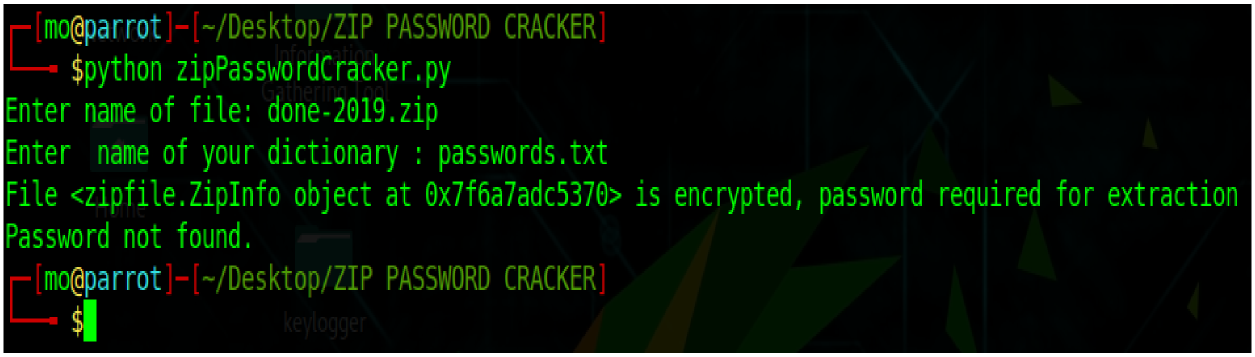
Content of file.zip


mo
Desktop
ZIP PASSWORD CRACKER
file
Information Gathering Tool
keylogger
PANDAS TOOL FOR DATA SCIENTIST .pdf
WIFI HACKING IN FEW STEPS.pdf

Ooooh this is the zip that I kept those my two books I I wrote and those two tools, if you want them then you can see my g-mail at then of this book then I will send, but the password used was weak, lol, you can not be serious if you put your password as 123456 .

5. Cracking done-2009.zip

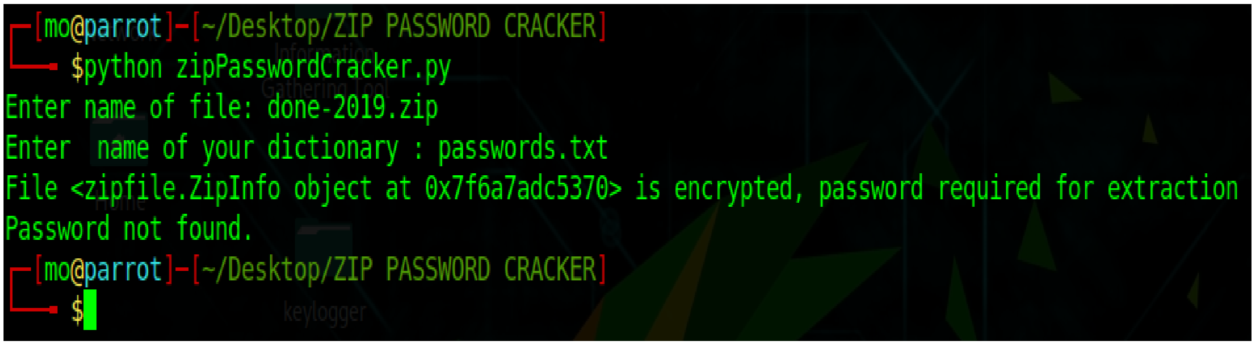
python zipPasswordCracker.py run it on your terminal enter the name of the file to be racked which is kawa.zip, finally write the name of your dictionary, press enter.



```
┌─[mo@parrot]─[~/Desktop/ZIP PASSWORD CRACKER]
└──╼ $python zipPasswordCracker.py
Enter name of file: done-2019.zip
Enter  name of your dictionary : passwords.txt
File <zipfile.ZipInfo object at 0x7f6a7adc5370> is encrypted, password required for extraction
Password not found.
┌─[mo@parrot]─[~/Desktop/ZIP PASSWORD CRACKER]
└──╼ $
```

Wow, the password is not found for the first time, read below to see why password was not   found.

Failed Cracking done-2009.zip

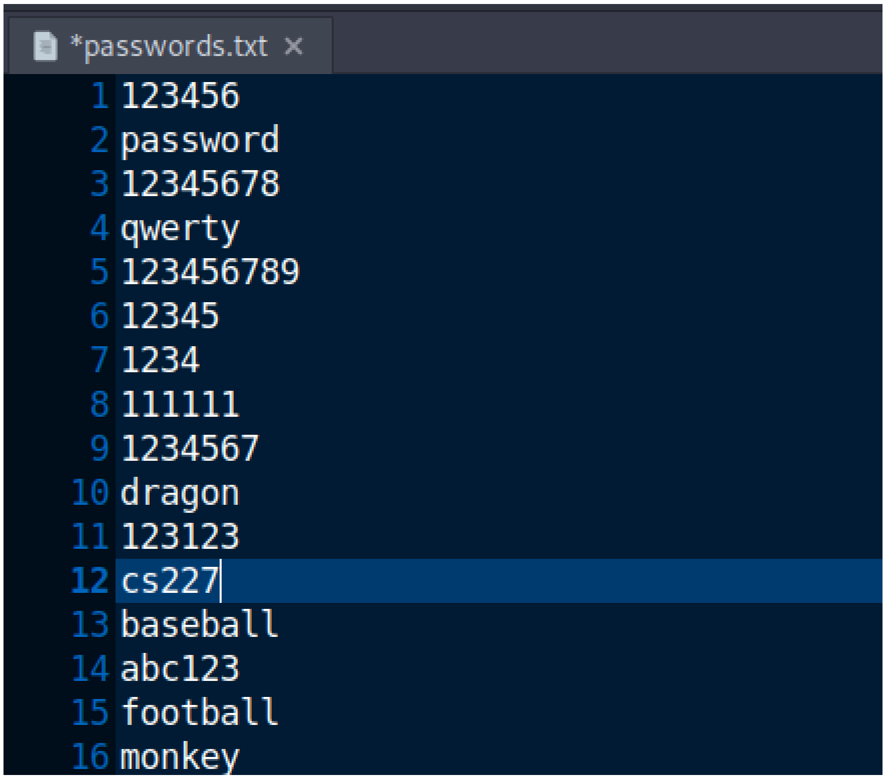


```
┌─[mo@parrot]─[~/Desktop/ZIP PASSWORD CRACKER]
└──╼ $python zipPasswordCracker.py
Enter name of file: done-2019.zip
Enter  name of your dictionary : passwords.txt
File <zipfile.ZipInfo object at 0x7f6a7adc5370> is encrypted, password required for extraction
Password not found.
┌─[mo@parrot]─[~/Desktop/ZIP PASSWORD CRACKER]
└──╼ $
```

What am doing here is to crack zipped file given by my instructor of security Sir L Mutembei, as this instructor have taught me cs215 (Information Security Technologies) and right now is still teaching me cs217 (Network Security) knows the rule of password one of the greatest rule is that “Do not use password that are commonly found in dictionary” , as instructor of security knows that it is difficult to find cs217 as password in dictionary .

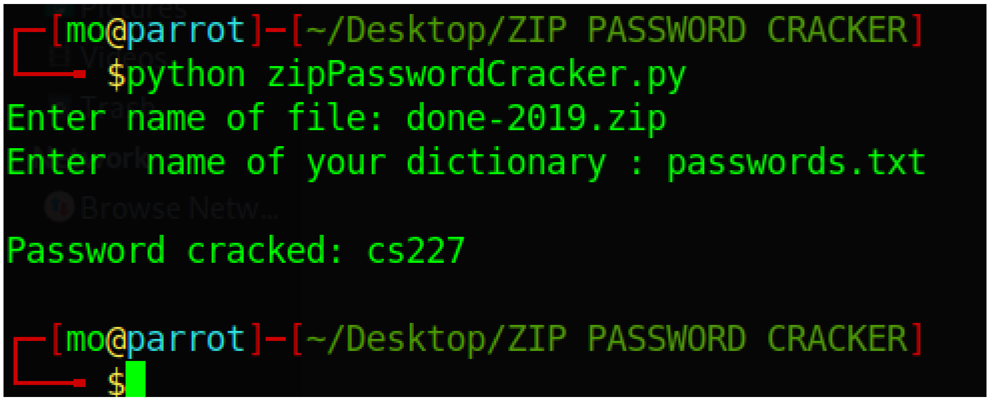
Adding cs227 in our dictionary

As we have seen above that my instructor L Mutembei used cs217 as password, because cs217 was not found in the dictionary the crack failed, here I want to show that this tool or most of bruforcing tool are efficient do not be discouraged if you cracking password by using dictiobary attack and being told that the password is not found, I even insisted this in the book of “WIFI HACKING IN FEW STEPS” , why can’t you change dictionary, cracking or bruteforcing password something it is not easy, be flexible hacker, change type of dictionary and tool being used, although Hydra is considered one of powerful for brutrforcing but you can’t succeed by one crack.



```
123456
password
12345678
qwerty
123456789
12345
1234
111111
1234567
dragon
123123
cs227
baseball
abc123
football
monkey
```

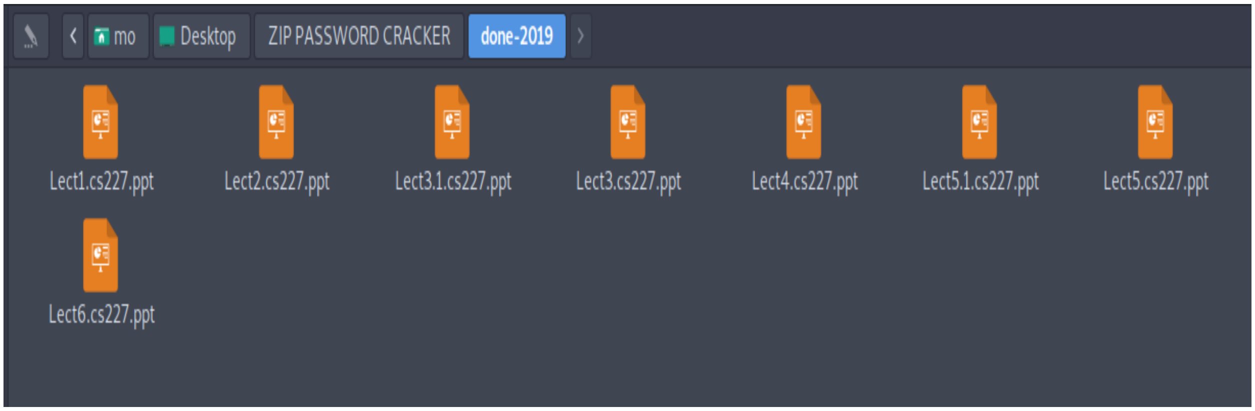
Succeed Cracking done-2009.zip



```
┌─[mo@parrot]─[~/Desktop/ZIP PASSWORD CRACKER]
└──╼ $python zipPasswordCracker.py
Enter name of file: done-2019.zip
Enter name of your dictionary : passwords.txt

Password cracked: cs227

┌─[mo@parrot]─[~/Desktop/ZIP PASSWORD CRACKER]
└──╼ $
```

You can see that now it has successfully cracked, so if crack has fail is the weakness of tool no, just find more dictionary.

Content of done-2019.zip



Wow those are the contents of our file from our instructor, thanks instructor for such good work, I know it is not easy to prepare such written material as they take time in organizing, designing, writing and everything.

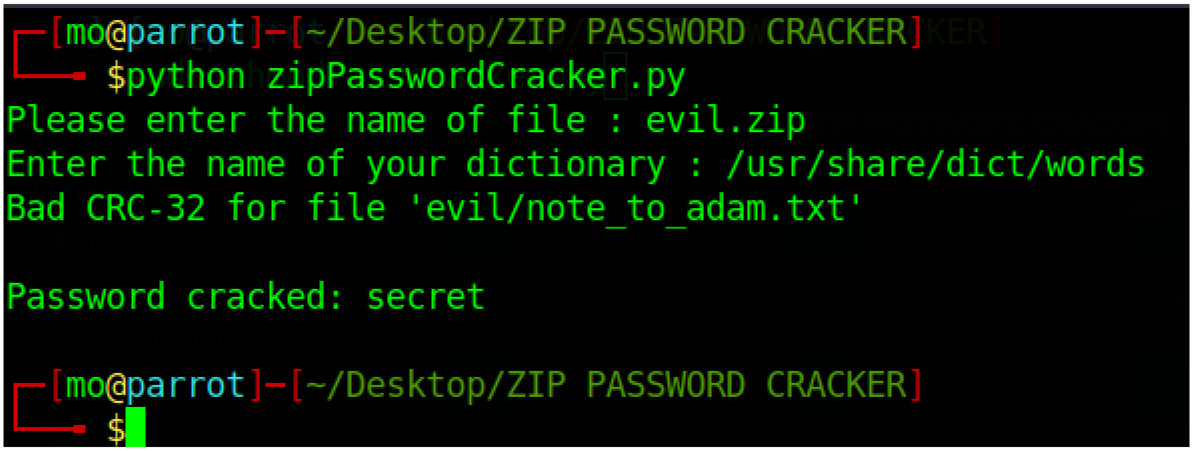
7. HOW THE TOOL IS EFFECIENT AND FLEXIBLE

The tool is very efficient and flexible, you can use different dictionary and it works fine, below i will show you how it become sucessfully to crack password by two different dictionary.

CRACKING BY USING /usr/share/dict/words dictionary

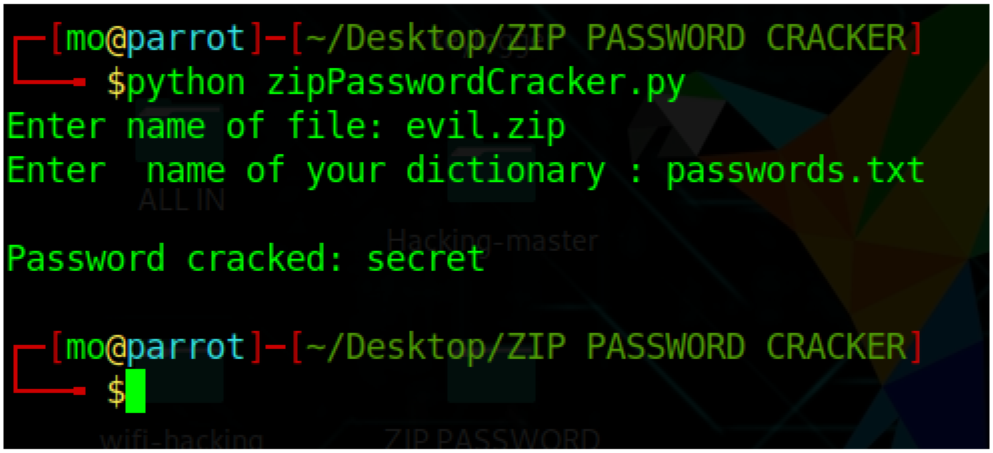
Name of the file is evil.zip

Name of the dictionary is /usr/share/dict/words dictionary



```
┌─[mo@parrot]─[~/Desktop/ZIP PASSWORD CRACKER]
└──╼ $python zipPasswordCracker.py
Please enter the name of file : evil.zip
Enter the name of your dictionary : /usr/share/dict/words
Bad CRC-32 for file 'evil/note_to_adam.txt'

Password cracked: secret

┌─[mo@parrot]─[~/Desktop/ZIP PASSWORD CRACKER]
└──╼ $
```

You can see I have used different dictionary but still cracking and that is password.



```
┌─[mo@parrot]─[~/Desktop/ZIP PASSWORD CRACKER]
└──╼ $python zipPasswordCracker.py
Enter name of file: evil.zip
Enter  name of your dictionary : passwords.txt

Password cracked: secret

┌─[mo@parrot]─[~/Desktop/ZIP PASSWORD CRACKER]
└──╼ $
```

Just compare these two images you may notice something if you carefully, the first image used dictionary present in the same directory called passwords.txt but the second image used dictionary provided by default in parrot security that is /usr/share/dict/words.

8. WARNING

Downloading different materials from unknown site is not good, and don't like to extract each zipped folder you download online , some zipped folder contain malware , and during the packing of those malicious file in that zipped folder are set to execute as soon as you finish to extract it , have ever extracted some zipped folder and you meet nothing within it ? it is possible that folder had malicious files and were set to execute as you extract it , so be carefully.

9. CONCLUSION

Inoder to become powerfully password cracker by using dictionary attack , you must be flexible and change your mind according to the environment , let's say you are trying to crack router password , you must have a file that contain all possible passwords used in routers, if you are cracking admin login page you should have a file that contain all possible passwords used by admin , be flexible and tune your mind according to the environment.

Thank you for your attention, this is just the end if you want any of the resources I have been using in this experiment you can hook me through anonymousmr663@gmail.com, if you need zipPasswordCracker.py, password.txt, Information Gathering Hacking , python keylogger, my written book, any support in hacking, you feedback and those zip file I have used for showing demonstration or you can see clear back the part of about the author, by looking at those fields I have mastered, you can choose one or more and then after I will guide and help accordingly, see what field attract you most then check me through that g-mail also I remember in my book of PANDAS TOOL FOR DATA SCIENTIST I did not provide e-mail for feedback and for those who get trouble, if you're then one faced with any problem also use the same g-mail, i hope you have enjoyed it ? , happy hour.

10. **REFERENCES**

-https://www.programcreek.com/python/example/3149/zipfile.BadZipfile

-https://www.datacamp.com/community/tutorials/zip-file

-https://realpython.com/python-exceptions/

-https://www.geeksforgeeks.org/python-string-strip-2/

-https://www.geeksforgeeks.org/time-functions-in-python-set-1-time-ctime-sleep/

-Kali Linux Cookbook - Second Edition