ZYDRA

30th Sep 2022

OVERVIEW

Zydra is one of the easy and simple tools for file password recovery and it helps to crack the password of Linux shadow files. It contains a dictionary attack or the Brute force technique for recovering the passwords. This tool can recover passwords of these file types:

- **PDF Files**
- **ZIP Files**
- **RAR Files**

Installation of Zydra:

We can find Zydra on **its** GitHub repository but before that, we will install some dependencies to work with Zydra perfectly.

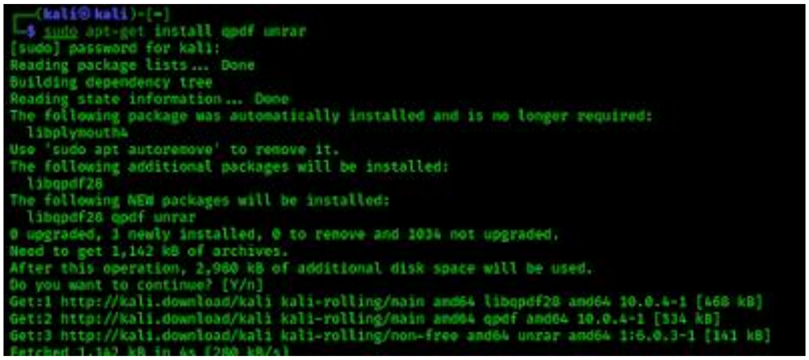
First of all, we update our system by using the following command:

```
sudo apt-get update
```

Then we download some dependencies by using the following command:

```
sudo apt-get install qpdf unrar
```

The above command will install qpdf and unrar on our system as we can see in the following screenshot:

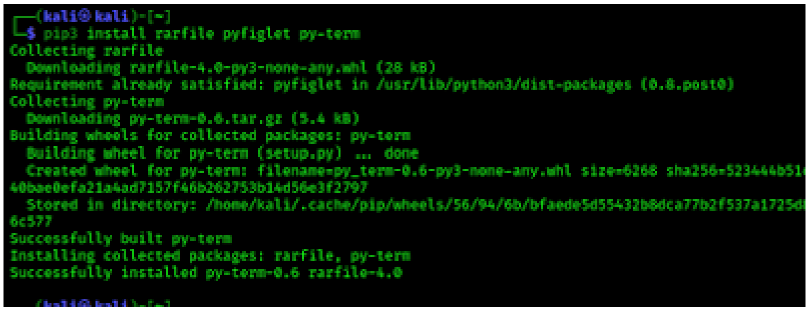


```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install qpdf unrar
[sudo] password for kali:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libplymouth4
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  libqpdf28
The following NEW packages will be installed:
  libqpdf28 qpdf unrar
0 upgraded, 3 newly installed, 0 to remove and 1034 not upgraded.
Need to get 1,142 kB of archives.
After this operation, 2,980 kB of additional disk space will be used.
Do you want to continue? [Y/n]
Get:1 http://kali.download/kali kali-rolling/main amd64 libqpdf28 amd64 10.0.4-1 [468 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 qpdf amd64 10.0.4-1 [534 kB]
Get:3 http://kali.download/kali kali-rolling/non-free amd64 unrar amd64 1:6.0.3-1 [141 kB]
Fetched 1,142 kB in 4s (280 kB/s)
```

Then we need to install some Python3 modules using pip.

```
pip3 install rarfile pyfiglet py-term
```

These will be installed on our system after using the above command as we can see it.



```
┌──(kali㉿kali)-[~]
└─$ pip3 install rarfile pyfiglet py-term
Collecting rarfile
  Downloading rarfile-4.0-py3-none-any.whl (28 kB)
Requirement already satisfied: pyfiglet in /usr/lib/python3/dist-packages (0.8.post0)
Collecting py-term
  Downloading py-term-0.6.tar.gz (5.4 kB)
Building wheels for collected packages: py-term
  Building wheel for py-term (setup.py) ... done
  Created wheel for py-term: filename=py_term-0.6-py3-none-any.whl size=6268 sha256=523444b51
40bae0efa21a4ad7157f46b262753b14d56e3f2797
  Stored in directory: /home/kali/.cache/pip/wheels/56/94/6b/bfaede5d55432b8dca77b2f537a1725d
6c577
Successfully built py-term
Installing collected packages: rarfile, py-term
Successfully installed py-term-0.6 rarfile-4.0

┌──(kali㉿kali)-[~]
```

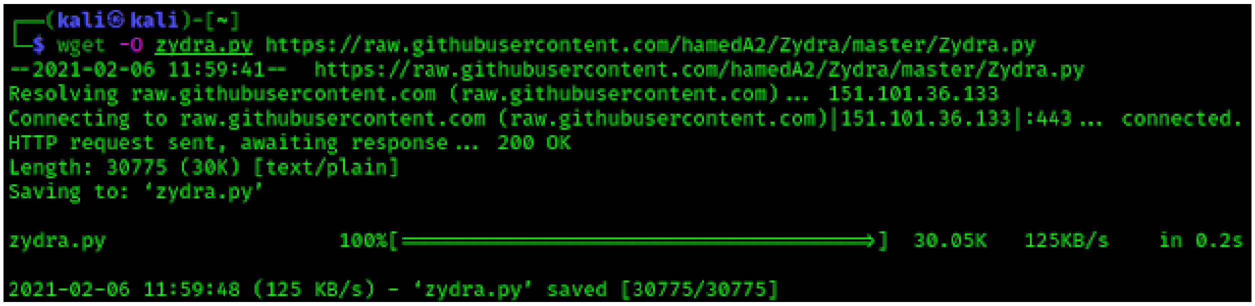
Now we just need to download figlet font "epic" for Zydra by using the following command:

```
sudo wget http://www.figlet.org/fonts/epic.flf -O /usr/share/figlet/epic.flf
```

Now it's time to download the [Zydra from GitHub](). Either we can clone the whole repository or we can just download the Python script. Let us download just the Python script by using the following command:

```
wget -O zydra.py
https://raw.githubusercontent.com/hamedA2/Zydra/master/Zydra.py
```

The python script will be saved in our current working directory by the name of zydra.py.

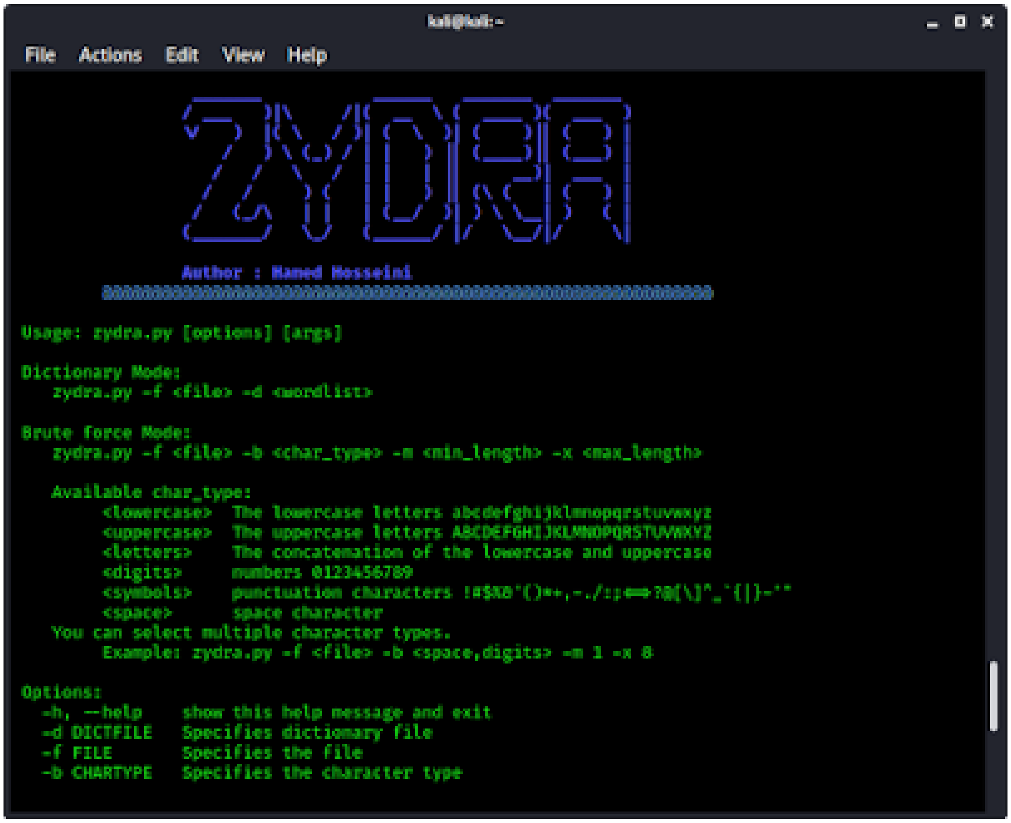


```
┌──(kali㉿kali)-[~]
└─$ wget -O zydra.py https://raw.githubusercontent.com/hamedA2/Zydra/master/Zydra.py
--2021-02-06 11:59:41--  https://raw.githubusercontent.com/hamedA2/Zydra/master/Zydra.py
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.36.133
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|151.101.36.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 30775 (30K) [text/plain]
Saving to: ‘zydra.py’

zydra.py                    100%[======================================>]  30.05K  125KB/s    in 0.2s

2021-02-06 11:59:48 (125 KB/s) - ‘zydra.py’ saved [30775/30775]
```

Now we can run the script. First of all, we check the help option by applying the following command:

```
python3 zydra.py --help
```

We can see the help menu of Zydra in the following screenshot:



```
                Author : Hamed Hosseini
        @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

Usage: zydra.py [options] [args]

Dictionary Mode:
   zydra.py -f <file> -d <wordlist>

Brute force Mode:
   zydra.py -f <file> -b <char_type> -m <min_length> -x <max_length>

   Available char_type:
        <lowercase>  The lowercase letters abcdefghijklmnopqrstuvwxyz
        <uppercase>  The uppercase letters ABCDEFGHIJKLMNOPQRSTUVWXYZ
        <letters>    The concatenation of the lowercase and uppercase
        <digits>     numbers 0123456789
        <symbols>    punctuation characters !#$%&'()*+,-./:;<=>?@[\]^_`{|}~'"
        <space>      space character
   You can select multiple character types.
        Example: zydra.py -f <file> -b <space,digits> -m 1 -x 8

Options:
  -h, --help     show this help message and exit
  -d DICTFILE    Specifies dictionary file
  -f FILE        Specifies the file
  -b CHARTYPE    Specifies the character type
```

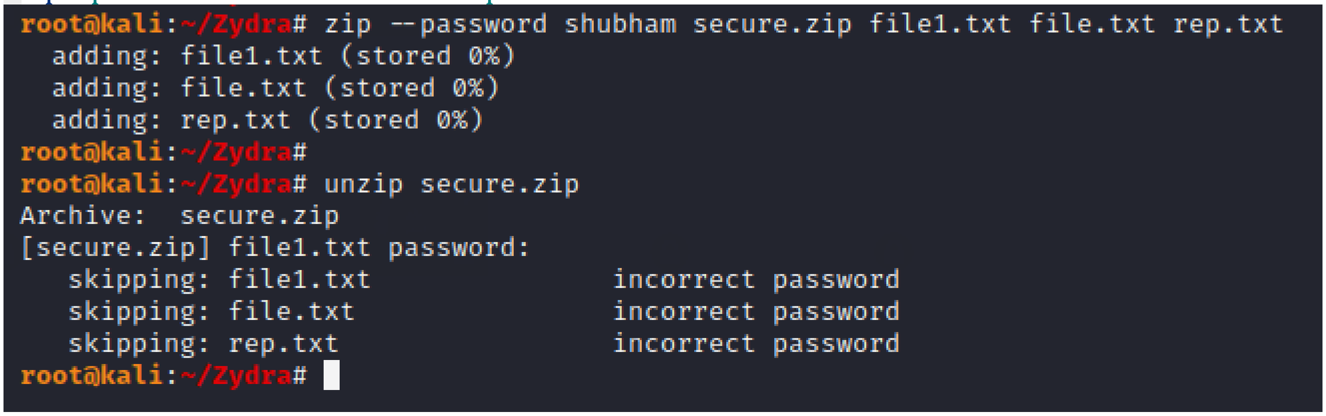
Password Cracking via Dictionary Attack:

Create ZIP file

We have to make a password-protected zip file in front of you to maintain transparency between us. Do not think so, just use the following command to create a zip file.

Command: zip –password < your password > < give zip file name > < files that you want compressed >

```
zip --password shubham secure.zip file1.txt file.txt
```

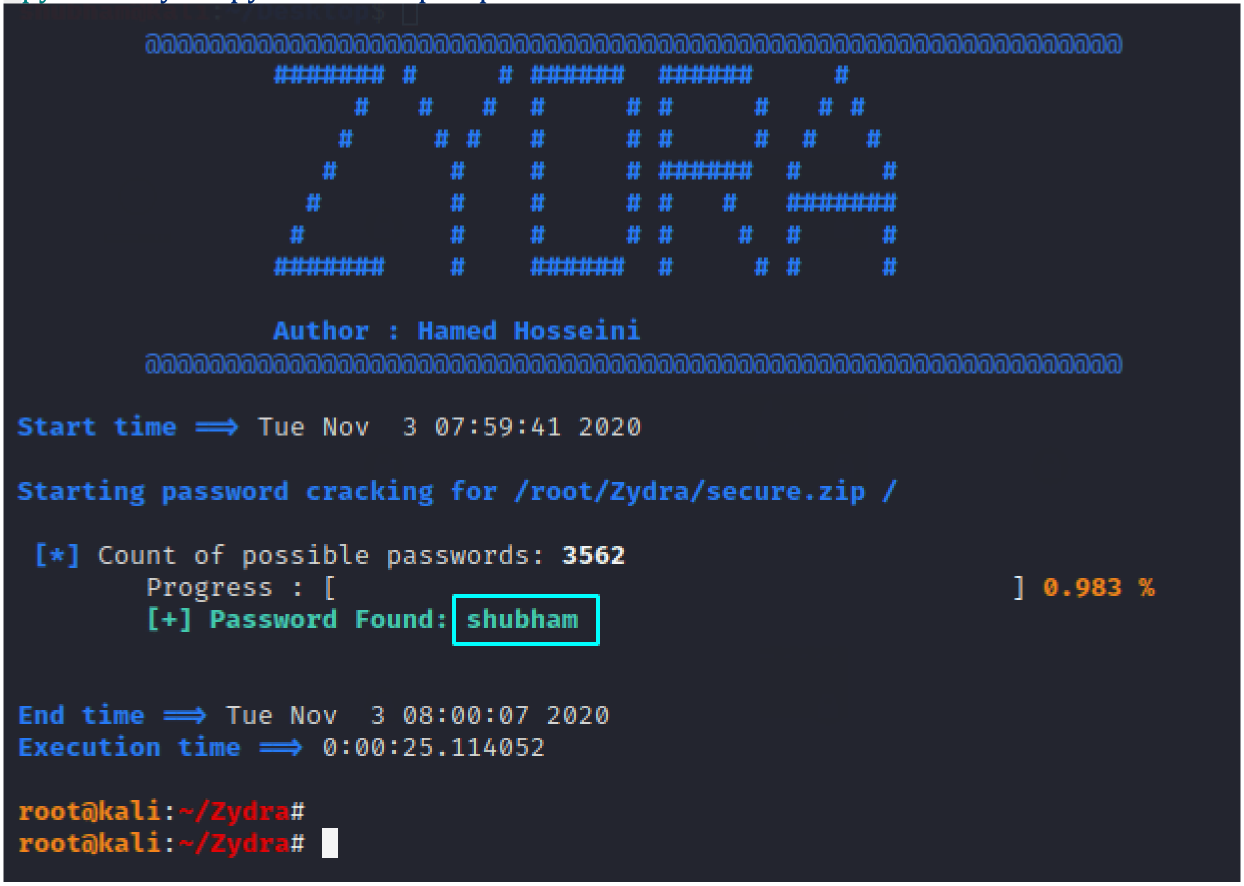


```
root@kali:~/Zydra# zip --password shubham secure.zip file1.txt file.txt rep.txt
  adding: file1.txt (stored 0%)
  adding: file.txt (stored 0%)
  adding: rep.txt (stored 0%)
root@kali:~/Zydra#
root@kali:~/Zydra# unzip secure.zip
Archive:  secure.zip
[secure.zip] file1.txt password:
   skipping: file1.txt               incorrect password
   skipping: file.txt                incorrect password
   skipping: rep.txt                 incorrect password
root@kali:~/Zydra# 
```

First, we select the dictatorial attack and as you can see we have our own wordlist to crack the zip file password.

python3 Zydra.py -f < zip file > < wordlist >

```
python3 Zydra.py -f secure.zip -d password.lst
```

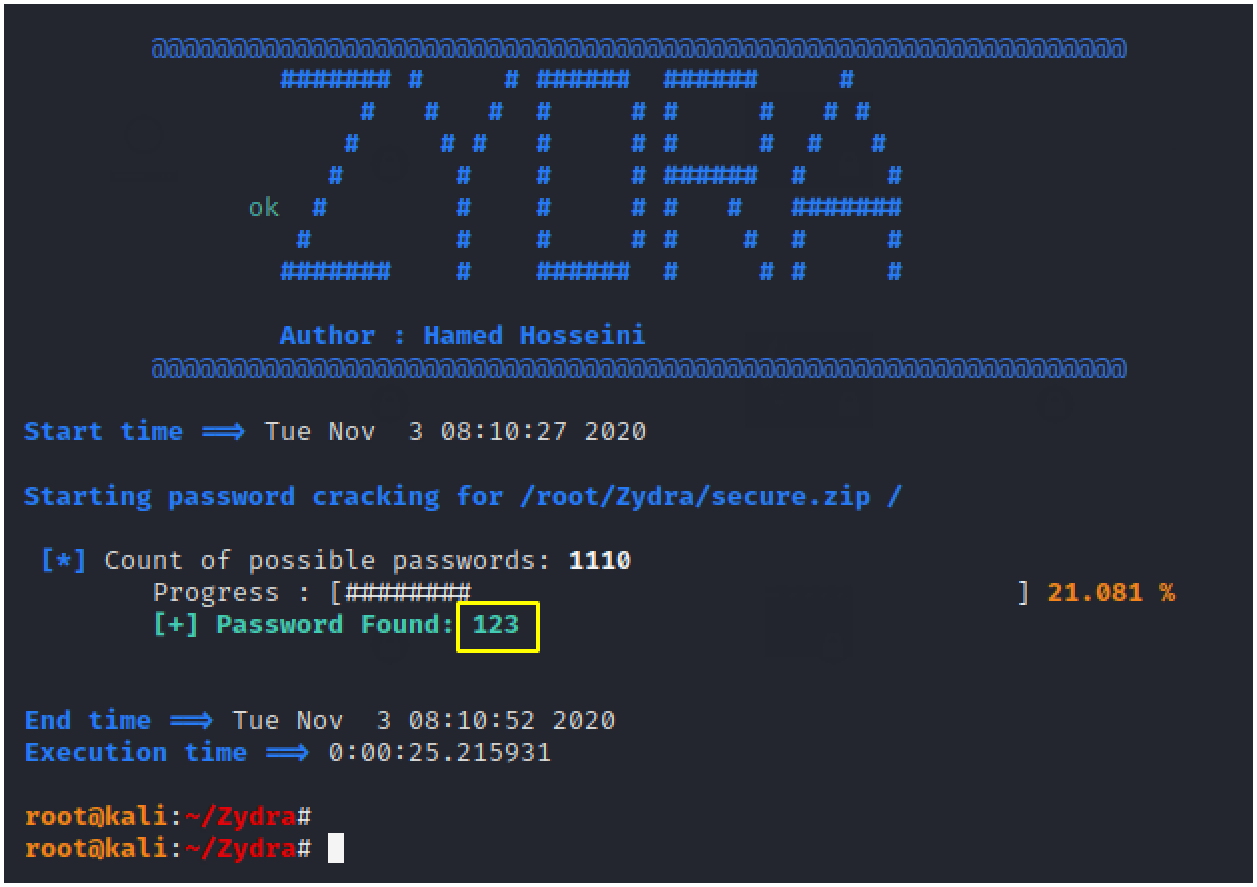


```
        @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
                ####### #     # ######  ######     #
                     #   #   #  #     # #     #   # #
                    #     # #   #     # #     #  #   #
                   #       #    #     # ######  #     #
                  #        #    #     # #   #   #######
                 #         #    #     # #    #  #     #
                #######    #    ######  #     # #     #

                Author : Hamed Hosseini
        @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

Start time ⟹ Tue Nov  3 07:59:41 2020

Starting password cracking for /root/Zydra/secure.zip /

 [*] Count of possible passwords: 3562
        Progress : [                                          ] 0.983 %
        [+] Password Found: shubham


End time ⟹ Tue Nov  3 08:00:07 2020
Execution time ⟹ 0:00:25.114052

root@kali:~/Zydra#
root@kali:~/Zydra# 
```

Password Cracking via Brute force Attack:

python3 Zydra.py -f < zip file > -b < digits, letters etc > -m < minimum > -x < maximum >

```
python3 Zydra.py -f secure.zip -b digits -m 1 -x 3
```



```
        @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
                ####### #     # ######  ######     #
                     #   #   #  #     # #     #   # #
                    #     # #   #     # #     #  #   #
                   #       #    #     # ######  #     #
              ok  #        #    #     # #   #   #######
                 #         #    #     # #    #  #     #
                #######    #    ######  #     # #     #

                Author : Hamed Hosseini
        @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

Start time ⟹ Tue Nov  3 08:10:27 2020

Starting password cracking for /root/Zydra/secure.zip /

 [*] Count of possible passwords: 1110
        Progress : [########                                  ] 21.081 %
        [+] Password Found: 123


End time ⟹ Tue Nov  3 08:10:52 2020
Execution time ⟹ 0:00:25.215931

root@kali:~/Zydra#
root@kali:~/Zydra# 
```