This blog is NOT OFFICIAL website of Kali Linux. We just share Tutorials to learn Cybersecurity.

DMCA PROTECTED

Zydra -- ZIP Password Cracker

14 February 2021 Kali Linux

+ size −

Zydra is a password recovery tool that can recover passwords from files and Linux shadow files using brute-force or dictionary attack. That means, it can **crack passwords of ZIP, RAR and PDF files**. Also it can recover passwords of Linux systems using the shadow file (shadow file stores user passwords in Linux system).

Key Features of Zydra

Zydra's main features are following:

- The most important features of Zydra is the multiprocessing feature that speeds up the program. For example if we have 8 CPU cores, Zydra will use all of them for processing at the same time.
- It can be use against Legacy ZIP files, RAR files, PDF files and shadow files.
- Cracking files password using two methods dictionary method and brute force method.
- In the brute force method, we can specify the min length and max length of the passwords, also we can specify the type of characters that may be used in the password.
- A percent progress bar showing how much of the process has been performed.
- Error handling.

Installing Zydra on Kali Linux

We can found Zydra on it's GitHub repository but before that we will install some dependencies to work Zydra perfectly.

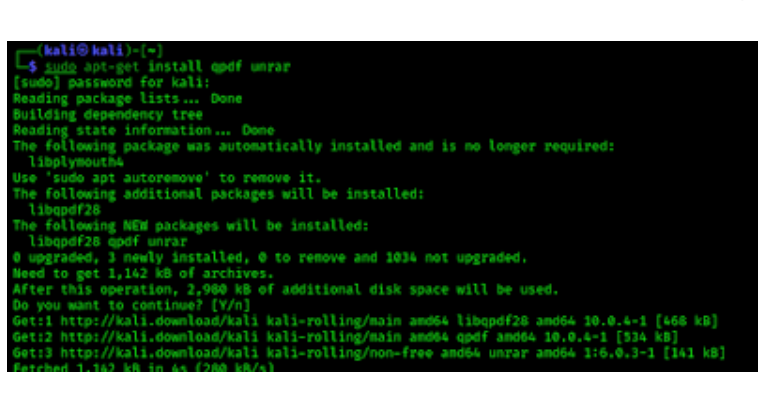
First of all we update our system by using following command:

```
sudo apt-get update
```

Then we download some dependencies by using 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:

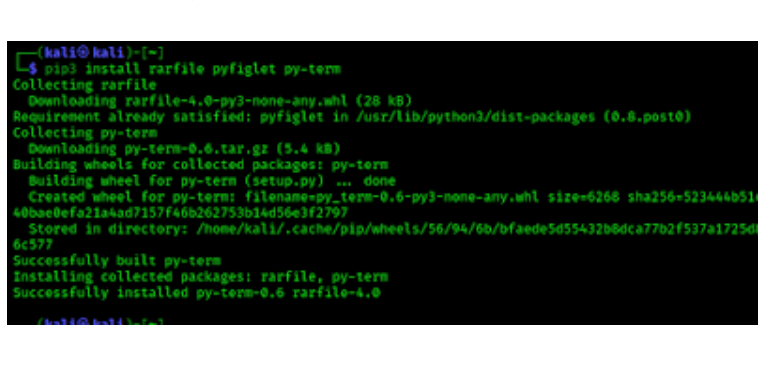


```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install qpdf unrar
[sudo] password for kali:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libplymouth4
Use 'sudo apt autoremove' to remove 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]
```

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 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
```

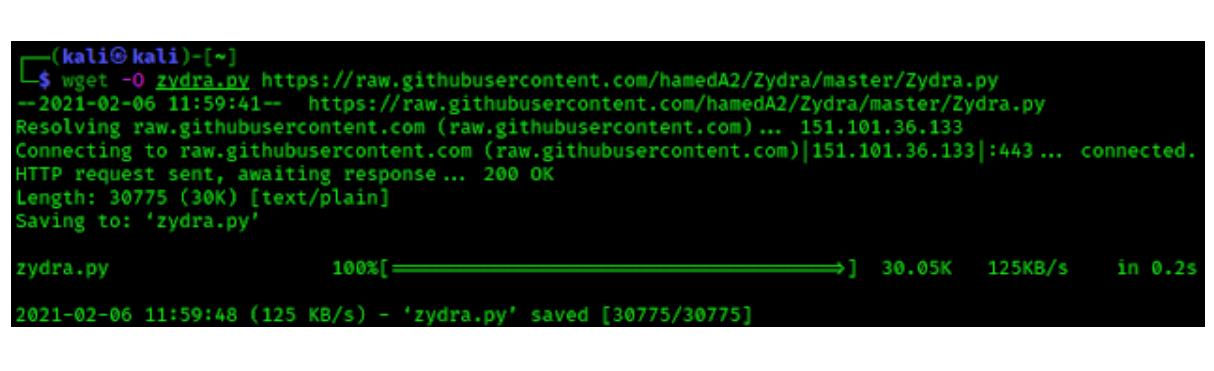
Now we just need to download figlet font "epic" for Zydra by using following command:

```
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 we download just the Python script by using following command:

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

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

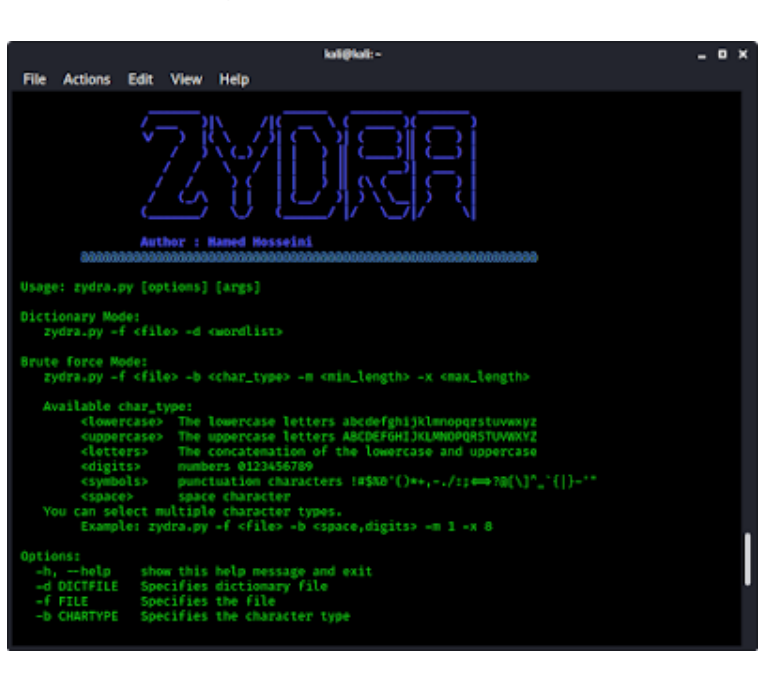


```
┌──(kali㉿kali)-[~]
└─$ wget -O zydra.py https://raw.githubusercontent.com/hamedA2/Zydra/master/Zydra.py
--2021-02-06 11:59:41--  https://raw.githubusercontent.com/hamedA2/Zydra/master/Zydra.py
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 151.101.36.133
Connecting to raw.githubusercontent.com (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 following command:

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

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

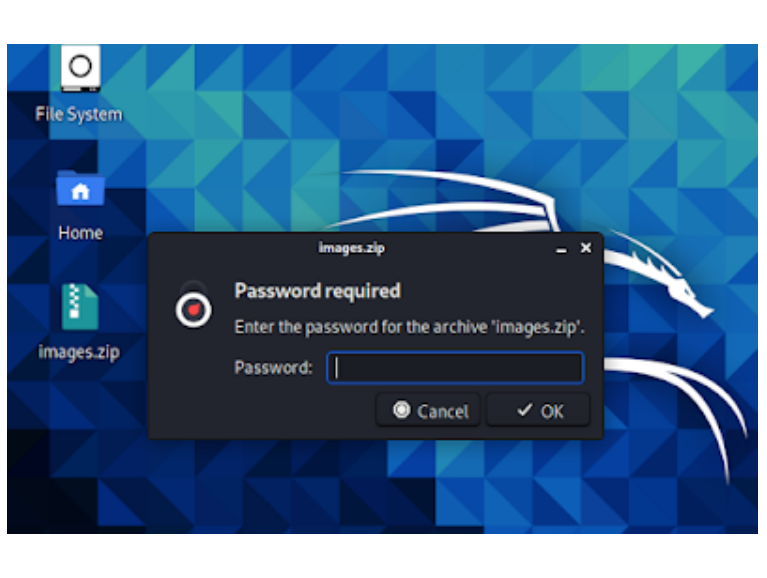


```
Author : Hamed Hosseini

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
```

Either we can read the boring help section of Zydra or continue reading out guide to know the important uses of this tool.

How to Crack ZIP files password on Kali Linux

Here we have a ZIP file on our Desktop which is protected by a password. We can see that it prompt for password on the following screenshot:

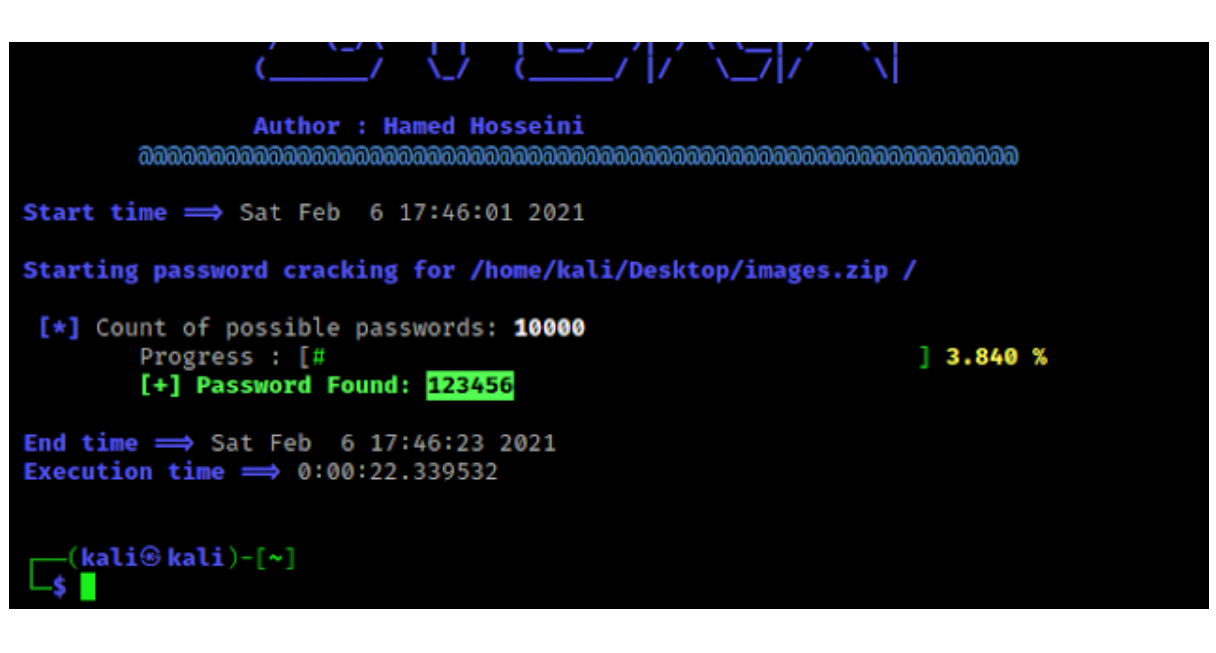


Now we try to brake the password with dictionary attack. To perform this we **need a password list**. We will use the 10k-most-common.txt (password list). It comes with our Kali Linux (/usr/share/seclists/Passwords/Common-Credentials/10k-most-common.txt), which contains 10,000 most commonly used passwords.

So we open our terminal and our command will be following:

```
python3 zydra.py -f /home/kali/Desktop/images.zip -d /usr/share/seclists/Passwords/Common-
```

Here we have used the `-f` flag to specify the location of the ZIP file (in our case which is /home/kali/Desktop/images.zip) and using the `-d` flag we have specify the location of the dictionary (password list). Output shown in the following screenshot:



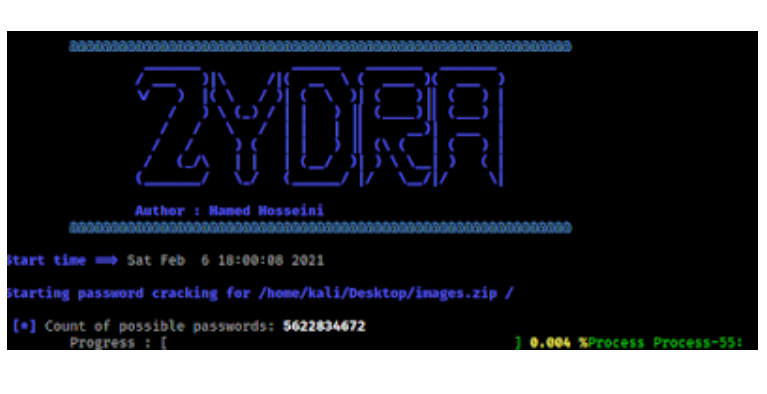
```
Author : Hamed Hosseini

Start time ⟹ Sat Feb  6 17:46:01 2021

Starting password cracking for /home/kali/Desktop/images.zip /

 [+] Count of possible passwords: 10000
       Progress : [#                                        ] 3.840 %
       [+] Password Found: 123456

End time ⟹ Sat Feb  6 17:46:23 2021
Execution time ⟹ 0:00:22.339532

┌──(kali㉿kali)-[~]
└─$
```

On the above screenshot we can see that we have successfully **cracked the password of the ZIP file using Zydra.**

This is how we can use the dictionary attack we also can try without password list. In that case we need to use brute-force attack and we need to specify the type of characters that may be used in the password.

```
python3 zydra.py -f /home/kali/Desktop/images.zip -b digits,symbols -m 4 -x 6
```

Here we have choose `-b` flag for brute force attack and specified our password (mixing digits and symbols), then we use `-m` flag for minimum length of our password (we choose 4) and `-x` for maximum length of our password (we choose 6).



```
Author : Hamed Hosseini

Start time ⟹ Sat Feb  6 18:00:08 2021

Starting password cracking for /home/kali/Desktop/images.zip /

 [+] Count of possible passwords: 5622834672
       Progress : [                                         ] 0.004 %Process Process-55:
```

On the above screenshot we can see that Zydra has created a count of possible password list which is very big (5622834672 passwords). Which will take a lot of time. Also may gives error (but the scan continues).

Note: Zydra can recover legacy ZIP files password (The standard one). We have created a ZIP file on Linux system (using Archive Manager) Zydra can't break it. But ZIP files created from Windows and internet works perfectly.

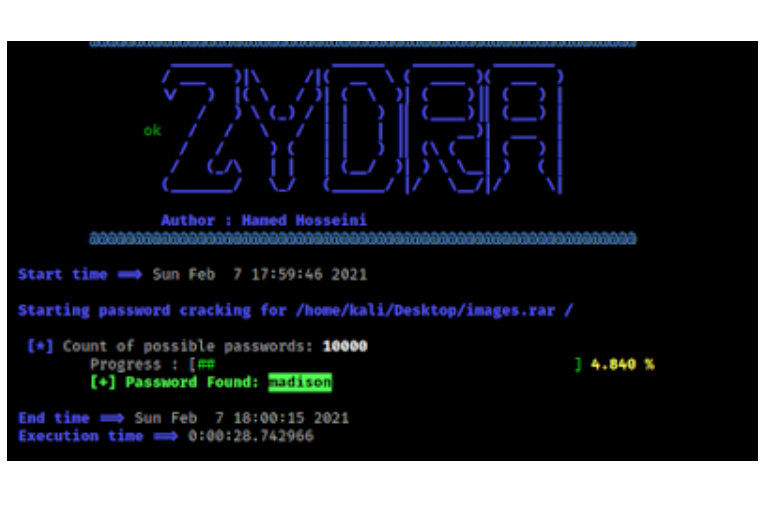
How to crack RAR files password using Zydra

Cracking a RAR file's password is very similar to cracking ZIP file's password on Zydra. To do it we need to run following command on our terminal:

```
python3 zydra.py -f /home/kali/Desktop/images.rar -d /usr/share/seclists/Passwords/Common-
```

Then Zydra will start scanning the process. Here we have again choose 10k-most-common.txt password list inside our /usr/share/seclists/Passwords directory which is specified by `-d` flag and our target RAR file is specified by `-f` flag located on our Desktop.

After waiting very few moments we got our password, as we can see in the screenshot:



```
ok
Author : Hamed Hosseini

Start time ⟹ Sun Feb  7 17:59:46 2021

Starting password cracking for /home/kali/Desktop/images.rar /

 [+] Count of possible passwords: 10000
       Progress : [##                                       ] 4.840 %
       [+] Password Found: madison

End time ⟹ Sun Feb  7 18:00:15 2021
Execution time ⟹ 0:00:28.742966
```

Now we can see on the above screenshot that we have successfully recovered the password of the RAR file.

We also can use bruteforce attack to recover the password. To do that we need to use `-b` flag in the place of `-d` flag and we should specify the type of password and length as we did on ZIP files section, an example command is following:

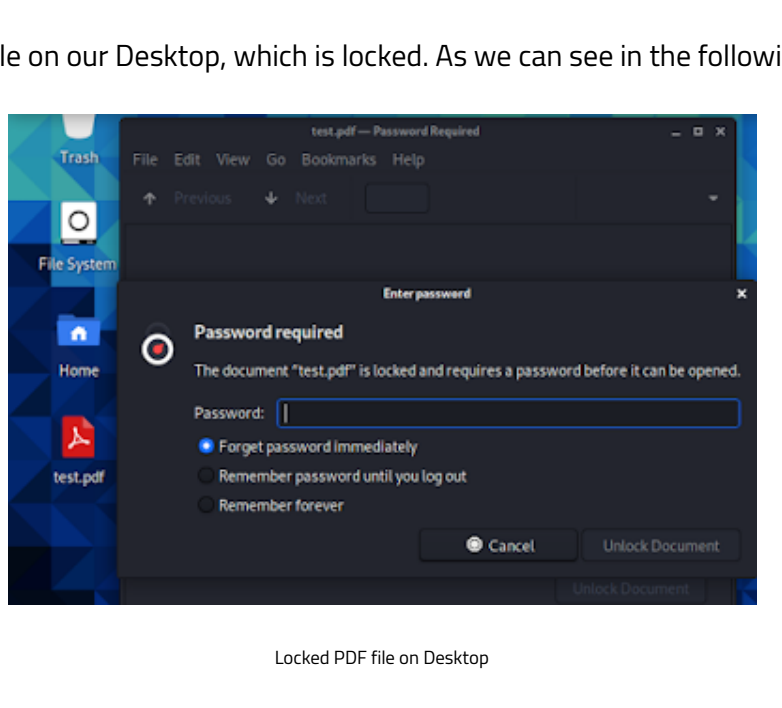
```
python3 zydra.py -f /home/kali/Downloads/file.rar -b digits,symbols -m 4 -x 6
```

This is how we can **Crack RAR file's password on our Kali Linux** system.

How to Break or Crack Password of PDF file

Cracking PDF file's password is also very similar as ZIP and RAR. We just need to use Zydra and tell Zydra the location of PDF file and the location of password list.

Here we have an example PDF file on our Desktop, which is locked. As we can see in the following screenshot:



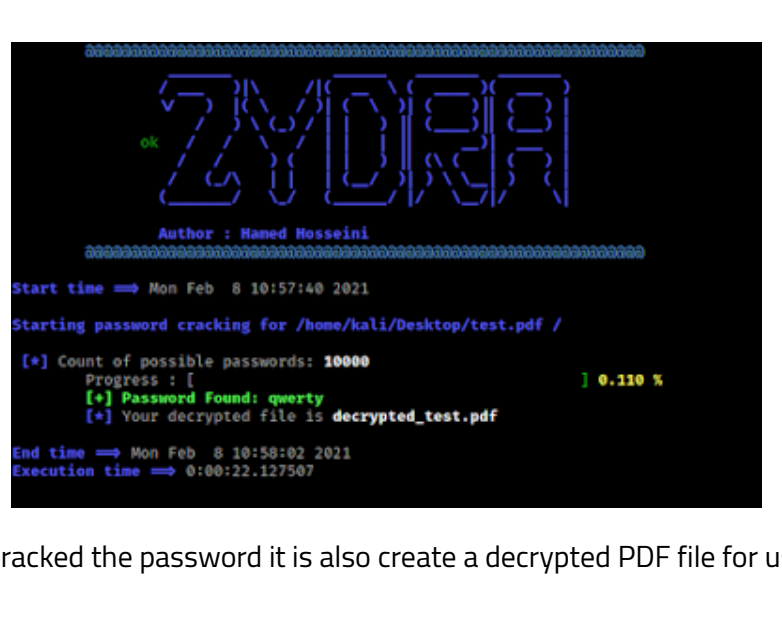
Trash
File System
Home
test.pdf
test.pdf — Password Required
File Edit View Go Bookmarks Help
Previous
Next
Enter password
Password required
The document "test.pdf" is locked and requires a password before it can be opened.
Password:
Forget password immediately
Remember password until you log out
Remember forever
Cancel
Unlock Document

Locked PDF file on Desktop

Now we run Zydra and try to break the password of this PDF file by using following command:

```
python3 zydra.py -f /home/kali/Desktop/test.pdf -d /usr/share/seclists/Passwords/Common-Cre
```

Here we have used `-f` flag to specify our PDF file location and we used `-d` to specify location of our passsword list. The output of the command shows in the following screenshot:



```
ok
Author : Hamed Hosseini

Start time ⟹ Mon Feb  8 10:57:40 2021

Starting password cracking for /home/kali/Desktop/test.pdf /

 [+] Count of possible passwords: 10000
       Progress : [                                         ] 0.110 %
       [+] Password Found: qwerty
       [+] Your decrypted file is decrypted_test.pdf

End time ⟹ Mon Feb  8 10:58:02 2021
Execution time ⟹ 0:00:22.127507
```

We can see that Zydra just not cracked the password it is also create a decrypted PDF file for us.

This is how we can **crack the password of a PDF file** using Zydra on our Kali Linux system.

Recover Linux passwords from shadow file

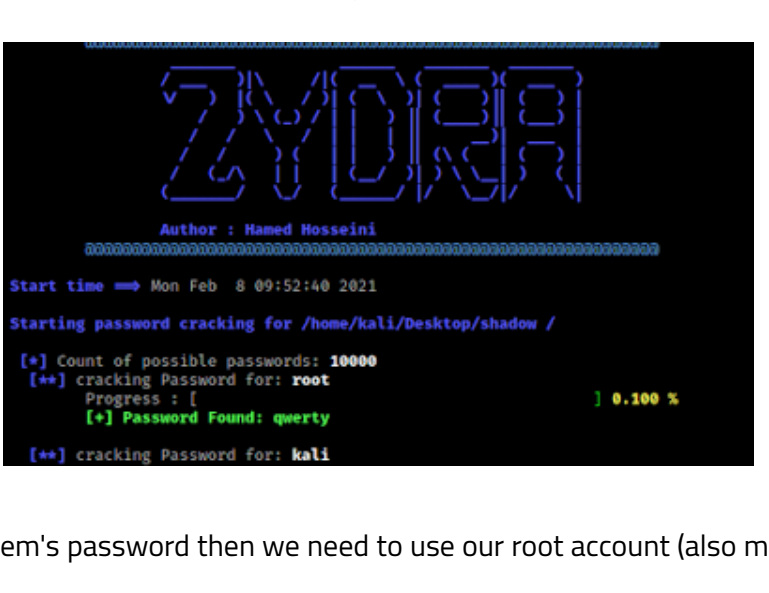
Linux's users password stored (encrypted) on the shadow file,located on /etc/shadow. Using Zydra we also able to crack shadow file's passwords. Zydra will crack the passwords one by one for every user on the system.

Either we can copy the shadow file from a system or we can run Zydra on the target system. Here for an example we run copied all the texts from shadow file from another system and saved it on our system (Desktop) in a file called shadow without file extension and try recover the password.

To do so we can apply following command on our terminal:

```
python3 zydra.py -f /home/kali/Desktop/shadow -d /usr/share/seclists/Passwords/Common-Cre
```

The screenshot shows that Zydra cracked one user and trying for the other



```
Author : Hamed Hosseini

Start time ⟹ Mon Feb  8 09:52:40 2021

Starting password cracking for /home/kali/Desktop/shadow /

 [+] Count of possible passwords: 10000
  [**] cracking Password for: root
       Progress : [                                         ] 0.100 %
       [+] Password Found: qwerty

  [**] cracking Password for: kali
```

If we need to crack our own system's password then we need to use our root account (also may need to install rarfile pyfiglet py-term there). The command will be following(we need to log in as root, sudo command from non-root user may show error here):

```
python3 zydra.py -f /etc/shadow -d /usr/share/seclists/Passwords/Common-Credentials/10k-m
```

Conclusion

This is how to **crack password protected ZIP, RAR, PDF files using Zydra on Kali Linux** or other debian based Linux system. We also can recover password of Linux users using Zydra.

This is created for educational perpose only we also can use it to recover forgotten password of files. But using Zydra against other's protected file will be considered crime as per law. So please do not use it to others without proper permission. We will not be responsible if anyone did this.

Liked our article then please follow our blog's email subscription for free. We also have Telegram group to direct conversation with everyone. We also update our new articles on Twitter and GitHub make sure to follow us there.

For any kind of query or problem our comment box is always open to everyone. We read each and every comment and we always reply.

Publish | Tweet | Share | Save | Share | Send | Print

You may like these posts

Comments

No comments

Show Comments Only | ✓ Show Comments & Replies

Post a Comment

Please do not spam here. It is comment box not a spambox. Promotional links are not allowed.

Join Telegam Group

Join us on Telegram

Popular Posts

26 April 2021
Facebook Account Hacking -- The Best 9 Methods
So, we have searched for Facebook account hacking . Almost all new comer in hacking field wants to hack Facebook or ...

05 July 2019
Easy Port Forwarding using SSH
Sometime we need to run our localhost website or server over internet. To do this we need to forward our port that oth...

01 April 2021
Canarytokens -- Danger For Attackers
Canarytokens are one type of customisable unique links that someone click or access this links we can get many informa...

09 October 2021
Best USB WiFi Adapter For Kali Linux 2021 [Updated October]
Best WiFi Adapter for Kali Linux The all new Kali Linux 2021.1 was rolling out and we can simply use it as our ...

19 August 2019
SocialFish V3 -- Next Generation Phishing Toolkit | Kali Linux
Phishing is to easiest method to get anyone's social media password. We have learned many ways to do phishing in s...

Recent posts

Comments

James Woodard — September 21, 2022 at 10:37 AM
If you are having troubles accessing your cryptocurrency investment account or unable to make withdrawals from your wallet then i suggest you contact (recoverfunds.investigator247 @ gmail . com). This privateinvestigator saved me when I thought I lost my ($180 k) 180 thousand dollars that I invested in Mlee platform.He used a brutal force program that got me back into my
Leave Reply

Anonymous — September 20, 2022 at 9:23 PM
I never believed it was possible to recover lost cryptocurrency until few days ago I lost $10.000 to an online purchase scam, I was so sad because I wouldn't afford to purchase another and then my step mom introduced me to this guy that helped me recover the full amount, I was shocked and didn't even know it was possible. You can contact him through (hackerlloriservice@gmail.com) or
Leave Reply

Anonymous — September 20, 2022 at 9:23 PM
I never believed it was possible to recover lost cryptocurrency until few days ago I lost $10.000 to an online purchase scam, I was so sad because I wouldn't afford to purchase another and then my step mom introduced me to this guy that helped me recover the full amount, I was shocked and didn't even know it was possible. You can contact him through (hackerlloriservice@gmail.com) or
Leave Reply

Anonymous — September 18, 2022 at 5:46 PM
it is very easy
Leave Reply

Anonymous — September 16, 2022 at 12:37 PM
how to install ngrok in kali linux, i'm not understand how to install
Leave Reply

Labels

Attack Strategies | Configure | Custom Tools For Kali Linux | Forensic | Information Gathering Tools | Password Attacks | Scanning

Pages

Privacy Policy
Terms and Condition
Write for us
Contact
About

Featured Post

WeBaCoo -- Web Backdoor Cookie Script-Kit
Kali Linux 23 September 2022
WeBaCoo (Web Backdoor Cookie) is a web backdoor script tool used to provide a stealth terminal-like connection via HTTP between the client and web server. It is a post exploitation tool capable to maintain access to a compromised web ser...

All copyrights reserved