

R V COLLEGE OF ENGINEERING

Name: Dhanush M USN: 1RV18IS011 Dept/Lab: ISE/CSDF Expt No.: 03 b
Date: 03/12/2021 Title: PASSWORD ATTACK TOOLS

b. CRUNCH

INTRODUCTION

Collection of a different combination of characters is called a wordlist. And in order to crack a password or a hash, we need to have a good wordlist which could break the password. So to do so we have a tool in kali Linux called **crunch**.

Crunch is a wordlist generating tool that comes pre-installed with Kali Linux. It is used to generate custom keywords based on wordlists. It generates a wordlist with permutation and combination. We could use some specific patterns and symbols to generate a wordlist.

Objectives - To generate wordlists with certain patterns and symbols in order to break passwords. .

EXECUTION STEPS

Basic syntax of crunch -

This structure takes in mandatorily the minimum and maximum number of characters to be used to form words. The argument **-f** is used to access files from some specific charsets of crunch and **-o** is to save the output in the mentioned file, this file will be created during execution. By default crunch uses only lowercase alphabets in its charset.

Syntax: *crunch <min> <max> -f <charset> -t <pattern> -o <filename>*

Other arguments,

- **-t** is used to specify our own patterns of characters. The symbols used to represent some group of characters are as follows,
 - , for all uppercase letters.
 - @ for all lowercase letters.
 - % for all numeric characters.
 - ^ for all special characters.
- **-c** is used to create a file based on breaking output with respect to the number of lines that were specified.
- **-b** is used to split and create files based on the size specified.
- **-z** is used to compress the files created in compressed format, for example gzip, bzip, lzma, 7z.
- **-i** is used to generate all the possible passwords from the specified wordlist in inverted format.

Examples cases -

1.

```
(root@kali)-[/home/kali]
# crunch 3 5 -f /usr/share/crunch/charset.lst mixalpha -o file.txt | more
Crunch will now generate the following amount of data: 2318344704 bytes
2210 MB
2 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 387656256
```

```
crunch: 100% completed generating output
```

2.

```
(root@kali)-[/home/kali]
# crunch 3 3 -t ,%% -b 1kb -o START -i | more
Crunch will now generate the following amount of data: 10400 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 2600
```

```
crunch: 19% completed generating output
```

```
crunch: 48% completed generating output
```

```
crunch: 67% completed generating output
```

```
crunch: 86% completed generating output
```

```
crunch: 100% completed generating output
```

3.

```
(root@kali)-[/home/kali]
# crunch 5 5 -f /usr/share/crunch/charset.lst ualpha -t Aa00Dd -l a00000 -c 100 -o START | more
Crunch will now generate the following amount of data: 600 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 100
crunch: 100% completed generating output
crunch: 200% completed generating output
crunch: 300% completed generating output
crunch: 400% completed generating output
crunch: 500% completed generating output
crunch: 600% completed generating output
crunch: 676% completed generating output
```

```
(root@kali)-[/home/kali]
# crunch 4 6 -p hello world !
Crunch will now generate approximately the following amount of data: 72 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 6
!helloworld
!worldhello
hello!world
helloworld!
world!hello
worldhello!
```

4.

CONCLUSION

1. Crunch can generate a wordlist subject to the conditions you specify and its output file can be used in any other program or file.
2. Crunch can generate all possible permutations and combinations.
3. The generated wordlist is used by John the Ripper which is a free password cracking software tool developed by Openwall. It is one of the most popular password testings and breaking programs as it combines a number of password crackers into one package, auto-detects password hash types, and includes a customizable cracker

REFERENCES

1. Crunch Password list generation in Kali Linux - <https://www.hackingtutorials.org/general-tutorials/crunch-password-list-generation>
2. Kali Linux - Crunch Utility - <https://www.geeksforgeeks.org/kali-linux-crunch-utility>
3. Comprehensive Guide on Crunch Tool - <https://www.hackingarticles.in/comprehensive-guide-on-crunch-tool>