

ROLL NO:241901047
NAME:KEERTHISRI D

Exercise-2

Cracking the hashes using John-the-Ripper tool

Aim:

To install and crack the hashed passwords using John-the-Ripper tool in Kali Linux.

Algorithm:

1. Install John-the-Ripper on your system using sudo apt install john
2. Prepare the hash file hashes.txt that is to be cracked.
3. Run John-the-Ripper specifying the path to the wordlist.txt and hashes.txt
4. Monitor the cracking process using status option in another terminal

Output:

```
root@ip-10-10-88-66:~  
File Edit View Search Terminal Help  
root@ip-10-10-88-66:~# sudo apt-get install john  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  docutils-common gir1.2-goa-1.0 gir1.2-snapd-1 libpkcs11-helper1  
  linux-headers-4.15.0-115 linux-headers-4.15.0-115-generic  
  linux-image-4.15.0-115-generic linux-modules-4.15.0-115-generic  
  linux-modules-extra-4.15.0-115-generic python-bs4 python-chardet  
  python-dicttoxml python-dnspython python-html5lib python-jsonrpclib  
  python-lxml python-mechanize python-olefile python-pypdf2 python-slowaes  
  python-webencodings python-xlsxwriter python3-botocore python3-docutils  
  python3-jmespath python3-pygments python3-roman python3-rsa  
  python3-s3transfer  
Use 'sudo apt autoremove' to remove them.  
The following additional packages will be installed:  
  john-data  
The following NEW packages will be installed  
  john john-data  
0 to upgrade, 2 to newly install, 0 to remove and 356 not to upgrade.  
Need to get 4,466 kB of archives.  
After this operation, 7.875 kB of additional disk space will be used.
```

```
root@ip-10-10-233-209:~  
File Edit View Search Terminal Help  
root@ip-10-10-233-209:~# echo -n joshua1993| md5sum | awk '{print $1}' > hashes.txt  
root@ip-10-10-233-209:~# cat hashes.txt  
046df2d40bc0a99fd11a1cc0a8e67434  
root@ip-10-10-233-209:~# john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt  
Using default input encoding: UTF-8  
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])  
Warning: no OpenMP support for this hash type, consider --fork=2  
Press 'q' or Ctrl-C to abort, almost any other key for status  
joshua1993      (?)  
1g 0:00:00:00 DONE (2024-06-19 07:30) 33.33g/s 6668Kp/s 6668Kc/s 6668KC/s kensley..joseph85  
Use the "--show --format=Raw-MD5" options to display all of the cracked password  
s reliably  
Session completed.  
root@ip-10-10-233-209:~#
```

```
root@ip-10-10-233-209:~  
File Edit View Search Terminal Help  
0g 0:00:00:01 0g/s 0p/s 0c/s 0C/s  
root@ip-10-10-233-209:~# john --status  
0g 0:00:00:01 3/3 0g/s 71632p/s 71632c/s 143264C/s
```

Result: Thus, successfully installed John-the-Ripper tool and cracked the password hashes