

Practical – 11

Perform brute force attack using John the RIPPER.

Introduction -

John the Ripper is a free password cracking tool that runs on a large number of different platforms. It is one of the most used password cracking tools because it combines several other password crackers into a single package and has a number of handy features such as automatic hash type detection. Cracking password in Kali Linux using John the Ripper is very straight forward. In this post, I will demonstrate that. John the Ripper uses a 2-step process to cracking a password. First it will use the passwd and shadow file to create an output file. Next, you then actually use dictionary attack against that file to crack it. In short, John the Ripper will use the following two files:

```
/etc/passwd
/etc/shadow
```

Unshadowing Password

The unshadow command will combine the extrics of /etc/passwd and /etc/shadow to create

Cmd :- unshadow /etc/passwd /etc/shadow > /root/my_passwd

```
Do you want to install it? (N/y)n
(root@kali)~/home/kali
# unshadow /etc/passwd /etc/shadow > /root/johns_passwd
```

Cracking process with John the Ripper

At this point we just need a dictionary file and get on with cracking. John comes with it's own small password file and it can be located in **/usr/share/john/password.lst**.

Cmd :- john --wordlist=/usr/share/john/password.lst /root/my_passwd

```
(root@kali)~/home/kali
# john --wordlist=/usr/share/john/password.lst /root/johns_passwd
Using default input encoding: UTF-8
Loaded 1 password hash (HMAC-SHA256 [password is key, SHA256 256/256 AVX2 8x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:00 DONE (2024-02-22 04:19) 0g/s 354600p/s 354600c/s 354600C/s 123456..sss
Session completed.
```

decryption cmd :- john --format-crypt /usr/share/john/password.lst /root/my_passwd

```

root@kali: /home/kali
File Actions Edit View Help
john --format-crypt /usr/share/john/password.lst /root/johns_passwd
Warning: hash encoding string length 66, type id #0
appears to be unsupported on this system; will not load such hashes.
Warning: hash encoding string length 65, type id #0
appears to be unsupported on this system; will not load such hashes.
Warning: hash encoding string length 68, type id #0
appears to be unsupported on this system; will not load such hashes.
Warning: hash encoding string length 67, type id #0
appears to be unsupported on this system; will not load such hashes.
Warning: hash encoding string length 64, type id #0
appears to be unsupported on this system; will not load such hashes.
Warning: hash encoding string length 31, type id #0
appears to be unsupported on this system; will not load such hashes.
Warning: hash encoding string length 30, type id #0
appears to be unsupported on this system; will not load such hashes.
Using default input encoding: UTF-8
Loaded 3 password hashes with 3 different salts (crypt, generic crypt(3) [??/64])
Loaded hashes with cost 1 (algorithm [1:descript 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) varying from 0 to 1
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 94 candidates buffered for the current salt, minimum 96 needed for performance.
kali (kali)
Warning: Only 1 candidate buffered for the current salt, minimum 96 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
12345 (john)
Proceeding with incremental:ASCII
2g 0:00:01:07 3/3 0.02985g/s 423165p/s 423168c/s 423168C/s blinkase..blingeng
2g 0:00:01:08 3/3 0.02914g/s 424988p/s 424991c/s 424991C/s bcop9s..bcomos
Use the "--show" option to display all of the cracked passwords reliably
Session aborted

```

it can be seen by :- `john --show /root/my_passwd`

```

(root@kali)-[/home/kali]
# john --show /root/johns_passwd
kali:kali:1000:1000::,,:/home/kali:/usr/bin/zsh

1 password hash cracked, 1 left

(root@kali)-[/home/kali]
#

```