# Cracking password in Kali Linux using John the Ripper

John the Ripper is a free password cracking software tool. Initially developed for the Unix operating system, it now runs on fifteen different platforms (eleven of which are architecture-specific versions of Unix, DOS, Win32, BeOS, and OpenVMS). It is one of the most popular password testing and breaking programs as it combines a number of password crackers into one package, autodetects password hash types, and includes a customizable cracker. It can be run against various encrypted password formats including several crypt password hash types most commonly found on various Unix versions (based on DES, MD5, or Blowfish), Kerberos AFS, and Windows NT/2000/XP/2003 LM hash. Additional modules have extended its ability to include MD4-based password hashes and passwords stored in LDAP, MySQL, and others. Cracking password in Kali Linux using John the Ripper is very straight forward. In this post, I will demonstrate that.


John the Ripper is different from tools like Hydra. Hydra does blind brute-forcing by trying username/password combinations on a service daemon like ftp server or telnet server. John however needs the hash first. So the greater challenge for a hacker is to first get the hash that is to be cracked. Now a days hashes are more easily crackable using free rainbow tables available online.

Just go to one of the sites, submit the hash and if the hash is made of a common word, then the site would show the word almost instantly. Rainbow tables basically store common words and their hashes in a large database. Larger the database, more the words covered.

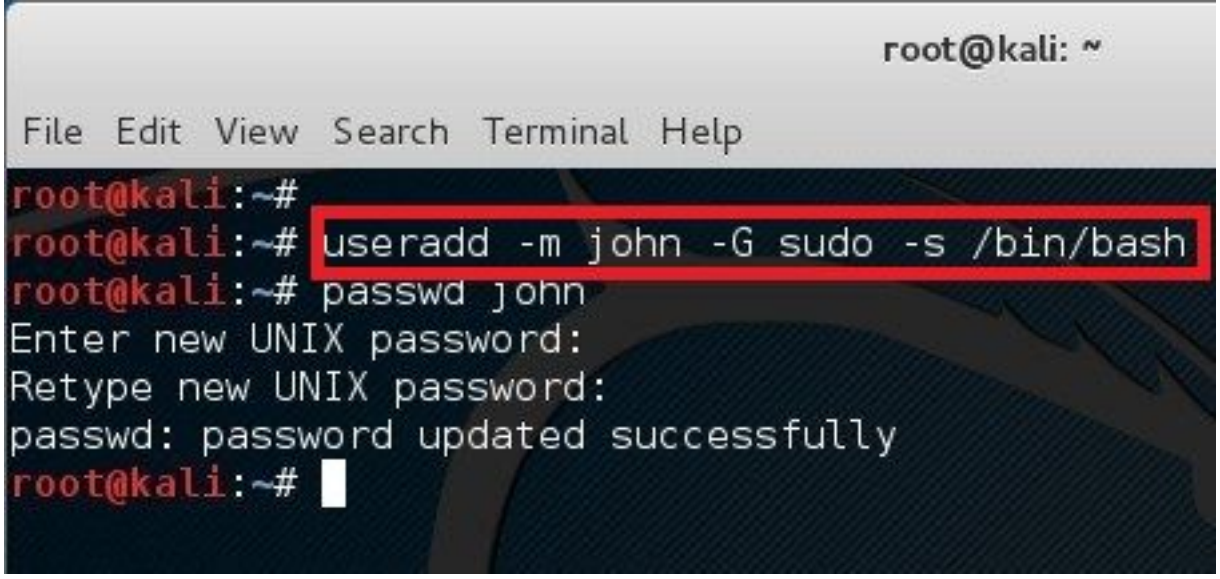
One of the modes John the Ripper can use is the dictionary attack. It takes text string samples (usually from a file, called a wordlist, containing words found in a dictionary or real passwords cracked before), encrypting it in the same format as the password being examined (including both the encryption algorithm and key), and comparing the output to the encrypted string. It can also perform a variety of alterations to the dictionary words and try these. Many of these alterations are also used in John's single attack mode, which modifies an associated plaintext (such as a username with an encrypted password) and checks the variations against the hashes.

John also offers a brute force mode. In this type of attack, the program goes through all the possible plaintexts, hashing each one and then comparing it to the input hash. John uses character frequency tables to try plaintexts containing more frequently used characters first. This method is useful for cracking passwords which do not appear in dictionary wordlists, but it takes a long time to run.

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
```

## Cracking password using John the Ripper




In Linux, password hash is stored in /etc/shadow file. For the sake of this exercise, I will create a new user names john and assign a simple password 'password' to him.

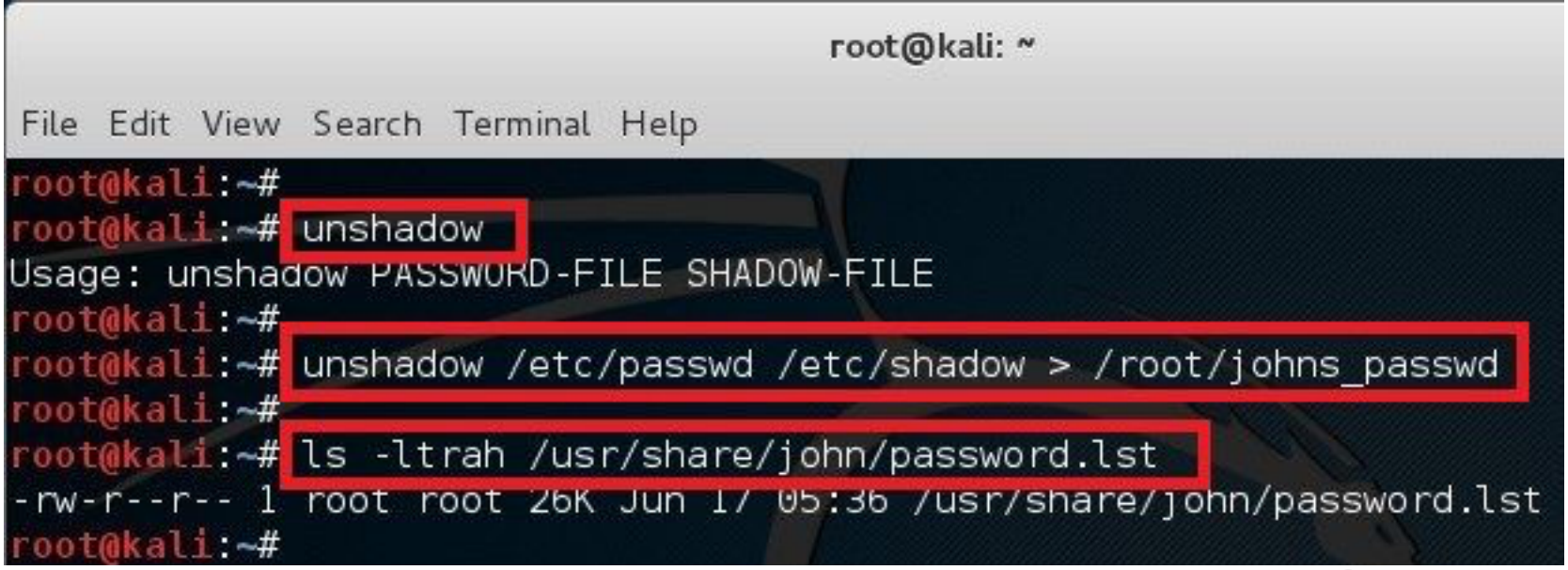
I will also add john to sudo group, assign /bin/bash as his shell. There's a nice article I posted last year which explains user creating in Linux in great details. It's a good read if you are interested to know and understand the flags and this same structure can be used to almost any Linux/Unix/Solaris operating system. Also, when you create a user, you need their home directories created, so yes, go through creating user in Linux post if you have any doubts. Now, that's enough mambo jumbo, let's get to business.

First let's create a user named john and assign password as his password. (very secured..yeah!)

```
root@kali:~# useradd -m john -G sudo -s /bin/bash
root@kali:~# passwd john
Enter new UNIX password: <password>
Retype new UNIX password: <password>
passwd: password updated successfully
root@kali:~#
```

## Unshadowing password

Now that we have created our victim, let's start with unshadow commands.




The unshadow command will combine the extries of /etc/passwd and /etc/shadow to create 1 file with username and password details. When you just type in unshadow, it shows you the usage anyway.

```
root@kali:~# unshadow
Usage: unshadow PASSWORD-FILE SHADOW-FILE
root@kali:~# unshadow /etc/passwd /etc/shadow > /root/johns_passwd
```

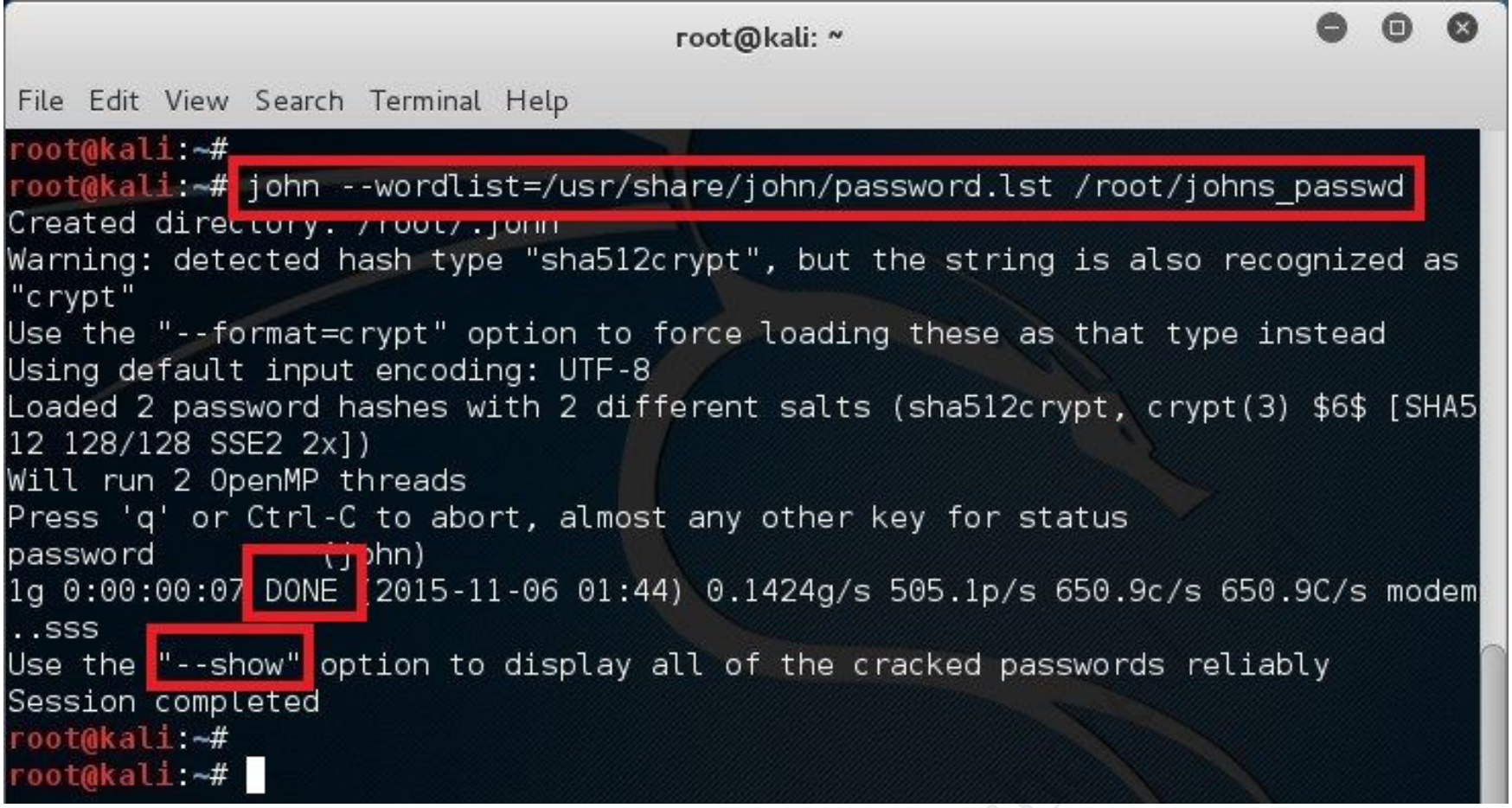
I've redirected the output to /root/johns_passwd file because I got the ticks for organizing things. Do what you feel like here.

## Cracking process with John the Ripper

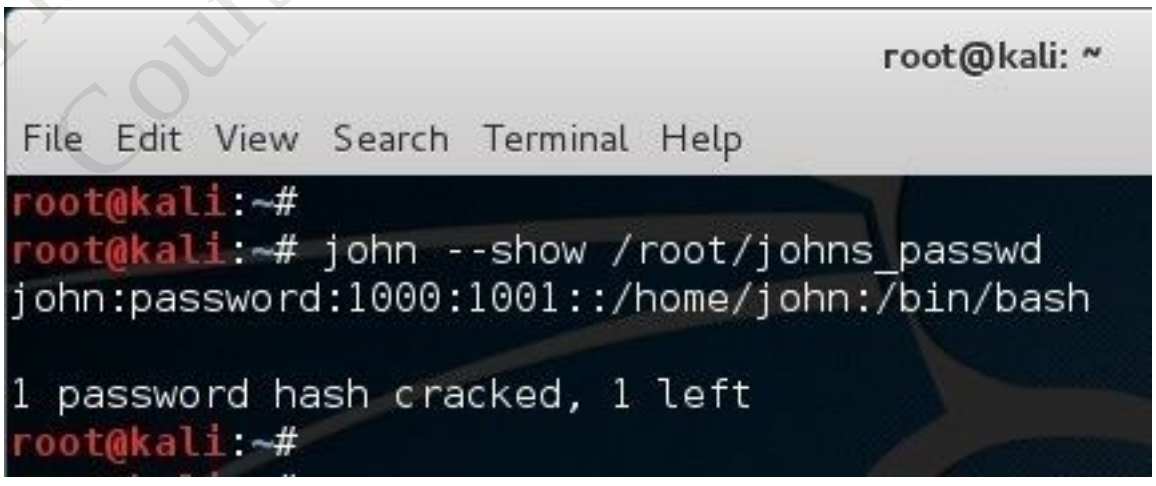
At this point we just need a dictionary file and get on with cracking. John comes with it's own small password file and it can be located in /usr/share/john/password.lst. I've showed the size of that file using the following command.

```
root@kali:~# ls -ltrah /usr/share/john/password.lst
```

You can use your own password lists too or download a large one from Internet (there's lots of dictionary file in terabyte size).




```
root@kali:~# john --wordlist=/usr/share/john/password.lst /root/johns_passwd
Created directory: /root/.john
Warning: detected hash type "sha512crypt", but the string is also recognized a
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SH
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (john)
1g 0:00:00:06 DONE (2015-11-06 13:30) 0.1610g/s 571.0p/s 735.9c/s 735.9C/s moc
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~#
```






Looks like it worked. So we can now use john –show option to list cracked

passwords. Note that it's a simple password that existed in the dictionary so it worked. If it wasn't a simple password, then you would need a much bigger dictionary and lot longer to to crack it.

```
root@kali:~# john --show /root/johns_passwd
john:password:1000:1001::/home/john:/bin/bash

1 password hash cracked, 1 left
root@kali:~#
```

## John the Ripper advanced commands:

Now that we have completed the basics of John the Ripper and cracked a password using it, it's possibly time to move on to bigger and more complex things. For that you should check the documentation on cracking MODES and examples of John the Ripper usage.

## John the Ripper's cracking modes - Click to expand

## John the Ripper - Usage Examples - Click to expand