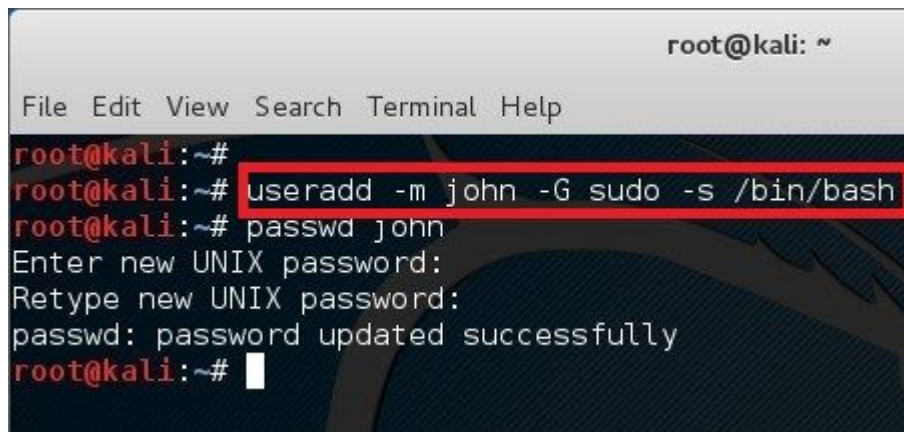


John the Ripper uses a 2 step process to cracking a password. First it will use the passwd and shadow file to create an output file. Next, you then actually use dictionary attack against that file to crack it. In short, John the Ripper will use the following two files:

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

Cracking password using John the Ripper

A terminal window titled 'root@kali: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

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

The command 'useradd -m john -G sudo -s /bin/bash' is highlighted with a red box.

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.

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~#
root@kali:~# unshadow
Usage: unshadow PASSWORD-FILE SHADOW-FILE
root@kali:~#
root@kali:~# unshadow /etc/passwd /etc/shadow > /root/johns_passwd
root@kali:~#
root@kali:~# ls -ltrah /usr/share/john/password.lst
-rw-r--r-- 1 root root 26K Jun 17 05:36 /usr/share/john/password.lst
root@kali:~#
```

The unshadow command will combine the entries 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 its 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: ~
File Edit View Search Terminal Help
root@kali:~#
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 as
"crypto"
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
12 128/128 SSE2 2x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password (john)
lg 0:00:00:07 DONE (2015-11-06 01:44) 0.1424g/s 505.1p/s 650.9c/s 650.9C/s mo
..sss
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~#
root@kali:~#
```

```
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 as "crypto"
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) $6$
[SHA512 128/128 SSE2 2x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password (john)
lg 0:00:00:06 DONE (2015-11-06 13:30) 0.1610g/s 571.0p/s 735.9c/s 735.9C/s
modem..sss
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~#
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~#
root@kali:~# john --show /root/johns_passwd
john:password:1000:1001::/home/john:/bin/bash

1 password hash cracked, 1 left
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:~#
```