# Practical – 11

## Perform brute force attack using John the RIPPER.

**Introduction -**

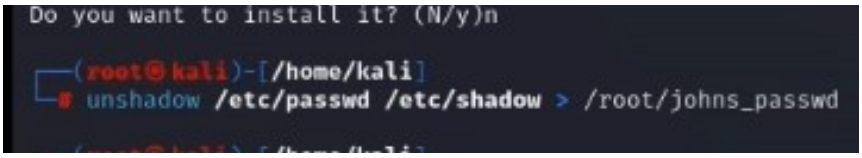
John the Ripper is a free password cracking tool that runs on a large number of different platforms. It is one of the most used password cracking tools because it combines several other password crackers into a single package and has a number of handy features such as automatic hash type detection. Cracking 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 extries of /etc/passwd and /etc/shadow to create

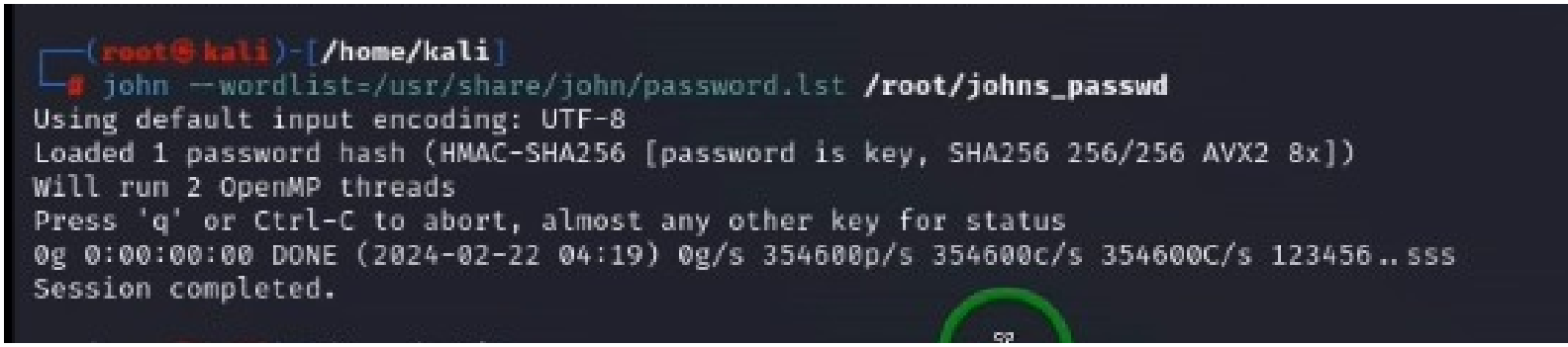
Cmd :- unshadow /etc/passwd /etc/shadow > /root/my_passwd



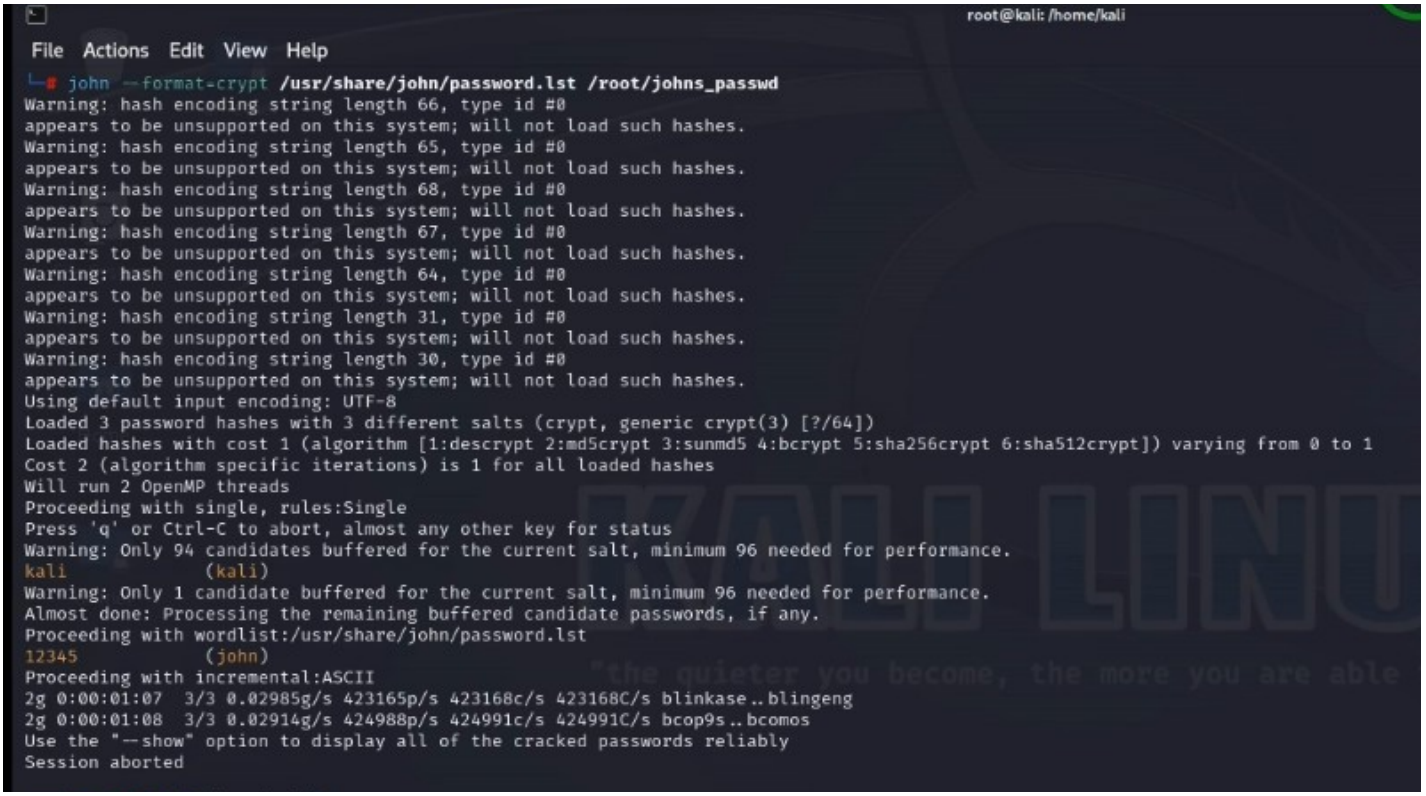

**Cracking process with John the Ripper**

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




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




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