**John The Ripper: Password Cracking Tool**

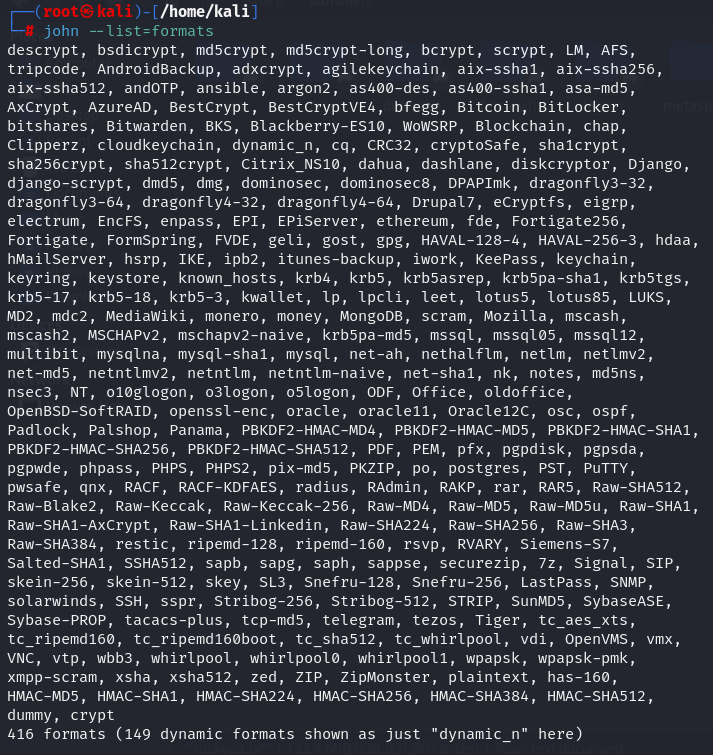
John the Ripper is a free, open-source password cracking tool commonly used for security testing. It's designed to detect weak passwords in Unix-based systems but also supports Windows and other operating systems.

John the Ripper works by using various attack methods, including dictionary attacks, brute force, and hybrid attacks, to guess passwords.

Its flexibility and power make it popular among cybersecurity professionals for testing password strength and ensuring better security practices.

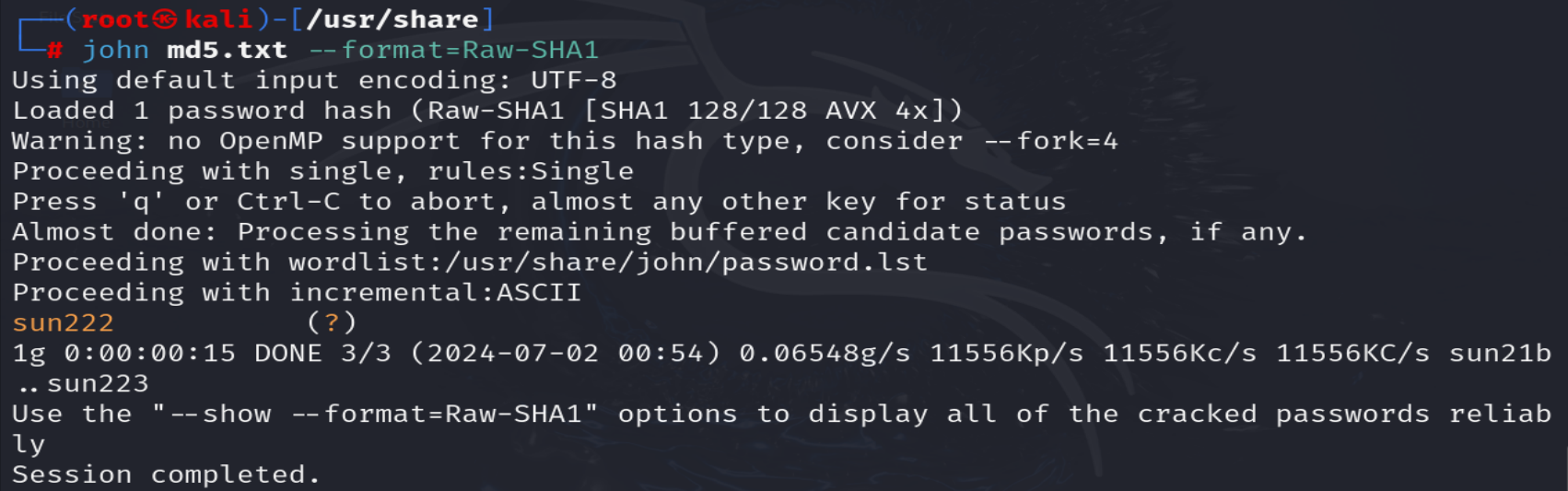
The tool is highly customizable, allowing users to tweak settings and rules to improve its effectiveness in different scenarios.

Formats which john the ripper supports: By using following command.



Basic Syntax:

John (Hash filename) --format=RAW-MD5

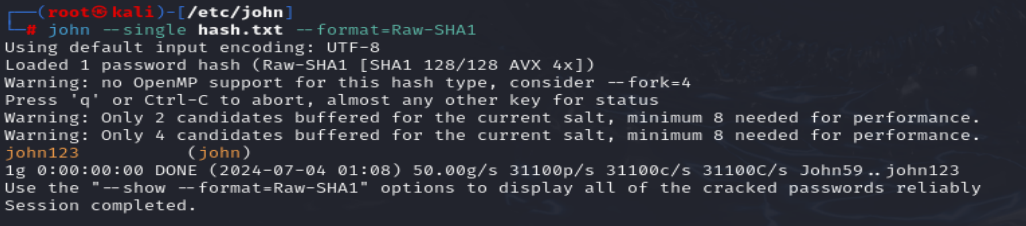


**Single Mode:**

In single-crack mode, John takes a string and generates variations of that string to generate a set of passwords.

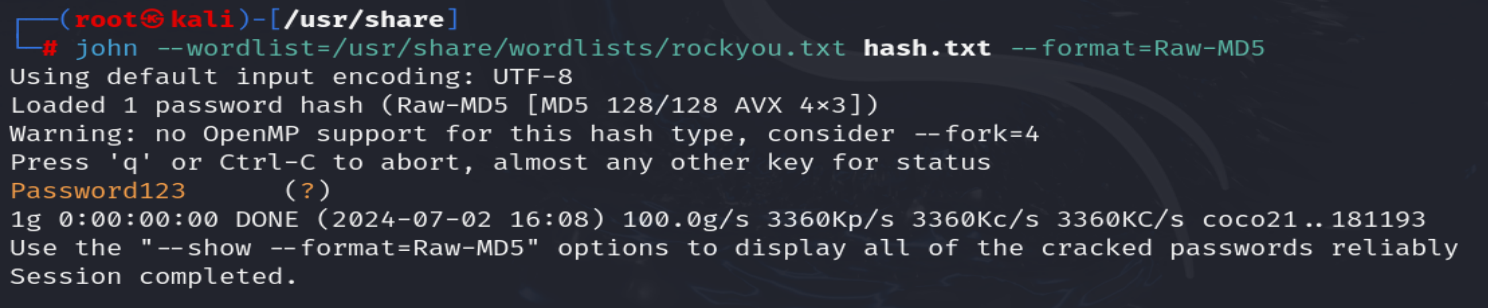
We use the “format” flag to specify the hash type and the “single” flag to let John know we want to use the single crack mode. We will also create a hash.txt file which will contain the username and the hash value of the password.

John –single (hash filename) --format=Raw-SHA1



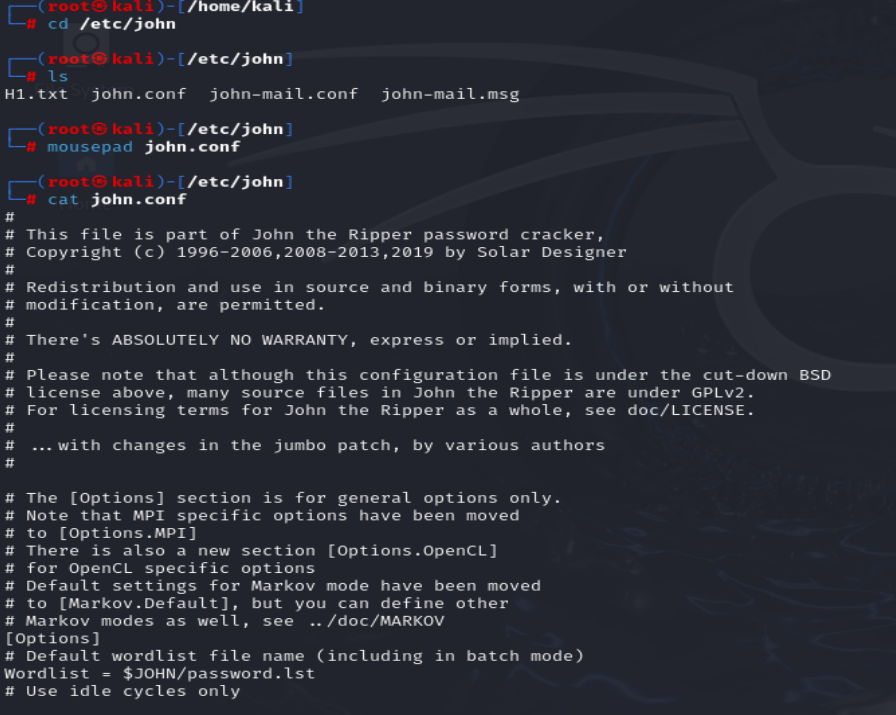
**Wordlist Mode:**

John –wordlist=path of wordlist file (hash filename) --format=Raw-MD5



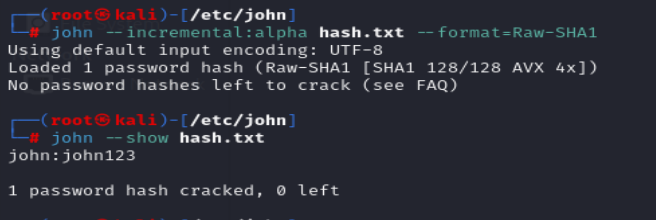
**Rules:**

We can check rules by performing following commands and see them in mousepad by using mousepad john.conf command as show in picture.



**Incremental Mode:**

John –incremental:alpha (hash filename) –format= Raw-SHA1



**Break shadow file:**

In Linux, there are two important files saved in the /etc folder: passwd and shadow.

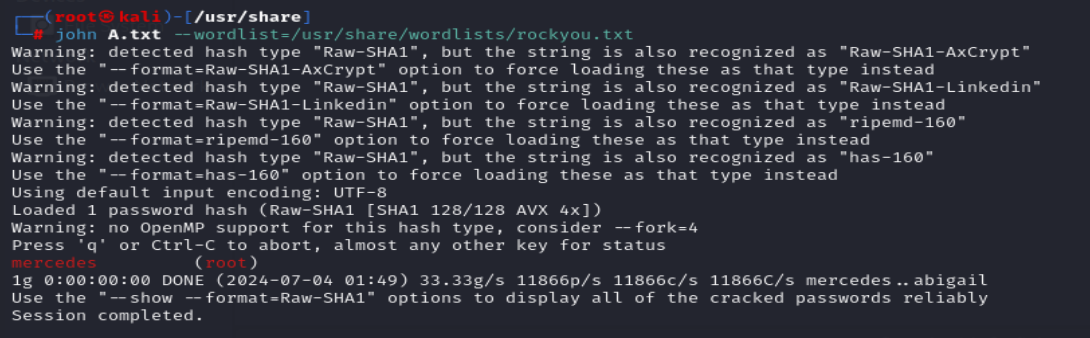
* /etc/passwd -> stores information like username, user id, login shell, and so on.
* /etc/shadow -> contains password hash, password expiry, and so on.

In addition to the “john” command, John comes with a few other utilities. One of them is called “unshadow”.

The unshadow command combines the passwd and shadow files together into a single file. This can then be used by John to crack passwords.

Sudo unshadow /etc/passwd /etc/shadow by this command we unshadow both files and save hash in new .txt file as shown in pictures and perform

john (hash filename) --wordlist=/usr/share/wordlists/rockyou.txt command to crack hash.



**Zip File:**

Here we are creating zip file and encrypting it by password using -e command.

Zip2jhon (filename)> zipHash.txt using this command to store zip hash in zipHash.txt file.

Now we will use john to break password :

John zipHash.txt –wordlist=/usr/share/wordlists/rockyou.txt



As we get the password of the file by using this password we can access file.

**Multiple Files:**  john h1.txt hash.txt – format=Raw-MD5

