**Lab 3 - Cracking Passwords using John the Ripper**

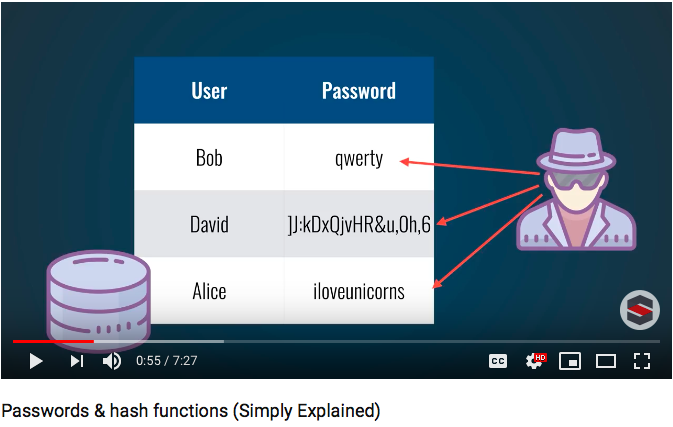
Introduction

**What is John the Ripper?**

John the Ripper is a popular password cracking software tool that was developed by Openwall. It is one of the most popular password testing and breaking programs- it combines a number of password crackers into one program, automatically detects the type of hash encryption of the password, and includes a customizable cracker.

To get a better understanding of password hashing, you can watch this video: <https://www.youtube.com/watch?v=cczlpiiu42M>

**Password & Hash Functions (Simply Explained)-**

[](https://www.youtube.com/watch?v=cczlpiiu42M)

Today, we will be using Kali Linux on our VirtualBox to crack passwords. What we need is a text file, the linux terminal, and a website that generates password hashes.

John the Ripper works in 3 distinct modes to crack passwords:

1. **Single Crack Mode**
2. **Wordlist Crack Mode**
3. **Incremental Mode**

Let’s get started! We will deep-dive into single-crack mode & wordlist crack more

**Setting Up the Environment**

* Open VirtualBox and start your Kali Linux VM.
  + **Username:** root  
    **Password:** toor
* Once you’re at the start page, click on the grid located in the dock on the left side of your screen. Then, select “Text Editor”. This should open a blank text file.

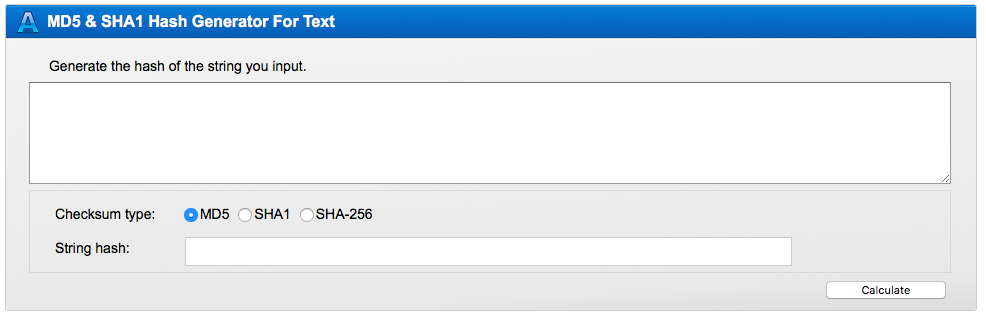


* Click on **File** -> **Save As** -> “**crack.txt**” to your **Desktop**.
* Open terminal and type (case sensitive!):

|  |
| --- |
| root@kali:~# cd \Desktop |

This will take open the Desktop directory in terminal, so that we can access our “crack.txt” file easily. **\*\*Keep your terminal open!\*\***

* On your laptop, keep this website open: <http://onlinemd5.com>. Scroll down to “MD5 and SHA1 Generator for Text”. We will be using this to generate password hashes.



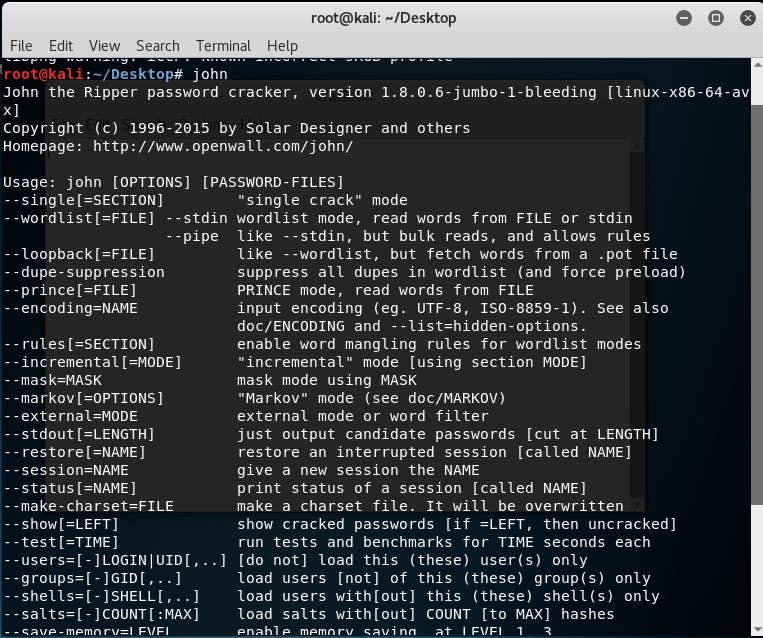
Awesome, your environment is all set!

**Exploring Johnny the Ripper**

* Going back to terminal, type:

|  |
| --- |
| root@kali:~Desktop# john |

**The output (next page):**

HH

* The output shows various options that can be used under John The Ripper. The ones we will be focusing on are:
  + **--single**
    - A single crack mode, which will try to crack the password using information it already knows about the user
  + -**-wordlist**
    - A file that contains a list of common password combinations and is used as a reference by John the Ripper
  + **--format** 
    - Specifies the type of password - if it’s SHA1, MD5, etc.

**Part 1 - Single Crack Mode**

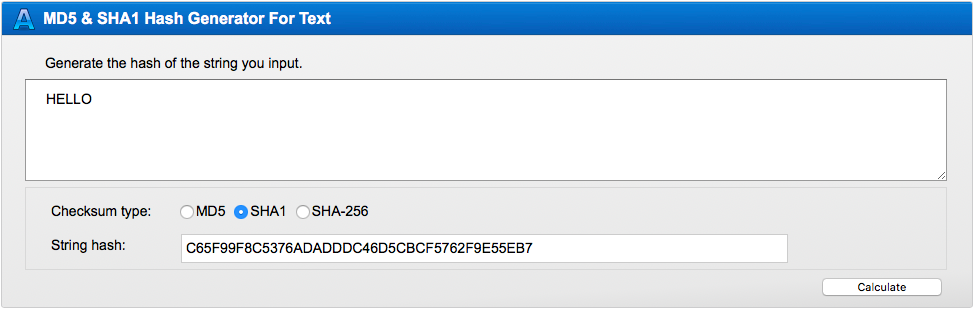
In this mode, John will try to crack the password using information that the hacker already has available, including the username and GECOS.

GECOS includes:

* User’s full name
* Building and room number
* Office telephone number
* Any contact information

For instance, if the username is set as “Hack” and the password is “HaCk”, the single crack mode will detect it.

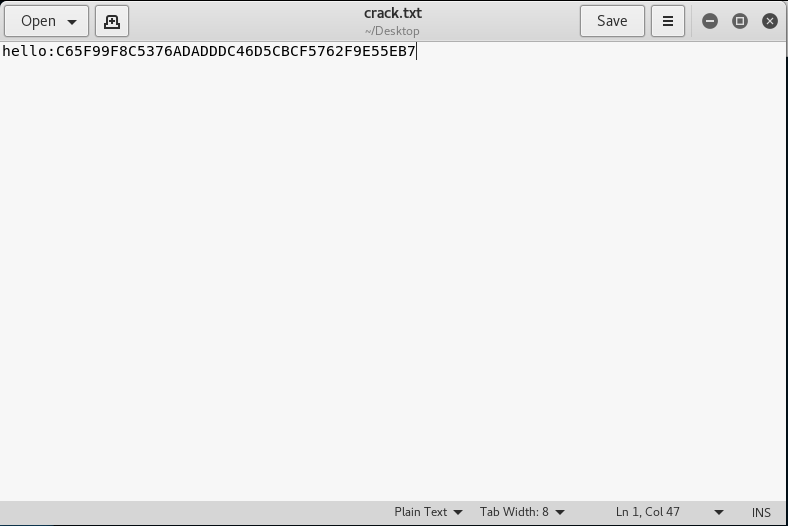
1. Open your “crack.txt” file.
2. For this example, the username is “Hello” and our password is “HELLO”.
3. To encrypt our password to SHA1, go to the website <http://onlinemd5.com>. Scroll down to the Generator for Text, select SHA1 and input “HELLO”



1. The hash output should be:   
     
   **C65F99F8C5376ADADDDC46D5CBCF5762F9E55EB7**
2. On the first line, write:

hello:C65F99F8C5376ADADDDC46D5CBCF5762F9E55EB7

<--**Note: This format is Username:Password-->**

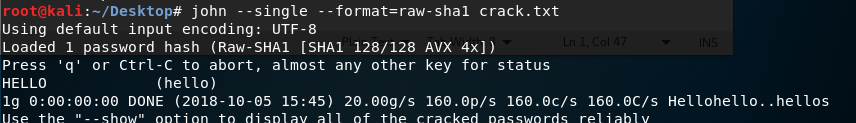


1. Save the file
2. In terminal, type:

|  |
| --- |
| root@kali:~/Desktop# john --single --format=raw-sha1 crack.txt |

Here, we are invoking the single crack mode to crack the password with the format “raw-sha1”, under the file name “crack.txt”.

1. The output should look like this:



**HELLO (hello)**

^ The cracked password

1. **Troubleshooting:** You may not get this output, which means that john was not able to crack the password. To check the status you can type:

root@kali:~Desktop# john --show crack.txt

This will indicate if the password was cracked.



**Part 2 - Wordlist Crack Mode**

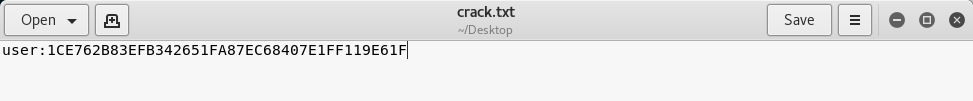
**In this mode, John the Ripper uses a wordlist, also known as a Dictionary, to compare the password hash to the list of words present in the Dictionary. We can use any wordlist of our choice, but John comes built in with several wordlists, including “password.lst”.**

“Password.lst” contains a list of the most common passwords.

Let’s see how John the Ripper cracks passwords in Wordlist Crack Mode:

1. Going back to our text file, we will replace the username with “user” and password with “asdfasdf1”:

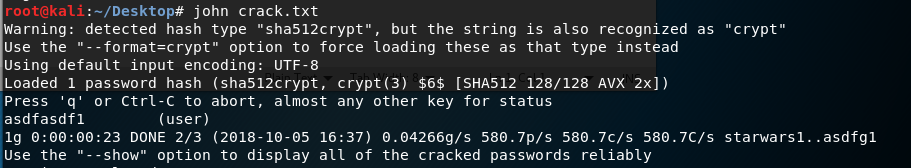
First, we get the sha1 encryption of the password “asdfasdf1”, and the output should look like this:



1. After saving the file, go back to terminal and type:

|  |
| --- |
| root@kali:~/Desktop# John --wordlist=/usr/share/john/password.lst --format=raw-sha1 crack.txt |

The output should contain the cracked password:



**Exercise**

What are some other common passwords that you know? Try testing them out and see if you can get John to crack it!

**Cracking User Credentials**

We are going to demonstrate two ways that we can crack the credentials of a Linux user by using a shadow file.

**What is a shadow file?**

It is a hidden password file in the system that contains encrypted user passwords

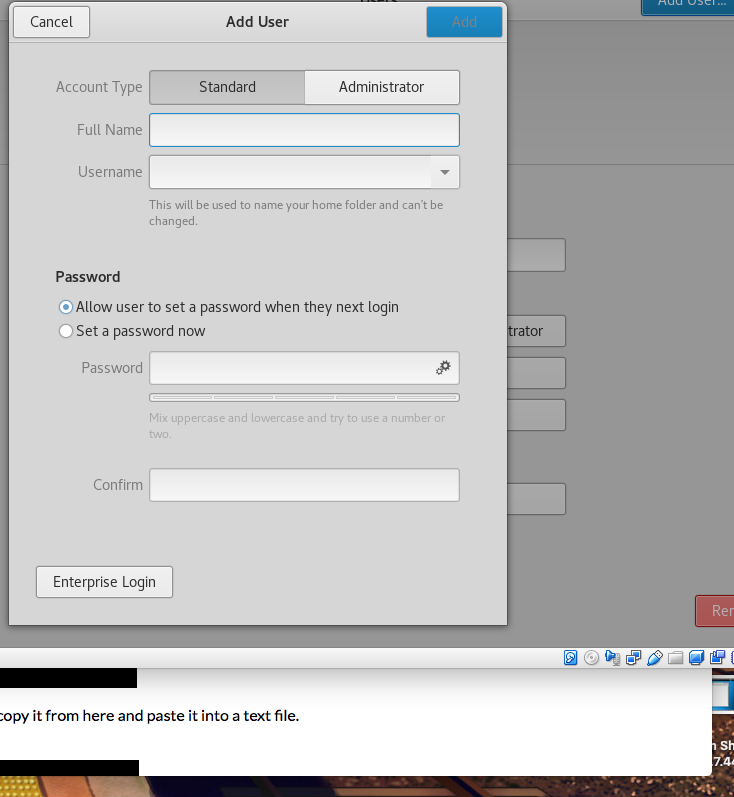
so that they are not available to people who try to break into the system. It is

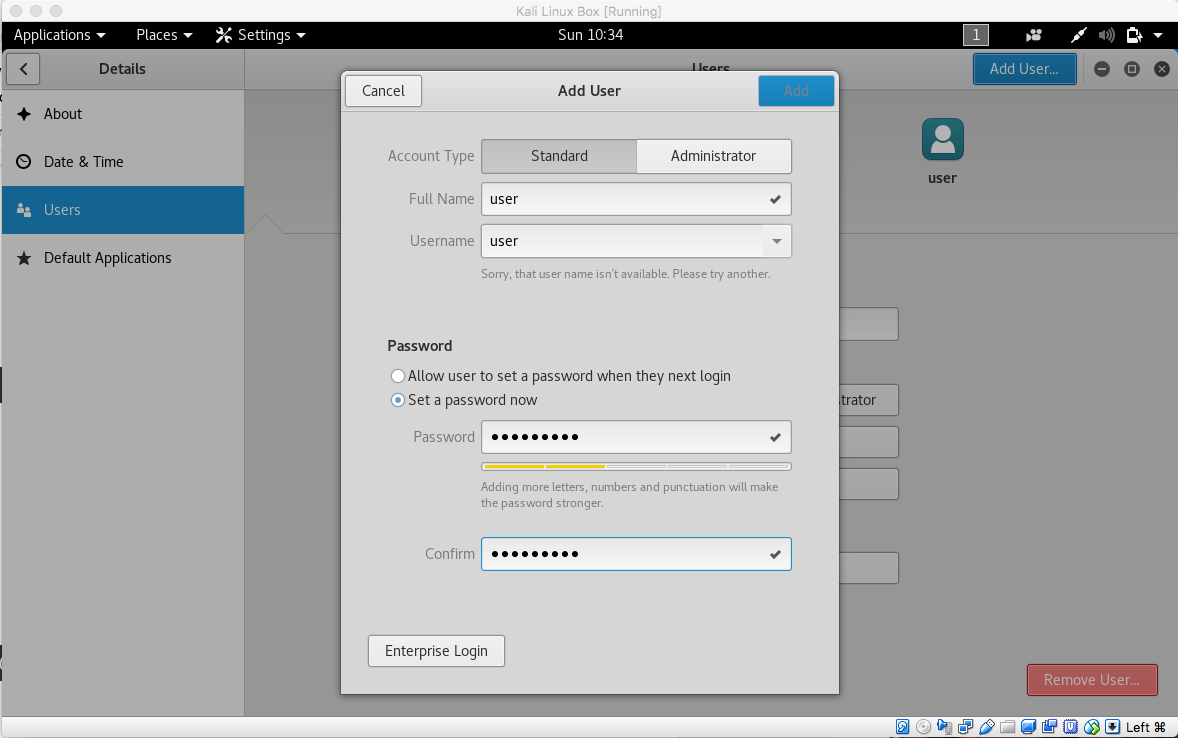
located in the directory /etc/shadow.

* **First Method**We will now crack the credentials of a new user. To create a new user:
  + Click on the grid icon located on the dock in the home screen



* + Click on settings->search->users
  + On the top right corner, select -> add user

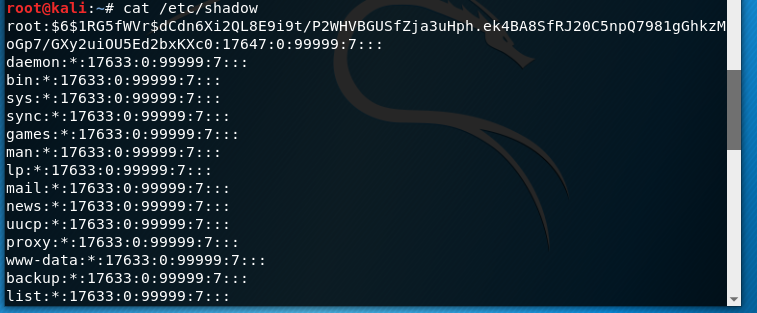


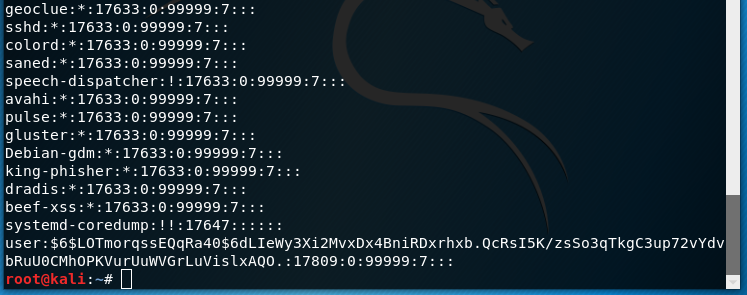
* Follow the format below, and with the password “**asdfasdf1”  
  **

Once a new user has been made, type this in terminal:

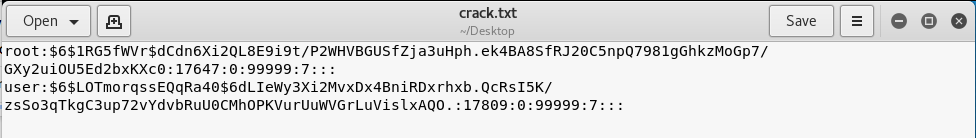
|  |
| --- |
| root@kali:~Desktop# cat /etc/shadow |

This will reveal the data in the shadow file. Within this list, we can see **2 users: the root and the new user that we have created**. Copy and paste their credentials into “crack.txt”:





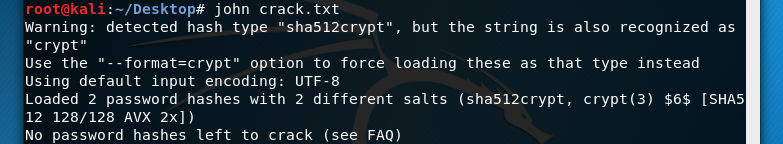
The crack.txt file should look like this:



Once you save the file, go back to terminal and type:

|  |
| --- |
| root@kali:~/Desktop# john crack.txt |

This will take a moment to load, but eventually John will crack the password!

The output:

* **Second Method**For the second method, we will collectively crack the credentials for all users. To do this, we will have to use a John the Ripper utility called “unshadow”

First, close your “crack.txt” file. Then, type the following command in terminal:

|  |
| --- |
| **root@kali:~/Desktop# unshadow /etc/passwd /etc/shadow > crack.txt** |

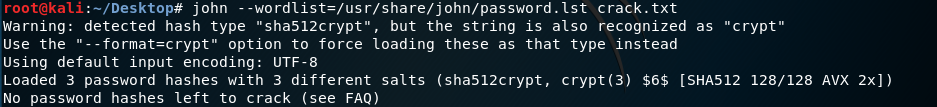
Reopen your “crack.txt” file. It should now be compiled with a list of credentials:



Now we will use John to crack all of the credentials collectively:

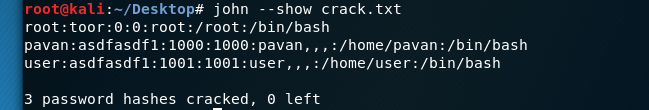
|  |
| --- |
| root@kali:~/Desktop# john --wordlist=/usr/share/john/password.lst crack.txt |

You may get this output:



In order to see the credentials, use “show”:

|  |
| --- |
| root@kali:~/Desktop# john --show crack.txt |



Congrats, you have now successfully cracked user credentials!

**Stopping and Restoring Cracking**

* While John the Ripper is working, enter ‘q’ in terminal to stop execution.
* To restore, type “john --restore”.

**Different formats**

To decrypt different hashes, we will use the option format to change our input type.

We will also use the RockYou wordlist.

*--format=raw-[enter type of encryption]*

* **SHA1**

|  |
| --- |
| john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-sha1 crack.txt |

* **MD5**

|  |
| --- |
| **john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-sha1 crack.txt** |

* **MD4**

|  |
| --- |
| **john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md4 crack.txt** |

* **SHA256**

|  |
| --- |
| **john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-sha256 crack.txt** |

* **RIPEMD128**

|  |
| --- |
| **john --wordlist=/usr/share/wordlists/rockyou.txt --format=ripemd-128 crack.txt** |

* **Whirlpool**

|  |
| --- |
| **john --wordlist=/usr/share/wordlists/rockyou.txt --format=whirlpool crack.txt** |

**Stopping and Restoring Cracking**

To view all formats that John supports, type:

|  |
| --- |
| john --list=formats |

**Abbreviations**

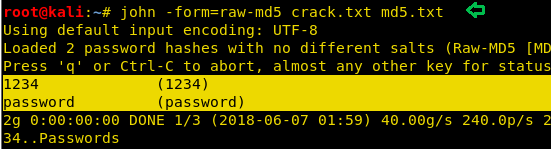
In terminal, we can abbreviate our options and shorten them. A few examples include:

* Single
  + **Original:** --single
  + **Abbreviated:** -si
* Wordlist
  + **Original:** --wordlist
  + **Abbreviated:** -w
* Format
  + **Original:** --format
  + **Abbreviated:** -form

**Cracking Multiple Files at Once**

The syntax to crack multiple files is:

John [file1] [file2]

****

**Congratulations, the lab is complete!**