CYBERTECH AWARENESS PROGRAM

CYBERSECURITY AWARENESS AND EDUCATIONAL OUT-REACH

BURLINGTON, VT

John

Password Cracking

@cybertechvt @cybertechvt cybertechvt.com

Disclaimer/Warning

The Kali Guides provided to you by the Cyber Tech Awareness team are meant for educational purposes ONLY.

The tools covered in the Kali Guides can be used for malicious purposes, but should not be used as such.

The CyberTech Awareness team and the Leahy Center for Digital Forensics and Cybersecurity is NOT responsible any malicious activity conduced with aid from these Kali Guides.

Only use this tool on domains, addresses, files and resources that you have permission to.

Brief Summary

John (the Ripper) is a tool to **brute-force** passwords and **crack password hashes**, or even combine these capabilities to run brute-force attacks that accounts for forms of **encryption**.

Helpful Vocabulary

Encryption:

- The process of making something unreadable without the required information. This is done by using algorithms to change the message by using the key/password to ensure only specific people can understand the message.

Hash:

- Hashes are an encryption method that involves a function that turns data into a unique, fixed-number string output. By design, hashes cannot be reverted back into the original data. There are different hashing algorithms that can be used to create these random strings.

Brute Force Attack:

- A method of guessing login info by running through every single combination within a set of parameters (e.g. a “dictionary attack” would be checking for every word within an established list of common words and phrases)

/etc/shadow:

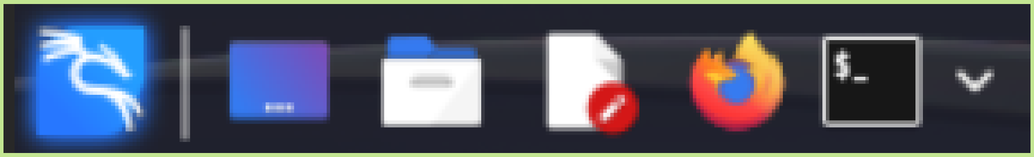
- **T**he file that holds hashed passwords of the users on a system, viewing this file requires certain permissions

/etc/passwd:

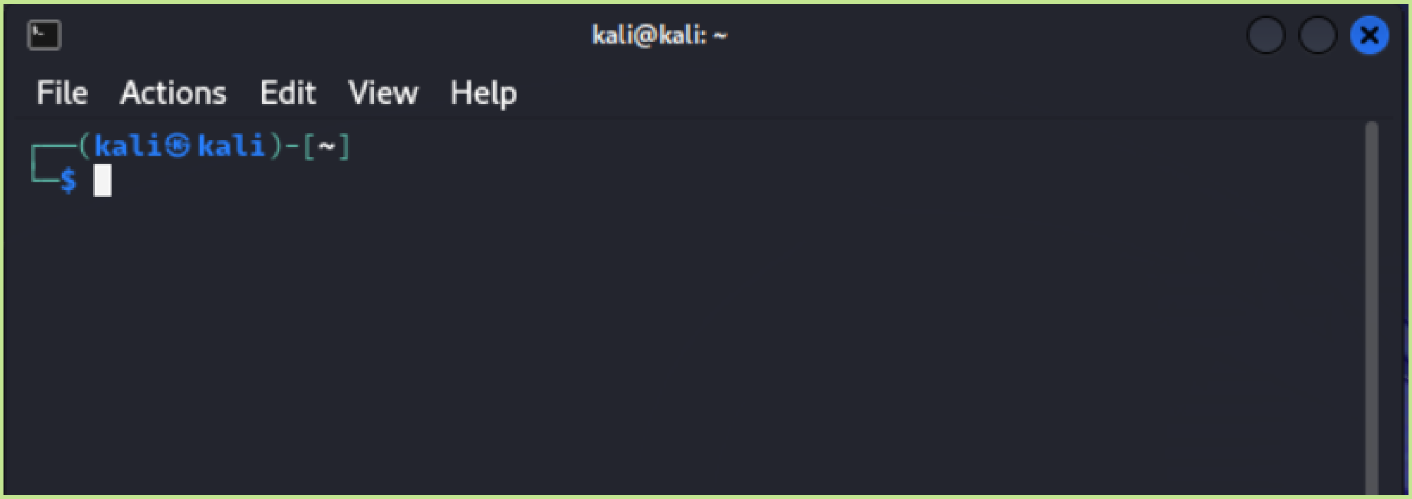
- The file that holds database of users that can login to a system

How to Access John Through the Terminal

In your taskbar, which should be located at the top left of your screen, click on the black box with white text that looks like “$_”.



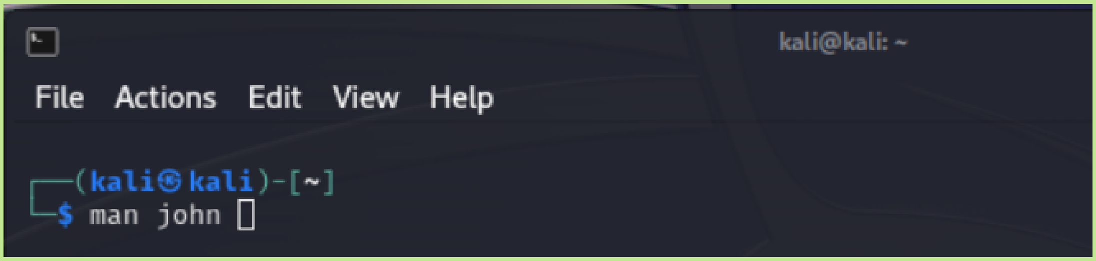
*If the black box isn't there, click on the blue dragon symbol and type “**Terminal Emulator”** into the search bar.*



```
┌──(kali㉿kali)-[~]
└─$ █
```

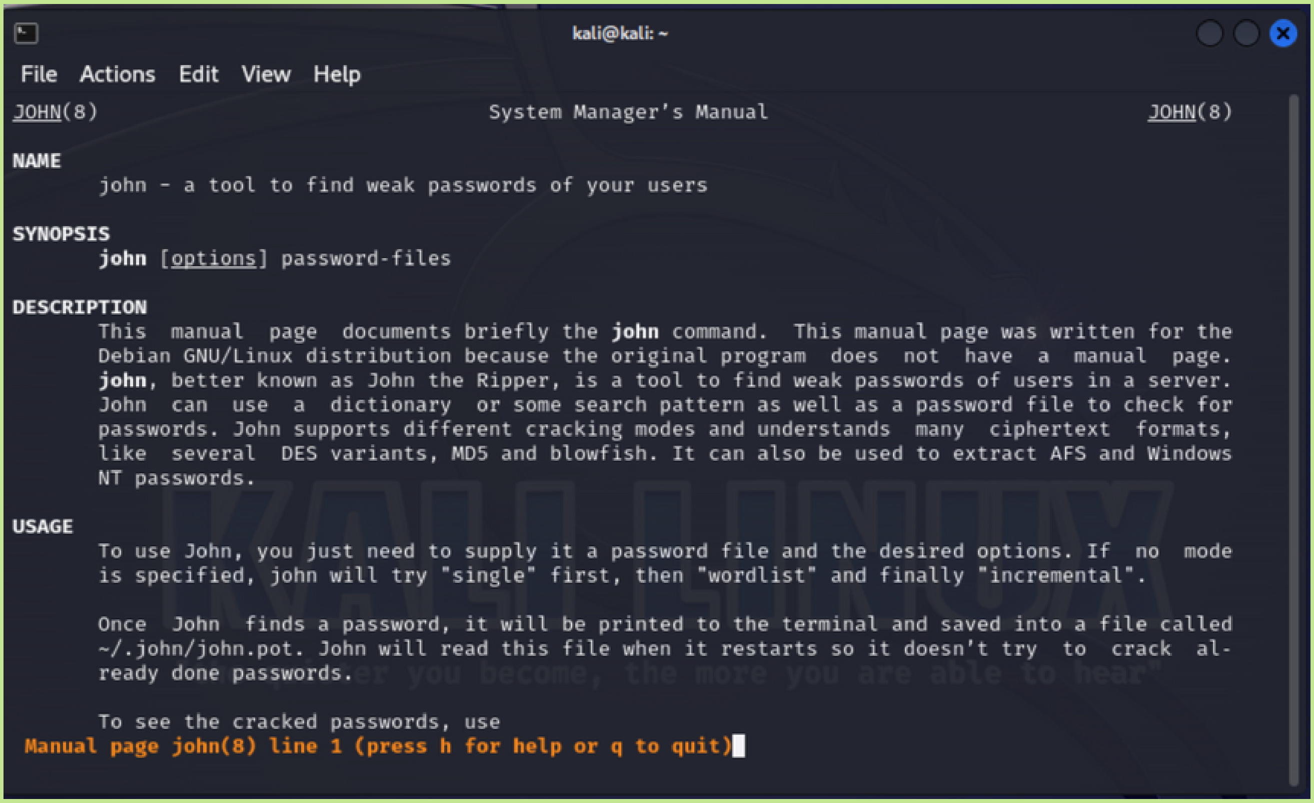
This is what the terminal looks like once it’s opened. The default user is “kali@kali”.

How to Find the Manual for Commands and Tools



```
┌──(kali㉿kali)-[~]
└─$ man john
```

The “man” command displays the manual for the command that can be run in the terminal.

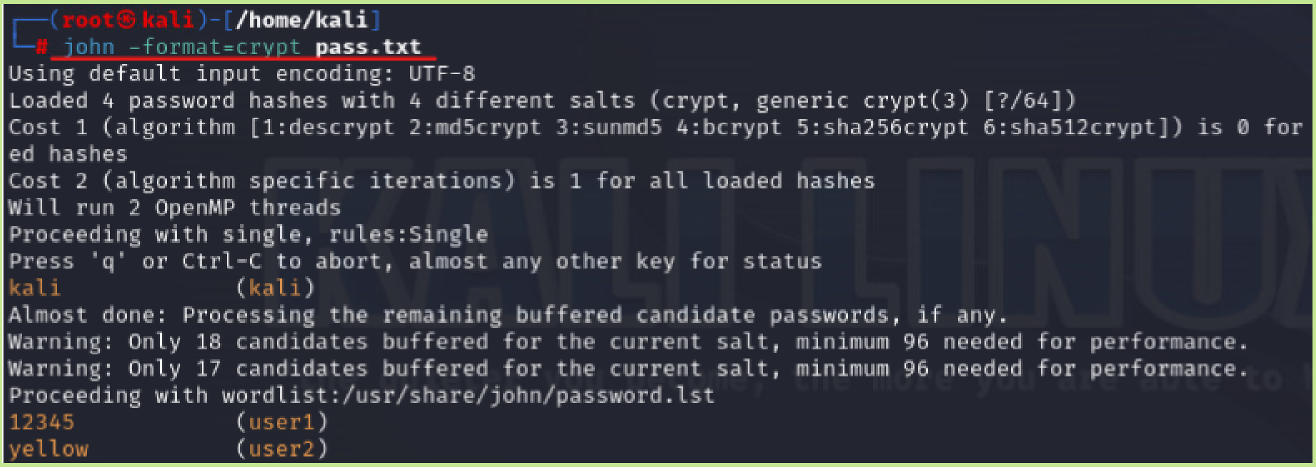


```
JOHN(8)                        System Manager's Manual                       JOHN(8)

NAME
       john - a tool to find weak passwords of your users

SYNOPSIS
       john [options] password-files

DESCRIPTION
       This  manual  page  documents briefly the john command.  This manual page was written for the
       Debian GNU/Linux distribution because the original program  does  not  have  a  manual  page.
       john, better known as John the Ripper, is a tool to find weak passwords of users in a server.
       John  can  use  a  dictionary  or some search pattern as well as a password file to check for
       passwords. John supports different cracking modes and understands  many  ciphertext  formats,
       like  several  DES variants, MD5 and blowfish. It can also be used to extract AFS and Windows
       NT passwords.

USAGE
       To use John, you just need to supply it a password file and the desired options. If  no  mode
       is specified, john will try "single" first, then "wordlist" and finally "incremental".

       Once  John  finds a password, it will be printed to the terminal and saved into a file called
       ~/.john/john.pot. John will read this file when it restarts so it doesn't try  to  crack  al-
       ready done passwords.

       To see the cracked passwords, use
 Manual page john(8) line 1 (press h for help or q to quit)
```

Above is the user manual for the “john” command

Example 1: john format=crypt

*****Running this command on any passwords you are not authorized to is ILLEGAL*****



```
┌──(root㉿kali)-[/home/kali]
└─# john -format=crypt pass.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with 4 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for
ed hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
kali             (kali)
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 18 candidates buffered for the current salt, minimum 96 needed for performance.
Warning: Only 17 candidates buffered for the current salt, minimum 96 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst
12345            (user1)
yellow           (user2)
```

What is this command doing?

This command is using John to **crack password hashes** that are stored in a file called pass.txt. The three hashes that have been cracked are “kali”, “12345”, and “yellow”, as used by users kali, user1, and user2, respectively.

john

- Tells the system that it is using the **john** tool

-format=crypt

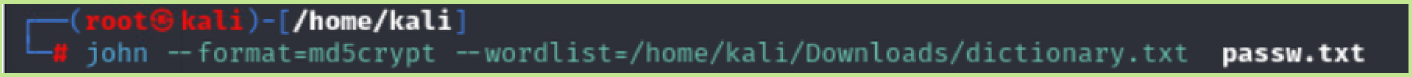
- Tells the john command to crack hashes that are in the “crypt” format which is based on the Data Encryption Standard Algorithm(DES)
    - there are many different types of hashing algorithms, so it’s important that you specific how the passwords have been hashed so John and decrypt them correctly.

pass.txt

- The file that holds the hashes that john in trying to crack

Example 2: john --format=md5crypt --wordlist

*****Running this command on any passwords you are not authorized to is ILLEGAL*****



```
┌──(root㉿kali)-[/home/kali]
└─# john --format=md5crypt --wordlist=/home/kali/Downloads/dictionary.txt  passw.txt
```

What is this command doing?

This command is using John to crack password hashes that are stored in a file called passw.txt using a wordlist in a file called dictionary.txt, and the hash type it is trying to crack is MD5.

john

- Tells the system that it is using the **john** tool

-format=md5crypt

- Tells the john command to crack hashes that are in the "md5crypt" format which is based on the md5 hashing algorithm.
  - there are many different types of hashing algorithms, so it's important that you specific how the passwords have been hashed so John and decrypt them correctly.

–wordlist=/home/kali/Downloads/dictionary.txt

- Sets the wordlist for john to use by including the directory of the file that holds the wordlist.

passw.txt

- The file that holds the hashes that john in trying to crack

Additional Resources:

Kali Linux John Official Webpage:
https://www.kali.org/tools/john/

John the Ripper Password Cracker:
https://www.openwall.com/john/

How to use the John the Ripper password cracker:
https://www.techtarget.com/searchsecurity/tutorial/How-to-use-the-John-the-Ripper-password-cracker

How to use the John the Ripper password cracker:
https://www.techtarget.com/searchsecurity/tutorial/How-to-use-the-John-the-Ripper-password-cracker

How to Crack Passwords using John The Ripper – Pentesting Tutorial:
https://www.freecodecamp.org/news/crack-passwords-using-john-the-ripper-pentesting-tutorial/