**Application Security Project**

**Date** : - 5/10/2022

**Project Description**: - Identifying, cracking techniques and tools for Password attacks & Hashes

* **Authentication:**  Authentication is process to identified someone (generally used user) who is claims to be. Mostly used technique is username and password for verify or authenticate user identity

**Ex:** The website provides login form for username and password

* **There 3 types of authentication:**

1. **Single-Factor authentication**
2. **Two-factor Authentication**
3. **Multi-Factor authentication**

**1. Single-Factor authentication:** – This was the first method of security that was developed. On this authentication system, the user has to enter the username and the password to confirm whether that user is logging in or not. Now if the username or password is wrong, then the user will not be allowed to log in or access the system.

**Advantage: –**

* It is a very simple to use and straightforward system.
* it is not at all costly.
* The user does not need any huge technical skills.

**Disadvantage: –**

* It is not at all password secure. It will depend on the strength of the password entered by the user.
* The protection level in Single-Factor Authentication is much low.

**2. Two-factor Authentication: –** In this authentication system, the user has to give a username, password, and other information. There are various types of authentication systems that are used by the user for securing the system. Some of them are: – wireless tokens and virtual tokens. OTP and more.

**Advantage: –**

* The Two-Factor Authentication System provides better security than the Single-factor Authentication system.
* The productivity and flexibility increase in the two-factor authentication system.
* Two-Factor Authentication prevents the loss of trust.

**Disadvantage: –**

* It is time-consuming.

**3.Multi-Factor authentication : –** In this type of authentication, more than one factor of authentication is needed. This gives better security to the user. Any type of keylogger or phishing attack will not be possible in a Multi-Factor Authentication system. This assures the user, that the information will not get stolen from them.

**Advantage: –**

* No risk of security.
* No information could get stolen.
* No risk of any key-logger activity.
* No risk of any data getting captured.

**Disadvantage: –**

* It is time-consuming.
* it can rely on third parties. The main objective of authentication is to allow authorized users to access the computer and to deny access to unauthorized users. Operating Systems generally identify/authenticates users using the following 3 ways: Passwords, Physical identification, and Biometrics. These are explained as following below.
* Passwords: Password verification is the most popular and commonly used authentication technique. A password is a secret text that is supposed to be known only to a user. In a password-based system, each user is assigned a valid username and password by the system administrator.
* The system stores all usernames and Passwords. When a user logs in, their user name and password are verified by comparing them with the stored login name and password. If the contents are the same then the user is allowed to access the system otherwise it is rejected.Physical Identification: This technique includes machine-readable badges(symbols), cards, or smart cards. In some companies, badges are required for employees to gain access to the organization’s gate.
* Biometrics: This method of authentication is based on the unique biological characteristics of each user such as fingerprints, voice or face recognition, signatures, and eyes.
* A scanner or other devices to gather the necessary data about the user
* Software to convert the data into a form that can be compared and stored.
* A database that stores information for all authorized users.
* **Password Attacks**
* **Types Of Password attacks**
* Simple Brute Force Attack
* Dictionary Attack
* Hybrid Brute Force Attack
* Reverse Brute Force Attack
* Credential Stuffing
* Rule-based attack
* Rainbow table attack
* **Simple Brute Force Attack :**

A simple brute force attack uses automation and scripts to guess passwords. Typical brute force attacks make a few hundred guesses every second. Simple passwords, such as those lacking a mix of upper- and lowercase letters and those using common expressions like '123456' or 'password,' can be cracked in minutes

* **Dictionary Attack :**

A Dictionary Attack is an attack vector used by the attacker to break in a system, which is password protected, by putting technically every word in a dictionary as a form of password for that system. This attack vector is a form of Brute Force Attack.

The dictionary can contain words from an English dictionary and also some leaked list of commonly used passwords and when combined with common character replacing with numbers, can sometimes be very effective and fast.

* **Hybrid Brute Force Attack :**

A hybrid brute force attack combines a dictionary attack and a brute force attack

* **Reverse Brute Force Attack :**

A reverse brute-force attack is a type of brute-force attack in which an attacker uses a common password against multiple usernames in an attempt to gain access to a network. This term can also be written as reverse brute force attack, without the hyphen.

* **Credential Stuffing**

Credential stuffing is a cyberattack method in which attackers use lists of compromised user credentials to breach into a system. The attack uses bots for automation and scale and is based on the assumption that many users reuse usernames and passwords across multiple services.

* **Rule-based attack**

A rule-based password attack is a way of focusing a password cracking technique when an attacker knows which rules passwords in a particular system are based on, such as “alphanumeric and eight characters long.”

* **Rainbow table attack**

A rainbow table attack is a password cracking method that uses a special table (a “rainbow table”) to crack the password hashes in a database

* **Demonstration :**
* **There are some tools which is widely used for password attacks and its listed below**
* **Crunch**
* **Hydra**
* **john the ripper**
* **hashcat**
* **Rainbow cracker**
* **Crunch**

**Description:**

Crunch is a wordlist generator where you can specify a standard character set or any set of characters to be used in generating the wordlists.

**Installation:**

Crunch is available by default in kali linux.

Command line code : sudo apt install crunch

Git clone: <https://github.com/jim3ma/crunch.git>

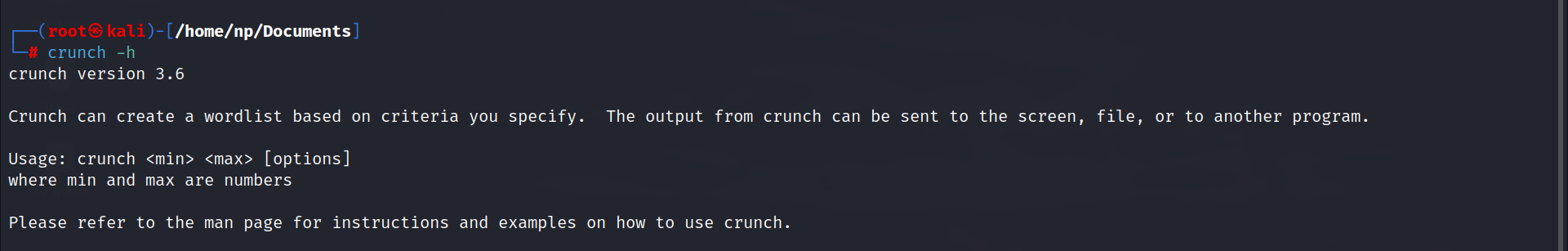
**Usage :**

Syntax:

# crunch <min> <max> [options]

Help:

# crunch -h



Creating wordlists

There are many options and way to create different types of wordlists according to the need.

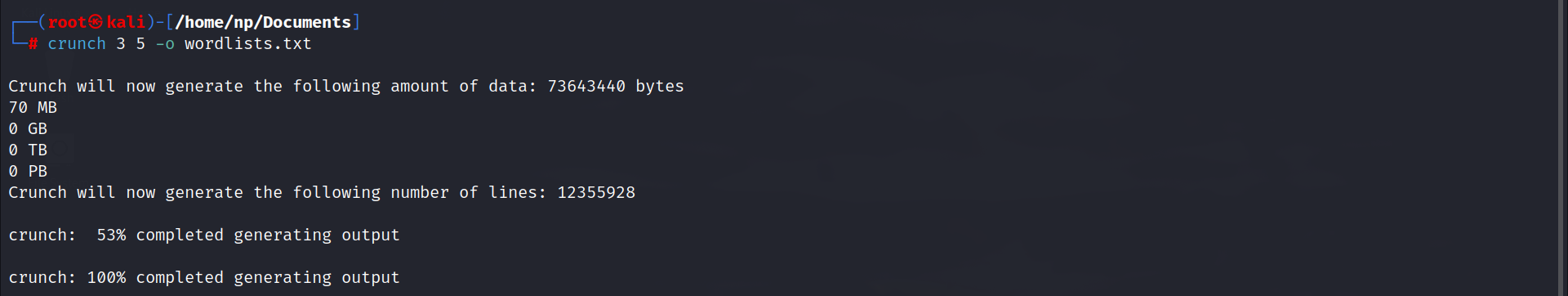
We can find the options in manual page of crunch.

# crunch 3 5 -o wordlists.txt

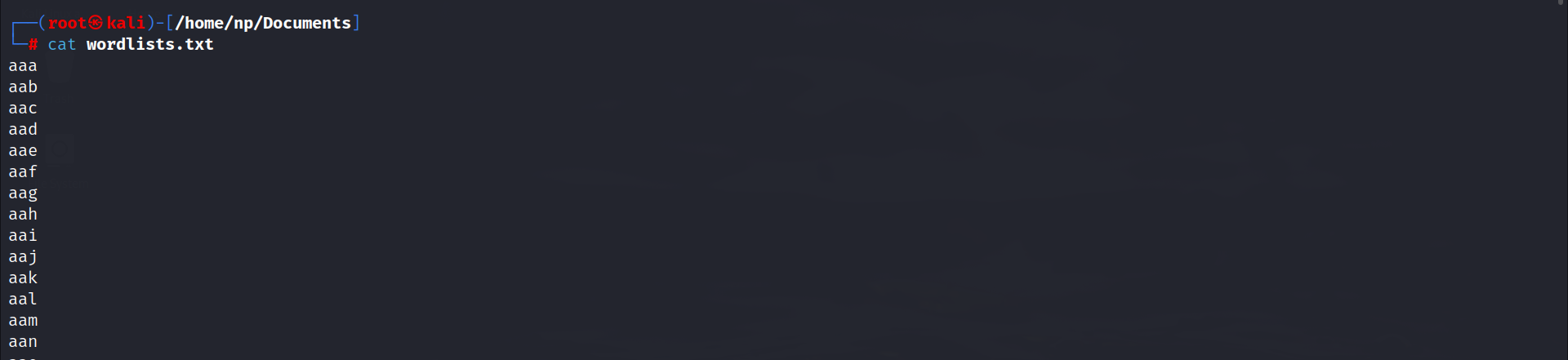
3=minimum length

5=maximum length

o=for saving file



Result:



Here are some more examples:

* For specific characters

#crunch 3 5 abcd123 -o wordlists.txt

* For inverting

# crunch 3 5 abcd123 -i -o wordlists.txt

* wordlists start with specific string

# crunch 3 5 -s passwd -o wordlists.txt

* **Hydra**

**Description:**

Hydra is a parallelized login cracker which supports numerous protocols to attack. It is very fast and flexible, and new modules are easy to add. This tool makes it possible for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely

**Installation:**

Hydra is available by default in kali linux.

Command line code : sudo apt install hydra

Git clone: <https://github.com/vanhauser-thc/thc-hydra.git>

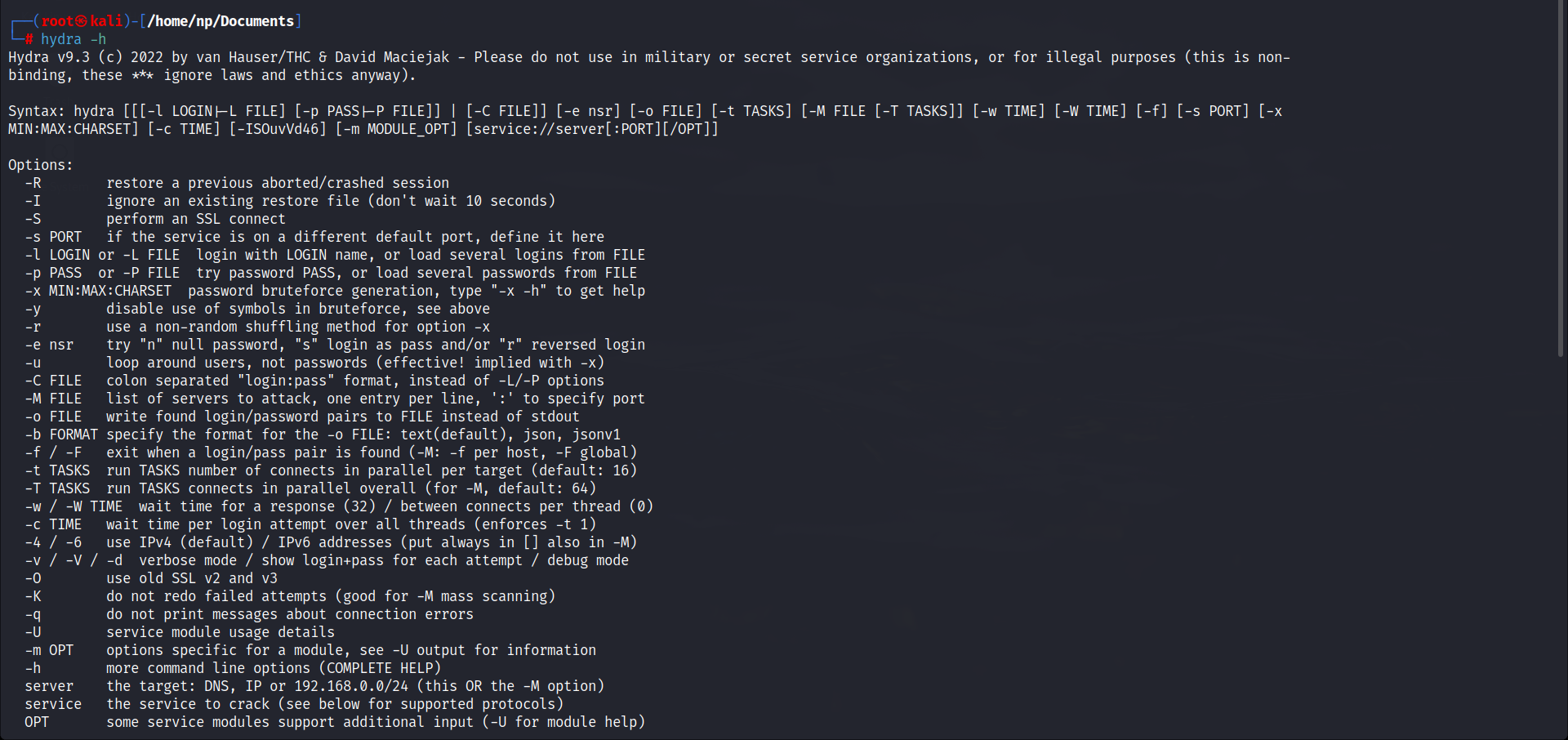
**Usage :**

Syntax:

# hydra [options]

Help:

# hydra -h



Hydra is brute forcing tool which is provide many options and many services for attack like ssh,ftp etc..

In this example we are going to brute force password.

# hydra -L <wordlists> -P <wordlist> MACHINE\_IP http-post-form "<login page url>/:username=^USER^&password=^PASS^:F=incorrect" -V

#hydra -L username.txt -P password.txt 10.10.202.75 http-post-form "/login/:username=^USER^&password=^PASS^:F=incorrect" -V



Result

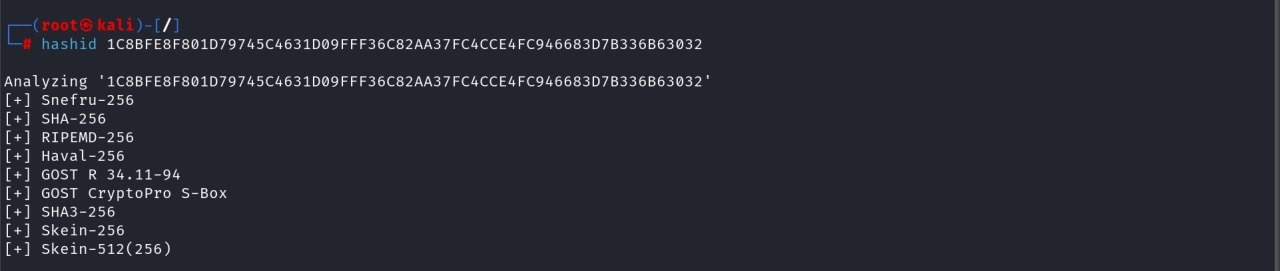
Username=molly & password = sunshine



**HASH identifier**

The tools **hashid** & **hash-identifier** are used For identifying the hashes.

**Hashid**

****

**hash-identifier**

****

* **John the ripper**

**Description:**

John the Ripper is an Open Source password security auditing and password recovery tool available for many operating systems, that combines several different cracking programs and runs in both brute force and dictionary attack modes and supports hundreds type of hash and cipher.

**Installation:**

John the Ripper is available by default in kali linux.

Git clone : <https://github.com/openwall/john.git>

Window/Others : <https://www.openwall.com/john/>

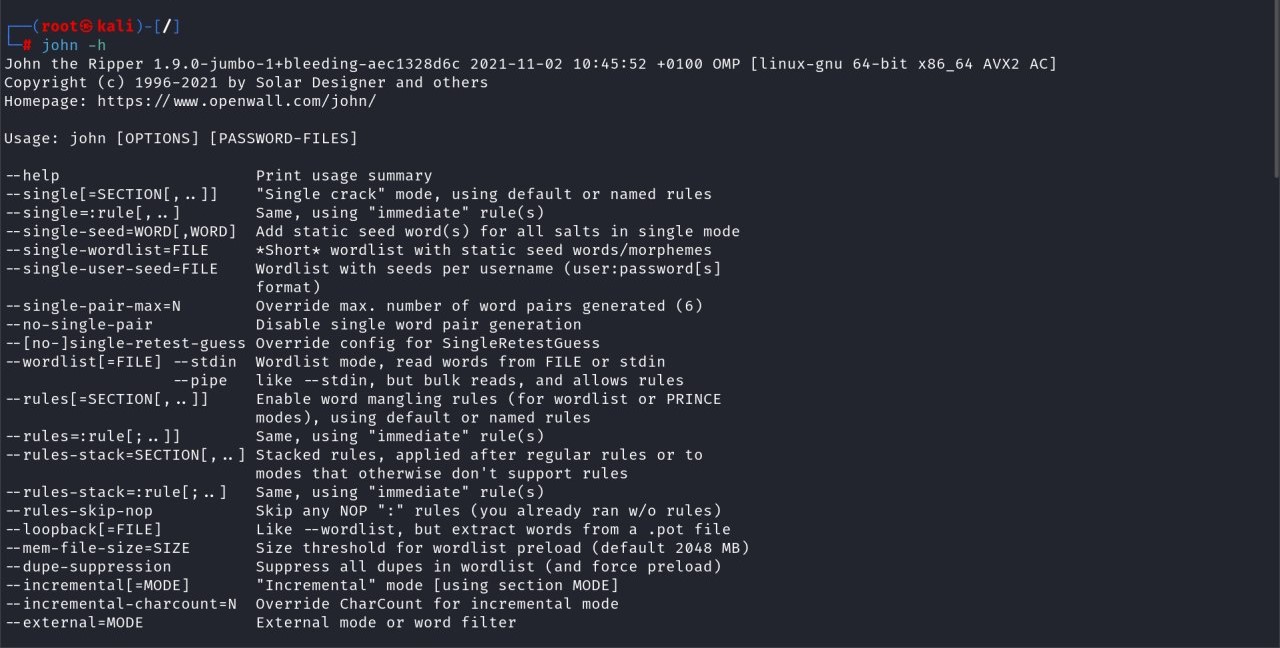
**Usage :**

Syntax:

# john [options] [password files]

Help:

# john -h

****

John the ripper provides many options with many services such as ftp,ssh etc..

It’s also supports many hashes algorithms

In this the SHA256 encrypted hash is performed

**Hash:**

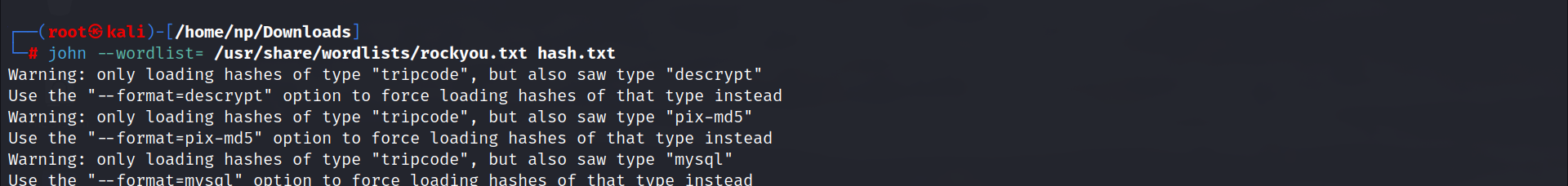
1C8BFE8F801D79745C4631D09FFF36C82AA37FC4CCE4FC946683D7B336B63032

**Hash type** :SHA256

->Store the hash in file and name hash.txt(anything)

john –wordlist <wordlist path> <file name>

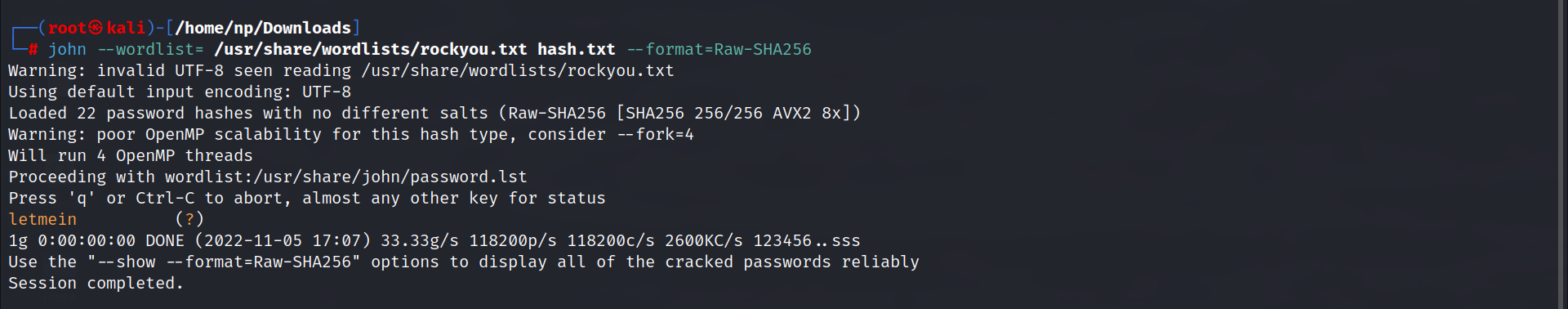
#john –wordlist= /usr/share/wordlists/rockyou.txt hash.txt



Result

Because of this hash is following SHA256 algorithem ww put it Raw-SHA256 in format option

The password is: letmein



* **Hashcat**

**Description:**

Hashcat is the world's fastest and most advanced password recovery utility, used for licit and illicit purposes. Hashat is a particularly fast, efficient, and versatile hacking tool that assists brute-force attacks by conducting them with hash values of passwords that the tool is guessing or applying.

World's first and only in-kernel rule engine.

Supporting five unique modes of attack for over 300 highly-optimized hashing.

**Installation:**

Hashcat is available by default in kali linux.

Git clone: <https://github.com/hashcat/hashcat.git>

Window/Others : <https://hashcat.net/hashcat/>

**Usage :**

Syntax:

# hashcat [options] hash ,hash file, [dictionary]

Help:

# hashcat -h

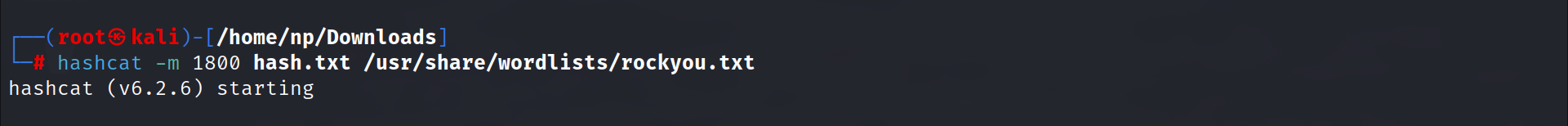
****

**Hash:**

$6$aReallyHardSalt$6WKUTqzq.UQQmrm0p/T7MPpMbGNnzXPMAXi4bJMl9be.cfi3/qxIf.hsGpS41BqMhSrHVXgMpdjS6xeKZAs02.

**Hash type** :SHA12

# hashcat -m 1800 hash.txt /usr/share/wordlists/rockyou.txt



-m 0 designates the type of hash we are cracking (MD5)

-a 0 designates a dictionary attack

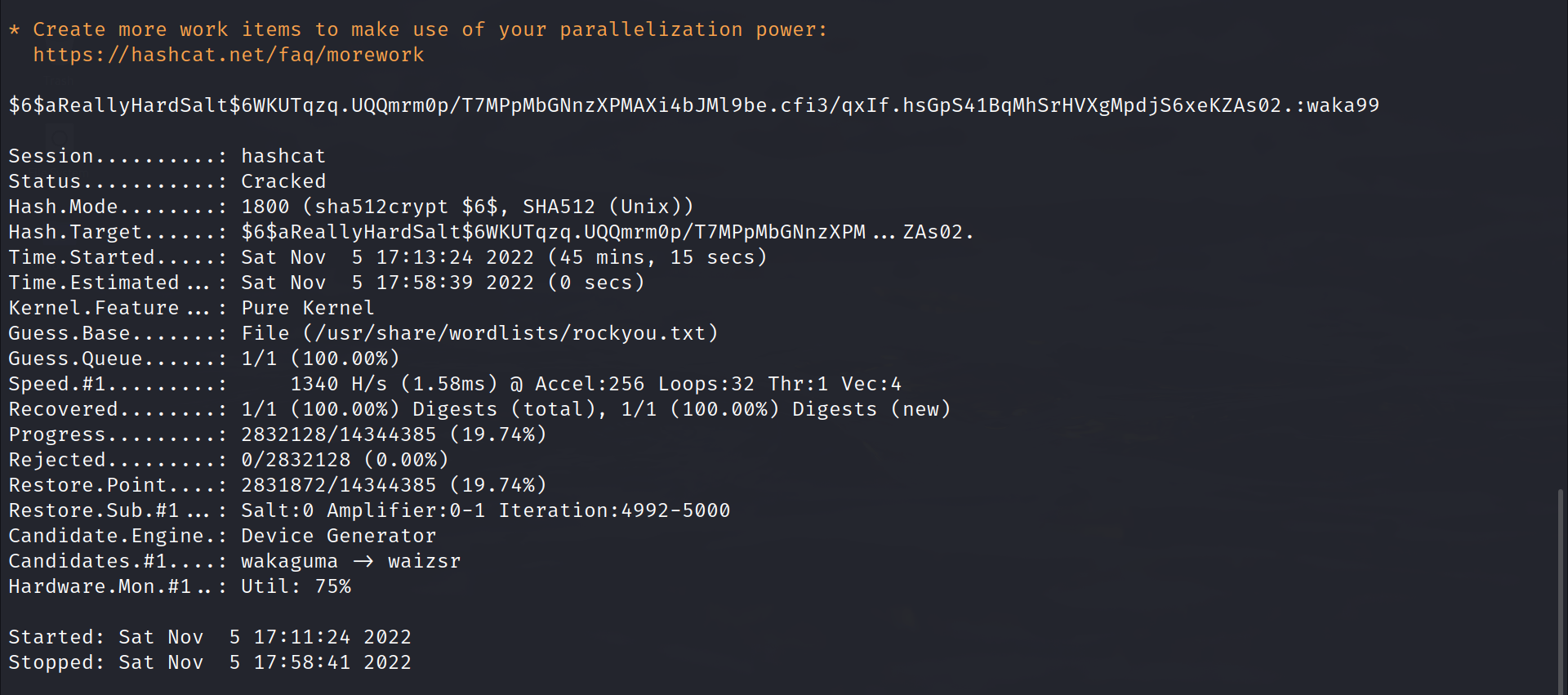
-o <name of file>is the output file for the cracked passwords

hashe.txt is our input file of hashes

/usr/share/wordlists/rockyou.txt is the absolute path to the wordlist file for this dictionary attack

Result

password:= waka99



* **Rainbow cracker**

**Description:**

RainbowCrack is a general propose implementation of Philippe Oechslin's faster time-memory trade-off technique. It crack hashes with rainbow tables. RainbowCrack uses time-memory tradeoff algorithm to crack hashes. It differs from the hash crackers that use brute force algorithm.

**Installation:**

Rainbow cracker is available by default in kali linux.

Git clone: <https://gitlab.com/kalilinux/packages/rainbowcrack.git>

**Usage :**

Syntax:

#rtgen md5 lowercase(character set) 1 <minimum length> 3 <maximum length> 0 <table index> 1000<chain length> 1000 <chain number> 0 <part index>

#rtgen md5 lowercase-numeric 1 3 0 1000 1000 0

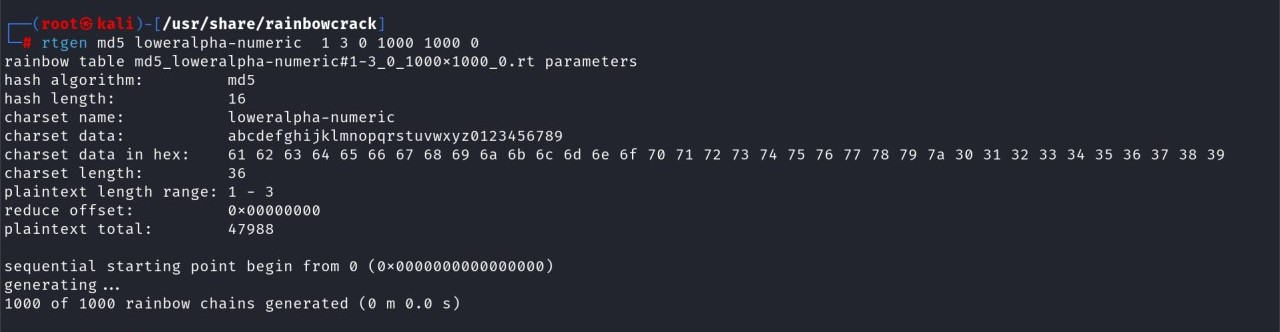
Help:

#rtgen -h

****

Creating rainbow table of md5

# rtgen md5 lowercase-numeric 1 3 0 1000 1000 0



You can find this table in **/usr/share/rainbowcrack/** directory

Now short the table

#rtsort <table name>

#rtsort .



Creating 3 number hash of md5

#echo -n "etc" | md5sum

****

The “etc” is now md5 encrypted

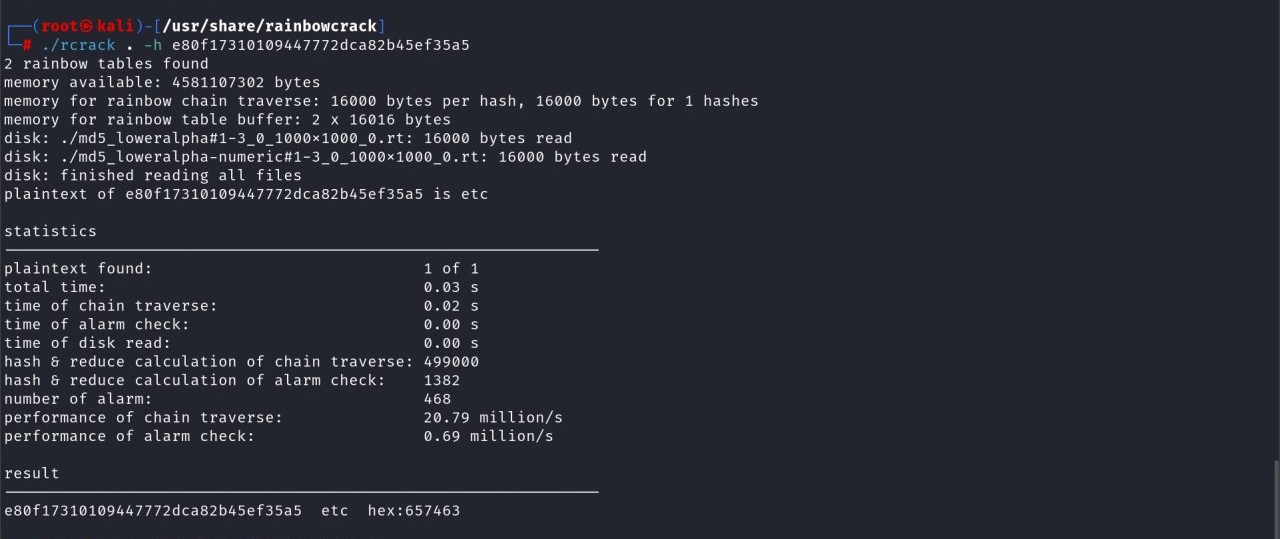
created hash : e80f17310109447772dca82b45ef35a5

Result

Cracking the hashes

#rcrack <table name> -h <hashes> hase

#./rcrack . -h e80f17310109447772dca82b45ef35a5



We get the etc in normal from after cracking the hash

* **Data Breach**

There are many reasons of data breach but authentication failure Is common .there are some issue that raise a attack like password attacks, mis-configuration, authentication bypass.

Because of this security loophole’s an attacker is able to successfully execute a cyber attack

A attacker use’s this details and credential for more impact and also for ransomware attack .

If a data breach is happen with any company then its big loss for company in all terms like reputation, financial, customer relationships etc…

There are some world biggest company’s who had faced some cyber attack and data breach and they lost millions of dollars .

Here is the one popular data breach in the history .

**The biggest attack in history Yahoo cyber attack**

[**https://www.yahoo.com/now/worst-cyber-attacks-past-10-202226243.html?guccounter=1&guce\_referrer=aHR0cHM6Ly9kdWNrZHVja2dvLmNvbS8&guce\_referrer\_sig=AQAAAHxl3gD6DU7AvMBEkUiU4fuvFkBB7cwT3nmt9IfwOjUCbOu1aM\_RQ2-S80fACTGXkm2kAhjooEsmAvNUhjGWWAfdlo\_ZIyeirKpYhABzXQuLYGKlAIQEkyOle8w\_tHuGVHUfhAd8zauceYrhHRfeEf5VjlgwtYrClfJUCnnbkPv3**](https://www.yahoo.com/now/worst-cyber-attacks-past-10-202226243.html?guccounter=1&guce_referrer=aHR0cHM6Ly9kdWNrZHVja2dvLmNvbS8&guce_referrer_sig=AQAAAHxl3gD6DU7AvMBEkUiU4fuvFkBB7cwT3nmt9IfwOjUCbOu1aM_RQ2-S80fACTGXkm2kAhjooEsmAvNUhjGWWAfdlo_ZIyeirKpYhABzXQuLYGKlAIQEkyOle8w_tHuGVHUfhAd8zauceYrhHRfeEf5VjlgwtYrClfJUCnnbkPv3)