

PRACTICAL-7

AIM:-

System hacking is the way hackers get access into individual's computer on a network. Ethical hackers learn system hacking to detect, prevent, and counter these types of attacks. Study practical approach to implement system hacking and learn different ways to crack password.

- 1) OPHCRACK
- 2) John The Ripper

Theory:

System hacking is defined as the compromise between computer systems and software to access the target computer and steal or misuse their sensitive information. The malware and the attacker identify and exploit the vulnerability of the computer system to gain unauthorized access.

Ophcrack is an extremely fast password cracker because it uses a special algorithm called rainbow tables. Brute-force cracking tools typically try thousands of combinations of letters, numbers and special characters each second, but cracking a password by attempting every conceivable combination can take hours or days. Rainbow tables pre-computes the hashes used by passwords, allowing for a speedy password lookup by comparing the hashes it has, instead of computing them from scratch.

John the Ripper is password cracking software used by penetration testers and cyber security experts. It is completely free. In starting it was only made for Unix operating system but now it can be used on several other platforms also like windows, mac, etc. It was first released in 1996 by OpenWall. Its latest version is 1.9.0 which was released in 2019. It has the ability to crack passwords and also it automatically detects the hash type if passwords are saved in a hash rather than plain text, it combines a number of strategies to crack passwords. It is mainly used to perform dictionary attacks and brute force attacks on any system or application.

John also offers a brute force mode. In this type of attack, the program goes through all the possible plaintexts, hashing each one and then comparing it to the input hash. John uses character frequency tables to try plaintexts containing more frequently used characters first. This method is useful for cracking passwords that do not appear in dictionary wordlists, but it takes a long time to run.

Code:

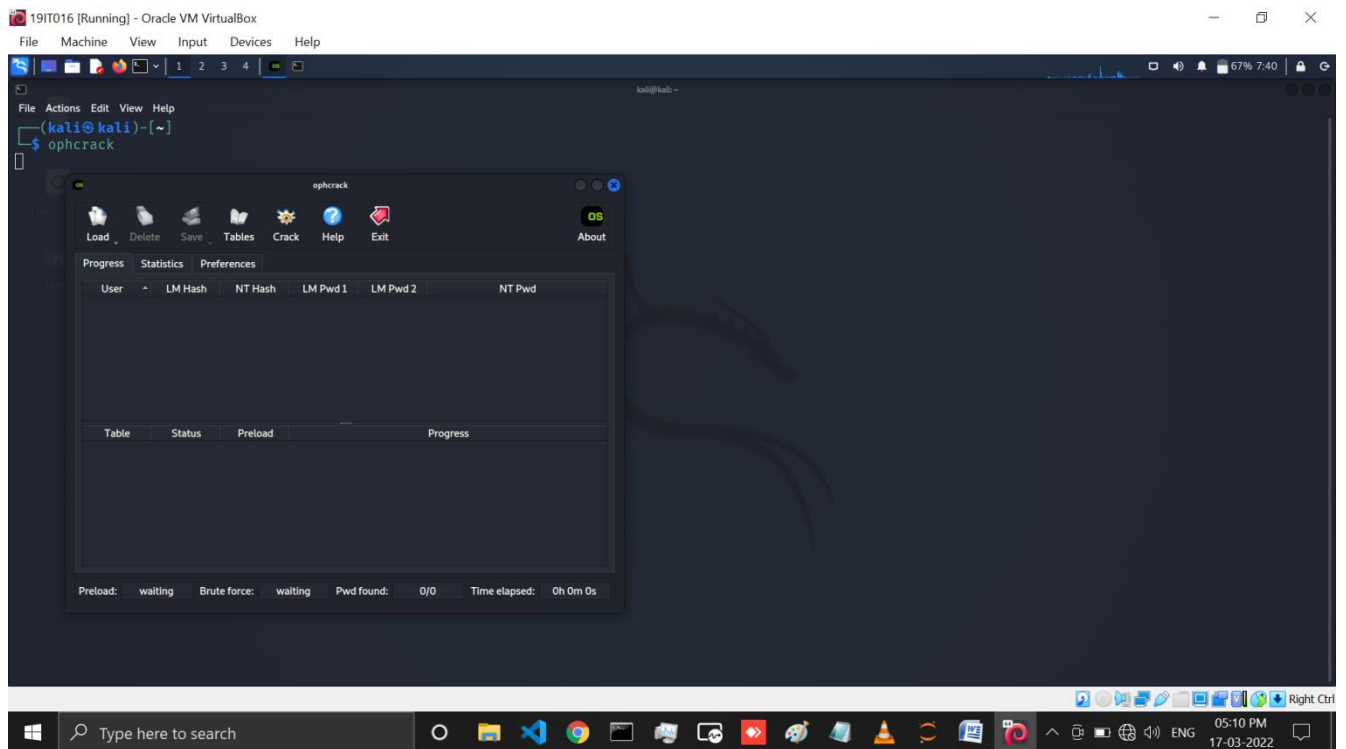
```
ophcrack  
  
john the ripper  
sudo apt-get install johnny  
sudo nano text1.txt  
sudo john --format=RAW-MD5 text1.txt
```

```
sudo cat /usr/share/john/password.lst
```

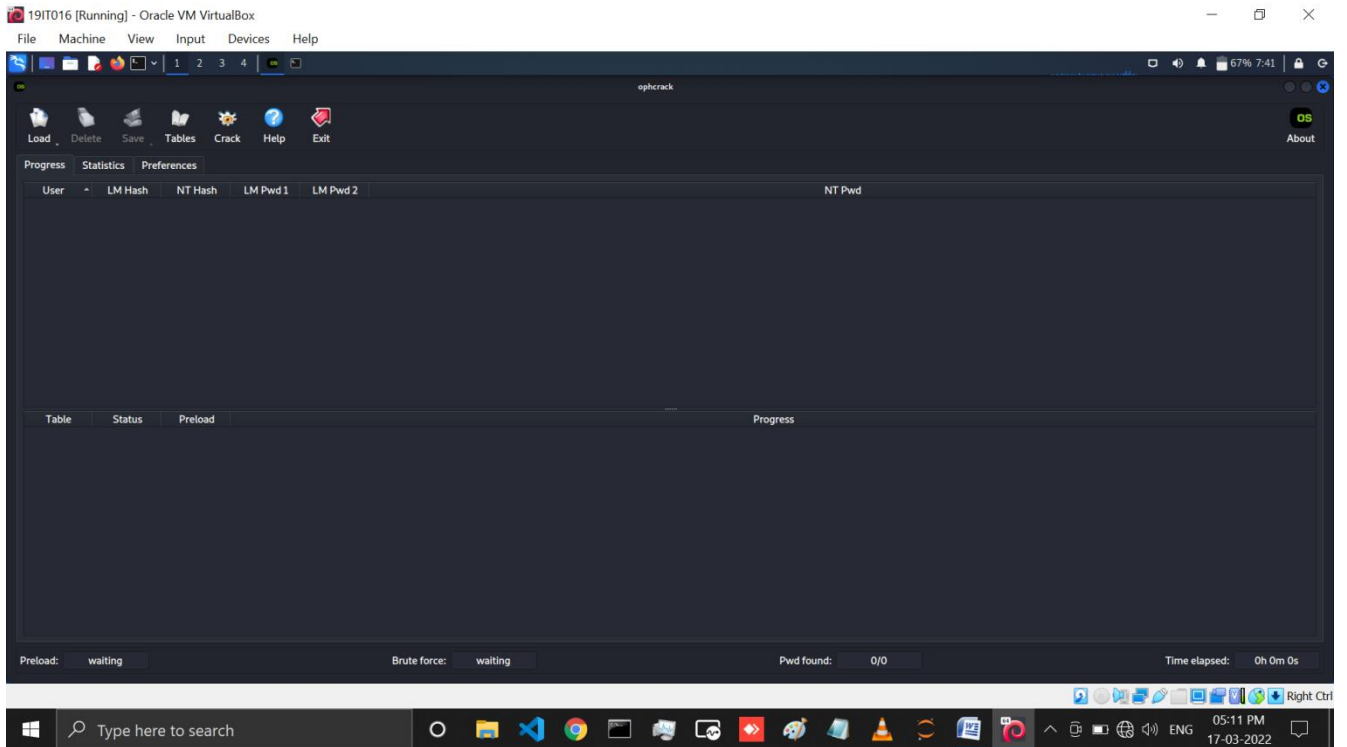
Output:

1) OPHCRACK

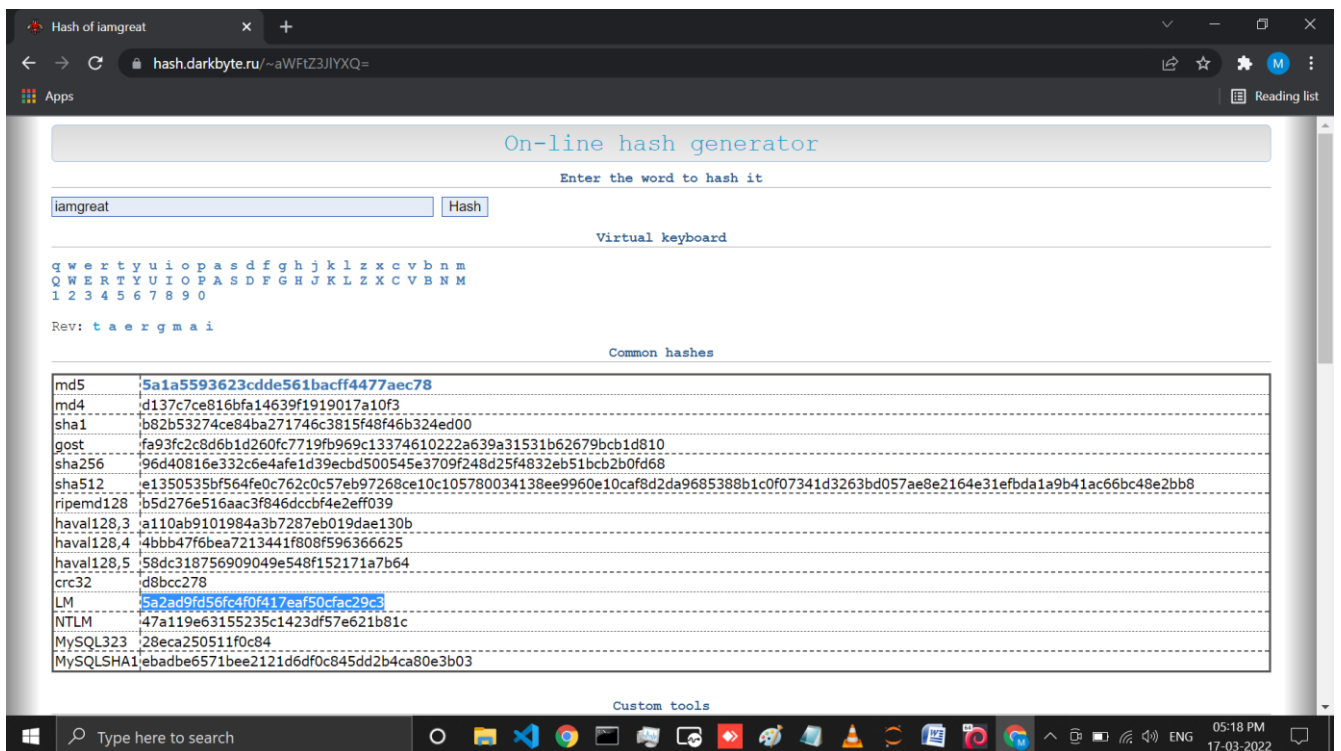
Here we do this practical using ophcrack so write command ophcrack in terminal.



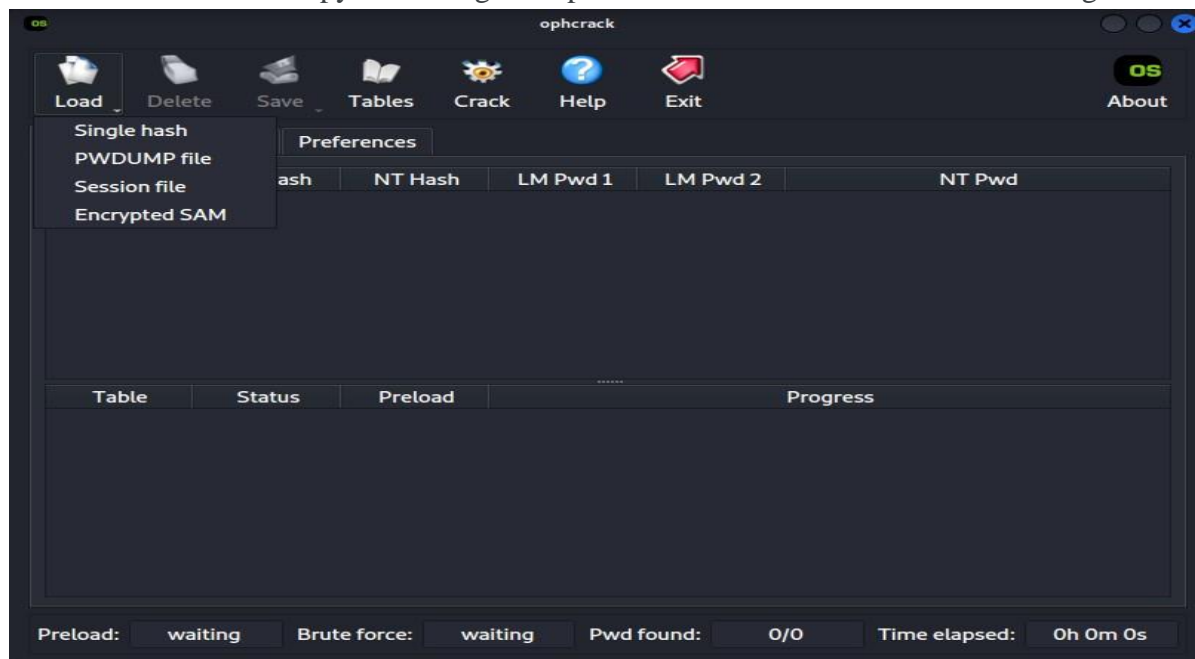
Then after enter it shows like below GUI. This is ophcrack.



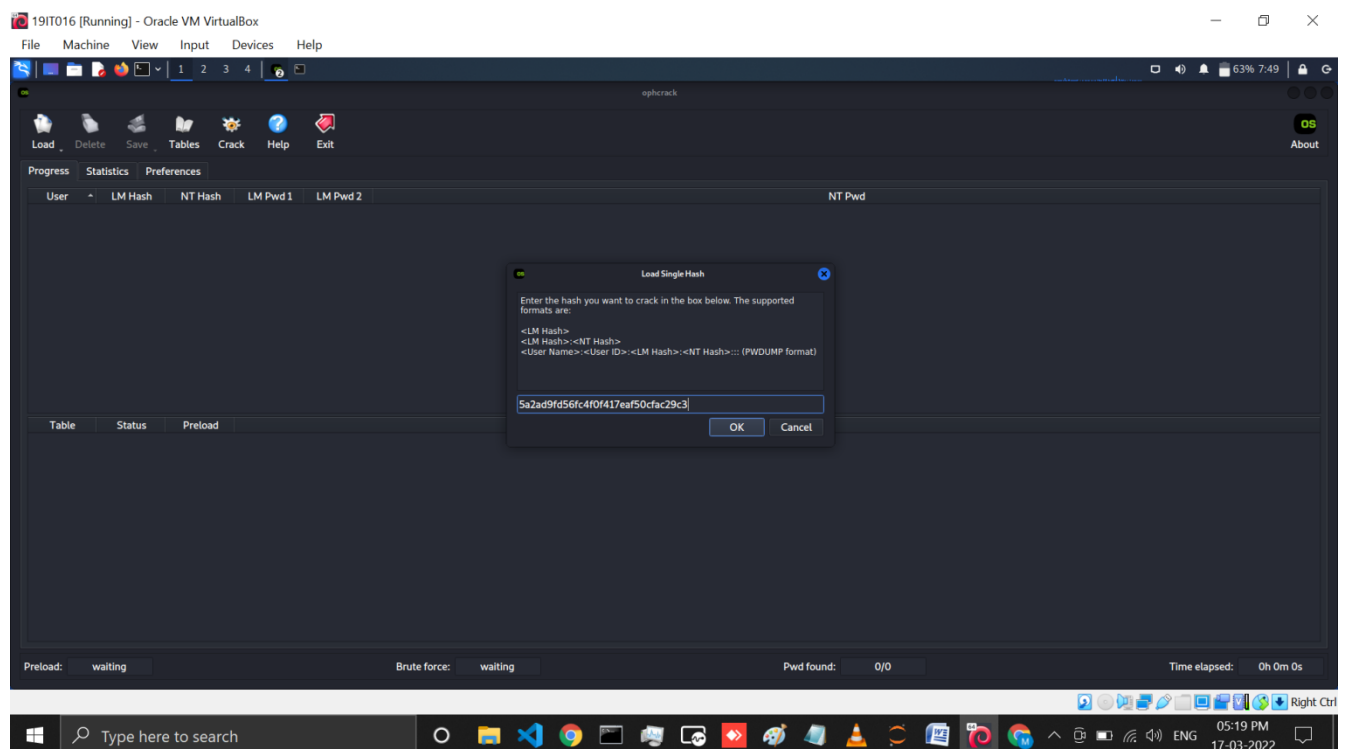
First we do practical using LM hash so crate LM hash using <https://hash.darkbyte.ru/> link.



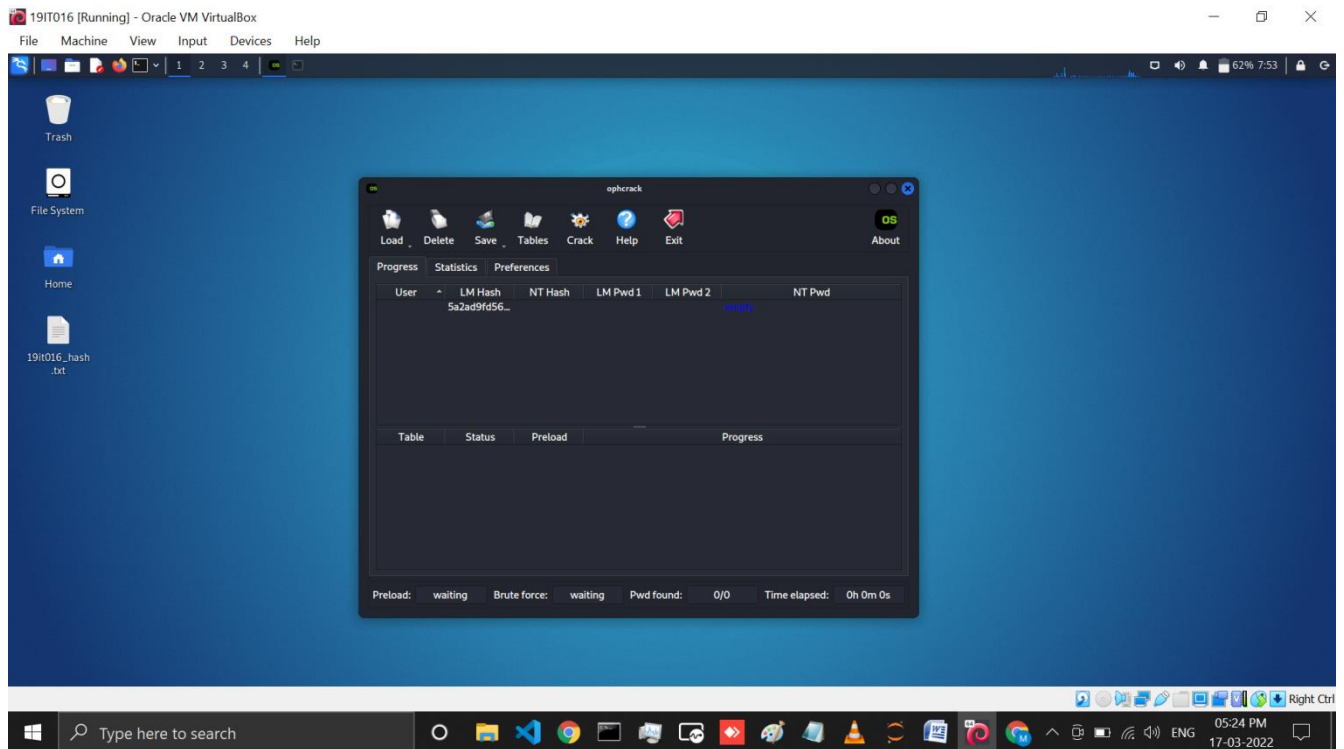
Now select LM hash copy that and go in ophcrack and click on load and select Single hash.



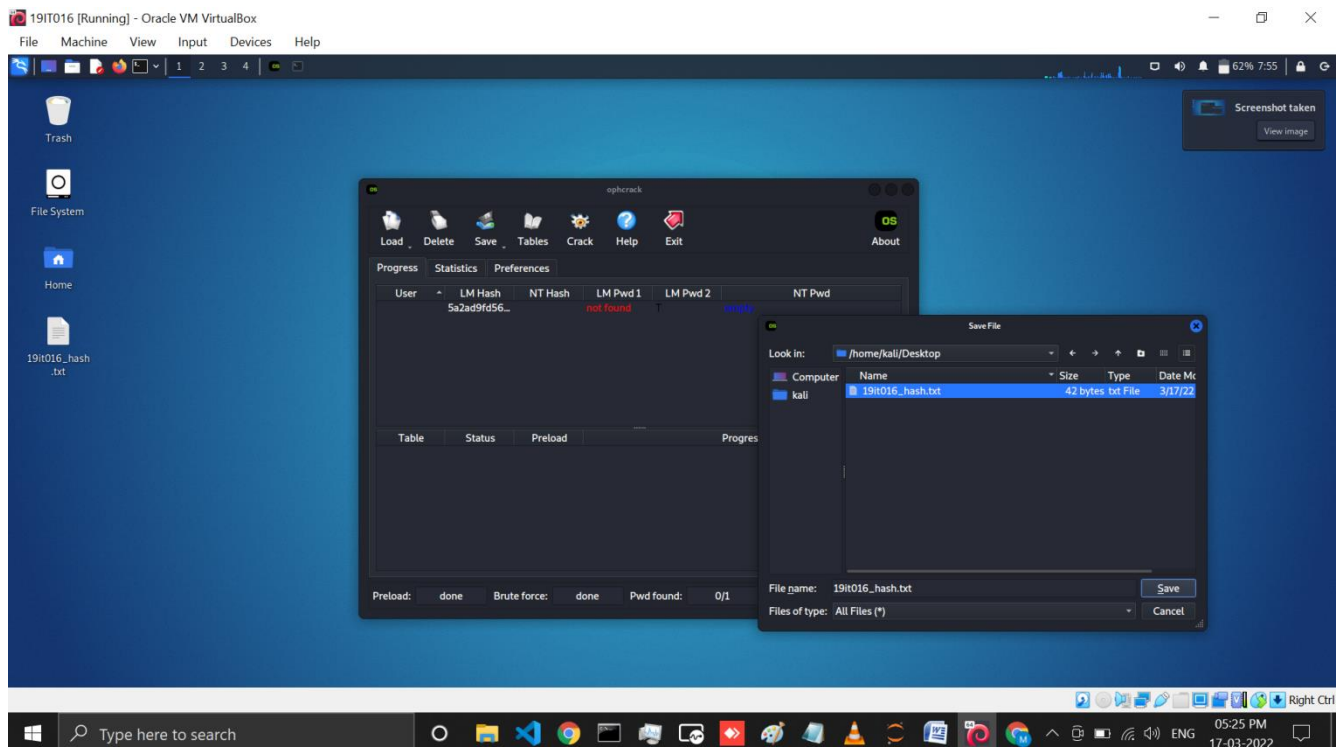
Then after it shows below GUI . In this we have to paste LM hash which we copied. Then click on OK.



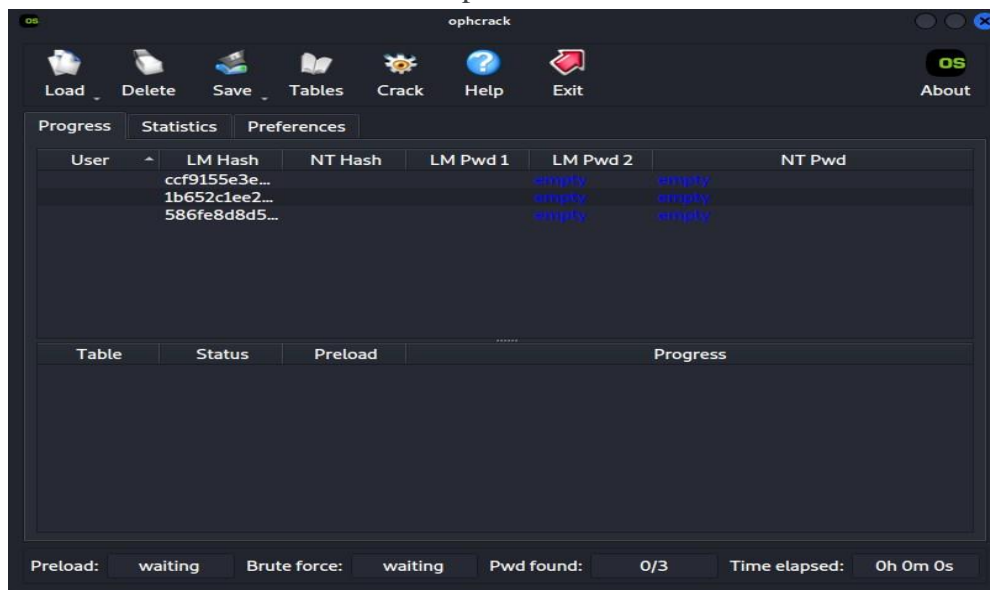
Here we can see which hash we can crack the hash value in it.



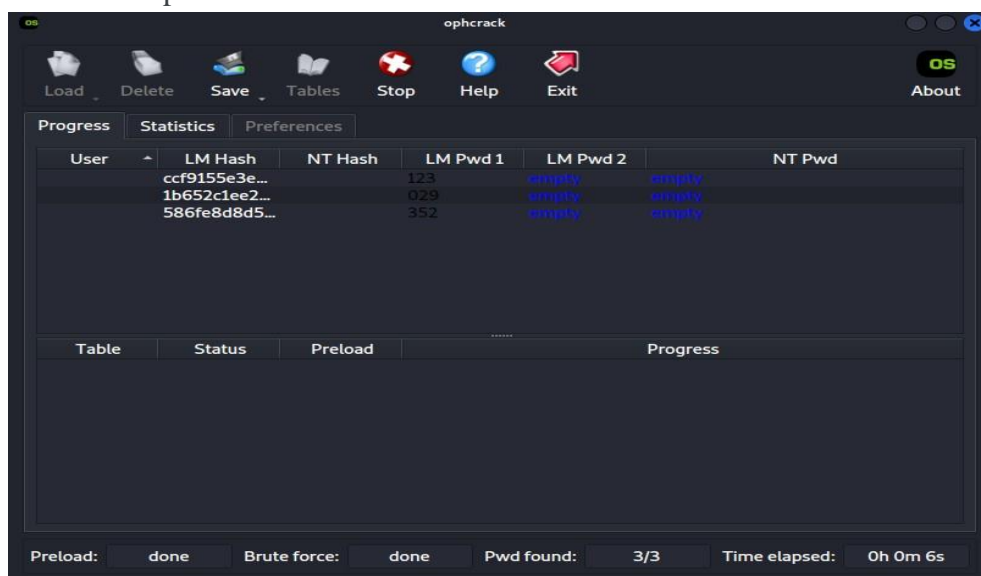
Now we will crack a text file in which we paste our hash using save option.



Then load a file in session file and crack a password of them.



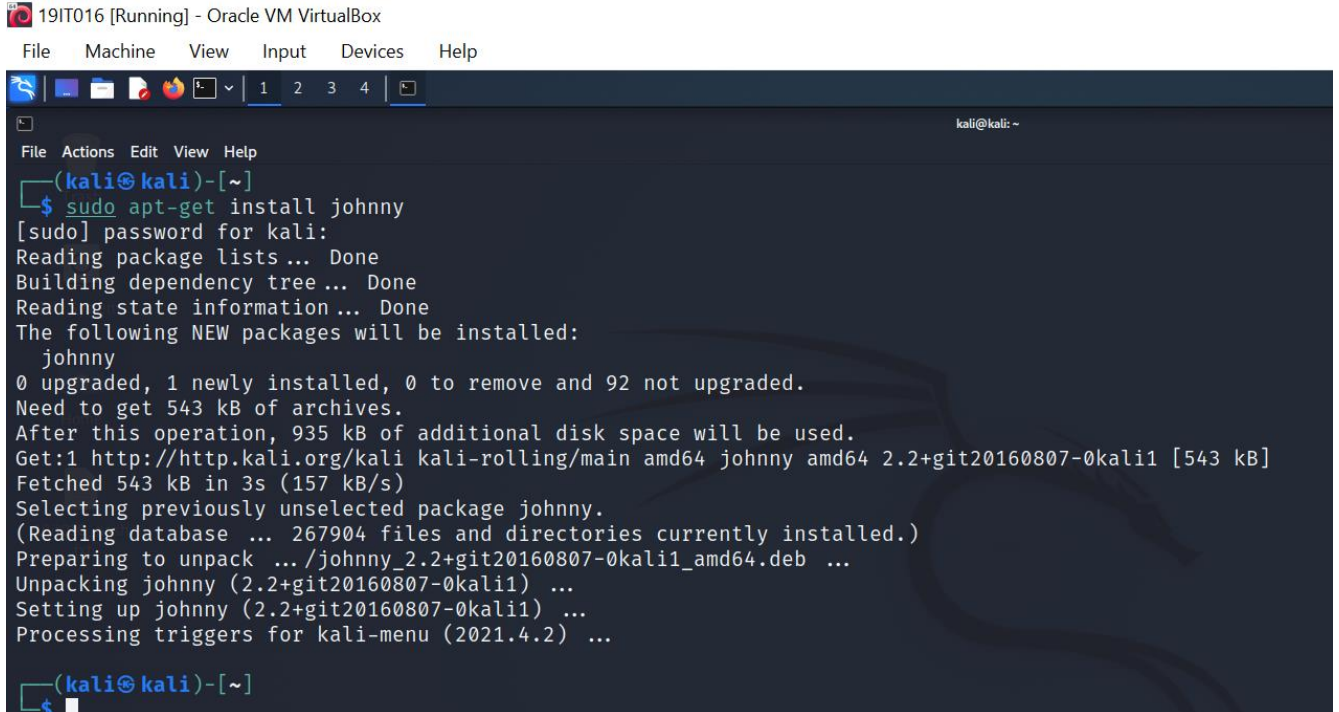
Here we can see all password are cracked.



2) John The Ripper

Here we perform john the ripper practical using john or johnny.

First we have to install johnny using `sudo apt-get install johnny`.



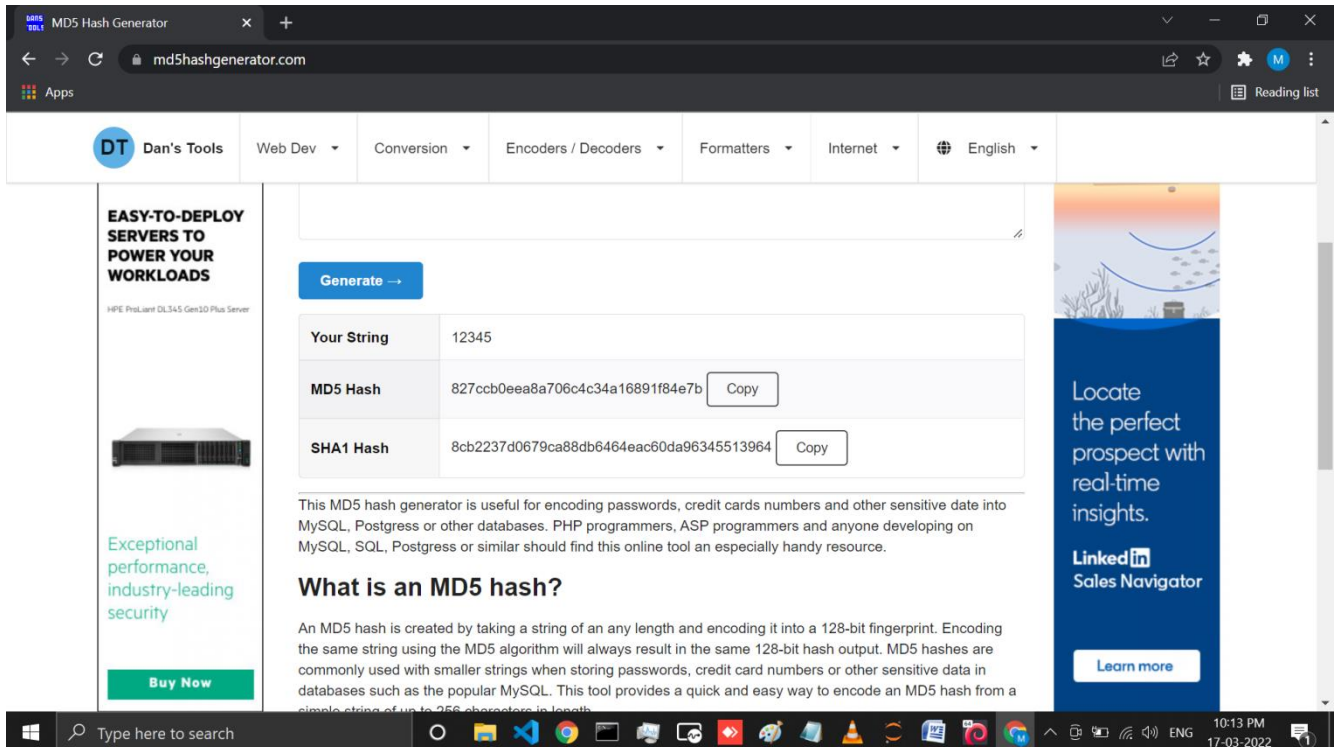
```

19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

(kali@kali)-[~]
$ sudo apt-get install johnny
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  johnny
0 upgraded, 1 newly installed, 0 to remove and 92 not upgraded.
Need to get 543 kB of archives.
After this operation, 935 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 johnny amd64 2.2+git20160807-0kali1 [543 kB]
Fetched 543 kB in 3s (157 kB/s)
Selecting previously unselected package johnny.
(Reading database ... 267904 files and directories currently installed.)
Preparing to unpack .../johnny_2.2+git20160807-0kali1_amd64.deb ...
Unpacking johnny (2.2+git20160807-0kali1) ...
Setting up johnny (2.2+git20160807-0kali1) ...
Processing triggers for kali-menu (2021.4.2) ...

(kali@kali)-[~]
$
  
```

Here we have to create one MD5 hash.



The screenshot shows the MD5 Hash Generator website. The 'Your String' field contains '12345'. The 'MD5 Hash' field displays '827ccb0eea8a706c4c34a16891f84e7b' with a 'Copy' button. The 'SHA1 Hash' field displays '8cb2237d0679ca88db6464eac60da96345513964' with a 'Copy' button.

Field	Value	Action
Your String	12345	
MD5 Hash	827ccb0eea8a706c4c34a16891f84e7b	Copy
SHA1 Hash	8cb2237d0679ca88db6464eac60da96345513964	Copy

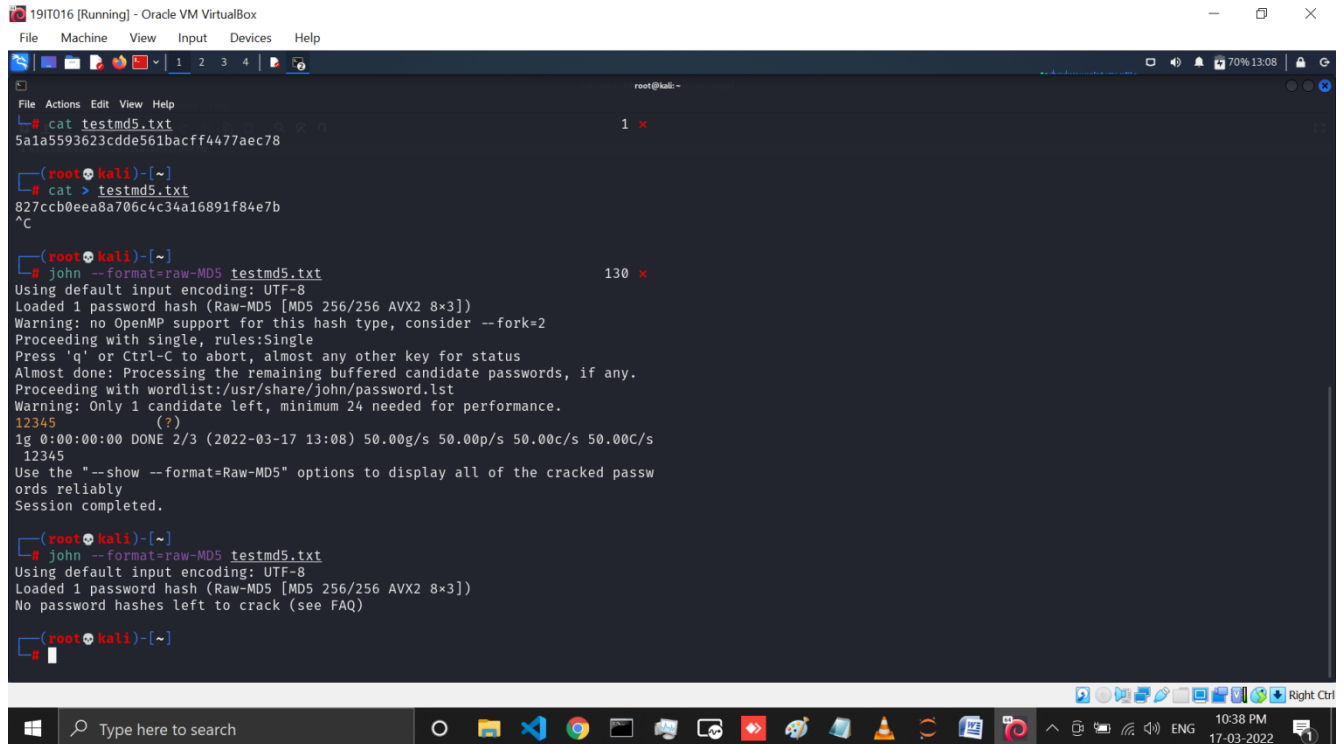
This MD5 hash generator is useful for encoding passwords, credit cards numbers and other sensitive data into MySQL, Postgress or other databases. PHP programmers, ASP programmers and anyone developing on MySQL, SQL, Postgress or similar should find this online tool an especially handy resource.

What is an MD5 hash?

An MD5 hash is created by taking a string of any length and encoding it into a 128-bit fingerprint. Encoding the same string using the MD5 algorithm will always result in the same 128-bit hash output. MD5 hashes are commonly used with smaller strings when storing passwords, credit card numbers or other sensitive data in databases such as the popular MySQL. This tool provides a quick and easy way to encode an MD5 hash from a single string of up to 256 characters in length.

The image shows a Kali Linux virtual machine interface. At the top, the title bar reads '1910T016 [Running] - Oracle VM VirtualBox'. Below the title bar is a menu bar with 'File', 'Machine', 'View', 'Input', 'Devices', and 'Help'. The main window is a terminal titled 'Shell No. 1'. The terminal output shows the 'hashcat' command being executed, which displays a large ASCII art dragon logo and the version 'v1.2.2'. Below the logo, it lists 'Possible Hashes' and 'Least Possible Hashes' for the MD4 hash 827ccb0eeba7b0c4c3a16891fb4e7b. The session is titled 'Shell No. 1'. The bottom of the image shows the Windows taskbar with various icons and the system clock indicating 10:41 PM on 17-03-2022.

Here we create one testmd5.txt file and past that hash in this file. Now we crack password through john using code `sudo john --format=RAW-MD5 testmd5.txt`



```
19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

root@kali: ~
# cat testmd5.txt
5a1a5593623cdde561bacff4477aec78

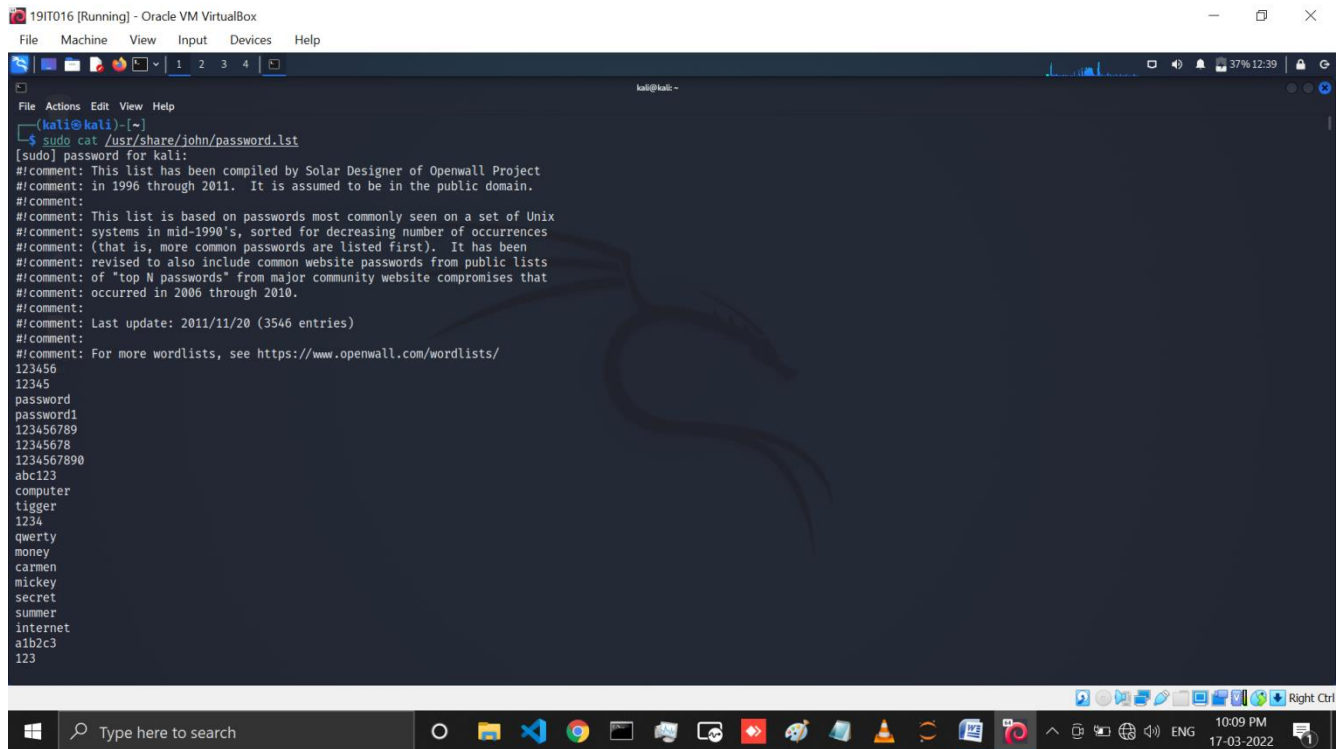
(root@kali)~# cat > testmd5.txt
827ccb0eea8a706c4c34a16891f84e7b
^C

(root@kali)~# john --format=raw-md5 testmd5.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Warning: Only 1 candidate left, minimum 24 needed for performance.
12345 (?)
ig 0:00:00:00 DONE 2/3 (2022-03-17 13:08) 50.00g/s 50.00p/s 50.00c/s 50.00C/s
12345
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(root@kali)~# john --format=raw-md5 testmd5.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
No password hashes left to crack (see FAQ)

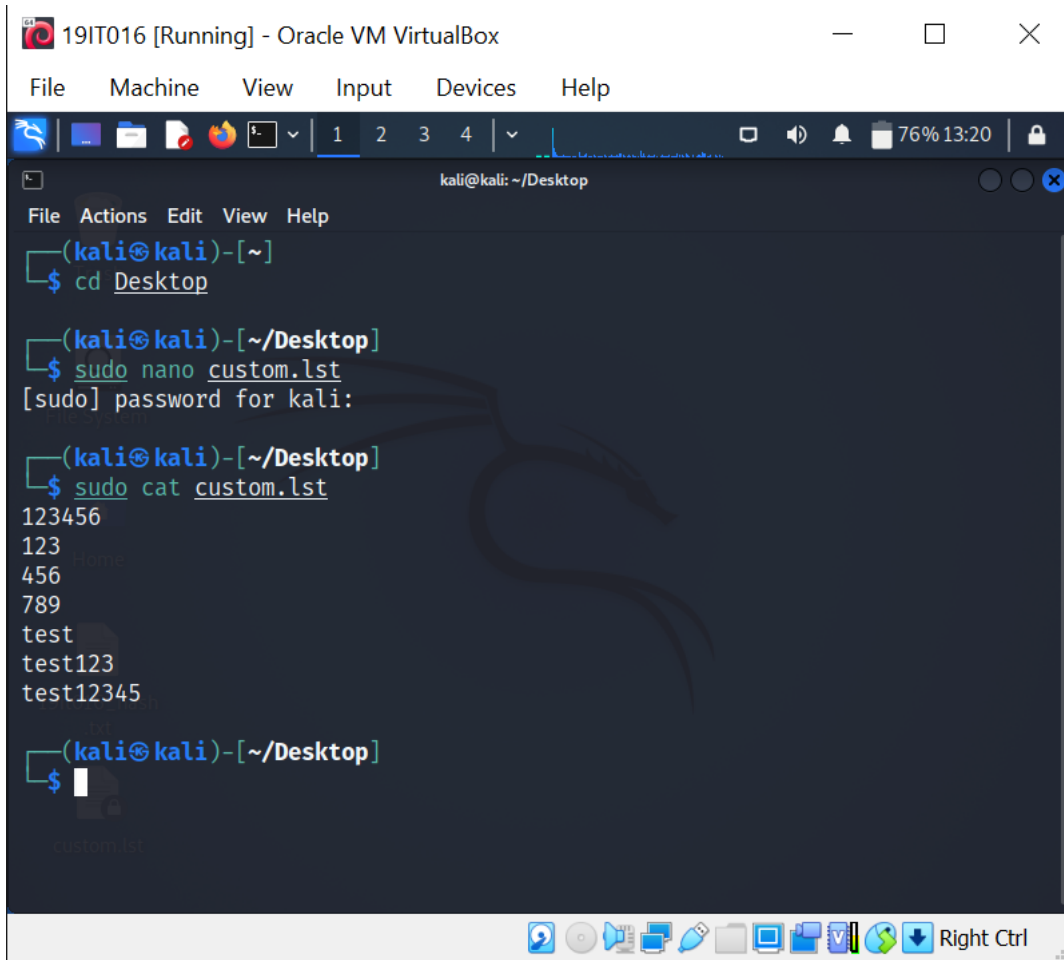
(root@kali)~#
```

Here We can see which are the password saved in password.lst file which is from john created.



```
kali@kali:~$ sudo cat /usr/share/john/password.lst
[sudo] password for kali:
#comment: This list has been compiled by Solar Designer of Openwall Project
#comment: in 1996 through 2011. It is assumed to be in the public domain.
#comment:
#comment: This list is based on passwords most commonly seen on a set of Unix
#comment: systems in mid-1990's, sorted for decreasing number of occurrences
#comment: (that is, more common passwords are listed first). It has been
#comment: revised to also include common website passwords from public lists
#comment: of "top N passwords" from major community website compromises that
#comment: occurred in 2006 through 2010.
#comment:
#comment: Last update: 2011/11/20 (3546 entries)
#comment:
#comment: For more wordlists, see https://www.openwall.com/wordlists/
123456
12345
password
password1
123456789
12345678
1234567890
abc123
computer
tigger
1234
qwerty
money
carmen
mickey
secret
summer
internet
a1b2c3
123
```

Now we create on custom.lst file where we manually take password.



```
19IT016 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~]
$ cd Desktop
(kali@kali)-[~/Desktop]
$ sudo nano custom.lst
[sudo] password for kali:
(kali@kali)-[~/Desktop]
$ sudo cat custom.lst
123456
123
456
789
test
test123
test12345
(kali@kali)-[~/Desktop]
$
```

LATEST APPLICATIONS:

Jphn the Ripper (jtr) is primarily a password cracker used during pentesting exercises that can help IT staff spot weak passwords and poor password policies. Here is the list of encryption technologies found in JtR:

- Work with Unix, Windows & Kerberos
- Compatible with LDAP, MySQL & MD4 with addition of extra modules.
- FreeBSD MD5-based (linux and Cisco IOS)
- OpenBSD Blowfish-based
- Kerberos/AFS
- Windows LM (DES-based)
- DES-based tripcodes

LEARNNG OUTCOME:

Here with this practical learned about system hacking and tools like OPHcrack and John the ripper how does they work, how we can get the password form the hash. We also learn how to use johnny and john. How we crack password from default list and how we can createa list and than crack password.

REFERENCE:

- 1) OPHCRACK: <https://www.youtube.com/watch?v=JaQ7w4iqInY>
- 2) John The Ripper: https://www.youtube.com/watch?v=oAuk3A2qB_c
<https://www.youtube.com/watch?v=4-kwklhxho>