# AIM:-

PRACTICAL-7

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

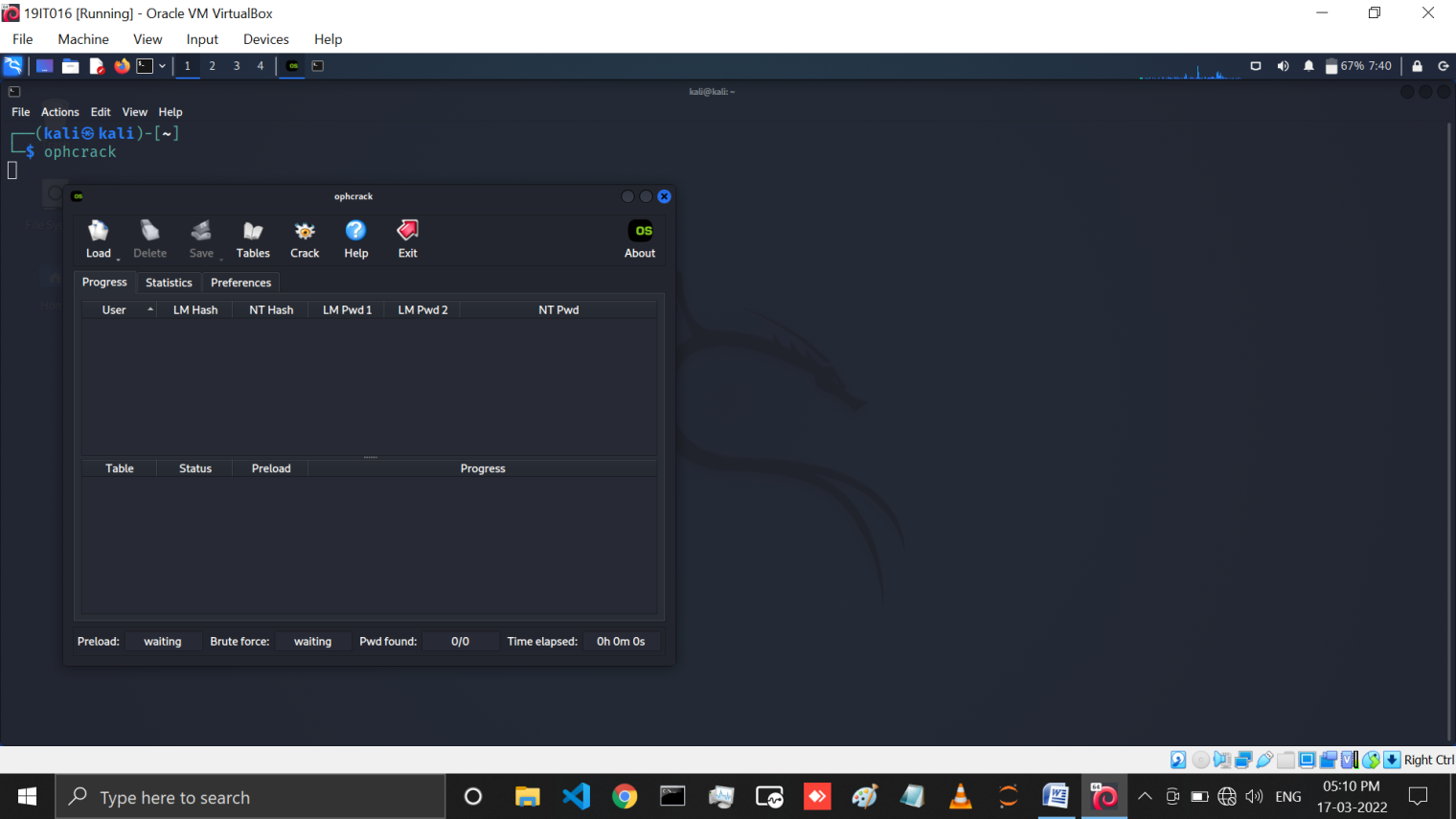
sudo john –format=RAW-MD5 text1.txt

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

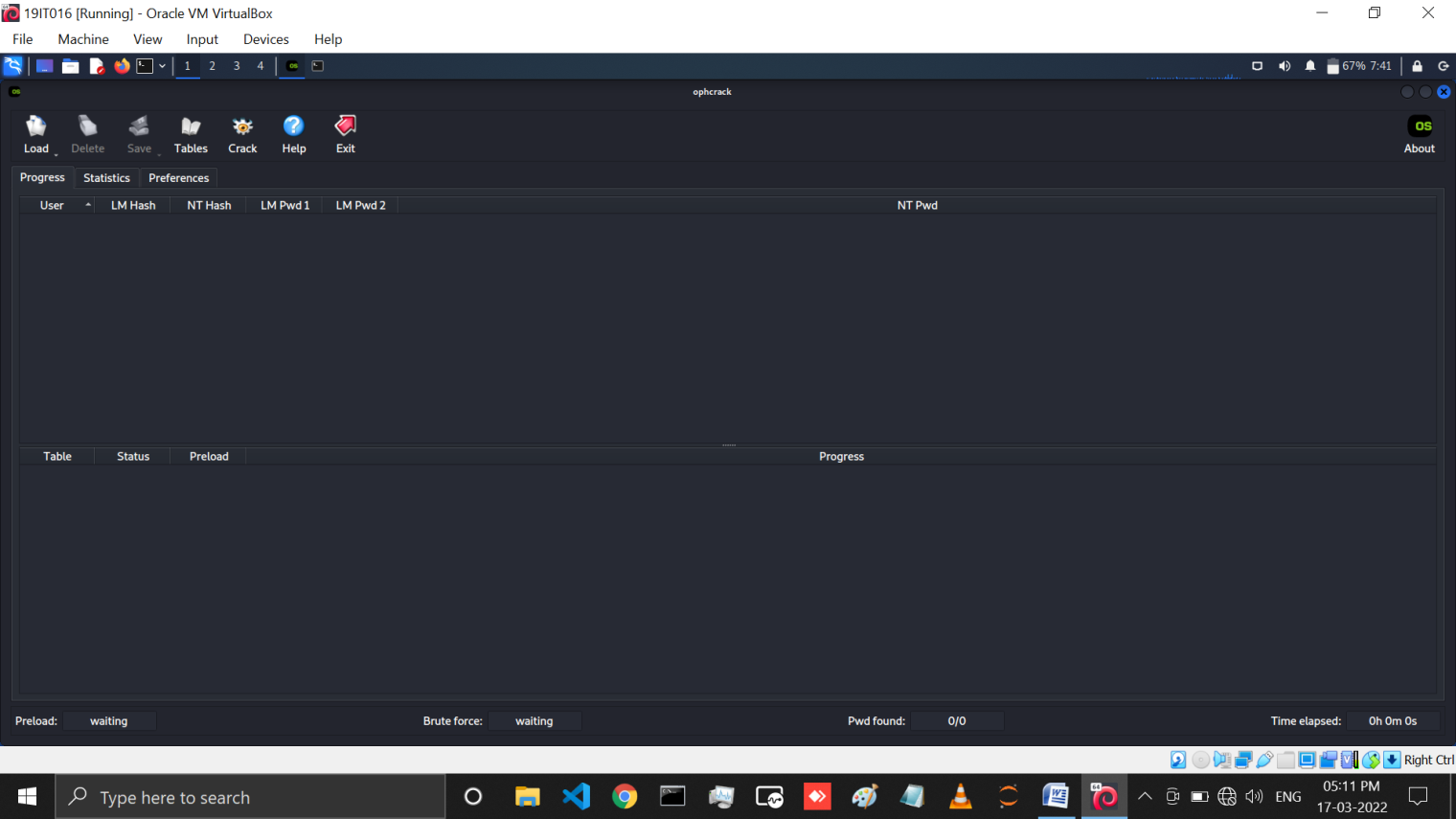
**Output:**

* 1. OPHCRACK

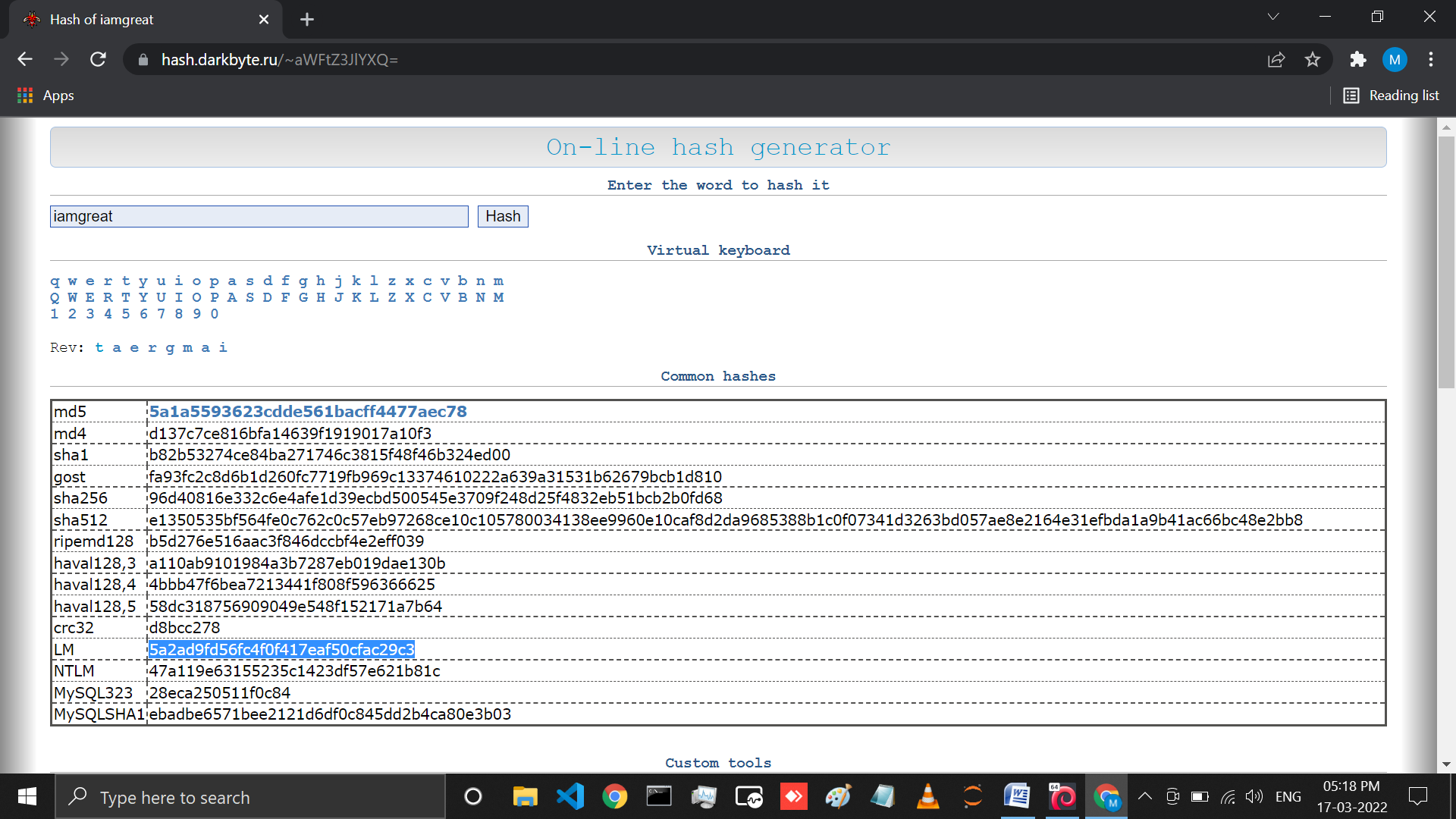
Here we do this practical using ophcrack so write command ophcrack in terminal.



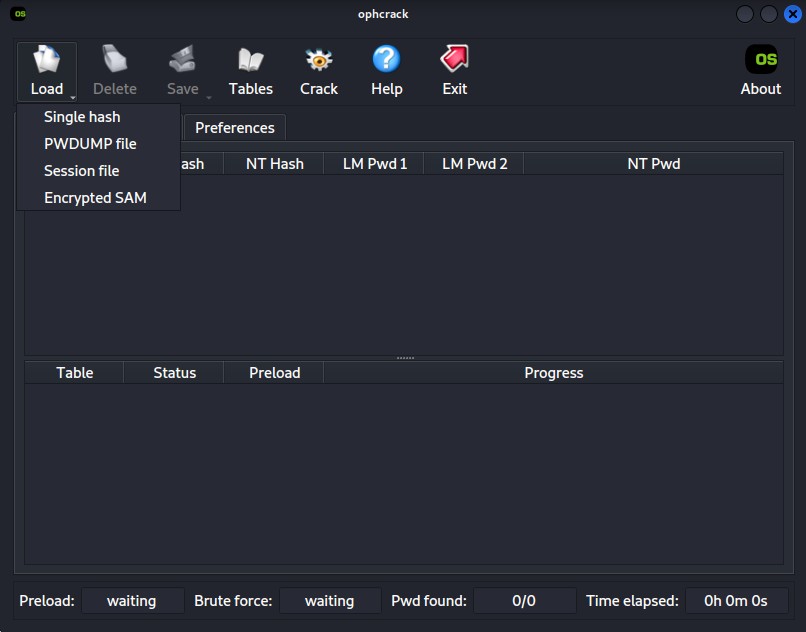
Then after enter it shows like below GUI. This is ophcrack.



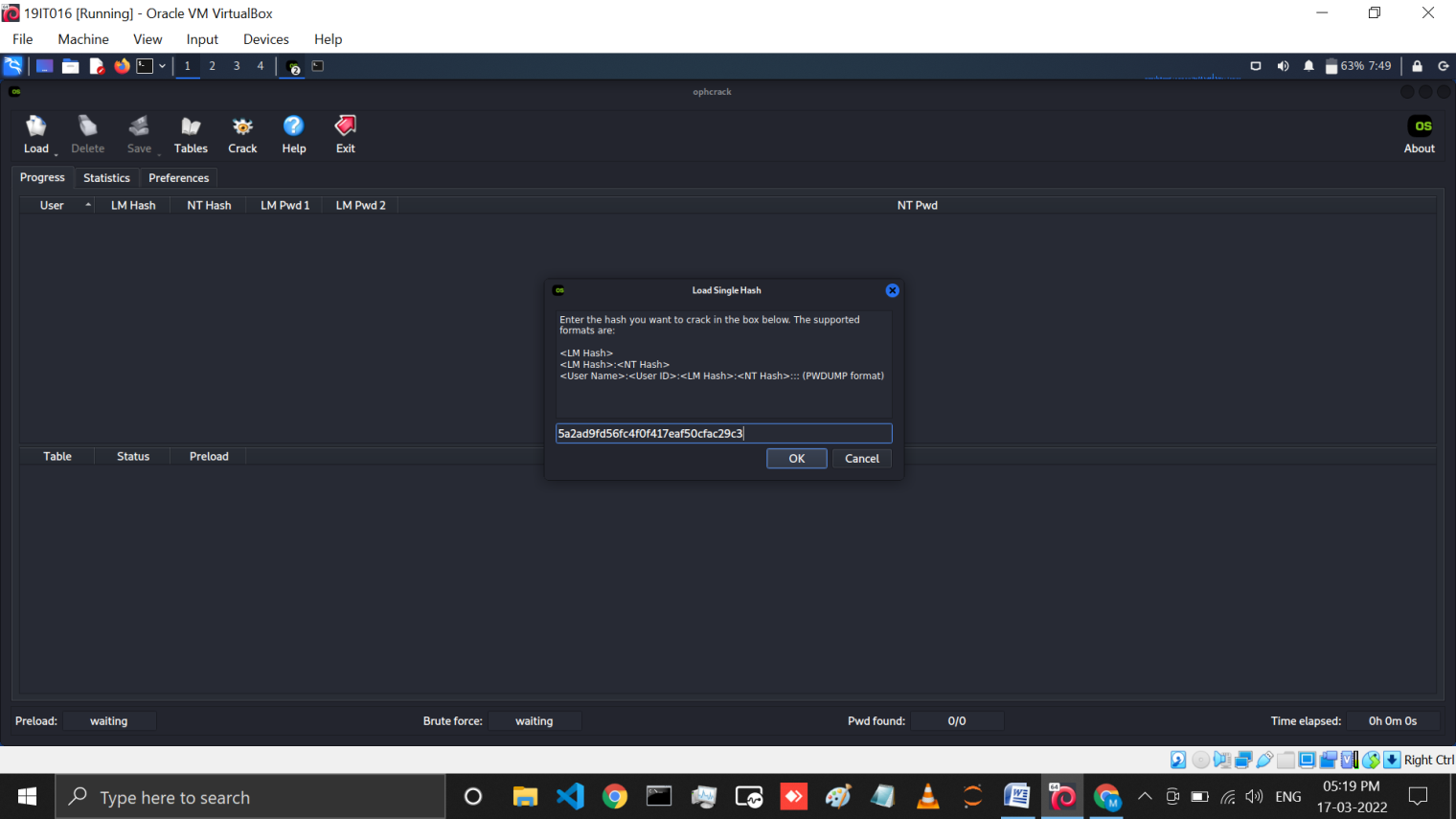
First we do practical using LM hash so crate LM hash using <https://hash.darkbyte.ru/> link.



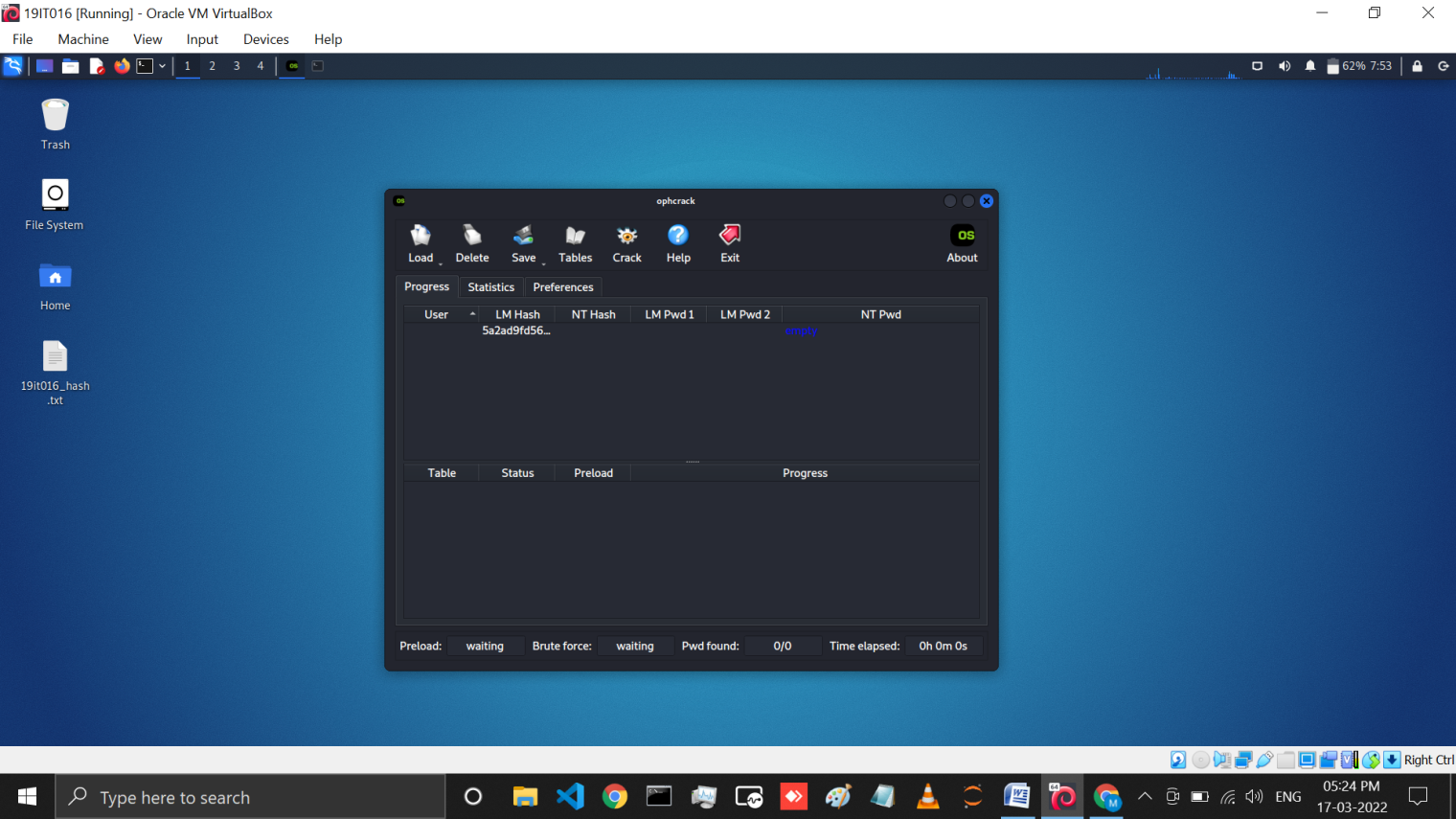
Now select LM hash copy that and go in ophcrack and click on load and select Single hash.



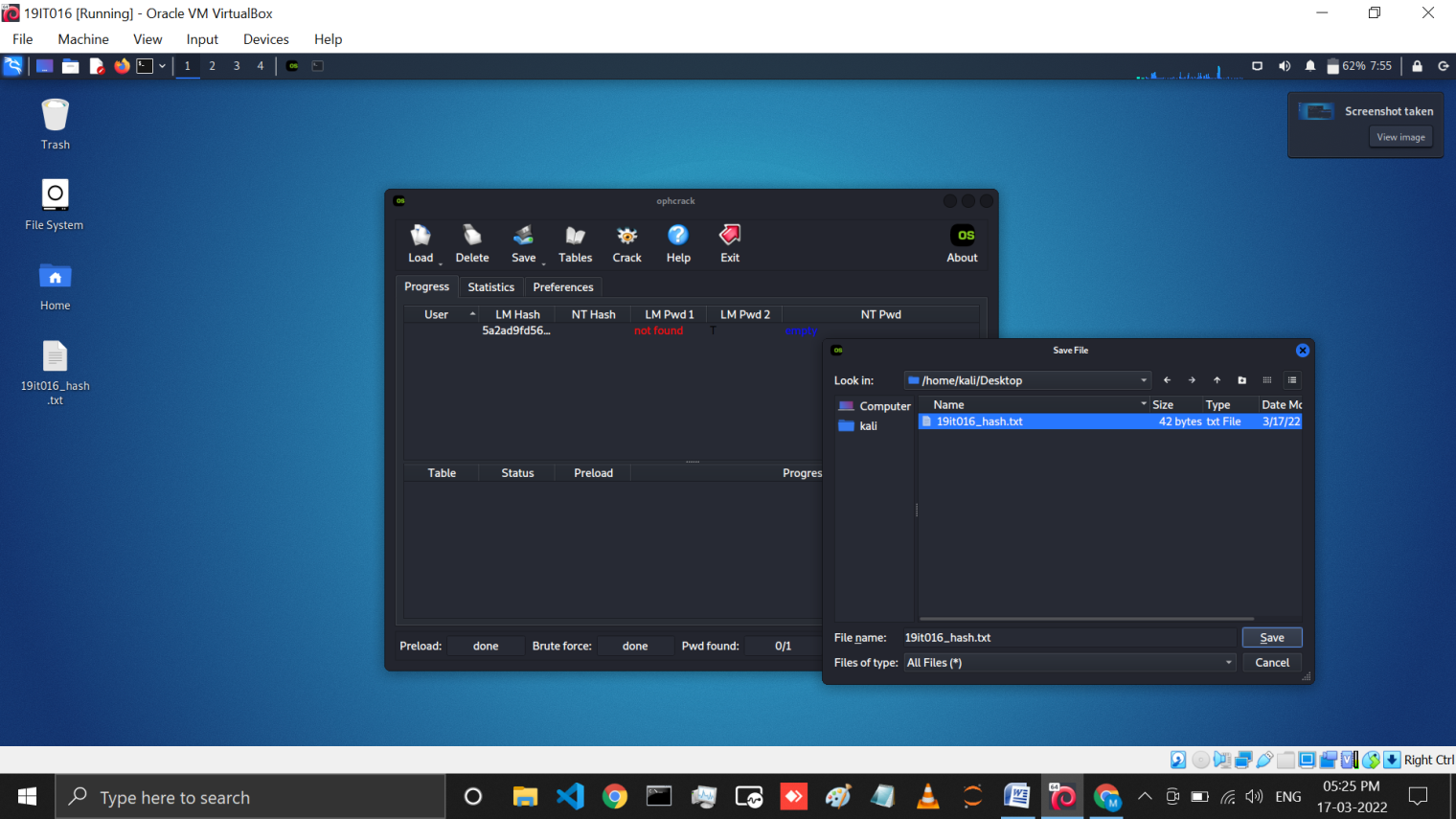
Then after it shows below GUI . In this we have to paste LM hash which we copied. Then click on OK.



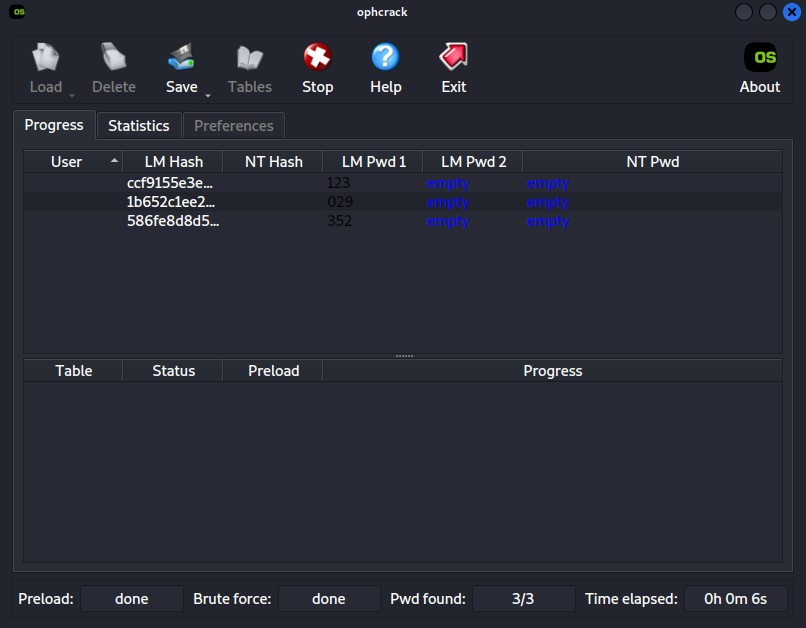
Here we can which we select hash we can crack the hash value in it.



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

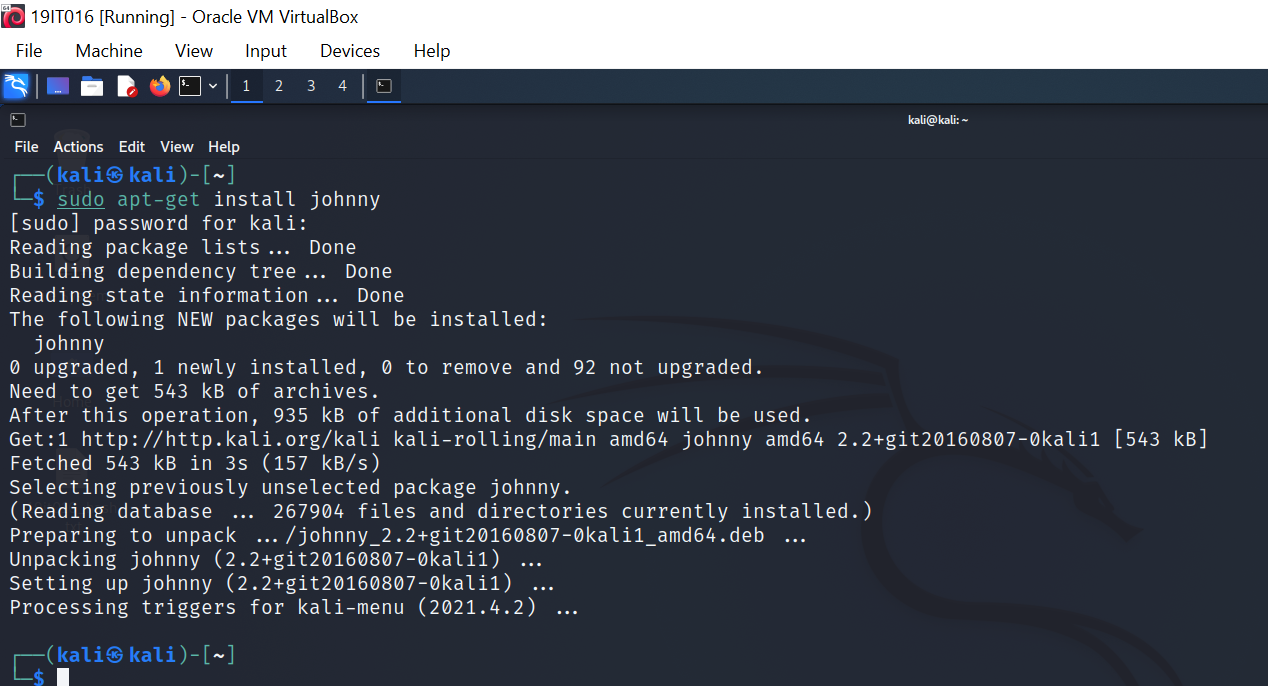


Then load a file in session file and crack a password of them.

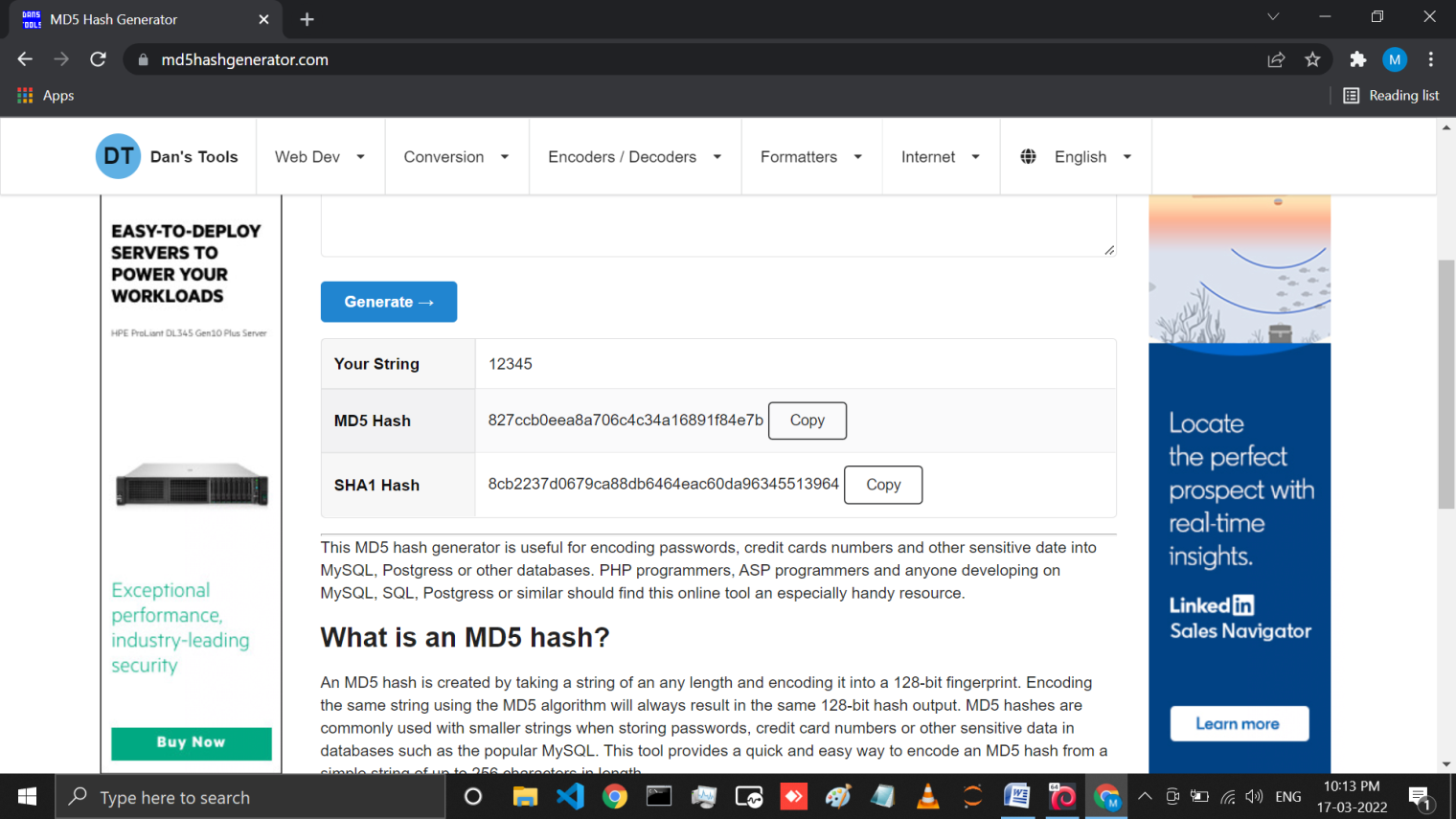
Here we can see all password are cracked.

* 1. John The Ripper

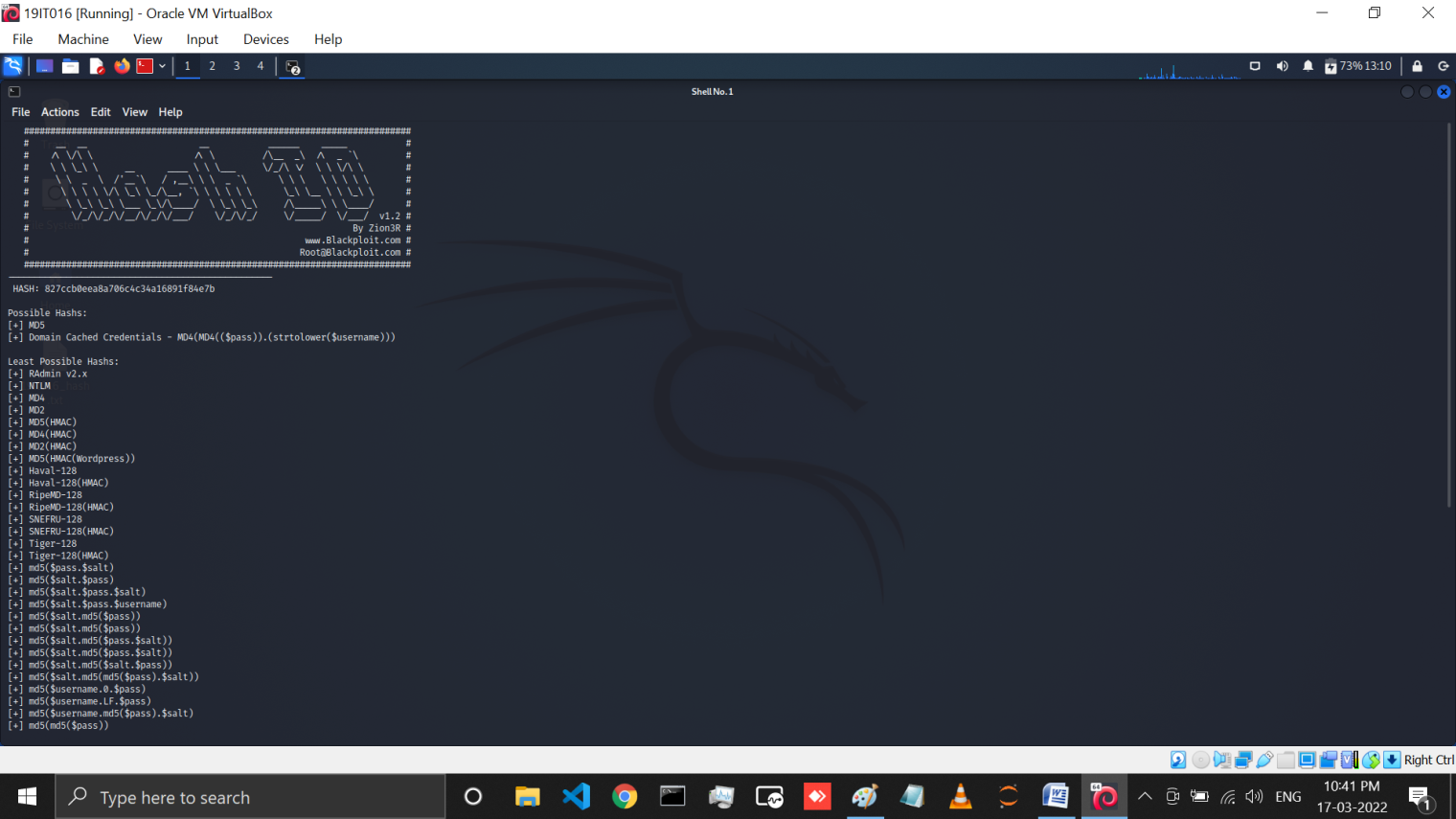
Here we perform john the ripper practical using john or johnny. First we have to install johnny using sudo apt-get install johnny.



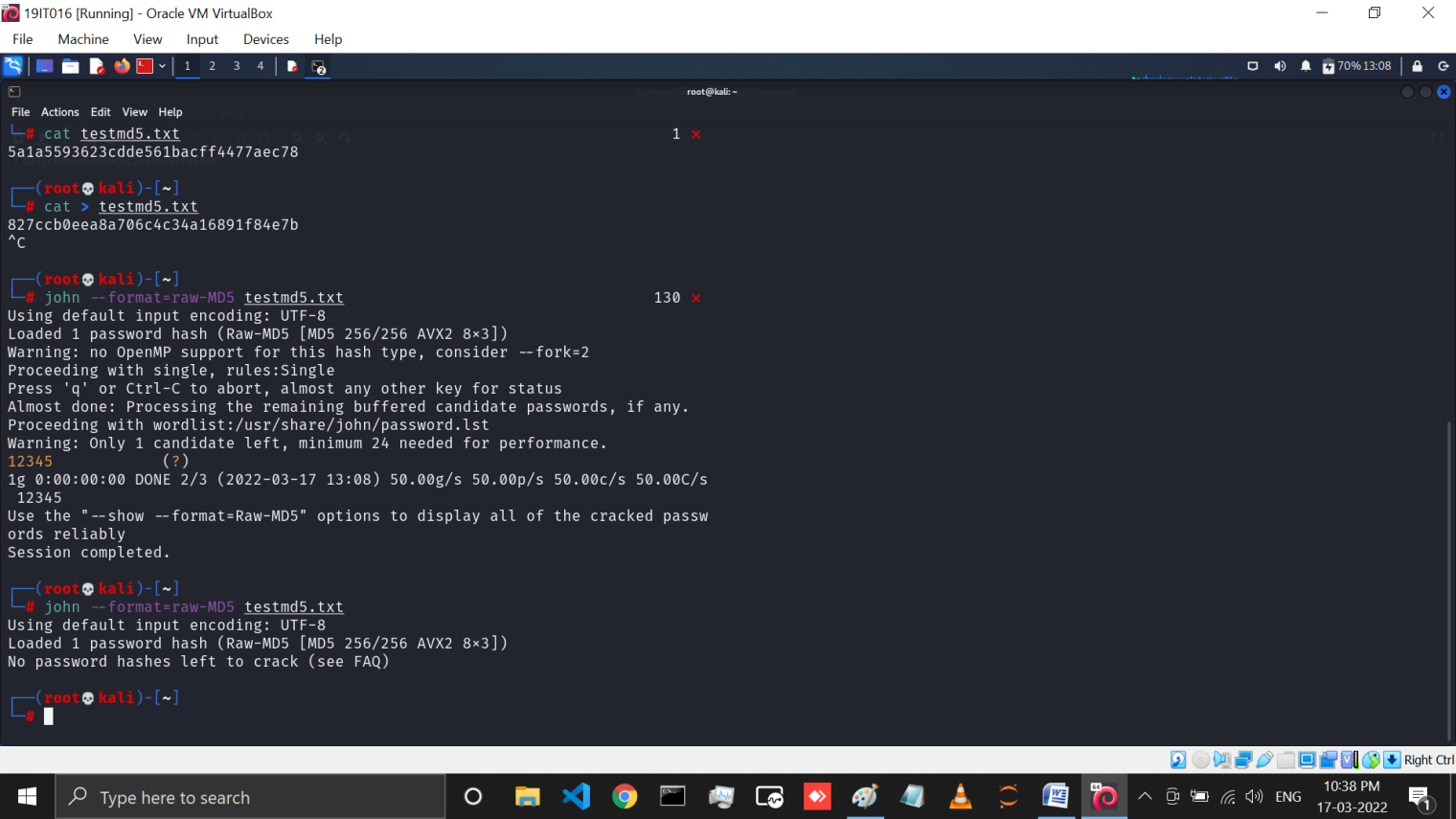
Here we have to create one MD5 hash.



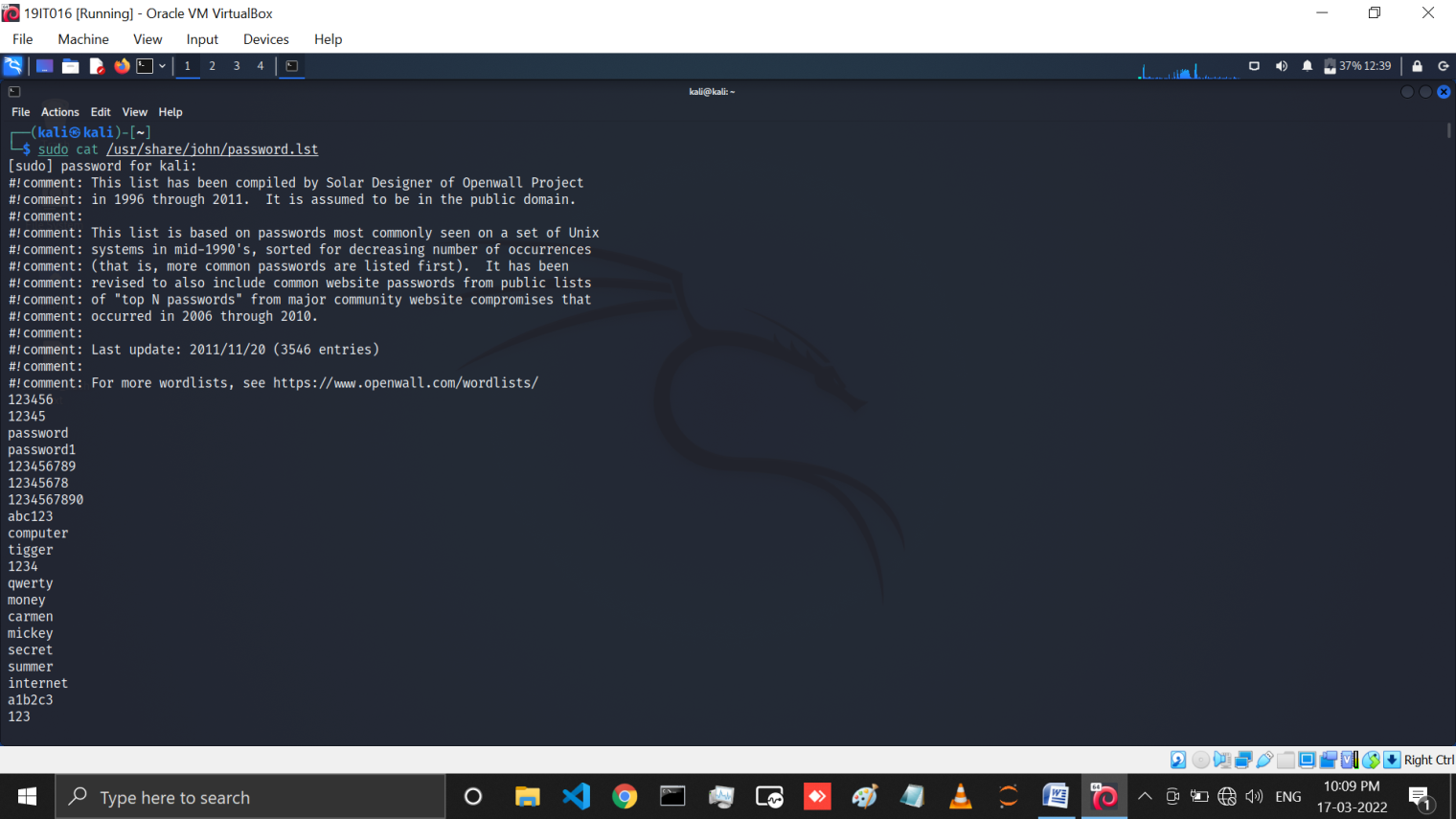
Here we check hash using hash-identifier.



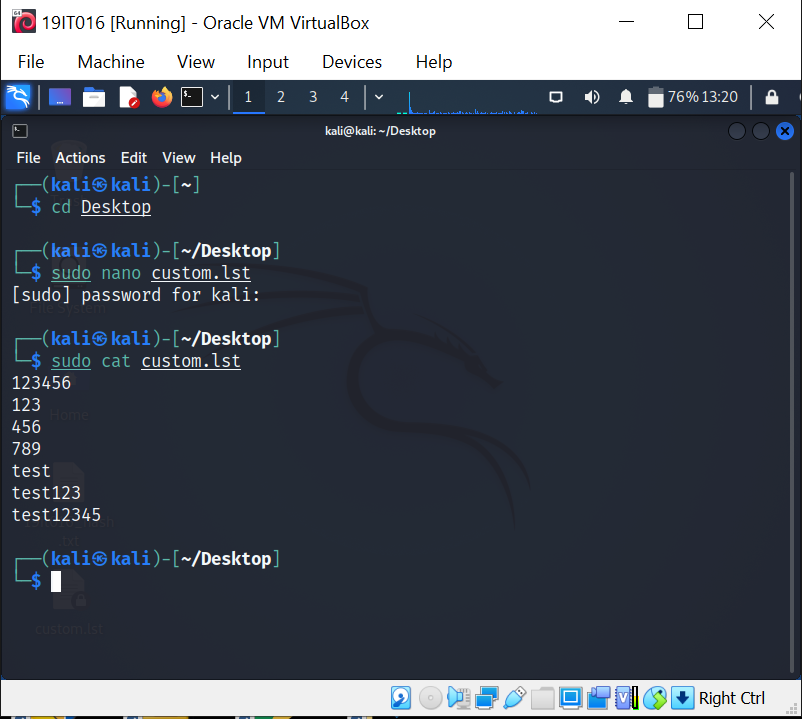
Here we create one testmd5.txt file and past that hash in this file. Now we crack password through john using code sudo john --format=RAW-MD5 testmd5.txt



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



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



# 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>