**Lab 9: Password Cracking of Windows Operating System.**

**What You Need for this lab**

* + Virtual pc with Windows 10 OS, Kali Linux
  + Mimikatz tool
    - <https://github.com/ParrotSec/mimikatz>
  + Hashcat tool

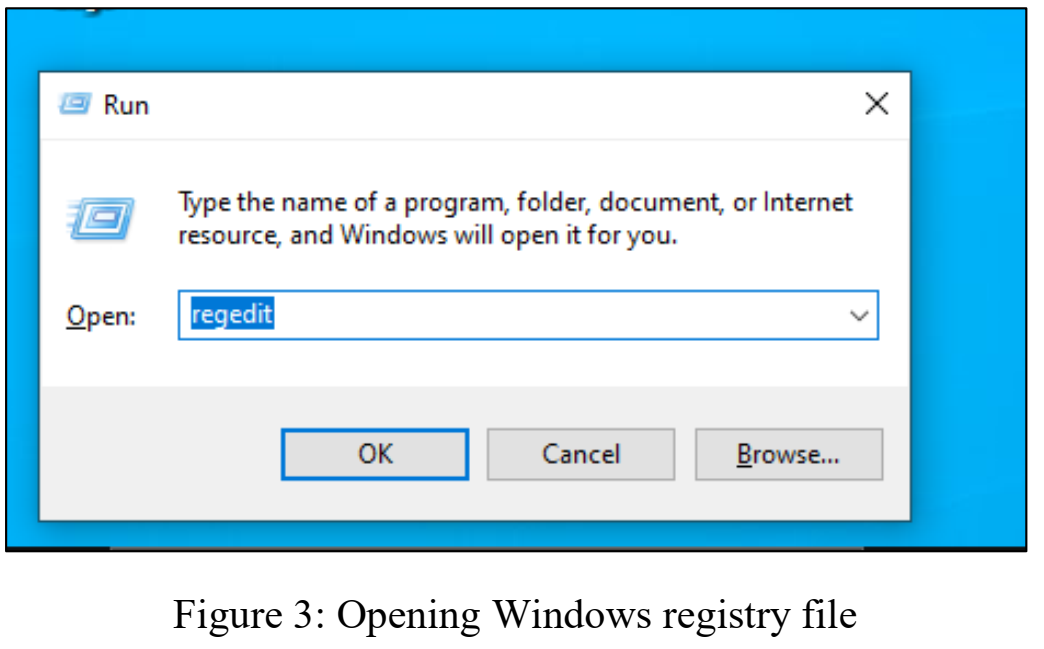
**Goal :**

* + Helps learners to understand the methods of breaking the password of the Windows operating system.
  + The password cracking techniques are used as follows : Brute force, Dictionary technique, Rainbow tables.

**Step 1.**

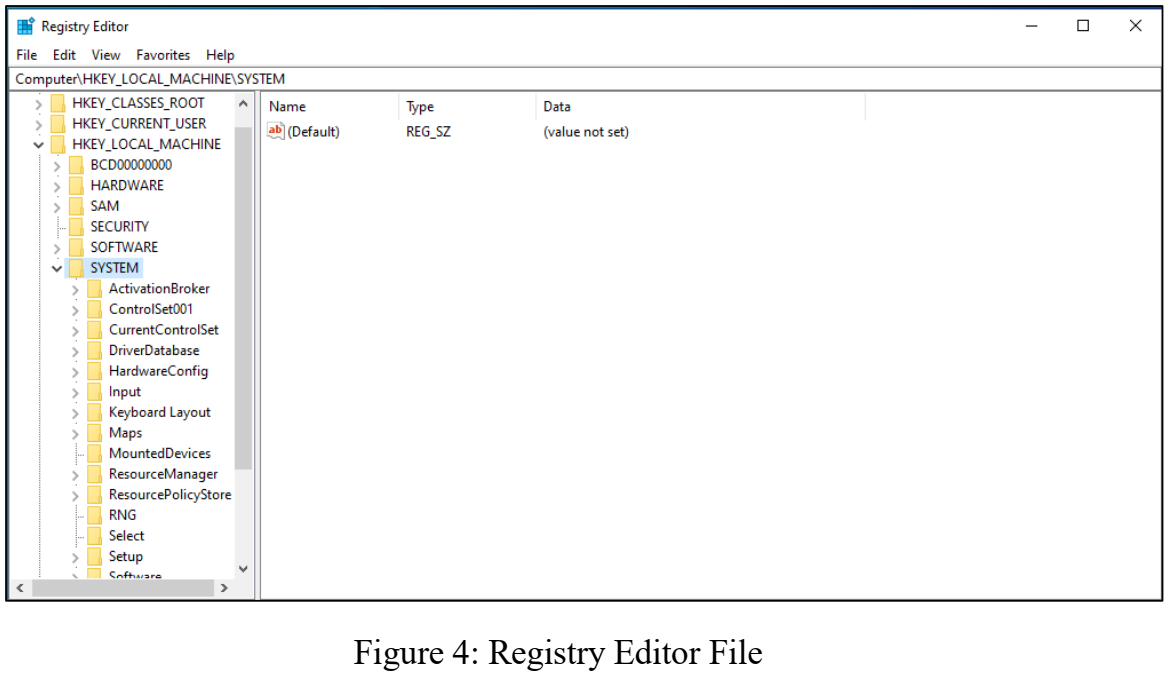
Open Run box by clicking “Window + R” on keyboard and type “regedit” as shown in Figure 2 and Figure 3 respectively. Click “OK” to proceed.

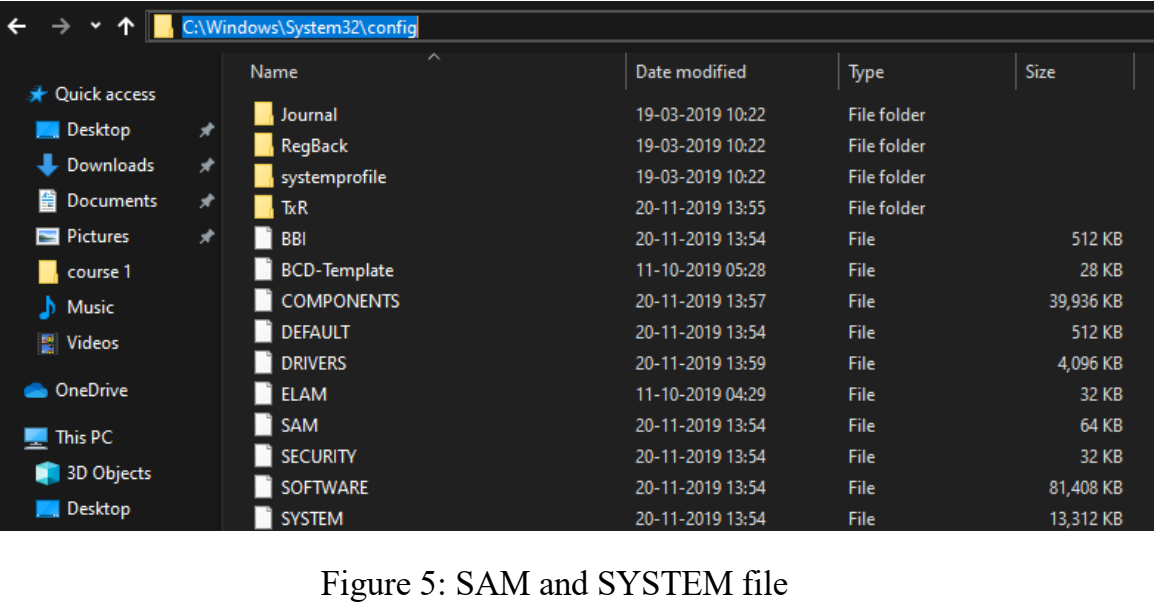




Step 2: A Registry Editor file with SAM and SYSTEM folder will open as shown in Figure 4.

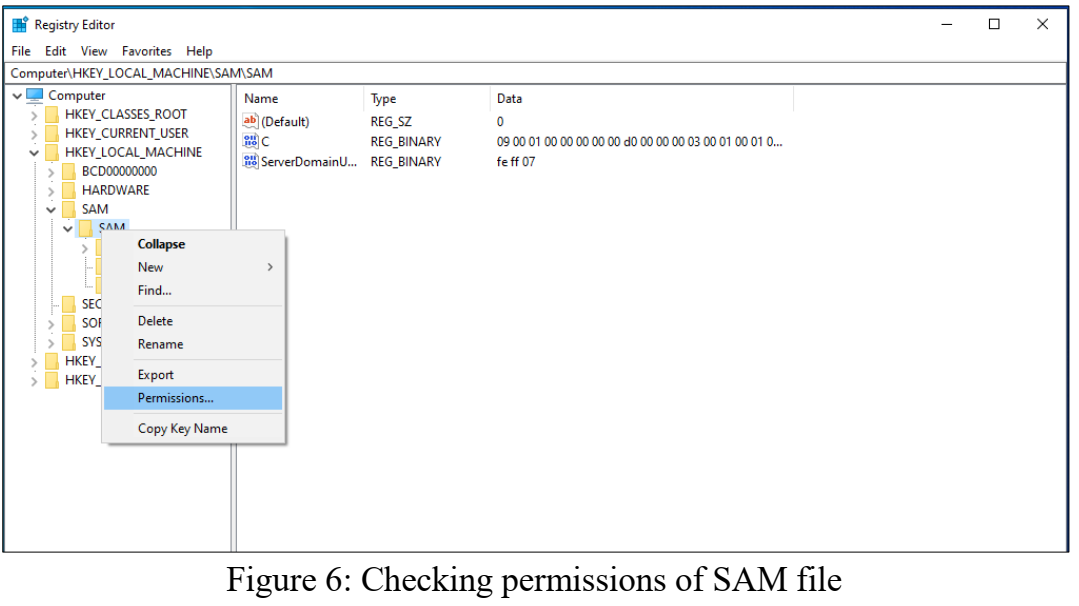
The SAM and SYSTEM files are located in : **“C:\Windows\System32\config”** path as shown in Figure 5.





**Step 3:**

These SAM and SYSTEM files can be accessed by registry editor after giving administrative permissions. Right click on the SAM file as shown in Figure 6. Then allow “Full Control” and “Read” by clicking the check box as shown in Figure 7.



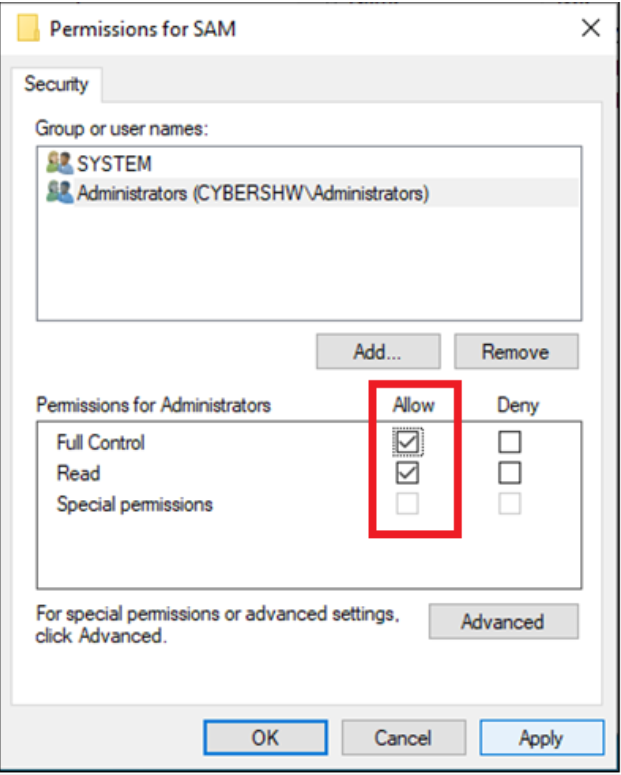


Figure 7: Giving permissions to the SAM file

**Step 4:**

Export the SAM file after giving the administrative permissions. Right click on the SAM file and click “Export” as shown in Figure 8. Save the file by giving file name as “SAM” and type as “Registry Hive Files” as shown in Figure 9.

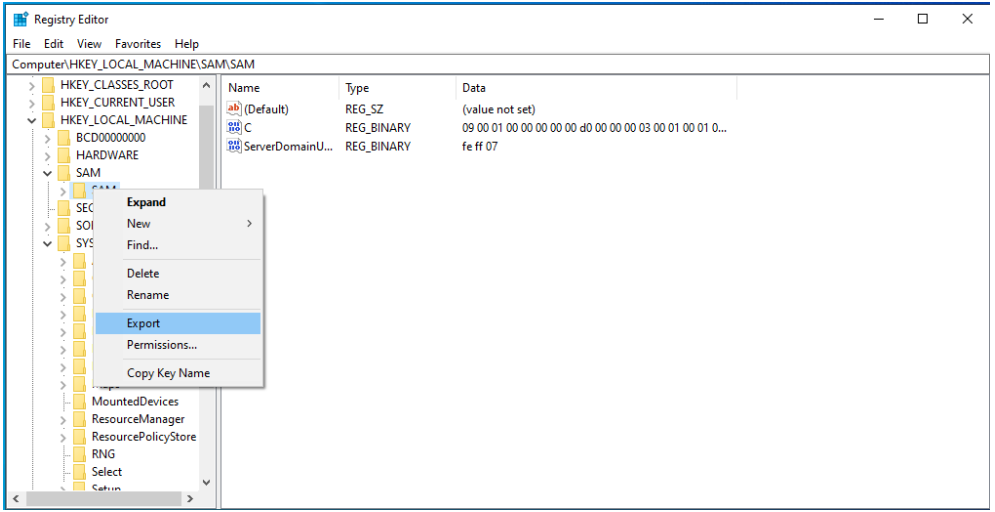


Figure 8: Exporting the SAM file

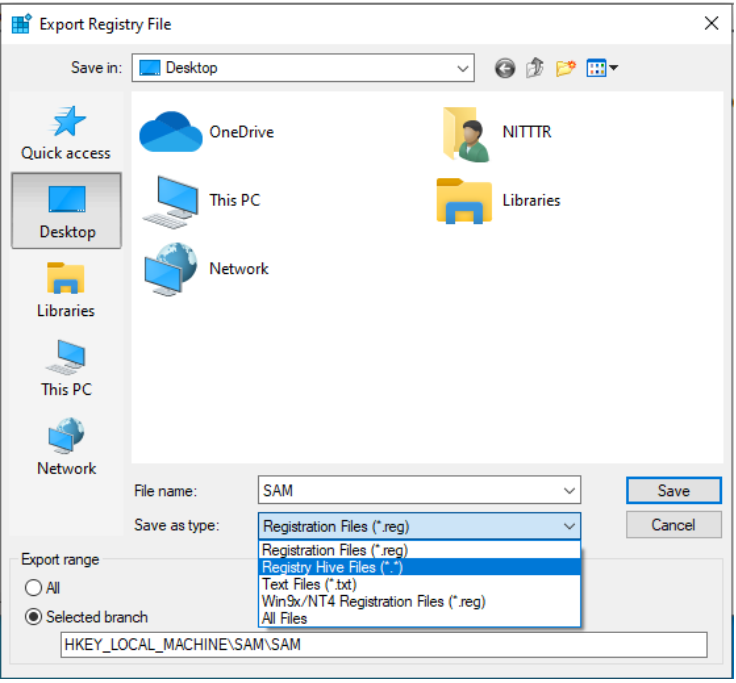


Figure 9: Saving the SAM file

**Step 5:**

In a similar fashion, right click on the SYSTEM file and give administrative permissions by allowing “Full Control” and “Read” after clicking the check box as shown in Figure 10.

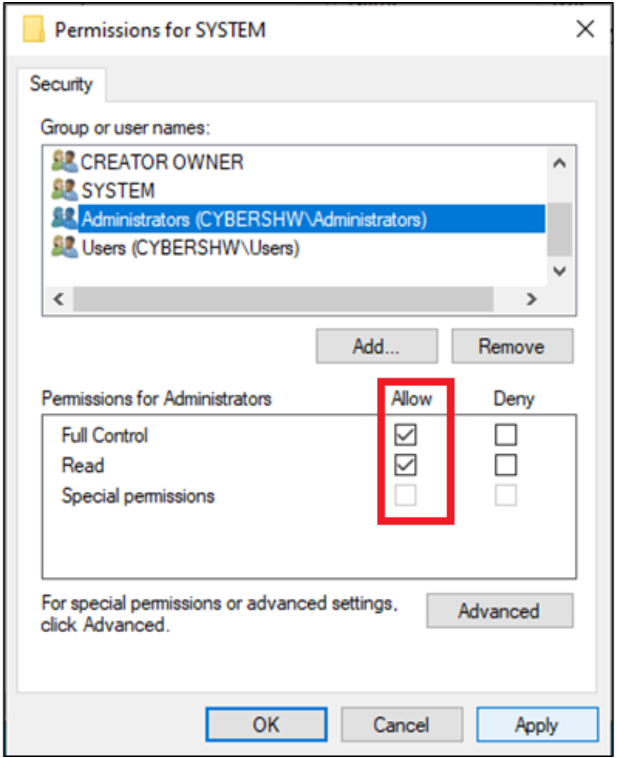


Figure 10: Giving permissions to the SYSTEM file

**Step 6:**

Export the SYSTEM file after giving the administrative permissions. Right click on SYSTEM file and click “Export” as shown in Figure 11. Save the file by giving file name as

“SYSTEM” and type as “Registry Hive Files” as shown in Figure 12.

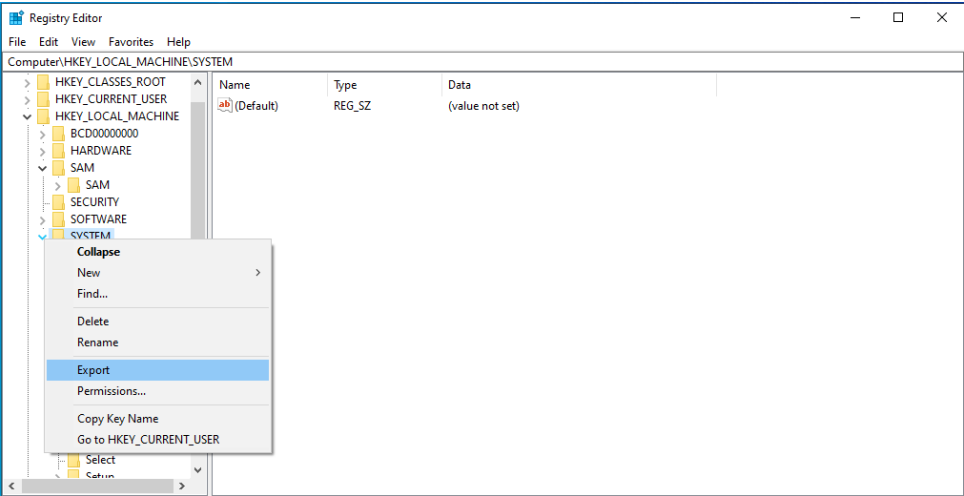


Figure 11: Exporting the SYSTEM file

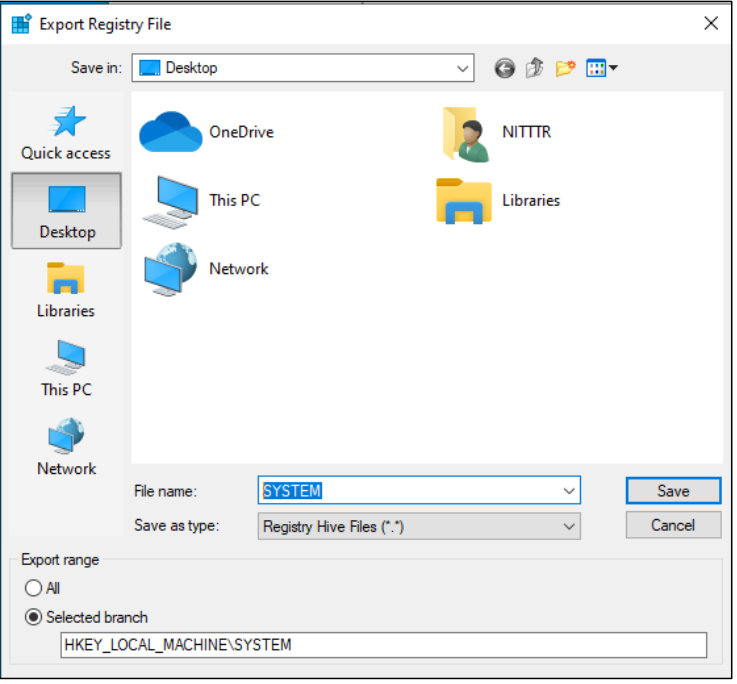


Figure 12: Saving the SYSTEM file

**Step 7:**

Download the “Mimikatz” tool by clicking the “mimikatz\_trunk.zip” file from GitHub website as shown in Figure 13 and Figure 14

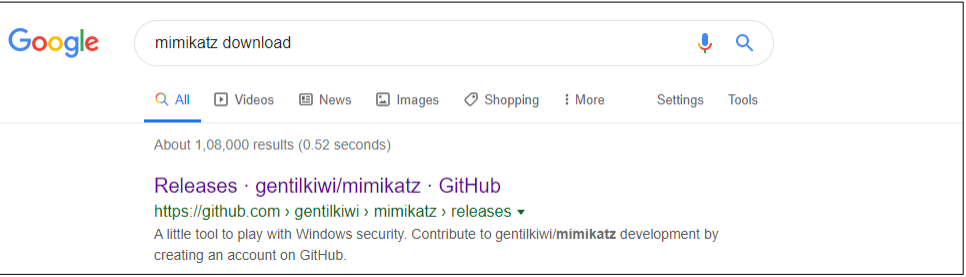


Figure 13: Search Mimikatz tool

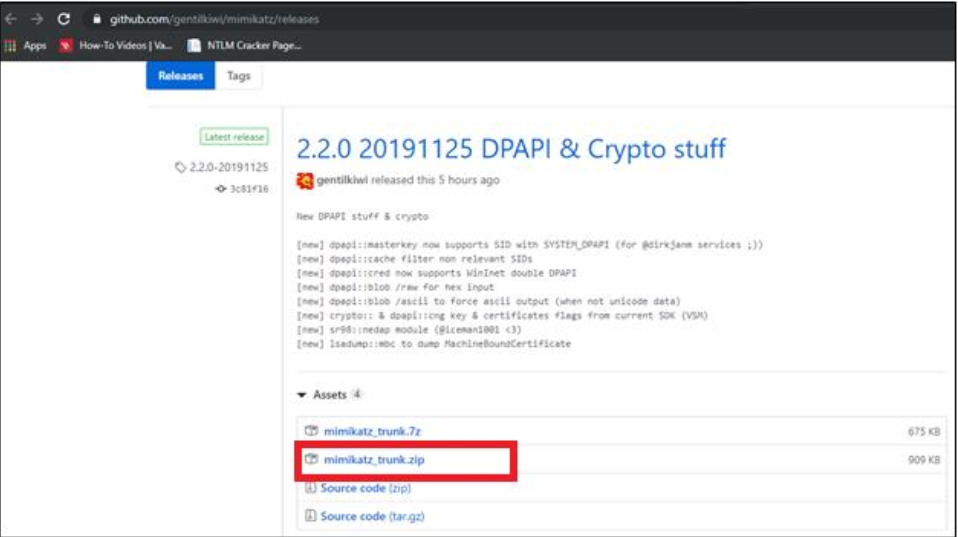


Figure 14: Download Mimikatz\_trunk file from GitHub

**Step 8:**

After downloading the file, unzip the“mimikatz\_trunk.zip” file. Now go to:

“C:/Downloads/mimikatz\_trunk/x64/mimikatz” and left click twice on mimikatz file as shown in Figure 15.

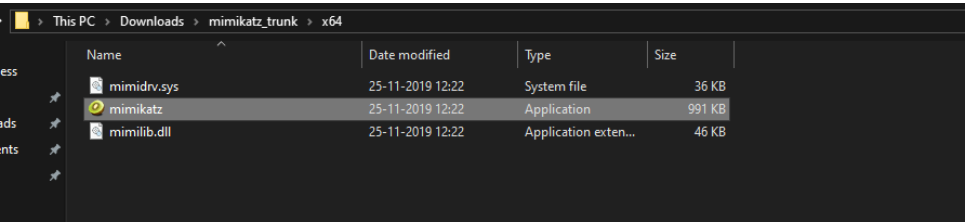


Figure 15: Downloaded file of mimikatz\_trunk

**Step 9:**

A command line prompt of Mimikatz tool will open as shown in Figure 16.

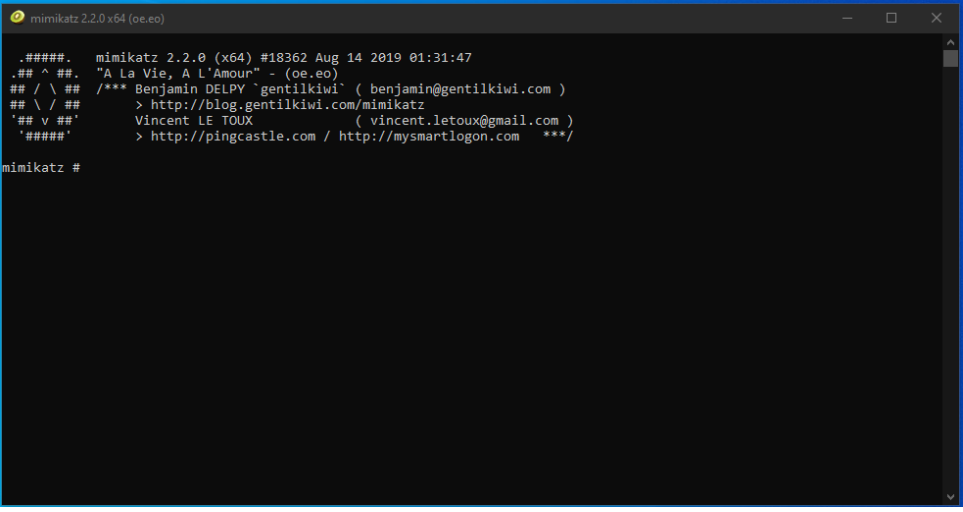


Figure 16: Mimikatz command line

**Step 11:**

Type “lsadump::sam /system:C:\Users\NITTTR\Desktop\SYSTEM /SAM:C:\Users\NITTTR\Desktop\SAM” command in command line prompt of Mimikatz tool. Press Enter.

The command will show NTLM hash password of Windows operating system as shown in Figure 17

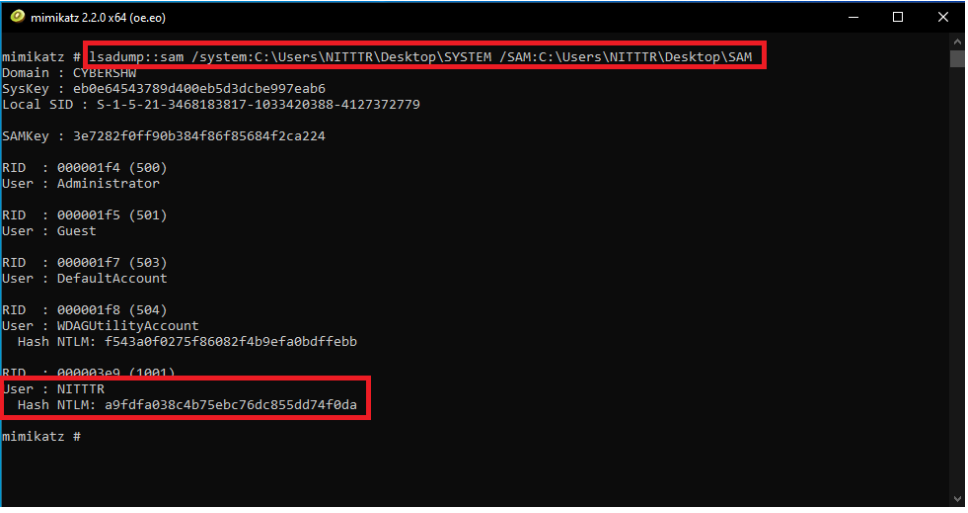


Figure 17: Typing the command and getting NTLM hash

**Step 12**

Open Kali Linux operating system as shown in Figure 18.

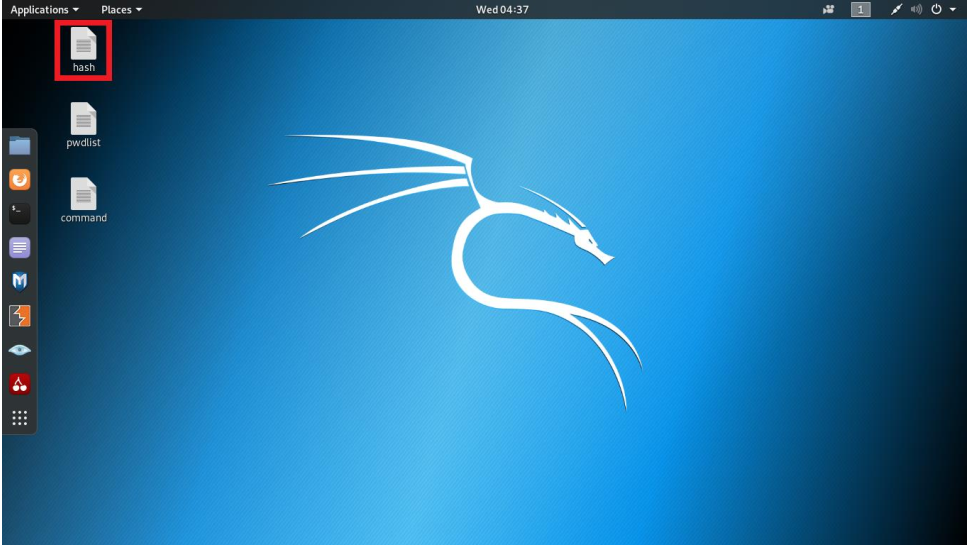


Figure 18: Kali Linux operating system

**Step 13:**

Copy the NTLM hash (recovered with Mimikatz tool, refer Figure 17) and store it in a file on Desktop as shown in Figure 19. Also, multiple NTLM hash can be stored in a file to get plaintext as shown in Figure 20.

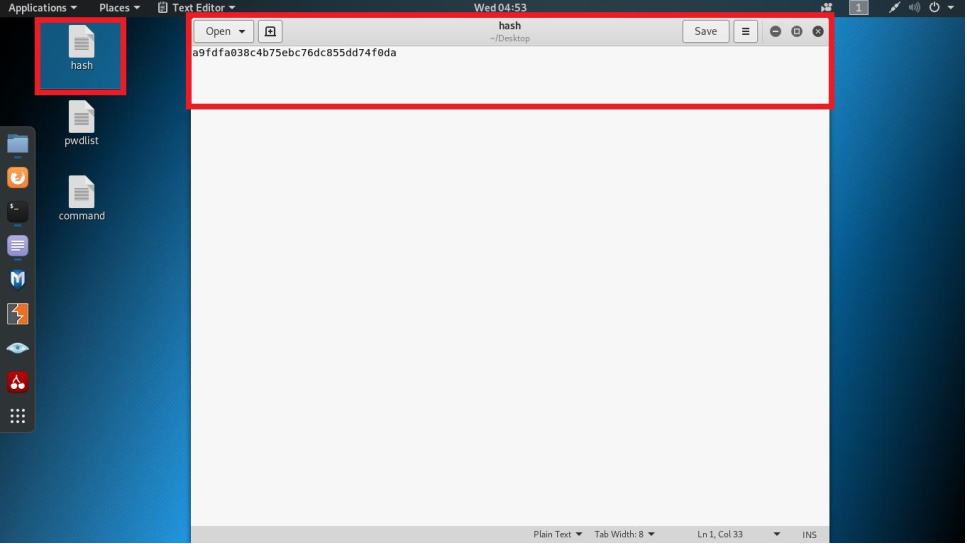


Figure 19: NTLM hash in a file

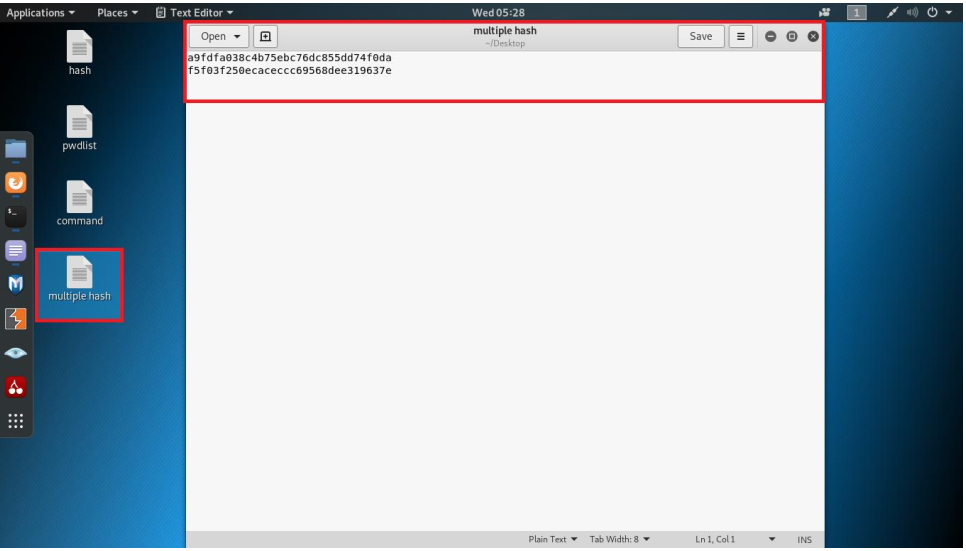


Figure 20: Multiple NTLM hash in a file

**Step 14:**

Search the password wordlist by browsing Google search engine as shown in Figure 21. Open the GitHub website and download the ZIP file as shown in Figure 22.

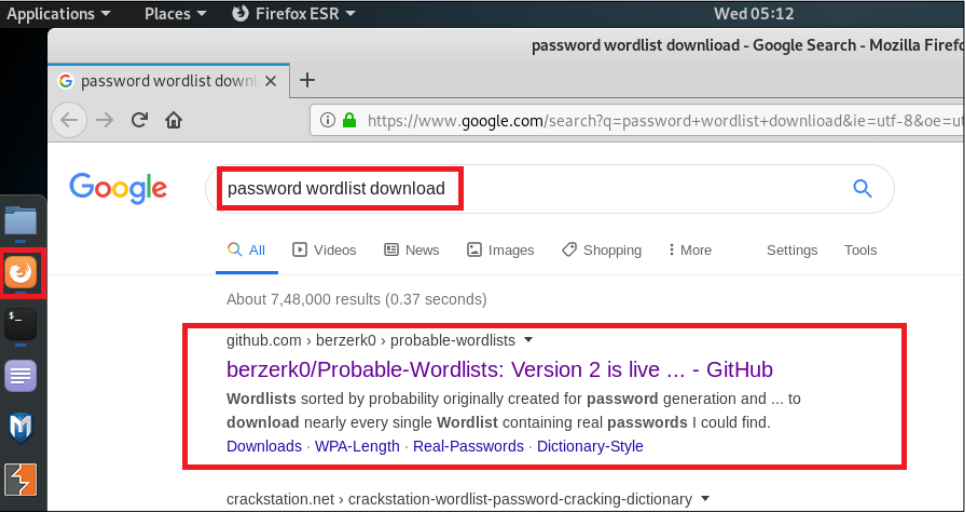


Figure 21: Search password wordlist

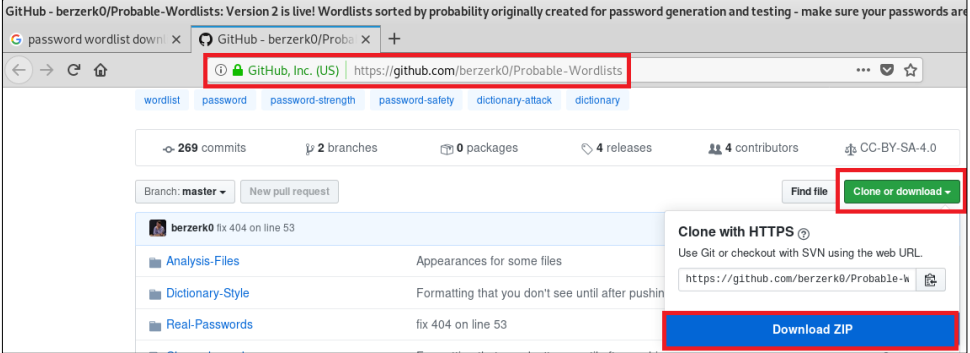


Figure 22: Download password wordlist

**Step 15:**

Save and open the downloaded file as shown in Figure 23. Open the “Real-Passwords” folder to see the passwords wordlist as shown in Figure 24

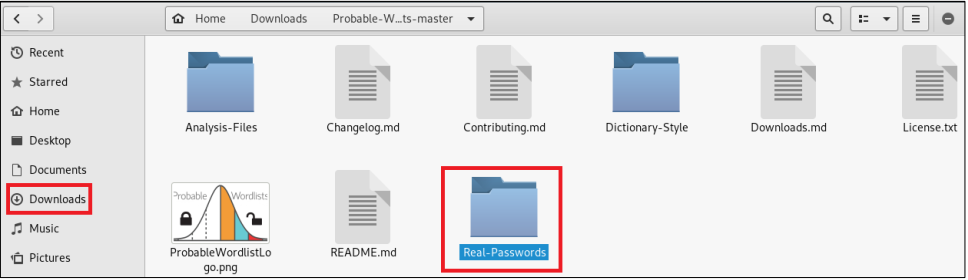


Figure 23: Password folder in downloaded file

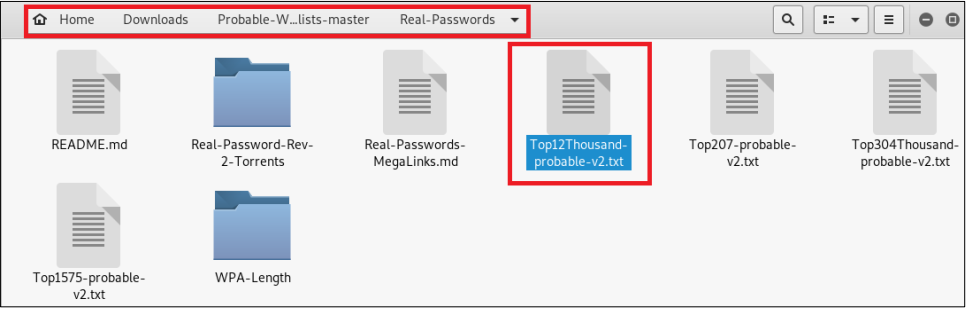


Figure 24: Password wordlist

**Step 16:**

Open any password wordlist (e.g., Top12Thousandprobable-v2.txt file) as shown in Figure 25. Copy the wordlist file on Desktop and rename as “pwdlist” as shown in Figure 26.

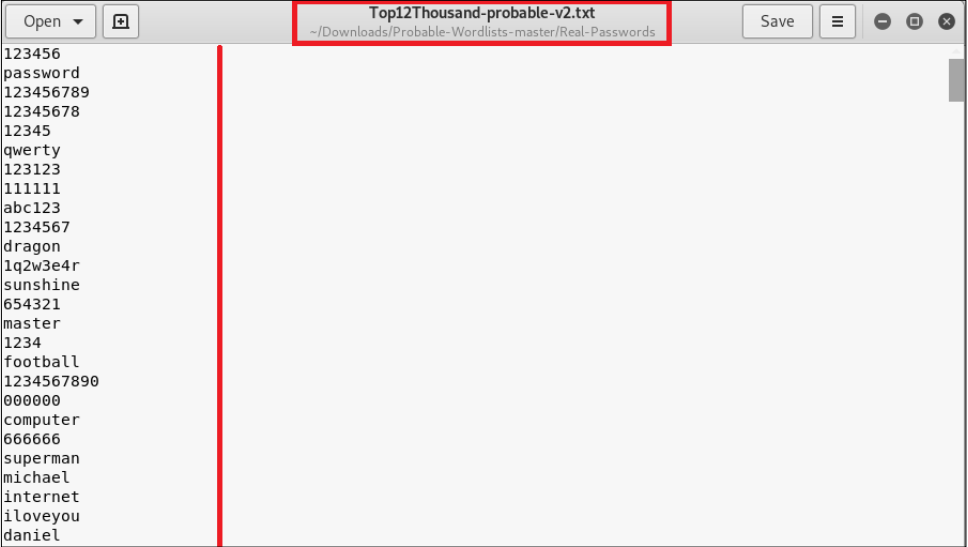


Figure 25: Top 12 thousand most frequently used passwords

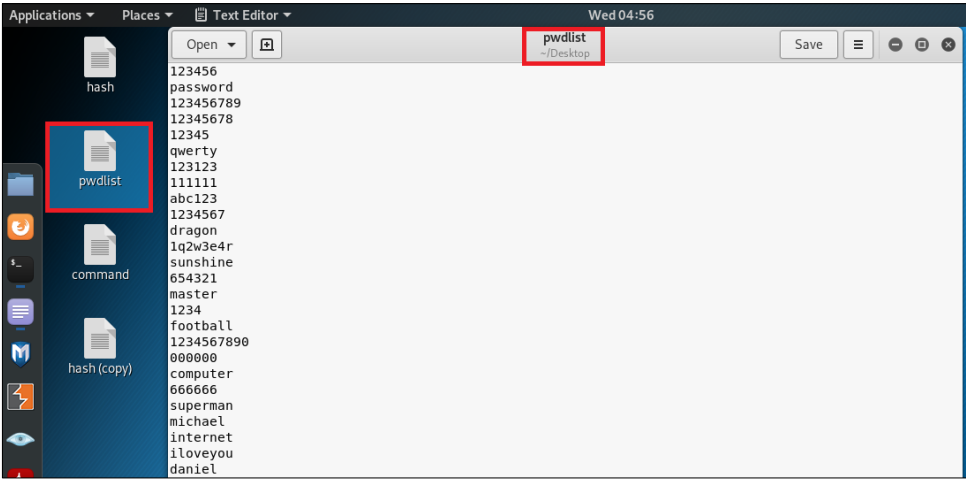


Figure 26: Copy the wordlist file on Desktop

**Step 17:**

In Kali Linux operating system, open the hashcat tool. Go to Applications-> Password attacks-> hashcat as shown in Figure 27.

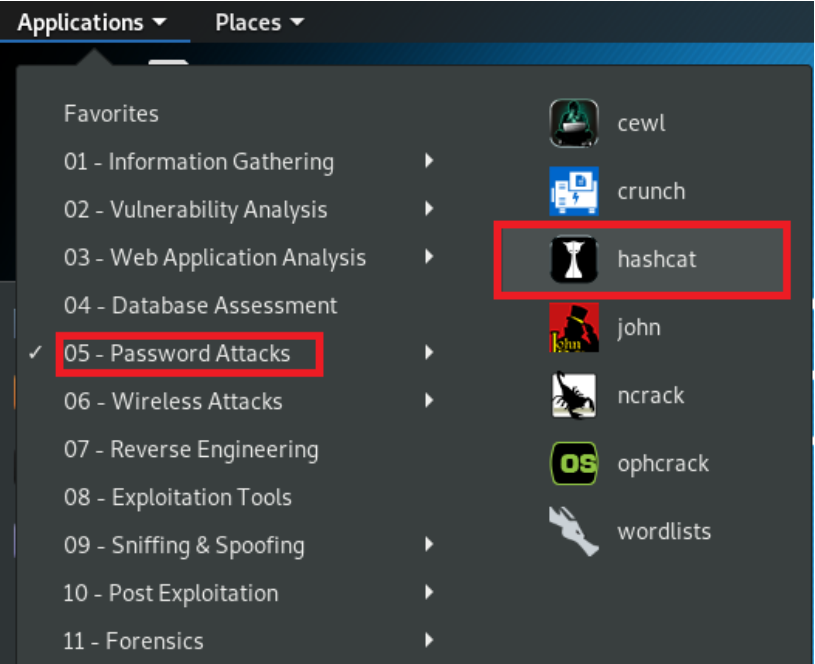


Figure 27: Opening hashcat tool

**Step 18:**

A terminal with usage of hashcat tool will open as shown in Figure 28. The tool states various hash modes which can be recovered as shown in Figure 29 and Figure 30.

The NTLM hash has ID of 1000 as shown in Figure 29. The tool also shows various attack modes as shown in Figure 30.

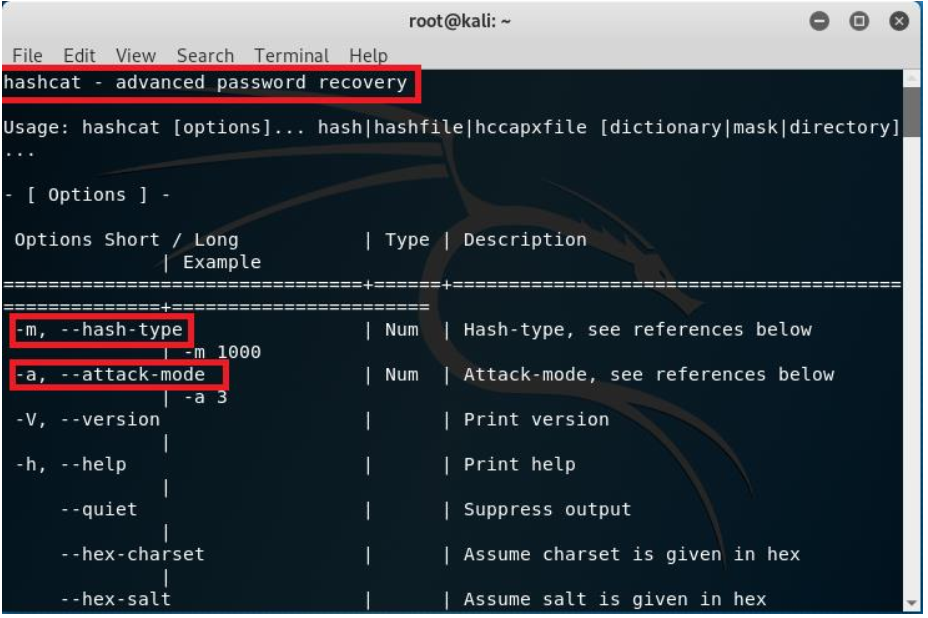


Figure 28: Hashcat terminal

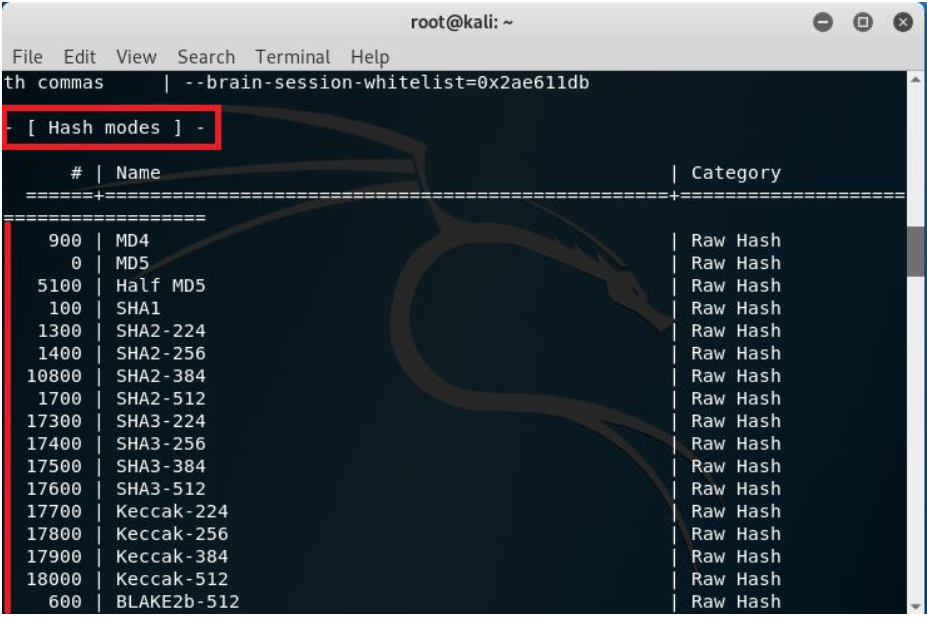


Figure 29: Hash modes



Figure 30: Hash modes displaying NTLM hash

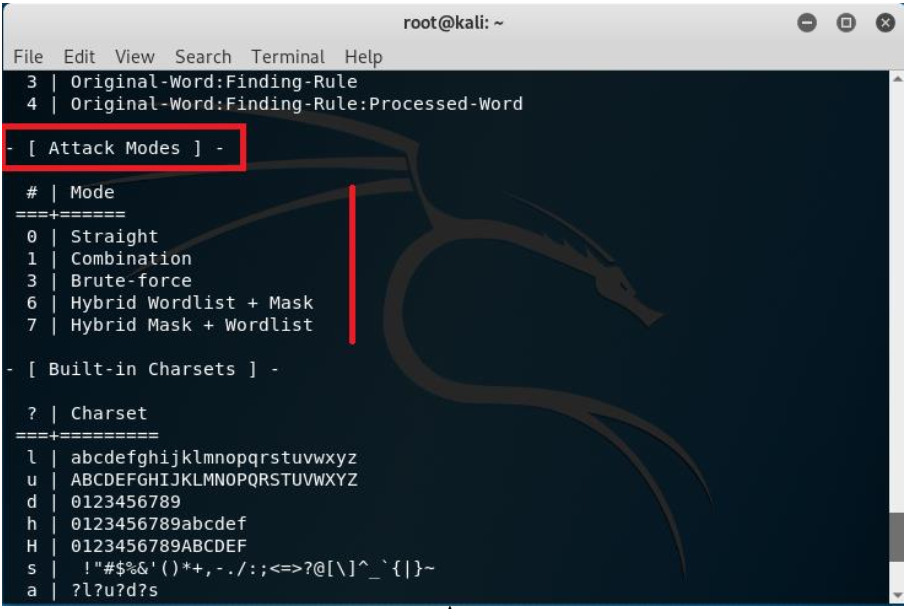


Figure 31: Attack modes

**Step 19:**

The basic examples regarding the usage of hashcat tool is shown in Figure 32.

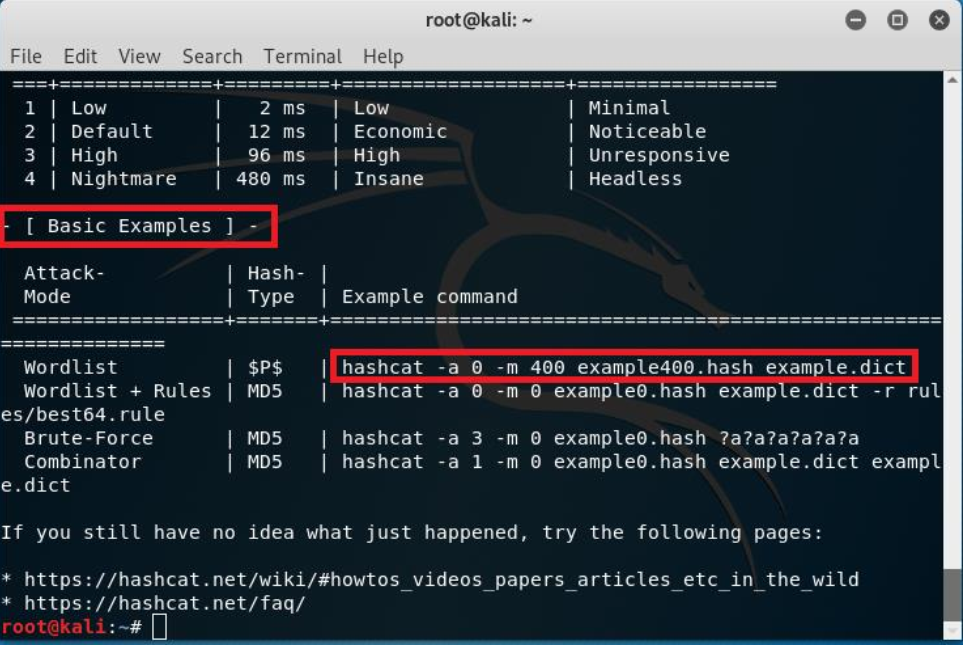


Figure 32: Example of hashcat

**Step 20:**

Write the command “hashcat –m 1000 –a 0 /root/Desktop/hash /root/Desktop/pwdlist --force” to recover the hash and “hashcat –m 1000 –a 0 /root/Desktop/hash /root/Desktop/pwdlist --force --show” to display the plaintext of NTLM hash as shown in Figure 33.

In this command, -m stands for hash mode (e.g., 1000 stands for NTLM hash, refer Figure 30) and -a stands for attack mode (e.g., 0 stands for straight attack, refer Figure 31). The26 path to the hash file and wordlist file is also given in the

command. The plaintext of the NTLM hash is displayed in the Figure 33 and highlighted in red rectangular box. The plaintext of the NTLM hash is “password123”.

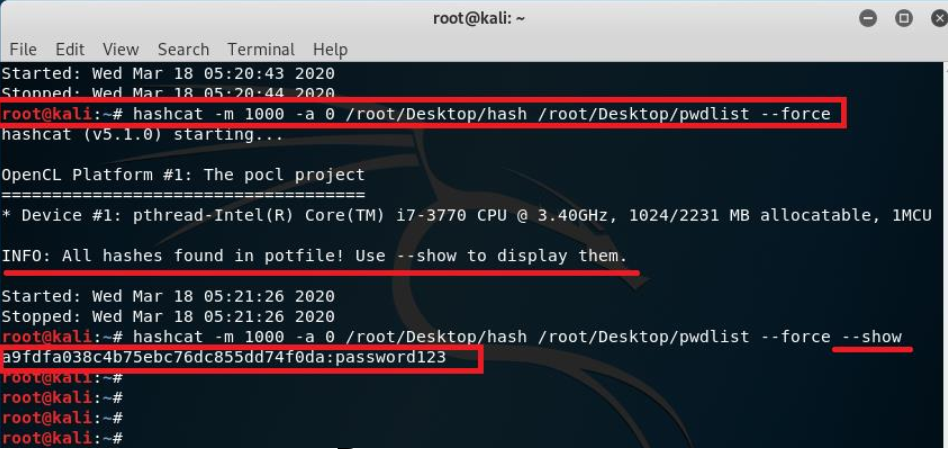


Figure 33: Recover plaintext of NTLM hash

**Step 21:**

Similarly, hashcat can recover plaintext of multiple hash file. Write the command “*hashcat –m 1000 –a 0 /root/Desktop/multiplehash /root/Desktop/pwdlist --force*” to recover the hash and “*hashcat –m 1000 –a 0 /root/Desktop/multiplehash /root/Desktop/pwdlist --force -- show*” to display the plaintext of multiple NTLM hash as shown in Figure 34.

The plaintext of the multiple NTLM hash is displayed in the Figure 34 and highlighted in red rectangular box. The 27 plaintext of the NTLM hash is “shweta123” and “password123” respectively.

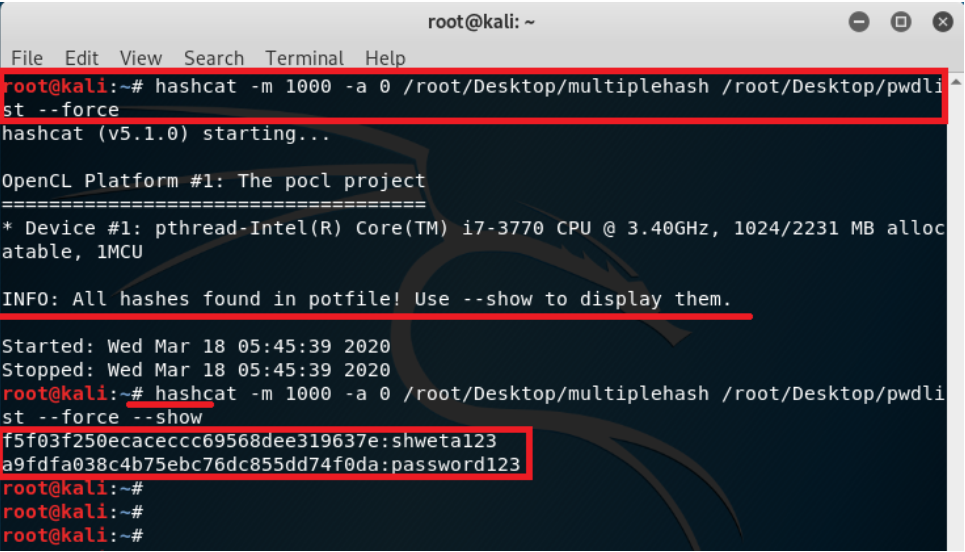


Figure 34: Recover plaintext of multiple NTLM hash

**Done lab.!**

**YOU MUST SUBMIT A FULL-SCREEN IMAGE FOR FULL CREDIT!**

Save the document with the filename "**YOUR NAME Lab 9.pdf**", replacing "YOUR NAME" with your real name.

Email the image to the instructor as an attachment to an e-mail message. Send it to: **xxx@fe.edu.vn** with a subject line of "**Lab 9 From YOUR NAME**", replacing "YOUR NAME" with your real name.