

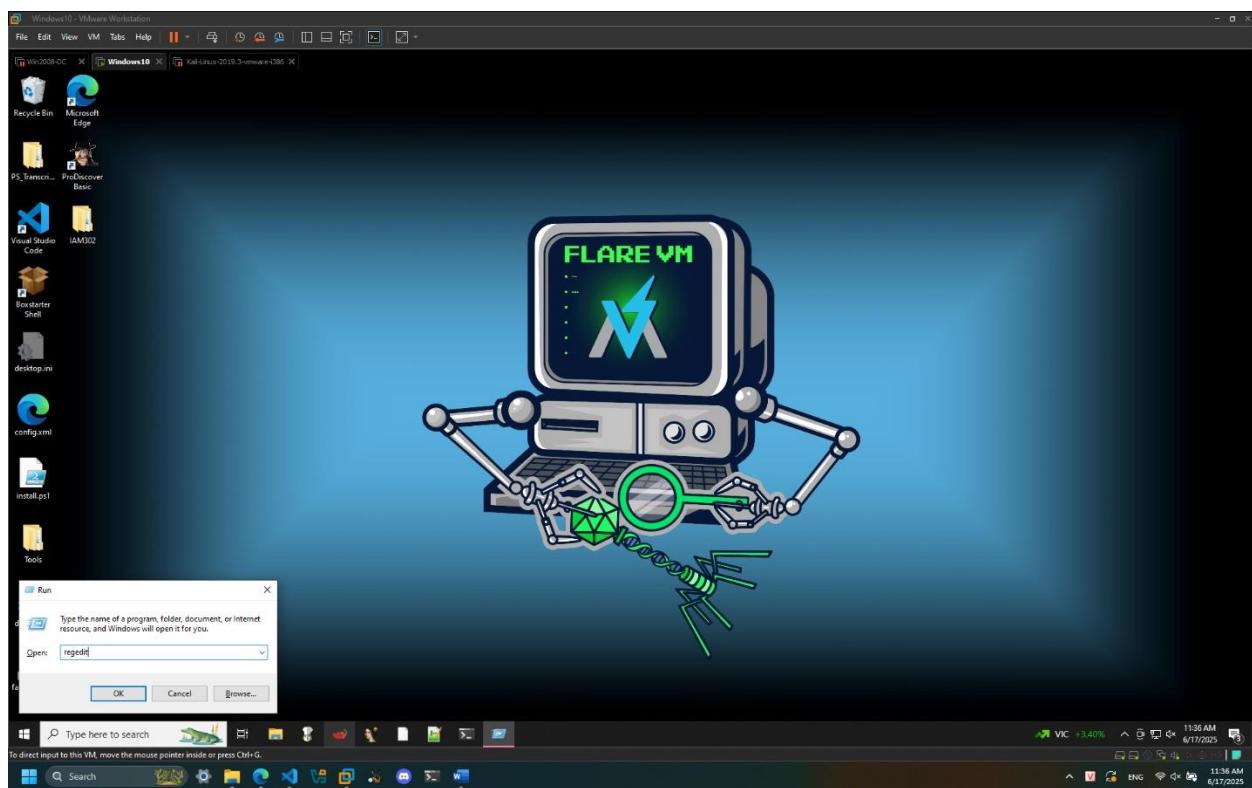
Họ và tên: Trần Trí Dũng

Mã số sinh viên: HE190680

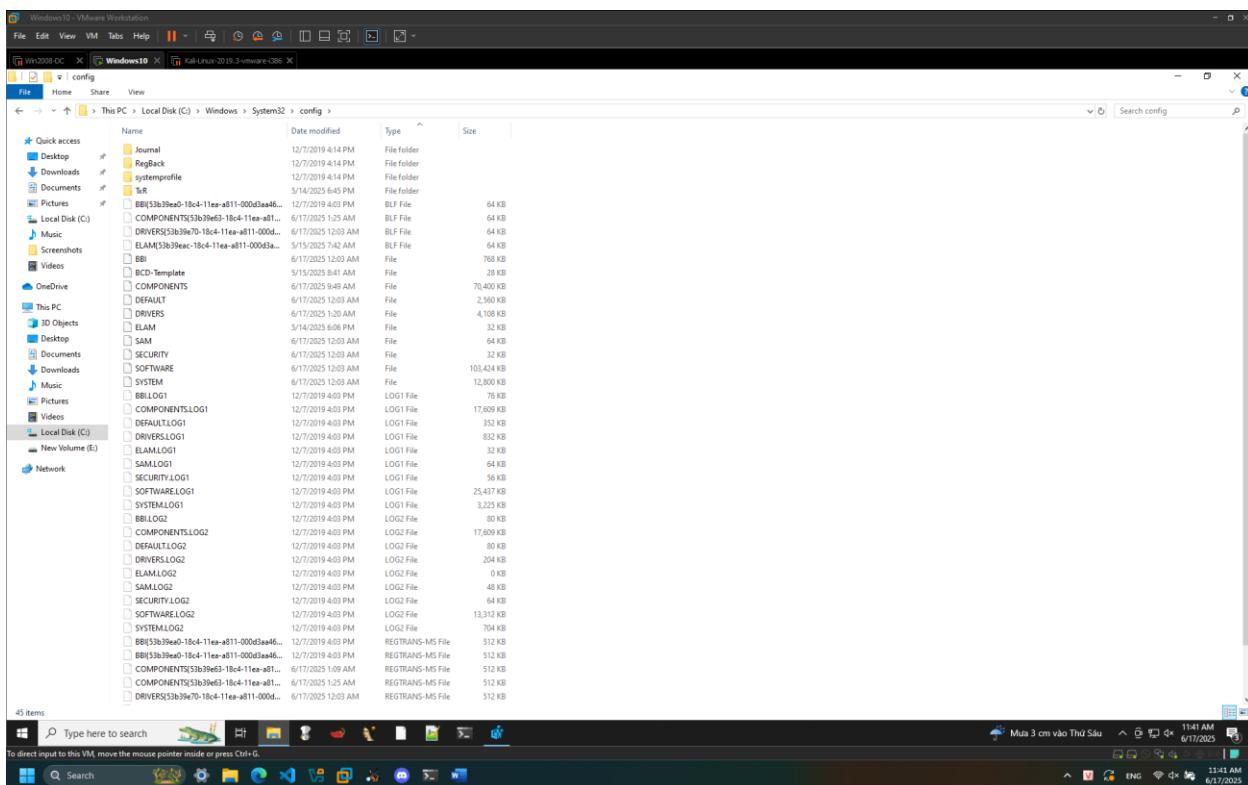
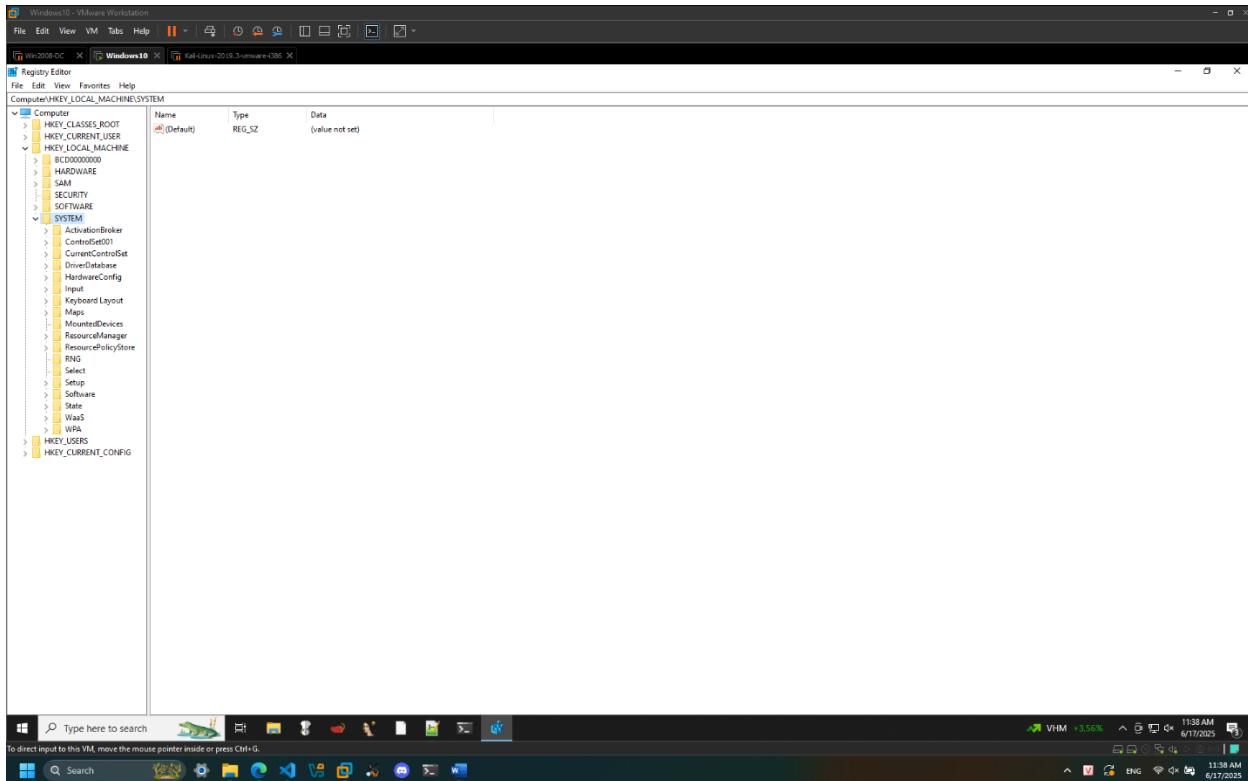
Lớp: IA1901

Lab 9: Password Cracking of Windows Operating System.

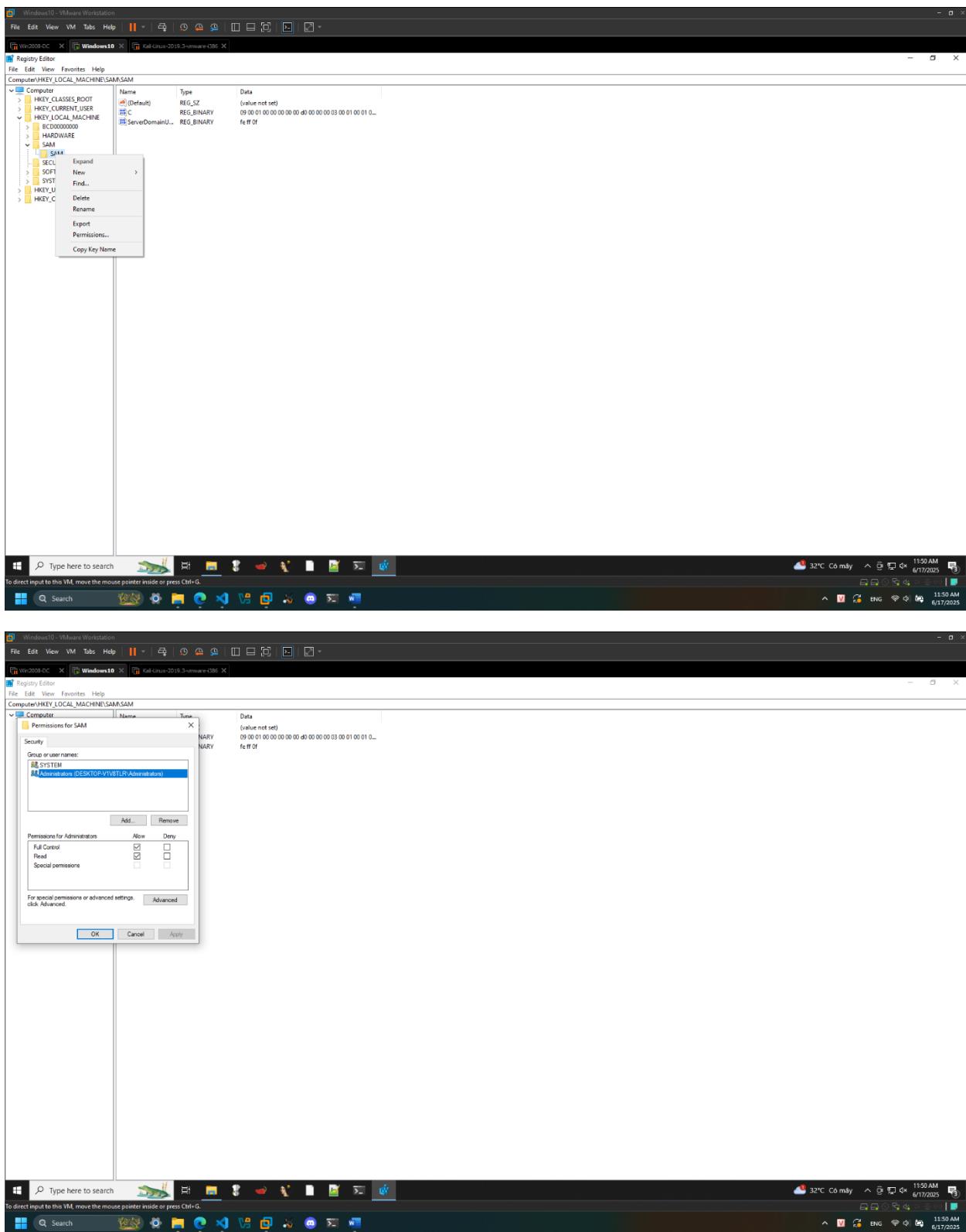
Step 1:



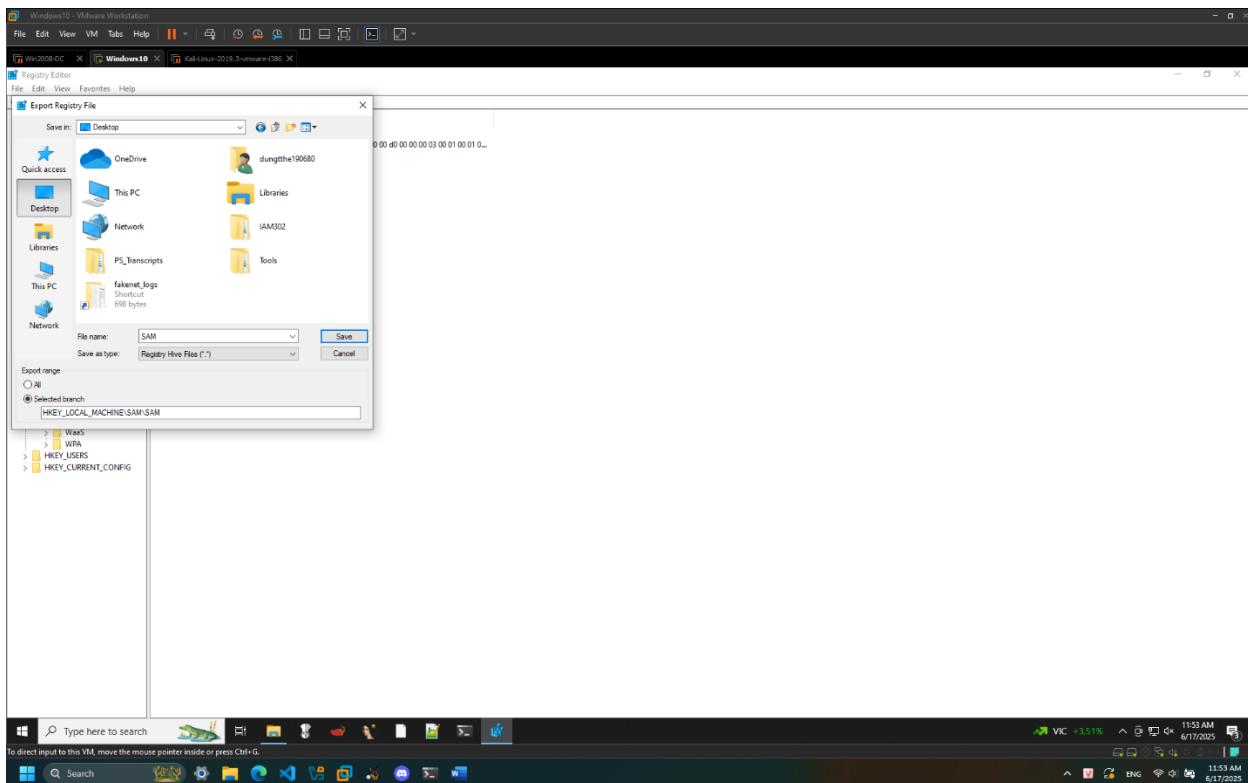
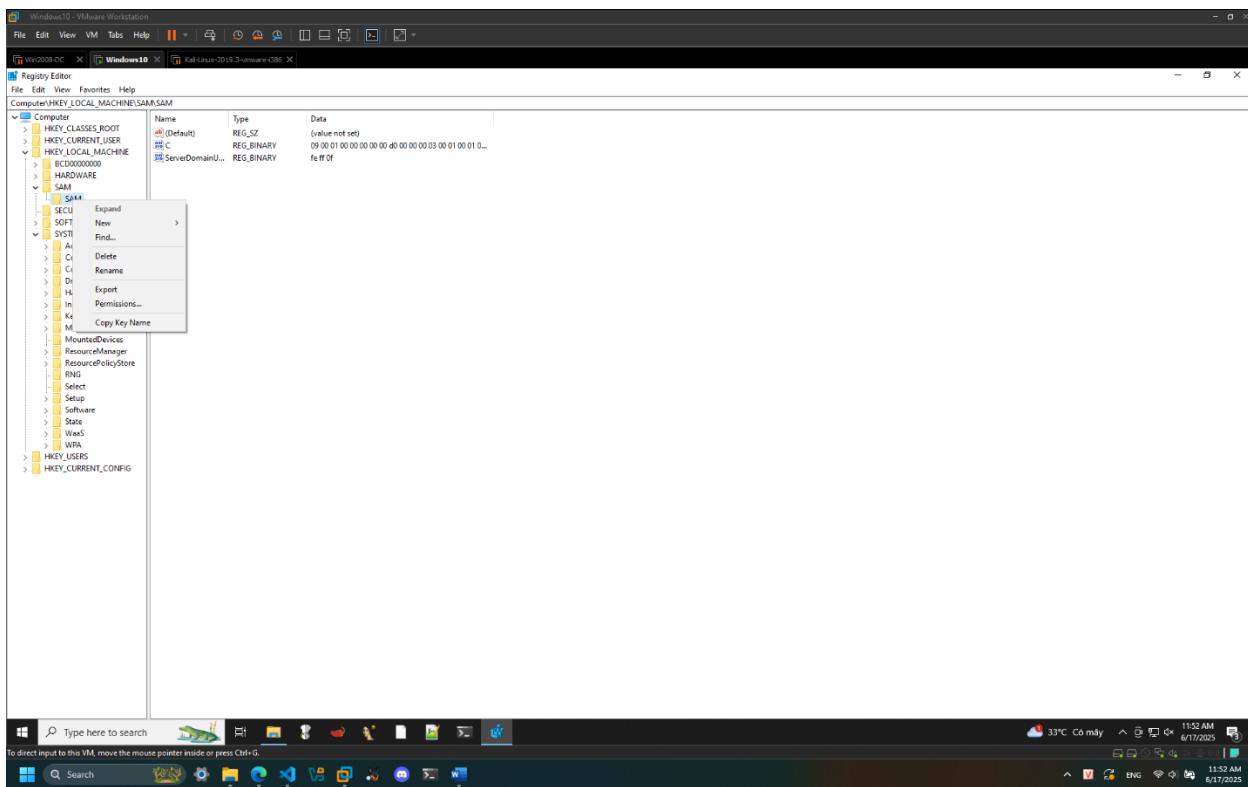
Step 2:



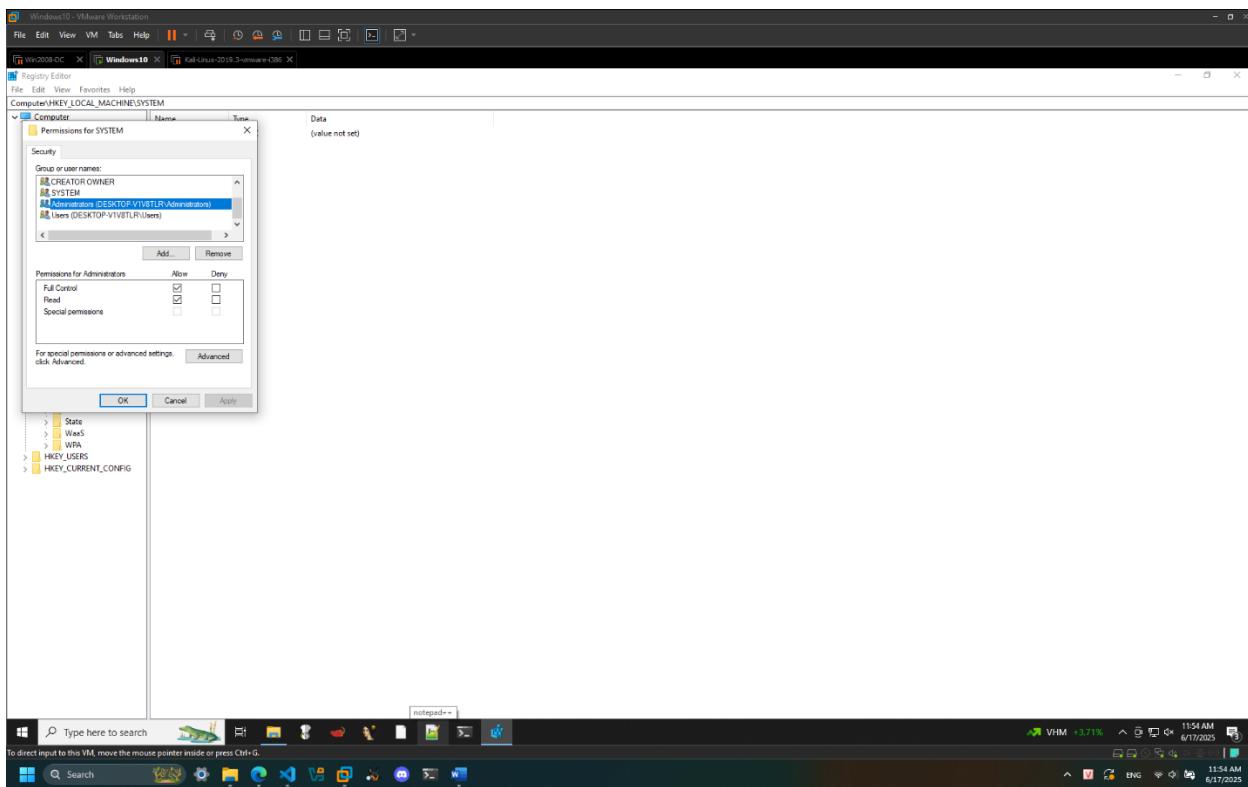
Step 3:



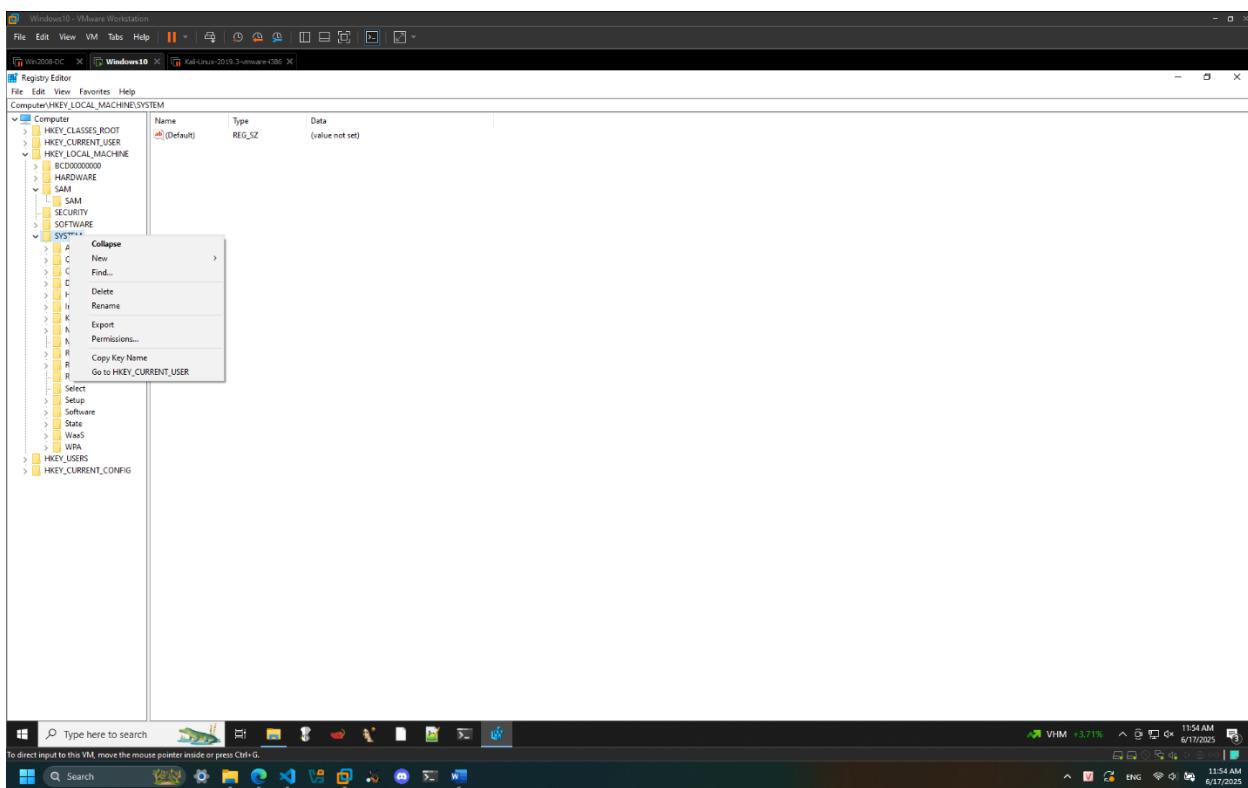
Step 4:

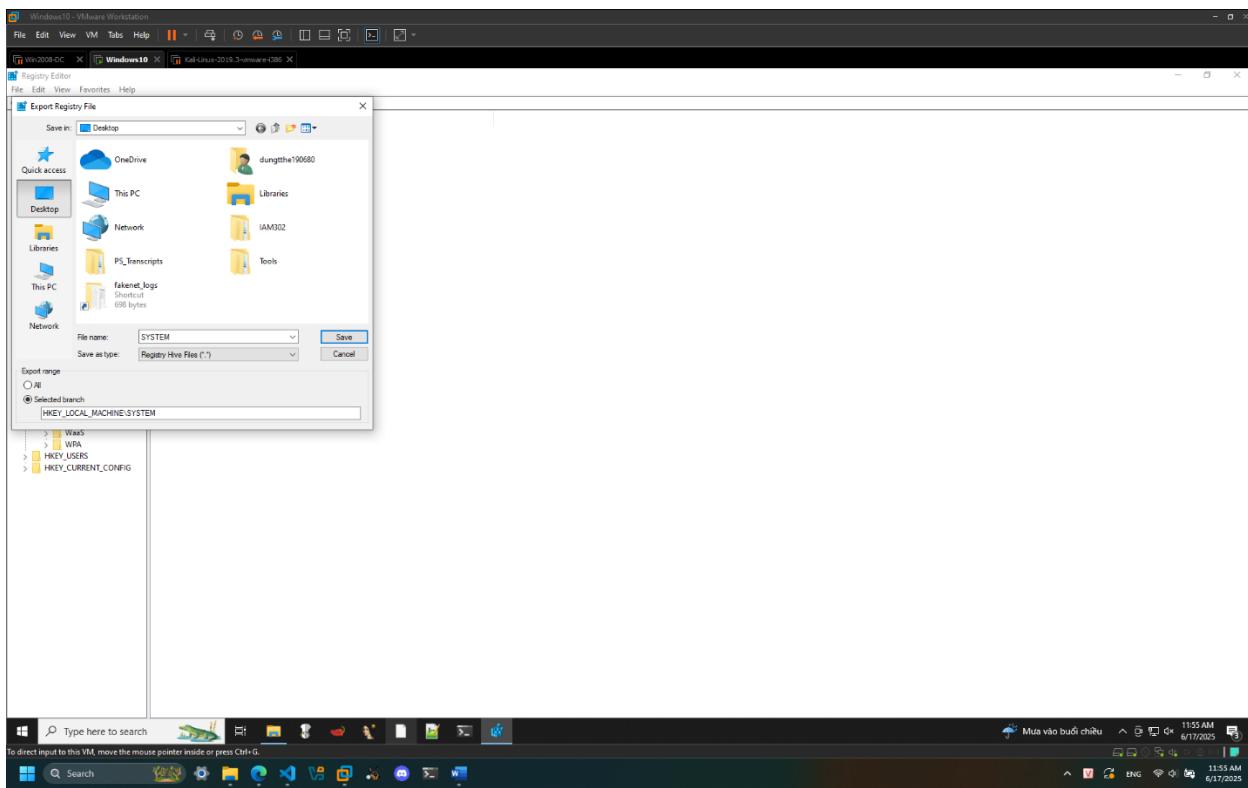


Step 5:

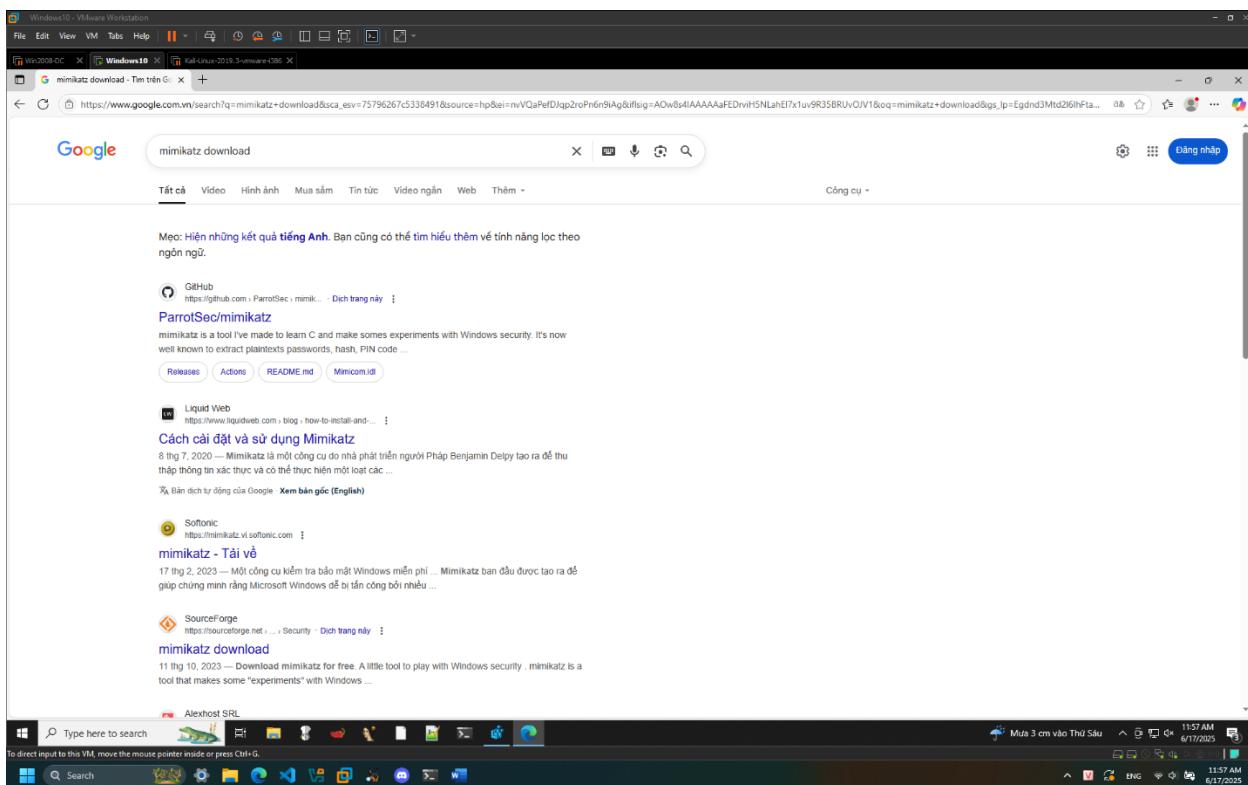


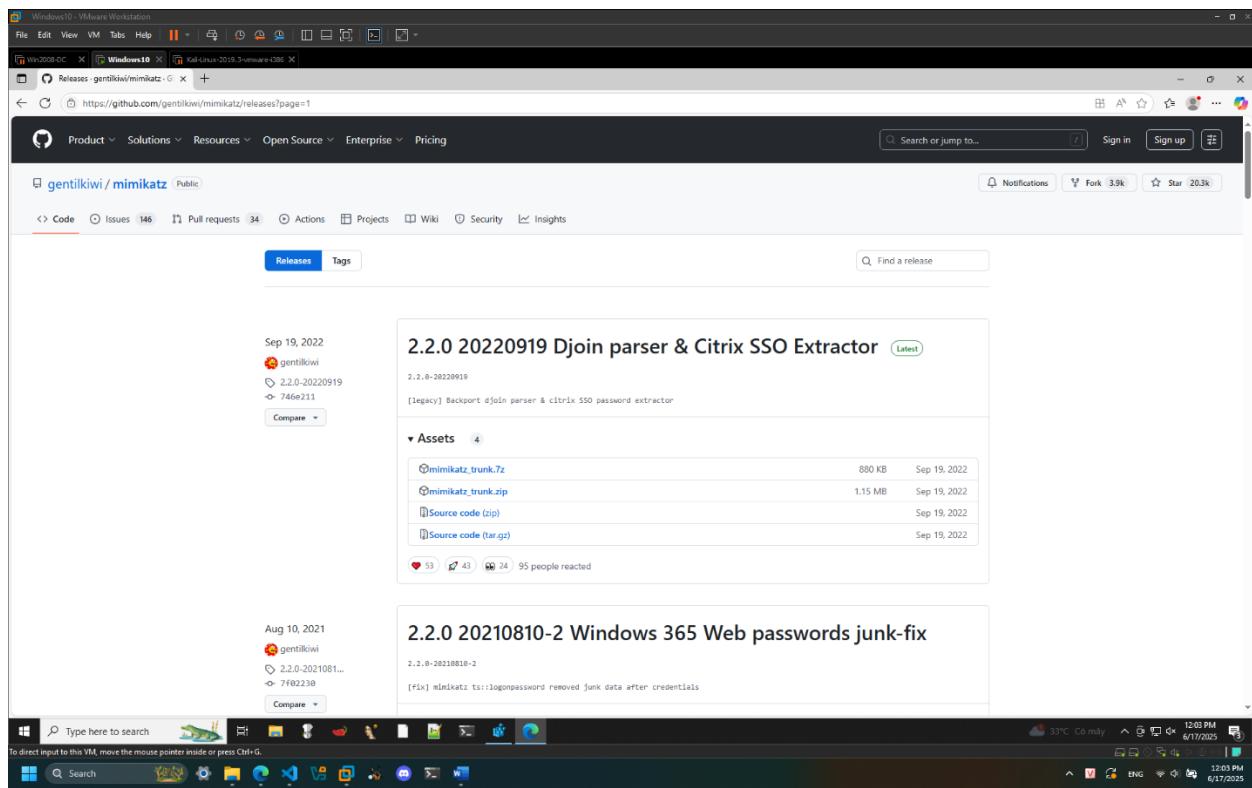
Step 6:



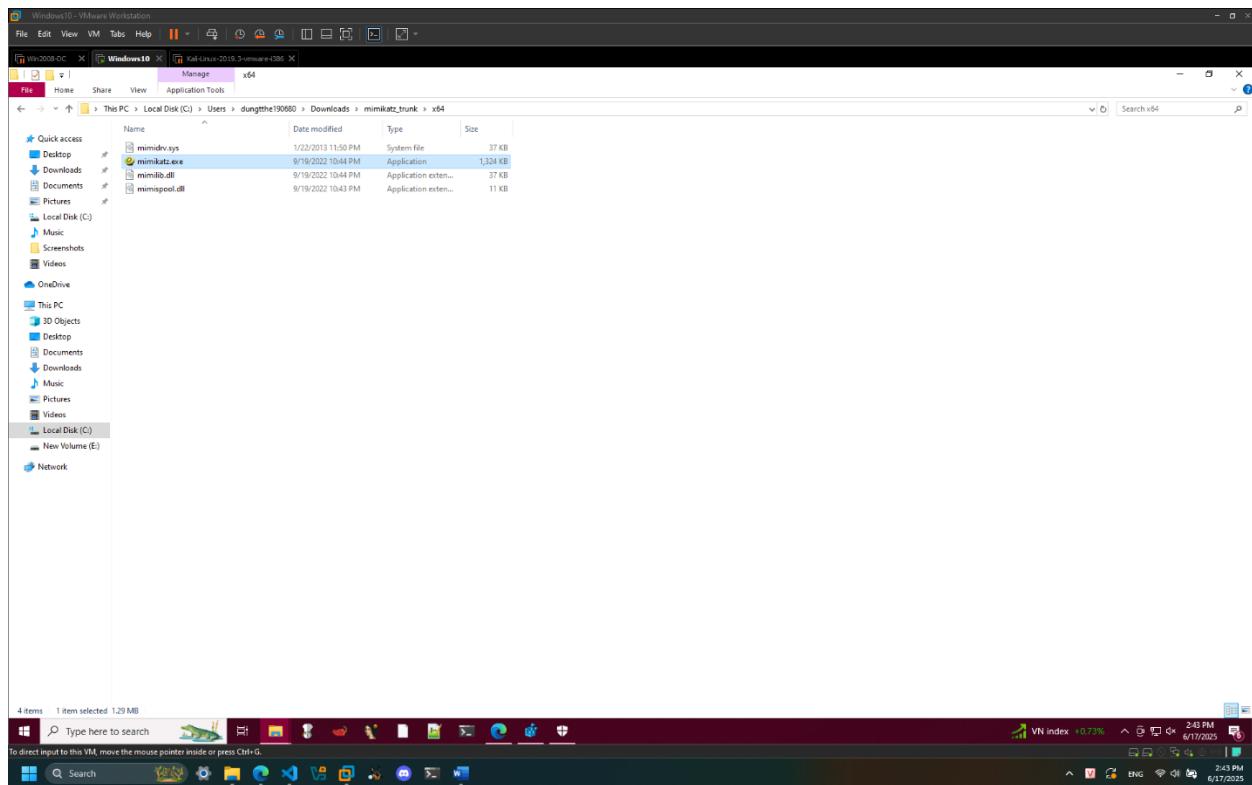


Step 7:

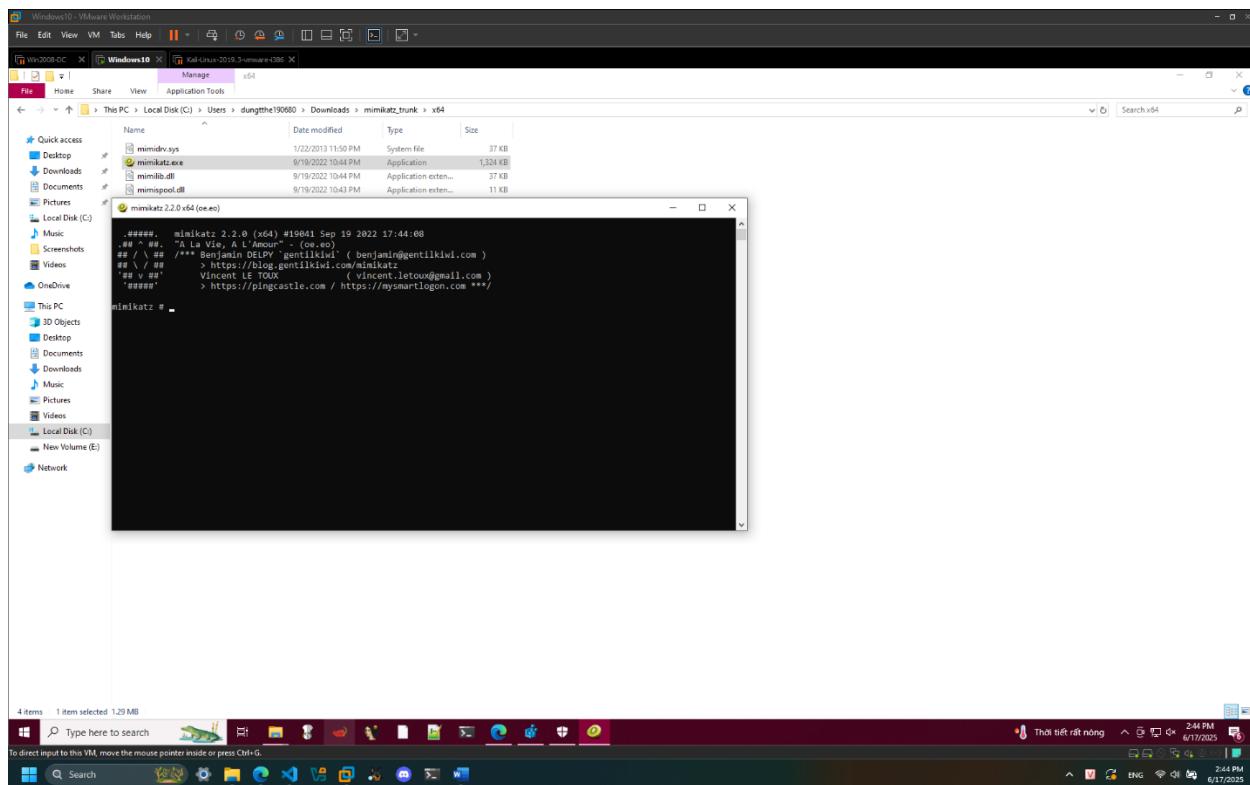




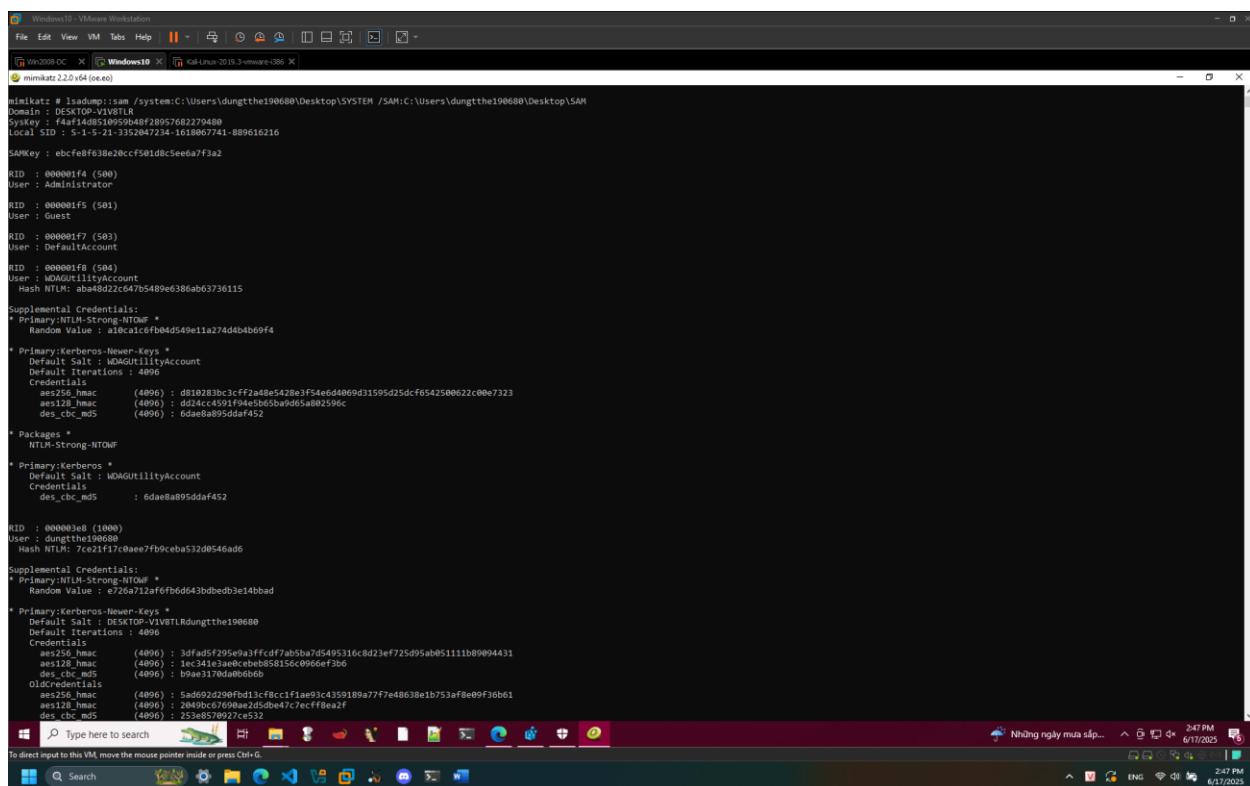
Step 8:



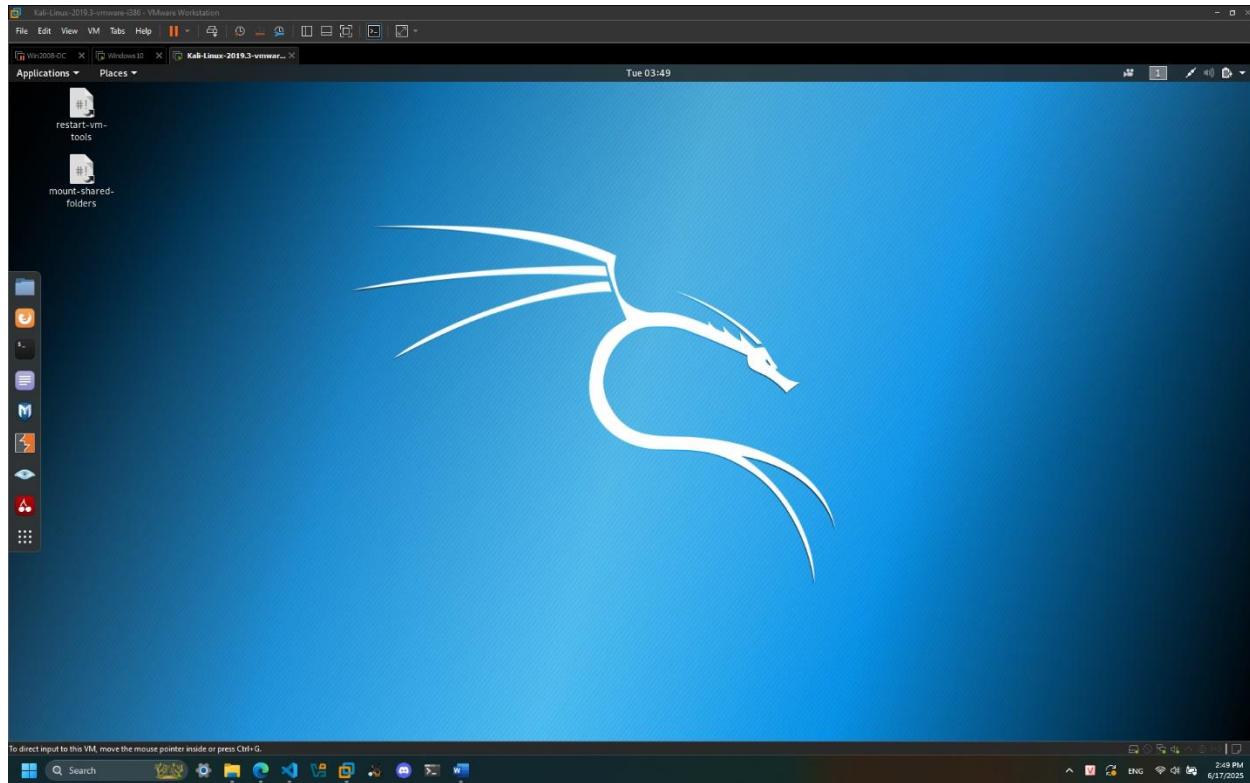
Step 9:



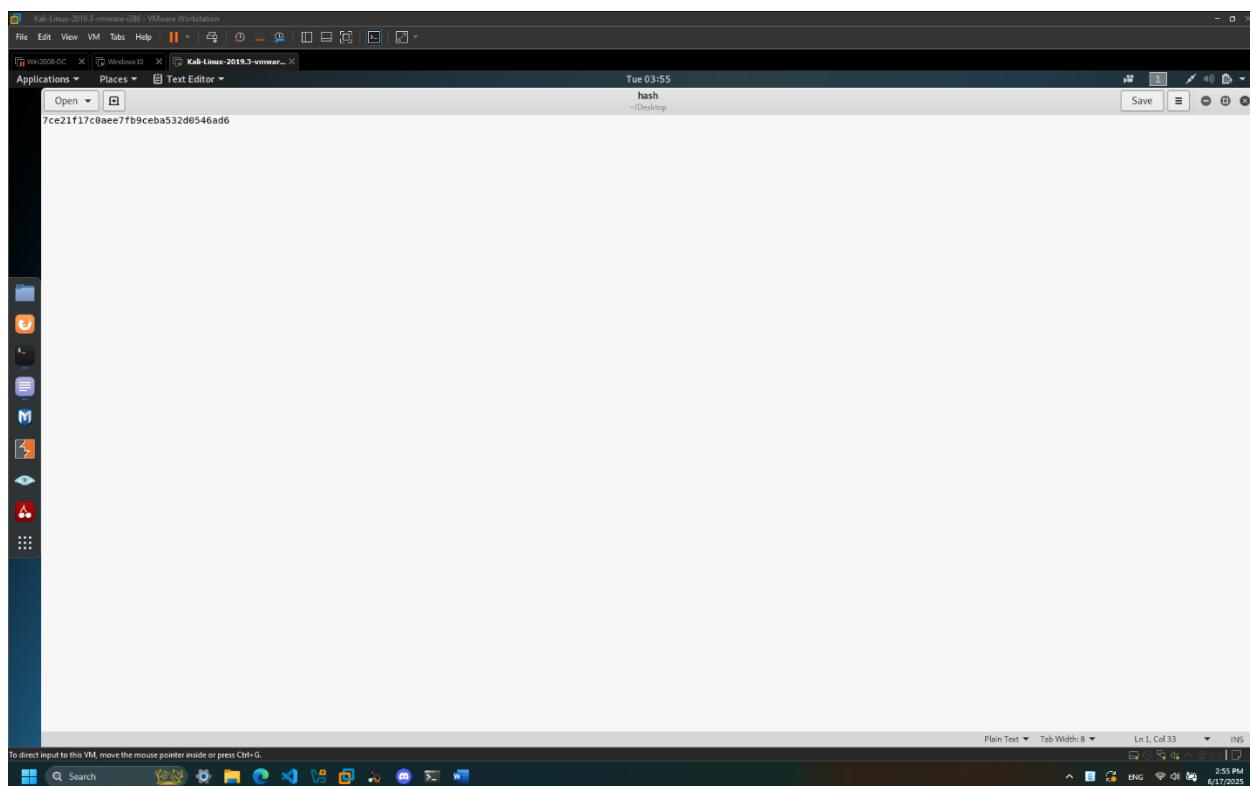
Step 11:

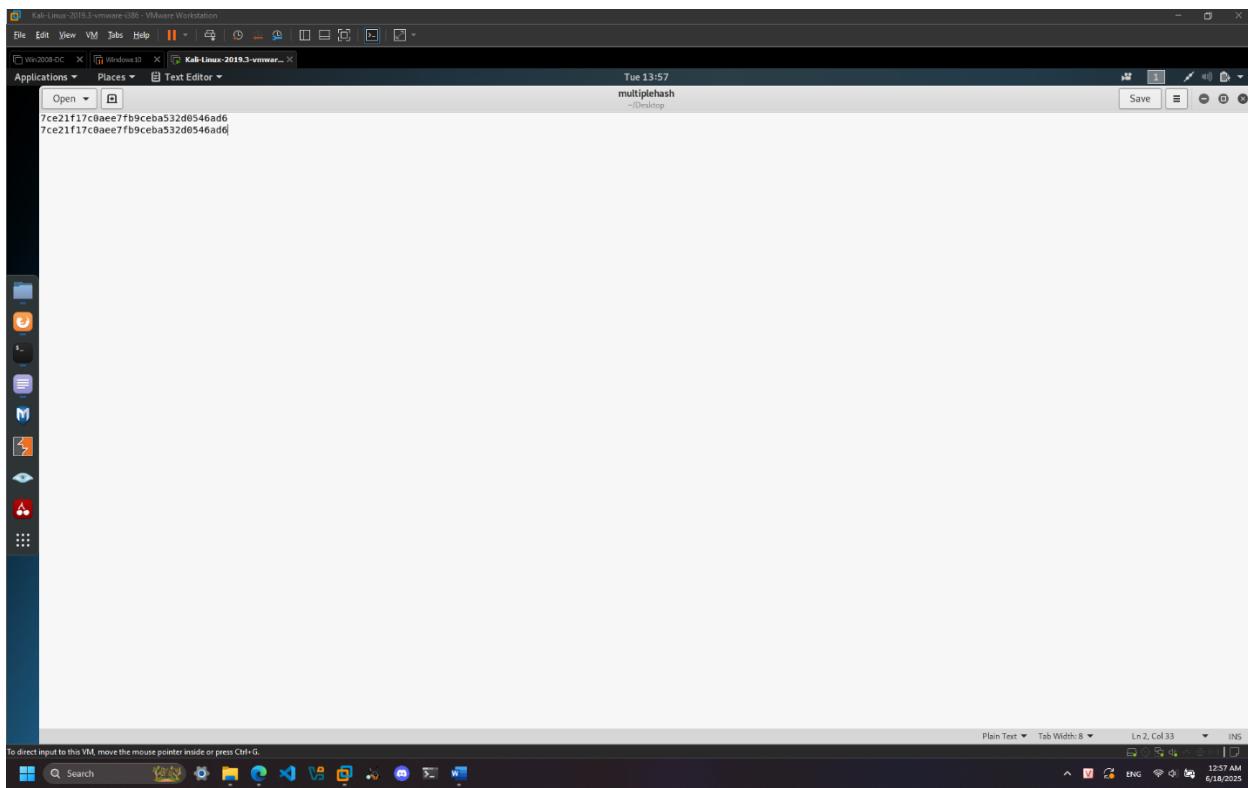


Step 12:

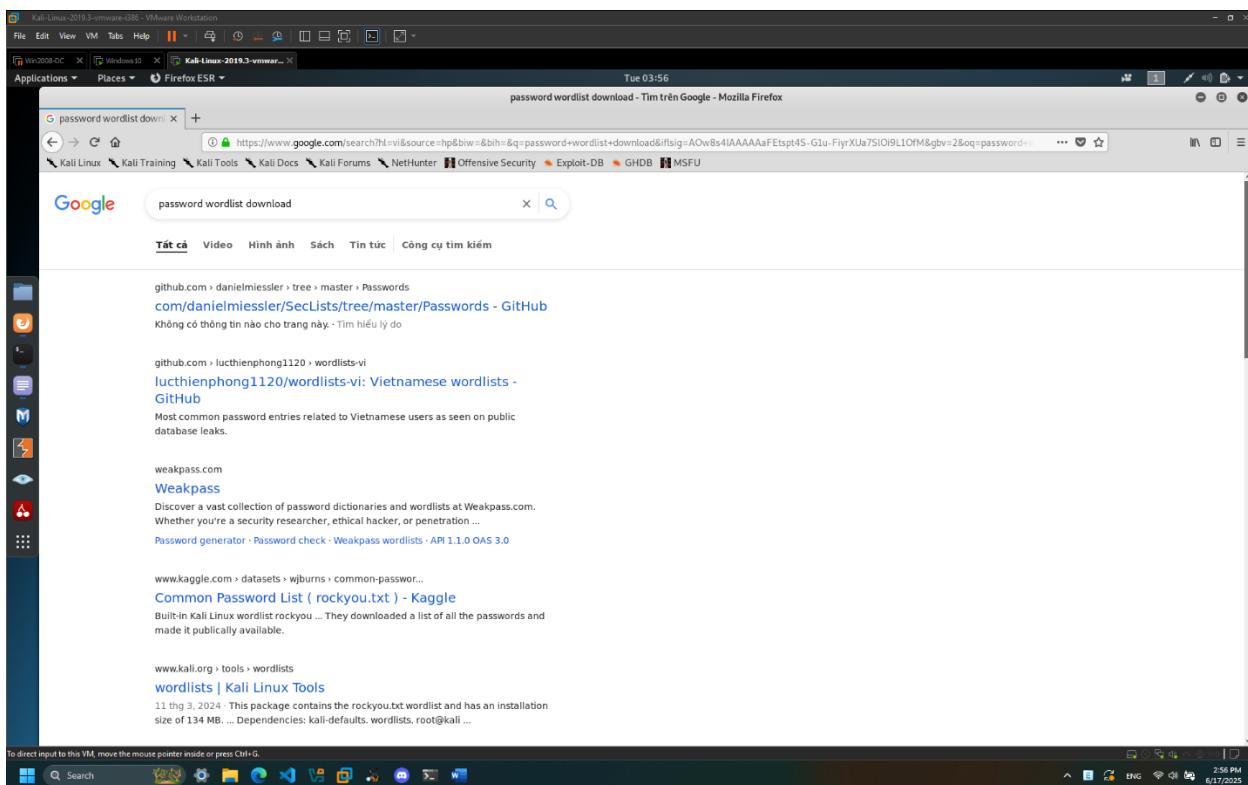


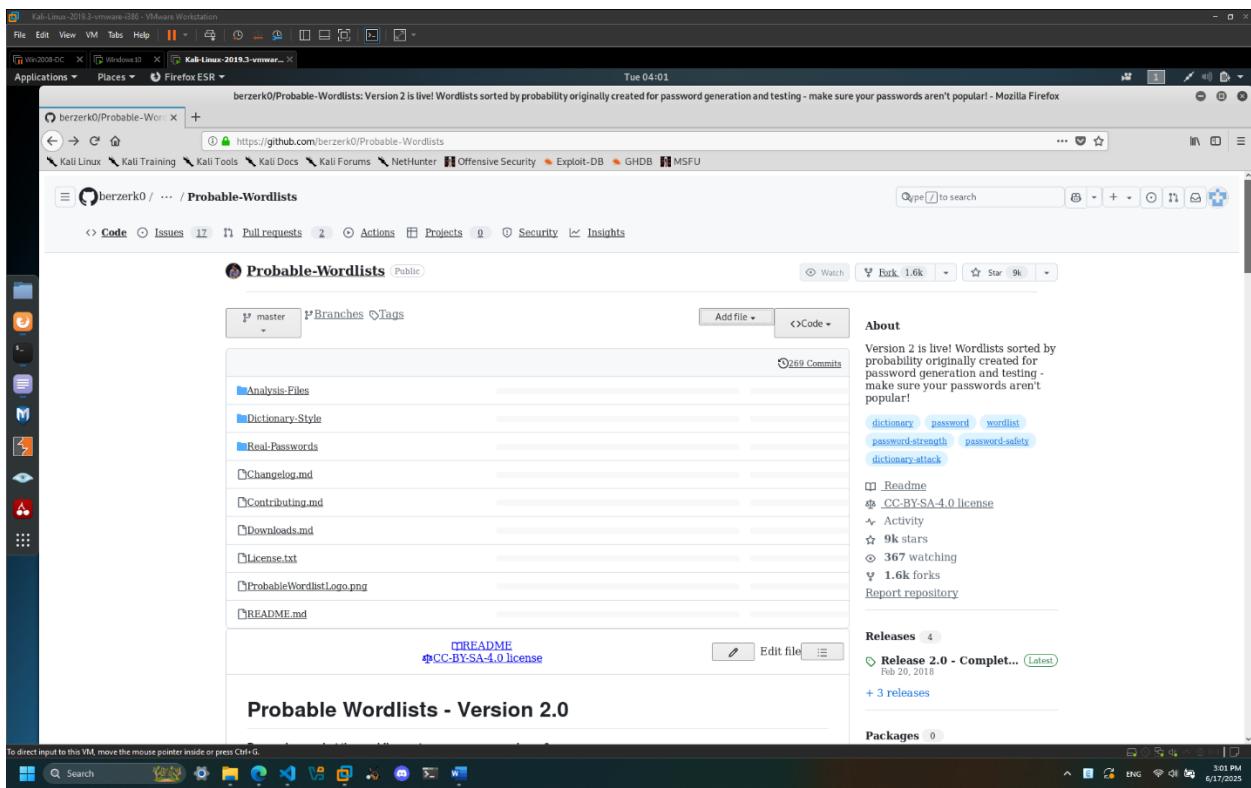
Step 13:



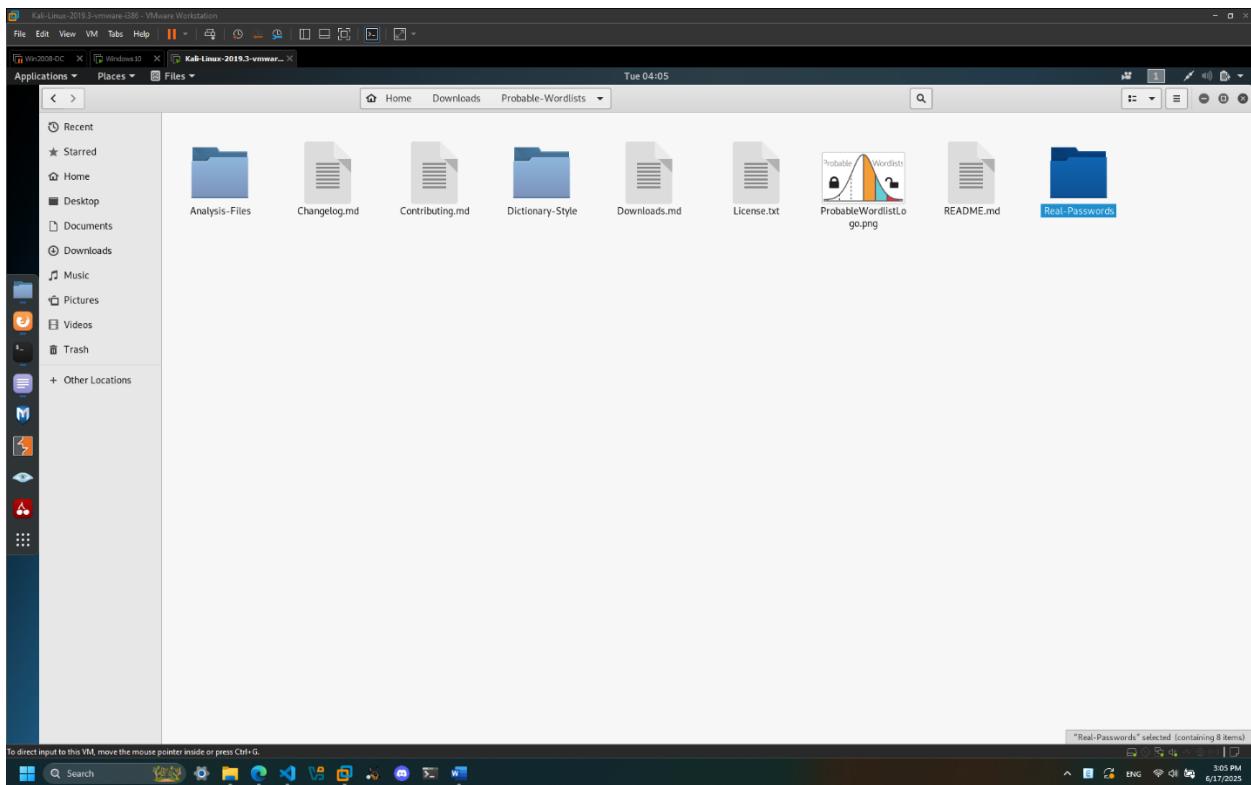


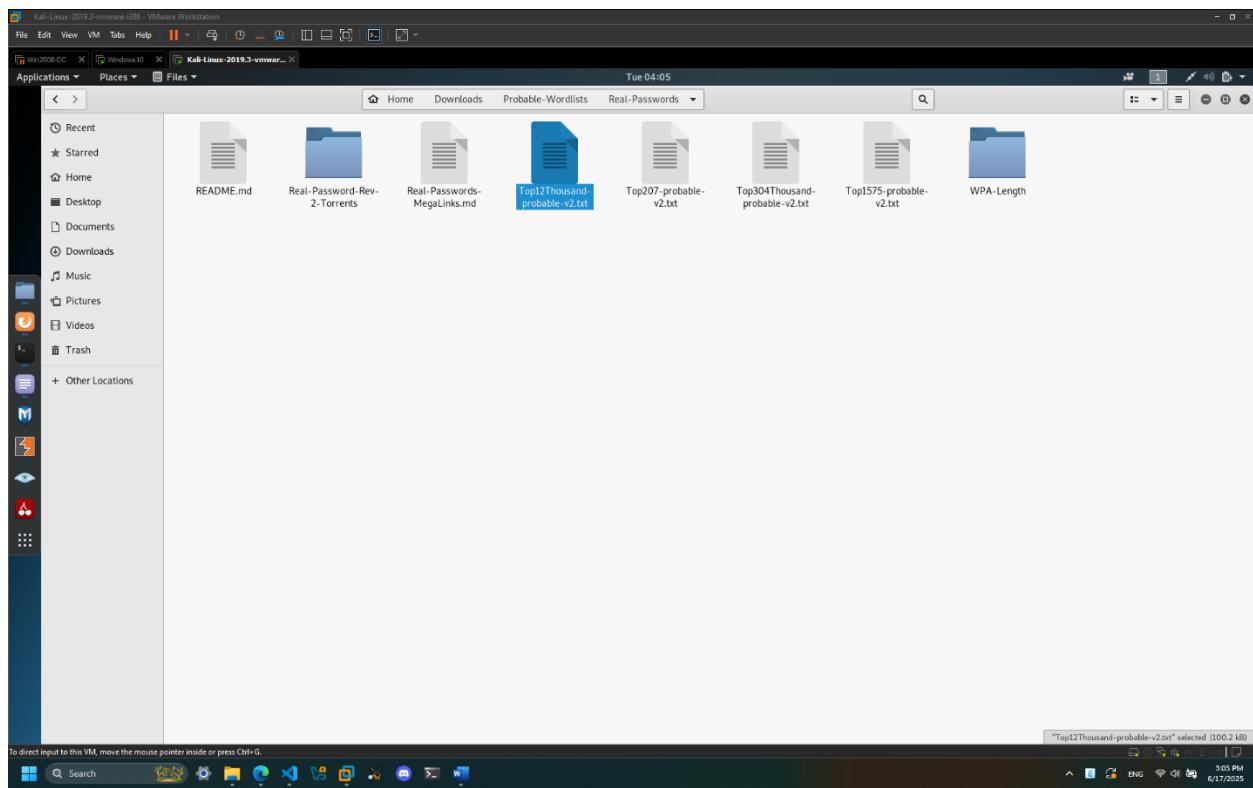
Step 14:



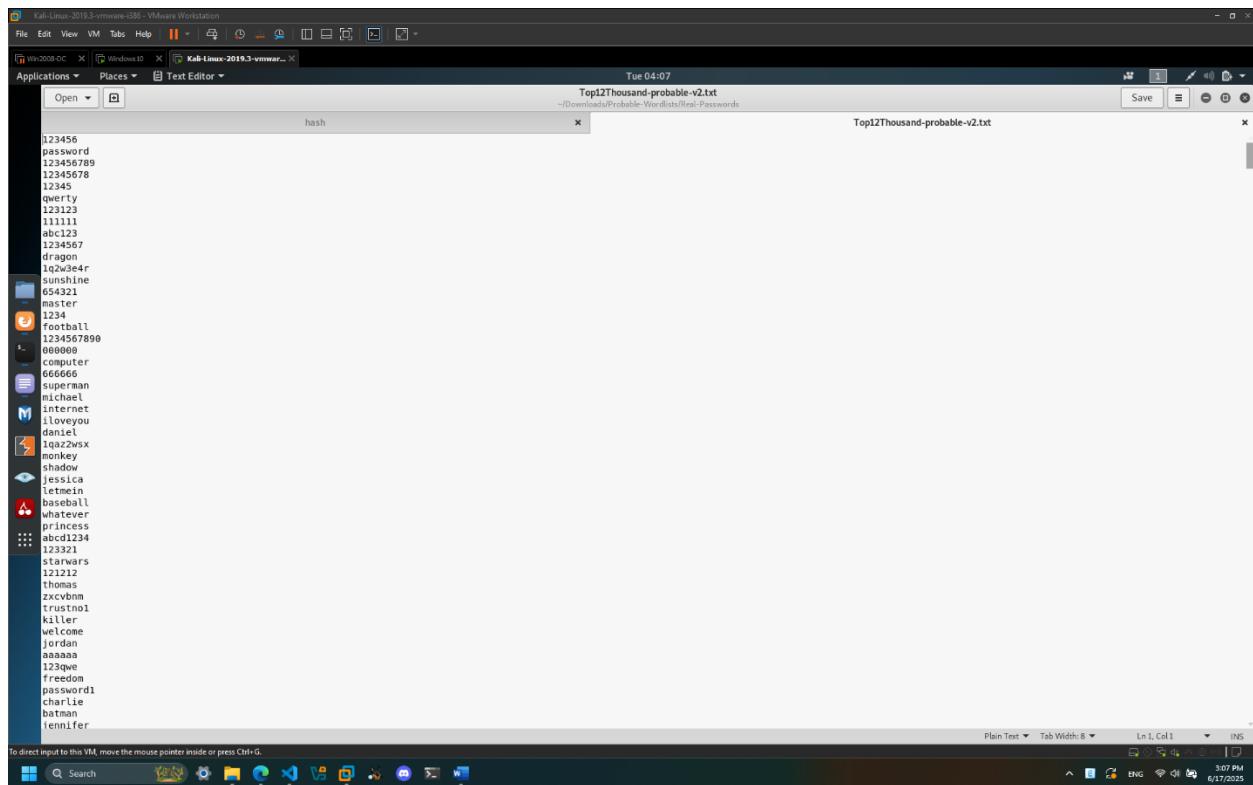


Step 15:



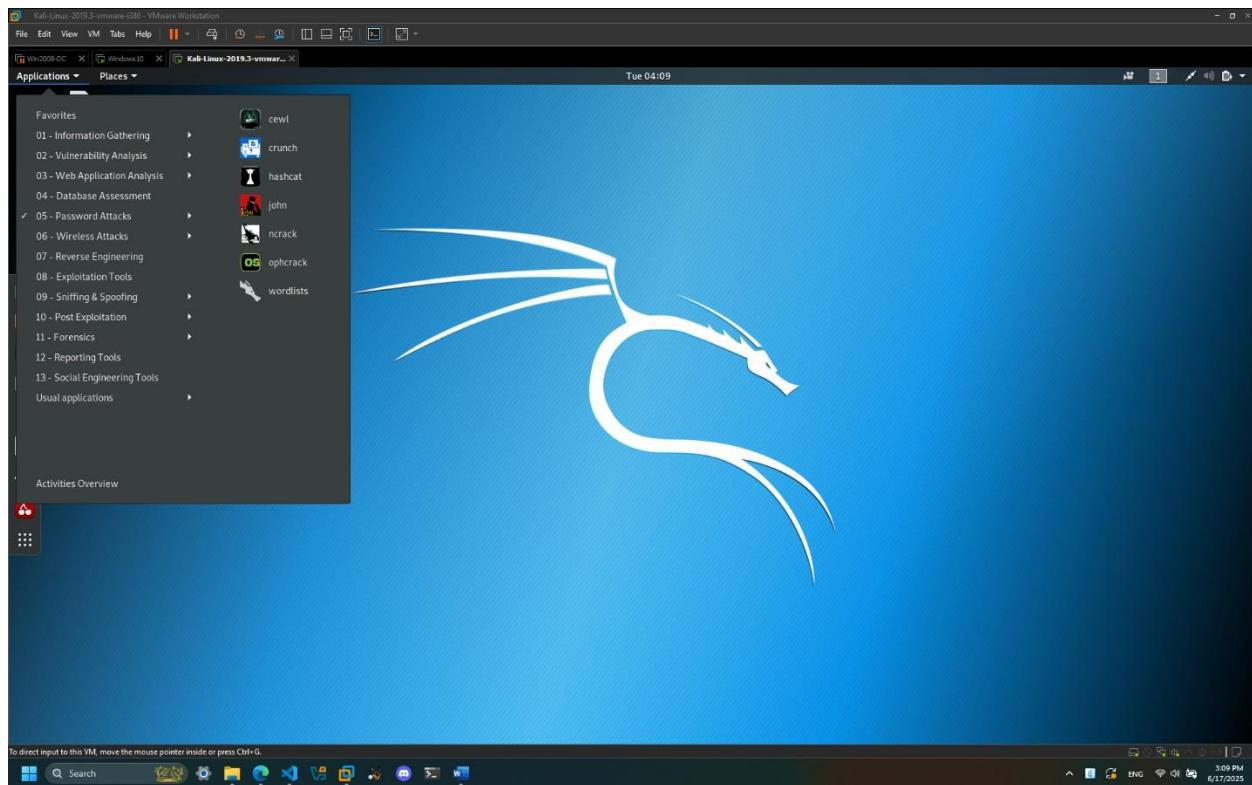


Step 16:



A screenshot of a Kali Linux desktop environment running in a VMware Workstation window. The desktop has a blue background featuring the Kali Linux logo (a stylized white dragon). A terminal window titled 'pwlist' is open, displaying a large list of password hashes and plain text passwords. The list includes common弱口令 (weak passwords) such as '123456', 'password', '123456789', '12345678', '12345', '1234567890', '123123', '111111', 'abc123', '1234567', 'dragon', 'sunshine', '654321', 'master', '1234', 'michael', 'internet', 'iloveyou', 'daniel', 'lqazwsx', 'monkey', 'now', 'jessica', 'lemin', 'baseball', 'whatever', 'princess', 'cd1234', '123321', 'starwars', '121212', 'thomas', 'zxcvbnm', '1234567890', 'killer', 'welcome', 'jordan', 'aaaaaa', '123qwe', 'fedoron', 'password1', 'charlie', 'batman', and 'ennifer'. The terminal window has tabs for 'hash' and 'pwlist', and includes standard file operations like Open, Save, and Print.

Step 17:



Step 18:

The image shows two terminal windows from Kali Linux 2019.3 running in VMware Workstation. Both windows are titled 'Terminal' and show a root shell prompt 'root@kali:~'. The top window displays the 'hashcat - advanced password recovery tools' command-line interface. It lists various options and their descriptions, such as '-m' for hash-type, '-a' for attack-mode, and '-r' for ruleset. The bottom window shows the output of the command 'res --brain-session-whitelist | Hex'. This command generates a hex dump of session whitelisted values, which is then processed by 'res'. The resulting output is a table with columns '#', 'Name', and 'Category'. The table lists numerous hashing algorithms and their properties, such as SHA2-256, SHA3-256, and various GOST and BLAKE2 variants.

Step 19:



```
# | Mode
=====
0 | Straight
1 | Combination
2 | Brute-Force
3 | Hybrid Wordlist + Mask
4 | Hybrid Mask + Wordlist
5 | Dictionary
6 | Mask
7 | Built-in Charsets
8 | OpenCL Device Types
9 | Device Type
M | Workload Profiles
10 | Basic Examples
11 | Hash-Mode
12 | Hash-Type
13 | Example command
Wordlist | Hash-Mode | Hash-Type | Example command
Wordlist | MD5 | hashcat -a 0 -m 400 example400.hash example.dict
Wordlist + Rules | MD5 | hashcat -a 0 -m 0 example0.hash example.dict -r rules/best64.rule
Brute-Force | MD5 | hashcat -a 3 -m 0 example0.hash ?a?/?a?/?a?/?a?
Combinator | MD5 | hashcat -a 1 -m 0 example0.hash example.dict example.dict

If you still have no idea what just happened, try the following pages:
* https://hashcat.net/wiki/howtos_videos_papers_articles/etc_in_the_wild
* https://hashcat.net/faq
root@kali:~#
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Step 20:

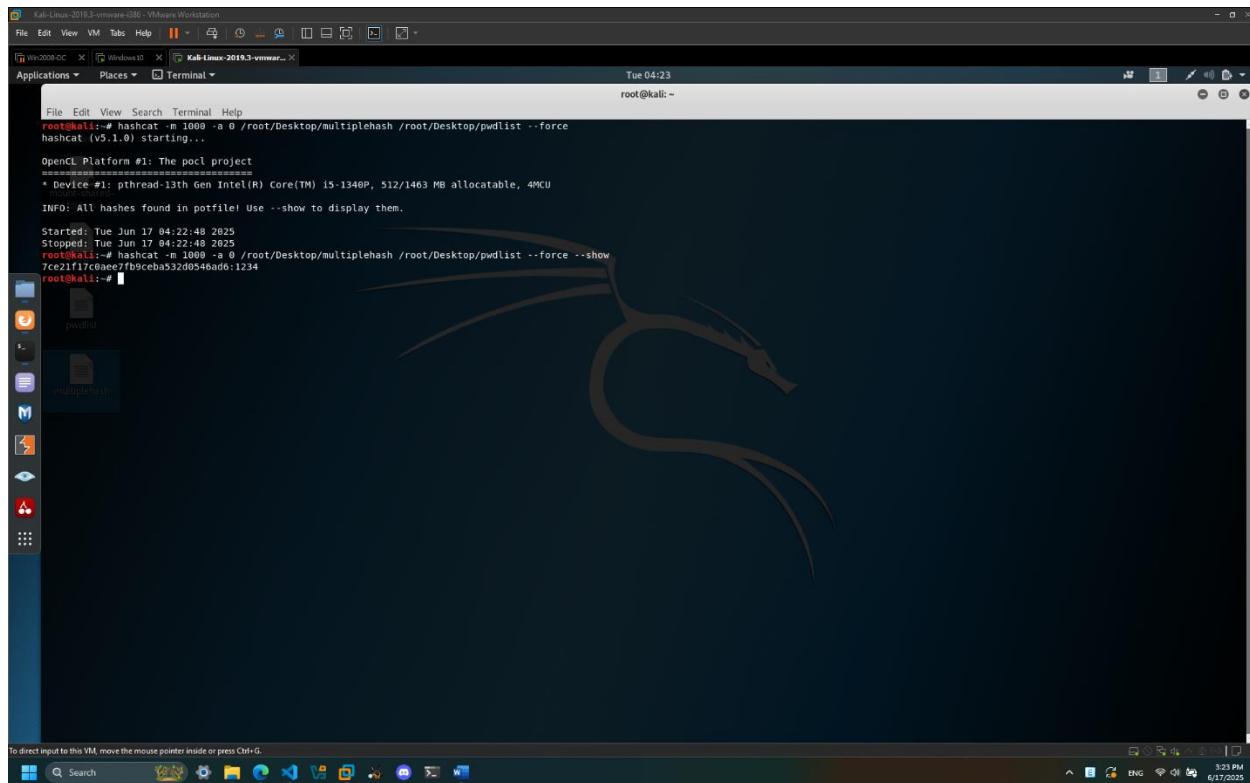


```
File Edit View VM Tabs Help ||| Applications Places Terminal
Tue 04:20
root@kali:~# hascat -m 1000 -a 0 /root/Desktop/hash /root/Desktop/pwdlist --force
hashcat (v5.1.0) starting...
OpenCL Platform #1: The pool project
* Device #1: pthread-13th Gen Intel(R) Core(TM) i5-1340P, 512/1463 MB allocatable, 4MCU
INFO: All hashes found in potfile! Use --show to display them.

Started: Tue Jun 17 04:20:44 2025
Stopped: Tue Jun 17 04:20:44 2025
root@kali:~# hascat -m 1000 -a 0 /root/Desktop/hash /root/Desktop/pwdlist --force --show
Tce21f17c0ae7fb3ceba532d0546a0d:1234
root@kali:~#
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Step 21:



The screenshot shows a Kali Linux terminal window titled "Terminal" running on a VM. The terminal session is as follows:

```
root@kali:~# hashcat -m 1000 -a 0 /root/Desktop/multiplehash /root/Desktop/pwdlist --force
hashcat (v5.1.0) starting...
OpenCL Platform #1: The pocl project
* Device #0: pthread-13th Gen Intel(R) Core(TM) i5-1340P, 512/1463 MB allocatable, 4MCU
INFO: All hashes found in potfile! Use --show to display them.

Started: Tue Jun 17 04:22:48 2025
Stopped: Tue Jun 17 04:22:48 2025
root@kali:~# hashcat -m 1000 -a 0 /root/Desktop/multiplehash /root/Desktop/pwdlist --force --show
7ce21f1c7d8e6e7fbceba532d0546ad6:1234
root@kali:~#
```

The terminal window has a dark background with a large, stylized dragon logo in the center. The desktop environment includes a dock with icons for various applications like a web browser, file manager, and terminal.