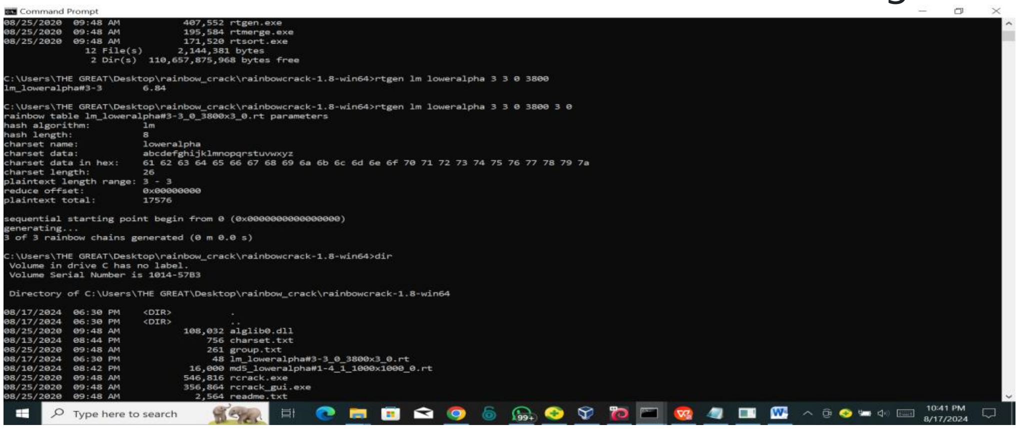
Decrypting a Windows LM Password Hash

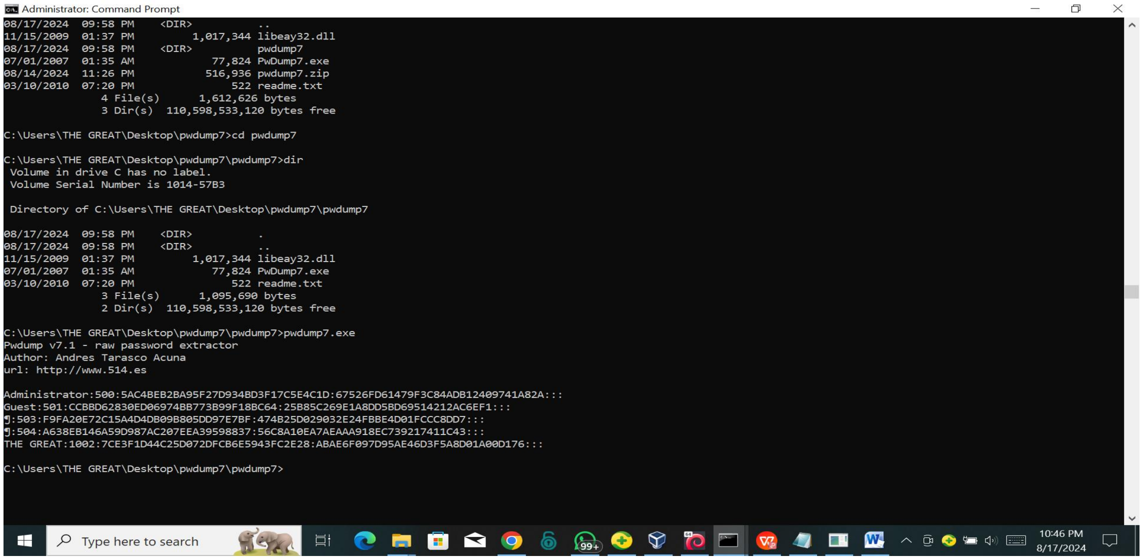
This task was so complicated for me to accomplish as it was my first time hearing it but after a series of research I was able to have some understanding regarding lm password hash and how to extract them from the SAM database. Below lies some of the steps I took to archive the the task though it was'nt a success as expected.

1. I started by generating a rainbow table using the rtgen command '*rtgen lm loweralpha 0 characters 0 1 0 0*' and later on sorted it using '*rtsort .*'



```
08/25/2020  09:48 AM           407,552 rtgen.exe
08/25/2020  09:48 AM           195,584 rtmerge.exe
08/25/2020  09:48 AM           171,520 rtsort.exe
              12 File(s)      2,144,381 bytes
               2 Dir(s)  110,657,875,968 bytes free

C:\Users\THE GREAT\Desktop\rainbow_crack\rainbowcrack-1.8-win64>rtgen lm loweralpha 3 3 0 3800
lm_loweralpha#3-3       6.84

C:\Users\THE GREAT\Desktop\rainbow_crack\rainbowcrack-1.8-win64>rtgen lm loweralpha 3 3 0 3800 3 0
rainbow table lm_loweralpha#3-3_0_3800x3_0.rt parameters
hash algorithm:         lm
hash length:            8
charset name:           loweralpha
charset data:           abcdefghijklmnopqrstuvwxyz
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
charset length:         26
plaintext length range: 3 - 3
reduce offset:          0x00000000
plaintext total:        17576

sequential starting point begin from 0 (0x0000000000000000)
generating...
3 of 3 rainbow chains generated (0 m 0.0 s)

C:\Users\THE GREAT\Desktop\rainbow_crack\rainbowcrack-1.8-win64>dir
 Volume in drive C has no label.
 Volume Serial Number is 1014-57B3

 Directory of C:\Users\THE GREAT\Desktop\rainbow_crack\rainbowcrack-1.8-win64

08/17/2024  06:30 PM    <DIR>          .
08/17/2024  06:30 PM    <DIR>          ..
08/25/2020  09:48 AM           108,032 alglib0.dll
08/13/2024  08:44 PM               756 charset.txt
08/25/2020  09:48 AM               261 group.txt
08/17/2024  06:30 PM                48 lm_loweralpha#3-3_0_3800x3_0.rt
08/10/2024  08:42 PM            16,000 md5_loweralpha#1-4_1_1000x1000_0.rt
08/25/2020  09:48 AM           546,816 rcrack.exe
08/25/2020  09:48 AM           356,864 rcrack_gui.exe
08/25/2020  09:48 AM             2,564 readme.txt
```

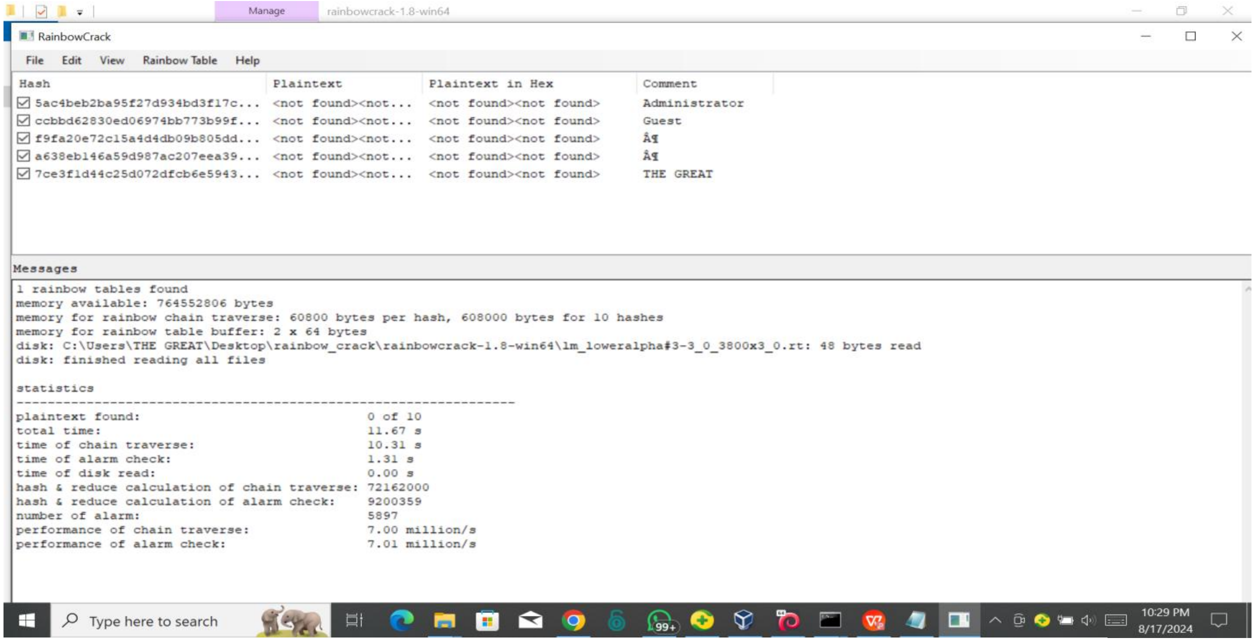
2. I later on went forward to extract lm hashes from the SAM database using a tool
   pwdump7



```
08/17/2024  09:58 PM    <DIR>          ..
11/15/2009  01:37 PM         1,017,344 libeay32.dll
08/17/2024  09:58 PM    <DIR>          pwdump7
07/01/2007  01:35 AM            77,824 PwDump7.exe
08/14/2024  11:26 PM           516,936 pwdump7.zip
03/10/2010  07:20 PM               522 readme.txt
               4 File(s)      1,612,626 bytes
               3 Dir(s)  110,598,533,120 bytes free

C:\Users\THE GREAT\Desktop\pwdump7>cd pwdump7

C:\Users\THE GREAT\Desktop\pwdump7\pwdump7>dir
 Volume in drive C has no label.
 Volume Serial Number is 1014-57B3

 Directory of C:\Users\THE GREAT\Desktop\pwdump7\pwdump7

08/17/2024  09:58 PM    <DIR>          .
08/17/2024  09:58 PM    <DIR>          ..
11/15/2009  01:37 PM         1,017,344 libeay32.dll
07/01/2007  01:35 AM            77,824 PwDump7.exe
03/10/2010  07:20 PM               522 readme.txt
               3 File(s)      1,095,690 bytes
               2 Dir(s)  110,598,533,120 bytes free

C:\Users\THE GREAT\Desktop\pwdump7\pwdump7>pwdump7.exe
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:5AC4BEB2BA95F27D934BD3F17C5E4C1D:67526FD61479F3C84ADB12409741A82A:::
Guest:501:CCBBD62830ED06974BB773B99F18BC64:25B85C269E1A8DD5BD69514212AC6EF1:::
¶:503:F9FA20E72C15A4D4DB09B805DD97E7BF:474B25D029032E24FBBE4D01FCCC8DD7:::
¶:504:A638EB146A59D987AC207EEA39598837:56C8A10EA7AEAAA918EC739217411C43:::
THE GREAT:1002:7CE3F1D44C25D072DFCB6E5943FC2E28:ABAE6F097D95AE46D3F5A8D01A00D176:::

C:\Users\THE GREAT\Desktop\pwdump7\pwdump7>
```

3. After saving the lm hashes in in file ‘*lmhashes.txt*’ I later on navigate to ‘*C:\Users\THE GREAT\Desktop\rainbow_crack\rainbowcrack-1.8-win64*’ and open the rcrack_gui and load the LM hashes from pwdump7, followed by selecting the above created rainbow

table



Hash	Plaintext	Plaintext in Hex	Comment
☑ 5ac4beb2ba95f27d934bd3f17c...	<not found><not...	<not found><not found>	Administrator
☑ ccbbd62830ed06974bb773b99f...	<not found><not...	<not found><not found>	Guest
☑ f9fa20e72c15a4d4db09b805dd...	<not found><not...	<not found><not found>	Â¶
☑ a638eb146a59d987ac207eea39...	<not found><not...	<not found><not found>	Â¶
☑ 7ce3f1d44c25d072dfcb6e5943...	<not found><not...	<not found><not found>	THE GREAT

Messages

```
1 rainbow tables found
memory available: 764552806 bytes
memory for rainbow chain traverse: 60800 bytes per hash, 608000 bytes for 10 hashes
memory for rainbow table buffer: 2 x 64 bytes
disk: C:\Users\THE GREAT\Desktop\rainbow_crack\rainbowcrack-1.8-win64\lm_loweralpha#3-3_0_3800x3_0.rt: 48 bytes read
disk: finished reading all files

statistics
----------------------------------------------------------------
plaintext found:                             0 of 10
total time:                                  11.67 s
time of chain traverse:                      10.31 s
time of alarm check:                         1.31 s
time of disk read:                           0.00 s
hash & reduce calculation of chain traverse: 72162000
hash & reduce calculation of alarm check:    9200359
number of alarm:                             5897
performance of chain traverse:               7.00 million/s
performance of alarm check:                  7.01 million/s
```

4. But now the challenge is that none of the hashes were cracked and I don’t know how to go about it.