**Pulling Hashes**

Cat etc/passwd

* Will show the password file but usually admins don’t keep password hashes in this folder anymore
* Probably in the shadow file
  + Etc/shadow

A computer screen capture

Description automatically generated with medium confidence

This is the password hash for the machine

* Standard procedure to just grab whatever hashes are available
* These logins can be used from a persistence standpoint

When in a meterpreter shell, the cmd hashdump can be used to obtain hashes

A picture containing text, screenshot, electronics, display

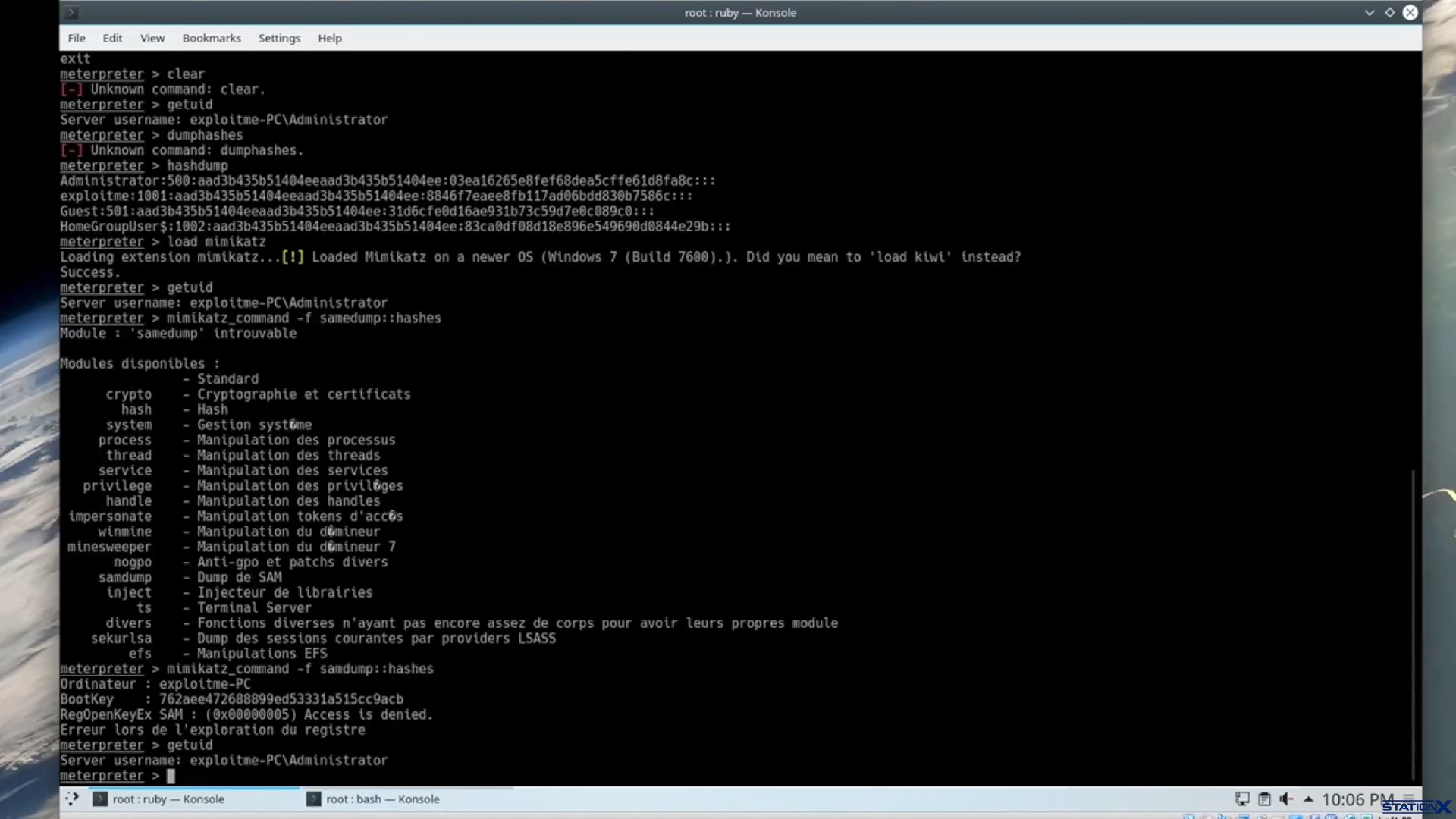
Description automatically generated

Usually when a usr is currently logged in, their password will be stored in memory in cleartext

* Best to just try and pull these than to crack the hashes

Mimikatz can be used for this

* Load mimikatz
* mimkatz\_command -f samdump: :hashes



Access denied because admin is lower than system and the sam file is protected by specific OS-based parameters, where the user needs to be system and it needs to be running a certain process.

* This is why booting kali over the top of a windows machine can allow you to rip the sam files off the system and pull the hashes

Getsystem # to get system privileges

Getuid #NT AUTHORITY\SYSTEM

mimkatz\_command -f samedump: :hashes

A screenshot of a computer

Description automatically generated with medium confidence

**Passwords from memory**

Text

Description automatically generated

Could create a binary that grabs any net new passwords in this file so whenever somebody logs in then their password will be pulled

* Can even phish the admin to login by making them think somethings wrong with the machine so they check

**Pass The Hash**

**Windows has a vulnerability where it can use the hashes to authenticate you rather than the cleartext versions**

* Pth-winexe -? # shows cmds
* Pth-winexe -U administrator**%**<insert hash> //<rhost> cmd.exe
  + -U # user
  + Rhost # target machine

HW – find out how to get around User Access Control for users as this will work on admin or normal accounts but wont work on the system user unless UAC is bypassed