# 计算机取证—Windows 系统初始响应方法

## Computer Forensics – Initial Response to Windows System

殷联甫　（嘉兴学院信息工程学院　314001）
张行文　（湖北师范学院计算机科学系　435002）

**摘要**：Windows 系统作为目前最常用的操作系统，研究 Windows 系统上的计算机取证方法具有非常重要的现实意义。本文介绍了对 Windows 系统进行初始响应所需的常用工具及基本步骤，并给出了几个常见工具的具体使用方法。

**关键词**：初始响应　计算机取证　计算机犯罪调查

## 1　引言

Windows 系统作为目前最常用的操作系统，研究 Windows 系统上的计算机取证方法具有非常重要的现实意义。

一般情况下，当发现 Windows 系统受到入侵而需要对系统进行取证分析时，首先需要关闭系统，然后对硬盘进行按位（bit – level）备份以作进一步的分析。但一旦关机，有些重要的入侵证据往往会丢失，这些证据一般存在于被入侵机器的寄存器、缓存或内存中，主要包括网络连接状态、正在运行的进程状态等信息。这些证据往往被称为易失性数据（volatile information）。系统关闭后这些数据就会全部丢失，而且不可能恢复。

初始响应就是在关闭系统之前收集受害者机器上的易失性数据的过程。主要的易失性数据包括：

（1）系统日期和时间；

（2）当前运行的活动进程；

（3）当前的网络连接；

（4）当前打开的端口；

（5）在打开的套接字（open sockets）上监听的应用程序；

（6）当前登录的用户。

## 2　创建初始响应工具包

对 Windows 系统进行初始响应之前，首先应创建初始响应工具包。目前，在 Windows 系统中常用的初始响应工具主要有以下几种：

（1）cmd. exe（系统内置）

Windows NT 和 Windows 2000 的命令行工具。

（2）ipconfig（系统内置）

显示系统 IP 地址。

（3）netstat（系统内置）

列出所有监听端口及与这些端口的所有连接。

（4）nbtstat（系统内置）

列出最近十分钟内的 NetBIOS 连接。

（5）env（http://unxutils. sourceforge. net/）

显示系统环境变量。

（6）psuptime（http://www. sysinternals. com/ntw2k/freeware/psuptime. shtml）

显示系统从开机到当前已正常运行的时间。

（7）net（系统内置）

列出 NetBIOS 连接、用户账号、共项文件夹等信息。

（8）loggedon（www. foundstone. com）

显示本地连接和远程连接的所有用户。

（9）pulist

（http://www. microsoft. com/windows2000/techinfo/reskit/tools/existing/pulist – o. asp）

列出在本地或远程计算机上运行的活动进程，也能捕获正在运行进程的用户。

（10）pslist（www. foundstone. com）

列出在目标系统中正在运行的所有进程。

（11）listdlls（www. foundstone. com）

列出所有正在运行的进程及其命令行参数和各自

运行所需的动态链接库。

(12) fport(www.foundstone.com)

列出 Windows NT/2000 系统中打开 TCP/IP 端口的所有进程。

(13) psservice (http://www.sysinternals.com/ntw2k/freeware/psservice.shtml)

列出服务的状态、结构和依赖关系,也可以启动、终止、暂停、恢复或重启服务。

(14) psinfo (http://www.sysinternals.com/ntw2k/freeware/psinfo.shtml)

收集本地或远程 Windows2000/NT 系统的关键信息,包括安装类型、内核构造、寄存器组成、处理器数目及类型、物理内存大小、系统安装时间、是否试用版本、失效时间等。

(15) arp(系统内置)

将逻辑 IP 地址转换为物理 MAC 地址。

(16) hfind (http://www.foundstone.com/resources/proddesc/forensic-toolkit.htm)

找出具有隐藏属性的文件。

(17) streams (http://www.sysinternals.com/ntw2k/source/misc.shtml)

显示 NTFS 文件流信息。

(18) ntlast (http://www.foundstone.com/resources/proddesc/ntlast.htm)

监视所有成功和失败的系统登录。

(19) reg(Windows NT 资源工具包(NTRK))

注册表操作命令。

(20) auditpol(Windows NT 资源工具包(NTRK))

显示系统的安全审计策略。

(21) regdmp(Windows NT 资源工具包(NTRK))

将注册表内容转储为一个文本文件。

(22) md5sum (www.cygwin.com)

为一个给定的文件创建 md5 散列。

(23) netcat(www.atstake.com/research/tools/network_utilities/)

用于在两个不同的系统之间创建通信信道。

(24) cryptcat (http://sourceforge.net/projects/cryptcat)

用来创建一个加密的通信信道。

(25) pclip(http://unxutils.sourceforge.net/)

将 Windiws 剪贴板的内容送到 stdout。

(26) tcpdump(http://www.tcpdump.org/)

网络分析工具。

(27) rasusers(Windows NT 资源工具包(NTRK))

显示对目标网络系统具有远程访问权限的所有用户。

(28) kill(Windows NT 资源工具包(NTRK))

中止正在运行的进程。

(29) rmtshare(Windows NT 资源工具包(NTRK))

显示远程计算机上可供访问的共享目录。

(30) psloglist(www.foundstone.com)

转储事件日志的内容。

(31) psfile(www.foundstone.com)

显示由远程打开的文件。

(32) doskey(系统内置)

显示打开的 cmd.exe 命令解释程序的命令记录。

## 3 收集易失性数据的步骤和方法

系统关机之前,可以使用前面介绍的初始响应工具来进行现场数据收集。现场数据收集主要分为以下几个步骤。

### 3.1 打开一个可信的命令解释程序

作为一名攻击者,总是希望把未经授权的访问隐藏到系统管理员账户中去(伪装成系统管理员进行未经授权的访问)。如果攻击者在已攻破的服务器上放置了一个经过修改的命令行 shell 版本,那么就可以隐藏从攻击工作站上发出的连接,这样,就可以进一步攻击了。

由于命令行 shell 可能被修改(通常在一个管理员账户被攻击后会出现这种情况),取证人员不能相信它的输出。因此,在进行现场数据收集时,取证人员必须带上自己的命令行解释程序(命令行 shell)。

初始响应工具包中所需的第一个工具便是可信的命令行 shell。登录到受害者机器后,请选择 Start | Run,然后输入下面的命令。

此时将在当前驱动器 e:上运行一个新的命令行 shell。任何在此使用的命令都被认为是可信的,因为它们并没有通过被攻击机器的不可信命令行 shell 运行。以后所有的命令都将在该可信的 shell 下运行。

### 3.2 数据收集系统的准备

在数据收集过程中,不能将收集到的证据写回到

被入侵机器的硬盘上。一个最简单的方法是将收集到的证据写到软盘上，但软盘的容量太小，有时无法容纳所有的证据。我们常用的方法是利用所谓的"TCP/IP瑞士军刀"工具 netcat，通过网络将收集到的证据传送到司法鉴定工作站（也叫响应系统，Responder's system）上。

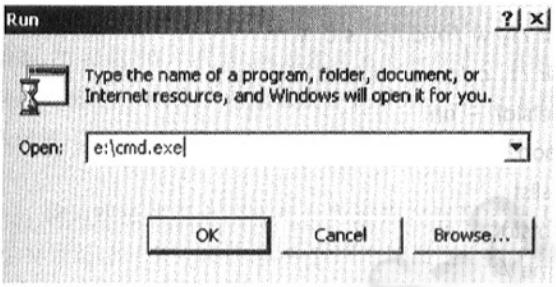


图 1　运行一个可信的命令解释程序

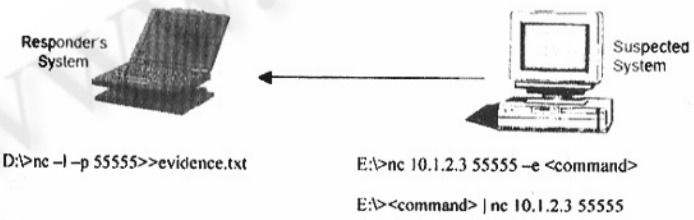


图 2　使用 netcat 收集证据

首先在响应系统中运行以下命令，使响应系统处于监听状态：

D:》nc - l - p 55555 > > evidence. txt

上面的命令在你的响应系统中打开一个监听端口，同时将接收到的数据重定向到文件 evidence. txt 中。参数"-l"表示监听模式，当监听方接收到数据后将关闭套接字端口，停止监听。如果希望监听方接收到数据后继续监听，可以选用参数"-L"。参数"-p"指定监听端口，你可以选择任何端口。

当响应系统准备就绪以后，你可以运行以下命令将收集到的证据通过网络传送到响应系统中（假设 E 驱动器是 CD ROM 驱动器，表示响应工具包建立在 CD ROM 上）：

E:》nc < IP address of responder's system > < port > -e < command >

或者：

E:《command > Inc < IP address of responder's system > < port >

例如，如果你准备将在被入侵机器上执行 dir 命令的运行结果传送到响应系统中（假设响应系统的 IP 地址为 10.1.2.3），你可以执行如下命令：

E:》nc 10.1.2.3 55555 - e dir

或者：

E:\dir| nc 10.1.2.3 55555

netcat 在数据传送时没有使用加密信道，如果你想使用加密信道，可以用 cryptcat 代替 netcat 命令。

### 3.3 收集易失性证据

有了前面二步的准备工作，现在你可以运行工具包来收集易失性证据了。必须收集的易失性证据主要有：

- 基本的系统信息；
- 正在运行的进程；
- 打开的套接字（sockets）；
- 网络连接；
- 网络共享；
- 网络用户。

下面介绍几个常用初始响应工具的使用方法。

（1）fport 命令

在响应过程中，首先在被攻击机器上使用的命令之一是 fport。fport 是一个由 Foundstone 公司发布的免费工具，可在如下网址找到：www.foundstone.com。该工具将受害者机器上每个打开的 TCP 与 UDP 端口映射到系统中的一个正在运行的文件上。fport 对于定位不同类型的后门程序很有用。

fport 的命令行用法很简单：

E:》fport

fport 将返回类似下面的输出信息：（略）。

看完 fport 返回的数据，我们觉得已经打开的 TCP 端口 62875 很可疑，因为它是被一个名为 C:\inetpub\scripts\nc. exe 的可执行文件打开的。另外，看到该过程的 ID 为 1464，这不是一个新系统通常所安装的程序，因此，它应该被进一步分析。

（2）netstat

netstat 显示了受害者机器的监听程序和当前连接的网络信息。该命令可以观察当前连接并监听应用，

这些信息可以帮助你发现一些犯罪行为以及安装在受害者机器上的后门程序。

该工具的使用相当简单。可以输入下面的命令得到被攻击系统的网络连接 IP 地址和所有打开的端口信息：

E:\>netstat -an

"-a"标志告诉程序显示所有的网络信息，"-n"标志告诉程序不对输出中所列的外部 IP 地址执行反向域名系统查询。

下面的内容是在对某受害者机器执行 netstat 命令后得到的输出结果：

Active Connections

| Proto | Local Address | Foreign Address | State |
|---|---|---|---|
| TCP | 0.0.0.0:7 | 0.0.0.0:0 | LISTENING |
| TCP | 0.0.0.0:9 | 0.0.0.0:0 | LISTENING |
| . | | | |
| . | | | |
| . | | | |
| TCP | 192.168.1.103:1041 | 0.0.0.0:0 | LISTENING |
| TCP | 192.168.1.103:1041 | 192.168.1.1:139 | ESTABLISHED |
| TCP | 192.168.1.103:62875 | 0.0.0.0:0 | LISTENING |
| TCP | 192.168.1.103:62875 | 192.168.1.1:139 | ESTABLISHED |
| UDP | 0.0.0.0:7 | *:* | |
| UDP | 0.0.0.0:9 | *:* | |
| . | | | |
| . | | | |
| . | | | |

有了这些信息后，我们看到 TCP 端口 62875 是打开的，这一结果与使用 fport 工具得到的结果相同。另外，我们看到 IP 地址为 192.168.1.1 的机器当前连接到了该端口。这告诉我们仍然有人在我们的机器上。

(3) pslist

进程表列表是我们想捕获的重要的易失性信息之一。可以使用 pslist 工具来完成这项工作。进程表列表将显示出任何恶意的进程，例如后门程序、嗅探器和口令破解程序。在攻击者击破一个系统后，可能会在该系统上运行这些程序。pslist 可以在 www.sysinternals.com 找到并自由下载。

## 4 编写初始响应脚本

初始响应中的许多操作可以合并成一个批处理脚本文件，因而通常将初始响应操作写入脚本文件，用 netcat 将该脚本文件的输出结果转存到司法鉴定工作站(响应系统)上。创建一个文本文件，加上.bat 扩展名就得到一个批处理文件。下面是一个可在 Windows NT/2000 上处理突发事件时使用的脚本文件的例子：

```
time /t
date /t
loggedon
dir /t:a /o:d /a /s c:\
dir /t:w /o:d /a /s c:\
dir /t:c /o:d /a /s c:\
netstat -an
fport
pslist
nbtstat -c
time /t
date /t
doskey /history
```

将上述文件命名为 ir.bat，在目标系统上运行，可以看到处理结果。

## 5 结束语

初始响应是计算机取证的关键步骤之一，通过初始响应可以获取非常有用的计算机犯罪信息。Windows 系统作为目前最常用的操作系统，研究 Windows 系统上的初始响应方法具有非常重要的现实意义。

### 参考文献


1 [美]Keith J. Jones, Mike Shema, Bradley C. Johnson 著，宋震、易晓东、肖国尊等译，《黑客大曝光》姊妹篇：阻击黑客，北京 电子工业出版社，2003 年。

2 [美]Mike Shema, Bradley C. Johnson 著，赵军锁、姜南等译，《黑客大曝光》姊妹篇：反黑客工具包(第二版)，北京 电子工业出版社，2005 年。

3 [美]Kevin Mandia, Chris Prosise 著，常晓波译，应急响应：计算机犯罪调查，北京：清华大学出版社，2002 年。

4 [美]Kevin Mandils Pra, Chrosise, Matt Pepe 著，汪青青、付宇光等译，应急响应 & 计算机司法鉴定，清华大学出版社，2004。

5 [美]Tan Koon Yaw. Windows Responder's Guide. http://www.sans.org/rr/paper.php? id=1120. 2005.