

获取易变数据

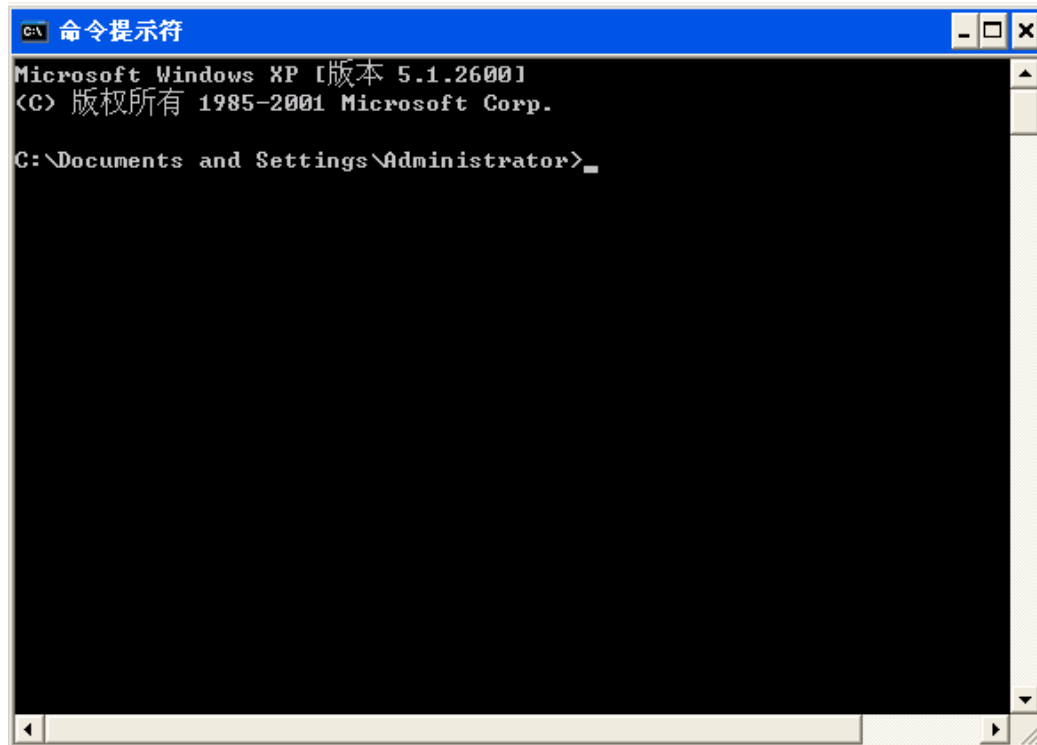
本节主要介绍取证时获取哪些易变数据以及获取的方法,本章讨论的工具以命令行形式为主。。命令行工具 (CLI) 比图形界面 (GUI) 的调查工具有特殊的优势。比较容易想到的优势包括命令行工具占用更小的内存,对内存的影响会比较小。命令行工具依赖的动态链接库更少,对系统的影响也比较少。使用命令行工具的主要原因在于命令行工具往往比较简洁,注重一个简单、特定功能的完成,因此比较容易通过批处理或脚本工具进行自动化。开机取证要求对系统影响最小,所以要避免写文件,并且在获取数据的时候越快越好。当然,GUI 工具并非完全不能用于开机取证过程,如果发现一个 GUI 工具可以很好地完成取证工作,那么就采用,毕竟获取数据是排在第一位的。

1、系统相关时间

时间调查过程中,首先要获取的信息包括系统时间。系统时间为以后获取的数据信息构建了时间上下文环境,并且会为系统事件时间线的正确分析提供帮助。除了系统时间外,系统上线时间 (Uptime) 信息也很重要,可以为调查提供另外一个线索。例如,比较系统运行时间和进程运行时间可以有效估计系统被入侵的可能时间。此外,调查人员在记录系统时间的同时也要记录真实时间,同时记录两者才可以确定系统时间是否正确。

获取系统时间实验

- 1、打开 cmd 命令窗口。

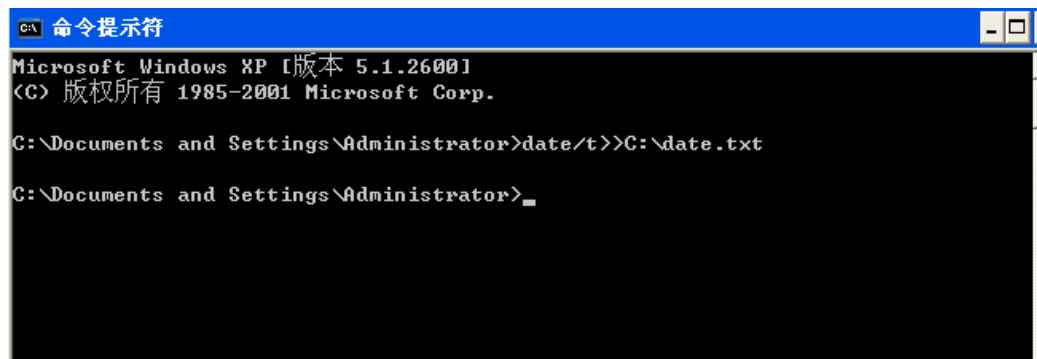


```
C:\> 命令提示符

Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>
```

2、先获取系统日期将信息输出文本，命令：`date/t>>C:\date.txt`，(/t : 换行)。

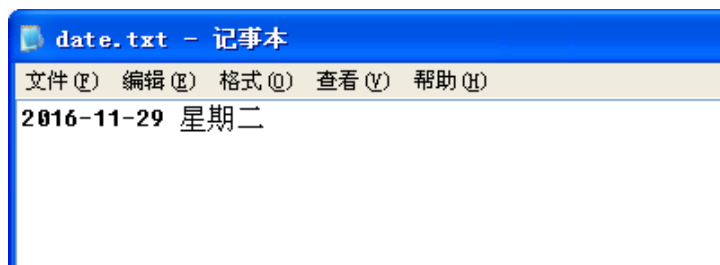


```
C:\> 命令提示符

Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>date/t>>C:\date.txt

C:\Documents and Settings\Administrator>
```



```
date.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
2016-11-29 星期二
```

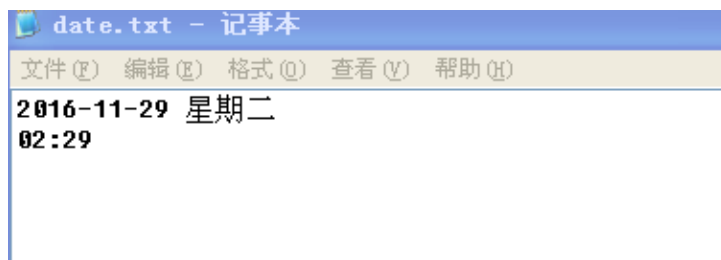
3、再获取系统时间将信息输出文本，命令：`time/t>>C:\date.txt`。

```
C:\ 命令提示符
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>date/t>>C:\date.txt

C:\Documents and Settings\Administrator>time/t>>C:\date.txt

C:\Documents and Settings\Administrator>_
```



4、获取系统上线时间(开机到现在的运行时间), 命令 : systeminfo>>C : \date.txt。

```
C:\ 命令提示符

C:\Documents and Settings\Administrator>systeminfo>>C:\date.txt

C:\Documents and Settings\Administrator>_
```



Systeminfo 除了可以显示系统上线时间 , 也可以获取其他更详细的系统信

息。系统时间为以后获取的数据信息构建了时间上下文环境，并且会为系统事件时间线的正确分析提供帮助。

2、当前系统登录的用户

调查过程中，有时需要知道系统的当前登录用户是谁，包括本地登录用户（通过控制台或键盘登录）和远程登录用户（`net use` 或共享）。登录用户为手机的其他系统信息提供了上下文线索，例如，运行进程的用户上下文、文件宿主、文件最后访问时间等。该信息也可以和安全日志进行相关分析，尤其是特殊审计开关打开的时候。

net sessions

该命令不仅可以查看通过远程登录访问系统的用户名，还可以显示使用的 IP 地址、客户端名称等信息。

psloggedon

该命令不但可以显示本地登录的用户，同时也可以显示远程登录的用户名。

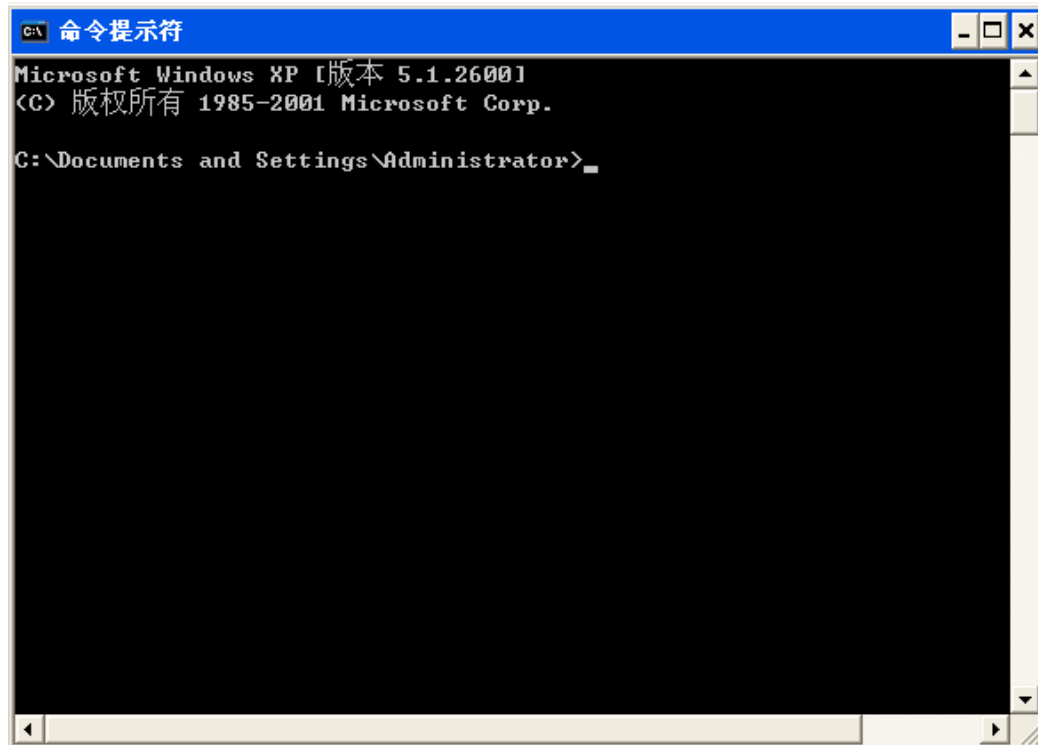
logonsessions

该命令可以列出系统的活动登录会话信息，登录使用的验证信息、登录的类型、活动进程等。

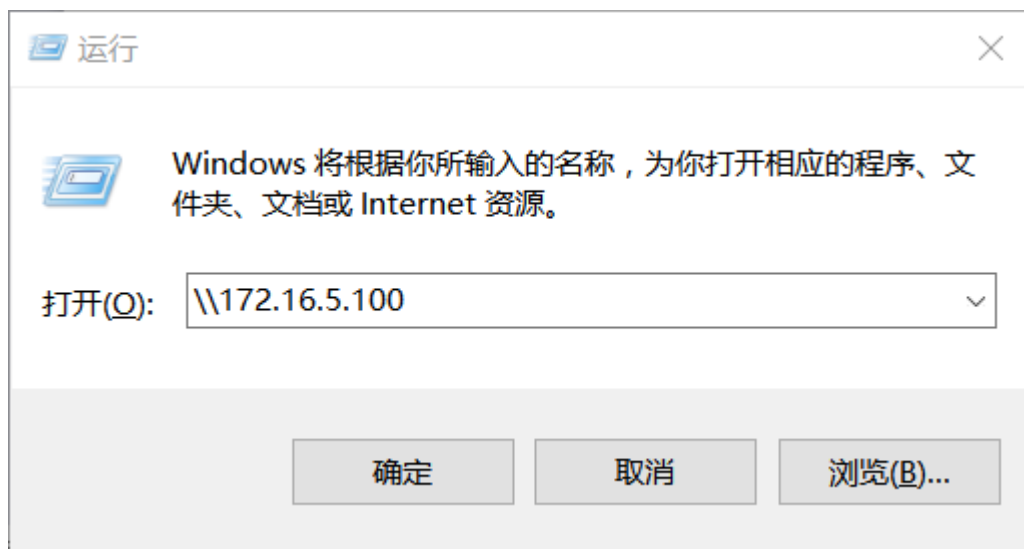
这些工具并不能显示是否有人通过后门登录到系统。

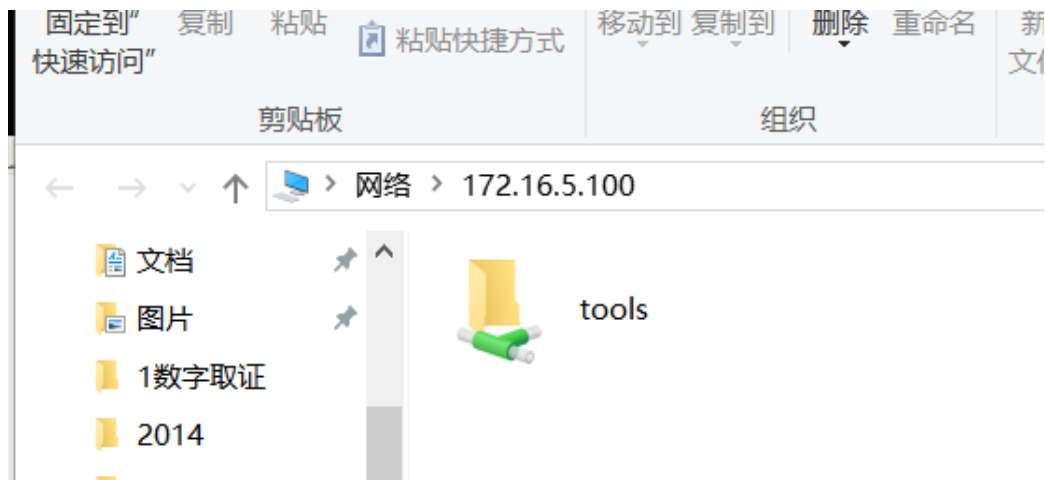
获取当前系统登录用户实验

- 1、登录虚拟机。
- 2、打开虚拟机 cmd 命令窗口。

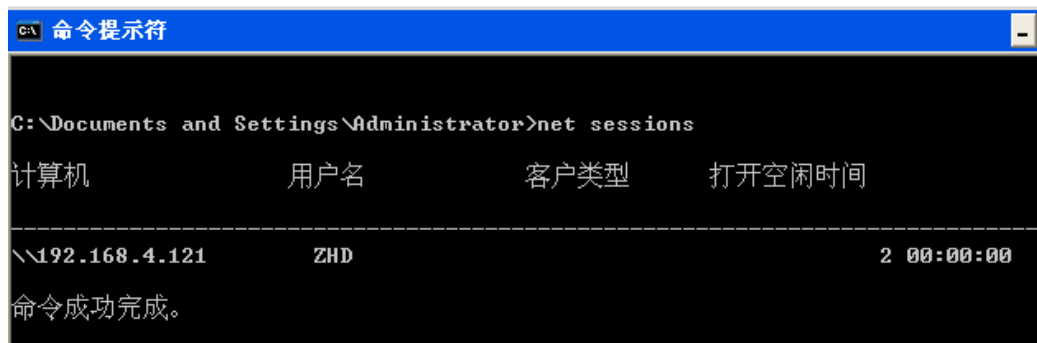


3、首先在本机通过 net use 连接虚拟机，访问虚拟机上共享的 tools 文件夹，命令：\\ip，下图的 ip 为虚拟机 ip，然后点击确定。





4、在虚拟机上获取通过 net use 远程登录访问系统的用户名、IP 地址、客户端信息等，命令：net sessions (需要管理员权限)。



上图的计算机即为本机 IP，用户名为本机用户名，还有本机连接时间

5、切换到 C : \tools\PsTools 目录，输入命令：psloggedon.exe。

C:\ 命令提示符

```
C:\Documents and Settings\Administrator>cd C:\tools\Pstools

C:\tools\Pstools>psloggedon.exe

loggedon v1.33 - See who's logged on
Copyright ?2000-2006 Mark Russinovich
Sysinternals - www.sysinternals.com

Users logged on locally:
    Error: could not retrieve logon time
NT AUTHORITY\LOCAL SERVICE
    Error: could not retrieve logon time
NT AUTHORITY\NETWORK SERVICE
    2016-11-29 0:55:17    ROOTT00R-58C7E0\Administrator
    Error: could not retrieve logon time
NT AUTHORITY\SYSTEM

Users logged on via resource shares:
    2016-11-29 2:56:01    (null)\ZHD
```

此命令显示的是本地连接和远程 net use 远程登录的所有用户。

6、输入命令：logonsessions.exe。

C:\ 命令提示符

```
C:\tools\Pstools>logonsessions.exe

Logonsessions v1.3
Copyright (C) 2004-2015 Mark Russinovich
Sysinternals - www.sysinternals.com

[0] Logon session 00000000:000003e7:
    User name:    WORKGROUP\ROOTT00R-58C7E0$
    Auth package: NTLM
    Logon type:   <none>
    Session:     0
    Sid:         S-1-5-18
    Logon time:   2016-11-29 0:53:39
    Logon server:
    DNS Domain:
    UPN:

[1] Logon session 00000000:00009232:
    User name:
    Auth package: NTLM
    Logon type:   <none>
    Session:     0
    Sid:         <none>
```

此命令显示的是本地和远程桌面登录系统用户信息（需要管理员权限）。

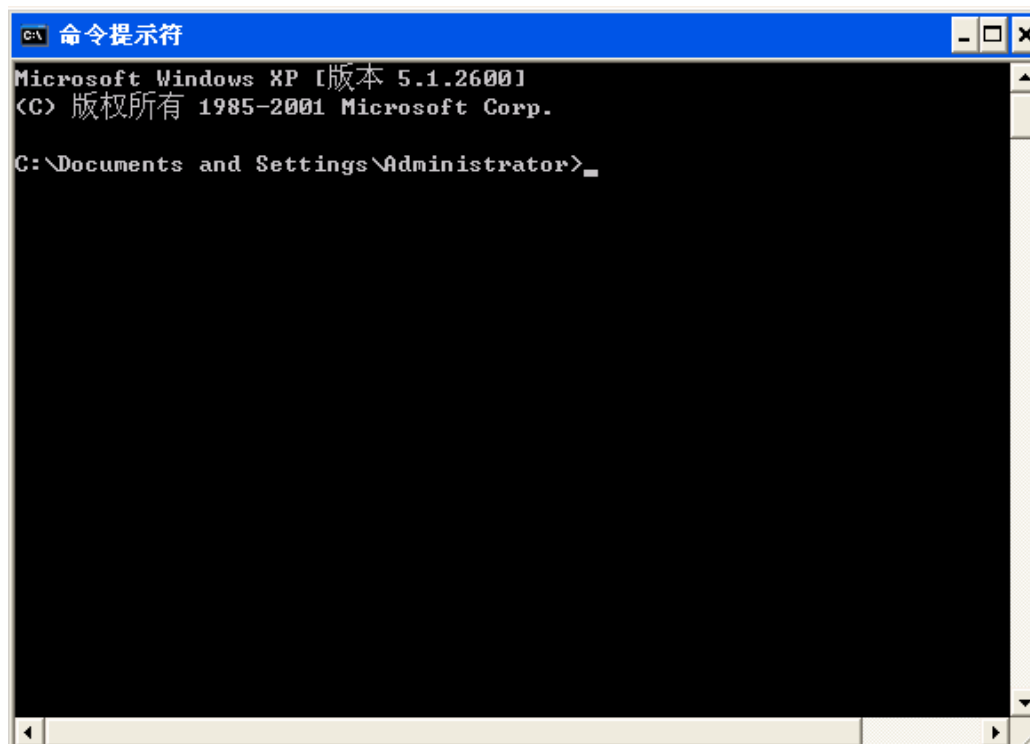
获取当前登录用户为收集的其他系统信息提供了上下文线索 ,该信息也可以和安全日志进行相关分析 ,尤其是在特殊审计开关打开的时候。

3、远程打开的文件

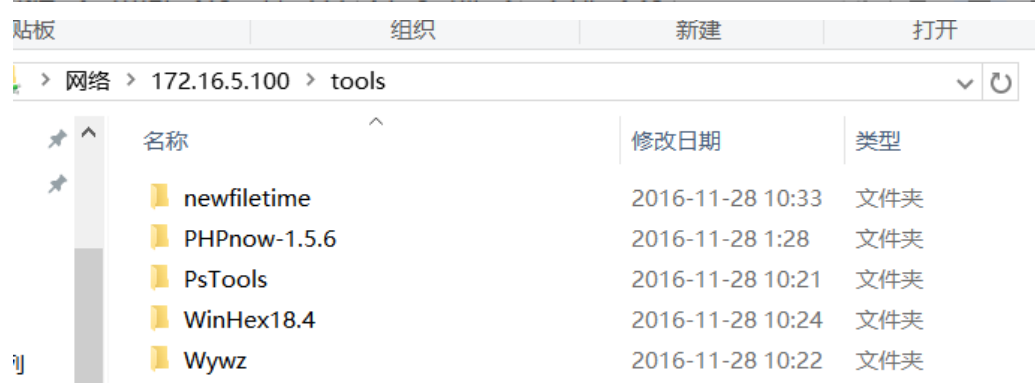
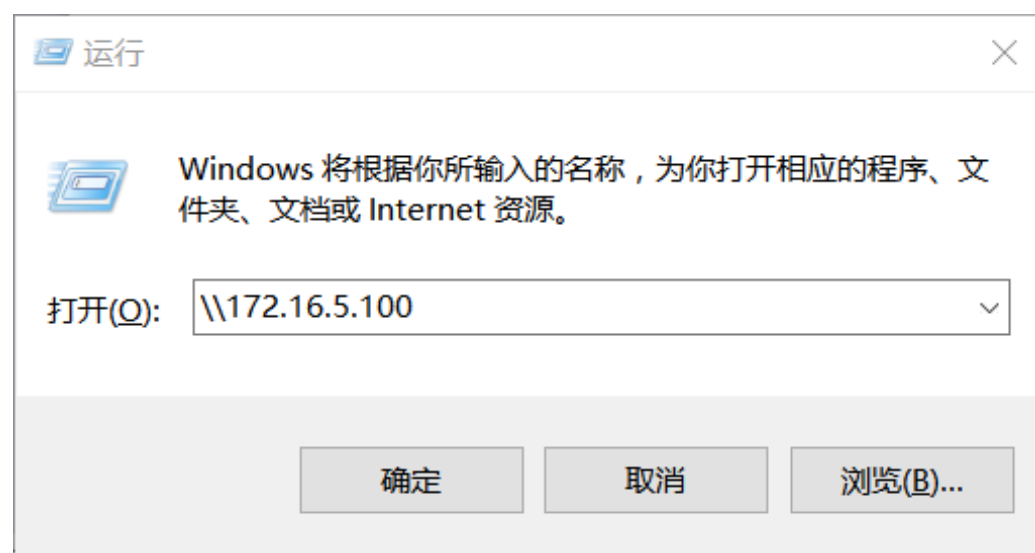
如果调查人员通过 psloggedon 命令找到有用户远程登录到系统中 ,那么同时也要了解该用户打开了什么文件。远程登录的用户总是要执行一些命令或者打开文件。公司环境中一般允许用户通过共享查看图片、歌曲等共享文件。net file、openfiles、psfile 等工具可以显示系统中被远程打开的文件。

获取远程登录打开的文件实验

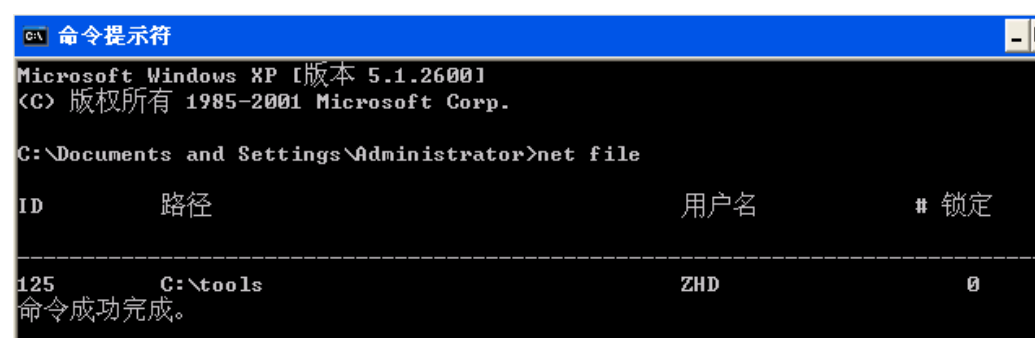
- 1、登录虚拟机系统。
- 2、打开虚拟机 cmd 命令窗口。



- 3、首先在本机通过 net use 连接虚拟机 , 访问虚拟机上共享的 tools 文件夹 , 命令 : \\ip , 下图的 ip 为虚拟机 ip , 然后点击确定 , 进入 tools 目录。



4、在虚拟机上获取通过 net use 远程登录访问的共享文件名和访问者信息，
命令：net file 和 openfiles (都需要管理员权限)。



从上图可看出，访问者为 ZHD，访问的共享文件为 C:\tools。

5、如果本机没有 net use 访问虚拟机共享文件，则列表为空。

```
C:\Documents and Settings\Administrator>net file  
列表是空的。
```

```
C:\Documents and Settings\Administrator>openfiles
```

信息：需要启用系统全局标志“维护对象列表”，才能看见本地打开的文件。有关详细信息，请参阅 `Openfiles /?`。

通过本地共享点远程打开的文件：

信息：没有找到打开的共享文件。

6、切换到 C:\tools\Pstools 目录，输入命令：psfile.exe，需要管理员权限。

```
C:\> 命令提示符  
  
C:\tools\Pstools>psfile.exe  
  
psfile v1.02 - psfile  
Copyright ?2001 Mark Russinovich  
Sysinternals  
  
Files opened remotely on R00T100R-58C7E0:  
  
[136] C:\tools  
      User:    ZHD  
      Locks:   0  
      Access:  Read
```

如果调查人员通过方法找到有用户远程登录到系统中，那么同时也要了解该用户打开了什么文件，以做进一步调查，前提是 net use 正处于连接状态。


4、域中共享的主机和文件

入侵者在获得系统访问权限之后，有时想要知道网络中还有哪些其他系统可以通过被入侵的系统访问。在调查中经常会碰到这类场景，形式各不相同。有时系统中创建了批处理文件，有时入侵者通过 SQL 注入执行 net view 命令（使用

浏览器,通过 Web 服务器、数据库服务器等给系统发命令)。如果通过 NetBIOS 通信和其他系统建立了连接(和登录系统或者通过共享连接类似),系统将会维护一个连接过的系统名字列表。通过查看缓存的名字列表,调查人员可以知道哪些系统已经受到影响。

获取域中共享的主机和文件实验

首先打开 cmd 命令,输入“net view”命令,查看共享主机,输入“net view \\主机名”,查看共享的文件。



```
管理员: 命令提示符
C:\WINDOWS\system32>net view
服务器名称                注解
-----
\\GBSK3ICVEMUDBXP
\\HACKER
\\HZ-PC
\\OPENWRT                  OpenWrt
\\PC-201605092054
\\PC-20161221BGWF
\\PC-20170208RRHB
\\SPSEC
\\XX00-PC
命令成功完成。

C:\WINDOWS\system32>net view \\HACKER
在 \\HACKER 的共享资源

共享名    类型    使用为    注解
-----
netshare  Disk
命令成功完成。

搜狗拼音输入法 全 :>
```

5、网络连接

一旦有报告说发生了安全事件,调查人员就应该收集针对被影响系统的网络连接信息。随着时间的消逝,连接信息会慢慢过期,事件越久,丢失的信息越多。调查人员在接触系统以后,通过初始的查看,可以确定攻击者是否还登陆在系统中。或者可能发现一个蠕虫、IRC 僵尸程序对外的连接,可能它们正在搜索其他入侵目标、正在进行自身的升级或者连接到一个入侵控制中心。连接信息可以提

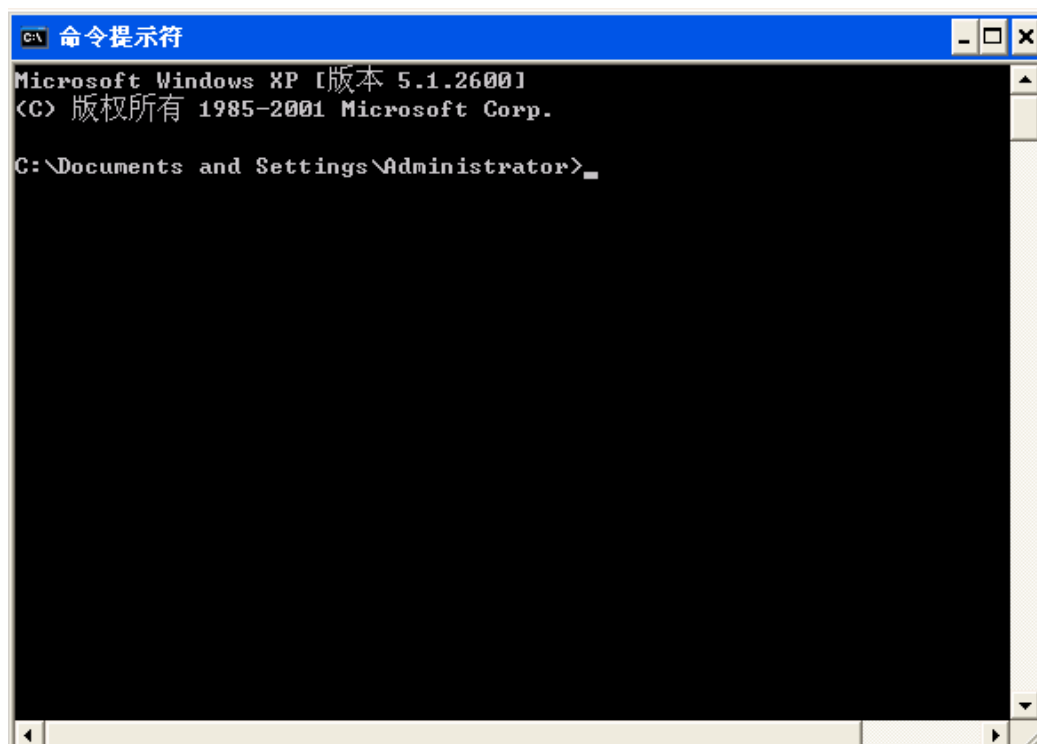
供重要的线索并为其他信息提供佐证。并非每个系统都安装了防火墙，尤其是防火墙也不会记录成功的进出连接信息。调查人员必须快速反应，在有限的时间内高效地收集需要的信息。

netstat

这个命令行工具简单而且直观地显示了 TCP 和 UDP 连接的状态、网络流量统计等信息。Netstat 最常用的方式是使用 -ano 选项开关，该选项设定程序显示 TCP/UDP 网络连接、侦听端口和使用网络连接的进程标识（PID）信息。例如，用户系统中一个高端口的客户进程连接到远程 80 端口就不正常，通常连接到 80 端口的应该是网络浏览器进程。Netstat 的 -r 选项将会显示路由表信息，并且可以看出哪些是系统的永久路由。这为调查人员提供了很有用的信息，系统管理员也可用来对系统排错。

获取网络连接状态实验

1、打开 cmd 命令窗口。



2、输入命令：netstat -ano。

```
C:\Documents and Settings\Administrator>netstat -ano

Active Connections

Proto Local Address           Foreign Address         State       PID
TCP    0.0.0.0:80              0.0.0.0:0               LISTENING   1520
TCP    0.0.0.0:135             0.0.0.0:0               LISTENING   928
TCP    0.0.0.0:445             0.0.0.0:0               LISTENING    4
TCP    0.0.0.0:3306            0.0.0.0:0               LISTENING  1604
TCP    0.0.0.0:3389            0.0.0.0:0               LISTENING   880
TCP    127.0.0.1:1026          0.0.0.0:0               LISTENING  5488
TCP    172.16.5.100:139        0.0.0.0:0               LISTENING    4
TCP    172.16.5.100:445        192.168.4.121:54501     ESTABLISHED  4
TCP    172.16.5.100:3389       192.168.4.121:54039     ESTABLISHED  880
UDP    0.0.0.0:445             *:*:                     716
UDP    0.0.0.0:500             *:*:                     716
UDP    0.0.0.0:4500            *:*:                     716
UDP    127.0.0.1:123           *:*:                     1020
UDP    127.0.0.1:1025          *:*:                     1020
UDP    127.0.0.1:1031          *:*:                     5612
UDP    127.0.0.1:1900          *:*:                     1124
UDP    172.16.5.100:123        *:*:                     1020
UDP    172.16.5.100:137        *:*:                     4
UDP    172.16.5.100:138        *:*:                     4
UDP    172.16.5.100:1900       *:*:                     1124
```

此命令用于显示活动的网络连接状态，包括查看端口占用情况。

3、输入命令：netstat -r。

```
C:\Documents and Settings\Administrator>netstat -r

Route Table
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x2 ...ea b6 36 84 1c a6 ..... Citrix PV Ethernet Adapter - 数据包计划程序微型
端口
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          172.16.5.1       172.16.5.100     10
127.0.0.0                  255.0.0.0        127.0.0.1        127.0.0.1        1
172.16.5.0                  255.255.255.0    172.16.5.100     172.16.5.100     10
172.16.5.100                255.255.255.255  127.0.0.1        127.0.0.1        10
172.16.255.255              255.255.255.255  172.16.5.100     172.16.5.100     10
224.0.0.0                  240.0.0.0        172.16.5.100     172.16.5.100     10
255.255.255.255             255.255.255.255  172.16.5.100     172.16.5.100     1
Default Gateway:          172.16.5.1
=====
Persistent Routes:
None
```

此命令用于显示路由表信息，并可以看出哪些是系统的永久路由（手动指定的网关）。

6、进程信息

调查人员对可能的被入侵系统的运行进程信息总是很关注,当然有时也会忽略。通过任务管理器查看进程信息时,可以看到每个进程的一些信息。不过。很多需要收集的信息并不能通过任务管理器看到,例如:

- ◆ 可执行文件的全路径
- ◆ 启动进程时的命令行参数信息
- ◆ 进程运行的时间
- ◆ 进程运行的安全/用户上下文环境
- ◆ 进程加载了哪些模块
- ◆ 进程的内存数据内容

为什么需要这些信息呢?如果在任务管理器中查看进程信息,我们怎么知道哪个进程是“可疑”的?一个简单的方法就是查看可执行文件的全路径。

Tasklist

该工具提供输出表格、CSV、列表等不同格式的选项。/v 选项参数提供进程的最多信息,包括程序名称(没有全路径)、PID、进程名、会话数量、进程状态、用户名、窗口标题。使用/svc 参数也可以列出进程相关的服务信息。

Pslist

Pslist 显示系统中运行进程的基本信息,包括每个进程已经运行的时间(用户模式和核心模式)。-x 选项显示线程及进程使用的内存详细信息。不过,pslist 没有提供执行进程的路径信息、命令行信息,也没有提供用户信息。

Listdlls

Listdlls 显示进程使用的动态链接库,同时还会显示加载模块镜像的全路径

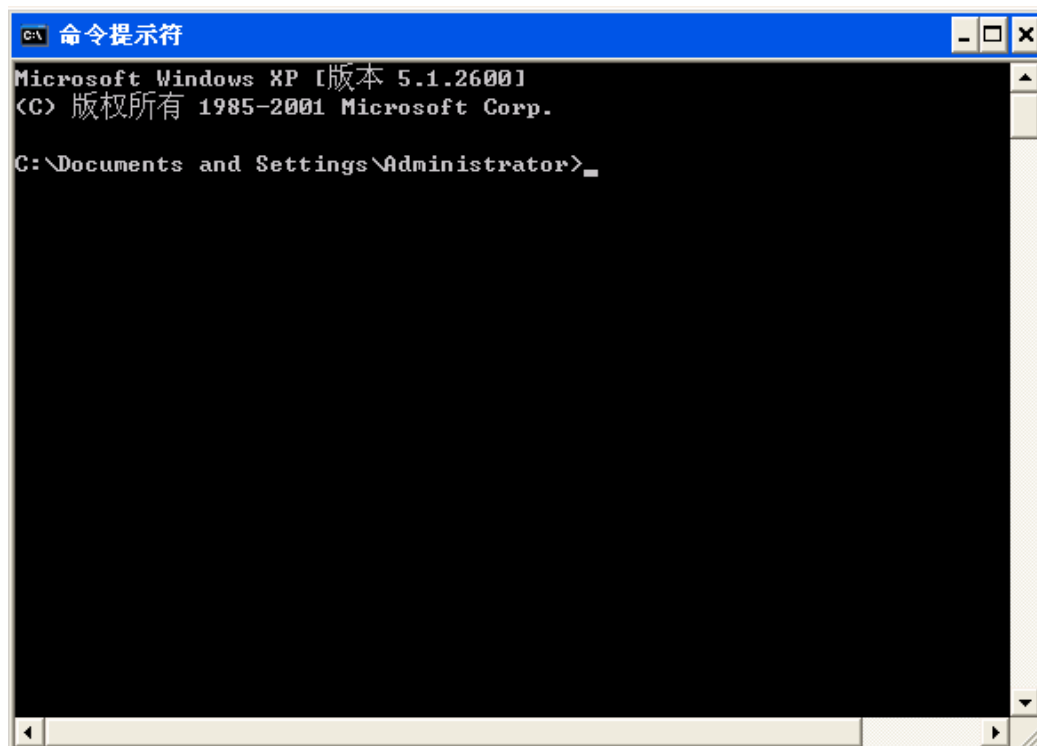
及内存中加载的动态链接库版本与磁盘上镜像版本的不同。这个信息对调查人员非常有用，因为每个程序都会加载或者“引入”特定的动态链接库。Listdlls 还可以显示加载特定动态链接库的进程（使用-d dllname），通过这个命令可以查看其他使用该动态链接库的进程。

Handle

Handle 显示系统中进程打开的句柄，包括打开的文件、端口、注册表项、线程等。Handle 有几个可用的选项参数，-a 显示所有的句柄，-u 显示某用户的句柄。

获取进程信息实验

1、打开 cmd 命令窗口。



2、输入命令：tasklist，列举所有进程及其 id 和内存使用情况。

```

C:\Documents and Settings\Administrator>tasklist

 图像名                      PID 会话名      会话#      内存使用
=====
System Idle Process          0 Console      0          28 K
System                        4 Console      0          296 K
smss.exe                     572 Console      0          412 K
csrss.exe                     636 Console      0         4,904 K
winlogon.exe                  660 Console      0        10,420 K
services.exe                  704 Console      0         4,080 K
lsass.exe                     716 Console      0         5,956 K
svchost.exe                   880 Console      0         5,132 K
svchost.exe                   928 Console      0         4,244 K
svchost.exe                  1020 Console      0        21,820 K
svchost.exe                  1064 Console      0         2,972 K
svchost.exe                  1124 Console      0         4,568 K
logonui.exe                   1164 Console      0         3,832 K
spoolsv.exe                   1384 Console      0         4,728 K
Apache.exe                   1520 Console      0        15,656 K
mysqld-nt.exe                 1604 Console      0         5,896 K
XenGuestAgent.exe            1752 Console      0        28,172 K
vmiprvse.exe                  220 Console      0         5,452 K
Apache.exe                    224 Console      0        40,748 K
alg.exe                       5488 Console      0         3,512 K
  
```

3、切换至 C :\tools\Pstools 目录 , 输入命令 : pslist.exe , 功能和 tasklist 类似。

```

C:\tools\Pstools>pslist.exe

pslist v1.28 - Sysinternals PsList
Copyright ? 2000-2004 Mark Russinovich
Sysinternals

Process information for ROOTT00R-58C7E0:

Name          Pid Pri Thd  Hnd  Priv      CPU Time  Elapsed Time
-----
Idle           0   0   1    0    0      4:58:01.562  0:00:00.000
System         4   8  63  515    0      0:00:28.765  0:00:00.000
smss           572  11   2   28   148      0:00:00.203  5:04:46.496
csrss          636  13  10  1362  2316      0:00:03.109  5:04:45.043
winlogon       660  13  18  451  7496      0:00:11.906  5:04:44.808
services       704   9  16  264  2040      0:00:01.734  5:04:44.527
lsass          716   9  20  354  3868      0:00:14.859  5:04:44.496
svchost        880   8  25  231  2924      0:00:27.671  5:04:44.105
svchost        928   8  11  263  1880      0:00:01.062  5:04:43.699
svchost       1020   8  58  1360  15752      0:00:43.046  5:04:43.574
svchost       1064   8   4   56  1236      0:00:00.187  5:04:43.511
svchost       1124   8  13  204  1868      0:00:00.093  5:04:41.339
logonui       1164   8   4  156  3580      0:00:04.000  5:04:41.246
spoolsv       1384   8  10  129  3168      0:00:00.296  5:04:40.605
Apache        1520   8   4   94  13628      0:00:01.265  5:04:37.402
mysqld-nt     1604   8   6  174  19632      0:00:00.125  5:04:37.183
  
```

4、输入命令 : listdlls , 此命令来列举进程以及其所使用的的 dll 文件。


```

CA 命令提示符
spoolsv.exe pid: 1384
Command line: C:\WINDOWS\system32\spoolsv.exe

Base      Size      Version    Path
0x01000000 0x10000    5.01.2600.2180 C:\WINDOWS\system32\spoolsv.exe
0x7c920000 0x94000    5.01.2600.2180 C:\WINDOWS\system32\ntdll.dll
0x7c800000 0x11c000    5.01.2600.2180 C:\WINDOWS\system32\kernel32.dll
0x77be0000 0x58000    7.00.2600.2180 C:\WINDOWS\system32\msvcrt.dll
0x77da0000 0xa9000    5.01.2600.2180 C:\WINDOWS\system32\ADVAPI32.dll
0x77e50000 0x91000    5.01.2600.2180 C:\WINDOWS\system32\RPCRT4.dll
0x77ef0000 0x46000    5.01.2600.2180 C:\WINDOWS\system32\GDI32.dll
0x77d10000 0x8f000    5.01.2600.2180 C:\WINDOWS\system32\USER32.dll
0x5cc30000 0x26000    5.01.2600.2180 C:\WINDOWS\system32\ShimEng.dll
0x58fb0000 0x1ca000    5.01.2600.2180 C:\WINDOWS\AppPatch\AcGenral.DLL
0x76b10000 0x2a000    5.01.2600.2180 C:\WINDOWS\system32\WINMM.dll
0x76990000 0x13c000    5.01.2600.2180 C:\WINDOWS\system32\ole32.dll
0x770f0000 0x8c000    5.01.2600.2180 C:\WINDOWS\system32\OLEAUT32.dll
0x77bb0000 0x15000    5.01.2600.2180 C:\WINDOWS\system32\MSACM32.dll
0x77bd0000 0x8000     5.01.2600.2180 C:\WINDOWS\system32\VERSION.dll
0x773a0000 0x7f1000    6.00.2900.2180 C:\WINDOWS\system32\SHELL32.dll
0x77f40000 0x76000    6.00.2900.2833 C:\WINDOWS\system32\SHLWAPI.dll
0x759d0000 0xae000    5.01.2600.2180 C:\WINDOWS\system32\USERENV.dll
0x5adc0000 0x37000    6.00.2900.2180 C:\WINDOWS\system32\UxTheme.dll
0x76300000 0x1d000    5.01.2600.2180 C:\WINDOWS\system32\IMM32.DLL
0x62c20000 0x9000     5.01.2600.2180 C:\WINDOWS\system32\LPK.DLL

```

5、输入命令：handle，此命令列出进程对应的权限以及该进程的句柄信息

(句柄：访问进程获得的指针，使用完毕必须释放，与 PID 不同)。

```

CA 命令提示符
25C: Section \BaseNamedObjects\__R_000000000007_SMem__
-----
Apache.exe pid: 1520 NT AUTHORITY\SYSTEM
50: File <RW-> C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_659
5b64144ccf1df_6.0.2600.2180_x-ww_a84f1ff9
54: File <RW-> C:\tools\PHPnow-1.5.6\Apache-20
84: File <RWD> C:\tools\PHPnow-1.5.6\Apache-20\logs\error.log
EC: File <RWD> C:\tools\PHPnow-1.5.6\Apache-20\logs\access.log
F0: File <RWD> C:\tools\PHPnow-1.5.6\Apache-20\logs\default-error_log
180: Section \BaseNamedObjects\ZendOptimizer.SharedMemoryArea@SYSTEM@118
3570551
1AC: Section \BaseNamedObjects\ShimSharedMemory
-----
mysqld-nt.exe pid: 1604 NT AUTHORITY\SYSTEM
1C4: File <RW-> C:\tools\PHPnow-1.5.6\MySQL-5.0.90\data
1D0: File <RW-> C:\tools\PHPnow-1.5.6\MySQL-5.0.90\data\roottoor-58c7e0.err
1D4: File <RW-> C:\tools\PHPnow-1.5.6\MySQL-5.0.90\data\roottoor-58c7e0.err
-----
XenGuestAgent.exe pid: 1752 NT AUTHORITY\SYSTEM
C: File <RW-> C:\WINDOWS\system32
28: Section \BaseNamedObjects\ShimSharedMemory
48: File <RW-> C:\WINDOWS\WinSxS\x86_Microsoft.UC80.CRT_1fc8b3b9a1e18e3b_8
.0.50727.3053_x-ww_b80fa8ca

```

查看进程信息，可以在电脑被入侵时找到可疑的进程，结束进程或进一步调查。

7、进程到端口的映射

系统中存在打开的网络连接的时候，一定是有进程在使用这个连接。也就是说，每一个网络连接和开放的端口都有进程相关联。有几个工具可以用来调查和获取这种进程到端口的映射信息。

Netstat

Netstat 提供-o 选项来显示网络连接对应的进程标识。

Fport

Fport 一直是 Windows 系统中用来获取进程到端口映射的首选工具之一。它的输出简明易懂，不过该工具需要管理员账户运行，这在使用不具有管理员权限的普通账户进行调查会是个问题。

Openports

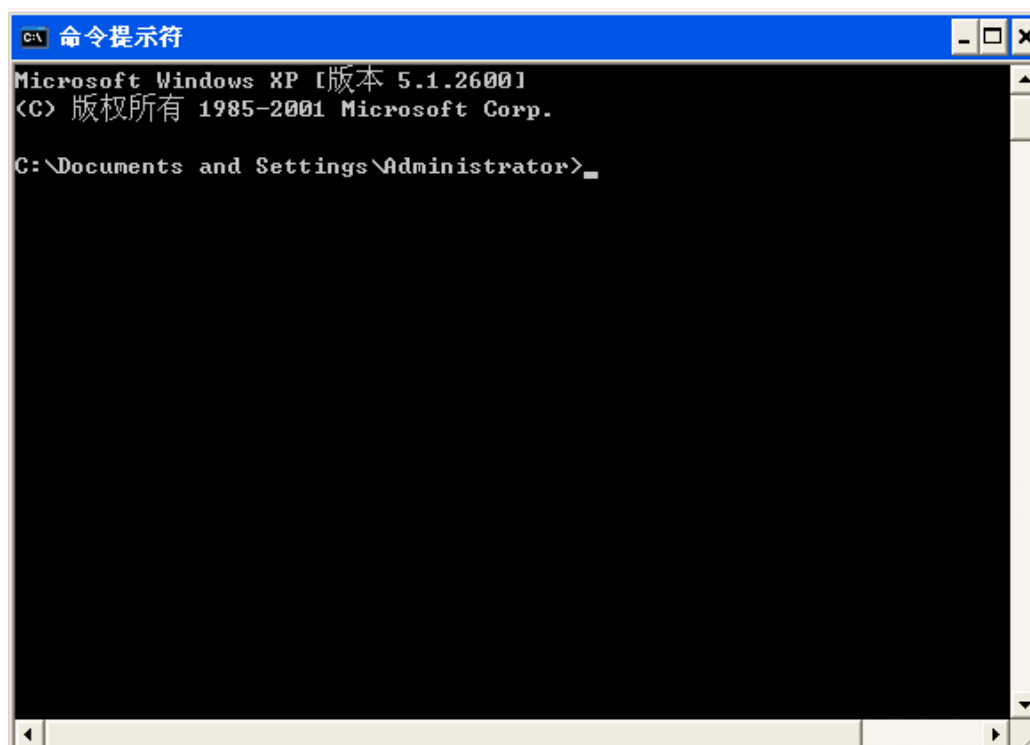
Openports 也许是 Windows 系统中获取进程到端口映射信息的最好工具。该工具允许输出为多种格式，包括 netstat 风格、fport 风格和 CVS 格式，并且不需要管理员权限来执行。使用-f port 选项，可以输出为 fport 风格，显示进程标识、进程名称、端口号、协议（TCP/UDP）和执行程序的路径。

Nmap

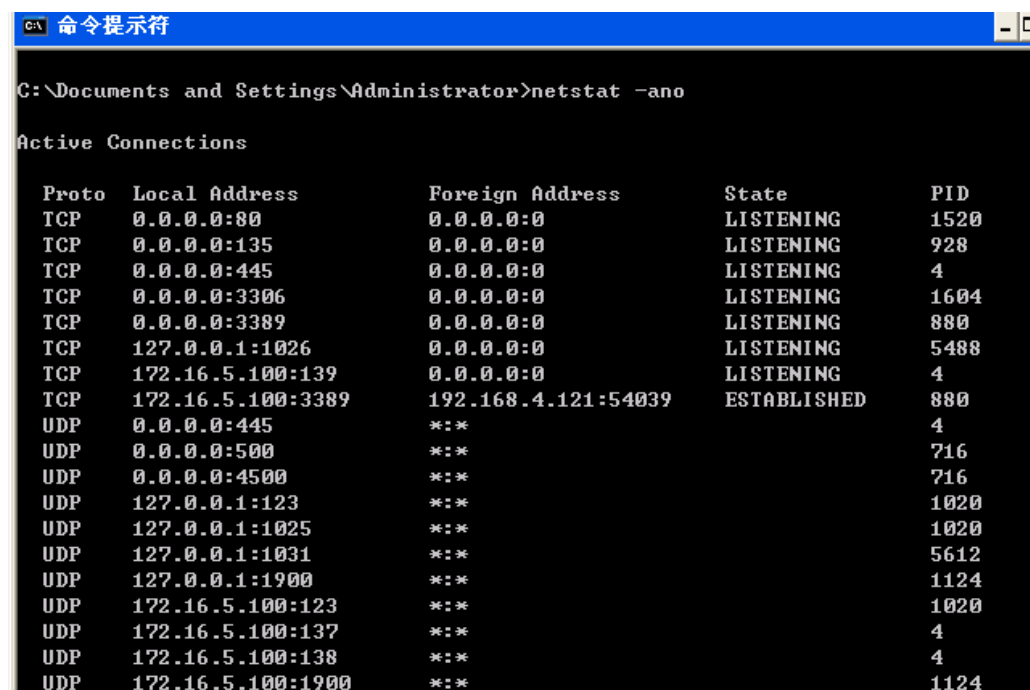
Nmap 扫描可以发现处于侦听模式的开放端口，侦听的服务可能是认证服务、Web 服务、FTP 服务，但也可能是后门。如果发现系统中有端口开放，但是不能通过 netstat 或其他工具显示该端口，进程到端口映射程序也不能显示，那就可以确定系统有异常。这时还要再次验证扫描结果以确认扫描的是正确的系统。如果问题还存在 那么大致可以确定存在一个内核级的木马，也就是 Rootkits（后面的章节会介绍）。

获取进程到端口映射实验

1、打开 cmd 命令窗口。

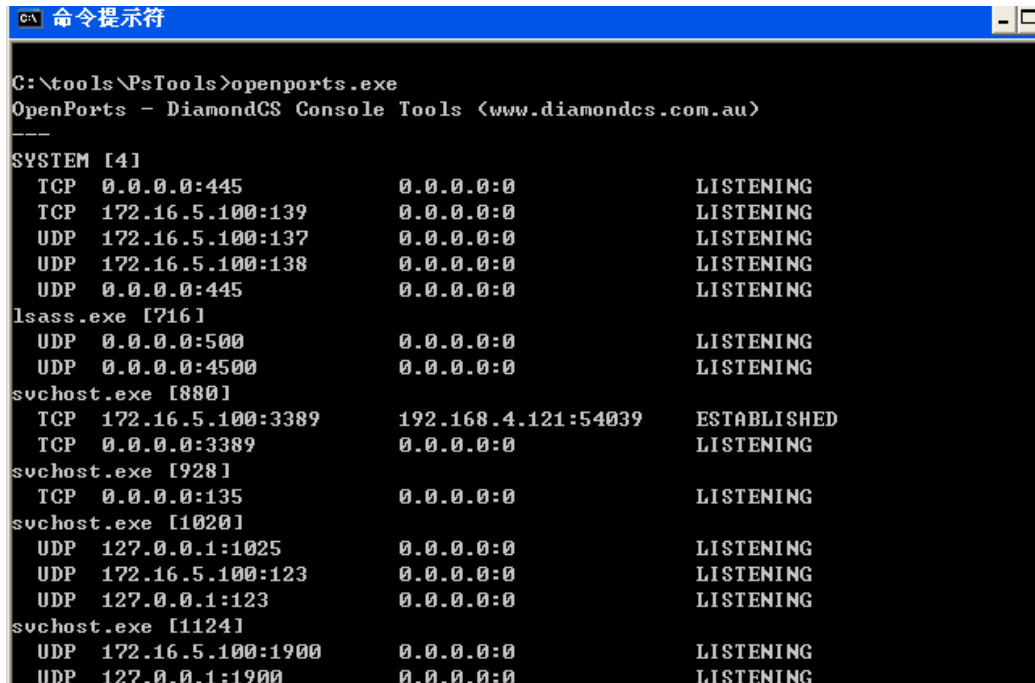


2、输入命令：netstat -ano，查看进程到端口的映射情况



3、切换至 C :\tools\Pstools 目录，输入命令：openports.exe，查看进程

及其端口。



```
C:\tools\PsTools>openports.exe
OpenPorts - DiamondCS Console Tools (www.diamondcs.com.au)
---
SYSTEM [4]
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 172.16.5.100:139 0.0.0.0:0 LISTENING
UDP 172.16.5.100:137 0.0.0.0:0 LISTENING
UDP 172.16.5.100:138 0.0.0.0:0 LISTENING
UDP 0.0.0.0:445 0.0.0.0:0 LISTENING
lsass.exe [716]
UDP 0.0.0.0:500 0.0.0.0:0 LISTENING
UDP 0.0.0.0:4500 0.0.0.0:0 LISTENING
svchost.exe [880]
TCP 172.16.5.100:3389 192.168.4.121:54039 ESTABLISHED
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING
svchost.exe [928]
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
svchost.exe [1020]
UDP 127.0.0.1:1025 0.0.0.0:0 LISTENING
UDP 172.16.5.100:123 0.0.0.0:0 LISTENING
UDP 127.0.0.1:123 0.0.0.0:0 LISTENING
svchost.exe [1124]
UDP 172.16.5.100:1900 0.0.0.0:0 LISTENING
UDP 127.0.0.1:1900 0.0.0.0:0 LISTENING
```

系统中存在打开的网络连接的时候，一定是有进程在使用这个连接。也就是说，每个网络连接和开放的端口都有进程相关联。调查人员可以通过这种方法察觉可以的进程和端口，可以进一步调查取证。

8、进程内存

开机系统会有一些列的运行进程，本质上任何一个进程都可能具有恶性性。当系统中的进程运行时，进程名基本上会和执行程序的文件名一致。以 Windows 为例，文件可以任意命名。坏人不会将恶意代码起一个容易辨认的名字，他们经常会起一个不会引起注意的名字，或者会使用一个 Windows 正常程序的名字来伪装。

调查过程中，调查员更关心的可能是某个特殊的进程而不是系统中所有进程，而且对内存中该进程所使用的内存信息更感兴趣。现在有办法提取进程使用的完整内存数据，不仅包括物理内存中的内容，还包括虚拟内存和页交换文件中的数据。

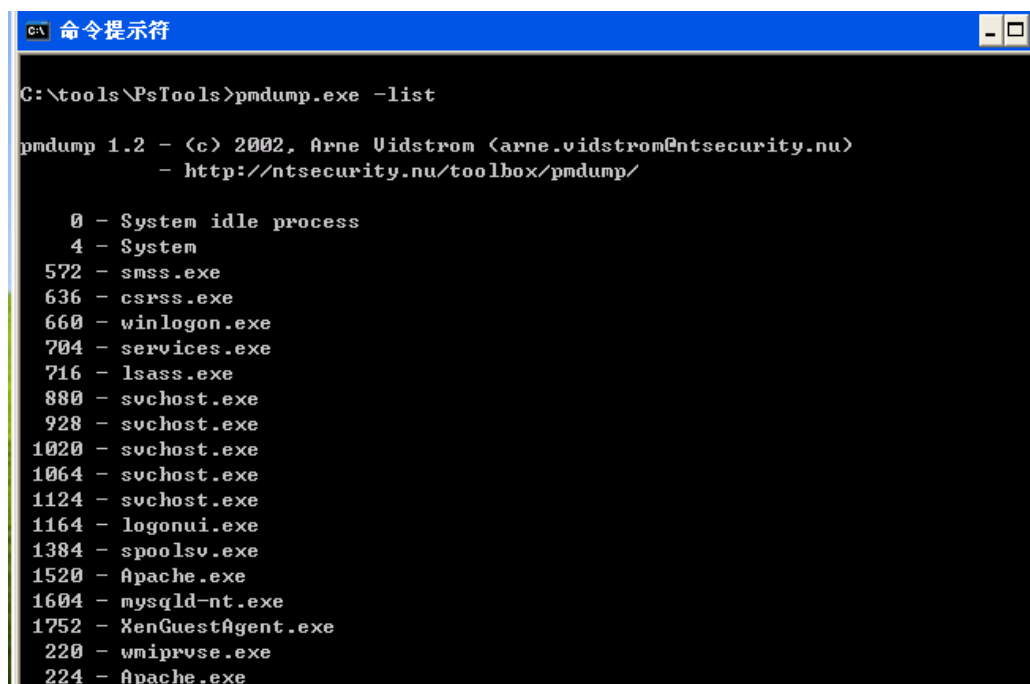
一旦发现并确定了可疑进程，调查员就需要知道该进程的更多信息。这可以通过获取进程的内存来得到。这里有几个工具可以完成这项任务：Pmdump.exe、Procdump.exe、Userdump.exe。对内存的收集和讨论更多会在后面的章节介绍。

获取进程转储文件实验

1、打开 cmd 命令窗口，切换到 C:\tools\PsTools 目录。



2、输入命令 :pmdump.exe -list 列出所有运行的进程与其对应的 pid。

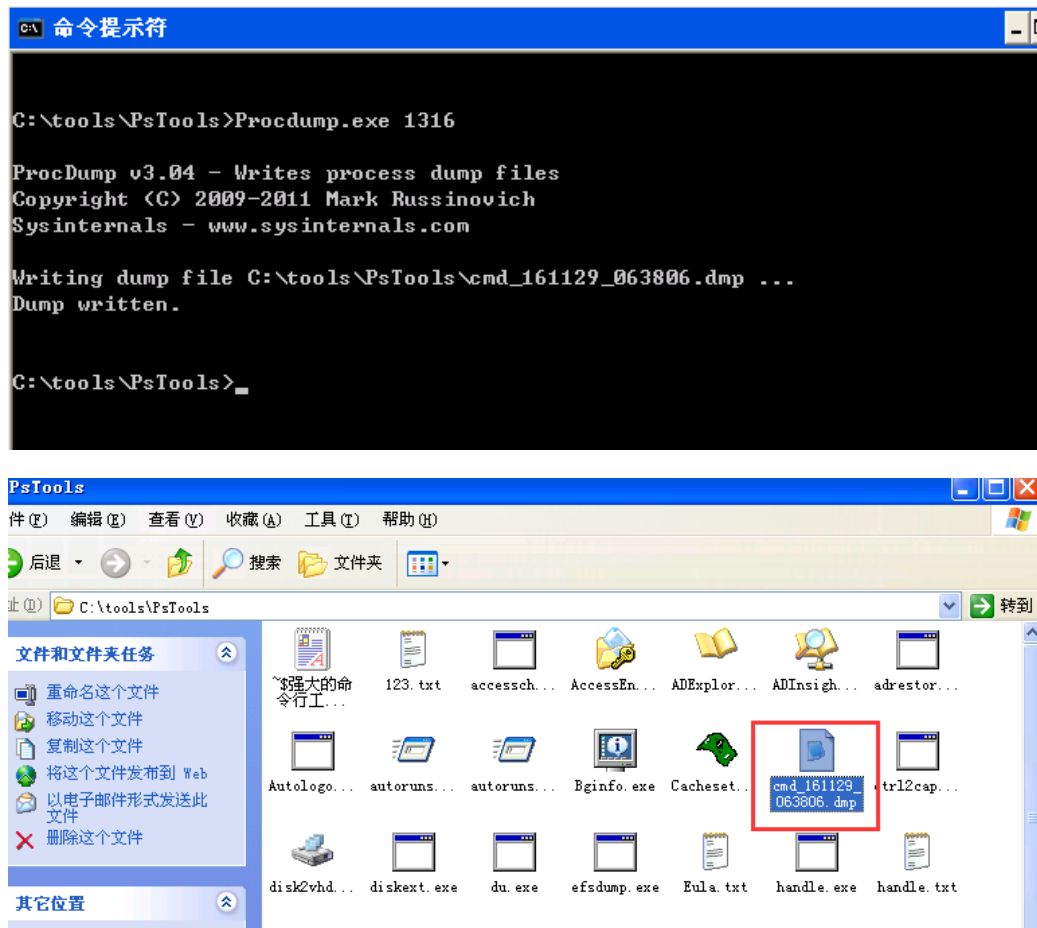


3、输入命令：pmdump.exe PID filename 可以将内存转储为文件。

pmdump.exe 工具可以在不停止进程的情况下获取进程的完整内存镜像。在获

取的过程中，进程的内存数据会发生改变，所以产生的是一个“模糊的”进程内存镜像。pmdump.exe 输出的文件不能使用调试工具来分析。

4、输入 procdump.exe PID 可以将进程内存转储为文件，保存在 procdump.exe 根目录下。进程名可以用 tasklist 获取。



5、切换到 C : \tools\userdump 目录，输入命令：userdump.exe -p ，列出进程 ID 和进程名。

```
C:\>命令提示符

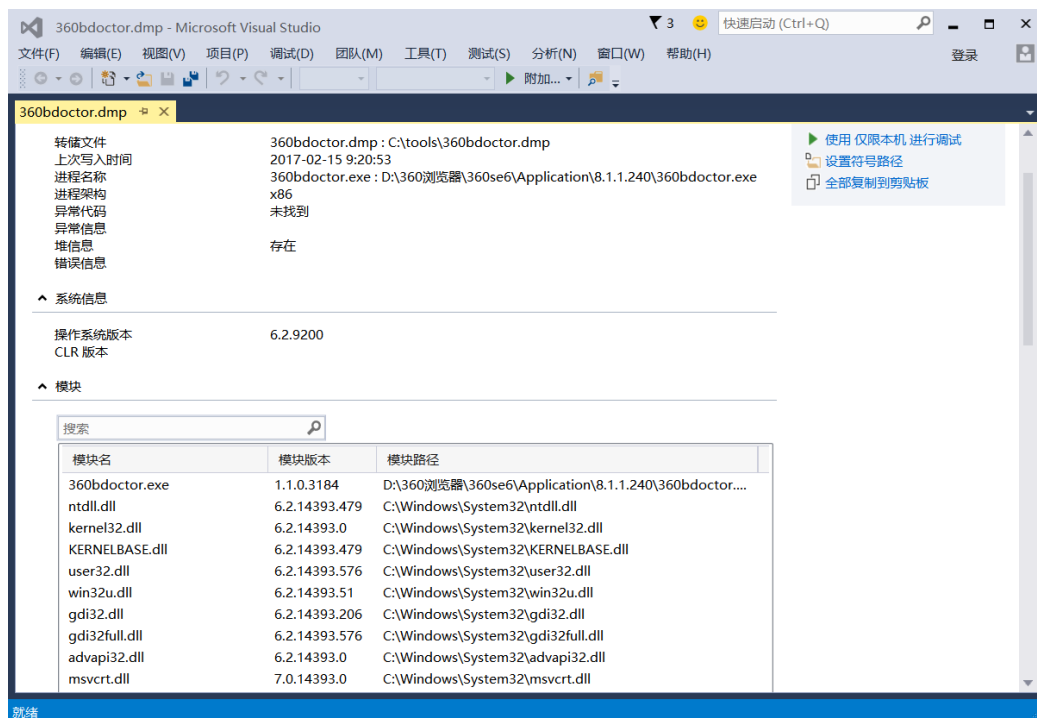
C:\tools\PsTools>cd C:\tools\userdump

C:\tools\userdump>userdump.exe -p
User Mode Process Dumper (Version 3.0)
Copyright (c) 1999 Microsoft Corp. All rights reserved.

  0 System Idle Process
  4 System
572 smss.exe
636 csrss.exe
660 winlogon.exe
704 services.exe
716 lsass.exe
880 svchost.exe
928 svchost.exe
1020 svchost.exe
1064 svchost.exe
1124 svchost.exe
1164 logonui.exe
1384 spoolsv.exe
1520 Apache.exe
1604 mysqld-nt.exe
1752 XenGuestAgent.exe
220 wmiprvse.exe
```

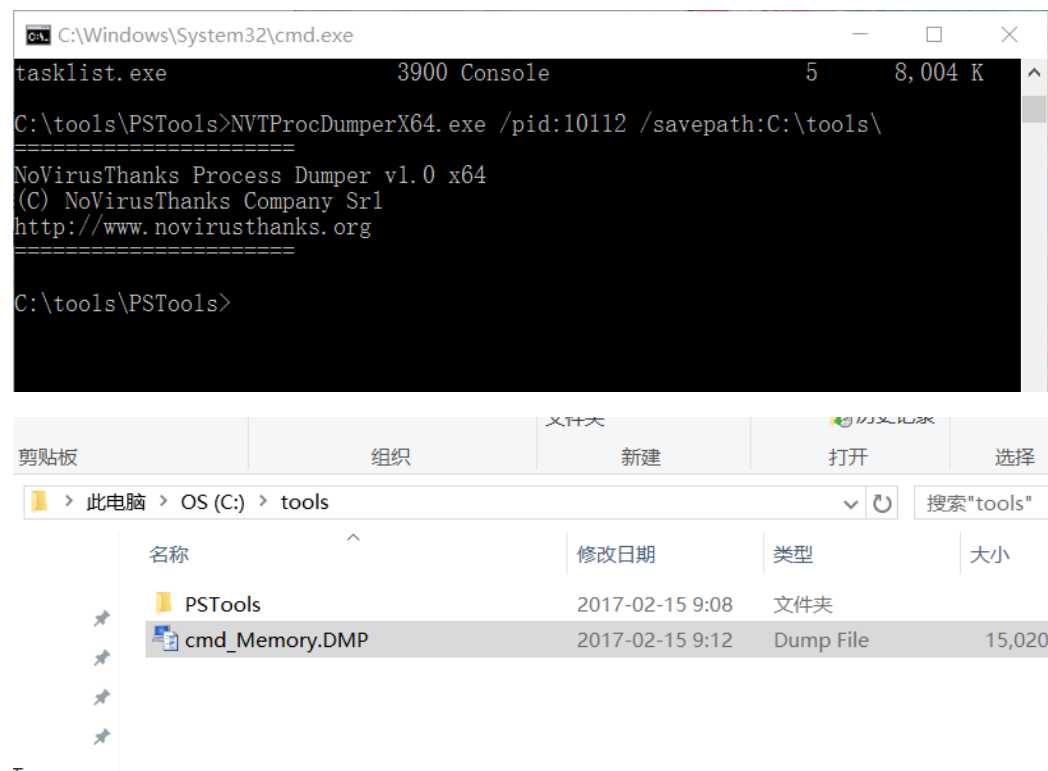
6、userdump.exe PID filename 命令可以将进程内存转储为文件。

userdump.exe 工具可以快速生成进程的内存镜像，既不用附加调试器，也不会终止进程，而且 userdump.exe 生成的内存镜像可以使用 Microsoft 提供的调试器进行调试。



7、切换到 NVTProcDumper.exe 所在目录，输入命令：

NVTProcDumperX64.exe /pid : 100 /savepath : C : \tools\.



NVTProcDumper 是一个命令行进程转储工具，可以将某个进程的内存信息转储到一个文件，稍后可以用 Debugging Tools 工具分析。

9、网络状态

对调查人员来说，系统中网卡连接的状态也很重要。例如，现在的笔记本都带内置的无线网卡，调查中可能需要确认系统是否连接到无线网络，分配的 IP 地址是多少。在系统获取之前查询网卡的状态对以后的调查会很有帮助。

Ipconfig

Ipconfig 可以用来显示网卡信息及其状态。该命令最有用的参数是/all，该参数显示系统中网卡的网络配置，包括网卡状态，是否使用 DHCP、当前 IP 地址等。

无线接入点可以用来连接到组织网络中，也可以被一些人用来窃取网络中的信息。

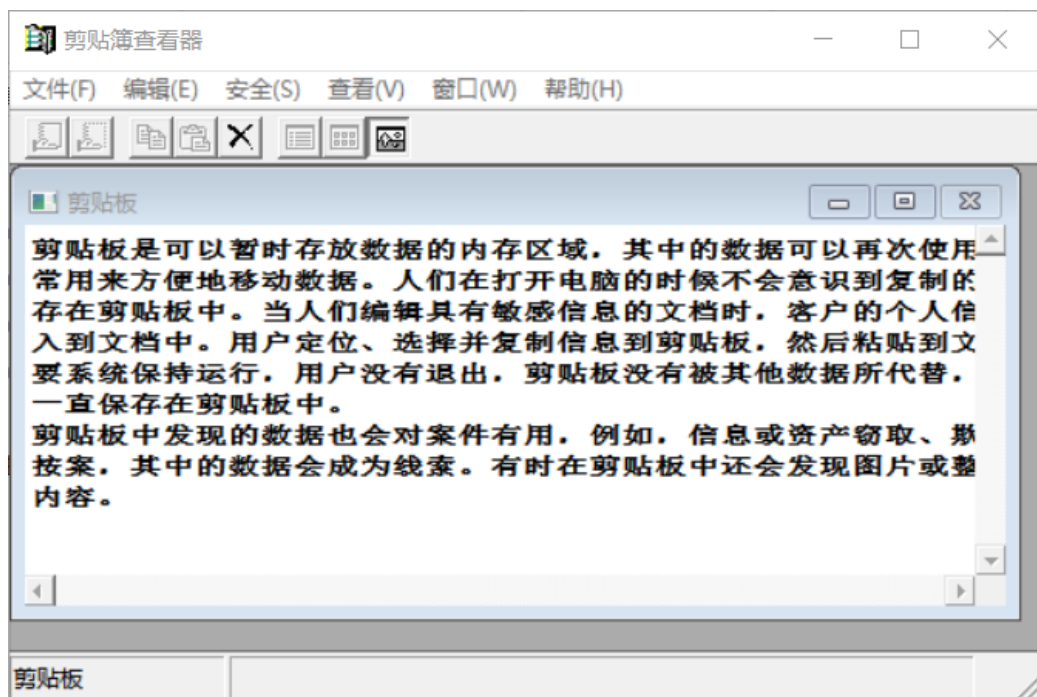
10、剪贴板内容

剪贴板是可以暂时存放数据的内存区域，其中的数据可以再次使用。剪贴板常用来方便地移动数据。人们在打开电脑的时候不会意识到复制的数据会保存在剪贴板中。当人们编辑具有敏感信息的文档时，客户的个人信息需要加入到文档中。用户定位、选择并复制信息到剪贴板，然后粘贴到文档中。只要系统保持运行，用户没有退出，剪贴板没有被其他数据所代替，则数据会一直保存在剪贴板中。

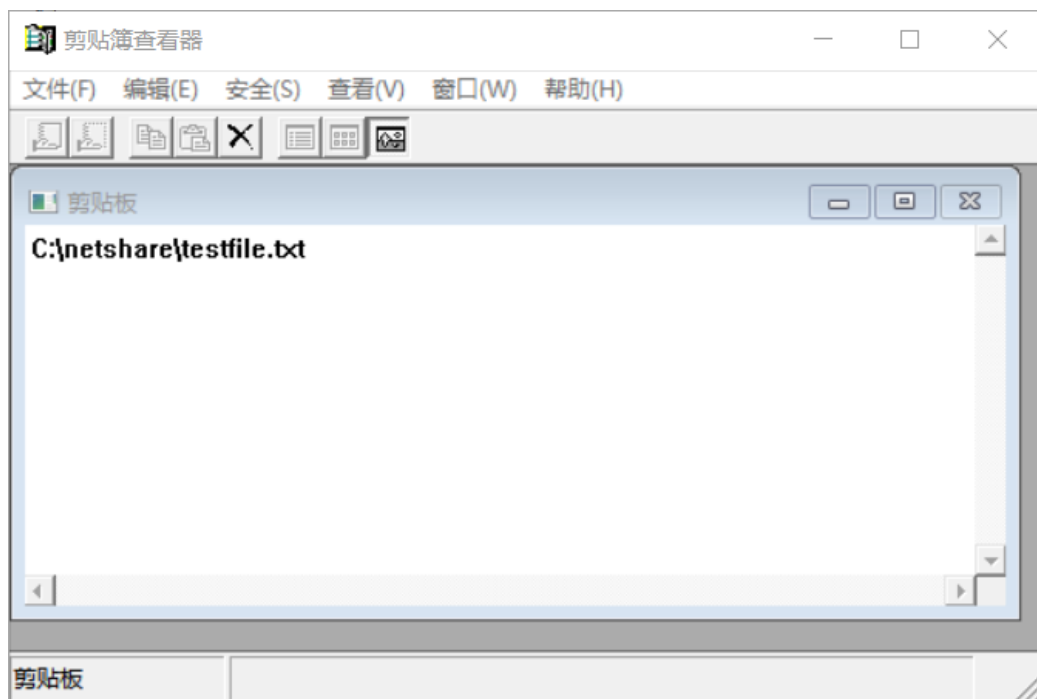
剪贴板中发现的数据也会对案件有用，例如，信息或资产窃取、欺诈和骚扰按案，其中的数据会成为线索。有时在剪贴板中还会发现图片或整段的文章内容。

获取剪贴板数据实验

1、首先复制一段文字，模拟剪贴板上的数据，再打开 clipbrd.exe 工具。



2、然后复制一个文件，再打开 clipbrd.exe，可以看到文件的路径。



11、服务/驱动信息

根据注册表中的配置，在系统启动的时候服务和驱动也会自动启动。大部分用户不会看到系统中作为进程运行的这些服务，因为进程中并没有服务的明显标志（通过任务管理器可以看到进程的运行，但不知是何服务），但是服务肯定是在运行。不是所有的服务都是通过用户或系统管理员安装。一些恶意软件会将自己安装为服务，甚至是系统驱动。

12、命令行历史

假设一个计算机调查现场，系统正开着且可以看到屏幕上有几个命令行窗口。这种情况下，线索可能就在用户输入的命令中，如 ftp 或 ping。如果用户输入 cls 命令来清除窗口，就不能使用滚动条来查看刚刚输入的命令。不过，可以使用 doskey /history 命令来显示前面输入的命令情况。在实际情况中，几乎不会碰到调查现场运行的计算机命令行窗口是打开的。但这并不意味着以后不会发生。

获取命令行历史实验

- 1、打开 cmd 命令窗口。

```
C:\ 命令提示符

C:\Documents and Settings\Administrator>_
```

2、输入命令：doskey /history 列出之前所有 dos 命令。

```
C:\ 命令提示符

C:\Documents and Settings\Administrator>doskey /history
net file
openfiles
net file
openfiles
nbtstat -c
nbtstat -a
nbtstat -s
nbtstat -S
nbtstat -c
netstat -ano
netstat -r
tasklist
cls
netstat -ano
openports
cls
doskey /history

C:\Documents and Settings\Administrator>_
```

13、映射的驱动器

调查过程中，也许需要掌握系统中映射的驱动器或共享来自哪里。映射可能由用户创建，可能出自不良意图。更进一步，也许从文件系统或注册表中不能发现这些映射的共享连接信息，不过这些驱动器映射动态信息还是可以与前面获取的网络连接信息相关联。

14、网络共享

除了调查系统中使用的网络资源之外，还需要获取系统中共享给网络的资源。

系统中共享的信息可以通过以下注册表键得到：

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Lanmanserver\Shares

也可以在开机取证时运行类似于 share.exe 的命令行工具得到。

Net share

Net share 不带参数时显示本地计算机上所有共享资源的信息。

获取网络共享实验

- 1、打开 cmd 命令窗口。
- 2、输入命令：net share，获取系统中共享给网络的资源。



注册表中共享信息位置：

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Lanmanserver\Shares

