Memory Forensics

Traditional Forensics

- Consists of
  - Install a write blocker
  - Take an image of the media
  - Make a copy of the image
  - Verify the copy
  - Analyze the image
  - Collect evidence
  - Maintain chain of custody

"Live" Forensics

- Traditional does not provide the complete picture
- Malware
- Processes
- Connections
- Memory

Limitations of "Traditional" Forensics

- All data is not preserved
- Presence of malware *invalidates* and weakens evidence admissibility
- How do you proceed when a "box" has a BSOD?
  - Key information can be lost if traditional forensics is used

“Live” Forensics

- Analyzing information *before* carrying out the traditional approach.
  - Capturing volatile memory
    - RAM
    - Process antecedence
      - Identify running context
    - Current connections
      - Remote hack?
    - Spawned processes
    - Handles
      - Registry
      - Files
      - etc

Examples of the Trojan Defense

- First appeared in the UK 2003
  - Case 1:
    - Suspect claimed a Trojan had conducted an attack and then after the attack erased itself
      - Jury agreed and he was acquitted
      - Set a precedence and set UK investigations back a large amount
  - Case 2:
    - Child pornography suspect
      - Cleared after 11 Trojan Programs were found on suspects computer

Examples of the Trojan Defense (cont)

- Case 3: July 2009
  - Child pornography suspect
  - Cleared after claiming Trojan downloaded images
  - Investigators did not collect “live” memory
- Expect to see more of this in the future
- Once word gets out, more defence teams will use it

Importance of collecting “live” memory

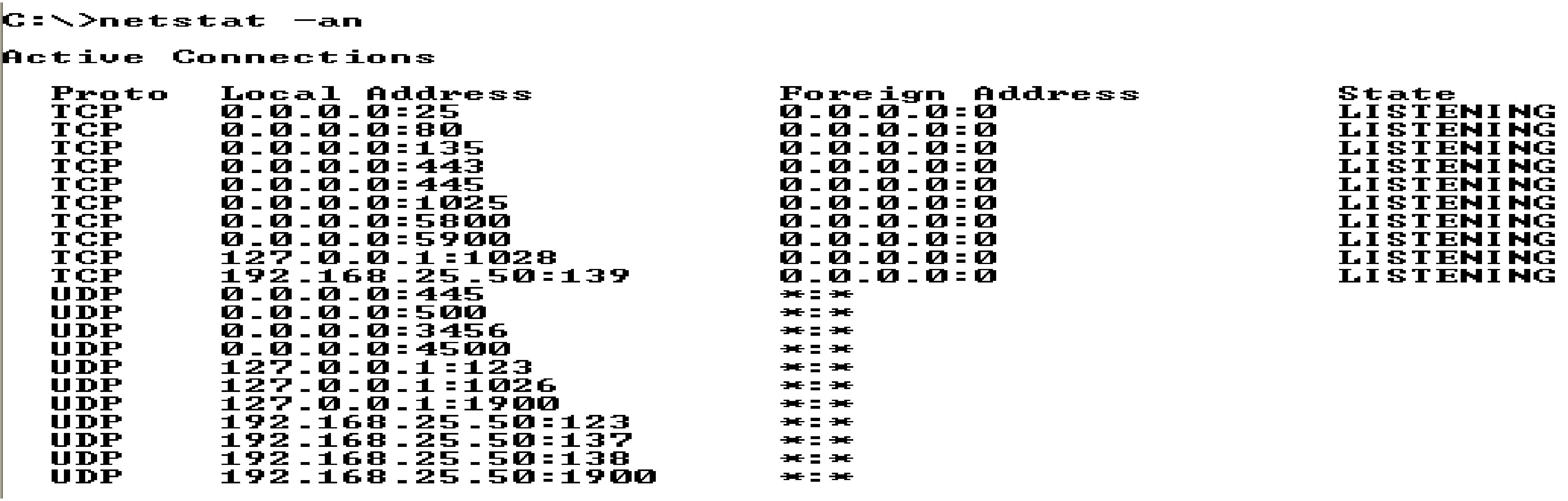
- Systems have large amounts of RAM today
- Defense team can argue that failing to collect the memory could
  - Have missed key *exculpatory* evidence
  - Could have cleared the suspect
- Expert witness cannot refute this
  - If the memory was not taken then it is gone *Forever!*
- Can cast that shadow of a doubt in the judges or jury’s mind

Volatile Data

- System date and time
- Current network connections
- Open ports
- Processes that opened ports
- Cached NetBIOS names
- Users currently logged on
- Internal routing
- Running processes and services
- Open files
- Process memory dumps

Current network connections and Open ports

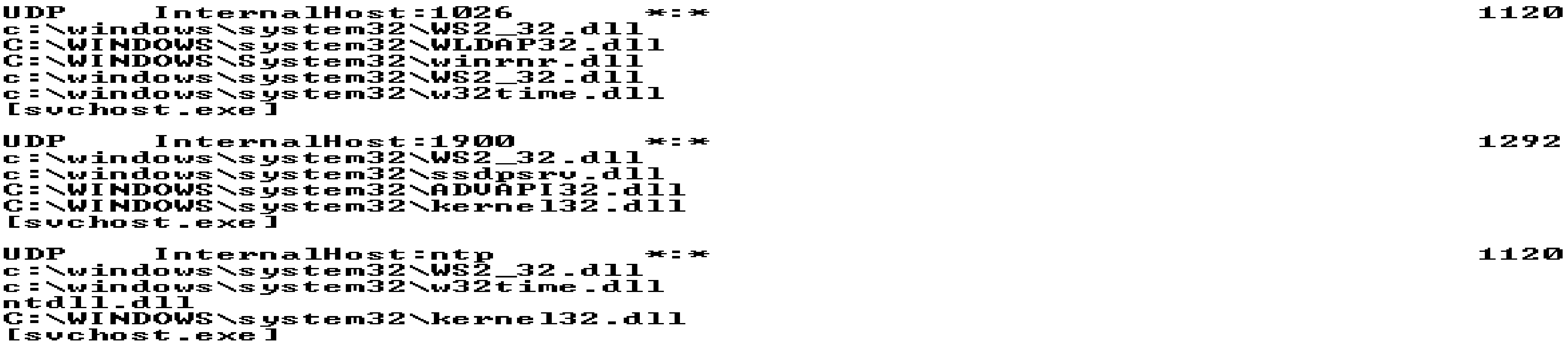
- To display these we use the *netstat* command



```
C:\>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:25             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5800           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5900           0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1028         0.0.0.0:0              LISTENING
  TCP    192.168.25.50:139      0.0.0.0:0              LISTENING
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:3456           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1026         *:*
  UDP    127.0.0.1:1900         *:*
  UDP    192.168.25.50:123      *:*
  UDP    192.168.25.50:137      *:*
  UDP    192.168.25.50:138      *:*
  UDP    192.168.25.50:1900     *:*
```

Processes that opened ports

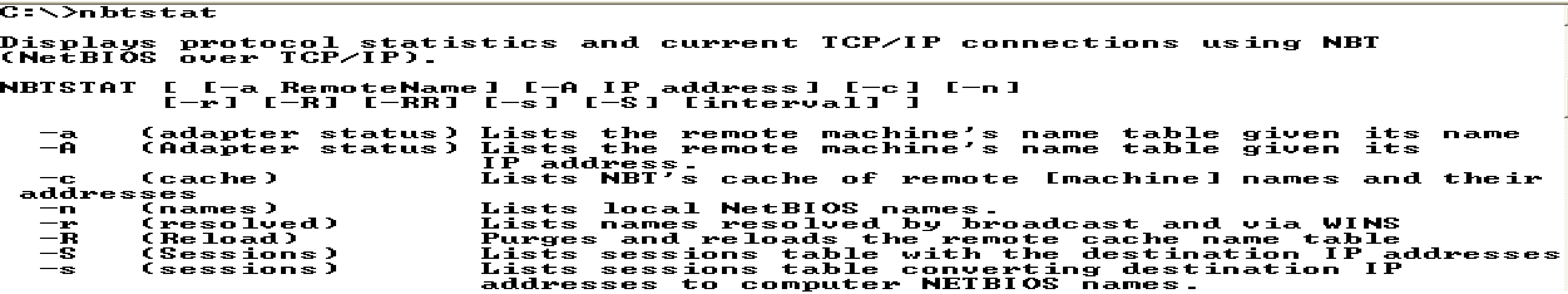
- After Windows XP SP2
  - *netstat -ab*



```
UDP    InternalHost:1026      *:*                                    1120
c:\windows\system32\WS2_32.dll
C:\WINDOWS\system32\WLDAP32.dll
C:\WINDOWS\System32\winrnr.dll
c:\windows\system32\WS2_32.dll
c:\windows\system32\w32time.dll
[svchost.exe]

UDP    InternalHost:1900      *:*                                    1292
c:\windows\system32\WS2_32.dll
c:\windows\system32\ssdpsrv.dll
C:\WINDOWS\system32\ADVAPI32.dll
C:\WINDOWS\system32\kernel32.dll
[svchost.exe]

UDP    InternalHost:ntp       *:*                                    1120
c:\windows\system32\WS2_32.dll
c:\windows\system32\w32time.dll
ntdll.dll
C:\WINDOWS\system32\kernel32.dll
[svchost.exe]
```

Cached NetBIOS Names

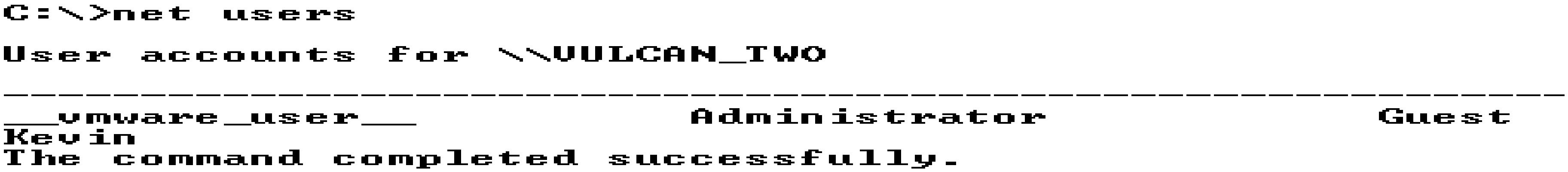
- We list with the *nbtstat* command



```
C:\>nbtstat

Displays protocol statistics and current TCP/IP connections using NBT
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
        [-r] [-R] [-RR] [-s] [-S] [interval] ]

  -a   (adapter status) Lists the remote machine's name table given its name
  -A   (Adapter status) Lists the remote machine's name table given its
                        IP address.
  -c   (cache)          Lists NBT's cache of remote [machine] names and their
 addresses
  -n   (names)          Lists local NetBIOS names.
  -r   (resolved)       Lists names resolved by broadcast and via WINS
  -R   (Reload)         Purges and reloads the remote cache name table
  -S   (Sessions)       Lists sessions table with the destination IP addresses
  -s   (sessions)       Lists sessions table converting destination IP
                        addresses to computer NETBIOS names.
```

Users Currently Logged On

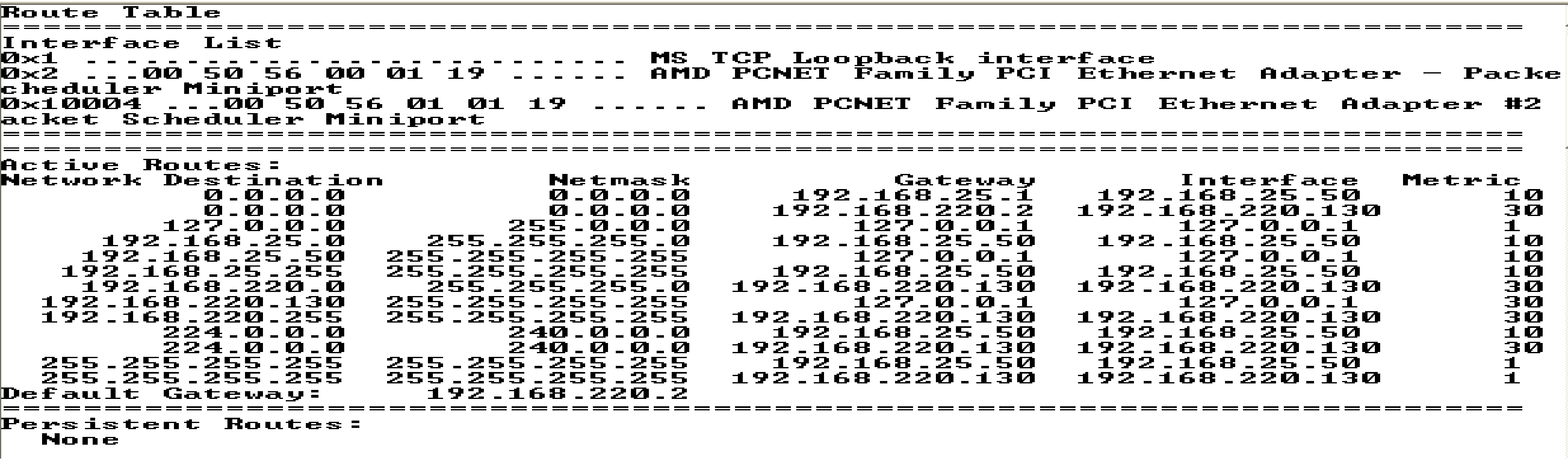
- Several choices
  - *net user*
  - *Psloggedon*
  - *net session*
  - *net file*



```
C:\>net users

User accounts for \\VULCAN_TWO

----------------------------------------------------------
__vmware_user__          Administrator            Guest
Kevin
The command completed successfully.
```

Internal routing

- We return to the versatile netstat command
  - *neststat -rn*

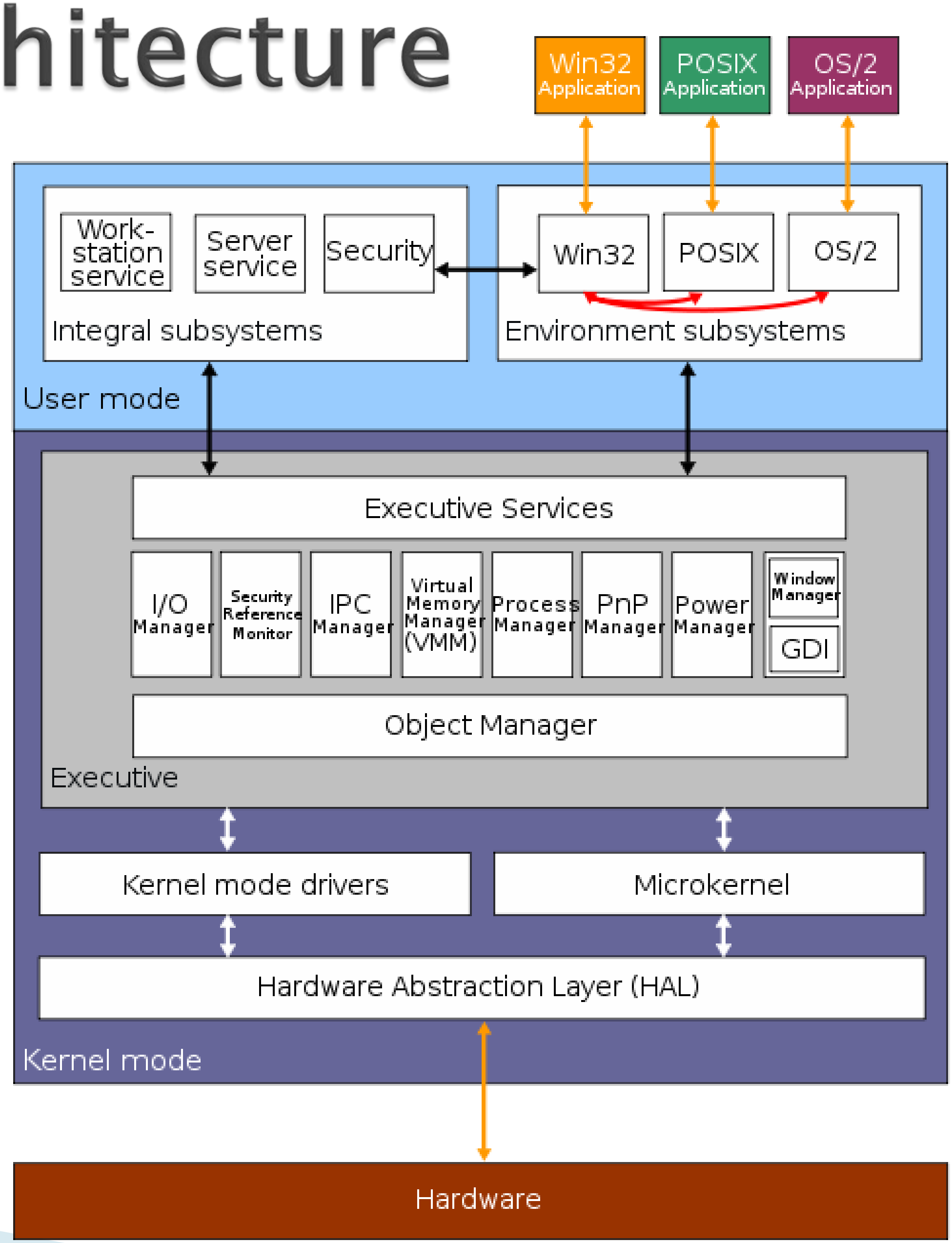


```
Route Table
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 50 56 00 01 19 ...... AMD PCNET Family PCI Ethernet Adapter – Packe
cheduler Miniport
0x10004 ...00 50 56 01 01 19 ...... AMD PCNET Family PCI Ethernet Adapter #2
acket Scheduler Miniport
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.25.1    192.168.25.50     10
          0.0.0.0          0.0.0.0    192.168.220.2  192.168.220.130     30
        127.0.0.0        255.0.0.0        127.0.0.1        127.0.0.1      1
     192.168.25.0    255.255.255.0    192.168.25.50    192.168.25.50     10
    192.168.25.50  255.255.255.255        127.0.0.1        127.0.0.1     10
   192.168.25.255  255.255.255.255    192.168.25.50    192.168.25.50     10
    192.168.220.0    255.255.255.0  192.168.220.130  192.168.220.130     30
  192.168.220.130  255.255.255.255        127.0.0.1        127.0.0.1     30
  192.168.220.255  255.255.255.255  192.168.220.130  192.168.220.130     30
        224.0.0.0        240.0.0.0    192.168.25.50    192.168.25.50     10
        224.0.0.0        240.0.0.0  192.168.220.130  192.168.220.130     30
  255.255.255.255  255.255.255.255    192.168.25.50    192.168.25.50      1
  255.255.255.255  255.255.255.255  192.168.220.130  192.168.220.130      1
Default Gateway:     192.168.220.2
===========================================================================
Persistent Routes:
  None
```

Running Processes

- We have to run several tools to extract needed information
  - Executable image
  - Command used to invoke
  - Runtime
  - Security context
  - DLLs and modules
  - Memory

Windows Architecture



Win32 Application
POSIX Application
OS/2 Application

Work-station service
Server service
Security
Integral subsystems

Win32
POSIX
OS/2
Environment subsystems

User mode

Executive Services

I/O Manager
Security Reference Monitor
IPC Manager
Virtual Memory Manager (VMM)
Process Manager
PnP Manager
Power Manager
Window Manager
GDI

Object Manager

Executive

Kernel mode drivers
Microkernel

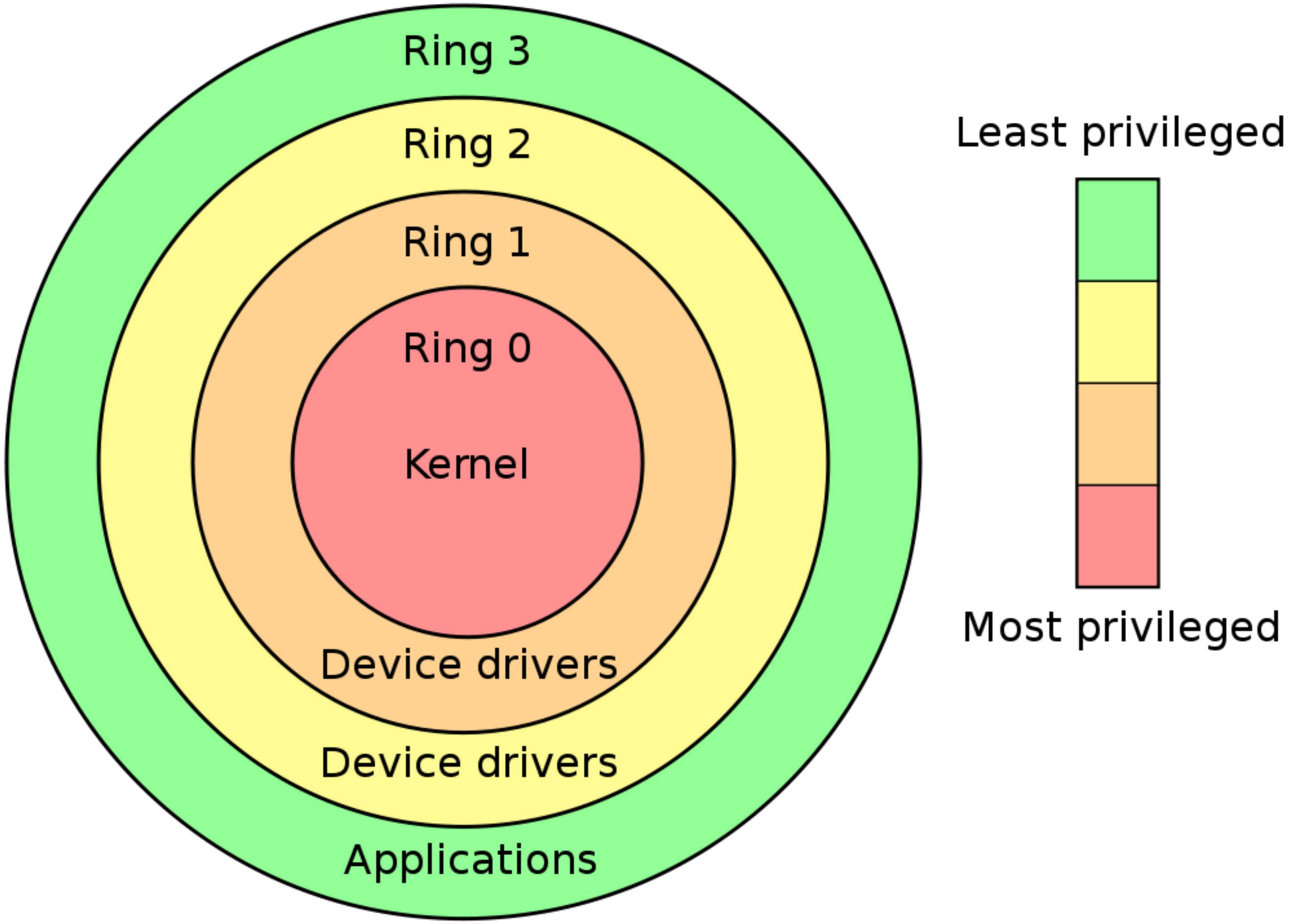
Hardware Abstraction Layer (HAL)

Kernel mode

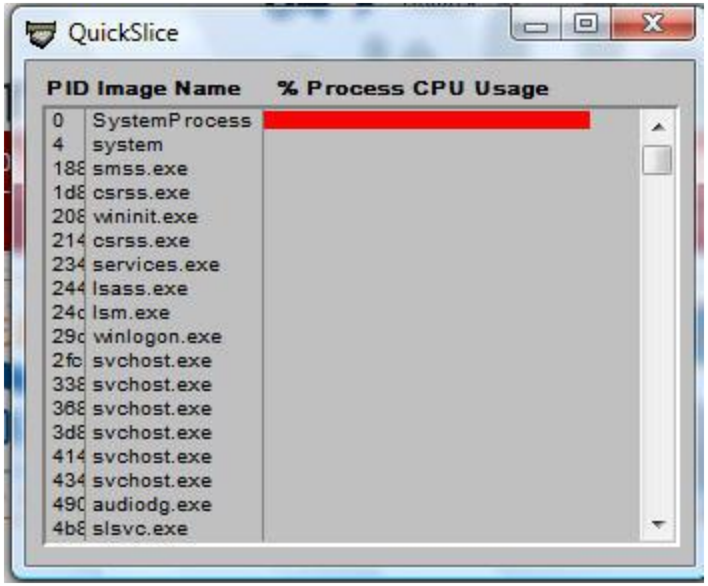
Hardware

Windows and Rings

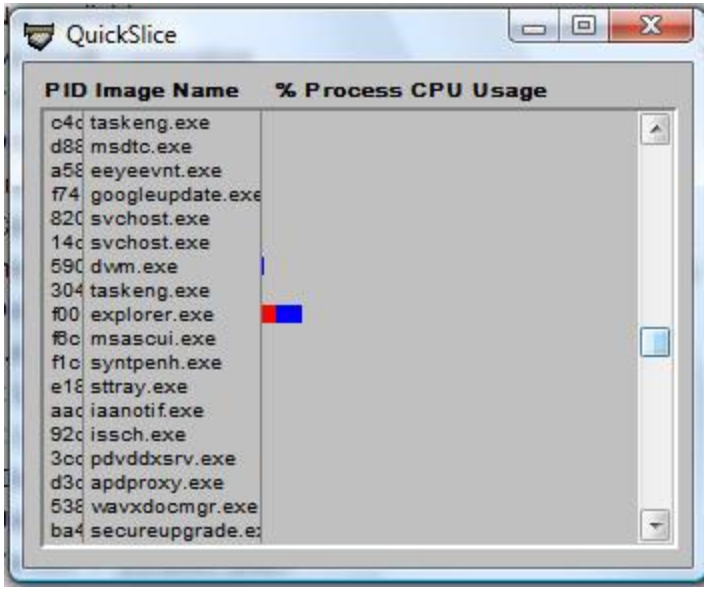
- Ring 3
  - User
- Ring 2
  - Not used
- Ring 1
  - Not used
- Ring 0
  - kernel



User and Kernel Mode



```
PID Image Name        % Process CPU Usage
0   SystemProcess
4   system
188 smss.exe
1d8 csrss.exe
208 wininit.exe
214 csrss.exe
234 services.exe
244 lsass.exe
24c lsm.exe
29c winlogon.exe
2fc svchost.exe
338 svchost.exe
368 svchost.exe
3d8 svchost.exe
414 svchost.exe
434 svchost.exe
490 audiodg.exe
4b8 slsvc.exe
```

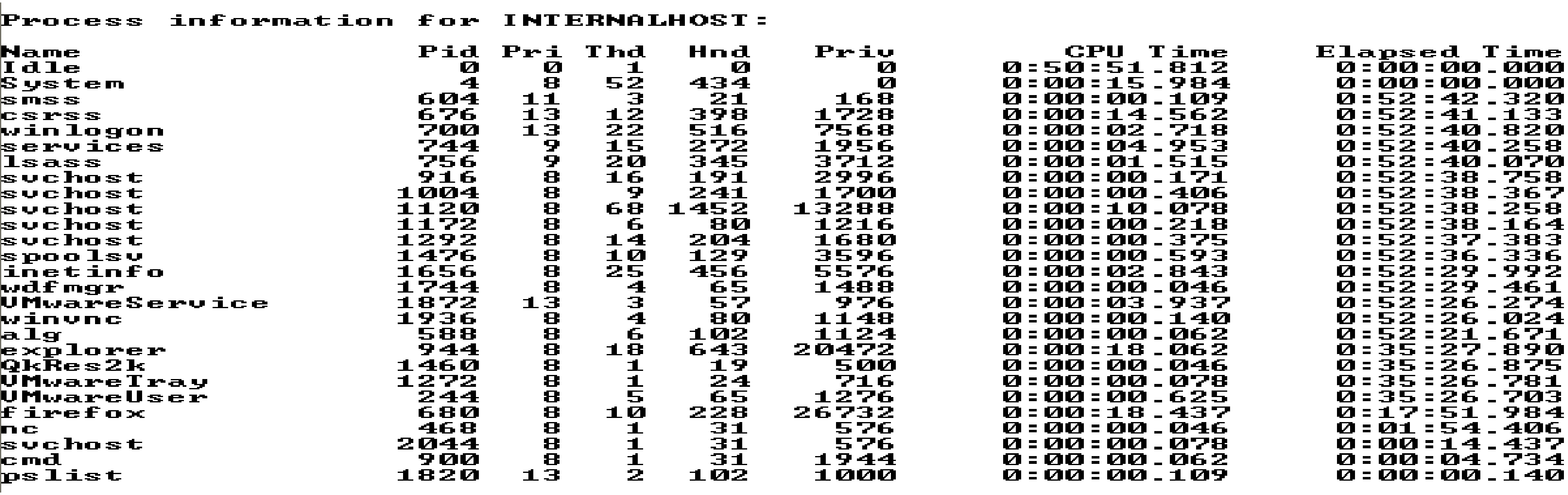


```
PID Image Name        % Process CPU Usage
c4c taskeng.exe
d88 msdtc.exe
a58 eeyeevnt.exe
f74 googleupdate.exe
820 svchost.exe
14c svchost.exe
590 dwm.exe
304 taskeng.exe
f00 explorer.exe
f8c msascui.exe
f1c syntpenh.exe
e18 sttray.exe
aac iaanotif.exe
92c issch.exe
3cc pdvddxsrv.exe
d3c apdproxy.exe
538 wavxdocmgr.exe
ba4 secureupgrade.e
```

Running Processes (cont)

- Tools
  - Pulist
    - User context
  - Pslist
    - Local and remote
    - –t displays process tree
  - listDLLs
  - Handle
  - Tlist
  - Tasklist

Pslist

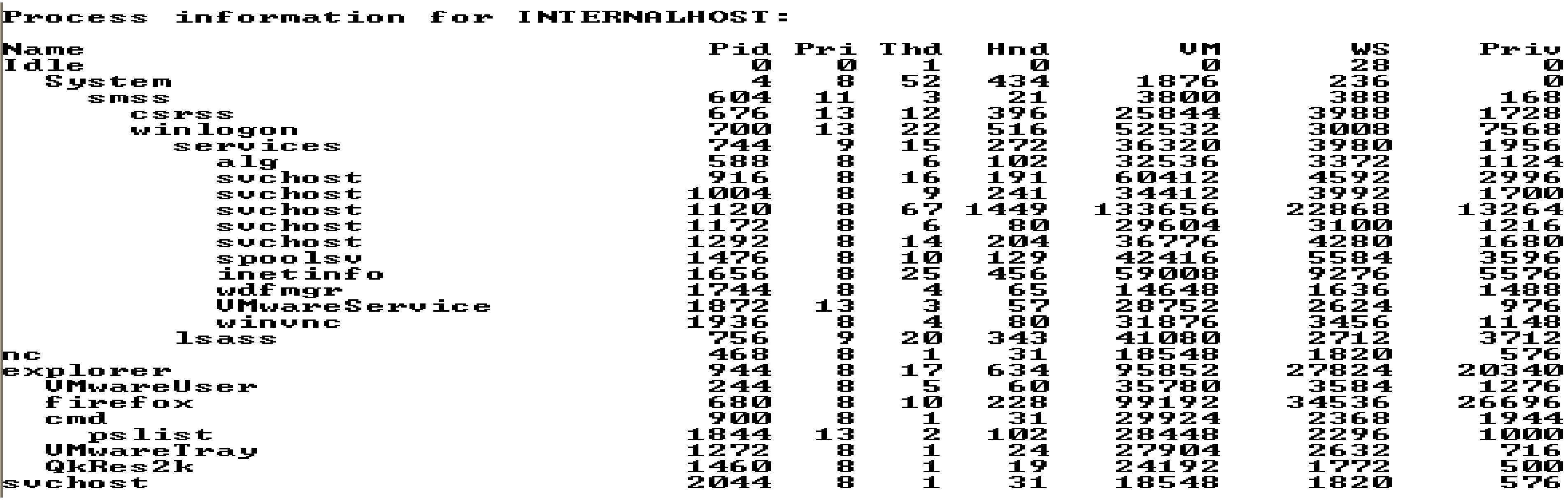


```
Process information for INTERNALHOST:

Name                Pid Pri Thd  Hnd   Priv        CPU Time    Elapsed Time
Idle                  0   0   1    0      0     0:50:51.812     0:00:00.000
System                4   8  52  434      0     0:00:15.984     0:00:00.000
smss                604  11   3   21    168     0:00:00.109     0:52:42.320
csrss               676  13  12  398   1728     0:00:14.562     0:52:41.133
winlogon            700  13  22  516   7568     0:00:02.718     0:52:40.820
services            744   9  15  272   1956     0:00:04.953     0:52:40.258
lsass               756   9  20  345   3712     0:00:01.515     0:52:40.070
svchost             916   8  16  191   2996     0:00:00.171     0:52:38.758
svchost            1004   8   9  241   1700     0:00:00.406     0:52:38.367
svchost            1120   8  68 1452  13288     0:00:10.078     0:52:38.258
svchost            1172   8   6   80   1216     0:00:00.218     0:52:38.164
svchost            1292   8  14  204   1680     0:00:00.375     0:52:37.383
spoolsv            1476   8  10  129   3596     0:00:00.593     0:52:36.336
inetinfo           1656   8  25  456   5576     0:00:02.843     0:52:29.992
wdfmgr             1744   8   4   65   1488     0:00:00.046     0:52:29.461
VMwareService      1872  13   3   57    976     0:00:03.937     0:52:26.274
winvnc             1936   8   4   80   1148     0:00:00.140     0:52:26.024
alg                 588   8   6  102   1124     0:00:00.062     0:52:21.671
explorer            944   8  18  643  20472     0:00:18.062     0:35:27.890
QkRes2k            1460   8   1   19    500     0:00:00.046     0:35:26.875
VMwareTray         1272   8   1   24    716     0:00:00.078     0:35:26.781
VMwareUser          244   8   5   65   1276     0:00:00.625     0:35:26.703
firefox             680   8  10  228  26732     0:00:18.437     0:17:51.984
nc                  468   8   1   31    576     0:00:00.046     0:01:54.406
svchost            2044   8   1   31    576     0:00:00.078     0:00:14.437
cmd                 900   8   1   31   1944     0:00:00.062     0:00:04.734
pslist             1820  13   2  102   1000     0:00:00.109     0:00:00.140
```

Trivia

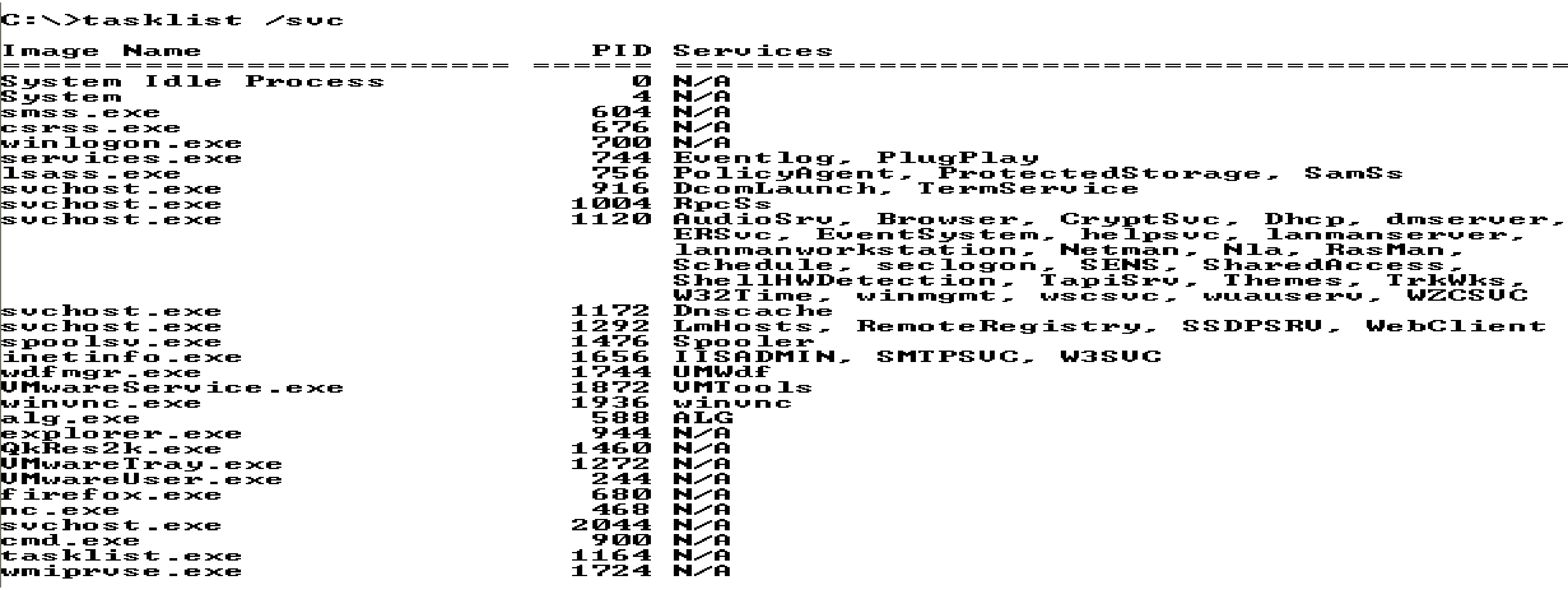
- On the previous slide what is the PID of the Trojan?

Pslist –t



```
Process information for INTERNALHOST:

Name                             Pid Pri Thd  Hnd      VM      WS    Priv
Idle                               0   0   1    0       0      28       0
   System                          4   8  52  434    1876     236       0
      smss                       604  11   3   21    3800     388     168
         csrss                   676  13  12  396   25844    3988    1728
         winlogon                700  13  22  516   52532    3008    7568
            services             744   9  15  272   36320    3980    1956
               alg               588   8   6  102   32536    3372    1124
               svchost           916   8  16  191   60412    4592    2996
               svchost          1004   8   9  241   34412    3992    1700
               svchost          1120   8  67 1449  133656   22868   13264
               svchost          1172   8   6   80   29604    3100    1216
               svchost          1292   8  14  204   36776    4280    1680
               spoolsv          1476   8  10  129   42416    5584    3596
               inetinfo         1656   8  25  456   59008    9276    5576
               wdfmgr           1744   8   4   65   14648    1636    1488
               VMwareService    1872  13   3   57   28752    2624     976
               winvnc           1936   8   4   80   31876    3456    1148
            lsass                756   9  20  343   41080    2712    3712
nc                               468   8   1   31   18548    1820     576
explorer                         944   8  17  634   95852   27824   20340
   VMwareUser                    244   8   5   60   35780    3584    1276
   firefox                       680   8  10  228   99192   34536   26696
   cmd                           900   8   1   31   29924    2368    1944
      pslist                    1844  13   2  102   28448    2296    1000
   VMwareTray                   1272   8   1   24   27904    2632     716
   QkRes2k                      1460   8   1   19   24192    1772     500
svchost                         2044   8   1   31   18548    1820     576
```

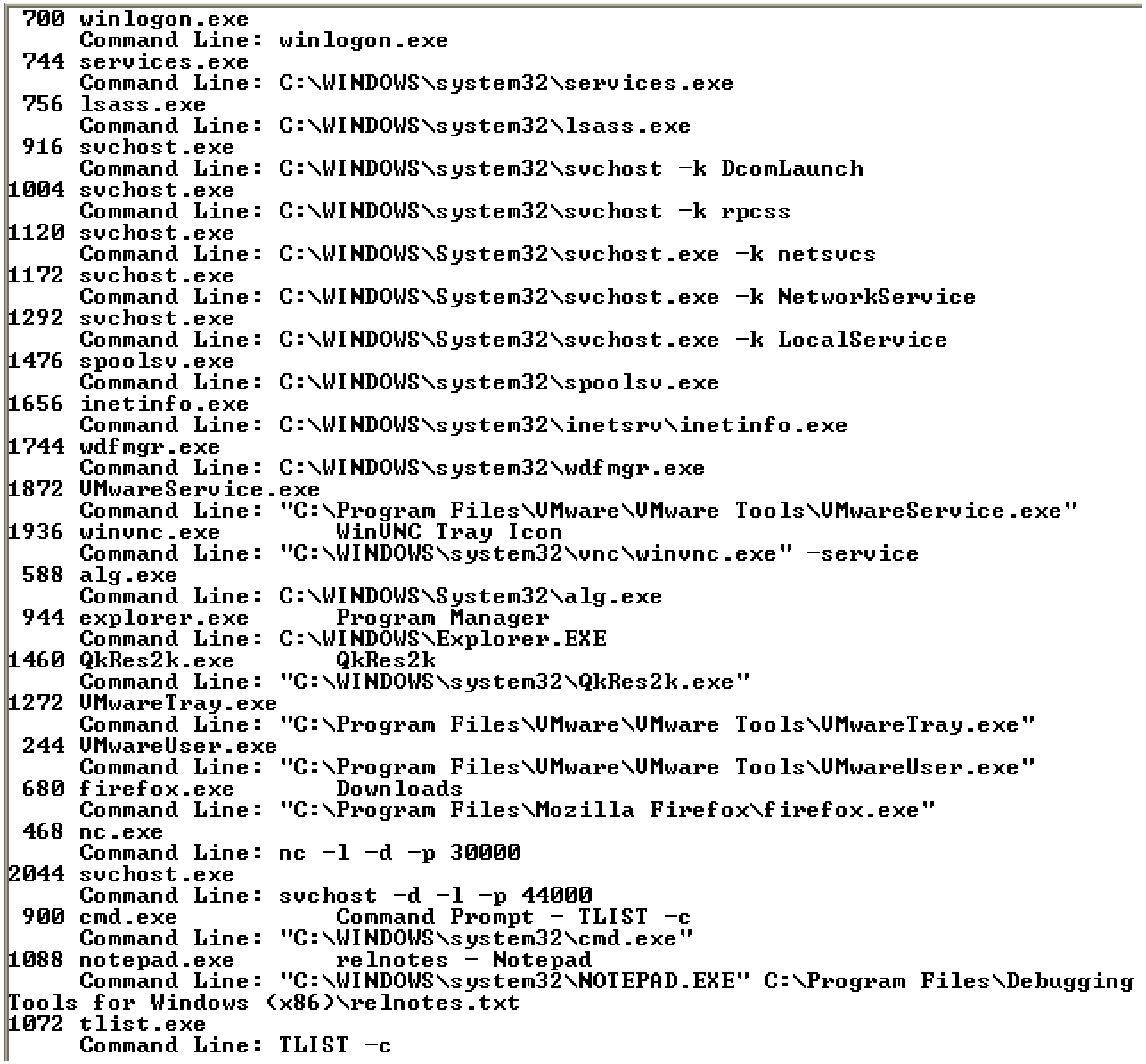
Tasklist



```
C:\>tasklist /svc

Image Name                     PID Services
========================= ======== ============================================
System Idle Process              0 N/A
System                           4 N/A
smss.exe                       604 N/A
csrss.exe                      676 N/A
winlogon.exe                   700 N/A
services.exe                   744 Eventlog, PlugPlay
lsass.exe                      756 PolicyAgent, ProtectedStorage, SamSs
svchost.exe                    916 DcomLaunch, TermService
svchost.exe                   1004 RpcSs
svchost.exe                   1120 AudioSrv, Browser, CryptSvc, Dhcp, dmserver,
                                   ERSvc, EventSystem, helpsvc, lanmanserver,
                                   lanmanworkstation, Netman, Nla, RasMan,
                                   Schedule, seclogon, SENS, SharedAccess,
                                   ShellHWDetection, TapiSrv, Themes, TrkWks,
                                   W32Time, winmgmt, wscsvc, wuauserv, WZCSVC
svchost.exe                   1172 Dnscache
svchost.exe                   1292 LmHosts, RemoteRegistry, SSDPSRV, WebClient
spoolsv.exe                   1476 Spooler
inetinfo.exe                  1656 IISADMIN, SMTPSVC, W3SVC
wdfmgr.exe                    1744 UMWdf
VMwareService.exe             1872 VMTools
winvnc.exe                    1936 winvnc
alg.exe                        588 ALG
explorer.exe                   944 N/A
QkRes2k.exe                   1460 N/A
VMwareTray.exe                1272 N/A
VMwareUser.exe                 244 N/A
firefox.exe                    680 N/A
nc.exe                         468 N/A
svchost.exe                   2044 N/A
cmd.exe                        900 N/A
tasklist.exe                  1164 N/A
wmiprvse.exe                  1724 N/A
```

Tlist

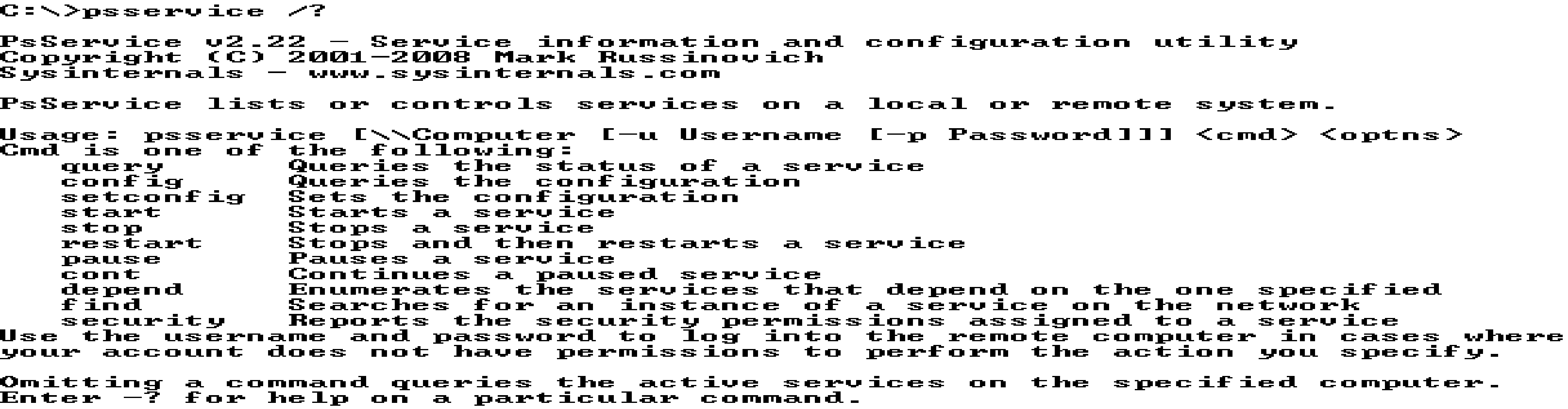
- Debugging
- tools



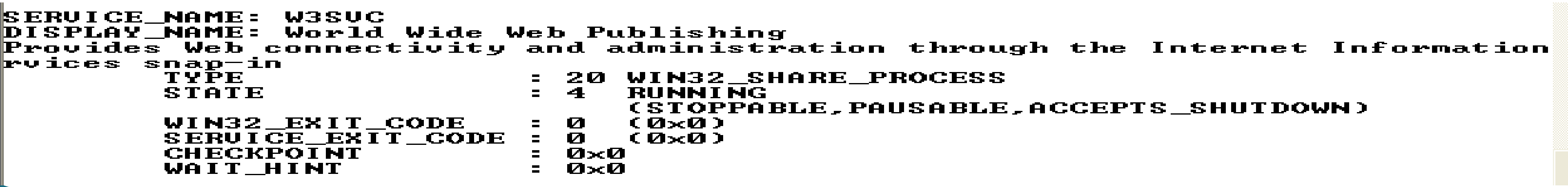
```
 700 winlogon.exe
     Command Line: winlogon.exe
 744 services.exe
     Command Line: C:\WINDOWS\system32\services.exe
 756 lsass.exe
     Command Line: C:\WINDOWS\system32\lsass.exe
 916 svchost.exe
     Command Line: C:\WINDOWS\system32\svchost -k DcomLaunch
1004 svchost.exe
     Command Line: C:\WINDOWS\system32\svchost -k rpcss
1120 svchost.exe
     Command Line: C:\WINDOWS\System32\svchost.exe -k netsvcs
1172 svchost.exe
     Command Line: C:\WINDOWS\System32\svchost.exe -k NetworkService
1292 svchost.exe
     Command Line: C:\WINDOWS\System32\svchost.exe -k LocalService
1476 spoolsv.exe
     Command Line: C:\WINDOWS\system32\spoolsv.exe
1656 inetinfo.exe
     Command Line: C:\WINDOWS\system32\inetsrv\inetinfo.exe
1744 wdfmgr.exe
     Command Line: C:\WINDOWS\system32\wdfmgr.exe
1872 VMwareService.exe
     Command Line: "C:\Program Files\VMware\VMware Tools\VMwareService.exe"
1936 winvnc.exe        WinVNC Tray Icon
     Command Line: "C:\WINDOWS\system32\vnc\winvnc.exe" -service
 588 alg.exe
     Command Line: C:\WINDOWS\System32\alg.exe
 944 explorer.exe      Program Manager
     Command Line: C:\WINDOWS\Explorer.EXE
1460 QkRes2k.exe       QkRes2k
     Command Line: "C:\WINDOWS\system32\QkRes2k.exe"
1272 VMwareTray.exe
     Command Line: "C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
 244 VMwareUser.exe
     Command Line: "C:\Program Files\VMware\VMware Tools\VMwareUser.exe"
 680 firefox.exe       Downloads
     Command Line: "C:\Program Files\Mozilla Firefox\firefox.exe"
 468 nc.exe
     Command Line: nc -l -d -p 30000
2044 svchost.exe
     Command Line: svchost -d -l -p 44000
 900 cmd.exe           Command Prompt - TLIST -c
     Command Line: "C:\WINDOWS\system32\cmd.exe"
1088 notepad.exe       relnotes - Notepad
     Command Line: "C:\WINDOWS\system32\NOTEPAD.EXE" C:\Program Files\Debugging
Tools for Windows (x86)\relnotes.txt
1072 tlist.exe
     Command Line: TLIST -c
```

Running Services

- *psservice*



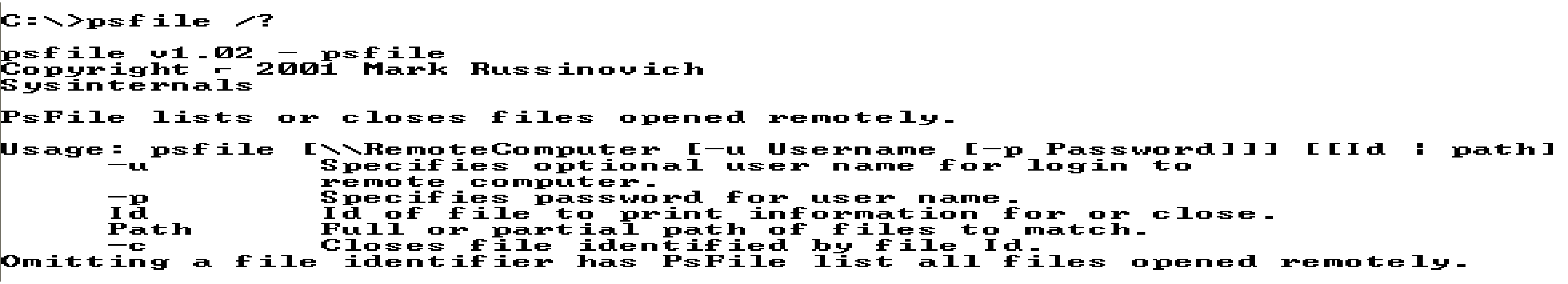
```
C:\>psservice /?

PsService v2.22 - Service information and configuration utility
Copyright (C) 2001-2008 Mark Russinovich
Sysinternals - www.sysinternals.com

PsService lists or controls services on a local or remote system.

Usage: psservice [\\Computer [-u Username [-p Password]]] <cmd> <optns>
Cmd is one of the following:
    query       Queries the status of a service
    config      Queries the configuration
    setconfig   Sets the configuration
    start       Starts a service
    stop        Stops a service
    restart     Stops and then restarts a service
    pause       Pauses a service
    cont        Continues a paused service
    depend      Enumerates the services that depend on the one specified
    find        Searches for an instance of a service on the network
    security    Reports the security permissions assigned to a service
Use the username and password to log into the remote computer in cases where
your account does not have permissions to perform the action you specify.

Omitting a command queries the active services on the specified computer.
Enter -? for help on a particular command.
```



```
SERVICE_NAME: W3SVC
DISPLAY_NAME: World Wide Web Publishing
Provides Web connectivity and administration through the Internet Information
rvices snap-in
          TYPE               : 20  WIN32_SHARE_PROCESS
          STATE              : 4   RUNNING
                                   (STOPPABLE,PAUSABLE,ACCEPTS_SHUTDOWN)
          WIN32_EXIT_CODE    : 0   (0x0)
          SERVICE_EXIT_CODE  : 0   (0x0)
          CHECKPOINT         : 0x0
          WAIT_HINT          : 0x0
```

Open Files

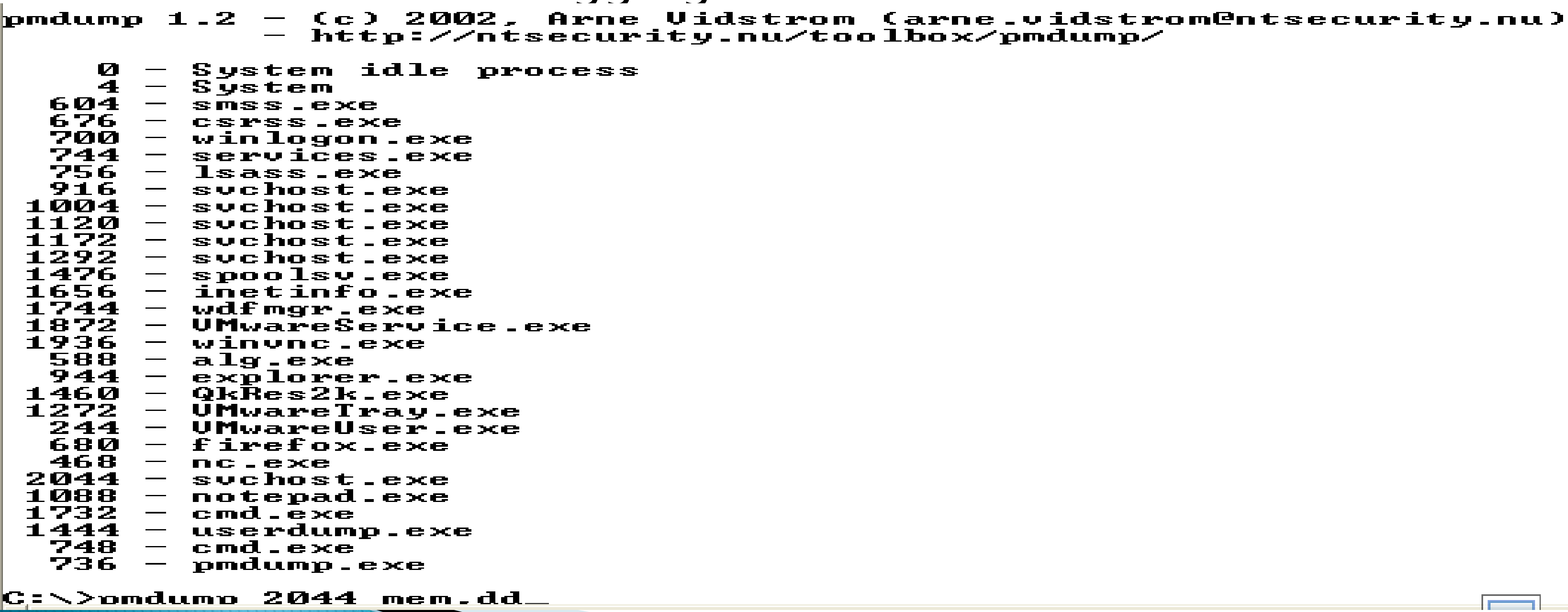
- psfile



```
C:\>psfile /?

psfile v1.02 - psfile
Copyright r 2001 Mark Russinovich
Sysinternals

PsFile lists or closes files opened remotely.

Usage: psfile [\\RemoteComputer [-u Username [-p Password]]] [[Id : path]
     -u         Specifies optional user name for login to
                remote computer.
     -p         Specifies password for user name.
     Id         Id of file to print information for or close.
     Path       Full or partial path of files to match.
     -c         Closes file identified by file Id.
Omitting a file identifier has PsFile list all files opened remotely.
```

Process Memory Dumps

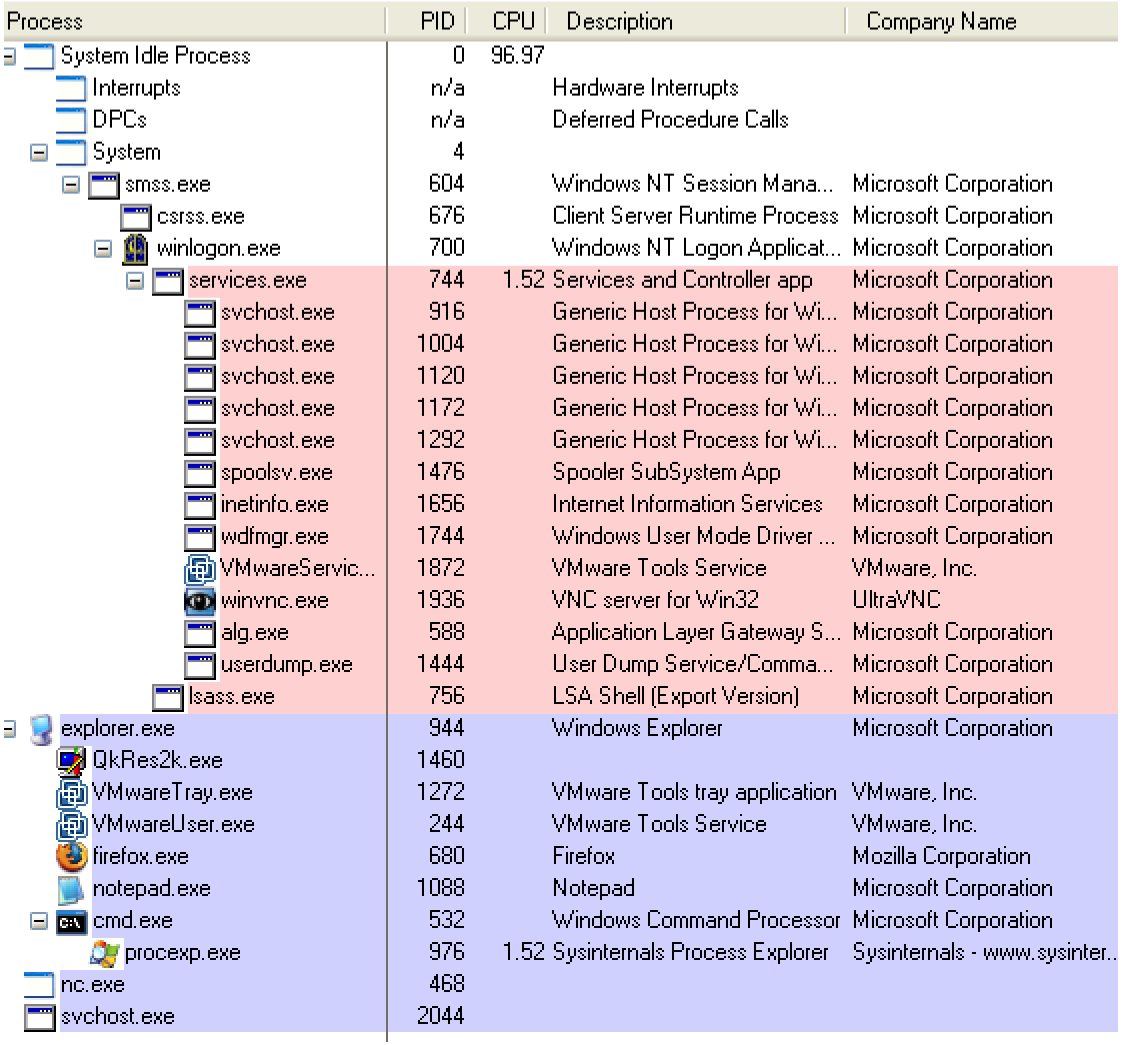
- *pmdump*
  - www.ntsecurity.nu
- *userdmp*
  - Microsoft debugging tools



```
pmdump 1.2 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
           - http://ntsecurity.nu/toolbox/pmdump/

    0 - System idle process
    4 - System
  604 - smss.exe
  676 - csrss.exe
  700 - winlogon.exe
  744 - services.exe
  756 - lsass.exe
  916 - svchost.exe
 1004 - svchost.exe
 1120 - svchost.exe
 1172 - svchost.exe
 1292 - svchost.exe
 1476 - spoolsv.exe
 1656 - inetinfo.exe
 1744 - wdfmgr.exe
 1872 - VMwareService.exe
 1936 - winvnc.exe
  588 - alg.exe
  944 - explorer.exe
 1460 - QkRes2k.exe
 1272 - VMwareTray.exe
  244 - VMwareUser.exe
  680 - firefox.exe
  468 - nc.exe
 2044 - svchost.exe
 1088 - notepad.exe
 1732 - cmd.exe
 1444 - userdump.exe
  748 - cmd.exe
  736 - pmdump.exe

C:\>pmdump 2044 mem.dd_
```

Process Memory Dumps (cont)

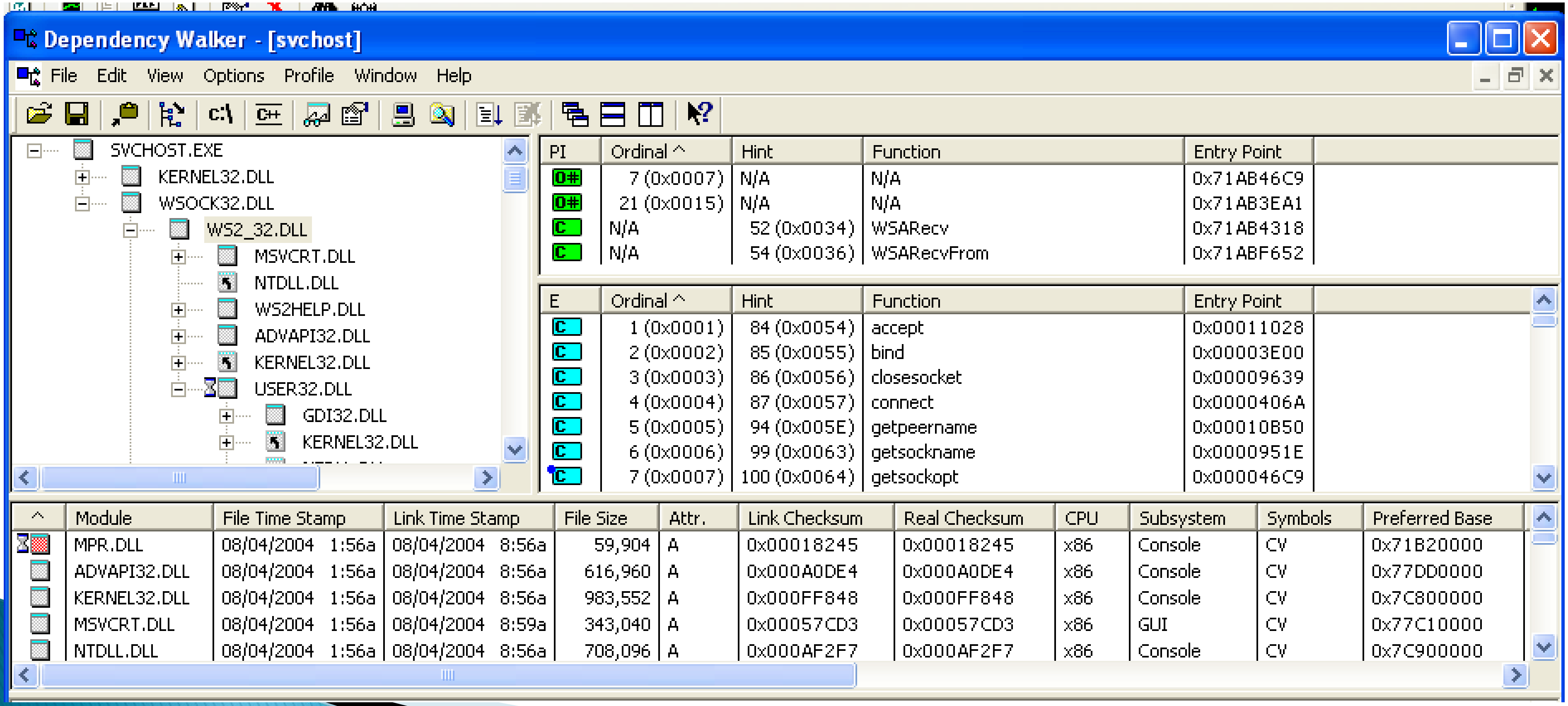
- Process dissection
  - *Process explorer*



Process	PID	CPU	Description	Company Name
System Idle Process	0	96.97		
Interrupts	n/a		Hardware Interrupts	
DPCs	n/a		Deferred Procedure Calls	
System	4			
smss.exe	604		Windows NT Session Mana...	Microsoft Corporation
csrss.exe	676		Client Server Runtime Process	Microsoft Corporation
winlogon.exe	700		Windows NT Logon Applicat...	Microsoft Corporation
services.exe	744	1.52	Services and Controller app	Microsoft Corporation
svchost.exe	916		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1004		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1120		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1172		Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1292		Generic Host Process for Wi...	Microsoft Corporation
spoolsv.exe	1476		Spooler SubSystem App	Microsoft Corporation
inetinfo.exe	1656		Internet Information Services	Microsoft Corporation
wdfmgr.exe	1744		Windows User Mode Driver ...	Microsoft Corporation
VMwareServic...	1872		VMware Tools Service	VMware, Inc.
winvnc.exe	1936		VNC server for Win32	UltraVNC
alg.exe	588		Application Layer Gateway S...	Microsoft Corporation
userdump.exe	1444		User Dump Service/Comma...	Microsoft Corporation
lsass.exe	756		LSA Shell (Export Version)	Microsoft Corporation
explorer.exe	944		Windows Explorer	Microsoft Corporation
QkRes2k.exe	1460			
VMwareTray.exe	1272		VMware Tools tray application	VMware, Inc.
VMwareUser.exe	244		VMware Tools Service	VMware, Inc.
firefox.exe	680		Firefox	Mozilla Corporation
notepad.exe	1088		Notepad	Microsoft Corporation
cmd.exe	532		Windows Command Processor	Microsoft Corporation
procexp.exe	976	1.52	Sysinternals Process Explorer	Sysinternals - www.sysinter..
nc.exe	468			
svchost.exe	2044			

Process Memory Dumps (cont)

- More dissection
  - *Dependency walker*



```
⊟ SVCHOST.EXE
    ⊞ KERNEL32.DLL
    ⊟ WSOCK32.DLL
        ⊟ WS2_32.DLL
            ⊞ MSVCRT.DLL
              NTDLL.DLL
            ⊞ WS2HELP.DLL
            ⊞ ADVAPI32.DLL
            ⊞ KERNEL32.DLL
            ⊟ USER32.DLL
                ⊞ GDI32.DLL
                ⊞ KERNEL32.DLL
```

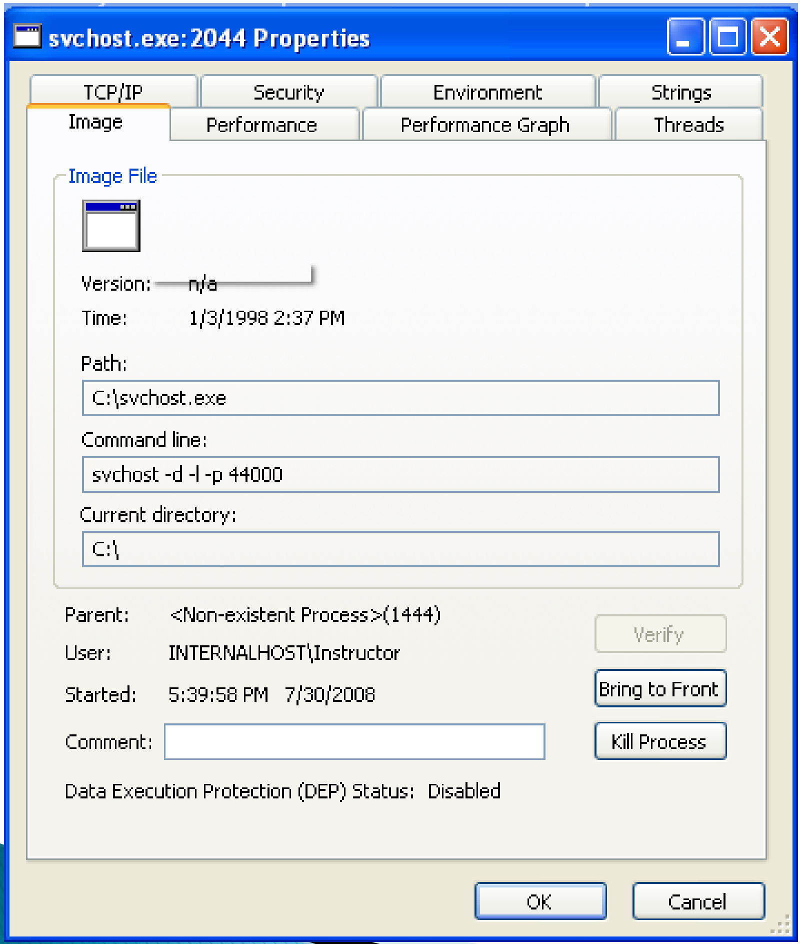
PI	Ordinal ^	Hint	Function	Entry Point
O#	7 (0x0007)	N/A	N/A	0x71AB46C9
O#	21 (0x0015)	N/A	N/A	0x71AB3EA1
C	N/A	52 (0x0034)	WSARecv	0x71AB4318
C	N/A	54 (0x0036)	WSARecvFrom	0x71ABF652

E	Ordinal ^	Hint	Function	Entry Point
C	1 (0x0001)	84 (0x0054)	accept	0x00011028
C	2 (0x0002)	85 (0x0055)	bind	0x00003E00
C	3 (0x0003)	86 (0x0056)	closesocket	0x00009639
C	4 (0x0004)	87 (0x0057)	connect	0x0000406A
C	5 (0x0005)	94 (0x005E)	getpeername	0x00010B50
C	6 (0x0006)	99 (0x0063)	getsockname	0x0000951E
C	7 (0x0007)	100 (0x0064)	getsockopt	0x000046C9

^	Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base
	MPR.DLL	08/04/2004 1:56a	08/04/2004 8:56a	59,904	A	0x00018245	0x00018245	x86	Console	CV	0x71B20000
	ADVAPI32.DLL	08/04/2004 1:56a	08/04/2004 8:56a	616,960	A	0x000A0DE4	0x000A0DE4	x86	Console	CV	0x77DD0000
	KERNEL32.DLL	08/04/2004 1:56a	08/04/2004 8:56a	983,552	A	0x000FF848	0x000FF848	x86	Console	CV	0x7C800000
	MSVCRT.DLL	08/04/2004 1:56a	08/04/2004 8:59a	343,040	A	0x00057CD3	0x00057CD3	x86	GUI	CV	0x77C10000
	NTDLL.DLL	08/04/2004 1:56a	08/04/2004 8:56a	708,096	A	0x000AF2F7	0x000AF2F7	x86	Console	CV	0x7C900000

Process Memory Dumps (cont)

- Game Over!



svchost.exe:2044 Properties

Version: n/a

Time: 1/3/1998 2:37 PM

Path: C:\svchost.exe

Command line: svchost -d -l -p 44000

Current directory: C:\

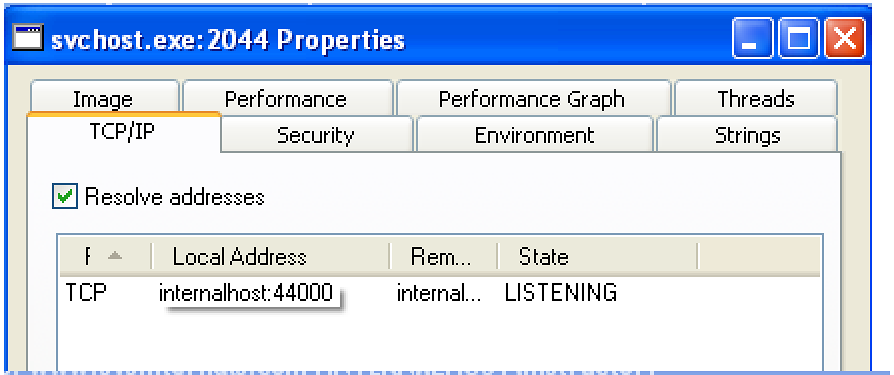
Parent: <Non-existent Process>(1444)

User: INTERNALHOST\Instructor

Started: 5:39:58 PM 7/30/2008

Comment:

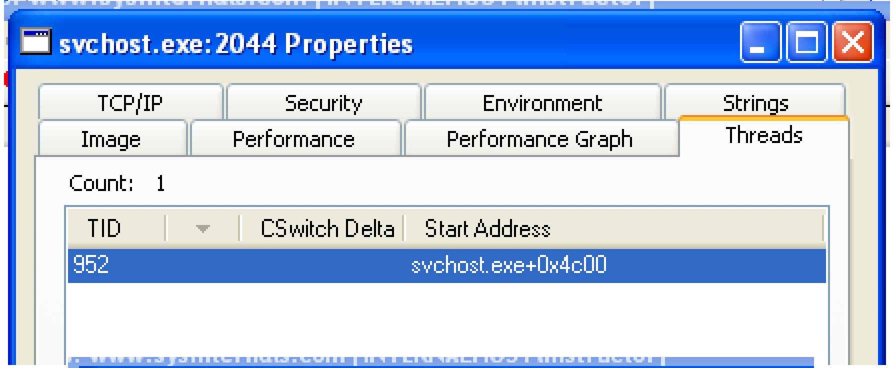
Data Execution Protection (DEP) Status: Disabled



svchost.exe:2044 Properties

☑ Resolve addresses

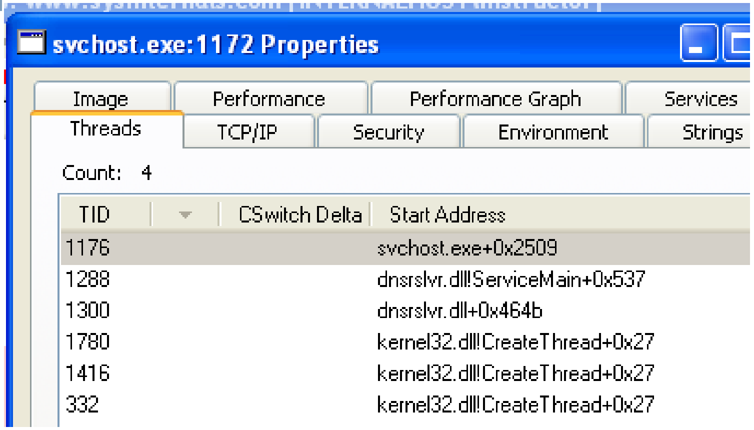
P	Local Address	Rem...	State
TCP	internalhost:44000	internal...	LISTENING



svchost.exe:2044 Properties

Count: 1

TID	CSwitch Delta	Start Address
952		svchost.exe+0x4c00



svchost.exe:1172 Properties

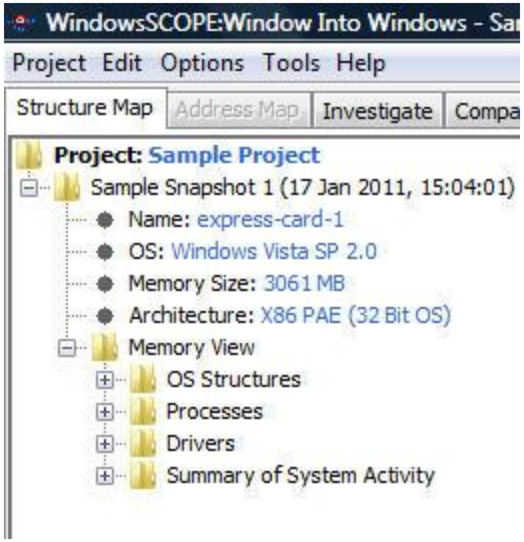
Count: 4

TID	CSwitch Delta	Start Address
1176		svchost.exe+0x2509
1288		dnsrslvr.dll!ServiceMain+0x537
1300		dnsrslvr.dll+0x464b
1780		kernel32.dll!CreateThread+0x27
1416		kernel32.dll!CreateThread+0x27
332		kernel32.dll!CreateThread+0x27

Sophisticated Malware

- None of the previous tools will work in most cases
- Perpetrators write their tools to avoid these
- Have to analyze the raw image
- Can do manually
- Tools work the best

Sophisticated Malware (cont)


WindowsSCOPE:Window Into Windows - Sa
Project Edit Options Tools Help
Structure Map
Address Map
Investigate
Compa

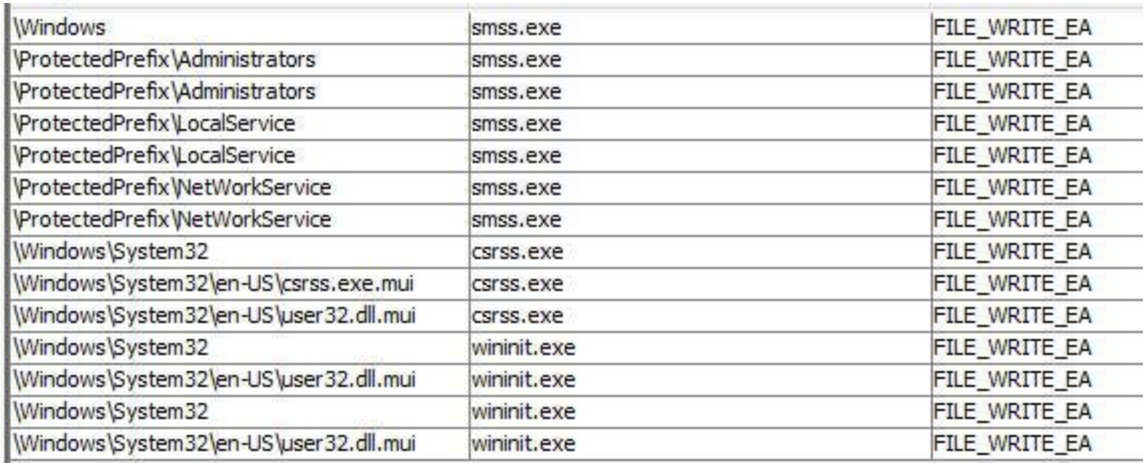
Project: Sample Project

Sample Snapshot 1 (17 Jan 2011, 15:04:01)

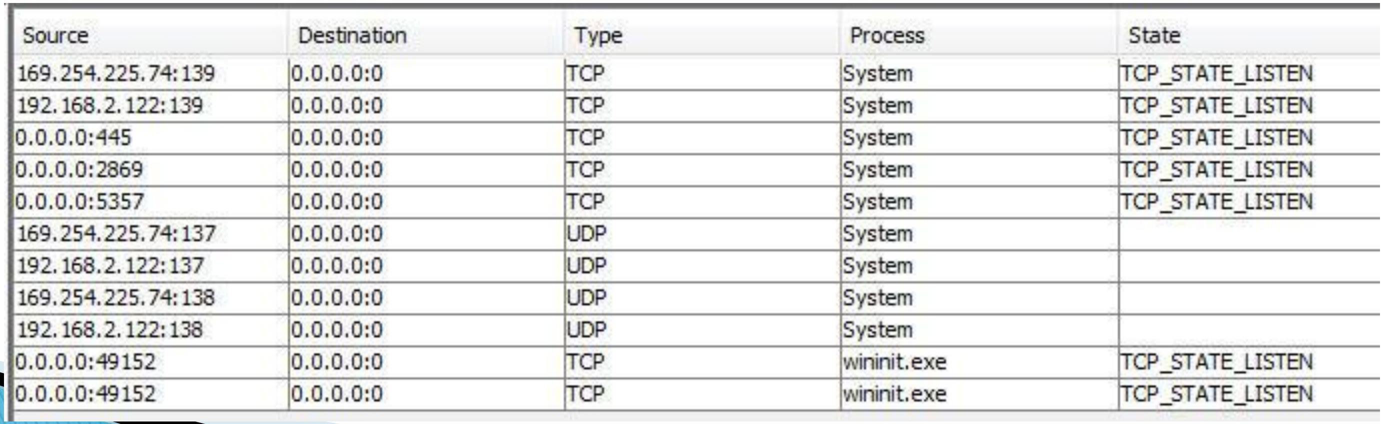
- Name: express-card-1
- OS: Windows Vista SP 2.0
- Memory Size: 3061 MB
- Architecture: X86 PAE (32 Bit OS)

Memory View

- OS Structures
- Processes
- Drivers
- Summary of System Activity

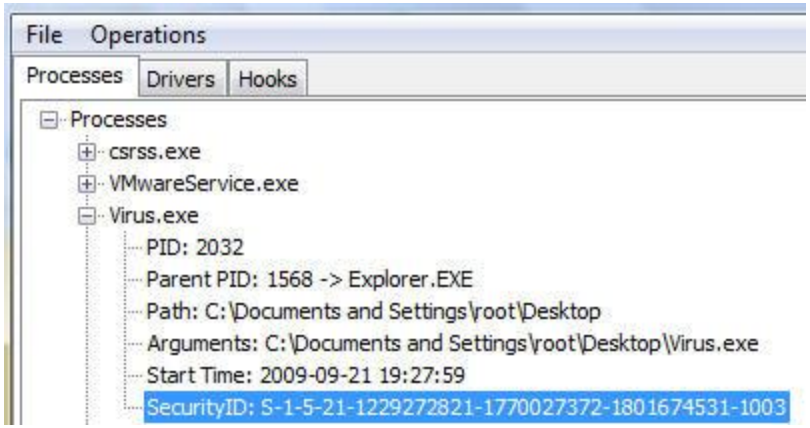


\Windows	smss.exe	FILE_WRITE_EA
\ProtectedPrefix\Administrators	smss.exe	FILE_WRITE_EA
\ProtectedPrefix\Administrators	smss.exe	FILE_WRITE_EA
\ProtectedPrefix\LocalService	smss.exe	FILE_WRITE_EA
\ProtectedPrefix\LocalService	smss.exe	FILE_WRITE_EA
\ProtectedPrefix\NetWorkService	smss.exe	FILE_WRITE_EA
\ProtectedPrefix\NetWorkService	smss.exe	FILE_WRITE_EA
\Windows\System32	csrss.exe	FILE_WRITE_EA
\Windows\System32\en-US\csrss.exe.mui	csrss.exe	FILE_WRITE_EA
\Windows\System32\en-US\user32.dll.mui	csrss.exe	FILE_WRITE_EA
\Windows\System32	wininit.exe	FILE_WRITE_EA
\Windows\System32\en-US\user32.dll.mui	wininit.exe	FILE_WRITE_EA
\Windows\System32	wininit.exe	FILE_WRITE_EA
\Windows\System32\en-US\user32.dll.mui	wininit.exe	FILE_WRITE_EA

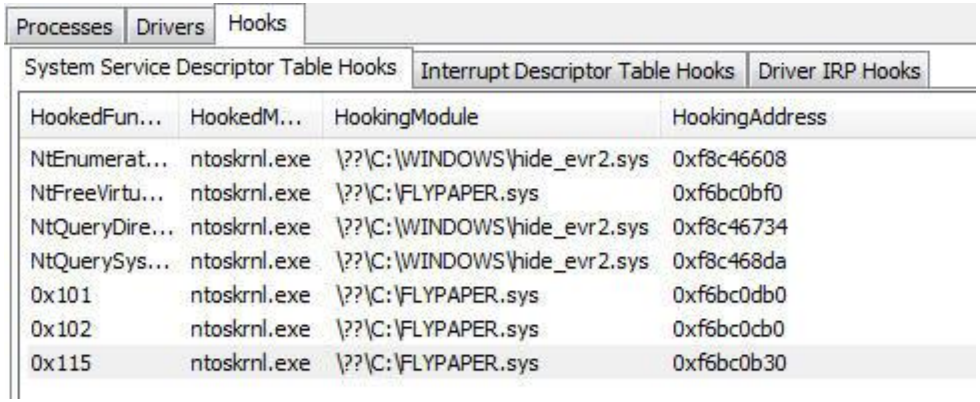


Source	Destination	Type	Process	State
169.254.225.74:139	0.0.0.0:0	TCP	System	TCP_STATE_LISTEN
192.168.2.122:139	0.0.0.0:0	TCP	System	TCP_STATE_LISTEN
0.0.0.0:445	0.0.0.0:0	TCP	System	TCP_STATE_LISTEN
0.0.0.0:2869	0.0.0.0:0	TCP	System	TCP_STATE_LISTEN
0.0.0.0:5357	0.0.0.0:0	TCP	System	TCP_STATE_LISTEN
169.254.225.74:137	0.0.0.0:0	UDP	System	
192.168.2.122:137	0.0.0.0:0	UDP	System	
169.254.225.74:138	0.0.0.0:0	UDP	System	
192.168.2.122:138	0.0.0.0:0	UDP	System	
0.0.0.0:49152	0.0.0.0:0	TCP	wininit.exe	TCP_STATE_LISTEN
0.0.0.0:49152	0.0.0.0:0	TCP	wininit.exe	TCP_STATE_LISTEN

Sophisticated Malware (cont)



```
Processes
  csrss.exe
  VMwareService.exe
  Virus.exe
    PID: 2032
    Parent PID: 1568 -> Explorer.EXE
    Path: C:\Documents and Settings\root\Desktop
    Arguments: C:\Documents and Settings\root\Desktop\Virus.exe
    Start Time: 2009-09-21 19:27:59
    SecurityID: S-1-5-21-1229272821-1770027372-1801674531-1003
```


Processes
Drivers
Hooks
System Service Descriptor Table Hooks
Interrupt Descriptor Table Hooks
Driver IRP Hooks

HookedFun...	HookedM...	HookingModule	HookingAddress
NtEnumerat...	ntoskrnl.exe	\??\C:\WINDOWS\hide_evr2.sys	0xf8c46608
NtFreeVirtu...	ntoskrnl.exe	\??\C:\FLYPAPER.sys	0xf6bc0bf0
NtQueryDire...	ntoskrnl.exe	\??\C:\WINDOWS\hide_evr2.sys	0xf8c46734
NtQuerySys...	ntoskrnl.exe	\??\C:\WINDOWS\hide_evr2.sys	0xf8c468da
0x101	ntoskrnl.exe	\??\C:\FLYPAPER.sys	0xf6bc0db0
0x102	ntoskrnl.exe	\??\C:\FLYPAPER.sys	0xf6bc0cb0
0x115	ntoskrnl.exe	\??\C:\FLYPAPER.sys	0xf6bc0b30

Demonstrations

Residual Risk

- www.zerodayinitiative.com

Thank You

- Kevin Cardwell
  - kevin@elitesecurityandforensics.com
- www.elitesecurityandforensics.com