

3rd Oct 2002 BlackHat Asia 2002, Singapore

Computer Forensics – Tracking the Cyber vandals

Martin Khoo, CISSP Assistant Director, Defence & Response Head, SingCERT Infocomm Development Authority of Singapore (IDA)

Scope

- What is an IR Toolkit ?
- Setting up a Forensic Analysis Workbench
- Forensic Process
- Tools of the trade
- Case Study
- Forensic Failure & Anti-Forensics

3rd Oct 2002 BlackHat Asia 2002, Singapore

So you have an incident.....

- Investigator needs to know
 - where to look for clues
 - how to obtain necessary information from the victim system
- Often times the search path is not very clear and the plain sight information is not sufficient
- Be mindful that the information may be needed for criminal proceedings

What is an IR Toolkit?

- A carpenter or mechanic has a toolkit to do their work ; a surgeon has a surgical kit to perform open heart surgery
- IR Toolkit is used by incident responder to assist them in carrying out their mission – investigate the cause of an incident
- Consists of a mixture of tools and utilities; most of them are system/platform specific because it has to be customised to the particular operating system
- Most of them are public domain and are pretty useful to the investigator

• Some develop their own for specific purposes

3rd Oct 2002 BlackHat Asia 2002, Singapore

Forensic Analysis Workbench

- Forensic Analysis Workbench (FAW)
 - Hardware
 - Processor PIII if you don't like waiting
 - RAM (min -128 MB)
 - disk space as much as you can (rule of thumb at least equal to the largest hdisk you have)
 - SCSI card
 - Tape Drive and media DDS2/3
 - CD Writer
 - Software
 - system tools (clean copy) statically linked
 - Freeware The Coroner's Toolkit (TCT) and related tools
 - Commercial Encase Professional

Assembling your toolkit

- Assemble your IR kit and put it on a CD
- This will prevent the tools themselves getting trojaned, deleted or infected with viruses
- Also essential to have a scripting tool such as Perl on the CD
- An important resource which many investigators do not have in their IR Kit
- Use it to parse collected information and as a glue language for combining and parsing commands
- Can also use it to create utilities that provide needed functionalities not found in other tools

Absolutely essential rules of forensic analysis

- Do NOT work on the actual system
- Make an image copy of the system's hard drive and work on the image
- If circumstances do not permit taking an image dump then be careful when working on the victim system so as not to contaminate the information on the system
- This is very IMPORTANT if there is a possibility that the case will turn into a criminal investigation

• Caveat: Collecting volatile information may require that you work on the victim system

3rd Oct 2002 BlackHat Asia 2002, Singapore

Image Copy

- There are tools available to do this commercial and freeware
 - Encase Professional
 - Symantec Norton Ghost
 - PowerQuest DriveImage, DriveCopy
 - Freeware "dd" utility
- Hardware disk imaging tool
 - Fastbloc (Encase)
 - AVCDEF (Vogon)
- Caveat: The tool must not alter the timestamp of the files on the original copy (victim system)

Forensic Process

Acquisition

Get the data (normally disk images of the compromised system)

Reconnaissance

Use a variety of tools to capture both volatile (if working on a live system) and non-volatile (disk related) information

3rd Oct 2002 BlackHat Asia 2002, Singapore

Forensic Process

Recovery

- Attempt to get back "evidence" that has been removed (although not completely)
- Typically these are disk-related information like files and directories
- Time Lining
 - Chronology of events ; who did what when and hopefully also how it was done

Phases

- Forensic investigation of a compromised hard drive has 2 major phases
 - Collection/acquisition of data
 - Analysis of collected data
- Phase I can be accomplished using tools mentioned in previous slide

Type of Information

- Volatile Information
 - Certain state information of the system is transient
 - Network connections
 - Routing table
 - Process Table
 - Open ports
 - Users
 - These information are critical to the investigation and should be recorded as soon as the incident is discovered
 - Need tools to assist in capturing these information
 - Some of the tools can be system tools provide by the operating system
 - Third-party freeware tools can be used to get to the rest



3rd Oct 2002 BlackHat Asia 2002, Singapore

Non-volatile Information

- Information that remains after a reboot
 - configuration settings
 - System and data files
 - Registry settings
- Can be accessed through mapping of drives from the victim system to the FAW
- If possible work on an image copy of the victim system

Non-volatile Information – MAC (1)

MAC Times

- Files on the victim system will potentially give important clues to the investigator ; not only from their content but certain attributes
- In particular the investigator should record 3 important time attributes of the files
 - Modified
 - Access
 - Creation
- Collectively referred to as MAC times
- MAC times are one of the most valuable information to an investigator

Non-volatile Information – MAC (2)

- How do we get the MAC times ?
- Careful not to inadvertently change those attributes while trying to determine their values
- There are tools that can assist in the culling of these information
 - Foundstone Forensic Toolkit Afind
 - Mac.pl Perl script to obtain the MACs in a commadelimited output format (can use it in Excel for further processing)
- Once the MAC times are obtained and recorded the investigator may then proceed to do perform other checks on the victim system

3rd Oct 2002 BlackHat Asia 2002, Singapore

Non-volatile Information – MAC(3)

- Note that calculating checksums or doing file signature analysis will alter the MAC times on the files
- Always do the MAC time capture BEFORE you do anything else to the files on the victim machine
- You should then do a MD5 checksum on the MAC time output file to ensure integrity is maintained
- Be mindful of chain-of-custody procedure

3rd Oct 2002 BlackHat Asia 2002, Singapore

Non-volatile Information – LOG (1)

System/Application Logs

- The trustworthiness of the system/application logs depends on the type of incident
- If privilege access is obtained by the intruder then the integrity of the logs is in doubt
- The logs of interest to an investigator
 - Event Logs (System, Security, Application)
 - Specific application logs (IIS,SQL Server etc)
- Tools available to dump the NT event logs for further processing (dumpevt.exe , dumpevt.pl)

Non-volatile Information – Strings

- Discovering what an unknown executable is trying to do
- Most programs will have ASCII strings in their code. These strings remain intact when the code is compiled
- Investigator is looking for:
 - Usage statement
 - Author
 - System/Function calls
- Can infer what the program will do when executed
- Tools: Strings.exe, Finfo.pl

You have data....

- Phase II is when you need to derive information out of the collected data
- As in Phase I, tools are needed to assist the investigator
- We will look at 3 major open source forensic tools
- They complement each other

Tools of the Trade

- Tools are platform specific and are mainly freeware contributed by the security community
 - windows specific tools consists of collection of Perl scripts
 - the flag bearer for Unix/Linux is a collection of tools known as The Coroner's Toolkit (TCT) and 2 other complementing utilities
 - TCTUtils
 - Autopsy Forensic Browser

3rd Oct 2002 BlackHat Asia 2002, Singapore

Bring in the coroner...

- ♦ TCT The Coroner's Toolkit
 - Collection of 4 distinct group of tools
 - Provide powerful techniques for collection and analysis of forensic data
 - Goal is to reconstruct past events and/or recover deleted data
 - Can analyse activities on a live system and capture state information

3rd Oct 2002 BlackHat Asia 2002, Singapore

Coroner's Toolkit (1)

Grave-robber [Acquisition]

- Captures various types of data and creates MD5 hashes of them to preserve integrity
- Information captured include the (M)odified , (A)ccess and ©hanged times, deleted files that are still open, memory contents
- MAC time can be changed and also if too much time have elapsed , data related to the attack may be overwritten

Coroner's Toolkit (2)

- Pcat,ils,icat,file [Reconnaissance]
 - Records and analyses processes and filesystem (inode) data
 - pcat copies process memory from a live system
 - ils list inode information
 - icat copies files by inode number
 - File classifies files into various types

3rd Oct 2002 BlackHat Asia 2002, Singapore

Coroner's Toolkit (3)

- Mactime [Timelining]
 - Creates a chronological timeline of when files have been Modified, Accessed , or Changed (MAC) for each inode, along with their filenames

Coroner's Toolkit (4)

- unrm,lazarus [Recovery]
 - Recovers and analyses unallocated disk blocks on a file system
 - unrm collects information in unallocated portion of the file system
 - lazarus analyses raw data from unrm and attempts to classify the data

Extending the TCT (1)

TCTutils

- Collection of utilities that adds functionality to the TCT
 - bcat display contents of disk block to stdout
 - blockcalc map dd images and unrm results
 - fls display file and directory entries that have been deleted (use with –d option will list the names of all the deleted files on the disk)
 - find_file -determine which file has allocated an inode

3rd Oct 2002 BlackHat Asia 2002, Singapore

Extending the TCT (2)

- find_inode determines which inode has allocated a disk block
- Istat display information about an inode
- mac_merge merges the output from "fls –m" with the output from "mactime" to create a consolidated timeline file

Forensic Browser

- GUI front end to TCT and TCTUtils
- Allows an investigator to browse and analyse forensic images at the file, block, and inode level
- Allow for searching for keywords
- Approaching the capability of forensic tools on Windows (e.g. Encase)



3rd Oct 2002 BlackHat Asia 2002, Singapore

Forensic Case Study



3rd Oct 2002 BlackHat Asia 2002, Singapore

Evidence Collection

 Evidence is acquired in the form of "dd" images of each of the partition of the hard disk.

Syntax of command used

- dd if=/dev/hda1 of=/forensic/images/hda1.dd
- You will also want to calculate checksums on the images to ensure that their integrity can be verified (MD5)

- Mount the captured images on the forensic machine with non-intrusive options
 - Read only
 - No execute

 This is to prevent altering the information during the forensic examination process

- The layout of the victim hard disk is as follows
 - / hda8.dd
 - /boot hda1.dd
 - /usr hda5.dd
 - /home hda6.dd
 - -/var-hda7.dd

- mount –o ro,loop,nodev,noexec images/hda8.dd mnt
- mount –o ro,loop,nodev,noexec images/hda1.dd mnt/boot
- mount –o ro,loop,nodev,noexec images/hda5.dd mnt/usr
- mount –o ro,loop,nodev,noexec images/hda6.dd mnt/home
- mount –o ro,loop,nodev,noexec images/hda7.dd mnt/var

Acquisition & Reconnaissance Phase

- We use a combination of TCT and TCTUTILS to accomplish this
- What this phase accomplishes are
 - Obtain the MACs for existing files (grave-robber)
 - Obtain the MACs of unallocated inodes (ils)
 - Convert the ils output to same format as "grave-robber" (ils2mac)
 - Collect MACs of recently deleted files (for Linux only) (fls –m)

Deleted Files (1)

- Two types of data are deleted when a file is deleted from the file system
 - (i) Inode value in the directory entry
 - (ii) Inode content such as file size and block pointers
- If (i) is deleted then only the filename can be recovered
- If (ii) is deleted then the MACs can be recovered

3rd Oct 2002 BlackHat Asia 2002, Singapore



Evidence Processing Scripts

Script to process images using ils and ils2mac

```
for i in 1 5 6 7 8
do
ils images/hda$i.dd | ils2mac > data/hda$i.ils
done
cat data/hda?.ils data/body.ils
```

#Script to process images using fls

fls -m "mnt/boot/" images/hda1.dd > data/hda1.fls
fls -m "mnt/usr/" images/hda5.dd > data/hda5.fls
fls -m "mnt/home/" images/hda6.dd > data/hda6.fls
fls -m "mnt/var/" images/hda7.dd > data/hda7.fls
fls -m "mnt/" images/hda8.dd > data/hda8.fls
cat data/hda?.fls data/body.fls

3rd Oct 2002 BlackHat Asia 2002, Singapore

Deleted Files (2)

- If nothing is deleted then, one can recover all or part of a file (good!)
- Different OS deletes one, both or none of these information
- ♦ Linux saves both
- ♦ OpenBSD saves (i) deletes (ii)
- Solaris deletes both (tough!)

Timelining Phase

- The output from the following are concatenated
 - Grave-robber
 - ils2mac
 - fls –m
- The output becomes the input to "mactime"
 - mactime -p mnt/etc/passwd -g mnt/etc/group -b data/body.all 11/07/2000 > data/mactime.txt

3rd Oct 2002 BlackHat Asia 2002, Singapore

Initial Analysis

- Now comes the crucial part analysing the output of "mactime"
- You are looking for something suspicious ; out of the norm
 - Hints
 - Directory(ies) with unusual name(s)
 - File(s) with unusual names
 - Execution of certain commands
 - Keywords

Nov	0 8	00	22	: 51	L:56		156	C	– I	rwχ	r – x :	r-x	1010		use	<u>í</u> s
/mnt	:/h	dbpa	art	/4/	/for	rensic	:/cha	l/mn	t/ı	ısr	/mai	n/.C	i/ne	e d z		
							4096	C	dı	rwx	r - x :	r – x	1010		use	<u>s</u>
/mnt	:/h	dbpa	art	/4/	/for	rensic	:/cha	l/mn	t/ı	ısr	/mai	n/.C	i/pa	ki		
						105	2024	C	נ –	rwx	r – x :	r-x	1010		use	C S
/mnt	:/h	dbpa	art	/4/	/for	rensic	:/cha	l/mn	t/ı	ısr	/mai	n/.C	i/bx			
						1	2408	C	- I	rwx	r - x :	r – x	1010		use	C S
/mnt	:/h	dbpa	art	/4/	/for	rensic	:/cha	l/mn	t/ı	ısr	/mai	n/.C	i/ad	dn		
							118	C	- I	rwx	r - x :	r – x	1010		use	C S
/mnt	:/h	dbpa	art	/4/	/for	rensic	:/cha	l/mn	t/ı	ısr	/maı	n/.C	i/ /	Anap		
							8524	C	- I	rwx	r - x :	r – x	1010		use	<u>s</u>
/mnt	:/h	dbpa	art	/4/	/for	rensic	:/cha	l/mn	t/ı	ısr	/maı	n/.C	i/pa	ki/sl	ice2	2
						1	8535	C	- I	rwx	r - x :	r – x	1010		use	<u>s</u>
/mnt	:/h	dbpa	art	/4/	/for	rensic	:/cha	l/mn	t/ı	ısr	/maı	n/.C	i/fi	Х		
							83	C	נ –	rwx	r – x :	r-x	1010		use	<u>s</u>
/mnt	:/h	dbpa	art	/4/	/for	rensic	c/cha	l/mn	t/ı	ısr	/mai	n/.C	i/ad	dps		
							328	• • C	- I	rwx	r - x :	r-x	1010		use	<u>s</u>
/mnt	:/h	dbpa	art	/4/	/for	rensic	c/cha	l/mn	t/ı	ısr	/mai	n/.C	i/do			
							4096	c	dı	rwx	r - x :	r - x	1010		use	rs
/mnt	:/h	dbpa	art	/4/	for	ensic	/cha	l/mn	t/ı	ısr	/mai	n / . C	i/			
							6793	• • C	- 1	r w -	r :	r – –	1010		use	ſS
/mnt	:/h	dbpa	art	/4/	/for	rensic	c/cha	l/mn	t/ı	ısr	/mai	n/.C	i/pa	ki/st	rear	n.C
,							699	•• C	– I	rwx	r - x :	r – x	1010		use	C S
/mnt	:/h	dbpa	art	/4/	/for	rensic	/cha	l/mn	t/ı	ısr	/mai	n/.C	i/ch	mod-i	t	
						18	5988	• • C	- 1	rwx	r - x :	r – x	1010		use	C S
/mnt	:/h	dbpa	art	/4/	/for	rensic	/cha	l/mn	t/ı	ısr	/mai	n/.C	i/fi	nd		
,							188	•• C	– I	rwx	r – x :	r – x	1010		use	C S
/mnt	:/h	dbpa	art	/4/	/for	rensic	:/cha	l/mn	t∕ı	lsr	/mai	n/.C	i/rm	S		
Nov	8 0	00	22	: 52	2:09		9	m.c	11	rwx	rwx	rwx	root		root	t
/mnt	:/h	dbpa	art	/4/	for	ensic	/cha	1/mn	t/.	.ba	sh_l	hist	ory	-> /d	ev/1	null
			_				9	m.c	11	rwx	rwx	rwx	root		root	
/mnt	:/h	dbpa	art	/4/	for	ensic	/cha	⊥/mn	t/1	roo	t/.]	oash	_his	tory	-> ,	/dev/null

Recovery Phase

- The main tool here is the Autopsy Forensic Browser (AFB)
- It allows an investigator to perform the following functions
 - File & Directory Browsing
 - Block Browsing
 - Inode Browsing
 - Block Searching



3rd Oct 2002 BlackHat Asia 2002, Singapore

File Browsing

- Use the directories/files identified in the "mactime" output as the source
- Use a graphical tool to perform browsing of the identified suspicious directory (/usr/man/.Ci)
- The purpose of this step is to accomplish 2 objectives:
 - View the contents of file(s) in the directory (both existing and also deleted ones
 - Attempt to recover deleted file(s)

🙀 🛏 Netscape: /mnt/hdbpart/4/for	rensic/chal/mnt/usr/ on	honeypot.hda5.dd				- • • •
File Edit View Go Commun	nicator					Help
i 살 🔊 🧟	A 🍂	m 🐇	f (a)			N
Back Forward Reload	Home Search	Netscape Print	Security Shop	Stop		
🛛 🗤 🖌 Bookmarks 🦧 Location: 🖪	ttp://10.75.230.118	:688/3634579880/aut	opsv?dir=&inode=2&fu	unc=3&img=honevpot.hda	5. dd&hour=0	V 👔 What's Related
Red Hat Natwork	Support Softwa	ra 🖉 Hardwara 🥒 Dai		Search & Documents	tion 🖉 Downloads	Shon Nowe
	🗶 Support 🧶 Soliwa	ie 🧶 Haluwale 🧶 De	veropers 🦟 Ellibedded	Z Search Z Documenta	alloh 🦟 Dowilloaus	Z Shop Z News
Main Menu Files	Entries in /mnt/hdb	part/4/forensic/chal/m	nt/usr/man/.Ci/			1
Inode	<u>d</u> tp <u>Name</u>	Modified	Accessed	Changed Size	UID GID Inode	
Blocks Search	d <u>/</u>	11.08.2000 22:5	6:08 11.08.2000 22:56:57	11.08.2000 22:56:08 4096	100 1010 <u>109798</u>	
Dettern	d <u>/</u>	11.08.2000 22:5	2:12 11.08.2000 22:53:28	11.08.2000 22:52:12 4096	0 0 <u>123137</u>	
All Deleted Files	* d <u>ssh-1.2.27/</u>	11.08.2000 22:5	6:08 11:08:2000 22:56:08	11.08.2000 22:56:08 0	20 17275 <u>92757</u>	4
/mnt/hdbpart/4/forensic/chal/mnt/u	d <u>scan/</u>	08.22.2000 10:3	1:00 11:08:2000 22:51:53	11.08.2000 22:51:55 4096	100 1010 <u>109820</u>	
+ <u>/lost+found</u> +/doc	* d <u>bin/</u>	11.08.2000 22:5	4:43 11.08.2000 22:54:43	11.08.2000 22:54:43 0	100 1002 <u>63098</u>	
++/ElectricFence-2.1	* d <u>.temp6/</u>	11.08.2000 22:5	6:05 11:08:2000 22:56:05	11.08.2000 22:56:05 0	20 17275 <u>109870</u>	
++/ <u>dconfig=1.9.5</u> ++/ <u>glibc=2.1.3</u>	d <u>paki/</u>	08.09.2000 19:3	5:28 11.08.2000 22:51:53	11.08.2000 22:51:56 4096	100 1010 <u>17495</u>	
+++/examples.threads	d <u>(</u>	07.07.2000 23:5	5:07 11:08:2000 22:51:53	11.08.2000 22:51:56 4096	100 1010 93898	
++/shadow-utils-19990827 ++/bash-1.14.7	d <u>backup/</u>	11.08.2000 22:3	2:10 11.08.2000 22:52:10	11.08.2000 22:52:10 4096	U U <u>79064</u>	
++/SysVinit-2.78	· r <u>mistan-nameu</u>	06.03.2000 14.1	2.21 11.08.2000 22.34.45 2.21 11.08.2000 22.52.12	11.08.2000 22.30.08 80	100 1010 109805	
++/ <u>ncurses-5.0</u> ++/grep-2.4	r ach	06.03.2000 14:1	2.21 11.08.2000 22.02.15	11.08.2000 22:51:54 7229	100 1010 109805	
++/XFree86-xfs-3.3.6	* r_named tgz	11 08 2000 22:5	4.24 11.08.2000 22:54:24	11.08.2000 22:54:24 1029928	0 0 109807	
++/anacron-2.1 ++/fileutils-4.0	r sn nl	06 03 2000 14:1	2:21 11:08:2000 22:51:53	11 08 2000 22:51:55 5324	100 1010 109808	
++/textutils-2.0a		00.00.0000 111		·· •• •• •• •• •• •• •• •• •• •• •• •• •		N .
++/apmd-3.0fmal ++/arpwatch-2.1a4						
++ <u>/at-3.1.7</u>						
++/automake-1.4 ++/bash2-2.03						
++ <u>/bind-8.2.2_P5</u>						
+++/bog +++/html						
+++/misc						
+++/ <u>notes</u> +++//fc						
100%					II 💥	- 🏎 🗗 🖬 🥩
				La voot⊗	ton V (Contu	
। 🐝 🔇 🚺 🛄 🚺) 🔊 🎑 ٨	i 🎉 🎇 🔊 .	🌮 🥢 🔒		itep 🔨 (Captu	, 🖬 🚺 🖌
	ngapore					

🗱 -🖂 Netscape: /mnt/hdbpart/4/for	ensic/chal/mnt/usr/ o	n honeypot.hda5	5.dd								• • ×
File Edit View Go Commun	licator										Help
🌒 🎻 🔊 🔊		m)	4	ef.	ô.						NT
Back Forward Reload	Home Search	Netscape	Print	Security	Shon	Stop					
Dockmarke 👘 Location: 🖪	ttp://10_75_020_11	0.000 (20245700	000 /====	orr2di =_Ci	nodo_005	uno-20in-her-	mot bd-r	ddShawa	-0	1 What	Polatad
	ccp://10.75.230.11	0.000/30343/90		syruff=&1	noue=28F	unc=sarmy=none	ypoc. nuas.	uusaiour=	-0 17	Windt s	Related
🖉 🥒 Red Hat Network 🥒 Training	🖉 Support 🥒 Softwa	are 🥒 Hardware	e 🥒 Deve	lopers 🥠	Embedded	l 🧶 Search 🧶 🛙	Documentati	on 🥒 Do	wnloads 🧃	🖉 Shop 🥠 M	lews
Main Menu	Entries in /mnt/hdl	opart/4/forensic	/chal/mnt	/usr/man/.	.Ci/						Δ
<u>Files</u>											
Blocks	<u>d</u> tp <u>Name</u>	<u> </u>	<u>Iodified</u>	Acce	essed	Changed	<u>Size</u> <u>I</u>	UID GID	Inode		- II.
Search	d <u>/</u>	11.08.	2000 22:56:0	08 11.08.200	0 22:56:57	11.08.2000 22:56:08	3 4096 1	00 1010	<u>109798</u>		
	d <u>/</u>	11.08.	2000 22:52:	12 11.08.200	0 22:53:28	11.08.2000 22:52:12	2 4096 0) 0	<u>123137</u>		
All Deleted Files	* d <u>ssh-1.2.27/</u>	11.08.	2000 22:56:0	08 11.08.200	0 22:56:08	11.08.2000 22:56:08	30 2	20 17275	<u>92757</u>		
/mnt/hdbpart/4/forensic/chal/mnt/u	d <u>scan/</u>	08.22.	2000 10:31:0	00 11.08.200	0 22:51:53	11.08.2000 22:51:55	5 4096 1	00 1010	<u>109820</u>		
+ <u>/lost+found</u> +/doc	* d <u>bin/</u>	11.08.	2000 22:54:4	43 11.08.200	0 22:54:43	11.08.2000 22:54:43	30 1	100 1002	<u>63098</u>		
++/ElectricFence-2.1	* d <u>.temp6/</u>	11.08.	2000 22:56:0	05 11.08.200	0 22:56:05	11.08.2000 22:56:05	50 2	20 17275	<u>109870</u>		
++ <u>Adconfig=1.9.5</u>	d <u>paki/</u>	08.09.	2000 19:35:2	28 11.08.200	0 22:51:53	11.08.2000 22:51:56	5 4096 1	00 1010	<u>17495</u>		
++ <u>renoc-2.1.5</u> +++/examples.threads	d <u>/</u>	07.07.	2000 23:55:0	07 11.08.200	0 22:51:53	11.08.2000 22:51:56	5 4096 1	00 1010	<u>93898</u>		
++/shadow-utils-19990827	d <u>backup/</u>	11.08.	2000 22:52:	10 11.08.200	0 22:52:10	11.08.2000 22:52:10) 4096 () ()	<u>79064</u>		
++/bash-1.14.7 ++/SusVinit=2.78	* r <u>install-named</u>	06.03.	2 000 14:12:2	21 11. 0 8.2 00	0 22:54:43	11.08.2000 22:56:08	3 80 1	00 1010	<u>109803</u>		
++ <u>/ncurses-5.0</u>	r <u>snif</u>	06.03.	2000 14:12:2	21 11. 0 8.2 00	0 22:52:13	11.08.2000 22:51:54	4 722 9 1	00 1010	<u>109805</u>	4	
++/grep-2.4	r <u>a.sh</u>	06.03.	2000 14:12:2	22 11. 0 8.2 00	0 22:52:15	11.08.2000 22:51:54	4 714 1	00 1010	<u>109806</u>		
++ <u>/AFTEE60-XIS-3.3.0</u> ++/anacron-2.1	•							-			
++/fileutils-4.0		/mnt/hdbpart/4	/forensic/ch	al/mnt/usr/m	an/.Ci/a.sh	: ascii (report) – st	rings (report)	- save as	file		
++/textutils-2.0a ++/apmd-3.0final	Contents Of File: /	nnt/hdbpart/4/fo	rensic/cha	l/mnt/usr/	nan/.Ci/a.	sh					
++/arpwatch-2.1a4											
++/ <u>at-3.1.7</u>	echo "killing gay s	hit"									
++/aatomake=1.4 ++/bash2=2.03	rm -rf /usr/sbin/rp rm -rf /usr/sbin/nm	c.* /usr/sbin/smi bd /usr/sbin/yps	bd /usr/sb erv /usr/s	in/portmap bin/snmpd							
++/ <u>bind-8.2.2_P5</u>	rm -rf /sbin/rpc.st rm -rf /usr/sbin/lo	atd /usr/sbin/at ckd /sbin/lockd	d /usr/sbi	n/rpc.rquo	tad						
+++/bog +++/html	rm -rf /usr/sbin/nf rm -rf /usr/sbin/rp	sd /usr/bin/nfsd ciod /usr/bin/rp	ciod								
+++/misc	rm -rf /usr/sbin/sm rm -rf /usr/sbin/nm	bd /usr/bin/smbd bd /usr/bin/nmbd									
+++/notes	rm -rf /usr/sbin/ap rm -rf /usr/sbin/am	nd /usr/bin/apmd d /usr/bin/amd									
	rm -rf /usr/sbin/am killall -9 rpc.stat	q /usr/bin/əmq d rpc.rquoatd at	d nfsd								
	billsll -9 loobd ro	rind smhd nmhd							:: 285	40. a.c. c	
									<u>e 786</u>		₩ %
NX 🕭 🥅 🛲 🏈	N 🔊 🏹 /N		200 2	× ×		3 🛛 🔪 (root@.	🔳 root@	p 🗙 (0	Captu 📗 (9 👝 🛛 🕻	
' 💖 🕪 🐝 🖷 🔛	» 🖓 💐 🖾 🕷	3 🍋 🖏	X III	V 🖉	2 4	4 🔲 (root@.	🕵 Netso	:a		U 🛛 🗖	/25/02
$\Box_{1} = \Box_{1} = \Box_{1$	11540010						WI VIII I XII				

Detail Analysis

- Some interesting deleted files that can be noticed includes named.tgz, named.tar, ssh-1.2.27.tar, nfsutils-0.1.9.1-1.i386.rpm and wuftpd.rpm
- These files can be recovered using the icat utility of TCT
- Need to specify the inode of the required file (obtain from the AFB listing)

3rd Oct 2002 BlackHat Asia 2002, Singapore

File Recovery

- We will attempt to recover two of the deleted files using icat.
 - Syntax: icat <image> <inode> > <save file>
 - icat images/hda5.dd 109791 > recovered/hda5.ssh-1.2.27.tar
 - icat images/hda5.dd 109861 > recovered/hda5.named.tar
 - icat images/hda5.dd 109866 > recovered/hda5.wuftpd.rpm

🐺 –🛤 Netscape: /mnt/h	dbpart/4/fon	ensic/chal/r	nnt/usr/ o	n honeypot.	hda5.dd									
File Edit View G	o Commun	icator												Help
i 🗳 💕	3		Ž	M.	ظ	a C	<u>@</u> ,							N
Back Forward	Reload	Home	Search	Netscape	Print	Security	Shop	Stop						
🚽 Bookmarks 🙏	Location: ht	ttp://10.7	5.230.11	8:688/3634	579880/aut	ops y ?dir=0	kinode=2&f	unc=3&imq=ho	oneypot.hda	5. dda	Shour=0)	/ () W	/hat's Related
Red Hat Network	🖉 Training		A Software	ara 🥒 Hard		volonore 🖌	Fmhaddad	Search	Document:	ation	Dou	nloade	 Shon	A Noure
	🛫 naning		- 0011MG		ware 🐙 De	2.24 44 0 0.2	000 00.54.50			400	4010	400000	Z oliop	A NCMO
<u>Main Menu</u> Files	l î l	r <u>qs</u> * r seb_1	1 2 27 tox	r r	18.10.2000 14:1	2:21 11.08.2 2:37 11.08.2	000 22:51:55	11.08.2000 22:5	6.08 18608240	100	1010	109809 109701 4		
Inode		r svelo	ad	r r	6 03 2000 03.3	2.07 11.00.2 2.21 11.08.2	000 22:02:09	11.08.2000 22.5	1.55 350006	100	1010	109791		
Blocks		* x temp	2 2	1	0.201006.07-0	2.21 11.00.2 2.27 11.08.2	000 22:01:00	11.08.2000 22:5	6.05 2286	20	17275	100916		
Search		r inetd	<u>14</u>	1 C	6.00.1990 07.0	2.27 11.00.2 2.21 11.08.2	000 22:02:00	11.08.2000 22.5	1.55 147000	100	1010	100814		
	III	* r temp	3	1	0 30 1006 07 0	2.21 11.00.2 2.27 11.08.2	000 22:51:55	11.08.2000 22.5	6.05 2414	20	17275	100818		
All Deleted Files /mnt/hdbnart/4/forensic/ch	hal/mnt/u	* r temp	. <u>.</u> .4	1	0.30.1990 07.0 0 30 1996 07.0	2.27 11.00.2 2.27 11.08.2	000 22:52:53	11.08.2000.22.5	6.05 2063	20	17275	109853		
+ <u>Aost+found</u>		* r temp	5	1	0.30.1996 01.0	2.28 11.00.2	000 22:52:53	11.08.2000.22.5	6.05 2843	20	17275	100860		
+ <u>/doc</u> ++/ElectricHence_21		r clean	<u></u>	- r	6 03 2000 14:1	7.56 11.00.2	000 22:52:14	11.08.2000.22.5	1.55 698	100	1010	109819		
++ <u>/ldconfig=1.9.5</u>		r snan	<u>-</u>	, C	6 03 2000 14:1	2.21 11 08 2	000 22:56:04	11.08.2000.22:5	1:55 3098	100	1010	109848		
++/glibc-2.1.3		* r ntron		1	0 30 1996 07 0	2.27 11 08 2	000 22:52:53	11.08.2000 22:5	6.05 2213	20	17275	100840		
+++/examples.ureads ++/shadow-utils-199908	27	r o		- C	6 03 2000 14:1	2.21 11.00.2	000 22:51:53	11.08.2000.22:5	1.55 133344	100	1010	109850		
++/bash-1.14.7		r killall		0	6 03 2000 14:1	2.21 11.08.2	000 22:51:53	11.08.2000.22:5	1:55 12495	100	1010	109852		
++ <u>/SysVinit-2.78</u> ++/ncurses-5.0		r nstre	e	, C	6 03 2000 14:1	2.21 11.08.2	000 22:51:53	11.08.2000 22:5	1:55 49800	100	1010	109851		
++/grep-2.4		r fix	<u>~</u>		6 03 2000 14:1	2.22 11 08 2	000 22:52:10	11.08.2000.22:5	1:56 18535	100	1010	109854		
++/XFree86-xfs-3.3.6 ++/anacron-2.1		1 114			0.00.2000 14.1	2.22 11.00.2	000 22.02.10	11.00.2000 22.0	1.50 10505	100	1010	102004		N.
++ <u>/fileutils-4.0</u>				/mnt/hdhn:	art/4/forensic/c	hal/mnt/usr/	nan/ Ci/ temn'	5 · ascii (renort)	– strings (ren	ort) -	catre ac	file		토
++ <u>/textutils=2.0a</u>		Contents 0)f File: /r	nnt/hdbpart/	4/forensic/c	hal/mnt/us:	c/man/.Ci/.t	cemp5						
++/apwatch-2.1a4														
++ <u>/at-3.1.7</u>		; 29000 _	_mpn_submu	1_1 Multi	ply a limb v	ector with	a single li	imb and						
++/automake=1.4 ++/bash2=2.03		; subtract	t the prod	uct from a s	econd limb v	ector.								
++/bind-8.2.2_P5		; Copyrigh	it (C) 1993	2, 1994 Free	Software Fo	undation, :	Inc.							
+++/ <u>bog</u> +++/btml		; This fil	le is part	of the GNU	MP Library.									
+++ <u>/misc</u>		; The GNU ; it under	MP Library the term:	y is free so s of the GNU	ftware; you Library Gen	can redist: eral Publi	cibute it an C License as	id/or modify ; published by						
+++ <u>/notes</u>		; the Free ; option)	2 Software any later	Foundation; version.	either vers	ion 2 of t	ne License,	or (at your						
		; The GNU	MP Library	y is distrib	uted in the	hope that .	it will be u	seful, but						Υ.
												8	, 🧤 🧃	P 🖪 🎸
								ПП - Г			1			
• 🐝 🕸 🐻	I) 🔊 🖗	Q. 🕂) 🔏 🕯	阕 🎉	Ø 🕺	2 4	3 (roo 4 (roo	it@ 🔳 roo it@ 🐺 Net	t@p tsca	X (C:	aptu	<u>ය</u> ව	01/28/02

😹 – 🖬 Netscape: /mnt/hdbpart/4/fo	rensic/chal/mnt/usr/ o	n honeypot.hda5.	dd					- ×
File Edit View Go Commun	nicator							Help
A A A A A A A A A A A A A A A A A A A	🔬 💉 Home Search	M. Netscape	ा हिं Print Security	🔕 Shop	Stop			N
📲 Bookmarks 🛷 Location: 🖟	nttp://10.75.230.11	3:688/363457988	30/autopsy?dir=8	kinode=2&f	unc=3&img=honeypot.hd	a5. dd&hour=0	7 👘 v	Vhat's Related
Red Hat Network 🥠 Training	🧶 Support 🥠 Softwa	are 🧶 Hardware	🧶 Developers 🦼	Embedded	🥒 Search 🧶 Documen	tation 🥒 Downl	oads 🧶 Shop	🥒 News
Main Menu Files Inode Blocks Search All Deleted Files /mnt/hdbpart/4/forensic/chal/mnt/us +/lost+found +/doc ++/ElectricFence-2.1 ++/dconfig-1.9.5 ++/gibc-2.1.3 +++/examples.threads ++/shadow-utils-19990827 ++/bash-1.14.7 ++SysVinit-2.78 ++/ncurses-5.0 ++/grep-2.4 ++/free-216	r do r addn * r named.tar * r install-sshd1 r mS r bx * r in.ftpd r chmod-it r needz * r install-statd * r nfs-utils-0.1.9.1 * r wuftpd.rpm * r install-wu * r install-sshd * r temp7	06.03.2 06.03.2 06.03.2 10.12.2 08.09.2 06.03.2 08.22.2 08.22.2 08.22.2 10.12.2 10.12.2 10.12.2 06.03.2 10.12.2	000 14:12:22 11.08.2 000 14:12:22 11.08.2 000 14:12:21 11.08.2 000 15:12:42 11.08.2 000 05:12:42 11.08.2 000 05:12:42 11.08.2 000 05:43:31 11.08.2 000 19:19:02 11.08.2 000 14:12:21 11.08.2 000 14:12:21 11.08.2 000 10:38:03 11.08.2 000 10:38:03 11.08.2 000 10:48:36 11.08.2 000 10:47:03 11.08.2 000 06:37:06 11.08.2 000 06:40:59 11.08.2 000 06:40:59 11.08.2 000 14:24:29 11.08.2 000 14:24:29 11.08.2 000 14:24:29 11.08.2	000 22:55:58 000 22:55:47 000 22:54:21 000 22:56:11 000 22:56:25 000 22:56:25 000 22:54:21 000 22:51:53 000 22:51:53 000 22:53:41 000 22:53:43 000 22:53:13 000 22:53:13	11.08.2000 22:51:56 328 11.08.2000 22:51:56 12408 11.08.2000 22:54:43 1026048 11.08.2000 22:56:08 1153 11.08.2000 22:51:56 188 11.08.2000 22:51:56 1052024 11.08.2000 22:51:56 699 11.08.2000 22:51:56 156 11.08.2000 22:51:56 156 11.08.2000 22:56:08 180703 11.08.2000 22:56:08 195637 11.08.2000 22:56:08 1075 11.08.2000 22:56:08 1076 11.08.2000 22:56:08 1076 11.08.2000 22:56:08 1076	100 1010 10 100 1010 10	9857 9858 9861 9801 9859 9860 9861 9862 9863 9864 9865 9866 9865 9866 9867 9802 9871	
++/anacron-2.1 ++/filentils-4.0		/mnt/hdhnavt/4/fo	rensic/chal/mnt/usr/r	nan/ Ci/ temp	5 · ascii (renort) – strings (re	nort) – save as file		<u>म</u>
++/ <u>textutils-2.0a</u> ++/apmd-3.0final ++/arpwatch-2.1a4 ++/at-3.1.7 ++/automake-1.4	Contents Of File: /m ; 29000 _mpn_submul ; subtract the produ	nt/hdbpart/4/for L_1 Multiply a Lot from a second	ensic/chal/mnt/us; limb vector with limb vector.	:/mən/.Ci/.t a single li	xemp5 mb and			
++ <u>/bash2-2.03</u> ++ <u>/bind-8.2.2_P5</u> +++ <u>/bog</u> +++ <u>/html</u> +++ <u>/misc</u> +++ <u>/notes</u> +++ <u>/nfc</u>	; Copyright (C) 1992 ; This file is part ; The GNU MP Library ; it under the terms ; the Free Software ; option) any later	2, 1994 Free Soft of the GNU MP Lil is free softwar of the GNU Libr Foundation; eith version.	ware Foundation, 1 brary. e; you can redist, ary General Public er version 2 of th	inc. Tibute it an License as License,	d/or modify : published by or (at your			
	; The GNU MP Library • ыттысыт вым марран) is distributed . TV: without even	in the hope that : the implied warrs	it will be u	Iseful, but WANTARTI TTV			Y
	-						i 🐝 🐜 d)P 🖬 🎸
• 🐝 🐟 🐼 💷 🤇) 🔊 🎑 🕅	3	à 🔊 🖉	2 4	3 (root@) ro 4 (root@) N	ot@p 🗙 (Cap etsca	tu	B:35

File Analysis

- AFB also allows an investigator to do a "strings" on binary files
- "Strings" is used to find out what are the ASCII strings embedded in an unknown executable
- The output can be used to infer the functionalities of the executable



Reporting

- AFB also provides the ability to generate a report containing the strings output and all the necessary attributes of a binary
 - UID, GID, inode, MACs, disk blocks allocated, MD5 checksums
- This will form part of the forensic report that an investigator would need to produce

-

autopsy string Report (ver 1.01)

File: /mnt/hdbpart/4/forensic/chal/mnt/usr/man/.Ci/fix MD5 of file: 26d58504aa969f095043a9fabf684b57 MD5 of strings: de5376687d0131791d6818f7987cef70 Image: /mnt/hdbpart/4/forensic/chal/honeypot.hda5.dd Date Generated: Mon Jan 28 08:38:03 2002 Investigator: mkhoo inode: 109854 Allocated uid / gid: 1010 / 100 mode: rwxr-xr-x size: 18535 num of links: 1 Modified: 06.03.2000 14:12:22 (SGT+0) Accessed: 11.08.2000 22:52:10 (SGT+0) Changed: 11.08.2000 22:51:56 (SGT+0) 01.01.1970 07:30:00 Deleted: (SGT+0) Direct Blocks: 240901 240902 240903 240904 240905 /lib/ld-linux.so.2 gmon_start__ libc.so.6 strepy chown utimes system settimeofday chmod strrchr fprintf deregister frame info fseek ferror strncpy IO getc fread gettimeofday ftell sprintf fclose stderr fwrite exit fopen _IO_stdin_used ____libc_start_main ___register_frame_info xstat GLIBC_2.0 GLIBC_2.1 PTRh QVhp cp %s %s mv %s %s fix: Can't open %s fix: Last 17 bytes not zero F 100%



And so.....

- TCTUTILS and the Autopsy Forensic Browser provides many critical functions that complement that of the TCT
- The AFB provides a GUI front end to make the low-level forensic tools in the TCT and TCTUTILS easier to use
- However, the investigator has to come up with his/her analysis and conclusion



3rd Oct 2002 BlackHat Asia 2002, Singapore_____

Forensic Failure & Anti-Forensic

Forensic Failure

- Compromise is at the kernel space instead of user space
- Traditional forensic tools completely failed during an investigation
- Change the behavior of ANY command executed on the system without changing the program binaries themselves
- Any trusted toolkit an investigator used will be useless in such a situation

Loadable Kernel Module

 LKM provides dynamic functionalities by altering a running kernel without rebooting – Linux - insmod <module name>

 LKM can access all functions and memory areas of a kernel

• A rouge LKM will create untold havoc

3rd Oct 2002 BlackHat Asia 2002, Singapore

LKM gone awry....

- LKM intercepts system calls made by user space programs
- The "syscall" table is altered which changes the OS behavior
- "syscall" table is the entry point into the OS provided to user space programs and lives in kernel space

Evil LKM

- OS maps all user space commands to the function calls on the syscall table
- KNARK (a evil Linux LKM) alters the following system calls on the syscall table

- Getdents - get directory entries

• By compromising this call, knark is able to hide files and directories from user-level program

Evil LKM

- kill sends a signal to a process to kill it Extra signals (#31) will trigger the option flags of a process to be set to the "hidden" state. Signal #32 unhides the process
- read reads content from a disk file. Knark compromises this system call to hide intruder connection specifics from netstat
- ioctl changes the behavior of files and devices. Use to clear the promiscuous flag on the network interface
- fork,clone spawns a new process. Use to hide all child process created from a hidden parent process

So How.....

Preventive Measures

- Securing the "syscall" table
 - Using a LKM (of course) to watch the syscall table and monitor when othe LKM are loaded
 - This "sentry" module will alert the sysadmin when changes are made to the syscall table
- Investigative Measures
 - Kernel mode "ps-like" tool
 - Retrieves executable images of each process (Carbonite)

3rd Oct 2002 BlackHat Asia 2002, Singapore

Anti-Forensics

- Attempt to downgrade the quantity and quality of the "evidence" that will be able to an investigator
- Data hiding and Data destruction
- Exploiting limitations of the current forensic tools (TCT, TCTUTILS)
- The anti-forensic techniques works for the ext2 file system (Linux)

Anti-forenic Toolkit

- The Runefs toolkit allows hiding of data in areas of the hard drive that the TCT will never look
- The Defiler's Toolkit (TDT) performs file system sanitization "with surgical precision"
- Removes not only data blocks but also all entries in the file system pertaining to the existence of a file (inodes & directory entries)

Is there hope?

- Not to rely on the local file system as the only record of disk operations
- Storing inode updates to a remote and secure syslog server
- Requires modifying the kernel vfs layer to accomplish this

Resources

- The Coroner's Toolkit (TCT)
 - http://www.porcupine.org/forensics
- TCTUTILS & Autopsy Forensic Browser (AFB)
 - http://www.cerias.purdue.edu/homes/carrier/forensics/
- The @stake Sleuth Kit (TASK)
 - http://www.atstake.com/research/tools/index.html#fore nsics
- ♦ TDT, Runefs
 - Phrack 59 http://www.phrack.org

Thank You markhoo@singcert.org.sg

3rd Oct 2002 BlackHat Asia 2002, Singapore