

Re: Hacked or not ?

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-05/0101.html>

From: Matthew Seaman (*m.seaman_at_infracaninophile.co.uk*)

Date: 05/21/04

Date: Fri, 21 May 2004 22:40:58 +0100

To: Tom Rhodes <trhodes@FreeBSD.org>

On Fri, May 21, 2004 at 04:11:33PM -0400, Tom Rhodes wrote:

> *On Fri, 21 May 2004 21:02:54 +0100*

> *Matthew Seaman <m.seaman@infracaninophile.co.uk> wrote:*

>

>> *On Fri, May 21, 2004 at 03:52:45PM +0200, RazorOnFreeBSD wrote:*

>>

>>> *I have a 4.9-STABLE FreeBSD box apparently hacked!*

>>> *Yesterday I ran chkrootkit-0.41 and I don't like some of the outputs.*

>>> *Those are:*

>>> *chfn ... INFECTED*

>>> *chsh ... INFECTED*

>>> *date ... INFECTED*

>>> *ls ... INFECTED*

>>> *ps ... INFECTED*

>>

>> *Sheesh. Not this *again*. This is a false alarm: chkrootkit is*

>> *exceedingly sensitive to something about the way such programs work*

>> *under FreeBSD and has to be continually futzed so that it knows not to*

>> *complain on each successive version of FreeBSD. Comes up in this or*

>> *other FreeBSD lists just about every week.*

>>

>> *Relax. You're not compromised. You just need better tools.*

>>

>

> *I love the "just need better tools." without any recommendation*

> *for him.*

Well, the question was "has my machine been compromised", which I answered.

The current version of chkrootkit in ports (0.43) has a problem whereby it thinks FreeBSD 4.10 is a higher version than FreeBSD 5.0, which means that it reports certain programs are infected because they *don't* fail in the expected way found on 5.0 or above. Here's a patch:

FreeBSD–Security: Re: Hacked or not ?

```
--- chkrootkit.orig Fri May 21 22:19:16 2004
+++ chkrootkit Fri May 21 22:36:29 2004
@@ -257,7 +257,7 @@
{
  prog=""
  if [ \( "${SYSTEM}" = "Linux" -o \( "${SYSTEM}" = "FreeBSD" -a \
- ${V} -gt 43 \) \) -a "${ROOTDIR}" = "/" ]; then
+ ${V} -gt 403 \) \) -a "${ROOTDIR}" = "/" ]; then
    [ ! -x /usr/local/sbin/chkproc ] && prog="/usr/local/sbin/chkproc"
    [ ! -x /usr/local/sbin/chkdirs ] && prog="$prog /usr/local/sbin/chkdirs"
    if [ "$prog" != "" ]; then
@@ -1080,7 +1080,7 @@
    STATUS=${INFECTED}
  fi;;
  FreeBSD)
- [ $V -gt 50 ] && n=1 || n=2
+ [ $V -gt 500 ] && n=1 || n=2
    if [ ` ${strings} -a ${CMD} | \
      ${egrep} -c "${GENERIC_ROOTKIT_LABEL}"` -ne $n ]
    then
@@ -1114,7 +1114,7 @@
    fi
  fi;;
  FreeBSD)
- [ $V -gt 50 ] && n=1 || n=2
+ [ $V -gt 500 ] && n=1 || n=2
    if [ ` ${strings} -a ${CMD} | ${egrep} -c "${GENERIC_ROOTKIT_LABEL}"` -ne $n ]
    then
      STATUS=${INFECTED}
@@ -1145,10 +1145,10 @@
    ret=` ${strings} -a ${CMD} | ${egrep} -c "${GENERAL}"`
    if [ ${ret} -gt 0 ]; then
      case ${ret} in
- 1) [ "${SYSTEM}" = "OpenBSD" -a ${V} -le 27 -o ${V} -ge 30 ] && \
+ 1) [ "${SYSTEM}" = "OpenBSD" -a ${V} -le 207 -o ${V} -ge 300 ] && \
      STATUS=${NOT_INFECTED} || STATUS=${INFECTED};;
      2) [ "${SYSTEM}" = "FreeBSD" -o ${SYSTEM} = "NetBSD" -o ${SYSTEM} = \
- "OpenBSD" -a ${V} -ge 28 ] && STATUS=${NOT_INFECTED} || STATUS=${INFECTED};;
+ "OpenBSD" -a ${V} -ge 208 ] && STATUS=${NOT_INFECTED} || STATUS=${INFECTED};;

      *) STATUS=${INFECTED};;
    esac
@@ -1622,7 +1622,7 @@
  expertmode_output "${ls} -l ${CMD}"
  return 5
fi
- [ "${SYSTEM}" = "FreeBSD" -a $V -gt 50 ] &&
+ [ "${SYSTEM}" = "FreeBSD" -a $V -gt 500 ] &&
{
  if [ ` ${strings} -a ${CMD} | ${egrep} "${GENERIC_ROOTKIT_LABEL}" | \
    ${egrep} -c "$$_L" ` -ne 2 ]; then
```

Re: Hacked or not ?

FreeBSD–Security: Re: Hacked or not ?

```
@@ -2398,9 +2398,9 @@
SYSTEM=${uname} -s`
VERSION=${uname} -r`
if [ "${SYSTEM}" != "FreeBSD" -a "${SYSTEM}" != "OpenBSD" ]; then
- V=44
+ V=404
else
- V=`echo $VERSION | cut -d- -f 1 | ${sed} 's\./g`
+ V=$(( `echo $VERSION | cut -d- -f 1 | ${sed} 's\./ * 100 + /g` ))
fi

# ps command
```

Better tools in this case: in this case, I'd say tripwire or one of the work-alikes.

Cheers,

Matthew

--

Dr Matthew J Seaman MA, D.Phil.

PGP: <http://www.infracaninophile.co.uk/pgpkey>
Tel: +44 1628 476614

26 The Paddocks
Savill Way
Marlow
Bucks., SL7 1TH UK

-
- application/pgp–signature attachment: stored