

FreeBSD-Security: Re: ttyv for local only?

Re: ttyv for local only?

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-06/0064.html>

From: Dave (*mudman_at_metafocus.net*)

Date: 06/30/04

Date: Tue, 29 Jun 2004 17:50:21 -0700 (PDT)

To: Igor Roshchin <str@komkon.org>

```
console none unknown off secure
ttyv0 "/usr/libexec/getty Pc" cons25 on secure
# Virtual terminals
ttyv1 "/usr/libexec/getty Pc" cons25 on secure
ttyv2 "/usr/libexec/getty Pc" cons25 on secure
ttyv3 "/usr/libexec/getty Pc" cons25 on secure
ttyv4 "/usr/libexec/getty Pc" cons25 on secure
ttyv5 "/usr/libexec/getty Pc" cons25 on secure
ttyv6 "/usr/libexec/getty Pc" cons25 on secure
ttyv7 "/usr/libexec/getty Pc" cons25 on secure
ttyv8 "/usr/X11R6/bin/xdm -nodaemon" xterm off secure
```

I don't really see a problem here. My mystery logins are actually still continuing. I'm going to see if I can code a mousetrap to find out who is doing it. I did a fresh source compile of world from the latest cvsup for 5.2.1 REL, and ran mergemaster to look for differing startup scripts...

No luck yet. I wrote down the byte-sizes of sockstat, ps, and getty on a piece of paper. I'm going to watch them over the next couple of days.

On Mon, 28 Jun 2004, Igor Roshchin wrote:

```
> You might want to check your /etc/ttys file,
> if it still shows ttyv* as for the console logins or for network logins.
```

>

```
> Igor
```

>

>

```
> Igor Roshchin
```

```
> System Administrator
```

```
> KomKon Sites
```

>

>

```
> > From igor@giganda.komkon.org Mon Jun 28 18:19:49 2004
```

```
> > Date: Mon, 28 Jun 2004 14:13:25 -0700 (PDT)
```

```
> > From: Dave <mudman@metafocus.net>
```

```
> > To: Neo-Vortex <root@Neo-Vortex.Ath.Cx>
```

```
> > Cc: freebsd-security@freebsd.org
```

```
> > Subject: Re: ttyv for local only?
```

> >

> >

> >

```
> > Hmm, I think I am in some kind of trouble. I have been getting login
```

```
> > errors on ttyv that definitely couldn't be me. The only other person who
```

```
> > lives with me is my wife, and it isn't her either.
```

Re: ttyv for local only?

FreeBSD-Security: Re: ttyv for local only?

```
> >
> > gmail, popa3d, etc.. I am even getting them on my ftp too.
> >
> > If someone had root access, they should be able to know what I am running
> > on my system rather than trying these idiotic logins. In fact, they could
> > telnet to my mail port and look for the Sendmail greeting to know that I
> > don't run gmail, or portping 125 to see if I am running any kind of POP3
> > server. A piece of me feels it is just some internet sweeper that
> > mindlessly tries logging in or ftping to certain things, and moves to the
> > next IP address. I am also wondering if it is just a syslogd thing that
> > the login failures were simply reported on ttyv2 rather than actually
> > happening there, but then why not ttyv0, which is the 'main' thing it
> > prints to?
> >
> > I recently just backed up my system so I'm not feeling that bad but...
> > but... how? There is no sense in making the same mistake twice. I could
> > run cvsup, compile a fresh binary of sockstat and ps to see if anything is
> > running...
> >
> > I'll consider turning snp off and recompiling my kernel. But that would
> > just get rid of the messages, not help me get to the heart of it.
> >
> >
> > On Sun, 27 Jun 2004, Neo-Vortex wrote:
> >
> > > Hmmm, ttyv* is for local console's only (normally anyway) and tty* is for
> > > remote (ssh, screen, telnet, etc), are you sure some idiot didnt try to
> > > logon as qmaild in the third console when you wernt looking?
> > >
> > > On Sat, 26 Jun 2004, Dave wrote:
> > >
> > > >
> > > > I get this in my security postings.
> > > >
> > > > Jun [undisclosed time] [undiscl.] login: 2 LOGIN FAILURES ON ttyv2
> > > > Jun [undisclosed time] [undiscl.] login: 2 LOGIN FAILURES ON ttyv2, qmaild
> > > >
> > > > As it turns out, I'm not running gmail :) And if I did, it would
> > > > definitely have a nologin shell. But that's beside the point-
> > > >
> > > > I have had a perception that ttyv was for local/console logins, and that
> > > > just "tty" was for remote logins.
> > > >
> > > > Is my understanding wrong here?
> > > >
> > > >
> > > > _____
> > > > freebsd-security@freebsd.org mailing list
> > > > http://lists.freebsd.org/mailman/listinfo/freebsd-security
> > > > To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"
> > > >
> > > >
> > > > _____
> > > > freebsd-security@freebsd.org mailing list
> > > > http://lists.freebsd.org/mailman/listinfo/freebsd-security
> > > > To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"
> > > >
> > > >
> > > > _____
> > > > freebsd-security@freebsd.org mailing list
> > > > http://lists.freebsd.org/mailman/listinfo/freebsd-security
> > > > To unsubscribe, send any mail to "freebsd-security-unsubscribe@freebsd.org"
```