

Re: last command – strange entries?

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-06/0010.html>

From: Neo-Vortex (root_at_Neo-Vortex.net)

Date: 06/16/05

Date: Thu, 16 Jun 2005 23:24:30 +1000 (EST)

To: Saurabh Bhasin <sbhasin@gmail.com>

On Wed, 15 Jun 2005, Saurabh Bhasin wrote:

> Greetings,
>
> I am seeing strange entries when i perform "last -20" for example.
> Here's a sample output becuase I can not seem to make any sense out of
> this in the last two days and can't find any information online. Any
> help is appreciated.
>
> 0 F=°Btty Wed Dec 31 16:00 still logged in
> 0 6Û~Btty Wed Dec 31 16:00 still logged in
> 0 mÛ~Btty Wed Dec 31 16:00 still logged in
> 7 mÛ~Btyv Wed Dec 31 16:00 still logged in
> 0 ~Btty Wed Dec 31 16:00 still logged in
> 0 (o~Btty Wed Dec 31 16:00 still logged in
> 2 ëg~Btty Wed Dec 31 16:00 still logged in
> .
>
> and it keeps going for 20 lines.

The last command uses /var/log/wtmp and /var/log/utmp (mabe even /var/log/lastlog) – anyway, the point is, it uses those files to get the information, now, it appears as if they have become corrupt, mabe by userland/kernel land desynch? bad upgrade? tried a reboot?

Else, can you give us more details about the system, past upgrades, intrusions?

~NVX

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"