

Re: Xwindow "ghost"?

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux.x/2005-03/0108.html>

From: Larry I Smith (larryXiXsmith_at_verizon.net)

Date: 03/17/05

Date: Thu, 17 Mar 2005 18:35:35 GMT

Larry I Smith wrote:

> *mjt* wrote:

>> (Larry I Smith <larryXiXsmith@verizon.net>) scribbled:

>>

>>>> as we say in Texas, "He's got a big hole in his screen door." :)

>>>>

>>>> *mtobler@stimp*y:~> whois 220.154.236.183

>>>> *descr*: Asia Pacific Network Information Center, Pty. Ltd.

>>

>>> *There's no network activity, and I'm behind 2 firewalls*

>>> (*one hardware and one software*).

>>>

>>> *Since this IP ALWAYS shows as the X IP for the currently*

>>> *logged on user, and moves from user to user as I log off*

>>> *then log on as a different user (via kdm), I'm thinking*

>>> *that it is some kind of pseudo IP used by either X or KDE.*

>>>

>>> *If I've been 'invaded', how do I tell, and what can I*

>>> *do about it?*

>> [*snip*]

>>

>>

>> <http://www.chkrootkit.org/>

>> <http://www.rootkit.nl/>

>>

>

> *I ran both tools. Neither tool found anything.*

>

> *I'm stumped...*

>

> *Regards,*

> *Larry*

>

Hmm, I did this:

- 1) shutdown linux and power-off the pc
- 3) turn off the DSL modem

comp.os.linux.x: Re: Xwindow "ghost"?

- 4) power-on pc
- 5) waited for the 'kdm' GUI logon screen
- 6) started a terminal as root (ctrl-alt-f2)
- 7) from the terminal 'last -di' shows NO IP connections
- 8) switch back to kdm screen and logon as 'user1'
- 9) switch back to the terminal and run 'last -di'
- 10) 'last -di' now shows a 'still logged in' entry
for 220.170.236.183:

```
user1 pts/1 0.0.0.0 Thu Mar 17 12:18 still logged in
user1 pts/0 0.0.0.0 Thu Mar 17 12:07 still logged in
user1 :0 220.170.236.183 Thu Mar 17 12:07 still logged in
```

This can not be correct. The DSL modem is turned off, and there are no other machines on this (home) network.

Notice that the IP changed from 220.154.236.183 to 220.170.236.183 after the power off/on cycle.

Surely this is either a bug in 'last' -or- there is some kind of 'magic' IP manipulation going on in either X or KDE????

Regards,
Larry

--

Anti-spam address, change each 'X' to '.' to reply directly.