

Re: Xwindow "ghost"?

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux.x/2005-03/0112.html>

From: Larry I Smith (larryXiXsmith_at_verizon.net)

Date: 03/17/05

Date: Thu, 17 Mar 2005 20:38:43 GMT

Geoff wrote:

> *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@stimpy:~> 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*

>>

>

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

> *I get much the same thing here, though with a different ip. Haven't got
> time now to work out what's going on and googling for the "last command"
> is not very helpful! Logging on from a virtual terminal gives an ip of
> 0.0.0.0
>
> Geoff*

It seems to be KDM causing the IP entry.
I traced it backwards.

First, run "last" to find the unexpected IP address that
is logged on. Here's a snip of the output from "last -di":

```
user1 :0 220.170.236.183 Thu Mar 17 13:24 still logged in
```

Second, run "who" to get the PID associated with the session
at user1:0. Here's a snip of the output from "who -H -a":

```
NAME LINE TIME IDLE PID COMMENT  
user1 ? :0 Mar 17 13:24 ? 6604 (console)
```

Third, run "ps" to get the process-tree. Here's a
snip of the process-tree from "ps -ejH":

```
   PID PGID SID TTY TIME CMD  
     1  0  0 ? 00:00:03 init  
<snip>  
  6588 6573 4534 ? 00:00:00 kdm  
  6602 6602 4534 ? 00:01:06 X  
  6604 6573 4534 ? 00:00:00 kdm  
  7383 7383 4534 ? 00:00:00 kde  
  7418 7383 4534 ? 00:00:00 gpg-agent  
  7419 7419 7419 ? 00:00:00 ssh-agent
```

So, the 2nd instance of KDM holds the session belonging
to 220.170.236.183.

My conclusions are:

Either KDM is putting bad data into /var/log/wtmp –or–
'last' is interpreting the wtmp data incorrectly –or–
KDM is do something very non-standard.

Regards,
Larry

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