

Re: Reboot in output from "last":

Source: <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2002-10/6415.html>

From:

Date: 10/25/02

Date: Fri, 25 Oct 2002 09:00:39 +0100

>Well that's what chkrootkit tells you. I hope you read the FAQs and stuff –
>it's no guarantee, just a pointer in the direction of either cleanliness or
>crackedness, depending.
>
>If you want to be sure, you're going to have to reboot the machine off a
>trusted rescue CD, mount the disks and check it out by hand.

Yup, i'll be sorting one of these out asap

>> How do i stop this rpc.statd thing starting on startup? I killed it with
>> kill –TERM, but want to find where it starts and struggling (RH 7.3)
>
> bash# grep –rile statd /etc/init.d/
>
>that should help identify it. You don't need portmapper or statd unless you
>know otherwise.

Right ok cheers,

>> If it's supposedly so insecure, why have RH opted to install it
>> automatically?
>
>Because you chose a package selection that requires it.
>
>Fortunately, *I* don't know of an exploit to it since RH7.3; however, that
>doesn't stop it historically being one of *the* most–exploited services
>around (alongside bind and wu–ftpd, 111/tcp (portmapper, with a view to
>finding rpc.statd) is my most–frequently scanned port#). Nor does it stop
>there being another exploit in 10mins' time.
>
>What else have you got listening for all to see? What kind of firewalling
>do you have?

Whoops! Well i've just been in and stopped every service i dont know what it is :) So now all i basically have running are the services i wanted the box for, mainly web development so i wont go into _exactly_ what they are! I'm running iptables firewalling, not entirely sure what rule's i've got going

comp.os.linux.security: Re: Reboot in output from "last":

on, the box is my network router too you see, but i also run personal firewalls on all the internal network'd machines. Mind u since installing the router, zonealarm hasnt come up once with any warnings, and i used to get loads, so clearly they're all hitting the linux box, and hopefully getting turned away !!

>*By the sound of things, you *might* have had a lucky escape. However, >phrases involving "wind" and "sailing waaaaaay too close to" come to mind.*

Thaaaanks for all the help :) I'm verging on upgrading to RH8, then i'll inspect my configuration again exceedingly closely !! Thanks again!

Cheers,
Dan

-
- **Next message:** [2Host.com – Robert: "Re: Reboot in output from "last":"](#)
 - **Previous message:** [Les Mikesell: "Re: Firewall where internal hosts have non-reserved IPs?"](#)
 - **In reply to:** [Tim Haynes: "Re: Reboot in output from "last":"](#)
 - **Next in thread:** [: "Re: Reboot in output from "last":"](#)
 - **Reply:** [: "Re: Reboot in output from "last":"](#)
 - **Messages sorted by:** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)