Subject: Re: error from RkHunter and ChkRootKit
Posted by Daniel Pittman on Tue, 08 May 2007 12:12:37 GMT
View Forum Message <> Reply to Message

Markus Hardiyanto <informatics2k1@yahoo.com> writes:

> I install RkHunter and ChkRootKit inside VE. the VE is using Centos
> 4.4 minimal installation. i download the Centos image from the list on
> OpenVZ Wiki. here is the error that i got:
>
> from RkHunter:
>
> Performing 'known good' check...
> /bin/kill [BAD]
> /sbin/insmod [BAD]
> /sbin/lsmod [BAD]
> /sbin/modprobe [BAD]
> /usr/bin/file [BAD]

[...]

> is this false positives??

Yes and no -- those are modified from the standard packages you would have in a normal system, but the modification is to be expected with OpenVZ. Er, except maybe the /usr/bin/file binary...

> from ChkRootKit:
> Checking `lkm'... You have   74 process hidden for readdir command
> chkproc: Warning: Possible LKM Trojan installed

Again, probably expected: the proc file system within the VE isn't identical to a physical system.

 Daniel
--
Digital Infrastructure Solutions -- making IT simple, stable and secure
Phone: 0401 155 707   email: contact@digital-infrastructure.com.au
                 http://digital-infrastructure.com.au/