Subject: Re: error from RkHunter and ChkRootKit
Posted by Markus Hardiyanto on Wed, 09 May 2007 02:20:22 GMT
View Forum Message <> Reply to Message

i tried to install force util-linux rpm, the installation is succeeded. then i run rkhunter again, but still get the same error on this files:

> /bin/kill [BAD]
> /sbin/insmod [BAD]
> /sbin/lsmod [BAD]
> /sbin/modprobe [BAD]
> /usr/bin/file [BAD]

does a rpm -ivh --force do overwrite the current installation files on the server?

i do this inside VE

Best Regards,
Markus

----- Original Message ----
From: Daniel Pittman <daniel@rimspace.net>
To: users@openvz.org
Sent: Tuesday, May 8, 2007 7:12:37 PM
Subject: Re: [Users] error from RkHunter and ChkRootKit

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/
Send instant messages to your online friends http://uk.messenger.yahoo.com