Subject: error from RkHunter and ChkRootKit

Posted by Markus Hardiyanto on Tue, 08 May 2007 02:40:28 GMT

View Forum Message <> Reply to Message

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 ]
 --------------------------------------------------------- -------------------
Rootkit Hunter has found some bad or unknown hashes. This can happen due to replaced
binaries or updated packages (which give other hashes). Be sure your hashes are
up-to-date (rkhunter --update). If you're in doubt about these hashes, contact
us through the Rootkit Hunter mailinglist at rkhunter-users@lists.sourceforge.net.
 --------------------------------------------------------- -------------------
```

is this false positives??

from ChkRootKit:

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

note that this VPS is a fresh install, how come there is several errors above?

Best Regards,
Markus

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/

Subject: Re: error from RkHunter and ChkRootKit
Posted by Gregor Mosheh on Tue, 08 May 2007 14:40:51 GMT

View Forum Message <> Reply to Message

> Markus Hardiyanto <informatics2k1@yahoo.com> writes:
>> I install RkHunter and ChkRootKit inside VE.
>> Performing 'known good' check...
>> /bin/kill [BAD]
(etc)
> 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

Thanks for the reply on this. Starting over the next few days, I was about
to implement our policy of using chkrootkit and rkhunter on customer VEs.
so this was good to know ahead of time.

What is the nature of the modifications, and to which files? We're running
Slackware (actuallly, HostGIS Linux, which is Slackware-based) using a
hand-made template cache I made per some directions I found in the Wiki.
So if some binaries need to be modified, that'd be good to know too.

>> 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.

Right. Still a scary message to receive. What is the nature of the
discrepancy here? What would show up in the VE's /proc area that wouldn't
also show up in their ps output?

More importantly: Is it even possible for a VE to load a kernel module at
all? Or is a LKM check completely irrelelvant in a VE context?

--
HostGIS
Cartographic development and hosting services
707-822-9355
http://www.HostGIS.com/

"Remember that no one cares if you can back up, only if you can restore."
- AMANDA

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/

Subject: Re: error from RkHunter and ChkRootKit
Posted by Vasily Tarasov on Wed, 09 May 2007 08:56:08 GMT
View Forum Message <> Reply to Message

Hello,

Actually all the binaries (of user-space applications) that exists in VE are the same, that are used on appropriate distribution. So RkHunter should not complain on bad hashes. I see two possible reasons of this problem:

1. RkHunter stores a database of hashes of "important" binaries per-distribution. So, probably it doesn't understand what distribution is installed in VE and uses wrong hashes.

2. Hashes are out of date.

As concerns ChkRootKit and /proc in VE. /proc in VE differs quite a lot from /proc on HN. But AFAIK ChkRootKit checks for the number of processes to be the same in /proc and in `ps` output... So it should not alarm. So I ask you to investigate, _why_ does it alarm. Please, find out what is the initial reason why ChkRootKit considers your VE to have LKM Trojan.

BTW, you can not bother about LKM Trojan in VE: VE isn't allowed to load kernel modules ;)

Vasily

On Tue, 2007-05-08 at 19:20 -0700, Markus Hardiyanto wrote:
> 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