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