

---

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/lsmmod [ 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](mailto: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

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

---