

Re: chkrootkit V. 0.47

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2007-11/msg00017.html>

- *From:* Robert Watson <rwatson@xxxxxxxxxxxx>
 - *Date:* Wed, 28 Nov 2007 11:45:28 +0000 (GMT)
-

On Tue, 20 Nov 2007, JP wrote:

--and--

Checking `lkm'... You have 131 process hidden for readdir command
chkproc: Warning: Possible LKM Trojan installed

I wonder if it's trying to use procfs, which isn't mounted by default in FreeBSD, and as a result reporting that /proc is empty (which is expected). You could try mounting procfs and see if the message goes away, which would answer the question -- however, we don't generally advise mounting procfs unless it is required, as it is a deprecated feature.

Robert N M Watson
Computer Laboratory
University of Cambridge

freebsd-security@xxxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@xxxxxxxxxxxx"