

## Re: Hacked or not ?

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-06/0025.html>

---

*jon.mercer\_at\_achean.com*

**Date:** 06/12/04

Date: Sat, 12 Jun 2004 13:01:38 +0100 (BST)

To: [freebsd-security@freebsd.org](mailto:freebsd-security@freebsd.org)

I have seen this as well, it is most likely a false positive.  
Additionally, slower or more heavily loaded machines seem more likely to generate false positive for LKM.

As a side note, there really ought to be a way for admins to double check the output from chkrootkit Google helps little. Any offers..?

Jon

> *Hi all,*  
>  
> *please advice me – I was on holidays for one week. After return I found*  
> *in security mails from router (chkrootkit) following message:*  
> *Checking `lkm'... You have 1 process hidden for readdir command You*  
> *have 1 process hidden for ps command*  
> *Warning: Possible LKM Trojan installed*  
>  
> *It apeared only onece. From previous and next days reports, the message*  
> *is not present.*  
>  
> *How could I be sure, the machine is not hacked ?*  
>  
> *Many thanks for any response.*  
>  
> *Peter Rosa*  
>  
>  
>  
> \_\_\_\_\_  
> *freebsd-security@freebsd.org mailing list*  
> *<http://lists.freebsd.org/mailman/listinfo/freebsd-security>*  
> *To unsubscribe, send any mail to*  
> *"freebsd-security-unsubscribe@freebsd.org"*  
>

---

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

FreeBSD-Security: Re: Hacked or not ?

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