

Re: chkrootkit-0.34 report

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-linux/2001-10/0245.html>

From: dewt (dewt@kc.rr.com)

Date: 10/30/01

From: dewt <dewt@kc.rr.com>
To: Herbert Kwong <cancerroach@yahoo.com>, focus-linux@securityfocus.com
Subject: Re: chkrootkit-0.34 report
Date: Tue, 30 Oct 2001 16:21:48 -0600
Message-ID: <0b4934723221ealFE7@mail7.kc.rr.com>

On Monday 29 October 2001 09:46 pm, Herbert Kwong wrote:

> *Hi,*
>
> *I just used chkrootkit 0.34 to check my system. It*
> *reports the following message:*
> *Checking 'lkm'... You have 2 process hidden for ps*
> *command*
> *Warning: Possible LKM Trojan installed*
>
> *What can I do to see what are those 2 processes?*
> *Thanks.*
>
> *Regards,*
> *Herbert*

they should have entires in /proc/nnn , nnn being the process id number of the process, a klunky little script kind of like this should help you find the pids, however it will catch the ps,awk, sort, and grep, so those process will be in the list but not in the /proc, any ones still there would be suspect

```
#!/bin/bash
cd /proc
ps aux | awk '{print $2}' | sort | grep -v PID > /tmp/ps1
ls -1d [0-9]* > /tmp/ps2
diff /tmp/ps1 /tmp/ps2
rm -f /tmp/ps1
rm -f /tmp/ps2
```

- *Previous message:* [Seth Arnold: "Re: chkrootkit-0.34 report"](#)
- *In reply to:* [Herbert Kwong: "chkrootkit-0.34 report"](#)
- *Next in thread:* [Aj Effin Reznor: "Re: chkrootkit-0.34 report"](#)
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)