

Chkrootkit - Check for signs of a rootkit

```
apt-get install chkrootkit
//configure yes for run daily

//options are in /etc/chkrootkit.conf
RUN_DAILY="true"
RUN_DAILY_OPTS="-q"
DIFF_MODE="false" //note - this line may/maynot be in Debian Sarge.

//check in /etc/cron.daily/chkrootkit for the cron daily entry.
```

Links:

<http://softice.lakeland.usf.edu/wiki/index.php/ELSA:lab-08>

<http://www.chkrootkit.org/README>

<http://www.chkrootkit.org/#tests>

Further rootkit reasoning and detection is discussed here:

<http://linuxhelp.blogspot.com/2006/12/various-ways-of-detecting-rootkits-in.html>