CHECKING FOR ROOT KITS

“A root kit is one variety of hacker tool kit. It can perform a number of functions depending on the flavor of the root kit. The original core of most root kit applications was some kind of network-sniffing tool designed to allow the attacker to find additional usernames and passwords. More recently, these functions have expanded to include capturing passwords using Trojan programs, providing back doors into your system, and masking that your system has been penetrated by purging or filtering logs. Root kits can also contain functionality designed to hide the attacker’s logins and any processes they are running.” – Hardening Linux, p. 282

Although there is no way to detect every root kit all the time, you can run programs that identify common ones. I will go over installing two such programs for Linux.

Rootkit Hunter

```
# Check for the latest version at http://sourceforge.net/projects/rkhunter/

cd /root

wget http://downloads.sourceforge.net/project/rkhunter/rkhunter/1.3.6/rkhunter-1.3.6.tar.gz?use_mirror=superb-sea2

tar -xvzf rkhunter-1.3.6.tar.gz

cd rkhunter-1.3.6.tar.gz

./installer.sh

/usr/local/bin/rkhunter --checkall --createlogfile
```

Now you should automate it. Add this as a cron (crontab -e on most systems)

```
0 0 * * * /usr/local/bin/rkhunter --cronjob --append-log --report-warnings-only |/bin/mail -s "[Rootkit Hunter] report" your-email@domain.com
```

Now it will run every night and email you any warnings detected. I recommend reading the help file for more options (/usr/local/bin/rkhunter –help)

chkrootkit

```
# Check for the latest version at http://www.chkrootkit.org/download/

wget ftp://ftp.pangeia.com.br/pub/seg/pac/chkrootkit.tar.gz


# Compare with ftp://ftp.pangeia.com.br/pub/seg/pac/chkrootkit.md5

md5sum chkrootkit.tar.gz


tar -xvzf chkrootkit.tar.gz

cd chkrootkit

make sense

rm -f *.c Makefile

mkdir /usr/local/chkrootkit

mv * /usr/local/chkrootkit

/usr/local/chkrootkit

ln -s /usr/local/chkrootkit/chkrootkit /usr/local/bin/chkrootkit

/usr/local/bin/chkrootkit
```

And you could automate this as a cron job as well

```
0 0 * * * /usr/local/bin/chkrootkit |/bin/mail -s "[chkrootkit] report" your-email@domain.com
```

PLEASE keep in mind that these programs can return false positives. I advise you Google any positives to see if they could be mistakes. I get one for “Checking `bindshell’… INFECTED (PORTS: 465)” which is really just my Postfix server running SSL.

Source : http://brandonwamboldt.ca/checking-for-root-kits-239/