

Rootkits

Table des matières

1	chkrootkit	1
2	rkhunter	1
3	logwatch	1

1 chkrootkit

- Installation :

```
# apt-get install chkrootkit
# chkrootkit
```

- Crontab :

```
– /etc/cron.daily/chkrootkit
```

2 rkhunter

- Installation :

```
# apt-get install rkhunter
# rkhunter --update
# rkhunter --checkall
```

- Crontab :

```
– /etc/cron.daily/rkhunter
– /etc/cron.weekly/rkhunter
```

3 logwatch

- Installation :

```
# apt-get install logwatch
# mkdir /var/cache/logwatch
# cp /usr/share/default.conf/logwatch.conf /etc/logwatch/conf
# logwatch
```

- Configuration :

```
– /etc/logwatch/conf/logwatch.conf
    Output = stdout
    Format = text
– /etc/cron.daily/00logwatch
    /usr/sbin/logwatch --output mail --format html
```