

RKHUNTER

Installation de RKHUNTER (cherche root kit):

```
apt install rkhunter
```

Modifier le fichier de configuration pour recevoir les courriels

```
sudo nano /etc/rkhunter.conf
```

```
MAIL-ON-WARNING=postmaster@infolaf.net
MAIL_CMD=mail -s "[rkhunter] Avertissements trouvés pour ${HOST_NAME}"
UPDATE_MIRRORS=1
MIRRORS_MODE=0
ALLOW_SSH_ROOT_USER=prohibit-password
WEB_CMD=""
```

Éditer */etc/default/rkhunter*

```
nano /etc/default/rkhunter
```

```
# Defaults for rkhunter automatic tasks
# sourced by /etc/cron.*/rkhunter and /etc/apt/apt.conf.d/90rkhunter
#
# This is a POSIX shell fragment
#
# Set this to yes to enable rkhunter daily runs
# (default: true)
CRON_DAILY_RUN="true"

# Set this to yes to enable rkhunter weekly database updates
# (default: true)
CRON_DB_UPDATE="true"

# Set this to yes to enable reports of weekly database updates
# (default: false)
DB_UPDATE_EMAIL="true"
```

```
# Set this to the email address where reports and run output should be sent
# (default: root)
REPORT_EMAIL="root"

# Set this to yes to enable automatic database updates
# (default: false)
APT_AUTOGEN="true"

# Nicenesses range from -20 (most favorable scheduling) to 19 (least favorable)
# (default: 0)
NICE="0"

# Should daily check be run when running on battery
# powermgmt-base is required to detect if running on battery or on AC power
# (default: false)
RUN_CHECK_ON_BATTERY="false"
```