Install RKHunter which is the Rootkit Detection tool.

Install RKHunter

```
apt install rkhunter curl -y
```

Configure and Use RKHunter

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

# if set [yes], daily cron job will be run
CRON_DAILY_RUN=""

# set email address to receive report
REPORT_EMAIL="root"

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

# line 107 : change
UPDATE_MIRRORS=1

# line 122 : change
MIRRORS_MODE=0

# line 1190 : change to blank
WEB_CMD=""

update database

```
sudo rkhunter --update
```

```
[ Rootkit Hunter version 1.4.6 ]

Checking rkhunter data files...
  Checking file mirrors.dat                    [ Updated ]
  Checking file programs_bad.dat               [ No update ]
  Checking file backdoorports.dat              [ No update ]
  Checking file suspscan.dat                   [ No update ]
  Checking file i18n/cn                        [ Skipped ]
```

```
Checking file i18n/de                         [ Skipped ]
Checking file i18n/en                         [ No update ]
Checking file i18n/tr                        [ Skipped ]
Checking file i18n/tr.utf8                    [ Skipped ]
Checking file i18n/zh                        [ Skipped ]
Checking file i18n/zh.utf8                     [ Skipped ]
Checking file i18n/ja                       [ Skipped ]
```

#update system file properties

```
sudo rkhunter --propupd
```

run checking
[--sk] means skipping to push Enter key
[--rwo] means display only warnings

Install RKHunter

```
apt install rkhunter curl -y
```

Configure and Use RKHunter

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

# if set [yes], daily cron job will be run
CRON_DAILY_RUN=""

# set email address to receive report
REPORT_EMAIL="root"

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

# line 107 : change
UPDATE_MIRRORS=1

# line 122 : change
MIRRORS_MODE=0

# line 1190 : change to blank
WEB_CMD=""

update database

```
sudo rkhunter --update
```

```
[ Rootkit Hunter version 1.4.6 ]

Checking rkhunter data files...
  Checking file mirrors.dat                          [ Updated ]
  Checking file programs_bad.dat                       [ No update ]
  Checking file backdoorports.dat                      [ No update ]
  Checking file suspscan.dat                         [ No update ]
  Checking file i18n/cn                              [ Skipped ]
  Checking file i18n/de                              [ Skipped ]
  Checking file i18n/en                              [ No update ]
  Checking file i18n/tr                              [ Skipped ]
  Checking file i18n/tr.utf8                         [ Skipped ]
  Checking file i18n/zh                              [ Skipped ]
  Checking file i18n/zh.utf8                         [ Skipped ]
  Checking file i18n/ja                              [ Skipped ]
```

#update system file properties

```
sudo rkhunter --propupd
```

run checking
[--sk] means skipping to push Enter key
[--rwo] means display only warnings

```
sudo rkhunter --check --sk
```

Revisie #1
Gemaakt: 24 januari 2025 17:51:10 door Gert
Bijgewerkt: 24 januari 2025 17:52:38 door Gert