How to Install RKHunter (RootKit Hunter) On Ubuntu 18.04

By **koromicha** - October 28, 2018

RootKit Hunter is a Unix-based shell script that can scan the local system for rootkits, backdoors and possible local exploits. It does this by comparing the SHA-1 hashes of the local files with the known good hashes in an online database.

It can also monitor the local system commands, startup files, network interfaces for any alteration as well as listening applications.

Installing RKHunter

The rkhunter packages is available in standard Ubuntu repositories hence we can install it by running the command below;

```
# apt install rkhunter -y
```

Configure and Use RKHunter

Once the installation is done, you need to configure RKHunter before you can use it to scan your system. Therefore open the configuration file, **`/etc/rkhunter.conf`**, and make the changes as shown below.

```
# vim /etc/rkhunter.conf
```

Set the value of `UPDATE_MIRRORS` to 1. This ensures that the mirror files are also checked for updates when checking for rkhunter updated date files with the **`--update`** option.

```
UPDATE_MIRRORS=1
```

Set the value of `MIRRORS_MODE` to 0. The MIRRORS_MODE option tells rkhunter which mirrors are to be used when the –update or **`--versioncheck`** command-line options are given. There are three possible values for this;

- 0 – use any mirror
- 1 – only use local mirrors
- 2 – only use remote mirrors

```
MIRRORS_MODE=0
```

Set the value of `WEB_CMD` to null, **“”**. This option can be set to a command which rkhunter will use when downloading files from the Internet – that is, when the –versioncheck or –update option is used. In this case we are not specifying any command.

```
WEB_CMD=""
```

Enable regular scan and updates with cron

RKHunter script is installed under under cron.daily directory for regular scan and updates. the script is therefore executed everyday by Cron.

Edit the `/etc/default/rkhunter.conf` and make the following changes.

Enable rkhunter scan checks to run daily by setting the value of `CRON_DAILY_RUN` to **“true”.**

```
CRON_DAILY_RUN="true"
```

Set the value of `CRON_DB_UPDATE` to **true** to enable rkhunter weekly database updates.

```
CRON_DB_UPDATE="true"
```

Set the value of to `APT_AUTOGEN` to **true** to enable automatic database updates. This ensures that `rkhunter --propupd` is run automatically after software updates in order to reduce false positives.

```
APT_AUTOGEN="true"
```

Once you are done, save the configuration file and quit.

Run the command below to check for any unrecognised configuration options. If any configuration problems are found, then they will be displayed and the return code will be set to 1.

```
# rkhunter -C
```

You can also use `--config-check` option instead of **-C**.

Update rkhunter text data files

After configuring rkhunter, run the command below to update rkhunter text data files. Note that these are the files that rkhunter uses to determine suspicious activities on the system and thus they should be kept upto-date.

```
# rkhunter --update
[ Rootkit Hunter version 1.4.6 ]

Checking rkhunter data files...
  Checking file mirrors.dat                                  [ No update ]
  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 ]
```

The `i18n/*` files are just for localization purposes, so they are not essential for core program functionality. So the output above, **`i18n/en`**, shows that English strings are already on the system.

Note that it may not be a good idea to run rkhunter with **`--update`** as it posses a security risk. Therefore let your package manager take care of keeping it updated.

You can also the version of the rkhunter by running the command below;

```
# rkhunter --versioncheck
[ Rootkit Hunter version 1.4.6 ]

Checking rkhunter version...
  This version  : 1.4.6
  Latest version: 1.4.6
```

Set the Security Baseline for your system

RKHhunter compares various current file properties of various commands within the system against those it has previously stored. To update rkhunter data file of stored values with the current values, run the rkhunter with `--propupd` option.

```
# rkhunter --propupd
[ Rootkit Hunter version 1.4.6 ]
File updated: searched for 180 files, found 147
```

Perform System Check

Now that we are done with configuring rkhunter, run the command below to perform test scan against your system.

```
# rkhunter --check
```

This is the sample output of the command above.

```
...output snipped...
Checking the network...

  Performing checks on the network ports
    Checking for backdoor ports                             [ None found ]

  Performing checks on the network interfaces
    Checking for promiscuous interfaces                     [ None found ]

Checking the local host...

  Performing system boot checks
    Checking for local host name                            [ Found ]
    Checking for system startup files                       [ Found ]
    Checking system startup files for malware               [ None found ]

  Performing group and account checks
    Checking for passwd file                                [ Found ]
    Checking for root equivalent (UID 0) accounts           [ None found ]
```

```
    Checking for passwordless accounts                        [ None found ]
    Checking for passwd file changes                          [ None found ]
    Checking for group file changes                           [ None found ]
    Checking root account shell history files                 [ OK ]

  Performing system configuration file checks
    Checking for an SSH configuration file                    [ Found ]
    Checking if SSH root access is allowed                    [ Warning ]
    Checking if SSH protocol v1 is allowed                    [ Not set ]
    Checking for other suspicious configuration settings      [ None found ]
    Checking for a running system logging daemon              [ Found ]
    Checking for a system logging configuration file          [ Found ]
    Checking if syslog remote logging is allowed              [ Not allowed ]

  Performing filesystem checks
    Checking /dev for suspicious file types                   [ None found ]
    Checking for hidden files and directories                 [ Warning ]

[Press <ENTER> to continue]

System checks summary
=====================

File properties checks...
    Files checked: 147
    Suspect files: 0

Rootkit checks...
    Rootkits checked : 503
    Possible rootkits: 0

Applications checks...
    All checks skipped

The system checks took: 1 minute and 43 seconds

All results have been written to the log file: /var/log/rkhunter.log
```

```
One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)
```

As you can see above, there are some warnings for example **SSH root access is allowed**. You can the remediate whatever the issue found on your system by rkhunter.

To avoid having to press ENTER for every check, you can pass the `--sk or --skip-keypress` option.

```
# rkhunter --check --sk
```

To display warning messages only, use the `--rwo or --report-warnings-only` option.

```
# rkhunter --check --rwo
```

RKHunter log file is:

```
/var/log/rkhunter.log
```

You also noticed that hidden files and directories warnings are given. To avoid these warnings, you can reconfigure rkhunter to ignore these files via whitelisting. For example in my test, i found this warning;

```
Warning: Hidden directory found: /etc/.java
```

To whitliest this file, open the rkhunter config file and uncomment the line `#ALLOWHIDDENDIR=/etc/.java` such that it looks like;

```
ALLOWHIDDENDIR=/etc/.java
```

If you got other files, you can uncomment them in the rkhunter configuration file as shown above.

Email Notifications

You may also want to send the results via Email in case a threat is found on your system. To do this, you need to edit rkhunter configuration file and set a value of `MAIL-ON-WARNING` to your email address.

```
# vim /etc/rkhunter.conf
```

```
MAIL-ON-WARNING=username@domain
```

Replace **username@domain** with your email address

You also set the email command to use.

```
MAIL_CMD=mail -s "[rkhunter] Warnings found for ${HOST_NAME}"
```

Once done, save the configuration file and check for any misconfigurations as shown above.

You can now be able to receive emails in case any threat is found on your system. See the example mail below.

rkhunacter-email-notification

That is all we could cover about RKHunter. We hope this article helped. Happy threat hunting.