Table of Contents

Rootkit Hunter

- As the name implies, its a tool to detect rootkits.
- I will describe installation and configuration for arch and ubuntu

Links

http://www.rootkit.nl/projects/rootkit_hunter.html

Arch

- I used rkhunter 1.3.8-1

Installation

- You need two packages: unhide and rkhunter itself both available in the AUR.
- download pkgbuild (I use slurpy you also can download the pkgbuild manual) an install it.

```
slurpy -d rkhunter
 cd rkhunter
 makepkg
 pacman -U rkhunter-1.3.8-1-any.pkg.tar.xz
 cd ..
slurpy -d unhide
 cd unhide
 makepkg
 pacman -U unhide-20100819-1-x86_64.pkg.tar.xz
```

Configuration

- There are a lot of comments which describe the use of these many options.
- My Config “/etc/rkhunter.conf”:

```
ROTATE_MIRRORS=1
UPDATE_MIRRORS=1
MIRRORS_MODE=0
MAIL-ON-WARNING=""
MAIL_CMD=mail -s "[rkhunter] Warnings found for ${HOST_NAME}"
TMPDIR=/var/lib/rkhunter/tmp
DBDIR=/var/lib/rkhunter/db
SCRIPTDIR=/usr/local/lib/rkhunter/scripts
BINDIR="/bin /usr/bin /sbin /usr/sbin /usr/local/bin /usr/local/sbin"
```

```
UPDATE_LANG=""
LOGFILE=/var/log/rkhunter.log
APPEND_LOG=0
COPY_LOG_ON_ERROR=0
COLOR_SET2=0
AUTO_X_DETECT=1
WHITELISTED_IS_WHITE=0
ALLOW_SSH_ROOT_USER=unset
ALLOW_SSH_PROT_V1=0
ENABLE_TESTS="all"
DISABLE_TESTS="suspscan hidden_ports hidden_procs deleted_files
packet_cap_apps"
SCRIPTWHITELIST="/bin/egrep /bin/fgrep /bin/which /usr/bin/groups
/usr/bin/ldd /usr/bin/lwp-request /usr/sbin/adduser /usr/sbin/prelink"
IMMUTABLE_SET=0
ALLOWHIDDENDIR="/dev/.udev /dev/.udevdb /dev/.udev.tdb /etc/.java"
PHALANX2_DIRTEST=0
SYSLOG_CONFIG_FILE=/etc/syslog-ng.conf
ALLOW_SYSLOG_REMOTE_LOGGING=0
SUSPSCAN_TEMP=/dev/shm
SUSPSCAN_MAXSIZE=10240000
SUSPSCAN_THRESH=200
RTKT_FILE_WHITELIST="/usr/sbin/kfd"
USE_LOCKING=0
LOCK_TIMEOUT=300
SHOW_LOCK_MSGS=1
INSTALLDIR=/usr
DBDIR=/var/lib/rkhunter/db
SCRIPTDIR=/usr/lib/rkhunter/scripts
TMPDIR=/var/lib/rkhunter/tmp
USER_FILEPROP_FILES_DIRS="/etc/rkhunter.conf /usr/sbin/kfd"
```

- Heimdal is detected as “adore” rootkit therefore this line.
- First line whitelist the file and the second checks for changes.

```
RTKT_FILE_WHITELIST="/usr/sbin/kfd"
USER_FILEPROP_FILES_DIRS="/etc/rkhunter.conf /usr/sbin/kfd"
```

Using

- First you have to create checksums so rkhunter checks for changes in files. This you have to do after every change to the files which are checked.

```
rkhunter --propupd
```

- Then you could run first check this will take some time.

```
sudo /usr/bin/rkhunter -c
```

- To do this daily a cron is needed

- Here a script adapted from ubuntu auto created cron

```
#!/bin/sh
# übernahme von Ubuntu
RKHUNTER=/usr/bin/rkhunter
REPORT_EMAIL=root
if [ -z "$NICE" ]; then
    NICE=0
fi

OUTFILE=`mktemp` || exit 1
/usr/bin/nice -n $NICE $RKHUNTER --cronjob --report-warnings-only \
           --createlogfile /var/log/rkhunter.log $RK_OPT > $OUTFILE
if [ -s "$OUTFILE" ]; then
  (
    echo "Subject: [rkhunter] $(hostname -f) - Daily report"
    echo "To: $REPORT_EMAIL"
    echo ""
    cat $OUTFILE
  ) | /usr/sbin/sendmail $REPORT_EMAIL
fi
rm -f $OUTFILE
```

- This sends the Warnings to local root User and should be placed in “/etc/cron.daily/”.

Ubuntu

- I used rkhunter 1.3.6-3ubuntu1

Installation

```
apt-get install rkhunter unhide
```

Configuration

- My Config “/etc/rkhunter.conf”:

```
ROTATE_MIRRORS=1
UPDATE_MIRRORS=1
MIRRORS_MODE=0
MAIL-ON-WARNING=""
MAIL_CMD=mail -s "[rkhunter] Warnings found for ${HOST_NAME}"
TMPDIR=/var/lib/rkhunter/tmp
DBDIR=/var/lib/rkhunter/db
SCRIPTDIR=/usr/share/rkhunter/scripts
BINDIR="/bin /usr/bin /sbin /usr/sbin /usr/local/bin /usr/local/sbin
/usr/libexec /usr/local/libexec"
```

```
LOGFILE=/var/log/rkhunter.log
APPEND_LOG=0
COLOR_SET2=0
AUTO_X_DETECT=1
ALLOW_SSH_ROOT_USER=no
ALLOW_SSH_PROT_V1=0
ENABLE_TESTS="all"
DISABLE_TESTS="suspscan hidden_procs deleted_files packet_cap_apps apps"
SCRIPTWHITELIST=/bin/which
SCRIPTWHITELIST=/usr/bin/ldd
SCRIPTWHITELIST=/usr/bin/lwp-request
SCRIPTWHITELIST=/usr/sbin/adduser
ALLOWHIDDENDIR=/dev/.udev
ALLOWHIDDENDIR=/dev/.static
ALLOWHIDDENDIR=/dev/.initramfs
ALLOWDEVFILE=/dev/shm/pulse-shm-*
ALLOW_SYSLOG_REMOTE_LOGGING=0
SUSPSCAN_DIRS="/tmp /var/tmp"
SUSPSCAN_TEMP=/dev/shm
SUSPSCAN_MAXSIZE=10240000
SUSPSCAN_THRESH=200
INSTALLDIR="/usr"
USER_FILEPROP_FILES_DIRS="/etc/rkhunter.conf"
USER_FILEPROP_FILES_DIRS="/etc/ssh/sshd_config"
```

- For using with (e.g. a Xen based) host without Modules you have to add “os_specific” to the DISABLE_TESTS Variable.

Using

- First you have to create checksums so rkhunter checks for changes in files. This you have to do after every change to the files which are checked.

```
rkhunter --propupd
```

- Then you could run first check this will take some time.

```
sudo /usr/bin/rkhunter -c --pkgmgr dpkg
```

- The cron is autocreated in ubuntu and send info to the user root.
- It is placed in “cron.daily”.

Last

- To list all available tests

```
rkhunter --list tests
```