Installer et configurer Rootkit-Hunter

- **Ressources** :
  - Rkhunter - Wiki Ubuntu
  - Rkhunter : paramètre WEB_CMD invalide
- **Notes** :
  - Fichiers de config : `/etc/rkhunter.conf` et `/etc/default/rkhunter`
  - Fichier de log : `/var/log/rkhunter.log`

Installation de RKHunter

- Installer le paquet : `apt install rkhunter`
- Indiquer les options du Cron de Rkhunter, en éditant : `vi /etc/default/rkhunter`

/etc/default/rkhunter

```
CRON_DAILY_RUN="yes"
CRON_DB_UPDATE="yes"
DB_UPDATE_EMAIL="yes"
REPORT_EMAIL="adminsys@<domaine-sinp>"
REPORT_EMAIL_FROM="mailer@<domaine-sinp>"
APT_AUTOGEN="yes"
```

- Indiquer les faux positifs, en éditant le fichier de config : `vi /etc/rkhunter.conf`

/etc/rkhunter.conf

```
ALLOW_SSH_ROOT_USER=prohibit-password

# Config permettant la mise à jour pour éviter l'erreur :
# Invalid WEB_CMD configuration option: Relative pathname:
"/bin/false"
UPDATE_MIRRORS=1
MIRRORS_MODE=0
WEB_CMD=""

# (Ne pas renseigner MAIL-ON-WARNING ni MAIL_CMD ici pour éviter
le flood d'emails sur chaque warning.
# L'envoi d'alerte mail est géré uniquement par le script cron
patché.)

# Option évitant les faux positifs en se basant sur Dpkg
# ATTENTION : lancer ''rkhunter --propupd'' après avoir modifié
cette option !
PKGMGR=DPKG

# Pour Debian 10 uniquement, corriger l'emplacement des scripts
```

```
suivants (/usr/bin/ au lieu de /bin) :
SCRIPTWHITELIST=/usr/bin/egrep
SCRIPTWHITELIST=/usr/bin/fgrep
SCRIPTWHITELIST=/usr/bin/which

# Désactiver les faux positifs sur db-srv
ALLOWDEVFILE="/dev/shm/PostgreSQL.*"

# Exemples de faux positifs à désactiver :
ALLOWHIDDENDIR="/dev/.udev"
ALLOWHIDDENDIR="/dev/.static"
ALLOWDEVFILE="/dev/.udev/rules.d/root.rules"

# Désactiver les faux positifs liés à Byobu :
ALLOWDEVFILE="/dev/shm/byobu-*"
ALLOWDEVFILE="/dev/shm/byobu-*/*"
ALLOWDEVFILE="/dev/shm/byobu-*/*/*"
ALLOWDEVFILE="/dev/shm/byobu-*/.last.tmux"
ALLOWDEVFILE="/dev/shm/byobu-*/.last.tmux/*"
```

- **ATTENTION** : suite à l'installation et configuration de Rkhunter, il est nécessaire de lancer la commande suivante (⇒ indique à Rkhunter que tout est OK) : `rkhunter --propupd`

Envoi d'email

Pour recevoir les alertes de RKHunter sur la bonne adresse sans flood inutile :

- Définir l'adresse de réception dans /etc/default/rkhunter :

```
REPORT_EMAIL="adminsys@<domaine-sinp>"
REPORT_EMAIL_FROM="mailer@<domaine-sinp>"
```

- **Ne pas renseigner** (ou commenter) les options MAIL-ON-WARNING et MAIL_CMD dans /etc/rkhunter.conf.
- Vérifier que le script cron (/etc/cron.daily/rkhunter) est patché selon la section ci-dessous (voir Patch).

Utilisation et commandes

- Vérifier dernière version : `rkhunter --versioncheck`
- Mettre à jour le programme : `rkhunter --update`
- Lister les différents tests effectués : `rkhunter --list`
- **ATTENTION** : suite à l'installation et configuration de Rkhunter, il est nécessaire de lancer la commande suivante (⇒ indique à Rkhunter que tout est OK) : `rkhunter --propupd`
- Effectuer une vérification : `rkhunter --checkall`
- Vérification avec juste les alertes importantes : `rkhunter -c --rwo`

- Tester uniquement les *malwares* : `rkhunter -c -sk --enable malware`
- Accéder aux logs de RkHunter : `vi /var/log/rkhunter.log`

Avertissements Rkhunter

Suite à mise à jour des paquets

- Lorsqu'on réalise une mise à jour des paquets systèmes, il se peut que Rkhunter signale qu'un logiciel à sa signature modifiée. Ex. :

```
Warning: The file properties have changed:
         File: /usr/bin/curl
         Current inode: 14563    Stored inode: 8252
         Current file modification time: 1582383706 (22-févr.-2020
16:01:46)
         Stored file modification time : 1560536612 (14-juin-2019
20:23:32)
```

- Dans ce cas là, relever la date de la nouvelle version du binaire et se rendre sur le site suivant : https://www.debian.org/distrib/packages
  - Chercher le paquet Debian correspondant et vérifier la date de la dernière version publiée du paquet en question
    - Utiliser le moteur de recherche situé en bas de page permettant de rechercher un nom de fichier présent dans un paquet.
  - Sur la page du paquet :
    - sélectionner votre version de Debian.
    - Pour vérifier la date, cliquer dans le menu de droite sur le lien "**Journal des modifications Debian**". Le changelog du paquet s'affiche et contient la date de la dernière modification.
- Si les 2 dates correspondent, le message d'avertissement de Rkhunter est à ignorer.
- Il faut tout de même :
  - Se connecter sur le serveur
  - Lancer la commande de vérification (par acquis de conscience) : `rkhunter --checkall`
  - Si tout semble conforme, indiquer à Rkhunter de considérer les changements comme normaux : `rkhunter --propupd`
- **NOTE** : pour que Rhunter lance automatiquement `rkhunter --propupd` après une mise à jour des paquets, mettre `APT_AUTOGEN="yes"` dans le fichier `/etc/default/rkhunter`.

Patch : Limiter les mails de RKHunter aux vraies alertes (rootkit ou fichier suspect)

Par défaut, RKHunter envoie un mail à chaque “Warning”, même mineur (ex : fichiers temporaires de byobu, dossiers cachés, etc.). Pour ne recevoir un mail **que** si un rootkit ou un fichier suspect est détecté, il faut patcher le script cron `/etc/cron.daily/rkhunter` (ou `/etc/cron.weekly/rkhunter`).

/etc/cron.daily/rkhunter

```
# Ancienne section à commenter :
```

```
# if [ -s "$OUTFILE" -a -n "$REPORT_EMAIL" ]; then
#   (
#     echo "Subject: [rkhunter] $(hostname) - Daily report"
#     echo "To: $REPORT_EMAIL"
#     echo ""
#     cat $OUTFILE
#   ) | /usr/sbin/sendmail -t -f $REPORT_EMAIL_FROM
# fi

# Nouvelle section à ajouter :
if [ -s "$OUTFILE" ] && [ -n "$REPORT_EMAIL" ]; then
    if grep -q -E "Possible rootkits:[[:space:]]+[^0]" "$OUTFILE" || \
       grep -q -E "Suspect files:[[:space:]]+[^0]" "$OUTFILE"; then
        (
          echo "Subject: [rkhunter] ALERTE sur $(hostname)"
          echo "To: $REPORT_EMAIL"
          echo ""
          cat $OUTFILE
        ) | /usr/sbin/sendmail -t -f $REPORT_EMAIL_FROM
    fi
fi
```

Cette modification permet de ne recevoir un mail **qu'en cas d'incident réel** (fichiers suspects ou rootkits détectés), et d'ignorer tous les faux positifs récurrents (warnings bénins).

Pensez à faire une sauvegarde du script avant modification :

```
cp /etc/cron.daily/rkhunter /etc/cron.daily/rkhunter.bak
```

Avertissement "Spam tool component"

- Apparemment un faux positif lié aux services tournant dans des containers Docker : https://sourceforge.net/p/rkhunter/bugs/172/
  - Le problème se pose avec Gunicorn et PhpFPM.
- Pas de solution pour l'instant pour le mettre dans une whitelist, il est seulement possible de désactiver les tests correspondant :
  - Éditer le fichier de conf de Rkhunter : `vi /etc/rkhunter.conf`
  - Ajouter `running_procs` à la fin de la liste du paramètre `DISABLE_TESTS`.
- Si le problème persiste, une alternative intéressante à RKhunter est Lynis (à tester).