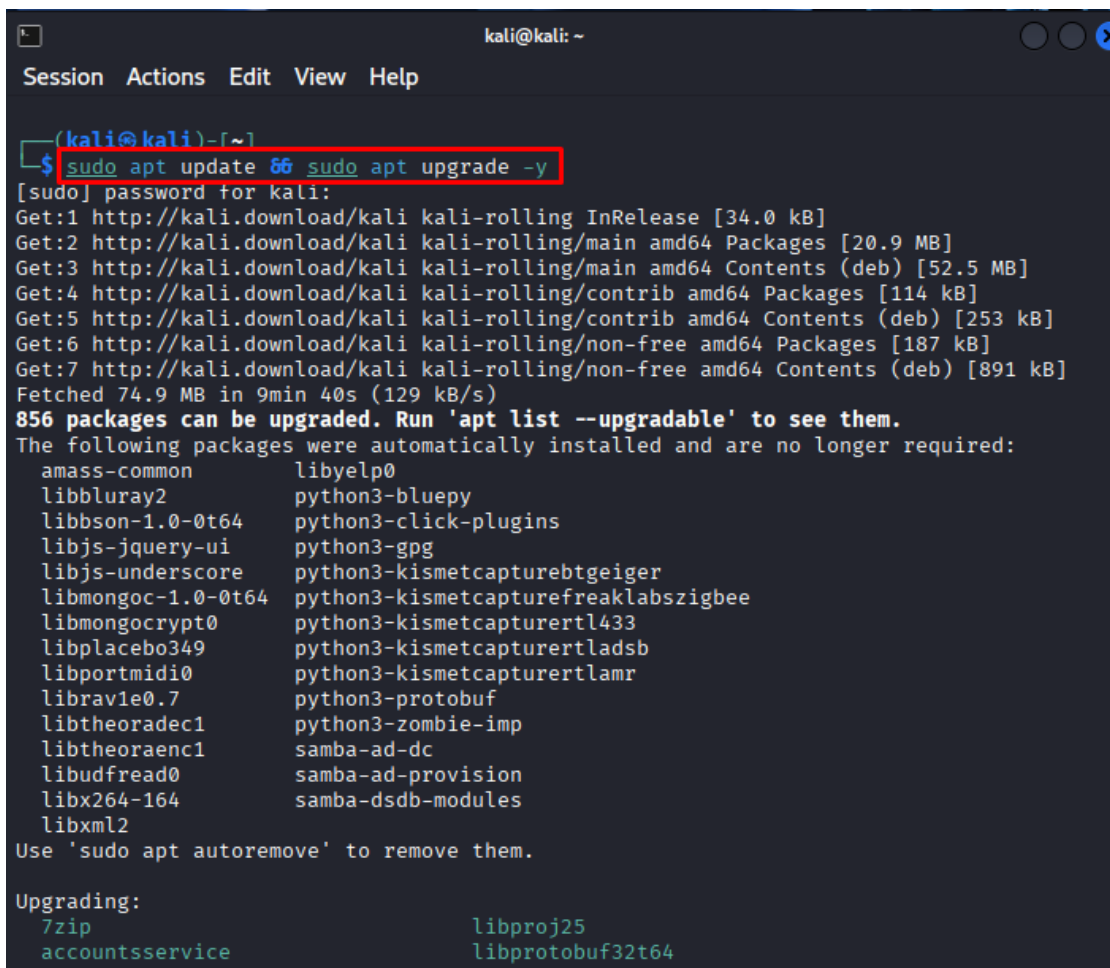


Práctica: Detección de Rootkits con Rootkit Hunter (rkhunter)

Parte 1: Instalación de Rootkit Hunter (rkhunter)

1. Actualizar el Sistema

`sudo apt update && sudo apt upgrade -y`



```
kali@kali: ~  
Session Actions Edit View Help  
  
(kali@kali)~  
$ sudo apt update && sudo apt upgrade -y  
[sudo] password for kali:  
Get:1 http://kali.download/kali kali-rolling InRelease [34.0 kB]  
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.9 MB]  
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [52.5 MB]  
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [114 kB]  
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [253 kB]  
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [187 kB]  
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [891 kB]  
Fetched 74.9 MB in 9min 40s (129 kB/s)  
856 packages can be upgraded. Run 'apt list --upgradable' to see them.  
The following packages were automatically installed and are no longer required:  
  amass-common          libyelp0  
  libbluray2            python3-bluepy  
  libbson-1.0-0t64      python3-click-plugins  
  libjs-jquery-ui        python3-gpg  
  libjs-underscore       python3-kismetcapturebtgeiger  
  libmongoc-1.0-0t64     python3-kismetcapturefreaklabszigbee  
  libmongocrypt0         python3-kismetcaptureertl433  
  libplacebo349          python3-kismetcaptureertladsb  
  libportmidi0           python3-kismetcaptureertlamr  
  librav1e0.7            python3-protobuf  
  libtheoradec1          python3-zombie-imp  
  libtheoraenc1          samba-ad-dc  
  libudfread0            samba-ad-provision  
  libx264-164            samba-dsdb-modules  
  libxml2  
Use 'sudo apt autoremove' to remove them.  
  
Upgrading:  
  7zip                                libproj25  
  accountsservice                    libprotobuf32t64
```

2. Instalar Rootkit Hunter

`sudo apt install rkhunter -y`

```
kali@kali: ~  
Session Actions Edit View Help  
  
(kali@kali)-[~]  
$ sudo apt install rkhunter -y  
[sudo] password for kali:  
The following packages were automatically installed and are no longer required:  
  amass-common libyelp0  
  libbluray2 python3-bluepy  
  libbson-1.0-0t64 python3-click-plugins  
  libjs-jquery-ui python3-gpg  
  libjs-underscore python3-kismetcapturebtgeiger  
  libmongoc-1.0-0t64 python3-kismetcapturefreaklabszigbee  
  libmongocrypt0 python3-kismetcapturertl433  
  libplacebo349 python3-kismetcapturertladsb  
  libportmidi0 python3-kismetcapturertlamr  
  librav1e0.7 python3-protobuf  
  libtheoradec1 python3-zombie-imp  
  libtheoraenc1 samba-ad-dc  
  libudfread0 samba-ad-provision  
  libx264-164 samba-dsdb-modules  
  libxml2  
Use 'sudo apt autoremove' to remove them.  
  
Installing:  
  rkhunter  
  
Installing dependencies:  
  bsd-mailx exim4-config liblockfile1 unhide.rb  
  exim4-base exim4-daemon-light unhide  
  
Suggested packages:  
  exim4-doc-html | exim4-doc-info eximon4 spf-tools-perl  
  
Summary:  
  Upgrading: 0, Installing: 8, Removing: 0, Not Upgrading: 3
```

3. Verificar la Instalación

rkhunter --versioncheck

```
(kali@kali)-[~]  
$ sudo rkhunter --versioncheck  
[ Rootkit Hunter version 1.4.6 ]  
  
Checking rkhunter version...  
  This version : 1.4.6  
  Latest version: Download failed  
  
(kali@kali)-[~]  
$
```

Parte 2: Análisis Inicial del Sistema con Rootkit Hunter

1. Ejecutar un Escaneo Completo

sudo rkhunter --checkall

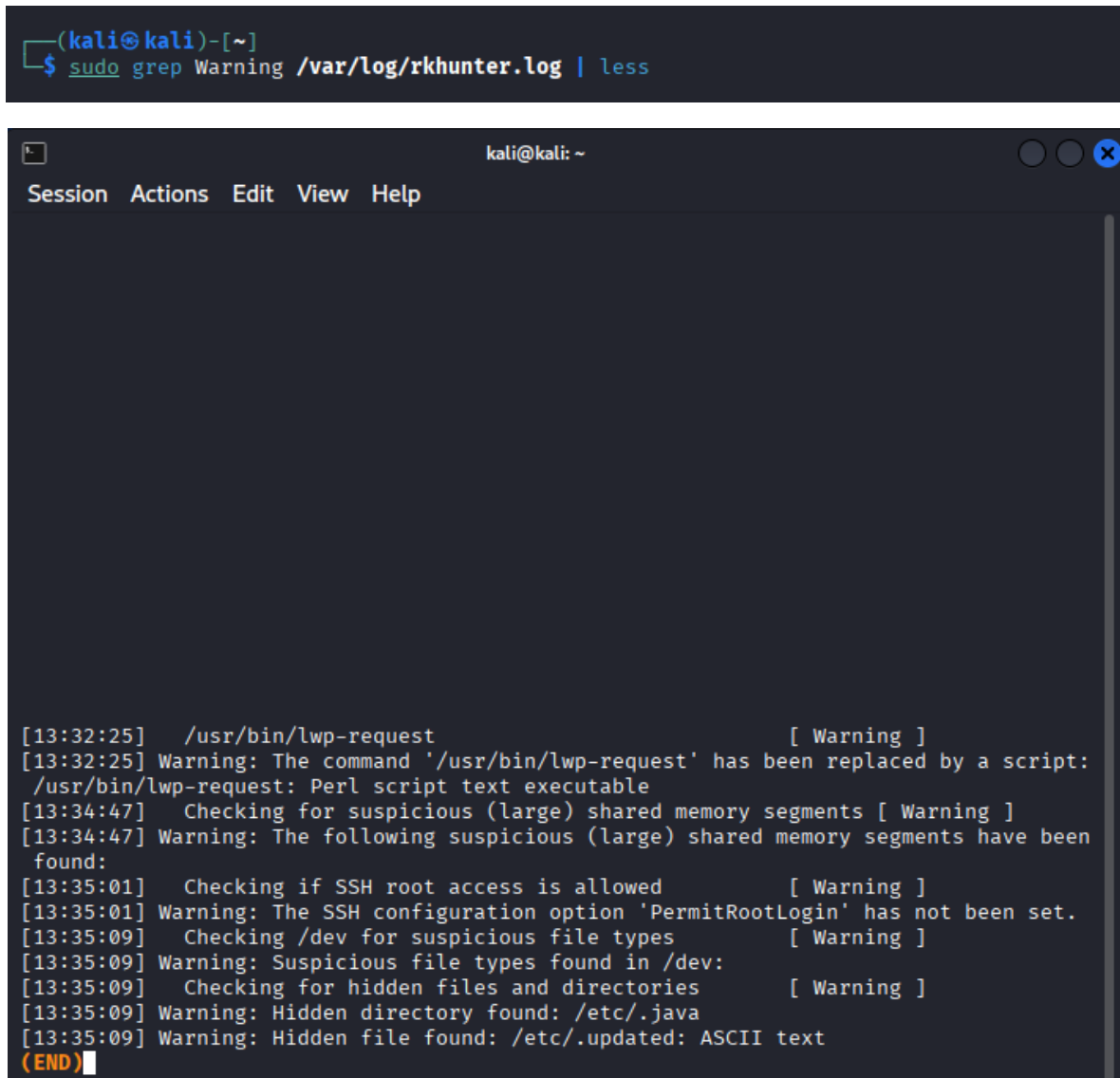
```
kali@kali: ~  
Session Actions Edit View Help  
(kali@kali)-[~]  
$ sudo rkhunter --checkall  
[ Rootkit Hunter version 1.4.6 ]  
  
Checking system commands...  
  
Performing 'strings' command checks  
Checking 'strings' command [ OK ]  
  
Performing 'shared libraries' checks  
Checking for preloading variables [ None found ]  
Checking for preloaded libraries [ None found ]  
Checking LD_LIBRARY_PATH variable [ Not found ]  
  
Performing file properties checks  
Checking for prerequisites [ OK ]  
/usr/sbin/adduser [ OK ]  
/usr/sbin/chroot [ OK ]  
/usr/sbin/cron [ OK ]  
/usr/sbin/depmod [ OK ]  
/usr/sbin/fsck [ OK ]  
/usr/sbin/groupadd [ OK ]  
/usr/sbin/groupdel [ OK ]  
/usr/sbin/groupmod [ OK ]  
/usr/sbin/grpck [ OK ]  
/usr/sbin/ifconfig [ OK ]  
/usr/sbin/ifdown [ OK ]  
/usr/sbin/ifup [ OK ]  
/usr/sbin/init [ OK ]  
/usr/sbin/inssmod [ OK ]  
/usr/sbin/ip [ OK ]  
/usr/sbin/lsmmod [ OK ]  
/usr/sbin/modinfo [ OK ]
```

```
kali@kali: ~  
Session Actions Edit View Help  
Checking for a system logging configuration file [ Found ]  
  
Performing filesystem checks  
Checking /dev for suspicious file types [ Warning ]  
Checking for hidden files and directories [ Warning ]  
  
[Press <ENTER> to continue]  
  
System checks summary  
  
File properties checks...  
Files checked: 143  
Suspect files: 1  
  
Rootkit checks...  
Rootkits checked : 498  
Possible rootkits: 2  
  
Applications checks...  
All checks skipped  
  
The system checks took: 3 minutes and 47 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)  
  
(kali@kali)-[~]  
$
```

2. Generar un Chequeo Resumido

`sudo grep Warning /var/log/rkhunter.log | less`

```
(kali㉿kali)-[~]
$ sudo grep Warning /var/log/rkhunter.log | less
```



```
[13:32:25] /usr/bin/lwp-request [ Warning ]
[13:32:25] Warning: The command '/usr/bin/lwp-request' has been replaced by a script:
/usr/bin/lwp-request: Perl script text executable
[13:34:47] Checking for suspicious (large) shared memory segments [ Warning ]
[13:34:47] Warning: The following suspicious (large) shared memory segments have been
found:
[13:35:01] Checking if SSH root access is allowed [ Warning ]
[13:35:01] Warning: The SSH configuration option 'PermitRootLogin' has not been set.
[13:35:09] Checking /dev for suspicious file types [ Warning ]
[13:35:09] Warning: Suspicious file types found in /dev:
[13:35:09] Checking for hidden files and directories [ Warning ]
[13:35:09] Warning: Hidden directory found: /etc/.java
[13:35:09] Warning: Hidden file found: /etc/.updated: ASCII text
(END)
```

Parte 3: Interpretación de los Resultados

1. Revisar las Advertencias

`sudo nano /var/log/rkhunter.log`

```
(kali㉿kali)-[~]
$ sudo nano /var/log/rkhunter.log
```

```
kali@kali: ~
Session Actions Edit View Help
GNU nano 8.6 /var/log/rkhunter.log
[13:31:26] Running Rootkit Hunter version 1.4.6 on kali
[13:31:26]
[13:31:26] Info: Start date is Wed Oct 22 01:31:26 PM EDT 2025
[13:31:26]
[13:31:26] Checking configuration file and command-line options...
[13:31:26] Info: Detected operating system is 'Linux'
[13:31:26] Info: Found O/S name: Kali GNU/Linux Rolling
[13:31:26] Info: Command line is /usr/bin/rkhunter --checkall
[13:31:26] Info: Environment shell is /usr/bin/zsh; rkhunter is using dash
[13:31:26] Info: Using configuration file '/etc/rkhunter.conf'
[13:31:26] Info: Installation directory is '/usr'
[13:31:26] Info: Using language 'en'
[13:31:26] Info: Using '/var/lib/rkhunter/db' as the database directory
[13:31:26] Info: Using '/usr/share/rkhunter/scripts' as the support script directory
[13:31:26] Info: Using '/usr/local/sbin /usr/local/bin /usr/sbin /usr/bin /sbin /bin'
[13:31:26] Info: Using '/var/lib/rkhunter/tmp' as the temporary directory
[13:31:26] Info: No mail-on-warning address configured
[13:31:26] Info: X will be automatically detected
[13:31:26] Info: Using second color set
[13:31:26] Info: Found the 'basename' command: /usr/bin/basename
[13:31:26] Info: Found the 'diff' command: /usr/bin/diff
[13:31:26] Info: Found the 'dirname' command: /usr/bin/dirname
[13:31:27] Info: Found the 'file' command: /usr/bin/file
[13:31:27] Info: Found the 'find' command: /usr/bin/find
[13:31:27] Info: Found the 'ifconfig' command: /usr/sbin/ifconfig
[13:31:27] Info: Found the 'ip' command: /usr/sbin/ip
[13:31:27] Info: Found the 'ipcs' command: /usr/bin/ipcs
[13:31:27] Info: Found the 'ldd' command: /usr/bin/ldd
[13:31:27] Info: Found the 'lsattr' command: /usr/bin/lsattr
[13:31:27] Info: Found the 'lsmod' command: /usr/sbin/lsmod
[ Read 1893 lines ]
^G Help      ^O Write Out ^F Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^N Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

```
kali@kali: ~
Session Actions Edit View Help
GNU nano 8.6 /var/log/rkhunter.log
[13:34:46] Checking for file '/dev/prom/sn.l' [ Not found ]
[13:34:47] Checking for file '/dev/fd/.88/zxsniiff.log' [ Not found ]
[13:34:47] Checking for sniffer log files [ None found ]
[13:34:47]
[13:34:47] Info: Starting test name 'tripwire'
[13:34:47] Checking for software intrusions [ Skipped ]
[13:34:47] Info: Check skipped - tripwire not installed
[13:34:47]
[13:34:47] Info: Starting test name 'susp_dirs'
[13:34:47] Checking for directory '/usr/X11R6/bin/./copy' [ Not found ]
[13:34:47] Checking for directory '/dev/rd/cdb' [ Not found ]
[13:34:47] Checking for suspicious directories [ None found ]
[13:34:47]
[13:34:47] Info: Starting test name 'ipc_shared_mem'
[13:34:47] Info: The minimum shared memory segment size to be checked (in bytes): 1048576 (1.0MB)
[13:34:47] Checking for suspicious (large) shared memory segments [ Warning ]
[13:34:47] Warning: The following suspicious (large) shared memory segments have been found:
[13:34:47] Process: /usr/bin/xfdesktop PID: 1111 Owner: kali Size: 2.0MB (configured s
[13:34:48] Process: /usr/bin/xfdesktop PID: 1111 Owner: kali Size: 64MB (configured s
[13:34:48]
[13:34:48] Info: Starting test name 'trojans'
[13:34:48] Performing trojan specific checks
[13:34:48] Checking for enabled inetd services [ Skipped ]
[13:34:48] Info: Check skipped - file '/etc/inetd.conf' does not exist.
[13:34:48] Checking for enabled xinetd services [ Skipped ]
[13:34:48] Info: Check skipped - file '/etc/xinetd.conf' does not exist.
[13:34:48] Checking for Apache backdoor [ Not found ]
[13:34:48]
[13:34:48] Info: Starting test name 'os_specific'
[13:34:48] Performing Linux specific checks
^G Help      ^O Write Out ^F Where Is  ^K Cut       ^T Execute   ^C Location  M-U Undo
^X Exit      ^R Read File ^N Replace   ^U Paste     ^J Justify   ^_ Go To Line M-E Redo
```

La alarma se debe al reporte de dos segmentos de memoria en el mismo proceso.

- **Proceso Alertado:** /usr/bin/xfdesktop. Este es el gestor de tu escritorio (XFCE).
- **Segmento 1:** Tamaño de **2.0MB**.
- **Segmento 2:** Tamaño de **64.0MB**.

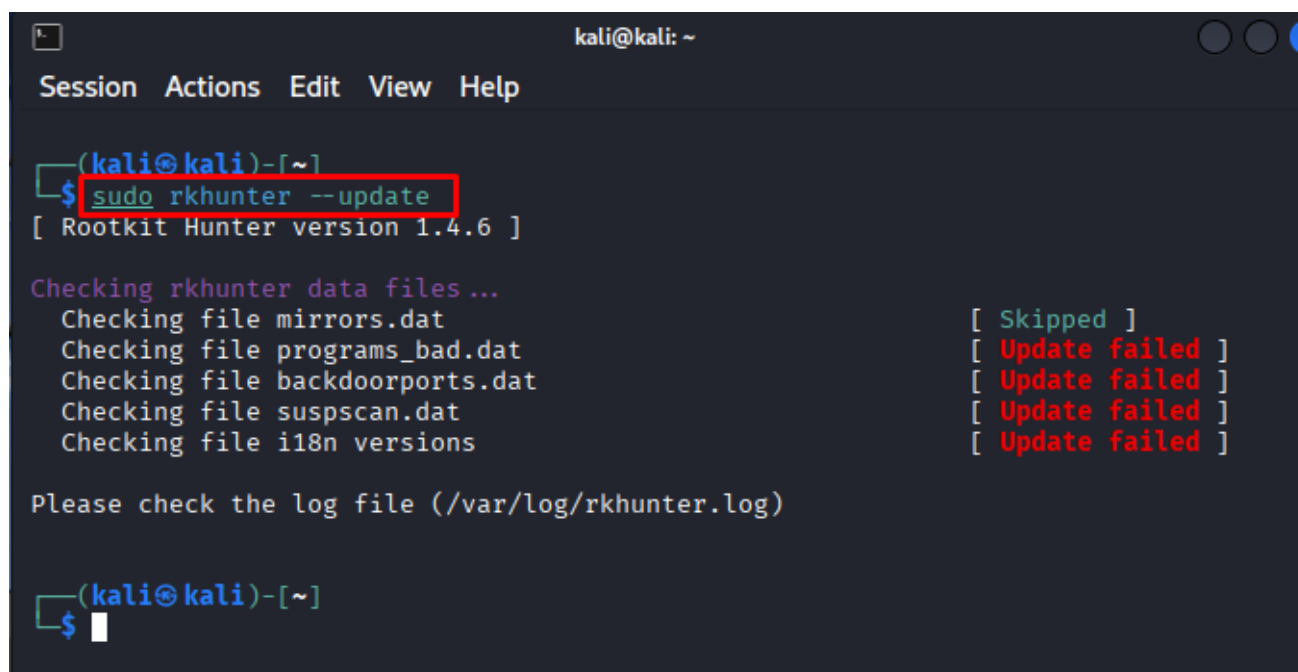
La Alarma es un Falso Positivo porque:

- a. Ambos segmentos pertenecen al mismo proceso legítimo de tu sistema operativo (xfdesktop).
- b. El segmento de **64.0MB** excede el umbral de tamaño de memoria compartida que rkhunter considera seguro.
- c. **No es un rootkit**; es una característica normal de tu entorno gráfico que rkhunter marca como sospechosa por su tamaño.

Parte 4: Actualización de Firmas y Bases de Datos de Rootkit Hunter

1. Actualización de Firmas

`sudo rkhunter --update`

A screenshot of a terminal window titled 'kali@kali: ~'. The window has a menu bar with 'Session', 'Actions', 'Edit', 'View', and 'Help'. The terminal shows the command '\$ sudo rkhunter --update' being entered, with 'sudo rkhunter --update' highlighted by a red box. Below the command, the output shows 'Rootkit Hunter version 1.4.6', followed by 'Checking rkhunter data files...'. A list of files is checked: 'mirrors.dat' (Skipped), 'programs_bad.dat' (Update failed), 'backdoorports.dat' (Update failed), 'suspscan.dat' (Update failed), and 'i18n versions' (Update failed). The output concludes with 'Please check the log file (/var/log/rkhunter.log)'. The prompt returns to '(kali@kali)-[~]' with a new '\$' character ready for input.

```
kali@kali: ~
Session Actions Edit View Help

(kali@kali)-[~]
$ sudo rkhunter --update
[ Rootkit Hunter version 1.4.6 ]

Checking rkhunter data files...
  Checking file mirrors.dat           [ Skipped ]
  Checking file programs_bad.dat      [ Update failed ]
  Checking file backdoorports.dat     [ Update failed ]
  Checking file suspscan.dat          [ Update failed ]
  Checking file i18n versions         [ Update failed ]

Please check the log file (/var/log/rkhunter.log)

(kali@kali)-[~]
$
```

2. Actualización de Propiedades

`sudo rkhunter --propupd`

```
(kali@kali)-[~]
$ sudo rkhunter --propupd
[ Rootkit Hunter version 1.4.6 ]
File updated: searched for 182 files, found 143

(kali@kali)-[~]
$
```

3. Programar un Análisis Automático

Ejecutar el comando para abrir el programador de tareas del usuario root con el editor nano
sudo crontab -e

```
kali@kali: ~
Session Actions Edit View Help

(kali@kali)-[~]
$ sudo crontab -e
no crontab for root - using an empty one
Select an editor. To change later, run select-editor again.
 1. /bin/nano          ← easiest
 2. /usr/bin/vim.basic
 3. /usr/bin/vim.tiny

Choose 1-3 [1]: 1
```

Añadir una línea para que se ejecute un escaneo diario a las 3:00 AM y posteriormente nos mande un email con los resultados del escaneo.

```
kali@kali: ~
Session Actions Edit View Help

GNU nano 8.6 /tmp/crontab.Jhg6hU/crontab *
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command
0 3 * * * /usr/sbin/rkhunter --checkall --cronjob | /usr/bin/mail -s "RKHunter Reporte Diario" root
```

Reflexión y Conclusiones

1. ¿Qué tipos de rootkits puede detectar rkhunter? ¿Por qué es importante realizar escaneos periódicos?

- **Tipos de Rootkits que detecta:** Rkhunter revisa si hay rootkits que se esconden en tres sitios principales:
 - **Archivos:** Revisa si los programas más importantes han sido cambiados o reemplazados por una versión infectada.
 - **Núcleo (Kernel):** Busca módulos o códigos extraños en el corazón del sistema operativo.
 - **Aplicaciones:** Revisa si los servicios y programas comunes tienen fallos que puedan ser usados por un *rootkit*.
- **Importancia de Escaneos Periódicos:**
 - **Detección Rápida:** Es crucial programar el escaneo (como se hizo en la Parte 5) para que se ejecute todos los días. Si un rootkit se instala durante la noche, el escaneo diario lo encontrará rápidamente.
 - **Seguridad Continua:** Al escanear a menudo, se verifica constantemente que nadie haya modificado los archivos o la memoria del sistema (como la memoria compartida que generó una alerta) desde la última revisión.

2. ¿Cuáles fueron las advertencias más comunes que encontraste? ¿Cómo podrías corregirlas?

Las advertencias que aparecieron en el chequeo son fallos de configuración o falsos positivos.

- **Archivos Extraños:** Rkhunter marcó archivos legítimos como /usr/bin/mail como sospechosos porque no estaban en su base de datos.
 - **Corrección:** Se corrigió con **sudo rkhunter --propupd**. Este comando le enseña a Rkhunter que esos archivos son normales.
- **Memoria Grande:** El programa de escritorio (xfdesktop) activó una alerta porque usaba 64.0MB de memoria compartida, un tamaño que Rkhunter considera "grande".

- **Corrección:** Se corrigió con **sudo rkhunter --propupd**, aceptando ese tamaño de memoria como seguro.
- **Fallo de SSH:** El programa alertó que la configuración de SSH podría ser insegura porque el inicio de sesión de root no estaba bloqueado.
 - **Corrección:** Para corregir la seguridad, hay que cambiar la configuración del archivo `/etc/ssh/sshd_config` para que solo los usuarios normales puedan iniciar sesión.

3. ¿Por qué es importante mantener actualizada la base de datos de rkhunter?

- **Conocer las Amenazas Nuevas:** La base de datos contiene las "firmas" (las huellas) de todos los rootkits conocidos. Si no se actualiza (Parte 4.1), Rkhunter solo buscará amenazas viejas y dejará pasar a los rootkits nuevos.
- **Evitar Falsos Negativos:** Una base de datos sin actualizar significa que el programa no tiene la información más reciente para verificar archivos. Esto puede llevar a un falso negativo, donde el programa te dice que estás limpio, pero en realidad tienes un *rootkit* nuevo que no pudo reconocer.
- **Problema Común:** El fallo en la actualización de la práctica demuestra un problema de seguridad grave: si las defensas no se renuevan constantemente, el software no puede reconocer las amenazas más modernas, dejando al sistema expuesto y vulnerable.