# Linux: Como proteger o Linux contra RootKits com o rkhunter!

## Aumente a segurança do seu Linux. Identifique e corrija possíveis brechas de segurança com o rkhunter!

Provavelmente, o malware mais perigoso que os usuários do GNU/Linux enfrentam é o rootkits. Para lutar contra rootkits e outras possíveis explorações, esta seção mostra como instalar e utilizar o rkhunter. Este programa varre seu desktop para verificar arquivos suspeitos que podem ter sido instalados por um hacker para obter controle do seu computador. Vale lembrar que este mesmo pacote esta disponível em todas as distribuições, ao menos até agora. Hoje, vamos abordar o processo de instalação para Ubuntu, Debian, Linux Mint, Fedora, Mageia, CentOS, Red Hat e derivados.

## Instalação e utilização do rkhunter

**Algumas distribuições já possuem o pacote rkhunter em seus repositórios, siga o processo de instalação de acordo com a sua distribuição.**

### Para Ubuntu, Linux Mint, Debian e derivados, execute:

**Para instalar o rkhunter, siga estas etapas:**

Para navegar de volta para o terminal, selecione Aplicativos > Acessórios > Terminal. Em seguida, cole o comando abaixo:

```
sudo apt install rkhunter
```

Assim que o rkhunter tiver sido instalado com êxito, você pode executá-lo para verificar várias explorações em seu desktop.

**Para iniciar o programa, vá abra o terminal e execute:**

```
sudo rkhunter --check
```

Se o rkhunter estiver executando apropriadamente, você começa a visualizar uma lista de diretórios com a palavra OK ou Aviso próxima a eles. Quando iniciado, o rkhunter executa vários tipos de varreduras. Após a conclusão de uma varredura, você começa a próxima pressionando Enter.

**Os diferentes tipos de varreduras são:**

- Diretórios;
- Exploram no desktop;
- Portas que são comumente utilizadas para acesso à porta dos fundos;
- Arquivos de inicialização, grupos e contas, arquivos de configuração do sistema e o sistema de arquivos;
- Aplicativos;

Após todas as varreduras serem concluídas, o rkhunter fornece um relatório e cria um arquivo de log com os resultados.

Assim como com o ClamAV, você precisa atualizar o rkhunter regularmente de forma que ele possa detectar as vulnerabilidades e explorações mais recentes:

```
sudo rkhunter --update
```

### EXTRA! Vamos agora instalar e utilizar o chkrootkit!

Embora a maioria do software antivírus não execute apropriadamente junto com um programa antivírus de outra empresa, os caçadores de rootkit executarão simbioticamente com outro. Portanto, para uma proteção mais abrangente, você pode instalar o chkrootkit e executá-lo junto com o rkhunter.

```
sudo apt install chkrootkit
```

Assim que o chkroot for instalado, você o executará assim como o rkhunter. No terminal, execute:

```
sudo chkrootkit
```

## Para instalar o rkhunter em qualquer distribuição Linux

Este processo de instalação funciona em qualquer distribuição Linux, inclusive nas anteriores que orientamos a instalação. Siga todos os passos para que a instalação ocorra sem erros. Abra um Terminal e execute:

Primeiro vamos entrar no diretório temporário:

```
cd /tmp
```

Agora, vamos fazer o download do pacote disponibilizado no site oficial do projeto.

```
wget -c https://sourceforge.net/projects/rkhunter/files/rkhunter/1.4.6/rkhunter-1.4.6.tar.gz
```

Agora vamos extrair o conteúdo baixado:

```
sudo tar -xvf rkhunter-1.4.6.tar.gz
sudo cd rkhunter-1.4.6
sudo ./installer.sh --layout default --install
```

Para atualizar a base do rkhunter através deste processo de instalação, execute:

```
sudo /usr/local/bin/rkhunter --update
sudo /usr/local/bin/rkhunter --propupd
```

## Checagem automática do rkhunter via cron

Se você estiver usando o rkhunter em algum servidor ou queira que ele faça checagem diárias automáticas, é possível adicioná-lo ao Cron. Essa etapa não é obrigatória, até porque você pode executar verificações manuais sem nenhum problema:

```
sudo vi /etc/cron.daily/rkhunter.sh
```

Dentro do arquivo cole o seguinte conteúdo, caso ele não exista, e altere os dados de exemplo, para os reais:

```
#!/bin/sh

(

/usr/local/bin/rkhunter –versioncheck

/usr/local/bin/rkhunter –update

/usr/local/bin/rkhunter –cronjob –report-warnings-only

) | /bin/mail -s ‘rkhunter Daily Run (ColoqueONomeDoSeuServidorAqui)’ seu@email.com
```

Alterando permissões:

```
sudo chmod 755 /etc/cron.daily/rkhunter.sh
```

# Checagem Manual

Se você optou pela checagem manual o processo também é muito simples, execute:

```
sudo rkhunter --check
```

E para verificar os logs, execute:

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

Caso você precise de ajuda ou queira verificar as possibilidades do rkhunter, execute:

```
rkhunter --help
```

# Conclusão

Quando o chkroot concluir sua varredura, você será levado de volta ao terminal. Se o rkhunter ou o descobrir algo fora do normal, eles simplesmente o informam sobre o possível problema. Nenhum destes programas realmente exclui arquivos do seu computador. Se você for alertado a algo por qualquer um dos programas, pesquise a exploração ou vulnerabilidade que foi relatada e certifique-se de que o que foi localizado não é um positivo falso.

Em seguida, determine as etapas necessárias para eliminar a ameaça. Algumas vezes, você só precisa atualizar o sistema operacional ou outro software. Outras vezes, pode ser necessário localizar um programa enganador e erradicá-lo do seu sistema.

https://sempreupdate.com.br/linux-como-proteger-o-linux-contra-rootkits/

# How to Install Chkrootkit

1 year ago
by Ivan Vanney

This tutorial focuses on rootkits and how to detect them using chkrootkit. Rootkits are tools designed to grant access or privileges while hiding their own presence, or the presence of an additional software granting the access, the “rootkit” term focuses on hiding aspect. To achieve hiding a malicious software rootkit manage to integrate into the target’s kernel, software or in the worst case within hardware firmware.

Usually, when detected the presence of a rootkit the victim needs to reinstall the OS and fresh hardware, analyze files to be transferred to the replacement and in the worst-case hardware replacement will be needed.It is important to highlight the possibility of false positives, this is the main problem of chkrootkit, therefore when a threat is detected the recommendation is to run additional alternatives before taking measures, this tutorial will also briefly explore rkhunter as an alternative. It is also important to say this tutorial is optimized for Debian and based Linux distributions users, the only limitation for other distributions users is the installation part, the usage of chkrootkit is the same for all distros.

Since rootkits have a variety of ways to achieve its goals hiding malicious software, Chkrootkit offers a variety of tools to afford these ways. Chkrootkit is a tools suite which include the main chkrootkit program and additional libraries which are listed below:

**chkrootkit**: Main program which checks operating system binaries for rootkit modifications to learn if the code was adulterated.

**ifpromisc.c**: checks if the interface is in promiscuous mode. If a network interface is in promiscuous mode, it can be used by an attacker or malicious software to capture the network traffic to later analyze it.

**chklastlog.c**: checks for lastlog deletions. Lastlog is a command which shows information on last logins. An attacker or rootkit may modify the file to avoid detection if the sysadmin checks this command to learn information on logins.

**chkwtmp.c**: checks for wtmp deletions. Similarly, to the previous script, chkwtmp checks the file wtmp, which contains information on users’ logins to try to detect modifications on it in case a rootkit modified the entries to prevent detection of intrusions.

**check_wtmpx.c**: This script is the same as the above but Solaris systems.
**chkproc.c**: checks for signs of trojans within LKM (Loadable Kernel Modules).
**chkdirs.c**: has the same function as the above, checks for trojans within kernel modules.
**strings.c**: quick and dirty strings replacement aiming to hide the nature of the rootkit.
**chkutmp.c**: this is similar to chkwtmp but checks the utmp file instead.

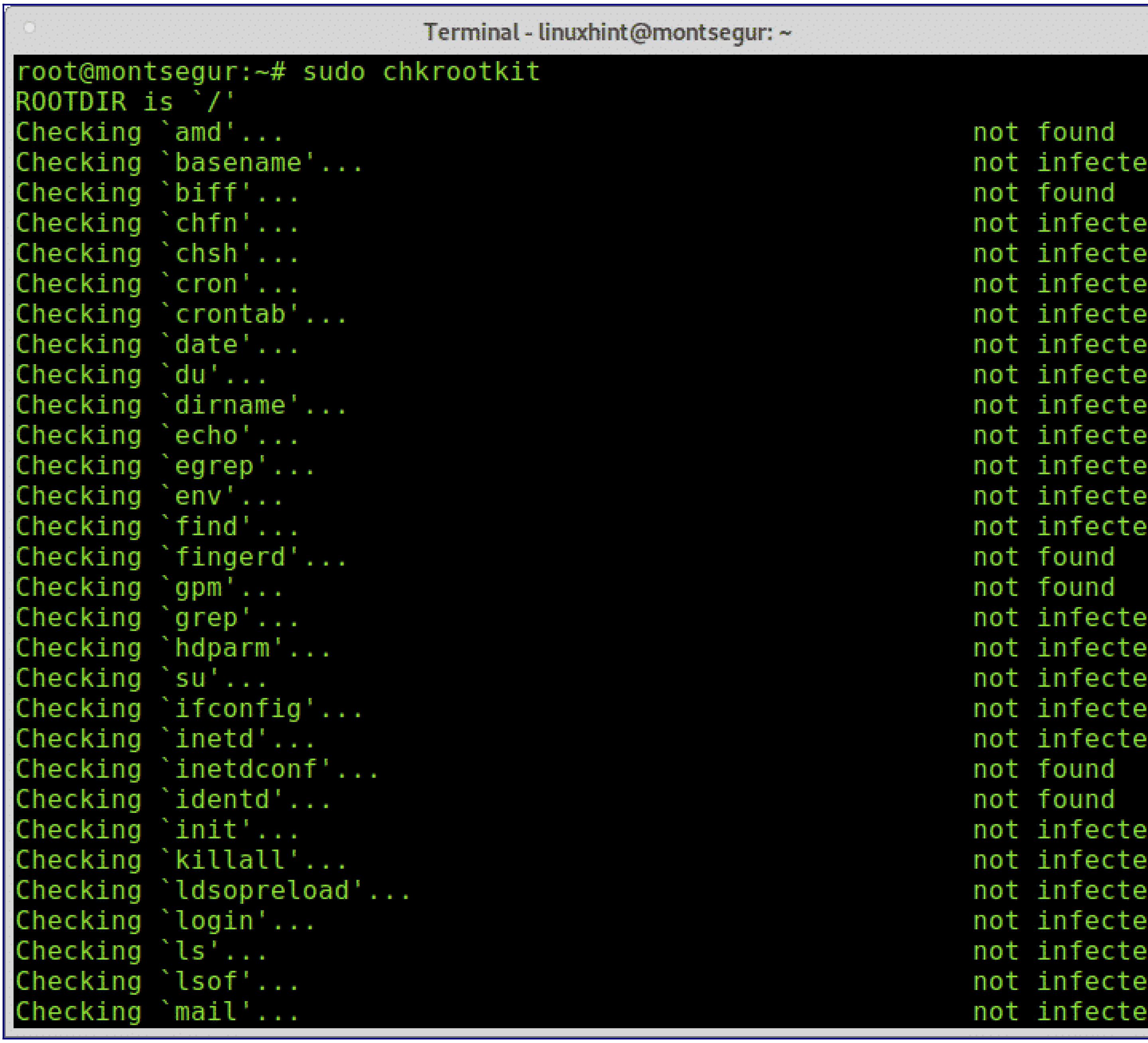
All the scripts mentioned above are executed when we run **chkrootkit**.

To begin installing chkrootkit on Debian and based Linux distributions run:

```
# apt install chkrootkit -y
```

Once installed to run it execute:

```
# sudo chkrootkit
```

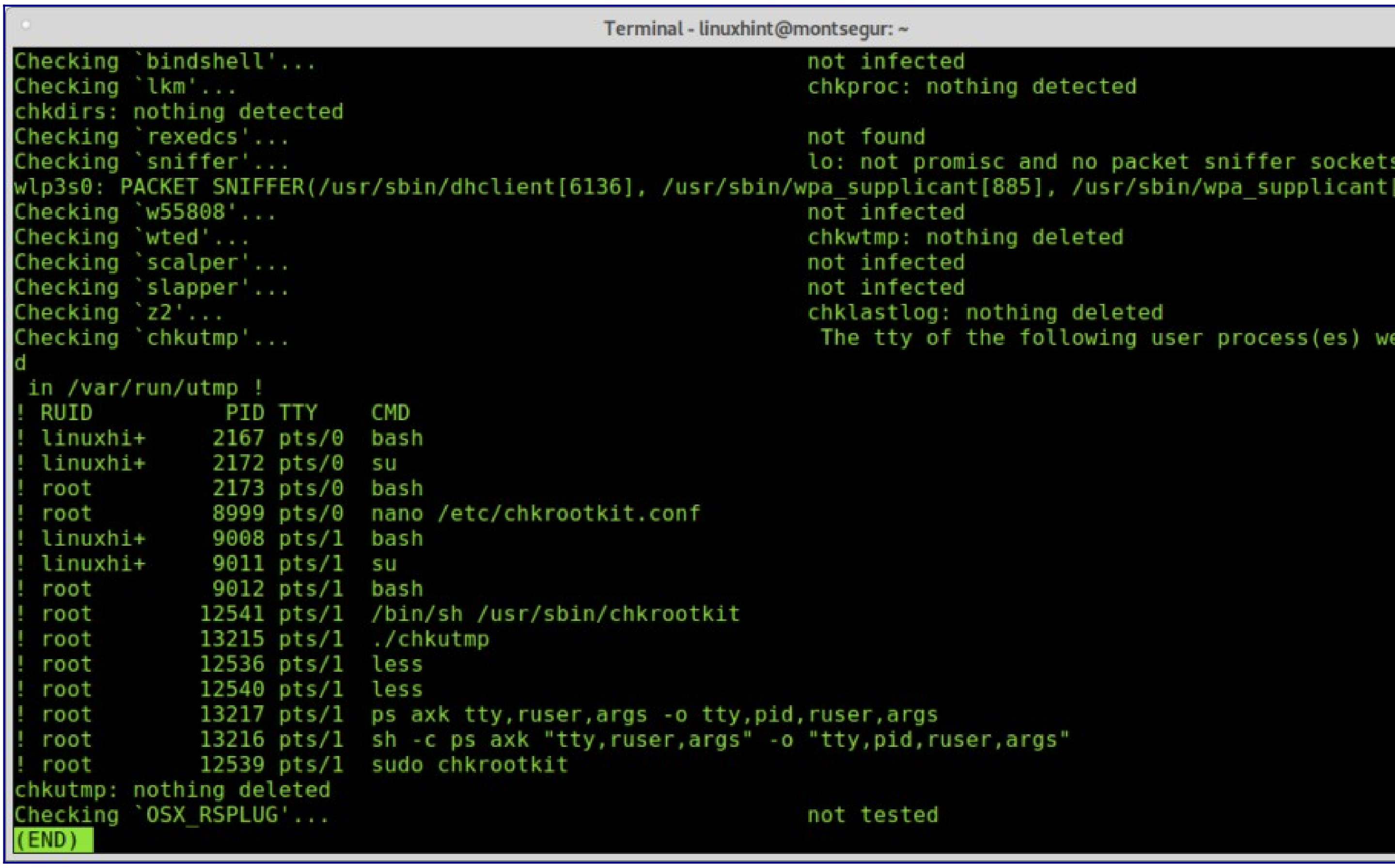


```
root@montsegur:~# sudo chkrootkit
ROOTDIR is `/'
Checking `amd'...                                            not found
Checking `basename'...                                       not infecte
Checking `biff'...                                           not found
Checking `chfn'...                                           not infecte
Checking `chsh'...                                           not infecte
Checking `cron'...                                           not infecte
Checking `crontab'...                                        not infecte
Checking `date'...                                           not infecte
Checking `du'...                                             not infecte
Checking `dirname'...                                        not infecte
Checking `echo'...                                           not infecte
Checking `egrep'...                                          not infecte
Checking `env'...                                            not infecte
Checking `find'...                                           not infecte
Checking `fingerd'...                                        not found
Checking `gpm'...                                            not found
Checking `grep'...                                           not infecte
Checking `hdparm'...                                         not infecte
Checking `su'...                                             not infecte
Checking `ifconfig'...                                       not infecte
Checking `inetd'...                                          not infecte
Checking `inetdconf'...                                      not found
Checking `identd'...                                         not found
Checking `init'...                                           not infecte
Checking `killall'...                                        not infecte
Checking `ldsopreload'...                                    not infecte
Checking `login'...                                          not infecte
Checking `ls'...                                             not infecte
Checking `lsof'...                                           not infecte
Checking `mail'...                                           not infecte
```

During the process you can see all scripts integrating chkrootkit are executed doing each its part.

You can get a more comfortable view with scrolling  adding  pipe and less:

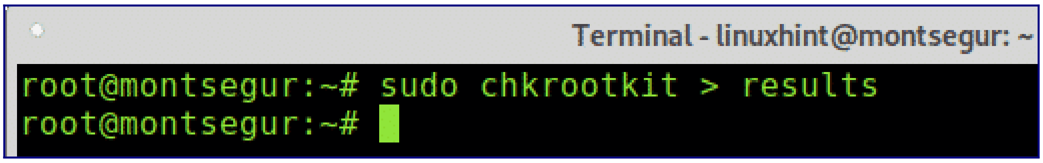
# sudo chkrootkit | less



```
Checking `bindshell'...                                     not infected
Checking `lkm'...                                           chkproc: nothing detected
chkdirs: nothing detected
Checking `rexedcs'...                                       not found
Checking `sniffer'...                                       lo: not promisc and no packet sniffer sockets
wlp3s0: PACKET SNIFFER(/usr/sbin/dhclient[6136], /usr/sbin/wpa_supplicant[885], /usr/sbin/wpa_supplicant[
Checking `w55808'...                                        not infected
Checking `wted'...                                          chkwtmp: nothing deleted
Checking `scalper'...                                       not infected
Checking `slapper'...                                       not infected
Checking `z2'...                                            chklastlog: nothing deleted
Checking `chkutmp'...                                        The tty of the following user process(es) we
d
 in /var/run/utmp !
! RUID          PID TTY    CMD
! linuxhi+     2167 pts/0  bash
! linuxhi+     2172 pts/0  su
! root         2173 pts/0  bash
! root         8999 pts/0  nano /etc/chkrootkit.conf
! linuxhi+     9008 pts/1  bash
! linuxhi+     9011 pts/1  su
! root         9012 pts/1  bash
! root        12541 pts/1  /bin/sh /usr/sbin/chkrootkit
! root        13215 pts/1  ./chkutmp
! root        12536 pts/1  less
! root        12540 pts/1  less
! root        13217 pts/1  ps axk tty,ruser,args -o tty,pid,ruser,args
! root        13216 pts/1  sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
! root        12539 pts/1  sudo chkrootkit
chkutmp: nothing deleted
Checking `OSX_RSPLUG'...                                    not tested
(END)
```

You can also export the results to a file using the following syntax:

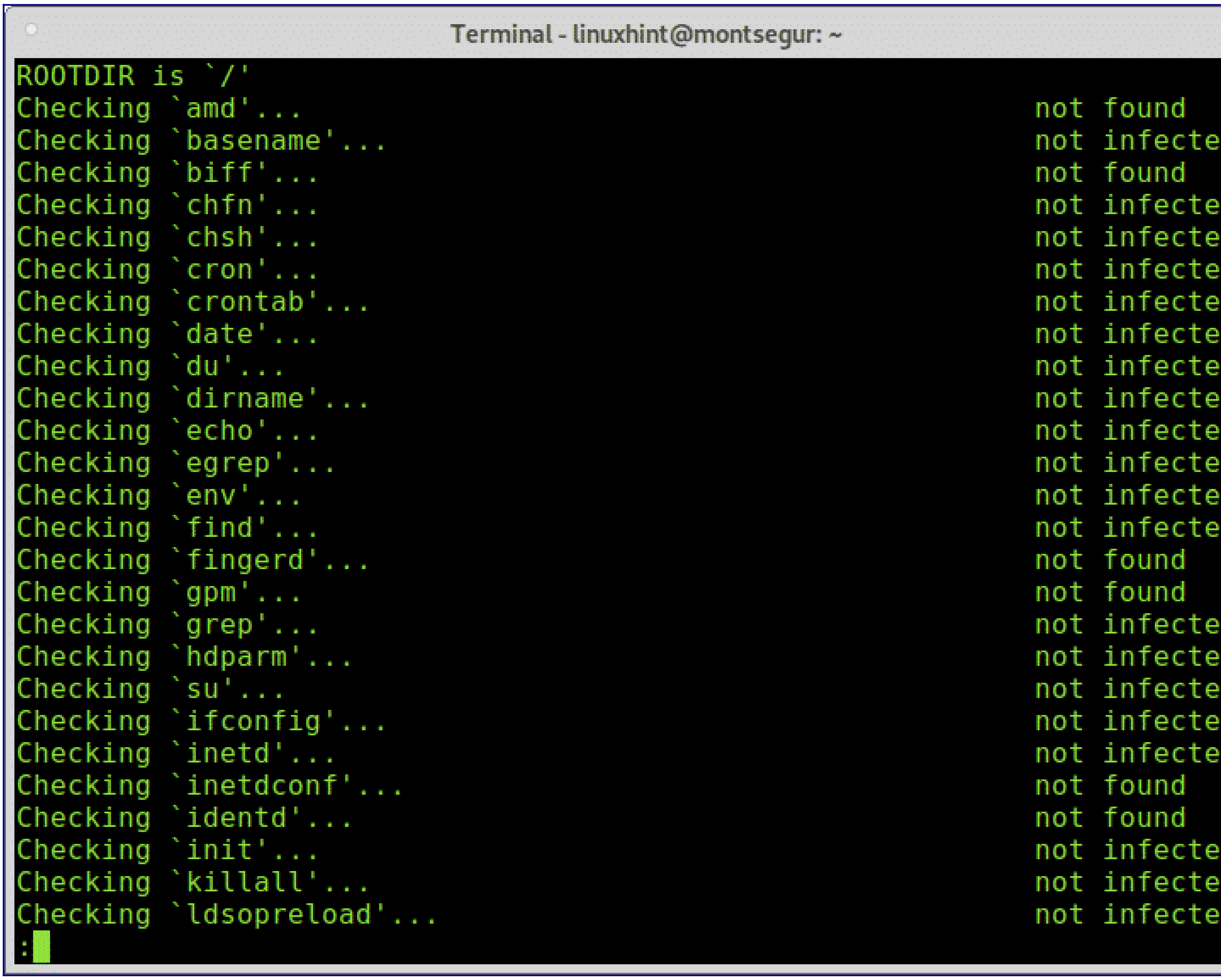
# sudo chkrootkit > results



```
root@montsegur:~# sudo chkrootkit > results
root@montsegur:~# 
```

Then to see the output type:

# less results



```
ROOTDIR is `/'
Checking `amd'...                                            not found
Checking `basename'...                                       not infecte
Checking `biff'...                                           not found
Checking `chfn'...                                           not infecte
Checking `chsh'...                                           not infecte
Checking `cron'...                                           not infecte
Checking `crontab'...                                        not infecte
Checking `date'...                                           not infecte
Checking `du'...                                             not infecte
Checking `dirname'...                                        not infecte
Checking `echo'...                                           not infecte
Checking `egrep'...                                          not infecte
Checking `env'...                                            not infecte
Checking `find'...                                           not infecte
Checking `fingerd'...                                        not found
Checking `gpm'...                                            not found
Checking `grep'...                                           not infecte
Checking `hdparm'...                                         not infecte
Checking `su'...                                             not infecte
Checking `ifconfig'...                                       not infecte
Checking `inetd'...                                          not infecte
Checking `inetdconf'...                                      not found
Checking `identd'...                                         not found
Checking `init'...                                           not infecte
Checking `killall'...                                        not infecte
Checking `ldsopreload'...                                    not infecte
:
```

**Note**: you can replace "results" for any name you want to give the output file.

By default you need to run chkrootkit manually as explained above, yet you can define daily automatic scans by editing chkrootkit configuration file located at /etc/chkrootkit.conf, try it using nano or any text editor you like:

# nano /etc/chkrootkit.conf

To achieve daily automatic scan the first line containing **RUN_DAILY="false"** should be edited to **RUN_DAILY="true"**

This is how it should look:

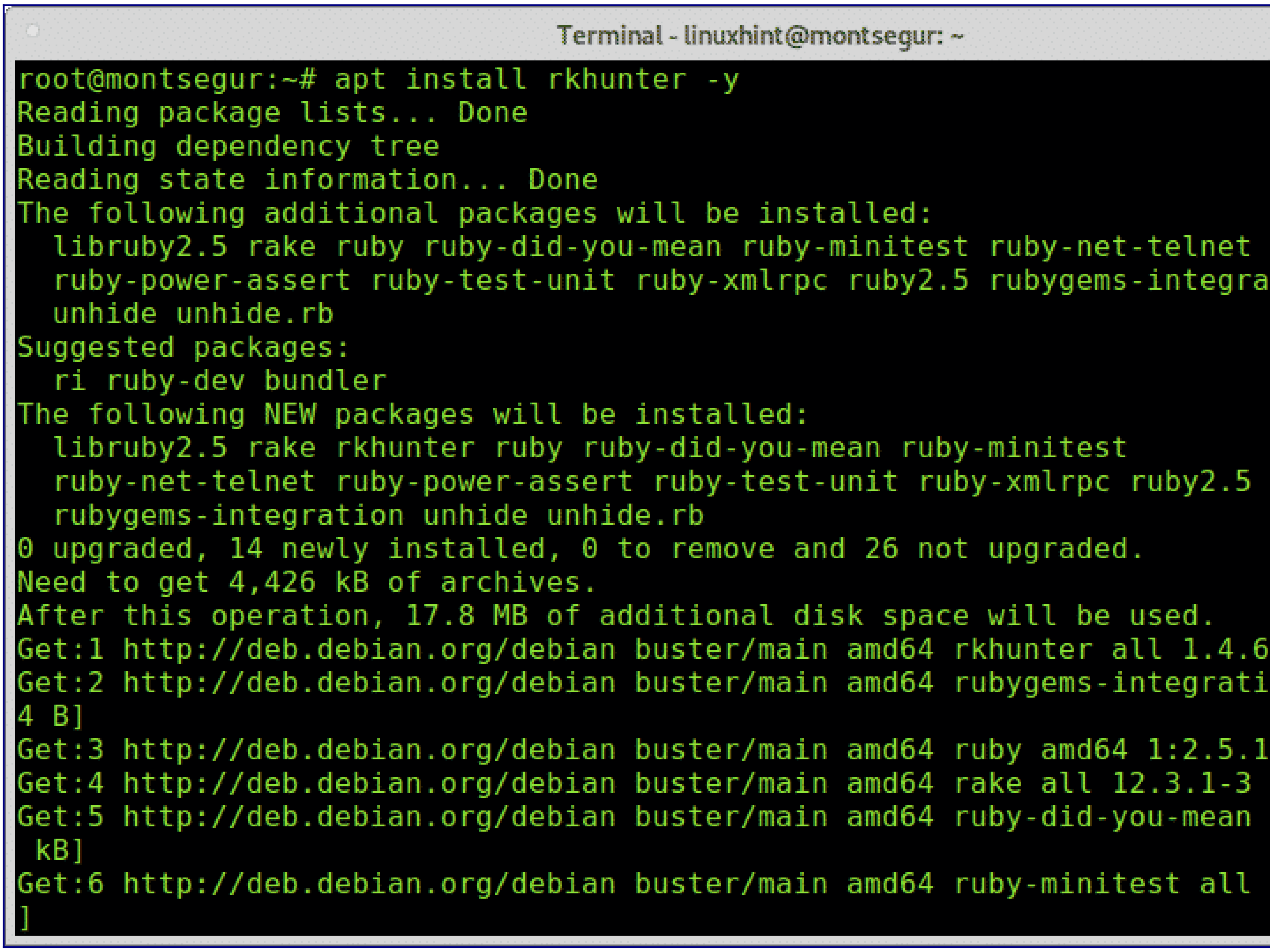
Press **CTRL**+**X** and **Y** to save and exit.

## Rootkit Hunter, an alternative to chkrootkit:

Another option to chkrootkit is RootKit Hunter,it is also a complement considering if you found rootkits using one of them, using the alternative is mandatory to discard false positives.

To begin with RootKitHunter, install it by running:

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

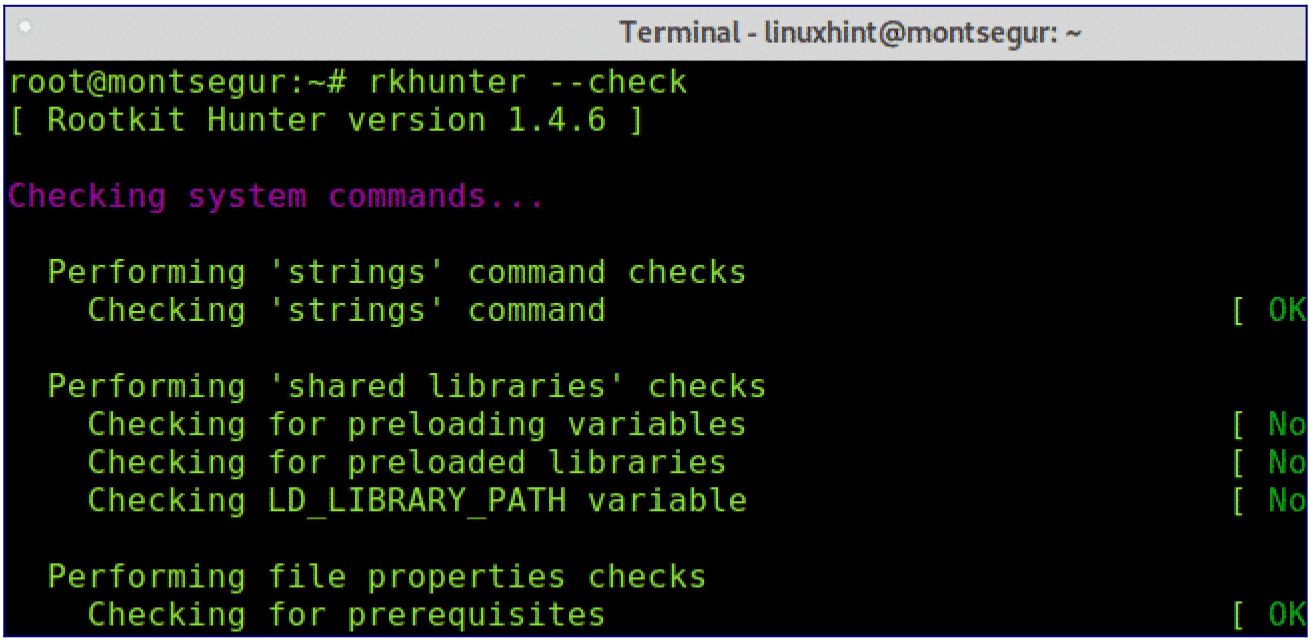


```
root@montsegur:~# apt install rkhunter -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libruby2.5 rake ruby ruby-did-you-mean ruby-minitest ruby-net-telnet
  ruby-power-assert ruby-test-unit ruby-xmlrpc ruby2.5 rubygems-integra
  unhide unhide.rb
Suggested packages:
  ri ruby-dev bundler
The following NEW packages will be installed:
  libruby2.5 rake rkhunter ruby ruby-did-you-mean ruby-minitest
  ruby-net-telnet ruby-power-assert ruby-test-unit ruby-xmlrpc ruby2.5
  rubygems-integration unhide unhide.rb
0 upgraded, 14 newly installed, 0 to remove and 26 not upgraded.
Need to get 4,426 kB of archives.
After this operation, 17.8 MB of additional disk space will be used.
Get:1 http://deb.debian.org/debian buster/main amd64 rkhunter all 1.4.6
Get:2 http://deb.debian.org/debian buster/main amd64 rubygems-integrati
4 B]
Get:3 http://deb.debian.org/debian buster/main amd64 ruby amd64 1:2.5.1
Get:4 http://deb.debian.org/debian buster/main amd64 rake all 12.3.1-3
Get:5 http://deb.debian.org/debian buster/main amd64 ruby-did-you-mean
 kB]
Get:6 http://deb.debian.org/debian buster/main amd64 ruby-minitest all
]
```

Once installed, to run a test execute the following command:

# rkhunter --check

As you can see, like chkrootkit the first step of RkHunter is to analyze the system binaries, but also libraries and strings:

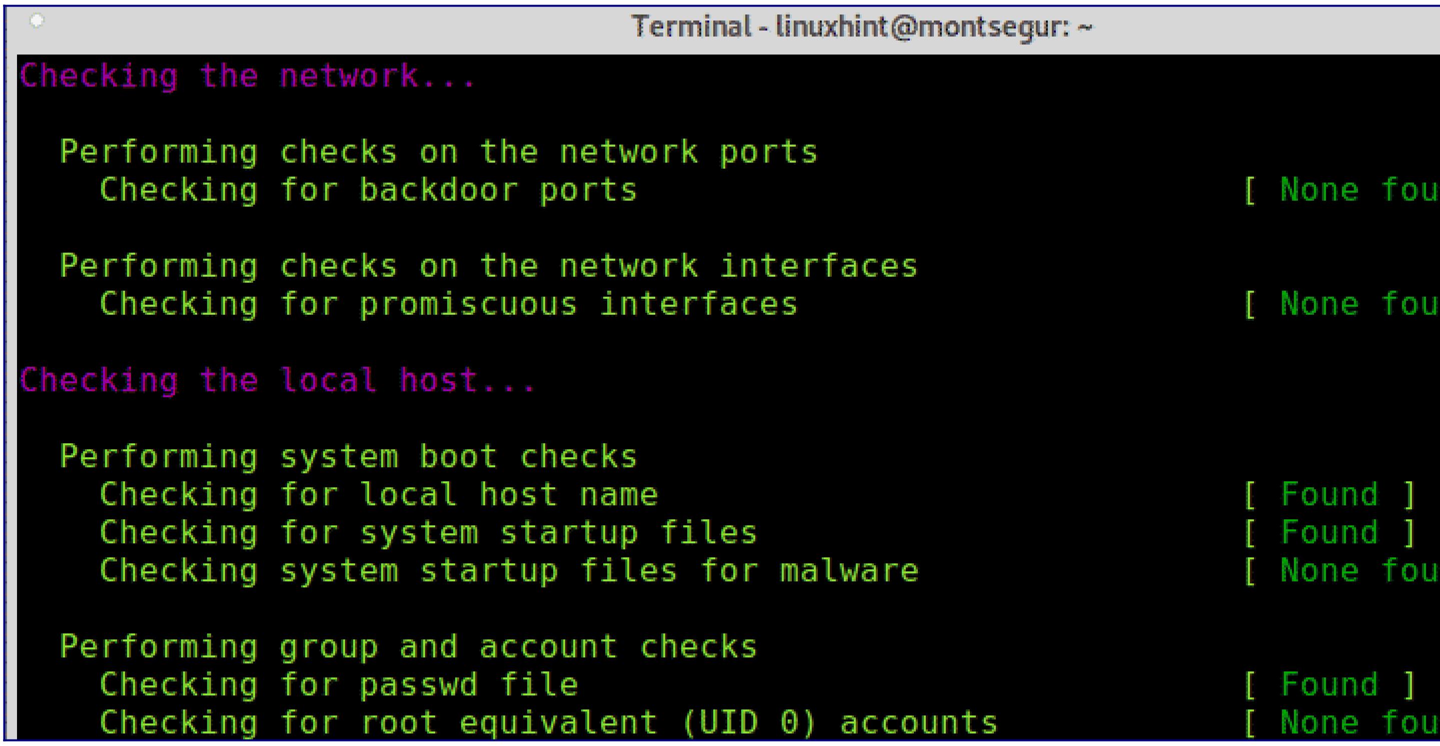


```
root@montsegur:~# rkhunter --check
[ Rootkit Hunter version 1.4.6 ]

Checking system commands...

  Performing 'strings' command checks
    Checking 'strings' command                                   [ OK

  Performing 'shared libraries' checks
    Checking for preloading variables                            [ No
    Checking for preloaded libraries                             [ No
    Checking LD_LIBRARY_PATH variable                            [ No

  Performing file properties checks
    Checking for prerequisites                                   [ OK
```

As you will see, contrary to chkrootkit RkHunter will request you to press ENTER to continue with next steps, previously RootKit Hunter checked the system binaries and libraries, now it will go for known rootkits:

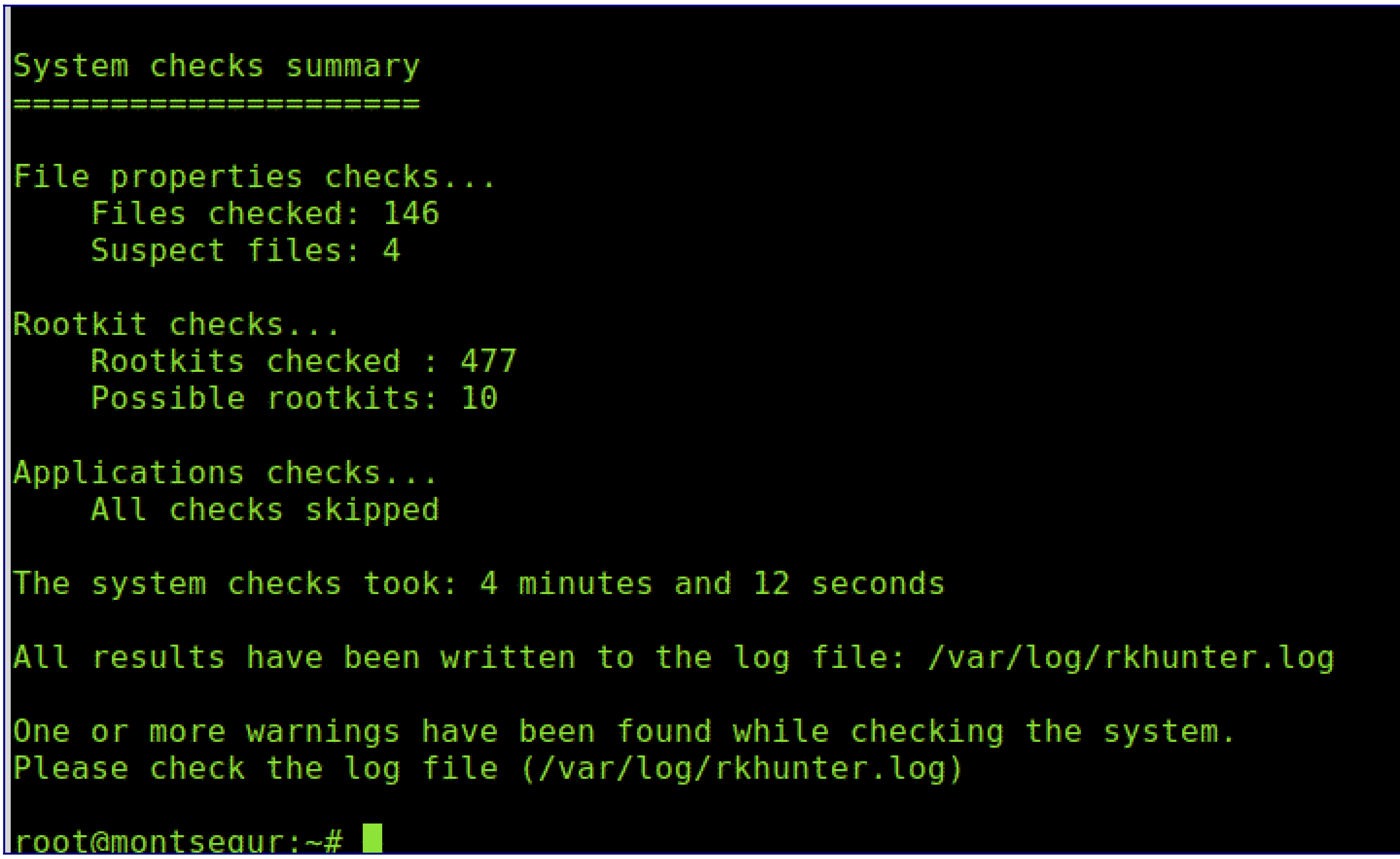
Press ENTER to let RkHunter to go ahead with rootkits search:

Then, like chkrootkit it will check your network interfaces and also ports known for being used by backdoors or trojans:



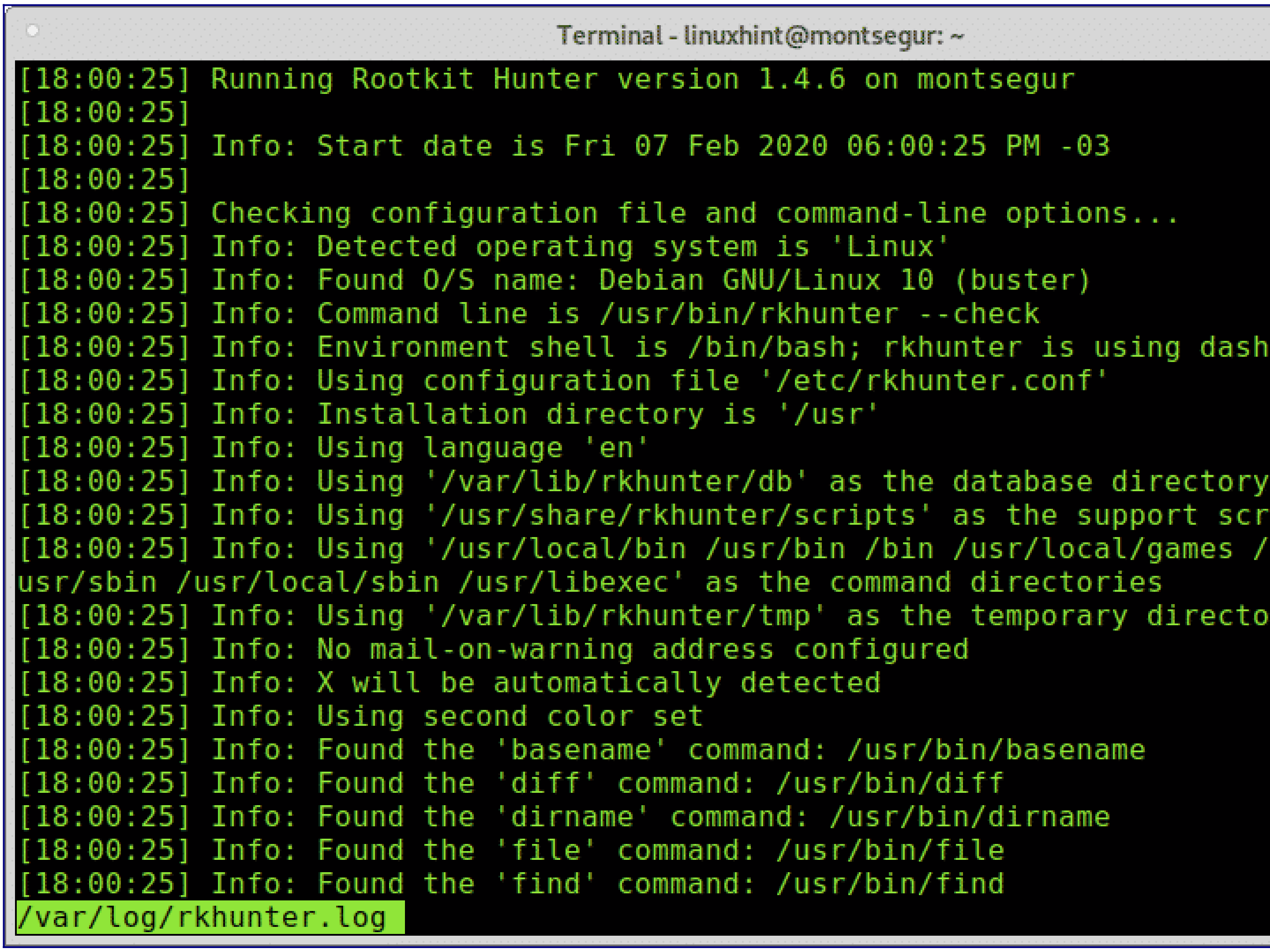
```
Checking the network...

  Performing checks on the network ports
    Checking for backdoor ports                                   [ None fou

  Performing checks on the network interfaces
    Checking for promiscuous interfaces                           [ None fou

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 fou

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

Finally it will print a summary of the results.



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

File properties checks...
    Files checked: 146
    Suspect files: 4

Rootkit checks...
    Rootkits checked : 477
    Possible rootkits: 10

Applications checks...
    All checks skipped

The system checks took: 4 minutes and 12 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)

root@montsegur:~#
```

You can always access results saved at **/var/log/rkhunter.log**:



```
[18:00:25] Running Rootkit Hunter version 1.4.6 on montsegur
[18:00:25]
[18:00:25] Info: Start date is Fri 07 Feb 2020 06:00:25 PM -03
[18:00:25]
[18:00:25] Checking configuration file and command-line options...
[18:00:25] Info: Detected operating system is 'Linux'
[18:00:25] Info: Found O/S name: Debian GNU/Linux 10 (buster)
[18:00:25] Info: Command line is /usr/bin/rkhunter --check
[18:00:25] Info: Environment shell is /bin/bash; rkhunter is using dash
[18:00:25] Info: Using configuration file '/etc/rkhunter.conf'
[18:00:25] Info: Installation directory is '/usr'
[18:00:25] Info: Using language 'en'
[18:00:25] Info: Using '/var/lib/rkhunter/db' as the database directory
[18:00:25] Info: Using '/usr/share/rkhunter/scripts' as the support scr
[18:00:25] Info: Using '/usr/local/bin /usr/bin /bin /usr/local/games /
usr/sbin /usr/local/sbin /usr/libexec' as the command directories
[18:00:25] Info: Using '/var/lib/rkhunter/tmp' as the temporary directo
[18:00:25] Info: No mail-on-warning address configured
[18:00:25] Info: X will be automatically detected
[18:00:25] Info: Using second color set
[18:00:25] Info: Found the 'basename' command: /usr/bin/basename
[18:00:25] Info: Found the 'diff' command: /usr/bin/diff
[18:00:25] Info: Found the 'dirname' command: /usr/bin/dirname
[18:00:25] Info: Found the 'file' command: /usr/bin/file
[18:00:25] Info: Found the 'find' command: /usr/bin/find
/var/log/rkhunter.log
```

If you suspect your device may be infected by a rootkit or compromised you can follow the recommendations listed at https://linuxhint.com/detect_linux_system_hacked/.

I hope you found this tutorial on How to install, configure and use chkrootkit useful. Keep following LinuxHint for more tips and updates on Linux and networking.

https://linuxhint.com/install_chkrootkit/