

**CS762 Memory Analysis and Forensics
PROJECT**

Name: Priyanka Vepuri

UIN: 01184333

Abstract:

The main purpose of the project is to develop a lab using virtual machines. The two major Operating Systems here are Windows and Linux. In general, the memory samples can be analyzed by a few tools and methods. These are useful for static memory analysis, which in turn gets into a dynamic memory analysis. Here are some of the tools that we used for Windows

- total viruses
- md5deep
- strings
- threat expert
- Dependency Walker

And some of the tools used for Linux are

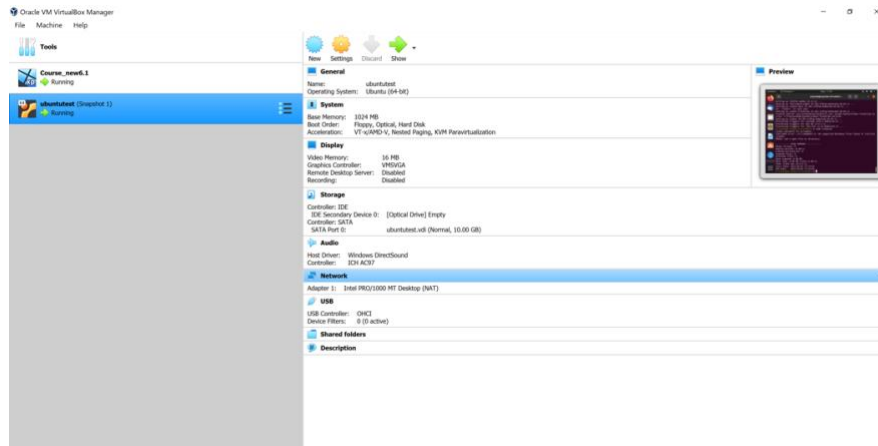
- RKhunter
- chkrootkit
- clamAV

Now, let's look how these tools are downloaded, installed, and used.

Virtual Box:

Oracle VM VirtualBox is a cross-platform virtualization application. For one thing, it installs on your current Intel or AMD-based PCs, regardless of whether they are running Windows, Mac OS X, Linux, or Oracle Solaris operating frameworks (OSes). Furthermore, it expands the abilities of your current PC with the goal that it can run different OSes, inside various virtual machines, simultaneously. Oracle VM VirtualBox is misleadingly basic yet additionally exceptionally powerful. It can run wherever from little embedded systems or then again desktop class machines as far as possible up to datacenter organizations and even Cloud environments. The accompanying screen capture shows how Oracle VM VirtualBox, installed on an Apple Mac Operating system X PC, is running Windows Server 2016 in a virtual machine window.

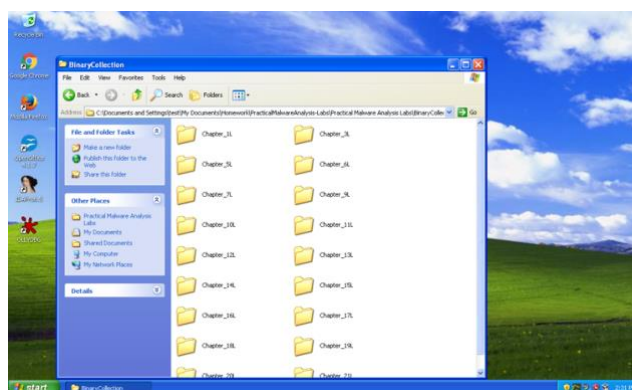
The strategies and highlights that Oracle VM VirtualBox gives are valuable since it assists us with running multiple operating systems in our current PC simultaneously. For instance, we can run Linux on our Windows system or run Windows and Linux on our Mac system. It also helps for installing the software easily, testing and disaster recovery, and infrastructure consolidation.



First, let's look at the tools used in Windows.

⇒ **Hashing:**

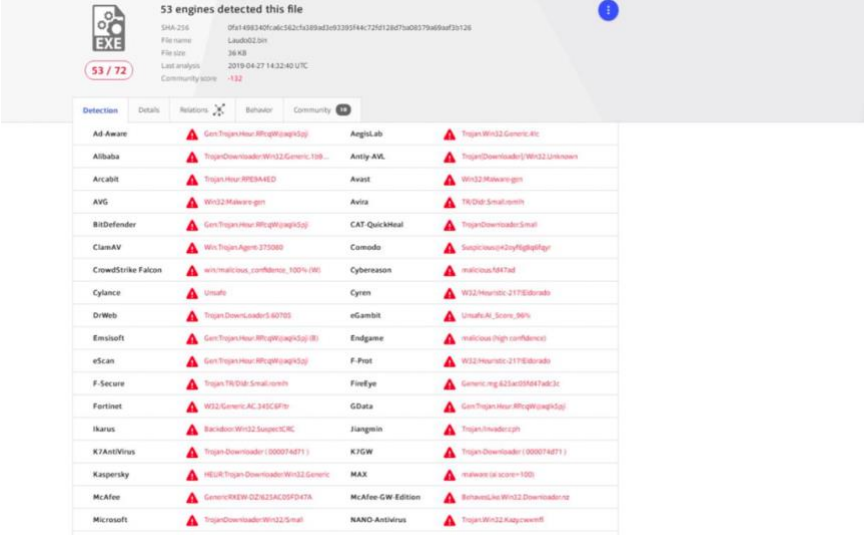
One of the most important method to refer to a malware is through its HASH value. A HASH value is a numeric value of a fixed length that uniquely identifies data. Hashing is a software process of creating fixed character length hash values for a text document. This is a single-way function meaning the original text document can't be produced back from the hash value. This hash value is utilized to check the integrity of original content when it is sent over a communication medium. Hash Tool is a utility to calculate the hash of multiple files.



A file hash can be said to be the 'signature' of a file and is used in many applications, including checking the integrity of downloaded files. This compact application helps you quickly and easily list the hashes of your files. Application developer likewise utilize this strategy for securing passwords of clients signing into their systems. Rather than putting away passwords in the back-end database in clear content, secret key hashes are utilized. This shield clear-text passwords from internal application engineers and furthermore from hackers in the case that they can penetrate the database. Hackers are aware of this cycle and have a lot of tools in their armory to effectively surmise the passwords from the hashes. I utilize the word 'surmise' in light of the fact that recollect hashes are single-way functions, you cannot decode them like you can do to an encoded string.

⇒ Virus Total:

VirusTotal aggregates numerous antivirus items and online scan engines to check for viruses that the client's own antivirus may have missed, or to confirm against any untrue positives. Files up to 550 MB can be transferred to the website or sent by means of email (max. 32MB).



53 engines detected this file		
Engine	Detection	Confidence
Ad-Aware	TrojanDownloader.Worm.Win32.Generic.108...	100%
Alibaba	TrojanDownloader.Worm.Win32.Generic.108...	100%
Arcabit	TrojanDownloader.Worm.Win32.Generic.108...	100%
AVG	Win32/Malware.gen	100%
BitDefender	Gen.TrojanDownloader.Worm.Win32.Generic.108...	100%
ClamAV	Win.Trojan.Agent-275080	100%
CrowdStrike Falcon	win/malicious_confidence_100%_100	100%
Cylance	Unknown	100%
DrWeb	TrojanDownloader.Worm.Win32.Generic.108...	100%
Emsisoft	Gen.TrojanDownloader.Worm.Win32.Generic.108...	100%
eScan	Gen.TrojanDownloader.Worm.Win32.Generic.108...	100%
F-Secure	Trojan.TrojanDownloader.Worm.Win32.Generic.108...	100%
Fortinet	Win32/Generic.ACI.345039	100%
Ikarus	Win32/TrojanDownloader.Worm.Win32.Generic.108...	100%
K7AntiVirus	TrojanDownloader.Worm.Win32.Generic.108...	100%
Kaspersky	HEUR:TrojanDownloader.Worm.Win32.Generic.108...	100%
McAfee	Gen.TrojanDownloader.Worm.Win32.Generic.108...	100%
Microsoft	TrojanDownloader.Worm.Win32.Generic.108...	100%
Avast	Win32/Malware.gen	100%
Avira	Win32/Malware.gen	100%
CAT-QuickHeal	TrojanDownloader.Worm.Win32.Generic.108...	100%
Comodo	Win32/Malware.gen	100%
Cybereason	malicious_confidence_100%_100	100%
Cyren	Win32/Malware.gen	100%
eSantitas	Win32/Malware.gen	100%
Endgame	malicious_confidence_100%_100	100%
F-Prot	Win32/Malware.gen	100%
FreeEye	Gen.TrojanDownloader.Worm.Win32.Generic.108...	100%
GData	Win32/Malware.gen	100%
Jiangmin	TrojanDownloader.Worm.Win32.Generic.108...	100%
K7GW	TrojanDownloader.Worm.Win32.Generic.108...	100%
MAX	Win32/Malware.gen	100%
McAfee-GW-Edit	Gen.TrojanDownloader.Worm.Win32.Generic.108...	100%
NANO-Antivirus	TrojanDownloader.Worm.Win32.Generic.108...	100%

Anti-virus software sellers can get duplicates of files that were hailed by different outputs yet passed by their own engine, to help improve their product and, likewise, Virus Total's own

capacity. Clients can likewise filter suspect URLs and search through the Virus Total dataset. Virus Total for dynamic examination of malware utilizes Cuckoo sandbox.

⇒ **Strings:**

A string in a program is a succession of characters, for example, "banana." A program contains strings in the event that it prints a message, associates with a URL, or duplicates a file to a particular area. Microsoft utilizes the term wide character string to depict its execution of Unicode strings, which shifts marginally from the Unicode guidelines.

```
C:\WINDOWS\system32\cmd.exe
Do not display the startup banner and copyright message.

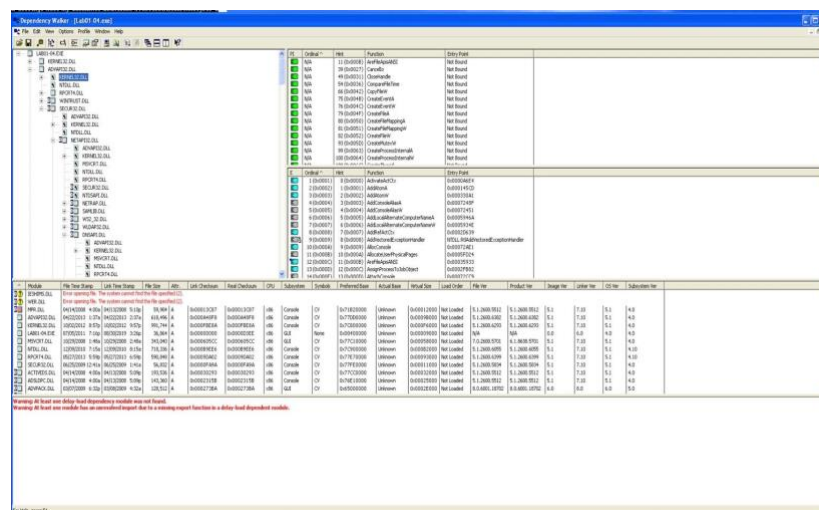
C:\>cd C:\Documents and Settings\Test\My Documents\Downloads\PracticalMalwareAna-
lysis-Labs\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L
C:\Documents and Settings\Test\My Documents\Downloads\PracticalMalwareAnalysis-La-
bs\Practical Malware Analysis Labs\BinaryCollection\Chapter_1L>strings Lab01-04
.exe
Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
Rich
.text
.rdata
.e.data
.rsrc
.o
.s
.coff
.o
.d
.l
.i
.h
.H
.Pj<
.H
.jjj
.h.0e
.h0e
.i
.D
.Jjj
.I
.K
.A
.hL0e
.Qhd0e
.I
.O
.h.L0e
.hp0e
.e
.L
?
.e
.H
.hx0e
.i
.<i
.<i
.<i
.<i
.<i
.<i
.<i
.<i
.I
.K
.I
.S
.V
.U
.e
.Die
.I
.<i
.X
.e
.t
.Hie
.Hie
.Hie
.S01e
.h
.a
'
X
^
>I
CloseHandle
OpenProcess
```

Strings application is utilized to get the lines that are available in malware tests, which could be links, keywords, kind of DLL files, website names, which would give us a thought of what malware expects to do and saving the data and do the ideal activities.

⇒ **Dependency Walker:**

The Dependency Walker tool can help to analyze the dependencies in Windows applications. This can be useful for solving dependency-related problems. Dependency Walker or depends.exe is a free program for Microsoft Windows used to list the imported and sent out functions of a compact executable document. It likewise shows a recursive tree of all the dependencies of the executable document. Dependency Walker was involved in Microsoft Visual Studio until Visual Studio 2005 (Version 8.0) and Windows XP SP2 support tools.



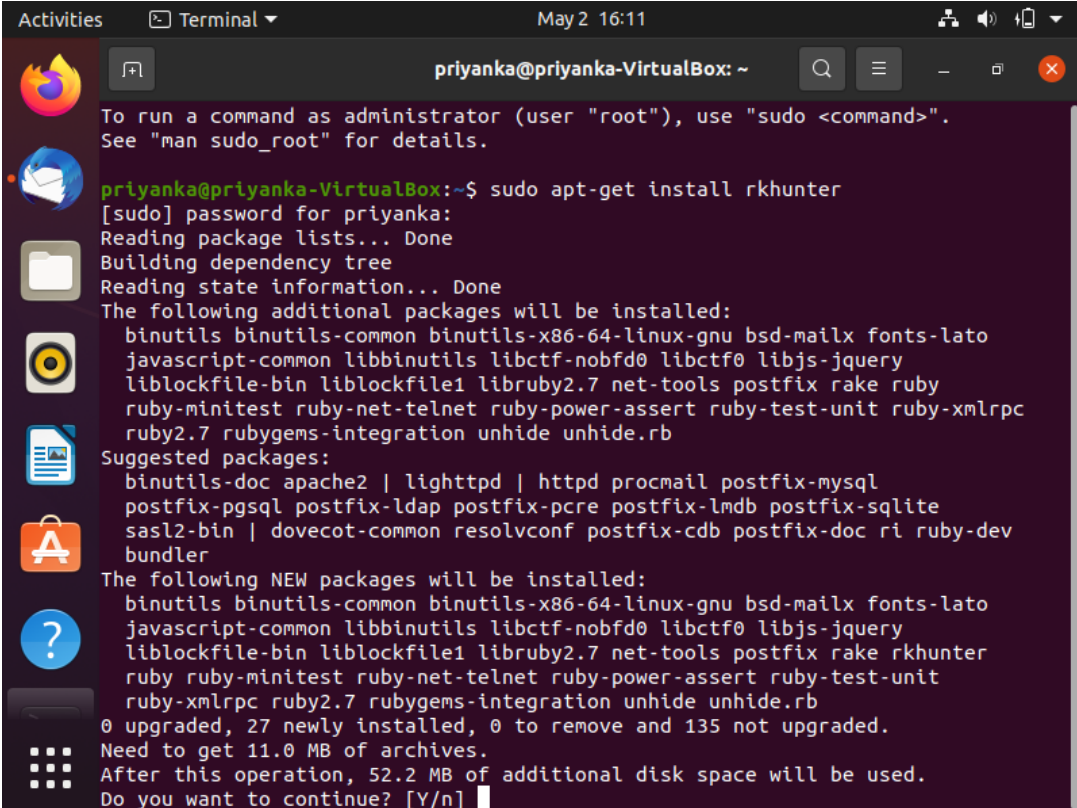
The most recent version v2.2.10011 isn't accessible on dependencywalker.com site yet is involved in the Windows Driver Kit v10. As of Windows 7, Microsoft presented the idea of Windows API-sets, a type of DLL redirection. Dependency Walker has not been refreshed to deal with this layer of indirection nimbly, and when utilized on Windows 7 and later it will probably show numerous mistakes. Dependency Walker can in any case be utilized for some application-level debugging in spite of this. When malware imports a function by ordinal, you can discover what function is being imported by looking into the ordinal worth.

Well, Now let's look at the tools used in Linux.

⇒ **RKhunter:**

Rkhunter (Rootkit Hunter) is an open-source Unix/Linux based scanner tool for Linux systems released under GPL that scans backdoors, rootkits, and local exploits on your systems. It scans hidden files, wrong permissions set on binaries, suspicious strings in the kernel, etc. RKHunter is a Unix-based tool that scans for rootkits, backdoors, and conceivable local exploits. It does this by contrasting SHA-1 hashes of significant documents with known great ones in online databases, looking for default registries of rootkits, wrong consents, covered up records, dubious strings modules and extraordinary tests for Linux and FreeBSD. RKHunter is eminent because of its consideration in famous OS. It is feasible for a bundle manager database to turn out to be noxiously corrupted.

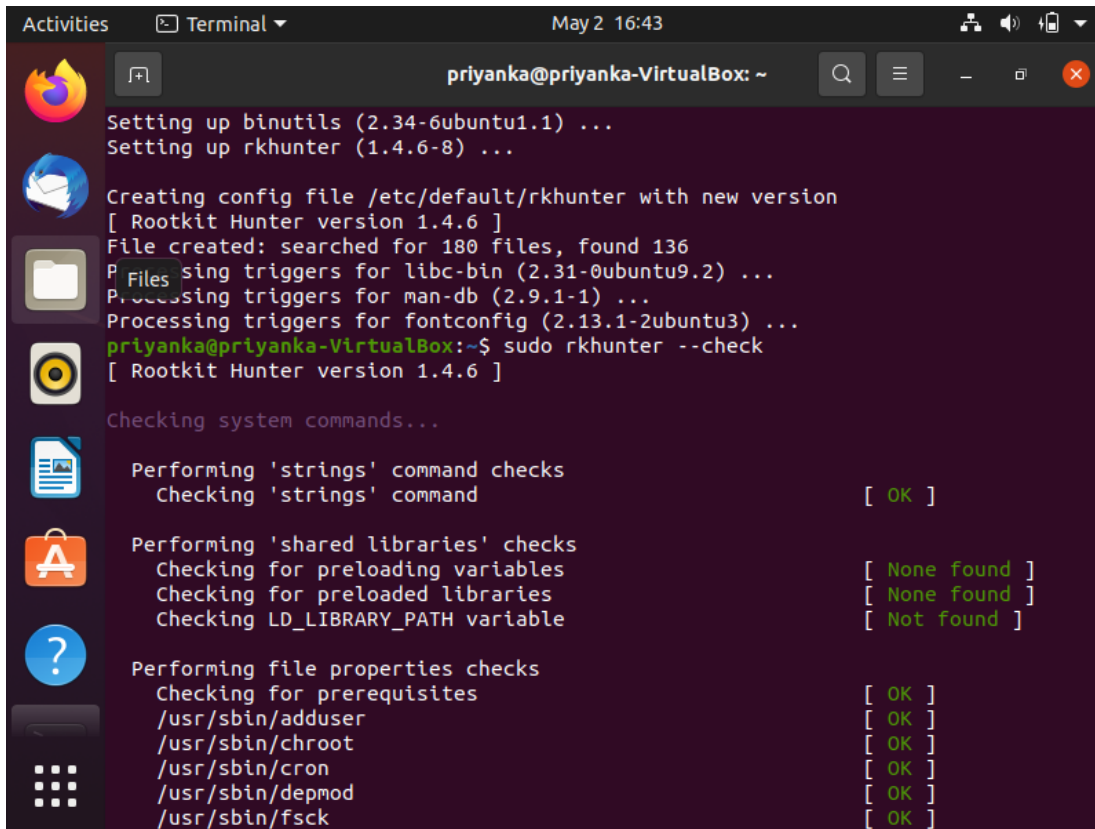
This can be installed utilizing the accompanying:



```
Activities Terminal May 2 16:11
priyanka@priyanka-VirtualBox: ~
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
priyanka@priyanka-VirtualBox:~$ sudo apt-get install rkhunter
[sudo] password for priyanka:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu bsd-mailx fonts-lato
  javascript-common libbinutils libctf-nobfd0 libctf0 libjs-jquery
  liblockfile-bin liblockfile1 libruby2.7 net-tools postfix rake ruby
  ruby-minitest ruby-net-telnet ruby-power-assert ruby-test-unit ruby-xmlrpc
  ruby2.7 rubygems-integration unhide unhide.rb
Suggested packages:
  binutils-doc apache2 | lighttpd | httpd procmail postfix-mysql
  postfix-pgsql postfix-ldap postfix-pcre postfix-lmdb postfix-sqlite
  sasl2-bin | dovecot-common resolvconf postfix-cdb postfix-doc ri ruby-dev
  bundler
The following NEW packages will be installed:
  binutils binutils-common binutils-x86-64-linux-gnu bsd-mailx fonts-lato
  javascript-common libbinutils libctf-nobfd0 libctf0 libjs-jquery
  liblockfile-bin liblockfile1 libruby2.7 net-tools postfix rake rkhunter
  ruby ruby-minitest ruby-net-telnet ruby-power-assert ruby-test-unit
  ruby-xmlrpc ruby2.7 rubygems-integration unhide unhide.rb
0 upgraded, 27 newly installed, 0 to remove and 135 not upgraded.
Need to get 11.0 MB of archives.
After this operation, 52.2 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

RKHunter can just provide details regarding changes, however not on what has caused the change, it is responsive. It will help Rootkit Hunter's clients on the rkhunter-clients mailing list.

We can check the malware as shown in the below image.



The screenshot shows a terminal window titled 'priyanka@priyanka-VirtualBox: ~' with a search icon, menu icon, and window control buttons. The terminal output shows the installation of binutils and rkhunter, followed by the creation of a config file and the execution of rkhunter --check. The checks performed include 'strings' command checks, shared libraries checks, and file properties checks for various system binaries.

```
Setting up binutils (2.34-6ubuntu1.1) ...
Setting up rkhunter (1.4.6-8) ...

Creating config file /etc/default/rkhunter with new version
[ Rootkit Hunter version 1.4.6 ]
File created: searched for 180 files, found 136
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for fontconfig (2.13.1-2ubuntu3) ...
priyanka@priyanka-VirtualBox:~$ sudo 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 [ 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 ]
```

```
Activities Terminal May 2 16:41 priyanka@priyanka-VirtualBox: ~
SHV4 Rootkit [ Not found ]
SHV5 Rootkit [ Not found ]
Sin Rootkit [ Not found ]
Slapper Worm [ Not found ]
Sneakin Rootkit [ Not found ]
'Spanish' Rootkit [ Not found ]
Suckit Rootkit [ Not found ]
Superkit Rootkit [ Not found ]
TBD (Telnet BackDoor) [ Not found ]
TeLeKiT Rootkit [ Not found ]
T0rn Rootkit [ Not found ]
trNkit Rootkit [ Not found ]
Trojanit Kit [ Not found ]
Tuxtendo Rootkit [ Not found ]
URK Rootkit [ Not found ]
Vampire Rootkit [ Not found ]
VcKit Rootkit [ Not found ]
Volc Rootkit [ Not found ]
Xzibit Rootkit [ Not found ]
zaRwT.KiT Rootkit [ Not found ]
ZK Rootkit [ Not found ]

[Press <ENTER> to continue]

Performing additional rootkit checks
Suckit Rootkit additional checks [ OK ]
Checking for possible rootkit files and directories [ None found ]
```

```
Activities Terminal May 2 16:42 priyanka@priyanka-VirtualBox: ~
Checking /dev for suspicious file types [ None found ]
Checking for hidden files and directories [ None found ]

[Press <ENTER> to continue]

System checks summary
=====
File properties checks...
Files checked: 136
Suspect files: 1

Rootkit checks...
Rootkits checked : 477
Possible rootkits: 2

Applications checks...
All checks skipped

The system checks took: 1 minute and 23 seconds

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

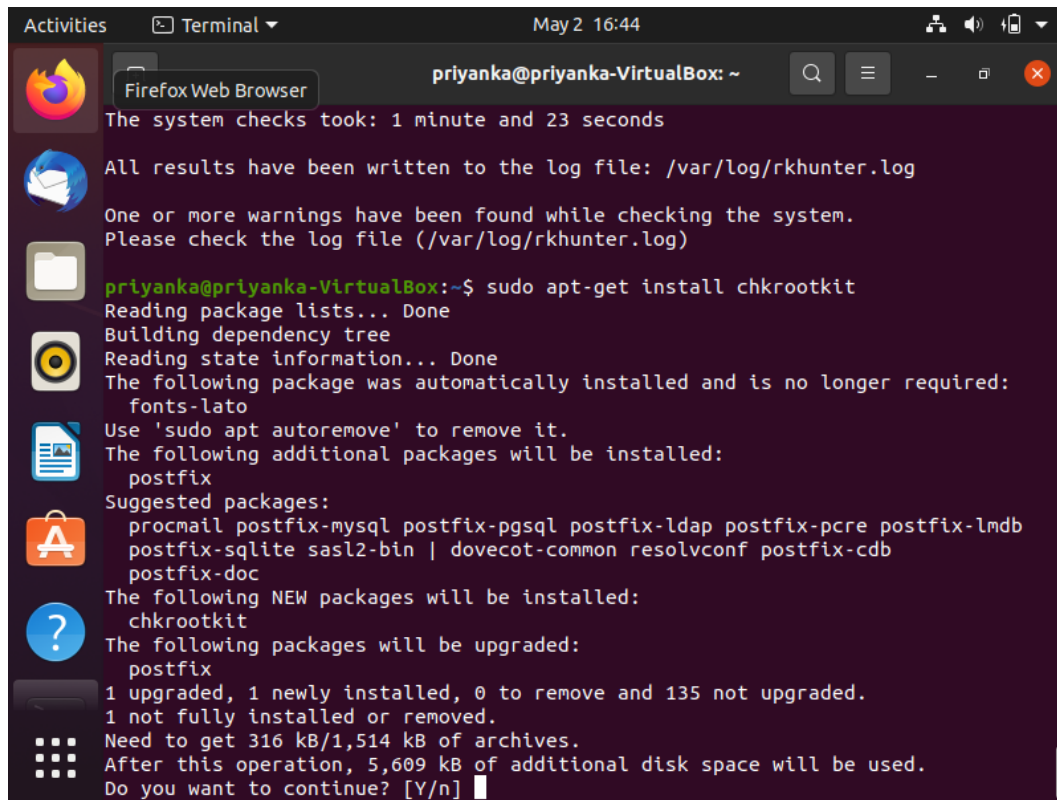
One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)

priyanka@priyanka-VirtualBox:~$
```

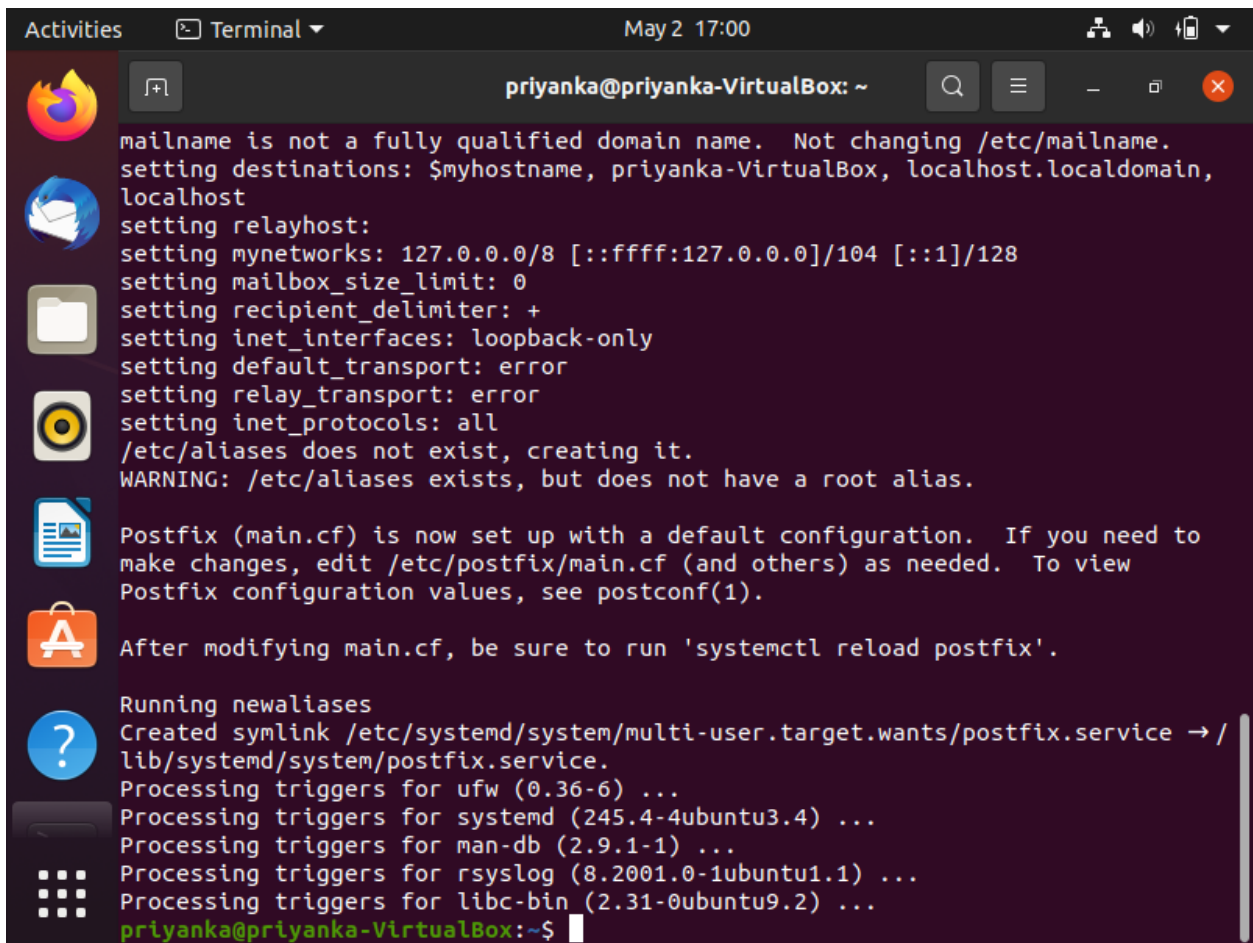

⇒ Chkrootkit:

It is a typical Unix - based program expected to help System administration check their systems for known rootkits. It is a shell script utilizing normal UNIX/Linux tools like the strings and grep commands to look through system programs for signatures and for contrasting a crossing of the/proc filesystem with the yield of the process status order to search for inconsistencies. It very well may be utilized from a rescue disc or it can alternatively utilize another directory from which to run the entirety of its own commands. These methods permit chkrootkit to believe the orders whereupon it depends somewhat more.

This can be installed utilizing the accompanying:



```
Activities Terminal May 2 16:44 priyanka@priyanka-VirtualBox: ~
Firefox Web Browser
The system checks took: 1 minute and 23 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)
priyanka@priyanka-VirtualBox:~$ sudo apt-get install chkrootkit
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  fonts-lato
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  postfix
Suggested packages:
  procmail postfix-mysql postfix-pgsql postfix-ldap postfix-pcre postfix-lmdb
  postfix-sqlite sasl2-bin | dovecot-common resolvconf postfix-cdb
  postfix-doc
The following NEW packages will be installed:
  chkrootkit
The following packages will be upgraded:
  postfix
1 upgraded, 1 newly installed, 0 to remove and 135 not upgraded.
1 not fully installed or removed.
Need to get 316 kB/1,514 kB of archives.
After this operation, 5,609 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```



The image shows a terminal window titled "priyanka@priyanka-VirtualBox: ~" with a search icon, a menu icon, and window control buttons. The terminal output shows the configuration of postfix, including setting destinations, relayhost, mynetworks, mailbox_size_limit, recipient_delimiter, inet_interfaces, default_transport, relay_transport, and inet_protocols. It also shows a warning about /etc/aliases and instructions on how to modify main.cf and run 'systemctl reload postfix'. The prompt is "priyanka@priyanka-VirtualBox:~\$".

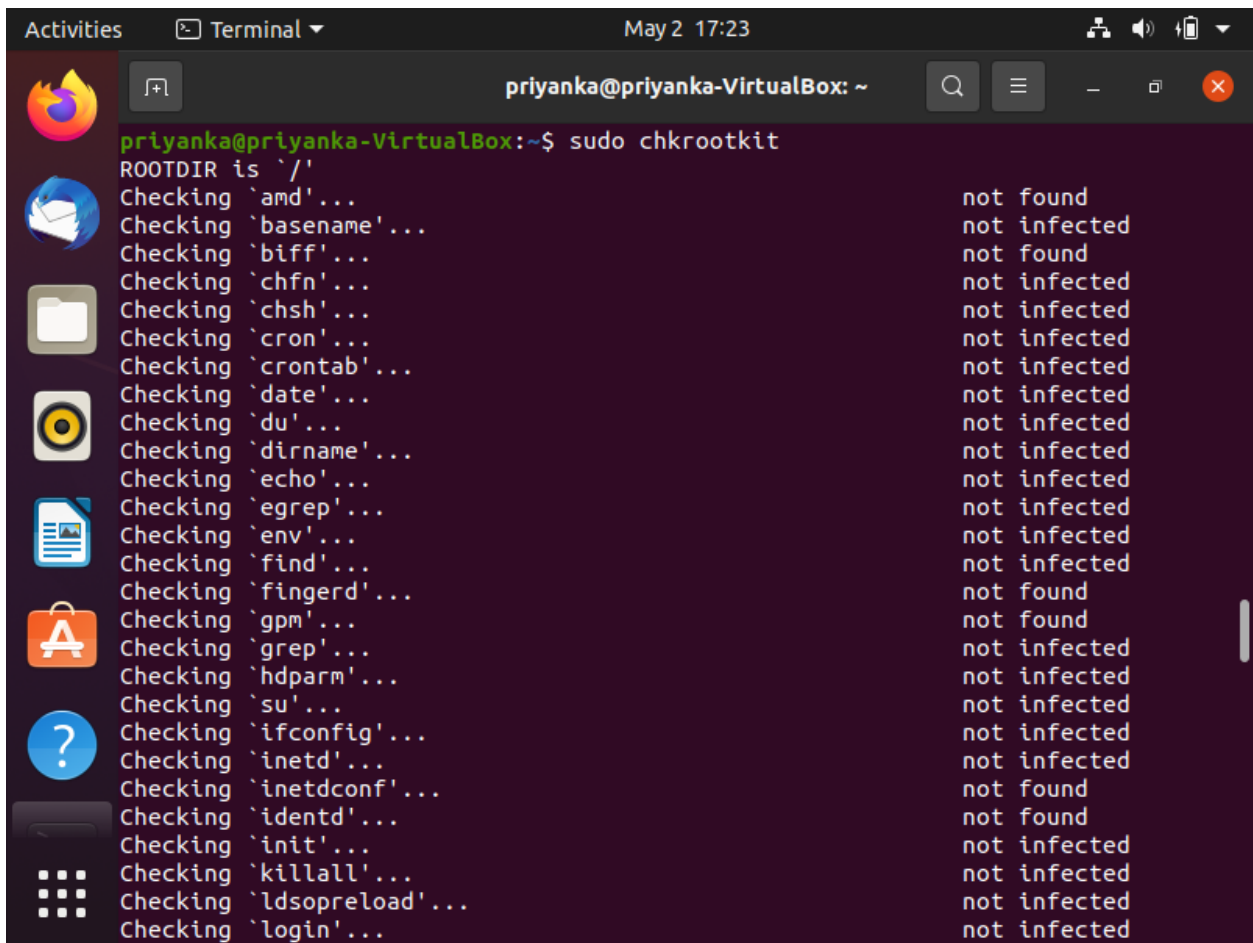
```
mailname is not a fully qualified domain name. Not changing /etc/mailname.
setting destinations: $myhostname, priyanka-VirtualBox, localhost.localdomain,
localhost
setting relayhost:
setting mynetworks: 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
setting mailbox_size_limit: 0
setting recipient_delimiter: +
setting inet_interfaces: loopback-only
setting default_transport: error
setting relay_transport: error
setting inet_protocols: all
/etc/aliases does not exist, creating it.
WARNING: /etc/aliases exists, but does not have a root alias.

Postfix (main.cf) is now set up with a default configuration. If you need to
make changes, edit /etc/postfix/main.cf (and others) as needed. To view
Postfix configuration values, see postconf(1).

After modifying main.cf, be sure to run 'systemctl reload postfix'.

Running newaliases
Created symlink /etc/systemd/system/multi-user.target.wants/postfix.service → /
lib/systemd/system/postfix.service.
Processing triggers for ufw (0.36-6) ...
Processing triggers for systemd (245.4-4ubuntu3.4) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for rsyslog (8.2001.0-1ubuntu1.1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
priyanka@priyanka-VirtualBox:~$
```

The below command is used to run chkrootkit.

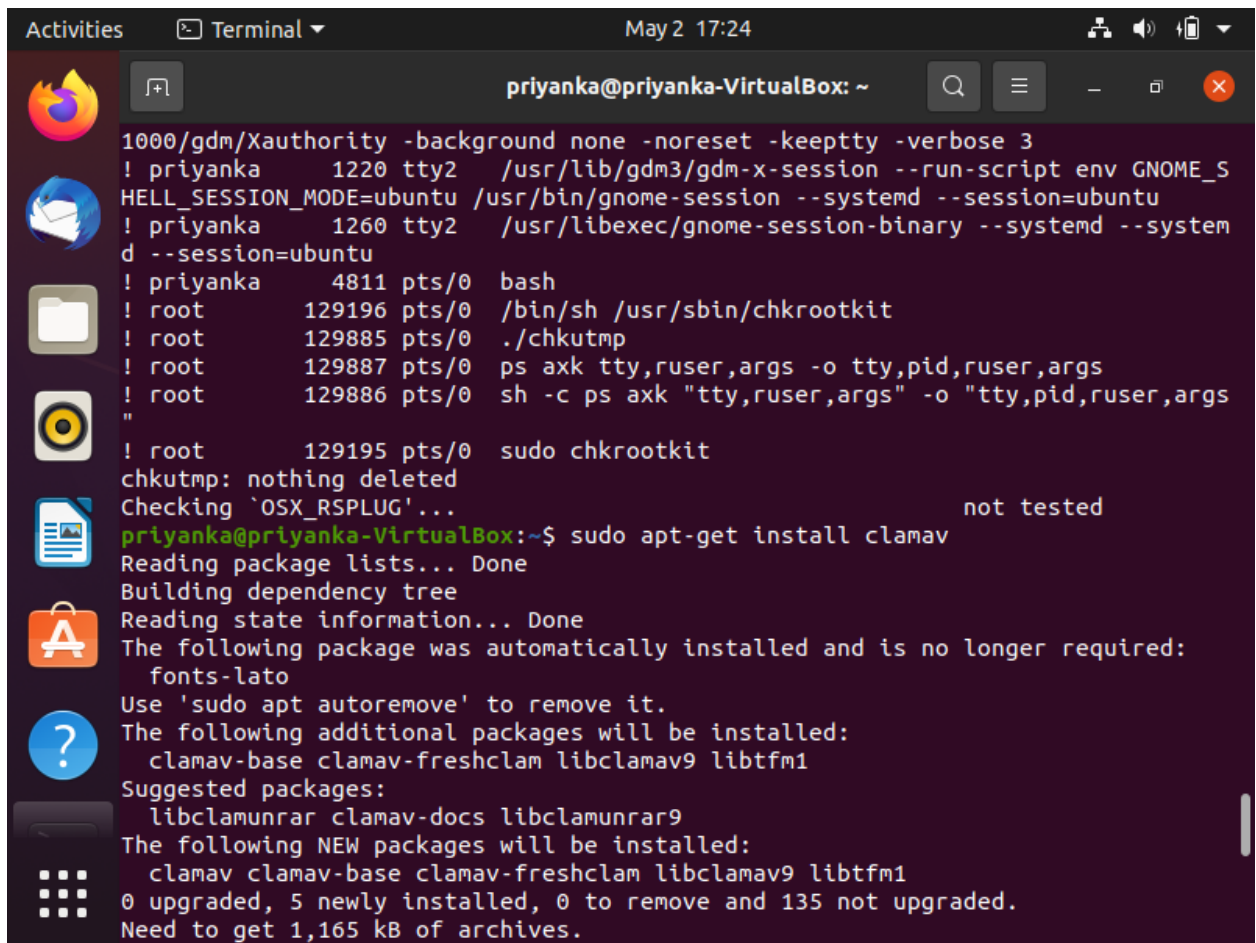


```
priyanka@priyanka-VirtualBox:~$ sudo chkrootkit
ROOTDIR is '/'
Checking `amd'... not found
Checking `basename'... not infected
Checking `biff'... not found
Checking `chfn'... not infected
Checking `chsh'... not infected
Checking `cron'... not infected
Checking `crontab'... not infected
Checking `date'... not infected
Checking `du'... not infected
Checking `dirname'... not infected
Checking `echo'... not infected
Checking `egrep'... not infected
Checking `env'... not infected
Checking `find'... not infected
Checking `fingerd'... not found
Checking `gpm'... not found
Checking `grep'... not infected
Checking `hdparm'... not infected
Checking `su'... not infected
Checking `ifconfig'... not infected
Checking `inetd'... not infected
Checking `inetdconf'... not found
Checking `identd'... not found
Checking `init'... not infected
Checking `killall'... not infected
Checking `ldsopreload'... not infected
Checking `login'... not infected
```

⇒ **ClamAV:**

Clam AntiVirus is an open source (GPL) anti-virus engine used in a variety of situations including email scanning, web scanning, and end point security. ClamAV is a free, cross-platform and open-source anti-virus software toolkit that is able to detect many types of malicious software, including viruses. Clam AV includes a number of utilities: a command-line scanner, automatic database updater and a scalable multi-threaded daemon, running on an anti-virus engine from a shared library. It provides several utilities including a flexible and scalable multi-threaded daemon, a command line scanner and an advanced tool for automatic database updates.

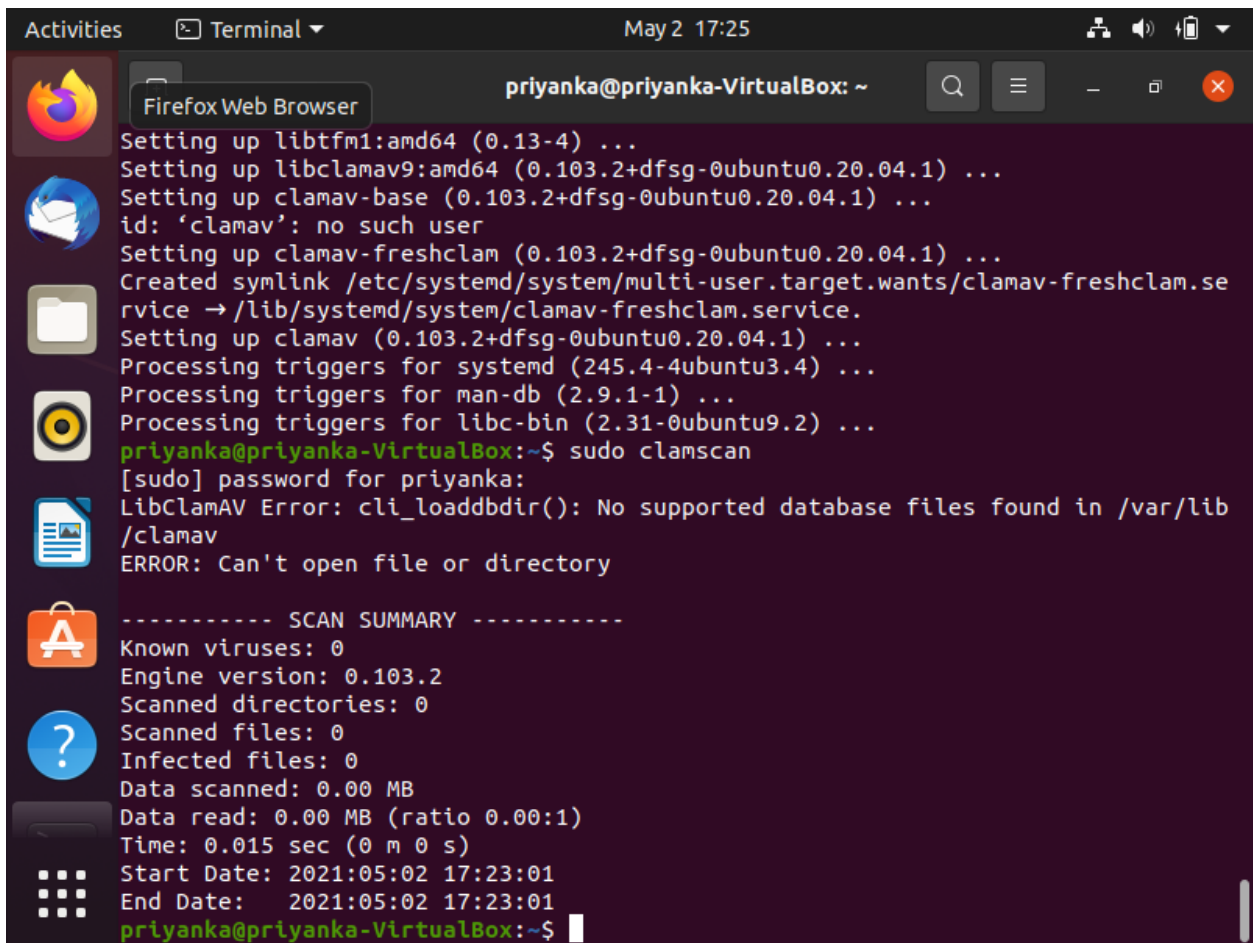
The below screenshot shows the installation of ClamAV.



The image shows a terminal window titled 'priyanka@priyanka-VirtualBox: ~' with a search icon, a menu icon, and window control buttons. The terminal output displays system boot logs, including GDM sessions and login attempts. It then shows the execution of 'sudo apt-get install clamav', which lists dependencies, suggests additional packages, and shows the final installation status: 0 upgraded, 5 newly installed, 0 to remove, and 135 not upgraded, requiring 1,165 kB of archives.

```
1000/gdm/Xauthority -background none -noreset -keeptty -verbose 3
! priyanka 1220 tty2 /usr/lib/gdm3/gdm-x-session --run-script env GNOME_S
HELL_SESSION_MODE=ubuntu /usr/bin/gnome-session --systemd --session=ubuntu
! priyanka 1260 tty2 /usr/libexec/gnome-session-binary --systemd --system
d --session=ubuntu
! priyanka 4811 pts/0 bash
! root 129196 pts/0 /bin/sh /usr/sbin/chkrootkit
! root 129885 pts/0 ./chkutmp
! root 129887 pts/0 ps axk tty,ruser,args -o tty,pid,ruser,args
! root 129886 pts/0 sh -c ps axk "tty,ruser,args" -o "tty,pid,ruser,args"
"
! root 129195 pts/0 sudo chkrootkit
chkutmp: nothing deleted
Checking `OSX_RSPLUG'... not tested
priyanka@priyanka-VirtualBox:~$ sudo apt-get install clamav
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
 fonts-lato
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
 clamav-base clamav-freshclam libclamav9 libtftm1
Suggested packages:
 libclamunrar clamav-docs libclamunrar9
The following NEW packages will be installed:
 clamav clamav-base clamav-freshclam libclamav9 libtftm1
0 upgraded, 5 newly installed, 0 to remove and 135 not upgraded.
Need to get 1,165 kB of archives.
```

The below command is used to run ClamAV.



```
Activities Terminal May 2 17:25 priyanka@priyanka-VirtualBox: ~
Setting up libtftm1:amd64 (0.13-4) ...
Setting up libclamav9:amd64 (0.103.2+dfsg-0ubuntu0.20.04.1) ...
Setting up clamav-base (0.103.2+dfsg-0ubuntu0.20.04.1) ...
id: 'clamav': no such user
Setting up clamav-freshclam (0.103.2+dfsg-0ubuntu0.20.04.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/clamav-freshclam.service → /lib/systemd/system/clamav-freshclam.service.
Setting up clamav (0.103.2+dfsg-0ubuntu0.20.04.1) ...
Processing triggers for systemd (245.4-4ubuntu3.4) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
priyanka@priyanka-VirtualBox:~$ sudo clamscan
[sudo] password for priyanka:
LibClamAV Error: cli_loaddbdir(): No supported database files found in /var/lib/clamav
ERROR: Can't open file or directory

----- SCAN SUMMARY -----
Known viruses: 0
Engine version: 0.103.2
Scanned directories: 0
Scanned files: 0
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 0.015 sec (0 m 0 s)
Start Date: 2021:05:02 17:23:01
End Date: 2021:05:02 17:23:01
priyanka@priyanka-VirtualBox:~$
```

References:

<https://en.wikipedia.org/wiki/Rkhunter>

http://venom630.free.fr/pdf/Practical_Malware_Analysis.pdf