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

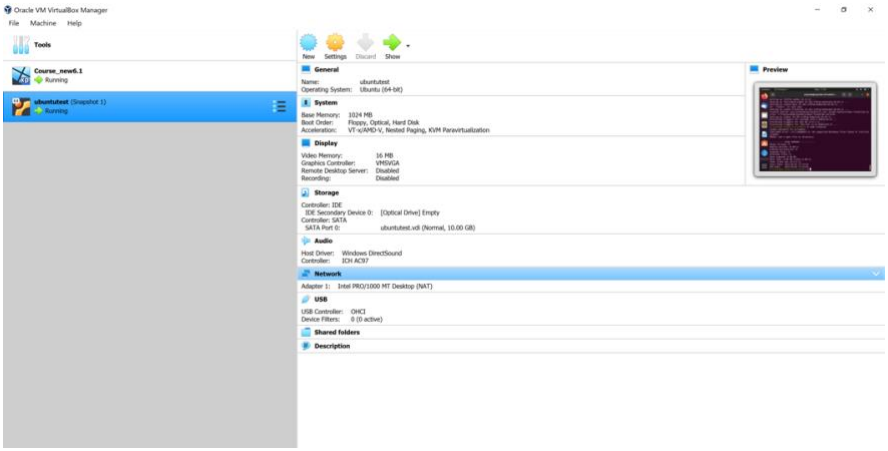
- RKhunter
- chkrootkit
- clamAV

Now, lets 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.

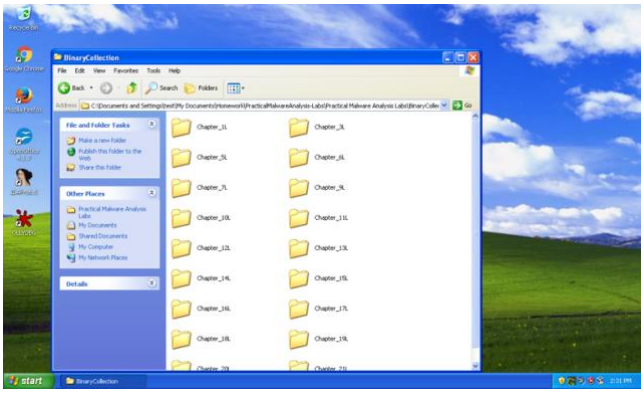
The strategies and highlights that Oracle VM VirtualBox gives are valuable since it assists us with running multiple operating systems in our current PC simultaneously. For instance, we can run Linux on our Windows system or run Windows and Linux on our Mac system. It also helps for installing the software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



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

⇒ **<u>Hashing:</u>**

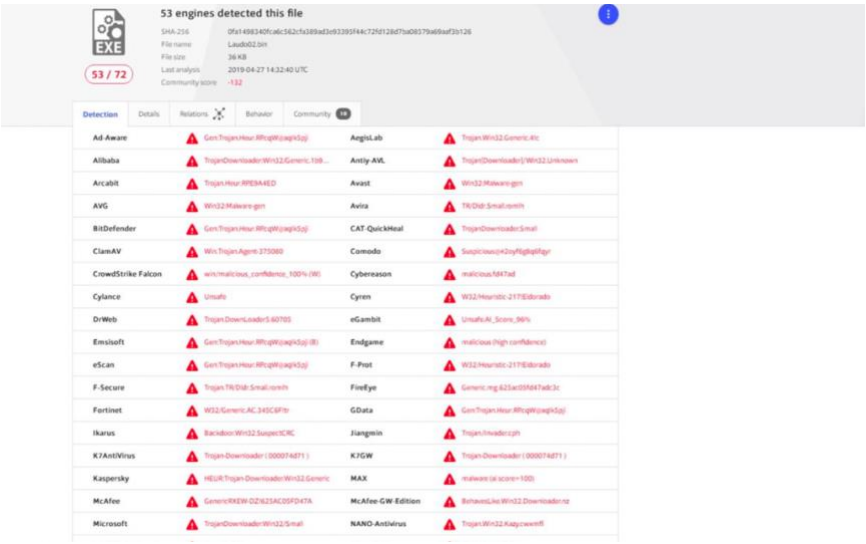
One of the most important method to refer to a malware is through its HASH value. A HASH value is a numeric value of a fixed length that uniquely identifies data. Hashing is a software process of creating fixed character length hash values for a text document. This is a single-way function meaning the 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.

⇒ **<u>Virus Total:</u>**

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).

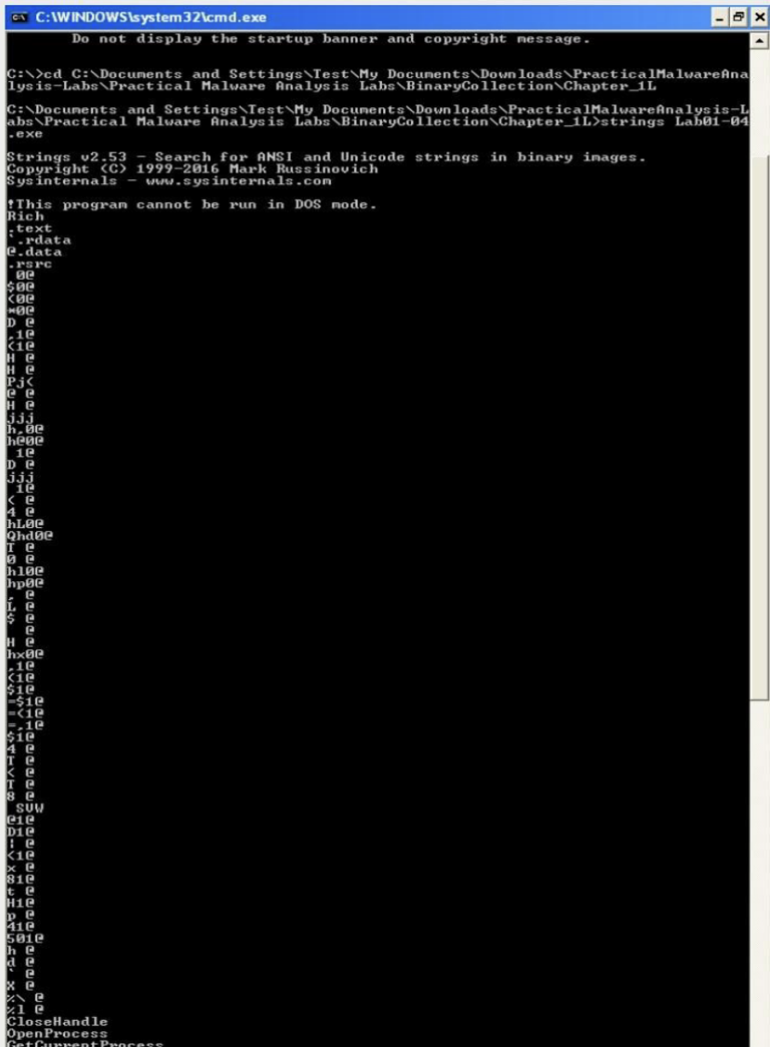


Anti-virus software sellers can get duplicates of files that were hailed by different outputs yet passed by their own engine, to help improve their product and, likewise, Virus Total's own

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:**

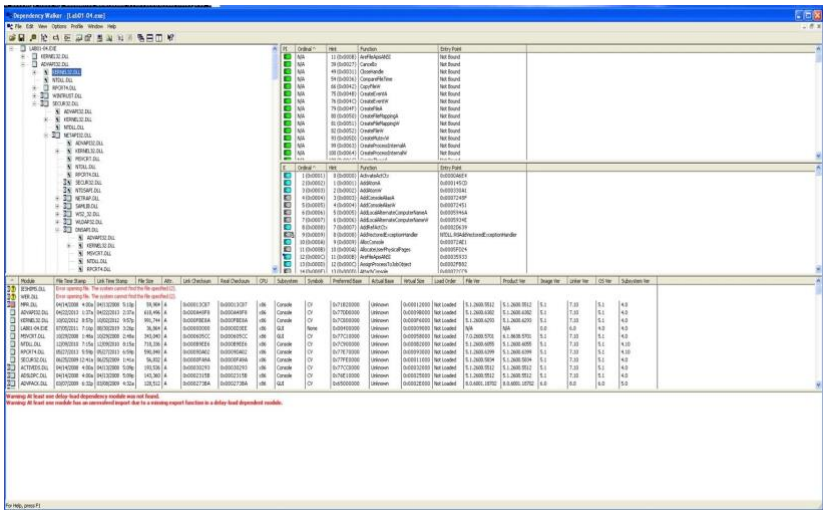
A string in a program is a succession of characters, for example, "banana." A program contains strings in the event that it prints a message, associates with a URL, or duplicates a file to a particular area. Microsoft utilizes the term wide character string to depict its execution of Unicode strings,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



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.



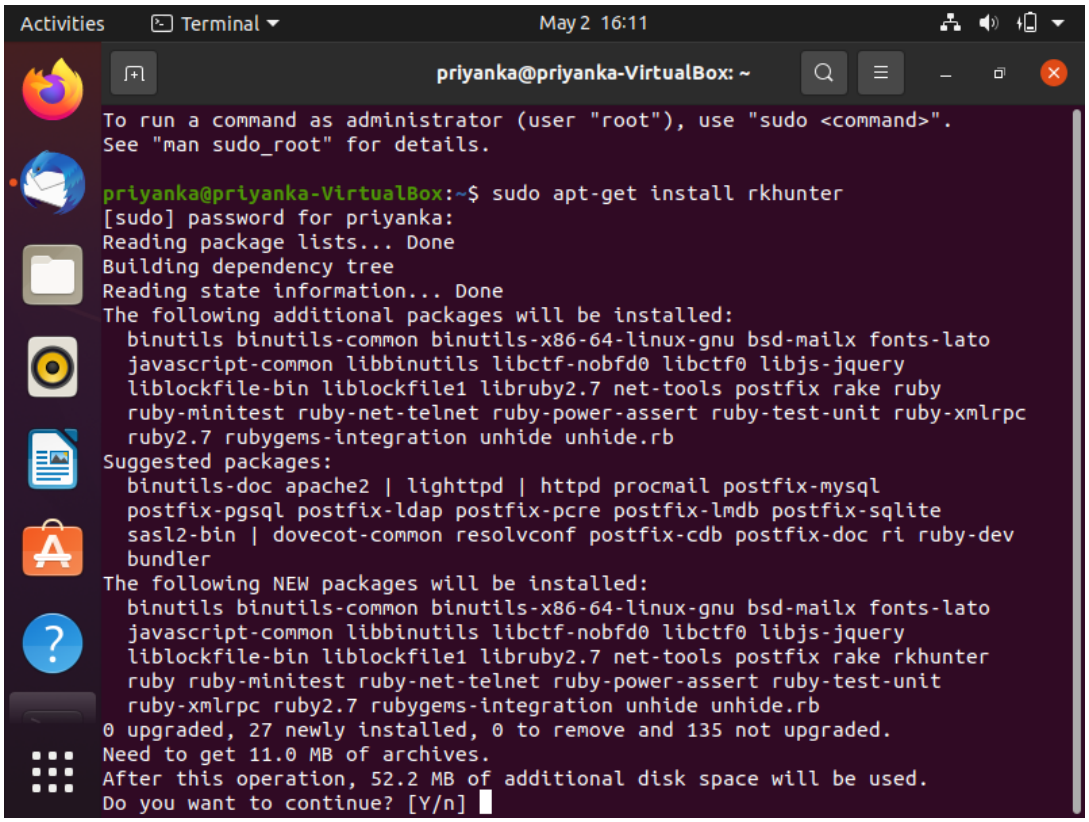
The most recent version v2.2.10011 isn't accessible on dependencywalker.com site yet is involved in the Windows Driver Kit v10. As of Windows 7, Microsoft presented the idea of Windows API-sets, a type of DLL redirection. Dependency Walker has not been refreshed to deal with this layer of indirection 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:**

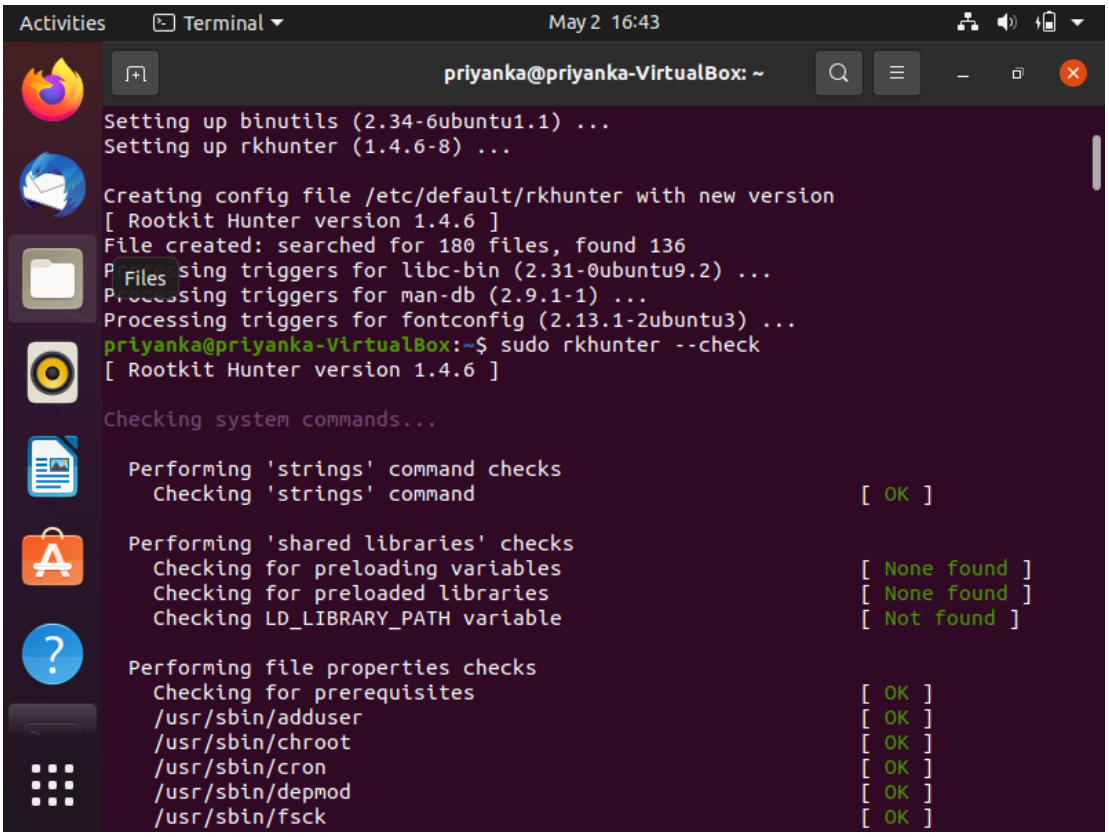
Rkhunter (Rootkit Hunter) is an open-source Unix/Linux based scanner tool for Linux systems released under GPL that scans backdoors, rootkits, and local exploits on your systems. It scans hidden files, wrong permissions set on binaries, suspicious strings in the kernel, etc. RKhunter is a Unix-based 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:



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.



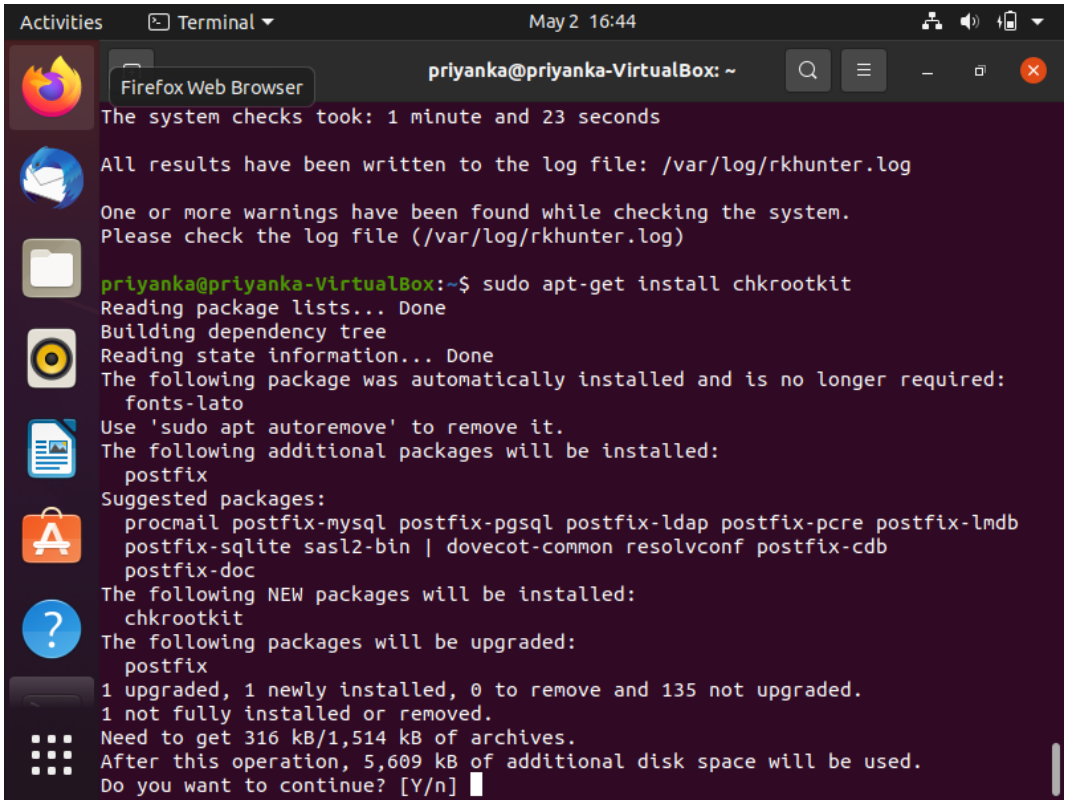
```
Activities   Terminal   May 2  16:41
priyanka@priyanka-VirtualBox: ~
    SHV4 Rootkit                                          [ Not found ]
    SHV5 Rootkit                                          [ Not found ]
    Sin Rootkit                                           [ Not found ]
    Slapper 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 ]
```

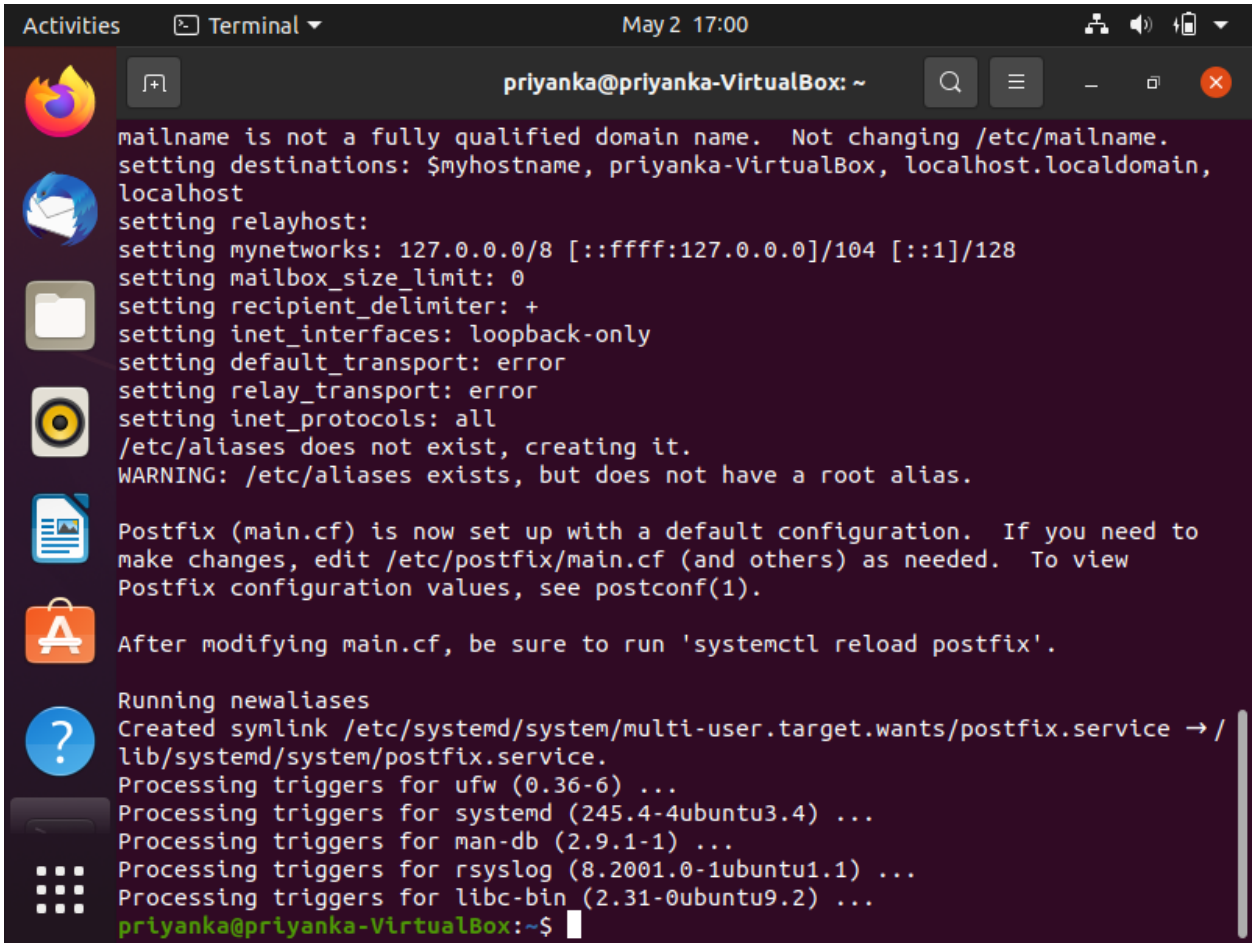
```
Activities   Terminal   May 2  16:42
priyanka@priyanka-VirtualBox: ~
    Checking /dev for suspicious file types               [ None found ]
    Checking for hidden files and directories             [ None found ]

[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:**

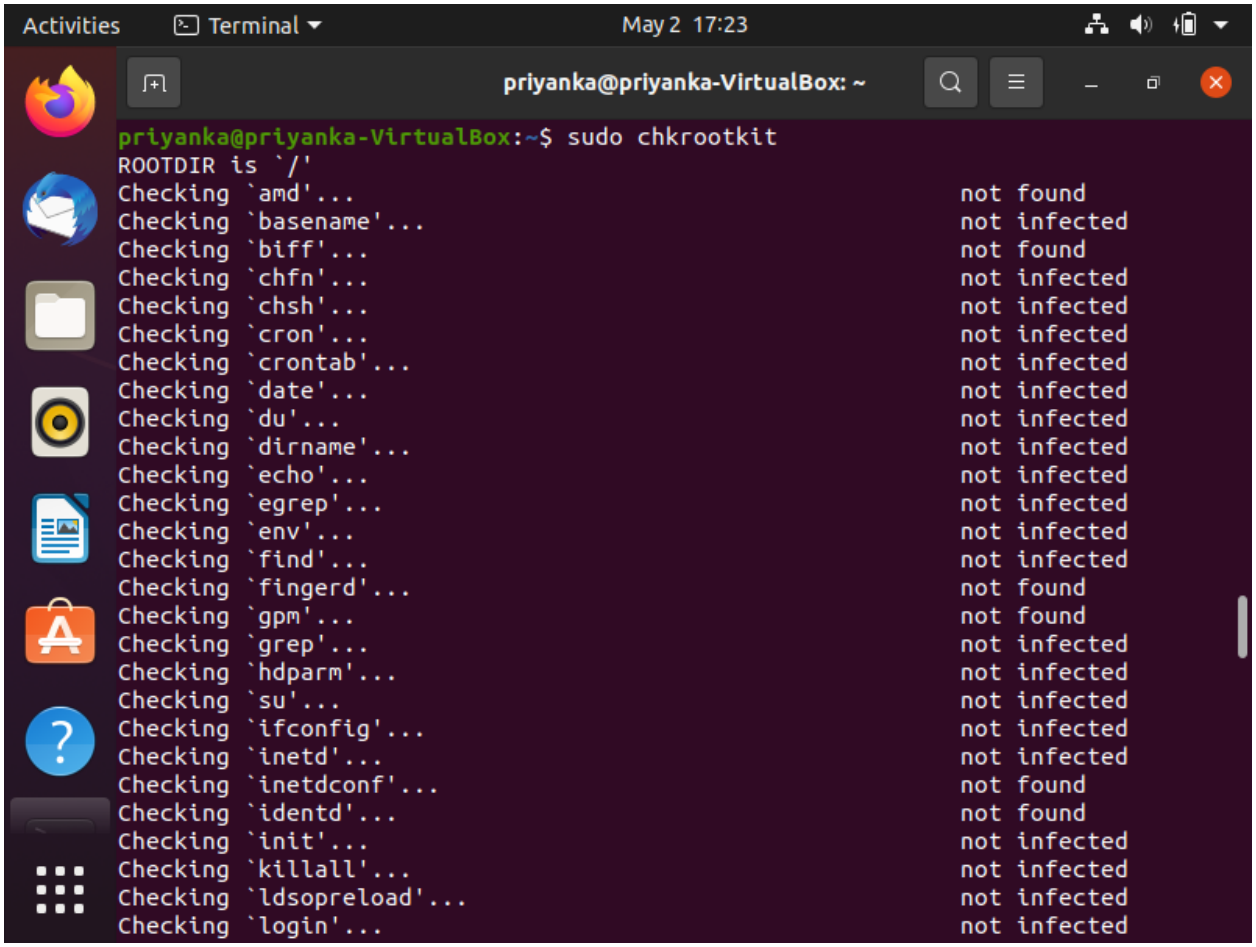
It is a typical Unix - based program expected to help System admintration check their systems for known rootkits. It is a sheel script utilizing normal UNIX/Linux tools like the strings and grep commands to look through center system programs for signatures and for contrasting a crossing of the/proc 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:





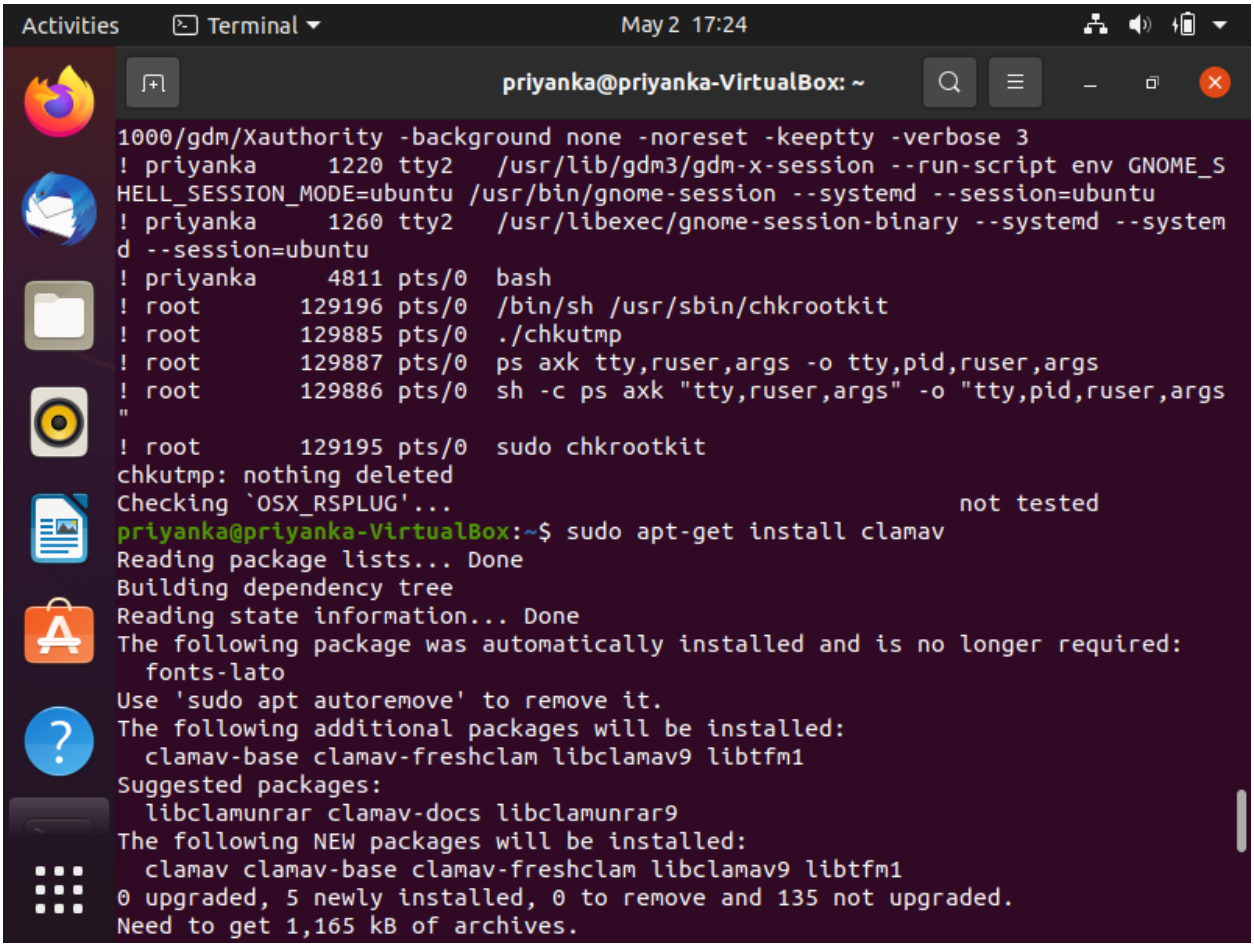
The below command is used to run chkrootkit.



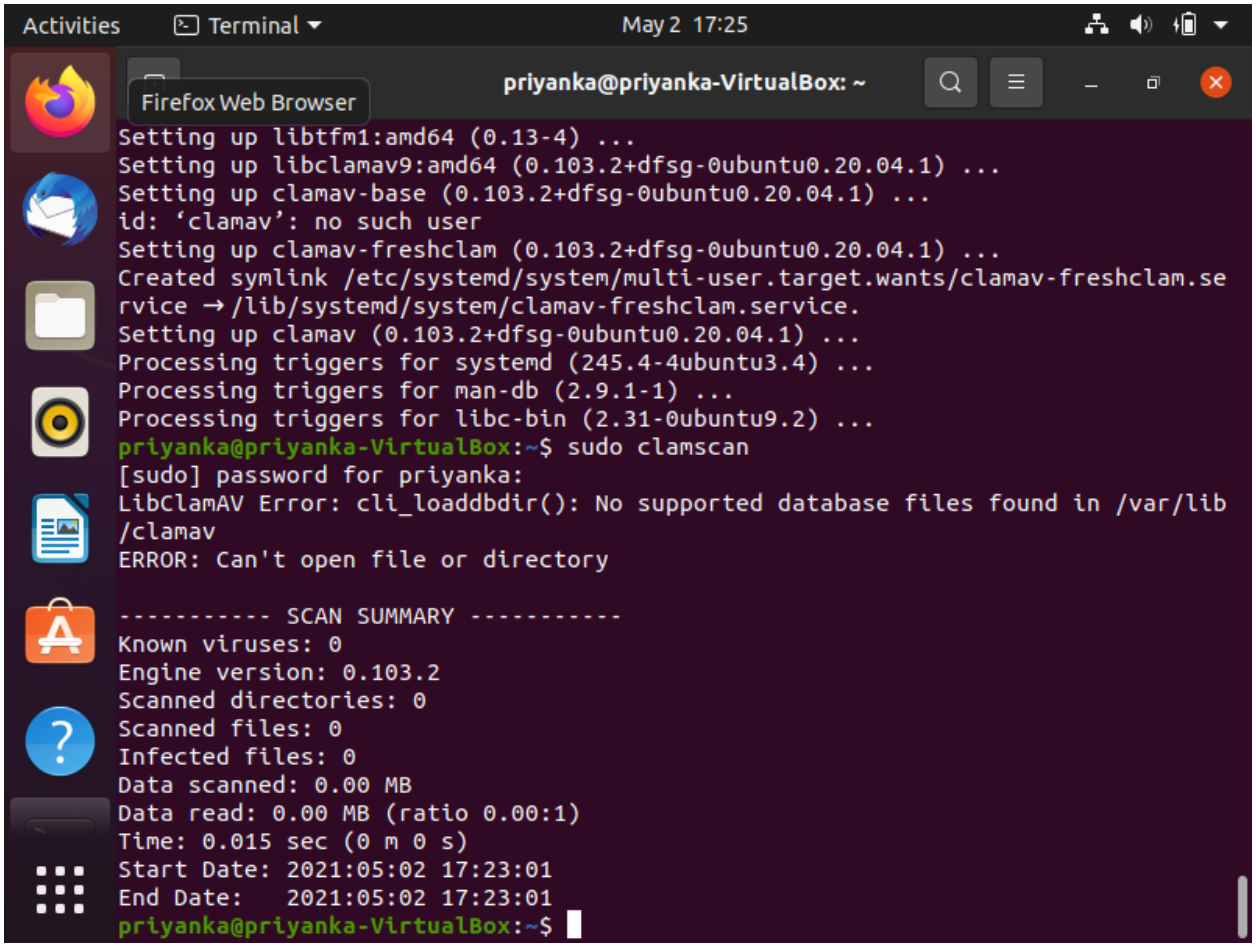
⇒ **ClamAV:**

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 below command is used to run ClamAV.



References:

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

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