Detecting & Preventing from Keyloggers

Keyloggers are activity-monitoring software programs that give hackers access to your personal data. The passwords and credit card numbers you type, the webpages you visit – all by logging your keyboard strokes. The software is installed on your computer and records everything you type. Then it sends this log file to a server, where cybercriminals wait to make use of all this sensitive information.

Types of Keyloggers

- **Hardware Keylogger:** Devices that can be attached in our computer will act as keylogger and collects information about specified target.
- **Software Keylogger:** Probably a malicious program that does not infect your system but still can steal your passwords, account details etc.

Users may be tricked into downloading and installing keyloggers by a variety of social engineering techniques, such as Web Page Scripts, Phishing, unsolicited/spam mails containing attachments that have malware embedded in them.

Once such emails are opened and attachments activated the malware gets discreetly downloaded and installed on your device. The malware could be a keylogger that captures and sends all the keyboard taps to the fraudsters, which includes your account passwords and other sensitive data.

Affected machines with this vulnerability:

Linux Devices, Windows Devices, Android Devices

In this exercise, you will learn about the Keylogger, how it works, and its potential impact on a victim's device. You will simulate the installation of a Keylogger application and observe its behavior, such as recording keystrokes. Additionally, you will explore mitigation and prevention techniques to protect against Keylogger applications and other types of malware. Through this exercise, you will gain a better understanding of the risks posed by keylogger applications and how to protect against them.

Indicator of Attack (IOA)

Indicators of attack(IOAs) are some events that could reveal an active attack before indicators of compromise become visible. It is not always possible to detect Indicators of attack, as the attackers generally target your machines when you are not available with them. IOAs disclose the motivations of the attacker and the specific tools used in each process.

Examples of Indicators of Attacks(IOA)

A. You may notice that your computer is unusually slow or unstable. This is usually a sign of malicious software running in the background.

B. You might also find that your keyboard is typing the wrong characters or keys are not working properly.

C. Another sign is if you notice any strange software installed on your device that you don't remember downloading.
D. You could also receive suspicious pop-up windows on your screen that you don't recognize.
E. You might notice that your online accounts have been accessed without your knowledge, which could be a sign of keyloggers or another compromise.

Indicators of Compromise (IOCs)

Indicators of Compromise (IOC) are pieces of forensic data, such as data found in host-based log entries or files, that identify potentially malicious activity on an application. An IOC is an indication that can be used to indicate an intrusion or compromise of a machine.

IOC can reveal:

A. **Clipboard logging:** Anything duplicated to the clipboard is caught.
B. **Screen logging:** Randomly coordinated screen captures of your PC are logged.
C. **Control text capture:** The Windows API allows for programs to request the text value of some controls, it means a password can still be captured albeit it is behind a password mask.
D. **Activity tracking:** Recording of which programs, folders, and windows are opened and also the screenshots of every.
E. Recording of program queries, instant message conversations, FTP downloads alongside the other internet activities.

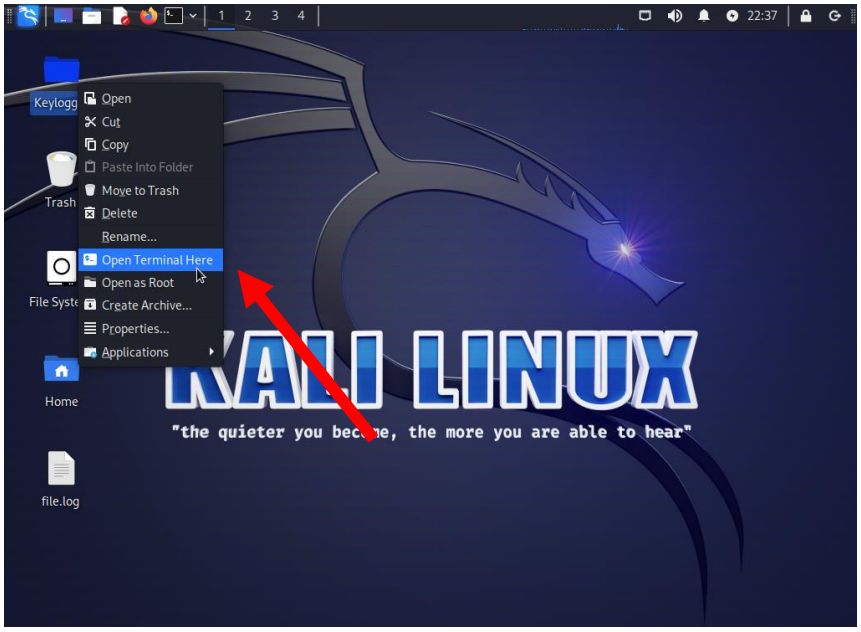
Guided Exercise

Step to Perform Phishing Attack

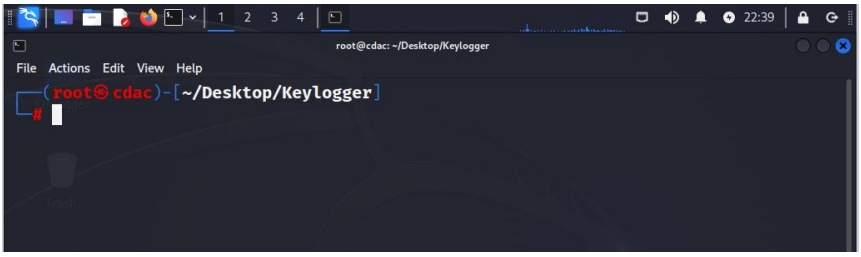
1. Connect to the kali Linux machine, created by you, using the RDP protocol. Kali Linux machine is being used as Attacker's machine.
2. When prompted for the username and password, enter **root** as username and **toor** as password. The root is the administrator user of the machine.

Once you successfully login, you will see a screen like this

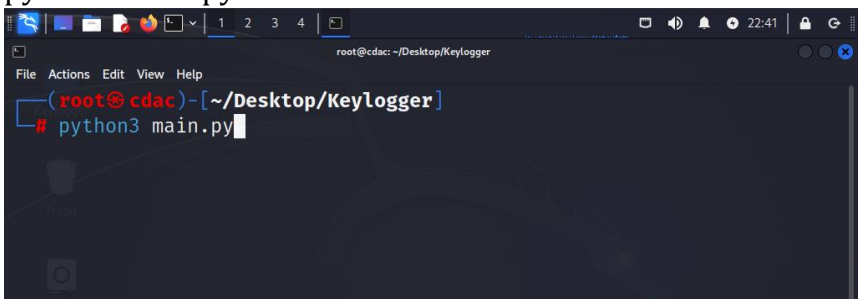
3. Here you can see on Application named as Keylogger, Right click on it and click on Open Terminal Here option



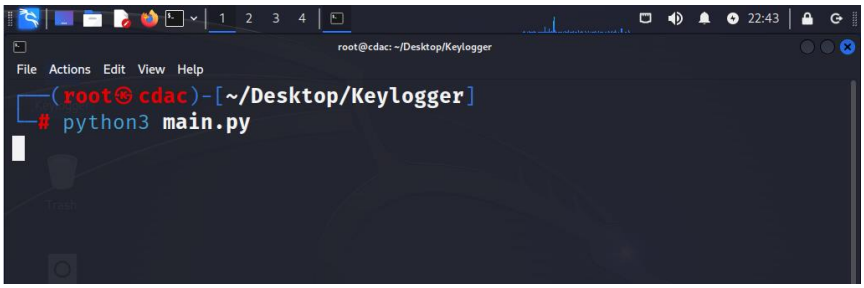
Now you will enter into the terminal



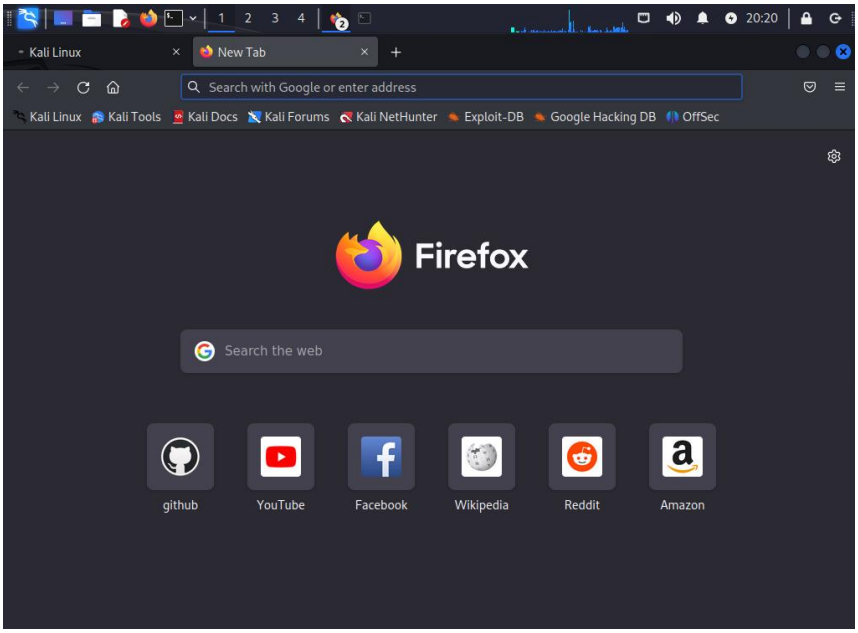
4. Now enter this command to run the Keylogger
   python3 main.py



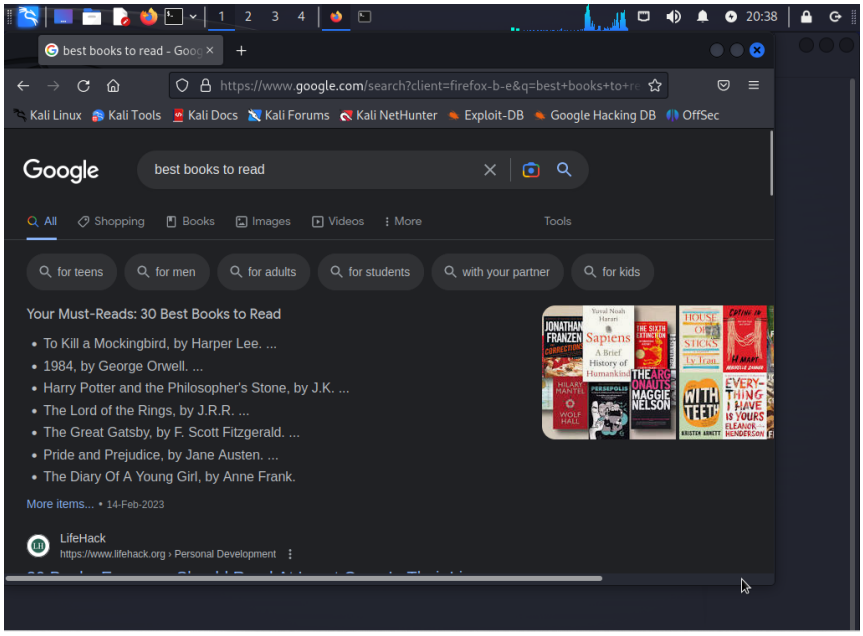
Keylogger has successfully activated in the machine



5. Now victim will open the browser of the machine and search for anything. Victim has no idea that the machine is infected with keylogger



Here victim is searching: **best books to read**



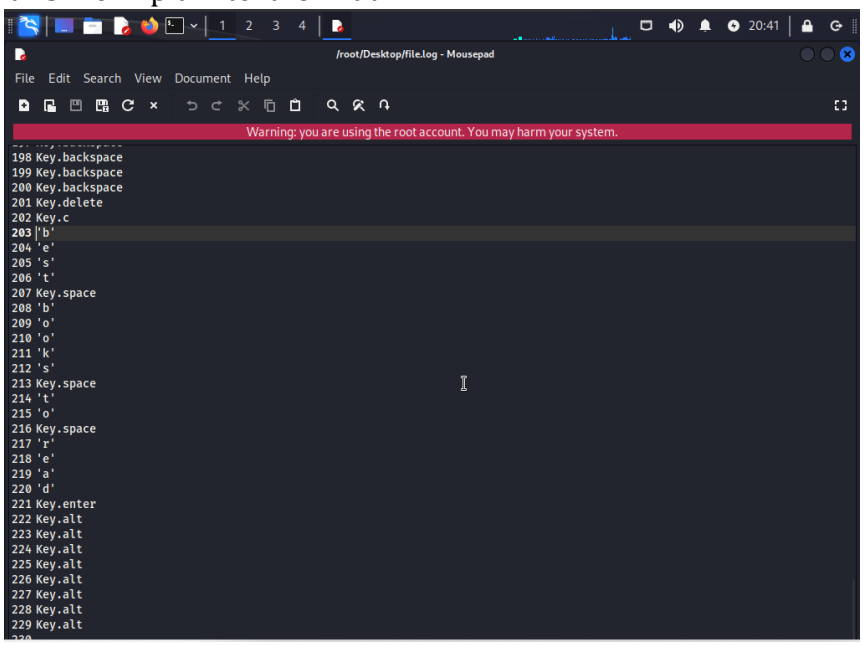
6. While a victim is busy in accessing the browser on the other hand hacker can see all the activities of the victim which is going on in the browser.

   Once the victim starts accessing the browser, Hacker will open the text file to check what keystrokes the victim is pressing and hence victim's credentials and sensitive information are stored in plain text files due to the installation of the keylogger in the machine.

   To open the file, go to the desktop here you can see one file **file.log**

   Double-click it to open it

And Here you can see whatever victim has typed in the browser everything is stored in this file in plain text format.



Similarly, if the victim will open the browser to login into his banking website, his username, and password of the bank will be stored in plain text format and the hacker will use those credentials to steal money and perform different cyber crimes.

Defense from Keylogger

How does a Keylogger get into your computer

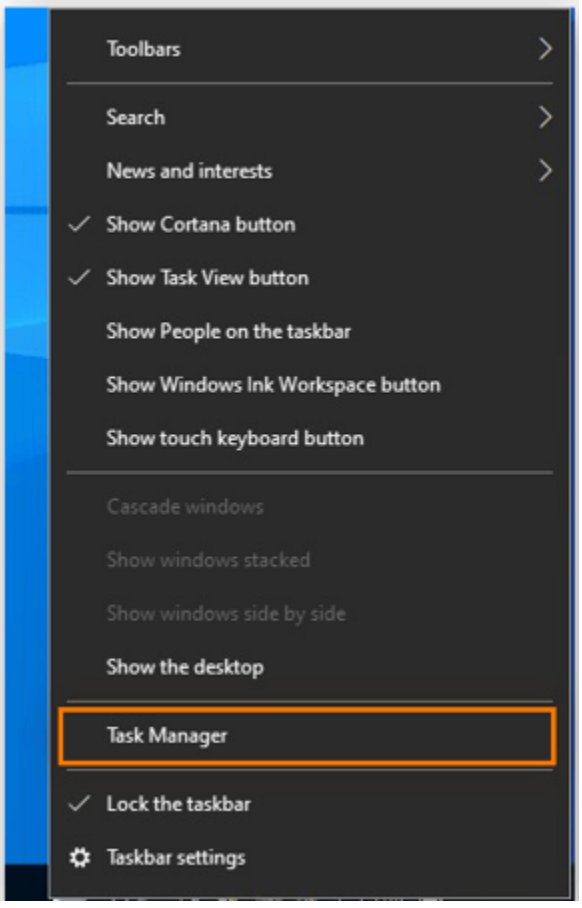
A keylogger can be installed on your computer in number of ways. Anyone with access to your computer could install it; keyloggers could come as a component part of a virus or from any application installation, despite how deceptively innocent it may look. This is part of the reason why you should always be sure you're downloading files from a trusted resource.

Steps to detect Keylogger in Windows Machine

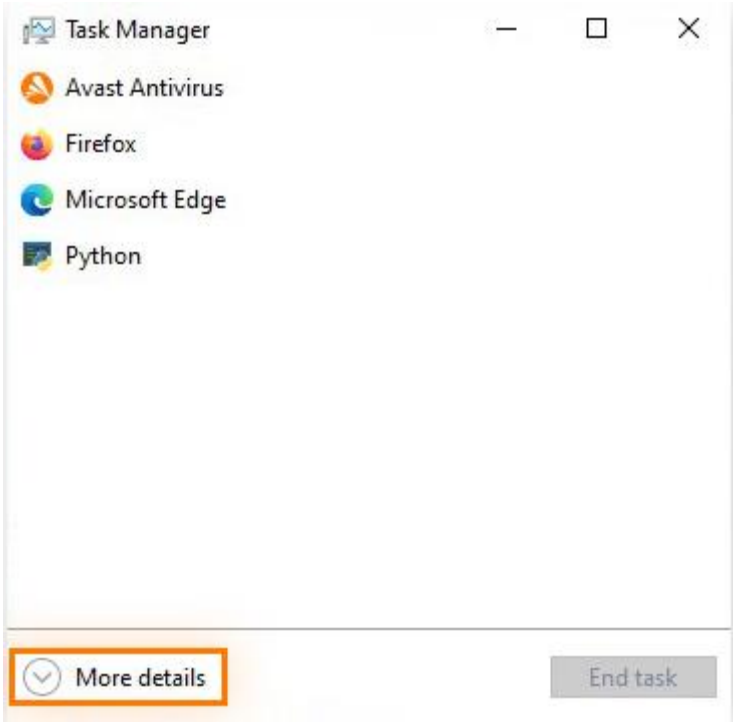
1. **Use the Task Manager**
   Task Manager is a quick way to check your computer for a keylogger. It's a utility program on PCs that shows you which applications and background processes are running (on Mac, use the Activity Monitor).

Follow these steps to check for a keylogger program on your PC.

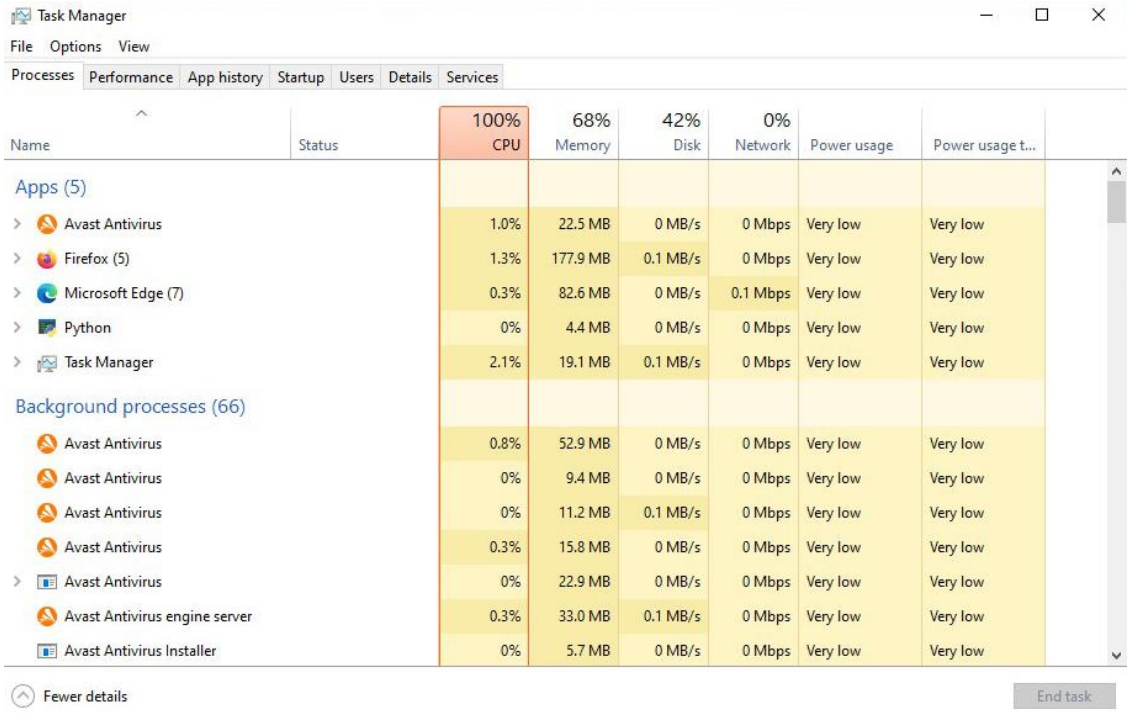
a) Right-click the taskbar and select **Task Manager**.



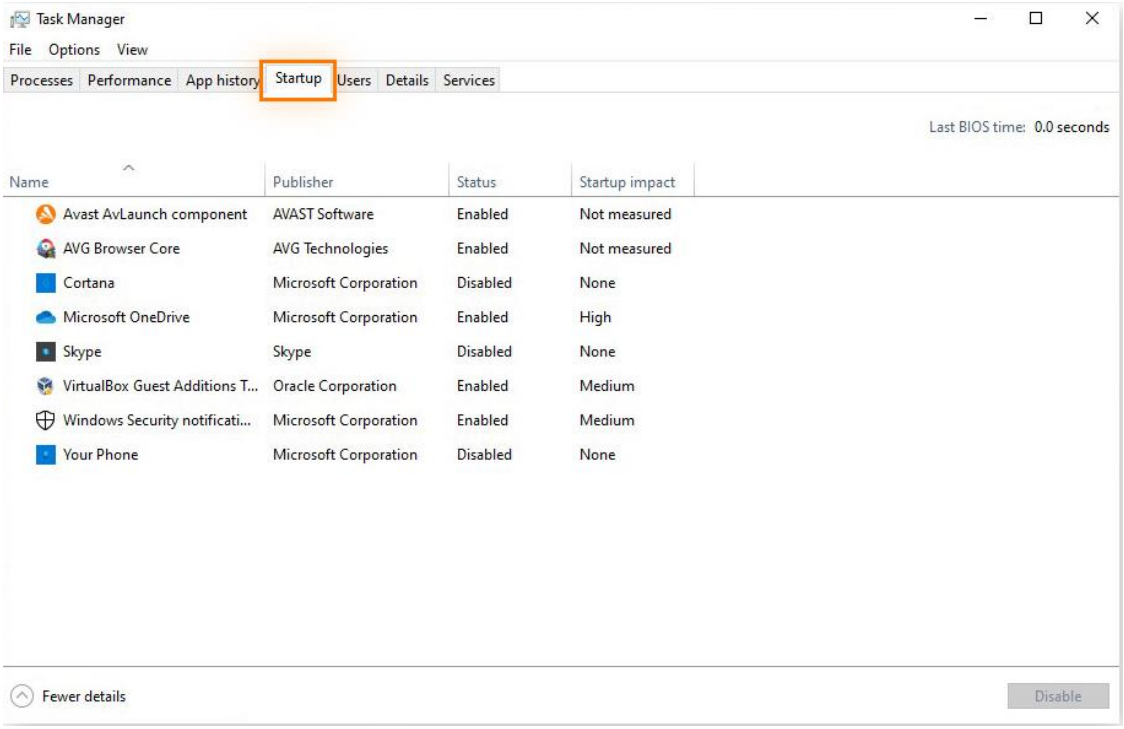
b) Click **More Details** in the lower-left corner to see a list of processes running on your computer.



c) Review the list of open apps and active processes. If you see any unknown programs that are consuming resources, search for them online. If they seem unnecessary or potentially dangerous, right-click on them and select **End task**.



d) Next, review the programs that turn on when your computer starts up by reviewing the **Startup tab**. This is located at the top of the **Task Manager**.



e) If you notice any unusual programs set to activate on startup, search for them online and if they're unnecessary or dangerous, disable them.

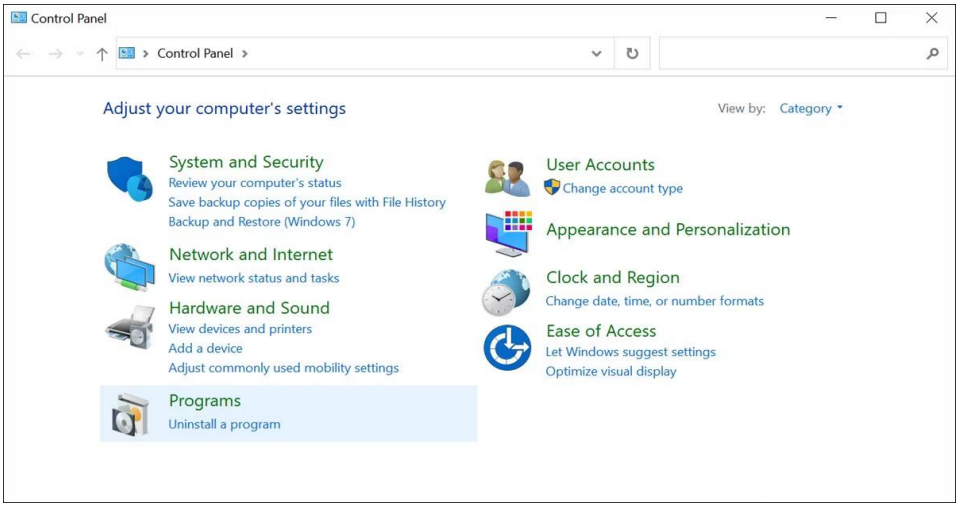
2. Uninstall Suspicious Programs

If you find any suspicious programs installed on your system, uninstall them immediately. You can do this on Windows by going to the Control Panel and following the instructions for uninstalling a program.

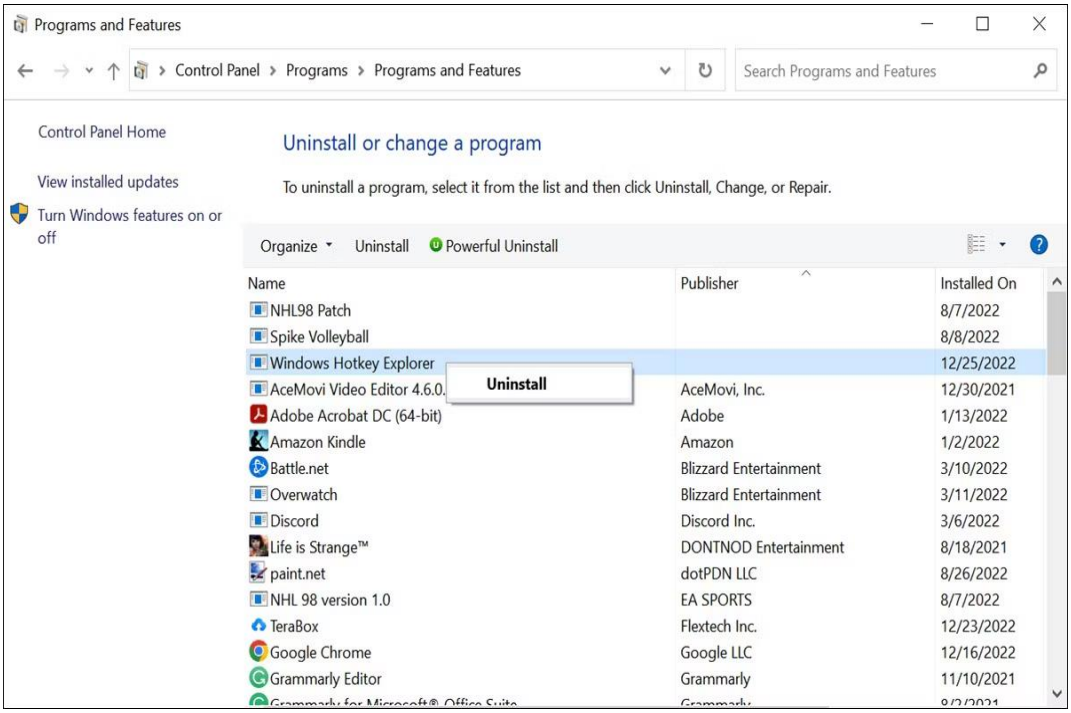
Here is how to do that.

a) On your Windows search bar, type "Control Panel" and click on its icon to launch.

b) Check for the "Programs" section and click on the **Uninstall a program** option below it.



c) Look for any suspicious programs installed on your system, then right-click on them and select **Uninstall**.



d) Follow the on-screen instructions to remove the program completely.

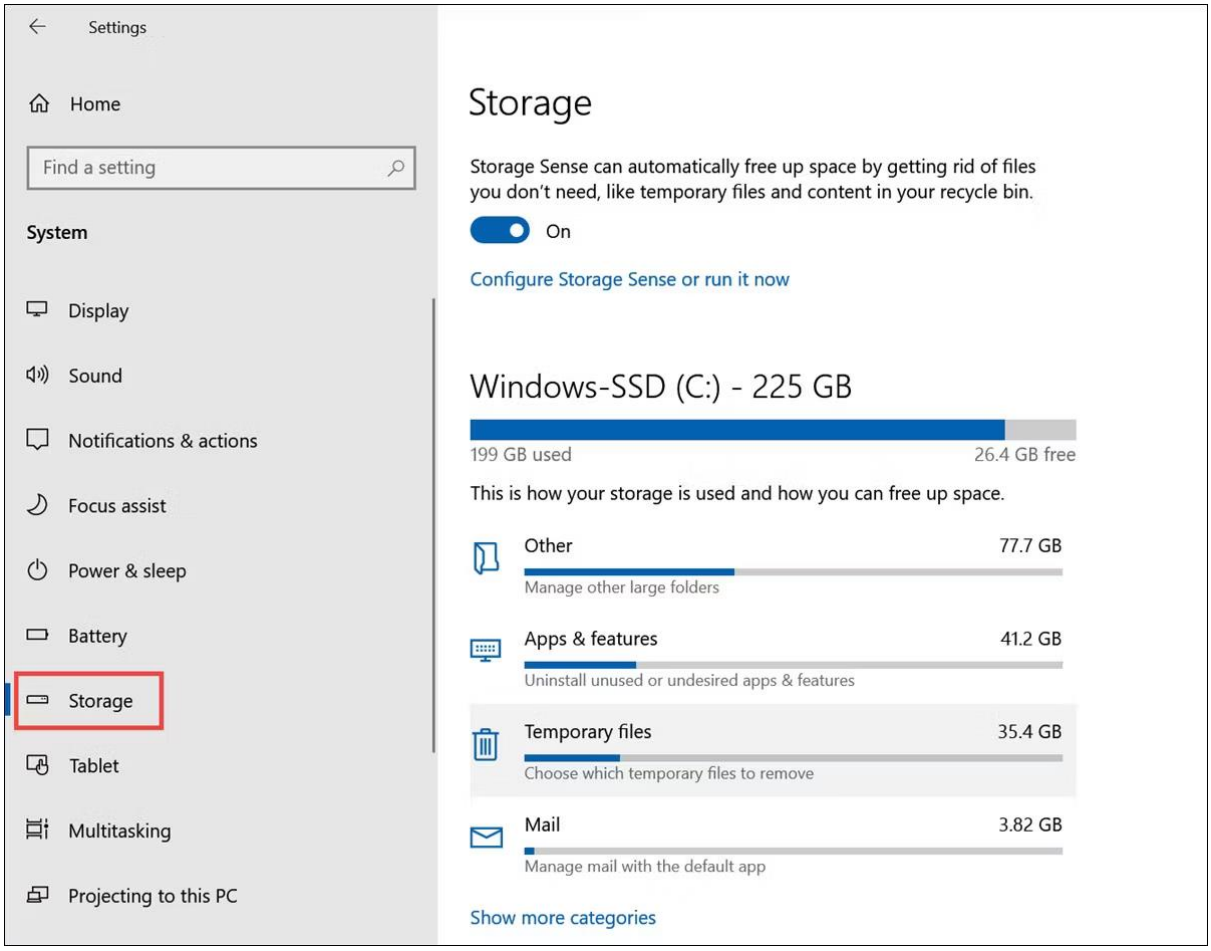
3. Scan for keyloggers using antivirus software

Antivirus software prevents malware and can identify and remove malware faster than you can manually.

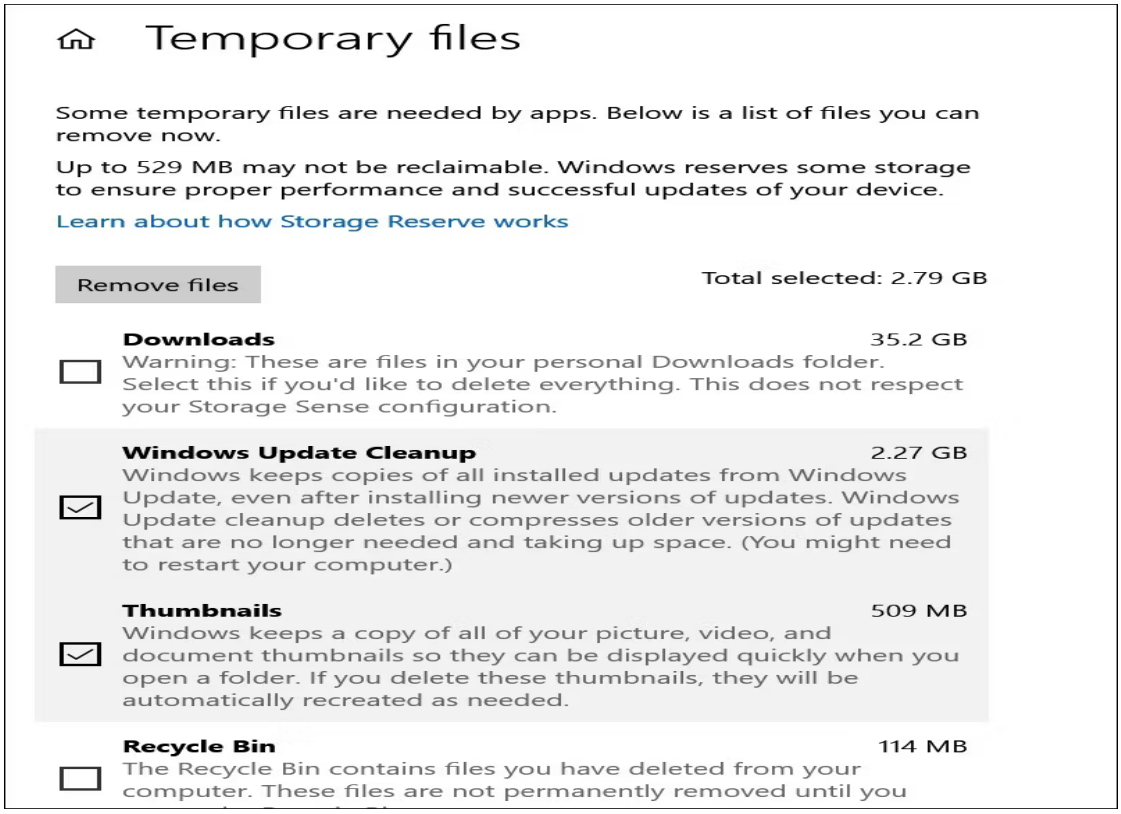
4. Clear Temporary Files

Keyloggers might also store malicious files in your system's temporary files folder. So, it is always a good idea to clear all the temporary files from your computer and ensure that any keylogger-related files have been removed. You can do this by using Windows Settings.

a) On your Windows system, click the Start button and select the Settings icon from the Start menu.
b) Choose **System** settings.
c) On the left pane, switch to the **Storage** tab and select **Temporary files** on the right.



d) On the next window, select the temporary files you want to delete and click the Remove files **button.**



5. **Reset Your PC**

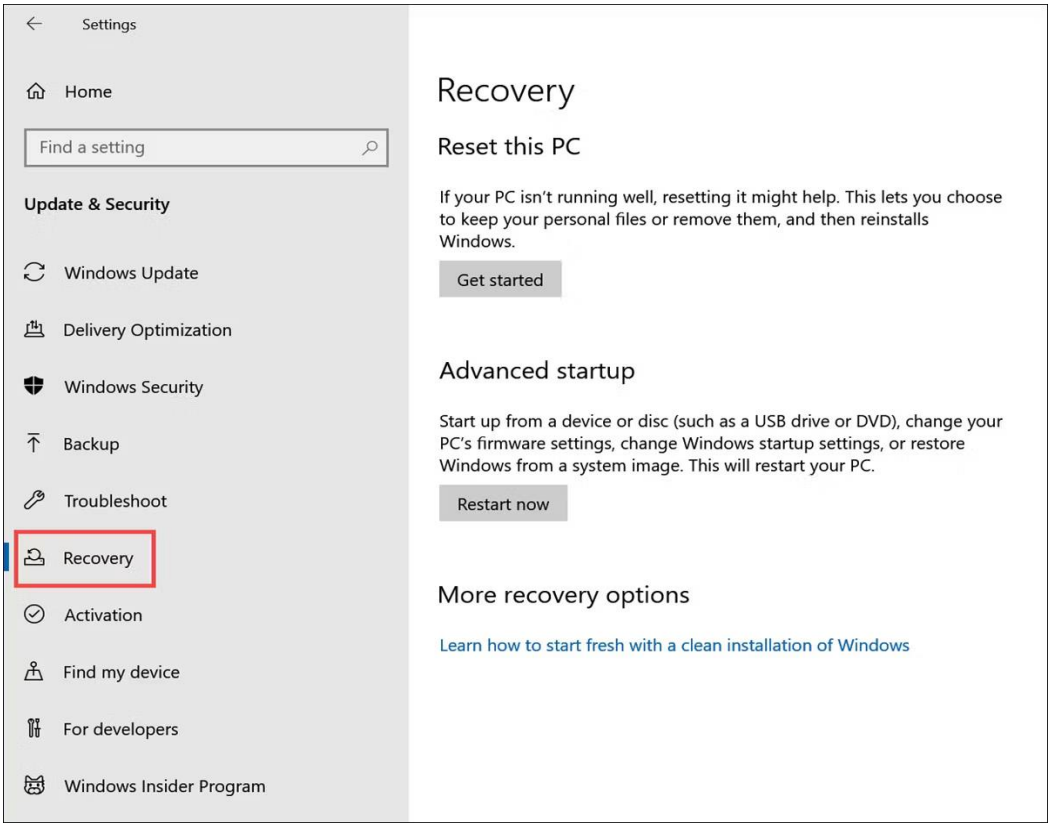
   If you are still unable to remove the keylogger using the above methods, you might want to consider resetting your PC. This will completely erase all the data stored on your system and reinstall a fresh copy of Windows.

   It is important to back up any important documents or files before resetting your system, as this process will delete them all. The problem is, you might be backing up the keylogger too. Make sure you're only backing up essentials.

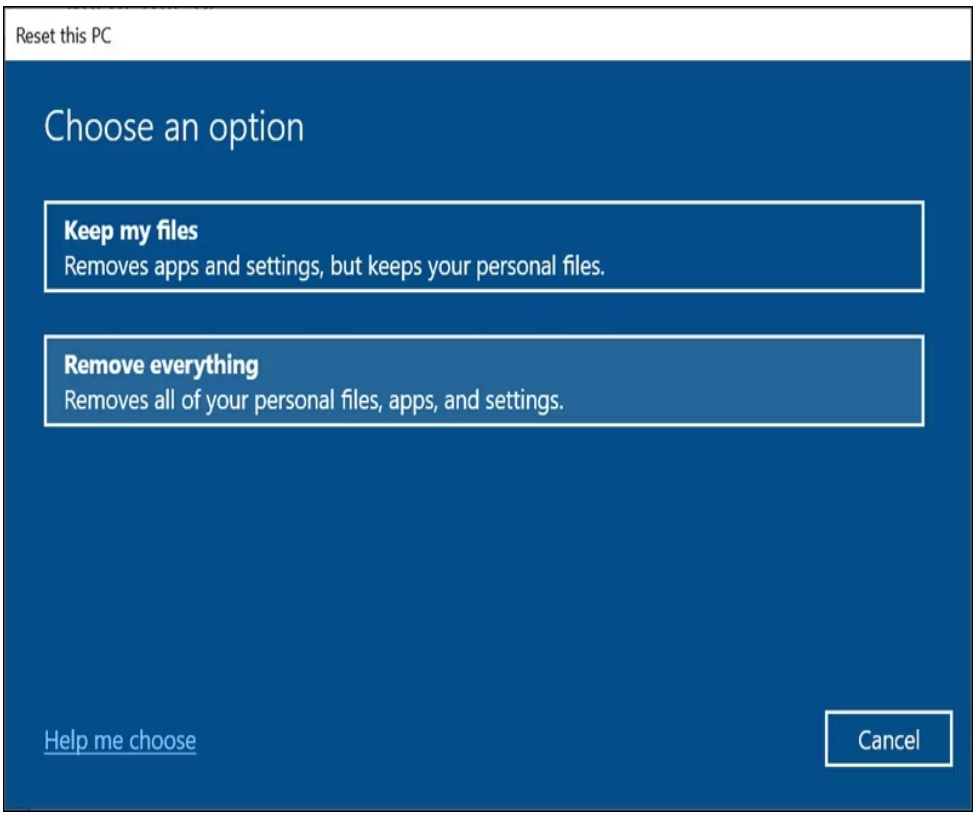
This is a drastic measure, but sometimes it is necessary to remove a keylogger from your system completely.

Here is how to reset a Windows PC.

a) Launch the Start menu and click on **Settings**.
b) Click on the **Update & Security** option.
c) Select the **Recovery** tab from the left panel, and then the **Get started** button on the right below the "Reset this PC" section.



e) On the next screen, select the **Remove everything** option.



f) Follow the onscreen instructions to complete the reset process and delete all keylogger-related files from your system.

Once you have finished resetting your PC, make sure you rerun a full malware scan to ensure that the keylogger has been completely removed and no traces remain.

Steps to detect Keylogger in Kali Machine

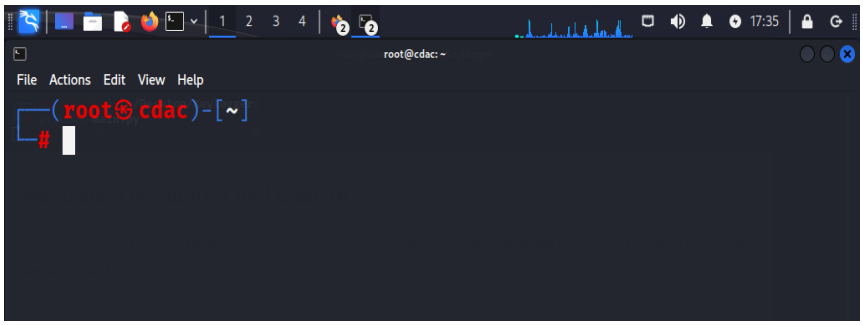
ClamAV and ClamTK Antivirus Scanner Tool for Kali Linux. In Kali Linux, Malware, viruses, and Trojans are uncommon however, they do exist. ClamAV is an excellent alternative if we only need an antivirus once in a while.

ClamAV is a free antivirus that we can use for online scanning, email scanning, and endpoint security. It comprises a multi-threaded daemon that is scalable and versatile, a command-line scanner, and a sophisticated tool for automated database updates, among other features.

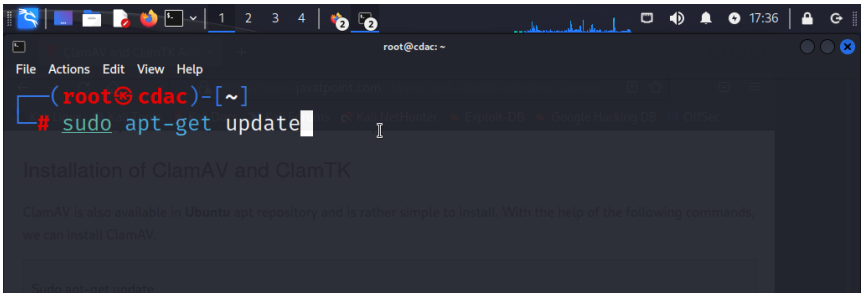
ClamAV is a command-line program, but it also has a graphical user interface called ClamAV which we can use to operate it. ClamAV is also cross-platform, supporting Windows and Mac OS X. It has the capacity to scan a wide range of files for security flaws. Tar, RAR, Cabinet, Zip, CHS. BinHex, OLE2, SIS format, and practically any email system is all supported.

Installation of ClamAV and ClamTK

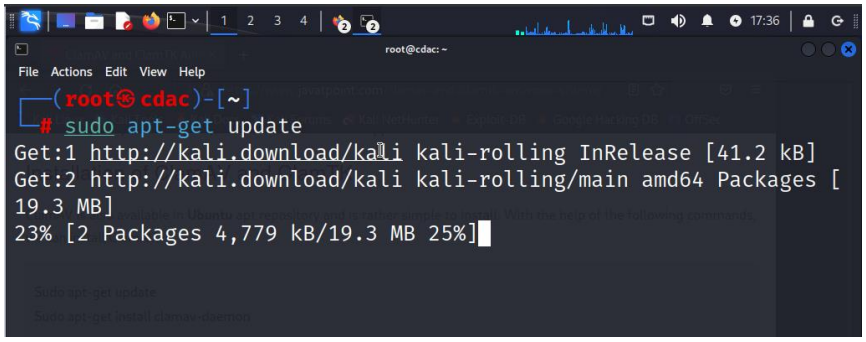
1. Open the terminal of your kali machine



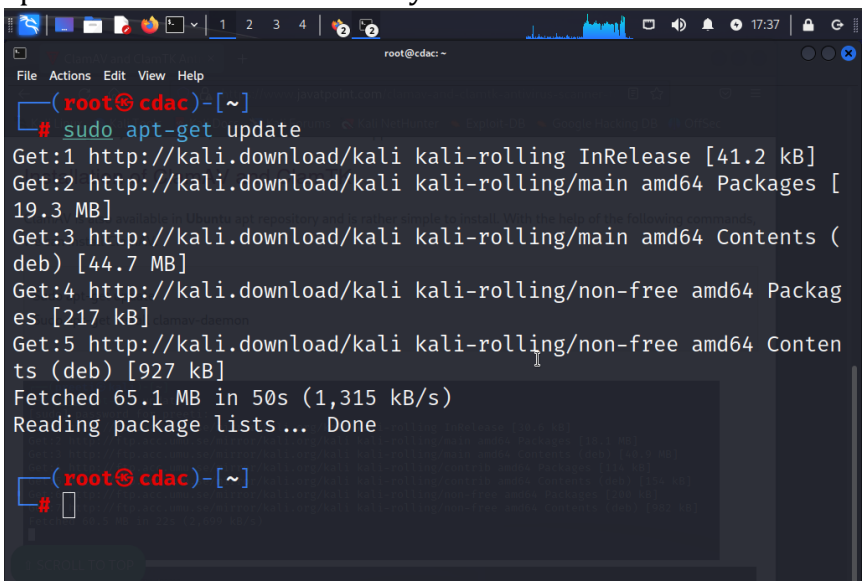
2. Type: **sudo apt-get update**



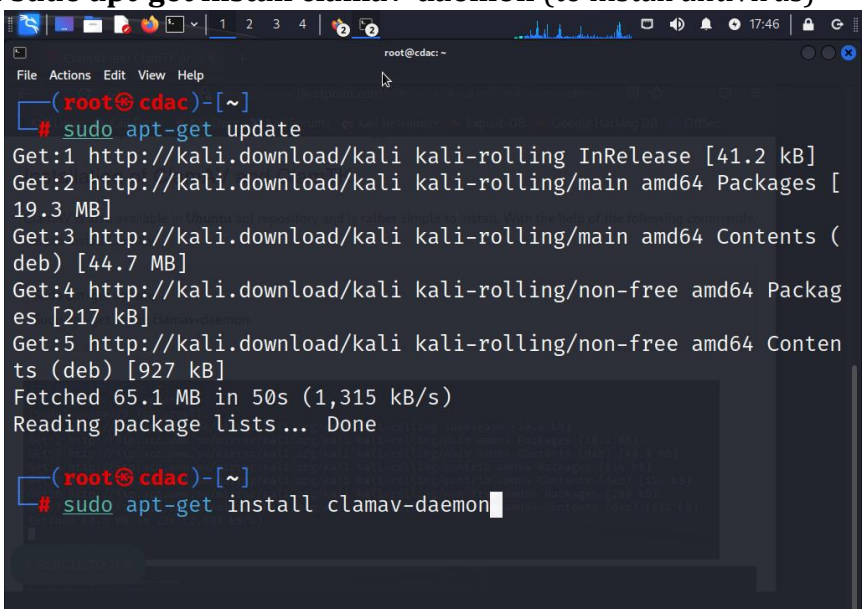
It has start updating



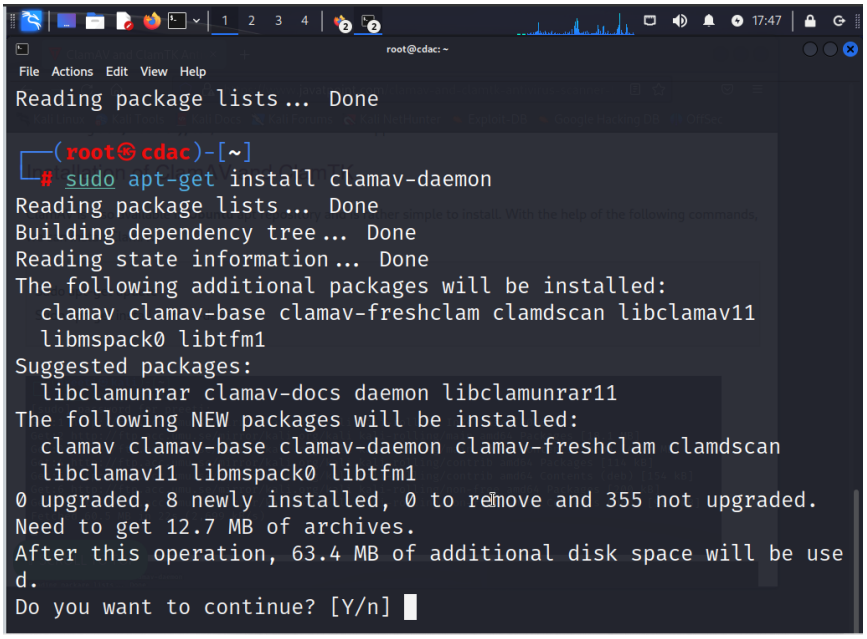
Updation has done successfully

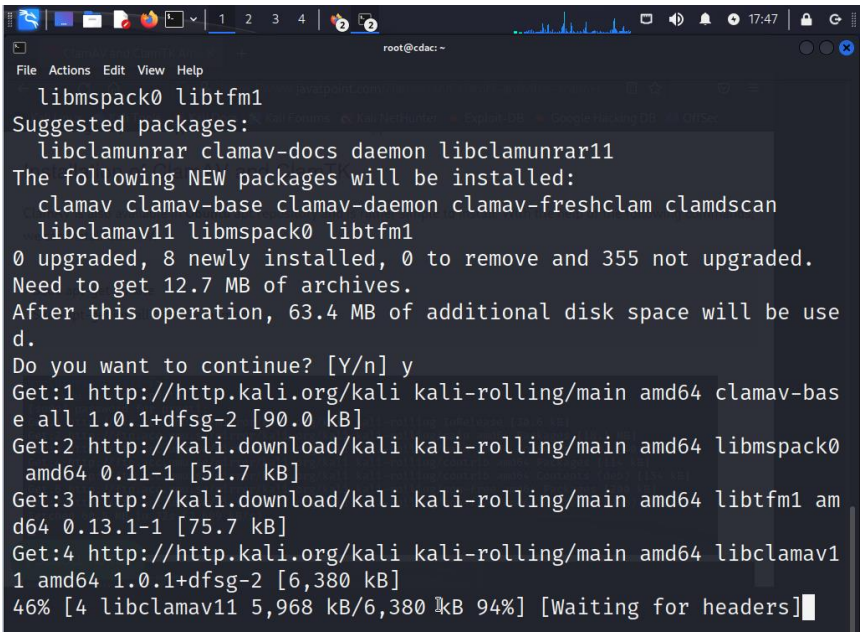


3. Type: **sudo apt-get install clamav-daemon** (to install antivirus)

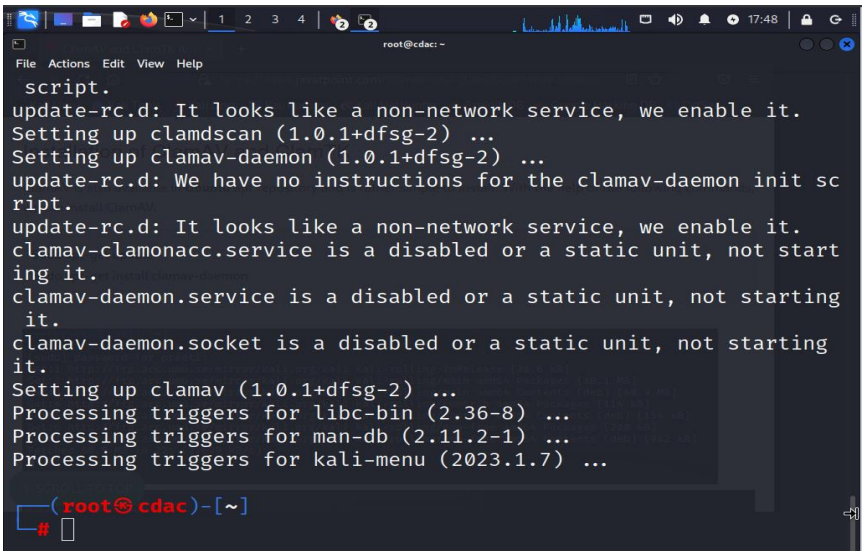


4. Type: **y** (to continue installation process)

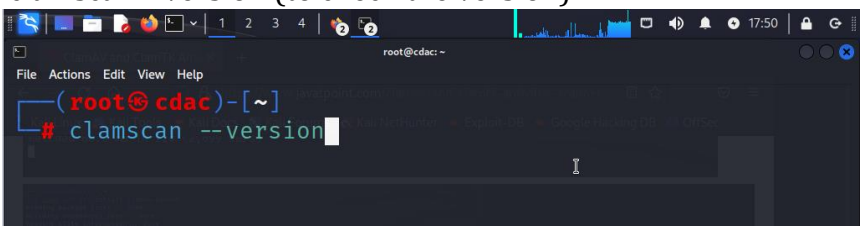

17:47
root@cdac: ~
File Actions Edit View Help
Reading package lists ... Done
(root㉿cdac)-[~]
sudo apt-get install clamav-daemon
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
clamav clamav-base clamav-freshclam clamdscan libclamav11
libmspack0 libtfm1
Suggested packages:
libclamunrar clamav-docs daemon libclamunrar11
The following NEW packages will be installed:
clamav clamav-base clamav-daemon clamav-freshclam clamdscan
libclamav11 libmspack0 libtfm1
0 upgraded, 8 newly installed, 0 to remove and 355 not upgraded.
Need to get 12.7 MB of archives.
After this operation, 63.4 MB of additional disk space will be use
d.
Do you want to continue? [Y/n]


17:47
root@cdac: ~
File Actions Edit View Help
libmspack0 libtfm1
Suggested packages:
libclamunrar clamav-docs daemon libclamunrar11
The following NEW packages will be installed:
clamav clamav-base clamav-daemon clamav-freshclam clamdscan
libclamav11 libmspack0 libtfm1
0 upgraded, 8 newly installed, 0 to remove and 355 not upgraded.
Need to get 12.7 MB of archives.
After this operation, 63.4 MB of additional disk space will be use
d.
Do you want to continue? [Y/n] y
Get:1 http://http.kali.org/kali kali-rolling/main amd64 clamav-bas
e all 1.0.1+dfsg-2 [90.0 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 libmspack0
amd64 0.11-1 [51.7 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 libtfm1 am
d64 0.13.1-1 [75.7 kB]
Get:4 http://http.kali.org/kali kali-rolling/main amd64 libclamav1
1 amd64 1.0.1+dfsg-2 [6,380 kB]
46% [4 libclamav11 5,968 kB/6,380 kB 94%] [Waiting for headers]

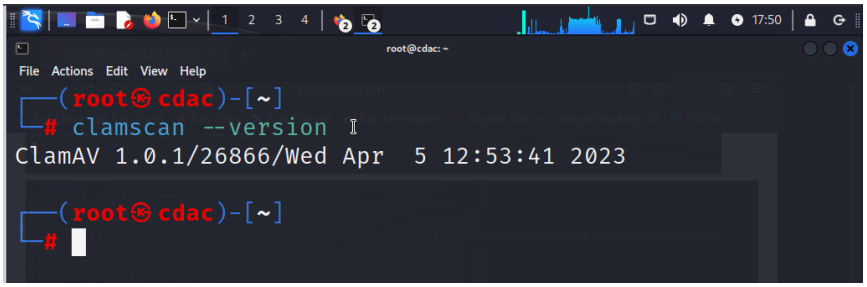
Antivirus successfully installed



5. Type: clamscan --version (to check the version)

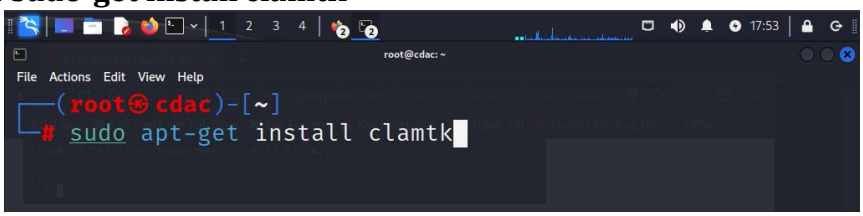


Antivirus latest version

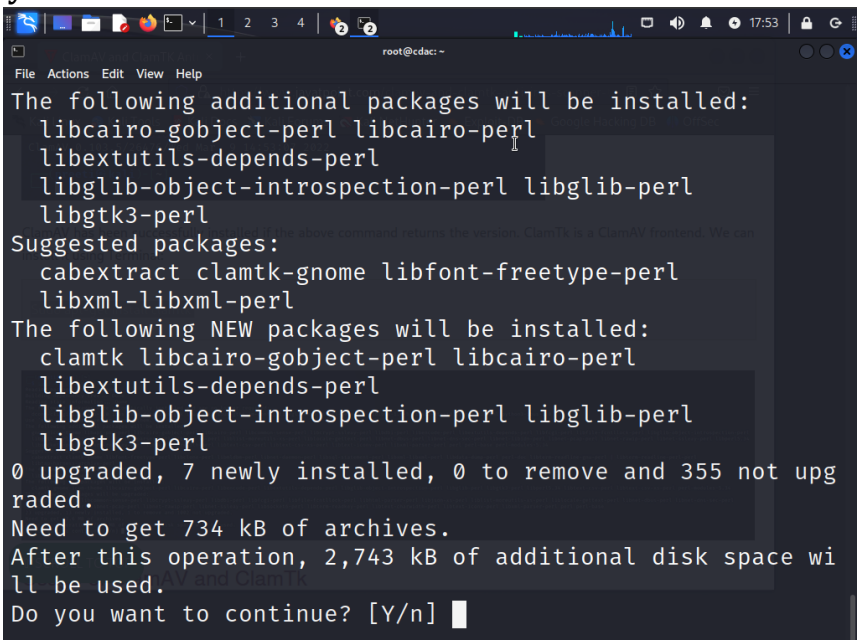


ClamAV has been successfully installed if the above command returns the version. ClamTk is a ClamAV frontend. We can install it using Terminal. ClamAV is command line based tool. Now lets also install clamtk (which is GUI version tool for easy access)

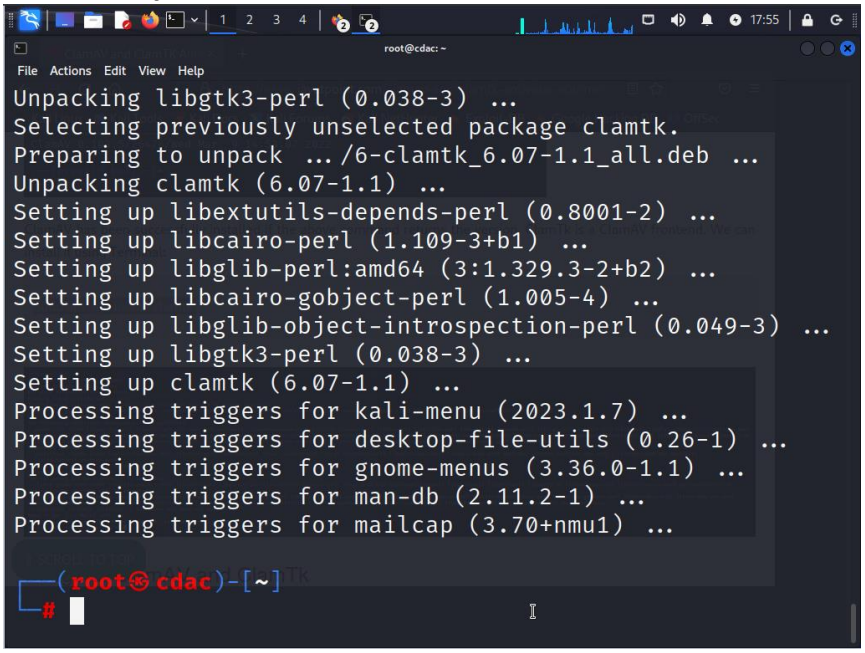
6. Type: **sudo-get install clamtk**



7. Type: **y** to continue



Successfully installed.



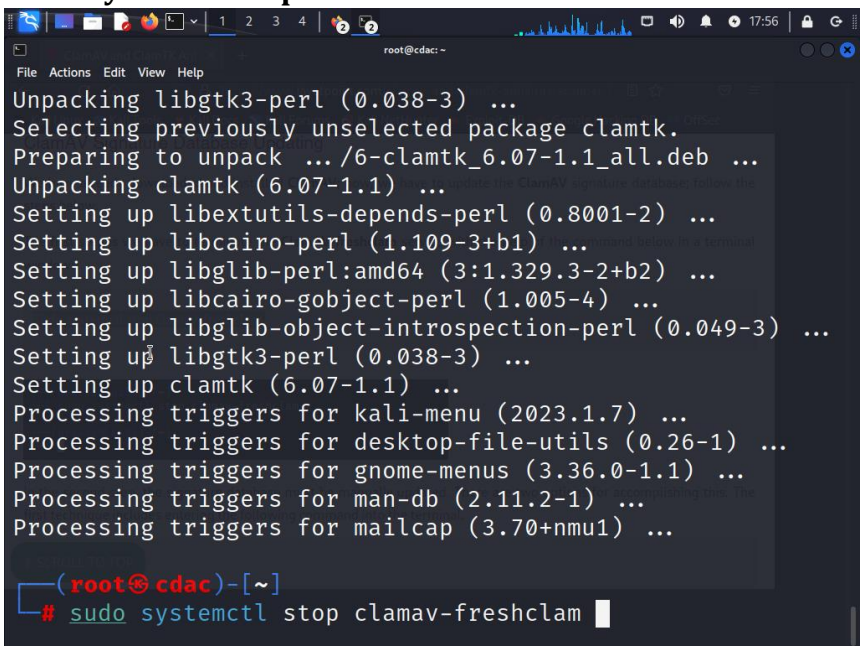
Usage of ClamAV and ClamTk

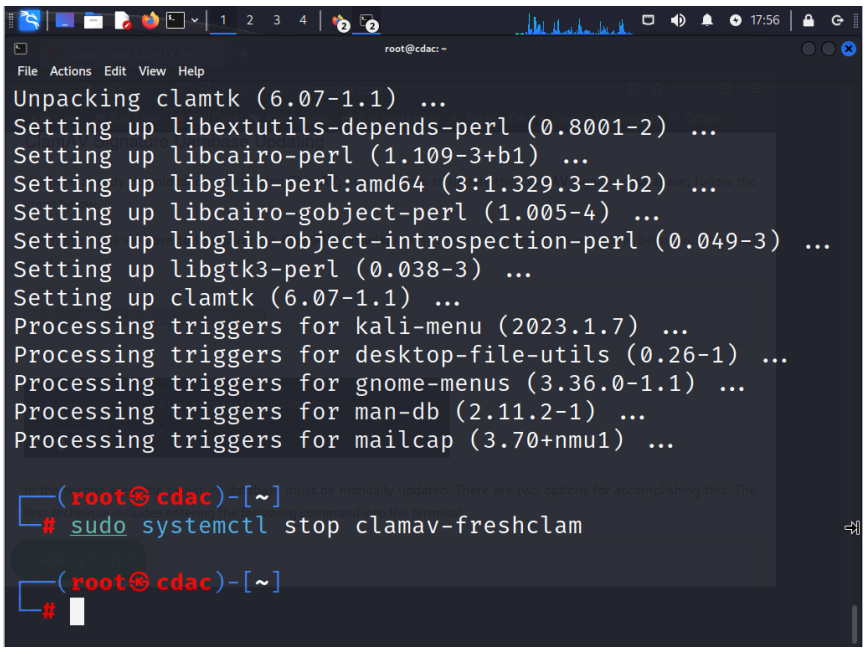
ClamAV Signature Database Updating

We have already downloaded and installed ClamAV; now, we have to update the ClamAV signature database; follow the steps below.

The first step is we have to terminate the ClamAV-freshclam service with the help of the command below in a terminal window:

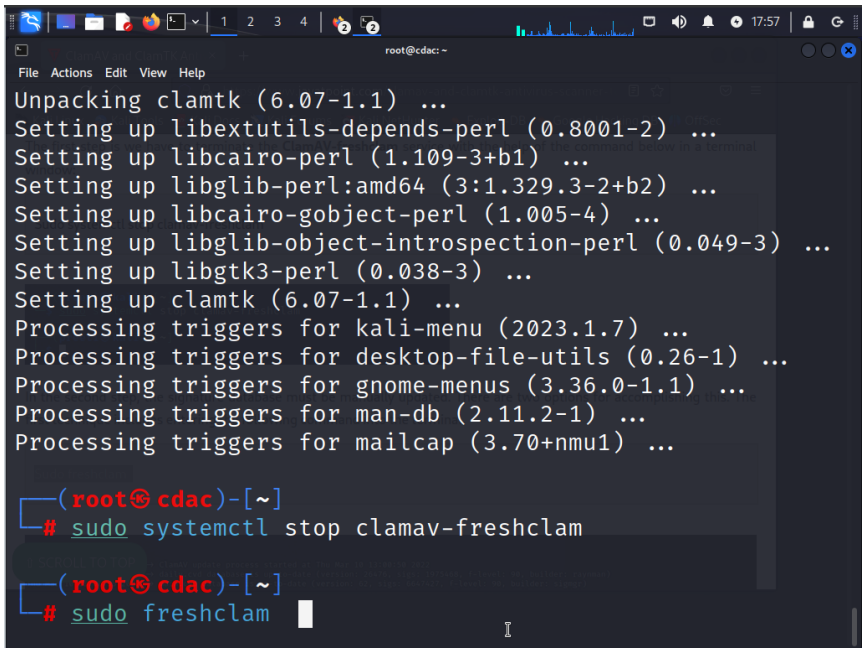
8. Type: **sudo systemctl stop clamav-freshclam**

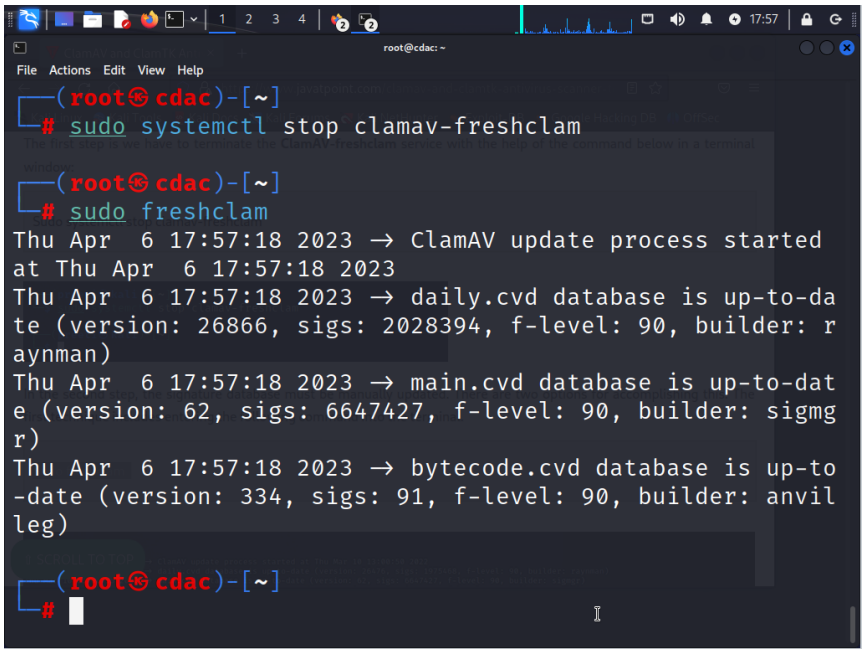




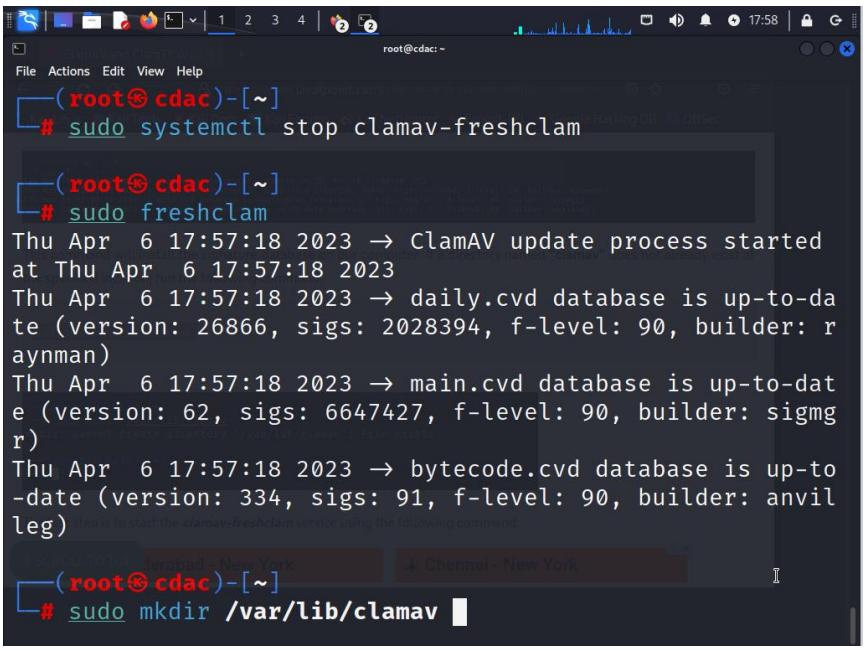
9. Type: **sudo freshclam**

In the second step, the signature database must be manually updated. There are two options for accomplishing this. The first technique includes entering the following command into the terminal.

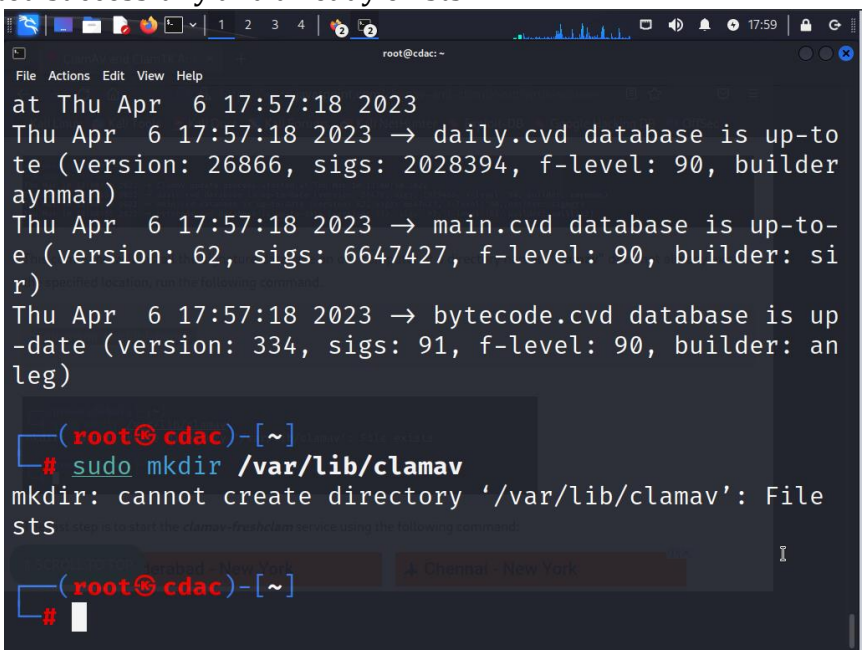




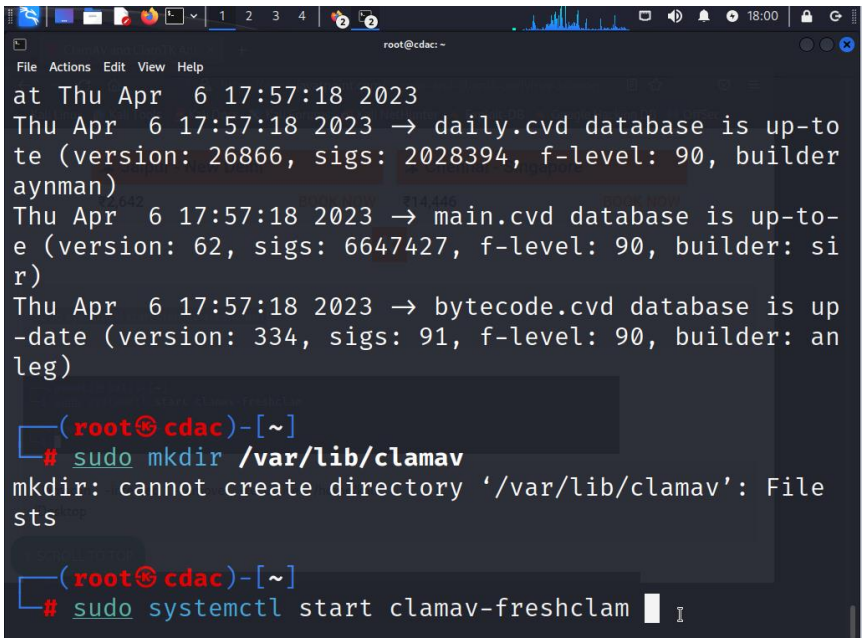
10. Type: **sudo mkdir /var/lib/clamav**
    This command will install the signature database on our computer. If a directory named **"clamav"** does not already exist at the specified location, run the following command.

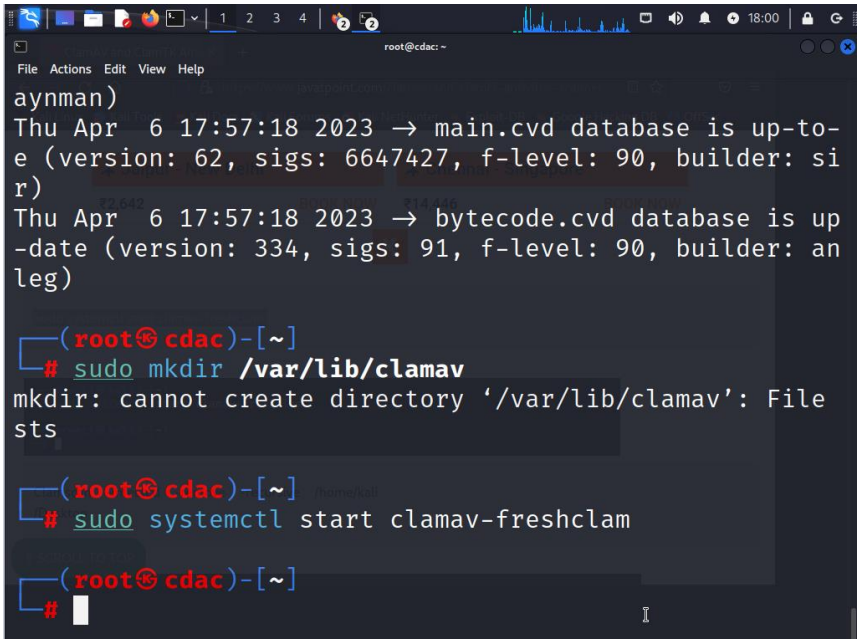


File created successfully and already exists.



11. Type: **sudo systemctl start clamav-freshclam**
    The last step is to start the **clamav-freshclam** service using the following command

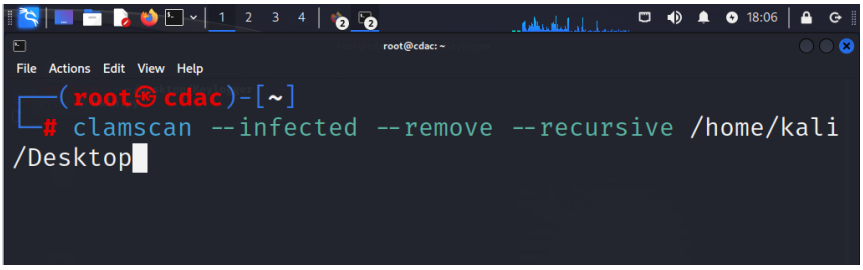




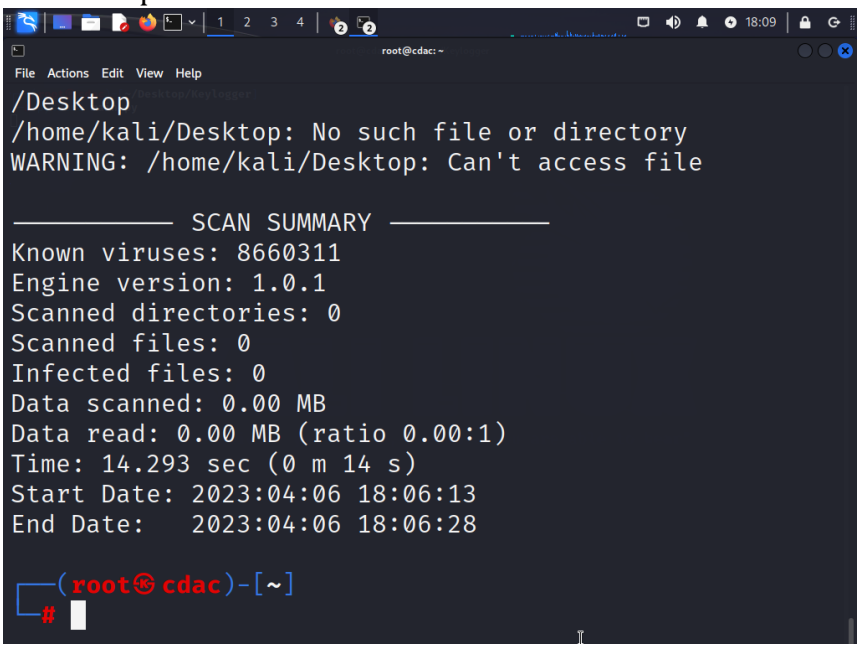
12. Type: **clamscan --infected --remove --recursive /home/kali/Desktop**

In the above command, we have used certain parameters. The following are the meanings of these options:

- **-injected: -** Only prints those files which are injected.
- **-remove: -** This command deletes infected files.
- **-recursive: -** The subdirectories of the directory will also be examined.



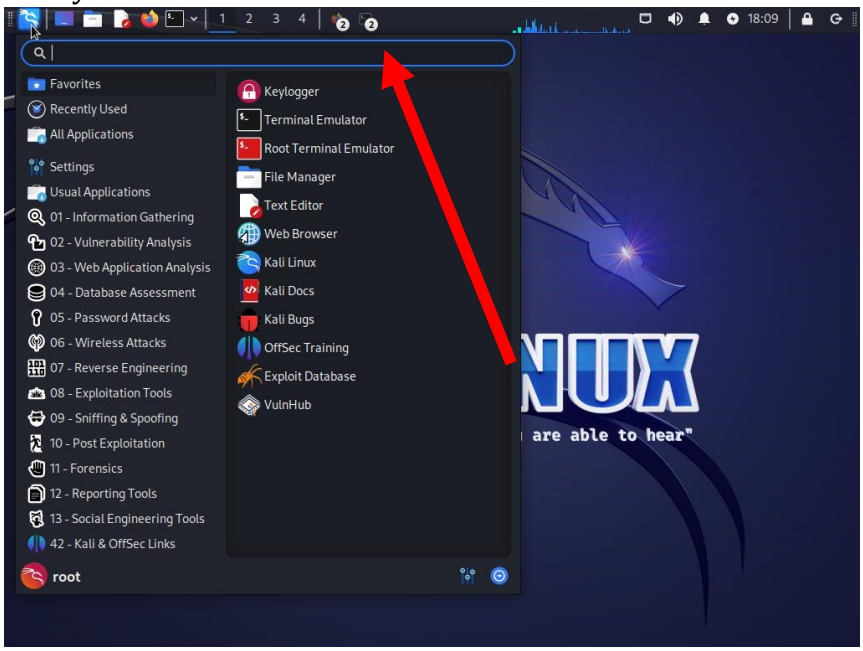
You can see the output here.



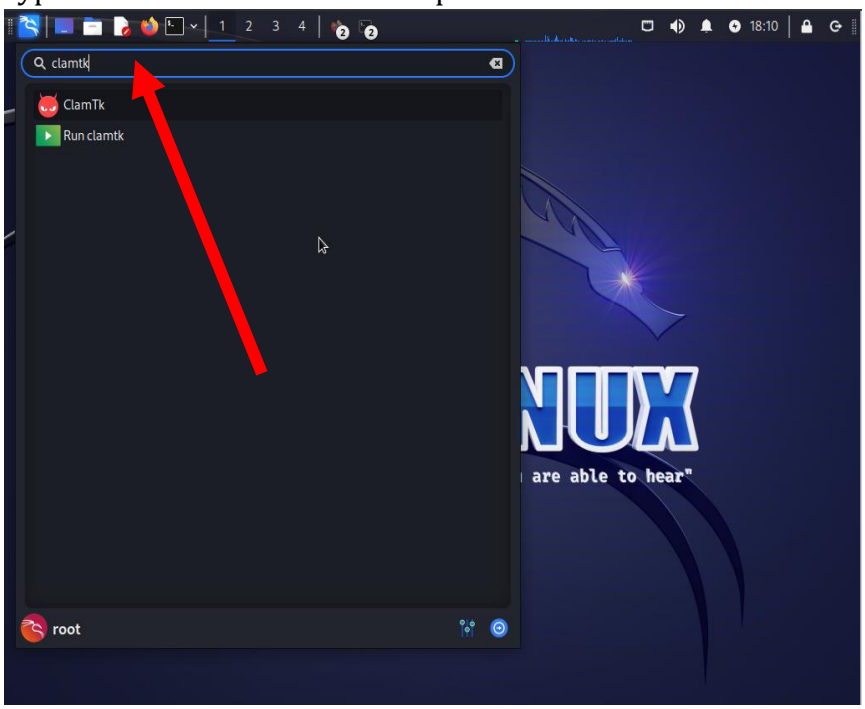
Now lets see how to use clamtk GUI based application to scan for any virus or threats.

1. Open the terminal and go to Applications

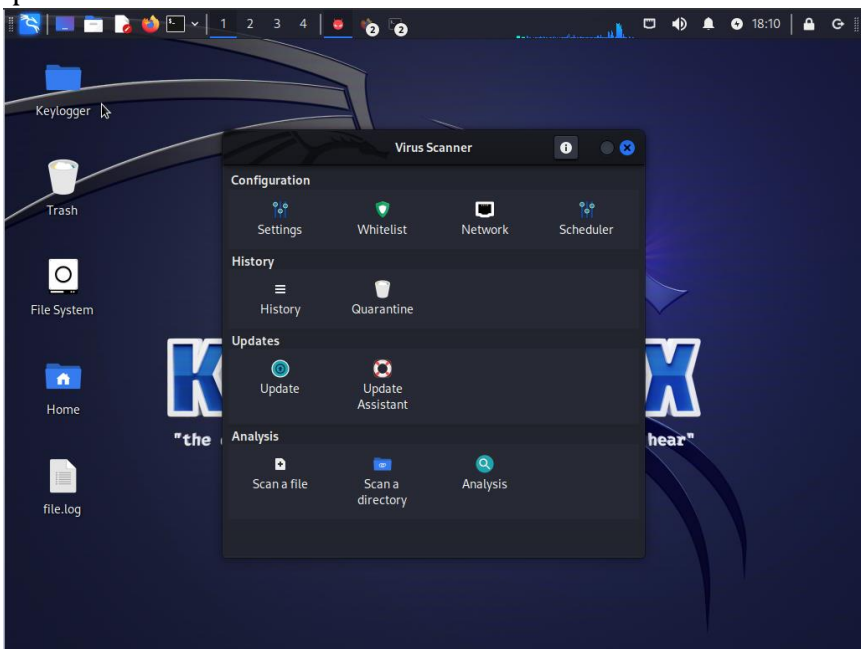
Here you can see search bar



Type **clamtk** in the search bar option

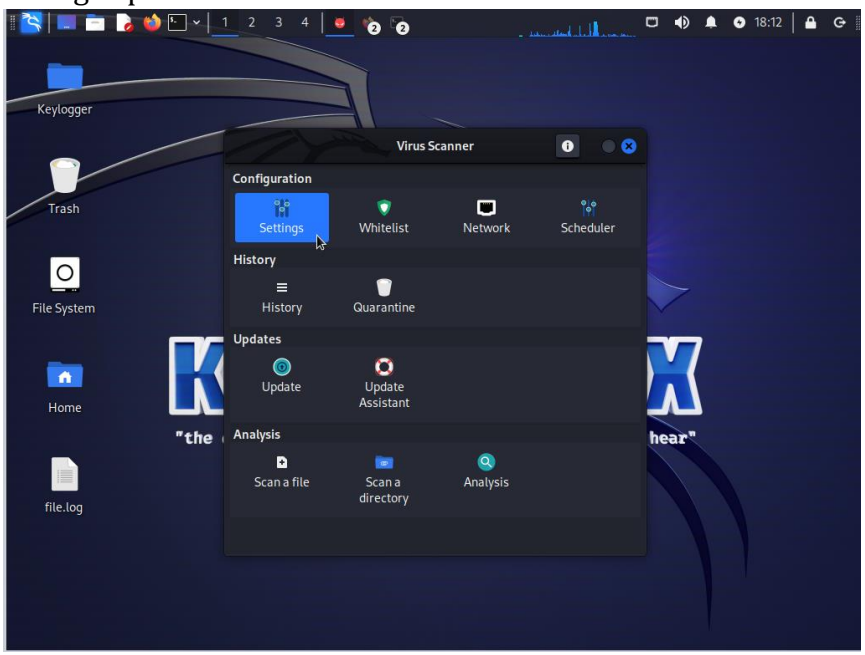


When we run ClamTk for the first time, we will see a simple interface with four main components.

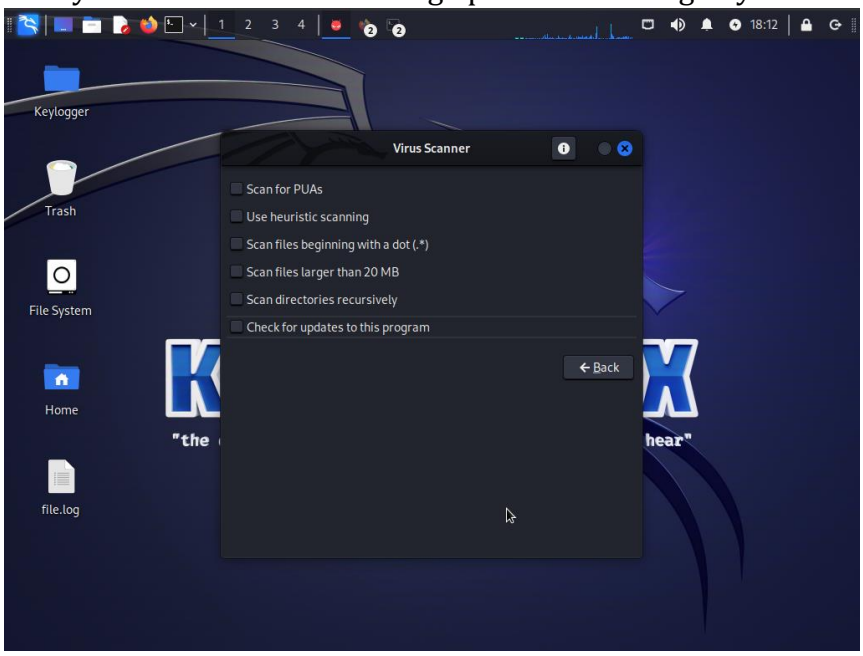


The first element is the setup area, which permits us to set up and adjust ClamAv and its behavior. For example, we can scan a folder but not its subfolders. We can exclude files or folders from scans by whitelisting them, and scan large files, hidden files, and password checkers.

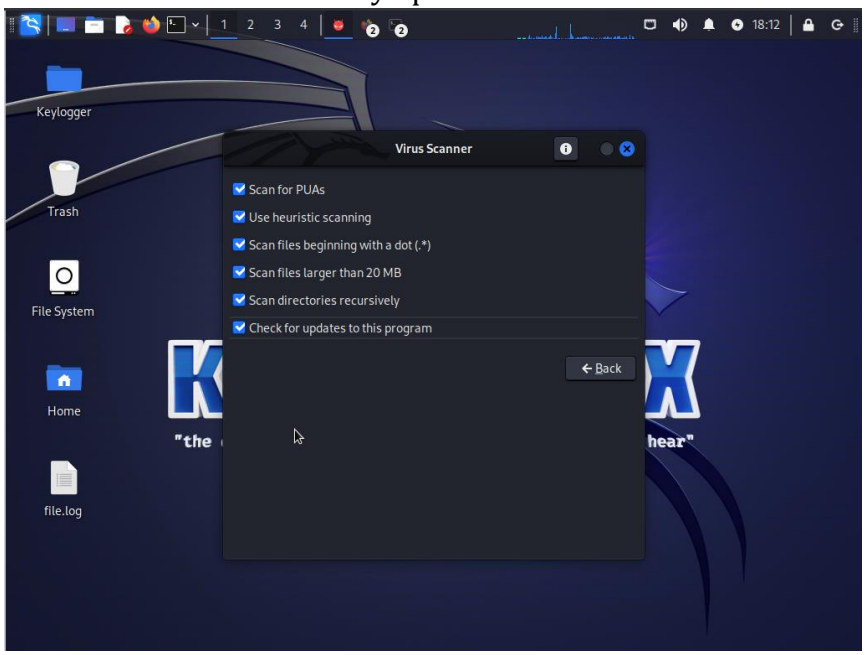
Click on Settings option



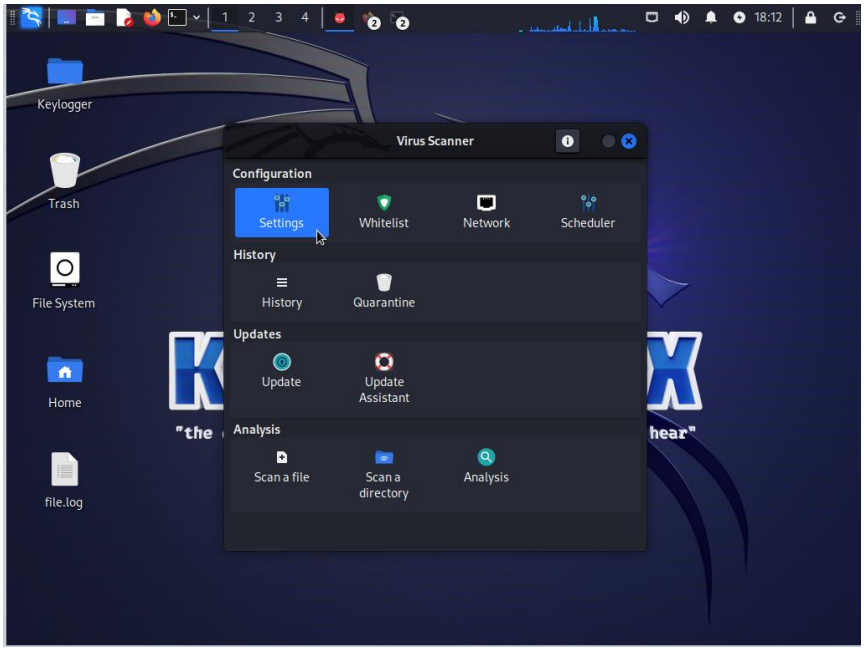
Here you can select the scanning options according to your own usage.



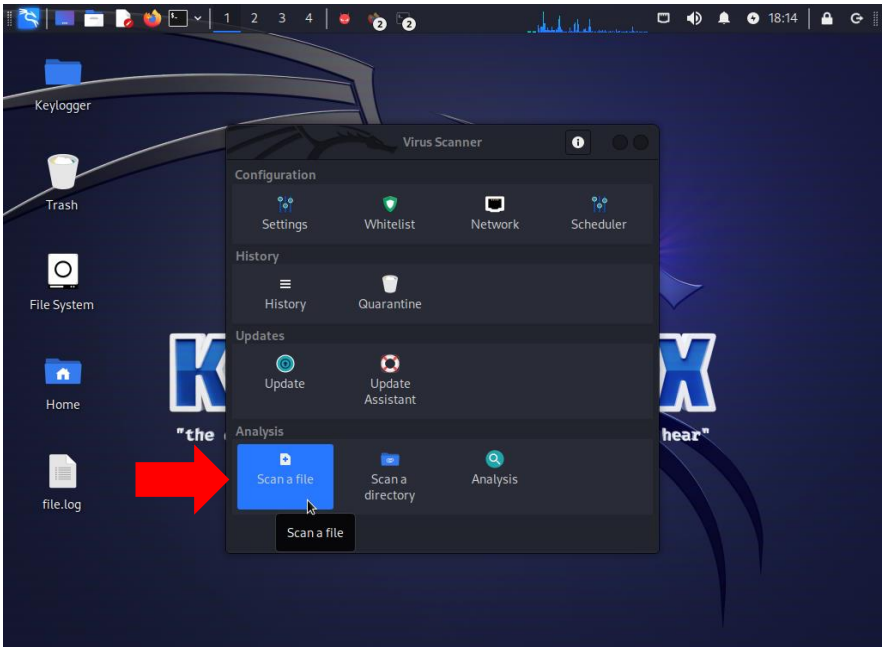
Here we have checked every option to scan



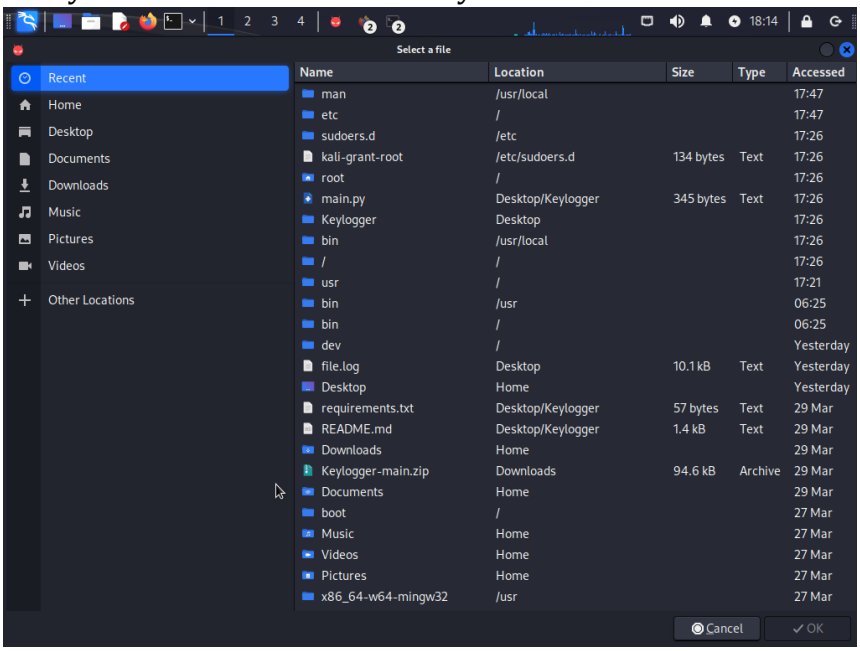
1. The history area, provides us the information related to the prior scans. A quarantine section is also available, where we can check for harmful files which have been confined as a result of scanning.
2. The third section is updated, ClamAV can use this to import new virus definitions; the first thing we should do after installing ClamAV is click updates to update the virus definitions.
3. The final portion is the analysis. Our ClamAV scans will begin here.



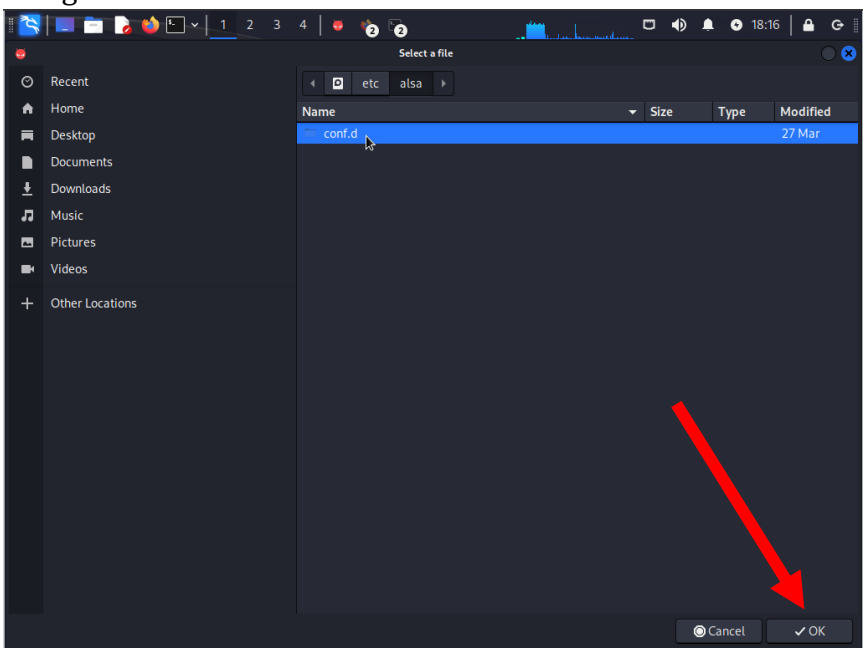
Now in the Analysis option you can scan for Files & Directories on your local machine. Lets scan for a file. Click on **Scan a file** option.



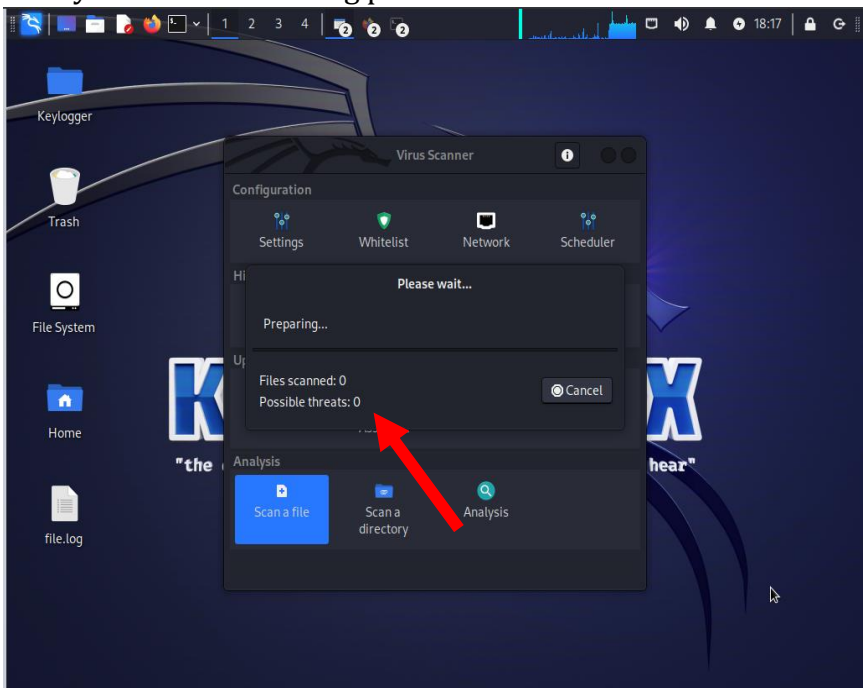
Here you can select the file which you want to scan for.



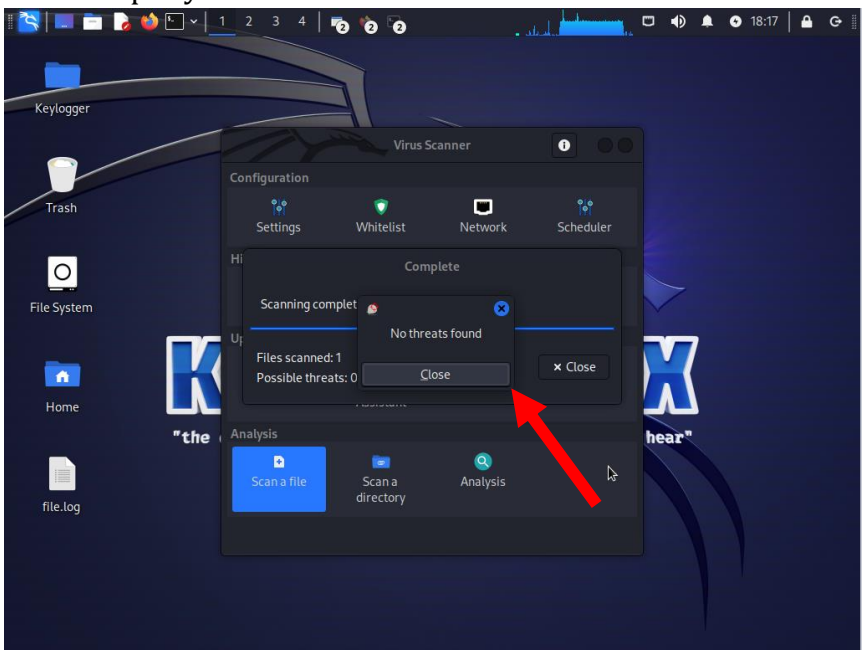
After selecting file click on ok.



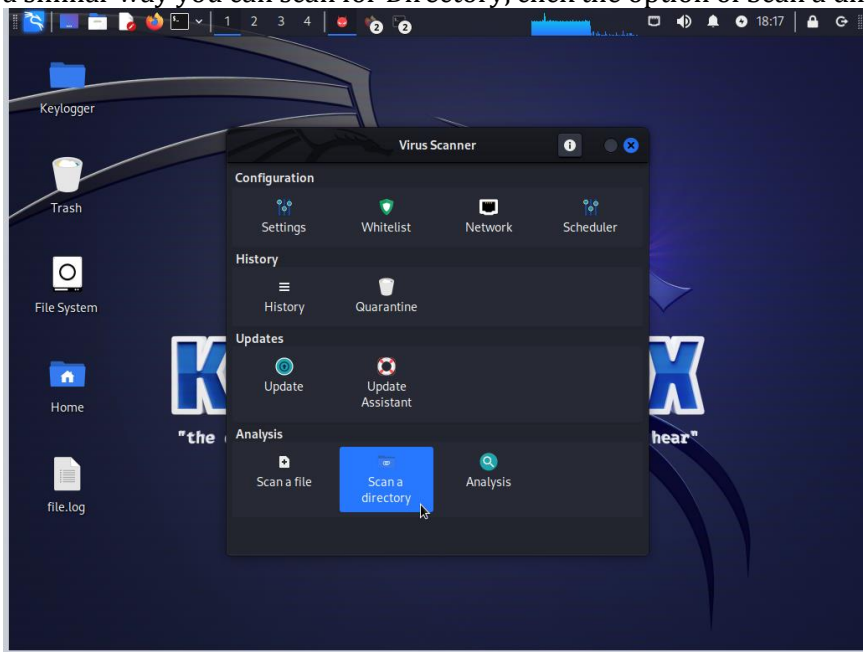
Here you can see scanning process has started.



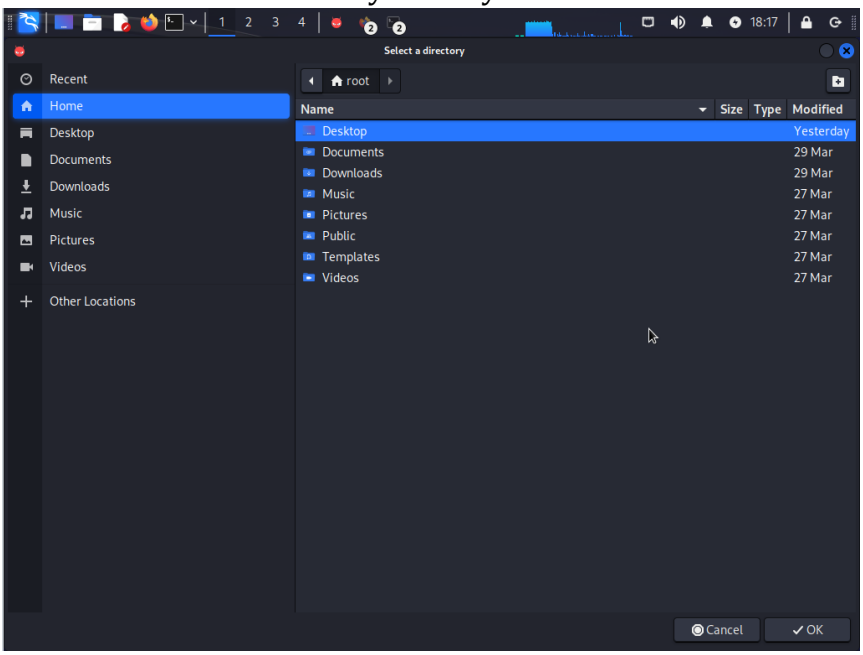
In the output you can see no threat found in the file.



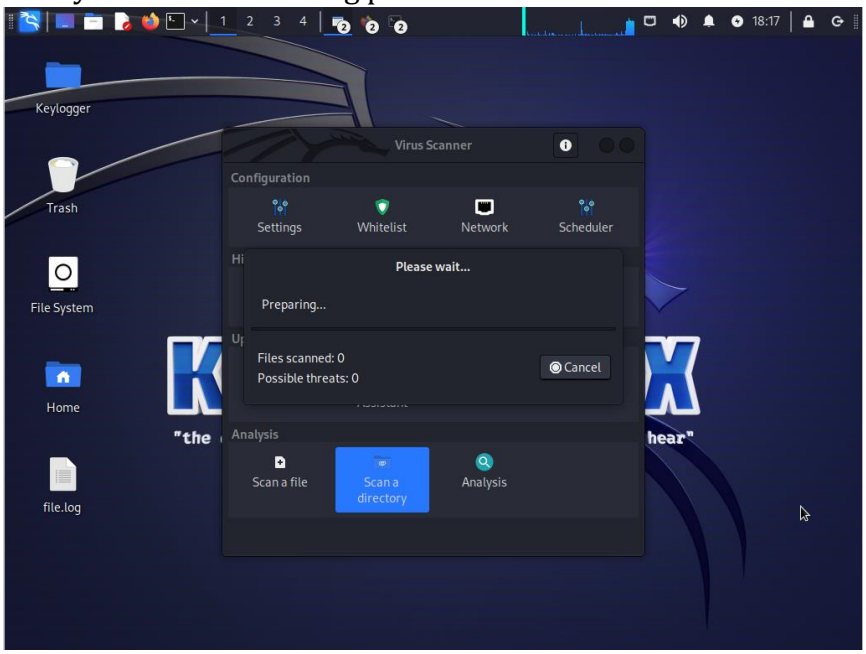
In a similar way you can scan for Directory, click the option of Scan a directory



You can choose the directory which you want to scan for and click ok



Here you can see scanning process has started.



In the output you can see no threat found in the directory.