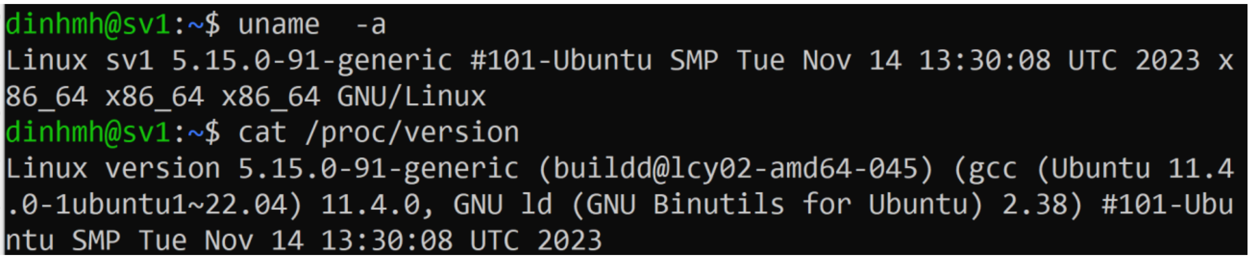
Install and Use ClamAV

OS Install:

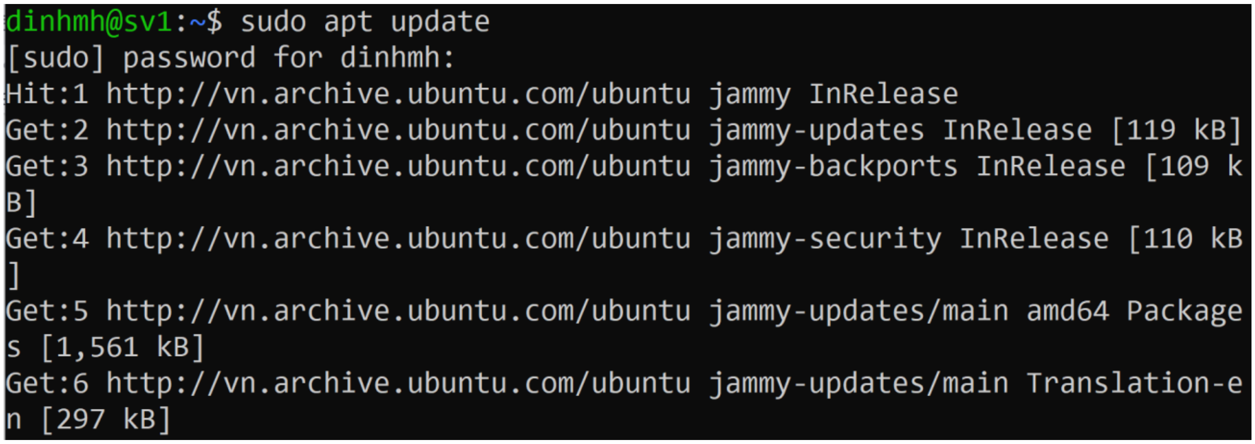


```
dinhmh@sv1:~$ uname  -a
Linux sv1 5.15.0-91-generic #101-Ubuntu SMP Tue Nov 14 13:30:08 UTC 2023 x
86_64 x86_64 x86_64 GNU/Linux
dinhmh@sv1:~$ cat /proc/version
Linux version 5.15.0-91-generic (buildd@lcy02-amd64-045) (gcc (Ubuntu 11.4
.0-1ubuntu1~22.04) 11.4.0, GNU ld (GNU Binutils for Ubuntu) 2.38) #101-Ubu
ntu SMP Tue Nov 14 13:30:08 UTC 2023
```

ClamAV is a well-reputed free and open-source antivirus software tool. It provides a command line interface that quickly scans the Linux system against viruses and malware attacks. The "ClamAV" helps scan the important part of Linux, i.e., mail gateways and emails directly affecting the network.

Install ClamAV on Ubuntu

Step 1: Update the Repository



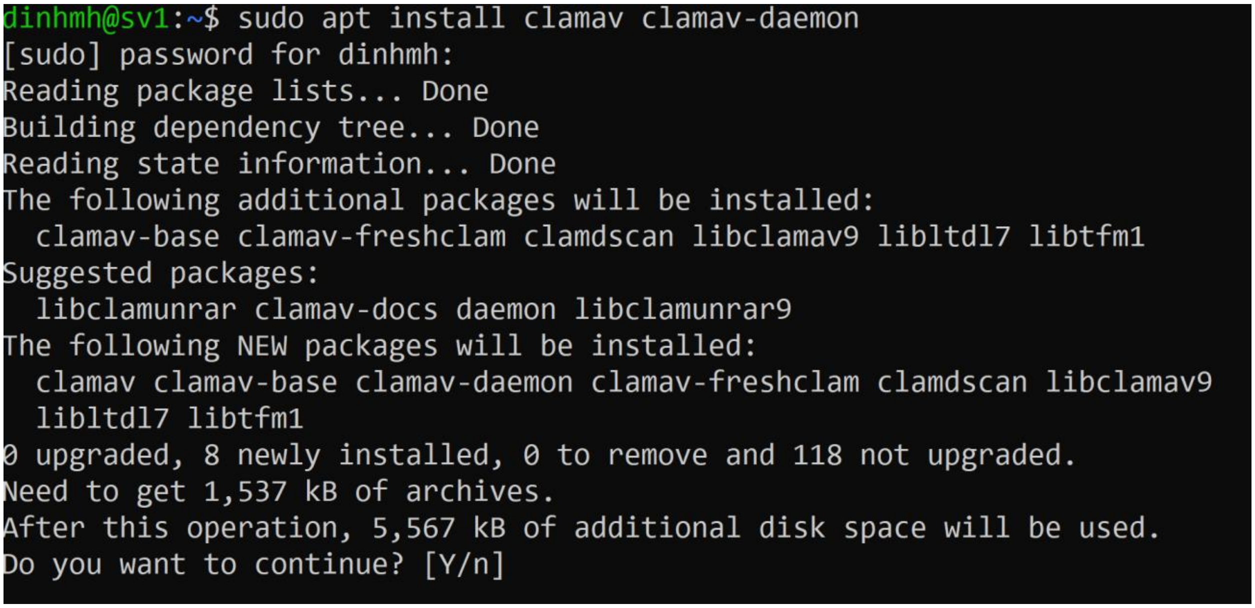
```
dinhmh@sv1:~$ sudo apt update
[sudo] password for dinhmh:
Hit:1 http://vn.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://vn.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:3 http://vn.archive.ubuntu.com/ubuntu jammy-backports InRelease [109 k
B]
Get:4 http://vn.archive.ubuntu.com/ubuntu jammy-security InRelease [110 kB
]
Get:5 http://vn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Package
s [1,561 kB]
Get:6 http://vn.archive.ubuntu.com/ubuntu jammy-updates/main Translation-e
n [297 kB]
```

We need to reboot after the update is complete

Step 2: Install ClamAV

Install the "ClamAV" application alongside the "clamav-daemon" from the standard repository of Ubuntu using the default "apt" package manager:

sudo apt install clamav clamav-daemon

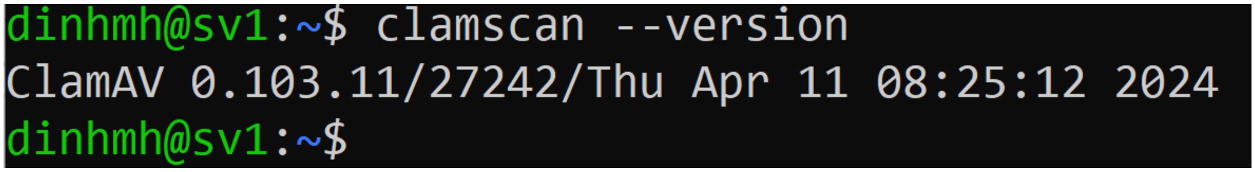


```
dinhmh@sv1:~$ sudo apt install clamav clamav-daemon
[sudo] password for dinhmh:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  clamav-base clamav-freshclam clamdscan libclamav9 libltdl7 libtfm1
Suggested packages:
  libclamunrar clamav-docs daemon libclamunrar9
The following NEW packages will be installed:
  clamav clamav-base clamav-daemon clamav-freshclam clamdscan libclamav9
  libltdl7 libtfm1
0 upgraded, 8 newly installed, 0 to remove and 118 not upgraded.
Need to get 1,537 kB of archives.
After this operation, 5,567 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

Step 3: Verify ClamAV

Check the installed version of the “clamav” scanner for verification purposes:

clamscan –version



```
dinhmh@sv1:~$ clamscan --version
ClamAV 0.103.11/27242/Thu Apr 11 08:25:12 2024
dinhmh@sv1:~$
```

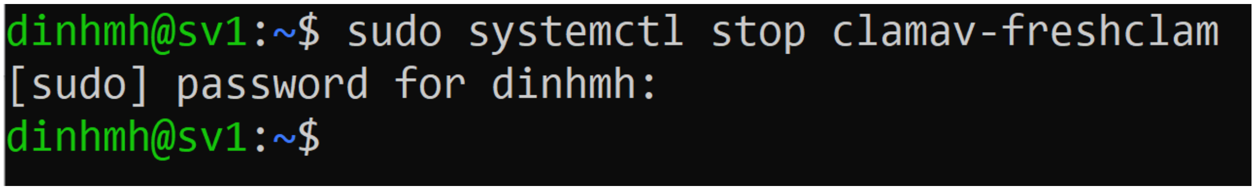
The “ClamAV” works on a signature database that identifies the malware. It requires updation regularly that ensures the application is up to date for protection against the latest threats.

Keeping this in view, Let’s update the installed “ClamAV” signature database:

Disable the “freshclam” Service

The pre-installed “**freshclam**” service automatically downloads the database updates. For the manual updation, disable/stop the “freshclam” service using the “systemctl” command:

sudo systemctl stop clamav-freshclam



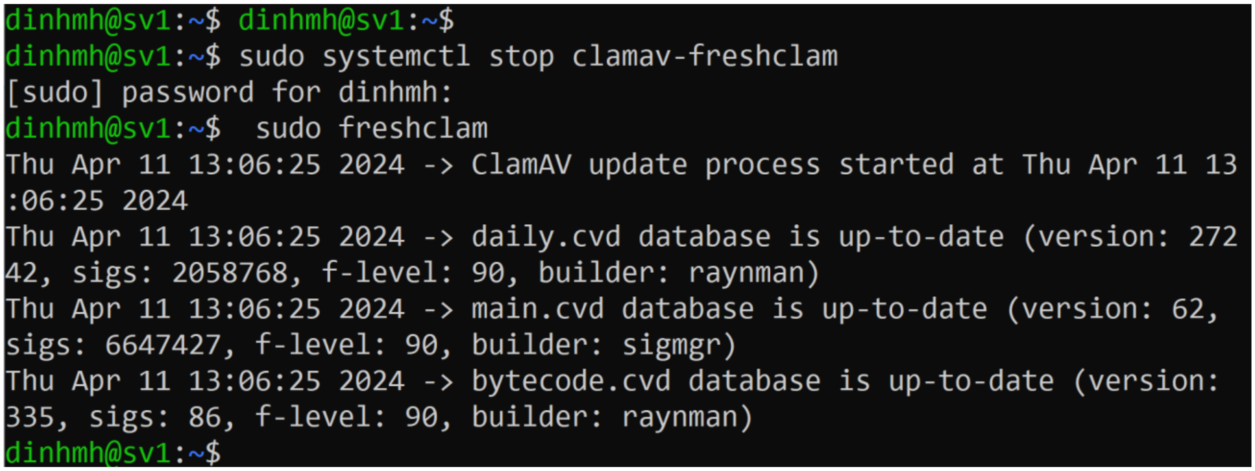
```
dinhmh@sv1:~$ sudo systemctl stop clamav-freshclam
[sudo] password for dinhmh:
dinhmh@sv1:~$
```

The “freshclam” service has been stopped

Download Updates Using freshclam (First Method)

The first convenient way is to download the latest signature database update using “freshclam” via the superuser privileges, i.e., “sudo” command:

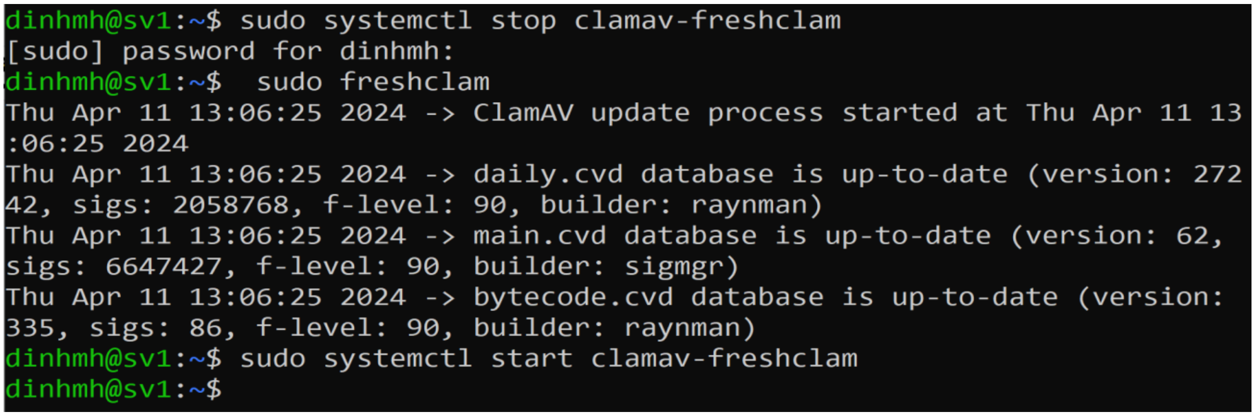
sudo freshclam



```
dinhmh@sv1:~$ dinhmh@sv1:~$
dinhmh@sv1:~$ sudo systemctl stop clamav-freshclam
[sudo] password for dinhmh:
dinhmh@sv1:~$  sudo freshclam
Thu Apr 11 13:06:25 2024 -> ClamAV update process started at Thu Apr 11 13
:06:25 2024
Thu Apr 11 13:06:25 2024 -> daily.cvd database is up-to-date (version: 272
42, sigs: 2058768, f-level: 90, builder: raynman)
Thu Apr 11 13:06:25 2024 -> main.cvd database is up-to-date (version: 62,
sigs: 6647427, f-level: 90, builder: sigmgr)
Thu Apr 11 13:06:25 2024 -> bytecode.cvd database is up-to-date (version:
335, sigs: 86, f-level: 90, builder: raynman)
dinhmh@sv1:~$
```

The output shows that the installed “ClamAV” database is up to date.

When all the updates are downloaded, start/enable the “freshclam” service again with the help of the “systemctl” command:



```
dinhmh@sv1:~$ sudo systemctl stop clamav-freshclam
[sudo] password for dinhmh:
dinhmh@sv1:~$  sudo freshclam
Thu Apr 11 13:06:25 2024 -> ClamAV update process started at Thu Apr 11 13
:06:25 2024
Thu Apr 11 13:06:25 2024 -> daily.cvd database is up-to-date (version: 272
42, sigs: 2058768, f-level: 90, builder: raynman)
Thu Apr 11 13:06:25 2024 -> main.cvd database is up-to-date (version: 62,
sigs: 6647427, f-level: 90, builder: sigmgr)
Thu Apr 11 13:06:25 2024 -> bytecode.cvd database is up-to-date (version:
335, sigs: 86, f-level: 90, builder: raynman)
dinhmh@sv1:~$ sudo systemctl start clamav-freshclam
dinhmh@sv1:~$
```

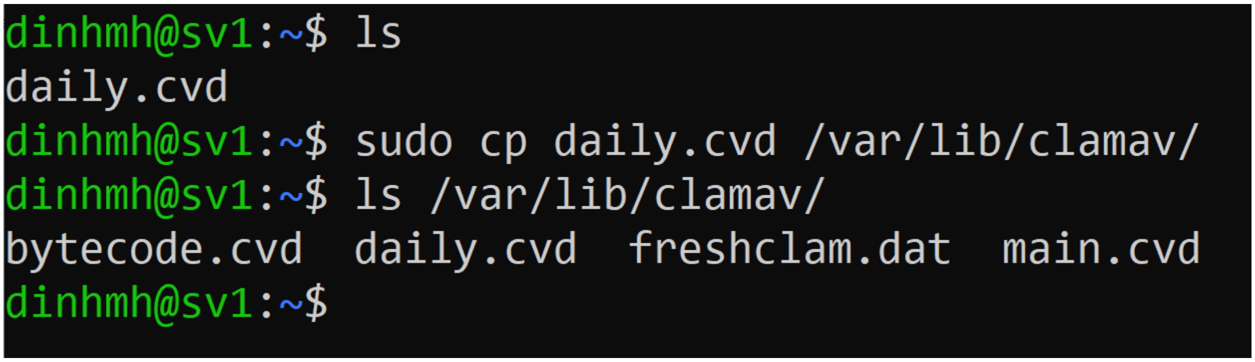
Download Updates Using Official Website (Second Method)

Another way is to download the “ClamAV” database from its official website https://database.clamav.net/daily.cvd

Click on the provided link, and it downloads the “daily.cvd” file.

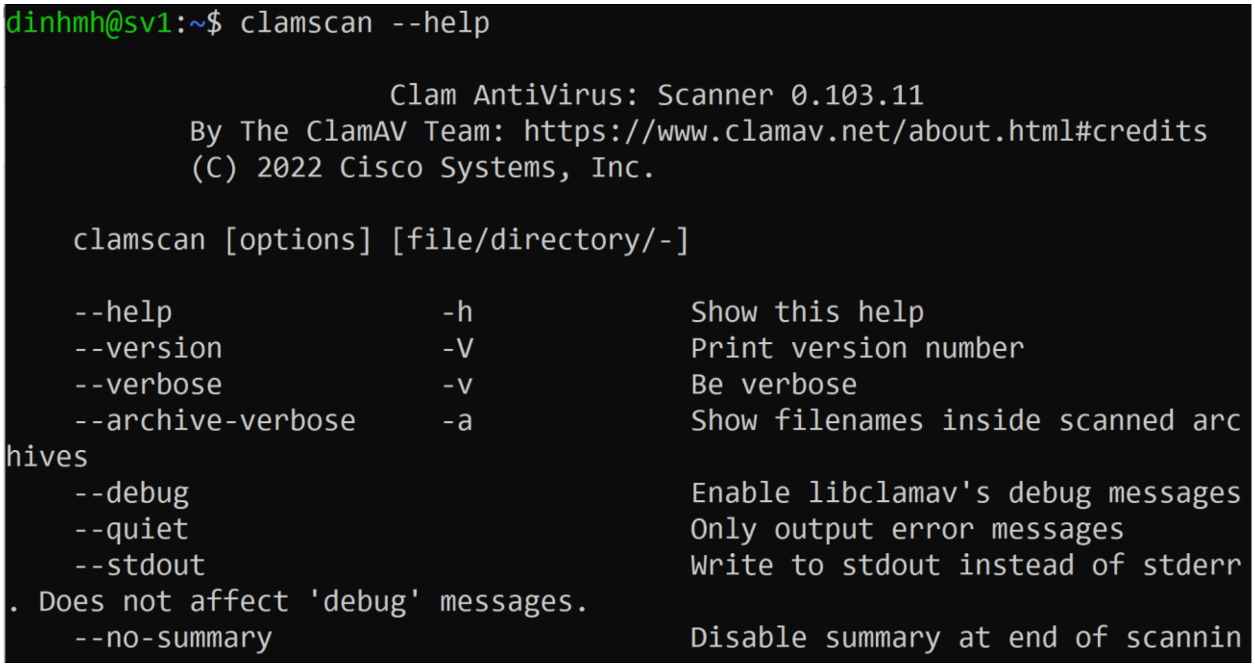
Copy the “daily.cvd” file into the “var/lib/clamav” file through the copy command “cp”:

sudo cp daily.cvd /var/lib/clamav/



```
dinhmh@sv1:~$ ls
daily.cvd
dinhmh@sv1:~$ sudo cp daily.cvd /var/lib/clamav/
dinhmh@sv1:~$ ls /var/lib/clamav/
bytecode.cvd  daily.cvd  freshclam.dat  main.cvd
dinhmh@sv1:~$
```

The “clamscan” provides a wide range of options that can be seen through its “help” command:

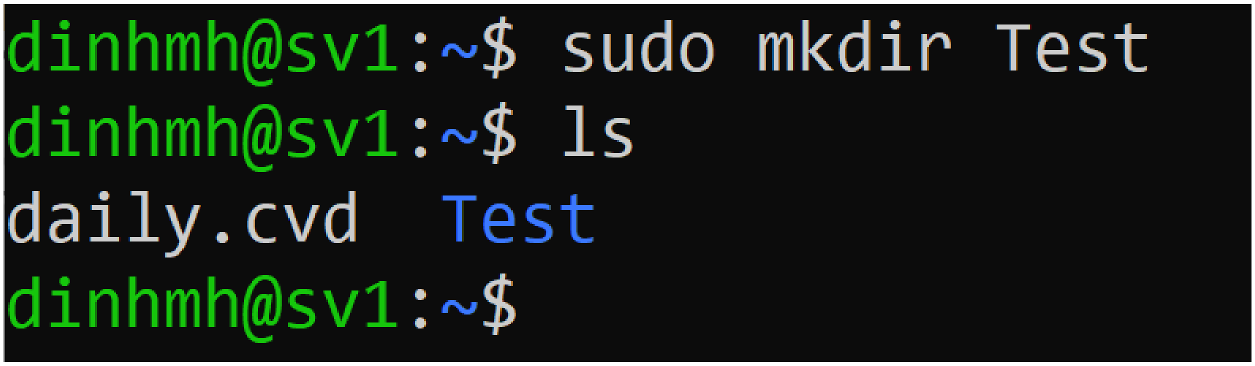


```
dinhmh@sv1:~$ clamscan --help

                       Clam AntiVirus: Scanner 0.103.11
           By The ClamAV Team: https://www.clamav.net/about.html#credits
           (C) 2022 Cisco Systems, Inc.

    clamscan [options] [file/directory/-]

    --help                -h             Show this help
    --version             -V             Print version number
    --verbose             -v             Be verbose
    --archive-verbose     -a             Show filenames inside scanned arc
hives
    --debug                              Enable libclamav's debug messages
    --quiet                              Only output error messages
    --stdout                             Write to stdout instead of stderr
. Does not affect 'debug' messages.
    --no-summary                         Disable summary at end of scannin
```

Scan a Directory

Execute the “clamscan” command with the “sudo” combination to scan the “Documents” directory “–recursive (including subdirectories)” in this format:

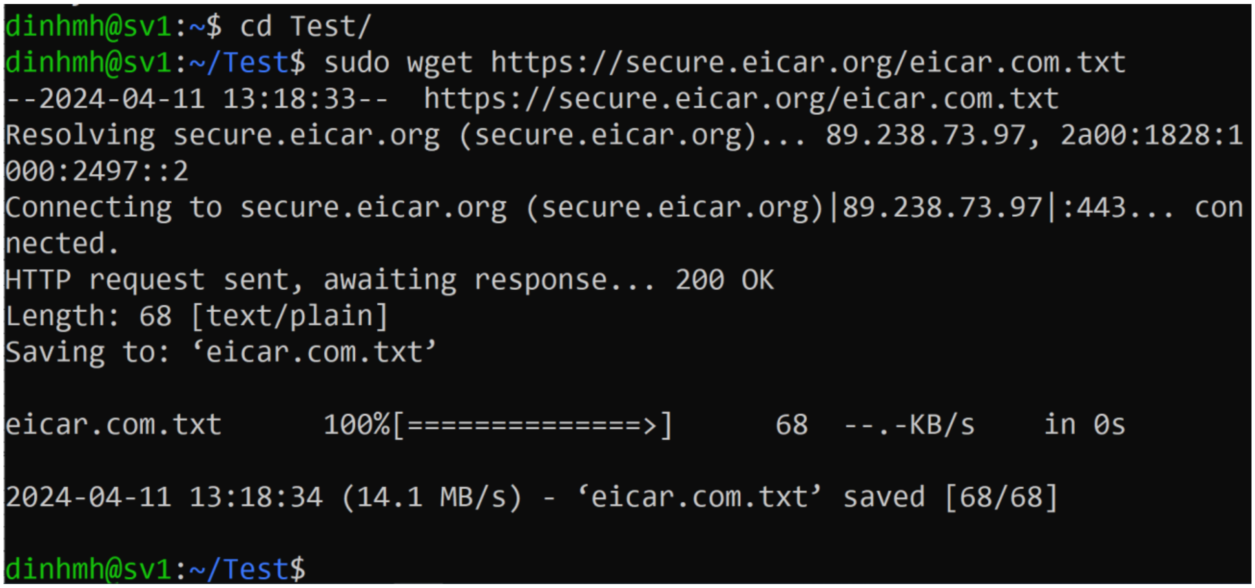
Create a Test folder for testing



```
dinhmh@sv1:~$ sudo mkdir Test
dinhmh@sv1:~$ ls
daily.cvd  Test
dinhmh@sv1:~$
```

Download a malicious code on https://secure.eicar.org/ to test

sudo wget https://secure.eicar.org/eicar.com.txt

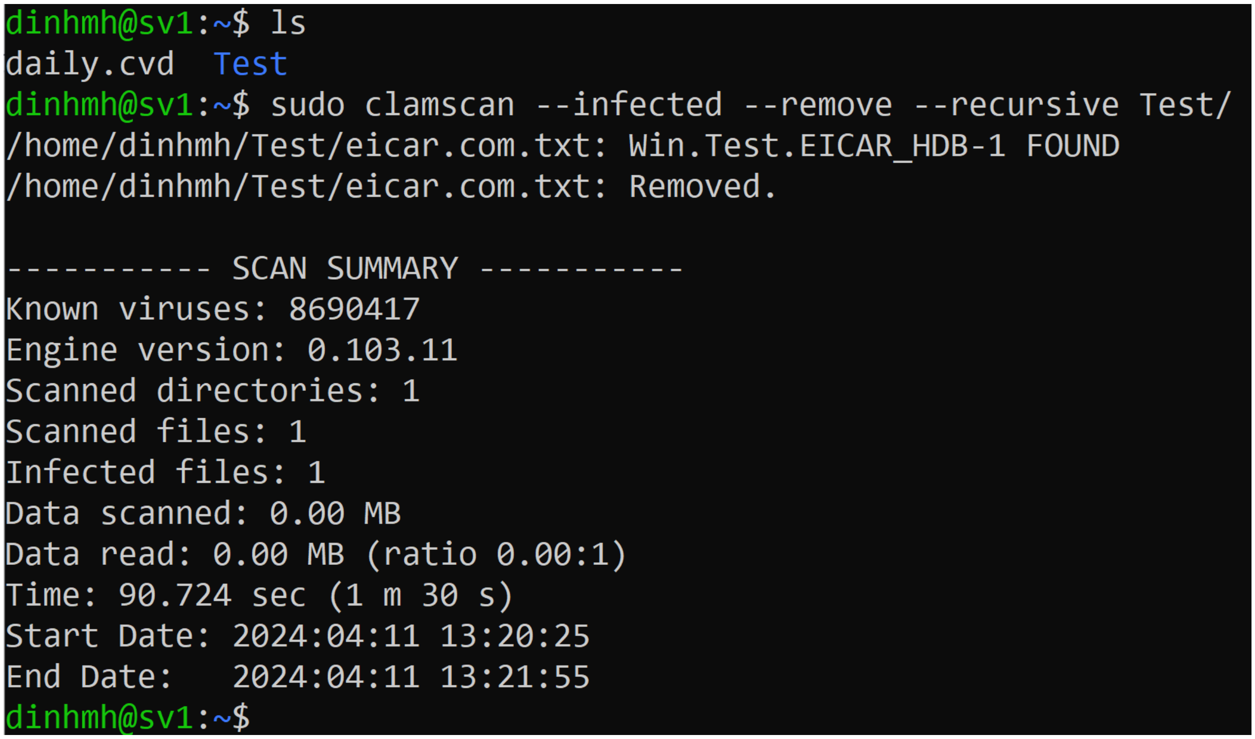


```
dinhmh@sv1:~$ cd Test/
dinhmh@sv1:~/Test$ sudo wget https://secure.eicar.org/eicar.com.txt
--2024-04-11 13:18:33--  https://secure.eicar.org/eicar.com.txt
Resolving secure.eicar.org (secure.eicar.org)... 89.238.73.97, 2a00:1828:1
000:2497::2
Connecting to secure.eicar.org (secure.eicar.org)|89.238.73.97|:443... con
nected.
HTTP request sent, awaiting response... 200 OK
Length: 68 [text/plain]
Saving to: ‘eicar.com.txt’

eicar.com.txt      100%[==============>]      68  --.-KB/s    in 0s

2024-04-11 13:18:34 (14.1 MB/s) - ‘eicar.com.txt’ saved [68/68]

dinhmh@sv1:~/Test$
```

Scan a Directory

Execute the “clamscan” command with the “sudo” combination to scan the “Documents” directory “–recursive (including subdirectories)” in this format:

sudo clamscan --infected --remove --recursive Test/

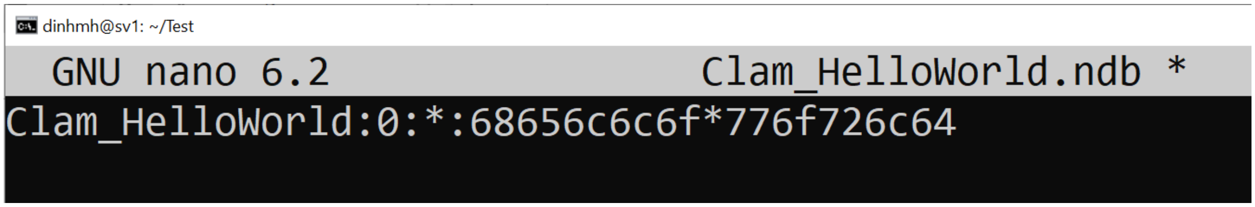


```
dinhmh@sv1:~$ ls
daily.cvd  Test
dinhmh@sv1:~$ sudo clamscan --infected --remove --recursive Test/
/home/dinhmh/Test/eicar.com.txt: Win.Test.EICAR_HDB-1 FOUND
/home/dinhmh/Test/eicar.com.txt: Removed.

----------- SCAN SUMMARY -----------
Known viruses: 8690417
Engine version: 0.103.11
Scanned directories: 1
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 90.724 sec (1 m 30 s)
Start Date: 2024:04:11 13:20:25
End Date:   2024:04:11 13:21:55
dinhmh@sv1:~$
```

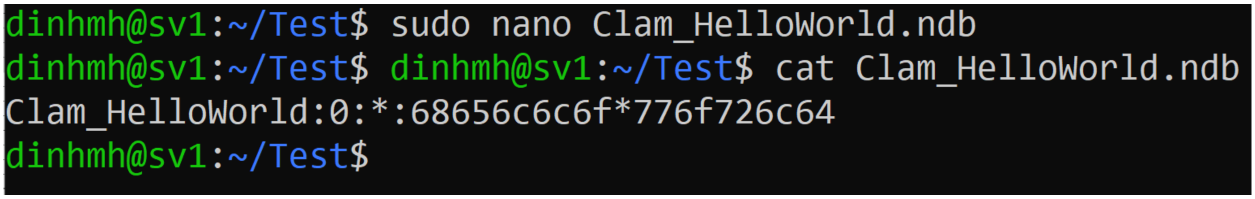
Use this command to create a signature for clamav:

sudo nano Clam_HelloWorld.ndb

Then we enter this Clam_HelloWorld:0:*:68656c6c6f*776f726c64 into the file Clam_HelloWorld.ndb. (This file will be signed so that ClamAV can scan the file, specifically if any txt file contains the words "hello" and the word "world" it will be considered to be injected with malicious code)

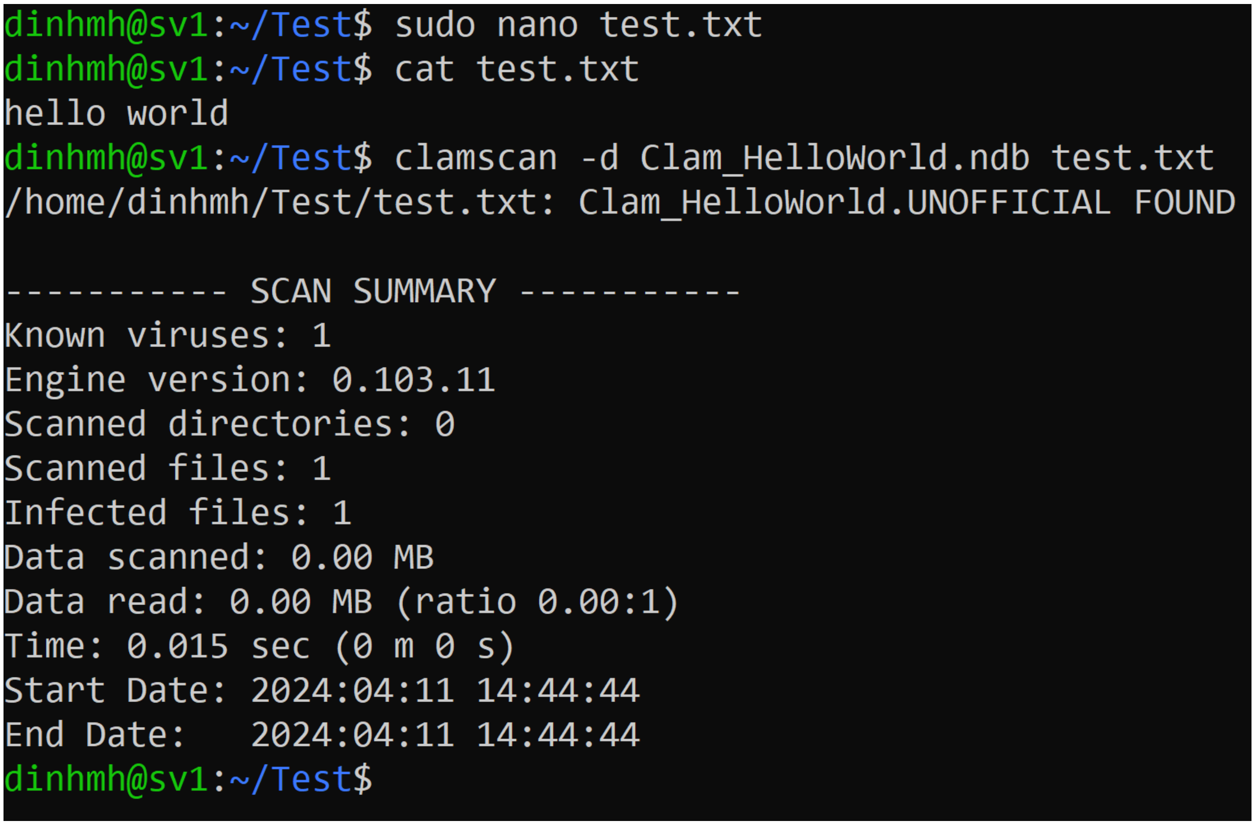


```
  GNU nano 6.2                    Clam_HelloWorld.ndb *
Clam_HelloWorld:0:*:68656c6c6f*776f726c64
```



```
dinhmh@sv1:~/Test$ sudo nano Clam_HelloWorld.ndb
dinhmh@sv1:~/Test$ dinhmh@sv1:~/Test$ cat Clam_HelloWorld.ndb
Clam_HelloWorld:0:*:68656c6c6f*776f726c64
dinhmh@sv1:~/Test$
```

Next, we create the file **test.txt** with the command **sudo nano test.txt**, this file will contain 2 words "hello world". Then we use this command to scan: ***clamscan -d Clam_HelloWorld.ndb test.txt***



```
dinhmh@sv1:~/Test$ sudo nano test.txt
dinhmh@sv1:~/Test$ cat test.txt
hello world
dinhmh@sv1:~/Test$ clamscan -d Clam_HelloWorld.ndb test.txt
/home/dinhmh/Test/test.txt: Clam_HelloWorld.UNOFFICIAL FOUND

----------- SCAN SUMMARY -----------
Known viruses: 1
Engine version: 0.103.11
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 0.015 sec (0 m 0 s)
Start Date: 2024:04:11 14:44:44
End Date:   2024:04:11 14:44:44
dinhmh@sv1:~/Test$
```