University of Science and Technology of Hanoi

ICT department

Administration of Computer Systems

Trinh Quoc Hieu (BI10-060)

University of Science and Technology of Hanoi

Hanoi, Feb 2022

Table of Contents

1. What is ClamAv

Clam AntiVirus (ClamAV) is a free and open source command line interface antivirus software program. It is used to detect trojans and malicious softwares including viruses. It can scan files quickly and can scan over one million viruses and trojans. One of its main uses is to scan emails on mail gateways. ClamAV is supported by the following Linux Operating Systems Ubuntu (16.04, 18.04), Debian (7,8), CentOS (6,7). In this blog we will discuss how to install and use ClamAV in Ubuntu.

2. Requirements

- FreeBSD/x86
- Linux/{x86,x86_64,ppc}
- Mac OS X/{x86,ppc}
- Solaris/sparcv9
- Windows/x86 using mingw32 or Visual Studio

The following packages are required to compile the ClamAV Bytecode Compiler:

- GCC C and C++ compilers (minimum 4.1.3, recommended: 4.3.4 or newer
- Perl (version 5.6.0+)
- GNU make (version 3.79+, recommended 3.81)

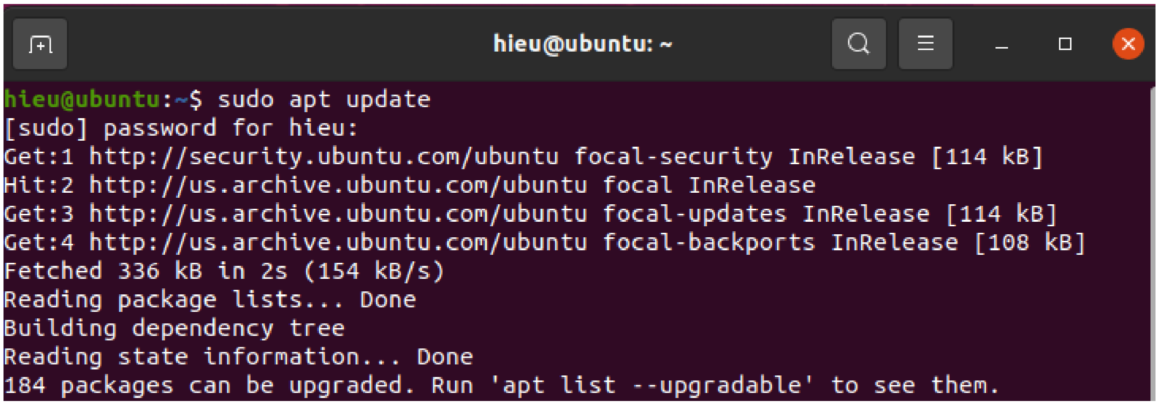
The following packages are optional, but highly recommended:

- Python (version 2.5.4+?) - for running the tests

3. How to install ClamAv

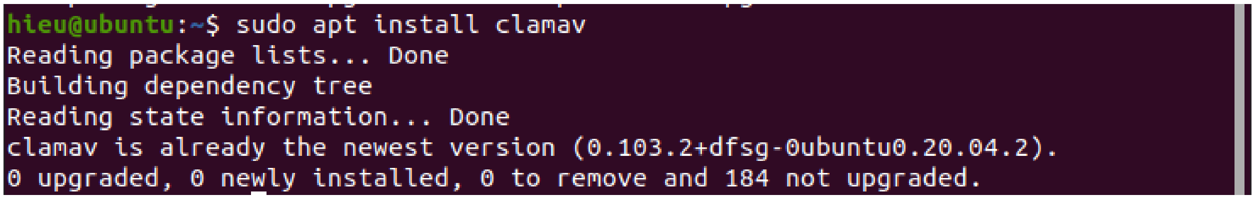
1st way : Install by pip install

Step 1: update repository of unbutu



```
hieu@ubuntu:~$ sudo apt update
[sudo] password for hieu:
Get:1 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Hit:2 http://us.archive.ubuntu.com/ubuntu focal InRelease
Get:3 http://us.archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Fetched 336 kB in 2s (154 kB/s)
Reading package lists... Done
Building dependency tree
Reading state information... Done
184 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

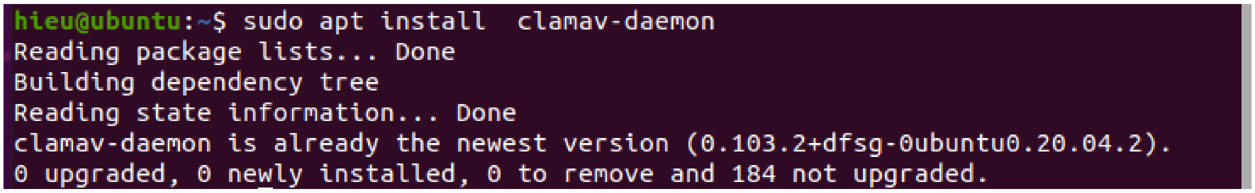
Step 2 : Install ClamAv



```
hieu@ubuntu:~$ sudo apt install clamav
Reading package lists... Done
Building dependency tree
Reading state information... Done
clamav is already the newest version (0.103.2+dfsg-0ubuntu0.20.04.2).
0 upgraded, 0 newly installed, 0 to remove and 184 not upgraded.
```

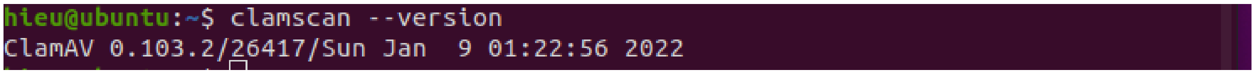
I have install it before so in this step system check ClamAv

Step 3 : Install Clamd (system)



```
hieu@ubuntu:~$ sudo apt install  clamav-daemon
Reading package lists... Done
Building dependency tree
Reading state information... Done
clamav-daemon is already the newest version (0.103.2+dfsg-0ubuntu0.20.04.2).
0 upgraded, 0 newly installed, 0 to remove and 184 not upgraded.
```

Step 4: Check the system

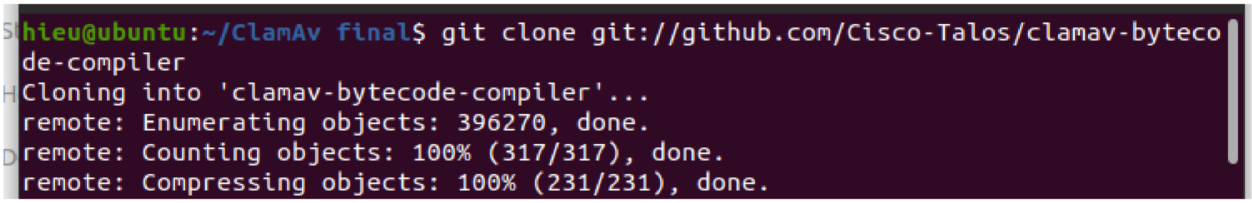


```
hieu@ubuntu:~$ clamscan --version
ClamAV 0.103.2/26417/Sun Jan  9 01:22:56 2022
```

2nd ClamAV Bytecode Compiler

Step 1: Getting the bytecode compiler repository

git clone git://github.com/Cisco-Talos/clamav-bytecode-compiler



```
hieu@ubuntu:~/ClamAv final$ git clone git://github.com/Cisco-Talos/clamav-byteco
de-compiler
Cloning into 'clamav-bytecode-compiler'...
remote: Enumerating objects: 396270, done.
remote: Counting objects: 100% (317/317), done.
remote: Compressing objects: 100% (231/231), done.
```

Step 2 : Quick start for building & installing

Requirements

LLVM and Clang, version 8 or newer

LLVM and Clang versions must match.

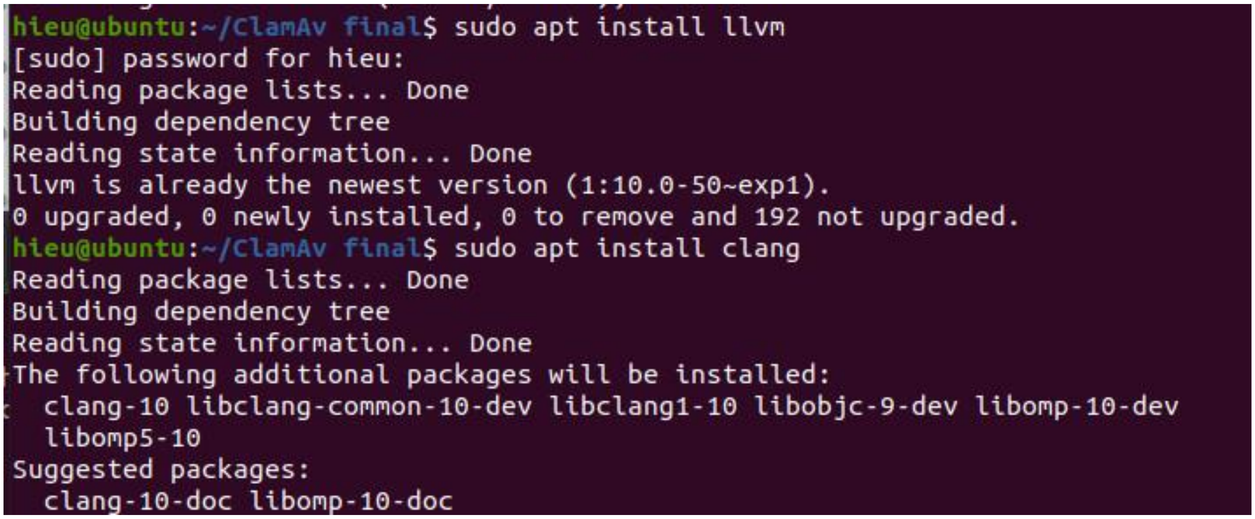
Version 8 is preferred, tested. Newer versions are not guaranteed to work correctly.

LLVM is required to build the bytecode compiler.

Clang is required to run the bytecode compiler.

Python 3.6 or newer.

Python is required to run the unit tests, and to run the bytecode compiler.

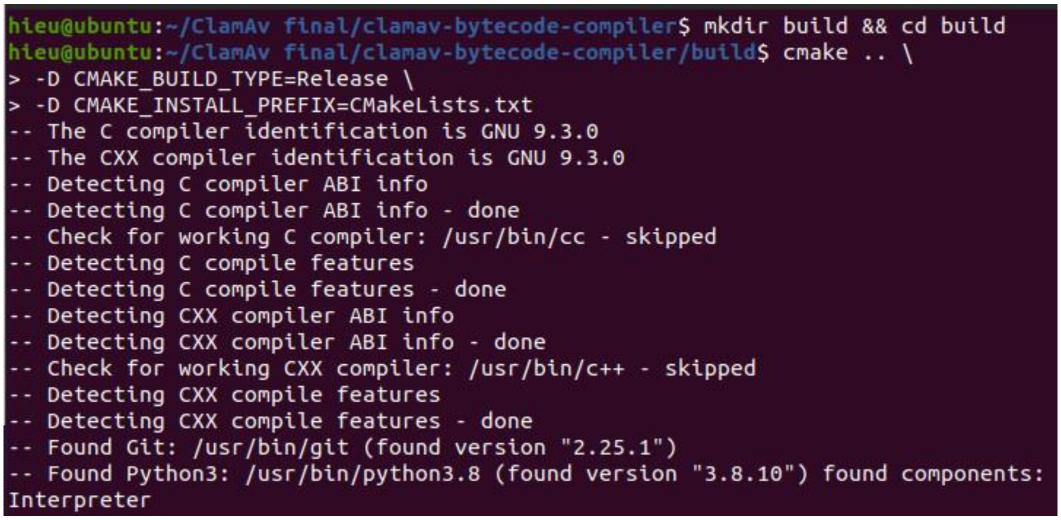


```
hieu@ubuntu:~/ClamAv final$ sudo apt install llvm
[sudo] password for hieu:
Reading package lists... Done
Building dependency tree
Reading state information... Done
llvm is already the newest version (1:10.0-50~exp1).
0 upgraded, 0 newly installed, 0 to remove and 192 not upgraded.
hieu@ubuntu:~/ClamAv final$ sudo apt install clang
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  clang-10 libclang-common-10-dev libclang1-10 libobjc-9-dev libomp-10-dev
  libomp5-10
Suggested packages:
  clang-10-doc libomp-10-doc
```

Step 3: Build & Install

Configure:

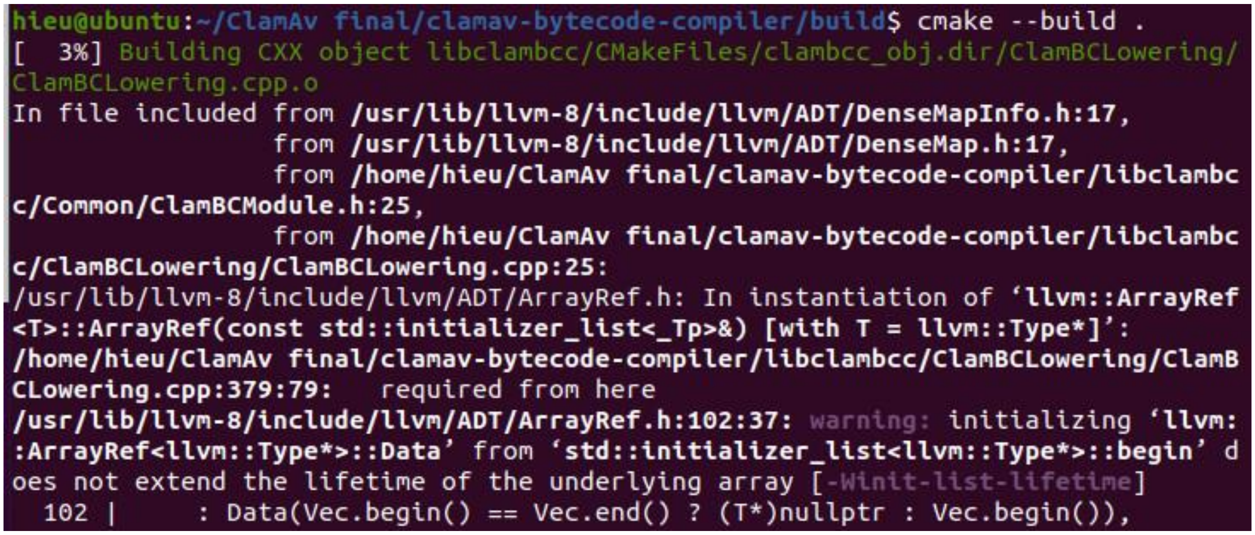
```
mkdir build && cd build

cmake .. \

    -D CMAKE_BUILD_TYPE=Release \

    -D CMAKE_INSTALL_PREFIX=<install path>
```



```
hieu@ubuntu:~/ClamAv final/clamav-bytecode-compiler$ mkdir build && cd build
hieu@ubuntu:~/ClamAv final/clamav-bytecode-compiler/build$ cmake .. \
> -D CMAKE_BUILD_TYPE=Release \
> -D CMAKE_INSTALL_PREFIX=CMakeLists.txt
-- The C compiler identification is GNU 9.3.0
-- The CXX compiler identification is GNU 9.3.0
-- Detecting C compiler ABI info
-- Detecting C compiler ABI info - done
-- Check for working C compiler: /usr/bin/cc - skipped
-- Detecting C compile features
-- Detecting C compile features - done
-- Detecting CXX compiler ABI info
-- Detecting CXX compiler ABI info - done
-- Check for working CXX compiler: /usr/bin/c++ - skipped
-- Detecting CXX compile features
-- Detecting CXX compile features - done
-- Found Git: /usr/bin/git (found version "2.25.1")
-- Found Python3: /usr/bin/python3.8 (found version "3.8.10") found components:
Interpreter
```

Step 4 : Build:

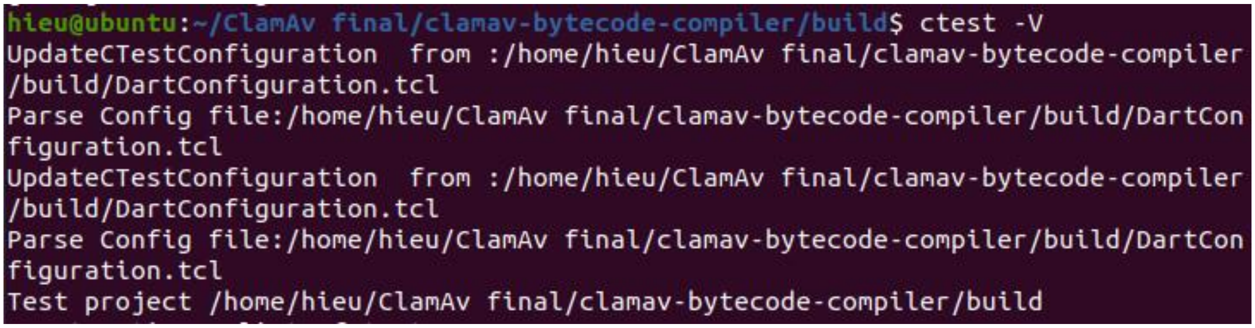
cmake --build .



```
hieu@ubuntu:~/ClamAv final/clamav-bytecode-compiler/build$ cmake --build .
[  3%] Building CXX object libclambcc/CMakeFiles/clambcc_obj.dir/ClamBCLowering/
ClamBCLowering.cpp.o
In file included from /usr/lib/llvm-8/include/llvm/ADT/DenseMapInfo.h:17,
                 from /usr/lib/llvm-8/include/llvm/ADT/DenseMap.h:17,
                 from /home/hieu/ClamAv final/clamav-bytecode-compiler/libclambc
c/Common/ClamBCModule.h:25,
                 from /home/hieu/ClamAv final/clamav-bytecode-compiler/libclambc
c/ClamBCLowering/ClamBCLowering.cpp:25:
/usr/lib/llvm-8/include/llvm/ADT/ArrayRef.h: In instantiation of ‘llvm::ArrayRef
<T>::ArrayRef(const std::initializer_list<_Tp>&) [with T = llvm::Type*]’:
/home/hieu/ClamAv final/clamav-bytecode-compiler/libclambcc/ClamBCLowering/ClamB
CLowering.cpp:379:79:   required from here
/usr/lib/llvm-8/include/llvm/ADT/ArrayRef.h:102:37: warning: initializing ‘llvm:
:ArrayRef<llvm::Type*>::Data’ from ‘std::initializer_list<llvm::Type*>::begin’ d
oes not extend the lifetime of the underlying array [-Winit-list-lifetime]
  102 |     : Data(Vec.begin() == Vec.end() ? (T*)nullptr : Vec.begin()),
```

Step 5 : Test:

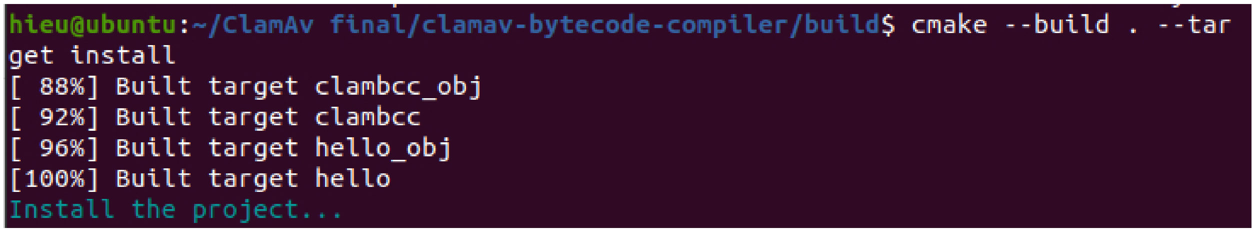
ctest –V



```
hieu@ubuntu:~/ClamAv final/clamav-bytecode-compiler/build$ ctest -V
UpdateCTestConfiguration  from :/home/hieu/ClamAv final/clamav-bytecode-compiler
/build/DartConfiguration.tcl
Parse Config file:/home/hieu/ClamAv final/clamav-bytecode-compiler/build/DartCon
figuration.tcl
UpdateCTestConfiguration  from :/home/hieu/ClamAv final/clamav-bytecode-compiler
/build/DartConfiguration.tcl
Parse Config file:/home/hieu/ClamAv final/clamav-bytecode-compiler/build/DartCon
figuration.tcl
Test project /home/hieu/ClamAv final/clamav-bytecode-compiler/build
```

Step 6 : Install:

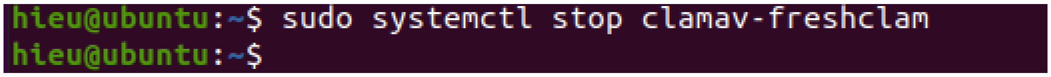
cmake --build . --target install



```
hieu@ubuntu:~/ClamAv final/clamav-bytecode-compiler/build$ cmake --build . --tar
get install
[ 88%] Built target clambcc_obj
[ 92%] Built target clambcc
[ 96%] Built target hello_obj
[100%] Built target hello
Install the project...
```

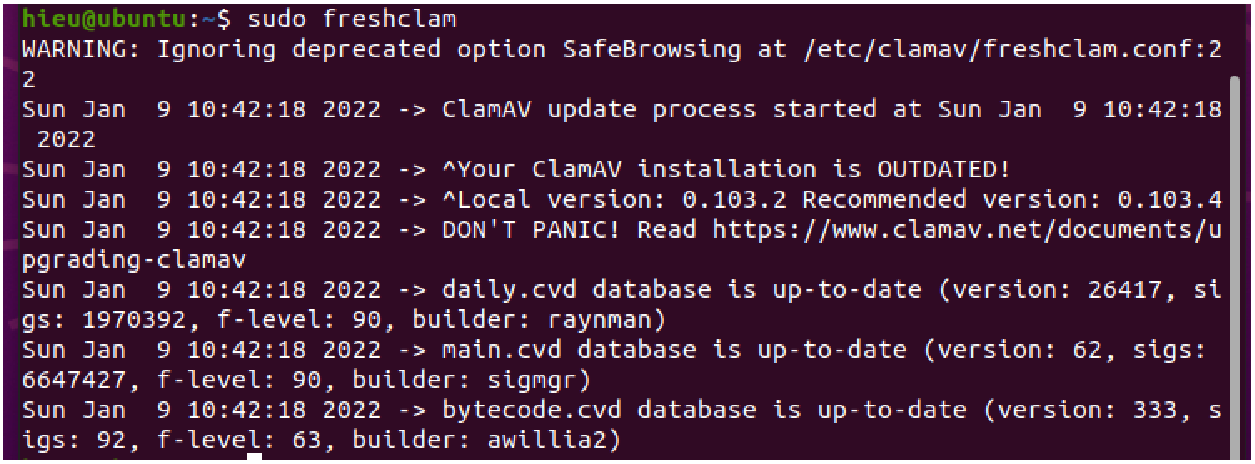
4. How to use ClamAv on system
   1st way

Step 1 : Stop clamav-freshclam service after we install



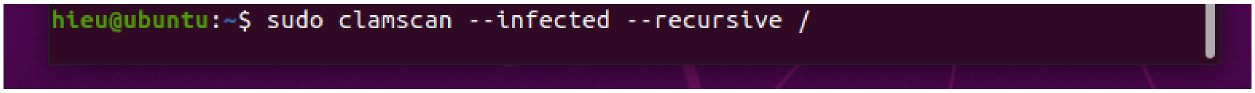
```
hieu@ubuntu:~$ sudo systemctl stop clamav-freshclam
hieu@ubuntu:~$
```

Step 2 : Run fresh-clam to update the new data about malware



```
hieu@ubuntu:~$ sudo freshclam
WARNING: Ignoring deprecated option SafeBrowsing at /etc/clamav/freshclam.conf:2
2
Sun Jan  9 10:42:18 2022 -> ClamAV update process started at Sun Jan  9 10:42:18
 2022
Sun Jan  9 10:42:18 2022 -> ^Your ClamAV installation is OUTDATED!
Sun Jan  9 10:42:18 2022 -> ^Local version: 0.103.2 Recommended version: 0.103.4
Sun Jan  9 10:42:18 2022 -> DON'T PANIC! Read https://www.clamav.net/documents/u
pgrading-clamav
Sun Jan  9 10:42:18 2022 -> daily.cvd database is up-to-date (version: 26417, si
gs: 1970392, f-level: 90, builder: raynman)
Sun Jan  9 10:42:18 2022 -> main.cvd database is up-to-date (version: 62, sigs:
6647427, f-level: 90, builder: sigmgr)
Sun Jan  9 10:42:18 2022 -> bytecode.cvd database is up-to-date (version: 333, s
igs: 92, f-level: 63, builder: awillia2)
```

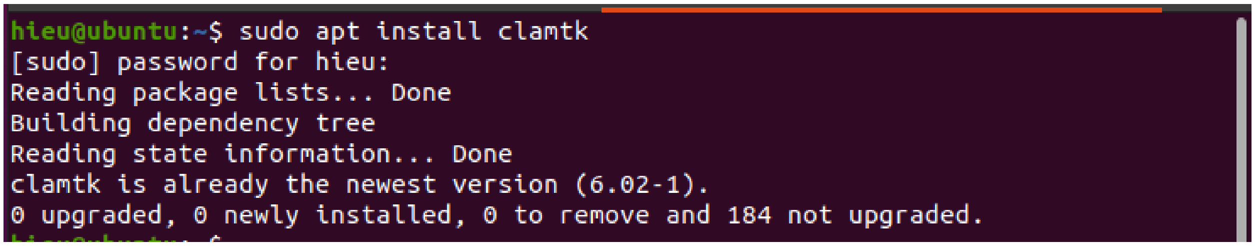
Step 3 : Scan (we scan all system so it take long time)



```
hieu@ubuntu:~$ sudo clamscan --infected --recursive /
```

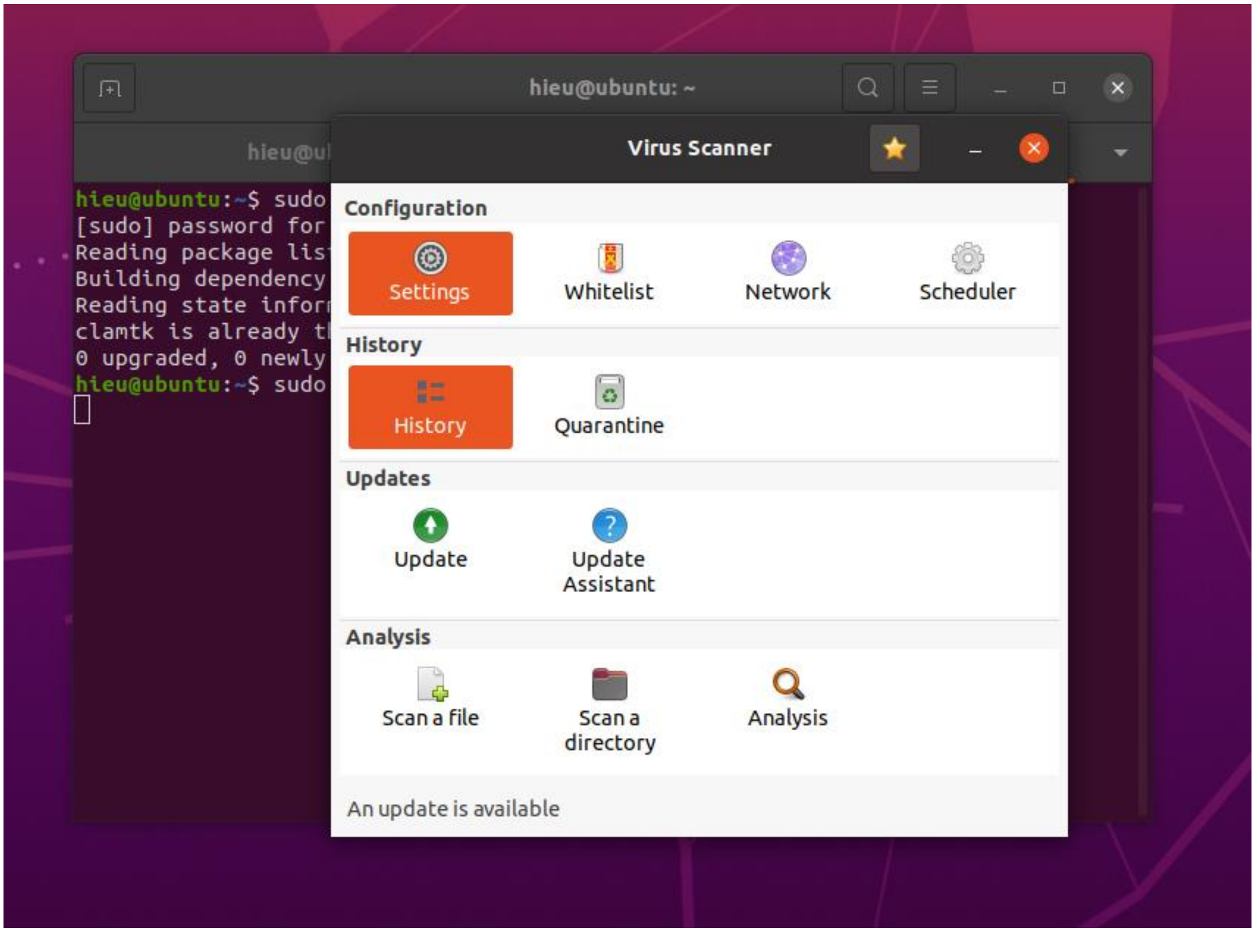
2nd way

Step 1 : We install ClamTk –ClamAv with UI , it easy to use



```
hieu@ubuntu:~$ sudo apt install clamtk
[sudo] password for hieu:
Reading package lists... Done
Building dependency tree
Reading state information... Done
clamtk is already the newest version (6.02-1).
0 upgraded, 0 newly installed, 0 to remove and 184 not upgraded.
hieu@ubuntu:~$
```

Step 2 : Run ClamTk

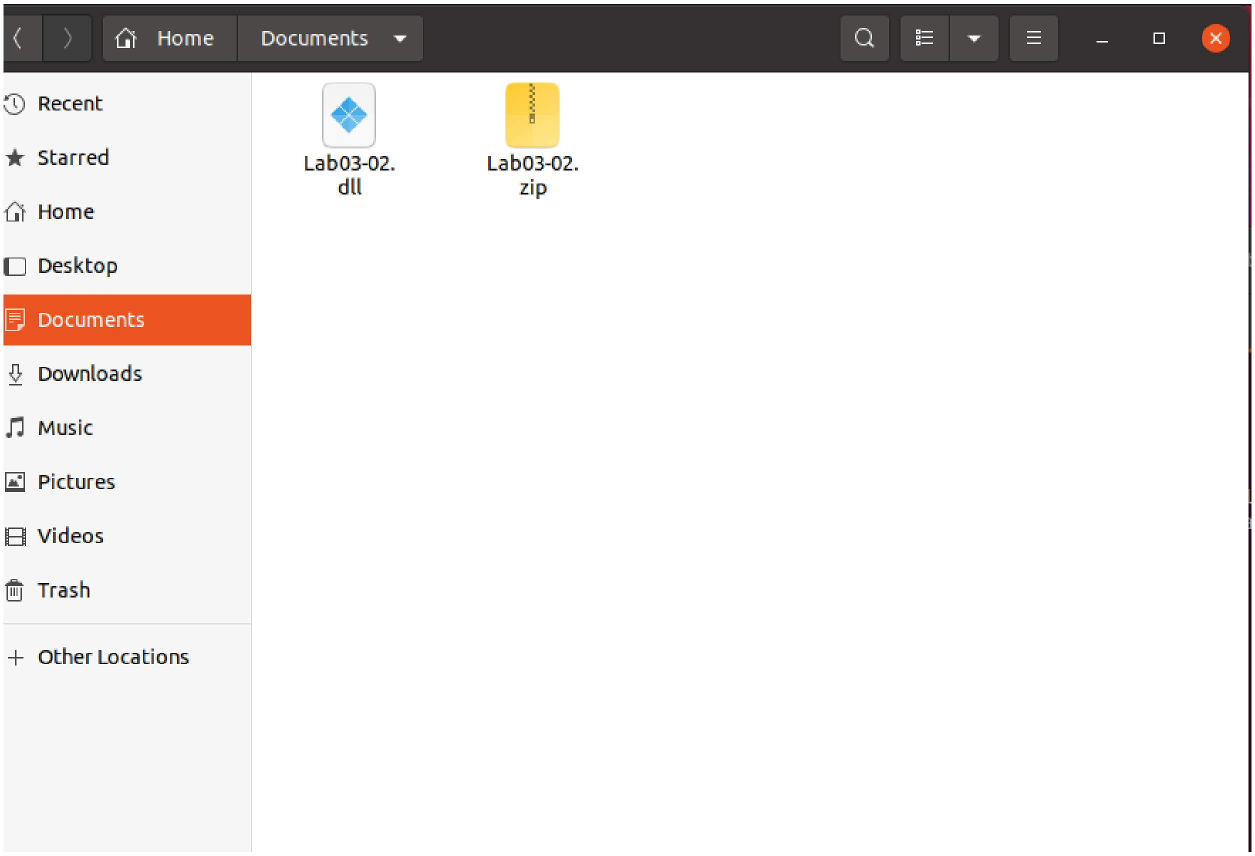


```
hieu@ubuntu:~$ sudo
[sudo] password for
Reading package lis
Building dependency
Reading state infor
clamtk is already t
0 upgraded, 0 newly
hieu@ubuntu:~$ sudo
```

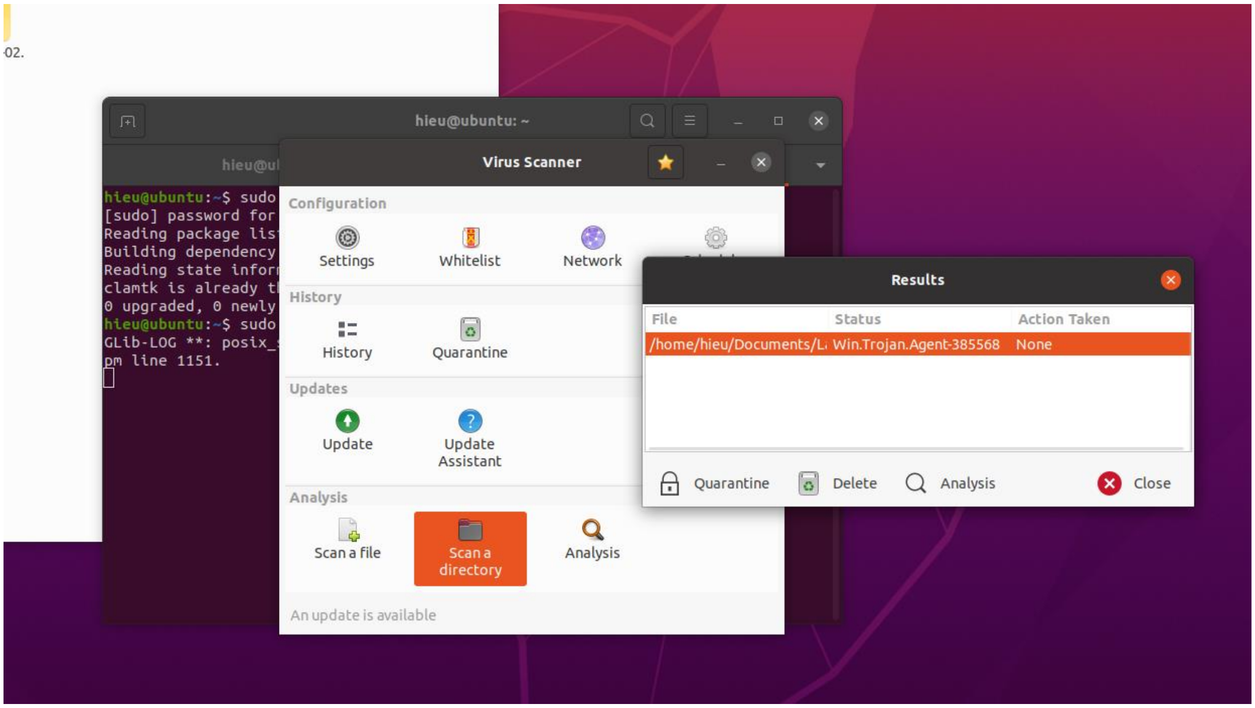
An update is available

5. Demo

We download malware to test ClamAv

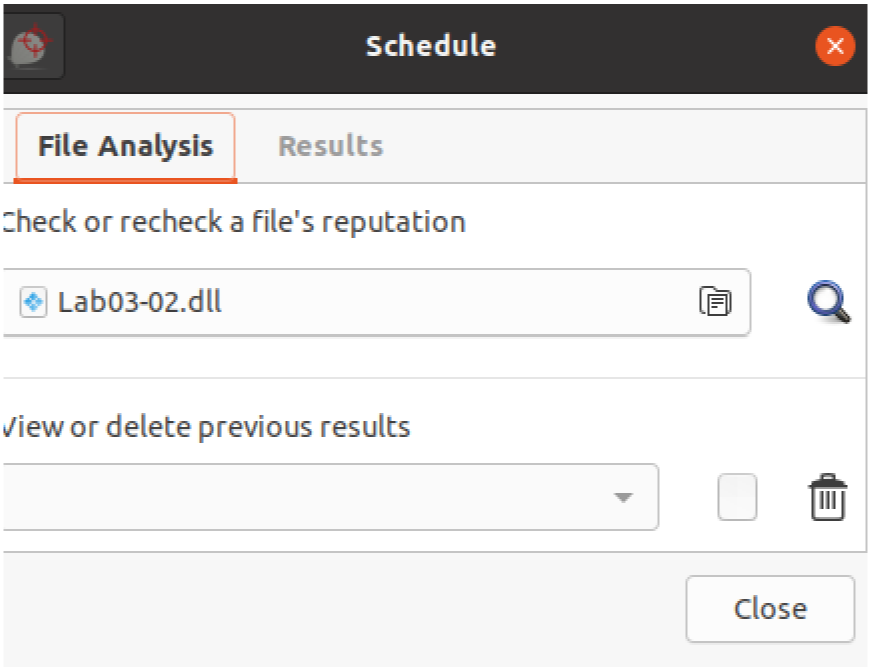


We scan file with ClamAv



```
hieu@ubuntu:~$ sudo
[sudo] password for
Reading package lis
Building dependency
Reading state infor
clamtk is already t
0 upgraded, 0 newly
hieu@ubuntu:~$ sudo
GLib-LOG **: posix_
pm line 1151.
```

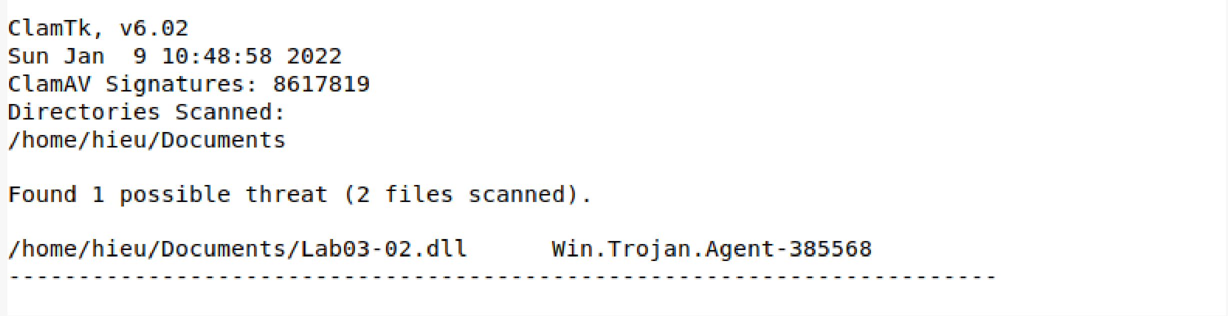
File	Status	Action Taken
/home/hieu/Documents/L	Win.Trojan.Agent-385568	None



Check or recheck a file's reputation

Lab03-02.dll

View or delete previous results



```
ClamTk, v6.02
Sun Jan  9 10:48:58 2022
ClamAV Signatures: 8617819
Directories Scanned:
/home/hieu/Documents

Found 1 possible threat (2 files scanned).

/home/hieu/Documents/Lab03-02.dll      Win.Trojan.Agent-385568
-----------------------------------------------------------------------
```