

Lab #4: ClamAV - Yara

Course Name: Malware Analysis and Reverse Engineering (IAM302)

Student Name: Nguyễn Trần Vinh – SE160258

Instructor Name: Mai Hoàng Đỉnh

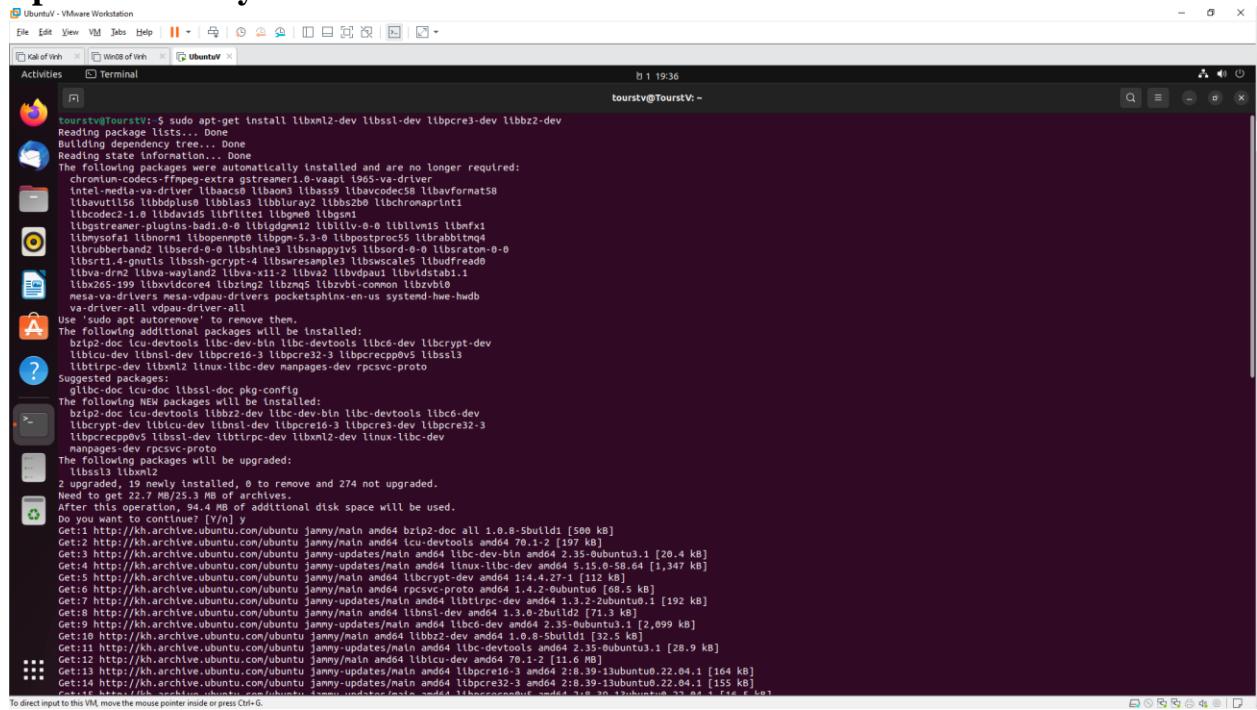
Lab Due Date: 1/2/2023

Purpose

Install ClamAV, Yara and scan file

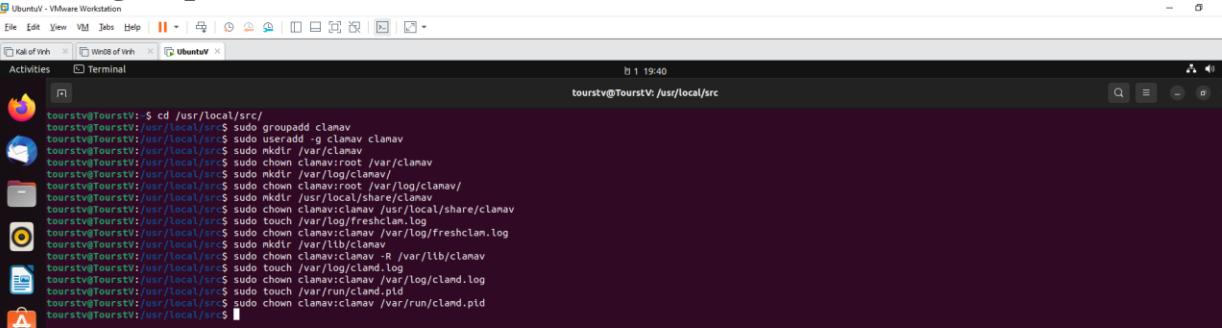
PART 1: ClamAV

Update Library:



```
tourstv@TourstV:~$ sudo apt-get install libxml2-dev libssl-dev libpcres3-dev libbz2-dev
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi 1965-va-driver
intel-media-va-driver libbacon0 libbass9 libavcodec58 libavformat58
libavutil56 libbdplus libblas1 libbluray2 libbs2b libchromaprint1
libcodec2-1.0 libdavids libflite1 libgme9 libgs1
libgstaudio0 libgstbase0.10-0 libgstgdkpixbuf0.10-0 liblwn15 libmf1
libmxf0.1 libnouveau libopenvg0.5.3.0 libpspcore55 librbltnq4
librubberband2 libserd-0.4 libshn1 libsnappyv5 libssord-0.0 libsrat0.0-0
libstt1.4-gnutls libssh-gcrypt-4 libwsresample3 libwscale5 libubfread0
libvba-driv2 libvba-wayland2 libvba-x11-2 libvba libvdpau libvldstab1.1
libx265-199 libxvidcore libzmq5 libzvbi-common libzb10
mesa-dri-drivers mesa-vdpau drivers pocketsphinx-en-us systemd-hwe-hwdb
v4l-dkms all video-dkms-all
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
bztp2-doc icu-devtools libc-dev-bin libc-devtools libca-dev libcrypt-dev
libcu-dev libns1-dev libpcres3-3 libpcres3-3 libpcrespp0v5 libss1
libtipc-dev libts12 linux-lbc-dev manpages-dev rpcsvc-proto
Some packages:
glibc-doc icu-doc libssl1-doc pkg-config
The following NEW packages will be installed:
bztp2-doc icu-devtools libbz2-dev libc-dev-bin libc-devtools libbc6-dev
libcrypt-dev libicu-dev libns1-dev libpcres3-3 libpcres3-3
libcredpv-dev libts12 libtipc-dev libtxmt2-dev linux-lbc-dev
manpages-dev rpcsvc-proto
The following packages will be upgraded:
libss1 libxml2
2 upgraded, 19 newly installed, 0 to remove and 274 not upgraded.
Need to get 22.7 MB/25.3 MB of archives.
Do you want to continue [Y/n] y
additional disk space will be used.
Do you want to continue [Y/n] y
Get:1 http://kh.archive.ubuntu.com/ubuntu jammy/main amd64 bztp2-doc all 1.0.8-5build1 [500 kB]
Get:2 http://kh.archive.ubuntu.com/ubuntu jammy/main amd64 icu-devtools amd64 70.1-2 [197 kB]
Get:3 http://kh.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libc-dev-bin amd64 2.35-0ubuntu3.1 [20.4 kB]
Get:4 http://kh.archive.ubuntu.com/ubuntu jammy-updates/main amd64 linux-libc-dev amd64 5.15.0-58.64 [1,347 kB]
Get:5 http://kh.archive.ubuntu.com/ubuntu jammy/main amd64 libcrore3-3 amd64 1.0.0-1 [10.5 kB]
Get:6 http://kh.archive.ubuntu.com/ubuntu jammy/main amd64 rpcsvc-proto amd64 1.4.2-0ubuntu6 [60.5 kB]
Get:7 http://kh.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libtipc-dev amd64 1.3.2-2ubuntu0.1 [192 kB]
Get:8 http://kh.archive.ubuntu.com/ubuntu jammy/main amd64 libns1-dev amd64 1.3.0-2build2 [75.3 kB]
Get:9 http://kh.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libbc6-dev amd64 2.35-0ubuntu3.1 [2,099 kB]
Get:10 http://kh.archive.ubuntu.com/ubuntu jammy/main amd64 libbz2-dev amd64 1.0.8-5build1 [32.5 kB]
Get:11 http://kh.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libcrore3-3 amd64 1.0.0-1 [10.5 kB]
Get:12 http://kh.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libicu-dev amd64 70.1-2 [11.6 kB]
Get:13 http://kh.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libpcres3-1 amd64 2:0.39-13ubuntu0.22.04.1 [164 kB]
Get:14 http://kh.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libpcres3-2-3 amd64 2:0.39-13ubuntu0.22.04.1 [155 kB]
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi 1965-va-driver
intel-media-va-driver libbacon0 libbass9 libavcodec58 libavformat58
libavutil56 libbdplus libblas1 libbluray2 libbs2b libchromaprint1
libcodec2-1.0 libdavids libflite1 libgme9 libgs1
libgstaudio0 libgstbase0.10-0 libgstgdkpixbuf0.10-0 liblwn15 libmf1
libmxf0.1 libnouveau libopenvg0.5.3.0 libpspcore55 librbltnq4
librubberband2 libserd-0.4 libshn1 libsnappyv5 libssord-0.0 libsrat0.0-0
libstt1.4-gnutls libssh-gcrypt-4 libwsresample3 libwscale5 libubfread0
libvba-driv2 libvba-wayland2 libvba-x11-2 libvba libvdpau libvldstab1.1
libx265-199 libxvidcore libzmq5 libzvbi-common libzb10
mesa-dri-drivers mesa-vdpau drivers pocketsphinx-en-us systemd-hwe-hwdb
v4l-dkms all video-dkms-all
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
bztp2-doc icu-devtools libc-dev-bin libc-devtools libbc6-dev
libcrypt-dev libicu-dev libns1-dev libpcres3-3 libpcres3-3 libpcrespp0v5 libss1
libtipc-dev libts12 libtipc-dev libtxmt2-dev linux-lbc-dev manpages-dev rpcsvc-proto
Some packages:
glibc-doc icu-doc libssl1-doc pkg-config
The following NEW packages will be installed:
bztp2-doc icu-devtools libbz2-dev libc-dev-bin libc-devtools libbc6-dev
libcrypt-dev libicu-dev libns1-dev libpcres3-3 libpcres3-3 libpcrespp0v5 libss1
libtipc-dev libts12 libtipc-dev libtxmt2-dev linux-lbc-dev manpages-dev rpcsvc-proto
The following packages will be upgraded:
libss1 libxml2
2 upgraded, 19 newly installed, 0 to remove and 274 not upgraded.
Need to get 22.7 MB/25.3 MB of archives.
Do you want to continue [Y/n] y
additional disk space will be used.
```

Create group, user and folder:



Kali of win Wind of win UbuntuV

Activities Terminal

tourstv@TourstV: ~

```
tourstv@TourstV: ~
```

```
tourstv@TourstV: $ cd /usr/local/src/
tourstv@TourstV: /usr/local/src$ sudo groupadd clamav
tourstv@TourstV: /usr/local/src$ sudo useradd -g clamav clamav
tourstv@TourstV: /usr/local/src$ sudo cp /usr/share/clamav/clamavd /var/log/clamav
tourstv@TourstV: /usr/local/src$ sudo chown clamav:root /var/log/clamav
tourstv@TourstV: /usr/local/src$ sudo mkdir /var/log/clamav/
tourstv@TourstV: /usr/local/src$ sudo chmod clamav:root /var/log/clamav/
tourstv@TourstV: /usr/local/src$ sudo chmod clamav:clamav /usr/local/share/clamav
tourstv@TourstV: /usr/local/src$ sudo chmod clamav:clamav /var/log/clamav.log
tourstv@TourstV: /usr/local/src$ sudo chmod clamav:clamav /var/log/clamscan.log
tourstv@TourstV: /usr/local/src$ sudo chmod clamav:clamav /var/lib/clamav
tourstv@TourstV: /usr/local/src$ sudo chmod clamav:clamav -R /var/lib/clamav
tourstv@TourstV: /usr/local/src$ sudo touch /var/log/clamd.log
tourstv@TourstV: /usr/local/src$ sudo chmod clamav:clamav /var/log/clamd.log
tourstv@TourstV: /usr/local/src$ sudo touch /var/run/clamd.pid
tourstv@TourstV: /usr/local/src$ sudo chmod clamav:clamav /var/run/clamd.pid
tourstv@TourstV: /usr/local/src$
```

Move file clamav-0.103.7.tar.gz from /home/touristv/Download to /usr/local/src

```
tourstv@TourstV:~/usr/local/src$ sudo mv /home/tourstv/Downloads/clamav-0.103.7.tar.gz .
tourstv@TourstV:~/usr/local/src$ sudo tar -xvf clamav-0.103.7.tar.gz
clamav-0.103.7//aclocal.m4
clamav-0.103.7//configure.ac
clamav-0.103.7//etc/freshclam.conf.sample
clamav-0.103.7//etc/clamd.conf.sample
clamav-0.103.7//etc/Makefile.am
clamav-0.103.7//etc/Makefile.in
clamav-0.103.7//etc/hosts.dbs.txt
clamav-0.103.7//COPYING
clamav-0.103.7//Config/
clamav-0.103.7//config/test-driver
clamav-0.103.7//config/lmain.sh
clamav-0.103.7//config/missing
clamav-0.103.7//config/config.guess
clamav-0.103.7//config/config.sub
clamav-0.103.7//config/config.rpath
clamav-0.103.7//config/install-sh
clamav-0.103.7//config/ar-lib
clamav-0.103.7//config/dcomp
clamav-0.103.7//config/compile
Clamav-0.103.7//config/ykwrap
clamav-0.103.7//shared/
clamav-0.103.7//shared/linux/
clamav-0.103.7//shared/linux/cert_util_linux.c
clamav-0.103.7//shared/linux/.deps/
clamav-0.103.7//shared/linux/.deps/cert_util_linux.Plo
clamav-0.103.7//shared/msc.h
clamav-0.103.7//shared/Makefile
clamav-0.103.7//shared/cert_util.h
clamav-0.103.7//shared/fdpassing.h
clamav-0.103.7//shared/hostid.c
clamav-0.103.7//shared/hostid.h
clamav-0.103.7//shared/.deps/
clamav-0.103.7//shared/.deps/getopt.Plo
clamav-0.103.7//shared/.deps/actions.Plo
clamav-0.103.7//shared/.deps/optparser.Plo
clamav-0.103.7//shared/.deps/counter.Plo
clamav-0.103.7//shared/.deps/cdiff.Plo
clamav-0.103.7//shared/.deps/cert_util.Plo
clamav-0.103.7//shared/.deps/msc.Plo
clamav-0.103.7//shared/.deps/hostid.Plo
clamav-0.103.7//shared/.deps/clandcmd.Plo
clamav-0.103.7//shared/.deps/dmef_logging.Plo
clamav-0.103.7//shared/cdiff/
clamav-0.103.7//shared/cdiff.c
clamav-0.103.7//shared/cdiff.h
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Unzip file

```
tourstv@TourstV:~/usr/local/src$ sudo mv /home/tourstv/Downloads/clamav-0.103.7.tar.gz .
tourstv@TourstV:~/usr/local/src$ sudo tar -xvf clamav-0.103.7.tar.gz
clamav-0.103.7//aclocal.m4
clamav-0.103.7//configure.ac
clamav-0.103.7//etc/freshclam.conf.sample
clamav-0.103.7//etc/clamd.conf.sample
clamav-0.103.7//etc/Makefile.am
clamav-0.103.7//etc/Makefile.in
clamav-0.103.7//etc/hosts.dbs.txt
clamav-0.103.7//COPYING
clamav-0.103.7//Config/
clamav-0.103.7//config/test-driver
clamav-0.103.7//config/lmain.sh
clamav-0.103.7//config/missing
clamav-0.103.7//config/config.guess
clamav-0.103.7//config/config.sub
clamav-0.103.7//config/config.rpath
clamav-0.103.7//config/install-sh
clamav-0.103.7//config/ar-lib
clamav-0.103.7//config/dcomp
clamav-0.103.7//config/compile
Clamav-0.103.7//config/ykwrap
clamav-0.103.7//shared/
clamav-0.103.7//shared/linux/
clamav-0.103.7//shared/linux/cert_util_linux.c
clamav-0.103.7//shared/linux/.deps/
clamav-0.103.7//shared/linux/.deps/cert_util_linux.Plo
clamav-0.103.7//shared/msc.h
clamav-0.103.7//shared/Makefile
clamav-0.103.7//shared/cert_util.h
clamav-0.103.7//shared/fdpassing.h
clamav-0.103.7//shared/hostid.c
clamav-0.103.7//shared/hostid.h
clamav-0.103.7//shared/.deps/
clamav-0.103.7//shared/.deps/getopt.Plo
clamav-0.103.7//shared/.deps/actions.Plo
clamav-0.103.7//shared/.deps/optparser.Plo
clamav-0.103.7//shared/.deps/counter.Plo
clamav-0.103.7//shared/.deps/cdiff.Plo
clamav-0.103.7//shared/.deps/cert_util.Plo
clamav-0.103.7//shared/.deps/msc.Plo
clamav-0.103.7//shared/.deps/hostid.Plo
clamav-0.103.7//shared/.deps/clandcmd.Plo
clamav-0.103.7//shared/.deps/dmef_logging.Plo
clamav-0.103.7//shared/cdiff/
clamav-0.103.7//shared/cdiff.c
clamav-0.103.7//shared/cdiff.h
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

List all file

```
File Edit View VM Jobs Help ||| Terminal tourstv@TourstV: /usr/local/src
```

Activities Terminal 0.1 20:40

```
clanav-0.103.7/clamonacc/Makefile.am
clanav-0.103.7/clamonacc/Makefile.in
clanav-0.103.7/clamonacc/scan/
clanav-0.103.7/clamonacc/scan/onas_queue.c
clanav-0.103.7/clamonacc/scan/onythread.h
clanav-0.103.7/clamonacc/scan/onas_queue.h
clanav-0.103.7/clamonacc/scan/thread.c
clanav-0.103.7/clamonacc/scan/thread.h
clanav-0.103.7/clamonacc/ChkElsts.txt
clanav-0.103.7/clamonacc/c-thread-pool/
clanav-0.103.7/clamonacc/c-thread-pool/tphpool.h
clanav-0.103.7/clamonacc/c-thread-pool/tphpool.c
clanav-0.103.7/clamonacc/fanotif/
clanav-0.103.7/clamonacc/fanotif/fanotif.h
clanav-0.103.7/clamonacc/fanotif/fanotif.c
clanav-0.103.7/clamonacc/client/
clanav-0.103.7/clamonacc/client/socket.c
clanav-0.103.7/clamonacc/client/socket.h
clanav-0.103.7/clamonacc/client/communication.c
clanav-0.103.7/clamonacc/client/protocol.h
clanav-0.103.7/clamonacc/client/client.c
clanav-0.103.7/clamonacc/client/socket.h
clanav-0.103.7/clamonacc/client/client.h
clanav-0.103.7/clamonacc/client/communication.h
clanav-0.103.7/clamonacc/clamav-clamonacc.service.in
clanav-0.103.7/clamonacc/misc/
clanav-0.103.7/clamonacc/misc/utils.h
clanav-0.103.7/clamonacc/misc/priv_fts.h
clanav-0.103.7/clamonacc/misc/fts.c
clanav-0.103.7/configure
clanav-0.103.7/database/
clanav-0.103.7/database/daily.csv
clanav-0.103.7/database/Makefile.am
clanav-0.103.7/database/Makefile.in
clanav-0.103.7/database/main.csv
clanav-0.103.7/configure-a
tourstv@TourstV: /usr/local/src$ ls -lah
total 68M
drwxr-xr-x  6 root  root  4.0K  1 20:39 .
drwxr-xr-x  27 root  root  4.0K  1 20:39 ..
drwxrwxr-x 27 clanav  clanav  4.0K  20:17 clamav-0.100.1
-rw-rw-r--  1 tourstv tourstv 16M  1 19:55 clamav-0.100.1.tar.gz
drwxrwxr-x 31 clanav  1005 4.0K  26 2022 clamav-0.103.7
-rw-rw-r--  1 tourstv tourstv 16M  1 20:37 clamav-0.103.7.tar.gz
drwxr-xr-x 30 root  root  4.0K  1 19:44 clamav-0.105.1
-rw-rw-r--  1 tourstv tourstv 16M  1 19:44 clamav-0.105.1.tar.gz
drwxrwxr-x 18 root  root  4.0K  20:13 openssl-1.1.1
-rw-r--r--  1 root  root  8.5M  28 2019 openssl-1.1.1c.tar.gz
tourstv@TourstV: /usr/local/src$
```

Go into folder and configure

```

UbuntuV - VMware Workstation
File Edit View VM Jobs Help || Terminal 1 20:40 tourstv@TourstV: /usr/local/src/clamav-0.103.7
Activities Terminal
tourstv@TourstV: /usr/local/src/clamav-0.103.7$ ls -lah
total 1.8M
drwxr-xr-x 31 clamav 1005 4.0K 26 2022 openssl-1.1.1c.tar.gz
tourstv@TourstV: /usr/local/src$ cd clamav-0.103.7/
tourstv@TourstV: /usr/local/src/clamav-0.103.7$ ls -lah
total 1.8M
drwxr-xr-x 1 clamav 1005 4.0K 26 2022 .
drwxr-xr-x 6 root  root  4.0K 26 2022 aclocal.m4
-rw-rw-r-- 1 clamav 1005 56K 26 2022 autogen.sh
-rw-rw-r-- 1 clamav 1005 552 26 2022 ChangeLog.md
-rw-rw-r-- 1 clamav 1005 124 26 2022 clamav-config.h.in
-rw-rw-r-- 1 clamav 1005 17K 26 2022 clamav-config.h.mk
-rw-rw-r-- 1 clamav 1005 1023 26 2022 clamav-config.h.in
drwxrwxr-x 2 clamav 1005 4.0K 26 2022 clamav
drwxrwxr-x 1 clamav 1005 1.9K 26 2022 clamav-types.h.in
-rw-rw-r-- 1 clamav 1005 2.1K 26 2022 clamav-version.h.in
drwxrwxr-x 2 clamav 1005 4.0K 26 2022 clambc
drwxrwxr-x 2 clamav 1005 4.0K 26 2022 clamconf
drwxrwxr-x 2 clamav 1005 4.0K 26 2022 clamd
drwxrwxr-x 2 clamav 1005 4.0K 26 2022 clamdscan
drwxrwxr-x 8 clamav 1005 4.0K 26 2022 clamdstop
drwxrwxr-x 2 clamav 1005 4.0K 26 2022 clamonacc
drwxrwxr-x 2 clamav 1005 4.0K 26 2022 clamscan
drwxrwxr-x 2 clamav 1005 4.0K 26 2022 clamsubmit
drwxrwxr-x 2 clamav 1005 4.0K 26 2022 cmake
drwxrwxr-x 1 clamav 1005 28K 26 2022 CMakeLists.txt
drwxrwxr-x 2 clamav 1005 4.0K 26 2022 CMakeOptions.cmake
drwxrwxr-x 2 clamav 1005 4.0K 26 2022 config
drwxrwxr-x 1 clamav 1005 1.2M 26 2022 configure.ac
drwxrwxr-x 1 clamav 1005 20K 26 2022 COPYING
drwxrwxr-x 1 clamav 1005 1.9K 26 2022 COPYING
drwxrwxr-x 1 clamav 1005 2.1K 26 2022 COPYING.bzip2
-rw-rw-r-- 1 clamav 1005 1.9K 26 2022 COPYING.file
-rw-rw-r-- 1 clamav 1005 1.1K 26 2022 COPYING.getopt
drwxrwxr-x 1 clamav 1005 20K 26 2022 COPYING.LGPL
drwxrwxr-x 1 clamav 1005 20K 26 2022 COPYING.MIT
drwxrwxr-x 1 clamav 1005 217 26 2022 COPYING.LICENSE
drwxrwxr-x 1 clamav 1005 2.5K 26 2022 COPYING.PCRE
drwxrwxr-x 1 clamav 1005 1.8K 26 2022 COPYING.REGEX
drwxrwxr-x 1 clamav 1005 2.4K 26 2022 COPYING.UNRAR
drwxrwxr-x 1 clamav 1005 12K 26 2022 COPYING.VARA
drwxrwxr-x 1 clamav 1005 20K 26 2022 COPYING.lib
drwxrwxr-x 2 clamav 1005 4.0K 26 2022 docs
drwxrwxr-x 4 clamav 1005 4.0K 26 2022 docs
drwxrwxr-x 2 clamav 1005 4.0K 26 2022 etc
drwxrwxr-x 3 clamav 1005 4.0K 26 2022 examples
drwxrwxr-x 2 clamav 1005 4.0K 26 2022 freshclan
drwxrwxr-x 2 clamav 1005 4.0K 26 2022 install
drwxrwxr-x 1 clamav 1005 9.2K 26 2022 INSTALL.autotools.md
-rw-rw-r-- 1 clamav 1005 17K 26 2022 INSTALL.cmake.md
drwxrwxr-x 0 clamav 1005 20K 26 2022 tests
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

UbuntuV - VMware Workstation
File Edit View VM Jobs Help || Terminal 1 20:40 tourstv@TourstV: /usr/local/src/clamav-0.103.7
Activities Terminal
tourstv@TourstV: /usr/local/src/clamav-0.103.7$ sudo ./configure --with-user=clamav --with-group=clamav
checking for g++... g++
checking whether the C++ compiler works... yes
checking for C++ compiler default output file name... a.out
checking for suffix of executables...
checking whether the linker accepts -s... no
checking for suffix of object files... o
checking whether we are using the GNU C++ compiler... yes
checking whether g++ accepts -g... yes
checking build system type... x86_64-pc-linux-gnu
checking host system type... x86_64-pc-linux-gnu
checking target system type... x86_64-pc-linux-gnu
creating target-canonical system defines
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... no
checking for sed... no
checking for make... make
checking whether make sets $(MAKE)... yes
checking for style of include used by make... GNU
checking whether make supports nested variables... yes
checking whether UID '0' is supported by stardt format... yes
checking whether GID '0' is supported by stardt format... yes
checking whether make supports a native -fno-strength-reduce... gnutar
checking dependency style of g++... gcc3
checking whether make supports nested variables... (cached) yes
checking for gcc... gcc
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
testing if compiler accepts -fno-common... none needed
checking whether gcc understands -c and -o together... yes
checking dependency style of gcc... gcc3
checking how to run the C preprocessor... gcc -E
checking for grep that handles long lines and -e... /usr/bin/grep
checking for egrep... /usr/bin/grep -E
checking for ANSI C header files... yes
checking for sys/types.h... yes
checking for sys/stat.h... yes
checking for stdlib.h... yes
checking for string.h... yes
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```

```
tourstv@TourstV: /usr/local/src/clamav-0.103.7$ ./configure
config.status: creating docs/man/clamd.conf
config.status: creating docs/man/clamscan.1
config.status: creating docs/man/clanscan.1
config.status: creating docs/man/freshclam.1
config.status: creating docs/man/freshclam.conf
config.status: creating docs/man/clandtop.1
config.status: creating docs/man/clansubmit.1
config.status: creating clamonacc/makefile
config.status: creating clamonacc/clamav-clamonacc.service
config.status: creating libcurl/makefile
config.status: creating libclamav/makefile
config.status: creating clamav-config.h
config.status: clamav-config.h is unchanged
config.status: creating libclammpack/config.h
config.status: libclammpack/config.h is unchanged
config.status: creating libcurl/config.h
config.status: executing libtool commands
configure: Summary of detected features follows
OS           : linux-gnu
ptthreads    : yes (-pthread)
configure: Summary of miscellaneous features
fanotify     : no (auto)
fdpassing    : 1
IPv6         : yes
openssl      : /usr
libcurl       : /usr
configure: Summary of optional tools
clandtop     : no (missing ncurses / pdcurses) (disabled)
milter       : no (missing libmilter) (disabled)
clansubmit   : no (missing libjson-c-dev. Use the website to submit FPs/FNs.) (disabled)
clamonacc   : yes (auto)
configure: Summary of engine performance features
release mode: yes
llvm          : no (disabled)
mempool      : yes
configure: Summary of engine detection features
iconv        : yes
bztp2         : ok
zlib          : yes (from system)
unrar         : yes
preclass     : no (missing libjson-c-dev) (disabled)
pcre          : /usr
libmpack     : yes (Internal)
libxml2       : yes, from /usr
yara         : yes
fts           : yes (lIBC)
tourstv@TourstV: /usr/local/src/clamav-0.103.7$
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Sudo make command

```
tourstv@TourstV: /usr/local/src/clamav-0.103.7$ sudo make install
Haking install in libltdl
make[1]: Entering directory '/usr/local/src/clamav-0.103.7/libltdl'
make install-am
make[2]: Entering directory '/usr/local/src/clamav-0.103.7/libltdl'
  CC      loaders/dlopen.lo
  CCLD    dlopen_la
ar: 'u' modifier ignored since 'D' is the default (see 'U')
  CC      loaders/lbltdlc_la-preopen.lo
  CC      libltdlc_la-lt_alloc.lo
  CC      libltdlc_la-lt_dloader.lo
  CC      libltdlc_la-lt_error.lo
  CC      libltdlc_la-ltdlo.lo
  CC      libltdlc_la-ltdlist.lo
  CC      lt_stl.lo
  CCLD    libltdlc_la
ar: 'u' modifier ignored since 'D' is the default (see 'U')
make[3]: Entering directory '/usr/local/src/clamav-0.103.7/libltdl'
make[3]: Leaving directory '/usr/local/src/clamav-0.103.7/libltdl'
make[3]: Entering directory '/usr/local/src/clamav-0.103.7/libltdl'
make[3]: Leaving directory '/usr/local/src/clamav-0.103.7/libltdl'
Making install in libclamav
make[1]: Entering directory '/usr/local/src/clamav-0.103.7/libclamav'
make install-recurse
make[2]: Entering directory '/usr/local/src/clamav-0.103.7/libclamav'
make[3]: Entering directory '/usr/local/src/clamav-0.103.7/libclamav'
  CXX    .../libclamunrar/libclamunrar_la-archive.lo
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Check version

```

make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/usr/local/src/clamav-0.103.7/clambc'
make[1]: Leaving directory '/usr/local/src/clamav-0.103.7/clambc'
Making install in unit_tests
make[2]: Entering directory '/usr/local/src/clamav-0.103.7/unit_tests'
make[2]: Nothing to be done for 'install-exec-am'.
make[2]: Leaving directory '/usr/local/src/clamav-0.103.7/unit_tests'
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/usr/local/src/clamav-0.103.7/unit_tests'
make[1]: Leaving directory '/usr/local/src/clamav-0.103.7'
Making install in clamonacc
make[1]: Entering directory '/usr/local/src/clamav-0.103.7/clamonacc'
  CC      clamonacc.o
  CC      client/client.o
  CC      client/protocol.o
  CC      client/communication.o
  CC      client/socket.o
  CC      inotify/inotify.o
  CC      fanotify/fanotify.o
  CC      inotify/hash.o
  CC      misc/utils.o
  CC      scan/thread.o
  CC      scan/onas_queue.o
  CC      c-thread-pool/threadpool.o
c-thread-pool/threadpool.c: In function 'jobqueue_pull':
c-thread-pool/threadpool.c:474:05: warning: implicit declaration of function 'syscall' [-Wimplicit-function-declaration]
    logg("jobqueue_pull: Thread %d pulled last job from queue.\n", syscall(SYS_gettid));
                                         ^
CCLD  clamonacc
make[2]: Entering directory '/usr/local/src/clamav-0.103.7/clamonacc'
/usr/bin/mkdir -p '/usr/local/sbin'
/bin/bash ./libtool --mode=Install /usr/bin/install -c clamonacc '/usr/local/sbin'
libtool: install: /usr/bin/install -c .libs/clamonacc /usr/local/sbin/clamonacc
make[2]: Leaving directory '/usr/local/src/clamav-0.103.7/clamonacc'
make[1]: Entering directory '/usr/local/src/clamav-0.103.7'
make[2]: Entering directory '/usr/local/src/clamav-0.103.7'
toursty@TourstyV:/usr/local/src/clamav-0.103.7$ sudo ldconfig
toursty@TourstyV:/usr/local/src/clamav-0.103.7$ clamscan --version
ClamAV 0.103.7
toursty@TourstyV:/usr/local/src/clamav-0.103.7$ 

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Move clamd.conf.sample to clamd.conf

```

make[1]: Leaving directory '/usr/local/src/clamav-0.103.7/clambc'
Making install in unit_tests
make[2]: Entering directory '/usr/local/src/clamav-0.103.7/unit_tests'
make[2]: Nothing to be done for 'install-exec-am'.
make[2]: Leaving directory '/usr/local/src/clamav-0.103.7/unit_tests'
make[2]: Nothing to be done for 'install-data-am'.
make[2]: Leaving directory '/usr/local/src/clamav-0.103.7/unit_tests'
make[1]: Leaving directory '/usr/local/src/clamav-0.103.7'
Making install in clamonacc
make[1]: Entering directory '/usr/local/src/clamav-0.103.7/clamonacc'
  CC      clamonacc.o
  CC      client/client.o
  CC      client/protocol.o
  CC      client/communication.o
  CC      client/socket.o
  CC      inotify/inotify.o
  CC      fanotify/fanotify.o
  CC      inotify/hash.o
  CC      misc/utils.o
  CC      scan/thread.o
  CC      scan/onas_queue.o
  CC      c-thread-pool/threadpool.o
c-thread-pool/threadpool.c: In function 'jobqueue_pull':
c-thread-pool/threadpool.c:474:05: warning: implicit declaration of function 'syscall' [-Wimplicit-function-declaration]
    logg("jobqueue_pull: Thread %d pulled last job from queue.\n", syscall(SYS_gettid));
                                         ^
CCLD  clamonacc
make[2]: Entering directory '/usr/local/src/clamav-0.103.7/clamonacc'
/usr/bin/mkdir -p '/usr/local/sbin'
/bin/bash ./libtool --mode=Install /usr/bin/install -c clamonacc '/usr/local/sbin'
libtool: install: /usr/bin/install -c .libs/clamonacc /usr/local/sbin/clamonacc
make[2]: Leaving directory '/usr/local/src/clamav-0.103.7/clamonacc'
make[1]: Entering directory '/usr/local/src/clamav-0.103.7'
make[2]: Entering directory '/usr/local/src/clamav-0.103.7'
toursty@TourstyV:/usr/local/src/clamav-0.103.7$ sudo ldconfig
toursty@TourstyV:/usr/local/src/clamav-0.103.7$ clamscan --version
ClamAV 0.103.7
toursty@TourstyV:/usr/local/src/clamav-0.103.7$ cd ../../etc/
toursty@TourstyV:/usr/local/etc$ sudo mv clamd.conf.sample clamd.conf
toursty@TourstyV:/usr/local/etc$ 

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Delete example

UbuntuV - VMware Workstation

Kali of VMs Wind of VMs UbuntuV

Activities Gedit 8:1 20:51

tourstv@TourstV: /usr/local/etc

```

CC      inotify/fanotify.o
CC      fanotify/fanotify.o
CC      inotify/hash.o
CC      misc/utilis
CC      scan/queue.o
CC      scan/queue.o
CC      c-thread-pool/threadpool.o

c-thread-pool/threadpool.c: In function 'jobqueue_pull':
c-thread-pool/threadpool.c:474:105: warning: implicit declaration of function 'logg'
        logg("jobqueue_pull: Thread
        ^

CCLD    clamavacc
make[2]: Entering directory '/usr/local/src/clamav-0.103.7/clamavacc'
/usr/bin/mkdir -p '/usr/local/sbin'
/bin/bash ./libtool --mode=Install /usr/bin/install -c clamavacc '/usr/local/sbin/clamavacc'
libtool: installing '/usr/bin/install -c clamavacc '/usr/local/sbin/clamavacc'
make[2]: Leaving directory '/usr/local/src/clamav-0.103.7/clamavacc'
make[1]: Leaving directory '/usr/local/src/clamav-0.103.7/clamavacc'
make[1]: Entering directory '/usr/local/src/clamav-0.103.7'
make[2]: Entering directory '/usr/local/src/clamav-0.103.7'
/usr/bin/mkdir -p '/usr/local/bin'
/usr/bin/install -c clamav-config '/usr/local/bin'
/usr/bin/install -c -n 644 clamav-types.h '/usr/local/include'
/usr/bin/install -c -n 644 clamav-version.h '/usr/local/include'
/usr/bin/install -c -n 644 libclamav.pc '/usr/local/lib/pkgconfig'
make[2]: Leaving directory '/usr/local/src/clamav-0.103.7'
make[1]: Leaving directory '/usr/local/src/clamav-0.103.7'
tourstv@TourstV:/usr/local/src/clamav-0.103.7$ sudo ldconfig
tourstv@TourstV:/usr/local/src/clamav-0.103.7$ clangscans -version
ClamAV 0.103.7
tourstv@TourstV:/usr/local/src/clamav-0.103.7$ cd ../../etc/
tourstv@TourstV:/usr/local/etc$ sudo mv clamd.conf.sample clamd.conf
tourstv@TourstV:/usr/local/etc$ sudo gedit clamd.conf

(gedit:139793): dconf-WARNING **: 20:50:49.838: failed to commit changes to dconf
(gedit:139793): dconf-WARNING **: 20:50:49.838: failed to commit changes to dconf
(gedit:139793): dconf-WARNING **: 20:50:50.877: failed to commit changes to dconf
(gedit:139793): dconf-WARNING **: 20:50:50.877: failed to commit changes to dconf
(gedit:139793): dconf-WARNING **: 20:50:50.877: failed to commit changes to dconf
(gedit:139793): dconf-WARNING **: 20:50:50.877: failed to commit changes to dconf
** (gedit:139793): WARNING **: 20:51:02.649: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported
** (gedit:139793): WARNING **: 20:51:02.650: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

UbuntuV - VMware Workstation

Kali of VMs Wind of VMs UbuntuV

Activities Gedit 8:1 20:51

tourstv@TourstV: /usr/local/etc

```

Open clamd.conf /usr/local/etc
Save E - X

1## Example config file for the Clam AV daemon
2## Please read the clamd.conf() manual before editing this file.
4##
5
6## Comment or remove the line below.
7## Example
9
10# Uncomment this option to enable logging.
11#LogFile must be writable for the user running daemon.
12# LogFile is required.
13# Default: disabled
14#LogFile /tmp/clamd.log
15
16# By default the log file is locked for writing - the lock protects against
17# multiple clamd instances. If you want to run another clamd, please
18# copy the configuration file, change the Logfile variable, and run
19# the daemon with -c<config-file> option.
20# This option disables log file locking.
21#Default: no
22#LogFileUnlock yes
23
24# Maximum size of the log file.
25# Value of 0 disables the limit.
26# You may use 'M' or 'm' for megabytes (1M = 1m = 1048576 bytes)
27# and 'K' or 'k' for kilobytes (1K = 1k = 1024 bytes). To specify the size
28# in bytes just don't use modifiers. IfLogFileMaxSize is enabled, log
29# rotation (the LogRotate option) will always be enabled.
30# rotation
31#Default: 1M
32#LogFileMaxSize 2M
33# Log time with each message.
34#Default: no
35#LogTime yes
36#Also log clean files. Useful in debugging but drastically increases the
Savingfile"/usr/local/etc/clamd.conf"...
Matlab Tab Width: 8 Ln 1, Col 3 INS
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Kali of VMs Wind of VMs UbuntuV

Activities Gedit 8:1 20:51

tourstv@TourstV: /usr/local/etc

```

Open freshclam.conf /usr/local/etc
Save E - X

1## Example config file for freshclam
2## Please read the freshclam.conf() manual before editing this file.
4##
5
6## Comment or remove the line below.
7## Example
9
10# Path to the database directory.
11# WARNING: It must match clamd.conf's directive!
12# Default: hardcoded (depends on installation options)
13#DatabaseDirectory /var/lib/clamav
14
15# Path to the log file (make sure it has proper permissions)
16#Default: disabled
17#UpdateLogFile /var/log/freshclam.log
18
19# Maximum size of the log file.
20# Value of 0 disables the limit.
21# You may use 'M' or 'm' for megabytes (1M = 1m = 1048576 bytes)
22# and 'K' or 'k' for kilobytes (1K = 1k = 1024 bytes).
23# rotation
24# log rotation (the LogRotate option) will always be enabled.
25#Default: 1M
26#LogFileMaxSize 2M
27
28# Log time with each message.
29#Default: no
30#LogTime yes
31
32# Enable verbose logging.
33#Default: no
34#LogVerbose yes
35
36# Use system logger (can work together with UpdateLogFile).
37#Default: no
Savingfile"/usr/local/etc/freshclam.conf"...
Matlab Tab Width: 8 Ln 1, Col 3 INS
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Install freshclam

```

UbuntuV - VMware Workstation
File Edit View VM Jobs Help | Terminal | Activities | Terminal | tourstv@TourstV: /usr/local/etc
tourstv@TourstV: /usr/local/src/clamav-0.103.7$ sudo ldconfig
tourstv@TourstV: /usr/local/src/clamav-0.103.7$ clamscan --version
ClamAV 0.103.7
tourstv@TourstV: /usr/local/src/clamav-0.103.7$ cd ../etc/
tourstv@TourstV: /usr/local/etc$ sudo mv clamd.conf.sample clamd.conf
tourstv@TourstV: /usr/local/etc$ sudo gedit clamd.conf
(gedit:139793): dconf-WARNING **: 20:50:49.01: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139793): dconf-WARNING **: 20:50:49.01: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139793): dconf-WARNING **: 20:50:50.07: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139793): dconf-WARNING **: 20:50:50.07: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139793): dconf-WARNING **: 20:50:50.07: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139793): dconf-WARNING **: 20:51:02.64: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported
** (gedit:139793): WARNING **: 20:51:02.65: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:139793): WARNING **: 20:51:05.91: Set document metadata failed: Setting attribute metadata::gedit-position not supported
(gedit:139793): dconf-WARNING **: 20:51:05.92: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
tourstv@TourstV: /usr/local/etc$ sudo mv freshclam.conf.sample freshclam.conf
tourstv@TourstV: /usr/local/etc$ sudo gedit freshclam.conf
(gedit:139831): dconf-WARNING **: 20:51:46.20: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139831): dconf-WARNING **: 20:51:46.20: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139831): dconf-WARNING **: 20:51:46.40: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139831): dconf-WARNING **: 20:51:46.40: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139831): dconf-WARNING **: 20:51:46.40: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139831): dconf-WARNING **: 20:51:46.40: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported
** (gedit:139831): WARNING **: 20:51:46.40: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:139831): WARNING **: 20:51:46.40: Set document metadata failed: Setting attribute metadata::gedit-position not supported
(gedit:139831): dconf-WARNING **: 20:51:46.40: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
tourstv@TourstV: /usr/local/etc$ sudo freshclam
ClamAV update process started at Wed Feb 1 20:52:26 2023
daily database available for download (remote version: 26799)
[Line: 2.5s, ETA: 7.1s [=====]] 57.82MB/57.82MB
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

UbuntuV - VMware Workstation
File Edit View VM Jobs Help | Terminal | Activities | Terminal | tourstv@TourstV: /usr/local/etc
tourstv@TourstV: /usr/local/src/clamav-0.103.7$ sudo ldconfig
tourstv@TourstV: /usr/local/src/clamav-0.103.7$ clamscan --version
ClamAV 0.103.7
tourstv@TourstV: /usr/local/src/clamav-0.103.7$ cd ../etc/
tourstv@TourstV: /usr/local/etc$ sudo mv clamd.conf.sample clamd.conf
tourstv@TourstV: /usr/local/etc$ sudo gedit clamd.conf
(gedit:139793): dconf-WARNING **: 20:50:50.07: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139793): dconf-WARNING **: 20:50:50.07: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
** (gedit:139793): WARNING **: 20:51:02.64: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported
** (gedit:139793): WARNING **: 20:51:02.65: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:139793): WARNING **: 20:51:05.91: Set document metadata failed: Setting attribute metadata::gedit-position not supported
(gedit:139793): dconf-WARNING **: 20:51:05.92: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
tourstv@TourstV: /usr/local/etc$ sudo mv freshclam.conf.sample freshclam.conf
tourstv@TourstV: /usr/local/etc$ sudo gedit freshclam.conf
(gedit:139831): dconf-WARNING **: 20:51:46.20: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139831): dconf-WARNING **: 20:51:46.20: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139831): dconf-WARNING **: 20:51:46.40: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139831): dconf-WARNING **: 20:51:46.40: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139831): dconf-WARNING **: 20:51:46.40: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139831): dconf-WARNING **: 20:51:46.40: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported
** (gedit:139831): WARNING **: 20:51:46.40: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:139831): WARNING **: 20:51:46.40: Set document metadata failed: Setting attribute metadata::gedit-position not supported
(gedit:139831): dconf-WARNING **: 20:51:46.40: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
tourstv@TourstV: /usr/local/etc$ sudo freshclam
ClamAV update process started at Wed Feb 1 20:52:26 2023
daily database available for download (remote version: 26799)
[Line: 7.9s, ETA: 0.0s [=====]] 57.82MB/57.82MB
Testing database: '/usr/local/share/clamav/tmp.80a519fd37/clamav-a0439bae8b5e5138825a3c5eea746f4.tmp-daily.csv' ...
Database test passed.
daily.csv updated (version: 26799, sigs: 2018949, f-level: 90, builder: rayman)
main database available for download (remote version: 62)
Time: 0.05s [=====]] 162.58MB/162.58MB
Testing database: '/usr/local/share/clamav/tmp.80a519fd37/clamav-804485570dd65062c0b43ad5f1fb7e1.tmp-main.csv' ...
Database test passed.
main.csv updated (version: 62, sigs: 6647427, f-level: 90, builder: sigmgr)
bytecode database available for download (remote version: 333)
Time: 0.05s [=====]] 286.79KiB/286.79KiB
Testing database: '/usr/local/share/clamav/tmp.80a519fd37/clamav-82bd8da5b0be8b33892c8bd1b3c1ba32.tmp-bytecode.csv' ...
Database test passed.
bytecode.csv updated (version: 333, sigs: 92, f-level: 63, builder: awillia2)
tourstv@TourstV: /usr/local/etc$ 

```

Test

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

UbuntuV - VMware Workstation

File Edit View VM Tabs Help | Activities Terminal tourstv@TourstV: ~/Desktop/QQ

```
tourstv@TourstV:~$ mkdir /home/tourstv/Desktop/QQ
tourstv@TourstV:~$ cd
.cache/.config/Desktop/Documents/Downloads/.gnupg/.local/Music/Pictures/Public/snap/.ssh/Templates/Videos/
tourstv@TourstV:~$ cd Desktop/QQ
tourstv@TourstV:~/Desktop/QQ$ sudo wget http://www.elcar.org/download/elcar.com.txt
--2023-02-01 20:55:42-- http://www.elcar.org/download/elcar.com.txt
Resolving www.elcar.org (www.elcar.org)... 2a00:1828:1000:2497::2, 89.238.73.97
Connecting to www.elcar.org (www.elcar.org)|2a00:1828:1000:2497::2|:80...
HTTP request sent, awaiting response... 200 OK
Length: 68 [text/plain]
Saving to: 'elcar.com.txt'

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

2023-02-01 20:55:43 (7.57 MB/s) - 'elcar.com.txt' saved [68/68]
tourstv@TourstV:~/Desktop/QQ$
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

UbuntuV - VMware Workstation

File Edit View VM Tabs Help | Activities Terminal tourstv@TourstV: ~/Desktop/QQ

```
tourstv@TourstV:~$ mkdir /home/tourstv/Desktop/QQ
tourstv@TourstV:~$ cd
.cache/.config/Desktop/Documents/Downloads/.gnupg/.local/Music/Pictures/Public/snap/.ssh/Templates/Videos/
tourstv@TourstV:~$ cd Desktop/QQ
tourstv@TourstV:~/Desktop/QQ$ sudo wget http://www.elcar.org/download/elcar.com.txt
--2023-02-01 20:55:42-- http://www.elcar.org/download/elcar.com.txt
Resolving www.elcar.org (www.elcar.org)... 2a00:1828:1000:2497::2, 89.238.73.97
Connecting to www.elcar.org (www.elcar.org)|2a00:1828:1000:2497::2|:80...
HTTP request sent, awaiting response... 200 OK
Length: 68 [text/plain]
Saving to: 'elcar.com.txt'

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

2023-02-01 20:55:43 (7.57 MB/s) - 'elcar.com.txt' saved [68/68]
tourstv@TourstV:~/Desktop/QQ$ ls
elcar.com.txt
tourstv@TourstV:~/Desktop/QQ$ clamscan --version
ClamAV 0.103.7/20799/Wed Feb 1 15:42:06 2023
tourstv@TourstV:~/Desktop/QQ$ clamscan /home/tourstv/Desktop/QQ
/home/tourstv/Desktop/QQ/elcar.com.txt: Wn.Test.EICAR_HDB-1 FOUND
----- SCAN SUMMARY -----
Known viruses: 8659884
Engine version: 0.103.7
Scanned directories: 1
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 43.774 sec (0 m 43 s)
Start Date: 2023:02:01 20:56:51
End Date: 2023:02:01 20:57:35
tourstv@TourstV:~/Desktop/QQ$
```

```

UbuntuV - VMware Workstation
File Edit View VM Jobs Help | Terminal tourstv@TourstV: ~/Desktop/QQ
Activities tourstv@TourstV: ~/Desktop/QQ
tourstv@TourstV: ~/Desktop/QQ$ ls
elcar.com
tourstv@TourstV: ~/Desktop/QQ$ clamscan --version
ClamAV 0.103.7/20799/Wed Feb 1 15:42:06 2023
tourstv@TourstV: ~/Desktop/QQ$ clamscan /home/tourstv/Desktop/QQ
/home/tourstv/Desktop/QQ/elcar.com.txt: WIn.Test.EICAR_HDB-1 FOUND
-----
SCAN SUMMARY
Known viruses: 8659884
Engine version: 0.103.7
Scanned directories: 1
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
TTime: 43.774 sec (0 m 43 s)
Start Date: 2023:02:01 20:56:51
End Date: 2023:02:01 20:57:35
tourstv@TourstV: ~/Desktop/QQ$ sudo wget http://www.elcar.org/download/elcar_com.zip
Resolving www.elcar.org (www.elcar.org)... 2a00:1828:1000:2497::2, 89.238.73.97
Connecting to www.elcar.org (www.elcar.org)|2a00:1828:1000:2497::2|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 184 [application/zip]
Saving to: 'elcar_com.zip'

elcar_com.zip          100%[=====] 184 --.-KB/s   in 0s
2023-02-01 20:58:01 (11.9 MB/s) - 'elcar_com.zip' saved [184/184]

tourstv@TourstV: ~/Desktop/QQ$ clamscan /home/tourstv/Desktop/QQ
/home/tourstv/Desktop/QQ/elcar.com.txt: WIn.Test.EICAR_HDB-1 FOUND
/home/tourstv/Desktop/QQ/elcar_com.zip: WIn.Test.EICAR_HDB-1 FOUND
-----
SCAN SUMMARY
Known viruses: 8659884
Engine version: 0.103.7
Scanned directories: 1
Scanned files: 2
Infected files: 2
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
TTime: 25.558 sec (0 m 25 s)
Start Date: 2023:02:01 20:58:05
End Date: 2023:02:01 20:58:31
tourstv@TourstV: ~/Desktop/QQ$ 

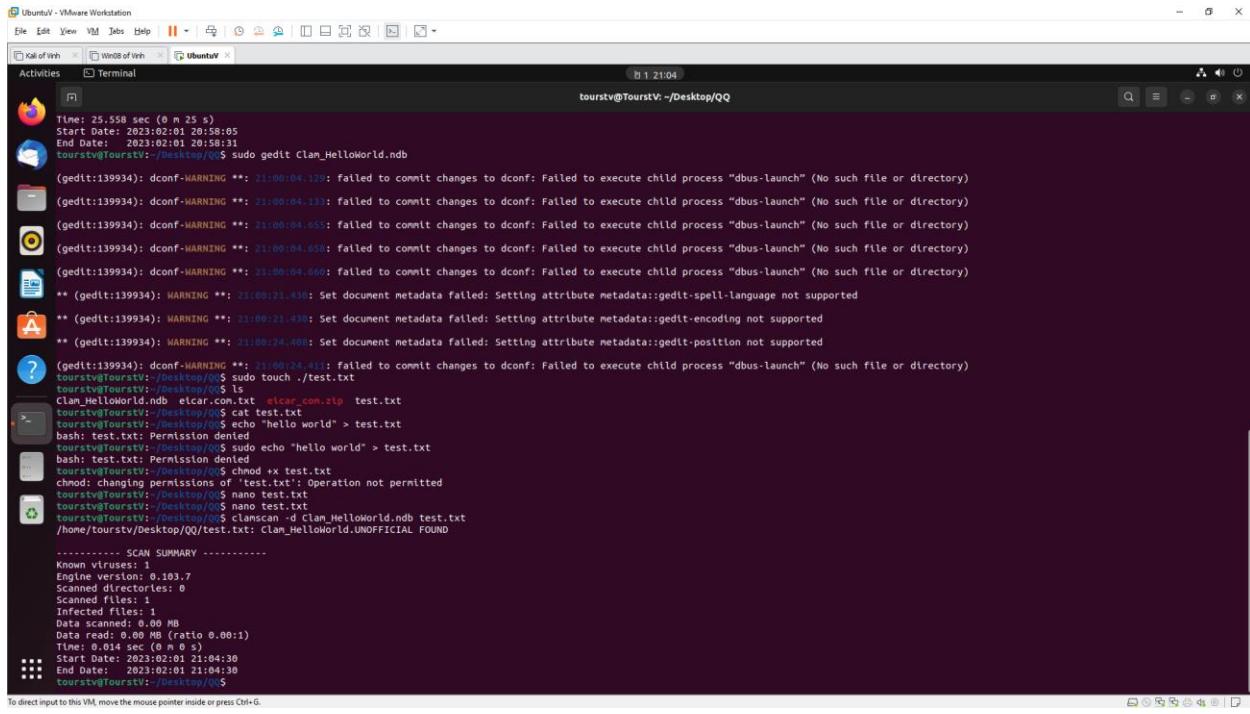
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
UbuntuV - VMware Workstation
File Edit View VM Jobs Help | Terminal tourstv@TourstV: ~/Desktop/QQ
Activities tourstv@TourstV: ~/Desktop/QQ
tourstv@TourstV: ~/Desktop/QQ$ ls
elcar.com
tourstv@TourstV: ~/Desktop/QQ$ clamscan --version
Clam_HelloWorld.ndb
/home/tourstv/Desktop/QQ
1 Clam_HelloWorld:0:*:68656c6c6f*776f726c64
tourstv@TourstV: ~/Desktop/QQ$ sudo wget http://www.elcar.org/download/elcar_com.zip
--2023-02-01 20:57:58-- http://www.elcar.org/download/elcar_com.zip
Resolving www.elcar.org (www.elcar.org)... 2a00:1828:1000:2497::2, 89.238.73.97
Connecting to www.elcar.org (www.elcar.org)|2a00:1828:1000:2497::2|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 184 [application/zip]
Saving to: 'elcar_com.zip'

elcar_com.zip          100%[=====] 184 --.-KB/s   in 0s
2023-02-01 20:58:01 (11.9 MB/s) - 'elcar_com.zip' saved [184/184]

tourstv@TourstV: ~/Desktop/QQ$ clamscan /home/tourstv/Desktop/QQ
/home/tourstv/Desktop/QQ/elcar.com.txt: WIn.Test.EICAR_HDB-1 FOUND
/home/tourstv/Desktop/QQ/elcar_com.zip: WIn.Test.EICAR_HDB-1 FOUND
-----
SCAN SUMMARY
Known viruses: 8659884
Engine version: 0.103.7
Scanned directories: 1
Scanned files: 2
Infected files: 2
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
TTime: 25.558 sec (0 m 25 s)
Start Date: 2023:02:01 20:58:05
End Date: 2023:02:01 20:58:31
tourstv@TourstV: ~/Desktop/QQ$ sudo gedit Clam_HelloWorld.ndb
(gedit:139934): dconf-WARNING **: 21:00:04.12: failed to commit changes to dconf
(gedit:139934): dconf-WARNING **: 21:00:04.13: failed to commit changes to dconf
(gedit:139934): dconf-WARNING **: 21:00:04.65: failed to commit changes to dconf
(gedit:139934): dconf-WARNING **: 21:00:04.66: failed to commit changes to dconf: Failed to execute child process "ibus-launch" (No such file or directory)
** (gedit:139934): WARNING **: 21:00:21.430: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported
** (gedit:139934): WARNING **: 21:00:21.430: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```



```
Time: 25.55 sec (0 m 25 s)
Start Date: 2023:02:01 20:58:05
End Date: 2023:02:01 20:58:31
tourstv@TourstV:~/Desktop/QQ$ sudo gedit Clam_Helloworld.ndb
(gedit:139934): dconf-WARNING **: 21:00:04.128: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139934): dconf-WARNING **: 21:00:04.128: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139934): dconf-WARNING **: 21:00:04.658: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139934): dconf-WARNING **: 21:00:04.658: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
(gedit:139934): dconf-WARNING **: 21:00:04.668: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
** (gedit:139934): WARNING **: 21:00:21.438: Set document metadata failed: Setting attribute metadata::gedit-spell-language not supported
** (gedit:139934): WARNING **: 21:00:21.438: Set document metadata failed: Setting attribute metadata::gedit-encoding not supported
** (gedit:139934): WARNING **: 21:00:24.408: Set document metadata failed: Setting attribute metadata::gedit-position not supported
(gedit:139934): dconf-WARNING **: 21:00:24.418: failed to commit changes to dconf: Failed to execute child process "dbus-launch" (No such file or directory)
tourstv@TourstV:~/Desktop/QQ$ ls
Clam_Helloworld.ndb  elcar.com.zip  test.txt
tourstv@TourstV:~/Desktop/QQ$ cat test.txt
tourstv@TourstV:~/Desktop/QQ$ echo "Hello world" > test.txt
bash: test.txt: Permission denied
tourstv@TourstV:~/Desktop/QQ$ chmod +x test.txt
bash: test.txt: Permission denied
tourstv@TourstV:~/Desktop/QQ$ chmod +x test.txt
chmod: changing permissions of 'test.txt': Operation not permitted
tourstv@TourstV:~/Desktop/QQ$ nano test.txt
tourstv@TourstV:~/Desktop/QQ$ nano test.txt
tourstv@TourstV:~/Desktop/QQ$ clamscan -d Clam_Helloworld.ndb test.txt
/home/tourstv/Desktop/QQ/test.txt: Clam_Helloworld.UNOFFICIAL FOUND
----- SCAN SUMMARY -----
Known viruses: 1
Engine version: 0.103.7
Scanned files: 0
Scanned files: 0
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 0.014 sec (0 m 0 s)
Start Date: 2023:02:01 21:04:38
End Date: 2023:02:01 21:04:38
tourstv@TourstV:~/Desktop/QQ$
```

PART 2: YARA

Install Yara

The image shows a dual-boot Linux desktop environment with two terminal windows side-by-side. Both terminals are running on the same physical machine, as evidenced by the identical command-line output.

Terminal 1 (Top):

```
tourstv@TourstV: ~$ sudo apt-get install yara
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi libva-driver intel-media-va-driver libvaacs0 libao0 libavcodec58 libavformat58 libavutil56 libbdplus0 libblas3 libbluray2 libbs2be
  libchromaprint1 libcodec2-1.0 libdavids libfdt1:2 libgme0 libgsml libgstreamer-plugins-bad1.0-0 libigdmm12 libilv0-0 libilm13 libmfx1 libnsofa1 libnorm1 libopenmp0
  libpng-5.3-0 libpostproc55 librabitmq4 librubberband2 libserd-0-0 libshlne3 libsnappy1v5 libsrord-0-0 libsratom-0-0 libsrtr1.4-grnuls libssh-gcrypt-4 libswresample3 libwscales libudfread0 libva-drm2
  libva-wayland2 libva-x11-2 libva libvidpau libvidstab1.i libx265-199 libxvidcore4 libzimg2 libzmq5 libzvbi-common libzvbi0 mesa-va-drivers mesa-vdpau-drivers pocketsphinx-en-us va-driver-all
  vdpau-driver-all
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libyara8
The following NEW packages will be installed:
  libyara8 yara
0 upgraded, 2 newly installed, 0 to remove and 17 not upgraded.
Need to get 179 kB of archives.
After this operation, 499 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

Terminal 2 (Bottom):

```
tourstv@TourstV: ~$ sudo apt-get install yara
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi libva-driver intel-media-va-driver libvaacs0 libao0 libavcodec58 libavformat58 libavutil56 libbdplus0 libblas3 libbluray2 libbs2be
  libchromaprint1 libcodec2-1.0 libdavids libfdt1:2 libgme0 libgsml libgstreamer-plugins-bad1.0-0 libigdmm12 libilv0-0 libilm13 libmfx1 libnsofa1 libnorm1 libopenmp0
  libpng-5.3-0 libpostproc55 librabitmq4 librubberband2 libserd-0-0 libshlne3 libsnappy1v5 libsrord-0-0 libsratom-0-0 libsrtr1.4-grnuls libssh-gcrypt-4 libswresample3 libwscales libudfread0 libva-drm2
  libva-wayland2 libva-x11-2 libva libvidpau libvidstab1.i libx265-199 libxvidcore4 libzimg2 libzmq5 libzvbi-common libzvbi0 mesa-va-drivers mesa-vdpau-drivers pocketsphinx-en-us va-driver-all
  vdpau-driver-all
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libyara8
The following NEW packages will be installed:
  libyara8 yara
0 upgraded, 2 newly installed, 0 to remove and 17 not upgraded.
Need to get 179 kB of archives.
After this operation, 499 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu jammy/universe amd64 libyara8 amd64 4.1.3-1build1 [157 kB]
Get:2 http://archive.ubuntu.com/ubuntu jammy/universe amd64 yara amd64 4.1.3-1build1 [22.3 kB]
Fetched 180 kB in 4s (41.8 kB/s)
Selecting previously unselected package libyara8:amd64.
(Reading database ... 293812 files and directories currently installed.)
Preparing to unpack .../libyara8:4.1.3-1build1_amd64.deb ...
Unpacking libyara8:amd64 (4.1.3-1build1) ...
Selecting previously unselected package yara.
Preparing to unpack .../yara_4.1.3-1build1_amd64.deb ...
Unpacking yara (4.1.3-1build1) ...
Setting up libyara8:amd64 (4.1.3-1build1) ...
Setting up yara (4.1.3-1build1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
tourstv@TourstV: ~$
```

Install p7zip-full

```

UbuntuV - VMware Workstation
File Edit View VM Jobs Help | Terminal | tourstv@TourstV: ~
Activities tourstv@TourstV: ~
Terminal tourstv@TourstV: ~
1 21:07
tourstv@TourstV: ~
libchromaprint1 libcodec2-1.0 libdavids libflashrom liblfrt1 liblbgm0 libbsm1 libbsr1 libmysofa1 libborm1 libbopenmp1
libpgm-5.3-0 libpostproc55 librabitmq4 librubberband2 libserd-0-0 libshn3 libsnappy1v5 libsr1.4-gruntls libssh-gcrypt-4 libswresample3 libwscale5 libudread0 libva-drm2
libva-wayland2 libva-x11-2 libvaz libvdpa libvidstab1 libx265-199 libxvidcore4 libzimg2 libzmq5 libzvbi-common libzvbi0 mesa-va-drivers mesa-vdpau-drivers pocketsphinx-en-us va-driver-all
vdpau-driver-all
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
libyara8
The following NEW packages will be installed:
libyara8
0 upgraded, 2 newly installed, 0 to remove and 17 not upgraded.
Need to get 499 kB of archives.
After this operation, 499 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://archive.ubuntu.com/ubuntu jammy/universe amd64 libyara8 amd64 4.1.3-1build1 [157 kB]
Get:2 http://archive.ubuntu.com/ubuntu jammy/universe amd64 yara amd64 4.1.3-1build1 [22.3 kB]
Fetched in 4s (41.9 MB/s)
Selecting previously unselected package libyara8:amd64.
(Reading database ... 23012 files and directories currently installed.)
Preparing to unpack .../libyara8_4.1.3-1build1_amd64.deb ...
Unpacking libyara8:amd64 (4.1.3-1build1) ...
Selecting previously unselected package yara.
Preparing to unpack .../yara_4.1.3-1build1_amd64.deb ...
Unpacking yara (4.1.3-1build1) ...
Setting up libyara8:amd64 (4.1.3-1build1) ...
Setting up yara (4.1.3-1build1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
tourstv@TourstV: ~ sudo apt-get install p7zip-full p7zip-rar unrar-free -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi libva-intel-driver intel-media-va-driver libva0 libbam3 libbass9 libavcodec58 libavformat58 libavutil56 libbdplus0 libbias3 libbluray2 libbs2be
libchromaprint1 libcodec2-1.0 libdavids libflashrom liblfrt1 liblbgm0 libbsm1 libbsr1 libmysofa1 libborm1 libbopenmp1
libpgm-5.3-0 libpostproc55 librabitmq4 librubberband2 libserd-0-0 libshn3 libsnappy1v5 libsr1.4-gruntls libssh-gcrypt-4 libswresample3 libwscale5 libudread0 libva-drm2
libva-wayland2 libva-x11-2 libvaz libvdpa libvidstab1 libx265-199 libxvidcore4 libzimg2 libzmq5 libzvbi-common libzvbi0 mesa-va-drivers mesa-vdpau-drivers pocketsphinx-en-us va-driver-all
vdpau-driver-all
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
p7zip
Suggested packages:
p7kis0.
The following NEW packages will be installed:
p7zip p7zip-full p7zip-rar unrar-free
0 upgraded, 4 newly installed, 0 to remove and 17 not upgraded.
Need to get 1,635 kB of archives.
After this operation, 6,817 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu jammy/universe amd64 p7zip amd64 16.02+dfsg-8 [363 kB]
0% [1/7 p7zip 6,817/8,363 kB 2%]

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Download clamav_to_yara.py

```

UbuntuV - VMware Workstation
File Edit View VM Jobs Help | Terminal | tourstv@TourstV: ~/Desktop/QQ2
Activities tourstv@TourstV: ~/Desktop/QQ2
Terminal tourstv@TourstV: ~/Desktop/QQ2
1 21:15
tourstv@TourstV: ~/Desktop/QQ2$ ls
package.01.ful7z
tourstv@TourstV: ~/Desktop/QQ2$ wget https://raw.githubusercontent.com/nattulm/volgul/master/tools/clamav_to_yara.py
Resolving raw.githubusercontent.com... (raw.githubusercontent.com)... 2606:50c:8003::154, 2606:50c:8002::154, 2606:50c:8000::154, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|2606:50c:8003::154|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9381 (9.1K) [text/plain]
Saving to 'clamav_to_yara.py'
Saving: "clamav_to_yara.py"
clamav_to_yara.py          100%[=====]  9.08K --.-KB/s   in 0.001s
2023-02-01 21:15:10 (11.0 MB/s) - 'clamav_to_yara.py' saved [9381/9381]
tourstv@TourstV: ~/Desktop/QQ2$ ls
clamav_to_yara.py  package.01.ful7z
tourstv@TourstV: ~/Desktop/QQ2$ cat clamav_to_yara.py
#!/usr/bin/python
#
# encoding: utf-8
#
# # Tested on LInux (Ubuntu), Windows XP/7, and Mac OS X
#
#
# clamav_to_yara.py
#
# Created by Matthew Richard on 2010-03-12.
# Copyright (c) 2010 __MyCompanyName__. All rights reserved.
#
#
# import sys
# import os
# import re
# from optparse import OptionParser
#
# def main():
#     parser = OptionParser()
#     parser.add_option("-f", "--file", action="store", dest="filename",
#                      type="string", help="scanned FILENAME")
#     parser.add_option("-o", "--output-file", action="store", dest="outfile",
#                      type="string", help="output filename")
#     parser.add_option("-v", "--verbose", action="store_true", default=False,
#                      dest="verbose")
#     parser.add_option("-s", "--search", action="store", dest="search",
#                      type="string", help="search filter", default="")
#
#     (opts, args) = parser.parse_args()
#
#     if opts.filename == None:
#         parser.print_help()
#         parser.error("You must supply a filename!")

```

To direct input to this VM, move the mouse pointer inside or press Ctrl-G.

Convert file clamav to yara:

The screenshot shows a Linux desktop environment with a terminal window and a file browser window.

Terminal Window:

```
tourstv@TourstV: ~$ cd Desktop/QQ2
tourstv@TourstV: ~/Desktop/QQ2$ sudo python /home/tourstv/Desktop/QQ2/clamav_to_yara.py -f /home/tourstv/Desktop/QQ2/package.01/package.clamsrch.ndb -o clamsrch.yara
[sudo] password for tourstv:
#####
# Malware Analyst's Cookbook - clamAV to YARA Converter 0.0.1
#####
[+] Read 2291 lines from /home/tourstv/Desktop/QQ2/package.01/package.clamsrch.ndb
[+] Wrote 2287 rules to clamsrch.yara

tourstv@TourstV: ~/Desktop/QQ2$ sudo python /home/tourstv/Desktop/QQ2/clamav_to_yara.py -f /home/tourstv/Desktop/QQ2/package.01.ful/package.clamsrch.ndb -o clamsrch.yara
#####
# Malware Analyst's Cookbook - ClamAV to YARA Converter 0.0.1
#####
[+] Read 2291 lines from /home/tourstv/Desktop/QQ2/package.01.ful/package.clamsrch.ndb
[+] Wrote 2287 rules to clamsrch.yara

tourstv@TourstV: ~/Desktop/QQ2$
```

File Browser Window:

The file browser shows the following files in the directory `/home/tourstv/Desktop/QQ2`:

- Recent
- Starred
- Home
- Documents
- Downloads
- Music
- Pictures
- Videos
- Trash
- vinhnt10062002@...
- + Other Locations

Files listed in the directory:

- package.01
- package.01.ful
- clamav_to_yara.py
- clamsrch.yara
- package.01.7z
- package.01.ful.7z

Scan with yara:

Yara rule:

A screenshot of a Linux desktop environment (Ubuntu) running in a VMware Workstation window. The terminal window shows the following YARA rule code:

```
GNU nano 6.2
rule ConditionsExample {
    strings:
        $string1 = "hello"
        $string2 = "Hello"
        $string3 = "hello"

    condition:
        any of them
}
rule GlobalRuleExample {
    condition:
        filesize < 2MB
}
rule NumberStringExample {
    strings:
        $hello = "hello"

    condition:
        $hello >= 5
}
rule CheckImage {
    strings:
        $a = {89 50 4e 47 0d 0a 1a 0a}

    condition:
        any of them
}
```

The terminal window title is "rule.yara". The status bar at the bottom shows keyboard shortcuts for various functions like Help, Write Out, Read File, Replace, Cut, Paste, Execute, Justify, Go To Line, Undo, Redo, Set Mark, To Bracket, Where Was, Previous, Next, Back, Forward, Prev Word, and Next Word.

Test yara rule

A screenshot of a Linux desktop environment (Ubuntu) running in a VMware Workstation window. The terminal window shows the following command-line session:

```
tourstv@TourstV:~/Desktop/QQ$ nano rule.yara
tourstv@TourstV:~/Desktop/QQ$ rule over_500kb
Command 'rule' not found, did you mean:
  command 'rule' from snap darkdimension-rule (0.3.6)
  command 'rule' from snap jhawkins-rust (0.1.0)
See 'snap info ' for additional versions.
tourstv@TourstV:~/Desktop/QQ$ yara -r rule.yara /home/tourstv/Desktop/QQ
ConditionsExample /home/tourstv/Desktop/QQ/test.txt
GlobalRuleExample /home/tourstv/Desktop/QQ/test.txt
GlobalRuleExample /home/tourstv/Desktop/QQ/elcar_con.zip
GlobalRuleExample /home/tourstv/Desktop/QQ/Clam_Helloworld.ndb
GlobalRuleExample /home/tourstv/Desktop/QQ/elcar.com.trt
tou
```

The terminal window title is "rule.yara". The status bar at the bottom shows keyboard shortcuts for various functions like Help, Write Out, Read File, Replace, Cut, Paste, Execute, Justify, Go To Line, Undo, Redo, Set Mark, To Bracket, Where Was, Previous, Next, Back, Forward, Prev Word, and Next Word.