

Nama : Muhammad Khairil amin

Nim : L200160162

Kelas : A

Modul 9

Update

```
root@aulia-VirtualBox:/home/aulia# apt-get update
Get:1 http://security.ubuntu.com/ubuntu xenial-security InRelease [109 kB]
Hit:2 http://id.archive.ubuntu.com/ubuntu xenial InRelease
Get:3 http://security.ubuntu.com/ubuntu xenial-security/main amd64 Packages [647
kB]
Get:4 http://id.archive.ubuntu.com/ubuntu xenial-updates InRelease [109 kB]
Get:5 http://security.ubuntu.com/ubuntu xenial-security/main i386 Packages [535
kB]
Hit:6 http://id.archive.ubuntu.com/ubuntu xenial-backports InRelease
Get:7 http://security.ubuntu.com/ubuntu xenial-security/main Translation-en [264
kB]
Get:8 http://id.archive.ubuntu.com/ubuntu xenial-updates/main amd64 Packages [95
7 kB]
Get:9 http://security.ubuntu.com/ubuntu xenial-security/universe amd64 Packages
[435 kB]
Get:10 http://security.ubuntu.com/ubuntu xenial-security/universe i386 Packages
[378 kB]
Get:11 http://id.archive.ubuntu.com/ubuntu xenial-updates/main i386 Packages [82
4 kB]
Get:12 http://id.archive.ubuntu.com/ubuntu xenial-updates/main Translation-en [3
81 kB]
Get:13 http://id.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 Package
s [748 kB]
Get:14 http://id.archive.ubuntu.com/ubuntu xenial-updates/universe i386 Packages
```

Cek kompatibilitas antivirus

```
root@aulia-VirtualBox:/home/aulia# apt-cache search clamav
amavisd-new - Interface between MTA and virus scanner/content filters
clamav - anti-virus utility for Unix - command-line interface
clamav-base - anti-virus utility for Unix - base package
clamav-daemon - anti-virus utility for Unix - scanner daemon
clamav-dbg - debug symbols for ClamAV
clamav-docs - anti-virus utility for Unix - documentation
clamav-freshclam - anti-virus utility for Unix - virus database update utility
clamscan - anti-virus utility for Unix - scanner client
libclamav-dev - anti-virus utility for Unix - development files
libclamav7 - anti-virus utility for Unix - library
amavisd-new-postfix - part of Ubuntu mail stack provided by Ubuntu server team
clamassassin - email virus filter wrapper for ClamAV
clamav-milter - anti-virus utility for Unix - sendmail integration
clamav-testfiles - anti-virus utility for Unix - test files
clamav-unofficial-sigs - update script for 3rd-party clamav signatures
clamfs - user-space anti-virus protected file system
clamsmtp - virus-scanning SMTP proxy
clamtk - graphical front-end for ClamAV
clamtk-gnome - GNOME (Nautilus) MenuProvider extension for ClamTk
claws-mail-clamd-plugin - ClamAV socket-based plugin for Claws Mail
courier-filter-perl - purely Perl-based mail filter framework for the Courier MT
A
```

Install Clamav

```
root@aulia-VirtualBox:/home/aulia# apt-cache search clamav
amavisd-new - Interface between MTA and virus scanner/content filters
clamav - anti-virus utility for Unix - command-line interface
clamav-base - anti-virus utility for Unix - base package
clamav-daemon - anti-virus utility for Unix - scanner daemon
clamav-dbg - debug symbols for ClamAV
clamav-docs - anti-virus utility for Unix - documentation
clamav-freshclam - anti-virus utility for Unix - virus database update utility
clamscan - anti-virus utility for Unix - scanner client
libclamav-dev - anti-virus utility for Unix - development files
libclamav7 - anti-virus utility for Unix - library
amavisd-new-postfix - part of Ubuntu mail stack provided by Ubuntu server team
clamassassin - email virus filter wrapper for ClamAV
clamav-milter - anti-virus utility for Unix - sendmail integration
clamav-testfiles - anti-virus utility for Unix - test files
clamav-unofficial-sigs - update script for 3rd-party clamav signatures
clamfs - user-space anti-virus protected file system
clamsmtp - virus-scanning SMTP proxy
clamtk - graphical front-end for ClamAV
clamtk-gnome - GNOME (Nautilus) MenuProvider extension for ClamTk
claws-mail-clamd-plugin - ClamAV socket-based plugin for Claws Mail
courier-filter-perl - purely Perl-based mail filter framework for the Courier MT
```


Scanning menggunakan clamscan engine pada direktori /home/aulia

```
root@aulia-VirtualBox:/home/aulia# clamscan
LibClamAV Error: cli_loaddbdir(): No supported database files found in /var/lib/
clamav
ERROR: Can't open file or directory

----- SCAN SUMMARY -----
Known viruses: 0
Engine version: 0.100.3
Scanned directories: 0
Scanned files: 0
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 0.015 sec (0 m 0 s)
root@aulia-VirtualBox:/home/aulia#
```

Scanning menggunakan clamscan engine pada direktori /var/www

```
root@aulia-VirtualBox:/var/www# clamscan -r /www
LibClamAV Error: cli_loaddbdir(): No supported database files found in /var/lib/
clamav
ERROR: Can't open file or directory

----- SCAN SUMMARY -----
Known viruses: 0
Engine version: 0.100.3
Scanned directories: 0
Scanned files: 0
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 0.007 sec (0 m 0 s)
root@aulia-VirtualBox:/var/www#
```

Update clamav

```
root@aulia-VirtualBox:/# freshclam
Tue May 28 21:41:16 2019 -> ClamAV update process started at Tue May 28 21:41:16
2019
Tue May 28 21:41:51 2019 -> ^Can't query current.cvd.clamav.net
Tue May 28 21:41:51 2019 -> ^Invalid DNS reply. Falling back to HTTP mode.
Tue May 28 21:45:17 2019 -> Downloading main.cvd [100%]
Tue May 28 21:45:27 2019 -> main.cvd updated (version: 58, sigs: 4566249, f-level:
60, builder: sigmgr)
Tue May 28 21:46:24 2019 -> Downloading daily.cvd [100%]
Tue May 28 21:46:51 2019 -> daily.cvd updated (version: 25463, sigs: 1583021, f-
level: 63, builder: raynman)
Tue May 28 21:46:53 2019 -> Downloading bytecode.cvd [100%]
Tue May 28 21:46:54 2019 -> bytecode.cvd updated (version: 328, sigs: 94, f-level:
63, builder: neo)
Tue May 28 21:47:06 2019 -> Database updated (6149364 signatures) from db.local.
clamav.net (IP: 104.16.219.84)
Tue May 28 21:47:06 2019 -> !NotifyClamd: Can't find or parse configuration file
/etc/clamav/clamd.conf
root@aulia-VirtualBox:/#
```

Download test virus

```
root@aulia-VirtualBox:/home/aulia# wget http://www.eicar.org/download/eicar.com
--2019-05-28 21:50:13-- http://www.eicar.org/download/eicar.com
Resolving www.eicar.org (www.eicar.org)... 213.211.198.62
Connecting to www.eicar.org (www.eicar.org)|213.211.198.62|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 68 [application/octet-stream]
Saving to: 'eicar.com'

eicar.com          100%[=====>]          68  --.-KB/s    in 0s
2019-05-28 21:50:15 (5.82 MB/s) - 'eicar.com' saved [68/68]

root@aulia-VirtualBox:/home/aulia#
```

Scan test virus

```
root@aulia-VirtualBox:/home/aulia# clamscan --infected --remove --recursive ./eicar.com
./eicar.com: Eicar-Test-Signature FOUND
./eicar.com: Removed.

----- SCAN SUMMARY -----
Known viruses: 6140217
Engine version: 0.100.3
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 60.980 sec (1 m 0 s)
root@aulia-VirtualBox:/home/aulia#
```

Tugas

1. Scanning direktori dibawah direktori utama (root)

```
root@aulia-VirtualBox:/# ls
bin      dev      initrd.img  lost+found  opt      run      srv      usr
boot     etc      lib         media       proc     sbin     sys      var
cdrom    home     lib64       mnt         root     snap     tmp      vmlinuz
```

- Dibawah Root

```
root@aulia-VirtualBox:/# clamscan ./ root
./vmlinuz: Symbolic link
./initrd.img: Symbolic link
root/.rnd: OK
root/.bashrc: OK
root/.bash_history: OK
root/.profile: OK

----- SCAN SUMMARY -----
Known viruses: 6143694
Engine version: 0.100.3
Scanned directories: 2
Scanned files: 4
Infected files: 0
Data scanned: 0.02 MB
Data read: 0.01 MB (ratio 2.00:1)
Time: 39.841 sec (0 m 39 s)
root@aulia-VirtualBox:/#
```

- Bin

```
/bin/lessecho: OK
/bin/fusermount: OK
/bin/mt-gnu: OK
/bin/true: OK
/bin/zmore: OK
/bin/nc: Symbolic link
/bin/mount: OK
/bin/lowntfs-3g: OK
/bin/lesspipe: OK
/bin/open: Symbolic link
/bin/findmnt: OK
/bin/uname: OK
/bin/bzip2recover: OK

----- SCAN SUMMARY -----
Known viruses: 6143694
Engine version: 0.100.3
Scanned directories: 1
Scanned files: 138
Infected files: 0
Data scanned: 12.22 MB
Data read: 12.16 MB (ratio 1.00:1)
Time: 48.514 sec (0 m 48 s)
root@aulia-VirtualBox:/bin#
```

- Home

```
root@aulia-VirtualBox:/home# clamscan

----- SCAN SUMMARY -----
Known viruses: 6143694
Engine version: 0.100.3
Scanned directories: 1
Scanned files: 0
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 59.037 sec (0 m 59 s)
root@aulia-VirtualBox:/home#
```


- Etc

```
/etc/group-: OK
/etc/logrotate.conf: OK
/etc/fuse.conf: OK
/etc/subgid: OK
/etc/kerneloops.conf: OK
/etc/subuid-: Empty file
/etc/.pwd.lock: Empty file
/etc/gai.conf: OK
/etc/rpc: OK
/etc/subgid-: Empty file
/etc/.host.conf.swp: OK
/etc/bash.bashrc: OK
/etc/hdparm.conf: OK

----- SCAN SUMMARY -----
Known viruses: 6143694
Engine version: 0.100.3
Scanned directories: 1
Scanned files: 98
Infected files: 0
Data scanned: 0.52 MB
Data read: 0.26 MB (ratio 1.99:1)
Time: 45.105 sec (0 m 45 s)
root@aulia-VirtualBox:/etc#
```

2. Konfigurasi user permission berpengaruh pada saat melakukan scanning pada direktori root. Terdapat **warning : root: can't access file.**

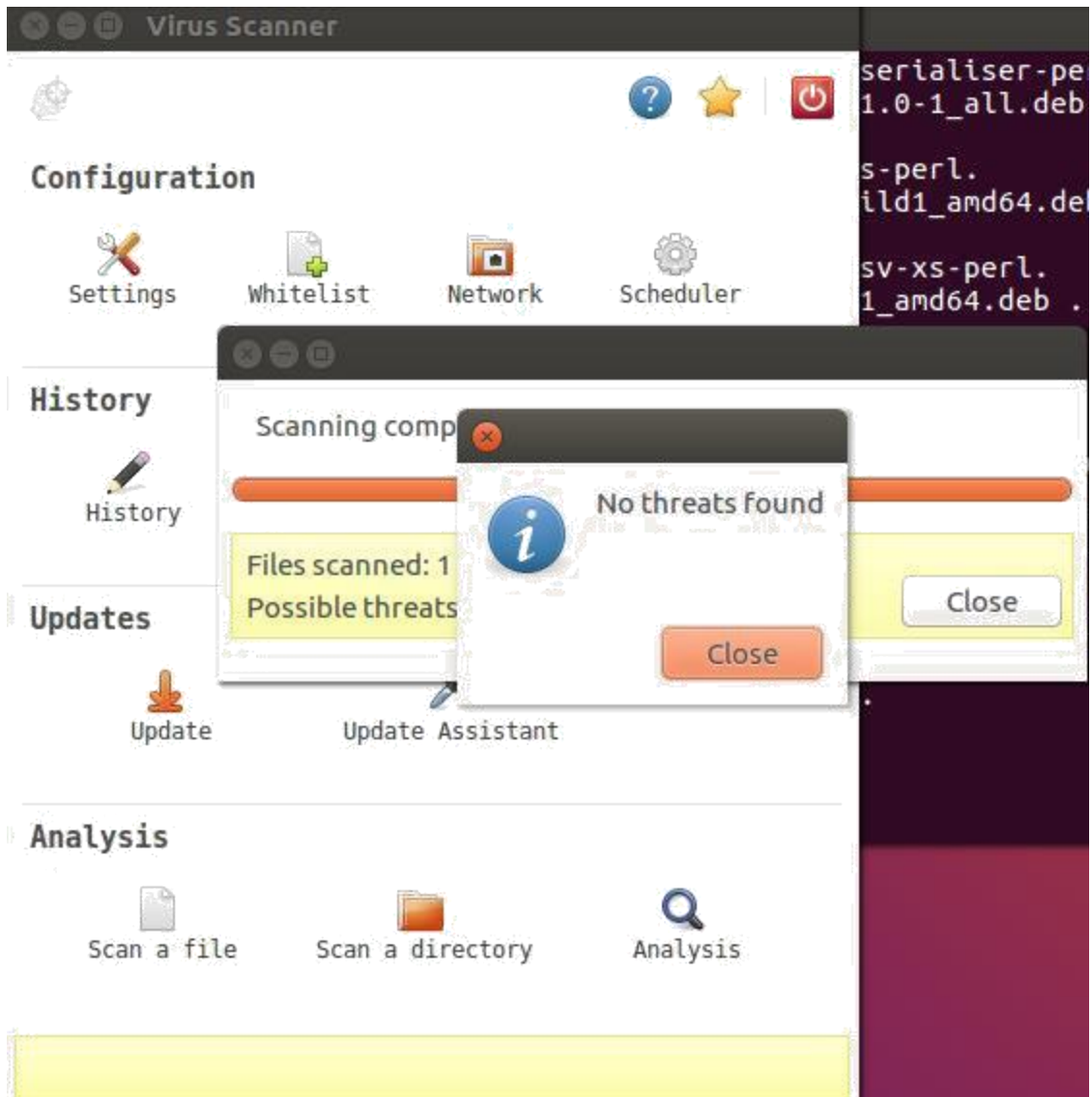
```
aulia@aulia-VirtualBox:~$ clamscan ./ root
./Xauthority: OK
./xsession-errors: OK
./bash_logout: OK
./dmrc: OK
./xsession-errors.old: OK
./examples.desktop: OK
./sudo_as_admin_successful: Empty file
./bashrc: OK
./bash_history: OK
./a.out: Empty file
./profile: OK
./ICEauthority: OK
root: No such file or directory
WARNING: root: Can't access file

----- SCAN SUMMARY -----
Known viruses: 6143694
Engine version: 0.100.3
Scanned directories: 1
Scanned files: 10
Infected files: 0
Data scanned: 0.04 MB
Data read: 0.02 MB (ratio 1.83:1)
```

3. Install 2 aplikasi antivirus

- ClamTK

```
root@aulia-VirtualBox:/home/aulia# apt-get install clamtk
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  gnome-icon-theme libcommon-sense-perl libjson-perl libjson-xs-perl
  libtext-csv-perl libtext-csv-xs-perl libtypes-serialiser-perl
Suggested packages:
  cabextract clamtk-nautilus
The following NEW packages will be installed:
  clamtk gnome-icon-theme libcommon-sense-perl libjson-perl libjson-xs-perl
  libtext-csv-perl libtext-csv-xs-perl libtypes-serialiser-perl
0 upgraded, 8 newly installed, 0 to remove and 298 not upgraded.
Need to get 10,4 MB of archives.
After this operation, 18,2 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://id.archive.ubuntu.com/ubuntu xenial/universe amd64 libtext-csv-perl
  all 1.33-1 [48,2 kB]
Get:2 http://id.archive.ubuntu.com/ubuntu xenial/main amd64 libjson-perl all 2.9
  0-1 [79,4 kB]
Get:3 http://id.archive.ubuntu.com/ubuntu xenial/universe amd64 gnome-icon-theme
  all 3.12.0-1ubuntu3 [9.630 kB]
Get:4 http://id.archive.ubuntu.com/ubuntu xenial/universe amd64 clamtk all 5.20-
  1 [455 kB]
```

- Sophos Antivirus

```
Sophos Anti-Virus
=====
Copyright 1989-2018 Sophos Limited. All rights reserved.

Welcome to the Sophos Anti-Virus installer. Sophos Anti-Virus contains an on-
access scanner, an on-demand command-line scanner and the Sophos Anti-Virus
daemon.

On-access scanner      Scans files as they are accessed, and grants access
                        to only those that are threat-free.
On-demand scanner      Scans the computer, or parts of the computer,
                        immediately.
Sophos Anti-Virus daemon Background process that provides control, logging,
                        and email alerting for Sophos Anti-Virus.

Press <return> to display Licence. Then press <spc> to scroll forward.
*****
NOTICE
This Sophos software contains software licensed by Sophos as well as software
licensed by other parties. Some software license terms may grant You rights with
respect to such software (including distribution rights) which are in addition
to those rights granted to You by Sophos with respect to this Sophos product in

root@aulia-VirtualBox:/opt/sophos-av/bin# ./savdstatus
Sophos Anti-Virus is active and on-access scanning is running
root@aulia-VirtualBox:/opt/sophos-av/bin# ./savescan /home/aulia
bash: ./savescan: No such file or directory
root@aulia-VirtualBox:/opt/sophos-av/bin# ls
_  savconfig  savdctl  savdstatus  savlog  savscan  savsetup  savupdate
root@aulia-VirtualBox:/opt/sophos-av/bin# ./savscan /home/aulia
SAVScan virus detection utility
Version 5.53.0 [Linux/AMD64]
Virus data version 5.55, September 2018
Includes detection for 25676226 viruses, Trojans and worms
Copyright (c) 1989-2018 Sophos Limited. All rights reserved.

System time 11:47:57 AM, System date 02 June 2019

Useful life of Scan has been exceeded

Quick Scanning

2004 files scanned in 21 seconds.
No viruses were discovered.
End of Scan.
root@aulia-VirtualBox:/opt/sophos-av/bin#
```