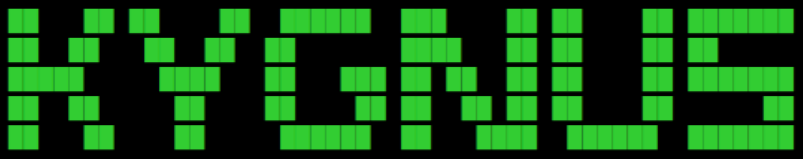


KooshaYeganehGnuLinuxSoftwares

|<[][]$#/-\ `/[-(_+[-|\|[-# (_+|\||_| |_!|\||_|)($[]|='|'\|//-\/2[-$

openSUSE Malware Detection Tools

clamAV - LMD (maldet) - rkhunter - chkrootkit - Lynis

clamAV

Install

```
sudo zypper install clamav
```

```
sudo systemctl start clamd
```

Updating the ClamAV Signature Database

- Stop freshclam service
- Update the signature database (Two methods)
    - Update by running the command in the terminal
    - Update by downloading daily.cvd file
- Start freshclam service

```
sudo systemctl stop freshclam
```

```
sudo freshclam
```

This command will install the signature database in your machine. If this command does not work, then goto the following link to download signature database file

https://database.clamav.net/daily.cvd

Now create a directory named “clamav”, if does not exist, in a specific location by running the following command

sudo mkdir /var/lib/clamav

And move the downloaded file in this location by running the following command

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

Now the third step is to start the clamav-freshclam service by running the following command.

```
sudo systemctl start freshclam
```

- –infected: prints only infected files
- –remove: removes infected files
- –recursive: all the subdirectories in the directory will be scanned
- --max-filesize
- --exclude-dir=/proc/*
- --exclude-dir=/sys/*
- --cross-fs=[yes(*)/no] : Scan files and directories on other filesystems.
- --log = FILE
- --file-list=FILE : Scan files listed line by line in FILE.

```
sudo clamscan -remove -infected -recursive /home/koosha/Documents
```

```
sudo clamscan -remove -infected -recursive  --exclude-dir=/proc/*
--exclude-dir=/sys/*
```

Understanding clamd, clamdscan and clamscan

When you run the libclamav engine and signatures are loaded at runtime. The other way to run the scanning engine is via clamd.

Clamd runs as a background process that has the engine and signatures in memory. A clamd client (clamdscan) then connects to the service in order to have the scanning performed. The clamd service accepts various commands in order to perform the scanning.

Configuration of the scanning is controlled via the clamd.conf configuration and cannot be specified at runtime. Whereas using clamscan it is possible to configure a large number of options at runtime from the command line.

Note that the clamd service is unauthenticated. Do not make it accessible from the Internet.

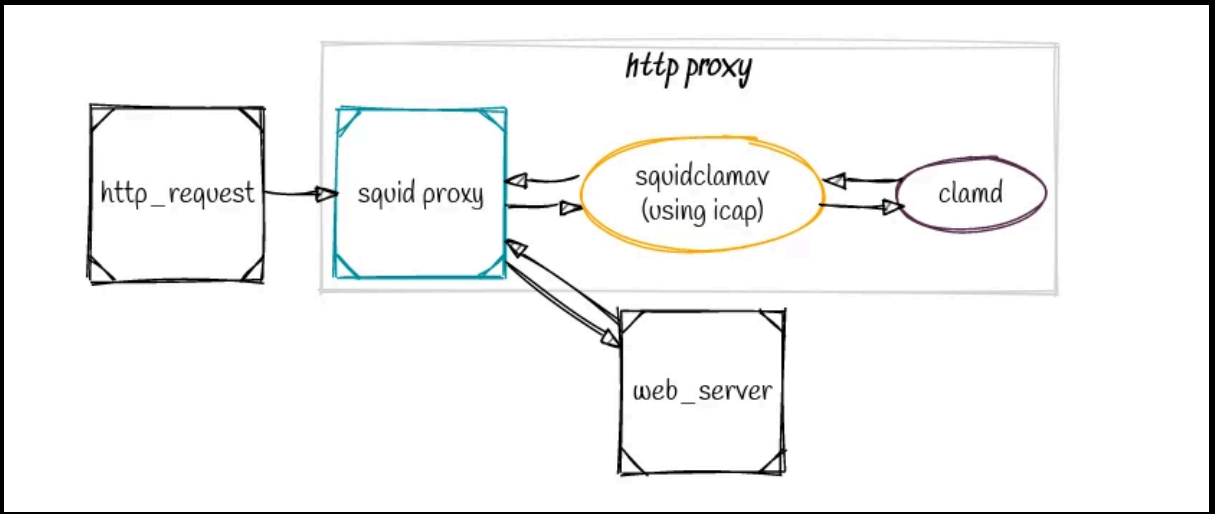
Integrate ClamAV in a HTTP Proxy

By integrating ClamAV into a HTTP proxy such as Squid it is possible to have transparent antivirus across all your web traffic.

Using Squid it is possible to configure the proxy to perform SSL/TLS bumping (decryption) enabling scanning of SSL/TLS encrypted traffic.

squidclamav icap module

Squid is a popular open source HTTP proxy that can work with modules using the ICAP protocol. ICAP is standard that allows HTTP proxies to outsource content inspection and manipulation to an external process or server.



SquidClamAV is an antivirus for the Squid proxy based on ICAP, it is highly performant and able to handle thousands of HTTP connections simultaneously.

https://squidclamav.darold.net/index.html#download

Installation and Configuration of SquidClamAV goes beyond the scope of this guide.

```
------------------------------------------------------------
```

chkrootkit

```
sudo zypper addrepo
https://download.opensuse.org/repositories/security/15.5/security.repo
```

```
sudo zypper refresh
```

```
sudo zypper -n install chkrootkit
```

or

```
sudo yum update
```

```
sudo yum install wget gcc-c++ glibc-static
```

```
sudo wget -c ftp://ftp.chkrootkit.org/pub/seg/pac/chkrootkit.tar.gz
```

```
sudo tar -xzf chkrootkit.tar.gz
```

```
sudo mkdir /usr/local/chkrootkit
```

```
sudo mv chkrootkit-0.58b/* /usr/local/chkrootkit
```

```
cd /usr/local/chkrootkit
```

```
sudo make sense
```

USE

```
sudo chkrootkit
```

```
------------------------------------------------------------
```

Rkhunter

```
sudo zypper install rkhunter
```

USE

```
sudo rkhunter -c
```

or

```
sudo rkhunter -check
```

```
————————————————————————————————————————————————————
```

Maldet

```
wget http://www.rfxn.com/downloads/maldetect-current.tar.gz
```

```
tar xfv maldetect-current.tar.gz
```

```
cd maldetect-1.*
```

```
sudo ./install
```

The configuration of LMD is handled through /usr/local/maldetect/conf.maldet and all options are well commented to make configuration a rather easy task. In case you get stuck, you can also refer to /maldetect-1.6.4/README for further instructions.

In the configuration file you will find the following sections, enclosed inside square brackets:

1. EMAIL ALERTS
2. QUARANTINE OPTIONS
3. SCAN OPTIONS
4. STATISTICAL ANALYSIS
5. MONITORING OPTIONS

Each of these sections contains several variables that indicate how LMD will behave and what features are available.

1. Set email_alert=1 if you want to receive email notifications of malware inspection results. For the sake of brevity, we will only relay mail to local system users, but you can explore other options such as sending mail alerts to the outside as well.
2. Set email_subj="Your subject here" and email_addr=username@localhost if you have previously set email_alert=1.

3. With quar_hits, the default quarantine action for malware hits (0 = alert only, 1 = move to quarantine & alert) you will tell LMD what to do when malware is detected.
4. quar_clean will let you decide whether you want to clean string-based malware injections. Keep in mind that a string signature is, by definition, “a contiguous byte sequence that potentially can match many variants of a malware family”.
5. quar_susp, the default suspend action for users with hits, will allow you to disable an account whose owned files have been identified as hits.
6. clamav_scan=1 will tell LMD to attempt to detect the presence of ClamAV binary and use as default scanner engine. This yields an up to four times faster scan performance and superior hex analysis. This option only uses ClamAV as the scanner engine, and LMD signatures are still the basis for detecting threats.

```
vi /usr/local/maldetect/conf.maldet
```

```
email_alert=1
email_addr=gacanepa@localhost
email_subj="Malware alerts for $HOSTNAME - $(date +%Y-%m-%d)"
quar_hits=1
```

```
quar_clean=1

quar_susp=1

clam_av=1
```

Update

```
sudo /usr/local/sbin/maldet -u
```

```
sudo /usr/local/sbin/maldet -d
```

Scan

```
sudo /usr/local/sbin/maldet -a
```

Lynis

```
sudo zypper -n install lynis
```

```
sudo lynis audit system
```

```
------------------------------------------------------------------
```

Reference :

https://hackertarget.com/clamav-tutorial-antivirus-linux/

https://software.opensuse.org/download/package?package=chkrootkit&project=security

https://www.tecmint.com/scan-linux-for-malware-and-rootkits/

https://squidclamav.darold.net/index.html