Install and configure LMD and Clam AntiVirus on CentOS 7 withou internet access

Thursday, November 29, 2018 17:10

Introduction

Linux Malware Detect is a malware detector and scanner for GNU/Linux, designed particularly for shared hosting environments. It is released under the GNU GPLv2 license, and it supports installation on cPanel WHM and GNU/Linux environments concurrently with other detection softwares like ClamAV.

This one is an open source antivirus solution to detect trojans, malware, viruses and other malicious software that supports multiple platforms, including Windows, MacOS, and GNU/Linux.

This tutorials explains how to install LMD and Clam Antivirus on a CentOS 7 server which has **no internet access**.

Mount CD-ROM

```
# mkdir /cdrom
# mount /dev/cdrom /cdrom/
```

Setup local repository based on CentOS iso

Check the guide of '**How To Create Local YUM repository on CentOS 7 / RHEL 7 using DVD**'.

Install LMD

Download LMD and extract it:

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

As root, run the installer script `install.sh` present in extracted directory:

```
# cd maldetect-x.x
# ./install.sh
```

If you see this error, '**could not find required binary perl, aborting**', use below command and re-install.

```
# yum install perl -y
```

If you see this error, '**{sigup} could not download signature data from server, please try again later.**', you can ignore it at this moment.

After installation, you can update the **/usr/local/maldetect/sigs/maldet.sigs.ver** from https://cdn.rfxn.com/downloads/maldet.sigs.ver.

You can execute **maldet --help** to verify the installation.

Configure LMD

LMD has been installed into `/usr/local/maldet/`. In that directory, there is a configuration file – we're going to modify it:

```
# $EDITOR /usr/local/maldetect/conf.maldet
```

Enable email alerts by changing the value to `1` on line 17 if needed.

email_alert="1"

Then, search for the email address line, and modify it as follow:

email_addr="root@mydomain.me"

ClamAV clamscan binary will be used as default scan engine; that's because it provides a high-performance scan on large file sets. To allow this, search and edit following line:

scan_clamscan="1"

Next, it's possible to enable quarantining to move malware to the quarantine during the scan process. To do this, change the following line:

quarantine_hits="1"

Next, enable clean based malware injections by changing:

quarantine_clean="1"

That's all for LMD configuration.

If you find sometimes maldet can not find any file even there files DO exist, it because those files belong to root user and will be ignored by default. You can change the set scan_ignore_root="0" to disable it.

Install ClamAV

Now that LMD is correctly installed and configured, let's install Clam AntiVirus to get the best scanning results. ClamAV rpm is available in the https://pkgs.org/. You need to download these rpm files, json-c + clamav-db + clamav. You need to install them follow the order.

After download and transfer to the server (The file names depend on the latest version you get):

```
# rpm -Uvh ./json-c-0.11-4.el7_0.x86_64.rpm
# rpm -Uvh ./clamav-db-0.100.2-5671.el7.art.x86_64.rpm
# rpm -Uvh ./clamav-0.100.2-5671.el7.art.x86_64.rpm
```

After ClamAV has been installed, we need to update the ClamAV virus databases.
Download **main.cvd**, **daily.cvd** and **bytecode.cvd**.
Put these files to **/var/lib/clamav** (If the directory does not exist then just create one)

Testing LMD and ClamAV

Now it's possible to test LMD with a manual scan.

Download some sample malware with wget or download on other PC and transfer to the directory:

```
# mkdir /home/{your user name}/virus-samples
# cd /home/{your user name}/virus-samples
# wget http://www.eicar.org/download/eicar.com.txt
# wget http://www.eicar.org/download/eicar_com.zip
# wget http://www.eicar.org/download/eicarcom2.zip
```

Next, it's possible to scan the directory, as previously said, with `maldet`:

```
# maldet -a /home/{your user name}/virus-samples
```

During this process, it's possible to see that LMD is using the ClamAV scanner engine to perform the scan: it will find three *malware hits*.

Check the report with the following command:

```
# maldet --report SCANID
```

SCANID is a numerical value found in the Maldet output.

Next, acquire a list of all reports:

```
# maldet -e list
```

Or "filter" files to scan. For instance, to scan files modified in the last 10 days:

```
# maldet -r /home/{your user name}/virus-samples 10
```

Monitoring only works against new files after being enabled. Those existing file will be not scanned by monitor.

Enable directory monitor (Have to install inotify-tools rpm which you can get from https://centos.pkgs.org). You also can check the monitor log in **/usr/local/maldetect/logs/inotify_log**

```
# maldet -m /home/{your user name}/virus-samples
```

Kill directory monitor

```
# maldet -k
```

Check the quarantine queue in **/usr/local/maldetect/quarantine**

Restore quarantined file

```
# maldet --restore /usr/local/maldetect/quarantine/eicar.com.txt.1271525999 (Restore sepcific file)
# maldet --restore 050910-1534.21135 (Restore from specific report)
```

For more information, just call the help with:

```
# maldet --help
```

that contains all options recognized by LMD.

There you go! That's one great way to protect from web server infections on a GNU/Linux system.

From <https://www.unixmen.com/lmd-and-clam-antivirus-centos-7/>