Exercises: ClamAV Install with Exim: PacNOG I Workshop

June 21, 2005

Note: The "#" and "$" characters before commands represents your system prompt and is not part of the command itself. "#" indicates a command issued as root while "$" indicates a command issued as a normal user.

Note 2: If you install software, update your environment as root and the change is not immediately available try typing `rehash` at the root shell prompt. This is only necessary when running a C shell (e.g., like /bin/csh).

Note 3: If you need to update ClamAV at some point you can read about this here:

> http://wiki.clamav.net/index.php/UpgradeInstructions

and here:

> http://www.freshports.org/security/clamav

Newer versions may be available at the FreshPorts site.

Note 4: These exercises are based on materials from Philip Hazel.

Basic ClamAV Installation using Ports

You need to be root to do this. Using ports downloads all the dependencies. Compilation may take some time to complete.

```
# cd /usr/ports/security/clamav
# make install
```

At this point, a dialog box pops up; use TAB to move to 'OK' (without selecting anything), then hit ENTER.

Once compilation finishes if you are using the C-shell, you must run the command:

```
# rehash
```

ClamAV needs its own user called *clamav*, which must be in the *mail* group so that it can access Exim's spool files (per installation of Exim via the ports system). The ports system created the user *clamav*, and it added this user to the *mail* group. You can verify this by typing:

```
# groups clamav
```

ClamAV has two daemons: one is the actual virus scanner, and the other (called *freshclam*) updates the virus database periodically over the Internet. New viruses are being created all the time. When you run anti-virus software, it is important to keep it updated. The *freshclam* daemon makes this very easy. It is also possible to run the *freshclam* command manually (see the man page for details).

The configuration files for the ClamAV daemons are */usr/local/etc/clamd.conf* and */usr/local/etc/freshclam.conf*. The ports system installs suitable defaults, so you do not need to change these files.

Before starting the two ClamAV daemons, you must edit */etc/rc.conf* to enable them:

```
# vi /etc/rc.conf
```

Add these lines to the file:

```
clamav_clamd_enable="YES"
clamav_freshclam_enable="YES"
```

The daemons should now start automatically whenever you reboot. Next time you reboot, check that the ClamAV daemons have started.

Now we can start the ClamAV daemons manually:

```
# /usr/local/etc/rc.d/clamav-clamd.sh start
# /usr/local/etc/rc.d/clamav-freshclam.sh start
```

If all has worked, we can now run some tests of the scanner. How can you test an anti-virus scanner? You don't want to be sending yourself a real virus! Luckily, a test virus called "eicar" exists. It consists of a short string of printing characters.

To test your scanner first create the file */tmp/eicar* that contains this string (you can do this as a non-root account):

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

The third character is the letter 'O', not the digit 0. To copy and past this, if you have web access, you can find this string here:

> http://www.eicar.org/anti_virus_test_file.htm

To do this you can do:

```
$ vi /tmp/eicar
```

Then paste the text above in the file and save the file:

```
1.) i   (for insert mode)
2.) Paste the text, or type it in. Don't hit RETURN/ENTER.
3.) ESC key, then press :wq to write the file and quit.
```

We can use the *clamdscan* command to check an individual file (or a directory of files) for viruses:

```
$ clamdscan /tmp/eicar
```

You should see output like this:

```
/tmp/eicar: Eicar-Test-Signature FOUND

----------- SCAN SUMMARY -----------
Infected files: 1
Time: 0.003 sec (0 m 0 s)
```

Now that we have ClamAV working, we can edit Exim's configuration so that every message is scanned for viruses.

Edit */usr/local/etc/exim/configure* (as root) and insert this line somewhere near the top, in the main section, before the first "begin" line (maybe right after "hostlist"):

```
av_scanner = clamd:/var/run/clamav/clamd
```

This option tells Exim where to find its anti-virus scanner: */var/run/clamav/clamd* is a socket that the ClamAV daemon creates for communication.

Now add some more lines to the **acl_check_data** ACL that you created earlier for SpamAassassin. Add these lines at the start:

```
  deny  message = This message contains \
                  a virus ($malware_name).
        malware = *
```

For reference, the entire ACL show now look like this:

```
acl_check_data:
  deny  message = This message contains \
                  a virus ($malware_name).
        malware = *
  warn  spam    = nobody
        message = X-is-spam: over spam threshold
  warn  message = X-Spam_score: $spam_score\n\
                  X-Spam_score_int: $spam_score_int\n\
                  X-Spam_bar: $spam_bar\n\
                  X-Spam_report: $spam_report
  accept
```

Now restart the Exim daemon in place to make sure that all updates are read:

```
# cat /var/run/exim.pid
# kill -HUP nnn
```

Where "nnn" is the process ID number from */var/run/exim.pid*.

Send yourself the eicar test string and see what happens (use copy-paste to copy the test data):

```
$ exim -bs

mail from:<>
rcpt to:<username@pcnn.pacnog.school.fj>
data
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
.
quit
```

You could also try using your MUA of choice to send the test virus to yourself as an attachment. If you do this, what happens?

Hervey Allen
Philip Hazel

Last modified: Wed Jun 15 10:52:32 CLT 2005