Metascan Email Relay

Matthew Ghafary

Written January 2014

1 Introduction

This python script is written for the Metascan student programming competition. This sits in front of a "real" mail server and scans incoming emails for attachments. If there are not attachments it simply forwards the emails. If there is one or more attachments then the attachment(s) will be sent to Metascan to be evaluated by **40** antivirus engines. When the results get back the email subject is modified to begin with any of these: [Clean], [Infected], [Scan Error]. The results of the "Clean" and "Infected" scans will attach a text file to the email to allow a user to review the information.

2 Requirements

- An actual email server (such as postfix).
- DNS Servers Setup to receive email through the internet. MX records need to point to the IP address of the email relay. Through domain registrar, web host, or self hosted name servers.
- Two seperate IP addresses. I am using two external IP addresses, with some "know how" one can probably set the "real" mailserver on an internal IP address. **NOTE:** I am not a postfix expert, but I believe it may possible to run both on a single IP address if one is careful to avoid port conflicts in the configuration of the mail relay and the actual server.

3 Installation Options

1. CentOS6 Install Script Method

This method will use a bash script to install the relay into /opt/metascan directory. It will also add the metascan relay to the rc.local init script to be run at system boot everytime.

2. Custom Installation
This requires python3 installed (I tested with version 3.3.3). It is the source file and can be adapted/placed anywhere one needs.

4 CentOS6 Install Script Method (Tested on 32-bit)

1. After you have downloaded the compressed file. Extract it using something like: tar -jxvf metascan_relay.tar.bz2
2. Make sure you have root privileges. Make setup.sh executable by running: chmod +x setup.sh
3. Now run it by doing: ./setup.sh
4. If all went well you should see the metascan_relay folder in /opt, and the /etc/rc.local file has a link to run the program at bootup.
5. Now just go into the /opt/metascan_relay directory and edit the config.ini
6. Now reboot and it should be running.

5 Custom Installation

- To run the script directly which leads to a lot more flexibility, one needs python3. This is not included by default in CentOS 6, so I used this link for instructions:

`http://toomuchdata.com/2012/06/25/how-to-install-python-2-7-3-on-centos-6-2/`

6 Configuration Options

config.ini file located in /opt/metascan_relay Or in same directory as the python file for custom installs.

LISTEN_ON
: The IP or hostname the email relay is to be run on.

LISTEN_ON_PORT
: The port to run the email relay on.

MAIL_SERVER_DEST
: Set to the smart SMTP server you want to send email to.

MAIL_SERVER_PORT

Set to the port the smart SMTP server is run on. If running on the same IP do not let it run on port 25.

NOTE: Metascan Email Relay does all its listening on port 25 by default.

DOMAIN_ACCEPTED

Make sure to put yourdomain.com with the @ symbol in front. So "@yourdomain.com"

MAX_EMAIL_SIZE

The email size in MB to take. I would set it about 2-3 MB over what you really want. For example if you want emails that are only size 15MB set it for 18MB.

META_SCAN_API_LINK

The Metascan link to use, should not need to change.

META_SCAN_API_KEY

Your personal Metascan API key.

SCAN_LOOKUP_SLEEP_TIME

How many seconds to wait in between polls to the scan server for results. Defaults to 5 seconds.

SCAN_MAX_LOOKUP_TIME

The maximum time to wait for total polls, If takes more than 30 seconds will still send email with error message. Defaults to 30 seconds.